تكوين SSL VPN دون عميل (WebVPN) على Cisco IOS باستخدام SDM

المحتويات

المقدمة

يسمح WebVPN (Client SSL VPN) للمستخدم بالوصول بأمان إلى الموارد على شبكة LAN الخاصة بالشركة من أي مكان باستخدام مستعرض ويب يدعم SSL. يقوم المستخدم أولا بالمصادقة باستخدام بوابة WebVPN التي تسمح بعد ذلك للمستخدم بالوصول إلى موارد الشبكة التي تم تكوينها مسبقا. يمكن تكوين بوابات WebVPN على موجهات Cisco IOS®، وأجهزة الأمان المعدلة (ASA) من Cisco، ومركزات Cisco VPN 3000، والوحدة النمطية لخدمات Cisco WebVPN لموجهات Catalyst 6500 و 7600.

يمكن تكوين تقنية طبقة مأخذ التوصيل الآمنة (SSL) الشبكة الخاصة الظاهرية (VPN) على أجهزة Cisco في ثلاثة أوضاع رئيسية: Thin-Client SSL VPN (WebVPN)، ClientLess SSL VPN (إعادة توجيه المنفذ)، ووضع SSL VPN Client (SVC). يوضح هذا المستند تكوين WebVPN على موجهات Cisco IOS.

ملاحظة: لا تقم بتغيير اسم مجال IP أو اسم المضيف للموجه لأن ذلك سيؤدي إلى تشغيل إعادة إنشاء الشهادة الموقعة ذاتيا وسيتجاوز TrustPoint التي تم تكوينها. يتسبب إعادة إنشاء الشهادة الموقعة ذاتيا في حدوث مشاكل في الاتصال إذا تم تكوين الموجه ل WebVPN. يربط WebVPN اسم SSL TrustPoint بتكوين عبارة WebVPN.

لذلك، في حالة إصدار شهادة موقعة ذاتيا جديدة، لا يتطابق اسم TrustPoint الجديد مع تكوين WebVPN ولا يمكن للمستخدمين الاتصال.

ملاحظة: إذا قمت بتشغيل الأمر **ip https-secure server** على موجه WebVPN الذي يستخدم شهادة دائمة موقعة ذاتيا، يتم إنشاء مفتاح RSA جديد وتصبح الشهادة غير صالحة. يتم إنشاء TrustPoint جديد، مما يكسر SSL WebVPN. إذا قام الموجه الذي يستخدم عمليات إعادة تمهيد الشهادة الموقعة ذاتيا الدائمة بعد تشغيل الأمر **ip https-secure server**، تحدث نفس المشكلة.

ارجع إلى مثال تكوين IOS الخاص بـ SSL VPN (WebVPN) Thin-Client مع SDM لمعرفة المزيد حول Thin-Client SSL VPN.

ارجع إلى مثال تكوين SDM مع IOS على SSL VPN Client (SVC) لمعرفة المزيد حول عميل SSL VPN.

يتم تشغيل SSL VPN على الأنظمة الأساسية التالية من Cisco Router:

- الموجهات من السلسلة 870 و 1811 و 1841 و 2801 و 2811 و 2821 و 2851 من Cisco
- الموجهات من السلسلة 3725 و 3745 و 3825 و 3845 و 7200 و 7301 من Cisco

المتطلبات الأساسية

المتطلبات

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

- صورة متقدمة لبرنامج Cisco IOS الإصدار T(6)12.4 أو إصدار أحدث
- أحد الأنظمة الأساسية لموجهات Cisco المدرجة في المقدمة

المكونات المستخدمة

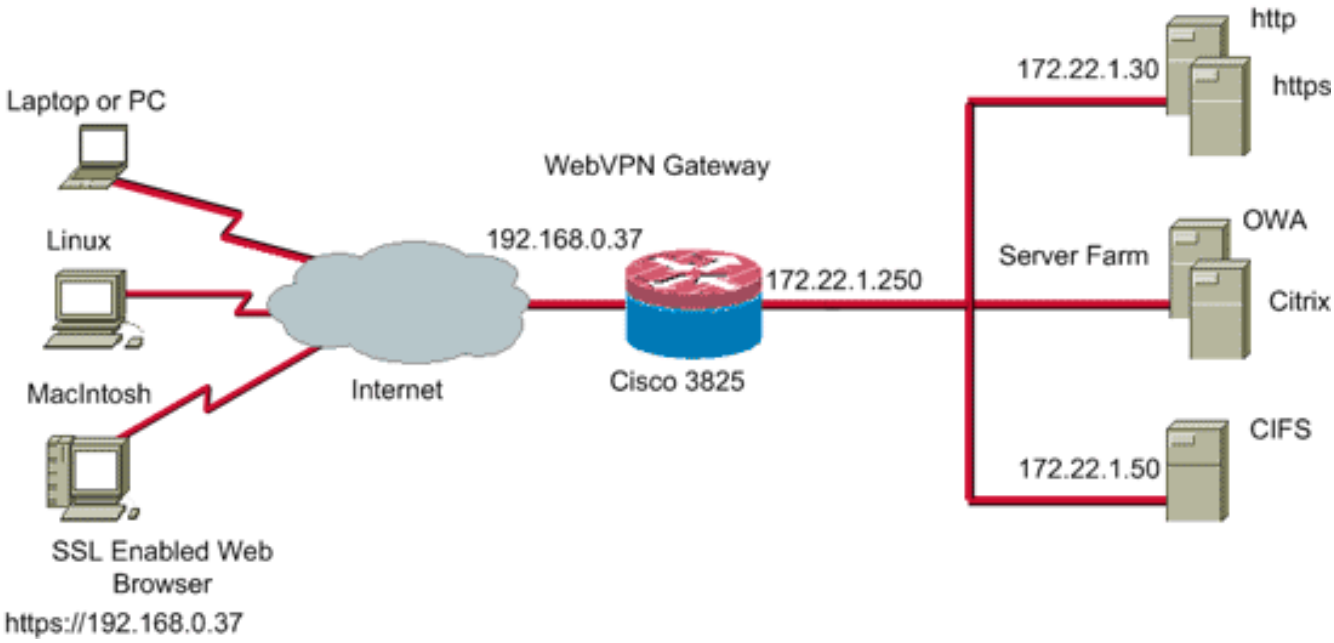
تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- موجّه Cisco 3825
- صورة برنامج Advanced Enterprise - برنامج Cisco IOS الإصدار T(9)12.4
- مدير أجهزة الأمان والموجه من Cisco (SDM) - الإصدار 2.3.1

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. يتم أخذ عناوين IP المستخدمة في هذا المثال من عناوين RFC 1918 الخاصة وغير القانونية للاستخدام على الإنترنت.

الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة التالي:



الاصطلاحات

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

مهام ما قبل التكوين

قبل البدء، أكمل المهام التالية:

1. قم بتكوين اسم مضيف واسم مجال.
2. قم بتكوين الموجه ل SDM. تقوم Cisco بشحن بعض الموجهات باستخدام نسخة مثبتة مسبقا من إدارة قاعدة بيانات المحول (SDM).إذا لم يتم تحميل إدارة قاعدة بيانات المحول (SDM) من Cisco بالفعل على الموجه الخاص بك، فيمكنك الحصول على نسخة مجانية من البرنامج من تنزيل البرامج (للعملاء المسجلين فقط). أنت ينبغي يتلقى حساب CCO مع عقد خدمة. لمزيد من المعلومات التفصيلية حول تثبيت إدارة قاعدة بيانات المحول (SDM) وتكوينها، ارجع إلى مدير أجهزة الأمان والموجه من Cisco.
3. قم بتكوين التاريخ والوقت والمنطقة الزمنية الصحيحة للموجه الخاص بك.

تكوين Weben على Cisco IOS

يمكن أن يكون لديك أكثر من عبارة WebVPN واحدة مقترنة بجهاز ما. يتم ربط كل بوابة WebVPN بعنوان IP واحد فقط على الموجه. يمكنك إنشاء أكثر من سياق WebVPN لبوابة WebVPN معينة. لتحديد السياقات الفردية، قم بتزويد كل سياق باسم فريد. يمكن إقران مجموعة نهج واحدة بسياق WebVPN واحد فقط. تصف مجموعة السياسات الموارد المتوفرة في سياق WebVPN معين.

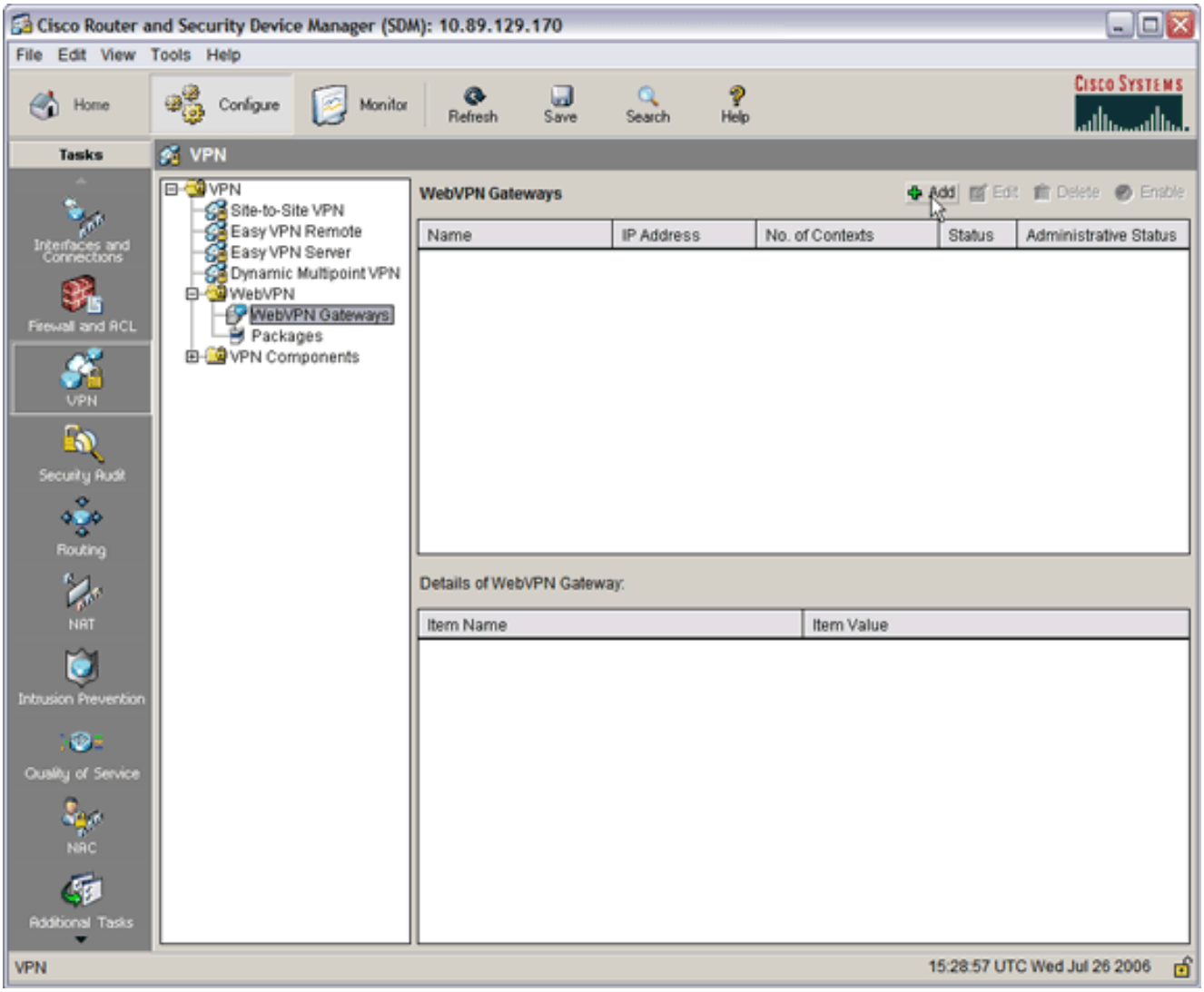
أتمت هذا steps in order to شكلت WebVPN على cisco ios:

1. تكوين بوابة WebVPN
2. تكوين الموارد المسموح بها لمجموعة النهج
3. تكوين مجموعة نهج WebVPN وتحديد الموارد
4. تكوين سياق WebVPN
5. تكوين قاعدة بيانات المستخدم وطريقة المصادقة

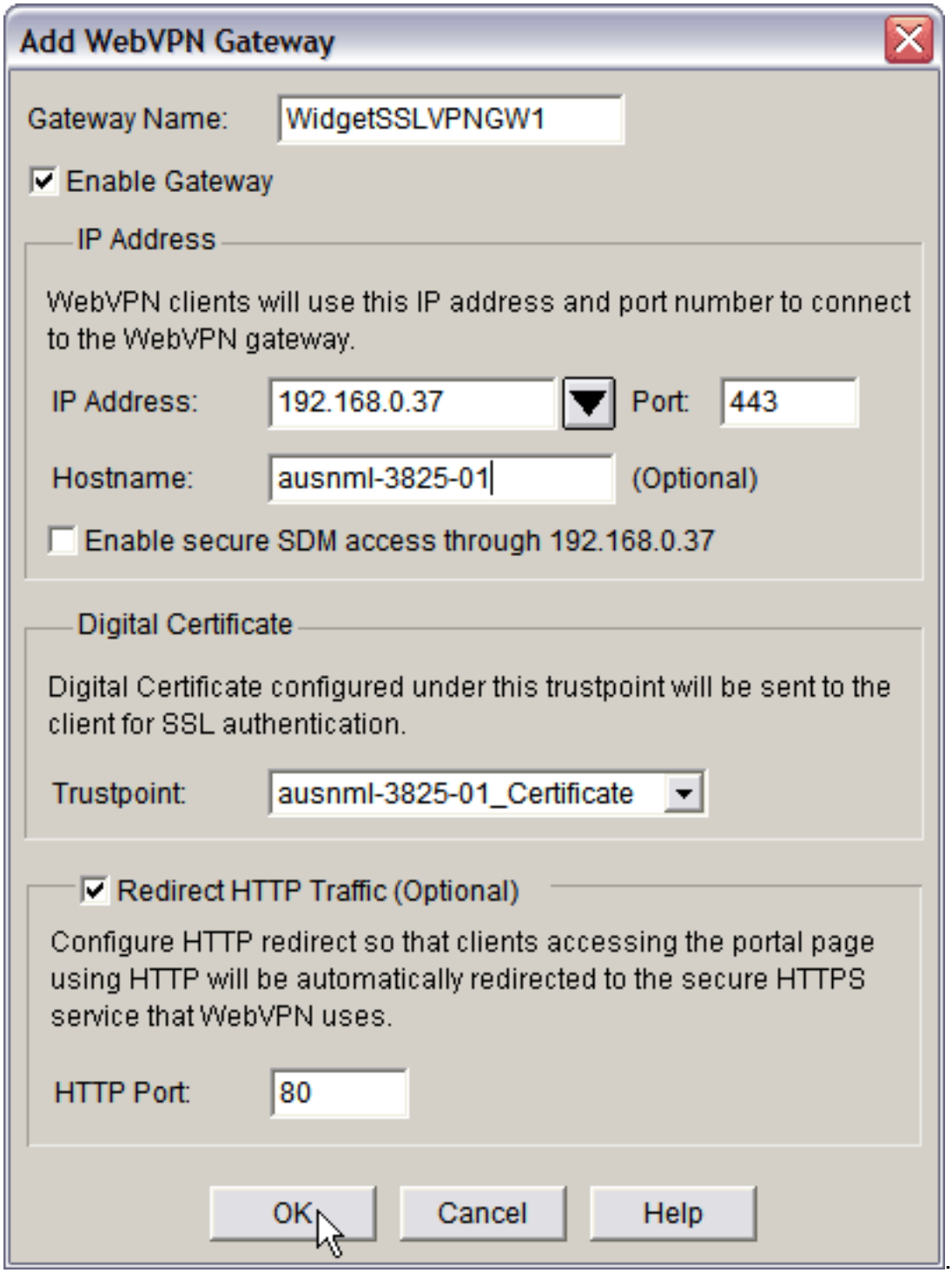
الخطوة 1. تكوين بوابة WebVPN

أكمل الخطوات التالية لتكوين بوابة WebVPN:

1. ضمن تطبيق إدارة قاعدة بيانات المحول (SDM)، انقر فوق **تكوين**، ثم انقر فوق **VPN**.
2. قم بتوسيع **WebVPN**، واختر **بوابات WebVPN**.



3. انقر فوق **إضافة (Add)**.يظهر مربع الحوار إضافة عبارة



.WebVPN

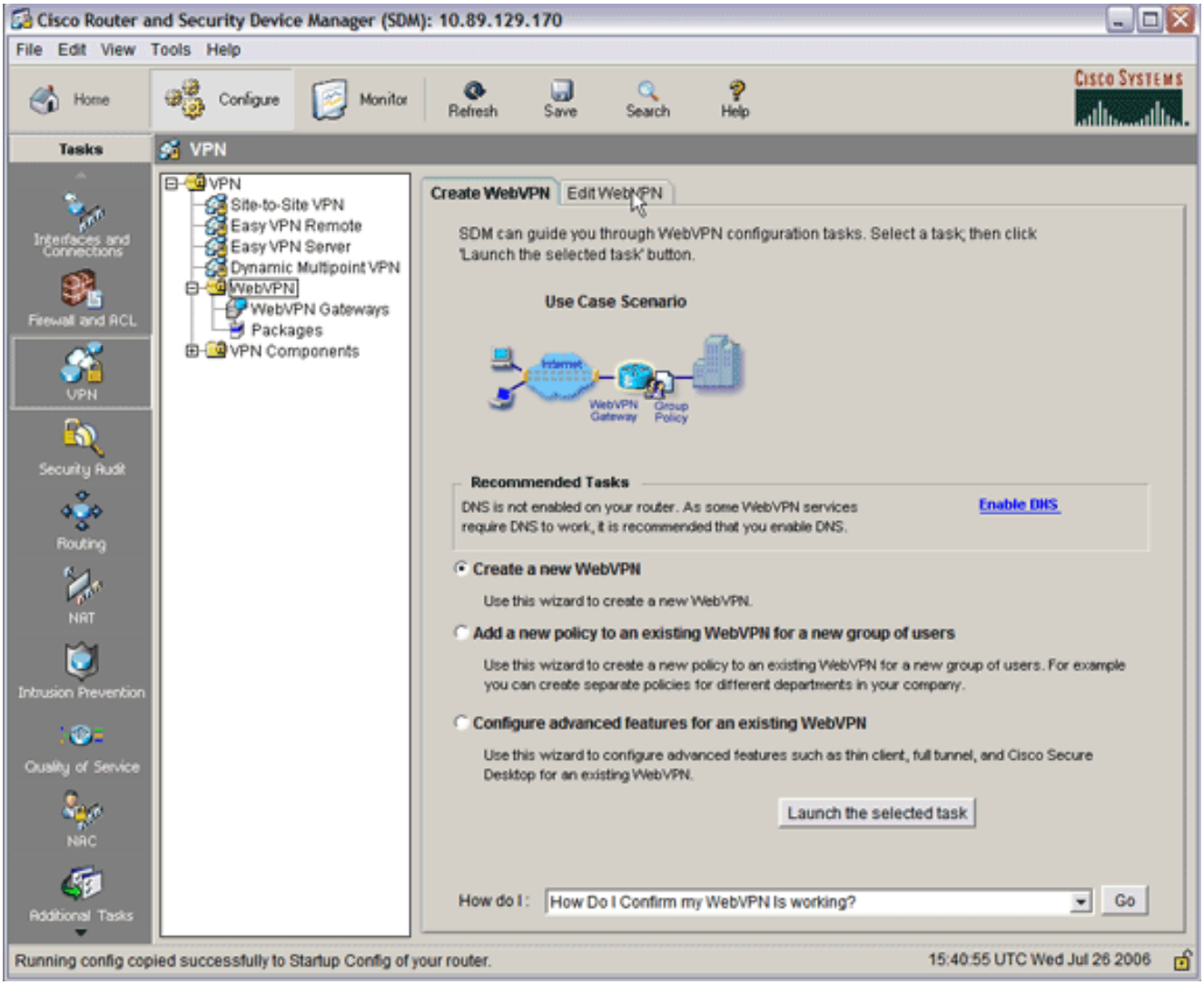
4. أدخل القيم في حقلي اسم البوابة وعنوان IP، ثم حدد خانة الاختيار **تمكين البوابة**.
5. حدد خانة الاختيار **إعادة توجيه حركة مرور HTTP**، ثم انقر فوق **موافق**.
6. انقر فوق **حفظ**، ثم انقر فوق **نعم** لقبول التغييرات.

الخطوة 2. تكوين الموارد المسموح بها لمجموعة النهج

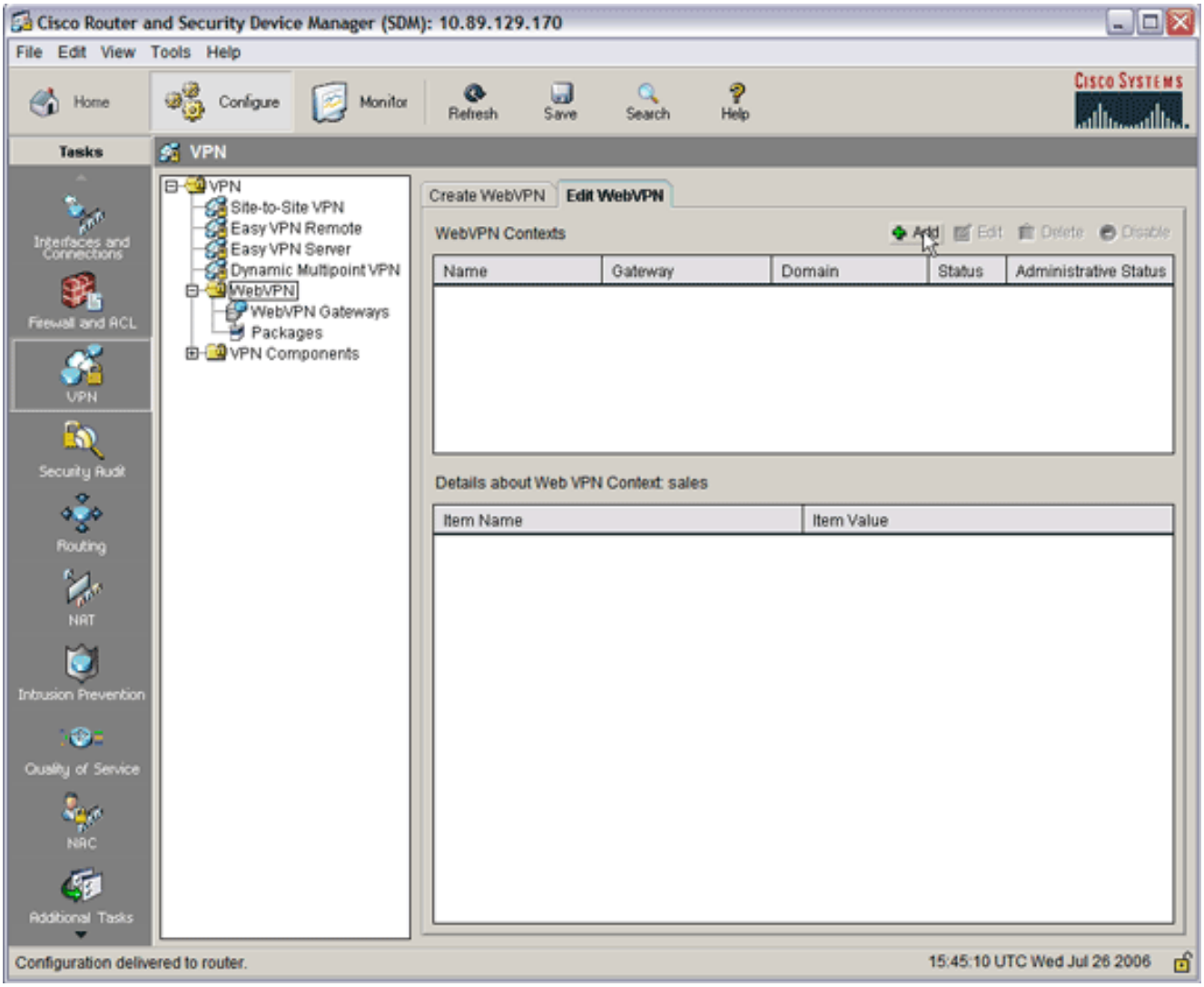
لتسهيل إضافة موارد إلى مجموعة نهج، يمكنك تكوين الموارد قبل إنشاء مجموعة النهج.

أكمل الخطوات التالية لتكوين الموارد المسموح بها لمجموعة النهج:

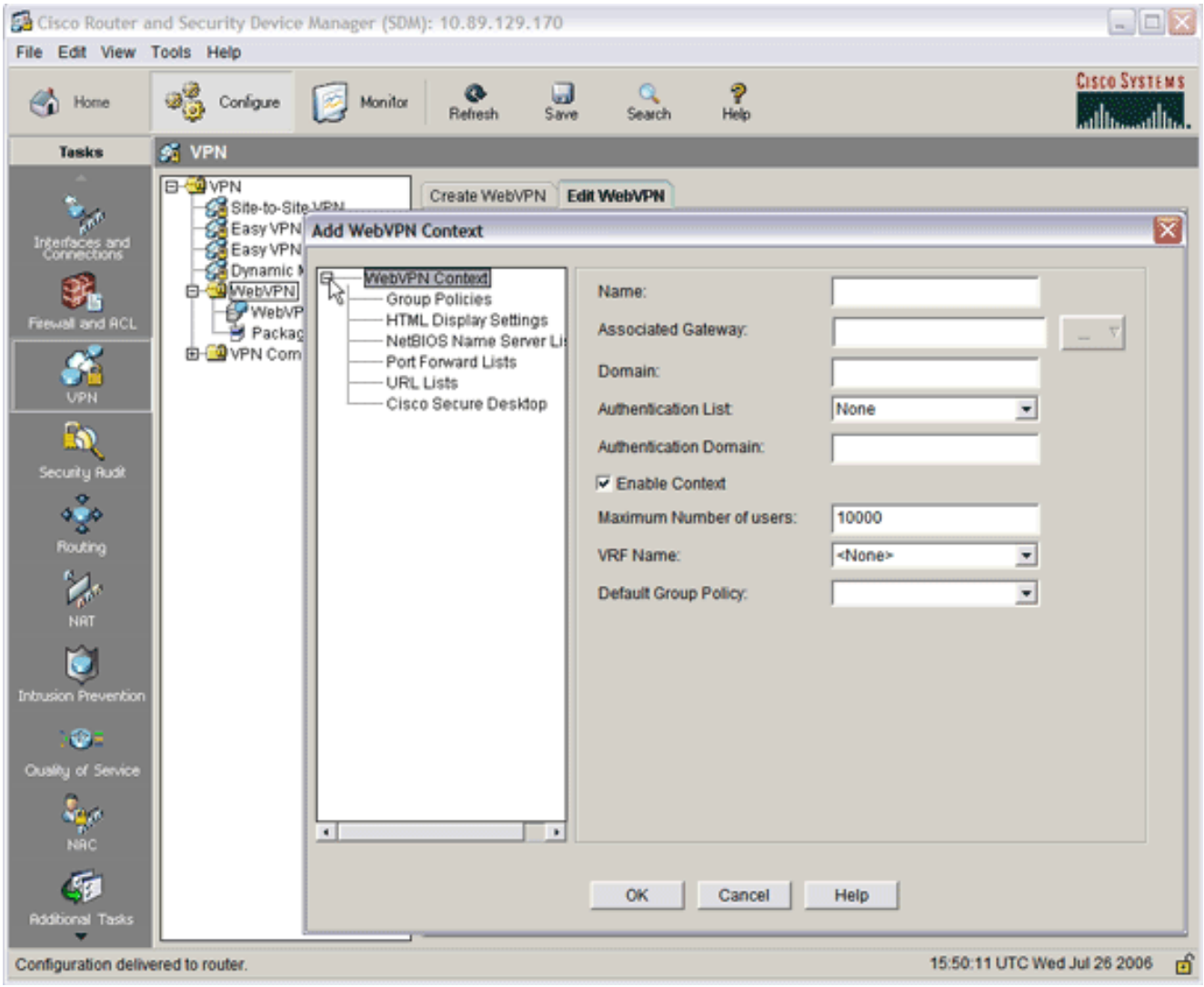
1. طقطقت **يشكل**، وبعد ذلك طقطقت
.VPN



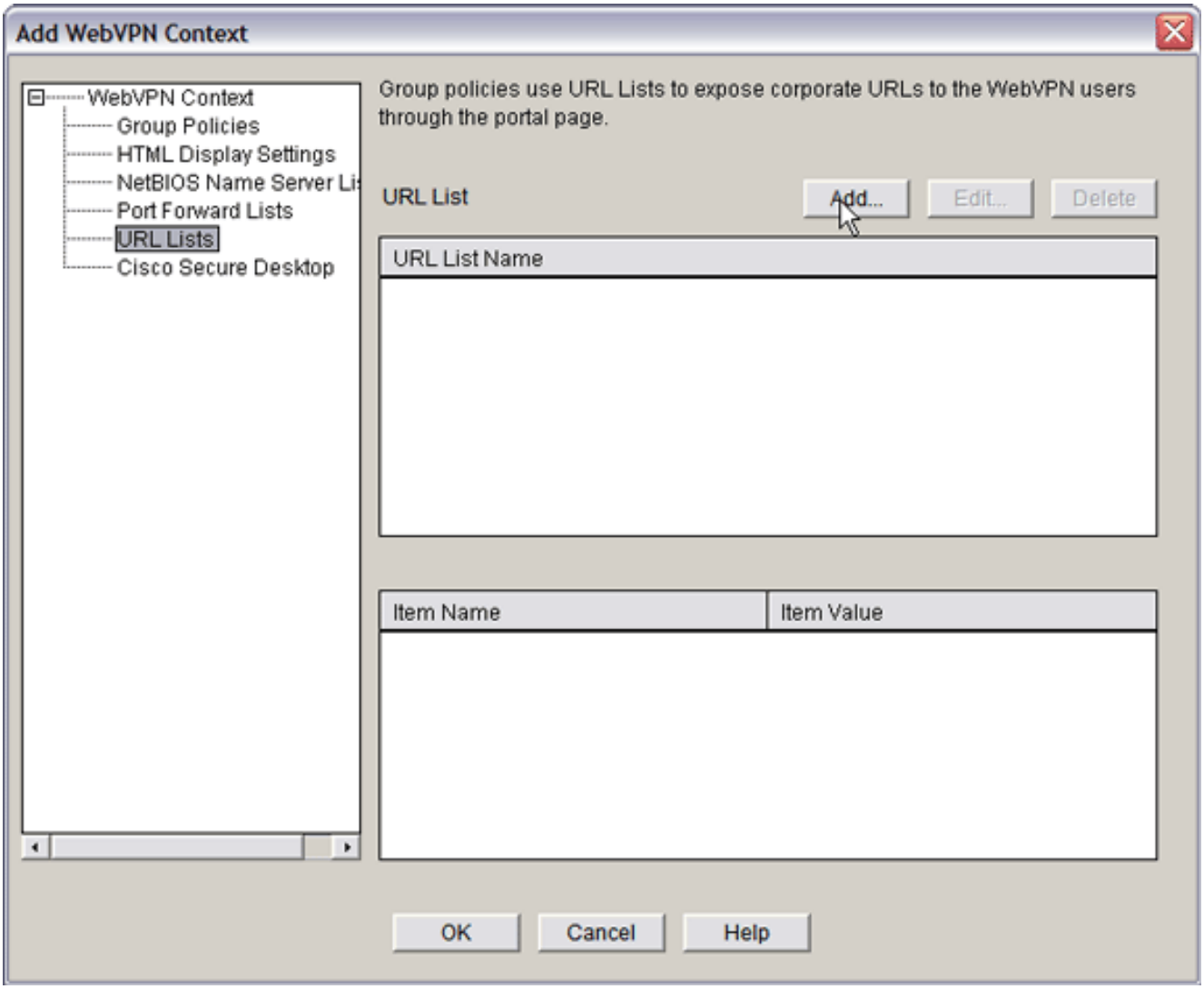
2. أختر **WebVPN**، ثم انقر فوق علامة التبويب **Edit WebVPN**.**ملاحظة:** يسمح لك WebVPN بتكوين الوصول إلى HTTP و HTTPS و Windows لتصفح الملفات من خلال بروتوكول نظام ملف الإنترنت الشائع (CIFS) و Citrix.



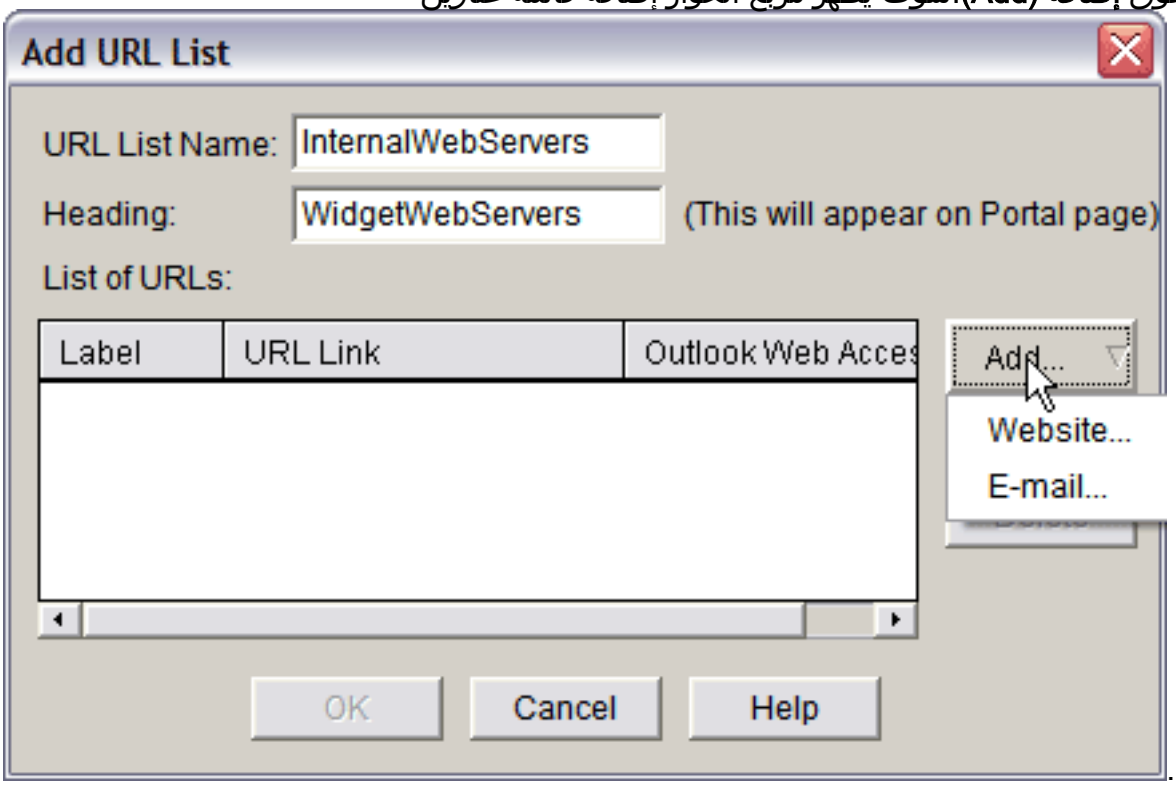
3. انقر فوق **إضافة (Add)**.يظهر مربع الحوار إضافة سياق WebVPN.



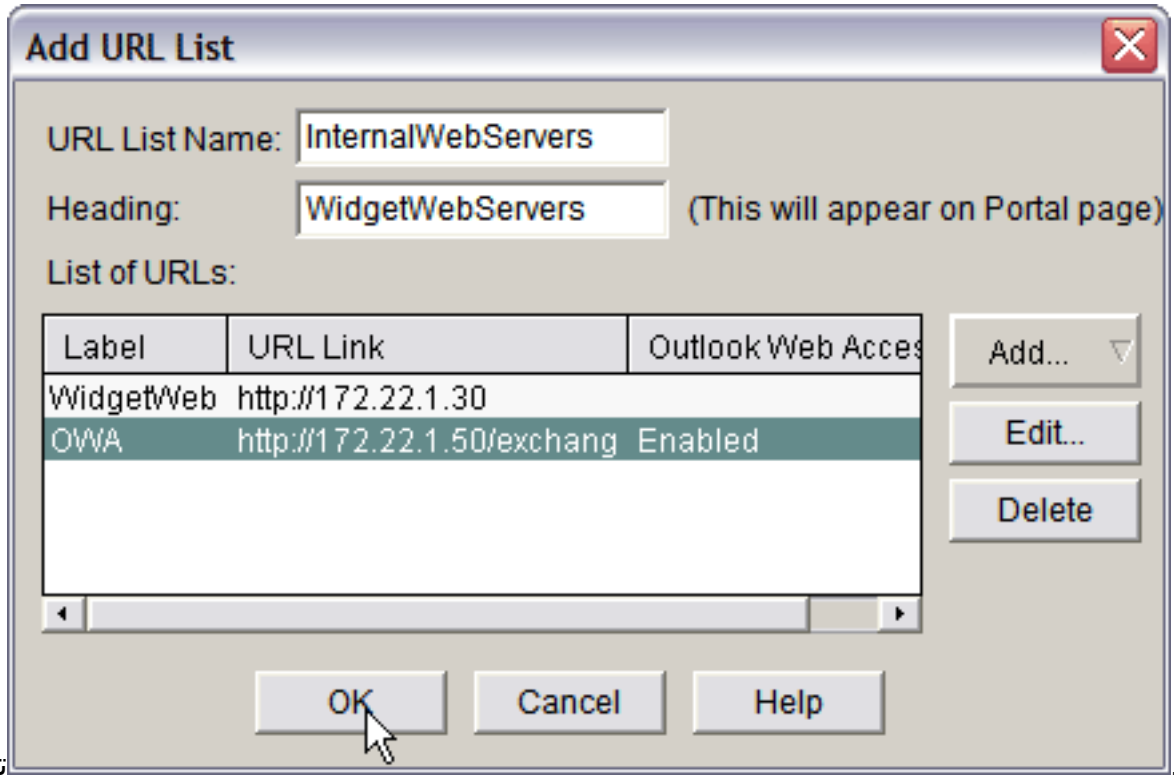
4. قم بتوسيع **سياق WebVPN**، واختر **قوائم عنوان URL**.



5. انقر فوق **إضافة (Add)**.سوف يظهر مربع الحوار إضافة قائمة عناوين URL.

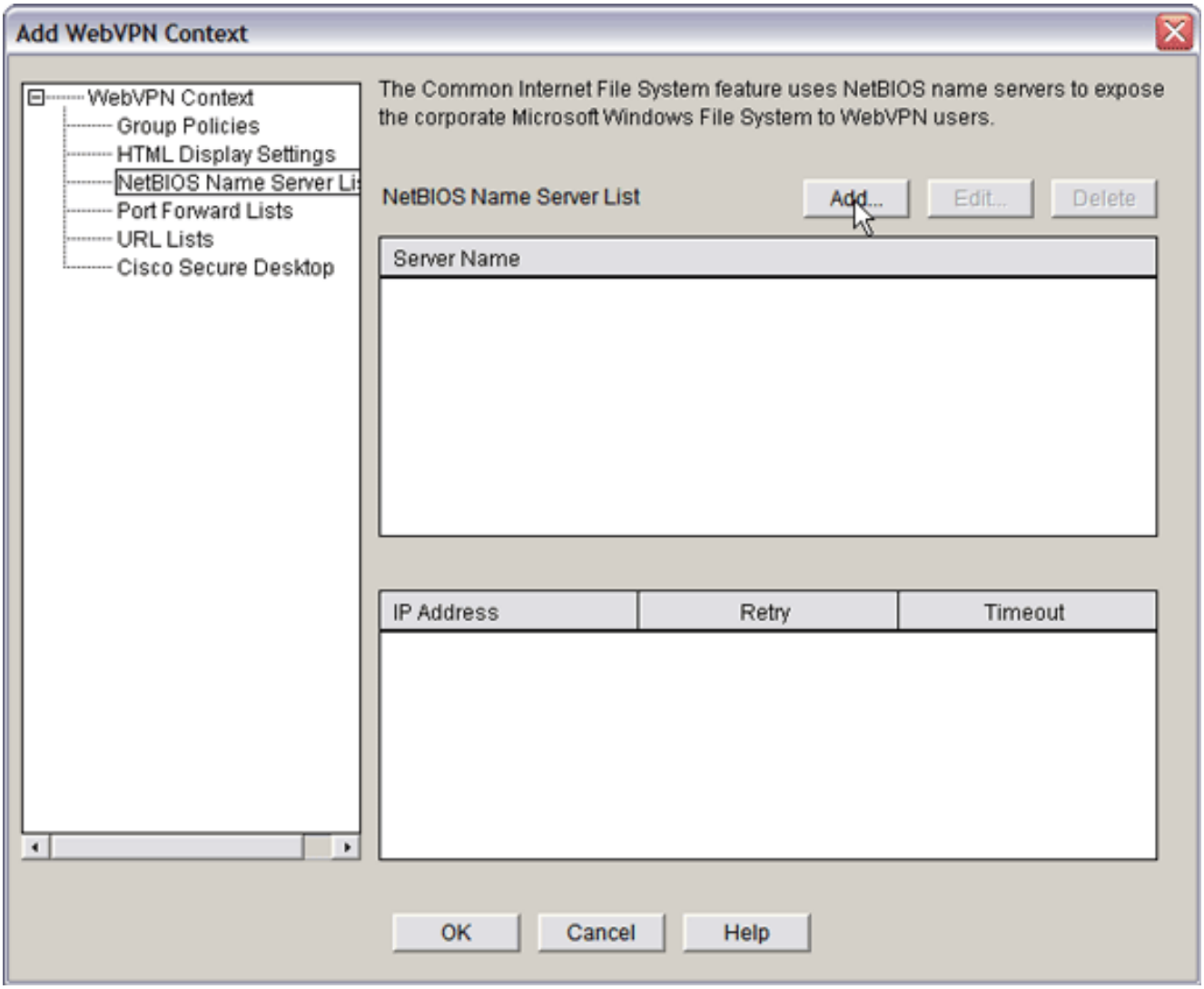


6. قم بإدخال القيم في حقلي اسم قائمة عنوان الربط والعنوان.
7. طقطقة **يضيف**، واخترت

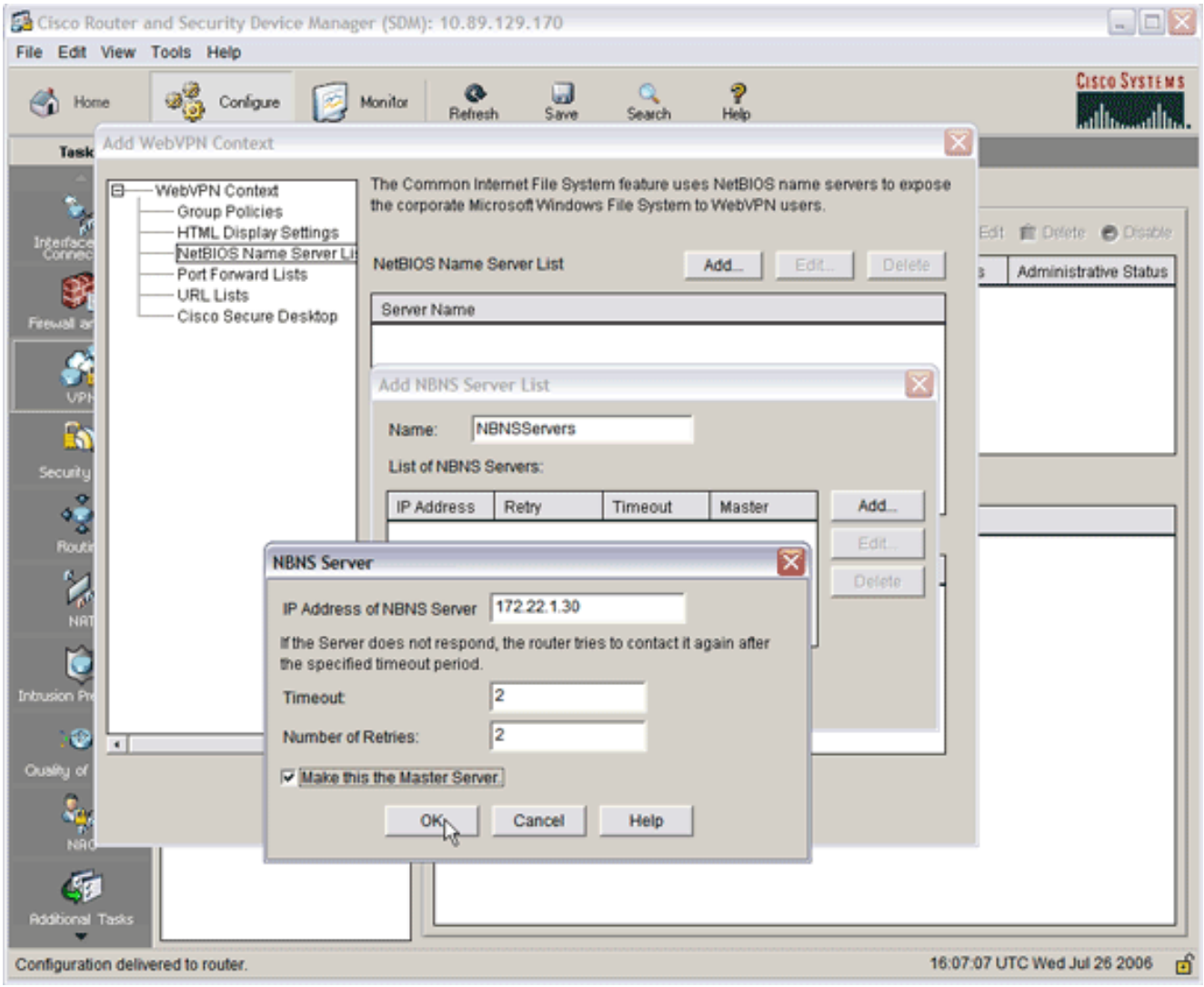


موقع. تحتوي هذه القائمة على كافة خوادم ويب HTTP و HTTPS التي تريد أن تكون متوفرة لاتصال WebVPN هذا.

8. لإضافة الوصول إلى Outlook Web Access (OWA)، انقر فوق **إضافة**، واختر **البريد الإلكتروني**، ثم انقر فوق **موافق** بعد أن تكون قد قمت بتعبئة كافة الحقول المطلوبة.
9. للسماح باستعراض ملفات Windows من خلال CIFS، يمكنك تعيين خادم خدمة أسماء NetBIOS (NBNS) وتكوين المشاركات المناسبة في مجال Windows بالترتيب.من قائمة سياق WebVPN، أختر **قوائم خادم اسم NetBIOS**.



انقر فوق **إضافة (Add)**.سوف يظهر مربع الحوار إضافة قائمة خوادم NBNS.أدخل اسم للقائمة، وانقر **إضافة**.تظهر شاشة خادم NBNS.

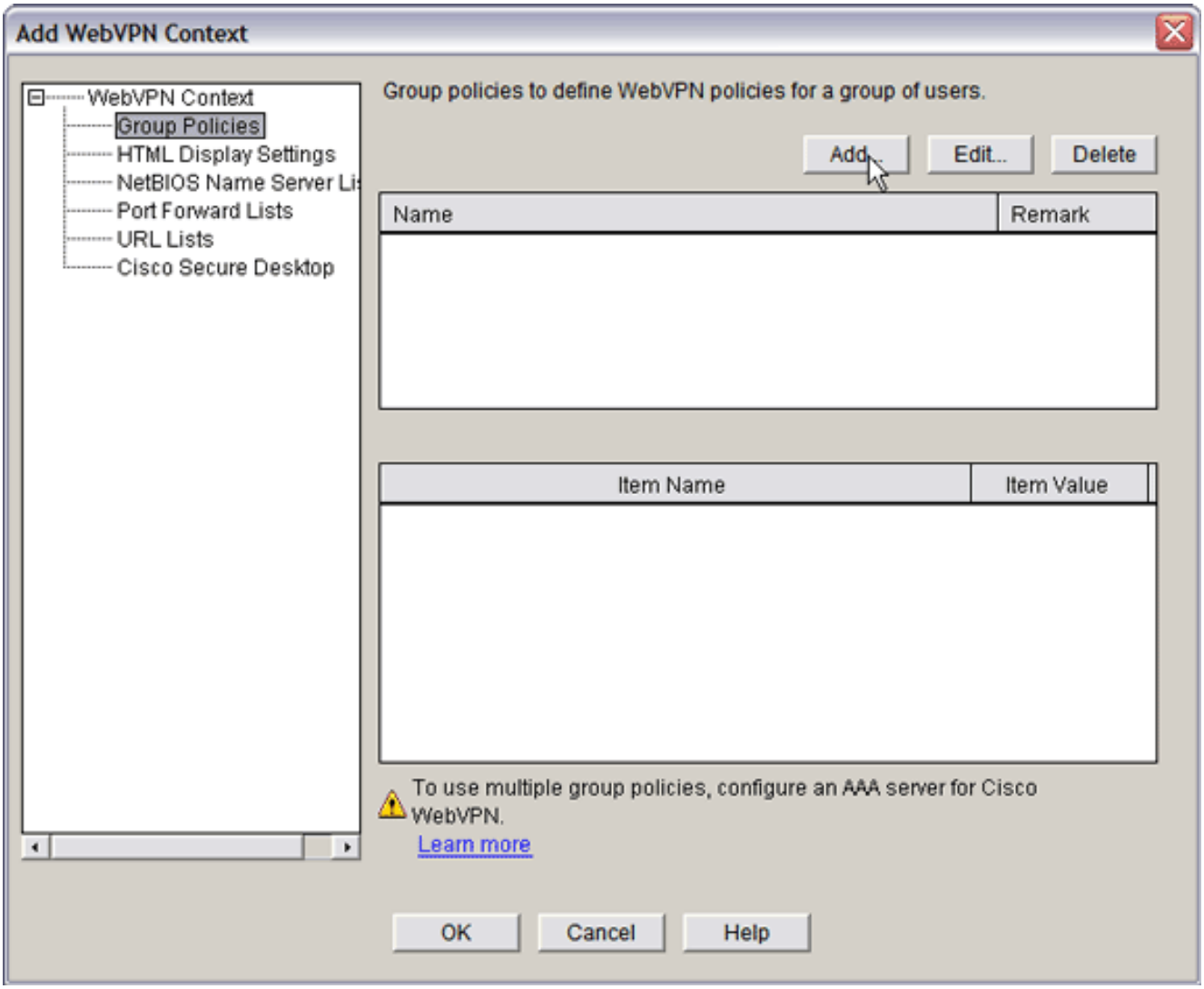


إن أمكن، حدد خانة الاختيار **جعل هذا هو الخادم الرئيسي**.طقطقت **ok**، وبعد ذلك طقطقت **ok**.

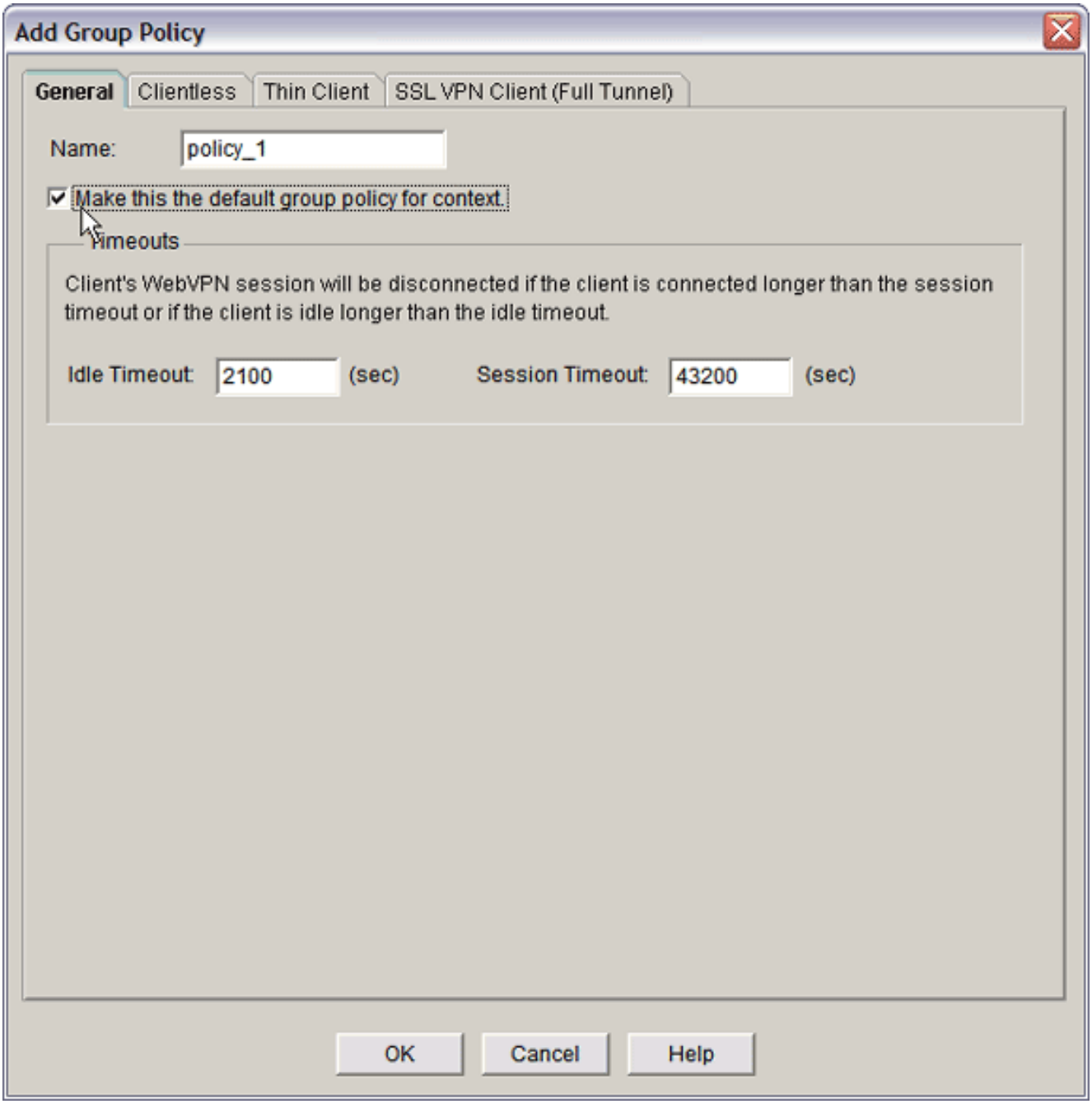
الخطوة 3. تكوين مجموعة نهج WebVPN وتحديد الموارد

أكمل الخطوات التالية لتكوين مجموعة نهج WebVPN وحدد الموارد:

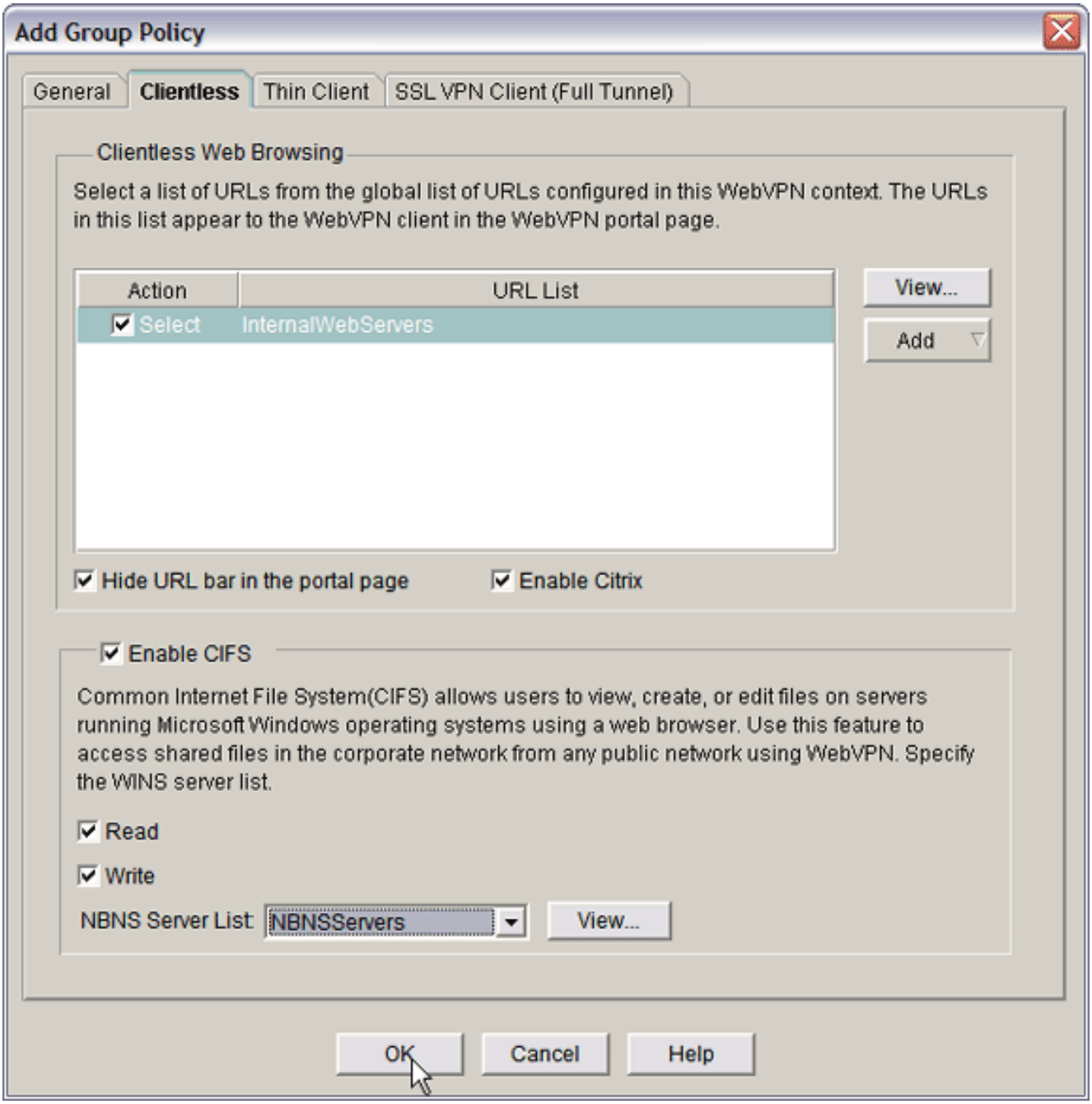
1. طقطقت **يشكل**، وبعد ذلك طقطقت **VPN**.
2. قم بتوسيع **WebVPN**، واختر **سياق WebVPN**.



3. أختر **نهج مجموعة**، وانقر **إضافة**.يظهر مربع الحوار إضافة نهج مجموعة.



4. أدخل اسما للنهج الجديد، وحدد خانة الاختيار **جعل هذا النهج نهج المجموعة الافتراضي للسياق**.
5. انقر صفحة **بدون زوايا** الموجودة في أعلى الشاشة.

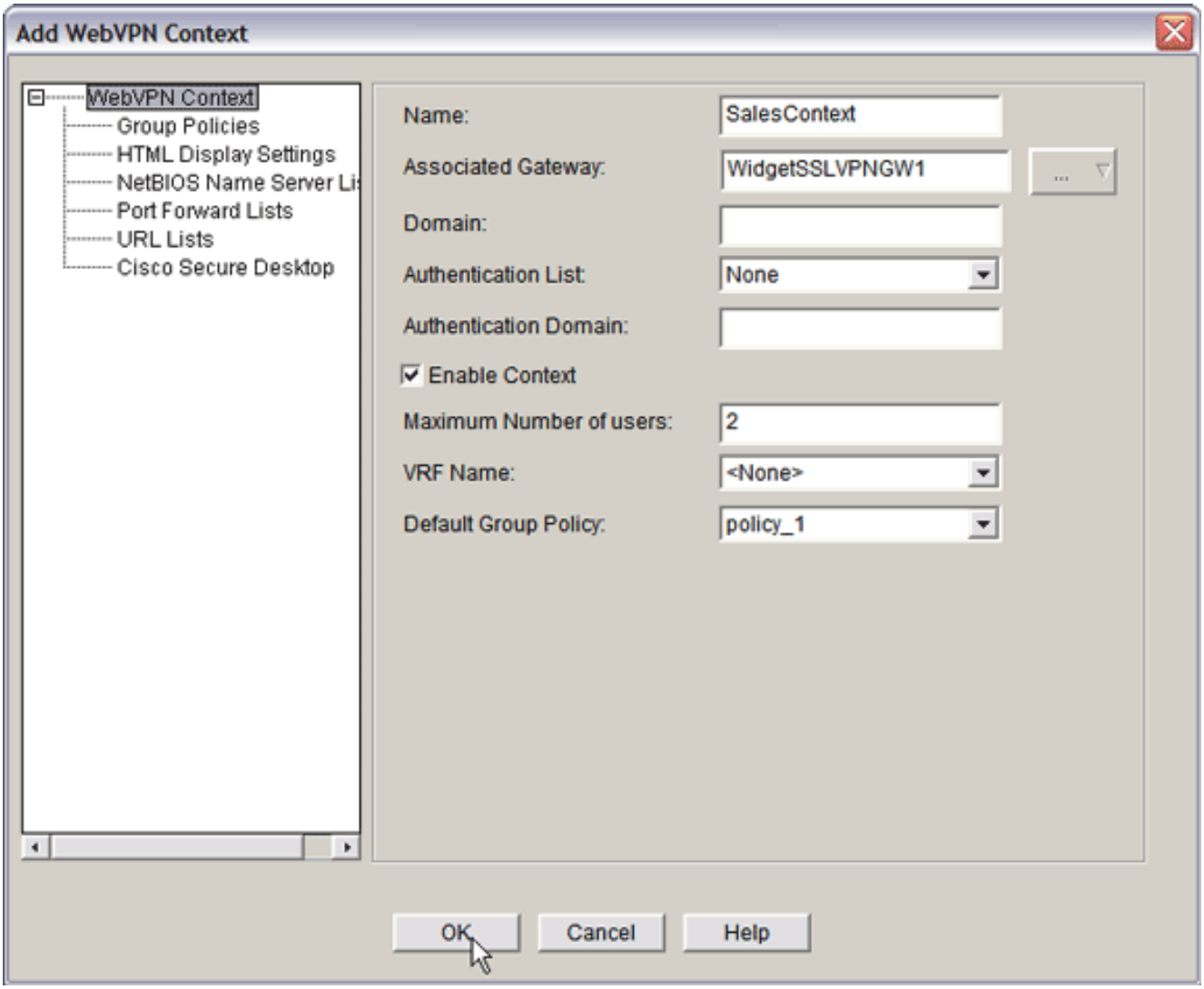


6. حدد خانة الاختيار **تحديد** لقائمة URL المطلوبة.
7. إذا كان عملاؤك يستخدمون عملاء Citrix الذين يحتاجون إلى الوصول إلى خوادم Citrix، فتحقق من خانة الاختيار **تمكين Citrix**.
8. حدد خانات الاختيار **تمكين CIFS**، **والقراءة**، **والكتابة**.
9. انقر فوق السهم المنسدل **لقائمة خوادم NBNS**، واختر قائمة خوادم NBNS التي قمت بإنشائها لاستعراض ملف Windows في الخطوة 2.
10. وانقر فوق **OK**.

الخطوة 4. تكوين سياق WebVPN

لربط بوابة WebVPN ونهج المجموعة والموارد معا، يجب تكوين سياق WebVPN. لتكوين سياق WebVPN، أكمل الخطوات التالية:

1. أختر **سياق WebVPN**، وأدخل اسما للسياق.



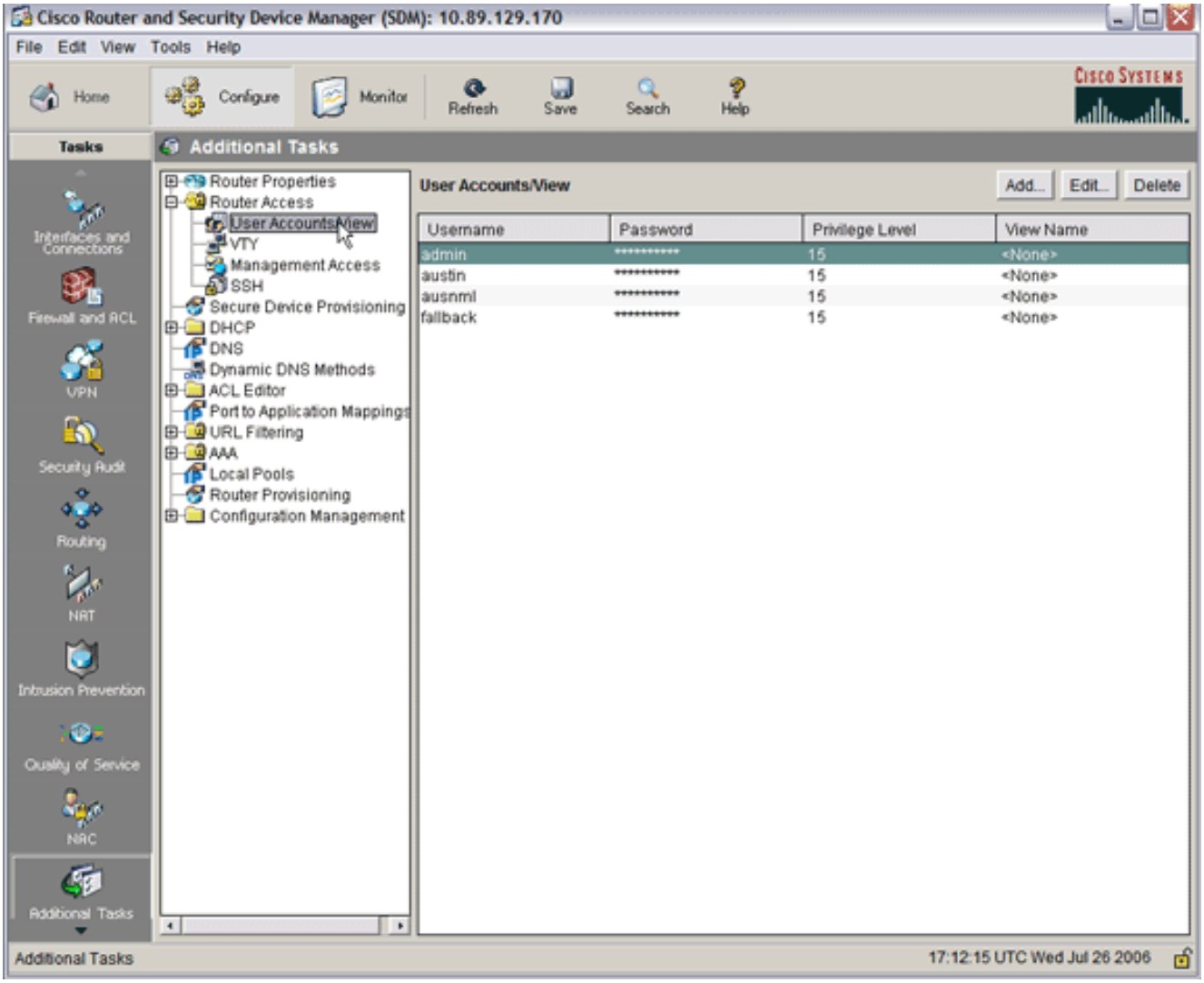
2. انقر فوق السهم المنسدل للعبارة المقترنة واختر بوابة مقترنة.
3. إذا كنت ترغب في إنشاء أكثر من سياق واحد، فأدخل اسما فريدا في حقل المجال لتعريف هذا السياق. إذا تركت حقل المجال فارغا، فيجب على المستخدمين الوصول إلى WebVPN باستخدام **https://**IPAress . إذا قمت بإدخال اسم مجال (على سبيل المثال، *Sales*)، فيجب على المستخدمين الاتصال ب **https://*IPAddress*/**Sales.
4. حدد خانة الاختيار **تمكين السياق**.
5. في حقل الحد الأقصى لعدد المستخدمين، أدخل الحد الأقصى لعدد المستخدمين المسموح بهم من قبل ترخيص الجهاز.
6. انقر فوق السهم المنسدل **لنهج المجموعة الافتراضي**، وحدد نهج المجموعة لإقرانه بهذا السياق.
7. طقطقت **ok**، وبعد ذلك طقطقت **ok**.

الخطوة 5. تكوين قاعدة بيانات المستخدم وطريقة المصادقة

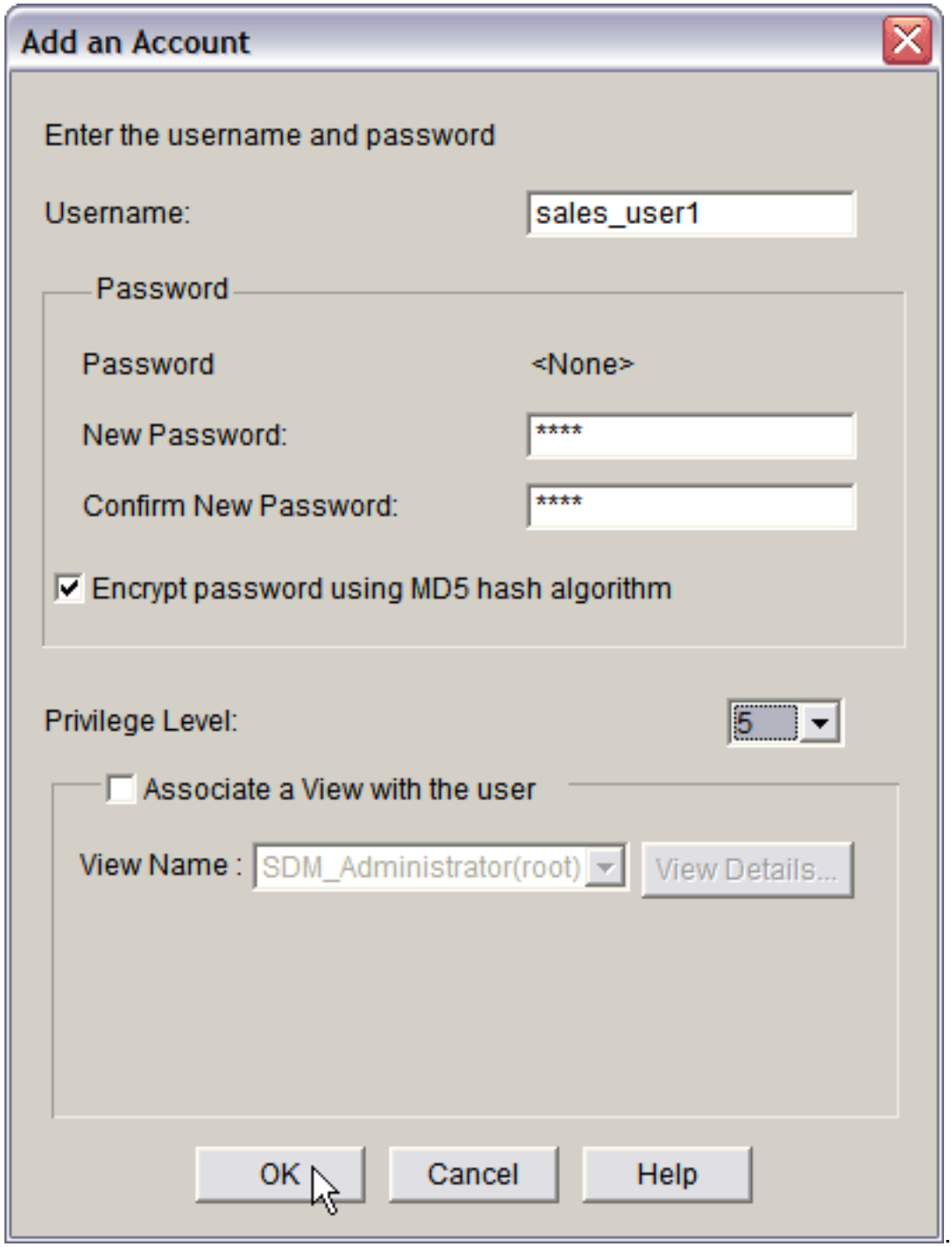
يمكنك تكوين جلسات عمل SSL VPN (WebVPN) بدون عملاء للمصادقة باستخدام RADIUS أو خادم Cisco AAA أو قاعدة بيانات محلية. يستخدم هذا المثال قاعدة بيانات محلية.

أتمت هذا steps in order to شكلت المستعمل قاعدة معطيات وطريق صحة هوية:

1. انقر فوق **تكوين**، ثم انقر فوق **مهام إضافية**.
2. قم بتوسيع **الوصول إلى الموجه**، واختر **حسابات/عرض المستخدم**.



3. انقر فوق الزر **إضافة**.يظهر مربع الحوار إضافة



حساب.

4. أدخل حساب مستخدم وكلمة مرور.
5. طقطقت **ok**، وبعد ذلك طقطقت **ok**.
6. انقر فوق **حفظ**، ثم انقر فوق **نعم** لقبول التغييرات.

النتائج

يقوم ASDM بإنشاء تكوينات سطر الأوامر هذه:

أوسن01-ml-3825
...Building configuration Current configuration : 4190 bytes ! Last configuration change at 17:22:23 UTC Wed Jul 26 ! 2006 by ausnml

```
NVRAM config last updated at 17:22:31 UTC Wed Jul 26 !
                                                2006 by ausnml
                                                          !
                                                 version 12.4
                        service timestamps debug datetime msec
                          service timestamps log datetime msec
                                   service password-encryption
                                                          !
                                        hostname ausnml-3825-01
                                                          !
                                                boot-start-marker
  boot system flash c3825-adventerprisek9-mz.124-9.T.bin
                                                boot-end-marker
                                                          !
                                             no logging buffered
          /enable secret 5 $1$KbIu$5o8qKYAVpWvyv9rYbrJLi
                                                          !
                                                aaa new-model
                                                          !
                        aaa authentication login default local
       aaa authentication login sdm_vpn_xauth_ml_1 local
                        aaa authorization exec default local
                                                          !
                                          aaa session-id common
                                                          !
                                                 resource policy
                                                          !
                                                      ip cef
                                                          !
                                       ip domain name cisco.com
                                                          !
                                                 voice-card 0
                                                  no dspfarm
                                                          !
     Self-Signed Certificate Information crypto pki ---!
        trustpoint ausnml-3825-01_Certificate enrollment
           selfsigned serial-number none ip-address none
            revocation-check crl rsakeypair ausnml-3825-
     01_Certificate_RSAKey 1024 ! crypto pki certificate
chain ausnml-3825-01_Certificate certificate self-signed
02 30820240 308201A9 A0030201 02020102 300D0609 2A864886
   F70D0101 04050030 29312730 2506092A 864886F7 0D010902
   16186175 736E6D6C 2D333832 352D3031 2E636973 636F2E63
   6F6D301E 170D3036 30373133 32333230 34375A17 0D323030
   31303130 30303030 305A3029 31273025 06092A86 4886F70D
   01090216 18617573 6E6D6C2D 33383235 2D30312E 63697363
   6F2E636F 6D30819F 300D0609 2A864886 F70D0101 01050003
   818D0030 81890281 8100C97D 3D259BB7 3A48F877 2C83222A
   A1E9E42C 5A71452F 9107900B 911C0479 4D31F42A 13E0F63B
   E44753E4 0BEFDA42 FE6ED321 8EE7E811 4DEEC4E4 319C0093
   C1026C0F 38D91236 6D92D931 AC3A84D4 185D220F D45A411B
   09BED541 27F38EF5 1CC01D25 76D559AE D9284A74 8B52856D
   BCBBF677 0F444401 D0AD542C 67BA06AC A9030203 010001A3
   78307630 0F060355 1D130101 FF040530 030101FF 30230603
   551D1104 1C301A82 18617573 6E6D6C2D 33383235 2D30312E
   63697363 6F2E636F 6D301F06 03551D23 04183016 801403E1
   5EAABA47 79F6C70C FBC61B08 90B26C2E 3D4E301D 0603551D
   0E041604 1403E15E AABA4779 F6C70CFB C61B0890 B26C2E3D
   4E300D06 092A8648 86F70D01 01040500 03818100 6938CEA4
   2E56CDFF CF4F2A01 BCD585C7 D6B01665 595C3413 6B7A7B6C
   F0A14383 4DA09C30 FB621F29 8A098FA4 F3A7F046 595F51E6
   7C038112 0934A369 D44C0CF4 718A8972 2DA33C43 46E35DC6
   5DCAE7E0 B0D85987 A0D116A4 600C0C60 71BB1136 486952FC
   55DE6A96 1135C9D6 8C5855ED 4CD3AE55 BDA966D4 BE183920
```

```
      88A8A55E quit username admin privilege 15 secret 5
$1$jm6N$2xNfhupbAinq3BQZMRzrW0 username ausnml privilege
        15 password 7 15071F5A5D292421 username fallback
privilege 15 password 7 08345818501A0A12 username austin
    privilege 15 secret 5 $1$3xFv$W0YUsKDx1adDc.cVQF2Ei0
              username sales_user1 privilege 5 secret 5
             $1$2/SX$ep4fsCpodeyKaRji2mJkX/ ! interface
GigabitEthernet0/0 ip address 192.168.0.37 255.255.255.0
      duplex auto speed auto media-type rj45 ! interface
GigabitEthernet0/1 ip address 172.22.1.151 255.255.255.0
       duplex auto speed auto media-type rj45 ! ip route
     0.0.0.0 0.0.0.0 172.22.1.1 ! ip http server ip http
    authentication local ip http timeout-policy idle 600
    life 86400 requests 100 ! control-plane ! line con 0
     stopbits 1 line aux 0 stopbits 1 line vty 0 4 exec-
             timeout 40 0 privilege level 15 password 7
  071A351A170A1600 transport input telnet ssh line vty 5
       15 exec-timeout 40 0 password 7 001107505D580403
   transport input telnet ssh ! scheduler allocate 20000
             1000 ! !--- WebVPN Gateway webvpn gateway
      WidgetSSLVPNGW1 hostname ausnml-3825-01 ip address
         192.168.0.37 port 443 http-redirect port 80 ssl
trustpoint ausnml-3825-01_Certificate inservice ! webvpn
 context SalesContext ssl authenticate verify all ! !---
     Identify resources for the SSL VPN session url-list
"InternalWebServers" heading "WidgetWebServers" url-text
     "WidgetWeb" url-value "http://172.22.1.30" url-text
   "OWA" url-value "http://172.22.1.50/exchange" ! nbns-
list NBNSServers nbns-server 172.22.1.30 ! !--- Identify
the policy which controls the resources available policy
  group policy_1 url-list "InternalWebServers" nbns-list
     "NBNSServers" functions file-access functions file-
 browse functions file-entry hide-url-bar citrix enabled
   default-group-policy policy_1 gateway WidgetSSLVPNGW1
                                max-users 2 inservice ! end
```

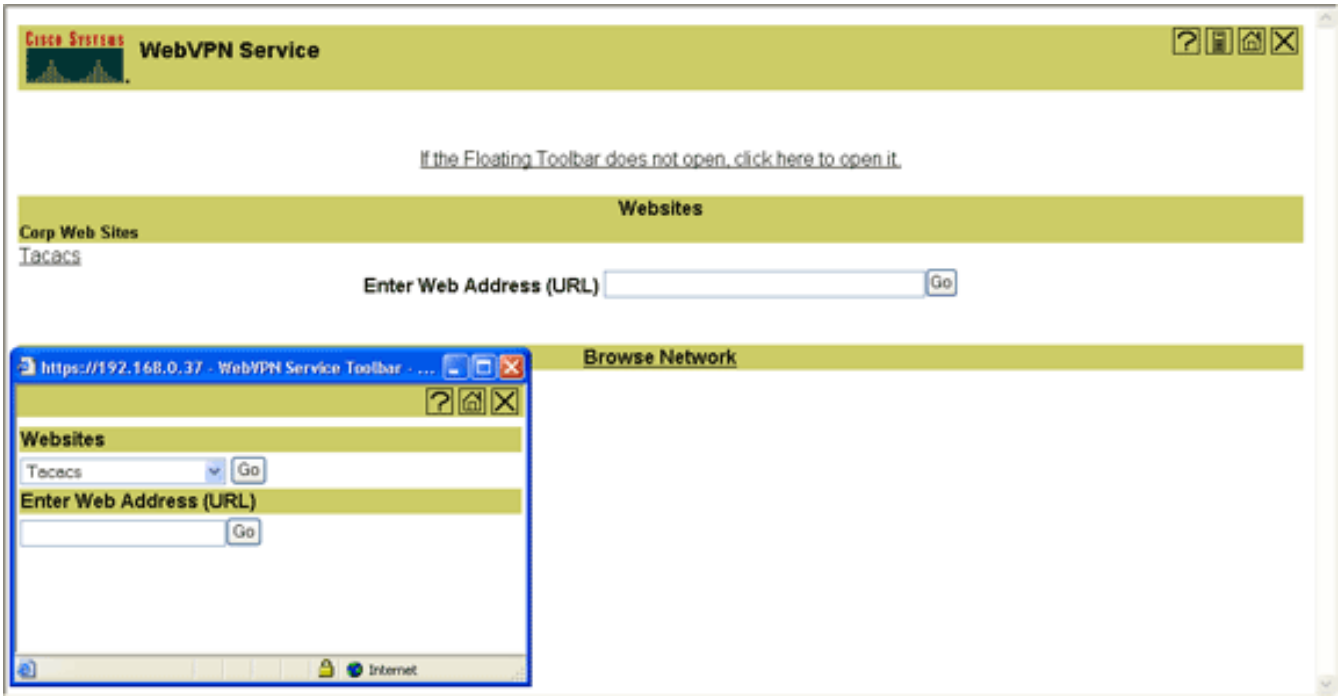
التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

الإجراء

أكمل هذه الإجراءات للتأكد من أن التكوين لديك يعمل بشكل صحيح:

- اختبر التكوين الخاص بك مع مستخدم ما. أدخل **https://*WebVPN_GATEWAY_IP_ADDRESS*** في مستعرض ويب تم تمكين SSL به؛ حيث يمثل *WebVPN_GATEWAY_IP_ADDRESS* عنوان IP الخاص بخدمة WebVPN. بعد أن تقوم بقبول الترخيص وإدخال اسم مستخدم وكلمة مرور، يجب أن تظهر شاشة مماثلة لهذه
الصورة.



- تحقق من جلسة عمل SSL VPN. ضمن تطبيق إدارة قاعدة بيانات المحول (SDM)، انقر فوق الزر **جهاز العرض**، ثم انقر فوق **حالة الشبكة الخاصة الظاهرية (VPN)**. قم بتوسيع **WebVPN (كل السياقات)**، وتوسعة السياق المناسب، واختر **المستخدمين**.
- تحقق من رسائل الخطأ. ضمن تطبيق إدارة قاعدة بيانات المحول (SDM)، انقر فوق زر **جهاز العرض**، ثم انقر فوق **تسجيل**، ثم انقر فوق علامة التبويب **syslog**.
- عرض التكوين الجاري تشغيله للجهاز. ضمن تطبيق إدارة قاعدة بيانات المحول (SDM)، انقر فوق الزر **تكوين**، ثم انقر فوق **مهام إضافية**. قم بتوسيع **إدارة التكوين**، واختر **محرر التكوين**.

الأوامر

يتم إقران العديد من أوامر **العرض** مع WebVPN. يمكنك تنفيذ هذه الأوامر في واجهة سطر الأوامر (CLI) لإظهار الإحصائيات ومعلومات أخرى. للحصول على معلومات تفصيلية حول **أوامر العرض**، ارجع إلى التحقق من تكوين WebVPN.

ملاحظة: الإنتاج مترجم يساند أداة (يسجل زبون فقط) (OIT) مؤكد **عرض** أمر. استخدم أداة مترجم الإخراج (OIT) لعرض تحليل مُخرَج الأمر **show** .

استكشاف الأخطاء وإصلاحها

أستخدم هذا القسم لاستكشاف أخطاء التكوين وإصلاحها.

ملاحظة: لا تقاطع الأمر **نسخ ملف إلى الخادم** أو انتقل إلى نافذة مختلفة أثناء عملية النسخ. يمكن أن يؤدي توقف العملية إلى حفظ ملف غير مكتمل على الخادم.

ملاحظة: يمكن للمستخدمين تحميل الملفات الجديدة وتنزيلها باستخدام عميل WebVPN، ولكن غير مسموح للمستخدم باستبدال الملفات الموجودة في نظام ملف الإنترنت الشائع (CIFS) على WebVPN باستخدام الأمر **نسخ الملف إلى الخادم**. يتلقى المستخدم هذه الرسالة عندما يحاول المستخدم إستبدال ملف على الخادم:

```
Unable to add the file
```

الإجراء

أتمت هذا steps in order to تحريت تشكيلك:

1. تأكد من تعطيل العملاء لمحولات الإطارات المنبثقة.
2. تأكد من تمكين ملفات تعريف الارتباط للعملاء.
3. تأكد من أن العملاء يستخدمون مستعرضات الويب Netscape أو Internet Explorer أو Firefox أو Mozilla.

الأوامر

تقترن العديد من أوامر **تصحيح الأخطاء** ب WebVPN. راجع إستخدام أوامر تصحيح الأخطاء ل WebVPN للحصول على معلومات تفصيلية حول هذه الأوامر.

ملاحظة: يمكن أن يؤثر إستخدام أوامر **تصحيح الأخطاء سلبا** على جهاز Cisco الخاص بك. قبل إستخدام أوامر **debug**، ارجع إلى معلومات مهمة عن أوامر تصحيح الأخطاء.

معلومات ذات صلة

- Cisco من IOS SSLVPN
- Cisco IOS SSLVPN Q&A
- مثال تكوين IOS للعميل قليل السمك (SSL VPN (WebVPN مع SDM
- (SSL VPN Client (SVC على IOS مع مثال تكوين SDM
- 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).