Cerrojo y Llave: Listas de acceso dinámico

Contenido

Introducción

El acceso Lock-and-key (Llave y cerrojo) le permite configurar listas de acceso dinámicas que garantizan el acceso para cada usuario a un host de destino/origen específico mediante un proceso de autenticación de usuario. El acceso del usuario se permite con un Firewall del ® del Cisco IOS dinámicamente, sin ningún compromiso en las restricciones de seguridad.

prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

La información que se presenta en este documento se originó a partir de dispositivos dentro de un ambiente de laboratorio específico. En este caso, el ambiente de laboratorio consistió en un 2620 Router que funcionaba con el Software Release 12.3(1) de Cisco IOS®. 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 Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

Consideraciones de simulación

El acceso lock-and-key permite que un evento externo ponga una apertura en el Firewall Cisco IOS. Luego de que exista esta apertura, el router es susceptible a la vigilancia de dirección de origen. Para prevenir esto, proporcione el soporte de encripción usando el cifrado IP con la autenticación o el cifrado.

La simulación es un problema con todas las listas de acceso existentes. El acceso lock-and-key no trata este problema.

Debido a que el acceso lock-and-key introduce un camino potencial a través del firewall de la red, deberá analizar el acceso dinámico. Otro host, spoofing su dirección autenticada, accede detrás del Firewall. Con el acceso dinámico, hay la posibilidad que un host no autorizado, spoofing su dirección autenticada, accede detrás del Firewall. El acceso lock-and-key no causa el problema de la simulación de dirección. El problema sólo se identifica aquí como una preocupación del usuario.

Rendimiento

El funcionamiento se afecta en estas dos situaciones.

- Cada lista de acceso dinámica fuerza una reconstrucción de lista de acceso en el Motor de conmutación de silicio (SSE). Esto hace que el trayecto de conmutación SSE funcione más lento momentáneamente.
- Las listas de acceso dinámicas requieren el recurso del tiempo de inactividad (incluso si el descanso se deja para omitir). Por lo tanto, las listas de acceso dinámicas no pueden ser SSE conmutaron. Estas entradas se manejan en el trayecto de Switching rápido del protocolo.

Mire las configuraciones del Router del borde. Los usuarios remotos crean las entradas de lista de acceso en el Router del borde. La lista de acceso crece y se encoge dinámicamente. Las entradas se eliminan dinámicamente de la lista luego de que caducan los períodos idle-timeout o max-timeout. Listas de acceso grandes degradan el rendimiento de conmutación del paquete.

Cuando utilizar el acceso Lock-and-Key

Dos ejemplos de cuando usted utiliza el acceso lock-and-key se enumeran aquí:

- Cuando usted quisiera que un host remoto pudiera acceder un host en su red interna a través de Internet. El acceso lock-and-key limita el acceso más allá de su Firewall sobre una base del host individual o de la red.
- Cuando desea que un subgrupo de hosts en una red acceda a un host en una red remota protegido por un firewall. Por medio del acceso con cerrojo y llave, puede habilitar sólo un conjunto deseado de hosts para que tengan acceso. Para hacerlo, deberá autenticarlos a

través de un servidor TACACS+ o RADIUS.

Operación de acceso con cerrojo y llave

Este proceso describe la operación de acceso con cerrojo y llave.

1. Un usuario abre una sesión Telnet en un router de borde configurado para acceso con cerrojo y llave.
2. El Cisco IOS Software recibe el paquete Telnet. Realiza un proceso de autenticación de usuario. El usuario debe aprobar la autenticación antes de que se le permita el acceso. El proceso de autenticación es hecho por el router o un Access Server central tal como un TACACS+ o un servidor de RADIUS.

Configuración de muestra y solución de problemas

Diagrama de la red

Cisco recomienda que usted utiliza un servidor TACACS+ para su proceso de la interrogación de la autenticación. TACACS+ proporciona servicios de autenticación, autorización y contabilidad. También proporciona el soporte a protocolo, la especificación del protocolo, y una base de datos de seguridad centralizada.

Usted puede autenticar al usuario en el router o con un TACACS+ o un servidor de RADIUS.

Nota: Estos comandos son globales salvo indicación contraria.

En el router, usted necesita un **nombre de usuario** para el usuario para la autenticación local.

```
username test password test
```

La presencia de **login local** en las líneas del vty hace este nombre de usuario ser utilizada.

```
line vty 0 4
login local
```

Si usted no confía en al usuario para publicar el **comando access-enable**, usted puede hacer una de dos cosas:

- Asocie el descanso al usuario sobre por usuario una base.
  ```
  username test autocommand access-enable host
  timeout 10
  ```
  o
- Fuerce a todos los usuarios ese Telnet adentro a tener el mismo descanso.
  ```
  line vty 0 4
  login local
  autocommand access-enable host timeout 10
  ```

Nota: Los 10 en el sintaxis es el *tiempo de inactividad de la* lista de acceso. Es reemplazada por el tiempo de espera absoluto en la lista de acceso dinámica.

Defina una lista de acceso ampliada que sea aplicada cuando se publica un usuario (cualquier usuario) registra en el router y el **comando access-enable**. La época absoluta máxima para este

“agujero” en el filtro se fija a 15 minutos. Después de 15 minutos, el agujero se cierra independientemente de si cualquier persona lo utiliza. El testlist del nombre necesita existir sino ser no significativo. Limite las redes a las cuales el usuario tiene acceso configurando a la dirección de origen o de destino (aquí, el usuario no es limitado).

```
access-list 120 dynamic testlist timeout 15 permit ip any any
```

Defina la lista de acceso necesaria para bloquear todo a menos que la capacidad a Telnet en el router (para abrir un agujero, el usuario necesita Telnet al router). La dirección IP aquí es el Ethernet IP Address del router.

```
access-list 120 permit tcp any host 171.68.117.189 eq telnet
```

Hay un implícito niega todos en el extremo (no ingresado aquí).

Aplique esta lista de acceso a la interfaz en la cual los usuarios vienen.

```
interface ethernet1
       ip access-group 120 in
```

Le hacen.

Esto es lo que parece el filtro en el router ahora:

```
Router#show access-lists
Extended IP access list 120
    10 Dynamic testlist permit ip any any log
    20 permit tcp any host 171.68.117.189 eq telnet (68 matches)
```

Los usuarios que consiguen el acceso a su red interna no pueden ver cualquier cosa hasta ellos Telnet al router.

Nota: Los 10 aquí es el *tiempo de inactividad de la* lista de acceso. Es reemplazada por el tiempo de espera absoluto en la lista de acceso dinámica.

```
%telnet 2514A
Trying 171.68.117.189 ...
Connected to 2514A.network.com.
Escape character is '^]'.

User Access Verification

Username: test
Password: test

Connection closed by foreign host.
```

El filtro parece esto.

```
Router#show access-lists
Extended IP access list 120
    10 Dynamic testlist permit ip any any log
       permit ip host 171.68.109.158 any log (time left 394)
    20 permit tcp any host 171.68.117.189 eq telnet (68 matches)
```

Hay un agujero en el filtro para este un usuario basado en la dirección IP de origen. Cuando algún otro hace esto, usted ve *dos agujeros*.

```
Router#show ip access-lists 120
Extended IP access list 120
```

```
    10 Dynamic testlist permit ip any any log
       permit ip host 171.68.109.64 any log
       permit ip host 171.68.109.158 any log
    20 permit tcp any host 171.68.117.189 eq telnet (288 matches)
```

Estos usuarios pueden tener IP Access completo a cualquier IP Address de destino de su *dirección IP de origen*.

Uso de TACACS+

Configuración TACACS+

Configure un servidor TACACS+ para forzar la autenticación y autorización para ser hecho en el servidor TACACS+ para utilizar el TACACS+, como esta salida muestra:

```
Router#show ip access-lists 120
Extended IP access list 120
    10 Dynamic testlist permit ip any any log
       permit ip host 171.68.109.64 any log
       permit ip host 171.68.109.158 any log
    20 permit tcp any host 171.68.117.189 eq telnet (288 matches)
```

Complete estos pasos para configurar el TACACS+ en el Cisco Secure ACS for Windows:

1. Abra a un buscador Web. Ingrese el direccionamiento de su servidor ACS, que está bajo la forma de ***<IP_address de* http:// *o DNS_name>:2002***. (Este ejemplo utiliza un puerto predeterminado de 2002.) Inicie sesión como admin.
2. Haga clic en la configuración de red. El tecleo **agrega la entrada** para crear a un grupo de dispositivos de red que contenga a los servidores de acceso a la red (NAS). Ingrese un nombre para el grupo y el tecleo **somete**.
3. El tecleo **agrega la entrada** para agregar a un cliente del Authentication, Authorization, and Accounting (AAA) (NAS).
4. Ingrese el nombre del host, el IP Address, y la clave usada para cifrar la comunicación entre el servidor de AAA y el NAS. Seleccione **TACACS+ (Cisco IOS)** como el método de autentificación. Cuando le acaban, el tecleo **somete +Restart** para aplicar los cambios.
5. Haga clic la **configuración de usuario**, ingrese una identificación del usuario, y el tecleo **agrega/edita**.
6. Elija una base de datos para autenticar al usuario. (En este ejemplo, el usuario es “prueba” y la base de datos interna del ACS se utiliza para la autenticación). Ingrese una contraseña para el usuario, y confirme la contraseña.
7. Elija al grupo a quien asignan el usuario y marque la **configuración de grupo del uso**. Haga clic en Submit (Enviar).
8. **Configuración de grupo del** tecleo. Seleccione al grupo a quien asignaron el usuario en el tecleo del paso 7. **edita las configuraciones**.
9. Navegue hacia abajo a las configuraciones TACACS+ la sección. Marque el cuadro para el **ejecutivo del shell**. Marque el cuadro para el **comando auto**. Ingrese el auto de ser realizado sobre la autorización exitosa del usuario. (Este ejemplo utiliza el **comando 10 del descanso del host del acceso-permiso**.) Haga clic **Submit+Restart**.

Resuelva problemas el TACACS+

Utilice estos **comandos debug** en el NAS de resolver problemas los problemas TACACS+.

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

- **autenticación de TACACS del debug** — Visualiza la información sobre autenticación de TACACS+ el proceso. Solamente disponible en algunas versiones de software. Si es inasequible, utilice los **tacacs del debug** solamente.
- **haga el debug de la autorización de los tacacs** — Visualiza la información sobre autorización TACACS+ el de proceso. Solamente disponible en algunas versiones de software. Si es inasequible, utilice los **tacacs del debug** solamente.
- **haga el debug de los eventos de los tacacs** — Visualiza la información del proceso del ayudante TACACS+. Solamente disponible en algunas versiones de software. Si es inasequible, utilice los **tacacs del debug** solamente.

Utilice estos comandos de resolver problemas los problemas AAA:

- debug aaa authentication — Muestra información sobre autenticación de AAA/TACACS+.
- **debug aaa authorization** — Visualiza la información sobre la autorización AAA/TACACS+.

El ejemplo de salida del debug aquí muestra una autenticación satisfactoria y un proceso de la autorización en el servidor ACS TACACS+.

```
Router#show debug
General OS:
  TACACS+ events debugging is on
  TACACS+ authentication debugging is on
  TACACS+ authorization debugging is on
  AAA Authentication debugging is on
  AAA Authorization debugging is on
======================================================
Router#
 AAA/BIND(00000009): Bind i/f
 AAA/AUTHEN/LOGIN (00000009): Pick method list 'default'
 TPLUS: Queuing AAA Authentication request 9 for processing
 TPLUS: processing authentication start request id 9
 TPLUS: Authentication start packet created for 9()
 TPLUS: Using server 10.48.66.53
 TPLUS(00000009)/0/NB_WAIT/82A2E088: Started 5 sec timeout
 TPLUS(00000009)/0/NB_WAIT: socket event 2
 TPLUS(00000009)/0/NB_WAIT: wrote entire 36 bytes request
 TPLUS(00000009)/0/READ: socket event 1
 TPLUS(00000009)/0/READ: Would block while reading
 TPLUS(00000009)/0/READ: socket event 1
 TPLUS(00000009)/0/READ: read entire 12 header bytes
   (expect 16 bytes data)
 TPLUS(00000009)/0/READ: socket event 1
 TPLUS(00000009)/0/READ: read entire 28 bytes response
 TPLUS(00000009)/0/82A2E088: Processing the reply packet
 TPLUS: Received authen response status GET_USER (7)
 TPLUS: Queuing AAA Authentication request 9 for processing
 TPLUS: processing authentication continue request id 9
 TPLUS: Authentication continue packet generated for 9
 TPLUS(00000009)/0/WRITE/8347F3FC: Started 5 sec timeout
 TPLUS(00000009)/0/WRITE: wrote entire 22 bytes request
 TPLUS(00000009)/0/READ: socket event 1
 TPLUS(00000009)/0/READ: read entire 12 header bytes
   (expect 16 bytes data)
 TPLUS(00000009)/0/READ: socket event 1
 TPLUS(00000009)/0/READ: read entire 28 bytes response
 TPLUS(00000009)/0/8347F3FC: Processing the reply packet
 TPLUS: Received authen response status GET_PASSWORD (8)
```

```
 TPLUS: Queuing AAA Authentication request 9 for processing
 TPLUS: processing authentication continue request id 9
 TPLUS: Authentication continue packet generated for 9
 TPLUS(00000009)/0/WRITE/8347EE4C: Started 5 sec timeout
 TPLUS(00000009)/0/WRITE: wrote entire 25 bytes request
 TPLUS(00000009)/0/READ: socket event 1
 TPLUS(00000009)/0/READ: read entire 12 header bytes
   (expect 6 bytes data)
 TPLUS(00000009)/0/READ: socket event 1
 TPLUS(00000009)/0/READ: read entire 18 bytes response
 TPLUS(00000009)/0/8347EE4C: Processing the reply packet
 TPLUS: Received authen response status PASS (2)
 AAA/AUTHOR (0x9): Pick method list 'default'
 TPLUS: Queuing AAA Authorization request 9 for processing
 TPLUS: processing authorization request id 9
 TPLUS: Protocol set to None .....Skipping
 TPLUS: Sending AV service=shell
 TPLUS: Sending AV cmd
 TPLUS: Authorization request created for 9(tne-1)
 TPLUS: using previously set server 10.48.66.53
   from group tacacs+
 TPLUS(00000009)/0/NB_WAIT/8347F508: Started 5 sec timeout
 TPLUS(00000009)/0/NB_WAIT: socket event 2
 TPLUS(00000009)/0/NB_WAIT: wrote entire 60 bytes request
 TPLUS(00000009)/0/READ: socket event 1
 TPLUS(00000009)/0/READ: Would block while reading
 TPLUS(00000009)/0/READ: socket event 1
 TPLUS(00000009)/0/READ: read entire 12 header bytes
   (expect 44 bytes data)
 TPLUS(00000009)/0/READ: socket event 1
 TPLUS(00000009)/0/READ: read entire 56 bytes response
 TPLUS(00000009)/0/8347F508: Processing the reply packet
 TPLUS: Processed AV autocmd=access-enable host timeout 10
 TPLUS: received authorization response for 9: PASS
 AAA/AUTHOR/EXEC(00000009): processing AV cmd=
 AAA/AUTHOR/EXEC(00000009): processing AV
   autocmd=access-enable host timeout 10
 AAA/AUTHOR/EXEC(00000009): Authorization successful
```

Uso de RADIUS

Configuración RADIUS

Para utilizar el RADIUS, configure a un servidor de RADIUS para forzar la autenticación para ser hecho en el servidor de RADIUS con los parámetros de autorización (el autocommand) que se enviarán abajo en el atributo específico del proveedor 26, como se muestra aquí:

```
Router#show debug
General OS:
  TACACS+ events debugging is on
  TACACS+ authentication debugging is on
  TACACS+ authorization debugging is on
  AAA Authentication debugging is on
  AAA Authorization debugging is on
======================================================
Router#
 AAA/BIND(00000009): Bind i/f
 AAA/AUTHEN/LOGIN (00000009): Pick method list 'default'
 TPLUS: Queuing AAA Authentication request 9 for processing
 TPLUS: processing authentication start request id 9
 TPLUS: Authentication start packet created for 9()
 TPLUS: Using server 10.48.66.53
```

```
TPLUS(00000009)/0/NB_WAIT/82A2E088: Started 5 sec timeout
TPLUS(00000009)/0/NB_WAIT: socket event 2
TPLUS(00000009)/0/NB_WAIT: wrote entire 36 bytes request
TPLUS(00000009)/0/READ: socket event 1
TPLUS(00000009)/0/READ: Would block while reading
TPLUS(00000009)/0/READ: socket event 1
TPLUS(00000009)/0/READ: read entire 12 header bytes
  (expect 16 bytes data)
TPLUS(00000009)/0/READ: socket event 1
TPLUS(00000009)/0/READ: read entire 28 bytes response
TPLUS(00000009)/0/82A2E088: Processing the reply packet
TPLUS: Received authen response status GET_USER (7)
TPLUS: Queuing AAA Authentication request 9 for processing
TPLUS: processing authentication continue request id 9
TPLUS: Authentication continue packet generated for 9
TPLUS(00000009)/0/WRITE/8347F3FC: Started 5 sec timeout
TPLUS(00000009)/0/WRITE: wrote entire 22 bytes request
TPLUS(00000009)/0/READ: socket event 1
TPLUS(00000009)/0/READ: read entire 12 header bytes
  (expect 16 bytes data)
TPLUS(00000009)/0/READ: socket event 1
TPLUS(00000009)/0/READ: read entire 28 bytes response
TPLUS(00000009)/0/8347F3FC: Processing the reply packet
TPLUS: Received authen response status GET_PASSWORD (8)
TPLUS: Queuing AAA Authentication request 9 for processing
TPLUS: processing authentication continue request id 9
TPLUS: Authentication continue packet generated for 9
TPLUS(00000009)/0/WRITE/8347EE4C: Started 5 sec timeout
TPLUS(00000009)/0/WRITE: wrote entire 25 bytes request
TPLUS(00000009)/0/READ: socket event 1
TPLUS(00000009)/0/READ: read entire 12 header bytes
  (expect 6 bytes data)
TPLUS(00000009)/0/READ: socket event 1
TPLUS(00000009)/0/READ: read entire 18 bytes response
TPLUS(00000009)/0/8347EE4C: Processing the reply packet
TPLUS: Received authen response status PASS (2)
AAA/AUTHOR (0x9): Pick method list 'default'
TPLUS: Queuing AAA Authorization request 9 for processing
TPLUS: processing authorization request id 9
TPLUS: Protocol set to None .....Skipping
TPLUS: Sending AV service=shell
TPLUS: Sending AV cmd
TPLUS: Authorization request created for 9(tne-1)
TPLUS: using previously set server 10.48.66.53
  from group tacacs+
TPLUS(00000009)/0/NB_WAIT/8347F508: Started 5 sec timeout
TPLUS(00000009)/0/NB_WAIT: socket event 2
TPLUS(00000009)/0/NB_WAIT: wrote entire 60 bytes request
TPLUS(00000009)/0/READ: socket event 1
TPLUS(00000009)/0/READ: Would block while reading
TPLUS(00000009)/0/READ: socket event 1
TPLUS(00000009)/0/READ: read entire 12 header bytes
  (expect 44 bytes data)
TPLUS(00000009)/0/READ: socket event 1
TPLUS(00000009)/0/READ: read entire 56 bytes response
TPLUS(00000009)/0/8347F508: Processing the reply packet
TPLUS: Processed AV autocmd=access-enable host timeout 10
TPLUS: received authorization response for 9: PASS
AAA/AUTHOR/EXEC(00000009): processing AV cmd=
AAA/AUTHOR/EXEC(00000009): processing AV
  autocmd=access-enable host timeout 10
AAA/AUTHOR/EXEC(00000009): Authorization successful
```

Complete estos pasos para configurar el RADIUS en el Cisco Secure ACS for Windows:

1. Abra a un buscador Web y ingrese el direccionamiento de su servidor ACS, que está bajo la forma de *<IP_address de* **http://** *o DNS_name>:2002*. (Este ejemplo utiliza un puerto predeterminado de 2002.) Inicie sesión como admin.
2. Haga clic en la configuración de red. El tecleo **agrega la entrada** para crear a un grupo de dispositivos de red que contenga el NAS. Ingrese un nombre para el grupo y el tecleo **somete**.
3. El tecleo **agrega la entrada** para agregar a un cliente AAA (NAS).
4. Ingrese el nombre del host, el IP Address, y la clave usada para cifrar la comunicación entre el servidor de AAA y el NAS. Seleccione **RADIUS (Cisco IOS/PIX)** como el método de autentificación. Cuando le acaban, el tecleo **somete +Restart** para aplicar los cambios.
5. Haga clic la **configuración de usuario**, ingrese una identificación del usuario, y el tecleo **agrega/edita**.
6. Elija una base de datos para autenticar al usuario. (En este ejemplo, el usuario es “prueba” y la base de datos interna del ACS se utiliza para la autenticación). Ingrese una contraseña para el usuario, y confirme la contraseña.
7. Elija al grupo a quien asignan el usuario y marque la **configuración de grupo del uso**. Haga clic en Submit (Enviar).
8. Haga clic la **configuración de grupo** y seleccione al grupo a quien asignaron el usuario en el paso anterior. El tecleo **edita las configuraciones**.
9. Navegue hacia abajo a los atributos de RADIUS de Cisco IOS/PIX la sección. Marque el cuadro para el **Cisco-av-pair**. Ingrese el **comando shell** de ser realizado sobre la autorización exitosa del usuario. (Este ejemplo utiliza el **shell:** tecleo **autocmd=access-enable Submit+Restart del descanso 10. del host**).

Troubleshooting RADIUS

Utilice estos **comandos debug** en el NAS de resolver problemas los problemas de RADIUS.

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

- debug radius - Muestra información asociada con RADIUS.

Utilice estos comandos de resolver problemas los problemas AAA:

- debug aaa authentication — Muestra información sobre autenticación de AAA/TACACS+.
- **debug aaa authorization** — Visualiza la información sobre la autorización AAA/TACACS+.

El ejemplo de salida del debug aquí muestra una autenticación satisfactoria y un proceso de la autorización en el ACS configurado para el RADIUS.

```
Router#show debug
General OS:
  AAA Authentication debugging is on
  AAA Authorization debugging is on

Radius protocol debugging is on
Radius packet protocol debugging is on
=====================================================
Router#
 AAA/BIND(00000003): Bind i/f
 AAA/AUTHEN/LOGIN (00000003): Pick method list 'default'
 RADIUS/ENCODE(00000003): ask "Username: "
```

```
RADIUS/ENCODE(00000003): send packet; GET_USER
RADIUS/ENCODE(00000003): ask "Password: "
RADIUS/ENCODE(00000003): send packet; GET_PASSWORD
RADIUS:  AAA Unsupported     [152] 5
RADIUS:   74 74 79                        [tty]
RADIUS(00000003): Storing nasport 66 in rad_db
RADIUS/ENCODE(00000003): dropping service type,
  "radius-server attribute 6 on-for-login-auth" is off
RADIUS(00000003): Config NAS IP: 0.0.0.0
RADIUS/ENCODE(00000003): acct_session_id: 1
RADIUS(00000003): sending
RADIUS/ENCODE: Best Local IP-Address 172.18.124.1
  for Radius-Server 10.48.66.53
RADIUS(00000003): Send Access-Request to 10.48.66.53:1645
  id 21645/1, len 77
RADIUS:  authenticator 5A 95 1F EA A7 94 99 E5 -
  BE B5 07 BD E9 05 5B 5D
RADIUS:  User-Name           [1]   7   "test"
RADIUS:  User-Password       [2]   18  *
RADIUS:  NAS-Port            [5]   6   66
RADIUS:  NAS-Port-Type       [61]  6   Virtual     [5]
RADIUS:  Calling-Station-Id  [31]  14  "171.68.109.158"
RADIUS:  NAS-IP-Address      [4]   6   171.68.117.189
RADIUS: Received from id 21645/1 10.48.66.53:1645,
  Access-Accept, len 93
RADIUS:  authenticator 7C 14 7D CB 33 19 97 19 -
  68 4B C3 FC 25 21 47 CD
RADIUS:  Vendor, Cisco       [26]  51
RADIUS:   Cisco AVpair       [1]   45
  "shell:autocmd=access-enable host timeout 10"
RADIUS:  Class               [25]  22
RADIUS:   43 49 53 43 4F 41 43 53 3A 61 63 31 32 37 63 30
  [CISCOACS:ac127c0]
RADIUS:   31 2F 36 36                  [1/66]
RADIUS(00000003): Received from id 21645/1
AAA/AUTHOR/EXEC(00000003): processing AV
  autocmd=access-enable host timeout 10
AAA/AUTHOR/EXEC(00000003): Authorization successful
```

Información Relacionada

- Seguridad del Cerrojo y Llave del Cisco IOS
- Página de soporte de TACACS/TACACS+
- TACACS+ en documentación de IOS
- Página de soporte de RADIUS
- Solicitudes de Comentarios (RFC)
- Soporte Técnico y Documentación - Cisco Systems