Integración de la configuración WSA con el ISE para los servicios enterados de TrustSec

Contenido

Introducción

Este documento describe cómo integrar el dispositivo de seguridad de la red (WSA) con el Identity Services Engine (ISE). La versión 1.3 ISE soporta un nuevo pxGrid llamado API. Estos soportes a protocolo modernos y flexibles autenticación, cifrado, y privilegios (grupos) que permite la

integración fácil con otras soluciones acerca de la seguridad.

La versión 8.7 WSA soporta el protocolo del pxGrid y puede extraer la información de identidad del contexto del ISE. Como consecuencia, WSA permite que usted construya las directivas basadas en los grupos de la etiqueta del grupo de seguridad de TrustSec (SGT) extraídos del ISE.

Prerequisites

Requisitos

Cisco recomienda que usted tiene experiencia con la configuración de Cisco ISE y el conocimiento básico de estos temas:

- Implementaciones y configuración de la autorización ISE
- Configuración CLI adaptante del dispositivo de seguridad (ASA) para el acceso de TrustSec y VPN
- Configuración WSA
- Comprensión básica de las implementaciones de TrustSec

Componentes Utilizados

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

- Microsoft Windows 7
- Versión de software 1.3 de Cisco ISE y posterior
- Versión 3.1 y posterior del Mobile Security de Cisco AnyConnect
- Versión de ASA 9.3.1 de Cisco y posterior
- Versión 8.7 y posterior de Cisco WSA

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.

Configurar

> **Note**: Use la Command Lookup Tool (clientes registrados solamente) para obtener más información sobre los comandos usados en esta sección.

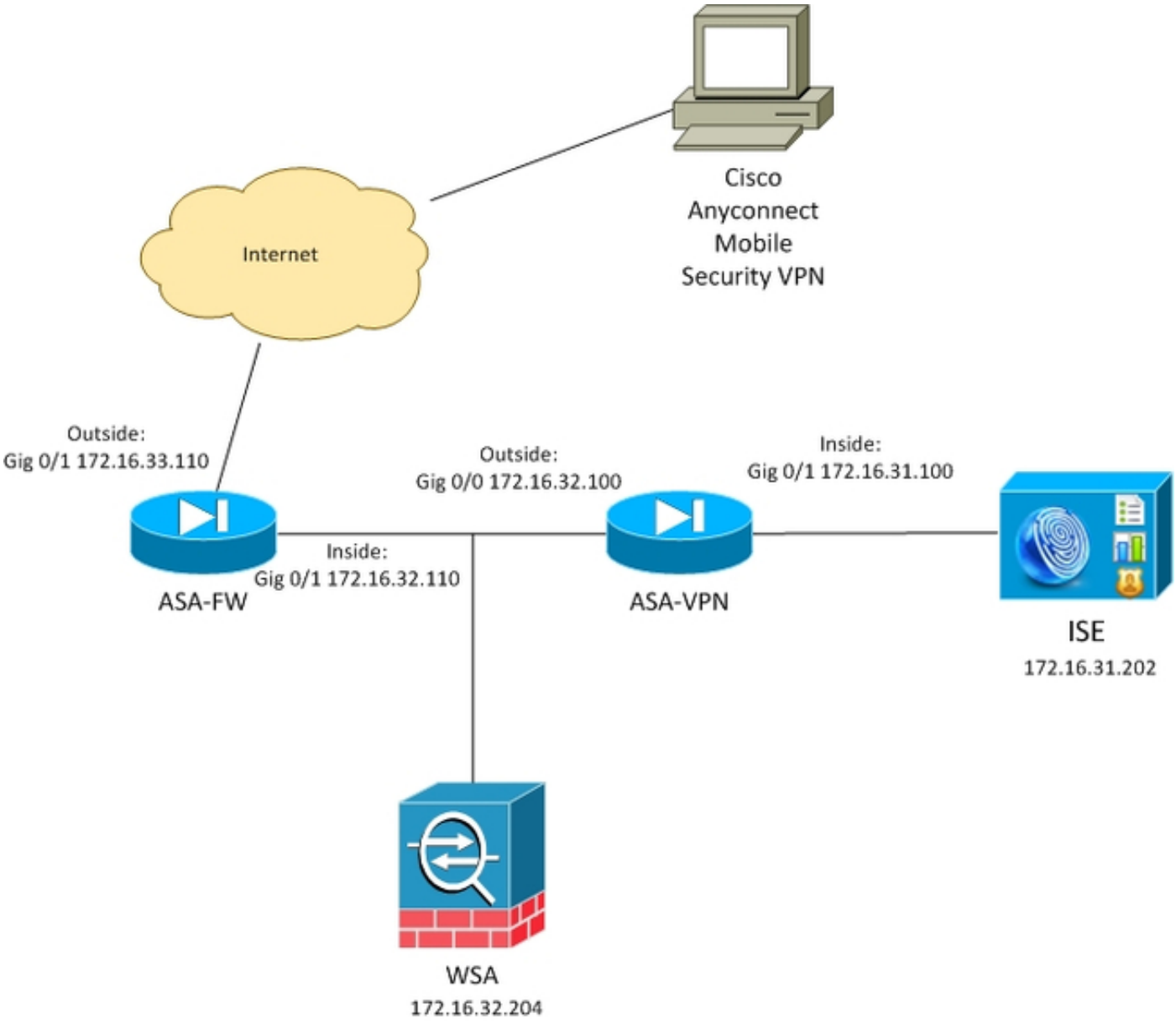
Diagrama de la red y flujo de tráfico

Las etiquetas de TrustSec SGT son asignadas por el ISE usado como servidor de autenticación para todos los tipos de usuarios que accedan la red corporativa. Esto implica atado con

alambre/los usuarios de red inalámbrica que autentican vía los portales del 802.1x o del invitado ISE. También, usuarios de VPN remotos que utilizan el ISE para la autenticación.

Para WSA, no importa cómo el usuario ha accedido la red.

Este ejemplo presenta a los usuarios de VPN remotos que terminan la sesión sobre el ASA-VPN. Han asignado esos usuarios una etiqueta específica SGT. Todo el tráfico HTTP a Internet será interceptado por el ASA-FW (Firewall) y reorientado al WSA para el examen. El WSA utiliza el perfil de la identidad que permite que clasifique a los usuarios basados en la etiqueta SGT y que construya el acceso o las políticas de descifrado basadas en ése.



El flujo detallado es:

1. El usuario de VPN de AnyConnect termina la sesión de Secure Sockets Layer (SSL) sobre el ASA-VPN. El ASA-VPN se configura para TrustSec y utiliza el ISE para la autenticación de usuarios VPN. Asignan el usuario autenticado un valor de la etiqueta SGT = 2 (name= las TIC). El usuario recibe una dirección IP de la red 172.16.32.0/24 (172.16.32.50 en este ejemplo).
2. El usuario intenta acceder la página web en Internet. El ASA-FW se configura para el protocolo web cache communication (WCCP) que reorienta el tráfico al WSA.

3. El WSA se configura para la integración ISE. Utiliza el pxGrid para descargar la información del ISE: el IP address 172.16.32.50 del usuario se ha asignado la etiqueta 2. SGT.
4. El WSA procesa el pedido de HTTP del usuario y golpea la política de acceso PolicyForIT. Que la directiva está configurada para bloquear el tráfico a los sitios de los deportes. El resto de los usuarios (que no pertenecen a SGT 2) golpean la política de acceso predeterminada y tienen acceso total a los deportes localizan.

ASA-VPN

Esto es un gateway de VPN configurado para TrustSec. La configuración detallada está fuera de alcance de este documento. Refiera a estos ejemplos:

- ASA y ejemplo de configuración de TrustSec del Catalyst 3750X Series Switch y guía del Troubleshooting
- Ejemplo de configuración de la clasificación y de la aplicación de la Versión de ASA 9.2 VPN SGT

ASA-FW

El Firewall ASA es responsable del redireccionamiento de WCCP al WSA. Este dispositivo no es consciente de TrustSec.

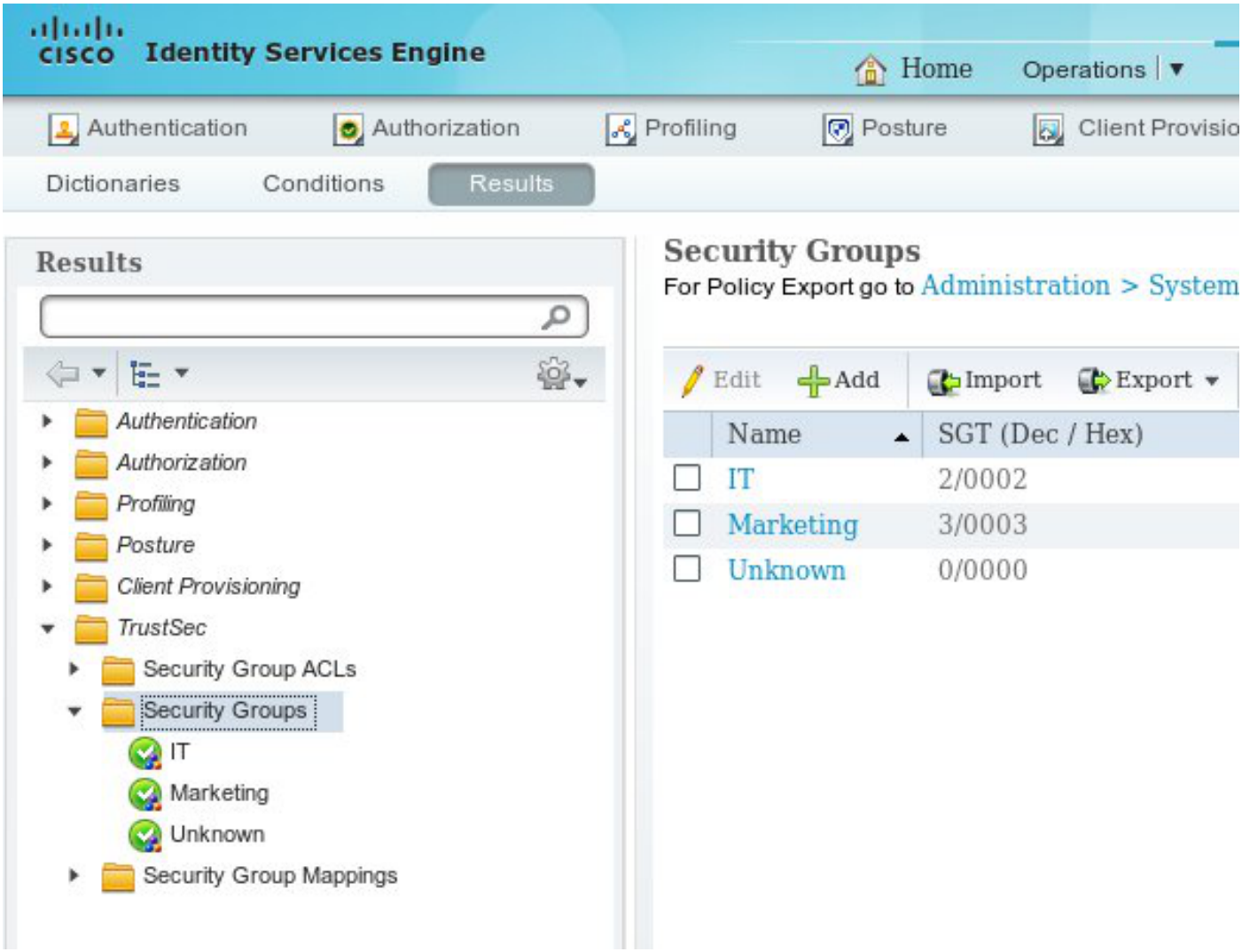
```
interface GigabitEthernet0/0
 nameif outside
 security-level 100
 ip address 172.16.33.110 255.255.255.0

interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 172.16.32.110 255.255.255.0

access-list wccp-routers extended permit ip host 172.16.32.204 any
access-list wccp-redirect extended deny tcp any host 172.16.32.204
access-list wccp-redirect extended permit tcp any any eq www
access-list wccp-redirect extended permit tcp any any eq https

wccp 90 redirect-list wccp-redirect group-list wccp-routers
wccp interface inside 90 redirect in
```

ISE

El ISE es un punto central en el despliegue de TrustSec. Asigna las etiquetas SGT a todos los usuarios que accedan y autentiquen a la red. Los pasos requeridos para la configuración básica se enumeran en esta sección.

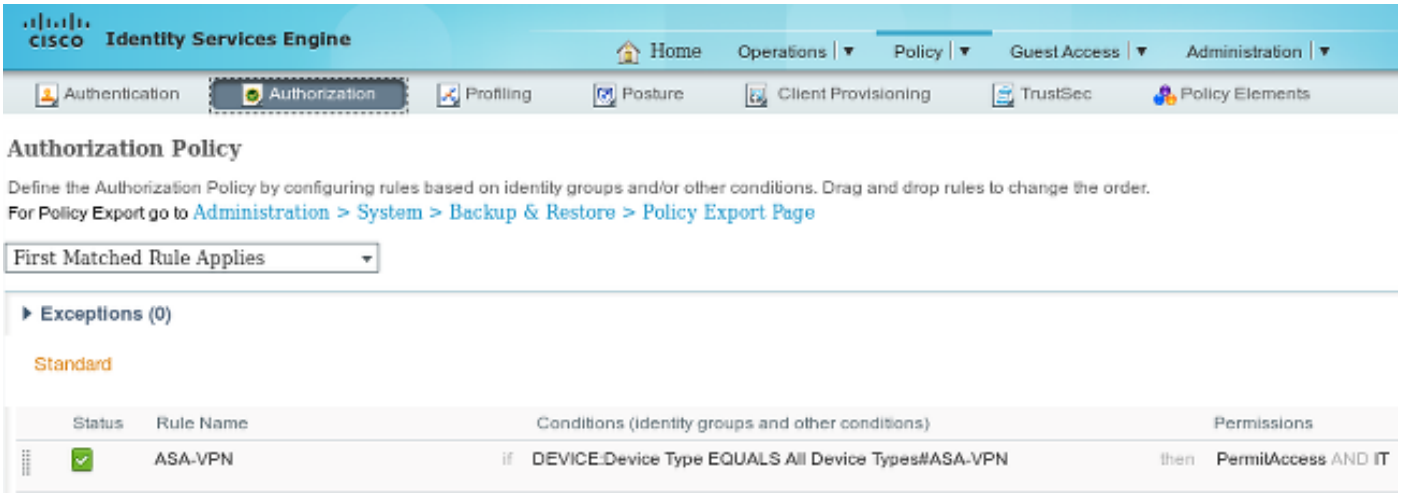
Paso 1. SGT para el TIC y el otro grupo

Elija los **grupos del > Security (Seguridad) del acceso del grupo del > Security (Seguridad) de la directiva > de los resultados** y cree el SGT:



Paso 2. Regla de la autorización para el acceso VPN que asigna SGT = 2 (las TIC)

Elija la **directiva > la autorización** y cree una regla para el acceso del telecontrol VPN. Todas las conexiones VPN establecidas vía ASA-VPN conseguirán el acceso total (PermitAccess) y serán asignadas la etiqueta 2 (las TIC) SGT.



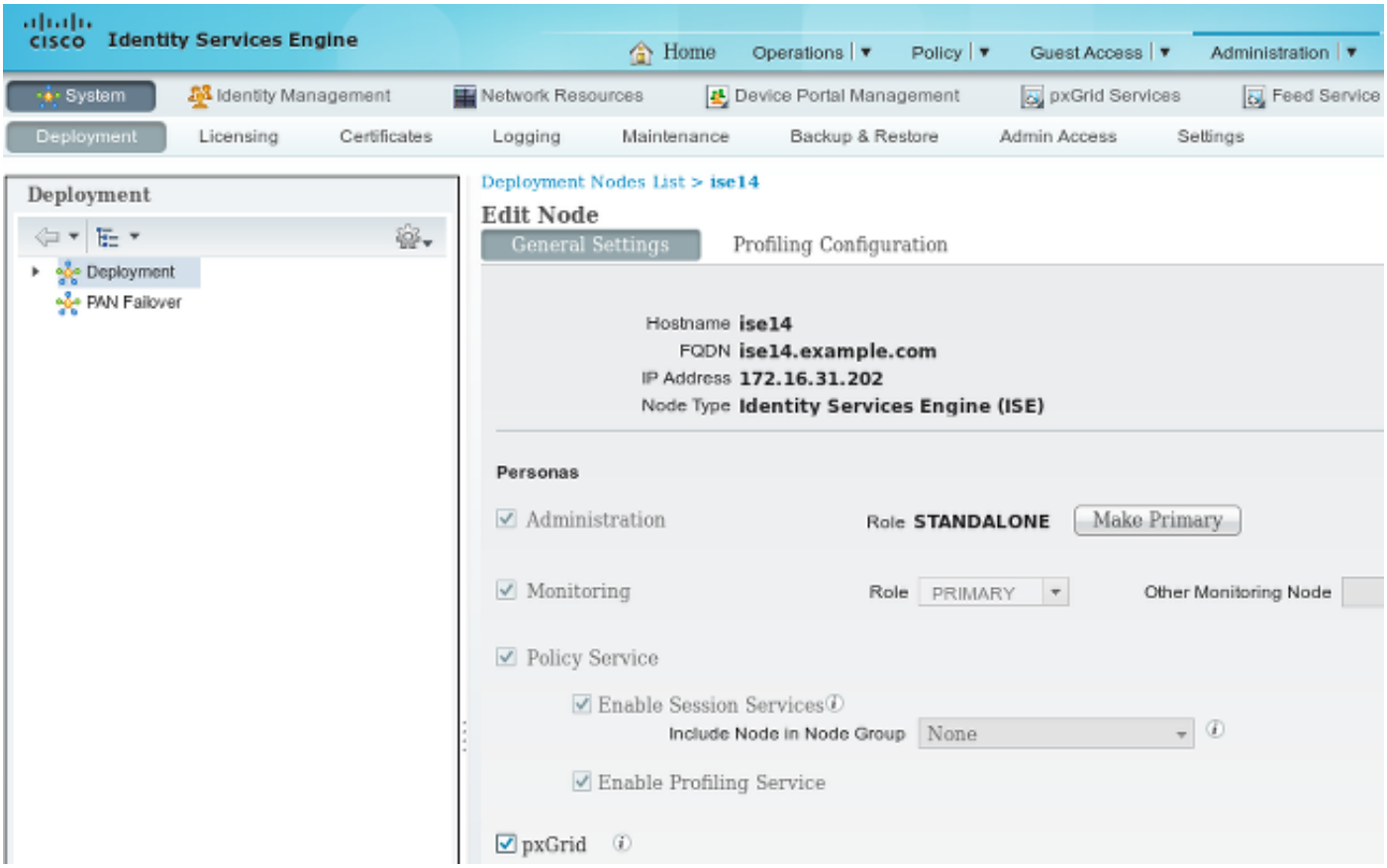
Paso 3. Agregue el dispositivo de red y genere el archivo PAC para ASA-VPN

Para agregar el ASA-VPN al dominio de TrustSec, es necesario generar el archivo auto de los Config del proxy (PAC) manualmente. Ese archivo será importado en el ASA.

Eso se puede configurar de la **administración > de los dispositivos de red**. Después de que se agregue el ASA, navegue hacia abajo a las configuraciones de TrustSec y genere el archivo PAC. Los detalles para ése se describen en un documento (referido) separado.

Paso 4. Papel del pxGrid del permiso

Elija la **administración > el despliegue** para habilitar el papel del pxGrid.



Paso 5. Genere el certificado para la administración y el papel del pxGrid

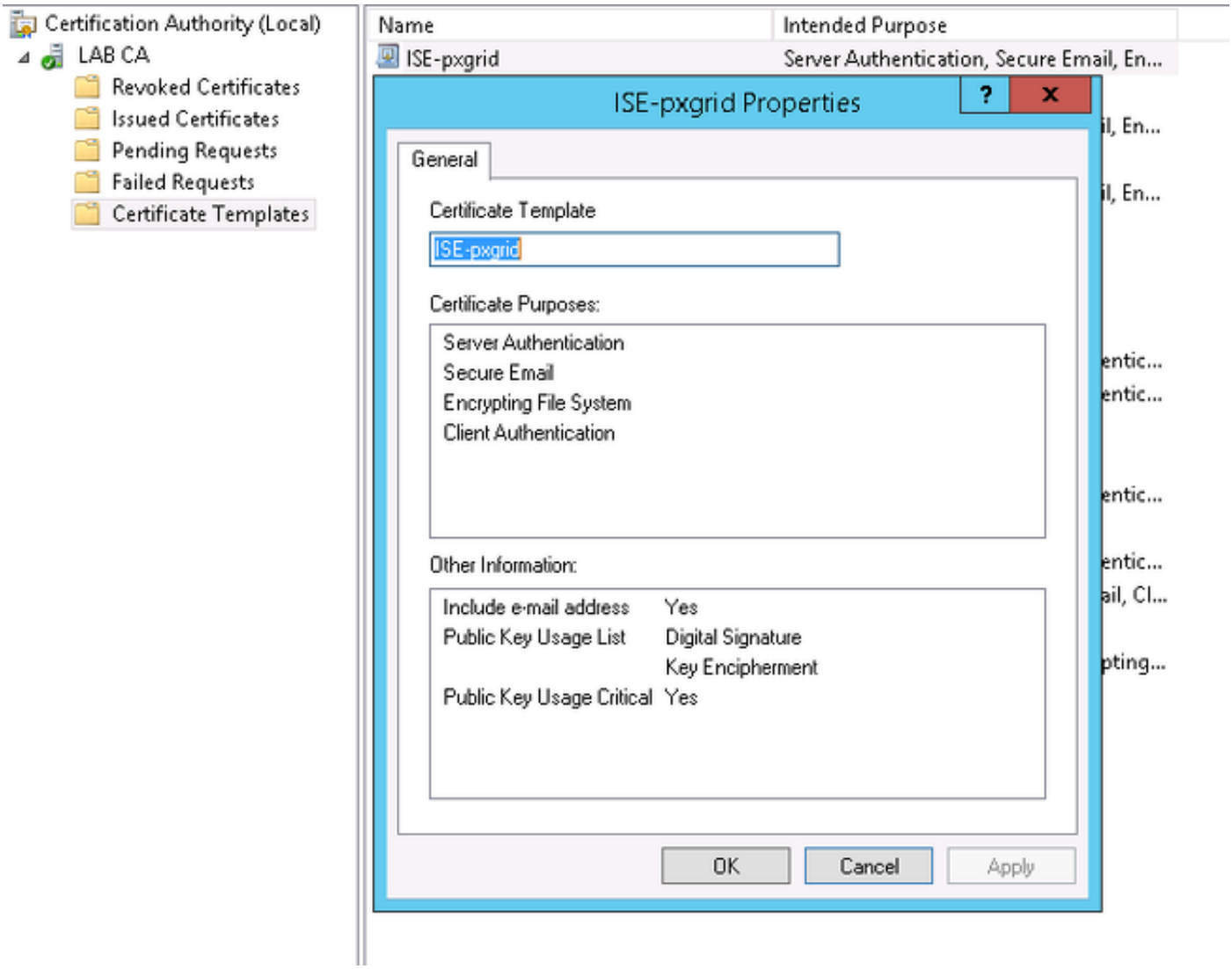
El protocolo del pxGrid utiliza la autenticación certificada para el cliente y el servidor. Es muy importante configurar los Certificados correctos para el ISE y el WSA. Ambos Certificados deben incluir el nombre de dominio completo (FQDN) en el tema y las Extensiones x509 para la autenticación de cliente y la autenticación de servidor. También, aseegurese el expediente correcto DNS A se crea para el ISE y el WSA y hace juego el FQDN correspondiente.

Si ambos Certificados son firmados por un diverso Certificate Authority (CA), es importante incluir esos CA en el almacén de confianza.

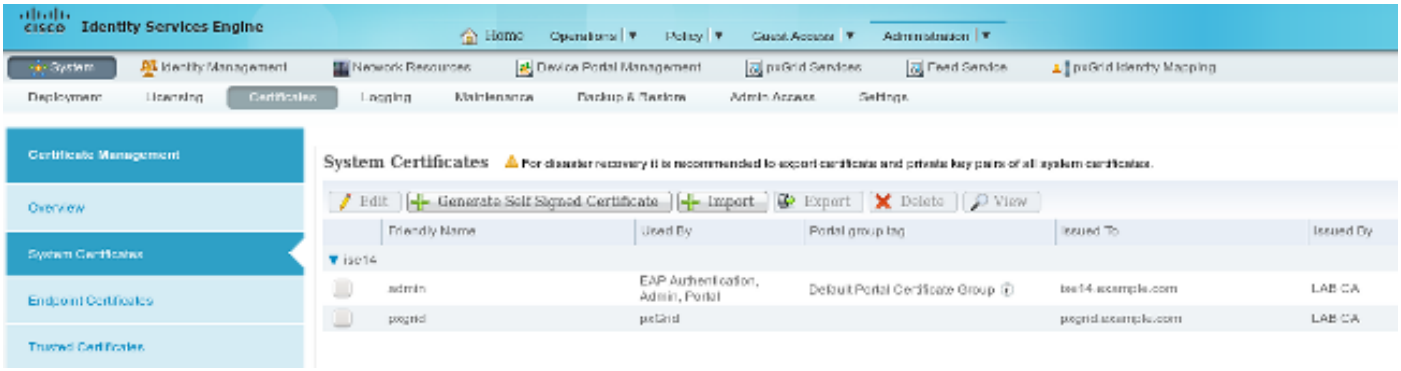
Para configurar los Certificados, elija la **administración > los Certificados**.

El ISE puede generar un pedido de firma de certificado (CSR) para cada papel. Para el papel del pxGrid, la exportación y firma el CSR con CA externo.

En este ejemplo, Microsoft CA se ha utilizado con esta plantilla:



El resultado final pudo parecer:

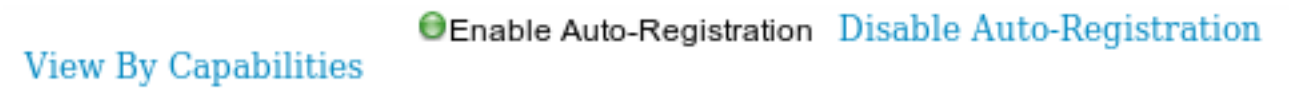


No olvide crear los expedientes DNS A para ise14.example.com y pxgrid.example.com que señalan a 172.16.31.202.

Inscripción automática del pxGrid del paso 6.

Por abandono, el ISE no registrará automáticamente a los suscriptores del pxGrid. Eso se debe aprobar manualmente por el administrador. Esa configuración se debe cambiar para la integración WSA.

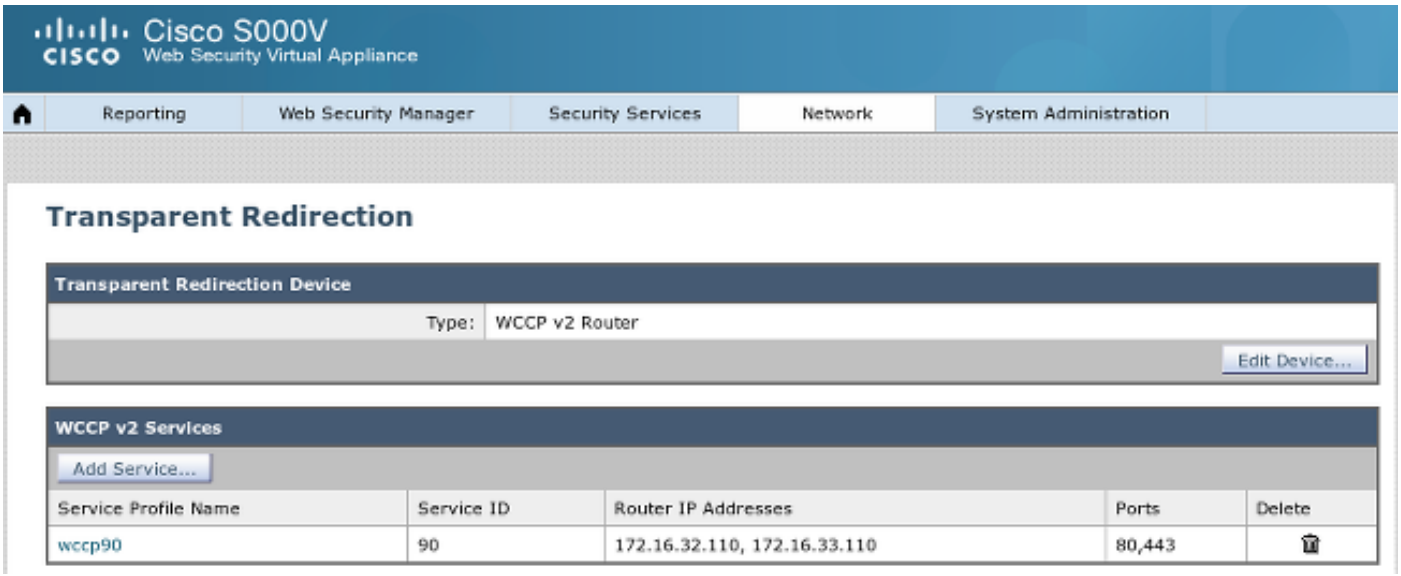
Elija los **servicios de la administración > del pxGrid** y el **autoregistro del permiso del** conjunto.



WSA

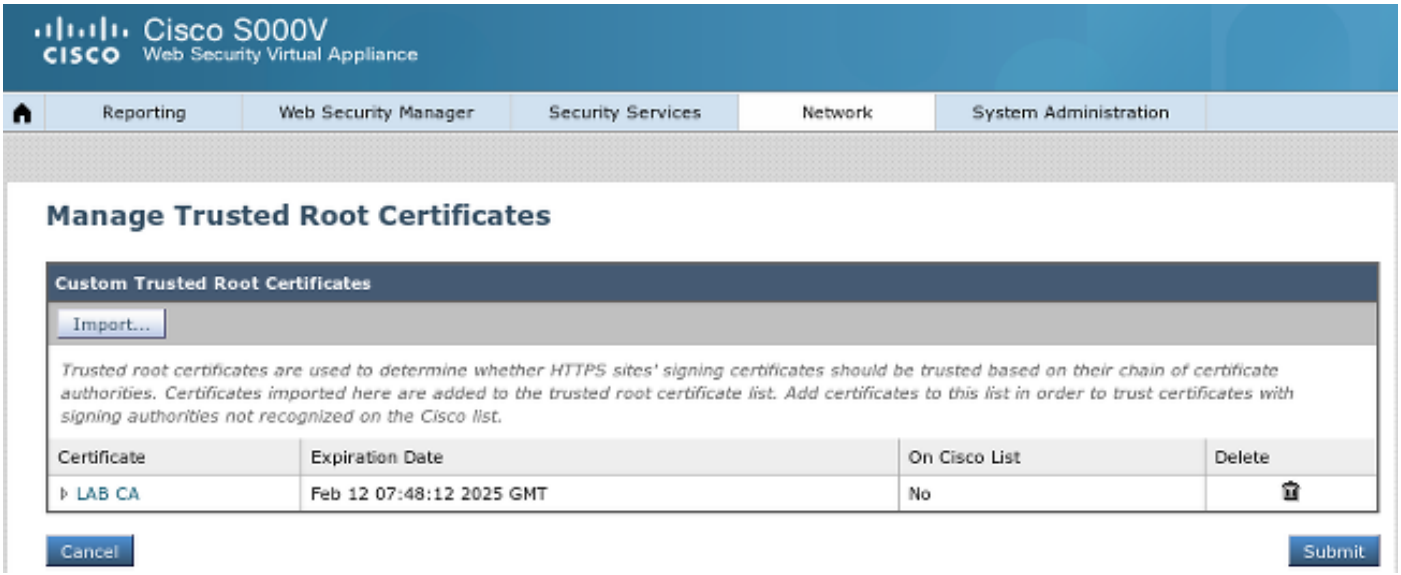
Paso 1. Modo transparente y cambio de dirección

En este ejemplo, el WSA se configura con apenas la interfaz de administración, el modo transparente, y el cambio de dirección del ASA:



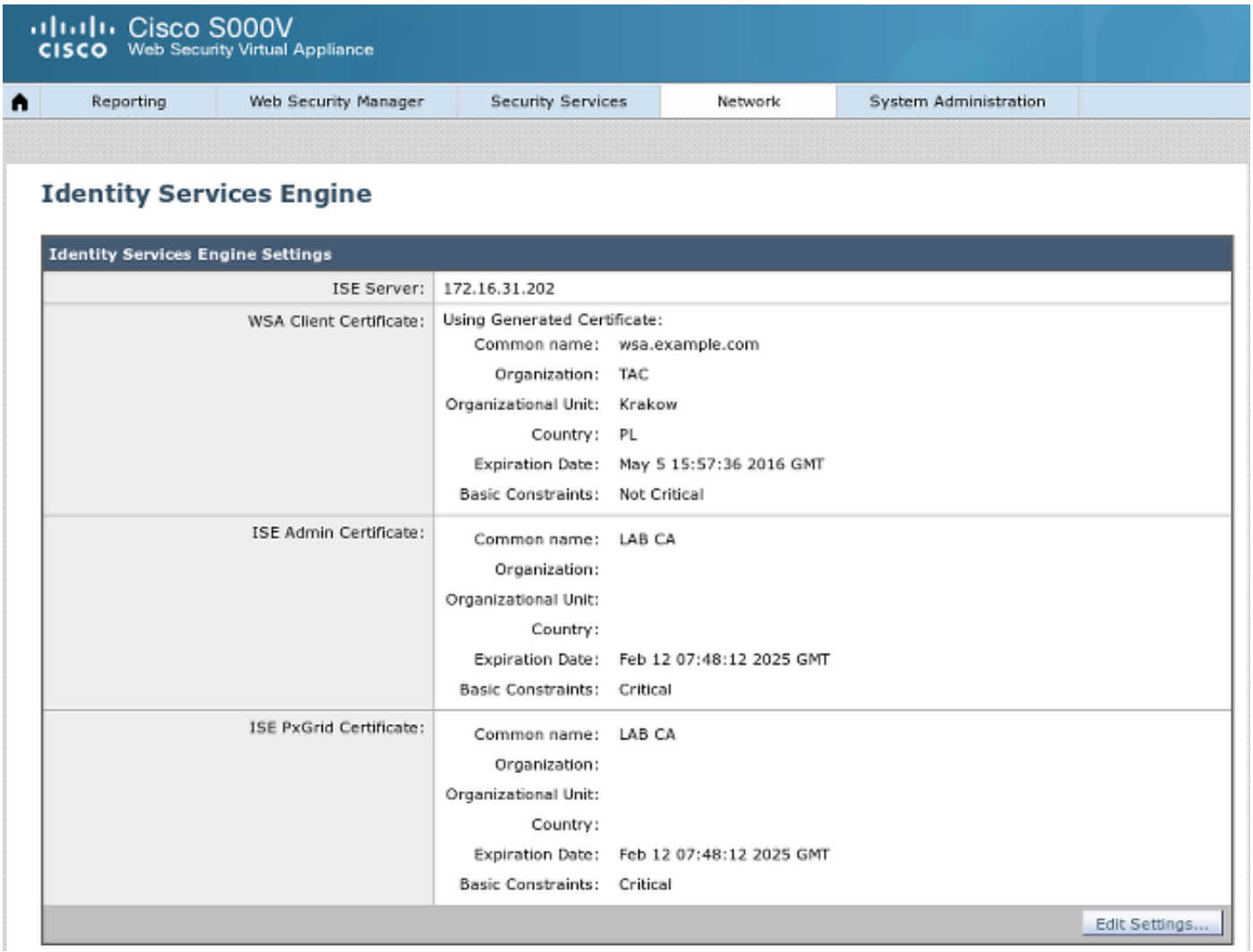
Paso 2. Generación del certificado

El WSA necesita confiar en CA para firmar todos los Certificados. Elija el **Certificate Management (Administración de certificados) de la red** para agregar un certificado de CA:



Es también necesario generar un certificado que el WSA utilizará para autenticar al pxGrid. Elija la **red > el Identity Services Engine > el certificado del cliente WSA** para generar el CSR, fírmelo con la plantilla correcta de CA (ISE-pxgrid), e impórtelo detrás.

También, para el “certificado ISE Admin” y “el certificado del pxGrid ISE”, importe el certificado de CA (para confiar en el certificado del pxGrid presentado por el ISE):

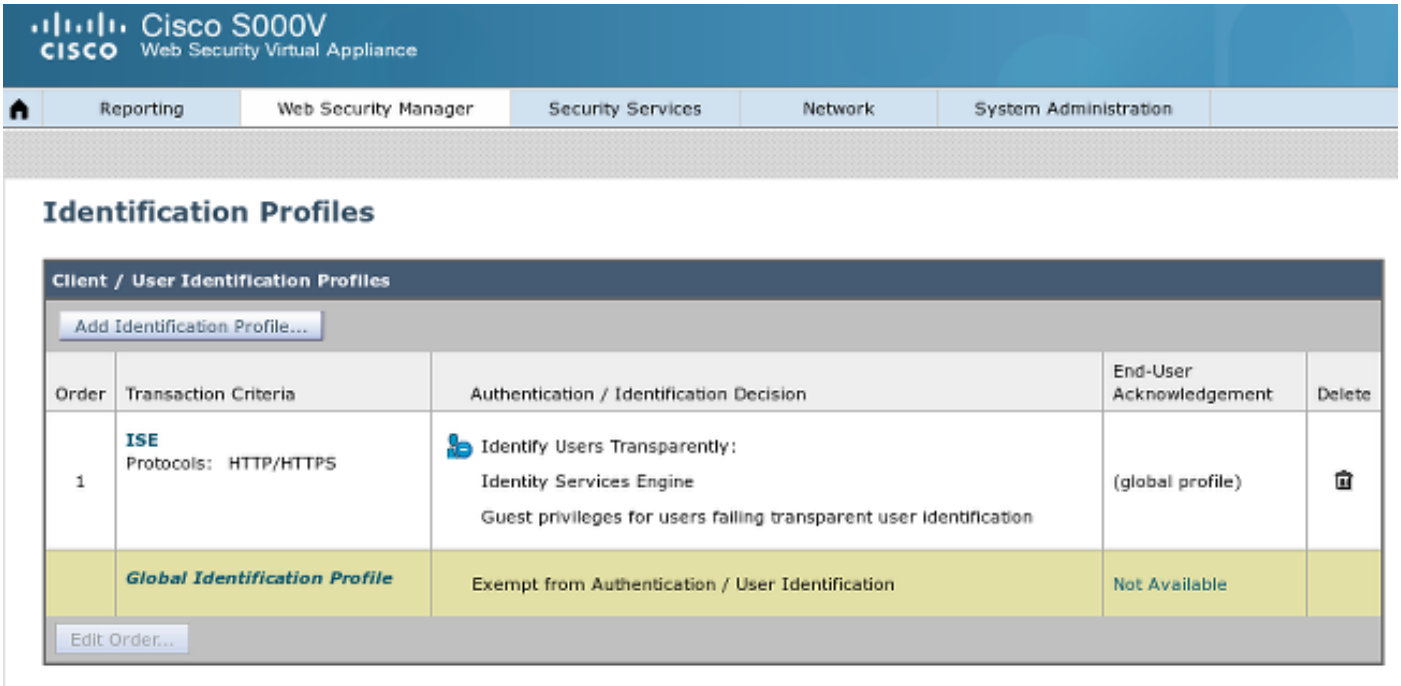


Paso 3. Pruebe la Conectividad ISE

Elija la **red > el Identity Services Engine** para probar la conexión al ISE:

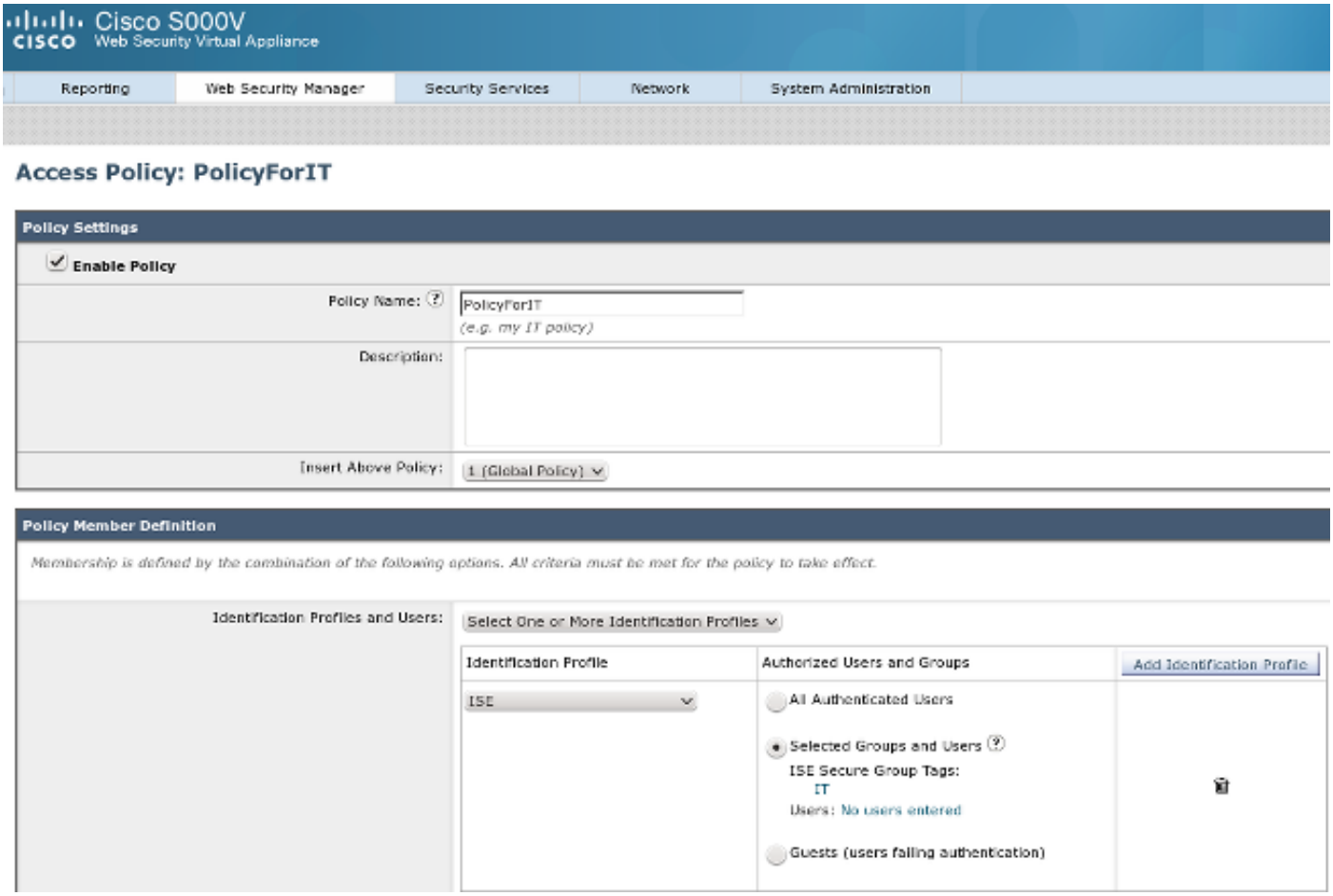
Paso 4. Perfiles de la identificación ISE

Elija los **perfiles del administrador de seguridad > de la identificación de la red** para agregar un nuevo perfil para el ISE. Para" el uso "de la "*identificación y de la autenticación transparente identifique a los usuarios con el ISE".*

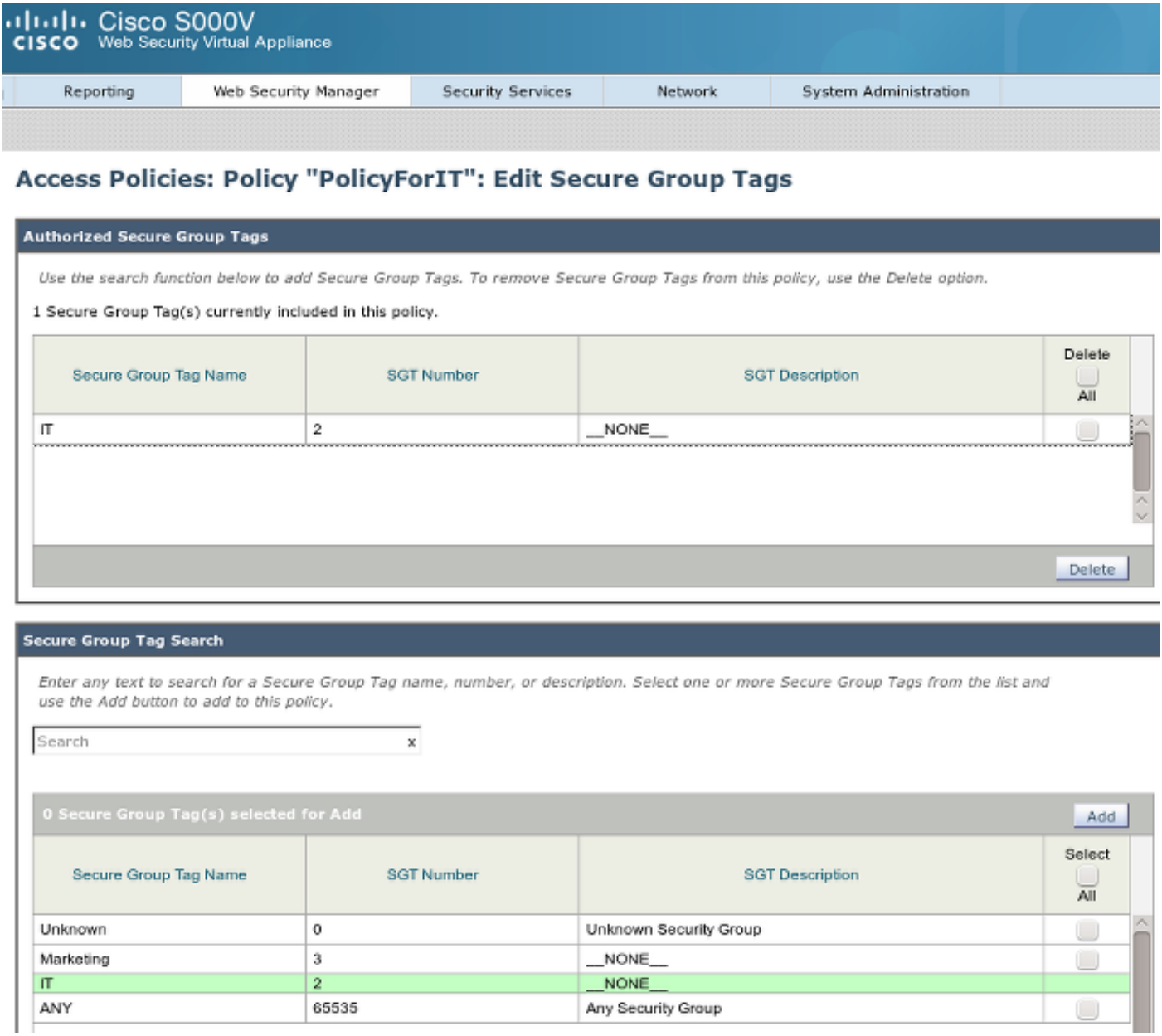


Paso 5. Acceda la directiva basada en la etiqueta SGT

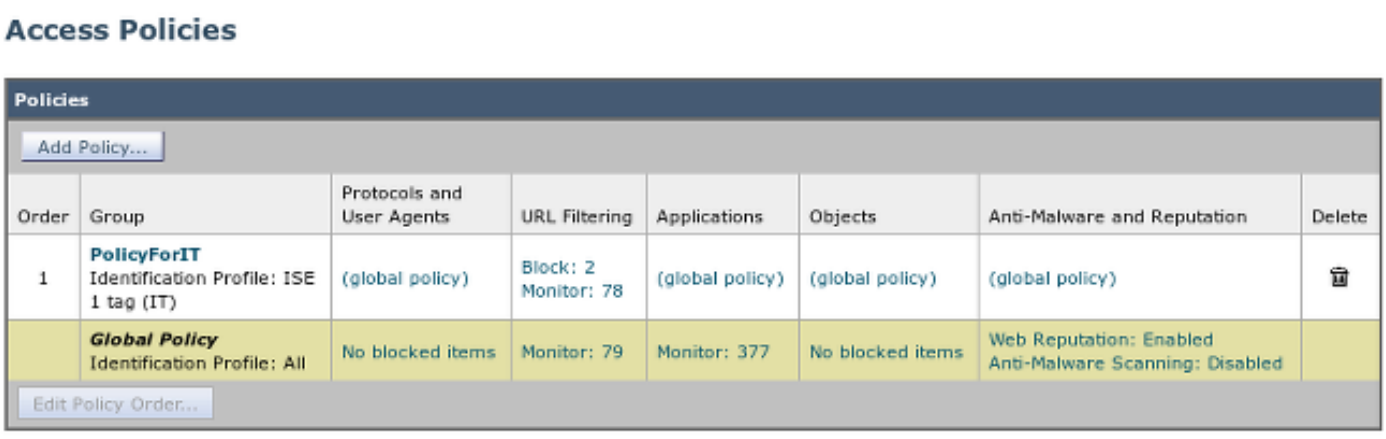
Elija el **administrador de seguridad > las políticas de acceso de la red** para agregar una nueva directiva. La calidad de miembro utiliza el perfil ISE:



Para los grupos y los usuarios seleccionados la etiqueta 2 SGT será agregada (las TIC):



La directiva niega el acceso a todos los sitios de los deportes para los usuarios que pertenecen a SGT LAS TIC:

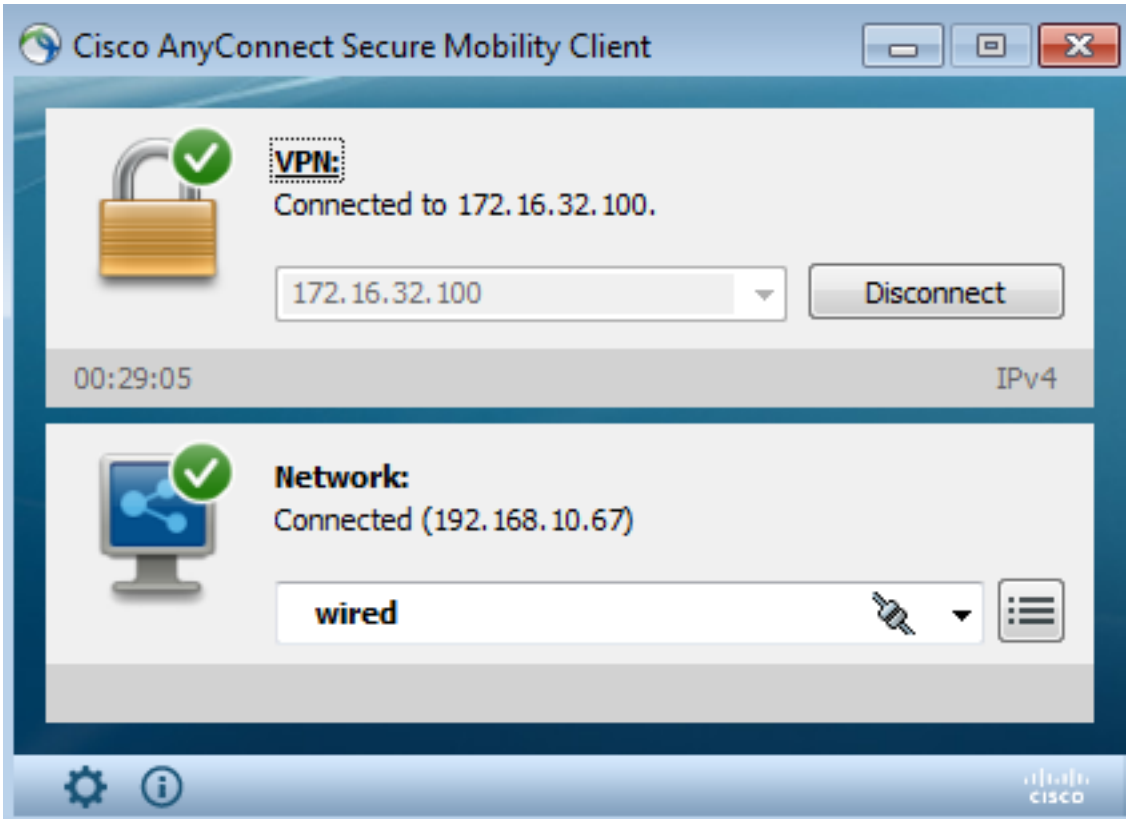


Verificación

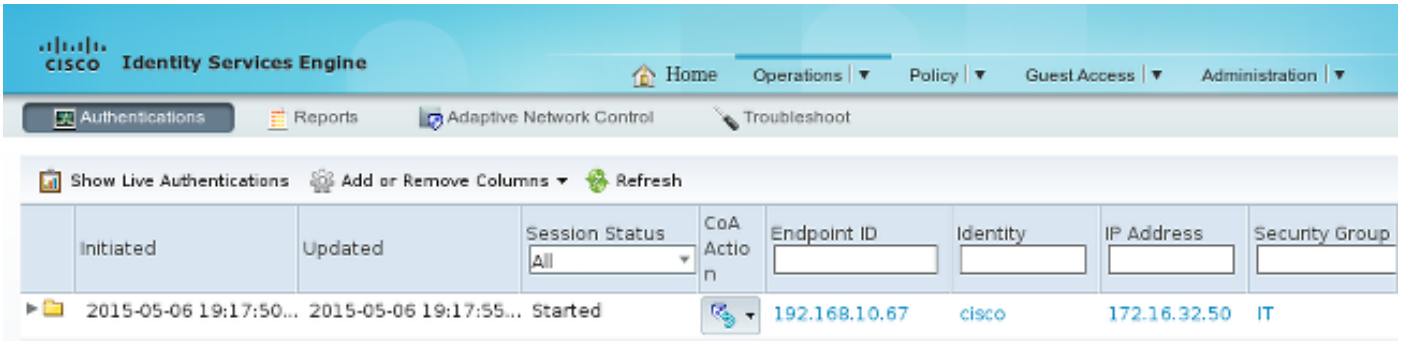
Utilize esta sección para confirmar que su configuración funcione correctamente.

Paso 1. Sesión de VPN

El usuario de VPN inicia a una sesión de VPN hacia el ASA-VPN:



El ASA-VPN utiliza el ISE para la autenticación. El ISE crea una sesión y asigna la etiqueta 2 (las TIC) SGT:



Después de la autenticación satisfactoria, el ASA-VPN crea a una sesión de VPN con la etiqueta 2 SGT (vuelta en el access-accept del radio en el Cisco-av-pair):

```
asa-vpn# show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username     : cisco                  Index        : 2
Assigned IP  : 172.16.32.50           Public IP    : 192.168.10.67
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     : 12979961               Bytes Rx     : 1866781
```

```
Group Policy : POLICY                 Tunnel Group : SSLVPN
Login Time   : 21:13:26 UTC Tue May 5 2015
Duration     : 6h:08m:03s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                    VLAN         : none
Audt Sess ID : ac1020640000200055493276
Security Grp : 2:IT
```

Puesto que el link entre el ASA-VPN y el ASA-FW no es TrustSec habilitado, el ASA-VPN envía las tramas sin Tags para ese tráfico (no pueda al GRE encapsulan las tramas Ethernet con el campo CMD/TrustSec inyectado).

Paso 2. Información de la sesión extraída por el WSA

En esta etapa, el WSA debe recibir la asignación entre la dirección IP, el nombre de usuario, y el SGT (vía el protocolo del pxGrid):

```
wsa.example.com> isedata


Choose the operation you want to perform:
- STATISTICS - Show the ISE server status and ISE statistics.
- CACHE - Show the ISE cache or check an IP address.
- SGTS - Show the ISE Secure Group Tag (SGT) table.
[]> CACHE


Choose the operation you want to perform:
- SHOW - Show the ISE ID cache.
- CHECKIP - Query the local ISE cache for an IP address
[]> SHOW


IP              Name                                                    SGT#
172.16.32.50    cisco                                                   2

Choose the operation you want to perform:
- SHOW - Show the ISE ID cache.
- CHECKIP - Query the local ISE cache for an IP address
[]>
```

Paso 3. Cambio de dirección del tráfico al WSA

El usuario de VPN inicia una conexión a sport.pl, que es interceptado por el ASA-FW:

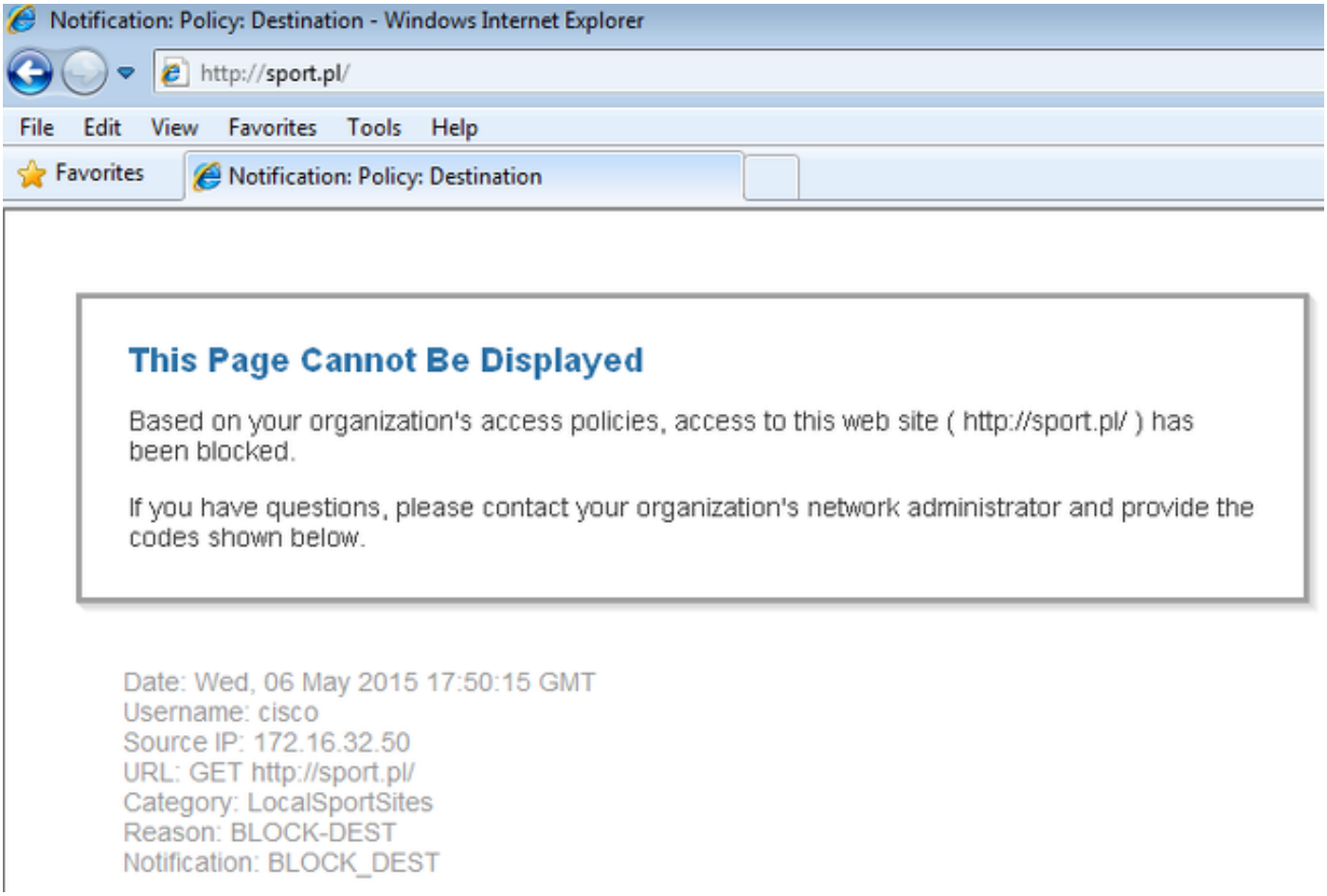
```
asa-fw# show wccp

Global WCCP information:
   Router information:
       Router Identifier:                   172.16.33.110
       Protocol Version:                    2.0

   Service Identifier: 90
```

```
        Number of Cache Engines:              1
        Number of routers:                    1
        Total Packets Redirected:             562
        Redirect access-list:                 wccp-redirect
        Total Connections Denied Redirect:    0
        Total Packets Unassigned:             0
        Group access-list:                    wccp-routers
        Total Messages Denied to Group:       0
        Total Authentication failures:        0
        Total Bypassed Packets Received:      0

asa-fw# show access-list wccp-redirect
access-list wccp-redirect; 3 elements; name hash: 0x9bab8633
access-list wccp-redirect line 1 extended deny tcp any host 172.16.32.204 (hitcnt=0)
0xfd875b28
access-list wccp-redirect line 2 extended permit tcp any any eq www (hitcnt=562)
0x028ab2b9
access-list wccp-redirect line 3 extended permit tcp any any eq https (hitcnt=0)
0xe202a11e
```

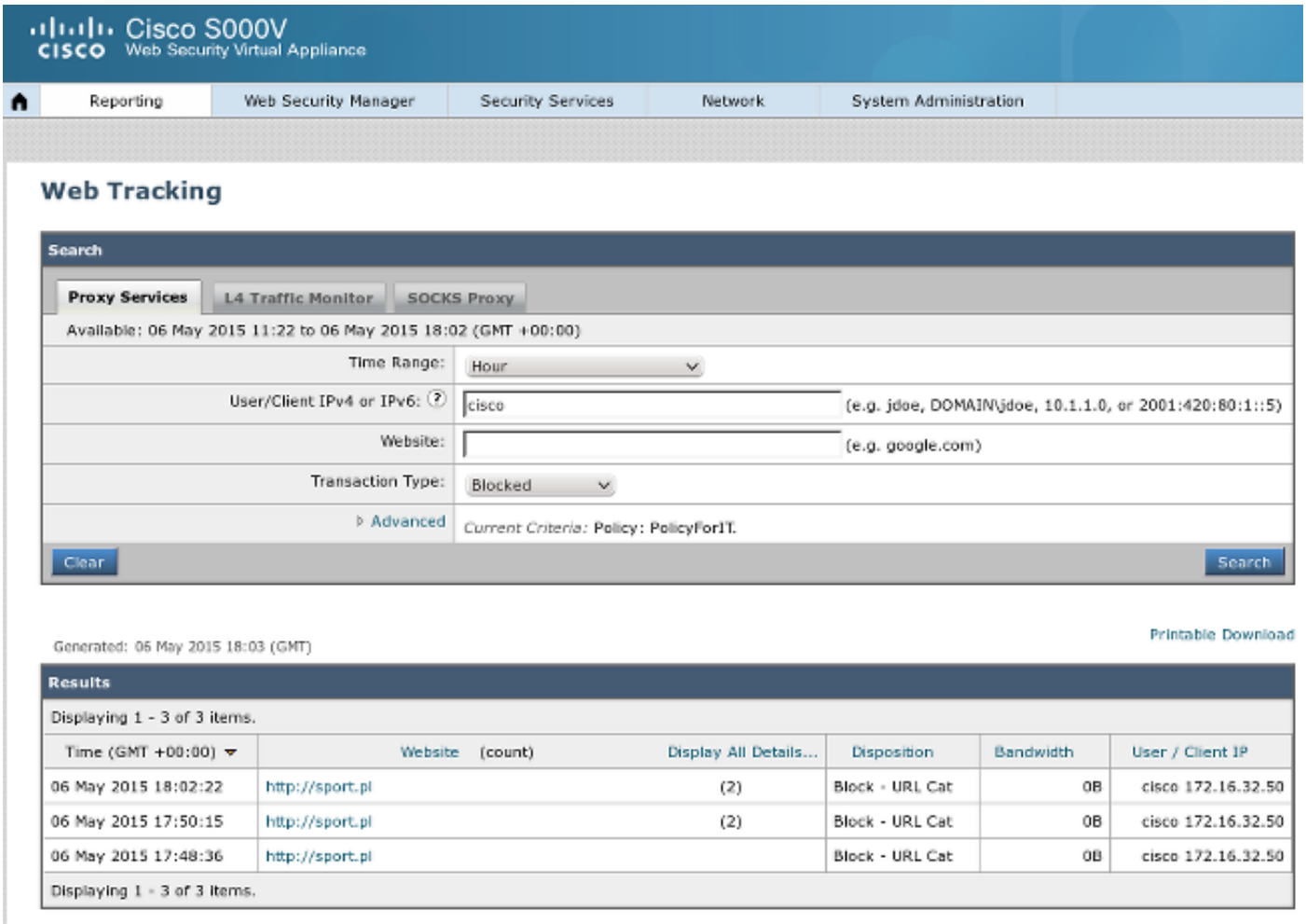
y tunneled en el GRE al WSA (aviso que la router-identificación WCCP es el IP Address más alto configurado):

```
asa-fw# show capture
capture CAP type raw-data interface inside [Capturing - 70065 bytes]
 match gre any any

asa-fw# show capture CAP

525 packets captured

  1: 03:21:45.035657       172.16.33.110 > 172.16.32.204:  ip-proto-47, length 60
  2: 03:21:45.038709       172.16.33.110 > 172.16.32.204:  ip-proto-47, length 48
  3: 03:21:45.039960       172.16.33.110 > 172.16.32.204:  ip-proto-47, length 640
```

El WSA continúa la aceptación decontacto con TCP y procesa la petición get. Como consecuencia, la directiva nombrada PolicyForIT es golpear y se bloquea el tráfico:



Eso es confirmada por el informe WSA:



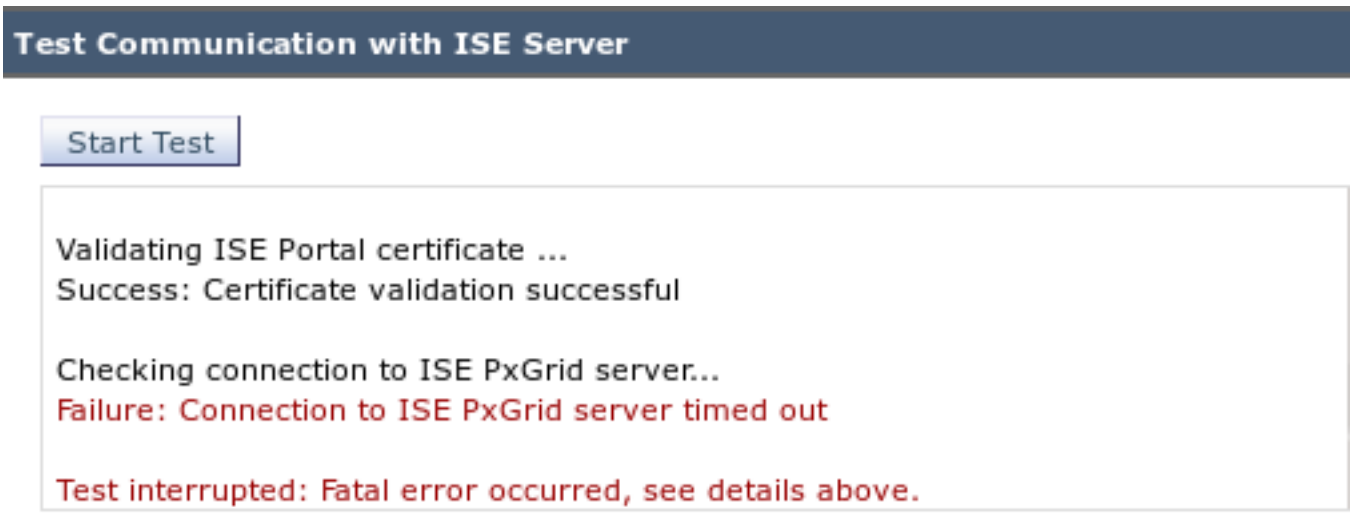
Note que el ISE visualiza el nombre de usuario.

Troubleshooting

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

Certificados incorrectos

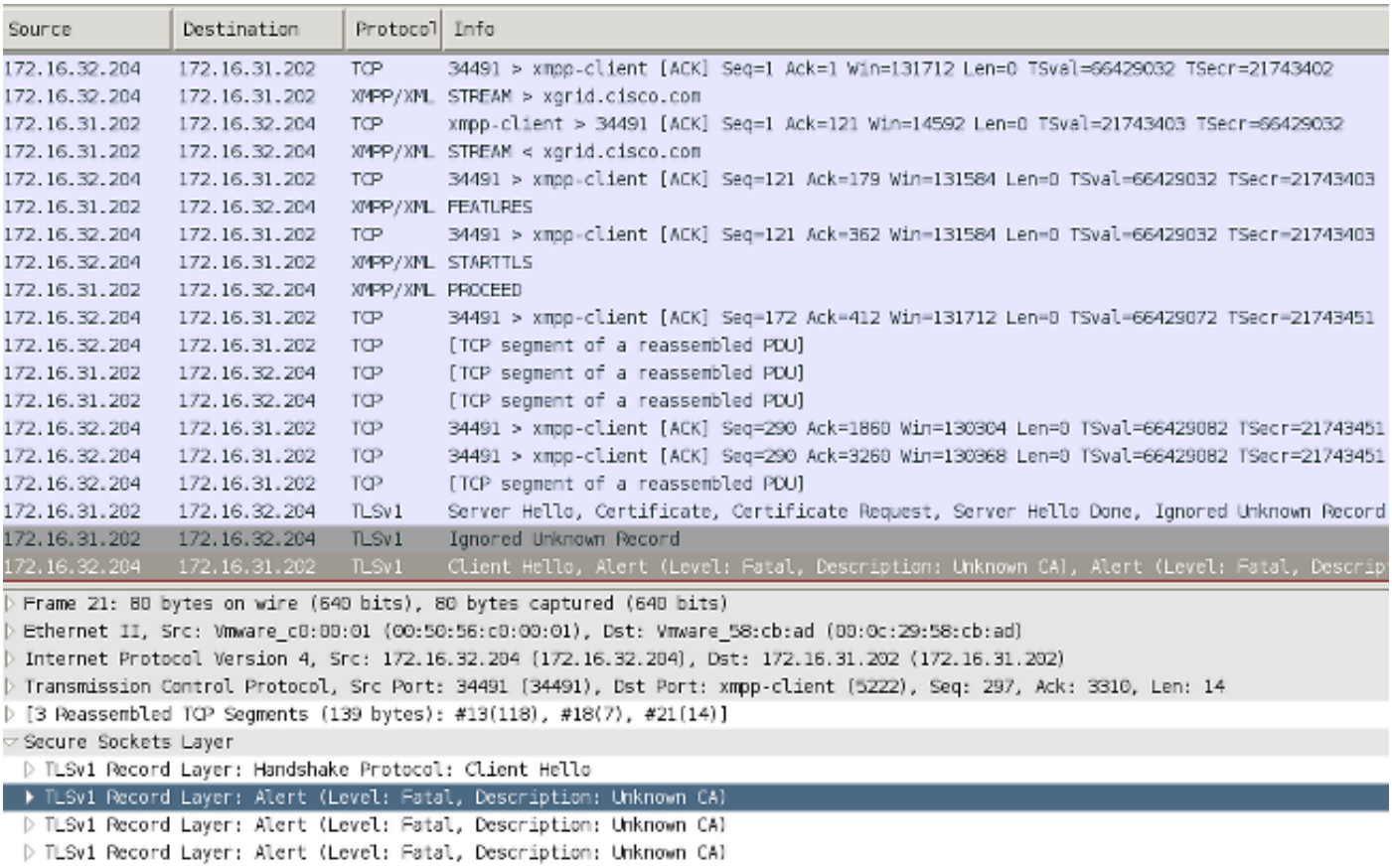
Cuando el WSA no se inicializa correctamente (los Certificados), pruebe para la falla de conexión ISE:



Los informes ISE pxgrid-cm.log:

```
[2015-05-06T16:26:51Z] [INFO ] [cm-1.jabber-172-16-31-202]
[TCPSocketStream::_doSSLHandshake] [] Failure performing SSL handshake: 1
```

La razón del error se puede considerar con Wireshark:



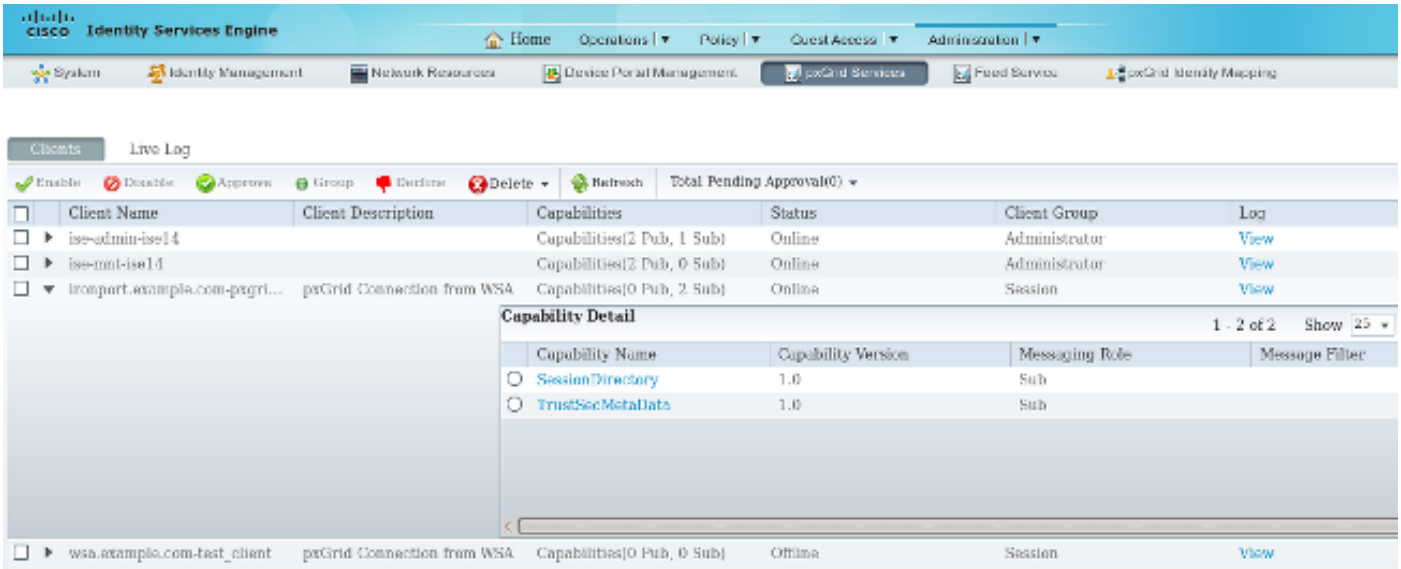
Para una sesión SSL usada para proteger el intercambio extensible de la Mensajería y del protocolo de la presencia (XMPP) (usado por el pxGrid), el error de los informes SSL del cliente debido a una Cadena de certificados desconocida presentada por el servidor.

Escenario correcto

Para el escenario correcto, los registros ISE pxgrid-controller.log:

```
2015-05-06 18:40:09,153 INFO [Thread-7][] cisco.pxgrid.controller.sasl.SaslWatcher
-::::::- Handling authentication for user name wsa.example.com-test_client
```

También, el ISE GUI presenta el WSA como suscriptor con las capacidades correctas:



Información Relacionada

- Postura de la Versión de ASA 9.2.1 VPN con el ejemplo de configuración ISE
- Guía de usuarios WSA 8.7
- ASA y ejemplo de configuración de TrustSec del Catalyst 3750X Series Switch y guía del Troubleshooting
- Guía de configuración del switch de Cisco TrustSec: Comprensión de Cisco TrustSec
- 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