

Configurez l'intégration WSA avec ISE pour des services avertis de TrustSec

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Configurez](#)

[Schéma de réseau et circulation](#)

[ASA-VPN](#)

[ASA-FW](#)

[ISE](#)

[Étape 1. SGT pour le service informatique et tout autre groupe](#)

[Étape 2. Règle d'autorisation pour l'accès VPN qui assigne SGT = 2 \(service informatique\)](#)

[Étape 3. Ajoutez le périphérique de réseau et générez le fichier PAC pour ASA-VPN](#)

[Étape 4. Rôle de pxGrid d'enable](#)

[Étape 5. Générez le certificat pour la gestion et le rôle de pxGrid](#)

[Enregistrement d'automatique de pxGrid d'étape 6.](#)

[WSA](#)

[Étape 1. Mode transparent et redirection](#)

[Étape 2. Génération de certificat](#)

[Étape 3. Connectivité du test ISE](#)

[Étape 4. Profils d'identification ISE](#)

[Étape 5. Accédez à la stratégie basée sur la balise SGT](#)

[Vérifiez](#)

[Étape 1. Session VPN](#)

[Étape 2. Les informations de session récupérées par le WSA](#)

[Étape 3. Redirection du trafic au WSA](#)

[Dépannez](#)

[Certificats incorrects](#)

[Scénario correct](#)

[Informations connexes](#)

Introduction

Ce document décrit comment intégrer l'appliance de sécurité Web (WSA) avec le Cisco Identity Services Engine (ISE). La version 1.3 ISE prend en charge un nouveau pxGrid appelé par API. Ce protocole moderne et flexible prend en charge l'authentification, le cryptage, et les privilèges

(groupes) qui tient compte de l'intégration facile avec d'autres solutions de sécurité.

La version 8.7 WSA prend en charge le protocole de pxGrid et peut récupérer les informations d'identité de contexte d'ISE. En conséquence, WSA te permet pour établir des stratégies basées sur des groupes de la balise de groupe de sécurité de TrustSec (SGT) récupérés d'ISE.

Conditions préalables

Conditions requises

Cisco recommande que vous ayez l'expérience avec la configuration de Cisco ISE et la connaissance de base de ces thèmes :

- Déploiements ISE et configuration d'autorisation
- Configuration CLI de l'appliance de sécurité adaptable (ASA) pour TrustSec et accès VPN
- Configuration WSA
- Compréhension de base des déploiements de TrustSec

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Microsoft Windows 7
- Version de logiciel 1.3 de Cisco ISE et plus tard
- Version 3.1 et ultérieures mobile de Sécurité de Cisco AnyConnect
- Version 9.3.1 et ultérieures de Cisco ASA
- Version 8.7 et ultérieures de Cisco WSA

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Configurez

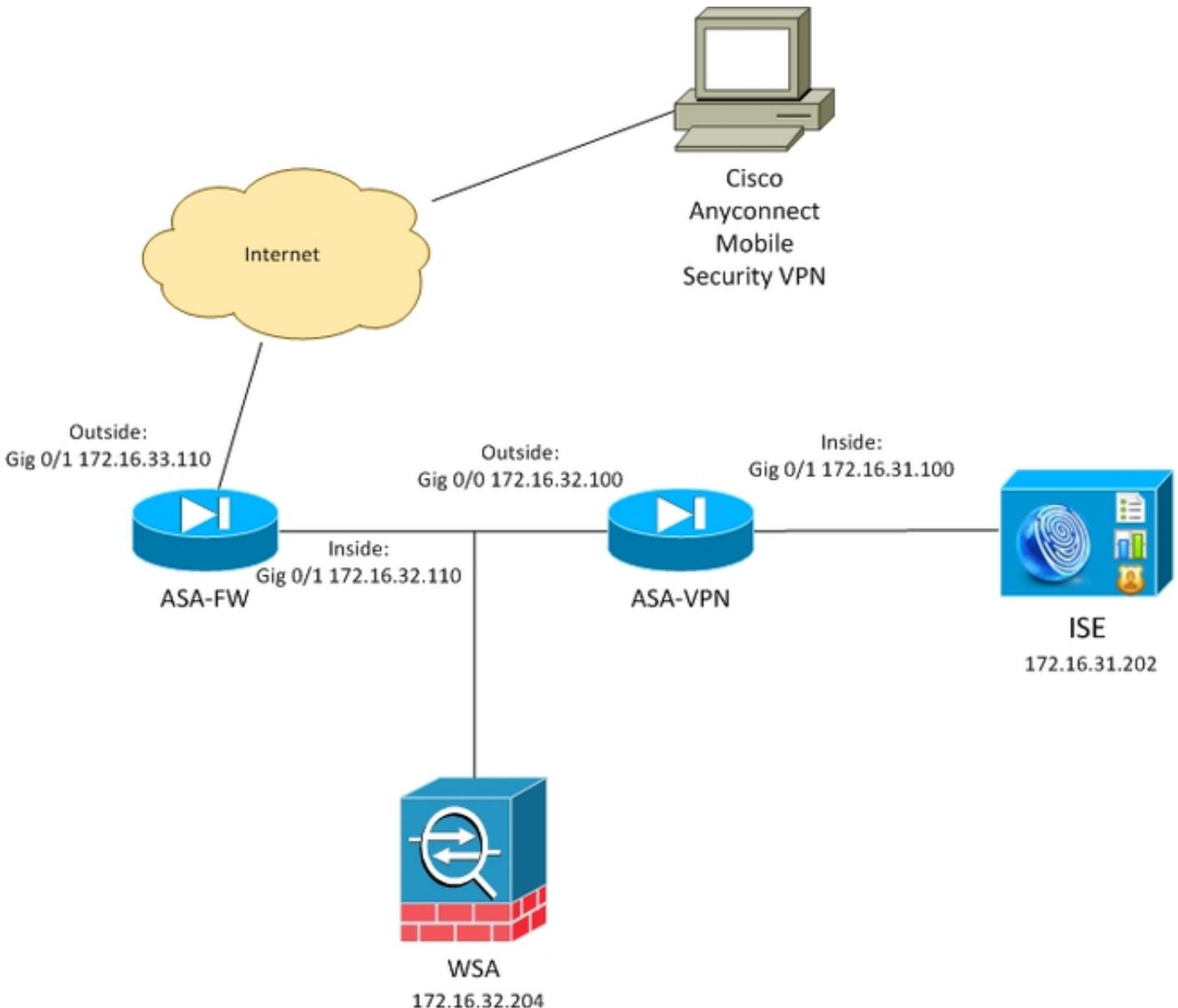
Note: Utilisez l'[Outil de recherche de commande](#) (clients [enregistrés](#) seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Schéma de réseau et circulation

Des balises de TrustSec SGT sont assignées par ISE utilisé en tant que serveur d'authentification pour tous les types d'utilisateurs qui accèdent au réseau d'entreprise. Ceci implique de câble/utilisateurs de sans fil qui authentifient par l'intermédiaire des portails de 802.1x ou d'invité ISE. En outre, utilisateurs distants VPN qui utilisent ISE pour l'authentification.

Pour WSA, il n'importe pas comment l'utilisateur a accédé au réseau.

Cet exemple présente des utilisateurs du distant un VPN terminant la session sur l'ASA-VPN. Ces utilisateurs ont été assignés une balise de la particularité SGT. Tout le trafic http à l'Internet sera intercepté par l'ASA-FW (Pare-feu) et réorienté au WSA pour l'inspection. Le WSA utilise l'identity profile qui lui permet pour classifier des utilisateurs basés sur la balise SGT et pour établir des stratégies d'accès ou de déchiffrement basées sur celle.



L'écoulement détaillé est :

1. L'utilisateur d'AnyConnect VPN termine la session de Secure Sockets Layer (SSL) sur l'ASA-VPN. L'ASA-VPN est configuré pour TrustSec et utilise ISE pour l'authentification des utilisateurs VPN. L'utilisateur authentifié est assigné une valeur de balise SGT = 2 (nom = service informatique). L'utilisateur reçoit une adresse IP du réseau 172.16.32.0/24 (172.16.32.50 dans cet exemple).
2. Les essais d'utilisateur pour accéder à la page Web en Internet. L'ASA-FW est configuré pour le Web Cache Communication Protocol (WCCP) qui réoriente le trafic au WSA.
3. Le WSA est configuré pour l'intégration ISE. Il emploie le pxGrid afin de télécharger les informations de l'ISE : l'IP address 172.16.32.50 d'utilisateur a été assigné la balise 2. SGT.

4. Le WSA traite la demande de HTTP de l'utilisateur et les hit accèdent à la stratégie PolicyForIT. Que la stratégie est configurée pour bloquer le trafic aux sites de sports. Tous autres utilisateurs (qui n'appartiennent pas à SGT 2) frappent la stratégie par défaut d'accès et ont l'accès complet aux sports situent.

ASA-VPN

C'est une passerelle VPN configurée pour TrustSec. La configuration détaillée est hors de portée de ce document. Référez-vous à ces exemples :

- [L'ASA et les séries du Catalyst 3750X commutent l'exemple de configuration de TrustSec et dépannent le guide](#)
- [Exemple de configuration de classification et d'application de la version 9.2 VPN SGT ASA](#)

ASA-FW

Le Pare-feu ASA est responsable de la redirection WCCP au WSA. Ce périphérique ne se rend pas compte de 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 est un point central dans le déploiement de TrustSec. Il assigne des balises SGT à tous les utilisateurs qui accèdent à et authentifient au réseau. L'étape nécessaire pour la configuration de base sont répertoriées dans cette section.

Étape 1. SGT pour le service informatique et tout autre groupe

Choisissez la **stratégie > les résultats > le groupe de sécurité Access > groupes de sécurité** et créez le SGT :

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

Étape 2. Règle d'autorisation pour l'accès VPN qui assigne SGT = 2 (service informatique)

Choisissez la **stratégie > l'autorisation** et créez une règle pour l'accès VPN distant. Toutes les connexions VPN établies par l'intermédiaire d'ASA-VPN obtiendront l'accès complet (PermitAccess) et seront assignées la balise 2 (service informatique) SGT.

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

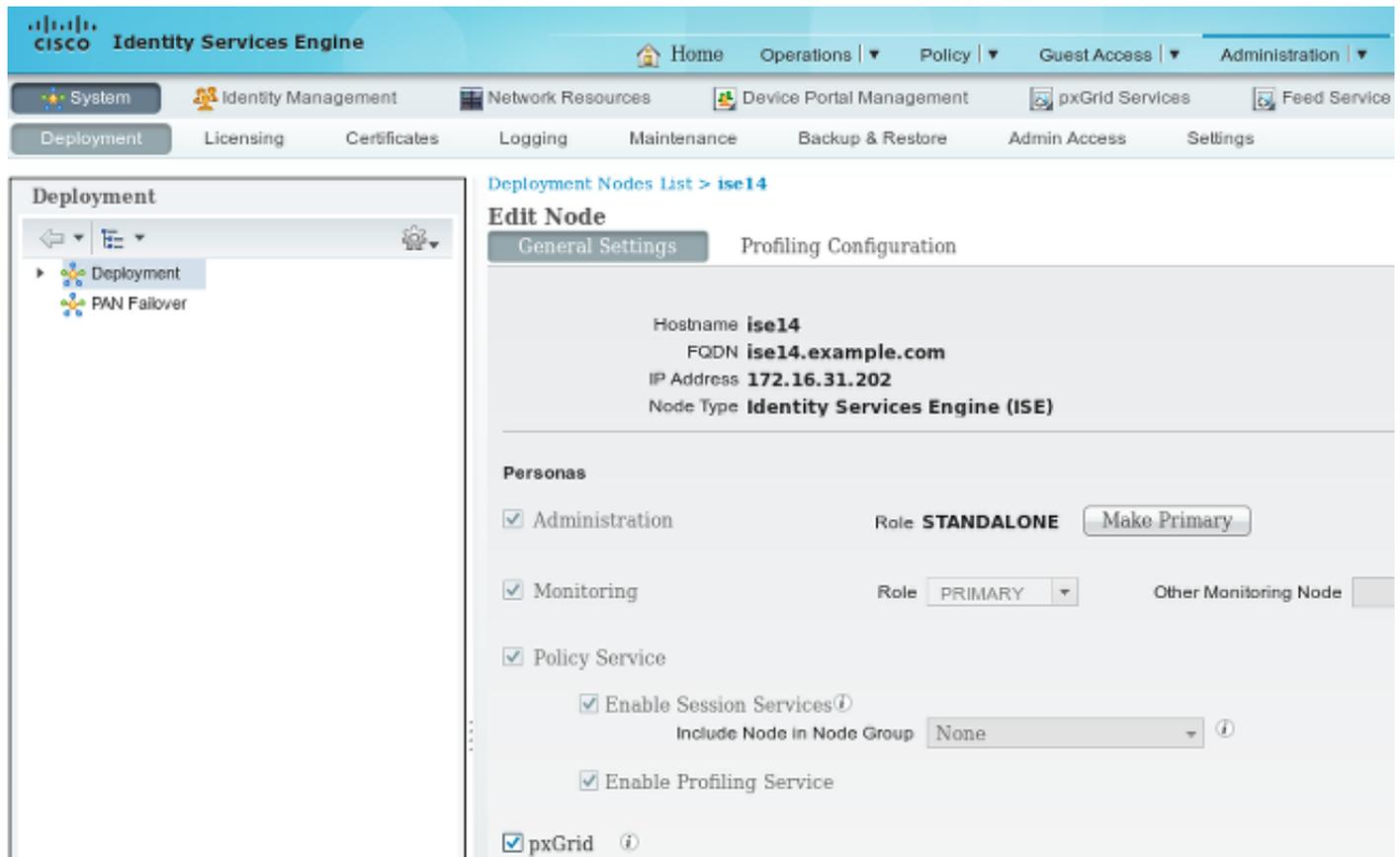
Étape 3. Ajoutez le périphérique de réseau et générez le fichier PAC pour ASA-VPN

Afin d'ajouter l'ASA-VPN au domaine de TrustSec, il est nécessaire de générer le fichier automatique du config de proxy (PAC) manuellement. Ce fichier sera importé sur l'ASA.

Cela peut être configuré des **périphériques de gestion > de réseau**. Après que l'ASA soit ajoutée, faites descendre l'écran aux configurations de TrustSec et générez le fichier PAC. Les détails pour celui sont décrits dans un document (référéncé) distinct.

Étape 4. Rôle de pxGrid d'enable

Choisissez la **gestion > le déploiement** afin d'activer le rôle de pxGrid.



The screenshot displays the Cisco Identity Services Engine (ISE) Administration interface. The top navigation bar includes 'Home', 'Operations', 'Policy', 'Guest Access', and 'Administration'. The main menu shows 'System', 'Identity Management', 'Network Resources', 'Device Portal Management', 'pxGrid Services', and 'Feed Service'. The 'Deployment' tab is selected, and the 'Edit Node' page for 'ise14' is shown. The 'General Settings' section includes fields for Hostname (ise14), FQDN (ise14.example.com), IP Address (172.16.31.202), and Node Type (Identity Services Engine (ISE)). The 'Personas' section is expanded, showing that 'Administration', 'Monitoring', and 'Policy Service' are enabled. The 'pxGrid' checkbox is also checked, indicating that the pxGrid role is enabled for this node.

Étape 5. Générez le certificat pour la gestion et le rôle de pxGrid

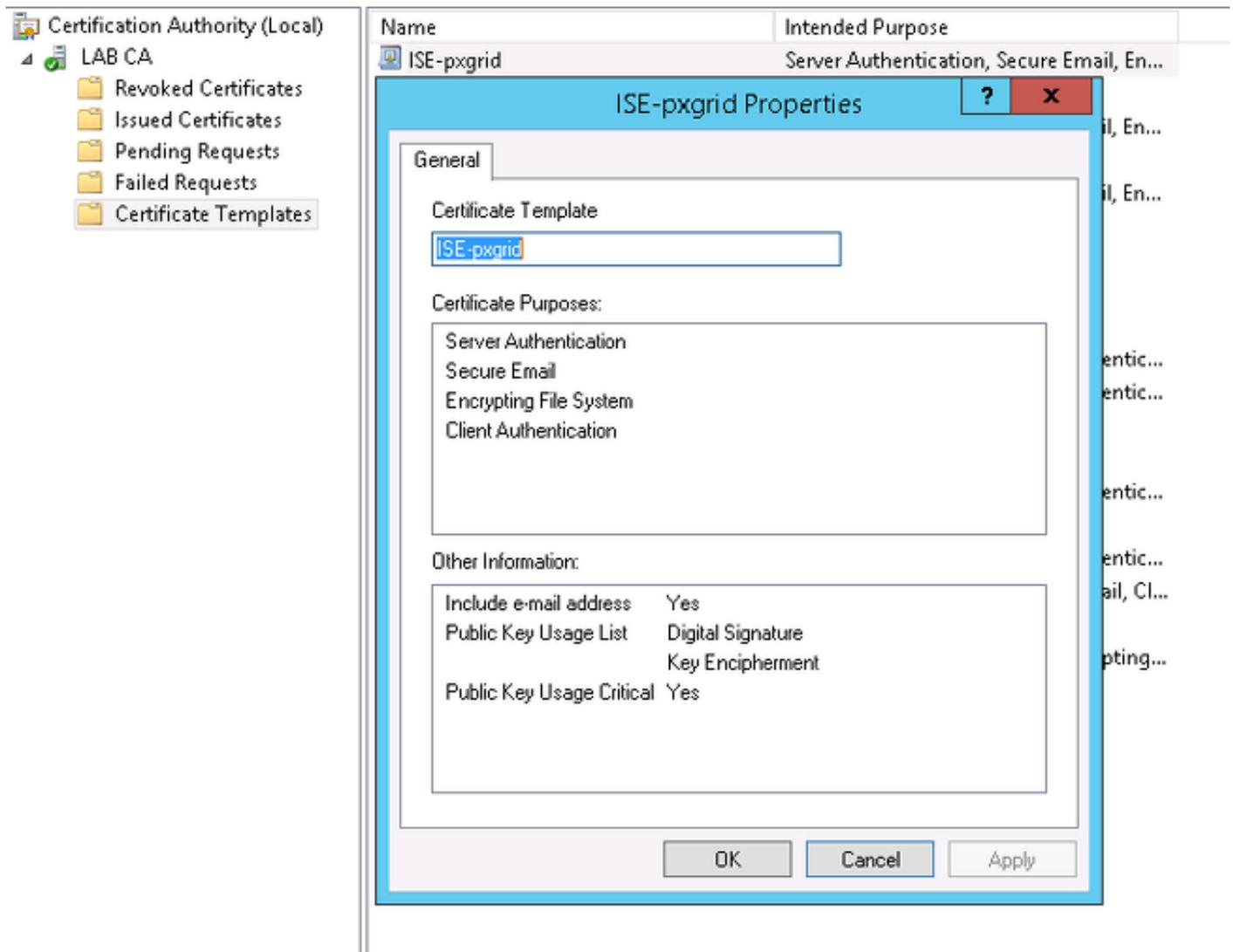
Les utilisations de protocole de pxGrid délivrent un certificat l'authentification pour le client et le serveur. Il est très important de configurer les Certificats corrects pour ISE et le WSA. Les deux Certificats devraient inclure le nom de domaine complet (FQDN) dans le sujet et les extensions x509 pour l'authentification client et l'authentification de serveur. En outre, assurez-vous que l'enregistrement correct des DN A est créé pour ISE et le WSA et apparie le FQDN correspondant.

Si les deux Certificats sont signés par un différent Autorité de certification (CA), il est important d'inclure ces CAs dans la mémoire de confiance.

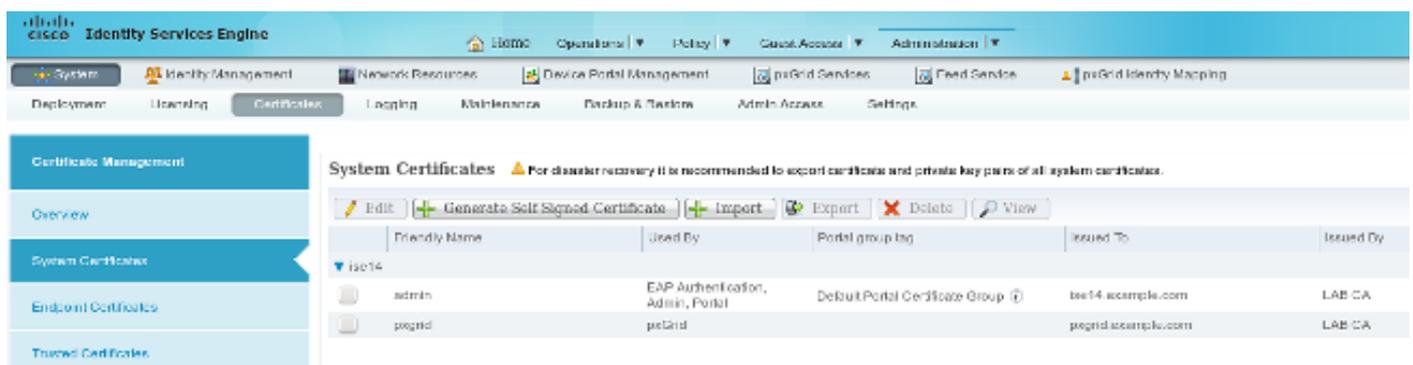
Afin de configurer des Certificats, choisissez la **gestion > les Certificats**.

ISE peut générer une demande de signature de certificat (CSR) de chaque rôle. Pour le rôle de pxGrid, exportez et signez le CSR avec un CA externe.

Dans cet exemple, Microsoft CA a été utilisé avec ce modèle :



Le résultat final pourrait ressembler à :



N'oubliez pas de créer les enregistrements des DN A pour ise14.example.com et pxgrid.example.com qui indiquent 172.16.31.202.

Enregistrement d'automatique de pxGrid d'étape 6.

Par défaut, ISE n'enregistrera pas automatiquement des abonnés de pxGrid. Cela devrait être manuellement approuvé par l'administrateur. Cette configuration devrait être changée pour l'intégration WSA.

Choisissez les **services de gestion > de pxGrid** et placez l'enregistrement automatique d'enable.

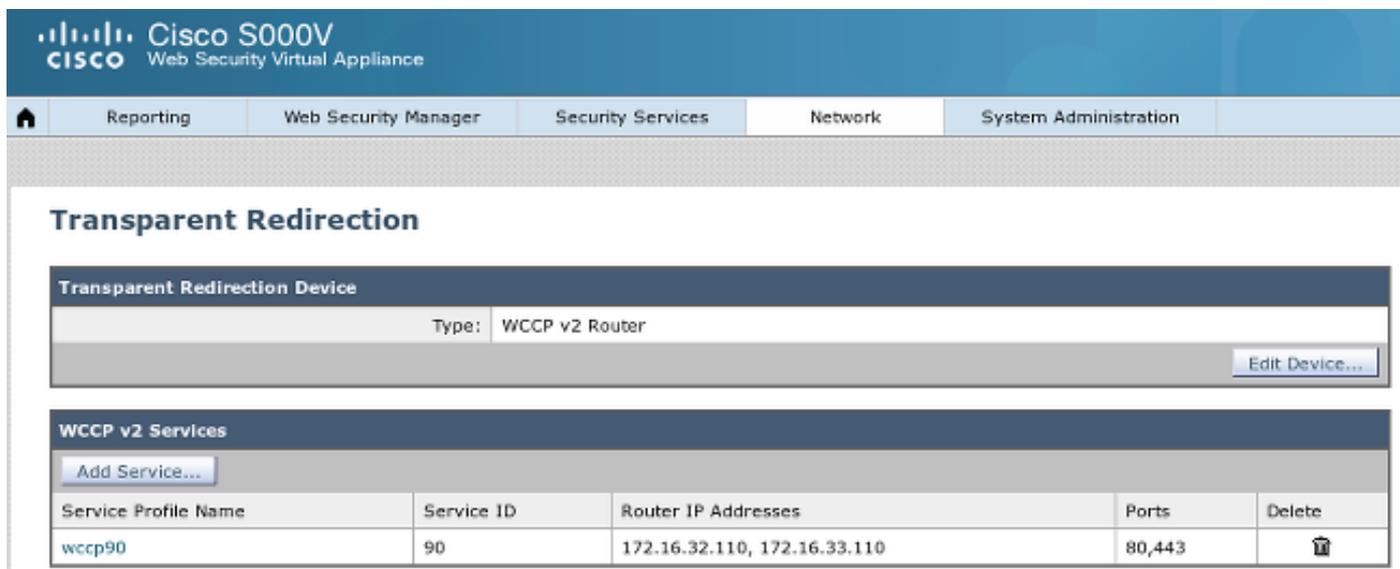
[View By Capabilities](#)

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

WSA

Étape 1. Mode transparent et redirection

Dans cet exemple, le WSA est configuré avec juste l'interface de gestion, le mode transparent, et la redirection de l'ASA :



The screenshot shows the configuration page for Transparent Redirection on a Cisco S000V Web Security Virtual Appliance. The page has a navigation bar with tabs for Reporting, Web Security Manager, Security Services, Network, and System Administration. The main content area is titled "Transparent Redirection" and contains 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	

Étape 2. Génération de certificat

Le WSA doit faire confiance au CA pour signer tous les Certificats. Choisissez la **Gestion de réseau > de certificat** afin d'ajouter un certificat de CA :

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

Il est également nécessaire de générer un certificat que le WSA l'utilisera afin d'authentifier au pxGrid. Choisissez le **réseau > le Cisco Identity Services Engine > le certificat client WSA** afin de générer le CSR, signez-le avec le modèle correct CA (ISE-pxgrid), et importez-le de retour.

En outre, parce que « le certificat d'admin ISE » et « le certificat de pxGrid ISE », importent le certificat de CA (afin de faire confiance au certificat de pxGrid présenté par ISE) :

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...

Étape 3. Connectivité du test ISE

Choisissez le **réseau** > le **Cisco Identity Services Engine** afin de tester la connexion à ISE :

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.

Étape 4. Profils d'identification ISE

Choisissez les **profils de gestionnaire** > **d'identification de sécurité Web** afin d'ajouter un nouveau profil pour ISE. Pour » l'usage « de « *identification et d'authentification identifiez d'une manière transparente les utilisateurs avec 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 the 'ISE' profile and one for the '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	

Étape 5. Accédez à la stratégie basée sur la balise SGT

Choisissez le **gestionnaire de sécurité Web** > les **stratégies d'Access** afin d'ajouter une nouvelle stratégie. L'adhésion utilise le profil ISE :

Access Policy: PolicyForIT

Policy Settings

Enable Policy

Policy Name:
(e.g. my IT policy)

Description:

Insert Above Policy:

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:

Identification Profile	Authorized Users and Groups	<input type="button" value="Add Identification Profile"/>
<input type="text" value="ISE"/>	<p><input type="radio"/> All Authenticated Users</p> <p><input checked="" type="radio"/> Selected Groups and Users <small>?</small></p> <p>ISE Secure Group Tags: IT</p> <p>Users: No users entered</p> <p><input type="radio"/> Guests (users failing authentication)</p>	

Pour des groupes sélectionnés et des utilisateurs la balise 2 SGT sera ajoutée (service informatique) :

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 checked="" type="checkbox"/>
ANY	65535	Any Security Group	<input type="checkbox"/>

La stratégie refuse l'accès à tous les sites de sports pour les utilisateurs qui appartiennent au service informatique SGT :

Access Policies

Policies							
Add Policy...							
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	

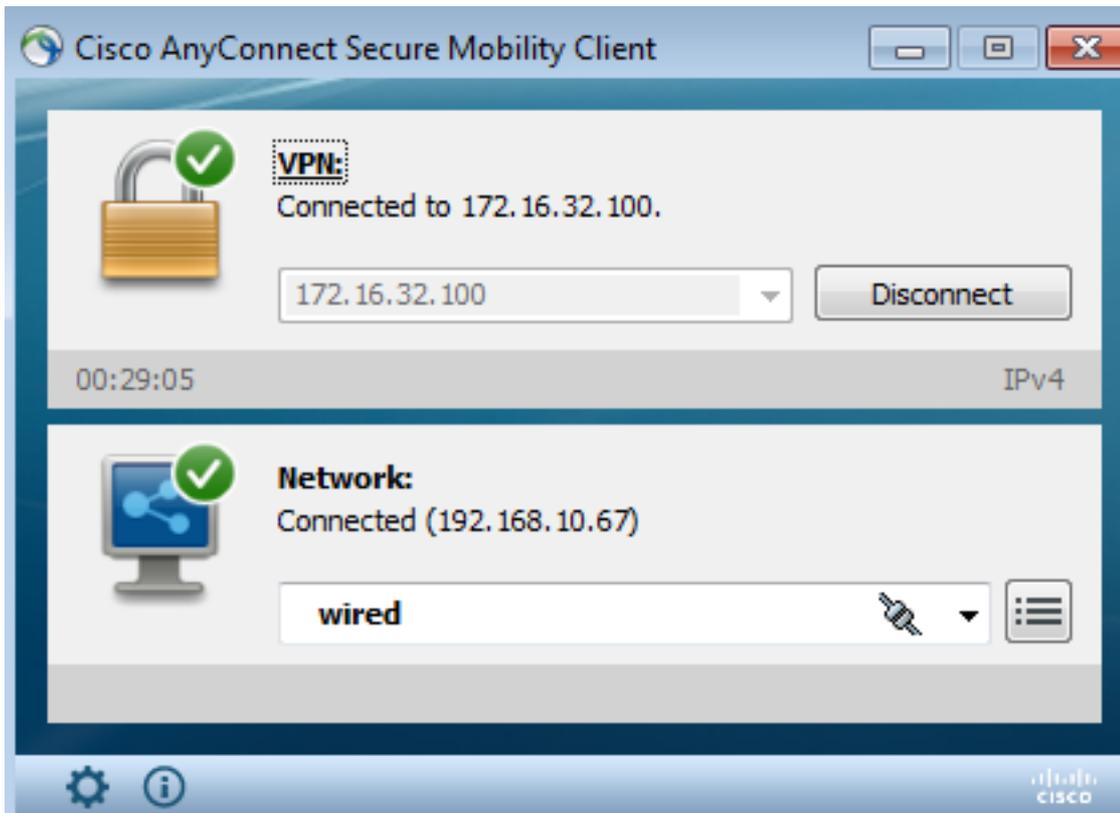
[Edit Policy Order...](#)

Vérifiez

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

Étape 1. Session VPN

L'utilisateur VPN initie une session VPN vers l'ASA-VPN :



L'ASA-VPN utilise ISE pour l'authentification. ISE crée une session et assigne la balise 2 (service informatique) SGT :

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

Après l'authentification réussie, l'ASA-VPN crée une session VPN avec la balise 2 SGT (retournée dans Radius Access-recevez dans les Cisco-poids du commerce-paires) :

```
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

Puisque le lien entre l'ASA-VPN et l'ASA-FW n'est pas TrustSec activé, l'ASA-VPN envoie des trames non marquées pour ce trafic (ne pourriez pas à GRE encapsulent des trames Ethernet avec le champ CMD/TrustSec injecté).

Étape 2. Les informations de session récupérées par le WSA

À ce stade, le WSA devrait recevoir le mappage entre l'adresse IP, le nom d'utilisateur, et le SGT (par l'intermédiaire du protocole de pxGrid) :

```
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
[ ]> █
```

Étape 3. Redirection du trafic au WSA

L'utilisateur VPN initie une connexion à sport.pl, qui est intercepté par l'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
```

et percé un tunnel dans GRE au WSA (avis que le router-id WCCP est l'adresse IP la plus élevée configurée) :

```
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
```

Le WSA continue la prise de contact de TCP et traite la demande GET. En conséquence, la stratégie nommée PolicyForIT est frappée et le trafic est bloqué :

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

Cela est confirmé par l'état WSA :

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.

Notez qu'ISE affiche le nom d'utilisateur.

Dépannez

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Certificats incorrects

Quand le WSA n'est pas correctement initialisé (des Certificats), déterminez la panne de connexion ISE :

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.

Les états ISE pxgrid-cm.log :

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

La raison pour la panne peut être vue avec 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)

Pour une session SSL utilisée pour protéger l'échange extensible de Protocole de Messagerie et de présence (XMPP) (utilisé par le pxGrid), la panne SSL d'états de client en raison d'une chaîne de certificat inconnue a présenté par le serveur.

Scénario correct

Pour le scénario correct, l'ISE pxgrid-controller.log se connecte :

```
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
```

En outre, le GUI ISE présente le WSA en tant qu'abonné avec les capacités correctes :

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-pxgrid...	pxGrid Connection from WSA	Capabilities(0 Pub, 2 Sub)	Online	Session	View

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

Client Name	Client Description	Capabilities	Status	Client Group	Log
wsa.example.com-test_client	pxGrid Connection from WSA	Capabilities(0 Pub, 0 Sub)	Offline	Session	View

Informations connexes

- [Posture de la version 9.2.1 VPN ASA avec l'exemple de configuration ISE](#)
- [Guide des utilisateurs WSA 8.7](#)
- [L'ASA et les séries du Catalyst 3750X commutent l'exemple de configuration de TrustSec et dépannent le guide](#)
- [Guide de configuration de commutateur de Cisco TrustSec : Compréhension du Cisco TrustSec](#)
- [Configurer un serveur externe pour l'autorisation d'utilisateur de dispositifs de sécurité](#)
- [Guide de configuration de la gamme VPN CLI de Cisco ASA, 9.1](#)
- [Guide de l'utilisateur de Logiciel Cisco Identity Services Engine, version 1.2](#)
- [Support et documentation techniques - Cisco Systems](#)