PIX/ASA como um servidor de VPN remoto com autenticação extendida usando o CLI e o exemplo da configuração ASDM

Índice

Introdução

Este documento descreve como configurar o Adaptive Security Appliance (ASA) da Cisco 5500 Series para atuar como um servidor de VPN remoto usando o Adaptive Security Device Manager (ASDM) ou a CLI. O ASDM oferece gerenciamento de segurança de nível mundial e monitoramento através de uma interface de gerenciamento baseada na Web intuitiva e fácil de usar. Quando a configuração de roteador Cisco estiver concluída, ela pode ser verificada usando o Cisco VPN Client.

Refira PIX/ASA 7.x e Cisco VPN Client 4.x com exemplo da configuração de autenticação do RAIO de Windows 2003 IAS (contra o diretório ativo) a fim estabelecer a conexão VPN de acesso remoto entre um Cisco VPN Client (4.x para Windows) e a ferramenta de segurança 7.x da série PIX 500. O usuário de cliente VPN remoto autentica contra o diretório ativo usando um servidor Radius do Internet Authentication Service de Microsoft Windows 2003 (IAS).

Refira PIX/ASA 7.x e Cisco VPN Client 4.x para o exemplo da configuração de autenticação do Cisco Secure ACS a fim estabelecer uma conexão VPN de acesso remoto entre um Cisco VPN Client (4.x para Windows) e a ferramenta de segurança 7.x da série PIX 500 usando um Serviço de controle de acesso Cisco Secure (versão de ACS 3.2) para a autenticação extendida

(XAUTH).

Pré-requisitos

Requisitos

Este documento supõe que o ASA é plenamente operacional e configurado para permitir que Cisco ASDM ou CLI faça alterações de configuração.

Nota: Refira permitir o acesso HTTPS para ASDM ou PIX/ASA 7.x: SSH no exemplo de configuração da interface interna e externa para permitir que o dispositivo seja configurado remotamente pelo ASDM ou pelo Shell Seguro (ssh).

Componentes Utilizados

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

- Versão de software adaptável 7.x da ferramenta de segurança de Cisco e mais tarde
- Versão 5.x e mais recente adaptável do Security Device Manager
- Versão Cliente VPN Cisco 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.

Produtos Relacionados

Esta configuração pode igualmente ser usada com versão 7.x e mais recente da ferramenta de segurança de Cisco PIX.

Convenções

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

Informações de Apoio

As configurações do Acesso remoto fornecem o Acesso remoto seguro para Cisco VPN Client, tais como usuários móveis. Um acesso remoto VPN deixa usuários remotos firmemente alcançar recursos de rede centralizada. O Cisco VPN Client segue com o protocolo IPSec e é projetado especificamente trabalhar com a ferramenta de segurança. Contudo, a ferramenta de segurança pode estabelecer conexões IPSec com muitos clientes protocolo-complacentes. Refira os manuais de configuração ASA para obter mais informações sobre do IPsec.

Os grupos e os usuários são conceitos do núcleo no Gerenciamento da Segurança dos VPN e na configuração da ferramenta de segurança. Especificam os atributos a que determine o acesso de usuários e o uso do VPN. Um grupo é uma coleção de usuários tratada como uma entidade única. Os usuários obtêm seus atributos das políticas do grupo. Os grupos de túneis identificam a política do grupo para conexões específicas. Se você não atribui a uma política do grupo

particular ao usuários, a política do grupo padrão para a conexão aplica-se.

Um grupo de túneis consiste em um grupo de registros que determine políticas da conexão de túnel. Estes registros identificam os server a que os server a que os usuários do túnel são autenticados, assim como os servidores de contabilidade, eventualmente, a que a informação das conexões é enviada. Igualmente identificam uma política do grupo padrão para as conexões, e contêm parâmetros de conexão do específico de protocolo. Os grupos de túneis incluem um pequeno número de atributos que se refere a criação do túnel própria. Os grupos de túneis incluem um ponteiro a uma política do grupo que defina atributos USER-orientados.

Nota: Na configuração de exemplo neste documento, as contas de usuário local são usadas para a autenticação. Se você gostaria de usar um outro serviço, tal como o LDAP e o RAIO, refira configurar um servidor de raio externo para a autorização e a autenticação.

O Internet Security Association and Key Management Protocol (ISAKMP), igualmente chamado IKE, é o protocolo da negociação que os anfitriões concordam com como construir uma associação de segurança IPSec. Cada negociação de ISAKMP é dividida em duas seções, Phase1 e Phase2. Phase1 cria o primeiro túnel para proteger umas mensagens mais atrasadas da negociação de ISAKMP. Phase2 cria o túnel que protege os dados que viajam através da conexão segura. Refira palavras-chaves da política de ISAKMP para comandos CLI para obter mais informações sobre do ISAKMP.

Configurações

Configurar o ASA/PIX como um servidor de VPN remoto usando o ASDM

Termine estas etapas a fim configurar Cisco ASA como um servidor de VPN remoto usando o ASDM:

1. Selecione **assistentes > wizard VPN do** indicador home.
2. Selecione o tipo de túnel do **acesso remoto VPN** e assegure-se de que a interface de túnel VPN esteja ajustada como desejada.
3. O único tipo do cliente VPN disponível é selecionado já. Clique em Next.
4. Dê entrada com um nome para o nome de grupo de túneis. Forneça a informação da autenticação para usar-se.**A chave pré-compartilhada** é selecionada neste exemplo.**Nota:** Não há uma maneira de esconder/cifra a chave pré-compartilhada no ASDM. A razão é que o ASDM deve somente ser usado pelos povos que configuram o ASA ou pelos povos que estão ajudando ao cliente com esta configuração.
5. Escolha se você quer usuários remotos ser autenticado à base de dados de usuário local ou a um Grupo de servidores AAA externo.**Nota:** Você adiciona usuários à base de dados de usuário local na etapa 6.**Nota:** Refira grupos de servidor da authentication e autorização PIX/ASA 7.x para usuários VPN através do exemplo da configuração ASDM para obter informações sobre de como configurar um Grupo de servidores AAA externo através do ASDM.
6. Adicionar usuários ao base de dados local caso necessário.**Nota:** Não remova os usuários existentes deste indicador. Selecione a **configuração > a administração do dispositivo > a administração > as contas de usuário na janela principal de ASDM** para editar entradas existentes no base de dados ou para removê-las do base de dados.
7. Defina um pool dos endereços locais a ser atribuídos dinamicamente aos clientes VPN

remotos quando conectam.
8. *Opcional:* Especifique o DNS e GANHE a informação do servidor e um Domain Name do padrão a ser empurrado para clientes VPN remotos.
9. Especifique os parâmetros para o IKE, igualmente conhecidos como a fase 1. IKE.As configurações em ambos os lados do túnel devem combinar exatamente. Contudo, o Cisco VPN Client seleciona automaticamente a configuração apropriada para se. Consequentemente, nenhuma configuração de IKE é necessária no PC cliente.
10. Especifique os parâmetros para o IPsec, igualmente conhecidos como a fase 2. IKE.As configurações em ambos os lados do túnel devem combinar exatamente. Contudo, o Cisco VPN Client seleciona automaticamente a configuração apropriada para se. Consequentemente, nenhuma configuração de IKE é necessária no PC cliente.
11. Especifique qual, eventualmente, os host internos ou as redes devem ser expostos aos usuários remotos VPN.Se você deixa esta lista vazia, permite que os usuários remotos VPN alcancem a rede interna inteira do ASA.Você pode igualmente permitir o Split Tunneling neste indicador. O Split Tunneling cifra o tráfego aos recursos definidos mais cedo neste procedimento e fornece acesso unencrypted ao Internet em grande não escavando um túnel esse tráfego. Se o Split Tunneling não é permitido, todo o tráfego dos usuários remotos VPN está escavado um túnel ao ASA. Esta pode transformar-se muito largura de banda e utilização de processador, com base em sua configuração.
12. Este indicador mostra um sumário das ações que você tomou. Clique o **revestimento** se você é satisfeito com sua configuração.

Configurar o ASA/PIX como um servidor de VPN remoto usando o CLI

Termine estas etapas a fim configurar um servidor de acesso remoto VPN da linha de comando. Refira configurar referências adaptáveis do Dispositivo-comando da Segurança do 5500 Series dos acessos remoto VPN ou do Cisco ASA para obter mais informações sobre de cada comando que é usado.

1. Inscreva o **comando ip local pool no** modo de config global a fim configurar associações do endereço IP de Um ou Mais Servidores Cisco ICM NT para usar-se para túneis de acesso remoto VPN. A fim suprimir de conjuntos de endereços, não incorpore nenhum formulário deste comando.A ferramenta de segurança usa os conjuntos de endereços baseados no grupo de túneis para a conexão. Se você configura mais de um conjunto de endereços para um grupo de túneis, a ferramenta de segurança usa-os na ordem em que são configurados. Emita este comando a fim criar um pool dos endereços locais que podem ser usados para atribuir endereços dinâmicos aos clientes VPN de acesso remoto:`ASA-AIP-CLI(config)#` **`ip local pool vpnpool 172.16.1.100-172.16.1.199 mask 255.255.255.0`**
2. Emita este comando:`ASA-AIP-CLI(config)#` **`username marty password 12345678`**
3. Emita este conjunto de comandos a fim configurar o túnel específico:**Política ASA-**AIP-CLI(config)#isakmp **1 pré associação de autenticação**ASA-AIP-CLI(config)#isakmp **criptografia 3des da política 1**ASA-AIP-CLI(config)#isakmp **sha da mistura da política 1**ASA-AIP-CLI(config)#isakmp **grupo2 da política 1**ASA-AIP-CLI(config)#isakmp **vida 43200 da política 1**O ASA-AIP-CLI(config)#isakmp **permite foraEsp-sha-hmac do esp-3des do conjunto de transformação ESP-3DES-SHA do IPsec ASA-**AIP-CLI(config)#crypto**Conjunto de transformação ajustado ESP-3DES-SHA do outside_dyn_map 10 do mapa dinâmico ASA-**AIP-CLI(config)#crypto**Reverso-rota ajustada do outside_dyn_map 10 do mapa dinâmico ASA-**AIP-CLI(config)#crypto**A vida ajustada da associação de segurança do**

outside_dyn_map 10 do mapa dinâmico ASA-AIP-CLI(config)#crypto **secunda 288000Outside_dyn_map dinâmico do outside_map 10 IPsec-ISAKMP do mapa ASA-**AIP-CLI(config)#crypto**Relação do outside_map do mapa ASA-**AIP-CLI(config)#crypto **fora**ASA-AIP-CLI(config)#crypto **isakmp NAT-Traversal**

4. *Opcional:* Se você como a conexão contornearia a lista de acesso que é aplicada à relação, emita este comando:`ASA-AIP-CLI(config)#`**`sysopt connection permit-ipsec`** **Nota:** Este comando trabalha nas imagens 7.x antes de 7.2(2). Se você usa a imagem 7.2(2), emita ASA-`AIP-CLI(config)#sysopt o` comando da `conexão licença-VPN`.
5. Emita este comando:`ASA-AIP-CLI(config)#`**`group-policy hillvalleyvpn internal`**
6. Emita estes comandos a fim configurar ajustes da conexão de cliente:**atributos do hillvalleyvpn da ASA-AIP-CLI(config)#group-**política(Configuração-grupo-política) **valor 172.16.1.11 do #dns-**server ASA-AIP-CLI(config)#(Configuração-grupo-política) **IPsec do #vpn-túnel-**protocolo ASA-AIP-CLI(config)#(Configuração-grupo-política) **valor test.com do #default-**domínio ASA-AIP-CLI(config)#
7. Emita este comando:`ASA-AIP-CLI(config)#`**`tunnel-group hillvalleyvpn ipsec-ra`**
8. Emita este comando:`ASA-AIP-CLI(config)#`**`tunnel-group hillvalleyvpn ipsec-attributes`**
9. Emita este comando:`ASA-AIP-CLI(config-tunnel-ipsec)#`**`pre-shared-key cisco123`**
10. Emita este comando:`ASA-AIP-CLI(config)#`**`tunnel-group hillvalleyvpn general-attributes`**
11. Emita este comando a fim consultar a base de dados de usuário local para a autenticação.`ASA-AIP-CLI(config-tunnel-general)#`**`authentication-server-group LOCAL`**
12. Associe a política do grupo ao grupo do túnel.`ASA-AIP-CLI(config-tunnel-ipsec)#` **`default-group-policy hillvalleyvpn`**
13. Emita este comando quando no modo dos geral-atributos do grupo de túneis do hillvalleyvpn a fim atribuir o vpnpool criado em etapa 1 ao grupo do hillvalleyvpn.`ASA-AIP-CLI(config-tunnel-general)#`**`address-pool vpnpool`**

Configuração running no dispositivo ASA

```
ASA-AIP-CLI(config)#show running-config ASA Version
7.2(2) ! hostname ASAwAIP-CLI domain-name corp.com
enable password WwXYvtKrnjXqGbu1 encrypted names !
interface Ethernet0/0 nameif outside security-level 0 ip
address 10.10.10.2 255.255.255.0 ! interface Ethernet0/1
nameif inside security-level 100 ip address 172.16.1.2
255.255.255.0 ! interface Ethernet0/2 shutdown no nameif
no security-level no ip address ! interface Ethernet0/3
shutdown no nameif no security-level no ip address !
interface Management0/0 shutdown no nameif no security-
level no ip address ! passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive dns server-group DefaultDNS domain-name
corp.com pager lines 24 mtu outside 1500 mtu inside 1500
ip local pool vpnpool 172.16.1.100-172.16.1.199 mask
255.255.255.0 no failover icmp unreachable rate-limit 1
burst-size 1 no asdm history enable arp timeout 14400
timeout xlate 3:00:00 timeout conn 1:00:00 half-closed
0:10:00 udp 0:02:00 icmp 0:00:02 timeout sunrpc 0:10:00
h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00
sip-disconnect 0:02:00 timeout uauth 0:05:00 absolute
group-policy hillvalleyvpn1 internal group-policy
hillvalleyvpn1 attributes dns-server value 172.16.1.11
vpn-tunnel-protocol IPSec default-domain value test.com
username marty password 6XmYwQOO9tiYnUDN encrypted no
snmp-server location no snmp-server contact snmp-server
enable traps snmp authentication linkup linkdown
coldstart crypto ipsec transform-set ESP-3DES-SHA esp-
3des esp-sha-hmac crypto dynamic-map outside_dyn_map 10
```

```
set transform-set ESP-3DES-SHA crypto dynamic-map
outside_dyn_map 10 set security-association lifetime
seconds 288000 crypto map outside_map 10 ipsec-isakmp
dynamic outside_dyn_map crypto map outside_map interface
outside crypto isakmp enable outside crypto isakmp
policy 10 authentication pre-share encryption 3des hash
sha group 2 lifetime 86400 crypto isakmp nat-traversal
20 tunnel-group hillvalleyvpn type ipsec-ra tunnel-group
hillvalleyvpn general-attributes address-pool vpnpool
default-group-policy hillvalleyvpn tunnel-group
hillvalleyvpn ipsec-attributes pre-shared-key * telnet
timeout 5 ssh timeout 5 console timeout 0 ! class-map
inspection_default match default-inspection-traffic ! !
policy-map type inspect dns preset_dns_map parameters
message-length maximum 512 policy-map global_policy
class inspection_default inspect dns preset_dns_map
inspect ftp inspect h323 h225 inspect h323 ras inspect
netbios inspect rsh inspect rtsp inspect skinny inspect
esmtp inspect sqlnet inspect sunrpc inspect tftp inspect
sip inspect xdmcp ! service-policy global_policy global
prompt hostname context
Cryptochecksum:0f78ee7ef3c196a683ae7a4804ce1192 : end
ASA-AIP-CLI(config)#
```

Configuração do armazenamento de senha do Cisco VPN Client

Se você tem Cisco VPN Client numerosos, é muito duro recordar todos os nomes de usuário e senha do cliente VPN. A fim armazenar as senhas na máquina de cliente VPN, configurar o ASA/PIX e o cliente VPN como esta seção descreve.

ASA/PIX

Use o **comando group-policy attributes no** modo de configuração global:

```
group-policy VPNusers attributes password-storage enable
```

Cisco VPN Client

Edite o **arquivo do .pcf** e altere estes parâmetros:

```
SaveUserPassword=1 UserPassword= <type your password>
```

Desabilite a autenticação extendida

No modo do grupo de túneis, incorpore este comando a fim desabilitar a autenticação extendida, que é permitida à revelia, no PIX/ASA 7.x:

```
asa(config)#tunnel-group client ipsec-attributes asa(config-tunnel-ipsec)#isakmp ikev1-user-
authentication none
```

Depois que você desabilita a autenticação extendida, os clientes VPN não fazem PNF-acima um username/senha para uma autenticação (Xauth). Consequentemente, o ASA/PIX não exige a configuração do nome de usuário e senha autenticar os clientes VPN.

Verificar

Tente conectar a Cisco ASA usando o Cisco VPN Client a fim verificar que o ASA está configurado com sucesso.

1. Selecione **entradas de conexão > novo**.
2. Preencha os detalhes de sua nova conexão.O campo do host deve conter o endereço IP ou nome do host de Cisco previamente configurado ASA. A informação da autenticação do grupo deve corresponder àquela usada na **salvaguarda do** clique de etapa 4. quando você é terminado.
3. Selecione a conexão recém-criado, e o clique **conecta**.
4. Incorpore um nome de usuário e senha para a autenticação extendida. Esta informação deve combinar aquela especificada nas etapas 5 e 6.
5. Uma vez que a conexão é **estatísticas** seletas com sucesso estabelecidas do menu de status para verificar os detalhes do túnel.Este indicador mostra o tráfego e a informação de criptografia:Este indicador mostra a informação do Split Tunneling:

Troubleshooting

Use esta seção para resolver problemas de configuração.

ACL cripto incorreto

O ASDM 5.0(2) é sabido para criar e para aplicar um Access Control List cripto (ACL) que possa causar problemas para os clientes VPN que usam o Split Tunneling, assim como para clientes da ferragem no modo da extensão de rede. Use a versão 5.0(4.3) ou mais recente ASDM para evitar este problema. Refira a identificação de bug Cisco CSCsc10806 (clientes registrados somente) para mais detalhes.

Informações Relacionadas

- Cisco ASA 5500 Series Adaptive Security Appliances
- A maioria de IPSec VPN comum L2L e de Acesso remoto que pesquisa defeitos soluções
- O Dispositivos de segurança adaptáveis Cisco ASA série 5500 pesquisa defeitos e alertas
- Suporte Técnico e Documentação - Cisco Systems