配置与ISE的WSA集成TrustSec意识服务的

目录

简介

本文描述如何集成Web安全工具(WSA)用身份服务引擎(ISE)。ISE版本1.3支持一新的API呼叫的pxGrid。允许与其他安全问题解决方案的容易集成的此现代和灵活协议支持验证、加密和权限(组)。

WSA版本8.7支持pxGrid协议并且能从ISE获取上下文身份信息。结果， WSA允许您建立根据

TrustSec安全组标记(SGT)组的策略检索从ISE。

先决条件

要求

思科建议您有与思科ISE这些主题配置和基础知识的体验：

- ISE部署和授权配置
- TrustSec和VPN访问的可适应安全工具(ASA) CLI配置
- WSA配置
- TrustSec部署基本的了解

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Microsoft Windows 7
- Cisco ISE软件版本1.3及以后
- Cisco AnyConnect移动安全版本3.1和以上
- Cisco ASA版本9.3.1和以上
- Cisco WSA版本8.7和以上

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

配置

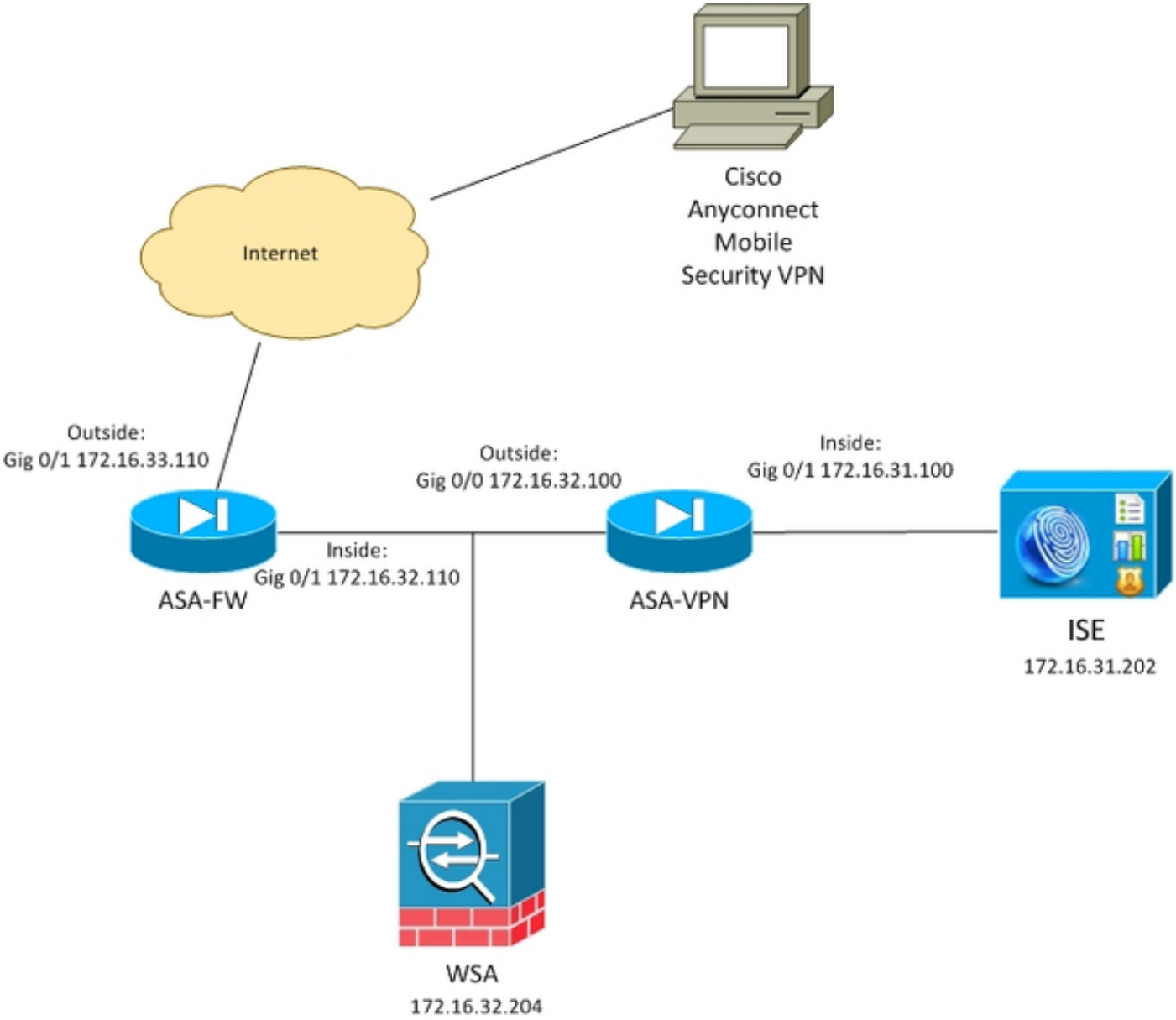
> **Note**:使用命令查找工具（仅限注册用户）可获取有关本部分所使用命令的详细信息。

网络图和通信流

TrustSec SGT标记由作为认证服务器的ISE分配用于访问公司网络用户的所有类型。这涉及通过802.1x或ISE访客门户验证的有线的/无线用户。并且，使用ISE验证的远程VPN用户。

对于WSA，不重要用户如何访问网络。

此示例提交终止ASA-VPN的远程VPN用户会话。那些用户分配特定SGT标记。对互联网的所有HTTP数据流将被ASA-FW (防火墙)拦截并且重定向对检查的WSA。WSA使用允许它分类根据SGT标记的用户和建立根据那的访问或解密策略的标识配置文件。



详细的流是：

1. AnyConnect VPN用户终止ASA-VPN的安全套接字协议层(SSL)会话。ASA-VPN为TrustSec配置并且使用ISE VPN用户的验证。已认证的用户分配SGT标记value= 2 (name= IT)。用户收到从172.16.32.0/24网络(在本例中的172.16.32.50的一个IP地址)。
2. 用户在互联网里设法访问网页。重定向流量对WSA的ASA-FW为WEB缓存通信协议(WCCP)配置。
3. WSA为ISE集成配置。它使用pxGrid为了下载从ISE的信息：用户IP地址172.16.32.50分配SGT标记2。
4. WSA处理从用户的HTTP请求并且点击访问策略PolicyForIT。该策略配置阻塞流量到运动站点。不属于SGT 2)点击默认访问策略并且有对运动站点的完全权限的其他用户(。

ASA-VPN

这是为TrustSec配置的VPN网关。详细配置是出于范围本文。参考这些示例：

- ASA和Catalyst 3750X系列交换机TrustSec配置示例和排除故障指南
- ASA版本9.2 VPN SGT分类和执行配置示例

ASA-FW

ASA防火墙对WCCP重定向负责对WSA。此设备不知道TrustSec。

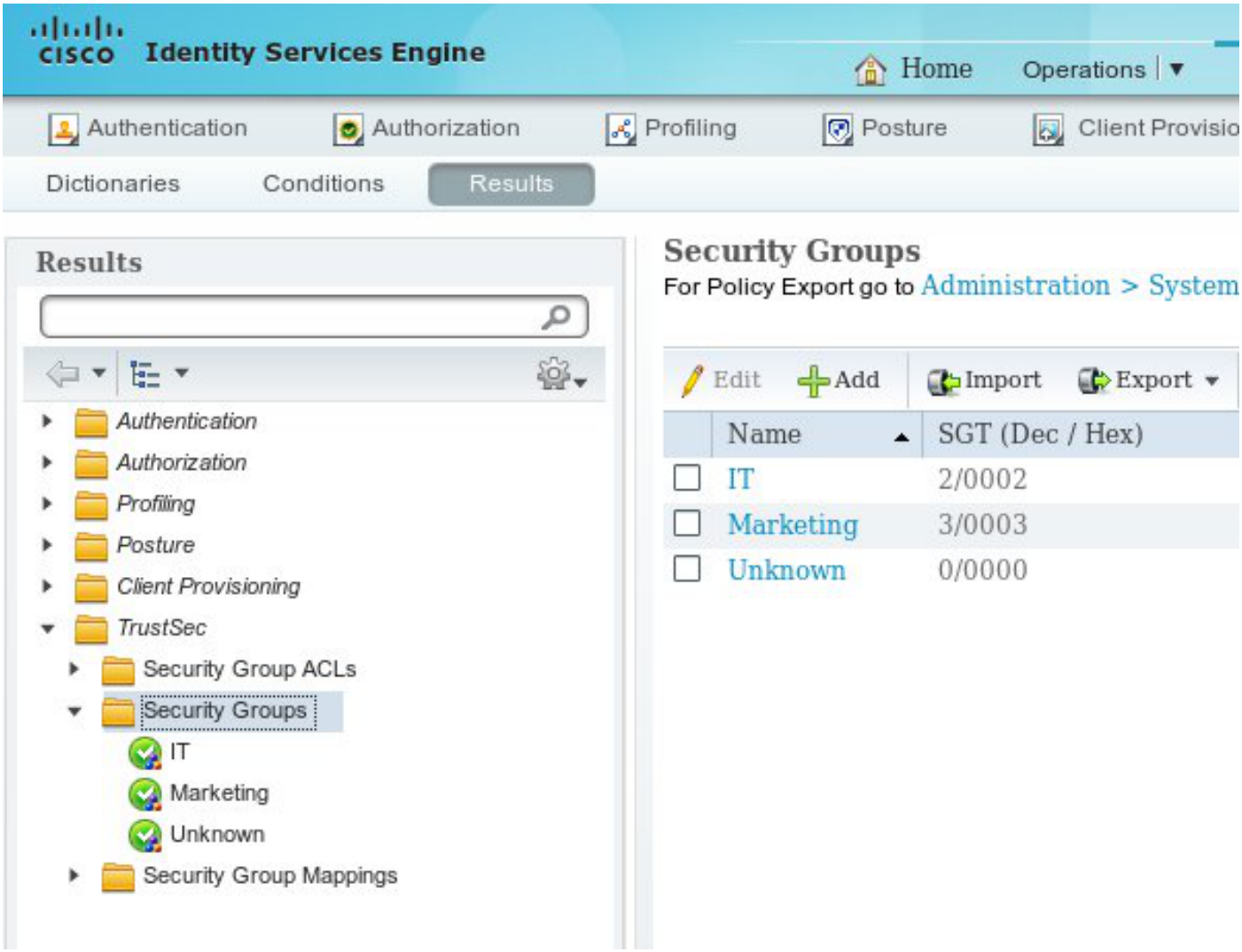
```
interface GigabitEthernet0/0
 nameif outside
 security-level 100
 ip address 172.16.33.110 255.255.255.0

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

ISE是在TrustSec部署的一个中心点。它分配SGT标记到访问并且验证对网络的所有用户。为基本配置要求的步骤在此部分列出。

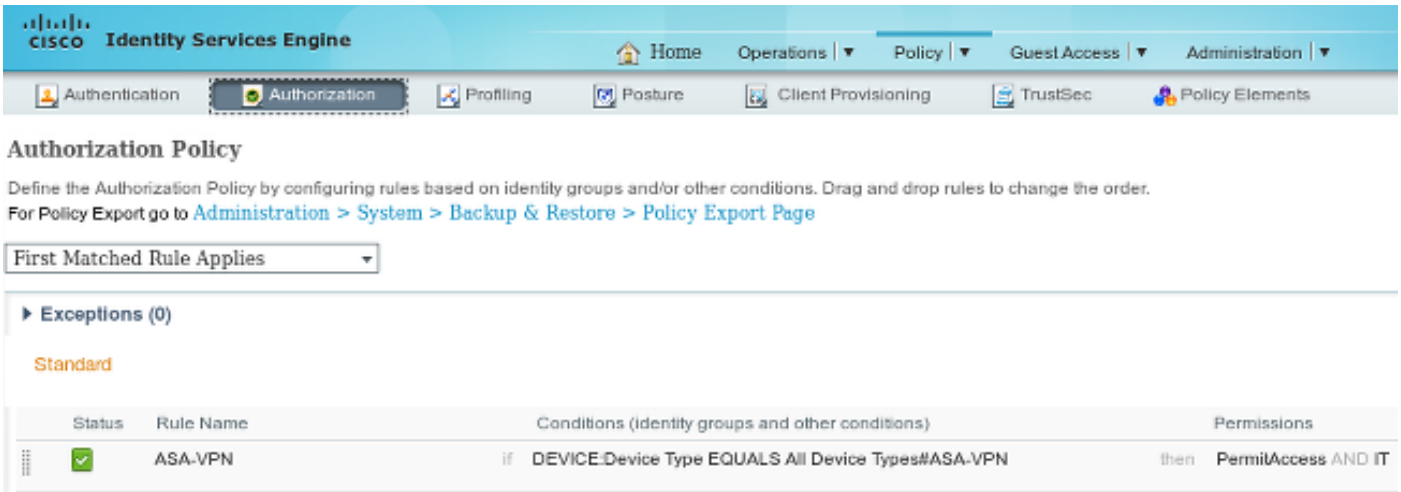
步骤1. IT和其他组的SGT

选择**策略>结果> Security组访问> Security组**并且创建SGT ：



步骤2.分配SGT = 2的VPN访问的授权规则(IT)

选择**策略>授权**并且创建远程VPN访问的一个规则。通过ASA-VPN被建立的所有VPN连接将获得完全权限(PermitAccess)，并且分配SGT标记2 (IT)。



步骤3.添加网络设备并且生成ASA-VPN的PAC文件

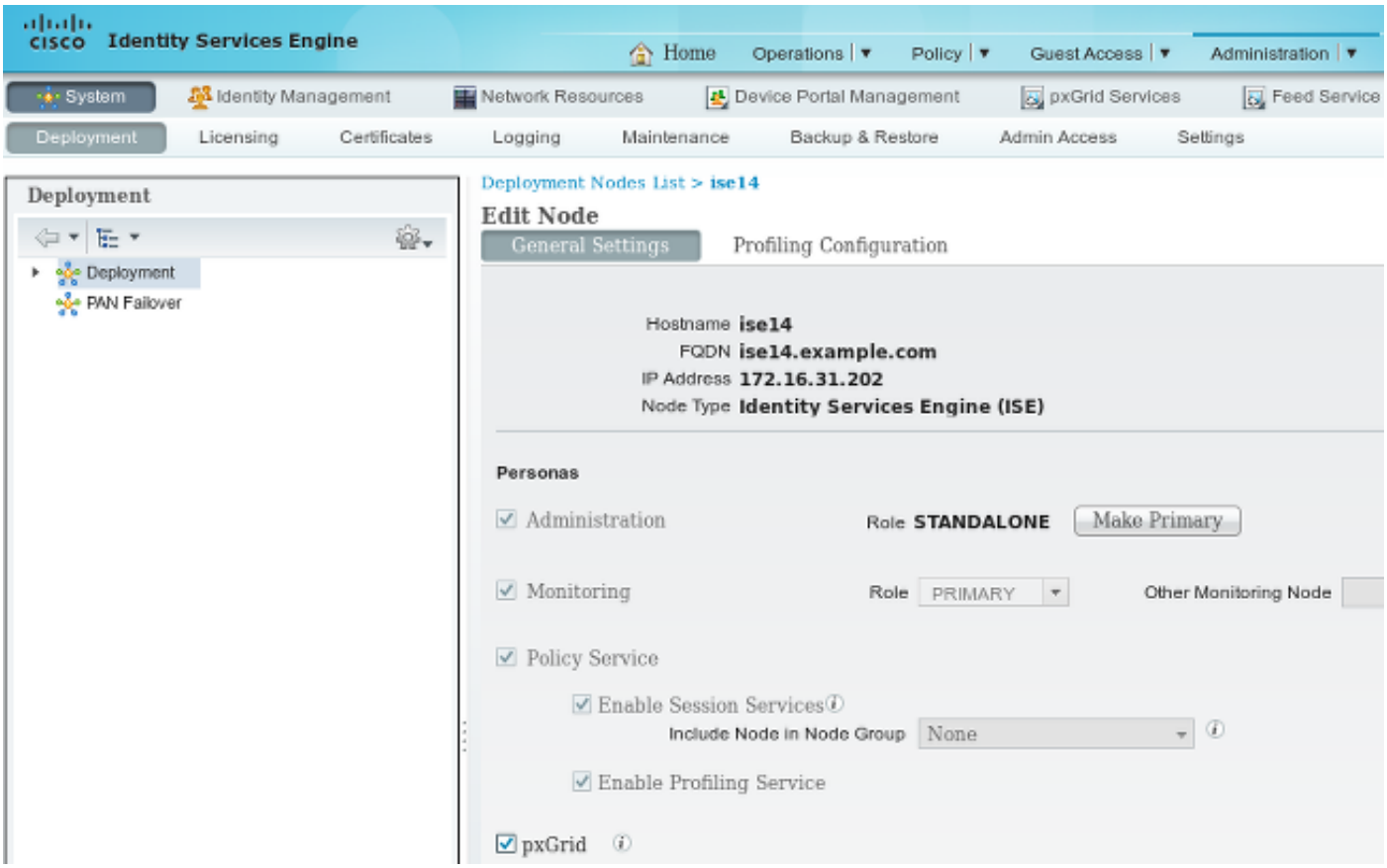
为了添加ASA-VPN到TrustSec域，生成手工代理自动设定(PAC)是必要的文件。该文件在ASA将导

入。

那可以从**Administration >网络设备**配置。在ASA被添加后，请移下来对TrustSec设置并且生成PAC文件。那的详细信息在一个分开的(被参考的)文档描述。

步骤4. Enable (event) pxGrid角色

选择**Administration >部署**为了启用pxGrid角色。



步骤5.生成管理和pxGrid角色的证书

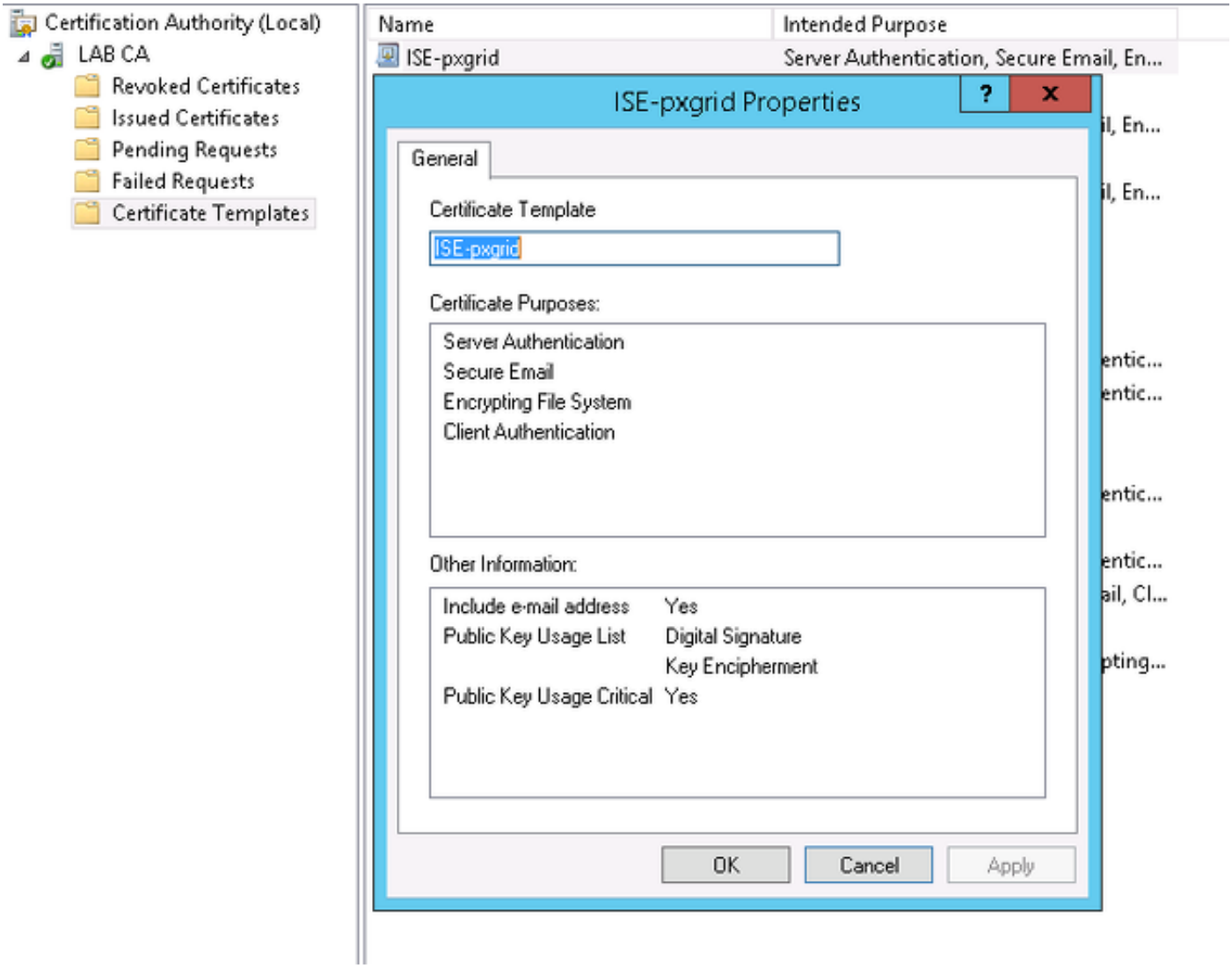
pxGrid协议使用证书验证客户端和服务器。配置ISE和WSA的正确证书是非常重要的。两证书在主题应该包括客户端验证和服务器验证的完全合格的域名(FQDN)和x509扩展。并且，请确保正确DNS记录为两个ISE和WSA创建并且匹配对应的FQDN的A。

如果两证书由一不同的Certificate Authority (CA)签字，在委托存储包括那些CA是重要的。

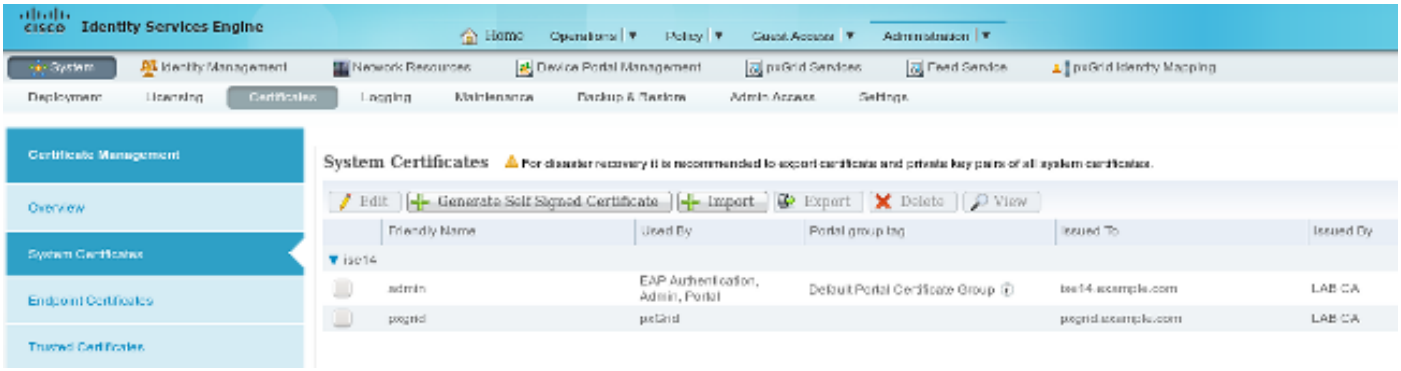
为了配置证书，请选择**Administration >证书**。

ISE能生成一证书签名请求(CSR)每个角色的。对于pxGrid角色，出口和签署与外部CA的CSR。

在本例中， Microsoft CA与此模板一起使用：



最终结果也许看起来象：



请勿忘记创建指向172.16.31.202 ise14.example.com和pxgrid.example.com的DNS A记录。

步骤6. pxGrid自动注册

默认情况下，ISE不会自动地注册pxGrid用户。应该由管理员手工审批那。应该为WSA集成更改该设置。

选择**Administration > pxGrid服务**和集**Enable (event)自动注册**。

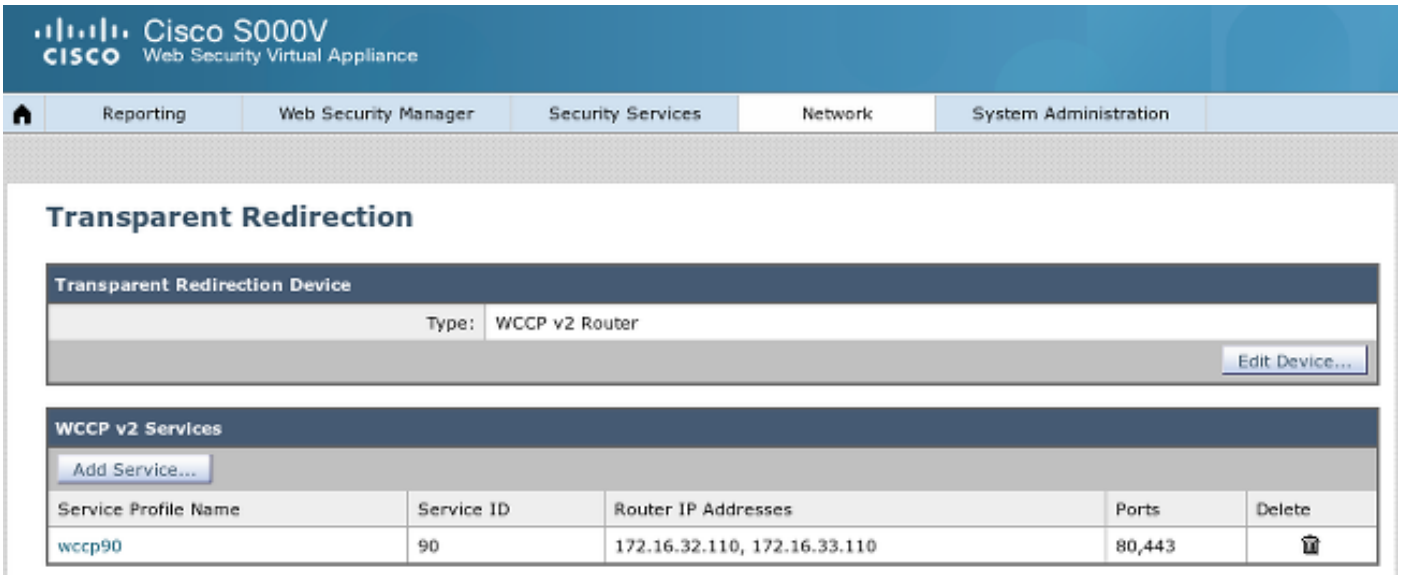
View By Capabilities

Enable Auto-Registration Disable Auto-Registration

WSA

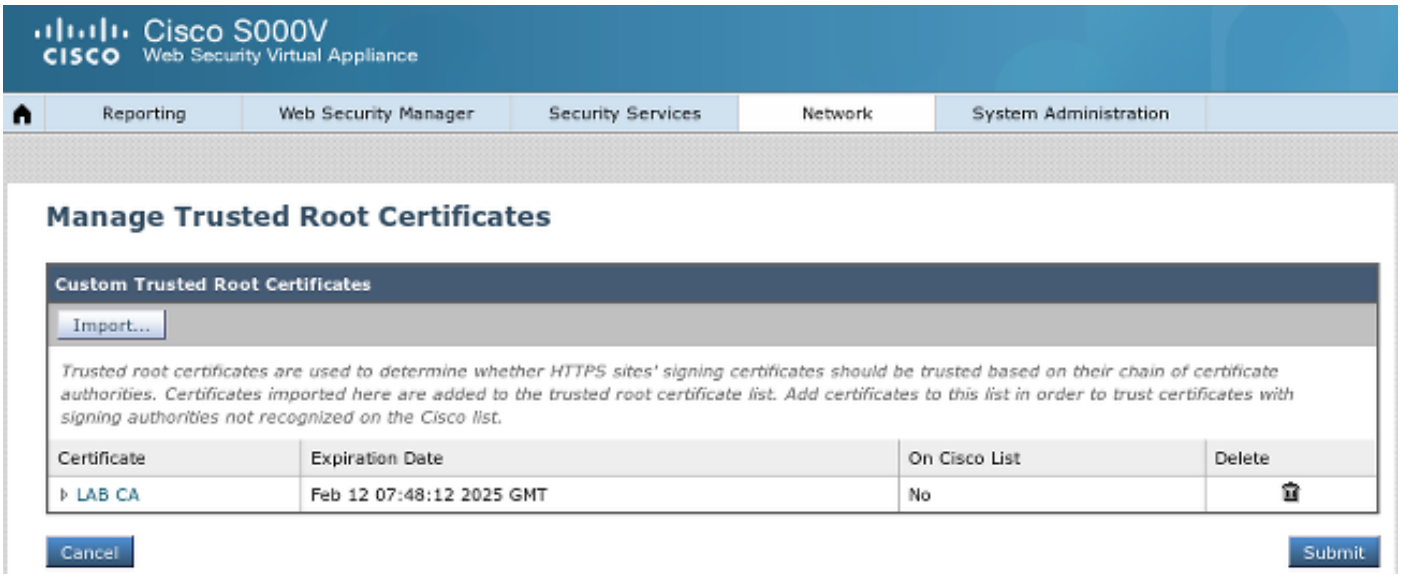
步骤1.透明模式和重定向

在本例中，WSA配置与管理接口、透明模式和重定向从ASA ：



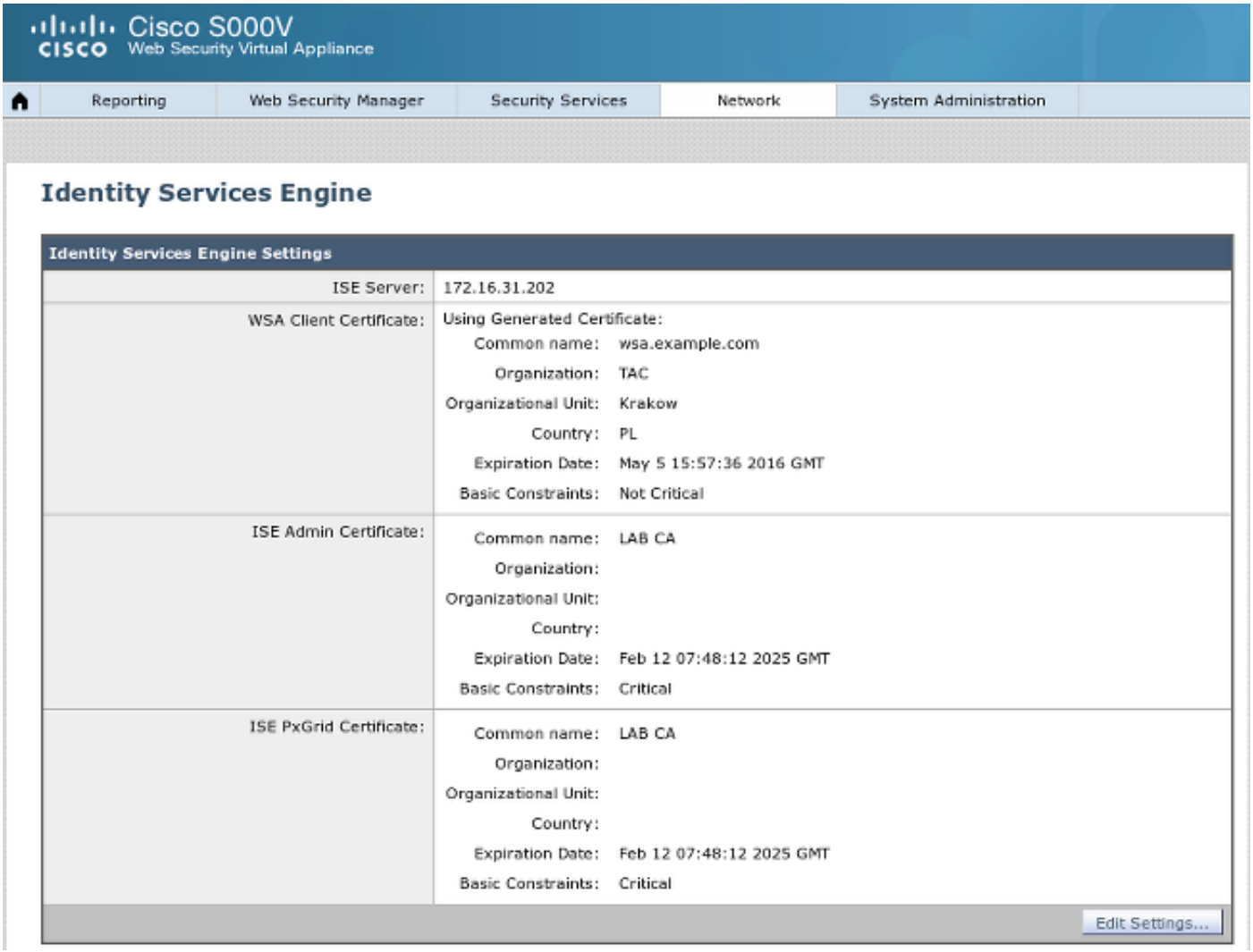
步骤2.证书生成

WSA需要委托CA签署所有证书。选择**网络> Certificate Management**为了添加CA证书：



生成WSA将使用为了验证到pxGrid的证书也是必要的。选择**网络>身份服务引擎> WSA客户端证书**为了生成CSR，用正确CA模板(ISEpxgrid)签署它和导入它回到。

并且，对于“ISE Admin证书”和“ISE pxGrid证书”，请导入CA证书(为了委托ISE提交的pxGrid证书)：

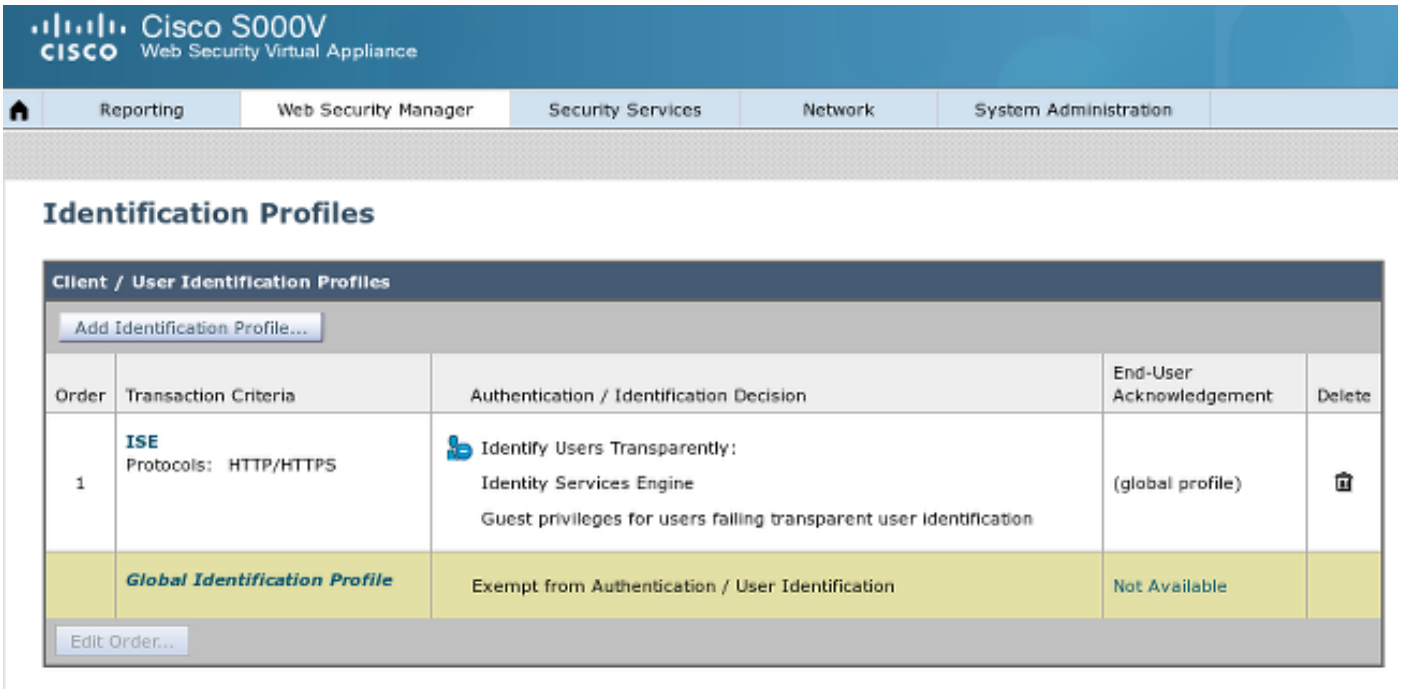


步骤3.测验ISE连接

选择**网络>身份服务引擎**为了测试对ISE的连接：

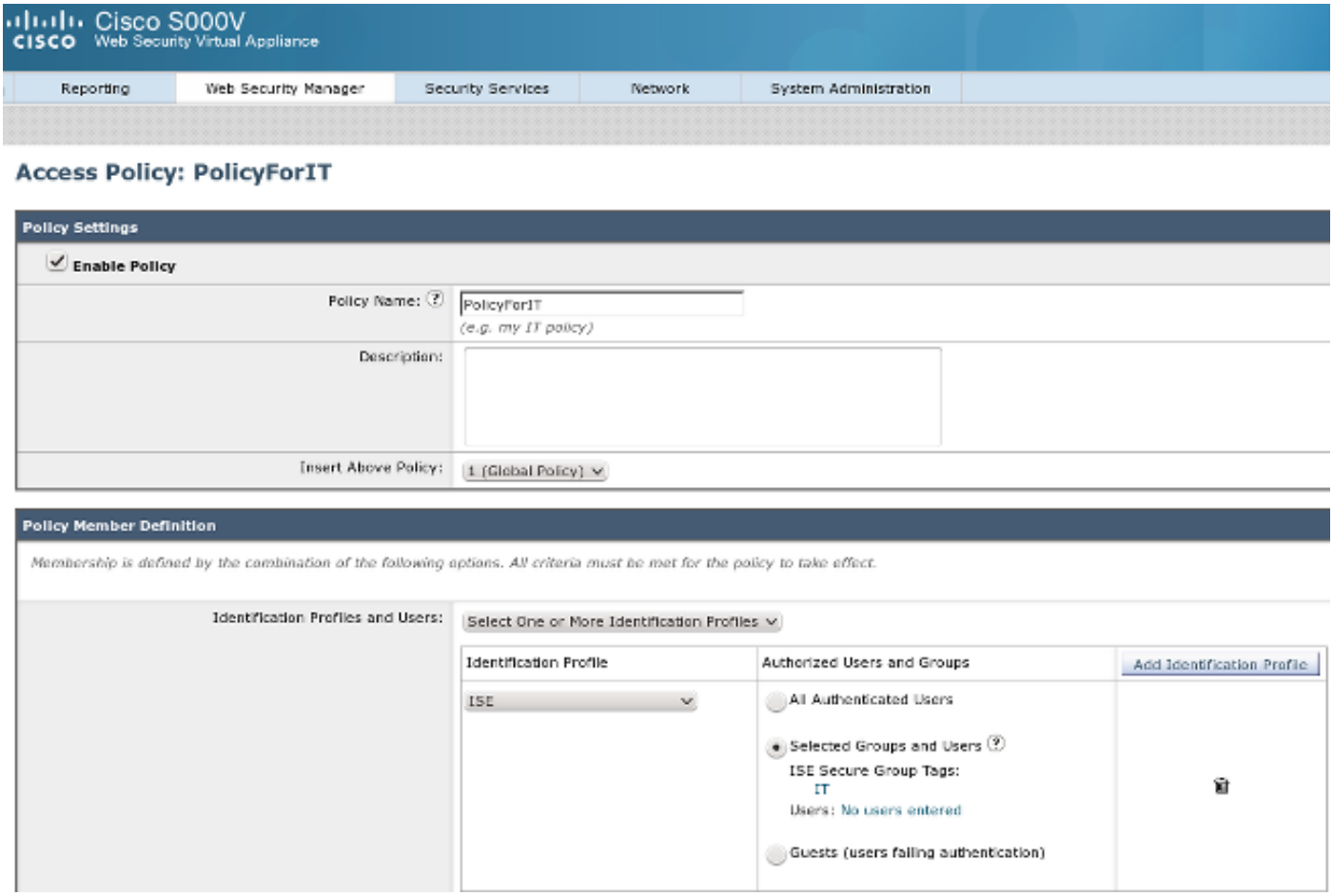
步骤4. ISE识别配置文件

选择**Web安全经理>识别配置文件**为了添加ISE的新配置文件。为“*识别和验证*”使用“*透明地请识别有ISE的用户*”。

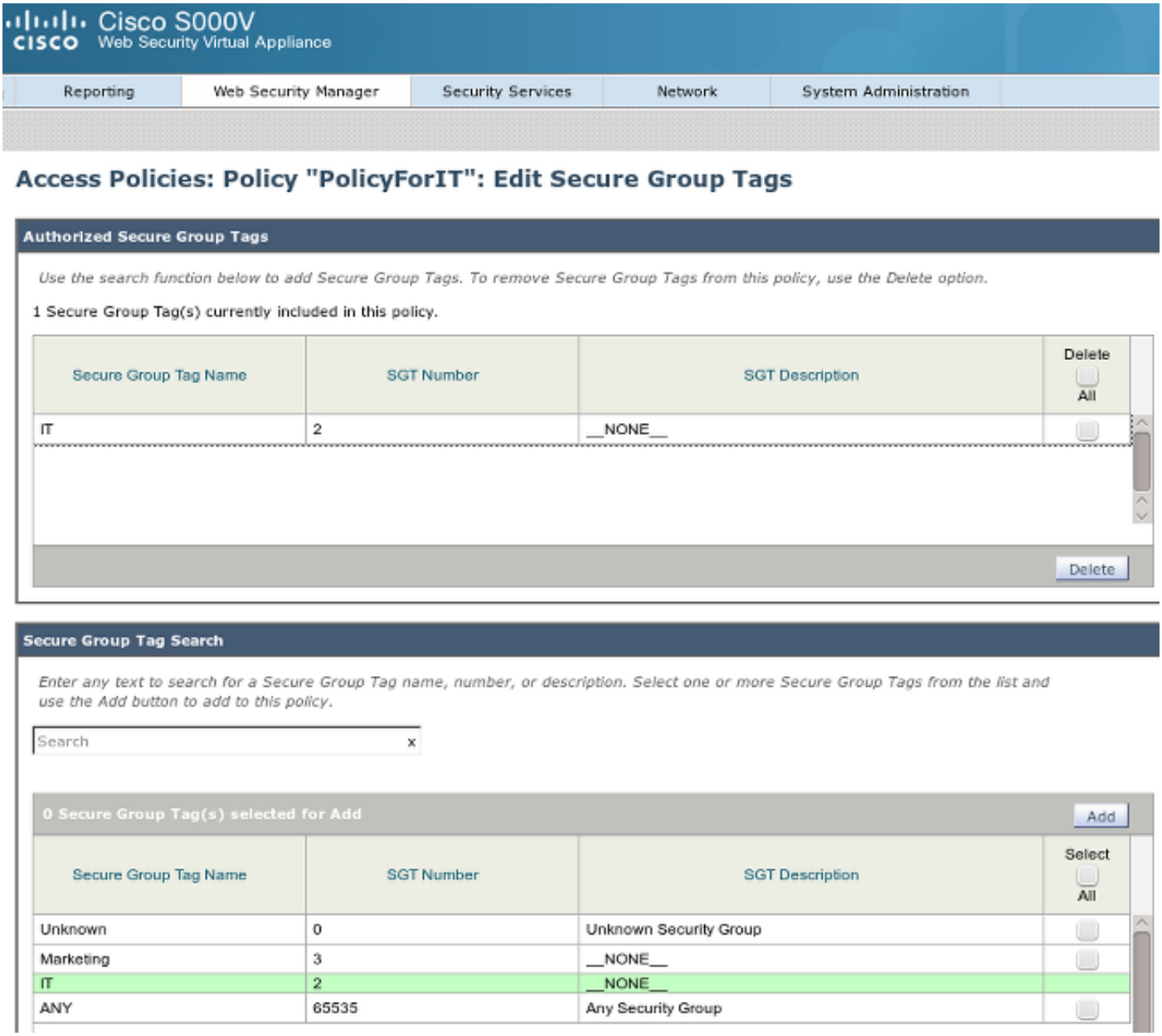


步骤5.访问根据SGT标记的策略

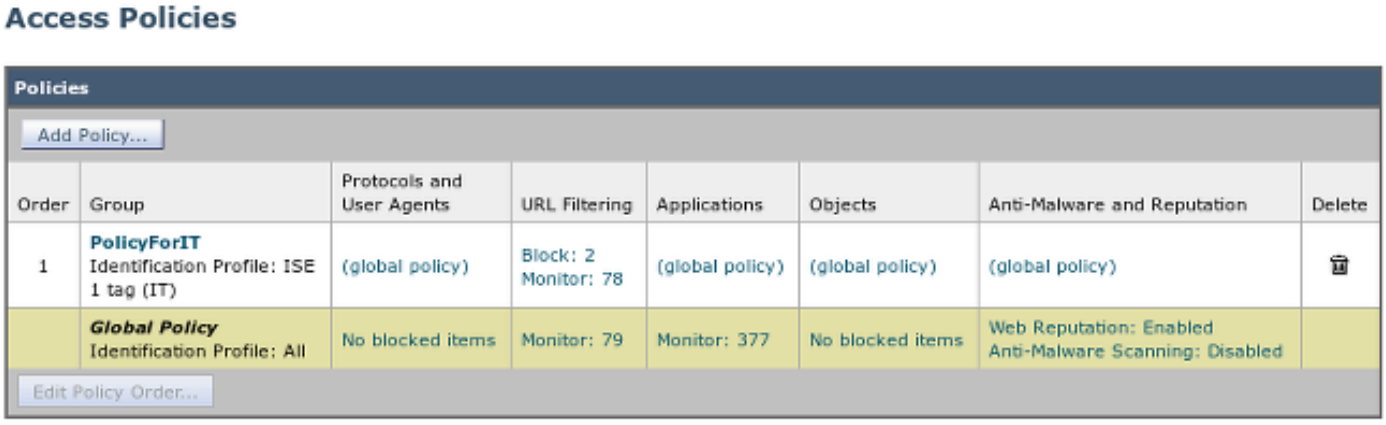
选择**Web安全经理>Access策略**为了添加新的策略。成员关系使用ISE配置文件：



对于选定组和用户SGT标记2将被添加(IT) ：



策略拒绝对所有运动站点的访问属于SGT IT:的用户的

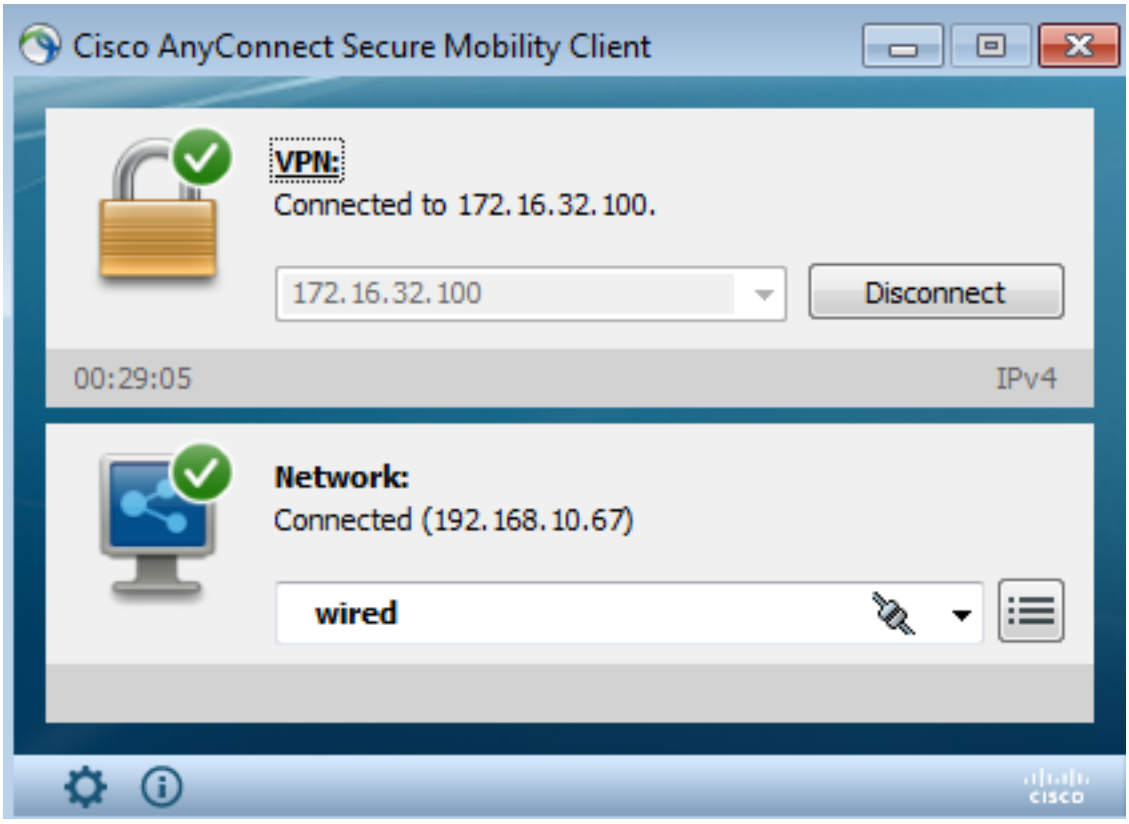


验证

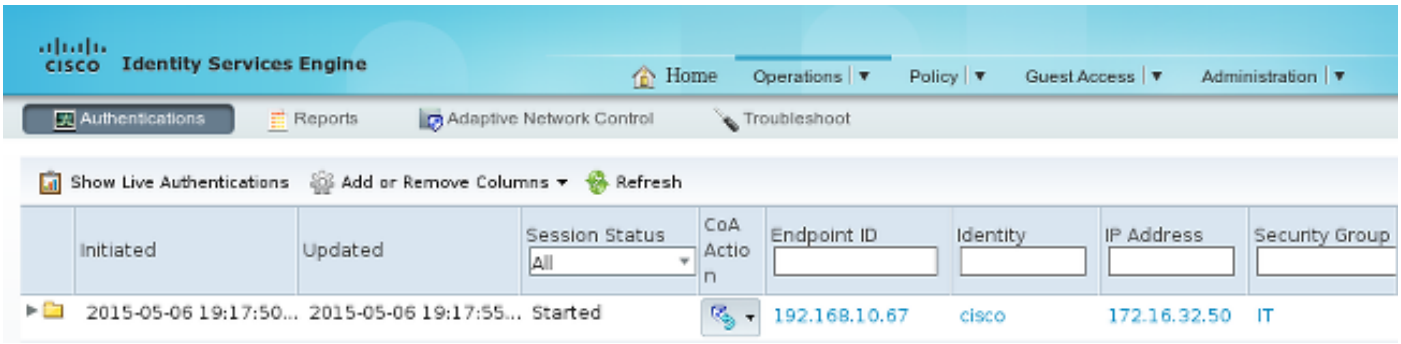
使用本部分可确认配置能否正常运行。

步骤1. VPN会话

VPN用户启动往ASA-VPN的VPN会话：



ASA-VPN使用ISE验证。ISE创建会话并且分配SGT标记2 (IT) ：



在成功认证以后，ASA-VPN创建有SGT标记的2 VPN会话(返回在Radius Access-Accept 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
```

因为ASA-VPN和ASA-FW之间的链路不是启用的TrustSec， ASA-VPN发送该流量的无标记帧(请勿能对GRE封装有被注入的CMD/TrustSec字段的以太网帧)。

步骤2. WSA获取的会话信息

在此阶段， WSA应该接收IP地址、用户名和SGT之间的映射(通过pxGrid协议) ：

```
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
[]>
```

步骤3.对WSA的流量重定向

VPN用户首次对sport.pl的连接， ASA-FW拦截：

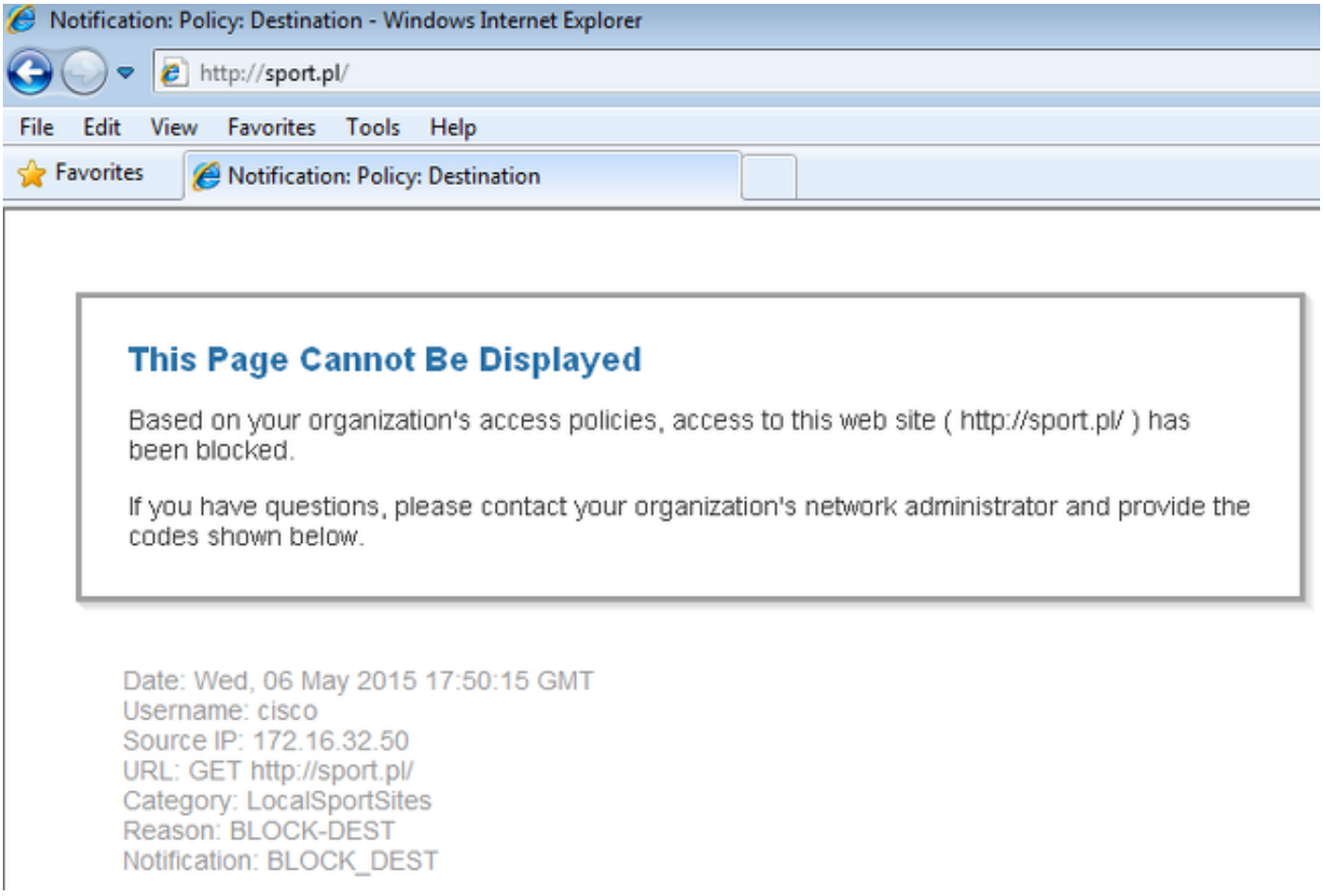
```
asa-fw# show wccp

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
```

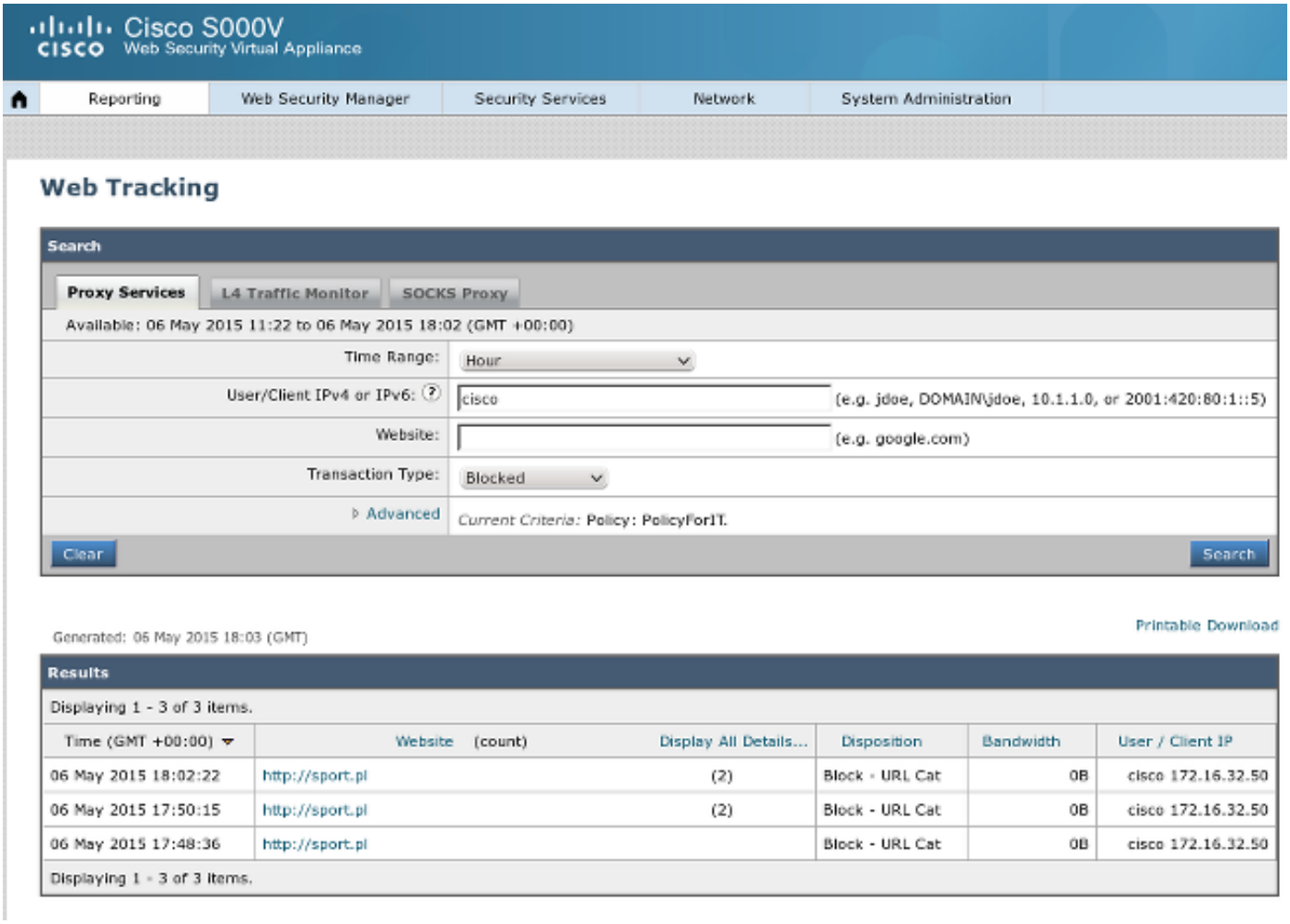
并且建立隧道在GRE对WSA (公告WCCP router-id是配置的最高的IP地址) ：

```
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
```

WSA继续TCP握手并且处理GET请求。结果，名为PolicyForIT的策略是点击，并且流量阻塞：



那由WSA报告确认：



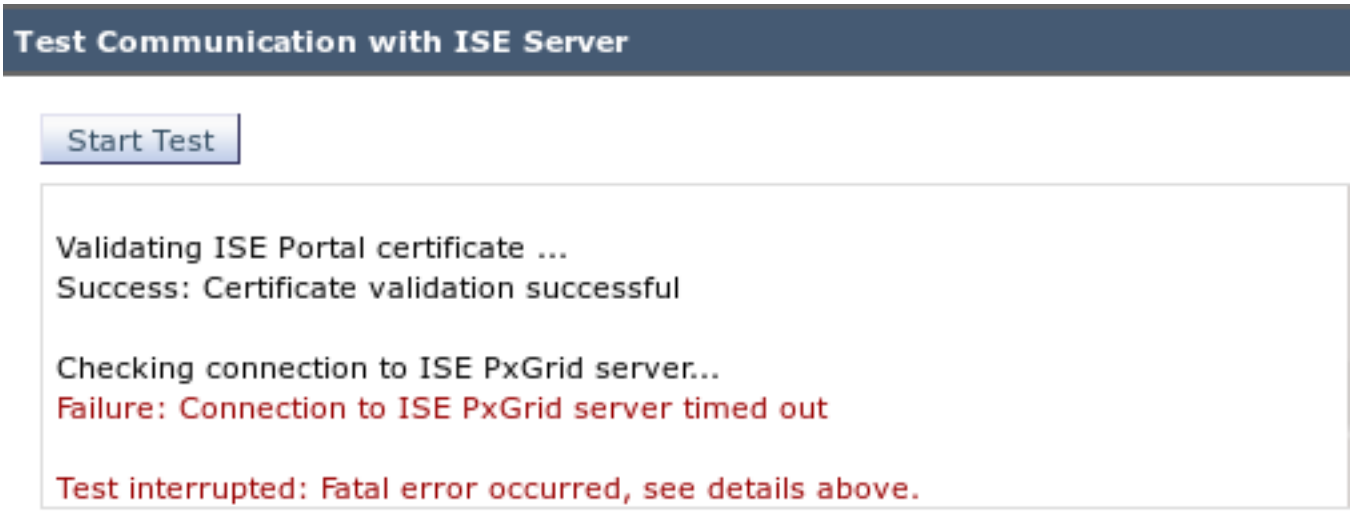
注意ISE显示用户名。

故障排除

本部分提供了可用于对配置进行故障排除的信息。

不正确证书

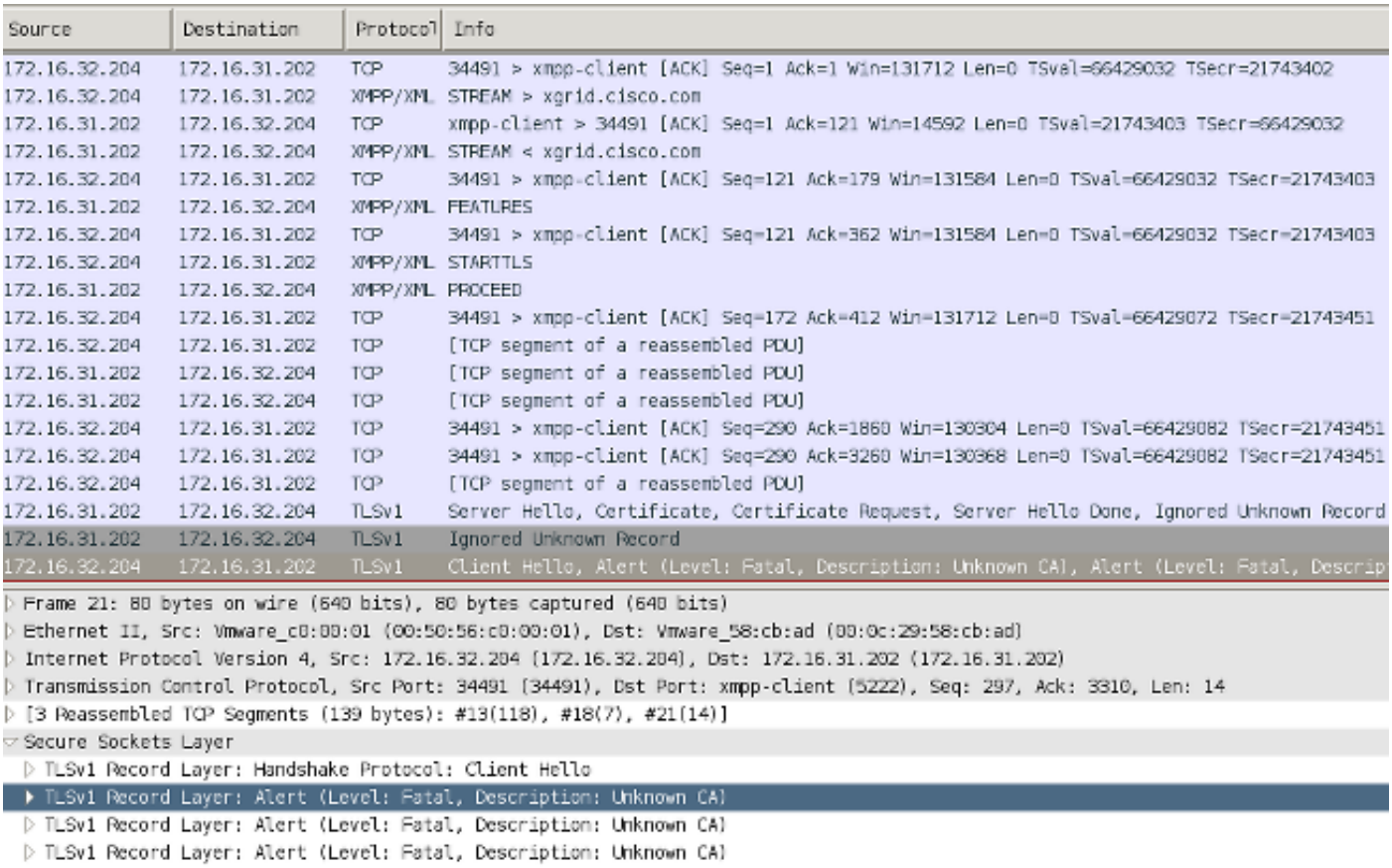
当WSA没有正确地初始化(证书)，请测试对于ISE连接失败：



ISE pxgrid-cm.log报告：

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

失败的原因能在Wireshark看到：



Source	Destination	Protocol	Info
172.16.32.204	172.16.31.202	TCP	34491 > xmpp-client [ACK] Seq=1 Ack=1 Win=131712 Len=0 TSval=66429032 TSecr=21743402
172.16.32.204	172.16.31.202	XMPP/XML	STREAM > xgrid.cisco.com
172.16.31.202	172.16.32.204	TCP	xmpp-client > 34491 [ACK] Seq=1 Ack=121 Win=14592 Len=0 TSval=21743403 TSecr=66429032
172.16.31.202	172.16.32.204	XMPP/XML	STREAM < xgrid.cisco.com
172.16.32.204	172.16.31.202	TCP	34491 > xmpp-client [ACK] Seq=121 Ack=179 Win=131584 Len=0 TSval=66429032 TSecr=21743403
172.16.31.202	172.16.32.204	XMPP/XML	FEATURES
172.16.32.204	172.16.31.202	TCP	34491 > xmpp-client [ACK] Seq=121 Ack=362 Win=131584 Len=0 TSval=66429032 TSecr=21743403
172.16.32.204	172.16.31.202	XMPP/XML	STARTTLS
172.16.31.202	172.16.32.204	XMPP/XML	PROCEED
172.16.32.204	172.16.31.202	TCP	34491 > xmpp-client [ACK] Seq=172 Ack=412 Win=131712 Len=0 TSval=66429072 TSecr=21743451
172.16.32.204	172.16.31.202	TCP	[TCP segment of a reassembled PDU]
172.16.31.202	172.16.32.204	TCP	[TCP segment of a reassembled PDU]
172.16.31.202	172.16.32.204	TCP	[TCP segment of a reassembled PDU]
172.16.32.204	172.16.31.202	TCP	34491 > xmpp-client [ACK] Seq=290 Ack=1860 Win=130304 Len=0 TSval=66429082 TSecr=21743451
172.16.32.204	172.16.31.202	TCP	34491 > xmpp-client [ACK] Seq=290 Ack=3260 Win=130368 Len=0 TSval=66429082 TSecr=21743451
172.16.32.204	172.16.31.202	TCP	[TCP segment of a reassembled PDU]
172.16.31.202	172.16.32.204	TLSv1	Server Hello, Certificate, Certificate Request, Server Hello Done, Ignored Unknown Record
172.16.31.202	172.16.32.204	TLSv1	Ignored Unknown Record
172.16.32.204	172.16.31.202	TLSv1	Client Hello, Alert (Level: Fatal, Description: Unknown CA), Alert (Level: Fatal, Descrip

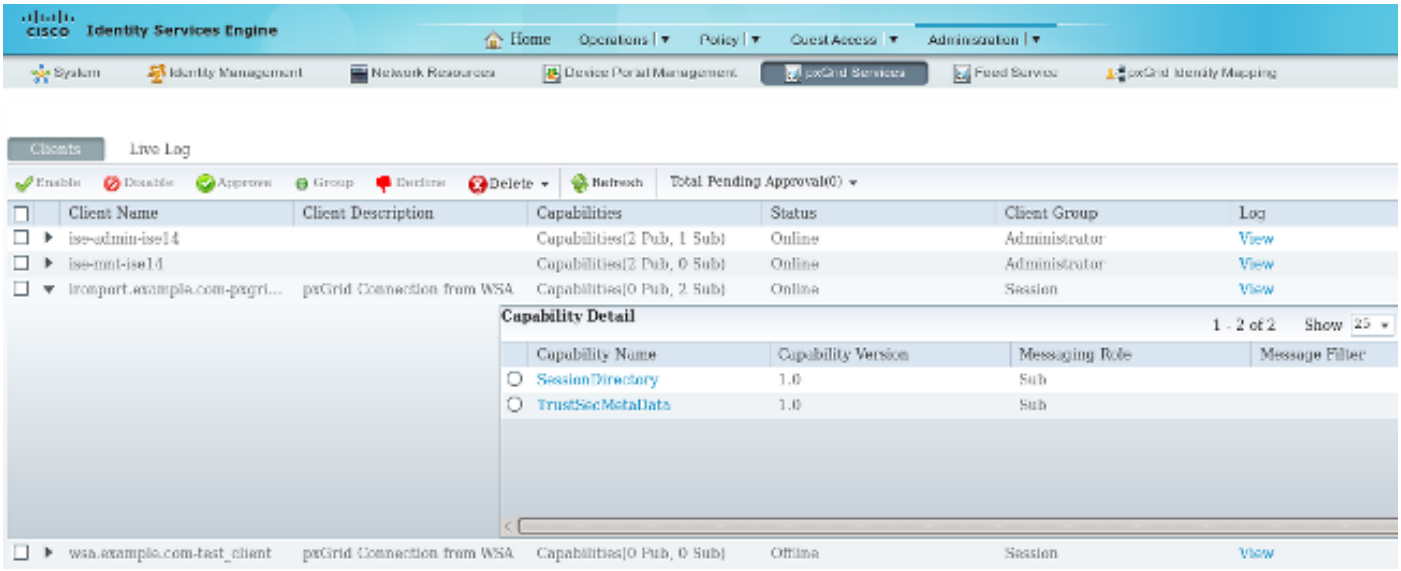
对于SSL会话过去常常保护可扩展消息传送和在线状态协议(XMPP)请交换(使用由pxGrid)，客户端报告SSL失败由于服务器提交的未知证书链。

更正方案

对于正确方案， ISE pxgrid-controller.log记录：

```
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
```

并且， ISE GUI提交WSA作为用户以正确功能：



相关信息

- [ASA与ISE配置示例的版本9.2.1 VPN状态]
- [WSA 8.7用户指南]
- [ASA和Catalyst 3750X系列交换机TrustSec配置示例和排除故障指南]
- [思科TrustSec交换机配置指南：了解思科TrustSec]
- [配置安全工具用户授权的外部服务器]
- [思科ASA系列VPN CLI配置指南， 9.1]
- [思科身份服务引擎用户指南，版本1.2]
- [技术支持和文档 - Cisco Systems]