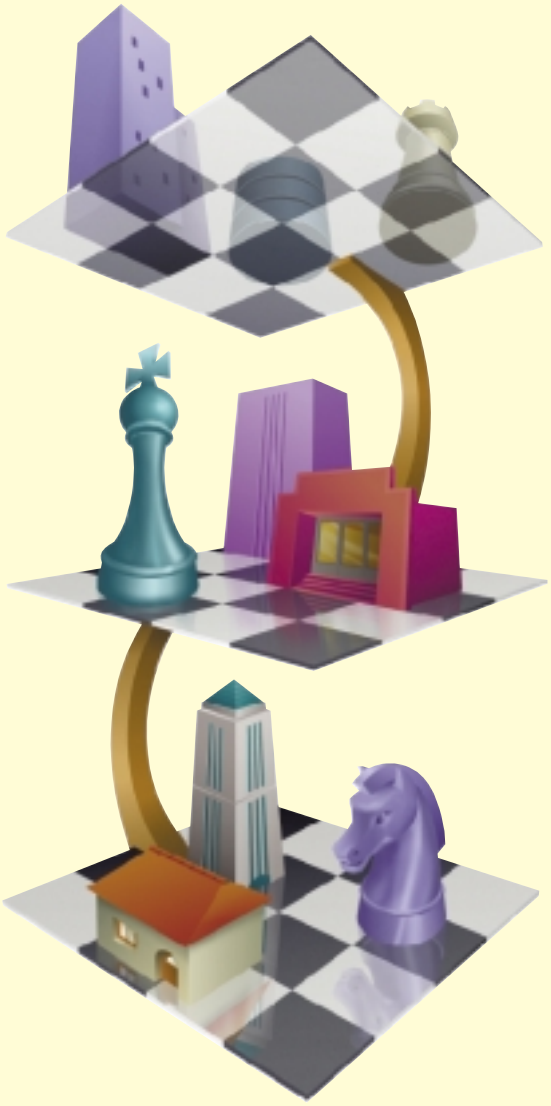


Решения компании Cisco Systems по обеспечению безопасности корпоративных сетей (издание II)

Cisco Systems

Empowering the Internet Generation℠

Содержание

Введение

В сетевой отрасли все большее распространение получает термин «безопасность сетей предприятия». Безопасность сетей является сложным вопросом отчасти из-за того, что в современном мире существует великое множество технологий безопасности, многие из которых решают сходные задачи и представляют собой лишь ступень на пути к более полным стратегическим решениям в данной области. В настоящем документе дается обзор технологий безопасности, который даст читателям общее представление о перспективах безопасности сетей и о том, как можно использовать продукты и средства компании Cisco для создания защищенных сетей предприятий. Этот документ может использоваться в сочетании с так называемыми «белыми книгами» (White Papers) Cisco и документацией, где детально описываются продукты и средства, упоминаемые в данном тексте.

В первом разделе поясняются элементарные термины и обсуждаются причины, приводящие к необходимости защиты современных сетей. Затем описываются базовые понятия криптографии и различные методы поддержки безопасности, которые широко применяются в современной промышленности. В настоящее время компания Cisco Systems уже поддерживает эти методы или работает над ними. Большинство из них — это стандартные методы, которые разработаны «инженерной группой Интернет» (Internet Engineering Task Force — IETF) и связаны с сетевым протоколом IP. Обычно, когда необходимо поддержать услуги в области безопасности для других сетевых протоколов, не имеющих подобных стандартных решений, используется метод туннелирования этих протоколов с помощью протокола IP. За обзором технологий следует детальное описание архитектуры обеспечения безопасности современных корпоративных сетей, а также разъяснения по поводу того, как продукты и функции операционной системы Cisco вписываются в архитектуру защищенной сети предприятия.

Терминология

Чтобы понять основы безопасности, необходимо прояснить терминологию, которая широко используется в данной области. Вот некоторые базовые термины и их определения:

Аутентификация: определение источника информации, то есть конечного пользователя или устройства (центрального компьютера, сервера, коммутатора, маршрутизатора и т. д.).
Целостность данных: обеспечение неизменности данных в ходе их передачи.
Конфиденциальность данных: обеспечение просмотра данных в приемлемом формате только для лиц, имеющих право на доступ к этим данным.
Шифрование: метод изменения информации таким образом, что прочитать ее не может никто, кроме адресата, который должен ее расшифровать.
Расшифровка: метод восстановления измененной информации и приведения ее в читаемый вид.
Ключ: цифровой код, который может использоваться для шифрования и расшифровки информации, а также для ее подписи.
Общий ключ: цифровой код, используемый для шифрования/расшифровки информации и проверки цифровых подписей; этот ключ может быть широко распространен; общий ключ используется с соответствующим частным ключом.
Частный ключ: цифровой код, используемый для шифрования/расшифровки информации и проверки цифровых подписей; владелец этого ключа должен держать его в секрете; частный ключ используется с соответствующим общим ключом.
Секретный ключ: цифровой код, совместно используемый двумя сторонами для шифрования и расшифровки данных.
Ключевой отпечаток пальца: читаемый код, который является уникальным для общего ключа и может использоваться для проверки подлинности его владельца.
Хэш-функция: математический расчет, результатом которого является последовательность битов (цифровой код). Имея этот результат, невозможно восстановить исходные данные, использованные для расчета.
Хэш: последовательность битов, полученная в результате расчета хэш-функции.
Результат обработки сообщения (Message digest): величина, выдаваемая хэш-функцией (то же, что и «хэш»).
Шифр: любой метод шифрования данных.
Цифровая подпись: последовательность битов, прилагаемая к сообщению (зашифрованный хэш), которая обеспечивает аутентификацию и целостность данных.
AAA — Authentication, Authorization, Accounting: архитектура аутентификации, авторизации и учета компании Cisco Systems.
Кампус: группа или комплекс рядом расположенных зданий предприятия или организации.
NAS — Network Access Server: сервер удаленного доступа к сети.
VLAN — Virtual Local Area Networks: виртуальные локальные сети.
VPN — Virtual Private Networks: виртуальные частные сети.
VPDN — Virtual Private Dial-Up Networks: виртуальные коммутируемые частные сети.

Основы безопасности данных

В этом разделе описаны основные «строительные кирпичики», необходимые для понимания более сложных технологий безопасности. Криптография является основой любой защищенной связи, и поэтому так важно познакомиться с тремя основными криптографическими функциями: симметричным шифрованием, асимметричным шифрованием и односторонними хэш-функциями. Все существующие технологии аутентификации, целостности и конфиденциальности созданы на основе именно этих трех функций. Цифровые подписи будут представлены в виде практического примера сочетания асимметричного шифрования с алгоритмом односторонней хэш-функции для поддержки аутентификации и целостности данных.

Криптография

Криптографией называется наука составления и расшифровки закодированных сообщений. Кроме того, криптография является важным строительным кирпичиком для механизмов аутентификации, целостности и конфиденциальности. Аутентификация является средством подтверждения личности отправителя или получателя информации. Целостность означает, что данные не были изменены, а конфиденциальность создает ситуацию, при которой данные не может понять никто, кроме их отправителя и получателя. Обычно криптографические механизмы существуют в виде алгоритма (математической функции) и секретной величины (ключа). Алгоритмы широко известны. В секрете необходимо держать только ключи. Ключ можно сравнить с номерным кодом для номерного замка. Хотя общая концепция номерного замка хорошо известна, вы не сможете открыть такой замок, если не знаете, какой код следует набрать. И чем больше разрядов у этого кода, тем дольше нужно потрудиться, чтобы подобрать его методом простого перебора. То же самое можно сказать и о криптографических ключах: чем больше битов в таком ключе, тем менее он уязвим.

Аутентификация, целостность данных и конфиденциальность данных поддерживаются тремя типами криптографических функций: симметричным шифрованием, асимметричным шифрованием и хэш-функциями.

Симметричное шифрование

Симметричное шифрование, которое часто называют шифрованием с помощью секретных ключей, в основном используется для обеспечения конфиденциальности данных. На рисунке 1 показаны два пользователя, Алиса и Боб, которые хотят установить между собой конфиденциальную связь. Для этого Алиса и Боб должны совместно выбрать единый математический алгоритм, который будет использоваться для шифрования и расшифровки данных. Кроме того, им нужно выбрать общий ключ (секретный ключ), который будет использоваться с принятым ими алгоритмом шифрования/расшифровки.

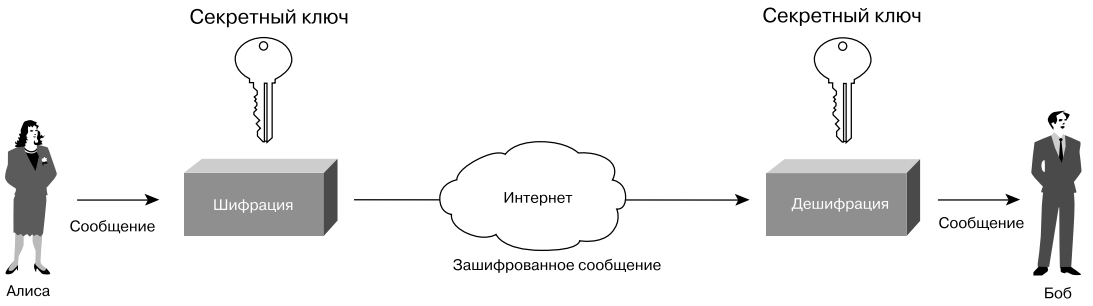


Рисунок 1. Шифрование секретным ключом

Весьма упрощенным примером алгоритма секретного ключа является так называемый шифр Цезаря, показанный на рисунке 2. Этот метод шифрования заключается в том, что каждая буква в тексте заменяется на другую букву, находящуюся на определенном расстоянии от нее в алфавите. При шифровании или расшифровке этот алгоритм как бы сдвигает буквы вверх и вниз по алфавиту. Ключом в этом примере являются три буквы.

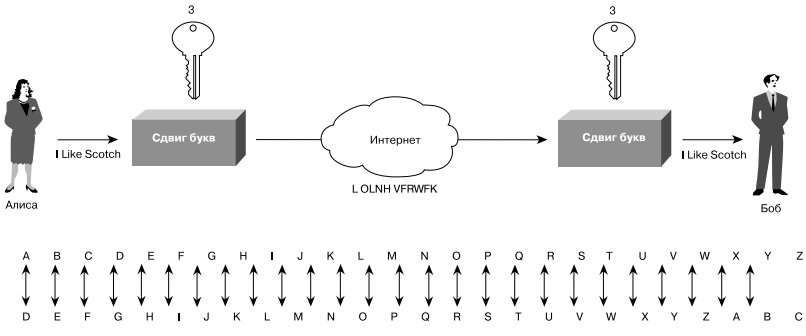


Рисунок 2. Шифр Цезаря

Совершенно ясно, что если кто-нибудь получит зашифрованное этим способом сообщение и будет знать алгоритм (куда сдвигать буквы — вверх или вниз по алфавиту), он сможет легко раскрыть ключ методом простого перебора, который заключается в том, что человек перебирает все возможные комбинации алгоритма до тех пор, пока не получит в результате расшифрованный текст. Обычно, чем длиннее ключ и чем сложнее алгоритм, тем труднее решить задачу расшифровки простым перебором вариантов.

Сегодня широко используются такие алгоритмы секретных ключей, как Data Encryption Standard (DES), 3DES (или «тройной DES») и International Data Encryption Algorithm (IDEA). Эти алгоритмы шифруют сообщения блоками по 64 бита. Если объем сообщения превышает 64 бита (как это обычно и бывает), необходимо разбить его на блоки по 64 бита в каждом, а затем каким-то образом свести их воедино. Такое объединение, как правило, происходит одним из следующих четырех методов: электронной кодовой книги (ECB), цепочки зашифрованных блоков (CBC), x-битовой зашифрованной обратной связи (CFB-x) или выходной обратной связи (OFB).

Шифрование с помощью секретного ключа чаще всего используется для поддержки конфиденциальности данных и очень эффективно реализуется с помощью неизменяемых «вшитых» программ (firmware). Этот метод можно использовать для аутентификации и поддержания целостности данных, но метод цифровой подписи (о котором мы скажем позже) является более эффективным. С методом секретных ключей связаны следующие проблемы:

- Необходимо часто менять секретные ключи, поскольку всегда существует риск их случайного раскрытия.
- Трудно обеспечить безопасное генерирование и распространение секретных ключей.

Для получения и безопасного распространения секретных ключей обычно используется алгоритм Диффи-Хеллмана (Diffie-Hellman), который описывается ниже.

Асимметричное шифрование

Асимметричное шифрование часто называют шифрованием с помощью общего ключа, при котором используются разные, но взаимно дополняющие друг друга ключи и алгоритмы шифрования и расшифровки. Этот механизм полагается на два взаимосвязанных ключа: общий ключ и частный ключ. Если Алиса и Боб хотят установить связь с использованием шифрования через общий ключ, обоим нужно получить два ключа: общий и частный (см. рисунок 3). Для шифрования и расшифровки данных Алиса и Боб будут пользоваться разными ключами.

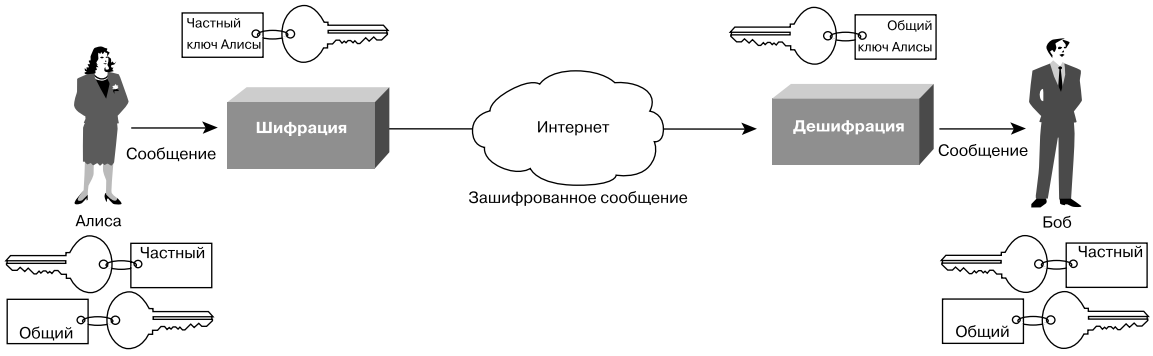


Рисунок 3. Шифрование с помощью общего ключа

Вот некоторые наиболее типичные цели использования алгоритмов общих ключей:

- обеспечение конфиденциальности данных;
- аутентификация отправителя;
- безопасное получение общих ключей для совместного использования.

Чтобы лучше понять, как достигается конфиденциальность данных и проводится аутентификация отправителя, пройдем по всему процессу шаг за шагом. Сначала и Алиса, и Боб должны создать свои пары общих/частных ключей. После создания таких пар Алиса и Боб должны обменяться своими общими ключами.

На рисунке 4 показано, как шифрование с помощью общих ключей обеспечивает конфиденциальность информации. Если Алиса хочет отправить Бобу конфиденциальные данные (другими словами, если она хочет, чтобы никто, кроме Боба, не смог их прочесть), она шифрует данные с помощью общего ключа Боба и отправляет Бобу данные, зашифрованные этим способом. Получив сообщение от Алисы, Боб расшифровывает его с помощью своего частного ключа. Так как никто, кроме Боба, не имеет этого частного ключа, данные, отправленные Алисой, может расшифровать только Боб. Таким образом поддерживается конфиденциальность данных.

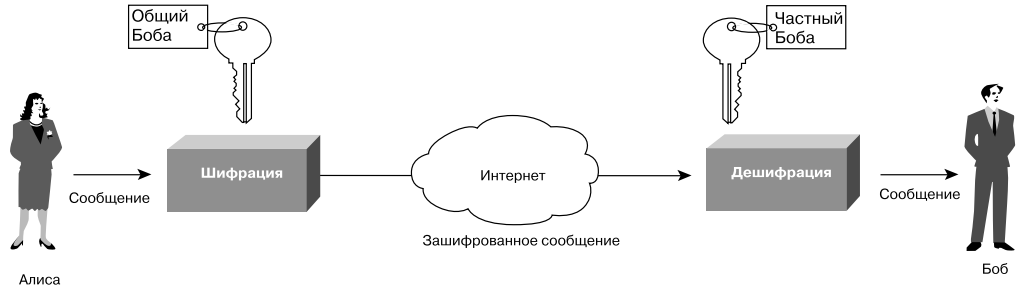


Рисунок 4. Конфиденциальность данных, зашифрованных с помощью общего ключа

На рисунке 5 показано, как шифрование с помощью общего ключа помогает проводить аутентификацию отправителя. Боб хочет быть уверен, что сообщение отправлено именно Алисой, а не человеком, который выдает себя за нее. Поскольку общий ключ не является секретным, доступ к нему может получить кто угодно. Но если Алиса зашифрует сообщение своим частным ключом, Боб должен расшифровать его с помощью общего ключа Алисы. Аутентификация происходит потому, что доступ к частному ключу Алисы имеет только она одна, и поэтому данные могли быть зашифрованы только ею.

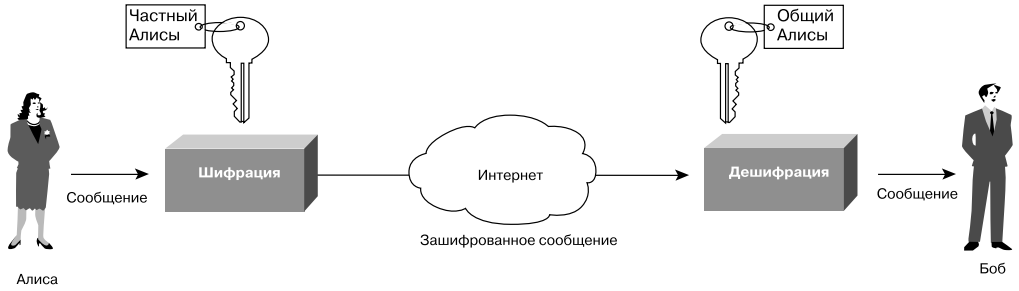


Рисунок 5. Аутентификация отправителя с помощью шифрования общим ключом

Важным аспектом асимметричного шифрования является то, что частный ключ должен храниться в тайне. Если частный ключ будет раскрыт, то человек, знающий этот ключ, сможет выступать от вашего имени, получать ваши сообщения и отправлять сообщения так, будто это делаете вы.

Механизмы генерирования пар общих/частных ключей являются достаточно сложными, но в результате получаются пары очень больших случайных чисел, одно из которых становится общим ключом, а другое — частным. Генерирование таких чисел требует больших процессорных мощностей, поскольку эти числа, а также их произведения должны отвечать строгим математическим критериям. Однако этот процесс генерирования абсолютно необходим для обеспечения уникальности каждой пары общих/частных ключей. Алгоритмы шифрования с помощью общих ключей редко используются для поддержки конфиденциальности данных из-за ограничений производительности. Вместо этого их часто используют в приложениях, где аутентификация проводится с помощью цифровой подписи и управления ключами.
Среди наиболее известных алгоритмов общих ключей можно назвать RSA (Ривест, Шамир, Адельман) и ElGamal.

Безопасные хэш-функции

Безопасной хэш-функцией называется функция, которую легко рассчитать, но обратное восстановление которой требует непропорционально больших усилий. Входящее сообщение пропускается через математическую функцию (хэш-функцию), и в результате на выходе мы получаем некую последовательность битов. Эта последовательность называется «хэш» (или «результат обработки сообщения»). (См. рисунок 6.) Этот процесс невозможно восстановить. Другими словами, имея выходные данные, невозможно получить входные. Хэш-функцию можно сравнить с кофемолкой. Если сообщение — это кофейные зерна, а хэш на выходе — это размолотый кофе, то, имея такой размолотый кофе, вы не сможете восстановить кофейные зерна.

Рисунок 6. Хэш-функция

Хэш-функция принимает сообщение любой длины и выдает на выходе хэш фиксированной длины. Обычные хэш-функции включают:

- алгоритм Message Digest 4 (MD4);
- алгоритм Message Digest 5 (MD5);
- алгоритм безопасного хэша (Secure Hash Algorithm — SHA).

Применения технологии шифрования

Технология шифрования часто используется в приложениях, связанных с управлением ключами и аутентификацией. Эти приложения описаны ниже.

Алгоритм Диффи-Хеллмана

Алгоритм Диффи-Хеллмана позволяет двум сторонам, Алисе и Бобу, создать общий для них секретный ключ, известный только им двоим, несмотря на то, что связь между ними осуществляется по незащищенному каналу. Затем этот секретный ключ используется для шифрования данных с помощью алгоритма секретного ключа. На рисунке 7 показан пример использования алгоритма Диффи-Хеллмана в сочетании с алгоритмом DES для создания секретных ключей и последующего использования этих ключей для поддержки конфиденциальности данных. Два числа, p (простое число) и g (меньшее, чем p, но с некоторыми исключениями), используются совместно. И Алиса, и Боб генерируют (каждый для себя) большое случайное число. Эти числа (XA и XB) держатся в секрете. Далее используется алгоритм Диффи-Хеллмана. И Алиса, и Боб проводят вычисления с помощью этого алгоритма и обмениваются их результатами. Окончательным результатом является общая величина Z. Этот ключ Z используется как ключ DES для шифрования и расшифровки данных. Человек, который знает величину p или g, не сможет легко рассчитать общую величину Z из-за трудностей с факторизацией очень больших простых чисел.

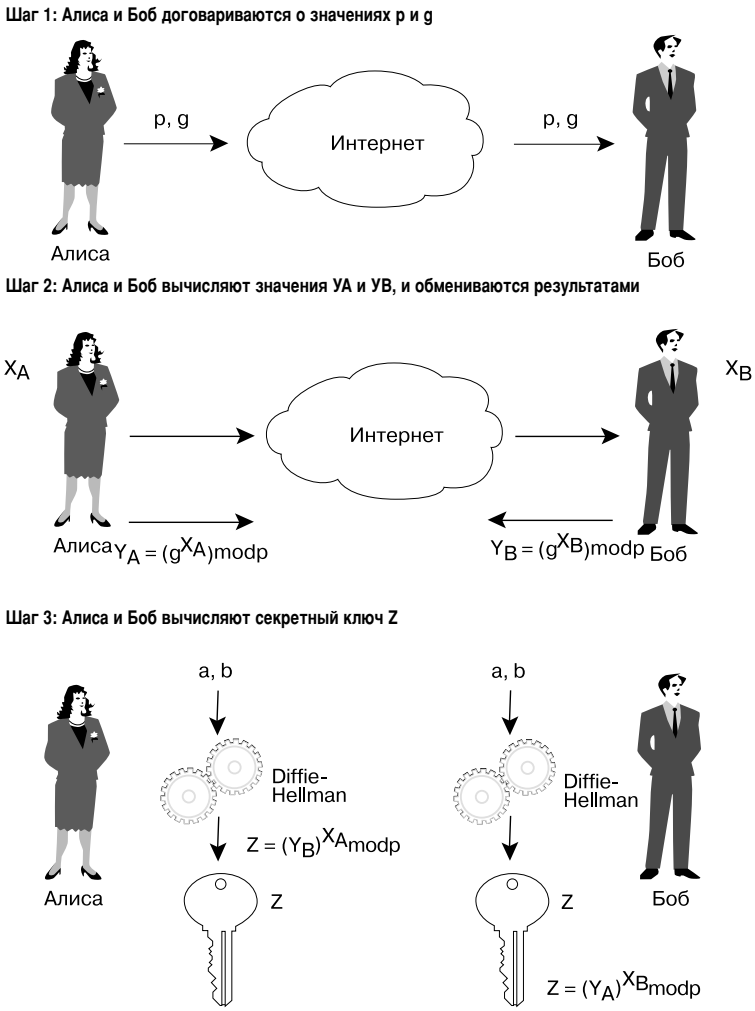


Рисунок 7. Алгоритм Диффи-Хеллмана с ключом DES

Важно отметить, что на сегодня пока не создано средств для определения автора такого ключа, поэтому обмен сообщениями, зашифрованными этим способом, может подвергаться хакерским атакам. Алгоритм Диффи-Хеллмана используется для поддержки конфиденциальности данных, но не используется для аутентификации. Аутентификация в данном случае достигается с помощью цифровой подписи.

Цифровые подписи

Цифровая подпись представляет собой зашифрованный хэш, который добавляется к документу. Она может использоваться для аутентификации отправителя и целостности документа. Цифровые подписи можно создавать с помощью сочетания хэш-функций и криптографии общих ключей. На рисунке 8 показан пример создания цифровой подписи. Сначала Алиса и Боб должны договориться об алгоритме шифрования общим ключом (например, Digital Signature Standard — DSS), создать пары общих/частных ключей и обменяться своими общими ключами. Им также нужно прийти к согласию о том, какую хэш-функцию использовать для создания цифровых подписей и их проверки. Предположим, что выбран алгоритм MD5. Алиса берет оригинальный документ и подает его на вход MD5, получая на выходе блок длиной в 128 бит. Эти выходные данные называются результатом обработки сообщения (хэшем документа). Алиса зашифровывает этот хэш с помощью сво-

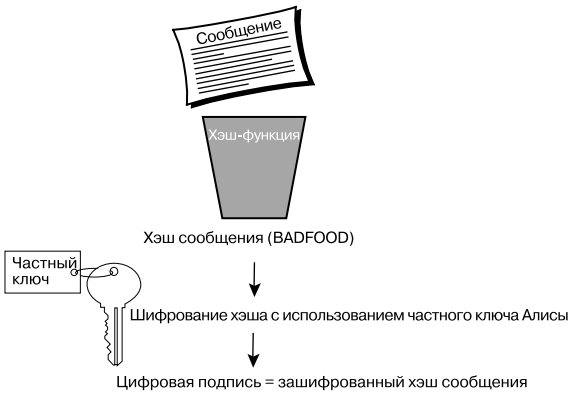


Рисунок 8. Создание цифровой подписи

его частного ключа. Этот зашифрованный хэш является цифровой подписью, которая прибавляется к тексту оригинального документа.

Сообщение, которое Алиса отправляет Бобу, будет состоять из документа как такового и цифровой подписи. На рисунке 9 показано, как происходит проверка цифровой подписи. На другом конце канала связи Боб получает сообщение и делит его на оригинальный документ и цифровую подпись. Так как цифровая подпись была зашифрована частным ключом Алисы, Боб может провести расшифровку с помощью ее общего ключа. Теперь у Боба есть расшифрованный хэш. Далее Боб подает текст документа на вход той же функции, которую использовала Алиса. Если на выходе Боб получит тот же хэш, который прислала в своем сообщении Алиса, целостность документа и личность отправителя можно считать доказанными.

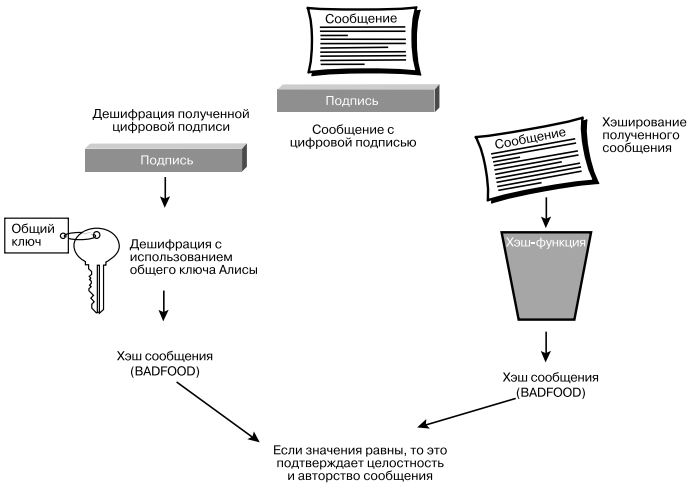


Рисунок 9. Проверка цифровой подписи

Цифровые сертификаты

Цифровым сертификатом называется сообщение с цифровой подписью, которое в настоящее время обычно используется для подтверждения действительности общего ключа. На рисунке 10 показан пример цифрового сертификата в стандартном формате X.509. Общий формат сертификата X.509 включает следующие элементы:

- номер версии;
- серийный номер сертификата;
- эмитент информации об алгоритме;
- эмитент сертификата;
- даты начала и окончания действия сертификата;
- информацию об алгоритме общего ключа субъекта сертификата;
- подпись эмитирующей организации.

Цифровой сертификат содержит:
– Серийный номер сертификата
– Используемые алгоритмы
– Срок действия
– Информацию об общем ключе пользователя
– Подпись организации, выдавшей сертификат

0000123
SHA, DH, 3837829
1/1/93 to 12/31/99
Alice Smith, Acme Corp.
DH, 3813710
Acme Corporation Security Dept.
SHA, DH, 239702317 …

Рисунок 10. Пример сертификата X.509

Эмитирующая организация, назовем ее CA, является надежной третьей стороной, которой вы полностью доверяете. На рисунке 11 показано, что Боб, прежде чем отправить данные Алисе, хочет проверить ее общий ключ с помощью CA. Алиса имеет действующий сертификат, который хранится в CA. Боб запрашивает у CA цифровой сертификат Алисы. CA подписывает сертификат своим частным ключом. Боб имеет доступ к общему ключу CA и может убедиться в том, что сертификат, подписанный CA, является действительным. Так как сертификат Алисы содержит ее общий ключ, Боб получает «заверенную» версию общего ключа Алисы.

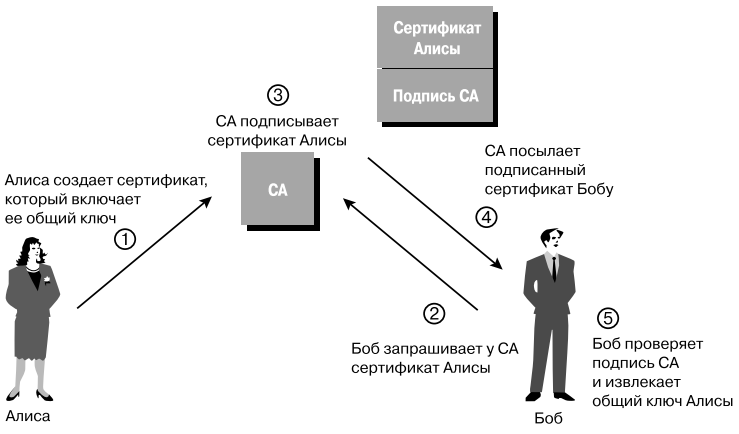


Рисунок 11. Получение цифрового сертификата

Заметим, что для реализации этой схемы необходима надежная система распространения общего ключа CA среди пользователей. В настоящее время создание больших инфраструктур, пользующихся общими ключами (PKI), сопряжено с трудностями, так как ряд вопросов, связанных с такими инфраструктурами, остается нерешенным. Еще предстоит разработать эффективные процедуры отзыва и изменения сертификатов, а также определить, как обращаться с иерархиями CA, где разные пользователи могут полагаться на услуги разных CA. Тем не менее все эти вопросы постепенно решаются.

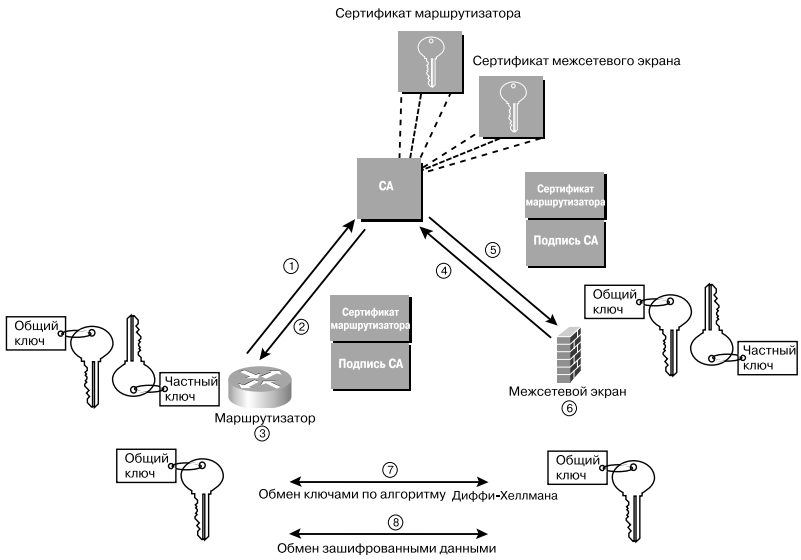


Рисунок 12. Безопасная связь с использованием шифрования

Рассмотрим простой сценарий безопасной связи с использованием шифрования, который показан на рисунке 12.

Маршрутизатор и межсетевой экран имеют по одной паре общих/частных ключей. Предположим, что CA удалось получить сертификаты X.509 для маршрутизатора и межсетевого экрана по защищенным каналам. Далее предположим, что маршрутизатор и межсетевой экран тоже получили копии общего ключа CA по защищенным каналам. Теперь, если на маршрутизаторе имеется трафик, предназначенный для межсетевого экрана, и если маршрутизатор хочет обеспечить аутентификацию и конфиденциальность данных, необходимо предпринять следующие шаги:

1. Маршрутизатор отправляет в CA запрос на получение общего ключа межсетевого экрана.
2. CA отправляет ему сертификат межсетевого экрана, зашифрованный частным ключом CA.
3. Маршрутизатор расшифровывает сертификат общим ключом CA и получает общий ключ межсетевого экрана.
4. Межсетевой экран направляет CA запрос на получение общего ключа маршрутизатора.
5. CA отправляет ему сертификат маршрутизатора, зашифрованный частным ключом CA.
6. Межсетевой экран расшифровывает сертификат общим ключом CA и получает общий ключ маршрутизатора.
7. Маршрутизатор и межсетевой экран используют алгоритм Диффи-Хеллмана и шифрование с помощью общих ключей для аутентификации.
8. С помощью секретного ключа, полученного в результате использования алгоритма Диффи-Хеллмана, маршрутизатор и межсетевой экран проводят обмен конфиденциальными данными.

Технологии безопасности данных

Существует множество технологий безопасности, и все они предлагают решения для важнейших компонентов политики в области защиты данных: аутентификации, поддержания целостности данных и активной проверки. Мы определяем аутентификацию как аутентификацию пользователя или конечного устройства (клиента, сервера, коммутатора, маршрутизатора, межсетевого экрана и т. д.) и его местоположения с последующей авторизацией пользователей и конечных устройств. Целостность данных включает такие области, как безопасность сетевой инфраструктуры, безопасность периметра и конфиденциальность данных. Активная проверка помогает удостовериться в том, что установленная политика в области безопасности выдерживается на практике, и отследить все аномальные случаи и попытки несанкционированного доступа. В следующем разделе описаны технологии безопасности, которые часто применяются для аутентификации и поддержания целостности данных в сети, и продукты компании Cisco, которые уже поддерживают или должны в будущем поддерживать эти технологии. Мы хотим, чтобы читатель понял область применения каждой из этих технологий, но не будем глубоко вдаваться в их технические особенности. Все эти технологии уже стандартизированы IETF, либо находятся в процессе стандартизации, поэтому для получения технических деталей и самых последних данных вы можете обратиться на web-страницу IETF по адресу: http://www.ietf.org.

Технологии аутентификации

В этом разделе описываются основные технологии, которые используются для аутентификации центрального компьютера, конечного пользователя или и того, и другого. Первым шагом на пути аутентификации было использование паролей, но для поддержания высокого уровня безопасности пароли прихо-

дится часто менять. Методы использования одноразовых паролей применяются по-прежнему широко. Среди них можно упомянуть методы аутентификации по протоколу S/Key или при помощи специальных аппаратных средств (token password authentication). Механизм аутентификации по протоколу Point-to-Point Protocol (PPP) часто применяется в среде модемного доступа и включает использование протоколов Password Authentication Protocol (PAP), Challenge Handshake Protocol (CHAP) и Extensible Authentication Protocol (EAP). Разработка протокола EAP все еще продолжается, но уже сейчас он дает возможность более гибкого использования существующих и только появляющихся технологий аутентификации в каналах PPP. TACACS+ и Remote Access Dial-In User Service (RADIUS) — это протоколы, которые поддерживают масштабируемые решения в области аутентификации.

S/Key

Система одноразовых паролей S/Key, определенная в RFC 1760, представляет собой систему генерирования одноразовых паролей на основе стандартов MD4 и MD5. Она предназначена для борьбы с так называемыми «повторными атаками», когда хакер подслушивает канал, выделяет из трафика аутентификатор пользователя и его пароль и в дальнейшем использует их для несанкционированного доступа.
Система S/Key основана на технологии клиент/сервер, где клиентом обычно является персональный компьютер, а сервером — сервер аутентификации. Вначале и клиента, и сервер нужно настроить на единую парольную фразу и счет итерации. Клиент начинает обмен S/Key, отправляя серверу пакет инициализации, а сервер в ответ отправляет порядковый номер и случайное число, так называемое «зерно» (seed). После этого клиент генерирует одноразовый пароль в ходе операции, состоящей из трех этапов: подготовительного этапа, этапа генерирования и функции выхода.

На подготовительном этапе клиент вводит секретную парольную фразу любой длины (рекомендуется длина более восьми знаков). Парольная фраза соединяется с «зерном», полученным от сервера в незашифрованном виде. Это несекретное «зерно» дает клиенту возможность использовать одну и ту же парольную фразу на множестве машин (с разными «зернами») и повторно использовать пароли, заменяя «зерно».

Далее, на этапе генерирования, клиент многократно использует хэш-функцию и получает 64-разрядную итоговую величину. При каждом новом использовании количество хэш-циклов уменьшается на один, создавая тем самым уникальную последовательность генерируемых паролей. Для совместимости клиента и сервера они должны использовать одну и ту же защищенную хэш-функцию.

Функция выхода воспринимает 64-разрядный одноразовый пароль и переводит его в читаемую форму. Далее этот пароль может вводиться следующими способами:

- через программу-калькулятор, которая будет включать пароль в поток данных;
- с помощью функции вырезания и сбрасывания (cut and paste);
- с помощью ручного ввода.

В случае ручного ввода одноразовый пароль превращается в последовательность из шести коротких английских слов (от одной до четырех букв каждое). Эти слова выбираются из словаря, в который входит 2048 слов. Таким образом, на одно слово приходится по 11 бит, что позволяет кодировать любые одноразовые пароли. Для совместимости систем S/Key и калькуляторов все они должны пользоваться одним и тем же словарем.

После создания одноразового пароля его нужно проверить. Для этого клиент передает одноразовый пароль на сервер, где он и проверяется. На сервере есть файл (в системе UNIX это /etc/skeykeys), в котором хранится одноразовый пароль, использованный в последнем успешном сеансе связи с каждым отдельным пользователем. Кроме того, эта запись может инициализироваться с помощью ввода первого одноразового пароля из данной последовательности с помощью команды keyinit (название этой команды в разных версиях системы может быть разным). Для проверки аутентификации система однократно пропускает полученный одноразовый пароль через защищенную хэш-функцию. Если результат этой операции совпадает с предыдущим паролем, хранящимся в файле, результат аутентификации считается положительным, а новый пароль сохраняется для дальнейшего использования. Поскольку количество хэш-циклов, которые использует клиент, постоянно сокращается, в какой-то момент пользователю придется инициализировать систему. Это достигается с помощью команды keyinit, которая дает возможность изменить секретную парольную фразу, количество циклов итерации и «зерно».

На рисунке 13 показано, как действует система одноразовых паролей S/Key у пользователя, который пытается подключиться через Telnet к конкретной UNIX-машине, которая одновременно является сервером S/Key.

Более подробную информацию о технологии одноразовых паролей можно получить у рабочей группы IETF, занимающейся этим вопросом (One-Time Password (OTP) Authentication Working Group). Адрес группы:
http://www.ietf.org/html.charters/otp-charter.html.

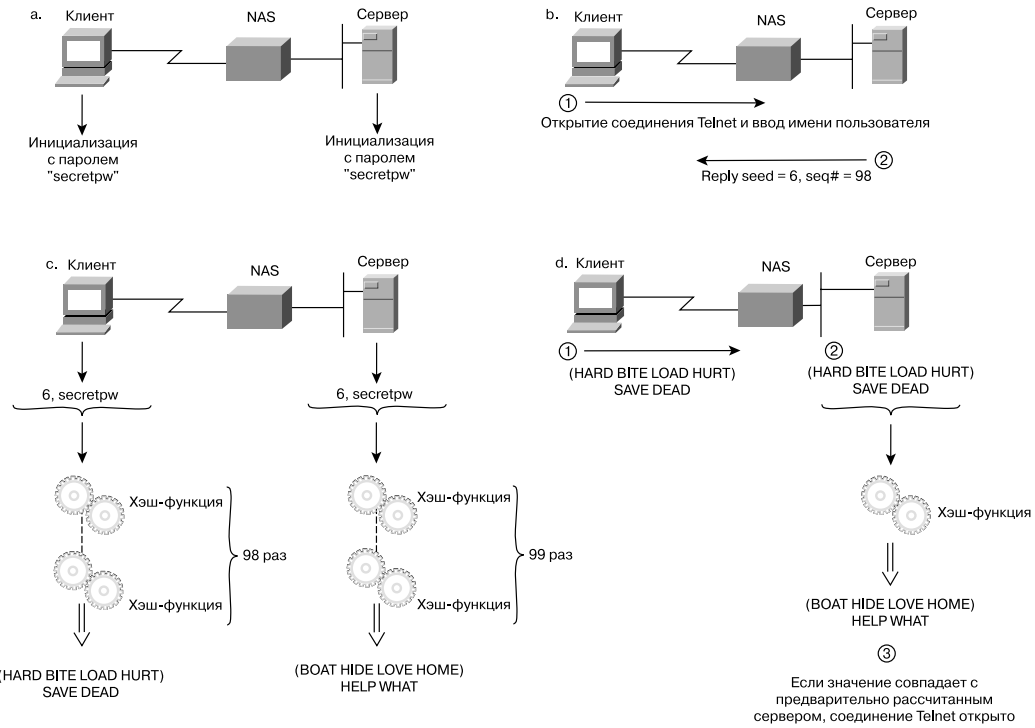


Рисунок 13. Функционирование системы S/Key

Аутентификация с помощью аппаратных средств (Token Password Authentication)

Аутентификация с помощью аппаратных средств работает по одной из двух альтернативных схем: по схеме запрос-ответ или по схеме аутентификации с синхронизацией по времени. В схеме запрос-ответ пользователь подключается к серверу аутентификации, который в свою очередь предлагает ввести персональный аутентификационный номер (PIN) или пользовательский аутентификатор (user ID). Пользователь передает PIN или user ID на сервер, который затем делает «запрос» (передает случайное число, которое появляется на экране пользователя). Пользователь вводит это число в специальное аппаратное устройство, похожее на кредитную карточку, где число запроса шифруется с помощью пользовательского шифровального ключа. Результат шифрования отображается на экране. Пользователь отправляет этот результат на сервер аутентификации. В то время как пользователь подсчитывает этот результат, сервер аутентификации рассчитывает этот же результат самостоятельно, используя для этого базу данных, где хранятся все пользовательские ключи. Получив ответ от пользователя, сервер сравнивает его с результатом собственных вычислений. Если оба результата совпадают, пользователь получает доступ к сети. Если результаты оказываются разными, доступ к сети не предоставляется.

При использовании схемы с синхронизацией по времени на аппаратном устройстве пользователя и на сервере работает секретный алгоритм, который через определенные синхронизированные промежутки времени генерирует идентичные пароли и заменяет старые пароли на новые. Пользователь подключается к серверу аутентификации, который запрашивает у пользователя код доступа. После этого пользователь вводит свой PIN в аппаратное карточное устройство, и в результате на экран выводится некоторая величина, которая представляет собой одноразовый пароль. Этот пароль и отправляется на сервер. Сервер сравнивает его с паролем, который был вычислен на самом сервере. Если пароли совпадают, пользователь получает доступ к сети.

Аутентификация PPP

PPP — это популярное средство инкапсуляции (упаковки), которое часто используется в глобальных сетях. В его состав входят три основных компонента:

- метод инкапсуляции датаграмм в последовательных каналах;
- протокол Link Control Protocol (LCP), который используется для установления, конфигурирования и тестирования связи;
- семейство протоколов Network Control Protocols (NCP) для установки и конфигурирования различных протоколов сетевого уровня.

Чтобы установить прямую связь между двумя точками по каналу PPP, каждая из этих точек должна сначала отправить пакеты LCP для конфигурирования связи на этапе ее установления. После установления

связи и, прежде чем перейти к этапу работы на протоколах сетевого уровня, протокол PPP дает (при необходимости) возможность провести аутентификацию.

По умолчанию аутентификация является необязательным этапом. На случай, если аутентификация потребуется, в момент установления связи система указывает дополнительную конфигурацию протоколов аутентификации. Эти протоколы используются, в основном, центральными компьютерами и маршрутизаторами, которые связаны с сервером PPP через коммутируемые каналы или линии телефонной связи, а возможно, и через выделенные каналы. Во время согласования на сетевом уровне сервер может выбрать опцию аутентификации центрального компьютера или маршрутизатора.

PAP и CHAP представляют собой два метода аутентификации соединения PPP. EAP — это общий протокол аутентификации PPP, который поддерживает множество аутентификационных механизмов. Этот протокол находится в процессе доработки, и в будущем он сможет поддерживать более современные механизмы аутентификации в рамках аутентификации PPP. Аутентификация происходит после согласования LCP и до согласования IP Control Protocol (IPCP), в ходе которого происходит обмен адресами IP. Этот процесс аутентификации проходит в автоматическом режиме и не требует от пользователей ввода в компьютер каких-либо данных при подключении PPP. Часто аутентификация PAP или CHAP занимает место переговорного сценария, который отвечает на запросы о вводе сетевого имени пользователя (login) и пароля. CHAP поддерживает более высокий уровень безопасности, поскольку не передает реальный пароль по каналу PPP. Однако PAP используется чаще. Ниже приводится упрощенный обзор этих трех протоколов. Более подробные технические детали и самую свежую информацию можно получить в рабочей группе IETF по расширениям PPP (pppext) по адресу:
http://www.ietf.org/html.charters/pppext-charter.html.

Протокол PPP PAP

На рисунке 14 показаны действия по аутентификации с использованием протокола PAP.
Маршрутизатор отделения пытается провести аутентификацию сервера сетевого доступа (NAS) или «аутентификатора». По завершении этапа установления связи маршрутизатор передает пару «аутентификатор-пароль» серверу NAS до тех пор, пока аутентификация не будет проведена или пока связь не прервется.

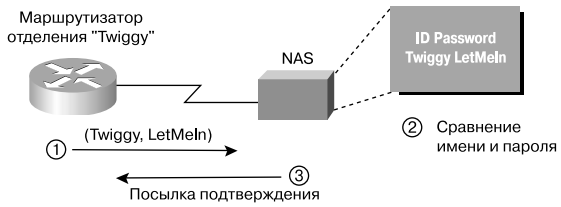


Рисунок 14. Аутентификация PPP PAP

PAP не является сильным аутентификационным методом. PAP аутентифицирует только вызывающего оператора, а пароли пересылаются по каналу, который считается уже «защищенным». Таким образом, этот метод не дает защиты от использования чужих паролей и неоднократных попыток подбора пароля. Частота и количество неудачных попыток входа в сеть контролируются на уровне вызывающего оператора.

Протокол PPP CHAP

CHAP используется для периодической аутентификации центрального компьютера или конечного пользователя с помощью согласования по трем параметрам. Аутентификация происходит в момент установления связи, но может повторяться и после ее установления.

На рисунке 15 показан процесс аутентификации CHAP.

Маршрутизатор отделения пытается провести аутентификацию сервера сетевого доступа (NAS) или «аутентификатора». CHAP обеспечивает безопасность сети, требуя от операторов обмена «текстовым секретом». Этот секрет никогда не передается по каналу связи. По завершении этапа установления связи аутентификатор передает вызывающей машине запрос, который состоит из аутентификатора (ID), случайного числа и имени центрального компьютера (для местного устройства) или имени пользователя (для удаленного устройства). Вызывающая машина проводит

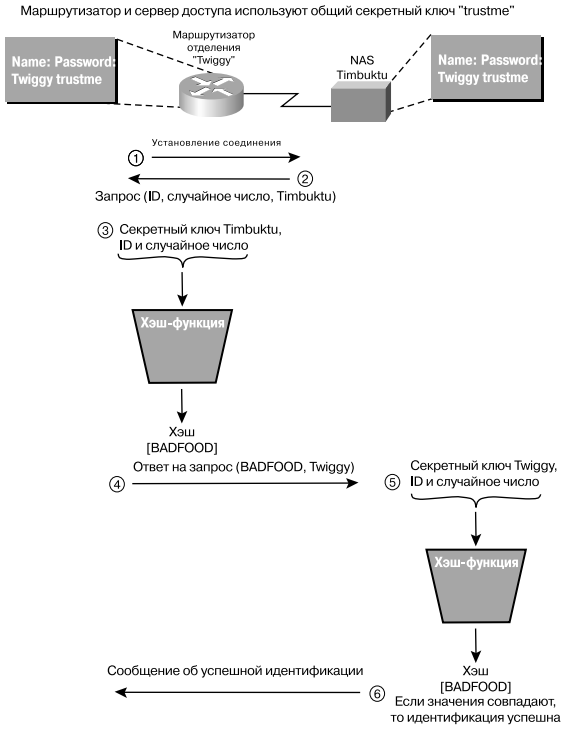


Рисунок 15. Аутентификация PPP CHAP

вычисления с помощью односторонней хэш-функции. Аутентификатор, случайное число и общий «текстовый секрет» один за другим подаются на вход хэш-функции. После этого вызывающая машина отправляет серверу ответ, который состоит из хэша и имени центрального компьютера или имени пользователя удаленного устройства. По получении ответа аутентификатор проверяет проставленное в ответе имя и выполняет те же вычисления. Затем результат этих вычислений сравнивается с величиной, проставленной в ответе. Если эти величины совпадают, результат аутентификации считается положительным, система выдает соответствующее уведомление, и LCP устанавливает связь. Секретные пароли на местном и удаленном устройстве должны быть идентичны. Поскольку «текстовый секрет» никогда не передается по каналам связи, никто не может подслушать его с помощью каких-либо устройств и использовать для нелегального входа в систему. Пока сервер не получит адекватный ответ, удаленное устройство не сможет подключиться к местному устройству.

CHAP обеспечивает защиту от использования чужих паролей за счет пошаговых изменений аутентификатора и применения переменной величины запроса. Повторяющиеся запросы предназначены для ограничения времени, в течение которого система теоретически остается подверженной любой отдельной хакерской атаке. Частоту и количество неудачных попыток входа в систему контролирует аутентификатор.

Примечание. Обычно в качестве односторонней хэш-функции CHAP используется MD5, а общий секрет хранится в текстовой форме. У компании Microsoft есть свой вариант протокола CHAP (MS-CHAP), где пароль (на вызывающей машине и на аутентификаторе) хранится в зашифрованном виде. Это дает протоколу MS-CHAP некоторое преимущество: в отличие от стандартного протокола CHAP, он может пользоваться широкодоступными базами данных постоянно зашифрованных паролей.

Протокол PPP EAP

PPP EAP является общим протоколом аутентификации PPP, который поддерживает множество аутентификационных механизмов. EAP не производит выбор конкретного аутентификационного механизма на этапе контроля соединения, но откладывает этот выбор до этапа аутентификации. Этот сценарий позволяет аутентификатору запросить больше информации до определения конкретного аутентификационного механизма. Кроме того, это дает возможность использовать «внутренний» сервер, который реально запускает различные механизмы, тогда как аутентификатор PPP служит лишь для обмена аутентификационными данными.

На рисунке 16 показано, как работает PPP EAP.

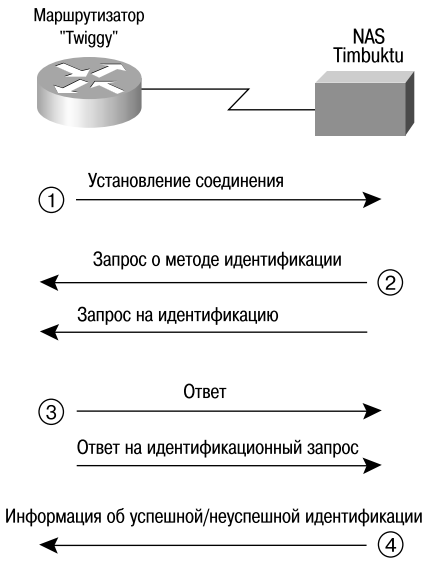


Рисунок 16. Аутентификация PPP EAP

Маршрутизатор отделения пытается провести аутентификацию сервера сетевого доступа (NAS) или «аутентификатора». По завершении этапа установления связи аутентификатор отправляет один или несколько запросов для аутентификации вызывающей машины. В запросе имеется поле типа запроса, где указано, что именно запрашивается. Так, например, здесь можно указать такие типы запросов, как аутентификация MD5, S/Key, аутентификация с использованием аппаратной карты для генерирования паролей и т. д. Запрос типа MD5 очень сходен с протоколом аутентификации CHAP. Обычно аутентификатор отправляет первоначальный аутентификационный запрос, за которым следует один или несколько дополнительных запросов о предоставлении аутентификационной информации. При этом первоначальный запрос не является обязательным и может опускаться в случаях, когда аутентификация обеспечивается иными способами (при связи по выделенным каналам, выделенным номерам и т. д.). В этих случаях вызывающая машина отправляет пакет ответных данных в ответ на каждый запрос. Как и пакет запроса, пакет ответных данных содержит поле, соответствующее полю типа запроса. И наконец, аутентификатор завершает процесс отправлением пакета, который свидетельствует о положительном или отрицательном результате аутентификации.

TACACS+

TACACS+ является протоколом последнего поколения из серии протоколов TACACS. TACACS — это простой протокол управления доступом, основанный на стандартах User Datagram Protocol (UDP) и разработанных компанией Bolt, Beranek and Newman, Inc. (BBN) для военной сети Military Network (MILNET). Компания Cisco несколько раз совершенствовала и расширяла протокол TACACS, и в результате появилась ее собственная версия TACACS, известная как TACACS+.

TACACS+ пользуется транспортным протоколом TCP. «Демон» сервера «слушает» порт 49, который является портом протокола IP, выделенным для протокола TACACS. Этот порт зарезервирован для выде-

ленных номеров RFC в протоколах UDP и TCP. Все текущие версии TACACS и расширенные варианты этого протокола используют порт 49.

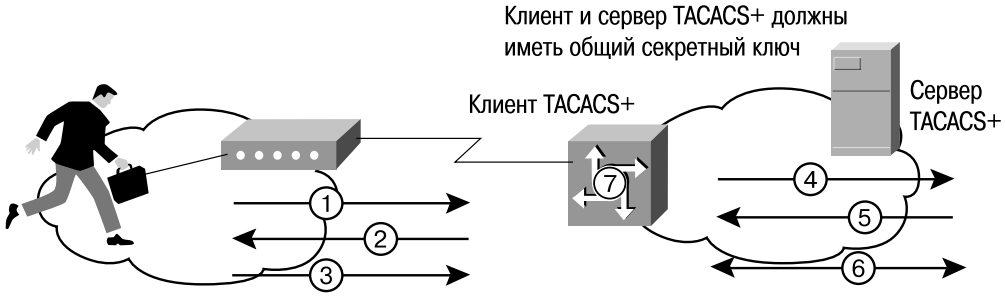
Протокол TACACS+ работает по технологии клиент/сервер, где клиентом TACACS+ обычно является NAS, а сервером TACACS+, как правило, считается «демон» (процесс, запускаемый на машине UNIX или NT). Фундаментальным структурным компонентом протокола TACACS+ является разделение аутентификации, авторизации и учета (AAA — Authentication, Authorization, Accounting). Это позволяет обмениваться аутентификационными сообщениями любой длины и содержания, и, следовательно, использовать для клиентов TACACS+ любой аутентификационный механизм, в том числе PPP PAP, PPP CHAP, аппаратные карты и Kerberos. Аутентификация не является обязательной. Она рассматривается как опция, которая конфигурируется на месте. В некоторых местах она вообще не требуется, в других местах она может применяться лишь для ограниченного набора услуг.

Авторизация — это процесс определения действий, которые позволены данному пользователю. Обычно аутентификация предшествует авторизации, однако это необязательно. В запросе на авторизацию можно указать, что аутентификация пользователя не проведена (личность пользователя не доказана). В этом случае лицо, отвечающее за авторизацию, должно самостоятельно решить, допускать такого пользователя к запрашиваемым услугам или нет. Протокол TACACS+ допускает только положительную или отрицательную авторизацию, однако этот результат допускает настройку на потребности конкретного заказчика. Авторизация может проводиться на разных этапах, например, когда пользователь впервые входит в сеть и хочет открыть графический интерфейс или когда пользователь запускает PPP и пытается использовать поверх PPP протокол IP с конкретным адресом IP. В этих случаях «демон» сервера TACACS+ может разрешить предоставление услуг, но наложить ограничения по времени или потребовать список доступа IP для канала PPP.

Учет обычно следует за аутентификацией и авторизацией. Учет представляет собой запись действий пользователя. В системе TACACS+ учет может выполнять две задачи. Во-первых, он может использоваться для учета использованных услуг (например, для выставления счетов). Во-вторых, его можно использовать в целях безопасности. Для этого TACACS+ поддерживает три типа учетных записей. Записи «старт» указывают, что услуга должна быть запущена. Записи «стоп» говорят о том, что услуга только что окончилась. Записи «обновление» (update) являются промежуточными и указывают на то, что услуга все еще предоставляется. Учетные записи TACACS+ содержат всю информацию, которая используется в ходе авторизации, а также другие данные, такие как время начала и окончания (если это необходимо) и данные об использовании ресурсов.

Транзакции между клиентом TACACS+ и сервером TACACS+ идентифицируются с помощью общего «секрета», который никогда не передается по каналам связи. Обычно этот секрет вручную устанавливается на сервере и на клиенте. TACACS+ можно настроить на шифрование всего трафика, который передается между клиентом TACACS+ и демоном сервера TACACS+.

На рисунке 17 показано взаимодействие между пользователем, с одной стороны, и клиентом и сервером TACACS+, с другой.



1. Пользователь инициирует соединение PPP с сервером доступа.
2. Сервер доступа запрашивает у пользователя имя и пароль.
3. Пользователь отвечает на запрос.
4. Клиент TACACS+ посылает зашифрованный пакет серверу TACACS+.
5. Сервер TACACS+ сообщает результаты идентификации.
6. Клиент и сервер обмениваются авторизованной информацией.
7. Клиент TACACS+ обрабатывает параметры, полученные во время авторизации.

Рисунок 17. Взаимодействие между пользователем и системой TACACS+

В ходе аутентификации TACACS+ используются пакеты трех типов: START, CONTINUE и REPLY. START и CONTINUE всегда отправляются клиентом, а REPLY всегда отправляется сервером.

Аутентификация начинается, когда клиент отправляет серверу сообщение START. Сообщение START

описывает тип будущей аутентификации и может содержать имя пользователя и некоторые аутентификационные данные. Пакет START отправляется только в качестве первого сообщения аутентификационной сессии TACACS+ или сразу же после повторного запуска этой сессии. (Повторный запуск может проводиться по просьбе сервера, которая содержится в пакете REPLY.) Пакет START всегда имеет порядковый номер, равный единице.

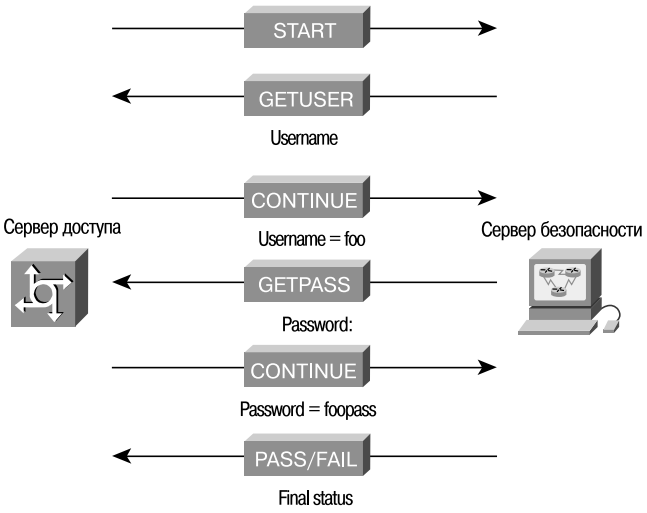


Рисунок 18. Процесс аутентификации TACACS+

В ответ на пакет START сервер отправляет пакет REPLY. Сообщение REPLY указывает, завершилась ли аутентификация или ее следует продолжить. Если пакет REPLY требует продолжения аутентификации, он также указывает, какую дополнительную информацию ему нужно предоставить. Клиент собирает эту информацию и отправляет ее серверу в сообщении CONTINUE.

По завершении аутентификации клиент может начать процесс авторизации (если она требуется). Сессия авторизации состоит из двух сообщений: сообщения REQUEST (запрос) и следующего за ним сообщения RESPONSE (ответ). Сообщение REQUEST содержит фиксированное количество полей, которые описывают пользователя или процесс, и переменный набор аргументов, которые описывают услуги и опции, требующие авторизации.

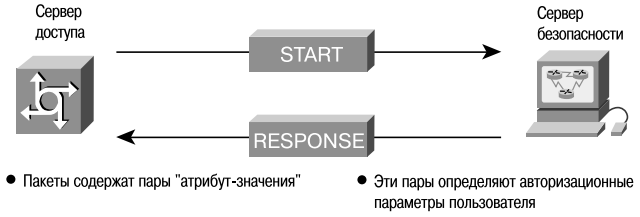


Рисунок 19. Процесс авторизации TACACS+

На рисунках 18 и 19 показаны процессы аутентификации и авторизации TACACS+.

RADIUS

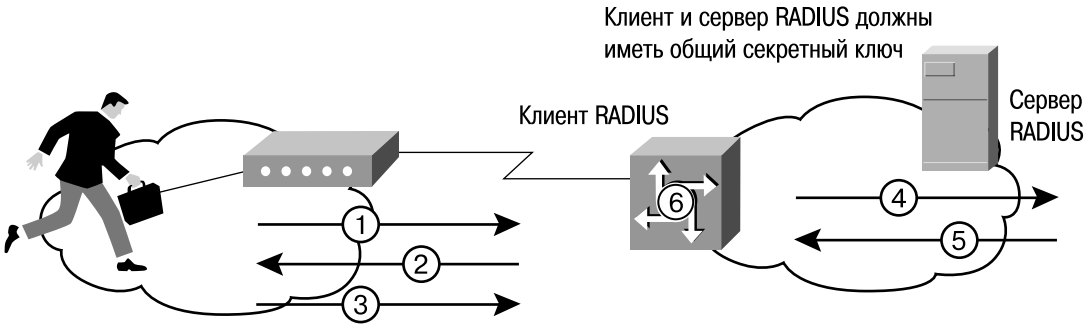
Протокол RADIUS был разработан компанией Livingston Enterprises, Inc. в качестве протокола аутентификации серверного доступа и учета. В июне 1996 года пятый проектный вариант протокола RADIUS был представлен на рассмотрение IETF. В настоящее время спецификация RADIUS (RFC 2058) и стандарт учета RADIUS (RFC 2059) предложены для утверждения в качестве общепринятых стандартов.

Связь между NAS и сервером RADIUS основана на UDP. В целом считается, что протокол RADIUS не имеет отношения к подключению. Все вопросы, связанные с доступностью сервера, повторной передачей данных и отключениями по истечении времени ожидания, контролируются устройствами, работающими под управлением протокола RADIUS, но не самим протоколом передачи.

Протокол RADIUS основан на технологии клиент/сервер. Клиентом RADIUS обычно является NAS, а сервером RADIUS считается «демон», работающий на машине UNIX или NT. Клиент передает пользовательскую информацию на определенные серверы RADIUS, а затем действует в соответствии с полученными от сервера инструкциями. Серверы RADIUS принимают запросы пользователей на подключение, проводят аутентификацию пользователей, а затем отправляют всю конфигурационную информацию, которая необходима клиенту для обслуживания пользователя. Для других серверов RADIUS или аутентификационных серверов других типов сервер RADIUS может выступать в роли клиента-посредника (proxy).

На рисунке 20 показано взаимодействие между пользователем, с одной стороны, и клиентом и сервером RADIUS, с другой.

Сервер RADIUS может поддерживать разные методы аутентификации пользователя. Если пользователь предоставит ему свое имя и оригинальный пароль, этот сервер может поддержать PPP PAP или CHAP, UNIX login и другие механизмы аутентификации. Обычно регистрация пользователя состоит из запроса (Access Request), который поступает из NAS на сервер RADIUS, и соответствующего ответа (положительного или отрицательного), который дает сервер. Пакет Access Request содержит имя пользователя, зашифрованный пароль, IP-адрес системы NAS и номер порта. Формат запроса дает возможность пользователю запросить определенный тип сессии. Например, если запрос производится в алфавитно-цифровом режиме, из этого следует, что запрашивается услуга одного типа («Service-Type = Exec-User»), но если запрос делается в пакетном режиме PPP, значит услуга должна быть другой («Service Type = Framed User» или «Framed Type = PPP»).



1. Пользователь инициирует соединение PPP с сервером доступа.
2. Сервер доступа запрашивает у пользователя имя и пароль.
3. Пользователь отвечает на запрос.
4. Клиент RADIUS посылает имя пользователя и зашифрованный пароль серверу RADIUS.
5. Сервер RADIUS отвечает сообщениями Accept, Reject или Challenge.
6. Клиент RADIUS обрабатывает параметры, полученные от сервера, вместе с сообщениями Accept, Reject или Challenge.

Рисунок 20. Взаимодействие между пользователем и системой RADIUS

Когда сервер RADIUS получает от NAS запрос Access Request, он проводит поиск указанного имени пользователя в базе данных. Если в базе данных такого имени нет, то сервер загружает стандартный профиль, используемый по умолчанию, или отправляет пользователю отрицательный ответ. Этот отрицательный ответ может при необходимости сопровождаться текстом, поясняющим причины отказа.

В системе RADIUS функции аутентификации и авторизации совмещены. Если имя пользователя найдено в базе данных и если пароль указан правильно, сервер RADIUS дает положительный ответ, в котором приводится список пар атрибутов для данной сессии. Типичными параметрами этого типа являются тип услуги (shell или framed), тип протокола, адрес IP, присваиваемый пользователю (статический или динамический), список объектов доступа или статический маршрут, который необходимо добавить в таблицу маршрутизации NAS. Конфигурационная информация на сервере RADIUS определяет, какие средства следует установить на машине NAS. На рисунке 21 показана процедура аутентификации и авторизации RADIUS.

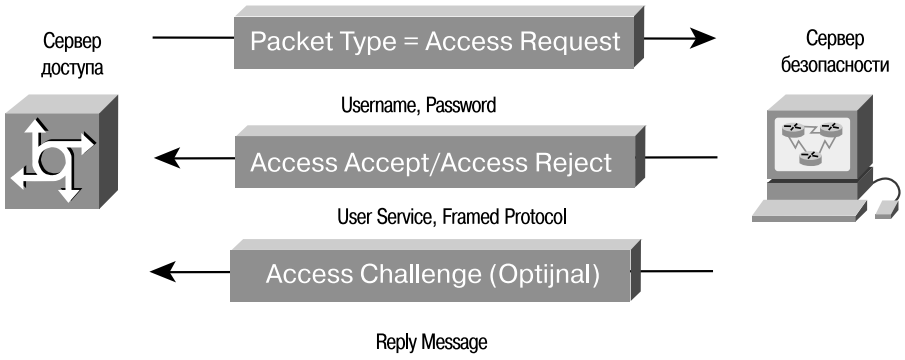


Рисунок 21. Процедура аутентификации и авторизации RADIUS

Учетные функции протокола RADIUS могут использоваться независимо от функций аутентификации и авторизации. Учетные функции RADIUS позволяют в начале и в конце каждой сессии отправлять данные о количестве ресурсов (то есть времени, пакетов, байтов и т. д.), использованных в ходе этой сессии. Провайдер услуг Интернет (ISP) может использовать программные средства контроля доступа и учета RADIUS для удовлетворения специальных требований безопасности и биллинга.

Транзакции между клиентом и сервером RADIUS аутентифицируются с помощью общего «секрета», который никогда не передается по сетевым каналам. Кроме того, обмен любыми пользовательскими паролями между клиентом и сервером RADIUS идет только в зашифрованном виде, что исключает подслушивание чужих паролей и последующее злоупотребление ими.

Самую свежую информацию и подробные технические детали можно получить в рабочей группе RADIUS IETF по адресу: http://www.ietf.org/html.charters/radius-charter.html.

Технологии целостности и конфиденциальности

В этом разделе описаны технологии, которые используются для поддержки целостности и конфиденциальности данных. Протоколами безопасности на транспортном уровне являются SSL и Secure Shell Protocol (SSH), которые обеспечивают безопасную передачу данных между клиентом и сервером. Оба протокола разработаны рабочей группой IETF по безопасности транспортного уровня (Transport Layer Security — TLS). Безопасный протокол передачи гипертекста (S-HTTP) предоставляет надежный механизм web-транзакций, однако в настоящее время наиболее популярным средством является SSL. Средство SOCKS является рамочной структурой, позволяющей приложениям клиент/сервер в доменах TCP и UDP удобно и безопасно пользоваться услугами сетевого межсетевого экрана. Протокол безопасности IP (IPSec) представляет собой набор стандартов поддержки целостности и конфиденциальности данных на сетевом уровне (в сетях IP). X.509 — это стандарт безопасности и аутентификации, который поддерживает структуры безопасности электронного информационного транспорта. Он определяет структуру данных цифрового сертификата и решает вопросы обращения общих ключей. X.509 является важнейшим компонентом инфраструктуры общих ключей (PKI).

SSL

SSL — это открытый протокол, разработанный компанией Netscape. SSL определяет механизм поддержки безопасности данных на уровне между протоколами приложений (такими как Hypertext Transfer Protocol [HTTP], Telnet, Network News Transfer Protocol [NNTP] или File Transfer Protocol [FTP]) и протоколом TCP/IP. Он поддерживает шифрование данных, аутентификацию серверов, целостность сообщений и (в качестве опции) аутентификацию клиентов в канале TCP/IP. SSL был представлен рабочей группе по безопасности консорциума W3 (W3C) для утверждения в качестве стандартного средства безопасности Web-браузеров и серверов в сети Интернет.

Основная цель протокола SSL состоит в том, чтобы обеспечить защищенность и надежность связи между двумя подключенными друг к другу приложениями. Этот протокол состоит из двух уровней. Нижний уровень, который располагается поверх надежного транспортного протокола (например, TCP), называется SSL Record Protocol. SSL Record Protocol используется для встраивания различных протоколов высокого уровня. Один из таких встроенных протоколов, SSL Handshake Protocol, позволяет серверу и клиенту аутентифицировать друг друга и согласовывать алгоритм шифрования и криптографические ключи, прежде чем протокол приложения произведет обмен первыми битами данных. Одно из преимуществ SSL состоит в том, что он независим от протоколов приложений. Протокол высокого уровня может совершенно прозрачно располагаться поверх протокола SSL. Протокол SSL поддерживает безопасность связи, придавая ей следующие свойства:

- Защищенность связи. После первоначального квитирования связи применяются средства шифрования и определяется секретный ключ. Для шифрования данных используются средства симметричной криптографии (например, DES, RC4 и т. д.).
- Участник сеанса связи может быть аутентифицирован и с помощью общих ключей, то есть средствами асимметричной криптографии (например, RSA, DSS и т.д.).
- Надежность связи. Транспортные средства проводят проверку целостности сообщений с помощью зашифрованного кода целостности (MAC). Для вычисления кодов MAC используются безопасные хэш-функции (например, безопасный хэш-алгоритм [SHA], MD5 и т. д.).

Протокол SSL состоит из нескольких уровней. На каждом уровне сообщения имеют ряд полей для указания длины, описания и содержания. SSL воспринимает данные, предназначенные для передачи, делит их на управляемые блоки, проводит компрессию данных (если это необходимо), использует код MAC, производит шифрование и передает результат. Принятые данные расшифровываются, проверяются, декомпрессируются и реассемблируются, а затем передаются клиентам более высокого уровня.

Протокол SSL принят только в рамках HTTP. Другие протоколы доказали свою способность работать с SSL, но используют ее не часто.

SSH

Протокол Secure Shell (SSH) предназначен для защиты удаленного доступа и других сетевых услуг в незащищенной сети. Он поддерживает безопасный удаленный вход в сеть, безопасную передачу файлов и безопасную эстафетную передачу сообщений по протоколам TCP/IP и X11. SSH может автоматически шифровать, аутентифицировать и сжимать передаваемые данные. В настоящее время SSH достаточно хорошо защищен от криптоанализа и протокольных атак. Он довольно хорошо работает при отсутствии глобальной системы управления ключами и инфраструктуры сертификатов и при необходимости может поддерживать инфраструктуры сертификатов, которые существуют в настоящий момент (например, DNSSEC, простую инфраструктуру общих ключей [SPKI], X.509).

Протокол SSH состоит из трех основных компонентов:

- Протокол транспортного уровня. Обеспечивает аутентификацию сервера, конфиденциальность и целостность данных с отличной защищенностью эстафетной передачи. В качестве опции может поддерживаться компрессия данных.
- Протокол аутентификации пользователя позволяет серверу аутентифицировать клиента.
- Протокол соединения мультиплексирует зашифрованный туннель, создавая в нем несколько логических каналов.

Все сообщения шифруются с помощью IDEA или одного из нескольких других шифровальных средств (тройного DES с тремя ключами, DES, RC4-128, Blowfish). Обмен ключами шифрования происходит с помощью RSA, а данные, использованные при этом обмене, уничтожаются каждый час (ключи нигде не сохраняются). Каждый центральный компьютер имеет ключ RSA, который используется для аутентификации центрального компьютера при использовании специальной технологии аутентификации RSA. Для защиты от подслушивания (спуфинга) сети IP используется шифрование; для защиты от DNS и спуфинга маршрутизации используется аутентификация с помощью общих ключей. Кроме того, ключи RSA используются для аутентификации центральных компьютеров.

Недостатком протоколов безопасности, действующих на уровне сессий, является их зависимость от инструкций протокола транспортного уровня. В случае SSL это означает, что атака на TCP может быстро прервать сессию SSL и потребовать формирования новой сессии, в то время как TCP будет считать, что все идет нормально.

Самую свежую информацию и более подробные технические детали о протоколе SSH можно получить в рабочей группе IEFT Secure Shell (secsh) по адресу: http://www.ietf.org/html.charters/secsh-charter.html.

Преимущества средств безопасности транспортного уровня (например, SSL или SSH) включают:

- возможность действий на сквозной основе (end-to-end) с существующими стеками TCP/IP, существующими интерфейсами прикладного программирования (API) (WinSock, Berkeley Standard Distribution [BSD] и т. д.);
- повышенная эффективность по сравнению с медленными каналами, поддержка технологии Van Jacobson для компрессии заголовков, поддержка различных средств контроля за переполнением сети, просматривающих заголовки TCP/IP;
- отсутствие каких-либо проблем с фрагментацией, определением максимального объема блоков, передаваемых по данному маршруту (MTU) и т. д.;
- сочетание компрессии с шифрованием. На этом уровне такое сочетание оказывается гораздо более эффективным, чем на уровне пакетов.

S-HTTP

S-HTTP представляет собой безопасный протокол связи, ориентированный на сообщения и разработанный для использования в сочетании с HTTP. Он предназначен для совместной работы с моделью сообщений HTTP и легкой интеграции с приложениями HTTP. Этот протокол предоставляет клиенту и серверу одинаковые возможности (он одинаково относится к их запросам и ответам, а также к предпочтениям обеих сторон). При этом сохраняется модель транзакций и эксплуатационные характеристики HTTP.

Клиенты и серверы S-HTTP допускают использование нескольких стандартных форматов криптографических сообщений. Клиенты, поддерживающие S-HTTP, могут устанавливать связь с серверами S-HTTP и наоборот, эти серверы могут связываться с клиентами S-HTTP, хотя в процессе подобных транзакций функции безопасности S-HTTP использоваться скорее всего не будут. S-HTTP не требует от клиента сертификатов общих ключей (или самих общих ключей), потому что этот протокол поддерживает только операции с симметричными шифровальными ключами. Хотя S-HTTP может пользоваться преимуществами глобальных сертификационных инфраструктур, для его работы такие структуры не обязательны.

Протокол S-HTTP поддерживает безопасные сквозные (end-to-end) транзакции, что выгодно отличает его от базовых механизмов аутентификации HTTP, которые требуют, чтобы клиент попытался получить доступ и получил отказ, и лишь затем включают механизм безопасности. Клиенты могут быть настроены таким образом, чтобы любая их транзакция автоматически защищалась (обычно с помощью специальной метки в заголовке сообщения). Такая настройка, к примеру, часто используется для передачи заполненных бланков. Если вы используете протокол S-HTTP, вам никогда не придется отправлять важные данные по сети в незащищенном виде.

S-HTTP поддерживает высокий уровень гибкости криптографических алгоритмов, режимов и параметров. Для того, чтобы клиенты и серверы смогли выбрать единый режим транзакции (так, например, им нужно решить, будет ли запрос только шифроваться или только подписываться или и шифроваться, и подписываться одновременно; такое же решение нужно принять и для ответов), используется механизм согласования опций, криптографических алгоритмов (RSA или Digital Signature Standard [DSA] для подписи, DES или RC2 для шифрования и т. д.), и выбора сертификатов (например: «Подписывайтесь своим

сертификатом Verisign»). S-HTTP поддерживает криптографию общих ключей и функцию цифровой подписи и обеспечивает конфиденциальность данных.

Протокол S-HTTP распространен не очень широко. Самые свежие данные и более подробные технические детали можно получить в рабочей группе IETF по безопасности web-транзакций (wts) по адресу: http://www.ietf.org/html.charters/wts-charter.html.

SOCKS

SOCKS разработан для того, чтобы дать возможность приложениям клиент/сервер в доменах TCP и UDP удобно и безопасно пользоваться услугами межсетевого экрана. Он дает пользователям возможность преодолевать межсетевой экран организации и получать доступ к ресурсам, расположенным в сети Интернет. SOCKS является «посредником уровня приложений»: он взаимодействует с общими сетевыми средствами (например, Telnet и браузер Netscape) и с помощью центрального сервера (прокси-сервера) от имени вашего компьютера устанавливает связь с другими центральными компьютерами.

SOCKS был разработан много лет назад Дейвом Кобласом (Dave Koblas) из компании SGI, и сегодня этот код можно бесплатно получить через Интернет. С момента первого выпуска этот код пережил несколько крупных модификаций, но каждая из них распространялась совершенно бесплатно. SOCKS версия 4 решает вопрос незащищенного пересечения межсетевых экранов приложениями клиент/сервер, основанными на протоколе TCP, включая Telnet, FTP и популярные информационные протоколы, такие как HTTP, Wide Area Information Server (WAIS) и GOPHER. SOCKS версия 5, RFC 1928, является дальнейшим расширением четвертой версии SOCKS. Он включает в себя UDP, расширяет общую рамочную структуру, придавая ей возможность использования мощных обобщенных схем аутентификации, и расширяет систему адресации, включая в нее имя домена и адреса IP v6.

В настоящее время предлагается создать механизм управления входящими и исходящими многоадресными сообщениями IP, которые проходят через межсетевой экран. Это достигается определением расширений для существующего протокола SOCKS V.5, что создает основу для аутентифицированного перехода межсетевого экрана одноадресным пользовательским трафиком TCP и UDP. Однако ввиду того, что поддержка UDP в текущей версии SOCKS V.5 имеет проблемы с масштабируемостью и другие недостатки (и их обязательно нужно разрешить, прежде чем переходить к многоадресной передаче), расширения определяются двояко: как базовые расширения UDP и как многоадресные расширения UDP.

Функционирование SOCKS заключается в замене стандартных сетевых системных вызовов в приложении их специальными версиями. Эти новые системные вызовы устанавливают связь с прокси-сервером SOCKS (который конфигурируется самим пользователем в приложении или системным файлом конфигурации), подключаясь к хорошо известному порту (обычно это порт 1080/TCP). После установления связи с сервером SOCKS приложение отправляет серверу имя машины и номер порта, к которому хочет подключиться пользователь. Сервер SOCKS реально устанавливает связь с удаленным центральным компьютером, а затем прозрачно передает данные между приложением и удаленной машиной. При этом пользователь даже не подозревает, что в канале связи присутствует сервер SOCKS.

Трудность с использованием SOCKS состоит в том, что кто-то должен проводить работу по замене сетевых системных вызовов версиями SOCKS (этот процесс обычно называется «SOCKS-ификацией» приложения). К счастью, большинство обычных сетевых приложений (Telnet, FTP, finger, whois) уже SOCKS-ифицированы, и многие производители включают поддержку SOCKS в свои коммерческие приложения. Кроме того, SOCKS V.5 включает эти процедуры в свою общую библиотеку: на некоторых системах (например, на машинах Solaris) можно автоматически SOCKS-ифицировать приложение, поставив общую библиотеку SOCKS перед «shared libc» в вашей строке поиска библиотек (переменная среды LD_LIBRARY_PATH в системах Solaris).

Самую свежую информацию и более подробные технические детали можно получить в рабочей группе IETF, работающей над проблемой аутентифицированного пересечения межсетевых экранов, по адресу: http://www.ietf.org/html.charters/aft-charter.html.

IPSec

Безопасный протокол IP (IPSec) представляет собой набор стандартов, используемых для защиты данных и для аутентификации на уровне IP. Текущие стандарты IPSec включают независимые от алгоритмов базовые спецификации, которые являются стандартными RFC.

Эти RFC, перечисленные ниже, сейчас пересматриваются с целью разрешения различных проблем безопасности, которые имеются в текущих спецификациях.

- RFC 2401 (Security Architecture for the Internet Protocol) — Архитектура защиты для протокола IP.
- RFC 2402 (IP Authentication header) — Аутентификационный заголовок IP.
- RFC 2403 (The Use of HMAC-MD5-96 within ESP and AH) — Использование алгоритма хэширования MD-5 для создания аутентификационного заголовка.

- RFC 2404 (The Use of HMAC-SHA-1-96 within ESP and AH) — Использование алгоритма хэширования SHA-1 для создания аутентификационного заголовка.
- RFC 2405 (The ESP DES-CBC Cipher Algorithm With Explicit IV) — Использование алгоритма шифрования DES.
- RFC 2406 (IP Encapsulating Security Payload (ESP)) — Шифрование данных.
- RFC 2407 (The Internet IP Security Domain of Interpretation for ISAKMP) — Область применения протокола управления ключами.
- RFC 2408 (Internet Security Association and Key Management Protocol (ISAKMP)) — Управление ключами и аутентификаторами защищенных соединений.
- RFC 2409 (The Internet Key Exchange (IKE)) — Обмен ключами.
- RFC 2410 (The NULL Encryption Algorithm and Its Use With IPsec) — Нулевой алгоритм шифрования и его использование.
- RFC 2411 (IP Security Document Roadmap) — Дальнейшее развитие стандарта.
- RFC 2412 (The OAKLEY Key Determination Protocol) — Проверка аутентичности ключа.

Заметим, что со временем будут разработаны новые алгоритмы аутентификации и шифрования. Работа над ними не прекращается, и в результате мы будем иметь смесь из этих алгоритмов, одни из которых будут сильнее, а другие слабее.
Протокол IPSec также включает криптографические методы, удовлетворяющие потребности управления ключами на сетевом уровне безопасности. Протокол управления ключами Ассоциации безопасности Интернет (Internet Security Association Key Management Protocol — ISAKMP) создает рамочную структуру для управления ключами в сети Интернет и предоставляет конкретную протокольную поддержку для согласования атрибутов безопасности. Само по себе это не создает ключей сессии, однако эта процедура может использоваться с разными протоколами, создающими такие ключи (например, с Oakley), и в результате мы получаем полное решение для управления ключами в Интернет.

Протокол определения ключей Oakley Key Determination Protocol пользуется гибридным методом Диффи-Хеллмана, чтобы создать ключи сессии Интернет для центральных компьютеров и маршрутизаторов. Протокол Oakley решает важную задачу обеспечения полной безопасности эстафетной передачи данных. Он основан на криптографических методах, прошедших серьезное испытание практикой. Полная защита эстафетной передачи означает, что если хотя бы один ключ раскрыт, раскрыты будут только те данные, которые зашифрованы этим ключом. Что же касается данных, зашифрованных последующими ключами, они останутся в полной безопасности.

Протоколы ISAKMP и Oakley были совмещены в рамках гибридного протокола IKE — Internet Key Exchange. Протокол IKE, включающий ISAKMP и Oakley, использует рамочную структуру ISAKMP для поддержки подмножества режимов обмена ключами Oakley. Новый протокол обмена ключами обеспечивает (в виде опции) полную защиту эстафетной передачи данных, полную защиту ассоциаций, согласования атрибутов, а также поддерживает методы аутентификации, допускающие отказ от авторства и не допускающие такого отказа. Этот протокол может, к примеру, использоваться для создания виртуальных частных сетей (VPN) и для того, чтобы предоставить пользователям, находящимся в удаленных точках (и пользующимся динамически распределяемыми адресами IP), доступ к защищенной сети.

Стандарт IPSec позволит поддержать на уровне IP потоки безопасных и аутентичных данных между взаимодействующими устройствами, включая центральные компьютеры, межсетевые экраны (сетевые фильтры) различных типов и маршрутизаторы. Ниже приводится пример использования IPSec для обеспечения обмена аутентифицированными конфиденциальными данными между удаленным маршрутизатором и межсетевым экраном (см. рисунок 22).

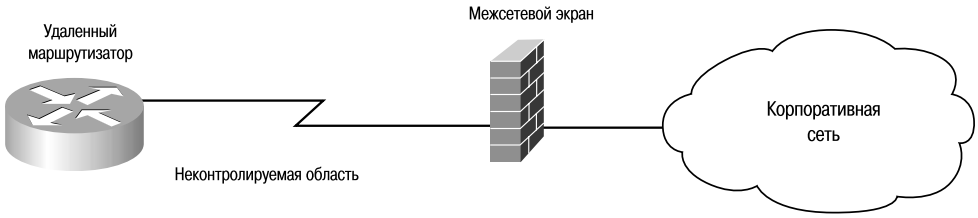


Рисунок 22. Безопасность обмена данными между удаленным маршрутизатором и межсетевым экраном

Прежде чем пройти через межсетевой экран предприятия, весь трафик, идущий от удаленного маршрутизатора, должен быть аутентифицирован. Маршрутизатор и межсетевой экран должны согласовать «ассоциацию безопасности» (SA), то есть прийти к согласию относительно политики в области безопасности. SA включает:
- алгоритм шифрования;
- алгоритм аутентификации;
- общий ключ сессии;
- срок действия ключа.

Ассоциация SA является однонаправленной, поэтому для двусторонней связи нужно устанавливать две SA, по одной для каждого направления. Как правило, в обоих случаях политика остается той же самой, но существует возможность и для асимметричной политики в разных направлениях. Согласование SA проводится через ISAKMP. Кроме того, SA могут определяться вручную. На рисунке 23 показан процесс согласования через ISAKMP, который происходит, когда на маршрутизатор поступает пакет, предназначенный для межсетевого экрана предприятия.

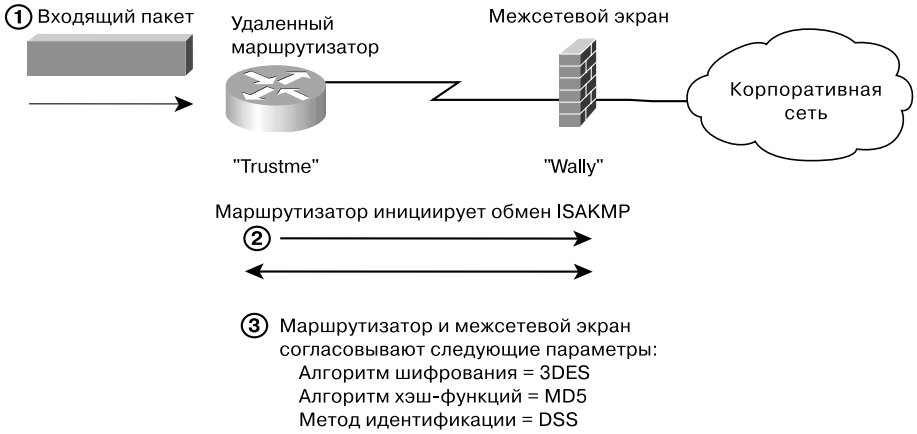


Рисунок 23. Согласование SA через ISAKMP

После согласования SA принимается решение о том, следует ли использовать средства аутентификации, конфиденциальности и целостности данных или ограничиться только аутентификацией. Если использоваться будут только средства аутентификации, текущий стандарт предполагает применение хэш-функции, а точнее алгоритма не ниже MD5 с 128-разрядными ключами. Заголовок пакета и данные пропускаются через хэш-функцию, и результаты этого вычисления вводятся в специальное поле заголовка AH, как показано на рисунке 24.

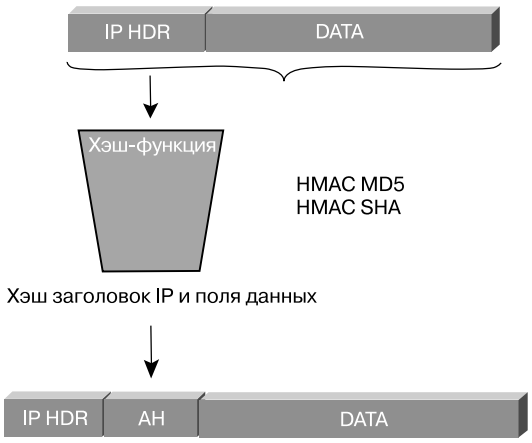


Рисунок 24. Создание нового аутентификационного заголовка IP

Новый пакет с аутентификационным заголовком, расположенным между заголовком IP и данными, отправляется через маршрутизатор в пункт назначения. Когда этот пакет попадает на межсетевой экран, который проверяет его аутентичность, вычисляя хэш с помощью хэш-функции, указанной в SA, обе стороны должны использовать одни и те же хэш-функции. Как показано на рисунке 25, межсетевой экран сравнивает вычисленный им хэш с параметрами, указанными в соответствующем поле AH. Если эти величины совпадают, аутентичность и целостность данных считается доказанной (если пакет передан из удаленной точки и при передаче не был искажен ни один бит).

Заметим, что вставка заголовка AH расширяет пакет, и поэтому для данного пакета может потребоваться фрагментация. Фрагментация производится после заголовка AH для исходящих пакетов и перед ним для входящих пакетов.

Если, помимо всего вышесказанного, стороны пожелают использовать средства поддержки конфиденциальности, SA указывает, что весь трафик, поступающий из удаленного маршрутизатора на межсетевой экран предприятия, должен аутентифицироваться и шифроваться. В противном случае межсетевой экран его не пропустит. ESP поддерживает аутентификацию, целостность и конфиденциальность данных и работает в двух режимах: туннельном и транспортном, как показано на рисунках 26 и 27.

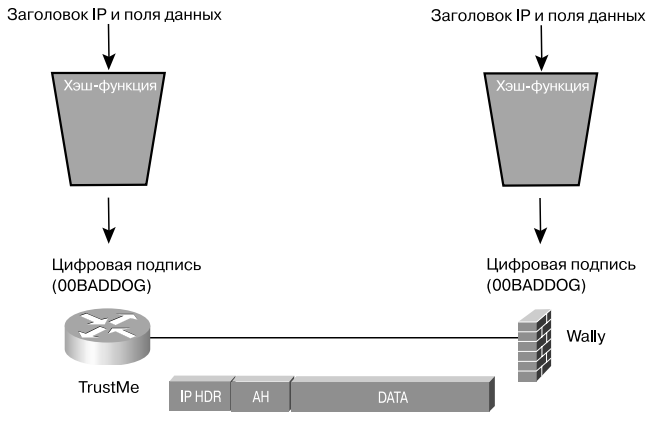


Рисунок 25. Проверка аутентичности и целостности данных

В туннельном режиме вся датаграмма IP, заголовок IP и данные встраиваются в заголовок ESP. В транспортном режиме шифруются только данные, а заголовок IP передается в незашифрованном виде. Современные стандарты требуют использования DES в режиме цепочки зашифрованных блоков (CBC).

Заметим, что вставка заголовка AH расширяет пакет, и поэтому для данного пакета может потребоваться фрагментация. Фрагментация производится после ESP для исходящих пакетов и перед ESP для входящих пакетов.

Преимущества поддержки безопасности на сетевом уровне с помощью IPSec включают:

- поддержку совершенно немодифицированных конечных систем, хотя в этом случае шифрование нельзя назвать в полном смысле слова сквозным (end-to-end);
- частичную поддержку виртуальных частных сетей (VPN) в незащищенных сетях;
- поддержку транспортных протоколов, иных, чем TCP (например, UDP);
- защиту заголовков транспортного уровня от перехвата и, следовательно, более надежную защиту от анализа трафика;
- при использовании AH и средств обнаружения повторяющихся операций обеспечивается защита от атак типа «отказ от обслуживания», основанных на «затоплении» систем ненужной информацией (например, от атак TCP SYN).

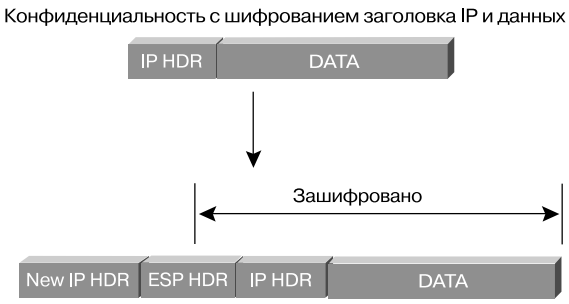


Рисунок 26. Туннельный режим ESP

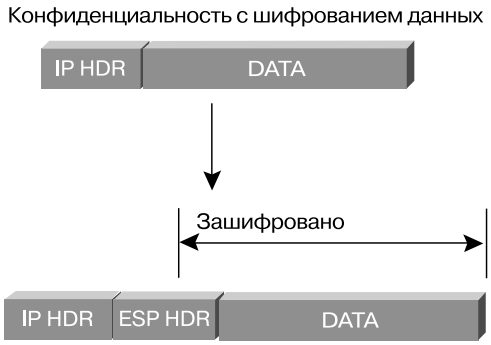


Рисунок 27. Транспортный режим ESP

Самую свежую информацию и более подробные технические детали можно получить в рабочей группе IETF по протоколу безопасности IP (IPSEC) по адресу:
http://www.ietf.org/html.charters/ipsec-charter.html.

X.509

Многие протоколы и приложения, которые пользуются услугами Интернет, применяют в целях безопасности технологию общих ключей. Для безопасного управления общими ключами в среде широкораспределенных пользователей или систем им необходим PKI. Стандарт X.509 представляет собой весьма популярную основу для подобной инфраструктуры. Он определяет форматы данных и процедуры распределения общих ключей с помощью сертификатов с цифровыми подписями, которые проставляются сертификационными органами (CA). RFC 1422 создает основу для PKI на базе X.509, что позволяет удовлетворить потребности электронной почты с повышенным уровнем защищенности, передаваемой через Интернет (PEM). С момента появления RFC 1422 требования приложений к PKI для сети Интернет резко выросли. Столь же резко возросли и возможности X.509. Предстоит большая работа по поддержке цифровых сертификатов в web-приложениях, а также в приложениях электронной почты и приложениях IPSec. В действующих стандартах определен сертификат X.509 версия 3 и список отзыва сертификатов (CRL) версия 2.

Для технологии общих ключей необходимо, чтобы пользователь общего ключа был уверен, что этот ключ принадлежит именно тому удаленному субъекту (пользователю или системе), который будет использовать средства шифрования или цифровой подписи. Такую уверенность дают сертификаты общих ключей, то есть структуры данных, которые связывают величины общих ключей с субъектами. Эта связь достигается цифровой подписью доверенного CA под каждым сертификатом. Сертификат имеет ограниченный срок действия, указанный в его подписанном содержании. Поскольку пользователь сертификата может самостоятельно проверить его подпись и срок действия, сертификаты могут распространяться через незащищенные каналы связи и серверные системы, а также храниться в кэш-памяти незащищенных пользовательских систем. Содержание сертификата должно быть одинаковым в пределах всего PKI. В настоящее время в этой области предлагается общий стандарт для Интернет с использованием формата X.509 v3 (см. рисунок 28).

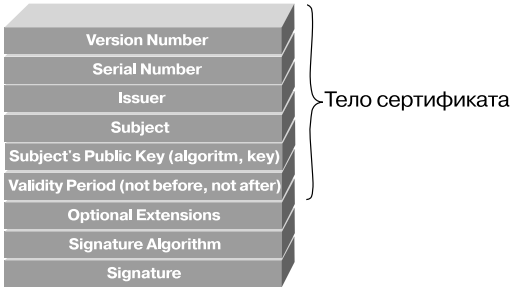


Рисунок 28. Формат сертификата X.509 v3

Каждый сертификат состоит из трех основных полей: текста сертификата, алгоритма подписи и самой подписи. В тексте сертификата указывается номер версии, серийный номер, имена эмитента и субъекта, общий ключ для субъекта, срок действия (дата и время начала и окончания действия сертификата). Иногда в этом тексте содержится дополнительная опционная информация, которую помещают в уникальные поля, связывающие пользователей или общие ключи с дополнительными атрибутами. Алгоритм подписи — это алгоритм, который использует CA для подписи сертификата. Подпись создается пропусканием текста сертификата через одностороннюю хэш-функцию. Величина, получаемая на выходе хэш-функции, зашифровывается частным ключом CA. Результат этого шифрования и является цифровой подписью (см. рисунок 29).

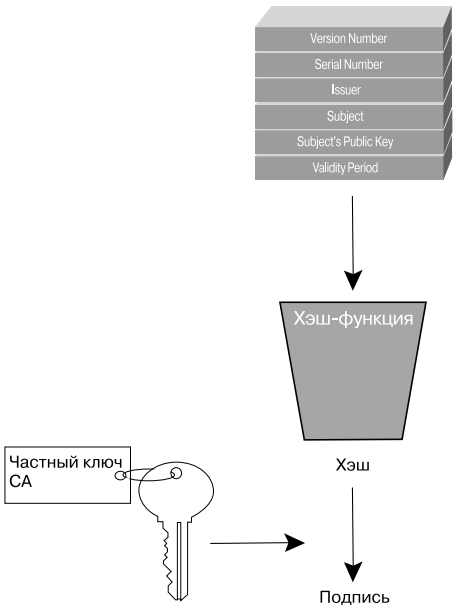


Рисунок 29. Создание цифровой подписи для сертификата X.509 v3

При выдаче сертификата подразумевается, что он будет действовать в течение всего указанного срока. Однако могут возникнуть обстоятельства, требующие досрочного прекращения действия сертификата. Эти обстоятельства могут быть связаны с изменением имени, изменением ассоциации между субъектом и CA (если, например, сотрудник уходит из организации), а также с раскрытием или угрозой раскрытия соответствующего частного ключа. В этих случаях CA должен отозвать сертификат.

CRL представляет собой список отозванных сертификатов с указанием времени. Он подписывается CA и свободно распространяется через общедоступный репозиторий. В списке CRL каждый отозванный сертификат опознается по своему серийному номеру. Когда у какой-то системы возникает необходимость в использовании сертификата (например, для проверки цифровой подписи удаленного пользователя), эта система не только проверяет подпись сертификата и срок его действия, но и просматривает последний из доступных списков CRL, проверяя, не отозван ли этот сертификат. Значение термина «последний из доступных» зависит от местной политики в области безопасности, но обычно здесь имеется в виду самый последний список CRL. CA составляет новые списки CRL на регулярной основе с определенной периодичностью (например, каждый час, каждый день или каждую неделю). Отозванные сертификаты немедленно вносятся в список CRL. Записи об отозванных сертификатах удаляются из списка в момент истечения официального срока действия сертификатов.

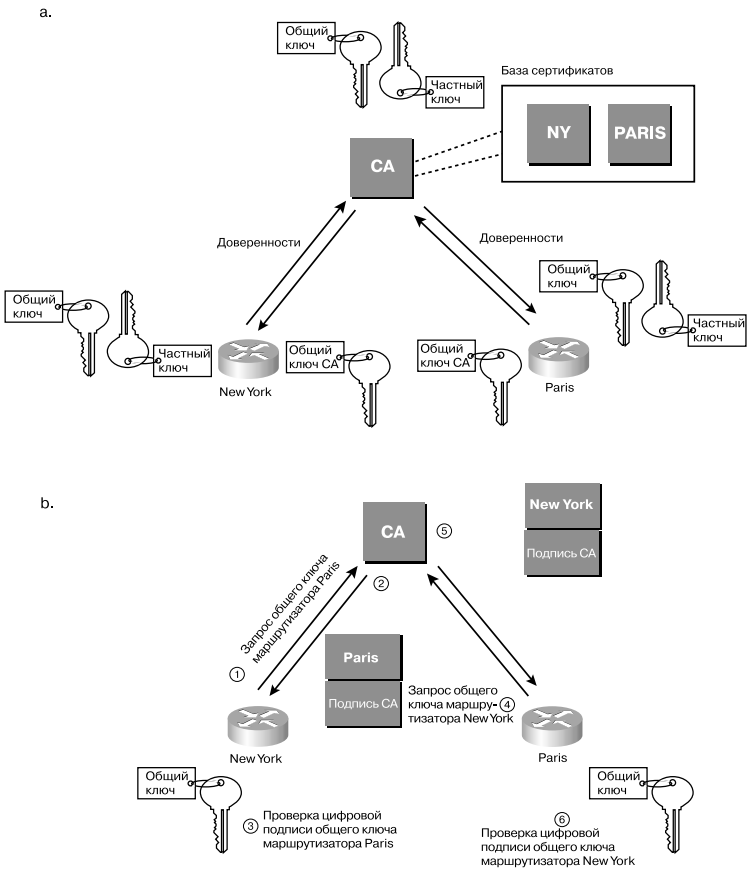


Рисунок 30. Передача цифрового сертификата

На рисунке 30 показан пример связи между системами и единым CA при помощи цифровых сертификатов.

Оба маршрутизатора и CA имеют свои пары общих/частных ключей. Вначале CA должен передать обоим маршрутизаторам по защищенным каналам сертификат X.509 v3. Кроме того, оба маршрутизатора должны получить по защищенным каналам копию общего ключа CA. После этого, если маршрутизатор в Нью-Йорке имеет трафик для отправки парижскому маршрутизатору и хочет передать этот трафик аутентичным и конфиденциальным способом, он должен предпринять следующие шаги:

1. Маршрутизатор в Нью-Йорке направляет запрос в CA для получения общего ключа парижского маршрутизатора.
2. CA отправляет ему сертификат парижского маршрутизатора, подписанный своим частным ключом.
3. Маршрутизатор в Нью-Йорке проверяет подпись общим ключом CA и убеждается в аутентичности общего ключа парижского маршрутизатора.
4. Парижский маршрутизатор направляет запрос в CA для получения общего ключа нью-йоркского маршрутизатора.
5. CA отправляет ему сертификат нью-йоркского маршрутизатора, подписанный своим частным ключом.
6. Парижский маршрутизатор проверяет подпись общим ключом CA и убеждается в аутентичности общего ключа нью-йоркского маршрутизатора.

Теперь, когда оба маршрутизатора обменялись своими общими ключами, они могут пользоваться средствами шифрования и с помощью общих ключей отправлять друг другу аутентичные конфиденциальные данные. Для получения общего секретного ключа обычно используется метод Диффи-Хеллмана, поскольку общий секретный ключ, как правило, применяется для шифрования больших объемов данных.

Предстоит большая работа по созданию эффективной инфраструктуры обращения общих ключей в среде Интернет и в корпоративной среде. Еще не решены вопросы ввода в действие новых сертификатов (как регистрировать новый сертификат в CA?), распределения сертификатов через какую-то службу директорий (рассматривается возможность использования для этой цели FTP или Lightweight Directory Access Protocol [LDAP]) и перекрестной сертификации сертификатов (управления иерархией сертификатов).

Самую свежую информацию и более подробные технические детали можно получить в рабочей группе IETF по инфраструктуре общих ключей (PKIX) по адресу:
http://www.ietf.org/html.charters/pkix-charter.html.

Технологии удаленного доступа к виртуальным частным сетям

Виртуальные частные сети с удаленным доступом (Virtual Private Dialup Networks — VPDN) позволяют крупным компаниям расширять свои частные сети, используя линии удаленной связи. Новые технологии снимают проблему высокой стоимости междугородней или международной связи и проблему низкой защищенности общих телефонных линий и каналов Интернет, через которые удаленный пользователь получает доступ к корпоративной сети. Новые технологии предоставляют удаленным офисам и пользователям безопасный доступ к инфраструктуре предприятия через местное подключение к сети Интернет. В настоящее время для этого используются три протокола: протокол эстафетной передачи на втором уровне (Layer 2 Forwarding — L2F), сквозной туннельный протокол (Point-to-Point Tunneling Protocol — PPTP) и туннельный протокол второго уровня (Layer 2 Tunneling Protocol — L2TP).

L2F

Протокол эстафетной передачи на втором уровне (Layer 2 Forwarding — L2F) был разработан компанией Cisco Systems. Он обеспечивает туннелирование протоколов канального уровня (то есть фреймов High-Level Data Link Control [HDLC], async HDLC или Serial Line Internet Protocol [SLIP]) с использованием протоколов более высокого уровня, например, IP. С помощью таких туннелей можно разделить местоположение сервера удаленного доступа, к которому подключается пользователь, используя местные коммутируемые линии связи, и точки, где происходит непосредственная обработка протокола удаленного доступа (SLIP, PPP), и пользователь получает доступ в сеть. Эти туннели дают возможность использовать приложения, требующие удаленного доступа с частными адресами IP, IPX и AppleTalk через протокол SLIP/PPP по существующей инфраструктуре Интернет. Поддержка таких многопротокольных приложений виртуального удаленного доступа очень выгодна конечным пользователям и независимым поставщикам услуг, поскольку позволяет разделить на всех расходы на средства доступа и базовую инфраструктуру и дает возможность осуществлять доступ через местные линии связи. Кроме того, такой подход защищает инвестиции, сделанные в существующие приложения, работающие не по протоколу IP, предоставляя защищенный доступ к ним и в то же время поддерживая инфраструктуру доступа к Интернет.

PPTP

Сквозной туннельный протокол Point-to-Point Tunneling Protocol (PPTP) создан корпорацией Microsoft. Он никак не меняет протокол PPP, но предоставляет для него новое транспортное средство. В рамках этого протокола определяется архитектура клиент/сервер, предназначенная для разделения функций, которые существуют в текущих NAS, и для поддержки виртуальных частных сетей (VPN). Сервер сети PPTP (PNS) должен работать под управлением операционной системы общего назначения, а клиент, который называется концентратором доступа к PPTP (PAC), работает на платформе удаленного доступа. PPTP определяет протокол управления вызовами, который позволяет серверу управлять удаленным коммутируемым доступом через телефонные сети общего пользования (PSTN) или цифровые каналы ISDN или ини-

циализировать исходящие коммутируемые соединения. PPTP использует механизм общей маршрутной инкапсуляции (GRE) для передачи пакетов PPP, обеспечивая при этом контроль потоков и сетевых заторов. Безопасность данных в PPTP может обеспечиваться при помощи протокола IPSec.

L2TP

Как видим, протоколы L2F и PPTP имеют сходную функциональность. Компании Cisco и Microsoft согласились вместе (в рамках IETF) разработать единый стандартный протокол, который получил название туннельного протокола второго уровня (Layer 2 Tunneling Protocol — L2TP). Обе компании будут и далее поддерживать свои собственные решения для виртуальных частных сетей (L2F и PPTP), а также путь перехода от этих решений к L2TP. Поэтому сегодня заказчики могут внедрять существующие решения для виртуальных частных сетей и быть абсолютно уверены в том, что их инвестиции не будут потеряны, когда на рынке появится L2TP.

Пример использования этих протоколов приведен на рисунке 31.

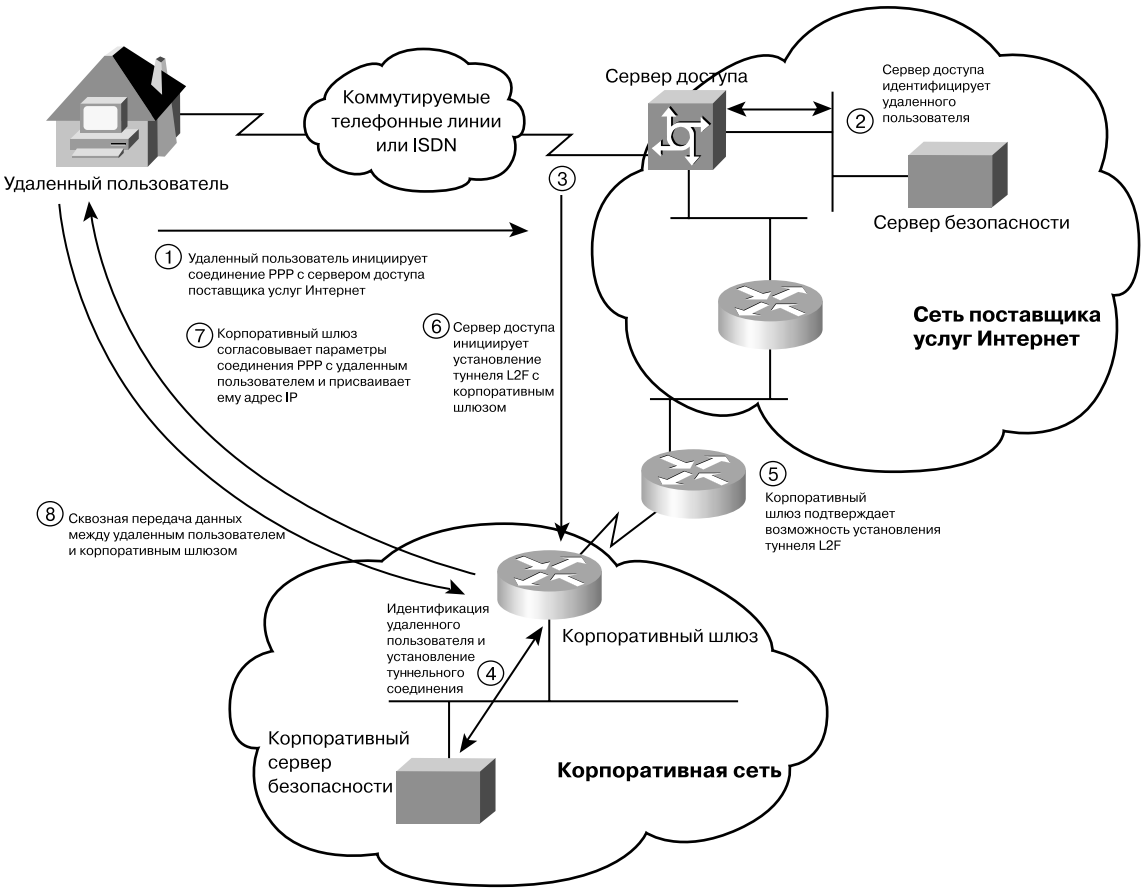


Рисунок 31. Пример виртуального удаленного доступа

Самую свежую информацию и более подробные технические детали можно получить в рабочей группе IETF по расширениям протокола PPP (pppext) по адресу:
http://www.ietf.org/html.charters/pppext-charter.html.

Сервис Директории и Служб Имен

В настоящее время все больше исследований проводится для решения проблем, связанных с безопасностью при обеспечении надежного механизма для распределения общих ключей. Большая часть этой работы выполняется в области сервиса имени домена и сервиса директорий. В данном разделе рассматриваются разработки протоколов LDAP и DNSSEC.

LDAP

Lightweight Directory Access Protocol (LDAP) — это протокол для обращения к сервису директорий в режиме реального времени. Протокол LDAP был разработан Университетом шт. Мичиган в 1995 г. для обеспечения более легкого доступа к директориям X.500. Протокол X.500 был слишком сложными и требовал слишком много ресурсов компьютера для многих потребителей, поэтому и был разработан упрощенный

вариант. Протокол LDAP особо ориентирован на приложения управления и просмотра, которые обеспечивают интерактивный доступ к директориям в режиме чтение/запись.

При совместном использовании с директорией, поддерживающей протоколы X.500, данный протокол предполагается применять в качестве дополнения к протоколу доступа к директории X.500 Directory Access Protocol (DAP). RFC 1777 — это версия 2 протокола LDAP. В настоящее время ведется работа над версией 3, которая будет являться базовой для сети Интернет. Протокол LDAP использует непосредственно протокол TCP и может быть использован для обращения как к автономному сервису директории LDAP, так и для обращения к сервису директории, которая заканчивается директорией X.500.

Данный стандарт определяет:

- сетевой протокол для получения доступа к информации в директории;
- информационную модель, которая определяет форму и характер информации;
- пространство имен, которое устанавливает, как информация снабжена ссылками и организована;
- распределенную модель функционирования, которая устанавливает, как данные могут быть распределены и снабжены ссылками (в версии 3).

Общая модель, принятая в LDAP, — это один из клиентов, выполняющий протокольные операции с серверами. В этой модели клиент передает запрос протокола, описывающий серверу операцию, которую необходимо выполнить. Этот сервер становится ответственным за проведение необходимых операций в директории. По завершении операций сервер посылает ответ, содержащий какие-либо результаты или ошибки. Этот сценарий показан на рисунке 32.

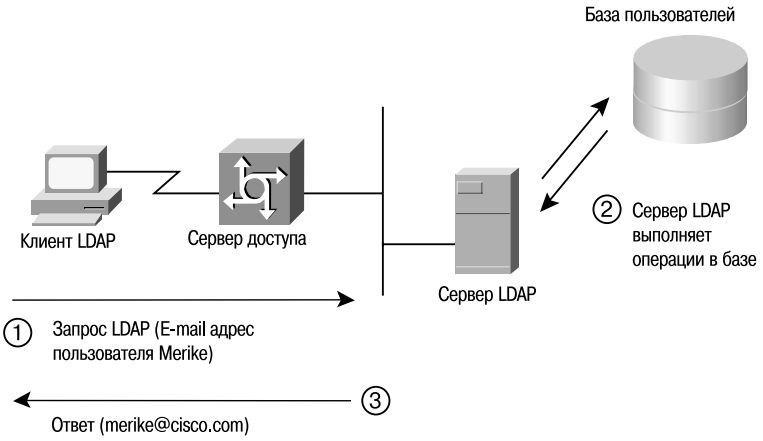


Рисунок 32. Работа протокола LDAP

В версиях 1 и 2 протокола LDAP не был предусмотрен возврат ссылок сервером клиенту. Если сервер LDAP не знает ответа на запрос, он скорее обратится к другому серверу за информацией, чем пошлет клиенту сообщение о необходимости перейти к данному другому серверу. Однако, для улучшения функционирования и распределения эта версия протокола позволяет серверам возвращать клиентам ссылки на другие серверы. Такая установка позволяет серверам отбросить работу по установлению контактов с другими серверами для ускорения выполняемых операций. Протокол LDAP оперирует на допущении того, что существуют один или более серверов, которые совместно обеспечивают доступ к информационному дереву директории DIT. Это дерево составлено из входов, которые имеют имена: одно или более атрибутивное значение входа формирует его соответствующее отличительное имя RDN, которое должно быть уникальным среди других таких же входов. Соединение имен RDN в последовательности входов от конкретного входа к непосредственному подуровню корня дерева формирует это отличительное имя, которое является уникальным в дереве. Некоторые серверы могут содержать кэш-память или теневые копии входов, которые могут быть использованы для ответа на поисковый запрос, сравнительные запросы, но будут возвращать ссылки или взаимодействовать с другими серверами, если поступил запрос на операции по модификации.

Протокол LDAP устанавливает следующие операции:

- Связывающая операция инициирует протокольный сеанс между клиентом и сервером и обеспечивает аутентификацию клиента для сервера. Связывающая операция должна быть первым оперативным запросом, полученным сервером от клиента в протокольном сеансе в версиях 1 и 2, однако данное ограничение было отменено в версии 3.
- Операция по прекращению связи завершает протокольный сеанс.
- Поисковая операция позволяет клиенту сделать запрос на выполнение сервером поиска от его имени.
- Операция по модификации позволяет клиенту сделать запрос на выполнение модификации информационной базы директории сервером от его имени.
- Операция по дополнению позволяет клиенту сделать запрос на введение дополнительного входа в директории.
- Операция по удалению позволяет клиенту запросить удаление какого-либо входа из директории.
- Операция по модификации имени RDN позволяет клиенту изменить последний компонент имени входа в директории.

- Операция по сравнению позволяет клиенту сравнивать утверждение, обеспечиваемое входом директории.
- Операция на завершение позволяет клиенту запросить сервер отставить невыполненную операцию.
- Расширенная операция является новой в версии 3, она введена для обеспечения определения дополнительных операций для тех видов сервиса, которые недоступны где-либо еще в протоколе; например, отмеченные цифровым способом операции и результаты.

Примечание. Связывающая операция протокола LDAP в версии 2 позволяет лишь простую аутентификацию, состоящую из пароля открытого (незашифрованного текста), и аутентификацию Kerberos версии 4. В версии 3 допущен любой механизм SASL уровня безопасности и простой аутентификации. SASL позволяет обращаться к сервису обеспечения целостности и секретности. Также допускается возврат аутентификационных данных сервером клиенту, если сервер изберет именно этот путь.

Для получения большего объема технической информации и последних достижений обращайтесь в ASID (поиск, поиск и индексирование директорий) и рабочие группы IETF по созданию новых версий протокола LDAP, имеющие следующие адреса в сети Интернет, соответственно:
http://www.ietf.org/html.charters/asid-charter.html и http://www.ietf.org/html.charters/ldapext-charter.html.

DNSSEC

Система имени домена DNS стала важной действующей частью инфраструктуры сети Интернет. И все же она еще не имеет сильного механизма защиты для обеспечения целостности данных или аутентификации. Расширения к DSN обеспечивают эти виды сервиса для устройств с функциями защиты или для приложений за счет использования криптографических цифровых подписей. Эти цифровые подписи включены в защищенные зоны в виде ресурсных записей. Во многих случаях защита все еще может быть обеспечена даже через DNS серверы, в которых функции защиты не предусмотрены. Эти расширения также предусматривают хранение аутентифицированных общих ключей в DSN. Такое хранение ключей может поддерживать общий сервис распределения общих ключей так же, как и безопасность DNS. Хранящиеся ключи позволяют устройствам с функциями защиты запомнить аутентифицирующий ключ зон в дополнение к тем зонам, к которым они изначально настроены. Ключи, связанные с именами DNS, могут быть запрошены для поддержки других протоколов. Предусмотрено применение целого ряда алгоритмов и типов ключей. Расширения защиты предусматривают дополнительную аутентификацию транзакций протокола DSN.

Для ознакомления с текущими разработками и получения дополнительных технических подробностей обращайтесь к рабочей группе IETF Domain Name System Security (dnssec) по адресу в сети Интернет:
http://www.ietf.org/html.charters/dnssec-charter.html.

Cisco SAFE: Архитектура безопасности корпоративных сетей

Аннотация

Главная цель архитектуры Cisco для безопасности корпоративных сетей (SAFE) состоит в том, чтобы предоставить заинтересованным сторонам информацию о современном опыте проектирования и развертывания защищенных сетей. SAFE призвана помочь тем, кто проектирует сети и анализирует требования к сетевой безопасности. SAFE исходит из принципа глубоко эшелонированной обороны сетей от внешних атак. Этот подход нацелен не на механическую установку межсетевого экрана и системы обнаружения атак, а на анализ ожидаемых угроз и разработку методов борьбы с ними. Эта стратегия приводит к созданию многоуровневой системы защиты, при которой прорыв одного уровня не означает прорыва всей системы безопасности. SAFE основывается на продуктах компании Cisco и ее партнеров.

Вначале мы рассмотрим саму архитектуру SAFE. Затем следует подробное описание модулей, из которых состоит реальная сеть, как крупного предприятия, так и малых сетей, в том числе сетей филиалов предприятий, средних сетей и сетей удаленных и мобильных пользователей. Дизайны малых и средних сетей применяются в двух возможных вариантах. Во-первых, это может быть дизайн основной сети предприятия, которая имеет соединения с другими офисами подобных предприятий. Например, крупное юридическое агентство может построить главную сеть на основе дизайна среднего предприятия, а сети филиалов — на основе малого. Во-вторых, дизайн может быть разработан как сеть филиала, т. е. как часть сети крупного предприятия. В этом случае примером может служить крупная автомобильная компания, где дизайн крупной сети используется в штаб-квартирах, а для прочих подразделений — от филиалов до удаленных работников — применяются дизайны средних и малых предприятий.

В первых разделах, посвященных модулям, описываются потоки трафика, основные устройства, ожидаемые угрозы и общие схемы их преодоления. Далее приводится технический анализ дизайна, более детальное описание методов предотвращения угроз и стратегий миграции. В Приложении А описывается лаборатория, которая служит для оценки базовых концепций безопасности, и даются примеры возмож-

ных конфигураций. В Приложении B представлены основы сетевой безопасности. Тем читателям, кто не знаком с основными концепциями сетевой защиты, рекомендуется сначала изучить этот раздел и лишь затем перейти к остальному документу. В Приложении C вы увидите определения технических терминов, используемых в документе, а также расшифровку условных обозначений.

Настоящий документ посвящен угрозам, характерным для корпоративной среды. Сетевые разработчики, знакомые с этими угрозами, смогут лучше спланировать место и способ реализации противодействующих технологий. При отсутствии полного понимания характера угроз внедрение технологий защиты будет скорее всего неверно сконфигурировано, слишком сильно сконцентрировано на устройствах и не будет иметь достаточного количества вариантов реагирования. Именно поэтому авторы данного документа предлагают сетевым инженерам информацию, которая поможет им принять правильные и обоснованные решения по защите сетей.

Кому адресован документ

Поскольку документ является техническим, он адресован разным группам читателей и допускает разные акценты и глубину прочтения. Например, сетевой администратор, ознакомившись с вводными частями каждого раздела, получит представление о стратегиях и возможностях защиты сетей. Сетевому инженеру или проектировщику сети будет полезно прочесть документ полностью, чтобы получить информацию о предлагаемых дизайнах, а также выяснить подробности анализа угроз, соответствующие особенностям конфигураций используемых устройств.

Позиционирование

Авторы документа исходят из предположения о том, что у вас уже имеется политика безопасности. Cisco Systems не рекомендует внедрять технологии защиты сетей без такой политики. Настоящий документ нацелен на потребности крупных корпоративных заказчиков. Хотя большинство обсуждаемых здесь принципов можно напрямую использовать в малом и среднем бизнесе и даже в домашних офисах, масштаб этого использования будет совсем иным. Детальный анализ потребностей этих видов бизнеса выходит за рамки данного документа. Однако, чтобы дать хотя бы ограниченное представление о потребностях малых сетей, в разделах «Альтернативы» и «Корпоративные опции» перечислены устройства, без которых можно обойтись, если вы хотите сократить общую стоимость архитектуры.

Следование рекомендациям настоящего документа не гарантирует вам безопасной среды или защиты от всех атак. Полная и абсолютная безопасность может быть достигнута только отключением вашей системы от сети и заключением ее в бетонный саркофаг, который лучше всего поместить в подвалы Форт Нокса, где хранится золотой запас США. Там ваши данные будут отлично защищены, но совершенно недоступны. Однако вы можете в достаточной степени защитить свою сеть, если будете внедрять разумную политику безопасности, следовать рекомендациям данного документа, постоянно следить за последними событиями в мире хакеров и достижениями в области защиты сетей и если вы будете постоянно отслеживать все системы с помощью надежных процедур системной администрации. Для этого нужно знать и те вопросы безопасности, которые недостаточно полно раскрыты в данном документе.

Хотя виртуальные частные сети (VPN) входят в состав данной архитектуры, их описание в данном документе не является очень подробным. В этом документе вы не найдете информации о подробностях масштабирования, стратегиях устойчивости и других вопросах, касающихся VPN. Кроме VPN в этом документе недостаточно подробно раскрыты стратегии аутентификации (в том числе вопросы, связанные с инфраструктурой цифровых сертификатов (certificate authorities — CA). Этот вопрос требует отдельного детального рассмотрения. В настоящем документе также не упоминается целый ряд передовых сетевых приложений и технологий (например технологии информационного наполнения, кэширования и балансировки серверной нагрузки). Хотя эти технологии скорее всего будут использоваться в программе SAFE, данный документ не рассматривает их специфические требования к системе безопасности.

SAFE базируется на продуктах компании Cisco и ее партнеров. Однако в этом документе продукты не называются по имени. Это означает, что вместо номера или названия конкретной модели мы приводим функциональное описание соответствующего устройства. Во время оценки системы SAFE будет проводиться конфигурирование реальных продуктов для установки в специфических условиях конкретной сети, как описано в данном документе. Примеры реальных конфигураций приведены в Приложении A «Оценочная лаборатория».

В настоящем документе слово «хакер» обозначает лицо, которое пытается со злым умыслом получить несанкционированный доступ к сетевым ресурсам. Хотя эти намерения можно более точно выразить термином «злоумышленник», мы для краткости используем более распространенный термин «хакер».

Обзор архитектуры

Основы дизайна

SAFE с максимальной точностью имитирует функциональные потребности современных корпоративных сетей. Решения о внедрении той или иной системы безопасности могут быть разными в зависимости от сетевой функциональности. Однако на процесс принятия решения оказывают влияние следующие задачи, перечисленные в порядке приоритетности:

- безопасность и борьба с атаками на основе политики;
- внедрение мер безопасности по всей инфраструктуре (а не только на специализированных устройствах защиты);
- безопасное управление и отчетность;
- аутентификация и авторизация пользователей и администраторов для доступа к критически важным сетевым ресурсам;
- обнаружение атак на критически важные ресурсы и подсети;
- поддержка новых сетевых приложений.

Во-первых (и это самое главное), SAFE представляет собой архитектуру безопасности, которая должна предотвратить нанесение хакерами серьезного ущерба ценным сетевым ресурсам. Атаки, которые преодолевают первую линию обороны или ведутся не извне, а изнутри, нужно обнаруживать и быстро отражать, чтобы предотвратить ущерб для остальной сети. Однако даже хорошо защищенная сеть должна предоставлять пользователям сервисы, которых от нее ожидают. Нужно одновременно обеспечить и надежную защиту, и хорошую функциональность сети — и это вполне возможно. Архитектура SAFE не является революционным способом проектирования сетей. Это просто система обеспечения сетевой безопасности.

Кроме этого, система SAFE является устойчивой и масштабируемой. Устойчивость сетей включает физическую избыточность, защищающую сеть от любых аппаратных отказов, в том числе отказов, которые могут произойти из-за ошибочной конфигурации, физического сбоя или хакерской атаки. Хотя возможны и более простые проекты, особенно если требования к производительности сети не являются высокими, в настоящем документе в качестве примера используется более сложный дизайн, поскольку планирование безопасности представляет собой более сложную проблему именно в сложной, а не в простой среде. Тем не менее, на всем протяжении этого документа мы рассматриваем возможности ограничения сложности дизайна.

На многих этапах проектирования сети инженер встает перед выбором между интеграцией множества функций в едином сетевом устройстве и использованием специализированных сетевых средств. Интеграция функций часто является более привлекательной, потому что ее можно реализовать на существующем оборудовании и потому что функции могут взаимодействовать в рамках единого устройства, создавая более эффективное функциональное решение. Специализированные устройства чаще всего используются для поддержки весьма продвинутых функций или высокой производительности. Решение принимается на основе сравнения емкости и функциональности отдельного устройства и преимуществ, которые может дать интеграция. Например, в некоторых случаях вы можете выбрать интегрированный высокопроизводительный маршрутизатор с операционной системой Cisco IOS (и встроенным программным межсетевым экраном, а в других — менее крупный маршрутизатор с отдельным межсетевым экраном. В нашей архитектуре используются как тот, так и другой типы систем. Наиболее важные функции безопасности передаются выделенным устройствам, чтобы поддержать высокую производительность крупных корпоративных сетей.

Принцип модульности

Хотя по мере роста требований большинство сетей развивается, архитектура SAFE использует открытый модульный подход. Такой подход имеет два основных преимущества: во-первых, он описывает дизайн с точки зрения защиты взаимодействия отдельных модулей сети, а во-вторых, позволяет проектировщику оценивать защищенность каждого модуля по отдельности, а не только всей системы в целом. Защищенный дизайн каждого модуля можно описать и реализовать по отдельности, а оценить в рамках всей системы.

Хотя многие сети нельзя четко разграничить на отдельные модули, такой подход дает ориентиры при внедрении в сети функций защиты. Сетевым инженерам не предлагается строить свои сети в строгом соответствии с SAFE, но рекомендуется комбинировать описанные здесь модули и использовать их в имеющихся сетях.

На рисунке 33 показан первый уровень модульности SAFE. Каждый блок представляет определенную функциональную

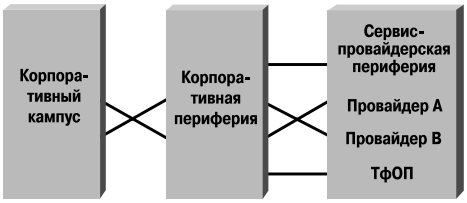


Рисунок 33. Корпоративный композитный модуль

зону. Модуль Интернет-провайдера (ISP) не устанавливается на предприятии, но включается в общую схему, так как для подавления некоторых атак предприятию необходимо запрашивать у Интернет-провайдера ряд конкретных функций безопасности.

Второй уровень модульности, показанный на рисунке 34, демонстрирует модули в каждой функциональной области. Эти модули выполняют в сети вполне определенную роль и имеют определенные потребности в области безопасности. Размер того или иного модуля на схеме не обязательно соответствует его масштабу в реальной сети. Так, например, «модуль здания», представляющий устройства конечных пользователей, может включать в себя до 80% всех сетевых устройств. Дизайн безопасности каждого модуля описывается отдельно, но проверяется в комплексе, т. е. в составе всей корпоративной системы.

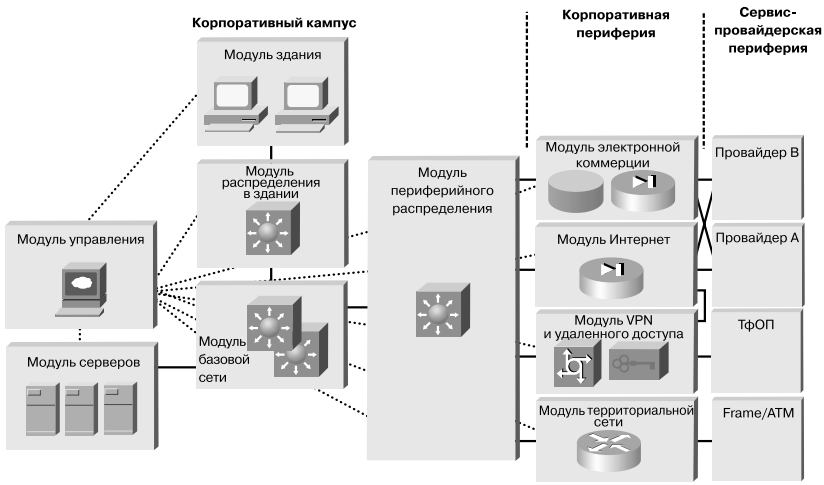


Рисунок 34. Блок-схема корпоративной системы SAFE

Хотя большинство существующих корпоративных сетей нелегко разделить на отдельные модули, этот подход позволяет реализовать разные функции безопасности по всей сети. Авторы не думают, что сетевые инженеры будут проектировать сети, идентичные схеме SAFE. Скорее всего они будут пользоваться сочетанием описанных модулей, интегрированных в существующую сеть.

Аксиомы SAFE

Цель — маршрутизаторы

Маршрутизаторы контролируют доступ из любой сети к любой сети. Они рекламируют сети и определяют тех, кто может получать к ним доступ. Поэтому потенциально маршрутизатор — это «лучший друг хакера». Безопасность маршрутизаторов является критически важным элементом любой системы сетевой безопасности. Основной функцией маршрутизаторов является предоставление доступа, и поэтому маршрутизаторы нужно обязательно защищать, чтобы исключить возможность прямого взлома. Вы можете обратиться и к другим документам, где описана защита маршрутизаторов. Эти документы более детально рассматривают следующие вопросы:

- блокировка доступа к маршрутизатору из сетей связи общего доступа;
- блокировка доступа к маршрутизатору через протокол SNMP;
- управление доступом к маршрутизатору через TACACS+;
- отключение ненужных услуг;
- вход в систему на определенных уровнях;
- аутентификация обновлений маршрутов.

Самые свежие документы, посвященные безопасности маршрутизаторов, можно найти по следующему адресу: http://www.cisco.com/warp/customer/707/21.html

Цель — коммутаторы

Коммутаторы (обычные и многоуровневые), как и маршрутизаторы, имеют свои требования к безопасности. Однако данные об угрозах для безопасности коммутаторов и о смягчении этих угроз распространены гораздо меньше, чем аналогичные данные для маршрутизаторов. Большинство соображений, приведенных в предыдущем разделе для маршрутизаторов, годятся и для коммутаторов. Кроме того, в случае с коммутаторами вы должны предпринимать следующие меры предосторожности:

- Если порт не должен подключаться к транку, то параметры транковых соединений на нем должны не устанавливаться в положение «auto», а отключаться (off). В результате хост не сможет стать транковым портом и получать трафик, который обычно поступает на такой порт.

- Убедитесь в том, что транковые порты используют уникальный номер VLAN (виртуальной локальной сети), который не используется ни в каком другом месте этого коммутатора. В результате пакеты, имеющие метку с тем же номером, будут передаваться в другую сеть VLAN только через устройство Уровня 3. Более подробную информацию см. на сайте http://www.sans.org/newlook/resources/IDFAQ/vlan.htm
- Объедините все неиспользуемые порты коммутатора в сеть VLAN, которая не имеет выхода на Уровень 3. Будет еще лучше, если вы вообще отключите все порты, которые реально не используются. В результате хакеры не смогут подключаться к таким портам и через них получать доступ к другим сетевым ресурсам.
- Старайтесь не использовать технологию VLAN в качестве единственного способа защиты доступа между двумя подсетями. Постоянно присутствующая вероятность ошибок, а также тот факт, что сети VLAN и протоколы маркирования VLAN разрабатывались без учета требований безопасности, — все это не позволяет рекомендовать применение этих технологий в чувствительной среде. Если вы все-таки используете сети VLAN в защищенной среде, обратите особое внимание на конфигурации и рекомендации, перечисленные выше.

В существующей сети VLAN дополнительную защиту для некоторых сетевых приложений могут дать виртуальные частные локальные сети (private VLAN). Основной принцип их работы состоит в том, что они ограничивают число портов, которым разрешается связываться с другими портами в пределах одной и той же сети VLAN. Порты, которые относятся к определенному сообществу, могут сообщаться только с другими портами того же сообщества и портами общего доступа (promiscuous ports). Порты общего доступа могут связываться с любым портом. Это позволяет минимизировать ущерб от хакерского проникновения на один из хостов. Рассмотрим в качестве примера стандартный сетевой сегмент, состоящий из web-сервера, сервера FTP и сервера доменных имен (DNS). Если хакер проник на сервер DNS, для работы с двумя другими серверами ему уже не нужно преодолевать межсетевой экран. Но если у вас имеются виртуальные локальные частные сети, то в случае проникновения хакера на одну из систем она не сможет связываться с другими системами. Единственными целями для хакера остаются хосты, находящиеся по другую сторону межсетевого экрана.

Цель — хосты

Хост является наиболее вероятной целью хакерской атаки. Кроме того, хост создает самые сложные проблемы для обеспечения безопасности. Существует множество аппаратных платформ, операционных систем и приложений — и все это периодически обновляется, модернизируется и корректируется, причем в разные сроки. Поскольку хосты предоставляют другим хостам услуги по требованию, их очень хорошо видно в сети. К примеру, многие посещали сайт Белого Дома http://www.whitehouse.gov (это хост), но вряд ли кто-нибудь пытался получить доступ к адресу s2-0.whitehouse.net (это маршрутизатор). Поскольку хосты так хорошо видны, именно через них чаще всего совершаются попытки несанкционированного доступа в сеть.

По этим причинам хосты чаще других устройств становятся жертвами удачных атак. Зачастую web-сервер в сети Интернет работает на аппаратной платформе одного производителя с сетевым адаптером другого производителя, с операционной системой третьего поставщика и серверным программным обеспечением, которое либо является открытым, либо поставлено четвертой компанией. Кроме того, на этом web-сервере могут работать приложения, свободно распространяемые через Интернет. И, наконец, этот сервер может связываться с сервером базы данных, где все «разнообразие» повторяется еще раз. Мы не хотим сказать, что угроза безопасности происходит из-за разнородности источников сетевых устройств. Цель у нас другая: показать, что по мере увеличения сложности системы повышается вероятность сбоев и отказов.

Для защиты хоста необходимо внимательно следить за всеми компонентами системы. Все они должны быть самыми свежими, со всеми «заплатками» и коррекционными модулями. В частности, следите за тем, как эти модули влияют на функционирование других системных компонентов. Прежде чем установить модуль или новую версию в производственную среду, тщательно протестируйте их в испытательной среде. Если этого не сделать, новый модуль может привести к отказу в обслуживании (denial of service — DoS).

Цель — сеть

Самая ужасная атака — та, которую вы не можете остановить. При тщательной подготовке и исполнении именно такой является атака типа «распределенный отказ в обслуживании» (distributed denial of service — DDoS). Как показано в Приложении В «Основы сетевой безопасности», эта атака заставляет десятки или даже сотни машин одновременно отправлять ненужные данные на определенный IP-адрес. Цель атаки состоит в том, чтобы не просто «повесить» отдельный хост, а прекратить функционирование целой сети. Представьте себе организацию с каналом доступа DS3 (45 Мбит/с), которая предоставляет услуги электронной коммерции пользователям своего web-сайта. Этот сайт хорошо защищен от самых разных атак. Он имеет систему обнаружения атак, межсетевые экраны, систему авторизации доступа и средства ак-

тивного мониторинга. К сожалению, все эти средства не могут защитить от хорошо подготовленной атаки типа DDoS.

Представьте себе сто устройств, находящихся в разных уголках мира. Каждое из них имеет канал доступа DS1 (1,5 Мбит/с). Если этим системам в удаленном режиме дать соответствующую команду, они легко и просто заполнят канал DS3 ненужной информацией. Даже если каждый хост может сгенерировать трафик объемом 1 Мбит/с (а лабораторные испытания показали, что при наличии специального средства DDoS обычная рабочая станция Unix может легко сгенерировать и 50 Мбит/с), это более чем в два раза перекроет полосу пропускания атакуемого сайта. В результате сайт не сможет реагировать на реальные запросы и с точки зрения пользователей будет неработоспособным. Разумеется, местный межсетевой экран отфильтрует ложные данные, но будет поздно. Ущерб уже будет нанесен. Трафик пройдет по каналу связи с территориальной сетью и заполнит весь канал до предела.

Компания может надеяться на отражение таких атак только с помощью Интернет-провайдера. Провайдер может определить максимально допустимые границы для трафика, передаваемого на корпоративный сайт. При достижении пороговой величины нежелательный трафик будет отбраковываться. Главное здесь — правильно пометить трафик как нежелательный.

Обычно атаки типа DDoS проводятся в форме переполнения ICMP, переполнения TCP SYN или переполнения UDP. В среде электронной коммерции этот тип трафика очень легко категоризировать. Только в случае ограничения атаки TCP SYN на порту 80 (http) администратор рискует блокировать санкционированных пользователей. И даже в этом случае лучше временно блокировать несколько пользователей и сохранить маршрутизацию и каналы управления, чем «повесить» маршрутизатор и потерять все соединения.

Более изощренные хакеры используют атаки через порт 80 с установленным битом ACK таким образом, что трафик выглядит как обычный результат web-транзакций. Администратор вряд ли сможет правильно распознать такую атаку, поскольку используемый ею трафик TCP носит точно такой же характер, что и обычный трафик, который необходимо пропускать в сеть.

Одним из способов ограничения опасности таких атак является четкое следование рекомендациям RFC 1918 и RFC 2827. RFC 1918 определяет сети, зарезервированные для частного пользования, которые никогда не должны связываться с общедоступной сетью Интернет. Фильтрация RFC 2827 описана в разделе «IP-спуфинг» Приложения В «Основы сетевой безопасности». Вы можете использовать RFC 1918 и RFC 2827 для фильтрации входящего трафика на маршрутизаторе, подключенном к Интернет, чтобы предотвратить проникновение несанкционированного трафика в корпоративную сеть. При использовании у Интернет-провайдера такая фильтрация не позволяет передавать по каналам WAN пакеты DDoS, использующие эти адреса в качестве источников, что в принципе должно защитить полосу пропускания в случае атаки. Если бы все Интернет-провайдеры мира следовали рекомендациям RFC 2827, угроза спуфинга исходных адресов потеряла бы свою остроту. Хотя подобная стратегия не дает стопроцентной защиты от атак типа DDoS, она не позволяет хакерам маскировать источник атаки, что значительно облегчает поиск атакующей сети.

Цель — приложения

Исходные коды приложений, как правило, пишутся людьми и поэтому неизбежно содержат ошибки. Ошибки могут быть мелкими (например ошибки, возникающие при распечатке документов) или весьма неприятными (к примеру, в результате ошибки номер вашей кредитной карты, хранящийся в базе данных, может стать доступным по протоколу FTP для анонимного пользователя). На обнаружение ошибок второго типа, а также других слабостей более общего характера и нацелены системы обнаружения вторжений (intrusion detection system — IDS), которые действуют как системы предупреждения. Когда IDS обнаруживает что-то похожее на атаку, она может предпринять самостоятельные действия или уведомить систему управления, чтобы соответствующие действия мог предпринять сетевой администратор. Некоторые системы такого типа снабжаются более или менее эффективными средствами реагирования и отражения атак. Системы обнаружения атак, работающие на хостах (host-based IDS — HIDS), могут перехватывать вызовы операционных систем и приложений на отдельном хосте. Кроме того, они могут впоследствии проводить анализ локальных лог-файлов. Перехват позволяет лучше предотвращать атаки, а анализ представляет собой пассивное средство реагирования. Специфика хост-систем (HIDS) делает их более эффективными для предотвращения атак некоторых типов по сравнению с сетевыми системами NIDS (network IDS), которые обычно выдают сигнал тревоги только после обнаружения атаки. Однако та же специфика не дает хост-системам общесетевой перспективы, которой в полной мере обладают системы NIDS. Поэтому Cisco рекомендует сочетать системы обоих типов и размещать HIDS на критически важных хостах, а NIDS — для наблюдения за всей сетью. В результате такого сочетания возникает полномасштабная система обнаружения атак.

После установки системы необходимо настроить ее, чтобы повысить эффективность и сократить число ложных срабатываний. Под ложным срабатыванием понимается сигнал тревоги, вызванный не атакой, а обычным трафиком или обычной деятельностью. Отрицательным срабатыванием называется случай,

когда система не обнаруживает настоящей атаки. После настройки системы IDS вы можете точно сконфигурировать ее для конкретных действий по ликвидации угроз. Как уже отмечалось, нужно нацеливать HIDS на ликвидацию наиболее опасных угроз на уровне хоста, потому что именно здесь HIDS может работать с наибольшей эффективностью.

Определяя роль системы NIDS, вы можете выбрать один из двух основных вариантов.

Первый вариант (и потенциально — в случае неправильного внедрения — наиболее опасный) — это «отрубание» трафика с помощью фильтров управления доступом, установленных на маршрутизаторах. Если система NIDS обнаруживает атаку, источником которой является какой-либо хост, она блокирует этот хост, не давая ему возможности на определенное время связываться с данной сетью. На первый взгляд этот способ кажется очень удобным и хорошо помогает администратору безопасности, однако в действительности прибегать к нему следует с большой осторожностью, а, возможно, и не прибегать вовсе. Первая проблема состоит в том, что хакер может пользоваться чужими адресами. Если система NIDS решает, что атака идет с определенного устройства, и «отрубает» это устройство, оно теряет права доступа к вашей сети. Однако, если хакер пользуется чужим адресом, NIDS блокирует адрес, хозяин которого никогда не планировал никаких атак. Если для атаки хакер использовал IP-адрес мощного прокси-сервера HTTP, вы блокируете множество ни в чем не повинных пользователей. В руках творчески настроенного хакера этот механизм сам по себе может стать удобным инструментом для атаки типа DoS.

Для смягчения описанного выше риска метод «отрубания» нужно использовать только для трафика TCP, но там, где спуфинг адресов осуществить гораздо труднее, чем в области UDP. Пользуйтесь этим методом только в случае реальной угрозы и при минимальной вероятности ложного срабатывания. Однако в пределах одной сети существует гораздо больше вариантов. Эффективное внедрение фильтрации RFC 2827 может значительно ограничить объем трафика, поступающего с чужих адресов. Кроме того, поскольку заказчики обычно не включаются в состав внутренней сети, вы можете предпринять более жесткие меры против атак, исходящих из внутрикорпоративных источников. Еще одна причина для более жестких внутренних мер состоит в том, что внутренние сети, как правило, не имеют таких мощных средств фильтрации с учетом состояния соединений (stateful filtering), которые обычно используются на границе сети. Поэтому во внутренней сети вам следует более серьезно полагаться на систему IDS, чем во внешней среде.

Вторым вариантом для NIDS является сокращение угроз за счет использования сброса TCP (TCP reset). Как видно из названия этого метода, он используется только для трафика TCP. Прекращение атаки производится отправлением сообщений «TCP reset» на атакующий и атакуемый хост. Поскольку трафик TCP хуже поддается спуфингу, этот метод является более предпочтительным, чем метод грубого «отрубания» адресов.

Этот метод чувствителен к производительности. Система NIDS отслеживает передаваемые пакеты. Если скорость передачи пакетов превосходит возможности NIDS, снижения производительности в сети не происходит, так как NIDS не находится на пути потоков данных. Однако при этом теряется эффективность самой системы NIDS, которая начинает терять пакеты, срабатывать в спокойной обстановке и не замечать настоящих атак. Поэтому, чтобы в полной мере воспользоваться всеми преимуществами NIDS, не превышайте возможностей этой системы. С точки зрения маршрутизации, IDS, как и многие системы, способные учитывать состояние, некорректно функционирует в асимметрично маршрутизируемой среде. Если группа маршрутизаторов и коммутаторов передает пакеты по одному маршруту, а принимает по другому, система IDS будет видеть только половину трафика, что вызовет ложные срабатывания и нулевую реакцию на реальные атаки.

Безопасное управление и отчетность

«Хотите записать данные? Тогда попробуйте сначала их прочитать». Простая мысль, не так ли? Любой специалист по сетевой безопасности наверняка высказывал ее хотя бы однажды. И все же запись и чтение информации, поступающей со ста с лишним устройств, представляет собой сложную задачу. Какие записи являются наиболее важными? Как отделить важные сообщения от рутинных уведомлений? Как обеспечить защиту данных во время передачи? Как синхронизировать метки времени, если множество устройств одновременно регистрируют атаку? Какую информацию нужно предоставлять правоохранительным органам, ведущим расследование? Как справиться с огромным объемом данных, которые генерирует большая сеть? Для эффективного управления журналами событий (лог-файлами) вам нужно найти ответ на каждый из этих вопросов. На уровне сетевого управления можно предложить другой набор вопросов. Как управлять устройством в безопасном режиме? Как передавать содержание на серверы общего доступа, чтобы исключить искажение данных во время передачи? Как отслеживать изменения в устройствах, чтобы исправить положение в случае атаки или сетевого сбоя?

С архитектурной точки зрения, первым шагом в реализации любой стратегии управления и отчетности является управление сетевыми системами по выделенной сети (out-of-band — OOB). Как видно из названия, это означает, что для управления используется сеть, по которой не передается производственный

трафик. По возможности, устройства должны иметь прямой локальный доступ к такой сети. Если такой возможности нет (по географическим или системным причинам), подключение устройств должно происходить через производственную сеть по частному зашифрованному туннелю. Этот туннель должен быть настроен на связь только через определенные порты, предназначенные для управления и отчетности. Кроме того, туннель должен блокироваться так, чтобы открывать или закрывать его могли только определенные хосты. Убедитесь в том, что дополнительная сеть (OOB) не имеет своих собственных проблем с безопасностью. Более подробную информацию можно получить в разделе «Модуль управления».

После развертывания сети управления OOB работа с лог-файлами и отчетностью становится более простой и логичной. При этом большинство сетевых устройств будут генерировать системные данные (syslog data), имеющие огромную ценность для диагностики сетевых проблем и анализа угроз безопасности. Эти данные можно передавать одному или нескольким хостам, отвечающим за анализ системных данных в сети управления. В зависимости от устройства, можно выбирать разные уровни регистрации данных, чтобы в лог-файлы поступало необходимое количество информации. Кроме того, вам необходимо помечать данные, относящиеся к тому или иному устройству, чтобы обеспечить точное и детальное рассмотрение и анализ данных. К примеру, во время атаки данные, предоставляемые коммутаторами Уровня 2, могут быть не столь интересны, как данные, предоставляемые системой обнаружения атак (IDS). Специализированные приложения, такие как IDS, часто пользуются собственными протоколами для передачи уведомлений об атаках. Обычно данные подобного типа должны сохраняться на отдельных хостах управления, которые лучше приспособлены для обработки таких уведомлений. Обобщение данных об атаке может дать представление об общем состоянии безопасности сети. Чтобы синхронизировать лог-сообщения о времени, необходимо синхронизировать системное время на хостах и сетевых устройствах. Точное время на всех устройствах можно поддерживать с помощью протокола сетевого времени NTP (Network Time Protocol), если устройства его поддерживают. При отражении атак счет времени идет на секунды, и поэтому очень важно определить точную последовательность событий.

При управлении, к которому в настоящем документе мы относим все, что делает с устройством администратор, за исключением отчетности и записей в лог-файлы, существуют другие проблемы и решения. Так же, как и в случае с записями в лог-файлы и отчетностью, сеть OOB позволяет передавать информацию в контролируемой защищенной среде, где ее невозможно исказить. И все же, если есть возможность использовать дополнительные средства защиты, такие как SSL (secure socket layer) или SSH (secure shell), то они позволяют повысить уровень защищенности. К протоколу управления SNMP нужно относиться с величайшей осторожностью, так как этот протокол имеет свои точки уязвимости. Подумайте о том, чтобы предоставить доступ к устройствам по SNMP только на чтение. При этом к паролю для доступа к переменным SNMP (SNMP community string) следует относиться с таким же вниманием, как к корневому паролю на критически важном Unix-хосте.

Управление изменениями конфигурации также имеет отношение к безопасности. Когда сеть подвергается атаке, очень важно знать состояние критически важных сетевых устройств и сроки их последней модификации. План управления изменениями конфигурации должен быть составной частью вашей политики безопасности. Как минимум, следует записывать все изменения с помощью имеющихся на устройствах систем аутентификации и архивировать конфигурации через FTP или TFTP.

Корпоративный модуль крупного предприятия

Корпорация состоит из двух функциональных областей: кампуса и периферии. Эти области, в свою очередь, делятся на модули, которые определяют детали функционирования каждой из областей. Модули подробно описываются в разделах «Корпоративный кампус» и «Корпоративная периферия». После этого в разделе «Корпоративные опции» описываются различные варианты дизайна.

Ожидаемые угрозы

Говоря об угрозах, следует отметить, что корпоративная сеть, как и большинство других сетей, подключена к Интернет. Внутренние пользователи должны получать выход в Интернет, а внешние пользователи должны получать доступ к внутрикорпоративной сети. Это создает ряд угроз общего характера, которые могут дать хакеру щелочку, через которую он может проникнуть к важным сетевым ресурсам.

Первая угроза — это угроза со стороны внутренних пользователей. Статистика приводит разные цифры, но все исследователи сходятся в том, что большинство атак начинается изнутри корпоративной сети. Потенциальными источниками таких атак являются обиженные сотрудники, промышленные шпионы, посетители и беспечные пользователи, допускающие ошибки. Разрабатывая систему безопасности, необходимо уделять особое внимание внутренним угрозам.

Второй является угроза подключенным к Интернет хостам общего доступа. Эти системы являются потенциальными объектами атак на уровне приложений и атак типа DoS.

И наконец, еще одна угроза связана с тем, что хакер может попытаться определить ваши телефонные номера, которые используются для передачи данных, с помощью аппаратного и/или программного устрой-

ства под названием «war-dialer». Это устройство набирает множество телефонных номеров и определяет тип системы, находящейся на другом конце провода. Наиболее уязвимыми для них являются слабо защищенные персональные системы с программными средствами удаленного доступа, установленными пользователем. Такие системы расположены внутри зоны, защищенной межсетевым экраном, и поэтому хакер пытается получить доступ к ним через хост, поскольку это позволяет обезличить пользователя.

Подробное описание угроз содержится в Приложении В «Основы сетевой безопасности».

Корпоративный кампус

Ниже следует детальное описание всех модулей, расположенных в корпоративном кампусе.

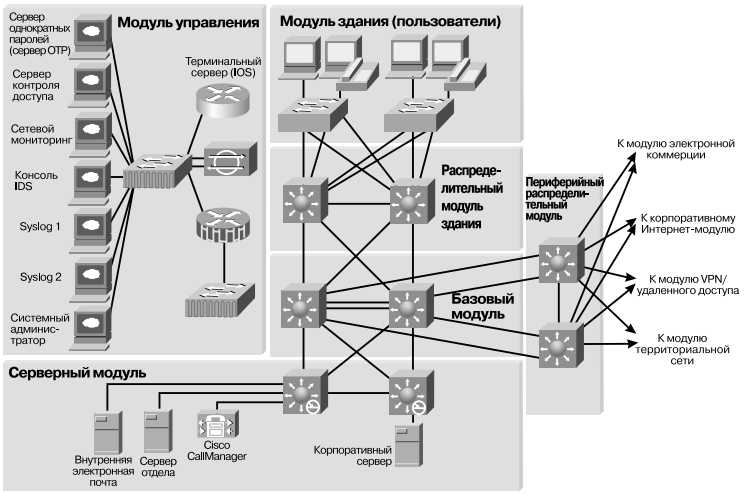


Рисунок 35. Подробная схема корпоративного кампуса

Модуль управления

Главная цель модуля управления состоит в том, чтобы обеспечить безопасное управление всеми устройствами и хостами в корпоративной архитектуре SAFE. Потоки отчетности и информации для лог-файлов поступают с устройств на хосты управления, тогда как изменения конфигурации и новое программное обеспечение поступают с хостов управления на устройства.

Основные устройства:

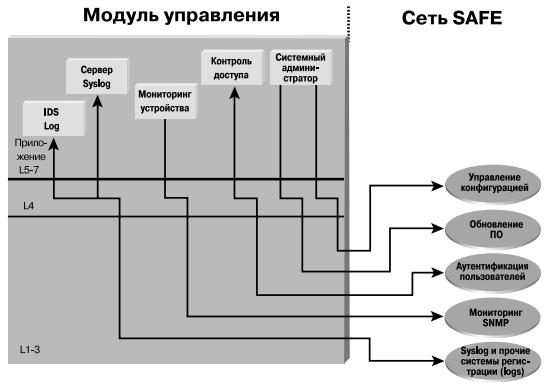


Рисунок 36. Поток трафика управления

- *хост управления SNMP* — поддерживает функции управления устройствами по протоколу SNMP;
- *хост NIDS* — собирает сигналы тревоги по всем устройствам NIDS в сети;
- *хост(ы) Syslog* — получает информацию от межсетевого экрана и хостов NIDS;
- *сервер контроля доступа* — обеспечивает аутентификацию доступа к сетевым устройствам с помощью однократных паролей;
- *сервер одноразовых паролей (сервер OTP)* — авторизует информацию по однократным паролям, поступающую с сервера контроля доступа;
- *хост системного администратора* — обеспечивает изменение конфигурации устройств и их программного обеспечения;
- *устройство NIDS* — позволяет мониторить потоки трафика между хостами управления и управляемыми устройствами;
- *коммутатор Уровня 2 (с поддержкой виртуальных локальных частных сетей)* — обеспечивает передачу данных с управляемых устройств только на межсетевой экран IOS.

Предотвращаемые угрозы:

- *несанкционированный доступ* — фильтры межсетевого экрана IOS пресекают почти все потоки несанкционированного трафика в обоих направлениях;
- *атаки типа Man-in-the-Middle* — информация, связанная с управлением, передается по частной сети, что весьма затрудняет атаки этого типа;
- *хакерская разведка сети* — поскольку весь трафик, связанный с управлением, передается по частной сети, он не попадает в производственную сеть, где его может перехватить хакер-разведчик;
- *атаки на пароли* — сервер контроля доступа поддерживает мощную двухфакторную аутентификацию на каждом устройстве;
- *IP-спуфинг* — межсетевой экран IOS пресекает (в обоих направлениях) потоки трафика, использующие чужие адреса;

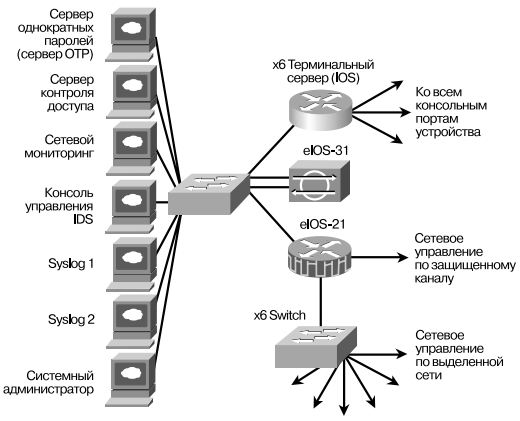


Рисунок 37. Модуль управления

- *сниффинг пакетов* — коммутируемая инфраструктура снижает эффективность сниффинга;
- *злоупотребление доверием* — виртуальные локальные частные сети не дают возможности выдавать за хост управления устройства, попавшие под контроль хакера.

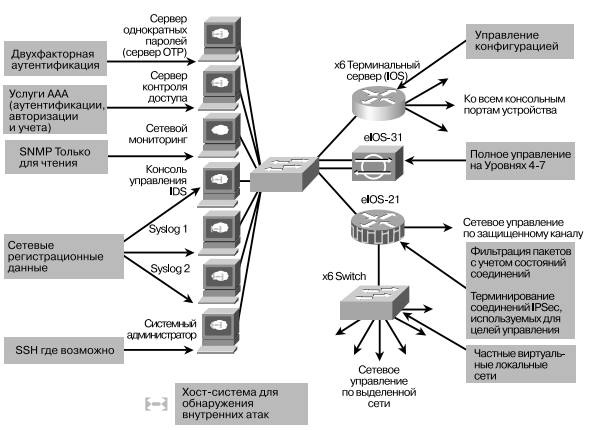


Рисунок 38. Модуль управления: функции предотвращения атак

Рекомендации по дизайну

Как видно из приведенной выше схемы, корпоративная сеть управления SAFE имеет два сетевых сегмента, которые разделены маршрутизатором IOS, выполняющим роль межсетевого экрана и устройства терминирования виртуальной частной сети (VPN). Сегмент, находящийся с внешней стороны межсетевого экрана, соединяется со всеми устройствами, которые нуждаются в управлении. Сегмент, находящийся с внутренней стороны, включает хосты управления и маршрутизаторы IOS, которые выступают в качестве терминальных серверов. Другой интерфейс подключается к производственной сети, но лишь для передачи защищенного средствами IPSec трафика управления с заранее определенных хостов. Это позволяет управлять даже теми устройствами Cisco, которые не имеют достаточного числа интерфейсов для подключения к внешней сети управления. Межсетевой экран IOS конфигурируется таким образом, чтобы передавать информацию syslog в сегмент управления, а также соединения Telnet, SSH и SNMP, если таковые инициированы из внутренней сети.

Обе подсети управления работают в адресном пространстве, которое полностью отделено от производственной сети. В результате протоколы маршрутизации не распространяют данные о сети управления. Кроме того, устройства производственной сети блокируют любой трафик, попадающий из сети управления в производственные сегменты.

Модуль управления поддерживает управление конфигурацией практически всех сетевых устройств с помощью двух базовых технологий: маршрутизаторов Cisco IOS, действующих в качестве терминальных серверов, и сетевого сегмента, специально выделенного для управления. Маршрутизаторы выполняют функцию reverse-telnet для доступа к консольным портам на устройствах Cisco по всей корпорации. Более широкие функции управления (изменения ПО, обновления содержания, обобщение лог-данных и сигналов тревоги, управление SNMP) поддерживаются с помощью выделенного сегмента сетевого управления. Все остающиеся неуправляемые устройства и хосты (а их остается крайне мало) управляются через туннели IPSec, которые идут от маршрутизатора управления.

Поскольку сеть управления имеет доступ с правами администратора практически ко всем областям сети, она может стать весьма привлекательной целью для хакеров. Поэтому в модуль управления встроено сразу несколько технологий, специально предназначенных для смягчения подобных рисков. Первым и основным риском является попытка хакера получить доступ к самой сети управления. Все остальные риски исходят из того, что первая линия обороны уже прорвана. Чтобы не дать хакеру завладеть каким-либо сетевым устройством, на межсетевом экране и на каждом устройстве имеются средства контроля доступа, которые предотвращают несанкционированный доступ к каналу управления. Захваченное хакером устройство не сможет связаться с другими хостами, находящимися в той же подсети, поскольку сегмент управления направляет весь трафик с управляемых устройств непосредственно на межсетевой экран IOS, где производится фильтрация. Сниффинг паролей вообще оказывается неэффективным, поскольку пароли являются одноразовыми. Кроме того, в подсети управления устанавливаются системы HIDS и NIDS, которые настраиваются на очень жесткий режим. Поскольку в этой подсети передается весьма ограниченное количество типов трафика, любое совпадение сигнатуры должно вызывать немедленную реакцию.

Управление по протоколу SNMP имеет собственные требования к безопасности. Поддержка трафика SNMP в сегменте управления позволяет ему пересекать изолированный сегмент, собирая информацию с устройств. В архитектуре SAFE средства управления SNMP только собирают информацию, но не имеют возможности принудительно вносить изменения в конфигурацию. Для этого каждое устройство настраивается на работу с SNMP в режиме «только для чтения».

Большое значение для правильного управления сетью имеет правильный сбор и анализ системной информации (syslog). Syslog предоставляет важные данные о нарушениях безопасности и изменениях конфигурации. От разных устройств могут потребоваться разные уровни информации syslog. Полная информация обо всех отправленных сообщениях является слишком объемной, что не позволяет эффективно обработать ее ни человеку, ни алгоритму syslog. Таким образом, запись всех данных в лог-файлы «на всякий случай» не может повысить безопасность сети.

Для оценочной лаборатории SAFE использовались конфигурации только с отдельными приложениями управления и интерфейсом командной строки (CLI). Однако в SAFE нет никаких препятствий для использования систем конфигурирования, основанных на политике безопасности. Использование нашего модуля управления позволяет с успехом внедрять подобные технологии. Мы выбрали интерфейс командной строки и отдельные приложения управления, поскольку сегодня такой метод конфигурирования используется в большинстве развернутых сетей.

Альтернативы

Полномасштабное управление по отдельному каналу не всегда возможно, так как некоторые устройства могут его не поддерживать. Кроме того, управление по основному каналу связи может потребоваться в силу некоторых географических различий. Если вы передаете управляющие сигналы по основному каналу связи, следует обратить особое внимание на защиту транспорта протоколов управления. Это достигается с помощью IPSec, SSH SSL или любых других технологий шифрования и аутентификации транспорта, позволяющих передавать данные управления в безопасном режиме. Когда для управления используется тот же интерфейс, что и для передачи пользовательских данных, особое внимание нужно обратить на пароли, community strings, криптографические ключи и списки доступа, которые контролируют связь с услугами управления.

Требования к архитектуре будущего

В настоящее время задачи отчетности и аварийной сигнализации распределены между множеством хостов. Некоторые из них лучше обрабатывают данные межсетевых экранов и систем IDS, другие лучше приспособлены для анализа данных маршрутизации и коммутации. В будущем все данные будут агрегироваться на одном и том же массиве избыточных хостов, что позволит сравнивать события, происходящие на всех устройствах.

Базовый модуль

В архитектуре SAFE базовый модуль практически идентичен базовому модулю любой другой сетевой архитектуры. Его задача состоит в маршрутизации и коммутации межсетевого трафика с как можно более высокой скоростью.

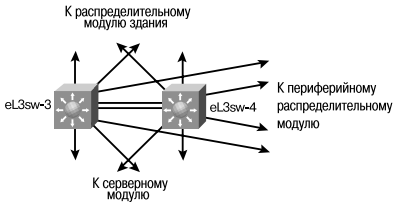


Рисунок 39. Базовый модуль

Основные устройства

- *Коммутация Уровня 3* — маршрутизация и коммутация данных в производственной сети с одного модуля на другой.

Предотвращаемые угрозы

- Сниффинг пакетов — коммутируемая инфраструктура ограничивает эффективность сниффинга.

Рекомендации по дизайну

Мы следовали стандартным рекомендациям по дизайну, которые обычно используются в хорошо спроектированных сетях Cisco на базовом уровне, уровне распределения и уровне доступа.

Хотя архитектура SAFE не предъявляет никаких особых требований к базовой части корпоративной сети, при настройке коммутаторов этой сети необходимо следовать «аксиомам безопасности», изложенным в разделе «Цель — коммутаторы», чтобы должным образом защитить эти устройства от прямых атак.

Распределительный модуль здания

Этот модуль предоставляет услуги доступа коммутаторам здания. Услуги включают маршрутизацию, поддержку гарантированного качества услуг (QoS) и контроль доступа. Запросы о предоставлении данных поступают на коммутаторы и далее в базовую сеть. Ответный трафик следует по тому же маршруту в обратном направлении.

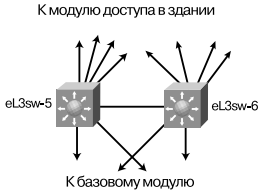


Рисунок 40. Распределительный модуль здания: детали, направленные на предотвращение угроз

Основные устройства

- Коммутаторы Уровня 3 — агрегируют коммутаторы Уровня 2 в модуль здания и предоставляют продвинутые услуги.

Предотвращаемые угрозы

- Несанкционированный доступ — атаки на ресурсы серверного модуля ограничиваются фильтрацией определенных подсетей на Уровне 3.
- IP-спуфинг — фильтрация RFC 2827 пресекает практически любые попытки спуфинга.
- Сниффинг пакетов — коммутируемая инфраструктура ограничивает эффективность сниффинга.

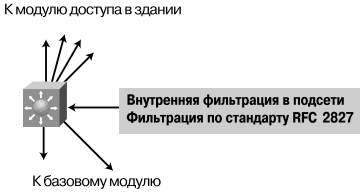


Рисунок 41. Функции распределительного модуля здания, направленный на смягчение угроз

Рекомендации по дизайну

Для усиления защищенности корпоративных пользователей использовались не только стандартные принципы сетевого проектирования, но и оп-

тимизации, описанные в разделе «Цель — коммутаторы». Распознавание атак происходит не в распределительном модуле здания, а в модулях, где имеются ресурсы, которые являются потенциальными объектами атак из-за своего содержания (серверы, средства удаленного доступа, средства Интернет и т. д.). Распределительный модуль здания представляет собой первую линию обороны и предотвращения атак, источник которых находится внутри корпорации. Этот модуль с помощью средств контроля доступа может снизить вероятность получения одним отделом конфиденциальной информации с сервера другого отдела. К примеру, в сети, где имеются данные о маркетинге и НИОКР, можно выделить сервер НИОКР в отдельную виртуальную сеть (VLAN) и установить фильтр, допускающий к этой информации только сотрудников научно-исследовательского отдела. Для поддержки высокой производительности очень важно иметь контроль доступа на аппаратной платформе, которая могла бы фильтровать трафик со скоростью, близкой к скорости передачи трафика по каналам связи. Обычно для этого используют не традиционные маршрутизирующие устройства, а коммутацию Уровня 3. Та же система контроля доступа с помощью фильтрации RFC 2827 может предотвращать локальный спуфинг адресов источника информации. И наконец, для маршрутизации трафика типа «голос поверх IP» (VoIP) на CallManager и любые ассоциированные шлюзы используются отдельная виртуальная локальная сеть и подсеть IP. Эта система не позволяет трафику VoIP пересекать те же сетевые сегменты, что и трафику данных. В результате снижается вероятность сниффинга голосовых сообщений и оптимизируется поддержка гарантированного качества услуг (QoS).

Альтернативы

В зависимости от размеров сети и проектируемой производительности, уровень распределения может объединяться с базовым уровнем, чтобы снизить общее число устанавливаемых устройств.

Модуль здания

SAFE определяет модуль здания как значительную часть сети, которая содержит рабочие станции конечных пользователей, телефоны и связанные с ними точки доступа Уровня 2. Главная цель этого модуля состоит в том, чтобы предоставлять услуги конечным пользователям.

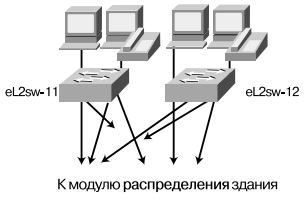


Рисунок 42. Модуль доступа для здания

Основные устройства

- *Коммутатор Уровня 2* — оказывает услуги Уровня 2 телефонам и рабочим станциям конечных пользователей.
- *Пользовательская рабочая станция* — оказывает авторизованным пользователям услуги по обработке данных.
- *IP-телефон* — оказывает пользователям сети услуги IP-телефонии.

Предотвращаемые угрозы

- *Сниффинг пакетов* — коммутируемая инфраструктура и услуги VLAN по умолчанию ограничивают эффективность сниффинга.
- *Вирусы и приложения типа «троянский конь»* — сканирование программ на вирусы производится на хостах, что позволяет эффективно избавляться от большинства вирусов и многих «троянских коней».

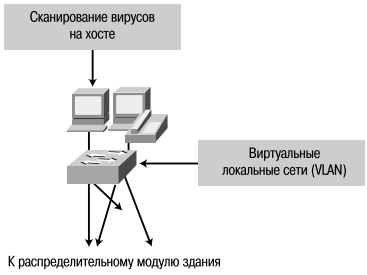


Рисунок 43. Борьба с атаками на уровне модуля доступа для здания

Рекомендации по дизайну

Поскольку пользовательские устройства являются основным сетевым элементом, для них очень важно проведение последовательной и эффективной политики безопасности. С точки зрения безопасности, распределительный модуль здания — более, чем какой-либо другой элемент в модуле здания, — обеспечивает контроль доступа на уровне конечных пользователей. Это происходит потому, что коммутатор Уровня 2, к которому подключаются рабочие станции и телефоны, не имеет возможностей контроля, характерных для Уровня 3. Помимо принципов сетевой безопасности, описанных в разделе, где говорилось об аксиомах безопасности серверов, на уровне рабочих станций реализуется еще и сканирование программ на наличие вирусов. Такое сканирование обычно проводится на хостах.

Серверный модуль

Основная задача серверного модуля состоит в предоставлении прикладных услуг устройствам и конечным пользователям. Потоки трафика в серверном модуле проверяются средствами IDS, встроенными в коммутаторы Уровня 3.

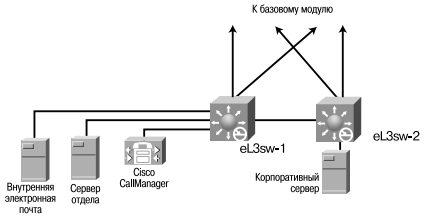


Рисунок 44. Серверный модуль

Основные устройства

- *Коммутатор Уровня 3* — оказывает серверам услуги Уровня 3 и проверяет проходящий по серверному модулю трафик с помощью системы NIDS.
- *CallManager* — выполняет функции маршрутизации вызовов для устройств IP-телефонии, установленных на предприятии.

- *Корпоративные серверы и серверы отделов* — оказывают рабочим станциям модуля здания услуги по обработке файлов, услуги печати и услуги DNS.
- *Сервер электронной почты* — оказывает корпоративным пользователям услуги SMTP и POP3.

Предотвращаемые угрозы

- *Несанкционированный доступ* — препятствием для несанкционированного доступа служат средства обнаружения атак на хостах и средства контроля доступа.
- *Атаки на уровне приложений* — операционные системы, устройства и приложения постоянно обновляются, к ним добавляются самые свежие модули безопасности. Кроме того, они защищаются системой HIDS.
- *IP-спуфинг* — фильтрация RFC 2827 предотвращает спуфинг адресов источников информации.
- *Сниффинг пакетов* — коммутируемая инфраструктура снижает эффективность сниффинга.
- *Злоупотребление доверием* — поскольку механизмы доверия являются весьма открытыми, частные сети VLAN позволяют хостам одной и той же подсети связываться друг с другом лишь в случае необходимости.
- *Переадресация портов* — система HIDS не позволяет устанавливать программные агенты, которые занимаются переадресацией портов.

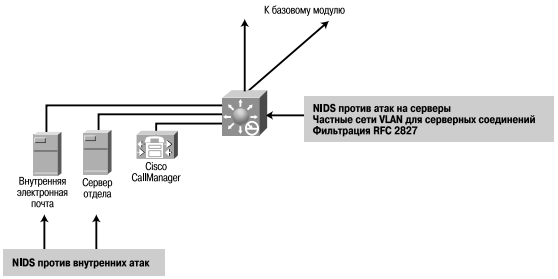


Рисунок 45. Борьба с атаками на серверном модуле

Рекомендации по дизайну

При проектировании систем безопасности на серверный модуль обычно обращают мало внимания. Однако если посмотреть, какой уровень доступа к корпоративным серверам имеет большинство сотрудников, станет ясным, почему эти серверы часто становятся главным объектом внутренних атак. Внедрение эффективных паролей само по себе не может считаться надежной стратегией защиты от атак. Гораздо более надежную защиту дает сочетание систем HIDS, NIDS, частных локальных сетей (VLAN), средств контроля доступа и эффективных процедур системного администрирования (включая установку самых свежих версий ПО и коррекционных модулей).

Поскольку системы NIDS могут анализировать ограниченный объем трафика, очень важно отправлять для анализа лишь тот трафик, который в наибольшей степени подвержен хакерским атакам. В разных сетях этот трафик может быть разным, но, как правило, он включает трафик SMTP, Telnet, FTP и WWW. Для этого выбирается система NIDS, работающая с серверами, поскольку эта система может отслеживать только интересующий вас трафик, передаваемый по всем сетям VLAN. Типы отслеживаемого трафика определяются политикой безопасности. После тщательной настройки эта система может устанавливаться на работу в очень строгом режиме, так как отслеживаемые потоки трафика являются хорошо известными.

Альтернативы

Серверный модуль, как и распределительный модуль здания, может объединяться с базовым модулем, если необходимость поддержки высокой производительности не потребует их разделения. В особо чувствительных сетях с высокой производительностью функции NIDS на коммутаторе Уровня 3 могут масштабироваться за счет установки нескольких модулей (blades) NIDS и балансирования трафика разных категорий безопасности между ними.

Периферийный распределительный модуль

Задача этого модуля состоит в агрегации соединений разных сетевых элементов на сетевой периферии. Трафик фильтруется и направляется с периферийных модулей в базовую сеть.

Основные устройства

- *Коммутаторы Уровня 3* — агрегируют периферийные соединения и предоставляют продвинутые услуги.

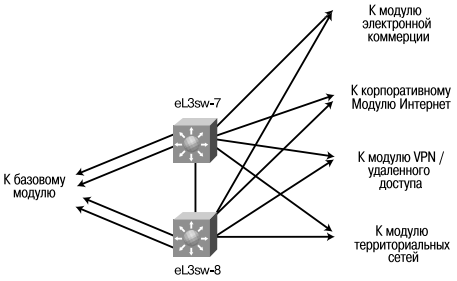


Рисунок 46. Периферийный распределительный модуль

Предотвращаемые угрозы

- *Несанкционированный доступ* — фильтрация предоставляет детальный контроль над отдельными периферийными подсетями и их способностью связываться с сетевыми элементами, расположенными в кампусе.
- *IP-спуфинг* — фильтрация RFC 2827 ограничивает возможности внутренних атак, пользующихся результатами спуфинга.
- *Сетевая разведка* — фильтрация ограничивает объем ненужного трафика, попадающего в кампус, и тем самым ограничивает возможности хакеров по ведению сетевой разведки.

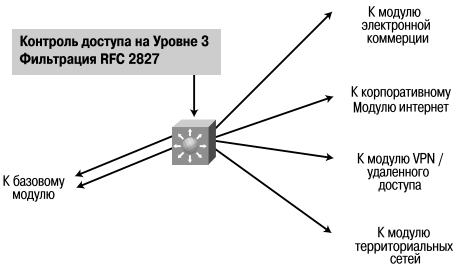


Рисунок 47. Борьба с атаками на периферийном распределительном модуле

- *Сниффинг пакетов* — коммутируемая инфраструктура ограничивает эффективность сниффинга.

Рекомендации по дизайну

По своей общей функциональности периферийный распределительный модуль похож на распределительный модуль здания. Оба модуля пользуются средствами контроля доступа для фильтрации трафика, хотя ряд возможностей сетевой периферии позволяет периферийному распределительному модулю поддерживать дополнительные функции безопасности. Для поддержки высокой производительности оба модуля пользуются коммутацией Уровня 3, но периферийный распределительный модуль обладает дополнительными возможностями в области безопасности, поскольку на сетевой периферии требования к производительности не столь высоки. Периферийный распределительный модуль представляет собой последнюю линию обороны для всего трафика, который передается с периферийного модуля на кампусный модуль. Эта линия должна пресекать попытки передачи пакетов с ложных адресов и несанкционированного изменения маршрутов, а также обеспечивать контроль доступа на уровне сети.

Альтернативы

Подобно серверному модулю и распределительному модулю здания, периферийный распределительный модуль может объединяться с базовым модулем, если требования производительности не являются такими же жесткими, как в приводимых здесь примерах архитектуры SAFE. В этом модуле отсутствует система NIDS, однако ее можно установить с помощью модулей IDS, работающих на коммутаторах Уровня 3. В этом случае сокращается необходимость в устройствах NIDS на выходе критически важных периферийных модулей, подключаемых к кампусу. Однако необходимость поддержки высокой производительности (как и в приводимом здесь примере архитектуры SAFE) может потребовать установки средств обнаружения атак на разных периферийных модулях, а не только на периферийном распределительном модуле.

Корпоративная периферия

В данном разделе приводится детальный анализ всех модулей, находящихся на периферии корпоративной сети.

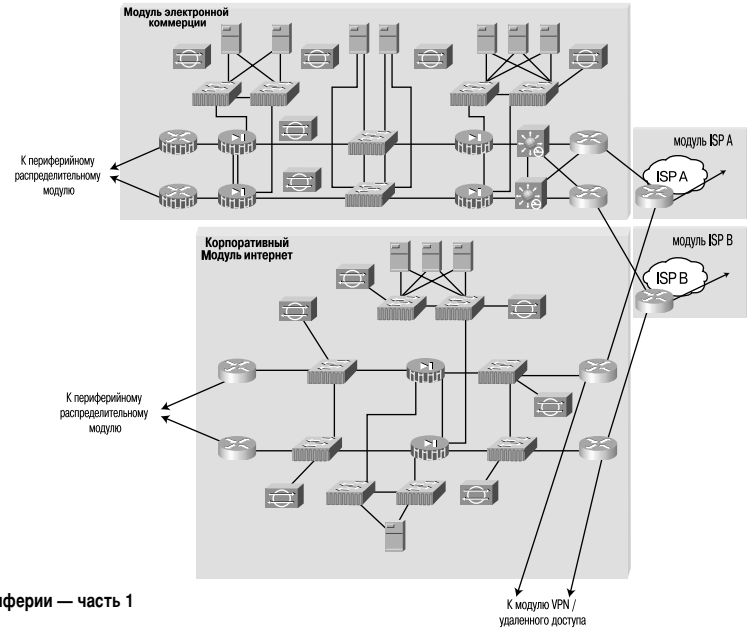


Рисунок 48. Детали корпоративной периферии — часть 1

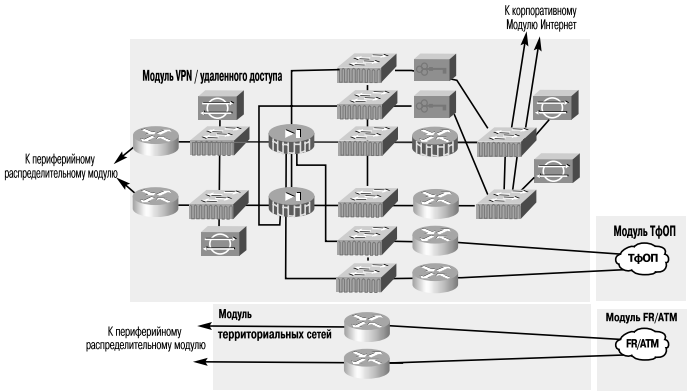


Рисунок 49. Детали корпоративной периферии — часть 2

Корпоративный модуль Интернет

Корпоративный модуль Интернет предоставляет внутрикорпоративным пользователям доступ к Интернет-услугам и информации, расположенной на серверах общего доступа. Трафик с этого модуля передается в виртуальные частные сети (VPN) и на модуль удаленного доступа, где происходит терминирование VPN. Этот модуль не предназначен для поддержки приложений электронной коммерции. Более подробная информация об электронной коммерции содержится в разделе «Модуль электронной коммерции».

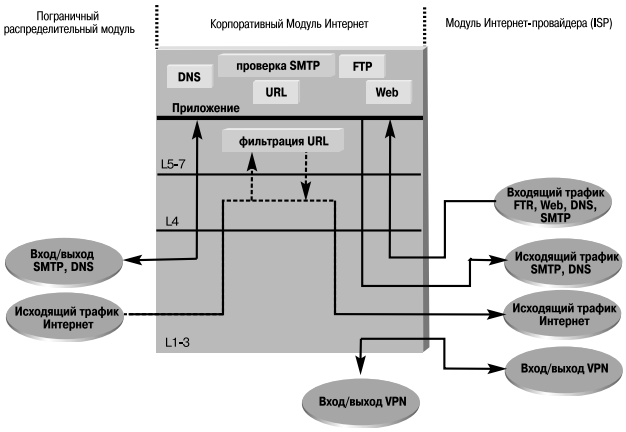


Рисунок 50. Поток корпоративного Интернет-трафика

Основные устройства

- *Сервер SMTP* — служит мостом между Интернет и серверами Интернет-почты — проверяет содержание.
- *Сервер DNS* — служит внешним сервером DNS для предприятия, передает в Интернет запросы внутренних пользователей.
- *Сервер FTP/HTTP* — предоставляет открытую информацию об организации.
- *Межсетевой экран* — защищает ресурсы на уровне сети и производит фильтрацию трафика.
- *Устройство NIDS* — поддерживает мониторинг ключевых сетевых сегментов модуля на Уровнях 4—7.
- *Сервер фильтрации URL* — отфильтровывает несанкционированные запросы URL, исходящие от предприятия.

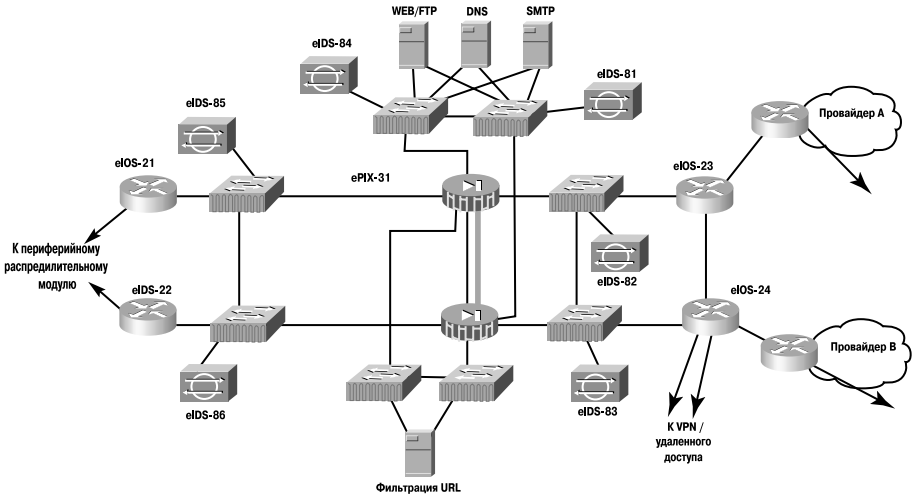


Рисунок 51. Корпоративный модуль Интернет

Предотвращаемые угрозы

- *Несанкционированный доступ* — угроза ликвидируется с помощью фильтрации на уровне провайдера (ISP), периферийного маршрутизатора и корпоративного межсетевого экрана.
- *Атаки на уровне приложений* — ликвидируются с помощью IDS на уровне хоста и сети.
- *Вирусы и «троянские кони»* — ликвидируются с помощью фильтрации содержания электронной почты и системы HIDS.
- *Атаки на пароли* — ограничение возможностей смены паролей, контролируемых средствами операционной системы и IDS.
- *Отказ в обслуживании (DoS)* — борьба с этой угрозой проводится с помощью CAR на периферии ISP и с помощью контроля установлений сессий TCP на межсетевом экране.
- *IP-спуфинг* — фильтрация RFC 2827 и 1918 на периферии ISP и корпоративном периферийном маршрутизаторе.
- *Сниффинг пакетов* — коммутируемая инфраструктура и система HIDS снижают эффективность сниффинга.
- *Сетевая разведка* — IDS обнаруживает попытки ведения разведки, а фильтрация на уровне протоколов снижает ее эффективность.
- *Злоупотребление доверием* — эта угроза снижается с помощью строгой модели доверия и за счет использования частных сетей VLAN.

- *Переадресация портов* — эта угроза снижается с помощью строгой фильтрации и системы HIDS.

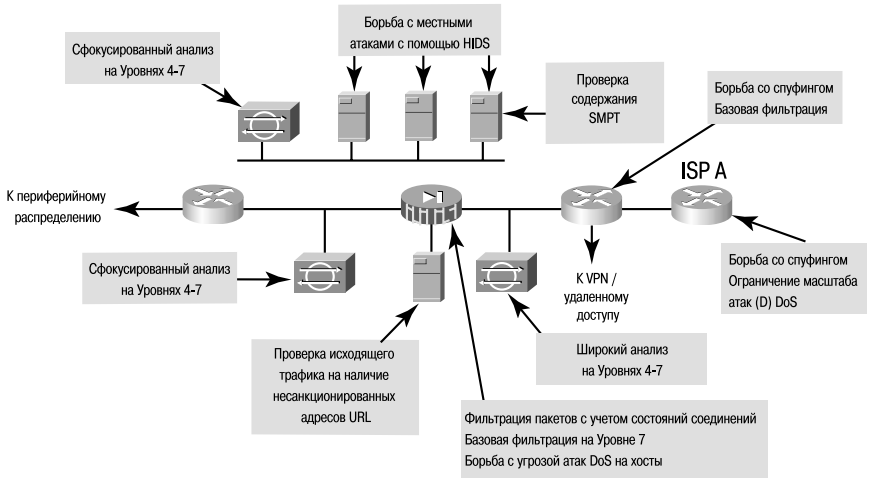


Рисунок 52. Борьба с угрозами с помощью корпоративного модуля Интернет

Рекомендации по дизайну

В основе модуля лежит пара отказоустойчивых межсетевых экранов, защищающих общедоступные услуги Интернет и внутренних пользователей. Экраны проверяют трафик, передаваемый во всех направлениях, и гарантируют пропускание только санкционированного трафика. Кроме средств, обеспечивающих устойчивость на Уровнях 2 и 3, и средств аварийного подхвата, все остальные элементы модуля нацелены на безопасность и борьбу с угрозами.

Начиная с маршрутизатора, находящегося на периферии сети заказчика ISP, происходит отбрасывание несущественного трафика, объем которого превышает заранее установленные пороговые значения, что в значительной степени снижает угрозу атак типа (D)DoS. Кроме того, на выходе маршрутизатора ISP производится фильтрация RFC 1918 и 2827, что снижает угрозу спуфинга адресов локальных сетей и частных адресов.

На входе первого маршрутизатора корпоративной сети производится базовая фильтрация, которая пропускает только ожидаемый (по адресам и IP-услугам) трафик. Этот фильтр «грубой очистки» помогает бороться с большинством наиболее распространенных атак. Здесь же происходит фильтрация RFC 1918 и RFC 2827 для подкрепления фильтрации, проведенной на уровне ISP. Кроме этого, ввиду огромной угрозы, исходящей от фрагментированных пакетов, маршрутизатор настраивается на отбрасывание большинства таких пакетов, которые обычно не соответствуют стандартным типам трафика Интернет. Происходящие при этом потери санкционированного трафика считаются приемлемыми, если принять во внимание огромный риск, который несут в себе фрагментированные пакеты. И наконец, любой трафик IPSec, адресованный на модуль VPN / удаленного доступа, передается по назначению. Фильтры, установленные на входе VPN пропускают только трафик IPSec, передаваемый с авторизованных узлов на авторизованные узлы. В сетях VPN с удаленным доступом IP-адрес системы, отправившей входящее сообщение, как правило, остается неизвестным, и поэтому фильтрация производится по центральным сетевым узлам, с которыми непосредственно связывается удаленный пользователь.

Устройство NIDS, которое находится на общедоступной стороне межсетевого экрана, производит мониторинг атак, анализируя Уровни 4—7 и сравнивая результаты с известными сигнатурами. Поскольку ISP и периферийный маршрутизатор корпоративной сети отфильтровывают некоторые диапазоны адресов и портов, NIDS может сконцентрировать усилия на борьбе с более изощренными атаками. И все же это устройство NIDS работает в менее строгом режиме, чем аналогичные устройства, находящиеся с внутренней стороны межсетевого экрана. Это происходит, потому, что замеченная им несанкционированная активность представляет собой не прорыв обороны, а лишь попытку такого прорыва.

Межсетевой экран контролирует состояние соединения и производит тщательную фильтрацию проходящих через него сессий. Серверы общего доступа получают некоторую защиту от переполнения TCP SYN за счет использования лимитов полуоткрытых соединений на межсетевом экране. Эти экраны не только ограничивают трафик на серверах общего доступа по определенному набору адресов и портов, но и фильтруют трафик, идущий в обратном направлении. Если хакер получил контроль над одним из серверов (обойдя межсетевой экран и системы HIDS и NIDS), такому серверу нельзя позволить стать платформой для дальнейших атак. Для этого используется специальная фильтрация, отбраковывающая любые несанкционированные запросы, которые генерируются серверами общего доступа для передачи в любом направлении. К примеру, web-сервер может фильтроваться таким образом, чтобы не генериро-

вать собственные запросы, а лишь отвечать на запросы клиентов. Это не позволит хакеру после первой удачной атаки загрузить на сервер дополнительные утилиты. Одним из примеров возможной атаки такого типа может служить генерация xterm с web-сервера через межсетевой экран на машину хакера. Кроме того, частные сети VLAN не позволяют серверу общего доступа атаковать другие серверы, находящиеся в одном и том же сегменте. Такой трафик не проходит через межсетевой экран, поэтому использование здесь частных сетей VLAN является критически важным.

В сегменте инспекции содержания передается только трафик, связанный с запросами URL, идущими от межсетевого экрана к устройству, которое осуществляет фильтрацию URL. Кроме этого, разрешаются авторизованные запросы от корпоративного устройства URL-фильтрации к мастер-серверу для обновления информации в базе данных. Устройство URL-фильтрации проверяет исходящий трафик на наличие несанкционированных запросов WWW. Это устройство напрямую связывается с межсетевым экраном и одобряет или отклоняет запросы URL, которые межсетевой экран передает своему механизму URL-инспекции. Решение об одобрении или отклонении запроса зависит от корпоративной политики безопасности, в которой используется классификация ресурсов WWW, предоставляемая третьей стороной. Инспекция URL является более предпочтительной по сравнению с обычной фильтрацией доступа, потому что IP-адреса несанкционированных web-сайтов часто меняются, и поэтому стандартные фильтры могут разрастаться до весьма больших размеров. Установленные на этом сервере средства HIDS предоставляют защиту от атак, которым по какой-либо причине удается обойти межсетевой экран.

Сегмент услуг общего доступа включает устройство NIDS. Оно предназначено для обнаружения атак на те порты, которые межсетевой экран считает разрешенными. Таким образом пресекаются атаки на уровне приложений, направленные против конкретного устройства, или атаки против услуг, защищенных паролями. Это устройство NIDS должно настраиваться на более жесткий режим работы по сравнению с устройством NIDS, установленным с внешней стороны межсетевого экрана, поскольку здесь обнаруживаются атаки, успешно преодолевшие межсетевой экран. На каждом сервере устанавливаются программные средства для обнаружения атак, пресекающие любую несанкционированную активность на уровне операционной системы и на уровне обычных серверных приложений (HTTP, FTP, SMTP и т. д.). Хост DNS должен защищаться и реагировать только на разрешенные команды. Он не должен выдавать никаких ненужных ответов, которые могут облегчить хакерам задачу ведения сетевой разведки. Сюда входит запрещение передачи доменной информации (zone-transfers), кроме случаев, когда такая передача осуществляется внутренним сервером DNS. На сервере SMTP установлены услуги проверки содержания электронной почты, защищающие от вирусов и «троянских коней», которые обычно проникают в систему с почтовыми сообщениями. Межсетевой экран сам проводит фильтрацию сообщений SMTP на Уровне 7 и пропускает на почтовый сервер только необходимые команды.

Устройство NIDS, установленное с внутренней стороны межсетевого экрана, производит окончательный анализ атак. Обнаружение атак на этом этапе должно происходить крайне редко, так как сюда допускаются только ответы на санкционированные запросы и трафик, исходящий с нескольких санкционированных портов сегмента общего доступа. До этого уровня могут доходить только особо изощренные атаки, потому что обычно хакер стремится получить контроль над устройством общего доступа и использовать его в качестве платформы для последующей атаки внутренней сети. К примеру, если хакер захватил сервер SMTP, работающий в сети общего доступа, он может попытаться атаковать внутренний почтовый сервер через TCP-порт 25, которому разрешено передавать почтовые сообщения между хостами. Если атака обнаруживается на этом уровне, реакция должна быть намного более жесткой, чем в других сегментах, поскольку в данном случае какие-то системы уже наверняка находятся под контролем хакера. Следует серьезно рассмотреть вариант использования сброса TCP (TCP reset), который позволит, к примеру, отразить описанную выше атаку SMTP.

Альтернативы

Существует несколько альтернативных вариантов проектирования данного модуля. Так, например, в зависимости от вашего отношения к атакам, вы можете отказаться от установки устройства NIDS с внешней стороны межсетевого экрана. Кроме того, этот тип мониторинга вообще не рекомендуется использовать без базовой фильтрации на маршрутизаторе доступа. Однако при наличии необходимых фильтров доступа, включенных в наш дизайн, внешнее устройство NIDS может дать ценную информацию об атаках, которая в любом другом случае была бы отбракована межсетевым экраном. Поскольку это устройство будет, по всей видимости, генерировать множество сигналов тревоги, эти сигналы должны иметь меньшую приоритетность по сравнению с сигналами, поступающими с внутренней стороны межсетевого экрана. Следует рассмотреть возможность регистрации этих сигналов на отдельной станции управления, чтобы не терять их для последующего анализа. Это важно еще и потому, что множество неудавшихся попыток атаки, регистрируемых внешним устройством NIDS, может дать представление о том, какие типы атак нацелены на вашу организацию. Кроме того, это позволит оценить эффективность фильтров провайдера (ISP) и фильтров, установленных на периферии корпоративной сети.

Еще одна возможная альтернатива предложенному дизайну состоит в удалении маршрутизатора, распо-

ложенного между межсетевым экраном и периферийным распределительным модулем. Его функции вполне могут быть интегрированы в периферийный распределительный модуль, однако при этом будут нивелированы функциональные разграничения между модулями, поскольку для корректной маршрутизации коммутаторам периферийного распределения нужно знать всю топологию корпоративного Интернет-модуля. Кроме того, это ограничит возможности поэтапного модульного внедрения и масштабирования данной архитектуры. К примеру, если базовая сеть предприятия реализована на Уровне 2, вам потребуются функции маршрутизации, которые обеспечивает корпоративный Интернет-модуль.

Модуль виртуальных частных сетей (VPN) и удаленного доступа

Как видно из названия, этот модуль выполняет три основных задачи: терминирует трафик VPN, поступающий от удаленных пользователей, действует в качестве концентратора для терминирования этого трафика, а также терминирует обычных абонентов с модемным доступом. Весь трафик, направляемый в сегмент периферийного распределения, поступает от удаленных корпоративных пользователей, которые так или иначе аутентифицируются и лишь затем получают право прохода через межсетевой экран.

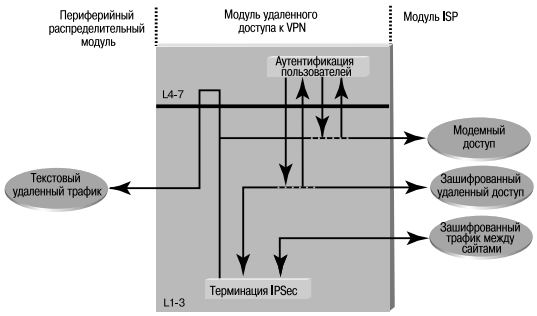


Рисунок 53. Поток трафика через модуль VPN / удаленного доступа

Основные устройства

- *Концентратор VPN* — аутентифицирует удаленных пользователей с помощью средства расширенной аутентификации XAUTH и терминирует их туннели IPSec.
- *Маршрутизатор VPN* — аутентифицирует доверенные удаленные сайты и обеспечивает связь через туннели GRE/IPSec.
- *Сервер модемного доступа* — аутентифицирует индивидуальных удаленных пользователей с помощью TACACS+ и терминирует их аналоговые соединения.
- *Межсетевой экран* — поддерживает свой уровень безопасности для каждого из трех типов удаленного доступа.
- *Устройство NIDS* — поддерживает мониторинг ключевых сетевых сегментов данного модуля на Уровнях 4–7.

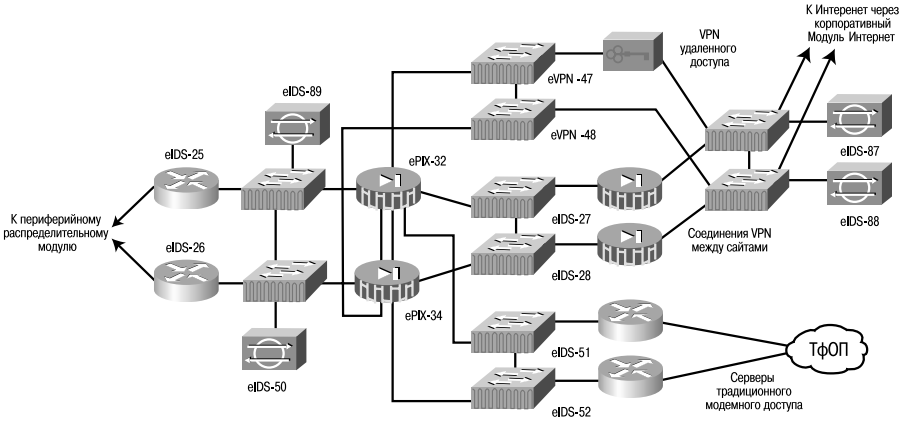


Рисунок 54. Модуль VPN / удаленного доступа

Предотвращаемые угрозы

- *Раскрытие сетевой топологии* — в этот сегмент из Интернет допускаются только данные Internet Key Exchange (IKE) и Encapsulated Security Payload (ESP).
- *Атака на пароли* — аутентификация с использованием однократных паролей (OTP) снижает вероятность успеха такой атаки.
- *Несанкционированный доступ* — услуги межсетевого экрана, следующие за расшифровкой пакетов, не дают возможности передавать трафик на несанкционированные порты.
- *Атака типа Man-in-the-Middle* — вероятность снижается с помощью шифрования удаленного трафика.
- *Снифинг пакетов* — коммутируемая инфраструктура снижает эффективность снифинга.

Рекомендации по дизайну

Кроме надежности, базовыми требованиями к этому модулю являются аутентификация и терминация трех типов услуг для внешних пользователей. Поскольку трафик в корпоративную сеть поступает из разных внешних источников, было принято решение о поддержке отдельного интерфейса для каждой из трех услуг. Ниже приводятся рекомендации по проектированию этих услуг.

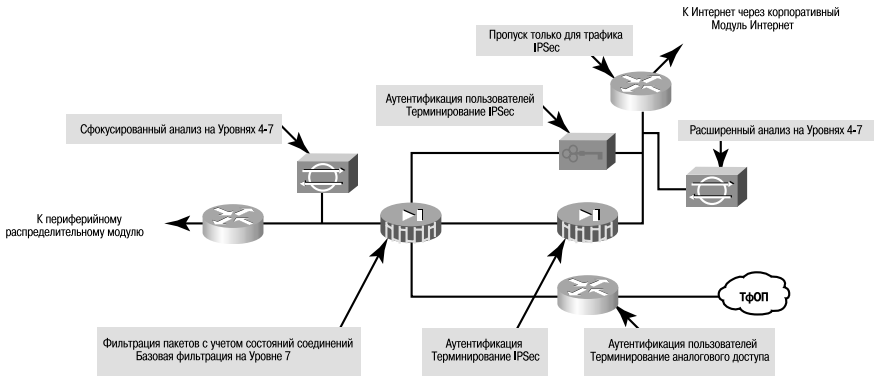


Рисунок 55. Борьба с угрозами на уровне модуля VPN / удаленного доступа

VPN удаленного доступа

Трафик VPN передается с маршрутизаторов доступа, являющихся частью корпоративного Интернет-модуля. На выходе этих маршрутизаторов трафик фильтруется по IP-адресам и протоколам, входящим в состав услуг VPN. Современные виртуальные частные сети с удаленным доступом могут пользоваться несколькими протоколами туннелирования и безопасности. Хотя наиболее оптимальным является протокол IPSec, многие организации выбирают такие протоколы, как PPTP или L2TP, которые изначально поддерживаются наиболее популярными операционными системами для настольных устройств. В архитектуре SAFE используется протокол IPSec, потому, что с одной стороны, он требует минимальных усилий по конфигурированию клиентов, а с другой стороны, поддерживает достаточно высокий уровень безопасности.

Трафик VPN с удаленным доступом будет направляться на единый адрес общего доступа с помощью протокола IKE (UDP 500). Поскольку соединение IKE не может производиться без корректной аутентификации, на этом уровне потенциальный хакер должен испытывать определенные трудности. Технология XAUTH, которая является одним из расширений IKE (draft RFC), создает дополнительный механизм аутентификации пользователя, прежде чем этому пользователю будут присвоены какие-либо параметры IP. Концентратор VPN «подключается» к серверу контроля доступа через подсеть управления и интерфейс управления. При этом надежную защиту с помощью паролей предоставляет сервер однократных паролей.

После аутентификации удаленный пользователь получает доступ. Для этого ему присваиваются IP-параметры с помощью MODCFG, еще одного расширения IKE. Кроме IP-адреса и местонахождения серверов имен (DNS и WINS), MODCFG предоставляет услуги аутентификации для контроля доступа данного удаленного пользователя. К примеру, в архитектуре SAFE абоненты не могут работать в туннеле и одновременно иметь прямой доступ в сеть Интернет. Вместо этого им приходится получать доступ в Интернет только через корпоративные каналы. При этом используются такие параметры IPSec, как 3DES (для шифрования) и SHA-HMAC (для контроля целостности данных). Модуль аппаратного шифрования, который входит в состав концентратора VPN, позволяет масштабировать услуги удаленного доступа VPN и предлагать их тысячам удаленных пользователей. После терминации туннеля VPN трафик передается через межсетевой экран, где происходит необходимая фильтрация пользователей VPN.

Безопасное управление этой услугой достигается с помощью навязывания удаленным пользователям всех параметров IPSec и параметров безопасности с центрального сайта. Кроме того, подключение ко всем функциям управления происходит через специальный выделенный интерфейс.

Пользователи с модемным доступом

Традиционные пользователи с модемным доступом терминируются на одном из двух маршрутизаторов доступа, где имеются встроенные модемы. После установления связи между пользователем и сервером на Уровне 1 для аутентификации пользователя применяется протокол CHAP. Как и в случае с VPN удаленного доступа, для аутентификации и предоставления паролей используются сервер AAA и сервер однократных паролей. После аутентификации пользователей им присваиваются IP-адреса, которые выбираются из IP-пула при установлении соединения протокола PPP.

VPN для связи между сайтами

Трафик VPN, предназначенный для связи между сайтами, состоит из туннелей GRE, защищенных протоколом IPSec в транспортном режиме с использованием технологии ESP (Encapsulated Security Payload). Как и в случае с удаленным доступом, трафик, исходящий из корпоративного модуля Интернет, может поступать только на определенные адреса двух маршрутизаторов VPN. При этом адреса источников ограничиваются ожидаемыми адресами удаленных сайтов. Единственными ожидаемыми протоколами в этом канале являются протокол ESP (IP 50) и протокол IKE (UDP 500).

Протокол GRE используется для обеспечения полнофункционального маршрутизируемого канала, по которому передается многопротокольный трафик. Здесь же поддерживаются протоколы маршрутизации и режим многоадресной передачи (multicast). Поскольку протоколы маршрутизации могут распознавать обрыв связи в канале (для связи с удаленными сайтами используется протокол EIGRP — Enhanced Interior Gateway Routing Protocol), туннель GRE создает механизм устойчивости для удаленных сайтов, которые имеют два канала с инкапсуляцией GRE (по одному на каждый центральный маршрутизатор VPN).

Как и в случае с VPN удаленного доступа, максимальная безопасность с приемлемым ущербом для производительности достигается с помощью алгоритмов шифрования и контроля целостности 3DES и SHA-HMAC. На маршрутизаторах VPN могут использоваться аппаратные акселераторы IPSec.

Остальные компоненты модуля

Межсетевой экран агрегирует трафик всех трех типов и направляет его на внутренний интерфейс, а затем — через пару маршрутизаторов — в периферийный распределительный модуль. На маршрутизаторе должен быть правильно настроен контроль доступа, чтобы пропускать к внутреннему интерфейсу экрана только санкционированный трафик. С внешней стороны межсетевого экрана устанавливается пара устройств NIDS для обнаружения любой «разведывательной» деятельности, направленной против устройств терминации VPN. В этом сегменте может передаваться только трафик IPSec (IKE/ESP). Поскольку системы NIDS не могут анализировать содержание пакетов IPSec, любой генерируемый ими сигнал тревоги может означать только отказ или захват хакером одного из окружающих устройств. В любом случае все подобные сигналы должны иметь высокий уровень приоритетности. Вторая пара устройств NIDS устанавливается с внутренней стороны межсетевого экрана для обнаружения любых атак, которым удалось обойти все предыдущие преграды. Эти устройства также должны устанавливаться на весьма жесткий режим работы. Весь трафик, проходящий через этот сегмент, должен передаваться на удаленный сайт или поступать с удаленного сайта, и поэтому любые операции типа «отрубания» адресов (shunning) или переустановки TCP (TCP reset) будут влиять только на удаленных пользователей.

Альтернативы

В технологиях VPN и аутентификации существует множество альтернатив, применение которых зависит от специфических требований конкретной сети. Ниже приводится список этих альтернатив, однако их детальное описание выходит за рамки данного документа.

- Аутентификация с помощью смарт-карт и/или биометрических устройств.
- Туннели L2TP и/или PPTP для удаленного доступа к VPN.
- Certificate Authorities (CA).
- Механизм устойчивости IKE (IKE keep-alive resilience mechanism).
- VPN с многопротокольной коммутацией по меткам (MPLS).

Модуль территориальных сетей (WAN)

Этот модуль предназначается для поддержки устойчивости и безопасности терминации соединений с территориальными сетями. При этом трафик передается между удаленными сайтами и центральным сайтом по сети Frame Relay.

Основные устройства

- *Маршрутизатор IOS* — использует механизмы маршрутизации, контроля доступа и гарантированного качества услуг (QoS).

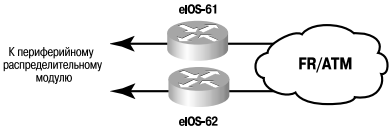


Рисунок 56. Модуль территориальных сетей

Предотвращаемые угрозы

- *IP-спуфинг* — борьба ведется с помощью фильтрации на Уровне 3.
- *Несанкционированный доступ* — простой контроль доступа на маршрутизаторе может ограничить типы протоколов, к которым имеют доступ отделения компании.

Рекомендации по дизайну

Устойчивость обеспечивается двойным соединением, идущим от сервис-провайдера через маршрутизаторы к периферийному распределительному модулю. Безопасность поддерживается с помощью функций IOS. Для блокирования всего нежелательного трафика, поступающего от отделений компании, используются списки доступа на входе.

Рисунок 57. Борьба с угрозами на уровне модуля территориальных сетей

Альтернативы

Некоторые организации, особо озабоченные защитой информации, шифруют конфиденциальный трафик, передаваемый по каналам глобальных сетей. Как и в случае с виртуальными частными сетями, для связи между сайтами поддержка такой политики безопасности может обеспечиваться с помощью протокола IPSec.

Модуль электронной коммерции

Поскольку главной заботой данного модуля является электронная коммерция, здесь необходимо найти оптимальное соотношение между удобством доступа и безопасностью. Разделение транзакции электронной коммерции на три компонента позволяет нашей архитектуре поддерживать разные уровни безопасности без ущерба для удобства доступа.

Основные устройства

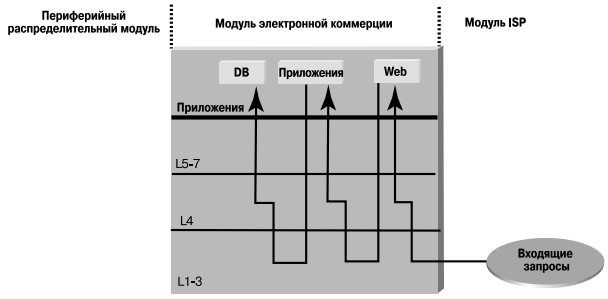


Рисунок 58. Поток трафика электронной коммерции

- *Web-сервер* — служит основным пользовательским интерфейсом для навигации по магазину электронной коммерции.
- *Сервер приложений* — является платформой для различных приложений, которые требуются web-серверу.
- *Сервер баз данных* — содержит критически важную информацию, которая служит основой для электронной коммерции.
- *Меж сетевой экран* — управляет уровнями безопасности и доступа в системе.
- *Устройство NIDS* — поддерживает мониторинг ключевых сетевых сегментов в модуле.
- *Коммутатор Уровня 3 с модулем ISP* — масштабируемое устройство ввода для электронной коммерции с интегрированными средствами мониторинга безопасности.

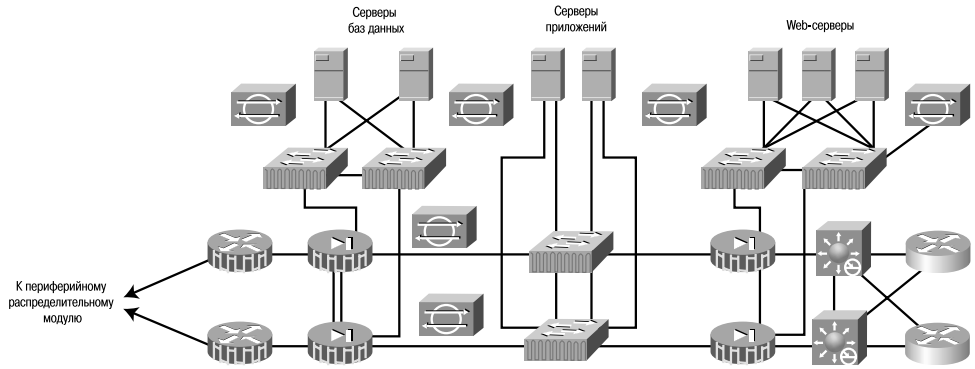


Рисунок 59. Модуль электронной коммерции

Предотвращаемые угрозы

- *Несанкционированный доступ* — межсетевой экран и списки доступа (ACL) снижают уязвимость протоколов.
- *Атаки на уровне приложений* — борьба ведется с помощью систем обнаружения атак (IDS).
- *Отказ в обслуживании (DoS)* — фильтрация на устройствах провайдера (ISP) и ограничение объемов снижают остроту атак типа (D)DoS.
- *IP-спуфинг* — фильтрация в соответствии с RFC 2827 и 1918 ограничивает возможности удаленного спуфинга.

Рисунок 60. Борьба с атаками на уровне модуля электронной коммерции

- *Сниффинг пакетов* — коммутируемая инфраструктура и системы HIDS ограничивают эффективность сниффинга.
- *Сетевая разведка* — работать можно только с ограниченным числом необходимых портов; возможности ICMP ограничены.
- *Злоупотребление доверием* — межсетевые экраны обеспечивают поток трафика только в правильном направлении и для правильных услуг.
- *Переадресация портов* — HIDS и фильтрация с помощью межсетевого экрана ограничивают эффективность этих атак.

Описание внедрения

В основе модуля лежат две пары отказоустойчивых межсетевых экранов, которые защищают три вида серверов: web-серверы, серверы приложений и серверы баз данных. Дополнительная защита обеспечивается периферийными маршрутизаторами провайдерской (ISP) и корпоративной сети. Этот дизайн легко понять, если рассмотреть поток трафика и направление типовой электронной коммерческой транзакции.

Заказчик, входящий в систему электронной коммерции, инициирует соединение HTTP с web-сервером после получения IP-адреса с сервера DNS, находящегося в сети ISP. Сервер DNS находится в другой сети, чтобы сократить число протоколов, необходимых для приложения электронной коммерции. Первая группа межсетевых экранов должна пропускать этот протокол по конкретному адресу. Ответный трафик по этому же каналу также пропускается через экран, но для этого web-серверу не нужно снова инициировать соединение для выхода в Интернет. Межсетевой экран блокирует этот маршрут, чтобы ограничить возможности хакеров, если они завладели одним из web-серверов.

Когда пользователь просматривает web-сайт и выбирает переход по гиперссылке, web-сервер инициирует запросы к серверу приложений, который находится с внутренней стороны межсетевого экрана. Это соединение вместе с ответным трафиком также должно разрешаться первым межсетевым экраном. Как и в случае с web-сервером, серверу приложений не нужно инициировать соединение с web-сервером или выход в Интернет. Вся пользовательская сессия проходит поверх HTTP и SSL без прямой связи с сервером приложений или сервером баз данных.

В какой-то момент пользователь захочет совершить транзакцию. web-сервер захочет защитить эту транзакцию, и ему понадобится протокол SSL. В то же время сервер приложений может сделать запрос или передать информацию серверу баз данных. Как правило, это происходит в форме запросов SQL, которые инициируются сервером приложений для сервера баз данных, но не наоборот. Эти запросы проходят через второй межсетевой экран и передаются на сервер баз данных. В зависимости от специфики используемого приложения, серверу баз данных может потребоваться связь с внутренними системами (back-end), которые находятся в корпоративном серверном модуле.

В общем и целом, межсетевые экраны должны разрешать передачу трафика только по трем маршрутам, каждый из которых работает со своим протоколом, и блокировать все остальные попытки связи, если они не представляет собой передачу пакетов в ответ на запросы, поступившие по трем первоначальным маршрутам.

Сами серверы также должны быть полностью защищены. Особое внимание следует уделять защите web-сервера, предназначенного для общего доступа. Необходимо пользоваться самыми последними версиями операционной системы и приложений web-сервера со всеми коррекционными модулями (патчами). Кроме того, эти средства должны находиться под постоянным наблюдением со стороны средств обнаружения атак (HIDS). Эти меры позволят снизить эффективность большинства первичных и вторичных атак, включая переадресацию портов и атаки типа root kit. Все другие серверы также должны иметь аналогичные средства защиты на случай, если хакеры захватят первый сервер или межсетевой экран.

Сегменты, защищенные межсетевым экраном

Межсетевые экраны для электронной коммерции обычно защищаются периферийным маршрутизатором заказчика, установленным у ISP. В точке выхода этого маршрутизатора, направленной к корпорации, ISP может до предела ограничить количество протоколов, необходимых для электронной коммерции, а также разрешить передачу трафика только на адрес web-серверов. Кроме того, периферийным серверам необходимо обновление протокола маршрутизации (обычно это BGP — Border Gateway Protocol). Весь остальной трафик должен блокироваться. Для борьбы с атаками типа (D)DoS провайдер (ISP) должен ограничивать объемы трафика, как указано в разделе «Аксиомы SAFE». ISP должен также проводить фильтрацию по стандартам RFC 1918 и RFC 2827.

В помещении предприятия первый маршрутизатор служит только в качестве интерфейса для связи с провайдером (ISP). Всю сетевую работу выполняет коммутатор Уровня 3, функции которого выполняются на аппаратных процессорах. Именно коммутаторы Уровня 3 принимают все решения по маршрутизации BGP, определяя, маршрут какого провайдера (ISP) наиболее оптимален для того или иного пользователя. Во-вторых, коммутаторы Уровня 3 выполняют функцию проверки фильтрации, обеспечивая ее соответствие описанной выше фильтрации ISP, что повышает уровень безопасности. В-третьих, коммута-

торы Уровня 3 имеют встроенную функцию мониторинга для распознавания атак (IDS). Если емкость соединения с Интернет превышает возможности линейной карты IDS, вы можете проверять только входящие web-запросы, поступающие на карту IDS из сети Интернет. Хотя в этом случае вы будете терять до 10 % аварийных сигналов, это все-таки лучше, чем проверять трафик, передаваемый в обоих направлениях, потому что при этом число пропускаемых аварийных сигналов будет больше. Другие средства NIDS, находящиеся с внутренней стороны межсетевого экрана, проверяют сегменты, пытаясь распознать атаки, успешно преодолевшие первую линию обороны. Так, например, если версия web-сервера устарела, хакер, преодолевший систему HIDS, может захватить его с помощью атаки на уровне приложений. Как и в корпоративном Интернет-модуле, нужно попытаться свести к минимуму число ложных срабатываний систем распознавания атак, чтобы каждый сигнал тревоги вызывал должное внимание. Поскольку в определенных сегментах может присутствовать только определенный трафик, вы можете очень точно настроить свою сетевую систему обнаружения атак (NIDS).

С точки зрения приложений, маршруты связи между разными уровнями (web, приложения, базы данных) должны быть защищенными, транзакционными и обладать надежной системой аутентификации. К примеру, если сервер приложений получает данные от сервера баз данных через интерактивную сессию (SSH, FTP, Telnet и т. д.), хакер может воспользоваться интерактивностью для проведения атаки на уровне приложений. Использование надежных каналов связи поможет снизить потенциальный риск.

Коммутаторы Уровня 2, поддерживающие разные сегменты, защищенные межсетевыми экранами, создают возможность использования частных сетей VLAN, создавая модель доверия, которая пропускает трафик, отвечающий определенным требованиям в рамках определенного сегмента, и отбраковывает весь остальной трафик. К примеру, нет никаких причин для того, чтобы позволять одному web-серверу связываться с другим web-сервером.

Управление всем модулем (как и всеми другими элементами данной архитектуры) происходит только по отдельной сети (out-of-band).

Альтернативы

Основной альтернативой данной архитектуре является размещение всей систему у провайдера (ISP). При этом (хотя общий дизайн системы не меняется) появляются два существенных различия. Во-первых, связь с ISP осуществляется по каналу LAN с более широкой полосой пропускания. Это, в принципе, позволяет избавиться от пограничных маршрутизаторов, хотя такой вариант использовать не рекомендуется. Кроме того, более широкая полоса пропускания выдвигает новые требования в области борьбы с атаками типа (D)DoS. Во-вторых, обратное соединение с корпорацией должно по-другому управляться. Альтернативы включают шифрование и использование частных линий связи. Эти технологии выдвигают дополнительные требования к системе безопасности в зависимости от местонахождения каналов связи и их использования.

Существует несколько вариантов проектирования этого модуля. Мы лишь перечислим эти альтернативы. Их подробное освещение выходит за рамки данного документа.

- В качестве альтернативы можно использовать дополнительные межсетевые экраны. В этом случае поток трафика будет выглядеть следующим образом: периферийный маршрутизатор — межсетевой экран — web-сервер — межсетевой экран — сервер приложений — межсетевой экран — сервер баз данных. В результате каждый межсетевой экран будет контролировать связь только с одной базовой системой.
- Технологии балансировки нагрузки и кэширования не рассматриваются в настоящем документе, однако они могут накладываться на данную архитектуру без особых модификаций. В будущем этот вопрос будет рассмотрен в отдельном документе.
- Для среды с очень высокими требованиями к безопасности можно рассмотреть возможность использования межсетевых экранов разных типов. Сразу заметим, что это создает дополнительные проблемы в области управления, так как требует дублирования политики безопасности на разнородных системах. Этот вариант реализуется для того, чтобы прорыв одного межсетевого экрана не становился прорывом всей системы безопасности. Этот тип дизайна сфокусирован на межсетевых экранах. Он в недостаточной степени использует преимущества систем обнаружения атак (IDS) и других технологий безопасности, которые позволяют снизить риск прорыва одного межсетевого экрана.

Варианты проектирования

Процесс проектирования часто связан с компромиссами. В этом кратком разделе мы рассмотрим некоторые варианты, к которым может прибегнуть инженер, который проектирует сеть в условиях нехватки средств. Одни компромиссы возможны на уровне модулей, другие — на уровне компонентов.

Первая возможность состоит в свертывании модуля распределения и его слиянии с базовым модулем. В результате наполовину сокращается количество коммутаторов Уровня 3. Экономия средств достигается за счет некоторого сокращения производительности базовой сети и снижения гибкости, необходимой для фильтрации на уровне распределения.

Второй вариант состоит в слиянии функциональности модуля VPN / удаленного доступа и корпоративного модуля Интернет. Структуры этих модулей очень сходны: пара межсетевых экранов в центре плюс устройства NIDS. Такое слияние не приводит к потере функциональности, если производительность компонентов соответствует общему объему трафика, который должны передавать оба модуля, и если межсетевой экран имеет достаточное количество интерфейсов для поддержки необходимых услуг. При этом следует помнить, что по мере концентрации функций на единых устройствах увеличивается вероятность человеческих ошибок. Некоторые организации идут еще дальше и включают в корпоративный модуль VPN/Интернет функции электронной коммерции. Авторы считают, что при этом варианте риск намного перевешивает любую экономию, кроме случаев, когда потребности электронной торговли являются минимальными. Отделение трафика электронной коммерции от общего Интернет-трафика позволяет лучше оптимизировать полосу пропускания за счет более строгой фильтрации и ограничений атак типа (D)DoS на уровне ISP.

Третий возможный вариант состоит в удалении некоторых устройств NIDS. В зависимости от стратегии реагирования на угрозы вам действительно может понадобиться меньше таких устройств. Кроме того, их количество зависит от числа установленных устройств HIDS, поскольку в некоторых случаях последние могут снизить потребность в обнаружении атак на сетевом уровне (NIDS). Этот вопрос обсуждается (там, где необходимо) в разделах, посвященных конкретным модулям.

Совершенно ясно, что проектирование сетей не относится к числу точных наук. Проектировщик всегда может сделать тот или иной выбор в зависимости от реальных потребностей. Авторы не требуют обязательного принятия своей архитектуры в неизменном виде. Они просто хотят, чтобы инженеры, проектирующие сеть, сознательно выбирали варианты систем безопасности на основе опыта, полученного их предшественниками в ходе предыдущей работы.

Дизайн малой сети

Дизайн малой сети имеет два модуля: корпоративный модуль Интернет и модуль кампуса. Первый модуль имеет подключения к Интернет, на него замыкаются VPN и трафик открытых сервисов (DNS, HTTP, FTP, SMTP). Ко второму модулю относятся коммутация Уровня 2, все пользователи, а также управление и серверы внутренней сети. Обсуждение этого дизайна большей частью ведется на основе малой сети как главной сети предприятия; также говорится о специфических изменениях дизайна при конфигурации для филиала.

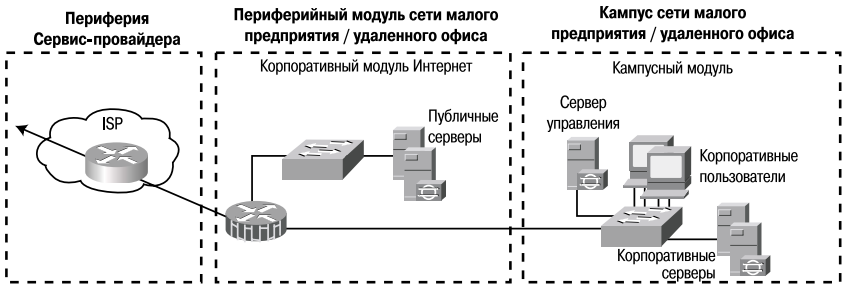


Рисунок 61. Модель сети малого предприятия

Корпоративный модуль Интернет

Корпоративный модуль Интернет обеспечивает внутренним пользователям подключение к Интернет и доступ к сервисам всемирной Сети, внешним пользователям — доступ к информации на общедоступных серверах, а для удаленных работников этот же модуль предоставляет доступ с использованием ВЧС (VPN). Однако, модуль не предназначен для поддержки приложений электронной коммерции.

Основные устройства

- Сервер SMTP — передаточное звено между Интернет и внутрисетевыми почтовыми серверами.
- Сервер DNS — служит внешним сервером DNS для предприятия; передает внутренние запросы в Интернет.
- Сервер FTP/HTTP — предлагает общедоступную информацию о предприятии
- Межсетевой экран или межсетевой маршрутизатор — обеспечивают защиту ресурсов на сетевом уровне, динамическое фильтрование трафика, поддержку подключений ВЧС для удаленных сайтов и пользователей.

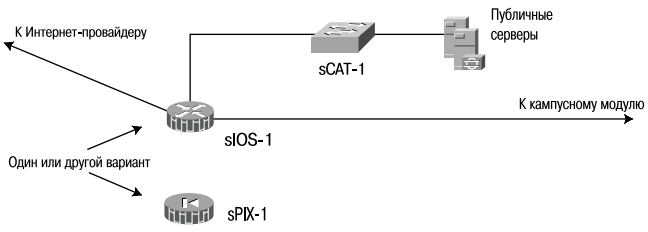


Рисунок 62. Детальный дизайн модуля модуль Интернет

- Коммутатор Уровня 2 (с функциями поддержки частных виртуальных локальных сетей) — арантирует передачу данных от управляемых устройств непосредственно на межсетевой экран IOS.

Предотвращаемые угрозы

Чаще всего объектами атаки становятся общедоступные серверы. Это предполагает следующие угрозы:

- Неавторизованный доступ-нейтрализуется фильтрованием на межсетевых экранах.
- Атаки уровня приложений — нейтрализуются сетевой IDS на открытых серверах.
- Вирусы и «троянские» программы − нейтрализуются антивирусной проверкой на уровне хоста.
- Парольные атаки — нейтрализуются сокращением сервисов, уязвимых для лобовой атаки; обнаружить такую угрозу позволяют ОС и система IDS.
- Отказ в обслуживании — нейтрализуется заданием скорости доступа (Committed access rate — CAR) на соединеняхс оператором связи и настройкой контроля соединений TCP на межсетевом экране.
- Подмена (спуфинг) адресов IP — ограничивается фильтрованием согласно RFC 2827 и RFC 1918 на выходе провайдера услуг и на локальном межсетевом экране.
- Прослушивание пакетов — ограничивается коммутируемой инфраструктурой и хостовой системой обнаружения вторжений.
- Изучение сети — хостовая система обнаружения вторжений обнаруживает попытки изучения сети; ограничивается фильтрованием протоколов.
- Злоупотребление доверием — ограничить атаки, основанные на доверии, позволяют запретительная модель доверия и частные виртуальные локальные сети.
- Перенаправление портов — ограничить эти атаки позволяет запретительное фильтрование и хостовая система обнаружения вторжений.

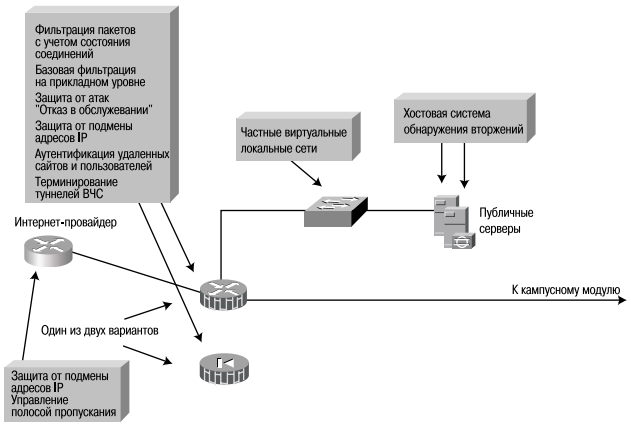


Рисунок 63. Отражение угроз в модуле Интернет

Рекомендации по дизайну

Здесь представлен законченный детализированный дизайн защиты сети, в котором все сервисы защиты и виртуальных частных сетей (ВЧС) сведены в единый блок. При практическом внедрении возникают два пути реализации этой функциональности. Первый: использовать маршрутизатор с межсетевым экраном и возможности ВЧС. Это дает малой сети наибольшую гибкость, так как маршрутизатор поддерживает все расширенные сервисы (QoS, маршрутизация, многопротокольность), необходимые современной сети. Второй путь: использовать вместо маршрутизатора выделенный межсетевой экран. На эту реализацию накладываются некоторые ограничения: во-первых, межсетевые экраны в основном рассчитаны только на Ethernet, а для поддержки ими протоколов WAN требуются некоторые изменения. В современных условиях большинство кабельных и DSL (digital-subscriber-line) модемов и маршрутизаторов предлагаются сервис-провайдерами и могут использоваться для подключения к межсетевому экрану по Ethernet. Если от устройства требуются интерфейсы подключения к территориальным сетям, то в обязательном порядке используются маршрутизаторы. Применение выделенного межсетевого экрана упрощает конфигурирование сервисов защиты и повышает эффективность функций самого экрана. С любым выбранным устройством применяется динамическая проверка трафика всех направлений — это гарантирует, что через межсетевой экран проходит только разрешенный трафик. В идеале трафик, поступающий на межсетевой экран, должен предварительно фильтроваться у Интернет-провайдера. Помните, что маршрутизаторы настроены пересылать разрешенный трафик, а межсетевые экраны трафик по умолчанию запрещают.

Начиная с выхода оконечного маршрутизатора в сети Интернет-провайдера малозначительный трафик ограничивается некоторым пределом по занимаемой полосе пропускания с целью нейтрализовать атаки типа «отказ в обслуживании». Плюс к этому фильтрование по RFC 1918 и RFC 2827 на выходе маршрутизатора Интернет-провайдера нейтрализует подделку исходных адресов локальных сетей и частных адресных пространств.

Фильтрование RFC 1918 и RFC 2827 на входе межсетевого экрана в первую очередь выполняется для проверки фильтрования Интернет-провайдера. По причине особой угрозы, создаваемой фрагментированными пакетами, большинство межсетевых экранов настроены на сброс большинства фрагментированных пакетов, которые, как правило, невидимы в стандартных типах Интернет-трафика. То, что из-за такого фильтрования будет теряться некоторый разрешенный трафик, считается более приемлемым, чем риск пропустить подобный трафик в сеть. Поступающий извне трафик, предназначенный самому межсетевому экрану, ограничивается протоколом IPSec и протоколами, необходимыми для маршрутизации.

Межсетевой экран выполняет принудительное и динамическое фильтрование сессий, инициированных через него. Общедоступные серверы защищаются от «затоплений» TCP SYN при помощи ограничений ти-

па контроля «наполовину открытых сессий» на межсетевом экране. С точки зрения фильтрования, в дополнение к ограничению трафика публичных сервисов адресов и портов имеет место фильтрование трафика в обратном направлении. Если в ходе атаки один из общедоступных серверов оказывается скомпрометированным, нельзя оставлять возможность использовать его для продолжения атаки на сеть. Для нейтрализации этого типа атак специальное фильтрование отсекает все неавторизованные запросы, генерируемые сервером и адресуемые куда бы то ни было. Например, необходимо фильтровать web-сервер, чтобы он не генерировал запросы самому себе, но в то же время, чтобы он отвечал на запросы пользователей. Такая настройка не позволяет хакеру после первичной атаки загрузить на сервер собственные утилиты, а также позволяет остановить сессии, которые хакер переключил в ходе первичной атаки. Атака, которая генерирует приложение xterm от web-сервера к компьютеру хакера, является примером подобной первичной атаки. Плюс к этому частные виртуальные локальные сети коммутатора демилитаризованной зоны (DMZ) не позволяют атаковать со взломанного сервера другие серверы в том же сегменте. Межсетевые экраны не всегда могут отследить такой трафик, и этим объясняется важность использования частных виртуальных локальных сетей (PVLAN).

С точки зрения хостов, каждый сервер, предлагающий общедоступные сервисы, должен иметь систему обнаружения вторжений для отслеживания подозрительной активности на уровне операционной системы, а также работу обычных серверных приложений (HTTP, FTP, SMTP и проч.).

DNS-хост должен быть доступен только для разрешенных команд и отсекать излишние запросы, с помощью которых хакер может изучать сеть. Сюда же относятся обмены зонной информацией, откуда бы ни было, кроме вторичных DNS-серверов. Работая с почтовыми сервисами, межсетевой экран фильтрует SMTP-сообщения по Уровню 7, пропуская на почтовый сервер только необходимые команды.

Межсетевые экраны и маршрутизаторы с возможностями межсетевых экранов в числе прочих защитных функций частично обладают функциональностью сетевых систем обнаружения вторжений. Использование этой функциональности сказывается на производительности устройства, но вместе с этим позволяет лучше наблюдать ведущуюся атаку.

Помните, что вы жертвуете производительностью в пользу лучшего наблюдения за атакой. Многие из атак можно отразить и без участия систем обнаружения вторжений, но в некоторых случаях такая возможность окажется далеко не лишней. ВЧС подключаются через межсетевые экраны и/или маршрутизаторы. Удаленные сайты аутентифицируют друг друга по предварительно распределенным ключам, а пользователи аутентифицируются сервером контроля доступа, который встроен в кампусный модуль.

Альтернативы

Улучшения этого дизайна могут быть направлены на повышение возможностей сети или на разнесение защитных функций на отдельные устройства. В ходе этих улучшений дизайн малой сети все более и более походит на дизайн сети среднего размера, который обсуждается в этом же документе ниже. Первым шагом при этом должна стать не общая адаптация дизайна, а введение в структуру выделенного концентратора удаленного доступа по VPN, чтобы повысить управляемость сообществом удаленных пользователей.

Кампусный модуль

В кампусный модуль входят рабочие станции конечных пользователей, корпоративные Интернет-серверы, серверы управления и соответствующая инфраструктура Уровня 2, необходимая для поддержки устройств. В случае дизайна малой сети функциональность Уровня 2 входит в состав единого коммутатора.

Основные устройства

- *Коммутация Уровня 2 (с поддержкой виртуальных локальных сетей)* — обеспечивает сервисы Уровня 2 для рабочих станций пользователей.
- *Корпоративные серверы* — обеспечивают сервисы электронной почты (SMTP и POP3) для внутренних пользователей, а также доставку файлов, печать и услуги DNS для рабочих станций.
- *Рабочие станции пользователей* — обеспечивают услуги работы с данными для авторизованных пользователей сети.
- *Хост управления* — поддерживает системы обнаружения вторжений, syslog, TACACS+/RADIUS и общее управление конфигурацией.

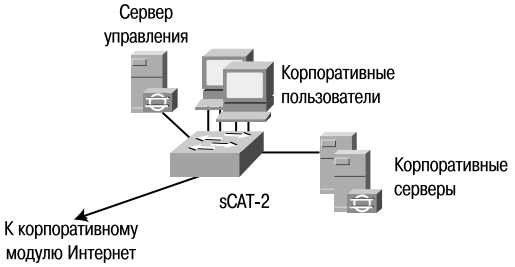


Рисунок 64. Дизайн кампусного модуля малого предприятия

Предотвращаемые угрозы

- *Прослушивание пакетов* — эффективность прослушивания органичивает коммутируемая инфраструктура.
- *Вирусы и «троянские» приложения* — антивирусная проверка на хосте предотвращает большинство вирусов и многие «троянские» программы.

- *Неавторизованный доступ* — такой доступ нейтрализуется хостовой системой обнаружения вторжений и приложениями контроля доступа.
- *Атаки уровня приложений* — операционные системы, устройства и приложения должны использовать все предлагаемые обновления и программные «заплатки», а также должны быть защищены хостовой системой обнаружения вторжений.
- *Злоупотребление доверием* — частные виртуальные локальные сети запрещают излишнее взаимодействие хостов внутри подсети.

Рисунок 65. Отражение атак в кампусном модуле

- *Переадресация портов* — серверная система обнаружения вторжений запрещает инсталляцию агентов переадресации портов.

Рекомендации по дизайну

Главными функциями кампусного коммутатора являются коммутация рабочего и управляющего трафика, а также обеспечение связи для корпоративных и управляющих серверов и пользователей. На коммутаторе могут использоваться частные виртуальные локальные сети — это позволяет нейтрализовать атаку типа «злоупотребление доверием» между устройствами. Например, корпоративным пользователям бывает нужно обратиться к корпоративному серверу, но не требуется общаться между собой. Поскольку кампусный коммутатор не содержит сервисов Уровня 3, то надо помнить, что при подобном дизайне возрастает значение защиты приложений и хостов по причине открытости внутренней сети. Поэтому на важнейшие системы кампуса (в том числе на корпоративные серверы и на системы управления) устанавливаются сетевые системы обнаружения вторжений.

Альтернативы

Повысить общую защищенность позволяет установка небольшого фильтрующего маршрутизатора или межсетевого экрана между управляющей станцией и остальной сетью. Это разрешит передачу управляющего трафика только в направлении, заданном администратором. При высоком уровне взаимного доверия внутри сети можно обойтись и без сетевой системы обнаружения вторжений, хотя это не рекомендуется.

Независимые и филиальные реализации

Для филиальной реализации не требуется функциональность ВЧС удаленного доступа, поскольку она обычно предоставляется штаб-квартирой. В дальнейшем управляющие хосты, как правило, будут размещаться в центре, и потребуется возможность обратного отслеживания управляющего трафика по подключению ВЧС к штаб-квартире.

Дизайн сети среднего размера

Дизайн SAFE средней сети состоит из трех модулей: корпоративного модуля Интернет, кампусного модуля и модуля территориальных сетей. Как и в случае дизайна малой сети, корпоративный модуль Интернет имеет подключение к Интернет и поддерживает со своей стороны ВЧС и трафик общедоступных сервисов (DNS, HTTP, FTP и SMTP). На этот же модуль выведен трафик входящего дозвона. К кампусному модулю относится инфраструктура коммутации Уровня 2 и Уровня 3, а также корпоративные пользователи, управляющие серверы и интранет-серверы. С точки зрения территориальных сетей, в рамках этого дизайна существуют два способа подключения удаленных сайтов. Первый способ — это подключение по частным каналам, а второй — IPSec ВЧС внутри корпоративного Интернет-модуля. Основные вопросы, связанные с этим дизайном, относятся к работе сети головного офиса корпорации, а также к специфическим изменениям в случае использования в качестве сети филиала.

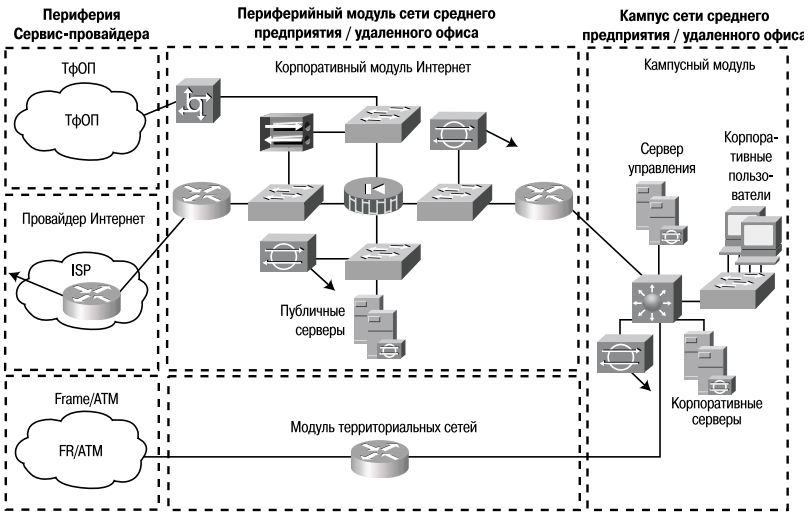


Рисунок 66. Дизайн сети среднего предприятия

Корпоративный модуль Интернет

Задача корпоративного модуля Интернет — предоставить внутренним пользователям доступ к услугам Интернет, а пользователям внешним обеспечить доступ к информации на общедоступных серверах (HTTP, FTP, SMTP и DNS). Кроме этого, модуль поддерживает трафик ВЧС от удаленных серверов и пользователей, а также трафик обычных пользователей, подключающихся при помощи дозвона. Корпоративный модуль Интернет не предназначен для поддержки приложений электронной коммерции.

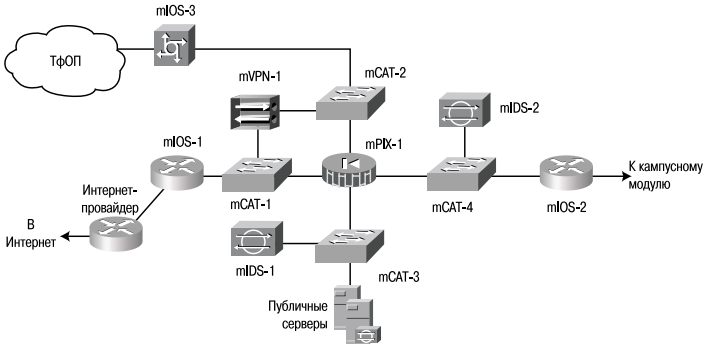


Рисунок 67. Дизайн модуля Интернет

Основные устройства

- *Сервер дозвона (удаленного доступа)* — аутентифицирует отдельных пользователей и поддерживает их аналоговые подключения.
- Сервер DNS — служит авторизованным внешним сервером DNS для средней сети; передает внутренние запросы в Интернет.
- *Сервер FTP/http* — предоставляет открытую информацию предприятия.
- *Межсетевой экран* — обеспечивает защиту ресурсов на сетевом уровне и динамическое фильтрование трафика; поддерживает дифференцированную защиту удаленных пользователей; проводит аутентификацию удаленных сайтов и поддерживает подключения по туннелям IPSec.
- *Коммутатор Уровня 2 (с поддержкой частных виртуальных локальных сетей)* — обеспечивает подключение устройств по Уровню 2.
- *Применение сетевых систем обнаружения вторжений* — обеспечивает наблюдение по Уровням 4 — 7 за важнейшими сегментами сети.
- *Сервер SMTP* — выполняет промежуточную роль между внутренними почтовыми серверами и Интернет; контролирует пересылаемое содержание.
- Концентратор ВЧС — аутентифицирует отдельных удаленных пользователей и со своей стороны поддерживает с ними туннели IPSec.
- *Оконечный маршрутизатор* — обеспечивает базовое фильтрование и подключение к Интернет по Уровню 3.

Предотвращаемые угрозы

В рамках этого модуля наиболее вероятными объектами атаки являются открытые и общедоступные серверы. Ниже приведены предполагаемые угрозы:

- *Неавторизованный доступ* — нейтрализуется фильтрованием у Интернет-провайдера, на оконечном маршрутизаторе и корпоративном межсетевом экране.
- *Атаки уровня приложений* — нейтрализуются системой обнаружения вторжений в сетевом и хостовом вариантах.
- *Вирусы и «троянские» атаки* — нейтрализуются фильтрованием электронной почты, сетевой системой обнаружения вторжений и антивирусным сканированием хостов.
- *Атаки на пароли* — сокращаются путем уменьшения сервисов, уязвимых для прямого перебора. Эту угрозу позволяют отследить операционная система и системы обнаружения вторжений.
- *Отказ в обслуживании* — управление полосой пропускания на стороне Интернет-провайдера и контроль соединений TCP на межсетевом экране.
- *Подмена адресов IP (spoofing)* — нейтрализуется фильтрованием согласно RFC 2827 и RFC 1918 на выходе от Интернет-провайдера и на оконечном маршрутизаторе сети средней величины.

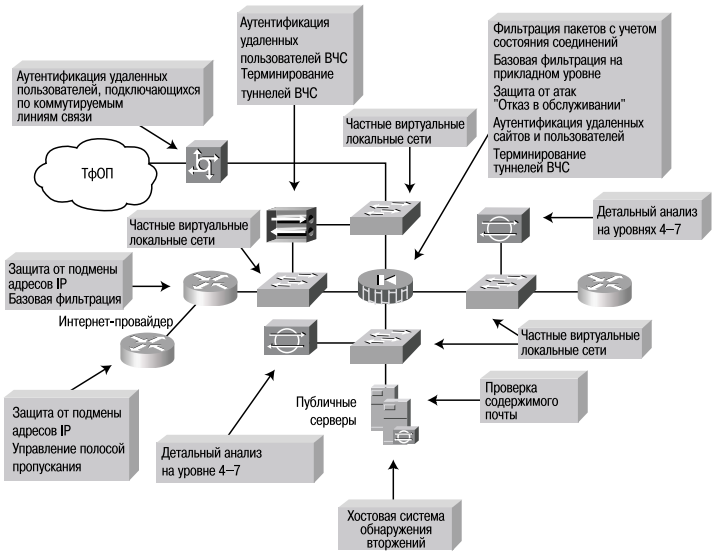


Рисунок 68. Отражение атак в модуле Интернет

- *Прослушиватели пакетов* — эта угроза снижается благодаря коммутируемой инфраструктуре и хостовым системам обнаружения вторжений.
- *Изучение сети* — система обнаружения вторжений распознает попытку изучения, а фильтрование протоколов снижает ее эффективность.
- *Злоупотребление доверием* — запретительная модель доверия и частные виртуальные локальные сети для ограничения атак на основе доверия.
- *Переадресация портов* — запретительное фильтрование и хостовая система обнаружения вторжений, ограничивающая атаки.

В этом модуле объектами атак являются также сервисы удаленного доступа и сети ВЧС между сайтами. Для этих объектов существуют следующие угрозы:
- *Раскрытие топологии сети* — списки контроля доступа (Access control lists — ACLs) на входном маршрутизаторе ограничивают доступ из Интернет к VPN-концентратору, межсетевому экрану (когда они используются для поддержки со своей стороны IPSec-туннелей к удаленным сайтам), к Internet Key Exchange (IKE) и Encapsulating Security Payload (ESP).
- *Атаки на пароли* — атаки методом перебора нейтрализуют одноразовые пароли.
- *Неавторизованный доступ* — трафик от неавторизованных портов после расшифровки пакетов запрещают сервисы межсетевого экрана.
- *Атаки «посредника»* — такие атаки нейтрализуются шифрованием удаленного трафика.
- *Прослушивание пакетов* — эффективность прослушивания ограничивается коммутируемой инфраструктурой.

Рекомендации по дизайну

В этом разделе подробно описываются функции устройств, входящих в корпоративный модуль Интернет.

Маршрутизатор Интернет-провайдера

Важнейшей задачей оконечного маршрутизатора у Интернет-провайдера является обеспечение связи пользователей с сетью Интернет. На выходе маршрутизатора задаются некоторые пределы, которые ограничивают некритичный исходящий трафик, превышающий заданный порог, что позволяет нейтрализовать атаки DDoS. Организованное на выходе маршрутизатора Интернет-провайдера фильтрование нейтрализует подделки адресов локальной сети и частных адресных пространств.

Оконечный маршрутизатор

Функции оконечного маршрутизатора в средней сети заключаются в том, чтобы разграничивать сеть Интернет-провайдера и сеть предприятия. Базовое фильтрование на входе оконечного маршрутизатора ограничивает доступ, пропуская только разрешенный IP-трафик и блокируя большинство известных атак. Здесь же в качестве проверки проводится фильтрование по RFC 1918 и RFC 2827. В дополнение к этому маршрутизатор конфигурируется на сброс фрагментированных пакетов, которые в обычных типах Интернет-трафика не видны, а для защиты сети являются серьезной опасностью. Эта опасность настолько велика, что считается допустимым терять из-за такого фильтрования даже часть разрешенного трафика. Наконец, маршрутизатор пересылает любой IPSec-трафик, предназначенный для концентратора ВЧС или межсетевого экрана. Поскольку для ВЧС удаленного доступа IP-адрес удаленной системы не разглашается, то фильтруется трафик только отвечающего хоста (концентратора ВЧС), к которому обращается удаленный пользователь. При ВЧС-подключении «сайт с сайтом» IP-адрес удаленного сайта, как правило, известен, и поэтому фильтровать трафик можно в обоих направлениях.

Межсетевой экран

Главная задача межсетевого экрана — выполнять принудительное и подробное фильтрование инициированных через него сессий связи. Кроме этого, межсетевой экран работает как конечная точка для IPSec туннелей для управляющего и рабочего трафика удаленного сайта. В межсетевом экране различаются несколько сегментов. Во-первых, сегмент общедоступных сервисов, к которому относятся все общедоступные хосты. Второй сегмент — ВЧС удаленного доступа и дозвон — описан ниже. Общедоступные серверы в какой-то мере защищены от «затоплений» TCP SYN при помощи контроля «наполовину открытых соединений» на межсетевом экране. С точки зрения фильтрования в дополнение к ограничению трафика по адресам и портам в сегменте общедоступных сервисов используется также фильтрование в противоположном направлении. Если в ходе атаки взламывается один из общедоступных серверов, этот хост невозможно использовать как плацдарм для атаки других хостов сети.

Нейтрализовать этот тип атак позволяет специальное фильтрование неавторизованных запросов, генерируемых общедоступными серверами и направляемых на какой-либо еще адрес. Например, фильтрование web-сервера ведется так, что сам web-сервер не может генерировать запросы, а может только отвечать на запросы клиентов. Это предотвращает хакеру возможность загрузить на взломанный в ходе первичной атаки web-сервер собственные утилиты. Также это запрещает хакеру переключать в ходе первичной атаки некоторые сессии. В дополнение к этому атаковать другие серверы в своем сегменте не позволяют частные виртуальные локальные сети. Такой трафик не всегда отслеживается межсетевым экраном, и поэтому частные виртуальные локальные сети являются весьма важным элементом.

Обнаружение вторжений

К сегменту общедоступных сервисов относится и работа сетевой системы обнаружения вторжений, основной задачей которой является отслеживание атак по портам, которые указаны на межсетевом экране как разрешенные. Сетевая система обнаружения вторжений в сегменте общедоступных сервисов должна реализовывать запретительную политику, поскольку межсетевой экран в некоторых случаях оказывается бессилен. Плюс к этому каждый сервер дол-

жен иметь собственную систему обнаружения вторжений. Основной задачей хостовой системы обнаружения вторжений является отслеживание вредоносной активности на уровне операционной системы, а также на уровне серверных приложений (HTTP, FTP, SMTP и т. д.). DNS должен откликаться исключительно на разрешенные команды и не допускать никаких второстепенных откликов, которые могут помочь хакеру в изучении сети. Сюда относится запрещение межзональных пересылок (zone transfers) откуда бы ни было, кроме разрешенных вторичных серверов DNS. Сервер SMTP имеет сервисы проверки электронных сообщений, нейтрализующие вирусы и «троянские» атаки на внутреннюю сеть, которые обычно поступают по электронной почте. Межсетевой экран фильтрует SMTP-сообщения на Уровне 7, разрешая только необходимые команды для почтового сервера.
Размещение сетевой системы обнаружения вторжений между частным интерфейсом межсетевого экрана и внутренним маршрутизатором обеспечивает окончательный анализ атак.
В этом сегменте могут обнаруживаться всего лишь несколько типов атак, поскольку внутрь пропускаются только отклики на инициированные запросы, некоторые выбранные порты сервисов общедоступного сегмента и трафик сегмента удаленного доступа. Здесь будут обнаруживаться только сложные атаки, которые подразумевают, что система в сегменте общедоступных сервисов взломана и хакер пытается реализовать этот плацдарм для нападения на внутреннюю сеть. Например, когда взломан общедоступный сервер SMTP, хакер может попытаться взломать внутренний почтовый сервер по порту 25 TCP, который предназначен для передачи электронных сообщений между двумя хостами. Если атака обнаруживается именно в этом сегменте, то реакция на нее должна быть более жесткой, так как это означает, что взлом уже произошел. Внимательно рассмотрите применение TCP-сбросов и блокирование, вплоть до обрыва атак, подобных вышеназванной атаке по SMTP.

ВЧС удаленного доступа
Важнейшая функция концентратора ВЧС удаленного доступа заключается в обеспечении защищенных подключений к сети среднего размера удаленных пользователей. Перед тем как разрешить пользователю подключение, концентратор ВЧС инициирует сессию связи с сервером контроля доступа во внутренней сети, а сервер контроля доступа в свою очередь запрашивает систему одноразового пароля провести аутентификацию электронных идентификаторов пользователя. Благодаря пересылке политик IPSec между концентратором и клиентом пользователям запрещается запускать раздельное туннелирование (split tunneling), и они выходят в сеть только через корпоративное подключение. Для шифрования в протоколе IPSec используется алгоритм TripleDES или AES и алгоритм secure hash algorithm / hash-based message authentication code (SHA/HMAC) для проверки целостности данных. После туннеля трафик ВЧС проходит через межсетевой экран, гарантируя этим надежную фильтрацию пользователей. Такая организация также допускает блокирование атак на межсетевом экране системой обнаружения вторжений. Этот сценарий отличается от большинства прочих сценариев, в которых межсетевой экран размещается перед устройством ВЧС. При размещении перед устройством ВЧС межсетевой экран «не видит» типы трафика пользователей, так как весь трафик на этом этапе зашифрован.

Пользователи, подключающиеся по телефонным линиям
Сеансы пользователей, которые связываются с сетью, дозваниваясь по телефонным линиям, осуществляются через маршрутизатор дозвона со встроенными модемами. После того как подключение по Уровню 2 между пользователем и сервером установлено, проводится аутентификация пользователя по протоколу Challenge Handshake Authentication Protocol (CHAP). Как и в случае с сервисом удаленного доступа ВЧС, для аутентификации используется сервер AAA (authentication, authorization and accounting). Аутентифицированные пользователи получают IP-адреса в адресном пространстве.

Коммутаторы Уровня 2
Важнейшей функцией коммутаторов в рамках корпоративного Интернет-модуля является обеспечение связей между различными устройствами, входящими в этот модуль. Для обеспечения физического разделения внешнего сегмента, сегмента общедоступных сервисов, сегмента ВЧС и внутреннего сегмента применяется несколько коммутаторов, а не один коммутатор с множеством виртуальных локальных сетей. Такая организация нейтрализует возможность изменения конфигурации коммутатора, которая может привести к взлому защиты.

Внутренний маршрутизатор
Важнейшей функцией внутреннего маршрутизатора является разделение по Уровню 3 и маршрутизация между корпоративным Интернет-модулем и кампусным модулем. Это устройство работает исключительно как маршрутизатор без каких-то списков доступа, запрещающих трафик по какому-либо интерфейсу.
Поскольку сведения о маршрутизации могут использоваться для проведения атаки DoS, то должна использоваться аутентификация маршрутной информации, чтобы нейтрализовать возможность такой атаки. Этот маршрутизатор является границей между маршрутизируемой внутренней сетью и внешним миром. Так как большинство межсетевых экранов конфигурируется без протоколов маршрутизации, внутри корпоративного Интернет-модуля необходимо обеспечить такую точку маршрутизации, которая не зависела бы от остальной сети.

Альтернативы
Для этого модуля допустимы два разных дизайна. Вместо внедрения базового фильтрования на оконечном маршрутизаторе администратор может применить на этом устройстве динамическое фильтрование. Наличие двух динамических межсетевых экранов обеспечивает большую защиту модуля при эшелонированном подходе. В зависимости от взгляда администратора на вероятность атак, перед межсетевым экраном, возможно, потребуется сетевая система обнаружения вторжений. Кроме базовых функций фильтрования система обнаружения вторжений, будучи вынесена за межсетевой экран, обеспечивает важные сведения при возникновении тревог; в ином случае эта информация просто теряется. Поскольку количество возникающих в этом сегменте тревог достаточно велико, реагирование на возникающие здесь тревоги может быть менее жестким, чем на тревоги, источники которых находятся за межсетевым экра-

ном. Также предусмотрите отдельную управляющую станцию для регистрации тревог, поступающих из этого сегмента, чтобы каждой группе тревог уделялось необходимое внимание. Предлагаемое системой обнаружения вторжений наблюдение за пределами межсетевого экрана улучшает оценку атак, а плюс к этому позволяет оценить эффективность фильтров Интернет-провайдера и оконечных фильтров предприятия.

Существуют и две другие возможности. Первая — удаление маршрутизатора, расположенного между межсетевым экраном и кампусным модулем. Несмотря на то, что его функции могут быть переданы коммутатору кампусного модуля Уровня 3, такое изменение сделает невозможным работу корпоративного Интернет-модуля из другой части сети без обращения к сервисам Уровня 3.
Вторая возможность — организация проверки контента помимо проверки электронной почты. Например, в общедоступный сегмент можно вынести сервер проверки адресов URL, будет проверять страницы, к которым обращаются сотрудники.

Кампусный модуль

К кампусному модулю относятся рабочие станции конечных пользователей, корпоративные интранет-серверы, серверы управления, а также инфраструктура Уровня 2 и Уровня 3, необходимая для поддержки устройств.

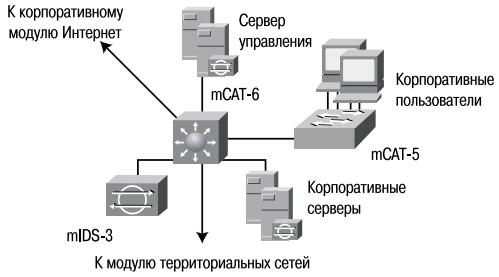


Рисунок 69. Дизайн кампусного модуля

Основные устройства

- Коммутатор Уровня 3 — маршрутизирует и коммутирует рабочий и управляющий трафик внутри кампусного модуля, предоставляет сервисы уровня распределения встраиваемым коммутаторам, предлагает расширенные сервисы, как например фильтрование трафика.
- Коммутаторы Уровня 2 (с поддержкой виртуальных локальных сетей) — обеспечивают рабочим станциям пользователей сервисы Уровня 2.
- Корпоративные серверы — поддерживают для внутренних пользователей сервисы электронной почты (SMTP и POP3), а также сервисы доставки файлов, печати и DNS для рабочих станций.
- Рабочие станции пользователей — предоставляют авторизованным пользователям сети сервисы
- Управляющий хост SNMP — выполняет управление устройствами по протоколу SNMP.
- Консоль системы обнаружения вторженй — собирает сведения о тревогах с установленных в сети устройств системы обнаружения вторжений.
- Хост(ы) Syslog — собирают журнальную информацию о межсетевых экранах и хостах NIDS.
- Сервер контроля доступа — поддерживает сервисы аутентификации для сетевых устройств.
- Сервер одноразовых паролей (One-time Password — OTP) — авторизует по одноразовому паролю информацию, поступающую от сервера контроля доступа.
- Хост администратора сети — поддерживает изменения конфигурации, программного обеспечения и контента устройств.
- Устройство сетевой системы обнаружения вторжений — наблюдает по Уровням 4-7 за важнейшими сетевыми сегментами модуля.

Предотвращаемые угрозы

- Прослушиватели пакетов — эта угроза снижается благодаря коммутируемой инфраструктуре.
- Вирусы и «троянские» атаки — нейтрализуются антивирусным сканированием хостов.
- Неавторизованный доступ — нейтрализуется обнаружением вторжений на хост и контролем доступа.
- Атаки на пароли — нейтрализуются тем, что сервер контроля доступа поддерживает жесткую двухфакторную аутентификацию для важнейших приложений.
- Атаки уровня приложений — нейтрализуются сетевой системой обнаружения вторжений, а также использованием предлагаемых производителем обновлений и программных «заплаток» для операционных систем, приложений.

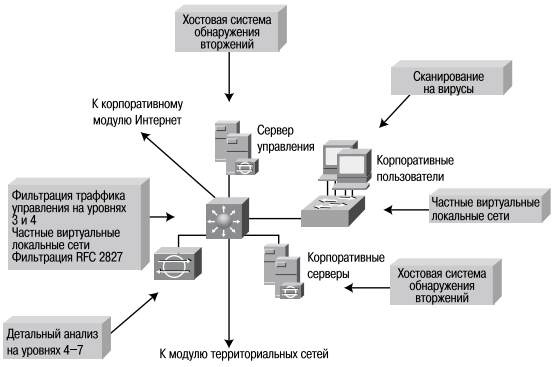


Рисунок 70. Отражение атак в кампусном модуле

- Подмена адресов IP (spoofing) — нейтрализуется фильтрованием по RFC 2827, которое предотвращает такую возможность.
- Злоупотребление доверием — частные виртуальные локальные сети запрещают хостам одной подсети обращаться друг к другу без необходимости.
- Переадресация портов — сетевая система обнаружения вторжений предотвращает инсталляцию агентов переадресации портов.

Рекомендации по дизайну

В этом разделе подробно описываются функции устройств, входящих в кампусный модуль.

Главный коммутатор

Основной функцией главного коммутатора является маршрутизация и коммутация рабочего и управляющего трафика, распределение сервисов разных уровней (маршрутизация, QoS и контроль доступа) для прочих коммутаторов сети здания, подключение к корпоративным серверам и серверам управления, а также расширенные сервисы, например фильтрование трафика между подсетями. Вместо коммутатора Уровня 2 выбран коммутатор Уровня 3 — это сделано для того, чтобы предоставить сегменту (или сегментам) корпоративных серверов, сегменту управляющих серверов, сегменту (или сегментам) корпоративных пользователей отдельные виртуальные локальные сети, а также чтобы обеспечить подключение к модулю территориальных сетей и к модулю корпоративных пользователей. Коммутатор Уровня 3 обеспечивает рубеж защиты и против атак, исходящих изнутри. Он запрещает департаменту доступ к конфиденциальной информации на сервере другого департамента, применяя для этого средства контроля доступа. Например, в сети предприятия существуют департамент маркетинга и департамент разработки и исследований; в этом случае сервер разработки и исследований выделяется в отдельную виртуальную локальную сеть, доступ к нему фильтруется, и это гарантирует его доступность только для сотрудников департамента разработки и исследований. По соображениям производительности важно, чтобы контроль доступа в данном случае был реализован на аппаратной платформе, которая способна фильтровать трафик со скоростью, близкой к скорости канала.

Такая организация сети диктует использование коммутации Уровня 3 в противоположность более традиционным выделенным устройствам маршрутизации. Подобный контроль доступа также позволяет предотвратить локальную подделку исходных адресов с помощью фильтрования по RFC 2827 — оно должно присутствовать в виртуальных локальных сетях корпоративных пользователей и корпоративных интранет-серверов.

Например, серверам в сегменте корпоративных серверов бывает необязательно связываться между собой, а только с устройствами, которые подключены к сегменту.

Чтобы организовать следующий рубеж защиты для серверов управления, на интерфейсе виртуальной локальной сети, исходящей к сегменту корпоративных серверов, настраивается экстенсивное фильтрование Уровня 3 и Уровня 4. Фильтр ограничивает подключения управляющих серверов, а также подключения к ним самим, разрешая это только контролируемым ими устройствам (по IP-адресу) и только по разрешенным протоколам. Сюда же входит контроль доступа для управляющего трафика, предназначенного устройствам на удаленных сайтах.

Этот трафик шифруется межсетевым экраном и отсылается удаленным сайтам. Доступ к управляемым устройствам и далее контролируется тем, что разрешается только одно обратное подключение через список доступа (фильтр — ACL).

Вторичные коммутаторы в сети здания

Главной задачей вторичных коммутаторов кампусного модуля является обеспечение сервисов Уровня 2 для рабочих станций корпоративных пользователей. Реализуемые на этих коммутаторах частные виртуальные локальные сети нейтрализуют атаки злоупотребления доверием, так как персональным рабочим станциям не требуется подключаться друг другу. В дополнение к принципам сетевой защиты, которые описываются как аксиомы защиты коммутаторов, на уровне рабочих станций организуется антивирусное сканирование.

Обнаружение вторжений

К кампусному модулю также относится сетевая система обнаружения вторжений. Подключенный к устройству системы обнаружения вторжений порт коммутатора конфигурируется таким образом, чтобы со всех виртуальных локальных сетей трафик, который необходимо наблюдать, зеркалировался бы на наблюдающий порт устройства. В этом месте обнаруживается очень немного атак, поскольку это устройство отслеживает те атаки, которые исходят из самого кампусного модуля. Например, когда рабочая станция пользователя взламывается через неопознанное модемное подключение, система обнаружения вторжений обнаруживает подозрительную активность, исходящую из этого места. Источниками других атак могут быть недовольные сотрудники, посторонние лица, воспользовавшиеся авторизованной в сети рабочей станцией в отсутствие ее пользователя, «троянские» приложения, случайно загруженные на мобильный компьютер, и проч. На каждом управляющем и корпоративном интранет-сервере плюс к этому устанавливается хостовая система обнаружения вторжений.

Альтернативы

Если сеть среднего размера относительно мала, то можно обойтись без вторичных коммутаторов, а их функции передать главному коммутатору. В этом случае рабочие станции конечных пользователей подключаются непосредственно к главному коммутатору, а для нейтрализации атак злоупотребления доверием на нем реализуется функциональность частных виртуальных локальных сетей.

Если требования к производительности внутренней сети невысоки, то вместо высокопроизводительного коммутатора Уровня 3 можно использовать отдельный маршрутизатор и коммутатор Уровня 2.

При желании отдельное устройство сетевой системы обнаружения вторжений можно заменить интегрированным модулем, который встраивается в главный коммутатор. Это обеспечивает ускоренную обработку трафика модулем системы обнаружения вторжений, поскольку в этом случае модуль с коммутатором объединен, а не ограничен скоростью порта подключения 10/100-Мбит Ethernet. Для контроля трафика, передаваемого модулю системы обнаружения вторжений можно, использовать ACL.

Модуль территориальных сетей

Этот модуль возникает только при необходимости подключения к удаленным сайтам по частной сети. Такая необходимость может возникнуть в

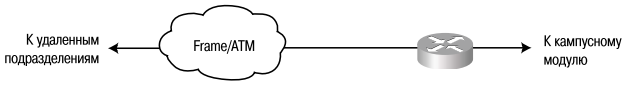


Рисунок 71. Дизайн модуля территориальных сетей

том случае, когда требования к качеству сервиса (QoS) уже не могут быть удовлетворены с помощью IPSec ВЧС или когда используются морально устаревшие подключения, а переход на IPSec не предполагается.

Основные устройства

- Маршрутизатор IOS — обеспечивает маршрутизацию, контроль доступа и механизм QoS для удаленных подключений

Предотвращаемые угрозы

- Подмена адресов IP (spoofing) — нейтрализуется фильтрованием по Уровню 3
- Неавторизованный доступ — простой контроль доступа позволяет ограничить филиалам типы протоколов, к которым они имеют доступ.

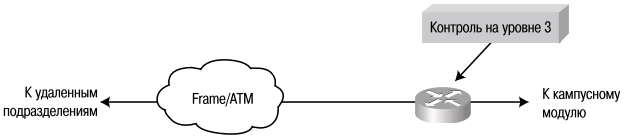


Рисунок 72. Отражение атак в территориальном модуле

Рекомендации по дизайну

Степень защищенности модуля WAN зависит от уровня доверия к удаленным сайтам, а также от Интернет-провайдера, предоставляющего связь. Защита обеспечивается средствами IOS. При этом дизайне приложенные к последовательному интерфейсу списки доступа на вход используются для блокирования попыток доступа в сеть любого нежелательного трафика. Будучи приложенными к Ethernet-интерфейсу, списки доступа на вход позволяют ограничивать трафик, направляемый из сети на удаленные сайты.

Альтернативы

Некоторые предприятия, трепетно следящие за приватностью информации, шифруют трафик в классических каналах территориальных сетей. Аналогично междусайтовым ВЧС такой же уровень защиты данных дает IPSec. Плюс к этому маршрутизатор, выполняя дополнительную роль межсетевого экрана в территориальной сети, обеспечивает больший набор функций контроля доступа по сравнению с классическими списками доступа (ACL), применяемыми в дизайне SAFE.

Сеть филиала

При конфигурации для филиала некоторые элементы дизайна среднего размера могут быть удалены. Во-первых, надо выяснить, как предприятие собирается подключаться к корпоративной штаб-квартире: по частному каналу или по IPSec VPN.

В пользу частного канала говорит более детализированная поддержка QoS, устойчивость сетевой инфраструктуры, поддержка многоадресной рассылки (multicast), требования к иному, чем IP, трафику. Помните, что при использовании IPSec поверх туннелей GRE (generic routing encapsulation) многоадресная рассылка и другие сетевые протоколы, а не только IP, могут поддерживаться средой ВЧС.

Есть несколько аргументов в пользу выбора IPSec VPN вместо подключения по территориальным сетям. Во-первых, IPSec ВЧС по Интернет может обеспечить локальный доступ в Инетернет ко всем удаленным сайтам, экономя при этом пропускную способность канала (и сокращая расходы) главной сети. Также во многих собственных и большинстве общеизвестных приложений IPSec ВЧС предлагает значительную экономию по сравнению с частными подключениями территориальных сетей.

Если для сети среднего размера, выполняющей роль сети филиала, выбирается частный канал, то корпоративный модуль Интернет становится не нужен (если в филиале не предполагается еще и собственный доступ в Интернет). С другой стороны, если выбран IPSec VPN, то становится ненужным частный канал, можно обойтись без концентратора ВЧС или маршрутизатора дозвона для удаленного доступа, если такие сервисы предоставляются штаб-квартирой.

С точки зрения управления, конфигурирование и управление защитой сети среднего размера должно выполняться из модуля управления, расположенного в штаб-квартире (предполагается централизация IT-ресурсов). Когда для взаимодействия сайтов выбран частный канал, то управляющий трафик может передаваться по нему ко всем управляемым устройствам. При выборе IPSec ВЧС большая часть управляющего трафика передается аналогичным образом, но некоторые устройства, например, оконечный маршрутизатор, размещенный вне межсетевого экрана, не являются частью канала IPSec и должны управляться иначе. В этом случае можно организовать к устройству дополнительный туннель IPSec или использовать для конфигурирования устройства шифрование приложений (SSH). Но, как упоминалось в аксиомах, не все приложения имеют защищенные варианты.

Дизайн для подключения удаленных пользователей

В этом разделе обсуждаются четыре варианта подключения удаленных пользователей к дизайну SAFE. Удаленное подключение применяется для мобильных и надомных сотрудников. Основная задача этого дизайна: обеспечить подключение удаленных пользователей к штаб-квартире, а в некоторых случаях и к Интернет.

Предлагаются следующие решения доступа: программное, программно-аппаратное, аппаратное.

- *Программный доступ* — на компьютере удаленного пользователя установлен программный клиент ВЧС и персональный межсетевой экран.
- *Межсетевой экран на удаленном сайте* — удаленный сайт защищен выделенным межсетевым экраном, который плюс к этому поддерживает подключение к корпоративной штаб-квартире по IPSec ВЧС; подключение поддерживается предоставляемым провайдером устройством широкополосного доступа (например DSL или кабельным модемом).
- *Аппаратный клиент ВЧС* — на удаленном сайте установлен аппаратный клиент ВЧС, который поддерживает IPSec ВЧС — подключение к корпоративной штаб-квартире; подключение WAN обеспечивается предоставляемым провайдером устройством широкополосного доступа.
- *Маршрутизатор на удаленном сайте* — на удаленном сайте установлен маршрутизатор, выполняющий функции межсетевого экрана и поддерживающий подключение к штаб-квартире. Маршрутизатор может быть подключен либо напрямую, либо через Интернет-провайдера.

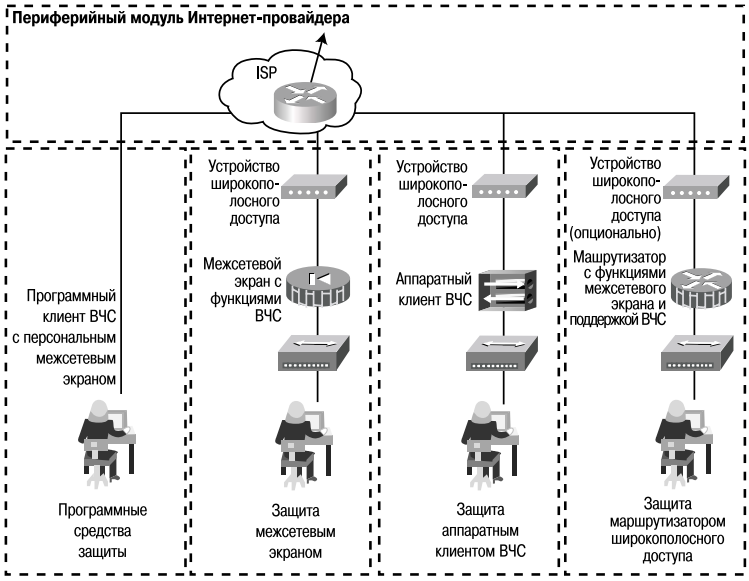


Рисунок 73. Дизайн удаленного доступа пользователей

Каждый из приведенных дизайнов обсуждается ниже в разделах «Рекомендации по дизайну». Во всех случаях предполагается подключение через Интернет; если же вместо этого используются частные каналы, то шифрование трафика становится необязательным. Помните, что в любом варианте с удаленным сайтом периметр защиты предприятия растягивается, чтобы охватить все подключаемые удаленные сайты.

Основные устройства

- *Устройство широкополосного доступа* — обеспечивает доступ к широкополосной сети (DSL, кабель и проч.).
- *Межсетевой экран с поддержкой ВЧС* — поддерживает защищенные шифрованные туннели между удаленным сайтом и корпоративным узлом. Обеспечивает на сетевом уровне защиту ресурсов удаленного сайта и динамическое фильтрование трафика.
- *Концентратор Ethernet или коммутатор Уровня 2* — поддерживает подключения устройств удаленного сайта (может быть интегрирован в межсетевой экран или в аппаратный клиент ВЧС)
- *Персональный программный межсетевой экран* — обеспечивает защиту отдельных компьютеров.
- *Маршрутизатор с функциями межсетевого экрана и ВЧС* — поддерживает защищенные шифрованные туннели между удаленным сайтом и корпоративным узлом. Обеспечивает на сетевом уровне защиту ресурсов удаленного сайта и динамическое фильтрование трафика; может поддерживать дополнительные сервисы (голос, QoS).

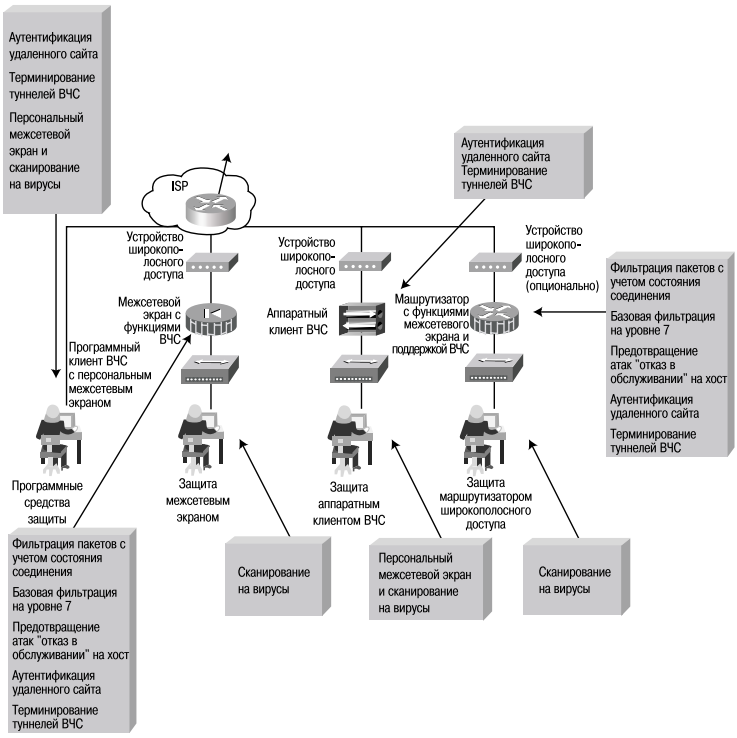


Рисунок 74. Отражение атак в модуле удаленного доступа

- *Программный клиент ВЧС* — поддерживает защищенные туннели между отдельным компьютером и корпоративным узлом.
- *Аппаратный клиент ВЧС* — поддерживает защищенные туннели между удаленным сайтом и корпоративным узлом.

Предотвращаемые угрозы

- *Неавторизованный доступ* — нейтрализуется фильтрованием и динамическим инспектированием сессий на маршрутизаторе/межсетевом экране удаленного сайта или же контролем доступа для приложений с помощью программного межсетевого экрана.
- *Изучение сети* — эффективность изучения можно снизить, применив фильтрование протоколов на удаленных устройствах.
- *Вирусы и «троянские» атаки* — нейтрализуются антивирусным сканированием на уровне хостов.
- *Подмена адресов IP (spoofing)* — нейтрализуется фильтрованием согласно RFC 2827 и RFC 1918 на стороне Интернет-провайдера и устройств удаленного сайта.
- *Атаки «посредника» (Man-in-the-middle)* — нейтрализуются шифрованием трафика удаленного сайта.

Рекомендации по дизайну

В этом разделе подробно описывается работа каждого варианта подключения удаленных пользователей.

Программный доступ

Программный доступ оптимален для мобильных пользователей и надомных работников. Всем удаленным пользователям необходим компьютер с установленным программным клиентом ВЧС, а также подключение к Интернет по сети Ethernet или по телефонному каналу.

Основной задачей программного клиента ВЧС является установление защищенного зашифрованного канала от устройства клиента до устройства ВЧС на узле отвечающей стороны. Доступ в сеть и авторизация контролируются из штаб-квартиры; фильтрование выполняется на межсетевом экране и непосредственно у клиента, если ему делегированы такие права. При очередном подключении удаленный пользователь в первую очередь проходит аутентификацию, затем получает динамический IP-адрес, который используется для всего трафика VPN, а также принимает имена серверов (DNS и Windows Internet Name Service — WINS). С центрального узла можно включить или, наоборот, выключить раздельное туннелирование. При дизайне SAFE раздельное туннелирование отключено, принуждая пользователей после установления туннеля ВЧС выходить в Интернет через корпоративное подключение. Поскольку удаленные пользователи не всегда используют туннели ВЧС при подключении к сети провайдера или к Интернет, то им рекомендуется иметь собственный межсетевой экран, чтобы нейтрализовать попытки несанкционированного доступа на их компьютер. Также им рекомендуется использовать программы-антивирусы, позволяющие защититься от заражения компьютера и от «троянских» атак.

Межсетевой экран на удаленном сайте

Межсетевой экран на удаленном сайте подходит для надомных сотрудников или для очень малого филиала. В этом случае предполагается, что удаленный сайт имеет какой-либо широкополосный канал связи с Интернет-провайдером. Межсетевой экран устанавливается позади DSL- или кабельного модема.

Главной задачей межсетевого экрана является установление защищенного зашифрованного туннеля между ним и устройством отвечающей стороны, а также поддержка связи и скрупулезное фильтрование проходящих через него сессий связи. Отдельно каждому компьютеру удаленной сети программный агент ВЧС для доступа к корпоративным ресурсам не требуется. Дополнительно к этому, поскольку динамический межсетевой экран защищает доступ в Интернет, то и индивидуальные межсетевые экраны каждому компьютеру тоже не требуются. Однако, если сетевой администратор считает необходимым повысить защищенность, то на удаленных компьютерах можно использовать и такие индивидуальные межсетевые экраны. Такое построение весьма полезно, если сотрудник часто выезжает в командировки и подключается к Интернет напрямую через сеть общего пользования. Благодаря установленному на хосте динамическому межсетевому экрану и фильтрованию удаленный сайт может иметь прямой выход в Интернет вместо передачи всего трафика через штаб-квартиру. Пока для подключения к штаб-квартирам используется трансляция сетевых адресов (NAT), распределяемые между удаленными устройствами адреса IP не должны конфликтовать между собой и с адресным пространством самой штаб-квартиры. Для устройств удаленного сайта, которым требуется прямой доступ в Интернет, необходима трансляция адресов на адреса зарегистрированные. Такую трансляцию можно организовать, транслируя все идущие в Интернет сессии на публичные IP-адреса на межсетевом экране.

Доступ к корпоративной сети и Интернет, а также авторизация контролируются и межсетевым экраном удаленного сайта, и ответным устройством ВЧС в штаб-квартире. Настройка и защищенное управление межсетевого экрана на удаленном сайте осуществляются по туннелю IPSec из головного офиса. При таком построении удаленным пользователям не требуется изменять настройки своего индивидуального межсетевого экрана. Доступ к настройкам такого экрана должен открываться только после аутентификации, чтобы локальный пользователь не имел возможности случайно изменить его настройки и таким образом нарушить политику безопасности устройства. При обращении удаленного пользователя к корпоративной сети его аутентификация не проводится. Вместо этого проводится взаимная аутентификация межсетевого экрана удаленного сайта и устройства ВЧС отвечающей стороны.

Как и на любом компьютере предприятия, на компьютерах удаленных пользователей рекомендуется использовать антивирусные программы, чтобы защититься от вирусов и «троянских» атак.

Аппаратный клиент ВЧС

Вариант с аппаратным клиентом ВЧС идентичен варианту с межсетевым экраном на удаленном сайте, за исключением того, что аппаратный клиент не имеет постоянного динамического межсетевого экрана. Это требует применения индивидуального межсетевого экрана на каждом хосте и в частности при включенном разделении туннелей.

В отсутствие индивидуального межсетевого экрана защищенность хоста, расположенного позади устройства VPN, зависит от неспособности нападающего «обойти» трансляцию сетевых адресов (Network Address Translation — NAT). Это имеет место потому, что, когда разделение туннелей включено, все подключения к Интернет проходят через простую трансляцию типа «все в одно» и не проходят фильтрование Уровня 4 и выше. Если же разделение туннелей выключено, все подключения к Интернет должны в обязательном порядке осуществляться через штаб-квартиру. Это частично смягчает требования к персональным межсетевым экранам на конечных системах.

Применение аппаратного клиента имеет два основных преимущества. Во-первых, как и в случае с программным клиентом ВЧС, доступ и авторизация в корпоративную сеть и в Интернет контролируются централизованно из штаб-квартиры. Конфигурирование и защищенное управление аппаратным клиентом выполняются с центрального сайта по SSL-подключению, и потому конечному пользователю не нужно заниматься этим самостоятельно. Во-вторых, при аппаратном клиенте не нужно использовать программный клиент ВЧС, чтобы получить доступ к корпоративным ресурсам. Аутентификацию пользователя при подключении к корпоративной сети аппаратный VPN-клиент не поддерживает. Вместо этого взаимную аутентификацию проводят аппаратный клиент ВЧС и центральный концентратор.

Маршрутизатор на удаленном сайте
Вариант маршрутизатора на удаленном сайте во многом аналогичен варианту с межсетевым экраном, но имеет и некоторые отличия.
Когда маршрутизатор установлен после специального устройства широкополосного доступа, единственным отличием является то, что маршрутизатор может поддерживать такие расширенные приложения, как QoS, маршрутизация и дополнительная инкапсуляция. Если при этом маршрутизатор имеет встроенные функции поддержки широкополосного доступа, то специальное устройство становится ненужным. В этом варианте подразумевается, что Интернет-провайдер позволяет вам управлять маршрутизатором доступа самостоятельно, что не всегда возможно.

Стратегии миграции

SAFE представляет собой руководство по внедрению систем безопасности в корпоративных сетях. Это не идеальная политика безопасности, годная для любой корпоративной сети, и не идеальный дизайн, гарантирующий полную безопасность всех существующих сетей. Это лишь шаблон, позволяющий инженерам проектировать и развертывать корпоративные сети с учетом требований безопасности.

Первым шагом на пути к безопасной инфраструктуре является разработка политики безопасности. Базовые рекомендации к политике безопасности можно найти в конце этого документа в Приложении В «Основы сетевой безопасности». После разработки стратегии проектировщик должен рассмотреть аксиомы безопасности, описанные в первом разделе настоящего документа, и определить, каким образом реализовать политику безопасности в существующей сетевой инфраструктуре.

Наша архитектура является достаточно гибкой, а вопросы дизайна описаны достаточно подробно, что позволяет адаптировать элементы архитектуры SAFE к большинству корпоративных сетей. К примеру, в модуле ВЧС/удаленного доступа различным потокам трафика, поступающего из сетей общего пользования, соответствует своя пара терминирующих устройств и отдельный интерфейс межсетевого экрана. С другой стороны, весь трафик ВЧС можно сконцентрировать на одной паре устройств, если это допускают параметры нагрузки и если для обоих типов трафика действует единая политика безопасности. В другой сети пользователи с традиционным модемным доступом и пользователи ВЧС с удаленным доступом могут беспрепятственно входить в сеть, поскольку система безопасности в достаточной степени доверяет механизмам аутентификации, допускающим подключение только санкционированных пользователей.

SAFE позволяет проектировщику решать проблемы безопасности отдельно для каждой сетевой функции. Каждый модуль, как правило, является самодостаточным и исходит из того, что любой другой подключаемый к нему модуль имеет только базовые средства защиты. Это позволяет инженерам использовать поэтапный подход к проектированию безопасности корпоративной сети. Они могут повысить степень защиты наиболее важных сетевых функций, подчинив их определенной политике безопасности и не меняя при этом архитектуру всей остальной сети. Исключением является модуль управления. В ходе первоначального развертывания архитектуры SAFE модуль управления должен устанавливаться одновременно с первым модулем, а затем последовательно подключаться ко всем остальным модулям по мере их установки.

Настоящая первая версия архитектуры SAFE предназначена для решения вопросов безопасности корпоративной сети общего характера. Авторы вполне отдают себе отчет в том, что существует множество областей, требующих более детальной проработки, изучения и совершенствования. Вот лишь некоторые из них:

- глубокий анализ управления безопасностью и внедрения систем безопасности;
- специализированная информация по проектированию малых сетей;
- глубокий анализ систем аутентификации, услуг директорий, технологий AAA (аутентификации, авторизации и учета) и выдачи сертификатов (certificate authority);
- масштабируемые версии центральной части ВЧС и проектирование территориальных сетей (WAN).

Приложение A. Оценочная лаборатория

В лабораторных условиях была создана типовая реализация архитектуры SAFE, которая служит для оценки функциональности, описанной в настоящем документе. В данном приложении детально описываются конфигурации конкретных устройств каждого модуля и приводятся общие указания по конфигурированию устройств. Ниже следуют примеры конфигураций, снятые с реальных устройств, установленных в лаборатории. Авторы не рекомендуют слепо копировать эти настройки на устройства, установленные в производственной сети.

Общие указания

Маршрутизаторы

Вот базовые опции конфигурации, реализованные почти на всех маршрутизаторах в лаборатории SAFE.

```
! turn off unnecessary services
!
no ip domain-lookup
no cdp run
no ip http server
no ip source-route
no service finger
no ip bootp server
no service udp-small-s
no service tcp-small-s
!
!turn on logging and snmp
!
service timestamp log datetime localtime
logging 192.168.253.56
logging 192.168.253.51
snmp-server community Txo~QbW3XM ro 98
!
!set passwords and access restrictions
!
service password-encryption
enable secret %Z<)|z9~zq
no enable password
no access-list 99
access-list 99 permit 192.168.253.0 0.0.0.255
access-list 99 deny any log
no access-list 98
access-list 98 permit host 192.168.253.51
access-list 98 deny any log
line vty 0 4
access-class 99 in
login
password 0 X)[^j+#T98
exec-timeout 2 0
line con 0
login
password 0 X)[^j+#T98
exec-timeout 2 0
line aux 0
transport input none
password 0 X)[^j+#T98
no exec
exit
banner motd #
                This is a private system operated for and by Cisco VSEC BU.
          Authorization from Cisco VSEC management is required to use this system.
                         Use by unauthorized persons is prohibited.
#
!
!Turn on NTP
!
clock timezone PST -8
clock summer-time PST recurring

ntp authenticate
ntp authentication-key 1 md5 -UN&/6[oh6
ntp trusted-key 1
ntp access-group peer 96
ntp server 192.168.254.57 key 1
access-l 96 permit host 192.168.254.57
```

```
access-l 96 deny any log
!
!Turn on AAA
!
aaa new-model
aaa authentication login default tacacs+
aaa authentication login no_tacacs line
aaa authorization exec tacacs+
aaa authorization network tacacs+
aaa accounting network start-stop tacacs+
aaa accounting exec start-stop tacacs+
tacacs-server host 192.168.253.54 single
tacacs-server key SJj)j~t]6-
line con 0
login authentication no_tacacs
```

Следующая ниже конфигурация определяет параметры аутентификации OSPF и фильтрации для всех маршрутизаторов OSPF в сети. Заметим, что аутентификация MD5 и списки распределения не анонсируют сеть, используемую для управления (OOB).

```
interface Vlan13
ip address 10.1.13.3 255.255.255.0
ip ospf authentication message-digest
ip ospf message-digest-key 1 md5 7 024D105641521F0A7E
ip ospf priority 3
!
router ospf 1
area 0 authentication message-digest
network 10.1.0.0 0.0.255.255 area 0
distribute-list 1 out
distribute-list 1 in
!
access-list 1 deny 192.168.0.0 0.0.255.255
access-list 1 permit any
```

Следующий пример конфигурации определяет параметры контроля доступа на всех интерфейсах сети управления по всей сети. Заметим, что это делается в дополнение к частным сетям VLAN, блокирующим доступ к управляемым IP-адресам хостов.


```
interface FastEthernet1/0
ip address 192.168.254.15 255.255.255.0
ip access-group 101 in
ip access-group 102 out
no cdp enable
!
access-list 101 permit icmp any any
access-list 101 permit tcp 192.168.253.0 0.0.0.255 host 192.168.254.15 established
access-list 101 permit udp 192.168.253.0 0.0.0.255 host 192.168.254.15 gt 1023
access-list 101 permit tcp 192.168.253.0 0.0.0.255 host 192.168.254.15 eq telnet
access-list 101 permit udp host 192.168.253.51 host 192.168.254.15 eq snmp
access-list 101 permit udp host 192.168.253.53 host 192.168.254.15 eq tftp
access-list 101 permit udp host 192.168.254.57 host 192.168.254.15 eq ntp
access-list 101 deny ip any any log
access-list 102 deny ip any any log
```

Коммутаторы

Ниже следует базовая конфигурация безопасности, установленная почти на всех коммутаторах CAT OS в лаборатории SAFE. Коммутаторы IOS используют конфигурацию, практически идентичную конфигурациям маршрутизаторов.

```
!
!Turn on NTP
!
set timezone PST -8
set summertime PST
set summertime recurring
set ntp authentication enable
set ntp key 1 trusted md5 -UN&/6[oh6
set ntp server 192.168.254.57 key 1
set ntp client enable
!
! turn off un-needed services
!
set cdp disable
set ip http server disable
!
!turn on logging and snmp
!
```

```
set logging server 192.168.253.56
set logging server 192.168.253.51
set logging timestamp enable
set snmp community read-only Txo~QbW3XM
set ip permit enable snmp
set ip permit 192.168.253.51 snmp
!
!Turn on AAA
!
set tacacs server 192.168.253.54 primary
set tacacs key SJj)j~t]6-
set authentication login tacacs enable telnet
set authentication login local disable telnet
set authorization exec enable tacacs+ deny telnet
set accounting exec enable start-stop tacacs+
set accounting connect enable start-stop tacacs+
!
!set passwords and access restrictions
!
set banner motd <c>
                This is a private system operated for and by Cisco VSEC BU.
          Authorization from Cisco VSEC management is required to use this system.
                        Use by unauthorized persons is prohibited.
<c>
!console password is set by 'set password'
!enter old password followed by new password
!console password = X)[^j+#T98
!
!enable password is set by 'set enable'
!enter old password followed by new password
!enable password = %Z<)|z9~zq
!
!the following password configuration only works the first time
!
set password
X)[^j+#T98
X)[^j+#T98
set enable
cisco
%Z<)|z9~zq
%Z<)|z9~zq
!
!the above password configuration only works the first time
!
set logout 2
set ip permit enable telnet
set ip permit 192.168.253.0 255.255.255.0 telnet
```

Хосты

На хостах используются самые свежие коррекционные модули (патчи). Кроме того, используются средства HIDS (приложение ClickNet Entercept). Более подробную информацию можно получить на сайте http://www.clicknet.com

Сеть крупного предприятия

Модуль управления

Используемые продукты

- Коммутаторы Уровня 2 Cisco Catalyst 3500XL (все — в качестве коммутаторов)
- Маршрутизатор Cisco 3640 IOS с функциями межсетевого экрана (eIOS-21)
- Маршрутизатор Cisco 2511 IOS (терминальные серверы)
- Сенсор обнаружения атак Cisco Secure IntrusionDetection System (CSIDS)
- Сервер RSA SecureID OTP Server
- Сервер безопасного доступа Cisco Secure Access Control Server
- Cisco Works 2000
- Cisco Secure Policy Manager
- Средство анализа netForensics syslog analysis tool
- Система обнаружения атак на уровне хостов CiscoSecure Host IDS

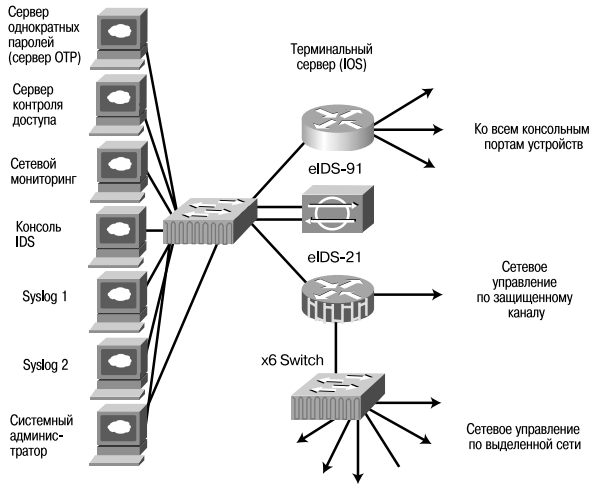


Рисунок 75. Модуль управления

EIOS-21

Ниже следуют параметры межсетевых экранов IOS Firewall, устанавливаемые по умолчанию:

```
ip inspect audit-trail
ip inspect max-incomplete low 150
ip inspect max-incomplete high 250
ip inspect one-minute low 100
ip inspect one-minute high 200
ip inspect udp idle-time 20
ip inspect dns-timeout 3
ip inspect tcp idle-time 1800
ip inspect tcp finwait-time 3
ip inspect tcp synwait-time 15
ip inspect tcp max-incomplete host 40 block-time 0
ip inspect name mgmt_fw tcp timeout 300
ip inspect name mgmt_fw udp
ip inspect name mgmt_fw tftp
ip inspect name mgmt_fw http
ip inspect name mgmt_fw fragment maximum 256 timeout 1
ip audit notify log
ip audit po max-events 100
```

Ниже следуют настройки защищенного сетевого управления по основному каналу:

```
crypto isakmp policy 1
encr 3des
authentication pre-share
group 2
crypto isakmp key A%Xr)7,_) address 172.16.224.24
crypto isakmp key A%Xr)7,_) address 172.16.224.23
!
crypto ipsec transform-set vpn_module_mgmt esp-3des esp-sha-hmac
!
crypto map mgmt1 100 ipsec-isakmp
set peer 172.16.224.24
set transform-set vpn_module_mgmt
match address 111
crypto map mgmt1 200 ipsec-isakmp
set peer 172.16.224.23
set transform-set vpn_module_mgmt
match address 110
access-list 110 permit ip 192.168.253.0 0.0.0.255 host 172.16.224.23
access-list 110 permit udp 192.168.254.0 0.0.0.255 host 172.16.224.23
access-list 111 permit ip 192.168.253.0 0.0.0.255 host 172.16.224.24
access-list 111 permit udp 192.168.254.0 0.0.0.255 host 172.16.224.24
```


Следующая конфигурация определяет параметры контроля доступа для трафика, входящего из сети, где находятся администрируемые системы IDS. Порт 45000 предназначен для CSIDS, а порт 5000 — для CiscoSecure Host IDS.

```
access-list 114 permit icmp 192.168.254.0 0.0.0.255 192.168.253.0 0.0.0.255 echo-reply
access-list 114 permit udp 192.168.254.0 0.0.0.255 host 192.168.253.56 eq syslog
access-list 114 permit udp 192.168.254.0 0.0.0.255 host 192.168.253.51 eq syslog
access-list 114 permit udp 192.168.254.0 0.0.0.255 host 192.168.253.50 eq 45000
access-list 114 permit tcp 192.168.254.0 0.0.0.255 host 192.168.253.50 eq 5000
access-list 114 permit udp 192.168.254.0 0.0.0.255 host 192.168.253.53 eq tftp
access-list 114 permit udp 192.168.254.0 0.0.0.255 host 192.168.254.57 eq ntp
access-list 114 permit tcp 192.168.254.0 0.0.0.255 host 192.168.253.54 eq tacacs
access-list 114 permit udp 192.168.254.0 0.0.0.255 host 192.168.253.54 eq 1645
access-list 114 permit udp 192.168.254.0 0.0.0.255 host 192.168.253.52 eq syslog
access-list 114 deny ip any any log
```

Следующая конфигурация определяет параметры контроля доступа для трафика, выходящего из сети управления:

```
access-list 113 permit icmp 192.168.253.0 0.0.0.255 192.168.254.0 0.0.0.255
access-list 113 permit icmp 192.168.253.0 0.0.0.255 host 192.168.253.57
access-list 113 permit tcp 192.168.253.0 0.0.0.255 host 192.168.253.57 eq telnet
access-list 113 permit tcp 192.168.253.0 0.0.0.255 192.168.254.0 0.0.0.255 eq telnet
access-list 113 permit tcp 192.168.253.0 0.0.0.255 192.168.254.0 0.0.0.255 eq 443
access-list 113 permit tcp 192.168.253.0 0.0.0.255 192.168.254.0 0.0.0.255 eq 22
access-list 113 permit udp host 192.168.253.50 192.168.254.0 0.0.0.255 eq 45000
access-list 113 permit tcp host 192.168.253.50 192.168.254.0 0.0.0.255 eq 5000
access-list 113 permit udp host 192.168.253.51 192.168.254.0 0.0.0.255 eq snmp
access-list 113 permit udp host 192.168.253.53 gt 1023 host 192.168.253.57 gt 1023
access-list 113 permit udp 192.168.253.0 0.0.0.255 host 192.168.254.57 eq ntp
```

```
access-list 113 permit tcp host 192.168.253.54 eq tacacs host 192.168.253.57 gt 1023
access-list 113 permit icmp 192.168.253.0 0.0.0.255 host 172.16.224.23
access-list 113 permit icmp 192.168.253.0 0.0.0.255 host 172.16.224.24
access-list 113 permit tcp 192.168.253.0 0.0.0.255 host 172.16.224.23 eq telnet
access-list 113 permit tcp 192.168.253.0 0.0.0.255 host 172.16.224.24 eq telnet
access-list 113 permit udp host 192.168.253.51 host 172.16.224.23 eq snmp
access-list 113 permit udp host 192.168.253.51 host 172.16.224.24 eq snmp
access-list 113 deny ip any any log
```

Следующая конфигурация определяет параметры доступа для трафика, входящего из производственной сети. Разрешается доступ только для защищенного трафика, поскольку только такой трафик допускается в модуль управления из производственной сети. Первые четыре строки определяют параметры доступа для защищенного трафика. После дешифрации, прежде чем получить доступ к модулю управления, трафик должен снова пройти через список доступа.

```
access-list 112 permit esp host 172.16.224.23 host 10.1.20.57
access-list 112 permit esp host 172.16.224.24 host 10.1.20.57
access-list 112 permit udp host 172.16.224.24 host 10.1.20.57 eq isakmp
access-list 112 permit udp host 172.16.224.23 host 10.1.20.57 eq isakmp
access-list 112 permit udp host 172.16.224.24 host 192.168.253.56 eq syslog
access-list 112 permit udp host 172.16.224.23 host 192.168.253.56 eq syslog
access-list 112 permit udp host 172.16.224.24 host 192.168.253.51 eq syslog
access-list 112 permit udp host 172.16.224.23 host 192.168.253.51 eq syslog
access-list 112 permit udp host 172.16.224.24 host 192.168.253.53 eq tftp
access-list 112 permit udp host 172.16.224.23 host 192.168.253.53 eq tftp
access-list 112 permit udp host 172.16.224.24 host 192.168.253.57 eq ntp
access-list 112 permit udp host 172.16.224.23 host 192.168.253.57 eq ntp
access-list 112 permit tcp host 172.16.224.24 host 192.168.253.54 eq tacacs
access-list 112 permit tcp host 172.16.224.23 host 192.168.253.54 eq tacacs
access-list 112 permit icmp host 172.16.224.24 192.168.253.0 0.0.0.255 echo-reply
access-list 112 permit icmp host 172.16.224.23 192.168.253.0 0.0.0.255 echo-reply
access-list 112 deny ip any any log
```

Базовый модуль

Используемые продукты

- Коммутаторы Уровня 3 Cisco Catalyst 6500 Layer 3 Switches

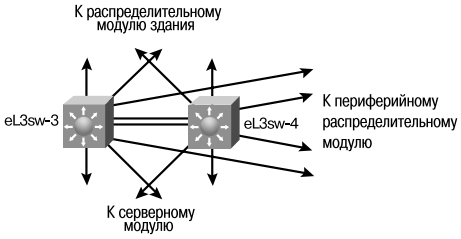


Рисунок 75. Базовый модуль

Распределительный модуль здания

Используемые продукты

- Коммутаторы Уровня 3 Cisco Catalyst 6500 Layer 3 Switches

EL3SW-5

Следующая конфигурация определяет параметры контроля доступа на Уровне 3 для связи между подсетями данного модуля. VLAN 5 определяет подсеть маркетинга, VLAN 6 определяет подсеть НИОКР (R&D), VLAN 7 определяет IP-телефоны сети маркетинга, а VLAN 8 определяет IP-телефоны сети НИОКР.

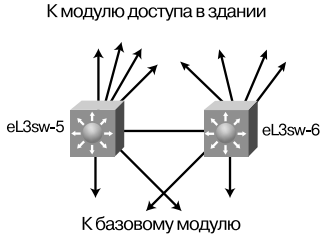


Рисунок 76. Распределительный модуль здания

```
interface Vlan5
ip address 10.1.5.5 255.255.255.0
ip access-group 105 in
!
interface Vlan6
ip address 10.1.6.5 255.255.255.0
ip access-group 106 in
!
interface Vlan7
ip address 10.1.7.5 255.255.255.0
ip access-group 107 in
!
interface Vlan8
ip address 10.1.8.5 255.255.255.0
ip access-group 108 in
!
access-list 105 deny ip 10.1.5.0 0.0.0.255 10.1.6.0 0.0.0.255
access-list 105 deny ip 10.1.5.0 0.0.0.255 10.1.7.0 0.0.0.255
access-list 105 deny ip 10.1.5.0 0.0.0.255 10.1.8.0 0.0.0.255
access-list 105 deny ip 10.1.5.0 0.0.0.255 10.1.16.0 0.0.0.255
access-list 105 permit ip 10.1.5.0 0.0.0.255 any
access-list 105 deny ip any any log
access-list 106 deny ip 10.1.6.0 0.0.0.255 10.1.5.0 0.0.0.255
access-list 106 deny ip 10.1.6.0 0.0.0.255 10.1.7.0 0.0.0.255
```

```
access-list 106 deny ip 10.1.6.0 0.0.0.255 10.1.8.0 0.0.0.255
access-list 106 deny ip 10.1.6.0 0.0.0.255 10.1.15.0 0.0.0.255
access-list 106 deny ip 10.1.6.0 0.0.0.255 10.1.16.0 0.0.0.255
access-list 106 permit ip 10.1.6.0 0.0.0.255 any
access-list 106 deny ip any any log
access-list 107 permit ip 10.1.7.0 0.0.0.255 10.1.8.0 0.0.0.255
access-list 107 permit ip 10.1.7.0 0.0.0.255 10.1.16.0 0.0.0.255
access-list 107 permit ip 10.1.7.0 0.0.0.255 host 10.1.11.50
access-list 107 deny ip any any log
access-list 108 permit ip 10.1.8.0 0.0.0.255 10.1.7.0 0.0.0.255
access-list 108 permit ip 10.1.8.0 0.0.0.255 10.1.16.0 0.0.0.255
access-list 108 permit ip 10.1.8.0 0.0.0.255 host 10.1.11.50
access-list 108 deny ip any any log
```

Модуль доступа здания

Используемые продукты

- Коммутаторы Уровня 2 Cisco Catalyst 4003 Layer 2 Switches
- IP-телефон Cisco IP Phone

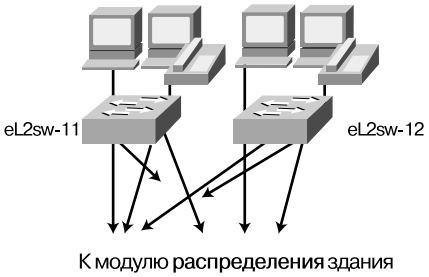


Рисунок 78. Модуль здания

EL2SW-11 и 12

Следующая конфигурация показывает некоторые настройки VLAN на коммутаторах Уровня 2, установленных в данном модуле. Заметим, что ненужные порты отключаются и настраиваются на несуществующую сеть VLAN. Транкинг также отключается на всех портах, кроме тех, к которым подключены IP-телефоны. На этих портах транкинг используется для разделения VLAN между IP-телефоном и рабочей станцией.

```
set vlan 5 2/5,2/17
set vlan 6 2/6,2/18
set vlan 99 2/34
set vlan 999 2/1-3,2/7-16,2/19-33
set port disable 2/7-33
set trunk 2/1-34 off
set trunk 2/4 on dot1q 1,5-8
```


Серверный модуль

Используемые продукты

- Коммутаторы Уровня 3 Cisco Catalyst 6500 Layer 3 switches
- Уровень распознавания атак Cisco Catalyst 6500 Intrusion Detection Module
- Cisco Call Manager
- CiscoSecure Host IDS

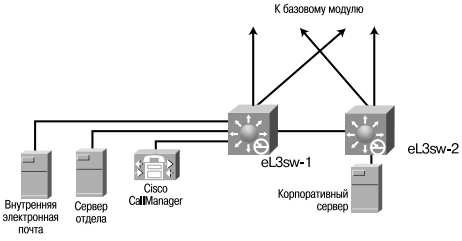


Рисунок 79. Серверный модуль

EL3SW-1 и 2

Следующая конфигурация определяет параметры частных VLAN на некоторых портах одной и той же сети VLAN. Эта конфигурация не позволяет внутреннему серверу электронной почты связываться с корпоративным сервером.

```
! CAT OS Config
!
#private vlans
set pvlan 11 437
set pvlan 11 437 3/3-4,3/14
set pvlan mapping 11 437 15/1
!
! MSFC Config
!
interface Vlan11
ip address 10.1.11.1 255.255.255.0
ip access-group 111 in
no ip redirects
```

Следующая конфигурация определяет параметры фильтрации на нескольких интерфейсах этого модуля, включая фильтрацию RFC 2827.

```
interface Vlan11
ip address 10.1.11.1 255.255.255.0
ip access-group 111 in
!
```

```
interface Vlan15
ip address 10.1.15.1 255.255.255.0
ip access-group 115 in
!
interface Vlan16
ip address 10.1.16.1 255.255.255.0
ip access-group 116 in
ip access-group 126 out
!
access-list 111 permit ip 10.1.11.0 0.0.0.255 any
access-list 111 deny ip any any log
access-list 115 permit ip 10.1.15.0 0.0.0.255 any
access-list 115 deny ip any any log
access-list 116 permit ip 10.1.16.0 0.0.0.255 10.1.7.0 0.0.0.255
access-list 116 permit ip 10.1.16.0 0.0.0.255 10.1.8.0 0.0.0.255
access-list 116 permit ip 10.1.16.0 0.0.0.255 10.1.11.0 0.0.0.255
access-list 116 deny ip any any log
access-list 126 permit ip 10.1.7.0 0.0.0.255 10.1.16.0 0.0.0.255
access-list 126 permit ip 10.1.8.0 0.0.0.255 10.1.16.0 0.0.0.255
access-list 126 permit ip 10.1.11.0 0.0.0.255 10.1.16.0 0.0.0.255
```

Следующая конфигурация определяет capture port для модуля Cat 6000 IDS:

```
#module 4 : 2-port Intrusion Detection System
set module name 4
set module enable 4
set vlan 1 4/1
set vlan 99 4/2
set port name 4/1 Sniff-4
set port name 4/2 CandC-4
set trunk 4/1 nonegotiate dot1q 1-1005,1025-4094
set security acl capture-ports 4/1
```

Периферийный распределительный модуль

Используемые продукты

- Коммутаторы Уровня 3 Cisco Catalyst 6500 Layer 3 Switch

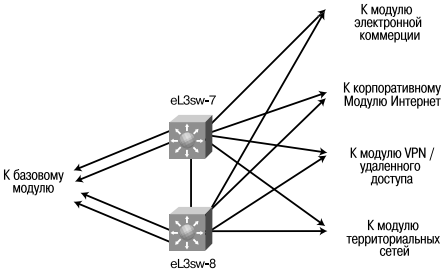


Рисунок 80. Периферийный распределительный модуль

Корпоративный модуль Интернет

Используемые продукты

- Межсетевой экран Cisco Secure PIX Firewall
- Сенсор CSIDS
- Коммутаторы Уровня 2 Catalyst 3500 Layer 2 switches
- Маршрутизатор Cisco 7100 IOS Router
- CiscoSecure Host IDS
- Сервер фильтрации URL Websense URL Filtering Server

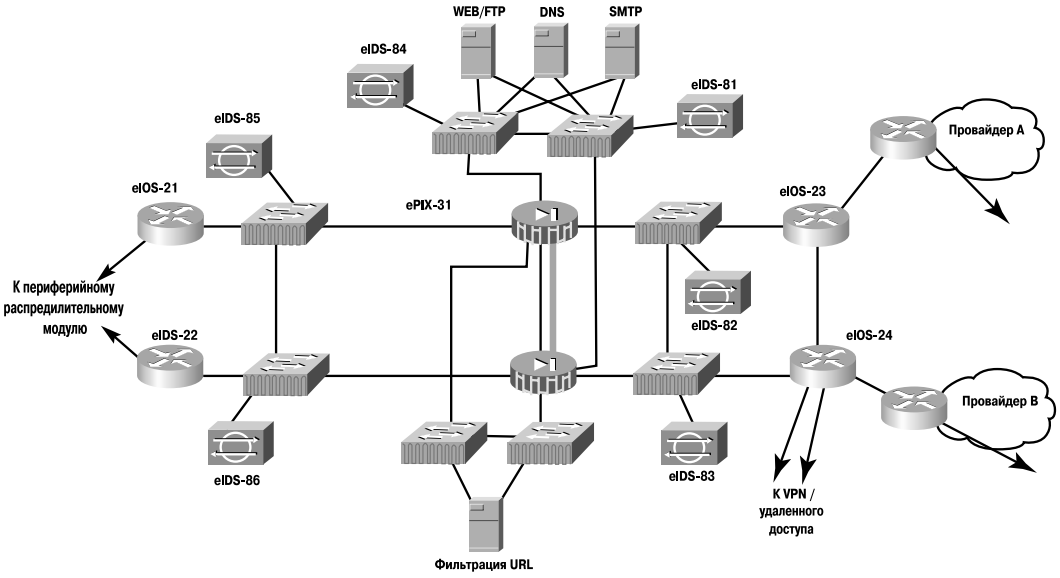


Рисунок 81. Корпоративный модуль Интернет

EPIX-31 и 33

Следующая конфигурация определяет детали контроля доступа на межсетевом экране PIX. Имя списка доступа определяет местонахождение входящего ACL. «In» означает «входящий», «Out» — «исходящий», «pss» означает сегмент общего доступа (DMZ), «url» — сегмент фильтрации содержания, а «mgmt» — интерфейс OOB.

```
access-list out deny ip any 192.168.254.0 255.255.255.0
access-list out deny ip any 192.168.253.0 255.255.255.0
access-list out permit icmp any any echo-reply
access-list out permit tcp any host 172.16.225.52 eq www
access-list out permit tcp any host 172.16.225.52 eq ftp
access-list out permit tcp any host 172.16.225.50 eq smtp
access-list out permit udp any host 172.16.225.51 eq domain
access-list out permit esp host 172.16.224.23 host 172.16.224.57
access-list out permit esp host 172.16.224.24 host 172.16.224.57
access-list out permit udp host 172.16.224.23 host 172.16.224.57 eq isakmp
access-list out permit udp host 172.16.224.24 host 172.16.224.57 eq isakmp
access-list in deny ip any 192.168.254.0 255.255.255.0
access-list in deny ip any 192.168.253.0 255.255.255.0
access-list in permit icmp any any echo
access-list in permit udp host 10.1.11.50 host 172.16.225.51 eq domain
access-list in permit tcp 10.0.0.0 255.0.0.0 host 172.16.225.52 eq www
access-list in permit tcp 10.0.0.0 255.0.0.0 host 10.1.103.50 eq 15871
access-list in permit tcp host 10.1.11.51 host 172.16.225.50 eq smtp
access-list in permit tcp host 10.1.11.51 host 172.16.225.50 eq 20389
access-list in permit tcp 10.0.0.0 255.0.0.0 host 172.16.225.52 eq ftp
access-list in deny ip any 172.16.225.0 255.255.255.0
access-list in permit ip 10.0.0.0 255.0.0.0 any
access-list in permit esp host 10.1.20.57 host 172.16.224.23
access-list in permit esp host 10.1.20.57 host 172.16.224.24
access-list in permit udp host 10.1.20.57 host 172.16.224.23 eq isakmp
access-list in permit udp host 10.1.20.57 host 172.16.224.24 eq isakmp
access-list pss deny ip any 192.168.254.0 255.255.255.0
access-list pss deny ip any 192.168.253.0 255.255.255.0
access-list pss permit tcp host 172.16.225.50 host 10.1.11.51 eq 20025
access-list pss permit tcp host 172.16.225.50 host 10.1.11.51 eq 20389
access-list pss deny ip 172.16.225.0 255.255.255.0 10.0.0.0 255.0.0.0
access-list pss permit tcp host 172.16.225.50 any eq smtp
access-list pss permit udp host 172.16.225.51 any eq domain
access-list url permit udp host 10.1.103.50 host 172.16.225.51 eq domain
access-list url permit ip any any
access-list mgmt permit icmp 192.168.253.0 255.255.255.0 any
```


EIOS-23 и 24

Эта конфигурация определяет детали команд протокола HSRP (hot standby router protocol) на многих маршрутизаторах, использующих HSRP для обеспечения отказоустойчивости.

```
interface FastEthernet0/0
ip address 172.16.226.23 255.255.255.0
standby 2 timers 5 15
standby 2 priority 110 preempt delay 2
standby 2 authentication k&>9NG@6
standby 2 ip 172.16.226.100
standby 2 track ATM4/0 50
```

Следующая конфигурация устанавливает параметры защищенного сетевого управления по основному каналу связи с модулем управления:

```
crypto isakmp policy 1
encr 3des
authentication pre-share
group 2
crypto isakmp key A%Xr)7,_) address 172.16.224.57
!
crypto ipsec transform-set vpn_module_mgmt esp-3des esp-sha-hmac
!
crypto map mgmt1 100 ipsec-isakmp
set peer 172.16.224.57
set transform-set vpn_module_mgmt
match address 103
access-list 103 permit ip host 172.16.224.23 192.168.253.0 0.0.0.255
access-list 103 permit udp host 172.16.224.23 192.168.254.0 0.0.0.255
```

ACL для трафика, поступающего из корпоративной сети:

```
access-list 112 permit udp host 172.16.224.57 host 172.16.224.23 eq isakmp
```

```
access-list 112 permit esp host 172.16.224.57 host 172.16.224.23
access-list 112 permit tcp 192.168.253.0 0.0.0.255 host 172.16.224.23 established
access-list 112 permit udp 192.168.253.0 0.0.0.255 host 172.16.224.23 gt 1023
access-list 112 permit tcp 192.168.253.0 0.0.0.255 host 172.16.224.23 eq telnet
access-list 112 permit udp host 192.168.253.51 host 172.16.224.23 eq snmp
access-list 112 permit udp host 192.168.254.57 host 172.16.224.23 eq ntp
access-list 112 permit icmp any any
access-list 112 deny ip any host 172.16.224.23 log
access-list 112 deny ip any host 172.16.226.23 log
access-list 112 deny ip any host 172.16.145.23 log
access-list 112 permit ip 172.16.224.0 0.0.0.255 any
access-list 112 permit ip 172.16.225.0 0.0.0.255 any
```

ACL для трафика, поступающего от провайдера (ISP). Заметим, что фильтрация RFC 1918 является неполной, так как в лабораторных условиях эти адреса используются в качестве производственных. В реальных сетях нужно использовать полную фильтрацию RFC 1918.

```
access-list 150 deny ip 10.0.0.0 0.255.255.255 any
access-list 150 deny ip 192.168.0.0 0.0.255.255 any
access-list 150 deny ip 172.16.224.0 0.0.7.255 any
access-list 150 permit ip any 172.16.224.0 0.0.7.255
access-list 150 permit ip any 172.16.145.0 0.0.0.255
access-list 150 permit esp any 172.16.226.0 0.0.0.255 fragments
access-list 150 deny ip any any fragments
access-list 150 deny ip any any log
```

Следующая фильтрация предназначена для исходящего трафика, который поступает в модуль VPN/удаленного доступа. Заметим, что здесь разрешаются только IKE и ESP:

```
access-list 160 permit esp any host 172.16.226.27
access-list 160 permit esp any host 172.16.226.28
access-list 160 permit esp any host 172.16.226.48
access-list 160 permit udp any host 172.16.226.27 eq isakmp
access-list 160 permit udp any host 172.16.226.28 eq isakmp
access-list 160 permit udp any host 172.16.226.48 eq isakmp
access-list 160 deny ip any any log
```

Catalyst 3500XL Private VLANs

Эта конфигурация определяет параметры частных сетей VLAN в сегменте общего доступа:

```
interface FastEthernet0/1
port protected
!
interface FastEthernet0/2
port protected
```


Модуль VPN / удаленного доступа

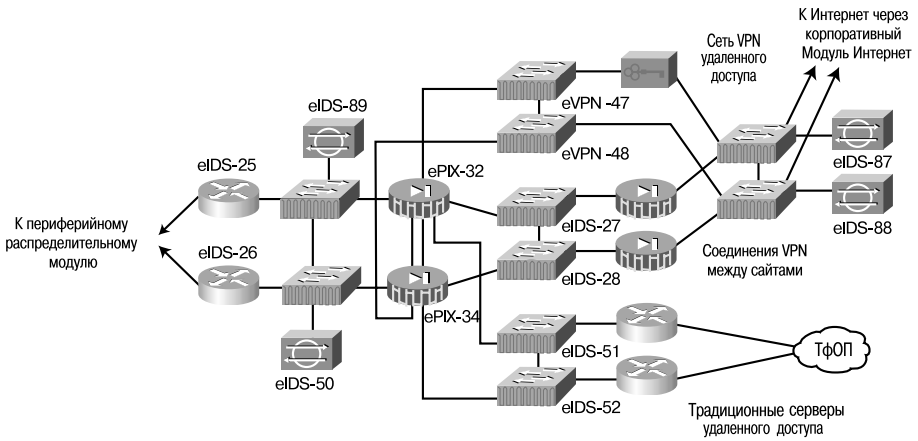


Рисунок 82. Модуль VPN / удаленного доступа

Используемые продукты

- Межсетевой экран Cisco Secure PIX Firewall
- Сенсор CSIDS
- Коммутаторы Уровня 2 Catalyst 3500 Layer 2 switches
- Маршрутизатор Cisco 7100 IOS Router
- Концентратор Cisco VPN 3060 Concentrator
- Сервер доступа Cisco IOS Access Server
- CiscoSecure Host IDS

- Сервер фильтрации Websense URL Filtering Server

EPIX-32 и 34

Эта конфигурация определяет детали контроля доступа на межсетевом экране PIX. Имя списка доступа определяет местонахождение входящего ACL. «In» означает «входящий», «Out» — «трафик между сайтами VPN», «dun» означает модемный доступ через ТфОП, «ra» — VPN с удаленным доступом, а «mgmt» — интерфейс OOB.

```
access-list in deny ip any 192.168.253.0 255.255.255.0
access-list in deny ip any 192.168.254.0 255.255.255.0
access-list in permit icmp any any
access-list in permit tcp 10.0.0.0 255.0.0.0 10.0.0.0 255.0.0.0 eq smtp
access-list in permit tcp 10.0.0.0 255.0.0.0 10.0.0.0 255.0.0.0 eq pop3
access-list in permit tcp 10.0.0.0 255.0.0.0 10.0.0.0 255.0.0.0 eq www
access-list in permit tcp 10.0.0.0 255.0.0.0 10.0.0.0 255.0.0.0 eq ftp
access-list in permit udp 10.0.0.0 255.0.0.0 10.0.0.0 255.0.0.0 eq netbios-ns
access-list in permit udp 10.0.0.0 255.0.0.0 10.0.0.0 255.0.0.0 eq netbios-dgm
access-list in permit udp 10.0.0.0 255.0.0.0 10.0.0.0 255.0.0.0 eq domain
access-list out deny ip any 192.168.253.0 255.255.255.0
access-list out deny ip any 192.168.254.0 255.255.255.0
access-list out permit icmp any any
access-list out permit tcp 10.0.0.0 255.0.0.0 10.0.0.0 255.0.0.0 eq smtp
access-list out permit tcp 10.0.0.0 255.0.0.0 10.0.0.0 255.0.0.0 eq pop3
access-list out permit tcp 10.0.0.0 255.0.0.0 10.0.0.0 255.0.0.0 eq www
access-list out permit tcp 10.0.0.0 255.0.0.0 10.0.0.0 255.0.0.0 eq ftp
access-list out permit udp 10.0.0.0 255.0.0.0 10.0.0.0 255.0.0.0 eq netbios-ns
access-list out permit udp 10.0.0.0 255.0.0.0 10.0.0.0 255.0.0.0 eq netbios-dgm
access-list out permit udp 10.0.0.0 255.0.0.0 10.0.0.0 255.0.0.0 eq domain
access-list out permit tcp 10.0.0.0 255.0.0.0 172.16.255.0 255.255.255.0 eq www
access-list out permit tcp 10.0.0.0 255.0.0.0 172.16.255.0 255.255.255.0 eq ftp
access-list ra deny ip any 192.168.253.0 255.255.255.0
access-list ra deny ip any 192.168.254.0 255.255.255.0
access-list ra permit icmp any any
access-list ra permit tcp 10.1.198.0 255.255.254.0 10.0.0.0 255.0.0.0 eq smtp
access-list ra permit tcp 10.1.198.0 255.255.254.0 10.0.0.0 255.0.0.0 eq pop3
access-list ra permit tcp 10.1.198.0 255.255.254.0 10.0.0.0 255.0.0.0 eq www
access-list ra permit tcp 10.1.198.0 255.255.254.0 10.0.0.0 255.0.0.0 eq ftp
access-list ra permit udp 10.1.198.0 255.255.254.0 10.0.0.0 255.0.0.0 eq netbios-ns
access-list ra permit udp 10.1.198.0 255.255.254.0 10.0.0.0 255.0.0.0 eq netbios-dgm
access-list ra permit udp 10.1.198.0 255.255.254.0 10.0.0.0 255.0.0.0 eq domain
access-list ra deny ip 10.1.198.0 255.255.254.0 10.0.0.0 255.0.0.0
access-list ra permit tcp 10.1.198.0 255.255.254.0 172.16.225.0 255.255.255.0 eq www
access-list ra permit tcp 10.1.198.0 255.255.254.0 172.16.225.0 255.255.255.0 eq ftp
access-list ra deny ip 10.1.198.0 255.255.254.0 172.16.224.0 255.255.248.0
access-list ra permit ip 10.1.198.0 255.255.254.0 any
access-list dun deny ip any 192.168.253.0 255.255.255.0
access-list dun deny ip any 192.168.254.0 255.255.255.0
access-list dun permit icmp any any
access-list dun permit tcp 10.1.196.0 255.255.254.0 10.0.0.0 255.0.0.0 eq smtp
access-list dun permit tcp 10.1.196.0 255.255.254.0 10.0.0.0 255.0.0.0 eq pop3
access-list dun permit tcp 10.1.196.0 255.255.254.0 10.0.0.0 255.0.0.0 eq www
access-list dun permit tcp 10.1.196.0 255.255.254.0 10.0.0.0 255.0.0.0 eq ftp
access-list dun permit udp 10.1.196.0 255.255.254.0 10.0.0.0 255.0.0.0 eq netbios-ns
access-list dun permit udp 10.1.196.0 255.255.254.0 10.0.0.0 255.0.0.0 eq netbios-dgm
access-list dun permit udp 10.1.196.0 255.255.254.0 10.0.0.0 255.0.0.0 eq domain
access-list dun deny ip 10.1.196.0 255.255.254.0 10.0.0.0 255.0.0.0
access-list dun permit tcp 10.1.196.0 255.255.255.0 172.16.225.0 255.255.255.0 eq www
access-list dun permit tcp 10.1.196.0 255.255.255.0 172.16.225.0 255.255.255.0 eq ftp
access-list dun deny ip 10.1.196.0 255.255.254.0 172.16.224.0 255.255.248.0
access-list dun permit ip 10.1.196.0 255.255.254.0 any
access-list mgmt permit icmp 192.168.253.0 255.255.255.0 any
```

Следующая конфигурация показывает детали трансляций NAT, необходимых для выхода трафика VPN из корпоративного Интернет-модуля в Интернет:

```
 static (inside,ravpn) 128.0.0.0 128.0.0.0 netmask 128.0.0.0 0 0
static (inside,ravpn) 64.0.0.0 64.0.0.0 netmask 192.0.0.0 0 0
static (inside,ravpn) 32.0.0.0 32.0.0.0 netmask 224.0.0.0 0 0
static (inside,ravpn) 16.0.0.0 16.0.0.0 netmask 240.0.0.0 0 0
static (inside,ravpn) 8.0.0.0 8.0.0.0 netmask 248.0.0.0 0 0
static (inside,ravpn) 4.0.0.0 4.0.0.0 netmask 252.0.0.0 0 0
static (inside,ravpn) 2.0.0.0 2.0.0.0 netmask 254.0.0.0 0 0
static (inside,ravpn) 1.0.0.0 1.0.0.0 netmask 255.0.0.0 0 0
```

EIOS-27 и 28

Здесь показаны детали конфигурации шифрования для виртуальных частных сетей (VPN), обеспечивающих связь между сайтами:

```
!
! Basic Crypto Information
!
crypto isakmp policy 1
encr 3des
authentication pre-share
group 2
crypto isakmp key 7Q!r$y$+xE address 172.16.132.2
crypto isakmp key 52TH^m&^qu address 172.16.131.2
!
!
crypto ipsec transform-set smbranch esp-3des esp-sha-hmac
mode transport
!
crypto map secure1 100 ipsec-isakmp
set peer 172.16.132.2
set transform-set smbranch
match address 105
crypto map secure1 300 ipsec-isakmp
set peer 172.16.131.2
set transform-set smbranch
match address 107
!
!
! GRE Tunnel Information
!
interface Tunnel0
ip address 10.1.249.27 255.255.255.0
tunnel source 172.16.226.27
tunnel destination 172.16.132.2
crypto map secure1
!
interface Tunnel1
ip address 10.1.247.27 255.255.255.0
tunnel source 172.16.226.27
tunnel destination 172.16.131.2
crypto map secure1
!
!
! EIGRP Routing to keep links up
!
router eigrp 1
redistribute static
passive-interface FastEthernet0/1
passive-interface FastEthernet4/0
network 10.0.0.0
distribute-list 2 out
distribute-list 2 in
!
! Crypto ACLs
!
access-list 105 permit gre host 172.16.226.27 host 172.16.132.2
access-list 107 permit gre host 172.16.226.27 host 172.16.131.2
!
! Inbound ACLs from Internet
!
access-list 110 permit udp 172.16.0.0 0.0.255.255 host 172.16.226.27 eq isakmp
access-list 110 permit esp 172.16.0.0 0.0.255.255 host 172.16.226.27
access-list 110 permit gre 172.16.0.0 0.0.255.255 host 172.16.226.27
access-list 110 deny ip any any log
```

Модуль территориальных сетей (WAN)

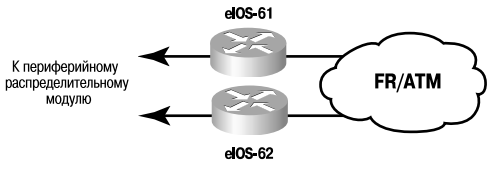


Рисунок 83. Модуль территориальных сетей

Используемые продукты

- Маршрутизатор Cisco 3640 IOS Router

EIOS-61

Эта конфигурация показывает детали контроля доступа на маршрутизаторах модуля территориальных сетей:

```
!
! Inbound from the WAN
!
access-list 110 deny ip any 192.168.253.0 0.0.0.255 log
```

```
access-list 110 deny ip any 192.168.254.0 0.0.0.255 log
access-list 110 permit ospf any any
access-list 110 permit ip 10.2.0.0 0.0.255.255 10.1.0.0 0.0.255.255
access-list 110 permit ip 10.2.0.0 0.0.255.255 10.3.0.0 0.0.255.255
access-list 110 permit ip 10.2.0.0 0.0.255.255 10.4.0.0 0.0.255.255
access-list 110 permit ip 10.2.0.0 0.0.255.255 172.16.224.0 0.0.7.255
access-list 110 deny ip any any log
!
! Inbound from the Campus
!
access-list 111 deny ip any 192.168.253.0 0.0.0.255 log
access-list 111 deny ip any 192.168.254.0 0.0.0.255 log
access-list 111 permit ospf any any
access-list 111 permit ip 10.1.0.0 0.0.255.255 10.2.0.0 0.0.255.255
access-list 111 permit ip 10.3.0.0 0.0.255.255 10.2.0.0 0.0.255.255
access-list 111 permit ip 10.4.0.0 0.0.255.255 10.2.0.0 0.0.255.255
access-list 111 permit ip 172.16.224.0 0.0.7.255 10.2.0.0 0.0.255.255
access-list 111 deny ip any any log
```

Сеть малого предприятия

Ниже приведены примеры конфигурации для сети малого предприятия.

Модуль Интернет

Используемые продукты

- Коммутатор уровня 2 Cisco Catalyst (sCAT-1)
- Маршрутизатор Cisco IOS Router с поддержкой протокола IPsec (sIOS-1)
- Межсетевой экран Cisco Secure PIX Firewall (sPIX-1)
- Система обнаружения вторжений CiscoSecure Host IDS

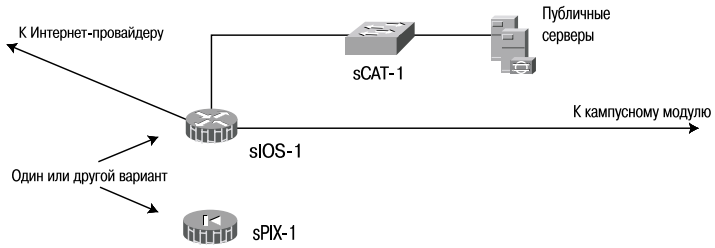


Рисунок 84. Дизайн модуля Интернет

sIOS-1

Эта конфигурация показывает списки доступа на пограничном маршрутизаторе предприятия, контролирующие входящий и исходящий трафики.

Основные команды встроенной в IOS системы обнаружения вторжений. Для отчетов используется протокол syslog.

```
ip audit attack action alarm drop reset
ip audit notify log
ip audit name alarm1 info action alarm
ip audit name alarm1 attack action alarm drop
```

Конфигурация IPSec для подключения удаленных подразделений:

```
crypto isakmp policy 1
encr 3des
authentication pre-share
group 2
crypto isakmp key 7Q!r$y$+xE address 172.16.128.2
crypto isakmp key 7Q!r$y$+xE address 172.16.128.5
!
!
crypto ipsec transform-set remote1 esp-3des esp-sha-hmac
!
crypto map ent1 30 ipsec-isakmp
set peer 172.16.128.2
set transform-set remote1
match address 107
crypto map ent1 40 ipsec-isakmp
set peer 172.16.128.5
set transform-set remote1
match address 108
```

Списки доступа указывают, что как пользовательский трафик, так и трафик управления должны быть зашифрованы.

```
access-list 107 permit ip 10.4.0.0 0.0.255.255 10.5.0.0 0.0.255.255
access-list 107 permit ip host 10.4.1.253 host 172.16.128.2
access-list 108 permit ip 10.4.0.0 0.0.255.255 10.6.0.0 0.0.255.255
access-list 108 permit ip host 10.4.1.253 host 172.16.128.5
```

Настройки внутреннего интерфейса маршрутизатора, включая трансляцию адресов, межсетевой экран и обнаружение вторжений.

```
interface FastEthernet0/0
```

```
description Inside Interface
ip address 10.4.1.1 255.255.255.0
ip access-group 109 in
ip nat inside
ip inspect smbranch_fw in
ip audit alarm1 in
```

Разрешение на использование протокола ICMP из внутренней сети:

```
access-list 109 permit icmp any any echo
```

Разрешение взаимодействия внутреннего сервера DNS с публичным сервером DNS:

```
access-list 109 permit udp host 10.4.1.201 host 10.4.2.50 eq domain
```

Разрешение внутренним пользователям доступа к внешним сервисам, таким как HTTP, SSL и FTP:

```
access-list 109 permit tcp 10.4.0.0 0.0.255.255 host 10.4.2.50 eq www
access-list 109 permit tcp 10.4.0.0 0.0.255.255 host 10.4.2.50 eq 443
access-list 109 permit tcp 10.4.0.0 0.0.255.255 host 10.4.2.50 eq ftp
```

Разрешение взаимодействия внутреннего почтового сервера с внешним:

```
access-list 109 permit tcp host 10.4.1.201 host 10.4.2.50 eq smtp
```

Доступ по протоколу telnet от станции управления к коммутатору:

```
access-list 109 permit tcp host 10.4.1.253 host 10.4.2.4 eq telnet
```

Запрещение всех остальных типов доступа и протоколов:

```
access-list 109 deny ip any 10.4.2.0 0.0.0.255
```

Разрешение синхронизации сетевого времени между маршрутизатором sIOS-1 и коммутатором sCAT-2:

```
access-list 109 permit udp host 10.4.1.4 host 10.4.1.1 eq ntp
```

Разрешение доступа к маршрутизатору от станции управления по протоколу SSH:

```
access-list 109 permit tcp host 10.4.1.253 host 10.4.1.1 eq 22
```

Разрешение установленных соединений между станцией управления и маршрутизатором:

```
access-list 109 permit tcp host 10.4.1.253 eq tacacs host 10.4.1.1 established
```

Разрешение протокола TFTP между станцией управления и маршрутизатором:

```
access-list 109 permit udp host 10.4.1.253 gt 1023 host 10.4.1.1 gt 1023
```


Блокировать все остальные типы доступа к маршрутизатору из внутренней сети:

```
access-list 109 deny ip 10.4.0.0 0.0.255.255 host 10.4.1.1
access-list 109 deny ip 10.4.0.0 0.0.255.255 host 172.16.132.2
```

Разрешить выход всем остальным внутренним устройствам в Интернет:

```
access-list 109 permit ip 10.4.0.0 0.0.255.255 any
```

Блокировать весь остальной трафик:

```
access-list 109 deny ip any any log
```

Настройки публичного интерфейса маршрутизатора, включая функции трансляции адресов, системы обнаружения вторжений и межсетевого экрана.

```
interface FastEthernet0/1
description DMZ Interface
ip address 10.4.2.1 255.255.255.0
ip access-group 105 in
no ip redirects
ip nat inside
ip inspect smbranch_fw in
ip audit alarm1 in
```

Разрешение синхронизации времени между коммутатором sCAT-1 и маршрутизатором sIOS-1:

```
access-list 105 permit udp host 10.4.2.4 host 10.4.2.1 eq ntp
```

Взаимодействие по протоколам TACACS+, TFTP и syslog между коммутатором sCAT-1 и станцией управления:

```
access-list 105 permit tcp host 10.4.2.4 host 10.4.1.253 eq tacacs
access-list 105 permit udp host 10.4.2.4 host 10.4.1.253 eq tftp
access-list 105 permit udp host 10.4.2.4 host 10.4.1.253 eq syslog
```

Разрешение передачи управляющего трафика хостовой системы обнаружения вторжений от публичных серверов к станции управления:

```
access-list 105 permit tcp host 10.4.2.50 host 10.4.1.253 eq 5000
```

Разрешение внешнему почтовому серверу посылать почту на внутренний почтовый сервер:

```
access-list 105 permit tcp host 10.4.2.50 host 10.4.1.201 eq smtp
```

Запретить все остальные типы соединений из зоны публичных серверов во внутреннюю сеть:

```
access-list 105 deny ip any 10.4.0.0 0.0.255.255
```

Разрешить почтовый и DNS трафик из зоны публичных серверов:

```
access-list 105 permit tcp host 10.4.2.50 any eq smtp
access-list 105 permit udp host 10.4.2.50 any eq domain
```

Запретить весь остальной трафик и вести журнал учета:

```
access-list 105 deny ip any any log
```

Настройки внешнего интерфейса маршрутизатора, включая трансляцию адресов, обнаружение вторжений, межсетевой экран и ВЧС.

```
interface Serial1/0
description Outside Interface
ip address 172.16.132.2 255.255.255.0
ip access-group 103 in
no ip redirects
ip nat outside
ip inspect smbranch_fw in
ip audit alarm1 in
crypto map ent1
```

Разрешить трафик от удаленных подразделений:

```
access-list 103 permit ip 10.5.0.0 0.0.255.255 10.4.0.0 0.0.255.255
access-list 103 permit ip 10.6.0.0 0.0.255.255 10.4.0.0 0.0.255.255
```

Фильтрование по RFC 1918. Примечание: сеть 172.16.x.x не включена в список, потому что использовалась как сеть Интернет-провайдера в данном примере:

```
access-list 103 deny ip 10.0.0.0 0.255.255.255 any
access-list 103 deny ip 192.168.0.0 0.0.255.255 any
```

Разрешить пакеты ICMP echo-reply из сети провайдера:

```
access-list 103 permit icmp any 172.16.132.0 0.0.0.255 echo-reply
```


Разрешить пакеты ICMP, необходимые для работы path MTU discovery (PMTUD):

```
access-list 103 permit icmp any 172.16.132.0 0.0.0.255 unreachable
```

Разрешить трафик ВЧС от удаленных подразделений:

```
access-list 103 permit esp host 172.16.128.2 host 172.16.132.2
access-list 103 permit udp host 172.16.128.2 host 172.16.132.2 eq isakmp
access-list 103 permit esp host 172.16.128.5 host 172.16.132.2
access-list 103 permit udp host 172.16.128.5 host 172.16.132.2 eq isakmp
```

Разрешить трафик управления удаленными подразделениями:

```
access-list 103 permit tcp host 172.16.128.2 host 10.4.1.253 eq tacacs
access-list 103 permit udp host 172.16.128.2 host 10.4.1.253 eq syslog
access-list 103 permit udp host 172.16.128.2 host 10.4.1.253 eq tftp
access-list 103 permit tcp host 172.16.128.5 host 10.4.1.253 eq tacacs
access-list 103 permit udp host 172.16.128.5 host 10.4.1.253 eq syslog

access-list 103 permit udp host 172.16.128.5 host 10.4.1.253 eq tftp
```

Разрешить доступ к публичному сегменту по протоколам DNS, FTP, HTTP, SSL и почте:

```
access-list 103 permit udp any host 172.16.132.50 eq domain
access-list 103 permit tcp any host 172.16.132.50 eq ftp
access-list 103 permit tcp any host 172.16.132.50 eq www
access-list 103 permit tcp any host 172.16.132.50 eq 443
access-list 103 permit tcp any host 172.16.132.50 eq smtp
```

Запретить весь остальной трафик и вести его учет:

```
access-list 103 deny ip any any log
```

Настройка трансляции сетевых адресов. Создание пула публичных адресов, которые будут использоваться внутренними устройствами при выходе в Интернет.

```
ip nat pool small_pool 172.16.132.101 172.16.132.150 netmask 255.255.255.0
ip nat inside source route-map nat_internet pool small_pool
```

Статическая трансляция сетевых адресов для публичных серверов, доступных из Интернет.

```
ip nat inside source static 10.4.2.50 172.16.132.50
!
```

```
route-map nat_internet permit 10
match ip address 104
```

Не использовать трансляцию адресов для взаимодействия внутренних устройств между собой или трафика управления:

```
access-list 104 deny ip 10.4.0.0 0.0.255.255 10.0.0.0 0.255.255.255
access-list 104 deny ip host 10.4.1.253 host 172.16.128.2
access-list 104 deny ip host 10.4.1.253 host 172.16.128.5
access-list 104 permit ip 10.4.1.0 0.0.0.255 any
!
```

Изменения в том случае, если малое предприятие является подразделением крупного предприятия

Приведенная ниже конфигурация отображает те изменения, которые надо сделать для подключения малой сети к основной сети предприятия, используя резервированное подключение ВЧС.

Настройки политик шифрования.

```
crypto isakmp policy 1
encr 3des
authentication pre-share

group 2
crypto isakmp key 7Q!r$y$+xE address 172.16.226.28
crypto isakmp key 7Q!r$y$+xE address 172.16.226.27
!
!
crypto ipsec transform-set 3dessha esp-3des esp-sha-hmac
mode transport
!
crypto map ent1 10 ipsec-isakmp
set peer 172.16.226.28
set transform-set 3dessha
match address 101
crypto map ent1 20 ipsec-isakmp
set peer 172.16.226.27
set transform-set 3dessha
match address 102
!
access-list 101 permit gre host 172.16.132.2 host 172.16.226.28
access-list 102 permit gre host 172.16.132.2 host 172.16.226.27
```

Настройки туннельного протокола GRE.

```
interface Tunnel0
bandwidth 8
ip address 10.1.249.2 255.255.255.0
tunnel source 172.16.132.2
tunnel destination 172.16.226.27
crypto map ent1
!
interface Tunnel1
ip address 10.1.248.2 255.255.255.0
tunnel source 172.16.132.2
tunnel destination 172.16.226.28
crypto map ent1
```

Привязка ВЧС к физическому интерфейсу.

```
interface Serial1/0
ip address 172.16.132.2 255.255.255.0
ip access-group 103 in
crypto map ent1
```

Список доступа должен быть модифицирован для пропуска трафика ВЧС IPsec и GRE от головного офиса.

```
access-list 103 permit gre host 172.16.226.28 host 172.16.132.2
access-list 103 permit gre host 172.16.226.27 host 172.16.132.2
access-list 103 permit esp host 172.16.226.27 host 172.16.132.2
access-list 103 permit udp host 172.16.226.27 host 172.16.132.2 eq isakmp

access-list 103 permit esp host 172.16.226.28 host 172.16.132.2
access-list 103 permit udp host 172.16.226.28 host 172.16.132.2 eq isakmp
```

Вся конфигурация, связанная с другими удаленными подразделениями, должна быть удалена.

```
access-list 103 deny ip 10.0.0.0 0.255.255.255 any
access-list 103 deny ip 192.168.0.0 0.0.255.255 any
access-list 103 permit udp any host 172.16.132.50 eq domain
access-list 103 permit tcp any host 172.16.132.50 eq ftp
access-list 103 permit tcp any host 172.16.132.50 eq www
access-list 103 permit tcp any host 172.16.132.50 eq 443
```

```
access-list 103 permit tcp any host 172.16.132.50 eq smtp
access-list 103 permit icmp any 172.16.132.0 0.0.0.255 echo-reply
access-list 103 permit icmp any 172.16.132.0 0.0.0.255 unreachable
access-list 103 deny ip any any log
```

Небольшие изменения в других списках доступа тоже требуются, но не показаны.

sPIX-1

Приведенная ниже конфигурация детализирует настройки списков доступа и ВЧС, когда в качестве головного устройства в малой сети используется межсетевой экран PIX Firewall. Этот межсетевой экран настраивается для взаимодействия с удаленными подразделениями и доступа по ВЧС удаленных пользователей.

Настройки внешнего интерфейса.

```
ip address outside 172.16.144.3 255.255.255.0
access-group 103 in interface outside
```

Разрешение зашифрованного трафика удаленных подразделений и пользователей:

```
access-list 103 permit ip 10.5.0.0 255.255.0.0 10.4.0.0 255.255.0.0
access-list 103 permit ip 10.6.0.0 255.255.0.0 10.4.0.0 255.255.0.0
access-list 103 permit ip 10.4.3.0 255.255.255.0 10.4.0.0 255.255.0.0
```

Фильтрование в соответствии с RFC 1918. Примечание: сеть 172.16.x.x не включена в список, потому что использовалась как сеть Интернет-провайдера в данном примере.

```
access-list 103 deny ip 10.0.0.0 255.0.0.0 any
access-list 103 deny ip 192.168.0.0 255.255.0.0 any
```

Разрешить доступ к публичным серверам для приложений DNS, FTP, HTTP SSL и почты:

```
access-list 103 permit udp any host 172.16.144.50 eq domain
access-list 103 permit tcp any host 172.16.144.50 eq ftp
access-list 103 permit tcp any host 172.16.144.50 eq www
access-list 103 permit tcp any host 172.16.144.50 eq 443
access-list 103 permit tcp any host 172.16.144.50 eq smtp
```

Разрешить ответные пакеты ICMP на инициированные из внутренней сети запросы:

```
access-list 103 permit icmp any 172.16.144.0 255.255.255.0 echo-reply
```

Разрешить пакеты ICMP, необходимые для работы path MTU discovery (PMTUD):

```
access-list 103 permit icmp any 172.16.144.0 255.255.255.0 unreachable
```

Разрешить протоколы управления syslog, TFTP и TACACS+ от удаленных подразделений:

```
access-list 103 permit udp host 172.16.128.2 host 172.16.144.51 eq syslog
access-list 103 permit udp host 172.16.128.2 host 172.16.144.51 eq tftp
access-list 103 permit tcp host 172.16.128.2 host 172.16.144.51 eq tacacs
access-list 103 permit udp host 172.16.128.5 host 172.16.144.51 eq syslog
access-list 103 permit udp host 172.16.128.5 host 172.16.144.51 eq tftp
access-list 103 permit tcp host 172.16.128.5 host 172.16.144.51 eq tacacs
```

Настройки внутреннего интерфейса.

```
ip address inside 10.4.1.1 255.255.255.0
access-group 109 in interface inside
```

Разрешить ICMP echo от внутренних устройств:

```
access-list 109 permit icmp any any echo
```

Разрешить взаимодействие внешнего сервера DNS и внешнего почтового сервера с соответствующими внутренними серверами:

```
access-list 109 permit udp host 10.4.1.201 host 10.4.2.50 eq domain
access-list 109 permit tcp host 10.4.1.201 host 10.4.2.50 eq smtp
```

Разрешить доступ от внутренних устройств к публичным серверам по протоколам HTTP, FTP и SSL:

```
access-list 109 permit tcp 10.4.0.0 255.255.0.0 host 10.4.2.50 eq www
access-list 109 permit tcp 10.4.0.0 255.255.0.0 host 10.4.2.50 eq ftp
access-list 109 permit tcp 10.4.0.0 255.255.0.0 host 10.4.2.50 eq 443
```

Разрешить доступ по протоколу Telnet от станции управления к коммутатору sCAT-1:

```
access-list 109 permit tcp host 10.4.1.253 host 10.4.2.4 eq telnet
```

Блокировать весь остальной доступ в публичный сегмент:

```
access-list 109 deny ip any 10.4.2.0 255.255.255.0
```

Разрешить выход из внутренней сети в Интернет:

```
access-list 109 permit ip 10.4.0.0 255.255.0.0 any
```

Настройки публичного (DMZ) интерфейса.

```
ip address pss 10.4.2.1 255.255.255.0
access-group 105 in interface pss
```

Разрешить передачу пакетов ICMP echo-reply через межсетевой экран:

```
access-list 105 permit icmp 10.4.2.0 255.255.255.0 10.4.1.0 255.255.255.0 echo-reply
```

Разрешить доступ по протоколам TACACS+, TFTP и syslog от коммутатора sCAT-1 на станцию управления:

```
access-list 105 permit tcp host 10.4.2.4 host 10.4.1.253 eq tacacs
access-list 105 permit udp host 10.4.2.4 host 10.4.1.253 eq tftp
access-list 105 permit udp host 10.4.2.4 host 10.4.1.253 eq syslog
```

Разрешить трафик управления от хостовых систем обнаружения вторжений, установленных на публичных серверах, к станции управления:

```
access-list 105 permit tcp host 10.4.2.50 host 10.4.1.253 eq 5000
```

Разрешить взаимодействие между публичным и внутренним почтовыми серверами:

```
access-list 105 permit tcp host 10.4.2.50 host 10.4.1.201 eq smtp
```

Блокировать весь остальной доступ из этого сегмента во внутреннюю сеть:

```
access-list 105 deny ip any 10.4.0.0 255.255.0.0
```

Разрешить доступ от публичных серверов в Интернет для почты и службы имен (DNS):

```
access-list 105 permit tcp host 10.4.2.50 any eq smtp
access-list 105 permit udp host 10.4.2.50 any eq domain
```

Настройки функций обнаружения вторжений.

```
ip audit name full info action alarm
ip audit name fullb attack action alarm drop
ip audit interface outside full
ip audit interface outside fullb
ip audit interface inside full
ip audit interface inside fullb
ip audit interface pss full
ip audit interface pss fullb
```

Настройка трансляции сетевых адресов. Создание пула публичных адресов, которые будут использоваться внутренними устройствами при выходе в Интернет.

```
global (outside) 1 172.16.144.201-172.16.144.220
!
nat (inside) 0 access-list nonat
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
nat (pss) 0 access-list nonat
```

Настройка статической трансляции сетевых адресов для публичных серверов, доступных из Интернет.

```
static (pss,outside) 172.16.144.50 10.4.2.50 netmask 255.255.255.255 0 0
!
static (inside,pss) 10.4.1.253 10.4.1.253 netmask 255.255.255.255 0 0
static (inside,pss) 10.4.1.201 10.4.1.201 netmask 255.255.255.255 0 0
static (inside,outside) 172.16.144.51 10.4.1.253 netmask 255.255.255.255 0 0
```

Список доступа nonat определяет, для каких адресов использовать трансляцию.

```
access-list nonat permit ip 10.4.0.0 255.255.0.0 10.5.0.0 255.255.0.0
access-list nonat permit ip 10.4.0.0 255.255.0.0 10.6.0.0 255.255.0.0
access-list nonat permit ip 10.4.1.0 255.255.255.0 10.4.3.0 255.255.255.0
access-list nonat permit ip 10.4.2.0 255.255.255.0 10.4.3.0 255.255.255.0
access-list nonat permit ip 10.4.1.0 255.255.255.0 10.4.2.0 255.255.255.0
```

Приведенные ниже настройки ВЧС используются для взаимодействия с удаленными подразделениями.

```
no sysopt route dnat
crypto ipsec transform-set 3dessha esp-3des esp-sha-hmac
crypto ipsec transform-set remote1 esp-3des esp-sha-hmac
crypto dynamic-map vpnuser 20 set transform-set remote1
crypto map ent1 30 ipsec-isakmp
crypto map ent1 30 match address 107
crypto map ent1 30 set peer 172.16.128.2
crypto map ent1 30 set transform-set remote1
crypto map ent1 40 ipsec-isakmp
crypto map ent1 40 match address 108
crypto map ent1 40 set peer 172.16.128.5
```

```
crypto map ent1 40 set transform-set remote1
crypto map ent1 50 ipsec-isakmp dynamic vpnuser
crypto map ent1 client configuration address initiate
crypto map ent1 client authentication vpnauth
crypto map ent1 interface outside
!
access-list 107 permit ip 10.4.0.0 255.255.0.0 10.5.0.0 255.255.0.0
access-list 107 permit ip host 172.16.144.51 host 172.16.128.2
access-list 108 permit ip 10.4.0.0 255.255.0.0 10.6.0.0 255.255.0.0
access-list 108 permit ip host 172.16.144.51 host 172.16.128.5
!
isakmp enable outside
isakmp key 7Q! r$y$+xE address 172.16.128.5 netmask 255.255.255.255
isakmp key 7Q!r$y$+xE address 172.16.128.2 netmask 255.255.255.255
isakmp key 7Q!r$y$+xE address 172.16.226.28 netmask 255.255.255.255
isakmp key 7Q!r$y$+xE address 172.16.226.27 netmask 255.255.255.255
isakmp policy 1 authentication pre-share
isakmp policy 1 encryption 3des
isakmp policy 1 hash sha
isakmp policy 1 group 2
isakmp policy 1 lifetime 86400
```

Настройки, используемые для подключения по ВЧС удаленных пользователей.

```
vpngroup VPN1 address-pool vpnpool
vpngroup VPN1 dns-server 10.4.1.201
vpngroup VPN1 default-domain safe-small.com
vpngroup VPN1 idle-time 1800
vpngroup VPN1 password Y0eS)3/i6y
ip local pool vpnpool 10.4.3.1-10.4.3.254
```

Кампусный модуль

Используемые продукты

- Коммутатор уровня 2 Cisco Catalyst Layer (sCAT-2)
- CiscoSecure HOST IDS
- Cisco Secure Access Control Server
- Клиент SSH компании F-Secure

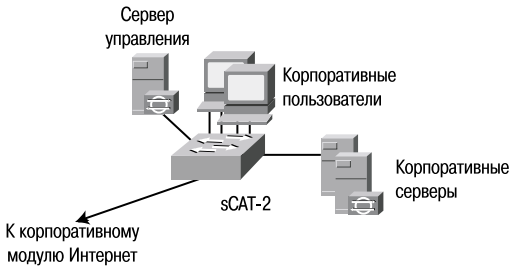


Рисунок 85. Дизайн кампусного модуля

Сеть среднего предприятия

Приводимые ниже конфигурации показывают пример настройки устройств в сети среднего предприятия. Если не указано иное, приведены конфигурации для центральной сети предприятия.

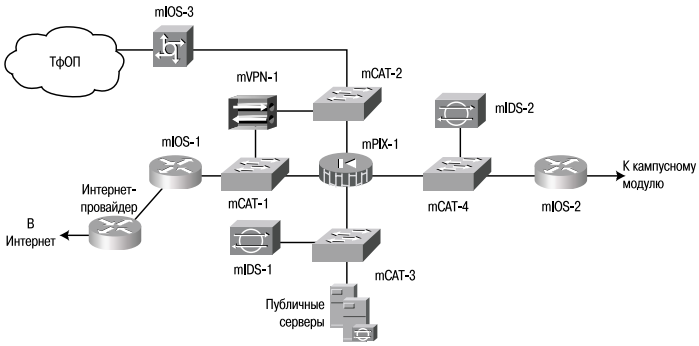


Рисунок 86. Дизайн модуля Интернет

Модуль Интернет

Используемые продукты

- Коммутаторы уровня 2 Cisco Catalys (mCAT-1 по mCAT-4)
- Маршрутизаторы Cisco IOS Routers с поддержкой ВЧС (mIOS-1 и mIOS-2)
- Сервер удаленного доступа Cisco IOS (mIOS-3)
- Концентратор ВЧС Cisco VPN 3000 (mVPN-1)
- Межсетевой экран Cisco Secure PIX Firewall (mPIX-1)
- Сетевая система обнаружения вторжений Cisco Secure IDS Sensors (mIDS-1 и mIDS-2)
- Хостовая система обнаружения вторжений CiscoSecure HOST IDS
- Система фильтрации почты Baltimore MIMESweeper

mIOS-1

Приведенная ниже конфигурация детализирует настройки списков доступа на граничном маршрутизаторе сети, контролирующем трафик между Интернет-провайдером и сетью предприятия.

```
interface FastEthernet0/0
ip address 172.16.240.2 255.255.255.0
ip access-group 112 in
no ip redirects
no cdp enable
!
interface Serial1/0
ip address 172.16.131.2 255.255.255.0
```

```
ip access-group 150 in
dsu bandwidth 44210
framing c-bit
no cdp enable
```

Фильтрование в соответствии с RFC 1918. Примечание: сеть 172.16.x.x не включена в список, потому что использовалась как сеть Интернет-провайдера в данном примере.

```
access-list 150 deny ip 10.0.0.0 0.255.255.255 any
access-list 150 deny ip 192.168.0.0 0.0.255.255 any
```

Предотвращение использования внешними устройствами адресов, используемых внутри сети предприятия:

```
access-list 150 deny ip 172.16.240.0 0.0.0.255 any
```

Разрешение передачи трафика протоколов ВЧС к устройствам ВЧС:

```
access-list 150 permit esp any host 172.16.240.3
access-list 150 permit udp any host 172.16.240.3 eq isakmp
access-list 150 permit esp host 172.16.128.2 host 172.16.240.1
access-list 150 permit udp host 172.16.128.2 host 172.16.240.1 eq isakmp
access-list 150 permit esp host 172.16.128.5 host 172.16.240.1
access-list 150 permit udp host 172.16.128.5 host 172.16.240.1 eq isakmp
```

Запрещение всех других типов взаимодействия, направленных на mIOS-1, mVPN-1, mPIX-1 и mCAT-1:

```
access-list 150 deny ip any host 172.16.240.3
access-list 150 deny ip any host 172.16.240.4
access-list 150 deny ip any host 172.16.240.2
access-list 150 deny ip any host 172.16.240.1
```

Разрешить все остальные протоколы в сеть 172.16.240.0, так как адреса внутренних устройств транслируются в эту сеть на межсетевом экране:

```
access-list 150 permit ip any 172.16.240.0 0.0.0.255
```

Блокировать и вести учет всего остального:

```
access-list 150 deny ip any any log
```

Приведенная далее конфигурация детализирует контроль трафика, идущего из сети предприятия к провайдеру.

Разрешить соединения TCP, идущие от маршрутизатора к станциям управления. Адреса станций управления 172.16.240.151 и 172.16.240.152 транслируются на межсетевом экране:

```
access-list 112 permit tcp host 172.16.240.151 host 172.16.240.2 established
access-list 112 permit tcp host 172.16.240.152 host 172.16.240.2 established
```

Разрешить доступ по протоколу SSH от станций управления к маршрутизатору:

```
access-list 112 permit tcp host 172.16.240.151 host 172.16.240.2 eq 22
access-list 112 permit tcp host 172.16.240.152 host 172.16.240.2 eq 22
```

Необходимо для использования протокола TFTP между станцией управления и маршрутизатором:

```
access-list 112 permit udp host 172.16.240.151 host 172.16.240.2 gt 1024
```

Разрешить синхронизацию сетевого времени в сети 172.16.240.0:

```
access-list 112 permit udp 172.16.240.0 0.0.0.255 host 172.16.240.2 eq ntp
```

Разрешить ping из внутренней сети в Интернет:

```
access-list 112 permit icmp 172.16.240.0 0.0.0.255 any
```

Блокировать и вести журнал всех других попыток доступа к маршрутизатору:

```
access-list 112 deny ip any host 172.16.240.2 log
```

Разрешить доступ в Интернет из сети 172.16.240.0:

```
!
access-list 112 permit ip 172.16.240.0 0.0.0.255 any
!
!
```

mPIX-1

Приведенная ниже конфигурация детализирует настройки межсетевого экрана PIX Firewall, mPIX-1.

```
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 pss security10
nameif ethernet3 vpn security15
!
ip address outside 172.16.240.1 255.255.255.0
```

```
ip address inside 10.3.4.1 255.255.255.0
ip address pss 10.3.6.1 255.255.255.0
ip address vpn 10.3.5.1 255.255.255.0
```

Эта часть конфигурации детализирует настройки трансляции сетевых адресов на PIX Firewall.
В комбинации со списком доступа nonat конфигурация, приведенная ниже, не позволяет выполняться трансляции между внутренними адресами, но позволяет трансляцию адресов между внутренними устройствами, устройствами удаленного доступа и Интернет:

```
global (outside) 100 172.16.240.101-172.16.240.150 netmask 255.255.255.0
global (outside) 200 172.16.240.201-172.16.240.250 netmask 255.255.255.0
nat (inside) 0 access-list nonat
nat (inside) 100 10.0.0.0 255.0.0.0 0 0
nat (pss) 0 access-list nonat
nat (vpn) 200 10.3.7.0 255.255.255.0 0 0
static (inside,vpn) 10.3.0.0 10.3.0.0 netmask 255.255.0.0 0 0
static (inside,pss) 10.3.8.253 10.3.8.253 netmask 255.255.255.255 0 0
static (inside,pss) 10.3.8.254 10.3.8.254 netmask 255.255.255.255 0 0
```

Трансляция частных адресов IP публичных серверов в зарегистрированные адреса IP для обеспечения доступа к ним из Интернет.

```
static (pss,outside) 172.16.240.50 10.3.6.50 netmask 255.255.255.255 0 0
```

Трансляция частных адресов IP станций управления в зарегистрированные адреса IP для обеспечения доступа к ним от управляемых устройств, расположенных за межсетевым экраном.

```
static (inside,outside) 172.16.240.151 10.3.8.254 netmask 255.255.255.255 0 0
static (inside,outside) 172.16.240.152 10.3.8.253 netmask 255.255.255.255 0 0
!
!
!
access-list nonat permit ip 10.0.0.0 255.0.0.0 10.0.0.0 255.0.0.0
access-list nonat deny ip 10.0.0.0 255.0.0.0 any
```

Приведенный ниже фрагмент конфигурации описывает контроль доступа на межсетевом экране. Имя списка доступа (ACL) говорит, где он должен быть применен.

Разрешить трафик ВЧС от удаленных подразделений:

```
access-list out permit ip 10.5.0.0 255.255.0.0 10.3.0.0 255.255.0.0
access-list out permit ip 10.6.0.0 255.255.0.0 10.3.0.0 255.255.0.0
```


Фильтрование в соответствии с RFC 1918. Примечание: сеть 172.16.x.x не включена в список, потому что использовалась как сеть Интернет-провайдера в данном примере:

```
access-list out deny ip 10.0.0.0 255.0.0.0 any
access-list out deny ip 192.168.0.0 255.255.0.0 any
```

Доступ внешних устройств к публичным серверам по протоколам HTTP, SSL, FTP, SMTP, и DNS.

```
!
access-list out permit tcp any host 172.16.240.50 eq www
access-list out permit tcp any host 172.16.240.50 eq 443
access-list out permit tcp any host 172.16.240.50 eq ftp
access-list out permit tcp any host 172.16.240.50 eq smtp
access-list out permit udp any host 172.16.240.50 eq domain
```

Разрешить ответные пакеты ICMP на инициированные из внутренней сети запросы:

```
access-list out permit icmp any 172.16.240.0 255.255.255.0 echo-reply
```

Разрешить пакеты ICMP, необходимые для работы path MTU discovery (PMTUD):

```
access-list out permit icmp any 172.16.240.0 255.255.255.0 unreachable
```

Разрешить трафик протоколов управления syslog, TFTP и TACACS+ от удаленных подразделений:

```
access-list out permit udp host 172.16.128.2 host 172.16.240.151 eq syslog
access-list out permit udp host 172.16.128.2 host 172.16.240.152 eq syslog
access-list out permit udp host 172.16.128.2 host 172.16.240.151 eq tftp
access-list out permit tcp host 172.16.128.2 host 172.16.240.152 eq tacacs
access-list out permit udp host 172.16.128.5 host 172.16.240.151 eq syslog
access-list out permit udp host 172.16.128.5 host 172.16.240.152 eq syslog
access-list out permit udp host 172.16.128.5 host 172.16.240.151 eq tftp
access-list out permit tcp host 172.16.128.5 host 172.16.240.152 eq tacacs
```

Разрешить протоколы syslog, TFTP и TACACS+ от маршрутизатора mIOS-1 и коммутатора mCAT-1 на станции сетевого управления:

```
access-list out permit udp host 172.16.240.2 host 172.16.240.151 eq syslog
access-list out permit udp host 172.16.240.2 host 172.16.240.152 eq syslog
access-list out permit udp host 172.16.240.2 host 172.16.240.151 eq tftp
```

```
access-list out permit tcp host 172.16.240.2 host 172.16.240.152 eq tacacs
access-list out permit udp host 172.16.240.4 host 172.16.240.151 eq syslog
access-list out permit udp host 172.16.240.4 host 172.16.240.152 eq syslog
access-list out permit udp host 172.16.240.4 host 172.16.240.151 eq tftp
access-list out permit tcp host 172.16.240.4 host 172.16.240.152 eq tacacs
```

Список доступа «in» расположен на входе внутреннего интерфейса межсетевого экрана.

Разрешить трафик ICMP echo из внутренней сети:

```
access-list in permit icmp any any echo
```

Разрешить внутреннему серверу DNS обращаться к внешним серверам DNS:

```
access-list in permit udp host 10.3.2.50 host 10.3.6.50 eq domain
```

Разрешить внутренним пользователям использовать протоколы HTTP, SSL, и FTP для доступа к внешним серверам:

```
access-list in permit tcp 10.0.0.0 255.0.0.0 host 10.3.6.50 eq www
access-list in permit tcp 10.0.0.0 255.0.0.0 host 10.3.6.50 eq 443
access-list in permit tcp 10.0.0.0 255.0.0.0 host 10.3.6.50 eq ftp
```

Разрешить передачу почты между внешним и внутренним почтовыми серверами:

```
access-list in permit tcp host 10.3.2.50 host 10.3.6.50 eq smtp
```

Разрешить доступ по протоколу Telnet от станций управления к коммутатору mCAT-2, который не поддерживает протокол SSH:

```
access-list in permit tcp host 10.3.8.253 host 10.3.6.4 eq telnet
access-list in permit tcp host 10.3.8.254 host 10.3.6.4 eq telnet
```

Запретить все остальные типы доступа из внутренней сети к публичным серверам:

```
access-list in deny ip any 10.3.6.0 255.255.255.0
```

Разрешить всем внутренним пользователям доступ в Интернет:

```
access-list in permit ip 10.0.0.0 255.0.0.0 any
```

Список доступа «pss» расположен на интерфейсе публичных серверов (DMZ) межсетевого экрана.

Разрешить протоколы syslog, TACACS+ и TFTP от коммутатора mCAT-2 к станциям управления:

```
access-list pss permit udp host 10.3.6.4 host 10.3.8.254 eq syslog
access-list pss permit udp host 10.3.6.4 host 10.3.8.253 eq syslog
access-list pss permit tcp host 10.3.6.4 host 10.3.8.253 eq tacacs
access-list pss permit udp host 10.3.6.4 host 10.3.8.254 eq tftp
```

Разрешить синхронизацию времени между коммутатором mCAT-2 и маршрутизатором mIOS-2:

```
access-list pss permit udp host 10.3.6.4 host 10.3.4.4 eq ntp
```

Разрешить управляющий трафик хостовых систем обнаружения вторжений от публичных серверов к станциям управления:

```
access-list pss permit tcp host 10.3.6.50 host 10.3.8.253 eq 5000
```

Разрешить передачу почты от публичного почтового сервера к внутреннему почтовому серверу.

```
access-list pss permit tcp host 10.3.6.50 host 10.3.2.50 eq smtp
```

Запретить все остальные типы трафика во внутреннюю сеть

```
access-list pss deny ip any 10.3.0.0 255.255.0.0
```

Разрешить передачу почты и работу службы имен (DNS) между публичными серверами и Интернет:

```
access-list pss permit tcp host 10.3.6.50 any eq smtp
access-list pss permit udp host 10.3.6.50 any eq domain
```

Список доступа «vpn» привязан на вход к интерфейсу, за которым расположены устройства ВЧС. Удаленным пользователям ВЧС назначаются адреса из сети 10.3.7.0, настроенной на сервере контроля доступа CiscoSecure ACS. Удаленным пользователям, подключающимся по коммутируемым линиям связи, выдаются адреса из сети 10.3.8.0.

Разрешить удаленным пользователям работать с публичными серверами только по протоколам HTTP, SSL и FTP:

```
access-list vpn permit tcp 10.3.7.0 255.255.255.0 host 10.3.6.50 eq www
access-list vpn permit tcp 10.3.8.0 255.255.255.0 host 10.3.6.50 eq www
access-list vpn permit tcp 10.3.7.0 255.255.255.0 host 10.3.6.50 eq 443
access-list vpn permit tcp 10.3.8.0 255.255.255.0 host 10.3.6.50 eq 443
access-list vpn permit tcp 10.3.7.0 255.255.255.0 host 10.3.6.50 eq ftp
access-list vpn permit tcp 10.3.8.0 255.255.255.0 host 10.3.6.50 eq ftp
access-list vpn deny ip 10.3.7.0 255.255.255.0 10.3.6.0 255.255.255.0
access-list vpn deny ip 10.3.8.0 255.255.255.0 10.3.6.0 255.255.255.0
```

Разрешить удаленным пользователям доступ в остальную часть внутренней сети и Интернет:

```
access-list vpn permit ip 10.3.7.0 255.255.255.0 any
access-list vpn permit ip 10.3.8.0 255.255.255.0 any
```

Разрешить трафик syslog, TFTP и TACACS+ от концентратора ВЧС к станциям сетевого управления:

```
access-list vpn permit udp host 10.3.5.5 host 10.3.8.254 eq tftp
access-list vpn permit udp host 10.3.5.5 host 10.3.8.254 eq syslog
access-list vpn permit udp host 10.3.5.5 host 10.3.8.253 eq syslog
access-list vpn permit tcp host 10.3.5.5 host 10.3.8.253 eq tacacs
```

Разрешить синхронизацию сетевого времени между концентратором ВЧС и маршрутизатором mIOS-2:

```
access-list vpn permit udp host 10.3.5.5 host 10.3.4.4 eq ntp
```

Разрешить протокол аутентификации, авторизации и учета RADIUS от концентратора ВЧС к станциям управления:

```
access-list vpn permit udp host 10.3.5.5 host 10.3.8.253 eq 1645
```

Разрешить syslog, TFTP, и TACACS+ от сервера удаленного доступа mIOS-3 к станциям сетевого управления:

```
access-list vpn permit udp host 10.3.5.2 host 10.3.8.254 eq tftp
access-list vpn permit udp host 10.3.5.2 host 10.3.8.254 eq syslog
access-list vpn permit udp host 10.3.5.2 host 10.3.8.253 eq syslog
access-list vpn permit tcp host 10.3.5.2 host 10.3.8.253 eq tacacs
```

Разрешить синхронизацию времени между mIOS-3 и mIOS-2:

```
access-list vpn permit udp host 10.3.5.2 host 10.3.4.4 eq ntp
```

Разрешить syslog, TFTP и TACACS+ от коммутатора mcAT-3 к станциям сетевого управления:

```
access-list vpn permit udp host 10.3.5.4 host 10.3.8.254 eq tftp
access-list vpn permit udp host 10.3.5.4 host 10.3.8.254 eq syslog
access-list vpn permit udp host 10.3.5.4 host 10.3.8.253 eq syslog
access-list vpn permit tcp host 10.3.5.4 host 10.3.8.253 eq tacacs
```

Разрешить синхронизацию времени между коммутатором mCAT-3 и маршрутизатором mIOS-2:

```
access-list vpn permit udp host 10.3.5.4 host 10.3.4.4 eq ntp
!
```

Виртуальные частные сети

Приведенная ниже конфигурация добавлена для использования ВЧС между головным офисом и удаленными подразделениями.

Шифрование пользовательского трафика и трафика управления, направленного на первое удаленное устройство.

```
access-list remote1 permit ip 10.3.0.0 255.255.0.0 10.5.0.0 255.255.0.0
access-list remote1 permit ip host 172.16.240.151 host 172.16.128.2
access-list remote1 permit ip host 172.16.240.152 host 172.16.128.2
```

Шифрование пользовательского трафика и трафика управления, направленного на второе удаленное устройство.

```
access-list remote2 permit ip 10.3.0.0 255.255.0.0 10.6.0.0 255.255.0.0
access-list remote2 permit ip host 172.16.240.151 host 172.16.128.5
access-list remote2 permit ip host 172.16.240.152 host 172.16.128.5
```

Определение крипто карты и присвоение ее на внешний интерфейс.

```
crypto ipsec transform-set 3dessha esp-3des esp-sha-hmac
crypto map remote1 10 ipsec-isakmp
crypto map remote1 10 match address remote1
crypto map remote1 10 set peer 172.16.128.2
crypto map remote1 10 set transform-set 3dessha
crypto map remote1 20 ipsec-isakmp
crypto map remote1 20 match address remote2
crypto map remote1 20 set peer 172.16.128.5
crypto map remote1 20 set transform-set 3dessha
crypto map remote1 interface outside
```

Определение общих ключей.

```
isakmp enable outside
isakmp key 7Q!r$y$+xE address 172.16.128.2 netmask 255.255.255.255
isakmp key 7Q!r$y$+xE address 172.16.128.5 netmask 255.255.255.255
isakmp identity address
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption 3des
isakmp policy 10 hash sha
isakmp policy 10 group 2
isakmp policy 10 lifetime 86400
!
```

Кампусный модуль

Используемые продукты

- Коммутатор уровня 3 Cisco Catalyst (mCAT-6)
- Коммутатор уровня 2 Cisco Catalyst (mCAT-5)
- Сетевая система обнаружения вторжений Cisco Secure IDS Sensors (mIDS-3)
- Хостовая система обнаружения вторжений CiscoSecure Host IDS
- Cisco Secure Access Control Server
- CiscoWorks 2000
- Клиент SSH F-Secure
- Система однократных паролей RSA SecureID

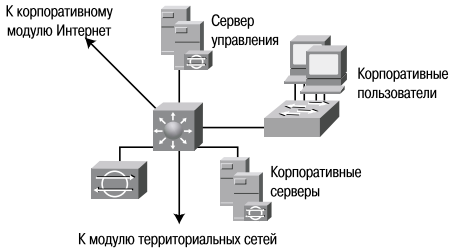


Рисунок 87. Дизайн кампусного модуля

Приведенная ниже конфигурация детализирует контроль доступа на коммутаторе Уровня 4, который контролирует доступ в виртуальной локальной сети управления, фильтрацию сегмента публичных серверов и т. п. VLAN 10 используется для корпоративных пользователей. VLAN 11 используется для корпоративных серверов интранет. VLAN 12 и 13 подключены к модулям Интернет и территориальных сетей. В VLAN 99 размещены станции сетевого управления.

mCAT-6

Корпоративные пользователи:

```
interface Vlan10
ip address 10.3.1.1 255.255.255.0
ip access-group 101 in
no ip redirects
no cdp enable
```

Корпоративные серверы:

```
interface Vlan11
ip address 10.3.2.1 255.255.255.0
ip access-group 102 in
no ip redirects
no cdp enable
!
!
interface Vlan12
ip address 10.3.3.1 255.255.255.0
no ip redirects
ip ospf authentication message-digest
ip ospf message-digest-key 1 md5 7 134E031F4158140119
no cdp enable
!
interface Vlan13
ip address 10.3.9.1 255.255.255.0
no ip redirects
ip ospf authentication message-digest
ip ospf message-digest-key 1 md5 7 024D105641521F0A7E
no cdp enable
!
```

Сегмент управления:

```
interface Vlan99
ip address 10.3.8.1 255.255.255.0
ip access-group 103 out
no ip redirects
no cdp enable
```

Фильтрация в соответствии с RFC 2827 на пользовательском сегменте:

```
access-list 101 permit ip 10.3.1.0 0.0.0.255 any
access-list 101 deny ip any any
```

Фильтрация в соответствии с RFC 2827 на сегменте корпоративных серверов:

```
access-list 102 permit ip 10.3.2.0 0.0.0.255 any
access-list 102 deny ip any any log
```

Пример фильтрации для сегмента сетевого управления (неполный):

```
access-list 103 permit udp host 10.3.2.50 eq domain host 10.3.8.253
access-list 103 permit udp host 10.3.2.50 eq domain host 10.3.8.254
```

```
access-list 103 permit tcp host 10.3.2.50 eq www host 10.3.8.253 established
access-list 103 permit tcp host 10.3.2.50 eq www host 10.3.8.254 established
access-list 103 permit tcp host 10.3.2.50 eq ftp host 10.3.8.253 established
access-list 103 permit tcp host 10.3.2.50 eq ftp host 10.3.8.254 established
access-list 103 permit tcp host 10.3.2.50 eq ftp-data host 10.3.8.253
access-list 103 permit tcp host 10.3.2.50 eq ftp-data host 10.3.8.254
access-list 103 permit tcp host 10.3.2.50 host 10.3.8.253 eq 5000
access-list 103 permit udp host 10.3.1.4 host 10.3.8.253 eq syslog
access-list 103 permit udp host 10.3.1.4 host 10.3.8.254 eq syslog
access-list 103 permit tcp host 10.3.1.4 host 10.3.8.253 eq tacacs
access-list 103 permit udp host 10.3.1.4 host 10.3.8.254 eq tftp
access-list 103 permit udp host 10.3.1.4 host 10.3.8.254 gt 1023
access-list 103 permit udp host 10.3.1.4 eq snmp host 10.3.8.254
access-list 103 permit tcp host 10.3.1.4 eq telnet host 10.3.8.253 established
access-list 103 permit tcp host 10.3.1.4 eq telnet host 10.3.8.254 established
access-list 103 deny ip any any
!
```

Главная сеть или сеть филиала

Приведенная ниже конфигурация добавляется в том случае, когда необходимо разрешить трафик управления от удаленных подразделений.

```
access-list 103 permit udp host 172.16.128.5 host 10.3.8.253 eq syslog
access-list 103 permit udp host 172.16.128.5 host 10.3.8.254 eq syslog
access-list 103 permit tcp host 172.16.128.5 host 10.3.8.253 eq tacacs
access-list 103 permit udp host 172.16.128.5 host 10.3.8.254 eq tftp
access-list 103 permit udp host 172.16.128.5 host 10.3.8.254 gt 1023
access-list 103 permit tcp host 172.16.128.5 eq 22 host 10.3.8.253 established
access-list 103 permit tcp host 172.16.128.5 eq 22 host 10.3.8.254 established
access-list 103 permit tcp host 172.16.128.5 eq 443 host 10.3.8.253 established
access-list 103 permit tcp host 172.16.128.5 eq 443 host 10.3.8.254 established
access-list 103 permit udp host 172.16.128.2 host 10.3.8.253 eq syslog
access-list 103 permit udp host 172.16.128.2 host 10.3.8.254 eq syslog
access-list 103 permit tcp host 172.16.128.2 host 10.3.8.253 eq tacacs
access-list 103 permit udp host 172.16.128.2 host 10.3.8.254 eq tftp
access-list 103 permit udp host 172.16.128.2 host 10.3.8.254 gt 1023
access-list 103 permit tcp host 172.16.128.2 eq 22 host 10.3.8.253 established
access-list 103 permit tcp host 172.16.128.2 eq 22 host 10.3.8.254 established
```


mCAT-5

Приведенная ниже конфигурация показывает некоторые настройки виртуальных локальных сетей (VLAN) на коммутаторе уровня 2. Неиспользуемые порты должны быть заблокированы. Частные виртуальные локальные сети (PVLAN) настроены на всех портах кроме идущих на центральный коммутатор.

Пользовательские порты:

```
interface FastEthernet0/1
port protected
switchport access vlan 99
no cdp enable
!
interface FastEthernet0/2
port protected
switchport access vlan 99
no cdp enable
```

Неиспользуемые порты:

```
interface FastEthernet0/3
port protected
shutdown
no cdp enable
!
interface FastEthernet0/4
port protected
shutdown
no cdp enable
```

Порты, подключенные к центральному коммутатору:

```
interface GigabitEthernet0/1
switchport access vlan 99
no cdp enable
```

Управляющий VLAN:

```
interface VLAN99
ip address 10.3.1.4 255.255.255.0
no ip directed-broadcast
no ip route-cache
!
```

Модуль территориальных сетей

Используемые продукты

- Маршрутизатор Cisco IOS (mIOS-4)

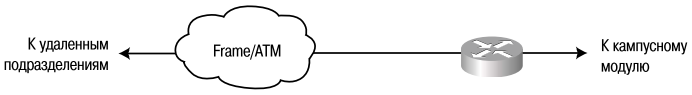


Рисунок 88. Дизайн модуля территориальных сетей

Подключение удаленных пользователей

Используемые продукты

- Маршрутизатор Cisco IOS Router с поддержкой ВЧС (rIOS-1)
- Аппаратный клиент ВЧС Cisco VPN 3002 Hardware Client (rVPN3002-1)
- Межсетевой экран Cisco Secure PIX Firewall (rPIX-1)
- Программный клиент ВЧС Cisco VPN 3000
- Концентратор Ethernet (внешний или интегрированный)
- Персональный межсетевой экран Zone Alarm Pro Personal Firewall

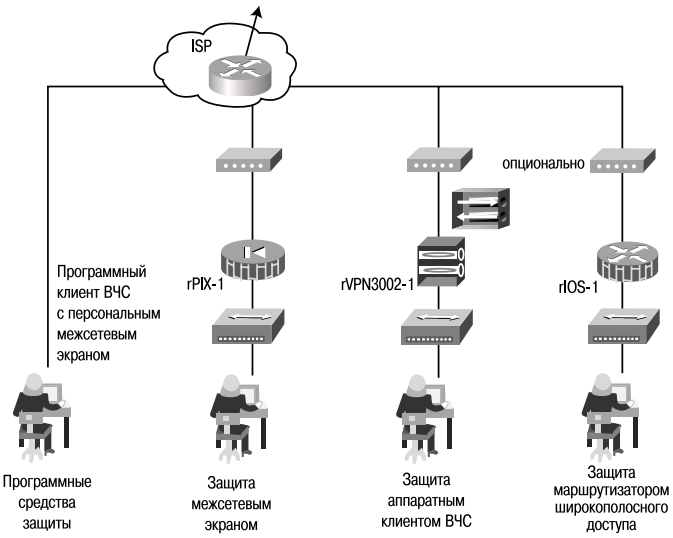


Рисунок 89. Дизайн удаленного подключения пользователей

Ниже приведены примеры настройки устройств, используемых для удаленного доступа пользователей.

rIOS-1 (Удаленное подразделение)

Пример настройки при подключении к головному офису.

```
crypto isakmp policy 1
encr 3des
authentication pre-share
group 2
crypto isakmp key 7Q!r$y$+xE address 172.16.240.1
!
!
crypto ipsec transform-set 3dessha esp-3des esp-sha-hmac
!
crypto map remote1 10 ipsec-isakmp
set peer 172.16.240.1
set transform-set 3dessha
match address 101
```

Первая запись указывает на то, что весь трафик между сетями 10.5.0.0 и 10.3.0.0 должен быть зашифрован. Последние две записи указывают что трафик управления тоже должен шифроваться

```
access-list 101 permit ip 10.5.0.0 0.0.255.255 10.3.0.0 0.0.255.255
access-list 101 permit ip host 172.16.128.2 host 172.16.240.151
access-list 101 permit ip host 172.16.128.2 host 172.16.240.152
!
```

Здесь показан контроль доступа на публичном (FastEthernet0/1) и частном (FastEthernet0/0) интерфейсах маршрутизатора, так же, как и использование встроенного межсетевого экрана IOS Firewall.

```
interface FastEthernet0/0
ip address 10.5.1.2 255.255.255.0
ip access-group 105 in
ip nat inside
ip inspect remote_fw in
!
interface FastEthernet0/1
ip address 172.16.128.2 255.255.255.0
ip access-group 102 in
ip nat outside
crypto map remote1
```

Трафик протоколов IKE и ESP от корпоративного шлюза ВЧС должен быть разрешен. Весь трафик между сетями 10.5.0.0 и 10.3.0.0 тоже должен быть разрешен так же как и трафик управления.

```
access-list 102 permit ip 10.3.0.0 0.0.255.255 10.5.0.0 0.0.255.255
access-list 102 deny ip 10.0.0.0 0.255.255.255 any
access-list 102 deny ip 192.168.0.0 0.0.255.255 any
access-list 102 permit icmp any host 172.16.128.2 echo-reply
access-list 102 permit icmp any host 172.16.128.2 unreachable
access-list 102 permit esp host 172.16.240.1 host 172.16.128.2
```

```
access-list 102 permit udp host 172.16.240.1 host 172.16.128.2 eq isakmp
access-list 102 permit tcp host 172.16.240.151 host 172.16.128.2 eq 22
access-list 102 permit tcp host 172.16.240.152 host 172.16.128.2 eq 22
access-list 102 permit tcp host 172.16.240.152 eq tacacs host 172.16.128.2
access-list 102 permit udp host 172.16.240.151 host 172.16.128.2 gt 1023
access-list 102 deny ip any any log
```

Фильтрование в соответствии с RFC 2827 позволяет только сети с адресом 10.5.0.0 получить доступ как к головному офису, так и к Интернет.

```
access-list 105 permit ip 10.5.0.0 0.0.255.255 any
access-list 105 deny ip any any log
!
```

Здесь показана настройка трансляции адресов множества внутренних устройств в один внешний адрес IP (PAT). Все внутренние устройства будут использовать адрес самого маршрутизатора для выхода в Интернет.

```
ip nat pool remote_pool 172.16.128.2 172.16.128.2 netmask 255.255.255.0
ip nat inside source route-map nat_internet pool remote_pool
!
route-map nat_internet permit 10
match ip address 104
!
access-list 104 deny ip 10.5.0.0 0.0.255.255 10.0.0.0 0.255.255.255
access-list 104 permit ip 10.5.0.0 0.0.255.255 any
```

rPIX-1 (Межсетевой экран удаленного офиса)

Пример настройки ВЧС при подключении к головному офису.

```
crypto ipsec transform-set 3dessha esp-3des esp-sha-hmac
crypto map remote1 10 ipsec-isakmp
crypto map remote1 10 match address remote1
crypto map remote1 10 set peer 172.16.240.1
crypto map remote1 10 set transform-set 3dessha
crypto map remote1 interface outside
isakmp enable outside
isakmp key 7Q!r$y$+xE address 172.16.240.1 netmask 255.255.255.255
isakmp identity address
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption 3des
isakmp policy 10 hash sha
isakmp policy 10 group 2
isakmp policy 10 lifetime 86400
```


Первая запись указывает на то, что весь трафик между сетями 10.6.0.0 и 10.3.0.0 должен быть зашифрован. Последние две записи указывают на то, что трафик управления тоже должен шифроваться.

```
access-list remote1 permit ip 10.6.0.0 255.255.0.0 10.3.0.0 255.255.0.0
access-list remote1 permit ip host 172.16.128.5 host 172.16.240.151
access-list remote1 permit ip host 172.16.128.5 host 172.16.240.152
!
```

Здесь приведена настройка контроля доступа на внешнем (outside) и внутреннем (inside) интерфейсах.

```
nameif ethernet0 outside security0
nameif ethernet1 inside security100
!
ip address outside 172.16.128.5 255.255.255.0
ip address inside 10.6.1.1 255.255.255.0
!
access-group out in interface outside
access-group in in interface inside
```

Фильтрование в соответствии с RFC 2827 позволяет только сети с адресом 10.6.0.0 получить доступ как к головному офису, так и к Интернет.

```
access-list in permit ip 10.6.0.0 255.255.0.0 any
```

Разрешение трафика ВЧС от головного офиса:

```
access-list out permit ip 10.3.0.0 255.255.0.0 10.6.0.0 255.255.0.0
```

Фильтрование в соответствии с RFC 1918. Примечание: сеть 172.16.x.x не включена в список, потому что использовалась как сеть Интернет-провайдера в данном примере.

```
access-list out deny ip 10.0.0.0 255.0.0.0 any
access-list out deny ip 192.168.0.0 255.255.0.0 any
```

Разрешение протокола ICMP для использования ping и path MTU discovery (PMTU):

```
access-list out permit icmp any host 172.16.128.5 echo-reply
```

```
access-list out permit icmp any host 172.16.128.5 unreachable
```

Разрешение протоколов ESP и IKE от головного офиса:

```
access-list out permit esp host 172.16.240.1 host 172.16.128.5
access-list out permit udp host 172.16.240.1 host 172.16.128.5 eq isakmp
```

Здесь показана настройка трансляции адресов множества внутренних устройств в один внешний адрес IP (PAT). Все внутренние устройства будут использовать адрес публичного интерфейса самого межсетевого экрана для выхода в Интернет.

```
global (outside) 100 interface
nat (inside) 0 access-list nonat
nat (inside) 100 10.6.1.0 255.255.255.0 0 0
```

Этот список доступа предотвращает трансляцию адресов трафика, направленного в головной офис.

```
access-list nonat permit ip 10.6.0.0 255.255.0.0 10.0.0.0 255.0.0.0
access-list nonat deny ip 10.6.0.0 255.255.0.0 any
```

Приложение B. Основы сетевой безопасности

Необходимость защиты сетей

Интернет полностью меняет то, как мы работаем, живем, развлекаемся и учимся. Эти изменения будут происходить в уже известных нам областях (электронная коммерция, доступ к информации в реальном времени, расширение возможностей связи и т. д.), а также в областях, о которых мы пока не подозреваем. Может даже наступить такой день, когда корпорация сможет делать все свои телефонные звонки через Интернет и совершенно бесплатно. В личной жизни возможны появления воспитательских web-сайтов, через которые родители смогут в любой момент узнать, как обстоят дела у детей. Наше общество только начинает осознавать возможности Интернет. Однако вместе с колоссальным ростом популярности этой технологии возникает беспрецедентная угроза разглашения персональных данных, критически важных корпоративных ресурсов, государственных тайн и т. д. Каждый день хакеры подвергают угрозе эти ресурсы, пытаясь получить к ним доступ с помощью специальных атак. Эти атаки, которые будут описаны ниже, становятся все более изощренными и простыми в исполнении. Этому способствуют два основных фактора.

Во-первых, это повсеместное проникновение Интернет. Сегодня к этой сети подключены миллионы устройств. Многие миллионы устройств будут подключены к Интернет в ближайшем будущем. И поэтому вероятность доступа хакеров к уязвимым устройствам постоянно возрастает. Кроме того, широкое распространение Интернет позволяет хакерам обмениваться информацией в глобальном масштабе. Простой поиск по ключевым словам типа «хакер», «взлом», «hack», «crack» или «phreak» даст вам тысячи сайтов, на многих из которых можно найти вредоносные коды и способы их использования.

Во-вторых, это всеобщее распространение простых в использовании операционных систем и сред разработки. Этот фактор резко снижает уровень знаний и навыков, которые необходимы хакеру. Раньше хакер должен был обладать хорошими навыками программирования, чтобы создавать и распространять простые в использовании приложения. Теперь, чтобы получить доступ к хакерскому средству, нужно просто знать IP-адрес нужного сайта, а для проведения атаки достаточно щелкнуть мышкой.

Классификация сетевых атак

Сетевые атаки столь же разнообразны, как и системы, против которых они направлены. Некоторые атаки отличаются большой сложностью. Другие может осуществить обычный оператор, даже не предполагающий, какие последствия может иметь его деятельность. Для оценки типов атак необходимо знать некоторые ограничения, изначально присущие протоколу TPC/IP. Сеть Интернет создавалась для связи между государственными учреждениями и университетами в помощь учебному процессу и научным исследованиям. Создатели этой сети не подозревали, насколько широко она распространится. В результате в спецификациях ранних версий Интернет-протокола (IP) отсутствовали требования безопасности. Именно поэтому многие реализации IP являются изначально уязвимыми. Через много лет, получив множество рекламаций (RFC — Request for Comments), мы, наконец, стали внедрять средства безопасности для IP. Однако ввиду того, что изначально средства защиты для протокола IP не разрабатывались, все его реализации стали дополняться разнообразными сетевыми процедурами, услугами и продуктами, снижающими риски, присущие этому протоколу. Далее мы кратко обсудим типы атак, которые обычно применяются против сетей IP, и перечислим способы борьбы с ними.

Снифферы пакетов

Сниффер пакетов представляет собой прикладную программу, которая использует сетевую карту, работающую в режиме promiscuous mode (в этом режиме все пакеты, полученные по физическим каналам, сетевой адаптер отправляет приложению для обработки). При этом сниффер перехватывает все сетевые пакеты, которые передаются через определенный домен. В настоящее время снифферы работают в сетях на вполне законном основании. Они используются для диагностики неисправностей и анализа тра-

фика. Однако ввиду того, что некоторые сетевые приложения передают данные в текстовом формате (Telnet, FTP, SMTP, POP3 и т. д.), с помощью сниффера можно узнать полезную, а иногда и конфиденциальную информацию (например, имена пользователей и пароли).
Перехват имен и паролей создает большую опасность, так как пользователи часто применяют один и тот же логин и пароль для множества приложений и систем. Многие пользователи вообще имеют один пароль для доступа ко всем ресурсам и приложениям. Если приложение работает в режиме клиент/сервер, а аутентификационные данные передаются по сети в читаемом текстовом формате, эту информацию с большой вероятностью можно использовать для доступа к другим корпоративным или внешним ресурсам. Хакеры слишком хорошо знают и используют наши человеческие слабости (методы атак часто базируются на методах социальной инженерии). Они прекрасно знают, что мы пользуемся одним и тем же паролем для доступа к множеству ресурсов, и поэтому им часто удается, узнав наш пароль, получить доступ к важной информации. В самом худшем случае хакер получает доступ к пользовательскому ресурсу на системном уровне и с его помощью создает нового пользователя, которого можно в любой момент использовать для доступа в сеть и к ее ресурсам.
Смягчить угрозу сниффинга пакетов можно с помощью следующих средств:

- Аутентификация. Сильные средства аутентификации являются первым способом защиты от сниффинга пакетов. Под «сильным» мы понимаем такой метод аутентификации, который трудно обойти. Примером такой аутентификации являются однократные пароли (OTP — One-Time Passwords). OTP — это технология двухфакторной аутентификации, при которой происходит сочетание того, что у вас есть, с тем, что вы знаете. Типичным примером двухфакторной аутентификации является работа обычного банкомата, который опознает вас, во-первых, по вашей пластиковой карточке и, во-вторых, по вводимому вами ПИН-коду. Для аутентификации в системе OTP также требуется ПИН-код и ваша личная карточка. Под «карточкой» (token) понимается аппаратное или программное средство, генерирующее (по случайному принципу) уникальный одномоментный однократный пароль. Если хакер узнает этот пароль с помощью сниффера, эта информация будет бесполезной, потому что в этот момент пароль уже будет использован и выведен из употребления. Заметим, что этот способ борьбы со сниффингом эффективен только для борьбы с перехватом паролей. Снифферы, перехватывающие другую информацию (например, сообщения электронной почты), не теряют своей эффективности.
- Коммутируемая инфраструктура. Еще одним способом борьбы со сниффингом пакетов в вашей сетевой среде является создание коммутируемой инфраструктуры. Если, к примеру, во всей организации используется коммутируемый Ethernet, хакеры могут получить доступ только к трафику, поступающему на тот порт, к которому они подключены. Коммутируемая инфраструктура не ликвидирует угрозу сниффинга, но заметно снижает ее остроту.
- Анти-снифферы. Третий способ борьбы со сниффингом заключается в установке аппаратных или программных средств, распознающих снифферы, работающие в вашей сети. Эти средства не могут полностью ликвидировать угрозу, но, как и многие другие средства сетевой безопасности, они включаются в общую систему защиты. Так называемые «анти-снифферы» измеряют время реагирования хостов и определяют, не приходится ли хостам обрабатывать «лишний» трафик. Одно из таких средств, поставляемых компанией LOpht Heavy Industries, называется AntiSniff. Боле подробную информацию можно получить на сайте http://www.l0pht.com/antisniff/
- Криптография. Самый эффективный способ борьбы со сниффингом пакетов не предотвращает перехвата и не распознает работу снифферов, но делает эту работу бесполезной. Если канал связи является криптографически защищенным, это значит, что хакер перехватывает не сообщение, а зашифрованный текст (то есть непонятную последовательность битов). Криптография Cisco на сетевом уровне базируется на протоколе IPSec. IPSec представляет собой стандартный метод защищенной связи между устройствами с помощью протокола IP. К прочим криптографическим протоколам сетевого управления относятся протоколы SSH (Secure Shell) и SSL (Secure Socket Layer).

IP-спуфинг

IP-спуфинг происходит, когда хакер, находящийся внутри корпорации или вне ее, выдает себя за санкционированного пользователя. Это можно сделать двумя способами. Во-первых, хакер может воспользоваться IP-адресом, находящимся в пределах диапазона санкционированных IP-адресов, или авторизованным внешним адресом, которому разрешается доступ к определенным сетевым ресурсам. Атаки IP-спуфинга часто являются отправной точкой для прочих атак. Классический пример — атака DoS, которая начинается с чужого адреса, скрывающего истинную личность хакера.
Обычно IP-спуфинг ограничивается вставкой ложной информации или вредоносных команд в обычный поток данных, передаваемых между клиентским и серверным приложением или по каналу связи между одноранговыми устройствами. Для двусторонней связи хакер должен изменить все таблицы маршрутизации, чтобы направить трафик на ложный IP-адрес. Некоторые хакеры, однако, даже не пытаются получить ответ от приложений. Если главная задача состоит в получении от системы важного файла, ответы приложений не имеют значения.
Если же хакеру удается поменять таблицы маршрутизации и направить трафик на ложный IP-адрес, хакер получит все пакеты и сможет отвечать на них так, будто он является санкционированным пользователем.

Угрозу спуфинга можно ослабить (но не устранить) с помощью следующих мер:

- Контроль доступа. Самый простой способ предотвращения IP-спуфинга состоит в правильной настройке управления доступом. Чтобы снизить эффективность IP-спуфинга, настройте контроль доступа на отсечение любого трафика, поступающего из внешней сети с исходным адресом, который должен располагаться внутри вашей сети. Заметим, что это помогает бороться с IP-спуфингом, когда санкционированными являются только внутренние адреса. Если санкционированными являются и некоторые адреса внешней сети, данный метод становится неэффективным.
- Фильтрация RFC 2827. Вы можете пресечь попытки спуфинга чужих сетей пользователями вашей сети (и стать добропорядочным «сетевым гражданином»). Для этого необходимо отбраковывать любой исходящий трафик, исходный адрес которого не является одним из IP-адресов вашей организации. Этот тип фильтрации, известный под названием «RFC 2827», может выполнять и ваш провайдер (ISP). В результате отбраковывается весь трафик, который не имеет исходного адреса, ожидаемого на определенном интерфейсе. К примеру, если ISP предоставляет соединение с IP-адресом 15.1.1.0/24, он может настроить фильтр таким образом, чтобы с данного интерфейса на маршрутизатор ISP допускался только трафик, поступающий с адреса 15.1.1.0/24. Заметим, что до тех пор, пока все провайдеры не внедрят этот тип фильтрации, его эффективность будет намного ниже возможной. Кроме того, чем дальше от фильтруемых устройств, тем труднее проводить точную фильтрацию. Так, например, фильтрация RFC 2827 на уровне маршрутизатора доступа требует пропуска всего трафика с главного сетевого адреса (10.0.0.0/8), тогда как на уровне распределения (в данной архитектуре) можно ограничить трафик более точно (адрес — 10.1.5.0/24).

Наиболее эффективный метод борьбы с IP-спуфингом тот же, что и в случае со сниффингом пакетов: необходимо сделать атаку абсолютно неэффективной. IP-спуфинг может функционировать только при условии, что аутентификация происходит на базе IP-адресов. Поэтому внедрение дополнительных методов аутентификации делает этот вид атак бесполезными. Лучшим видом дополнительной аутентификации является криптографическая. Если она невозможна, хорошие результаты может дать двухфакторная аутентификация с использованием одноразовых паролей.

Отказ в обслуживании (Denial of Service — DoS)

DoS, без всякого сомнения, является наиболее известной формой хакерских атак. Кроме того, против атак такого типа труднее всего создать стопроцентную защиту. Даже среди хакеров атаки DoS считаются тривиальными, а их применение вызывает презрительные усмешки, потому что для организации DoS требуется минимум знаний и умений. Тем не менее, именно простота реализации и огромный причиняемый вред привлекают к DoS пристальное внимание администраторов, отвечающих за сетевую безопасность. Если вы хотите побольше узнать об атаках DoS, вам следует рассмотреть их наиболее известные разновидности, а именно:

- TCP SYN Flood
- Ping of Death
- Tribe Flood Network (TFN) и Tribe Flood Network 2000 (TFN2K)
- Trinco
- Stacheldracht
- Trinity

Отличным источником информации по вопросам безопасности является группа экстренного реагирования на компьютерные проблемы (CERT — Computer Emergency Response Team), опубликовавшая отличную работу по борьбе с атаками DoS. Эту работу можно найти на сайте
http://www.cert.org/tech_tips/denial_of_service.html

Атаки DoS отличаются от атак других типов. Они не нацелены на получение доступа к вашей сети или на получение из этой сети какой-либо информации. Атака DoS делает вашу сеть недоступной для обычного использования за счет превышения допустимых пределов функционирования сети, операционной системы или приложения.
В случае использования некоторых серверных приложений (таких как web-сервер или FTP-сервер) атаки DoS могут заключаться в том, чтобы занять все соединения, доступные для этих приложений, и держать их в занятом состоянии, не допуская обслуживания обычных пользователей. В ходе атак DoS могут использоваться обычные Интернет-протоколы, такие как TCP и ICMP (Internet Control Message Protocol). Большинство атак DoS опирается не на программные ошибки или бреши в системе безопасности, а на общие слабости системной архитектуры. Некоторые атаки сводят к нулю производительность сети, переполняя ее нежелательными и ненужными пакетами или сообщая ложную информацию о текущем состоянии сетевых ресурсов. Этот тип атак трудно предотвратить, так как для этого требуется координация действий с провайдером. Если трафик, предназначенный для переполнения вашей сети, не остановить у провайдера, то на входе в сеть вы это сделать уже не сможете, потому что вся полоса пропускания будет занята. Когда атака этого типа проводится одновременно через множество устройств, мы говорим о распределенной атаке DoS (DDoS — distributed DoS).

Угроза атак типа DoS может снижаться тремя способами:

- Функции анти-спуфинга. Правильная конфигурация функций анти-спуфинга на ваших маршрутизаторах и межсетевых экранах поможет снизить риск DoS. Эти функции, как минимум, должны включать фильтрацию RFC 2827. Если хакер не сможет замаскировать свою истинную личность, он вряд ли решится провести атаку.
- Функции анти-DoS. Правильная конфигурация функций анти-DoS на маршрутизаторах и межсетевых экранах может ограничить эффективность атак. Эти функции часто ограничивают число полуоткрытых каналов в любой момент времени.
- Ограничение объема трафика (traffic rate limiting). Организация может попросить провайдера (ISP) ограничить объем трафика. Этот тип фильтрации позволяет ограничить объем некритического трафика, проходящего по вашей сети. Обычным примером является ограничение объемов трафика ICMP, который используется только для диагностических целей. Атаки (D)DoS часто используют ICMP.

Парольные атаки

Хакеры могут проводить парольные атаки с помощью целого ряда методов, таких как простой перебор (brute force attack), «троянский конь», IP-спуфинг и сниффинг пакетов. Хотя логин и пароль часто можно получить при помощи IP-спуфинга и сниффинга пакетов, хакеры часто пытаются подобрать пароль и логин, используя для этого многочисленные попытки доступа. Такой подход носит название простого перебора (brute force attack).

Часто для такой атаки используется специальная программа, которая пытается получить доступ к ресурсу общего пользования (например, к серверу). Если в результате хакер получает доступ к ресурсам, он получает его на правах обычного пользователя, пароль которого был подобран. Если этот пользователь имеет значительные привилегии доступа, хакер может создать для себя «проход» для будущего доступа, который будет действовать, даже если пользователь изменит свой пароль и логин.

Еще одна проблема возникает, когда пользователи применяют один и тот же (пусть даже очень хороший) пароль для доступа ко многим системам: корпоративной, персональной и системам Интернет. Поскольку устойчивость пароля равна устойчивости самого слабого хоста, хакер, узнавший пароль через этот хост, получает доступ ко всем остальным системам, где используется тот же пароль.

Прежде всего, парольных атак можно избежать, если не пользоваться паролями в текстовой форме. Одноразовые пароли и/или криптографическая аутентификация могут практически свести на нет угрозу таких атак. К сожалению, не все приложения, хосты и устройства поддерживают указанные выше методы аутентификации.

При использовании обычных паролей старайтесь придумать такой пароль, который было бы трудно подобрать. Минимальная длина пароля должна быть не менее восьми символов. Пароль должен включать символы верхнего регистра, цифры и специальные символы (#, %, $ и т. д.). Лучшие пароли трудно подобрать и трудно запомнить, что вынуждает пользователей записывать пароли на бумаге. Чтобы избежать этого, пользователи и администраторы могут поставить себе на пользу ряд последних технологических достижений. Так, например, существуют прикладные программы, шифрующие список паролей, который можно хранить в карманном компьютере. В результате пользователю нужно помнить только один сложный пароль, тогда как все остальные пароли будут надежно защищены приложением. С точки зрения администратора, существует несколько методов борьбы с подбором паролей. Один из них заключается в использовании средства L0phtCrack, которое часто применяют хакеры для подбора паролей в среде Windows NT. Это средство быстро покажет вам, легко ли подобрать пароль, выбранный пользователем. Дополнительную информацию можно получить по адресу http://www.l0phtcrack.com/

Атаки типа Man-in-the-Middle

Для атаки типа Man-in-the-Middle хакеру нужен доступ к пакетам, передаваемым по сети. Такой доступ ко всем пакетам, передаваемым от провайдера в любую другую сеть, может, к примеру, получить сотрудник этого провайдера. Для атак этого типа часто используются снифферы пакетов, транспортные протоколы и протоколы маршрутизации. Атаки проводятся с целью кражи информации, перехвата текущей сессии и получения доступа к частным сетевым ресурсам, для анализа трафика и получения информации о сети и ее пользователях, для проведения атак типа DoS, искажения передаваемых данных и ввода несанкционированной информации в сетевые сессии.

Эффективно бороться с атаками типа Man-in-the-Middle можно только с помощью криптографии. Если хакер перехватит данные зашифрованной сессии, у него на экране появится не перехваченное сообщение, а бессмысленный набор символов. Заметим, что если хакер получит информацию о криптографической сессии (например, ключ сессии), это может сделать возможной атаку Man-in-the-Middle даже в зашифрованной среде.

Атаки на уровне приложений

Атаки на уровне приложений могут проводиться несколькими способами. Самый распространенный из них состоит в использовании хорошо известных слабостей серверного программного обеспечения (sendmail, HTTP, FTP). Используя эти слабости, хакеры могут получить доступ к компьютеру от имени пользователя, работающего с приложением (обычно это бывает не простой пользователь, а привилегированный администратор с правами системного доступа). Сведения об атаках на уровне приложений

широко публикуются, чтобы дать возможность администраторам исправить проблему с помощью корреционных модулей (патчей). К сожалению, многие хакеры также имеют доступ к этим сведениям, что позволяет им учиться.
Главная проблема с атаками на уровне приложений состоит в том, что они часто пользуются портами, которым разрешен проход через межсетевой экран. К примеру, хакер, эксплуатирующий известную слабость web-сервера, часто использует в ходе атаки TCP порт 80. Поскольку web-сервер предоставляет пользователям web-страницы, межсетевой экран должен предоставлять доступ к этому порту. С точки зрения межсетевого экрана, атака рассматривается как стандартный трафик для порта 80.
Полностью исключить атаки на уровне приложений невозможно. Хакеры постоянно открывают и публикуют в Интернет все новые уязвимые места прикладных программ. Самое главное здесь — хорошее системное администрирование. Вот некоторые меры, которые можно предпринять, чтобы снизить уязвимость для атак этого типа:

- Читайте лог-файлы операционных систем и сетевые лог-файлы и/или анализируйте их с помощью специальных аналитических приложений.
- Подпишитесь на услуги по рассылке данных о слабых местах прикладных программ: Bugtrad (http://www.securityfocus.com) и CERT (http://www.cert.com)
- Пользуйтесь самыми свежими версиями операционных систем и приложений и самыми последними коррекционными модулями (патчами).
- Кроме системного администрирования, пользуйтесь системами распознавания атак (IDS). Существуют две взаимодополняющие друг друга технологии IDS:
  - сетевая система IDS (NIDS) отслеживает все пакеты, проходящие через определенный домен. Когда система NIDS видит пакет или серию пакетов, совпадающих с сигнатурой известной или вероятной атаки, она генерирует сигнал тревоги и/или прекращает сессию;
  - хост-система IDS (HIDS) защищает хост с помощью программных агентов. Эта система борется только с атаками против одного хоста.
- В своей работе системы IDS пользуются сигнатурами атак, которые представляют собой профили конкретных атак или типов атак. Сигнатуры определяют условия, при которых трафик считается хакерским. Аналогами IDS в физическом мире можно считать систему предупреждения или камеру наблюдения. Самым большим недостатком IDS является ее способность генерировать сигналы тревоги. Чтобы минимизировать количество ложных сигналов тревоги и добиться корректного функционирования системы IDS в сети, необходима тщательная настройка этой системы.

Сетевая разведка

Сетевой разведкой называется сбор информации о сети с помощью общедоступных данных и приложений. При подготовке атаки против какой-либо сети хакер, как правило, пытается получить о ней как можно больше информации. Сетевая разведка проводится в форме запросов DNS, эхо-тестирования (ping sweep) и сканирования портов. Запросы DNS помогают понять, кто владеет тем или иным доменом и какие адреса этому домену присвоены. Эхо-тестирование (ping sweep) адресов, раскрытых с помощью DNS, позволяет увидеть, какие хосты реально работают в данной среде. Получив список хостов, хакер использует средства сканирования портов, чтобы составить полный список услуг, поддерживаемых этими хостами. И наконец, хакер анализирует характеристики приложений, работающих на хостах. В результате добывается информация, которую можно использовать для взлома.

Полностью избавиться от сетевой разведки невозможно. Если, к примеру, отключить эхо ICMP и эхо-ответ на периферийных маршрутизаторах, вы избавитесь от эхо-тестирования, но потеряете данные, необходимые для диагностики сетевых сбоев. Кроме того, сканировать порты можно и без предварительного эхо-тестирования. Просто это займет больше времени, так как сканировать придется и несуществующие IP-адреса. Системы IDS на уровне сети и хостов обычно хорошо справляются с задачей уведомления администратора о ведущейся сетевой разведке, что позволяет лучше подготовиться к предстоящей атаке и оповестить провайдера (ISP), в сети которого установлена система, проявляющая чрезмерное любопытство.

Злоупотребление доверием

Собственно говоря, этот тип действий не является «атакой» или «штурмом». Он представляет собой злонамеренное использование отношений доверия, существующих в сети. Классическим примером такого злоупотребления является ситуация в периферийной части корпоративной сети. В этом сегменте часто располагаются серверы DNS, SMTP и HTTP. Поскольку все они принадлежат к одному и тому же сегменту, взлом одного из них приводит к взлому и всех остальных, так как эти серверы доверяют другим системам своей сети. Другим примером является система, установленная с внешней стороны межсетевого экрана, имеющая отношения доверия с системой, установленной с его внутренней стороны. В случае взлома внешней системы хакер может использовать отношения доверия для проникновения в систему, защищенную межсетевым экраном.
Риск злоупотребления доверием можно снизить за счет более жесткого контроля уровней доверия в пределах своей сети. Системы, расположенные с внешней стороны межсетевого экрана, никогда не должны пользоваться абсолютным доверием со стороны защищенных экраном систем. Отношения доверия должны ограничиваться определенными протоколами и, по возможности, аутентифицироваться не только по IP-адресам, но и по другим параметрам.

Переадресация портов

Переадресация портов представляет собой разновидность злоупотребления доверием, когда взломанный хост используется для передачи через межсетевой экран трафика, который в противном случае был бы обязательно отбракован. Представим себе межсетевой экран с тремя интерфейсами, к каждому из которых подключен определенный хост. Внешний хост может подключаться к хосту общего доступа (DMZ), но не к хосту, установленному с внутренней стороны межсетевого экрана. Хост общего доступа может подключаться и к внутреннему, и к внешнему хосту. Если хакер захватит хост общего доступа, он сможет установить на нем программное средство, перенаправляющее трафик с внешнего хоста прямо на внутренний хост. Хотя при этом не нарушается ни одно правило, действующее на экране, внешний хост в результате переадресации получает прямой доступ к защищенному хосту. Примером приложения, которое может предоставить такой доступ, является netcat. Более подробную информацию можно получить на сайте http://www.avian.org

Основным способом борьбы с переадресацией портов является использование надежных моделей доверия (см. предыдущий раздел). Кроме того, помешать хакеру установить на хосте свои программные средства может хост-система IDS (HIDS).

Несанкционированный доступ

Несанкционированный доступ не может считаться отдельным типом атаки. Большинство сетевых атак проводятся ради получения несанкционированного доступа. Чтобы подобрать логин Telnet, хакер должен сначала получить подсказку Telnet на своей системе. После подключения к порту Telnet на экране появляется сообщение «authorization required to use this resource» (для пользования этим ресурсом нужна авторизация). Если после этого хакер продолжит попытки доступа, они будут считаться несанкционированными. Источник таких атак может находиться как внутри сети, так и снаружи.

Способы борьбы с несанкционированным доступом достаточно просты. Главным здесь является сокращение или полная ликвидация возможностей хакера по получению доступа к системе с помощью несанкционированного протокола. В качестве примера можно рассмотреть недопущение хакерского доступа к порту Telnet на сервере, который предоставляет web-услуги внешним пользователям. Не имея доступа к этому порту, хакер не сможет его атаковать. Что же касается межсетевого экрана, то его основной задачей является предотвращение самых простых попыток несанкционированного доступа.

Вирусы и приложения типа «троянский конь»

Рабочие станции конечных пользователей очень уязвимы для вирусов и «троянских коней». Вирусами называются вредоносные программы, которые внедряются в другие программы для выполнения определенной нежелательной функции на рабочей станции конечного пользователя. В качестве примера можно привести вирус, который прописывается в файле command.com (главном интерпретаторе систем Windows) и стирает другие файлы, а также заражает все другие найденные им версии command.com. «Троянский конь» — это не программная вставка, а настоящая программа, которая выглядит как полезное приложение, а на деле выполняет вредную роль. Примером типичного «троянского коня» является программа, которая выглядит, как простая игра для рабочей станции пользователя. Однако пока пользователь играет в игру, программа отправляет свою копию по электронной почте каждому абоненту, занесенному в адресную книгу этого пользователя. Все абоненты получают по почте игру, вызывая ее дальнейшее распространение.

Борьба с вирусами и «троянскими конями» ведется с помощью эффективного антивирусного программного обеспечения, работающего на пользовательском уровне и, возможно, на уровне сети. Антивирусные средства обнаруживают большинство вирусов и «троянских коней» и пресекают их распространение. Получение самой свежей информации о вирусах поможет эффективнее бороться с ними. По мере появления новых вирусов и «троянских коней» предприятие должно устанавливать новые версии антивирусных средств и приложений.

Что такое политика безопасности?

Политикой безопасности можно назвать и простые правила использования сетевых ресурсов, и детальные описания всех соединений и их особенностей, занимающие сотни страниц. Определение RFC 2196 (которое считается несколько узким и ограниченным) описывает политику безопасности следующим образом:

«Политика безопасности — это формальное изложение правил, которым должны подчиняться лица, получающие доступ к корпоративной технологии и информации».

Подробности разработки политики безопасности выходят за рамки настоящего документа. В RFC 2196 имеется полезная информация по этому вопросу. Кроме этого, с инструкциями и примерами политики безопасности можно познакомиться на следующих web-страницах:

- RFC 2196 «Site Security Handbook» (Настольная книга по сетевой безопасности) — http://www.ietf.org/rfc/rfc2196.txt
- Пример политики безопасности из университета штата Иллинойс — http://www.aits.uillinois.edu/security/securestandards.html
- Проектирование и реализация корпоративной политики безопасности — http://www.knowcisco.com/content/1578700434/ch06.shtml

Необходимость политики безопасности

Важно понять, что сетевая безопасность — это эволюционный процесс. Нет ни одного продукта, способного предоставить корпорации полную безопасность. Надежная защита сети достигается сочетанием продуктов и услуг, а также грамотной политикой безопасности и ее соблюдением всеми сотрудниками сверху донизу. Можно заметить, что правильная политика безопасности даже без выделенных средств защиты дает лучшие результаты, чем средства защиты без политики безопасности.

Приложение C. Архитектурная классификация

Сервер приложений. Напрямую или косвенно предоставляет услуги конечным пользователям, работающим в корпорации. В число услуг могут входить: поддержка рабочих потоков, офисные услуги общего характера и приложения безопасности.

Межсетевой экран (с учетом состояний). Устройство фильтрации пакетов с учетом состояний соединений. Поддерживает таблицы состояний для протоколов, работающих по стандартам IP. Трафик пропускается через межсетевой экран только в случае его соответствия настройкам управления доступом, или если этот трафик является частью сессии, которая уже разрешена в таблице состояний.

Система HIDS. Система обнаружения атак на уровне хоста. Программное приложение, отслеживающее активность на одном определенном хосте. Способы отслеживания могут включать проверку вызовов со стороны операционных систем и приложений, проверку лог-файлов, мониторинг информации о файловой системе и сетевых соединениях.

Система NIDS. Система обнаружения атак на уровне сети. Как правило, функционирует, не нарушая нормальной работы сети. Записывает трафик, проходящий через сегмент локальной сети и сравнивает его в реальном времени с известными сигнатурами атак. Эти сигнатуры могут быть атомарными (сигнатура индивидуального пакета или направления) или комплексными (многопакетными), которым необходимы таблицы состояний и отслеживание приложений на Уровне 7.

Межсетевой экран IOS. Межсетевой экран для фильтрации пакетов с учетом состояний соединений. Работает под управлением операционной системы Cisco IOS.

Маршрутизатор IOS. Широкий круг гибких сетевых устройств, предоставляющих разнообразные услуги маршрутизации и безопасности для всех работающих элементов. Большинство этих устройств имеют модульную конструкцию и ряд физических интерфейсов для подключения к локальных и глобальным сетям.

Коммутатор Уровня 2. Предоставляет полосу пропускания и услуги виртуальных локальных сетей (VLAN) сетевым элементам на уровне Ethernet. Обычно эти устройства поддерживают индивидуальные коммутируемые порты Ethernet 10/100 и Gigabit Ethernet, транкинг VLAN и фильтрацию на Уровне 2.

Коммутатор Уровня 3. Поддерживает те же функции, что и коммутатор Уровня 2, плюс функции маршрутизации, качества услуг (QoS) и безопасности. Коммутаторы Уровня 3 часто имеют выделенные процессоры для поддержки специальных функций.

Сервер управления. Предоставляет услуги сетевого управления операторам корпоративных сетей. Эти услуги включают общее управление конфигурацией, мониторинг устройств сетевой безопасности и непосредственное исполнение функций безопасности.

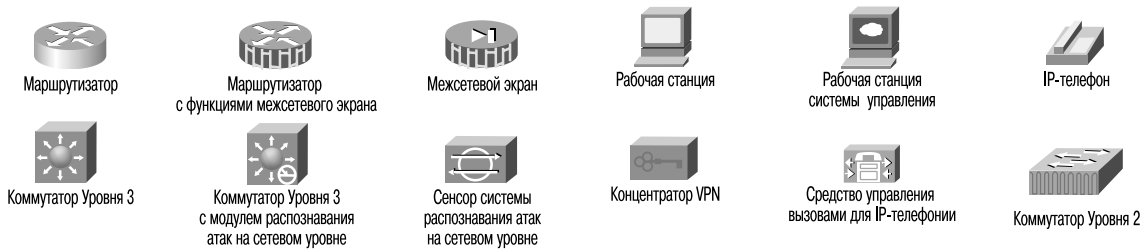
Сервер фильтрации содержания SMTP. Прикладная программа, обычно работающая на внешнем сервере SMTP. Проводит мониторинг содержания входящих и исходящих сообщений электронной почты (включая присоединенные файлы). Принимает одно из следующих решений: передать сообщение без изменений, передать сообщение с предупреждением, запретить передачу сообщения.

Сервер фильтрации URL. Прикладная программа, обычно работающая на отдельном сервере. Проводит мониторинг запросов URL, передаваемых сетевым устройством, и информирует это устройство о том, будет ли запрос передан в Интернет. Этот сервер позволяет корпорации реализовать политику безопасности, определяющую, какие категории Интернет-сайтов являются несанкционированными.

Устройство терминирования VPN. Терминирует туннели IPSec, используемые для связи между сайтами или для сетей VPN с удаленным доступом. Для поддержки функциональности, сравнимой с функциями классических каналов глобальных сетей (WAN) или модемного доступа, это устройство должно предоставлять дополнительные услуги.

Рабочая станция или пользовательский терминал. Любое устройство, подключенное к сети и непосредственно используемое конечным пользователем. В число этих устройств входят персональные компьютеры, IP-телефоны, беспроводные устройства и т. д.

Условные обозначения



Ссылки

Руководства Cisco по конфигурации для программных продуктов в области обеспечения безопасности и для соответствующих программных компонентов

Cisco SAFE — http://www.cisco.com/go/safe
Improving Security on Cisco Routers — http://www.cisco.com/warp/customer/707/21.html
PIX Firewall — http://www.cisco.com/warp/public/cc/pd/fw/sqfw500/
Cisco IOS Firewall Feature Set — http://www.cisco.com/warp/public/cc/pd/iosw/ioft/iofwft/
Cisco Secure IDS — http://www.cisco.com/warp/public/cc/pd/sqsw/sqidsz/
Cisco Secure Scanner — http://www.cisco.com/warp/public/cc/pd/sqsw/nesn/
Cisco Secure Access Control Server — http://www.cisco.com/warp/public/cc/pd/sqsw/sq/
Cisco VPN 3000 Concentrator — http://www.cisco.com/warp/public/cc/pd/hb/vp3000/
Catalyst 6000 series — http://www.cisco.com/warp/public/cc/pd/si/casi/ca6000/
NetFlow White Paper — http://wwwin.cisco.com/Mkt/cc/cisco/mkt/core/netflow/nflow_wp.htm

Интернет-ссылки (RFC)

RFC 2196 «Site Security Handbook» (настольная книга безопасности сайтов) — http://www.ietf.org/rfc/rfc2196.txt
RFC 1918 «Address Allocation for Private Internets» (распределение адресов в частных сетях Интернет) — http://www.ietf.org/rfc/rfc1918.txt
RFC 2827 «Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing» (фильтрация на входе в сеть: борьба с атаками DoS, использующими чужие адреса) — http://www.ietf.org/rfc/rfc2827.txt

Прочие ссылки

VLAN Security Test Report (отчет о безопасности сетей VLAN) —
http://www.sans.org/newlook/resources/IDFAQ/vlan.htm
AntiSniff (антиснифферы) — http://www.l0pht.com/antisniff/
L0phtCrack – http://www.l0pht.com/l0phtcrack/
Denial of Service Attacks (атаки DoS) — http://www.cert.org/tech_tips/denial_of_service.html
Computer Emergency Response Team (CERT — группа экстренного реагирования на компьютерные проблемы) – http://www.cert.org
Security Focus (Bugtraq) — http://www.securityfocus.com
Avian Research (netcat) — http://www.avian.org
University of Illinois Security Policy (политика безопасности университета штата Иллинойс) — http://www.aits.uillinois.edu/security/securestandards.html
Design and Implementation of the Corporate Security Policy (разработка и внедрение корпоративной политики безопасности) — http://www.knowcisco.com/content/1578700434/ch06.shtml

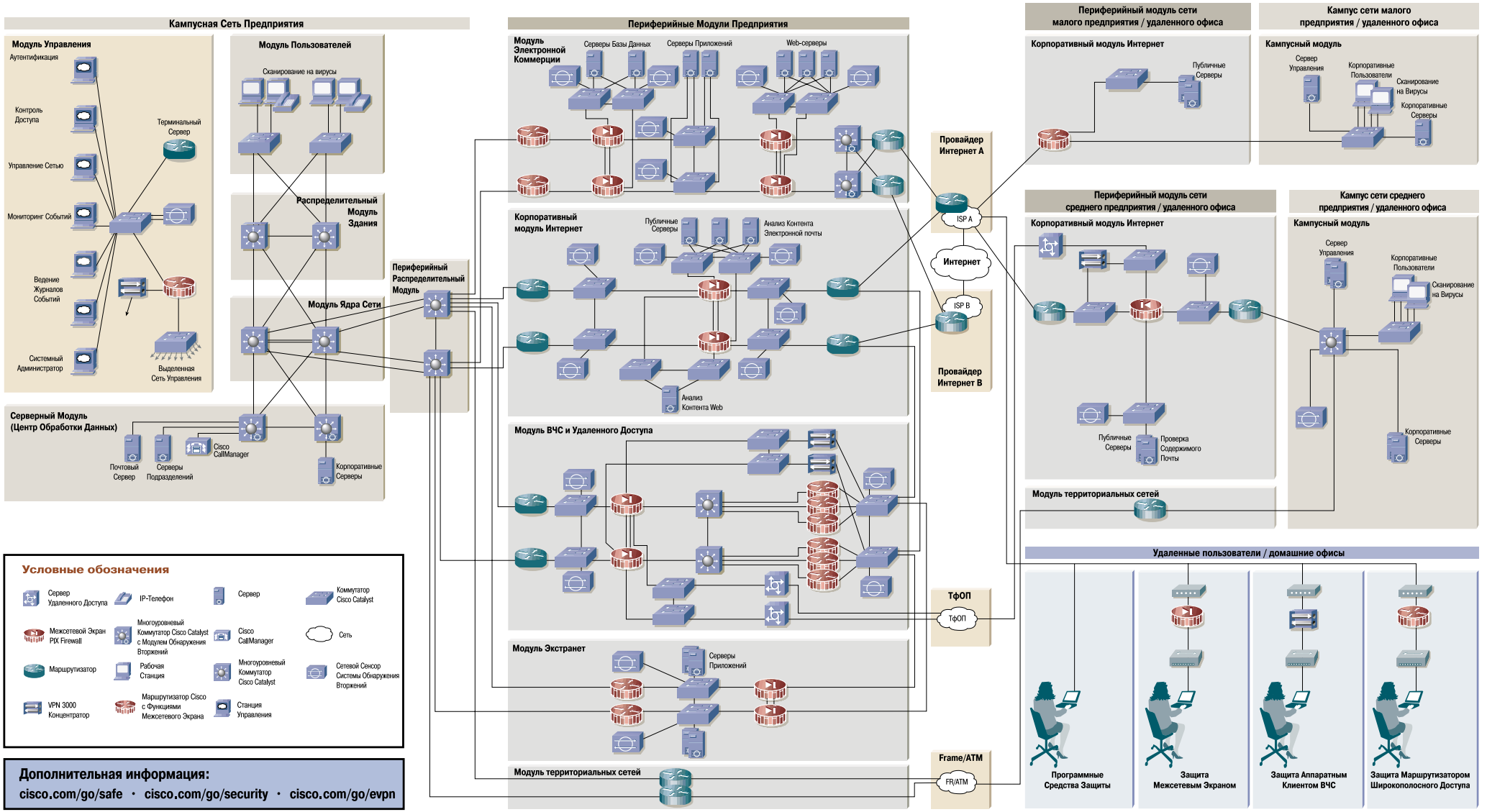
Ссылки на продукты партнеров

Система одноразовых паролей RSA SecureID OTP System — http://www.rsasecurity.com/products/securid/
Система фильтрации содержания электронной почты Content Technologies MIMESweeper Email Filtering System – http://www.contenttechnologies.com
Система фильтрации адресов URL Websense URL Filtering — http://www.websense.com/products/integrations/ciscopix.cfm
Средство анализа системной информации (Syslog) netForensics Syslog Analysis — http://www.netforensics.com/

Cisco IOS™ TECHNOLOGIES

Составитель: М.Кадер

Архитектура SAFE
Основа Безопасного Электронного Бизнеса



Cisco Systems
Россия, 113054 Москва
бизнес центр “Риверсайд Тауэрз”
Космодамианская наб., 52
Стр. 1, 4-й этаж
Тел.: +7 (095) 961 14 10
Факс: +7 (095) 961 14 69
Internet: www.cisco.ru
www.cisco.com

Cisco Systems
Казахстан, 480099 Алматы
бизнес центр “Самал 2”
Ул. О. Жолдасбекова, 97
блок А2, этаж 14
Тел.: +7 (3272) 58 46 58
Факс: +7 (3272) 58 46 60
Internet: www.cisco.ru
www.cisco.com

Cisco Systems
Украина, 252004 Киев
бизнес центр “Горайзон Тауэрз”
Ул. Шовковична, 42-44, этаж 9
Тел.: (044) 490 36 00
Факс: (044) 490 56 66
Internet: www.cisco.ua
www.cisco.com

Cisco Systems has more than 200 offices in the following countries. Addresses, phone numbers, and fax numbers are listed on the **Cisco Connection Online Web site at http://www.cisco.com. //www.cisco.ru.**

Argentina • Australia • Austria • Belgium • Brazil • Canada • Chile • China (PRC) • Colombia • Costa Rica • Czech Republic • Denmark England • Finland • France • Germany • Greece • Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxemburg • Malaysia Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Russia • Saudi Arabia • Scotland • Singapore South Africa • Spain • Sweden • Switzerland • Taiwan, ROC • Thailand • Turkey • United Arab Emirates • United States • Venezuela