БЕЗОПАСНОСТЬ СЕТЕВОГО ЦЕНТРА ОБРАБОТКИ ДАННЫХ

В корпоративных центрах обработки данных содержатся ресурсы, приложения и информация, которые часто становятся целью сетевых атак злоумышленников. Оконечные устройства, например, серверы центров обработки данных, являются "лакомым кусочком" для злоумышленника и потому нуждаются в надежной защите. Атаки против групп серверов могут привести к нарушению работоспособности приложений электронной коммерции и приложений типа B2B, а также к краже конфиденциальной информации или информации, представляющей для организации особую ценность. Для того чтобы снизить вероятность катастрофических последствий, организациям необходимо обеспечить надежную защиту как локальных сетей, так и сетей хранения данных (SAN).

Сети SAN традиционно считались относительно безопасными, в первую очередь потому, что способ подключения SAN предусматривает весьма ограниченный доступ к ним со стороны других компонентов центра данных – по существу, SAN представляет собой изолированную сеть. Такое представление является сильно упрощенным; один-единственный пораженный хост может потенциально заблокировать работу других хостов, подключенных к сети SAN, получить несанкционированный доступ к данным в пределах SAN и, наконец, обойти существующие межсетевые экраны и системы обнаружения вторжений в случае использования каналов IP поверх соединений Fibre Channel.

Кроме того, нередко встречаются сети SAN, которые простираются за физические пределы центров обработки данных с целью обеспечения непрерывности бизнеса и скорейшего восстановления после аварий. Распространение таких технологий, как SCSI over IP (iSCSI) и Fibre Channel over IP (FCIP), использующих протокол TCP/IP в качестве транспорта, обуславливает требования по надежной защите SAN, т.к. эти технологии предполагают передачу конфиденциальной информации по сетям передачи данных общего пользования.

В этом документе рассматриваются технологии, реализованные в продуктах Cisco для коммутации в рамках ЦОД класса "премьер" (коммутаторах семейства Cisco Catalyst 6500 Series и коммутаторах класса "директор" семейства Cisco MDS 9000), и решениях Cisco, которые позволяет сделать группы серверов менее уязвимыми перед сетевыми атаками, направленными на локальные сети и сети SAN.

МЕХАНИЗМЫ ОСУЩЕСТВЛЕНИЯ СЕТЕВЫХ АТАК

Понимание механизмов проведения сетевых атак двух наиболее распространенных типов позволяет лучше оценить, насколько решения Cisco® для центров обработки данных смягчают последствия таких атак или предотвращают их осуществление.

В данном документе рассматриваются атаки двух типов: кража данных и распространение Интернет-червей. Атаки первого типа направлены на кражу информации; целью атак второго типа является блокирование нормальной работы приложений, поэтому их можно классифицировать как атаки типа "отказ в обслуживании" (DoS).

Кража данных

Атаки, направленные на похищение конфиденциальной информации, как правило, начинаются с этапа зондирования и сканирования целевой системы с целью сбора сведений о ней. Злоумышленники могут использовать общедоступные инструменты, например, nmap (http://www.insecure. org) для получения информации об операционной системе целевого хоста (зондирование), а также сервисов, работающих на сервере (сканирование).

Следующий этап атаки заключается в идентификации уязвимостей удаленной системы. Злоумышленники могут использовать общедоступные инструменты, например, nessus (http://www.nessus.org) для выявления уязвимостей, которыми можно воспользоваться при осуществлении атаки.

Вслед за этим злоумышленники могут внедрить на атакуемый хост фрагмент программного кода, который будет выполнять нужные им функции (троянская программа). На этом этапе злоумышленник получает управление сервером ЦОД, и с помощью этого сервера может получать доступ к другим хостам, на которых хранятся конфиденциальные данные (эксплуатация доверительных отношений) или

установить необходимые программные инструменты для проведения атак со стороны группы серверов.

На этом этапе злоумышленник может действовать либо в локальной сети, либо в сети SAN. Если взломанный сервер подключен к локальной сети, злоумышленник может проводить атаки уровня 2 (Ethernet) для перехвата IP-трафика, включая трафик storage-over-IP (т.е. трафика, используемого для обмена данными с хранилищами по IP-сети). Для подмены информации о соответствии IP- и MAC-адресов злоумышленник может использовать атаки с опережающим ответом, использующие уязвимости протокола ARP, (ARP-spoofing) или выполнить лавинообразную генерацию трафика на уровне 2 (MAC flooding). Если взломанный сервер подключен к сети SAN с использованием HBA-адаптера, то злоумышленник может получить доступ к данным, хранящимся в сети SAN, с помощью атак, использующих подмену глобальных имен (WWN-spoofing), или осуществить доступ к другим серверам по каналам IPFC.

Другой хорошо известный метод получения управления сервером заключается во взломе TCP-сеанса. Успешная реализация таких способов атаки, как подмена IP-адреса источника пакетов, эксплуатация доверительных отношений и подбор ISN-номера TCP-соединения позволяет получить управление серверами с предсказуемым ISN-номером TCP-соединения.

Интернет-черви

Некоторые атаки, например, атаки DoS и эпидемии Интернет-червей, направлены на блокирование доступа пользователей к приложениям. В процессе проведения этих атак генерируется большой объем трафика и множество запросов на установление соединения (лавины SYN-запросов) или запросов, требующих обработки сервером (лавины ping), что приводит к истощению ресурсов серверов. Дополнительные сложности создаются тем фактом, что Интернет-черви тиражируют себя самостоятельно, безо всякого человеческого участия.

Высокая скорость распространения делает эпидемии Интернет-червей особенно опасными. Например, известно, что во время атаки червя "SQL slammer" число зараженных хостов удваивалось каждые 8,5 секунд, а генерируемый ими трафик мог вырастать до таких масштабов, что полностью "заполнял" канал с пропускной способностью 1 Гбит/с менее, чем за одну минуту. Атаки червей на группу серверов влекут за собой проблемы двух типов: взломанные серверы и неработоспособные сетевые соединения.

В последнее время миру пришлось столкнуться с несколькими эпидемиями Интернет-червей, например, Code Red (CERT Advisory CA-2001-19), Nimda (CERT Advisory CA-2001-26 Nimda Worm), SQL slammer (CERT Advisory CA-2003-04) и другие. Каждый Интернет-червь использует особую уязвимость, но при этом все Интернет-черви обладают некоторыми общими свойствами. Высокоуровневое описание одного Интернет-червя помогает лучше понять, как следует защищать группу серверов от атак других Интернет-червей.

Например, Code Red рассылает запросы на установление TCP-соединения с портом 80 на случайные IP-адреса, выискивая уязвимый хост. Затем Code Red использует конкретную уязвимость Microsoft IIS, связанную с переполнением буфера (Microsoft Security Bulletin MS01-033). После того, как уязвимый хост найден, Code Red вызывает переполнение буфера на сервере и устанавливает на сервере троянскую программу, которая в свою очередь атакует другие серверы.

Примечание: Информация о последних эпидемиях Интернет-червей предоставляется организацией CAIDA: http: //www.caida.org/analysis/security/.

ОТ ЧЕГО ЖЕ СЛЕДУЕТ ЗАЩИЩАТЬСЯ?

Сведения об уязвимостях операционных систем регулярно публикуются в открытых источниках информации. Инструменты осуществления мощных атак также общедоступны, а их интерфейс становится все более простым. Это означает, что каждый пользователь, обладающий доступом в сеть Интернет, может найти достаточно количество инструментов для взлома и информацию о большом количестве уязвимостей, которыми можно воспользоваться.

В ходе исследований, проведенных в 2002 году Институтом компьютерной безопасности (CSI) и ФБР, респонденты отмечали, что примерно 40 - 45 процентов всех атак на их системы были инициированы источниками, находящимися во внутренней сети. Результаты исследований отчетливо свидетельствуют о том, что внутренние устройства сети и приложения, функционирующие во внутренней сети, нуждаются в серьезной защите от атак и попыток несанкционированного доступа.

Архитектура центров обработки данных должна обеспечивать защиту от атак, исходящих от внешних клиентских компьютеров (из Интернет), внутренних клиентских компьютеров и взломанных серверов.

ИНСТРУМЕНТЫ ДЛЯ ЛОКАЛЬНЫХ СЕТЕЙ

Коммутаторы семейства Cisco Catalyst 6500 Series, сервисные модули Catalyst 6500 Series и продукты Cisco для обнаружения вторжений реализуют различные функции обеспечения безопасности, в частности:

- **Контролируемый доступ к группе серверов.** Сегодня большинство приложений выполнены в соответствии с многоуровневой архитектурой. Многоуровневая модель предусматривает распределение различных функций между отдельными серверами. Обычно выделают функции

представления, функции бизнес-логики и функции для работы с базами данных. Использование многоуровневой архитектуры при построении группы серверов позволяет обеспечить дополнительный уровень безопасности: клиент сможет нарушить безопасность web-сервера, но не сможет получить доступ ни к самому приложению, ни к базе данных. Разделение между уровнями обеспечивается путем использования сетей VLAN. В каналах клиент-сервер и сервер-сервер допускается прохождение только легитимного трафика (обеспечивается за счет использования таких технологий, как списки контроля доступа (ACL), сети VLAN и частные сети VLAN, причем все эти технологии реализованы на аппаратном уровне и работают на скорости среды передачи).

- **Защита от распределенных атак типа "отказ в обслуживании" (DDoS)**. Модули Cisco Guard и Cisco Traffic Anomaly Detector для коммутатора Cisco Catalyst 6500 Series позволяют автоматически обнаруживать огромное количество разнообразных DDoS-атак и противостоять им. При внедрении этих функций обеспечения безопасности в сетевую инфраструктуру сеть оказывается в состоянии выдержать даже самые интенсивные DDoS-атаки и обеспечить защиту ЦОД и его критически важных приложений.
- **Дополнительные меры по защите протоколов стека TCP/IP.** При разработке многих протоколов стека TCP/IP соображения безопасности не учитывались, поэтому некоторые протоколы крайне уязвимы для атаки подмены адреса отправителя. Протокол TCP предлагает некоторые средства защиты от подмены адреса отправителя, но все равно остается уязвимым для более изощренных атак. Коммутатор Cisco Catalyst 6500 Series позволяет обеспечить защиту многих протоколов стека TCP/IP благодаря таким функциям, как контроль ARP, использование механизма TCP SYN-COOKIE, обеспечение случайного выбора ISN-номера, аутентификация при использовании протоколов обмена маршрутной информацией и т.д.
- **Аутентификация клиентов и серверов, целостность и конфиденциальность данных.** Средства шифрования SSL и IPSec позволяют обеспечить аутентификацию клиентов при доступе к серверным приложениям, а также обеспечить целостность и конфиденциальность данных. Коммутаторы Cisco Catalyst 6500 Series могут снять с серверов вычислительную нагрузку по выполнению операций шифрования и обеспечить распространение открытых ключей.
- **Обнаружение и предотвращение вторжений.** Решения для обнаружения вторжений, такие как сервисный модуль IDSM2 для коммутатора Cisco Catalyst 6500 Series, и решения для предотвращения вторжений, такие как программное обеспечение Cisco Security Agent, позволяют защитить группу серверов от атак, использующих уязвимости операционной системы и приложений. Эти технологии дополняются технологиями зеркалирования Catalyst 6500 Series, такими как, виртуализация ACL (VACL), анализ коммутируемых портов удаленного устройства (Remote Switched Port Analyzer, RSPAN) и NetFlow.
- **Защита сетевых устройств.** Защита механизма управления сетевыми устройствами в ЦОД позволяет предотвратить несанкционированный доступ и атаки DoS. Для реализации механизма защищенного управления используются такие технологии, как списки контроля доступа (ACL), средства аутентификации, авторизации и учета (AAA), протокол Secure Shell (SSH) и средства Syslog. Функции защиты уровня управления, работающие на Supervisor Engine 720 для коммутаторов семейства Cisco Catalyst 6500 Series и на маршрутизаторах, защищают их центральные процессоры от перегрузок в случае атак DoS.

Разграничение доступа и сегментация доступа

Коммутаторы Cisco Catalyst 6500 Series в сочетании с сервисным модулем межсетевого экрана (FWSM) поддерживают следующие функции:

- **Списки контроля доступа (ACL).** Коммутаторы Cisco Catalyst 6500 Series обеспечивают фильтрацию пакетов на скорости среды передачи с использованием списков контроля доступа программного обеспечения Cisco IOS® и VLAN (VACL). Списки контроля доступа ACL и VACL обеспечивают детальную фильтрацию трафика на уровне 4 (на уровне порта), предотвращая таким образом доступ к сервисам, которые были случайно оставлены доступными на серверах. Модуль FWSM для Catalyst 6500 Series реализует функции фильтрации пакетов, аналогичные функциям коммутатора Catalyst 6500 Series, и позволяет строить такие схемы маршрутизации, при которых трафик, идущий от клиента к серверу, проходит через несколько уровней ACL. Использование механизма управляющих сеансов (fixup) обеспечивает возможность открытия портов уровня 4 на межсетевых экранах.
- **Сети VLAN**. Коммутатором уровня 2 называется устройство, способное группировать подмножества портов в виртуальные домены широковещательной передачи, изолированные друг от друга. Такие домены называют виртуальными локальными сетями (VLAN). Cisco Catalyst 6500 Series поддерживает популярные технологии маркирования трафика VLAN Inter-Switch Link (ISL) и 802.1Q на физических соединениях (иногда их называют магистральными каналами или транками) и использует дополнительные методы маркирования трафика для сохранения информации VLAN. Сети VLAN могут служить для разделения групп серверов, а в сочетании с модулем FWSM их можно использовать для фильтрации трафика, направленного из одной сети VLAN в другую. Дополнительную информацию об использовании сетей VLAN в качестве средства обеспечения безопасности можно найти в отчете @stake Security Assessment по адресу http://www.cisco.com/warp/public/cc/pd/si/casi/ca6000/tech/stake_wp.pdf.

- **Частные сети VLAN (PVLAN).** Сети PVLAN обеспечивают изоляцию портов друг от друга в пределах одной сети VLAN. С помощью частных сетей VLAN можно использовать единственную подсеть и направлять весь генерируемый сервером трафик через "прозрачный" порт или порт масштабирования, в качестве которого обычно выступает порт маршрутизатора, или через интерфейс VLAN модуля FWSM. Эта схема позволяет защитить серверы от атак на уровне 2, таких как атаки с опережающим ARP-ответом, даже в случае, когда устройства в той же сети VLAN не устояли перед атакой. Коммутатор Cisco Catalyst 6500 Series поддерживает разделение сетей PVLAN на аппаратном уровне.
- **Сети MPLS VPN.** Применение технологии MPLS для построения VPN позволяет выполнить сегментацию сети с сохранением прозрачности адресного пространства. Такой подход предоставляет возможность построить максимально масштабируемую сеть, в которой используются механизмы идентификации, и одновременно воспользоваться всеми сильными сторонами и гибкостью протокола IP. Сети MPLS VPN обеспечивают тот же уровень конфиденциальности и защищенности информации, что и сети VPN уровня 2 – за счет распространения сведений о маршрутах VPN только на те маршрутизаторы, которые входят в сеть VPN. Модуль Supervisor Engine 720 для Cisco Catalyst 6500 Series в сочетании с платой Cisco Policy Feature 3B (PFC3BXL) обеспечивает поддержку MPLS VPN на аппаратном уровне. Сети MPLS VPN можно использовать в сочетании с виртуальными межсетевыми экранами на базе FWSM для осуществления контроля состояния соединений VPN.
- **Безопасность портов.** Центры обработки данных Cisco поддерживают полностью коммутируемую топологию, в которой отсутствует концентратор, а все соединения являются полнодуплексными. Лавинное передачу информации о маршрутизации на уровне 2 следует использовать только в ходе изменения топологии, чтобы ускорить процесс конвергенции сети уровня 2. Технологии, основанные на лавинной передаче информации о маршрутизации, приводят к снижению производительности, не говоря уже о потенциальных проблемах с безопасностью. Лавинное распространение информации о маршрутизации может быть результатом успешной атаки на сеть, поэтому на портах доступа необходимо сконфигурировать функции защиты на уровне порта. Безопасность на уровне порта позволяет предотвратить лавинное распространение информации на уровне MAC за счет назначения каждому порту списка конкретных MAC-адресов или выдачи разрешения на ограниченное количество MAC-адресов. При получении пакета защищенным портом система выполняет поиск MAC-адреса источника пакета в списке разрешенных адресов источников, составленном администратором вручную или составленном в процессе использования порта. Если MAC-адрес устройства, подключенного к порту, отсутствует в списке разрешенных адресов, порт блокируется насовсем (по умолчанию), блокируется на определенное время или отбрасывает входящие пакеты, поступающие от неизвестного хоста.
- **IEEE 802.1X.** Стандарт IEEE 802.1X определяет правила контроля доступа для соединений клиент-сервер и протокол аутентификации, который используется для предотвращения несанкционированного доступа клиентов к локальной сети через общедоступные порты. Сервер аутентификации выполняет аутентификацию каждого клиента, подключенного к порту коммутатора, и включает порт в состав VLAN перед тем, как предоставить клиенту доступ к каким-либо сервисам, предлагаемым коммутатором или локальной сетью. До момента прохождения клиентом процедуры аутентификации механизм управления доступом 802. 1X пропускает через порт, к которому подключен этот клиент, только трафик протокола EAPOL. После успешного прохождения аутентификации порт открывается для нормального трафика.

Безопасность протоколов стека TCP/IP

Коммутаторы семейства Cisco Catalyst 6500 Series в сочетании с сервисными модулями FWSM и ACE обеспечивают реализацию следующих функций безопасности:

- **Контроль ARP.** Механизмы контроля ARP обеспечивают сопоставление IP-адреса шлюза по умолчанию с его MAC-адресом. Если коммутатор обнаруживает пакет ARP, в котором содержится неверная комбинация адресов, коммутатор отбрасывает этот пакет, предотвращая таким образом атаки, связанные с внесением изменений в ARP-таблицы хостов.
- **Средства URPF.** Средства URPF обеспечивают проверку каждого пакета с тем, чтобы убедиться, что пакет пришел от нужного источника по соответствующему интерфейсу. Такая проверка позволяет предотвратить подмену адреса источника пакета. В ходе проверки система проверяет соответствие записи для адреса источника в таблице маршрутизации и идентификатора интерфейса, с которого поступил пакет. Коммутаторы семейства Cisco Catalyst 6500 Series и модуль FWSM реализуют проверку URPF на аппаратном уровне. Модуль Supervisor Engine 720 коммутатора Catalyst 6500 Series поддерживает работу механизма URPF одновременно на нескольких параллельных каналах передачи (до шести).
- **Фильтрация фрагментов пакетов.** Коммутаторы семейства Cisco Catalyst 6500 Series позволяют создавать списки ACL Cisco IOS и списки VACL, позволяющие разрешать или запрещать пересылку фрагментов пакетов. Фильтрацию фрагментов можно использовать для предотвращения атак с использованием фрагментации пакетов (например, атак, описанных в документе RFC 1858). Использование фильтрации фрагментов в сочетании с возможностями контроля состояния соединения модуля FWSM для Cisco Catalyst 6500 Series позволяет реализовать повторную сборку и проверку (виртуальную сборку) фрагментов перед их пересылкой.

- **Обеспечение случайного характера ISN-номера.** Реализации стека TCP/IP в некоторых операционных системах генерируют ISN-номера при установлении TCP-соединения предсказуемым образом, что делает возможным захват TCP-соединений. В прошлом эта уязвимость была обнаружена во многих операционных системах (см. CERT Advisory CA-1995.01, CERT Advisory CA-1998.13, CERT Advisory CA-2001-09, US CERT Vulnerability Note VU#498440). Модуль FWSM для Cisco Catalyst 6500 Series позволяет обеспечить действительно случайный закон выбора ISN-номеров, используемых при установлении TCP-соединения сервером.
- **Использование TCP SYN cookies** – SYN cookies представляют собой конкретные ISN-номера TCP, выбранные серверами. SYN cookies можно использовать для защиты очереди SYN-запросов стека TCP/IP устройств (сетевых устройств или серверов) от переполнения посредством выбора ISN (значения cookie) с помощью алгоритма Message Digest Algorithm 5 (MD5), использующего в качестве параметров IP-адреса и номера портов источника и приемника пакета. При достижении определенного порогового значения в очереди система продолжает посылать ответы SYN/ACK (второй пакет в трехэтапной схеме установления TCP-соединения), но не сохраняет информацию о состоянии соединения. При получении заключительного ответа ACK сервер вычисляет исходную информацию на основании значения ISN. SYN cookies являются эффективным механизмом защиты группы серверов от DoS-атак. С помощью этой технологии модуль Cisco ACE может выдерживать атаки, интенсивность которых измеряется сотнями тысяч запросов на установление соединения в секунду, и сохранить при этом легитимные соединения пользователей.
- **Контроль состояния TCP-соединений** – Модули FWSM и ACE для Cisco Catalyst 6500 Series поддерживают информацию о состоянии TCP-соединений, проходящих через них. К примеру, поддельный сегмент TCP, отправленный на маршрутизатор, подлежит пересылке точно так же, как и любой другой пакет IP. Модули FWSM и ACE для Cisco Catalyst 6500 Series не будут пересылать этот сегмент, т.к. поддельному сегменту не соответствует ни одно из существующих TCP-соединений.
- **Аутентификация при взаимодействии по протоколу VTP.** VTP представляет собой протокол уровня 2, предназначенный для обмена сообщениями, которые обеспечивают целостность конфигурации VLAN путем управления процедурами добавления, удаления и именования сетей VLAN в масштабе всей сети. Аутентификация VTP помогает обеспечить аутентификацию и целостность сообщений VTP, передаваемых от коммутатора к коммутатору. В протоколе VTP версии 3 предусмотрен дополнительный механизм аутентификации первичного сервера VTP в качестве единственного устройства, которому разрешено менять конфигурацию VLAN в масштабе всей сети.
- **Аутентификация при взаимодействии маршрутизаторов.** Аутентификация соседних маршрутизаторов, которую иногда называют "аутентификацией маршрутов", служит для удостоверения в подлинности соседних маршрутизаторов и обеспечения целостности обновлений маршрутной информацией при распространении между маршрутизаторами (между коммутаторами уровня 3) и между хостами и маршрутизаторами (коммутаторами уровня 3). В качестве хостов могут выступать серверы уровня 3, оборудованные несколькими сетевыми адаптерами, или мэйнфреймы. К числу протоколов обмена информацией о маршрутизации, поддерживающих этот вид аутентификации, относятся такие протоколы, как OSPF, EIGRP, IS-IS и BGP.

Аутентификация, вопросы целостности и конфиденциальности данных при взаимодействии клиентов и серверов

Коммутаторы семейства Cisco Catalyst 6500 Series, сервисный модуль SSL для Cisco Catalyst 6500 Series и сервисный модуль IPSec VPN для Cisco 7600/Catalyst 6500 обеспечивают реализацию следующих функций безопасности:

- **Шифрование SSL.** Протокол SSL позволяет обеспечить аутентификацию, конфиденциальность и целостность данных, а также неотказуемость от передачи при взаимодействиях клиент-сервер и сервер-сервер. Практически любое приложение, использующее протокол TCP в качестве транспортного, может использовать сервисы, предоставляемые SSL, и создавать соединения SSL при помощи сокетов SSL. Сервисный модуль SSL для Cisco Catalyst 6500 Series снимает с серверов вычислительную нагрузку по расшифрованию сложных шифров (например, 3DES) и одновременно поддерживает механизмы сквозного шифрования в масштабе сети. Кроме того, данный модуль упрощает процесс управления цифровыми сертификатами и может использоваться для внедрения модели доверия, позволяющей управлять правами на использование определенных приложений.
- **Шифрование IPSec.** Протокол IPSec позволяет обеспечить конфиденциальность и целостность передаваемой информации, аутентификацию участников соединения, а также защиту от атак типа "воспроизведение". Протокол IPSec работает между сетевым и транспортным уровнями стека протоколов TCP/IP. IPSec полностью прозрачен для приложений, которым не требуется "знать" о существовании протокола IPSec и, тем более, поддерживать его. IPSec часто используется для создания защищенных туннелей между центрами обработки данных.

Анализ трафика, обнаружение и предотвращение вторжений

Коммутаторы семейства Cisco Catalyst 6500 Series обеспечивают реализацию следующих функций

анализа трафика:

- **SPAN и RSPAN**. Технология SPAN служит для зеркалирования трафика с одного или нескольких портов коммутатора Cisco Catalyst 6500 Series (источник SPAN) на другой порт того же коммутатора (приемник SPAN). Такую схему зеркалирования часто называют "локальной схемой SPAN". RSPAN позволяет расширить диапазон анализа и включить в него несколько коммутаторов, подключенных к одному и тому же домену уровня 2. Сочетание технологии RSPAN и списков доступа VACL позволяет выполнять глубокий анализ трафика посредством распределения зеркального трафика по группам, количество которых может достигать 64.
- **VACL.** Технология VACL, реализованная в коммутаторах семейства Cisco Catalyst 6500 Series, позволяет создавать списки ACL для тонкой настройки признаков собираемого трафика.
- **NetFlow.** Технология NetFlow позволяет оперативно собирать и экспортировать статистические сведения о трафике, полученные в результате анализа трафика, передаваемого через коммутаторы и маршрутизаторы. В сфере обеспечения безопасности NetFlow применяется для предотвращения атак типа "отказ в обслуживании", распределенных атак типа "отказ в обслуживании" и противодействия распространению Интернет-червей. Коммутаторы семейства Cisco Catalyst 6500 Series поддерживают экспорт данных NetFlow в формате NetFlow версий 5, 7 и 8. Для уменьшения объема собираемой статистики можно использовать средства дискретизации и агрегирования NetFlow.

Коммутаторы семейства Cisco Catalyst 6500 Series в сочетании с сенсорами Cisco IDS 4200 Series или сервисным модулем IDSM-2 для Cisco Catalyst 6500 Series обеспечивают реализацию следующих функций обнаружения вторжений:

- **IDS для мультигигабитных сетей.** Сенсоры IDS обнаруживают вредоносную активность в сети группы серверов за счет выявления аномалий на уровне протоколов или общего трафика, либо сопоставления событий, описываемых сигнатурами, с состоянием TCP-соединения. Сенсор IDS способен обнаружить атаку на самых ранних этапах благодаря умению идентифицировать процедуры зондирования. Кроме того, такой сенсор может обнаруживать попытки использования широкоизвестных уязвимостей. Список сигнатур IDS представлен на web-сайте http://www.cisco.com/cgi-bin/front.x/csec/idsServiceList.pl

  При использовании совместно с коммутатором семейства Cisco Catalyst 6500 Series или модулем FWSM для Cisco Catalyst 6500 series сенсоры IDS позволяют изолировать взломанный сервер до того, как он сможет заразить другие устройства. Для проведения анализа трафика мультигигабитной сети можно выполнять распределение трафика по многим сенсорам IDS за счет использования технологий зеркалирования Catalyst 6500 Series (RSPAN и VACL).

Помимо средств анализа трафика, а также средств обнаружения и предотвращения вторжений на уровне сети можно установить дополнительные элементы защиты на сами серверы. Для этого можно воспользоваться программным обеспечением Cisco Security Agent, которое реализует следующие функции безопасности:

- **Предотвращение вторжений на хост.** Программное обеспечение Cisco Security Agent, установленное на сервер, позволяет предотвращать переполнение буфера приложений и выполнение вредоносных операции с регистром операционной системы, файловой системой и стеком TCP/IP. Программное обеспечение для защиты от вторжений, устанавливаемое на хостах, защищает серверы от заражения новыми червями и от манипуляций злоумышленников, снижая, таким образом, известные и пока неизвестные ("0 day") риски в области безопасности.

Обеспечение безопасности сетевых устройств

Для предотвращения несанкционированного доступа необходимо обеспечить защиту управляющих интерфейсов сетевых устройств: злоумышленник, обладающий доступом к консоли сетевого устройства, может легко изменить конфигурацию сети и создать "люк", позволяющий обойти систему безопасности. Коммутаторы и сервисные модули семейства Cisco Catalyst 6500 Series обеспечивают следующие функции защиты управляющих интерфейсов:

- **Аутентификация, авторизация и учет (AAA).** Архитектуру AAA можно использовать для управления доступом к критически важным ресурсам, например, серверам или сетевым устройствам, с учетом прав, предоставленных различным пользователям и их группам. AAA позволяет использовать локальную базу данных имен/паролей пользователей коммутатора или специальные протоколы, например, TACACS+ или RADIUS, для доступа к серверу аутентификации.
- **Протокол SSH версии 2 (SSHv2).** SSHv2 позволяет реализовать безопасный удаленный доступ за счет использования механизмов аутентификации и шифрования. Протокол SSH следует использовать в качестве альтернативы небезопасным протоколам, таким как telnet и rlogin. SSHv2 допускает совместное использование с протоколами TACACS+ и RADIUS. Коммутаторы семейства Cisco Catalyst 6500 Series поддерживают протокол SSH версии 2.
- **Протокол SNMP версии 3 (SNMPv3).** SNMP представляет собой протокол прикладного уровня, который обеспечивает обмен управляющей информацией между сетевыми устройствами. Коммутаторы семейства Cisco Catalyst 6500 Series поддерживают версии протокола SNMP 1, 2c и 3. Протокол SNMPv3 (RFC 2271-2275) обеспечивает аутентификацию участников взаимодействия, целостность и шифрование данных. Для шифрования трафика SNMPv3 используется алгоритм DES, контроль целостности и аутентификация обеспечивается с

помощью алгоритмов MD5 HMAC или SHA HMAC.

- **Syslog.** Сообщения Syslog представляют собой произвольные уведомления, которые сетевые устройства могут сохранять в файле журнала или отправлять на сервер Syslog, например, CiscoWorks2000 Resource Manager Essentials (RME). Сообщения Syslog содержат временную метку сервера Syslog, имя устройства, порядковый номер, временную метку сетевого устройства и собственно само сообщение. Типы сообщений Syslog используются для указания сетевых ресурсов. Полный список возможных сообщений Syslog для коммутатора Catalyst 6500 представлен по адресу http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/msgguide/edesc.htm.
- **Протокол NTP версии v3.** Этот протокол (RFC1305) используется для синхронизации системных часов сетевых устройств. Он имеет особое значение при обработке сообщений Syslog, поступающих из различных источников, временные метки которых позволяют проводить корреляционный анализ событий, сведения о которых заносятся в журнал.

Помимо защиты уровня управления от несанкционированного доступа не менее важной задачей представляется предотвращение атак типа "отказ в обслуживании" и противодействие распространению Интернет-червей. Коммутаторы Cisco Catalyst 6500 Series реализуют следующие функции:

- **Cisco Express Forwarding**. Такие источники угроз, как Интернет-черви, выполняют поиск уязвимый устройств путем постоянной передачи запросов на установление соединения на выбираемыми случайным образом IP-адреса. Такой объем трафика может легко заблокировать работу потоковых коммутаторов уровня 3, т.к. они обрабатывают первый пакет потока на программном уровне. Функция аппаратного уровня Cisco Express Forwarding, поддерживаемая модулями Supervisor Engine II и 720 для коммутаторов семейства Cisco Catalyst 6500 Series, позволяет предотвратить такую неполадку посредством переноса всех функций пересылки пакетов на аппаратный уровень и отделения процедур обработки пакетов от уровня управления, функционирующего на программном уровне.
- **Аппаратные устройства ограничения скорости.** Коммутаторы уровня 3 обычно выполняют пересылку пакетов и фильтрацию трафика на аппаратном уровне. Некоторые типы трафика требуют обработки на программном уровне (сообщения ICMP unreacheable, ICMP redirect, или обработка MTU/TTL IP-пакета с целью генерации сообщений ICMP "packet too big" или "time exceeded"). Модуль Supervisor Engine II для Cisco Catalyst 6500 Series позволяет воспользоваться заранее сконфигурированными ограничителями скорости, а модуль Supervisor Engine 720 для Catalyst 6500 Series обеспечивает дополнительные возможности управления путем использования 12 ограничителей скорости для специальных случаев.
- **Политики уровня управления (CoPP).** Функция Control Plane Policing дает возможность создавать фильтры по признаку качества обслуживания (QoS), которые управляют потоками пакетов через уровень управления для защиты последнего от "разведывательных" действий и атак типа "отказ в обслуживании". Функция фильтрации позволяет выполнять пересылку пакетов и контроль состояния протоколов, невзирая на атаки или огромные объемы трафика, которые приходится обрабатывать коммутатору.
- **Регулировка пропускной способности ARP.** Механизм регулировки пропускной способности ARP ограничивает скорость пересылки пакетов, адресованных в сегмент сети, подключенный к данному коммутатору, на процессор маршрутизации в том случае, если MAC-адреса получателей пакетов еще неизвестны. Модуль Supervisor Engine II для Cisco Catalyst 6500 Series реализует предустановленное ограничение пропускной способности, а Supervisor Engine 720 для Catalyst 6500 Series позволяет задать параметры ограничения пропускной способности .

  Использование механизма ролевого доступа (RBAC) позволяет обеспечить дополнительную защиту. Механизм RBAC поддерживается сервером системы контроля доступа Cisco Secure Access Control Server (ACS). Решения Cisco 1105 для Hosting Solution Engine и Cisco Works VPN/Security Management Solution также предлагают возможности конфигурирования RBAC.

ИНСТРУМЕНТЫ SAN

Сети SAN традиционно считались относительно безопасными, в первую очередь потому, что способ подключения SAN предусматривает весьма ограниченный доступ к ним со стороны других компонентов центра данных – по существу, SAN представляет собой изолированную сеть. Такое представление является сильно упрощенным; один-единственный пораженный хост может потенциально заблокировать работу других хостов, подключенных к сети SAN, получить несанкционированный доступ к данным в пределах SAN и, наконец, обойти существующие межсетевые экраны и системы обнаружения вторжений в случае использования каналов IP поверх соединений Fibre Channel (RFC 2625).

Кроме того, нередко встречаются сети SAN, которые простираются за физические пределы центров обработки данных с целью обеспечения непрерывности бизнеса и скорейшего восстановления после аварий. Распространение таких технологий, как SCSI over IP (iSCSI) и Fibre Channel over IP (FCIP), использующих протокол TCP/IP в качестве транспорта, обуславливает требования по надежной защите SAN, т.к. эти технологии предполагают передачу конфиденциальной информации по сетям передачи данных общего пользования.

При обеспечении безопасности SAN необходимо рассмотреть три различных аспекта:

1. Защита SAN от внешних угроз (например, хакеров и пользователей с недобрыми намерениями)
2. Защита SAN от внутренних угроз (например, от несанкционированного доступа со стороны пользователей и от воздействий со стороны взломанных или недостаточно защищенных устройств)
3. Защита SAN от непреднамеренных угроз со стороны авторизованных пользователей (неправильные настройки параметров и ошибки, вызванные "человеческим фактором")

Первые два аспекта относительно просты и хорошо понятны с точки зрения безопасности. Третий аспект не столь прост; при этом следует заметить, что в недавнем прошлом непреднамеренным угрозам безопасности со стороны авторизованных пользователей уделялось недостаточно внимания. Разумная стратегия обеспечения безопасности для сред UNIX и Windows предполагает предоставление прав суперпользователя или администратора для выполнения задач администрирования минимальному количеству пользователей; тот же осторожный подход, предусматривающий предоставление минимального объема привилегий для решения определенной задачи, следует использовать и при работе с сетями SAN. Эта проблема достаточно многогранна – например, преимущества изоляции "операторских" привилегий на коммутаторе с использованием ролевой модели контроля доступа очевидны, но другие меры, например, меры, направленные на снижения вероятности ошибок в конфигурации коммутационной структуры, связанных с неправильной настройкой коммутатора и выражающихся в появлении перекрывающихся идентификаторов доменов – не столь очевидны. Многие из этих подходов размывают границы между процессами обеспечения безопасности SAN, проектирования SAN на основе оптимальных подходов и проектирования SAN с высоким уровнем доступности, но все эти подходы важны с той точки зрения, что правильно настроенный, защищенный коммутатор позволяет предотвратить как умышленные, так и непреднамеренные деструктивные действия.

Средства обеспечения безопасности SAN лучше всего изучать на уровне архитектуры, на котором можно выделить шесть основных зон. К числу шести указанных зон относятся:

- **Доступ к структуре коммутации.** – Защищенные обращения структуры к сервисам коммутации.
- **Доступ к целевым устройствам.** Защищенный доступ к целевым устройствам и модулям LUN.
- **Протокол SAN.** Защищенные каналы связи и механизм авторизации между коммутаторами.
- **Доступ к хранилищу по протоколу IP.** Защищенные сервисы FCIP и iSCSI.
- **Целостность и конфиденциальность данных.** Шифрование передаваемых данных.
- **Управление SAN.** Защищенный доступ к сервисам управления.

В следующем параграфе рассматриваются особенности каждой из зон, а также дополнительные функции безопасности, реализованные в рамках платформы Cisco MDS 9000 Series для каждой из зон.

Доступ к структуре коммутации и целевым устройствам

Многоуровневые коммутаторы семейства Cisco MDS 9000 Series предлагают следующие функции безопасного доступа к структуре коммутации и целевым устройствам по каналам Fibre Channel:

- **Зонирование Fibre Channel.** Зонированием называется внутренний механизм обеспечения безопасности Fibre Channel, который используется для ограничения связи между устройствами, подключенными к одной структуре Fibre Channel. К сети подключено множество серверов и устройств хранения различных типов. Это создает возможность подключения какого-либо хоста к диску, используемому другим хостом, возможно, с другой операционной системой, и порчи данных на диске. Различают зонирование двух типов: программное и аппаратное. Программным зонированием называют зонирование, выполняемое на программном уровне; иными словами, так именуют зонирование, выполняемое программным обеспечением плоскости управления на коммутаторах Fibre Channel в рамках сервиса Fibre Channel Name Server. Аппаратным зонированием называют зонирование, выполняемое на аппаратном уровне; иными словами, так именуют зонирование, реализуемое посредством аппаратных списков контроля доступа (ACL), применяемых к каждому коммутируемому фрейму Fibre Channel.

  Программное зонирование обеспечивает достаточный уровень защиты для предотвращения случайных потерь данных; однако его возможностей недостаточно для предотвращения несанкционированного доступа к данным. Аппаратное зонирование обеспечивает достаточный уровень защиты для предотвращения несанкционированного доступа к данным, но только в том случае, если злоумышленники не используют механизм подмены глобальных имен (WWN spoofing).

  Все многоуровневые интеллектуальные коммутаторы семейства Cisco MDS 9000 поддерживают как программное, так и аппаратное зонирование (до 2 000 зон и до 20 000 членов зон).
- **Зонирование номеров логических устройств (LUN) и зоны только для чтения.** Коммутаторы семейства Cisco MDS 9000 предлагают более детальные варианты зонирования в дополнение к общеизвестным способам. Благодаря средствам детального анализа фреймов механизм аппаратного зонирования, реализованный в коммутаторах семейства Cisco MDS 9000, позволяет ограничить доступ к явно заданным блокам LUN в пределах определенного массива хранилища и даже запретить возможность выполнения операции записи по шине SCSI, оставив только право чтения.
- **Виртуальные сети SAN (VSAN).** Технология VSAN позволяет создавать множество логических сетей SAN на базе общей физической инфраструктуры. Каждая сеть VSAN использует собственный набор сервисов коммутирующей структуры. Это позволяет полностью разделить

виртуальные коммутирующие структуры.

Сети VSAN позволяют обеспечить более высокий уровень безопасности и стабильности коммутирующих структур Fibre Channel благодаря изоляции устройств, физически подключенных к одной и той же группе коммутаторов. Ошибки, возникающие в какой-либо коммутирующей структуре, будут изолированы в пределах одной сети VSAN и не будут распространяться на другие сети VSAN. Связь между устройствами, принадлежащими разным сетям VSAN, невозможна, за исключением тех случаев, когда ее явно разрешают с помощью механизма маршрутизации между сетями VSAN Inter-VSAN Routing.

- **Механизмы маршрутизации между сетями VSAN (IVR).** Маршрутизация IVR позволяет создавать защищенные маршруты, объединяющие устройство, находящееся в одной сети VSAN, с одним или несколькими устройствами, находящимися в другой сети VSAN, не объединяя при этом коммутирующие матрицы соответствующих VSAN (т.е., не создавая единый слитый домен ошибок). Технология Inter-VSAN Routing обеспечивает эффективную трансляцию сетевых адресов (Network Address Translation, NAT) только для трафика данных (Fibre Channel Class 2 и 3).
- **Безопасность на уровне портов.** Функции обеспечения безопасности на уровне портов позволяют обеспечить предоставление доступа к коммутирующей структуре Fibre Channel на основании идентификационных атрибутов устройства. Механизм безопасности на уровне порта предотвращает несанкционированный доступ к порту коммутатора путем привязки конкретных глобальных имен (WWN) к одному или нескольким портам коммутатора. Если на каком-либо порту коммутатора включена функция обеспечения безопасности, то все устройства, подключающиеся к этому порту, должны быть указаны в базе данных безопасности порта в качестве привязанных к данному порту. В случае устройства хранения данных или хоста для привязки авторизованных устройств хранения к конкретному порту коммутатора можно использовать имя порта (pWWN) или имя узла (nWWN). В случае порта E_Port/TE_Port для привязки авторизованных коммутаторов к определенному порту данного коммутатора используется имя коммутатора (sWWN).
- **Функция безопасности режимов порта.** Функция безопасности режимов порта позволяет ограничивать функциональность порта. Например, режим порта можно настроить таким образом, чтобы исключить непреднамеренное использование граничных портов для ISL.
- **Протокол FCSP.** Протокол FCSP (Fibre Channel Security Protocol) с расширением DH-CHAP (Diffie-Hellman Challenge Handshake Authentication Protocol) позволяет обеспечить целостность данных (защиту от несанкционированного изменения) и их аутентификацию (неотказуемость) в процессе взаимодействия между хостом и коммутатором или двумя коммутаторами. Аутентификация может проходить с использованием локальной базы данных коммутатора или с использованием удаленной базы данных централизованного сервера RADIUS или TACACS+.

  Протокол FCSP DH-CHAP обеспечивает стопроцентную защиту от подмены глобальных имен (WWN) на взломанном порту, даже если физическая безопасность коммутатора была нарушена, и устройство злоумышленника было подключено к тому же физическому порту, что и легитимный хост.

  Протокол FCSP DH-CHAP поддерживается всеми основные производители HBA-адаптеров и некоторые производители коммутаторов SAN.

Безопасность протоколов SAN

Многие из функций безопасности, обеспечивающих контроль и разграничение доступа к коммутирующим структурам и целевым устройствам, такие как сети VSAN, механизмы маршрутизации между сетями VSAN, функции безопасности на уровне портов, безопасность режимов порта и протокол FCSP DH-CHAP имеют отношение к безопасности протоколов SAN постольку, поскольку они обеспечивают безопасность доступа к коммутирующим матрицам и целевым устройствам. Помимо вышеперечисленного в коммутаторах серии Cisco MDS 9000 Series предусмотрен ряд дополнительных функций обеспечения безопасности протоколов SAN:

- **Предотвращение разрушительной переконфигурации коммутирующей структуры.** Возможность отклонения запросов на разрушительную переконфигурацию коммутирующей структуры, поступающих от коммутаторов, неправильно настроенных злоумышленниками или новых, еще не настроенных коммутаторов, которые подключены к действующей структуре. Если бы такой возможности не было, неправильно настроенный злоумышленниками коммутатор или новый, еще не настроенный коммутатор могли бы вызвать выход структуры из строя.
- **Привязка к структуре FICON.** Возможность введения перечня коммутаторов и идентификаторов доменов, которым предоставлен доступ к структуре FICON.
- **Кэширование идентификаторов Fiber Channel, выделение постоянных идентификаторов Fiber Channel** и **присваивание статических идентификаторов Fiber Channel.** Возможность ограничения перечня идентификаторов Fibre Channel, присваиваемых определенным глобальным именам pWWN, а также использования постоянных идентификаторов Fibre Channel при перезапуске системы.

БЕЗОПАСНОСТЬ ДОСТУПА К ХРАНИЛИЩУ С ИСПОЛЬЗОВАНИЕМ ПРОТОКОЛА IP

В конструкции сервисных модулей IP коммутаторов семейства Cisco MDS 9000 предусмотрены порты Gigabit Ethernet, которые могут как принимать входящие соединения от хостов (инициаторов iSCSI), так и обеспечивать расширение SAN по протоколу IP (Fibre Channel over IP). Коммутаторы семейства Cisco MDS 9000 поддерживают следующие функции безопасности на уровне протокола IP:

- **Аутентификация iSCSI.** Аутентификация инициаторов входящих сеансов iSCSI (запросы на которые поступают от инициаторов iSCSI), выполняется с помощью протокола CHAP до установления сеанса iSCSI.
- **Динамическое и статическое выделение постоянных имен WWN для инициаторов iSCSI.** Система позволяет динамически или статически сопоставлять инициаторов iSCSI с виртуальными инициаторами Fibre Channel посредством присваивания уникальных для данного инициатора и для данной сети VSAN имен nWWN и pWWN (по сути, каждый инициатор iSCSI представляется как "виртуальный" N_Port). Присваивание постоянных имен nWWN и pWWN может происходить как в статическом, так и в динамическом режиме (в последнем случае имя выбирается динамически из диапазона имен WWN, хранящихся в памяти коммутатора).

  Это позволяет использовать такие функции, как безопасность LUN, сопоставление LUN и маскирование LUN для массивов хранилищ среднего и корпоративного класса, т.к. они могут использовать для однозначной идентификации хостов, подключенных через интерфейс iSCSI, те же механизмы, с помощью которых выполняется идентификация хостов, подключенных к адаптеру HBA Fibre Channel.
- **Средства контроля доступа iSCSI.** Существуют различные способы контроля доступа, которые могут примениться к инициаторам iSCSI. Во-первых, инициатору iSCSI разрешен доступ только к тем целевым устройствам Fibre Channel (виртуальным целевым устройствам iSCSI), для которых этот доступ был задан явным образом. Во-вторых, инициатор iSCSI (виртуальный N_Port) явно указывается в качестве инициатора в рамках одной сети VSAN. Для зонирования виртуальных портов N_Port и устройств хранения можно использовать стандартные технологии зонирования Fibre Channel. Наконец, ограничения, накладываемые на интерфейс, позволяют выбрать режим объявления об отдельных целевых устройствах iSCSI: глобальный (по всем интерфейсам Gigabit Ethernet) или только по определенным интерфейсам и субинтерфейсам Gigabit Ethernet либо сетям VLAN.
- **Протокол FCIP.** Протокол FCIP обеспечивает передачу данных Fibre Channel по IP-сети путем туннелирования фреймов Fibre Channel по паре TCP-соединений между двумя коммутаторами. Необработанные фреймы Fibre Channel (содержащие полный заголовок Fibre Channel) инкапсулируются в TCP-сегменты при помещении в туннель и реконструируются во фреймы Fibre Channel при извлечении из туннеля.

  Технология FCIP сама по себе не предлагает какие-либо явные инструменты обеспечения безопасности, но она может использовать все существующие механизмы безопасности, доступные для "родной" среды Fibre Channel. Сюда относятся такие механизмы, как безопасность на уровне портов и аутентификация в соединениях между коммутаторами по протоколу FCSP DH-CHAP.

Целостность и конфиденциальность данных

Ни протокол iSCSI, ни протокол FCIP не обеспечивают защиту передаваемых данных. Таким образом, если устройство злоумышленника, способное перехватывать трафик, будет установлено на маршруте его передачи, то оно сможет прослушивать все данные хранилища, передаваемые по данному соединению. Исходя из этого рабочая группа IP Storage комиссии IETF разработала концепцию обеспечения безопасности каналов связи с хранилищами, использующих протокол IP (см. документ "Securing Block Storage Protocols over IP" (draft-ietf-ips-security-19.txt). Если сеть передачи данных не является доверенной, комиссия IETF настоятельно рекомендует использовать для передачи данных протокол IPSec. Как линейная карта мультипротокольной коммутации MPS 14+2, так и многоуровневая коммутирующая структура Cisco MDS 9216i Multilayer Fabric Switch обеспечивают поддержку IPSec на аппаратном уровне, что позволяет обеспечить шифрование и дешифрование данных IPSec с использованием алгоритмов AES и 3DES на скорости среды передачи.

8-портовый сервисный модуль Cisco IP Storage (IPS-8) и 4-портовый сервисный модуль Cisco IP Storage (IPS-4) могут использоваться в сочетании с целым рядом устройств обеспечения безопасности для создания защищенных туннелей IPSec. Сервисный модуль IPSec VPN для коммутаторов Cisco 7600/Catalyst 6500 предлагает интегрированные на уровне инфраструктуры сервисы IPSec VPN, обеспечивающие скорость шифрования 3DES 1,9 Гбит/с, поддерживающие до 8000 активных туннелей и позволяющие создавать до 60 туннелей в секунду.

Для создания туннелей IPSec можно использовать целый ряд других устройств. Их перечень приведен в документе SAFE Blueprint, разработанном компанией Cisco и посвященном безопасности сетей VPN. Документ SAFE Blueprint находится по адресу http://www.cisco.com/go/safe.

Доступ к механизмам сетевого управления SAN

Для предотвращения несанкционированного доступа необходимо обеспечить безопасность процесса

управления сетевыми устройствами, подключенными к центру обработки данных: злоумышленник, обладающий доступом к консоли сетевого устройства, может легко изменить конфигурацию сети. Продукты семейства Cisco MDS 9000 предлагают следующие защищенные функции управления:

- **Аутентификация, авторизация и учет (AAA)**. Архитектуру AAA можно использовать для управления доступом к критически важным ресурсам, таким как серверы или сетевые устройства, с учетом прав, предоставленных различным пользователям и их группам. AAA может использовать локальную базу данных имен/паролей пользователей коммутатора или специальные протоколы, например, TACACS+ или RADIUS, для доступа к серверу аутентификации.
- **Механизм ролевого доступа (RBAC).** RBAC позволяет назначать различным пользователям различные роли, обязанности, возможности управления и вводить для различных пользователей соответствующие ограничения. В пределах одной системы могут существовать не более 64 ролей. Назначение пользователей на роли выполняется либо на локальном уровне (на уровне конфигурации коммутатора), либо централизованно, с помощью механизма AAA.
- **Ролевой доступ для VSAN.** Система позволяет давать администраторам хранилищ выборочные привилегии доступа и права, указывая их отдельно для каждой сети VSAN. Это позволяет реализовать дополнительный уровень детализации привилегий и прав доступа, предоставляемых администратору.
- **Протокол SSH версии 2.** SSHv2 позволяет реализовать безопасный удаленный доступ за счет использования механизмов аутентификации и шифрования. Протокол SSH следует использовать в качестве альтернативы небезопасным протоколам, таким как telnet и rlogin. SSHv2 допускает совместное использование с протоколами TACACS+ и RADIUS. SSHv2 также можно использовать для безопасной передачи файлов образов, файлов журналов и информации о конфигурации коммутаторов с использованием Secure Copy или Secure FTP.
- **Протокол SSL версии 2 и прозрачные сервисы LAN (TLS) 1.0.** В спецификации SMI-S приводится описание общих интерфейсов, основанных на Общей информационной модели (CIM) и позволяющих обеспечить совместимость компонентов различных производителей в инфраструктуре SAN. Управляющие клиенты SAN могут связываться с серверами CIM для управления большими объемами ресурсов хранилищ с помощью унифицированного интерфейса SMI-S.

  В продуктах семейства Cisco MDS 9000 предусмотрен встроенный агент, который реализует функции CIM Object Manager и CIM Provider. Этот агент поддерживает доступ по протоколам SSL и TLS и обеспечивает возможность использования технологий AAA и RBAC.
- **Протокол SNMP версии 3**. SNMP представляет собой протокол прикладного уровня, который обеспечивает обмен управляющей информацией между сетевыми устройствами. Коммутаторы семейства Cisco Catalyst 6500 Series поддерживают версии протокола SNMP 1, 2c и 3. Протокол SNMPv3 (RFC 2271-2275) обеспечивает аутентификацию участников взаимодействия, целостность и шифрование данных. Для шифрования трафика SNMPv3 используется алгоритм DES, контроль целостности и аутентификация обеспечивается с помощью алгоритмов MD5 HMAC или SHA HMAC. Кроме того, продукты семейства Cisco MDS 9000 поддерживают более мощный 128-битный алгоритм шифрования AES для SNMPv3 (RFC 3826).
- **Syslog.** Сообщения Syslog представляют собой произвольные уведомления, которые сетевые устройства могут сохранять в файле журнала или отправлять на сервер Syslog, например, CiscoWorks2000 Resource Manager Essentials (RME). Сообщения Syslog содержат временную метку сервера Syslog, имя устройства, порядковый номер, временную метку сетевого устройства и собственно само сообщение.
- **Протокол NTP версии v3.** Этот протокол (RFC1305) используется для синхронизации системных часов сетевых устройств. Он имеет особое значение при обработке сообщений Syslog, поступающих из различных источников, временные метки которых позволяют проводить корреляционный анализ событий, сведения о которых заносятся в журнал.
- **Журнал учета.** Аудиторский учет команд конфигурации ведется внутри коммутатора (критически важные сообщения сохраняются в энергонезависимой памяти NVRAM); кроме того, команды конфигурации можно фиксировать на центральных серверах Syslog и AAA с помощью учетных сообщений RADIUS или TACACS+.
- **Функция "Call Home".** Функция Call Home позволяет рассылать уведомления о критически важных системных событиях по электронной почте. Примерами применения этой функции могут служить отправка сообщений непосредственно на пейджер инженера службы сетевой поддержки, отправка уведомлений по электронной почте в центр управления работой сети (NOC) и использование сервисов Cisco AutoNotify для непосредственной регистрации инцидентов в Центре технической поддержки Cisco (TAC). Call Home поддерживает такие возможности, как одновременная рассылка уведомлений по многим адресам, классификация сообщений по категориям и различные опции доставки сообщений. Все это позволяет адаптировать функцию Call Home к любым специфическим требованиям, касающимся управления сетью и мониторинга ее состояния. Сообщения могут рассылаться в коротком текстовом формате (для сообщений на пейджеры и SMS-сообщений), в обычном текстовом формате и в формате XML (для сообщений электронной почты).
- **Проверка целостности коммутирующей структуры.** Fabric Manager (административный пакет на основе JAVA с графическим интерфейсом пользователя, который использует протокол SNMP для связи с коммутаторами Cisco семейства MDS 9000) содержит встроенный мастер,

именуемый Fabric Consistency Checker. Этот инструмент служит для проверки согласованности конфигурационной политики на всех коммутаторах в рамках одной коммутирующей структуры. Он позволяет выделить отличия конфигурации в тех случаях, когда обнаруживает несоответствия с конфигурационной политикой "главного" коммутатора, и предлагает механизм разрешения противоречий. Fabric Consistency Checker предлагает методику, которая позволяет убедиться, что политика и конфигурации безопасности носят согласованный характер для всех коммутаторов в пределах одной коммутирующей структуры. При этом предлагаемая методика практически не требует никаких усилий со стороны администратора.

- **Списки контроля доступа (ACL).** Списки ACL могут применяться к управляющим интерфейсам и интерфейсам Gigabit Ethernet сервисных модулей IPS-4, IPS-8 и MPS 14+2 IP Storage для ограничения доступа к средствам управления и доступа по IP-каналам к определенному подмножеству IP-адресов.
- **Механизм SPAN.** SPAN позволяет копировать все фреймы, поступающие через целевой порт SPAN и отправляемые через него, для любых интерфейсов или сетей VSAN, для которых ведется мониторинг. В качестве целевого порта SPAN можно указать любой порт Fibre Channel коммутатора. Для получения копии всего отслеживаемого трафика к целевому порту SPAN можно подключать Fibre Channel Analyzer (например, Finisar Analyzer) или Cisco Port Adapter Analyzer.

  SPAN представляет собой исключительно мощную функцию диагностики проблем и мониторинга трафика. В силу того, что функция SPAN позволяет копировать все фреймы Fibre Channel, пересылаемые внутри коммутатора, она представляет собой определенный риск в сфере безопасности, т.к. дает возможность зарегистрировать критически важные данные, которые ранее нельзя было прослушать. По этой причине рекомендуется применять механизм ролевого управления доступом (RBAC) для предотвращения возможности использования функции SPAN неавторизованными пользователями.

ИНТЕГРАЛЬНАЯ ЦЕННОСТЬ

Технологии локальных сетей и сетей SAN предлагают экономичный способ защиты приложений ЦОД благодаря использованию интеллектуальных функций сети для снижения рисков успешной реализации наиболее распространенных угроз.

Сеть ЦОД позволяет защитить приложения групп серверов за счет разделения трафика, принадлежащего различным группам. Механизм разделения можно реализовать как в локальной сети, так и в сети SAN с помощью следующих технологий:

- Сети VLAN (для локальных сетей) и сети VSAN (для сетей SAN);
- Списки контроля доступа (ACL) в локальных сетях и аппаратное зонирование в сетях SAN;
- Безопасность на уровне портов Ethernet в локальных сетях и безопасность на уровне портов Fibre Channel в сетях SAN.

Функции безопасности протоколов уровней 2 и 3 и протокола Fibre Channel помогают реализовать механизм аутентификации и обеспечить целостность данных в соединениях между коммутаторами с помощью следующих технологий:

- Протокол VTP версии 3 средства RPA в локальных сетях и средства аутентификации FCSP DH-CHAP в сетях SAN;

Нарушение конфиденциальности информации затрудняется путем использования средств шифрования, обеспечивающих аутентификацию абонентов, конфиденциальность и целостность данных с помощью следующих технологий:

- SSL и IPSec в локальных сетях и – в будущем – Fibre Channel Security (FCSec) (часть стандарта FCSP) в сетях SAN.

Мониторинг трафика помогает идентифицировать действия злоумышленника с использованием следующих технологий:

- SPAN, RSPAN, VACL, NetFlow и Call Home в локальных сетях; SPAN, RSPAN, статистика потоков Fibre Channel, Call Home и RMON Threshold Alarms в сетях SAN.

Защита механизмов управления с использованием следующих средств сводит к минимуму возможности злоумышленников по контролю за устройствами локальной сети и сети SAN :

- AAA, SSHv2, SNMPv3, syslog, NTPv3 и RBAC – все эти технологии применимы как для устройств локальной сети, так и для коммутаторов SAN.

Серверы и хосты присутствуют в ЦОД в локальной сети, а некоторые серверы присутствуют и в локальной сети, и в сети SAN. Для обеспечения безопасности этих серверов может использоваться программное обеспечение Cisco Security Agent.

Интегрированное решение Cisco для ЦОД позволяет реализовать всеобъемлющую систему безопасности, которая охватывает протоколы уровня 2, протоколы прикладного уровня и серверные операционные системы.

АРХИТЕКТУРА СИСТЕМЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ И ПРОДУКТЫ, НЕОБХОДИМЫЕ ДЛЯ ЕЕ СОЗДАНИЯ

В состав архитектуры системы обеспечения безопасности входят следующие отдельные продукты и компоненты:

- **Коммутатор Cisco Catalyst 6500 Series**. Первоклассный интеллектуальный многоуровневый модульный коммутатор Cisco Catalyst 6500 Series идеально подходит для ЦОД. Высокая скорость пересылки пакетов и поддержка сервисных модулей для уровней с 4 по 7, порты 10/100/1000 Мбит/с, 10 Gigabit Ethernet, поддержка кадров большого объема, стандартов 802.1s, 802.1w, списков контроля доступа VLAN, SPAN, механизмов управления качеством обслуживания (QoS), механизмов групповой адресации , uRPF на аппаратном уровне и т.д. делает это устройство оптимальным для выбора качестве агрегирующего коммутатора и коммутатора доступа ЦОД.

  Сервисный модуль FWSM для Cisco Catalyst 6500 Series. Этот модуль реализует функции встроенного высокопроизводительного межсетевого экрана для коммутатора Catalyst 6500 Series. Он обеспечивает пропускную способность на уровне 5 Гбит/с, поддерживает 100,000 соединений в секунду и 1 миллион параллельных соединений. В одном корпусе могут быть установлены до четырех таких модулей; таким образом, совокупная пропускная способность корпуса может достигать 20 Гбит/с. Модуль FWSM для Catalyst 6500 Series, базирующийся на технологии Cisco PIX ®, обеспечивает крупным компаниям и провайдерам услуг непревзойденный уровень безопасности, надежности и производительности.
- **Сервисный модуль IDSM-2 или сенсор Cisco IDS 4200 Series для Cisco Catalyst 6500 Series.** Сенсоры Cisco IDS 4200 Series используют инновационные интеллектуальные методики обнаружения угроз в различных сочетаниях, в том числе такие методики, как распознавание характерных шаблонов с учетом состояния, синтаксический разбор протоколов, эвристическое обнаружение угроз и обнаружение аномалий состояния. В совокупности эти методики позволяют обеспечить всеобъемлющую защиту как от известных, так и от неизвестных киберугроз. Ожидающая патента технология Threat Analysis Micro-Engine (T.A.M.E) позволяет выполнять детальное конфигурирование сигнатур сенсоров, что дает возможность проводить тонкую настройку сенсоров и существенно уменьшать тем самым количество "ложных угроз". В семейство Cisco IDS 4200 Series входят четыре продукта: сенсоры Cisco IDS 4215, IDS 4235, IDS 4250 и IDS 4250 XL. Сенсор Cisco IDS 4250 XL обеспечивает непревзойденную производительность на скорости 1 Гбит/с благодаря специализированному механизму аппаратного ускорения, позволяющему защитить полностью насыщенные гигабитные соединения, равно как и многие частично используемые гигабитные подсети. Интеграция модуля IDSM-2 для Cisco Catalyst 6500 Series в корпус Catalyst 6500 Series облегчает процедуру установки и позволяет более эффективно использовать пространство в стойке.
- **Сервисный модуль SSL Services Module для Cisco Catalyst 6500 Series.** Этот модуль интегрируется в коммутатор Catalyst 6500 Series и обеспечивает увеличение числа поддерживаемых защищенных соединений. Такие защищенные соединения позволяют повысить производительность web-приложений путем снятия с серверов задачи шифрования трафика с помощью протокола SSL, интенсивно потребляющей ресурсы процессора. Применение протокола SSL позволяет обеспечить должный уровень конфиденциальности и аутентификации. Средства взаимодействия по SSL используют широкий диапазон сертификатов, которые располагаются в памяти данного модуля. Это позволяет централизовать процесс управления сертификатами и исключить необходимость в управлении сертификатами, размещенными на нескольких серверах. Наличие единственной копии сертификата вместо нескольких копий, разбросанных по разным серверам, позволяет снизить затраты. Данный модуль поддерживает до 3000 установленных соединений в секунду (12 000 на корпус); модуль обеспечивает возможность шифрования со скоростью 300 Мбит/с (1,2 Гбит/с на корпус), обеспечивая при этом поддержку 60,000 параллельных клиентских соединений (240 000 на корпус).
- **Модуль Cisco ACE.** Модуль Cisco ACE интегрирует мощные функции коммутации контента на уровнях с 4 по 7 в коммутаторы Cisco Catalyst 6500 Series и обеспечивает высокопроизводительное распределение нагрузки с высоким уровнем доступности. Модуль Cisco ACE обеспечивает гибкие возможности повышения производительности и надежности крупных групп серверов благодаря таким функциям, как дублирование с полным учетом состояния соединений, постепенный запуск и корректное завершение работы сервера, поддержка SYN cookies, поддержка постоянных соединений HTTP 1.1, поддержка постоянных соединений с использованием файлов cookie и URL, глобальное распределение нагрузки между серверами, контроль состояния маршрутов, контроль соединений с использованием сценариев, мониторинг состояния системы в процессе работы, проверка кодов откликов HTTP.
- **Модули Cisco Guard и детекторы Cisco Traffic Anomaly.** Эти модули, предназначенные для коммутаторов Cisco Catalyst 6500 Series, позволяют автоматически выявлять широчайший спектр DDoS-атак, угрожающих сегодня компаниям, и противостоять им. Благодаря этим встроенным функциям безопасности сетевая инфраструктура в состоянии выдержать даже самые тяжелые атаки DDoS и обеспечить защиту ЦОД и связанных с ним критически важных приложений.
- **Коммутаторы Cisco семейства MDS 9000.** Семейство Cisco MDS 9000 предлагает полную линейку продуктов, позволяющих удовлетворить требования к построению сетей хранилищ

самых разных размеров и архитектурных типов. Продукты семейства Cisco MDS 9000 реализуют интеллектуальные сетевые сервисы, такие как сети VSAN и всеобъемлющие сервисы безопасности; они поддерживают мощные средства управления трафиком, интеллектуальной диагностики и унифицированного управления SAN. Коммутаторы класса "директор" Cisco MDS 9500 Series и матричные коммутаторы Cisco MDS 9200 Series обеспечивают интеграцию различных протоколов и транспортных сред в рамках единой открытой платформы, способной поддерживать интеллектуальные сервисы хранилищ, например, механизм виртуализации на сетевом уровне. Благодаря многоуровневому подходу к реализации интеллектуальных функций сетевой инфраструктуры и хранилищ данных решения Cisco семейства MDS 9000 открывают новую эру в технологиях построения сетевых хранилищ.

- **Cisco Security Agent.** Этот программный компонент, устанавливаемый на хостах, идентифицирует и блокирует злонамеренные действия, устраняя известные и пока неизвестные ("0 day") угрозы безопасности и помогая снизить затраты на эксплуатацию. Cisco Security Agent агрегирует и расширяет функции обеспечения безопасности оконечных устройств за счет реализации таких возможностей, как предотвращение вторжений на хост, создание распределенных межсетевых экранов, защита от вредоносного мобильного кода, обеспечение целостности ОС и консолидация журналов аудита, – и все это в рамках одного-единственного продукта.

ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ

Дополнительную информацию о решениях Cisco для обеспечения безопасности можно найти на web-сайтах, адреса которых приведены ниже.

Коммутаторы семейства Cisco Catalyst 6500 Series
http://www.cisco.com/en/US/products/hw/switches/ps708/

Коммутаторы Cisco семейства MDS 9000
http://www.cisco.com/go/storagenetworking

Сервисный модуль FWSM для Cisco Catalyst 6500 Series
http://www.cisco.com/en/US/products/hw/modules/ps2706/ps4452/

Сенсор DS 4200 Series Sensor
http://www.cisco.com/en/US/products/hw/vpndevc/ps4077/

Сервисный модуль IDSM-2 для Cisco Catalyst 6500 Series
http://www.cisco.com/en/US/products/hw/modules/ps2706/ps5058/

Сервисный модуль SSL для Cisco Catalyst 6500 Series
http://www.cisco.com/en/US/products/hw/modules/ps2706/ps4156/

Модуль Cisco ACE
http://www.cisco.com/en/US/products/ps6906/

Программное обеспечение Cisco Security Agent
http://www.cisco.com/en/US/products/sw/secursw/ps5057/

Безопасность VLAN
http://www.cisco.com/warp/public/cc/pd/si/casi/ca6000/prodlit/vlnwp wp.pdf

Cisco Systems
Россия, 115054, Москва,
бизнес-центр
«Риверсайд Тауерс»
Космодамианская наб., 52,
стр. 1, этаж 4
Тел.: +7 (495) 961 14 10
Факс: +7 (495) 961 14 60
www.cisco.ru
www.cisco.com

Cisco Systems
Россия, 191186,
Санкт-Петербург,
бизнес-центр «Регус»
Невский проспект, 25,
этаж 2, офис 30
Тел.: +7 (812) 346 77 17,
Факс: +7 (812) 346 78 00
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
www.cisco.ru
www.cisco.com

Cisco Systems
Украина, 252004, Киев,
бизнес-центр
«Горайзон Тауерс»
Ул. Шовковична, 42-44,
этаж 9
Тел.: + 7 (38044) 490 36 00
Факс: + 7 (38044) 490 56 66
www.cisco.ua
www.cisco.com

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the **Cisco Website at www.cisco.com/go/offices.**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus • Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong • SAR • Hungary • India • Indonesia • Ireland • Israel •Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe