

# Configurazione dell'integrazione WSA con ISE per i servizi compatibili con TrustSec

## Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Esempio di rete e flusso del traffico](#)

[ASA-VPN](#)

[ASA-FW](#)

[ISE](#)

[Passaggio 1. SGT per IT e altri gruppi](#)

[Passaggio 2. Regola di autorizzazione per l'accesso VPN che assegna SGT = 2 \(IT\)](#)

[Passaggio 3. Aggiungere un dispositivo di rete e generare il file PAC per ASA-VPN](#)

[Passaggio 4. Abilitare il ruolo pxGrid](#)

[Passaggio 5. Generare il certificato per l'amministrazione e il ruolo pxGrid](#)

[Passaggio 6. Registrazione automatica di pxGrid](#)

[WSA](#)

[Passaggio 1. Modalità trasparente e reindirizzamento](#)

[Passaggio 2. Generazione del certificato](#)

[Passaggio 3. Test della connettività ISE](#)

[Passaggio 4. Profili di identificazione ISE](#)

[Passaggio 5. Accedere al criterio basato sul tag SGT](#)

[Verifica](#)

[Passaggio 1. Sessione VPN](#)

[Passaggio 2. Informazioni sulla sessione recuperate dal WSA](#)

[Passaggio 3. Reindirizzamento del traffico verso il WSA](#)

[Risoluzione dei problemi](#)

[Certificati non corretti](#)

[Scenario corretto](#)

[Informazioni correlate](#)

## Introduzione

In questo documento viene descritto come integrare Web Security Appliance (WSA) con Identity Services Engine (ISE). ISE versione 1.3 supporta una nuova API chiamata pxGrid. Questo protocollo moderno e flessibile supporta l'autenticazione, la crittografia e i privilegi (gruppi) che

consentono una facile integrazione con altre soluzioni di sicurezza.

WSA versione 8.7 supporta il protocollo pxGrid ed è in grado di recuperare le informazioni sull'identità del contesto da ISE. Di conseguenza, WSA consente di creare policy basate sui gruppi TrustSec Security Group Tag (SGT) recuperati da ISE.

## Prerequisiti

### Requisiti

Cisco raccomanda la conoscenza della configurazione di Cisco ISE e delle conoscenze base su questi argomenti:

- Implementazioni ISE e configurazione dell'autorizzazione
- Configurazione CLI di Adaptive Security Appliance (ASA) per l'accesso a TrustSec e VPN
- Configurazione WSA
- Informazioni di base sulle distribuzioni TrustSec

### Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Microsoft Windows 7
- Software Cisco ISE versione 1.3 e successive
- Cisco AnyConnect Mobile Security versione 3.1 e successive
- Cisco ASA versione 9.3.1 e successive
- Cisco WSA versione 8.7 e successive

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

## Configurazione

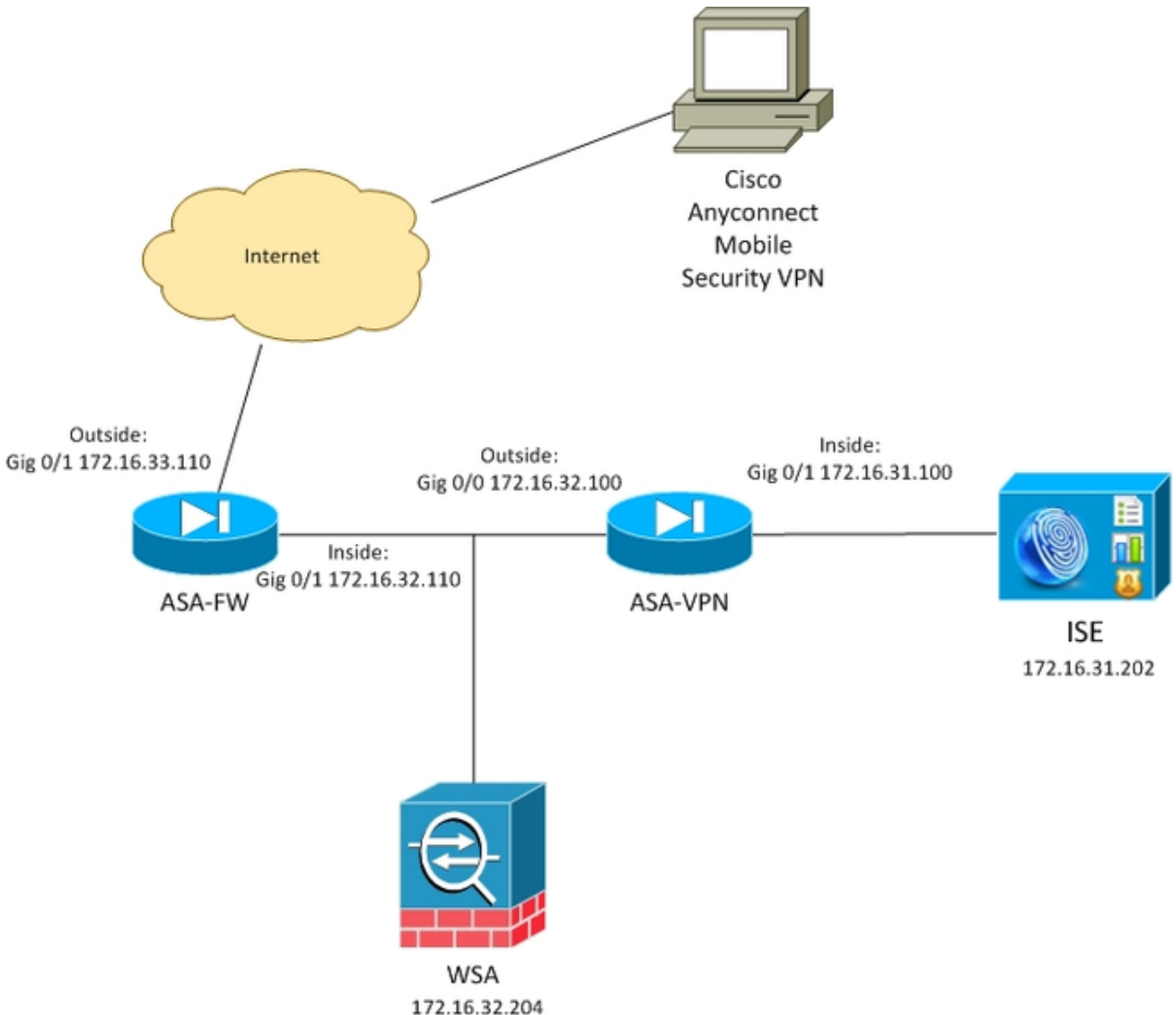
**Nota:** per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo [strumento di ricerca dei comandi \(solo utenti registrati\)](#).

### Esempio di rete e flusso del traffico

I tag SGT TrustSec vengono assegnati da ISE utilizzato come server di autenticazione per tutti i tipi di utenti che accedono alla rete aziendale. Ciò implica il coinvolgimento di utenti cablati/wireless che eseguono l'autenticazione tramite i portali guest 802.1x o ISE. Inoltre, gli utenti VPN remoti che usano ISE per l'autenticazione.

Per WSA, non importa come l'utente ha effettuato l'accesso alla rete.

Nell'esempio viene mostrato come interrompere una sessione su ASA-VPN per utenti VPN remoti. A tali utenti è stato assegnato un tag SGT specifico. Tutto il traffico HTTP diretto a Internet verrà intercettato da ASA-FW (firewall) e reindirizzato al WSA per l'ispezione. WSA utilizza il profilo di identità che consente di classificare gli utenti in base al tag SGT e di creare criteri di accesso o decrittografia basati su tale tag.



Il flusso dettagliato è:

1. L'utente VPN AnyConnect termina la sessione SSL (Secure Sockets Layer) sull'appliance ASA-VPN. L'appliance ASA-VPN è configurata per TrustSec e utilizza ISE per l'autenticazione degli utenti VPN. All'utente autenticato viene assegnato un valore di tag SGT = 2 (nome = IT). L'utente riceve un indirizzo IP dalla rete 172.16.32.0/24 (nell'esempio riportato, 172.16.32.50).
2. L'utente tenta di accedere alla pagina Web su Internet. L'ASA-FW è configurata per il protocollo WCCP (Web Cache Communication Protocol), che reindirizza il traffico al WSA.
3. Il WSA è configurato per l'integrazione con ISE. Utilizza pxGrid per scaricare informazioni dall'ISE: all'indirizzo IP dell'utente 172.16.32.50 è stato assegnato il tag SGT 2.

4. WSA elabora la richiesta HTTP dell'utente e accede a PolicyForIT dei criteri di accesso. Questa policy è configurata per bloccare il traffico verso i siti sportivi. Tutti gli altri utenti (che non appartengono a SGT 2) hanno rispettato le regole di accesso predefinite e hanno accesso completo ai siti sportivi.

## ASA-VPN

Questo è un gateway VPN configurato per TrustSec. La configurazione dettagliata non rientra nell'ambito di questo documento. Fare riferimento agli esempi seguenti:

- [Esempio di configurazione di ASA e Catalyst serie 3750X Switch TrustSec e guida alla risoluzione dei problemi](#)
- [Esempio di configurazione della classificazione e dell'applicazione ASA VPN SGT versione 9.2](#)

## ASA-FW

Il firewall ASA è responsabile del reindirizzamento WCCP al server WSA. Il dispositivo non riconosce 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 è un punto centrale dell'implementazione di TrustSec. Assegna tag SGT a tutti gli utenti che accedono e si autenticano alla rete. In questa sezione sono elencati i passaggi necessari per la configurazione di base.

### Passaggio 1. SGT per IT e altri gruppi

Scegliere **Criteri > Risultati > Accesso al gruppo di sicurezza > Gruppi di sicurezza** e creare il modulo SGT:

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes 'Home' and 'Operations'. Below it are tabs for 'Authentication', 'Authorization', 'Profiling', 'Posture', and 'Client Provisioning'. The 'Results' tab is active, showing a search bar and a tree view of the configuration hierarchy. The 'TrustSec' folder is expanded, and 'Security Groups' is selected. A table on the right lists the Security Groups:

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

### Passaggio 2. Regola di autorizzazione per l'accesso VPN che assegna SGT = 2 (IT)

Scegliere **Criteri > Autorizzazione** e creare una regola per l'accesso VPN remoto. Tutte le connessioni VPN stabilite tramite ASA-VPN avranno accesso completo (PermitAccess) e verranno assegnate al tag SGT 2 (IT).

The screenshot shows the Cisco Identity Services Engine (ISE) interface for configuring an Authorization Policy. The top navigation bar includes 'Home', 'Operations', 'Policy', 'Guest Access', and 'Administration'. The 'Policy' tab is active, and the 'Authorization Policy' configuration page is displayed. The page includes a search bar, a dropdown menu for 'First Matched Rule Applies', and a table of rules. The 'ASA-VPN' rule is highlighted, showing its status, name, conditions, and permissions.

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

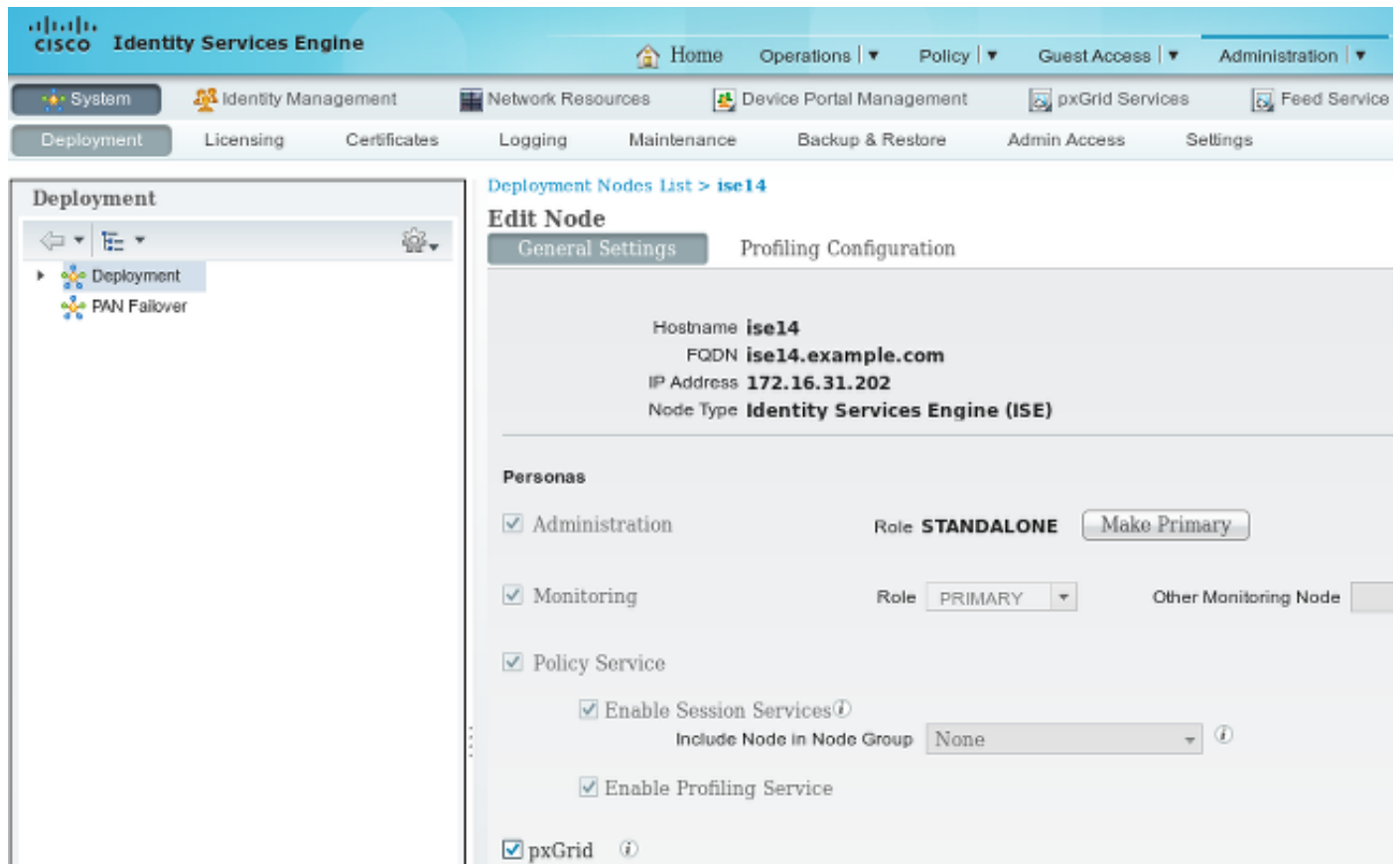
### Passaggio 3. Aggiungere un dispositivo di rete e generare il file PAC per ASA-VPN

Per aggiungere l'appliance ASA-VPN al dominio TrustSec, è necessario generare manualmente il file PAC (proxy Auto Config). Il file verrà importato sull'appliance ASA.

Configurabile da **Amministrazione > Dispositivi di rete**. Dopo aver aggiunto l'ASA, scorrere verso il basso fino alle impostazioni TrustSec e generare il file PAC. I dettagli relativi a tali elementi sono descritti in un documento separato (di riferimento).

#### Passaggio 4. Abilitare il ruolo pxGrid

Per abilitare il ruolo pxGrid, scegliere **Amministrazione > Distribuzione**.



The screenshot displays the Cisco Identity Services Engine (ISE) Administration interface. The top navigation bar includes 'Home', 'Operations', 'Policy', 'Guest Access', and 'Administration'. Below this, a secondary navigation bar lists various services: System, Identity Management, Network Resources, Device Portal Management, pxGrid Services, and Feed Service. The main content area is titled 'Deployment Nodes List > ise14' and shows the 'Edit Node' configuration for 'ise14'. The 'General Settings' tab is active, displaying the following information:

- Hostname: **ise14**
- FQDN: **ise14.example.com**
- IP Address: **172.16.31.202**
- Node Type: **Identity Services Engine (ISE)**

Under the 'Personas' section, the following roles are configured:

- Administration: Role **STANDALONE**, with a 'Make Primary' button.
- Monitoring: Role **PRIMARY**, with an 'Other Monitoring Node' field.
- Policy Service:
  - Enable Session Services ⓘ
  - Include Node in Node Group: **None** ⓘ
  - Enable Profiling Service
- pxGrid ⓘ

#### Passaggio 5. Generare il certificato per l'amministrazione e il ruolo pxGrid

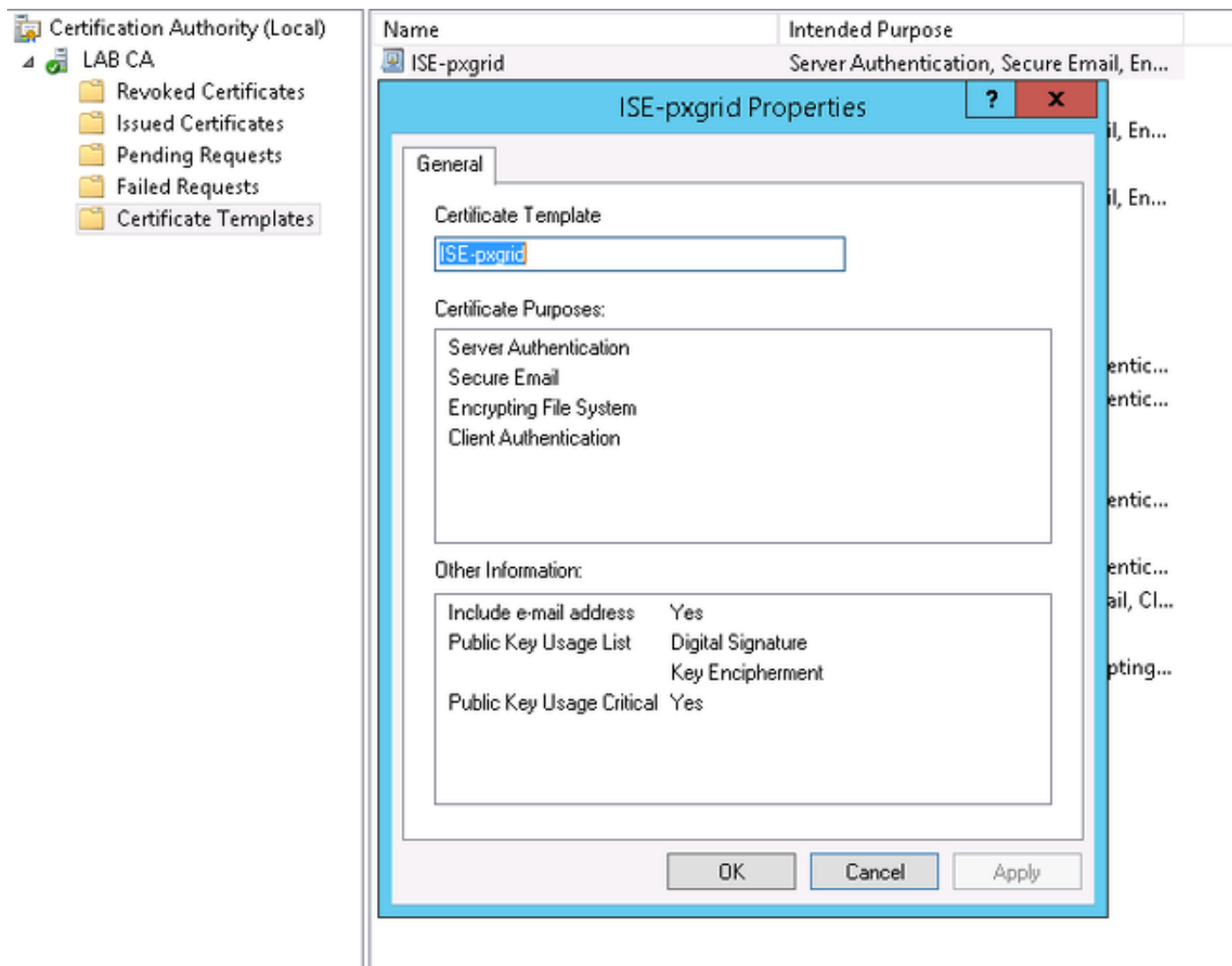
Il protocollo pxGrid utilizza l'autenticazione del certificato sia per il client che per il server. È molto importante configurare i certificati corretti sia per ISE che per WSA. Entrambi i certificati devono includere il nome di dominio completo (FQDN) nell'oggetto e le estensioni x509 per l'autenticazione client e l'autenticazione server. Inoltre, verificare che sia stato creato il record A DNS corretto sia per ISE che per WSA e che corrisponda all'FQDN corrispondente.

Se entrambi i certificati sono firmati da un'Autorità di certificazione (CA) diversa, è importante includere tali CA nell'archivio attendibile.

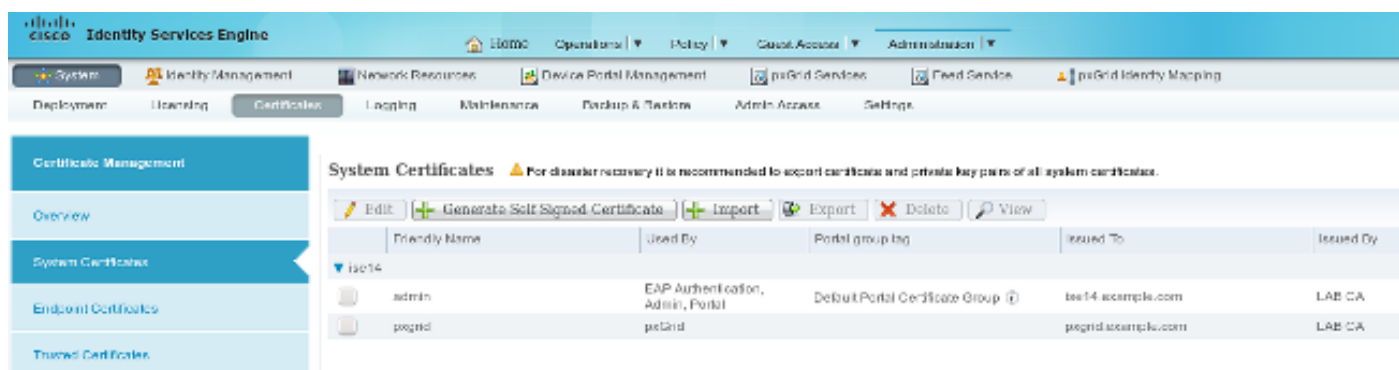
Per configurare i certificati, scegliere **Amministrazione > Certificati**.

ISE può generare una richiesta di firma del certificato (CSR) per ogni ruolo. Per il ruolo pxGrid, esportare e firmare il CSR con una CA esterna.

Nell'esempio riportato di seguito, la CA Microsoft è stata utilizzata con questo modello:



Il risultato finale potrebbe essere simile al seguente:



Non dimenticare di creare record A DNS per ise14.example.com e pxgrid.example.com che puntano a 172.16.31.202.

## Passaggio 6. Registrazione automatica di pxGrid

Per impostazione predefinita, ISE non registrerà automaticamente gli abbonati a pxGrid. che deve essere approvato manualmente dall'amministratore. Questa impostazione deve essere modificata per l'integrazione WSA.



Scegliere **Amministrazione > pxGrid Services** e impostare **Abilita registrazione automatica**.

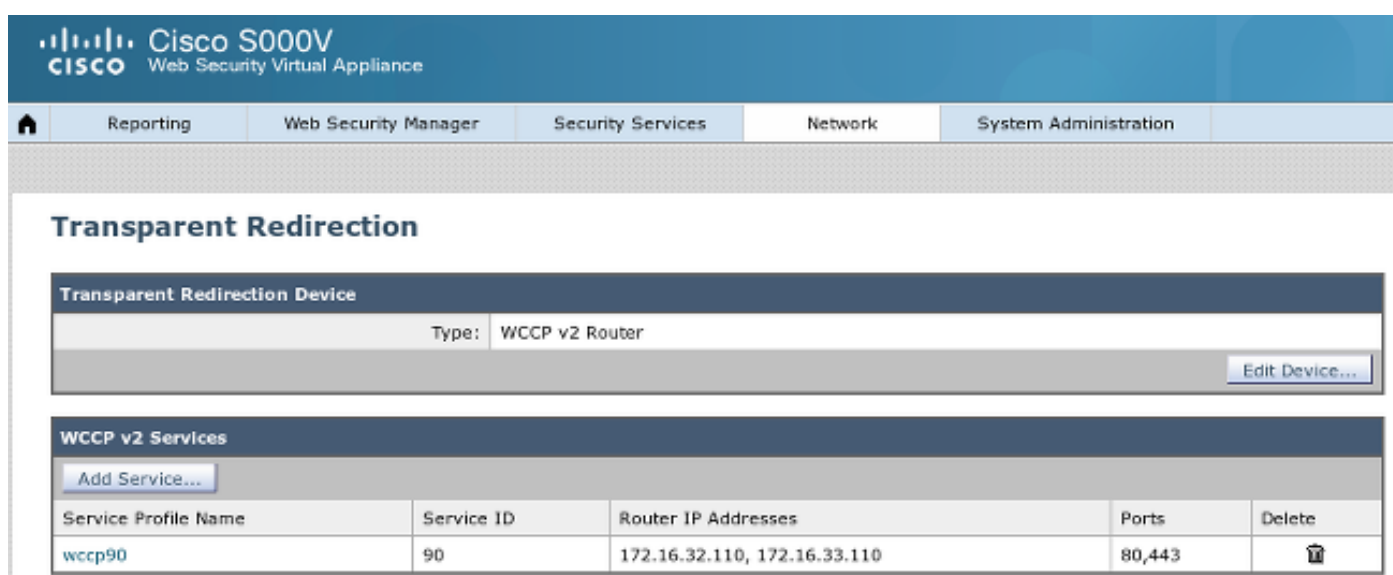
[View By Capabilities](#)

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

## WSA

### Passaggio 1. Modalità trasparente e reindirizzamento

Nell'esempio, il server WSA è configurato solo con l'interfaccia di gestione, la modalità trasparente e il reindirizzamento dall'appliance ASA:



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	

### Passaggio 2. Generazione del certificato

Il server WSA deve considerare attendibile la CA per firmare tutti i certificati. Per aggiungere un certificato CA, scegliere **Rete > Gestione certificati**:



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

È inoltre necessario generare un certificato che verrà utilizzato da WSA per l'autenticazione a pxGrid. Scegliere **Rete > Identity Services Engine > WSA Client certificate** per generare il CSR, firmarlo con il modello CA corretto (ISE-pxgrid) e reimportarlo.

Inoltre, per "ISE Admin Certificate" e "ISE pxGrid Certificate", importare il certificato CA (per considerare attendibile il certificato pxGrid presentato da ISE):

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...

### Passaggio 3. Test della connettività ISE

Per verificare la connessione ad ISE, scegliere **Network > Identity Services Engine**:

## 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.

## Passaggio 4. Profili di identificazione ISE

Per aggiungere un nuovo profilo per ISE, scegliere **Web Security Manager > Profili di identificazione**. Per "*Identification and Authentication*" (Identificazione e autenticazione), usare "*Transparency identifier with ISE*" (Identificazione e autenticazione degli utenti con 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 section for "Client / User Identification Profiles".

At the top of the section is a button "Add Identification Profile...". Below it is a table with the following columns: Order, Transaction Criteria, Authentication / Identification Decision, End-User Acknowledgement, and Delete.

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	

At the bottom of the table is a button "Edit Order...".

## Passaggio 5. Accedere al criterio basato sul tag SGT

Per aggiungere un nuovo criterio, scegliere **Web Security Manager > Criteri di accesso**. L'appartenenza al gruppo usa il profilo 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 Users: No users entered</p> <p><input type="radio"/> Guests (users failing authentication)</p>	

Per i gruppi e gli utenti selezionati verrà aggiunto il tag SGT 2 (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"/>

La policy nega l'accesso a tutti i siti sportivi agli utenti che appartengono al SGT IT:

## Access 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...](#)

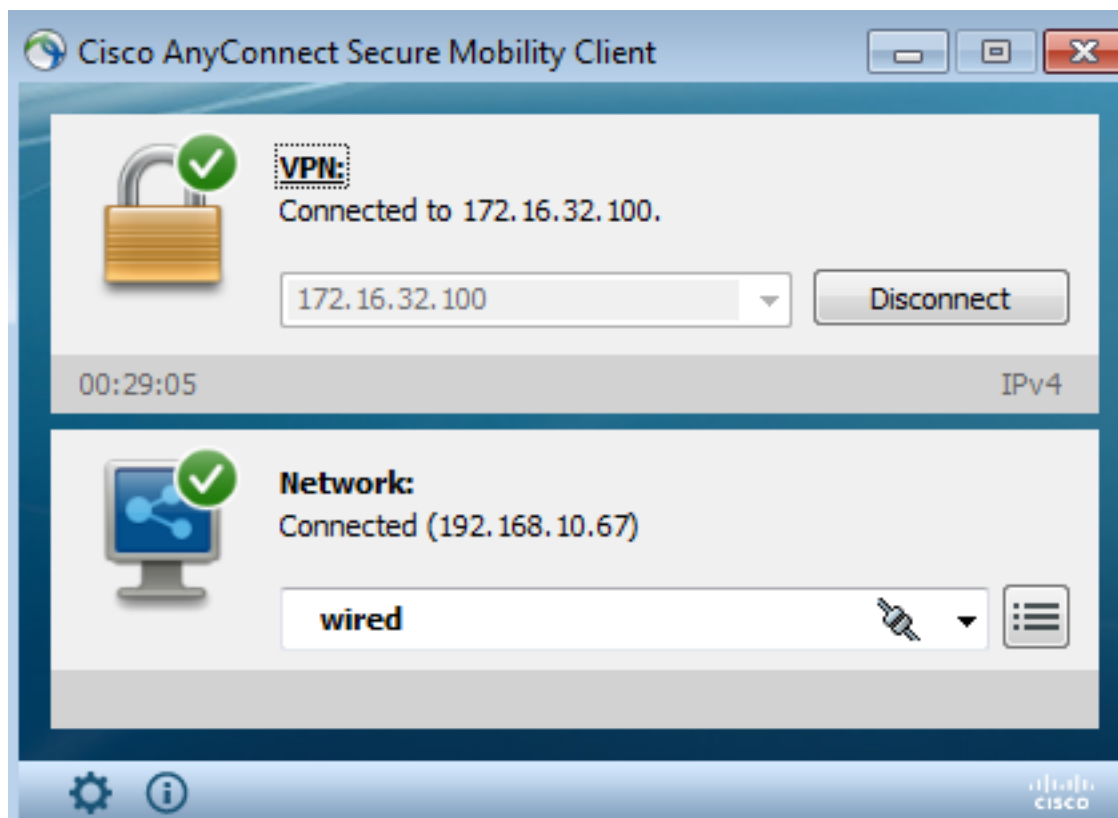
[Edit Policy Order...](#)

## Verifica

Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente.

## Passaggio 1. Sessione VPN

L'utente VPN avvia una sessione VPN verso l'appliance ASA-VPN:



L'ASA-VPN usa l'ISE per l'autenticazione. ISE crea una sessione e assegna il tag SGT 2 (IT):

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

Dopo un'autenticazione riuscita, ASA-VPN crea una sessione VPN con il tag SGT 2 (restituito 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**

Poiché il collegamento tra ASA-VPN e ASA-FW non è abilitato per TrustSec, ASA-VPN invia frame senza tag per il traffico (non sarà possibile incapsulare i frame Ethernet del GRE con il campo CMD/TrustSec inserito).

## Passaggio 2. Informazioni sulla sessione recuperate dal WSA

In questa fase, il WSA deve ricevere il mapping tra l'indirizzo IP, il nome utente e il SGT (tramite protocollo 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
[ ]> █
```

## Passaggio 3. Reindirizzamento del traffico verso il WSA

L'utente VPN avvia una connessione a sport.pl, che viene intercettata da 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
```

e tunneling in GRE su WSA (notare che l'ID router WCCP è l'indirizzo IP configurato più alto):

```
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 continua l'handshake TCP ed elabora la richiesta GET. Di conseguenza, il criterio denominato PolicyForIT viene raggiunto e il traffico viene bloccato:



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

Ciò è confermato dalla relazione del 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.

Il nome utente viene visualizzato in ISE.

## Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

### Certificati non corretti

Se il WSA non è inizializzato correttamente (certificati), verificare la presenza di errori di connessione 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.**

Il file ISE pxgrid-cm.log riporta:

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

La ragione del fallimento può essere vista con 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)

Per una sessione SSL utilizzata per proteggere lo scambio XMPP (Extensible Messaging and Presence Protocol) (utilizzato da pxGrid), il client segnala un errore SSL a causa di una catena di certificati sconosciuta presentata dal server.

## Scenario corretto

Per uno scenario corretto, il file pxgrid-controller.log di ISE visualizza:

```
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
```

Inoltre, la GUI di ISE presenta il WSA come un abbonato con le funzionalità corrette:

The screenshot shows the Cisco Identity Services Engine (ISE) GUI. The top navigation bar includes 'Home', 'Operations', 'Policy', 'Guest Access', and 'Administration'. The main content area is titled 'Live Log' and displays a table of clients. The table has columns for 'Client Name', 'Client Description', 'Capabilities', 'Status', 'Client Group', and 'Log'. A client named 'Ironport.example.com-pxgr...' is selected, and its 'Capability Detail' is expanded, showing two capabilities: 'SessionDirectory' and 'TrustSecMetaData', both with a version of 1.0 and a 'Sub' messaging role.

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-pxgr...	pxGrid Connection from WSA	Capabilities(0 Pub, 2 Sub)	Online	Session	<a href="#">View</a>

**Capability Detail** (1 - 2 of 2)

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

## Informazioni correlate

- [Esempio di postura di VPN con ISE versione 9.2.1 di ASA](#)
- [Guida per l'utente di WSA 8.7](#)
- [Esempio di configurazione di ASA e Catalyst serie 3750X Switch TrustSec e guida alla risoluzione dei problemi](#)
- [Guida alla configurazione dello switch Cisco TrustSec: Informazioni su Cisco TrustSec](#)
- [Configurazione di un server esterno per l'autorizzazione utente di Security Appliance](#)
- [Guida alla configurazione di Cisco ASA VPN CLI, 9.1](#)
- [Guida dell'utente di Cisco Identity Services Engine, versione 1.2](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)