ASA 8. X: Позвольте пользовательскому приложению работать с восстановлением VPN-туннеля L2L

Содержание

Введение
Предварительные условия
Требования
Используемые компоненты
Условные обозначения
Настройка
Схема сети
Подробные данные совместимости для этой Функции
Конфигурации
Активируйте эту Опцию
Проверка
Устранение неполадок
Обнулите значение срока действия IKE
Сообщение об ошибках, когда Туннельные Отбрасывания
Как эта Функция Не соглашается с Опцией reclassify-vpn
Дополнительные сведения

Введение

Этот документ предоставляет сведения о Туннелировавшей функции Потоков Персистентного IPSec и как сохранить поток TCP по разрушению VPN-туннеля.

Предварительные условия

Требования

У читателей данной документации должно быть основное понимание того, как работает VPN. Дополнительные сведения см. в следующих документах:

- Типовая конфигурация VPN L2L
- VPN L2L с ASA

Используемые компоненты

Сведения в этом документе основываются на устройстве адаптивной защиты Cisco (ASA) с версией 8.2 и позже.

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.

Условные обозначения

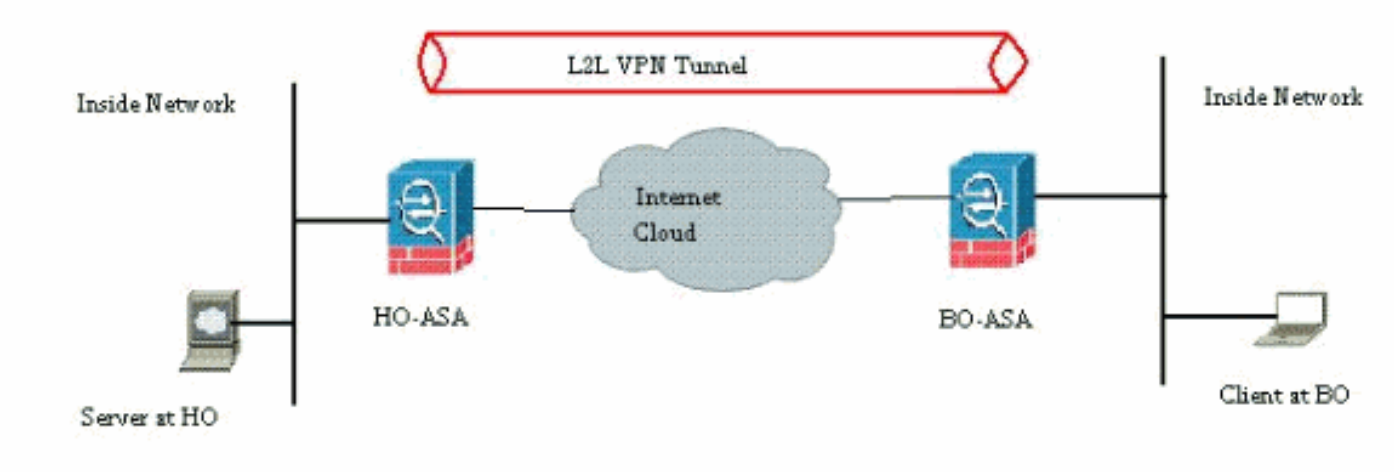
Более подробную информацию о применяемых в документе обозначениях см. в описании условных обозначений, используемых в технической документации Cisco.

Настройка

Как показано в схеме сети, филиал компании (BO) связан с головным офисом (HO) через сквозное VPN-соединение. Рассмотрите конечного пользователя в филиале компании, пытающемся загружать большой файл от сервера, расположенного в головном офисе. Загрузка длится часы. Передача файла хорошо работает, пока VPN не хорошо работает. Однако, когда VPN разрушена, передача файла "зависнута", и пользователь должен повторно инициировать запрос передачи файла снова с начала после того, как установлен туннель.

Схема сети

В настоящем документе используется следующая схема сети:



Эта проблема возникает из-за встроенной функциональности о том, как работает ASA. ASA контролирует каждое соединение, которое проходит через него и поддерживает запись в ее таблице состояний согласно функции контроля приложения. Подробные данные зашифрованного потока данных, которые проходят через VPN, поддержаны в форме базы данных сопоставления безопасности (SA). Для сценария этого документа это поддерживает два других трафика. Каждый - зашифрованный поток данных между Шлюзами VPN, и другой трафик между Сервером в головном офисе и конечным пользователем в филиале компании. Когда VPN завершена, подробные данные потока для этого определенного SA удалены. Однако запись таблицы состояний, поддержанная ASA для этого TCP - подключения, становится устаревшей ни из-за какого действия, которое препятствует загрузке. Это означает, что ASA все еще сохранит TCP - подключение для того отдельного

потока, в то время как завершается пользовательское приложение. Однако TCP - подключения станут случайными и в конечном счете таймаут после того, как истечет таймер простоя TCP.

Эта проблема была решена путем представления функции под названием Туннелировавшие Потоки Персистентного IPSec. Новая команда была интегрирована в Cisco ASA для сохранения информации о таблице состояний на пересмотре VPN-туннеля. Команду показывают здесь:

```
sysopt connection preserve-vpn-flows
```

По умолчанию эта команда отключена. Путем включения этого Cisco ASA поддержит сведения таблицы состояния TCP, когда VPN L2L восстановится с разрушения, и восстановите туннель.

В этом сценарии эта команда должна быть выполнена на обоих концах туннеля. Если это - устройство не марки CISCO с другой стороны, выполнение этой команды на Cisco ASA должно быть достаточным. Если команда выполнена, когда туннели были уже активны, туннели должны быть очищены и восстановлены для этой команды для вступления в силу. Для получения дополнительной информации при очистке и восстановлении туннелей, обратитесь для Очистки Сопоставлений безопасности.

Подробные данные совместимости для этой Функции

Эта функция была представлена в версии программного обеспечения 8.0.4 Cisco ASA и позже. Это поддерживается только для этих типов VPN:

- LAN в туннели LAN
- Туннели удаленного доступа в режиме расширения сети (NEM)

Эта функция не поддерживается для этих типов VPN:

- Туннели удаленного доступа IPSec в клиентском режиме
- AnyConnect или VPN-туннели SSL

Эта функция не существует на этих платформах:

- PIX Cisco с версией программного обеспечения 6.0
- Концентраторы Cisco VPN
- Платформы Cisco IOS®

Активация этой опции не создает дополнительной перегрузки на внутренней Обработке ЦПУ ASA, потому что это переходит, поддерживают те же TCP - подключения, которые имеет устройство, когда туннель подключен.

Примечание: Эта команда применима для TCP - подключений только. Это не имеет никакого эффекта на трафик UDP. UDP - подключения будут таймаут согласно настроенному периоду ожидания.

Конфигурации

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

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

В данном документе используется следующая конфигурация:

- Cisco ASA

Это - типовые выходные данные рабочей конфигурации межсетевого экрана Cisco ASA в одном конце VPN-туннеля:

Cisco ASA

```
ASA Version 8.2(1)
!
hostname CiscoASA
domain-name example.com
enable password <removed>
passwd <removed>
names
!
interface Ethernet0/0
 speed 100
 duplex full
 nameif outside
 security-level 0
 ip address 209.165.201.2 255.255.255.248
!
interface Ethernet0/1
 nameif inside
 security-level 100
 ip address 10.224.9.5 255.255.255.0
!
interface Ethernet0/2
 shutdown
 no nameif
 no security-level
 no ip address
!
!
interface Management0/0
 nameif management
 security-level 100
 ip address 10.224.14.10 255.255.255.0
!
boot system disk0:/asa822-k8.bin
ftp mode passive
 !---Output Suppressed ! access-list test extended
permit ip 10.224.228.0 255.255.255.128 any access-list
test extended permit ip 10.224.52.0 255.255.255.128 any
access-list 100 extended permit ip 10.224.228.0
255.255.255.128 any access-list 100 extended permit ip
10.224.52.0 255.255.255.128 any access-list
inside_access_out extended permit ip any 10.224.228.0
255.255.255.1 ! !---Output Suppressed global (outside) 1
interface nat (inside) 0 access-list test nat (inside) 1
10.224.10.0 255.255.255.0 ! !---Output Suppressed route
inside 10.0.0.0 255.0.0.0 10.224.9.1 1 route outside
0.0.0.0 255.255.255.255 209.165.201.1 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 sip-provisional-media 0:02:00
uauth 0:05:00 absolute timeout tcp-proxy-reassembly
```

```
0:01:00 dynamic-access-policy-record DfltAccessPolicy !
!---Output Suppressed http server idle-timeout 40 http
10.224.3.0 255.255.255.0 management http 0.0.0.0 0.0.0.0
inside ! snmp-server enable traps snmp authentication
linkup linkdown coldstart ! !--- To preserve and resume
stateful (TCP) tunneled IPsec LAN-to-LAN traffic within
the timeout period after the tunnel drops and recovers.
sysopt connection preserve-vpn-flows service
resetoutside ! crypto ipsec transform-set ESP-AES-256-
MD5 esp-aes-256 esp-md5-hmac crypto ipsec transform-set
testSET esp-3des esp-md5-hmac crypto map map1 5 match
address 100 crypto map map1 5 set peer 209.165.200.10
crypto map map1 5 set transform-set testSET crypto map
map1 interface outside crypto isakmp enable outside
crypto isakmp policy 5 authentication pre-share
encryption 3des hash sha group 2 lifetime 86400 crypto
isakmp policy 10 authentication pre-share encryption des
hash sha group 2 lifetime 86400 !---Output Suppressed !
telnet timeout 5 ssh timeout 5 console timeout 0 threat-
detection basic-threat threat-detection statistics
access-list ! !---Output Suppressed ! tunnel-group
209.165.200.10 type ipsec-l2l tunnel-group
209.165.200.10 ipsec-attributes pre-shared-key * !---
Output Suppressed 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 rsh inspect rtsp inspect esmtp
inspect sqlnet inspect skinny inspect sunrpc inspect
xdmcp inspect sip inspect netbios inspect tftp !
service-policy global_policy global prompt hostname
state Cryptochecksum:5c228e7131c169f913ac8198ecf8427e :
end
```

Активируйте эту Опцию

По умолчанию эта опция отключена. Это может быть включено при помощи этой команды в CLI ASA:

```
CiscoASA(config)#sysopt connection preserve-vpn-flows
```

Это может быть просмотрено при помощи этой команды:

```
CiscoASA(config)#show run all sysopt no sysopt connection timewait sysopt connection tcpmss 1380
sysopt connection tcpmss minimum 0 sysopt connection permit-vpn sysopt connection reclassify-vpn
sysopt connection preserve-vpn-flows no sysopt nodnsalias inbound no sysopt nodnsalias outbound
no sysopt radius ignore-secret no sysopt noproxyarp outside
```

При использовании ASDM эта опция может быть активирована следующим этот путь:

Конфигурация> VPN для удаленного доступа> сетевой доступ (клиент)> Усовершенствованный> IPsec> Параметры системы.

Затем проверьте *Заповедник потоки VPN с отслеживанием состояния, когда туннель понизится для* опции *Режима расширения сети (NEM)*.

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.**

- **подробность покажите контекст vpn таблицы гадюки** — Показывает содержание контекста VPN ускоренного пути безопасности, который мог бы помочь вам устранять проблему. Ниже приводится пример выходных данных от **команды show asp table vpn-context**, когда персистентный IPSec туннелировал, опция потоков активирована. Обратите внимание на то, что это содержит определенный флаг **PRESERVE**.
```
CiscoASA(config)#show asp table vpn-context VPN CTX=0x0005FF54, Ptr=0x6DE62DA0,
DECR+ESP+PRESERVE, UP, pk=0000000000, rk=0000000000, gc=0 VPN CTX=0x0005B234,
Ptr=0x6DE635E0, ENCR+ESP+PRESERVE, UP, pk=0000000000, rk=0000000000, gc=0
```

Устранение неполадок

В этом разделе определенные обходные пути представлены для предотвращения переброски туннелей. За и против обходных путей также детализированы.

Обнулите значение срока действия IKE

Можно заставить VPN-туннель остаться в живых в течение бесконечного времени, но не пересмотреть, путем хранения значения Срока действия IKE как нуля. Информация о SA сохранена узлами VPN, пока не истекает срок действия. Путем присвоения значения как нуля можно сделать этот сеанс IKE в последний раз навсегда. Через это можно избежать неустойчивых проблем разъединения потока во время смены ключа туннеля. Это может быть сделано с этой командой:

```
CiscoASA(config)#crypto isakmp policy 50 lifetime 0
```

Однако это имеет определенный недостаток с точки зрения заключения компромисса уровня безопасности VPN-туннеля. Смена ключа сеанса IKE в интервалах заданного времени предоставляет больше безопасности VPN-туннелю с точки зрения модифицированных ключей шифрования каждый раз, когда и для любого злоумышленника становится трудным декодировать информацию.

Примечание: Отключение Срока действия IKE не означает, что туннель не повторно вводит вообще. Однако, КОНТЕКСТ БЕЗОПАСНОСТИ IPSEC повторно введет в указанном временном интервале, потому что это не может быть обнулено. Минимальное пожизненное значение обеспечило КОНТЕКСТ БЕЗОПАСНОСТИ IPSEC, 120 секунд, и максимум составляет 214783647 секунд. Для получения дополнительной информации об этом, обратитесь к сроку действия КОНТЕКСТА БЕЗОПАСНОСТИ IPSEC.

Сообщение об ошибках, когда Туннельные Отбрасывания

Когда эта функция не использована в конфигурации, Cisco ASA возвращает это сообщение журнала, когда разрушен VPN-туннель:

```
%ASA-6-302014: Teardown TCP connection 57983 for outside:XX.XX.XX.XX/80 to
inside:10.0.0.100/1135 duration 0:00:36 bytes 53947 Tunnel has been torn down
```

Вы видите, что причина состоит в том, что **был разъединен Туннель**.

Примечание: Регистрации уровня 6 нужно позволить видеть это сообщение.

Как эта Функция Не соглашается с Опцией reclassify-vpn

Когда туннель возвращается, опция потока vpn заповедника используется. Это позволяет предыдущему потоку TCP оставаться открытым поэтому, когда туннель возвращается, тот же поток может использоваться.

Когда **команда sysopt connection reclassify-vpn** используется, она очищает любой предыдущий поток, который принадлежит туннельному трафику и классифицирует поток для прохождения через туннеля. Опция reclassify-vpn используется в ситуации, когда поток TCP был уже создан, который не отнесенная VPN. Это создает ситуацию, куда трафик не течет через туннель после того, как установлена VPN. Для получения дополнительной информации об этом, обратитесь к реклассифицировать-vpn sysopt.

Дополнительные сведения

- Узел к VPN узла (L2L) с ASA
- Страница документации Cisco ASA
- Cisco Systems – техническая поддержка и документация