ASA/PIX: Tráfico del paso que explica a los clientes VPN que usan el ejemplo de la configuración de ACS

Contenido

Introducción

Este documento aporta una configuración de muestra para la contabilización de clientes VPN (IPSec/SSL) mediante el uso de PIX/ASA con ACS. El dispositivo de seguridad adaptable puede enviar información de contabilización al servidor RADIOS o TACAS+ sobre todo tipo de tráfico TCP o UDP que pase por este dispositivo de seguridad adaptable. Si ese tráfico también se autentica, después el servidor de AAA puede mantener la información de la cuenta por el nombre de usuario. Si el tráfico no se autentica, el servidor de AAA puede mantener la información de la cuenta por la dirección IP. La información de la cuenta incluye cuando las sesiones comienzan y paran, nombre de usuario, la cantidad de bytes que pasan a través del dispositivo de seguridad adaptante para la sesión, el servicio utilizado, y la duración de cada sesión.

Antes de que usted pueda utilizar este comando, usted debe primero señalar a un servidor de AAA con el **comando aaa-server**. La información de la cuenta se envía solamente al servidor activo en un grupo de servidores a menos que usted habilite las estadísticas simultáneas usando el comando estadística-**MODE** en el modo de la configuración del protocolo del AAA-servidor.

Usted no puede utilizar **coincidencia de contabilidad AAA el** comando en la misma configuración mientras que las **estadísticas aaa incluyen** y los **comandos exclude**. Sugerimos que usted utilice el **comando match** en vez del **incluir** y de los **comandos exclude**; **el incluir** y a los **comandos exclude** no soportan el ASDM.

Este documento asume que el VPN de acceso remoto usando ASA/PIX con la configuración del cliente VPN del IPSec VPN Client/SSL (Anyconnect) con el ACS para la autenticación está hecho

ya y trabaja correctamente. Este documento se centra en cómo configurar el AAA que explica a los clientes VPN en el dispositivo de seguridad ASA con el ACS.

Refiera al PIX/ASA 7.x y al Cliente Cisco VPN 4.x por el ejemplo de la configuración de autenticación del Cisco Secure ACS para aprender más sobre cómo configurar una conexión VPN de acceso remoto entre un Cliente Cisco VPN (4.x para Windows) y el dispositivo de seguridad 7.x de la serie PIX 500 usando un Cisco Secure Access Control Server (ACS versión 3.2) para el Autenticación ampliada (Xauth).

Refiera a ASA 8.x: Cliente VPN de AnyConnect para el Internet pública VPN en un ejemplo de configuración del palillo para aprender más sobre cómo configurar un dispositivo de seguridad adaptante (ASA) 8.0.2 para realizar SSL VPN en un palillo con el Cliente Cisco AnyConnect VPN.

prerrequisitos

Requisitos

Aseegurese al cliente VPN puede establecer la conexión y alcanzar el End to End correctamente.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- 5500 Series de Cisco ASA que ejecuta 7.x y posterior
- Cisco Secure ACS 4.x

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Productos Relacionados

Este documento se puede también utilizar con el dispositivo de seguridad de la serie del Cisco PIX 500 con la versión de software 7.x y posterior.

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

Configurar

Configuración ASA

Para configurar las estadísticas, realice estos pasos:

1. Si usted quisiera que el dispositivo de seguridad adaptante proporcionara los datos de

contabilidad por el usuario, usted debe habilitar la autenticación. Si usted quisiera que el dispositivo de seguridad adaptante proporcionara los datos de contabilidad por la dirección IP, habilitar la autenticación no es necesario y usted puede continuar al paso 2.

2. Usando el **comando access-list**, cree una lista de acceso que identifique a las direcciones de origen y consideraron las direcciones destino del tráfico que usted quiere.**Nota:** Si usted ha configurado la autenticación y quiere los datos de contabilidad para todo el tráfico que era autenticado, usted puede utilizar la misma lista de acceso que usted creó para el uso con el **comando match de la autenticación aaa**.
3. Para habilitar las estadísticas, ingrese este comando:`hostname(config)# aaa accounting match acl_name interface_name server_group` Donde:El argumento del *acl_name* es el nombre de la lista de acceso fijado en el **comando access-list**.El argumento del *interface_name* es el nombre de la interfaz fijado en el **comando nameif**.El argumento del *server_group* es el nombre de grupo de servidores fijado en el **comando aaa-server**.**Nota:** Alternativamente, usted puede utilizar el **comando include de las estadísticas aaa** (que identifica el tráfico dentro del comando), pero usted no puede utilizar ambos métodos en la misma configuración. Vea la referencia de comandos del Dispositivo de seguridad adaptable Cisco ASA 5580 para más información.

Estos comandos autentican, autorizan, y explican el tráfico saliente:

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
```

Estadísticas RADIUS usando la configuración de ACS

El maderero CSV registra los datos para los atributos de registración en las columnas separadas

por las comas (,). Usted puede importar este formato en una variedad de aplicaciones de terceros, tales como Microsoft Excel o Microsoft Access. Después de que usted importe los datos de a archivo CSV en tales aplicaciones, usted puede preparar las cartas o realizar las interrogaciones, tales como determinar cuántas horas registraron un usuario en la red durante un período dado. Para la información sobre cómo utilizar a archivo CSV en una aplicación de terceros tal como Microsoft Excel, vea la documentación del proveedor externo.

Usted puede acceder los archivos CSV en la unidad de disco duro del servidor ACS o usted puede descargar archivo CSV de la interfaz Web.

Por abandono, el ACS mantiene los archivos del registro los directorios que son únicos al registro. Usted puede configurar la ubicación de archivo de registro de los registros CSV. Los directorios predeterminados para todos los registros residen en **sysdrive: \ Archivos de programa \ CiscoSecure ACS vx.x.**

Para configurar el CiscoSecure ACS para realizar las estadísticas RADIUS usando el CSV, realice estos pasos:

1. En la barra de navegación, haga clic en Configuración del sistema.
2. Haga clic el **registro**. La página de la configuración de registro aparece.
3. Seleccione las **estadísticas CSV RADIUS**.
4. Confirme que el **registro a casilla de verificación del informe de contabilidad de radius CSV** está seleccionado. Si no se selecciona, ahora selecciónelo.
5. En los **atributos selectos para registrar la** tabla, aseegurese que los atributos de RADIUS que usted quiere ver en el archivo de registro RADIUS aparecen en la lista de **atributos registrada**. Además de los atributos RADIUS estándars, hay varios atributos especiales del registro proporcionados por el CiscoSecure ACS, tal como Nombre real, información de ExtDB, y registrados remotamente.
6. (Opcional) si usted está utilizando el servidor del CiscoSecure ACS for Windows, usted puede especificar la Administración de archivo del registro, que determina cómo los archivos de cuenta grandes del RADIO pueden ser, se conservan cuántos, durante cuánto tiempo, y se salva donde ellos.
7. Si usted ha realizado los cambios a la configuración de las estadísticas RADIUS, el tecleo **somete**. El CiscoSecure ACS guarda y implementa los cambios que usted realizó a su configuración de las estadísticas del RADIO.

Estos temas describen cómo ver y descargar los informes ACS CSV:

- Nombres del archivo del registro CSV
- Ver un informe CSV
- Descargar un informe CSV

Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

Troubleshooting

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

Información Relacionada

- Guía del usuario para el Cisco Secure Access Control Server 4.2 - Registro e informes
- Página de Soporte de Cisco ASA 5500 Series Adaptive Security Appliances
- PIX/ASA: Corte-por el proxy para el acceso a la red usando el TACACS+ y el ejemplo de la configuración de servidor de RADIUS
- Cisco Secure Access Control Server para Windows
- Dispositivos de seguridad Cisco PIX de la serie 500
- Soporte Técnico y Documentación - Cisco Systems