ZBF를 사용하여 Cisco IOS 라우터에서 AnyConnect VPN 클라이언트 구성

목차

소개

Cisco IOS® Software Release 12.4(20)T 이상에서는 AnyConnect VPN 클라이언트 연결을 위해 가상 인터페이스 SSLVPN-VIF0이 도입되었습니다. 그러나 이 SSLVPN-VIF0 인터페이스는 사용자 컨피그레이션을 지원하지 않는 내부 인터페이스입니다. 방화벽으로 인해 AnyConnect VPN 및 Zone Based Policy Firewall에 문제가 발생했습니다. 두 인터페이스가 모두 보안 영역에 속할 때 두 인터페이스 간에 트래픽이 이동할 수 있기 때문입니다. 사용자가 SSLVPN-VIF0 인터페이스를 영역 멤버로 구성할 수 없으므로 암호 해독 후 Cisco IOS WebVPN 게이트웨이에서 종료된 VPN 클라이언트 트래픽은 보안 영역에 속하는 다른 인터페이스로 전달할 수 없습니다. 방화벽에서 보고한 이 로그 메시지에서 이 문제의 증상을 확인할 수 있습니다.

```
*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
```

이 문제는 나중에 Cisco IOS의 최신 소프트웨어 릴리스에서 해결되었습니다. 사용자는 새 코드를 사용하여 보안 영역을 WebVPN 컨텍스트와 연결하기 위해 WebVPN 컨텍스트에서 참조되는 가상 템플릿 인터페이스에 보안 영역을 할당할 수 있습니다.

사전 요구 사항

요구 사항

Cisco IOS의 새로운 기능을 활용하려면 Cisco IOS WebVPN 게이트웨이 디바이스에서 Cisco IOS

Software 릴리스 12.4(20)T3, Cisco IOS Software 릴리스 12.4(22)T2 또는 Cisco IOS Software 릴리스 12.4(24)T1 이상을 실행하고 있는지 확인해야 합니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 버전 15.0(1)M1 Advanced Security 기능 집합을 실행하는 Cisco IOS 3845 Series 라우터
- Windows 2.4.1012용 Cisco AnyConnect SSL VPN Client 버전

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 규칙을 참조하십시오.

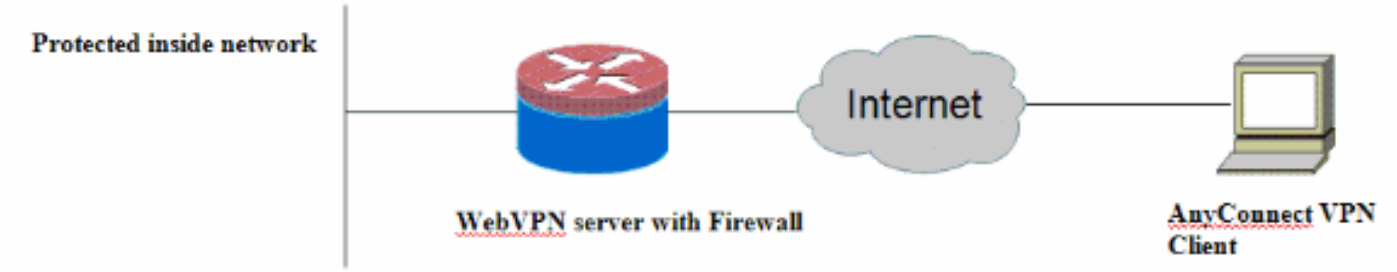
구성

이 섹션에는 이 문서에서 설명하는 기능을 구성하기 위한 정보가 표시됩니다.

참고: 명령 조회 도구(등록된 고객만 해당)를 사용하여 이 섹션에 사용된 명령에 대한 자세한 내용을 확인하십시오.

네트워크 다이어그램

이 문서에서는 다음 네트워크 설정을 사용합니다.



Cisco IOS AnyConnect 서버 구성

다음은 Zone Based Policy Firewall과 상호 운용되도록 하기 위해 Cisco IOS AnyConnect 서버에서 수행해야 하는 높은 수준의 컨피그레이션 단계입니다. 최종 구성은 이 문서의 뒷부분에 나오는 두 가지 일반적인 구축 시나리오에 포함됩니다.

1. 가상 템플릿 인터페이스를 구성하고 AnyConnect 연결에서 해독된 트래픽에 대해 보안 영역에 할당합니다.
2. AnyConnect 컨피그레이션을 위해 이전에 구성된 가상 템플릿을 WebVPN 컨텍스트에 추가합니다.
3. 나머지 WebVPN 및 Zone Based Policy Firewall 컨피그레이션을 완료합니다.AnyConnect와 ZBF의 일반적인 시나리오는 두 가지가 있으며, 각 시나리오의 최종 라우터 컨피그레이션이 여

기에 나와 있습니다.

구축 시나리오 1

VPN 트래픽은 내부 네트워크와 동일한 보안 영역에 속합니다.

AnyConnect 트래픽은 내부 LAN 인터페이스가 암호 해독 후 속해 있는 동일한 보안 영역으로 이동합니다.

참고: 자체 영역은 액세스 제한을 위해 라우터 자체에 http/https 트래픽만 허용하도록 정의됩니다.

라우터 컨피그레이션

```
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
```

구축 시나리오 2

VPN 트래픽은 내부 네트워크와 다른 보안 영역에 속합니다.

AnyConnect 트래픽은 별도의 VPN 영역에 속하며, 내부 영역으로 이동할 수 있는 vpn 트래픽을 제어하는 보안 정책이 있습니다. 이 특정 예에서는 텔넷과 http 트래픽이 AnyConnect 클라이언트에서 내부 LAN 네트워크로 허용됩니다.

라우터 컨피그레이션

```
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
```

다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

Output Interpreter 도구(등록된 고객만 해당)(OIT)는 특정 **show** 명령을 지원합니다. OIT를 사용하여 **show** 명령 출력의 분석을 봅니다.

여러 **show** 명령이 WebVPN과 연결되어 있습니다. CLI(Command Line Interface)에서 이러한 명령을 실행하여 통계 및 기타 정보를 **표시할** 수 있습니다. show 명령에 대한 자세한 내용은 WebVPN 컨피그레이션 확인을 참조하십시오. Zone Based Policy Firewall 컨피그레이션을 확인하는 데 사용되는 명령에 대한 자세한 내용은 Zone-Based Policy Firewall 컨피그레이션 설명서를 참조하십시오.

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

문제 해결 명령

참고: debug **명령**을 사용하기 전에 디버그 명령에 대한 중요 정보를 참조하십시오.

여러 디버그 명령이 WebVPN과 연결되어 있습니다. 이러한 명령에 대한 자세한 내용은 WebVPN 디버그 명령 사용을 참조하십시오. 영역 기반 정책 방화벽 디버깅 명령에 대한 자세한 내용은 명령을 참조하십시오.

관련 정보

- Cisco IOS 소프트웨어
- 기술 지원 및 문서 – Cisco Systems