PIX/ASA 7.x والإصدارات الأحدث: شبكة VPN سهلة مع ASA 5500 للاتصال النفقي المنقسم كخادم و Cisco 871 كمثال التكوين عن بعد ل VPN السهل

المحتويات

المقدمة

يقدم هذا المستند نموذجا لتكوين IPsec بين جهاز الأمان القابل للتكيف (5520 ASA) من Cisco وموجه Cisco 871 باستخدام شبكة VPN سهلة. يعمل ASA 5520 كخادم VPN سهل ويعمل الموجه Cisco 871 كالعميل البعيد VPN السهل. بينما يستخدم هذا التكوين جهاز ASA 5520 الذي يشغل برنامج ASA الإصدار 7.1(1)، يمكنك أيضا إستخدام هذا التكوين لأجهزة جدار حماية PIX التي تشغل الإصدار 7.1 من نظام تشغيل PIX والإصدارات الأحدث.

من أجل تكوين موجه Cisco IOS® كموجه EzVPN في وضع امتداد الشبكة (NEM) الذي يتصل بمركز Cisco VPN 3000، ارجع إلى تكوين عميل Cisco EzVPN على Cisco IOS باستخدام مركز VPN 3000.

لتكوين IPsec بين عميل الأجهزة البعيدة ل VPN سهل CISCO IOS وخادم PIX سهل VPN، ارجع إلى عميل الأجهزة البعيدة VPN سهل IOS إلى مثال تكوين خادم VPN سهل PIX.

أحلت in order to شكلت cisco 7200 مسحاج تخديد ك EzVPN و ال cisco 871 مسحاج تخديد ك ال VPN بعيد سهل، 7200 ييسر VPN نادل إلى 871 ييسر VPN تشكيل بعيد مثال.

المتطلبات الأساسية

المتطلبات

تأكد من توفر فهم أساسي لديك لأنظمة تشغيل IPsec وASA 7.x.

المكونات المستخدمة

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

- خادم VPN السهل هو ASA 5520 الذي يشغل الإصدار 7.1(1).
- ال VPN سهل جهاز عميل cisco 871 مسحاج تخديد أن يركض cisco ios ® برمجية إطلاق T1(4)12.4.

ملاحظة: يشغل الإصدار x.7 من Cisco ASA 5500 Series إصدار برنامج مماثل يظهر في الإصدار x.7 من PIX. تنطبق التكوينات الواردة في هذا المستند على كل من سطور المنتجات.

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.

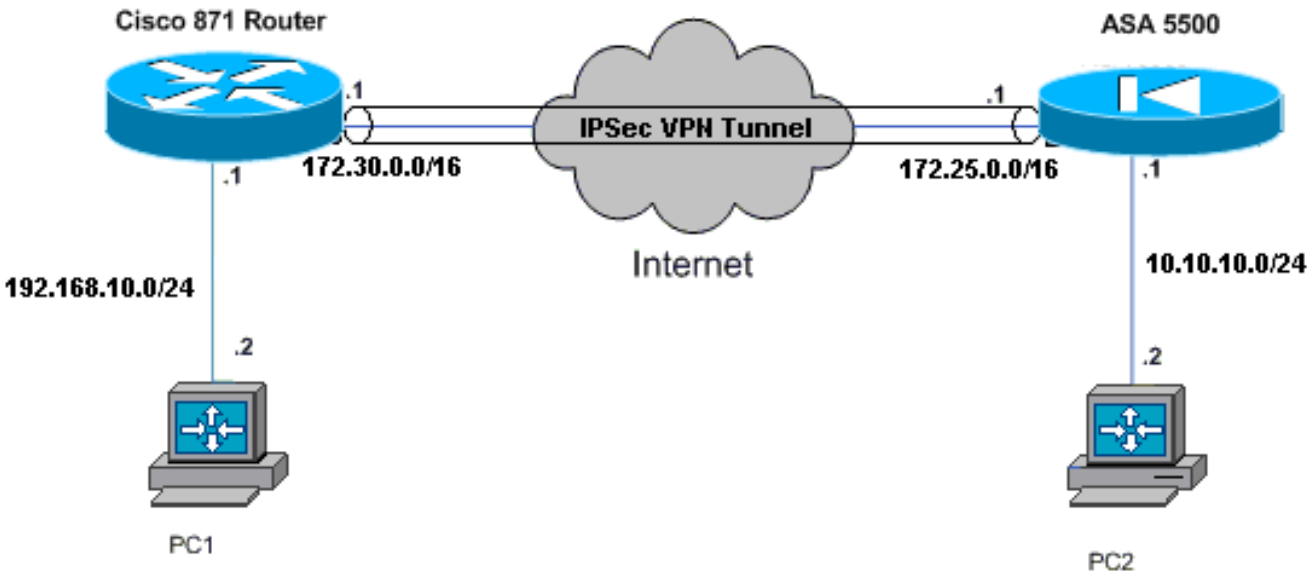
التكوين

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

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

الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة التالي:



التكوينات

يستخدم هذا المستند التكوينات التالية:

- Cisco ASA 5520
- موجّه Cisco 871

Cisco ASA 5520

```
ciscoasa#show run
Saved :
:
(ASA Version 7.1(1
!
hostname ciscoasa
!
interface GigabitEthernet0/0
 nameif outside
 security-level 0
 ip address 172.25.171.1 255.255.0.0
!
interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 10.10.10.1 255.255.255.0
!
interface Management0/0
 shutdown
 no nameif
 no security-level
 no ip address
Output is suppressed. access-list no-nat extended ---!
```

```
        permit ip 10.10.10.0 255.255.255.0 192.168.10.0
    255.255.255.0 access-list ezvpn extended permit ip
   10.10.10.0 255.255.255.0 192.168.10.0 255.255.255.0

    access-list Split_Tunnel_List remark The corporate
                                        network behind the ASA
access-list Split_Tunnel_List standard permit 10.10.10.0
                                        255.255.255.0
                    nat (inside) 0 access-list no-nat
                 access-group OUT in interface outside
          route outside 0.0.0.0 0.0.0.0 172.25.171.2 1
  Use the group-policy attributes command in !--- ---!
   global configuration mode to enter the group-policy
                                        .attributes mode

                group-policy DfltGrpPolicy attributes
                                        banner none
                                    wins-server none
                                     dns-server none
                                  dhcp-network-scope none
                                    vpn-access-hours none
                                vpn-simultaneous-logins 3
                                      vpn-idle-timeout 30
                                 vpn-session-timeout none
                                        vpn-filter none
                                vpn-tunnel-protocol IPSec
                                  password-storage enable
                                        ip-comp disable
                                    re-xauth disable
                                     group-lock none
                                         pfs disable
                                    ipsec-udp enable
                                ipsec-udp-port 10000

                    split-tunnel-policy tunnelspecified

    split-tunnel-network-list value Split_Tunnel_List
                                  default-domain none
                                       split-dns none
                    secure-unit-authentication disable
                           user-authentication disable
                user-authentication-idle-timeout 30
                                ip-phone-bypass disable
                                    leap-bypass disable
  Network Extension mode allows hardware clients to ---!
   present a single, !--- routable network to the remote
        private network over the VPN tunnel. nem enable
                        backup-servers keep-client-config
                                  client-firewall none
                                client-access-rule none
    username cisco password 3USUcOPFUiMCO4Jk encrypted
                                      http server enable
                                 no snmp-server location
                                  no snmp-server contact
   snmp-server enable traps snmp authentication linkup
                                      linkdown coldstart
These are IPsec Phase I and Phase II parameters. !- ---!
  -- The parameters have to match in order for !--- the
   IPsec tunnel to come up. crypto ipsec transform-set
                                  mySET esp-des esp-md5-hmac
crypto dynamic-map myDYN-MAP 5 set transform-set mySET
    crypto map myMAP 60 ipsec-isakmp dynamic myDYN-MAP
                    crypto map myMAP interface outside
                                  isakmp identity address
```

```
isakmp enable outside
isakmp policy 1 authentication pre-share
isakmp policy 1 encryption 3des
isakmp policy 1 hash md5
isakmp policy 1 group 2
isakmp policy 1 lifetime 86400

tunnel-group DefaultRAGroup general-attributes
default-group-policy DfltGrpPolicy

tunnel-group DefaultRAGroup ipsec-attributes
* pre-shared-key

telnet timeout 5
ssh timeout 5
console timeout 0
!
end :
#ciscoasa
```

موجّه Cisco 871

```
C871#show running-config
Current configuration : 1639 bytes
!
version 12.4
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname C871
!
boot-start-marker
boot-end-marker
!
!
ip cef
!
Creates a Cisco Easy VPN Remote configuration and ---!
enters the !--- Cisco Easy VPN Remote configuration
mode. crypto ipsec client ezvpn ASA
The IPsec VPN tunnel is automatically connected ---!
when the Cisco !--- Easy VPN Remote feature is
configured on an interface. connect auto
The group name should match the remote group name. ---!
group DefaultRAGroup key cisco
Specifies that the router should become a remote ---!
extension of the !--- enterprise network at the other
end of the VPN connection. mode network-extension
Sets the peer IP address or hostname for the VPN ---!
connection. peer 172.25.171.1
Specifies how the Easy VPN Client handles extended ---!
authentication (Xauth) requests. xauth userid mode
interactive
Output is suppressed. ! interface FastEthernet0 ! ---!
interface FastEthernet1 ! interface FastEthernet2 !
interface FastEthernet3 ! !--- Assigns a Cisco Easy VPN
Remote configuration to an outside interface. interface
FastEthernet4 ip address 172.30.171.1 255.255.0.0 ip
access-group 101 in no ip redirects no ip unreachables
no ip proxy-arp ip nat outside ip virtual-reassembly ip
route-cache flow duplex auto speed auto crypto ipsec
```

```
client ezvpn ASA
!
Assigns a Cisco Easy VPN Rremote configuration to ---!
an outside interface. interface Vlan1 ip address
192.168.10.1 255.255.255.0 ip access-group 100 out no ip
redirects no ip unreachables no ip proxy-arp ip nat
inside ip virtual-reassembly ip route-cache flow ip tcp
adjust-mss 1452 crypto ipsec client ezvpn ASA inside
!
ip classless
ip route 0.0.0.0 0.0.0.0 172.30.171.2
!
Enables NAT on the inside source address. ip nat ---!
inside source route-map EzVPN1 interface FastEthernet4
overload
!
access-list 100 permit ip any any
access-list 101 permit ip any any
access-list 103 permit ip 192.168.10.0 0.0.0.255 any
!
route-map EzVPN1 permit 1
match ip address 103
!
end
C871#
```

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** .

ما إن يشكل أنت كلا أداة، ال cisco 871 مسحاج تخديد يحاول أن setup ال VPN نفق ب يتصل ASA 5520 تلقائيا يستعمل النظير عنوان. بعد تبادل معلمات ISAKMP الأولية، يعرض الموجه هذه الرسالة:

```
Pending XAuth Request, Please enter the
following command: crypto ipsec client ezvpn xauth
```

يجب إدخال الأمر **crypto ipSec client ezVPN xauth** الذي يطالبك باسم مستخدم وكلمة مرور. هذا ينبغي طابقت ال username وكلمة يشكل على ال ASA 5520. بمجرد الموافقة على اسم المستخدم وكلمة المرور من قبل كلا النظيرين، يتم الاتفاق على باقي المعلمات ويتم ظهور نفق IPsec VPN.

```
:EZVPN(ASA): Pending XAuth Request, Please enter the following command

EZVPN: crypto ipsec client ezvpn xauth

.Enter the crypto ipsec client ezvpn xauth command ---!

crypto ipsec client ezvpn xauth

Enter Username and Password.: cisco
Password: : test
```

أستخدم هذه الأوامر للتحقق من عمل النفق بشكل صحيح على كل من ASA 5520 وموجه 871 من Cisco:

- show crypto isakmp sa — يعرض جميع اقترانات أمان IKE (SAs) الحالية في نظير. تشير حالة QM_IDLE إلى أن SA لا يزال مصدقا عليه مع نظيره ويمكن إستخدامه لمبادلات الوضع السريع اللاحقة.

```
show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot status
QM_IDLE           1011    0 ACTIVE    172.30.171.1    172.25.171.1

IPv6 Crypto ISAKMP SA
```

- show crypto ipSec — يعرض الإعدادات المستخدمة من قبل موجهات الخدمات (SAs) الحالية. تحقق من عناوين IP النظيرة والشبكات التي يمكن الوصول إليها عند كل من النهايات المحلية والبعيدة ومجموعة التحويل التي يتم إستخدامها. هناك نوعان من شبكات SA لبروتوكول أمان التضمين (ESP)، واحد في كل إتجاه. نظرا لعدم إستخدام مجموعات تحويل رأس المصادقة (AH)، فإنها فارغة.

```
show crypto ipsec sa

interface: FastEthernet4
Crypto map tag: FastEthernet4-head-0, local addr 172.30.171.1

(protected vrf: (none
(local  ident (addr/mask/prot/port): (192.168.10.0/255.255.255.0/0/0
(remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0
current_peer 172.25.171.1 port 500
{,PERMIT, flags={origin_is_acl
pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0#
pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0#
pkts compressed: 0, #pkts decompressed: 0#
pkts not compressed: 0, #pkts compr. failed: 0#
pkts not decompressed: 0, #pkts decompress failed: 0#
send errors 0, #recv errors 0#

local crypto endpt.: 172.30.171.1, remote crypto endpt.: 172.25.171.1
path mtu 1500, ip mtu 1500
(current outbound spi: 0x2A9F7252(715092562

:inbound esp sas
(spi: 0x42A887CB(1118341067
, transform: esp-des esp-md5-hmac
{ ,in use settings ={Tunnel
conn id: 39, flow_id: C87X_MBRD:39, crypto map: FastEthernet4-head-0
(sa timing: remaining key lifetime (k/sec): (4389903/28511
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE

:inbound ah sas

:inbound pcp sas

:outbound esp sas
(spi: 0x2A9F7252(715092562
, transform: esp-des esp-md5-hmac
{ ,in use settings ={Tunnel
conn id: 40, flow_id: C87X_MBRD:40, crypto map: FastEthernet4-head-0
(sa timing: remaining key lifetime (k/sec): (4389903/28503
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE
```

```
:outbound ah sas

:outbound pcp sas
```

- show ipsEc sa — يعرض الإعدادات المستخدمة من قبل موجهات الخدمات (SAs) الحالية. تحقق من عناوين IP النظيرة والشبكات التي يمكن الوصول إليها عند كل من النهايات المحلية والبعيدة ومجموعات التحويل التي يتم إستخدامها. يوجد إثنان من ESP SAs، واحد في كل إتجاه.

```
ciscoasa#show ipsec sa
interface: outside
Crypto map tag: myDYN-MAP, seq num: 5, local addr: 172.25.171.1

(local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0
(remote ident (addr/mask/prot/port): (192.168.10.0/255.255.255.0/0/0
current_peer: 172.30.171.1, username: cisco
dynamic allocated peer ip: 0.0.0.0

pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0#
pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0#
pkts compressed: 0, #pkts decompressed: 0#
pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0#
send errors: 0, #recv errors: 0#

local crypto endpt.: 172.25.171.1, remote crypto endpt.: 172.30.171.1

path mtu 1500, ipsec overhead 60, media mtu 1500
current outbound spi: 42A887CB

:inbound esp sas
(spi: 0x2A9F7252 (715092562
transform: esp-des esp-md5-hmac
{ ,in use settings ={RA, Tunnel
slot: 0, conn_id: 8, crypto-map: myDYN-MAP
sa timing: remaining key lifetime (sec): 28648
IV size: 8 bytes
replay detection support: Y
:outbound esp sas
(spi: 0x42A887CB (1118341067
transform: esp-des esp-md5-hmac
{ ,in use settings ={RA, Tunnel
slot: 0, conn_id: 8, crypto-map: myDYN-MAP
sa timing: remaining key lifetime (sec): 28644
IV size: 8 bytes
replay detection support: Y
```

- show isakmp sa — يعرض جميع شبكات IKE الحالية في نظير. تشير حالة AM_ACTIVE إلى إستخدام الوضع المتميز لتبادل المعلمات.

```
ciscoasa#show 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: 172.30.171.1    1
Type    : user            Role    : responder
Rekey   : no              State   : AM_ACTIVE
```

استكشاف الأخطاء وإصلاحها

أستخدم هذا القسم لاستكشاف أخطاء التكوين وإصلاحها.

- أستكشاف أخطاء الموجه وإصلاحها
- أستكشاف أخطاء ASA وإصلاحها

تدعم أداة مترجم الإخراج (للعملاءالمسجلين 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**.

أستكشاف أخطاء الموجه وإصلاحها

- **debug crypto isakmp**—يعرض مفاوضات ISAKMP للمرحلة 1 من IKE.
- **debug crypto ips**—يعرض مفاوضات IPsec للمرحلة 2 من IKE.

أستكشاف أخطاء ASA وإصلاحها

- **debug crypto isakmp 127**—يعرض مفاوضات ISAKMP للمرحلة 1 من IKE.
- **debug crypto isec 127**—يعرض مفاوضات IPsec للمرحلة 2 من IKE.

معلومات ذات صلة

- شبكة VPN سهلة مع ASA 5500 كخادم و PIX 506e كمثال تكوين العميل (NEM)
- دعم منتجات أجهزة الأمان القابلة للتكيف ASA 5500 Series من Cisco
- دعم منتجات الموجهات من السلسلة Cisco 800
- 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).