ASA 8.X: Configuração do recurso Iniciar antes do Logon do AnyConnect

Contents

Introduction

Com a opção *Start Before Logon* (SBL) habilitada, o usuário vê a caixa de diálogo de logon da GUI do AnyConnect antes que a caixa de diálogo de logon do Windows® apareça. Isso estabelece a conexão de VPN antes. Disponível somente para plataformas Windows, Start Before Logon permite que o administrador controle o uso de scripts de login, cache de senha, mapeamento de unidades de rede para unidades locais, entre outros. É possível usar o recurso SBL para ativar a VPN como parte da sequência de login. O SBL é desabilitado por padrão.

Para obter mais informações sobre como configurar os recursos do AnyConnect VPN Client, consulte a seção Configuração de recursos do AnyConnect Client.

Observação: no cliente AnyConnect, a única configuração que você faz para SBL é habilitar o recurso. Os administradores de rede lidam com o processamento que ocorre antes do logon com base nos requisitos de sua situação. Os scripts de logon podem ser atribuídos a um domínio ou a usuários individuais. Geralmente, os administradores do domínio têm arquivos em lote ou semelhantes definidos com usuários ou grupos no Ative Diretory. Assim que o usuário faz logon, o script de login é executado.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco ASA 5500 Series Adaptive Security Appliances que executam a versão de software 8.x
- Cisco AnyConnect VPN versão 2.0

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Informações de Apoio

O objetivo do SBL é conectar um computador remoto à infraestrutura da empresa antes de fazer logon no PC. Por exemplo, um usuário pode estar fora da rede corporativa física, incapaz de acessar recursos corporativos até que seu PC tenha ingressado na rede corporativa. Com o SBL ativado, o cliente AnyConnect se conecta antes que o usuário veja a janela de login da Microsoft. O usuário também deve fazer login, como de costume, no Windows quando a janela de login da Microsoft for exibida.

Estes são vários motivos para usar o SBL:

- O PC do usuário está conectado a uma infraestrutura do Ative Diretory.
- O usuário não pode ter credenciais em cache no PC, isto é, se a política de grupo desabilitar credenciais em cache.
- O usuário deve executar scripts de login que são executados a partir de um recurso de rede ou que exigem acesso a um recurso de rede.
- Um usuário tem unidades mapeadas na rede que exigem autenticação com a infraestrutura do Ative Diretory.
- Os componentes de rede, como o MS NAP/CS NAC, podem exigir conexão com a infraestrutura.

O SBL cria uma rede equivalente à inclusão na LAN corporativa local. Com o SBL ativado, como o usuário tem acesso à infraestrutura local, os scripts de login que normalmente são executados para um usuário no escritório também estão disponíveis para o usuário remoto.

Para obter informações sobre como criar scripts de login, consulte este artigo do Microsoft TechNet .

Para obter informações sobre como usar scripts de login local no Windows XP, consulte este artigo da Microsoft.

Em outro exemplo, um sistema pode ser configurado para não permitir credenciais em cache para logon no PC. Neste cenário, os usuários devem ser capazes de se comunicar com um controlador de domínio na rede corporativa para que suas credenciais sejam validadas antes do acesso ao PC. O SBL exige que uma conexão de rede esteja presente no momento em que é chamado. Em alguns casos, isso não é possível porque uma conexão sem fio pode depender das credenciais do usuário para se conectar à infraestrutura sem fio. Como o modo SBL precede a fase de credencial de um login, uma conexão não está disponível neste cenário. Nesse caso, a conexão sem fio precisa ser configurada para colocar as credenciais em cache no login, ou outra autenticação sem fio precisa ser configurada para que o SBL funcione.

Instalar o Start Before Logon Components (Somente Windows)

Os componentes Start Before Logon devem ser instalados depois que o cliente principal tiver sido instalado. Além disso, os componentes Start Before Logon do AnyConnect 2.2 exigem que a versão 2.2 ou posterior do software cliente principal do AnyConnect esteja instalada. Se você pré-implantar o cliente AnyConnect e os componentes Start Before Logon com os arquivos MSI (por exemplo, você está em uma grande empresa que tem sua própria implantação de software (Altiris, Ative Diretory ou SMS), você deve fazer o pedido corretamente. A ordem da instalação é tratada automaticamente quando o administrador carrega o AnyConnect se ele estiver implantado na Web e/ou atualizado na Web. Para obter informações completas sobre a instalação, consulte as Release Notes do Cisco AnyConnect VPN Client, Release 2.2.

Diferenças entre o Windows Vista\Windows 7 e o Pré-Vista começam antes do início da sessão

Os procedimentos para habilitar a SBL diferem ligeiramente nos sistemas Windows Vista e Windows 7. Os sistemas pré-Vista usam um componente chamado de identificação e autenticação gráfica de rede privada virtual (VPNGINA) para implementar o SBL. Os sistemas Vista e Windows 7 usam um componente chamado PLAP para implementar o SBL.

No cliente AnyConnect, o recurso Iniciar antes do login do Windows Vista é conhecido como Provedor de acesso de pré-login (PLAP), que é um provedor de credenciais conectável. Esse recurso permite que os administradores de rede executem tarefas específicas, como a coleta de credenciais ou a conexão com os recursos de rede, antes do login. O PLAP fornece as funções Iniciar antes do Logon no Windows Vista, Windows 7 e Windows 2008 Server. O PLAP suporta versões de 32 e 64 bits do sistema operacional com vpnplap.dll e vpnplap64.dll, respectivamente. A função PLAP suporta as versões x86 e x64 do Windows Vista.

Observação: nesta seção, o VPNGINA refere-se ao recurso Iniciar antes do logon para plataformas anteriores ao Vista e o PLAP refere-se ao recurso Iniciar antes do logon para sistemas Windows Vista e Windows 7.

Nos sistemas pré-Vista, Start Before Logon usa um componente conhecido como VPN Graphical Identification and Authentication Dynamic Link Library (vpngina.dll) para fornecer recursos Start Before Logon (Iniciar antes de fazer logon). O componente Windows PLAP, que faz parte do Windows Vista, substitui o componente Windows GINA.

Uma GINA é ativada quando um usuário pressiona a combinação de teclas Ctrl+Alt+Del. Com o

PLAP, a combinação de teclas Ctrl+Alt+Del abre uma janela na qual o usuário pode optar por fazer login no sistema ou ativar qualquer Conexão de rede (componentes PLAP) com o botão Network Connect (Conexão de rede) no canto inferior direito da janela.

As seções a seguir descrevem as configurações e os procedimentos para VPNGINA e PLAP SBL. Para obter uma descrição completa da ativação e do uso do recurso SBL (PLAP) em uma plataforma Windows Vista, consulte Configuração de Iniciar Antes do Logon (PLAP) em Sistemas Windows Vista.

Configurações XML para ativar SBL

O valor do elemento para UseStartBeforeLogon permite que esse recurso seja ativado (verdadeiro) ou desativado (falso). Se você definir esse valor como **verdadeiro** no perfil, o processamento adicional ocorrerá como parte da sequência de logon. Consulte a descrição Start Before Logon (Iniciar antes do logon) para obter mais detalhes. Defina o valor **<**UseStartBefore Logon**>** no arquivo CiscoAnyConnect.xml como **verdadeiro** para ativar o SBL:

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

Para desabilitar o SBL, defina o mesmo valor como **false**.

Para habilitar o recurso UserControllable, use esta instrução quando habilitar o SBL:

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

Qualquer configuração de usuário associada a este atributo é armazenada em outro lugar.

Habilitar SBL

Para minimizar o tempo de download, o cliente AnyConnect solicita downloads (do Security Appliance) apenas de módulos principais necessários para cada recurso que ele suporta. Para ativar novos recursos, como SBL, você deve especificar o nome do módulo com o comando **svc modules** do modo de configuração WebVPN da política de grupo ou WebVPN do nome de usuário:

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

O valor de string para SBL é **vpngina**.

Neste exemplo, o administrador de rede entra no modo de atributos de política de grupo para os trabalhadores à distância da política de grupo; entra no modo de configuração WebVPN para a política de grupo; e especifica a string VPNGINA para ativar SBL:

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

Além disso, o administrador deve garantir que o arquivo AnyConnect <profile.xml>, em que <profile.xml> é o nome atribuído pelo administrador da rede ao arquivo XML, tenha a instrução <UseStartBeforeLogon> definida como **true**, por exemplo:

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

O sistema deve ser reinicializado antes de Iniciar antes que o Logon entre em vigor. Você também deve especificar no Security Appliance que deseja permitir SBL ou em qualquer outro módulo para recursos adicionais. Consulte a descrição na seção Ativação de módulos para recursos adicionais do AnyConnect, página 2-5 (ASDM) ou Ativação de módulos para recursos adicionais do AnyConnect, página 3-4 (CLI) para obter mais informações.

Iniciar antes da configuração de logon com CLI

Este cenário mostra como configurar o arquivo XML com CLI:

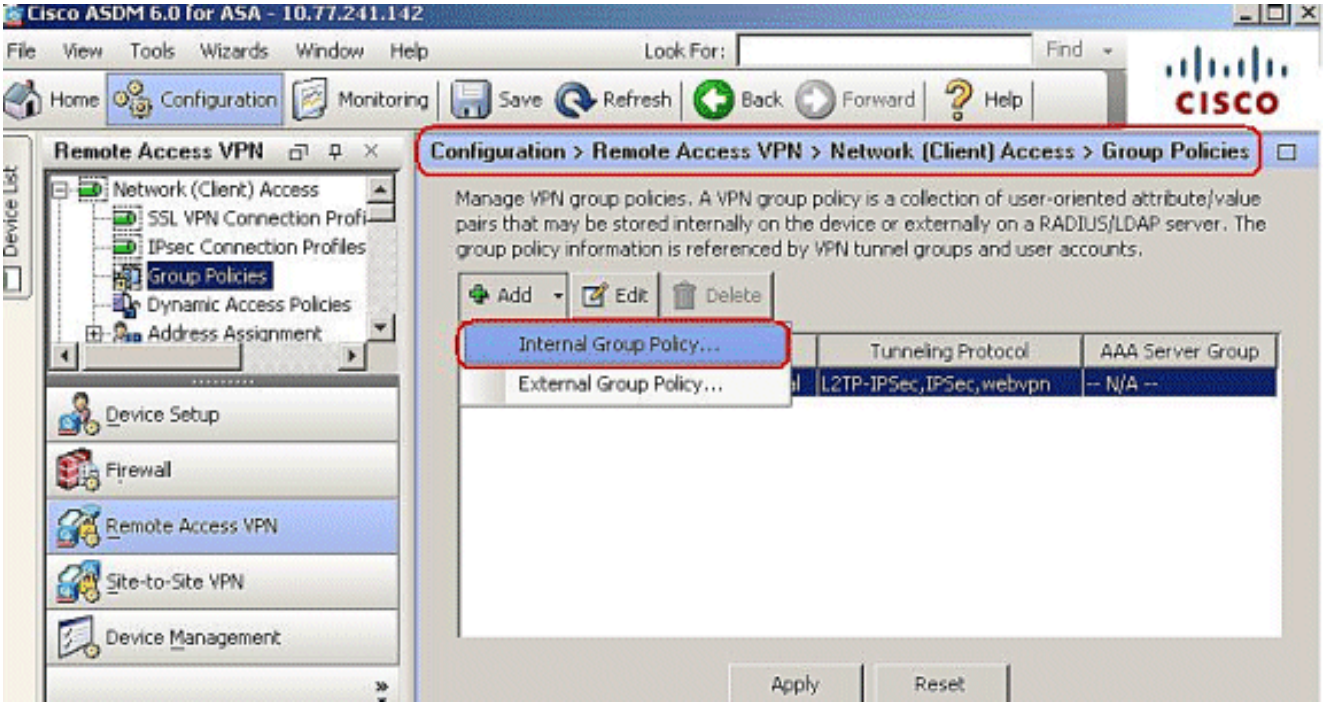
1. Crie um perfil a ser empurrado para os PCs clientes que se pareçam com este:
```
<?xml version="1.0" encoding="UTF-8" ?>
<AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi :schemaLocation=
   "http://schemas.xmlsoap.org/encoding/ 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. Copie o arquivo para o Flash no Security Appliance:
```
Copy tftp://x.x.x.x/AnyConnectProfile.xml AnyConnectProfile.xml
```
3. No Security Appliance, adicione o perfil como um perfil disponível à seção global do WebVPN, desde que tudo o resto esteja configurado corretamente para conexões do AnyConnect:
```
hostname(config-group-policy)# webvpn
hostame(config-group-webvpn)#
   svc profiles ReallyNewProfile disk0:/AnyConnectProfile.xml
```
4. Edite a política de grupo que você usa e adicione os **módulos svc** e os comandos **svc profile**:
```
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
```

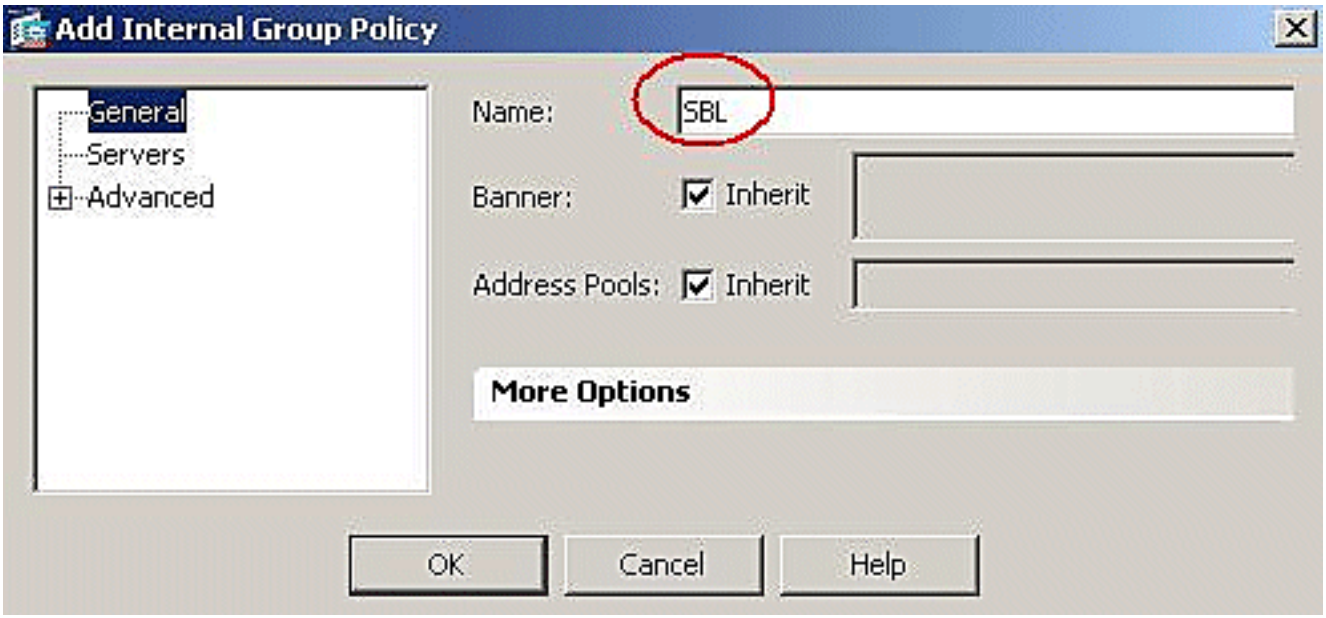
Iniciar antes da configuração de logon com o ASDM

Conclua estes passos para configurar o SBL com ASDM:

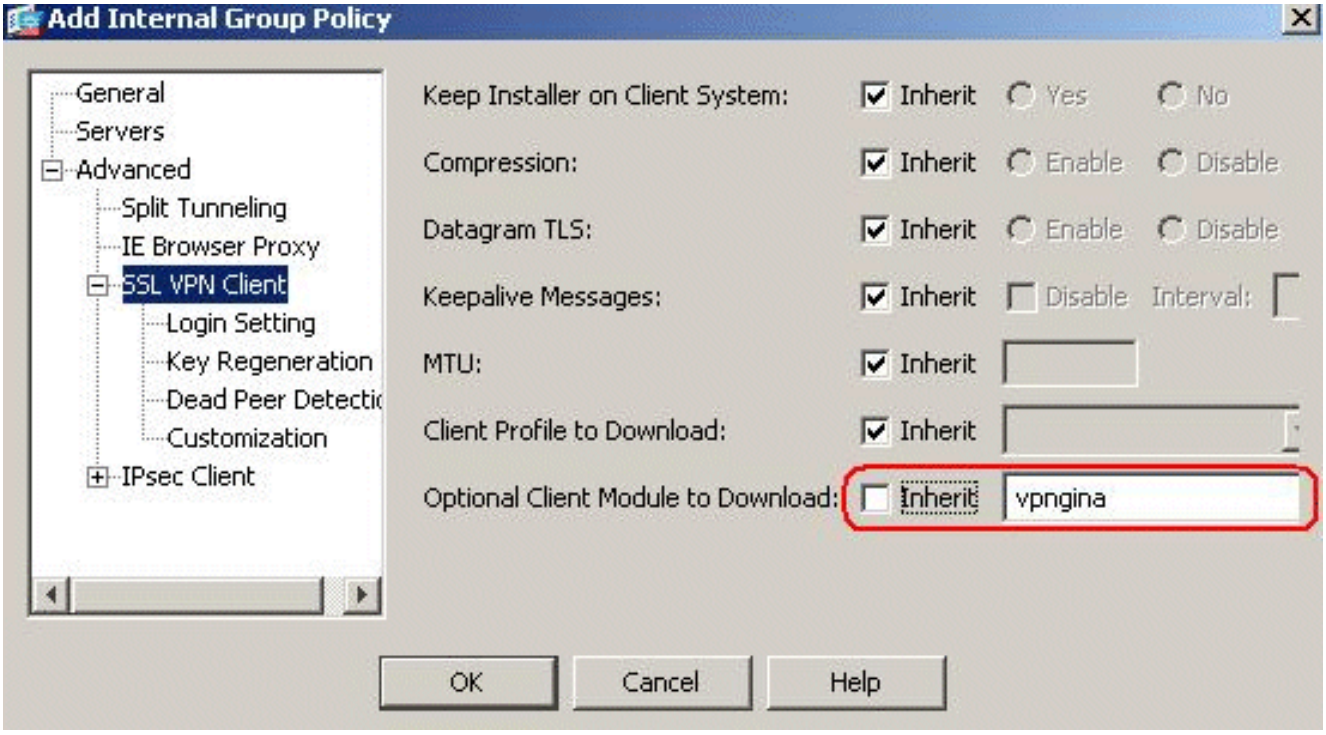
1. Crie um perfil a ser empurrado para os PCs clientes que se pareçam com este:
```
<?xml version="1.0" encoding="UTF-8" ?>
<AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi :schemaLocation=
   "http://schemas.xmlsoap.org/encoding/ 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. Salve o perfil como **AnyConnectProfile.xml** no computador local.
3. Inicie o ASDM e vá para a página inicial.
4. Vá para **Configuration > Remote Access VPN > Network (Client) Access > Group Policies > Add** e clique em **Internal Group Policy**.



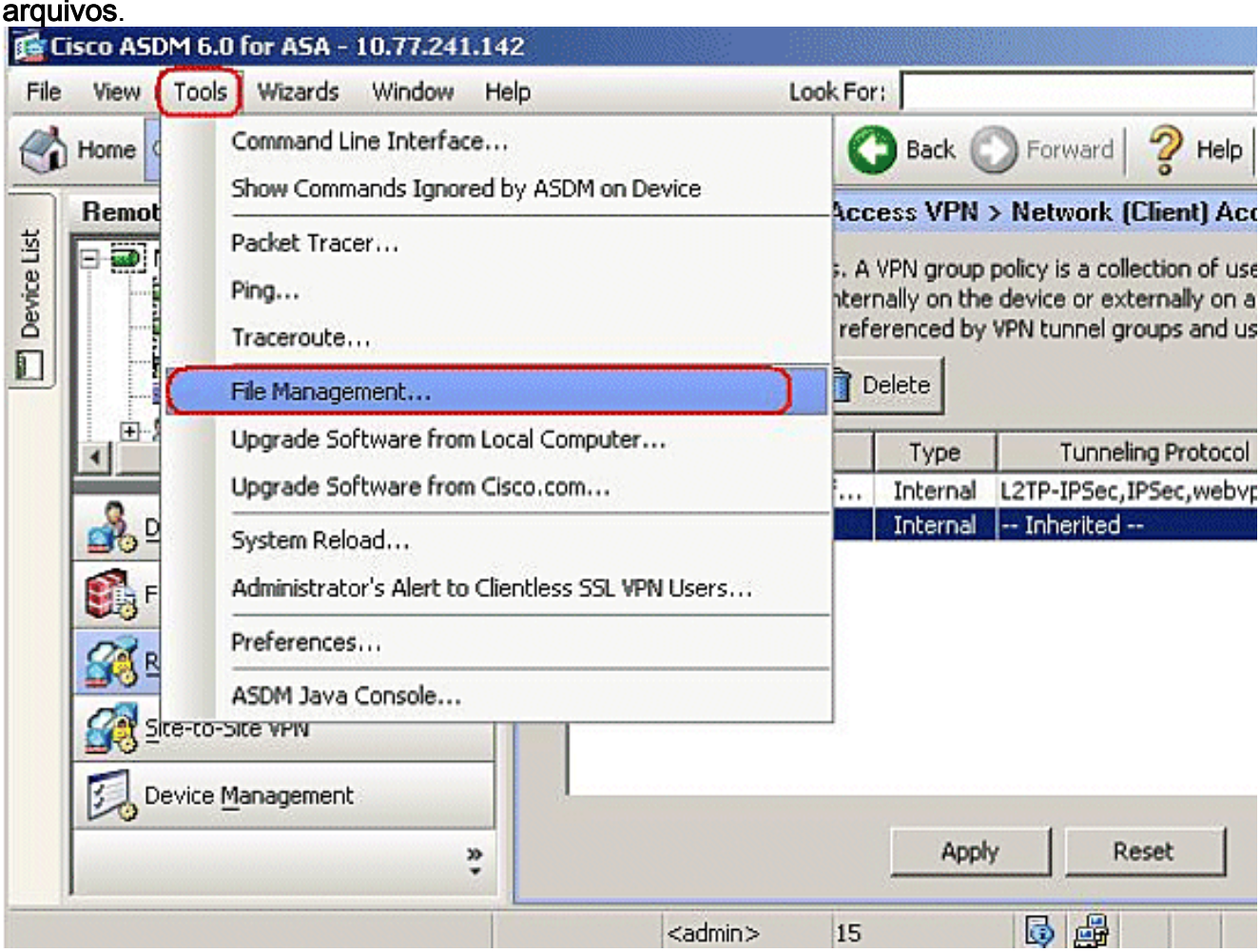
5. Digite o nome da política de grupo, por exemplo, **SBL**.



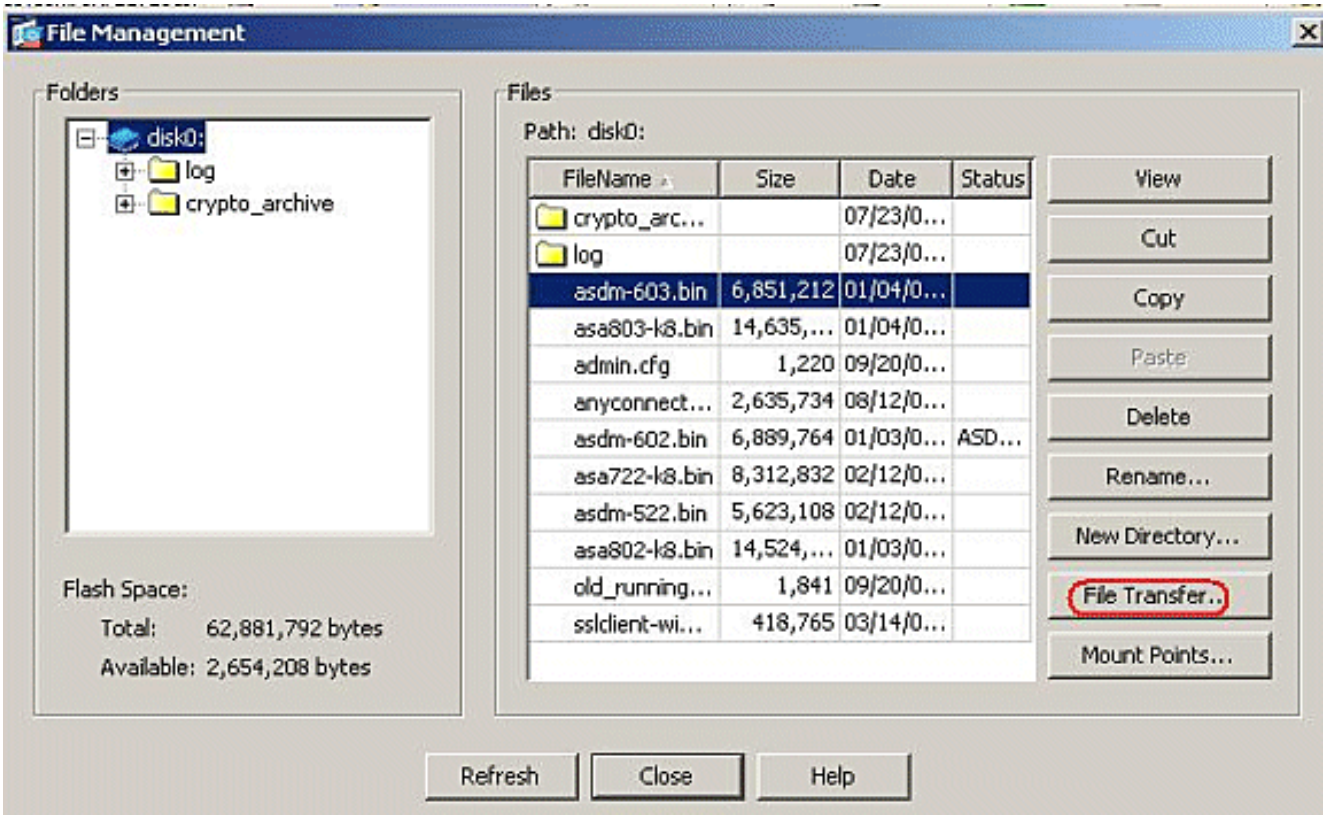
6. Vá para **Advanced > SSL VPN Client**. Remova a marca de seleção Herdar no **Módulo cliente opcional para download** e escolha **vpngina** na caixa suspensa.



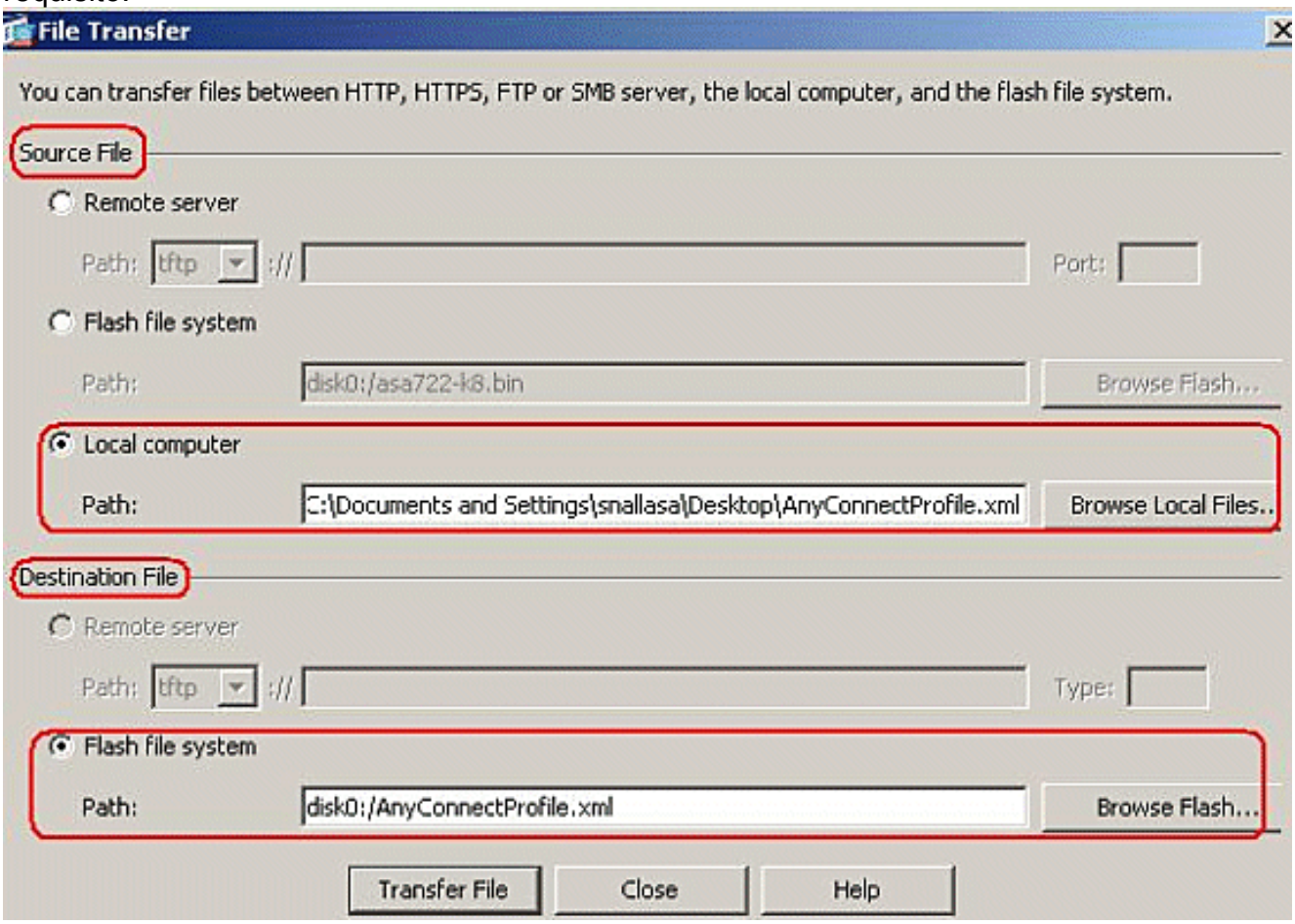
7. Para transferir o perfil **AnyConnectProfile.xml** do computador local para Flash, vá para **Ferramentas** e clique em **Gerenciamento de arquivos**.



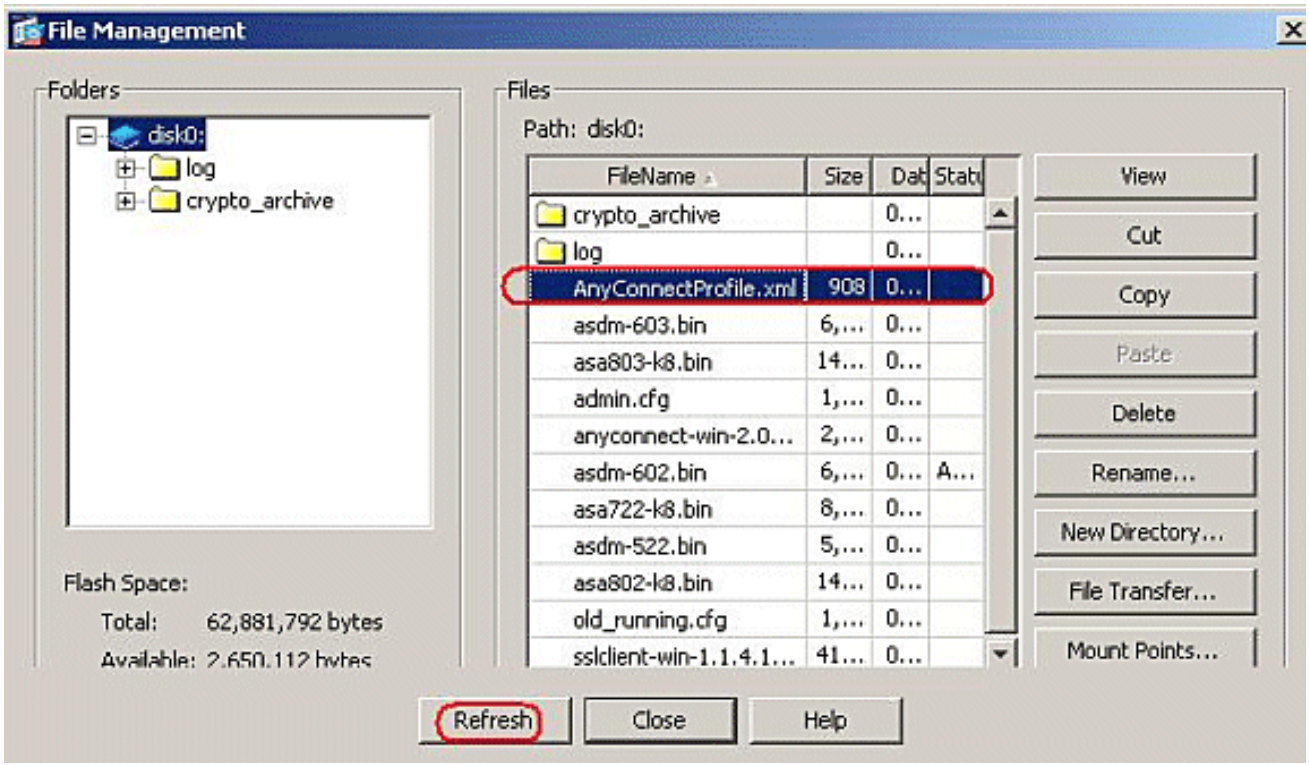
8. Clique no botão **Transferência de arquivo**.



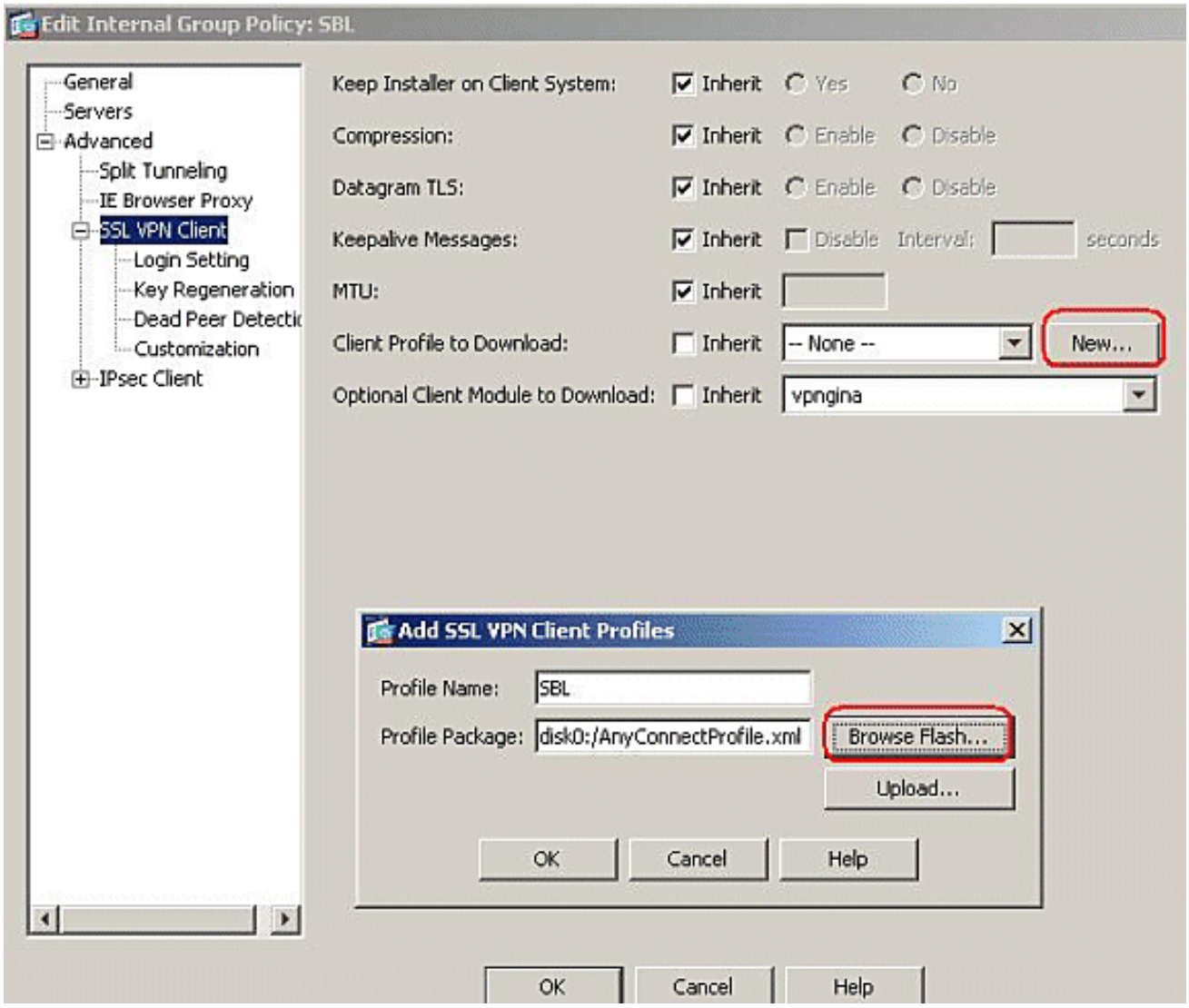
9. Para transferir o perfil do computador local para a memória Flash ASA, escolha o **Arquivo de Origem**, o caminho do arquivo XML (computador local) e o caminho **Arquivo de Destino** conforme o seu
requisito.



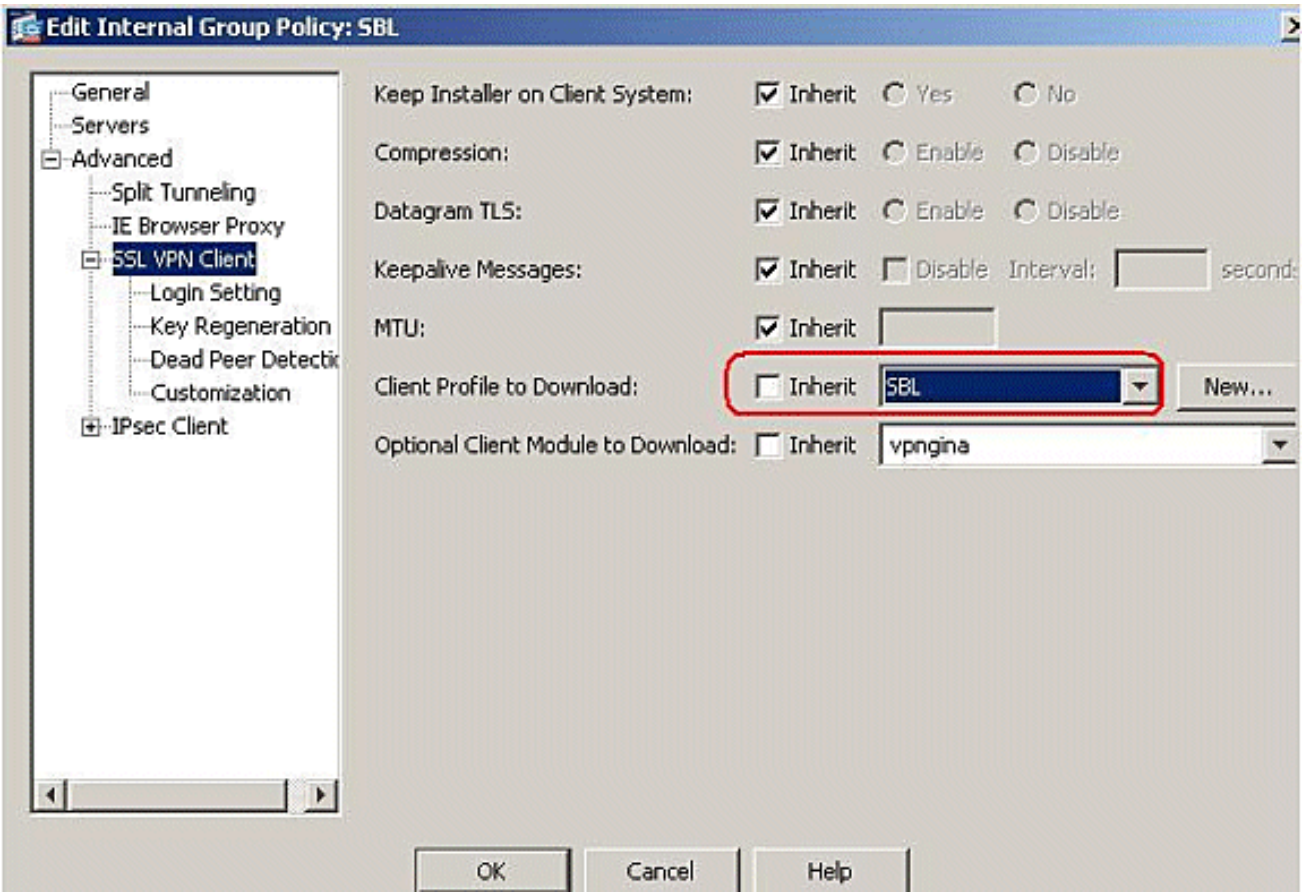
10. Após a transferência, clique no botão **Atualizar** para verificar se o arquivo de perfil está na memória
Flash.



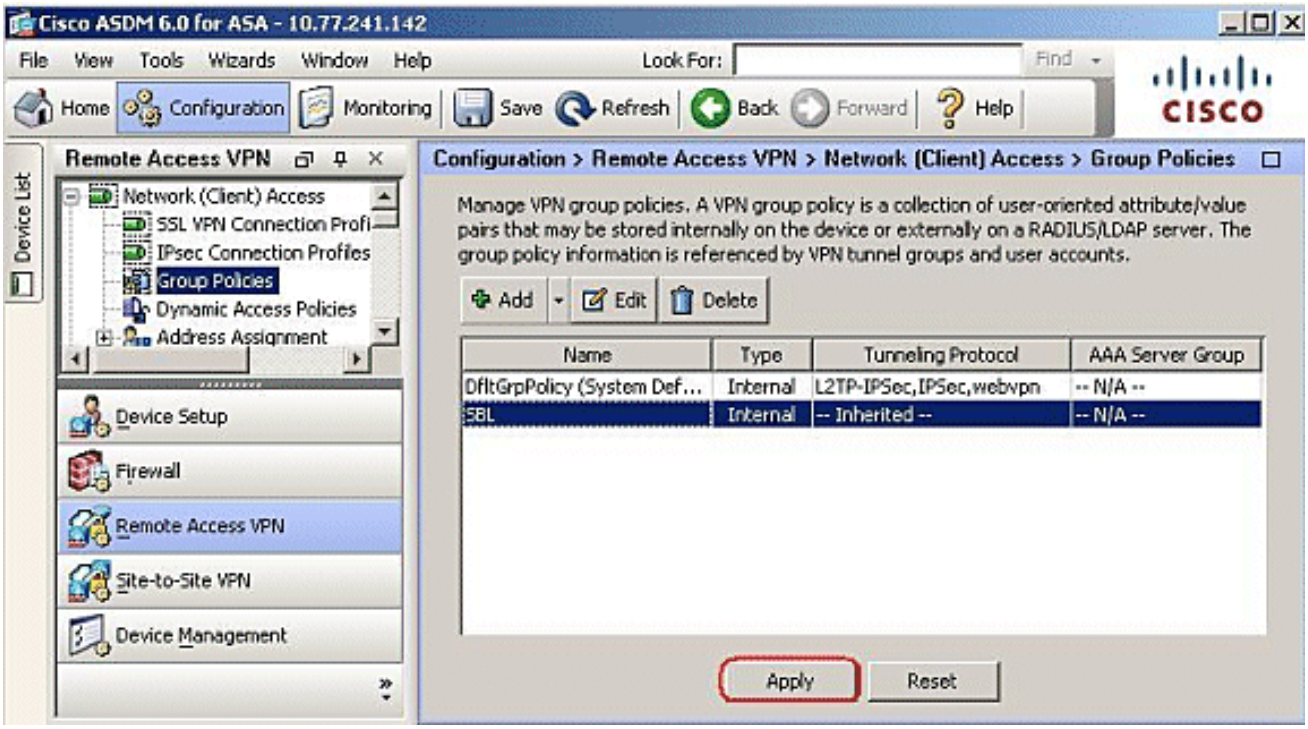
11. Atribua o perfil à política interna do grupo (**SBL**).Siga este caminho, **Configuration > Remote Access VPN > Network (Client) Access > Group Policies > Edit SBL (Internal Group Policy) > Advanced > SSL VPN Client > Client Profile to Download**, e clique no botão **New**.Em **Add SSL VPN Client Profiles**, clique no botão **Browse** para escolher o local do perfil (**AnyConnectProfile.xml**) armazenado na memória Flash do ASA. Atribua o **nome** do perfil, por exemplo, **SBL**. Clique em **OK** para concluir.



12. Remova a caixa de seleção Herdar e escolha **SBL** no campo **Perfil do cliente para download**. Click
OK.



13. Clique em **Apply** para concluir.



Usar o arquivo de manifesto

O pacote do AnyConnect que é carregado no Security Appliance contém um arquivo chamado VPNManifest.xml. Este exemplo mostra um conteúdo de exemplo deste arquivo:

```
<?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>
```

O Security Appliance armazenou em perfis configurados, como explicado na Etapa 1, e também armazena um ou vários pacotes do AnyConnect que contêm o próprio cliente do AnyConnect, o utilitário de download, o arquivo de manifesto e qualquer outro módulo opcional ou arquivo de suporte.

Quando um usuário remoto se conecta ao Security Appliance com WebLaunch ou um cliente autônomo atual, o download é feito primeiro e executado. Ele usa o arquivo de manifesto para verificar se há um cliente atual no PC do usuário remoto que precisa ser atualizado ou se uma nova instalação é necessária. O arquivo de manifesto também contém informações sobre se há módulos opcionais que devem ser baixados e instalados, neste caso, o VPNGINA. O perfil do cliente também é removido do Security Appliance. A instalação do VPNGINA é ativada pelo comando **svc modules value vpngina** configurado no modo de comando **group-policy (webvpn)** como explicado na Etapa 4. O cliente AnyConnect e o VPNGINA estão instalados, e o usuário vê o AnyConnect Client na próxima reinicialização, antes do login de domínio do Windows.

Quando o usuário se conecta, o cliente e o perfil são passados para o PC do usuário; O cliente e o VPNGINA estão instalados; e o usuário vê o cliente AnyConnect na próxima reinicialização, antes do login.

Um exemplo de perfil é fornecido no PC cliente quando o AnyConnect está instalado: **C:\Documents and Settings\All Users\Application Data\Cisco\Cisco\AnyConnect VPN Client\Profile\AnyConnectProfile**.

Solucionar problemas de SBL

Use este procedimento se encontrar um problema com o SBL:

1. Verifique se o perfil foi impresso.
2. Excluir perfis anteriores; procure-os no disco rígido para encontrar o local: *.xml.
3. Quando você vai para Adicionar/remover programas, você tem uma instalação do AnyConnect e do AnyConnect VPNGINA?
4. Desinstale o cliente AnyConnect.
5. Limpe o log do AnyConnect do usuário no Visualizador de eventos e teste novamente.
6. Navegue na Web novamente até o Security Appliance para reinstalar o cliente.
7. Verifique se o perfil também é exibido.
8. Reinicialize uma vez. Na próxima reinicialização, você será solicitado a exibir o prompt Iniciar antes do logon.
9. Envie o registro de eventos do AnyConnect para a Cisco no formato .evt .
10. Se esse erro for exibido, exclua o perfil de usuário e use o perfil padrão:

    ```
    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

Esta mensagem de erro é exibida ao tentar carregar o perfil do AnyConnect: `Erro ao validar o arquivo XML no esquema mais recente`. Como solucionar esse erro?

Solução 1

Essa mensagem de erro ocorre principalmente devido a problemas de sintaxe ou configuração no perfil do AnyConnect. Para resolver esse problema, certifique-se de que o perfil do AnyConnect configurado seja semelhante ao perfil do AnyConnect de amostra presente na seção Perfil do AnyConnect e Esquema XML do Cisco AnyConnect VPN Client Administrator Guide.

Informações Relacionadas

- Guia do administrador do Cisco AnyConnect VPN Client, versão 2.0
- Criando scripts de login - Windows TechNet
- Configurando o Iniciar Antes do Logon (PLAP) em Sistemas Windows Vista
- Exemplo de configuração do ASA 8.x VPN Access com o AnyConnect SSL VPN Client
- Cisco AnyConnect VPN Client
- Dispositivos de segurança adaptáveis Cisco ASA 5500 Series
- Suporte Técnico e Documentação - Cisco Systems