PIX/ASA 7.x: пример включения служб FTP/TFTP

Содержание

Введение

В данном документе описываются действия, которые необходимо выполнить пользователям, не подключенным к вашей сети, для получения доступа к FTP и TFTP-службам DMZ-сети.

Протокол передачи данных (FTP)

Существует две формы FTP:

- Активный режим
- Пассивный режим

В активном режиме работы FTP клиент подключается с использованием случайного неспециализированного порта (N>1023) к командному порту (21) FTP-сервера. Затем клиент начинает прослушивать порт N+1 и отправляет FTP-серверу команду port N+1. Затем сервер повторно подключается к указанным портам данных клиента от локального порта

данных, а именно порта 20.

В пассивном режиме работы FTP-клиент инициирует оба подключения к серверу, что устраняет проблему межсетевого экрана, фильтрующего входящие подключения по порту данных к клиенту от сервера. При открытии FTP-соединения клиент локально открывает два случайных неспециализированных порта (N>1023 и N+1). Первый порт связывается с сервером на порту 21. **Но затем, вместо отправки port и обеспечения серверу возможности подключения к порту данных, клиент отправляет команду PASV. В результате сервер открывает случайный неспециализированный порт (P>1023) и отправляет команду port P обратно на сервер.** После этого клиент инициирует подключение от порта N+1 к порту P на сервере для передачи данных. Без **инспекционной** настройки команды на Устройстве безопасности FTP из пользователей возглавил исходящие работы только в Пассивном режиме. Кроме того, пользователи снаружи возглавили входящий к вашему серверу FTP, запрещены доступ.

См. ASA 8.3 и Позже: Пример конфигурации Enable FTP/TFTP Services для получения дополнительной информации об одинаковой конфигурации с помощью ASDM с устройством адаптивной защиты Cisco (ASA) с версией 8.3 и позже.

Упрощенный протокол передачи файлов (TFTP)

TFTP, как описывается в RFC 1350, — это простой протокол, используемый для чтения и записи файлов между сервером и клиентом TFTP. TFTP использует UDP-порт 69.

Предварительные условия

Требования

Убедитесь, что вы обеспечили выполнение следующих требований, прежде чем попробовать эту конфигурацию:

- Существует базовое взаимодействие между необходимыми интерфейсами.
- Имеется сконфигурированный FTP-сервер, расположенный в сети DMZ.

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- Adaptive Security Appliance серия ASA 5500, на котором запускается образ программного обеспечения 7.2(2)
- Windows 2003 Server, который выполняет сервисы FTP
- Windows 2003 Server, который выполняет Сервисы TFTP
- Компьютер пользователя расположен вне сети

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.

Схема сети

В настоящем документе используется следующая схема сети:

Примечание: Схемы IP-адресации, которые использованы в данной конфигурации, не поддерживаются официальной маршрутизацией в Интернете. Это адреса RFC 1918, используемые в лабораторной среде.

Родственные продукты

Эта конфигурация также может быть использована для PIX Security Appliance 7.x.

Условные обозначения

Более подробную информацию о применяемых в документе обозначениях см. в описании условных обозначений, используемых в технической документации Cisco.

Общие сведения

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.

Обработка сложных протоколов

Ftp

Для некоторых приложений необходима специальная обработка с использованием функции проверки приложений Cisco Security Appliance. Эти типы приложений обычно встраивают данные, связанные с IP-адресацией в пакет данных пользователя или в открытые дополнительные каналы на динамически назначенных портах. Функция проверки приложений с использованием преобразования сетевых адресов (NAT) используется для идентификации местоположения встроенных данных адресации.

В дополнение к идентификации встроенной адресной информации контроль приложения функционирует сеансы мониторов для определения номеров портов для дополнительных каналов. Много протоколов открывают вторичный TCP или порты UDP для улучшения производительности. Исходный сеанс связи на стандартном порту используется для согласования номеров динамически назначенных портов. Функция контроля приложения контролирует эти сеансы, определяет динамические назначения порта и разрешает обмен данными на этих портах на время определенных сеансов. Мультимедиа и приложения FTP

показывают этот тип поведения.

Для протокола FTP необходима специальная обработка из-за использования двух портов при каждом сеансе связи по протоколу FTP. При включении протокол FTP использует два порта для передачи данных: контрольный канал и канал данных, использующие соответственно порты 2 и 20. Пользователь, инициирующий сеанс FTP по контрольному каналу, отправляет все запросы данных по этому каналу. После этого FTP-сервер инициирует запрос на открытие порта с 20 порта сервера на компьютер пользователя. Протокол FTP всегда использует порт 20 для передачи данных по каналу данных. Если проверка FTP не была включена для Security Appliance, этот запрос отвергается и при сеансах связи по протоколу FTP не выполняется передача запрошенных данных. Если проверка FTP включена для Security Appliance, то Security Appliance отслеживает контрольный канал и пытается распознать запрос на открытие канала данных. Протокол FTP встраивает спецификации порта канала данных в трафик контрольного канала, после чего Security Appliance выполняет проверку контрольного канала на наличие изменений порта данных. Если Security Appliance распознает запрос, он создает временную область для трафика канала данных, которая существует, пока выполняется сеанс связи. При этом режиме работы функция проверки FTP выполняет мониторинг контрольного канала, определяет назначения портов данных и обеспечивает возможность передачи данных для порта данных на протяжении сеанса связи.

Security Appliance по умолчанию проверяет подключения с использованием порта 21 для трафика FTP с помощью команды global-inspection class-map. Security Appliance также распознает различие между активными и пассивными сеансами связи по протоколу FTP. **Если сеансы связи по протоколу FTP поддерживают пассивный режим передачи данных, Security Appliance с помощью команды inspect ftp распознает запрос порта данных от пользователя и открывает новый порт данных, значение которого больше 1023.**

Функция проверки приложений FTP проверяет сеансы связи по протоколу FTP и выполняет четыре задачи:

- Подготавливает динамическое подключение по второму каналу
- Отслеживает последовательность команд и откликов FTP
- Генерирует след аудита
- Преобразовывает встроенные IP-адреса с помощью NAT

Проверка приложений FTP подготавливает дополнительные каналы для передачи данных по протоколу FTP. Каналы выделяются как отклик на загрузку и выгрузку файлов, или событие отображения списка каталогов; при этом каналы должны быть заранее согласованы. **Порт согласовывается с помощью команды PORT или PASV маршрутизатора 227.**

Tftp

Проверка TFTP по умолчанию включена.

Устройство защиты проверяет трафик TFTP и при необходимости динамически создает подключения и преобразования для поддержки передачи данных между клиентом и сервером TFTP. В частности инспекционный механизм осматривает запросы чтения TFTP (RRQ), запишите запросы (WRQ) и уведомления об ошибке (ОШИБКА).

Динамический дополнительный канал и трансляция PAT, при необходимости, выделены на приеме допустимого RRQ или WRQ. Этот дополнительный канал впоследствии

используется TFTP для передачи файла или уведомления об ошибке.

Только TFTP-сервер может инициировать передачу трафика по дополнительному каналу и в большинстве случаев между клиентом и сервером TFTP может существовать только один неполный канал. Уведомление об ошибке от сервера закрывает дополнительный канал.

Если статический PAT используется для перенаправления трафика TFTP, необходимо включить проверку TFTP.

Конфигурация базовой проверки приложений FTP

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. Можно только применить одну глобальную политику, поэтому если вы хотите изменить глобальную политику, например, применить контроль к нестандартным портам или добавить проверки, которые не включены по умолчанию, необходимо или отредактировать политику по умолчанию или отключить ее и применить новую. Полный список всех портов по умолчанию см. в разделе Политика проверок по умолчанию.

1. **Введите policy-map global_policy.**`ASAwAIP-CLI(config)#policy-map global_policy`
2. **Введите class inspection_default.**`ASAwAIP-CLI(config-pmap)#class inspection_default`
3. **Введите inspect FTP.**`ASAwAIP-CLI(config-pmap-c)#inspect FTP` **Поддерживается возможность использования команды inspect FTP strict.** Эта команда увеличивает безопасность защищенных сетей за счет предотвращения отправки веб-браузером встроенных команд по FTP-запросам.*После включения для интерфейса параметра strict, проверка FTP принудительно активирует следующую реакцию на событие:*Команда FTP должна быть подтверждена, прежде чем Устройство безопасности позволяет новую команду.Security Appliance сбрасывает подключение, отправляющее встроенные команды.**227** и команды **PORT** проверены, чтобы гарантировать, что они не появляются в строке с ошибкой.**% Warning:** *Использование параметра strict может привести к сбою в работе FTP-клиентов, которые не полностью соответствуют RFC для FTP.* См. Использование параметра strict для получения дополнительных сведений об использовании параметра strict.

Пример конфигурации

Имя устройства 1
ASA-AIP-CLI(config)#**show running-config** ASA Version 7.2(2) ! hostname ASA-AIP-CLI domain-name corp.com enable password WwXYvtKrnjXqGbu1 encrypted names ! interface Ethernet0/0 nameif Outside security-level 0 ip address 192.168.1.2 255.255.255.0 ! interface Ethernet0/1 nameif Inside security-level 100 ip address 10.1.1.1 255.255.255.0 ! interface Ethernet0/2 nameif DMZ security-level 50 ip address 172.16.1.12 255.255.255.0 ! interface Ethernet0/3 no nameif no security-level no ip address ! interface Management0/0 no nameif no security-level no ip address ! *!--- Output is suppressed. !--- Permit inbound FTP control traffic.* **access-list 100 extended permit tcp any host 192.168.1.5**

```
eq ftp !--- Permit inbound FTP data traffic. access-list
100 extended permit tcp any host 192.168.1.5 eq ftp-data
! !--- Command to redirect the FTP traffic received on
IP 192.168.1.5 !--- to IP 172.16.1.5. static
(DMZ,outside) 192.168.1.5 172.16.1.5 netmask
255.255.255.255 access-group 100 in interface outside
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 ! !---
This command tells the device to !--- use the
"global_policy" policy-map on all interfaces. service-
policy global_policy global prompt hostname context
Cryptochecksum:4b2f54134e685d11b274ee159e5ed009 : end
ASA-AIP-CLI(config)#
```

Настройте контроль протокола FTP на нестандартном порте TCP

Можно настроить Контроль Протокола FTP для нестандартных портов TCP с этими строками настройки (замените XXXX новым номером порта):

```
access-list ftp-list extended permit tcp any any eq XXXX
!
class-map ftp-class
  match access-list ftp-list
!
policy-map global_policy
  class ftp-class
   inspect ftp
```

Настройте основной контроль приложения TFTP

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 вы хотите изменить глобальную политику, например, применить контроль к нестандартным портам или добавить проверки, которые не включены по умолчанию, необходимо или отредактировать политику по умолчанию или отключить ее и применить новую. Полный список всех портов по умолчанию см. в разделе Политика проверок по умолчанию.

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

Пример конфигурации

Имя устройства 1
`ASA-AIP-CLI(config)#`**`show running-config`** `ASA Version`

```
7.2(2) ! hostname ASA-AIP-CLI domain-name corp.com
enable password WwXYvtKrnjXqGbu1 encrypted names !
interface Ethernet0/0 nameif Outside security-level 0 ip
address 192.168.1.2 255.255.255.0 ! interface
Ethernet0/1 nameif Inside security-level 100 ip address
10.1.1.1 255.255.255.0 ! interface Ethernet0/2 nameif
DMZ security-level 50 ip address 172.16.1.12
255.255.255.0 ! interface Ethernet0/3 no nameif no
security-level no ip address ! interface Management0/0
no nameif no security-level no ip address ! !--- Output
is suppressed. !--- Permit inbound TFTP traffic. access-
list 100 extended permit udp any host 192.168.1.5 eq
tftp ! !--- Command to redirect the TFTP traffic
received on IP 192.168.1.5 !--- to IP 172.16.1.5. static
(DMZ,outside) 192.168.1.5 172.16.1.5 netmask
255.255.255.255 access-group 100 in interface outside
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 ! !---
This command tells the device to !--- use the
"global_policy" policy-map on all interfaces. service-
policy global_policy global prompt hostname context
Cryptochecksum:4b2f54134e685d11b274ee159e5ed009 : end
ASA-AIP-CLI(config)#
```

Проверка

Чтобы убедиться в успешном завершении конфигурации, воспользуйтесь командой show service-policy и ограничьте использование выходных данных только для проверки FTP с помощью команды show service-policy inspect ftp.

Устранение неполадок

Проблема: Синтаксис в Конфигурации Не Работает, и Ошибка контроля class-map Получена

В конфигурации представлен неправильный синтаксис и была получена такая ошибка, как эта:

```
ERROR: % class-map inspection_default not configured
```

Решение

Конфигурация зависит от проверок, заданных по умолчанию в конфигурации. Если они не находятся в конфигурации, воссоздают их с этими командами:

1. class-map inspection_defaultmatch default-inspection-traffic
2. dns policy-map type inspect preset_dns_map параметрыmessage-length maximum 512
3. !--- карту политик global_policyclass inspection_defaultinspect dns preset_dns_mapinspect ftp inspect h323 h225inspect h323 rasinspect rshinspect rtspinspect esmtpinspect

sqlnetinspect skinnyinspect sunrpcinspect xdmcpinspect sipinspect netbiosinspect tftp

4. service-policy global_policy global

% Warning: Если бы проверки по умолчанию были ранее удалены для решения другой проблемы, то та проблема могла бы возвратиться, когда реактивируют проверкам по умолчанию. Вы или ваш администратор должны знать, были ли проверки по умолчанию удалены ранее как действие по устранению проблем.

Неспособный выполнить FTPS (FTP по SSL) через ASA

FTP с TLS/SSL (SFTP / FTPS) не поддерживается через Устройство безопасности. FTP - соединение зашифрован, таким образом, нет никакого способа, которым межсетевой экран в состоянии дешифровать пакет. См. PIX/ASA: часто задаваемые вопросы Устройства безопасности для получения дополнительной информации.

Дополнительные сведения

- Устройства адаптивной безопасности серии 5500 ASA
- Справочник по командам устройства защиты Cisco
- Устройство защиты PIX 500 Series
- Информационные сообщения Cisco Security и предупреждения
- Cisco Systems – техническая поддержка и документация