ASA: Túnel inteligente usando o exemplo de configuração de ASDM

Contents

[Introduction](#)
[Prerequisites](#)
[Requirements](#)
[Componentes Utilizados](#)
[Conventions](#)
[Informações de Apoio](#)
[Configuração de acesso ao túnel inteligente](#)
[Requisitos, restrições e limitações do túnel inteligente](#)
[Requisitos gerais e limitações](#)
[Requisitos e limitações do Windows](#)
[Requisitos e limitações do Mac OS](#)
[Configurar](#)
[Adicionar ou editar lista de túneis inteligentes](#)
[Adicionar ou editar entrada de túnel inteligente](#)
[Configuração do ASA Smart Tunnel (Exemplo de Lotus) usando o ASDM 6.0(2)](#)
[Troubleshoot](#)
[Não consigo me conectar usando um URL do Smart Tunnel marcado como favorito no portal sem cliente. Por que esse problema ocorre e como posso resolvê-lo?](#)
[Posso organizar a URL de um link de túnel inteligente configurado na WebVPN?](#)
[Informações Relacionadas](#)

Introduction

Um túnel inteligente é uma conexão entre um aplicativo baseado em TCP e um site privado, usando uma sessão VPN SSL sem cliente (baseada em navegador) com o Security Appliance como o caminho e o Security Appliance como um servidor proxy. Você pode identificar aplicativos aos quais deseja conceder acesso ao túnel inteligente e especificar o caminho local para cada aplicativo. Para aplicativos executados no Microsoft Windows, você também pode exigir uma correspondência do hash SHA-1 do checksum como condição para conceder acesso ao túnel inteligente.

O Lotus SameTime e o *Microsoft Outlook Express* são exemplos de aplicativos para os quais você pode querer conceder acesso ao túnel inteligente.

Dependendo do aplicativo ser um cliente ou um aplicativo habilitado para Web, a configuração do túnel inteligente requer um destes procedimentos:

- Crie uma ou mais listas de túneis inteligentes dos aplicativos do cliente e atribua a lista às políticas de grupo ou às políticas de usuário local para quem você deseja fornecer acesso ao túnel inteligente.

- Crie uma ou mais entradas da lista de favoritos que especifiquem os URLs dos aplicativos habilitados para Web qualificados para acesso ao túnel inteligente e atribua a lista aos DAPs, políticas de grupo ou políticas de usuário local para os quais você deseja fornecer acesso ao túnel inteligente.Você também pode listar aplicativos habilitados para Web para os quais automatizar o envio de credenciais de login em conexões de túnel inteligente em sessões VPN SSL sem cliente.

Este documento pressupõe que a configuração do Cisco AnyConnect SSL VPN Client já foi feita e funciona corretamente para que o recurso de túnel inteligente possa ser configurado na configuração existente. Para obter mais informações sobre como configurar o cliente Cisco AnyConnect SSL VPN, consulte o ASA 8.x: Permitir o tunelamento dividido para AnyConnect VPN Client no exemplo de configuração do ASA.

Observação: certifique-se de que as etapas *4.b a 4.l* descritas na seção Configuração do ASA com o ASDM 6.0(2) do *ASA 8.x: O Exemplo de Configuração de Permitir Tunelamento Dividido para AnyConnect VPN Client no ASA* não é executado para configurar o recurso de túnel inteligente.

Este documento descreve como configurar o túnel smart nos Cisco ASA 5500 Series Adaptive Security Appliances.

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 executa a versão de software 8.0(2)
- PC com Microsoft Vista, Windows XP SP2 ou Windows 2000 Professional SP4 com Microsoft Installer versão 3.1
- Cisco Adaptive Security Device Manager (ASDM) versão 6.0(2)

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

Configuração de acesso ao túnel inteligente

A tabela do túnel inteligente exibe as listas do túnel inteligente, cada uma identificando um ou mais aplicativos qualificados para acesso ao túnel inteligente e seu sistema operacional associado (SO). Como cada política de grupo ou política de usuário local suporta uma lista de túneis inteligentes, você deve agrupar os aplicativos não baseados em navegador para que sejam suportados em uma lista de túneis inteligentes. Após a configuração de uma lista, você pode atribuí-la a uma ou mais políticas de grupo ou políticas de usuário local.

A janela de túneis inteligentes (**Configuração > VPN de acesso remoto > Acesso VPN SSL sem cliente > Portal > Túneis inteligentes**) permite concluir estes procedimentos:

- **Adicione uma lista de túneis inteligentes e adicione aplicativos à lista**Conclua estes passos para adicionar uma lista de túneis inteligentes e adicionar aplicativos à lista:Clique em Add.A caixa de diálogo Adicionar lista de túneis inteligentes é exibida.Insira um nome para a lista e clique em **Add**.O ASDM abre a caixa de diálogo Add Smart Tunnel Entry, que permite atribuir os atributos de um túnel inteligente à lista.Depois de atribuir os atributos desejados para o túnel inteligente, clique em **OK**.O ASDM exibe esses atributos na lista.Repita essas etapas conforme necessário para completar a lista e clique em **OK** na caixa de diálogo Adicionar lista de túneis inteligentes.
- **Alterar uma lista de túneis inteligentes**Conclua estes passos para alterar uma lista de túneis inteligentes:Clique duas vezes na lista ou escolha a lista na tabela e clique em **Editar**.Clique em **Adicionar** para inserir um novo conjunto de atributos de túnel inteligente na lista ou escolha uma entrada na lista e clique em **Editar** ou **Excluir**.
- **Remover uma lista**Para remover uma lista, escolha a lista na tabela e clique em **Excluir**.
- **Adicionar um favorito**Após a configuração e atribuição de uma lista de túneis inteligentes, você pode facilitar o uso de um túnel inteligente adicionando um marcador para o serviço e clicando na opção **Ativar Túnel Inteligente** na caixa de diálogo Adicionar ou Editar Marcador.

O acesso ao túnel inteligente permite que um aplicativo cliente baseado em TCP use uma conexão VPN baseada em navegador para se conectar a um serviço. Ele oferece as seguintes vantagens aos usuários, em comparação com plug-ins e a tecnologia antiga, o encaminhamento de portas:

- O túnel inteligente oferece melhor desempenho do que os plug-ins.
- Ao contrário do encaminhamento de portas, o túnel inteligente simplifica a experiência do usuário ao não exigir a conexão do usuário do aplicativo local à porta local.
- Ao contrário do encaminhamento de portas, o túnel inteligente não exige que os usuários tenham privilégios de administrador.

Requisitos, restrições e limitações do túnel inteligente

Requisitos gerais e limitações

O túnel inteligente tem os seguintes requisitos e limitações gerais:

- O host remoto que origina o túnel inteligente deve executar uma versão de 32 bits do Microsoft Windows Vista, Windows XP ou Windows 2000; ou Mac OS 10.4 ou 10.5.
- O início de sessão automático do túnel inteligente suporta apenas o Microsoft Internet Explorer no Windows.
- O navegador deve ser ativado com Java, Microsoft AtiveX ou ambos.

- O túnel inteligente suporta apenas proxies colocados entre computadores que executam o Microsoft Windows e o Security Appliance. O túnel inteligente usa a configuração do Internet Explorer (ou seja, a destinada para uso em todo o sistema no Windows). Se o computador remoto exigir que um servidor proxy acesse o Security Appliance, a URL da extremidade de terminação da conexão deve estar na lista de URLs excluídas dos serviços de proxy. Se a configuração de proxy especificar que o tráfego destinado ao ASA passa por um proxy, todo o tráfego de túnel inteligente passa pelo proxy.Em um cenário de acesso remoto baseado em HTTP, às vezes uma sub-rede não fornece acesso de usuário ao gateway de VPN. Nesse caso, um proxy colocado em frente ao ASA para rotear o tráfego entre a Web e o local do usuário final fornece acesso à Web. No entanto, somente usuários VPN podem configurar proxies colocados em frente ao ASA. Ao fazer isso, eles devem garantir que esses proxies suportem o método CONNECT. Para proxies que exigem autenticação, o túnel inteligente suporta apenas o tipo de autenticação de resumo básico.
- Quando o túnel inteligente é iniciado, o Security Appliance tunela todo o tráfego do processo do navegador usado pelo usuário para iniciar a sessão sem cliente. Se o usuário iniciar outra instância do processo do navegador, ele passará todo o tráfego para o túnel. Se o processo do navegador for o mesmo e o Security Appliance não fornecer acesso a um determinado URL, o usuário não poderá abri-lo. Como solução alternativa, o usuário pode usar um navegador diferente do usado para estabelecer a sessão sem cliente.
- Um failover stateful não retém conexões de túnel inteligente. Os usuários devem se reconectar após um failover.

Requisitos e limitações do Windows

Os seguintes requisitos e limitações aplicam-se apenas ao Windows:

- Somente os aplicativos baseados em TCP Winsock 2 estão qualificados para acesso ao túnel inteligente.
- O Security Appliance não oferece suporte ao proxy do Microsoft Outlook Exchange (MAPI). Nem o encaminhamento de portas nem o túnel inteligente suportam MAPI. Para a comunicação do Microsoft Outlook Exchange usando o protocolo MAPI, os usuários remotos devem usar o AnyConnect.
- Os usuários do Microsoft Windows Vista que usam o smart tunnel ou o encaminhamento de porta devem adicionar o URL do ASA à zona Site Confiável. Para acessar a zona Site confiável, inicie o Internet Explorer, escolha **Ferramentas > Opções da Internet** e clique na guia **Segurança**. Os usuários do Vista também podem desativar o Modo Protegido para facilitar o acesso ao túnel inteligente; no entanto, a Cisco recomenda contra esse método porque ele aumenta a vulnerabilidade ao ataque.

Requisitos e limitações do Mac OS

Esses requisitos e limitações aplicam-se apenas ao Mac OS:

- Safari 3.1.1 ou posterior ou Firefox 3.0 ou posterior
- Sun JRE 1.5 ou posterior
- Somente aplicativos iniciados na página do portal podem estabelecer conexões de túnel inteligente. Esse requisito inclui suporte a túnel inteligente para o Firefox. Usar o Firefox para iniciar outra instância do Firefox durante o primeiro uso de um túnel inteligente requer o perfil

do usuário chamado csco_st. Se esse perfil de usuário não estiver presente, a sessão solicitará que o usuário crie um.
- Os aplicativos que usam TCP que estão dinamicamente vinculados à biblioteca SSL podem funcionar em um túnel inteligente.
- O túnel inteligente não suporta estes recursos e aplicativos no Mac OS:Serviços de proxyInício de sessão automáticoAplicativos que usam espaços de nomes de dois níveisAplicativos baseados em console, como Telnet, SSH e cURLAplicativos que usam dlopen ou dlsys para localizar chamadas libsocketAplicações vinculadas estaticamente para localizar chamadas em libsocket

Configurar

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Adicionar ou editar lista de túneis inteligentes

A caixa de diálogo Add Smart Tunnel List permite adicionar uma lista de entradas de túnel inteligente à configuração do Security Appliance. A caixa de diálogo Editar lista de túneis inteligentes permite modificar o conteúdo da lista.

Campo

Nome da lista — Insira um nome exclusivo para a lista de aplicativos ou programas. Não há restrição no número de caracteres no nome. Não use espaços. Após a configuração da lista de túneis inteligentes, o nome da lista aparece ao lado do atributo Smart Tunnel List nas políticas de grupo de VPN SSL sem cliente e nas políticas de usuário local. Atribua um nome que o ajudará a distinguir seu conteúdo ou finalidade de outras listas que você provavelmente configurará.

Adicionar ou editar entrada de túnel inteligente

A caixa de diálogo Adicionar ou Editar entrada de túnel inteligente permite especificar os atributos de um aplicativo em uma lista de túneis inteligentes.

- **ID do aplicativo** — Digite uma string para nomear a entrada na lista de túneis inteligentes. A string é exclusiva para o SO. Geralmente, ele nomeia o aplicativo a receber acesso ao túnel inteligente. Para suportar várias versões de um aplicativo para o qual você escolhe especificar diferentes caminhos ou valores de hash, você pode usar esse atributo para diferenciar entradas, especificando o SO e o nome e a versão do aplicativo suportado por cada entrada de lista. A string pode ter até 64 caracteres.
- **Nome do processo** — Insira o nome ou o caminho do arquivo para o aplicativo. A string pode ter até 128 caracteresO Windows exige uma correspondência exata desse valor com o lado direito do caminho do aplicativo no host remoto para qualificar o aplicativo para acesso ao túnel inteligente. Se você especificar apenas o nome do arquivo para Windows, a VPN SSL não aplicará uma restrição de local no host remoto para qualificar o aplicativo para acesso ao túnel inteligente.Se você especificar um caminho e o usuário tiver instalado o aplicativo em outro local, o aplicativo não será qualificado. O aplicativo pode residir em qualquer caminho, desde que o lado direito da string corresponda ao valor digitado.Para autorizar um aplicativo

para acesso ao túnel inteligente se ele estiver presente em um dos vários caminhos no host remoto, especifique apenas o nome e a extensão do aplicativo neste campo ou crie uma entrada exclusiva de túnel inteligente para cada caminho.Para o Windows, se você quiser adicionar o acesso ao túnel inteligente a um aplicativo iniciado a partir do prompt de comando, especifique "cmd.exe" no nome do processo de uma entrada na lista de túneis inteligentes e especifique o caminho para o próprio aplicativo em outra entrada porque "cmd.exe" é o pai do aplicativo.O Mac OS requer o caminho completo para o processo e diferencia maiúsculas de minúsculas. Para evitar especificar um caminho para cada nome de usuário, insira um til (~) antes do caminho parcial (por exemplo, ~/bin/vnc).

- **SO** —Clique em Windows ou Mac para especificar o SO do host do aplicativo.
- **Hash** —(*Opcional e aplicável somente para Windows*) Para obter esse valor, insira a soma de verificação do arquivo executável em um utilitário que calcula um hash usando o algoritmo SHA-1. Um exemplo desse utilitário é o Microsoft File Checksum Integrity Verifier (FCIV), que está disponível em Availability and description do utilitário File Checksum Integrity Verifier. Depois de instalar o FCIV, coloque uma cópia temporária do aplicativo a ser colocada com hash em um caminho que não contenha espaços (por exemplo, c:/fciv.exe) e insira o aplicativo fciv.exe -sha1 na linha de comando (por exemplo, fciv.exe -sha1 c:\msimn.exe) para exibir o hash SHA-1.O hash SHA-1 tem sempre 40 caracteres hexadecimais.Antes de autorizar um aplicativo para acesso ao túnel inteligente, a VPN SSL sem cliente calcula o hash do aplicativo correspondente à ID do aplicativo. Ele qualifica o aplicativo para acesso ao túnel inteligente se o resultado corresponder ao valor do hash.Inserir um hash fornece uma garantia razoável de que a VPN SSL não qualifica um arquivo ilegítimo que corresponde à string especificada na ID do aplicativo. Como a soma de verificação varia com cada versão ou patch de um aplicativo, o hash inserido pode corresponder apenas a uma versão ou patch no host remoto. Para especificar um hash para mais de uma versão de um aplicativo, crie uma entrada de túnel inteligente exclusiva para cada valor de hash.**Observação:** você deve atualizar a lista de túneis inteligentes no futuro se inserir valores de hash e desejar oferecer suporte a versões ou patches futuros de um aplicativo com acesso ao túnel inteligente. Um problema repentino com o acesso ao túnel inteligente pode ser uma indicação de que o aplicativo que contém valores de hash não está atualizado com uma atualização do aplicativo. Você pode evitar esse problema não inserindo um hash.
- Depois de configurar a lista de túneis inteligentes, você deve atribuí-la a uma política de grupo ou a uma política de usuário local para que ela se torne ativa da seguinte maneira:Para atribuir a lista a uma política de grupo, escolha **Config > Remote Access VPN> Clientless SSL VPN Access > Group Policies > Add or Edit > Portal** e escolha o nome do túnel inteligente na lista suspensa ao lado do atributo Smart Tunnel List.Para atribuir a lista a uma política de usuário local, escolha **Config > Remote Access VPN> AAA Setup > Local Users > Add or Edit > VPN Policy > Clientless SSL VPN** e escolha o nome do túnel inteligente na lista suspensa ao lado do atributo Smart Tunnel List.

Configuração do ASA Smart Tunnel (Exemplo de Lotus) usando o ASDM 6.0(2)

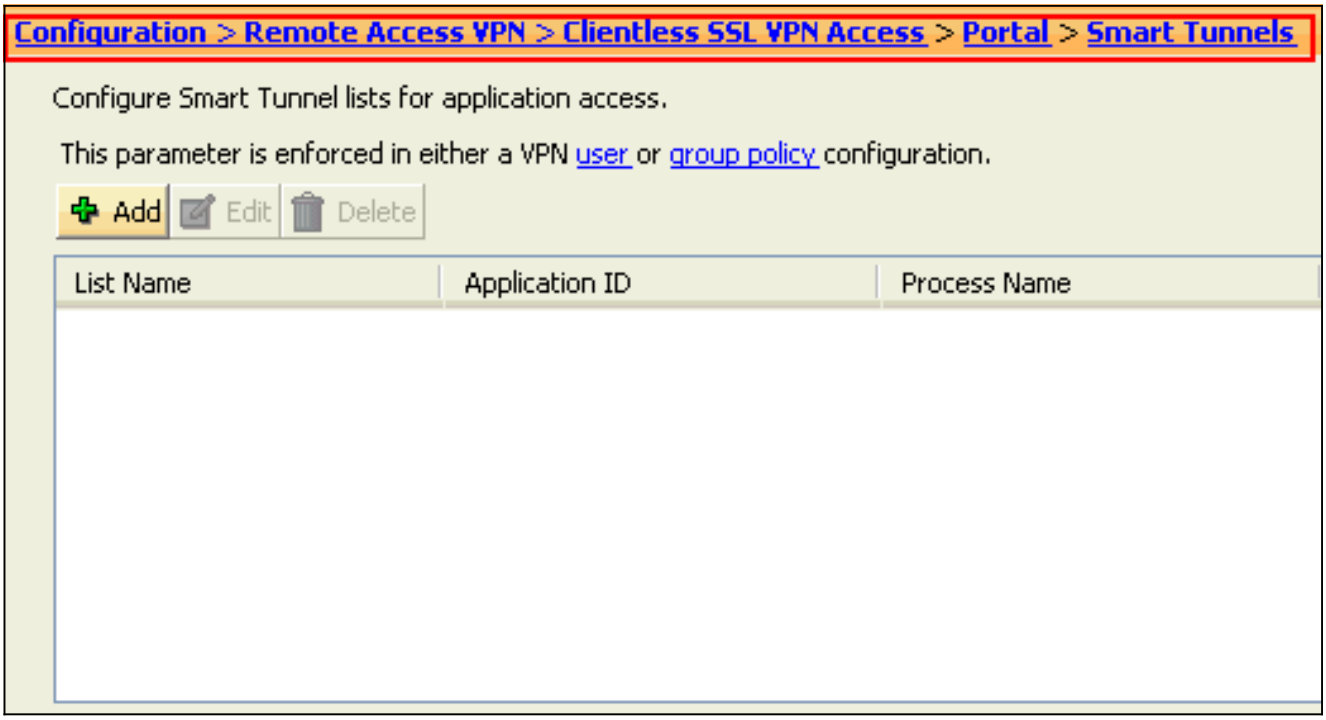
Este documento pressupõe que a configuração básica, como a configuração de interface, está completa e funciona corretamente.

Conclua estes passos para configurar um túnel inteligente:

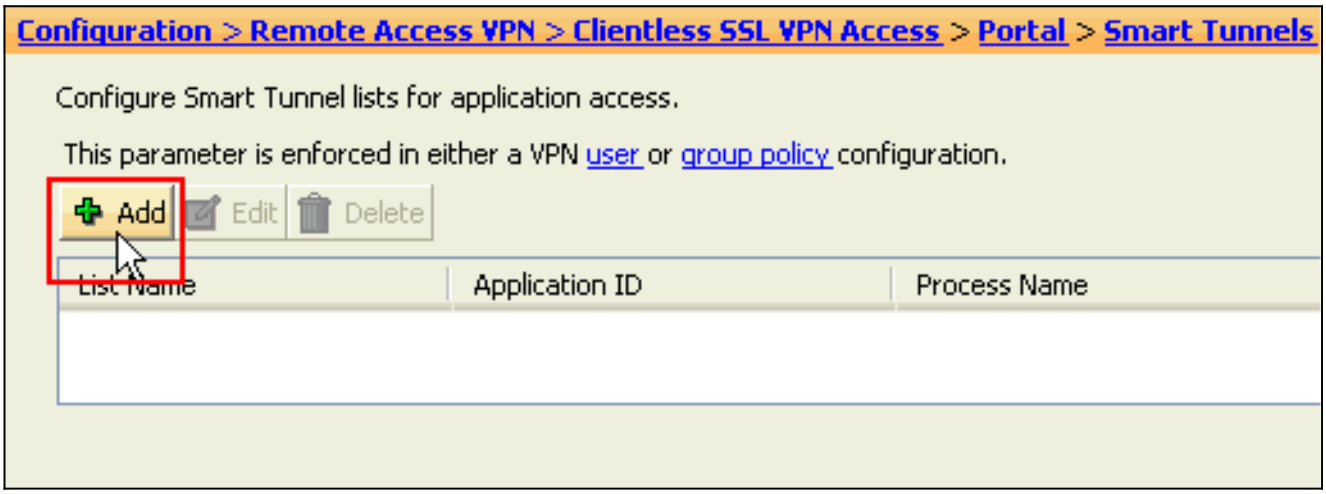
Observação: neste exemplo de configuração, o túnel inteligente está configurado para o aplicativo

Lotus.

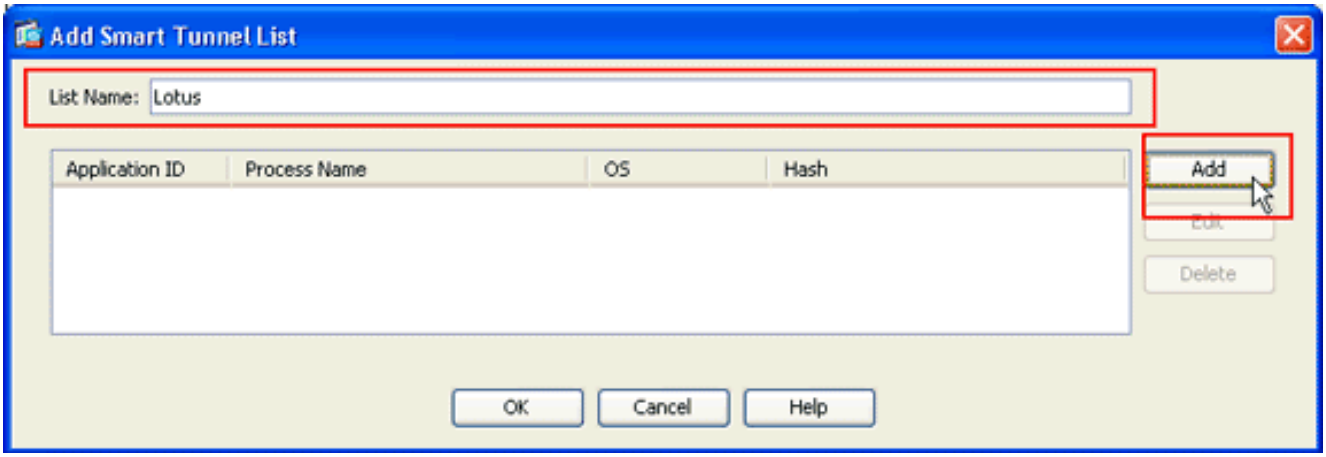
1. Escolha **Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Smart Tunneis** para iniciar a configuração do Smart Tunnel.



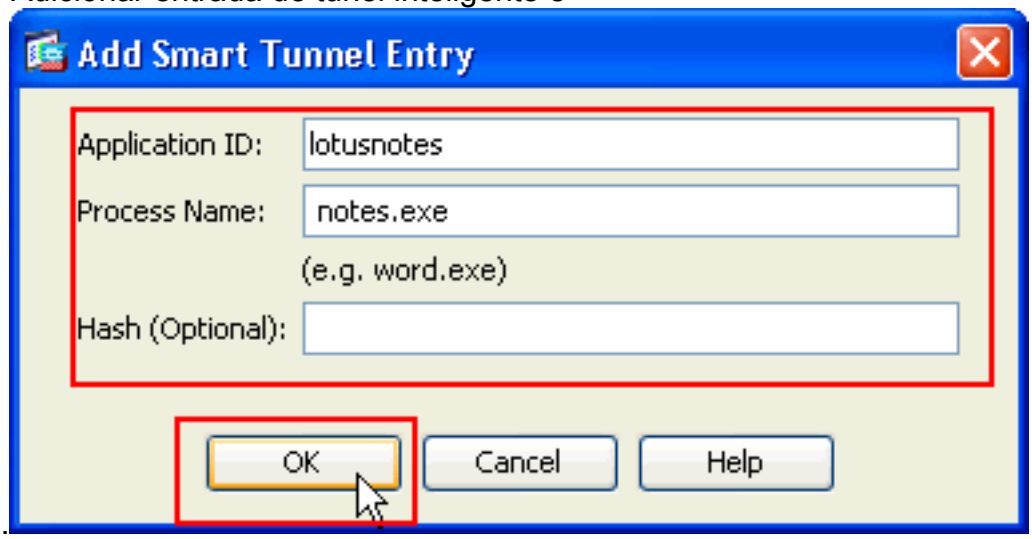
2. Clique em Add.



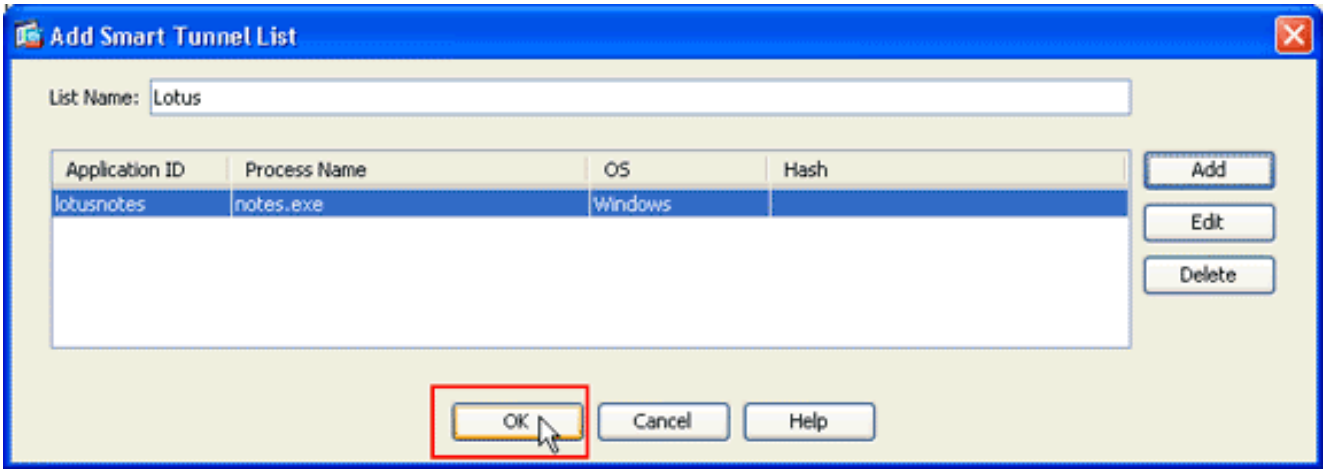
A caixa de diálogo Adicionar lista de túneis inteligentes é exibida.



3. Na caixa de diálogo Adicionar lista de túneis inteligentes, clique em **Adicionar**.A caixa de diálogo Adicionar entrada de túnel inteligente é exibida.

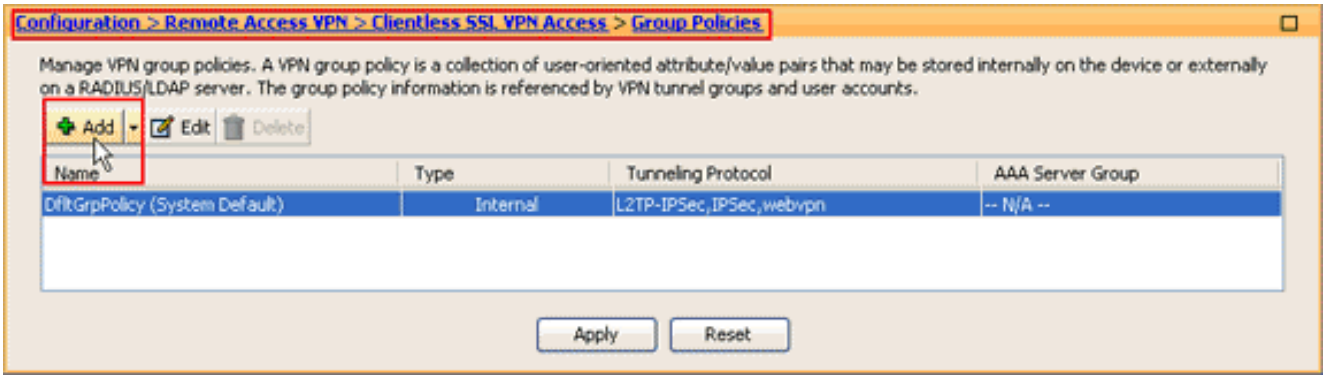


4. No campo ID do aplicativo, digite uma string para identificar a entrada na lista de túneis inteligentes.
5. Insira um nome de arquivo e um ramal para o aplicativo e clique em **OK**.
6. Na caixa de diálogo Adicionar lista de túneis inteligentes, clique em **OK**.

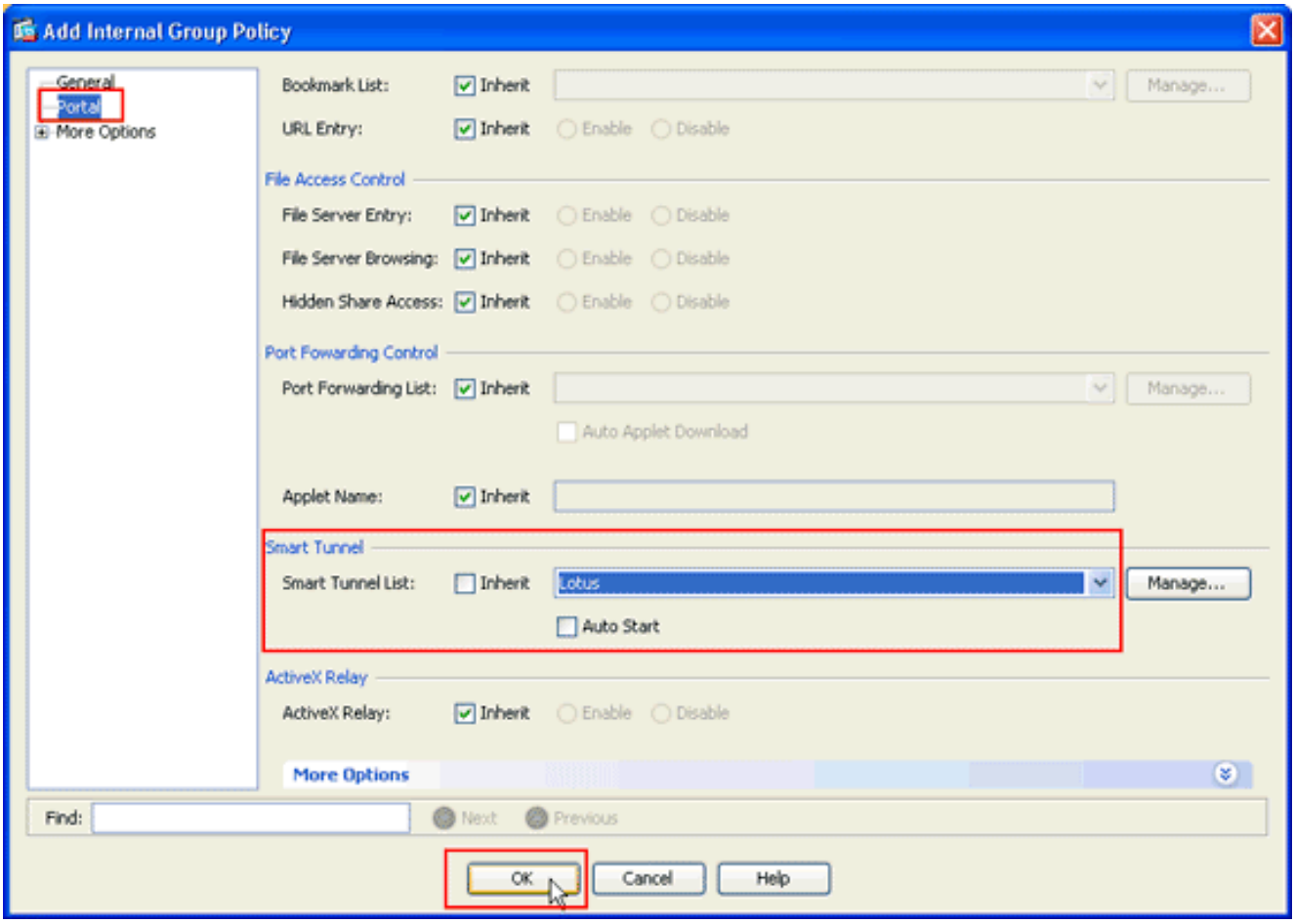


Observação: aqui está o comando de configuração de CLI equivalente:

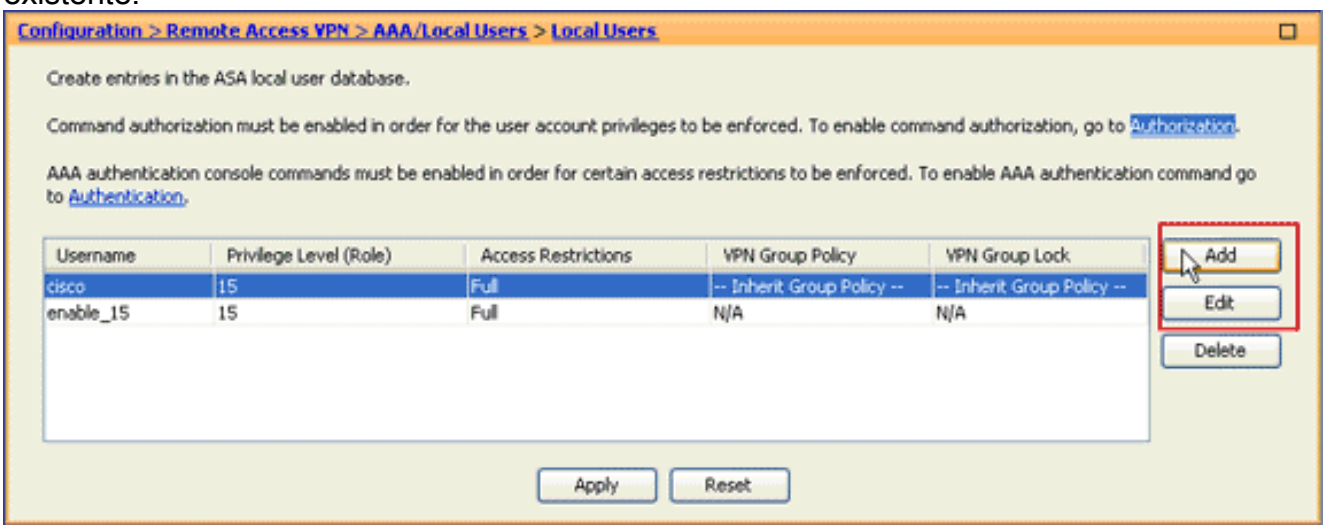
7. Atribua a lista às políticas de grupo e às políticas de usuário local para as quais deseja fornecer acesso ao túnel inteligente aos aplicativos associados da seguinte maneira:Para atribuir a lista a uma política de grupo, escolha **Configuration > Remote Access VPN> Clientless SSL VPN Access > Group Policies** e clique em **Add** ou **Edit.**



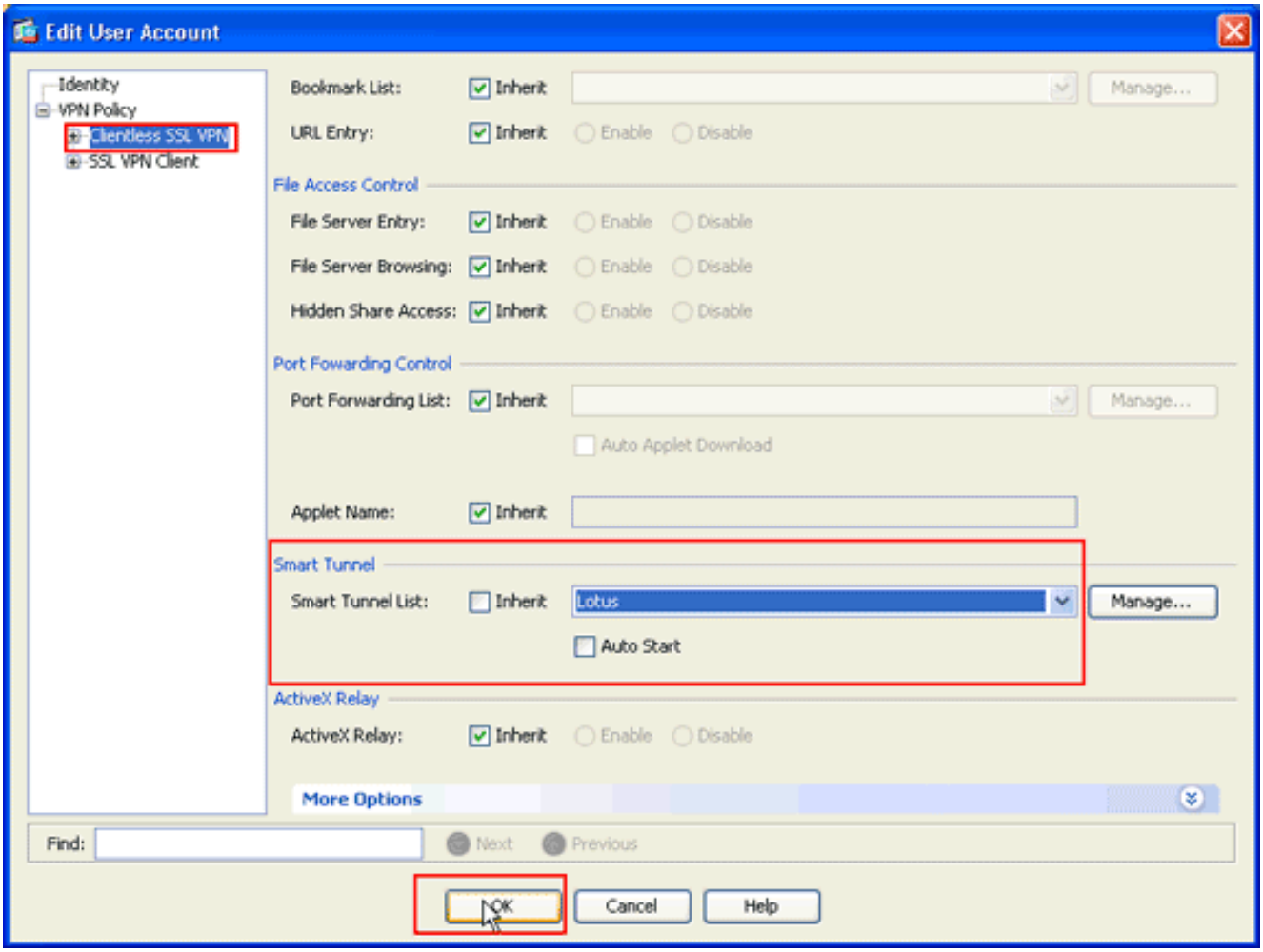
A caixa de diálogo Add Internal Group Policy é exibida.



8. Na caixa de diálogo Add Internal Group Policy, clique em **Portal**, escolha o nome do túnel inteligente na lista suspensa Smart Tunnel List e clique em **OK**.**Observação:** este exemplo usa o *Lotus* como o nome da lista de túneis inteligentes.
9. Para atribuir a lista a uma política de usuário local, escolha **Configuration > Remote Access VPN> AAA Setup > Local Users** e clique em **Add** para configurar um novo usuário ou clique em **Edit** para editar um usuário existente.



A caixa de diálogo Editar conta de usuário é exibida.



10. Na caixa de diálogo Editar conta de usuário, clique em **VPN SSL sem cliente**, escolha o nome do túnel inteligente na lista suspensa Lista de túneis inteligentes e clique em **OK**.**Observação:** este exemplo usa o *Lotus* como o nome da lista de túneis inteligentes.

A configuração do túnel inteligente está concluída.

Troubleshoot

Não consigo me conectar usando um URL do Smart Tunnel marcado como favorito no portal sem cliente. Por que esse problema ocorre e como posso resolvê-lo?

Esse problema ocorre devido ao problema descrito na ID de bug da Cisco CSCsx05766 **(somente clientes registrados)** . Para resolver esse problema, faça o downgrade do plug-in Java Runtime para uma versão mais antiga.

Posso organizar a URL de um link de túnel inteligente configurado na WebVPN?

Quando o túnel inteligente é usado no ASA, você não pode distorcer a URL ou ocultar a barra de endereços do navegador. Os usuários podem visualizar as URLs dos links configurados na WebVPN que usam o túnel inteligente. Como resultado, eles podem alterar a porta e acessar o servidor para algum outro serviço.

Para resolver esse problema, use as ACLs WebType. Consulte Listas de Controle de Acesso do Tipo Web para obter mais informações.

Informações Relacionadas

- Dispositivos de segurança adaptáveis Cisco ASA 5500 Series
- Exemplo de Configuração de Cliente VPN SSL (SVC) no ASA com o ASDM
- Suporte Técnico e Documentação - Cisco Systems