Клиент AnyConnect VPN Client на маршрутизаторе IOS с зоной IOS базирующийся пример конфигурации межсетевого экрана политики

Содержание

Введение

В Выпуске 12.4 (20) T программного обеспечения Cisco IOS и позже, виртуальный интерфейс SSLVPN-VIF0 был представлен для соединений Клиента AnyConnect VPN Client. Однако этот интерфейс SSLVPN-VIF0 является внутренним интерфейсом, не поддерживающим пользовательские конфигурации. Это создало проблему с VPN AnyConnect и Зональным Базирующимся Межсетевым экраном Политики, так как с межсетевым экраном, трафик может только течь между двумя интерфейсами, когда оба интерфейса принадлежат зонам безопасности. Так как пользователь не может настроить интерфейс SSLVPN-VIF0 для создания его зональным участником, трафик клиента VPN завершенный на Шлюзе WebVPN Cisco IOS после того, как расшифровка не сможет быть передана никакому другому интерфейсу, принадлежащему зоне безопасности. Признак этой проблемы может быть замечен с этим сообщением журнала, о котором сообщает межсетевой экран:

```
*Mar 4 16:43:18.251: %FW-6-DROP_PKT: Dropping icmp
   session 192.168.1.12:0 192.168.10.1:0 due to One
   of the interfaces not being cfged for zoning
   with ip ident 0
```

Эта проблема была позже решена в более новых выпусках ПО Cisco IOS. С новым кодом пользователь может назначить зону безопасности на виртуальный интерфейс, на который ссылаются под контекстом WebVPN для соединения зоны безопасности к контексту WebVPN.

Предварительные условия

Требования

Для использования преимуществ новой возможности в Cisco IOS необходимо гарантировать, что устройство Шлюза WebVPN Cisco IOS выполняет Cisco IOS Software Release 12.4 (20) T3, программное обеспечение Cisco IOS Release12.4 (22) T2 или программное обеспечение Cisco IOS Release12.4 (24) T1 и позже.

Используемые компоненты

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

- Cisco IOS Расширенная функция безопасности маршрутизатора под управлением версии 15.0 (1) M1 серии 3845 установлена
- Версия VPN-клиента SSL (SVC) AnyConnect Cisco для Windows 2.4.1012

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

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.

Схема сети

В настоящем документе используется следующая схема сети:

Настройте сервер AnyConnect Cisco IOS

Вот действия настройки высокого уровня, которые должны быть выполнены на сервере AnyConnect Cisco IOS, чтобы заставить его взаимодействовать с Зональным Базирующимся Межсетевым экраном Политики. Получающаяся окончательная конфигурация включена для двух типичных сценариев развертывания позже в этом документе.

1. Настройте Интерфейс виртуального шаблона и назначьте его в зоне безопасности для трафика, дешифрованного от Соединения AnyConnect.

2. Добавьте ранее настроенный Виртуальный шаблон к контексту WebVPN для конфигурации AnyConnect.
3. Завершенный остаток WebVPN и Зональной Базирующейся Конфигурации межсетевого экрана Политики.Существует два типичных сценария с AnyConnect и ZBF, и здесь заключительные конфигурации маршрутизатора для каждого сценария.

Сценарий развертывания 1

Трафик VPN принадлежит той же зоне безопасности как внутренняя сеть.

Трафик AnyConnect входит в ту же зону безопасности, что внутренний интерфейс LAN (локальной сети) принадлежит почтовой расшифровке.

Примечание: Сам зона также определена, чтобы только позволить http/трафик HTTPS самому маршрутизатору для ограничения доступа.

Настройка маршрутизатора

```
Router#show run
Building configuration...

Current configuration : 5225 bytes
!
! Last configuration change at 16:25:30 UTC Thu Mar 4
2010 by cisco
!
version 15.0
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
boot-start-marker
boot system flash:
boot-end-marker
!
aaa new-model
!
aaa authentication login default local
aaa authentication login webvpn local
!
aaa session-id common
!
!
ip cef
!
!
ip inspect log drop-pkt
no ip domain lookup
!
!
parameter-map type inspect audit-map
 audit-trail on
 tcp idle-time 20
!
parameter-map type inspect global
!
!
```

```
crypto pki trustpoint TP-self-signed-2692466680
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-2692466680
 revocation-check none
 rsakeypair TP-self-signed-2692466680
!
!
crypto pki certificate chain TP-self-signed-2692466680
 certificate self-signed 01
 <actual certificate deleted here for brevity>
        quit
!
!
username cisco password 0 cisco
!
!
class-map type inspect match-any test
 match protocol tcp
 match protocol udp
 match protocol icmp
class-map type inspect match-all router-access
 match access-group name router-access
!
!
policy-map type inspect firewall-policy
 class type inspect test
  inspect audit-map
 class class-default
  drop
policy-map type inspect out-to-self-policy
 class type inspect router-access
  inspect
 class class-default
  drop
policy-map type inspect self-to-out-policy
 class type inspect test
  inspect
 class class-default
  drop
!
zone security inside
zone security outside
zone-pair security in-out source inside destination
outside
 service-policy type inspect firewall-policy
zone-pair security out-self source outside destination
self
 service-policy type inspect out-to-self-policy
zone-pair security self-out source self destination
outside
 service-policy type inspect self-to-out-policy
!
!
interface Loopback0
 ip address 172.16.1.1 255.255.255.255
!
interface GigabitEthernet0/0
 ip address 192.168.10.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly
 zone-member security inside
!
interface GigabitEthernet0/1
 ip address 209.165.200.230 255.255.255.224
```

```
 ip nat outside
 ip virtual-reassembly
 zone-member security outside
!
interface Virtual-Template1
 ip unnumbered Loopback0
 zone-member security inside
 !
!
ip local pool test 192.168.1.1 192.168.1.100
ip forward-protocol nd
!
ip http server
ip http secure-server
ip nat inside source list 1 interface GigabitEthernet0/1
overload
ip route 0.0.0.0 0.0.0.0 209.165.200.225
!
ip access-list extended router-access
 permit tcp any host 209.165.200.230 eq www
 permit tcp any host 209.165.200.230 eq 443
!
access-list 1 permit 192.168.10.0 0.0.0.255
!
control-plane
 !
!
!
line con 0
 exec-timeout 0 0
 logging synchronous
line aux 0
 modem InOut
 transport input all
line vty 0 4
transport input all
!
exception data-corruption buffer truncate
scheduler allocate 20000 1000
!
webvpn gateway webvpn_gateway
 ip address 209.165.200.230 port 443
 http-redirect port 80
 ssl trustpoint TP-self-signed-2692466680
 inservice
 !
webvpn install svc flash:/webvpn/svc.pkg sequence 1
 !
webvpn context test
 secondary-color white
 title-color #669999
 text-color black
 ssl authenticate verify all
 !
 !
 policy group policy_1
   functions svc-enabled
   svc address-pool "test"
   svc keep-client-installed
   svc split include 192.168.10.0 255.255.255.0

 virtual-template 1
 default-group-policy policy_1
 aaa authentication list webvpn
```

```
 gateway webvpn_gateway
 inservice
!
end
```

Сценарий развертывания 2

Трафик VPN принадлежит другой зоне безопасности от внутренней сети.

Трафик AnyConnect принадлежит отдельной зоне VPN, и существует политика безопасности, которая управляет тем, какой трафик VPN может течь во внутреннюю зону. В этом конкретном примере трафик Telnet и трафик HTTP позволены от клиента AnyConnect внутренней локальной сети.

Настройка маршрутизатора

```
Router#show run
Building configuration...

Current configuration : 6029 bytes
!
! Last configuration change at 20:57:32 UTC Fri Mar 5
2010 by cisco
!
version 15.0
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
boot-start-marker
boot system flash:
boot-end-marker
!
aaa new-model
!
!
aaa authentication login default local
aaa authentication login webvpn local
!
!
aaa session-id common
!
ip cef
!
!
ip inspect log drop-pkt
no ip domain lookup
!
multilink bundle-name authenticated

parameter-map type inspect global

parameter-map type inspect audit-map
 audit-trail on
 tcp idle-time 20
!
!
crypto pki trustpoint TP-self-signed-2692466680
 enrollment selfsigned
```

```
 subject-name cn=IOS-Self-Signed-Certificate-2692466680
 revocation-check none
 rsakeypair TP-self-signed-2692466680
!
!
crypto pki certificate chain TP-self-signed-2692466680
 certificate self-signed 01
 <actual certificate deleted for brevity>
        quit
!
!
license udi pid CISCO3845-MB sn FOC09483Y8J
archive
 log config
  hidekeys
username cisco password 0 cisco
!
!
class-map type inspect match-any test
 match protocol tcp
match protocol udp
 match protocol icmp
class-map type inspect match-all router-access
 match access-group name router-access
class-map type inspect match-any http-telnet-ftp
 match protocol http
 match protocol telnet
 match protocol ftp
class-map type inspect match-all vpn-to-inside-cmap
 match class-map http-telnet-ftp
 match access-group name tunnel-traffic
!
!
policy-map type inspect firewall-policy
 class type inspect test
  inspect audit-map
 class class-default
  drop
policy-map type inspect out-to-self-policy
 class type inspect router-access
  inspect
 class class-default
  drop
policy-map type inspect self-to-out-policy
 class type inspect test
  inspect
 class class-default
  pass
policy-map type inspect vpn-to-in-policy
 class type inspect vpn-to-inside-cmap
  inspect
 class class-default
  drop
!
zone security inside
zone security outside
zone security vpn
zone-pair security in-out source inside destination
outside
 service-policy type inspect firewall-policy
zone-pair security out-self source outside destination
self
 service-policy type inspect out-to-self-policy
zone-pair security self-out source self destination
```

```
outside
 service-policy type inspect self-to-out-policy
zone-pair security in-vpn source inside destination vpn
 service-policy type inspect firewall-policy
zone-pair security vpn-in source vpn destination inside
 service-policy type inspect vpn-to-in-policy
!
!
interface Loopback0
 ip address 172.16.1.1 255.255.255.255
 !
!
interface GigabitEthernet0/0
 ip address 192.168.10.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly
 zone-member security inside
 !
!
interface GigabitEthernet0/1
 ip address 209.165.200.230 255.255.255.224
 ip nat outside
 ip virtual-reassembly
 zone-member security outside
 !
!
interface Virtual-Template1
 ip unnumbered Loopback0
 zone-member security vpn
 !
!
ip local pool test 192.168.1.1 192.168.1.100
ip forward-protocol nd
!
!
ip http server
ip http secure-server
ip nat inside source list 1 interface GigabitEthernet0/1
overload
ip route 0.0.0.0 0.0.0.0 209.165.200.225

!
ip access-list extended broadcast
 permit ip any host 255.255.255.255
ip access-list extended router-access
 permit tcp any host 209.165.200.230 eq www
 permit tcp any host 209.165.200.230 eq 443
ip access-list extended tunnel-traffic
 permit ip any 192.168.1.0 0.0.0.255
!
access-list 1 permit 192.168.10.0 0.0.0.255
!
!
control-plane
 !
!
!
line con 0
 exec-timeout 0 0
 logging synchronous
line aux 0
 modem InOut
 transport input all
line vty 0 4
```

```
 transport input all
!
exception data-corruption buffer truncate
scheduler allocate 20000 1000
!
webvpn gateway webvpn_gateway
 ip address 209.165.200.230 port 443
 http-redirect port 80
 ssl trustpoint TP-self-signed-2692466680
 inservice
 !
webvpn install svc flash:/webvpn/svc.pkg sequence 1
 !
webvpn context test
 secondary-color white
 title-color #669999
 text-color black
 ssl authenticate verify all
 !
 !
 policy group policy_1
   functions svc-enabled
   svc address-pool "test"
   svc keep-client-installed
   svc split include 192.168.10.0 255.255.255.0

 virtual-template 1
 default-group-policy policy_1
 aaa authentication list webvpn
 gateway webvpn_gateway
 inservice
!
end
```

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.**

Некоторые команды show связаны с WebVPN. Эти команды можно выполнить в интерфейсе командной строки (CLI) для отображения статистики и другой информации. См. Проверку конфигурации WebVPN для получения дополнительной информации о командах показа. См. Руководство по конфигурации Zone-Based Policy межсетевого экрана для получения дополнительной информации о командах, используемых для проверки Зональной Базирующейся Конфигурации межсетевого экрана Политики.

Устранение неполадок

В этом разделе описывается процесс устранения неполадок конфигурации.

Команды для устранения неполадок

Примечание: Прежде чем выполнять какие-либо команды отладки , ознакомьтесь с

документом "Важные сведения о командах отладки".

Некоторые команды debug связаны с WebVPN. См. Использование Команд отладки WebVPN для получения дополнительной информации об этих командах. См. команду для получения дополнительной информации о Зональных Базирующихся командах отладки Межсетевого экрана Политики.

Дополнительные сведения

- ПО Cisco IOS)
- Cisco Systems – техническая поддержка и документация