ASA/PIX - تكوين نفق IPsec لموجه Cisco IOS من LAN إلى LAN

المحتويات

المقدمة

يوضح هذا المستند كيفية تكوين نفق IPsec من جهاز أمان PIX 7.x والإصدارات الأحدث أو جهاز الأمان القابل للتكيف (ASA) مع شبكة داخلية واحدة إلى موجه 2611 الذي يشغل صورة تشفير. يتم استخدام المسارات الثابتة للتبسيط.

ارجع إلى تكوين IPSec - الموجه إلى PIX للحصول على مزيد من المعلومات حول تكوين نفق من شبكة LAN إلى شبكة LAN بين موجه و PIX.

ارجع إلى تكوين نفق IPSec من شبكة LAN إلى شبكة LAN بين مركز Cisco VPN 3000 وجدار حماية PIX للحصول على مزيد من المعلومات حول تكوين نفق من شبكة LAN إلى شبكة LAN بين جدار حماية PIX ومجمع Cisco VPN 3000.

ارجع إلى نفق IPsec بين مثال تكوين مركز PIX 7.x و VPN 3000 لمعرفة المزيد حول السيناريو حيث يكون نفق شبكة LAN إلى شبكة LAN بين مركز PIX و VPN.

ارجع إلى PIX/ASA 7.x Enhanced Talk-To-Client VPN مع مثال تكوين مصادقة TACACS+ لمعرفة المزيد حول السيناريو الذي يسمح فيه نفق شبكة LAN إلى شبكة LAN بين PIXs أيضا لعميل VPN بالوصول إلى PIX الذي يتم التحدث به من خلال PIX في المركز.

ارجع إلى SDM: شبكة VPN الخاصة ببروتوكول IPsec من موقع إلى موقع بين ASA/PIX ومثال تكوين موجه IOS لمعرفة المزيد حول نفس السيناريو حيث يشغل جهاز أمان PIX/ASA الإصدار 8.x من البرنامج.

أجلت [تشكيل محترف: موقع إلى موقع IPsec VPN بين ASA/PIX والثم تكوين موجه IOS](#) in order to [تعلم](#) المزيد حول السيناريو نفسه حيث يتم عرض التكوين المرتبط ASA بالموجه باستخدام واجهة المستخدم الرسومية (GUI) ل ASDM ويتم عرض التكوين المرتبط باستخدام واجهة المستخدم الرسومية (GUI) ل Cisco CP.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

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

- PIX-525 مع برنامج PIX، الإصدار 7.0
- cisco 2611 مسحاج تخديد مع cisco ios ® برمجية إطلاق 12.2(15)T13

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.](#)

معلومات أساسية

على ال PIX، ال access-list وnat 0 يعمل أمر معا. عندما يذهب مستخدم على شبكة 10.1.1.0 إلى شبكة 10.2.2.0، تستخدم قائمة الوصول للسماح بتشفير حركة مرور الشبكة 10.1.1.0 دون ترجمة عناوين الشبكة (NAT). على الموجه، يتم إستخدام أوامر route-map وaccess-list للسماح بتشفير حركة مرور الشبكة 10.2.2.0 دون NAT. ومع ذلك، عندما يذهب هؤلاء المستخدمون نفسهم إلى أي مكان آخر، تتم ترجمتهم إلى العنوان 172.17.63.230 من خلال ترجمة عنوان المنفذ (PAT).

هذا ال تشكيل أمر يتطلب على ال PIX أمن جهاز in order to ال يركض حركة مرور من خلال ال برض عبر النفق، وحركة مرور إلى الإنترنت أن يركض من خلال ال برض

<#root>

```
access-list nonat permit ip 10.1.1.0 255.255.255.0 10.2.2.0 255.255.255.0
nat (inside) 0 access-list nonat
nat (inside) 1 10.1.1.0 255.255.255.0 0 0
```

التكوين

يف اذه القسم، تُقدّم لك معلومات تكوين المميزات الموضحة في اذه المستند.

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

الرسم التخطيطي للشبكة

يستخدم اذه المستند إعداد الشبكة التالي:

التكوينات

هذه أمثلة التكوين هي لواجهة سطر الأوامر. ارجع قسم التكوين باستخدام مدير أجهزة الأمان باستخدام التكوين في اذه المستند إذا كنت تفضل التكوين باستخدام ASDM (المعدلة (ASDM.

- PIX لمقر
- موجه فرعي

PIX لمقر

```
<#root>

HQPIX(config)#

show run

PIX Version 7.0(0)102
names
!

interface Ethernet0
description WAN interface
nameif outside
security-level 0
ip address 172.17.63.229 255.255.255.240
!
interface Ethernet1
nameif inside
security-level 100
ip address 10.1.1.1 255.255.255.0

!
interface Ethernet2
shutdown
no nameif
no security-level
no ip address
!
interface Ethernet3
shutdown
no nameif
no security-level
no ip address
```

```
!
interface Ethernet4
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Ethernet5
 shutdown
 no nameif
 no security-level
 no ip address
!
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname HQPIX
domain-name cisco.com
ftp mode passive
clock timezone AEST 10

access-list Ipsec-conn extended permit ip 10.1.1.0 255.255.255.0 10.2.2.0 255.255.255.0
access-list nonat extended permit ip 10.1.1.0 255.255.255.0 10.2.2.0 255.255.255.0

pager lines 24
logging enable
logging buffered debugging
mtu inside 1500
mtu outside 1500
no failover
monitor-interface inside
monitor-interface outside
asdm image flash:/asdmfile.50073
no asdm history enable
arp timeout 14400

nat-control
global (outside) 1 interface
nat (inside) 0 access-list nonat
nat (inside) 1 10.1.1.0 255.255.255.0
access-group 100 in interface inside

route outside 0.0.0.0 0.0.0.0 172.17.63.230 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server partner protocol tacacs+

username cisco password 3USUcOPFUiMCO4Jk encrypted
http server enable
http 10.1.1.2 255.255.255.255 inside

no snmp-server location
no snmp-server contact
snmp-server community public
snmp-server enable traps snmp

crypto ipsec transform-set avalanche esp-des esp-md5-hmac
crypto ipsec security-association lifetime seconds 3600
crypto ipsec df-bit clear-df outside
```

```
crypto map forsberg 21 match address Ipsec-conn
crypto map forsberg 21 set peer 172.17.63.230
crypto map forsberg 21 set transform-set avalanche
crypto map forsberg interface outside

isakmp identity address

isakmp enable outside
isakmp policy 1 authentication pre-share
isakmp policy 1 encryption 3des
isakmp policy 1 hash sha
isakmp policy 1 group 2

isakmp policy 1 lifetime 86400
isakmp policy 65535 authentication pre-share
isakmp policy 65535 encryption 3des
isakmp policy 65535 hash sha
isakmp policy 65535 group 2
isakmp policy 65535 lifetime 86400
telnet timeout 5
ssh timeout 5
console timeout 0

tunnel-group 172.17.63.230 type ipsec-l2l
tunnel-group 172.17.63.230 ipsec-attributes
pre-shared-key *

!
class-map inspection_default
match default-inspection-traffic
!
!
policy-map asa_global_fw_policy
class inspection_default
inspect dns maximum-length 512
inspect ftp
inspect h323 h225
inspect h323 ras
inspect netbios
inspect rsh
inspect rtsp
inspect skinny
inspect esmtp
inspect sqlnet
inspect sunrpc
inspect tftp
inspect sip
inspect xdmcp
inspect http
!
service-policy asa_global_fw_policy global
Cryptochecksum:3a5851f7310d14e82bdf17e64d638738
: end
SV-2-8#
```

موجه فرعي
<#root>

```
BranchRouter#
show run
Building configuration...

Current configuration : 1719 bytes
!
! Last configuration change at 13:03:25 AEST Tue Apr 5 2005
! NVRAM config last updated at 13:03:44 AEST Tue Apr 5 2005
!
version 12.2
service timestamps debug datetime msec
service timestamps log uptime
no service password-encryption
!
hostname BranchRouter
!
logging queue-limit 100
logging buffered 4096 debugging
!
username cisco privilege 15 password 0 cisco
memory-size iomem 15
clock timezone AEST 10
ip subnet-zero
!
!
!
ip audit notify log
ip audit po max-events 100
!
!
!

crypto isakmp policy 11
encr 3des
authentication pre-share
group 2
crypto isakmp key cisco123 address 172.17.63.229

!
!

crypto ipsec transform-set sharks esp-des esp-md5-hmac

!

crypto map nolan 11 ipsec-isakmp
set peer 172.17.63.229
set transform-set sharks
match address 120

!
!
!
!
!
!
!
!
!
!
no voice hpi capture buffer
no voice hpi capture destination
```

```
!
!
mta receive maximum-recipients 0
!
!
!
!

interface Ethernet0/0
ip address 172.17.63.230 255.255.255.240
ip nat outside
no ip route-cache
no ip mroute-cache
half-duplex
crypto map nolan

!

interface Ethernet0/1
ip address 10.2.2.1 255.255.255.0
ip nat inside
half-duplex

!

ip nat pool branch 172.17.63.230 172.17.63.230 netmask 255.255.255.0
ip nat inside source route-map nonat pool branch overload

no ip http server
no ip http secure-server
ip classless
ip route 10.1.1.0 255.255.255.0 172.17.63.229
!
!
!

access-list 120 permit ip 10.2.2.0 0.0.0.255 10.1.1.0 0.0.0.255
access-list 130 deny ip 10.2.2.0 0.0.0.255 10.1.1.0 0.0.0.255
access-list 130 permit ip 10.2.2.0 0.0.0.255 any
!
route-map nonat permit 10
match ip address 130

!
call rsvp-sync
!
!
mgcp profile default
!
dial-peer cor custom
!
!
!
!
!
line con 0
line aux 0
line vty 0 4
login
!
!
end
```

التكوين باستخدام ASDM

يوضح هذا المثال كيفية تكوين PIX باستخدام واجهة المستخدم الرسومية (GUI) ل ASDM. يتم توصيل جهاز كمبيوتر مزود بمستعرض وعنوان IP 10.1.1.2 بالواجهة الداخلية E1 الخاصة ب PIX. تأكد من تمكين http على PIX.

يوضح هذا الإجراء تكوين ASDM الخاص ب PIX للمقر.

1. قم بتوصيل الكمبيوتر ب PIX واختر طريقة تنزيل.

   يقوم ASDM بتحميل التكوين الحالي من PIX.

   توفر هذه النافذة أدوات المراقبة والقوائم.

2. حدد تكوين > ميزات > واجهات وحدد إضافة للواجهات الجديدة أو تحرير لتكوين موجود.

3. حدد خيارات التأمين للواجهة الداخلية.

4. حدد NAT/PAT إلى القارن وكل آخر حركة مرور يعفي nat، يشفر حركة مرور nat في ال تشكيل خارجي.

5. حدد VPN >عام > مجموعة نفق وقم بتمكين مجموعة نفق.

6. حدد VPN > IKE > معلمات عمومية وقم بتمكين IKE على الواجهة الخارجية.

7. حدد VPN > IKE > السياسات واختر سياسات IKE.

8. حدد VPN > IPsec > قواعد IPsec واختر IPsec للنفق المحلي والعنونة عن بعد.

9. حدد VPN > IPsec > سياسة النفق واختر سياسة النفق.

10. حدد VPN > IPsec > مجموعات التحويل واختر مجموعة تحويل.

11. حدد توجيه > توجيه ساكن إستاتيكي واختر مسار ساكن إستاتيكي إلى موجه البوابة. في هذا المثال، يشير المسار الثابت إلى نظير شبكة VPN البعيد لضمان البساطة.

التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

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

- show crypto ips sa—يعرض اقترانات أمان المرحلة 2.
- show crypto isakmp sa—يعرض اقترانات أمان المرحلة 1.

استكشاف الأخطاء وإصلاحها

يمكنك إستخدام ASDM لتمكين التسجيل وعرض السجلات.

- حدد تكوين > خصائص > تسجيل > إعداد التسجيل، أختر تمكين التسجيل، وانقر فوق تطبيق لتمكين التسجيل.
- حدد مراقبة > تسجيل > مخزن السجل المؤقت > على مستوى التسجيل، واختر مخزن التسجيل المؤقت، وانقر فوق عرض لعرض السجلات.

أوامر استكشاف الأخطاء وإصلاحها

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

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

- debug crypto ipSec—يعرض مفاوضات IPsec للمرحلة 2.
- debug crypto isakmp—يعرض مفاوضات ISAKMP للمرحلة 1.
- debug crypto engine—يعرض حركة مرور البيانات التي يتم تشفيرها.
- مسح التشفير isakmp—يمحو اقترانات الأمان المتعلقة بالمرحلة 1.
- مسح التشفير sa—يمحو اقترانات الأمان المتعلقة بالمرحلة 2.
- debug icmp trace— يعرض ما إذا كانت طلبات ICMP من الأجهزة المضيفة تصل إلى PIX. تحتاج إلى إضافة أمر access-list للسماح ب ICMP في التكوين الخاص بك لتشغيل تصحيح الأخطاء هذا.
- تصحيح أخطاء مخزن التسجيل المؤقت— يعرض الاتصالات التي يتم إنشاؤها ويتم رفضها للمضيفين الذين يمرون عبر PIX. يتم تخزين المعلومات في المخزن المؤقت لسجل PIX ويمكنك رؤية الإخراج باستخدام الأمر show log.

معلومات ذات صلة

- حلول أستكشاف أخطاء الشبكة الخاصة الظاهرية (VPN) عبر بروتوكول IPSec للوصول عن بعد و L2L الأكثر شيوعا
- برنامج جدار حماية Cisco PIX
- مراجع أوامر جدار حماية PIX الآمن من Cisco
- الإعلامات الميدانية لمنتج الأمان (بما في ذلك PIX)
- طلبات التعليقات (RFCs)

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).