مثال تكوين موجه جدار الحماية المستند إلى المنطقة لاتصال VPN

المحتويات

المقدمة
المتطلبات الأساسية
المتطلبات
المكونات المستخدمة
الاصطلاحات
معلومات أساسية
التكوين
الرسم التخطيطي للشبكة
التكوينات
التحقق من الصحة
استكشاف الأخطاء وإصلاحها
معلومات ذات صلة

المقدمة

يزود هذا وثيقة عينة تشكيل أن يوضح كيف أن يشكل مسحاج تخديد مع منطقة baser جدار حماية أن يعمل أيضا كمنفذ VPN بعيد.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

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

- موجه IOS 1721 من Cisco
- برنامج Cisco IOS® الإصدار 12.4T والإصدارات الأحدث

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة 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.

معلومات أساسية

تقوم جدران الحماية القائمة على المناطق بتنفيذ سياسة جدار الحماية أحادي الإتجاه بين مجموعات الواجهات المعروفة باسم المناطق. تحقق هذه الخطوات في مناطق المصدر والوجهة من واجهات الدخول والخروج لسياسة جدار الحماية.

في السيناريو الحالي، يتم تكوين جدار الحماية المستند إلى المنطقة على موجه العبارة-VPN. وهو يسمح لحركة مرور VPN من الإنترنت (خارج المنطقة) إلى المنطقة الذاتية. يتم إنشاء واجهة القالب الظاهري كجزء من منطقة الأمان. تحتوي الشبكة الداخلية على خادم يمكن للمستخدمين على الإنترنت الوصول إليه بمجرد إتصالهم من خلال شبكة VPN للوصول عن بعد التي تنتهي على موجه عبارة VPN.

- عنوان IP الخاص بالخادم الداخلي—172.16.10.20
- عنوان IP الخاص بجهاز الكمبيوتر العميل البعيد—192.168.100.10

يسمح لجميع المستخدمين على الشبكة الداخلية بالوصول غير المقيد إلى الإنترنت. يتم فحص جميع حركات المرور من المستخدمين الداخليين عند المرور عبر الموجه.

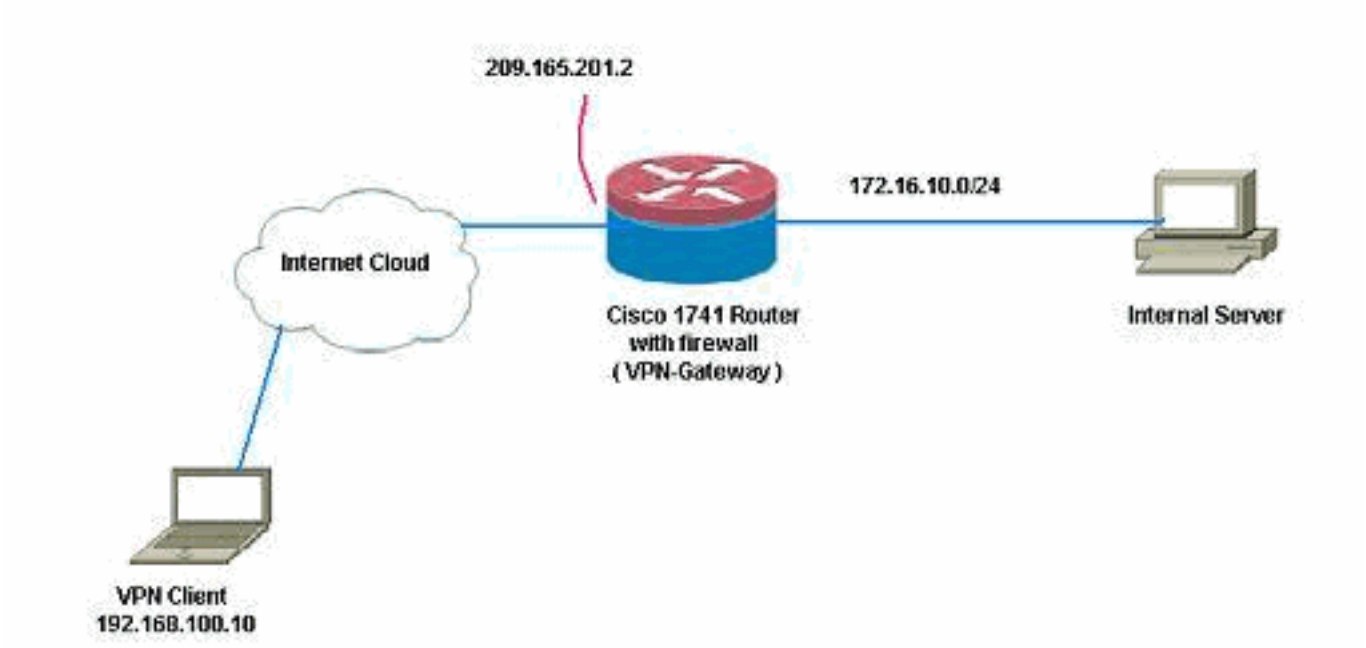
التكوين

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:



التكوينات

يستخدم هذا المستند التكوينات التالية:

VPN-Gateway

```
VPN-Gateway#show run
...Building configuration

Current configuration : 3493 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname VPN-Gateway
!
boot-start-marker
boot-end-marker
!
!
aaa new-model
!
!
Define local authentication aaa authentication ---!
login default local
aaa authorization network default local
!
Output suppressed ! ! !--- Define the isakmp ---!!
policy parameters crypto isakmp policy 1
encr 3des
authentication pre-share
group 2
!
crypto isakmp key cisco123 address 0.0.0.0 0.0.0.0
crypto isakmp keepalive 10
!
Define the group policy information crypto isakmp ---!!
client configuration group cisco
key cisco
dns 6.0.0.2
wins 7.0.0.1
domain cisco.com
pool dpool
acl 101
Define the ISAKMP profile crypto isakmp profile vi ---!!
match identity group cisco
isakmp authorization list default
client configuration address respond
virtual-template 1
!
Define the transform-set parameters crypto ipsec ---!!
transform-set set esp-3des esp-sha-hmac
!
Define the IPSec profile crypto ipsec profile vi ---!!
set transform-set set
set isakmp-profile vi
!
!
!
!
!
Define the local username and password username ---!!
```

```
cisco privilege 15 password 0 cisco
archive
log config
hidekeys
!
!
Define the Zone based firewall Class maps class- ---!
map type inspect match-any Internet-cmap
match protocol icmp
match protocol tcp
match protocol udp
match protocol http
match protocol https
match protocol pop3
match protocol pop3s
match protocol smtp
class-map type inspect match-all ICMP-cmap
match access-group name ICMP
class-map type inspect match-all IPSEC-cmap
match access-group name ISAKMP_IPSEC
class-map type inspect match-all SSHaccess-cmap
match access-group name SSHaccess
!
Define the Zone based firewall Policy maps policy- ---!
map type inspect inside-outside-pmap
class type inspect Internet-cmap
inspect
class type inspect ICMP-cmap
inspect
class class-default
drop
policy-map type inspect outside-inside-pmap
class type inspect ICMP-cmap
inspect
class class-default
drop
policy-map type inspect Outside-Router-pmap
class type inspect SSHaccess-cmap
inspect
class type inspect ICMP-cmap
inspect
class type inspect IPSEC-cmap
pass
class class-default
drop
!
Define zones zone security inside ---!
zone security outside
!
Define zone-pairs zone-pair security inside-to- ---!
outside source inside destination outside
service-policy type inspect inside-outside-pmap
zone-pair security outside-to-router source outside
destination self
service-policy type inspect Outside-Router-pmap
zone-pair security outside-to-inside source outside
destination inside
service-policy type inspect outside-inside-pmap
!
!
!
interface Ethernet0
ip address 172.16.10.20 255.255.255.0
Define interface as part of inside zone zone- ---!
```

```
 member security inside
  half-duplex
 !
interface FastEthernet0
 ip address 209.165.201.2 255.255.255.224
 Define interface as part of outside zone zone- ---!!
 member security outside
  speed auto
 !
interface Virtual-Template1 type tunnel
  ip unnumbered FastEthernet0
 Define interface as part of outside zone zone- ---!!
 member security outside
 tunnel source FastEthernet0
  tunnel mode ipsec ipv4
 tunnel protection ipsec profile vi
 !
 Define the local pool range ip local pool dpool ---!!
5.0.0.1 5.0.0.3 ! ! !--- Output suppressed ! ip access-
list extended ICMP permit icmp any any echo permit icmp
 any any echo-reply permit icmp any any traceroute ! ip
access-list extended ISAKMP_IPSEC permit udp any any eq
isakmp permit ahp any any permit esp any any permit udp
    any any eq non500-isakmp ! ip access-list extended
  SSHaccess permit tcp any any eq 22 ! access-list 101
permit ip 172.16.10.0 0.0.0.255 any ! ! ! control-plane
 ! ! line con 0 line aux 0 line vty 0 4 ! 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** .

1. أستخدم هذا الأمر للتحقق من حالة الواجهة.

```
VPN-Gateway#show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
      Ethernet0                172.16.10.20    YES NVRAM  up                    up
      FastEthernet0            209.165.201.2   YES NVRAM  up                    up
    Virtual-Access1          unassigned      YES unset  down                  down
      Virtual-Access2          209.165.201.2   YES TFTP   up                    up
    Virtual-Template1        209.165.201.2   YES TFTP   down                  down
```

2. أستخدم هذا الأمر للتحقق من حالة نفق ISAKMP.

```
VPN-Gateway#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot status
QM_IDLE           1001    0 ACTIVE  192.168.100.10   209.165.201.2

IPv6 Crypto ISAKMP SA
```

3. أستخدم هذا الأمر للتحقق من حالة مآخذ التشفير.

```
VPN-Gateway#show crypto socket

Number of Crypto Socket connections 1

Vi2 Peers (local/remote): 209.165.201.2/192.168.100.10
(Local Ident  (addr/mask/port/prot): (0.0.0.0/0.0.0.0/0/0
(Remote Ident (addr/mask/port/prot): (5.0.0.1/255.255.255.255/0/0
"IPSec Profile: "vi
 Socket State: Open
```

```
(Client: "TUNNEL SEC" (Client State: Active

:Crypto Sockets in Listen state
"Client: "TUNNEL SEC" Profile: "vi" Map-name: "Virtual-Template1-head-0
```

4. تحقق من المجموعات النشطة على الموجه.

```
VPN-Gateway#show crypto session summary detail
Crypto session current status

Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, X - IKE Extended Authentication

Interface: Virtual-Access2
Profile: vi
Group: cisco
Assigned address: 5.0.0.1
Uptime: 00:13:52
Session status: UP-ACTIVE
(Peer: 192.168.100.10 port 1069 fvrf: (none) ivrf: (none
Phase1_id: cisco
(Desc: (none
IKE SA: local 209.165.201.2/500 remote 192.168.100.10/1069 Active
Capabilities:CD connid:1001 lifetime:23:46:05
IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 host 5.0.0.1
Active SAs: 2, origin: crypto map
Inbound:  #pkts dec'ed 10 drop 0 life (KB/Sec) 4520608/2767
Outbound: #pkts enc'ed 10 drop 0 life (KB/Sec) 4520608/2767
```

5. أستخدم هذا الأمر لعرض إحصائيات مخطط سياسة نوع فحص وقت التشغيل.

```
VPN-Gateway#show policy-map type inspect zone-pair
Zone-pair: inside-to-outside

Service-policy inspect : inside-outside-pmap

(Class-map: Internet-cmap (match-any
Match: protocol icmp
packets, 0 bytes 0
second rate 0 bps 30
Match: protocol tcp
packets, 0 bytes 0
second rate 0 bps 30
Match: protocol udp
packets, 0 bytes 0
second rate 0 bps 30
Match: protocol http
packets, 0 bytes 0
second rate 0 bps 30
Match: protocol https
packets, 0 bytes 0
second rate 0 bps 30
Match: protocol pop3
packets, 0 bytes 0
second rate 0 bps 30
Match: protocol pop3s
packets, 0 bytes 0
second rate 0 bps 30
Match: protocol smtp
packets, 0 bytes 0
second rate 0 bps 30
Inspect
Session creations since subsystem startup or last reset 0
[Current session counts (estab/half-open/terminating) [0:0:0
```

```
[Maxever session counts (estab/half-open/terminating) [0:0:0
                                  Last session created never
                                  Last statistic reset never
                                Last session creation rate 0
                              Maxever session creation rate 0
                               Last half-open session total 0

                                 (Class-map: ICMP-cmap (match-all
                                  Match: access-group name ICMP
                                                       Inspect
   Session creations since subsystem startup or last reset 0
[Current session counts (estab/half-open/terminating) [0:0:0
[Maxever session counts (estab/half-open/terminating) [0:0:0
                                  Last session created never
                                  Last statistic reset never
                                Last session creation rate 0
                              Maxever session creation rate 0
                               Last half-open session total 0

                             (Class-map: class-default (match-any
                                                   Match: any
                                                         Drop
                                      packets, 0 bytes 0
                                  Zone-pair: outside-to-router

                        Service-policy inspect : Outside-Router-pmap

                             (Class-map: SSHaccess-cmap (match-all
                              Match: access-group name SSHaccess
                                                       Inspect
   Session creations since subsystem startup or last reset 0
[Current session counts (estab/half-open/terminating) [0:0:0
[Maxever session counts (estab/half-open/terminating) [0:0:0
                                  Last session created never
                                  Last statistic reset never
                                Last session creation rate 0
                              Maxever session creation rate 0
                               Last half-open session total 0

                                 (Class-map: ICMP-cmap (match-all
                                  Match: access-group name ICMP
                                                       Inspect
   [Packet inspection statistics [process switch:fast switch
                                         [icmp packets: [93:0

   Session creations since subsystem startup or last reset 6
[Current session counts (estab/half-open/terminating) [0:0:0
[Maxever session counts (estab/half-open/terminating) [0:2:0
                               Last session created 00:07:02
                                  Last statistic reset never
                                Last session creation rate 0
                              Maxever session creation rate 2
                               Last half-open session total 0

                                 (Class-map: IPSEC-cmap (match-all
                            Match: access-group name ISAKMP_IPSEC
                                                         Pass
                                    packets, 7145 bytes 57

                               (Class-map: class-default (match-any
                                                   Match: any
                                                         Drop
                                      packets, 44 bytes 2
                                  Zone-pair: outside-to-inside
```

```
                    Service-policy inspect : outside-inside-pmap

                                (Class-map: ICMP-cmap (match-all
                                 Match: access-group name ICMP
                                                      Inspect
   [Packet inspection statistics [process switch:fast switch
                                         [icmp packets: [1:14

   Session creations since subsystem startup or last reset 2
[Current session counts (estab/half-open/terminating) [0:0:0
[Maxever session counts (estab/half-open/terminating) [1:1:0
                                Last session created 00:09:15
                                   Last statistic reset never
                                 Last session creation rate 0
                               Maxever session creation rate 1
                                Last half-open session total 0

                             (Class-map: class-default (match-any
                                                 Match: any
                                                      Drop
                                          packets, 0 bytes 0
```

6. أستخدم إختبار الاتصال للتحقق من الاتصال بالخادم الداخلي.

```
E:\Documents and Settings\Administrator>ping 172.16.10.20

                    :Pinging 172.16.10.20 with 32 bytes of data

          Reply from 172.16.10.20: bytes=32 time=206ms TTL=254
           Reply from 172.16.10.20: bytes=32 time=63ms TTL=254
           Reply from 172.16.10.20: bytes=32 time=20ms TTL=254
           Reply from 172.16.10.20: bytes=32 time=47ms TTL=254

                               :Ping statistics for 172.16.10.20
       ,(Packets: Sent = 4, Received = 4, Lost = 0 (0% loss
                 :Approximate round trip times in milli-seconds
           Minimum = 20ms, Maximum = 206ms, Average = 84ms
```

استكشاف الأخطاء وإصلاحها

لا تتوفر حاليًا معلومات محددة لاستكشاف الأخطاء وإصلاحها لهذا التكوين.

معلومات ذات صلة

- جدار حماية Cisco IOS
- 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).