Configurar a integração WSA com o ISE para serviços cientes de TrustSec

Índice

Introdução

Este documento descreve como integrar a ferramenta de segurança da Web (WSA) com Identity Services Engine (ISE). A versão 1.3 ISE apoia um pxGrid chamado API novo. Estes suportes de protocolo modernos e flexíveis autenticação, criptografia, e privilégios (grupos) que permite a fácil

integração com outras soluções da Segurança.

A versão 8.7 WSA apoia o protocolo do pxGrid e pode recuperar a informação de identidade do contexto do ISE. Em consequência, WSA permite que você construa as políticas baseadas nos grupos da etiqueta do grupo de segurança de TrustSec (SGT) recuperados do ISE.

Pré-requisitos

Requisitos

Cisco recomenda que você tem a experiência com configuração de Cisco ISE e conhecimento básico destes assuntos:

- Disposições e configuração de autorização ISE
- Configuração de CLI adaptável da ferramenta de segurança (ASA) para o acesso de TrustSec e VPN
- Configuração WSA
- Compreensão básica de disposições de TrustSec

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Microsoft Windows 7
- Versão de software 1.3 de Cisco ISE e mais atrasado
- Versão 3.1 e mais recente do Mobile Security de Cisco AnyConnect
- Versão ASA 9.3.1 de Cisco e mais atrasado
- Versão 8.7 e mais recente de Cisco WSA

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Configurar

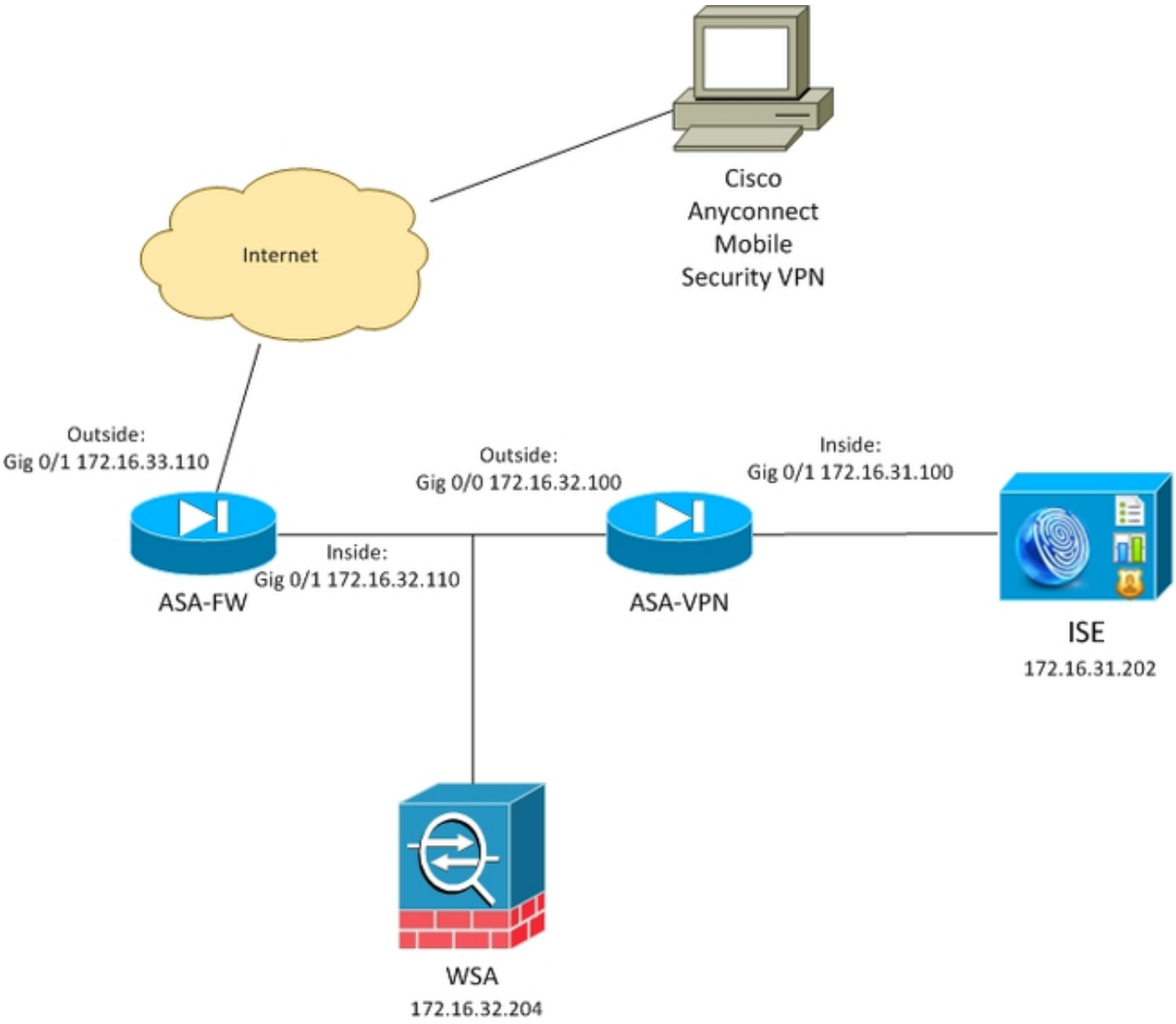
> **Note**: Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

Diagrama da rede e fluxo de tráfego

As etiquetas de TrustSec SGT são atribuídas pelo ISE usado como um Authentication Server para todos os tipos de usuários que alcançam a rede corporativa. Isto envolve prendido/usuários Wireless que autenticam através dos portais do 802.1x ou do convidado ISE. Também, usuários remotos VPN que usam o ISE para a autenticação.

Para WSA, não importa como o usuário alcançou a rede.

Este exemplo apresenta os usuários remotos VPN que terminam a sessão no ASA-VPN. Aqueles usuários foram atribuídos uma etiqueta específica SGT. Todo o tráfego de HTTP ao Internet será interceptado pelo ASA-FW (Firewall) e reorientado ao WSA para a inspeção. O WSA usa o perfil da identidade que permite que classifique os usuários baseados na etiqueta SGT e construa o acesso ou as políticas de descriptografia baseado naquele.



O fluxo detalhado é:

1. O usuário de AnyConnect VPN termina a sessão do secure sockets layer (SSL) no ASA-VPN. O ASA-VPN é configurado para TrustSec e usa o ISE para a autenticação de usuários do VPN. O usuário autenticado é atribuído um valor da etiqueta SGT = 2 (name= a TI). O usuário recebe um endereço IP de Um ou Mais Servidores Cisco ICM NT da rede 172.16.32.0/24 (172.16.32.50 neste exemplo).
2. O usuário tenta alcançar o página da web no Internet. O ASA-FW é configurado para o Protocolo de Comunicação de Cache da Web (WCCP) que reorienta o tráfego ao WSA.
3. O WSA é configurado para a integração ISE. Usa o pxGrid a fim transferir a informação do ISE: o IP address 172.16.32.50 do usuário foi atribuído a etiqueta 2. SGT.

4. O WSA processa o pedido do HTTP do usuário e bate a política de acesso PolicyForIT. Que a política está configurada para obstruir o tráfego aos locais dos esportes. Todos usuários restantes (que não pertencem a SGT 2) batem a política de acesso do padrão e têm o acesso direto aos locais dos esportes.

ASA-VPN

Este é um gateway de VPN configurado para TrustSec. A configuração detalhada é fora do espaço deste documento. Refira estes exemplos:

- O ASA e o exemplo de configuração de TrustSec do Catalyst 3750X Series Switch e pesquisam defeitos o guia
- Exemplo de configuração da classificação e da aplicação da versão ASA 9.2 VPN SGT

ASA-FW

O Firewall ASA é responsável para o redirecionamento de WCCP ao WSA. Este dispositivo não está ciente de TrustSec.

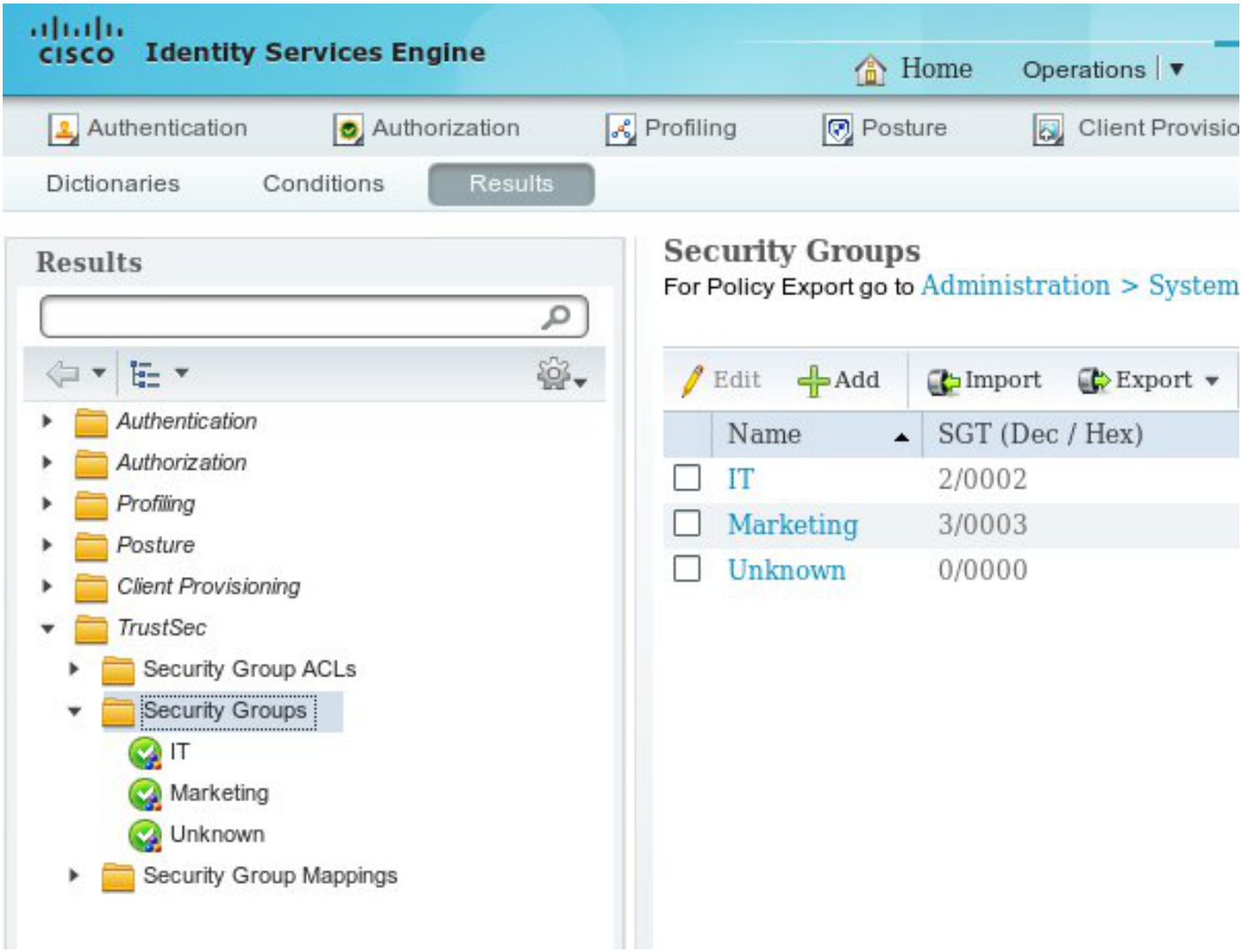
```
interface GigabitEthernet0/0
 nameif outside
 security-level 100
 ip address 172.16.33.110 255.255.255.0

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

O ISE é um ponto central no desenvolvimento de TrustSec. Atribui etiquetas SGT a todos os usuários que alcançam e autenticam à rede. As etapas exigidas para a configuração básica são alistadas nesta seção.

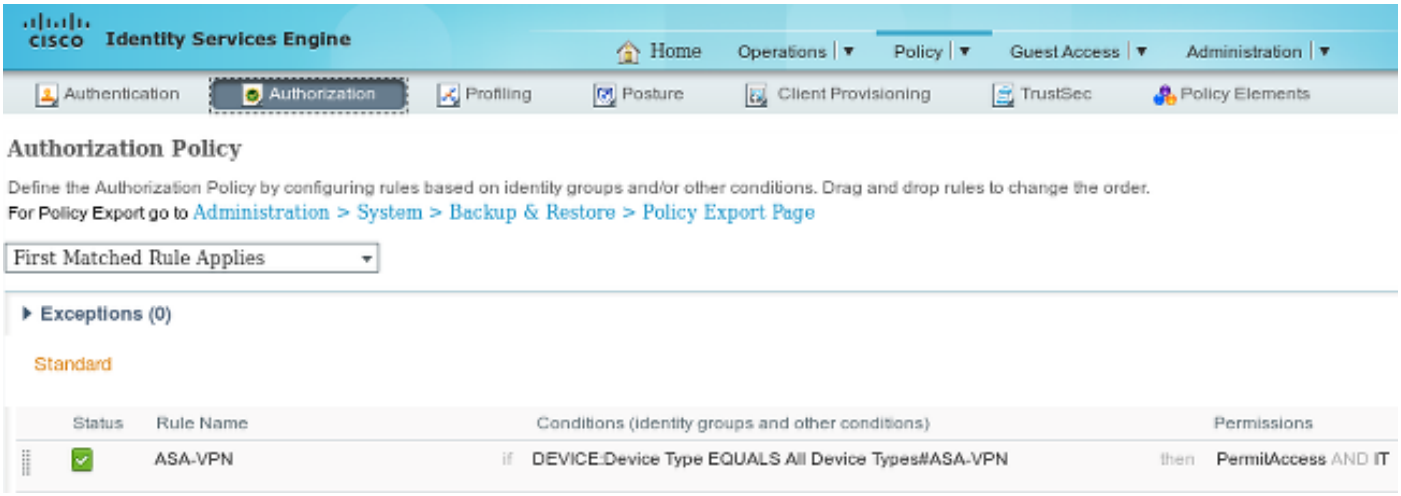
Etapa 1. SGT para o TI e o outro grupo

Escolha **grupos do > segurança do acesso do grupo do > segurança da política > dos resultados** e crie o SGT:



Etapa 2. Regra da autorização para o acesso VPN que atribui SGT = 2 (a TI)

Escolha a **política > a autorização** e crie uma regra para o acesso remoto VPN. Todas as conexões de VPN estabelecidas através de ASA-VPN obterão o acesso direto (PermitAccess) e serão atribuídas a etiqueta 2 SGT (a TI).



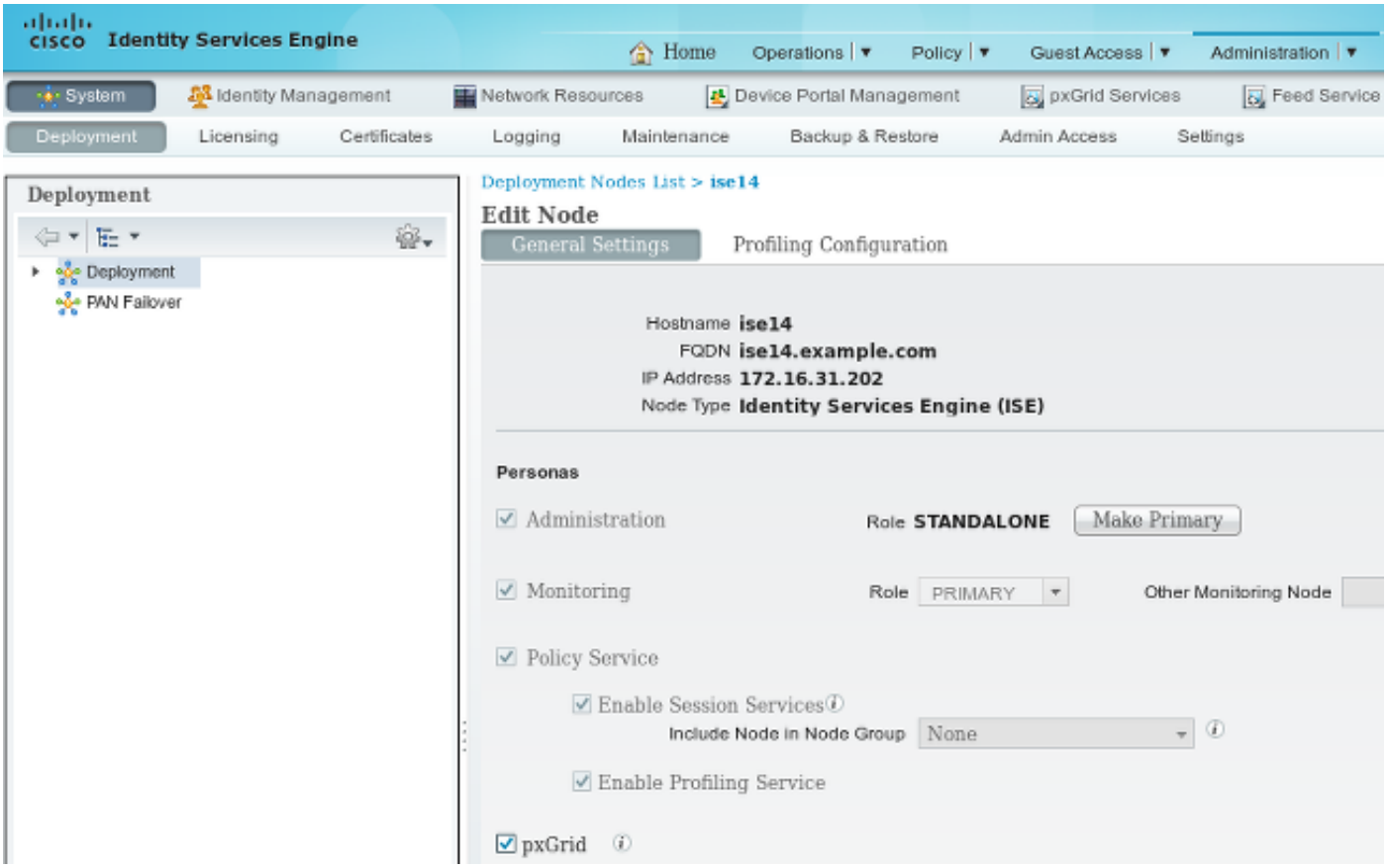
Etapa 3. Adicionar o dispositivo de rede e gerencia o arquivo PAC para ASA-VPN

A fim adicionar o ASA-VPN ao domínio de TrustSec, é necessário gerar arquivo da configuração do proxy o auto (PAC) manualmente. Esse arquivo será importado no ASA.

Isso pode ser configurado da **administração > dos dispositivos de rede**. Depois que o ASA é adicionado, enrole para baixo ajustes de TrustSec e gerencia o arquivo PAC. Os detalhes para aquele são descritos em um documento (provido) separado.

Etapa 4. Permita o papel do pxGrid

Escolha a **administração > o desenvolvimento** a fim permitir o papel do pxGrid.



Etapa 5. Gerencia o certificado para a administração e o papel do pxGrid

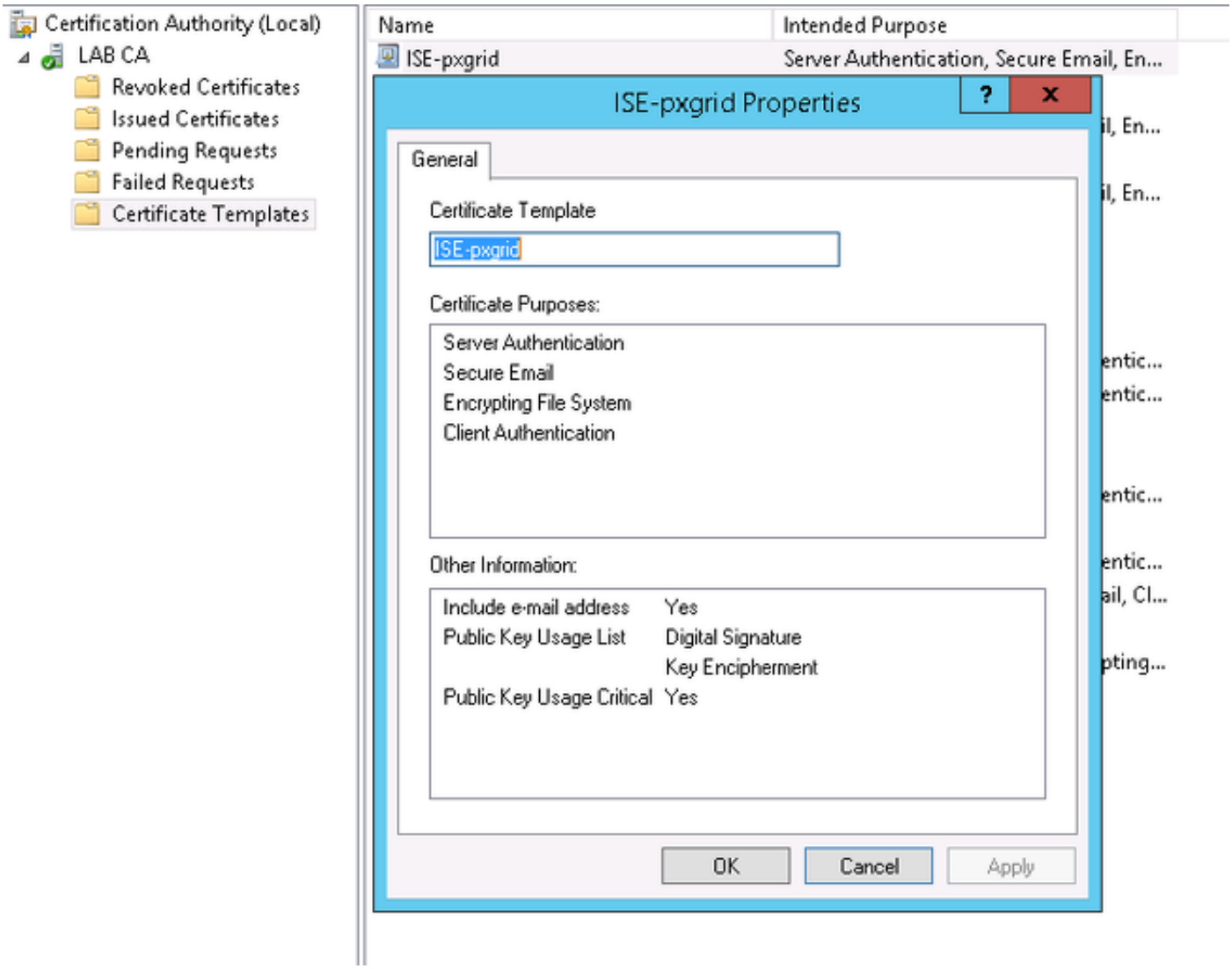
O protocolo do pxGrid usa o certificado de autenticação para o cliente e o server. É muito importante configurar os Certificados corretos para o ISE e o WSA. Ambos os Certificados devem incluir o nome de domínio totalmente qualificado (FQDN) no assunto e os Ramais x509 para a authenticação do cliente e a autenticação de servidor. Também, certifique-se que o registro correto DNS A está criado para o ISE e o WSA e combina o FQDN correspondente.

Se ambos os Certificados são assinados por um Certificate Authority (CA) diferente, é importante incluir aqueles CA na loja confiada.

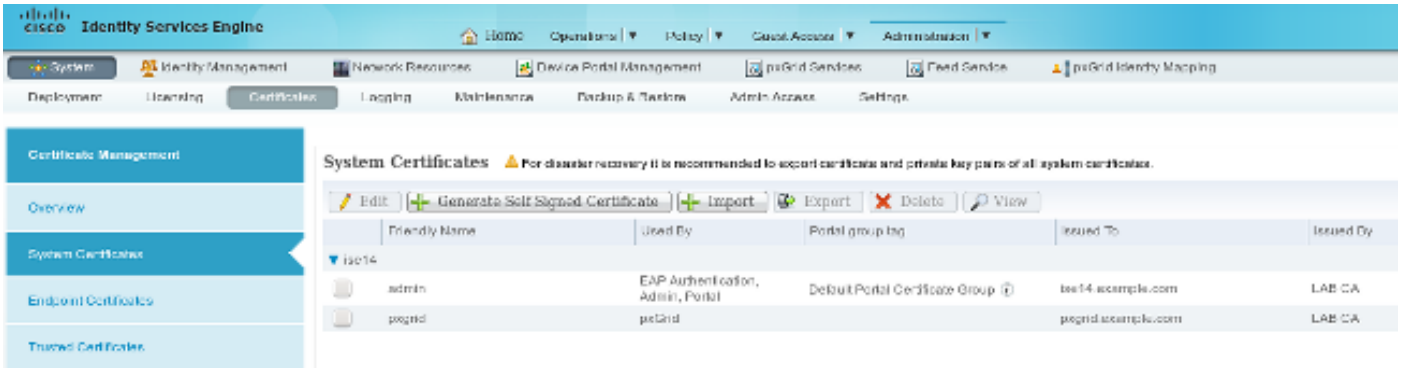
A fim configurar Certificados, escolha a **administração > Certificados**.

O ISE pode gerar uma solicitação de assinatura de certificado (CSR) para cada papel. Para o papel do pxGrid, a exportação e assina o CSR com CA externo.

Neste exemplo, Microsoft CA foi usado com este molde:



O resultado final pôde olhar como:

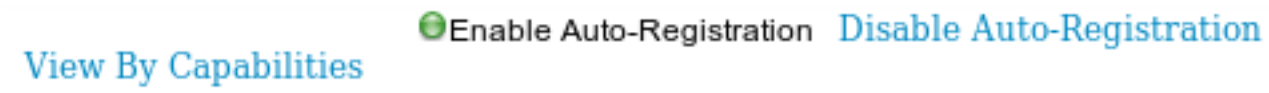


Não esqueça criar os registros DNS A para ise14.example.com e pxgrid.example.com que apontam a 172.16.31.202.

Registro automático do pxGrid de etapa 6.

Àrevelia, o ISE não registrará automaticamente assinantes do pxGrid. Isso deve manualmente ser aprovado pelo administrador. Esse ajuste deve ser mudado para a integração WSA.

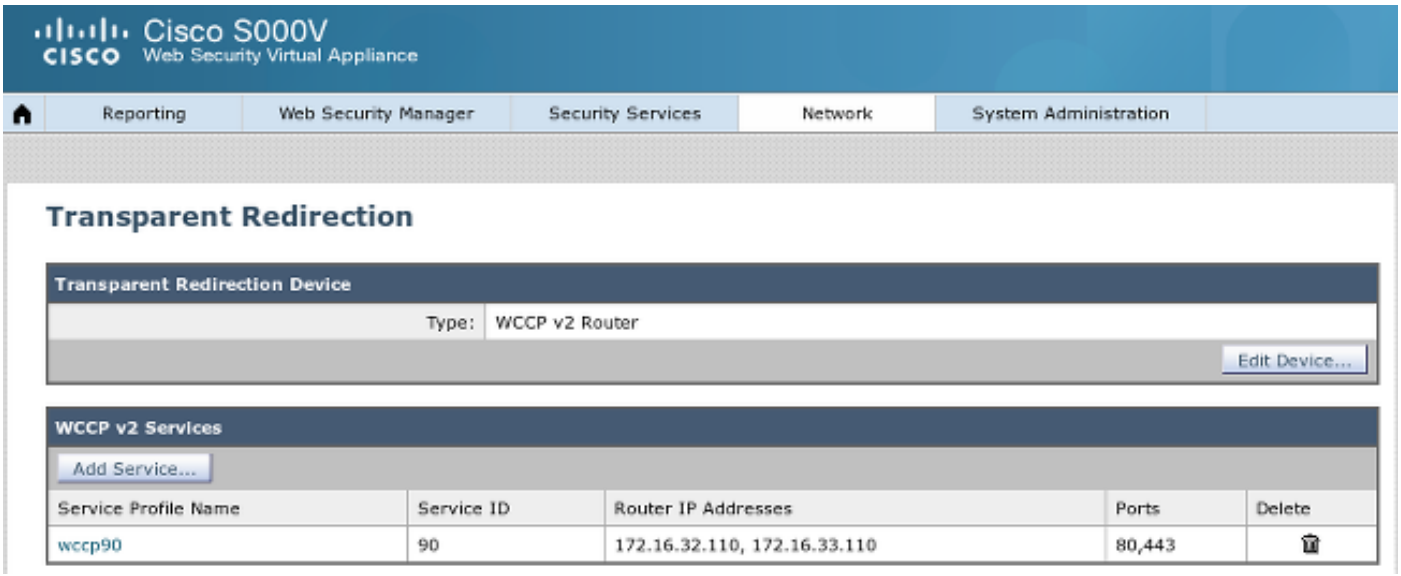
Escolha **serviços da administração > do pxGrid** e o grupo **permite o registro automático**.



WSA

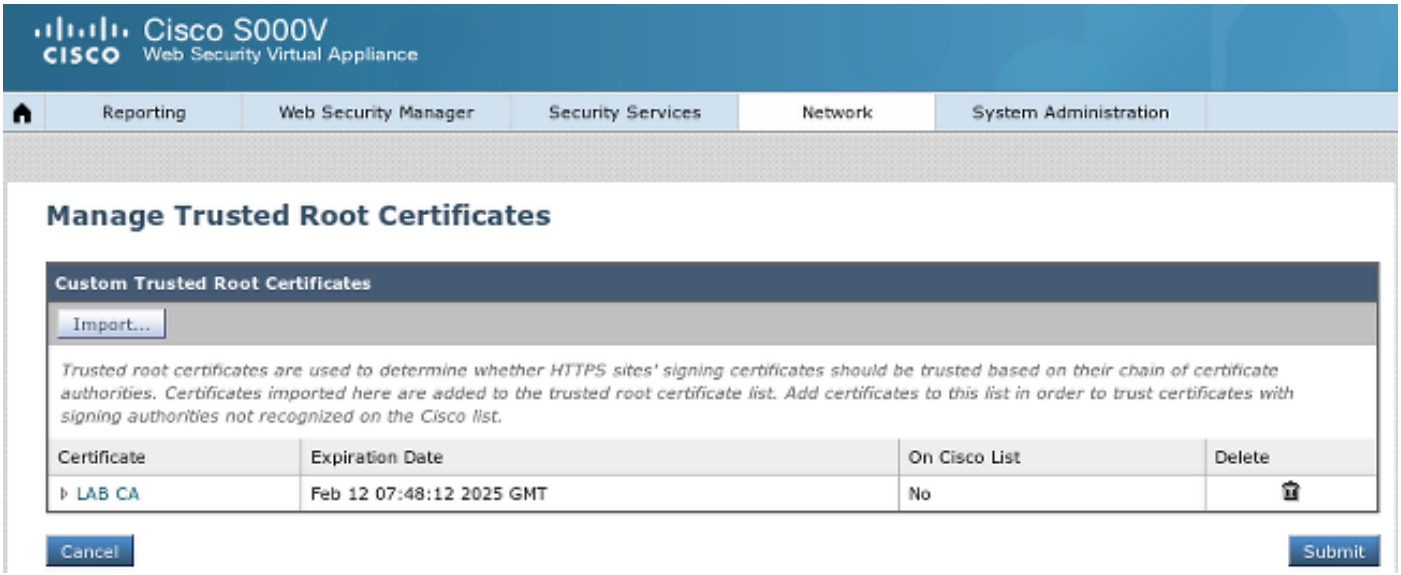
Etapa 1. Modo transparente e reorientação

Neste exemplo, o WSA é configurado com apenas a interface de gerenciamento, o modo transparente, e a reorientação do ASA:



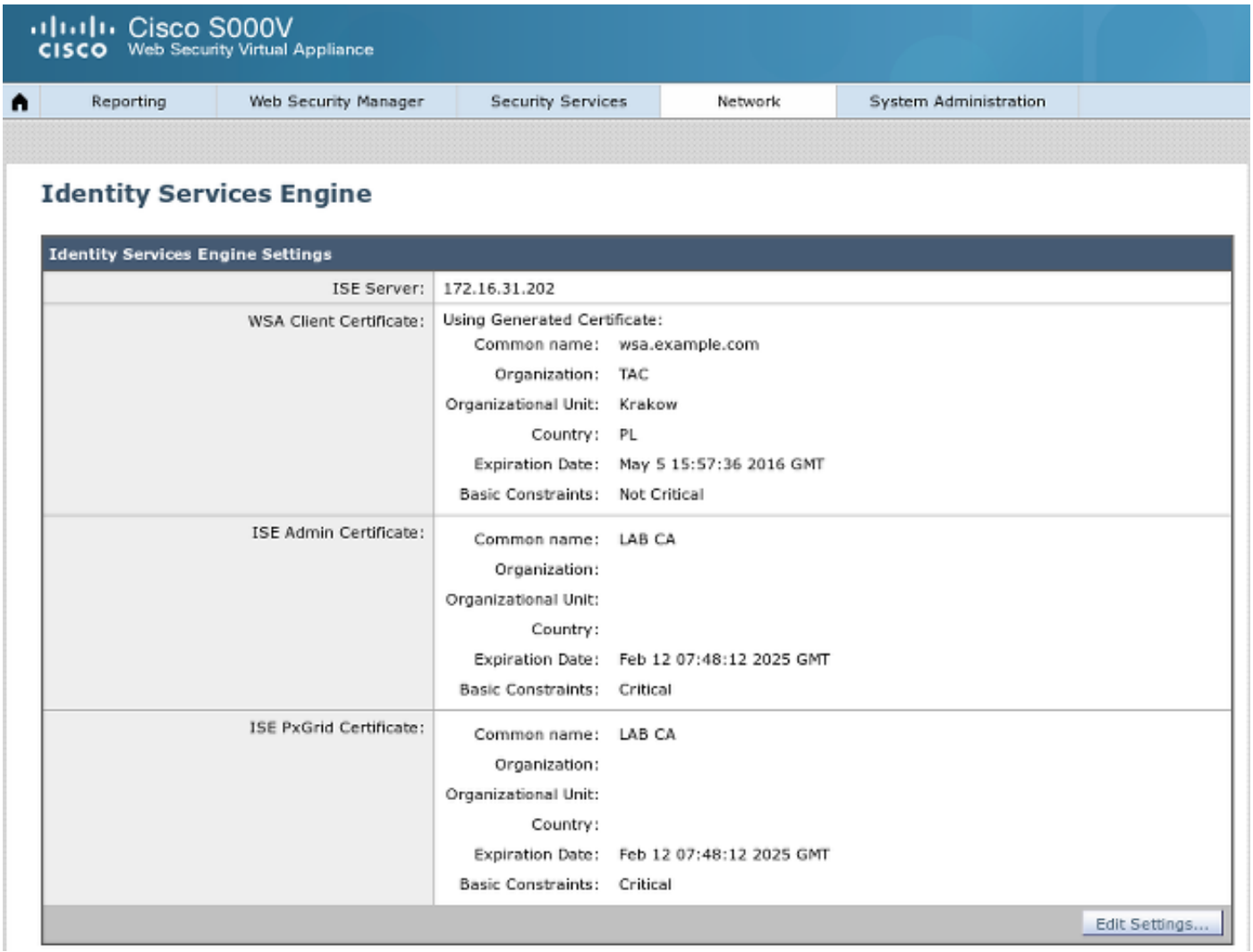
Etapa 2. Geração do certificado

O WSA precisa de confiar CA para assinar todos os Certificados. Escolha o **> gerenciamento de certificado da rede** a fim adicionar um certificado de CA:



Éigualmente necessário gerar um certificado que o WSA se usará a fim autenticar ao pxGrid. Escolha a **rede > o Identity Services Engine > o certificado de cliente WSA** a fim gerar o CSR, assine-o com o molde correto de CA (ISE-pxgrid), e importe-o para trás.

Também, para “o certificado ISE Admin” e “o certificado do pxGrid ISE”, importe o certificado de CA (a fim confiar o certificado do pxGrid apresentado pelo ISE):

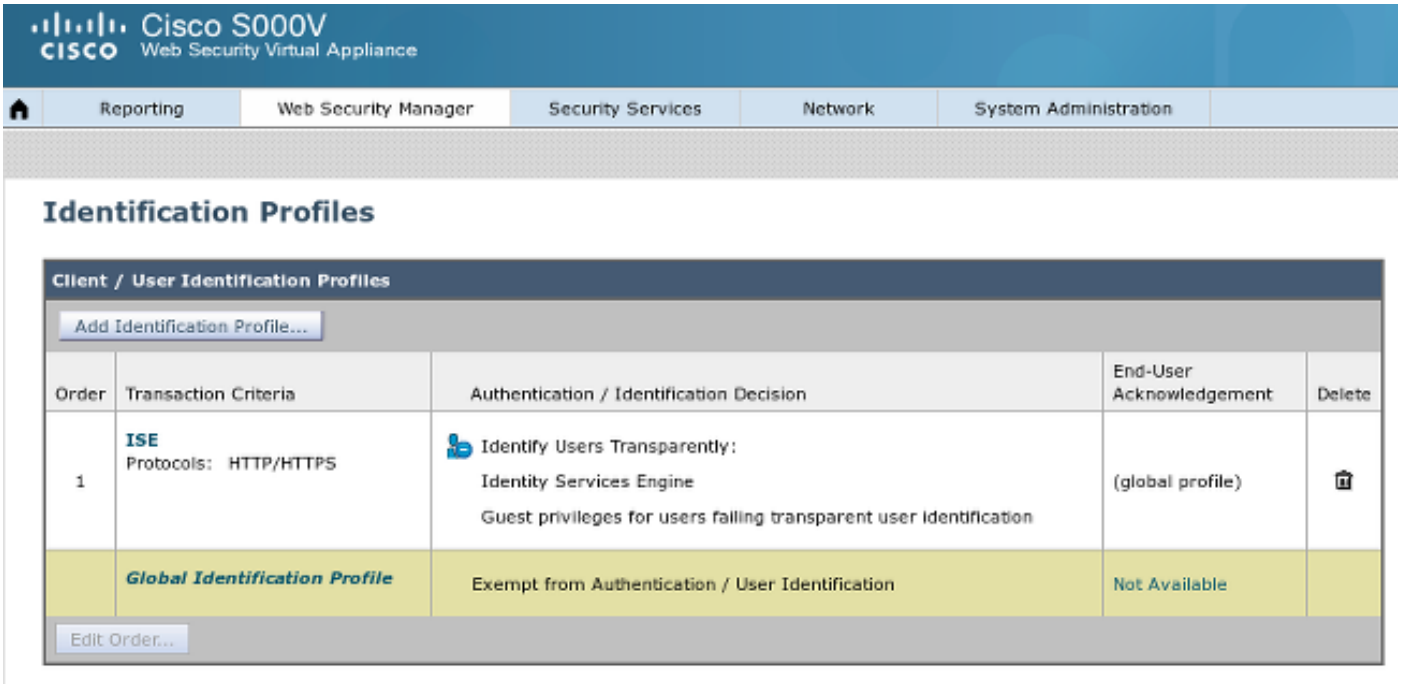


Etapa 3. Teste a Conectividade ISE

Escolha a **rede > o Identity Services Engine** a fim testar a conexão ao ISE:

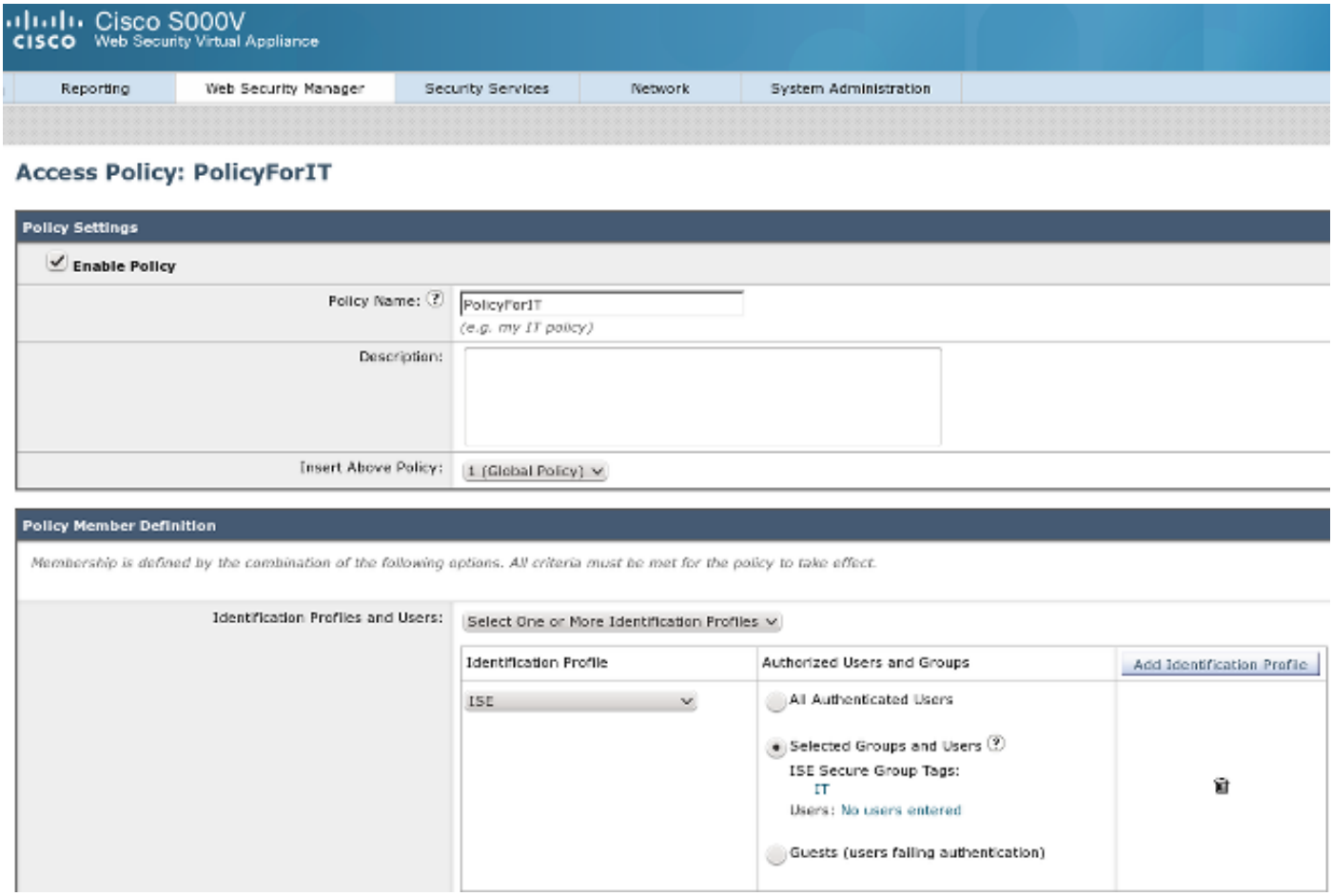
Etapa 4. Perfis da identificação ISE

Escolha **perfis do gerenciador de segurança > da identificação da Web** a fim adicionar um perfil novo para o ISE. Para da "" o uso "*identificação e da autenticação identifique transparentemente usuários com ISE".*

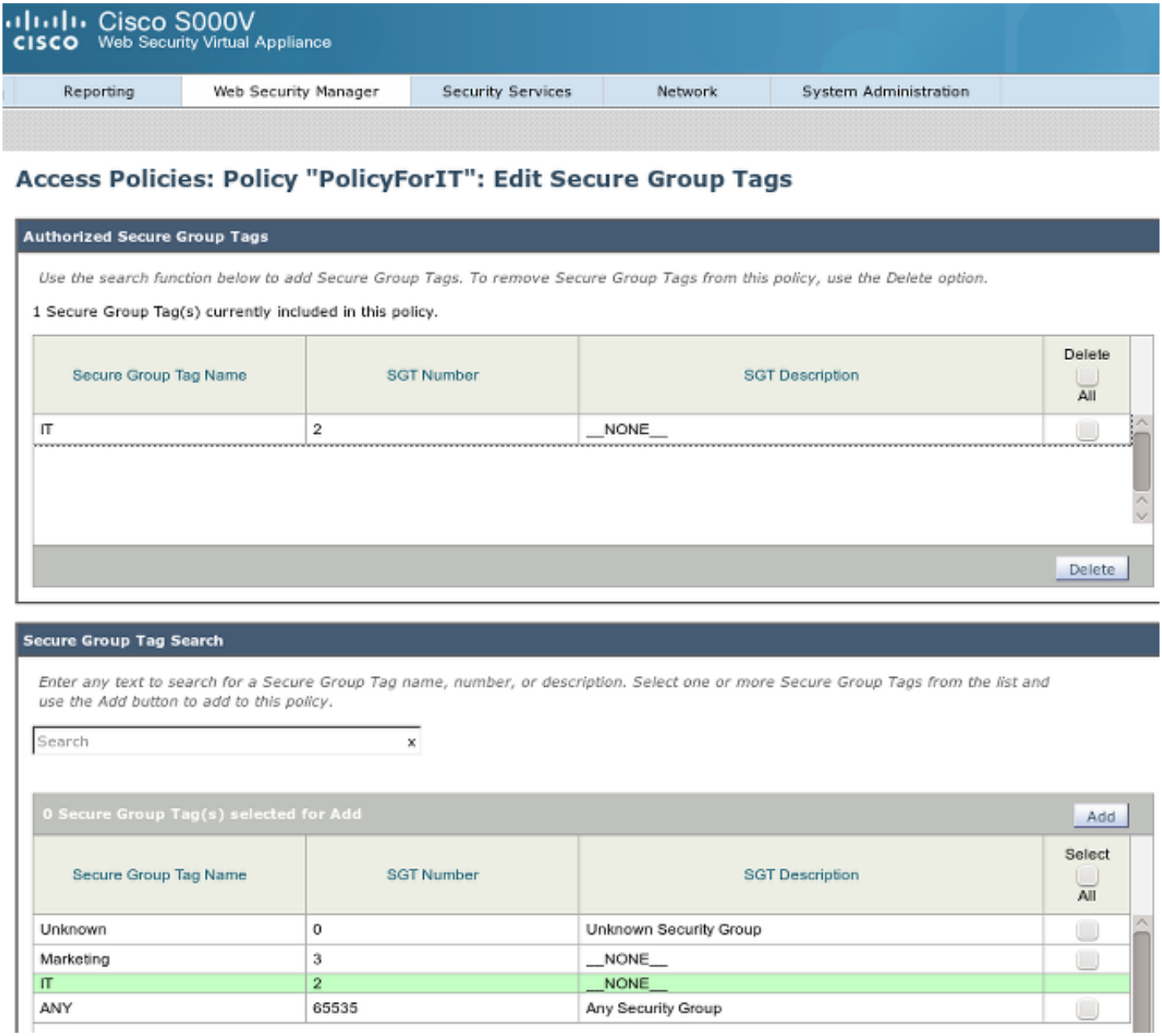


Etapa 5. Alcance a política baseada na etiqueta SGT

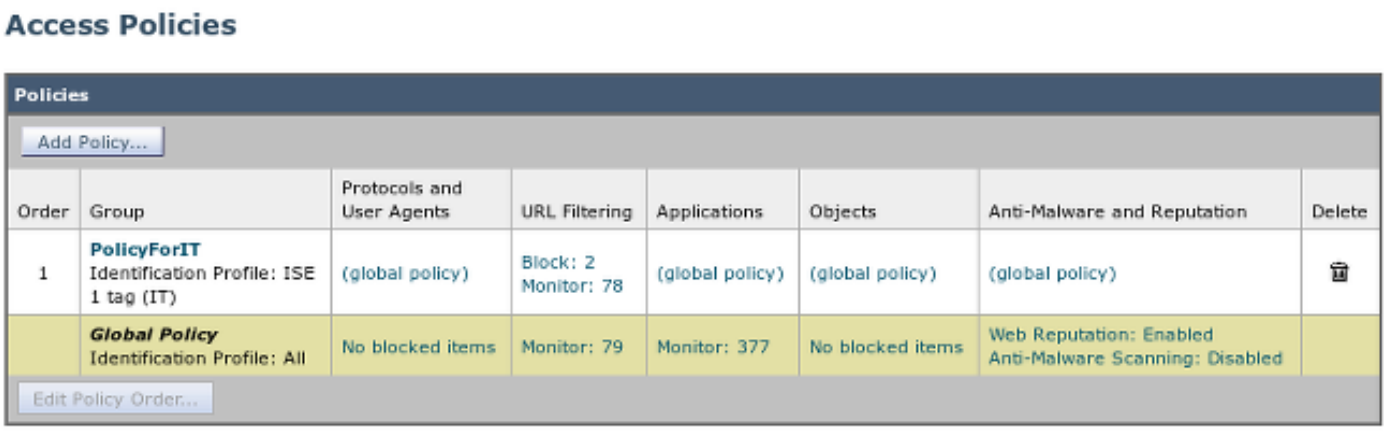
Escolha o **gerenciador de segurança > as políticas de acesso da Web** a fim adicionar uma política nova. A sociedade usa o perfil ISE:



Para grupos e usuários selecionados a etiqueta 2 SGT será adicionada (a TI):



A política nega o acesso a todos os locais dos esportes para os usuários que pertencem a SGT A TI:

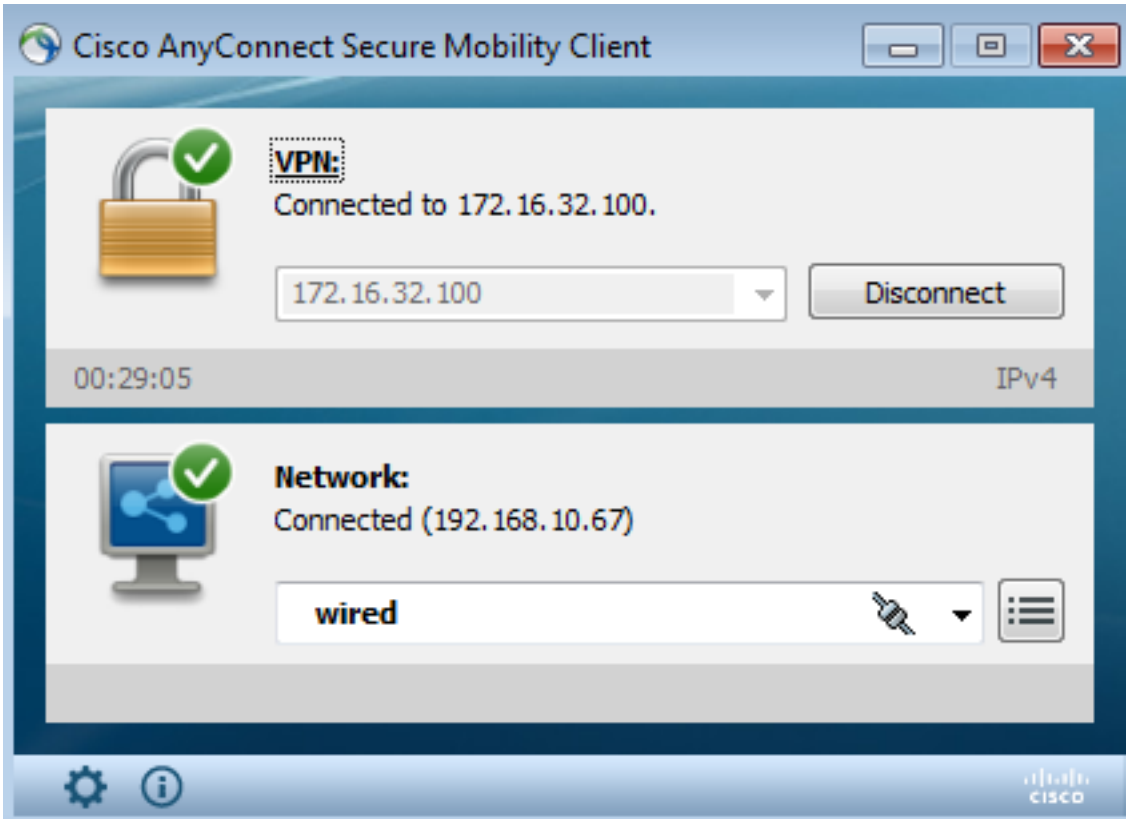


Verificar

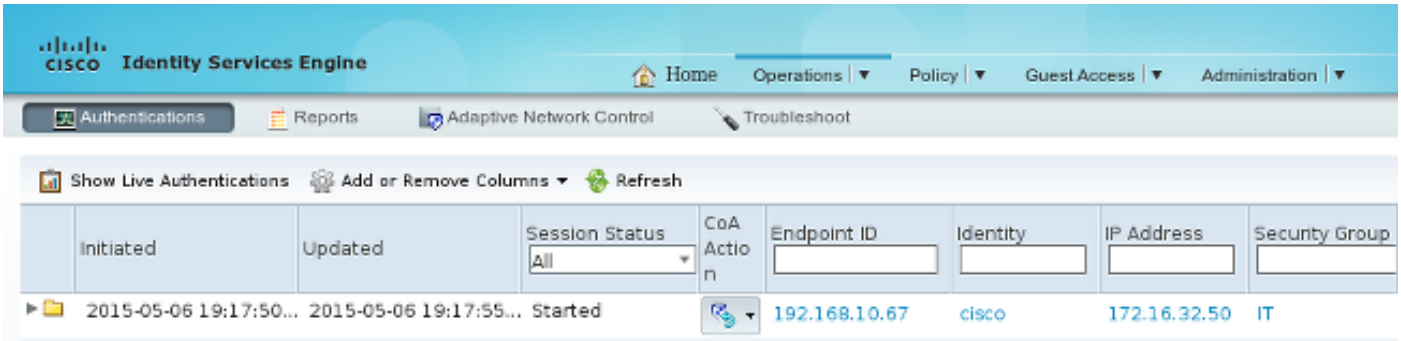
Use esta seção para confirmar se a sua configuração funciona corretamente.

Etapa 1. Sessão de VPN

O usuário VPN inicia uma sessão de VPN para o ASA-VPN:



O ASA-VPN usa o ISE para a autenticação. O ISE cria uma sessão e atribui a etiqueta 2 SGT (a TI):



Após a autenticação bem sucedida, o ASA-VPN cria uma sessão de VPN com a etiqueta 2 SGT (retornada na aceitação de acesso do raio no 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
```

Desde que o link entre o ASA-VPN e o ASA-FW não é TrustSec permitido, o ASA-VPN envia frames sem etiqueta para esse tráfego (não possa ao GRE encapsulam frames da Ethernet com o campo CMD/TrustSec injetado).

Etapa 2. Informação de sessão recuperada pelo WSA

Nesta fase, o WSA deve receber o mapeamento entre o endereço IP de Um ou Mais Servidores Cisco ICM NT, o username, e o SGT (através do protocolo do 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
[]>
```

Etapa 3. Reorientação do tráfego ao WSA

O usuário VPN inicia uma conexão a sport.pl, que é interceptado pelo ASA-FW:

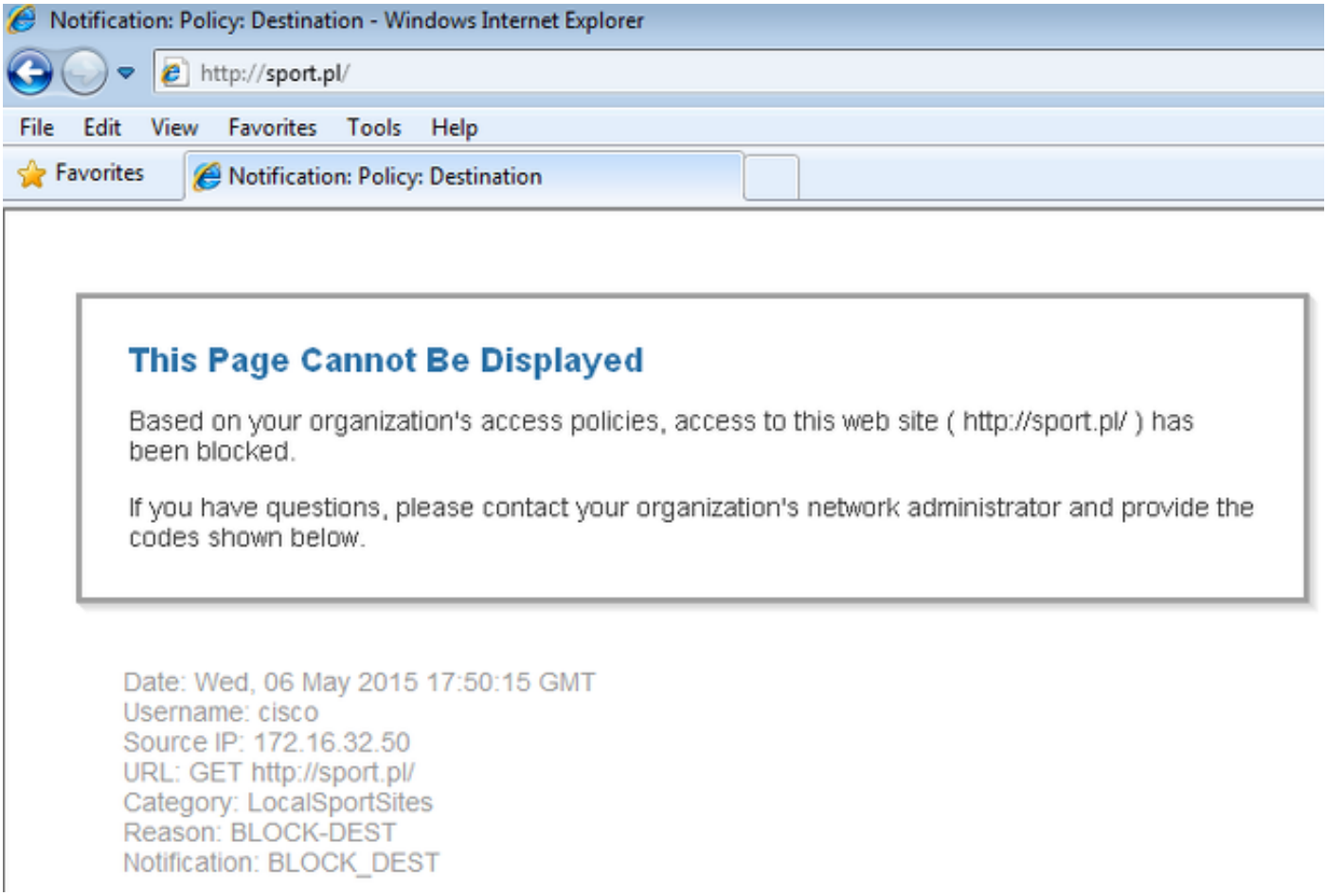
```
asa-fw# show wccp

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
```

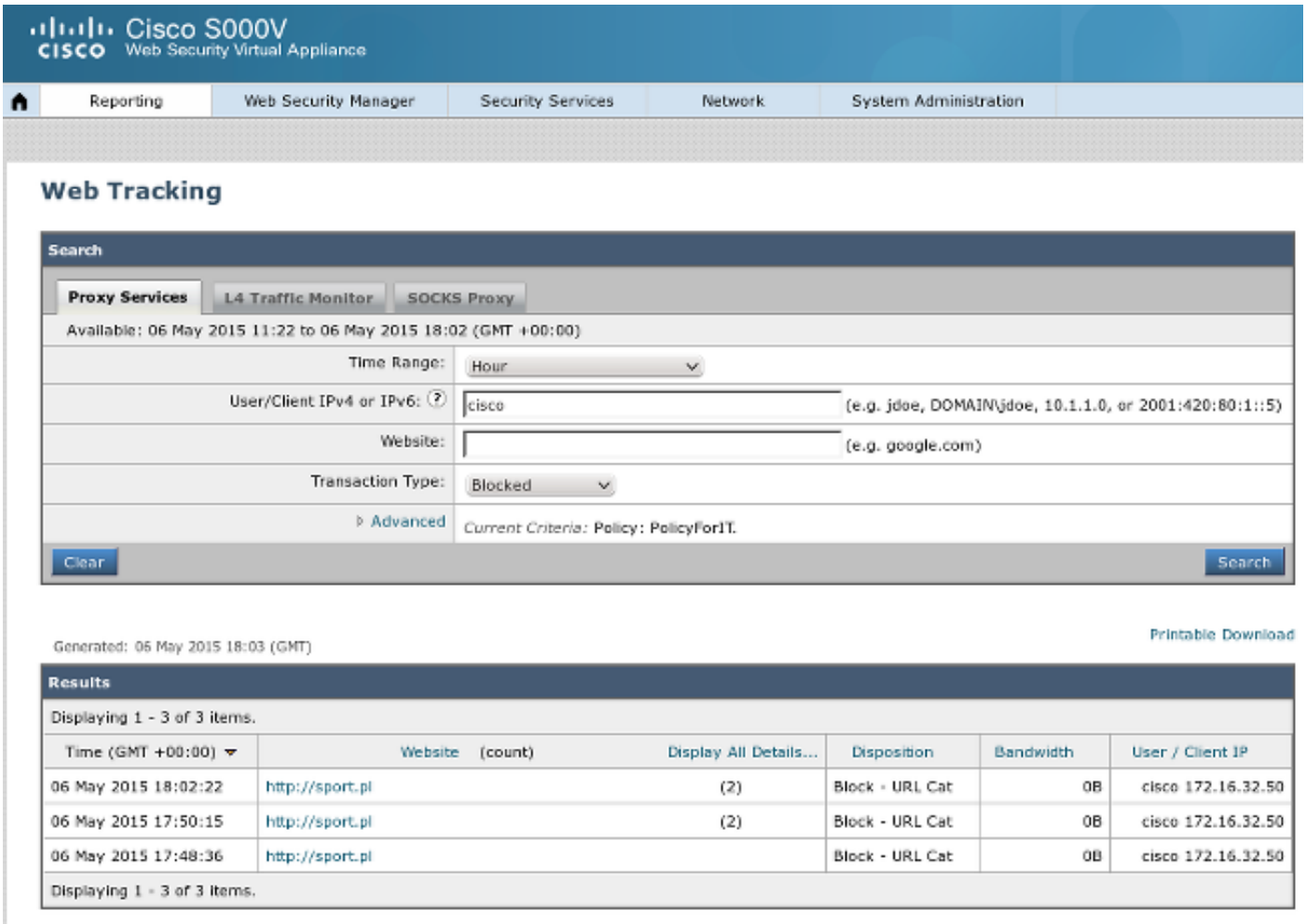
e escavado um túnel no GRE ao WSA (observação que a roteador-identificação WCCP é o endereço IP de Um ou Mais Servidores Cisco ICM NT o mais alto configurado):

```
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
```

O WSA continua o cumprimento de TCP e processa o pedido GET. Em consequência, a política nomeada PolicyForIT é bater e o tráfego é obstruído:



Isso é confirmado pelo relatório WSA:



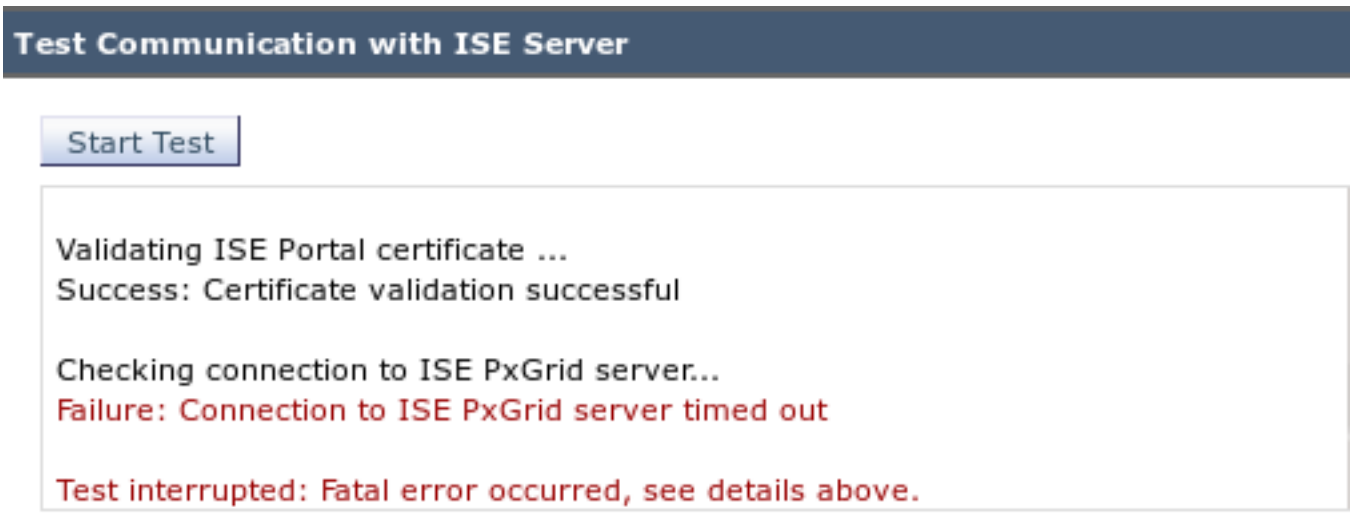
Observe que o ISE indica o username.

Troubleshooting

Esta seção fornece a informação que você pode se usar a fim pesquisar defeitos sua configuração.

Certificados incorretos

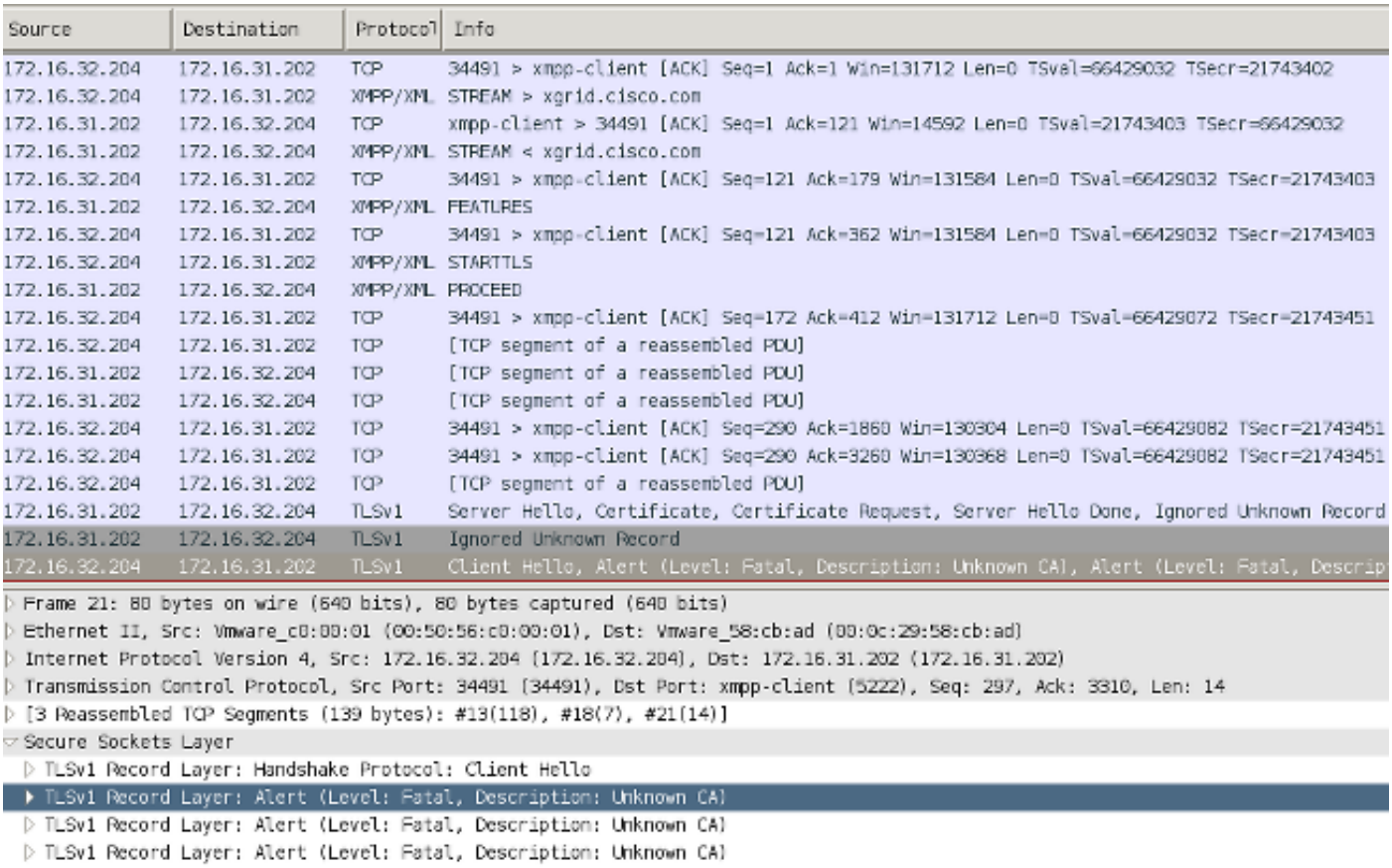
Quando o WSA não estiver inicializado corretamente (Certificados), teste para a falha de conexão ISE:



Os relatórios ISE pxgrid-cm.log:

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

A razão para a falha pode ser considerada com Wireshark:



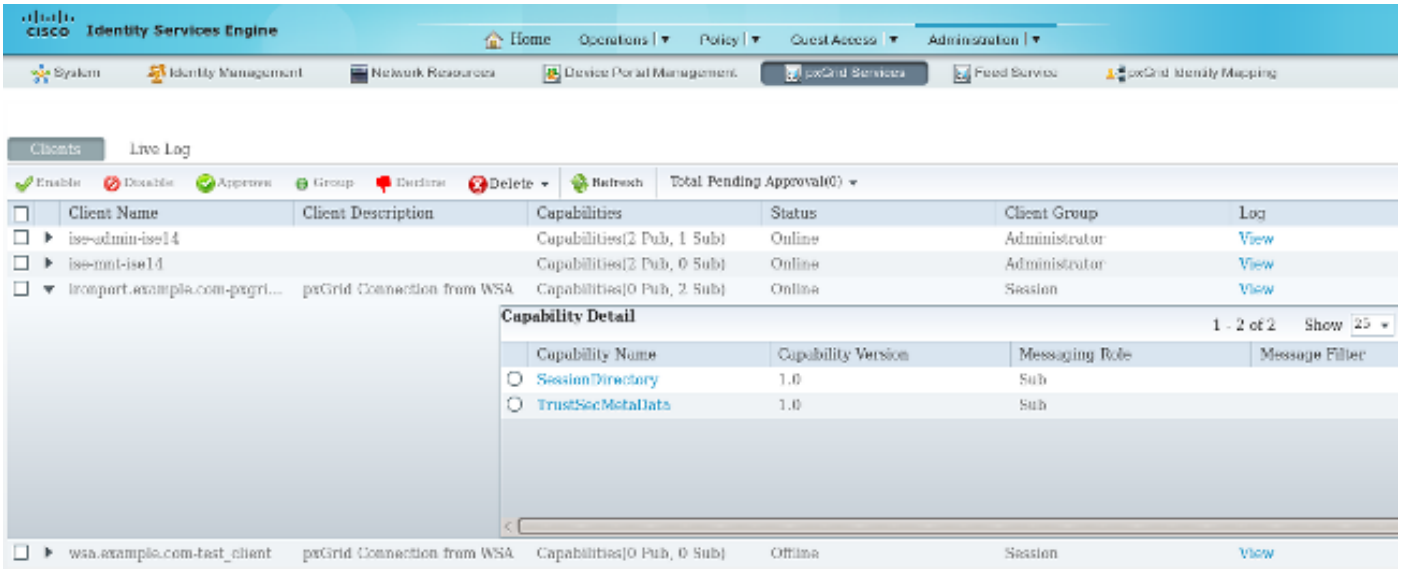
Para uma sessão de SSL usada para proteger a troca elástico do protocolo da Mensagem e da presença (XMPP) (usada pelo pxGrid), a falha dos relatórios SSL do cliente devido a um certificate chain desconhecido apresentado pelo server.

Encenação correta

Para a encenação correta, os logs 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
```

Também, o ISE GUI apresenta o WSA como um subscritor com as capacidades corretas:



Informações Relacionadas

- Postura da versão ASA 9.2.1 VPN com exemplo de configuração ISE
- Guia de usuários WSA 8.7
- O ASA e o exemplo de configuração de TrustSec do Catalyst 3750X Series Switch e pesquisam defeitos o guia
- Guia de configuração de switch de Cisco TrustSec: Compreendendo Cisco TrustSec
- Configurando um servidor interno para a autorização de usuário da ferramenta de segurança
- Guia de configuração de CLI da série VPN de Cisco ASA, 9.1
- Guia do Usuário do Cisco Identity Services Engine, liberação 1.2
- Suporte Técnico e Documentação - Cisco Systems