PIX/ASA: Exemplo de configuração da característica da atualização automática do cliente do IPSec VPN

Índice

Introdução

Este documento descreve como configurar a característica da atualização automática do Cisco VPN Client na ferramenta de segurança e no Dispositivos de segurança Cisco PIX série 500 adaptáveis do 5500 Series de Cisco ASA.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

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

- A ferramenta de segurança adaptável do 5500 Series de Cisco ASA executa a versão 7.x e mais recente
- Versão 7.x e mais recente das corridas do Dispositivos de segurança Cisco PIX série 500
- Versão 5.x e mais recente do Cisco Adaptive Security Device Manager (ASDM)
- Cisco VPN Client 4.x e mais tarde

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.

Como configurar a atualização do cliente para Windows com CLI

A característica da atualização do cliente deixa administradores em um local central automaticamente notificar usuários de cliente VPN quando é hora de atualizar o software do cliente VPN e a imagem do VPN 3002 Hardware Client.

Emita o comando da **atualização do cliente no** modo de configuração dos IPsec-`atributos do grupo de túneis` a fim configurar a atualização do cliente. Se o cliente já está executando uma versão de software na lista de números de revisão, não precisa de atualizar seu software. Se o cliente não executa uma versão de software na lista, deve atualizar. Você pode especificar até quatro entradas da atualização do cliente.

Veja abaixo a seqüência dos comandos:

client-update type *type* {url *url-string*} {rev-nums *rev-nums*} no client-update *[type]*

- **rev-NUM rev-***NUM* — Especifica o software ou as imagens de firmware para este cliente. Incorpore até quatro, separado por vírgulas.
- *tipo* — Especifica os sistemas operacionais para notificar de uma atualização do cliente. A lista de sistemas operacionais compreende destes:Microsoft Windows: todas as Plataformas baseados no WindowsWIN9X: Windows 95, Windows 98, e Windows MIM PlataformasWinNT: Plataformas do Windows NT 4.0, do Windows 2000, e do Windows XPvpn3002: VPN 3002 Hardware Client
- *série de URL* **URL** — Especifica a URL para o software/imagem de firmware. Esta URL deve apontar a um arquivo apropriado para o cliente.

Este exemplo configura parâmetros da atualização do cliente para o grupo de túneis do acesso remoto chamado remotegrp. Designa o número de revisão 4.6.1 e a URL para a recuperação da atualização, que é `https://support/updates`.

ASA
hostname(config)#**tunnel-group remotegrp type ipsec_ra** hostname(config)#**tunnel-group remotegrp ipsec-attributes** hostname(config-ipsec)#**client-update type windows url https://support/updates/rev-nums 4.6.1**

Como configurar a atualização do cliente para Windows com ASDM

Este documento supõe que a configuração básica, como a configuração da interface esteja pronta e funcionando corretamente.

Refira permitir o acesso HTTPS para o ASDM a fim permitir que o ASA seja configurado pelo ASDM

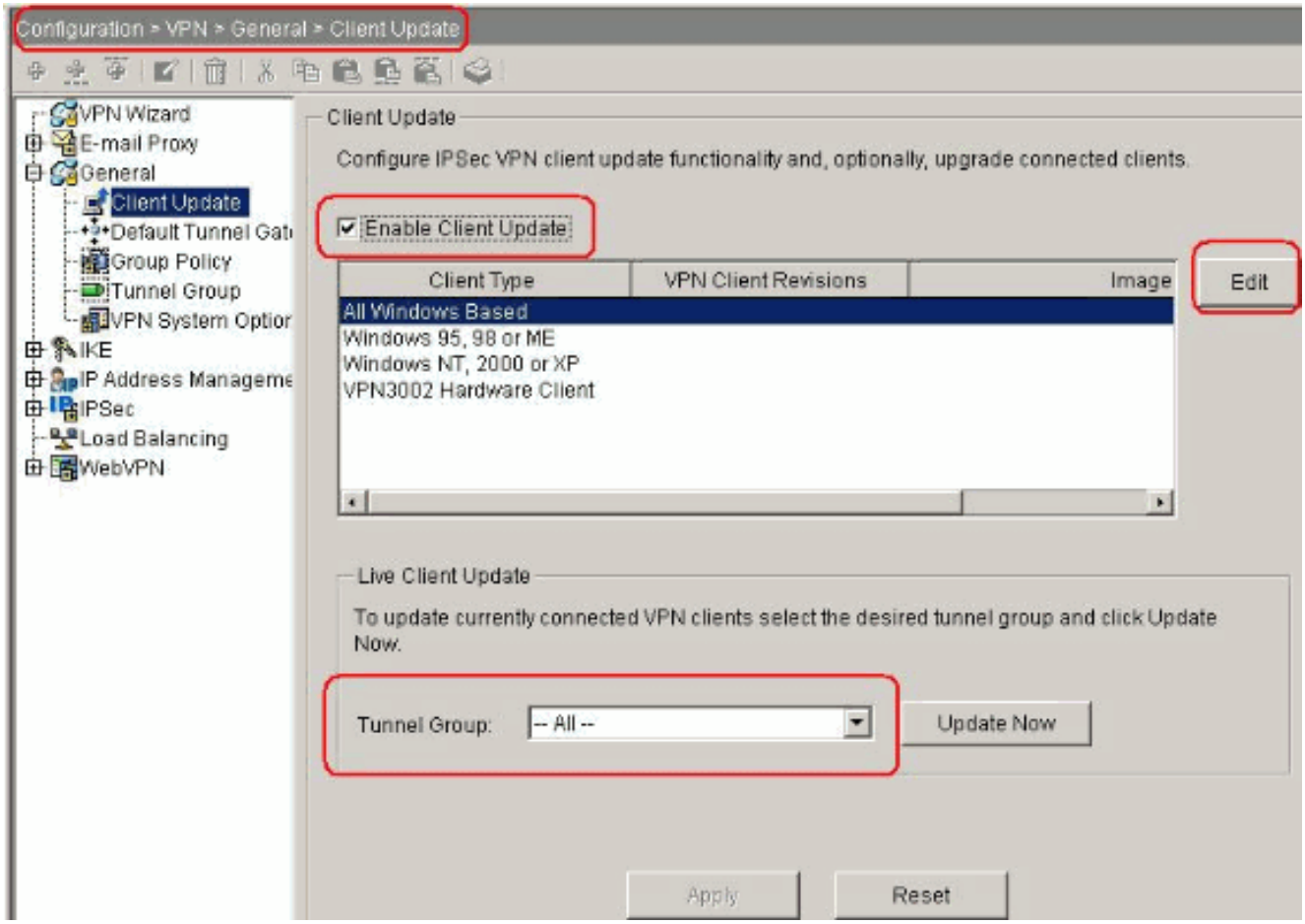
O ASDM abrange dois tipos da atualização do cliente: um que apoia clientes do Windows e VPN 3002 Hardware Client através de um grupo de túneis, e o outro que apoia os dispositivos ASA que atuam como um Auto Update Server.

Os usuários remotos podem usar versões antiquadas do software de VPN ou do cliente da ferragem. Você pode executar uma atualização do cliente a qualquer hora para fazer estas funções:

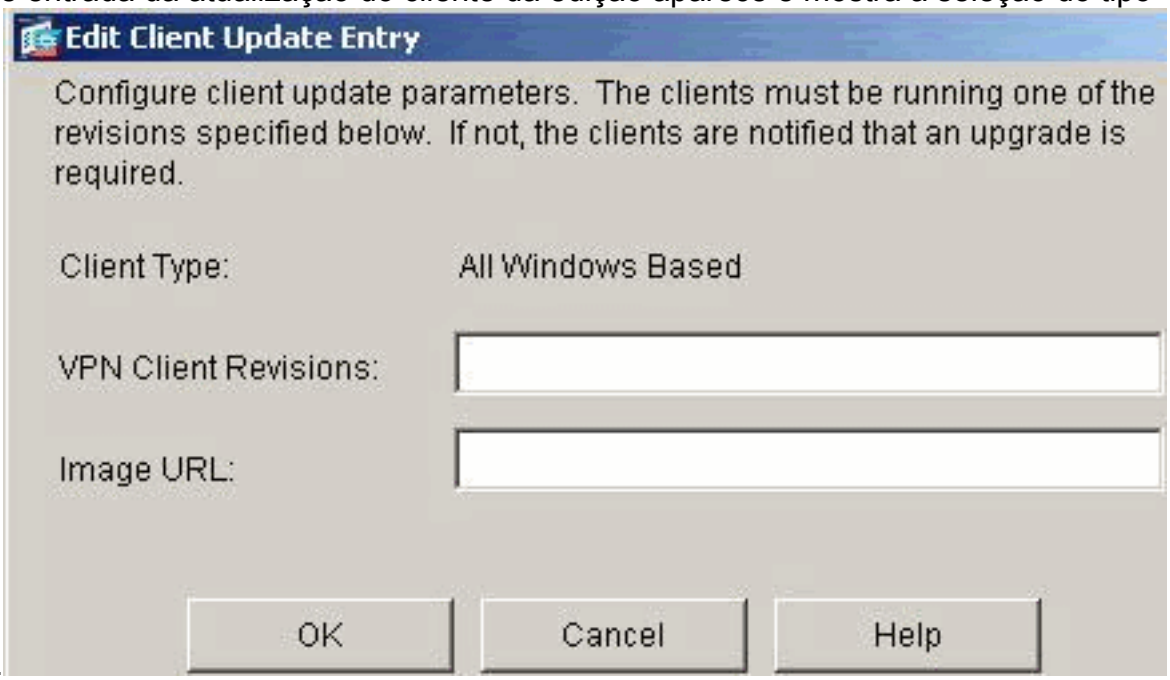
- Enable que atualiza revisões do cliente.
- Especifique os tipos e os números de revisão de clientes a que a atualização se aplica.
- Forneça uma URL ou um endereço IP de Um ou Mais Servidores Cisco ICM NT de que para obter a atualização.
- Notifique opcionalmente usuários de cliente do Windows que devem atualizar sua versão do cliente VPN.
- Para clientes do Windows, você pode fornecer um mecanismo para que os usuários realizem a atualização.
- Para usuários de VPN 3002 Hardware Client, a atualização ocorre automaticamente, sem a notificação.

Termine estas etapas a fim configurar uma atualização do cliente:

1. Escolha a **configuração > o VPN > o general > a atualização do cliente** a fim ir ao indicador da atualização do cliente. O indicador da atualização do cliente abre.Verifique a caixa de verificação da **atualização do cliente da possibilidade** a fim permitir a atualização do cliente.Escolha o tipo de cliente a que você quer aplicar a atualização do cliente. Os tipos de cliente disponíveis são **tudo baseados no Windows, Windows 95, 98 ou EU, o Windows NT 4.0, 2000 ou o XP, e o VPN 3002 Hardware Client.**Se o cliente já está executando uma versão de software na lista de números de revisão, não precisa de atualizar seu software. Se o cliente não está executando uma versão de software na lista, deve atualizar. Você pode especificar até três destas entradas da atualização do cliente. Toda a seleção baseada Windows cobre todas as plataformas Windows permissíveis. Se você seleciona este, não especifique os tipos individuais do cliente do Windows.O clique **edita** a fim especificar as revisões aceitáveis do cliente e a fonte para o software ou a imagem de firmware actualizado para a atualização do
   cliente.

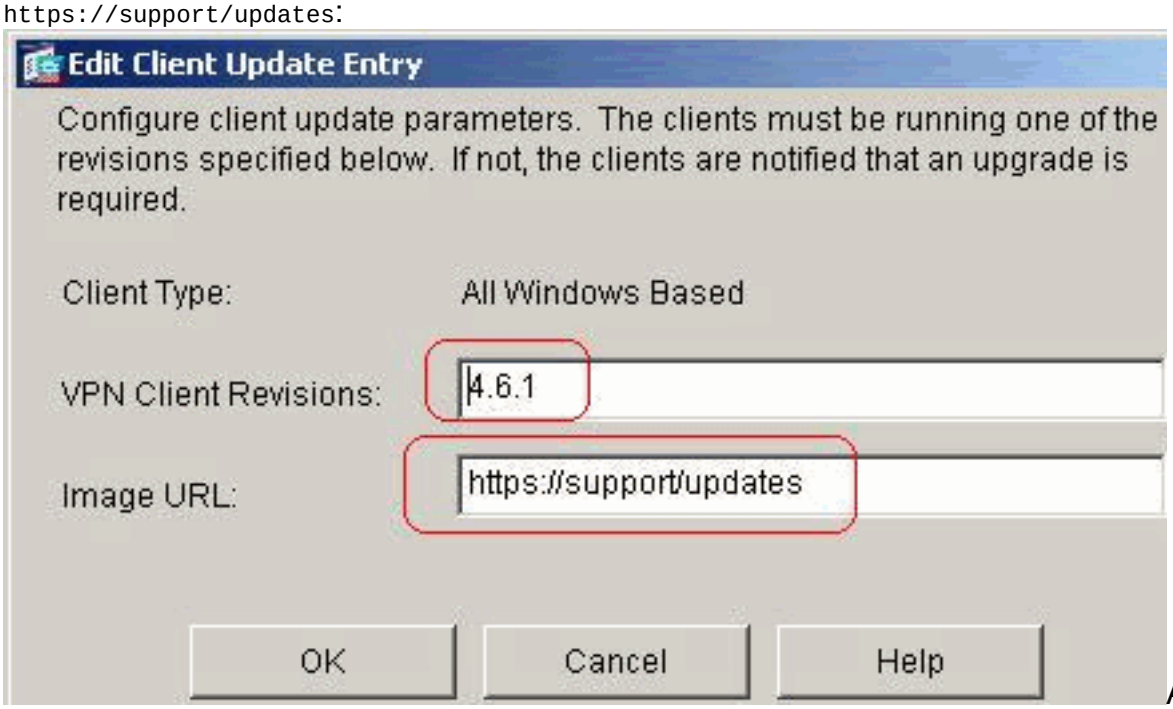


2. A janela de entrada da atualização do cliente da edição aparece e mostra a seleção do tipo de cliente.



3. Especifique a atualização do cliente que você quer aplicar a todos os clientes do tipo selecionado através da ferramenta de segurança inteira. Isto é, especifique o tipo de cliente, a URL ou o endereço IP de Um ou Mais Servidores Cisco ICM NT de que para obter a imagem actualizado, e o número de revisão ou os números aceitáveis para esse cliente. Você pode especificar até quatro números de revisão, separados por vírgulas. Suas entradas parecem nas colunas apropriadas a tabela no indicador da elevação do cliente depois que você clica a **APROVAÇÃO**.Se o número de revisão do cliente combina um dos números de revisão especificados, não há nenhuma necessidade de atualizar o cliente.**Nota:** Para todos os clientes do Windows, você deve usar o protocolo http:// ou

https:// como o prefixo para a URL. Para o VPN 3002 Hardware Client, você deve especificar o protocolo tftp:// pelo contrário.Inicia uma atualização do cliente para todos os clientes do Windows para as revisões running de um grupo de túneis do acesso remoto mais velhas de 4.6.1 e especifica a URL para a recuperação da atualização como `https://support/updates`:



Alternativamente, você pode configurar a atualização do cliente apenas para tipos de cliente individuais, um pouco do que para todos os clientes do Windows, que você pode ver se a etapa 1-c.A atualização dos clientes do VPN 3002 sem intervenção de usuário e os usuários não recebem nenhum mensagem de notificação.Você pode mandar o navegador automaticamente começar um aplicativo se você inclui o nome do aplicativo no fim da URL; por exemplo: **https://support/updates/vpnclient.exe.**

4. Opcionalmente, você pode enviar uma observação aos usuários ativo com clientes do Windows antiquados que precisam de atualizar seu cliente. Use a área viva da atualização do cliente do indicador da atualização do cliente a fim enviar esta observação. Escolha o grupo de túneis (ou tudo) e clique a **atualização agora**. Uma caixa de diálogo parece na figura e pede que você confirme que você quer notificar clientes conectados sobre a elevação.

Os usuários designados veem uma janela pop-up, que lhes ofereça a oportunidade de lançar um navegador e de transferir o software actualizado do local que você especificou na URL. O único parte de esta mensagem que você pode configurar é a URL. (Veja as etapas 1-b ou 1-c.) Os usuários que não são ativos recebem um mensagem de notificação a próxima vez

que entram. Você pode enviar esta observação a todos os clientes ativo em todos os grupos de túneis, ou você pode enviá-la aos clientes em um grupo do túnel específico.Se o número de revisão do cliente combina um dos números de revisão especificados, não há nenhuma necessidade de atualizar o cliente, e nenhum mensagem de notificação é enviado ao usuário. A atualização dos clientes do VPN 3002 sem intervenção de usuário e os usuários não recebem nenhum mensagem de notificação.

Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

Informações Relacionadas

- Suporte Técnico e Documentação - Cisco Systems