ASA 8.X: Começo de AnyConnect antes da configuração da característica do fazer logon

Índice

Introdução

Com *começo antes do fazer logon* (SBL) permitido, o usuário vê o diálogo de fazer logon de AnyConnect GUI antes que a caixa de diálogo do fazer logon do ® de 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 de configurar características do cliente VPN de AnyConnect, refira a seção que configura recursos de cliente de AnyConnect.

Nota: Dentro do cliente de AnyConnect, a única configuração que você faz para SBL é permitir a característica. Os administradores de rede seguram o processamento isso vão sobre antes do fazer logon baseado nas exigências de sua situação. Os scripts de logon podem ser atribuídos a um domínio ou aos usuários individuais. Geralmente, os administradores do domínio têm arquivos de lote ou The Like definido com usuários ou grupos no diretório ativo. Assim que o usuário entrar, o script do início de uma sessão está executado.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

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

- Dispositivos de segurança adaptáveis Cisco ASA série 5500 essa versão de software 8.x da corrida
- Versão de VPN 2.0 de Cisco AnyConnect

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

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

Informações de Apoio

O ponto de SBL é que conecta um computador remoto à infraestrutura da empresa antes do fazer logon ao PC. Por exemplo, um usuário pode ser fora da rede corporativa física, incapaz de alcançar recursos corporativos até que seu PC se junte à rede corporativa. Com o SBL permitido, o cliente de AnyConnect conecta antes que o usuário ver o indicador do início de uma sessão de Microsoft. O usuário deve igualmente entrar, como de costume, a Windows quando Microsoft entra o indicador aparece.

Estas são diversas razões usar SBL:

- O PC do usuário é juntado a uma infraestrutura do diretório ativo.
- O usuário não pode ter credenciais em cache no PC, isto é, se a política do grupo recusa credenciais em cache.
- O usuário deve executar os scripts do início de uma sessão que executam de uns recursos de rede ou que exigem o acesso a uns recursos de rede.
- Um usuário rede-traçou as movimentações que exigem a autenticação com a infraestrutura do diretório ativo.
- Os componentes de rede de comunicação, tais como MS NAP/CS NAC, podem exigir a conexão à infraestrutura.

SBL cria uma rede que seja equivalente à inclusão na LAN corporativa local. Com o SBL permitido, desde que o usuário tem o acesso à infraestrutura local, os scripts de logon que são executado normalmente para um usuário no escritório estão igualmente disponíveis ao usuário remoto.

Para obter informações sobre de como criar scripts de logon, refira este artigo do Microsoft TechNet .

Para obter informações sobre de como usar scripts de logon locais em Windows XP, refira este artigo Microsoft .

Em um outro exemplo, um sistema pode ser configurado para recusar credenciais em cache para o fazer logon ao PC. Nesta encenação, os usuários devem poder comunicar-se com um controlador de domínio na rede corporativa para que suas credenciais sejam validadas antes do acesso ao PC. SBL exige uma conexão de rede esta presente então é invocado. Em alguns casos, isto não é possível porque uma conexão Wireless pode depender das credenciais do usuário para conectar ao infraestrutura Wireless. Desde que o modo SBL precede a fase credencial de um início de uma sessão, uma conexão não está disponível nesta encenação. Neste caso, a conexão Wireless precisa de ser configurada para pôr em esconderijo as credenciais através do início de uma sessão, ou uma outra autenticação wireless precisa de ser configurada para que SBL trabalhe.

Instale o começo antes dos componentes do fazer logon (Windows somente)

O começo antes que os componentes do fazer logon deverem ser instalados depois que o cliente do núcleo esteve instalado. Adicionalmente, o começo de AnyConnect 2.2 antes que os componentes do fazer logon exijam essa versão 2.2, ou mais tarde, do software do cliente de AnyConnect do núcleo seja instalado. Se você PRE-distribui o cliente de AnyConnect e o começo antes dos componentes do fazer logon com os arquivos MSI (por exemplo, você está em uma empresa grande que tenha sua própria distribuição de software (Altiris, diretório ativo, ou SMS), você deve obter o direito da ordem. A ordem da instalação está segurada automaticamente quando o administrador carrega AnyConnect se é Web distribuída e/ou Web actualizada. Para a informação de instalação completa, refira Release Note para o Cisco AnyConnect VPN Client, a liberação 2.2.

As diferenças entre Windows Vista \ Windows 7 e PRE-vista começam antes do fazer logon

Os procedimentos para permitir SBL diferem levemente em sistemas de Windows Vista e de Windows 7. Os sistemas da PRE-vista usam um componente chamado a identificação da rede privada virtual e a autenticação gráficas (VPNGINA) para executar SBL. Os sistemas da vista e do Windows 7 usam um componente chamado PLAP para executar SBL.

No cliente de AnyConnect, o começo de Windows Vista antes que a característica do fazer logon estiver sabida como o provedor de acesso do PRE-início de uma sessão (PLAP), que é um fornecedor credencial ajustável. Esta característica deixa administradores de rede executar tarefas específicas, tais como a coleção das credenciais ou da conexão aos recursos de rede, antes do início de uma sessão. PLAP fornece o começo antes das funções do fazer logon em Windows Vista, em Windows 7 e no server de Windows 2008. PLAP suporta versões de 32 bits e 64-bit do sistema operacional com vpnplap.dll e vpnplap64.dll, respectivamente. A função PLAP suporta as versões x86 e x64 de Windows Vista.

Nota: Nesta seção, VPNGINA refere o começo antes da característica do fazer logon para Plataformas da PRE-vista, e PLAP refere o começo antes da característica do fazer logon para sistemas de Windows Vista e de Windows 7.

Em sistemas da PRE-vista, comece antes do fazer logon usa um componente conhecido como a biblioteca de link dinâmico gráfica da identificação e da autenticação VPN (vpngina.dll) para fornecer o começo antes das capacidades do fazer logon. O componente de Windows PLAP, que é parte de Windows Vista, substitui o componente de Windows GINA.

UMA GINA é ativada quando um usuário pressiona a combinação chave Ctrl+Alt+Del. Com PLAP, a combinação chave Ctrl+Alt+Del abre um indicador onde o usuário possa escolher entrar ao sistema ou ativar todas as conexões de rede (componentes PLAP) com o botão connect da rede no canto inferior direito do indicador.

As seções que seguem imediatamente descrevem os ajustes e os procedimentos para VPNGINA e PLAP SBL. Para uma descrição completa da habilitação e o uso da característica SBL (PLAP) em uma plataforma de Windows Vista, refira configurar o começo antes do fazer logon (PLAP) em sistemas de Windows Vista.

Ajustes XML para permitir SBL

O valor do elemento para UseStartBeforeLogon permite que esta característica seja girada em (verdadeiro) ou fora (falso). Se você ajusta este valor **para retificar no** perfil, o processamento adicional ocorre como parte da sequência do fazer logon. Veja o começo antes da descrição do fazer logon para detalhes adicionais. Ajuste o <UseStartBefore Logon> que o valor no arquivo CiscoAnyConnect.xml ao trueto permite SBL:

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

A fim desabilitar SBL, ajuste o mesmo valor a **falso**.

A fim permitir a característica de UserControllable, use esta indicação quando você permite SBL:

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

Toda a configuração de usuário associada com este atributo é armazenada em outra parte.

Permita SBL

A fim minimizar o tempo de download, os pedidos do cliente de AnyConnect transferem (da ferramenta de segurança) somente dos módulos centrais aquele que precisa para cada característica que apoia. A fim permitir novos recursos, tais como SBL, você deve especificar o nome do módulo com o comando dos **módulos svc da** política WebVPN do grupo ou do modo de configuração username WebVPN:

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

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

Neste exemplo, o administrador de rede entra no modo dos atributos da grupo-política para os trabalhadores à distância da política do grupo; incorpora o modo de configuração WebVPN para a política do grupo; e especifica a corda VPNGINA para permitir SBL:

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

Além, o administrador deve assegurar-se de que o arquivo de AnyConnect <profile.xml>, onde <profile.xml> é o nome que o administrador de rede atribuiu ao arquivo XML, tenha a indicação do <UseStartBeforeLogon> ajustada para retificar, **por exemplo**:

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

O sistema deve ser recarregado antes que o começo antes do fazer logon tome o efeito. Você deve igualmente especificar na ferramenta de segurança que você quer permitir SBL, ou em todos os outros módulos para recursos adicionais. Refira a descrição nos módulos de possibilidade para características adicionais de AnyConnect, pagine 2-5 a seção (ASDM) ou permitindo os módulos para características adicionais de AnyConnect, pagine 3-4 (CLI) para mais informação.

Comece antes da configuração do fazer logon com CLI

Esta encenação mostra-lhe como estabelecer o arquivo XML com CLI:

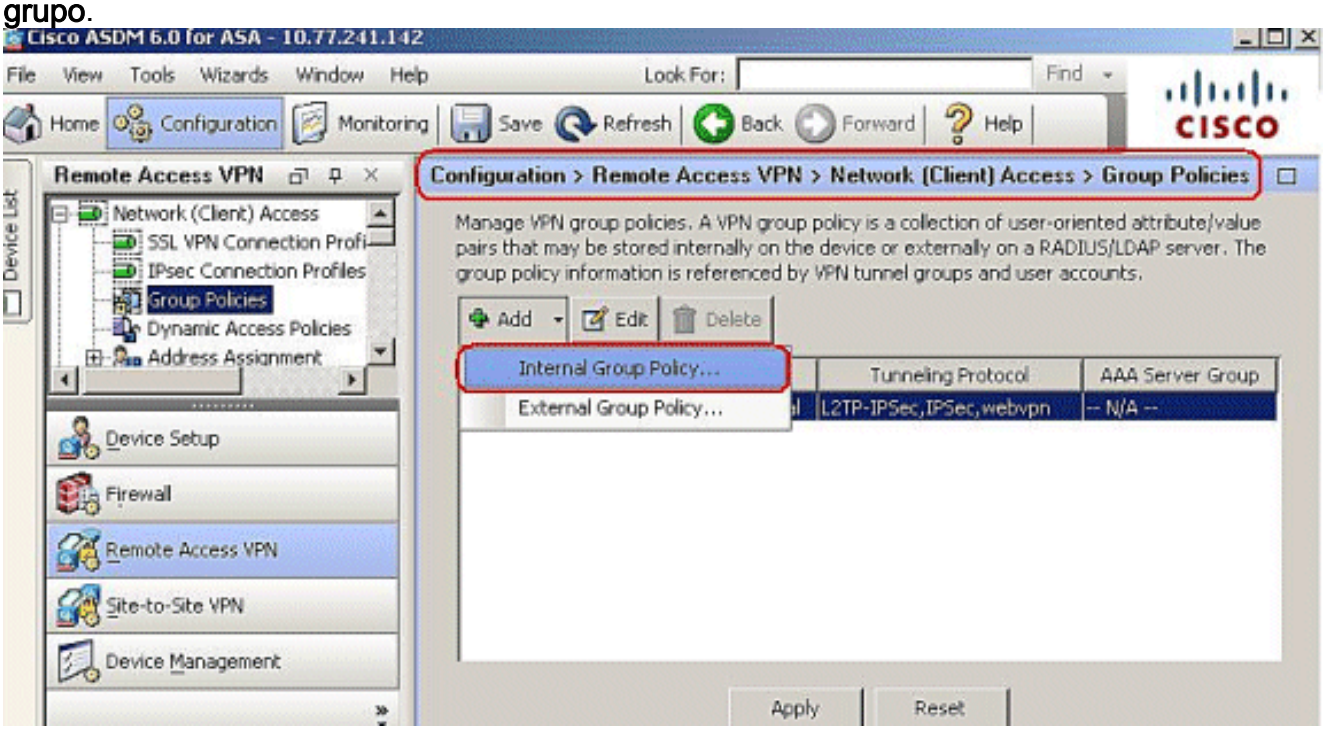
1. Crie um perfil a ser abaixado para o cliente PC que olha similar a este:
```
<?xml version="1.0" encoding="UTF-8" ?>
<AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi :schemaLocation=
   "http://schemas.xmlsoap.org/encoding/ AnyConnectProfile.xsd">
<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 ao flash na ferramenta de segurança:
```
Copy tftp://x.x.x.x/AnyConnectProfile.xml AnyConnectProfile.xml
```
3. Na ferramenta de segurança, adicionar o perfil como um perfil disponível à seção global WebVPN, enquanto tudo mais se estabelece corretamente para conexões de AnyConnect:
```
hostname(config-group-policy)# webvpn hostame(config-group-webvpn)# svc profiles ReallyNewProfile disk0:/AnyConnectProfile.xml
```
4. Edite a política do grupo que você uso, e adiciona os **módulos svc** e **comandos profile**

   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
```

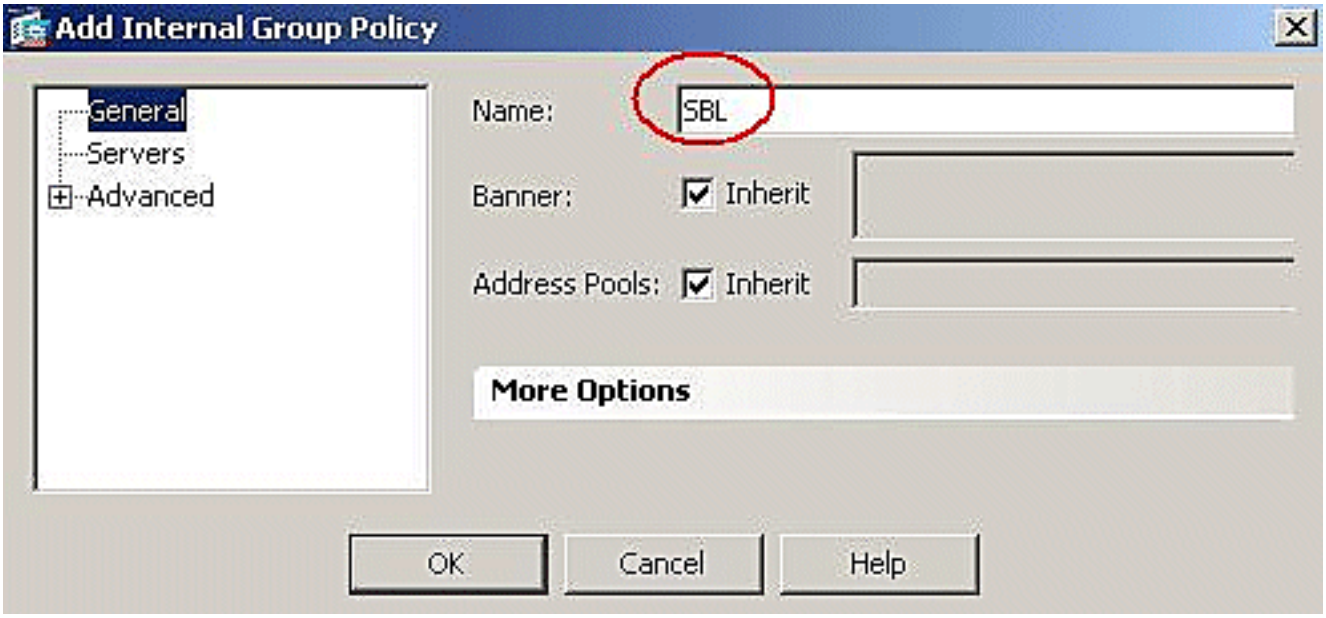
Comece antes da configuração do fazer logon com ASDM

Termine estas etapas para configurar o SBL com ASDM:

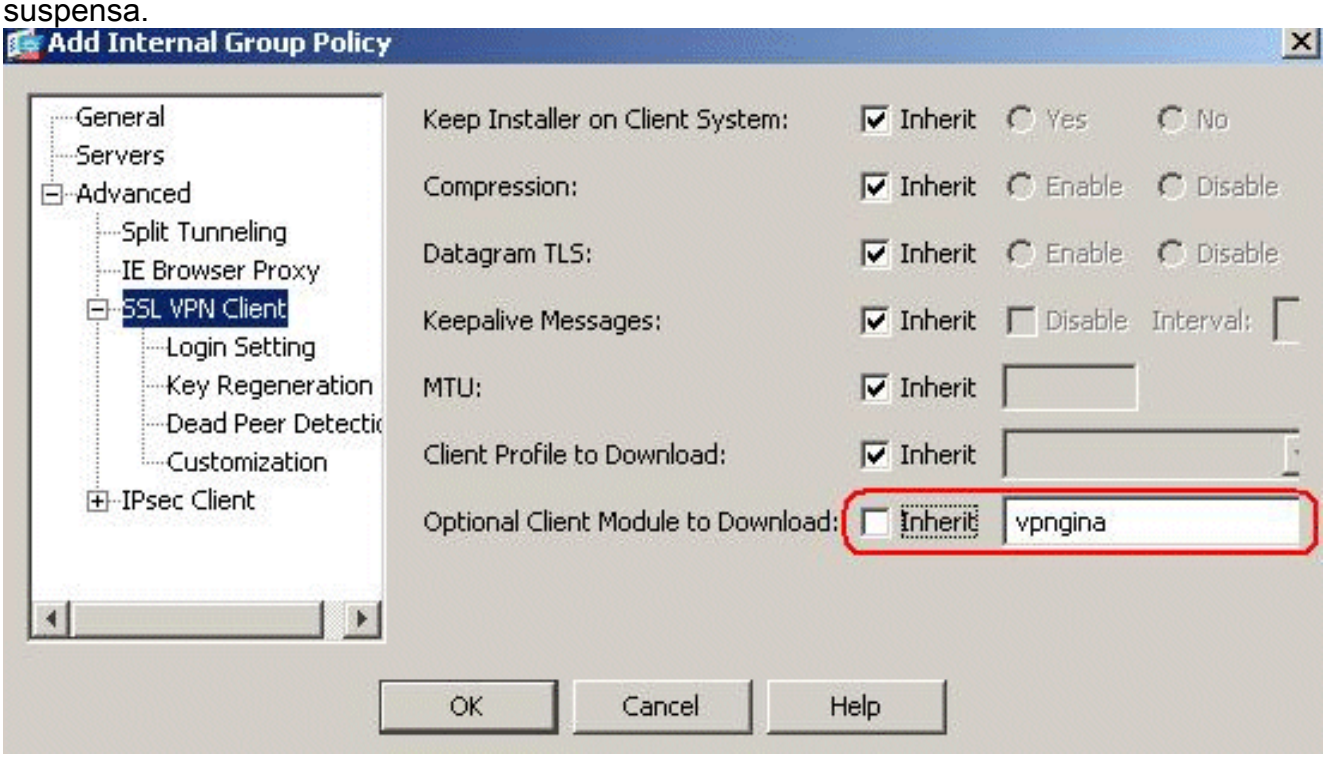
1. Crie um perfil a ser abaixado para o cliente PC que olha similar a este:
```
<?xml version="1.0" encoding="UTF-8" ?>
<AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi :schemaLocation=
   "http://schemas.xmlsoap.org/encoding/ AnyConnectProfile.xsd">
<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. Salvar o perfil como **AnyConnectProfile.xml no** computador local.
3. Lance o ASDM, e vá ao Home Page.
4. Vai à **configuração > ao acesso remoto VPN > ao acesso > ao grupo da rede (cliente) o > Add das políticas**, e clica a **Política interna de grupo**.



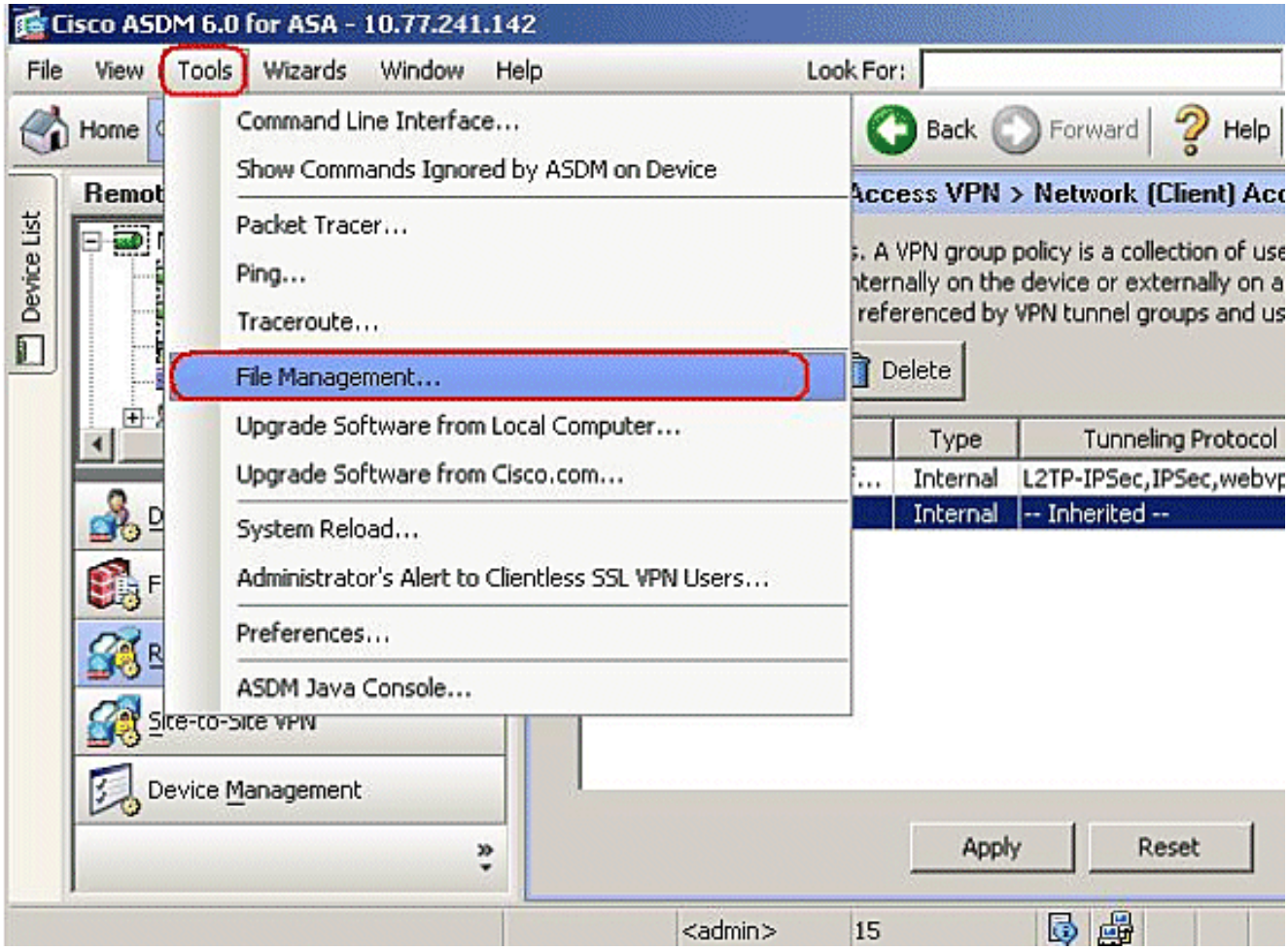
5. Dê entrada com o nome da política do grupo, por exemplo, **SBL**.



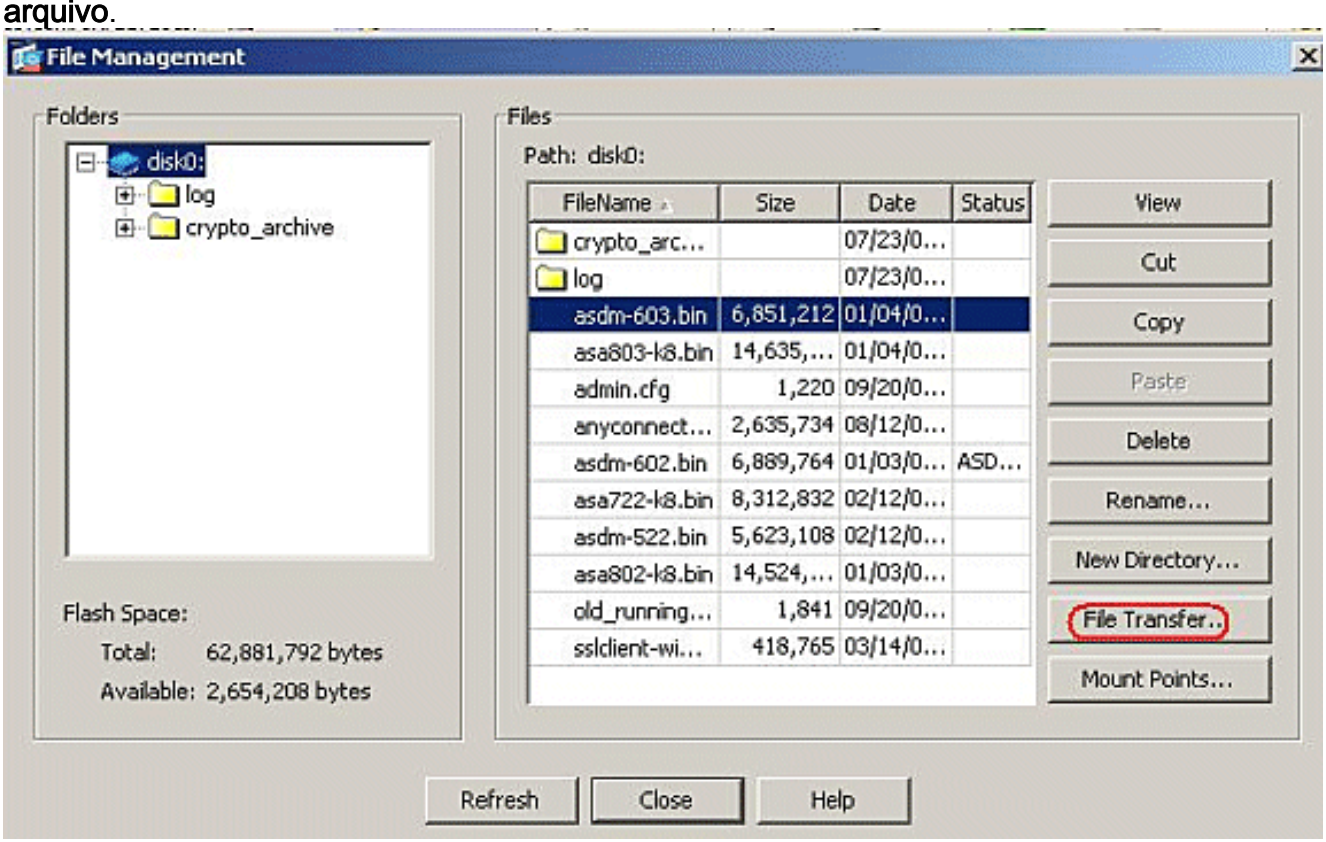
6. Vai a **avançado > o cliente VPN SSL**. Remova a marca de verificação herdar no **módulo cliente opcional para transferir**, e escolha o **vpngina da** caixa suspensa.



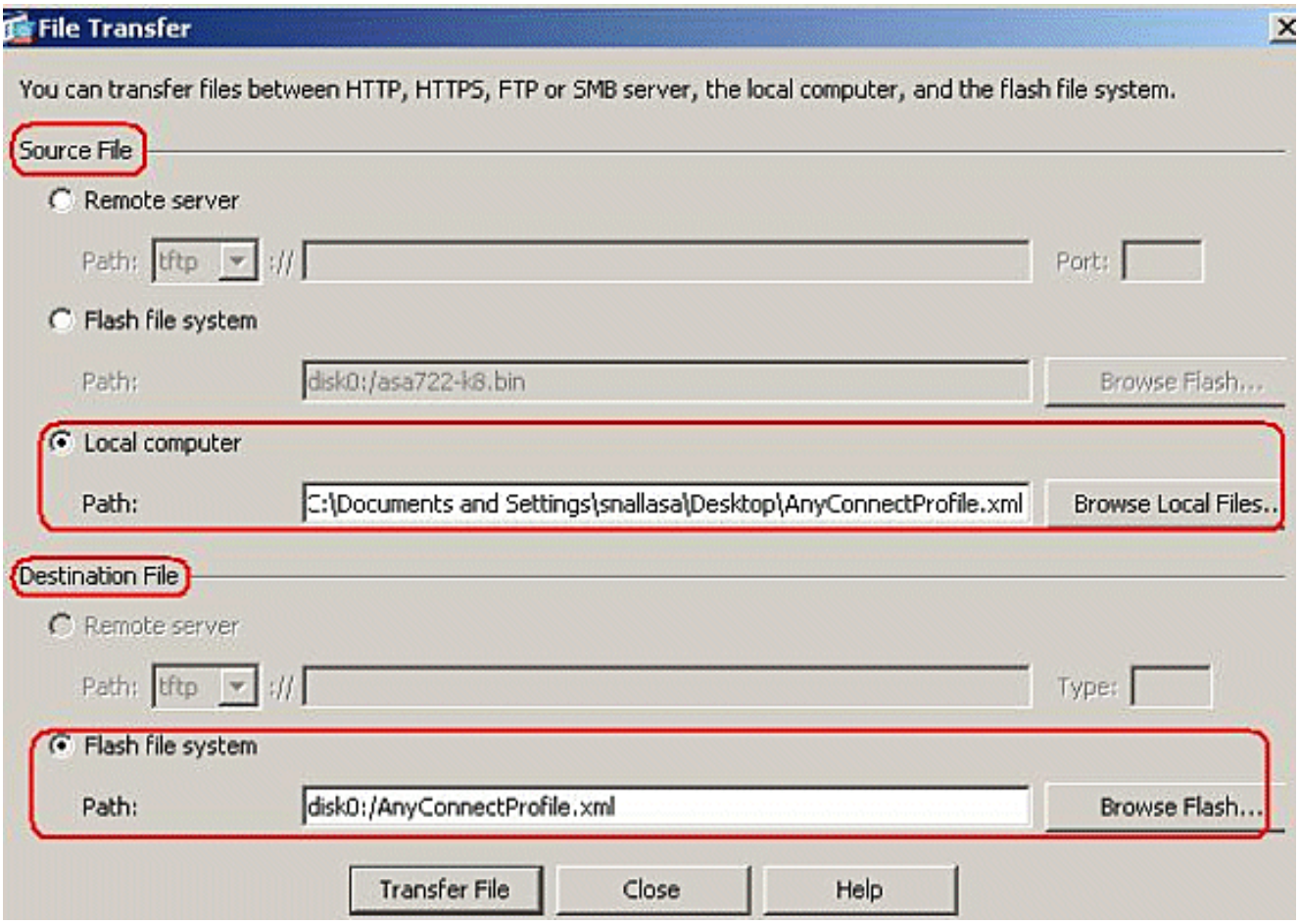
7. A fim transferir o perfil **AnyConnectProfile.xml do** computador local para piscar, vá às ferramentas**, e** clique FileManagement**.**



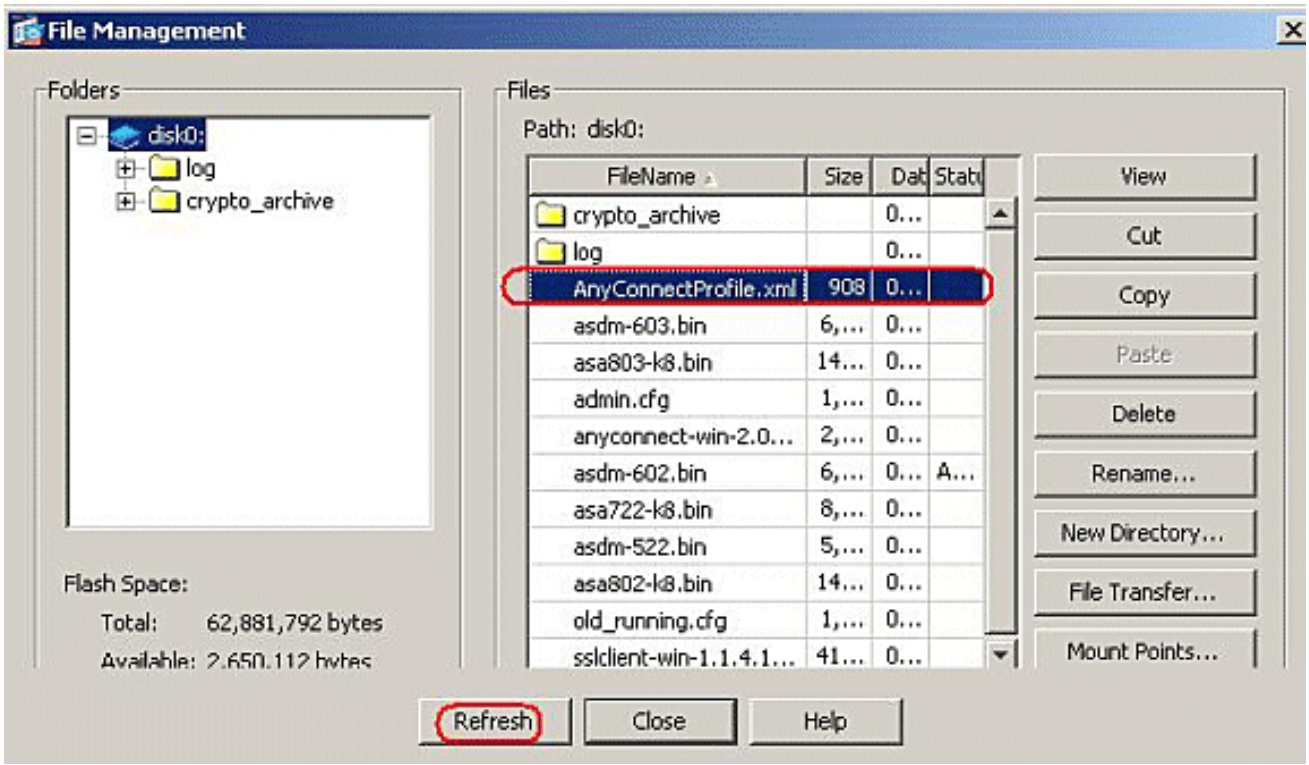
8. Clique o botão de **transferência de arquivo**.



9. A fim transferir o perfil do computador local à memória Flash ASA, escolha o **arquivo de origem**, o trajeto do arquivo XML (computador local), e o trajeto do **arquivo de destino** conforme sua
exigência.

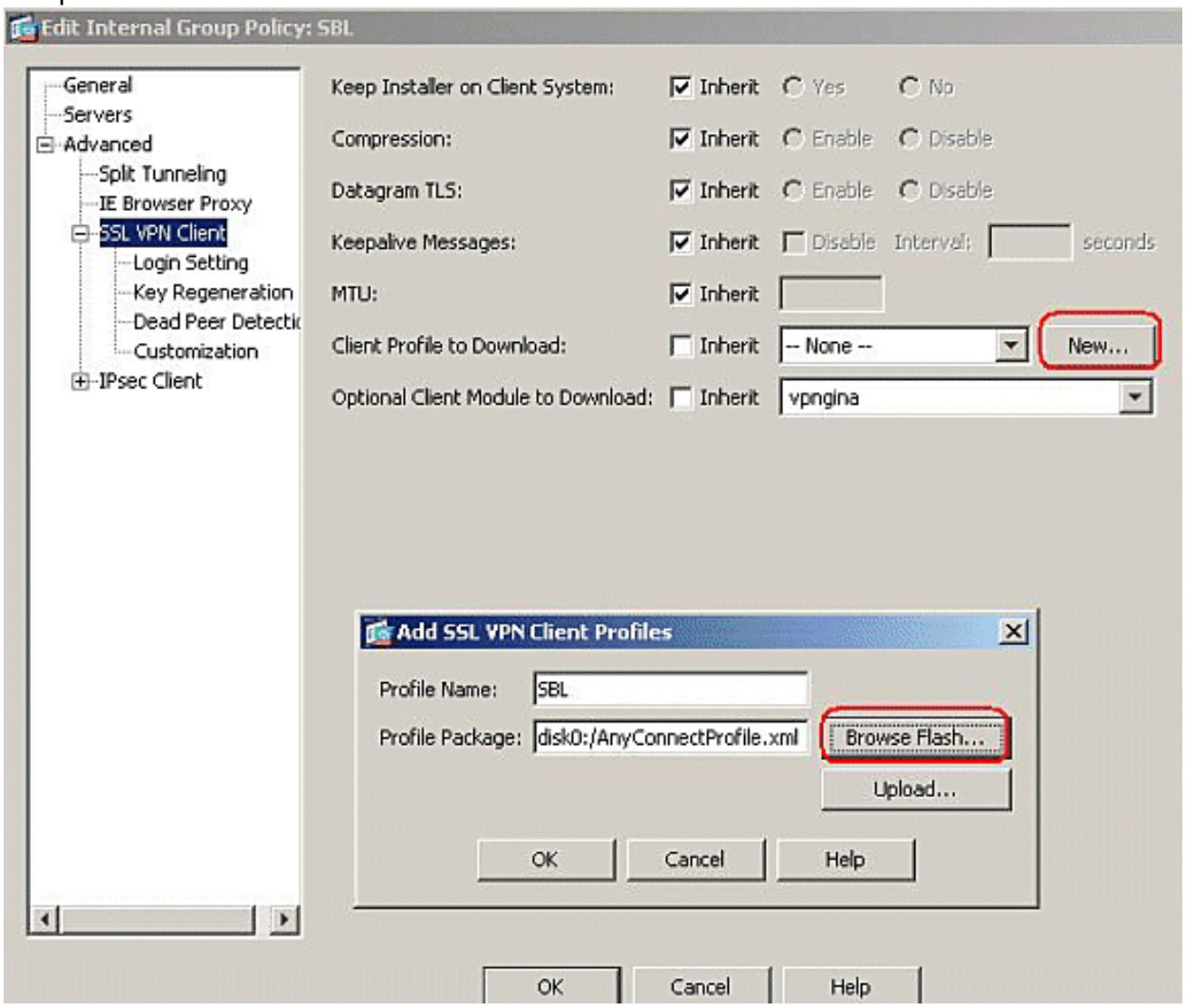


10. Depois que transferência, clica o **botão Refresh Button** para verificar se o arquivo de perfil está na memória
    Flash.

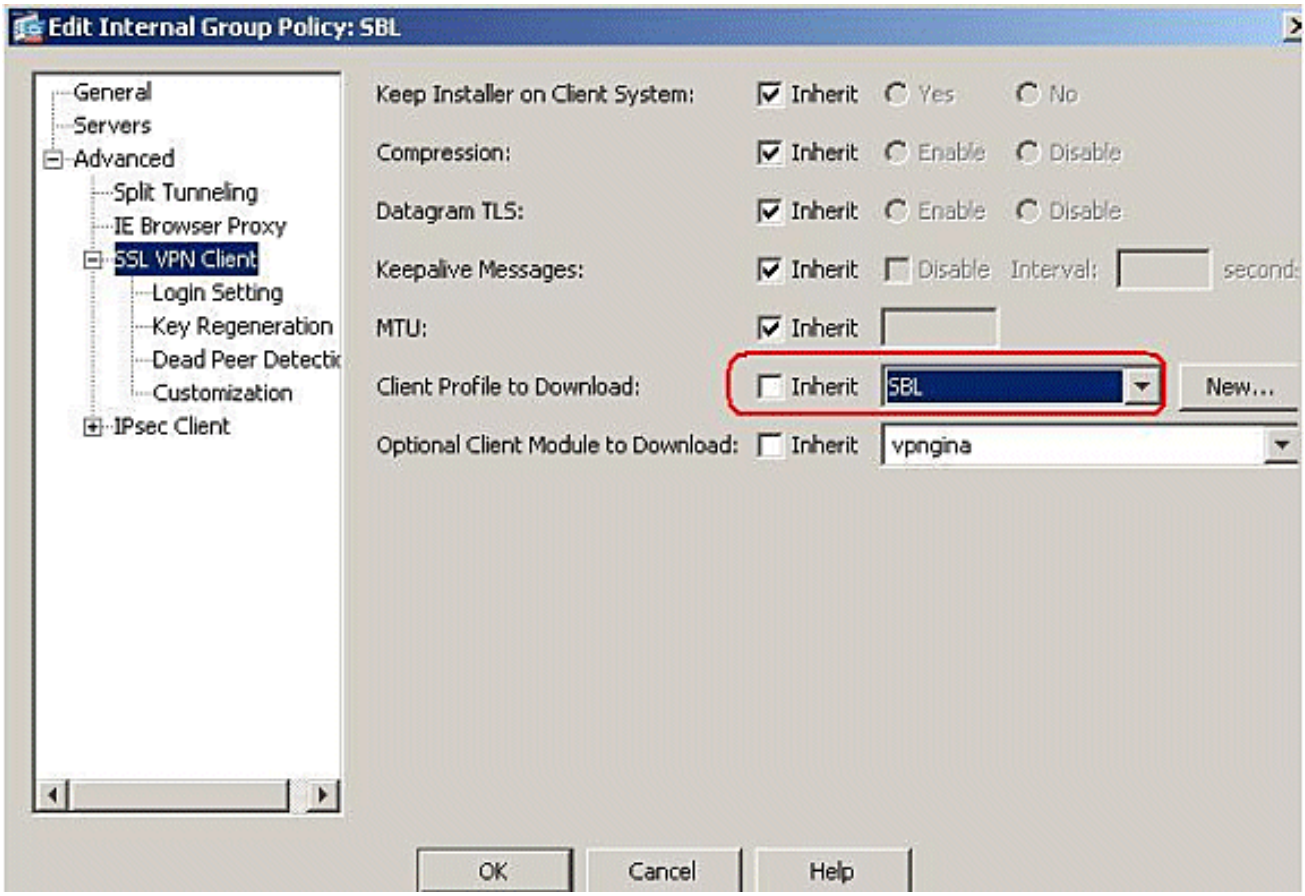


11. Atribua o perfil à política interna do grupo (**SBL**).Siga este trajeto, a **configuração > o acesso remoto VPN > do acesso > do grupo da rede (cliente) políticas > editam SBL (Política interna de grupo) > avançaram > perfil do cliente VPN > do cliente SSL a transferir**, e clicam o botão **novo.Nos perfis do cliente VPN adicionar SSL**, clique o **botão Browse** para escolher o lugar do profile(AnyConnectProfile.xml) **armazenado na** memória

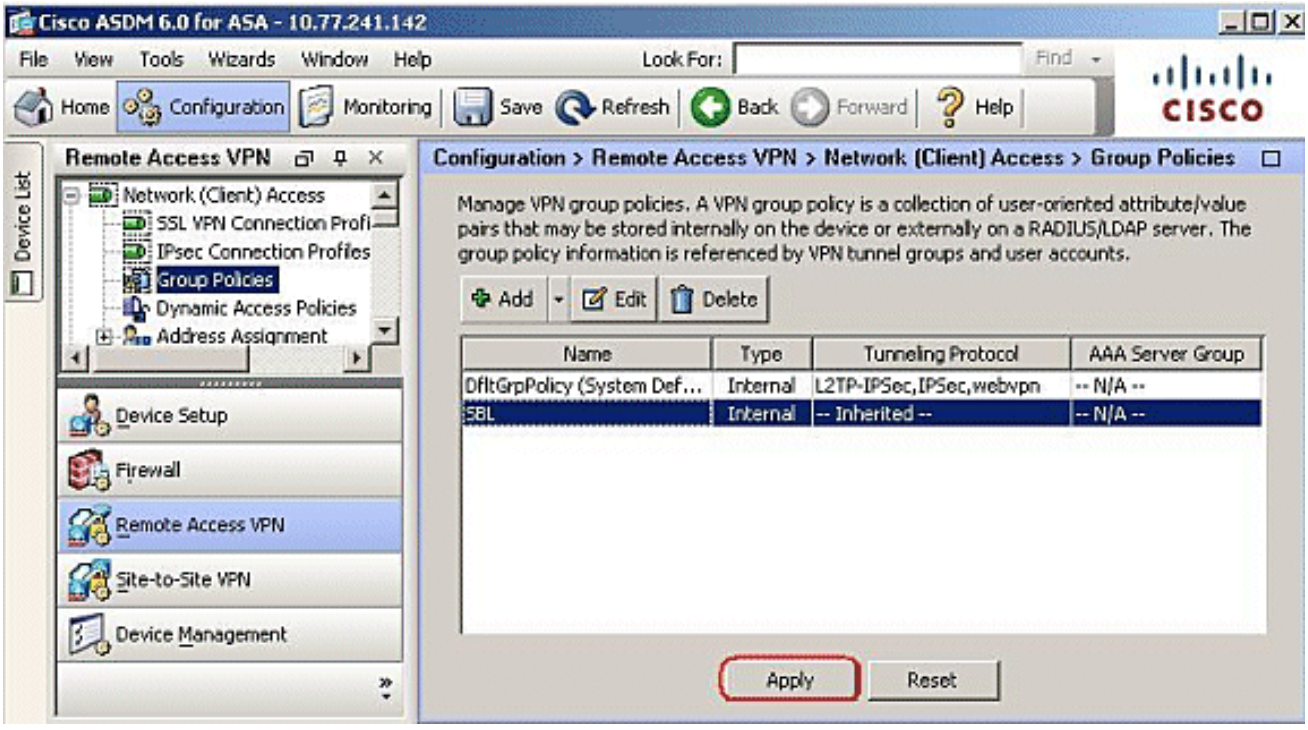
Flash ASA. Atribua ao Namefor o perfil, por exemplo, SBL. **Clique** OKTO completo.



12. Remova a caixa de verificação herdar e escolha **SBL no perfil do cliente transferir o** campo. Clique em **OK**.



13. O clique **aplica-se** para terminar.



Use o arquivo manifesto

O pacote de AnyConnect que é transferido arquivos pela rede na ferramenta de segurança contém um arquivo chamado VPNManifest.xml. Este exemplo mostra um índice da amostra 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>
```

A ferramenta de segurança armazenou nela configurou perfis, como explicado em etapa 1, e igualmente armazena um ou os pacotes múltiplos de AnyConnect que contêm o cliente próprio de AnyConnect, a utilidade do descargador, arquivo manifesto, e todos os outros módulos opcionais ou arquivos do apoio.

Quando um usuário remoto conecta à ferramenta de segurança com o WebLaunch ou um cliente autônomo atual, o descargador está transferido primeiramente e corrida. Usa o arquivo manifesto para verificar se há um cliente atual no usuário remoto PC que precisa de ser promovido, ou uma instalação de atualização é exigida. O arquivo manifesto igualmente contém a informação sobre se há algum módulo opcional que dever ser transferido e instalado, neste caso, o VPNGINA. O perfil do cliente é abaixado igualmente da ferramenta de segurança. A instalação de VPNGINA é ativada pelo **vpngina do valor dos módulos de** comando svc configurado sob o modo de comando da grupo-**política (webvpn)** como explicado em etapa 4. O cliente de AnyConnect e os VPNGINA são instalados, e o usuário vê o cliente de AnyConnect na repartição seguinte, antes do fazer logon do domínio do Windows.

Quando o usuário conecta, o cliente e o perfil estão passados para baixo ao usuário PC; o cliente e os VPNGINA são instalados; e o usuário vê o cliente de AnyConnect na repartição seguinte, antes do fazer logon.

Um exemplo de perfil está fornecido no PC cliente quando AnyConnect é instalado: **Usuários \ dados do aplicativo \ Cisco de C:\Documents and Settings\All \ Cisco \ cliente VPN \ perfil \ AnyConnectProfile de AnyConnect**.

Pesquise defeitos SBL

Use este procedimento se você encontra um problema com SBL:

1. Assegure-se de que o perfil esteja empurrado.
2. Suprima de perfis prévios; procure por eles no disco rígido para encontrar o lugar: *.xml.
3. Quando você vai aos adicionar/removeres programar, você tem uma instalação de AnyConnect e a instalação de AnyConnect VPNGINA?
4. Desinstale o cliente de AnyConnect.
5. Cancele o log de AnyConnect do usuário no visualizador de eventos e na contraprova.
6. A Web consulta de volta à ferramenta de segurança para reinstalar o cliente.
7. Certifique-se de que o perfil igualmente aparece.
8. Repartição uma vez. Na repartição seguinte, você é alertado com o começo antes da alerta de fazer logon.
9. Envie o log de eventos de AnyConnect a Cisco no formato .evt.
10. Se você vê este erro, suprima do 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

Este Mensagem de Erro é considerado ao tentar transferir arquivos pela rede o perfil de AnyConnect: `Erro em validar o arquivo XML contra o esquema o mais atrasado.` Como solucionar esse erro?

Solução 1

Este Mensagem de Erro ocorre na maior parte devido à sintaxe ou aos problemas de configuração no perfil de AnyConnect. A fim resolver esta edição, certifique-se de que o perfil de AnyConnect configurado é similar ao perfil de AnyConnect da amostra atual na seção do perfil de AnyConnect da amostra e do esquema XML do guia do administrador do Cisco AnyConnect VPN Client.

Informações Relacionadas

- Guia do administrador do Cisco AnyConnect VPN Client, versão 2.0
- Criando scripts de logon - Windows TechNet
- Configurando o começo antes do fazer logon (PLAP) em sistemas de Windows Vista
- Acesso ASA 8.x VPN com o exemplo de configuração do cliente VPN de AnyConnect SSL
- Cisco AnyConnect VPN Client
- Cisco ASA 5500 Series Adaptive Security Appliances
- Suporte Técnico e Documentação - Cisco Systems