

# 為TrustSec感知服務配置WSA與ISE整合

## 目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[設定](#)

[網路圖表和流量傳輸](#)

[ASA-VPN](#)

[ASA-FW](#)

[ISE](#)

[步驟1.面向IT和其他團隊的SGT](#)

[步驟2.分配SGT = 2\(IT\)的VPN訪問的授權規則](#)

[步驟3.新增網路裝置並生成ASA-VPN的PAC檔案](#)

[步驟4.啟用pxGrid角色](#)

[步驟5.生成管理證書和pxGrid角色](#)

[步驟6. pxGrid自動註冊](#)

[WSA](#)

[步驟1.透明模式和重新導向](#)

[步驟2.憑證產生](#)

[步驟3.測試ISE連線](#)

[步驟4. ISE標識配置檔案](#)

[步驟5.根據SGT標籤訪問策略](#)

[驗證](#)

[步驟1. VPN會話](#)

[步驟2. WSA檢索到的會話資訊](#)

[步驟3.流量重新導向至WSA](#)

[疑難排解](#)

[不正確的證書](#)

[正確案例](#)

[相關資訊](#)

## 簡介

本文檔介紹如何將網路安全裝置(WSA)與身份服務引擎(ISE)整合。ISE版本1.3支援稱為pxGrid的新API。這種現代而靈活的協定支援身份驗證、加密和許可權(組)，從而能夠方便地與其他安全解決方案整合。

WSA版本8.7支援pxGrid協定，並且能夠從ISE檢索上下文身份資訊。因此，WSA允許您根據從

ISE檢索的TrustSec安全組標籤(SGT)組構建策略。

## 必要條件

### 需求

思科建議您瞭解思科ISE配置和以下主題的基本知識：

- ISE部署和授權配置
- 適用於TrustSec和VPN訪問的自適應安全裝置(ASA)CLI配置
- WSA配置
- 對TrustSec部署的基本瞭解

### 採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Microsoft Windows 7
- Cisco ISE軟體版本1.3及更高版本
- Cisco AnyConnect移動安全版本3.1及更高版本
- Cisco ASA版本9.3.1及更高版本
- Cisco WSA版本8.7及更高版本

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

## 設定

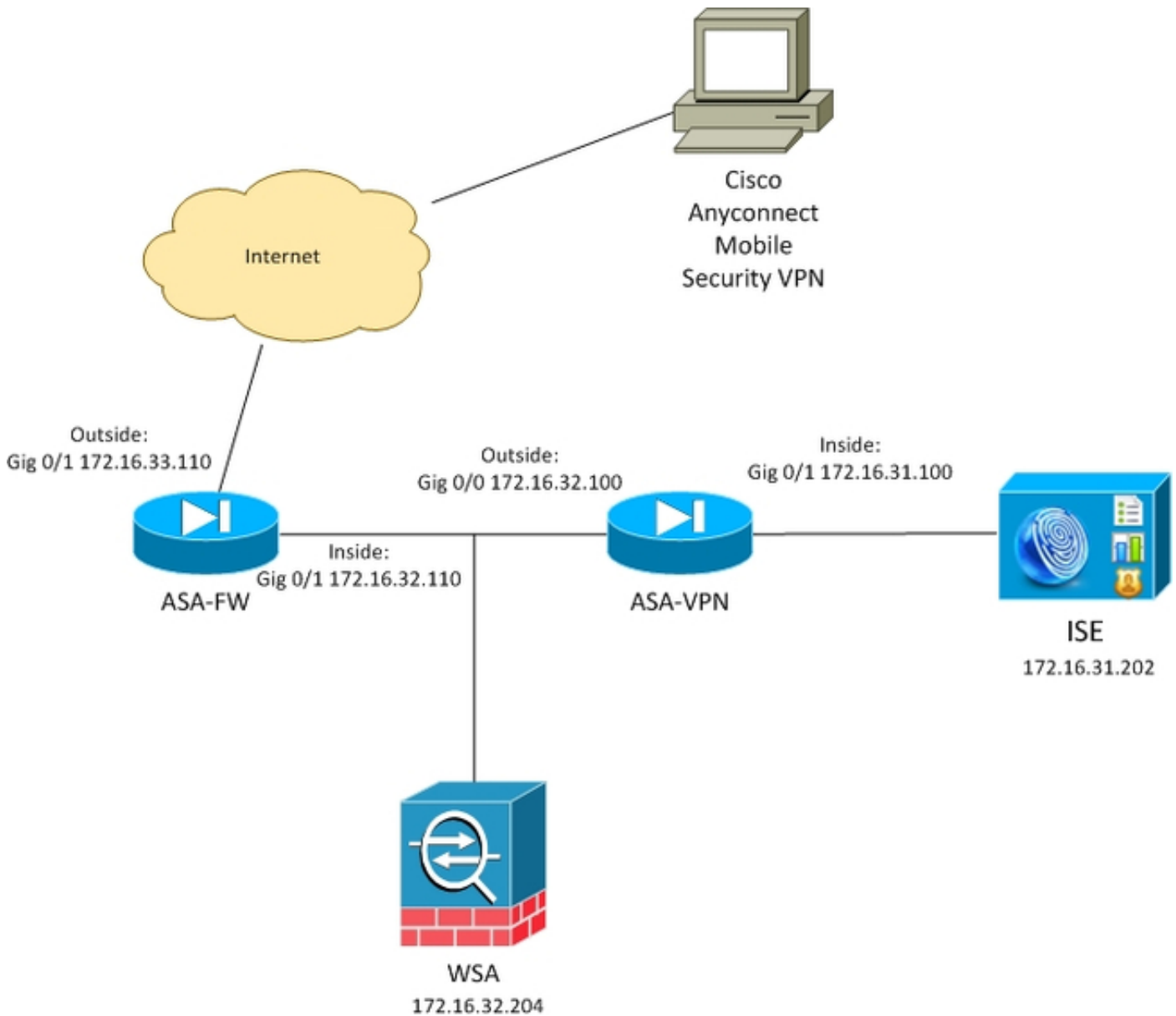
**附註：** 使用 [命令查詢工具](#) (僅供 [已註冊](#) 客戶使用) 可獲取本節中使用的命令的更多資訊。

### 網路圖表和流量傳輸

TrustSec SGT標籤由ISE分配，用作訪問企業網路的所有型別使用者的身份驗證伺服器。這涉及通過802.1x或ISE訪客門戶進行身份驗證的有線/無線使用者。此外，使用ISE進行身份驗證的遠端VPN使用者。

對於WSA，使用者如何訪問網路並不重要。

此示例展示在ASA-VPN上終止會話的遠端VPN使用者。這些使用者已分配特定的SGT標籤。所有到Internet的HTTP流量都將被ASA-FW（防火牆）攔截，並重定向到WSA進行檢查。WSA使用身份配置檔案，它允許根據SGT標籤對使用者進行分類，並據此構建訪問或解密策略。



詳細流程為：

1. AnyConnect VPN使用者終止ASA-VPN上的安全套接字層(SSL)會話。ASA-VPN配置為TrustSec並使用ISE對VPN使用者進行身份驗證。驗證後的使用者會指派一個SGT標籤值= 2(name = IT)。使用者從172.16.32.0/24網路 (本例中為172.16.32.50) 接收IP地址。
2. 使用者嘗試訪問Internet中的網頁。ASA-FW配置為網路快取通訊協定(WCCP)，該協定將流量重定向到WSA。
3. 為ISE整合配置WSA。它使用pxGrid從ISE下載資訊：已分配使用者IP地址172.16.32.50 SGT標籤2。
4. WSA處理來自使用者的HTTP請求並點選訪問策略PolicyForIT。該策略配置為阻止到體育網站的流量。所有其它使用者 (不屬於SGT 2) 都達到了預設訪問策略，並且擁有對體育網站的完全訪問許可權。

## ASA-VPN

這是為TrustSec配置的VPN網關。詳細設定超出本檔案的範圍。請參閱以下範例：

- [ASA和Catalyst 3750X系列交換機TrustSec配置示例和故障排除指南](#)
- [ASA 9.2版VPN SGT分類和實施配置示例](#)

## ASA-FW

ASA防火牆負責將WCCP重定向到WSA。此裝置不知道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是TrustSec部署的中心點。它將SGT標籤分配給所有訪問和驗證網路的使用者。本節列出了基本配置所需的步驟。

### 步驟1.面向IT和其他團隊的SGT

選擇Policy > Results > Security Group Access > Security Groups並建立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

## 步驟2.分配SGT = 2(IT)的VPN訪問的授權規則

選擇 **Policy > Authorization**，然後建立遠端VPN訪問的規則。通過ASA-VPN建立的所有VPN連線都將獲得完全訪問許可權(PermitAccess)，並將分配有SGT標籤2(IT)。

**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

## 步驟3.新增網路裝置並生成ASA-VPN的PAC檔案

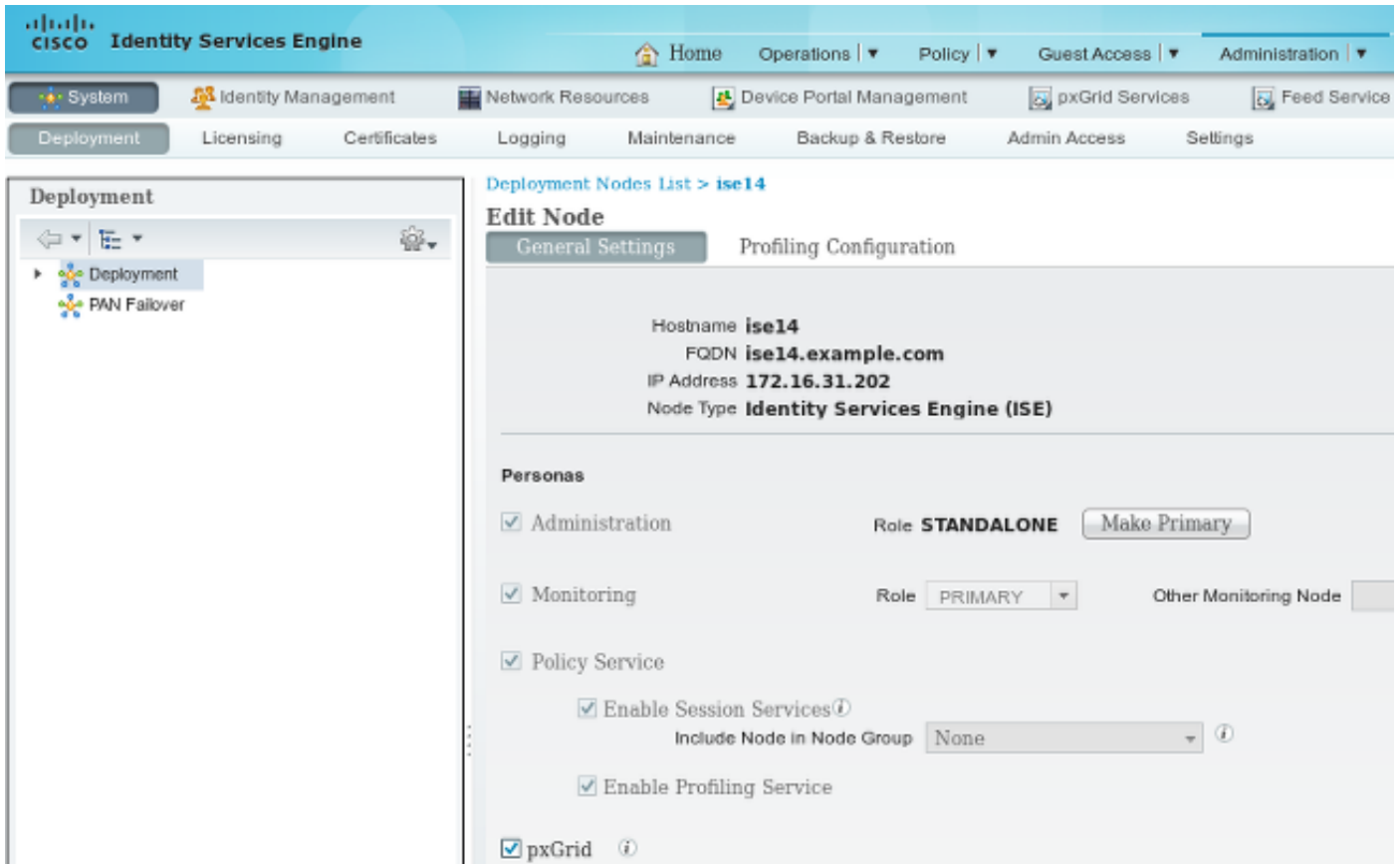
要將ASA-VPN新增到TrustSec域，必須手動生成代理自動配置(PAC)檔案。該檔案將在ASA上匯入

。

可從Administration > Network Devices配置。新增ASA後，向下滾動到TrustSec設定並生成PAC檔案。相關詳細資訊將在單獨的 ( 引用的 ) 文檔中說明。

#### 步驟4.啟用pxGrid角色

選擇Administration > Deployment以啟用pxGrid角色。



#### 步驟5.生成管理證書和pxGrid角色

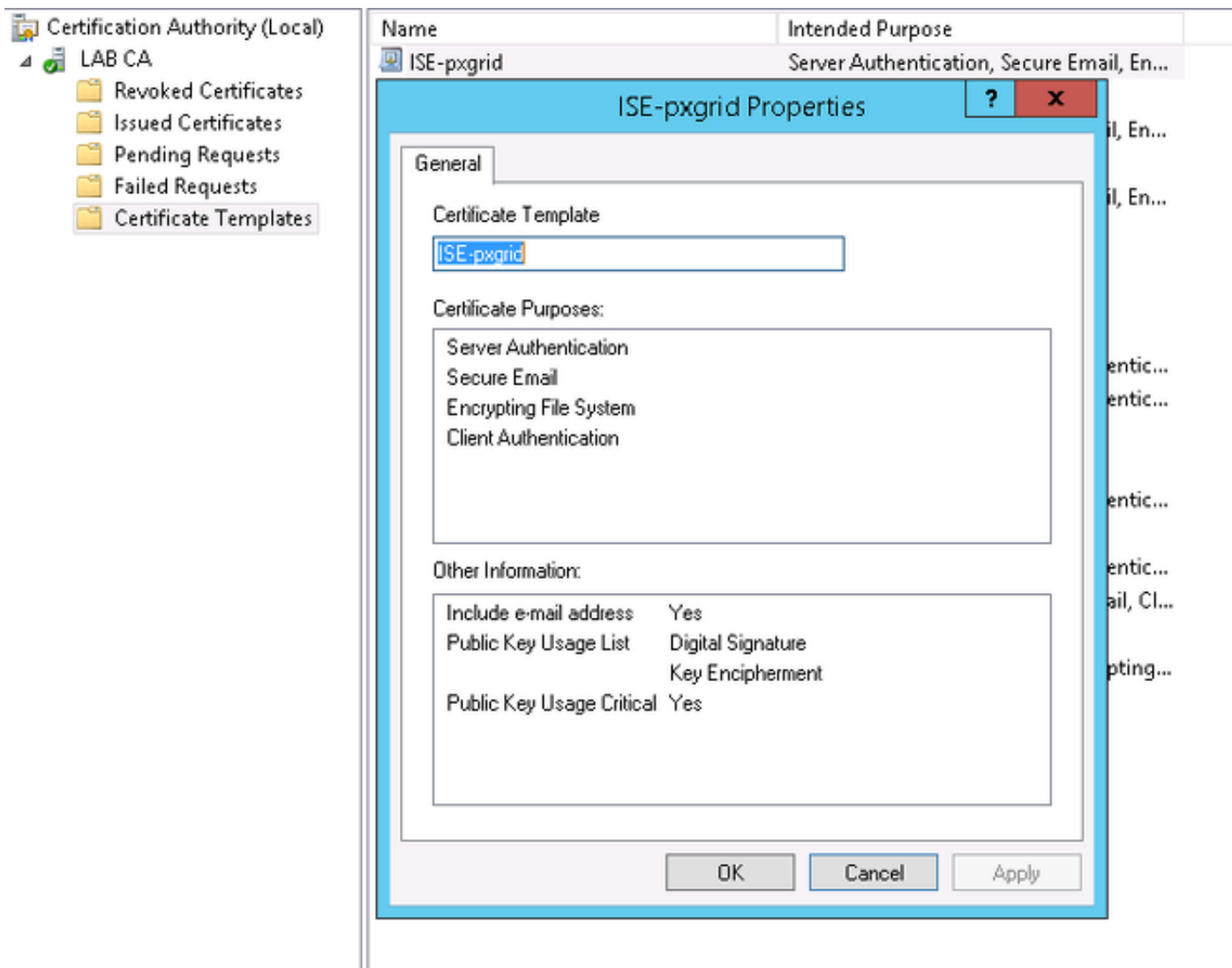
pxGrid協定對客戶端和伺服器都使用證書身份驗證。為ISE和WSA配置正確的證書非常重要。兩個證書都應在主題中包含完全限定域名(FQDN)，並為客戶端身份驗證和伺服器身份驗證包含x509擴展。此外，請確保為ISE和WSA建立了正確的DNS A記錄，並與相應的FQDN匹配。

如果兩個證書都是由不同的證書頒發機構(CA)簽名的，則必須在受信任的儲存中包括這些CA。

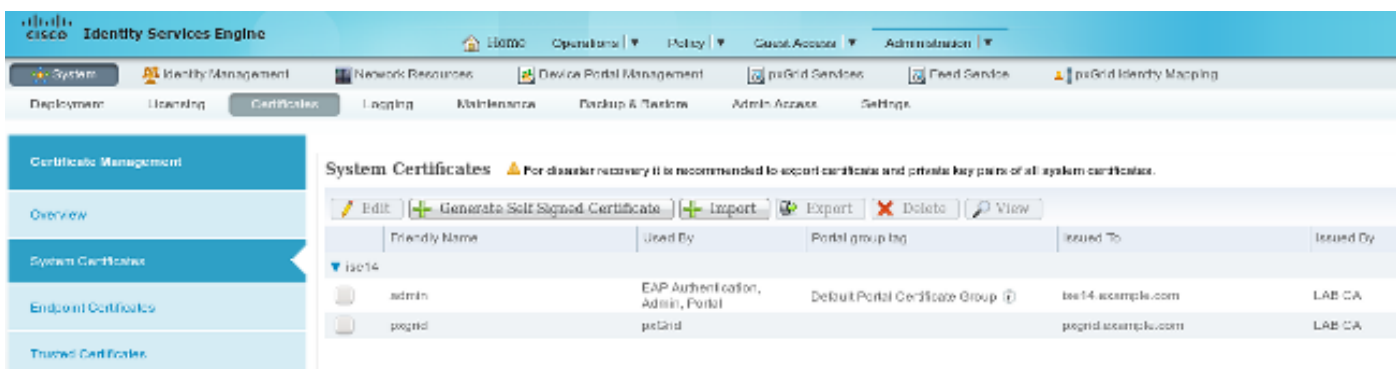
若要設定憑證，請選擇管理>憑證。

ISE可以為每個角色生成證書簽名請求(CSR)。對於pxGrid角色，請匯出外部CA並簽署CSR。

在此範例中，Microsoft CA已用於此範本：



最終結果可能如下所示：



不要忘記為ise14.example.com和pxgrid.example.com建立指向172.16.31.202的DNS A記錄。

## 步驟6. pxGrid自動註冊

預設情況下，ISE不會自動註冊pxGrid使用者。應該由管理員手動批准。應針對WSA整合更改該設定。

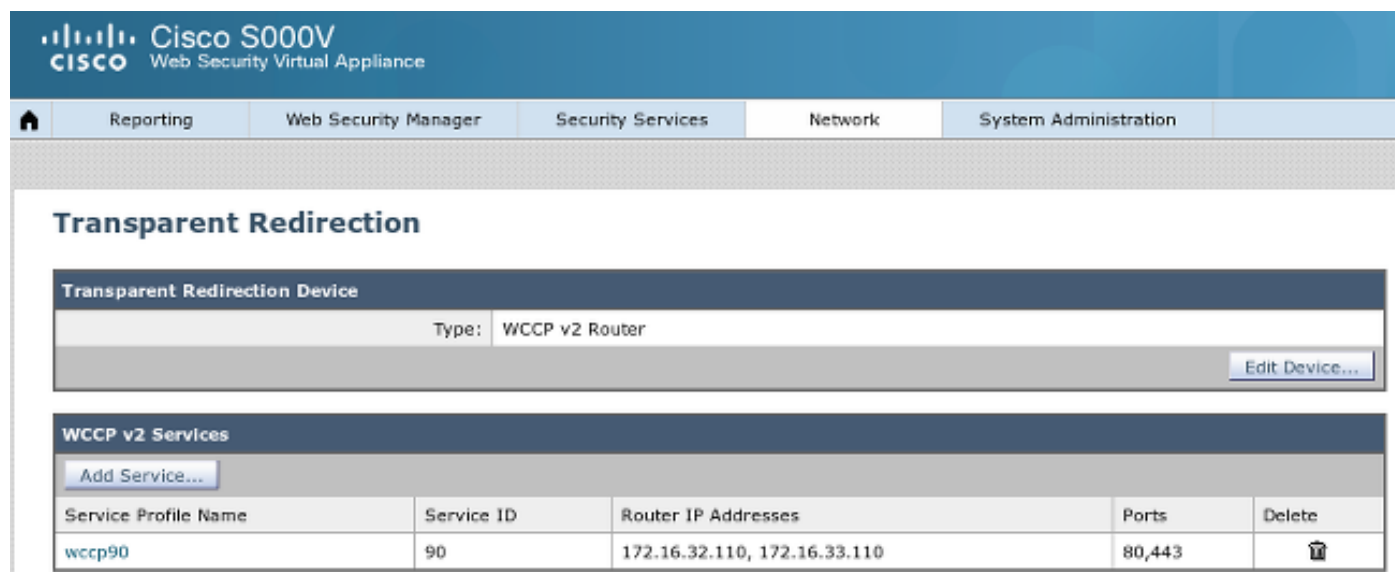
選擇Administration > pxGrid Services，然後設定Enable Auto-Registration。



## WSA

### 步驟1.透明模式和重新導向

在本示例中，僅使用管理介面、透明模式和從ASA重定向來配置WSA:




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 "Transparent Redirection".

**Transparent Redirection Device**

Type: WCCP v2 Router Edit Device...

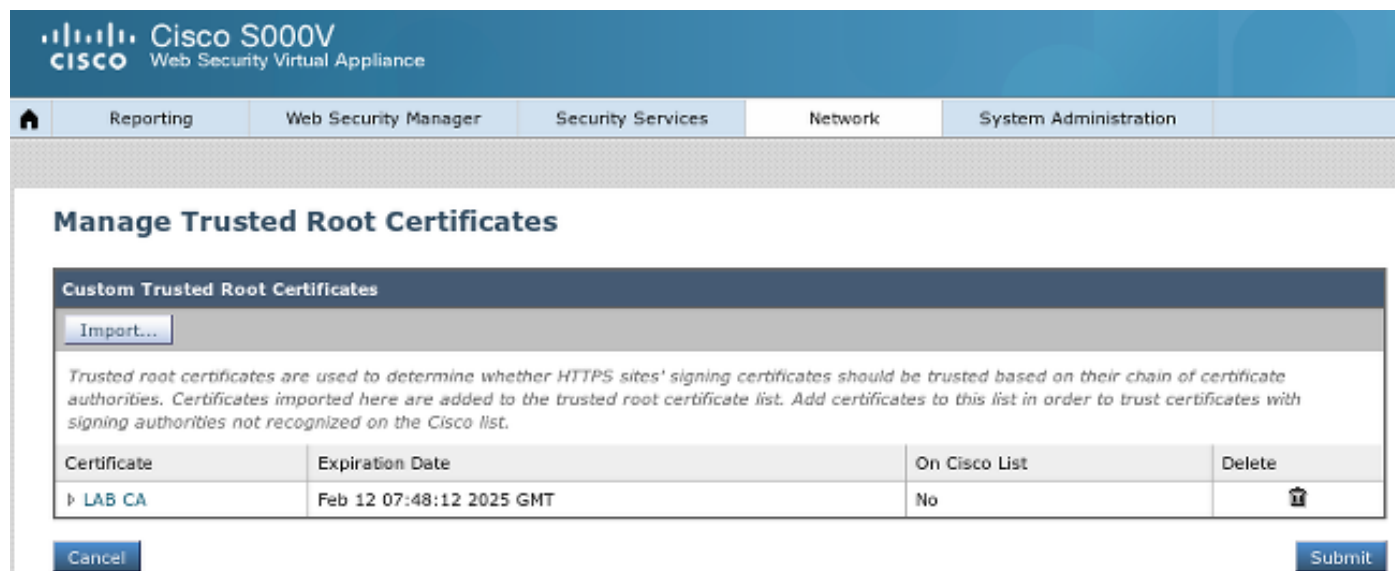
**WCCP v2 Services**

Add Service...

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

### 步驟2.憑證產生

WSA需要信任CA來簽署所有證書。選擇Network > Certificate Management以新增CA證書：




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 "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.*

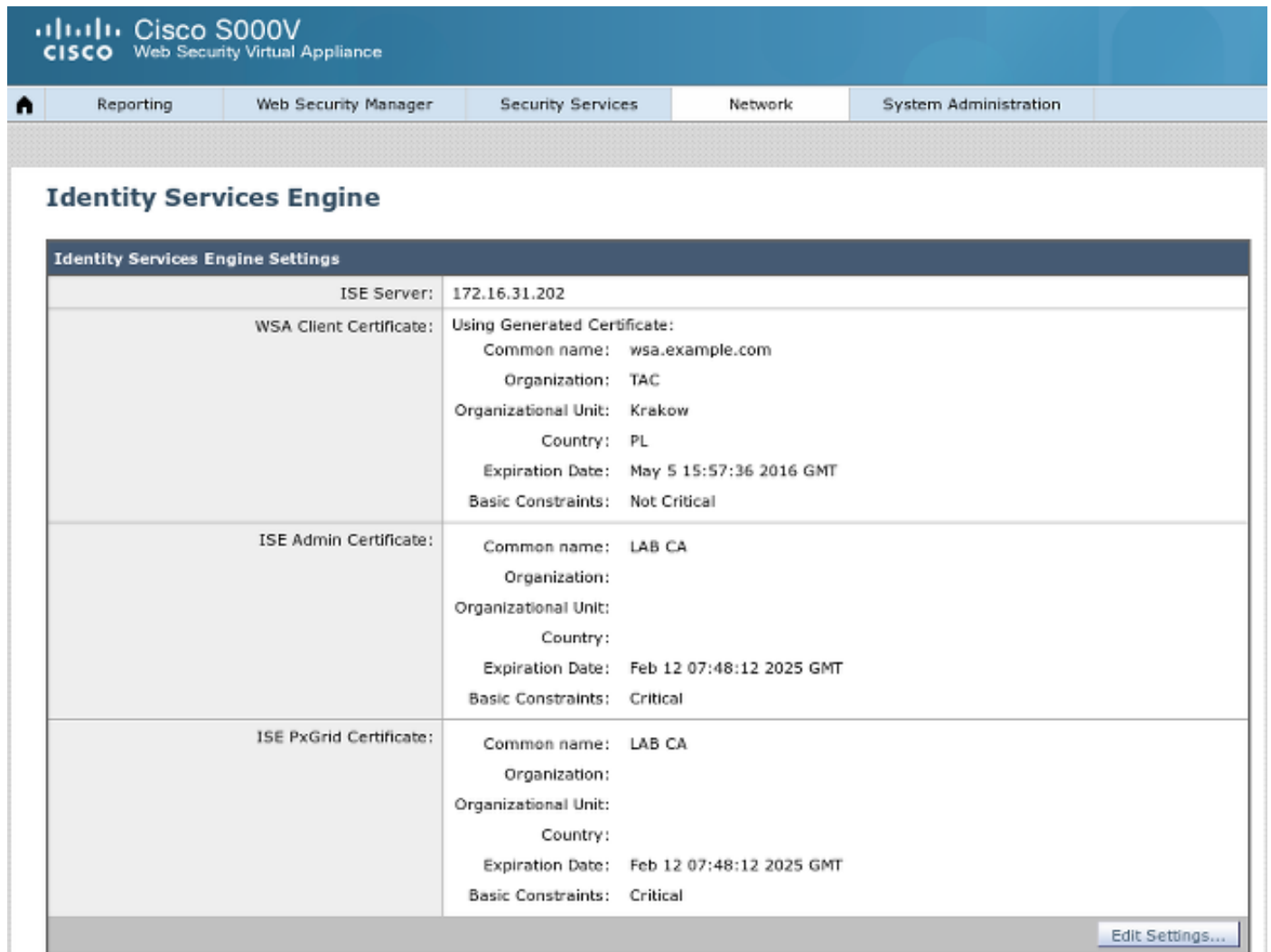
Certificate	Expiration Date	On Cisco List	Delete
LAB CA	Feb 12 07:48:12 2025 GMT	No	

Cancel Submit



還必須生成WSA將用於向pxGrid進行身份驗證的證書。選擇**Network > Identity Services Engine > WSA Client certificate**以生成CSR，使用正確的CA模板(ISE-pxgrid)對其進行簽名，然後將其匯入。

此外，對於「ISE管理員證書」和「ISE pxGrid證書」，請匯入CA證書（以便信任ISE提供的pxGrid證書）：



The screenshot displays 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 'Identity Services Engine' and contains a table of settings.

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

An 'Edit Settings...' button is located at the bottom right of the settings table.

### 步驟3.測試ISE連線

選擇**Network > Identity Services Engine**以測試與ISE的連線：



The screenshot shows the 'Test Communication with ISE Server' interface. It features a 'Start Test' button and a text area displaying the results of the test.

Start Test

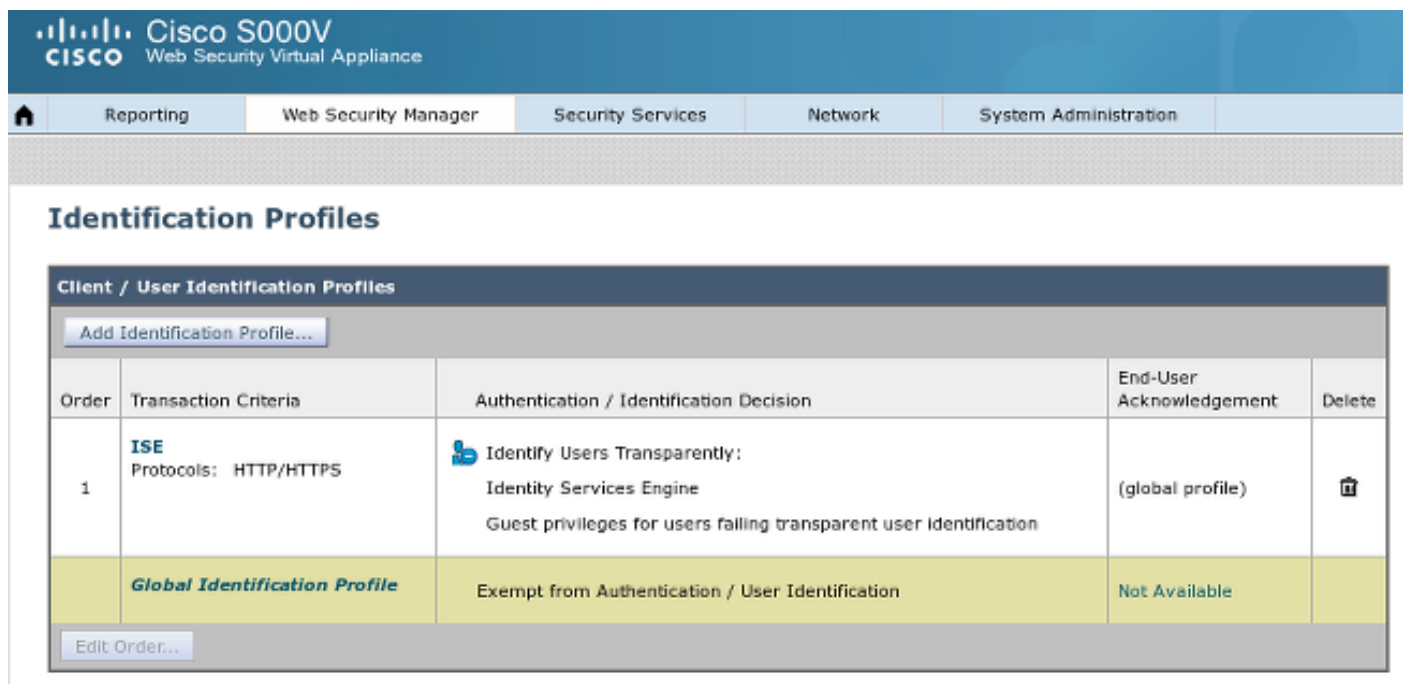
Checking connection to ISE PxGrid server...  
Success: Connection to ISE PxGrid server was successful. Retrieved 4 SGTs

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



Test completed successfully.

#### 步驟4. ISE標識配置檔案

選擇Web Security Manager > Identification profiles以便為ISE新增新配置檔案。對於「Identification and Authentication」，請使用「Transparently identify users with 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. The ISE profile is highlighted in yellow.

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	

#### 步驟5.根據SGT標籤訪問策略

選擇Web Security Manager > Access Policies以新增新策略。成員身份使用ISE配置檔案：

## 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

- All Authenticated Users
- Selected Groups and Users ?
  - ISE Secure Group Tags:
    - IT
  - Users: No users entered
- Guests (users failing authentication)



對於選定的組和使用者的，將新增SGT標籤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"/>

該策略拒絕屬於SGT IT的使用者訪問所有體育網站：

## 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...](#)

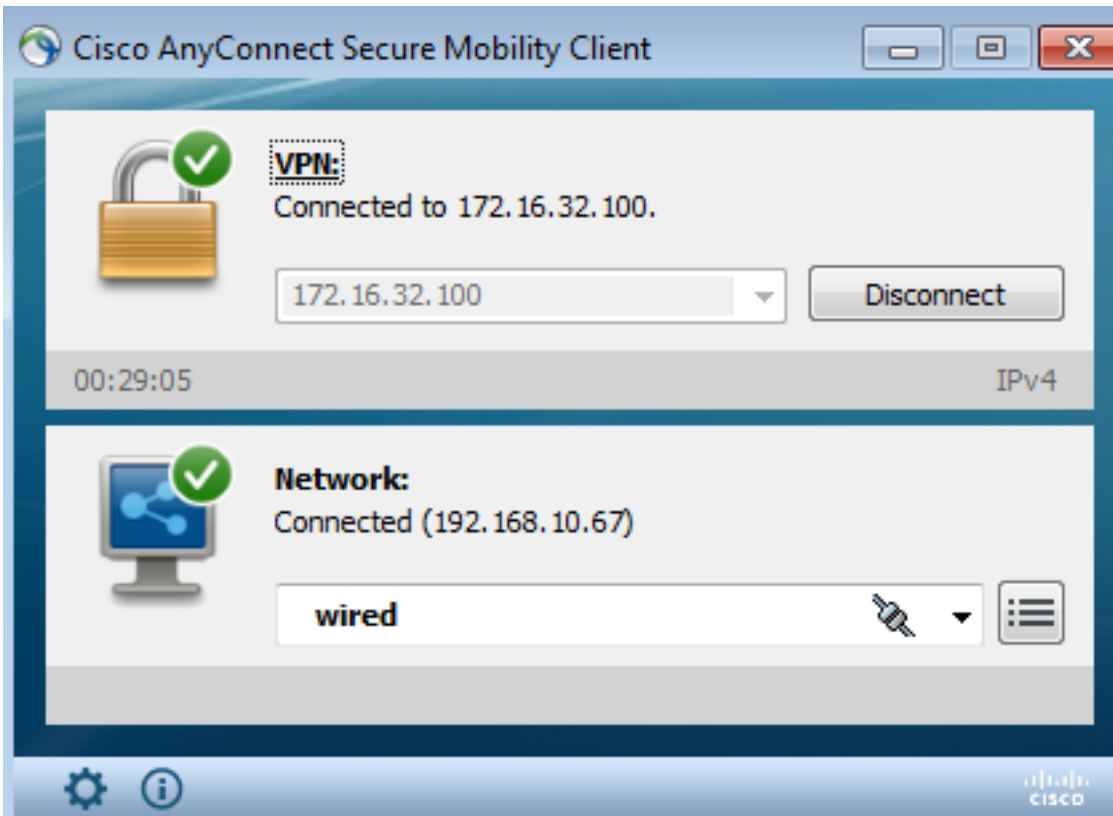
[Edit Policy Order...](#)

## 驗證

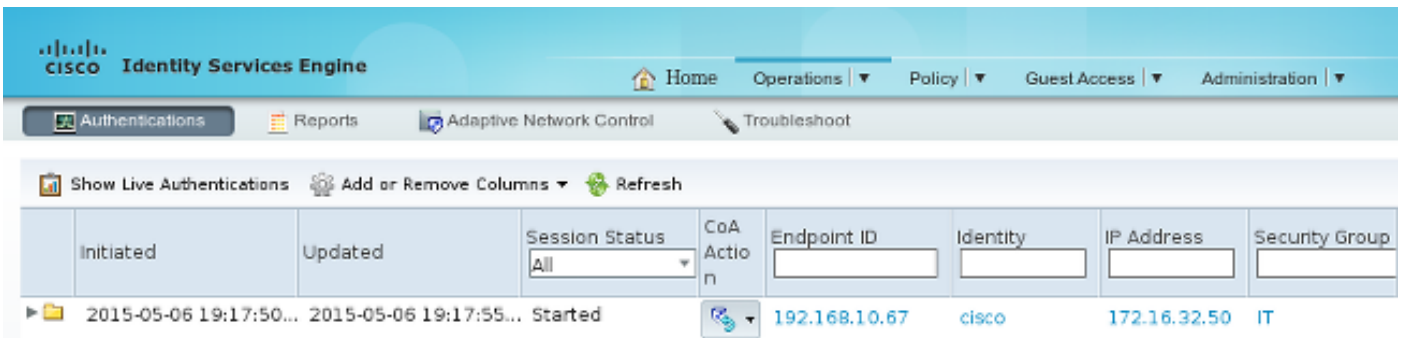
使用本節內容，確認您的組態是否正常運作。

## 步驟1. VPN會話

VPN使用者向ASA-VPN發起VPN會話：



ASA-VPN使用ISE進行身份驗證。ISE建立會話並分配SGT標籤2(IT):

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes "Home", "Operations", "Policy", "Guest Access", and "Administration". Below that, there are tabs for "Authentications", "Reports", "Adaptive Network Control", and "Troubleshoot". The main content area shows "Show Live Authentications" with a table of active sessions. The table has columns for "Initiated", "Updated", "Session Status", "CoA Action", "Endpoint ID", "Identity", "IP Address", and "Security Group". One session is listed with the following details: Initiated: 2015-05-06 19:17:50..., Updated: 2015-05-06 19:17:55..., Session Status: Started, CoA Action: (empty), Endpoint ID: 192.168.10.67, Identity: cisco, IP Address: 172.16.32.50, Security Group: IT.

身份驗證成功後，ASA-VPN會建立具有SGT標籤2的VPN會話（在cisco-av對中返回Radius Access-Accept）：

```
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
```

由於ASA-VPN與ASA-FW之間的鏈路未啟用TrustSec，因此ASA-VPN會為該流量傳送未標籤的幀（如果注入CMD/TrustSec欄位，則無法通過GRE封裝乙太網幀）。

## 步驟2. WSA檢索到的會話資訊

在此階段，WSA應接收IP地址、使用者名稱和SGT之間的對映（通過pxGrid協定）：

```
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
[ ]> █
```

## 步驟3.流量重新導向至WSA

VPN使用者發起到sport.pl的連線，該連線被ASA-FW攔截：

```
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
```

並通過GRE隧道連線到WSA ( 注意WCCP router-id是配置的最高IP地址 ) :

asa-fw# **show capture**

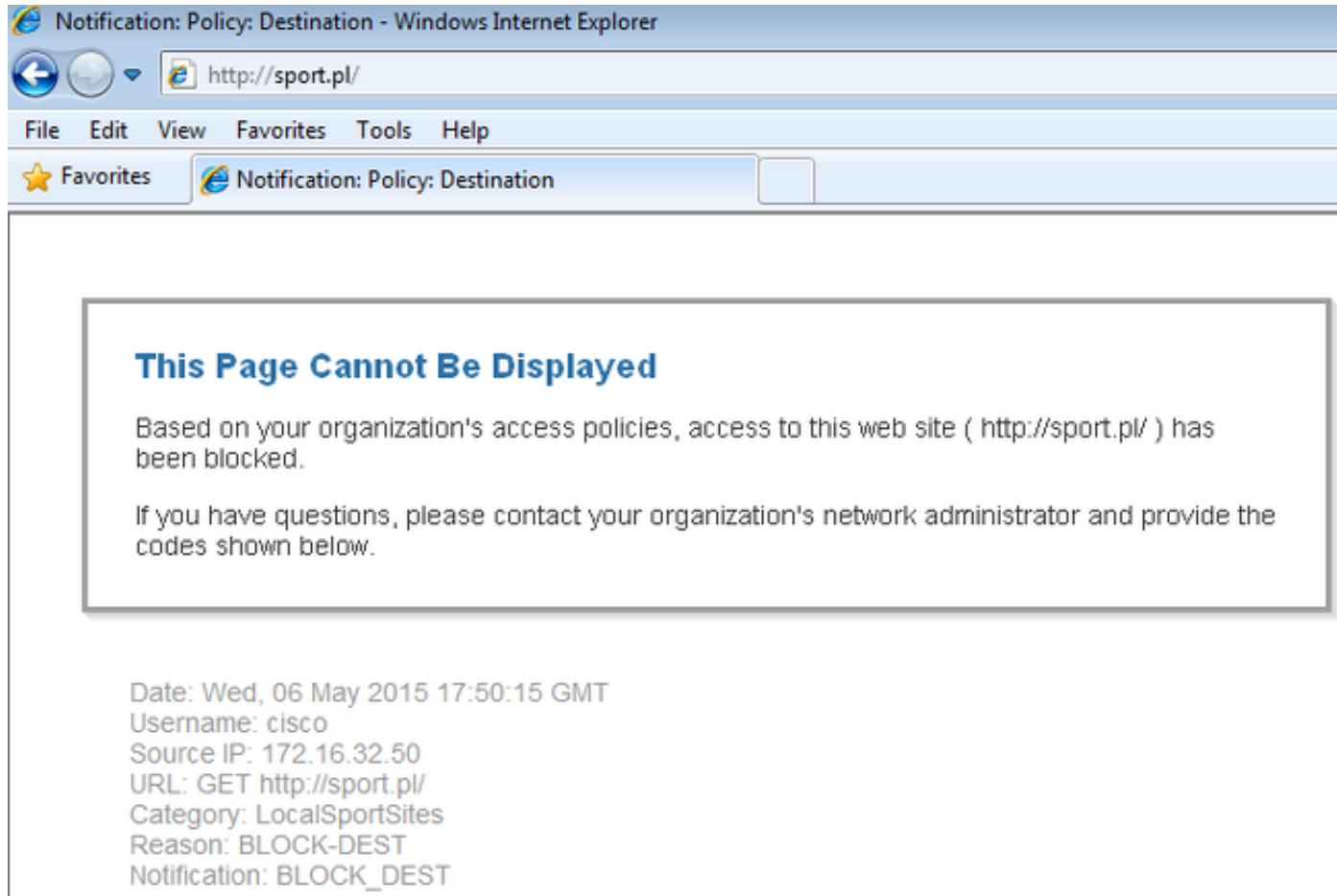
```
capture CAP type raw-data interface inside [Capturing - 70065 bytes]
match gre any any
```

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繼續TCP握手並處理GET請求。因此，名為PolicyForIT的策略會受到攻擊，流量會受到阻止：



這一點得到WSA報告的證實：



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

Displaying 1 - 3 of 3 items.

注意ISE顯示使用者名稱。

## 疑難排解

本節提供的資訊可用於對組態進行疑難排解。

### 不正確的證書

當WSA未正確初始化 ( 證書 ) 時，測試ISE連線故障：

#### 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.

## ISE pxgrid-cm.log報告：

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

使用Wireshark可以看到失敗的原因：

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	FEATURES
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(?), #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)

對於用於保護可擴展消息傳送和線上狀態協定(XMPP)交換 (由pxGrid使用) 的SSL會話，客戶端會由於伺服器提供的未知證書鍵而報告SSL故障。

## 正確案例

對於正確的場景，ISE pxgrid-controller.log將記錄：

```
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
```

此外，ISE GUI將WSA顯示為具有正確功能的使用者：

CISCO Identity Services Engine

Home Operations Policy Guest Access Administration

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Services pxGrid Identity Mapping

Clients Live Log

Enable Disable Approve Group Restore Delete Refresh Total Pending Approval(0)

Client Name	Client Description	Capabilities	Status	Client Group	Log
ise-admin-ise14		Capabilities(2 Pub, 1 Sub)	Online	Administrator	<a href="#">View</a>
ise-mnt-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 Show 25

Capability Name	Capability Version	Messaging Role	Message Filter
<input type="radio"/> SessionDirectory	1.0	Sub	
<input type="radio"/> TrustSecMetaData	1.0	Sub	

ise-admin-ise14	ise-mnt-ise14	ironport.example.com-pxgr...	ise-admin-ise14	ise-mnt-ise14	ironport.example.com-pxgr...	ise-admin-ise14	ise-mnt-ise14	ironport.example.com-pxgr...
ise-admin-ise14	ise-mnt-ise14	ironport.example.com-pxgr...	ise-admin-ise14	ise-mnt-ise14	ironport.example.com-pxgr...	ise-admin-ise14	ise-mnt-ise14	ironport.example.com-pxgr...
ise-admin-ise14	ise-mnt-ise14	ironport.example.com-pxgr...	ise-admin-ise14	ise-mnt-ise14	ironport.example.com-pxgr...	ise-admin-ise14	ise-mnt-ise14	ironport.example.com-pxgr...

ise-admin-ise14 pxGrid Connection from WSA Capabilities(2 Pub, 1 Sub) Online Administrator [View](#)

ise-mnt-ise14 pxGrid Connection from WSA Capabilities(2 Pub, 0 Sub) Online Administrator [View](#)

ironport.example.com-pxgr... pxGrid Connection from WSA Capabilities(0 Pub, 2 Sub) Online Session [View](#)

## 相關資訊

- [採用ISE的ASA 9.2.1版VPN安全評估配置示例](#)
- [WSA 8.7使用手冊](#)
- [ASA和Catalyst 3750X系列交換機TrustSec配置示例和故障排除指南](#)
- [Cisco TrustSec交換機配置指南：瞭解Cisco TrustSec](#)
- [配置外部伺服器以進行安全裝置使用者授權](#)
- [Cisco ASA系列VPN CLI配置指南9.1](#)
- [思科身份服務引擎使用手冊，版本1.2](#)
- [技術支援與文件 - Cisco Systems](#)