ASA 8.X: تكوين ميزة AnyConnect Start قبل تسجيل الدخول

المحتويات

المقدمة

مع تمكين SBL (*Start Before Logon*)، يظهر للمستخدم مربع حوار تسجيل الدخول إلى واجهة المستخدم الرسومية (GUI) ل AnyConnect قبل أن يظهر مربع حوار تسجيل الدخول إلى Windows®. وهذا يؤسس اتصال VPN أولا. يسمح Start Before Login للمسؤول، والمتوفر فقط للأنظمة الأساسية ل Windows، بالتحكم في إستخدام البرامج النصية لتسجيل الدخول وذاكرة التخزين المؤقت لكلمة المرور وتخطيط محركات أقراص الشبكة لمحركات الأقراص المحلية وغير ذلك. يمكنك إستخدام ميزة SBL لتنشيط شبكة VPN كجزء من تسلسل تسجيل الدخول. تم تعطيل SBL بشكل افتراضي.

للحصول على مزيد من المعلومات حول تكوين ميزات عميل AnyConnect VPN، ارجع إلى القسم تكوين ميزات عميل AnyConnect.

ملاحظة: ضمن عميل AnyConnect، يكون التكوين الوحيد الذي تقوم به ل SBL هو تمكين الميزة. يتعامل مسؤولو الشبكة مع المعالجة التي تتم قبل تسجيل الدخول بناء على متطلبات الموقف الخاص بهم. يمكن تعيين البرامج النصية لتسجيل الدخول إلى مجال أو إلى مستخدمين فرديين. بشكل عام، يمتلك المسؤولون عن المجال ملفات دفعة أو ما شابه ذلك معرفة مع المستخدمين أو المجموعات في Active Directory. بمجرد تسجيل دخول المستخدم، يتم تنفيذ البرنامج النصي لتسجيل الدخول.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

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

- أجهزة الأمان القابلة للتكيف ASA 5500 Series من Cisco التي تشغل الإصدار x.8 من البرنامج
- Cisco AnyConnect VPN، الإصدار 2.0

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.

معلومات أساسية

تتمثل نقطة SBL في أنها تقوم بتوصيل كمبيوتر بعيد بالبنية الأساسية للشركة قبل تسجيل الدخول إلى الكمبيوتر. على سبيل المثال، قد يكون المستخدم خارج شبكة الشركة الفعلية، وغير قادر على الوصول إلى موارد الشركة حتى ينضم جهاز الكمبيوتر الخاص به إلى شبكة الشركة. مع تمكين SBL، يتصل عميل AnyConnect قبل أن يرى المستخدم نافذة تسجيل الدخول إلى Microsoft. يجب على المستخدم أيضا تسجيل الدخول، كالعادة، إلى Windows عند ظهور نافذة تسجيل الدخول إلى Microsoft.

هذه أسباب عديدة لاستخدام SBL:

- تم ضم كمبيوتر المستخدم إلى بنية أساسية ل Active Directory.
- لا يمكن أن يكون لدى المستخدم بيانات اعتماد مخزنة مؤقتا على الكمبيوتر الشخصي، أي إذا كان نهج المجموعة لا يسمح ببيانات الاعتماد المخزنة مؤقتا.
- يجب على المستخدم تشغيل برامج نصية لتسجيل الدخول يتم تنفيذها من مورد شبكة أو تتطلب الوصول إلى مورد شبكة.
- لدى المستخدم محركات أقراص معينة على الشبكة تتطلب المصادقة مع البنية الأساسية ل Active Directory.
- قد تتطلب مكونات الشبكة، مثل MS NAP/CS NAC، الاتصال بالبنية الأساسية.

تقوم SBL بإنشاء شبكة مكافئة للتضمين على شبكة LAN الخاصة بالشركات المحلية. مع تمكين SBL، ونظرا لتمكين المستخدم من الوصول إلى البنية الأساسية المحلية، تتوفر أيضا البرامج النصية لتسجيل الدخول التي يتم تشغيلها عادة لأي مستخدم في المكتب للمستخدم البعيد.

للحصول على معلومات حول كيفية إنشاء برامج نصية لتسجيل الدخول، ارجع إلى مقالة Microsoft TechNet هذه .

لمزيد من المعلومات حول كيفية إستخدام البرامج النصية لتسجيل الدخول المحلي في Windows XP، ارجع إلى مقالة Microsoft هذه .

في مثال آخر، يمكن تكوين نظام لمنع بيانات الاعتماد المخزنة مؤقتا لتسجيل الدخول إلى الكمبيوتر. في هذا السيناريو، يجب أن يكون المستخدمون قادرين على الاتصال بوحدة تحكم بالمجال على شبكة الشركة للتحقق من صحة بيانات الاعتماد الخاصة بهم قبل الوصول إلى الكمبيوتر الشخصي. يتطلب SBL وجود اتصال شبكة في وقت إستدعائه. في بعض الحالات يكون هذا غير ممكن لأن التوصيل اللاسلكي يمكن أن يعتمد على مسوغات المستخدم للتوصيل بالبنية التحتية اللاسلكية. بما أن وضع SBL يسبق مرحلة بيانات الاعتماد لتسجيل الدخول، لا يتوفر اتصال في هذا السيناريو.

في هذه الحالة يلزم تكوين التوصيل اللاسلكي لتخزين بيانات الاعتماد مؤقتا عبر تسجيل الدخول، أو يلزم تكوين مصادقة لاسلكية أخرى لعمل SBL.

تثبيت مكونات البدء قبل تسجيل الدخول (في Windows فقط)

يجب تثبيت مكونات Start Before Logon بعد تثبيت العميل الأساسي. بالإضافة إلى ذلك، تتطلب مكونات AnyConnect 2.2 Start Before Logon تثبيت الإصدار 2.2 أو إصدار أحدث من برنامج عميل AnyConnect الأساسي. إذا قمت بنشر عميل AnyConnect ومكونات Start Before Logon مسبقا باستخدام ملفات MSI مسبقا (على سبيل المثال، فأنت في شركة كبيرة لديها عملية نشر برامج خاصة بها (Altiris أو Active Directory أو SMS)، فيجب عليك الحصول على الطلب بشكل صحيح. تتم معالجة ترتيب التثبيت تلقائيا عندما يقوم المسؤول بتحميل AnyConnect إذا تم نشره عبر الويب و/أو تحديثه عبر الويب. للحصول على معلومات تثبيت كاملة، ارجع إلى ملاحظات الإصدار الخاصة بعميل Cisco AnyConnect VPN، الإصدار 2.2.

الفروق بين Windows 7\Windows-Vista و Pre-Vista Start قبل تسجيل الدخول

تختلف إجراءات تمكين الارتباط بين المحولات (SBL) إختلافا طفيفا على نظامي التشغيل Windows Vista و Windows 7. تستخدم أنظمة ما قبل Vista مكونا يسمى Virtual Private Network Graphics Identification and Authentication (VPNGINA) لتنفيذ SBL. تستخدم أنظمة Vista و Windows 7 مكونا يسمى PLAP لتنفيذ SBL.

في عميل AnyConnect، تعرف ميزة "البدء قبل تسجيل الدخول إلى Windows Vista" باسم "موفر الوصول قبل تسجيل الدخول (PLAP)"، وهو موفر بيانات اعتماد قابل للاتصال. تتيح هذه الميزة لمسؤولي الشبكات تنفيذ مهام معينة، مثل تجميع بيانات الاعتماد أو الاتصال بموارد الشبكة، قبل تسجيل الدخول. يوفر PLAP وظائف Start Before Login على Windows Vista و Windows 7 وخادم Windows 2008. يدعم PLAP الإصدارات 32 بت و 64 بت من نظام التشغيل مع vpnplap.dll و VPNPLAP64.dll على التوالي. تدعم وظيفة نقطة الوصول عن بعد (PLAP) إصدارات Windows Vista x86 و x64.

ملاحظة: في هذا القسم، تشير VPNGINA إلى ميزة "البدء قبل تسجيل الدخول" لأنظمة ما قبل Vista ويشير PLAP إلى ميزة "البدء قبل تسجيل الدخول" لأنظمة Windows Vista و Windows 7.

في أنظمة ما قبل Vista، يستخدم Start Before Login مكونا يعرف ب VPN Graphical Identification and Authentication Dynamic Link Library (vpngina.dll) لتوفير إمكانيات Start Before Logon. يحل مكون Windows PLAP، الذي يعد جزءا من Windows Vista، محل مكون Windows GINA.

يتم تنشيط GINA عندما يقوم المستخدم بضغط مجموعة مفاتيح Ctrl+Alt+Del. باستخدام PLAP، تفتح مجموعة مفاتيح Ctrl+Alt+Del نافذة حيث يستطيع المستخدم إختيار إما تسجيل الدخول إلى النظام أو تنشيط أي إتصالات شبكة (مكونات PLAP) باستخدام زر توصيل الشبكة الموجود في الركن السفلي الأيمن من الإطار.

وتصف الأقسام التي تلي مباشرة الإعدادات والإجراءات لكل من VPNGINA و PLAP SBL. للحصول على وصف كامل لتمكين ميزة SBL (PLAP) واستخدامها على نظام Windows Vista الأساسي، ارجع إلى تكوين ميزة Start Before Login (PLAP) على أنظمة Windows Vista.

إعدادات XML لتمكين SBL

تسمح قيمة العنصر الخاصة ب UseStartBeforeLogon بتشغيل هذه الميزة (true) أو إيقاف تشغيلها (خطأ). إذا قمت بضبط هذه القيمة على **true** في التوصيف تحدث معالجة إضافية كجزء من تسلسل تسجيل الدخول. انظر وصف "البدء قبل تسجيل الدخول" للحصول على تفاصيل إضافية. قم بتعيين قيمة <UseStartBefore Logon> في ملف CiscoAnyConnect.xml إلى **true** لتمكين SBL:

```
<? "xml version="1.0" encoding="UTF-8?>
```

```
<Configuration>
<ClientInitialization>
<UseStartBeforeLogon>true</UseStartBeforeLogon>
<ClientInitialization/>
```

من أجل تعطيل SBL، قم بتعيين القيمة نفسها إلى **false**.

لتمكين ميزة UserControl، أستخدم هذه العبارة عند تمكين SBL:

```
<UseStartBeforeLogon userControllable="false">true</UseStartBeforeLogon>
```

يتم تخزين أي إعداد مستخدم مقترن بهذه السمة في مكان آخر.

تمكين SBL

لتقليل وقت التنزيل إلى الحد الأدنى، يطلب عميل AnyConnect تنزيلات (من جهاز الأمان) فقط الوحدات النمطية الأساسية التي يحتاج إليها لكل ميزة يدعمها. لتمكين الميزات الجديدة، مثل SBL، يجب عليك تحديد اسم الوحدة النمطية باستخدام الأمر **svc modules** من وضع تكوين WebVPN الخاص بنهج المجموعة أو اسم المستخدم WebVPN:

```
{no] svc modules {none | value string]
```

قيمة السلسلة ل SBL هي **vpngina**.

في هذا المثال، يدخل مسؤول الشبكة وضع سمات سياسة المجموعة لبرامج الإرسال عن بعد الخاصة بنهج المجموعة، ويدخل وضع تكوين WebVPN لنهج المجموعة، ويحدد السلسلة VPNGINA لتمكين SBL:

```
hostname(config)# group-policy telecommuters attributes
hostname(config-group-policy)# webvpn
hostame(config-group-webvpn)# svc modules value vpngina
```

بالإضافة إلى ذلك، يجب على المسؤول التأكد من أن ملف <profile.xml AnyConnect>، حيث <profile.xml> هو الاسم الذي عينه مسؤول الشبكة لملف XML، يحتوي على جملة <UseStartBeforeLogon> معينة إلى **true**، على سبيل المثال:

```
UseStartBeforeLogon UserControllable="false">true
```

يجب إعادة تشغيل النظام قبل بدء سريان تسجيل الدخول. يجب أيضا تحديد جهاز الأمان الذي ترغب في السماح ب SBL، أو أي وحدات نمطية أخرى للميزات الإضافية. ارجع إلى الوصف في وحدات التمكين الخاصة بميزات AnyConnect الإضافية، من الصفحة 2-5 (ASDM) قسم تمكين الوحدات النمطية لميزات AnyConnect الإضافية، الصفحة 4-3 (CLI) للحصول على مزيد من المعلومات.

البدء قبل تكوين تسجيل الدخول باستخدام CLI

يوضح هذا السيناريو كيفية إعداد ملف XML باستخدام CLI:

1. قم بإنشاء ملف تعريف ليتم دفعه لأسفل إلى أجهزة كمبيوتر العميل التي تبدو مشابهة لهذا:

```
<? "xml version="1.0" encoding="UTF-8?>
"/AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding>
"xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance
=xsi :schemaLocation
<"http://schemas.xmlsoap.org/encoding/ AnyConnectProfile.xsd"
```

```
                                        <ClientInitialization>
                                <UseStartBeforeLogon>true</UseStartBeforeLogon>
                                        <ClientInitialization/>
                                                <ServerList>
                                                 <HostEntry>
                                        <HostName>text.cisco.com</HostName>
                                                <HostEntry/>
                                                 <HostEntry>
                                        <HostName>test1.cisco.com</HostName>
                                          <HostAddress>1.1.1.1</HostAddress>
                                                <HostEntry/>
                                                        .
                                                        .
                                                        .
                                                 <HostEntry>
                                        <HostName>test2.cisco.com</HostName>
                                          <HostAddress>1.1.1.2</HostAddress>
                                                <HostEntry/>
                                               <ServerList/>
                                             <AnyConnectProfile/>
```

2. انسخ الملف إلى Flash (الذاكرة المؤقتة) على جهاز الأمان:

```
Copy tftp://x.x.x.x/AnyConnectProfile.xml AnyConnectProfile.xml
```

3. في جهاز الأمان، أضف ملف التعريف كملف تعريف متاح إلى القسم العمومي WebVPN، طالما تم إعداد كل شيء آخر بشكل صحيح لاتصالات AnyConnect:

```
hostname(config-group-policy)# webvpn
#(hostame(config-group-webvpn
svc profiles ReallyNewProfile disk0:/AnyConnectProfile.xml
```

4. قم بتحرير سياسة المجموعة التي تستخدمها، وأضفت **وحدات SVC النمطية** وأوامر **ملف تعريف SVC**:

```
hostname(config)# group-policy GroupPolicy internal
hostname(config)# group-policy GroupPolicy attributes
hostname(config-group-policy)# webvpn
hostame(config-group-webvpn)# svc modules value vpngina
hostame(config-group-webvpn)# svc profiles value ReallyNewProfile
```

البدء قبل تكوين تسجيل الدخول باستخدام ASDM

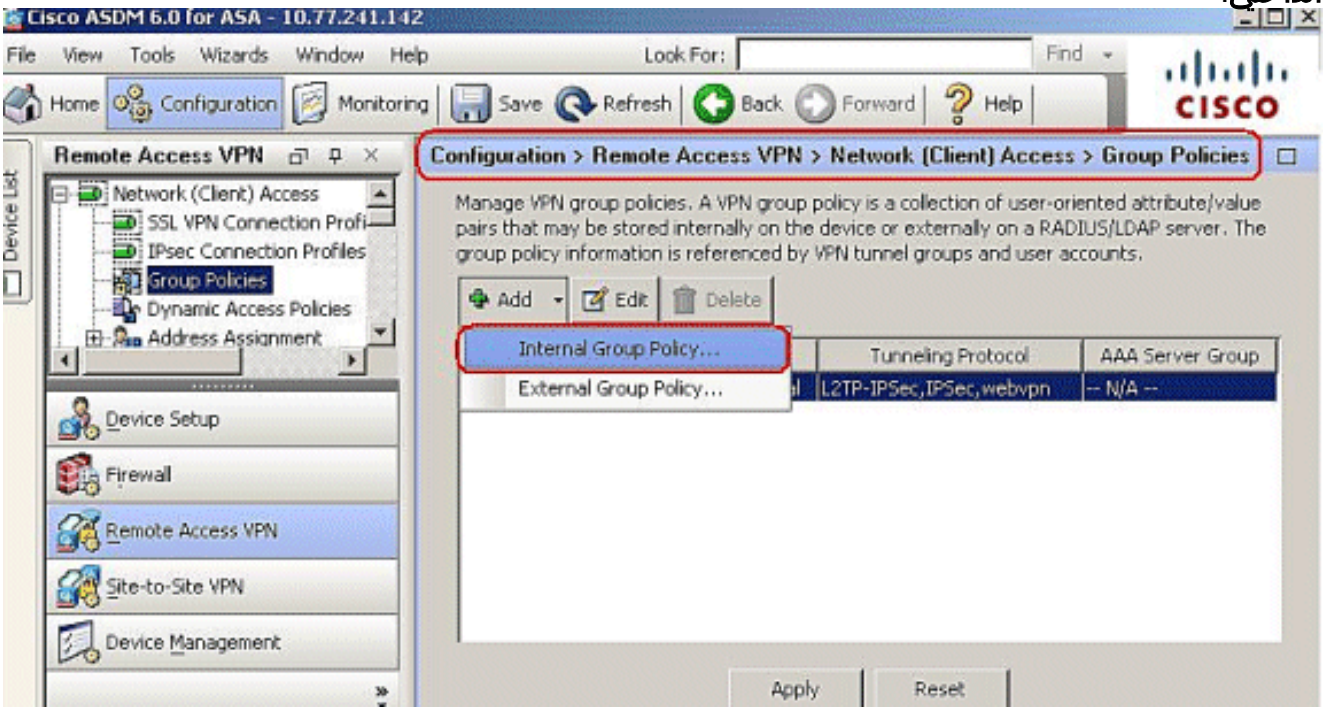
أكمل الخطوات التالية لتكوين SBL باستخدام ASDM:

1. قم بإنشاء ملف تعريف ليتم دفعه لأسفل إلى أجهزة كمبيوتر العميل التي تبدو مشابهة لهذا:

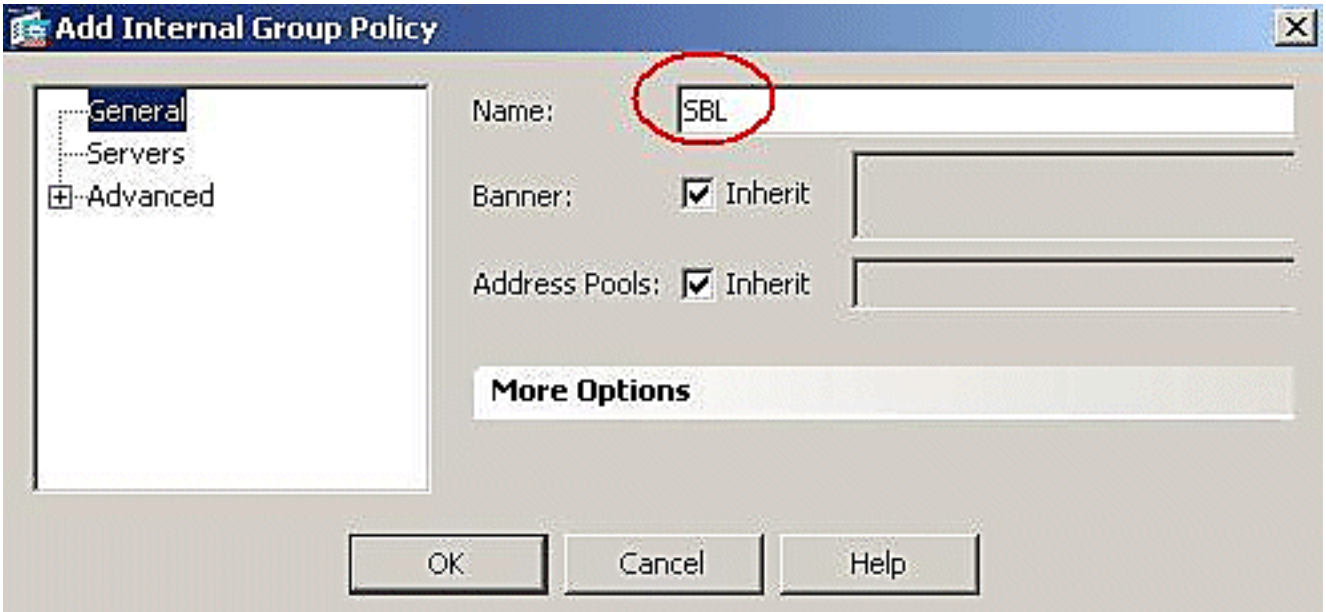
```
                                        <? "xml version="1.0" encoding="UTF-8?>
                                "/AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding>
                                        "xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance
                                                =xsi :schemaLocation
                                <"http://schemas.xmlsoap.org/encoding/ AnyConnectProfile.xsd"
                                                <ClientInitialization>
                                <UseStartBeforeLogon>true</UseStartBeforeLogon>
                                                <ClientInitialization/>
                                                        <ServerList>
                                                         <HostEntry>
                                                <HostName>text.cisco.com</HostName>
                                                        <HostEntry/>
                                                         <HostEntry>
                                                <HostName>test1.cisco.com</HostName>
                                                  <HostAddress>1.1.1.1</HostAddress>
                                                        <HostEntry/>
```

```
.
.
.
<HostEntry>
<HostName>test2.cisco.com</HostName>
<HostAddress>1.1.1.2</HostAddress>
<HostEntry/>
<ServerList/>
<AnyConnectProfile/>
```

2. احفظ التوصيف على هيئة **AnyConnectProfile.xml** في الكمبيوتر المحلي.
3. قم بتشغيل ASDM، ثم انتقل إلى الصفحة الرئيسية.
4. انتقل إلى **Configuration (التكوين) > Remote Access VPN (الوصول عن بعد) > Network (العميل) Access (الوصول إلى الشبكة) > Group Policies (نهج المجموعة) > Add (الإضافة)** وانقر فوق **نهج المجموعة الداخلي**.

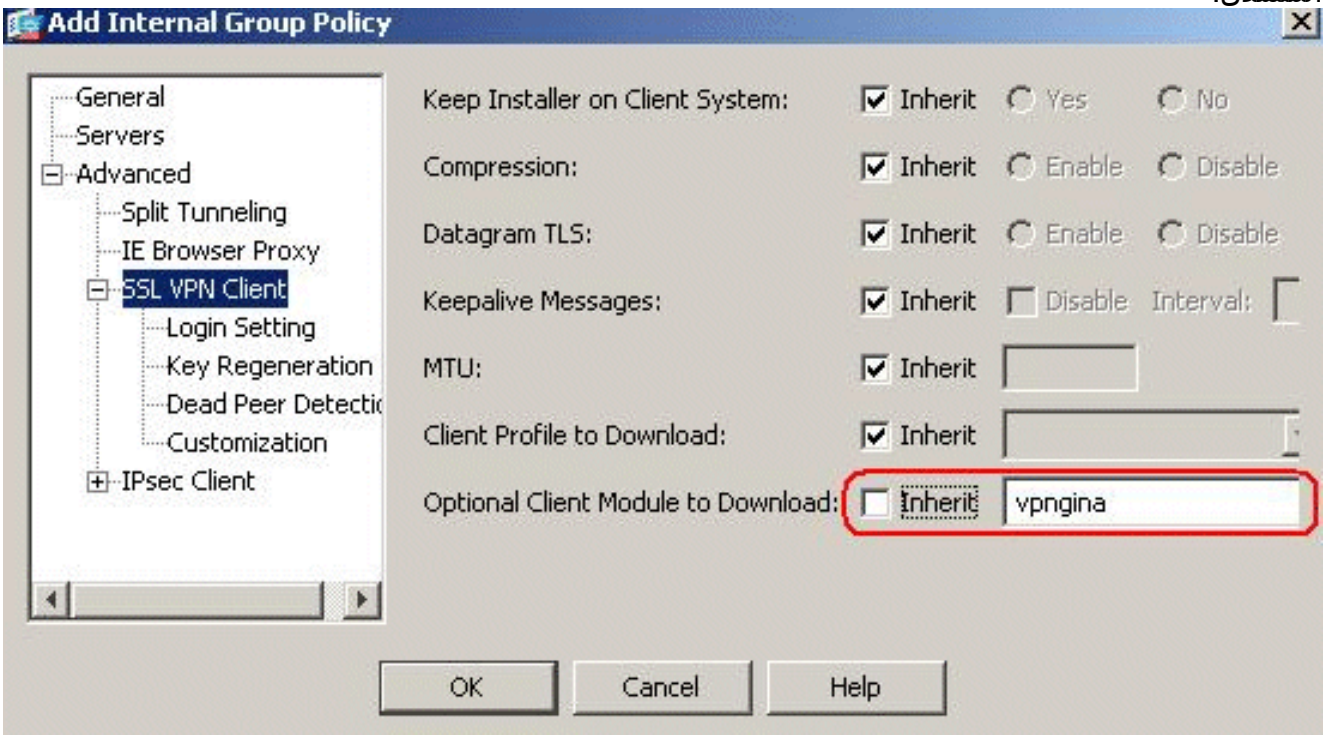


5. أدخل اسم نهج المجموعة، على سبيل المثال، **SBL**.

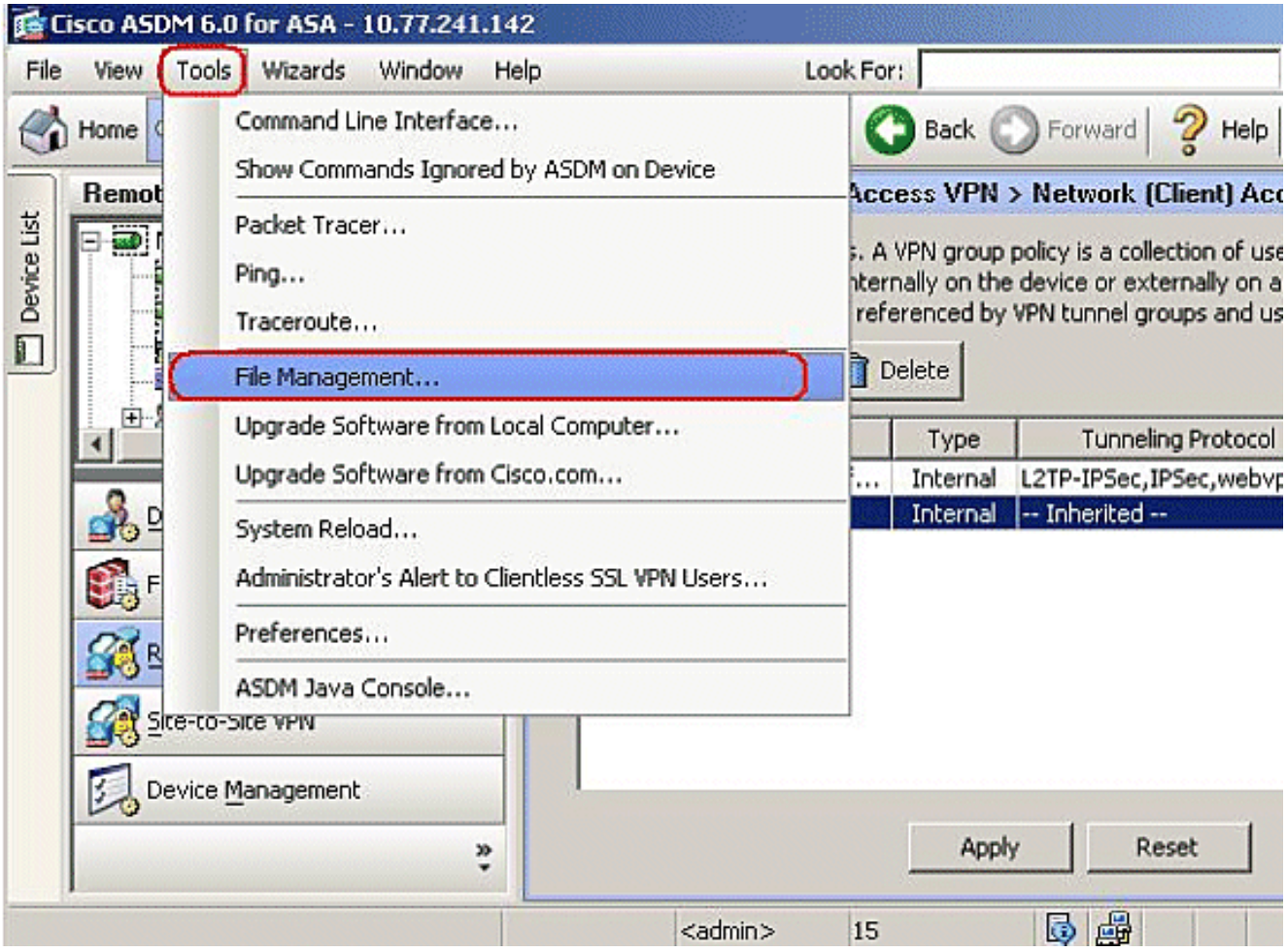


6. انتقل إلى **خيارات متقدمة > SSL VPN Client**. قم بإزالة علامة الاختيار Inherit (توريث) في **وحدة Client Module الاختيارية للتنزيل**، واختر **vpngina** من المربع

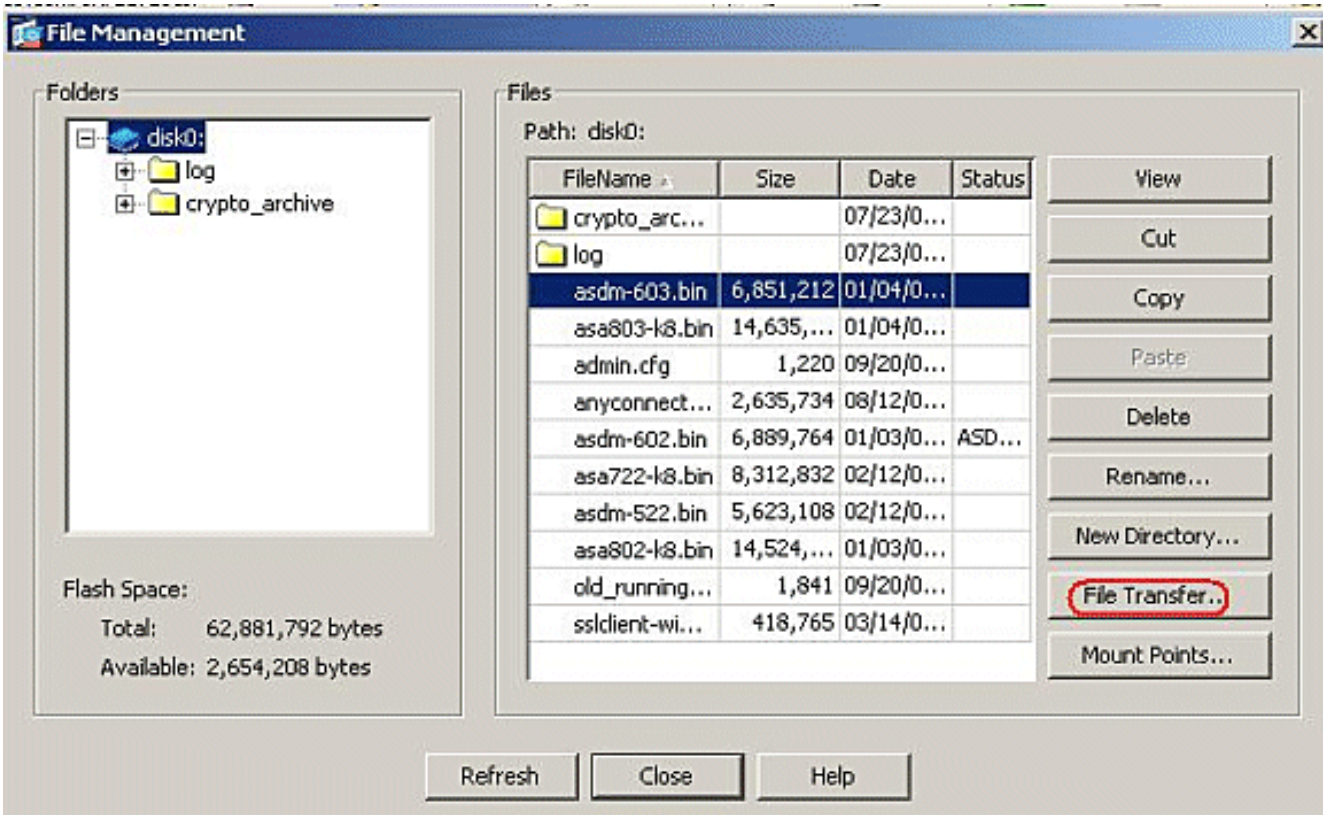
المنسدل.



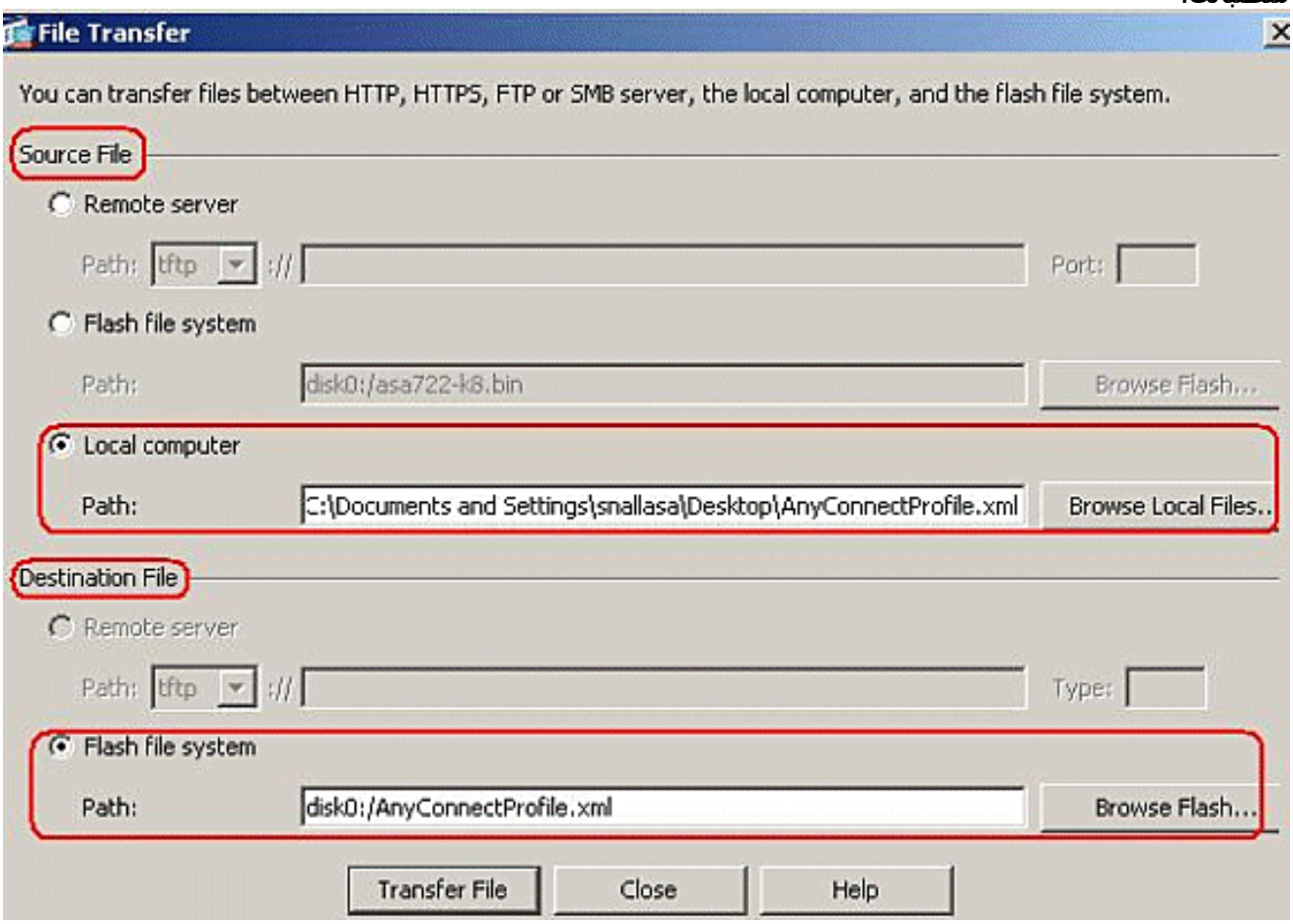
7. لنقل ملف التعريف **AnyConnectProfile.xml** من الكمبيوتر المحلي إلى الذاكرة المؤقتة (flash)، انتقل إلى **أدوات**، وانقر فوق **إدارة الملف**.



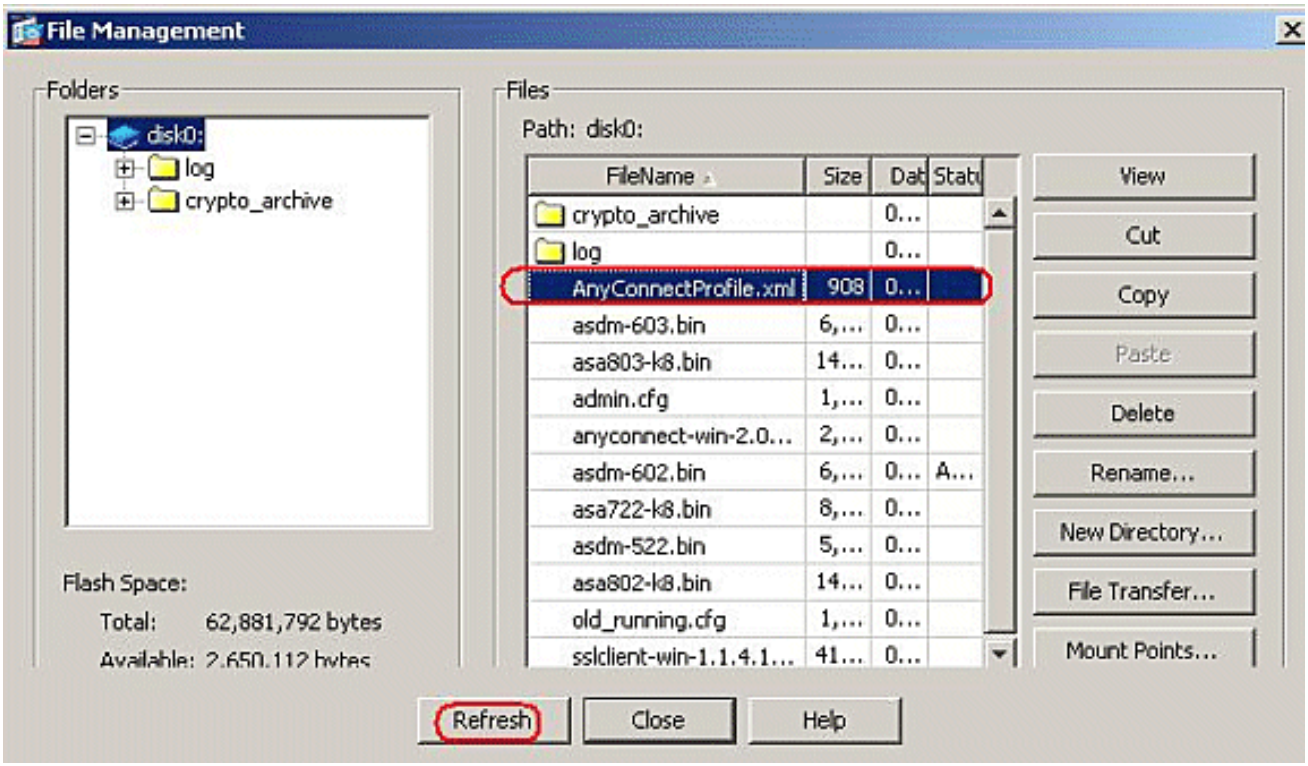
8. انقر فوق الزر **نقل الملفات**.



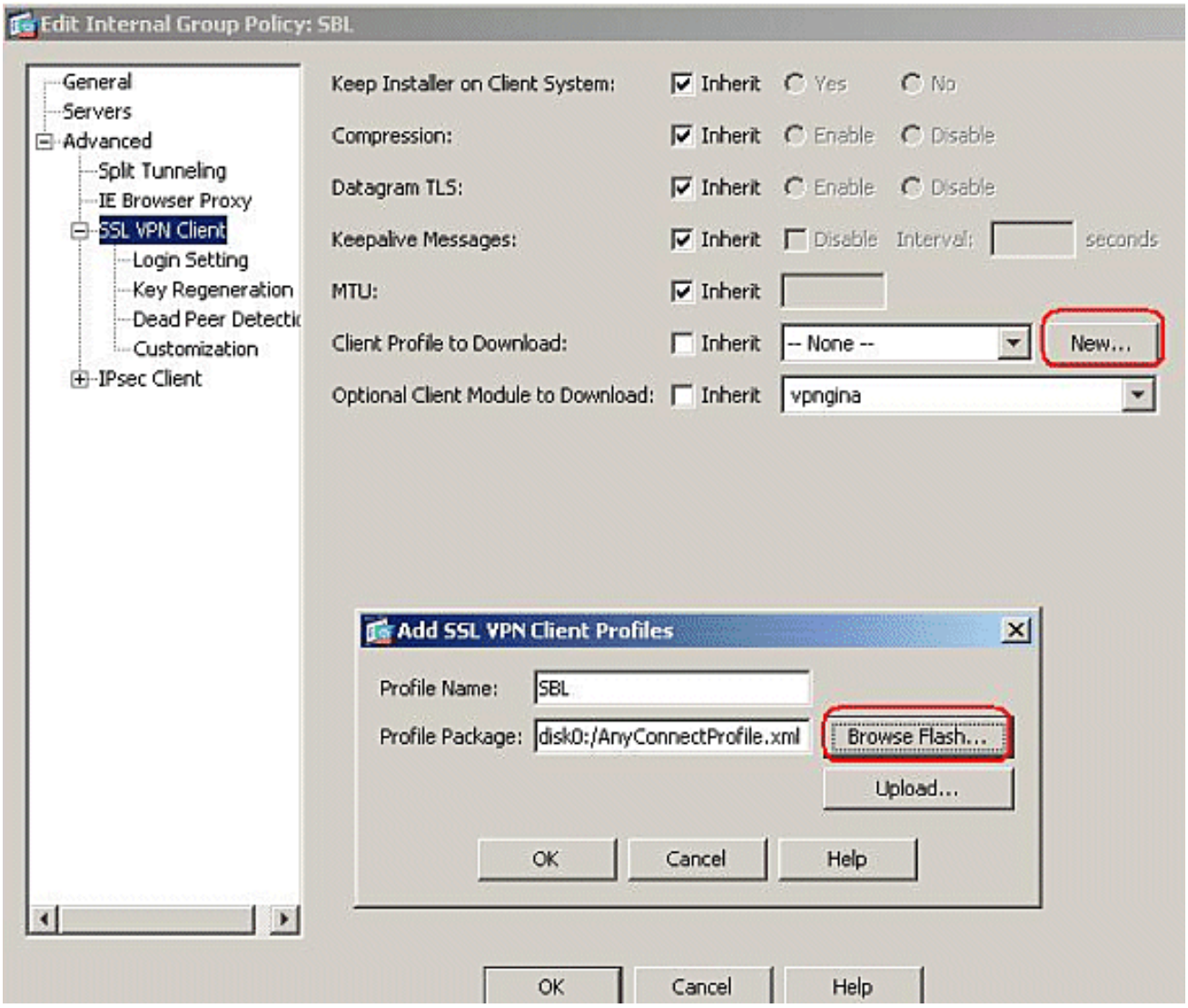
9. أخترت in order to نقلت التوصيف من الكمبيوتر المحلي إلى ASA Flash ذاكرة، **المصدر مبرد**، ممر من ال XML مبرد (حاسوب محلي)، **الغاية مبرد** مسار حسب متطلباتك.



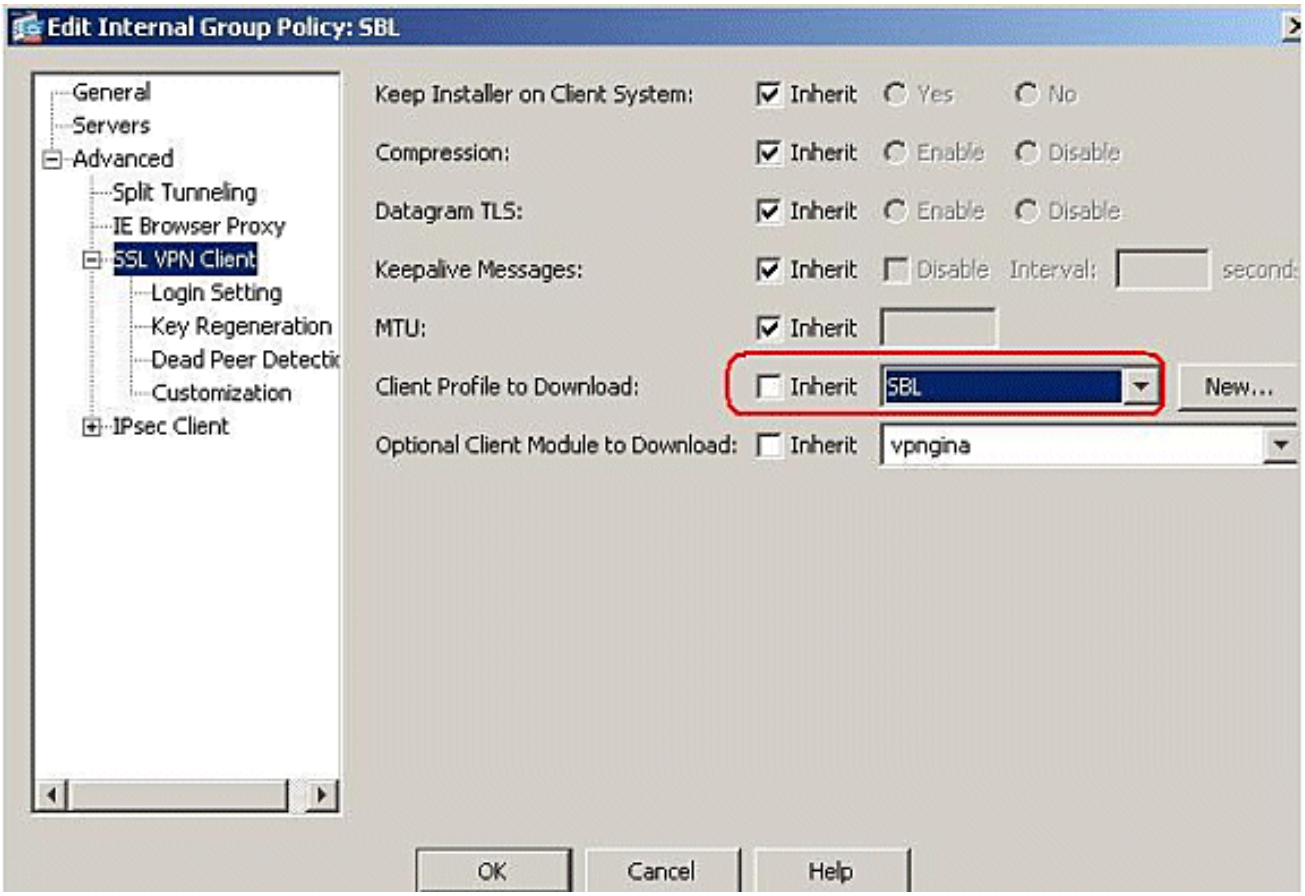
10. بعد النقل، انقر على زر **تحديث** للتحقق مما إذا كان ملف التخصيص في ذاكرة Flash (الذاكرة المؤقتة).



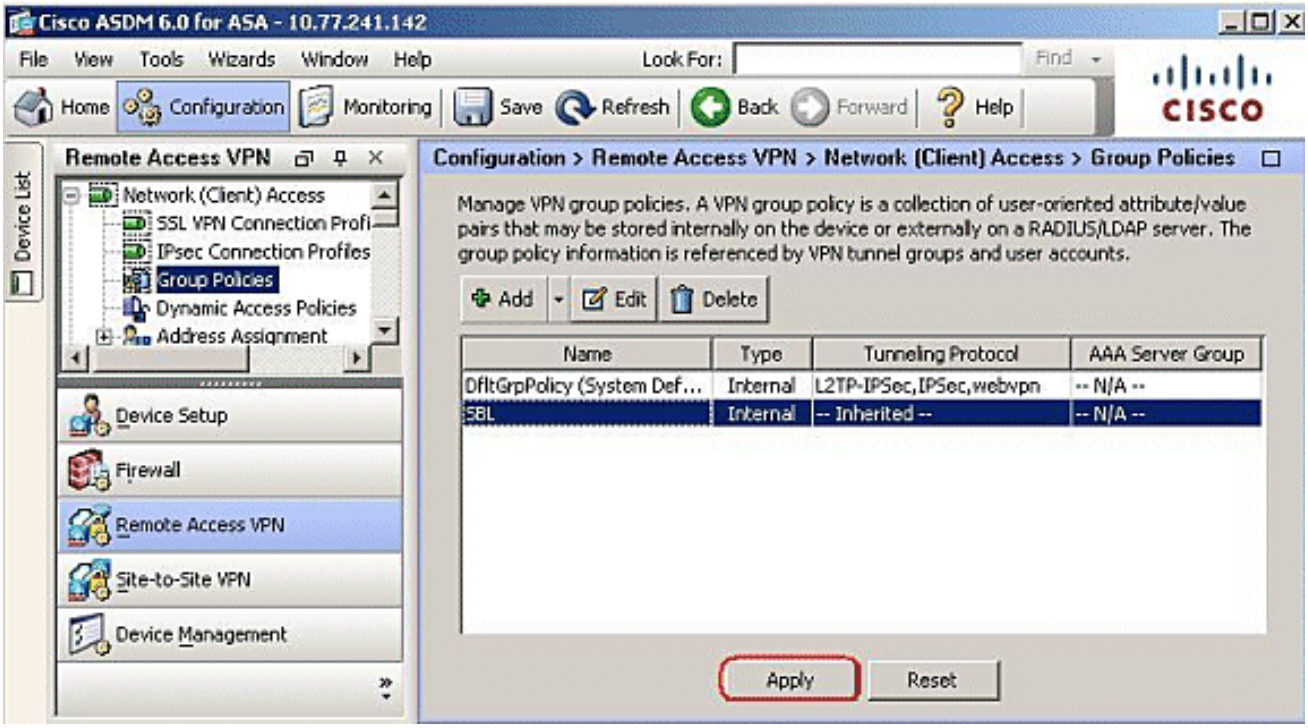
11. قم بتعيين ملف التعريف لنهج المجموعة الداخلي (SBL).اتبع هذا المسار، **التكوين > Remote Access VPN > للوصول عن بعد > Group Policies > Network (Client) Access (نهج المجموعة) > Edit SBL (نهج المجموعة الداخلي) > Client Profile > SSL VPN Client > Advanced للتنزيل**، وانقر فوق الزر **جديد**.في **إضافة ملفات تعريف عميل SSL VPN**، انقر على زر **إستعراض** لاختيار موقع ملف التعريف (AnyConnectProfile.xml) المخزن في ذاكرة ASA Flash. قم بتعيين **الاسم** لملف التعريف، على سبيل المثال، **SBL**. طقطقة **ok** أن يستكمل.



12. قم بإزالة خانة الاختيار "وراثة" واختر SBL في حقل **ملف تعريف العميل للتنزيل**. وانقر فوق OK.



13. انقر فوق **تطبيق** للاكتمال.



إستخدام ملف البيان

تحتوي حزمة AnyConnect التي يتم تحميلها على جهاز الأمان على ملف يسمى VPNManifest.xml. يوضح هذا المثال نموذجا لمحتوى هذا الملف:

```
<"xml version="1.0" encoding="UTF-7"?> <vpn rev="1.0?>
"file version="2.1.0150" id="VPNCore>
```

```
                                <"is_core="yes" type="exe" action="install
                        <uri>binaries/anyconnect-win-2.1.0150-web-deploy-k9.exe</uri>
                                                                    <file/>
                                                "file version="2.1.0150" id="gina>
                                    <"is_core="yes" type="exe" action="install" module="vpngina
                                <uri>binaries/anyconnect-gina-win-2.1.0150-web-deploy-k9.exe</uri>
                                                                    <file/>
                                                                    <vpn/>
```

قام جهاز الأمان بتخزين ملفات التعريف التي تم تكوينها عليه، كما هو موضح في الخطوة 1، كما يقوم بتخزين حزمة أو أكثر من حزم AnyConnect التي تحتوي على عميل AnyConnect نفسه وأداة تنزيل الأداة المساعدة وملف البيان وأي وحدات إختيارية أخرى أو ملفات دعم.

عند اتصال مستخدم بعيد بجهاز الأمان باستخدام WebLaunch أو عميل حالي مستقل، يتم تنزيل أداة تحميل التنزيل أولا وتشغيلها. وهو يستخدم ملف البيان للتأكد مما إذا كان هناك عميل حالي على كمبيوتر المستخدم البعيد يحتاج إلى ترقية أو أنه مطلوب تثبيت جديد. يحتوي ملف البيان أيضا على معلومات حول ما إذا كان هناك أي وحدات نمطية إختيارية يجب تنزيلها وتثبيتها، في هذه الحالة، ال VPNGINA. كما يتم دفع ملف تعريف العميل إلى أسفل من جهاز الأمان. يتم تنشيط تثبيت VPNGINA من خلال الأمر **svc modules value vpngina** الذي تم تكوينه ضمن وضع الأمر **group-policy (webVPN)** كما هو موضح في الخطوة 4. يتم تثبيت عميل AnyConnect و VPNGINA، ويرى المستخدم عميل AnyConnect في عملية إعادة التمهيد التالية، قبل تسجيل الدخول إلى مجال Windows.

عند اتصال المستخدم، يتم تمرير العميل والتوصيف إلى كمبيوتر المستخدم، ويتم تثبيت العميل و VPNGINA، ويرى المستخدم عميل AnyConnect في عملية إعادة التشغيل التالية، قبل تسجيل الدخول.

يتم توفير نموذج لملف التعريف على كمبيوتر العميل عند تثبيت AnyConnect: **C:\Documents and Settings\All Users\Application Data\Cisco\Cisco\AnyConnect VPN Client\Profile\AnyConnectProfile**.

أستكشاف أخطاء SBL وإصلاحها

أستخدم هذا الإجراء إذا واجهت مشكلة مع SBL:

1. تأكد من دفع التوصيف.
2. احذف ملفات التعريف السابقة، ابحث عنها على محرك القرص الثابت للعثور على الموقع: *.xml.
3. عند الانتقال إلى إضافة/إزالة البرامج، هل لديك كل من تثبيت AnyConnect وتثبيت AnyConnect VPNGINA؟
4. قم بإزالة تثبيت عميل AnyConnect.
5. قم بمسح سجل AnyConnect للمستخدم في عارض الأحداث وأعد الضبط.
6. إستعراض ويب مرة أخرى إلى جهاز الأمان لإعادة تثبيت العميل.
7. تأكد من أن ملف التخصيص يظهر أيضا.
8. أعد التشغيل مرة واحدة. في عملية إعادة التشغيل التالية، يوعز إليك بمطالبة "البدء قبل تسجيل الدخول".
9. إرسال سجل أحداث AnyConnect إلى Cisco بتنسيق .evt .
10. إذا ظهرت لك مشكلة الخطأ هذه، فقم بحذف ملف تعريف المستخدم واستخدم ملف التعريف الافتراضي:

```
Description: Unable to parse the profile
C:\Documents and Settings\All Users\Application Data\Cisco
.Cisco AnyConnect VPN Client\Profile\VABaseProfile.xml\
.Host data not available
```

المشكلة 1

تظهر رسالة الخطأ هذه أثناء محاولة تحميل ملف تعريف AnyConnect: `XML` . كيف يتم حل هذا الخطأ؟

الحل 1

غالبا ما تحدث رسالة الخطأ هذه بسبب الصياغة أو مشاكل التكوين في ملف تعريف AnyConnect. لحل هذه المشكلة، تأكد من أن ملف تعريف AnyConnect الذي تم تكوينه مماثل لملف تعريف AnyConnect العينة الموجود في قسم نموذج ملف تعريف AnyConnect ومخطط XML من دليل مسؤول عميل Cisco AnyConnect VPN.

معلومات ذات صلة

- دليل مسؤول عميل AnyConnect VPN من Cisco، الإصدار 2.0
- إنشاء برامج نصية لتسجيل الدخول - Windows TechNet
- تكوين PLAP (Start Before Login) على أنظمة Windows Vista
- وصول VPN ASA 8.x مع مثال تكوين عميل AnyConnect SSL VPN
- عميل AnyConnect VPN من Cisco
- 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).