Configure WSA Integration with ISE for TrustSec Aware Services

Document ID: 119212

Contributed by Michal Garcarz, Cisco TAC Engineer.
Jul 30, 2015

Contents

Introduction

This document describes how to integrate the Web Security Appliance (WSA) with Identity Services Engine (ISE). ISE Version 1.3 supports a new API called pxGrid. This modern and flexible protocol supports authentication, encryption, and privileges (groups) which allows for easy integration with other security solutions.

WSA Version 8.7 supports pxGrid protocol and is able to retrieve context identity information from ISE. As a result, WSA allows you to build policies based on TrustSec Security Group Tag (SGT) groups retrieved from ISE.

Prerequisites

Requirements

Cisco recommends that you have experience with Cisco ISE configuration and basic knowledge of these topics:

- ISE deployments and authorization configuration
- Adaptive Security Appliance (ASA) CLI configuration for TrustSec and VPN access
- WSA configuration
- Basic understanding of TrustSec deployments

Components Used

The information in this document is based on these software and hardware versions:

- Microsoft Windows 7
- Cisco ISE Software Version 1.3 and later
- Cisco AnyConnect Mobile Security Version 3.1 and later
- Cisco ASA Version 9.3.1 and later
- Cisco WSA Version 8.7 and later

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configure

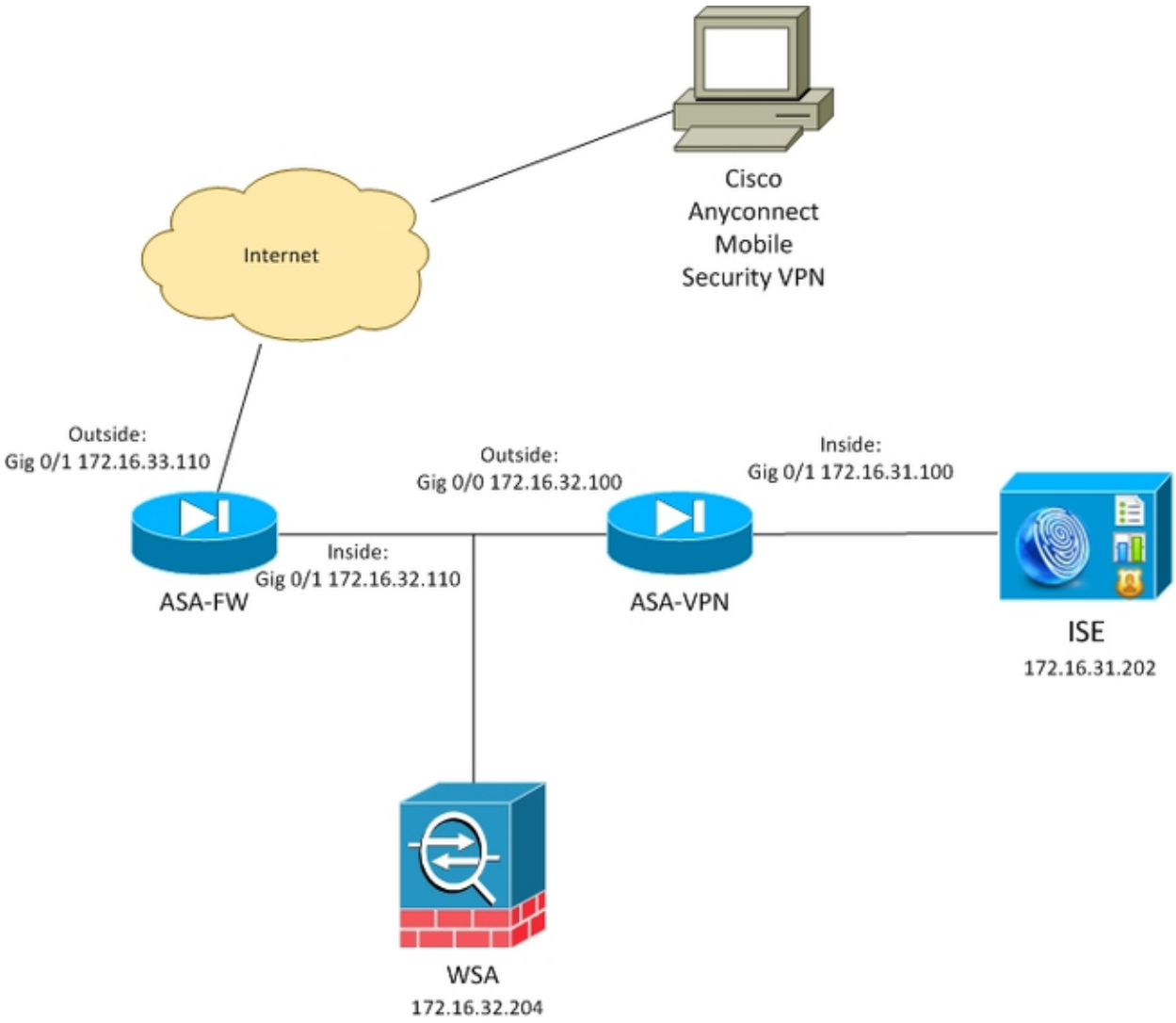
Note: Use the Command Lookup Tool (registered customers only) in order to obtain more information on the commands used in this section.

Network Diagram and Traffic Flow

TrustSec SGT tags are assigned by ISE used as an authentication server for all types of users that access the corporate network. This involves wired/wireless users that authenticate via 802.1x or ISE guest portals. Also, remote VPN users that use ISE for authentication.

For WSA, it does not matter how the user has accessed the network.

This example presents a remote VPN users terminating session on the ASA-VPN. Those users have been assigned a specific SGT tag. All HTTP traffic to the Internet will be intercepted by the ASA-FW (firewall) and redirected to the WSA for inspection. The WSA uses the identity profile which allows it to classify users based on the SGT tag and build access or decryption policies based on that.



The detailed flow is:

1. The AnyConnect VPN user terminates the Secure Sockets Layer (SSL) session on the ASA-VPN. The ASA-VPN is configured for TrustSec and uses ISE for authentication of VPN users. The authenticated user is assigned a SGT tag value = 2 (name = IT). The user receives an IP address from the 172.16.32.0/24 network (172.16.32.50 in this example).
2. The user tries to access the web page in the Internet. The ASA-FW is configured for Web Cache Communication Protocol (WCCP) which redirects traffic to the WSA.
3. The WSA is configured for ISE integration. It uses pxGrid in order to download information from the ISE: user IP address 172.16.32.50 has been assigned SGT tag 2.
4. The WSA processes the HTTP request from the user and hits access policy PolicyForIT. That policy is configured to block traffic to the sports sites. All other users (which do not belong to SGT 2) hit the default access policy and have full access to the sports sites.

ASA-VPN

This is a VPN gateway configured for TrustSec. Detailed configuration is out of scope of this document. Refer to these examples:

- ASA and Catalyst 3750X Series Switch TrustSec Configuration Example and Troubleshoot Guide
- ASA Version 9.2 VPN SGT Classification and Enforcement Configuration Example

ASA-FW

The ASA firewall is responsible for WCCP redirection to the WSA. This device is not aware of TrustSec.

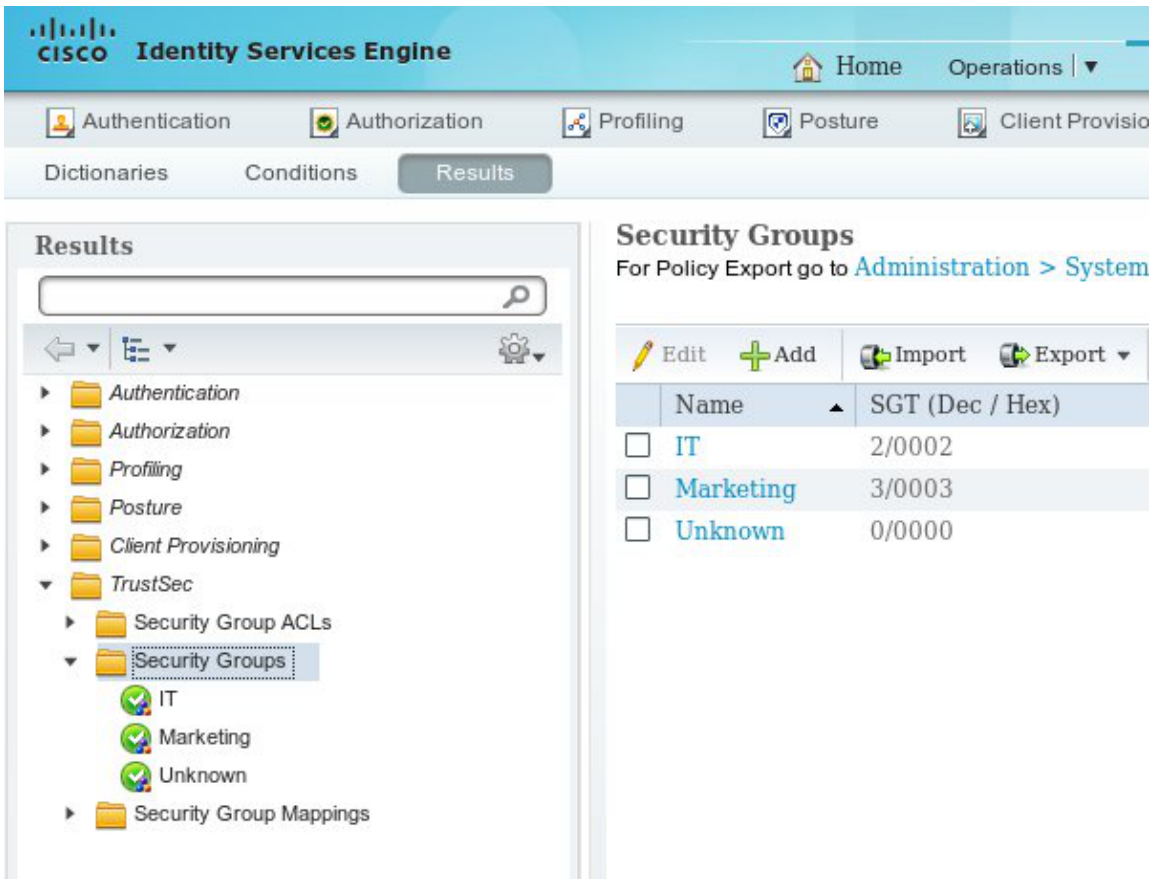
```
interface GigabitEthernet0/0
 nameif outside
 security-level 100
 ip address 172.16.33.110 255.255.255.0

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 is a central point in the TrustSec deployment. It assigns SGT tags to all users that access and authenticate to the network. Steps required for basic configuration are listed in this section.

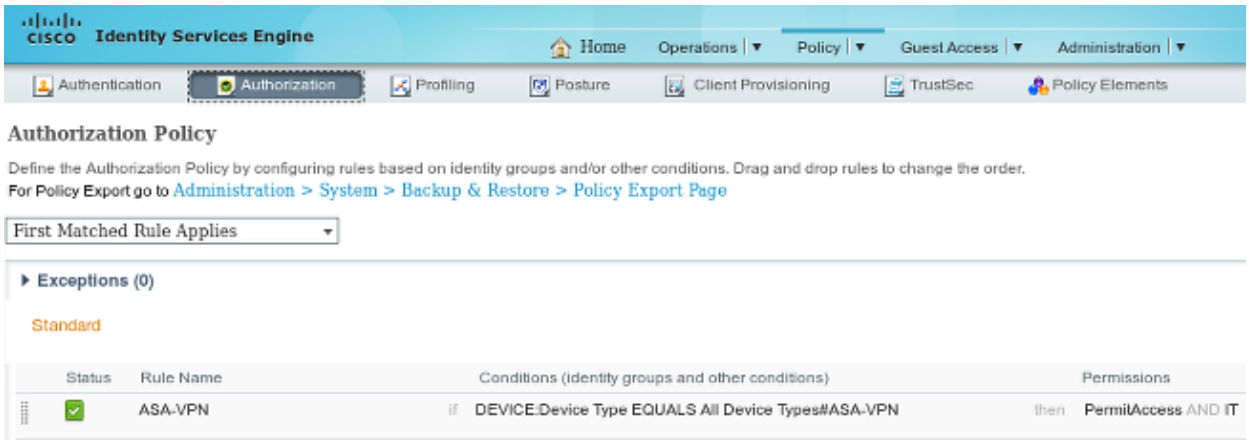
Step 1. SGT for IT and Other Group

Choose **Policy > Results > Security Group Access > Security Groups** and create the SGT:



Step 2. Authorization Rule for VPN Access That Assigns SGT = 2 (IT)

Choose **Policy > Authorization** and create a rule for remote VPN access. All VPN connections established via ASA-VPN will get full access (PermitAccess) and will be assigned SGT tag 2 (IT).



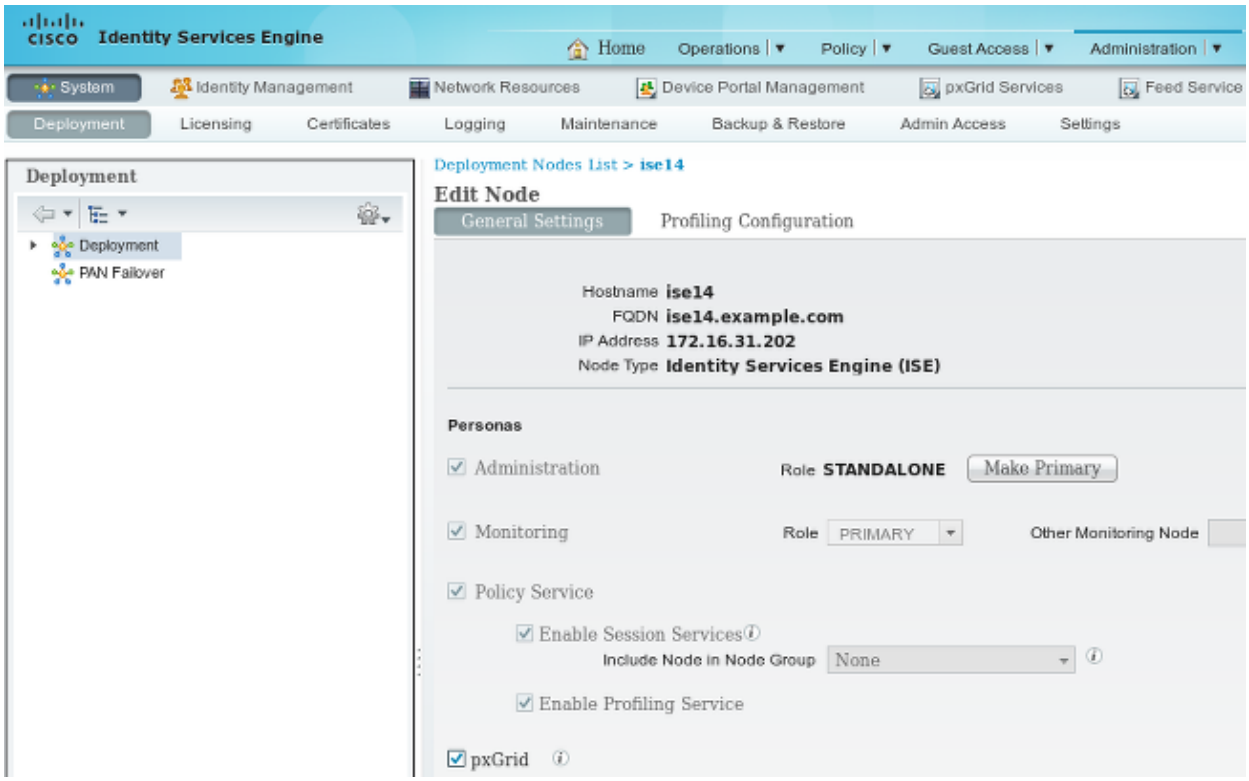
Step 3. Add Network Device and Generate PAC File for ASA-VPN

In order to add the ASA-VPN to the TrustSec domain, it is necessary to generate the proxy Auto Config (PAC) file manually. That file will be imported on the ASA.

That can be configured from **Administration > Network Devices**. After the ASA is added, scroll down to TrustSec settings and generate the PAC file. The details for that are described in a separate (referenced) document.

Step 4. Enable pxGrid Role

Choose **Administration > Deployment** in order to enable the pxGrid role.



Step 5. Generate the Certificate for Administration and the pxGrid Role

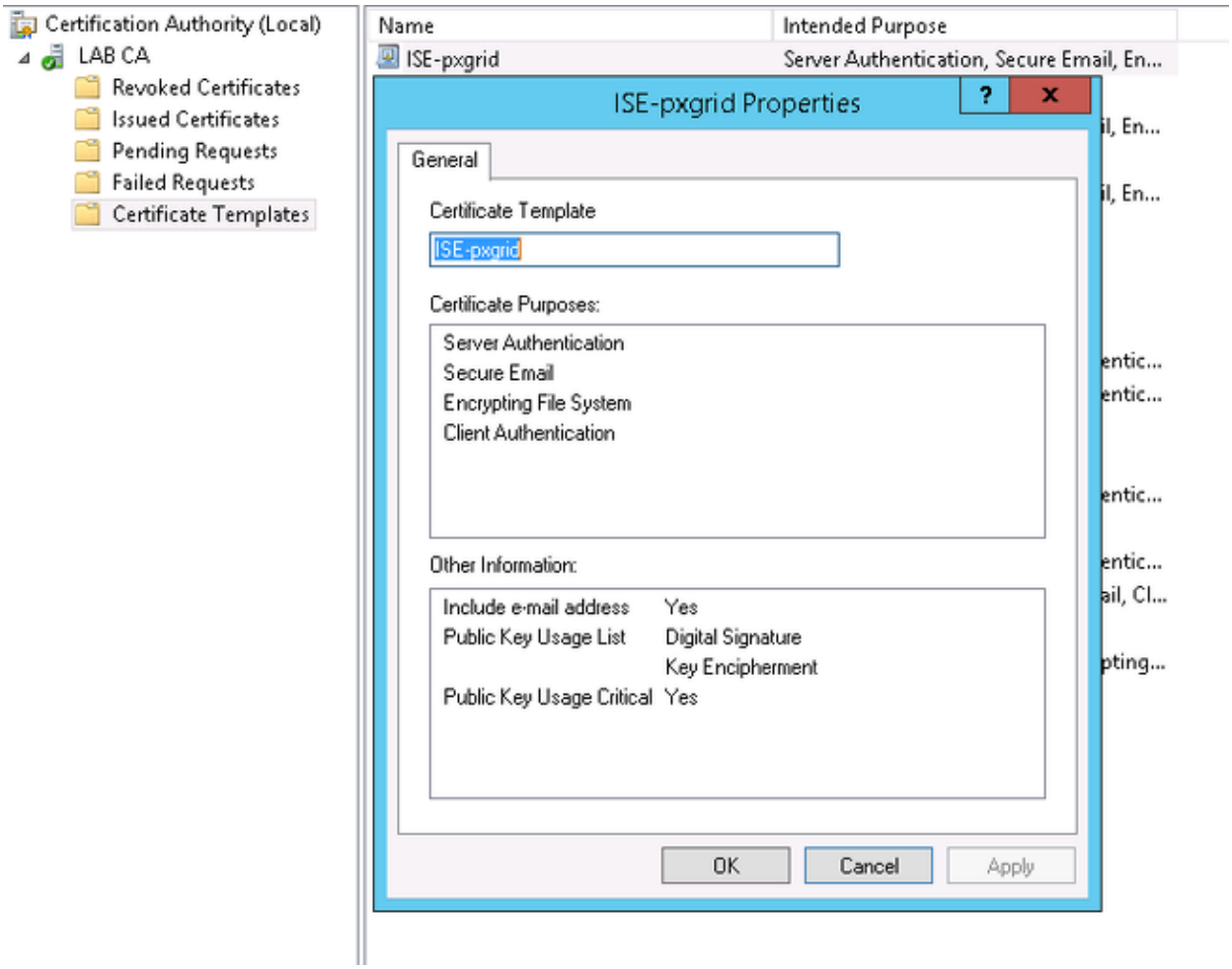
The pxGrid protocol uses certificate authentication for both the client and the server. It is very important to configure the correct certificates for both ISE and the WSA. Both certificates should include the Fully Qualified Domain Name (FQDN) in the Subject and x509 extensions for Client Authentication and Server Authentication. Also, make sure the correct DNS A record is created for both ISE and the WSA and matches the corresponding FQDN.

If both certificates are signed by a different Certificate Authority (CA), it is important to include those CAs in the trusted store.

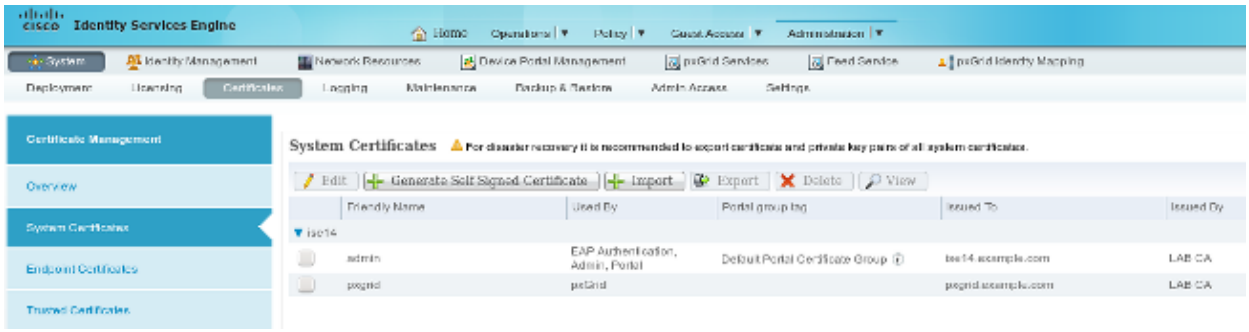
In order to configure certificates, choose **Administration > Certificates**.

ISE can generate a certificate signing request (CSR) for each role. For the pxGrid role, export and sign the CSR with an external CA.

In this example, the Microsoft CA has been used with this template:



The end result might look like:



Do not forget to create DNS A records for ise14.example.com and pxgrid.example.com that point to 172.16.31.202.

Step 6. pxGrid Auto Registration

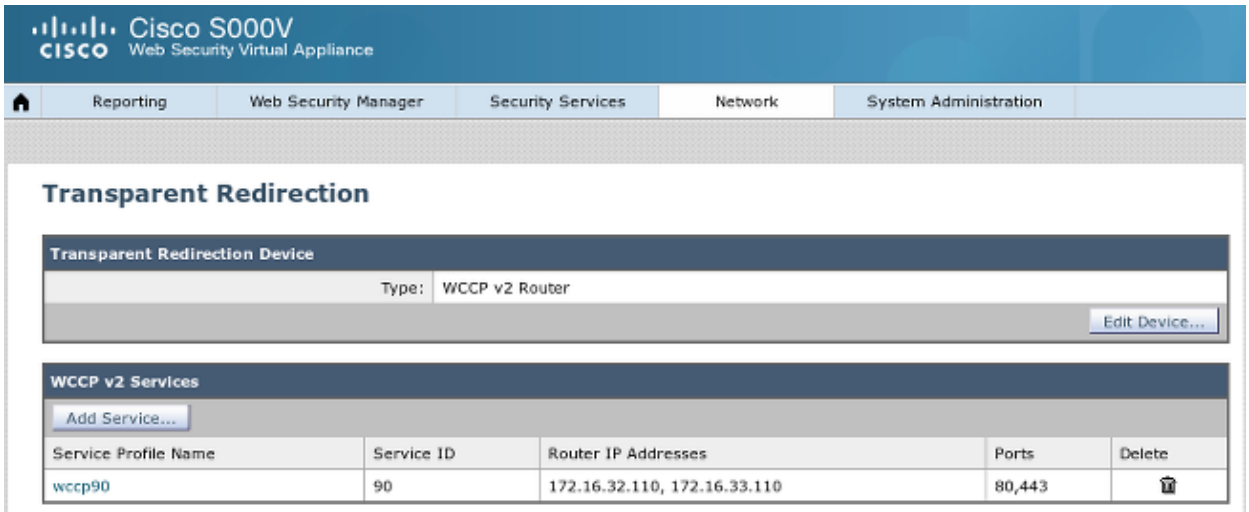
By default, ISE will not automatically register pxGrid subscribers. That should be manually approved by the administrator. That setting should be changed for WSA integration.

Choose **Administration > pxGrid Services** and set **Enable Auto-Registration**.

WSA

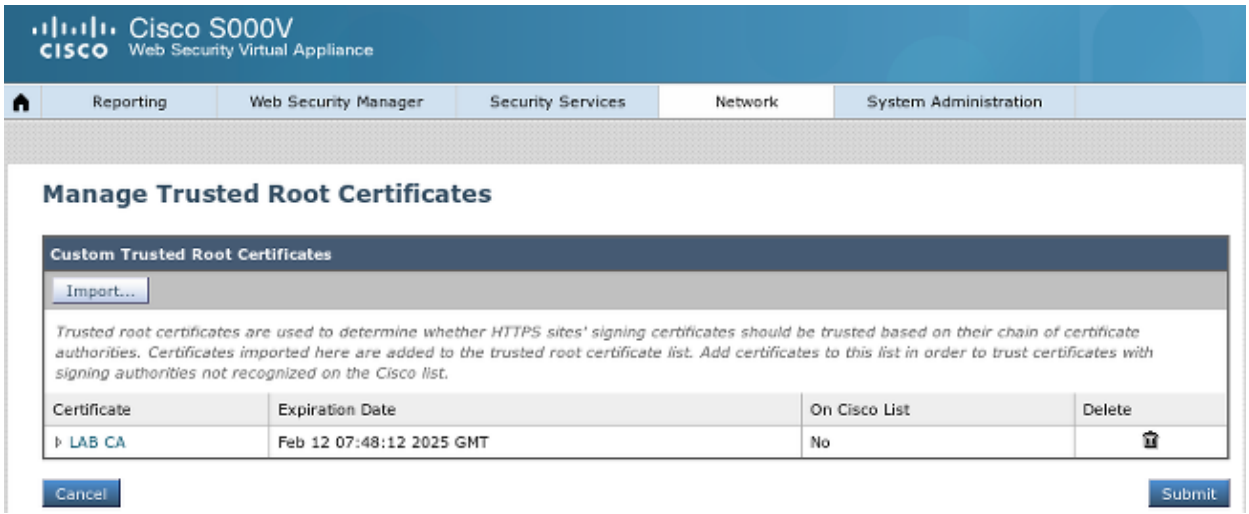
Step 1. Transparent Mode and Redirection

In this example, the WSA is configured with just the management interface, transparent mode, and redirection from the ASA:



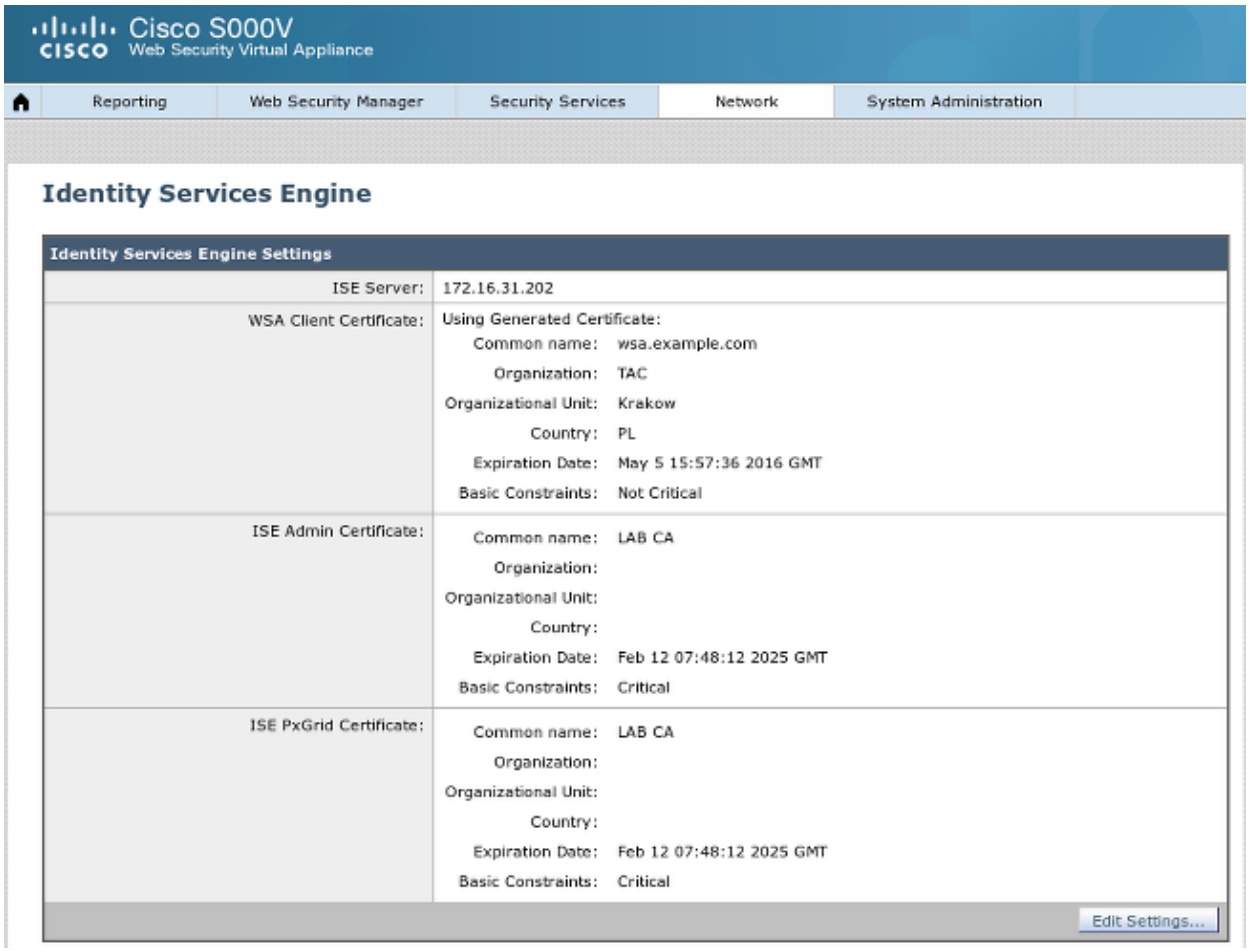
Step 2. Certificate Generation

The WSA needs to trust the CA to sign all certificates. Choose **Network > Certificate Management** in order to add a CA certificate:



It is also necessary to generate a certificate the WSA will use in order to authenticate to pxGrid. Choose **Network > Identity Services Engine > WSA Client certificate** in order to generate the CSR, sign it with the correct CA template (ISE-pxgrid), and import it back.

Also, for "ISE Admin Certificate" and "ISE pxGrid Certificate", import the CA certificate (in order to trust the pxGrid certificate presented by ISE):

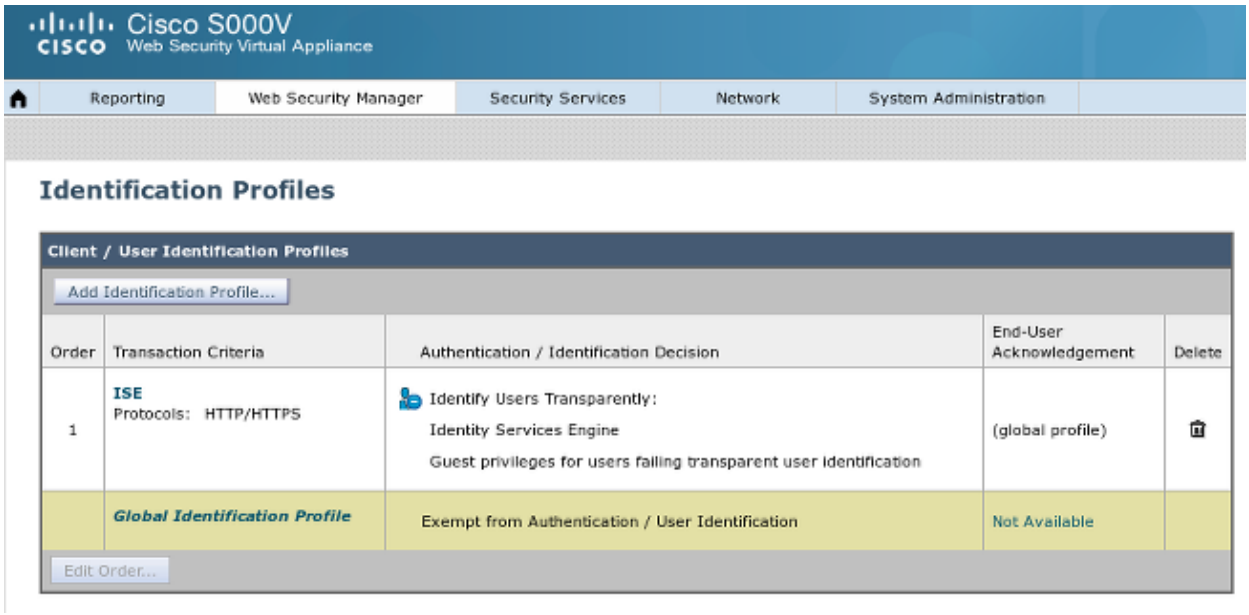


Step 3. Test ISE Connectivity

Choose **Network > Identity Services Engine** in order to test the connection to ISE:

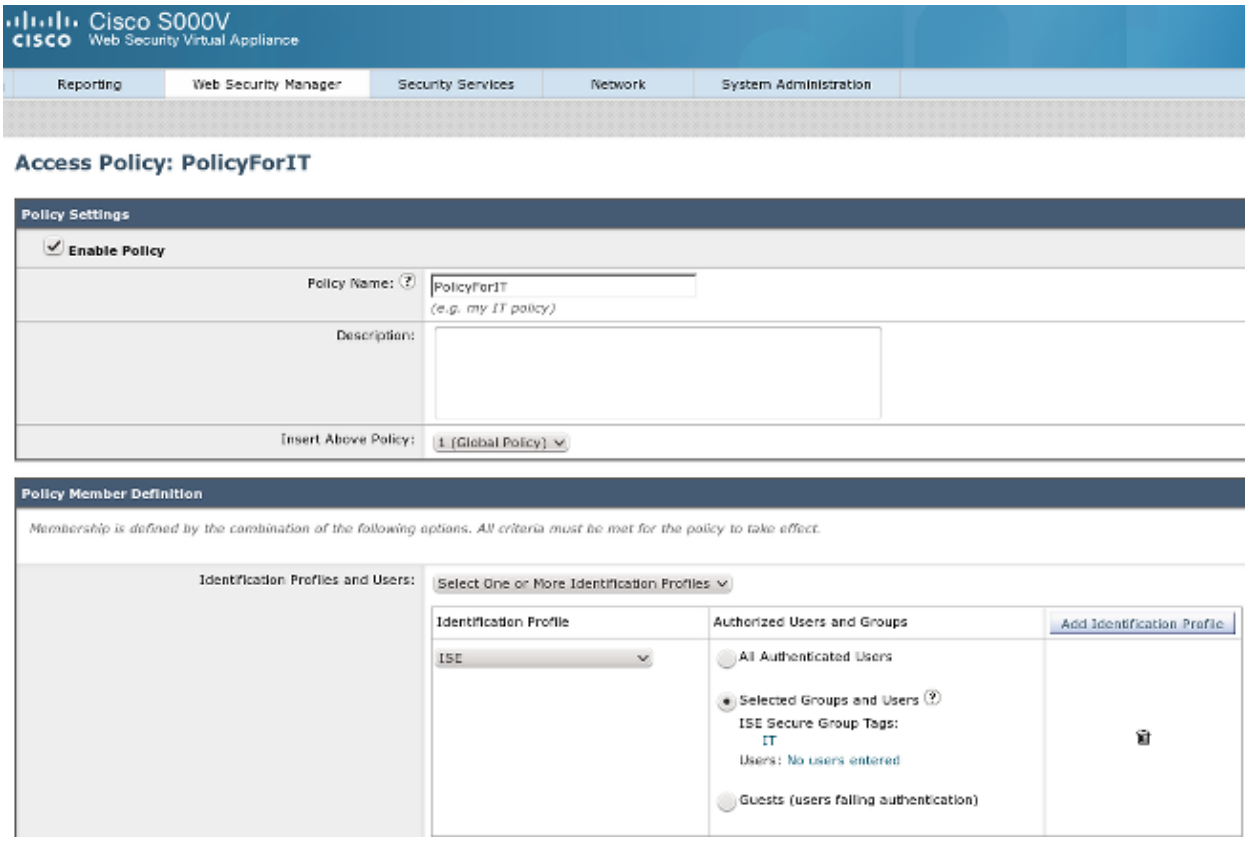
Step 4. ISE Identification Profiles

Choose **Web Security Manager > Identification profiles** in order to add a new profile for ISE. For "*Identification and Authentication*" use "*Transparently identify users with ISE*".

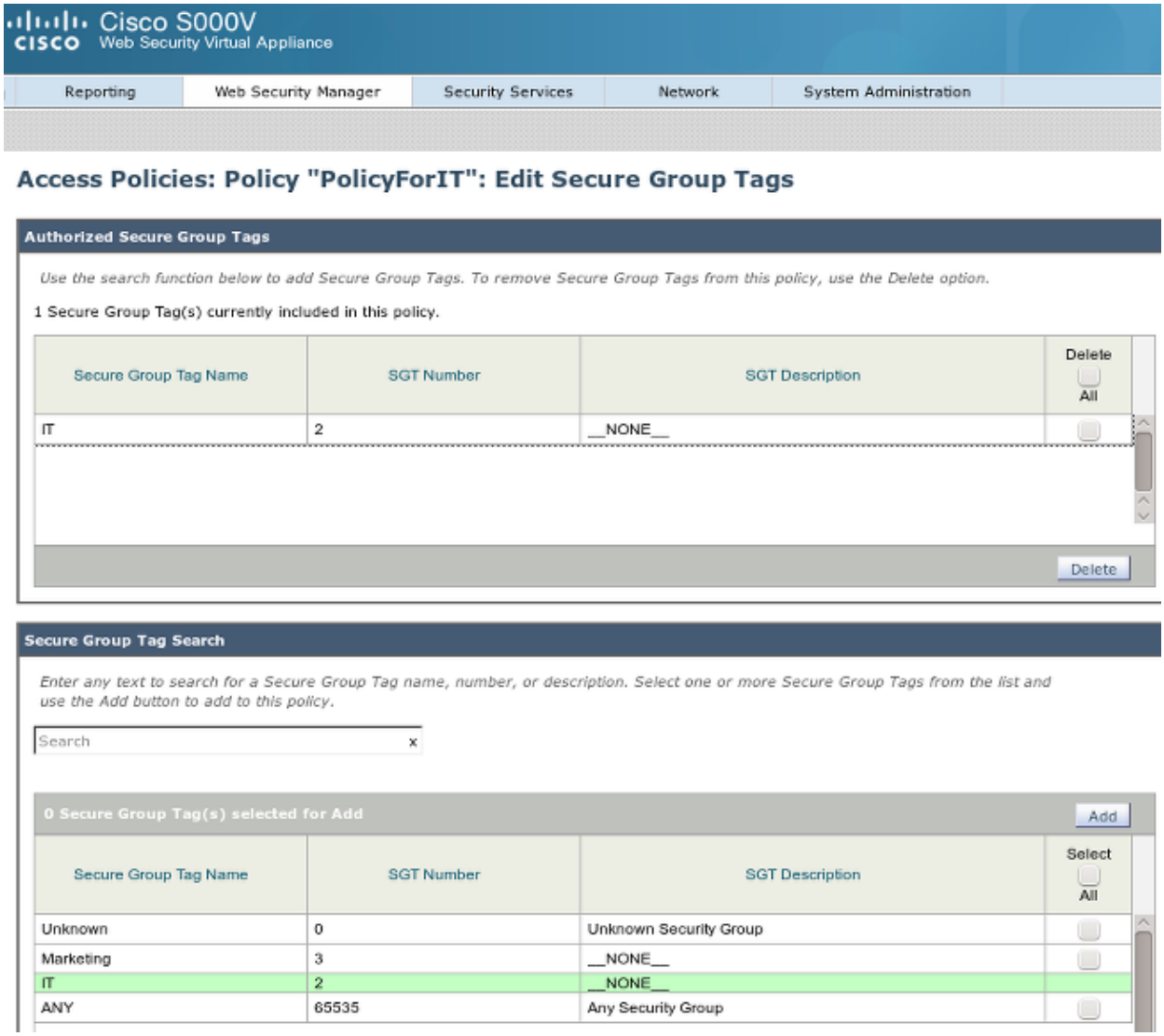


Step 5. Access the Policy Based on the SGT Tag

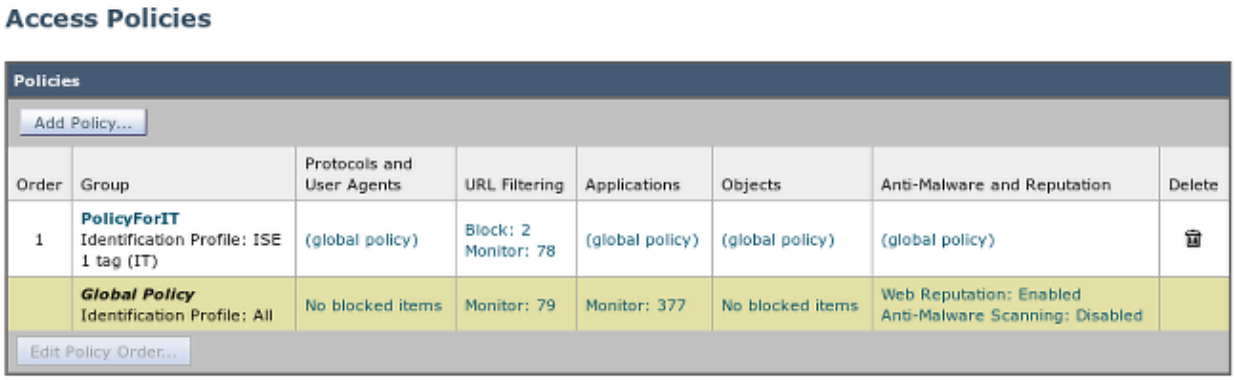
Choose **Web Security Manager > Access Policies** in order to add a new policy. Membership uses the ISE profile:



For Selected Groups and Users the SGT tag 2 will be added (IT):



The policy denies access to all sports sites for users which belong to SGT IT:

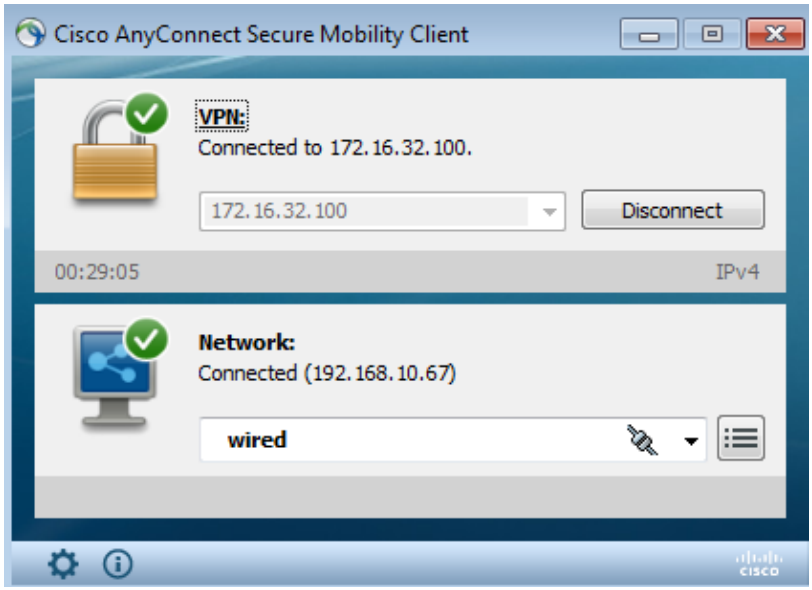


Verify

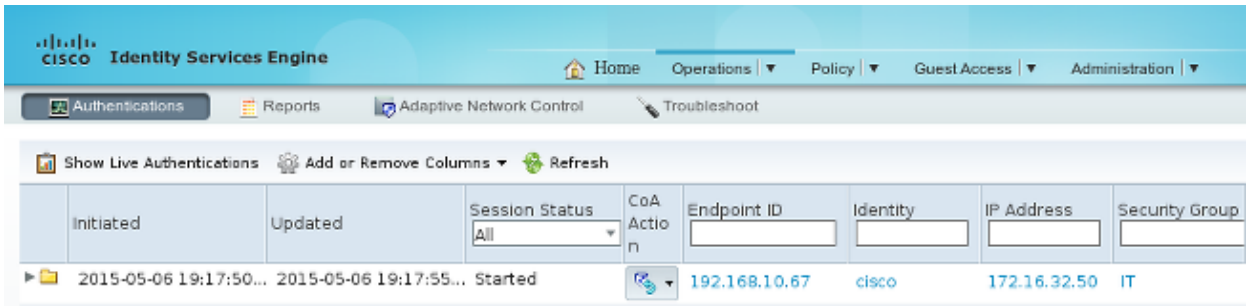
Use this section in order to confirm that your configuration works properly.

Step 1. VPN Session

The VPN user initiates a VPN session towards the ASA-VPN:



The ASA-VPN uses ISE for authentication. ISE creates a session and assigns the SGT tag 2 (IT):



After successful authentication, the ASA-VPN creates a VPN session with the SGT tag 2 (returned in Radius Access-Accept in 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
```

Since the link between the ASA-VPN and the ASA-FW is not TrustSec enabled, the ASA-VPN sends untagged frames for that traffic (would not be able to GRE encapsulate Ethernet frames with the

CMD/TrustSec field injected).

Step 2. Session Information Retrieved by the WSA

At this stage, the WSA should receive the mapping between the IP address, username, and SGT (via pxGrid protocol):

```
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
[]>
```

Step 3. Traffic Redirection to the WSA

The VPN user initiates a connection to sport.pl, which is intercepted by the ASA-FW:

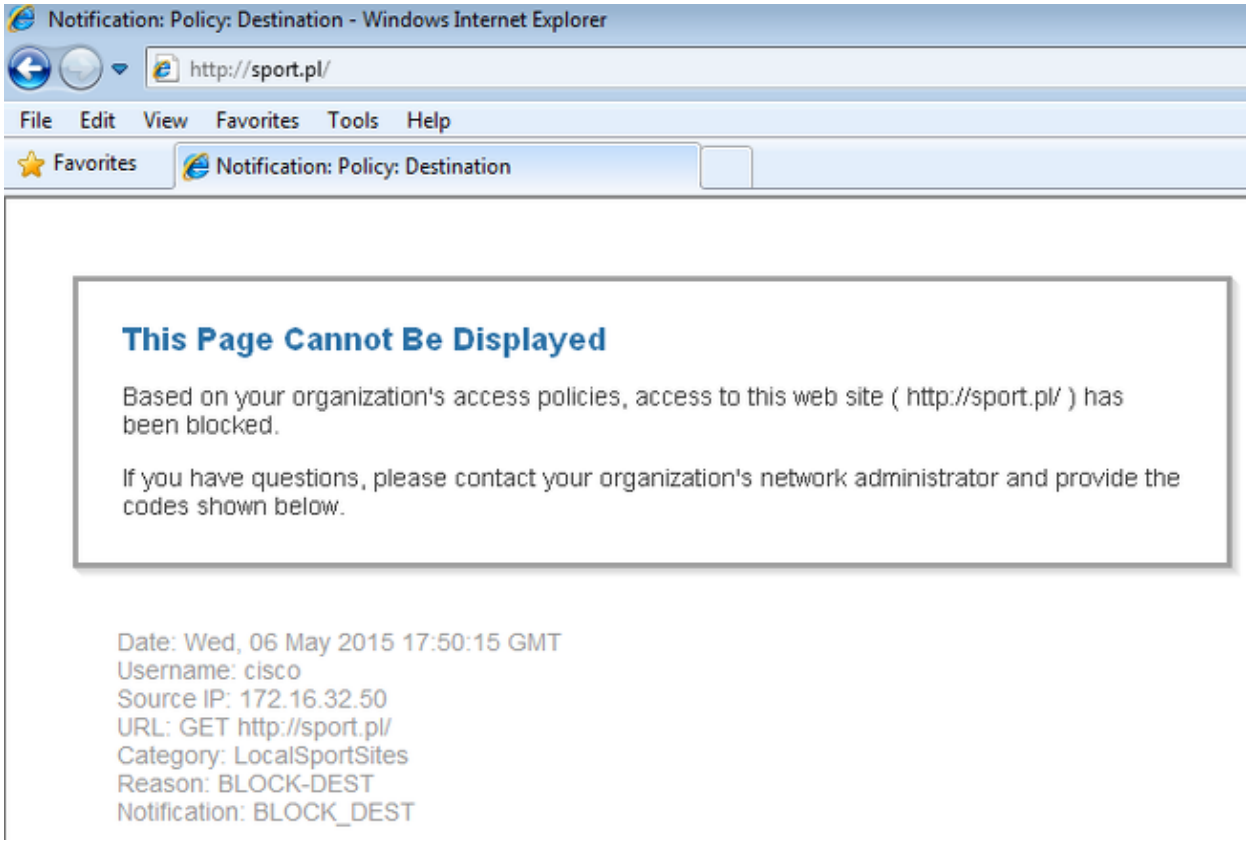
```
asa-fw# show wccp

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
```

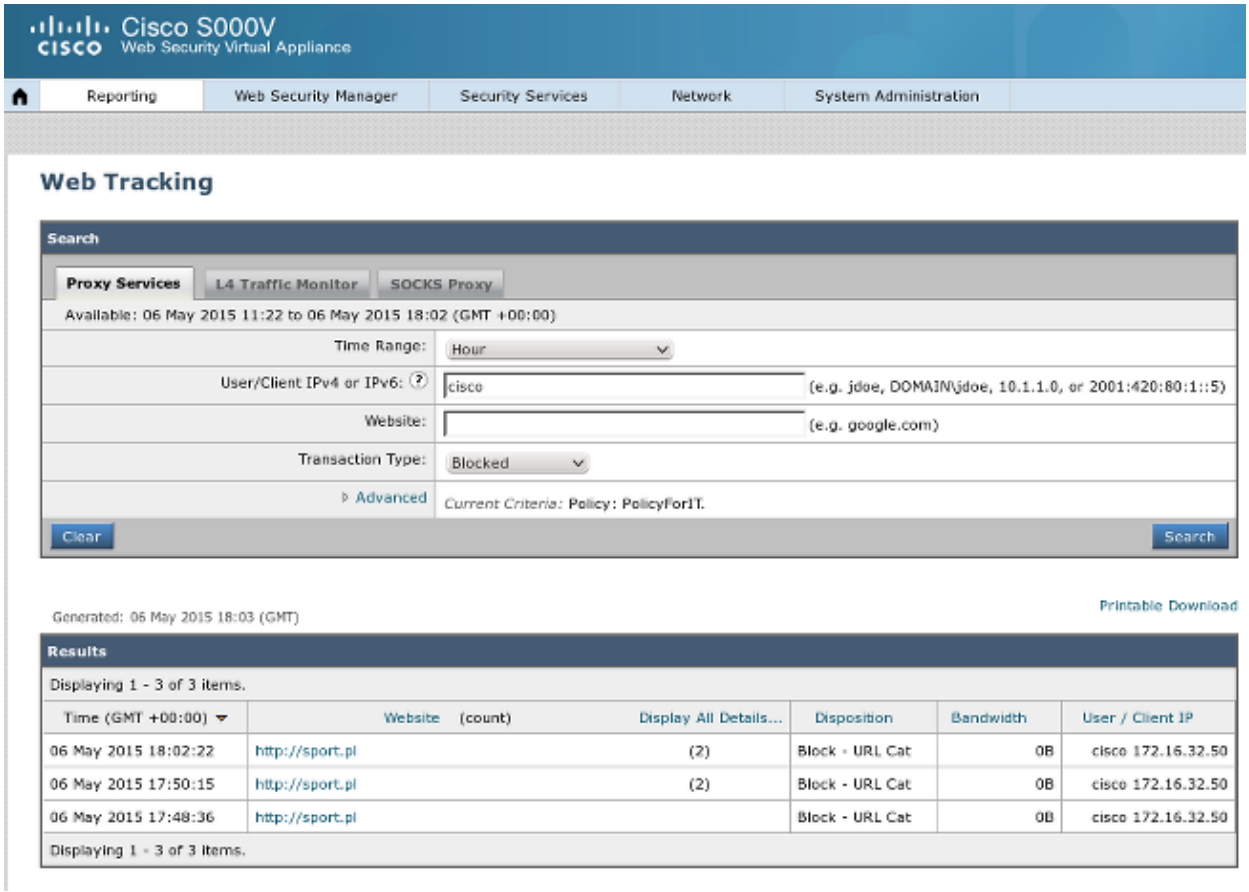
and tunneled in GRE to the WSA (notice that the WCCP router-id is the highest IP address configured):

```
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
```

The WSA continues the TCP handshake and processes the GET request. As a result, the policy named PolicyForIT is hit and traffic is blocked:



That is confirmed by the WSA Report:



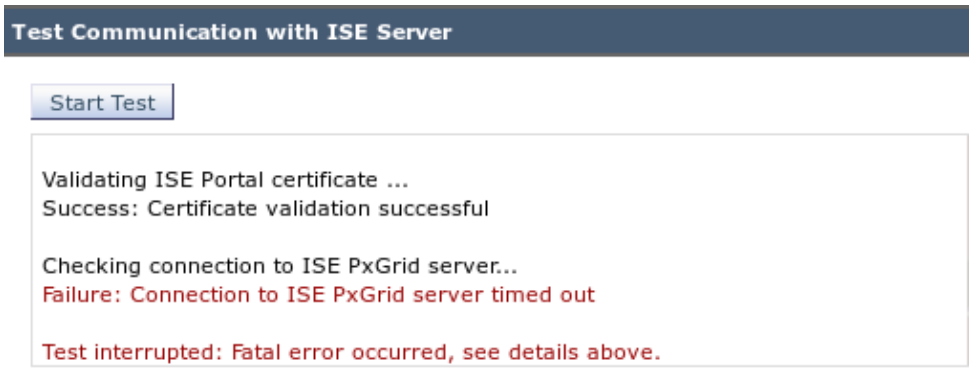
Notice that ISE displays the username.

Troubleshoot

This section provides information you can use in order to troubleshoot your configuration.

Incorrect Certificates

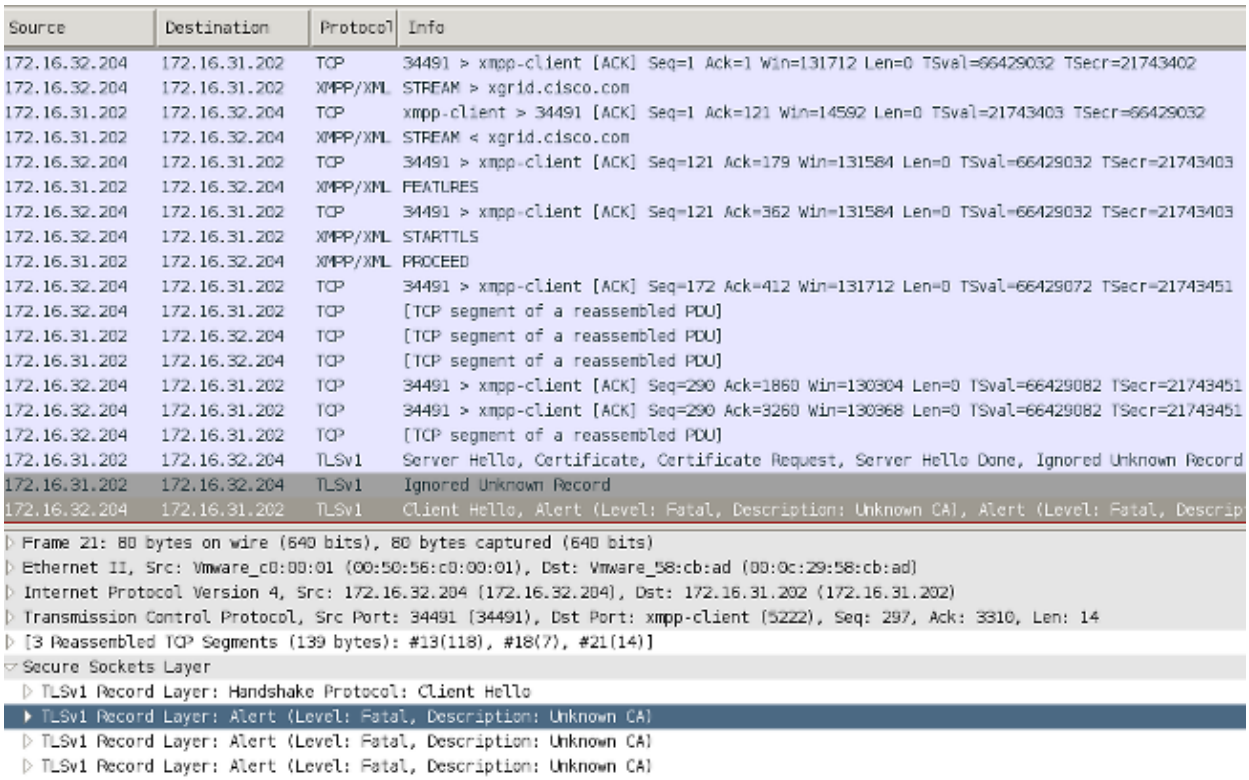
When the WSA is not correctly initialized (certificates), test for ISE connection failure:



The ISE pxgrid-cm.log reports:

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

The reason for the failure can be seen with Wireshark:



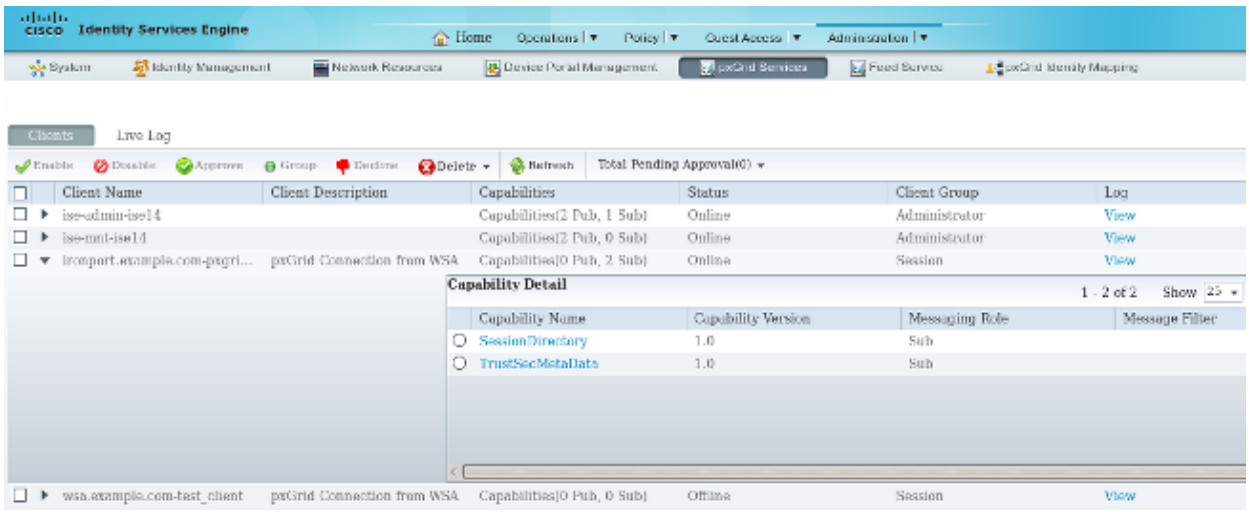
For an SSL session used to protect Extensible Messaging and Presence Protocol (XMPP) exchange (used by pxGrid), the Client reports SSL failure because of an unknown certificate chain presented by the server.

Correct Scenario

For the correct scenario, the ISE pxgrid-controller.log logs:

```
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
```

Also, the ISE GUI presents the WSA as a subscriber with the correct capabilities:



Related Information

- **ASA Version 9.2.1 VPN Posture with ISE Configuration Example**

- **WSA 8.7 Users Guide**
- **ASA and Catalyst 3750X Series Switch TrustSec Configuration Example and Troubleshoot Guide**
- **Cisco TrustSec Switch Configuration Guide: Understanding Cisco TrustSec**
- **Configuring an External Server for Security Appliance User Authorization**
- **Cisco ASA Series VPN CLI Configuration Guide, 9.1**
- **Cisco Identity Services Engine User Guide, Release 1.2**
- **Technical Support & Documentation - Cisco Systems**

Updated: Jul 30, 2015 Document ID: 119212
