PIX/ASA 7.x: Пример настройки служб для включения VoIP (SIP, MGCP, H323, SCCP)

Содержание

Введение

В документе описываются методы разрешения передачи трафика протоколов Voice over IP (VoIP) для внешнего интерфейса и включения проверки для каждого протокола в устройства защиты Cisco PIX/ASA.

Задействованные протоколы:

- **Протокол инициации сеанса (SIP). SIP — это протокол управления уровнями приложения (сигнализации), создающий, изменяющий и прерывающий сеансы связи с одним или несколькими участниками.** К таким сеансам связи относятся телефонные вызовы по Интернет-связи, распределение мультимедиа и мультимедийная конференц-связь.SIP, как определено Инженерной группой по развитию Интернета (IETF), обеспечивает поддержку вызовов по VoIP. SIP взаимодействует с протоколом описания сеансов (SDP) для передачи сигналов вызовов. SDP задает подробные данные потока

мультимедиа. Устройство защиты может поддерживать любые шлюзы SIP (VoIP) и прокси-серверы VoIP при использовании SIP . SIP и SDP определены в этих RFC:SIP: протокол установления сеанса, RFC 3261SDP: протокол описания сеанса, RFC 2327Чтобы обеспечить поддержку SIP-вызовов с помощью устройства защиты, необходимо выполнить проверку сообщений сигнализации для адресов медиаподключений, медиапортов и инициируемых подключений. **Причина заключается в том, что при отправке сигналов на стандартный порт назначения (UDP/TCP 5060) выполняется динамическое выделение медиапотоков.** Кроме того SIP встраивает IP-адреса в разделы данных пользователя IP-пакетов. Проверка SIP применяет преобразование сетевых адресов (NAT) для этих встроенных IP-адресов.**Примечание:** Если удаленная конечная точка выполняет попытку регистрации с использованием прокси-сервера SIP в сети, защищенной с помощью устройства защиты, в процессе регистрации происходит ошибка при выполнении строго определенных условий. Эти условия: использование преобразования адресов портов (PAT) для удаленной конечной точки, нахождение сервера регистратора SIP во внешней сети и отсутствие данных порта в поле контактов в сообщении REGISTER, отправленного конечной точкой на прокси-сервер.

- **Протокол управления медиашлюзом (MGCP) — MGCP является протоколом управления вызовами клиент-сервер, созданным на основе централизованной архитектуры управления.** Все сведения абонентской группы хранятся в отдельном агенте вызовов. Агент вызовов, управляющий портами на шлюзе, осуществляет контроль вызова. Шлюз осуществляет трансляцию медиасоединений между коммутируемыми телефонными сетями общего пользования (PSTN) и сетями VoIP для внешних вызовов. В сети Cisco функцию агента вызовов выполняет CallManager.MGCP — стандарт IETF, определенный в нескольких RFC, включая 2705 и 3435. Его функциональность можно расширить за счет использования пакетов, которые включают, например, обработку двухтональных многочастотных (DTMF) сигналов, защищенную RTP, удержание вызовов и передачу вызовов.Настройка MGCP-шлюза относительно проста. Поскольку агенты вызовов поддерживают все интеллектуальные функции маршрутизации вызовов, пользователю не нужно настраивать шлюз с использованием всех адресуемых точек вызова, которые понадобились бы в противном случае. Недостатком является необходимость непрерывной доступности агента вызовов. Шлюзы MGCP Cisco поддерживают Survivable Remote Site Telephony (SRST) и восстановление MGCP для обеспечения возможности для протокола H.323 вступить в работу и обеспечить локальную маршрутизацию вызовов при отсутствии CallManager. В этом случае необходимо настроить адресуемые точки вызова на шлюзе для использования H.323.
- **Проверка H.323 — H.323 обеспечивает поддержку для приложений, соответствующих H.323, таких как Cisco CallManager и VocalTec Gatekeeper.** H.323 — это набор протоколов, определенный стандартами Международного союза коммуникаций для мультимедийных конференций в локальных сетях. Устройство защиты поддерживает H.323 вплоть до версии 4, включая H.323 v3 с поддержкой канала сигнализации Multiple Calls on One Call.С включенной проверкой H.323, устройство защиты поддерживает обработку нескольких вызовов на одном канале сигнализации. Эта функция была реализована в H.323 версия 3. Эта функция уменьшает срок установки вызова и уменьшает использование портов на устройстве защиты.Это две главных функции контроля H.323:Применяется NAT для необходимых встроенных IPv4-адресов в сообщениях H.225 и H.245 . Поскольку кодирование H.323-сообщений выполняется с использованием формата PER, устройство защиты использует декодер ASN.1 для

расшифровки сообщений H.323 .Динамически выделяются согласованные соединения H.245 и RTP/RTCP .

- **Простой протокол управления клиентами (SCCP) — SCCP является упрощенным протоколом, используемым в VoIP-сетях.** Cisco IP Phones с использованием SCCP можно применять в среде H.323. При использовании с Cisco CallManager, клиент SCCP может взаимодействовать с терминалами, соответствующими H.323. Функции уровней приложения в устройстве защиты распознают версию SCCP. Функциональность программного обеспечения для работы с уровнями приложений обеспечивает возможность для всех пакетов сигнализации и носителей SCCP проходить через устройство защиты за счет обеспечения использования NAT для всех пакетов сигнализации SCCP.Существует 5 версий протокола SCCP: 2.4, 3.0.4, 3.1.1, 3.2 и 3.3.2. Устройство защиты поддерживает все версии вплоть до версии 3.3.2. Устройство защиты обеспечивает поддержку и PAT, и NAT для SCCP. Использование PAT необходимо, если имеется ограниченное количество глобальных IP-адресов для использования IP- телефонами.Стандартный трафик между Cisco CallManager и IP-телефонами Cisco IP использует SCCP и обрабатывается с помощью проверки SCCP без использования специальной конфигурации. Устройство защиты также поддерживает варианты DHCP 150 и 66, обеспечивающие ему возможность отправлять данные о местоположении сервера TFTP на IP-телефоны Cisco и другие клиенты DHCP. См. Настройка служб DHCP, DDNS и WCCP для получения дополнительных сведений.

Предварительные условия

Требования

В данном документе предполагается, что для всех устройств были настроены все необходимые параметры VPN и они работают стабильно.

В документе ASA/PIX: Устройство безопасности к Примеру конфигурации Туннеля IPSec между локальными сетями Маршрутизатора IOS для узнавания больше о конфигурации VPN.

Для получения дополнительных сведений о настройке взаимодействия между интерфейсами см. документ PIX/ASA 7.x: Enable Communication Between Interfaces (PIX/ASA 7.x: обеспечение взаимодействия между интерфейсами).

Используемые компоненты

Данный документ разработан на материале устройства адаптивной защиты Cisco 5500 Adaptive Security Appliance (ASA), на котором запущено программное обеспечение версии 7.x.

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Родственные продукты

Эту конфигурацию также можно использовать для сетевого экрана Cisco 500 PIX, на котором запущено программное обеспечение версии 7.x.

Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Условные обозначения технических терминов Cisco.

Общие сведения

SIP

Проверка SIP применяет NAT к текстовым сообщениям SIP, повторно рассчитывает длину содержания для раздела SDP сообщения и повторно рассчитывает длину и контрольную сумму пакета. Она динамически открывает медиа-соединения для портов, указанных в разделах SDP SIP-сообщений как адреса/порты, которые конечная точка должна прослушивать.

Для проверки SIP существует база данных с индексами CALL_ID/FROM/TO из полезной нагрузки SIP, определяющей вызов, а также исходные и конечные адреса. В базе данных содержатся адреса и порты медиа-соединений, указанные в полях SDP для сведений о медиа-соединениях и их типах. В одном сеансе возможно использование нескольких адресов и портов медиа-соединений. С помощью этих адресов/портов открываются соединения RTP/RTCP между двумя конечными точками.

В сообщении исходной установки вызова (INVITE) необходимо использовать стандартный порт 5060 . Однако последующие сообщения не могли бы иметь этого номера порта. Модуль проверки SIP открывает каналы для соединений сигнализации и помечает эти соединения как SIP-соединения. Это делается для доставки сообщений в приложение SIP и применения к ним NAT.

После установки вызова сеанс SIP рассматривается как находящийся в переходном состоянии. Это состояние сохраняется до тех пор, пока не будет получено сообщение отклика, указывающее адрес и порт носителя RTP, прослушиваемого конечной точкой. Если в течение одной минуты не удается получить сообщение отклика, соединение сигнализации разрывается.

После окончательного завершения установления связи вызов переходит в активное состояние и соединение сигнализации не прерывается до получения сообщения BYE.

Если внутренняя конечная точка инициирует вызов внешней конечной точки, в сторону внешнего интерфейса открывается медиаканал, который обеспечивает возможность передачи UDP-пакетов RTP/RTCP на медиаадрес и медапорт внутренней конечной точки, указанные в полученном от нее сообщении INVITE. Незатребованные UDP-пакеты RTP/RTCP на адрес внутреннего интерфейса не проходят устройство защиты, за исключением тех случаев, когда в конфигурации устройства защиты дано на это явное разрешение.

Медиа-соединения разрываются в течение двух минут после перехода соединения в состояние "бездействие". Для этого тайм-аута можно задать более короткий или длительный период времени.

MGCP

Как правило, для использования MGCP необходимо настроить как минимум две команды проверки: одну для порта, через который команды принимает шлюз, а другую - для порта, через который команды принимает агент вызовов. **При нормальных условиях работы агент вызовов отправляет команды на порт MGCP, настроенный по умолчанию для шлюзов, 2427, а шлюз отправляет команды на порт MGCP, настроенный по умолчанию для агентов вызовов, а именно: 2727.**

Сообщения MGCP переданы по **UDP**. Отклик отправляется обратно на исходный адрес (IP-адрес и номер UDP-порта) команды, однако он может быть доставлен не с того адреса, на который была отправлена команда. Такая ситуация может возникнуть, если в конфигурации аварийного перехода использовалось несколько агентов вызовов, и агент вызова, получивший команды, передал управление резервному агенту вызовов, который после этого и отправил отклик.

H.323

Набор протоколов H.323 поддерживает использование до двух подключений TCP и от четырех до шести UDP-подключений. FastConnect использует только одно подключение TCP, а служба Reliability, Availability, and Serviceability (RAS) использует одно UDP-подключение для регистрации, допусков и определения состояния.

Первоначально клиент H.323 может установить TCP-соединение с сервером H.323, используя TCP-порт 1720 для запроса установки вызова Q.931. Процесс установки вызова является частью самого вызова, при этом терминал H.323 указывает клиенту номер порта для TCP-соединения H.245. В среде, в которой используется привратник H.323, исходный пакет данных передается с помощью протокола UDP.

При проверке H.323 выполняется мониторинг TCP-соединения Q.931для определения номера порта H.245. Если терминалы H.323 не используют FastConnect, устройство защиты динамически выделяет H.245-соединение на основе проверки сообщений H.225.

В каждом сообщении H.245 конечные точки H.323 указывают номера портов, использующиеся для последующих передач данных в потоковом режиме UDP. При проверке H.323 проверяются сообщения H.245 для определения этих портов и динамического создания соединений для обмена медиаданными. RTP использует согласованный номер порта, а RTCP использует порт с номером на единицу большим.

Канал управления H.323 обрабатывает H.225 и H.245, а также H.323 RAS. При проверке H.323 используются следующие порты:

- 1718— UDP-порт поиска привратника
- 1719 — порт UDP RAS
- 1720 — управляющий порт TCP

Необходимо разрешить трафик для порта 1720 — стандартного порта H.323 для сигнализации вызова H.225. Однако порты сигнализации H.245 согласовываются между конечными точками в сигнализации H.225. Если используется привратник H.323, устройство защиты открывает H.225-соединение на основе проверки сообщения подтверждения доступа (ACF).

После проверки сообщений H.225 устройство защиты открывает канал H.245, а затем

выполняет проверку трафика, отправляемого по каналу H.245. Все сообщения H.245, проходящие через устройство защиты, проходят проверку H.245, в ходе которой преобразуются встроенные IP-адреса и открываются медиаканалы, согласованные в сообщениях H.245.

Для использования стандарта H.323 ITU необходимо, чтобы H.225 и H.245, до перехода к надежному соединению, предшествовал заголовок Transport Protocol Data Unit Packet (TPKT), определяющий длину сообщения. Поскольку заголовок TPKT не обязательно отправлять в том же TCP-пакете, что и сообщения H.225 и H.245, в устройстве защиты должны сохраняться данные о длине TPKT для правильной обработки и декодирования сообщений. Для каждого соединения устройство защиты сохраняет данные о длине TPKT для следующего запланированного сообщения.

Если устройству защиты необходимо использовать NAT для IP-адресов в сообщениях, то выполняется изменение контрольной суммы, длины UUIE, и TPKT, если он включен в TCP-пакет с сообщением H.225. Если TPKT отправляется в отдельном TCP-пакете, прокси устройства защиты подтверждает (ACK) TPKT и дополняет новым TPKT сообщение H.245 с новой длиной.

SCCP

В конфигурациях, где Cisco CallManager топологически располагается на интерфейсе с более высоким относительно IP-телефонов Cisco уровне безопасности, и для IP-адреса Cisco CallManager необходима трансляция адресов (NAT), сопоставление адресов должно быть статическим, поскольку для IP-телефона Cisco необходимо явным образом задать IP-адрес Cisco CallManager в его конфигурации. Статическая запись удостоверения позволяет Cisco CallManager на более защищенном интерфейсе принимать регистрации от IP-телефонов Cisco.

Для использования IP-телефонов Cisco необходим доступ к TFTP-серверу для загрузки данных конфигурации, необходимых для подключения к серверу Cisco CallManager.

Если IP-телефоны Cisco находятся на более низком уровне безопасности по сравнению с сервером TFTP, необходимо воспользоваться списком доступа для подключения к защищенному TFTP-серверу с использованием UDP-порта 69. Хотя TFTP-серверу необходима статическая запись, это не должна быть статическая запись удостоверения. Если используется NAT, выполняется соотнесение статической записи удостоверения с тем же IP-адресом. Если используется PAT, выполняется соотнесение статической записи удостоверения с тем же IP-адресом и портом.

Если IP-телефоны Cisco находятся на интерфейсе с более высоким уровнем безопасности по сравнению с сервером TFTP и Cisco CallManager, нет необходимости в списке доступа или статической записи, чтобы обеспечить IP-телефонам Cisco возможность инициации соединения.

Настройка

В этом разделе содержатся сведения о настройке функций, описанных в этом документе.

Примечание: Используйте инструмент Command Lookup (только для зарегистрированных пользователей) для того, чтобы получить более подробную информацию о командах,

использованных в этом разделе.

Диаграмма сети для SIP

В данном разделе используются следующие настройки сети:

Конфигурации для SIP

В этом разделе используются следующие конфигурации:

Устройство защиты поддерживает проверку приложений с помощью алгоритма адаптивной защиты (ASA). С помощью проверки с отслеживанием состояния соединений, используемой алгоритмом адаптивной защиты, устройство защиты отслеживает все подключения, использующие межсетевой экран, и подтверждает их допустимость. При помощи проверки с отслеживанием состояния межсетевой экран также отслеживает состояние подключений и собирает сведения, которые будут сохранены в таблице состояний. При использовании таблицы состояний в дополнение к правилам, определенным администратором, решения о фильтрации основываются на контексте, создаваемом пакетами, которые были переданы ранее через межсетевой экран. Реализация проверок приложений состоит из следующих этапов:

- Идентификация трафика.
- Применение проверки к трафику.
- Включение проверки для интерфейса.

Настройка базовой проверки SIP

По умолчанию в конфигурацию включается политика, соотносящая весь трафик проверок приложений, заданных по умолчанию, и применяющая проверку для трафика на всех интерфейсах (глобальная политика). Трафик проверки приложений по умолчанию включает трафик к портам по умолчанию для каждого протокола. Применять можно только одну глобальную политику. Таким образом, если необходимо изменить глобальную политику, например, для применения проверок нестандартных портов или для добавления проверок, не заданных по умолчанию, нужно либо изменить политику по умолчанию, либо отключить ее и применить новую политику. Полный список всех портов по умолчанию см. в разделе Политика проверок по умолчанию.

1. **Введите policy-map global_policy.** `ASA5510(config)#policy-map global_policy`
2. **Введите class inspection_default.** `ASA5510(config-pmap)#class inspection_default`
3. Выполните **команду inspect sip.** `ASA5510(config-pmap-c)#inspect sip`

Конфигурация ASA для SIP

```
ASA Version 7.2(1)24
!
ASA5510 ASA5510
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Ethernet0/0
 nameif inside
 security-level 100
 ip address 10.1.1.1 255.255.255.0
!
interface Ethernet0/1
 nameif outside
```

```
 security-level 0
 ip address 172.16.1.2 255.255.255.0
!
!--- Output suppressed. passwd 2KFQnbNIdI.2KYOU
encrypted ftp mode passive !--- Command to allow the
incoming SIP traffic. access-list 100 extended permit
tcp 10.2.2.0 255.255.255.0 host 172.16.1.5 eq sip pager
lines 24 mtu inside 1500 mtu outside 1500 no failover
asdm image disk0:/asdm-522.bin no asdm history enable
arp timeout 14400 !--- Command to redirect the SIP
traffic received on outside interface to !--- inside
interface for the specified IP address. static
(inside,outside) 172.16.1.5 10.1.1.10 netmask
255.255.255.255 access-group 100 in interface outside
route outside 0.0.0.0 0.0.0.0 172.16.1.1 1 timeout xlate
3:00:00 timeout conn 1:00:00 half-closed 0:10:00 udp
0:02:00 icmp 0:00:02 timeout sunrpc 0:10:00 h323 0:05:00
h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00 timeout sip
0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-
disconnect 0:02:00 timeout uauth 0:05:00 absolute no
snmp-server location no snmp-server contact snmp-server
enable traps snmp authentication linkup linkdown
coldstart telnet timeout 5 ssh timeout 5 console timeout
0 ! class-map inspection_default match default-
inspection-traffic ! ! policy-map type inspect dns
preset_dns_map parameters message-length maximum 512
policy-map global_policy class inspection_default
inspect dns preset_dns_map inspect h323 h225 inspect
h323 ras inspect netbios inspect rsh inspect rtsp
inspect skinny inspect esmtp inspect sqlnet inspect
sunrpc inspect tftp !--- Command to enable SIP
inspection. inspect sip inspect xdmcp inspect ftp ! !---
This command tells the device to !--- use the
"global_policy" policy-map on all interfaces. service-
policy global_policy global prompt ASA5510 context
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e : end
ASA5510#
```

Диаграмма сети для MGCP, H.323 и SCCP

В данном разделе используются следующие настройки сети:

Конфигурации для MGCP

В этом разделе используются следующие конфигурации:

Устройство защиты поддерживает проверку приложений с помощью алгоритма адаптивной защиты (ASA). С помощью проверки с отслеживанием состояния соединений, используемой алгоритмом адаптивной защиты, устройство защиты отслеживает все подключения, использующие межсетевой экран, и подтверждает их допустимость. При помощи проверки с отслеживанием состояния межсетевой экран также отслеживает состояние подключений и собирает сведения, которые будут сохранены в таблице состояний. При использовании таблицы состояний в дополнение к правилам, определенным администратором, решения о фильтрации основываются на контексте, создаваемом пакетами, которые были переданы ранее через межсетевой экран. Реализация проверок приложений состоит из следующих этапов:

- Идентификация трафика.

- Применение проверки к трафику.
- Включение проверки для интерфейса.

Настройка базовой проверки MGCP

По умолчанию в конфигурацию включается политика, соотносящая весь трафик проверок приложений, заданных по умолчанию, и применяющая проверку для трафика на всех интерфейсах (глобальная политика). Трафик проверки приложений по умолчанию включает трафик к портам по умолчанию для каждого протокола. Применять можно только одну глобальную политику. Таким образом, если необходимо изменить глобальную политику, например, для применения проверок нестандартных портов или для добавления проверок, не заданных по умолчанию, нужно либо изменить политику по умолчанию, либо отключить ее и применить новую политику. Полный список всех портов по умолчанию см. в разделе Политика проверок по умолчанию.

1. **Введите policy-map global_policy.**`ASA5510(config)#policy-map global_policy`
2. **Введите class inspection_default.**`ASA5510(config-pmap)#class inspection_default`
3. Выполните **команду inspect mgcp.**`ASA5510(config-pmap-c)#inspect mgcp`

Настройте карту политики проверки MGCP для дополнительного инспекционного контроля

Если сеть имеет агентов составного вызова и шлюзы, для которых устройство безопасности должно открыть крошечные отверстия, создать карту MGCP. Можно тогда применить карту MGCP при включении контроля MGCP. См. Контроль приложения Настройки для получения дополнительной информации.

```
!--- Permits inbound 2427 port traffic. ASA5510(config)#access-list 100 extended permit udp
10.2.2.0 255.255.255.0 host 172.16.1.5 eq 2427 !--- Permits inbound 2727 port traffic.
ASA5510(config)#access-list 100 extended permit udp 10.2.2.0 255.255.255.0 host 172.16.1.5 eq
2727 ASA5510(config)#class-map mgcp_port ASA5510(config-cmap)#match access-list 100
ASA5510(config-cmap)#exit !--- Command to create an MGCP inspection policy map.
ASA5510(config)#policy-map type inspect mgcp mgcpmap !--- Command to configure parameters that
affect the !--- inspection engine and enters into parameter configuration mode. ASA5510(config-
pmap)#parameters !--- Command to configure the call agents. ASA5510(config-pmap-p)#call-agent
10.1.1.10 101 !--- Command to configure the gateways. ASA5510(config-pmap-p)#gateway 10.2.2.5
101 !--- Command to change the maximum number of commands !--- allowed in the MGCP command
queue. ASA5510(config-pmap-p)#command-queue 150 ASA5510(config-pmap-p)# exit
ASA5510(config)#policy-map inbound_policy ASA5510(config-pmap)# class mgcp_port ASA5510(config-
pmap-c)#inspect mgcp mgcpmap ASA5510(config-pmap-c)# exit ASA5510(config)#service-policy
inbound_policy interface outside
```

Конфигурация ASA для MGCP

```
ASA Version 7.2(1)24
!
hostname ASA5510
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Ethernet0/0
 nameif inside
 security-level 100
 ip address 10.1.1.1 255.255.255.0
!
interface Ethernet0/1
 nameif outside
 security-level 0
 ip address 172.16.1.2 255.255.255.0
!
!--- Permits inbound 2427 and 2727 port traffic. access-
```

```
list 100 extended permit udp 10.2.2.0 255.255.255.0 host
172.16.1.5 eq 2427 access-list 100 extended permit udp
10.2.2.0 255.255.255.0 host 172.16.1.5 eq 2727 pager
lines 24 mtu inside 1500 mtu outside 1500 no failover no
asdm history enable arp timeout 14400 !--- Command to
redirect the MGCP traffic received on outside interface
to !--- inside interface for the specified IP address.
static (inside,outside) 172.16.1.5 10.1.1.10 netmask
255.255.255.255 access-group 100 in interface outside
timeout xlate 3:00:00 timeout conn 1:00:00 half-closed
0:10:00 udp 0:02:00 icmp 0:00:02 timeout sunrpc 0:10:00
h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00
sip-disconnect 0:02:00 timeout uauth 0:05:00 absolute no
snmp-server location no snmp-server contact snmp-server
enable traps snmp authentication linkup linkdown
coldstart telnet timeout 5 ssh timeout 5 console timeout
0 ! class-map mgcp_port match access-list 100 class-map
inspection_default match default-inspection-traffic ! !
policy-map type inspect dns preset_dns_map parameters
message-length maximum 512 policy-map global_policy
class inspection_default inspect dns preset_dns_map
inspect ftp inspect h323 h225 inspect h323 ras inspect
netbios inspect rsh inspect rtsp inspect skinny inspect
esmtp inspect sqlnet inspect sunrpc inspect tftp inspect
sip inspect xdmcp inspect mgcp policy-map type inspect
mgcp mgcpmap parameters call-agent 10.1.1.10 101 gateway
10.2.2.5 101 command-queue 150 policy-map inbound_policy
class mgcp_port inspect mgcp mgcpmap ! service-policy
global_policy global service-policy inbound_policy
interface outside prompt hostname context
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e : end
```

Конфигурации для H.323

В этом разделе используются следующие конфигурации:

Устройство защиты поддерживает проверку приложений с помощью алгоритма адаптивной защиты (ASA). С помощью проверки с отслеживанием состояния соединений, используемой алгоритмом адаптивной защиты, устройство защиты отслеживает все подключения, использующие межсетевой экран, и подтверждает их допустимость. При помощи проверки с отслеживанием состояния межсетевой экран также отслеживает состояние подключений и собирает сведения, которые будут сохранены в таблице состояний. При использовании таблицы состояний в дополнение к правилам, определенным администратором, решения о фильтрации основываются на контексте, создаваемом пакетами, которые были переданы ранее через межсетевой экран. Реализация проверок приложений состоит из следующих этапов:

- Идентификация трафика.
- Применение проверки к трафику.
- Включение проверки для интерфейса.

Настройка базовой проверки H.323

По умолчанию в конфигурацию включается политика, соотносящая весь трафик проверок приложений, заданных по умолчанию, и применяющая проверку для трафика на всех интерфейсах (глобальная политика). Трафик проверки приложений по умолчанию включает трафик к портам по умолчанию для каждого протокола. Применять можно только одну

глобальную политику. Таким образом, если необходимо изменить глобальную политику, например, для применения проверок нестандартных портов или для добавления проверок, не заданных по умолчанию, нужно либо изменить политику по умолчанию, либо отключить ее и применить новую политику. Полный список всех портов по умолчанию см. в разделе Политика проверок по умолчанию.

1. **Введите policy-map global_policy.** `ASA5510(config)#policy-map global_policy`
2. **Введите class inspection_default.** `ASA5510(config-pmap)#class inspection_default`
3. Выполните **команду inspect h323.** `ASA5510(config-pmap-c)#inspect h323 h225 ASA5510(config-pmap-c)#inspect h323 ras`

Конфигурация ASA для H.323

```
ASA Version 7.2(1)24
!
ASA5510 ASA5510
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Ethernet0/0
 nameif inside
 security-level 100
 ip address 10.1.1.1 255.255.255.0
!
interface Ethernet0/1
 nameif outside
 security-level 0
 ip address 172.16.1.2 255.255.255.0
!
!--- Output suppressed. passwd 2KFQnbNIdI.2KYOU
encrypted ftp mode passive !--- Command to allow the
incoming Gate Keeper Discovery UDP port traffic. access-
list 100 extended permit udp 10.2.2.0 255.255.255.0 host
172.16.1.5 eq 1718 !--- Command to allow the incoming
RAS UDP port. access-list 100 extended permit udp
10.2.2.0 255.255.255.0 host 172.16.1.5 eq 1719 !---
Command to allow the incoming h323 protocol traffic.
access-list 100 extended permit tcp 10.2.2.0
255.255.255.0 host 172.16.1.5 eq h323 pager lines 24 mtu
inside 1500 mtu outside 1500 no failover asdm image
disk0:/asdm-522.bin no asdm history enable arp timeout
14400 !--- Command to redirect the h323 protocol traffic
received on outside interface to !--- inside interface
for the specified IP address. static (inside,outside)
172.16.1.5 10.1.1.10 netmask 255.255.255.255 access-
group 100 in interface outside route outside 0.0.0.0
0.0.0.0 172.16.1.1 1 timeout xlate 3:00:00 timeout conn
1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp
0:05:00 mgcp-pat 0:05:00 timeout sip 0:30:00 sip_media
0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout uauth 0:05:00 absolute no snmp-server location
no snmp-server contact snmp-server enable traps snmp
authentication linkup linkdown coldstart telnet timeout
5 ssh timeout 5 console timeout 0 ! class-map
inspection_default match default-inspection-traffic ! !
policy-map type inspect dns preset_dns_map parameters
message-length maximum 512 policy-map global_policy
class inspection_default inspect dns preset_dns_map !---
Command to enable H.323 inspection. inspect h323 h225
inspect h323 ras inspect netbios inspect rsh inspect
rtsp inspect skinny inspect esmtp inspect sqlnet inspect
sunrpc inspect tftp inspect sip inspect xdmcp inspect
```

```
ftp ! !--- This command tells the device to !--- use the
"global_policy" policy-map on all interfaces. service-
policy global_policy global prompt ASA5510 context
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e : end
ASA5510#
```

Конфигурации для SCCP

В этом разделе используются следующие конфигурации:

Устройство защиты поддерживает проверку приложений с помощью алгоритма адаптивной защиты (ASA). С помощью проверки с отслеживанием состояния соединений, используемой алгоритмом адаптивной защиты, устройство защиты отслеживает все подключения, использующие межсетевой экран, и подтверждает их допустимость. При помощи проверки с отслеживанием состояния межсетевой экран также отслеживает состояние подключений и собирает сведения, которые будут сохранены в таблице состояний. При использовании таблицы состояний в дополнение к правилам, определенным администратором, решения о фильтрации основываются на контексте, создаваемом пакетами, которые были переданы ранее через межсетевой экран. Реализация проверок приложений состоит из следующих этапов:

- Идентификация трафика.
- Применение проверки к трафику.
- Включение проверки для интерфейса.

Настройте основной контроль SCCP

По умолчанию в конфигурацию включается политика, соотносящая весь трафик проверок приложений, заданных по умолчанию, и применяющая проверку для трафика на всех интерфейсах (глобальная политика). Трафик проверки приложений по умолчанию включает трафик к портам по умолчанию для каждого протокола. Применять можно только одну глобальную политику. Таким образом, если необходимо изменить глобальную политику, например, для применения проверок нестандартных портов или для добавления проверок, не заданных по умолчанию, нужно либо изменить политику по умолчанию, либо отключить ее и применить новую политику. Полный список всех портов по умолчанию см. в разделе Политика проверок по умолчанию.

1. **Введите policy-map global_policy.**`ASA5510(config)#`**`policy-map global_policy`**
2. **Введите class inspection_default.**`ASA5510(config-pmap)#`**`class inspection_default`**
3. **Введите inspect skinny.**`ASA5510(config-pmap-c)#`**`inspect skinny`**

Конфигурация ASA для SCCP

```
ASA Version 7.2(1)24
!
ASA5510 ASA5510
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Ethernet0/0
 nameif inside
 security-level 100
 ip address 10.1.1.1 255.255.255.0
!
interface Ethernet0/1
 nameif outside
 security-level 0
```

```
 ip address 172.16.1.2 255.255.255.0
!
!--- Output suppressed. passwd 2KFQnbNIdI.2KYOU
encrypted ftp mode passive !--- Command to allow the
incoming SCCP traffic. access-list 100 extended permit
tcp 10.2.2.0 255.255.255.0 host 172.16.1.5 eq 2000 pager
lines 24 mtu inside 1500 mtu outside 1500 no failover
asdm image disk0:/asdm-522.bin no asdm history enable
arp timeout 14400 !--- Command to redirect the SIP
traffic received on outside interface to !--- inside
interface for the specified IP address. static
(inside,outside) 172.16.1.5 10.1.1.10 netmask
255.255.255.255 access-group 100 in interface outside
route outside 0.0.0.0 0.0.0.0 172.16.1.1 1 timeout xlate
3:00:00 timeout conn 1:00:00 half-closed 0:10:00 udp
0:02:00 icmp 0:00:02 timeout sunrpc 0:10:00 h323 0:05:00
h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00 timeout sip
0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-
disconnect 0:02:00 timeout uauth 0:05:00 absolute no
snmp-server location no snmp-server contact snmp-server
enable traps snmp authentication linkup linkdown
coldstart telnet timeout 5 ssh timeout 5 console timeout
0 ! class-map inspection_default match default-
inspection-traffic ! ! policy-map type inspect dns
preset_dns_map parameters message-length maximum 512
policy-map global_policy class inspection_default
inspect dns preset_dns_map inspect h323 h225 inspect
h323 ras inspect netbios inspect rsh inspect rtsp !---
Command to enable SCCP inspection. inspect skinny
inspect esmtp inspect sqlnet inspect sunrpc inspect tftp
inspect sip inspect xdmcp inspect ftp ! !--- This
command tells the device to !--- use the "global_policy"
policy-map on all interfaces. service-policy
global_policy global prompt ASA5510 context
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e : end
ASA5510#
```

Проверка

Этот раздел позволяет убедиться, что конфигурация работает правильно.

Средство Output Interpreter (OIT) (только для зарегистрированных клиентов) поддерживает определенные команды show. Посредством OIT можно анализировать выходные данные команд show.

SIP:

Чтобы гарантировать, что конфигурация успешно взяла, использует команду show service-policy и ограничивает выходные данные проверкой SIP только, с помощью команды show service-policy inspect sip.

```
ASA5510#show service-policy inspect sip Global policy: Service-policy: global_policy Class-map:
inspection_default Inspect: sip, packet 0, drop 0, reset-drop 0 ASA5510#
```

MGCP:

```
ASA5510#show service-policy inspect mgcp Global policy: Service-policy: global_policy Class-map:
inspection_default Inspect: skinny, packet 0, drop 0, reset-drop 0
```

H.323:

```
ASA5510(config)#show service-policy inspect h323 h225 Global policy: Service-policy:
global_policy Class-map: inspection_default Inspect: h323 h225 _default_h323_map, packet 0, drop
0, reset-drop 0 h245-tunnel-block drops 0 connection ASA5510(config)#show service-policy inspect
h323 ras Global policy: Service-policy: global_policy Class-map: inspection_default Inspect:
h323 ras _default_h323_map, packet 0, drop 0, reset-drop 0 h245-tunnel-block drops 0 connection
```

SCCP:

```
ASA5510(config)#show service-policy inspect skinny Global policy: Service-policy: global_policy
Class-map: inspection_default Inspect: skinny, packet 0, drop 0, reset-drop 0
```

Устранение неполадок

Проблема

Коммуникатор офиса не может пройти через ASA, iPhone, зарегистрированный по VPN-туннелю, разъединен, или нет никакого аудио на IP-телефонах через VPN-туннели.

Решение

Коммуникатор офиса не использовал стандартного SIP, и по умолчанию, ASA отбрасывает его. Отключите SIP, Skinny и контроль H323 для решения этой проблемы и также `clear xlate` и `local-host` в ASA. То же решение просит iPhone также.

Проблема

Видеовызовы отказали с сообщением об ошибках `%ASA-4-405102: Unable to Pre-allocate H245 Connection for faddr XX.XX.XX.XX to laddr XX.XX.XX.XX/3239.`

Решение

Отключите контроль H323 для решения этого вопроса.

Дополнительные сведения

- PIX/ASA 7.X : Включите связь между интерфейсами
- Обработка трафика VoIP с помощью сетевого экрана PIX
- Cisco Unified CallManager 5.0 TCP и использование порта UDP
- Поддержка устройств адаптивной безопасности Cisco ASA серии 5500
- Поддержка продуктов устройств защиты Cisco PIX серии 500
- Поддержка технологии протокола MGCP
- Поддержка технологии протокола SCCP
- Поддержка технологии H.323
- Cisco Systems – техническая поддержка и документация