ASA 8.3 والإصدارات الأحدث: NTP مع مثال تكوين نفق IPsec وبدون هذا المثال

المحتويات

المقدمة
المتطلبات الأساسية
المتطلبات
المكونات المستخدمة
الاصطلاحات
التكوين
الرسم التخطيطي للشبكة
تكوين ASDM لنفق VPN
تكوين NTP ASDM
تكوين ASA1 CLI
تكوين ASA2 CLI
التحقق من الصحة
استكشاف الأخطاء وإصلاحها
أوامر استكشاف الأخطاء وإصلاحها
معلومات ذات صلة

المقدمة

يقدم هذا المستند نموذجا للتكوين لمزامنة ساعة جهاز الأمان القابل للتكيف (ASA) مع خادم وقت الشبكة باستخدام بروتوكول وقت الشبكة (NTP). يتصل ASA1 مباشرة بخادم وقت الشبكة. يقوم ASA2 بتمرير حركة مرور NTP من خلال نفق IPsec إلى ASA1، والذي يقوم بدوره بإعادة توجيه الحزم إلى خادم وقت الشبكة.

ارجع إلى ASA/PIX: NTP باستخدام مثال تكوين نفق IPsec وبدونه للحصول على تكوين مماثل على Cisco ASA مع الإصدارات 8.2 والإصدارات الأقدم.

ملاحظة: يمكن أيضا إستخدام موجه كخادم NTP لمزامنة ساعة جهاز الأمان ASA.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

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

- ASA مع الإصدار 8.3 والإصدارات الأحدث من Cisco
- Cisco Adaptive Security Device Manager (ASDM)، الإصدار x.6 والإصدارات الأحدث

ملاحظة: ارجع إلى السماح بوصول HTTPS إلى ASDM للسماح بتكوين ASA بواسطة ASDM.

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.

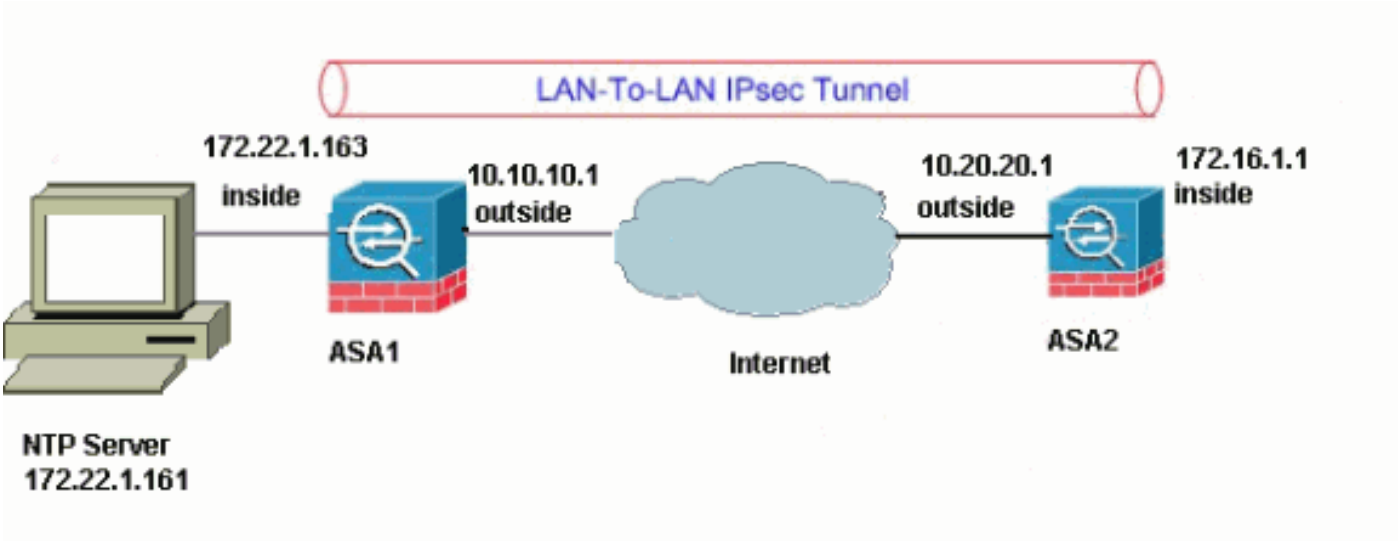
الاصطلاحات

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

التكوين

الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة التالي:



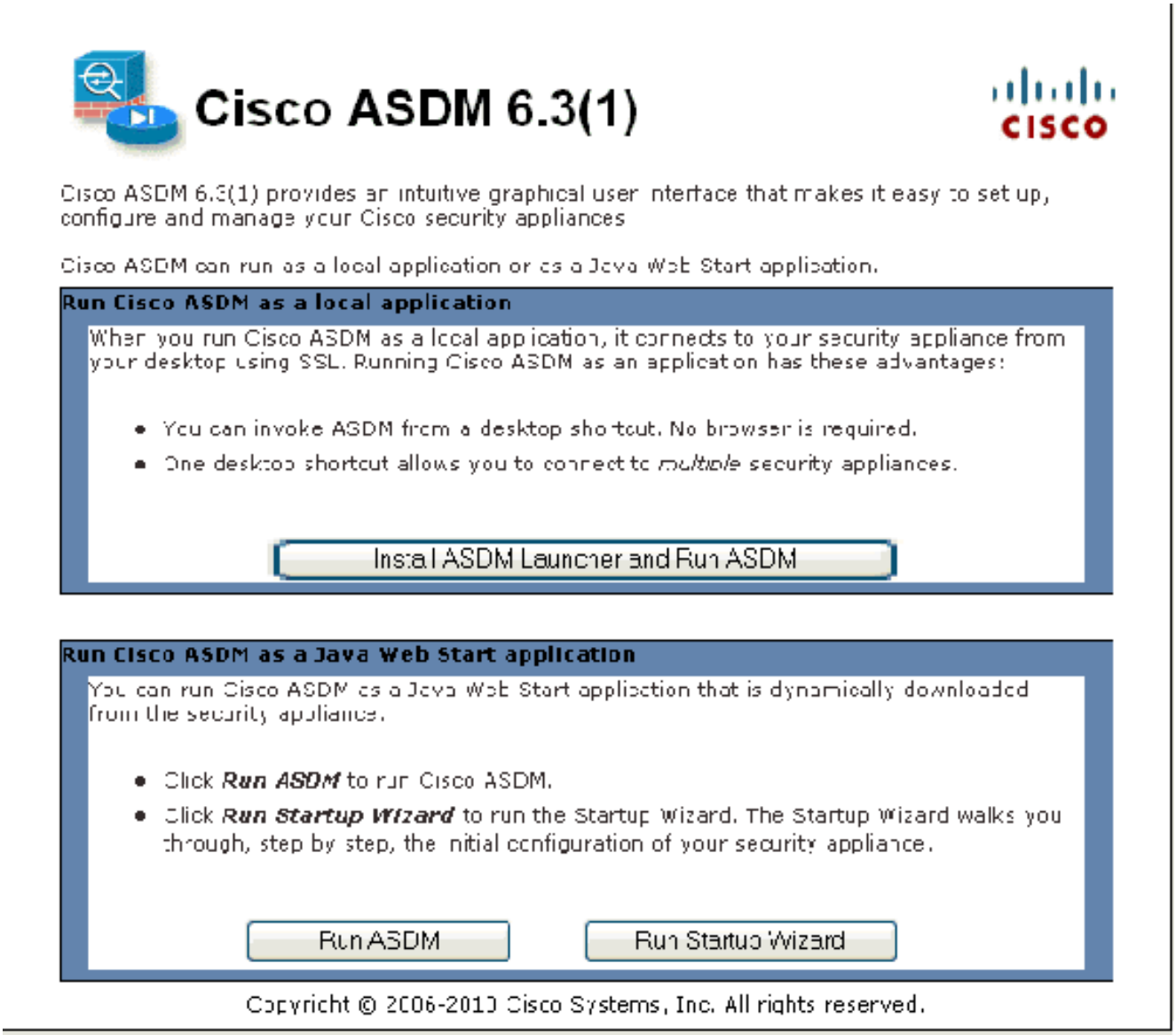
ملاحظة: ال ip ليس يخاطب خطة يستعمل في هذا تشكيل قانونيا routable على الإنترنت. هم rfc 1918 عنوان، أي يتلقى يكون استعملت في مختبر بيئة.

- تكوين ASDM لنفق VPN
- تكوين NTP ASDM
- تكوين ASA1 CLI
- تكوين ASA2 CLI

تكوين ASDM لنفق VPN

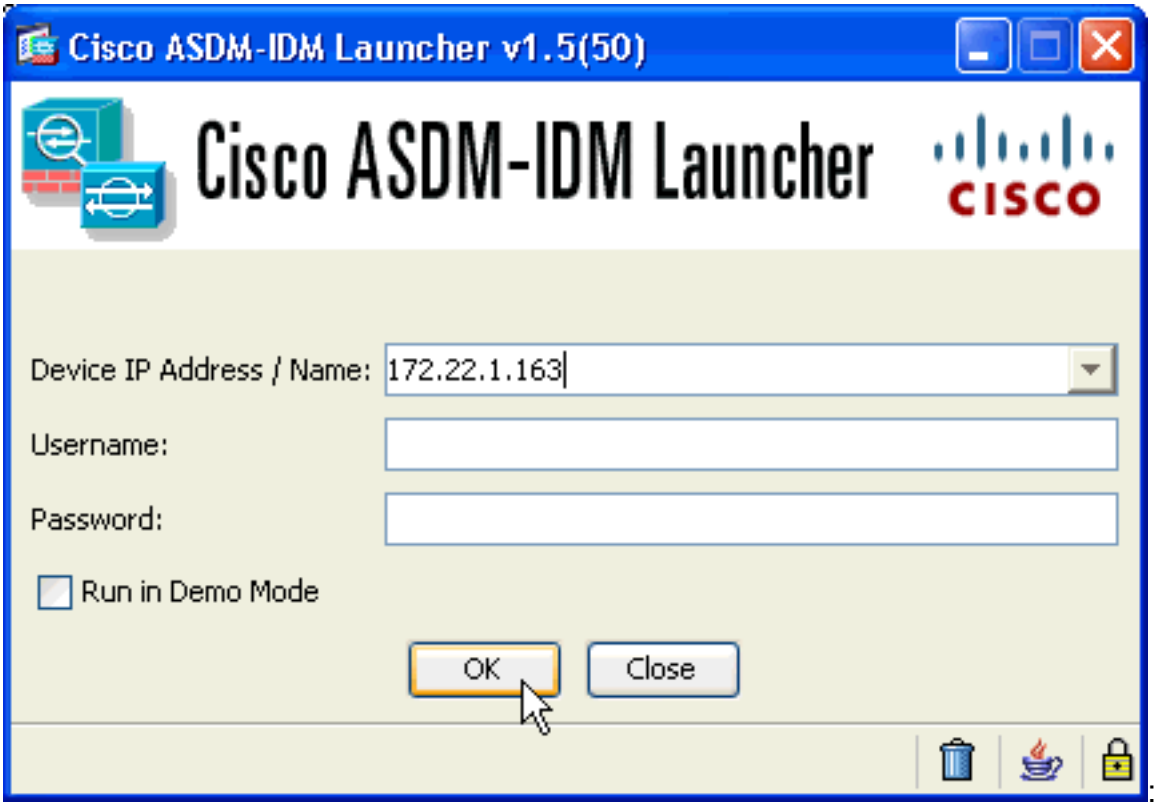
أتمت هذا steps in order to خلقت ال VPN نفق:

1. افتح المستعرض الخاص بك واكتب **https://<Inside_IP_ADDRESS_OF_ASA>**للوصول إلى ASDM على ASA.تأكد من تخويل أية تحذيرات يعطيك المستعرض لها علاقة بموثوقية شهادة SSL. التقصير username وكلمة على حد سواء فارغ.يقدم ASA هذه النافذة للسماح بتنزيل تطبيق ASDM.



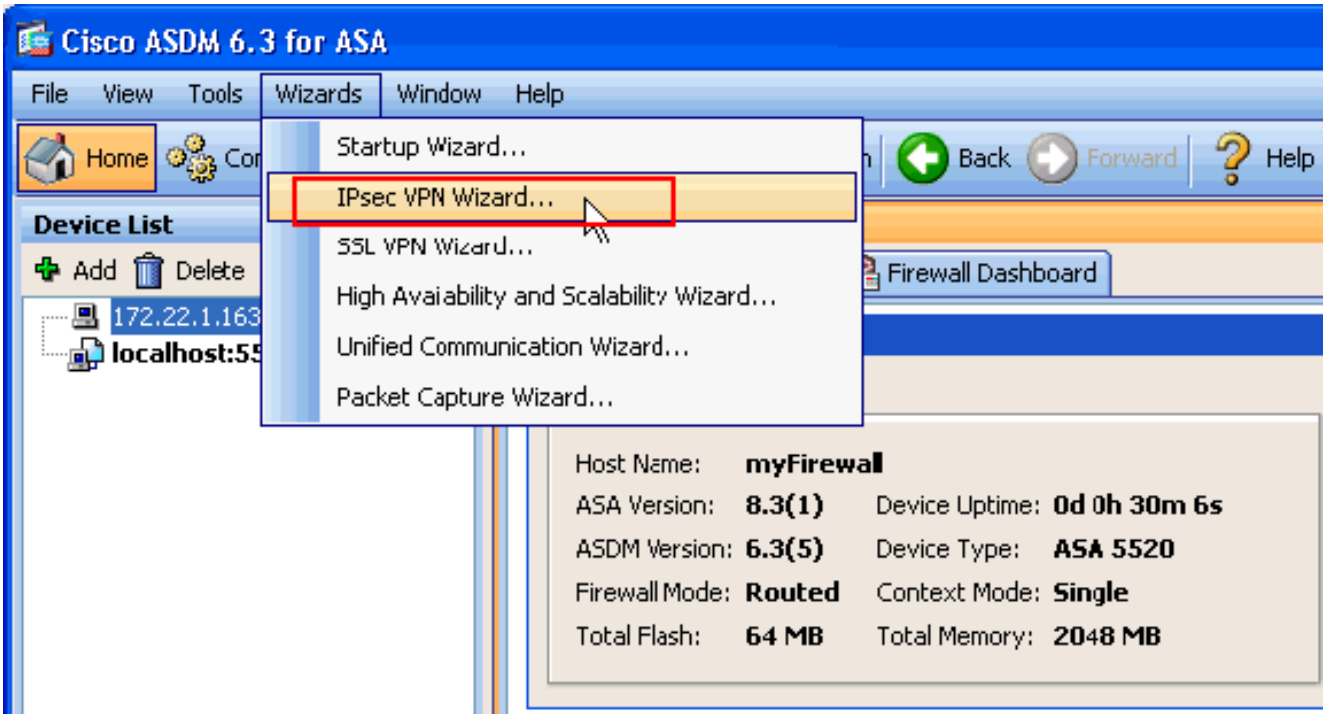
يقوم هذا المثال بتحميل التطبيق على الكمبيوتر المحلي ولا يعمل في تطبيق Java.

2. انقر على **تنزيل مشغل ASDM وابدأ ASDM** لتنزيل المثبت الخاص بتطبيق ASDM.
3. بمجرد تنزيل مشغل ASDM، قم بإكمال الخطوات التي توجهها المطالبات لتثبيت البرنامج وتشغيل مشغل ASDM من Cisco.
4. دخلت العنوان للقارن أنت تشكل مع **ال http -** أمر، واسم مستخدم وكلمة إن يعين أنت واحد.يستعمل هذا مثال التقصير فارغ username

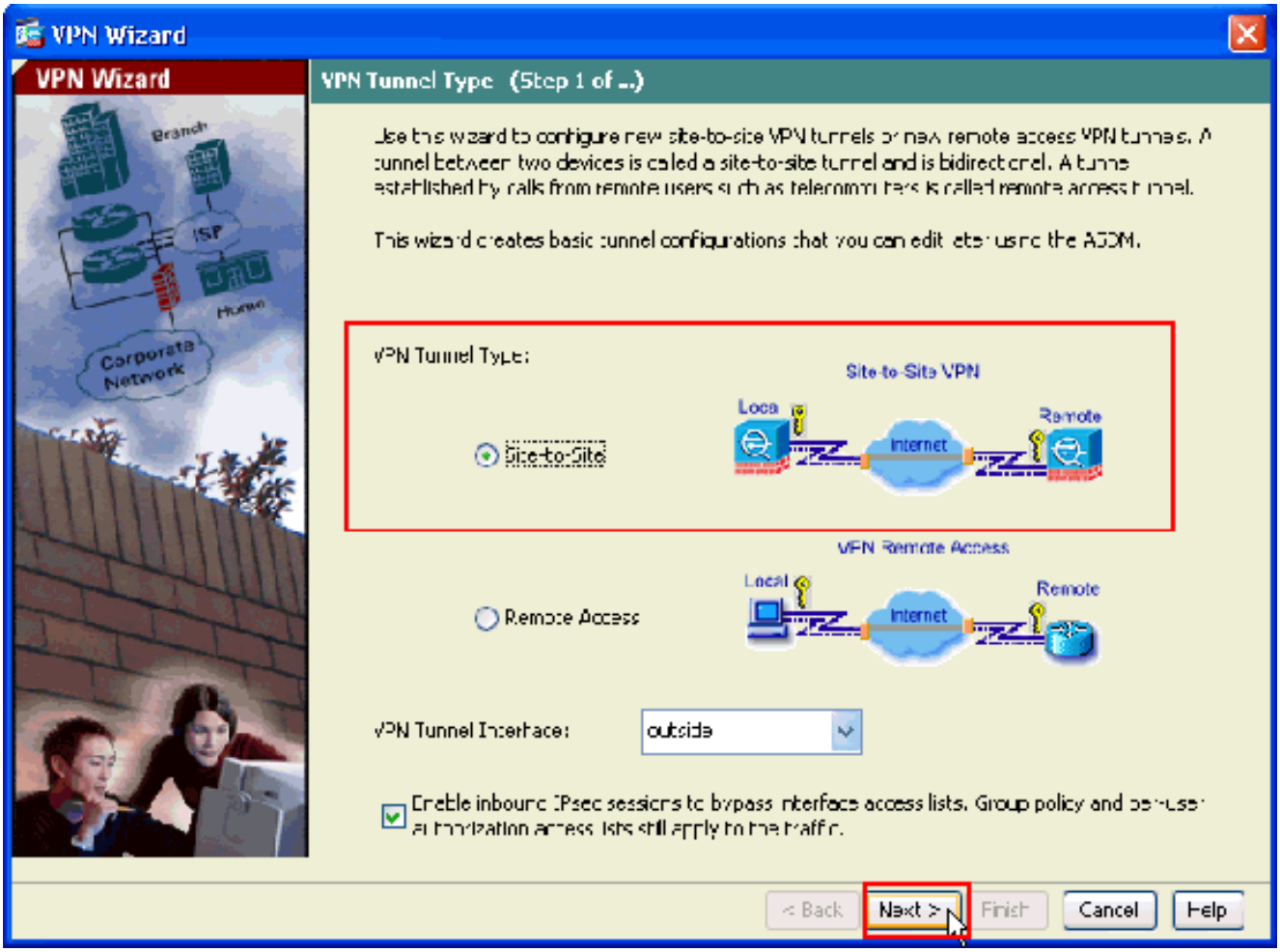


وكلمة.

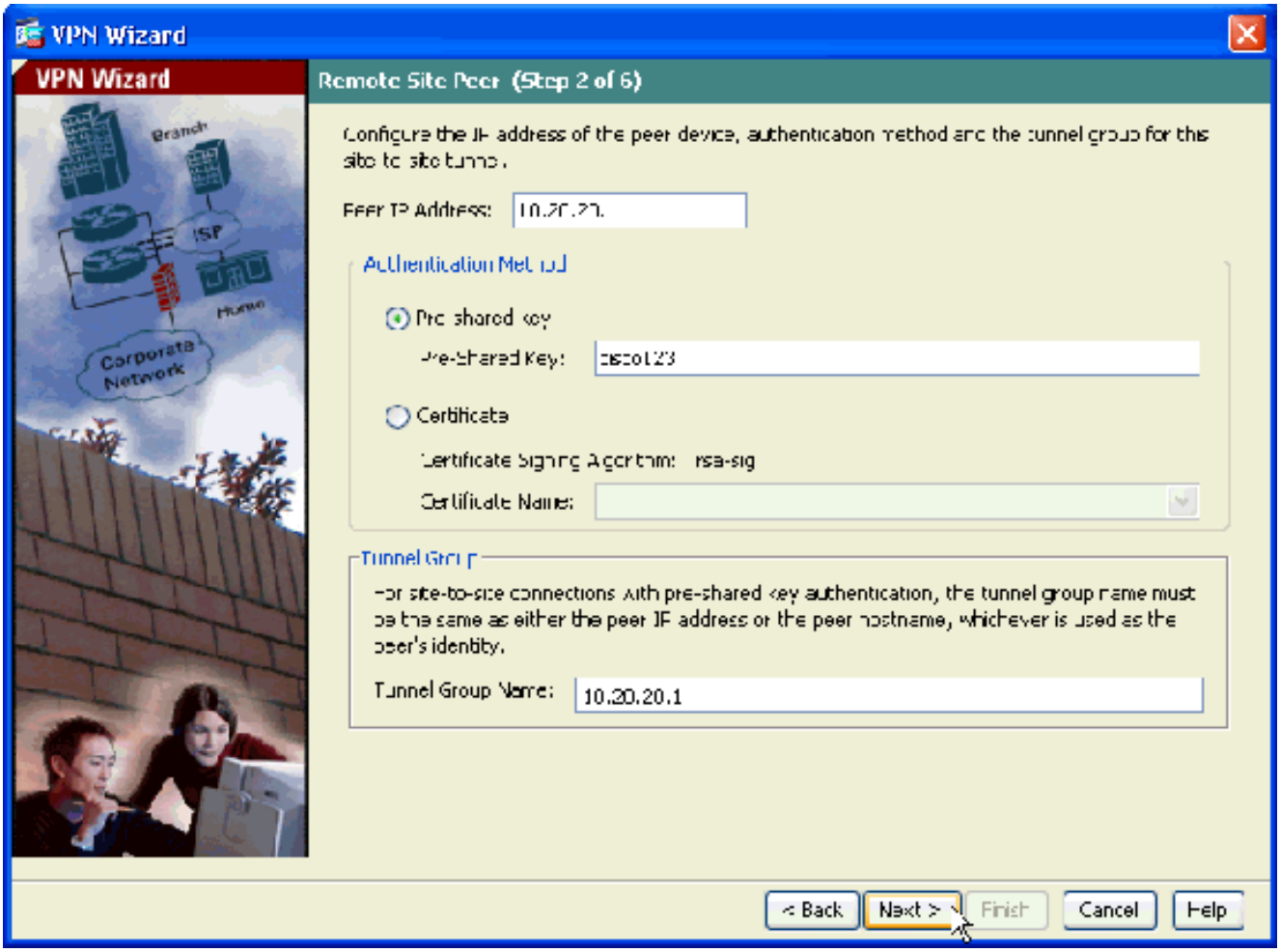
5. قم بتشغيل معالج VPN بمجرد اتصال تطبيق ASDM ب ASA.



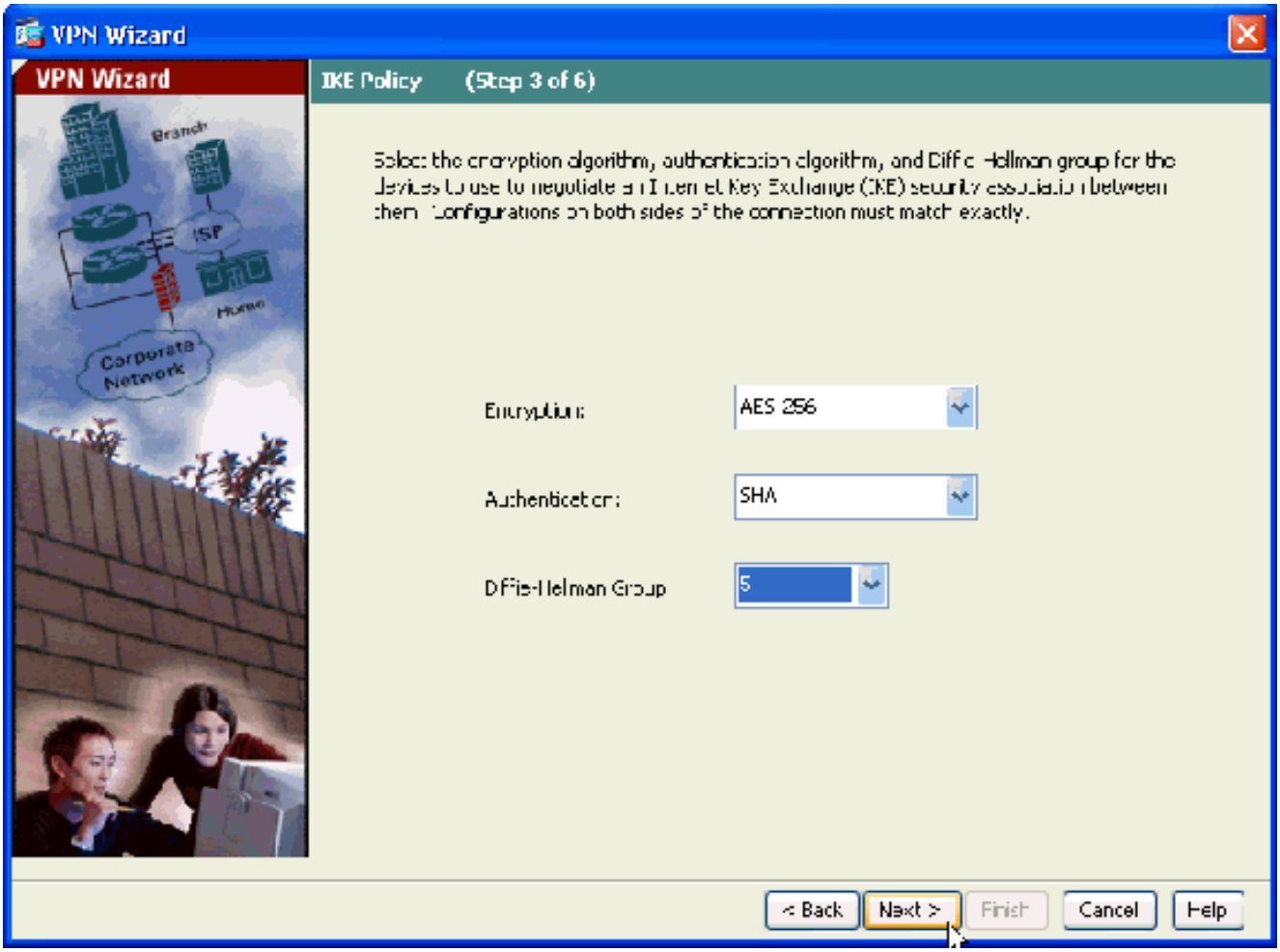
6. أخترت **موقع إلى موقع** ل ال IPsec VPN نفق نوع، وطقطقة **بعد ذلك**.



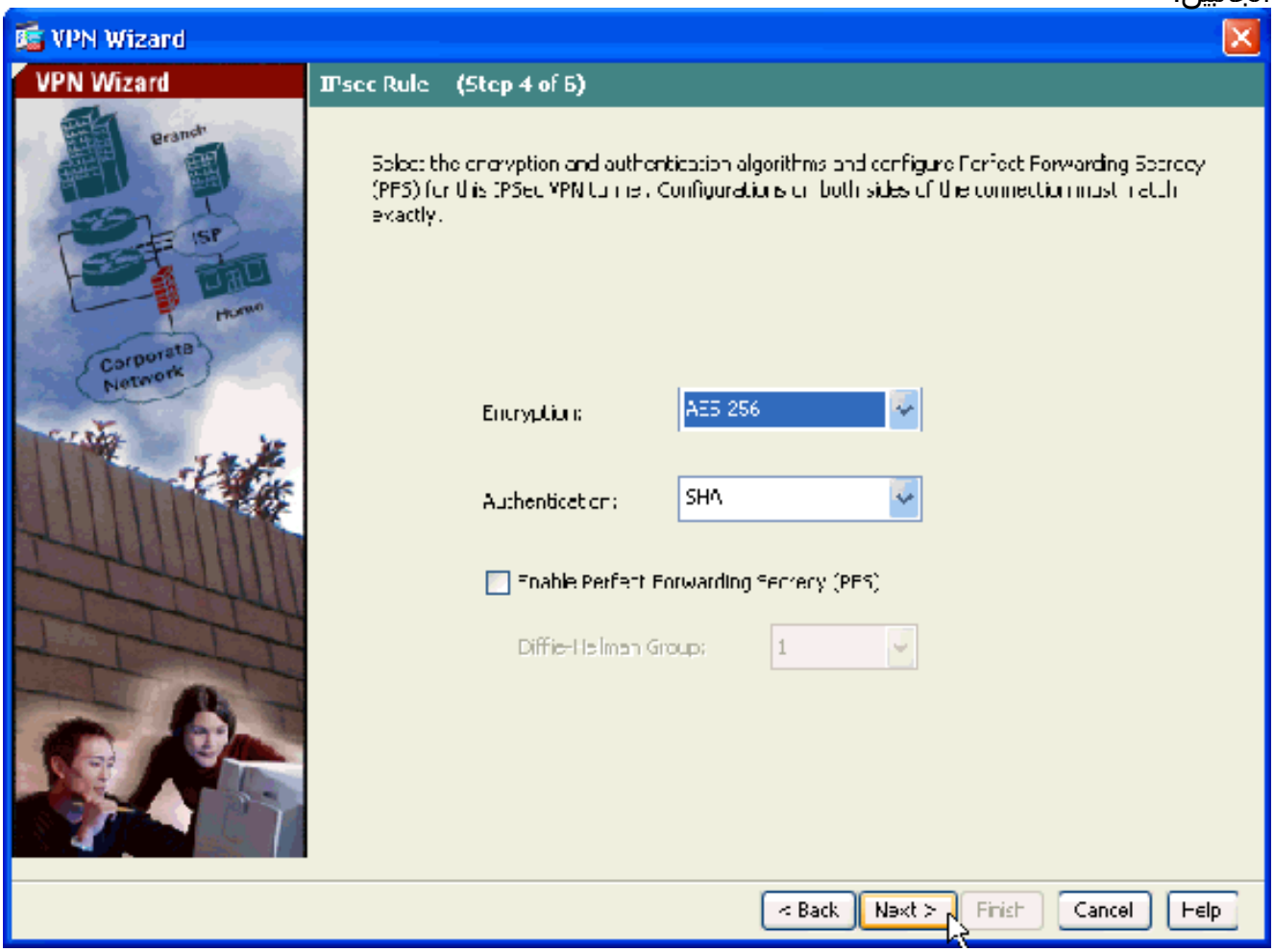
7. حدد عنوان IP الخارجي للنظير البعيد. أدخل معلومات المصادقة المراد إستخدامها، وهو المفتاح المشترك مسبقا في هذا
المثال:



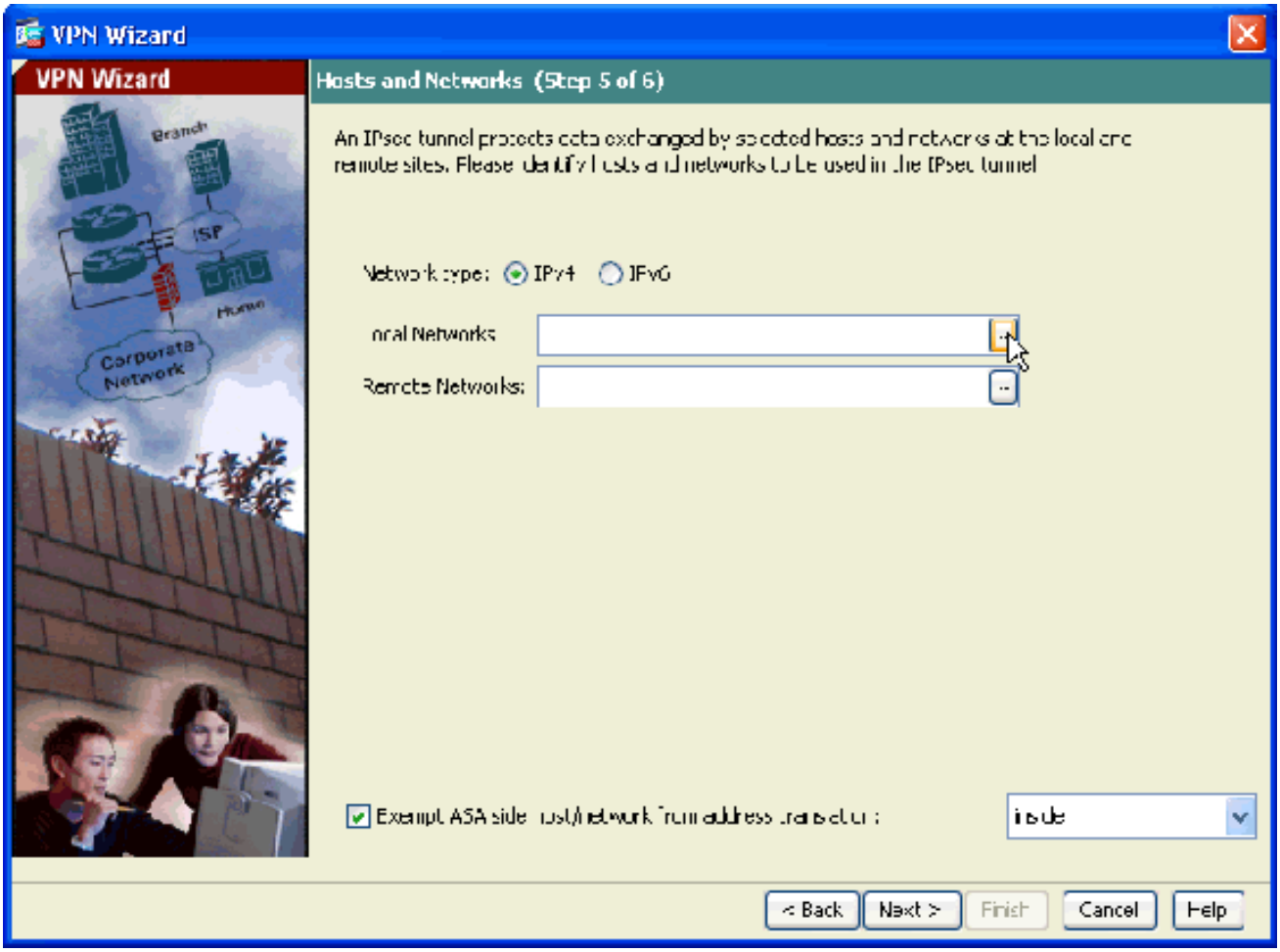
8. حدد السمات التي سيتم إستخدامها ل IKE، والمعروفة أيضا بالطور 1. يجب أن تكون هذه السمات واحدة على كلا جانبي
النفق.



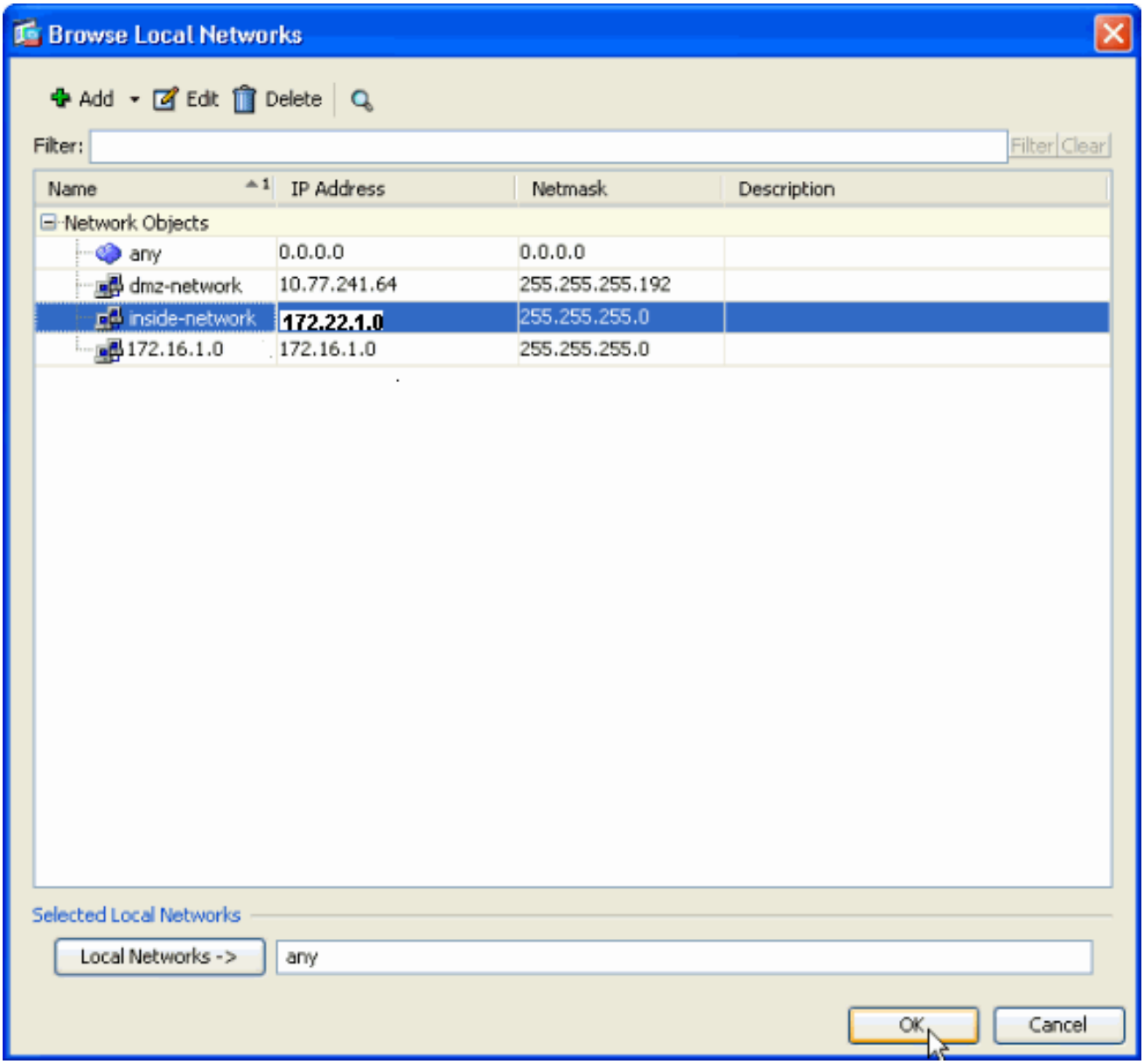
9. حدد السمات التي سيتم إستخدامها ل IPsec، المعروفة أيضا بالطور 2. يجب أن تتطابق هذه السمات على كلا الجانبين.



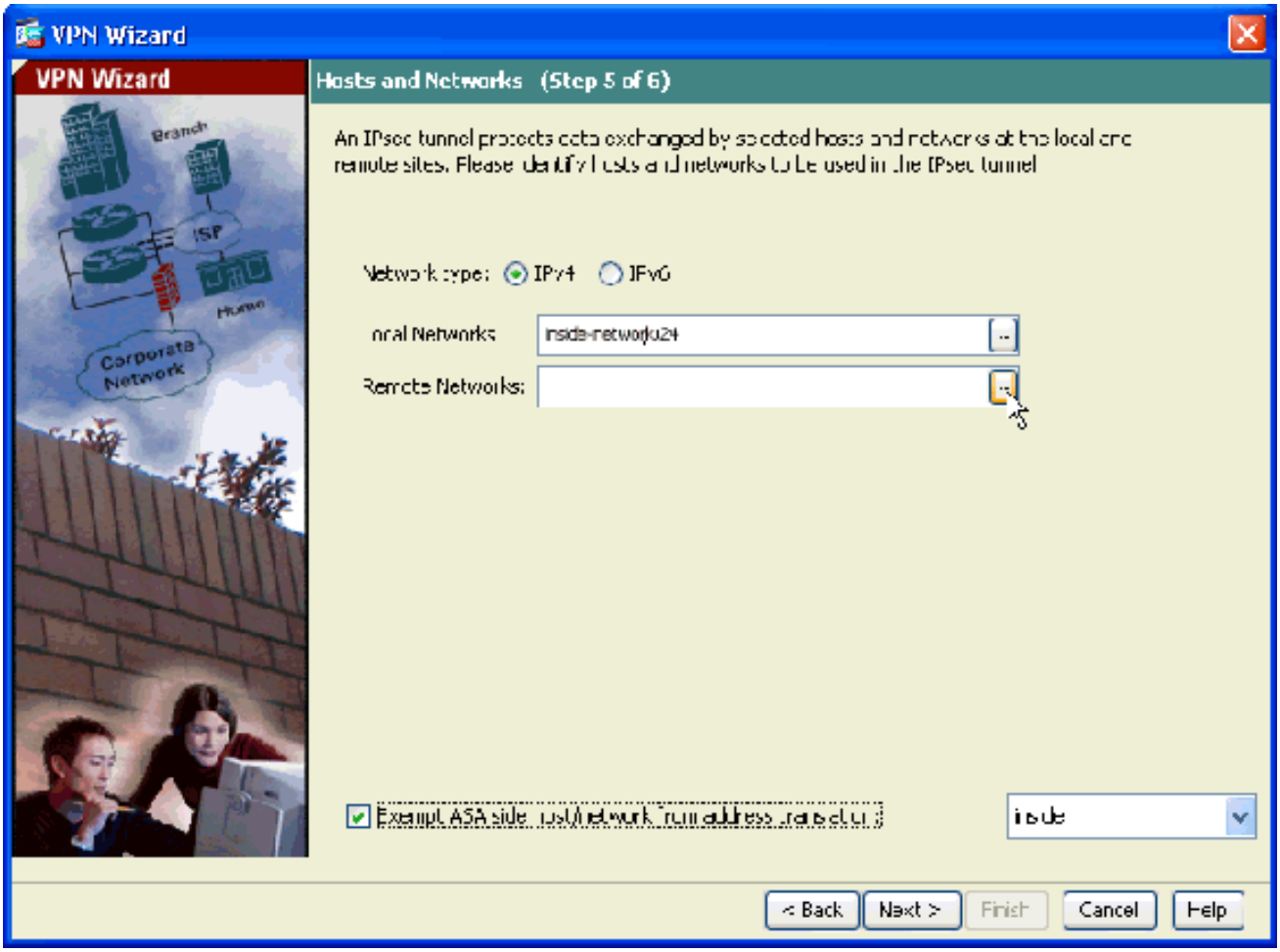
10. حدد البيئات المضيفة التي يجب السماح لحركة مرور البيانات الخاصة بها بالمرور من خلال نفق VPN. في هذه الخطوة، يجب عليك توفير الشبكات المحلية والشبكات البعيدة لنفق الشبكة الخاصة الظاهرية (VPN). انقر فوق الزر الموجود بجوار **الشبكات المحلية** (كما هو موضح هنا) لاختيار عنوان الشبكة المحلية من القائمة المنسدلة:



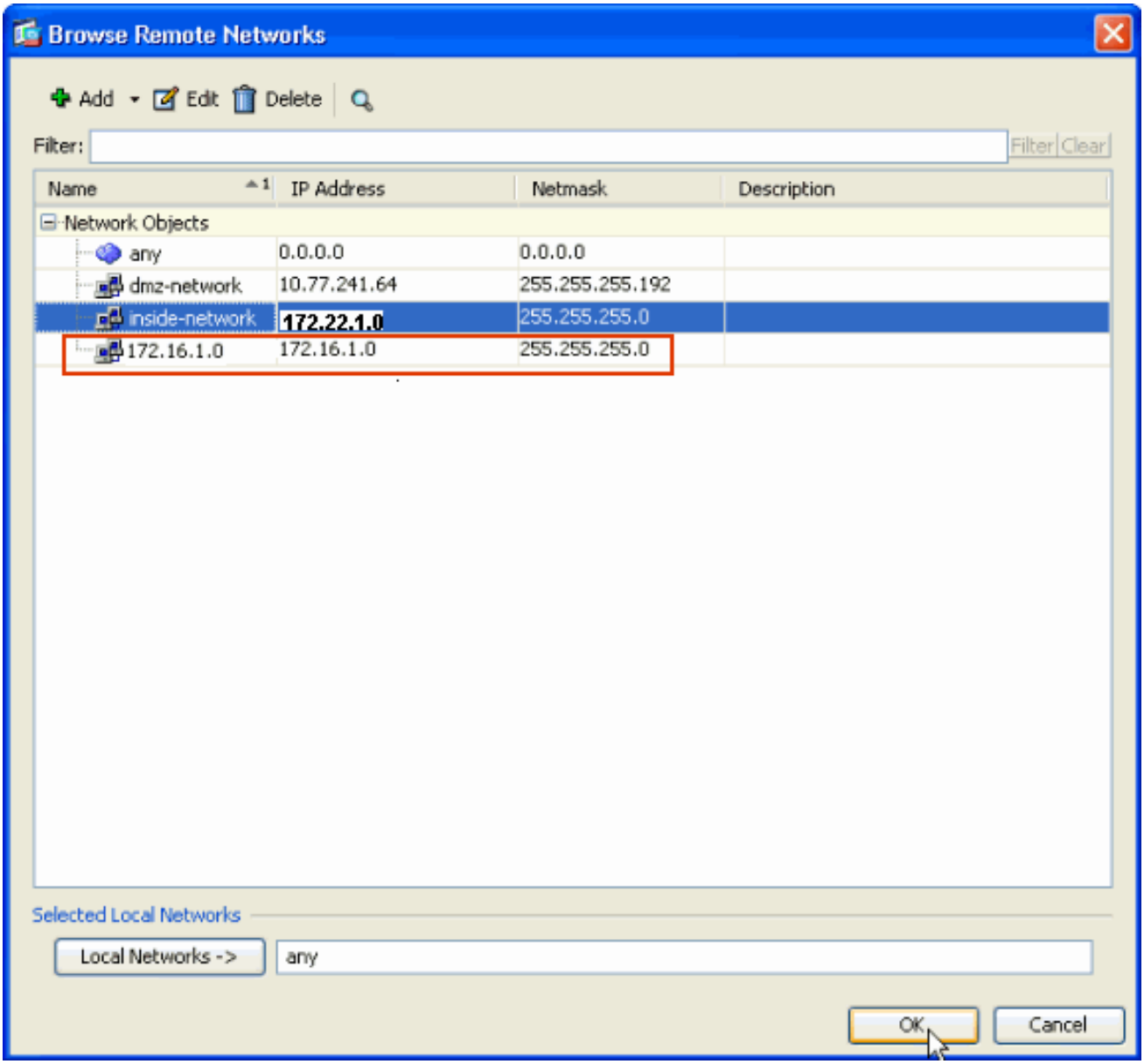
11. أخترت **الشبكة المحلية** عنوان، وطقطقة **ok**.



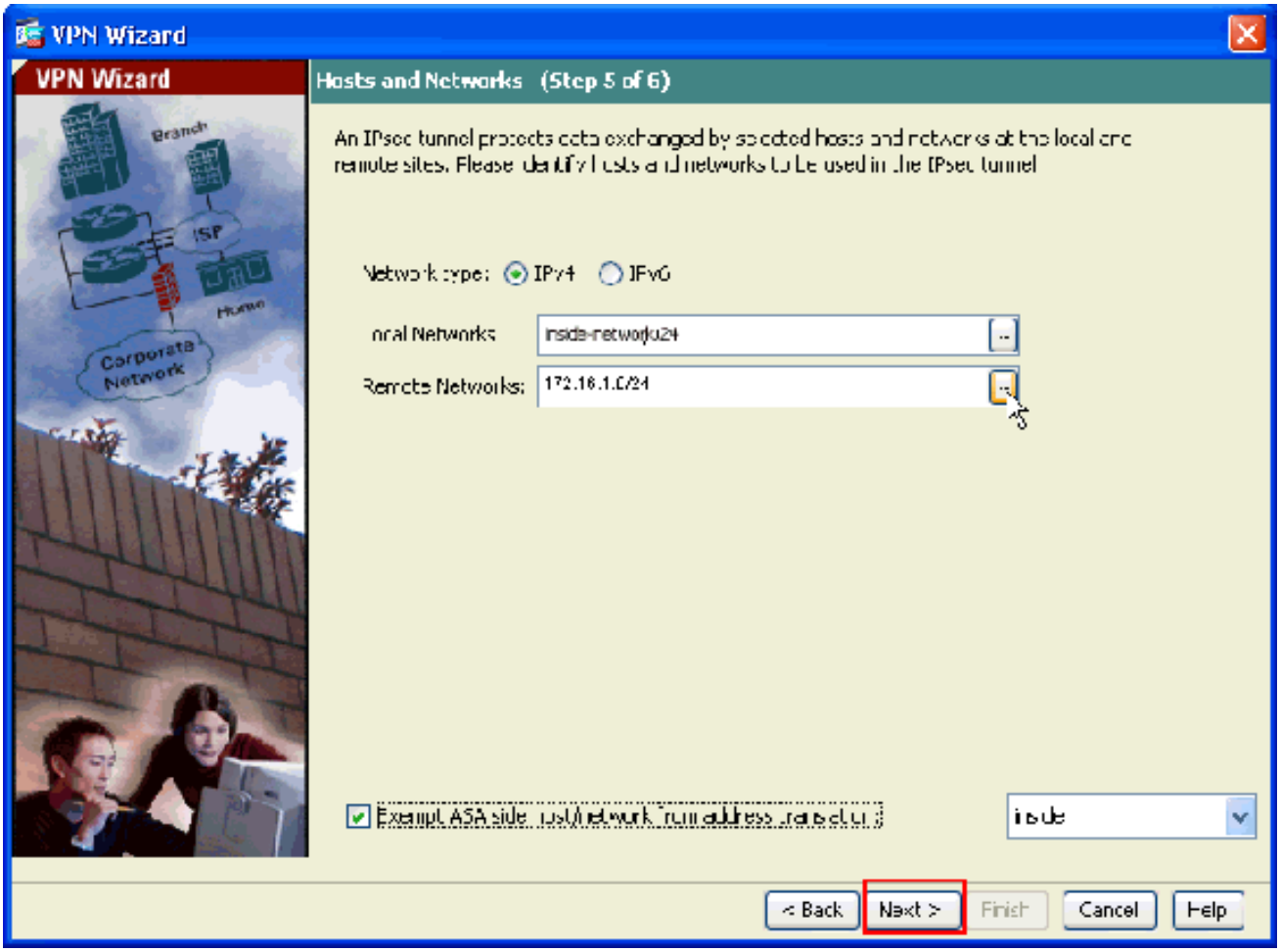
12. انقر فوق الزر الموجود بجوار **الشبكات البعيدة** لاختيار عنوان الشبكة البعيدة من القائمة المنسدلة.



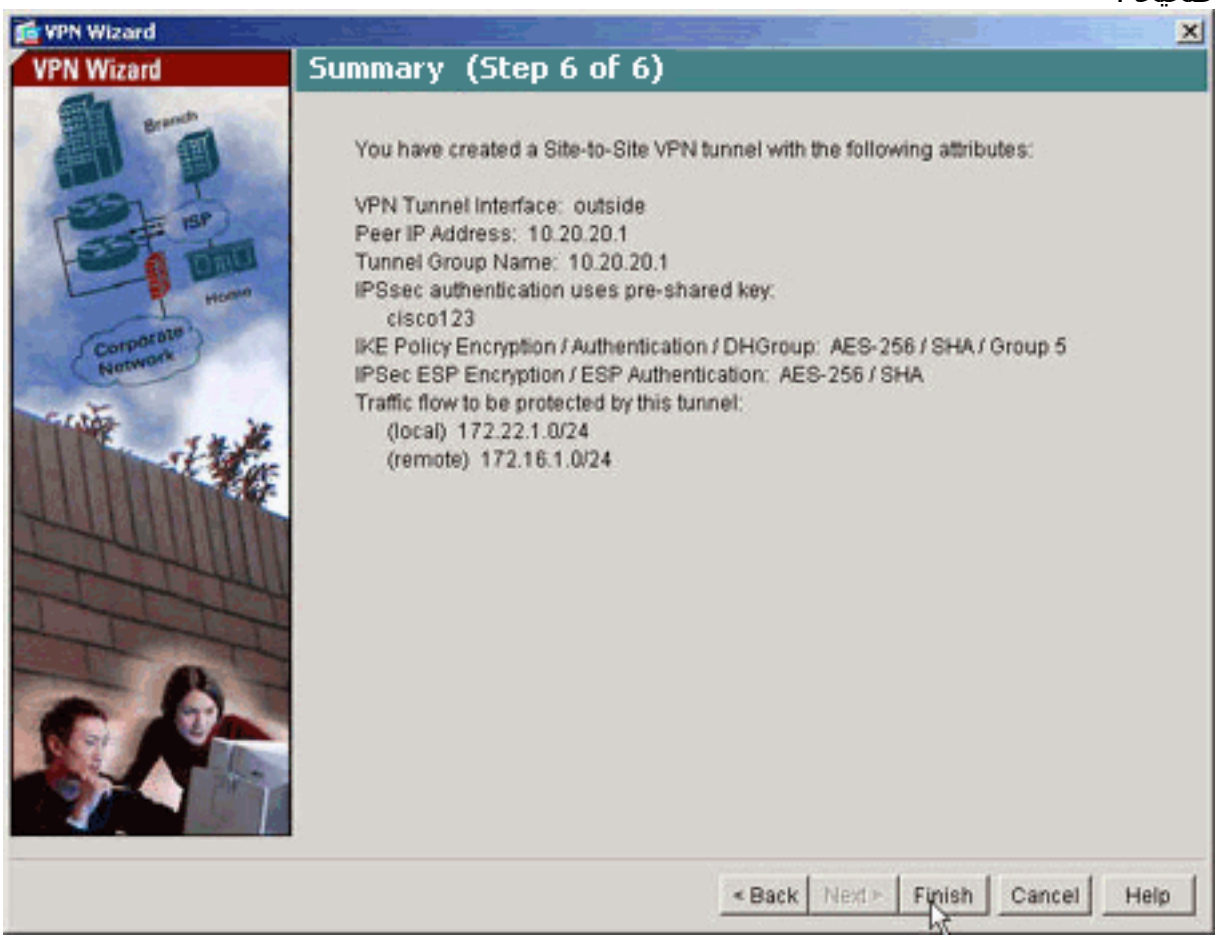
13. أخترت **الشبكة بعيد** عنوان، وطقطقة ok.**ملاحظة:** إذا لم يكن لديك الشبكة البعيدة في القائمة، فيجب إضافة الشبكة إلى القائمة. طقطقة **يضيف** in order to فعلت ذلك.



14. حدد خانة الاختيار **Exception ASA Side Host/Network من ترجمة العنوان** لمنع حركة مرور النفق من الخضوع لترجمة عنوان الشبكة. انقر فوق **Next (التالي)**.



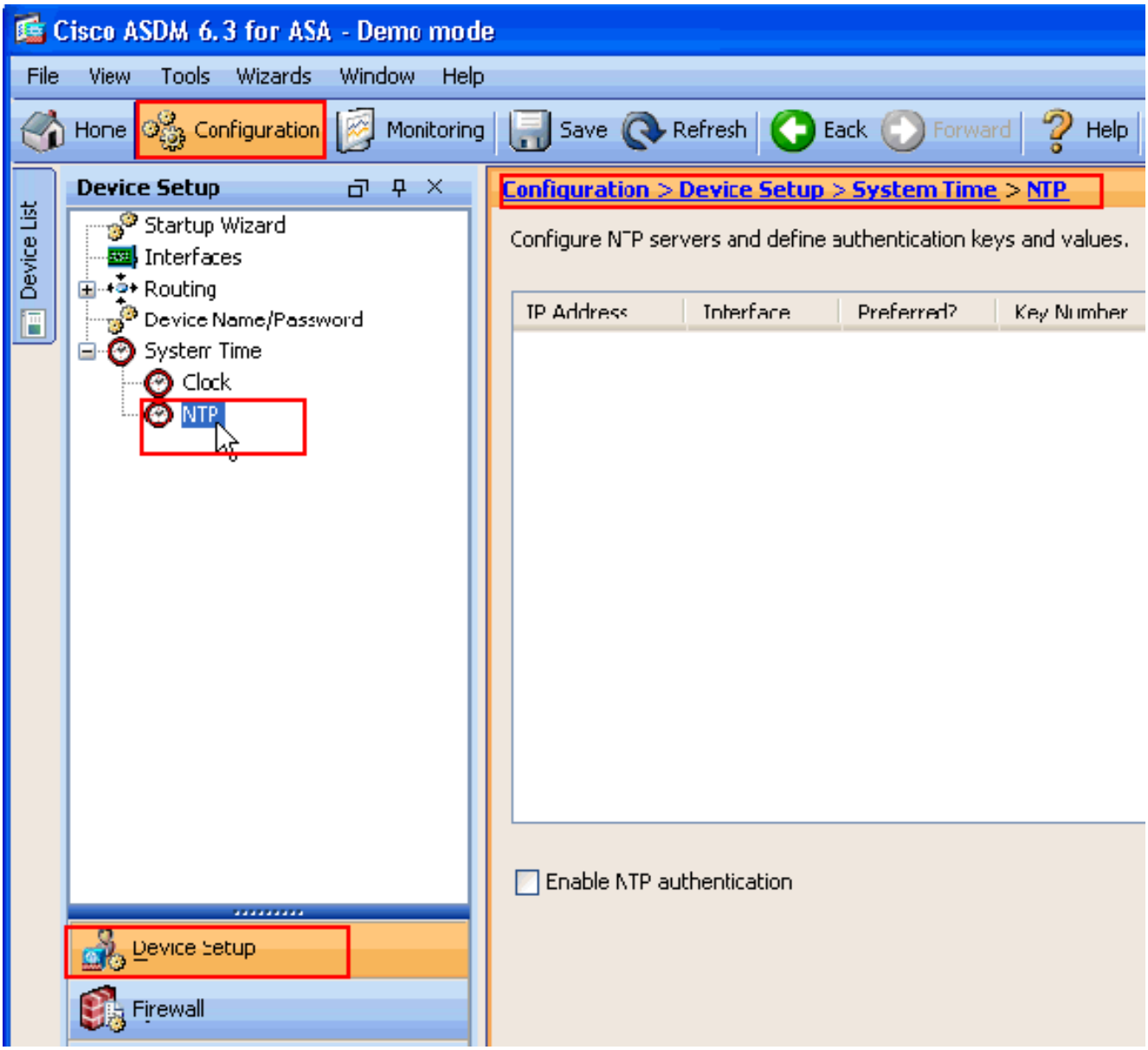
15. يتم عرض السمات التي تم تعريفها بواسطة معالج الشبكة الخاصة الظاهرية (VPN) في هذا الملخص. تحقق مرة أخرى من التكوين وانقر فوق **إنهاء** عندما ترضى بأن الإعدادات صحيحة.



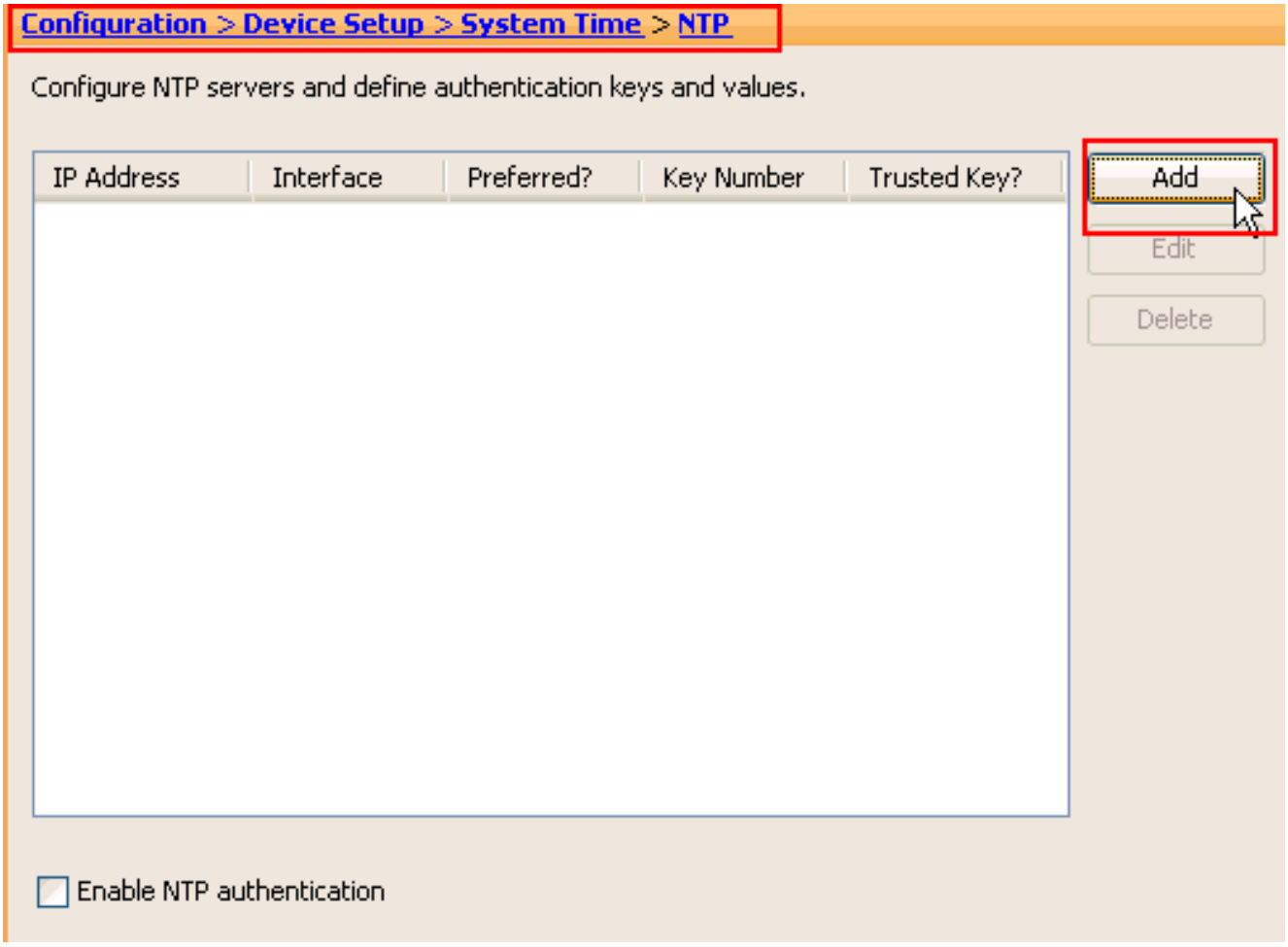
تكوين NTP ASDM

أتمت هذا steps in order to شكلت NTP على ال cisco أمن جهاز:

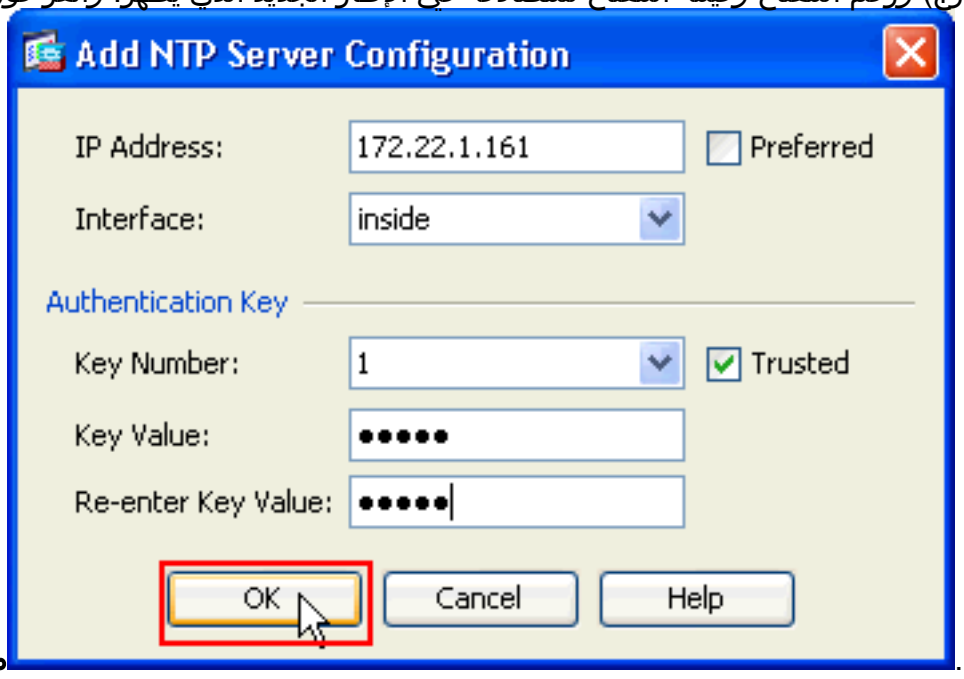
1. أختر **التكوين** في الصفحة الرئيسية ل ASDM.



2. أخترت **أداة setup>نظام وقت**<to in order NTP فتحت ال **NTP** تشكيل صفحة من ASDM.



3. انقر فوق **إضافة** لإضافة خادم NTP وتقديم السمات المطلوبة مثل عنوان IP واسم الواجهة (في الداخل أو الخارج) ورقم المفتاح وقيمة المفتاح للمصادقة في الإطار الجديد الذي يظهر. وانقر فوق

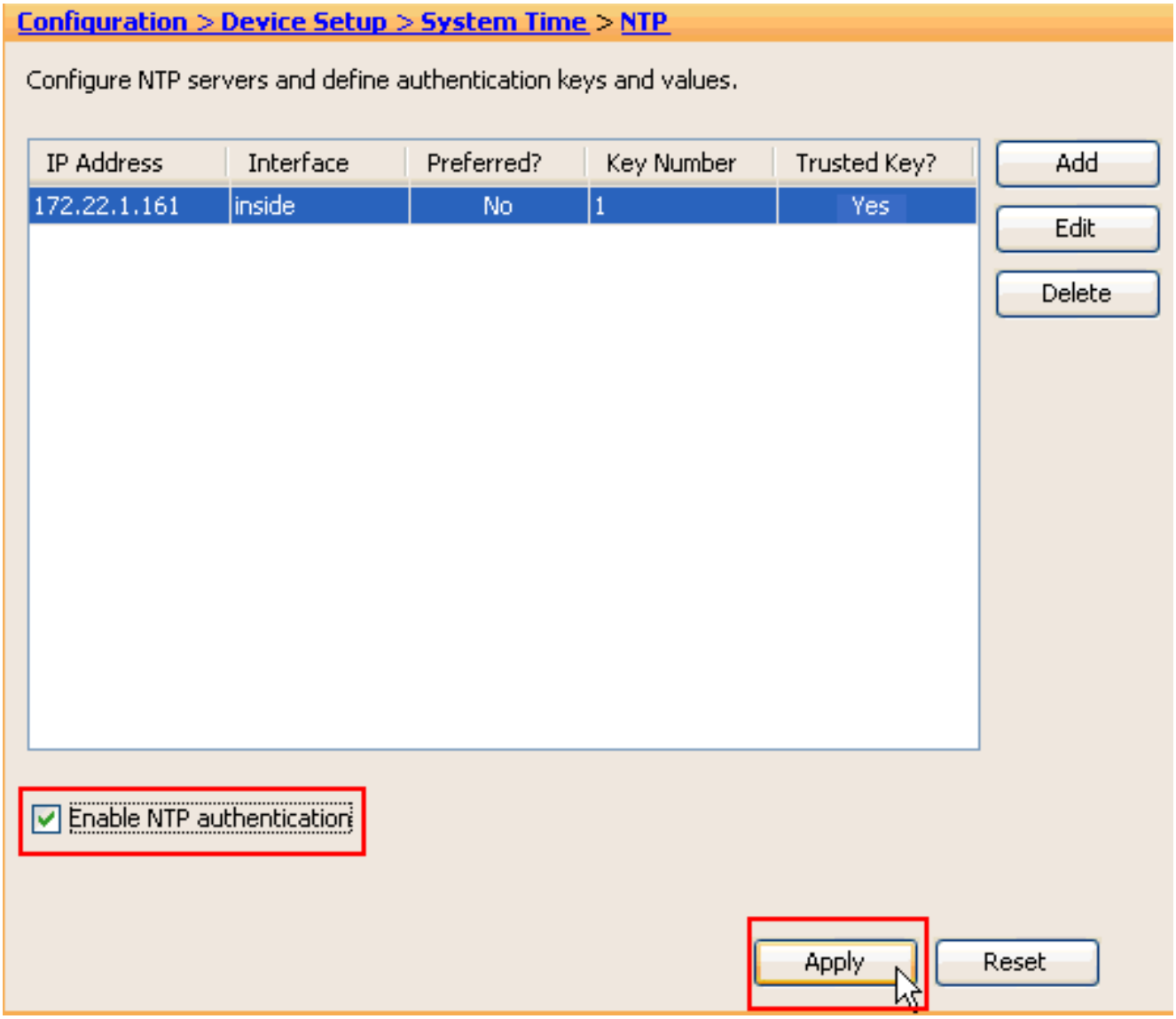


OK.

ملاحظة: ينبغي إختيار اسم الواجهة ليكون داخليا ل ASA1 وخارجا ل ASA2.**ملاحظة:** يجب أن يكون **مفتاح مصادقة NTP** هو نفسه في ASA وخادم NTP.يتم عرض تكوين سمة المصادقة في CLI ل ASA1 و ASA2 هنا:

```
ASA1#ntp authentication-key 1 md5 cisco
ntp trusted-key 1
ntp server 172.22.1.161 key 1 source inside


ASA2#ntp authentication-key 1 md5 cisco
ntp trusted-key 1
ntp server 172.22.1.161 key 1 source outside
```

4. انقر فوق خانة الاختيار **تمكين مصادقة NTP** وانقر فوق **تطبيق**، الذي يكمل مهمة تكوين NTP.



تكوين ASA1 CLI

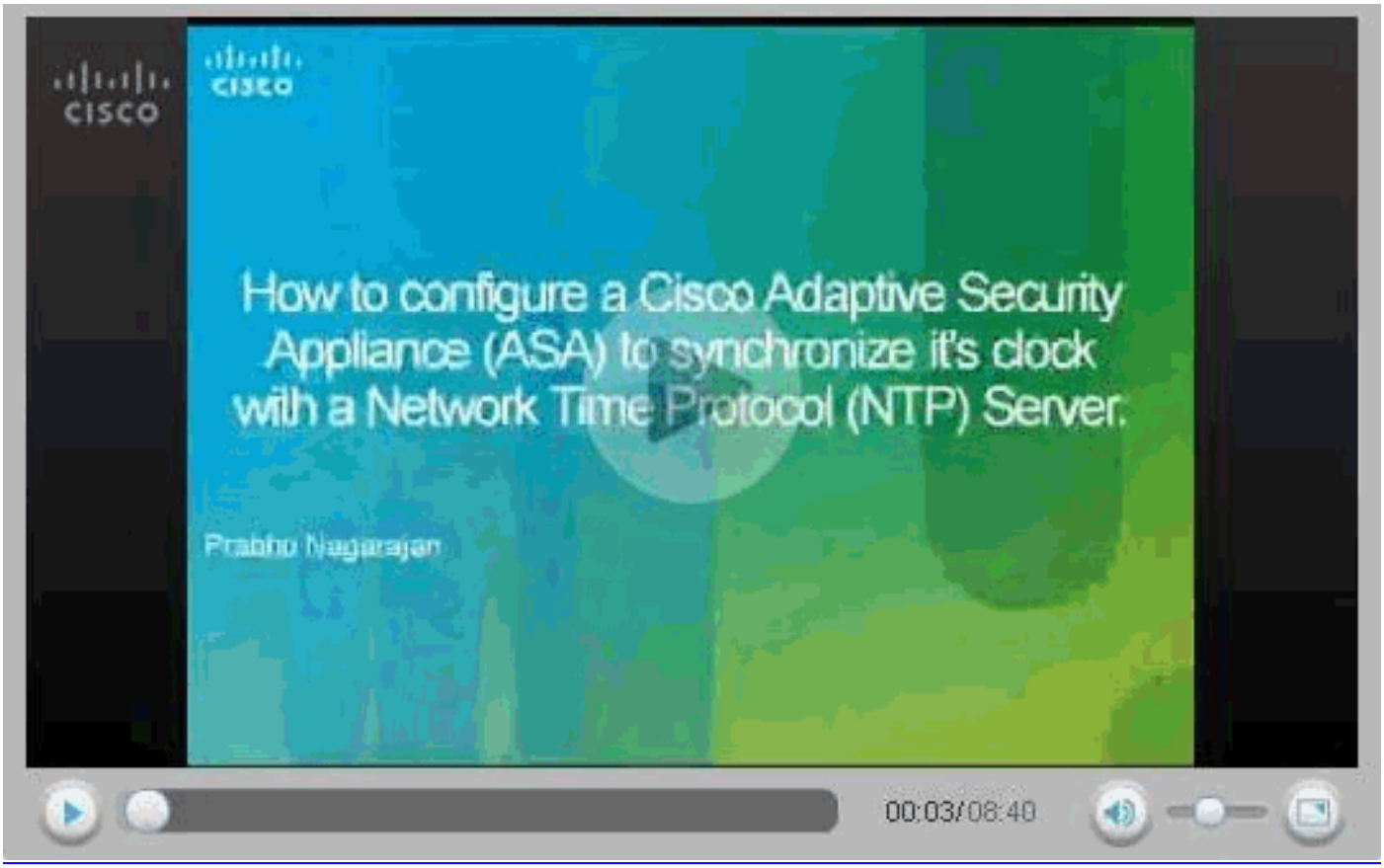
ASA1
ASA#**show run** Saved : (ASA Version 8.3(1 ! hostname ASA1 domain-name default.domain.invalid enable password 8Ry2YjIyt7RRXU24 encrypted names ! interface Ethernet0 nameif outside security-level 0 ip address 10.10.10.1 255.255.255.0 *Configure the outside interface. !* interface *---!* Ethernet1 nameif inside security-level 100 ip address 172.22.1.163 255.255.255.0 *!--- Configure the inside* *interface. ! !-- Output suppressed !* passwd

```
2KFQnbNIdI.2KYOU encrypted ftp mode passive dns server-
    group DefaultDNS domain-name default.domain.invalid
    access-list inside_nat0_outbound extended permit ip
172.22.1.0 255.255.255.0 172 .16.1.0 255.255.255.0 !---
   This access list (inside_nat0_outbound) is used !---
 with the nat zero command. This prevents traffic which
   !--- matches the access list from undergoing network
address translation (NAT). !--- The traffic specified by
   this ACL is traffic that is to be encrypted and !---
sent across the VPN tunnel. This ACL is intentionally !-
-- the same as (outside_cryptomap_20). !--- Two separate
            access lists should always be used in this
                                              .configuration

    access-list outside_cryptomap_20 extended permit ip
                              172.22.1.0 255.255.255.0 172
                                    255.255.255.0 16.1.0.
This access list (outside_cryptomap_20) is used !-- ---!
    - with the crypto map outside_map !--- to determine
 which traffic should be encrypted and sent !--- across
 the tunnel. !--- This ACL is intentionally the same as
 (inside_nat0_outbound). !--- Two separate access lists
          .should always be used in this configuration

                                          pager lines 24
                                        mtu inside 1500
                                       mtu outside 1500
                                            no failover

                                asdm image flash:/asdm-631.bin
 Enter this command to specify the location of the ---!
ASDM image. asdm history enable arp timeout 14400 object
network obj-local subnet 172.22.1.0 255.255.255.0 object
 network obj-remote subnet 172.16.1.0 255.255.255.0 nat
   (inside,outside) 1 source static obj-local obj-local
    destination static obj-remote obj-remote !--- NAT 0
    prevents NAT for networks specified in !--- the ACL
                                         .inside_nat0_outbound

            route outside 0.0.0.0 0.0.0.0 10.10.10.2 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



                                    http server enable
   Enter this command in order to enable the HTTPS ---!
   server !--- for ASDM. http 172.22.1.1 255.255.255.255
    inside !--- Identify the IP addresses from which the
   security appliance !--- accepts HTTPS connections. no
snmp-server location no snmp-server contact !--- PHASE 2
CONFIGURATION ---! !--- The encryption types for Phase 2
   are defined here. crypto ipsec transform-set ESP-AES-
        256-SHA esp-aes-256 esp-sha-hmac !--- Define the
    transform set for Phase 2. crypto map outside_map 20
    match address outside_cryptomap_20 !--- Define which
    traffic should be sent to the IPsec peer. crypto map
 outside_map 20 set peer 10.20.20.1 !--- Sets the IPsec
   peer crypto map outside_map 20 set transform-set ESP-
```

```
AES-256-SHA !--- Sets the IPsec transform set "ESP-AES-
      256-SHA" !--- 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 10. !--- Policy 65535 is included in the config
 by default. !--- The configuration commands here define
the Phase !--- 1 policy parameters that are used. isakmp
enable outside isakmp policy 10 authentication pre-share
    isakmp policy 10 encryption aes-256 isakmp policy 10
      hash sha isakmp policy 10 group 5 isakmp policy 10
  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 tunnel-group 10.20.20.1 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 command !--- tunnel-group
 in global configuration mode. !--- For L2L connections,
the name of the tunnel group MUST be the IP !--- address
                                        .of the IPsec peer




                tunnel-group 10.20.20.1 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
   !--- Define the NTP server authentication-key,Trusted-
key !--- and the NTP server address for configuring NTP.
                                 * ntp authentication-key 1 md5
                                       ntp trusted-key 1

 The NTP server source is to be mentioned as inside ---!
    for ASA1 ntp server 172.22.1.161 key 1 source inside
         Cryptochecksum:ce7210254f4a0bd263a9072a4ccb7cf7
                                                 end :
```

يشرح هذا الفيديو الذي تم نشره إلى مجتمع دعم Cisco باستخدام عرض توضيحي، وهو إجراء تكوين ASA كعميل NTP:

كيفية تكوين جهاز الأمان القابل للتكيف (ASA) من Cisco لمزامنة الساعة مع خادم بروتوكول وقت الشبكة (NTP).



تكوين ASA2 CLI

ASA2

```
                                    (ASA Version 8.3(1
                                                     !
                                          hostname ASA2
                                domain-name default.domain.invalid
                            enable password 8Ry2YjIyt7RRXU24 encrypted
                                                 names
                                                     !
                                      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 172.16.1.1 255.255.255.0
                                                     !
                                 passwd 2KFQnbNIdI.2KYOU encrypted
                                                ftp mode passive
                                       dns server-group DefaultDNS
                                 domain-name default.domain.invalid

access-list inside_nat0_outbound extended permit ip
                                      172.16.1.0 255.255.255.0 172
                                             255.255.255.0 22.1.0.
                                    Note that this ACL is a mirror of the ---!
                                        .inside_nat0_outbound !--- ACL on ASA1

access-list outside_cryptomap_20 extended permit ip
                                      172.16.1.0 255.255.255.0 172
```

```
                                                255.255.255.0 22.1.0.
                                    Note that this ACL is a mirror of the ---!
                                        .outside_cryptomap_20 !--- ACL on ASA1

                                                      pager lines 24
                                                     mtu inside 1500
                                                    mtu outside 1500
                                                         no failover
                                       asdm image flash:/asdm-631.bin
                                               no asdm history enable
                                                     arp timeout 14400
                                             object network obj-local
                                        subnet 172.22.1.0 255.255.255.0

                                           object network obj-remote
                                        subnet 172.16.1.0 255.255.255.0


    nat (inside,outside) 1 source static obj-local obj-local
                                                   destination static
                                            obj-remote obj-remote
                                            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
                                                 http server enable
                                    http 0.0.0.0 0.0.0.0 inside
                                        no snmp-server location
                                         no snmp-server contact
      crypto ipsec transform-set ESP-AES-256-SHA esp-aes-256
                                                      esp-sha-hmac
                        crypto map outside_map 20 match address
                                             outside_cryptomap_20
                   crypto map outside_map 20 set peer 10.10.10.1
    crypto map outside_map 20 set transform-set ESP-AES-256-
                                                             SHA
                        crypto map outside_map interface outside
                                         isakmp enable outside
                      isakmp policy 10 authentication pre-share
                           isakmp policy 10 encryption aes-256
                                     isakmp policy 10 hash sha
                                      isakmp policy 10 group 5
                                isakmp policy 10 lifetime 86400
                          tunnel-group 10.10.10.1 type ipsec-l2l
                       tunnel-group 10.10.10.1 ipsec-attributes
                                             * pre-shared-key
                                       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

  Define the NTP server authentication-key,Trusted- ---!
key !--- and the NTP server address for configuring NTP.
                                  * ntp authentication-key 1 md5
                                                ntp trusted-key 1

The NTP server source is to be mentioned as outside ---!
  for ASA2. ntp server 172.22.1.161 key 1 source outside
                        Cryptochecksum:d5e2ee898f5e8bd28e6f027aeed7f41b
                                                        end :
                                                       #ASA
```

التحقق من الصحة

يوفر هذا القسم معلومات يمكنك إستخدامها للتأكد من أن التكوين يعمل بشكل صحيح.

يتم دعم بعض أوامر **العرض بواسطة** أداة مترجم الإخراج (العملاء المسجلون فقط)، والتي تتيح لك عرض تحليل إخراج أمر **العرض**.

- show ntp status - يعرض معلومات ساعة NTP.

```
ASA1#show ntp status

Clock is synchronized, stratum 2, reference is 172.22.1.161
nominal freq is 99.9984 Hz, actual freq is 99.9983 Hz, precision is 2**6
reference time is ccf22b77.f7a6e7b6 (13:28:23.967 UTC Tue Dec 16 2008)
clock offset is 34.8049 msec, root delay is 4.78 msec
root dispersion is 60.23 msec, peer dispersion is 25.41 msec
```

- show ntp associations [detail] - يعرض اقترانات خادم وقت الشبكة التي تم تكوينها.

```
ASA1#show ntp associations detail

172.22.1.161 configured, authenticated, our_master, sane, valid, stratum 1
ref ID .LOCL., time ccf2287d.3668b946 (13:15:41.212 UTC Tue Dec 16 2008)
our mode client, peer mode server, our poll intvl 64, peer poll intvl 64
root delay 0.00 msec, root disp 0.03, reach 7, sync dist 23.087
delay 4.52 msec, offset 9.7649 msec, dispersion 20.80
precision 2**19, version 3
org time ccf22896.f1a4fca3 (13:16:06.943 UTC Tue Dec 16 2008)
rcv time ccf22896.efb94b28 (13:16:06.936 UTC Tue Dec 16 2008)
xmt time ccf22896.ee5691dc (13:16:06.931 UTC Tue Dec 16 2008)
filtdelay =     4.52    4.68    4.61    0.00    0.00    0.00    0.00    0.00
filtoffset =    9.76    7.09    3.85    0.00    0.00    0.00    0.00    0.00
filterror =    15.63   16.60   17.58 14904.3 14904.3 14904.3 14904.3 14904.3
```

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

أوامر استكشاف الأخطاء وإصلاحها

يتم دعم بعض أوامر **العرض بواسطة** أداة مترجم الإخراج (العملاء المسجلون فقط)، والتي تتيح لك عرض تحليل إخراج أمر **العرض**.

ملاحظة: قبل إصدار أوامر **تصحيح الأخطاء**، راجع المعلومات المهمة في أوامر تصحيح الأخطاء.

- **debug ntp صحة** - يعرض صحة ساعة نظير NTP.هذا output **debug** من عدم تطابق المفتاح:

```
NTP: packet from 172.22.1.161 failed validity tests 10
                                    Authentication failed
```

- **debug ntp packet** - يعرض معلومات حزمة NTP.عندما لا توجد إستجابة من الخادم، لا يتم مشاهدة سوى حزمة xmit `NTP` على ASA بدون حزمة `NTP rcv`.

```
:ASA1# NTP: xmit packet to 172.22.1.161
                        leap 0, mode 3, version 3, stratum 2, ppoll 64
(rtdel 012b (4.562), rtdsp 0cb6 (49.652), refid ac1601a1 (172.22.1.161
                    (ref ccf22916.f1211384 (13:18:14.941 UTC Tue Dec 16 2008
                    (org ccf22916.f426232d (13:18:14.953 UTC Tue Dec 16 2008
                    (rec ccf22916.f1211384 (13:18:14.941 UTC Tue Dec 16 2008
                    (xmt ccf22956.f08ee8b4 (13:19:18.939 UTC Tue Dec 16 2008
                :NTP: rcv packet from 172.22.1.161 to 172.22.1.163 on inside
                        leap 0, mode 4, version 3, stratum 1, ppoll 64
  (rtdel 0000 (0.000), rtdsp 0002 (0.031), refid 4c4f434c (76.79.67.76
                    (ref ccf2293d.366a4808 (13:18:53.212 UTC Tue Dec 16 2008
                    (org ccf22956.f08ee8b4 (13:19:18.939 UTC Tue Dec 16 2008
                    (rec ccf22956.f52e480e (13:19:18.957 UTC Tue Dec 16 2008
                    (xmt ccf22956.f5688c29 (13:19:18.958 UTC Tue Dec 16 2008
                    (inp ccf22956.f982bcd9 (13:19:18.974 UTC Tue Dec 16 2008
```

معلومات ذات صلة

- مدير أجهزة حلول الأمان المعدلة من Cisco
- أجهزة الأمان المعدلة Cisco ASA 5500 Series Adaptive Security Appliances
- 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).