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

Contenu

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

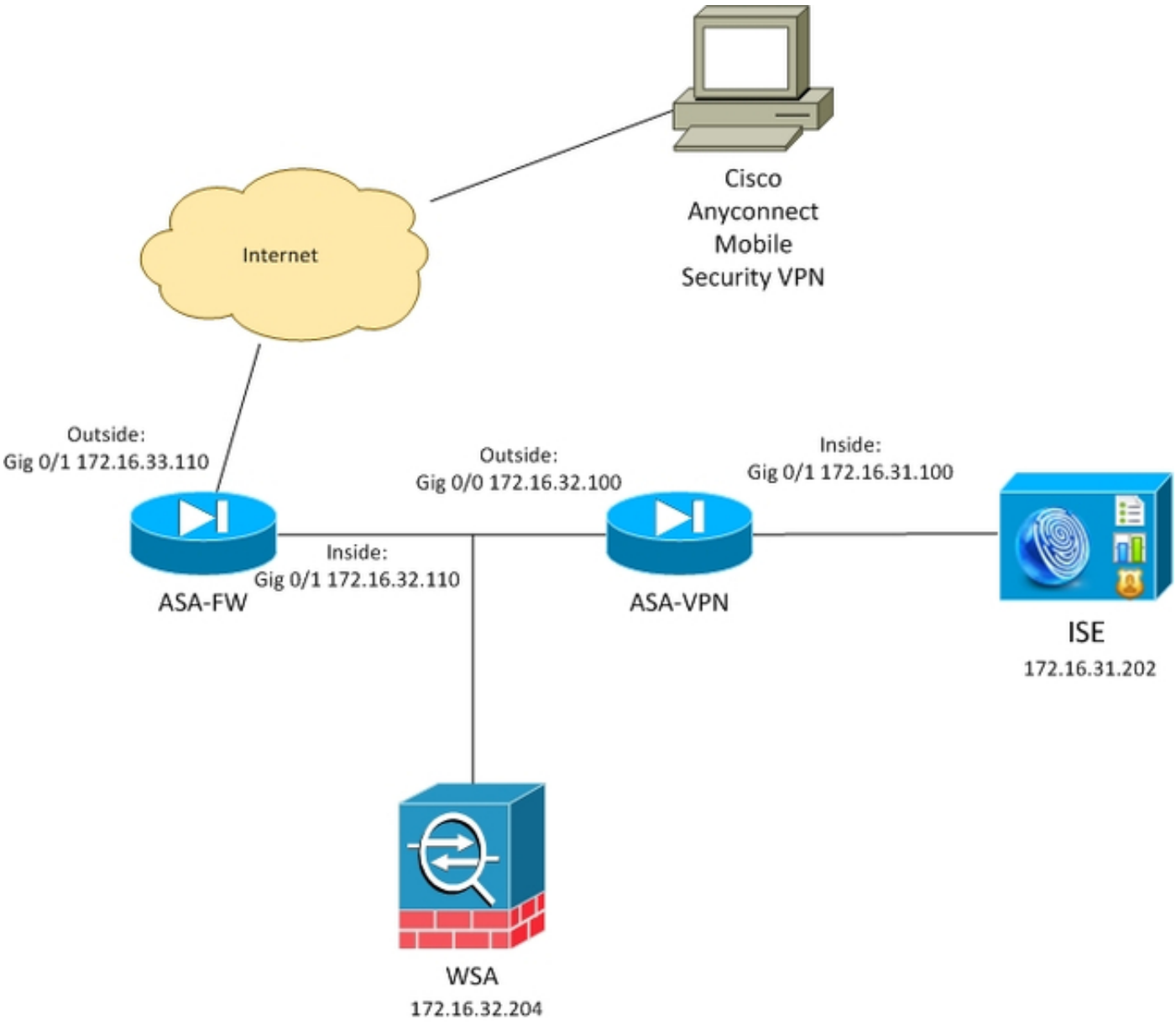
> **Note**: Utilisez l'Outil de recherche de commande (clients enregistrés seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

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.

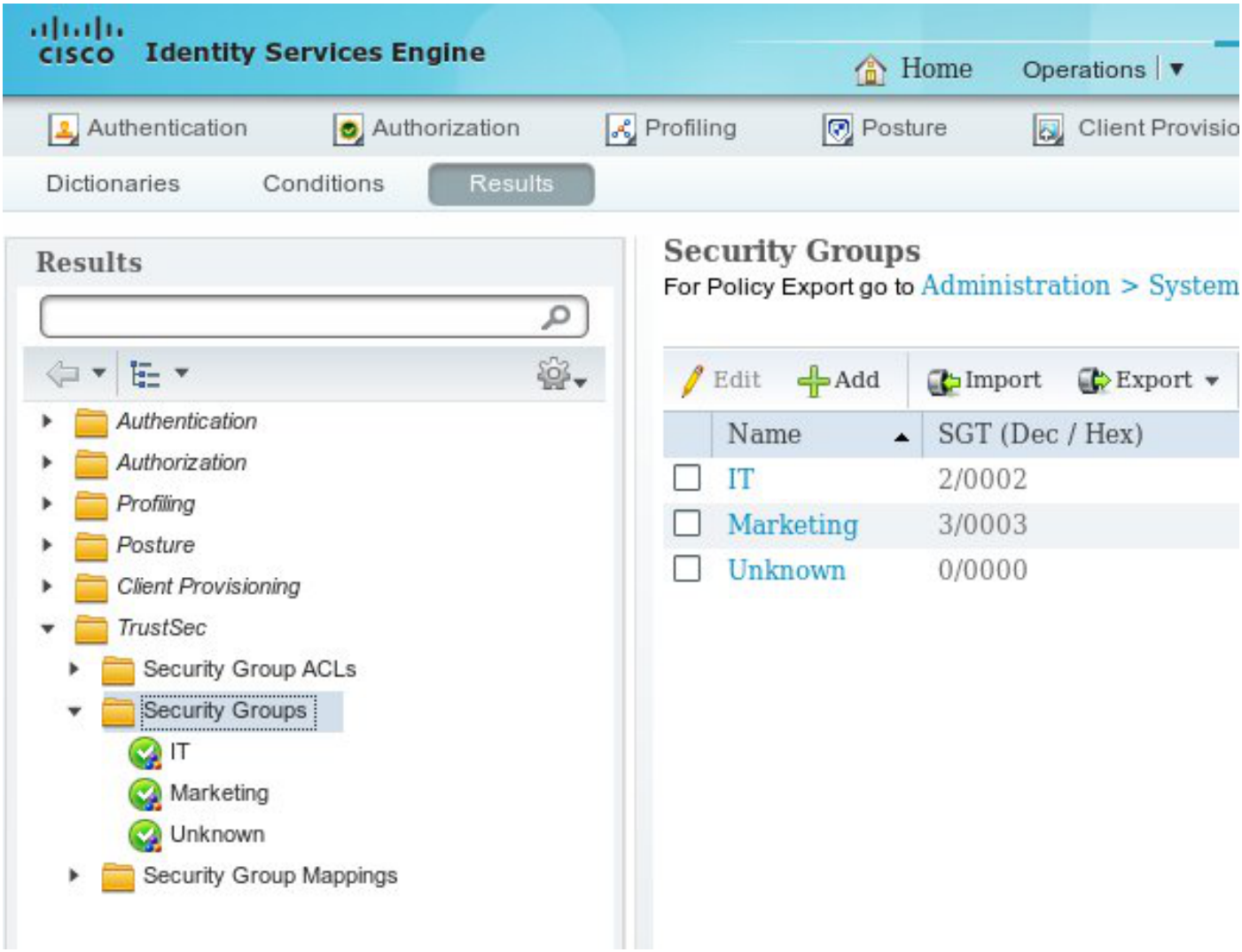
```
interface GigabitEthernet0/0
 nameif outside
 security-level 100
 ip address 172.16.33.110 255.255.255.0

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.

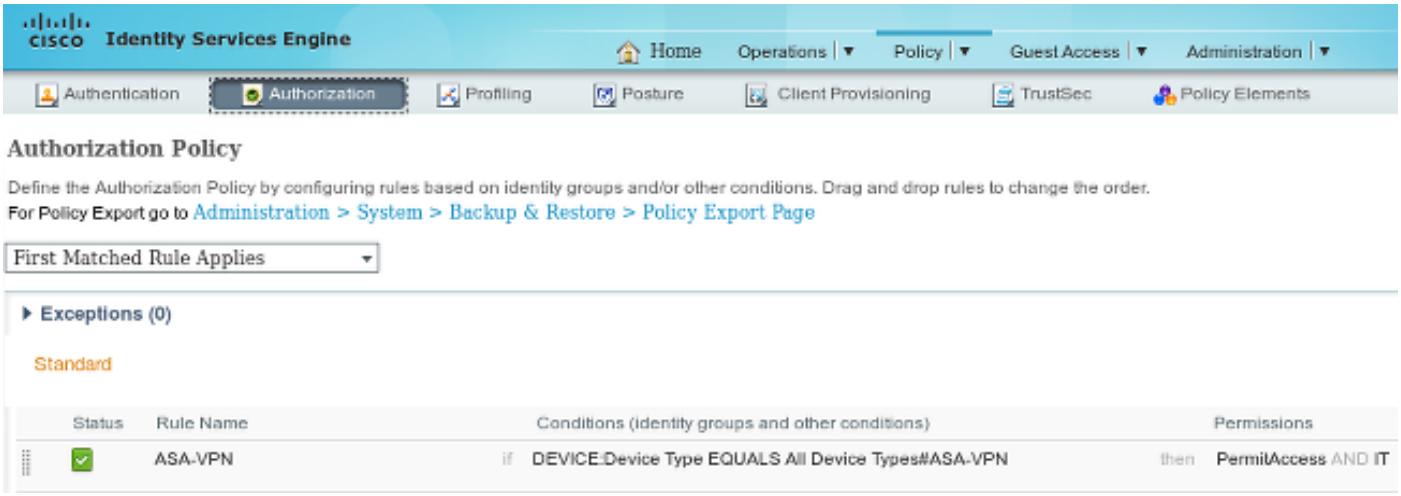
Étape 1. SGT pour le service informatique et tout autre groupe

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



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.



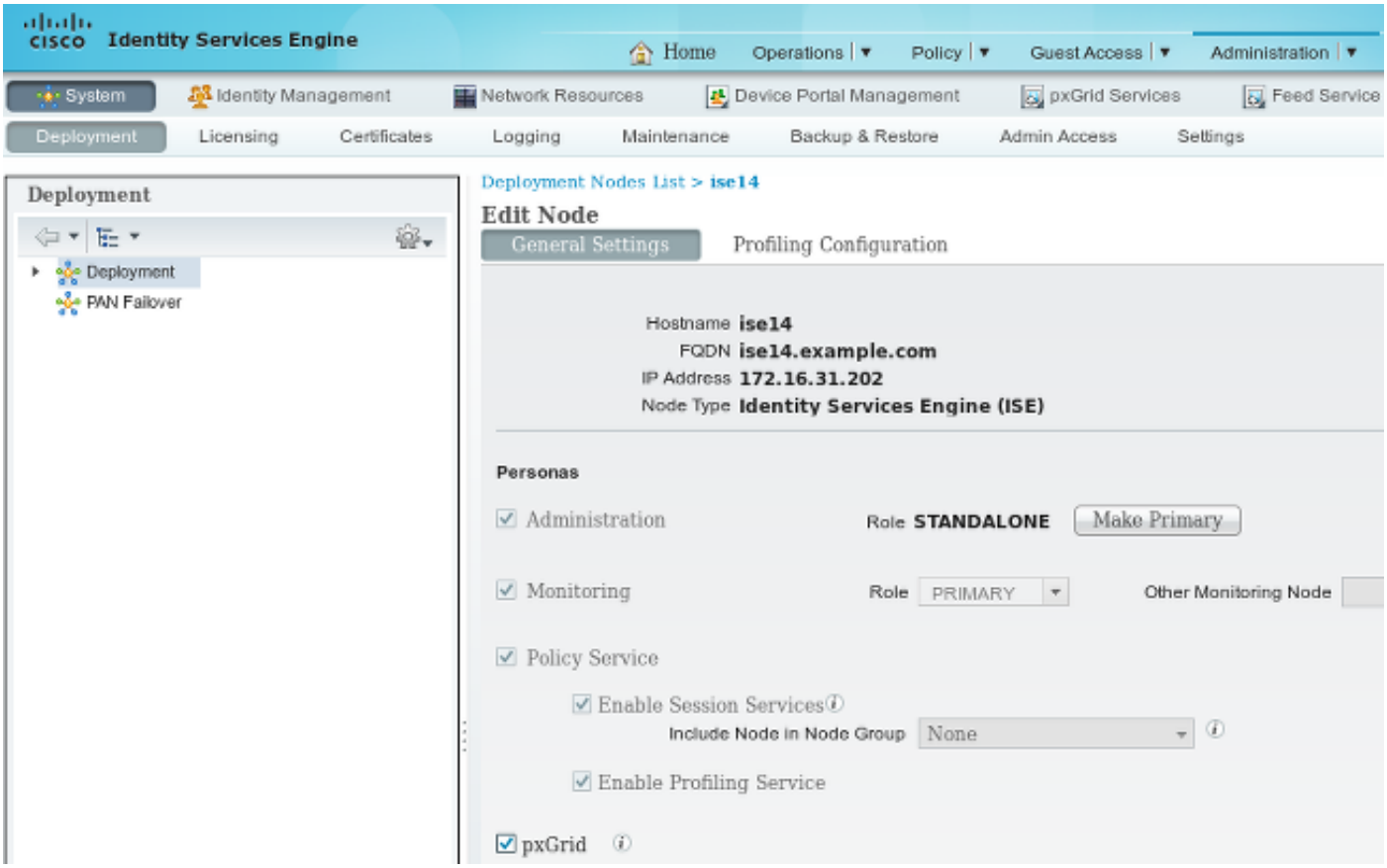
Étape 3. Ajoutez le périphérique de réseau et générez le fichier PAC pour ASA-VPN

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 (référencé) distinct.

Étape 4. Rôle de pxGrid d'enable

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



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

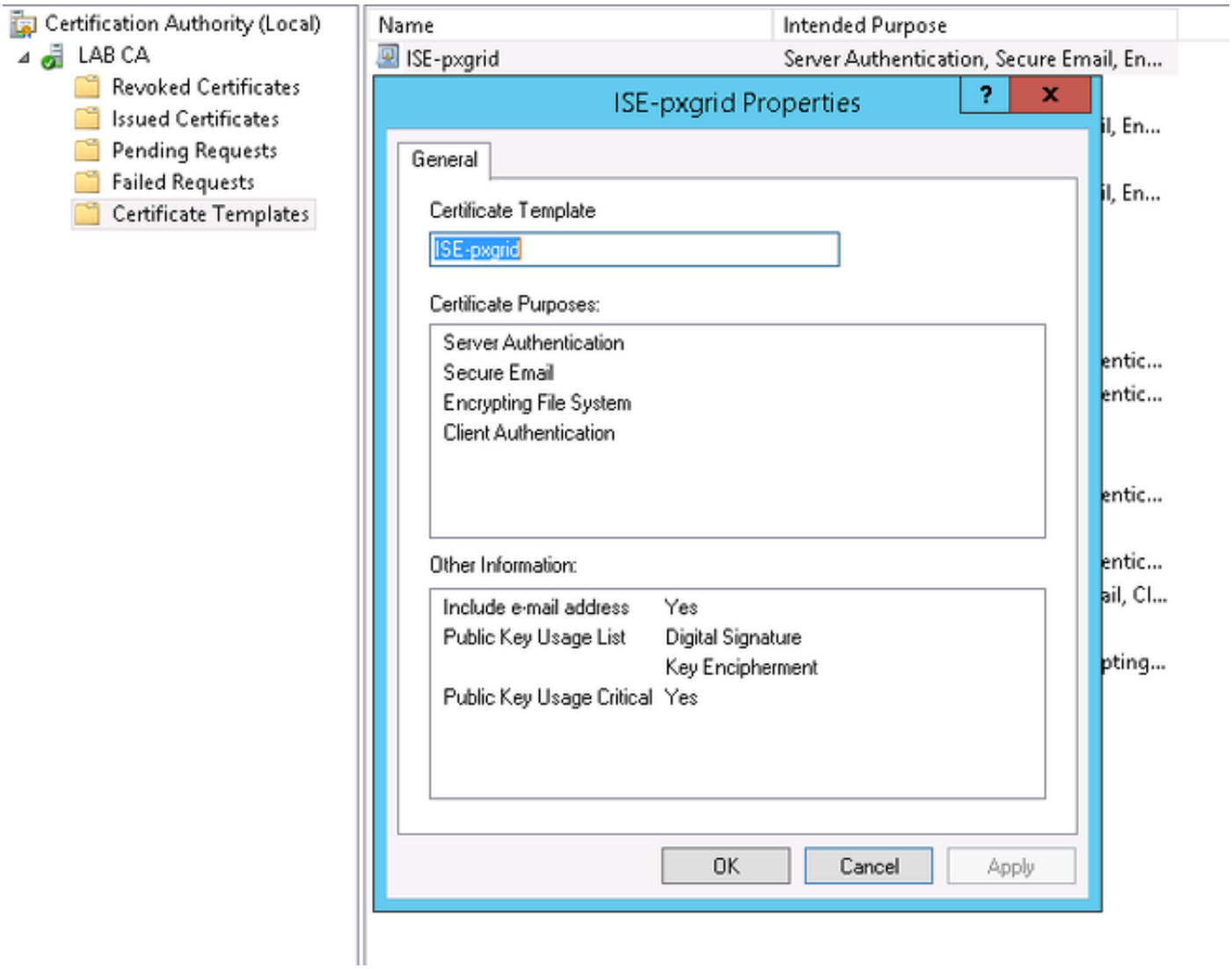
Les utilisations de protocole de pxGrid délivrent un certificat l'authentification pour le client et le serveur. Il est très important de configurer les Certificats corrects pour ISE et le WSA. Les deux Certificats devraient inclure le nom de domaine complet (FQDN) dans le sujet et les extensions x509 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.

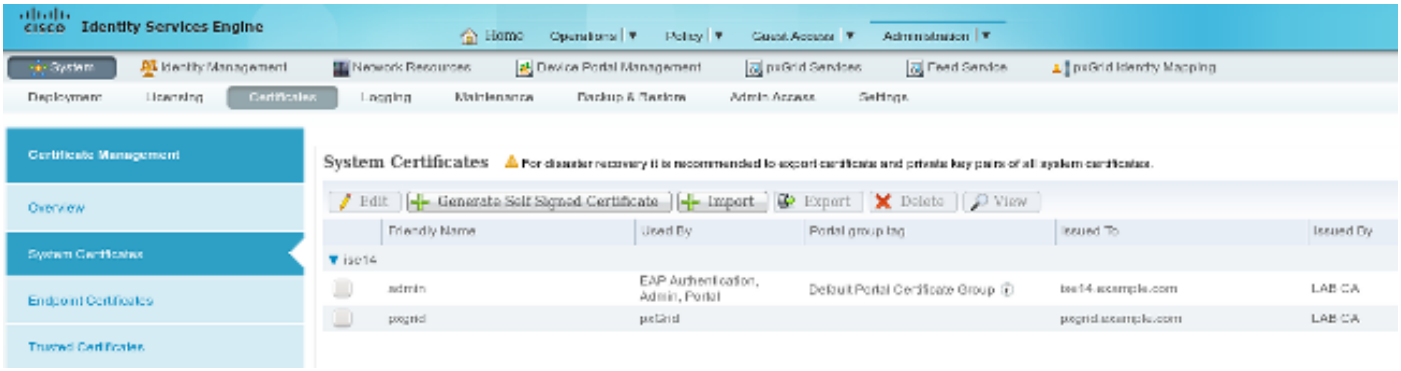
Afin de configurer des Certificats, choisissez la **gestion > les Certificats**.

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 :

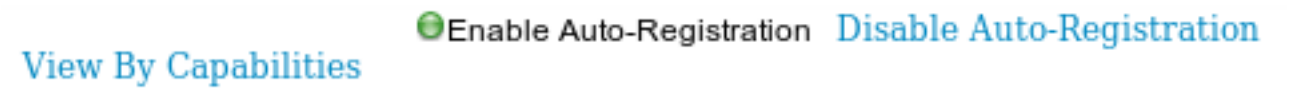


N'oubliez pas de créer les enregistrements des DN A pour ise14.example.com et pxgrid.example.com qui indiquent 172.16.31.202.

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.

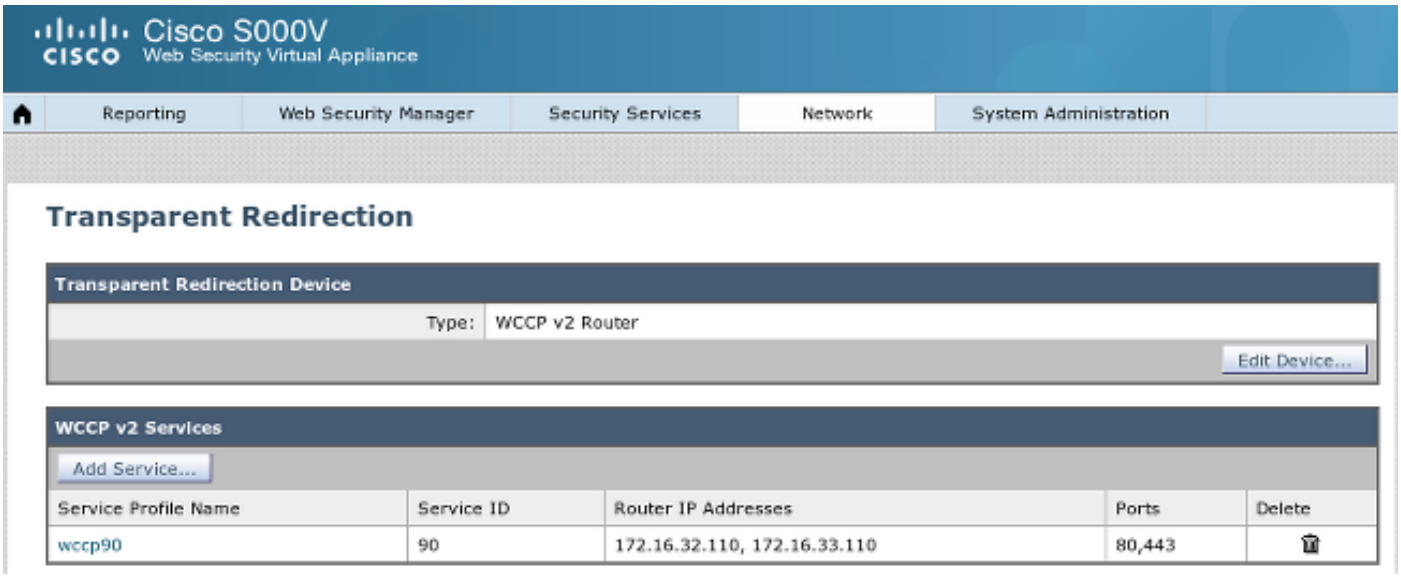
Choisissez les **services de gestion > de pxGrid** et placez l'**enregistrement automatique d'enable**.



WSA

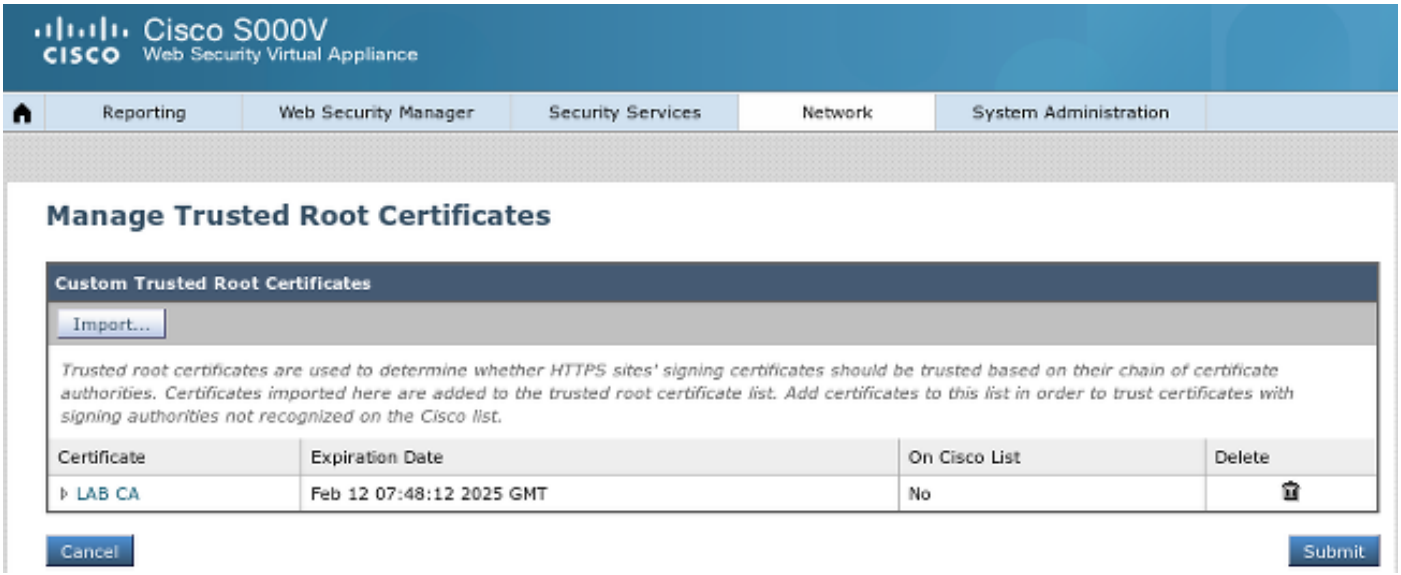
Étape 1. Mode transparent et redirection

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



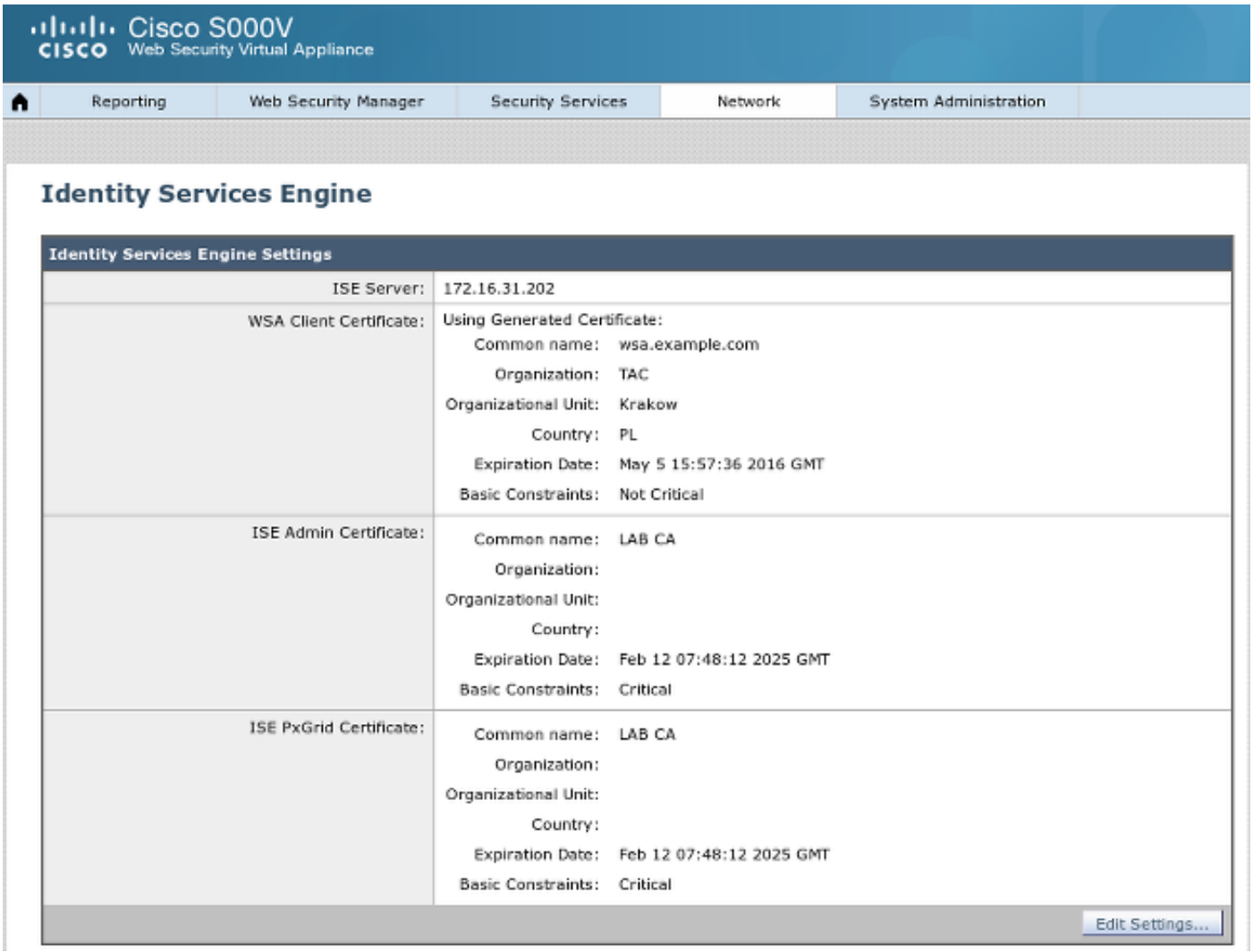
Étape 2. Génération de certificat

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 :



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) :

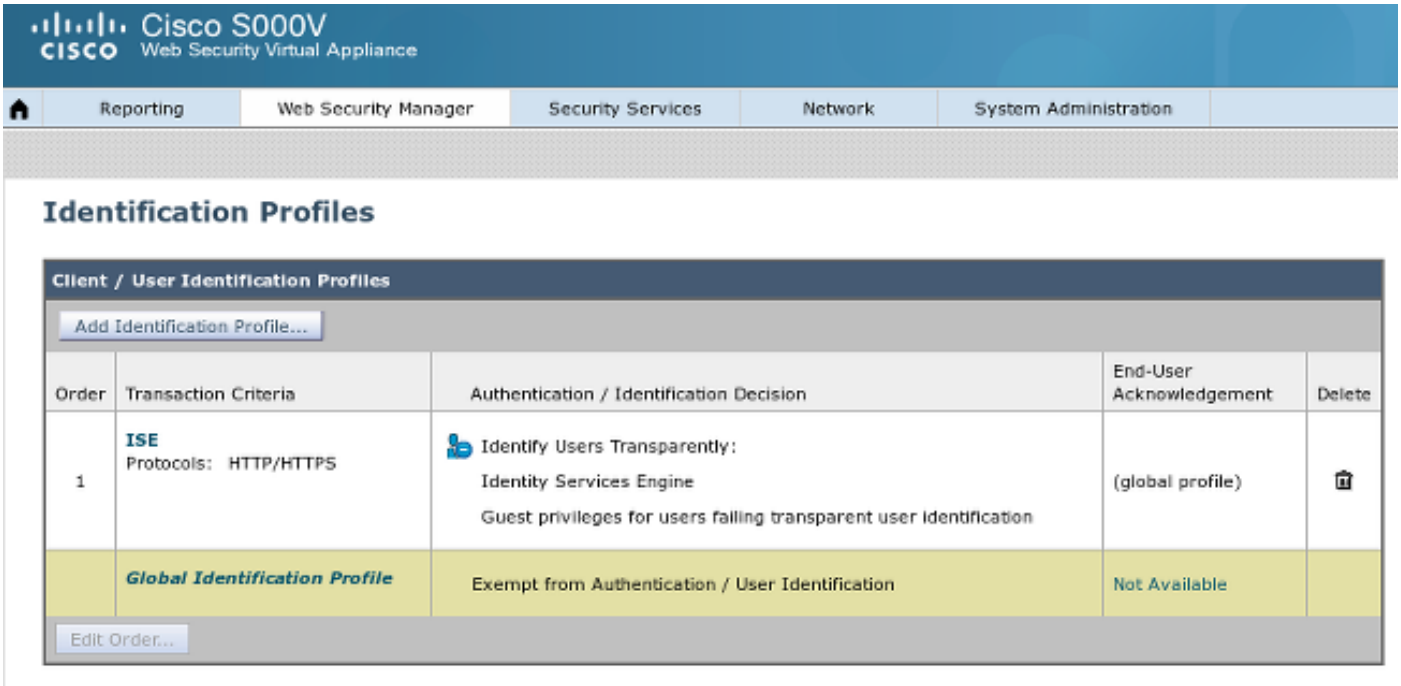


Étape 3. Connectivité du test ISE

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

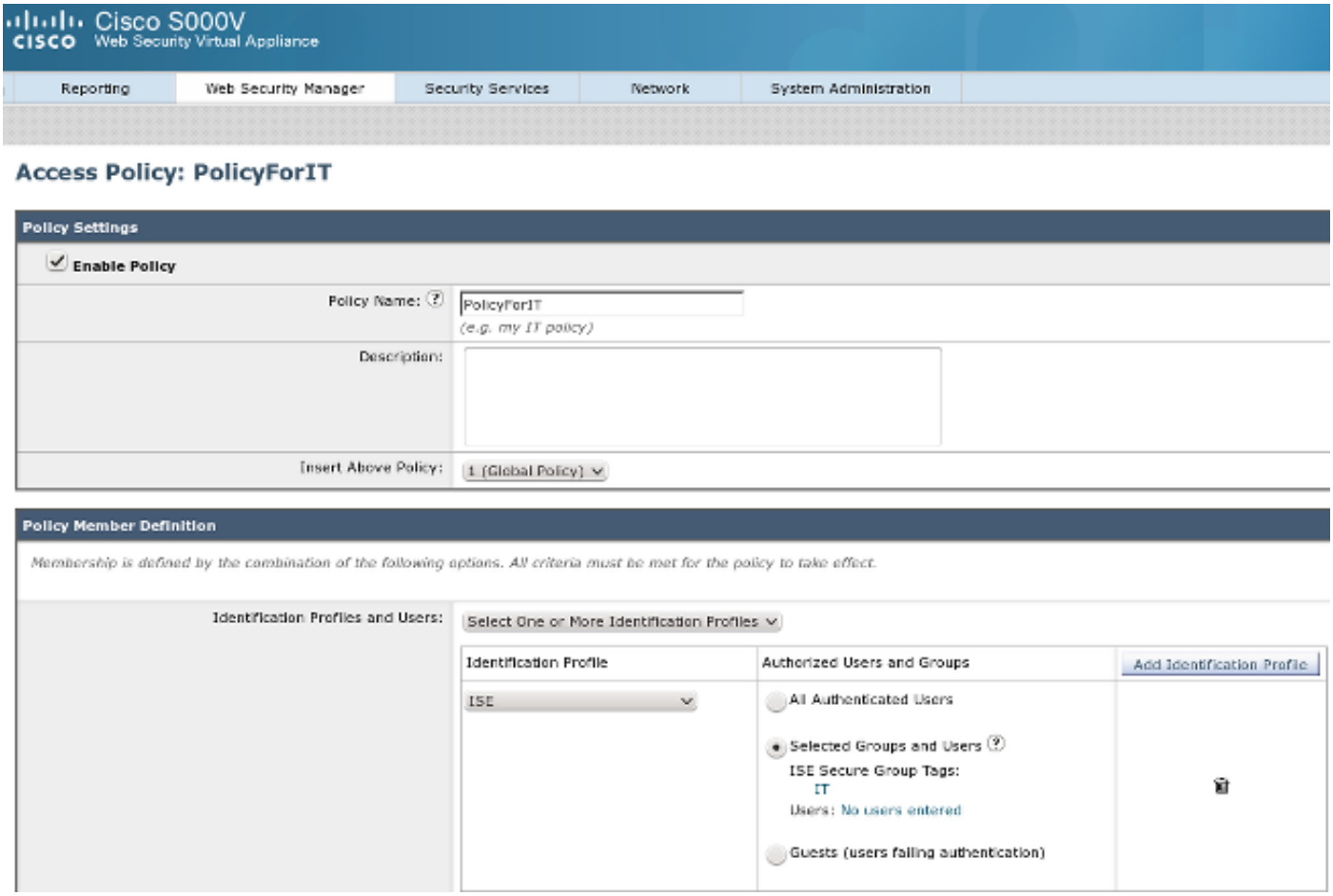
Étape 4. Profils d'identification ISE

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 ».*

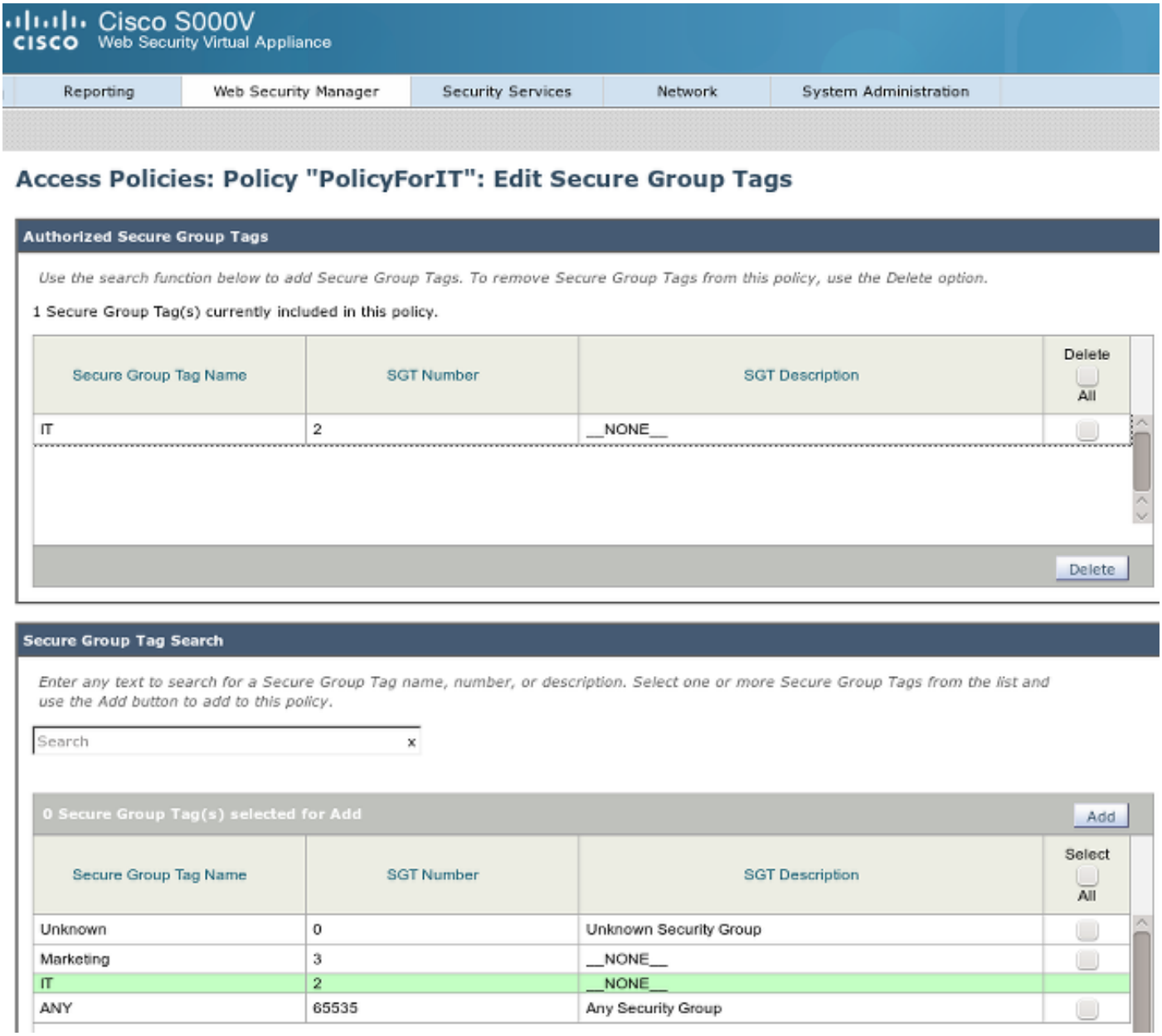


Étape 5. Accédez à la stratégie basée sur la balise SGT

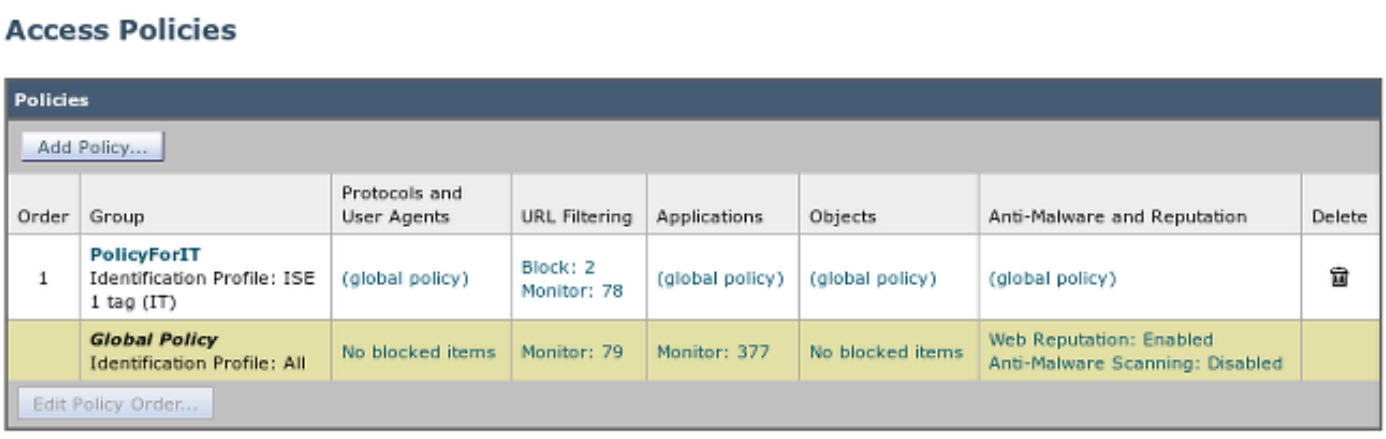
Choisissez le **gestionnaire de sécurité Web > les stratégies d'Access** afin d'ajouter une nouvelle stratégie. L'adhésion utilise le profil ISE :



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



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

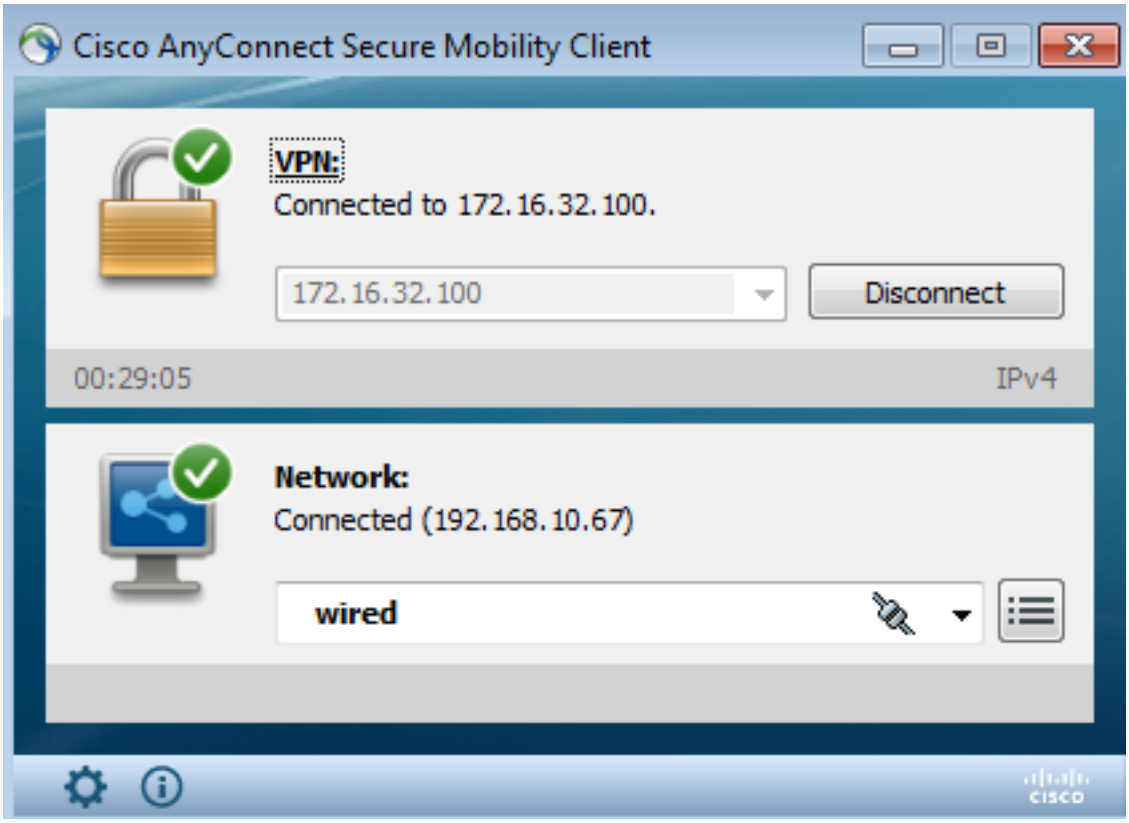


Vérifiez

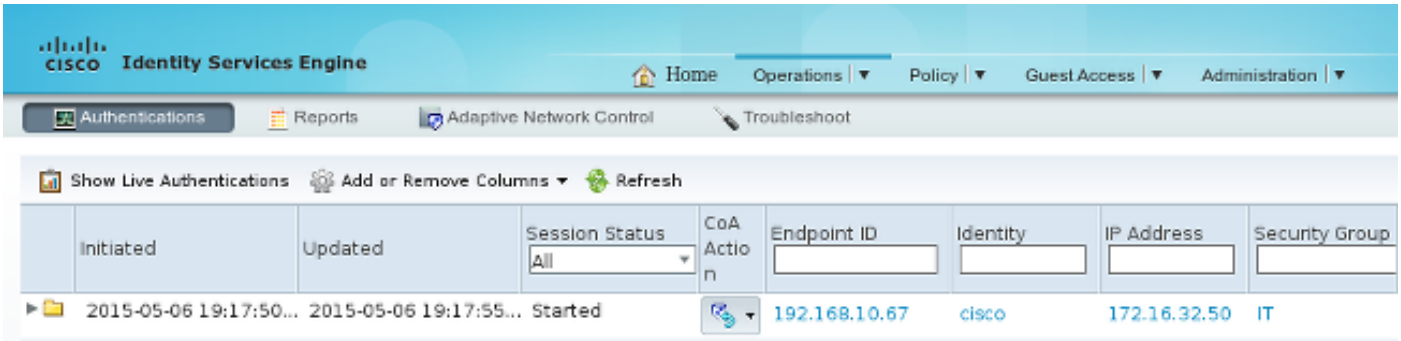
Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

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 :



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

Àce 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 :

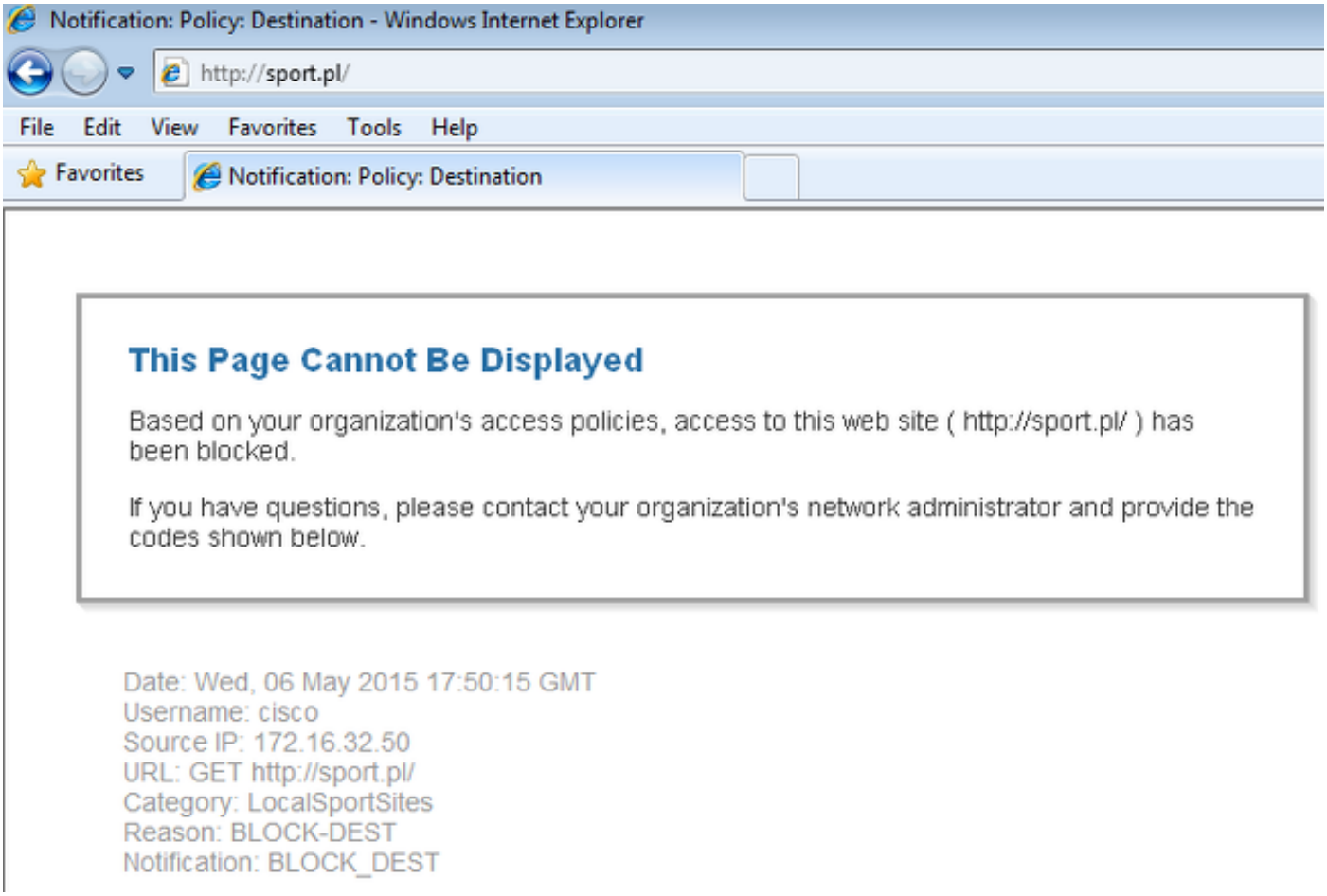
```
asa-fw# show wccp

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
```

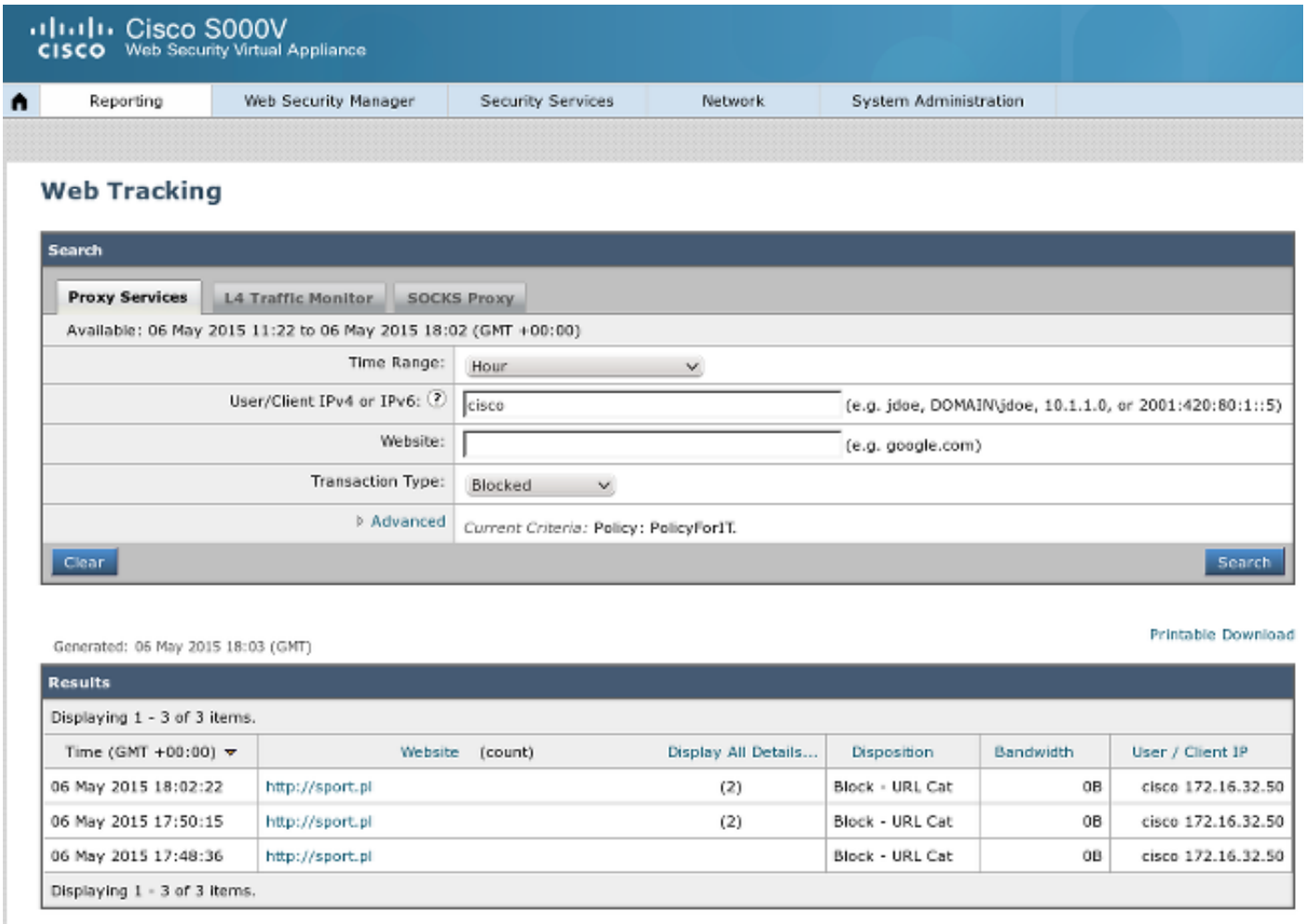
et percé un tunnel dans GRE au WSA (avis que le router-id WCCP est l'adresse IP la plus élevée configurée) :

```
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 :



Cela est confirmé par l'état WSA :



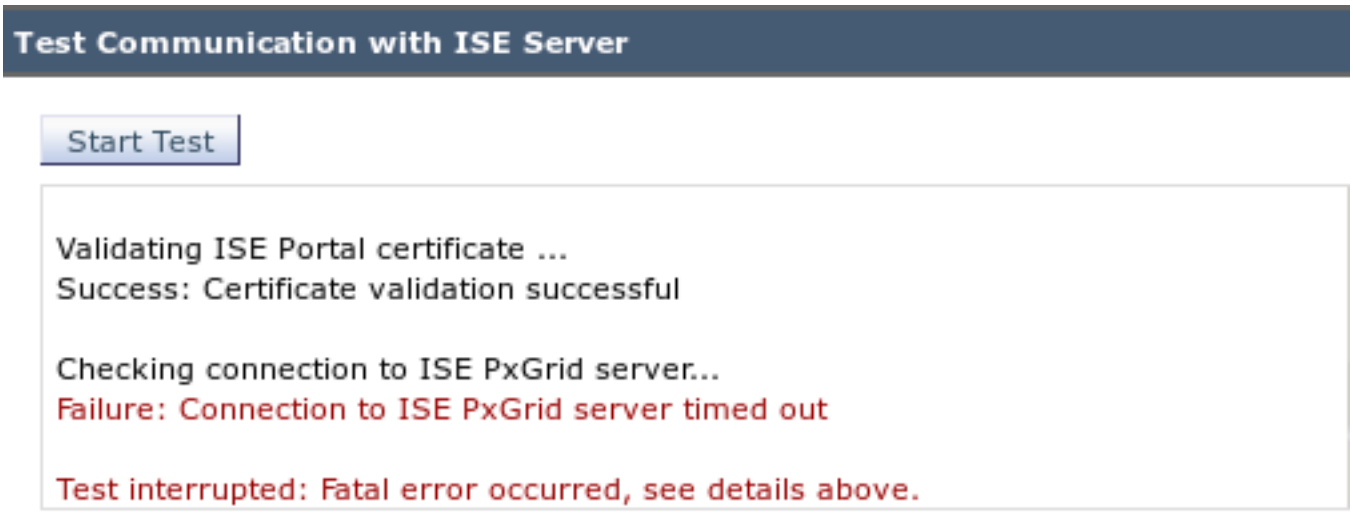
Notez qu'ISE affiche le nom d'utilisateur.

Dépannez

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

Certificats incorrects

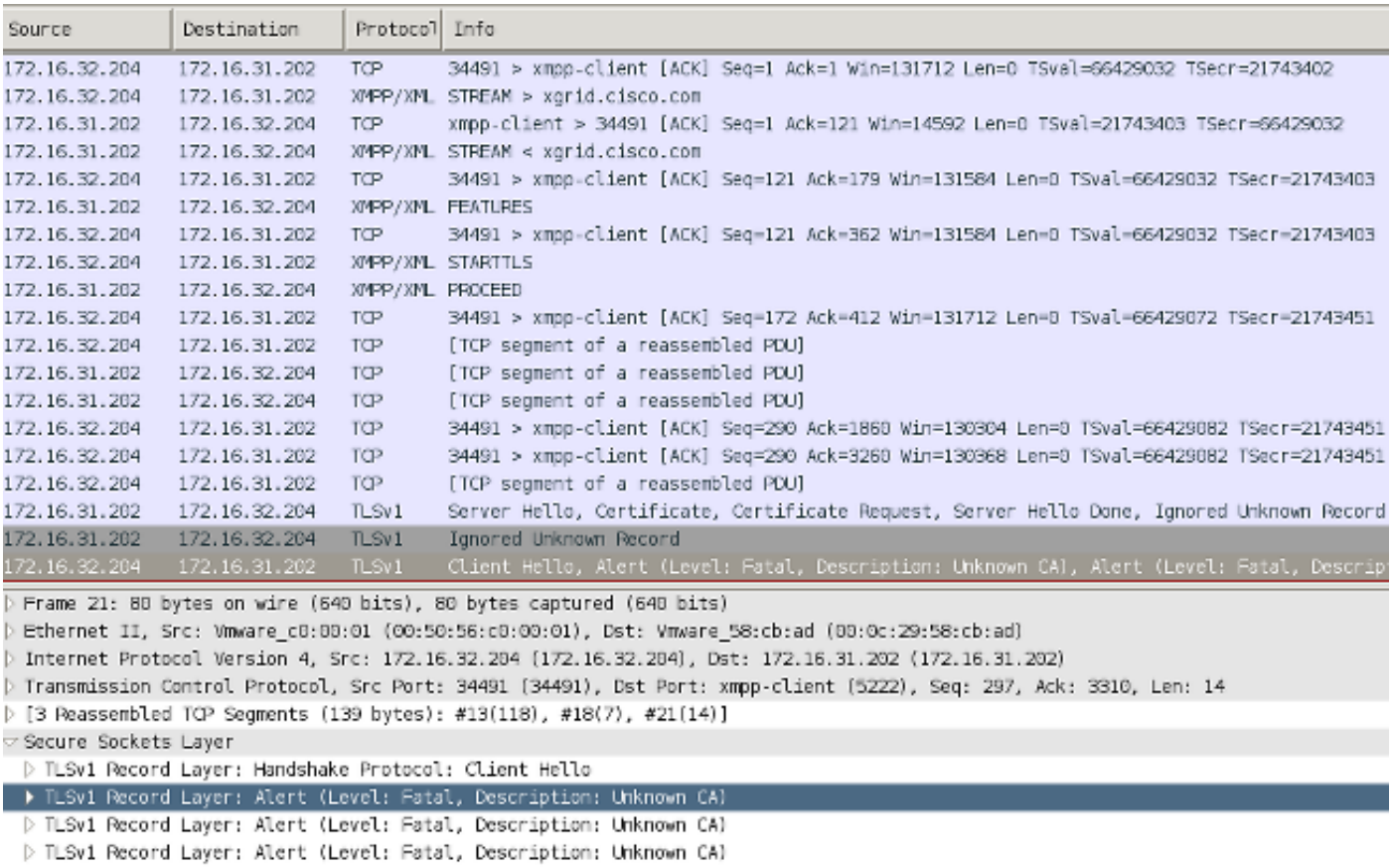
Quand le WSA n'est pas correctement initialisé (des Certificats), déterminez la panne de connexion ISE :



Les états ISE pxgrid-cm.log :

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

La raison pour la panne peut être vue avec Wireshark :



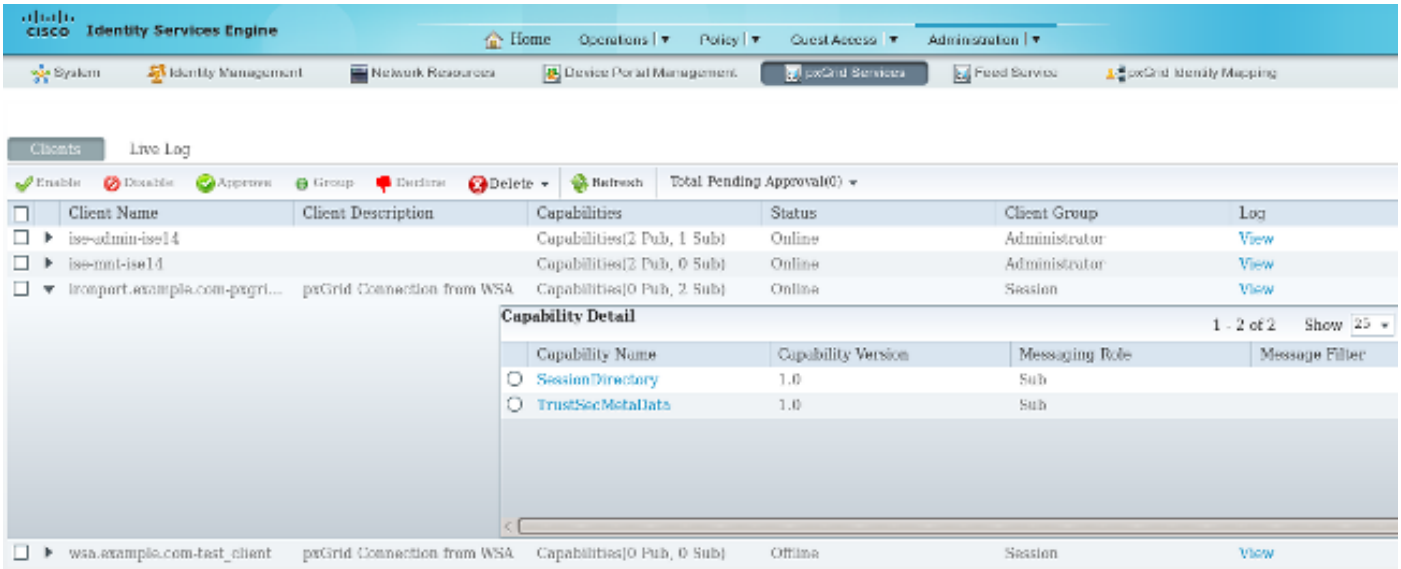
Pour une session SSL utilisée pour protéger l'échange extensible de Protocol de Messagerie et de présence (XMPP) (utilisé par le pxGrid), la panne SSL d'états de client en raison d'une chaîne de certificat inconnue a présenté par le serveur.

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 :



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