Konfigurationsbeispiel für einen AnyConnect VPN-Client auf dem IOS-Router mit IOS Zone-basierter Firewall-Richtlinie

Inhalt

Einführung

In der Cisco IOS® Softwareversion 12.4(20)T und höher wurde eine virtuelle Schnittstelle SSLVPN-VIF0 für AnyConnect VPN-Clientverbindungen eingeführt. Diese SSLVPN-VIF0-Schnittstelle ist jedoch eine interne Schnittstelle, die keine Benutzerkonfigurationen unterstützt. Dies führte zu einem Problem mit dem AnyConnect VPN und der zonenbasierten Firewall, da der Datenverkehr zwischen zwei Schnittstellen nur dann fließen kann, wenn beide Schnittstellen zu Sicherheitszonen gehören. Da der Benutzer die SSLVPN-VIF0-Schnittstelle nicht so konfigurieren kann, dass sie zu einem Zonenmitglied wird, kann der VPN-Client-Datenverkehr, der nach der Entschlüsselung auf dem Cisco IOS WebVPN-Gateway terminiert wird, nicht an eine andere Schnittstelle weitergeleitet werden, die einer Sicherheitszone angehört. Das Symptom dieses Problems zeigt sich in dieser Protokollmeldung, die von der Firewall gemeldet wurde:

```
*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
```

Dieses Problem wurde später in neueren Softwareversionen von Cisco IOS behandelt. Mit dem neuen Code kann der Benutzer einer virtuellen Vorlagenschnittstelle, auf die im WebVPN-Kontext verwiesen wird, eine Sicherheitszone zuweisen, um dem WebVPN-Kontext eine Sicherheitszone zuzuordnen.

Voraussetzungen

Anforderungen

Um die neuen Funktionen von Cisco IOS nutzen zu können, müssen Sie sicherstellen, dass auf dem Cisco IOS WebVPN-Gateway-Gerät die Cisco IOS Software Release 12.4(20)T3, die Cisco IOS Software Release 12.4(22)T2 oder die Cisco IOS Software Release 12.4(24)T1 und höher ausgeführt wird.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco Router der Serie IOS 3845 mit Version 15.0(1)M1 Advanced Security-Feature-Set
- Cisco AnyConnect SSL VPN Client-Version für Windows 2.4.1012

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

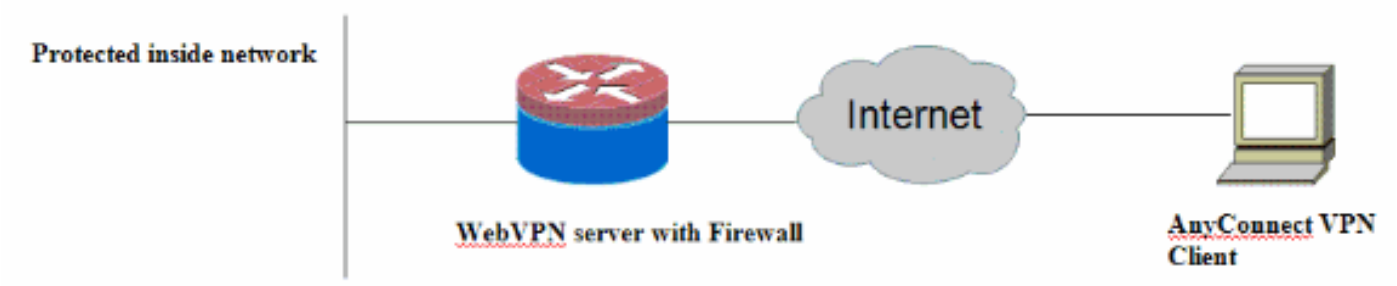
Konfigurieren

In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

Hinweis: Verwenden Sie das Command Lookup Tool (nur registrierte Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



Konfigurieren des Cisco IOS AnyConnect-Servers

Im Folgenden sind die allgemeinen Konfigurationsschritte aufgeführt, die auf dem Cisco IOS AnyConnect-Server ausgeführt werden müssen, damit er mit der zonenbasierten Firewall

kompatibel ist. Die resultierende endgültige Konfiguration ist für zwei typische Bereitstellungsszenarien weiter unten in diesem Dokument enthalten.

1. Konfigurieren Sie eine Virtual Template-Schnittstelle, und weisen Sie sie in einer Sicherheitszone für den von der AnyConnect-Verbindung entschlüsselten Datenverkehr zu.
2. Fügen Sie dem WebVPN-Kontext für die AnyConnect-Konfiguration die zuvor konfigurierte virtuelle Vorlage hinzu.
3. Schließen Sie den Rest der WebVPN- und zonenbasierten Firewall-Konfiguration ab.Bei AnyConnect und ZBF gibt es zwei typische Szenarien, und für jedes Szenario gibt es die abschließenden Routerkonfigurationen.

Bereitstellungsszenario 1

Der VPN-Datenverkehr gehört zur gleichen Sicherheitszone wie das interne Netzwerk.

Der AnyConnect-Datenverkehr geht in dieselbe Sicherheitszone, in der die interne LAN-Schnittstelle nach der Entschlüsselung gehört.

Hinweis: Eine Selbstzone ist auch so definiert, dass nur HTTP-/HTTPS-Datenverkehr zum Router selbst für Zugriffsbeschränkungen zugelassen wird.

Routerkonfiguration

```
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
```

Bereitstellungsszenario 2

Der VPN-Datenverkehr gehört zu einer anderen Sicherheitszone als das interne Netzwerk.

Der AnyConnect-Datenverkehr gehört zu einer separaten VPN-Zone, und es gibt eine Sicherheitsrichtlinie, die steuert, welcher VPN-Datenverkehr in die interne Zone fließen kann. In diesem Beispiel ist der Telnet- und HTTP-Datenverkehr vom AnyConnect-Client zum internen LAN-Netzwerk zulässig.

Routerkonfiguration

```
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
```

Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Das Output Interpreter Tool (nur registrierte Kunden) (OIT) unterstützt bestimmte **show**-Befehle. Verwenden Sie das OIT, um eine Analyse der **Ausgabe des** Befehls **show anzuzeigen**.

Mehrere **show**-Befehle sind WebVPN zugeordnet. Sie können diese Befehle in der Befehlszeilenschnittstelle (CLI) ausführen, um Statistiken und andere Informationen **anzuzeigen**. Weitere Informationen zu Anzeigebefehlen finden Sie unter Verifying WebVPN Configuration (Überprüfen der WebVPN-Konfiguration). Weitere Informationen zu Befehlen zum Überprüfen der Firewall-Konfiguration für zonenbasierte Richtlinien finden Sie im Konfigurationsleitfaden für zonenbasierte Firewall.

Fehlerbehebung

Dieser Abschnitt enthält Informationen zur Fehlerbehebung in Ihrer Konfiguration.

Befehle zur Fehlerbehebung

Hinweis: Beachten Sie vor der Verwendung von **Debug-**Befehlen die Informationen zu Debug-Befehlen.

Mehrere Debugbefehle sind WebVPN zugeordnet. Weitere Informationen zu diesen Befehlen finden Sie unter Verwenden von WebVPN-Debug-Befehlen. Weitere Informationen zu Befehlen zum Debuggen von zonenbasierten Firewall-Richtlinien finden Sie unter dem Befehl.

Zugehörige Informationen

- Cisco IOS-Software
- Technischer Support und Dokumentation - Cisco Systems