# ASA 8.x: يقفنلا لاصتالا ميسقتب حامسلا نيوكت لائم ىلع AnyConnect VPN ليمعل ASA

### المحتويات

<u>المقدمة</u> المتطلبات الأساسية <u>المكونات المستخدمة</u> <u>المكونات المستخدمة</u> معلومات أساسية <u>التكوين</u> <u>الرسم التخطيطي للشبكة</u> <u>الرسم التخطيطي للشبكة</u> <u>تكوين ASA باستخدام 2)AS MOM (ASDM 6.0</u> <u>تكوين ASA CLI باستخدام SVC التحقق من الصحة</u> <u>التحقق من الصحة</u> <u>الستكشاف الأخطاء وإصلاحها</u> <u>معلومات ذات صلة</u>

### <u>المقدمة</u>

يقدم هذا المستند إرشادات خطوة بخطوة حول كيفية السماح بوصول عميل Cisco AnyConnect VPN إلى الإنترنت أثناء إنشاء قنوات لها في جهاز الأمان القابل للتكيف (ASA) من Cisco 8.0.2. يتيح هذا التكوين للعميل إمكانية الوصول الآمن إلى موارد الشركة عبر SSL أثناء منح وصول غير آمن إلى الإنترنت باستخدام الاتصال النفقي المنقسم.

### <u>المتطلبات الأساسية</u>

#### <u>المتطلبات</u>

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

- يحتاج جهاز الأمان ASA إلى تشغيل الإصدار x.8
- العميل AnyConnect VPN (AnyConnect حظ**ة:** تنزيل حزمة عميل -AnyConnect VPN (AnyConnect العمل ASA من Cisco (<u>للعملاء</u> المسجلين فقط). انسخ عميل AnyConnect VPN إلى ذاكرة ASA (win\*.pkg) من <u>تنزيل برامج</u> Cisco (<u>للعملاء</u> المسجلين فقط). انسخ عميل AnyConnect VPN (بل ذاكرة ASA راجع قسم flash، والتي يجب تنزيلها إلى أجهزة كمبيوتر المستخدم البعيدة لإنشاء اتصال SSL VPN مع ASA. راجع قسم <u>تثبيت عميل AnyConnect</u> من دليل تكوين ASA للحصول على مزيد من المعلومات.

<u>المكونات المستخدمة</u>

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

- Cisco 5500 Series ASA أن يركض برمجية صيغة 8.0(2)
- إصدار عميل AnyConnect SSL VPN من Cisco ل Windows 2.0.0343
- جهاز الكمبيوتر الذي يقوم بتشغيل Microsoft Visa أو Windows XP SP2 أو Windows 2000 Professional As مع Microsoft Installer الإصدار 3.1
  - Cisco Adaptive Security Device Manager (ASDM)، الإصدار 2)6.0)، الإصدار 2)

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.

### <u>الاصطلاحات</u>

راجع <u>اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.</u>

### <u>معلومات أساسية</u>

يوفر عميل AnyConnect VPN من Cisco إتصالات SSL الآمنة بجهاز الأمان للمستخدمين عن بعد. دون وجود عميل تم تثبيته مسبقا، يقوم المستخدمون عن بعد بإدخال عنوان IP في المستعرض الخاص بهم من واجهة تم تكوينها لقبول إتصالات SSL VPN. ما لم يتم تكوين جهاز الأمان لإعادة توجيه طلبات http:// إلى https://، يجب على المستخدمين إدخال عنوان URL في النموذج https://saddress.

بعد إدخال عنوان URL، يتصل المستعرض بتلك الواجهة ويعرض شاشة تسجيل الدخول. إذا استوفى المستخدم تسجيل الدخول والمصادقة، وقام جهاز الأمان بتعريف المستخدم على أنه يتطلب من العميل، فإنه يقوم بتنزيل العميل الذي يتطابق مع نظام تشغيل الكمبيوتر البعيد. بعد التنزيل، يقوم العميل بتثبيت نفسه وتكوينه وإنشاء اتصال SSL آمن ويبقى أو يقوم بإلغاء تثبيت نفسه (حسب تكوين جهاز الأمان) عند إنهاء الاتصال.

في حالة عميل تم تثبيته مسبقا، عندما يقوم المستخدم بالتصديق، يقوم جهاز الأمان بفحص مراجعة العميل وترقية العميل حسب الضرورة.

عندما يقوم العميل بالتفاوض على اتصال SSL VPN باستخدام جهاز الأمان، فإنه يتصل باستخدام أمان طبقة النقل (TLS)، وبشكل إختياري، أمان طبقة نقل البيانات (DTLS). تتجنب DTLS مشاكل زمن الوصول والنطاق الترددي المقترنة ببعض إتصالات SSL، وتحسن أداء تطبيقات الوقت الفعلي الحساسة لتأخيرات الحزم.

يمكن تنزيل عميل AnyConnect من جهاز الأمان أو يمكن تثبيته يدويا على الكمبيوتر البعيد بواسطة مسؤول النظام. ارجع إلى <u>دليل مسؤول عميل AnyConnect VPN من Cisco</u> للحصول على مزيد من المعلومات حول كيفية تثبيت العميل يدويا.

يقوم جهاز الأمان بتنزيل العميل استنادا إلى نهج المجموعة أو سمات اسم المستخدم الخاصة بالمستخدم الذي يقوم بإنشاء الاتصال. يمكنك تكوين جهاز الأمان لتنزيل العميل تلقائيا، أو يمكنك تكوينه لمطالبة المستخدم البعيد حول ما إذا كان سيتم تنزيل العميل أم لا. وفي الحالة الأخيرة، إذا لم يستجب المستخدم، فيمكنك تكوين جهاز الأمان إما لتنزيل العميل بعد فترة المهلة أو لتقديم صفحة تسجيل الدخول.

## <u>التكوين</u>

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

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

#### <u>الرسم التخطيطي للشبكة</u>

يستخدم هذا المستند إعداد الشبكة التالي:



**ملاحظة:** ال ip ليس يخاطب خطة يستعمل في هذا تشكيل قانونيا routable على الإنترنت. وهي عناوين<u>RFC 1918</u> التي تم استخدامها في بيئة مختبرية.

#### <u>تكوين ASA باستخدام 2)6.0 (ASDM)</u>

يفترض هذا المستند أن التكوين الأساسي، مثل تكوين الواجهة، قد تم إنشاؤه بالفعل ويعمل بشكل صحيح.

ملاحظة: ارجع إلى <u>السماح بوصول HTTPS إلى ASDM</u> للسماح بتكوين ASA بواسطة ASDM.

**ملاحظة:** لا يمكن تمكين WebVPN و ASDM على واجهة ASA نفسها ما لم تقم بتغيير أرقام المنافذ. راجع <u>ASDM</u> <u>و WebVPN الذي تم تمكينه على نفس واجهة ASA</u> للحصول على مزيد من المعلومات.

أتمت هذا steps in order to شكلت ال SSL VPN على ASA مع انقسام tunneling:

1. أخترت تشكيل>وصول عن بعد VPN>شبكة (زبون) منفذ>عنوان إدارة>عنوان بركة>إضافة in order to خلقت

| 薩 Add IP Pool        |                |                |                    |            |
|----------------------|----------------|----------------|--------------------|------------|
|                      |                |                |                    |            |
| Name:                | vpnpool        |                |                    |            |
| Starting IP Address: | 192.168.10.1   |                |                    |            |
| Ending IP Address:   | 192.168.10.254 | _              |                    |            |
| Subnet Mask:         | 255.255.255.0  | •              |                    |            |
|                      |                |                |                    |            |
| ок                   | Cancel         | Help           | ور برور کې VPNpool | ic.        |
|                      |                | <br>بىل مكافى: | لوان برقة CLI تشك  | حد<br>2. ط |

3. تمكين WebVPN.أخترت **تشكيل>وصول عن بعد VPN>شبكة (زبون) منفذ>SSL VPN توصيل وتحت منفذ** قارن، طقطقت ال **يسمح منفذ ويمكن DTLS** للقارن خارجي. تحقق أيضا من **تمكين وصول عميل** AnyConnect VPN **من Cisco أو وصول عميل SSL VPN القديم على الواجهة المحددة في** خانة الاختيار **الجدول أدناه** لتمكين SSL VPN على الواجهة الخارجية.

Configuration > Remote Access VPN > Network (Client) Access > SSL VPN Connection Profiles

The security appliance automatically deploys the Cisco AnyConnect VPN Client or legacy SSL VPN Client to client deployment requires end-user administrative rights. The Cisco AnyConnect VPN Client supports the Layer Security (DTLS) tunneling options.

(More client-related parameters, such as client images and client profiles, can be found at <u>Client Settings</u>

| Acces | ss Interfaces -         |                           |                                      |                           |
|-------|-------------------------|---------------------------|--------------------------------------|---------------------------|
|       | Enable Cisco Any        | Connect VPN Client or la  | egacy SSL VPN Client access on the i | nterfaces selected in the |
|       | Interface               | Allow Access              | Require Client Certificate           | Enable DTLS               |
| out   | side                    |                           |                                      |                           |
| insi  | de                      |                           |                                      |                           |
|       |                         |                           |                                      |                           |
|       |                         |                           |                                      |                           |
|       |                         | _                         |                                      |                           |
| Acc   | ess Port: 443           | DTLS Port:                | 443                                  |                           |
| Clic  | k here to <u>Assign</u> | Certificate to Interface. |                                      |                           |

طقطقة **يطبق**.أختر Configuration > Remote Access VPN (التكوين) > Network (العميل) Configuration (العميل) Cisco (الوصول إلى الشبكة) > Add in order to إعدادات العميل > Add in order to أضفت ال Cisco من ذاكرة الماكرة المؤقتة) ل ASA كما هو

| ៅ Add SSL VPN Client Image | ×            | SSL VPN > Client Settings                   |
|----------------------------|--------------|---|
| Flash SVC Image:           | Browse Flash |   |
|                            | Upload       | puntered operation system to the top of the |
| OK Cancel                  | Help         |   |
| 薩 Browse Flash             |              | ×   |

#### 付 Browse Flash

| Folders               | Files                         |                  |                   |
|-----------------------|-------------------------------|------------------|-------------------|
| 🖃 🥏 disk0:            | FileName 🔬                    | Size (bytes)     | Date Modified     |
| 🗄 🛄 log               | crypto_archive                |                  | 07/24/07 05:21:48 |
| 🕀 🔁 crypto_archive    | 🗀 log                         |                  | 07/24/07 05:21:36 |
|                       | asdm-603.bin                  | 6,851,212        | 01/04/08 18:07:02 |
|                       | asa803-k8.bin                 | 14,635,008       | 01/04/08 17:49:50 |
|                       | admin.cfg                     | 1,220            | 09/20/07 09:51:38 |
|                       | anyconnect-win-2.0.03         | 2,635,734        | 08/13/07 04:14:50 |
|                       | asdm-602.bin                  | 6,889,764        | 01/03/08 21:38:26 |
|                       | asa722-k8.bin                 | 8,312,832        | 02/13/07 04:16:30 |
|                       | asdm-522.bin                  | 5,623,108        | 02/12/07 05:53:48 |
|                       | asa802-k8.bin                 | 14,524,416       | 01/03/08 21:24:42 |
|                       | old_running.cfg               | 1,841            | 09/20/07 09:51:38 |
|                       | sslclient-win-1.1.4.179       | 418,765          | 03/14/08 13:47:58 |
|                       |                               |                  |                   |
| File Name             | anyconnect-win-2.0.0343-k9.pl | kg               |                   |
| 🔂 Add                 | SSL VPN Client Image          |                  | 2                 |
| Flash S               | VC Image: ct-win-2.0.0343-ks  | 9.pkg Browse Fla | ash               |
|                       |                               | Upload           |                   |
|                       | OK Cancel                     | Help             |                   |
| انقر فوق <b>إضافة</b> |                               |                  | وانقر فوق OK.     |
|                       |                               |                  | Add).)            |

### 

اLL تشكيل مكافئ:

31. • 11

4. تكوين نهج المجموعة.أخترت **تشكيل>وصول عن بعد VPN>شبكة (زبون) منفذ>مجموعة نهج** in order to خلقت داخلي مجموعة **زبون** سياسة مجموعة. تحت علامة التبويب **عام**، حدد خانة الاختيار SSL VPN Client لتمكين WebVPN كبروتوكول

| I | Add Internal Group Policy | نفق.   |
|---|---------------------------|--|
|   | Servers<br>               | Name:     clientgroup       Banner:     Inherit       Address Pools:     Inherit |
|   |                           | More Options   |
|   |                           | Tunneling Protocols: 🔲 Inherit 📄 Clientless SSL VPN 🔽 SSL VPN Client 📄 IPsec     |
|   |                           | 1  |

في علامة التبويب **خيارات متقدمة > تقسيم** الاتصال النفقي، قم بإلغاء تحديد خانة الاختيار **Inherit** لنهج النفق المقسم واختر **قائمة شبكة النفق أدناه** من القائمة

|          |   |  | المىسدىة.                              |
|----------|---|--|--|
| <b>F</b> | Add Internal Group Policy   |  | ×                                      |
|          | General<br>Servers<br>Advanced<br>E-Advanced<br>E Browser Proxy<br>E-SSL VPN Client | Split tunneling network lists distinguish networks that require traffic to go through the tunnel and i require tunneling. The security appliance makes split tunneling decisions on the basis of a network ACL that consists of list of addresses on the private network.  | those that do not<br>list, which is an |
|          | ⊞–IPsec Client  | Network List:  Inherit | Manage                                 |

قم بإلغاء تحديد خانة الاختيار Inherit لقائمة **شبكات النفق المقسم** ثم انقر فوق Manage لتشغيل إدارة قائمة التحكم في الوصول ( LCA)

| Edit Internal Group Policy            | y: hivalleyvpn  |
|---------------------------------------|---|
| General<br>Servers<br>Advanced        | Split tunneling network lists distinguish networks that require traffic to go through the tunnel and those that do not<br>require tunneling. The security appliance makes split tunneling decisions on the basis of a network list, which is an<br>ACL that consists of list of addresses on the private network. |
| IE Browser Proxy                      | DNS Names: 🔽 Inherit  |
| SSL VPN Client     IPsec Client       | Policy: 🗂 Inherit Tunnel Network List Below 💌   |
| Client Access Rule<br>Client Firewall | Network List: None  |
| Hardware Client                       |   |

ضمن إدارة قائمة التحكم في الوصول (ACL)، أختر **إضافة > قائمة التحكم في الوصول (ACL)**.. لإنشاء قائمة وصول -

| ACL Manager  |            |        |             |  |
|--|------------|--------|-------------|--|
| Standard ACL Extended  | ACL        |        |             |  |
| 🗣 Add 🕞 🗹 Edit   | Delete 🛧 🗲 | 3 B B  | *           |  |
|  |            |        |             |  |
| 🔂 Add ACL  | dress      | Action | Description |  |
| <ul> <li>Add ACL</li> <li>Add ACE</li> </ul>                 | dress      | Action | Description |  |
| <ul> <li>Add ACL</li> <li>Add ACE</li> <li>Insert</li> </ul> | dress      | Action | Description |  |

قم بتوفير اسم لقائمة التحكم بالوصول (ACL) وانقر فوق **موافق**.

| 🛓 ACL Manage | er               |        |        |   |             |  |
|--------------|------------------|--------|--------|---|-------------|--|
| Standard AC  | L Extended ACL   |        |        |   |             |  |
| 🔂 Add 👻      | 💣 Edit 📋 Dele    | te 🕈 🗲 | አ 🖻 🛍  | * |             |  |
| No           | Address          | s      | Action |   | Description |  |
| 🔂 Add A      | iL               |        |        | × |             |  |
| ACL Nan      | ne: split-tunnel |        |        |   |             |  |
|              |                  |        | 1      | 1 |             |  |

بمجرد إنشاء اسم قائمة التحكم في الوصول، أختر **إضافة > إضافة ACE** لإضافة إدخال التحكم في الوصول (ACE).عينت ال ACE أن يماثل ال LAN خلف ال ASA. في هذه الحالة، الشبكة هي 26/10.77.241.128 وحدد **السماح** كإجراء.انقر فوق **موافق** للخروج من إدارة قائمة التحكم في الوصول (ACL).

| No           | Address             | Action | C | escription |          |
|--------------|---------------------|--------|---|------------|----------|
| split-tunnel |                     |        |   |            |          |
| 付 Add ACE    |                     |        |   |            |          |
| -Action-     |                     |        |   |            |          |
| Action:      | 🖌 Permit 💽          |        |   |            |          |
| Host/Net     | work                |        |   |            |          |
| IP Addr      | ress: 10.77.241.128 |        |   |            | <b>.</b> |
| Netmas       | sk: 255.255.255.192 |        |   |            | •        |
| Description  | n:                  |        |   |            |          |
|              |                     |        |   |            |          |

تاكد من تحديد قائمة التحكم في الوصول (ACL) التي قمت بإنشائها للتو لقائمة شبكات النفق المنقسم. انقر فوق **موافق** للعودة إلى تكوين "نهج المحمومة"

|  |  |   |  | لمجموعه .                    |
|--|--|---|--|------------------------------|
| 💏 Add Internal Group Policy  |  |   |  | ×                            |
| General<br>Servers<br>Advanced<br>JE Browser Proxy<br>SSL VPN Client | Split tunneling<br>require tunne<br>ACL that cons<br>DNS Names:<br>Policy: | g network lists<br>ling. The sect<br>sists of list of<br>I Inherit<br>Inherit | s distinguish networks that require traffic to go through the tunnel and those<br>urity appliance makes split tunneling decisions on the basis of a network list,<br>addresses on the private network. | a that do not<br>which is an |
|  | Network List:  | 🔲 Inherit   | split-tunnel   | Manage                       |
|  | Intercept  | DHCP Confi  | guration Message from Micosoft Clients   | ۲                            |

على الصفحة الرئيسية، انقر فوق **تطبيق** ثم إرسال (إذا كان ذلك مطلوبا) لإرسال الأوامر إلى ASA.قم بتكوين إعدادات **SSL VPN** ضمن وضع نهج المجموعة.للحصول على خيار إبقاء المثبت على نظام العميل، قم بإلغاء تحديد خائة الاختيار **توريث**، وانقر فوق الزر **نعم** للانتقاء.يسمح هذا الإجراء لبرنامج SVC بالبقاء على جهاز العميل. لذلك، لا يتطلب ASA تنزيل برنامج SVC إلى العميل في كل مرة يتم فيها الاتصال. يعد هذا الخيار خيارا جيدا للمستخدمين البعيدين الذين غالبا ما يصلون إلى شبكة الشركة.

| esi 🖉 🔿 No       |
|------------------|
|                  |
| nable 🔿 Disat    |
| - Maria de Disad |
| nable (O Disat   |
| isable Totorvoli |
| issues Tricervan |
|                  |

انقر فوق **إعداد تسجيل الدخول** لتعيين **إعداد تسجيل الدخول إلى مادة النشر** و**تحديد تسجيل الدخول إلى مادة النشر الافتراضي** كما هو

|  | موضح.   |
|--|---|
| -General<br>-Servers                   | <ul> <li>After successfully logging in, user can have the choice to download the client software, or g<br/>portal page. The following settings decides what will happen.</li> </ul> |
|  | 🔲 Inherit   |
|  | Post Login Setting  |
|  | <ul> <li>Do not prompt user to choose</li> </ul>  |
| Key Regeneration<br>—Dead Peer Detecti | C Prompt user to choose   |
| Customization                          | User has seconds to choose, or Default Post Login Selection below is take   |
|  | Default Post Login Selection  |
|  | C Go to Clientless SSL VPN portal   |
|  | Download SSL VPN Client   |

لخيار الفاصل الزمني لإعادة التفاوض، قم بإلغاء تحديد خانة الاختيار Inherit، وإلغاء تحديد خانة الاختيار Unlimited، وأدخل عدد الدقائق حتى المفتاح.يتم تحسين الأمان عن طريق تعيين حدود على طول الوقت الذي يكون فيه المفتاح صالحا.لخيار طريقة إعادة التفاوض، قم بإلغاء تحديد خانة الاختيار Inherit، وانقر فوق زر انتقاء SSL.يمكن أن تستخدم إعادة التفاوض نفق SSL الحالي أو نفق جديد تم إنشاؤه صراحة لإعادة التفاوض.

| Coporal            | Descentistics Tatawish  | The baselike | 🖂 i taliasika di |           |                      |
|--------------------|-------------------------|--------------|------------------|-----------|----------------------|
| General            | Renegotiation Interval: |              | j Uniimited      | 30        | minutes              |
| Servers            |                         |              | ~                | · · · · · |                      |
| 🖻 – Advanced       | Renegotiation Method:   | Inherit      |                  | © SSL     |                      |
| -Split Tunneling   |                         |              |                  |           |                      |
| IE Browser Proxy   |                         |              |                  |           |                      |
| 🖨 – SSL VPN Client |                         |              |                  |           |                      |
| Login Setting      |                         |              |                  |           |                      |
| Key Regeneration   | )                       |              |                  |           |                      |
|                    |                         |              |                  | ذاك       | مقطقت <b>مد</b> ويعد |

يطبق. Configuration > Remote Access VPN > Network (Client) Access > Group Policies Manage VPN group policies. A VPN group policy is a collection of user-oriented attribute/value pairs that may be stored inter externally on a RADIUS/LDAP server. The group policy information is referenced by VPN tunnel groups and user accounts. 📝 Edit 🔂 Add 前 Delete **Tunneling Protocol** Name Type clientgroup Internal svo -- N/A -DfltGrpPolicy (System Default) Internal -- N/A -L2TP-IPSec, IPSec, webvpn

اLL تشكيل مكافئ:

5. أخترت **تشكّيل>Remote Access VPN عن بعد>AAA setupمحلي مستعمل>يضيف** in order to خلقت جديد مستعمل حساب ssluser1. طقطقت ok وبعد ذلك

| Add User Assount         | بطبق.   |
|--------------------------|---|
| Add OSEF Account         |   |
| Identity<br>⊕-VPN Policy | Username: ssluser1  |
|                          | Password: ******  |
|                          | Confirm Password: ******  |
|                          | User authenticated using MSCHAP   |
|                          | Member-of   |
|                          | Member-of: Add >> Delete  |
|                          | Access Restriction  |
|                          | Select one of the options below to restrict ASDM, SSH, Telnet and Console access. |
|                          | Note: All users have network access, regardless of these settings.                |
|                          | Full access(ASDM, SSH, Telnet and Console)  |
|                          | Privilege level is used with command authorization.                               |
|                          | Privilege Level: 2  |
|                          | CLI login prompt for SSH, Telnet and console (no ASDM access)                     |
|                          | This setting is effective only if AAA authenticate console command is configured. |
|                          | No ASDM, SSH, Telnet or Console access  |
|                          | This setting is effective only if AAA authenticate console command is configured. |
|                          | CL تشكيل مكافئ:   |

in (الحترت **تشكيل) AAA بعداد > AAA (الوصول عن بعد) > AAA بعداد > AAA نادل مجموعة > تحرير** AAa (الخترت **تشكيل)** order to عدلت التقصير نادل مجموعة محلي ب يفحص ال enable محلي تأمين المستخدم مع أقصى قيمة محاولات ك 16.

#### **AAA Server Groups**

|  | Ser   | ver Group                                       | Protocol  | Accounting Mode   | Reactivation Mode                                     |   |  |
|--|-------|---|---|---|---|---|--|
|  | LOCAL |   | LOCAL   |   |   |   |  |
|  |       | 🔂 Edit LOCA                                     | L Server Group  |   | X   | 1 |  |
|  |       | This feature<br>before locking<br>when the lock | allows you to speci<br>g out and denying a<br>al database is used | fy the maximum number o<br>access to the user. This li<br>I for authentication. | of failed attempts to allow<br>mit is applicable only |   |  |
| Enable Local User Lockout     Maximum Attempts: 16 |       |   |   |   |   |   |  |
|  | •     |   | ОК  | Cancel  | Help  |   |  |

- 7. طقطقت ok وبعد ذلك يطبق.CLI تشكيل مكافئ:
- 8. تكوين مجموعة النفق.أخترت **تشكيل>SSL VPN>شبكة (زبون) منفذ>SSL VPN توصيل توصيفات>إضافة** in order to خلقت جديد نفق مجموعة ssigroup.في علامة التبويب **أساسي**، يمكنك تنفيذ قائمة التكوينات كما هو موضح:قم بتسمية مجموعة النفق باسم SSLGROUP.أخترت تحت عنوان تعيين، العنوان بركة vpnPool من القائمة المنسدلة.ضمن "نهج المجموعة الافتراضي"، أختر **مجموعة عملاء** نهج المجموعة من القائمة

|   |                        |                         |                                 | المنسدلة. |
|---|------------------------|-------------------------|---------------------------------|-----------|
| ٥ | Add SSL VPN Connection | Profile                 |                                 |           |
|   | Basic                  | Name:                   | sslgroup                        |           |
|   | E→Advanced             | Aliases:                |                                 |           |
|   |                        | Authentication ——       |                                 |           |
|   |                        | Method:                 | AAA C Certificate C Both        |           |
|   |                        | AAA Server Group:       | LOCAL                           | Manag     |
|   |                        |                         | Use LOCAL if Server Group fails |           |
|   |                        | Client Address Assign   | nent                            |           |
|   |                        | DHCP Servers:           |                                 |           |
|   |                        | Client Address Pools:   | vpnpool                         | Select    |
|   |                        | Default Group Policy    |                                 |           |
|   |                        | Group Policy:           | clientgroup                     | Manag     |
|   |                        | SSL VPN Client Protocol | Enabled                         |           |
|   |                        |                         | - Count - Units - 1             |           |
|   |                        | OK                      | Cancel Help                     |           |

تحت علامة التبويب SSL VPN > **أسماء** مستعارة **الاتصال،** حدد اسم اسم المجموعة المستعار على هيئة sslgroup\_users وانقر على

| Basic Advanced General Client Addressing Authentication Accounting SSL VPN Connection Aliases Alias: [sslgroup_users ] Connection Alias Alias: [sslgroup_users] Connection Alias Alias: [sslgroup_users] Connection Alias Alias: [sslgroup_users] Connection Alias Co | Add SSL VPN Connection  | Profile   |
|--|---|---|
| Add Connection Alias     Alias:   sslgroup_users   ✓ Enabled     OK   Cancel     Help  | Basic<br>Advanced<br>General<br>Client Addressing<br>Authentication<br>Authorization<br>Accounting<br>SSL VPN | Portal Page Customization: DfltCustomization<br>CSD Alternate Group Policy: DfltGrpPolicy<br>Enable the display of Radius Reject-Message on the<br>Connection Aliases |
| G OK Cancel Help   |   | Add      Delete      Add Connection Alias      Alias: sslgroup_users  |
|  |   |   |

outside

مترجع قت ok وبعد ذلك **يطبق.CLI تشكيل مكافئ:** 9. تكوين NAT.أخترت **تشكيل>جدار حماية>nat قاعدة>إضافة حركي nat قاعدة** لذلك الحركة مرور أن يأتي من الشبكة الداخلية يستطيع كنت ترجمت مع خارج عنوان 5 1 1 172 172

|   |           |                       |                        |             |                                     | .172.10.           | 1.5       |
|---|-----------|-----------------------|------------------------|-------------|-------------------------------------|--------------------|-----------|
|   | B         | 🔄 Add Dynamic         | NAT Rule               |             |                                     |                    |           |
|   |           | Original              |                        |             |                                     |                    |           |
|   |           |                       | <u></u>                |             |                                     |                    |           |
|   |           | Interface: insid      | de                     |             | <b>T</b>                            |                    |           |
|   |           | Source: any           | J                      |             |                                     |                    |           |
|   |           | Translated —          |                        |             |                                     |                    |           |
|   |           | Select a global p     | bool for dynamic trans | lation.     |                                     |                    |           |
|   |           | Pool ID               | Interfac               | e           | Addresses Pool                      |                    |           |
|   |           | 0                     | (outbound)             | 9           | Same as original address (identity) |                    |           |
|   |           | -0                    | (inbound)              |             | <del>Jame as origin</del> a         | address (identity  | )         |
|   | مانقر     | 1                     | outside                | 1           | 🖳 172.16.1.5                        | ļ                  |           |
|   | والعر     |                       |                        |             |                                     | ∪ OK.وانقر فوق     | فوق<br>OK |
| ¢ | Configura | ation > Firewall > NA | AT Rules               |             |                                     |                    | C         |
|   | 💠 Add     | 🝷 📝 Edit 📋 De         | lete 🗲 🗲 👗             | 🖻 🛍 - 🛛 🗸   | 🔍 Find  🚌 Diad                      | gram 🛛 🟹 Packet Tr | ace       |
|   |           | Tupo                  |                        | Original    |                                     |                    |           |
|   | *         | # Type Source De      |                        | Destination | Service                             | Interface          |           |

1

 $\boxdot$  inside (1 Dynamic rules) 📊 Dynamic

🏈 any

#### طقطقة **يطبق CLI تشكيل مكافئ:**

قم بتكوين إعفاء nat لحركة مرور البيانات العائدة من الشبكة الداخلية إلى عميل VPN. ciscoasa(config)#access-list nonat permit ip 10.77.241.0 192.168.10.0 ciscoasa(config)#access-list nonat permit ip 192.168.10.0 10.77.241.0 ciscoasa(config)#nat (inside) 0 access-list nonat

#### <u>تکوین ASA CLI</u>

```
(Cisco ASA 8.0(2
                    ciscoasa(config)#show running-config
                                                  Saved :
                                       (ASA Version 8.0(2
                                                        1
                                       hostname ciscoasa
                      domain-name default.domain.invalid
              enable password 8Ry2YjIyt7RRXU24 encrypted
                                                    names
                                                        !
                                    interface Ethernet0/0
                                           nameif inside
                                      security-level 100
               ip address 10.77.241.142 255.255.255.192
                                                        !
                                   interface Ethernet0/1
                                          nameif outside
                                       security-level 0
                    ip address 172.16.1.1 255.255.255.0
                                                        !
                                   interface Ethernet0/2
                                                shutdown
                                               no nameif
                                      no security-level
                                           no ip address
                                                        1
                                   interface Ethernet0/3
                                                shutdown
                                               no nameif
                                      no security-level
                                          no ip address
                                                        !
                                 interface Management0/0
                                                shutdown
                                               no nameif
                                      no security-level
                                           no ip address
                                                        1
                       passwd 2KFQnbNIdI.2KYOU encrypted
                        boot system disk0:/asa802-k8.bin
                                         ftp mode passive
                                 clock timezone IST 5 30
                             dns server-group DefaultDNS
                     domain-name default.domain.invalid
 access-list split-tunnel standard permit 10.77.241.128
                                          255.255.255.192
 ACL for Split Tunnel network list for encryption. ---!
    access-list nonat permit ip 10.77.241.0 192.168.10.0
access-list nonat permit ip 192.168.10.0 10.77.241.0 !--
    - ACL to define the traffic to be exempted from NAT.
```

pager lines 24 logging enable logging asdm informational mtu inside 1500 mtu outside 1500 ip local pool vpnpool 192.168.10.1-192.168.10.254 mask 255.255.255.0 The address pool for the Cisco AnyConnect SSL VPN ---! Clients no failover icmp unreachable rate-limit 1 burstsize 1 asdm image disk0:/asdm-602.bin no asdm history enable arp timeout 14400 global (outside) 1 172.16.1.5 The global address for Internet access used by VPN ---! Clients. !--- Note: Uses an RFC 1918 range for lab setup. !--- Apply an address from your public range provided by your ISP. nat (inside) 0 access-list nonat The traffic permitted in "nonat" ACL is exempted ---! from NAT. nat (inside) 1 0.0.0.0 0.0.0.0 route outside 0.0.0.0 0.0.0.0 172.16.1.2 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 mgcp-pat 0:05:00 timeout sip 0:30:00 sip\_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00 timeout uauth 0:05:00 absolute dynamic-access-policy-record DfltAccessPolicy http server enable http 0.0.0.0 0.0.0.0 inside no snmp-server location no snmp-server contact snmp-server enable traps snmp authentication linkup linkdown coldstart no crypto isakmp nat-traversal telnet timeout 5 ssh timeout 5 console timeout 0 threat-detection basic-threat threat-detection statistics access-list ! class-map inspection\_default match default-inspection-traffic ! 1 policy-map type inspect dns preset\_dns\_map parameters message-length maximum 512 policy-map global\_policy class inspection\_default inspect dns preset\_dns\_map 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   |
| enable outside   |
| Enable WebVPN on the outside interface <b>svc image</b> !  |
| disk0:/anyconnect-win-2.0.0343-k9.pkg 1  |
| Assign an order to the AnyConnect SSL VPN Client!<br>image <b>svc enable</b>   |
| Enable the security appliance to download SVC!<br>images to remote computers tunnel-group-list enable  |
| Enable the display of the tunnel-group list on the!<br>WebVPN Login page group-policy clientgroup internal   |
| Create an internal group policy "clientgroup"!<br>group-policy clientgroup attributes<br>vpn-tunnel-protocol svc   |
| Specify SSL as a permitted VPN tunneling protocol!<br>split-tunnel-policy tunnelspecified<br>split-tunnel-network-list value split-tunnel  |
| Encrypt the traffic specified in the split tunnel!<br>ACL only <b>webvpn</b>   |
| svc keep-installer installed   |
| When the security appliance and the SVC perform a!<br>rekey, they renegotiate ! the crypto keys and<br>initialization vectors, increasing the security of the<br>connection. svc rekey time 30 |
| Command that specifies the number of minutes from!<br>the start of the ! session until the rekey takes<br>place, from 1 to 10080 (1 week). <b>svc rekey method ssl</b>                         |
| Command that specifies that SSL renegotiation takes!<br>place during SVC rekey. <b>svc ask none default svc</b>  |
| username ssluser1 password ZRhW85jZqEaVd5P. encrypted  |
| Create a user account "ssluser1" tunnel-group!<br>sslgroup type remote-access  |
| Create a tunnel group "sslgroup" with type as!<br>remote access tunnel-group sslgroup general-attributes<br>address-pool vpnpool   |
| Associate the address pool vpnpool created default!<br>group-policy clientgroup  |
| Associate the group policy "clientgroup" created!  |
| tunnel-group sslgroup webvpn-attributes<br>group-alias sslgroup users enable   |
| Configure the group alias as sslgroup-users prompt   |
| hostname context   |
| Cryptochecksum:af3c4bfc4ffc07414c4dfbd29c5262a9 : end<br>#(ciscoasa(config   |

### إنشاء اتصال SSL VPN باستخدام SVC

أتمت هذا steps in order to خلقت SSL VPN توصيل مع ASA:

1. أدخل عنوان URL أو عنوان IP الخاص بواجهة WebVPN الخاصة ب ASA في مستعرض الويب لديك بالتنسيق كما هو موضح.

|  | nttps://uri   |
|--|---|
| <https: <ip<="" th=""><th>او<br/>address of the ASA WebVPN interface</th></https:> | او<br>address of the ASA WebVPN interface                             |
| WebVPN Service - Microsoft Internet Explorer                                       |   |
| File Edit View Favorites Tools Help  |   |
| 🚱 Back 🔹 🕥 - 💽 🛃 🚮 🔎 Search 🤸 Favo   | nites 🚱 🔗 🍓 🔜 🖓   |
| Address Address https://172.16.1.1/+webvpn+/index.html                             |   |
| CISCO SYSTEMS<br>  |   |
|  | Login   |
| Please enter your user   | rname and password  |
|  | name and password.  |
| OSERNAME.  |   |
| PASSWORD:  |   |
| GROUP: sslgr   | oup_users   |
| Lo   | gin Clear   |
| . بك أختر أيضا مجموعتك المقابلة من القائمة المنسدلة كما هو                         | ً<br>أدخا إسم المستخدم وكلمة المرور الخاصي:                           |
| Login  |   |
| Please enter your username a   | and password  |
|  | na passilora.   |
| USERNAME: ssluser1   |   |
| PASSWORD:  |   |
| GROUP: sslgroup_user   | rs 💌  |
| Login  | Clear   |
| ايطهر هدا ناقده  | موضح.<br>قيار أن ال SSL VPN أنشئت                                     |
|  | ىچى اى بى بى بى يە <u>ب</u> ى يە يە يە <u>ب</u> ە يە يە يەت<br>توصيل. |

| Cisco  | AnyConnect VPN Client                        |
|--|--|
| <ul> <li>✓ VPN Client Download</li> <li>✓ Please w</li> <li>✓ -</li> <li>✓ -</li> <li>✓ -</li> </ul> | ait while the VPN connection is established. |
| <ul> <li>Microsoft Java</li> <li>Sun Java</li> <li>Download</li> </ul>                               |  |
| Connected  | Help Cancel                                  |

**لاحظة:** يجب تثبيت برنامج ActiveX في الكمبيوتر قبل تنزيل SVC.تتلقى هذا الإطار بمجرد تأسيس الاتصال.



<sup>3.</sup> انقر فوق القفل الذي يظهر في شريط المهام







## التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

تدعم <u>أداة مترجم الإخراج (للعملاءالمسجلين فقط) بعض أوامر</u> show. استخدم أداة مترجم الإخراج (OIT) لعرض تحليل مُخرَج الأمر show .

```
show webVPN svc يعرض صور SVC المخزنة في ذاكرة ASA المؤقتة.
دiscoasa#show webvpn svc
disk0:/anyconnect-win-2.0.0343-k9.pkg 1 .1
+CISCO STC win2k
2,0,0343
Mon 04/23/2007 4:16:34.63
```

- SSL VPN Client(s) installed 1
- show vpn-sessiondb svc يعرض المعلومات حول إتصالات SSL الحالية. ciscoasa#show vpn-sessiondb svc

Session Type: SVC

Index : 12

Assigned IP : **192.168.10.1** Public IP : 192.168.1.1 Protocol : Clientless SSL-Tunnel DTLS-Tunnel Encryption : RC4 AES128 Hashing : SHA1 Bytes Tx : 194118 Bytes Rx : 197448 Group Policy : clientgroup Tunnel Group : **sslgroup** Login Time : 17:12:23 IST Mon Mar 24 2008 Duration : 0h:12m:00s NAC Result : Unknown VLAN Mapping : N/A VLAN : none show webVPN group-alias—يعرض الاسم المستعار الذي تم تكوينه لمجموعات مختلفة. ciscoasa#show webvpn group-alias Tunnel Group: sslgroup Group Alias: sslgroup\_users enabled

• في ASDM، أخترت **monitore>VPN>VPN إحصاء>جلسة** in order to عرفت الحالي WebVPN جلسة في ال ASA.

| Monitoring > VP                         | N > VPN S | tatistio           | s > Sessions | )                             |              |                                |                   |                  |
|---|-----------|--------------------|--------------|-------------------------------|--------------|--------------------------------|-------------------|------------------|
| Sessions                                |           |                    |              |                               |              |                                |                   |                  |
| Remote                                  | Remote    |                    | SSL VPN      |                               | E-mail Prove | VDN Load Palancin              | ~ [ ,             |                  |
| Access                                  | Sile-lu-  | Sice               | Clientless   | With Client                   | Total        | E-mail Proxy                   | VPN LUGU Dalahuli | 'y               |
| 0                                       | 0         |                    | 0            | 0                             | 0            | 0                              | 0                 |                  |
| Filter By: SSL VPN Client               |           |                    |              |                               | Fi           | ter                            |                   |                  |
| Username Group Policy Protocol          |           |                    |              | Logi                          | in Time      | Byt                            |                   |                  |
| IP Address Connection                   |           |                    | Encryp       | Encryption                    |              | ration                         | Byt               |                  |
| ssluser1 cliento<br>192.168.10.1 sslgro |           | clientg<br>sslgrou | roup<br>Ip   | Clientless SSL-<br>RC4 AES128 | Tunnel DT    | 17:12:23 IST Mor<br>0h:03m:31s | Mar 24 2008       | 194118<br>192474 |

### استكشاف الأخطاء وإصلاحها

ι.

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

1. VPN-sessiondb logoff name *<username – أ*مر أن يدون ال SSL VPN – أمر أن يدون ال

| حاص.   |
|--|
| ciscoasa# <b>vpn-sessiondb logoff name ssluser1</b>          |
| Do you want to logoff the VPN session(s)? [confirm] ${f Y}$  |
| INFO: Number of sessions with name "ssluser1" logged off : 1 |
| !ciscoasa#Called vpn_remove_uauth: success                   |
| webvpn_svc_np_tear_down: no ACL                              |
| webvpn_svc_np_tear_down: no IPv6 ACL                         |
| (np_svc_destroy_session(0xB000                               |
|  |
|  |

بالمثل، يمكنك إستخدام الأمر v**pn-sessiondb logoff svc** لإنهاء جميع جلسات عمل SVC. 2. **ملاحظة:** إذا انتقل الكمبيوتر إلى وضع الاستعداد أو الإسبات، يمكن إنهاء اتصال SSL VPN.

```
webvpn_rx_data_cstp
webvpn_rx_data_cstp: got message
SVC message: t/s=5/16: Client PC is going into suspend mode (Sleep, Hibernate, e
(tc
!Called vpn_remove_uauth: success
webvpn_svc_np_tear_down: no ACL
webvpn_svc_np_tear_down: no IPv6 ACL
(np_svc_destroy_session(0xA000
```

ciscoasa#**show vpn-sessiondb svc** INFO: There are presently no active sessions

3. WebVPN svc **<1-255 debug webVPN svc ي**وفر أحداث WebVPN في الوقت الفعلي لإنشاء الجلسة.

Ciscoasa#debug webvpn svc 7

```
webvpn_rx_data_tunnel_connect
                                                  CSTP state = HEADER_PROCESSING
                                                        ()http_parse_cstp_method
                                   'input: 'CONNECT /CSCOSSLC/tunnel HTTP/1.1...
                                               ()webvpn_cstp_parse_request_field
                                                     'input: 'Host: 172.16.1.1...
                                 'Processing CSTP header line: 'Host: 172.16.1.1
                                                ()webvpn_cstp_parse_request_field
                  'input: 'User-Agent: Cisco AnyConnect VPN Client 2, 0, 0343...
Processing CSTP header line: 'User-Agent: Cisco AnyConnect VPN Client 2, 0, 0343
                 'Setting user-agent to: 'Cisco AnyConnect VPN Client 2, 0, 0343
                                                ()webvpn_cstp_parse_request_field
input: 'Cookie: webvpn=16885952@12288@1206098825@D251883E8625B92C1338D631B08B...
                                                                    '7D75F4EDEF26
Processing CSTP header line: 'Cookie: webvpn=16885952@12288@1206098825@D251883E8
                                                 '625B92C1338D631B08B7D75F4EDEF26
Found WebVPN cookie: 'webvpn=16885952@12288@1206098825@D251883E8625B92C1338D631B
                                                                 '08B7D75F4EDEF26
WebVPN Cookie: 'webvpn=16885952@12288@1206098825@D251883E8625B92C1338D631B08B7D7
                                                                       '5F4EDEF26
                                               ()webvpn_cstp_parse_request_field
                                                    'input: 'X-CSTP-Version: 1...
                                'Processing CSTP header line: 'X-CSTP-Version: 1
                                                           'Setting version to '1
                                               ()webvpn_cstp_parse_request_field
                                              'input: 'X-CSTP-Hostname: tacweb...
                          'Processing CSTP header line: 'X-CSTP-Hostname: tacweb
                                                    'Setting hostname to: 'tacweb
                                                ()webvpn_cstp_parse_request_field
                               'input: 'X-CSTP-Accept-Encoding: deflate;q=1.0...
            'Processing CSTP header line: 'X-CSTP-Accept-Encoding: deflate;q=1.0
                                               ()webvpn_cstp_parse_request_field
                                                     'input: 'X-CSTP-MTU: 1206...
                                 'Processing CSTP header line: 'X-CSTP-MTU: 1206
                                                ()webvpn_cstp_parse_request_field
                                            'input: 'X-CSTP-Address-Type: IPv4...
                        'Processing CSTP header line: 'X-CSTP-Address-Type: IPv4
                                               ()webvpn_cstp_parse_request_field
input: 'X-DTLS-Master-Secret: CE151BA2107437EDE5EC4F5EE6AEBAC12031550B1812D40...
                               '642E22C6AFCB9501758FF3B7B5545973C06F6393C92E59693
Processing CSTP header line: 'X-DTLS-Master-Secret: CE151BA2107437EDE5EC4F5EE6AE
           'BAC12031550B1812D40642E22C6AFCB9501758FF3B7B5545973C06F6393C92E59693
                                                ()webvpn_cstp_parse_request_field
  'input: 'X-DTLS-CipherSuite: AES256-SHA:AES128-SHA:DES-CBC3-SHA:DES-CBC-SHA...
Processing CSTP header line: 'X-DTLS-CipherSuite: AES256-SHA:AES128-SHA:DES-CBC3
                                                                'SHA:DES-CBC-SHA-
                                                     Validating address: 0.0.0.0
                                                   CSTP state = WAIT_FOR_ADDRESS
                                webvpn_cstp_accept_address: 192.168.10.1/0.0.0.0
                                                       CSTP state = HAVE ADDRESS
                                              No subnetmask... must calculate it
                                                                    SVC: NP setup
                                 (np_svc_create_session(0x3000, 0xD41611E8, TRUE
                                                              webvpn_svc_np_setup
                                                               SVC ACL Name: NULL
```

SVC ACL ID: -1 SVC ACL ID: -1 !vpn\_put\_uauth success SVC IPv6 ACL Name: NULL SVC IPv6 ACL ID: -1 SVC: adding to sessmgmt SVC: sending response Unable to initiate NAC, NAC might not be enabled or invalid policy CSTP state = CONNECTED webvpn\_rx\_data\_cstp uebvpn\_rx\_data\_cstp: got internal message Unable to initiate NAC, NAC might not be enabled or invalid policy

4. في ASDM، أختر **مراقبة > تسجيل > عارض السجل في الوقت الفعلي > عرض** لعرض الأحداث في الوقت الفعلي ..

| G Cisco ASDM 6.0 for ASA - 10.77.241.142 |  |  |                      |  |  |  |  |  |  |  |
|--|--|--|----------------------|--|--|--|--|--|--|--|
| File                                     | <u>V</u> iew <u>T</u> ools Wi <u>z</u> ards <u>W</u> indow <u>H</u> e        | þ  | Look For:            |  |  |  |  |  |  |  |
|  | 😽 Home 🦓 Configuration 🔯 Monitoring 🔚 Save 🔇 Refresh 🔇 Back 🔘 Forward 🤗 Help |  |                      |  |  |  |  |  |  |  |
| Ţ  | Logging 🗗 🕂 🕹  | Monitoring > Logging > Real-Time Log Viewer  |                      |  |  |  |  |  |  |  |
| evice Lis                                | Real-Time Log Viewer   | Real-Time Log Viewer   |                      |  |  |  |  |  |  |  |
|  |  | Click the View button below to start displaying syslog messages in re<br>desired logging level to see messages at that severity or higher. | eal time. Select the |  |  |  |  |  |  |  |
|  |  | Logging Level: Debugging   |                      |  |  |  |  |  |  |  |
|  |  | Buffer Limit: 1000   |                      |  |  |  |  |  |  |  |
|  |  |  |                      |  |  |  |  |  |  |  |
|  |  | View   |                      |  |  |  |  |  |  |  |

يوضح هذا المثال أنه تم إنشاء جلسة عمل SSL باستخدام جهاز الطرف

| الرئيسي.<br>التا الحالي المالي ا |             |          |           |              |                |   |  |  |  |
|---|-------------|----------|-----------|--------------|----------------|---|--|--|--|
| Ele Tools Window Help   |             |          |           |              |                |   |  |  |  |
| 💷 Pause   🛍 Copy 🎧 Save 🖓 Clear   📓 Color Settings   🜓 Create Rule 🛃 Show Rule   🔞 Show Details   🤌 Help                    |             |          |           |              |                |   |  |  |  |
| Filter By: Filter 🗐 Show All Find:  |             |          |           |              |                |   |  |  |  |
| Severity  | Date        | Time     | Syslog ID | Source IP    | Destination IP |   |  |  |  |
| <u>4</u> 6  | Mar 21 2008 | 20:03:36 | 725007    | 10.77.233.74 |                | SSL session with client inside:10.77.233.74/1026 terminated.              |  |  |  |
| A 6   | Mar 21 2008 | 20:03:35 | 106015    | 10.77.233.74 | 10.77.241.142  | Deny TCP (no connection) from 10.77.233.74/1026 to 10.77.241.142/44:      |  |  |  |
| <u>4</u> 6  | Mar 21 2008 | 20:03:35 | 302014    | 10.77.233.74 | 10.77.241.142  | Teardown TCP connection 700 for inside:10.77.233.74/1026 to NP Identit    |  |  |  |
| <u>4</u> 6  | Mar 21 2008 | 20:03:35 | 605005    | 0.0.0.0      | 0.0.0.0        | Login permitted from 0.0.0.0/1026 to inside:0.0.0.0/https for user "enabl |  |  |  |
| <u>A</u> 6  | Mar 21 2008 | 20:03:35 | 725002    | 10.77.233.74 |                | Device completed SSL handshake with dient inside:10.77.233.74/1026        |  |  |  |
| <u>4</u> 6  | Mar 21 2008 | 20:03:35 | 725003    | 10.77.233.74 |                | SSL client inside:10.77.233.74/1026 request to resume previous session.   |  |  |  |
| A 6   | Mar 21 2008 | 20:03:35 | 725001    | 10.77.233.74 |                | Starting SSL handshake with client inside: 10.77.233.74/1026 for TLSv1 se |  |  |  |
| <u>4</u> 6  | Mar 21 2008 | 20:03:35 | 302013    | 10.77.233.74 | 10.77.241.142  | Built inbound TCP connection 700 for inside:10.77.233.74/1026 (10.77.23   |  |  |  |
|   |             |          |           |              |                |   |  |  |  |
| %ASA-6-725002 Device completed SSL handshake with remote_device-interface_name:IP_address/port                              |             |          |           |              |                |   |  |  |  |
| The SSL handshake has completed successfully with the remote device.  |             |          |           |              |                |   |  |  |  |

معلومات ذات صلة

- <u>صفحة دعم جهاز الأمان القابل للتكيف طراز Series 5500 من Cisco</u>
  - <u>ملاحظات الإصدار الخاصة بعميل AnyConnect VPN، الإصدار 2.0</u>
- ASA/PIX: السماح بنفقي انقسام لعملاء VPN على مثال تكوين ASA
- يسمح الموجه لعمّلاء VPN بتوصيل IPsec والإنترنت باستخدام مثال تكوين انقسام الاتصال النفقي
  - <u>عميل PIX/ASA 7.x و VPN لشبكة VPN العامة عبر الإنترنت على مثال تكوين العصا</u>
    - <u>SSL VPN Client (SVC) على ASA مع مثال تكوين ASDM</u>
      - <u>الدعم التقني والمستندات Cisco Systems</u>

ةمجرتاا مذه لوح

تمجرت Cisco تايان تايانق تال نم قعومجم مادختساب دنتسمل اذه Cisco تمجرت ملاعل العامي عيمج يف نيم دختسمل لمعد يوتحم ميدقت لقيرشبل و امك ققيقد نوكت نل قيل قمجرت لضفاً نأ قظعالم يجرُي .قصاخل امهتغلب Cisco ياخت .فرتحم مجرتم اممدقي يتل القيفارت عال قمجرت اعم ل احل اوه يل إ أم اد عوجرل اب يصوُتو تامجرت الاذة ققد نع اهتي لوئسم Systems الما يا إ أم الا عنه يل الان الانتيام الال الانتيال الانت الما