Аналитический обзор

Подробное описание функций обеспечения сетевой безопасности, реализованных в платформах маршрутизаторов Cisco ISR второго поколения

В этом аналитическом обзоре представлено подробное описание функций обеспечения безопасности сети, реализованных в маршрутизаторах Cisco® ISR серий 1900, 2900 и 3900.

Средства обеспечения информационной безопасности филиалов нового поколения

Маршрутизаторы Cisco ISR серий 1900, 2900 и 3900 являются основными компонентами набора решений и продуктов Cisco. В них реализованы встроенные средства обеспечения информационной безопасности и организации сетей VPN, которые позволяют организациям выявлять угрозы сетевой безопасности и противодействовать им непосредственно на периметре ИТ-инфраструктуры удаленного филиала в точке подключения к глобальной сети.

В число основных механизмов обеспечения информационной безопасности, позволяющих маршрутизаторам стать критически важными устройствами защиты сети, входят следующие:

- **Организация защищенных подключений.** Эти компоненты обеспечивает создание защищенных масштабируемых сетевых подключений для передачи трафика различных типов, например, IPsec VPN, GET VPN, DMVPN, Enhanced Easy VPN и SSL VPN.
- **Интегрированные средства управления угрозами.** Эти компоненты реагируют на сетевые атаки и угрозы, а также предотвращают их, используя сетевые сервисы, например, межсетевой экран Cisco IOS®, система предотвращения вторжений Cisco IOS, средства фильтрации контента, NetFlow и средства гибкого анализа пакетов FPM.
- **Обеспечение отношений доверия и аутентификация.** Эти средства позволяют сети осуществлять интеллектуальную защиту оконечных устройств с помощью таких технологий, как аутентификация, авторизация и учет (AAA), а также инфраструктура открытых ключей (PKI).
- **Базовые механизмы защиты сетевой инфраструктуры.** Эти компоненты обеспечивают надежную защиту инфраструктуры сети от атак и уязвимостей, особенно на сетевом уровне. Примеры: AutoSecure, политики и защита уровня управления, фильтрация на основе адреса отправителя по технологии RTBH и технология определения маршрута обратной передачи при использовании индивидуальной адресации URPF.

Защищенные подключения

В типовых IP-сетях выполняется бесчисленное количество приложений, как легитимных, так и установленных без согласования с ИТ-подразделением, которые конкурируют за пропускную способность сетевого подключения с приложениями передачи голоса, видео и данных в режиме реального времени. Например, трафик передачи голоса чувствителен к задержкам. Голосовые пакеты, как правило, имеют меньший размер и, если они помещаются в очередь после больших пакетов некритичных данных, то немедленно ощущается снижение качества – слышатся щелчки. Для передачи видео требуется большая пропускная способность, такой трафик чувствителен к колебаниям задержки (джиттеру). Буферирование видеоданных во время задержек часто оказывается неприемлемым, поэтому пакеты обычно отбрасываются для быстрого восстановления устойчивого потока. Если такая потеря пакетов происходит слишком часто, то в результате видеопоток становится прерывистым, и качество изображения существенно снижается.

Для сохранения качества звука и изображения корпоративные приложения передачи голоса и видео требуют сложных механизмов качества обслуживания (QoS) и передачи IP-трафика с использованием групповой адресации. Сети VPN типа «сеть-сеть» и сети VPN удаленного доступа предназначены для транспортировки такого смешанного трафика с использованием повсеместно распространенных и недорогих общедоступных каналов доступа в Интернет с шифрованием, как для основных, так и для резервных соединений. Необходимость повысить качество работы приложений передачи голоса и видео по сетям VPN устанавливает новые требования — интеграция протокола IPsec с функциями QoS или поддержкой групповой адресации IP-пакетов. Использование IP-телефонии [VoIP] и IP-телевидения (IPTV) уже является стандартом де-факто корпоративных ИТ-инфраструктур, а популярность систем Cisco TelePresence™ постоянно растет. По мере распространения этих приложений для видеотелефонии и передачи голосовых данных растут и требования к производительности, масштабируемости и интеграции средств организации VPN и средств обеспечения информационной безопасности.

Маршрутизаторы Cisco ISR серий 1900, 2900 и 3900 обеспечивают создание сетей VPN с высоким уровнем масштабируемости, поддерживающих передачу голоса, видео и данных в реальном времени за счет использования следующих механизмов.

- **Качество обслуживания (QoS).** Использование очередей с малой задержкой (Low-Latency Queuing, LLQ) перед шифрованием является важным требованием для обеспечения высокого качества передачи голоса по сетям VPN. Встроенный процессор поддерживает LLQ, а также средства QoS на уровне интерфейса после шифрования.
- **Групповая адресация IP-пакетов.** Технология Secure Multicast для защищенной передачи трафика с групповой адресацией является основной технологией, сочетающей протокол управления ключами GDOI с протоколом шифрования IPsec для обеспечения эффективной защиты IP-трафика с групповой адресацией. Она позволяет маршрутизатору применять шифрование к нетуннелированным (т. е. «исходным») IP-пакетам с групповой адресацией, что повышает эффективность, поскольку не требуется настраивать отдельные туннели. Благодаря инкапсуляции IP-пакетов с групповой адресацией становится возможной маршрутизация даже зашифрованных пакетов с групповой адресацией (например, при использовании технологии PIM). Использование инкапсуляции исходных IP-пакетов с групповой адресацией позволяет исключить излишнюю репликацию пакетов, которая обычно происходит при использовании туннелей с индивидуальной адресацией. Технология Secure Multicast хорошо подходит для шифрования IP-пакетов, передаваемых по каналам спутниковой связи, шифрования аудиотрафика, защищенной репликации контента в режиме реального времени, для построения сетей DMVPN и т. д.

Стандартная сеть IPsec VPN

Популярность сетей VPN быстро растет, и по мере распространения сетей VPN в динамичной среде филиалов предприятий растут и требования к их производительности и масштабируемости. Как правило, оптимальными платформами для построения таких сетей являются отдельные устройства, которые могут обслуживать как сети VPN удаленного доступа, так и сети VPN типа «сеть-сеть». В таких устройствах реализован целый ряд сервисов безопасности. Маршрутизаторы Cisco ISR серий 1900, 2900 и 3900 поддерживают встроенные средства аппаратного ускорения шифрования IPsec (AES, DES и 3DES), а также процессов VPN.

Эти средства обеспечивают реализацию следующих функций:

- ускорение алгоритмов шифрования DES, 3DES и AES (128, 192 и 256);
- поддержка алгоритмов создания подписей Rivest, Shamir, Aldeman (RSA) и Diffie-Hellman для аутентификации;
- использование алгоритмов хэширования Secure Hash Algorithm 1 (SHA-1) или Message Digest Algorithm 5 (MD5) для обеспечения целостности данных.

Для получения дополнительной информации о реализации стандарта IPsec в ПО Cisco IOS посетите web-сайты по адресам: http://www.cisco.com/go/ipsec
http://www.cisco.com/en/US/docs/ios/sec secure connectivity/configuration/guide/12_4t/sec_ secure_ connectivity_ 12 4t book.html

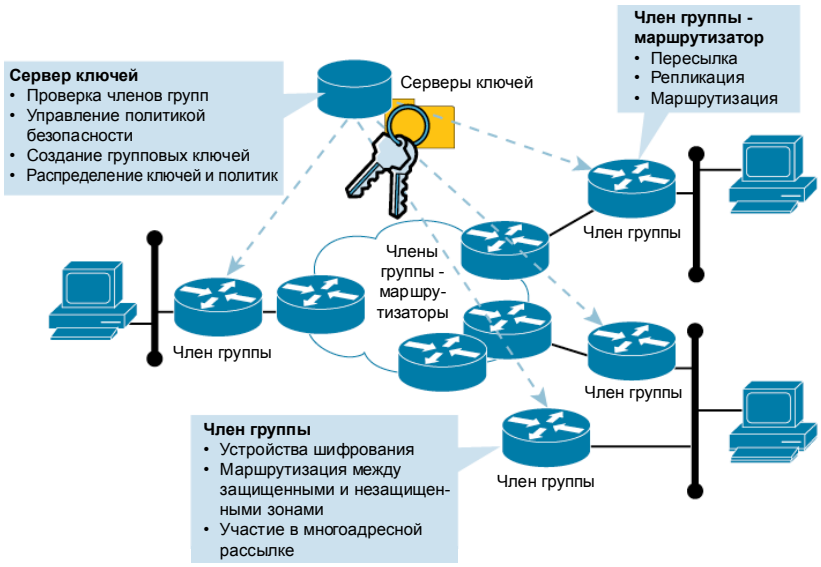
Если организация планирует передавать по каналам связи информацию, требующую защиты в соответствии с российским законодательством, то для этой цели компания Cisco совместно с российской компанией С-Терра СиЭсПи разработала специализированный аппаратный модуль NME-RVPN, который использует отечественные алгоритмы криптографической защиты информации, в частности, ГОСТ 28147-89. При этом криптографическое ядро, использованное в данном модуле, интегрируемом в маршрутизаторы Cisco ISR G2, имеет сертификат Федеральной службы безопасности России (ФСБ). Аналогичные модули были разработаны для выполнения украинских (модуль «Булава» - совместно с НПО «Криптон») и казахских (модуль KazVPN – совместно с компанией ZorSoft) регулятивных требований. В 2010 году модуль NME-RVPN (в варианте исполнения "модуль сетевой модернизированный" или MCM) получил сертификат ФСБ России по классу КС1 (сертификат № СФ/114-1624 от 28 февраля 2011 г.).

Технология Group Encrypted Transport VPN

С представлением технологии GET VPN компания Cisco создала современную масштабируемую категорию сетей VPN, устраняющую необходимость построения туннелей. Технология позволяет осуществлять маршрутизацию трафика с индивидуальной и групповой адресаций непосредственно на удаленные узлы на основании решений протокола маршрутизации и перестраивать маршруты в обход неработоспособных путей, обеспечивая повышение доступности. Она позволяет организациям опираться на существующую маршрутную информацию уровня 3, тем самым давая возможность разрешить проблемы неэффективности репликации при использовании трафика с групповой адресацией и повышая производительность сети. Распределенные сети филиалов могут масштабироваться более эффективно, кроме того, при этом сохраняются интеллектуальные функции сети, критически важные для поддержания качества голоса и видео, например функции QoS, маршрутизации и обработки трафика с групповой адресацией.

Технология GET VPN предлагает новую модель обеспечения безопасности с использованием стандартизованного протокола IPsec, которая опирается на концепцию «доверенных» участников групп. Маршрутизаторы, являющиеся доверенными участниками групп, используют общую методику обеспечения безопасности, независимую от каких-либо взаимосвязей «точка-точка» на основе туннелей IPsec. Сервер ключей распределяет ключи и политики на все зарегистрированные и аутентифицированные маршрутизаторы-участники групп (см. рис. 1).

Рисунок 1. Функции обеспечения безопасности групп



Технология GET VPN предоставляет преимущества для множества приложений. В частности, технология GET VPN:

- осуществляет защиту данных и аутентификацию на транспортном уровне, обеспечивая соответствие нормам по обеспечению безопасности и внутренним нормативным актам путем шифрования всего трафика, передаваемого по глобальной сети;
- позволяет организовать широкомасштабные полносвязные сети и исключает необходимость сложного управления ключами для одноранговых соединений за счет использования групповых ключей шифрования;
- для MPLS-сетей поддерживает интеллектуальные функции сети, в частности, полносвязную топологию, естественные пути маршрутизации и функцию QoS;
- поддерживает простое управление участием в сети с помощью централизованного сервера ключей;
- позволяет обеспечить низкую величину задержки и малые колебания задержки за счет поддержания постоянных соединений между узлами, не требуя транспорта через центральный узел-концентратор;
- снижает нагрузку трафика на оборудование, установленное у заказчика, и на устройства шифрования на уровне периметра сетей операторов связи за счет использования ядра сети для репликации трафика с групповой адресацией и исключения репликации пакетов на каждом отдельном узле.

Для получения дополнительных сведений о технологии Cisco GET VPN посетите web-сайты по адресам:

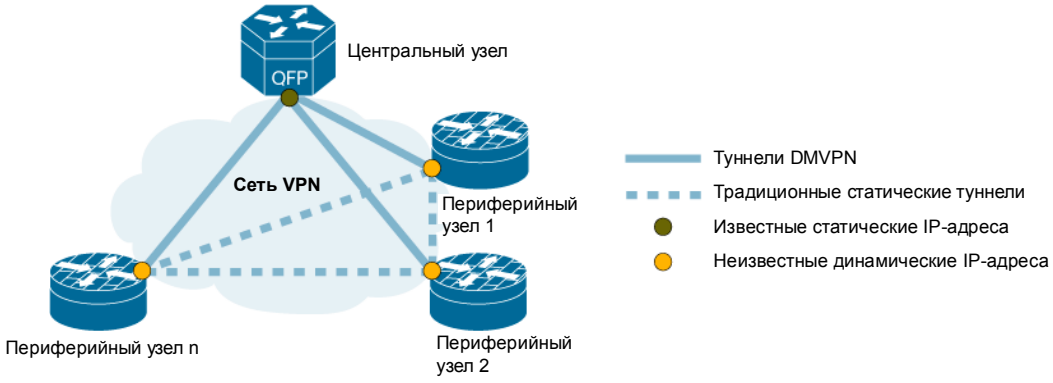
http://www.cisco.com/go/getvpn

http://www.cisco.com/en/US/docs/ios/sec secure connectivity/configuration/guide/sec encrypt trns vpn.html

Технология DMVPN

Маршрутизаторы Cisco поддерживают функции организации сети сети DMVPN. Реализация DMVPN в продукции Cisco позволяет организовать масштабируемую полносвязную сеть VPN «по запросу» для снижения задержки, экономии пропускной способности и упрощения развертывания сетей VPN (см. рис. 2). В основе технологии DMVPN лежит опыт компании Cisco в области использования протокола IPsec и протоколов маршрутизации, что позволяет выполнять динамическую настройку туннелей GRE, шифрования IPsec, протоколов NHRP, OSPF и EIGRP.

Рисунок 2. Сеть DMVPN



Реальная мощь технологии DMVPN проявляется в центральном офисе компании, где динамическая настройка VPN-туннелей в сочетании с технологиями QoS и поддержкой групповой IP-адресации позволяет оптимизировать производительность чувствительных к задержкам приложений при одновременном уменьшении сложности администрирования. Например, технология DMVPN позволяет получить одинаковую производительность для приложений

передачи голоса и видео по транспортной IP-сети и по альтернативному каналу глобальной сети при сохранении безопасности и эффективности.

Технология DMVPN широко использовалась для поддержки комбинации соединений с филиалами компании, удаленными работниками и внешними сетями. В число основных преимуществ входят следующие:

- обеспечение полносвязности сети при простой звездообразной конфигурации;
- автоматический запуск протокола IPsec для построения туннеля IPsec;
- поддержка автоматизированной настройки при добавлении новых периферийных сетей;
- поддержка динамически адресуемых периферийных сетей.

Для получения дополнительной информации о функции Cisco DMVPN посетите web-сайты по адресам:

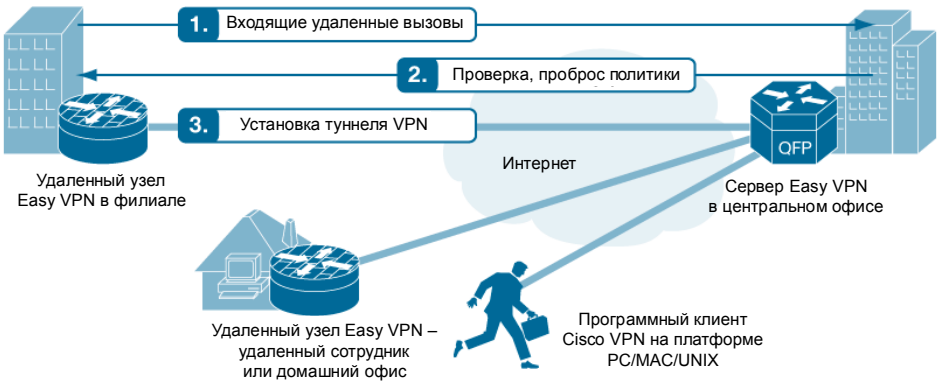
http://www.cisco.com/go/dmvpn

http://www.cisco.com/en/US/docs/ios/sec secure connectivity/configuration/guide/sec DMVPN.html

Easy VPN и Enhanced Easy VPN

Для удовлетворения требований к простоте организации удаленного доступа с высокой степенью масштабируемости Cisco предлагает решение Easy VPN, в котором используется технология «проброса политики», позволяющая упростить настройку при сохранении богатых функциональных возможностей и управления политикой. Сервер Easy VPN, определенный центральным офисом, внедряет политику безопасности на удаленных устройствах сети VPN, обеспечивая использование актуальных политик подключения перед тем, как само подключение будет установлено (см. рис. 3).

Рисунок 3. Установка туннеля Easy VPN.



Решение Easy VPN предоставляет следующие преимущества.

- Easy VPN поддерживает как оконечное пользовательское оборудование (маршрутизаторы доступа), так и программные клиенты удаленного доступа с использованием одного и того же маршрутизатора на центральном узле. Возможна установка программного обеспечения Cisco VPN Client на ПК, компьютеры Mac и системы под управлением ОС UNIX, что позволяет расширить возможности создания VPN-подключений для удаленного доступа на основе маршрутизатора без дополнительных затрат. Поскольку как для аппаратных клиентов (оконечного пользовательского оборудования), так и для программных клиентов используется единая технология (Easy VPN), совокупная стоимость владения снижается за счет упрощения и унификации подготовки, мониторинга и сервисов AAA.

- Easy VPN позволяет организовать как локальную аутентификацию (на основе маршрутизатора), так и централизованную аутентификацию на основе RADIUS и AAA как для маршрутизаторов, устанавливаемых у заказчика, так и для отдельных пользователей.
- Easy VPN поддерживает цифровые сертификаты, повышая безопасность по сравнению с использованием предварительно распространенных ключей.
- Технология обеспечивает распределение нагрузки для нескольких концентраторов Easy VPN на центральном узле. Проброс политики с информацией о резервном VPN-концентраторе на оборудование, устанавливаемое у заказчика, позволяет масштабировать решение без перенастройки этого оборудования.
- Технология поддерживает виртуализацию сервера Easy VPN, позволяя операторам связи предлагать сервисы сетей VPN множеству заказчиков с использованием единой платформы.
- Easy VPN предлагает полнофункциональную интеграцию, включая динамическое назначение политики QoS, межсетевой экран и систему предотвращения вторжений, поддержку раздельного туннелирования, соглашения об уровне обслуживания Cisco IP SLA и функцию NetFlow для мониторинга производительности.
- Программное средство Cisco Configuration Professional предоставляет возможность быстрого развертывания Easy VPN с помощью мастера, интеграцию этой технологии с функциями AAA и межсетевого экрана, а также мониторинг удаленных клиентов Easy VPN в режиме реального времени.
- Технология Easy VPN поддерживается во всех линейках продуктов Cisco, поддерживающих организацию сетей VPN, как работающих под управлением операционной системы Cisco IOS, так и устройств на платформе Cisco ASA.

В случае интеграции функций Enhanced Easy VPN с интерфейсами VTI имеется возможность настроить виртуальные интерфейсы непосредственно с Easy VPN, что обеспечит простоту развертывания и расширенную сетевую интеграцию. В числе преимуществ решения:

- значительное упрощение требований к процедуре настройки как в головном офисе, так и в удаленных филиалах;
- IP-сервисы можно настраивать с помощью интерфейсов VTI (или загружать настройки с серверов AAA). При установке соединения экземпляры VTI динамически клонируются на основе этих шаблонов. Отсутствует необходимость вручную создавать множество аналогичных наборов команд настройки для каждого удаленного узла.
- предлагая атрибуты для каждого отдельного пользователя, в частности, настройки QoS, VTI дает возможность легко выполнять настройку политик для каждого отдельного пользователя. Это позволяет администраторам в упреждающем режиме обеспечивать требуемую производительность приложений и поддерживать продуктивность и мотивацию пользователей;
- интерфейс VTI позволяет выполнять настройку VPN-туннелей с собственным набором параметров для каждого филиала, обеспечивая гибкость настройки и безопасность в соответствии с требованиями каждого конкретного объекта.

Для получения дополнительной информации о технологии Cisco Easy VPN посетите web-сайты по адресам:

http://www.cisco.com/go/easyvpn

http://www.cisco.com/en/US/docs/ios/sec secure connectivity/configuration/guide/sec easy vpn rem.html

http://www.cisco.com/en/US/docs/ios/sec secure connectivity/configuration/guide/sec easy vpn srvr.html

Поддержка SSL VPN в операционной системе Cisco IOS

Cisco IOS SSL VPN — это решение на основе маршрутизатора, обеспечивающее возможность создания подключений удаленного доступа SSL VPN в сочетании с лидирующими в отрасли функциями обеспечения безопасности и маршрутизации в рамках конвергентной платформы для передачи данных и голоса, а также построения беспроводных сетей. С помощью SSL VPN организации могут безопасно и прозрачно расширять свои корпоративные сети до любой точки подключения к Интернету. Реализация SSL VPN в операционной системе Cisco IOS поддерживает доступ к различным приложениям без использования клиента, включая интранет-контент на основе HTML, системы работы с электронной почтой, общие сетевые файловые ресурсы и Citrix. В то же время разработанный Cisco SSL VPN-клиент обеспечивает полный удаленный доступ к сети для практически любого приложения. Являясь частью решения Cisco IOS SSL VPN, приложение Cisco Secure Desktop обеспечивает защиту данных от кражи даже на устройствах, расположенных вне офиса организации. Cisco Configuration Professional упрощает развертывание решения Cisco IOS SSL VPN и осуществляет мониторинг и управление сеансами SSL VPN в режиме реального времени.

Для получения дополнительной информации о решении Cisco IOS SSL VPN посетите web-сайты по адресам:

http://www.cisco.com/go/iossslvpn

http://www.cisco.com/en/US/docs/ios/sec secure connectivity/configuration/guide/sec ssl vpn.html

Интерфейсы VTI

Сети VPN стали стандартом де-факто для организации защищенных подключений через глобальные сети. Они приходят на смену существующим и широко распространенным частным сетям, в которых используются выделенные линии, технологии Frame Relay или ATM, и обеспечивают соединение удаленных офисов и филиалов с центральными офисами более экономично и с повышенной гибкостью. Новый статус типового решения требует от устройств, на которых реализованы сети VPN, более высокой производительности, поддержки интерфейсов как локальных, так и глобальных сетей, а также высокой доступности сети.

Для настройки сетей IPsec VPN для связи между объектами можно использовать инструментальное средство Cisco IPsec VTI. Эта утилита позволяет создать маршрутизируемый интерфейс для оконечных точек туннелей IPsec, тем самым упрощая настройку. Туннели Cisco IPsec VTI поддерживают назначенные маршруты в глобальной сети общего пользования и инкапсулируют трафик с использованием новых заголовков пакетов, чтобы обеспечить доставку указанным получателям. Сеть является частной, поскольку трафик может поступить в туннель только с соответствующего оконечного устройства. Кроме того, протокол IPsec надежно обеспечивает конфиденциальность передаваемых данных (с помощью средств шифрования).

Используя Cisco IPsec VTI, предприятие может реализовать все возможности экономичных сетей VPN и добавить передачу голоса и видео к функциям имеющейся сети передачи данных без ущерба для качества и надежности. Технология обеспечивает коммуникации с высокой степенью защиты для сетей VPN типа «сеть-сеть», таким образом, обеспечивается защищенная передача голоса, видео и данных по IP-сетям общего пользования.

Для получения дополнительных сведений о Cisco IPsec VTI посетите web-сайт по адресу:

http://www.cisco.com/en/US/docs/ios/sec secure connectivity/configuration/guide/sec ipsec virt tunnl.html

Технология Multi-Virtual Route Forwarding (VRF) Customer Edge и контексты безопасности MPLS

Технология Multi-VRF CE (также называемая VRF-Lite) обеспечивает возможность настройки и поддержки нескольких экземпляров таблиц маршрутизации и пересылки трафика в рамках одного физического маршрутизатора. В сочетании с технологиями VLAN (Ethernet) и VPN (WAN), такими как Frame Relay, эта технология помогает предоставлять несколько логических сервисов с помощью одной физической сети, расширяя тем самым функции обеспечения конфиденциальности и безопасности до периметра сети клиента.

Один маршрутизатор Cisco с поддержкой технологией Multi-VRF CE может поддерживать несколько компаний с перекрывающимися пространствами IP-адресов, сохраняя при этом разделение данных, маршрутов и физических интерфейсов.

Для получения дополнительной информации о технологии Multi-VRF CE посетите web-сайт по адресу:

http://www.cisco.com/en/US/products/hw/routers/ps259/prod_bulletin09186a00800921d7.html.

Высокая надежность IPsec

Сети VPN, организованные с помощью маршрутизаторов Cisco, поддерживают широкий спектр механизмов резервирования и распределения нагрузки. Для небольших развертываний IPsec подойдут протоколы HSRP и RRI, обеспечивающие резервирование. Для обеспечения избыточности и распределения нагрузки в более крупных развертываниях можно использовать механизм распределения нагрузки Cisco SLB.

- **Аварийное переключение подключений IPsec с сохранением состояния.** Аварийное переключение подключений IPsec с сохранением состояния позволяет использовать резервный сервер IPsec для продолжения обработки и пересылки пакетов IPsec после планового или непредвиденного прерывания работы. Если активный маршрутизатор по какой-либо причине теряет соединение, резервный (дополнительный) IPsec-сервер автоматически принимает на себя выполнение задач активного (основного) маршрутизатора без потери защищенных соединений с соответствующими узлами. Эта процедура незаметна для конечного пользователя и не требует корректировок или перенастройки какого-либо удаленного узла. Механизм аварийного переключения подключений IPsec с сохранением состояния разработан для совместного использования с функцией аварийного переключения с сохранением состояния (SSO) и протоколом HSRP. HSRP обеспечивает резервирование оборудования IP-сетей, способствуя немедленному и прозрачному восстановлению трафика пользователей в случае сбоя устройств на периметре сети или нарушения работоспособности линий доступа. Аварийное переключение подключений IPsec с сохранением состояния используется для защиты туннелей IPsec, IPsec с поддержкой GRE и трафика Cisco IOS Easy VPN.
- **HSRP и RRI.** Протокол RRI поддерживает как динамические, так и статические криптографические сопоставления (crypto map) для упрощения сетевой структуры VPN, требующих либо высокой надежности, либо распределения нагрузки. Для динамического распространения маршрутной информации на головном устройстве создаются маршруты для каждой удаленной сети или узла. Протоколы HSRP и IPsec динамически перенаправляют трафик, обеспечивая максимальную доступность сервисов. Если при отказе основного маршрутизатора некоторым узлам не удается переключиться на резервное устройство, HSRP обеспечивает для них постоянный сетевой доступ. В этом случае для предоставления возможности аварийного переключения подключений IPsec с сохранением состояния виртуальный IP-адрес HSRP используется в качестве конечной точки туннеля VPN.
- **Распределение нагрузки (SLB).** Можно определить виртуальные серверы, которые будут представлять группу физических серверов в кластере сетевых серверов (ферме серверов). Когда клиент инициирует подключение к виртуальному серверу, ПО Cisco IOS выбирает физический сервер для подключения с учетом настроенного

алгоритма распределения нагрузки. В случае отказа физического сервера SLB динамически перенаправляет все новые входящие сессии IPsec на другой сервер, обеспечивая таким образом избыточность.

Для получения дополнительной информации об обеспечении высокой надежности IPsec посетите web-сайт по адресу:

http://www.cisco.com/en/US/docs/ios/sec_secure_connectivity/configuration/guide/sec_vpn_ha_enhance.html

Интегрированное управление угрозами

Средства интегрированного управления угрозами Cisco обеспечивают комплексную защиту сети с помощью механизмов упрощенного управления политиками и упреждающей защиты системы. В число средств обеспечения безопасности входят такие компоненты, как межсетевой экран Cisco IOS, система предотвращения вторжений Cisco IOS IPS, средства фильтрации контента Cisco IOS, NetFlow, средства распознавания сетевых приложений (NBAR) и гибкого анализа пакетов (FPM). Их совместное использование позволяет решать следующие задачи:

- защита сети, серверов, оконечных устройств и информации;
- управление доступом в сеть, изоляция инфицированных систем, предотвращение вторжений, защита критически важных активов бизнеса;
- блокировка вредоносного трафика (червей, вирусов, вредоносного ПО) до его распространения в системе.

Межсетевой экран Cisco IOS

Межсетевой экран Cisco IOS представляет собой программный межсетевой экран с учетом состояния соединений, благодаря которому маршрутизаторы Cisco ISR серий 1900, 2900 и 3900 становятся идеальным решением для маршрутизации и обеспечения безопасности, реализованным в рамках одного устройства и обеспечивающим полную защиту точки подключения к глобальной сети.

В качестве основных возможностей межсетевого экрана Cisco IOS можно выделить следующие.

- **Политики на основе зон.** Межсетевой экран на основе зон позволяет группировать физические и виртуальные интерфейсы в зоны, что упрощает логическую топологию сети. Создание этих зон способствует внедрению политик межсетевого экрана на основе зон и исключает необходимость настройки политик отдельно на каждом интерфейсе. Пакеты не пересылаются, если для каждого направления между парой зон не указаны в явном виде политики пары зон. Политика описывается с помощью языка Cisco Policy Language (т. е. интерфейса командной строки Modular QoS CLI, MQC) и устанавливает тип динамической проверки и параметры сеанса, применяемые для каждой пары зон. Например, на границе между Интернетом и демилитаризованной зоной (DMZ) требуется явное указание политики, разрешающей передачу пакетов HTTP и DNS через границу между зонами.
- **Расширенный анализ и контроль приложений (AIC).** Этот компонент использует средства анализа сетевого трафика для обеспечения соответствия протоколам и предотвращения злонамеренных или несанкционированных действий, например туннелирования порта 80 или ненадлежащего использования подключений для работы с электронной почтой (протоколы SMTP, ESMTP, POP3 и IMAP).
- **Межсетевой экран для защищенных унифицированных коммуникаций.** Межсетевой экран Cisco IOS поддерживает передачу голосового трафика, включая протоколы сигнализации и связанные открытые каналы. Он также поддерживает протоколы передачи голосовых данных, такие как H.323 версий 2, 3 и 4, SCCP и SIP, а также защищает такие компоненты системы унифицированных коммуникаций, как IP-АТС Cisco Unified Communications Manager, унифицированный элемент периметра Cisco CUBE и соответствующие оконечные устройства.

- **Межсетевой экран с поддержкой VRF.** Межсетевой экран включен в список сервисов, доступных на уровне отдельного контекста, при использовании VRF.
- **Высокая надежность межсетевого экрана.** Аварийное переключение межсетевого экрана с сохранением состояния упрощает процесс аварийного переключения в конфигурации «активный-резервный» по протоколу HSRP между двумя устройствами без нарушения активных сеансов.
- **Прозрачный межсетевой экран.** Эта функция обеспечивает сегментацию на уровне 2 для легкого внедрения межсетевого экрана в существующие сети без смены адресации на уровне IP-подсетей.
- **Межсетевой экран IPv6.** Средства поддержки IPv6 обеспечивают функционирование межсетевого экрана Cisco IOS в смешанных средах IPv6 и IPv4.
- **Детализированные политики безопасности.** Этот компонент поддерживает задание политик обеспечения безопасности для каждого отдельного пользователя, интерфейса или субинтерфейса.
- **Интегрированные сервисы проверки подлинности.** Интегрированные сервисы проверки подлинности обеспечивают аутентификацию и авторизацию для каждого отдельного пользователя.
- **Управление межсетевым экраном на основе политик.** Cisco Security Manager и Cisco Configuration Professional предоставляют интуитивно понятные способы для управления межсетевым экраном Cisco IOS на основе политик.

Для получения дополнительной информации о межсетевом экране Cisco IOS посетите web-сайты по адресам:

http://www.cisco.com/go/iosfw

http://www.cisco.com/en/US/docs/ios/sec data plane/configuration/guide/12_4t/sec_data_plane_12_4t_book.html

Система предотвращения вторжений Cisco IOS

В некоторых маршрутизаторах Cisco реализованы функции системы IPS. Cisco IOS IPS является встроенным решением для глубокого анализа сетевого трафика, которое помогает ПО Cisco IOS эффективно нейтрализовывать сетевые атаки. Cisco IOS IPS использует технологии сканирования пакетов с учетом состояния соединения, а также сигнатуры атак и уязвимостей, также поддерживаемые различными автономными устройствами и встраиваемыми модулями Cisco IPS.

Благодаря решению IPS, интегрированному в существующие маршрутизаторы для построения уровня доступа, появилась возможность развертывания дополнительных рубежей защиты на уровне периметра сети с минимальными затратами.

К основным возможностям системы предотвращения вторжений Cisco IOS относятся следующие.

- **Функционирование в режиме транзитной передачи данных.** Не ограничиваясь одним обнаружением, эта функция позволяет маршрутизатору немедленно реагировать на угрозы безопасности и защищать сеть. Маршрутизаторы могут удалять пакеты, отправлять оповещения, игнорировать соединения, а также при необходимости локально разрывать соединения, чтобы максимально быстро прекратить передачу вредоносного трафика в сеть. Эти действия можно настроить для каждой сигнатуры.
- **Обработчик реакций на события сигнатур (SEAP).** Уникальный обработчик реакции на события сигнатур на основе оценки рисков обеспечивает более точный и эффективный мониторинг событий IPS путем фильтрации или разделения событий с низким или высоким уровнем риска, существенно упрощая управление политиками IPS.
- **Готовые файлы сигнатур.** Эта функция позволяет пользователям, которым требуется максимальная защита от вторжений, выбирать простой в использовании файл сигнатур, содержащий сигнатуры наиболее распространенных сетевых червей и атак. Трафик, сопоставляющий эти сигнатуры червей и атак с высоким уровнем достоверности, настроен на отбрасывание. Cisco Configuration Professional располагает интуитивно понятным пользовательским

интерфейсов для предоставления этих сигнатур, включая возможность загрузки новых сигнатур с сайта Cisco.com без изменения образа программного обеспечения, и соответствующим образом настраивает маршрутизатор.

- **Настраиваемые сигнатуры.** С помощью этой функции можно изменить существующую сигнатуру или создать новую, которая будет применяться для устранения недавно обнаруженных угроз (каждая сигнатура может активироваться отдельно).
- **Прозрачная IPS.** Этот компонент реализует IPS уровня 3 для подключения уровня 2, позволяя без труда внедрять систему IPS в существующие сети без смены адресации на уровне IP-подсетей.
- **IPS с поддержкой VRF.** Система IPS включена в список сервисов, доступных на уровне отдельного контекста, при использовании VRF.
- **Большая база данных сигнатур.** Количество сигнатур постоянно увеличивается. На данный момент платформа сенсоров Cisco IPS поддерживает более 1200 сигнатур.
- **Согласованное управление.** Загрузка и активация выбранных сигнатур IPS выполняется так же, как на сенсорах Cisco IDS, выполненных в формате автономного устройства.

Для получения дополнительной информации о Cisco IOS IPS посетите web-сайт по адресу:

http://www.cisco.com/go/iosips

Средства фильтрации контента Cisco IOS

Средства фильтрации контента Cisco IOS используются для защиты организаций от известных и новых угроз из сети Интернет, повышения производительности сотрудников и соблюдения бизнес-политик для обеспечения соответствия нормативным требованиям. Эти средства отслеживают и регулируют все действия в Интернете и блокируют или ограничивают доступ к определенным web-сайтам, обеспечивают защиту от вредоносных сайтов, с которых распространяются вредоносные программы, рекламные программы и фишинг-атаки, а также помогают организации более эффективно управлять сетевыми ресурсами благодаря простоте развертывания.

Основные возможности средств фильтрации контента Cisco IOS:

- **Услуги на основе подписки.** Легко продлеваемая услуга по подписке на 1, 2 или 3 года связана с платформой маршрутизации. Отдельные пользовательские лицензии не требуются. За счет политик фильтрации, заданных на маршрутизаторе, эта подписка предоставляет доступ к базе данных Trend Micro.
- **Рейтинги безопасности.** Средства фильтрации контента Cisco IOS используются для защиты от различных web-угроз, включая совершенно новые атаки. Они оценивают риск безопасности, связанный с web-сайтом, на основе данных анализа лабораторий TrendLabs компании Trend Micro, помогают бороться с фишингом и обеспечивает защиту от шпионских программ, которые могут отправлять конфиденциальную информацию хакерам и компьютерным преступникам. При оценке безопасности конкретного URL-адреса TrendLabs принимает во внимание как поведение в прошлом, так и текущую предрасположенность к воздействию вредоносных, рекламных, шпионских программ, фишингу и действиям злоумышленников.
- **Классификация URL-адресов на основе категорий.** Классификация URL-адресов на основе контента полезна при ограничении доступа к нежелательным или негативно влияющим на производительность web-сайтам (например, сайты, связанные с азартными играми или оружием). Доступно более 70 категорий, включая блокировку на основе репутации (например, шпионские программы или клавиатурные шпионские программы).
- **Блокировка по ключевым словам.** Средства фильтрации контента Cisco IOS позволяют блокировать web-сайты на основании выбранных ключевых слов, отображаемых при переходе по URL-адресу.

- **Поддержка «черных» и «белых» списков.** Средства фильтрации контента Cisco IOS поддерживают 100 «черных» и 1000 «белых» URL-адресов. Например, доверенные web-сайты можно добавить в «белый» список.
- **Подготовка управления.** Средства фильтрации контента Cisco IOS просты в развертывании и использовании. Для управления ими служит утилита Cisco Configuration Professional.
- **Кэширование.** Функция кэширования сохраняет категории URL-адресов и принятые решения относительно политики (разрешить или запретить) локально на маршрутизаторе, что позволяет ускорить принятие решений о доступе в Интернет. Администраторы могут настроить в маршрутизаторе время хранения данных в кэше.

Для получения дополнительной информации о средствах фильтрации контента Cisco IOS посетите web-сайт по адресу:

http://www.cisco.com/go/ioscontentfiltering

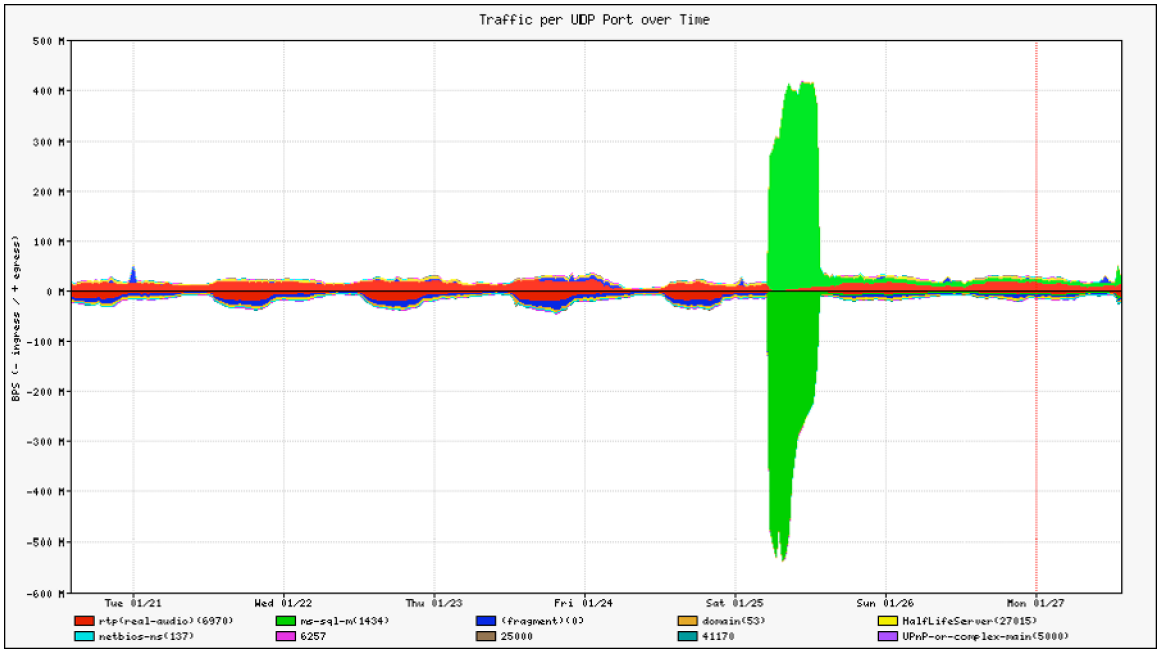
NetFlow

NetFlow является основной используемой в отрасли технологией выявления аномалий в сетях. Эта технология предоставляет данные телеметрии для анализа IP-трафика, например, она позволяет определить, между какими узлами поддерживается соединение, через какие протоколы и порты, в течение какого времени и на какой скорости.

DDoS-атаки создают внезапные всплески загрузки сети. Эти атаки могут быть быстро идентифицированы как аномальные сетевые события при сравнении с типовыми шаблонами трафика, извлеченными из ранее собранных профилей и базовых показателей.

Путем анализа подробных данных трафика NetFlow можно также классифицировать атаку (т. е. определить источник и цель атаки), установить ее продолжительность и размер используемых в ней пакетов. К средствам анализа относятся продукты партнеров Cisco по обеспечению безопасности (см. рис. 4).

Рисунок 4. Пример обнаружения DDoS-атак на основе аномалий с использованием NetFlow и решений Arbor Networks



Для получения дополнительной информации о Cisco IOS NetFlow посетите web-сайт по адресу: http://www.cisco.com/go/netflow.

Технология распознавания сетевых приложений (NBAR)

Технология NBAR представляет собой метод классификации трафика, реализованный в состав операционной системы Cisco IOS, который обеспечивает гибкий анализ пакетов с учетом состояния соединения для распознавания широкого круга приложений, включая протоколы, туннелируемые по HTTP, и другие трудно классифицируемые протоколы с динамическим назначением портов TCP и UDP. При использовании для обеспечения безопасности средства NBAR способны обнаруживать интернет-червей на основе сигнатур, описывающих передаваемые данные. Когда средства NBAR распознают и классифицирует приложение, сеть может предоставлять этому конкретному приложению соответствующие сервисы. Технология также способствует эффективному использованию пропускной способности сети за счет взаимодействия с функциями QoS, чтобы предоставлять гарантированную пропускную способность, определять пределы пропускной способности, осуществлять профилирование трафика и добавлять метки в пакеты.

В состав Cisco Configuration Professional входит простой в использовании мастер для включения NBAR. Кроме того, это средство обеспечивает графическое представление сведений о трафике приложений.

Для получения дополнительной информации о Cisco NBAR посетите web-сайт по адресу: http://www.cisco.com/go/nbar.

Гибкий анализ пакетов (FPM)

Средства гибкого анализа пакетов (Flexible Packet Matching, FPM) проверяют пакеты для выявления признаков атаки и предпринимают соответствующие действия (регистрация в журнале, отбрасывание или сообщение протокола ICMP о недоступности). Они предоставляют гибкий механизм классификации без учета состояния соединений для анализа трафика на уровнях 2-7. Имеется возможность указать критерии классификации на основе любого протокола и любого поля в стеке протоколов. На основании результатов классификации можно предпринять действия в отношении классифицированного трафика, например отбрасывание или регистрацию факта в журнале.

Для получения дополнительной информации о средствах FPM посетите web-сайты по адресам:

http://www.cisco.com/go/fpm

http://www.cisco.com/en/US/docs/ios/sec data plane/configuration/guide/sec_flex_pack_match.html

Формирование доверенной среды и аутентификация

Клиент PKI (цифровые сертификаты x.509)

Инфраструктура открытых ключей (PKI) предоставляет клиентам масштабируемый и надежный механизм для распространения, управления и отзыва информации о шифровании и проверке подлинности в защищенной сети. Операционная система Cisco IOS поддерживает функции клиента PKI, взаимодействующего с сервером сертификатов Cisco IOS и сторонними удостоверяющими центрами.

Маршрутизатор создает пару RSA-ключей (один закрытый и один открытый ключ), которая его идентифицирует. Сервер удостоверяющего центра (УЦ) подтверждает подлинность маршрутизатора и генерирует цифровой сертификат, предоставляя доступ к инфраструктуре PKI. С помощью информации в сертификате каждый маршрутизатор, включенный в инфраструктуру PKI, может проверить подлинность другого устройства и установить зашифрованное подключение с использованием открытых ключей, находящихся в сертификате.

Клиент PKI поддерживает следующие функциональные возможности.

- **Серверы сертификатов.** Поддержка внешних (например, VeriSign) или внутренних (например, Microsoft) серверов сертификатов. В небольших развертываниях можно использовать сервер сертификатов ОС Cisco IOS.

- **Аутентификация и регистрация сертификатов.** Поддержка работы с сертификатами с использованием протоколов SCEP, TFTP и выполнения необходимых действий вручную.
- **Автоматическая регистрация и обновление.** Маршрутизаторы могут автоматически запрашивать цифровые сертификаты и продлевать их до истечения срока действия. Пролонгация сертификата обеспечивает беспрепятственный переход при обновлении сертификата ЦС.
- **Защищенная настройка устройств.** Обеспечение безопасного развертывания маршрутизаторов с конфигурацией по умолчанию с использованием PKI и IPsec VPN без утомительных действий по настройке. Идеальный вариант для удаленных офисов или надомных работников.
- **Интеграция PKI – AAA.** Маршрутизатор может использовать сервер AAA внутренней системы для выполнения авторизации. Предоставление детализированного контроля на основе полей сертификатов.
- **Управление доступом на основе сертификатов.** Предоставление функции, аналогичной интеграции PKI – AAA, кроме использования списков ACL для принятия или отклонения сертификатов на основе полей сертификатов.
- **Управление HTTPS и средствами SSL VPN.** Поддержка постоянных самоподписанных сертификатов.
- **Проверка отзыва сертификата.** Поддержка списков отзыва сертификатов (CRL) и протокола OCSP.
- **Многоуровневая иерархия УЦ.** Возможность работы маршрутизатора с точками доверия УЦ на нескольких уровнях. Используется для настройки маршрутизаторов филиалов на взаимодействие с УЦ подразделений или с другими подчиненными серверами сертификатов.
- **Хранилище учетных данных PKI (RSA- ключей).** Защита закрытого ключа в NVRAM с возможностью шифрования ключей. Поддержка USB-токенов.
- **Дополнительные поддерживаемые функции PKI:** стирание ключа RSA в случае попытки пользователя восстановить пароль; несколько пар ключей; импорт пар ключей и сертификатов в формате PEM; открытые и закрытые ключи длиной 4096 бит.

Для получения дополнительной информации о клиенте PKI, реализованном в ОС Cisco IOS, посетите web-сайты по адресам:

http://www.cisco.com/en/US/products/ps6664/products_ios_protocol_option_home.html

http://www.cisco.com/en/US/docs/ios/sec secure connectivity/configuration/guide/sec_pki_feat_rmap_ps6441_TSD_Products_Configuration_Guide_Chapter.html

http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6660/prod_white_paper0900aecd8046cbc4.html

http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6660/ps6807/prod_white_paper0900aecd805_249e3_ns855_Networking_Solutions_White_Paper.html

Сервер сертификатов операционной системы Cisco IOS

Сервер сертификатов операционной системы Cisco IOS обеспечивает поддержку сервера сертификатов в ОС Cisco IOS, благодаря чему маршрутизатор начинает выполнять функции удостоверяющего центра в сети.

Увеличение количества сетей VPN, как правило, было связано с трудностями при создании ключевых данных и управлении ими. Эти проблемы решает простой, масштабируемый, легкий в управлении удостоверяющий центр, встроенный в оборудование с поддержкой IPsec VPN. Сервер сертификатов ОС Cisco IOS является значимой альтернативой простым вариантам симметричного развертывания ключей.

Поддерживаются следующие функциональные возможности:

- Протокол SCEP
- Формирование пары RSA-ключей
- Хранилище файлов базы данных
- Автоматическая архивация ключа и сертификата УЦ
- Автоматическое продление ключа и сертификата УЦ в случае истечения срока действия сертификата
- Списки отзыва сертификатов (CRL)
- Режимы подчиненного центра и центра регистрации

Для получения дополнительной информации о сервере сертификатов ОС Cisco IOS посетите web-сайты по адресам:

http://www.cisco.com/en/US/products/ps6664/products_ios_protocol_option_home.html

http://www.cisco.com/en/US/docs/ios/security/configuration/guide/sec_cfg_mng_cert_serv_external_docbase_0900e_4b1805afd65_4container_external_docbase_0900e4b1807b4277.html

Сервисы аутентификации на основе стандарта 802.1x

Приложения стандарта 802.1x усложняют несанкционированный доступ к защищенным информационным ресурсам за счет необходимости предоставления допустимых учетных данных. Внедряя инфраструктуру 802.1x, сетевые администраторы могут не допускать ситуаций, когда пользователи развертывают незащищенные точки доступа к беспроводной сети, и устранять тем самым одну из самых больших проблем, связанных с простым в использовании оборудованием для глобальных сетей.

Для получения дополнительной информации о стандарте 802.1 посетите web-сайты по адресам:

http://www.cisco.com/en/US/products/ps6662/products_ios_protocol_option_home.html

http://www.cisco.com/en/US/docs/ios/sec user services/configuration/guide/sec_cfg_ieee802_pba.html

http://www.cisco.com/en/US/docs/ios/sec user services/configuration/guide/sec_ieee loc_auth_sv.html

http://www.cisco.com/en/US/docs/ios/sec user services/configuration/guide/sec_vpn_ac_802_1x.html

AAA

Сервисы обеспечения сетевой безопасности AAA, реализованные в ОС Cisco IOS, являются основой системы управления доступом на маршрутизаторе или сервере доступа. Механизм AAA позволяет администраторам динамически настраивать требуемый тип аутентификации и авторизации отдельно для каждой линии (каждого пользователя) или для каждого сервиса (например, протоколов IP, IPX или сети VPDN), используя списки методов, применяемых для конкретных сервисов или интерфейсов.

Для получения дополнительной информации о сервисах AAA ОС Cisco IOS посетите web-сайты по адресам:

http://www.cisco.com/en/US/products/ps6663/products_ios_protocol_option_home.html

http://www.cisco.com/en/US/docs/ios/sec user services/configuration/guide/12 4T/sec_securing_user_services_12._4t_book.html

Базовые механизмы защиты сетевой инфраструктуры Cisco IOS

Постоянная доступность устройств сетевой инфраструктуры особенно важна в центральном офисе компании. Если безопасность сетевого маршрутизатора или коммутатора нарушена, злоумышленники получают полный доступ ко всей сети. Независимо от различных эффективных систем защиты, которые можно использовать против атак, необходимо также предусмотреть защиту от неизвестных угроз.

Перечисленные далее технологии подчеркивают важность базовых механизмов защиты сетевой инфраструктуры, включая самозащиту устройств под управлением операционной системы Cisco IOS в случае DDoS-атак и защищенный доступ для управления устройством для снижения до минимума возможности атак с использованием спуфинга на интерфейсы управления и мониторинга.

AutoSecure

Для настройки параметров безопасности необходимо осознавать их воздействие на систему. Ошибки или упущения при настройке таких параметров могут поставить под угрозу безопасность сети и подвергнуть риску доступность, целостность и конфиденциальность передаваемой по сети информации. Многие сетевые администраторы обладают ограниченными техническими знаниями и не до конца понимают воздействие каждого параметра операционной системы конфигурации Cisco IOS на безопасность инфраструктуры в целом.

Средства Cisco AutoSecure позволяют обеспечить выполнение жизненно важных требований к обеспечению безопасности корпоративных сетей и сетей операторов связи за счет использования простого и быстрого процесса блокировки устройств. Они упрощают процесс обеспечения безопасности путем быстрого внедрения политик и процедур безопасности, не требуя глубоких знаний особенностей программного обеспечения Cisco IOS или выполнения интерфейса командной строки (CLI) вручную. Средства AutoSecure позволяют подать всего одну команду интерфейса командной строки (CLI), которая мгновенно запускает процедуру оценки безопасности маршрутизаторов и отключает ненужные системные процессы и сервисы, исключая тем самым возможность возникновения угроз безопасности.

В зависимости от конкретного сценария развертывания клиента решение Cisco AutoSecure можно развернуть в одном из двух режимов.

- **Интерактивный режим:** вывод запросов на включение и отключение определенных сервисов и других функций безопасности.
- **Неинтерактивный режим:** автоматическое выполнение команды AutoSecure с рекомендуемыми параметрами Cisco по умолчанию.

Для получения дополнительной информации о функции AutoSecure посетите web-сайты по адресам:

http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6642/prod white paper09186a00801dbf61.html

http://www.cisco.com/en/US/products/ps6642/products white paper09186a0080183b83.shtml

http://www.cisco.com/en/US/docs/ios/sec user services/configuration/guide/sec autosecure.html

Политики и защита уровня управления

Атаки типа «отказ в обслуживании" опасны даже для самых надежных программных и аппаратных решений. Такие атаки нередко представляют собой злонамеренные действия с целью парализовать сетевую инфраструктуру путем ее перегрузки бесполезным трафиком, замаскированным под управляющие пакеты определенного типа и адресованных процессору уровня управления. Распределенные атаки типа «отказ в обслуживании» (DDoS) увеличивают количество ненужного IP-

трафика (иногда на целые гигабайты в секунду), задействуя сотни отправителей. Потоки IP-трафика содержат пакеты, предназначенные для обработки уровнем управления процессоров маршрутизаторов Cisco. Из-за высокой скорости поступления вредоносных пакетов в процессоре маршрутизации уровень управления вынужден тратить много времени на обработку и отброс DoS-трафика.

Для блокировки этих и аналогичных угроз, направленных на ядро системы (т. е. процессор), уровень управления располагает программируемой функцией ограничения на маршрутизаторах, которая ограничивает интенсивность трафика (или политики), адресатом которого является уровень управления. Механизм классификации QoS операционной системы Cisco IOS позволяет настроить эту функцию для идентификации и ограничения трафика определенных типов либо полностью, либо при превышении заданного порогового уровня (рис. 5).

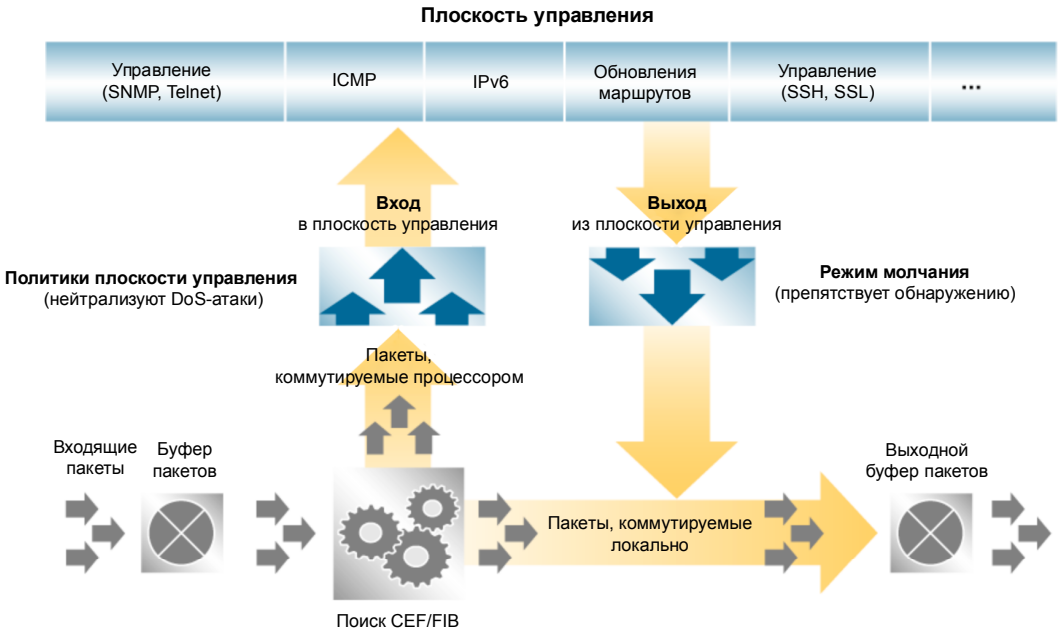
Средства защиты уровня управления расширяют эту возможность задания политик за счет большей детализованности.

Для получения дополнительной информации о политиках и защите уровня управления посетите web-сайты по адресам:

http://www.cisco.com/en/US/products/ps6642/prod white papers list.html

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122s18/gtrtlimt.htm

Рисунок 5. Политики уровня управления: буфер пакетов, входящие пакеты, технология Cisco Express Forwarding и поиск в базе Forwarding Information Base (FIB), выходной буфер пакетов и «режим молчания»



Уведомления о достижении пороговых значений ресурсов ЦП и памяти

Ресурсы ЦП и памяти имеют важное значение при нейтрализации возможной попытки ограничить доступность сетевого устройства. В настоящее время базы MIB SNMP позволяют система мониторинга контролировать доступность определенного ресурса. В связи с динамическим характером этих ресурсов плановый опрос переменных часто задерживает процесс принятия мер, необходимых для обеспечения максимальной доступности сети.

Функция формирования уведомлений о достижении пороговых значений памяти предназначена для управления объемом памяти, потребляемым различными группами ресурсов. Максимальный объем памяти можно указать в байтах или в виде

процентного значения от общих ресурсов процессора. Когда для группы ресурсов объем используемой памяти приближается к заданному пороговому значению, система формирует уведомление.

С помощью уведомления о достижении пороговых значений ресурсов ЦП можно настроить пороговые значения использования ЦП, превышение которых приводит к формированию оповещения. Операционная система Cisco IOS поддерживает два пороговых значения загрузки ЦП.

- Верхнее пороговое значение. Процент ресурсов ЦП, при превышении которого в течение заданного периода времени формируется уведомление о пороговом значении ресурсов ЦП.
- Нижнее пороговое значение. Если загрузка ЦП в течение заданного периода времени не достигает заданного значения, система формирует уведомление о пороговом значении ресурсов ЦП.

Для получения дополнительной информации об уведомлениях о достижении пороговых значений ресурсов ЦП и памяти посетите web-сайты по адресам:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_4/gt_cput.htm

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gt_memnt.html

Защита механизмов маршрутизации

- Аутентификация узлов, с которыми выполняется обмен маршрутной информацией, с помощью алгоритма MD5. Аутентификация таких узлов с помощью алгоритма MD5 гарантирует, что маршрутизатор получает только надежную маршрутную информацию и только от доверенных соседей. Каждое обновление маршрутизации хэшируется по алгоритму MD5, а затем итоговая подпись (дайджест) отправляется в виде части сообщения об обновлении маршрутизации. В этом случае маршрутизатор получает возможность подтвердить аутентичность каждого соседнего устройства и целостность обновлений маршрутизации.
- Проверка безопасности TTL для протокола BGP. Проверка TTL предотвращает распространение DoS-атак на основе маршрутизации, несанкционированный обмен маршрутной информацией, а также атаки, направленные на разрыв соединений, запускаемые из систем, не подключенных напрямую к той же сети, что и атакуемые маршрутизаторы.
- Проверка безопасности TTL позволяет настроить минимальное допустимое значение TTL для пакетов, обмен которыми осуществляется между одноранговыми узлами EBGP. Если эта функция включена, оба маршрутизатора передают весь трафик друг к другу со значением TTL, равным 255. Кроме того, маршрутизаторы устанавливают взаимодействие, только если один узел EBGP отправляет другому пакеты со значением TTL, равным или большим значению TTL, настроенному для взаимодействия с соседними узлами. Все пакеты, полученные со значениями TTL меньше предопределенного, отбрасываются без предупреждения.
- Эти функции рекомендуется включить на всех маршрутизаторах, особенно на тех, которые обмениваются маршрутной информацией с внешними устройствами. Для получения дополнительной информации об этих функциях посетите web-сайт по адресу: http://www.cisco.com/en/US/docs/solutions/Enterprise/Security/Baseline_Security/sec_chap3.html

Защита с использованием списков контроля доступа (ACL)

- Списки ACL защищают граничные маршрутизаторы от трафика злоумышленников. Они в явном виде разрешают санкционированный трафик (например, трафик маршрутизации и управления, отправляемый с авторизованных устройств), который может быть адресован граничному маршрутизатору.
- Выборочное удаление пакетов с опциями IP-заголовка. В связи с необходимостью обработки параметров и перезаписи IP-заголовка в большинстве маршрутизаторов Cisco пакеты с опциями IP-заголовка проходят фильтрацию и коммутируются с использованием программного обеспечения маршрутизатора. Это создает потенциальную угрозу безопасности, поскольку неправильно сформированные пакеты с IP-параметрами могут отрицательно повлиять на производительность устройства. Выборочное удаление пакетов с опциями IP-заголовка с помощью ACL позволяет маршрутизаторам Cisco выполнять фильтрацию пакетов с опциями IP-заголовка или нейтрализовывать последствия обработки опций IP-заголовка в маршрутизаторе путем удаления этих пакетов или игнорирования опций IP-заголовка.

Для получения дополнительной информации о выборочном удалении пакетов с опциями IP-заголовков с помощью ACL посетите web-сайт по адресу:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s23/sel drop.htm

Режим защищенного доступа (режим молчания)

Одним из этапов нарушения безопасности системы является разведка, то есть получение информации о сети. Хакеры проводят разведку путем анализа системных сообщений, например о состоянии доставки пакетов, в которых содержится определенная информация (к примеру, IP-адреса устройств).

Режим защищенного доступа (известный также как режим молчания) является новой функциональной возможностью ПО Cisco IOS, предназначенной для сокращения объема информации, которую злоумышленник может собрать о сети. Она препятствует созданию некоторых информационных пакетов маршрутизатором. Например, она подавляет отправку сообщений ICMP и сообщений SNMP Trap, которые обычно формирует маршрутизатор. Аналогично политикам уровня управления режим безопасного доступа использует преимущества известного интерфейса (MQC).

Для получения дополнительной информации о режиме безопасного доступа посетите web-сайт по адресу:

https://www.cisco.com/en/US/products/ps6540/prod_bulletin09186a00801d7229.html#wp1002091

Экспорт необработанного IP-трафика

Для проведения детального анализа безопасности сетевого трафика многим администраторам сети требуется подключать специальные средства, например анализаторы протоколов или серверы нейтрализации атак. Однако их подключение к маршрутизатору предполагает работу устройства в режиме транзитной передачи трафика, что приводит к сложностям при эксплуатации сети.

Функция экспорта необработанного IP-трафика представляет собой упрощенную функцию ПО Cisco IOS по экспорту IP-пакетов, которые поступают на сетевое устройство и отправляются с него. Выделенный интерфейс локальной сети экспортирует собранные IP-пакеты за пределы устройства. Цель заключается в экспорте необработанных IP-пакетов в их неизменном виде на указанное устройство (например, анализатор пакетов или устройство IDS).

Возможности экспорта необработанного IP-трафика:

- фильтрация (с использованием списков ACL), необходимая для экспорта только определенного вида трафика;
- возможность выборки для сокращения выходного объема трафика;
- возможность указания порта Ethernet для экспорта с помощью MAC-адреса, адреса 802.1q или ISL-адреса, связанного с узлом получателя, а не с помощью IP-адреса;
- регистрация включения или отключения функции с помощью средств Syslog.

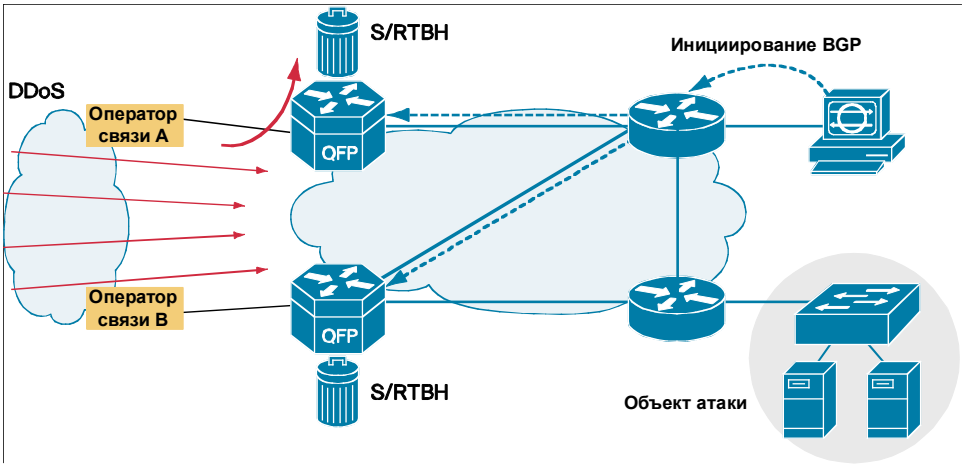
Для получения дополнительной информации об экспорте необработанного IP-трафика посетите web-сайт по адресу: http://www.cisco.com/en/US/docs/ios/12 3t/12 3t4/feature/guide/gt rawip.html.

Фильтрация на основе источника по технологии RTBH

Если организации известен источник атаки (например, на основе анализа данных NetFlow), можно применить механизмы сдерживания, такие как списки ACL. Если трафик атаки обнаружен и классифицирован, можно создать и развернуть на нужных маршрутизаторах соответствующие списки ACL. Поскольку развертывание вручную может быть трудоемким и сложным, многое заказчики используют протокол BGP, позволяющий быстро и эффективно распространить информацию об отбрасывании на все маршрутизаторы. Эта технология, известная под названием дистанционно активируемого режима удаления трафика (RTBH), устанавливает в качестве следующего узла маршрута для IP-адреса цели атаки интерфейс null. Трафик, направленный на цель атаки, отбрасывается на входе в сеть.

Другая возможность заключается в удалении трафика от конкретного источника. Этот метод аналогичен описанному выше, но опирается на существующее развертывание URPF, которое удаляет пакет, если его источник является «недопустимым». В число недопустимых пакетов входят пакеты, подлежащие передаче на интерфейс null0. Обновление BGP рассылается с использованием того же механизма удаления трафика на основе узла назначения, и в этом обновлении для источника в качестве следующего узла маршрута устанавливается null0. Теперь весь трафик от этого источника, поступающий на интерфейс с включенным механизмом URPF, удаляется. Несмотря на расширяемость, инициированное с помощью протокола BGP удаление трафика ограничивает возможный уровень детализации при реакции на атаку: удаляется весь трафик, адресованный конкретному хосту или исходящий от определенного источника, как описано выше. Во многих случаях такая реакция на массированную атаку эффективна, и это, безусловно, снижает уровень сопутствующего ущерба (см. рис. 6).

Рисунок 6. Защита от DDoS-атак с использованием фильтрации RTBH на основе адреса отправителя



Для получения дополнительной информации о фильтрации трафика на основе источника по технологии RTB посетите web-сайт по адресу:
http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6642/prod_white_paper0900aecd80313fac.pdf

Пересылка с индивидуальной адресацией по маршруту обратной передачи (URPF)

Средства URPF (пересылка с индивидуальной адресацией по маршруту обратной передачи) позволяет ограничить трафик злоумышленников в сети предприятия. Эти средства позволяют маршрутизатору проверять достижимость адреса отправителя, указанного в пересылаемых пакетах, чтобы выделять трафик с поддельных (подмененных) IP-адресов. Если IP-адрес отправителя недостоверен, пакет отбрасывается. Маршрутизаторы Cisco ISR серий 1900, 2900 и 3900 поддерживают строгий и нестрогий режимы URPF.

Если администраторы настраивают средства URPF на работу в строгом режиме, пакет должен быть получен на том интерфейсе, которой будет использоваться маршрутизатором для пересылки пакета по маршруту обратной передачи. Алгоритм URPF, настроенный на строгий режим, может отбрасывать легитимный трафик, поступающий на интерфейс, который не выбран маршрутизатором для отправки трафика по маршруту обратной передачи. Такое отбрасывание легитимного трафика может происходить при наличии в сети асимметричных маршрутов.

Если администраторы используют средства URPF на работу в нестрогом режиме, адрес отправителя должен присутствовать в таблице маршрутизации. Администраторы могут изменить это поведение с помощью параметра разрешения по умолчанию, который позволяет использовать маршрут по умолчанию в процессе проверки маршрута передачи к отправителю. Кроме того, будут отбрасываться пакеты с адресом отправителя, для которого маршрут обратной передачи проходит через интерфейс null0. Можно создать список контроля доступа, который при использовании URRF в нестрогом режиме разрешает или запрещает определенные адреса отправителей.

Для получения дополнительной информации о средствах URPF посетите web-сайты по адресам:

http://www.cisco.com/en/US/docs/ios/12_2/security/configuration/guide/scfrpf.html

http://www.cisco.com/en/US/docs/ios/sec_data_plane/configuration/guide/sec_cfg_unicast_rpf.html

http://www.cisco.com/en/US/docs/ios/sec_data_plane/configuration/guide/sec_urpf_mib.html

Цифровая подпись образа ОС

Цифровая подпись образа ОС позволяет гарантировать целостность образа программного обеспечения маршрутизатора. Для вычисления уникального 64-разрядного хэша для образа программного обеспечения используется алгоритм SHA-512. За тем хэш шифруется с помощью 2048-разрядного ключа RSA и к образу программного обеспечения добавляется полученная цифровая подпись.

Во время загрузки программного обеспечения маршрутизатор использует открытый ключ для расшифровки встроенного в образ хэша, а затем проверяет подлинность образа. Если образ отличается от эталонного даже на байт, его использование блокируется, а устройство остается защищенным.

Для получения дополнительной информации о цифровой подписи образа посетите web-сайт по адресу:

http://www.cisco.com/en/US/docs/ios/sec_data_plane/configuration/guide/sec_ips5_sig_fs_ue.html

Усовершенствования процедуры входа в систему, реализованные в ОС Cisco IOS

Контроль доступа к сетевому устройству реализован в операционной системе Cisco IOS путем запроса имени пользователя и пароля. К сожалению, злоумышленники могут решить этот вопрос с помощью словарных атак. В ходе этой атаки злоумышленник получает доступ к устройству путем программного перебора всех возможных сочетаний имен пользователей и паролей.

Усовершенствования процедуры входа в систему, реализованные в ОС Cisco IOS, добавляют временные параметры к процессу входа в систему. С помощью новых средств сетевой администратор может указать интервал времени между попытками входа, что позволяет нейтрализовать словарные атаки. Теперь в политике блокировки учетной записи пользователя можно задать период времени, в течение которого пользователь должен выполнить успешный вход в систему устройства.

Для получения дополнительной информации об усовершенствованиях входа в систему, реализованных в ОС Cisco IOS, посетите web-сайт по адресу:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gt_login.html

Ролевая модель контроля доступа к интерфейсу командной строки

Ролевая модель контроля доступа к интерфейсу командной строки позволяет сетевому администратору определить «представления», то есть набор рабочих команд и возможностей настройки, обеспечивающий выборочный или частичный доступ к программному обеспечению Cisco IOS. Представления ограничивают доступ пользователя к интерфейсу командной строки Cisco IOS и параметрам настройки, а также позволяют определять, какие команды принимаются и какие данные настройки доступны для просмотра. В качестве примера использования контроля доступа к интерфейсу командной строки можно привести ограничение доступа специалистов по информационной безопасности только к конкретным функциям.

Кроме того, операторы связи могут использовать эту функцию, чтобы предоставить заказчикам ограниченный доступ для помощи при диагностике сети и устранении неисправностей.

Для получения дополнительной информации о ролевой модели контроля доступа к интерфейсу командной строки посетите web-сайт по адресу:

http://www.cisco.com/en/US/docs/ios/security/configuration/guide/sec_role_base_cli.html

SSHv2

Протокол SSH версии 2 предоставляет новые эффективные возможности аутентификации и шифрования. Теперь доступно большее количество вариантов туннелирования дополнительных типов трафика поверх соединения с шифрованием, включая средства копирования файлов и работы с электронной почтой. Безопасность сети повышается за счет более широкого набора функций аутентификации, включая цифровые сертификаты и дополнительные варианты двухфакторной аутентификации.

Для получения дополнительной информации о протоколе SSH посетите web-сайт по адресу:

http://www.cisco.com/en/US/docs/ios/sec_user_services/configuration/guide/sec_cfg_secure_shell_ps6441_TSD_Products_Configuration_Guide_Chapter.html

SNMPv3

Протокол SNMPv3 является универсальным, основанным на стандартах протоколом управления сетевым оборудованием и обеспечивает защищенный доступ к устройствам за счет аутентификации и шифрования передаваемых по сети пакетов. В SNMPv3 предусмотрены следующие функции обеспечения безопасности.

- Целостность сообщений: позволяет проверить отсутствие несанкционированного изменения пакета в процессе передачи.
- Аутентификация: подтверждает достоверность источника сообщения.
- Шифрование: обеспечивает конфиденциальность передаваемых по сети данных.

SNMPv3 предусматривает модели безопасности и уровни безопасности. Модель безопасности — это метод аутентификации, настраиваемая для пользователя и группы, в которую входит пользователь. Уровень безопасности характеризует допустимую степень безопасности в рамках модели. Сочетание модели и уровня безопасности определяет механизмы безопасности, используемые при обработке SNMP-пакета. Имеются три модели безопасности: SNMPv1, SNMPv2c и SNMPv3.

Для получения дополнительной информации о SNMPv3 посетите web-сайты по адресам:

http://www.cisco.com/en/US/docs/ios/12_4t/12_4t2/snmpv3ae.html

http://www.cisco.com/en/US/docs/ios/sec_secure_connectivity/configuration/guide/sec_ipsec_snmp_supp.html

http://www.cisco.com/en/US/docs/ios/12_0t/12_0t3/feature/guide/Snmp3.html

Резюме

Маршрутизаторы Cisco поддерживают широкий спектр технологий для защиты удаленных офисов, удаленных сотрудников и мобильных пользователей. К ним относятся технологии организации VPN (как типа «сеть-сеть», так и удаленного доступа), гарантирующие конфиденциальность и целостность данных, средства обеспечения безопасности периметра, система предотвращения вторжений, средства защиты от совершенно новых атак, средства аутентификации, а также базовые средства обеспечения безопасности сети. Каждая из этих технологий может послужить основанием для приобретения маршрутизатора, поддерживающего функции обеспечения ИБ. Кроме того, простота развертывания маршрутизаторов Cisco и управления ими обеспечивает невысокую совокупную стоимость владения.

Cisco
Россия, 115054, Москва,
Космодамианская наб.,
52, стр.1, 4 этаж
Телефон: +7 495 9611410
Факс: +7 495 9611410
www.cisco.ru
www.cisco.com

Cisco
Россия, 197198,
Санкт-Петербург,
пр. Добролюбова, 16, лит. А, кор. 2
Телефон: +7 812 3136230
Факс: +7 812 3136280
www.cisco.ru
www.cisco.com

Cisco
Украина, 03038,
Киев,
ул.Николая Гринчинко, 4В
Тел: +38 044 3913600
Факс: +38 044 3913601
www.cisco.ru
www.cisco.com

Cisco
Казахстан, 050059, Алматы,
Ул. О. Жолдасбекова, 97,
блок А2, 14 этаж
Телефон: +7 727 2442101
Факс: +7 727 244 2102
www.cisco.ru
www.cisco.com

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