

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

## Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurieren](#)

[Netzwerkdigramm und Datenverkehrsfluss](#)

[ASA-VPN](#)

[ASA-FW](#)

[ISE](#)

[Schritt 1: SGT für IT und andere Gruppen](#)

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

[Schritt 3: Netzwerkgerät hinzufügen und PAC-Datei für ASA-VPN erstellen](#)

[Schritt 4: pxGrid-Rolle aktivieren](#)

[Schritt 5: Generieren des Zertifikats für Administration und die pxGrid-Rolle](#)

[Schritt 6: pxGrid-automatische Registrierung](#)

[WSA](#)

[Schritt 1: Transparenter Modus und Umleitung](#)

[Schritt 2: Zertifikatsgenerierung](#)

[Schritt 3: ISE-Verbindung testen](#)

[Schritt 4: ISE-Identifikationsprofile](#)

[Schritt 5: Zugriff auf die Richtlinie basierend auf dem SGT-Tag](#)

[Überprüfen](#)

[Schritt 1: VPN-Sitzung](#)

[Schritt 2: Von der WSA abgerufene Sitzungsinformationen](#)

[Schritt 3: Umleitung des Datenverkehrs zur WSA](#)

[Fehlerbehebung](#)

[Falsche Zertifikate](#)

[Szenario korrigieren](#)

[Zugehörige Informationen](#)

## 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

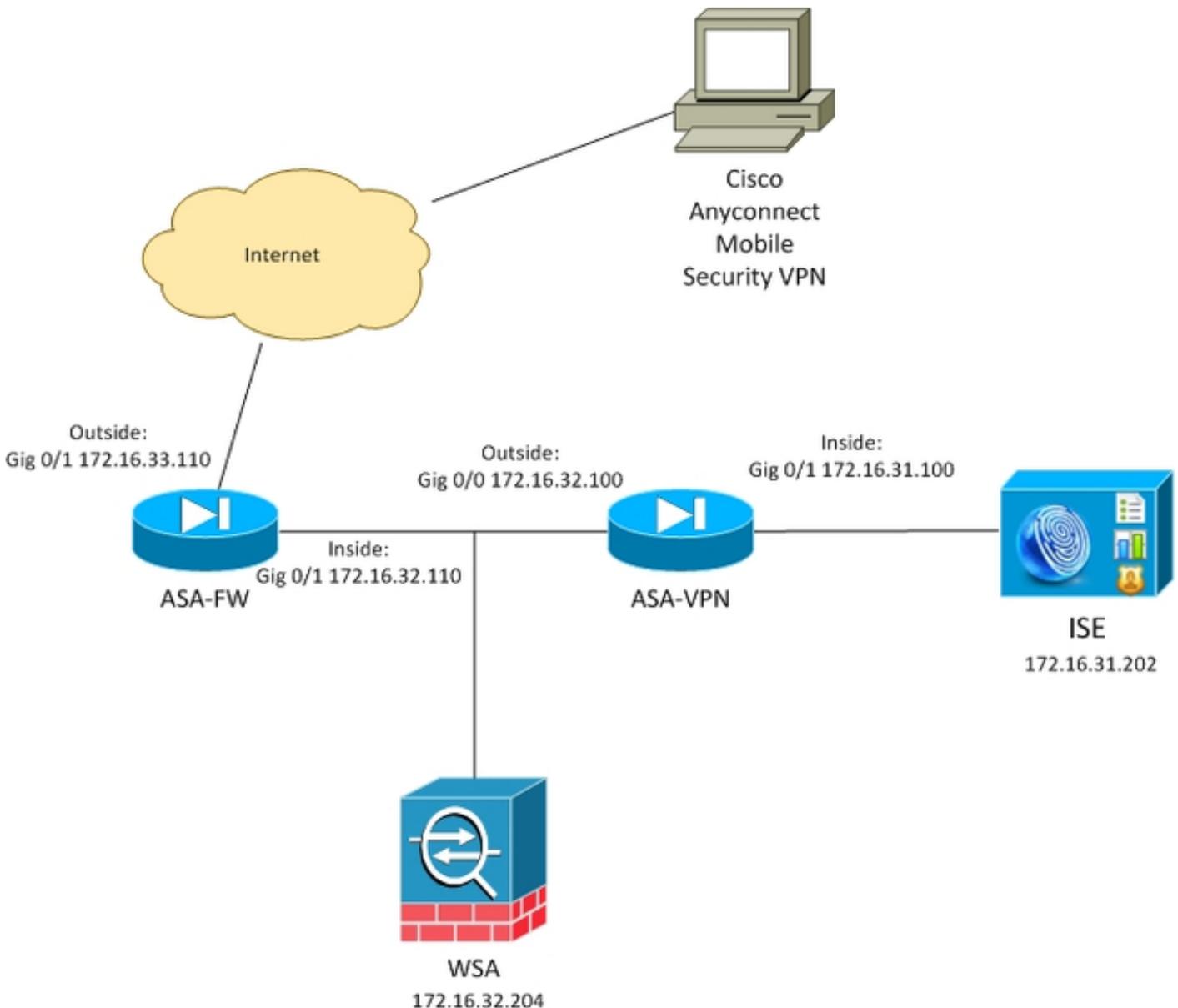
**Hinweis:** Verwenden Sie das [Command Lookup Tool](#) (nur [registrierte](#) Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

### 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:

**Results**

Search:

Navigation: Home, Operations, Authentication, Authorization, Profiling, Posture, Client Provisioning, Dictionaries, Conditions, Results

**Security Groups**  
For Policy Export go to [Administration > System](#)

Actions: Edit, Add, Import, Export

Name	SGT (Dec / Hex)
<input type="checkbox"/> IT	2/0002
<input type="checkbox"/> Marketing	3/0003
<input type="checkbox"/> Unknown	0/0000

### 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.

**Authorization Policy**

Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order.  
For Policy Export go to [Administration > System > Backup & Restore > Policy Export Page](#)

First Matched Rule Applies:

Exceptions (0)

Standard

Status	Rule Name	Conditions (Identity groups and other conditions)	Permissions
<input checked="" type="checkbox"/>	ASA-VPN	if DEVICE.Device Type EQUALS All Device Types#ASA-VPN	then PermitAccess AND IT

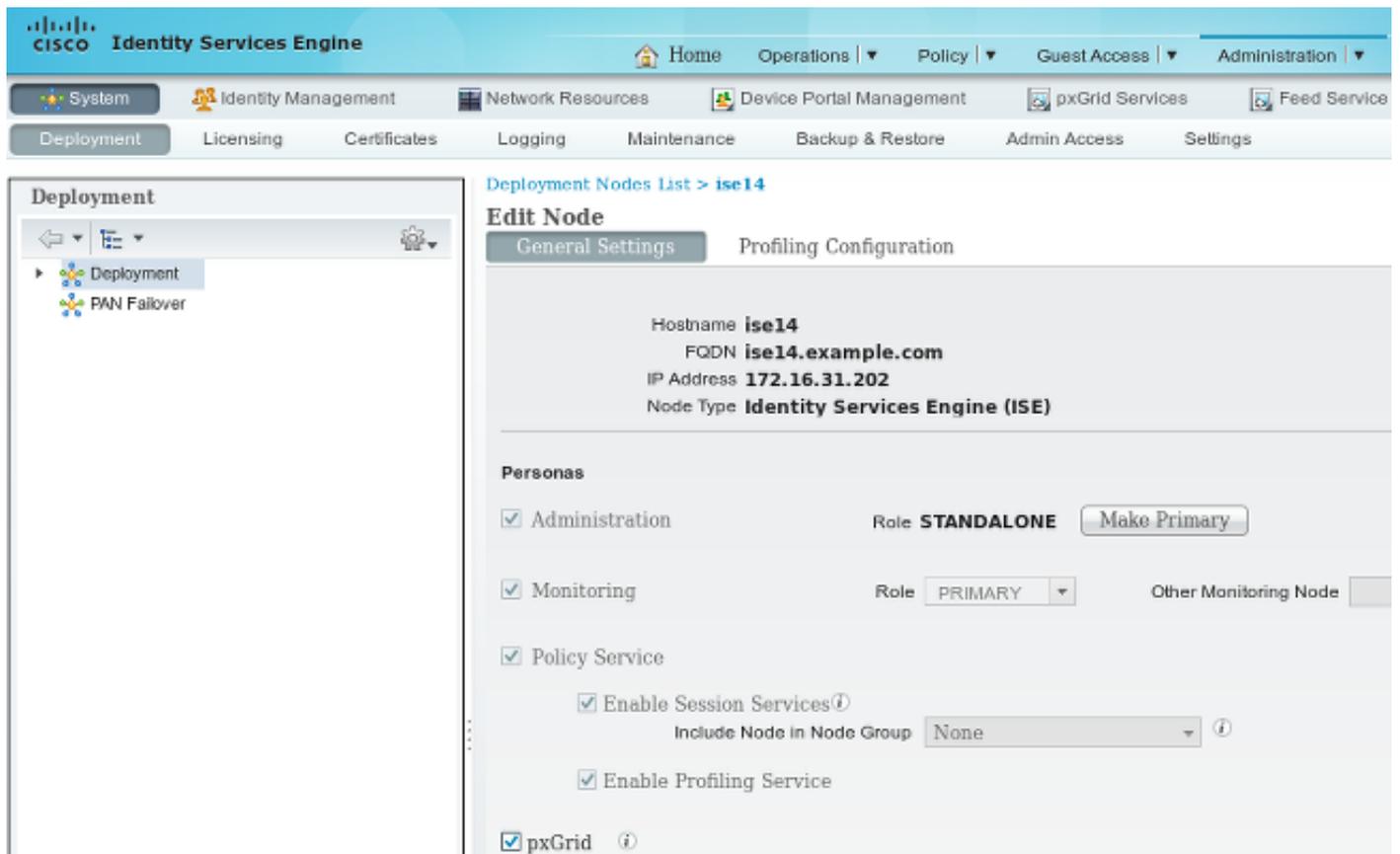
### Schritt 3: Netzwerkgerät hinzufügen und PAC-Datei für ASA-VPN erstellen

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.



The screenshot displays the Cisco Identity Services Engine (ISE) Administration interface. The top navigation bar includes 'Home', 'Operations', 'Policy', 'Guest Access', and 'Administration'. The left sidebar shows the 'Deployment' menu with 'Deployment' and 'PAN Failover' options. The main content area is titled 'Edit Node' for 'ise14' and is divided into 'General Settings' and 'Profiling Configuration' tabs. Under 'General Settings', the following information is visible: Hostname 'ise14', FQDN 'ise14.example.com', IP Address '172.16.31.202', and Node Type 'Identity Services Engine (ISE)'. The 'Personas' section includes checkboxes for 'Administration', 'Monitoring', and 'Policy Service'. The 'Administration' role is set to 'STANDALONE' with a 'Make Primary' button. The 'Monitoring' role is set to 'PRIMARY'. Under 'Policy Service', there are options to 'Enable Session Services' and 'Enable Profiling Service'. At the bottom, the 'pxGrid' checkbox is checked, indicating that the pxGrid role is activated.

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

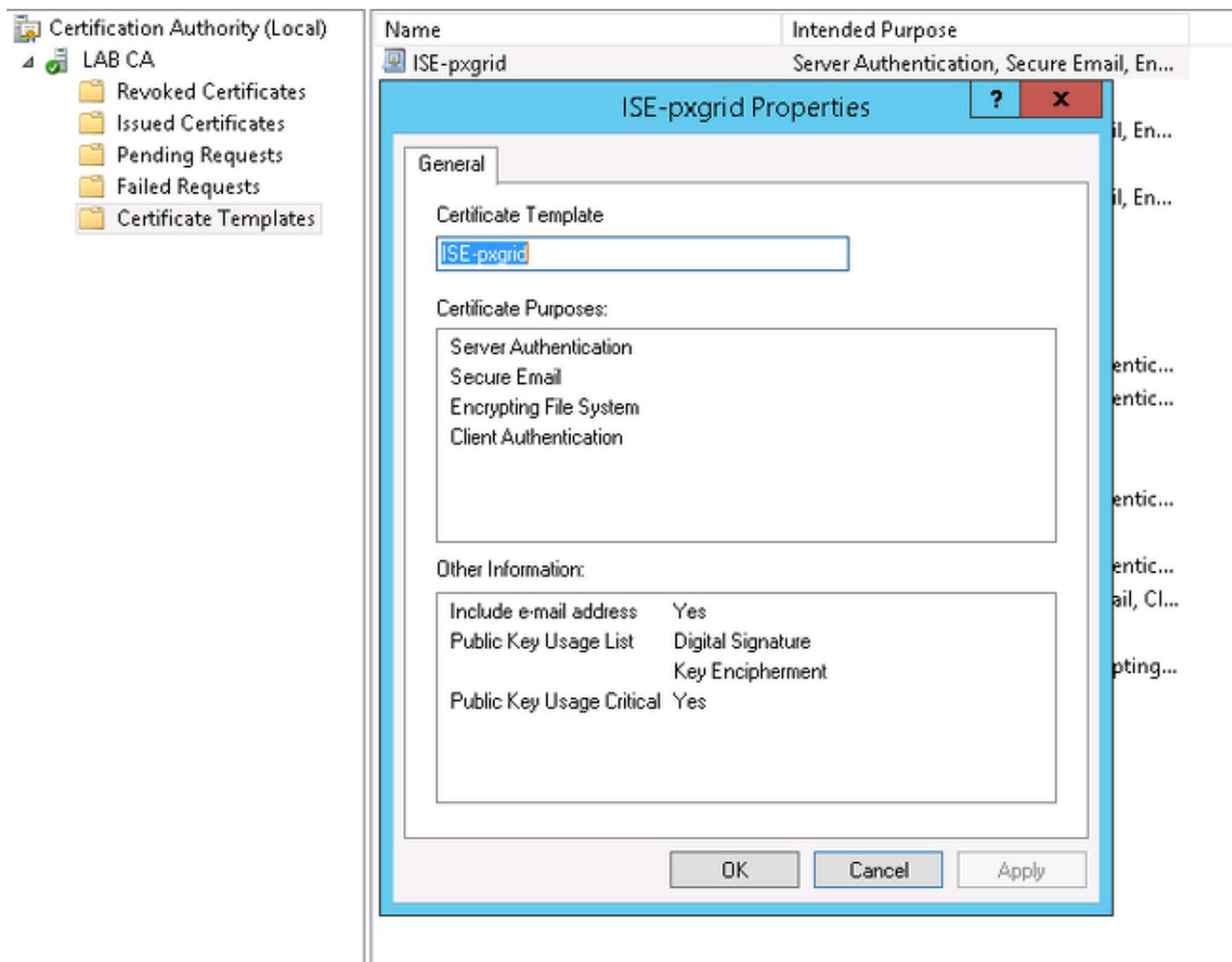
Das pxGrid-Protokoll verwendet die Zertifikatauthentifizierung sowohl für den Client als auch für den Server. Es ist sehr wichtig, die richtigen Zertifikate für die ISE und die WSA zu konfigurieren. Beide Zertifikate sollten den vollqualifizierten Domännennamen (Fully Qualified Domain Name, FQDN) im 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.

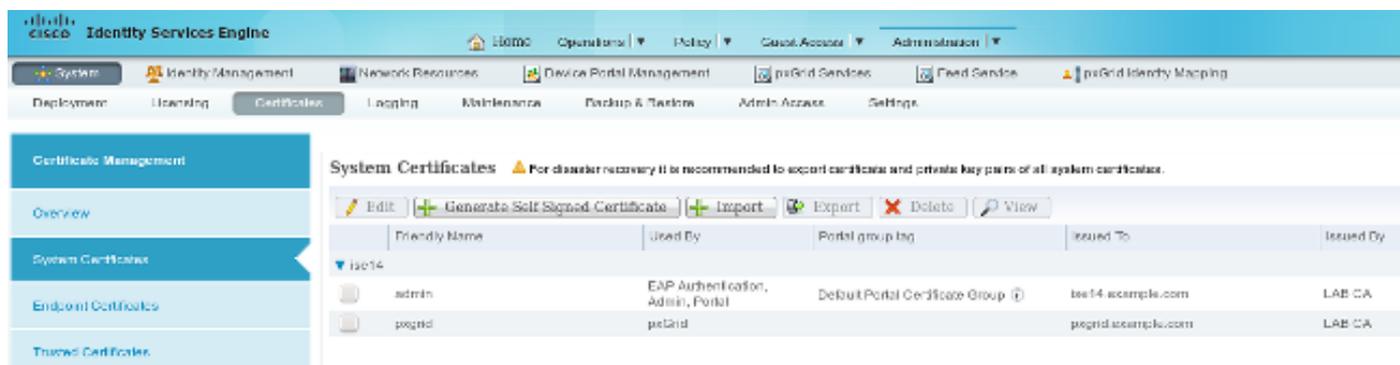
Um Zertifikate zu konfigurieren, wählen Sie **Administration > Certificates** (Verwaltung > Zertifikate).

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.

[View By Capabilities](#)  Enable Auto-Registration [Disable Auto-Registration](#)

## 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:

The screenshot shows the configuration page for a Cisco S000V Web Security Virtual Appliance. The page title is "Transparent Redirection". It features a navigation bar with tabs for Reporting, Web Security Manager, Security Services, Network, and System Administration. The main content area is divided into two sections: "Transparent Redirection Device" and "WCCP v2 Services".

**Transparent Redirection Device**

Type:	WCCP v2 Router
-------	----------------

[Edit Device...](#)

**WCCP v2 Services**

[Add Service...](#)

Service Profile Name	Service ID	Router IP Addresses	Ports	Delete
wccp90	90	172.16.32.110, 172.16.33.110	80,443	

### Schritt 2: Zertifikatsgenerierung

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

## Manage Trusted Root Certificates

### Custom Trusted Root Certificates

Import...

Trusted root certificates are used to determine whether HTTPS sites' signing certificates should be trusted based on their chain of certificate authorities. Certificates imported here are added to the trusted root certificate list. Add certificates to this list in order to trust certificates with signing authorities not recognized on the Cisco list.

Certificate	Expiration Date	On Cisco List	Delete
LAB CA	Feb 12 07:48:12 2025 GMT	No	

Cancel

Submit

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):

## Identity Services Engine

### Identity Services Engine Settings

ISE Server:	172.16.31.202
WSA Client Certificate:	Using Generated Certificate: Common name: wsa.example.com Organization: TAC Organizational Unit: Krakow Country: PL Expiration Date: May 5 15:57:36 2016 GMT Basic Constraints: Not Critical
ISE Admin Certificate:	Common name: LAB CA Organization: Organizational Unit: Country: Expiration Date: Feb 12 07:48:12 2025 GMT Basic Constraints: Critical
ISE PxGrid Certificate:	Common name: LAB CA Organization: Organizational Unit: Country: Expiration Date: Feb 12 07:48:12 2025 GMT Basic Constraints: Critical

Edit Settings...

### Schritt 3: ISE-Verbindung testen

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

#### Test Communication with ISE Server

Start Test

Checking connection to ISE PxGrid server...  
Success: Connection to ISE PxGrid server was successful. Retrieved 4 SGTs

Checking connection to ISE REST server...  
Success: Connection to ISE REST server was successful.

Test completed successfully.

### 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".

The screenshot shows the Cisco S000V Web Security Virtual Appliance interface. The top navigation bar includes 'Reporting', 'Web Security Manager', 'Security Services', 'Network', and 'System Administration'. The main content area is titled 'Identification Profiles' and contains a table of 'Client / User Identification Profiles'. The table has five columns: Order, Transaction Criteria, Authentication / Identification Decision, End-User Acknowledgement, and Delete. There are two rows: one for an ISE profile and one for a Global Identification Profile.

Order	Transaction Criteria	Authentication / Identification Decision	End-User Acknowledgement	Delete
1	<b>ISE</b> Protocols: HTTP/HTTPS	Identify Users Transparently: Identity Services Engine Guest privileges for users falling transparent user identification	(global profile)	
	<b>Global Identification Profile</b>	Exempt from Authentication / User Identification	Not Available	

### 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:

## Access Policy: PolicyForIT

### Policy Settings

Enable Policy

Policy Name: ?

PolicyForIT

(e.g. my IT policy)

Description:

Insert Above Policy:

1 [Global Policy] v

### Policy Member Definition

Membership is defined by the combination of the following options. All criteria must be met for the policy to take effect.

Identification Profiles and Users:

Select One or More Identification Profiles v

Identification Profile

ISE v

Authorized Users and Groups

All Authenticated Users

Selected Groups and Users ?

ISE Secure Group Tags:

IT

Users: No users entered

Guests (users failing authentication)

Add Identification Profile



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

## Access Policies: Policy "PolicyForIT": Edit Secure Group Tags

### Authorized Secure Group Tags

Use the search function below to add Secure Group Tags. To remove Secure Group Tags from this policy, use the Delete option.

1 Secure Group Tag(s) currently included in this policy.

Secure Group Tag Name	SGT Number	SGT Description	Delete
IT	2	__NONE__	<input type="checkbox"/>

[Delete](#)

### Secure Group Tag Search

Enter any text to search for a Secure Group Tag name, number, or description. Select one or more Secure Group Tags from the list and use the Add button to add to this policy.

Search  x

0 Secure Group Tag(s) selected for Add

[Add](#)

Secure Group Tag Name	SGT Number	SGT Description	Select
Unknown	0	Unknown Security Group	<input type="checkbox"/>
Marketing	3	__NONE__	<input type="checkbox"/>
IT	2	__NONE__	<input type="checkbox"/>
ANY	65535	Any Security Group	<input type="checkbox"/>

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

## Access Policies

Policies							
Order	Group	Protocols and User Agents	URL Filtering	Applications	Objects	Anti-Malware and Reputation	Delete
1	<b>PolicyForIT</b> Identification Profile: ISE 1 tag (IT)	(global policy)	Block: 2 Monitor: 78	(global policy)	(global policy)	(global policy)	
	<b>Global Policy</b> Identification Profile: All	No blocked items	Monitor: 79	Monitor: 377	No blocked items	Web Reputation: Enabled Anti-Malware Scanning: Disabled	

[Add Policy...](#)

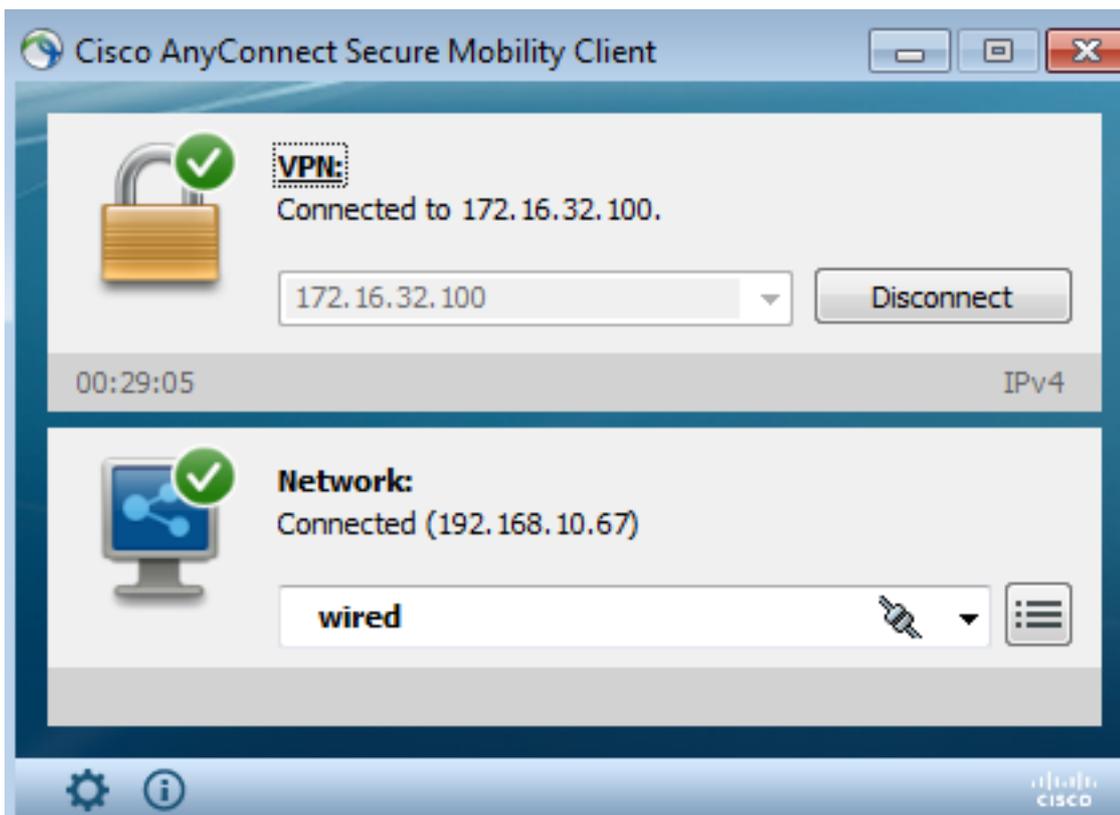
[Edit Policy Order...](#)

## 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:

Initiated	Updated	Session Status	CoA Action	Endpoint ID	Identity	IP Address	Security Group
2015-05-06 19:17:50...	2015-05-06 19:17:55...	Started		192.168.10.67	cisco	172.16.32.50	IT

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:

Notification: Policy: Destination - Windows Internet Explorer

http://sport.pl/

File Edit View Favorites Tools Help

★ Favorites Notification: Policy: Destination

### This Page Cannot Be Displayed

Based on your organization's access policies, access to this web site ( http://sport.pl/ ) has been blocked.

If you have questions, please contact your organization's network administrator and provide the codes shown below.

Date: Wed, 06 May 2015 17:50:15 GMT  
 Username: cisco  
 Source IP: 172.16.32.50  
 URL: GET http://sport.pl/  
 Category: LocalSportSites  
 Reason: BLOCK-DEST  
 Notification: BLOCK\_DEST

Dies wird im WSA-Bericht bestätigt:

Cisco S000V  
 Web Security Virtual Appliance

Reporting
Web Security Manager
Security Services
Network
System Administration

### Web Tracking

**Search**

Proxy Services
L4 Traffic Monitor
SOCKS Proxy

Available: 06 May 2015 11:22 to 06 May 2015 18:02 (GMT +00:00)

Time Range:	Hour	
User/Client IPv4 or IPv6: (?)	cisco	(e.g. jdoe, DOMAIN/jdoe, 10.1.1.0, or 2001:420:80:1::5)
Website:		(e.g. google.com)
Transaction Type:	Blocked	
<a href="#">Advanced</a>		Current Criteria: Policy: PolicyForIT.

Clear
Search

Generated: 06 May 2015 18:03 (GMT) [Printable](#) [Download](#)

**Results**

Displaying 1 - 3 of 3 items.

Time (GMT +00:00)	Website (count)	Display All Details...	Disposition	Bandwidth	User / Client IP
06 May 2015 18:02:22	<a href="http://sport.pl">http://sport.pl</a>	(2)	Block - URL Cat	0B	cisco 172.16.32.50
06 May 2015 17:50:15	<a href="http://sport.pl">http://sport.pl</a>	(2)	Block - URL Cat	0B	cisco 172.16.32.50
06 May 2015 17:48:36	<a href="http://sport.pl">http://sport.pl</a>		Block - URL Cat	0B	cisco 172.16.32.50

Displaying 1 - 3 of 3 items.

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:

#### Test Communication with ISE Server

Start Test

```
Validating ISE Portal certificate ...  
Success: Certificate validation successful  
  
Checking connection to ISE PxGrid server...  
Failure: Connection to ISE PxGrid server timed out  
  
Test interrupted: Fatal error occurred, see details above.
```

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:

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	FEATLRES
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=130904 Len=0 TSval=66429082 TSecr=21743451
172.16.32.204	172.16.31.202	TCP	34491 > xmpp-client [ACK] Seq=290 Ack=3260 Win=130968 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, Description: Unknown CA)

> Frame 21: 80 bytes on wire (640 bits), 80 bytes captured (640 bits)  
 > Ethernet II, Src: Vmware\_c0:00:01 (00:50:56:c0:00:01), Dst: Vmware\_58:cb:ad (00:0c:29:58:cb:ad)  
 > Internet Protocol Version 4, Src: 172.16.32.204 (172.16.32.204), Dst: 172.16.31.202 (172.16.31.202)  
 > Transmission Control Protocol, Src Port: 34491 (34491), Dst Port: xmpp-client (5222), Seq: 297, Ack: 3310, Len: 14  
 > [3 Reassembled TCP Segments (139 bytes): #13(118), #18(7), #21(14)]

Secure Sockets Layer  
 > TLsv1 Record Layer: Handshake Protocol: Client Hello  
 > TLsv1 Record Layer: Alert (Level: Fatal, Description: Unknown CA)  
 > TLsv1 Record Layer: Alert (Level: Fatal, Description: Unknown CA)  
 > TLsv1 Record Layer: Alert (Level: Fatal, Description: Unknown CA)

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 unbekanntenen 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:

Client Name	Client Description	Capabilities	Status	Client Group	Log
ise-admin-ise14		Capabilities(2 Pub, 1 Sub)	Online	Administrator	<a href="#">View</a>
ise-mn1-ise14		Capabilities(2 Pub, 0 Sub)	Online	Administrator	<a href="#">View</a>
Ironport.example.com-pxgrl...	pxGrid Connection from WSA	Capabilities(0 Pub, 2 Sub)	Online	Session	<a href="#">View</a>

Capability Detail			
Capability Name	Capability Version	Messaging Role	Message Filter
SessionDirectory	1.0	Sub	
TrustSecMetaData	1.0	Sub	

wsa.example.com-test_client	pxGrid Connection from WSA	Capabilities(0 Pub, 0 Sub)	Offline	Session	<a href="#">View</a>
-----------------------------	----------------------------	----------------------------	---------	---------	----------------------

# 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](#)