ASA/PIX: Транзитный трафик, составляющий клиенты VPN Использование примера конфигурации AcS

Содержание

Введение

Этот документ предоставляет пример конфигурации для того, чтобы Составлять Клиенты VPN (IPsec/SSL) с помощью PIX/ASA с ACS. Устройство адаптивной безопасности может передать учетную информацию к RADIUS или TACACS + сервер о любом Трафике TCP или трафике UDP, который проходит через устройство адаптивной безопасности. Если тот трафик также аутентифицируется, то AAA-сервер может поддержать учетную информацию именем пользователя. Если трафик не аутентифицируется, AAA-сервер может поддержать учетную информацию IP-адресом. Учетная информация включает, когда сеансы запускаются и останавливаются, имя пользователя, количество байтов, которые проходят через устройство адаптивной безопасности для сеанса, сервис, используемый, и продолжительность каждого сеанса.

Прежде чем можно будет использовать эту команду, необходимо сначала определять AAA-сервер с **командой aaa-server**. Учетная информация передается только активному серверу в группе серверов, пока вы не включаете одновременный учет с помощью **команды accounting-mode** в режиме конфигурации протокола aaa-server.

Вы не можете использовать команду **совпадения данных учета AAA (проверка подлинности, авторизация и учет)** в одинаковой конфигурации как **команды aaa accounting включает и exclude**. Мы предлагаем, чтобы вы использовали команду **соответствия** вместо **того, чтобы включать** и **команды exclude**; **включать** и **команды exclude** не поддерживаются ASDM.

Этот документ предполагает, что VPN для удаленного доступа с помощью ASA/PIX с VPN-

клиентом IPSec / VPN-КЛИЕНТ SSL (SVC) (Anyconnect) конфигурация с ACS для аутентификации уже сделана и работает должным образом. Этот документ фокусируется о том, как настроить Учет AAA для Клиентов VPN на Устройстве обеспечения безопасности ASA с ACS.

См. PIX/ASA 7.x и Cisco VPN Client 4.x для Примера Конфигурации аутентификации Cisco Secure ACS, чтобы узнать больше, как установить соединение VPN для удаленного доступа между Cisco VPN Client (4.x для Windows) и устройством защиты PIX 500 Series 7.x использование сервера Cisco Secure Access Control Server (Версия ACS 3.2) для расширенной проверки подлинности (XAUTH).

См. ASA 8. x: Клиент AnyConnect VPN Client для VPN Общедоступного Интернета на Примере конфигурации Палки, чтобы узнать больше, как установить Устройство адаптивной защиты (ASA) 8.0.2 для выполнения VPN SSL на палке с Cisco AnyConnect VPN Client.

Предварительные условия

Требования

Удостоверьтесь, что клиент VPN в состоянии установить соединение и достигнуть End to End должным образом.

Используемые компоненты

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

- Серия 5500 Cisco ASA, которая выполняется 7.x и позже
- Cisco Secure ACS 4. 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

Этот документ может также использоваться с устройством защиты Cisco PIX серии 500 с Версией программного обеспечения 7.x и позже.

Условные обозначения

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

Настройка

Конфигурация ASA

Для настройки учета выполните эти шаги:

1. Если вы хотите, чтобы устройство адаптивной безопасности предоставило учетные данные на пользователя, необходимо включить аутентификацию. Если вы хотите, чтобы устройство адаптивной безопасности предоставило учетные данные на IP-адрес, разрешение аутентификации не необходимо, и можно продолжить к шагу 2.
2. Использование **команды access-list**, создайте список доступа, который определяет адреса источника и адреса назначения (DA) трафика, который вы хотите считавший.**Примечание:** Если вы настроили аутентификацию и хотите учетные данные для всего аутентифицируемого трафика, можно использовать тот же список доступа, который вы создали для использования с **командой aaa authentication match**.
3. Чтобы позволить считать, введите эту команду:`hostname(config)# **aaa accounting match** *acl_name interface_name server_group*` Где:Аргумент *acl_name* является набором названия списка доступа в **команде access-list**.*interface_name* аргумент является набором имени интерфейса в **команде nameif**.*server_group* аргумент является набором имени серверной группы в **команде aaa-server**.**Примечание:** Также можно использовать **команду aaa accounting include** (который определяет трафик в рамках команды), но вы не можете использовать оба метода в одинаковой конфигурации. Посмотрите Справочник по командам многофункционального устройства защиты Cisco ASA серии 5580 для получения дополнительной информации.

Эти команды аутентифицируют, авторизуют и составляют исходящий трафик:

ASA

```
!--- Using the aaa-server command, identify your AAA
servers. If you have already !--- identified your AAA
servers, continue to the next step. hostname(config)#
aaa-server AuthOutbound protocol RADIUS hostname(config-
aaa-server-group)# exit !--- Identify the server,
including the AAA server group it belongs to and !---
enter the IP address, Shared key of the AAA Server.
hostname(config)# aaa-server AuthOutbound (inside) host
10.1.1.1 hostname(config-aaa-server-host)# key
TACPlusUauthKey hostname(config-aaa-server-host)# exit
!--- Using the access-list command, create an access
list that identifies the source !--- addresses
anddestination addresses of traffic you want to
authenticate. hostname(config)# access-list TELNET_AUTH
extended permit tcp any any eq telnet !--- Using the
access-list command, create an access list that
identifies the source !--- addresses anddestination
addresses of traffic you want to Authorize and
Accounting. hostname(config)# access-list SERVER_AUTH
extended permit tcp any any !--- configure
authentication, enter this command: hostname(config)#
aaa authentication match TELNET_AUTH inside AuthOutbound
!--- configure authorization, enter this command:
hostname(config)# aaa authorization match SERVER_AUTH
inside AuthOutbound
!--- This command causes the PIX Firewall to send !---
RADIUS accounting packets for RADIUS-authenticated
outbound sessions to the AAA !--- server group named
"AuthOutbound": hostname(config)# aaa accounting match
SERVER_AUTH inside AuthOutbound
```

RADIUS Accounting Использование конфигурации AcS

Регистратор CSV делает запись данных для регистрации атрибутов в столбцах, разделенных запятыми (). Можно импортировать этот формат во множество сторонних приложений, таких как Microsoft Excel или Microsoft Access. После импорта данных из Файла csv в такие приложения можно подготовить диаграммы или выполнить запросы, такие как определение, сколько часов пользователь был зарегистрирован в сеть во время установленного срока. Для получения информации о том, как использовать Файл csv в стороннем приложении, таком как Microsoft Excel, см. документацию от стороннего поставщика.

Можно обратиться к Файлам csv на жестком диске сервера ACS, или можно загрузить Файл csv от веб-интерфейса.

По умолчанию ACS поддерживает файлы журнала в каталогах, которые уникальны для журнала. Можно настроить размещение файла журнала журналов CSV. Каталоги по умолчанию для всех журналов находятся в **sysdrive:\Program Files\CiscoSecure ACS vx. x.**

Для настройки CiscoSecure ACS, чтобы выполнить учет RADIUS с помощью CSV, выполнить эти шаги:

1. **На панели переходов нажмите "System Configuration (Настройка системы)".**
2. **Нажмите Logging.** Страница Logging Configuration появляется.
3. Выберите **CSV RADIUS Accounting**.
4. Подтвердите, что выбран **Журнал к** флажку **отчёта о RADIUS Accounting CSV**. Если это не выбрано, выберите его теперь.
5. В **Выбрать** таблице **Attributes To Log** удостоверьтесь, что атрибуты RADIUS, которые вы хотите видеть в журнале учета RADIUS, появляются в **Зарегистрированном** списке **Атрибутов**. В дополнение к стандартным атрибутам RADIUS существует несколько специальных атрибутов регистрации, предоставленных CiscoSecure ACS, таких как Настоящее имя, Информация ExtDB, и Зарегистрированы Удаленно.
6. (Необязательно) при использовании Сервера CiscoSecure ACS для Windows можно задать управление файла журнала, которое определяет, как большие файлы учетной записи RADIUS могут быть, сколько сохранено, как долго, и где они сохранены.
7. При внесении изменений в RADIUS бухгалтерской конфигурацией нажмите **Submit**. CiscoSecure ACS сохраняет и внедряет изменения, вы сделали к его RADIUS бухгалтерскую конфигурацию.

Эти темы описывают, как просмотреть и загрузить отчёты о CSV ACS:

- Названия файла журнала CSV
- Просматривание отчета о CSV
- Загрузка отчёта о CSV

Проверка

В настоящее время для этой конфигурации нет процедуры проверки.

Устранение неполадок

Для этой конфигурации в настоящее время нет сведений об устранении проблем.

Дополнительные сведения

- Руководство пользователя для сервера Cisco Secure Access Control Server 4.2 - Регистрация и отчёты
- Страница поддержки устройств адаптивной безопасности Cisco ASA серии 5500
- PIX/ASA: Пример настройки сетевого доступа через Cut-through прокси с использованием серверов проверки подлинности TACACS+ и RADIUS
- Cisco Secure Access Control Server for Windows
- Cisco PIX 500 Series Security Appliances
- Cisco Systems – техническая поддержка и документация