ASA 8.X: Configurazione della funzionalità AnyConnect Start prima dell'accesso

Sommario

Introduzione

Se l'opzione *Start Before Logon* (SBL) è abilitata, l'utente visualizza la finestra di dialogo di accesso dell'interfaccia utente di AnyConnect prima che venga visualizzata la finestra di dialogo di accesso di Windows®. In questo modo viene prima stabilita la connessione VPN. Disponibile solo per le piattaforme Windows, Avvia prima dell'accesso consente all'amministratore di controllare l'utilizzo degli script di accesso, la memorizzazione delle password nella cache, la mappatura delle unità di rete alle unità locali e altro ancora. È possibile utilizzare la funzionalità SBL per attivare la VPN come parte della sequenza di accesso. SBL è disattivato per impostazione predefinita.

Per ulteriori informazioni sulla configurazione delle funzionalità dei client VPN AnyConnect, consultare la sezione Configurazione delle funzionalità dei client AnyConnect.

Nota: sul client AnyConnect, l'unica configurazione che si esegue per SBL è abilitare questa funzione. Gli amministratori di rete gestiscono l'elaborazione che viene eseguita prima dell'accesso in base ai requisiti della propria situazione. Gli script di accesso possono essere assegnati a un dominio o a singoli utenti. In genere, gli amministratori del dominio dispongono di file batch o simili definiti con utenti o gruppi in Active Directory. Non appena l'utente accede, viene eseguito lo script di accesso.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco ASA serie 5500 Adaptive Security Appliance con software versione 8.x
- Cisco AnyConnect VPN versione 2.0

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Fare riferimento a Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti.

Premesse

Il punto di SBL è che connette un computer remoto all'infrastruttura aziendale prima di accedere al PC. Ad esempio, un utente può trovarsi all'esterno della rete aziendale fisica e non può accedere alle risorse aziendali finché il suo PC non si unisce alla rete aziendale. Se l'opzione SBL è abilitata, il client AnyConnect si connette prima che l'utente visualizzi la finestra di accesso a Microsoft. L'utente deve inoltre accedere, come di consueto, a Windows quando viene visualizzata la finestra di accesso a Microsoft.

Di seguito sono riportati diversi motivi per cui utilizzare le licenze SBL:

- Il PC dell'utente fa parte di un'infrastruttura di Active Directory.
- L'utente non può avere credenziali memorizzate nella cache nel PC, ovvero se i Criteri di gruppo non consentono le credenziali memorizzate nella cache.
- L'utente deve eseguire script di accesso che vengono eseguiti da una risorsa di rete o che richiedono l'accesso a una risorsa di rete.
- Un utente dispone di unità di rete che richiedono l'autenticazione con l'infrastruttura di Active Directory.
- I componenti di rete, ad esempio MS NAP/CS NAC, possono richiedere la connessione all'infrastruttura.

SBL crea una rete equivalente all'inclusione nella LAN aziendale locale. Se è abilitata la SBL, poiché l'utente ha accesso all'infrastruttura locale, gli script di accesso normalmente eseguiti per un utente in ufficio sono disponibili anche per l'utente remoto.

Per informazioni sulla creazione di script di accesso, fare riferimento a questo articolo di Microsoft

TechNet .

Per informazioni sull'utilizzo degli script di accesso locali in Windows XP, fare riferimento a questo articolo di Microsoft .

In un altro esempio, è possibile configurare un sistema in modo da non consentire le credenziali memorizzate nella cache per l'accesso al PC. In questo scenario, gli utenti devono essere in grado di comunicare con un controller di dominio sulla rete aziendale affinché le loro credenziali vengano convalidate prima di accedere al PC. SBL richiede che una connessione di rete sia presente nel momento in cui viene richiamata. In alcuni casi, ciò non è possibile perché una connessione wireless può dipendere dalle credenziali utente per la connessione all'infrastruttura wireless. Poiché la modalità SBL precede la fase delle credenziali di un accesso, in questo scenario non è disponibile una connessione. In questo caso, è necessario configurare la connessione wireless per memorizzare nella cache le credenziali tra un accesso e l'altro oppure configurare un'altra autenticazione wireless per il funzionamento di SBL.

Installa componenti di avvio prima dell'accesso (solo Windows)

I componenti Start Before Logon devono essere installati dopo l'installazione del client principale. Inoltre, i componenti AnyConnect 2.2 Start Before Logon richiedono l'installazione della versione 2.2 o successive del software client AnyConnect. Se si pre-distribuiscono il client AnyConnect e i componenti Start Before Logon con i file MSI (ad esempio, una grande azienda con una propria implementazione software (Altiris, Active Directory o SMS), l'ordine deve essere corretto. L'ordine di installazione viene gestito automaticamente quando l'amministratore carica AnyConnect se questo è distribuito sul Web e/o aggiornato sul Web. Per informazioni complete sull'installazione, fare riferimento alle note sulla versione per Cisco AnyConnect VPN Client, versione 2.2.

Differenze tra Windows-Vista\Windows 7 e versioni precedenti a Vista Start Before Logon

Le procedure per abilitare SBL sono leggermente diverse nei sistemi Windows Vista e Windows 7. I sistemi in versione pre-Vista utilizzano un componente chiamato VPNGINA (Virtual Private Network Graphical Identification and Authentication) per implementare le SBL. I sistemi Vista e Windows 7 utilizzano un componente denominato PLAP per implementare SBL.

Nel client AnyConnect, la funzionalità Windows Vista Start Before Logon è nota come provider di credenziali di pre-accesso (PLAP, Pre-Login Access Provider). Questa funzionalità consente agli amministratori di eseguire attività specifiche, ad esempio la raccolta di credenziali o la connessione a risorse di rete, prima dell'accesso. PLAP fornisce le funzioni Avvia prima dell'accesso su Windows Vista, Windows 7 e il server Windows 2008. PLAP supporta le versioni a 32 bit e a 64 bit del sistema operativo rispettivamente con vpnplap.dll e vpnplap64.dll. La funzione PLAP supporta le versioni x86 e x64 di Windows Vista.

Nota: in questa sezione, VPNGINA fa riferimento alla funzione Avvia prima dell'accesso per le piattaforme precedenti a Vista e PLAP alla funzione Avvia prima dell'accesso per i sistemi Windows Vista e Windows 7.

Nei sistemi precedenti a Vista, il comando Avvia prima dell'accesso utilizza un componente noto come libreria a collegamento dinamico di autenticazione e identificazione grafica VPN (vpngina.dll) per fornire le funzionalità Avvia prima dell'accesso. Il componente PLAP di Windows, che fa parte di Windows Vista, sostituisce il componente GINA di Windows.

La funzione GINA viene attivata quando l'utente preme la combinazione di tasti Ctrl+Alt+Canc. Con PLAP, la combinazione di tasti Ctrl+Alt+Canc apre una finestra in cui l'utente può scegliere se accedere al sistema o attivare le connessioni di rete (componenti PLAP) con il pulsante Connessione di rete nell'angolo inferiore destro della finestra.

Le sezioni che seguono descrivono le impostazioni e le procedure sia per VPNGINA che per PLAP SBL. Per una descrizione completa dell'abilitazione e dell'utilizzo della funzionalità SBL (PLAP) su una piattaforma Windows Vista, fare riferimento alla sezione Configurazione del protocollo di avvio prima dell'accesso (PLAP) sui sistemi Windows Vista.

Impostazioni XML per abilitare SBL

Il valore di elemento per UseStartBeforeLogon consente di attivare (true) o disattivare (false) questa funzionalità. Se si imposta questo valore su **true** nel profilo, si verificherà un'ulteriore elaborazione come parte della sequenza di accesso. Per ulteriori informazioni, vedere la descrizione di Avvia prima di accedere. Per abilitare le licenze SBL, impostare il valore **<**UseStartBefore Logon**>** nel file CiscoAnyConnect.xml su **true**:

```
<?xml version="1.0" encoding="UTF-8" ?>
<Configuration>
<ClientInitialization>
<UseStartBeforeLogon>true</UseStartBeforeLogon>
</ClientInitialization>
```

Per disabilitare il filtro SBL, impostare lo stesso valore su **false**.

Per abilitare la funzione UserControllable, utilizzare questa istruzione quando si abilita SBL:

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

Qualsiasi impostazione utente associata a questo attributo viene memorizzata altrove.

Abilita SBL

Per ridurre al minimo il tempo di download, il client AnyConnect richiede di scaricare (dall'appliance di sicurezza) solo i moduli principali necessari per ciascuna funzionalità supportata. Per abilitare nuove funzionalità, ad esempio SBL, è necessario specificare il nome del modulo con il comando **svc modules** dalla modalità di configurazione WebVPN di Criteri di gruppo o nomeutente WebVPN:

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

Il valore stringa per SBL è **vpngina**.

In questo esempio, l'amministratore di rete accede alla modalità attributi di Criteri di gruppo per i telelavoratori di Criteri di gruppo; attiva la modalità di configurazione WebVPN per Criteri di gruppo; e specifica la stringa VPNGINA per abilitare SBL:

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

Inoltre, l'amministratore deve verificare che per il file AnyConnect <profile.xml>, dove <profile.xml> è il nome assegnato dall'amministratore di rete al file XML, l'istruzione <UseStartBeforeLogon> sia impostata su **true**, ad esempio:

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

Per rendere effettivo il comando Avvia prima di accedere, è necessario riavviare il sistema. È inoltre necessario specificare sull'accessorio di protezione che si desidera consentire l'utilizzo di SBL o di qualsiasi altro modulo per funzionalità aggiuntive. Per ulteriori informazioni, consultare la descrizione nella sezione Abilitazione dei moduli per le funzionalità AnyConnect aggiuntive, pagina 2-5 (ASDM) o Abilitazione dei moduli per le funzionalità AnyConnect aggiuntive, pagina 3-4 (CLI).

Avvia configurazione prima dell'accesso con CLI

Questo scenario mostra come impostare il file XML con CLI:

1. Creare un profilo da inserire nei PC client simile al seguente:

```
<?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. Copiare il file nella memoria flash sull'appliance di sicurezza:

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

3. Sull'appliance di sicurezza aggiungere il profilo come profilo disponibile alla sezione globale WebVPN, a condizione che le altre impostazioni siano corrette per le connessioni AnyConnect:

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

4. Modificare i criteri di gruppo utilizzati e aggiungere i **moduli svc** e i comandi del **profilo 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
```

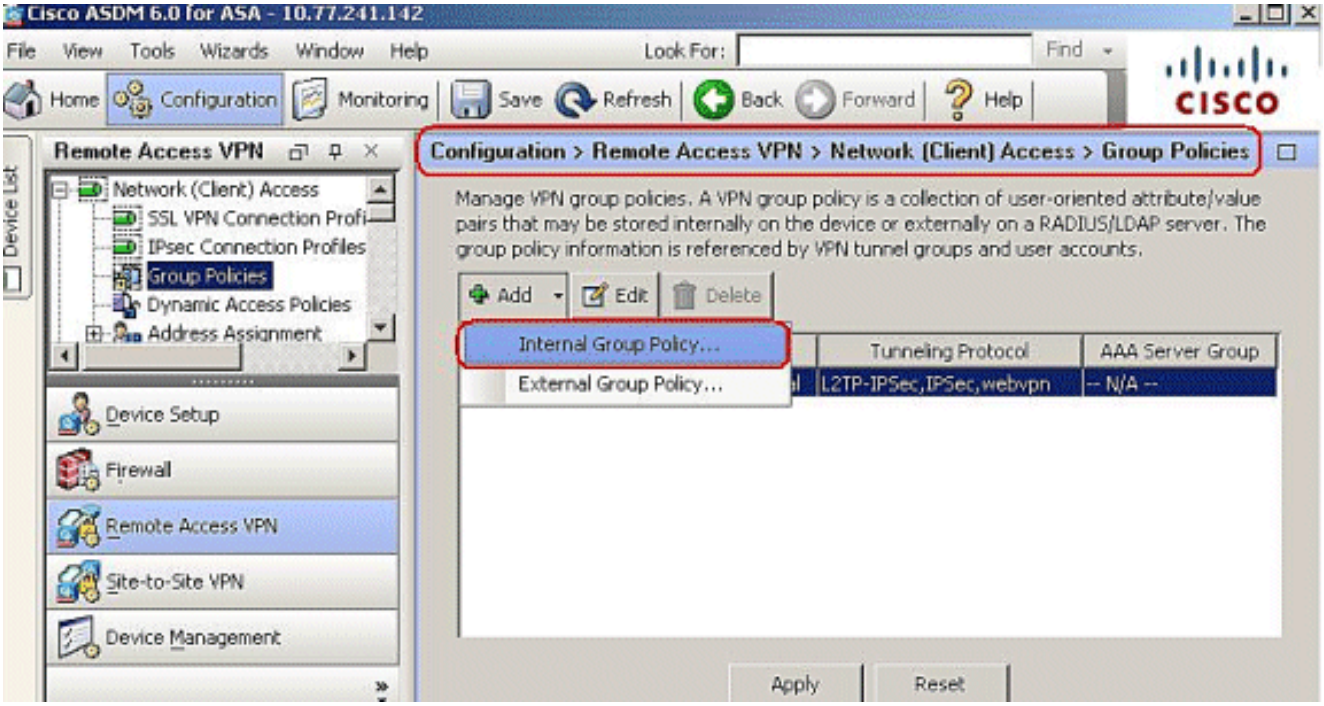
Avvia configurazione prima dell'accesso con ASDM

Completare la procedura seguente per configurare l'SBL con ASDM:

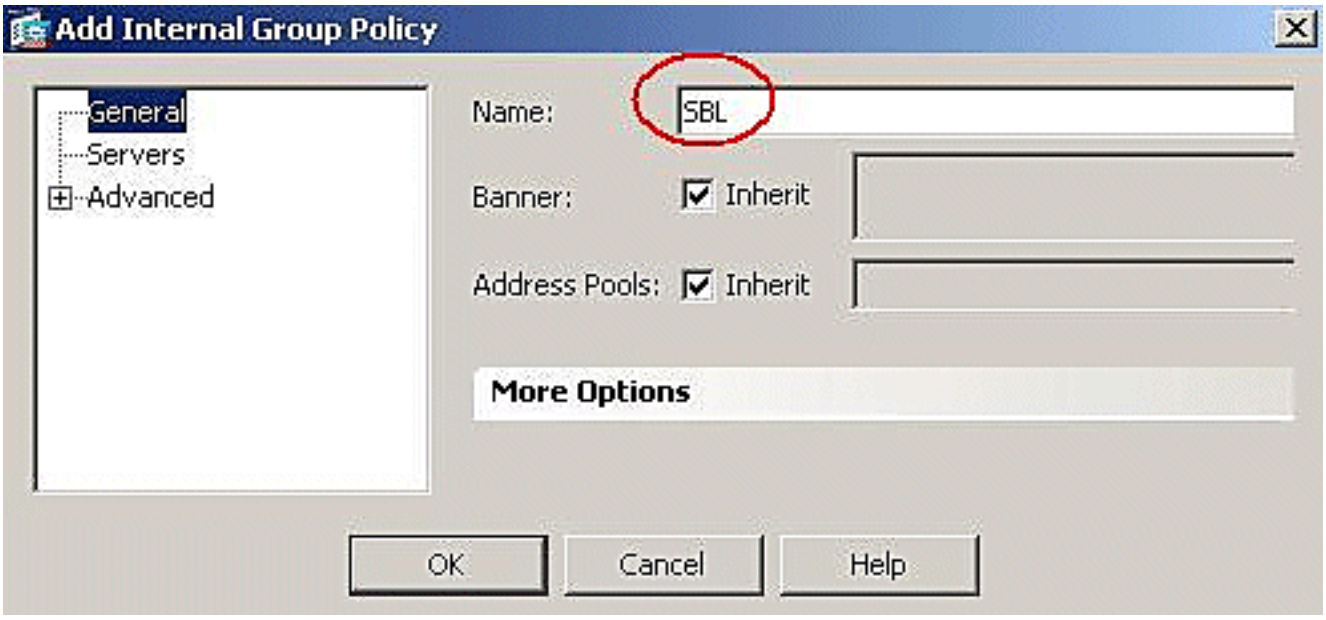
1. Creare un profilo da inserire nei PC client simile al seguente:

```
<?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>
```

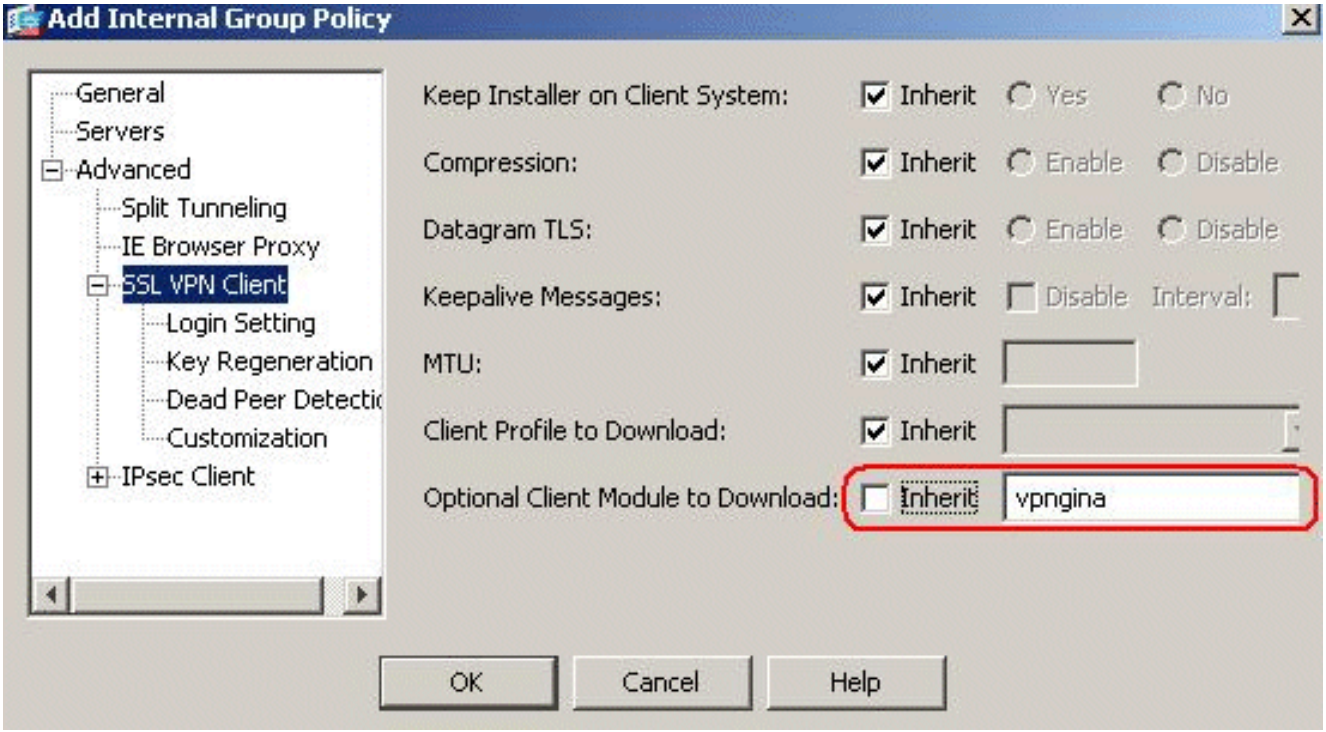
2. Salvare il profilo come **AnyConnectProfile.xml** nel computer locale.
3. Avviare ASDM e andare alla home page.
4. Selezionare **Configurazione > VPN ad accesso remoto > Accesso di rete (client) > Criteri di gruppo > Aggiungi** , quindi fare clic su **Criteri di gruppo interni**.



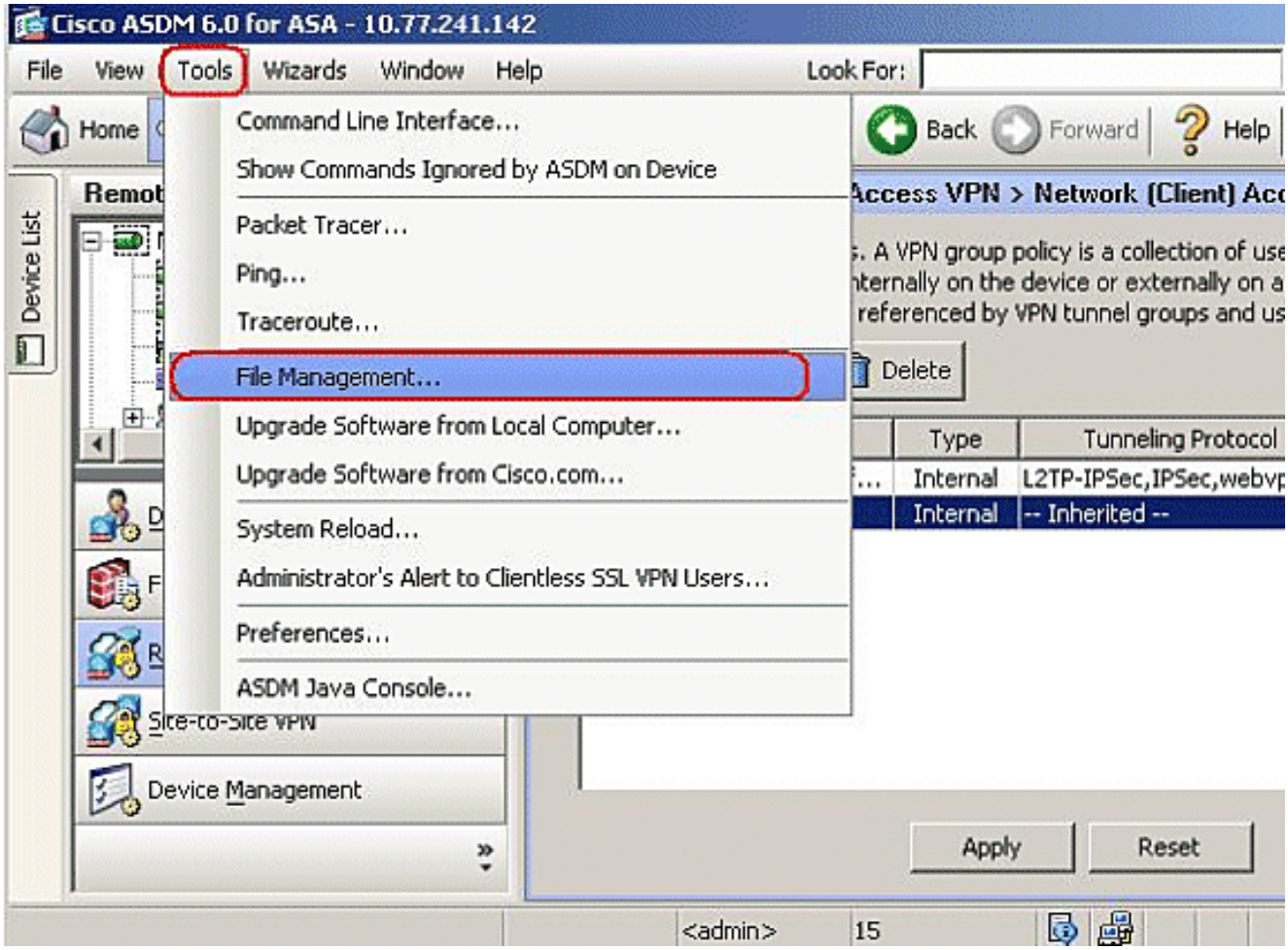
5. Immettere il nome del criterio di gruppo, ad esempio **SBL**.



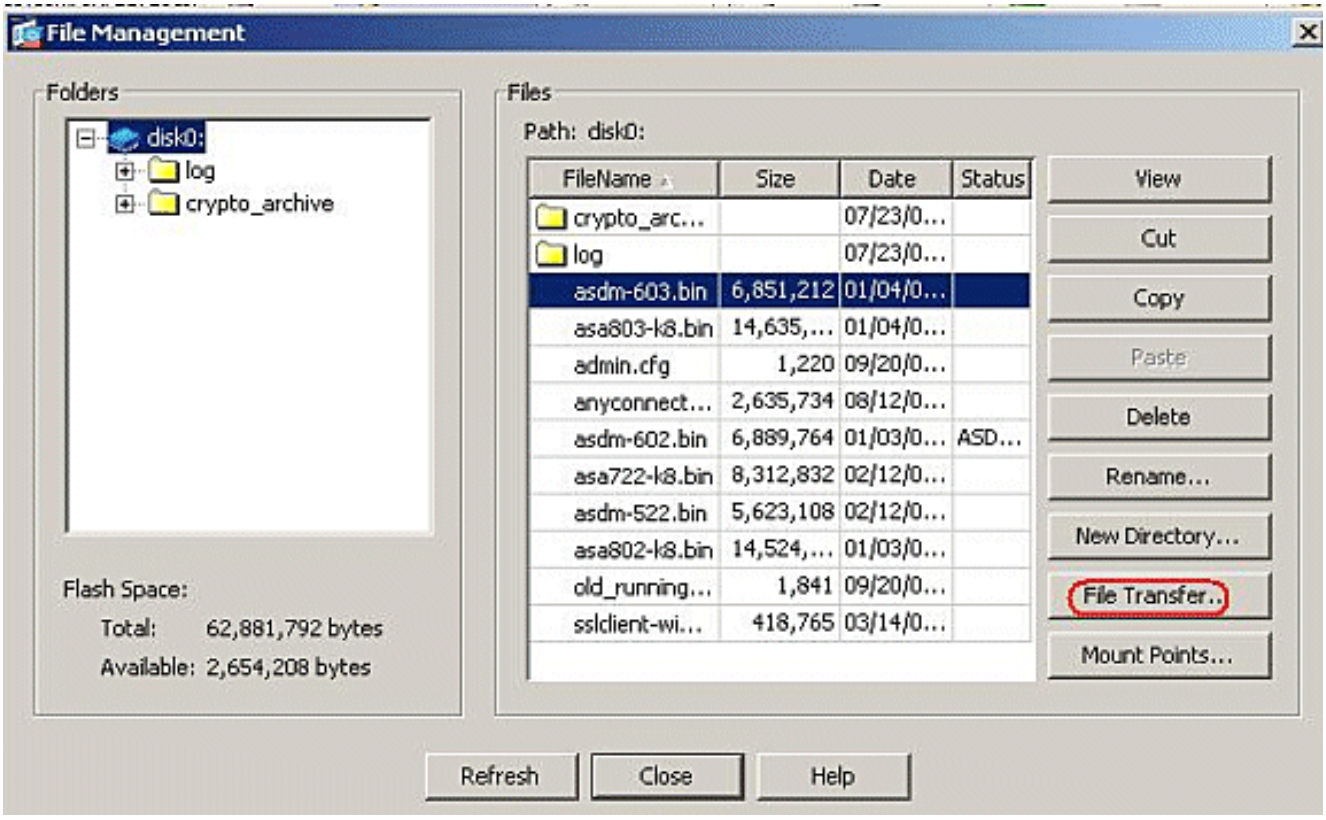
6. Selezionare **Avanzate > SSL VPN Client**. Rimuovere il segno di spunta Inherit (Eredita) nel **modulo client facoltativo da scaricare**, quindi selezionare **vpngina** dall'elenco a discesa.



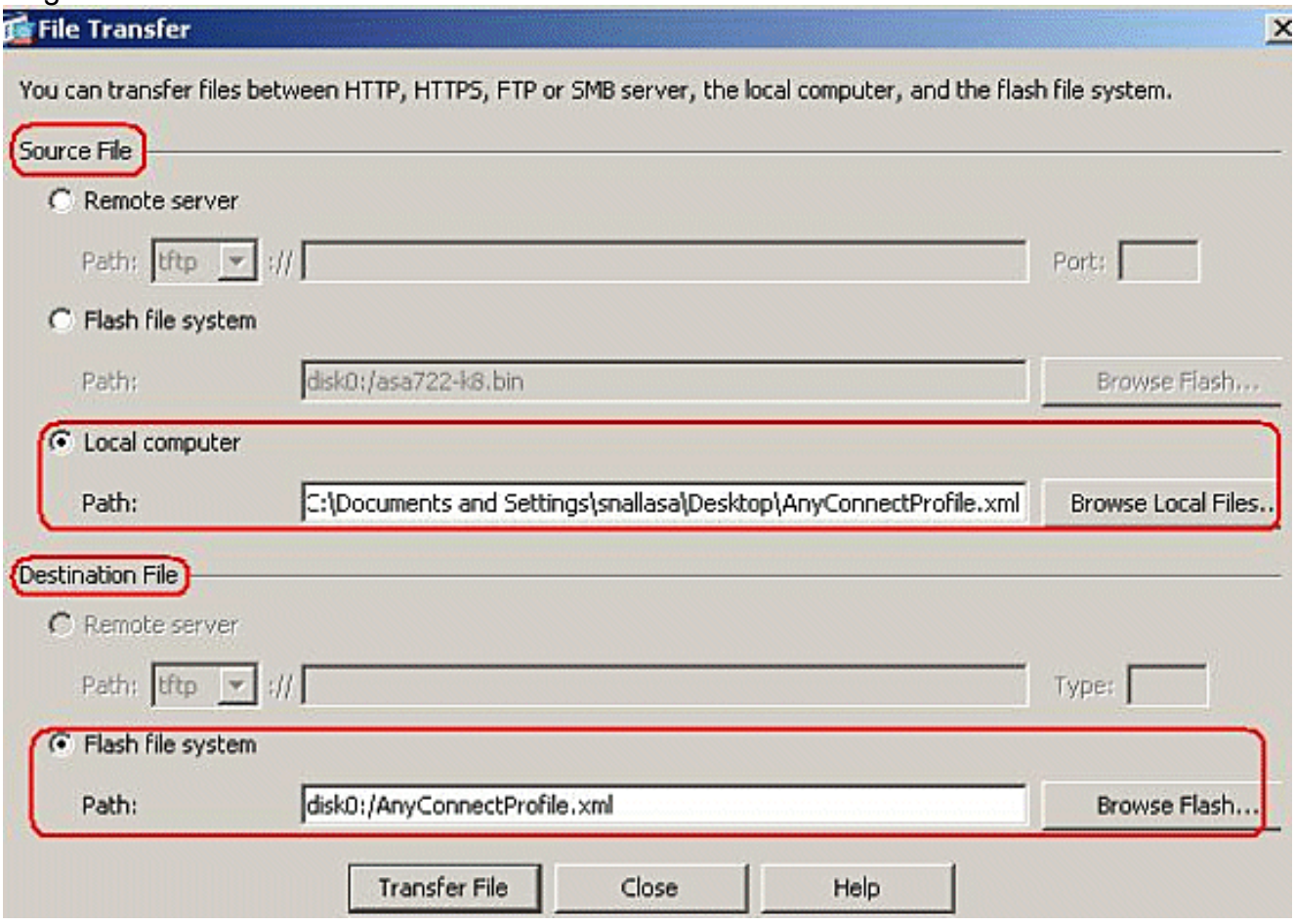
7. Per trasferire il profilo **AnyConnectProfile.xml** dal computer locale a Flash, andare in **Strumenti** e fare clic su **Gestione file**.



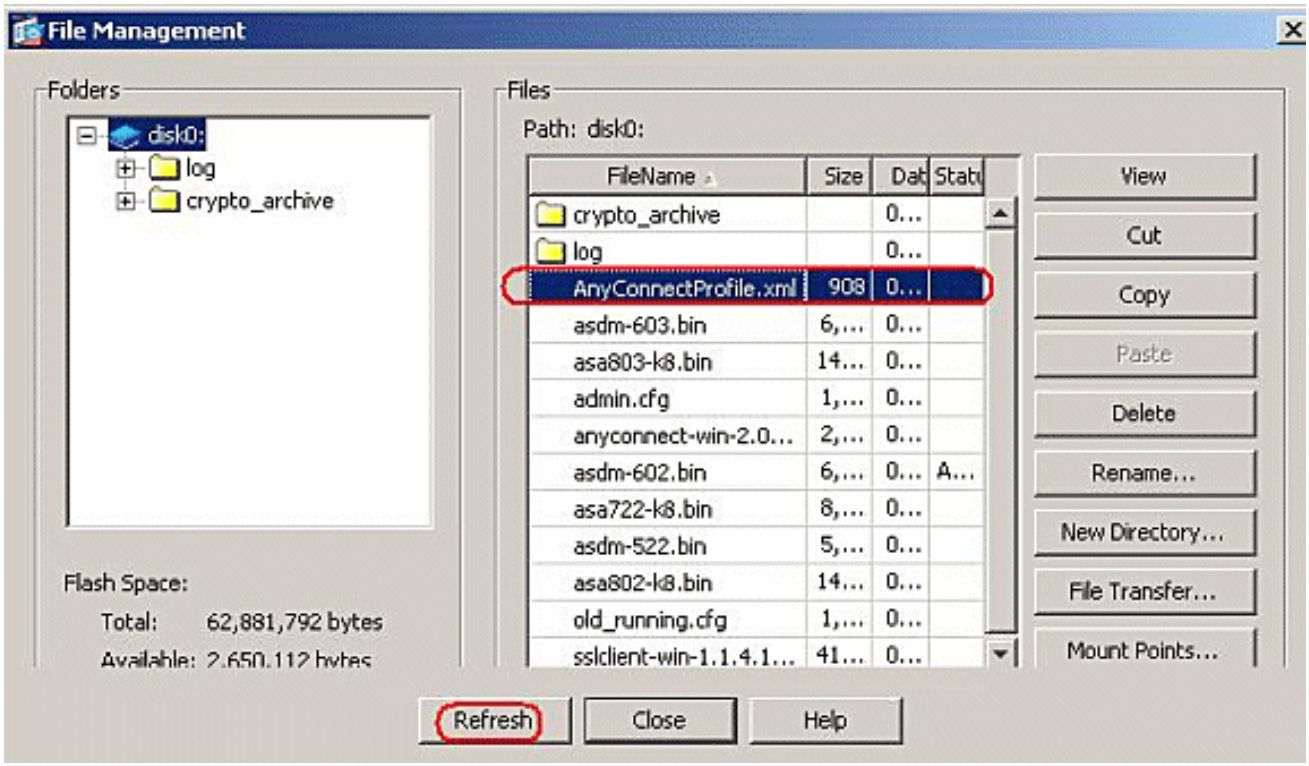
8. Fare clic sul pulsante **Trasferimento file**.



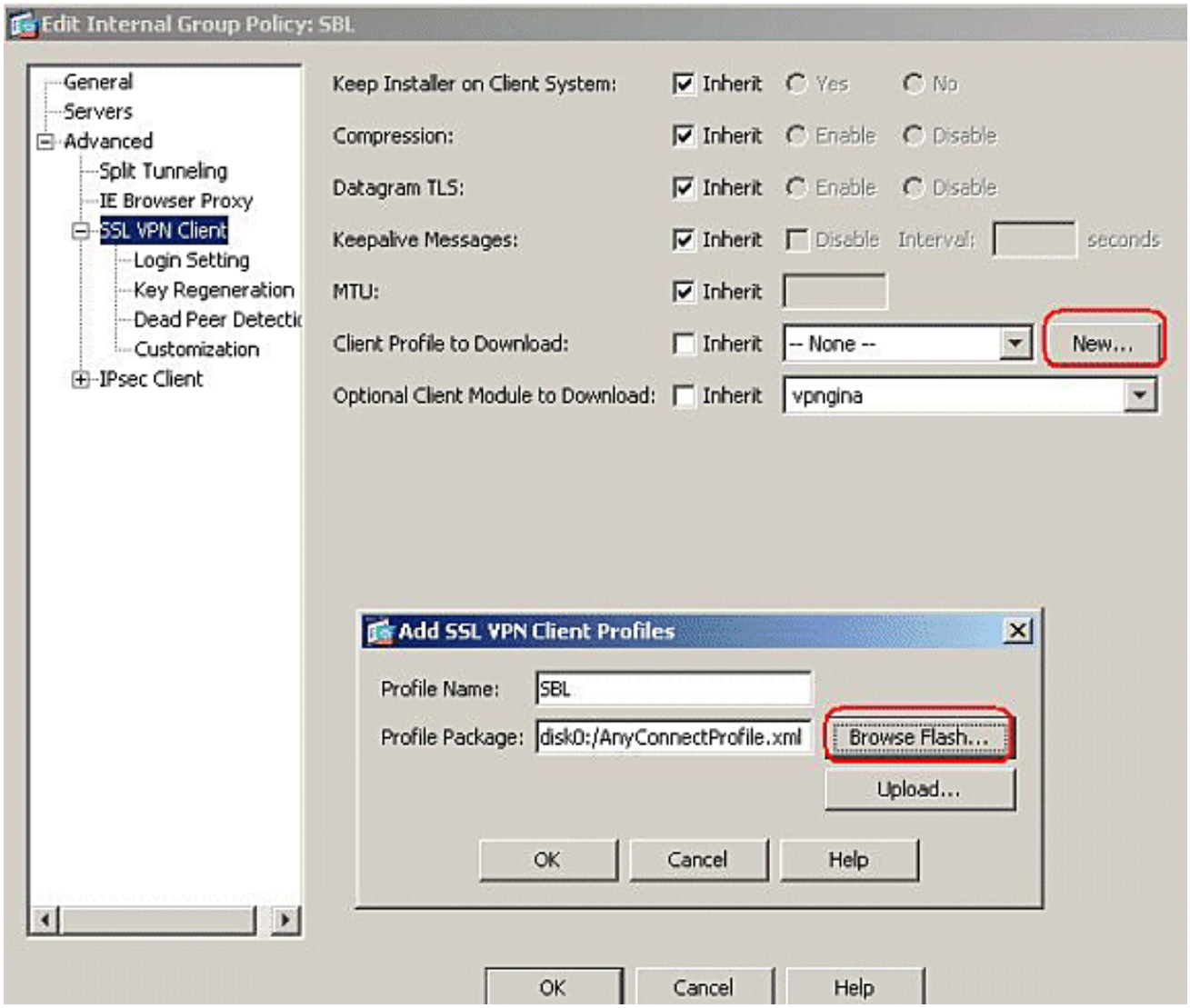
9. Per trasferire il profilo dal computer locale alla memoria flash ASA, scegliere il **file di origine**, il percorso del file XML (computer locale) e il percorso del **file di destinazione** in base alle proprie
esigenze.



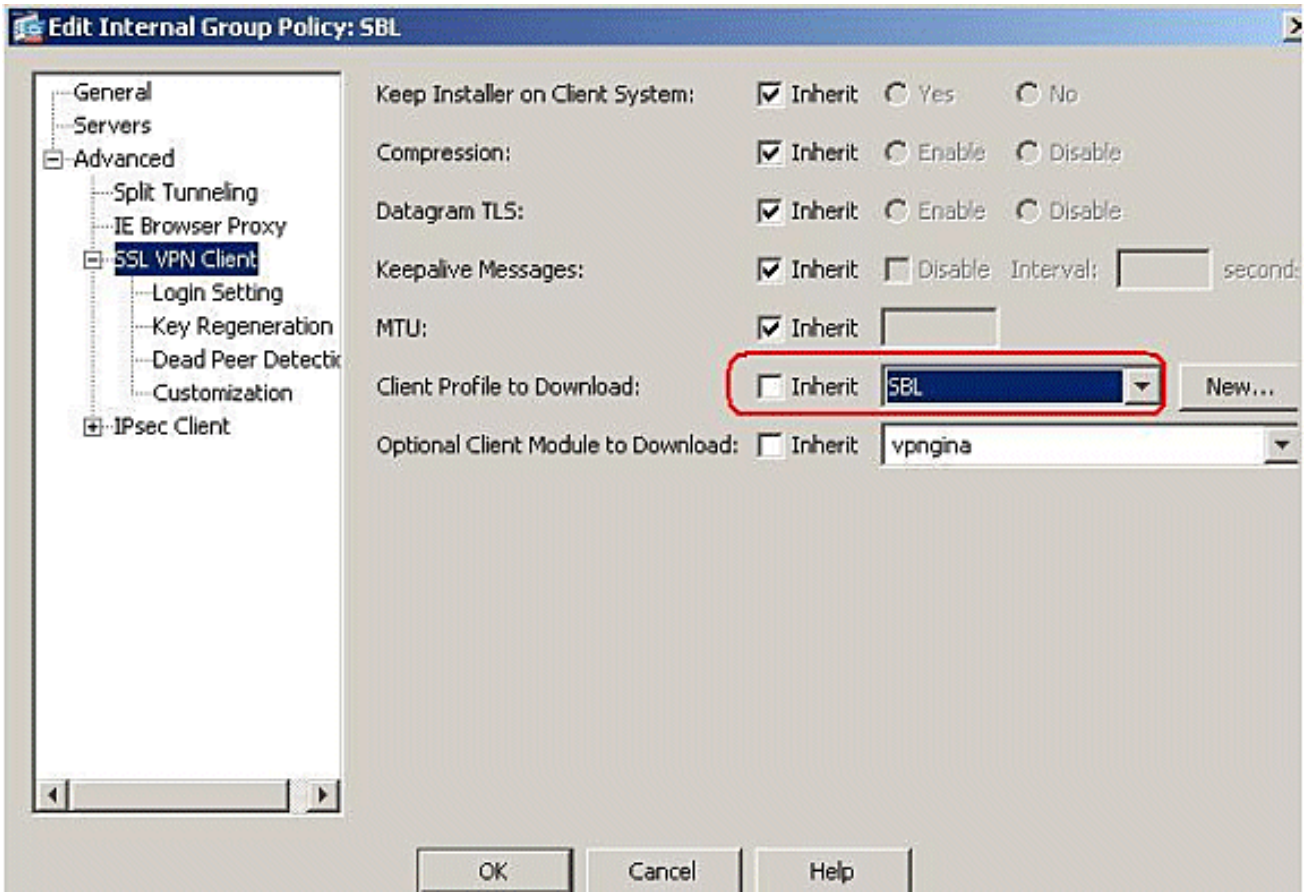
10. Dopo il trasferimento, fare clic sul pulsante **Aggiorna** per verificare se il file del profilo si trova nella memoria
flash.



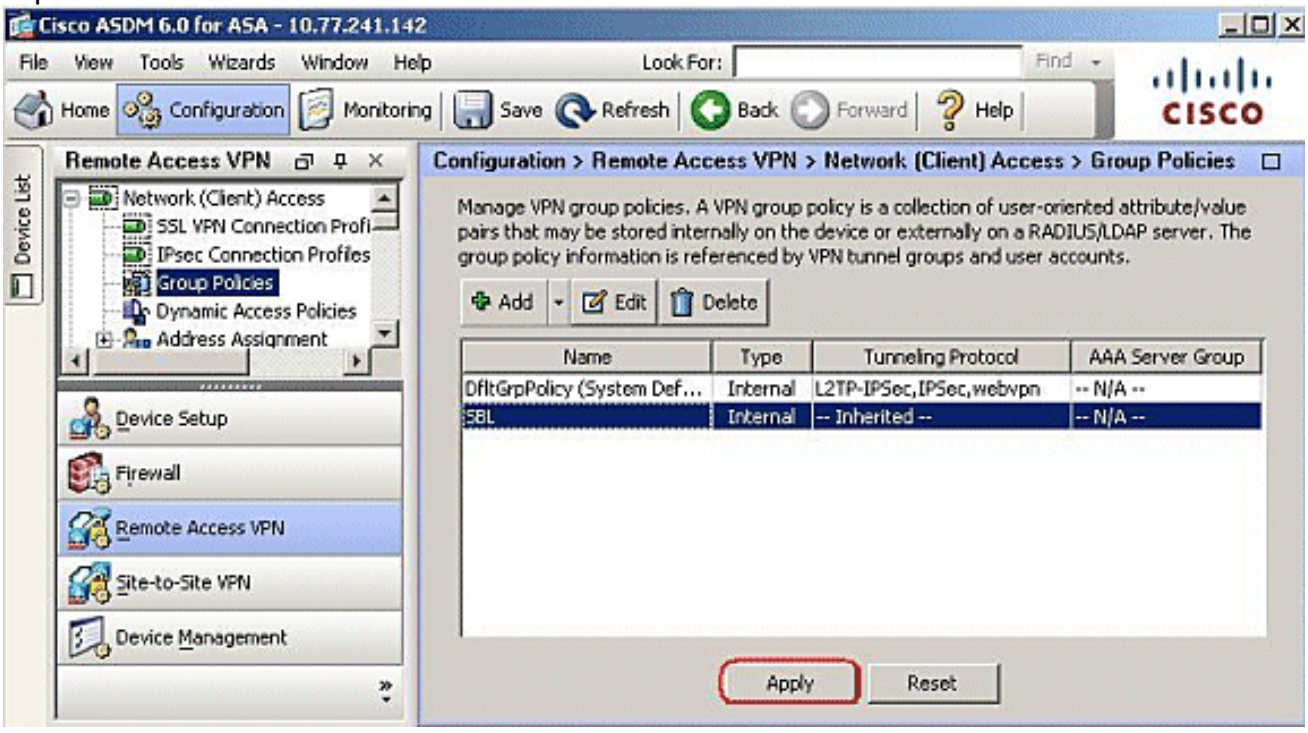
11. Assegnare il profilo ai Criteri di gruppo interni (**SBL**).Seguire questo percorso, **Configurazione > VPN ad accesso remoto > Accesso di rete (client) > Criteri di gruppo > Modifica SBL (Criteri di gruppo interni) > Avanzate > Client VPN SSL > Profilo client da scaricare**, quindi fare clic sul pulsante **Nuovo**.In **Add SSL VPN Client Profiles**, fare clic sul pulsante **Browse** (Sfoglia) per scegliere la posizione del profilo (**AnyConnectProfile.xml**) memorizzato nella memoria flash ASA. Assegnare il **Nome** del profilo, ad esempio **SBL**. Fare clic su **OK** per completare l'operazione.



12. Rimuovere la casella di controllo Eredita e scegliere **SBL** nel campo **Profilo client da scaricare**. Fare clic su
OK.



13. Fare clic su **Apply** (Applica) per completare l'operazione.



Utilizzare il file manifesto

Il pacchetto AnyConnect caricato sull'appliance di sicurezza contiene un file denominato VPNManifest.xml. Nell'esempio viene mostrato un contenuto di esempio di questo file:

```
<?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>
```

L'appliance di sicurezza ha memorizzato i profili configurati, come spiegato nel passaggio 1, e anche uno o più pacchetti AnyConnect che contengono il client AnyConnect stesso, l'utilità di download, il file manifesto e altri moduli facoltativi o file di supporto.

Quando un utente remoto si connette all'accessorio di protezione tramite WebLaunch o un client autonomo corrente, il downloader viene scaricato per primo ed eseguito. Utilizza il file manifesto per verificare se sul PC dell'utente remoto è presente un client che deve essere aggiornato o se è necessaria una nuova installazione. Il file manifesto contiene inoltre informazioni sull'eventuale presenza di moduli facoltativi da scaricare e installare, in questo caso la VPNGINA. Il profilo del client viene inoltre rimosso dall'appliance di sicurezza. L'installazione di VPNGINA viene attivata dal comando **svc modules value vpngina** configurato nella modalità comando **criteri di gruppo (webvpn)**, come spiegato nel passaggio 4. Il client AnyConnect e VPNGINA vengono installati e l'utente vede il client AnyConnect al successivo riavvio, prima dell'accesso al dominio di Windows.

Quando l'utente si connette, il client e il profilo vengono trasmessi al PC dell'utente; il client e VPNGINA siano installati; e l'utente vede il client AnyConnect al successivo riavvio, prima di accedere.

Quando si installa AnyConnect, sul PC client viene fornito un profilo di esempio: **C:\Documents and Settings\All Users\Applicazione Data\Cisco\Cisco\AnyConnect VPN Client\Profile\AnyConnectProfile**.

Risoluzione dei problemi SBL

Utilizzare questa procedura se si verifica un problema con SBL:

1. Verificare che il profilo sia stato sottoposto a push.
2. Eliminare i profili precedenti; ricercarli sul disco rigido per trovare il percorso: xml
3. Quando si accede a Installazione applicazioni, si dispone sia di un'installazione AnyConnect che di un'installazione AnyConnect VPN?
4. Disinstallare il client AnyConnect.
5. Cancellare il registro AnyConnect dell'utente nel Visualizzatore eventi e riprovare.
6. Per reinstallare il client, tornare all'appliance di sicurezza.
7. Assicurarsi che venga visualizzato anche il profilo.
8. Riavviare una volta. Al successivo riavvio, verrà visualizzato il prompt Avvia prima di accedere.
9. Inviare il registro eventi di AnyConnect a Cisco in formato .evt.
10. Se viene visualizzato questo errore, eliminare il profilo utente e utilizzare quello predefinito:

```
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.
```

Problema 1

Questo messaggio di errore viene visualizzato durante il tentativo di caricare il profilo AnyConnect: `Errore durante la convalida del file XML rispetto allo schema più recente`. Come viene risolto questo errore?

Soluzione 1

Questo messaggio di errore si verifica principalmente a causa di problemi di sintassi o configurazione nel profilo AnyConnect. Per risolvere il problema, verificare che il profilo AnyConnect configurato sia simile al profilo AnyConnect di esempio presente nella sezione Sample AnyConnect Profile and XML Schema della Guida dell'amministratore dei client VPN di Cisco AnyConnect.

Informazioni correlate

- Cisco AnyConnect VPN Client Administrator Guide, versione 2.0
- Creazione di script di accesso - Windows TechNet
- Configurazione di Start Before Logon (PLAP) sui sistemi Windows Vista
- Esempio di configurazione del client VPN AnyConnect SSL con accesso VPN ASA 8.x
- Client VPN di Cisco AnyConnect
- Cisco ASA serie 5500 Adaptive Security Appliance
- Documentazione e supporto tecnico – Cisco Systems