

Начинающему СІО

Обеспечение безопасности



Евгения ШУМИЛОВА,
ведущий инженер
компании ComPTek

Оснащение сети средствами безопасности начнем с пограничного (edge) уровня, устройства которого обеспечивают выход «во внешний мир». Обязательным элементом данного уровня является маршрутизатор доступа, обеспечивающий как обработку пакетов на границе с WAN-сетью, так и терминирование сервисов IP-телефонии. В качестве такого устройства рекомендуем использовать одну из моделей маршрутизаторов с интегрированными сервисами Cisco ISR. Эти маршрутизаторы способны выполнять широкий набор функций сетевой защиты, но с учетом небольшого масштаба рассматриваемой сети (порядка 500 рабочих станций) лучше возложить эти функции на отдельное устройство Cisco ASA, устанавливаемое за маршрутизатором доступа.

В первой статье серии «Начинающему СІО» (Connect! № 12/2007) подробно рассматривались три из четырех основных характеристик современных ЛВС – производительность, надежность, и управляемость. Теперь пришло время поговорить о четвертой характеристике – безопасности. Технические средства обеспечения безопасности мы постараемся «наложить» на ту структуру сети, которая была описана в двух предыдущих статьях («Начинающему СІО: архитектура сети», Connect! № 3/2008; № 4/2008). Напомним, что в серии «Начинающему СІО» рассматривается относительно небольшая корпоративная сеть (до 500 рабочих мест). В качестве примеров технических решений приводятся продукты компании Cisco (см. рисунок).

ASA на границе

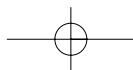
ASA (Adaptive Security Appliance) – многофункциональный программно-аппаратный комплекс, выполняющий, в частности, функции межсетевого экрана и системы предотвращения атак (IPS). Система Cisco IPS обнаруживает вредоносную активность в трафике и способна блокировать атаки в режиме реального времени. Сегодня поддерживается более 1500 сигнатур атак в таких протоколах, как IP, TCP, UDP, DNS, FTP и HTTP, причем возможно постоянное обновление сигнатур.

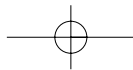
Функции IPS могут быть реализованы различными способами, например, программно (в IOS) на маршрутизаторах ISR или на отдельном устройстве. Однако для рассматриваемого проекта первый вариант чреват проблемами с производительностью маршрутизатора (алгоритмы IPS сильно загружают процессор), а второй – «великоват» и дорогое.

Оптимально, как уже говорилось, использовать функции IPS в устройстве ASA, где они реализуются с помощью специального модуля.

Система Cisco IPS обеспечивает также частичную защиту от атак типа «отказ в обслуживании» (DOS). Однако, на наш взгляд, компания с штатом в несколько сот сотрудников вряд ли способна сама эффективно защититься от DOS-атак, особенно от распределенных (DDOS), – такую защиту ей должен обеспечить оператор связи. Даже если компания готова потратиться на эффективные средства защиты от атак DOS и DDOS, в ходе таких атак могут быть «забиты» все каналы доступа в WAN-сеть и Интернет. И это еще одна причина, по которой целесообразно поручить защиту оператору.

Говоря об ASA, стоит отметить, что вместо модуля IPS в данное устройство можно поставить другой модуль – CSC (Content Security and Control), ко-

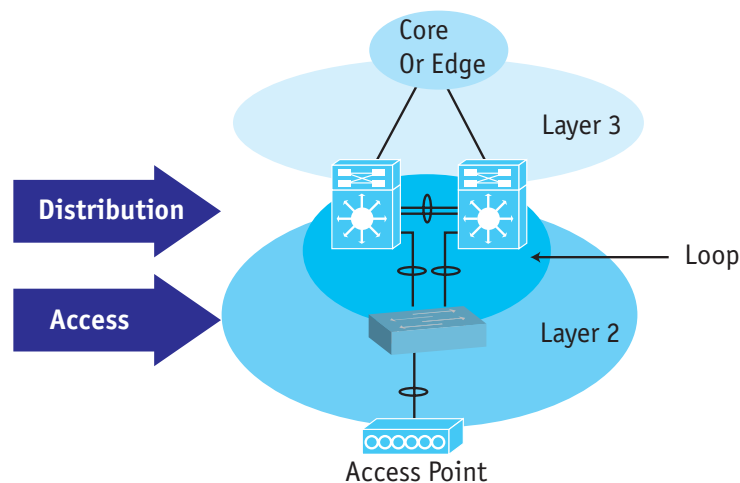




торый обеспечивает функции антиспама, антивируса и антифишинга (защиты от перехвата и подмены идентификационной информации). Однако в рассматриваемом проекте эти функции можно реализовать и в других точках, например на компьютерах конечных пользователей или на сервере-посреднике, а место в ASA отдать под модуль IPS. Кстати, компания Cisco предлагает выделенные устройства IronPort, которые выполняют не только функции CSC, но и массу других. Но это уже очень мощные и дорогие решения, ориентированные на крупные предприятия.

Управление доступом

Обеспечив (с помощью устройства ASA) сетевую безопасность на периметре сети, обратимся к задаче управления доступом корпоративных пользователей. Центрированно она лучше решается с помощью сервера Cisco ACS (Access Control Server). Он поддерживает все широко используемые механизмы аутентификации (RADIUS, TACACS+,



коммутаторам). Она позволяет проверить конечный узел и приписать его к подходящей сети VLAN. Но аутентификация 802.1x и приписка узла к VLAN-сети осуществляются после входа в домен Windows, что может затруднить обновление групповых политик. Конечно, при наличии «правильных» клиентов, например Cisco Secure Services Client, эти проблемы решаются, но важно подчерк-

никационную розетку к сети, то для доступа к важным ресурсам и приложениям ему все равно потребуется ввести пароль. Так что ответ на вопрос о необходимости применения технологии 802.1x далеко не очевиден.

А вот что совершенно ясно, так это польза функции Port Security, имеющейся в большинстве современных коммутаторов. Она позволяет, например, ограничить количество MAC-адресов на порт коммутатора (если ПК подсоединяется к ЛВС через IP-телефон, то на порт коммутатора приходится три MAC-адреса), что исключает несанкционированное подключение пользователями дополнительных устройств. Такое подключение чревато не только проблемами безопасности, но и сбоями в работе сети из-за возможных петель на уровне 2 (L2 Loop). Кроме того, функция Port Security исключит возможность переполнения таблицы MAC-адресов коммутатора.

Защита на уровне хостов

Для защиты от вредоносных действий приложений мы рекомендуем решение CSA (Cisco Security Agent), состоящее из сервера и программ, устанавливаемых на компьютерах конечных пользователей. Решение CSA

Архитектура ЛВС
небольшой компании

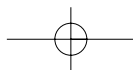
Система Cisco IPS обнаруживает вредоносную активность в трафике и способна блокировать атаки в режиме реального времени.

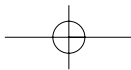
LDAP, AD и др.) и стандарт 802.1x, кроме того, может быть интегрирован с решениями различных производителей токенов, одноразовых паролей и смарт-карт. Этот сервер способен ограничивать доступ по времени, количеству сессий и другим параметрам, а также предоставляет возможность проверки дополнительных условий перед разрешением доступа в сеть.

Хотелось бы сказать пару слов о технологии 802.1x, которая обеспечивает аутентификацию на уровне 2 (при подключении к

нуть, что использование технологии 802.1x не сводится к принципу plug-and-play. Для ее корректной работы может потребоваться серьезная совместная работа сетевых менеджеров с администраторами систем Windows.

Кроме того, возникает вопрос: «А зачем вообще нужна аутентификация на уровне 2?» Ситуации, когда посторонний приходит на ваше рабочее место и подключает свой ноутбук, можно исключить и другими способами. Но даже если злоумышленник с ноутбуком подключится через вашу комму-





объединяет в себе различные защитные механизмы и функции: предотвращение атак, персональный межсетевой экран, защиту от вредоносного кода, блокирование утечки информации через USB-порты и другие внешние устройства (PCMCIA, CD и т. д.), ограничение возможностей интернет-пейджеров (например, ICQ) и т. п. За счет интеграции с технологией Intel AMT система CSA позволяет контролировать загрузку с несанкционированных носителей (CD, дискет, сети и пр.). Агенты CSA функционируют на плат-

на дополнительно приобретаемом выделенном устройстве Cisco NAC Appliance. Но в любом случае развертывание и использование NAC требуют высокой квалификации и дополнительных временных и денежных затрат. Например, недостаточно зафиксировать, что антивирусный пакет устарел, нужно еще обеспечить возможность его обновления, а для этого необходим дополнительный сервер – и так на все основные программы. Короче, NAC – явно не для «начинающего CIO». Для рассматриваемой

отображение пути распространения атаки в режиме реального времени. Отсекая ложные срабатывания и в то же время обнаруживая атаки, пропущенные отдельными средствами защиты, система MARS позволяет повысить скорость локализации проблем в сети и эффективность их устранения.

Будучи чрезвычайно важным компонентом сети, система безопасности должна быть надежной. Для повышения отказоустойчивости все перечисленные средства можно (а в некоторых случаях и нужно) продублировать. Так, вполне логично резервировать маршрутизатор ISR (или хотя бы его блоки питания), установить два устройства ASA (в режиме fail over), лучше два сервера ACS. Впрочем, конкретные рекомендации могут меняться в зависимости от специфики сети: одно дело, когда она обслуживает обычный офис, и совсем другое, когда обеспечиваются финансовые транзакции.

Рисуя полную картину безопасности, необходимо сказать и о разработке единой политики безопасности. Собственно говоря, именно с нее и надо начинать, а уже под выработанную политику подбирать технические средства безопасности. Политика безопасности должна предусматривать не только технические, но и административные меры: установление правил смены пароля и правил удаленного доступа, разделение сфер ответственности и установление ответственности отдельных сотрудников. Кроме того, необходимо предусмотреть комплексный подход к решению задач обеспечения безопасности. Согласитесь, глупо вкладывать огромные средства в электронные системы защиты, если не обеспечена физическая защита серверов и сетевого оборудования, и можно просто зайти в серверную, открыть шкаф и унести под мышкой сервер с важнейшей информацией. Так что не забудьте и о надежных замках в технологические помещения. ■

Компания Cisco предлагает выделенные устройства IronPort, которые выполняют не только функции CSC, но и массу других.

формах Windows, Linux, Solaris и VMware. Короче говоря, это очень полезное средство обеспечения безопасности, но для его настройки и отладки потребуется отдельный специалист – хотя бы в первый месяц после инсталляции системы.

В последнее время вошел в моду термин NAC, или Network Admission Control. Эта технология позволяет предотвратить доступ к корпоративным ресурсам устройств, не отвечающих политике безопасности, например, таких, на которых нет должного сервисного пакета (Service Pack) операционной системы, устарел антивирус, обнаружена вредоносная программа и т. п. При обнаружении такого несоответствия доступ узла блокируется либо узел перенаправляется в карантинную сеть, в которой на него может быть установлено отсутствующее ПО. Есть два варианта NAC: не требующий каких-либо дополнительных затрат (NAC Framework) и основанный

модели сети эту технологию можно рекомендовать только при наличии у заказчика свободных денег и ресурсов.

Управление безопасностью и политика безопасности

Как уже говорилось, для установки в сети рекомендуется несколько различных средств защиты, причем желательно иметь единый центр управления всеми угрозами безопасности. Для этой цели служит система Cisco MARS (Monitoring, Analysis and Response System), которая собирает информацию с сетевого оборудования, средств защиты, журналов регистрации ОС и приложений. Она способна проанализировать и сопоставить события, информация о которых получена от разных средств защиты. Возможна визуализация наиболее важных событий на карте сети, а также

