ASA/PIX: Passagem-através do tráfego que esclarece os clientes VPN que usam o exemplo da configuração ACS

Índice

Introdução

Este documento fornece uma configuração de exemplo esclarecendo os clientes VPN (IPsec/SSL) que usam o PIX/ASA O ACS. A ferramenta de segurança adaptável pode enviar a informação de contabilidade a um server do RAIO ou TACACS+ sobre todo o tráfego TCP ou UDP que passar através da ferramenta de segurança adaptável. Se esse tráfego é autenticado igualmente, a seguir o servidor AAA pode manter a informação de contabilidade pelo username. Se o tráfego não é autenticado, o servidor AAA pode manter a informação de contabilidade pelo endereço IP de Um ou Mais Servidores Cisco ICM NT. A informação de contabilidade inclui quando as sessões começam e param, username, o número de bytes que passam através da ferramenta de segurança adaptável para a sessão, o serviço usado, e a duração de cada sessão.

Antes que você possa usar este comando, você deve primeiramente designar um servidor AAA com o **comando aaa-server**. A informação de contabilidade está enviada somente ao servidor ativo em um grupo de servidor a menos que você permitir a contabilidade simultânea usando o comando contabilidade-**MODE no** modo da configuração de protocolo do AAA-server.

Você não pode usar o comando da **correspondência de contabilidade AAA na** mesma configuração enquanto a **contabilidade aaa inclui** e **comandos exclude**. Nós sugerimos que você use o **comando match** em vez **incluir** e dos **comandos exclude**; **incluir** e os **comandos exclude** não são apoiados pelo ASDM.

Este documento supõe que o acesso remoto VPN que usa ASA/PIX com configuração do cliente VPN do IPSec VPN Client/SSL (Anyconnect) com o ACS para a autenticação está feito já e

trabalha corretamente. Este documento focaliza em como configurar o AAA que esclarece clientes VPN na ferramenta de segurança ASA com ACS.

Refira PIX/ASA 7.x e Cisco VPN Client 4.x para o exemplo da configuração de autenticação do Cisco Secure ACS a fim aprender mais sobre como 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).

Refira ASA 8.x: Cliente VPN de AnyConnect para os Internet públicas VPN em um exemplo de configuração da vara a fim aprender mais sobre como estabelecer uma ferramenta de segurança adaptável (ASA) 8.0.2 para executar SSL VPN em uma vara com o Cisco AnyConnect VPN Client.

Pré-requisitos

Requisitos

Certifique-se que o cliente VPN pode estabelecer a conexão e alcançar corretamente o End to End.

Componentes Utilizados

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

- 5500 Series de Cisco ASA que executa 7.x e mais tarde
- Cisco Secure ACS 4.x

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

Este documento pode igualmente ser usado com a ferramenta de segurança da série do Cisco PIX 500 com versão de software 7.x e mais tarde.

Convenções

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

Configurar

Configuração ASA

Para configurar a contabilidade, execute estas etapas:

1. Se você quer a ferramenta de segurança adaptável fornecer dados de contabilidade pelo usuário, você deve permitir a autenticação. Se você quer a ferramenta de segurança adaptável fornecer dados de contabilidade pelo endereço IP de Um ou Mais Servidores Cisco ICM NT, permitir a autenticação não é necessária e você pode continuar a etapa 2.
2. Usando o **comando access-list**, crie uma lista de acessos que identifique os endereços de origem e os endereços de destino do tráfego que você quer expliquem.**Nota:** Se você configurou a autenticação e quer dados de contabilidade para todo o tráfego que está sendo autenticado, você pode usar a mesma lista de acessos que você criou para o uso com o **comando match da autenticação aaa**.
3. A fim permitir a contabilidade, incorpore este comando:`hostname(config)# aaa accounting match acl_name interface_name server_group` Em que:O argumento do *acl_name* é o nome da lista de acessos ajustado no **comando access-list**.O argumento do *interface_name* é o nome da relação ajustado no **comando nameif**.O argumento do *server_group* é o nome de grupo de servidor ajustado no **comando aaa-server**.**Nota:** Alternativamente, você pode usar o **comando include da contabilidade aaa** (que identifica o tráfego dentro do comando), mas você não pode usar ambos os métodos na mesma configuração. Veja a referência de comandos do Dispositivo de segurança adaptativo Cisco ASA 5580 para mais informação.

Estes comandos autenticam, autorizam, e esclarecem o tráfego de saída:

ASA

```
!--- Using the aaa-server command, identify your AAA
servers. If you have already !--- identified your AAA
servers, continue to the next step. hostname(config)#
aaa-server AuthOutbound protocol RADIUS hostname(config-
aaa-server-group)# exit !--- Identify the server,
including the AAA server group it belongs to and !---
enter the IP address, Shared key of the AAA Server.
hostname(config)# aaa-server AuthOutbound (inside) host
10.1.1.1 hostname(config-aaa-server-host)# key
TACPlusUauthKey hostname(config-aaa-server-host)# exit
!--- Using the access-list command, create an access
list that identifies the source !--- addresses
anddestination addresses of traffic you want to
authenticate. hostname(config)# access-list TELNET_AUTH
extended permit tcp any any eq telnet !--- Using the
access-list command, create an access list that
identifies the source !--- addresses anddestination
addresses of traffic you want to Authorize and
Accounting. hostname(config)# access-list SERVER_AUTH
extended permit tcp any any !--- configure
authentication, enter this command: hostname(config)#
aaa authentication match TELNET_AUTH inside AuthOutbound
!--- configure authorization, enter this command:
hostname(config)# aaa authorization match SERVER_AUTH
inside AuthOutbound
!--- This command causes the PIX Firewall to send !---
RADIUS accounting packets for RADIUS-authenticated
outbound sessions to the AAA !--- server group named
"AuthOutbound": hostname(config)# aaa accounting match
SERVER_AUTH inside AuthOutbound
```

Contabilidade do RAIO usando a configuração ACS

O registador CSV grava dados para atributos de registro nas colunas separadas por vírgulas (,).

Você pode importar este formato em uma variedade de aplicativos de terceiros, tais como Microsoft Excel ou Microsoft Access. Depois que você importa dados de um arquivo CSV em tais aplicativos, você pode preparar cartas ou executar perguntas, tais como a determinação do quantas horas um usuário foi registrado na rede durante um período dado. Para obter informações sobre de como usar um arquivo CSV em um aplicativo de terceiros tal como Microsoft Excel, veja a documentação do fornecedor de terceira parte.

Você pode alcançar os arquivos CSV no disco rígido do servidor ACS ou você pode transferir o arquivo CSV da interface da WEB.

Àrevelia, o ACS mantém arquivos de registro nos diretórios que são originais ao log. Você pode configurar a localização do arquivo de registro de logs CSV. Os diretórios padrão para todos os logs residem em **sysdrive: \ Arquivos de programa \ CiscoSecure ACS vx.x.**

A fim configurar o CiscoSecure ACS para executar a contabilidade do RAIO usando o CSV, execute estas etapas:

1. Na barra de navegação, clique em System Configuration.
2. Clique o **registro**. A página da configuração de registro publica-se.
3. Selecione a **contabilidade do RAIO CSV**.
4. Confirme que o **log à caixa de verificação de registro de contabilidade de CSV RADIUS** está selecionado. Se não é selecionado, selecione-o agora.
5. **Nos atributos seletos para registrar a** tabela, certifique-se de que os atributos RADIUS que você quer ver no log de contabilidade do RAIO aparecem na lista de **atributos registrada**. Além do que os atributos de RADIUS padrão, há diversos atributos de registro especiais fornecidos pelo CiscoSecure ACS, tal como o nome real, informação de ExtDB, e registrados remotamente.
6. (Opcional) se você está usando o server do CiscoSecure ACS for Windows, você pode especificar o Gerenciamento de arquivo de registro, que determina como os grandes arquivos de conta do RAIO podem ser, quanto são retidos, durante quanto tempo, e onde eles é armazenado.
7. Se você fez mudanças à configuração da contabilidade do RAIO, o clique **submete-se**. O CiscoSecure ACS salvar e executa as mudanças que você fez a sua configuração da contabilidade do RAIO.

Estes assuntos descrevem como ver e transferir relatórios ACS CSV:

- Nomes do arquivo de registro CSV
- Vendo um relatório CSV
- Transferindo um relatório CSV

Verificar

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

Troubleshooting

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

Informações Relacionadas

- Guia do Usuário para o Serviço de controle de acesso Cisco Secure 4.2 - Registro e relatórios
- Página de Suporte dos Cisco ASA 5500 Series Adaptive Security Appliances
- PIX/ASA: Corte-através do proxy para o acesso de rede usando o TACACS+ e o exemplo da configuração de servidor RADIUS
- Cisco Secure Access Control Server for Windows
- Cisco PIX 500 Series Security Appliances
- Suporte Técnico e Documentação - Cisco Systems