Виталий Зорин

Система защищенного доступа в Internet

Решение для защиты от атак на браузер и почтового клиента

Неконтролируемый и незащищенный доступ в Internet из корпоративной сети представляет определенную опасность для корпоративной информационной системы. Internet не является доверенной средой, поэтому любая поступающая оттуда информация может рассматриваться как потенциальный источник угрозы. Как правило, клиентским программным обеспечением для доступа в Internet является браузер типа Microsoft Internet Explorer или Netscape Communicator. При свободной и неконтролируемой работе пользователей в среде Internet браузер осуществляет соединение с различными Web-сайтами по протоколу HTTP/1.1. Следует отметить, что актуальная версия HTTP/1.1 (в отличие от HTTP/1.0) может передавать данные между браузером и Web-сайтом в обоих направлениях, что увеличивает количество вариантов проникновения вредоносного кода на компьютер пользователя и в конечном счете облегчает вторжение в корпоративную сеть.

Известны два вида атак из среды Internet, которые не могут быть отражены методом защиты периметра, так как разрушительный код проникает через открытые шлюзы, которые принципиально не могут быть закрыты:

- атаки на браузер при посещении Web-сайтов;
- атаки на почтового клиента.

В первом случае при выводе HTML-страниц Web-сайта вредоносный мобильный код, включенный в страницу, автоматически начнет выполняться на системе клиента. Атаки на почтового клиента происходят при получении сообщения электронной почты в формате HTML с внедренным разрушительным кодом. Как только сообщение открывается или просматривается в окне предварительного просмотра, мобильный код начинает выполняться. И в том и в другом случае HTML-документы содержат небольшие части кода, которые могут выполняться при открытии документа. Этот код способен нанести ущерб, так как он имеет доступ ко многим системным ресурсам. Мобильный код в виде Java-апплетов, Java-сценариев и компонентов ActiveX проникает в компьютеры компании при работе с информационными ресурсами сети Internet. Неконтролируемые апплеты не копируют себя и не разрушают данные, как делают это вирусы, но они часто предпринимают атаки, ведущие к краже информационных ресурсов или к нарушению работы информационной системы компании.

Виталий Зорин (zorin@elvis.ru) — системный аналитик ОАО «Элвис-Плюс», к.т.н.

Предназначение системы

Задача предлагаемого решения состоит в обеспечении безопасной работы пользователей корпоративной сети с Internet. Решение предназначено для защиты внутренних сегментов сети от проникновения вредоносного кода при работе браузера пользователя с ресурсами Internet либо при получении почтовым клиентом пользователя электронных сообщений в формате HTML от неизвестных/недоверенных источников. Решение может применяться в любых коммерческих и государственных сетях, работающих с конфиденциальной информацией и имеющих необходимость использовать Internet, для которых жизненно важным является обеспечение конфиденциальности, целостности и доступности информации.

Выбор решения

Существует типовое решение для безопасного доступа корпоративных пользователей в Internet, включающее организационно-правовые и программно-технические методы.

К организационно-правовым методам относится разработка корпоративных правил работы с Internet, соблюдение которых рассматривается как одно из условий при найме сотрудников и как один из важных пунктов заключаемого с сотрудником контракта. Обычно вводная часть правил содержит требования общего характера:

- необходимость подписания сотрудником соглашения о правилах пользования Internet;
- разрешение пользования ресурсами Internet только по служебной необходимости;
- условие периодической перлюстрации сообщений электронной почты для исключения нецелевого использования;
- условие периодического аудита журналов работы в Internet.

Правила должны определять допустимые действия пользователя в процессе его работы с Internet, которые излагаются в основной части правил:

- разрешение на работу с Internet только по авторизованным протоколам (состав протоколов определяется индивидуально);
- недопустимость несанкционированной установки программного обеспечения, загруженного из Internet;
- запрет доступа к популярным развлекательным (игровым, музыкальным и т. д.) Web-сайтам, определен-

ным группам новостей Usenet, которые не имеют отношения к выполняемой сотрудником работе;
• разрешение на загрузку из файлов Internet только при условии их проверки антивирусными средствами;
• запрет на передачу служебной информации лицам, не работающим в компании;
• запрет на «обход» корпоративных систем безопасности;
• недопустимость дискредитации компании в Internet-форумах, дискуссионных комнатах и т. п.;
• запрет на отправку спама по электронной почте.

Правила должны четко определять ответственность пользователя за их нарушение, например: ограничение или запрет доступа в Internet, увольнение, преследование в судебном порядке по статьям ТК РФ, КоАП РФ или УК РФ. Правила и соглашения по работе с Internet должны быть проверены юристом организации на предмет соответствия законодательству и доведены до сведения всех сотрудников.

Программно-технические методы, как правило, заключаются в применении следующих систем:
• управления доступом в Internet групп пользователей;
• аудита доступа пользователей;
• антивирусной защиты, обнаружения и предотвращения вторжений;
• предотвращения обхода сотрудниками механизмов безопасности;
• контроля несанкционированной установки программ и вредоносного кода.

Если первые четыре системы можно реализовать на основе существующих программно-технических средств, то защита от несанкционированного внедрения вредоносного мобильного кода является практически неразрешимой задачей.

Во-первых, механизм проверки подлинности посредством цифровой подписи, например для ActiveX-компонентов, не позволяет работать с программными компонентами большинства Web-сайтов, не подписывающих свои компоненты. Кроме того, непонятен результат проверки подписи, если неизвестен ни подписчик, ни удостоверяющий центр, подписавший сертификат.

Во-вторых, несмотря на наличие сенсоров вредоносного мобильного кода (например, продукт AppletTrap компании Trend Micro), возможно опережающее нанесение ущерба системе до получения результатов проверки поведения мобильного кода в ограниченной среде (методом sandboxing).

В-третьих, как правило, создание и применение хакерами новых вирусов и вредоносного мобильного кода опережает по времени разработку средств защиты. В таких условиях наличие самых последних обновлений защитных средств не может обеспечить гарантию от несанкционированного проникновения злоумышленников во внутреннюю сеть компании через браузеры и почтовые клиенты пользователей, работающих с Internet.

В связи с этим, с одной стороны, необходим «вынос» пользовательских приложений, работающих с ресурсами Internet, за пределы внутренней защищенной сети компании, а с другой — требуется обеспечить пользователям возможность работы с такими приложениями.

На наш взгляд, эти противоречивые требования можно удовлетворить путем создания дополнительной демилитаризованной зоны (DMZ-2 на рис.1), на многопользовательских серверах которой будут работать все клиентские Internet-приложения. Данная зона существенно ограничит возможности вредоносного кода по отношению к приложениям и информационным ресурсам внутренней сети компании. Она в какой-то степени будет играть роль ограниченной среды типа sandboxing по аналогии с механизмами безопасности Java. Постоянный аудит среды DMZ-2, применение средств обнаружения вторжений, антивирусных продуктов, специальных методов за-

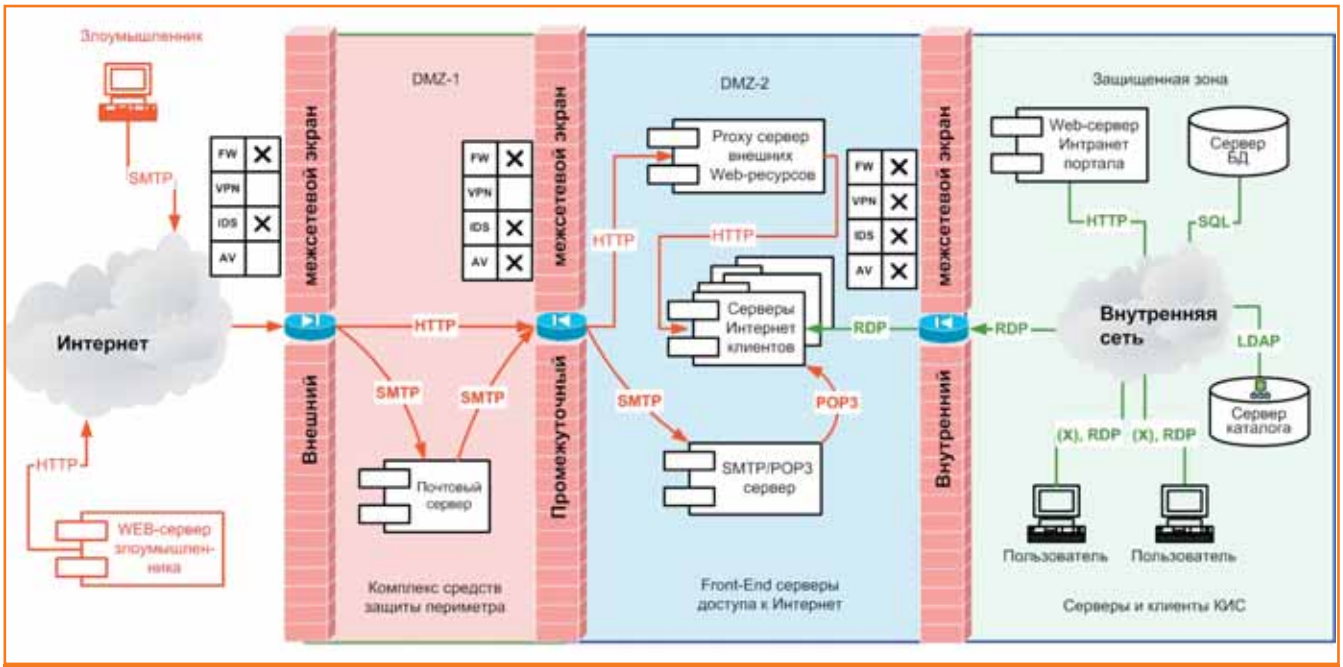

Рисунок 1. Архитектура решения

щиты от вредоносного кода обеспечат своевременное выявление, а также активную защиту от любых атак через клиентские Internet-приложения. С этой точки зрения среда DMZ-2 является защищенной на уровне современных требований и типовых решений. Однако она не может быть квалифицирована как доверенная среда с учетом трех приведенных выше аргументов.

Основная проблема — обеспечение возможности работы пользователей с клиентскими Internet-приложениями из внутренней, доверенной среды. На наш взгляд, такая проблема может быть решена с помощью терминального доступа. На многопользовательских серверах Internet-клиентов устанавливаются серверы терминальных служб, которые обеспечивают работу пользователей внутренней сети с Internet-приложениями через «сверхтонкий» терминальный клиент. Известно, что при терминальном взаимодействии между клиентом и сервером не передается какой-либо программный код, в том числе — мобильный вредоносный код. От терминального клиента к серверу следует поток кодов нажатых клавиш клавиатуры и состояний мыши пользователя, а обратно, от сервера клиенту, поступают бинарные образы экранов серверной сессии Internet-браузера или почтового клиента пользователя. Таким образом, с помощью терминального доступа пользователей к клиентским Internet-приложениям можно полностью изолировать внутреннюю доверенную среду сети компании от вероятного проникновения разрушительного мобильного кода из Internet.

Архитектура системы

Техническая структура, определяющая состав и размещение в сети комплекса средств защиты доступа в Internet, включает (см. рис.1):

- комплекс средств защиты периметра;
- многопользовательские серверы Internet-клиентов;
- proxy-сервер внешних Web-ресурсов.

Структура программных компонентов состоит из серверных и клиентских компонентов с описанием интерфейса и схемы их размещения на элементах технической структуры.

В состав серверных компонентов входят приложения:

- терминальных служб;
- защиты от вредоносного мобильного кода;
- антивирусной защиты;
- системы обнаружения и предотвращения вторжений;
- аудита безопасности.

В состав клиентских компонентов входят браузеры и почтовые программы, запускаемые пользователями на серверах DMZ-2 через терминальный доступ, а также терминальные клиенты, установленные на рабочих станциях пользователей внутренней сети. Для защиты от проникновения во внутреннюю сеть через внутренний межсетевой экран (открытый порт для терминального протокола) на многопользовательских серверах Internet-клиентов и рабочих станциях пользователей устанавливаются клиенты VPN. Клиенты обеспечивают терминальному протоколу защищенный транспорт через внутренний брандмауэр и недоверенную зону DMZ-2.

Кроме того, на все серверы и рабочие станции зоны DMZ-2 устанавливаются клиентские приложения антивирусной защиты, защиты от вредоносного мобильного кода, системы обнаружения (сенсоры) и предотвращения вторжений.

Средства защиты периметра

Защита сетевого периметра осуществляется за счет межсетевого экранирования, в результате которого формируются две демилитаризованные зоны (DMZ-1 и DMZ-2). Зона DMZ-1 содержит серверы, которые должны быть доступны из Internet, такие как почтовый SMTP-сервер, публичный Web-сервер, FTP-сервер, DNS-сервер. Из-за возможности сканирования публичных серверов этой зоны и реальных попыток вторжения данная зона является недоверенной, но контролируемой областью. Контроль в виде протоколирования и аудита событий доступа из Internet, а также попыток сканирования и осуществления различных схем атак позволяет предотвратить возможное развитие вторжений и нанесение ущерба.

Внешний межсетевой экран обеспечивает функции экранирования, маскирование адресного пространства корпоративной сети посредством NAT, а также выполняет функции системы обнаружения вторжений.

Кроме функций брандмауэра, промежуточный межсетевой экран выполняет функции системы обнаружения вторжений (IDS) и антивирусной защиты входящего SMTP-трафика.

Не показанный на рис.1 сервер аудита обеспечивает через собственные адаптеры сбор и обработку событийной информации с систем обнаружения вторжений, данных от межсетевого экрана, а также от средств антивирусной защиты. Дополнительная информация по комплексу средств защиты периметра и типовой системе обнаружения и предотвращения вторжений содержится во врезке «Источники».

Терминальные службы серверов Internet-клиентов

В качестве терминальной службы была выбрана служба Terminal Services Windows 2000 Server. Выбор определила главным образом высокая производительность Terminal Services, так как в отличие от прототипа, терминального сервиса компании Citrix, терминальная служба Windows 2000 интегрирована с ядром операционной системы. Производительность работы также повышается за счет кэширования графических образов. Кроме того, служба Terminal Services интегрирована со службой балансировки сетевого трафика (NLB) Windows 2000 Advanced Server, за счет чего потребители получают

Литература

1. Подсистема защиты периметра. Решения компании «Элвис-Плюс». М., 2003. 13 с.
2. Подсистема защиты от вредоносных программ. Решения компании «Элвис-Плюс». М., 2003. 11 с.
3. Подсистема предотвращения вторжений. Решения компании «Элвис-Плюс». М., 2003. 11 с.
4. Windows Server 2003. Terminal Server Capacity and Scaling. White Paper. MS., 2003. 39 p.

встроенную возможность дополнительной масштабируемости при организации многомашинных комплексов (ферм).

В документации по Windows 2000 Server приведены данные по количеству одновременно работающих пользователей на одном терминальном сервере в зависимости от технических характеристик сервера и типа операционной системы (Windows 2000 или Windows 2003 Server). При тестировании моделировалась работа пользователей с приложениями Microsoft Office. Так, например, для конфигурации двухпроцессорного сервера с Intel Xeon частотой 2,4 ГГц, кэшем второго уровня емкостью 2 Мбайт и оперативной памятью 4 Гбайт и при использовании Windows 2000 Server зарегистрирована возможность одновременной работы 200 пользователей. В той же конфигурации сервера, но при использовании Windows 2003 Server количество пользователей увеличивалось почти в два раза. Клиент терминальной службы позволяет задействовать наследуемые системы Windows — 32-разрядный терминальный клиент работает под Windows 95, 98, NT Workstation 3.51, 4.0, Windows 2000 Professional.

Установка Terminal Services поддерживает выполнение всех клиентских Internet-приложений на сервере, обеспечивая тем самым безопасность рабочих станций внутренней зоны корпоративной сети. Терминальная служба должна быть настроена только на выполнение браузера Internet (например, MS Internet Explorer) и почтового клиента (например, Outlook).

Для защиты от перехвата терминальной сессии, а также от атак на открытый для протокола RDP порт внутреннего брандмауэра производится защита трафика между сервером и клиентом в транспортном режиме протокола IPSec. На терминальный сервер устанавливается VPN-клиент «ЗАСТАВА-Сервер», а на рабочие станции пользователей — VPN-клиент «ЗАСТАВА-Клиент». Внутренний брандмауэр закрывает все порты (кроме UDP-порта 500 для протокола обмена ключами IKE) и разрешает соединение между DMZ-2 и защищенной зоной только по протоколу IPSec. Если использовать IPSec по каким-либо причинам невозможно, допустимо применение механизмов шифрования, встроенных в терминальную службу. Однако при этом нельзя гарантировать, что злоумышленник не проникнет в защищенную зону через открытый порт.

В соответствии с рекомендациями компании Microsoft сервер с терминальной службой не должен устанавливаться на контроллере домена. Домен серверов и рабочих станций, расположенных в DMZ-2, не должен быть связан с доменами защищенной зоны.

Proxy-сервер внешних Web-ресурсов

Proxy-сервер внешних Web-ресурсов предназначен для управления доступом пользователей к ресурсам Internet. При этом действуют установленные корпоративные правила работы с Internet, в том числе определяющие доступ отдельных групп пользователей к его ресурсам. Proxy-сервер реализован на базе продукта ISA Server 2000 компании Microsoft. ISA-сервер обладает широкими возможностями фильтрации информационного содержимого сети Internet. Помимо фильтрации по адресам IP, доменным именам, URL, контенту Web-страниц и расписанию, ISA-сервер обеспечивает кэширование внешней информации, что существенно уменьшает время выполнения запроса для пользователей.

Защита от вирусов и вредоносного мобильного кода

Система антивирусной защиты устанавливается как на серверах и рабочих станциях, размещенных в DMZ-2, так и на SMTP-шлюзе для контроля и фильтрации почтовых сообщений. Система защиты от вредоносного мобильного кода устанавливается на серверах Internet-клиентов и на SMTP-шлюзе. Средства системы позволяют проверять (по сигнатуре и цифровой подписи) и блокировать известный вредоносный мобильный код, загружаемый браузерами из сети Internet или внедренный в почтовые сообщения, имеющие HTML-формат. Неизвестный мобильный код проходит проверку по технологии тестирования в изолированной среде — sandboxing.

Рекомендации

Для обеспечения пользователям корпоративной сети защищенного доступа в Internet требуется применять как типовые подходы, так и специальные методы.

Типовые подходы заключаются в организационно-правовых мероприятиях и разработке системы обеспечения безопасного доступа к Internet.

Организационно-правовые мероприятия должны включать разработку и утверждение корпоративных правил доступа пользователей в Internet, а также юридически обоснованных норм ответственности за их нарушение.

Система обеспечения безопасного доступа должна содержать: комплекс средств защиты периметра корпоративной сети; proxy-сервер, регламентирующий и контролирующий доступ групп пользователей к ресурсам Internet; средства обнаружения и предотвращения вторжений, а также средства защиты от вирусов и вредоносного мобильного кода.

Типовой подход не обеспечивает полную и гарантированную защиту от проникновения разрушительного мобильного кода через браузеры пользователей и почтовые сообщения в формате HTML.

Специальный подход заключается в создании особой демилитаризованной зоны, в которой размещаются многопользовательские серверы Internet-клиентов с установленной на них терминальной службой. Данная демилитаризованная зона изолирована от защищенной зоны корпоративной сети посредством межсетевого экранирования. Рабочая станция пользователя защищенной зоны взаимодействует с Internet-браузером и почтовым клиентом через защищенную терминальную сессию. В терминальной сессии невозможно передать на рабочую станцию пользователя программный код, и вредоносный мобильный код в том числе.