ASA: Túnel esperto usando o exemplo da configuração ASDM

Índice

Introdução

Um túnel esperto é uma conexão entre um aplicativo com base em TCP e um local privado, usando uma sessão de VPN dos sem clientes SSL (com base em navegador) com a ferramenta de segurança como o caminho e a ferramenta de segurança como um servidor proxy. Você pode identificar os aplicativos a que você quer conceder o acesso esperto do túnel e especificar o caminho local a cada aplicativo. Para os aplicativos que são executado em Microsoft Windows, você pode igualmente exigir um fósforo da mistura SHA-1 da soma de verificação enquanto uma circunstância para conceder o acesso esperto do túnel.

Lotus SameTime e *Microsoft Outlook Express* são exemplos dos aplicativos a que você pôde querer conceder o acesso esperto do túnel.

O dependente sobre se o aplicativo é um cliente ou é um aplicativo Web-permitido, configuração de túnel esperta exige um destes procedimentos:

- Crie umas ou várias lista espertas do túnel dos aplicativos do cliente, e atribua então a lista

às políticas do grupo ou às políticas do usuário local para quem você quer fornecer o acesso esperto do túnel.
- Crie umas ou várias entradas de lista do endereço da Internet que especificam as URL dos pedidos Web-permitidos elegíveis para o acesso esperto do túnel, e atribuem então a lista aos DAP, as políticas do grupo, ou políticas do usuário local para quem você quer fornecer o acesso esperto do túnel.Você pode igualmente alistar os aplicativos Web-permitidos para que que automatizem a submissão de credenciais do início de uma sessão em conexões de túnel espertas sobre sessões de VPN dos sem clientes SSL.

Este documento supõe que a configuração de cliente VPN de Cisco AnyConnect SSL está feita já e trabalha corretamente de modo que a característica esperta do túnel possa ser configurada na configuração existente. Para obter mais informações sobre de como configurar o cliente VPN de Cisco AnyConnect SSL, refira ASA 8.x: Permita o Split Tunneling para o cliente VPN de AnyConnect no exemplo de configuração ASA.

Refira configurar uma política esperta do túnel do túnel para obter mais informações sobre de como configurar o Split Tunneling junto com o túnel esperto.

Nota: Certifique-se de que as etapas *4.b a 4.l* descreveram na configuração ASA usando a seção ASDM 6.0(2) do *ASA 8.x: Permita o Split Tunneling para o cliente VPN de AnyConnect no exemplo de configuração ASA* não é executado a fim configurar a característica esperta do túnel.

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

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

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

Configuração esperta do acesso do túnel

A tabela esperta do túnel indica as lista espertas do túnel, cada qual identifica uns ou vários pedidos elegíveis para o acesso esperto do túnel e seu operating system (OS) associado. Porque cada política do grupo ou os suportes à política do usuário local uma lista esperta do túnel, você devem agrupar os aplicativos nonbrowser-baseados ser apoiado em uma lista esperta do túnel. Depois da configuração de uma lista, você pode atribui-la a um ou vário grupo policia ou a políticas do usuário local.

Nota: Para obter mais informações sobre da configuração de túnel esperta, refira configurar o acesso esperto do túnel.

O indicador esperto dos túneis (**configuração > acesso remoto VPN > acesso > portal dos sem clientes SSL VPN > túneis espertos**) permite que você termine estes procedimentos:

- **Adicionar uma lista esperta do túnel e adicionar aplicativos à lista**Termine estas etapas a fim adicionar uma lista esperta do túnel e adicionar aplicativos à lista:Clique em Add.A caixa de diálogo esperta da lista do túnel adicionar aparece.Insira um nome para a lista e clique em **Add**.O ASDM abre a caixa esperta do diálogo de entrada do túnel adicionar, que permite que você atribua os atributos de um túnel esperto à lista.Depois que você atribui os atributos desejados para o túnel esperto, clique a **APROVAÇÃO**.O ASDM indica aqueles atributos na lista.Repita estas etapas como necessário a fim terminar a lista, e clique então a **APROVAÇÃO na** caixa de diálogo esperta da lista do túnel adicionar.
- **Mude uma lista esperta do túnel**Termine estas etapas a fim mudar uma lista esperta do túnel:Fazer duplo clique a lista ou escolha a lista na tabela, e o clique **edita**.Clique **adicionam** para introduzir um grupo novo de atributos de túnel espertos na lista ou para escolher uma entrada na lista, e o clique **edita** ou **suprime**.
- **Remova uma lista**A fim remover uma lista, escolher a lista na tabela, e clicar a **supressão**.
- **Adicionar um endereço da Internet**Depois da configuração e da atribuição de uma lista esperta do túnel, você pode fazer um túnel esperto fácil de usar adicionando um endereço da Internet para o serviço e clicando a opção **esperta do túnel da possibilidade** adicionar ou editar a caixa de diálogo do endereço da Internet.

O acesso esperto do túnel permite a um cliente o aplicativo com base em TCP usar uma conexão de VPN com base em navegador para conectar a um serviço. Oferece as seguintes vantagens aos usuários, comparados aos encaixes e à tecnologia do legado, transmissão da porta:

- O túnel esperto oferece o melhor desempenho do que encaixes.
- Ao contrário da transmissão da porta, o túnel esperto simplifica o usuário que a experiência por não exige a conexão do usuário do aplicativo local à porta local.
- Ao contrário da transmissão da porta, o túnel esperto não exige usuários ter privilégios do administrado.

Exigências, limitações, e limitações espertas do túnel

Requisitos gerais e limitações

O túnel esperto tem os seguintes requisitos gerais e limitações:

- O host remoto que origina o túnel esperto deve executar uma versão de 32 bits da vista, do Windows XP, ou do Windows 2000 de Microsoft Windows; ou Mac OS 10.4 ou 10.5.
- Automóvel esperto do túnel sinal-no Microsoft Internet explorer dos apoios somente em Windows.
- O navegador deve ser permitido com Javas, Microsoft ActiveX, ou ambos.
- O túnel esperto apoia somente os proxys colocados entre os computadores que executam Microsoft Windows e a ferramenta de segurança. O túnel esperto usa a configuração do internet explorer (isto é, essa pretendida para o uso sistema-largo em Windows). Se o computador remoto exige um servidor proxy alcançar a ferramenta de segurança, a URL da extremidade de terminação da conexão deve estar na lista de URL excluídas dos serviços de proxy. Se a configuração de proxy especifica que o tráfego destinado para o ASA atravessa um proxy, todo o tráfego de túnel esperto atravessa o proxy.Em uma encenação HTTP-baseada do Acesso remoto, às vezes uma sub-rede não fornece o acesso de usuário ao gateway de VPN. Neste caso, um proxy colocado na frente do ASA para distribuir o tráfego entre a Web e o lugar do utilizador final fornece o acesso à Web. Contudo, somente os usuários VPN podem configurar os proxys colocados na frente do ASA. Ao fazer assim, devem certificar-se que estes proxys apoiam o método da CONEXÃO. Para os proxys que exigem a autenticação, o túnel esperto apoia somente o tipo da autenticação de digest básica.
- Quando o túnel esperto começa, a ferramenta de segurança escava um túnel todo o tráfego do processo do navegador o usuário usado para iniciar a sessão dos sem clientes. Se o usuário começa um outro exemplo do processo do navegador, passa todo o tráfego ao túnel. Se o processo do navegador é o mesmo e a ferramenta de segurança não fornece o acesso a uma URL dada, o usuário não pode abri-la. Como uma ação alternativa, o usuário pode usar um navegador diferente de esse usado para estabelecer a sessão dos sem clientes.
- Uma comutação classificada não retém conexões de túnel espertas. Os usuários devem reconectar após um Failover.

Exigências e limitações de Windows

As seguintes exigências e limitações aplicam-se a Windows somente:

- Somente o Winsock 2, aplicativos com base em TCP é elegível para o acesso esperto do túnel.
- A ferramenta de segurança não apoia o proxy da troca do Microsoft outlook (MAPI). Nem mova a transmissão nem o túnel esperto apoia o MAPI. Para uma comunicação da troca do Microsoft outlook usando o protocolo MAPI, os usuários remotos devem usar AnyConnect.
- Os usuários da vista de Microsoft Windows que usam a transmissão esperta do túnel ou da porta devem adicionar a URL do ASA à zona da site confiável. A fim alcançar a zona da site confiável, comece o internet explorer, e escolha **ferramentas > opções de internet**, e clique a **ABA de segurança**. Os usuários da vista podem igualmente desabilitar o modo protegido a fim facilitar o acesso esperto do túnel; contudo, Cisco recomenda contra este método porque aumenta a vulnerabilidade para atacar.

Exigências e limitações do Mac OS

Estas exigências e limitações aplicam-se ao Mac OS somente:

- Safari 3.1.1 ou 3.0 mais atrasado ou de Firefox ou mais tarde
- Sun JRE 1.5 ou mais atrasado
- Somente os aplicativos começados da página portal podem estabelecer conexões de túnel espertas. Esta exigência inclui o apoio esperto do túnel para Firefox. Usar Firefox para começar um outro exemplo de Firefox durante o primeiro uso de um túnel esperto exige o perfil de usuário nomeado csco_st. Se este perfil de usuário não está atual, a sessão alerta o usuário criar um.
- Os aplicativos que usam o TCP que são ligados dinamicamente à biblioteca SSL podem trabalhar sobre um túnel esperto.
- O túnel esperto não apoia estes características e aplicativos no Mac OS:Serviços de proxyAutomóvel sinal-emAplicativos que usam os espaços de nome de dois níveisaplicativos Console-baseados, tais como o telnet, o SSH, e a ondaA utilização dos aplicativos dlopen ou dlsym para encontrar atendimentos do libsocketAplicativos estaticamente ligados encontrar atendimentos do libsocket

Configurar

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

Nota: Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

Adicionar ou edite a lista esperta do túnel

A caixa de diálogo esperta da lista do túnel adicionar deixa-o adicionar uma lista de entradas espertas do túnel à configuração da ferramenta de segurança. A caixa de diálogo esperta da lista do túnel da edição deixa-o alterar os índices da lista.

Campo

Nome de lista — Dê entrada com um nome exclusivo para a lista de aplicativo ou os programas. Não há nenhuma limitação no número de caráteres no nome. Não use espaços. Depois da configuração da lista esperta do túnel, o nome de lista aparece ao lado do atributo de lista esperto do túnel nas políticas do grupo de VPN dos sem clientes SSL e em políticas do usuário local. Atribua um nome que o ajude a distinguir sua índices ou finalidade de outras lista que você é provável configurar.

Adicionar ou edite a entrada esperta do túnel

Adicionar ou edita a caixa esperta do diálogo de entrada do túnel deixa-o especificar os atributos de um aplicativo em uma lista esperta do túnel.

- **ID de aplicativo** — Entre em uma corda para nomear a entrada na lista esperta do túnel. A corda é original para o OS. Tipicamente, nomeia o aplicativo ser concedido o acesso esperto do túnel. A fim apoiar versões múltiplas de um aplicativo para que você escolhe especificar trajetos diferentes ou valores de hash, você pode usar este atributo para diferenciar entradas,

especificando o OS e o nome e a versão do aplicativo apoiado por cada entrada de lista. A corda pode ser até 64 caráteres.

- **Nome de processo** — Entre no nome de arquivo ou no trajeto ao aplicativo. A corda pode ser até os caráteres 128Windows exige um exato - fósforo deste valor ao lado direito do trajeto do aplicativo no host remoto para qualificar o pedido para o acesso esperto do túnel. Se você especifica somente o nome de arquivo para Windows, o SSL VPN não reforça uma limitação do lugar no host remoto para qualificar o pedido para o acesso esperto do túnel.Se você especifica um trajeto e o usuário instalou o aplicativo em um outro lugar, esse aplicativo não qualifica. O aplicativo pode residir em todo o trajeto enquanto o lado direito das séries de compatibilidade o valor que você incorpora.A fim autorizar um pedido para o túnel esperto alcance se esta presente em um de diversos trajetos no host remoto, especifique somente o nome e a extensão do aplicativo neste campo ou crie uma entrada esperta original do túnel para cada trajeto.Para Windows, se você quer adicionar o acesso esperto do túnel a um aplicativo começado do comando prompt, você deve especificar “cmd.exe” no nome de processo de uma entrada na lista esperta do túnel e especificar o trajeto ao aplicativo próprio em uma outra entrada porque “cmd.exe” é o pai do aplicativo.O Mac OS exige o caminho cheio ao processo e é diferenciando maiúsculas e minúsculas. A fim evitar especificar um trajeto para cada nome de usuário, introduza um til (~) antes do trajeto parcial (por exemplo, ~/bin/vnc).
- **OS** — Clique Windows ou Mac a fim especificar o OS do host do aplicativo.
- **Mistura** — (*opcional e aplicável somente para Windows*) a fim obter este valor, incorpore a soma de verificação do arquivo executável em uma utilidade que calcule uma mistura usando o algoritmo SHA-1. Um exemplo de tal utilidade é o verificador da integridade da soma de verificação do arquivo de Microsoft (FCIV), que está disponível em http://support.microsoft.com/kb/841290/ . Após ter instalado FCIV, coloque uma cópia temporária do aplicativo ser picado em um trajeto que não contenha nenhum espaço (por exemplo, c: /fciv.exe), incorporam então o aplicativo fciv.exe -sha1 na linha de comando (por exemplo, fciv.exe -sha1 c:\msimn.exe) indicar a mistura SHA-1.A mistura SHA-1 é sempre 40 caracteres hexadecimais.Antes de autorizar um pedido para o acesso esperto do túnel, os sem clientes SSL VPN calculam a mistura do aplicativo que combina o ID de aplicativo. Qualifica o pedido para o acesso esperto do túnel se o resultado combina o valor da mistura.Entrar em uma mistura oferece uma garantia razoável que o SSL VPN não qualifica um arquivo ilegítimo que combine a corda que você especificou no ID de aplicativo. Porque a soma de verificação varia com cada versão ou correção de programa de um aplicativo, a mistura que você entra pode somente combinar uma versão ou correção de programa no host remoto. A fim especificar uma mistura para mais de uma versão de um aplicativo, crie uma entrada esperta original do túnel para cada valor de hash.**Nota:** Você deve atualizar a lista esperta do túnel no futuro se você incorpora valores de hash e você quer apoiar versões futuras ou as correções de programa de um aplicativo com túnel esperto alcançam. Um problema repentino com acesso esperto do túnel pôde ser uma indicação que o aplicativo que contém valores de hash não é atualizado com uma upgrade de aplicativo. Você pode evitar este problema não entrando em uma mistura.
- Uma vez que você configura a lista esperta do túnel, você deve atribui-la a uma política do grupo ou a uma política do usuário local para que torne-se ativo como segue:A fim atribuir a lista a uma política do grupo, escolher o **> Add dos Config > das políticas do acesso > do grupo dos sem clientes SSL VPN do Acesso remoto VPN> ou editá-lo > Portal**, e escolher o nome de túnel esperto da lista de drop-down ao lado do atributo de lista esperto do túnel.A fim atribuir a lista a uma política do usuário local, escolher os **Config > o Acesso remoto**

VPN> AAA Setup > > Add dos usuários locais ou editá-los > política de VPN > sem clientes SSL VPN, e escolher o nome de túnel esperto da lista de drop-down ao lado do atributo de lista esperto do túnel.

Configuração esperta do túnel ASA (exemplo de Lotus) usando o ASDM 6.0(2)

Este documento supõe que a configuração básica, tal como a configuração da interface, está completa e trabalha corretamente.

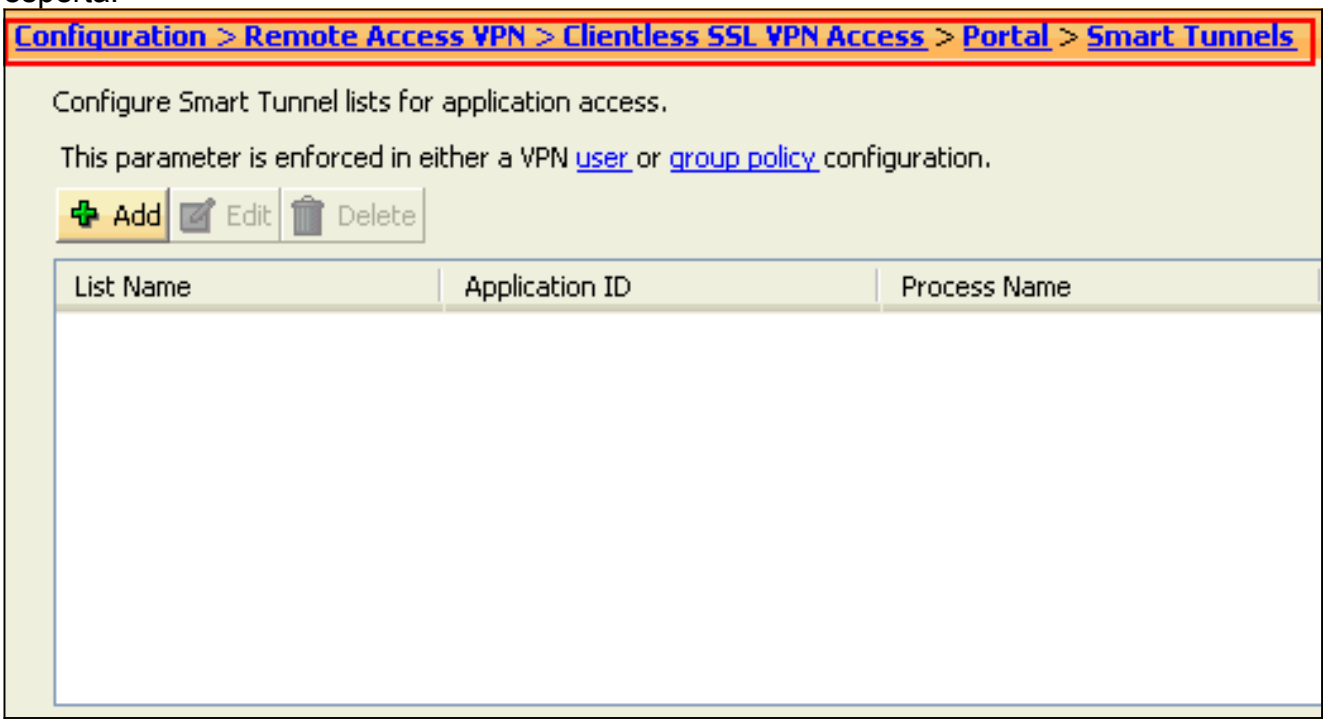
Nota: Consulte Habilitação de Acesso HTTPS para o ASDM para permitir que o ASA seja configurado pelo ASDM.

Nota: O WebVPN e o ASDM não podem ser ativados na mesma interface do ASA, a menos que você altere os números de porta. Consulte ASDM e WebVPN Habilitados na Mesma Interface do ASA para obter mais informações.

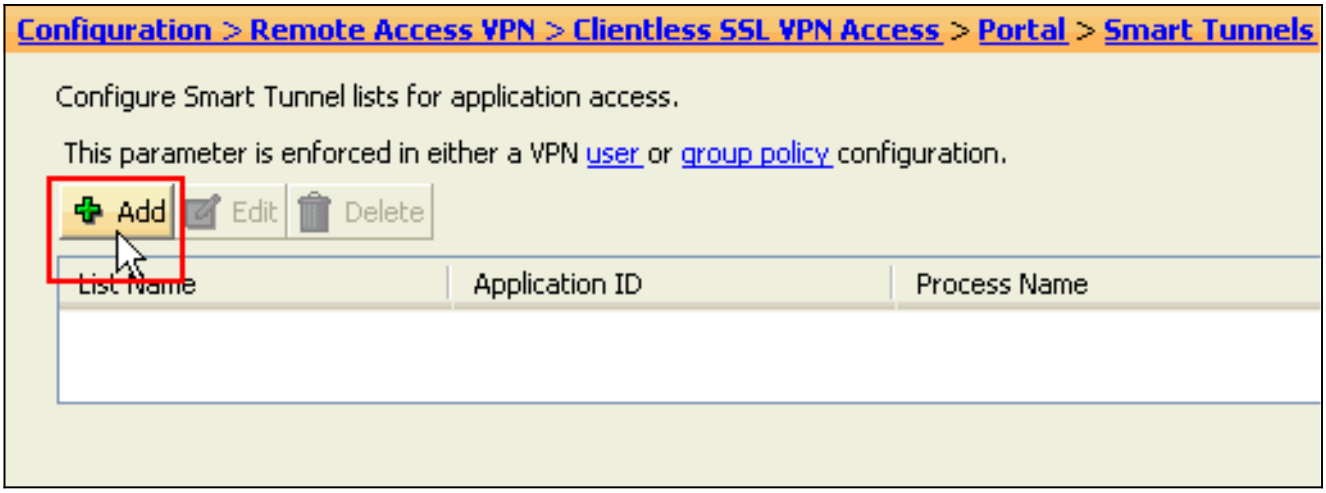
Termine estas etapas a fim configurar um túnel esperto:

Nota: Neste exemplo de configuração, o túnel esperto é configurado para o aplicativo de Lotus.

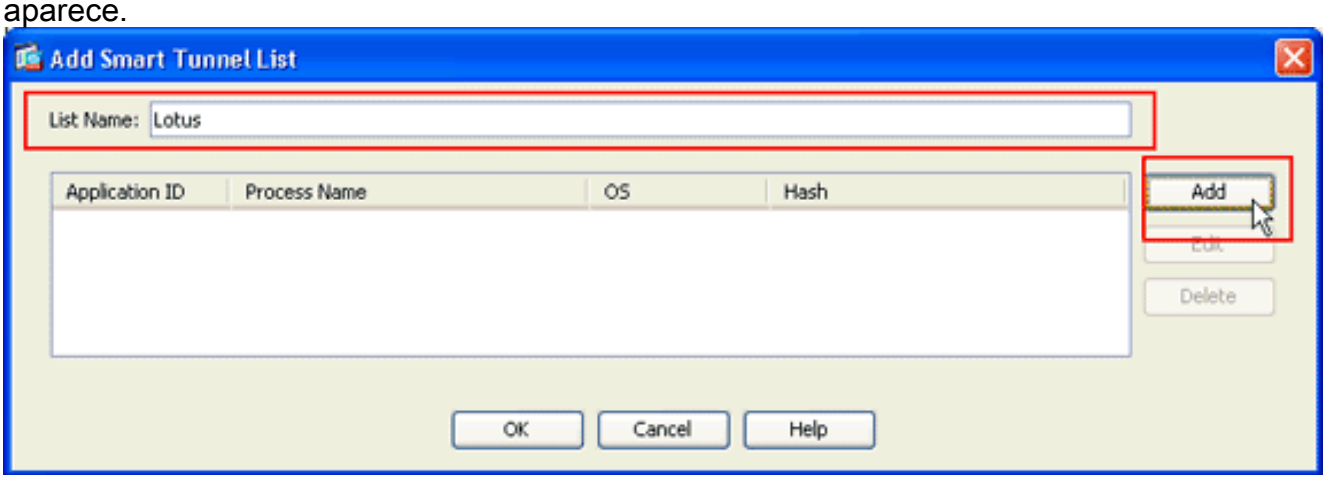
1. Escolha a **configuração > o acesso remoto VPN > o acesso > o portal dos sem clientes SSL VPN > túneis espertos** a fim começar a configuração de túnel esperta.



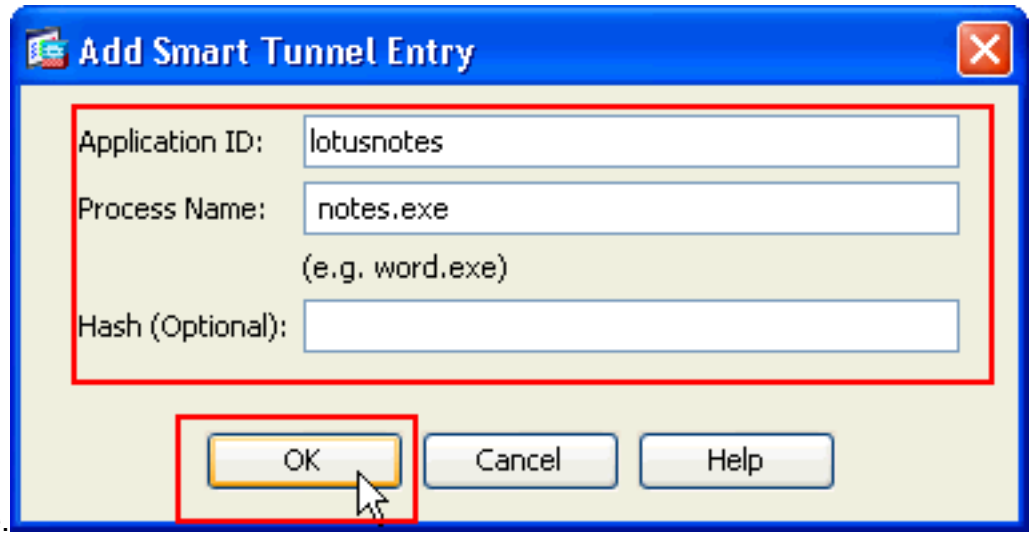
2. Clique em Add.



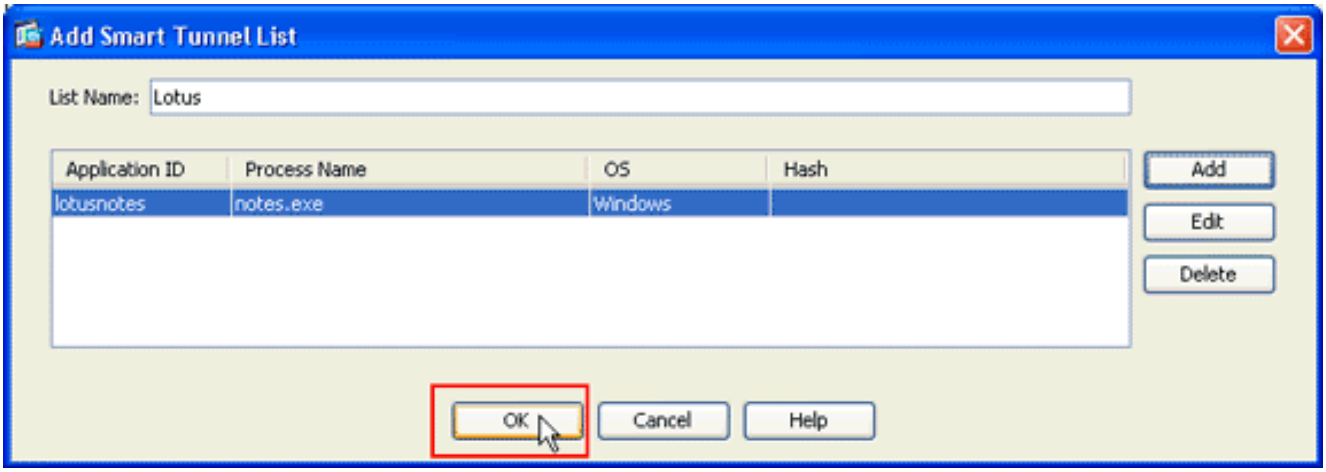
A caixa de diálogo esperta da lista do túnel adicionar aparece.



3. Na caixa de diálogo esperta da lista do túnel adicionar, o clique **adiciona**.A caixa esperta do diálogo de entrada do túnel adicionar aparece.

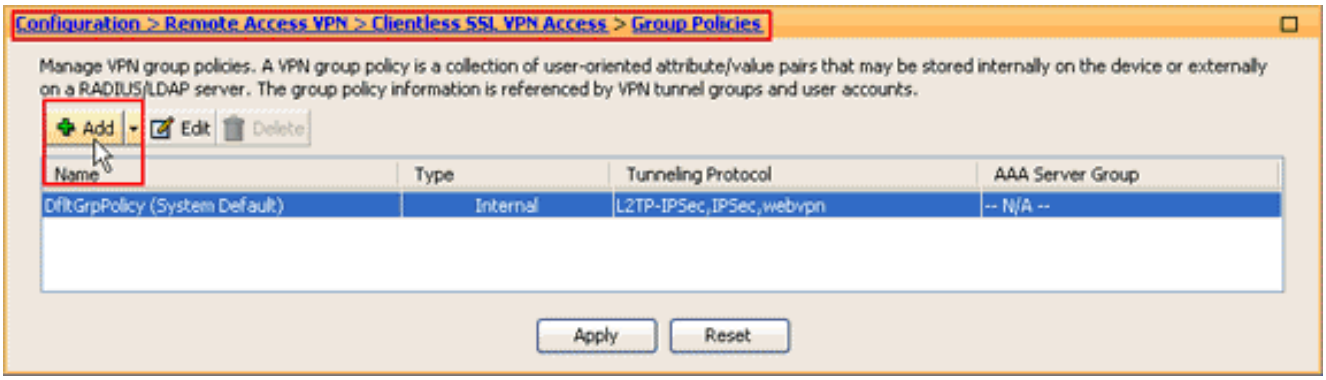


4. No campo do ID de aplicativo, entre em uma corda para identificar a entrada dentro da lista esperta do túnel.
5. Incorpore um nome de arquivo e uma extensão para o aplicativo, e clique a **APROVAÇÃO**.
6. Na caixa de diálogo esperta da lista do túnel adicionar, clique a **APROVAÇÃO**.

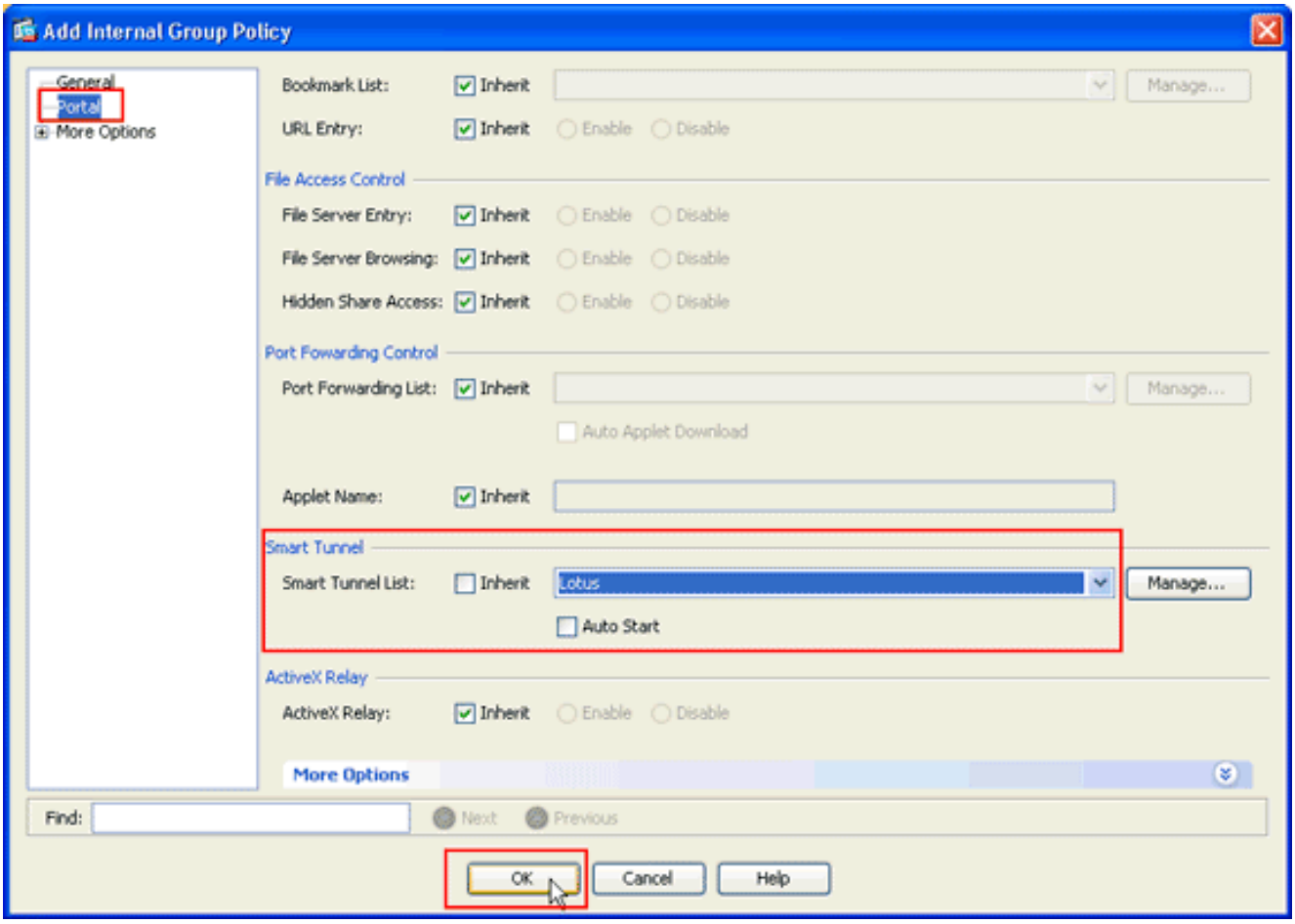


Nota: Está aqui o comando de configuração de CLI equivalente:

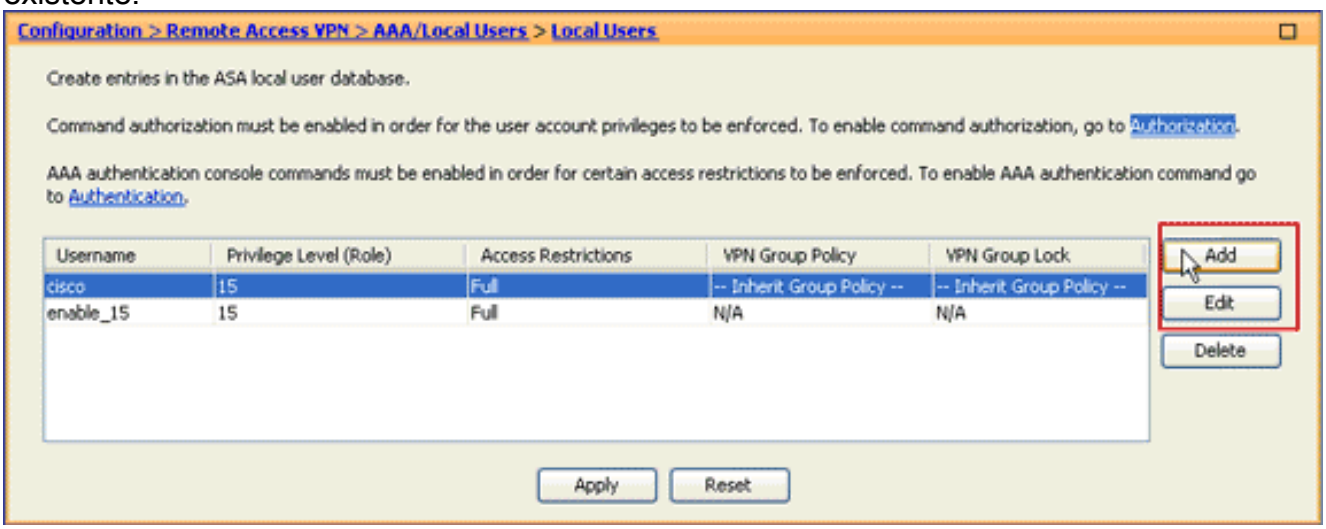
7. Atribua a lista às políticas do grupo e às políticas do usuário local a que você quer fornecer o acesso esperto do túnel aos aplicativos associados como segue:A fim atribuir a lista a uma política do grupo, para escolher **políticas do acesso > do grupo dos sem clientes SSL VPN da configuração > do Acesso remoto VPN>**, e clique **adicionar** ou **edite.**



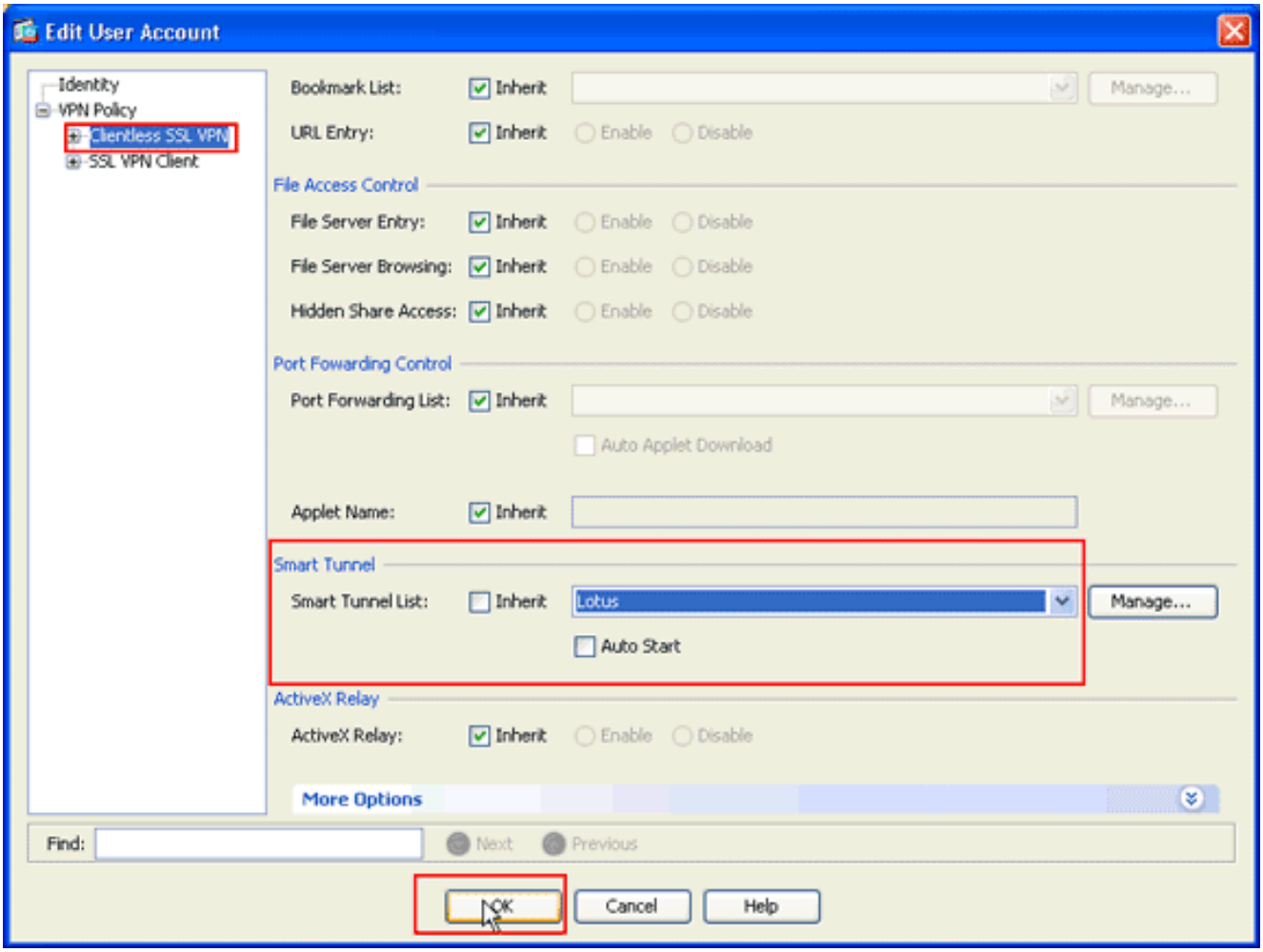
A caixa de diálogo da Política interna de grupo adicionar aparece.



8. Na caixa de diálogo da Política interna de grupo adicionar, clique o **portal**, escolha o nome de túnel esperto da lista de drop-down esperta da lista do túnel, e clique a **APROVAÇÃO**.**Nota:** Este exemplo usa *Lotus* como o nome de lista esperto do túnel.
9. A fim atribuir a lista a uma política do usuário local, para escolher a **configuração > o Acesso remoto VPN> AAA Setup > usuários locais**, e o clique **adiciona** para configurar configura um novo usuário ou o clique **edita** para editar um usuário existente.



A caixa de diálogo da conta de usuário da edição aparece.



10. Na caixa de diálogo da conta de usuário da edição, clique os **sem clientes SSL VPN**, escolha o nome de túnel esperto da lista de drop-down esperta da lista do túnel, e clique a **APROVAÇÃO**.**Nota:** Este exemplo usa *Lotus* como o nome de lista esperto do túnel.

A configuração de túnel esperta está completa.

Troubleshooting

Eu sou incapaz de conectar usando um túnel esperto marcado um endereço da Internet URL no portal dos sem clientes. Por que esta edição ocorre, e como posso eu resolvê-la?

Esta edição ocorre devido ao problema descrito na identificação de bug Cisco CSCsx05766 (clientes registrados somente). A fim resolver esta edição, degrade o tempo de execução de Java de encaixe a uma versão mais velha.

Posso eu truncar a URL de um link esperto do túnel configurado no WebVPN?

Quando o túnel esperto é usado no ASA, você não pode truncar a URL ou esconder a barra de endereços do navegador. Os usuários podem ver as URL dos links configurados no WebVPN que usam o túnel esperto. Em consequência, podem mudar a porta e alcançar o server para algum outro serviço.

A fim resolver esta edição, use WebType ACL. Refira a criação de WebType ACL para mais informação.

Informações Relacionadas

- Cisco ASA 5500 Series Adaptive Security Appliances
- Release Note para o cliente VPN de AnyConnect, liberação 2.3
- Exemplo de Configuração de Cliente VPN SSL (SVC) no ASA com o ASDM
- Suporte Técnico e Documentação - Cisco Systems