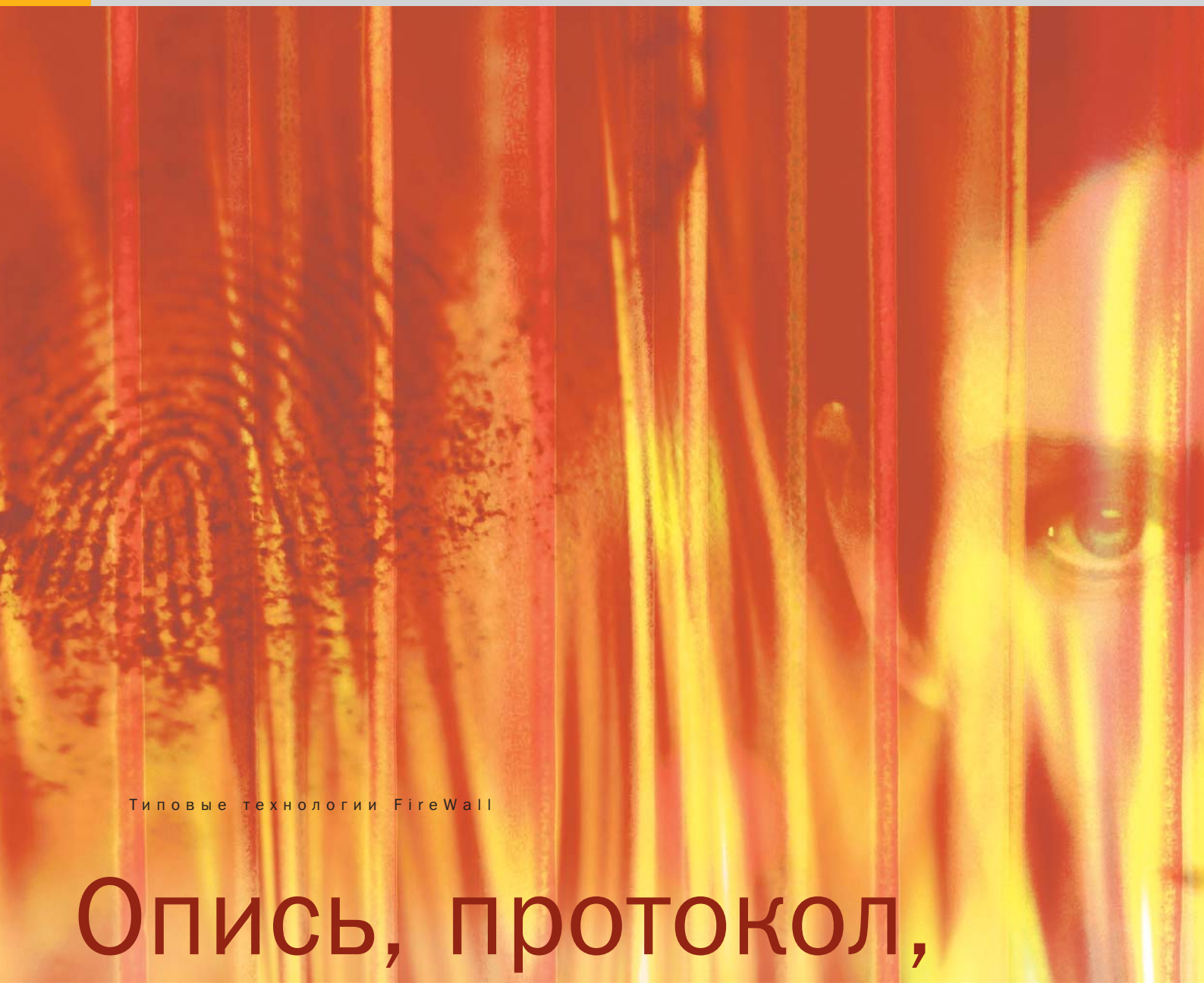


Типовые технологии FireWall

Опись, протокол, отпечатки пальцев...

На страницах нашего журнала уже неоднократно рассказывалось о технологиях сетевой безопасности. Сейчас мы не преследуем цели детализировать сказанное ранее, а хотим подойти к проблеме с практической точки зрения, рассмотрев ее на примере продукции компании Cisco Systems.

Современный Firewall — это набор аппаратно-программных компонентов для реализации определенной политики доступа к сетевым ресурсам. Брандмауэр, в зависимости от способа задания правил доступа и уровня модели OSI (операционной системы), в которой он функционирует, можно условно отнести к одной из четырех категорий: со статической фильтрацией пакетов (packet-filtering), сеансового (circuit-level), прикладного (application-level) и экспертного (stateful inspection) уровней.

Правила доступа указывают на необходимость разрешить (permit) или запретить (deny) прохождение входящих или исходящих пакетов. Правила могут быть привязаны к соответствующему сетевому интерфейсу и управлять трафиком статически либо динамически. Во втором случае таблица правил может изменяться в зависимости от содержания анализируемых пакетов, временных параметров и прочих факторов.

Статическая фильтрация пакетов

Брандмауэр с фильтрацией пакетов является средством, позволяющим в соответствии с некоторым набором статических правил фильтровать трафик. Обращайте внимание на информацию, содержащуюся »

» в заголовках пакетов IP, TCP, UDP и т. д. При этом обычно проверяются адреса и порты отправителя и получателя и информация о протоколе или приложении.

Функцию фильтрации в настоящее время обеспечивают в той или иной степени большинство известных маршрутизаторов от Cisco Systems, Allied Telesyn, 3Com и других производителей. Главные преимущества таких брандмауэров — невысокая стоимость и минимальные требования к аппаратным ресурсам.

Защита на сеансовом уровне

Подобные технологии позволяют отслеживать квитирование (статусные отношения) связи между авторизованным клиентом и сервисом TCP, определяя, является ли запрашиваемый сеанс допустимым. Таблицы доступа создаются и обновляются динамически в соответствии с заданными правилами и прохождением пакетов с флагами квитирования SYN, ACK, FIN, RST. Сеанс разрешается в том случае, если процедура квитирования происходит успешно и логически завершена, а хост, инициирующий соединение, действительно существует и корректно функционирует.

Недостатком такого подхода является возможность защиты только по протоколу TCP. Это связано с тем, что обмен информацией по протоколам UDP или ICMP не гарантирует доставку и не создает сеансов.

Следовательно, при использовании злоумышленником этих протоколов попытки проникновения в сеть невозможно адекватно идентифицировать, а значит, и предотвратить.

Защита на уровне приложений

Данный способ защиты позволяет в процессе анализа пакетов фильтровать отдельные виды команд или данных в протоколах прикладного уровня. Например, можно предотвратить запись на корпоративный FTP-сервер путем запрещения в фильтрах команды PUT, что уменьшит вероятность переполнения дискового пространства. В качестве другого примера можно привести возможность фильтрации HTTP-трафика в соответствии с «черным» или «белым» списками соответствующих URL-адресов или ключевых слов на web-страницах.

Брандмауэры экспертного уровня

На данном этапе развития технологий защиты данные брандмауэры сочетают в себе взаимодействие всех вышеперечисленных способов на основе специальных экспертных алгоритмов.

По сравнению с обычными брандмауэрами их можно сопоставить, пожалуй, не столько с пассивным заградительным экраном, сколько с организованным противопожарным подразделением, которое на основании анализа опасности и текущего состояния ситуации принимает решение о необходимых в данной ситуации активных действиях по ликвидации пожара и соответствующих профилактических мероприятиях.

Данные устройства являются самыми надежными, но, как следствие, и самыми дорогостоящими и максимально требовательными к аппаратным ресурсам.

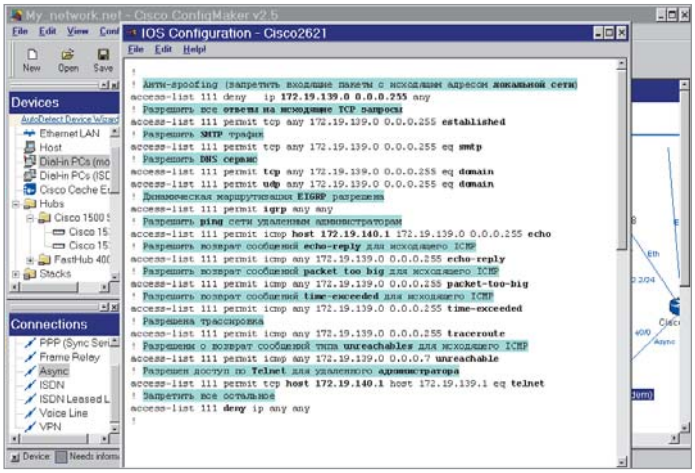
Брандмауэр с использованием продукции Cisco Systems

Не каждая организация может самостоятельно заниматься созданием брандмауэра, то есть объединением имеющихся программных компонентов и оборудования или написанием программ с нуля. В то же самое время существует ряд производителей, предлагающих разнообразные средства, позволяющие обеспечить безопасность корпоративных сетей.

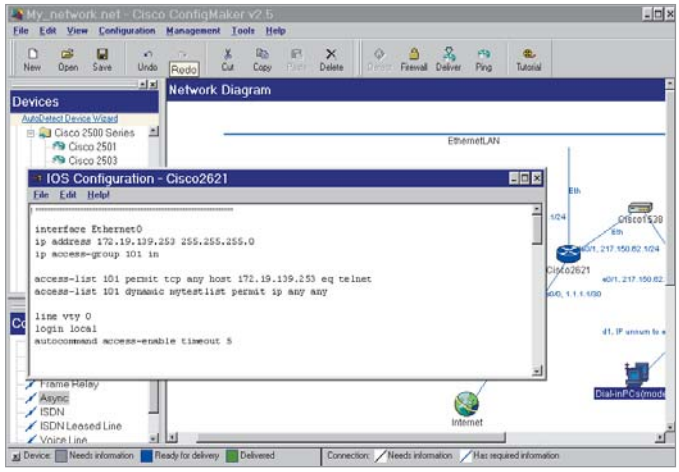
По данным статистических исследований, более 80% трафика Интернета обрабатывается оборудованием компании Cisco Systems (http://www.cisco.com/ru). Решения Cisco Systems подкреплены солидной репутацией, стабильным финансовым положением и взаимоотношениями с респектабельными заказчиками. В октябре 1998 года Cisco Systems получила сертификаты Государственного комитета по стандартизации РФ на оборудование, которое поставляется в Россию. Также компания сертифицировала свою продукцию в Государственном комитете связи и информатизации РФ: список оборудования, сертифицированного для применения во взаимоувязанной сети связи России, состоит из 33 позиций.

Кроме того, программно-аппаратный комплекс Cisco PIX Firewall + CiscoSecure прошел сертификацию Государственной Технической Комиссии РФ по требованиям безопасности на территории Российской Федерации (комплекс требований к аппаратуре и программному обеспечению, применяющемуся в сетях при доступе к информации конфиденциального характера).

Давайте рассмотрим основные механизмы организации защиты на примере продуктов Cisco Systems. »



▲ Рис. 1. Список статических правил фильтрации



▲ Рис. 2. После локальной авторизации возможен полный доступ к внешним ресурсам

Access Lists (статические списки доступа)

В соответствии с данной технологией для каждого сетевого интерфейса можно назначить по два списка доступа (входящий и исходящий); каждый такой список состоит из правил permit или deny с указанием соответствующих адресов, портов и протоколов. Маска подсети задается в инверсной форме. Мы рассмотрим расширенные списки доступа (Extended access lists), которые по сравнению со стандартными имеют гораздо более гибкие возможности. Формат правил для IP выглядит следующим образом:

```
Access-list {number} {permit | deny} {protocol } {source s_mask | any} {dest d_mask | any} [tos tos]
```

Здесь настраиваются следующие параметры: number — номер списка (от 100 до 199); permit/deny — правило доступа; protocol — протокол (ip, tcp, udp, icmp, igmp, gre, igrp, ospf или номер протокола); sourse и dest — адреса отправителя и получателя; s_mask и d_mask — инверсные маски; tos — уровень сервиса (от 0 до 15).

В правилах для ICMP присутствует параметр icmp_type — название icmp-события:

```
Access-list {number} {permit | deny} icmp {source s_mask | any} {dest d_mask | any} [icmp_type] [tos tos]
```

Для TCP/UDP можно указать также operator — логическая операция (lt, gt, eq, neg, range); s_port, d_port — порты источника и приемника; established — ключ для пакетов с флагами SYN или RST (только для TCP).

```
Access-list {number} {permit | deny} tcp {source s_mask | any} [operator s_port] {dest d_mask | any} [operator d_port] [established] [tos tos]
```

Метод достаточно тривиален, и поэтому я, не вдаваясь в подробности, приведу лишь пример, демонстрирующий неплохой стиль защиты (рис. 1). Здесь мы имеем сеть класса «С» 172.19.139.0 с SMTP-сервером 172.19.139.1, который должен быть доступен для удаленного администрирования с хоста 172.19.140.1.

После создания списка необходимо применить действие его правил к интерфейсу, в данном случае S1, соединяющему сеть с интернет-провайдером:

```
interface Serial
ip address 172. 19. 150. 253
           255. 255. 255. 252
ip-access-group 111 in
```

Как видите, все просто. Вроде бы ни одного лишнего входящего пакета, и многие системные администраторы считают данное средство панацеей от всех бед. Но у хакеров даже в данном случае есть все возможности нападения на хост 172.19.139.1 по протоколу SMTP. Многие его реализации имеют бреши в защите. Можно даже атаковать всю сеть по протоколу DNS. А представьте себе ситуацию, когда вы поддерживаете публичные FTP-сервер, виртуальные www-хосты, удаленный доступ на NT-сервер, ICQ и множество Unix-сервисов. Ситуация может еще в большей степени усложниться, если вы обмениваетесь данными с удаленными филиалами или деловыми партнерами.

Lock-And-Key (динамические списки доступа)

Динамические списки позволяют создавать временный доступ к определенным ресурсам, что не позволяет злоумышленнику действовать методом перебора паролей, а также ограничивает время авторизации и последующего доступа к ресурсам. Метод предполагает комбинацию как статических, так и динамических списков доступа. Данную технологию рекомендуется применять для временного открытия локальных или удаленных ресурсов только авторизованным пользователям.

Для начала давайте разрешим полный доступ к внешним ресурсам после локальной авторизации на роутере (рис. 2).

Первая запись в списке доступа 101 разрешает вход на порт Ethernet0 только по Telnet. Вторая всегда игнорируется до момента успешной авторизации, после которой выполняется autocommand и сессия Telnet обрывается. Autocommand создает временный доступ на Ethernet 0, основанный на правиле mytestlist. Этот временный доступ будет существовать 5 мин. (timeout 5).

» Следующий пример позволяет удаленному диалап-администратору после авторизации на сервере Tacacs получить полный доступ ко всем локальным ресурсам (рис. 3). Примеры наглядно демонстрируют недостатки технологии. После авторизации интерфейс временно открывается на фиксированное время, что позволяет злоумышленнику использовать атаки с подменой адресов и различные виды DoS-атак. Поэтому Lock-And-Key рекомендуется применять для временных Point-to-Point соединений (по DialUp, ISDN).

Reflexive Access Lists (фильтрация на уровне IP-сессий)

Данные правила позволяют фильтровать IP-трафик на основе информации, полученной на уровне сеансов с учетом их инициатора. Эту технологию возможно использовать только совместно с именованными списками доступа (Named Extended Assess-lists).

Такие фильтры позволяют определять временные правила доступа, которые вступают в действие только при открытии новой IP-сессии и ликвидируются при ее закрытии. Таким образом, время атаки ограничено. Трафик пропускается только в том случае, если он принадлежит сессии. Данные фильтры привязаны не к интерфейсам, а к имени листа, закрепленного за интерфейсом. В правилах может использоваться только директива permit. Сессия отслеживается по портам и адресам источника и адресата, а также флагам и номерам пакетов, что позволяет определить понятие виртуальной сессии не только для TCP, но также для UDP- и ICMP-трафика.

Для TCP-пакетов правило удаляется через 5 сек. после пакета с флагом FIN (завершение с возможностью восстановления) либо немедленно при получении флага RST (абсолютное завершение).

Для UDP и ICMP обрыв соединения происходит по timeout в случае, если принимается решение об окончании сессии. Таким образом, в технологии Reflexive Access List объединяются свойства как сеансового, так и экспертного способов защиты.

Предположим, на интерфейс Serial1 назначается reflect-список с именем outboundfilters для анализа исходящих сессий TCP, UDP и ICMP. Набор правил в данном случае имеет название chk_traffic. При этом для UDP и ICMP определяется максимальное время сессии, равное 120 сек. при отсутствии ответных пакетов. Для этого же интерфейса определяется список inboundfilters для фильтрации входящего трафика. В случае наличия корректной сессии к статическим правилам расширенного списка inboundfilters временно добавляется набор правил chk_traffic, разрешающий только ответный входящий трафик (рис. 4).

Этот пример — демонстрация возможностей защиты от Spoofing- и DoS-атак, динамической фильтрации входящего трафика, а также совместного использования статических и динамических списков доступа. По мнению специалистов Cisco Systems, описанный метод не всегда эффективен при наличии в сети демилитаризованной зоны, содержащей публичные сервисы.

TCP Intercept (TCP перехват)

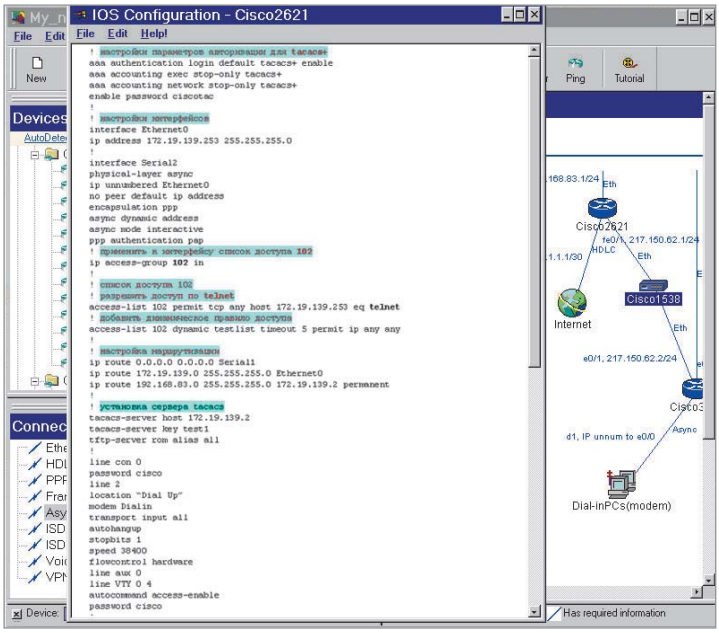
Технология перехвата эффективно предохраняет от SYN-флудинга (одной из разновидности DoS-атак). При реализации данной атаки хакер забивает локальные ресурсы пакетами с некорректными обратными адресами, в результате чего открывается множество сессий, и атакуемый сервер не справляется со своими задачами.

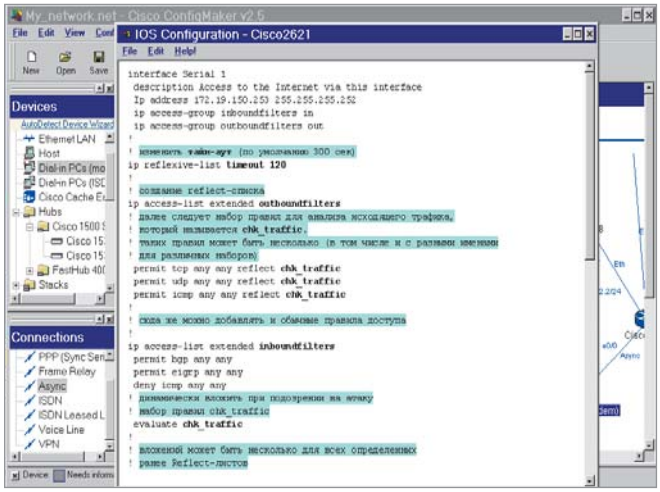
Интересным свойством данной технологии является то, что режимы ее установок не привязаны к конкретному интерфейсу и функционируют глобально. Фильтрация осуществляется методом перехвата входящих TCP-пакетов с установленным SYN-флагом, если аналогичные уже приходили с недоступного в данный момент IP-адреса. Отслеживание прохождения некорректных пакетов может проходить в одном из двух режимов: перехвата и наблюдения.

Заключение

Итак, мы рассмотрели современные виды обеспечения сетевой безопасности и поговорили о механизмах организации защиты на примере технологий от Cisco Systems. Неосвещенными остались вопросы последовательности конфигурирования оборудования, и об этом мы поговорим в следующий раз.

■ ■ ■ Юрий Калганников,
Анастасия Пшеницына





▲ Рис. 4. Правила фильтрации на уровне IP-сессий

◄ Рис. 3. Диалап-администратор после авторизации на сервере Tacacs получит полный доступ к локальным ресурсам