Exemple de configuration client VPN AnyConnect sur un routeur IOS avec pare-feu de stratégie basée sur les zones

Contenu

Introduction

Dans la version de logiciel 12.4(20)T et ultérieures de Cisco IOS®, une interface virtuelle SSLVPN-VIF0 a été introduite pour des connexions client VPN d'AnyConnect. Par contre, cette interface SSLVPN-VIF0 est interne : celle-ci ne prend pas en charge les configurations utilisateur. Ceci a créé un problème avec AnyConnect VPN et zone a basé le Pare-feu de stratégie puisqu'avec le Pare-feu, le trafic peut seulement circuler entre deux interfaces quand les deux interfaces appartiennent aux zones de Sécurité. Puisque l'utilisateur ne peut pas configurer l'interface SSLVPN-VIF0 pour lui faire un membre de zone, le trafic de client vpn terminé sur le webvpn gateway de Cisco IOS après le déchiffrement ne peut pas n'être expédié à aucune autre interface appartenant à une zone de Sécurité. Le symptôme de ce problème peut être vu avec ce message de log signalé par le Pare-feu :

```
*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
```

Cette question plus tard a été abordée dans de plus nouvelles versions logicielles de Cisco IOS. Avec le nouveau code, l'utilisateur peut assigner une zone de Sécurité à une interface de modèle virtuel, qui est mise en référence sous le contexte de webvpn, afin d'associer une zone de Sécurité avec le contexte de webvpn.

Conditions préalables

Conditions requises

Afin de tirer profit de la nouvelle capacité dans le Cisco IOS, vous devez s'assurer que le périphérique de webvpn gateway de Cisco IOS est la version du logiciel Cisco IOS courante 12.4(20)T3, le logiciel Release12.4(22)T2 de Cisco IOS, ou le logiciel Release12.4(24)T1 de Cisco IOS et plus tard.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Positionnement courant de fonctionnalité de sécurité avancée de version 15.0(1)M1 de routeur de gamme 3845 de Cisco IOS
- Version du client de VPN SSL de Cisco AnyConnect pour Windows 2.4.1012

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

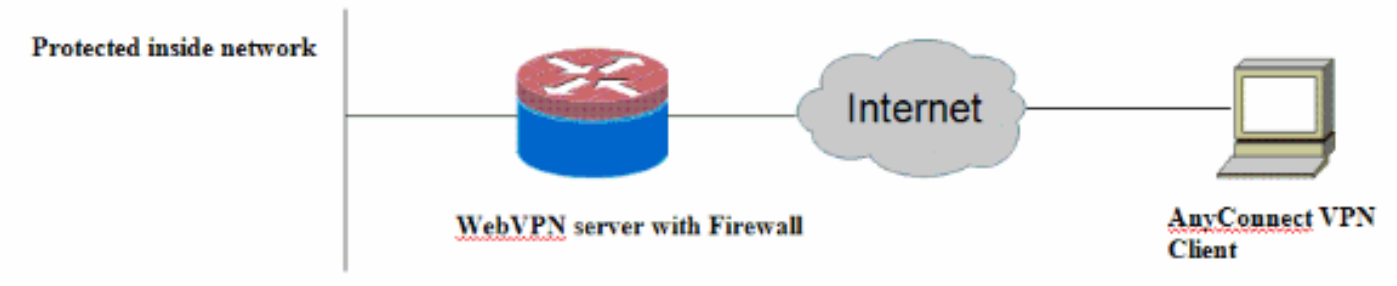
Configurez

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Remarque: Utilisez l'outil Command Lookup Tool (clients enregistrés seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



Configurez le serveur d'AnyConnect de Cisco IOS

Voici les étapes de haut niveau de configuration qui doivent être exécutées sur le serveur

d'AnyConnect de Cisco IOS afin de le faire interopérer avec le Pare-feu de stratégie basé par zone. La configuration finale en résultant sont incluses pour deux scénarios typiques de déploiement plus tard dans ce document.

1. Configurez une interface de modèle virtuel et assignez-la dans une zone de Sécurité pour le trafic déchiffré de la connexion d'AnyConnect.
2. Ajoutez le modèle virtuel précédemment configuré au contexte de webvpn pour la configuration d'AnyConnect.
3. Terminez-vous le reste du webvpn et de la configuration de Pare-feu de stratégie basée par zone.Il y a deux scénarios typiques avec AnyConnect et ZBF, et voici les configurations de routeur finales pour chaque scénario.

Scénario 1 de déploiement

Le trafic VPN appartient à la même zone de Sécurité que le réseau intérieur.

Le trafic d'AnyConnect entre dans la même zone de Sécurité que l'interface intérieure de RÉSEAU LOCAL appartient pour signaler le déchiffrement.

Remarque: Une zone d'individu est également définie pour permettre seulement le HTTP/trafic de https au routeur lui-même pour la restriction d'accès.

Configuration du routeur

```
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
```

Scénario 2 de déploiement

Le trafic VPN appartient à une zone de Sécurité différente du réseau intérieur.

Le trafic d'AnyConnect appartient à une zone distincte VPN, et il y a une stratégie de sécurité qui contrôle quel trafic de vpn peut circuler dans la zone intérieure. Dans cet exemple particulier, on permet le telnet et le trafic http du client d'AnyConnect au réseau intérieur de RÉSEAU LOCAL.

Configuration du routeur

```
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
```

Vérifiez

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

L'Outil Interpréteur de sortie (clients enregistrés uniquement) (OIT) prend en charge certaines commandes **show**. Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show** .

Plusieurs commandes **show** sont associées au WebVPN. Vous pouvez exécuter ces commandes dans l'interface de ligne de commande (CLI) afin d'afficher les statistiques et autres informations. Référez-vous à vérifier la configuration de webvpn pour plus d'informations sur des commandes show. Référez-vous au guide de configuration basé sur zone de Pare-feu de stratégie pour plus d'informations sur des commandes utilisées pour vérifier la configuration de Pare-feu de stratégie basée par zone.

Dépannez

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Dépannage des commandes

Remarque: Référez-vous aux informations importantes sur les commandes de débogage avant d'utiliser les commandes de **débogage**.

Plusieurs commandes **debug** sont associées à WebVPN. Référez-vous en utilisant des commandes de debug de webvpn pour plus d'informations sur ces commandes. Référez-vous à la commande pour plus d'informations sur des commandes de débogage de Pare-feu de stratégie basées par zone.

Informations connexes

- Logiciel Cisco IOS
- Support et documentation techniques - Cisco Systems