

# IPsec فن نيوكت لاثم عم ASA/PIX لاثم ل اذه نودبو

## المحتويات

- [المقدمة](#)
- [المتطلبات الأساسية](#)
- [المتطلبات](#)
- [المكونات المستخدمة](#)
- [المنتجات ذات الصلة](#)
- [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 نموذجاً للتكوين لمزامنة ساعة جهاز الأمان PIX/ASA مع خادم وقت الشبكة باستخدام بروتوكول وقت الشبكة (NTP). تتصل ASA1 مباشرة بخادم وقت الشبكة ASA2 عبر حركة مرور بيانات NTP من خلال نفق IPsec إلى ASA1، والذي يقوم بدوره بإعادة توجيه الحزم إلى خادم وقت الشبكة.

ارجع إلى [ASA 8.3 والإصدارات الأحدث: NTP مع مثال تكوين نفق IPsec وبدون](#) للحصول على مزيد من المعلومات حول التكوين المتطابق على Cisco ASA مع الإصدارات 8.3 والإصدارات الأحدث.

ملاحظة: يمكن أيضاً استخدام موجه كخادم NTP لمزامنة ساعة جهاز أمان PIX/ASA.

## المتطلبات الأساسية

### المتطلبات

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

- يجب إنشاء اتصال IPsec الشامل قبل بدء تكوين NTP هذا.
- يجب تمكين ترخيص جهاز الأمان لتشفير معيار تشفير البيانات (DES) (على أدنى مستوى تشفير).

## المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية أدناه.

- أجهزة الأمان المعدلة (Cisco Adaptive Security Appliance(ASA مع الإصدار x.7 والإصدارات الأحدث
- ASDM الإصدار x.5 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 المستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

## المنتجات ذات الصلة

كما يمكن استخدام هذا التكوين مع جهاز الأمان Cisco PIX 500 Series Security Appliance، والذي يشغل الإصدار x.7 والإصدارات الأحدث.

ملاحظة: تمت إضافة دعم NTP في الإصدار 6.2 من بروتوكول PIX. ارجع إلى [PIX 6.2: NTP باستخدام مثال تكوين نفق IPsec وبدون هذا المثال](#) لتكوين NTP على جدار حماية Cisco PIX.

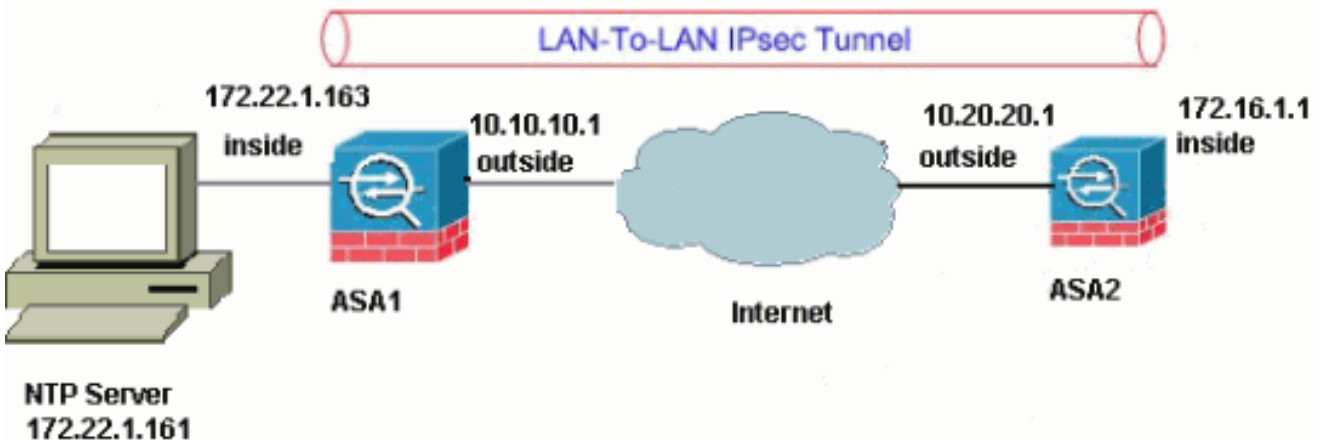
## الاصطلاحات

راجع [اصطلاحات تلميح Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.](#)

## التكوين

### الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة الموضح في هذا الرسم التخطيطي.



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 ASDM NTP](#)

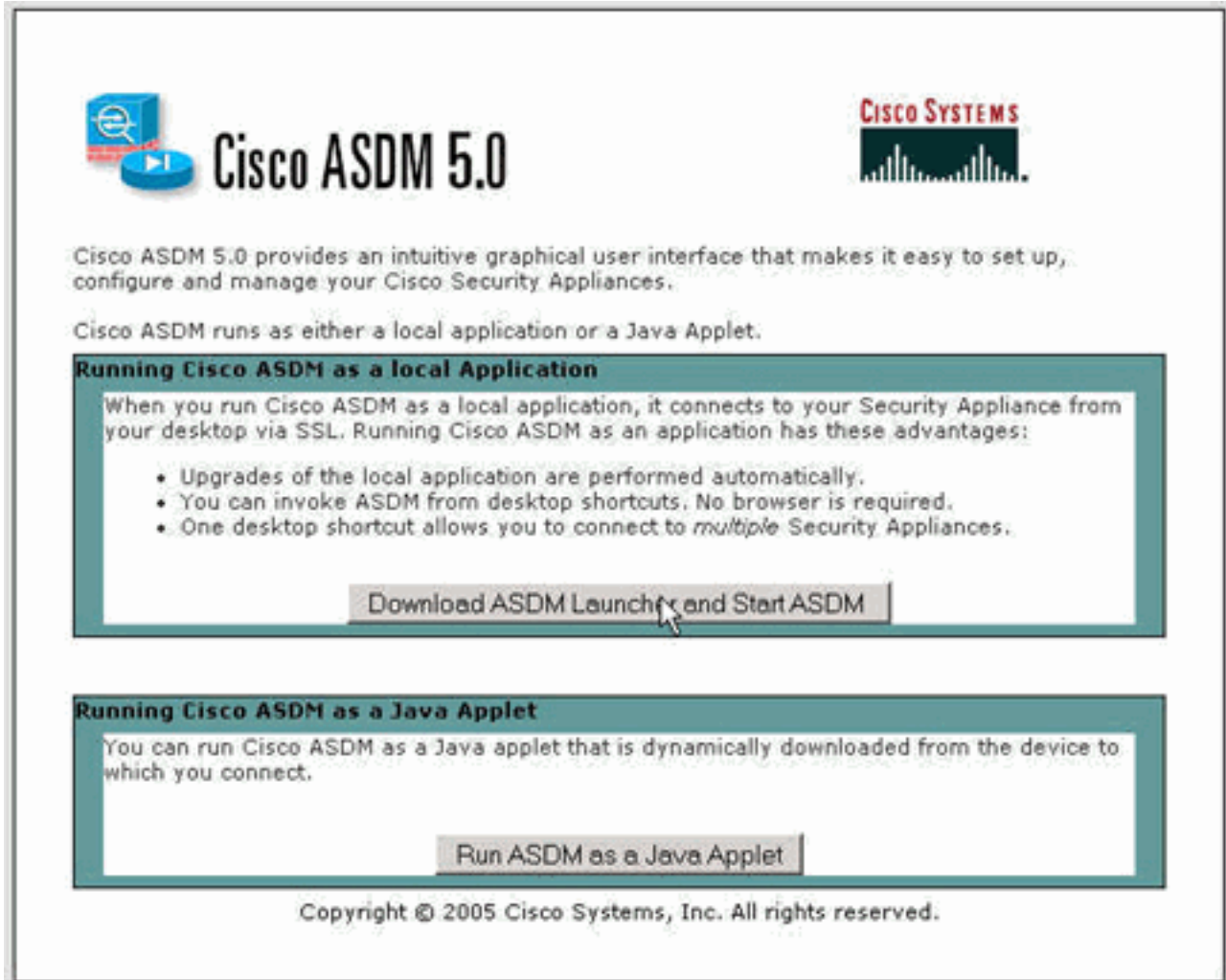
• [تكوين ASA1 CLI](#)

• [تكوين ASA2 CLI](#)

## تكوين ASDM لنفق VPN

أتمت هذا steps أن يخلق ال VPN نفق:

1. افتح المستعرض واكتب [https://<inside\\_ip\\_address\\_of\\_asa>](https://<inside_ip_address_of_asa>) للوصول إلى ASDM على ASA. تأكد من تحويل أية تحذيرات يعطيك المستعرض لها علاقة بموثوقية شهادة SSL. التقصير username وكلمة على حد سواء فارغ. يقدم ASA هذا الإطار للسماح بتنزيل تطبيق ASDM. يقوم هذا المثال بتحميل التطبيق على الكمبيوتر المحلي ولا يعمل في تطبيق Java.



**Cisco ASDM 5.0**

Cisco ASDM 5.0 provides an intuitive graphical user interface that makes it easy to set up, configure and manage your Cisco Security Appliances.

Cisco ASDM runs as either a local application or a Java Applet.

**Running Cisco ASDM as a local Application**

When you run Cisco ASDM as a local application, it connects to your Security Appliance from your desktop via SSL. Running Cisco ASDM as an application has these advantages:

- Upgrades of the local application are performed automatically.
- You can invoke ASDM from desktop shortcuts. No browser is required.
- One desktop shortcut allows you to connect to *multiple* Security Appliances.

[Download ASDM Launcher and Start ASDM](#)

**Running Cisco ASDM as a Java Applet**

You can run Cisco ASDM as a Java applet that is dynamically downloaded from the device to which you connect.

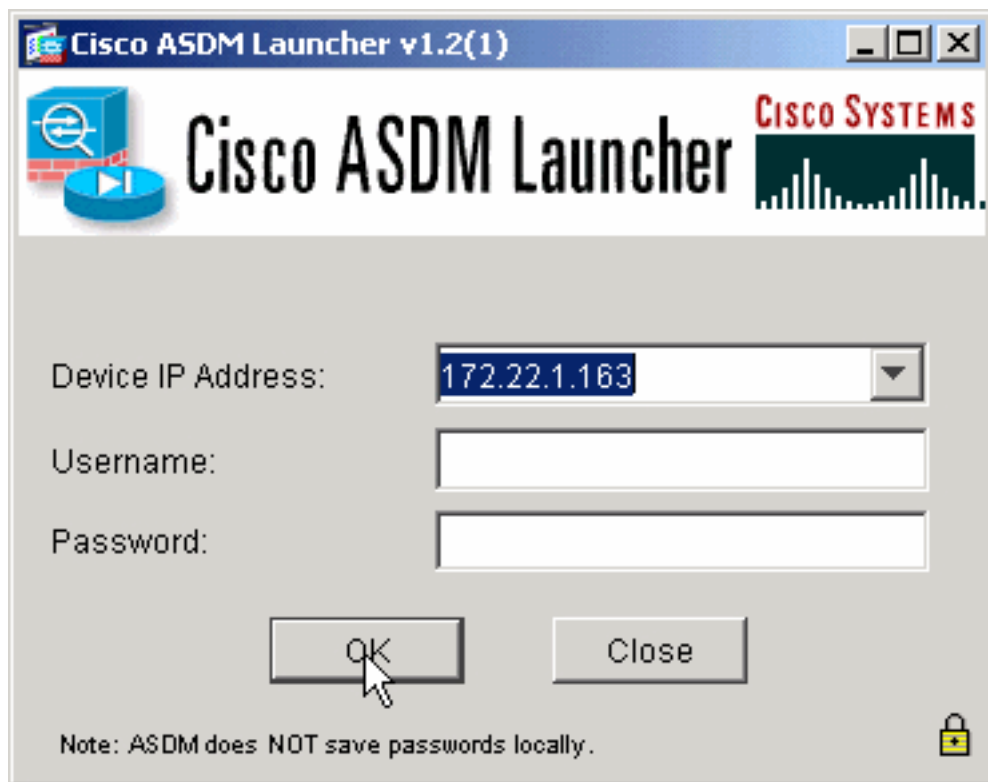
[Run ASDM as a Java Applet](#)

Copyright © 2005 Cisco Systems, Inc. All rights reserved.

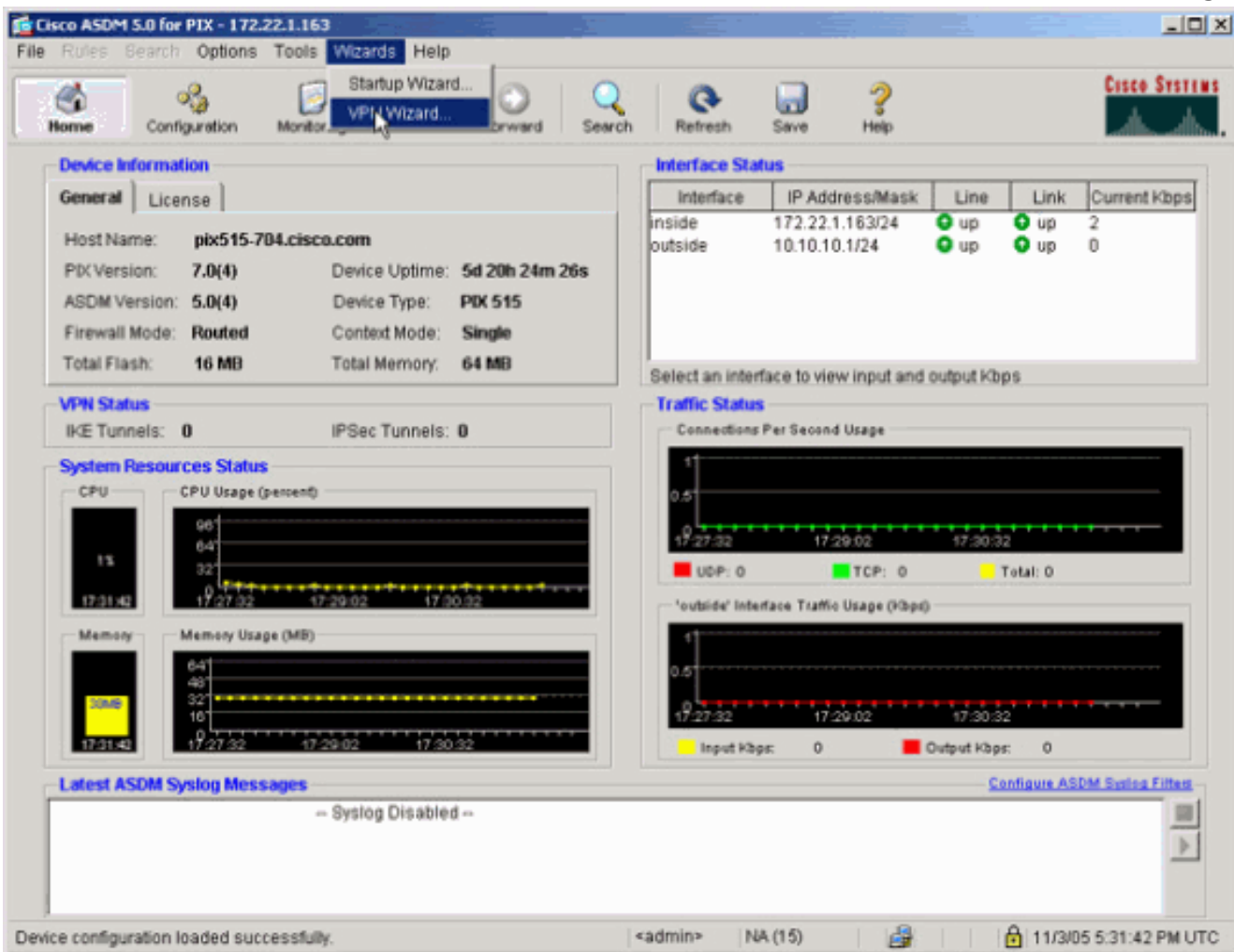
2. انقر على **تنزيل مشغل ASDM** وابدأ **ASDM** لتنزيل المثبت الخاص بتطبيق ASDM.

3. بمجرد تنزيل مشغل ASDM، قم بإكمال الخطوات التي توجهها المطالبات لتثبيت البرنامج وتشغيل مشغل ASDM من Cisco.

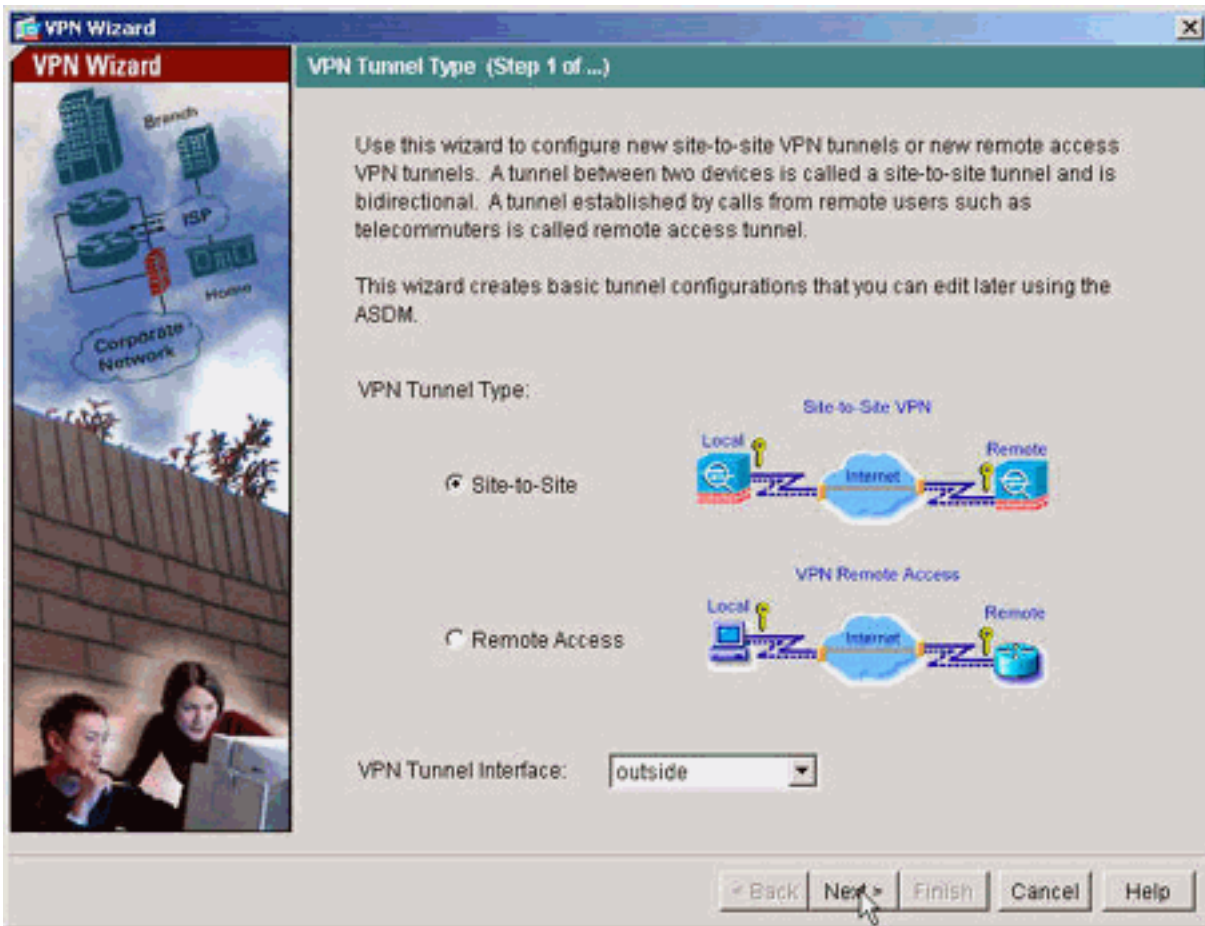
4. أدخل عنوان IP للواجهة التي قمت بتكوينها باستخدام الأمر **http** - واسم مستخدم وكلمة مرور إذا قمت بتحديد واحد. يستعمل هذا مثال التقصير فارغ **username**



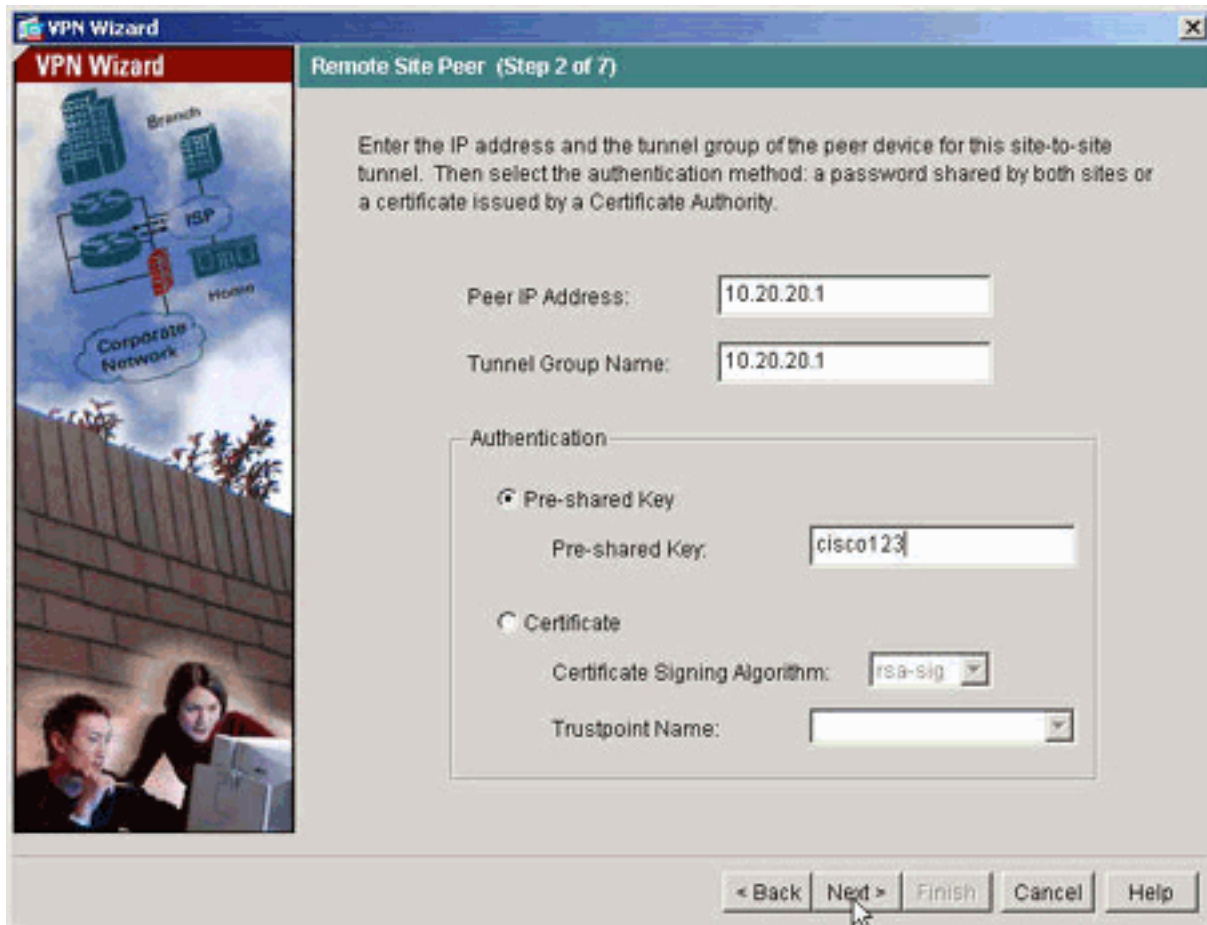
5. قم بتشغيل معالج VPN بمجرد اتصال تطبيق ASDM بـ ASA وكلمة.



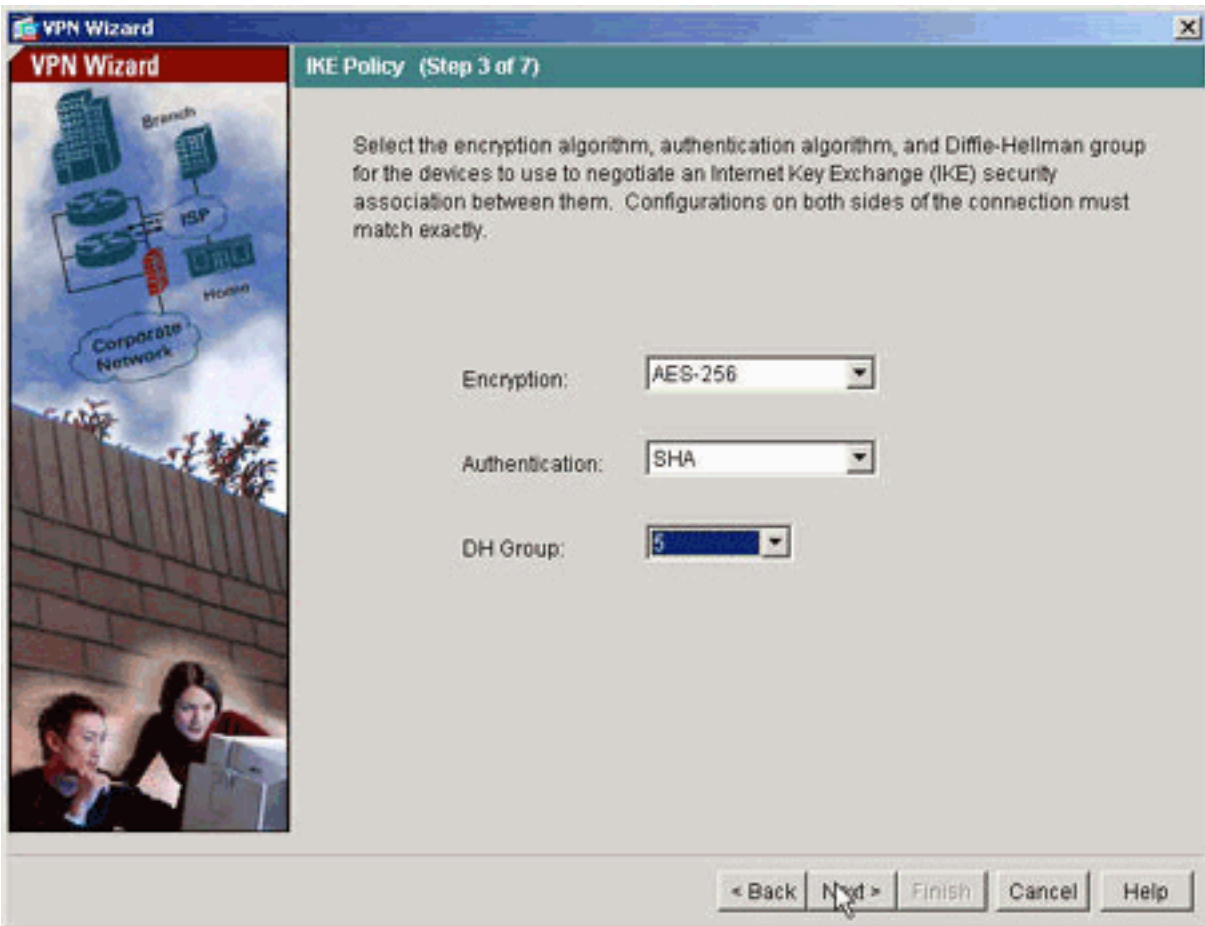
6. أختار نوع نفق VPN من موقع إلى موقع



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

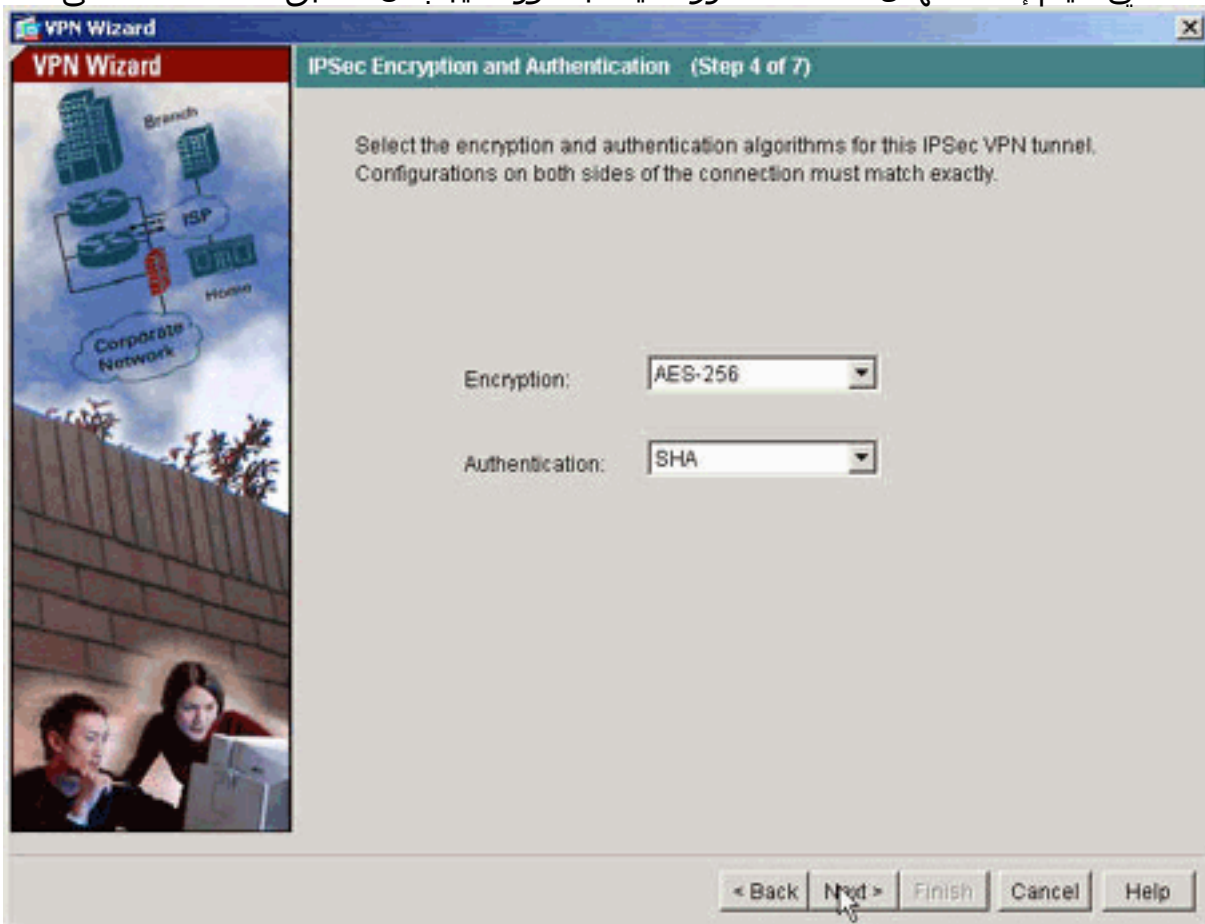


المثال. 8. حدد السمات التي سيتم إستخدامها ل IKE، والمعروفة أيضا بالطور 1. يجب أن تكون هذه السمات واحدة على كلا جانبي



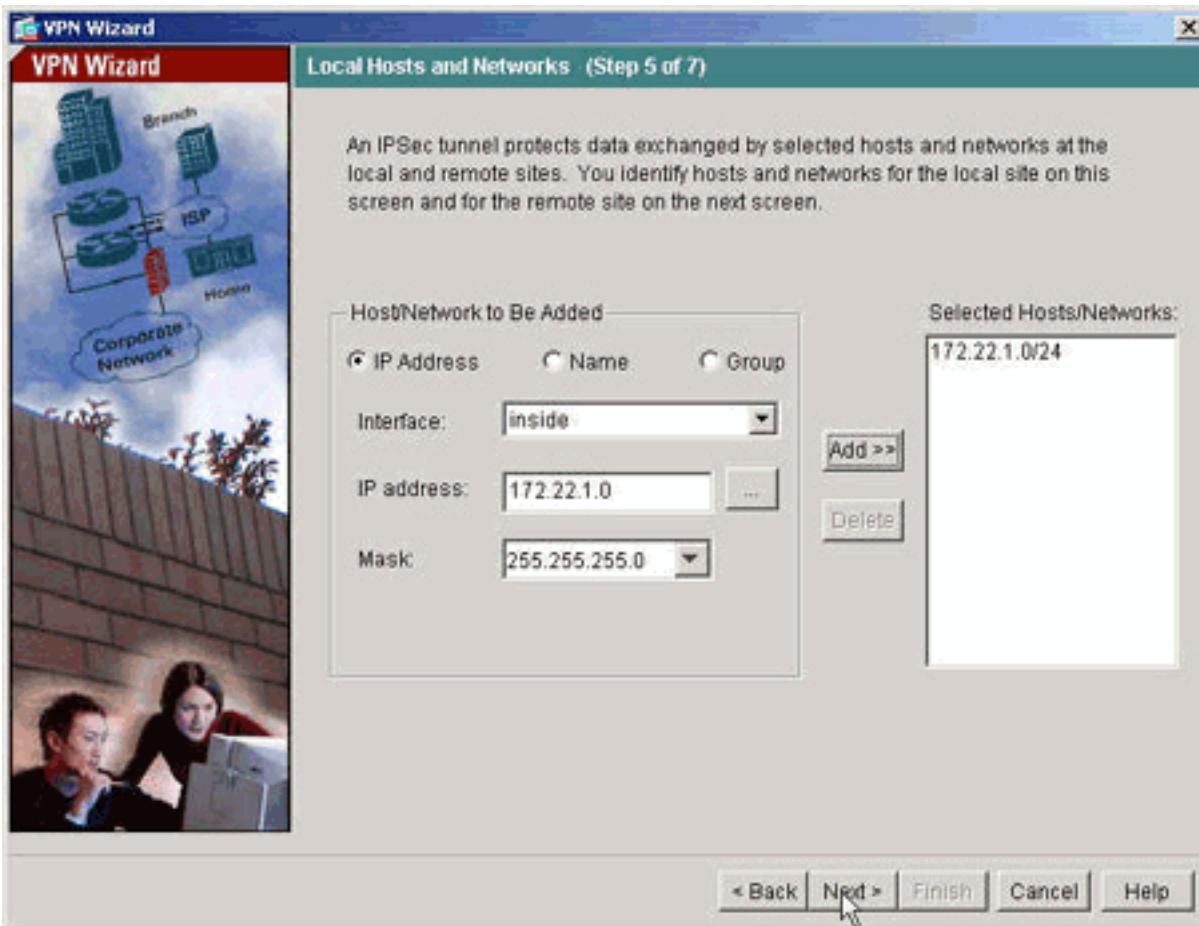
النفق.

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



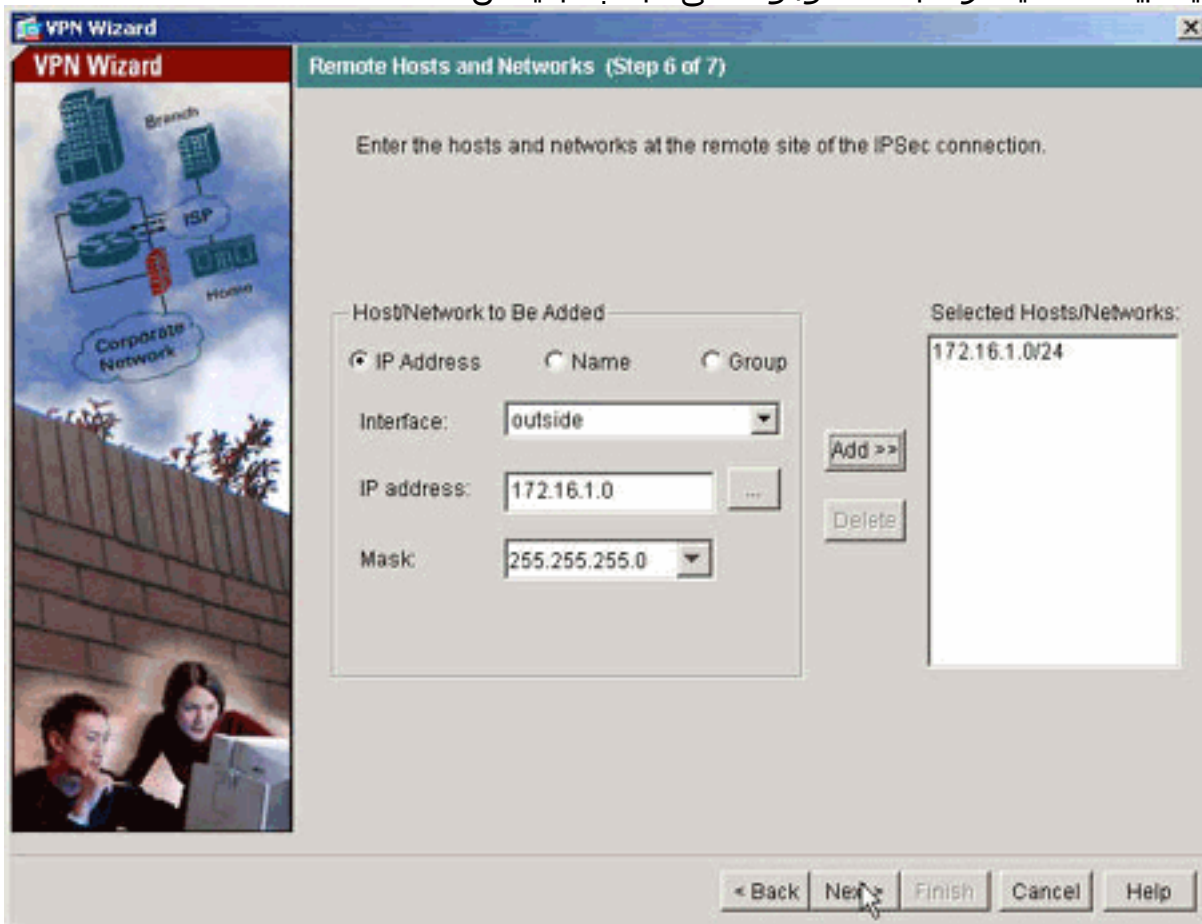
الجانين.

10. حدد البيانات المضيغة التي يجب السماح لحركة مرور البيانات الخاصة بها بالمرور من خلال نفق VPN. في هذه الخطوة، عينت المضيف محلي إلى



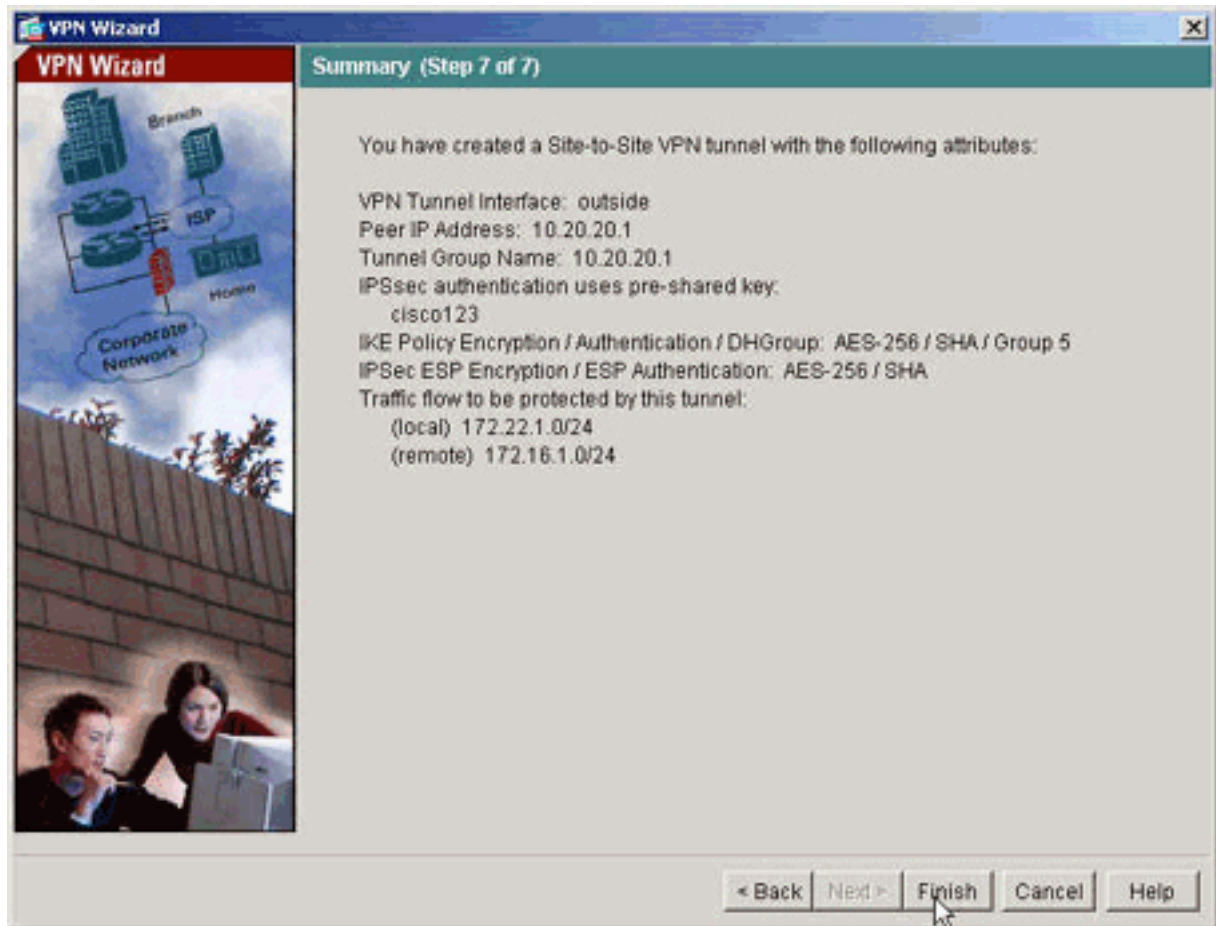
ASA1

11. يتم تحديد البيئات المضيفة والشبكات الموجودة على الجانب البعيد من



النفق.

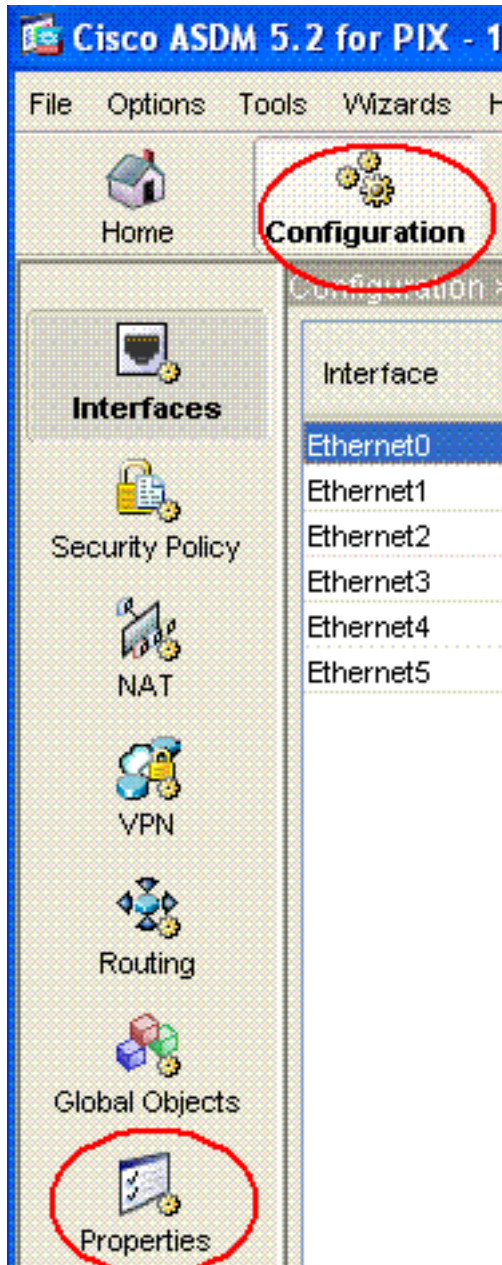
12. يتم عرض السمات التي تم تعريفها بواسطة معالج الشبكة الخاصة الظاهرية (VPN) في هذا الملخص. تحقق مرة أخرى من التكوين وانقر فوق إنهاء عندما ترضى بأن الإعدادات صحيحة.



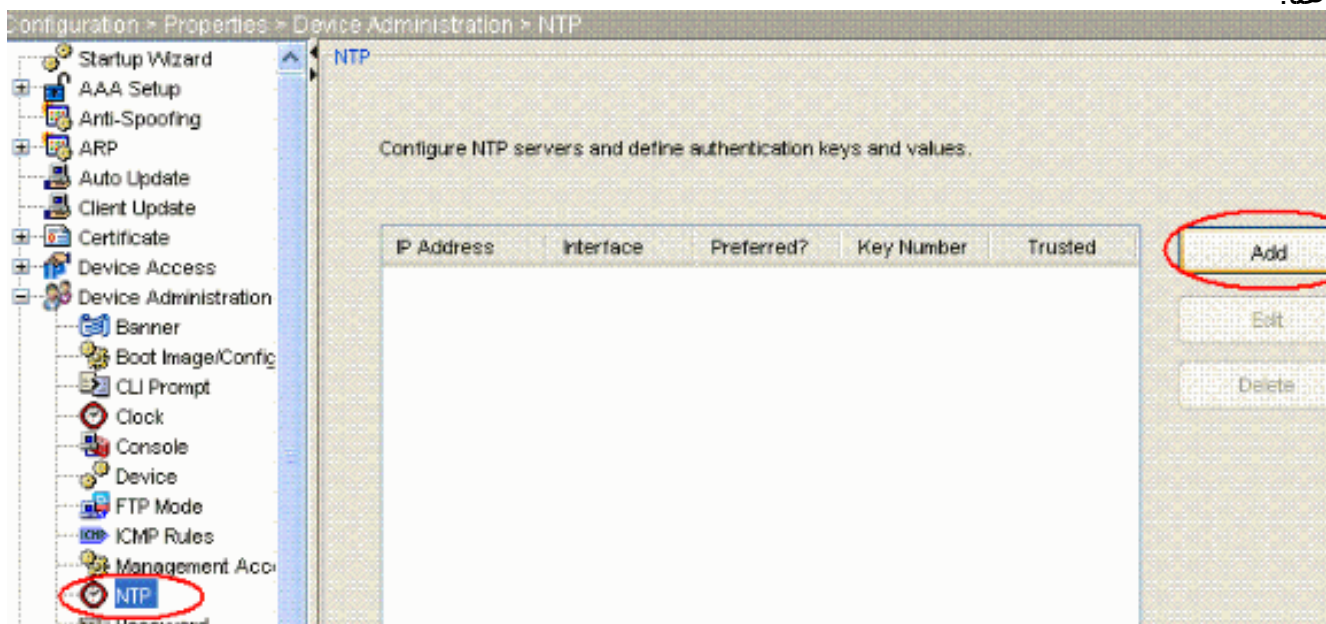
## [تكوين NTP ASDM](#)

أتمت هذا steps أن يشكّل NTP على ال Cisco أمن جهاز:





1. أختار التكوين في الصفحة الرئيسية ASDM كما هو موضح هنا:
2. أختار الآن خصائص < إدارة الأجهزة > NTP لفتح صفحة تكوين NTP ل ASDM كما هو موضح هنا:



3. انقر فوق الزر إضافة لإضافة خادم NTP وتوفير السمات المطلوبة مثل عنوان IP واسم الواجهة (في الداخل أو

الخارج) ورقم المفتاح وقيمة المفتاح لعملية المصادقة في النافذة الجديدة التي تظهر بعد النقر فوق الزر ADD كما هو موضح في لقطة الشاشة. ثم انقر فوق

The screenshot shows a dialog box titled "Add NTP Server Configuration". It has a blue header bar with a close button on the right. The main area is light gray with a grid pattern. It contains the following fields and controls:

- IP Address:** A text box containing "172.22.1.161" and a checkbox labeled "Preferred" which is unchecked.
- Interface:** A dropdown menu showing "inside".
- Authentication Key:** A section with a blue header containing:
  - Key Number:** A dropdown menu showing "1" and a checkbox labeled "Trusted" which is checked.
  - Key Value:** A text box containing "\*\*\*\*\*".
  - Reenter Key Value:** A text box containing "\*\*\*\*\*".
- Buttons:** At the bottom, there are three buttons: "OK", "Cancel", and "Help". The "OK" button is circled in red.

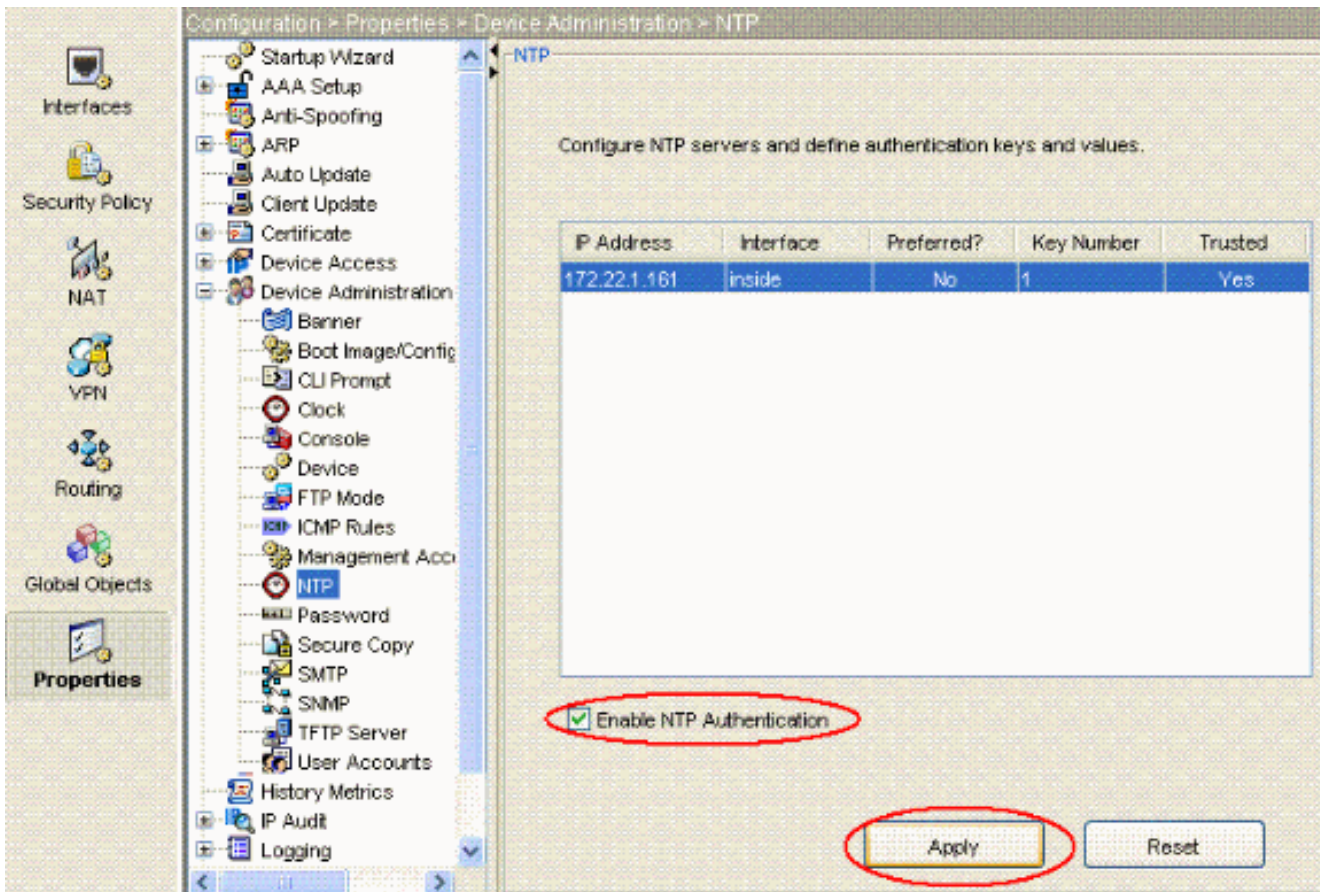
ملا .OK

حظة: 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 أدناه:

```
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 الآن فوق خانة الاختيار تمكين مصادقة NTP وانقر فوق تطبيق، الذي يكمل مهمة تكوين NTP.



## ASA1 CLI تڪوڻ

```

ASA1
ASA#show run
Saved :
(ASA Version 7.1(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
2KFQnbNIIdI.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-511.bin
Enter this command to specify the location of the ---!
ASDM image. asdm history enable arp timeout 14400 nat
    (inside) 0 access-list inside_nat0_outbound !--- 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-
121 !--- 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

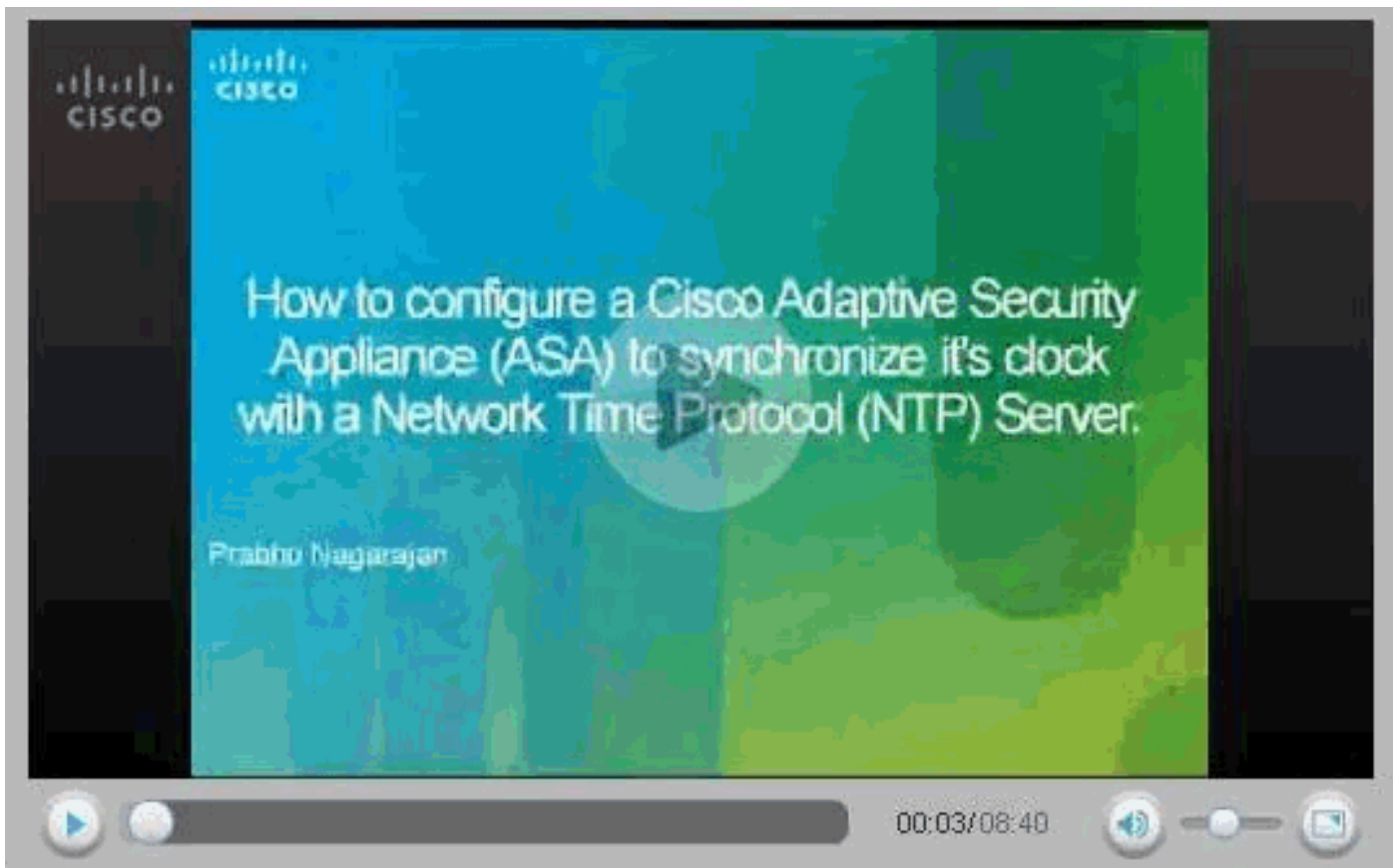
tunnel-group 10.20.20.1 ipsec-attributes
* pre-shared-key
Enter the pre-shared-key in order to configure the ---!
!--- authentication method. telnet timeout 5 ssh timeout
5 console timeout 0 ! class-map inspection_default match
default-inspection-traffic ! ! policy-map global_policy
class inspection_default inspect dns maximum-length 512
inspect ftp inspect h323 h225 inspect h323 ras inspect
netbios inspect rsh inspect rtsp inspect skinny inspect
esmtplib 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 نسخة تجريبية، وهو إجراء تكوين ASA كعميل :NTP

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



## [ASA2 CLI تكوين](#)

```
ASA2

      (ASA Version 7.1(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-511.bin
    no asdm history enable
    arp timeout 14400
    nat (inside) 0 access-list inside_nat0_outbound
        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 استخدامها 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

ASA1#show ntp associations [detail]
ASA1#show ntp associations detail
configured, authenticated, our_master, sane, valid, stratum 1 172.22.1.161
(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
filtererror = 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 debug output 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

```
.NTP rcv حزمة NTP xmit على ASA بدون حزمة NTP
: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

- [برنامج جدار حماية Cisco PIX](#)
- [مدير أجهزة حلول الأمان المعدلة من Cisco](#)
- [أجهزة الأمان المعدلة Cisco ASA 5500 Series Adaptive Security Appliances](#)
- [مراجع أوامر جدار حماية PIX الآمن من Cisco](#)
- [طلبات التعليقات \(RFCs\)](#)
- [الدعم التقني والمستندات - Cisco Systems](#)

ةمچرتل هذه ل و ح

ةيلأل تاي نقتل ن مة و مچم مادختساب دن تسمل اذ ه Cisco ت مچرت  
ملاعلاء ان أ عي مچ ي ف ن ي م دخت سمل ل م عدد ي و تح م مي دقت ل ي رش ب ل و  
امك ة ق ي قد ن و ك ت ن ل ة ي ل أ مچرت ل ض ف أ ن أ ة ظ حال م ي ج ر ي . ة ص ا خ ل م ه ت غ ل ب  
Cisco ي ل خ ت . ف ر ت ح م مچرت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة مچرت ل ا ع م ل ا ح ل ا و ه  
ي ل ا م ا د ع و ج ر ل ا ب ي ص و ت و ت ا مچرت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Cisco  
Systems (ر ف و ت م ط ب ا ر ل ا) ي ل ص أ ل ا ي ز ي ل ج ن إ ل ا دن تسمل ا