Postura de la Versión de ASA 9.2.1 VPN con el ejemplo de configuración ISE

Contenido

Introducción

Este documento describe cómo configurar la versión 9.2.1 adaptante del dispositivo de seguridad de Cisco (ASA) para posture a los usuarios de VPN contra el Cisco Identity Services Engine (ISE) sin la necesidad de un nodo en línea de la postura (IPN).

Prerrequisitos

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimiento básico de la configuración CLI ASA y de la configuración VPN del Secure Socket Layer (SSL)
- Conocimiento básico de la configuración del VPN de acceso remoto en el ASA

- Conocimiento básico del ISE y de los servicios de la postura

Componentes Utilizados

La información que contiene este documento se basa en estas versiones de software:

- Versiones de software 9.2.1 de Cisco ASA y posterior
- Versión 7 de Microsoft Windows con la versión 3.1 del Cliente de movilidad Cisco AnyConnect Secure
- Versión 1.2 de Cisco ISE con corrección 5 o más adelante

Antecedentes

El cambio de los soportes RADIUS de la Versión de ASA 9.2.1 de Cisco de la autorización (CoA) (RFC 5176). Esto permite posturing de los usuarios de VPN contra Cisco ISE sin la necesidad de un IPN. Después de que un usuario de VPN abra una sesión, el ASA reorienta el tráfico de la Web al ISE, donde está aprovisionado el usuario con un agente del Network Admission Control (NAC) o el agente de la red. El agente realiza los controles específicos en la máquina del usuario para determinar su conformidad contra un conjunto configurado de las reglas de la postura, tales como operating system (OS), correcciones, reglas del antivirus, del servicio, de la aplicación, o del registro.

Los resultados de la validación de la postura entonces se envían al ISE. Si la máquina es denuncia juzgada, después el ISE puede enviar un CoA RADIUS al ASA con el nuevo conjunto de las directivas de la autorización. Después de la validación acertada de la postura y del CoA, no prohiben el usuario el acceso a los recursos internos.

Configurar

Diagrama de la red y flujo de tráfico

Aquí está el flujo de tráfico, como se ilustra en el diagrama de la red:

1. El usuario remoto utiliza Cisco Anyconnect para el acceso VPN al ASA.

2. El ASA envía un pedido de acceso RADIUS para ese usuario al ISE.

3. Que la petición golpea la directiva nombró **ASA92-posture** en el ISE. Como consecuencia, se vuelve el perfil de la autorización **ASA92-posture**. El ISE envía un access-accept RADIUS con dos pares de valor de atributo de Cisco:

   url-redirect-acl=redirect - éste es el nombre de la lista de control de acceso (ACL) que se define localmente en el ASA, que decide al tráfico que debe ser reorientado.

   url-redirect=https://ise2.test-cisco.com:8443/guestportal/gateway?sessionId=xx&action=cpp -

éste es el URL al cual el usuario remoto debe ser reorientado.Consejo: Los servidores del Domain Name System (DNS) que se asignan a los clientes VPN deben poder resolver el nombre de dominio completo (FQDN) que se vuelve en la reorientación URL. Si los filtros VPN se configuran para restringir el acceso en el nivel de grupo de túnel, asegúrese de que el grupo de cliente pueda acceder el servidor ISE en el puerto configurado (**TCP 8443** en este ejemplo).

4. El ASA envía un paquete del comienzo de la Estadística-petición RADIUS y recibe una respuesta. Esto es necesario para enviar todos los detalles con respecto a la sesión al ISE. Estos detalles incluyen el session_id, el IP Address externo del cliente VPN, y la dirección IP del ASA. El ISE utiliza el session_id para identificar esa sesión. El ASA también envía la información de la cuenta interina periódica, donde está el Framed-IP-direccionamiento la mayoría del atributo importante con el IP que es asignado al cliente por el ASA (**10.10.10.10** en este ejemplo).

5. Cuando el tráfico del usuario de VPN hace juego el ACL local-definido (reoriente), se reorienta a **https://ise2.test-cisco.com:8443**. El dependiente sobre la configuración, el ISE provisions el agente del NAC o el agente de la red.

6. Después de que el agente esté instalado en la máquina del cliente, realiza automáticamente los controles específicos. En este ejemplo, busca para el archivo de **c:\test.txt**. También envía un informe de la postura al ISE, que puede incluir los intercambios múltiples con el uso del protocolo SWISS y vira TCP/UDP hacia el lado de babor 8905 para acceder el ISE.

7. Cuando el ISE recibe el informe de la postura del agente, procesa las reglas de la autorización de nuevo. Esta vez, el resultado de la postura se sabe y se golpea otra regla. Envía un paquete CoA RADIUS:

   Si el usuario es obediente, después el nombre a ACL descargable (DACL) que permite el acceso total se envía (la regla ASA92-compliant de AuthZ).

   Si el usuario es no obediente, después un nombre DACL que el acceso limitado los permisos se envía (la regla ASA92-noncompliant de AuthZ).Nota: El CoA RADIUS se confirma siempre; es decir, el ASA envía una respuesta al ISE para confirmar.
8. El ASA quita el cambio de dirección. Si no hace el DACLs ocultar, debe enviar un pedido de acceso para descargarlos del ISE. El DACL específico se asocia a la sesión de VPN.

9. La próxima vez que eso que el usuario de VPN intenta acceder la página web, puede acceder todos los recursos que sean permitidos por el DACL que está instalado en el ASA. Si el usuario no es obediente, sólo se concede el acceso limitado.
   Nota: Este modelo de flujo diferencia de la mayoría de los escenarios que utilicen el CoA RADIUS. Para las autenticaciones atadas con alambre/inalámbricas del 802.1x, el CoA RADIUS no incluye ninguna atributos. Acciona solamente la segunda autenticación en la cual todos los atributos, tales como DACL, se asocian. Para la postura ASA VPN, no hay segunda autenticación. Todo el los atributos se vuelven en el CoA RADIUS. La sesión de VPN es activa y no es posible cambiar la mayor parte de las configuraciones del usuario de VPN.

Configuraciones

Utilice esta sección para configurar el ASA y el ISE.

ASA

Aquí está la configuración básica ASA para el acceso de Cisco AnyConnect:

```
ip local pool POOL 10.10.10.10-10.10.10.100 mask 255.255.255.0

interface GigabitEthernet0/0
 nameif outside
 security-level 0
 ip address xxxx 255.255.255.0
!
interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 192.168.111.10 255.255.255.0

aaa-server ISE protocol radius
aaa-server ISE (inside) host 10.48.66.74
 key cisco

webvpn
 enable outside
 anyconnect-essentials
 anyconnect image disk0:/anyconnect-win-3.1.02040-k9.pkg 1
 anyconnect enable
 tunnel-group-list enable

group-policy GP-SSL internal
group-policy GP-SSL attributes
 vpn-tunnel-protocol ikev1 ikev2 ssl-client ssl-clientless

tunnel-group RA type remote-access
tunnel-group RA general-attributes
 address-pool POOL
 authentication-server-group ISE
 default-group-policy GP-SSL
tunnel-group RA webvpn-attributes
 group-alias RA enable
```

Para la integración ASA con la postura ISE, asegúrese de que usted:

- Configure el servidor del Authentication, Authorization, and Accounting (AAA) para la autorización dinámica para validar el CoA.
- Configure las estadísticas como un grupo de túnel para enviar a los detalles de la sesión de VPN hacia el ISE.
- Configure las estadísticas interinas que enviarán la dirección IP asignada al usuario y ponga al día periódicamente el estatus de la sesión en el ISE
- Configure la reorientación ACL, que decide a si se permiten el DNS y el tráfico ISE. El resto del tráfico HTTP se reorienta al ISE para la postura.

Aquí está el ejemplo de configuración:

```
access-list redirect extended deny udp any any eq domain
```

```
access-list redirect extended deny ip any host 10.48.66.74
access-list redirect extended deny icmp any any
access-list redirect extended permit tcp any any eq www

aaa-server ISE protocol radius
 authorize-only
 interim-accounting-update periodic 1
 dynamic-authorization
aaa-server ISE (inside) host 10.48.66.74
 key cisco

tunnel-group RA general-attributes
 address-pool POOL
 authentication-server-group ISE
 accounting-server-group ISE
default-group-policy GP-SSL
```

ISE

Complete estos pasos para configurar el ISE:

1. Navegue a la **administración > a los recursos de red > a los dispositivos de red** y agregue el ASA como dispositivo de red:

2. Navegue a la **directiva > a los resultados > a la autorización > ACL descargable** y configure el DACL de modo que permita el acceso total. La configuración del ACL predeterminado permite todo el tráfico IP en el ISE:

3. Configure un ACL similar que proporcione el acceso limitado (para los usuarios no obedientes).

4. Navegue a la **directiva > a los resultados > a la autorización > a los perfiles de la autorización** y configure el perfil de la autorización nombrado **ASA92-posture**, que reorienta a los usuarios para la postura. Marque la casilla de verificación del **cambio de dirección de la red**, seleccione el **aprovisionamiento del cliente de la** lista desplegable, y asegúrese que **reorienta** aparece en el campo ACL (que el ACL está definido localmente en el ASA):

5. Configure el perfil de la autorización nombrado **ASA92-compliant**, que debe volver solamente el **PERMIT_ALL_TRAFFIC** nombrado DACL que proporciona el acceso total para los usuarios obedientes:

6. Configure un perfil similar de la autorización nombrado **ASA92-noncompliant**, que debe volver el DACL con el acceso limitado (para los usuarios no obedientes).

7. Navegue a la **directiva > a la autorización** y configure las reglas de la autorización:

   Cree una regla que permita el acceso total si los resultados de la postura son obedientes. El resultado es la directiva **ASA92-compliant de la** autorización.

   Cree una regla que permita el acceso limitado si los resultados de la postura son no obedientes. El resultado es la directiva **ASA92-noncompliant de la** autorización.

   Asegure eso si ningunas de las dos reglas anteriores se golpean, entonces la regla predeterminada vuelve el **ASA92-posture**, que fuerza un cambio de dirección en el ASA.

8. Las reglas de la autenticación predeterminada marcan el Nombre de usuario en el almacén interno de la identidad. Si esto se debe cambiar (llegado el Active Directory (AD), por ejemplo), después navega a la **directiva > a la autenticación** y realiza el cambio:

9. Navegue a la **directiva > al aprovisionamiento del cliente** y configure las reglas del aprovisionamiento. Éstas son las reglas que deciden al tipo de agente que debe ser aprovisionado. En este ejemplo, solamente una regla sencilla existe, y el ISE selecciona el agente del NAC para todos los sistemas de Microsoft Windows:

   Cuando los agentes no están en el ISE, es posible descargarlos:

10. En caso necesario, usted puede navegar a la **administración > al sistema > a las configuraciones > al proxy** y configurar el proxy para el ISE (acceder Internet).

11. Configure las reglas de la postura, que verifican la configuración del cliente. Usted puede configurar las reglas que marcan:

    archivos - existencia, versión, fecha

    clave de registro, valor, existencia

    nombre del **proceso de la aplicación**, funcionamiento, no ejecutándose

    servicio - mantenga el nombre, funcionamiento, no ejecutándose

    antivirus - más de 100 vendedores soportados, versión, cuando las definiciones son actualizadas

    antispyware - más de 100 vendedores soportados, versión, cuando las definiciones son actualizadas

condición compuesta - mezcla de todos

el Diccionario personalizado condiciona - el uso la mayor parte de los diccionarios ISE

12. En este ejemplo, solamente se realiza un control simple de la existencia del archivo. Si el archivo de **c:\test.txt** está presente en la máquina del cliente, es acceso total obediente y permitido. Navegue a la **directiva > a las condiciones > a las condiciones del archivo** y configure la condición del archivo:

13. Navegue a la **directiva > a los resultados > a la postura > a los requisitos** y cree un requisito. Este requisito debe ser cumplido cuando se satisface la condición anterior. Si no es, después se ejecuta la acción de la corrección. Pudo haber muchos tipos de acciones de la corrección disponibles, pero en este ejemplo, se utiliza el más simple: se visualiza un mensaje específico.

    Nota: En las circunstancias normales, la acción de la corrección del archivo puede ser utilizada (el ISE proporciona el archivo transferible).
14. Navegue a la **directiva > a la postura** y utilice el requisito que usted creó en el paso anterior (**file_requirement** Nombrado) en las reglas de la postura. La única regla de la postura requiere que todos los sistemas de Microsoft Windows resuelvan el **file_requirement**. Si se cumple este requisito, después la estación es obediente; si no se resuelve, después la estación es no obediente.

Nueva valoración periódica

Por abandono, la postura es un evento de una sola vez. Sin embargo, hay a veces una necesidad de marcar la conformidad del usuario y de ajustar periódicamente el acceso a los recursos basados en los resultados. Esta información se avanza vía el protocolo SWISS (agente del NAC) o se codifica dentro de la aplicación (agente de la red).

Complete estos pasos para marcar la conformidad del usuario:

1. Navegue a la **administración > a las configuraciones > a la postura > a las nuevas valoraciones** y habilite la nueva valoración global (por la configuración de grupo de la identidad):

2. Cree una condición de la postura que haga juego todas las nuevas valoraciones:

3. Cree una condición similar que haga juego solamente las evaluaciones iniciales:

Ambas condiciones se pueden utilizar en las reglas de la postura. La primera regla hace juego solamente las evaluaciones iniciales y segunda hace juego todas las evaluaciones subsiguientes:

Verificación

Para confirmar que su configuración trabaja correctamente, asegúrese de que estos pasos estén completados según lo descrito:

1. El usuario de VPN conecta con el ASA.

2. El ASA envía un pedido de RADIUS y recibe una respuesta con la URL-**reorientación** y los atributos URL-reorientar-**ACL**:

3. Los registros ISE indican que la autorización hace juego el perfil de la postura (la primera entrada de registro):

4. El ASA agrega una reorientación a la sesión de VPN:
   ```
   aaa_url_redirect: Added url redirect:https://ise2.test-cisco.com:8443/
    guestportal/gateway?sessionId=c0a8700a0000900052b840e6&action=cpp
    acl:redirect for 10.10.10.10
   ```
5. El estatus de la sesión de VPN en el ASA muestra que la postura está requerida y reorienta el tráfico HTTP:
   ```
   ASA# show vpn-sessiondb detail anyconnect

   Session Type: AnyConnect Detailed

   Username     : cisco                  Index        : 9
   Assigned IP  : 10.10.10.10            Public IP    : 10.147.24.61
   Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
   License      : AnyConnect Essentials
   Encryption   : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)RC4  DTLS-Tunnel: (1)AES128
   Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA1  DTLS-Tunnel: (1)SHA1
   Bytes Tx     : 16077                  Bytes Rx     : 19497
   Pkts Tx      : 43                     Pkts Rx      : 225
   Pkts Tx Drop : 0                      Pkts Rx Drop : 0
   Group Policy : GP-SSL                 Tunnel Group : RA
   Login Time   : 14:55:50 CET Mon Dec 23 2013
   Duration     : 0h:01m:34s
   Inactivity   : 0h:00m:00s
   VLAN Mapping : N/A                    VLAN         : none
   Audt Sess ID : c0a8700a0000900052b840e6
   Security Grp : 0

   AnyConnect-Parent Tunnels: 1
   SSL-Tunnel Tunnels: 1
   DTLS-Tunnel Tunnels: 1

   AnyConnect-Parent:
    Tunnel ID    : 9.1
    Public IP    : 10.147.24.61
    Encryption   : none                   Hashing      : none
   ```

```
 TCP Src Port : 50025                 TCP Dst Port : 443
 Auth Mode    : userPassword
 Idle Time Out: 30 Minutes            Idle TO Left : 28 Minutes
 Client OS    : win
 Client Type  : AnyConnect
 Client Ver   : Cisco AnyConnect VPN Agent for Windows 3.1.02040
 Bytes Tx     : 5204                  Bytes Rx     : 779
 Pkts Tx      : 4                     Pkts Rx      : 1
 Pkts Tx Drop : 0                     Pkts Rx Drop : 0

SSL-Tunnel:
 Tunnel ID    : 9.2
 Assigned IP  : 10.10.10.10          Public IP    : 10.147.24.61
 Encryption   : RC4                   Hashing      : SHA1
 Encapsulation: TLSv1.0               TCP Src Port : 50044
 TCP Dst Port : 443                   Auth Mode    : userPassword
 Idle Time Out: 30 Minutes            Idle TO Left : 28 Minutes
 Client OS    : Windows
 Client Type  : SSL VPN Client
 Client Ver   : Cisco AnyConnect VPN Agent for Windows 3.1.02040
 Bytes Tx     : 5204                  Bytes Rx     : 172
 Pkts Tx      : 4                     Pkts Rx      : 2
 Pkts Tx Drop : 0                     Pkts Rx Drop : 0

DTLS-Tunnel:
 Tunnel ID    : 9.3
 Assigned IP  : 10.10.10.10           Public IP    : 10.147.24.61
 Encryption   : AES128                Hashing      : SHA1
 Encapsulation: DTLSv1.0              UDP Src Port : 63296
 UDP Dst Port : 443                   Auth Mode    : userPassword
 Idle Time Out: 30 Minutes            Idle TO Left : 29 Minutes
 Client OS    : Windows
 Client Type  : DTLS VPN Client
 Client Ver   : Cisco AnyConnect VPN Agent for Windows 3.1.02040
 Bytes Tx     : 5669                  Bytes Rx     : 18546
 Pkts Tx      : 35                    Pkts Rx      : 222
 Pkts Tx Drop : 0                     Pkts Rx Drop : 0

ISE Posture:
  Redirect URL : https://ise2.test-cisco.com:8443/guestportal/gateway?
   sessionId=c0a8700a0000900052b840e6&action=cpp
  Redirect ACL : redirect
```

6. Reorientan al cliente que inicia el tráfico HTTP que hace juego la reorientación ACL al ISE:

```
aaa_url_redirect: Created proxy for 10.10.10.10
aaa_url_redirect: Sending url redirect:https://ise2.test-cisco.com:8443/
 guestportal/gateway?sessionId=c0a8700a0000900052b840e6&action=cpp
 for 10.10.10.10
```

7. Reorientan al cliente al ISE para la postura:

8. El agente del NAC está instalado. Después de que el agente del NAC esté instalado, descarga las reglas de la postura vía el protocolo SWISS y realiza los controles para determinar la conformidad. El informe de la postura entonces se envía al ISE.

9. El ISE recibe el informe de la postura, evalúa de nuevo las reglas de la autorización, y (si es necesario) cambia el estatus de autorización y envía un CoA. Esto se puede verificar en **ise-**

psc.log:

```
cisco.cpm.posture.runtime.PostureHandlerImpl -:cisco:c0a8700a0000900052b840e6
 :::- Decrypting report
cisco.cpm.posture.runtime.PostureManager -:cisco:c0a8700a0000900052b840e6
 :::- User cisco belongs to groups NAC Group:NAC:IdentityGroups:User Identity
 Groups:Employee,NAC Group:NAC:IdentityGroups:An
cisco.cpm.posture.runtime.PostureManager -:cisco:c0a8700a0000900052b840e6
 :::- Posture report token for endpoint mac 08-00-27-CD-E8-A2 is Healthy
cisco.cpm.posture.runtime.PostureManager -:cisco:c0a8700a0000900052b840e6
 :::- Posture state is compliant for endpoint with mac 08-00-27-CD-E8-A2
cisco.cpm.posture.runtime.PostureCoA -:cisco:c0a8700a0000900052b840e6
 :::- Posture CoA is triggered for endpoint [null] with session
 [c0a8700a0000900052b840e6]
```

10. El ISE envía un CoA RADIUS que incluya el session_id y el nombre DACL que permite el acceso total:

    Esto se refleja en los registros ISE:

    La primera entrada de registro está para la autenticación inicial que vuelve el perfil de la postura (con el cambio de dirección).

    Se puebla la segunda entrada de registro después de que se reciba el informe SUIZO obediente.

    La tercera entrada de registro se puebla cuando se envía el CoA, junto con la confirmación (descrita como autorización dinámica tenida éxito).

    Se crea la entrada de registro final cuando el ASA descarga el DACL.

11. Los debugs en el ASA muestran que el CoA está recibido y la reorientación está quitada. El ASA descarga el DACLs si es necesario:

```
ASA# Received RAD_COA_REQUEST

RADIUS packet decode (CoA-Request)

Radius: Value (String) =
41 43 53 3a 43 69 73 63 6f 53 65 63 75 72 65 2d    |  ACS:CiscoSecure-
44 65 66 69 6e 65 64 2d 41 43 4c 3d 23 41 43 53    |  Defined-ACL=#ACS
41 43 4c 23 2d 49 50 2d 50 45 52 4d 49 54 5f 41    |  ACL#-IP-PERMIT_A
4c 4c 5f 54 52 41 46 46 49 43 2d 35 31 65 66 37    |  LL_TRAFFIC-51ef7
64 62 31                                           |  db1

Got AV-Pair with value audit-session-id=c0a8700a0000900052b840e6
Got AV-Pair with value ACS:CiscoSecure-Defined-ACL=
 #ACSACL#-IP-PERMIT_ALL_TRAFFIC-51ef7db1

aaa_url_redirect: Deleted url redirect for 10.10.10.10
```

12. Después de la sesión de VPN, Cisco tiene el DACL solicitado (acceso total) el usuario:

```
ASA# show vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed

Username     : cisco                 Index        : 9
```

```
Assigned IP  : 10.10.10.10           Public IP    : 10.147.24.61
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Essentials
Encryption   : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)RC4  DTLS-Tunnel: (1)AES128
Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA1  DTLS-Tunnel: (1)SHA1
Bytes Tx     : 94042                 Bytes Rx     : 37079
Pkts Tx      : 169                   Pkts Rx      : 382
Pkts Tx Drop : 0                     Pkts Rx Drop : 0
Group Policy : GP-SSL                Tunnel Group : RA
Login Time   : 14:55:50 CET Mon Dec 23 2013
Duration     : 0h:05m:30s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                   VLAN         : none
Audt Sess ID : c0a8700a0000900052b840e6
Security Grp : 0

AnyConnect-Parent Tunnels: 1
SSL-Tunnel Tunnels: 1
DTLS-Tunnel Tunnels: 1

AnyConnect-Parent:
 Tunnel ID    : 9.1
 Public IP    : 10.147.24.61
 Encryption   : none                  Hashing      : none
 TCP Src Port : 50025                 TCP Dst Port : 443
 Auth Mode    : userPassword
 Idle Time Out: 30 Minutes            Idle TO Left : 24 Minutes
 Client OS    : win
 Client Type  : AnyConnect
 Client Ver   : Cisco AnyConnect VPN Agent for Windows 3.1.02040
 Bytes Tx     : 5204                  Bytes Rx     : 779
 Pkts Tx      : 4                     Pkts Rx      : 1
 Pkts Tx Drop : 0                     Pkts Rx Drop : 0

SSL-Tunnel:
 Tunnel ID    : 9.2
 Assigned IP  : 10.10.10.10           Public IP    : 10.147.24.61
 Encryption   : RC4                   Hashing      : SHA1
 Encapsulation: TLSv1.0               TCP Src Port : 50044
 TCP Dst Port : 443                   Auth Mode    : userPassword
 Idle Time Out: 30 Minutes            Idle TO Left : 24 Minutes
 Client OS    : Windows
 Client Type  : SSL VPN Client
 Client Ver   : Cisco AnyConnect VPN Agent for Windows 3.1.02040
 Bytes Tx     : 5204                  Bytes Rx     : 172
 Pkts Tx      : 4                     Pkts Rx      : 2
 Pkts Tx Drop : 0                     Pkts Rx Drop : 0
 Filter Name  : #ACSACL#-IP-PERMIT_ALL_TRAFFIC-51ef7db1

DTLS-Tunnel:
 Tunnel ID    : 9.3
 Assigned IP  : 10.10.10.10           Public IP    : 10.147.24.61
 Encryption   : AES128                Hashing      : SHA1
 Encapsulation: DTLSv1.0              UDP Src Port : 63296
 UDP Dst Port : 443                   Auth Mode    : userPassword
 Idle Time Out: 30 Minutes            Idle TO Left : 29 Minutes
 Client OS    : Windows
 Client Type  : DTLS VPN Client
 Client Ver   : Cisco AnyConnect VPN Agent for Windows 3.1.02040
 Bytes Tx     : 83634                 Bytes Rx     : 36128
 Pkts Tx      : 161                   Pkts Rx      : 379
 Pkts Tx Drop : 0                     Pkts Rx Drop : 0
 Filter Name  : #ACSACL#-IP-PERMIT_ALL_TRAFFIC-51ef7db1
```

Nota: El ASA quita siempre las reglas de la reorientación, incluso cuando el CoA no tiene ningún DACL asociado.

Troubleshooting

Esta sección proporciona la información que usted puede utilizar para resolver problemas su configuración.

Debugs en el ISE

Navegue a la **administración > a la configuración del registro del registro > del debug** para habilitar los debugs. Cisco recomienda que usted habilita los debugs temporales para:

- SUIZO
- Expedición directa (NSF)
- NSF-sesión
- Disposición
- Postura

Ingrese este comando en el CLI para ver los debugs:

```
ise2/admin# show logging application ise-psc.log tail count 100
```

Navegue a las **operaciones > a los informes > al ISE señala > los puntos finales y los usuarios > los detalles de la postura evaluación** para ver los informes de la postura:

En la postura más página de la evaluación del detalle, allí es nombre de la directiva con un nombre del requisito se visualice que, junto con los resultados:

Debugs en el ASA

Usted puede habilitar estos debugs en el ASA:

- **el debug aaa URL-reorienta**
- **debug aaa authorization**
- **dinámico-autorización del radio del debug**
- **el radio del debug decodifica**
- **usuario de RADIUS Cisco del debug**

Debugs para el agente

Para el agente del NAC, es posible recolectar los debugs con el embalador del registro de Cisco, que se inicia del GUI o con el CLI: **CCAAgentLogPackager.app.**

Consejo: Usted puede decodificar los resultados con la herramienta del Centro de Asistencia Técnica (TAC).

Para extraer los registros para el agente de la red, navegue a estas ubicaciones:

- **C: > documento y configuraciones > *<user>* > Configuraciones locales > temporeros > webagent.log** (decodificado con la herramienta del TAC)
- **C: > documento y configuraciones > *<user>* > Configuraciones locales > temporeros > webagentsetup.log**

  Nota: Si los registros no están en estas ubicaciones, después verifique la **variable de entorno de los TEMPOREROS**.

Error de la postura del agente del NAC

Si la postura falla, presentan el usuario con la razón:

Entonces no prohiben el usuario las acciones de la corrección si se configuran:

Información Relacionada

- Configurar a un servidor externo para la autorización de usuario del dispositivo de seguridad
- Guía de configuración CLI de la serie VPN de Cisco ASA, 9.1
- Guía del usuario del Cisco Identity Services Engine, versión 1.2
- Soporte Técnico y Documentación - Cisco Systems