تكوين عميل AnyConnect VPN على موجه Cisco باستخدام ZBF IOS

المحتويات

المقدمة

في الإصدار 12.4(20)T من البرنامج Cisco IOS® Software والإصدارات الأحدث، تم تقديم واجهة افتراضية SSLVPN-VIF0 لاتصالات عميل AnyConnect VPN. ولكن، واجهة SSLVPN-VIF0 هذه هي واجهة داخلية، لا تدعم تكوينات المستخدم. أدى هذا إلى حدوث مشكلة في AnyConnect VPN وجدار حماية النهج المستند إلى المنطقة نظرا لأنه باستخدام جدار الحماية، يمكن لحركة مرور البيانات التدفق بين واجهات فقط عندما تنتمي كلا الواجهات إلى مناطق أمان. نظرا لتعذر على المستخدم تكوين واجهة SSLVPN-VIF0 لجعلها عضو منطقة، تم إنهاء حركة مرور عميل VPN على بوابة Cisco IOS WebVPN بعد فك التشفير ولا يمكن إعادة توجيهها إلى أي واجهة أخرى تنتمي إلى منطقة أمان. يمكن ملاحظة عرض هذه المشكلة مع رسالة السجل هذه التي تم الإبلاغ عنها بواسطة جدار الحماية:

```
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
```

تمت معالجة هذه المشكلة لاحقا في إصدارات البرامج الأحدث من Cisco IOS. باستخدام الرمز الجديد، يمكن للمستخدم تعيين منطقة أمان لواجهة القالب الظاهري، والتي تتم الإشارة إليها ضمن سياق WebVPN، من أجل إقران منطقة أمان بسياق WebVPN .

المتطلبات الأساسية

المتطلبات

من أجل الاستفادة من الإمكانات الجديدة في Cisco IOS، يلزمك التأكد من أن جهاز عبارة Cisco IOS WebVPN

يشغل برنامج Cisco IOS الإصدار T3(20)12.4 أو برنامج Cisco IOS الإصدار T2(22)12.4 أو برنامج Cisco IOS الإصدار T1(24)12.4 والإصدارات الأحدث.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- مجموعة ميزات الأمان المتقدم لموجه سلسلة Cisco IOS 3845 التي تشغل الإصدار M1(1)15.0
- إصدار عميل AnyConnect SSL VPN من Cisco لنظام التشغيل Windows 2.4.1012

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

الاصطلاحات

راجع اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.

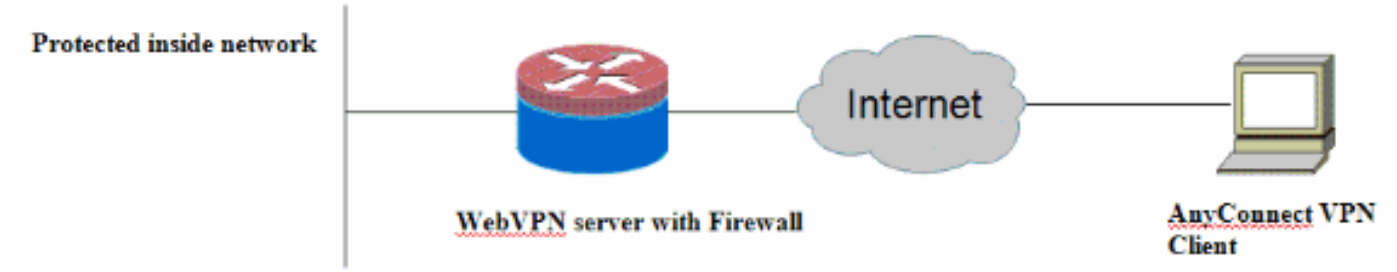
التكوين

في هذا القسم، تُقدّم لك معلومات تكوين الميزات الموضحة في هذا المستند.

ملاحظة: أستخدم أداة بحث الأوامر (للعملاء المسجلين فقط) للحصول على مزيد من المعلومات حول الأوامر المستخدمة في هذا القسم.

الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة التالي:



تكوين خادم AnyConnect من Cisco IOS

فيما يلي خطوات التكوين عالية المستوى التي يلزم تنفيذها على خادم Cisco IOS AnyConnect من أجل جعله يتفاعل مع جدار حماية السياسة المستند إلى المنطقة. يتم تضمين التكوين النهائي الناتج لسيناريوهين نموذجيين للنشر لاحقا في هذا المستند.

1. قم بتكوين واجهة قالب ظاهري وتعيينها في منطقة أمان لحركة مرور البيانات التي تم فك تشفيرها من اتصال AnyConnect.
2. إضافة "القالب الظاهري" الذي تم تكوينه مسبقا إلى سياق WebVPN لتكوين AnyConnect.
3. إكمال باقي تكوين جدار حماية النهج المستند إلى المنطقة و WebVPN.هناك سيناريوهان نموذجيان مع AnyConnect و ZBF، وإليك تكوينات الموجه النهائية لكل سيناريو.

سيناريو النشر 1

تنتمي حركة مرور VPN إلى منطقة الأمان نفسها الخاصة بالشبكة الداخلية.

تدخل حركة مرور AnyConnect في نفس منطقة الأمان التي تنتمي إليها واجهة شبكة LAN الداخلية إلى فك تشفير ما بعد.

ملاحظة: يتم أيضا تحديد منطقة ذاتية للسماح بحركة مرور HTTP/HTTPS فقط بالموجه نفسه لتقييد الوصول.

تكوين الموجّه

```
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
```

سيناريو النشر 2

تنتمي حركة مرور VPN إلى منطقة أمان مختلفة من الشبكة الداخلية.

تنتمي حركة مرور AnyConnect إلى منطقة VPN منفصلة، وهناك سياسة أمان تتحكم في حركة مرور VPN التي يمكن أن تتدفق إلى المنطقة الداخلية. في هذا المثال الخاص، يتم السماح بحركة مرور Telnet و http من عميل AnyConnect إلى شبكة LAN الداخلية.

تكوين الموجّه

```
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
```

التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

تدعم أداة مترجم الإخراج (للعملاءالمسجلين فقط) بعض أوامر **show**. استخدم أداة مترجم الإخراج (OIT) لعرض تحليل مُخرَج الأمر **show** .

يتم إقران العديد من أوامر **العرض** مع WebVPN. يمكنك تنفيذ هذه الأوامر في واجهة سطر الأوامر (CLI) **لإظهار** الإحصائيات ومعلومات أخرى. راجع التحقق من تكوين WebVPN للحصول على مزيد من المعلومات حول أوامر show. ارجع إلى دليل تكوين جدار حماية السياسة المستندة إلى المنطقة للحصول على مزيد من المعلومات حول الأوامر المستخدمة للتحقق من تكوين جدار حماية السياسة المستند إلى المنطقة.

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

أوامر استكشاف الأخطاء وإصلاحها

ملاحظة: ارجع إلى معلومات مهمة حول أوامر التصحيح قبل إستخدام أوامر **debug**.

تقترن العديد من أوامر تصحيح الأخطاء مع WebVPN. راجع إستخدام أوامر تصحيح الأخطاء ل WebVPN للحصول على مزيد من المعلومات حول هذه الأوامر. راجع الأمر للحصول على مزيد من المعلومات حول أوامر تصحيح أخطاء جدار الحماية المستندة إلى المنطقة.

معلومات ذات صلة

- برنامج IOS من Cisco
- الدعم التقني والمستندات - Cisco Systems

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).