ASA 8.3 y posterior: Autorización de RADIUS (ACS 5.x) para el acceso VPN usando ACL descargable con el CLI y el ejemplo de la Configuración de ASDM

Contenido

Introducción

Este documento describe cómo configurar el dispositivo de seguridad para autenticar a los usuarios para el acceso a la red. Puesto que usted puede habilitar implícito las autorizaciones de RADIUS, este documento no contiene ninguna información sobre la configuración de la autorización de 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.

Usted puede configurar a un servidor de RADIUS para descargar una lista de acceso al dispositivo de seguridad o un nombre de la lista de acceso a la hora de la autenticación. Autorizan al usuario a hacer solamente qué se permite en la lista de acceso específica del usuario.

Las Listas de acceso transferibles son los medios más scalable cuando usted utiliza el Cisco Secure Access Control Server (ACS) para proporcionar las Listas de acceso apropiadas para cada usuario. Para más información sobre las funciones de lista de acceso transferibles y el Cisco Secure ACS, refiera a configurar a un servidor de RADIUS para enviar las listas de control de acceso transferibles y IP transferible ACL.

Refiera ASA/PIX a 8.x: Autorización de RADIUS (ACS) para el acceso a la red usando ACL descargable con el CLI y el ejemplo de la Configuración de ASDM para la configuración idéntica en Cisco ASA con las versiones 8.2 y anterior.

prerrequisitos

Requisitos

Este documento asume que el dispositivo de seguridad adaptante (ASA) está completamente - operativo y configurado para permitir que el Cisco Adaptive Security Device Manager (ASDM) o el CLI realice los cambios de configuración.

Note: Refiera a permitir el acceso HTTPS para el ASDM para permitir que el dispositivo sea configurado remotamente por el ASDM o el Secure Shell (SSH).

Componentes Utilizados

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

- Versión de software 8.3 de Cisco ASA y posterior
- Cisco ASDM versión 6.3 y posterior
- Cliente VPN de Cisco versión 5.x y posterior
- Cisco Secure ACS 5.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.

Convenciones

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

Antecedentes

Usted puede utilizar IP transferible ACL para crear los conjuntos de las definiciones ACL que usted puede aplicar a muchos usuarios o grupos de usuarios. Estos conjuntos de las definiciones ACL se llaman contenido ACL.

El IP transferible ACL actúa esta manera:

1. Cuando el ACS concede un acceso del usuario a la red, el ACS determina si un IP transferible ACL está asignado al perfil de la autorización en la sección del resultado.
2. Si el ACS localiza un IP transferible ACL que se asigne al perfil de la autorización, el ACS envía un atributo (como parte de la sesión del usuario, en el paquete access-accept RADIUS) que especifica ACL mencionado, y la versión del ACL mencionado.
3. Si responde el cliente AAA que no tiene la versión actual del ACL en su caché (es decir, el ACL es nuevo o ha cambiado), el ACS envía el ACL (nuevo o actualizado) al dispositivo.

El IP transferible ACL es una alternativa a la configuración de los ACL en el atributo [26/9/1] del Cisco-av-pair RADIUS Cisco de cada usuario o grupo de usuarios. Usted puede crear un IP transferible ACL una vez, le da un nombre, y después asigna el IP transferible ACL a cualquier perfil de la autorización si usted se refiere a su nombre. Este método es más eficiente que si usted configura el atributo del Cisco-av-pair RADIUS Cisco para el perfil de la autorización.

Cuando usted ingresa las definiciones ACL en la interfaz Web ACS, no utilice la palabra clave o las entradas de nombre; por lo demás, utilice el sintaxis del comando acl y la semántica estándar para el cliente AAA en quien usted se prepone aplicar el IP transferible ACL. Las definiciones ACL que usted ingresa en el ACS comprenden uno o más comandos acl. Cada comando acl debe estar en una línea aparte.

En el ACS, usted puede definir IP transferible múltiple ACL y utilizarlos en diversos perfiles de la autorización. De acuerdo con las condiciones en las reglas de la autorización del servicio del acceso, usted puede enviar diversos perfiles de la autorización que contienen IP transferible ACL a diversos clientes AAA.

Además, usted puede cambiar la orden del contenido ACL en un IP transferible ACL. El ACS examina el contenido ACL, a partir del top de la tabla, y descarga el primer contenido ACL que encuentra. Cuando usted fija la orden, usted puede asegurar la eficiencia del sistema si usted coloca lo más extensamente posible el contenido aplicable ACL más arriba en la lista.

Para utilizar un IP transferible ACL en un cliente AAA determinado, el cliente AAA debe adherirse a estas reglas:

- Utilice RADIUS para la autenticación
- Soporte IP transferible ACL

Éstos son ejemplos de los dispositivos de Cisco que soportan IP transferible ACL:

- ASA
- Dispositivos de Cisco que funcionan con la versión de IOS 12.3(8)T y posterior

Éste es un ejemplo del formato que usted debe utilizar para ingresar ASA ACL en el rectángulo de las definiciones 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.

Diagrama de la red

En este documento, se utiliza esta configuración de red:

Note: 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.

VPN de acceso remoto de la configuración (IPSec)

Procedimiento del ASDM

Complete estos pasos para configurar el VPN de acceso remoto:

1. Seleccione los **Asisitente** > a los **Asistentes VPN** > **IPsec(IKEv1) Asisitente del VPN de acceso remoto de la** ventana casera.
2. Seleccione la **interfaz del túnel VPN** como sea necesario (**afuera**, en este ejemplo), y también aseegurese que el checkbox al lado de las **sesiones del permiso IPSec entrante para desviar las Listas de acceso de la interfaz** está marcado.
3. Elija el tipo del cliente VPN como **Cliente Cisco VPN, la versión 3.x o más arriba**. Haga clic en Next (Siguiente).
4. Elija el **método de autentificación** y proporcione la información de autenticación. El método de autentificación usado aquí es **clave previamente compartida**. También, proporcione un nombre de **grupo de túnel** en el espacio proporcionado. **La clave previamente compartida** usada aquí es **cisco123** y el **nombre de grupo de túnel** usado aquí es Cisco-**túnel**. Haga clic en Next (Siguiente).
5. Elija si desea que los usuarios remotos sean autenticados en las bases de datos de usuarios locales o en un grupo de servidores AAA externo. Aquí, elegimos **autenticamos usando un Grupo de servidores AAA**. Haga clic **nuevo** al lado del campo de nombre del Grupo de servidores AAA para crear un nuevo nombre de Grupo de servidores AAA.
6. Proporcione el nombre del nombre de grupo de servidores, del protocolo de autenticación, del dirección IP del servidor, de la interfaz, y la clave del Secreto de servidor en los espacios respectivos proporcionados, y la **AUTORIZACIÓN del** tecleo.
7. Haga clic en Next (Siguiente).
8. Defina un pool de las direcciones locales que se asignarán dinámicamente a los clientes de VPN remotos cuando se conectan. Haga clic **nuevo** para crear un nuevo pool de la dirección local.
9. En la ventana de la agrupación IP del agregar, proporcione el nombre del pool, comenzando la dirección IP, terminando la dirección IP, y a la máscara de subred. Click OK.

10. Seleccione el nombre del pool de la lista desplegable, y haga clic **después**. El nombre del pool por este ejemplo es Muestra-**pool** que fue creado en el paso 9.
11. *Opcional:* Especifique la información de servidor DNS y WINS y un Nombre de Dominio Predeterminado que se avanzará a los clientes de VPN remotos.
12. Especifique qué host internos (de haber alguno) o redes deben exponerse a los usuarios de VPN remotos. Haga clic **después** después de proporcionar al nombre de la interfaz y las redes que se eximirán en las redes exentas colocan.Si deja esta lista vacía, permita que los usuarios de VPN remotos acceden a la red interna completa del ASA.Puede también habilitar la tunelización dividida en esta ventana. La tunelización dividida encripta el tráfico a los recursos definidos anteriormente en este procedimiento y proporciona el acceso no cifrado a Internet en general al no tunelizar ese tráfico. Si la tunelización dividida no se habilita, todo el tráfico de los usuarios de VPN remotos se tuneliza al ASA. Éste puede convertirse en un gran ancho de banda y hacer un uso intensivo del procesador, sobre la base de su configuración.
13. Esta ventana muestra un resumen de las acciones que ha realizado. Haga clic en **Finalizar** si está satisfecho con la configuración.

Configure el ASA con el CLI

Ésta es la configuración CLI:

Configuración corriente en el dispositivo ASA

```
ASA# sh run
ASA Version 8.4(3)
!
!--- Specify the hostname for the Security Appliance.
hostname ciscoasa enable password y.tvDXf6yFbMTAdD
encrypted passwd 2KFQnbNIdI.2KYOU encrypted names ! !---
Configure the outside and inside interfaces. interface
Ethernet0/0 nameif dmz security-level 50 ip address
192.168.26.13 255.255.255.0 ! interface Ethernet0/1
nameif inside security-level 100 ip address 10.1.1.1
255.255.255.0 ! interface Ethernet0/2 nameif outside
security-level 0 ip address 172.16.1.1 255.255.255.0 !
!--- Output is suppressed. boot system disk0:/asa843-
k8.bin ftp mode passive object network
NETWORK_OBJ_10.1.1.0_24 subnet 10.1.1.0 255.255.255.0
object network NETWORK_OBJ_10.2.2.0_24 subnet 10.2.2.0
255.255.255.0 access-list OUTIN extended permit icmp any
any !--- This is the Access-List whose name will be sent
by !--- RADIUS Server(ACS) in the Filter-ID attribute.
access-list new extended permit ip any host 10.1.1.2
access-list new extended deny ip any any
pager lines 24
logging enable
logging asdm informational
mtu inside 1500
mtu outside 1500
mtu dmz 1500

ip local pool Sample-Pool 10.2.2.1-10.2.2.254 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-647.bin no asdm history enable arp timeout
14400 !--- Specify the NAT from internal network to the
Sample-Pool. nat (inside,outside) source static
NETWORK_OBJ_10.1.1.0_24 NETWORK_OBJ_10.1.1.0_24
destination static NETWORK_OBJ_10.2.2.0_24
NETWORK_OBJ_10.2.2.0_24 no-proxy-arp route-lookup
access-group OUTIN in interface outside !--- Create the
AAA server group "ACS5" and specify the protocol as
RADIUS. !--- Specify the ACS 5.x server as a member of
the "ACS5" group and provide the !--- location and key.
aaa-server ACS5 protocol radius
aaa-server ACS5 (dmz) host 192.168.26.51
timeout 5
key *****

aaa authentication http console LOCAL
http server enable 2003
http 0.0.0.0 0.0.0.0 inside


!--- PHASE 2 CONFIGURATION ---! !--- The encryption &
hashing types for Phase 2 are defined here. We are using
!--- all the permutations of the PHASE 2 parameters.
crypto ipsec ikev1 transform-set ESP-AES-256-MD5 esp-
aes-256 esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-DES-SHA esp-des
esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-3DES-SHA esp-3des
esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-DES-MD5 esp-des
esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-AES-192-MD5 esp-
aes-192 esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-3DES-MD5 esp-3des
esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-AES-256-SHA esp-
aes-256 esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-AES-128-SHA esp-aes
esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-AES-192-SHA esp-
aes-192 esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-AES-128-MD5 esp-aes
esp-md5-hmac


!--- Defines a dynamic crypto map with !--- the
specified transform-sets created earlier. We are
specifying all the !--- transform-sets. crypto dynamic-
map SYSTEM_DEFAULT_CRYPTO_MAP 65535 set ikev1 transform-
set
   ESP-AES-128-SHA ESP-AES-128-MD5
ESP-AES-192-SHA ESP-AES-192-MD5 ESP-AES-256-SHA ESP-AES-
256-MD5 ESP-3DES-SHA
   ESP-3DES-MD5 ESP-DES-SHA ESP-DES-MD5

!--- Binds the dynamic map to the IPsec/ISAKMP process.
crypto map outside_map 65535 ipsec-isakmp dynamic
SYSTEM_DEFAULT_CRYPTO_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 policies defined with all the permutation !-
-- of the 5 ISAKMP parameters. The configuration
commands here define the !--- Phase 1 policy parameters
that are used. crypto ikev1 enable outside

crypto ikev1 policy 10
authentication crack
encryption aes-256
hash sha
group 2
lifetime 86400

crypto ikev1 policy 20
authentication rsa-sig
encryption aes-256
hash sha
group 2
lifetime 86400

crypto ikev1 policy 30
authentication pre-share
encryption aes-256
hash sha
group 2
lifetime 86400

crypto ikev1 policy 40
authentication crack
encryption aes-192
hash sha
group 2
lifetime 86400

crypto ikev1 policy 50
authentication rsa-sig
encryption aes-192
hash sha
group 2
lifetime 86400

crypto ikev1 policy 60
authentication pre-share
encryption aes-192
hash sha
group 2
lifetime 86400

crypto ikev1 policy 70
authentication crack
encryption aes
hash sha
group 2
lifetime 86400

crypto ikev1 policy 80
authentication rsa-sig
encryption aes
hash sha
group 2
lifetime 86400
```

```
crypto ikev1 policy 90
authentication pre-share
encryption aes
hash sha
group 2
lifetime 86400

crypto ikev1 policy 100
authentication crack
encryption 3des
hash sha
group 2
lifetime 86400

crypto ikev1 policy 110
authentication rsa-sig
encryption 3des
hash sha
group 2
lifetime 86400

crypto ikev1 policy 120
authentication pre-share
encryption 3des
hash sha
group 2
lifetime 86400

crypto ikev1 policy 130
authentication crack
encryption des
hash sha
group 2
lifetime 86400

crypto ikev1 policy 140
authentication rsa-sig
encryption des
hash sha
group 2
lifetime 86400

crypto ikev1 policy 150
authentication pre-share
encryption des
hash sha
group 2
lifetime 86400


webvpn
group-policy Cisco-Tunnel internal
group-policy Cisco-Tunnel attributes
vpn-tunnel-protocol ikev1
default-domain value cisco.com
username admin password CdOTKv3uhDhHIw3A encrypted
privilege 15
!--- Associate the vpnclient pool to the tunnel group
using the address pool. !--- Associate the AAA server
group (ACS5) with the tunnel group. tunnel-group Cisco-
Tunnel type remote-access tunnel-group Cisco-Tunnel
general-attributes
address-pool Sample-Pool
```

```
authentication-server-group ACS5
default-group-policy Cisco-Tunnel

!--- Enter the pre-shared-key to configure the
authentication method. tunnel-group Cisco-Tunnel ipsec-
attributes
ikev1 pre-shared-key *****

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

Configuración ACS para ACL descargable para el usuario individual

Usted puede configurar las Listas de acceso transferibles en el Cisco Secure ACS 5.x pues Permissions Nombrados Object y después lo asigna a un perfil de la autorización que sea elegido en la sección del resultado de la regla en el Acceso-servicio.

En este ejemplo, el usuario **Cisco del** IPSec VPN autentica con éxito, y el servidor de RADIUS envía una lista de acceso transferible al dispositivo de seguridad. El usuario “Cisco” puede acceder solamente el servidor de 10.1.1.2 y niega el resto del acceso. Para verificar el ACL, vea ACL descargable para el usuario/la sección de grupo.

Complete estos pasos para configurar al cliente RADIUS en un Cisco Secure ACS 5.x:

1. Elija los **recursos de red** > los **dispositivos de red y a los clientes AAA**, y el tecleo **crea** para agregar una entrada para el ASA en la base de datos del servidor RADIUS.
2. Ingrese el nombre significativo a localmente - para el ASA (muestra-**ASA**, en este ejemplo), después ingrese **192.168.26.13** en el campo del IP Address. Elija el **RADIO** en la sección de las opciones de autenticación marcando el checkbox del **RADIO** y ingrese el **cisco123** para el campo secreto compartido. Haga clic en Submit (Enviar).
3. El ASA se agrega con éxito a la base de datos del servidor de RADIUS (ACS).
4. Elija a los **usuarios y la identidad salva** > los **almacenes internos de la identidad** > Users, y el tecleo **crea** para crear a un usuario en la base de datos local del ACS para la autenticación VPN.
5. Ingrese el nombre de usuario cisco. Seleccione el tipo de contraseña como **usuarios internos**, y ingrese la contraseña (**cisco123**, en este ejemplo). Confirme la contraseña, y el tecleo **somete**.
6. Crean al usuario **Cisco** con éxito.
7. Para crear ACL descargable, elegir los **elementos de la directiva** > la **autorización y los permisos** > **nombró a Permission Objects** > los **ACL transferibles**, y el tecleo **crea**.
8. Proporcione el **nombre** para ACL descargable, así como el **contenido ACL**. Haga clic en Submit (Enviar).
9. ACL descargable la **muestra-DACL** se crea con éxito.
10. Para configurar las políticas de acceso para la autenticación VPN, elija las **políticas de acceso** > el **acceso mantiene** > las **reglas de selección del servicio**, y determina qué servicio está abasteciendo al protocolo RADIUS. En este ejemplo, la **regla 1** hace juego el **RADIUS**, y el acceso de red predeterminada abastecerá al pedido de RADIUS.
11. Elija el **servicio del acceso** determinado del paso 10. En este ejemplo, se utiliza el **acceso de red predeterminada**. Elija la lengueta **permitida de los protocolos**, y aseegurese que **permita PAP/ASCII** y **permita MS-CHAPv2** estén seleccionados. Haga clic en Submit

(Enviar).
12. Haga clic en la **sección de la identidad de los servicios del acceso**, y aseegurese que seleccionan a los **usuarios internos** como la fuente de la identidad. En este ejemplo, hemos tomado el acceso de red predeterminada.
13. Elija las **políticas de acceso** > el **acceso mantiene** > **acceso** > **autorización de red predeterminada**, y el tecleo **personaliza**.
14. **Sistema del** movimiento**: Nombre de usuario de la** columna **disponible a la** columna **seleccionada**, y **AUTORIZACIÓN del** tecleo.
15. El tecleo **crea** para crear una nueva regla.
16. Aseegurese que el checkbox al lado del **sistema: El nombre de usuario** se selecciona, elige los **iguales de la** lista desplegable, y ingresa el nombre de usuario cisco.
17. Tecleo **selecto**.
18. El tecleo **crea** para crear un nuevo perfil de la autorización.
19. Proporcione un nombre para el **perfil de la autorización**. **El ejemplo de perfil** se utiliza en este ejemplo.
20. Elija la lengueta **común de las tareas**, y seleccione los **parásitos atmosféricos de la** lista desplegable para **ACL descargable el nombre**. Elija el **DACL** creado recientemente **(la muestra - DACL) de la** lista desplegable de valores.
21. Haga clic en Submit (Enviar).
22. Aseegurese que el checkbox al lado del **ejemplo de perfil** (el perfil creado recientemente de la autorización) está marcado, y haga clic la **AUTORIZACIÓN**.
23. Una vez que usted ha verificado que el **ejemplo de perfil** creado recientemente está seleccionado en la **autorización perfila el** campo, hace clic la **AUTORIZACIÓN**.
24. Verifique que la nueva regla (**Rule-2**) esté creada con el sistema: El nombre de usuario **iguala las** condiciones y el **ejemplo de perfil de Cisco** como el resultado. **Cambios de la salvaguardia del** tecleo. La regla 2 se crea con éxito.

Configuración ACS para ACL descargable para el grupo

Los pasos completos 1 a 12 de la configuración ACS para ACL descargable para el usuario individual y realizan estos pasos para configurar ACL descargable para el grupo en un Cisco Secure ACS.

En este ejemplo, el usuario “Cisco” del IPSec VPN pertenece al Muestra-**grupo**.

El usuario **Cisco del Muestra-grupo** autentica con éxito, y el servidor de RADIUS envía una lista de acceso transferible al dispositivo de seguridad. El usuario “Cisco” puede acceder solamente el servidor de 10.1.1.2 y niega el resto del acceso. Para verificar el ACL, refiera a ACL descargable para el usuario/la sección de grupo.

1. En la barra de navegación, haga clic a los **usuarios y la identidad salva** > los **grupos de la identidad**, y el tecleo **crea** para crear a un nuevo grupo.
2. Proporcione un nombre del grupo (Muestra-**grupo**), y el tecleo **somete**.
3. Elija los **almacenes de la Identificación del usuario** > los **almacenes internos de la identidad** > Users, y seleccione al usuario **Cisco**. El tecleo **edita** para cambiar la membresía del grupo de este usuario.
4. Tecleo **selecto** al lado del grupo de la identidad.
5. Seleccione al grupo creado recientemente (es decir, Muestra-**grupo**), y haga clic la **AUTORIZACIÓN**.

6. Haga clic en Submit (Enviar).
7. Elija las **políticas de acceso** > el **acceso mantiene** > **acceso** > **autorización de red predeterminada**, y el tecleo **crea** para crear una nueva regla.
8. Aseegurese que el checkbox al lado del **grupo de la identidad** está marcado, y haga clic **selecto**.
9. Elija al Muestra-**grupo**, y haga clic la **AUTORIZACIÓN**.
10. Haga clic **selecto**, en la sección de los perfiles de la autorización.
11. El tecleo **crea** para crear un nuevo perfil de la autorización.
12. Proporcione un nombre para el **perfil de la autorización**. **El ejemplo de perfil** es el nombre usado en este ejemplo.
13. Elija la lengueta **común de las tareas**, y seleccione los **parásitos atmosféricos de la** lista desplegable para **ACL descargable el nombre**. Elija el **DACL** creado recientemente **(la muestra - DACL) de la** lista desplegable de valores.
14. Haga clic en Submit (Enviar).
15. Elija el **ejemplo de perfil del** perfil de la autorización creado anterior, y haga clic la **AUTORIZACIÓN**.
16. Click OK.
17. Verifique que **Rule-1** esté creado con el Muestra-**grupo del** grupo de la identidad como la condición y el **ejemplo de perfil** como el resultado. Haga clic los **cambios de la salvaguardia**.

Configure el ACS para ACL descargable para un grupo de dispositivos de red

Complete los pasos 1 a 12 de la configuración ACS para ACL descargable para el usuario individual y realice estos pasos para configurar ACL descargable para un grupo de dispositivos de red en un Cisco Secure ACS.

En este ejemplo, el cliente RADIUS (ASA) pertenece al grupo de dispositivos de red que el pedido de autenticación VPN-Gateways.The VPN que viene del ASA para el usuario “Cisco” autentica con éxito, y el servidor de RADIUS envía una lista de acceso transferible al dispositivo de seguridad. El usuario “Cisco” puede acceder solamente el servidor de 10.1.1.2 y niega el resto del acceso. Para verificar el ACL, refiera a ACL descargable para el usuario/la sección de grupo.

1. Elija los **recursos de red** > los **grupos de dispositivos de red** > el **tipo de dispositivo**, y el tecleo **crea** para crear a un nuevo grupo de dispositivos de red.
2. Proporcione un nombre de **grupo de dispositivos de red** (**gatewayes de VPN** en este ejemplo), y el tecleo **somete**.
3. Elija los **recursos de red** > los **dispositivos de red y a los clientes AAA**, y seleccione al **cliente RADIUS muestra-ASA** creado anterior. El tecleo **edita** para cambiar la calidad de miembro de **grupo de dispositivos de red de** este cliente RADIUS (asa).
4. Tecleo **selecto** al lado del tipo de dispositivo.
5. Seleccione el grupo de dispositivos de red creado recientemente (que es **gatewayes de VPN**), y haga clic la **AUTORIZACIÓN**.
6. Haga clic en Submit (Enviar).
7. Elija las **políticas de acceso** > el **acceso mantiene** > **acceso** > **autorización de red predeterminada**, y el tecleo **personaliza**.
8. Movimiento **NDG: Tipo de dispositivo de la** sección **disponible a la sección seleccionada**, y **AUTORIZACIÓN del** tecleo.

9. El tecleo **crea** para crear una nueva regla.
10. Aseegurese que el checkbox al lado de **NDG:** Seleccionan y elige al **tipo de dispositivo adentro de la** lista desplegable. Tecleo **selecto**.
11. Elija los **gatewayes de VPN del** grupo de dispositivos de red creados anterior, y haga clic la **AUTORIZACIÓN**.
12. Haga clic **selecto**.
13. El tecleo **crea** para crear un nuevo perfil de la autorización.
14. Proporcione un nombre para el **perfil de la autorización**. **El ejemplo de perfil** es el nombre usado en este ejemplo.
15. Elija la lengueta **común de las tareas**, y seleccione los **parásitos atmosféricos de la** lista desplegable para ACL descargable el nombre. Elija el **DACL** creado recientemente **(muestra-DACL) de la** lista desplegable de valores.
16. Haga clic en Submit (Enviar).
17. Seleccione el **ejemplo de perfil** creado anterior, y haga clic la **AUTORIZACIÓN**.
18. Click OK.
19. Verifique que **Rule-1** esté creado con los **gatewayes de VPN** como NDG: Tipo de dispositivo como condición, y **ejemplo de perfil** como resultado. **Cambios de la salvaguardia del** tecleo.

Configuraciones del IETF RADIUS de la configuración para un grupo de usuarios

Para descargar un nombre para una lista de acceso que usted ha creado ya en el dispositivo de seguridad del servidor de RADIUS cuando un usuario autentica, configure el atributo filtro-identificación del IETF RADIUS (número de atributo 11):

```
filter-id=acl_name
```

El usercisco del Muestra-grupo autentica con éxito, y el servidor de RADIUS descarga un nombre ACL (nuevo) para una lista de acceso que usted ha creado ya en el dispositivo de seguridad. El usuario “Cisco” puede acceder todos los dispositivos que estén dentro de la red del ASA **excepto el** servidor de 10.1.1.2. Para verificar el ACL, vea la sección ACL del id del filtro.

Según el ejemplo, el **nuevo** nombrada ACL se configura para filtrar en el ASA:

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

Estos parámetros aparecen solamente cuando éstos son verdades. Usted ha configurado:

- Cliente AAA para utilizar uno de los protocolos RADIUS en configuración de red
- Un perfil de la autorización con el id del filtro RADIUS (IETF) se selecciona bajo sección del resultado de la regla en el Acceso-servicio.

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

Los pasos completos 1 a 6 y 10 a 12 de la configuración ACS para ACL descargable para el

usuario individual, seguido por los pasos 1 a 6 de la configuración ACS para ACL descargable para el grupo, y realizan estos pasos en esta sección para configurar el id del filtro en el Cisco Secure ACS.

Para configurar las configuraciones del **atributo IETF RADIUS** para aplicarse como en el perfil de la autorización, realice estos pasos:

1. Elija los **elementos de la directiva** > la **autorización y los permisos** > los **perfiles del acceso a la red** > de la **autorización**, y el tecleo **crea** para crear un nuevo perfil de la autorización.
2. Proporcione un nombre para el **perfil de la autorización**. **El id del filtro** es el nombre del perfil de la autorización elegido en este ejemplo con el fin de simplificar.
3. Haga clic la lengueta **común de las tareas**, y elija los **parásitos atmosféricos de la** lista desplegable para el **id del filtro ACL**. Ingrese el nombre de la lista de acceso como **nuevo** en el campo de valor, y el tecleo **somete**.
4. Elija las **políticas de acceso** > el **acceso mantiene** > **acceso** > **autorización de red predeterminada**, y el tecleo **crea** para crear una nueva regla.
5. Aseegurese que el checkbox al lado del **grupo de la identidad** está marcado, y haga clic **selecto**.
6. Elija al Muestra-**grupo**, y haga clic la **AUTORIZACIÓN**.
7. Haga clic **selecto** en la sección de los perfiles de la autorización.
8. Elija el **id del filtro del** perfil de la autorización creado anterior, y haga clic la **AUTORIZACIÓN**.
9. Click OK.
10. Verifique que **Rule-1** esté creado con el Muestra-**grupo del** grupo de la identidad como condición y el **id del filtro** como resultado. Haga clic los **cambios de la salvaguardia**.

Configuración de Cliente Cisco VPN

Conecte con Cisco ASA con el Cliente Cisco VPN para verificar que el ASA está configurado con éxito.

Complete estos pasos:

1. Elija el **Start (Inicio) > Programs (Programas) > Cisco Systems VPN Client (VPN Client de Cisco Systems)** > al **cliente VPN**.
2. Haga clic **nuevo** para iniciar la nueva ventana de entrada de la conexión VPN del crear.
3. Complete los detalles de su nueva conexión:Ingrese el nombre del Entrada de conexión junto con una descripción.Ingrese el **IP Address externo del ASA** en el rectángulo del host.Ingrese el nombre de grupo de túnel VPN (Cisco-**túnel**) y la contraseña (clave previamente compartida - **cisco123**) como está configurado en el ASA.Click **Save**.
4. Haga clic la conexión que usted quiere utilizar, y el tecleo **conecta de la** ventana principal del cliente VPN.
5. Cuando se le pregunte, ingrese el **cisco123 del** nombre de usuario cisco y de la contraseña como está configurado en el ASA para la autenticación, y haga clic la **AUTORIZACIÓN** para conectar con la red remota.
6. Una vez que la conexión se establece con éxito, elija las **estadísticas del** menú Status (Estado) para verificar los detalles del túnel.

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.

Comandos show crypto

- show crypto isakmp sa: muestra todas las asociaciones actuales de seguridad IKE (SA) de un par.

```
ciscoasa# sh crypto isakmp sa

IKEv1 SAs:

   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: 172.16.1.50
    Type    : user            Role    : responder
    Rekey   : no              State   : AM_ACTIVE
ciscoasa#
```

- **muestre IPSec crypto sa** - Muestra las configuraciones usadas por los SA actuales.

```
ciscoasa# sh crypto ipsec sa
interface: outside
    Crypto map tag: SYSTEM_DEFAULT_CRYPTO_MAP, seq num: 65535, local addr:
       172.16.1.1

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.2.2.1/255.255.255.255/0/0)
      current_peer: 172.16.1.50, username: cisco
      dynamic allocated peer ip: 10.2.2.1

      #pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 0
      #pkts decaps: 333, #pkts decrypt: 333, #pkts verify: 333
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #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.: 172.16.1.1/0, remote crypto endpt.: 172.16.1.50/0
      path mtu 1500, ipsec overhead 74, media mtu 1500
      current outbound spi: 9A06E834
      current inbound spi : FA372121

    inbound esp sas:
      spi: 0xFA372121 (4197916961)
         transform: esp-aes esp-sha-hmac no compression
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 16384, crypto-map: SYSTEM_DEFAULT_CRYPTO_MAP
         sa timing: remaining key lifetime (sec): 28678
         IV size: 16 bytes
         replay detection support: Y
         Anti replay bitmap:
          0xFFFFFFFF 0xFFFFFFFF
    outbound esp sas:
```

```
          spi: 0x9A06E834 (2584143924)
             transform: esp-aes esp-sha-hmac no compression
             in use settings ={RA, Tunnel, }
             slot: 0, conn_id: 16384, crypto-map: SYSTEM_DEFAULT_CRYPTO_MAP
             sa timing: remaining key lifetime (sec): 28678
             IV size: 16 bytes
             replay detection support: Y
             Anti replay bitmap:
              0x00000000 0x00000001
```

ACL descargable para el usuario/el grupo

Verifique ACL descargable para el usuario Cisco. Los ACL se descargan del CSACS.

```
ciscoasa# sh access-list
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
            alert-interval 300
access-list OUTIN; 1 elements; name hash: 0x683c318c
access-list OUTIN line 1 extended permit icmp any any (hitcnt=1) 0x2ba5809c
access-list #ACSACL#-IP-Sample-DACL-4f3b9117; 2 elements; name hash: 0x3c878038
   (dynamic)
access-list #ACSACL#-IP-Sample-DACL-4f3b9117 line 1 extended permit ip any host
   10.1.1.2 (hitcnt=0) 0x5e896ac3
access-list #ACSACL#-IP-Sample-DACL-4f3b9117 line 2 extended deny ip any any
   (hitcnt=130) 0x19b3b8f5
```

Id del filtro ACL

El id del filtro [011] ha solicitado el grupo - filtran al Muestra-grupo, y a los usuarios del grupo según el ACL (nuevo) definido en el ASA.

```
ciscoasa# sh access-list
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
            alert-interval 300
access-list OUTIN; 1 elements; name hash: 0x683c318c
access-list OUTIN line 1 extended permit icmp any any (hitcnt=1) 0x2ba5809c
access-list new; 2 elements; name hash: 0xa39433d3
access-list new line 1 extended permit ip any host 10.1.1.2 (hitcnt=4)
   0x58a3ea12
access-list new line 2 extended deny ip any any (hitcnt=27) 0x61f918cd
```

Troubleshooting

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

Note: Para más información sobre el IPSec VPN del Acceso Remoto del troubleshooting, refiera a la mayoría del IPSec VPN común L2L y del Acceso Remoto que resuelve problemas las soluciones.

Borre las asociaciones de seguridad

Cuando usted resuelve problemas, aseegurese borrar los SA existentes después de que usted

realice un cambio. En el modo privilegiado del PIX, utilice estos comandos:

- **clear [crypto] ipsec sa** - Borra el IPSec activo SA. La palabra clave crypto es opcional.
- **clear [crypto] isakmp sa** - Borra el IKE activo SA. 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.

Note: Consulte Información Importante sobre Comandos de Debug antes de usar un **comando debug**.

- **IPSec 7 del debug crypto** - Visualiza los IPSec Negotiations de la fase 2.
- **isakmp 7 del debug crypto** - Visualiza negociaciones ISAKMP de la fase 1.

Información Relacionada

- Página de Soporte de Cisco ASA 5500 Series Adaptive Security Appliances
- Referencias de comandos del Dispositivos de seguridad adaptable Cisco ASA de la serie 5500
- Cisco Adaptive Security Device Manager
- Página de Soporte de IPSec Negotiation/IKE Protocols
- Página de soporte para cliente Cisco VPN
- Cisco Secure Access Control System
- Solicitudes de Comentarios (RFC)
- Soporte Técnico y Documentación - Cisco Systems