Настройка концентратора Cisco VPN 3000 для блокирования с помощью фильтров и назначение фильтра RADIUS

Содержание

Введение

В этом примере конфигурации мы хотим использовать фильтры, чтобы позволить пользователю обращаться только к одному серверу (10.1.1.2) внутренняя часть сеть и блокировать доступ ко всем другим ресурсам. Cisco VPN 3000 Concentrator может быть установлен для управления IPsec, Протоколом PPTP и доступом клиента L2TP к сетевым ресурсам с фильтрами. Фильтры состоят из правил, которые подобны спискам доступа на маршрутизаторе. Если маршрутизатор был настроен для:

```
access-list 101 permit ip any host 10.1.1.2
access-list 101 deny ip any any
```

эквивалентный Концентратор VPN должен был бы установить фильтр с правилами.

Наше первое правило Концентратора VPN является **permit_server_rule**, который эквивалентен **команде permit ip any host 10.1.1.2** маршрутизатора. Наше второе правило Концентратора VPN является **deny_server_rule**, который эквивалентен **команде deny ip any any** маршрутизатора.

Наш фильтр Концентратора VPN является **filter_with_2_rules**, который эквивалентен списку доступа маршрутизатора 101; это использует **permit_server_rule** и **deny_server_rule** (в том заказе). Предполагается, что клиенты могут соединиться должным образом до добавления фильтров; они получают свои IP-адреса от пула на Концентраторе VPN.

См. PIX/ASA 7.x ASDM: Ограничьте Доступ к сети Пользователей VPN для удаленного доступа для узнавания больше о сценарии, где PIX/ASA 7.x блокирует доступ от пользователей VPN.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Сведения в этом документе основываются на версии 2.5.2. D Cisco VPN 3000 Concentrator.

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:

Условные обозначения

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

Конфигурация VPN 3000

Для настройки VPN-концентратора 3000 выполните следующие действия.

1. Выберите **Configuration> Policy Management> Traffic Management> Rules> Add** и определите первое правило Концентратора VPN, названное **permit_server_rule** с этими параметрами настройки:Направление — **Входящий**Действие — **Вперед**Исходный адресАдрес назначения (DA) — **10.1.1.2**Маска подстановочного знака — **0.0.0.0**
2. В той же области определите второе правило Концентратора VPN, названное **deny_server_rule** с этими настройками по умолчанию:Направление — **Входящий**Действие — **Отбрасывание**Адреса источника и назначения чего-либо (255.255.255.255):
3. Выберите **Configuration> Policy Management> Traffic Management> Filters** и добавьте свой фильтр **filter_with_2_rules**.
4. Добавьте два правила к filter_with_2_rules:
5. **Choose Configuration> User Management> Groups** и применяет фильтр к группе:

Фильтры для туннеля VPN между локальными сетями

От 3.6 и позднее кода Концентратора VPN вы можете трафик фильтрации для каждого VPN-туннеля IPSec LAN-LAN. Например, если вы создаете туннель между локальными сетями (LAN-to-LAN) к другому Концентратору VPN с адресом 172.16.1.1 и хотите разрешить доступ хоста 10.1.1.2 к туннелю при запрете всего другого трафика можно применить **filter_with_2_rules**, когда вы выбираете **Configuration> System> Tunneling Protocols> IPSec> LAN-to-LAN> Modify** и выбираете **filter_with_2_rules** под **Фильтром**.

Конфигурация VPN 3000 - назначение фильтра RADIUS

Также возможно определить фильтр в Концентраторе VPN и затем передать filter number от сервера RADIUS (в сроках RADIUS, для приписывания 11, Filter-Id), так, чтобы, когда пользователь аутентифицируется на сервере RADIUS, Filter-Id был привязан к тому соединению. В данном примере предположение - то, что Проверка подлинности RADIUS для пользователей Концентратора VPN уже в рабочем состоянии, и только Filter-Id должен быть добавлен.

Определите фильтр на Концентраторе VPN как в предыдущем примере:

Конфигурация сервера CSNT — назначение фильтра RADIUS

Настройте атрибут 11, Filter-Id на сервере Cisco Secure NT, чтобы быть **101**:

Отладка - назначение фильтра RADIUS

Если AUTHDECODE (Степени серьезности ошибки 1-13) идет в Концентраторе VPN, журнал показывает, что сервер Cisco Secure NT передает вниз access-list 101 в атрибуте 11 (0x0B):

```
207 01/24/2001 11:27:58.100 SEV=13 AUTHDECODE/0 RPT=228
0000: 020C002B 768825C5 C29E439F 4C8A727A     ...+v.%...C.L.rz
0010: EA7606C5 06060000 00020706 00000001     .v..............
0020: 0B053130 310806FF FFFFFF                   ..101......
```

Проверка

В настоящее время для этой конфигурации нет процедуры проверки.

Устранение неполадок

Когда вы выбираете **Configuration> System> Events> Classes** и добавляете класс **FILTERDBG** со **Степенями серьезности ошибки для Регистрации = 13,** для целей устранения проблем только, можно включить отладку фильтра. В правилах измените Действие по умолчанию от Форварда (или Отбрасывание), чтобы **Передать и Регистрировать** (или Отбрасывание и Журнал). Когда журнал событий получен в **Monitoring> Event Log**, он должен show entry, такой как:

```
221 12/21/2000 14:20:17.190 SEV=9 FILTERDBG/1 RPT=62
Deny In: intf 1038, ICMP, Src 10.99.99.1, Dest 10.1.1.3, Type 8

222 12/21/2000 14:20:18.690 SEV=9 FILTERDBG/1 RPT=63
```

```
Deny In: intf 1038, ICMP, Src 10.99.99.1, Dest 10.1.1.3, Type 8
```

Дополнительные сведения

- Согласование IPsec/Протоколы IKE
- Часто задаваемые вопросы VPN 3000 Concentrator
- Поддержка RADIUS
- Поддержка Cisco VPN 3000 Concentrator
- Поддержка Cisco VPN 3000 Client
- Поддержка Cisco Secure ACS для Windows
- Запрос на комментарии (RFC)
- Cisco Systems – техническая поддержка и документация