ASA/PIX 8.x: Ejemplo de Configuración de Radius Authorization (ACS 4.x) for VPN Access using Downloadable ACL with CLI and ASDM

Contenido

[Introducción](#)
[Prerequisites](#)
[Requirements](#)
[Componentes Utilizados](#)
[Productos Relacionados](#)
[Convenciones](#)
[Antecedentes](#)
[Configurar](#)
[Diagrama de la red](#)
[Configurar VPN de acceso remoto (IPSec)](#)
[Configurar ASA/PIX con la CLI](#)
[Configuración de Cisco VPN Client](#)
[Configuración de ACS para ACL descargable para usuarios individuales](#)
[Configuración de ACS para ACL descargable para el grupo](#)
[Configuración de RADIUS IETF para un Grupo de Usuarios](#)
[Verificación](#)
[Mostrar comandos criptográficos](#)
[ACL descargable para usuario/grupo](#)
[ACL con ID de filtro](#)
[Troubleshoot](#)
[Despeje las asociaciones de seguridad](#)
[Comandos para resolución de problemas](#)
[Información Relacionada](#)

Introducción

Este documento describe cómo configurar el dispositivo de seguridad para autenticar a los usuarios para el acceso a la red. Puesto que se pueden habilitar implícitamente las autorizaciones RADIUS, esta sección no contiene ninguna información sobre la configuración de la autorización RADIUS en el dispositivo de seguridad. Proporciona información sobre cómo gestiona el dispositivo de seguridad la información de la lista de acceso recibida de los servidores RADIUS.

Puede configurar un servidor RADIUS para descargar una lista de acceso al dispositivo de seguridad o un nombre de lista de acceso en el momento de la autenticación. El usuario está autorizado a hacer solamente lo que está permitido en la lista de acceso específica del usuario.

Las listas de acceso descargables son el medio más escalable cuando utiliza Cisco Secure ACS para proporcionar las listas de acceso adecuadas para cada usuario. Para obtener más información sobre las Funciones de la Lista de Acceso Descargable y Cisco Secure ACS, consulte Configuración de un Servidor RADIUS para Enviar Listas de Control de Acceso Descargables y ACL IP Descargables.

Consulte ASA 8.3 y versiones posteriores: Radius Authorization (ACS 5.x) for VPN Access Using Downloadable ACL with CLI and ASDM Configuration Example para obtener información sobre la configuración idéntica en Cisco ASA con las versiones 8.3 y posteriores.

Prerequisites

Requirements

Este documento asume que el ASA está completamente operativo y está configurado para permitir que el ASDM de Cisco o el CLI realice los cambios de configuración.

Nota: Refiérase a Cómo Permitir el Acceso HTTPS para ASDM o PIX/ASA 7.x: SSH en el Ejemplo de Configuración de la Interfaz Interna y Externa para permitir que el dispositivo sea configurado remotamente por ASDM o Secure Shell (SSH).

Componentes Utilizados

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

- Cisco Adaptive Security Appliance Software Version 7.x y posterior
- Cisco Adaptive Security Device Manager versión 5.x y posteriores
- Cisco VPN Client Version 4.x y posterior
- Cisco Secure Access Control Server 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). If your network is live, make sure that you understand the potential impact of any command.

Productos Relacionados

Esta configuración también se puede usar con Cisco PIX Security Appliance Version 7.x y posterior.

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Antecedentes

Puede utilizar ACL IP descargables para crear conjuntos de definiciones de ACL que puede aplicar a muchos usuarios o grupos de usuarios. Estos conjuntos de definiciones de ACL se denominan contenidos de ACL. Además, cuando incorpora NAF, controla el contenido ACL que se envía al cliente AAA desde el cual un usuario busca acceso. Es decir, una ACL IP descargable comprende una o más definiciones de contenido ACL, cada una de las cuales está asociada con un NAF o (de forma predeterminada) asociada a todos los clientes AAA. El NAF controla la aplicabilidad del contenido ACL especificado de acuerdo con la dirección IP del cliente AAA. Para obtener más información sobre los NAF y cómo regulan las ACL IP descargables, consulte Acerca de los Filtros de Acceso a la Red.

Las ACL IP descargables funcionan de esta manera:

1. Cuando ACS otorga a un usuario acceso a la red, ACS determina si una ACL IP descargable se asigna a ese usuario o al grupo del usuario.

2. Si ACS localiza una ACL IP descargable que se asigna al usuario o al grupo del usuario, determina si una entrada de contenido ACL está asociada con el cliente AAA que envió la solicitud de autenticación RADIUS.

3. ACS envía, como parte de la sesión de usuario, un paquete de aceptación de acceso RADIUS, un atributo que especifica la ACL nombrada y la versión de la ACL nombrada.

4. Si el cliente AAA responde que no tiene la versión actual de la ACL en su caché, es decir, la ACL es nueva o ha cambiado, ACS envía la ACL (nueva o actualizada) al dispositivo.

Las ACL IP descargables son una alternativa a la configuración de las ACL en el atributo Cisco-av-pair de RADIUS [26/9/1] de cada usuario o grupo de usuarios. Puede crear una ACL IP descargable una vez, darle un nombre y luego asignar la ACL IP descargable a cada usuario o grupo de usuarios aplicable si hace referencia a su nombre. Este método es más eficiente que si configura el atributo RADIUS Cisco-av-pair para cada usuario o grupo de usuarios.

Además, al emplear NAF, puede aplicar diferentes contenidos ACL al mismo usuario o grupo de usuarios con respecto al cliente AAA que utilizan. No es necesaria ninguna configuración adicional del cliente AAA después de haber configurado el cliente AAA para utilizar ACL IP descargables desde ACS. Las ACL descargables están protegidas por el régimen de copia de seguridad o replicación que haya establecido.

Cuando ingrese las definiciones de ACL en la interfaz web ACS, no utilice entradas de palabra clave o nombre; en todos los demás aspectos, utilice la sintaxis y semántica de comandos ACL estándar para el cliente AAA en el que pretende aplicar la ACL IP descargable. Las definiciones de ACL que ingresa en ACS comprenden uno o más comandos de ACL. Cada comando ACL debe estar en una línea independiente.

Puede agregar uno o más contenidos de ACL con nombre a una ACL IP descargable. De forma predeterminada, cada contenido ACL se aplica a todos los clientes AAA, pero, si ha definido NAF, puede limitar la aplicabilidad de cada contenido ACL a los clientes AAA que se enumeran en el

NAF que asocie a él. Es decir, cuando se emplean NAF, se puede hacer que cada contenido ACL, dentro de una única ACL IP descargable, se aplique a varios dispositivos de red diferentes o grupos de dispositivos de red de acuerdo con la estrategia de seguridad de la red.

Además, puede cambiar el orden del contenido de ACL en una ACL IP descargable. ACS examina el contenido de ACL, empezando desde la parte superior de la tabla, y descarga el primer contenido de ACL que encuentra con un NAF que incluye el cliente AAA que se utiliza. Al establecer el orden, puede garantizar la eficacia del sistema si coloca el contenido de ACL más aplicable en una posición superior de la lista. Debe darse cuenta de que, si sus NAF incluyen poblaciones de clientes AAA que se superponen, debe pasar de lo más específico a lo más general. Por ejemplo, ACS descarga cualquier contenido ACL con la configuración NAF All-AAA-Clients y no considera ninguno que esté más abajo en la lista.

Para utilizar una ACL IP descargable en un cliente AAA determinado, el cliente AAA debe seguir estas instrucciones:

- Usar RADIUS para autenticación
- Admitir ACL IP descargables

Estos son ejemplos de dispositivos de Cisco que admiten ACL IP descargables:

- Dispositivos ASA y PIX
- Concentradores VPN de la serie 3000
- Dispositivos de Cisco que ejecutan la versión 12.3(8)T o posterior del IOS

Este es un ejemplo del formato que debe utilizar para ingresar las ACL VPN 3000/ASA/PIX 7.x+ en el cuadro Definiciones de ACL:

```
permit ip 10.153.0.0 0.0.255.255 host 10.158.9.1
permit ip 10.154.0.0 0.0.255.255 10.158.10.0 0.0.0.255
permit 0 any host 10.159.1.22
deny ip 10.155.10.0 0.0.0.255 10.159.2.0 0.0.0.255 log
permit TCP any host 10.160.0.1 eq 80 log
permit TCP any host 10.160.0.2 eq 23 log
permit TCP any host 10.160.0.3 range 20 30
permit 6 any host HOSTNAME1
permit UDP any host HOSTNAME2 neq 53
deny 17 any host HOSTNAME3 lt 137 log
deny 17 any host HOSTNAME4 gt 138
deny ICMP any 10.161.0.0 0.0.255.255 log
permit TCP any host HOSTNAME5 neq 80
```

Configurar

En esta sección encontrará la información para configurar las funciones descritas en este

documento.

Nota: Use el Command Lookup Tool (únicamente clientes registrados) para obtener más información sobre los comandos que se utilizan en esta sección.

Diagrama de la red

En este documento, se utiliza esta configuración de red:

Nota: Los esquemas de direccionamiento IP usados en esta configuración no son legalmente enrutables en Internet. Son las direcciones RFC1918 que fueron utilizadas en un entorno de laboratorio.

Configurar VPN de acceso remoto (IPSec)

Procedimiento ASDM

Complete estos pasos para configurar la VPN de acceso remoto:

1. Elija Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPSec > IKE Policies> Add para crear una política ISAKMP.
2. Proporcione los detalles de la política ISAKMP como se muestra.

   Haga clic en Aceptar y Aplicar.
3. Elija Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPSec > IKE Parameters para habilitar IKE en la interfaz externa.
4. Elija Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPSec > IPSec Transform Sets > Add para crear el conjunto de transformación ESP-3DES-SHA, como se muestra.

   Haga clic en Aceptar y Aplicar.
5. Elija Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPSec > Crypto Maps > Add para crear un mapa criptográfico con política dinámica de prioridad 1, como se muestra.

   Haga clic en Aceptar y Aplicar.
6. Elija Configuration > Remote Access VPN > Network (Client) Access > Address Assignment > Address Pools y haga clic en Add para agregar VPN Client para los usuarios de VPN Client.
7. Elija Configuration > Remote Access VPN > AAA Setup > AAA Server Groups y haga clic en Add para agregar el nombre y el protocolo AAA Server Group .

   Agregue la dirección IP (ACS) del servidor AAA y la interfaz a la que se conecta. Agregue también la clave Server Secret en el área RADIUS Parameters. Click OK.

8. Elija Configuration > Remote Access VPN > Network (Client) Access > IPSec Connection Profiles > Add para agregar un grupo de túnel, por ejemplo, TunnelGroup1 y la clave previamente compartida como cisco123, como se muestra.

    - En la ficha Basic , elija el grupo de servidores como vpn para el campo User Authentication .
    - Elija vpnclient como los Pools de Direcciones de Cliente para los usuarios de VPN Client.

    Click OK.

9. Active la interfaz externa para el acceso IPSec. Haga clic en Apply para continuar.

Configurar ASA/PIX con la CLI

Complete estos pasos para configurar el servidor DHCP para proporcionar direcciones IP a los clientes VPN desde la línea de comandos. Consulte Configuración de VPN de Acceso Remoto o Referencias de Comandos de Cisco ASA 5500 Series Adaptive Security Appliance para obtener más información sobre cada uno de los comandos.

Configuración en ejecución en el disposi
<#root> ASA# sh run ASA Version 8.0(2) ! *!--- Specify the hostname for the Security Appliance.* hostname ASA enable password 8Ry2YjIyt7RRXU24 encrypted names !   *!--- Configure the outside and inside interfaces.* interface Ethernet0/0 nameif inside security-level 100 ip address 10.1.1.1 255.255.255.0 ! interface Ethernet0/1 nameif DMZ security-level 100 ip address 172.16.1.2 255.255.255.0 ! interface Ethernet0/2 nameif outside security-level 0 ip address 192.168.1.1 255.255.255.0 *!--- Output is suppressed.*

```
passwd 2KFQnbNIdI.2KYOU encrypted
boot system disk0:/asa802-k8.bin
ftp mode passive

access-list 101 extended permit ip 10.1.1.0 255.255.255.0
   192.168.5.0 255.255.255.0

!--- Radius Attribute Filter


access-list new extended deny ip any host 10.1.1.2
access-list new extended permit ip any any

pager lines 24
logging enable
logging asdm informational
mtu inside 1500
mtu outside 1500
mtu dmz 1500


ip local pool vpnclient1 192.168.5.1-192.168.5.10 mask 255.255.255.0


no failover
icmp unreachable rate-limit 1 burst-size 1


!--- Specify the location of the ASDM image for ASA to fetch the image for ASDM access.

asdm image disk0:/asdm-613.bin
no asdm history enable
arp timeout 14400

global (outside) 1 192.168.1.5
nat (inside) 0 access-list 101
nat (inside) 1 0.0.0.0 0.0.0.0
route outside 0.0.0.0 0.0.0.0 192.168.1.2 1
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
dynamic-access-policy-record DfltAccessPolicy

!--- Create the AAA server group "vpn" and specify the protocol as RADIUS. !--- Specify the CSACS serv


aaa-server vpn protocol radius
 max-failed-attempts 5
aaa-server vpn (DMZ) host 172.16.1.1
 retry-interval 1
 timeout 30
 key cisco123

http server enable
http 0.0.0.0 0.0.0.0 inside
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
```

```
!--- PHASE 2 CONFIGURATION ---! !--- The encryption types for Phase 2 are defined here. !--- A Triple

crypto ipsec transform-set ESP-3DES-SHA esp-3des esp-sha-hmac

!--- Defines a dynamic crypto map with !--- the specified encryption settings.

crypto dynamic-map outside_dyn_map 1 set transform-set ESP-3DES-SHA

!--- Binds the dynamic map to the IPsec/ISAKMP process.

crypto map outside_map 1 ipsec-isakmp dynamic outside_dyn_map

!--- Specifies the interface to be used with !--- the settings defined in this configuration.

crypto map outside_map interface outside

!--- PHASE 1 CONFIGURATION ---! !--- This configuration uses ISAKMP policy 2. !--- The configuration c

crypto isakmp enable outside

crypto isakmp policy 2
 authentication pre-share
 encryption 3des
 hash sha
 group 2
 lifetime 86400


no crypto isakmp nat-traversal

telnet timeout 5
ssh timeout 5
console timeout 0
threat-detection basic-threat
threat-detection statistics access-list
!
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
!
group-policy DfltGrpPolicy attributes
 vpn-tunnel-protocol IPSec webvpn
group-policy GroupPolicy1 internal

!--- Associate the vpnclient pool to the tunnel group using the address pool. !--- Associate the AAA s


tunnel-group TunnelGroup1 type remote-access

tunnel-group TunnelGroup1 general-attributes
 address-pool vpnclient
 authentication-server-group vpn



!--- Enter the pre-shared-key to configure the authentication method.

tunnel-group TunnelGroup1 ipsec-attributes
 pre-shared-key *

prompt hostname context
Cryptochecksum:e0725ca9ccc28af488ded9ee36b7822d
: end
ASA#
```

Configuración de Cisco VPN Client

Intente conectarse a Cisco ASA con Cisco VPN Client para verificar que ASA se haya configurado correctamente.

1. Elija Inicio > Programas > Cisco Systems VPN Client > VPN Client.
2. Haga clic en New para iniciar la ventana Create New VPN Connection Entry.
3. Complete la información de su nueva conexión.

   Introduzca el nombre de la entrada de conexión junto con una descripción. Ingrese la dirección IP externa del ASA en el cuadro Host. A continuación, introduzca el nombre del grupo de túnel VPN (TunnelGroup1) y la contraseña (Pre-shared Key - cisco123), tal y como se configuran en ASA. Click Save.

4. Haga clic en la conexión que desea utilizar y haga clic en Connect en la ventana principal de VPN Client.

5. Cuando se le solicite, ingrese el Nombre de usuario : cisco y la Contraseña : contraseña1 según lo configurado en el ASA para xauth, y haga clic en Aceptar para conectarse a la red remota.

6. El cliente VPN está conectado con el ASA en el sitio central.

7. Una vez establecida correctamente la conexión, elija Statistics en el menú Status (Estado) para verificar los detalles del túnel.

Configuración de ACS para ACL descargable para usuarios individuales

Puede configurar listas de acceso descargables en Cisco Secure ACS como un componente de perfil compartido y luego asignar la lista de acceso a un grupo o a un usuario individual.

Para implementar listas de acceso dinámicas, debe configurar el servidor RADIUS para que sea compatible. Cuando el usuario se autentica, el servidor RADIUS envía una lista de acceso descargable o un nombre de lista de acceso al dispositivo de seguridad. La lista de acceso permite o deniega el acceso a un servicio determinado. El dispositivo de seguridad elimina la lista de acceso cuando caduca la sesión de autenticación.

En este ejemplo, el usuario de VPN IPSec "cisco" se autentica correctamente y el servidor RADIUS envía una lista de acceso descargable al dispositivo de seguridad. El usuario "cisco" puede acceder solamente al servidor 10.1.1.2 y niega todos los demás accesos. Para verificar la ACL, vea la sección ACL descargable para usuario/grupo.

Complete estos pasos para configurar RADIUS en un Cisco Secure ACS.

1. Elija Network Configuration a la izquierda, y haga clic en Add Entry para agregar una entrada para ASA en la base de datos del servidor RADIUS.

2. Ingrese 172.16.1.2 en el campo de dirección IP del cliente e ingrese "cisco123" para el campo de clave secreta compartida. Elija RADIUS (Cisco VPN 3000/ASA/PIX 7.x+) en el cuadro desplegable Autenticar mediante. Haga clic en Submit (Enviar). .

3. Introduzca el nombre de usuario en el campo Usuario de la base de datos de Cisco Secure y haga clic en Agregar/Editar.

   En este ejemplo, el nombre de usuario es cisco.

4. En la siguiente ventana, ingrese la contraseña para "cisco". En este ejemplo, la contraseña también es password1. Cuando termine, haga clic en Enviar.

5. Utilice la página Opciones Avanzadas para determinar qué opciones avanzadas muestra ACS. Puede simplificar las páginas que aparecen en otras áreas de la interfaz web ACS si oculta las opciones avanzadas que no utiliza. Haga clic en Interface Configuration y, a continuación, haga clic en Advanced Options para abrir la página Advanced Options.

Marque la casilla para ACL descargables a nivel de usuario y ACL descargables a nivel de grupo.

ACL descargables a nivel de usuario: cuando se elige, esta opción habilita la sección ACL descargables (listas de control de acceso) en la página User Setup (Configuración de usuario).

ACL descargables a nivel de grupo: cuando se elige, esta opción habilita la sección ACL descargables en la página Group Setup .

6. En la barra de navegación, haga clic en Shared Profile Components, y haga clic en Downloadable IP ACLs.

   Nota: Si Downloadable IP ACLs no aparece en la página Shared Profile Components (Componentes del Perfil Compartido), debe activar las ACL Downloadable a Nivel de Usuario, la opción Group-Level Downloadable ACLs o ambas en la página Advanced Options (Opciones Avanzadas) de la sección Interface Configuration (Configuración de la Interfaz).

7. Haga clic en Add (Agregar). Aparecerá la página IP ACL descargables.

8. En el cuadro Nombre, escriba el nombre de la nueva ACL IP.

   Nota: El nombre de una ACL IP puede contener hasta 27 caracteres. El nombre no debe contener espacios ni ninguno de estos caracteres: guión (-), corchete de apertura ([), corchete de cierre (]), barra inclinada (/), barra inversa (\), comillas ("), corchete angular de cierre (<), corchete angular de cierre (>) o guión (-).

   En el cuadro Description (Descripción), escriba una descripción de la nueva ACL IP. La descripción puede tener hasta 1.000 caracteres.

   Para agregar un contenido ACL a la nueva ACL IP, haga clic en Add.

9. En el cuadro Nombre, escriba el nombre del nuevo contenido ACL.

   Nota: El nombre de un contenido ACL puede contener hasta 27 caracteres. El nombre no debe contener espacios ni ninguno de estos caracteres: guión (-), corchete de apertura ([), corchete de cierre (]), barra inclinada (/), barra inversa (\), comillas ("), corchete angular de cierre (<), corchete angular de cierre (>) o guión (-).

   En el cuadro Definiciones de ACL, escriba la nueva definición de ACL.

   Nota: Cuando ingresa las definiciones de ACL en la interfaz web ACS, no utilice palabras clave o entradas de nombre; en lugar de ello, comience con una palabra clave permit o deny.

   Para guardar el contenido ACL, haga clic en Submit.

10. Aparecerá la página ACL de IP descargables con el nuevo contenido de ACL enumerado por nombre en la columna Contenido de ACL. Para asociar un NAF al contenido ACL, elija

un NAF del cuadro Filtrado de acceso a la red a la derecha del nuevo contenido ACL. De forma predeterminada, NAF es (All-AAA-Clients). Si no asigna un NAF, ACS asocia el contenido ACL a todos los dispositivos de red, que es el valor predeterminado.

Para establecer el orden del contenido de ACL, haga clic en el botón de opción para una definición de ACL y luego haga clic en Arriba o Abajo para reposicionarla en la lista.

Para guardar la ACL IP, haga clic en Submit.

Nota: El orden de los contenidos de ACL es significativo. De arriba a abajo, ACS descarga solamente la primera definición de ACL que tiene una configuración de NAF aplicable, que incluye la configuración predeterminada All-AAA-Clients, si se utiliza. Normalmente, la lista de contenido de ACL pasa de la que tiene el NAF más específico (más estrecho) a la que tiene el NAF más general (Todos los clientes AAA).

Nota: ACS ingresa a la nueva ACL IP, que entra en vigencia inmediatamente. Por ejemplo, si la ACL IP se utiliza con los Firewalls PIX, está disponible para enviarse a cualquier Firewall PIX que intente la autenticación de un usuario que tenga esa ACL IP descargable asignada a su perfil de usuario o grupo.

11. Vaya a la página Configuración de usuario y edite la página Usuario. En la sección ACL descargables, haga clic en la casilla de verificación Asignar ACL IP:. Elija una ACL IP de la lista. Si ha finalizado la configuración de las opciones de cuenta de usuario, haga clic en Enviar para registrar las opciones.

Configuración de ACS para ACL descargable para el grupo

Complete los pasos del 1 al 9 de Configure ACS for Downloadable ACL for Individual User y siga estos pasos para configurar la ACL Descargable para el Grupo en un Cisco Secure ACS.

En este ejemplo, el usuario VPN IPSec "cisco" pertenece a los grupos VPN. Las políticas del grupo VPN se aplican a todos los usuarios del grupo.

El usuario del grupo VPN"cisco" se autentica correctamente y el servidor RADIUS envía una lista de acceso descargable al dispositivo de seguridad. El usuario "cisco" puede acceder solamente al servidor 10.1.1.2 y niega todos los demás accesos. Para verificar la ACL, consulte la sección ACL descargable para usuario/grupo.

1. En la barra de navegación, haga clic en Group Setup. Se abre la página Selección de configuración de grupo.
2. Cambie el nombre del Grupo 1 a VPN y haga clic en Enviar.
3. En la lista Grupo, elija un grupo y, a continuación, haga clic en Editar configuración.
4. En la sección ACL descargables, haga clic en la casilla de verificación Asignar ACL IP. Elija una ACL IP de la lista.
5. Para guardar la configuración del grupo que acaba de hacer, haga clic en Submit.

6. Vaya a User Setup (Configuración de usuario) y edite el usuario que desea agregar al grupo: VPN. Cuando termine, haga clic en Enviar.

   Ahora la ACL descargable configurada para el grupo VPN se aplica para este usuario.

7. Para seguir especificando otras configuraciones de grupo, realice otros procedimientos en este capítulo, según corresponda

Configuración de RADIUS IETF para un Grupo de Usuarios

Para descargar un nombre para una lista de acceso que ya ha creado en el dispositivo de seguridad desde el servidor RADIUS cuando un usuario autentica, configure el atributo de ID de filtro RADIUS IETF (atributo número 11) de la siguiente manera:

<#root>

```
filter-id=acl_name
```

El usuario del grupo VPN"cisco" se autentica correctamente y el servidor RADIUS descarga un nombre ACL (nuevo) para una lista de acceso que ya ha creado en el dispositivo de seguridad . El usuario "cisco" puede acceder a todos los dispositivos que se encuentran dentro de la red del ASA excepto el servidor 10.1.1.2. Para verificar la ACL, vea la sección Filtrar ID ACL.

Según el ejemplo, la ACL denominada new se configura para el filtrado en ASA.

<#root>

```
access-list new extended deny ip any host 10.1.1.2
access-list new extended permit ip any any
```

Estos parámetros aparecen sólo cuando son verdaderos. Usted ha configurado

- Cliente AAA para utilizar uno de los protocolos RADIUS en la configuración de red
- Atributos RADIUS de nivel de grupo en la página RADIUS (IETF) de la sección Interface Configuration (Configuración de la interfaz Web)

Los atributos RADIUS se envían como un perfil para cada usuario de ACS al cliente AAA solicitante.

Para configurar los valores del atributo IETF RADIUS para aplicarlos como una autorización para cada usuario del grupo actual, realice estas acciones:

1. En la barra de navegación, haga clic en Group Setup.

   Se abre la página Selección de configuración de grupo.

2. En la lista Grupo, elija un grupo y, a continuación, haga clic en Editar configuración.

   El nombre del grupo aparece en la parte superior de la página Configuración de grupo.

3. Desplácese hasta Atributos RADIUS de ITF. Para cada atributo RADIUS de IETF, debe autorizar el grupo actual. Marque la casilla de verificación del atributo [011] Filter-Id y, a continuación, agregue el nombre de ACL definido por ASA (new) en la autorización para el atributo en el campo. Consulte el resultado de ASA show running configuration.

4. Para guardar la configuración del grupo que acaba de hacer y aplicarla inmediatamente, haga clic en Enviar y Aplicar.

   Nota: Para guardar la configuración del grupo y aplicarla más tarde, haga clic en Enviar. Cuando esté listo para implementar los cambios, elija System Configuration > Service Control. A continuación, seleccione Reiniciar.

Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

La herramienta Output Interpreter Tool (clientes registrados solamente) (OIT) soporta ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

Mostrar comandos criptográficos

- show crypto isakmp sa—Muestra todas las asociaciones de seguridad (SA) IKE actuales en un par.

```
<#root>

ciscoasa#

sh crypto isakmp sa


   Active SA: 1
    Rekey SA: 0 (A tunnel will report 1 Active
   and 1 Rekey SA during rekey)
Total IKE SA: 1

1   IKE Peer: 192.168.10.2
    Type    : user            Role    : responder
    Rekey   : no              State   : AM_ACTIVE
ciscoasa#
```

- show crypto ipsec sa: muestra la configuración utilizada por las SA actuales.

```
<#root>
```

```
ciscoasa#
```

sh crypto ipsec sa

```
interface: outside
    Crypto map tag: outside_dyn_map, seq num: 1,
   local addr: 192.168.1.1

      local ident (addr/mask/prot/port):
   (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port):
   (192.168.5.1/255.255.255.255/0/0)
      current_peer: 192.168.10.2, username: cisco
      dynamic allocated peer ip: 192.168.5.1

      #pkts encaps: 65, #pkts encrypt:
   65, #pkts digest: 65
      #pkts decaps: 65, #pkts decrypt:
   65, #pkts verify: 65
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 4, #pkts comp failed:
   0, #pkts decomp failed: 0
      #pre-frag successes: 0, #pre-frag failures:
   0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0,
   #decapsulated frgs needing reassembly: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 192.168.1.1,
   remote crypto endpt.: 192.168.10.2

      path mtu 1500, ipsec overhead 58,
   media mtu 1500
      current outbound spi: EEF0EC32

    inbound esp sas:
      spi: 0xA6F92298 (2801345176)
         transform: esp-3des esp-sha-hmac none
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 86016, crypto-map:
   outside_dyn_map
         sa timing: remaining key lifetime (sec):
   28647
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0xEEF0EC32 (4008766514)
         transform: esp-3des esp-sha-hmac none
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 86016, crypto-map:
   outside_dyn_map
         sa timing: remaining key lifetime (sec): 28647
         IV size: 8 bytes
         replay detection support: Y
```

ACL descargable para usuario/grupo

Verifique la ACL descargable para el usuario Cisco. Las ACL se descargan de CSACS.

<#root>

```
ciscoasa(config)#
```

sh access-list

```
access-list cached ACL log flows: total 0,
   denied 0 (deny-flow-max 4096)
            alert-interval 300
access-list 101; 1 elements
access-list 101 line 1 extended permit ip 10.1.1.0 255.255.255.0
   192.168.5.0 255.255.255.0 (hitcnt=0) 0x8719a411
```

access-list #ACSACL#-IP-VPN_Access-49bf68ad; 2 elements (dynamic)
access-list #ACSACL#-IP-VPN_Access-49bf68ad line 1 extended permit
ip any host 10.1.1.2 (hitcnt=2) 0x334915fe
access-list #ACSACL#-IP-VPN_Access-49bf68ad line 2 extended deny
ip any any (hitcnt=40) 0x7c718bd1

ACL con ID de filtro

El ID de filtro [011] se ha aplicado para el grupo - VPN, y los usuarios del grupo se filtran según la ACL (nueva) definida en el ASA.

<#root>

```
ciscoasa# sh access-list
access-list cached ACL log flows: total 0,
   denied 0 (deny-flow-max 4096)
            alert-interval 300
access-list 101; 1 elements
access-list 101 line 1 extended permit ip 10.1.1.0
   255.255.255.0 192.168.5.0 255.255.255.0
   (hitcnt=0) 0x8719a411
access-list new; 2 elements
```

access-list new line 1 extended deny ip
any host 10.1.1.2 (hitcnt=4) 0xb247fec8
access-list new line 2 extended permit ip any any
(hitcnt=39) 0x40e5d57c

Troubleshoot

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración. También se muestra un ejemplo de salida del debug .

Nota: Para obtener más información sobre la resolución de problemas de VPN IPSec de acceso remoto, consulte Soluciones de resolución de problemas de VPN IPSec de acceso remoto y L2L más comunes.

Despeje las asociaciones de seguridad

Cuando resuelva problemas, asegúrese de borrar las asociaciones de seguridad existentes después de realizar un cambio. En el modo privilegiado de PIX, utilice estos comandos:

- clear [crypto] ipsec sa: elimina las SA IPSec activas. La palabra clave crypto es opcional.
- clear [crypto] isakmp sa: elimina las IKE SA activas. La palabra clave crypto es opcional.

Comandos para resolución de problemas

La herramienta Output Interpreter Tool (clientes registrados solamente) (OIT) soporta ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

Nota: Consulte Información Importante sobre Comandos Debug antes de utilizar los comandos debug.

- debug crypto ipsec 7 — Muestra negociaciones IPsec de la Fase 2.
- debug crypto isakmp 7 — Muestra negociaciones ISAKMP de la Fase 1.

Información Relacionada

- Página de Soporte de Cisco ASA 5500 Series Adaptive Security Appliances
- Referencias de Comandos de Cisco ASA 5500 Series Adaptive Security Appliances
- Página de Soporte de Cisco PIX 500 Series Security Appliances
- Cisco Adaptive Security Device Manager
- Página de Soporte de IPSec Negotiation/IKE Protocols
- Página de soporte para cliente Cisco VPN
- Cisco Secure Access Control Server para Windows
- Solicitudes de Comentarios (RFC)
- Soporte Técnico y Documentación - Cisco Systems

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).