ASA مع WebVPN وتسجيل دخول أحادي NTLMv1 و ASDM تكوين مثال تكوين باستخدام

المحتويات

المقدمة

يصف هذا المستند كيفية تكوين جهاز الأمان القابل للتكيف (ASA) من Cisco لتمرير بيانات اعتماد تسجيل دخول مستخدم WebVPN تلقائيا، بالإضافة إلى المصادقة الثانوية، إلى الخوادم التي تتطلب التحقق من تسجيل الدخول الإضافي مقابل Windows Active Directory الذي يشغل الإصدار 1 من مدير شبكة LAN NT (NTLMv1). تعرف هذه الميزة باسم تسجيل الدخول الأحادي (SSO). وهو يمنح الارتباطات التي تم تكوينها لمجموعة WebVPN معينة القدرة على تمرير معلومات مصادقة المستخدم هذه، وبالتالي تقليل مطالبات المصادقة المتعددة. كما يمكن إستخدام هذه الميزة على مستوى التكوين العام أو مستوى تكوين المستخدم.

المتطلبات الأساسية

المتطلبات

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

- تأكد من تكوين أذونات NTLMv1 و Windows لمستخدمي VPN الهدف. راجع وثائق Microsoft للحصول على مزيد من المعلومات حول حقوق الوصول إلى مجال Windows.

المكونات المستخدمة

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

- Cisco ASA 7.1(1)
- مدير أجهزة حلول الأمان المعدلة (ASDM) 5.1(2) من Cisco
- خدمات معلومات الإنترنت (IIS) من Microsoft

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.

الاصطلاحات

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

التكوين

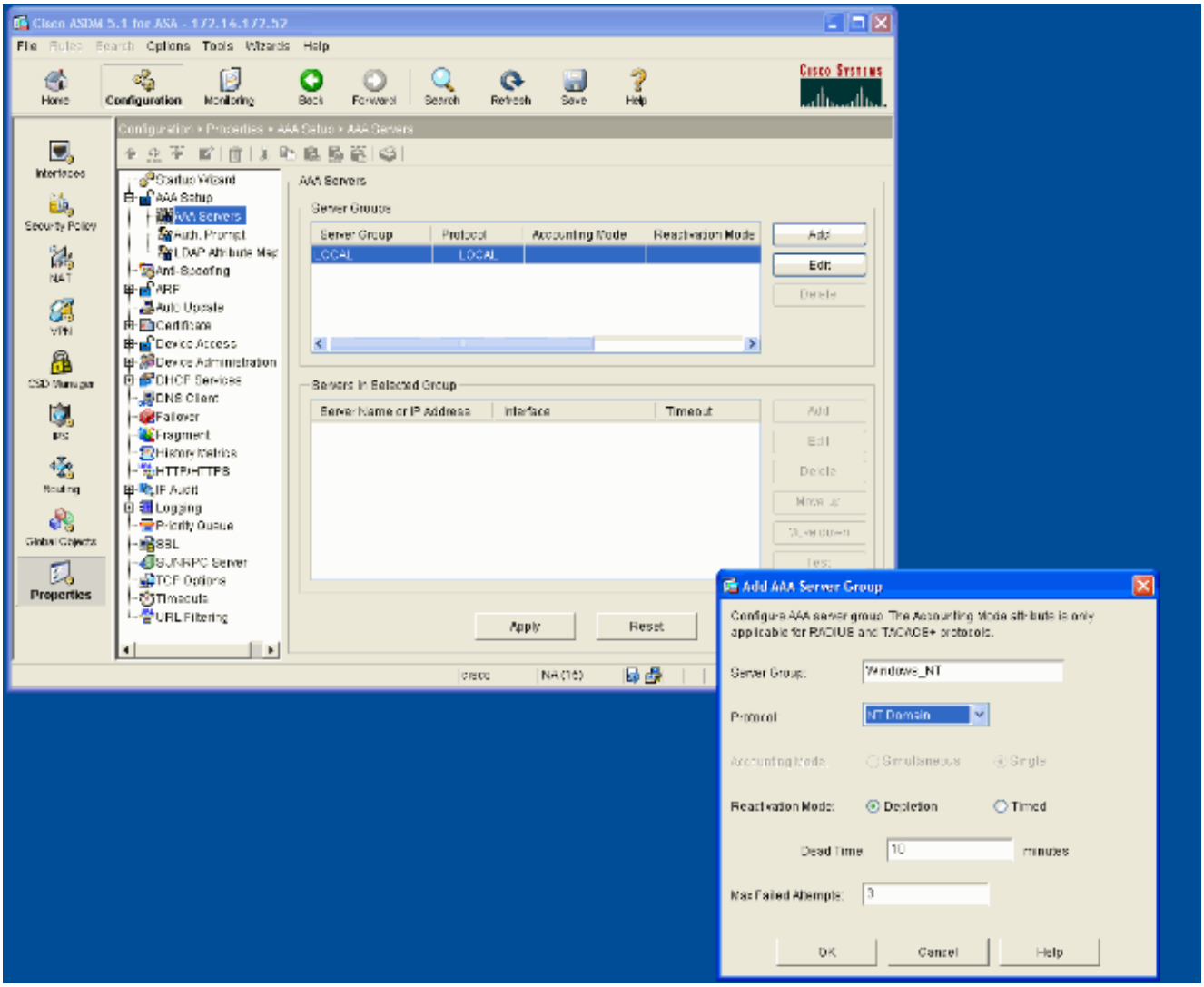
في هذا القسم، تقدم لك معلومات تكوين ASA كخادم WebVPN مع SSO.

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

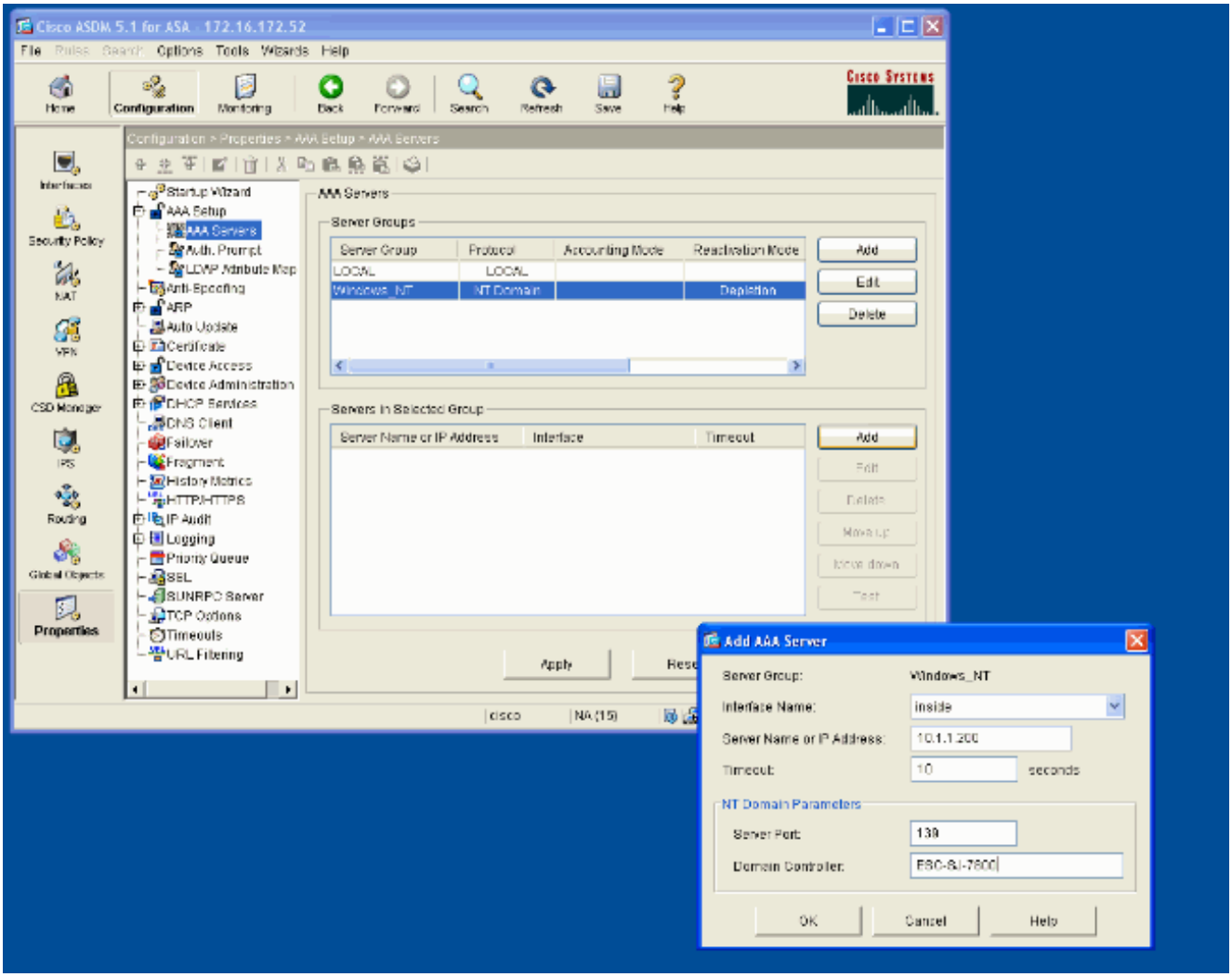
إضافة خادم AAA لمصادقة مجال Windows

أكمل هذه الخطوات لتكوين ASA لاستخدام وحدة تحكم بالمجال للمصادقة.

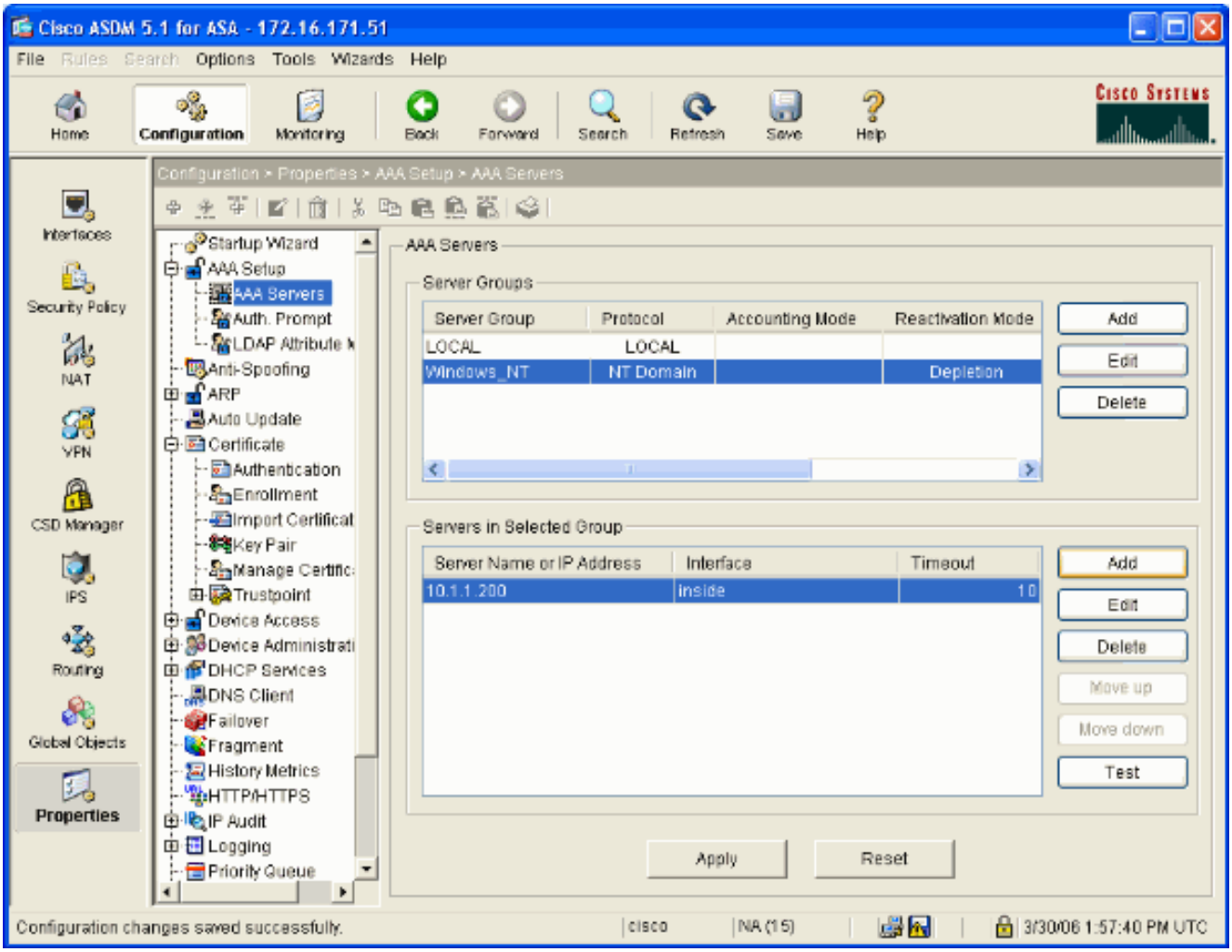
1. حدد **تكوين > خصائص > إعداد AAA > خوادم AAA** وانقر **إضافة**. قم بتوفير اسم لمجموعة الخوادم، مثل Windows_NT، واختر **مجال NT** كبروتوكول.



2. إضافة خادم Windows.حدد المجموعة التي تم إنشاؤها حديثا وانقر فوق **إضافة**. حدد الواجهة التي يوجد بها الخادم وأدخل عنوان IP واسم وحدة التحكم بالمجال. تأكد من إدخال اسم وحدة التحكم بالمجال في كافة الأحرف الكبيرة. انقر فوق موافق عند
الانتهاء.



تعرض هذه النافذة تكوين AAA
المكتمل:

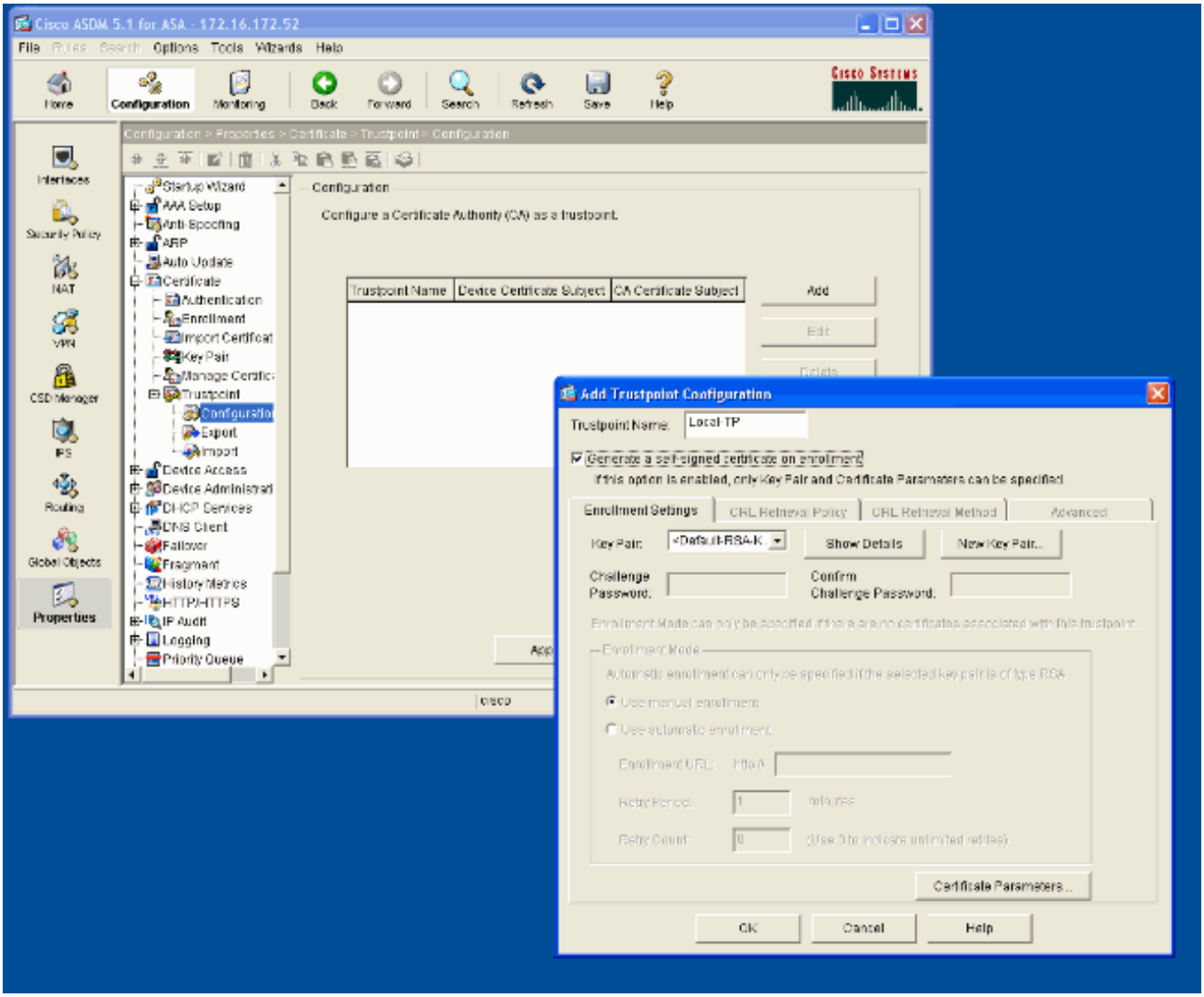


إنشاء شهادة موقعة ذاتيا

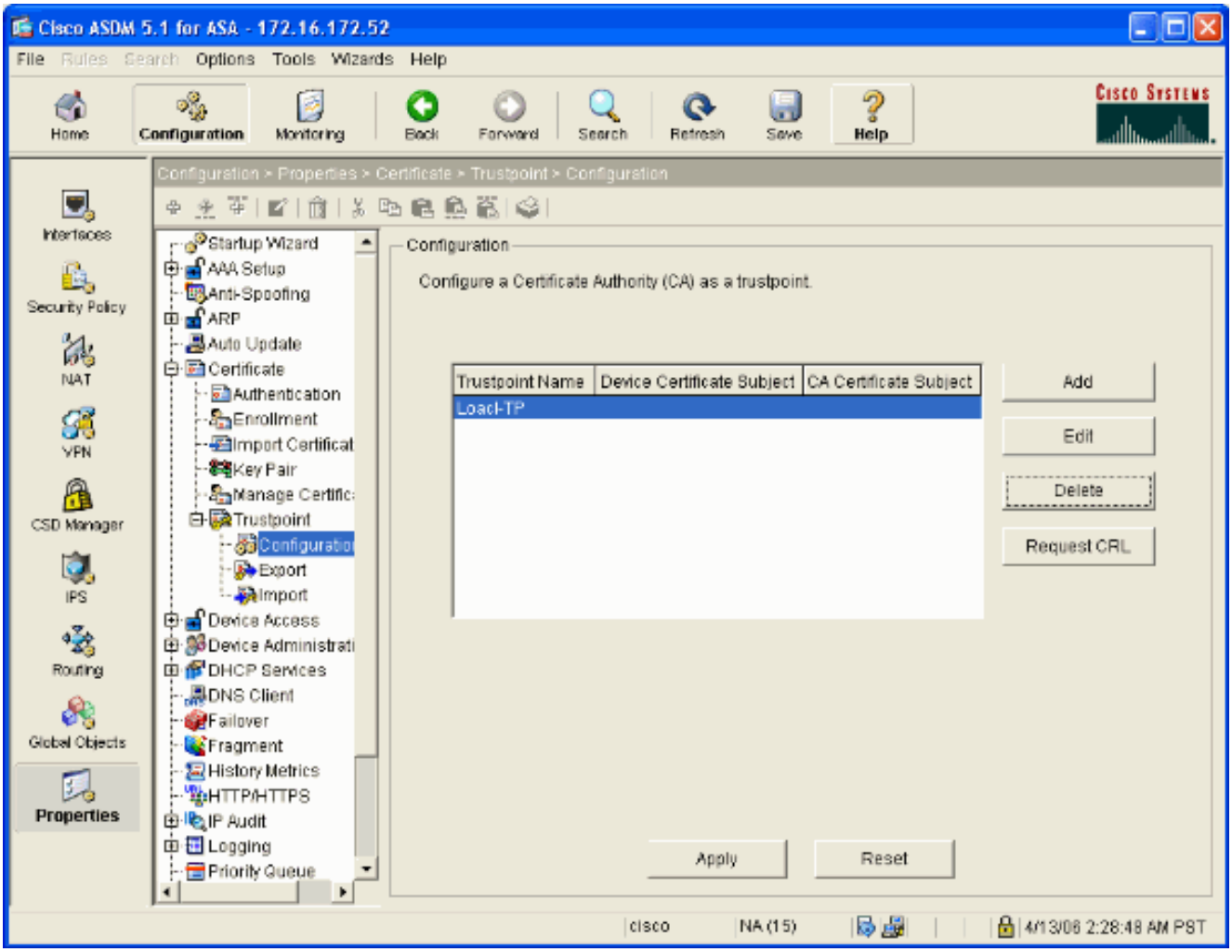
أكمل هذه الخطوات لتكوين ASA لاستخدام شهادة موقعة ذاتيا.

ملاحظة: في هذا المثال، يتم إستخدام شهادة موقعة ذاتيا لتحقيق البساطة. لخيارات تسجيل الشهادة الأخرى، مثل التسجيل مع مرجع شهادة خارجي، راجع تكوين الشهادات.

1. حدد **تشكيل > خصائص > ترخيص > TrustPoint > تشكيل** وانقر **إضافة**.
2. في النافذة التي تظهر أدخل اسم TrustPoint مثل Local-TP وحدد **إنشاء شهادة موقعة ذاتيا على التسجيل**. يمكن ترك الخيارات الأخرى مع إعداداتها الافتراضية. انقر فوق موافق عند الانتهاء.



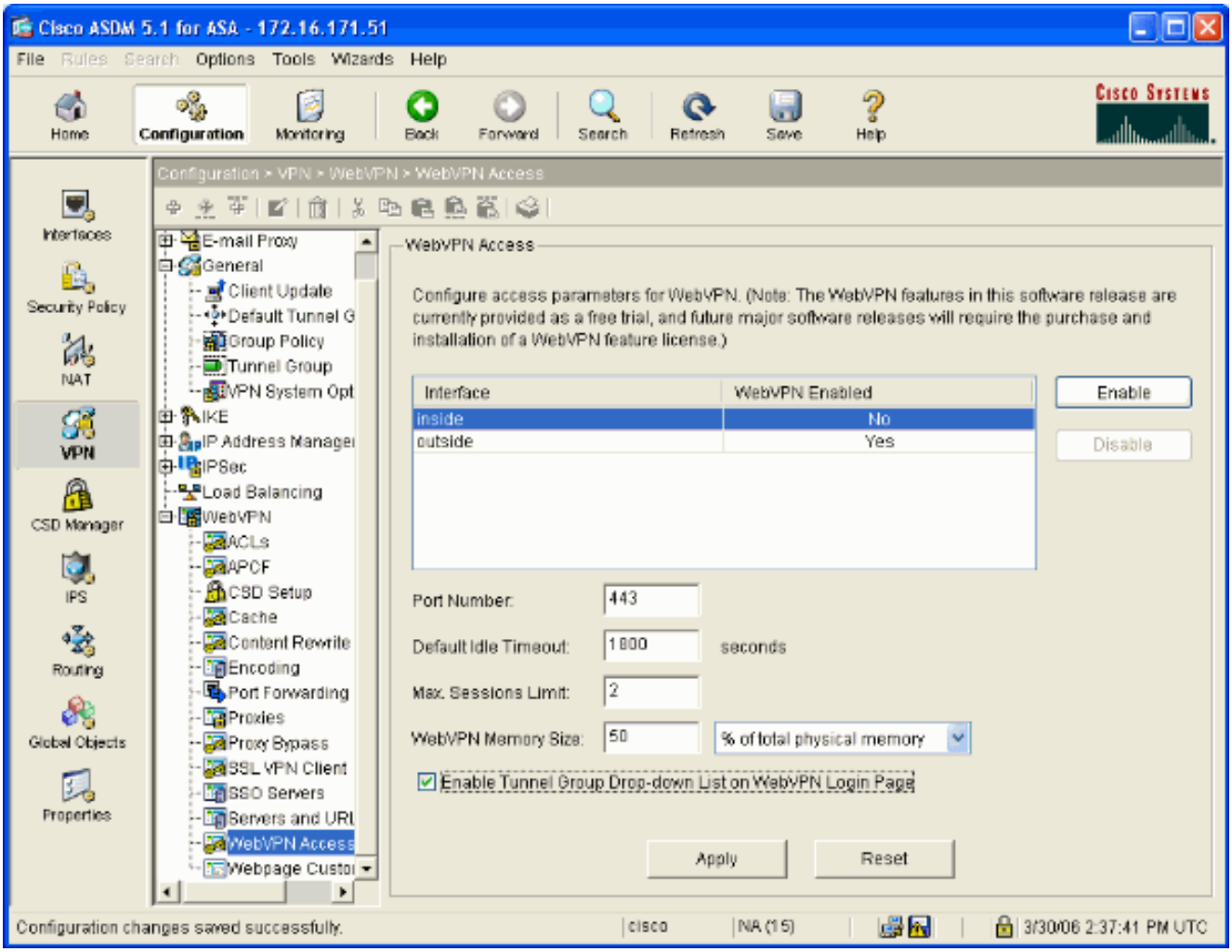
تعرض هذه النافذة تكوين TrustPoint المكتمل:



تمكين WebVPN على الواجهة الخارجية

أكمل هذه الخطوات للسماح للمستخدمين خارج الشبكة بالاتصال باستخدام WebVPN.

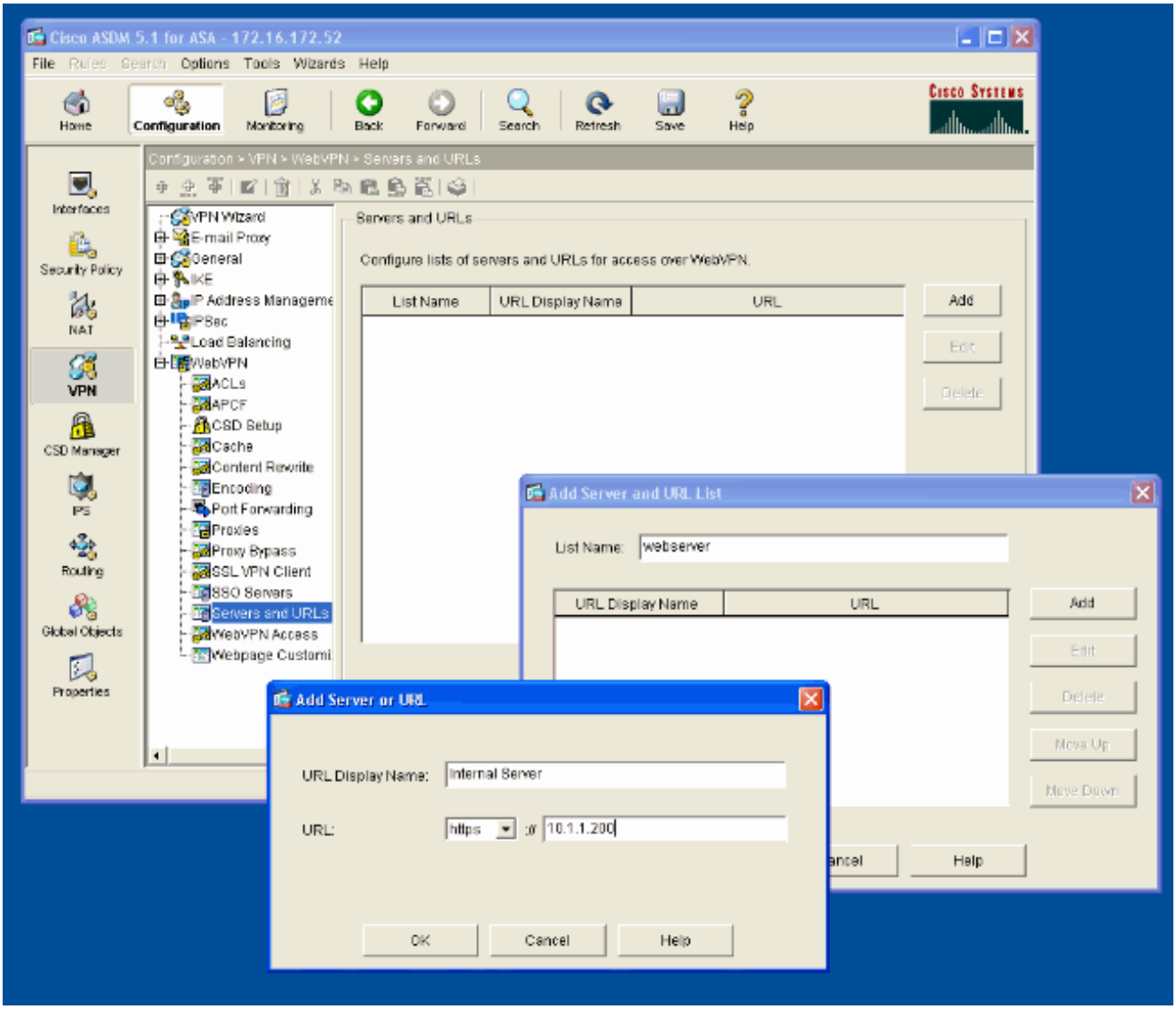
1. حدد **تكوين > WebVPN > VPN > وصول WebVPN**.
2. حدد الواجهة المطلوبة، وانقر فوق **تمكين**، ثم حدد **تمكين القائمة المنسدلة لمجموعة النفق في صفحة تسجيل الدخول إلى WebVPN.ملاحظة:** إذا تم إستخدام نفس الواجهة للوصول إلى WebVPN و ASDM، فيجب عليك تغيير المنفذ الافتراضي للوصول إلى ASDM من المنفذ 80 إلى منفذ جديد مثل 8080. ويتم القيام بذلك ضمن **التكوين > الخصائص > الوصول إلى الجهاز > HTTPS/ASDM.ملاحظة:** يمكنك إعادة توجيه مستخدم إلى المنفذ 443 تلقائيا في حالة تنقل مستخدم إلى **http://<ip_address>** بدلا من **https://<ip_address>**. حدد **تكوين > خصائص > HTTP/HTTPS**، واختر الواجهة المطلوبة، وانقر **تحرير** وحدد **إعادة توجيه HTTP إلى HTTPS**.



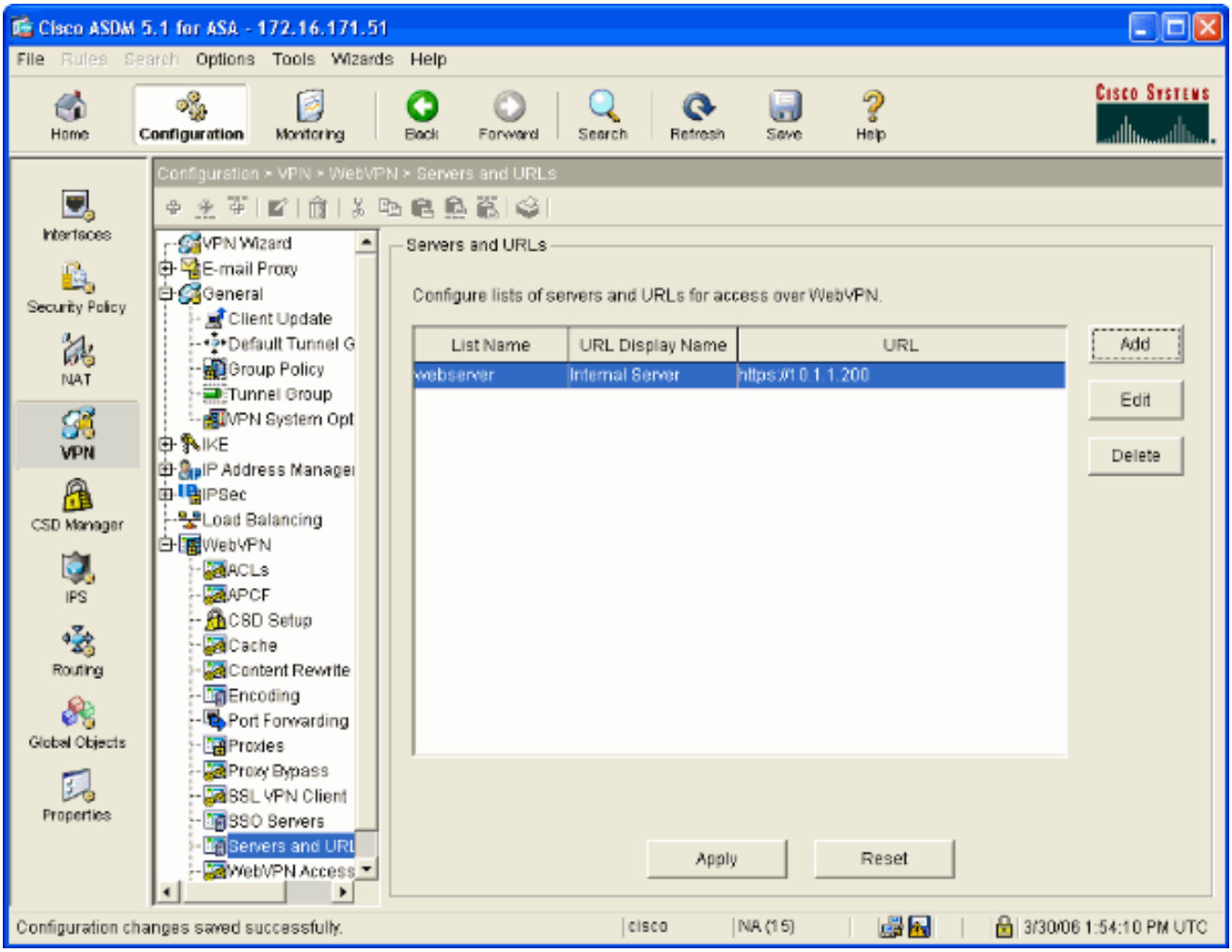
تكوين قائمة عناوين URL للخادم (الخوادم) الداخلي

أكمل الخطوات التالية لإنشاء قائمة تحتوي على الخوادم التي تريد منح مستخدمي WebVPN الوصول إليها.

1. حدد **تشكيل > WebVPN > VPN > خوادم و URLs** وانقر **إضافة**.
2. أدخل اسما لقائمة URL. هذا الاسم غير مرئي للمستخدمين النهائيين. انقر فوق **إضافة (Add)**.
3. أدخل اسم عرض عنوان URL كما سيتم عرضه للمستخدمين. أدخل معلومات عنوان URL الخاص بالخادم. يجب أن تكون هذه هي الطريقة التي تصل بها عادة إلى الخادم.



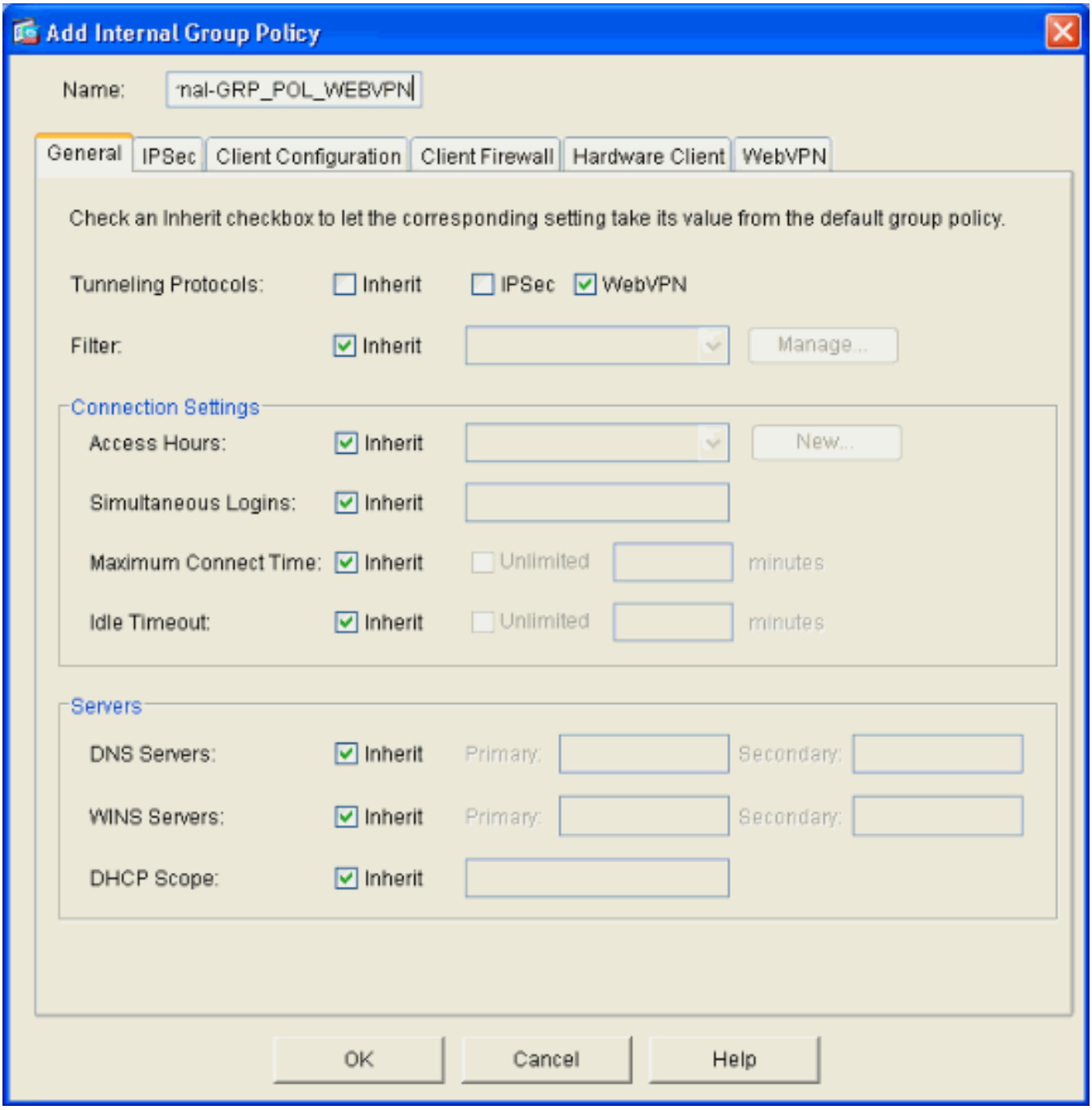
4. طقطقت **ok**، **ok**، وبعد ذلك **طبقت**.



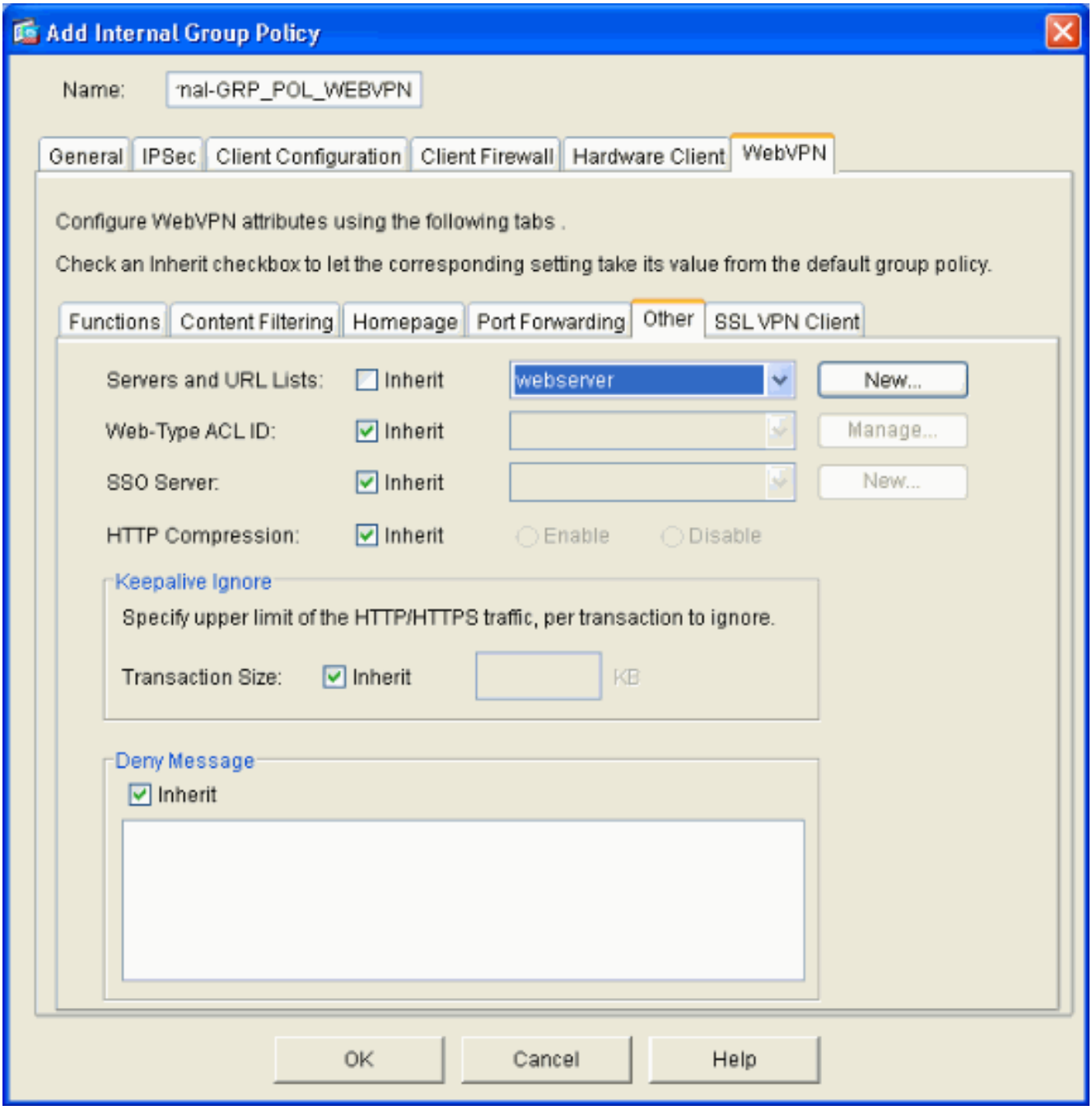
تكوين نهج مجموعة داخلي

أكمل هذه الخطوات لتكوين نهج مجموعة لمستخدمي WebVPN.

1. حدد **تشكيل > VPN > عام > نهج المجموعة**، انقر **إضافة**، وحدد **نهج المجموعة الداخلي**.
2. في علامة التبويب "عام"، حدد اسم نهج، مثل Internal-Group_POL_WEBVPN. ثم قم بإلغاء تحديد **Inherit** بجوار بروتوكولات الاتصال النفقي وفحص **WebVPN**.



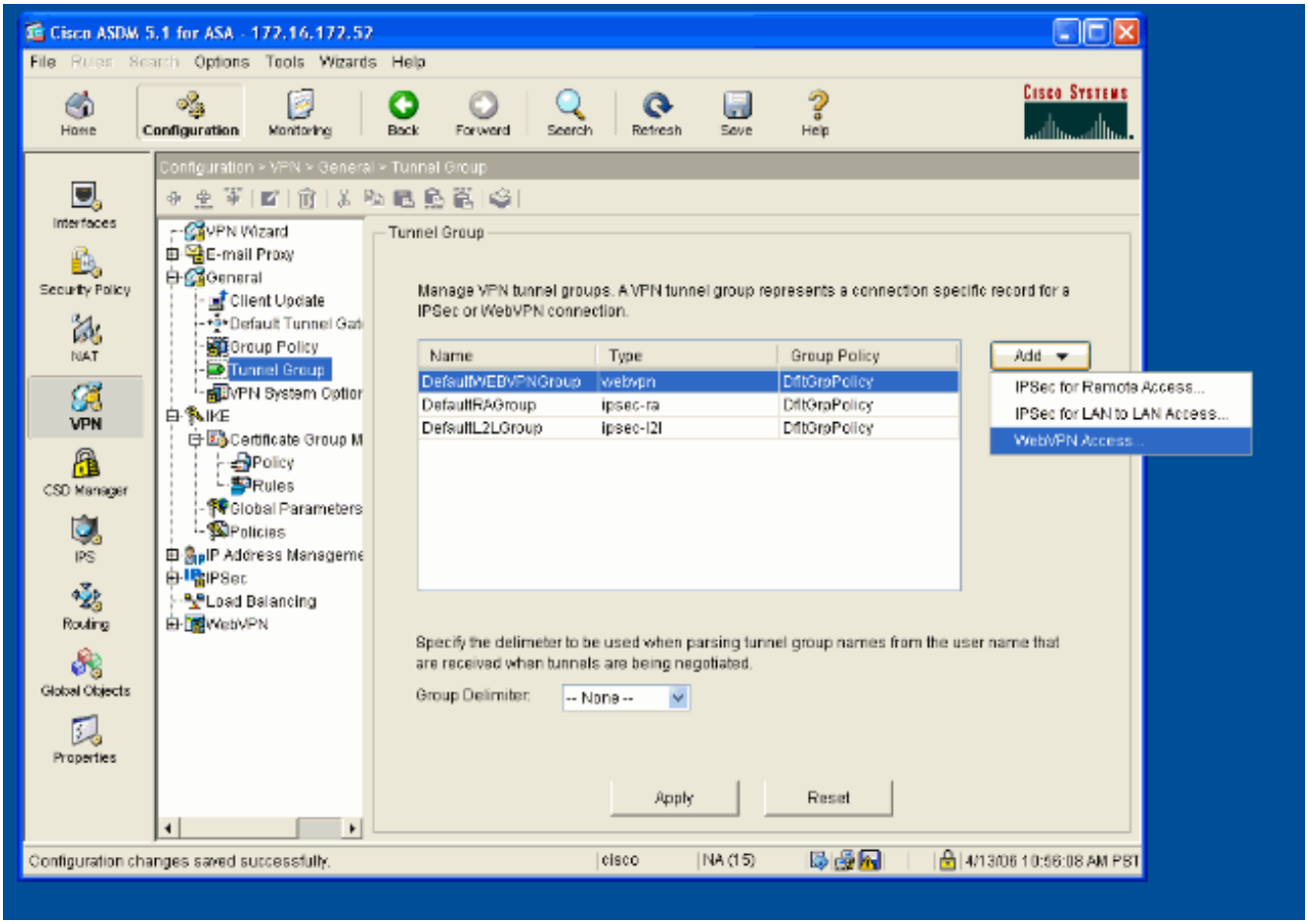
3. في علامة التبويب WebVPN حدد علامة التبويب الفرعية **أخرى**. قم بإلغاء تحديد **توريث** بجوار الخوادم وقوائم عناوين URL وحدد قائمة عناوين URL التي قمت بتكوينها من القائمة المنسدلة. انقر فوق موافق عند الانتهاء.



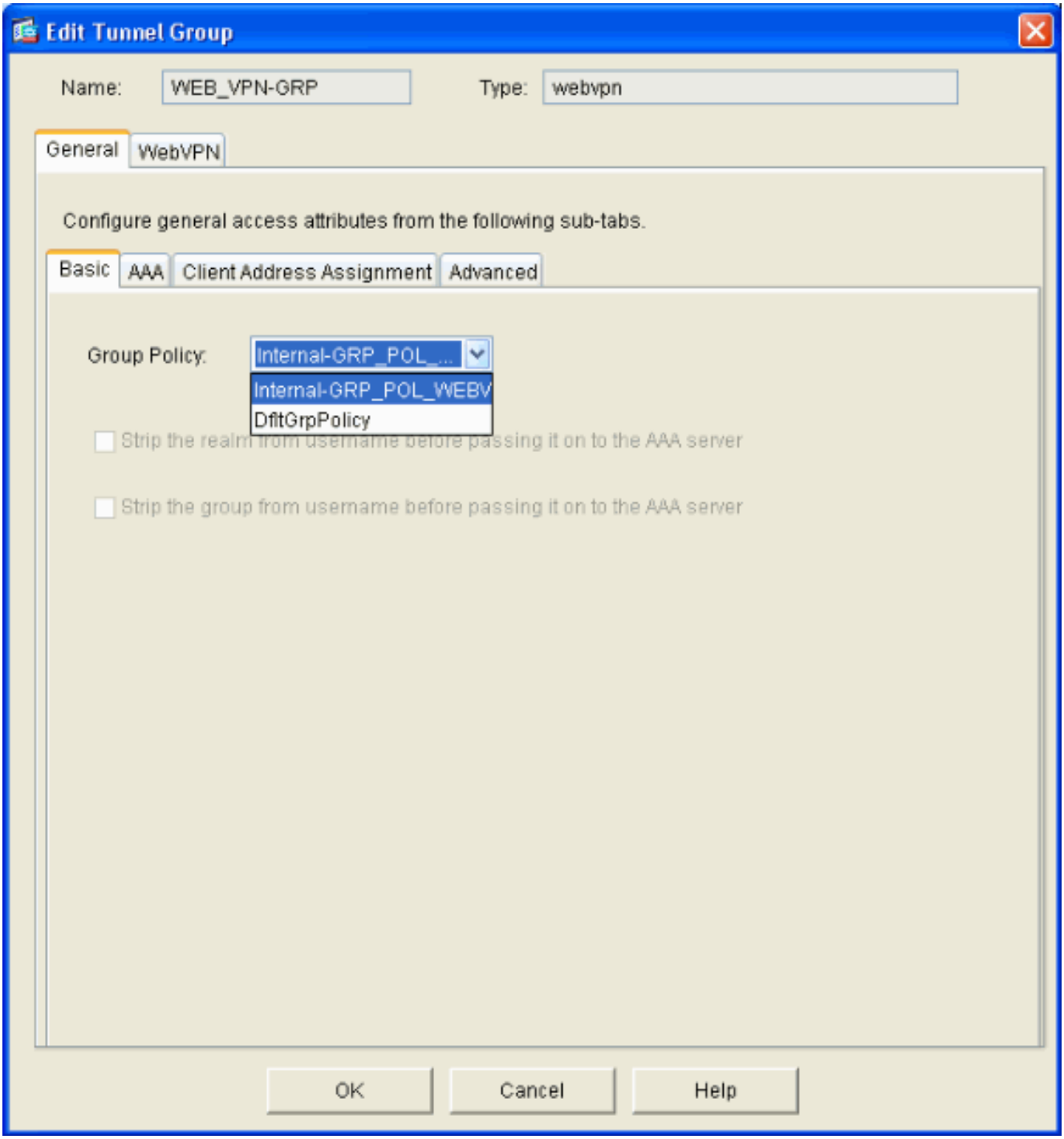
تكوين مجموعة نفق

أكمل هذه الخطوات لتكوين مجموعة نفق لمستخدمي WebVPN لديك.

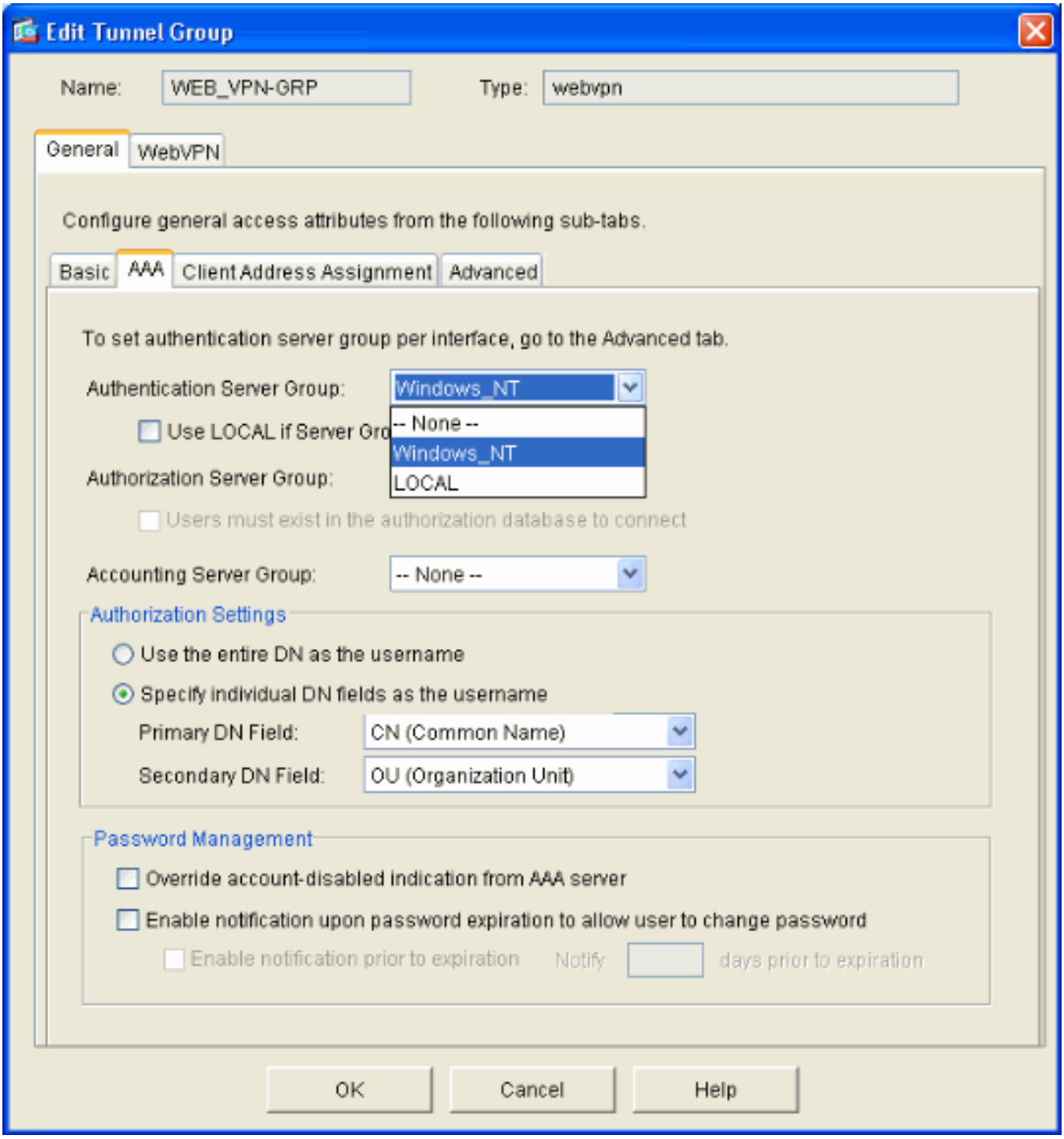
1. حدد **تكوين** > **VPN** > **عام** > **مجموعة أنفاق**، انقر فوق **إضافة** وحدد **وصول WebVPN**...



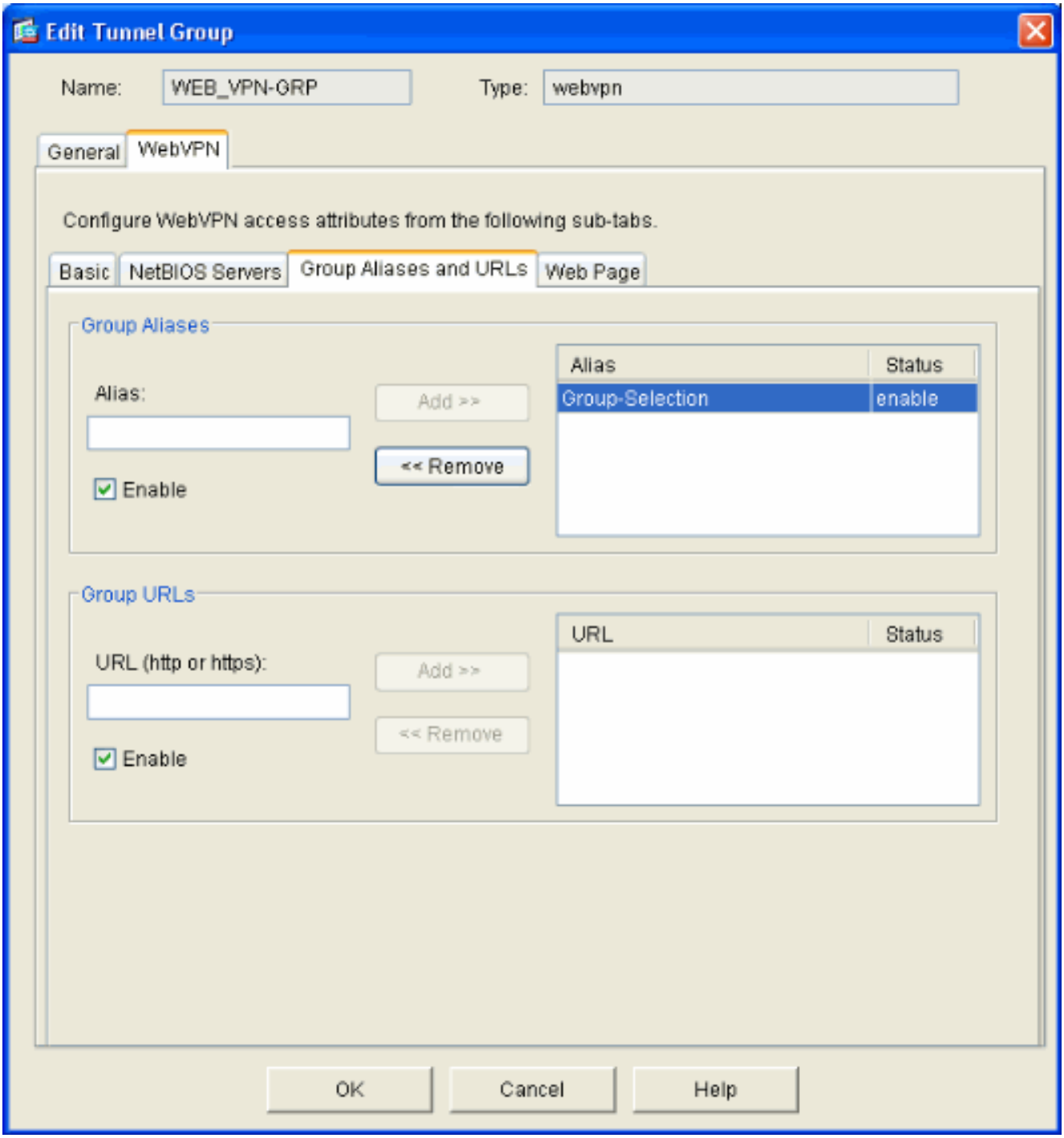
2. أدخل اسم لمجموعة النفق، مثل WEB_VPN-GRP. في علامة التبويب "أساسي" حدد "نهج المجموعة" الذي أنشأته وتحقق من أن "نوع المجموعة" هو **WebVPN**.



3. انتقل إلى علامة التبويب AAA.بالنسبة لمجموعة خوادم المصادقة، أختر المجموعة التي قمت بتكوينها لتمكين مصادقة NTLMv1 باستخدام وحدة التحكم في المجال الخاصة بك.**إختياري:** حدد **إستخدام محلي إذا فشلت مجموعة الخوادم** في تمكين إستخدام قاعدة بيانات المستخدم المحلية في حالة فشل مجموعة AAA التي تم تكوينها. يمكن أن يساعدك ذلك على أستكشاف الأخطاء وإصلاحها في وقت لاحق.



4. انتقل إلى علامة التبويب WebVPN ثم انتقل إلى علامة التبويب الفرعية **أسماء المجموعات المستعارة وعناوين URL**.
5. أدخل اسما مستعارا ضمن الأسماء المستعارة للمجموعة وانقر فوق **إضافة**. يظهر هذا الاسم المستعار في القائمة المنسدلة المقدمة إلى مستخدمي WebVPN عند تسجيل الدخول.



6. طقطقت **ok** وبعد ذلك **يطبق**.

تكوين الموقع التلقائي للخادم

قم بالتبديل إلى سطر الأوامر لتمكين SSO للخادم (الخوادم) الداخلية لديك.

ملاحظة: لا يمكن إكمال هذه الخطوة في ASDM ويجب إنجازها باستخدام سطر الأوامر. راجع الوصول إلى واجهة سطر الأوامر للحصول على مزيد من المعلومات.

أستخدم الأمر **auto-signon** لتحديد مورد الشبكة، مثل الخادم، الذي تريد منح المستخدمين إمكانية الوصول إليه. يتم تكوين عنوان IP لخادم واحد هنا، ولكن يمكن أيضا تحديد نطاق شبكة مثل **10.1.1.0 /24**. راجع أمر **الموقع التلقائي** للحصول على مزيد من المعلومات.

```
ASA>enable
ASA#configure terminal
```

```
ASA(config)#webvpn
ASA(config-webpvn)#auto-signon allow ip 10.1.1.200 255.255.255.255 auth-type ntlm
ASA(config-webvpn)#quit
ASA(config)#exit
ASA#write memory
```

في إخراج هذا المثال، يتم تكوين الأمر **auto-signon** ل WebVPN بشكل عام. كما يمكن إستخدام هذا الأمر في وضع تكوين مجموعة WebVPN أو وضع تكوين اسم مستخدم WebVPN. يحد إستخدام هذا الأمر في وضع تكوين مجموعة WebVPN هذا الأمر على مجموعة معينة. وعلى نحو مماثل، يحد إستخدام هذا الأمر في وضع تكوين اسم مستخدم WebVPN هذا الأمر على مستخدم واحد. راجع أمر **الموقع التلقائي** للحصول على مزيد من المعلومات.

تكوين ASA النهائي

يستعمل هذا وثيقة هذا تشكيل:

ASA الإصدار 7.1(1)

```
ASA# show running-config
Saved :
:
(ASA Version 7.1(1
!
terminal width 200
hostname ASA
domain-name cisco.com
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 172.16.171.51 255.255.255.0
!
interface GigabitEthernet0/1
nameif inside
security-level 100
ip address 10.1.1.1 255.255.255.0
!
interface GigabitEthernet0/2
shutdown
no nameif
no security-level
no ip address
!
interface GigabitEthernet0/3
shutdown
no nameif
no security-level
no ip address
!
interface Management0/0
shutdown
no nameif
no security-level
no ip address
!
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
dns server-group DefaultDNS
domain-name cisco.com
```

```
                                                pager lines 24
                                              mtu inside 1500
                                             mtu outside 1500
                                                  no failover
                                  asdm image disk0:/asdm512.bin
                                         no asdm history enable
                                              arp timeout 14400
                 route outside 0.0.0.0 0.0.0.0 172.16.171.1 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

     AAA server configuration aaa-server Windows_NT ---!
    protocol nt aaa-server Windows_NT host 10.1.1.200 nt-
  auth-domain-controller ESC-SJ-7800 !--- Internal group
              policy configuration group-policy Internal-
           GRP_POL_WEBVPN internal group-policy Internal-
    GRP_POL_WEBVPN attributes vpn-tunnel-protocol webvpn
 webvpn url-list value webserver username cisco password
              Q/odgwmtmVIw4Dcm encrypted privilege 15 aaa
authentication http console LOCAL aaa authentication ssh
   console LOCAL aaa authentication enable console LOCAL
 http server enable 8181 http 0.0.0.0 0.0.0.0 outside no
 snmp-server location no snmp-server contact snmp-server
         enable traps snmp authentication linkup linkdown
      coldstart !--- Trustpoint/certificate configuration
        crypto ca trustpoint Local-TP enrollment self crl
           configure crypto ca certificate chain Local-TP
      certificate 31 308201b0 30820119 a0030201 02020131
   300d0609 2a864886 f70d0101 04050030 1e311c30 1a06092a
   864886f7 0d010902 160d4153 412e6369 73636f2e 636f6d30
   1e170d30 36303333 30313334 3930345a 170d3136 30333237
   31333439 30345a30 1e311c30 1a06092a 864886f7 0d010902
   160d4153 412e6369 73636f2e 636f6d30 819f300d 06092a86
   4886f70d 01010105 0003818d 00308189 02818100 e47a29cd
   56becf8d 99d6d919 47892f5a 1b8fc5c0 c7d01ea6 58f3bec4
   a60b2025 03748d5b 1226b434 561e5507 5b45f30e 9d65a03f
   30add0b5 81f6801a 766c9404 9cabcbde 44b221f9 b6d6dc18
   496fe5bb 4983927f adabfb17 68b4d22c cddfa6c3 d8802efc
   ec3af7c7 749f0aa2 3ea2c7e3 776d6d1d 6ce5f748 e4cda3b7
   4f007d4f 02030100 01300d06 092a8648 86f70d01 01040500
   03818100 c6f87c61 534bb544 59746bdb 4e01680f 06a88a15
   e3ed8929 19c6c522 05ec273d 3e37f540 f433fb38 7f75928e
   1b1b6300 940b8dff 69eac16b af551d7f 286bc79c e6944e21
   49bf15f3 c4ec82d8 8811b6de 775b0c57 e60a2700 fd6acc16
   a77abee6 34cb0cad 81dfaf5a f544258d cc74fe2d 4c298076
       294f843a edda3a0a 6e7f5b3c quit !--- Tunnel group
      configuration tunnel-group WEB_VPN-GRP type webvpn
             tunnel-group WEB_VPN-GRP general-attributes
   authentication-server-group Windows_NT default-group-
 policy Internal-GRP_POL_WEBVPN tunnel-group WEB_VPN-GRP
    webvpn-attributes group-alias Group-Selection enable
      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
```

```
!--- WebVPN Configuration webvpn enable outside url-list
webserver "Internal Server" https://10.1.1.200 1 tunnel-
      group-list enable auto-signon allow ip 10.1.1.200
                                  255.255.255.255 auth-type ntlm
        Cryptochecksum:c80ac5f6232df50fc1ecc915512c3cd6
                                                  end :
```

التحقق من الصحة

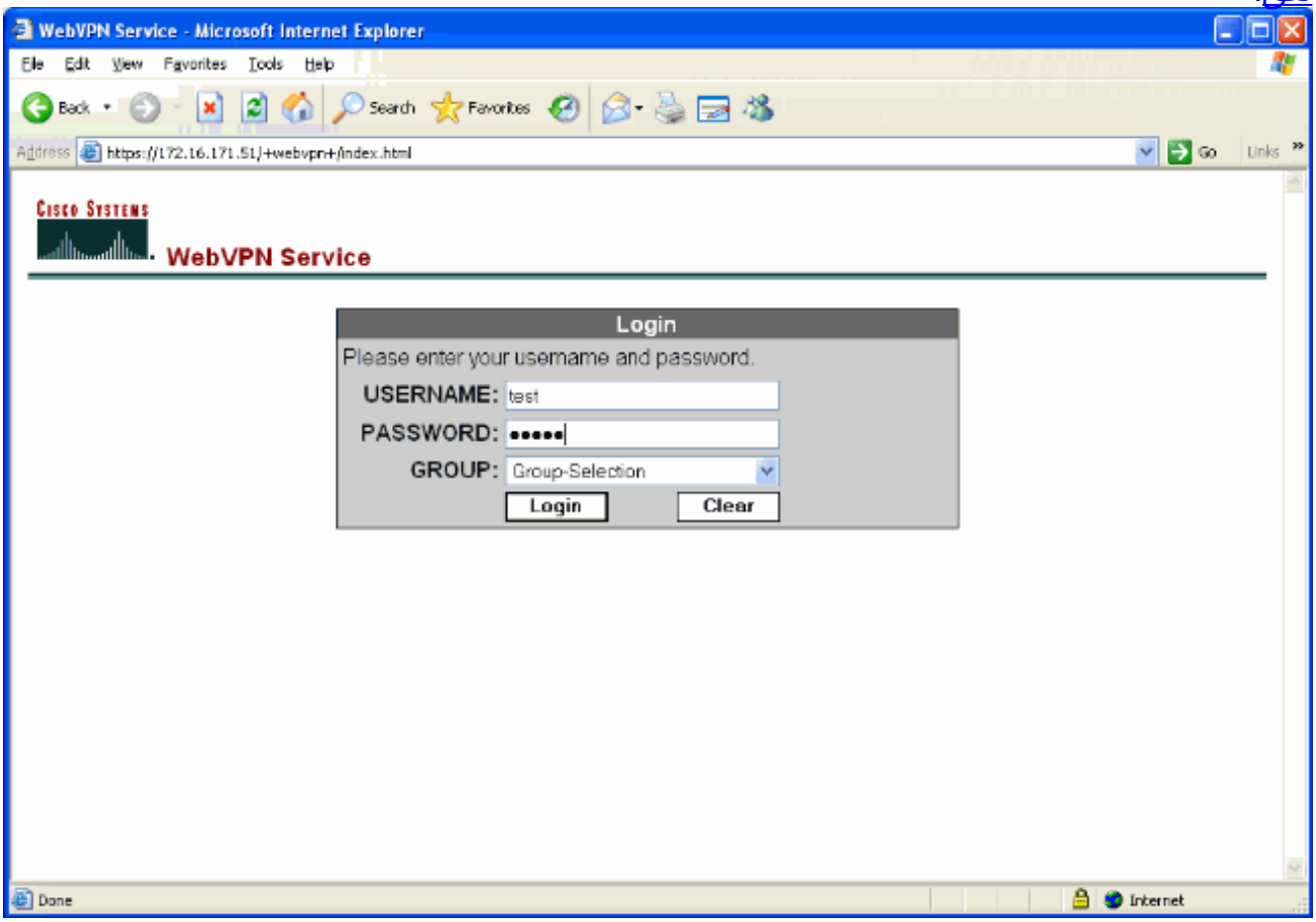
استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

تدعم أداة مترجم الإخراج (للعملاءالمسجلين فقط) بعض أوامر **show**. استخدم أداة مترجم الإخراج (OIT) لعرض تحليل مُخرَج الأمر **show** .

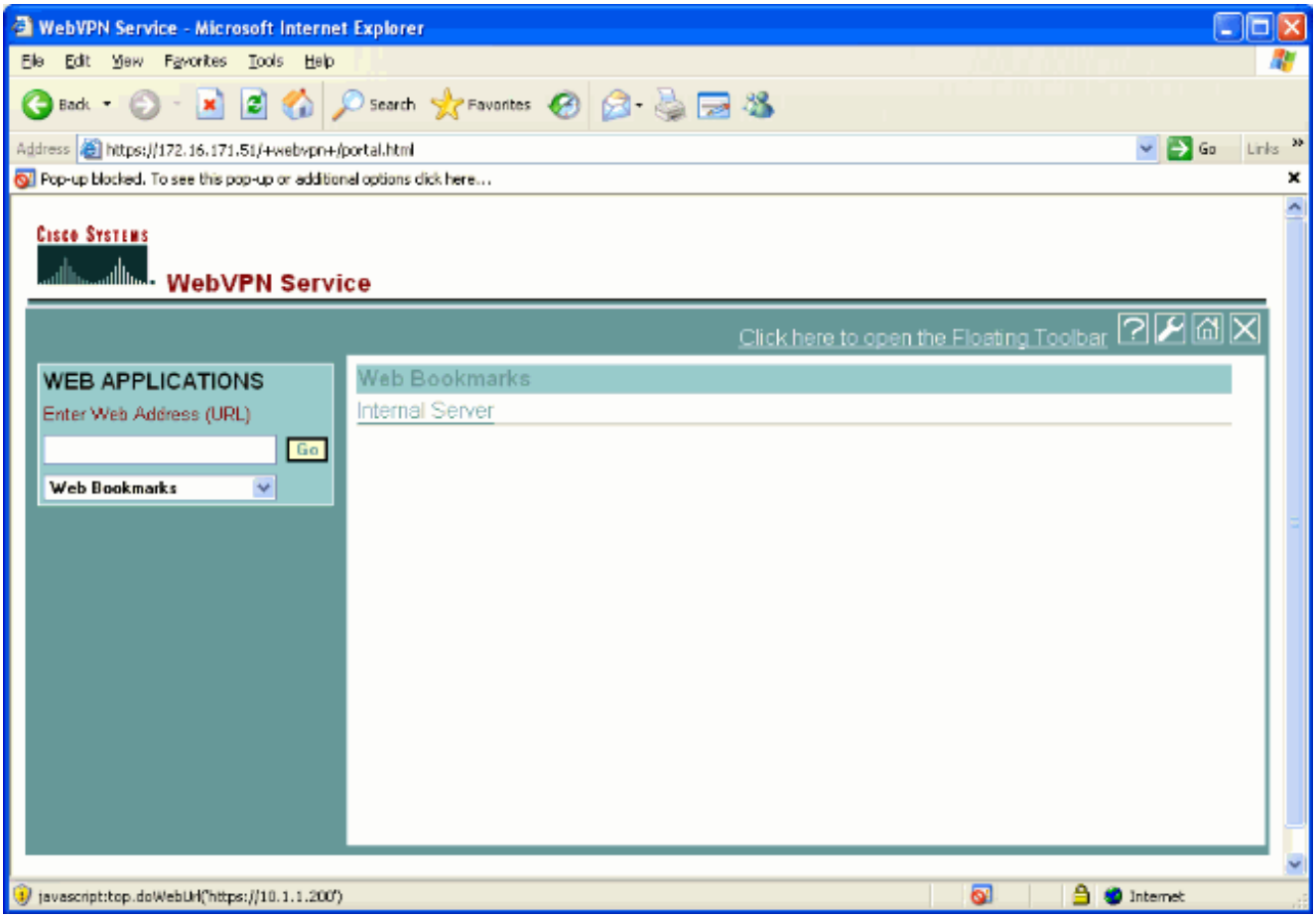
إختبار تسجيل دخول WebVPN

قم بتسجيل الدخول كمستخدم لاختبار التكوين الخاص بك.

1. حاول تسجيل الدخول إلى ASA مع معلومات المستخدم من مجال NT الخاص بك. حدد الاسم المستعار للمجموعة الذي تم تكوينه في الخطوة 5 ضمن تكوين مجموعة نفق.

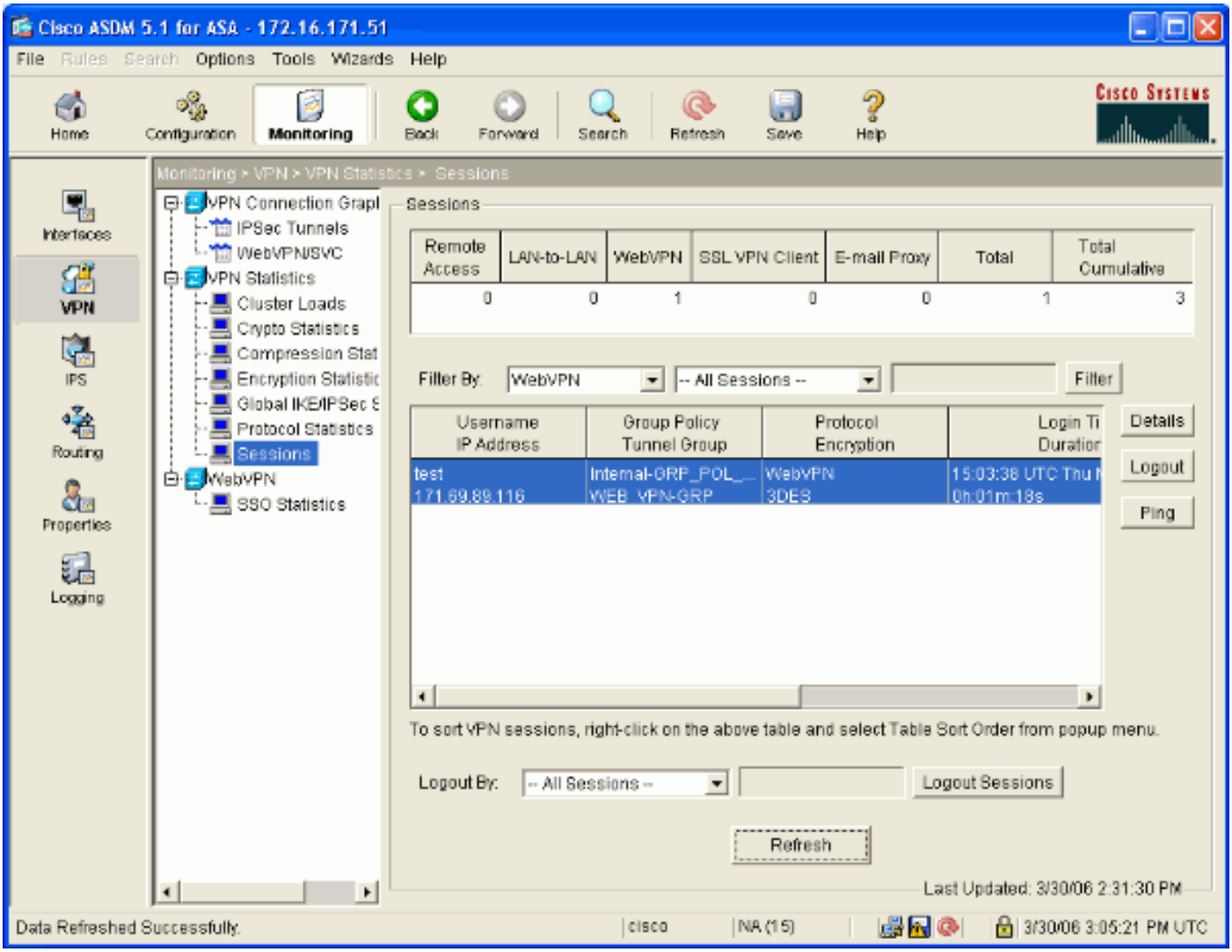


2. ابحث عن الارتباط (الارتباطات) الذي تم تكوينه للخادم (الخوادم) الداخلي. انقر فوق الارتباط للتحقق.



جلسات المراقبة

حدد **مراقبة > VPN > إحصائيات VPN > جلسات العمل** وابحث عن جلسة عمل WebVPN التي تنتمي إلى المجموعة التي تم تكوينها في هذا المستند.



تصحيح أخطاء جلسة WebVPN

هذا الإخراج هو نموذج تصحيح أخطاء لجلسة عمل WebVPN ناجحة.

ملاحظة: ارجع إلى معلومات مهمة حول أوامر التصحيح قبل إستخدام أوامر **debug**.

```
ASA#debug webvpn 255
INFO: debug webvpn enabled at level 255
#ASA
[ASA# webvpn_portal.c:ewaFormServe_webvpn_login[1570
[webvpn_portal.c:http_webvpn_kill_cookie[385
[webvpn_auth.c:webvpn_auth[286
!!WebVPN: no cookie present
[webvpn_portal.c:ewaFormSubmit_webvpn_login[1640
[webvpn_portal.c:http_webvpn_kill_cookie[385
[webvpn_auth.c:http_webvpn_pre_authentication[1782
Begin AAA WebVPN: calling AAA with ewsContext (78986968) and nh (78960800)! WebVPN: started ---!
...user authentication
[webvpn_auth.c:webvpn_aaa_callback[3422
(WebVPN: AAA status = (ACCEPT
[webvpn_portal.c:ewaFormSubmit_webvpn_login[1640
[webvpn_auth.c:http_webvpn_post_authentication[1095
.WebVPN: user: (test) authenticated
End AAA webvpn_auth.c:http_webvpn_auth_accept[2093] ---!
webvpn_session.c:http_webvpn_create_session[159] webvpn_session.c:http_webvpn_find_session[136]
!WebVPN session created
```

```
[webvpn_session.c:http_webvpn_find_session[136
[webvpn_db.c:webvpn_get_server_db_first[161
[webvpn_db.c:webvpn_get_server_db_next[202
(traversing list: (webserver
[webvpn_portal.c:ewaFormServe_webvpn_cookie[1421
[webvpn_auth.c:webvpn_auth[286
[webvpn_session.c:http_webvpn_find_session[136
[webvpn_session.c:webvpn_update_idle_time[924
.WebVPN: session has been authenticated
[webvpn_auth.c:webvpn_auth[286
[webvpn_session.c:http_webvpn_find_session[136
[webvpn_session.c:webvpn_update_idle_time[924
.WebVPN: session has been authenticated
Output supressed webvpn_auth.c:webvpn_auth[286] ---!
webvpn_session.c:http_webvpn_find_session[136] webvpn_session.c:webvpn_update_idle_time[924]
WebVPN: session has been authenticated. webvpn_auth.c:webvpn_auth[286]
webvpn_session.c:http_webvpn_find_session[136] webvpn_session.c:webvpn_update_idle_time[924]
WebVPN: session has been authenticated. webvpn_auth.c:webvpn_auth[286]
webvpn_session.c:http_webvpn_find_session[136] webvpn_session.c:webvpn_update_idle_time[924]
WebVPN: session has been authenticated. webvpn_auth.c:webvpn_auth[286]
webvpn_session.c:http_webvpn_find_session[136] webvpn_session.c:webvpn_update_idle_time[924]
WebVPN: session has been authenticated. webvpn_auth.c:webvpn_auth[286]
webvpn_session.c:http_webvpn_find_session[136] webvpn_session.c:webvpn_update_idle_time[924]
WebVPN: session has been authenticated. webvpn_session.c:http_webvpn_find_session[136]
[webvpn_session.c:webvpn_update_idle_time[924
```

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

- إذا لم يكن المربع المنسدل الخاص بالمجموعة موجودا في صفحة تسجيل الدخول إلى WebVPN، فتأكد من إكمال الخطوة 2 ضمن تمكين WebVPN على الواجهة الخارجية والخطوة 5 ضمن تكوين مجموعة نفق. إذا لم يتم إكمال هذه الخطوات وكانت القائمة المنسدلة مفقودة، تقع المصادقة ضمن المجموعة الافتراضية ومن المحتمل أن تفشل.
- على الرغم من أنه لا يمكنك تعيين حقوق الوصول للمستخدم في ASDM أو في ASA، إلا أنه يمكنك تقييد المستخدمين بحقوق الوصول إلى Microsoft Windows على وحدة التحكم بالمجال الخاصة بك. قم بإضافة أذونات مجموعة NT الضرورية لصفحة الويب التي يصادق المستخدم عليها. بمجرد أن يقوم المستخدم بتسجيل الدخول إلى WebVPN باستخدام أذونات المجموعة، يتم منح حق الوصول إلى الصفحات المحددة أو رفضه وفقا لذلك. يعمل ASA فقط كمضيف مصادقة وكيل نيابة عن وحدة التحكم في المجال وجميع الاتصالات هنا NTLMv1.
- لا يمكنك تكوين SSO ل SharePoint عبر WebVPN لأن خادم SharePoint لا يدعم المصادقة المستندة إلى النماذج. ونتيجة لذلك، فإن الإشارات المرجعية التي لها عملية مادة النشر أو إجراء إضافة مادة النشر غير قابلة للتطبيق هنا.

معلومات ذات صلة

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