تكوين VPN بين منتجات SONICWALL TZ ومثال تكوين جهاز الأمان Cisco ASA

المحتويات

المقدمة

يوضح هذا المستند كيفية تكوين نفق IPsec بمفاتيح مشتركة مسبقا للاتصال بين شبكتين خاصتين باستخدام كل من الوضعين المتميز والرئيسي. في هذا المثال، شبكات الاتصال هي الشبكة الخاصة x.192.168.1 داخل جهاز الأمان Cisco Security Appliance (PIX/ASA) والشبكة الخاصة x.172.22.1 داخل جدار حماية SonicwallTM TZ170.

المتطلبات الأساسية

المتطلبات

تأكد من استيفاء المتطلبات التالية قبل أن تحاول إجراء هذا التكوين:

- يجب أن تتدفق حركة المرور من داخل جهاز الأمان من Cisco ومن داخل Sonicwall TZ170 إلى الإنترنت (ممثلة هنا بشبكات x.x.x.10) قبل بدء هذا التكوين.
- يجب أن يكون المستخدمون على دراية بتفاوض IPsec. يمكن تقسيم هذه العملية إلى خمس خطوات تتضمن مرحلتين من عملية تبادل مفتاح الإنترنت (IKE).يتم بدء نفق IPsec بواسطة حركة مرور مثيرة للاهتمام. تعتبر حركة المرور مثيرة للاهتمام عندما تنتقل بين نظائر IPsec.في المرحلة الأولى من IKE، يتفاوض نظراء IPsec على سياسة اقتران أمان IKE (SA) التي تم إنشاؤها. بمجرد مصادقة النظراء، يتم إنشاء نفق آمن باستخدام بروتوكول إدارة المفاتيح وارتباط أمان الإنترنت (ISAKMP).في المرحلة 2 من IKE، يستخدم نظراء IPsec النفق الآمن والمصدع للتفاوض على تحويلات IPsec SA. يحدد التفاوض على السياسة المشتركة كيفية إنشاء نفق IPsec.يتم إنشاء نفق IPsec ويتم نقل البيانات بين نظائر IPsec استنادا إلى معلمات IPsec التي تم تكوينها في

مجموعات تحويل IPsec.ينتهي نفق IPsec عند حذف وحدات IPsec SAs أو عند انتهاء صلاحية مدة حياتها.

المكونات المستخدمة

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

- الإصدار 6.3(5) من Cisco PIX 515E
- Cisco PIX 515، الإصدار 7.0(2)
- Sonicwall TZ170، SonicOS Standard 2.2.0.1

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.

المنتجات ذات الصلة

كما يمكن إستخدام هذا التكوين مع إصدارات الأجهزة والبرامج التالية:

- يمكن إستخدام تكوين PIX 6.3(5) مع جميع منتجات جدار حماية Cisco PIX الأخرى التي تشغل هذا الإصدار من البرنامج (506، 501 PIX، وما إلى ذلك)
- يمكن إستخدام تكوين PIX/ASA 7.0(2) فقط على الأجهزة التي تشغل قطار PIX 7.0 من البرامج (باستثناء 501 و 506 وربما بعض الإصدارات 515s الأقدم) بالإضافة إلى ASA من السلسلة Cisco 5500.

الاصطلاحات

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

التكوين

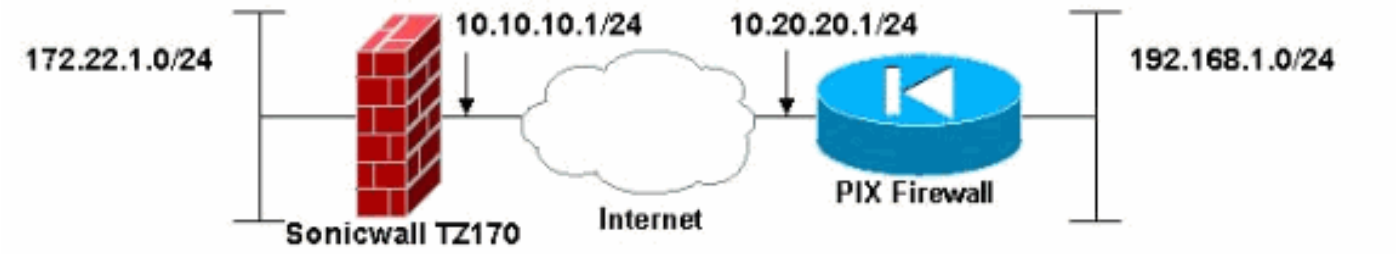
في هذا القسم، تُقدّم لك معلومات تكوين الميزات الموضحة في هذا المستند.

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

ملاحظة: في وضع الهجوم ل IPsec، من الضروري أن يقوم Sonicwall ببدء نفق IPsec إلى PIX. يمكنك رؤية ذلك عند تحليل تصحيح الأخطاء لهذا التكوين. وهذا أمر متأصل في طريقة عمل الوضع العدواني ل IPsec.

الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة التالي:

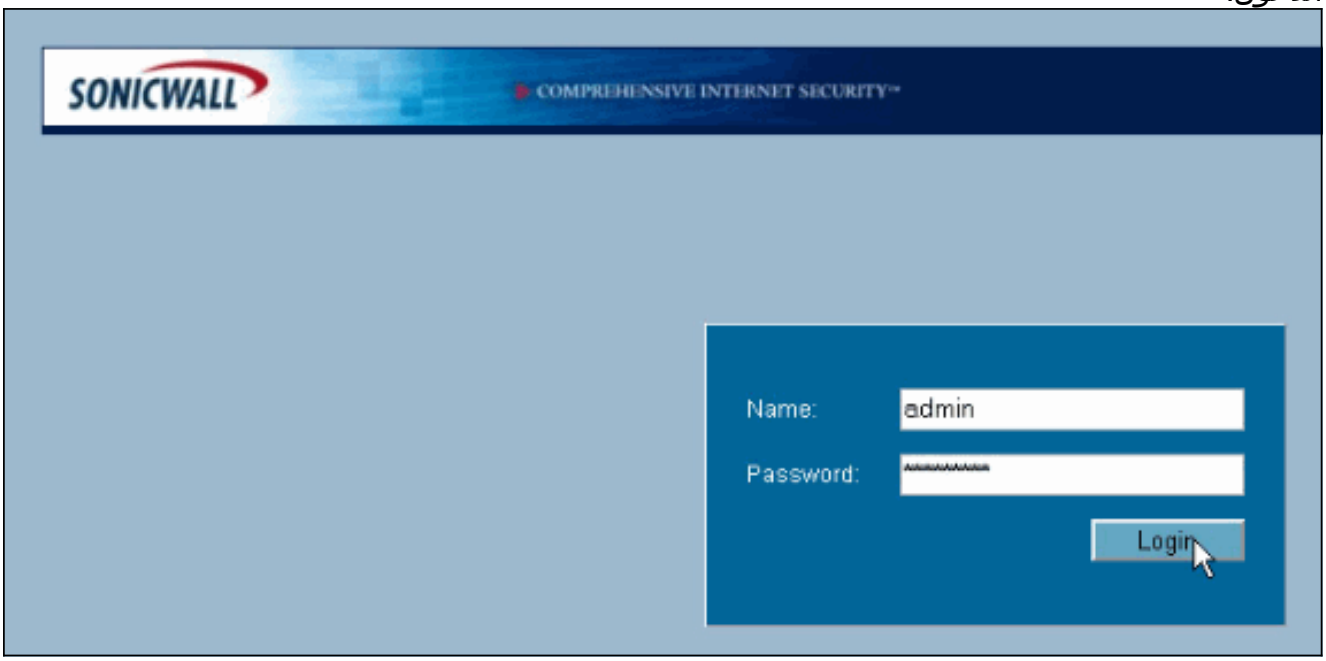


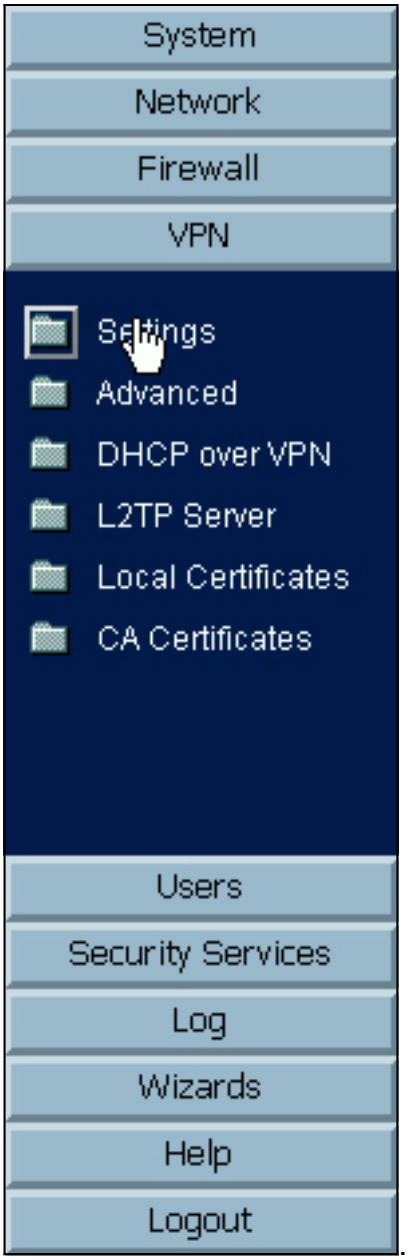
تكوين Sonicwall

يتم إجراء تكوين Sonicwall TZ170 من خلال واجهة مستندة إلى الويب.

أكمل الخطوات التالية:

1. قم بالاتصال بعنوان IP الخاص بالموجه على إحدى الواجهات الداخلية باستخدام مستعرض ويب قياسي.يؤدي ذلك إلى ظهور نافذة تسجيل
الدخول.

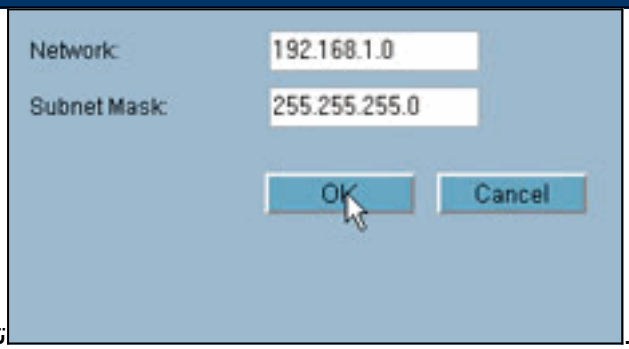


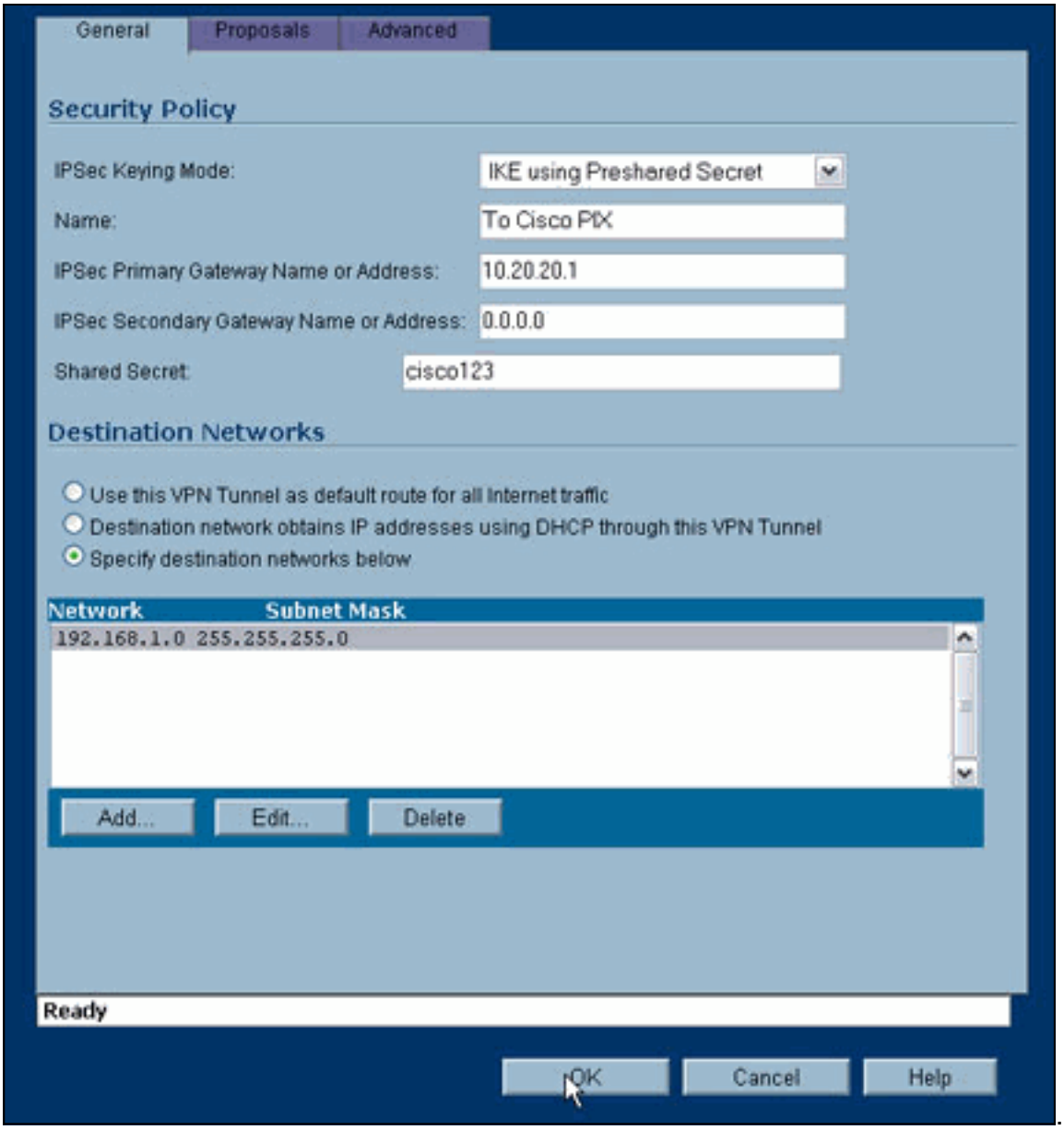


2. قم بتسجيل الدخول إلى جهاز Sonicwall وحدد **VPN > إعدادات**.
3. دخلت العنوان من ال VPN نظير وال مبرد سر أن يكون استعملت. طقطقة **يضيف** تحت غاية

شبكة.

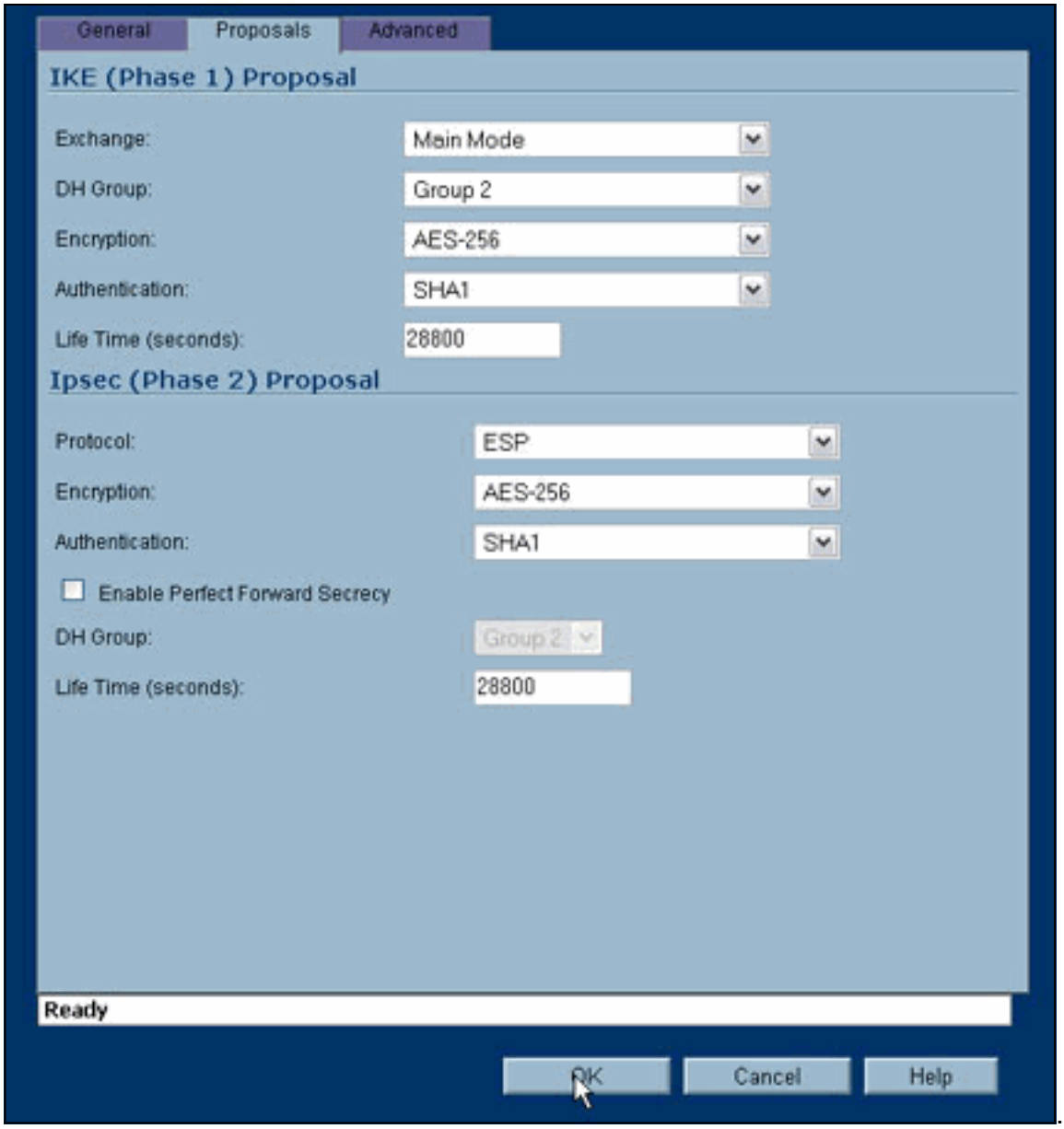
4. دخلت الغاية شبكة. تظهر نافذة





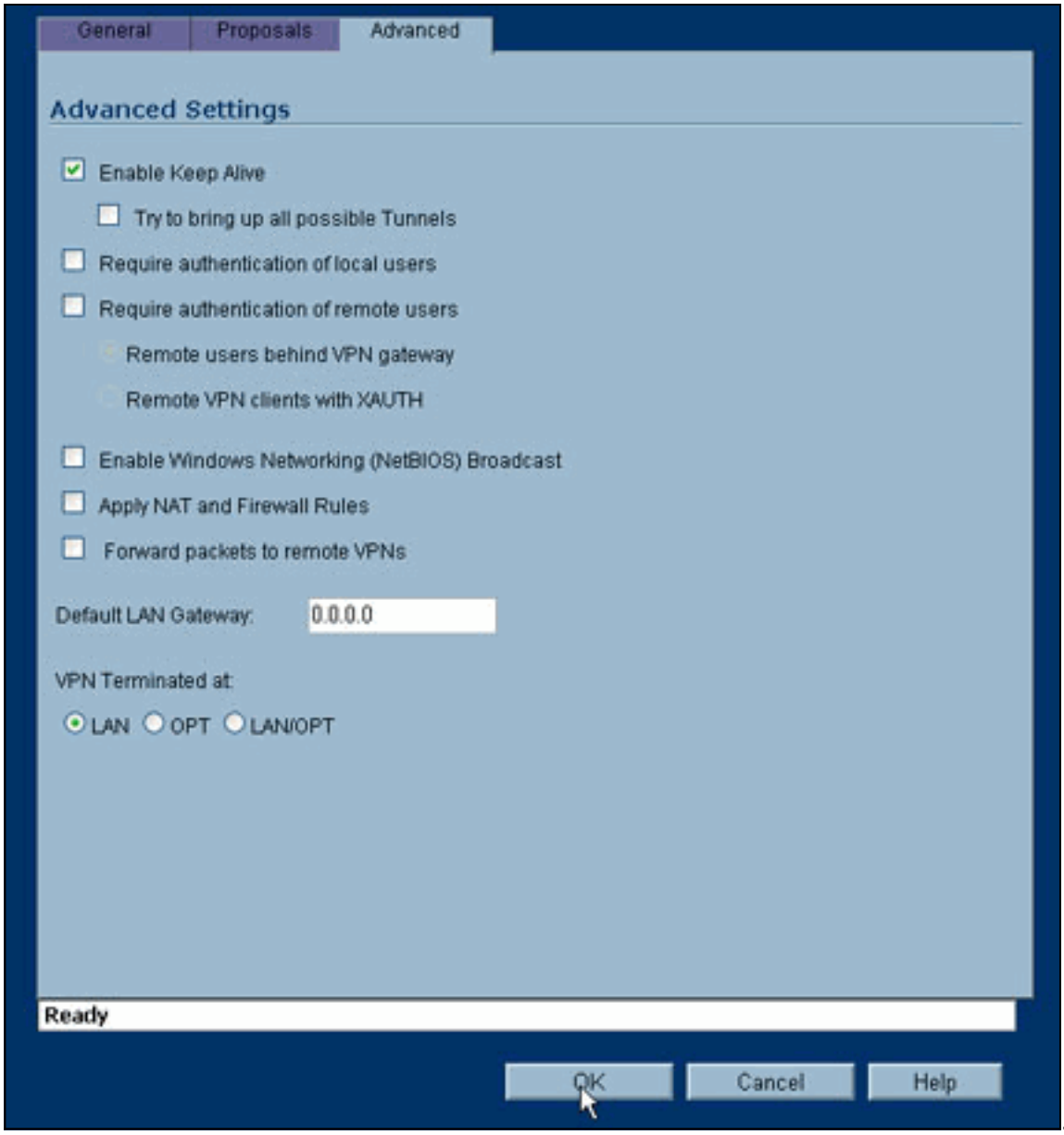
الإعدادات.

5. انقر فوق علامة التبويب عروض في أعلى نافذة الإعدادات.
6. حدد التبادل الذي تخطط لاستخدامه لهذا التكوين (الوضع الرئيسي أو الوضع المتميز) مع باقي إعدادات المرحلة 1 والمرحلة 2.يستخدم مثال التكوين هذا تشفير AES-256 لكلا المرحلتين مع خوارزمية تجزئة SHA1 للمصادقة ومجموعة 1024 بت 2 Diffie-Hellman لنهج



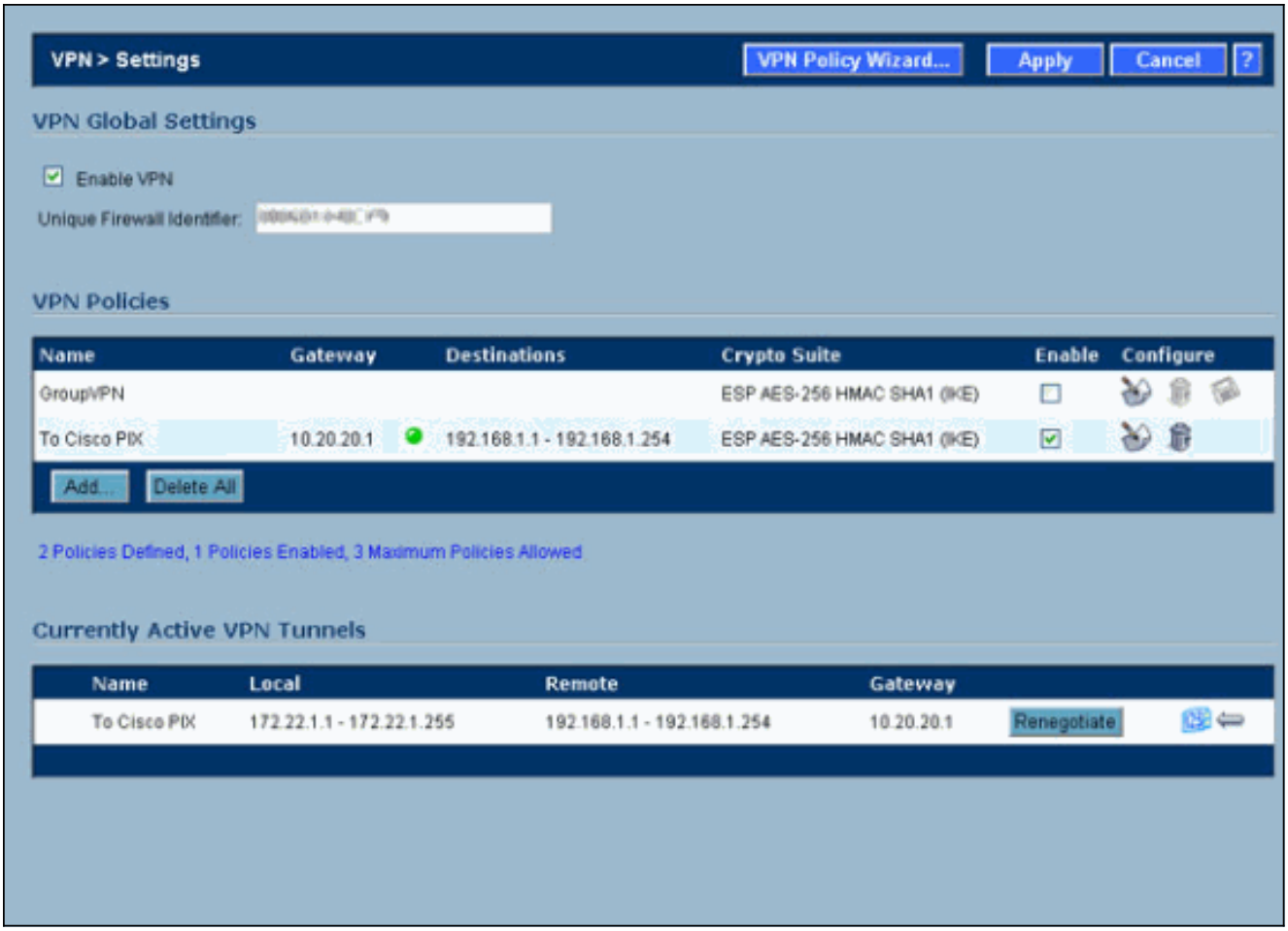
.IKE

7. انقر فوق علامة التبويب متقدمة.هناك خيارات إضافية قد ترغب في تكوينها ضمن علامة التبويب هذه. هذه هي الإعدادات المستخدمة لهذا النموذج من



التكوين.

8. وانقر فوق OK.بمجرد اكتمال هذا التكوين والتكوين على PIX البعيد، يجب أن يكون إطار "الإعدادات" مماثلا لنافذة "الإعدادات"
هذه.



تكوين الوضع الرئيسي ل IPsec

يستخدم هذا القسم التكوينات التالية:

- الإصدار 6.3(5) من Cisco PIX 515e
- Cisco PIX 515، الإصدار 7.0(2)

الإصدار 6.3(5) من Cisco PIX 515e

```
pix515e-635#show running-config
Saved :
:
(PIX Version 6.3(5
Sets the hardware speed to auto on both interfaces. ---!
  interface ethernet0 auto interface ethernet1 auto !---
     Specifies the inside and outside interfaces. nameif
     ethernet0 outside security0 nameif ethernet1 inside
  security100 enable password 8Ry2YjIyt7RRXU24 encrypted
  passwd 2KFQnbNIdI.2KYOU encrypted hostname pix515e-635
fixup protocol dns maximum-length 512 fixup protocol ftp
21 fixup protocol h323 h225 1720 fixup protocol h323 ras
 1718-1719 fixup protocol http 80 fixup protocol rsh 514
   fixup protocol rtsp 554 fixup protocol sip 5060 fixup
  protocol sip udp 5060 fixup protocol skinny 2000 fixup
       protocol smtp 25 fixup protocol sqlnet 1521 fixup
  protocol tftp 69 names !--- Specifies the traffic that
  can pass through the IPsec tunnel. access-list pixtosw
          permit ip 192.168.1.0 255.255.255.0 172.22.1.0
255.255.255.0 pager lines 24 mtu outside 1500 mtu inside
  1500 !--- Sets the inside and outside IP addresses and
```

```
            subnet masks. ip address outside 10.20.20.1
            255.255.255.0 ip address inside 192.168.1.1
255.255.255.0 ip audit info action alarm ip audit attack
  action alarm pdm history enable arp timeout 14400 !---
   Instructs PIX to perform PAT on the IP address on the
    outside interface. global (outside) 1 interface !---
Specifies addresses to be exempt from NAT (traffic to be
      tunneled). nat (inside) 0 access-list pixtosw !---
    Specifies which addresses should use NAT (all except
those exempted). nat (inside) 1 0.0.0.0 0.0.0.0 0 0 !---
   Specifies the default route on the outside interface.
route outside 0.0.0.0 0.0.0.0 10.20.20.2 1 timeout xlate
    3:00:00 timeout conn 1:00:00 half-closed 0:10:00 udp
  0:02:00 rpc 0:10:00 h225 1:00:00 timeout h323 0:05:00
 mgcp 0:05:00 sip 0:30:00 sip_media 0:02:00 timeout sip-
     disconnect 0:02:00 sip-invite 0:03:00 timeout uauth
    0:05:00 absolute aaa-server TACACS+ protocol tacacs+
     aaa-server TACACS+ max-failed-attempts 3 aaa-server
   TACACS+ deadtime 10 aaa-server RADIUS protocol radius
      aaa-server RADIUS max-failed-attempts 3 aaa-server
   RADIUS deadtime 10 aaa-server LOCAL protocol local no
 snmp-server location no snmp-server contact snmp-server
 community public no snmp-server enable traps floodguard
   enable !--- Implicit permit for all packets that come
 from IPsec tunnels. sysopt connection permit-ipsec !---
   PHASE 2 CONFIGURATION: !--- Defines the transform set
         for Phase 2 encryption and authentication. !---
    Austinlab is the name of the transform set that uses
        aes-256 encryption !--- as well as the SHA1 hash
                             .algorithm for authentication

   crypto ipsec transform-set austinlab esp-aes-256 esp-
                                                 sha-hmac

   Specifies IKE is used to establish the IPsec SAs ---!
     for the map "maptosw". crypto map maptosw 67 ipsec-
isakmp !--- Specifies the ACL "pixtosw" to use with this
  map . crypto map maptosw 67 match address pixtosw !---
       Specifies the IPsec peer for this map. crypto map
       maptosw 67 set peer 10.10.10.1 !--- Specifies the
         transform set to use. crypto map maptosw 67 set
 transform-set austinlab !--- Specifies the interface to
 use with this map. crypto map maptosw interface outside
 !--- PHASE 1 CONFIGURATION !--- Specifies the interface
                                .to use for the IPsec tunnel

                                      isakmp enable outside

   Specifies the preshared key and the addresses to ---!
use with that key. !--- In this case only one address is
        used with the preshared key cisco123. isakmp key
******** address 10.10.10.1 netmask 255.255.255.255 !---
       Defines how the PIX identifies itself in !--- IKE
 negotiations (IP address in this case). isakmp identity
    address !--- These five commands specify the Phase 1
     configuration settings !--- specific to this sample
configuration. isakmp policy 13 authentication pre-share
    isakmp policy 13 encryption aes-256 isakmp policy 13
      hash sha isakmp policy 13 group 2 isakmp policy 13
   lifetime 28800 telnet timeout 5 ssh timeout 5 console
                                  timeout 0 terminal width 80
   Cryptochecksum:07a3815d59db9965b72c7d8a7aaf7f5f : end
                                                 pix515e-635#
```

Cisco PIX 515، الإصدار 7.0(2)

```
pix515-702#show running-config
Saved :
:
(PIX Version 7.0(2
names
!

PIX 7 uses an interface configuration mode similar ---!
      to Cisco IOS®. !--- This output configures the IP
   address, interface name, !--- and security level for
interfaces Ethernet0 and Ethernet1. interface Ethernet0
  nameif outside security-level 0 ip address 10.20.20.1
      255.255.255.0 ! interface Ethernet1 nameif inside
security-level 100 ip address 192.168.1.1 255.255.255.0
  ! 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 pix515-702 domain-name cisco.com ftp
  mode passive !--- Specifies the traffic that can pass
 through the IPsec tunnel. access-list pixtosw extended
        permit ip 192.168.1.0 255.255.255.0 172.22.1.0
255.255.255.0 pager lines 24 mtu inside 1500 mtu outside
     1500 no failover monitor-interface inside monitor-
    interface outside no asdm history enable arp timeout
       14400 !--- Instructs PIX to perform PAT on the IP
    address on the outside interface. global (outside) 1
interface !--- Specifies addresses to be exempt from NAT
    (traffic to be tunneled). nat (inside) 0 access-list
   pixtosw !--- Specifies which addresses should use NAT
     (all except those exempted). nat (inside) 1 0.0.0.0
 0.0.0.0 !--- Specifies the default route on the outside
   interface. route outside 0.0.0.0 0.0.0.0 10.20.20.2 1
  timeout xlate 3:00:00 timeout conn 1:00:00 half-closed
 0:10:00 udp 0:02:00 icmp 0:00:02 timeout sunrpc 0:10:00
 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 timeout mgcp-pat
     0:05:00 sip 0:30:00 sip_media 0:02:00 timeout uauth
 0:05:00 absolute no snmp-server location no snmp-server
     contact snmp-server enable traps snmp !--- Implicit
    permit for all packets that come from IPsec tunnels.
            sysopt connection permit-ipsec !--- PHASE 2
CONFIGURATION !--- Defines the transform set for Phase 2
    encryption and authentication. !--- Austinlab is the
  name of the transform set that uses aes-256 encryption
            !--- as well as the SHA1 hash algorithm for
                                              .authentication

   crypto ipsec transform-set austinlab esp-aes-256 esp-
                                                 sha-hmac

    Specifies the ACL pixtosw to use with this map. ---!
        crypto map maptosw 67 match address pixtosw !---
       Specifies the IPsec peer for this map. crypto map
        maptosw 67 set peer 10.10.10.1 !--- Specifies the
         transform set to use. crypto map maptosw 67 set
 transform-set austinlab !--- Specifies the interface to
use with this map . crypto map maptosw interface outside
     !--- PHASE 1 CONFIGURATION !--- Defines how the PIX
```

```
  identifies itself in !--- IKE negotiations (IP address
                                                .(in this case

                                        isakmp identity address

      Specifies the interface to use for the IPsec ---!
  tunnel. isakmp enable outside !--- These five commands
specify the Phase 1 configuration !--- settings specific
          to this sample configuration. isakmp policy 13
    authentication pre-share isakmp policy 13 encryption
aes-256 isakmp policy 13 hash sha isakmp policy 13 group
  2 isakmp policy 13 lifetime 28800 telnet timeout 5 ssh
  timeout 5 console timeout 0 !--- These three lines set
    the IPsec attributes for the tunnel to the !--- remote
      peer. This is where the preshared key is defined for
    Phase 1 and the !--- IPsec tunnel type is set to site-
   to-site. tunnel-group 10.10.10.1 type ipsec-l2l tunnel-
        group 10.10.10.1 ipsec-attributes pre-shared-key *
   Cryptochecksum:092b6fc5370e2ef0cf07c2bc10f1d44a : end
                                                pix515-702#
```

تكوين الوضع العدواني ل IPsec

يستخدم هذا القسم التكوينات التالية:

- الإصدار 6.3(5) من Cisco PIX 515e
- Cisco PIX 515، الإصدار 7.0(2)

الإصدار 6.3(5) من Cisco PIX 515e

```
                                        pix515e-635#show running-config
                                                Saved :
                                                    :
                                                (PIX Version 6.3(5
Sets the hardware speed to auto on both interfaces. ---!
  interface ethernet0 auto interface ethernet1 auto !---
     Specifies the inside and outside interfaces. nameif
     ethernet0 outside security0 nameif ethernet1 inside
  security100 enable password 8Ry2YjIyt7RRXU24 encrypted
  passwd 2KFQnbNIdI.2KYOU encrypted hostname pix515e-635
fixup protocol dns maximum-length 512 fixup protocol ftp
21 fixup protocol h323 h225 1720 fixup protocol h323 ras
 1718-1719 fixup protocol http 80 fixup protocol rsh 514
   fixup protocol rtsp 554 fixup protocol sip 5060 fixup
  protocol sip udp 5060 fixup protocol skinny 2000 fixup
       protocol smtp 25 fixup protocol sqlnet 1521 fixup
  protocol tftp 69 names !--- Specifies the traffic that
  can pass through the IPsec tunnel. access-list pixtosw
          permit ip 192.168.1.0 255.255.255.0 172.22.1.0
255.255.255.0 pager lines 24 mtu outside 1500 mtu inside
  1500 !--- Sets the inside and outside IP addresses and
              subnet masks. ip address outside 10.20.20.1
              255.255.255.0 ip address inside 192.168.1.1
255.255.255.0 ip audit info action alarm ip audit attack
  action alarm pdm history enable arp timeout 14400 !---
    Instructs PIX to perform PAT on the IP address on the
     outside interface. global (outside) 1 interface !---
Specifies addresses to be exempt from NAT (traffic to be
       tunneled). nat (inside) 0 access-list pixtosw !---
     Specifies which addresses should use NAT (all except
```

```
those exempted). nat (inside) 1 0.0.0.0 0.0.0.0 0 0 !---
   Specifies the default route on the outside interface.
route outside 0.0.0.0 0.0.0.0 10.20.20.2 1 timeout xlate
    3:00:00 timeout conn 1:00:00 half-closed 0:10:00 udp
   0:02:00 rpc 0:10:00 h225 1:00:00 timeout h323 0:05:00
 mgcp 0:05:00 sip 0:30:00 sip_media 0:02:00 timeout sip-
     disconnect 0:02:00 sip-invite 0:03:00 timeout uauth
    0:05:00 absolute aaa-server TACACS+ protocol tacacs+
     aaa-server TACACS+ max-failed-attempts 3 aaa-server
   TACACS+ deadtime 10 aaa-server RADIUS protocol radius
      aaa-server RADIUS max-failed-attempts 3 aaa-server
   RADIUS deadtime 10 aaa-server LOCAL protocol local no
 snmp-server location no snmp-server contact snmp-server
 community public no snmp-server enable traps floodguard
   enable !--- Implicit permit for all packets that come
 from IPsec tunnels. sysopt connection permit-ipsec !---
PHASE 2 CONFIGURATION !--- Defines the transform set for
Phase 2 encryption and authentication. !--- Austinlab is
         the name of the transform set that uses aes-256
  encryption !--- as well as the SHA1 hash algorithm for
                                              .authentication

   crypto ipsec transform-set austinlab esp-aes-256 esp-
                                                 sha-hmac

 Creates the dynamic map ciscopix for the transform ---!
    set. crypto dynamic-map ciscopix 1 set transform-set
 austinlab !--- Specifies the IKE that should be used to
      establish SAs !--- for the dynamic map. crypto map
dynmaptosw 66 ipsec-isakmp dynamic ciscopix !--- Applies
 the settings above to the outside interface. crypto map
 dynmaptosw interface outside !--- PHASE 1 CONFIGURATION
!--- Specifies the interface to use for the IPsec tunnel
                                                        .
                                    isakmp enable outside

   Specifies the preshared key and the addresses to ---!
use with that key. !--- In this case only one address is
        used as the preshared key "cisco123". isakmp key
******** address 10.10.10.1 netmask 255.255.255.255 !---
       Defines how the PIX identifies itself in !--- IKE
 negotiations (IP address in this case). isakmp identity
    address !--- These five commands specify the Phase 1
     configuration settings !--- specific to this sample
configuration. isakmp policy 13 authentication pre-share
    isakmp policy 13 encryption aes-256 isakmp policy 13
      hash sha isakmp policy 13 group 2 isakmp policy 13
   lifetime 28800 telnet timeout 5 ssh timeout 5 console
                                    timeout 0 terminal width 80
   Cryptochecksum:07a3815d59db9965b72c7d8a7aaf7f5f : end
                                                pix515e-635#
```

Cisco PIX 515، الإصدار 7.0(2)

```
                                    pix515-702#show running-config
                                                  Saved :
                                                       :
                                          (PIX Version 7.0(2
                                                   names
                                                       !

 PIX 7 uses an interface configuration mode similar ---!
        to Cisco IOS. !--- This output configures the IP
```

```
address, interface name, and security level for !---
interfaces Ethernet0 and Ethernet1. interface Ethernet0
  nameif outside security-level 0 ip address 10.20.20.1
      255.255.255.0 ! interface Ethernet1 nameif inside
security-level 100 ip address 192.168.1.1 255.255.255.0
  ! 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 pix515-702 domain-name cisco.com ftp
  mode passive !--- Specifies the traffic that can pass
 through the IPsec tunnel. access-list pixtosw extended
        permit ip 192.168.1.0 255.255.255.0 172.22.1.0
255.255.255.0 pager lines 24 mtu inside 1500 mtu outside
      1500 no failover monitor-interface inside monitor-
    interface outside no asdm history enable arp timeout
       14400 !--- Instructs PIX to perform PAT on the IP
    address on the outside interface. global (outside) 1
interface !--- Specifies addresses to be exempt from NAT
    (traffic to be tunneled). nat (inside) 0 access-list
   pixtosw !--- Specifies which addresses should use NAT
     (all except those exempted). nat (inside) 1 0.0.0.0
 0.0.0.0 !--- Specifies the default route on the outside
   interface. route outside 0.0.0.0 0.0.0.0 10.20.20.2 1
  timeout xlate 3:00:00 timeout conn 1:00:00 half-closed
 0:10:00 udp 0:02:00 icmp 0:00:02 timeout sunrpc 0:10:00
 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 timeout mgcp-pat
     0:05:00 sip 0:30:00 sip_media 0:02:00 timeout uauth
 0:05:00 absolute no snmp-server location no snmp-server
     contact snmp-server enable traps snmp !--- Implicit
    permit for all packets that come from IPsec tunnels.
            sysopt connection permit-ipsec !--- PHASE 2
CONFIGURATION !--- Defines the transform set for Phase 2
    encryption and authentication. !--- Austinlab is the
  name of the transform set that uses aes-256 encryption
            !--- as well as the SHA1 hash algorithm for
                                              .authentication

   crypto ipsec transform-set austinlab esp-aes-256 esp-
                                                  sha-hmac

 Creates the dynamic map "ciscopix" for the defined ---!
       transform set. crypto dynamic-map ciscopix 1 set
  transform-set austinlab !--- Specifies that IKE should
   be used to establish SAs !--- for the defined dynamic
      map. crypto map dynmaptosw 66 ipsec-isakmp dynamic
       ciscopix !--- Applies the settings to the outside
 interface. crypto map dynmaptosw interface outside !---
          PHASE 1 CONFIGURATION !--- Defines how the PIX
  identifies itself in !--- IKE negotiations (IP address
                                              .(in this case

                                    isakmp identity address

      Specifies the interface to use for the IPsec ---!
   tunnel. isakmp enable outside !--- These five commands
specify the Phase 1 configuration settings !--- specific
            to this sample configuration. isakmp policy 13
    authentication pre-share isakmp policy 13 encryption
aes-256 isakmp policy 13 hash sha isakmp policy 13 group
  2 isakmp policy 13 lifetime 28800 telnet timeout 5 ssh
```

```
timeout 5 console timeout 0 !--- These three lines set
the IPsec attributes for the tunnel to the !--- remote
  peer. This is where the preshared key is defined for
 Phase 1 and the !--- IPsec tunnel type is set to site-
to-site. tunnel-group 10.10.10.1 type ipsec-l2l tunnel-
    group 10.10.10.1 ipsec-attributes pre-shared-key *
 Cryptochecksum:092b6fc5370e2ef0cf07c2bc10f1d44a : end
                                              pix515-702#
```

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** .

- **show crypto isakmp sa**— يعرض جميع شبكات IKE الحالية في نظير.
- **show crypto ipSec**—يعرض الإعدادات المستخدمة من قبل SAs الحالية.

توضح هذه الجداول نتائج بعض عمليات تصحيح الأخطاء الخاصة بالأوضاع الرئيسية والقوية في كل من PIX 6.3(5) و PIX 7.0(2) بعد إنشاء النفق بالكامل.

ملاحظة: يجب أن تكون هذه معلومات كافية لإنشاء نفق IPsec بين هذين النوعين من الأجهزة. إذا كان لديك أي تعليقات، أستخدم نموذج الملاحظات الموجود على الجانب الأيسر من هذا المستند.

- Cisco PIX 515e الإصدار 6.3(5) - الوضع الرئيسي
- Cisco PIX 515 الإصدار 7.0(2)- الوضع الرئيسي
- الإصدار 6.3(5) من Cisco PIX 515e - الوضع المتميز
- Cisco PIX 515، الإصدار 7.0(2) - الوضع المتميز

Cisco PIX 515e الإصدار 6.3(5) - الوضع الرئيسي

```
                    pix515e-635#show crypto isakmp sa
                                          Total     : 1
                                          Embryonic : 0
dst               src        state     pending
                                                created
QM_IDLE         0    10.20.20.1       10.10.10.1
                                                      1
                                       pix515e-635#



                     pix515e-635#show crypto ipsec sa


                        interface: outside
      Crypto map tag: maptosw, local addr.
                                             10.20.20.1

                  local ident (addr/mask/prot/port):
                      ((192.168.1.0/255.255.255.0/0/0
       remote ident (addr/mask/prot/port):
                       ((172.22.1.0/255.255.255.0/0/0
             current_peer: 10.10.10.1:500
           {,PERMIT, flags={origin_is_acl
   pkts encaps: 4, #pkts encrypt: 4, #pkts#
```

```
                                                    digest 4
     pkts decaps: 4, #pkts decrypt: 4, #pkts#
                                                    verify 4
   pkts compressed: 0, #pkts decompressed: 0#
pkts not compressed: 0, #pkts compr. failed:#
                              0, #pkts decompress failed: 0
               send errors 1, #recv errors 0#

 local crypto endpt.: 10.20.20.1, remote crypto endpt.:
                                                 10.10.10.1
  path mtu 1500, ipsec overhead 72, media mtu
                                                       1500
               current outbound spi: ed0afa33

                                        :inbound esp sas
                 (spi: 0xac624692(2892121746
       , transform: esp-aes-256 esp-sha-hmac
                 { ,in use settings ={Tunnel
    slot: 0, conn id: 1, crypto map: maptosw
  sa timing: remaining key lifetime (k/sec):
                                        ((4607999/28718
                              IV size: 16 bytes
                 replay detection support: Y


                               :inbound ah sas


                              :inbound pcp sas


                              :outbound esp sas
                 (spi: 0xed0afa33(3976919603
       , transform: esp-aes-256 esp-sha-hmac
                 { ,in use settings ={Tunnel
    slot: 0, conn id: 2, crypto map: maptosw
  sa timing: remaining key lifetime (k/sec):
                                        ((4607999/28718
                              IV size: 16 bytes
                 replay detection support: Y


                               :outbound ah sas


                              :outbound pcp sas

                                                  pix515e-635#
```

Cisco PIX 515 الإصدار 7.0(2)- الوضع الرئيسي

```
                        pix515-702#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: 10.10.10.1 1
                  Type : L2L Role : initiator
                 Rekey : no State : MM_ACTIVE
                                    pix515-702#
```

```
pix515-702#show crypto ipsec sa
interface: outside
Crypto map tag: maptosw, local addr: 10.20.20.1

local ident (addr/mask/prot/port):
((192.168.1.0/255.255.255.0/0/0
remote ident (addr/mask/prot/port):
((172.22.1.0/255.255.255.0/0/0
current_peer: 10.10.10.1

pkts encaps: 5, #pkts encrypt: 5, #pkts digest: 5#
pkts decaps: 5, #pkts decrypt: 5, #pkts#
verify: 5
pkts compressed: 0, #pkts decompressed: 0#
pkts not compressed: 5, #pkts comp failed:#
0, #pkts decomp failed: 0
send errors: 0, #recv errors: 0#

local crypto endpt.: 10.20.20.1, remote crypto endpt.:
10.10.10.1

path mtu 1500, ipsec overhead 76, media mtu 1500
current outbound spi: 2D006547

:inbound esp sas
(spi: 0x309F7A33 (815757875
transform: esp-aes-256 esp-sha-hmac
{ ,in use settings ={L2L, Tunnel
slot: 0, conn_id: 1, crypto-map: maptosw
sa timing: remaining key lifetime (kB/sec):
((4274999/28739
IV size: 16 bytes
replay detection support: Y
:outbound esp sas
(spi: 0x2D006547 (755000647
transform: esp-aes-256 esp-sha-hmac
{ ,in use settings ={L2L, Tunnel
slot: 0, conn_id: 1, crypto-map: maptosw
sa timing: remaining key lifetime (kB/sec):
((4274999/28737
IV size: 16 bytes
replay detection support: Y

pix515-702#
```

الإصدار 6.3(5) من Cisco PIX 515e - الوضع المتميز

```
pix515e-635#show crypto isakmp sa
Total     : 1
Embryonic : 0
dst               src        state     pending
created
QM_IDLE         0    10.10.10.1       10.20.20.1
1

pix515e-635#show crypto ipsec sa


interface: outside
Crypto map tag: dynmaptosw, local addr.
10.20.20.1

local ident (addr/mask/prot/port):
```

```
                        ((192.168.1.0/255.255.255.0/0/0
          remote ident (addr/mask/prot/port):
                        ((172.22.1.0/255.255.255.0/0/0
                current_peer: 10.10.10.1:500
                              {}=PERMIT, flags
     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 decompress failed: 0
               send errors 0, #recv errors 0#

 local crypto endpt.: 10.20.20.1, remote crypto endpt.:
                                             10.10.10.1
  path mtu 1500, ipsec overhead 72, media mtu
                                                   1500
               current outbound spi: efb1149d

                                    :inbound esp sas
                 (spi: 0x2ad2c13c(718455100
       , transform: esp-aes-256 esp-sha-hmac
                 { ,in use settings ={Tunnel
  slot: 0, conn id: 2, crypto map: dynmaptosw
   sa timing: remaining key lifetime (k/sec):
                                    ((4608000/28736
                           IV size: 16 bytes
                replay detection support: Y


                             :inbound ah sas


                            :inbound pcp sas


                           :outbound esp sas
                (spi: 0xefb1149d(4021359773
       , transform: esp-aes-256 esp-sha-hmac
                 { ,in use settings ={Tunnel
  slot: 0, conn id: 1, crypto map: dynmaptosw
   sa timing: remaining key lifetime (k/sec):
                                    ((4608000/28727
                           IV size: 16 bytes
                replay detection support: Y


                            :outbound ah sas


                           :outbound pcp sas

                                          pix515e-635#
```

Cisco PIX 515، الإصدار 7.0(2) - الوضع المتميز

```
                        pix515-702#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: 10.10.10.1 1
                Type : L2L Role : responder
               Rekey : no State : AM_ACTIVE
                                pix515-702#

                        pix515-702#show crypto ipsec sa
                          interface: outside
       Crypto map tag: ciscopix, local addr:
                                              10.20.20.1

                    local ident (addr/mask/prot/port):
                        ((192.168.1.0/255.255.255.0/0/0
          remote ident (addr/mask/prot/port):
                         ((172.22.1.0/255.255.255.0/0/0
                    current_peer: 10.10.10.1

     pkts encaps: 5, #pkts encrypt: 5, #pkts digest: 5#
     pkts decaps: 5, #pkts decrypt: 5, #pkts#
                                               verify: 5
   pkts compressed: 0, #pkts decompressed: 0#
 pkts not compressed: 5, #pkts comp failed:#
                                0, #pkts decomp failed: 0
            send errors: 0, #recv errors: 0#

local crypto endpt.: 10.20.20.1, remote crypto endpt.:
                                              10.10.10.1

      path mtu 1500, ipsec overhead 76, media mtu 1500
              current outbound spi: D7E2F5FD

                                      :inbound esp sas
                (spi: 0xDCBF6AD3 (3703532243
          transform: esp-aes-256 esp-sha-hmac
             { ,in use settings ={L2L, Tunnel
    slot: 0, conn_id: 1, crypto-map: ciscopix
     sa timing: remaining key lifetime (sec):
                                                28703
                             IV size: 16 bytes
                  replay detection support: Y
                             :outbound esp sas
                (spi: 0xD7E2F5FD (3621975549
          transform: esp-aes-256 esp-sha-hmac
             { ,in use settings ={L2L, Tunnel
    slot: 0, conn_id: 1, crypto-map: ciscopix
     sa timing: remaining key lifetime (sec):
                                                28701
                             IV size: 16 bytes
                  replay detection support: Y

                                              pix515-702#
```

استكشاف الأخطاء وإصلاحها

لا تتوفر حاليًا معلومات محددة لاستكشاف الأخطاء وإصلاحها لهذا التكوين.

معلومات ذات صلة

- برنامج جدار حماية Cisco PIX

- مراجع أوامر جدار حماية PIX الآمن من Cisco
- الإعلامات الميدانية لمنتج الأمان (بما في ذلك PIX)
- طلبات التعليقات (RFCs)
- 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).