Konfigurieren der WSA-Integration mit der ISE für TrustSec-basierte Services

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie die Web Security Appliance (WSA) in die Identity Services Engine (ISE) integriert wird. ISE Version 1.3 unterstützt die neue API pxGrid. Dieses moderne und flexible Protokoll unterstützt Authentifizierung, Verschlüsselung und Privilegien

(Gruppen), was eine einfache Integration mit anderen Sicherheitslösungen ermöglicht.

WSA Version 8.7 unterstützt das pxGrid-Protokoll und kann Kontextidentitätsinformationen von der ISE abrufen. So können Sie mit der WSA Richtlinien erstellen, die auf von der ISE abgerufenen TrustSec Security Group Tag (SGT)-Gruppen basieren.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Erfahrungen mit der Cisco ISE-Konfiguration und grundlegende Kenntnisse zu folgenden Themen zu verfügen:

- ISE-Bereitstellungen und Autorisierungskonfiguration
- Adaptive Security Appliance (ASA) CLI-Konfiguration für TrustSec- und VPN-Zugriff
- WSA-Konfiguration
- Grundlegende Kenntnisse von TrustSec-Bereitstellungen

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Microsoft Windows 7
- Cisco ISE Software Version 1.3 oder höher
- Cisco AnyConnect Mobile Security Version 3.1 und höher
- Cisco ASA Version 9.3.1 oder höher
- Cisco WSA Version 8.7 oder höher

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konfigurieren

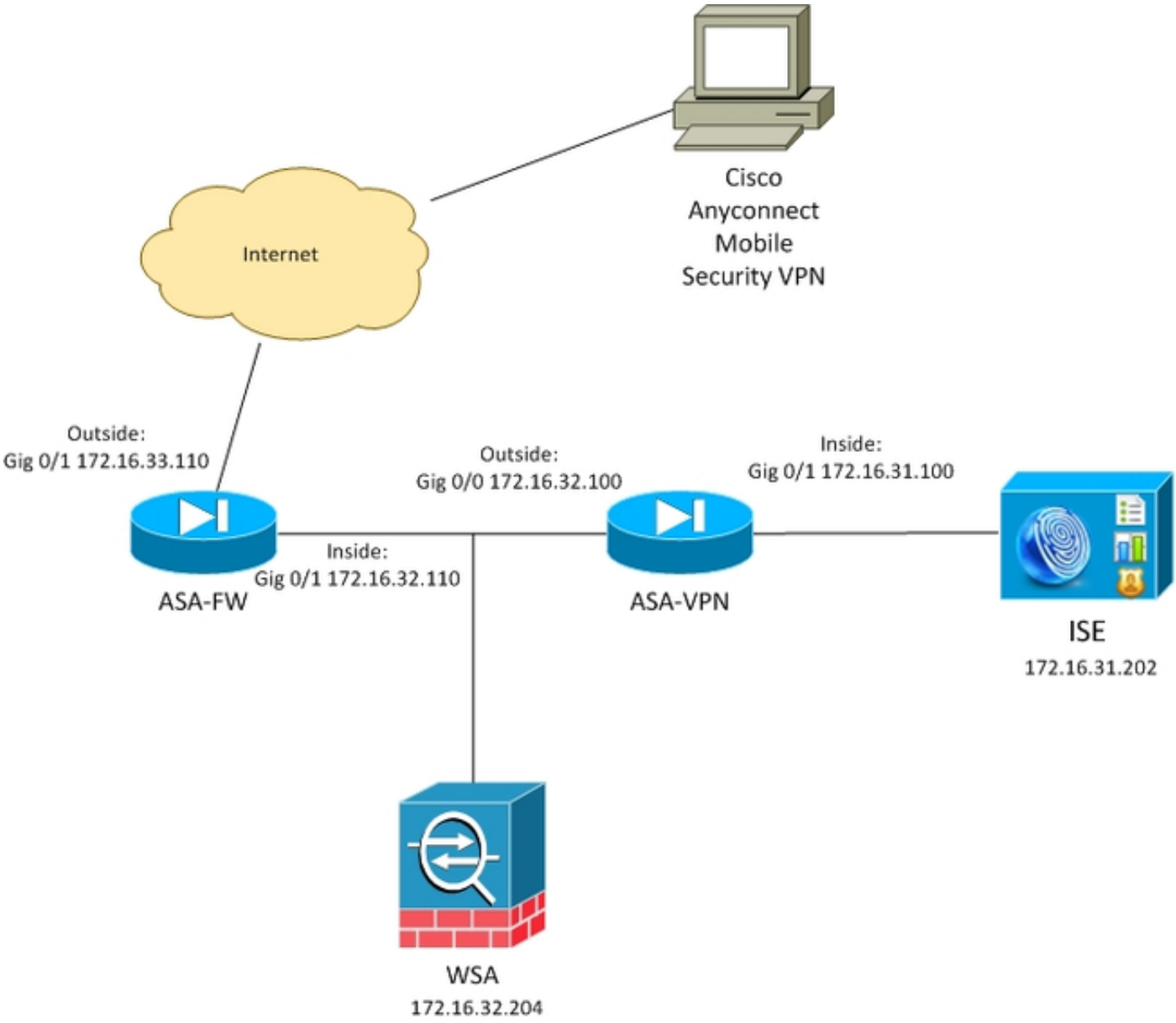
> **Hinweis**: Verwenden Sie das Command Lookup Tool (nur registrierte Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

Netzwerkdiagramm und Datenverkehrsfluss

TrustSec-SGT-Tags werden von der ISE als Authentifizierungsserver für alle Benutzertypen zugewiesen, die auf das Unternehmensnetzwerk zugreifen. Dies betrifft kabelgebundene/Wireless-Benutzer, die sich über 802.1x- oder ISE-Gastportale authentifizieren. Remote-VPN-Benutzer, die ISE für die Authentifizierung verwenden.

Bei der WSA spielt es keine Rolle, wie der Benutzer auf das Netzwerk zugegriffen hat.

Dieses Beispiel zeigt eine Remote-VPN-Benutzer, die die Sitzung auf dem ASA-VPN beenden. Diesen Benutzern wurde ein bestimmter SGT-Tag zugewiesen. Der gesamte HTTP-Datenverkehr zum Internet wird von der ASA-FW (Firewall) abgefangen und zur Überprüfung an die WSA umgeleitet. Die WSA verwendet das Identitätsprofil, mit dem Benutzer anhand des SGT-Tags klassifiziert und auf dieser Grundlage Zugriffs- oder Entschlüsselungsrichtlinien erstellt werden können.



Der detaillierte Fluss ist:

1. Der AnyConnect VPN-Benutzer beendet die SSL-Sitzung (Secure Sockets Layer) auf dem ASA-VPN. ASA-VPN ist für TrustSec konfiguriert und verwendet ISE für die Authentifizierung von VPN-Benutzern. Dem authentifizierten Benutzer wird ein SGT-Tag-Wert = 2 (Name = IT) zugewiesen. Der Benutzer erhält eine IP-Adresse aus dem Netzwerk 172.16.32.0/24 (in diesem Beispiel 172.16.32.50).
2. Der Benutzer versucht, auf die Webseite im Internet zuzugreifen. Die ASA-FW ist für das Web Cache Communication Protocol (WCCP) konfiguriert, das den Datenverkehr zur WSA umleitet.
3. Die WSA ist für die ISE-Integration konfiguriert. Es verwendet pxGrid, um Informationen von

der ISE herunterzuladen: Benutzer-IP-Adresse 172.16.32.50 wurde SGT-Tag 2 zugewiesen.
4. Die WSA verarbeitet die HTTP-Anforderung des Benutzers und trifft die Zugriffsrichtlinie PolicyForIT. Diese Richtlinie ist so konfiguriert, dass der Datenverkehr zu den Sportstätten blockiert wird. Alle anderen Benutzer (die nicht zum SGT 2 gehören) treffen die Standard-Zugriffsrichtlinie und haben vollen Zugriff auf die Sportwebsites.

ASA-VPN

Dies ist ein für TrustSec konfiguriertes VPN-Gateway. Detaillierte Konfigurationen werden in diesem Dokument nicht behandelt. Weitere Informationen finden Sie in den folgenden Beispielen:

- ASA und Catalyst Switch der Serie 3750X - TrustSec-Konfigurationsbeispiel und Leitfaden zur Fehlerbehebung
- Konfigurationsbeispiel für ASA Version 9.2 - VPN-SGT-Klassifizierung und -Durchsetzung

ASA-FW

Die ASA-Firewall ist für die WCCP-Umleitung an die WSA verantwortlich. Dieses Gerät kennt TrustSec nicht.

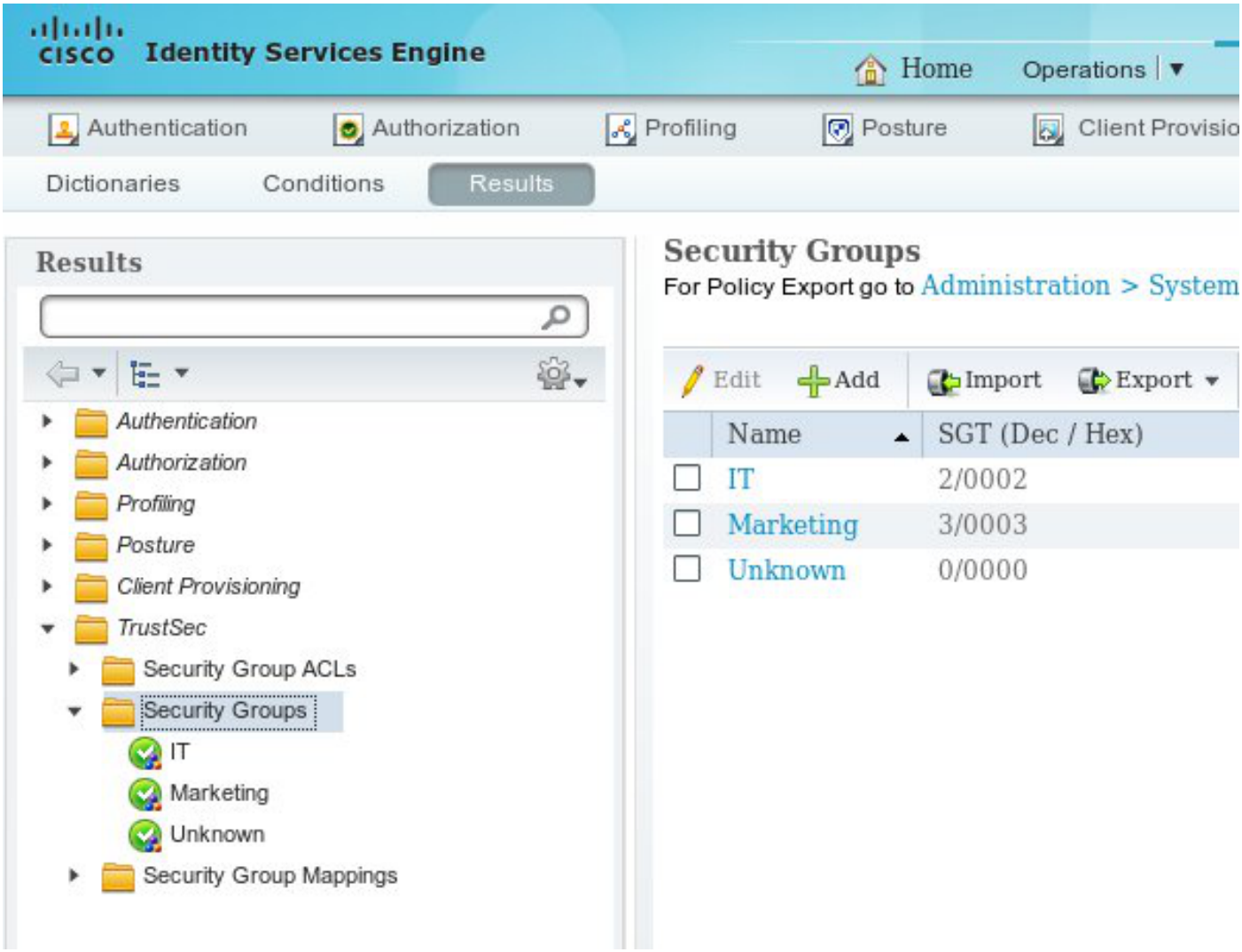
```
interface GigabitEthernet0/0
 nameif outside
 security-level 100
 ip address 172.16.33.110 255.255.255.0

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

Die ISE ist ein zentraler Punkt in der TrustSec-Bereitstellung. Er weist allen Benutzern, die auf das Netzwerk zugreifen und sich dort authentifizieren, SGT-Tags zu. Die für die Basiskonfiguration erforderlichen Schritte werden in diesem Abschnitt aufgelistet.

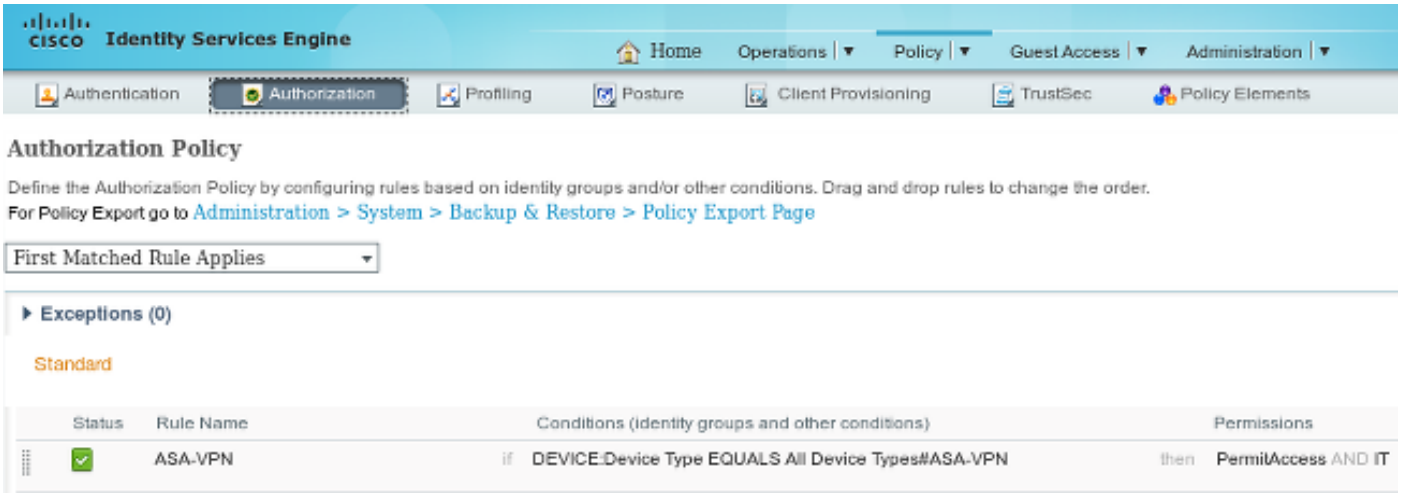
Schritt 1: SGT für IT und andere Gruppen

Wählen Sie **Policy > Results > Security Group Access > Security Groups (Richtlinien > Ergebnisse > Sicherheitsgruppenzugriff > Sicherheitsgruppen) aus,** und erstellen Sie das SGT:



Schritt 2: Autorisierungsregel für VPN-Zugriff, der SGT = 2 (IT) zuweist

Wählen Sie **Policy > Authorization** *(Richtlinie > Autorisierung),* und erstellen Sie eine Regel für den Remote-VPN-Zugriff. Alle über ASA-VPN eingerichteten VPN-Verbindungen erhalten vollständigen Zugriff (PermitAccess) und werden mit dem SGT-Tag 2 (IT) versehen.



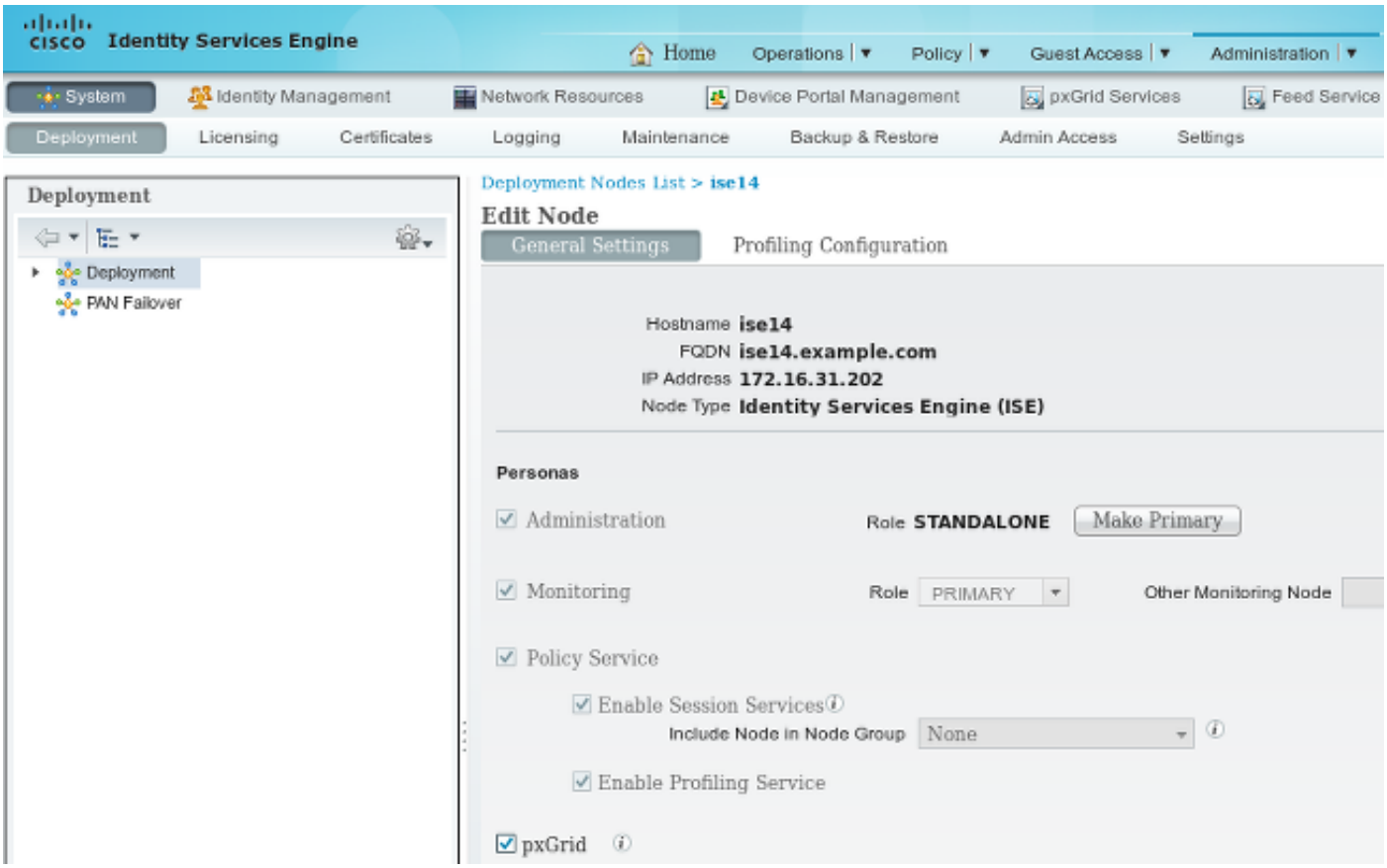
Schritt 3: Netzwerkgerät hinzufügen und PAC-Datei für ASA-VPN erstellen

Um die ASA-VPN zur TrustSec-Domäne hinzuzufügen, muss die Proxy-PAC-Datei (Auto Config) manuell generiert werden. Diese Datei wird auf die ASA importiert.

Dies kann über **Administration > Network Devices** konfiguriert werden. Scrollen Sie nach dem Hinzufügen der ASA zu den TrustSec-Einstellungen, und generieren Sie die PAC-Datei. Die Details dazu werden in einem separaten (referenzierten) Dokument beschrieben.

Schritt 4: pxGrid-Rolle aktivieren

Wählen Sie **Administration > Deployment** (Administration > Bereitstellung), um die pxGrid-Rolle zu aktivieren.



Schritt 5: Generieren des Zertifikats für Administration und die pxGrid-Rolle

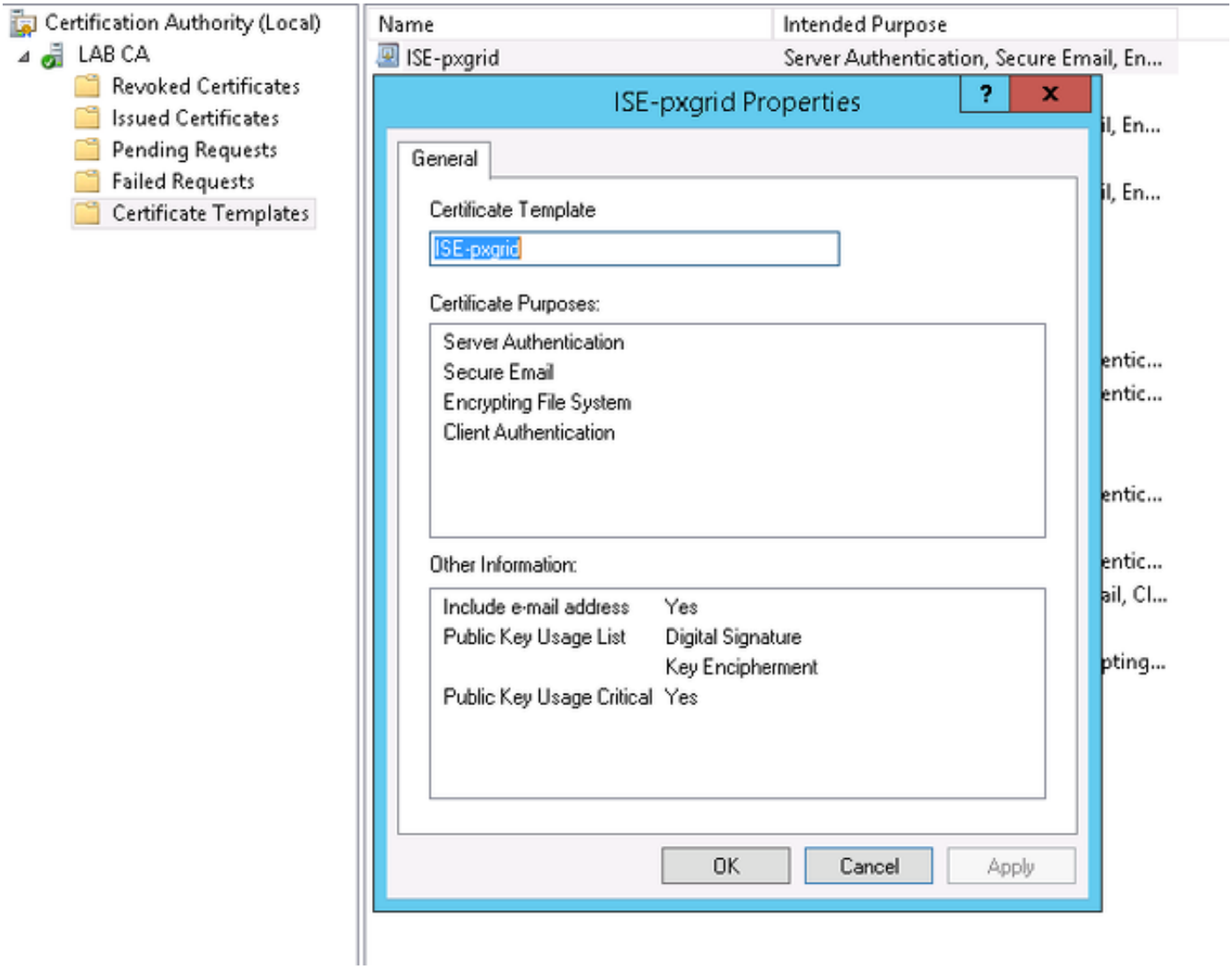
Das pxGrid-Protokoll verwendet die Zertifikatauthentifizierung sowohl für den Client als auch für den Server. Es ist sehr wichtig, die richtigen Zertifikate für die ISE und die WSA zu konfigurieren. Beide Zertifikate sollten den vollqualifizierten Domänennamen (Fully Qualified Domain Name, FQDN) im Betreff und die x509-Erweiterungen für die Client-Authentifizierung und Serverauthentifizierung enthalten. Stellen Sie außerdem sicher, dass der richtige DNS-A-Datensatz sowohl für die ISE als auch für die WSA erstellt wurde und mit dem entsprechenden FQDN übereinstimmt.

Wenn beide Zertifikate von einer anderen Zertifizierungsstelle (Certificate Authority, CA) signiert werden, ist es wichtig, diese Zertifizierungsstellen im vertrauenswürdigen Speicher zu speichern.

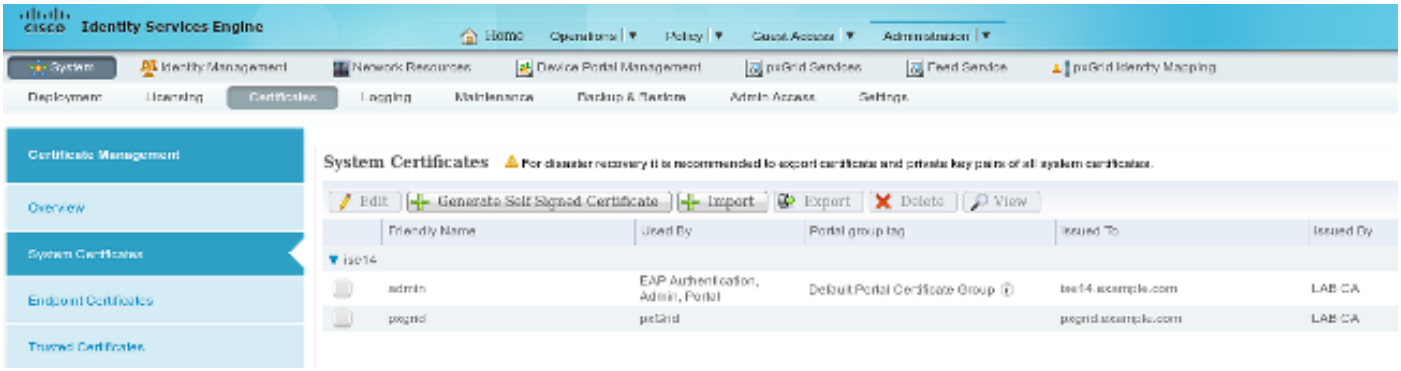
Um Zertifikate zu konfigurieren, wählen Sie **Administration > Certificates (Verwaltung > Zertifikate)**.

Die ISE kann für jede Rolle eine CSR-Anfrage (Certificate Signing Request) generieren. Für die pxGrid-Rolle muss die CSR exportiert und mit einer externen CA signiert werden.

In diesem Beispiel wurde die Microsoft CA mit der folgenden Vorlage verwendet:



Das Endergebnis könnte wie folgt aussehen:



Vergessen Sie nicht, DNS A-Datensätze für ise14.example.com und pxgrid.example.com zu erstellen, die auf 172.16.31.202 verweisen.

Schritt 6: pxGrid-automatische Registrierung

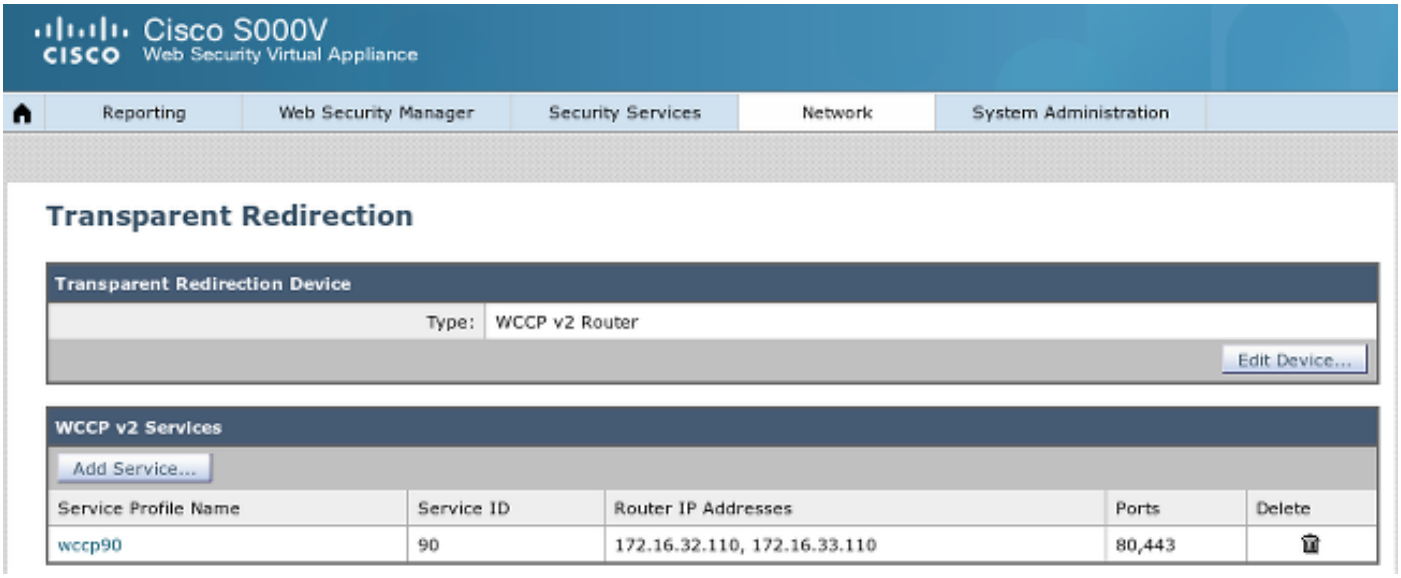
Standardmäßig registriert die ISE nicht automatisch pxGrid-Abonnenten. Dies sollte vom Administrator manuell genehmigt werden. Diese Einstellung sollte für die WSA-Integration geändert werden.

Wählen Sie **Administration > pxGrid Services aus**, und legen Sie **Enable Auto Registration (Automatische Registrierung aktivieren)** fest.

WSA

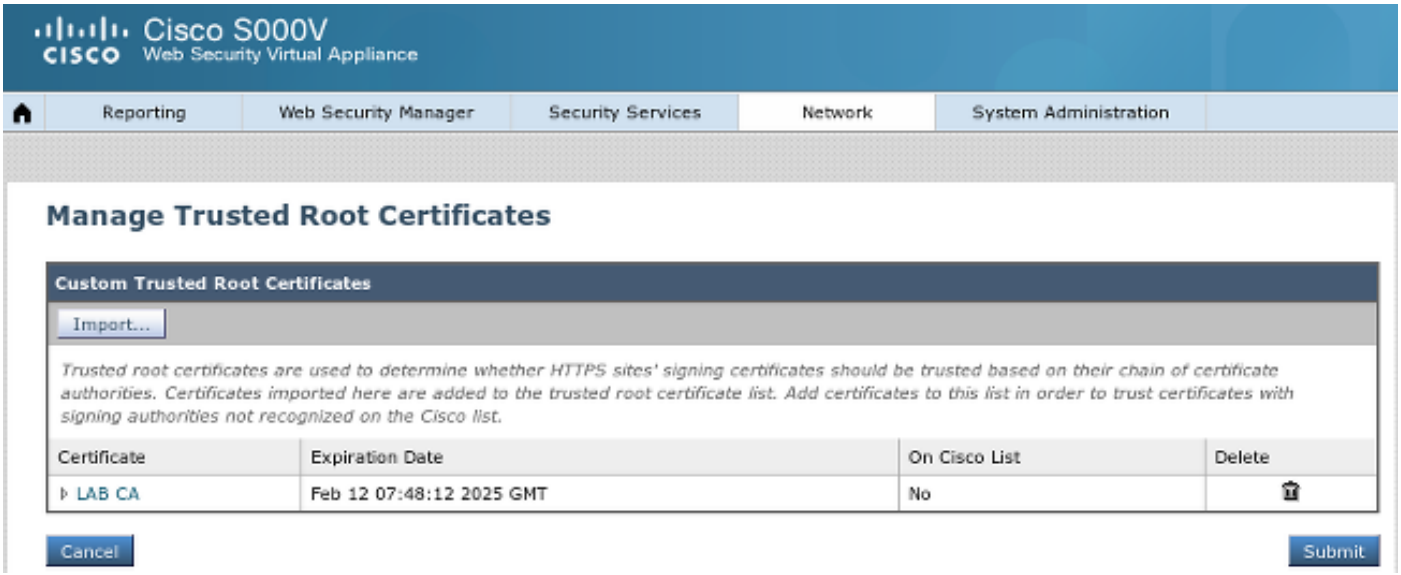
Schritt 1: Transparenter Modus und Umleitung

In diesem Beispiel wird die WSA nur mit der Verwaltungsschnittstelle, dem transparenten Modus und der Umleitung von der ASA konfiguriert:



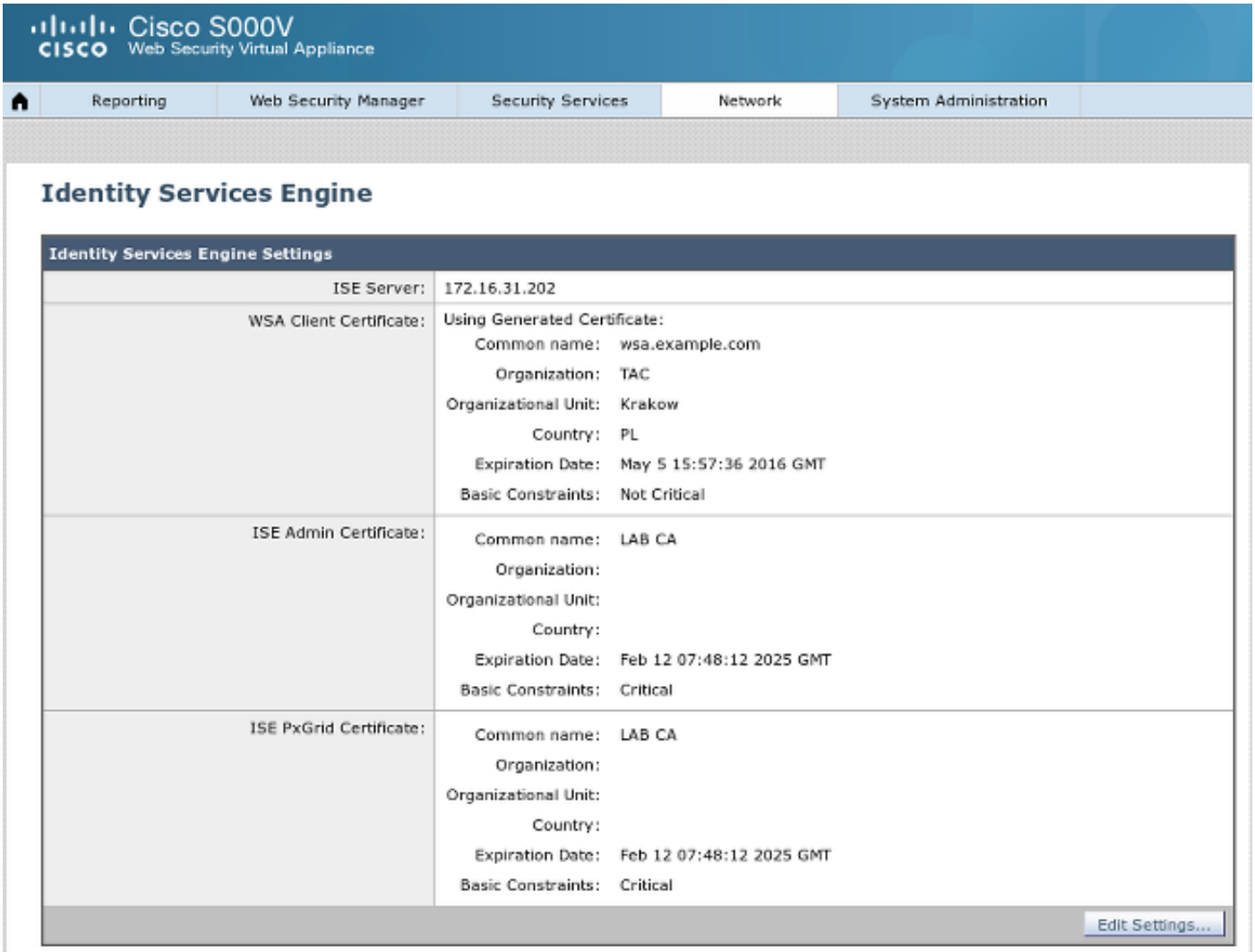
Schritt 2: Zertifikatsgenerierung

Die WSA muss der CA vertrauen, dass sie alle Zertifikate signiert. Wählen Sie **Netzwerk > Certificate Management**, um ein CA-Zertifikat hinzuzufügen:



Außerdem muss ein Zertifikat generiert werden, das die WSA für die Authentifizierung an pxGrid verwendet. Wählen Sie **Network > Identity Services Engine > WSA Client Certificate** aus, um den CSR zu generieren, ihn mit der richtigen CA-Vorlage (ISE-pxgrid) zu signieren und zurückzuimportieren.

Für "ISE Admin Certificate" und "ISE pxGrid Certificate" müssen Sie außerdem das Zertifizierungsstellenzertifikat importieren (um dem von der ISE vorgelegten pxGrid-Zertifikat zu vertrauen):

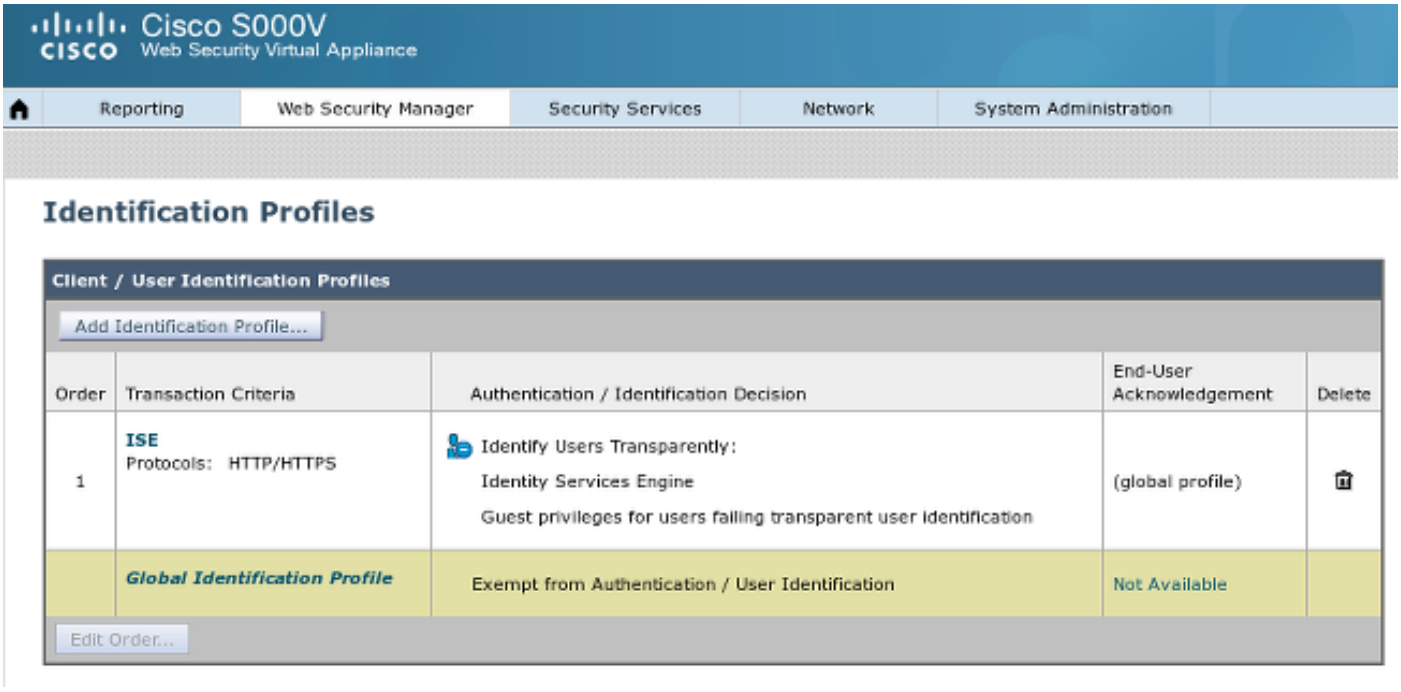


Schritt 3: ISE-Verbindung testen

Wählen Sie **Network > Identity Services Engine (Netzwerk > Identity Services Engine)**, um die Verbindung zur ISE zu testen:

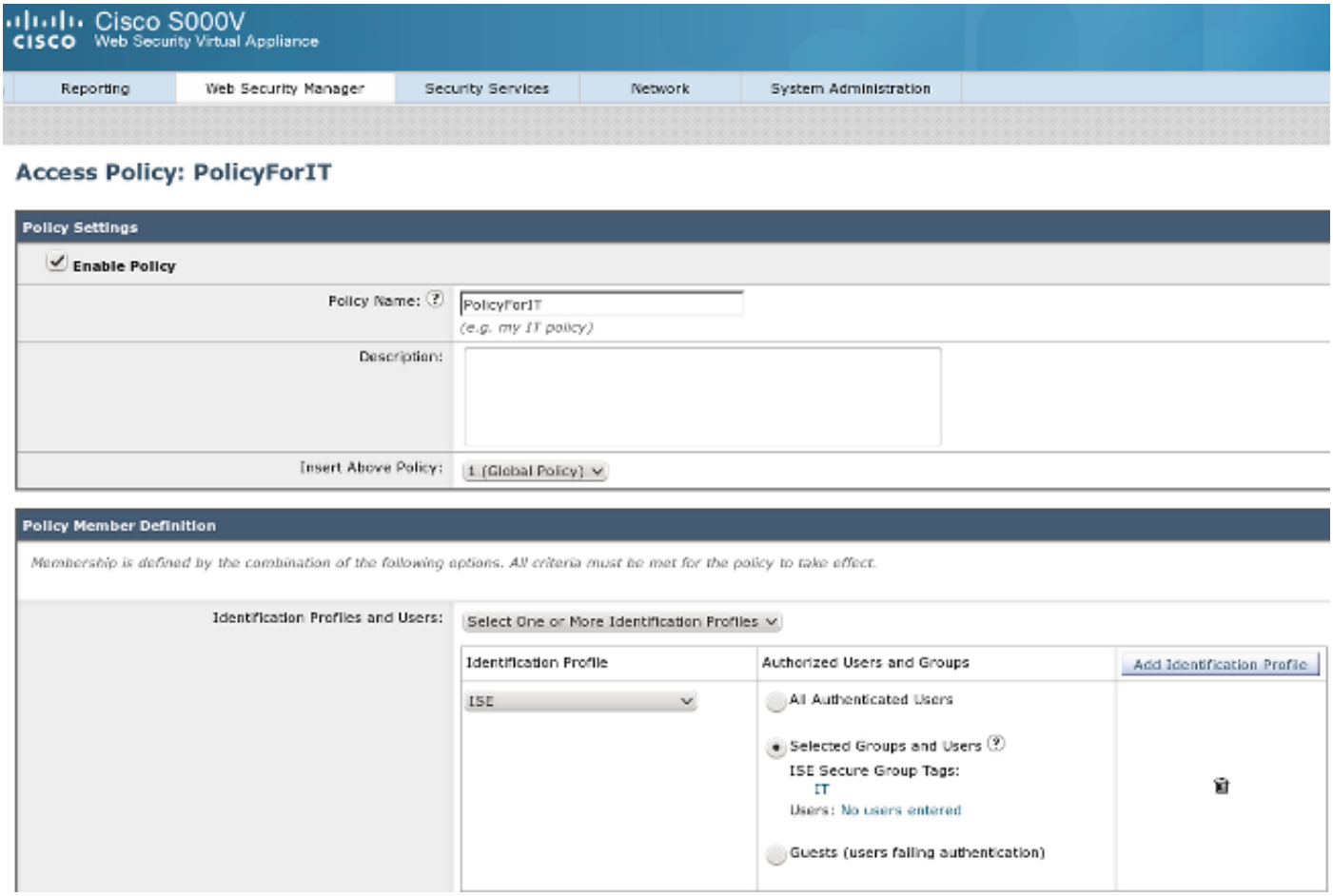
Schritt 4: ISE-Identifikationsprofile

Wählen Sie **Web Security Manager > Identification profiles (Websicherheits-Manager > Identifizierungsprofile)**, um ein neues Profil für die ISE hinzuzufügen. Verwenden Sie für "*Identifikation und Authentifizierung*" "*Benutzer transparent mit ISE identifizieren".*

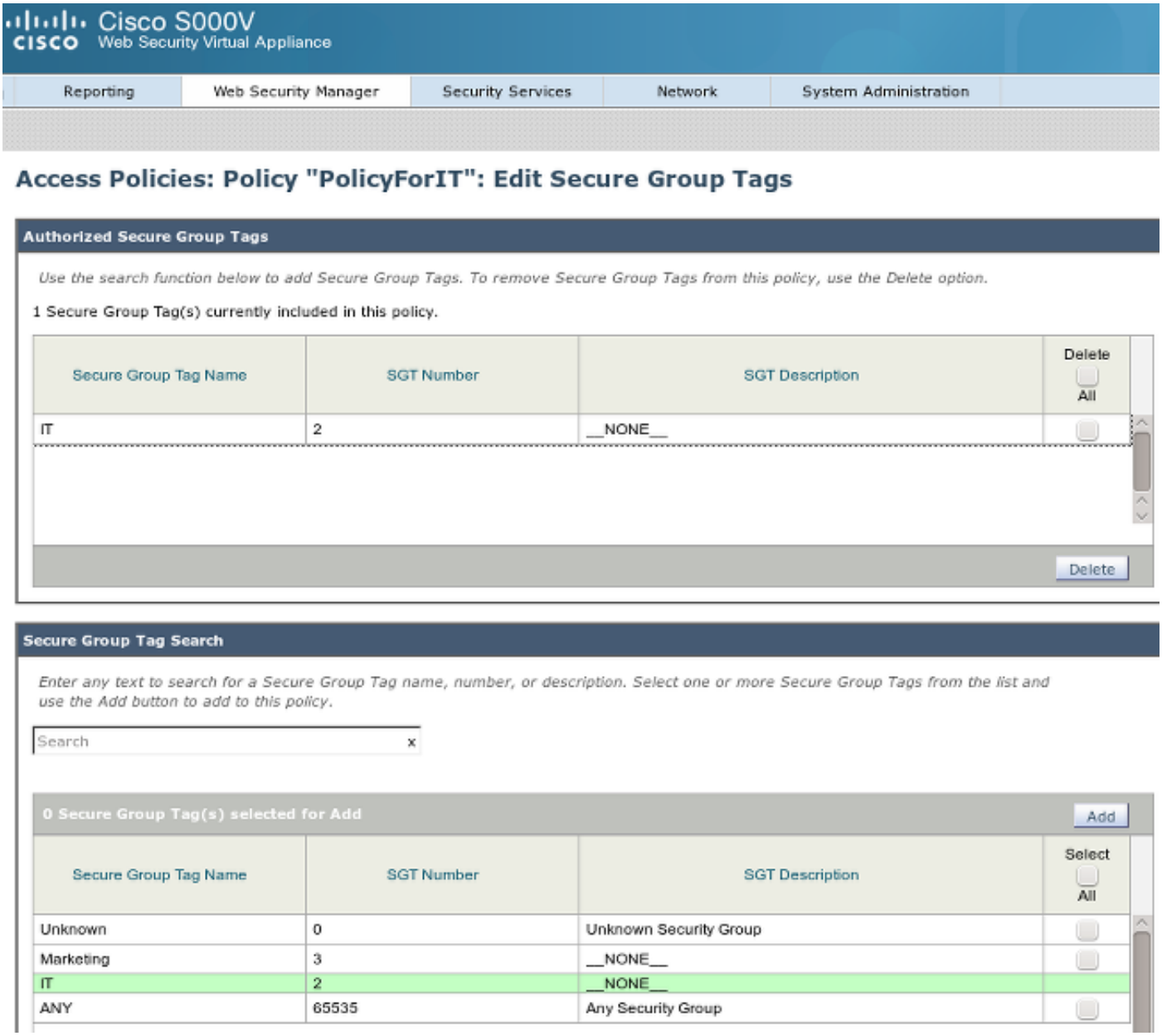


Schritt 5: Zugriff auf die Richtlinie basierend auf dem SGT-Tag

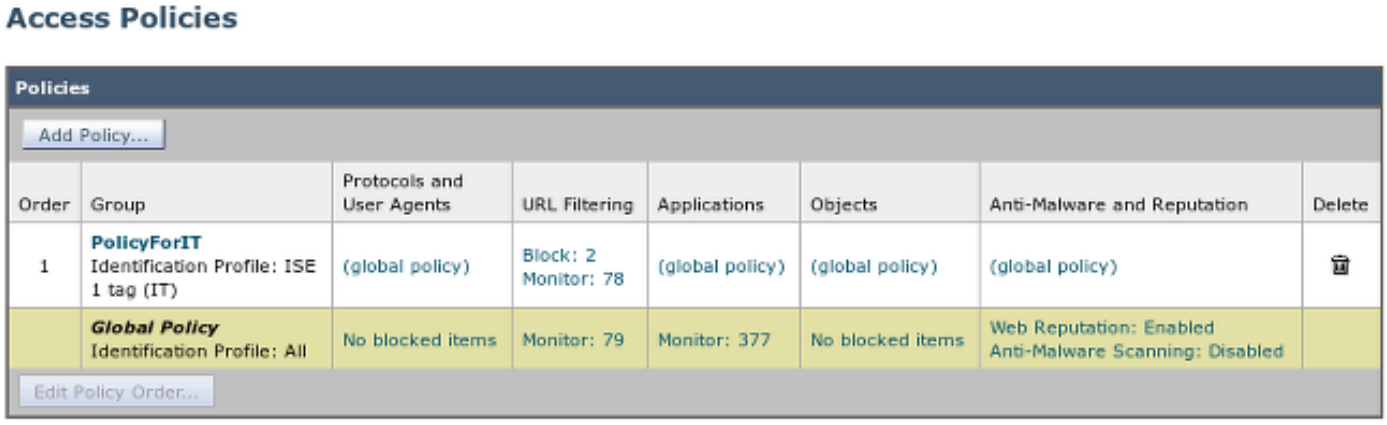
Wählen Sie **Websicherheits-Manager > Zugriffsrichtlinien**, um eine neue Richtlinie hinzuzufügen. Die Mitgliedschaft verwendet das ISE-Profil:



Für ausgewählte Gruppen und Benutzer wird der SGT-Tag 2 hinzugefügt (IT):



Die Richtlinie verweigert Benutzern, die der SGT IT angehören, den Zugriff auf alle Sportstätten:

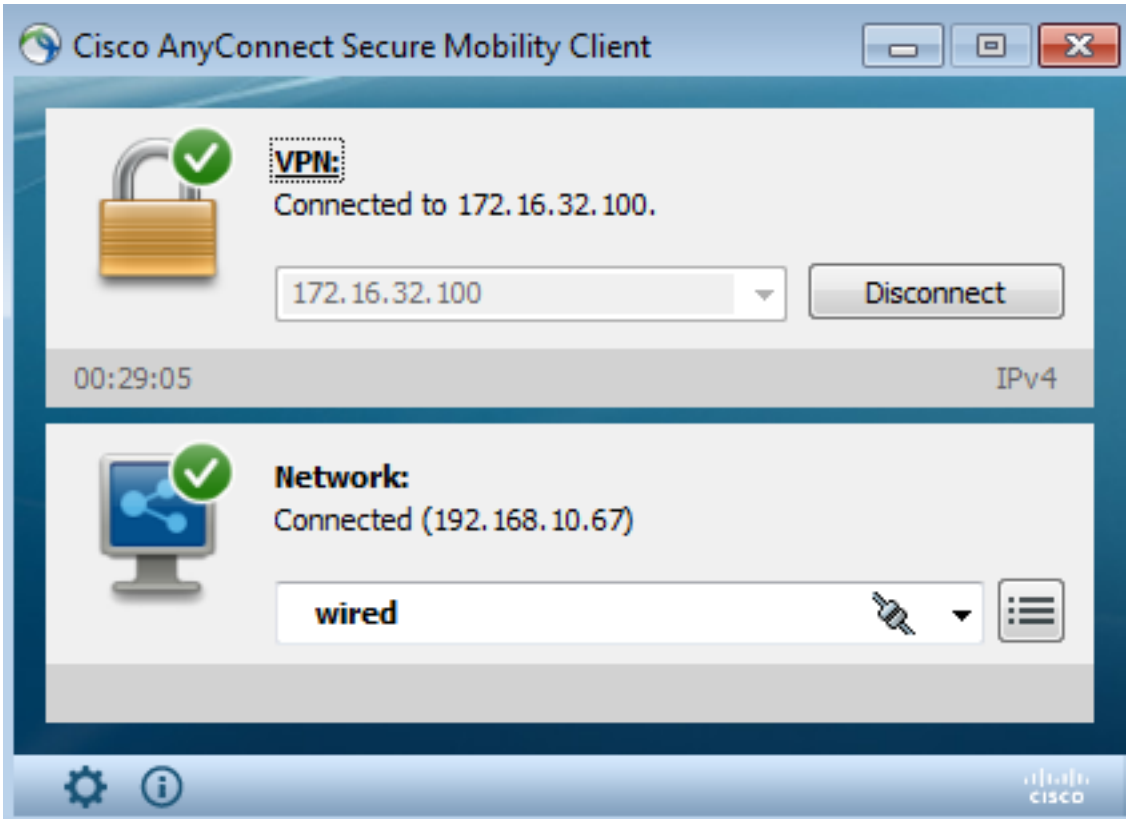


Überprüfen

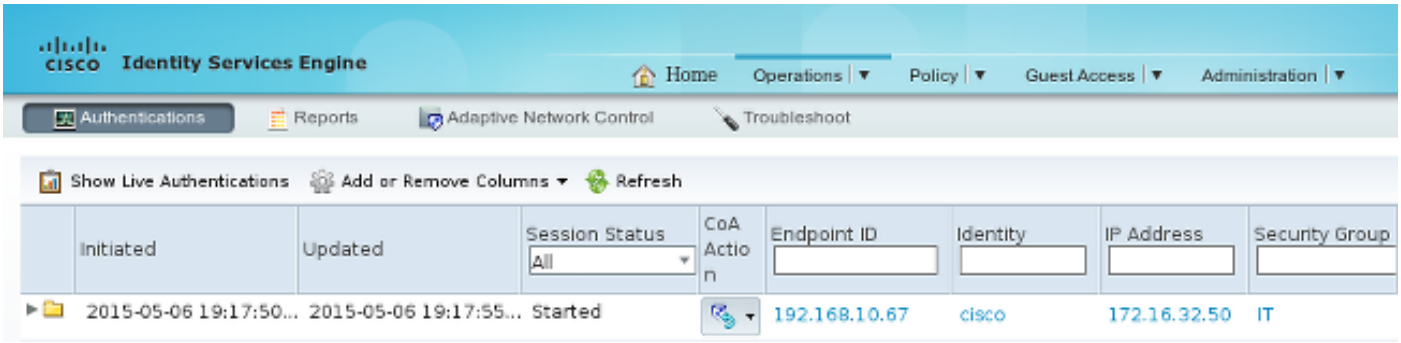
In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Schritt 1: VPN-Sitzung

Der VPN-Benutzer initiiert eine VPN-Sitzung zum ASA-VPN:



ASA-VPN verwendet ISE für die Authentifizierung. Die ISE erstellt eine Sitzung und weist den SGT-Tag 2 (IT) zu:



Nach erfolgreicher Authentifizierung erstellt ASA-VPN eine VPN-Sitzung mit dem SGT-Tag 2 (wird in Radius Access-Accept in cisco-av-pair zurückgegeben):

```
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
```

Da die Verbindung zwischen ASA-VPN und ASA-FW nicht TrustSec-aktiviert ist, sendet das ASA-VPN nicht getaggte Frames für diesen Datenverkehr (kann keine GRE-Kapselung für Ethernet-Frames mit dem CMD/TrustSec-Feld durchführen).

Schritt 2: Von der WSA abgerufene Sitzungsinformationen

Zu diesem Zeitpunkt sollte die WSA die Zuordnung zwischen IP-Adresse, Benutzername und SGT (über das pxGrid-Protokoll) erhalten:

```
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
[]>
```

Schritt 3: Umleitung des Datenverkehrs zur WSA

Der VPN-Benutzer initiiert eine Verbindung zu sport.pl, die von der ASA-FW abgefangen wird:

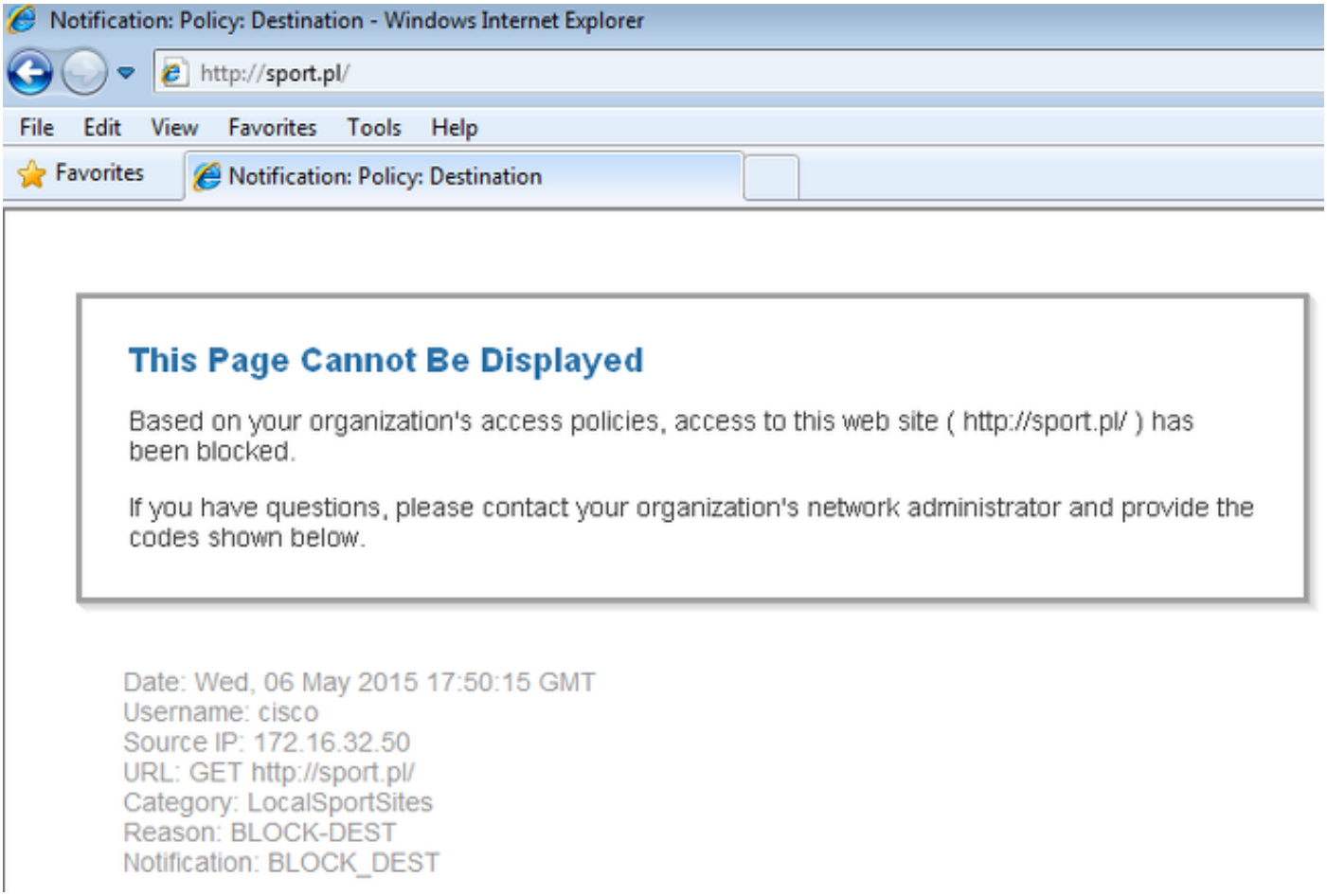
```
asa-fw# show wccp

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
```

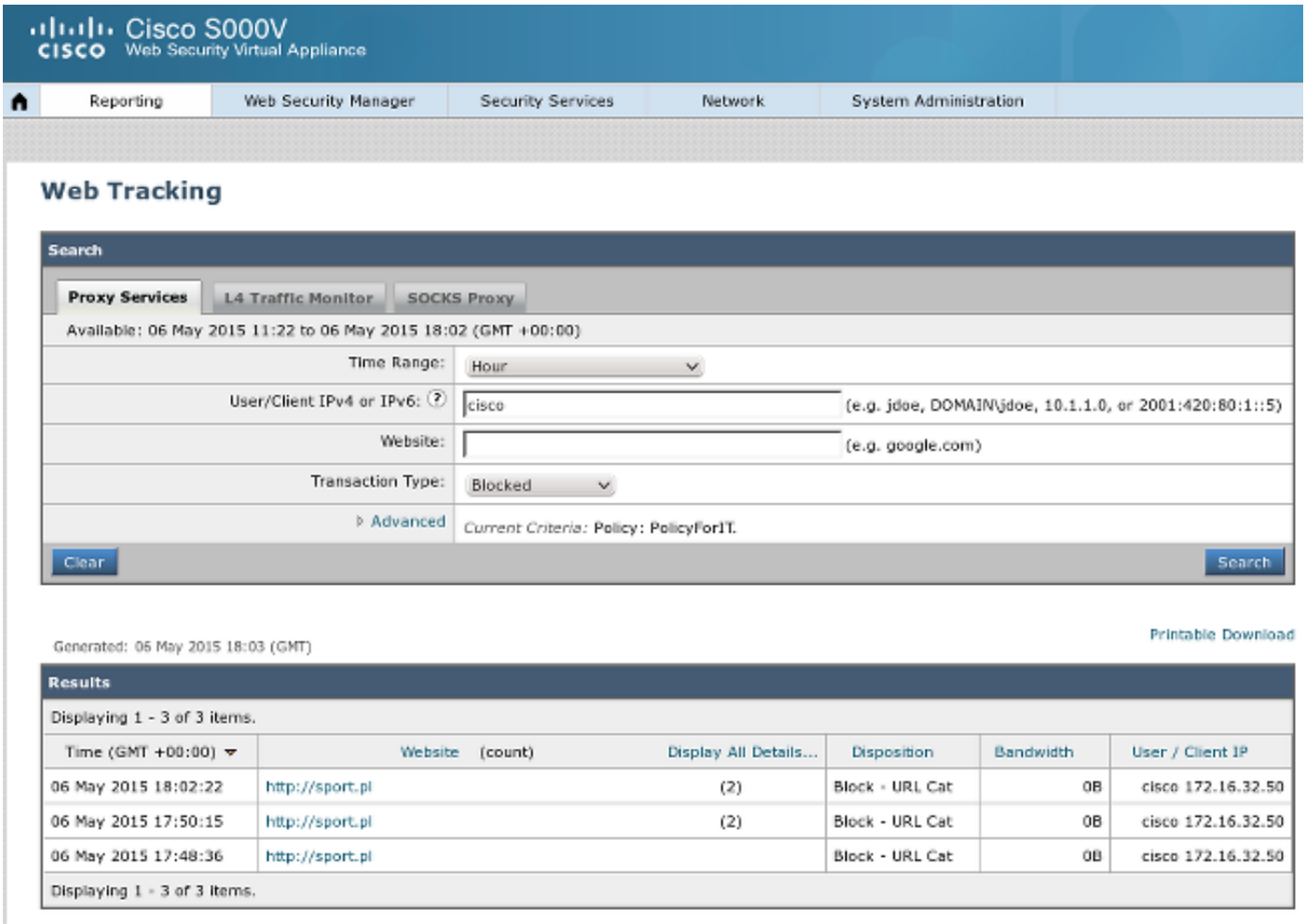
und in GRE an die WSA getunnelt (beachten Sie, dass die WCCP-Router-ID die höchste konfigurierte IP-Adresse ist):

```
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
```

Die WSA setzt den TCP-Handshake fort und verarbeitet die GET-Anforderung. Als Ergebnis wird die PolicyForIT-Richtlinie aufgerufen und der Datenverkehr blockiert:



Dies wird im WSA-Bericht bestätigt:



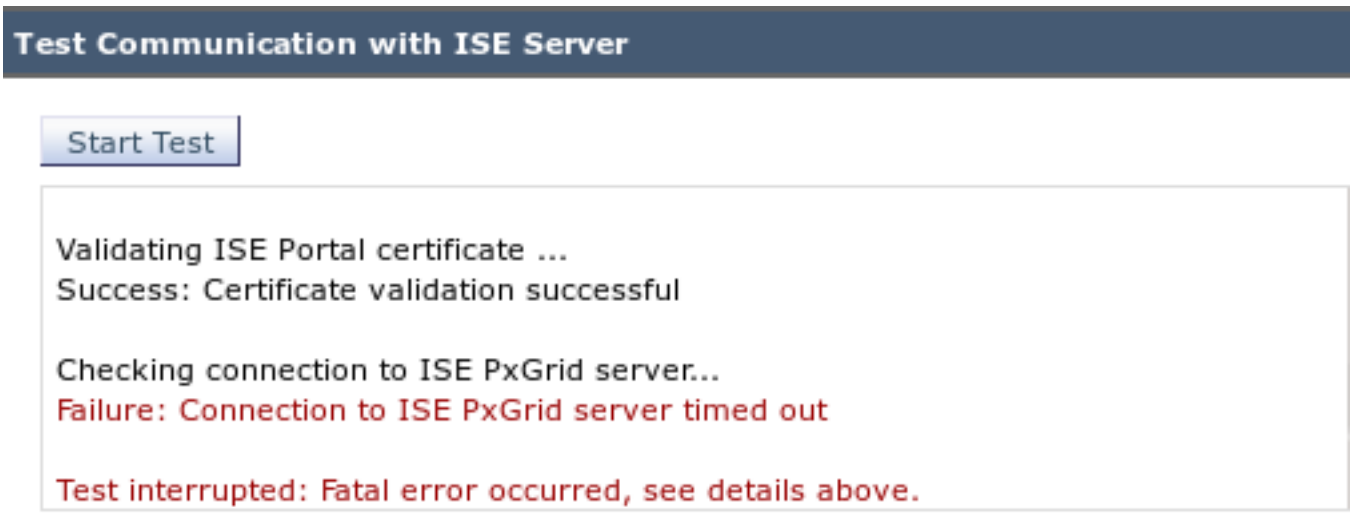
Beachten Sie, dass die ISE den Benutzernamen anzeigt.

Fehlerbehebung

Dieser Abschnitt enthält Informationen, die Sie zur Fehlerbehebung bei Ihrer Konfiguration verwenden können.

Falsche Zertifikate

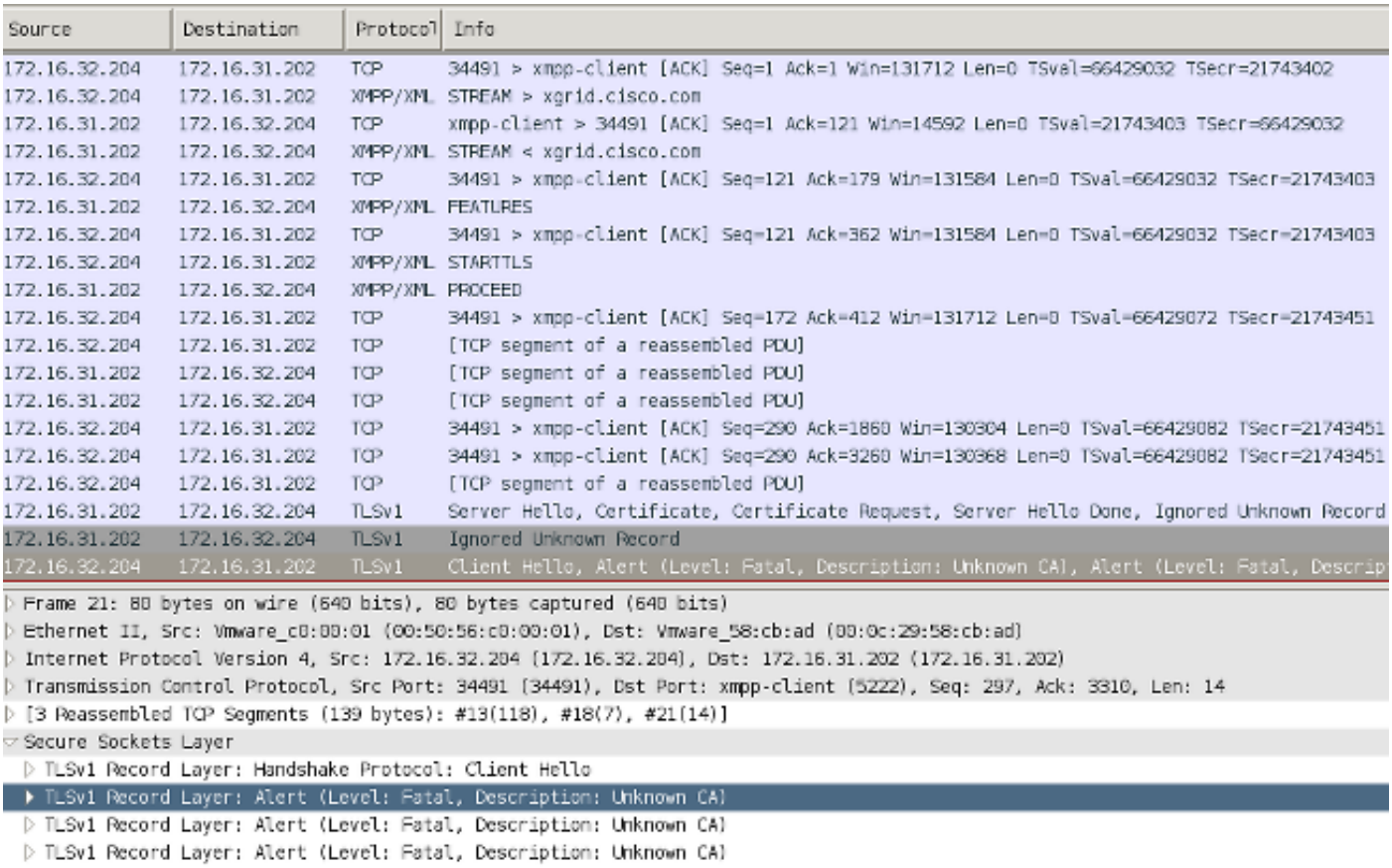
Wenn die WSA nicht korrekt initialisiert ist (Zertifikate), führen Sie einen Test auf ISE-Verbindungsfehler durch:



Die ISE pxgrid-cm.log berichtet:

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

Der Grund für den Ausfall ist in Wireshark zu sehen:



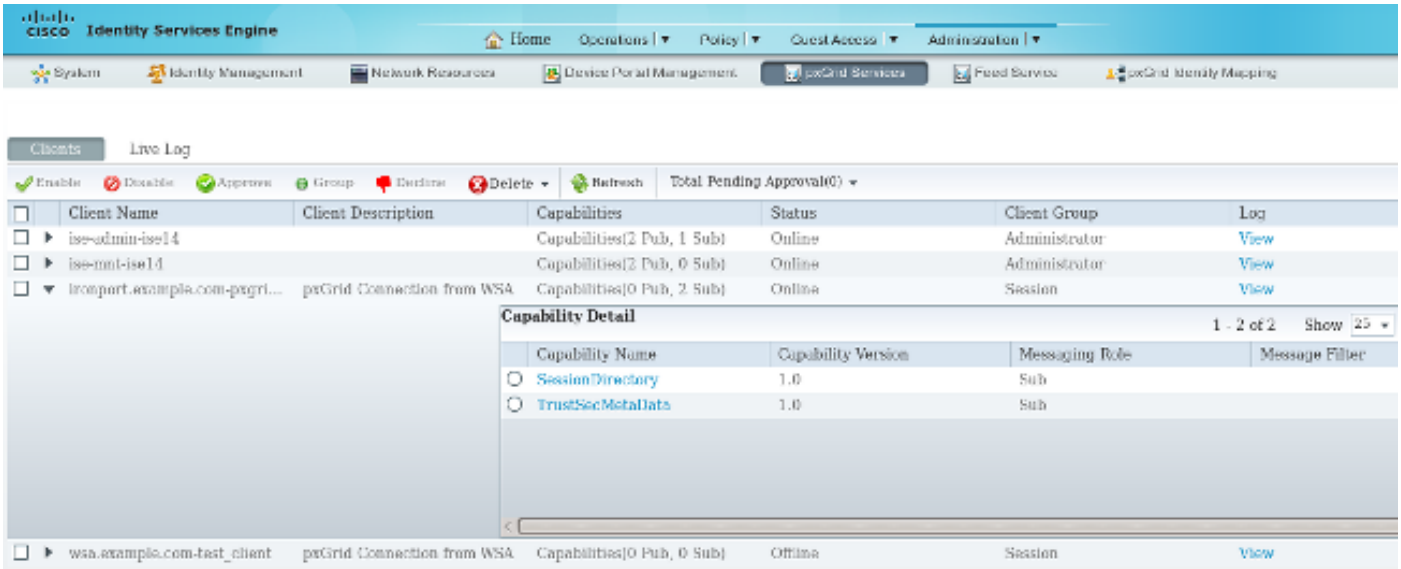
Bei einer SSL-Sitzung, die zum Schutz des XMPP-Austauschs (Extensible Messaging and Presence Protocol) (verwendet von pxGrid)) verwendet wird, meldet der Client SSL-Fehler aufgrund einer unbekannten Zertifikatskette, die vom Server präsentiert wird.

Szenario korrigieren

Für das richtige Szenario protokolliert die ISE pxgrid-controller.log Folgendes:

```
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
```

Die ISE-GUI stellt die WSA außerdem als Abonnent mit den richtigen Funktionen dar:



Zugehörige Informationen

- ASA Version 9.2.1 VPN-Status mit ISE-Konfigurationsbeispiel
- WSA 8.7 - Benutzerhandbuch
- ASA und Catalyst Switch der Serie 3750X - TrustSec-Konfigurationsbeispiel und Leitfaden zur Fehlerbehebung
- Konfigurationsanleitung für Cisco TrustSec-Switches: Cisco TrustSec im Überblick
- Konfigurieren eines externen Servers für die Benutzerautorisierung der Sicherheitsappliance
- Konfigurationsleitfaden für die CLI der Cisco ASA-Serie 9.1
- Cisco Identity Services Engine-Benutzerhandbuch, Version 1.2
- Technischer Support und Dokumentation - Cisco Systems