PIX/ASA 7.x والإصدارات الأحدث: شبكة VPN من LAN إلى LAN مع مثال تكوين الشبكات المتداخلة

المحتويات

المقدمة

يصف هذا وثيقة ال steps يستعمل أن يترجم (NAT) ال VPN حركة مرور أن يسافر عبر lan إلى (L2L) LAN بين إثنان أمن أداة وأيضا ضرب الإنترنت حركة مرور. يكون لكل جهاز أمان شبكة خاصة محمية خلفه. في هذا المثال، يتم توصيل جهازي أمان قابلين للتكيف (ASAs) من Cisco مزودين بشبكات داخلية متطابقة ومتداخلة عبر نفق VPN. في السيناريو العادي، لا يحدث الاتصال عبر شبكة VPN أبدا لأن حزم إختبار الاتصال لا تغادر الشبكة الفرعية المحلية مطلقا نظرا لأن المستخدم يقوم بسحب عنوان IP الخاص بالشبكة الفرعية نفسها. لهاتين الشبكتين الداخليتين الخاصتين للاتصال ببعضها البعض، يتم إستخدام Policy NAT على كل من ASAs لترجمة الشبكة الفرعية المحلية حتى يحدث الاتصال كما هو متوقع.

المتطلبات الأساسية

المتطلبات

تأكد من تكوين جهاز الأمان القابل للتكيف من Cisco باستخدام عناوين IP على الواجهات، ومن توفر إمكانية الاتصال الأساسية قبل المتابعة بمثال التكوين هذا.

المكونات المستخدمة

أسست المعلومة في هذا وثيقة على هذا برمجية صيغة:

- برنامج أجهزة الأمان المعدلة Cisco Adaptive Security Appliance Software، الإصدار x.7 والإصدارات الأحدث.

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.

المنتجات ذات الصلة

كما يمكن إستخدام هذا التكوين مع جهاز الأمان Cisco PIX الإصدار x.7 والإصدارات الأحدث.

الاصطلاحات

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

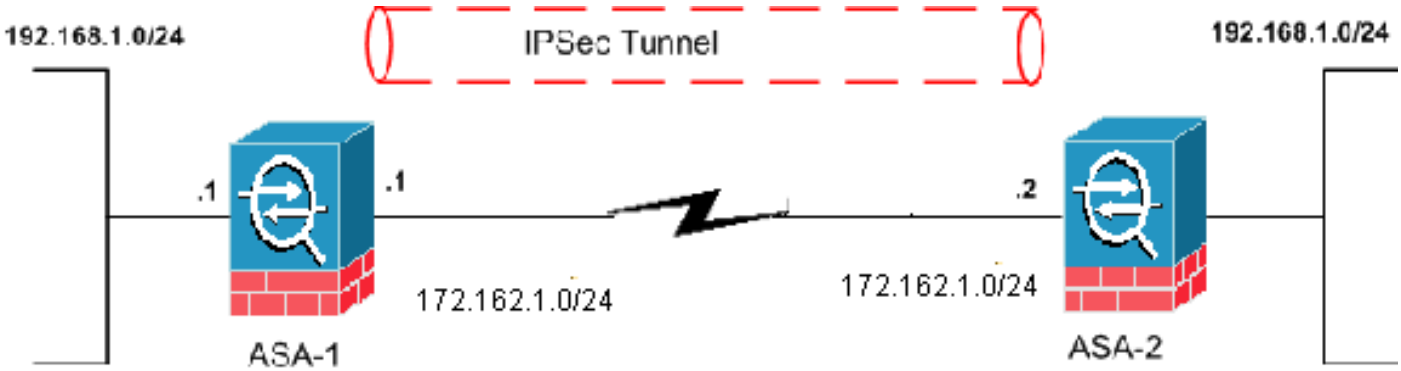
التكوين

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:



التكوينات

يستخدم هذا المستند التكوينات التالية:

- تكوين ASA-1
- تكوين ASA-2

ASA-1
ASA-1#**show running-config** Saved : :

```
(ASA Version 8.0(3
!
hostname ciscoasa
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Ethernet0
nameif outside
security-level 0
ip address 172.162.1.1 255.255.255.0
Configure the outside interface. ! interface ---!
Ethernet1 nameif inside security-level 100 ip address
192.168.1.1 255.255.255.0 !--- Configure the inside
interface. passwd 2KFQnbNIdI.2KYOU encrypted ftp mode
passive access-list new extended permit ip 192.168.2.0
255.255.255.0 192.168.3.0 255.255.255.0 !--- This access
list (new) is used with the crypto map (outside_map) !--
- in order to determine which traffic should be
.encrypted !--- and sent across the tunnel
access-list policy-nat extended permit ip 192.168.1.0
255.255.255.0 192.168.3.0 255.255.255.0

The policy-nat ACL is used with the static !--- ---!
command in order to match the VPN traffic for
.translation

pager lines 24
mtu outside 1500
mtu inside 1500
no failover
asdm image flash:/asdm-615.bin
no asdm history enable
arp timeout 14400


static (inside,outside) 192.168.2.0  access-list policy-
nat
It is a Policy NAT statement. !--- The static ---!
command with the access list (policy-nat), !--- which
matches the VPN traffic and translates the source
(192.168.1.0) to !--- 192.168.2.0 for outbound VPN
.traffic



global (outside) 1 interface
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
The previous statements PAT the Internet traffic !- ---!
-- except for the VPN traffic that uses the IP address
172.17.1.1. route outside 0.0.0.0 0.0.0.0 172.162.1.2 1
!--- Output is suppressed. !--- PHASE 2 CONFIGURATION --
-! !--- The encryption types for Phase 2 are defined
here. crypto ipsec transform-set CISCO esp-des esp-md5-
hmac !--- Define the transform set for Phase 2. crypto
map outside_map 20 match address new !--- Define which
traffic should be sent to the IPsec peer with the !---
access list (new). crypto map outside_map 20 set peer
172.162.1.2 !--- Sets the IPsec peer (remote end point)
crypto map outside_map 20 set transform-set CISCO !---
Sets the IPsec transform set "CISCO" !--- to be used
with the crypto map entry "outside_map" crypto map
outside_map interface outside !--- Specifies the
interface to be used with !--- the settings defined in
this configuration !--- PHASE 1 CONFIGURATION ---! !---
This configuration uses isakmp policy 65535. !--- Policy
```

```
65535 is included in the configuration by default. !---
   These configuration commands define the !--- Phase 1
policy parameters that are used. crypto isakmp identity
     address crypto isakmp enable outside crypto isakmp
   policy 65535 authentication pre-share encryption des
hash md5 group 2 lifetime 86400 tunnel-group 172.162.1.2
   type ipsec-l2l !--- In order to create and manage the
 database of connection-specific records !--- for IPsec-
L2L—IPsec (LAN-to-LAN) tunnels, use the tunnel-group !--
   - command in global configuration mode. !--- For L2L
 connections, the name of the tunnel group must be !---
    .(the IP address of the IPsec peer (remote peer end

            tunnel-group 172.162.1.2 ipsec-attributes
                                        * pre-shared-key
Enter the pre-shared key in order to configure the ---!
  authentication method. telnet timeout 5 ssh timeout 5
 console timeout 0 ! class-map inspection_default match
default-inspection-traffic ! ! policy-map global_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 ! service-policy global_policy global
  Cryptochecksum:33e1e37cd1280d908210dac0cc26e706 : end
```

ASA-2

```
                                ASA-2#show running-config
                                                Saved :
                                                    :
                                          (ASA Version 8.0(3
                                                    !
                                              hostname ASA-2
                        enable password 8Ry2YjIyt7RRXU24 encrypted
                                                   names
                                                    !
                                          interface Ethernet0
                                              nameif outside
                                            security-level 0
                              ip address 172.162.1.2 255.255.255.0
                                                    !
                                          interface Ethernet1
                                               nameif inside
                                          security-level 100
                              ip address 192.168.1.1 255.255.255.0
                                                    !
    Output is suppressed. access-list new extended ---!
        permit ip 192.168.3.0 255.255.255.0 192.168.2.0
 255.255.255.0 !--- This access list (new) is used with
 the crypto map (outside_map) !--- in order to determine
which traffic needs to be encrypted !--- and sent across
                                                .the tunnel
   access-list policy-nat extended permit ip 192.168.1.0
                        255.255.255.0 192.168.2.0 255.255.255.0

    The policy-nat ACL is used with the static !--- ---!
           command in order to match the VPN traffic for
                                               .translation

                                             pager lines 24
                                          mtu outside 1500
                                           mtu inside 1500
```

```
                                                    no failover
                                    asdm image flash:/asdm-615.bin
                                          no asdm history enable
                                               arp timeout 14400



static (inside,outside) 192.168.3.0  access-list policy-
                                                            nat
    This is a Policy NAT statement. !--- The static ---!
   command with the access list (policy-nat), !--- which
       matches the VPN traffic and translates the source
      (192.168.1.0) to !--- 192.168.3.0 for outbound VPN
                                                    .traffic

                                    global (outside) 1 interface
                                 nat (inside) 1 0.0.0.0 0.0.0.0 0 0
The previous statements PAT the Internet traffic !- ---!
         -- except the VPN traffic that uses the outside
     interface IP address. route outside 0.0.0.0 0.0.0.0
  172.162.1.2 1 !--- PHASE 2 CONFIGURATION ---! !--- The
    encryption types for Phase 2 are defined here. crypto
      ipsec transform-set CISCO esp-des esp-md5-hmac !---
        Define the transform set for Phase 2. crypto map
       outside_map 20 match address new !--- Define which
    traffic needs to be sent to the IPsec peer. crypto map
  outside_map 20 set peer 172.162.1.1 !--- Sets the IPsec
  peer. crypto map outside_map 20 set transform-set CISCO
     !--- Sets the IPsec transform set "CISCO" !--- to be
used with the crypto map entry "outside_map". crypto map
         outside_map interface outside !--- Specifies the
    interface to be used with !--- the settings defined in
this configuration. !--- PHASE 1 CONFIGURATION ---! !---
    This configuration uses isakmp policy 65535 !--- which
     is included in the configuration by default. !--- The
       configuration commands here define the !--- Phase 1
  policy parameters that are used. crypto isakmp identity
       address crypto isakmp enable outside crypto isakmp
     policy 65535 authentication pre-share encryption des
           hash md5 group 2 lifetime 86400 !--- Output is
       suppressed. !--- In order to create and manage the
  database of connection-specific !--- records for IPsec-
     L2L–IPsec (LAN-to-LAN) tunnels, use the !--- tunnel-
    group  command in global configuration mode. !--- For
L2L connections, the name of the tunnel group must be !-
                                        .-- the IP address of the IPsec peer


                                  tunnel-group 172.162.1.1 type ipsec-l2l
                               tunnel-group 172.162.1.1 ipsec-attributes
                                                    * pre-shared-key
  Enter the pre-shared key in order to configure the ---!
           authentication method. prompt hostname context
  Cryptochecksum:6b505b4a05c1aee96a71e67c23e71865 : end
```

التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

تدعم أداة مترجم الإخراج (للعملاءالمسجلين فقط) بعض أوامر **show**. استعملت ال OIT in order to شاهدت تحليل من **عرض** أمر إنتاج:

- **show crypto isakmp sa** - يعرض جميع اقترانات أمان IKE الحالية (SAs) في نظير.
- **show crypto ipSec** - يعرض الإعدادات المستخدمة من قبل SAs الحالية.

إظهار الأوامر من ASA-1

```
ASA-1#show crypto isakmp sa

                                                    Active SA: 1
(Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey
                                                  Total IKE SA: 1

                                          IKE Peer: 172.162.1.2   1
                        Type    : L2L               Role    : initiator
                        Rekey   : no                State   : MM_ACTIVE

                                                ASA-1#show crypto ipsec sa
                                                       interface: outside
    Crypto map tag: outside_map, seq num: 20, local addr: 172.162.1.1

    access-list new permit ip 192.168.2.0 255.255.255.0 192.168.3.0

                                                                255.255.2
                                                                      5.0
     (local ident (addr/mask/prot/port): (192.168.2.0/255.255.255.0/0/0
    (remote ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0
                                            current_peer: 172.162.1.2

                  pkts encaps: 9, #pkts encrypt: 9, #pkts digest: 9#
                  pkts decaps: 9, #pkts decrypt: 9, #pkts verify: 9#
                          pkts compressed: 0, #pkts decompressed: 0#
  pkts not compressed: 9, #pkts comp failed: 0, #pkts decomp failed: 0#
   pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0#
PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0#
                                        send errors: 0, #recv errors: 0#

    local crypto endpt.: 172.162.1.1, remote crypto endpt.: 172.162.1.2

                    path mtu 1500, ipsec overhead 58, media mtu 1500
                                  current outbound spi: 0BA6CD7E

                                                      :inbound esp sas
                                          (spi: 0xFB4BD01A (4216049690
                                transform: esp-des esp-md5-hmac none
                                    { ,in use settings ={L2L, Tunnel
                    slot: 0, conn_id: 8192, crypto-map: outside_map
        (sa timing: remaining key lifetime (kB/sec): (3824999/27738
                                                IV size: 8 bytes
                                          replay detection support: Y
                                                     :outbound esp sas
                                           (spi: 0x0BA6CD7E (195480958
                                transform: esp-des esp-md5-hmac none
                                    { ,in use settings ={L2L, Tunnel
                    slot: 0, conn_id: 8192, crypto-map: outside_map
        (sa timing: remaining key lifetime (kB/sec): (3824999/27738
                                                IV size: 8 bytes
                                          replay detection support: Y

ASA-1#show nat
```

```
                                        :NAT policies on Interface inside
 match ip inside 192.168.1.0 255.255.255.0 outside 192.168.3.0 255.255.255.0
                                    static translation to 192.168.2.0
                                translate_hits = 12, untranslate_hits = 5
                                    match ip inside any outside any
              ([dynamic translation to pool 1 (172.162.1.1 [Interface PAT
                                translate_hits = 0, untranslate_hits = 0
                                    match ip inside any inside any
                        (dynamic translation to pool 1 (No matching global
                                translate_hits = 0, untranslate_hits = 0
                                        match ip inside any dmz any
                        (dynamic translation to pool 1 (No matching global
                                translate_hits = 0, untranslate_hits = 0

                                                ASA-1#show xlate

                                                    in use, 1 most used 1
                                    Global 192.168.2.0 Local 192.168.1.0
```

إظهار الأوامر من ASA-2

```
                                                ASA-2#show crypto ipsec sa

                                                        interface: outside
            Crypto map tag: outside_map, seq num: 20, local addr: 172.162.1.2

            access-list new permit ip 192.168.3.0 255.255.255.0 192.168.2.0

                                                                    255.255.25
                                                                          5.0
             (local ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0
            (remote ident (addr/mask/prot/port): (192.168.2.0/255.255.255.0/0/0
                                                    current_peer: 172.162.1.1

                                pkts encaps: 9, #pkts encrypt: 9, #pkts digest: 9#
                                pkts decaps: 9, #pkts decrypt: 9, #pkts verify: 9#
                                    pkts compressed: 0, #pkts decompressed: 0#
           pkts not compressed: 9, #pkts comp failed: 0, #pkts decomp failed: 0#
            pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0#
        PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0#
                                    send errors: 0, #recv errors: 0#

             local crypto endpt.: 172.162.1.2, remote crypto endpt.: 172.162.1.1

                                path mtu 1500, ipsec overhead 58, media mtu 1500
                                    current outbound spi: FB4BD01A

                                                    :inbound esp sas
                                            (spi: 0x0BA6CD7E (195480958
                                transform: esp-des esp-md5-hmac none
                                    { ,in use settings ={L2L, Tunnel
                            slot: 0, conn_id: 8192, crypto-map: outside_map
                  (sa timing: remaining key lifetime (kB/sec): (4274999/26902
                                                    IV size: 8 bytes
                                            replay detection support: Y
                                                        :outbound esp sas
                                              (spi: 0xFB4BD01A (4216049690
                                transform: esp-des esp-md5-hmac none
                                    { ,in use settings ={L2L, Tunnel
                            slot: 0, conn_id: 8192, crypto-map: outside_map
```

```
(sa timing: remaining key lifetime (kB/sec): (4274999/26902
                                                IV size: 8 bytes
                                        replay detection support: Y


ASA-2#show crypto isakmp sa

                                                        Active SA: 1
(Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey
                                                      Total IKE SA: 1

                                                IKE Peer: 172.162.1.1   1
Type    : L2L                             Role    : responder
Rekey   : no                              State   : MM_ACTIVE
```

استكشاف الأخطاء وإصلاحها

مسح الاقترانات الأمنية

عند أستكشاف أخطاء SA وإصلاحها، تأكد من مسح رسائل SA الموجودة بعد إجراء تغيير. في الوضع ذي الامتيازات ل PIX، أستخدم الأوامر التالية:

- **مسح تشفير IPsec** - يحذف شبكات IPsec النشطة.
- **مسح التشفير isakmp sa** - يحذف شبكات IKE النشطة.

أوامر استكشاف الأخطاء وإصلاحها

تدعم أداة مترجم الإخراج (للعملاءالمسجلين فقط) بعض أوامر show. استعملت ال OIT in order to شاهدت تحليل من **عرض** أمر إنتاج.

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.

معلومات ذات صلة

- حلول أستكشاف أخطاء الشبكة الخاصة الظاهرية (VPN) عبر بروتوكول IPsec للوصول عن بعد و L2L الأكثر شيوعا
- PIX 7.0 وإعادة توجيه المنفذ (إعادة توجيه) جهاز الأمان القابل للتكيف مع أوامر NAT و global و static و access-list و channel
- PIX/ASA 7.x و FWSM: بيانات NAT و PAT
- أجهزة الأمان Cisco ASA 5500 Series Security Appliances
- أجهزة الأمان Cisco PIX 500 Series Security Appliances
- مفاوضة IPSec/بروتوكولات IKE
- 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).