МЕТАЛЛУРГИЯ

The perspectives of development of data networks at RUP «BMZ» are examined.

А. Г. НОВИКОВ, П. В. ПЕВНЕВ, РУП «БМЗ»

УДК 669.

ПЕРСПЕКТИВЫ РАЗВИТИЯ СЕТЕЙ ПЕРЕДАЧИ ДАННЫХ НА РУП «БМЗ»

На сегодняшний день локальная вычислительная сеть (далее ЛВС) РУП «БМЗ» – это распределенная инфраструктура более чем на 3000 портов. В большинстве случаев ЛВС сегментирована по логическому принципу. В подобных условиях обеспечение надежного контроля над доступом к сети и данным – трудоемкий, но необходимый процесс.

Специалистами управления автоматизации РУП «БМЗ» был проведен всесторонний анализ систем защиты доступа к сети с учетом эксплуатируемого на предприятии сетевого оборудования, клиентских операционных систем и серверных платформ. Анализ производился на основе следующих исходных данных.

- Широкое использование клиентских ОС Windows XP/Vista/7.
- Более 90% портов ЛВС построено на оборудовании Cisco Systems с поддержкой протокола 802.1x.
- На предприятии внедрена и расширяется служба Microsoft Active Directory.
- На предприятии используется единое корпоративное антивирусное ПО (Антивирус Касперского 6.0 для Windows Workstation).

Основной задачей, стоявшей перед специалистами, являлась реализация сервера политик для автоматической проверки подключаемых рабочих станций на соответствие критериям безопасности предприятия и назначения параметров подключения к ЛВС РУП «БМЗ».

Наиболее привлекательно (в наших условиях) выглядит служба Microsoft Network Access Protection (NAP).

Защита сетевого доступа (NAP) в Windows Server 2008

Защита доступа к сети (NAP) – это платформа применения политик, встроенная в операционные системы Microsoft Windows Vista, Microsoft Windows XP и Windows Server с кодовым названием Longhorn, которая обеспечивает повышенную безопасность сети за счет соответствия требованиям по поддержанию работоспособности системы.

Благодаря защите доступа к сети можно создавать специальные политики работоспособности для оценки состояния компьютера перед тем, как разрешить доступ или взаимодействие с сетью; автоматического обновления соответствующих требованиям компьютеров с целью обеспечения их постоянной совместимости; адаптации не соответствующих требованиям компьютеров таким образом, чтобы они удовлетворяли установленным требованиям.

Защита доступа к сети включает интерфейс прикладного программирования, который может быть использован разработчиками и поставщиками для создания полноценных решений по оценке с помощью политики работоспособности, ограничения доступа к сети и обеспечения постоянного соответствия требованиям.

Для оценки доступа к сети на основе работоспособности системы сетевая инфраструктура должна обеспечивать следующие функциональные области.

- Оценка с помощью политики работоспособности. Определяет, соответствует ли компьютер требованиям политики работоспособности.
- Ограничение доступа к сети. Ограничивает доступ для несовместимых компьютеров.
- Автоматическое исправление. Обеспечивает необходимые обновления для приведения несовместимых компьютеров к установленным требованиям.
- Обеспечение постоянного соответствия требованиям. Автоматическое обновление не соответ-

ствующих требованиям компьютеров с учетом постоянно изменяющихся требований политики работоспособности.

Сценарии защиты доступа к сети (NAP)

Представляя собой наиболее гибкое решение, защита доступа к сети взаимодействует с ПО поставщика, которое либо содержит агент System Health Agent (SHA) и средства оценки работоспособности системы System Health Validators (SHV), либо распознает опубликованный набор интерфейсов программирования. В качестве примеров решений сторонних поставщиков, которые работают с защитой доступа к сети, можно назвать антивирусную программу, виртуальную частную сеть или сетевое оборудование. Защита доступа к сети предоставляет решение для следующих распространенных сценариев.

Проверка работоспособности и состояния мобильных переносных компьютеров

С помощью защиты доступа к сети сетевые администраторы могут проверять состояние любого переносного компьютера, когда он повторно подключается к сети компании, без ущерба для его мобильности и гибкости.

Поддержание работоспособности настольных компьютеров

Благодаря дополнительному управляющему ПО можно создавать автоматические отчеты, выполнять автоматическое обновление компьютеров, не соответствующих требованиям, а в случае изменения администраторами политик работоспособности компьютеры могут автоматически получать последние обновления, которые предотвращают угрозы их работоспособности со стороны общедоступных ресурсов.

Определение состояния переносных компьютеров, получающих доступ в сеть

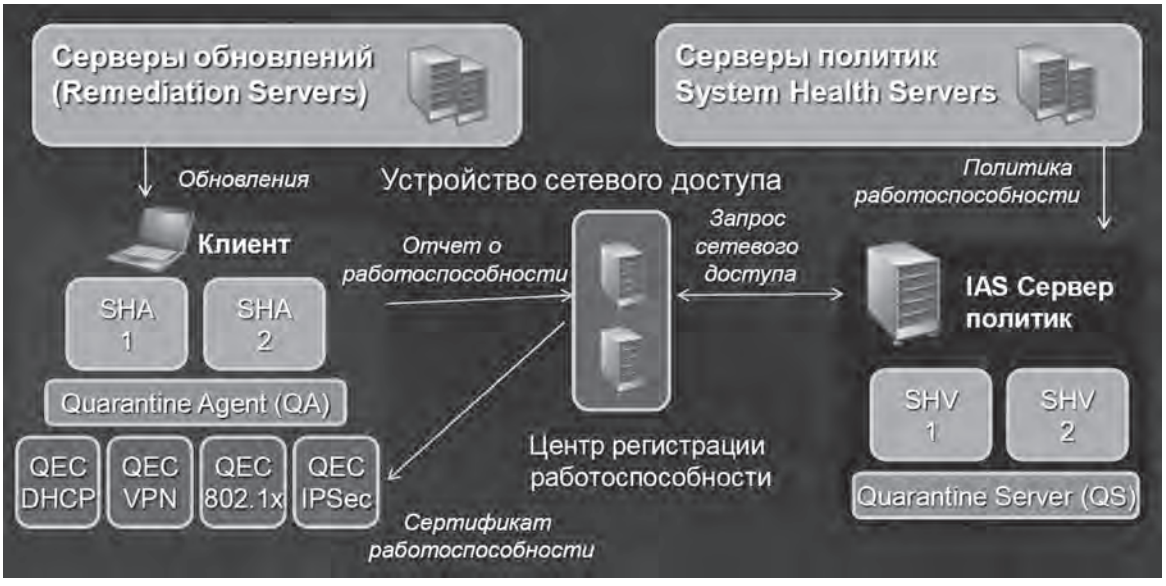
Благодаря защите доступа к сети администраторы могут определить, имеют ли посещающие ее переносные компьютеры полномочия на доступ и, если нет, лимитировать их доступ к ограниченной сети, не требуя обновления или изменения конфигурации этих переносных компьютеров.

Проверка соответствия требованиям и работоспособности неуправляемых домашних компьютеров

С помощью защиты доступа к сети (см. рисунок) сетевые администраторы могут проверять наличие необходимых программ, параметров реестра, файлов или их сочетания каждый раз, когда домашний компьютер подключается к сети через виртуальную частную сеть; также они могут лимитировать подключение к ограниченной сети, пока не будут выполнены требования к работоспособности системы.

NAP может работать в режиме мониторинга или в режиме изоляции

В режиме мониторинга авторизированные пользователи получают доступ к сети даже в том случае, если состояние их систем не удовлетворяет требованиям безопасности. Этим машинам присваивается соответствующий статус и администраторы могут дать пользователям необходимые инструкции. В изоляционном режиме неудовлетворяющие требования безопасности компьютеры переводятся в специальную карантинную сеть, где смогут установить все недостающие для утверждения ресурсы.



Компоненты защиты доступа к сети

Network Policy Server (NPS/RADIUS)

В компоненте RADIUS Network Policy Server (NPS) сервера Windows Server 2008 отсутствует компонент защиты доступа к сети (NAP) Enforcement Server (ES) или Enforcement Client (EC). Вместо этого он работает как сервер политик вместе с компонентами NAP ES и NAP EC. Администраторы должны задать требования к работоспособности системы в виде политик на сервере NPS. Серверы NPS обеспечивают проверку с помощью политик работоспособности и координируют свои действия со службой каталогов Active Directory каждый раз, когда компьютер пытается получить сертификат работоспособности или подключиться к точке доступа (коммутатору Ethernet) 802.1X, серверу виртуальной частной сети или службе DHCP-сервера.

Компоненты работоспособности

• Агенты работоспособности системы System Health Agents (SHA). Подтверждение работоспособности (состояние исправлений, сигнатуры вирусов, конфигурация системы и т. п.).

• Средства оценки работоспособности системы System Health Validators (SHV). Сертификация выводов агентов работоспособности.

• Серверы работоспособности системы System Health Servers. Определение требований к работоспособности системных компонентов клиента.

• Серверы исправления Remediation Servers. Установка необходимых исправлений, параметров конфигурации и приложений, а также обеспечение работоспособности клиентов.

Компоненты ограничения

• Клиент Enforcement Client (EC). Согласует условия доступа с устройствами доступа к сети.

• Устройство сетевого доступа. Обеспечивает сетевой доступ к работоспособным конечным точкам (это может быть коммутатор или точка доступа).

• Служба сертификации работоспособности. Выпускает сертификаты для клиентов, которые прошли проверку работоспособности.

Компоненты платформы

• Агент изоляции Quarantine Agent (QA). Создает отчеты о состоянии работоспособности клиентов и координирует действия SHA и EC.

• Сервер изоляции Quarantine Server (QS). Ограничивает доступ клиентов к сети на основе сертификатов SHV.

Механизмы применения защиты доступа к сети

Защита доступа к сети обеспечивает гибкую платформу, которая поддерживает несколько механизмов применения доступа, включая, но не ограничиваясь только ими:

- протокол IPsec для проверки подлинности на уровне узла;
- проверенные сетевые подключения на основе стандарта IEEE 802.1X;
- виртуальные частные сети для удаленного доступа;
- протокол DHCP.

Администраторы могут использовать эти технологии по отдельности или одновременно для ограничения не соответствующих требованиям компьютеров. Сервер NPS, заменивший службу проверки подлинности Windows Server 2003 в Windows Server 2008, действует как сервер политик работоспособности для всех этих технологий.

Защита доступа к сети требует, чтобы на серверах выполнялась ОС Windows Server 2008, а на клиентах – Windows Vista, Windows XP с пакетом обновления 2 (SP2) или Windows Server 2008.

IPsec Enforcement

IPsec Enforcement включает сервер сертификатов работоспособности и IPsec NAP EC. Сервер сертификатов работоспособности выпускает сертификаты X.509 для изоляции клиентов, после того, как определено их соответствие требованиям. Эти сертификаты затем используются для проверки подлинности клиентов NAP, когда они инициируют защищенные протоколом IPsec взаимодействия с другими клиентами NAP в интернет.

IPsec Enforcement ограничивает взаимодействие сети только с теми узлами, которые считаются соответствующими требованиям и поскольку здесь применяется протокол IPsec, можно задать требования к безопасным взаимодействиям с соответствующими требованиям клиентами на основе IP-адреса или номера порта TCP/UDP. IPsec Enforcement осуществляет взаимодействие только с совместимыми компьютерами, после того, как они получили допустимую конфигурацию IP-адреса. IPsec Enforcement – самая строгая форма ограничения доступа к сети платформы защиты доступа к сети (NAP).

802.1X Enforcement

802.1X Enforcement включает сервер NPS и компонент EAPHost NAP EC. С помощью 802.1X Enforcement сервер NPS отдает команду точке доступа 802.1X (коммутатору Ethernet или точке беспроводного доступа) разместить профиль ограниченного доступа на клиент 802.1X, пока он выполняет ряд функций по исправлению. Профиль ограниченного доступа может состоять из набора IP-фильтров или идентификатора виртуальной локальной сети для ограничения трафика клиента

802.1X. 802.1X Enforcement обеспечивает очень ограниченный доступ к сети для всех компьютеров, получающих доступ через подключение по стандарту 802.1X.

VPN Enforcement

VPN Enforcement включает компоненты VPN NAP ES и VPN NAP EC. С помощью VPN Enforcement серверы виртуальных частных сетей могут применять требования политики работоспособности каждый раз, когда компьютер пытается подключиться к сети через виртуальную частную сеть. VPN Enforcement обеспечивает очень ограниченный доступ для всех компьютеров, получающих доступ через подключение по виртуальной частной сети.

DHCP Enforcement

DHCP Enforcement включает компоненты DHCP NAP ES и DHCP NAP EC. С помощью DHCP Enforcement DHCP-серверы могут применять требования политики работоспособности каждый раз, когда компьютер пытается арендовать или обновить конфигурацию IP-адреса в сети. DHCP Enforcement – самый простой способ развертывания, потому что все клиентские компьютеры DHCP должны арендовать IP-адреса. Поскольку DHCP Enforcement использует записи в таблице маршрутизации, эта форма ограниченного доступа к сети платформы защиты доступа к сети является самой слабой.

Сервер NAP Administration Server

NAP Administration Server – это компонент сервера NPS, который координирует данные, полученные от всех средств оценки работоспособности системы (SHV), и определяет, должны ли компоненты NAP Enforcement Server (NAP ES) ограничивать доступ клиентов на основе требований политики работоспособности.

Средство System Health Validator

Средство System Health Validator (SHV) – это серверное ПО, которое проверяет, соответствует ли заявление о работоспособности Statement of Health (SoH), представленное агентом SHA, требуемому состоянию работоспособности. SHV выполняется на сервере NPS, который должен координировать выходные данные всех средств оценки работоспособности SHV. Средство оценки работоспособности использует ответ на заявление о работоспособности Statement of Health Response (SoHR), чтобы указать на соответствие или несоответствие требуемому состоянию работоспособности и дать команды по исправлению.

Политика работоспособности

Политика работоспособности указывает необходимые условия для неограниченного доступа. Политики работоспособности настраиваются на сервере NPS. В сети может применяться несколько политик работоспособности. Например, VPN Enforcement и DHCP Enforcement могут использовать разные политики.

База данных учетных записей

В базе данных учетных записей сохраняются учетные данные пользователей и компьютеров и их свойства сетевого доступа. В доменах Windows Server Longhorn роль базы данных учетных записей выполняет Active Directory.

Сервер сертификации работоспособности Health Certificate Server

Сервер сертификации работоспособности представляет собой сочетание службы сертификации работоспособности, компьютера под управлением Windows Server 2008, служб IIS и службы сертификации (CA). Служба сертификации может быть установлена на компьютер под управлением Windows Server 2008 или на отдельный компьютер. Сервер сертификации работоспособности получает сертификаты работоспособности для компьютеров, соответствующих требованиям. Сертификат работоспособности может быть использован вместо заявлений о работоспособности Statements of Health (SoHs), чтобы доказать соответствие клиента требованиям к работоспособности системы.

Сервер исправления

Сервер исправления состоит из серверов, служб и других ресурсов, к которым может получить доступ в ограниченной сети не соответствующий требованиям компьютер. Эти ресурсы могут выполнять разрешение имен или сохранять самые последние обновления ПО и компоненты, необходимые, чтобы привести компьютер в соответствие с требованиями к работоспособности. Например, серверами исправления могут быть дополнительный DNS-сервер, файловый сервер антивирусных продуктов или сервер обновления ПО. SHA может взаимодействовать с сервером исправления напрямую или с помощью средств установленного клиентского ПО.

Сервер политик

SHV взаимодействует с сервером политик для оценки заявления о работоспособности SoH соответствующего агента SHA.

Внедрение системы

Существенным моментом, облегчающим внедрение системы путем поэтапного охвата всего парка рабочих станций организации, является возможность работы NAP в трех режимах.

- наблюдение (мониторинга) – рабочая станция не помещается в карантин, событие помещается в журнал событий;

• отложенное принуждение – рабочая станция не помещается в карантин, событие помещается в журнал событий и пользователь рабочей станции получает периодические сообщения на экране;

• полное принуждение – рабочая станция помещается в карантин. В нашем случае изолированный сегмент ЛВС, из которого возможен доступ только к серверам обновлений антивирусного ПО и системных обновлений Windows (WSUS).

Имеется возможность создавать исключения, например, для рабочих станций, не имеющих в настоящий момент установленного System Health Agent (SHA). Существует возможность поэтапно внедрять механизмы применения защиты.

Необходимо отметить, что NAP не заменяет традиционную инфраструктуру информационной безопасности брандмауэры, приложения по борьбе с вредоносным ПО и системы обнаружения вторжений. Применение NAP позволит нам существенно снизить трудозатраты на контроль над рабочими станциями пользователей и более эффективно бороться с вирусными эпидемиями (вредоносным ПО в целом), что впоследствии уменьшит нагрузку на сеть и увеличит скорость доступа к информации.