

WSA-integratie met ISE configureren voor TrustSec Aware Services

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configureren](#)

[Netwerkdigram en verkeersstroom](#)

[ASA 5500-VPN](#)

[ASA-FW](#)

[ISE](#)

[Stap 1 SGT voor IT en andere groepen](#)

[Stap 2. Toestemming voor VPN-toegang waarbij SGT = 2 \(IT\) wordt toegekend](#)

[Stap 3. Voeg netwerkapparaat toe en genereer PAC-bestand voor ASA-VPN](#)

[Stap 4. Schakel PxGrid-rol in](#)

[Stap 5. Het certificaat voor beheer en de PxGrid-rol genereren](#)

[Stap 6. Automatische registratie van pxGrid](#)

[WSA](#)

[Stap 1. Transparante modus en omleiding](#)

[Stap 2. certificaatgeneratie](#)

[Stap 3. Test ISE-connectiviteit](#)

[Stap 4. ISE-identificatieprofielen](#)

[Stap 5. Toegang tot het op de SGT-tag gebaseerde beleid](#)

[Verifiëren](#)

[Stap 1. VPN-sessie](#)

[Stap 2. Door de WSA teruggewonnen sessieinformatie](#)

[Stap 3. Verkeersomleiding naar de WSA](#)

[Problemen oplossen](#)

[Onjuiste certificaten](#)

[Correct scenario](#)

[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft hoe u het web security applicatie (WSA) kunt integreren met Identity Services Engine (ISE). ISE versie 1.3 ondersteunt een nieuwe API met de naam pxGrid. Dit moderne en flexibele protocol ondersteunt verificatie, encryptie en privileges (groepen) die een

makkelijke integratie met andere veiligheidsoplossingen mogelijk maken.

WSA versie 8.7 ondersteunt pxGrid-protocol en kan context-identiteitsinformatie van ISE ophalen. Als resultaat hiervan staat WSA u toe om beleid te bouwen op basis van de Groepsmarkering (SGT) van de VertrouwenSec die van ISE wordt teruggevonden.

Voorwaarden

Vereisten

Cisco raadt u aan ervaring met de configuratie van Cisco ISE en basiskennis van deze onderwerpen te hebben:

- ISE-implementaties en configuratie van vergunningen
- Adaptieve security applicatie (ASA) CLI-configuratie voor TrustSec en VPN-toegang
- WSA-configuratie
- Basisbegrip van TrustSec-implementaties

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Microsoft Windows 7
- Cisco ISE-software-release 1.3 en hoger
- Cisco AnyConnect mobiele security versie 3.1 en hoger
- Cisco ASA versie 9.3.1 en hoger
- Cisco WSA versie 8.7 en hoger

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Configureren

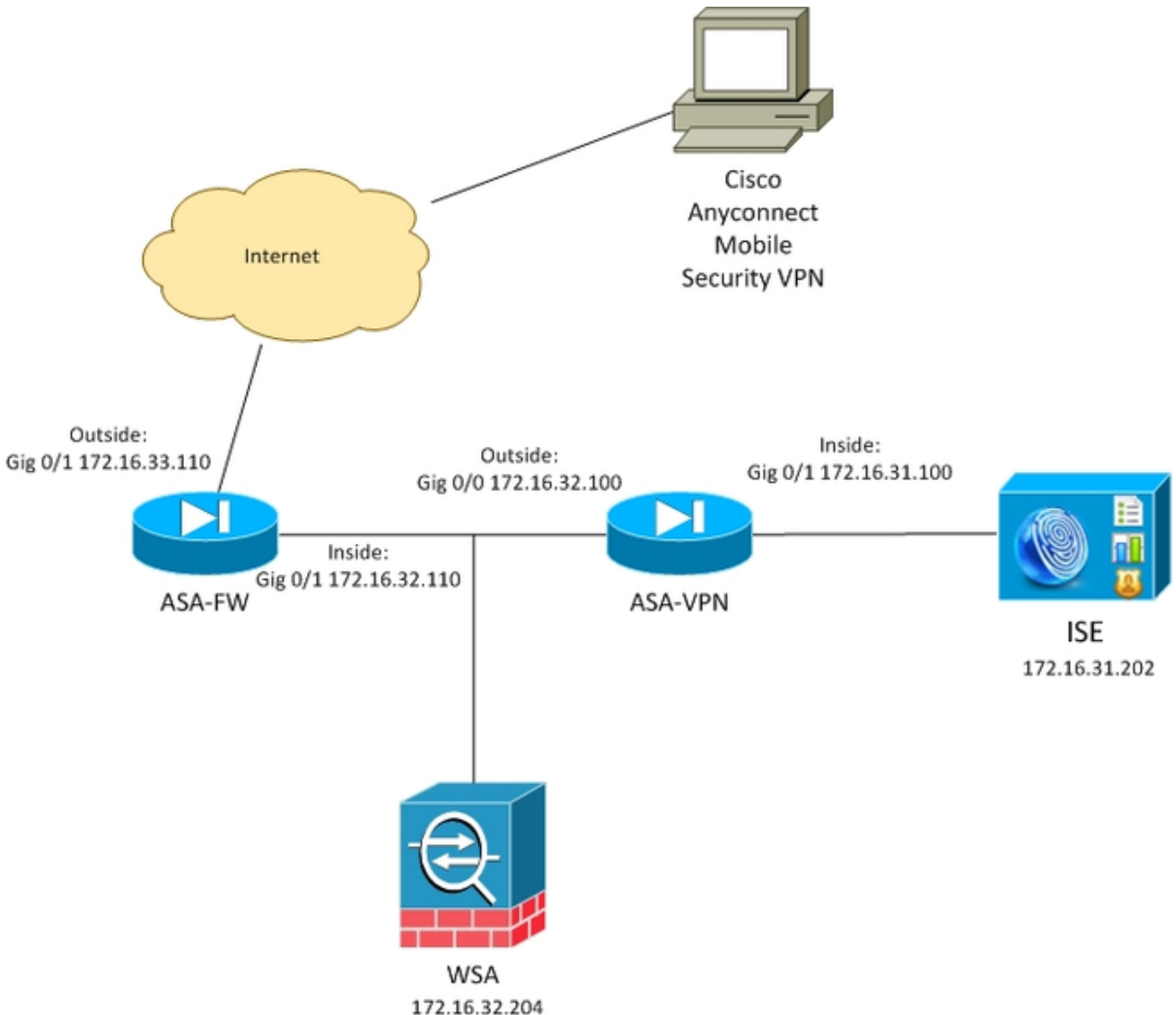
Opmerking: Gebruik de [Command Lookup Tool \(alleen voor geregistreerde gebruikers\) voor meer informatie over de opdrachten die in deze sectie worden gebruikt.](#)

Netwerkdigram en verkeersstroom

TrustSec SGT-tags worden toegewezen door ISE die als authenticatieserver voor alle types gebruikers die toegang hebben tot het bedrijfsnetwerk worden gebruikt. Dit betekent bedrading/draadloze gebruikers die zich via 802.1x of ISE gastportals authentiek verklaren. Ook externe VPN-gebruikers die ISE gebruiken voor verificatie.

Voor WSA, maakt het niet uit hoe de gebruiker het netwerk heeft benaderd.

Dit voorbeeld stelt een externe VPN gebruikers voor die sessie over ASA-VPN beëindigen. Aan deze gebruikers is een specifiek SGT-label toegekend. Al HTTP-verkeer naar het internet wordt door de ASA-FW (firewall) onderschept en voor inspectie naar de WSA doorgestuurd. De WSA maakt gebruik van het identiteitsprofiel dat het in staat stelt gebruikers te classificeren op basis van de SGT-tag en op basis daarvan toegangsbeleid of decryptie te ontwikkelen.



De gedetailleerde stroom is:

1. De AnyConnect VPN-gebruiker beëindigt de Secure Socket Layer (SSL) sessie op de ASA-VPN. ASA-VPN wordt geconfigureerd voor TrustSec en gebruikt ISE voor verificatie van VPN-gebruikers. De geauthentiseerde gebruiker krijgt een SGT-tag waarde = 2 (naam = IT) toegewezen. De gebruiker ontvangt een IP-adres van het 172.16.32.0/24 netwerk (172.16.32.50 in dit voorbeeld).
2. De gebruiker probeert de webpagina op het internet te benaderen. ASA-FW is geconfigureerd voor Web Cache Communication Protocol (WCCP), dat het verkeer omwijst naar de WSA.
3. De WSA wordt gevormd voor ISE integratie. Het gebruikt pxGrid om informatie van ISE te

downloaden: Aan gebruiker IP-adres 172.16.32.50 is SGT-tag 2 toegekend.

4. De WSA verwerkt het HTTP verzoek van de gebruiker en slaat toegangsbeleidForIT in. Dit beleid is zo ingesteld dat het verkeer naar de sportlocaties wordt geblokkeerd. Alle andere gebruikers (die niet tot SGT 2 behoren) hebben het standaardtoegangsbeleid en hebben volledige toegang tot de sportsites.

ASA 5500-VPN

Dit is een VPN-poort die is ingesteld voor TrustSec. Gedetailleerde configuratie is buiten het toepassingsgebied van dit document. Raadpleeg deze voorbeelden:

- [ASA en Catalyst 3750X Series switchstack-SEC Configuratievoorbeeld en probleemoplossing](#)
- [ASA versie 9.2 VPN SGT-classificatie en -handhaving Configuratievoorbeeld](#)

ASA-FW

De ASA Firewall is verantwoordelijk voor WCCP-omleiding naar de WSA. Dit apparaat is niet op de hoogte van 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 een centraal punt in de opstelling van TrustSec. Het wijst SGT tags toe aan alle gebruikers die toegang hebben tot het netwerk en deze authentiek verklaren. De stappen die voor de basisconfiguratie nodig zijn, worden in dit gedeelte vermeld.

Stap 1 SGT voor IT en andere groepen

Kies beleid > Resultaten > Beveiligingsgroepen Toegang > Beveiligingsgroepen en maak het SGT aan:

Results

Search:

← ▾ ▸ ▾ ⚙

- Authentication
- Authorization
- Profiling
- Posture
- Client Provisioning
- TrustSec
 - Security Group ACLs
 - Security Groups**
 - IT
 - Marketing
 - Unknown
 - Security Group Mappings

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

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

Stap 2. Toestemming voor VPN-toegang waarbij SGT = 2 (IT) wordt toegekend

Kies **beleid > autorisatie** en maak een regel voor externe VPN-toegang. Alle VPN-verbindingen die via ASA-VPN worden gemaakt, krijgen volledige toegang (PermitAccess) en krijgen SGT tag 2 (IT) toegewezen.

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
✓	ASA-VPN	if DEVICE.Device Type EQUALS All Device Types#ASA-VPN	then PermitAccess AND IT

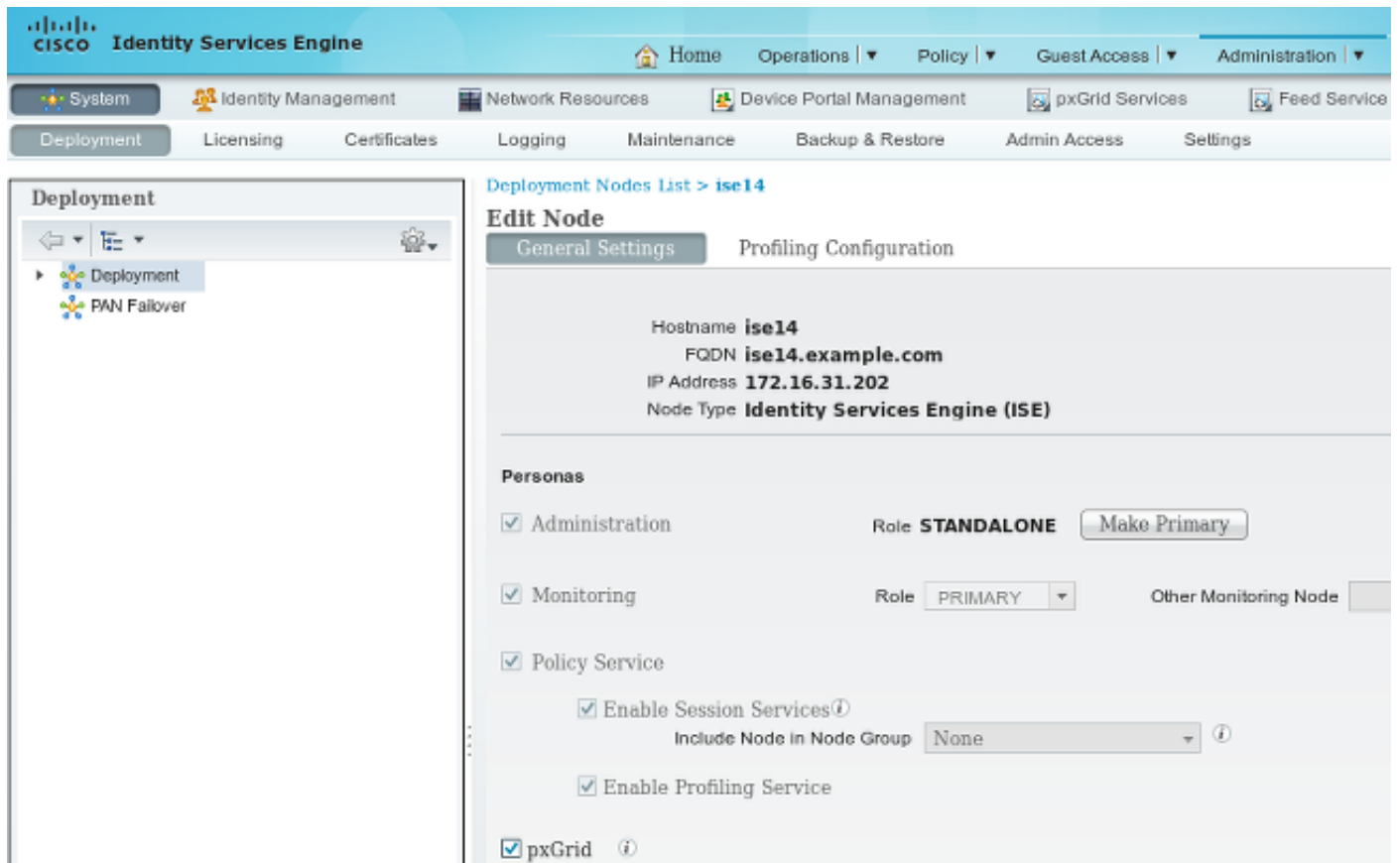
Stap 3. Voeg netwerkapparaat toe en genereer PAC-bestand voor ASA-VPN

Om het ASA-VPN aan het TrustSec-domein toe te voegen, is het nodig om het PAC-bestand (proxy Auto Config) handmatig te genereren. Dat bestand zal op de ASA worden geïmporteerd.

Dat kan worden ingesteld via **Beheer > Netwerkapparaten**. Nadat de ASA is toegevoegd, scrollen naar TrustSec instellingen en genereren het PAC bestand. De details hiervoor worden beschreven in een afzonderlijk (verwezen) document.

Stap 4. Schakel PxGrid-rol in

Kies **Administratie > Plaatsing** om de pxGrid rol toe te laten.



The screenshot displays the Cisco Identity Services Engine (ISE) Administration console. The top navigation bar includes 'Home', 'Operations', 'Policy', 'Guest Access', and 'Administration'. Below this, there are tabs for 'System', 'Identity Management', 'Network Resources', 'Device Portal Management', 'pxGrid Services', and 'Feed Service'. The 'Deployment' tab is active, showing a sidebar 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'. Under 'General Settings', the following information is displayed: 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' with an 'Other Monitoring Node' dropdown. The 'Policy Service' section has checkboxes for 'Enable Session Services' and 'Enable Profiling Service'. The 'Include Node in Node Group' dropdown is set to 'None'. At the bottom, the 'pxGrid' checkbox is checked.

Stap 5. Het certificaat voor beheer en de PxGrid-rol genereren

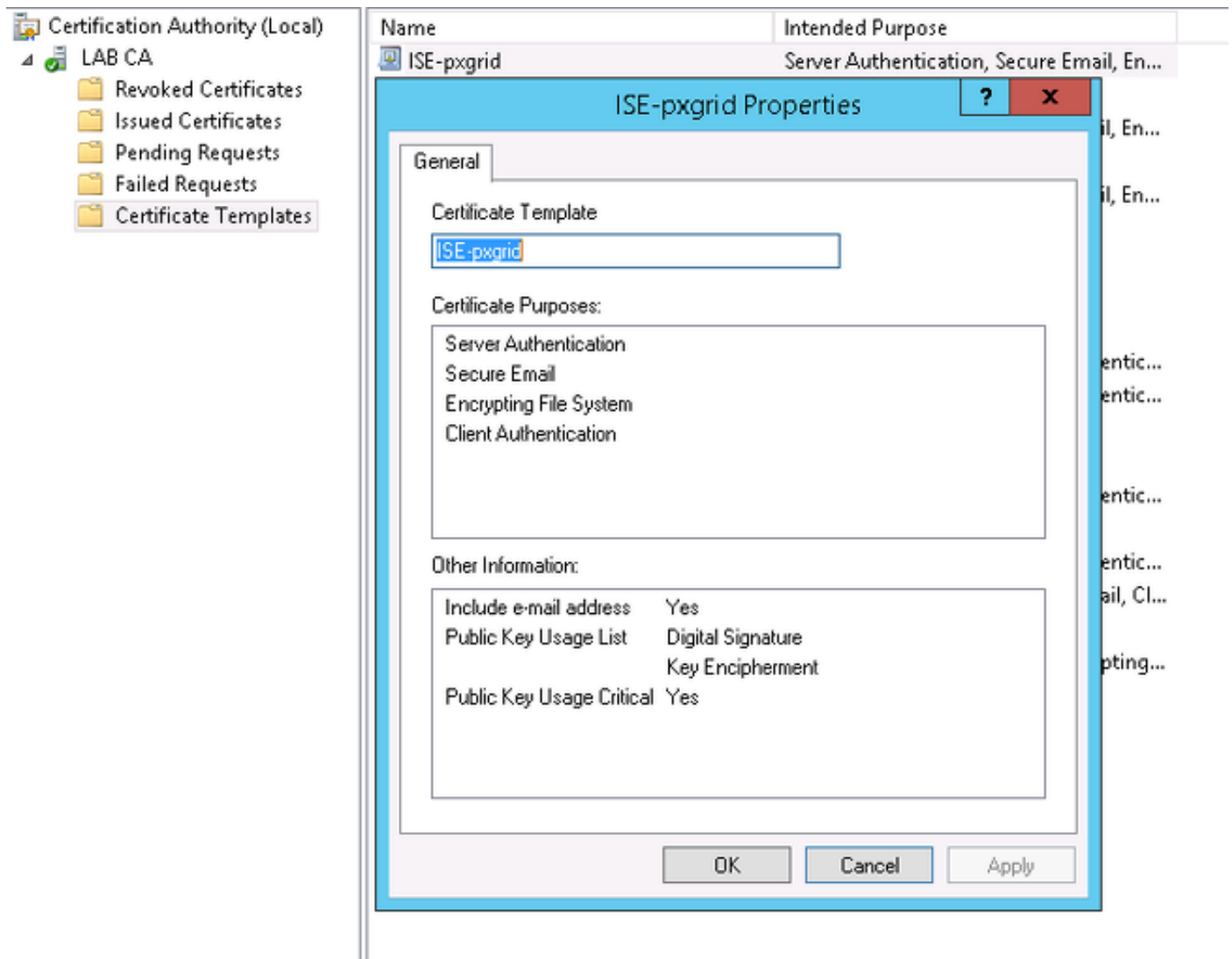
Het PxGrid-protocol gebruikt certificatie van certificaten voor zowel de client als de server. Het is zeer belangrijk om de juiste certificaten voor zowel ISE als WSA te configureren. Beide certificaten moeten de Full Qualified Domain Name (FQDN) in het Onderwerp en x509-uitbreidingen voor Clientverificatie en -serververificatie bevatten. Controleer ook of het juiste DNS A-record is gecreëerd voor zowel ISE als de WSA en op basis daarvan wordt de corresponderende FQDN-naam aangepast.

Als beide certificaten door een andere certificaatinstantie (CA) worden ondertekend, is het belangrijk deze CA's in de vertrouwde winkel op te nemen.

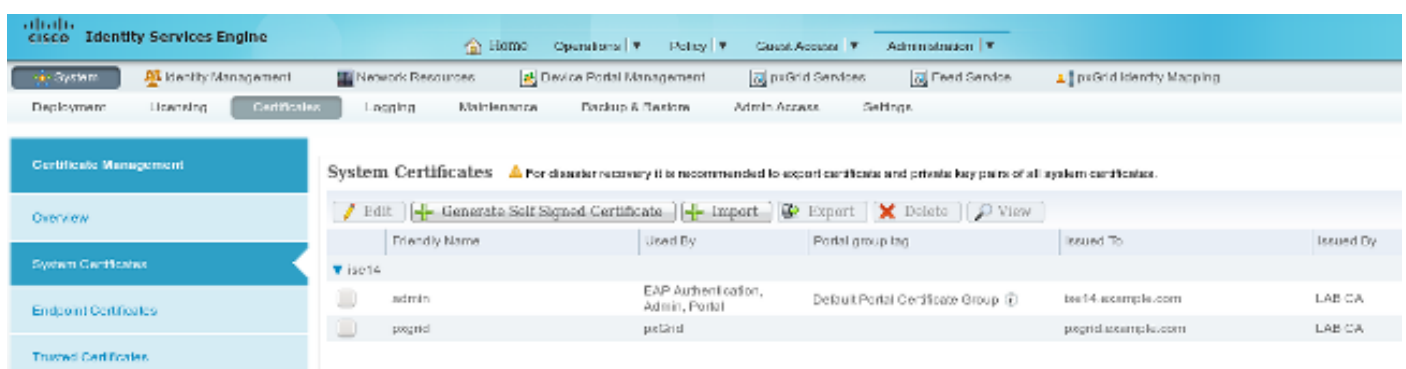
Om certificaten te configureren kiest u **Beheer > Certificaten**.

ISE kan een certificaat het ondertekenen verzoek (CSR) voor elke rol genereren. Voor de pxGrid-rol, exporteer en teken de CSR met een externe CA.

In dit voorbeeld is Microsoft CA met deze sjabloon gebruikt:



Het eindresultaat kan er als volgt uitzien:



Vergeet niet om DNS A-records te maken voor `ise14.voorbeeld.com` en `pxgrid.voorbeeld.com`, die op `172.16.31.202` wijzen.

Stap 6. Automatische registratie van pxGrid

Standaard zal ISE de PxGrid-abonnees niet automatisch registreren. Dit moet handmatig door de beheerder worden goedgekeurd. Die instelling moet worden gewijzigd voor de WSA-integratie.

Kies **Beheer > PxGrid Services** en stel **Auto-Registratie** inschakelen.

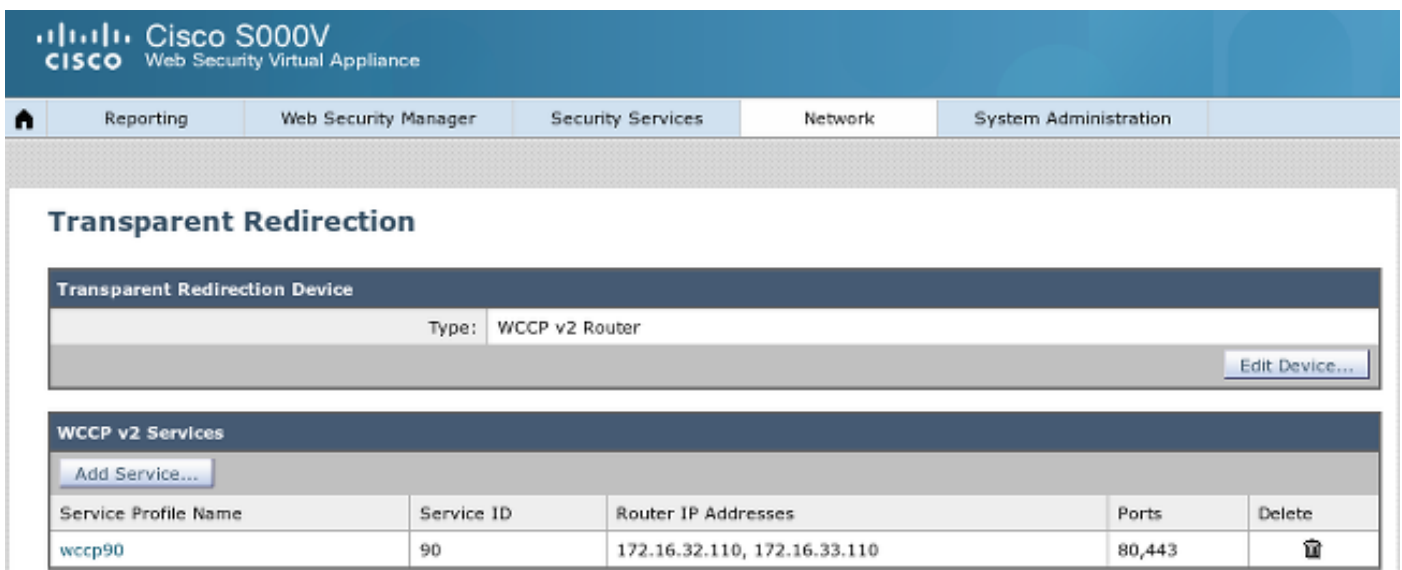
[View By Capabilities](#)

 [Enable Auto-Registration](#) [Disable Auto-Registration](#)

WSA

Stap 1. Transparante modus en omleiding

In dit voorbeeld wordt de WSA met slechts de beheersinterface, de transparante modus en de omleiding van de ASA geconfigureerd:




The screenshot shows the Cisco S000V Web Security Virtual Appliance management interface. The top navigation bar includes: Reporting, Web Security Manager, Security Services (selected), Network, and System Administration. The main content area is titled "Transparent Redirection".

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	

Stap 2. certificaatgeneratie

De WSA moet de CA vertrouwen om alle certificaten te ondertekenen. Kies **Netwerk > certificaatbeheer** om een CA-certificaat toe te voegen:

Cisco S000V Web Security Virtual Appliance

Reporting Web Security Manager Security Services Network System Administration

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

Het is ook nodig om een certificaat te genereren dat de WSA zal gebruiken om te authenticeren aan pxGrid. Kies **Network > Identity Services Engine > WSA Client certificaat** om de CSR te genereren, teken het met de juiste CA-sjabloon (ISE-pxgrid) en importeren het terug.

Voer ook voor "ISE Admin certificaatcertificaat" en "ISE pxGrid-certificaat" het CA-certificaat in (om het PxGrid-certificaat van ISE te vertrouwen):

Cisco S000V Web Security Virtual Appliance

Reporting Web Security Manager Security Services Network System Administration

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...

Stap 3. Test ISE-connectiviteit

Kies **Network > Identity Services Engine** om de verbinding met ISE te 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.

Stap 4. ISE-identificatieprofielen

Kies **Web Security Manager > Identificatieprofielen** om een nieuw profiel voor ISE toe te voegen. Gebruik voor "*Identificatie en verificatie*" "*Transparante gebruikers identificeren met ISE*".

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	ISE Protocols: HTTP/HTTPS	Identify Users Transparently: Identity Services Engine Guest privileges for users falling transparent user identification	(global profile)	
	Global Identification Profile	Exempt from Authentication / User Identification	Not Available	

Stap 5. Toegang tot het op de SGT-tag gebaseerde beleid

Kies **Web Security Manager > Toegangsbeleid** om een nieuw beleid toe te voegen. Het lidmaatschap gebruikt het ISE-profiel:

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



Voor geselecteerde groepen en gebruikers wordt SGT tag 2 toegevoegd (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"/>

Het beleid ontkent toegang tot alle sportlocaties voor gebruikers die deel uitmaken van SGT IT:

Access Policies

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

[Add Policy...](#)

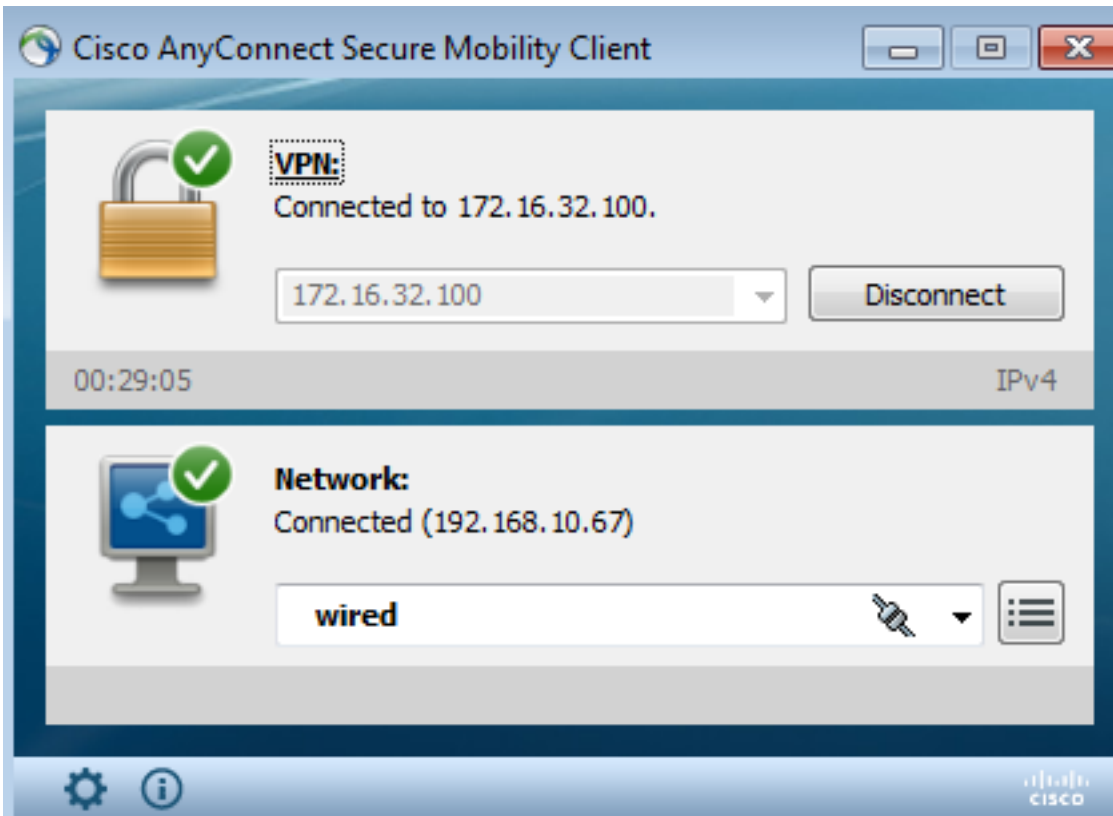
[Edit Policy Order...](#)

Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

Stap 1. VPN-sessie

De VPN-gebruiker start een VPN-sessie naar ASA-VPN:



ASA-VPN gebruikt ISE voor verificatie. ISE creëert een sessie en wijst SGT tag 2 (IT) toe:

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	(icon)	192.168.10.67	cisco	172.16.32.50	IT

Na succesvolle verificatie maakt de ASA-VPN een VPN-sessie met SGT tag 2 (teruggegeven 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

Aangezien de link tussen de ASA-VPN en de ASA-FW niet is ingeschakeld door TrustSec, stuurt de ASA-VPN niet-gelabelde frames naar dat verkeer door (zou niet in staat zijn om GRE Ethernet-frames in te sluiten met het geïnjecteerde CMD/TrustSec-veld).

Stap 2. Door de WSA teruggewonnen sessieinformatie

In dit stadium moet de WSA de mapping tussen het IP-adres, de gebruikersnaam en het SGT ontvangen (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
[ ]> █
```

Stap 3. Verkeersomleiding naar de WSA

De VPN-gebruiker initieert een verbinding met sport.pl, die door de ASA-FW wordt onderschept:

```
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
```

en in GRE naar het WSA (merk op dat de WCCP-router-id het hoogste IP-adres is ingesteld):

```
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 gaat verder de TCP handdruk en verwerkt het GET verzoek. Als gevolg daarvan wordt het beleid met de naam PolicyForIT geraakt en wordt het verkeer geblokkeerd:

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

Dit wordt bevestigd in het WSA-rapport:

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

Advanced 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	http://sport.pl (2)	(2)	Block - URL Cat	0B	cisco 172.16.32.50
06 May 2015 17:50:15	http://sport.pl (2)	(2)	Block - URL Cat	0B	cisco 172.16.32.50
06 May 2015 17:48:36	http://sport.pl (2)	(2)	Block - URL Cat	0B	cisco 172.16.32.50

Displaying 1 - 3 of 3 items.

Let op dat ISE de gebruikersnaam toont.

Problemen oplossen

Deze sectie verschaft informatie die u kunt gebruiken om problemen met uw configuratie op te lossen.

Onjuiste certificaten

Wanneer de WSA niet correct geformatteerd wordt (certificaten), test voor ISE verbindingssfalen:

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.

Het ISE pxgrid-cm.log meldt:

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

De reden voor deze fout is te zien bij Wireshark:

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)

Voor een SSL-sessie die wordt gebruikt om Extensible Messaging and Presence Protocol (XMPP)-uitwisseling (gebruikt door pxGrid) te beschermen, meldt de client SSL-storing vanwege een onbekende certificeringsketen die door de server wordt voorgesteld.

Correct scenario

Voor het juiste scenario logt de ISE pacgrid-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
```

Tevens presenteert ISE GUI het WSA als een abonnee met de juiste mogelijkheden:

Client Name	Client Description	Capabilities	Status	Client Group	Log
ise-admin-ise14		Capabilities(2 Pub, 1 Sub)	Online	Administrator	View
ise-mn1-ise14		Capabilities(2 Pub, 0 Sub)	Online	Administrator	View
Ironport.example.com-pxgr...	pxGrid Connection from WSA	Capabilities(0 Pub, 2 Sub)	Online	Session	View

Capability Detail 1 - 2 of 2 Show 25

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

Gerelateerde informatie

- [ASA versie 9.2.1 VPN-post met ISE Configuration Voorbeeld](#)
- [WSA 8007 gebruikersgids](#)
- [ASA en Catalyst 3750X Series switchstack-SEC Configuratievoorbeeld en probleemoplossing](#)
- [Cisco TrustSec-switchconfiguratie-gids: De betekenis van Cisco TrustSec](#)
- [Een externe server configureren voor security applicatie, gebruikersautorisatie](#)
- [Cisco ASA Series 5000 Series VPN CLI-configuratiegids, 9.1](#)
- [Gebruikershandleiding voor Cisco Identity Services Engine, release 1.2](#)
- [Technische ondersteuning en documentatie – Cisco Systems](#)