

TrustSec تامدخل ISE عم WSA ل م ا ك ت ن ي و ك ت ة ك ر د م ل ا

المحتويات

- [المقدمة](#)
- [المتطلبات الأساسية](#)
- [المتطلبات](#)
- [المكونات المستخدمة](#)
- [التكوين](#)
- [الرسم التخطيطي للشبكة وتدفق حركة مرور البيانات](#)
- [ASA-VPN](#)
- [أسا-فو](#)
- [محرك خدمات كشف الهوية \(ISE\)](#)
- [الخطوة 1. رقيب تكنولوجيا المعلومات ومجموعة أخرى](#)
- [الخطوة 2. قاعدة التفويض للوصول إلى الشبكة الخاصة الظاهرية \(VPN\) التي تعين الرقيب = 2 \(IT\)](#)
- [الخطوة 3. إضافة جهاز شبكة وإنشاء ملف PAC ل ASA-VPN](#)
- [الخطوة 4. تمكين دور pxGrid](#)
- [الخطوة 5. إنشاء شهادة للإدارة ودور pxGrid](#)
- [الخطوة 6. التسجيل التلقائي ل PxGrid](#)
- [WSA](#)
- [الخطوة 1. أسلوب شفاف وإعادة توجيه](#)
- [الخطوة 2. إنشاء الشهادة](#)
- [الخطوة 3. اختبار اتصال ISE](#)
- [الخطوة 4. ملفات تعريف ISE](#)
- [الخطوة 5. الوصول إلى السياسة القائمة على علامة الرقيب](#)
- [التحقق من الصحة](#)
- [الخطوة 1. جلسة شبكة VPN](#)
- [الخطوة 2. تم استرداد معلومات جلسة العمل بواسطة WSA](#)
- [الخطوة 3. إعادة توجيه حركة المرور إلى WSA](#)
- [استكشاف الأخطاء وإصلاحها](#)
- [شهادات غير صحيحة](#)
- [تصحيح السيناريو](#)
- [معلومات ذات صلة](#)

المقدمة

يوضح هذا المستند كيفية دمج جهاز أمان الويب (WSA) مع محرك خدمات الهوية (ISE). يدعم ISE الإصدار 1.3 واجهة برمجة تطبيقات (API) جديدة تسمى PxGrid. يدعم هذا البروتوكول العصري المرن المصادقة والتشفير والامتيازات (المجموعات) التي تسمح بالتكامل بسهولة مع حلول الأمان الأخرى.

يدعم WSA الإصدار 8.7 بروتوكول PXgrid ويمكنه إسترداد معلومات هوية السياق من ISE. ونتيجة لذلك، يسمح لك WSA بإنشاء سياسات تستند إلى مجموعات علامات مجموعة أمان (TrustSec (SGT التي تم إستردادها من ISE.

المتطلبات الأساسية

المتطلبات

cisco يوصي أن يتلقى أنت خبرة مع cisco ise تشكيل ومعرفة الأساسية من هذا موضوع:

- عمليات نشر ISE وتكوين التفويض
- تكوين واجهة سطر الأوامر (CLI) القابل للتكيف (ASA) للوصول إلى TrustSec و VPN
- تكوين WSA
- الفهم الأساسي لعمليات نشر TrustSec

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- نظام التشغيل Microsoft Windows 7
 - برنامج Cisco ISE Software، الإصدار 1.3 والإصدارات الأحدث
 - Cisco AnyConnect Mobile Security، الإصدار 3.1 والإصدارات الأحدث
 - ASA الإصدار 9.3.1 من Cisco والإصدارات الأحدث
 - Cisco WSA، الإصدار 8.7 والإصدارات الأحدث
- تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

التكوين

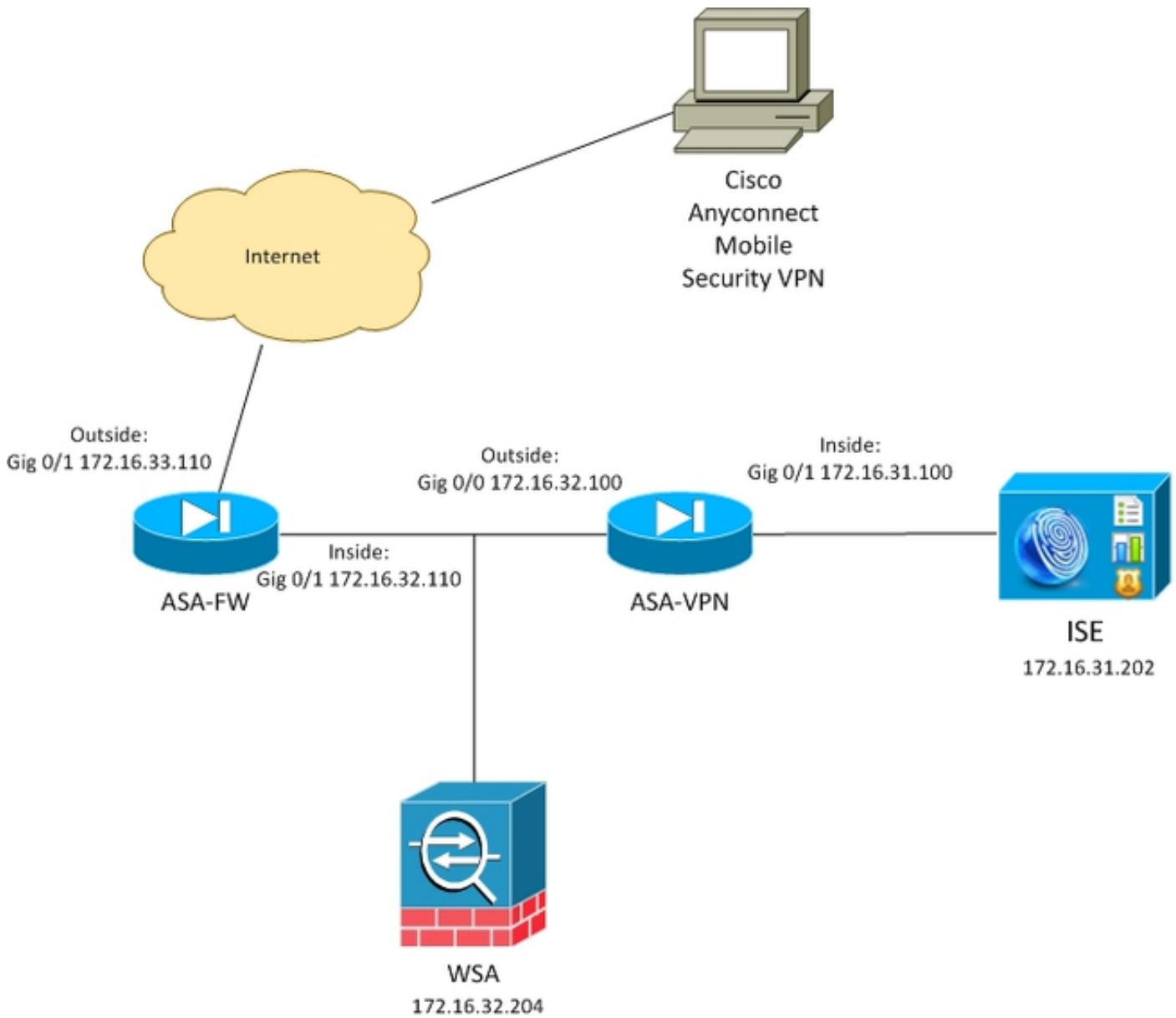
ملاحظة: أستخدم [أداة بحث الأوامر](#) (للعلماء [المسجلين](#) فقط) للحصول على مزيد من المعلومات حول الأوامر المستخدمة في هذا القسم.

الرسم التخطيطي للشبكة وتدفق حركة مرور البيانات

يتم تعيين علامات SGT الخاصة ب TrustSec بواسطة ISE المستخدم كخادم مصادقة لجميع أنواع المستخدمين الذين يصلون إلى شبكة الشركة. وهذا يتضمن المستخدمين السلبيين/اللاسلكي الذين تتم مصادقتهم عبر بوابات ضيف 802.1x أو ISE. أيضا، مستخدمو شبكة VPN البعيدة الذين يستخدمون ISE للمصادقة.

بالنسبة إلى WSA، لا يهم كيفية وصول المستخدم إلى الشبكة.

يقدم هذا المثال مستخدمى VPN البعيد الذين يقومون بإنهاء جلسة عمل على ASA-VPN. هؤلاء المستخدمين قد تم تعيينهم رقيب خاص. سيتم اعتراض جميع حركات مرور HTTP إلى الإنترنت من قبل ASA-FW (جدار الحماية) وإعادة توجيهها إلى WSA للتفتيش. يستخدم WSA ملف تعريف الهوية الذي يسمح له بتصنيف المستخدمين استنادا إلى علامة SGT وإنشاء سياسات الوصول أو فك التشفير بناء على ذلك.



التدفق التفصيلي هو:

1. يقوم مستخدم AnyConnect VPN بإنهاء جلسة عمل طبقة مآخذ التوصيل الآمنة (SSL) على ASA-VPN. يتم تكوين ASA-VPN ل TrustSec ويستخدم ISE لمصادقة مستخدمي VPN. يتم تعيين قيمة علامة الرقيب للمستخدم الذي تمت مصادقته = 2 (الاسم = المعلومات). يستلم المستخدم عنوان IP من شبكة 24/172.16.32.0 (172.16.32.50 في هذا المثال).
2. يحاول المستخدم الوصول إلى صفحة ويب في إنترنت. يتم تكوين ASA-FW لبروتوكول إتصالات ذاكرة التخزين المؤقت للويب (WCCP) الذي يعيد توجيه حركة مرور البيانات إلى WSA.
3. تم تكوين WSA لتكامل ISE. وهو يستخدم pxGrid لتنزيل المعلومات من ISE: تم تعيين عنوان IP للمستخدم 172.16.32.50 للرقيب رقم 2.
4. يقوم WSA بمعالجة طلب HTTP من المستخدم ويقوم بالوصول إلى نهج الوصول PolicyForIT. ويتم تكوين هذه السياسة لحظر حركة المرور إلى المواقع الرياضية. وكل المستخدمين الآخرين (الذين لا ينتمون إلى الرقيب 2) يطبقون سياسة الوصول الافتراضية ويتمتعون بإمكانية الوصول الكامل إلى المواقع الرياضية.

ASA-VPN

هذه عبارة VPN تم تكوينها ل TrustSec. التكوين التفصيلي خارج نطاق هذا المستند. ارجع إلى الأمثلة التالية:

- [مثال تكوين ASA و Catalyst 3750X Series Switch TrustSec ودليل أستكشاف الأخطاء وإصلاحها](#)

أسا-فو

جدار حماية ASA مسؤول عن إعادة توجيه WCCP إلى WSA. لا يعلم هذا الجهاز ب 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
```

محرك خدمات كشف الهوية (ISE)

ISE هي نقطة مركزية في نشر TrustSec. حيث تقوم بتعيين علامات الرقيب لجميع المستخدمين الذين يقومون بالوصول إلى الشبكة والمصادقة عليها. يتم سرد الخطوات المطلوبة للتكوين الأساسي في هذا القسم.

الخطوة 1. رقيب تكنولوجيا المعلومات ومجموعة أخرى

أختر سياسة < نتائج < وصول مجموعة الأمان < مجموعات الأمان وقم بإنشاء الرقيب:

CISCO Identity Services Engine Home Operations | ▾

Authentication Authorization Profiling Posture Client Provisioning

Dictionaries Conditions **Results**

Results

Search:

← ▾ [List Icon] ▾ [Settings Icon]

- 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

الخطوة 2. قاعدة التفويض للوصول إلى الشبكة الخاصة الظاهرية (VPN) التي تعين الرقيب = 2 (IT)

أخترت سياسة < تحويل وإنشاء قاعدة ل بعيد VPN منفذ. ستحصل جميع إتصالات الشبكة الخاصة الظاهرية (VPN) التي يتم إنشاؤها عبر شبكة ASA-VPN على الوصول الكامل (PermitAccess) وسيتم تعيين الرقيب رقم 2 (IT) له.

CISCO Identity Services Engine Home Operations | ▾ Policy ▾ Guest Access ▾ Administration | ▾

Authentication **Authorization** Profiling Posture Client Provisioning TrustSec Policy Elements

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

الخطوة 3. إضافة جهاز شبكة وإنشاء ملف PAC ل ASA-VPN

من أجل إضافة ASA-VPN إلى مجال TrustSec، من الضروري إنشاء ملف التكوين التلقائي للوكيل (PAC) يدويا.

سيتم إستيراد هذا الملف على ASA.

التي يمكن تكوينها من الإدارة < أجهزة الشبكة. بعد إضافة ASA، قم بالتمرير لأسفل إلى إعدادات TrustSec وقم بإنشاء ملف PAC. تفاصيل ذلك موضحة في مستند منفصل (مشار إليه).

الخطوة 4. تمكين دور pxGrid

أخترت إدارة < توزيع in order to مكن ال pxGrid دور.

الخطوة 5. إنشاء شهادة للإدارة ودور pxGrid

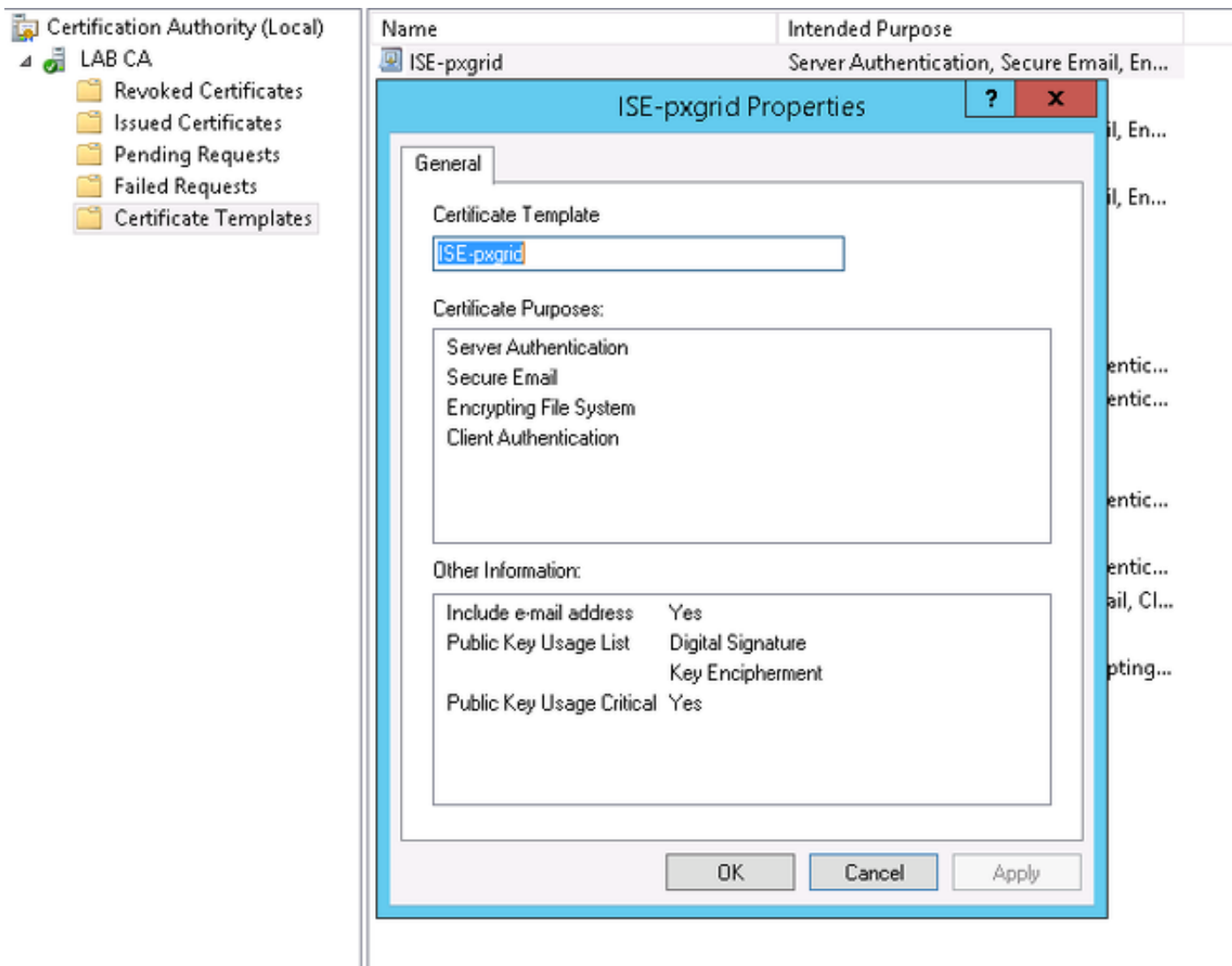
يستخدم بروتوكول pxGrid مصادقة الشهادة لكل من العميل والخادم. من المهم للغاية تكوين الشهادات الصحيحة لكل من ISE و WSA. يجب أن تتضمن كلتا الشهادتين اسم المجال المؤهل بالكامل (FQDN) في الموضوع وملحقات x509 لمصادقة العميل ومصادقة الخادم. تأكد أيضا من إنشاء سجل DNS A صحيح لكل من ISE و WSA ويطابق FQDN المتوافق.

إذا تم توقيع كلا الشهادتين من قبل مرجع مصدق مختلف (CA)، فمن المهم تضمين هذه الشهادات في المخزن الموثوق به.

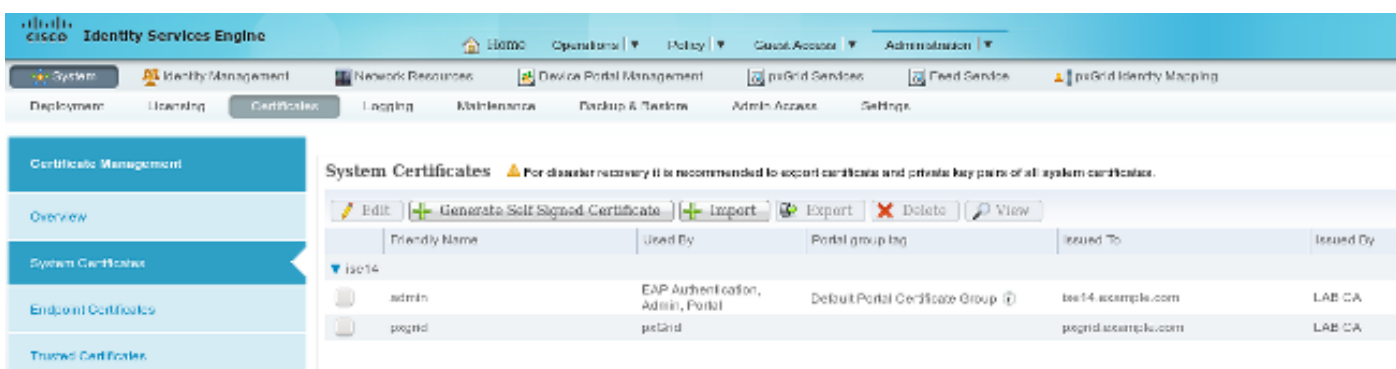
أخترت in order to شكلت شهادات، إدارة < شهادات.

يمكن أن يقوم ISE بإنشاء طلب توقيع شهادة (CSR) لكل دور. بالنسبة لدور pxGrid، قم بتصدير CSR وتوقيعه باستخدام مرجع مصدق خارجي.

في هذا المثال، تم استخدام Microsoft CA مع هذا القالب:



قد تبدو النتيجة النهائية كما يلي:



لا تنس إنشاء سجلات DNS A ل ise14.example.com و pxgrid.example.com التي تشير إلى 172.16.31.202.

الخطوة 6. التسجيل التلقائي ل PxGrid

بشكل افتراضي، لن يقوم ISE بتسجيل مشتركى PxGrid تلقائياً. وينبغي أن يوافق مدير البرنامج على ذلك يدوياً. يجب تغيير هذا الإعداد لتكامل WSA.

أختر إدارة < خدمات pxGrid واضبط تمكين التسجيل التلقائي.

WSA

الخطوة 1. أسلوب شفاف وإعادة توجيه

في هذا مثال، ال WSA شكلت مع فقط الإدارة قارن، أسلوب شفاف، وإعادة توجيه من ال ASA:

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	

الخطوة 2. إنشاء الشهادة

يجب أن تثق WSA في CA لتوقيع جميع الشهادات. اختر شبكة < إدارة الشهادات لإضافة شهادة مرجع مصدق:

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](#)

من الضروري أيضا إنشاء شهادة ستستخدمها WSA للمصادقة على pxGrid. أخترت شبكة < Identity Services Engine (محرك خدمات الهوية) < WSA زبون شهادة in order to خلقت ال CSR، وقمت بتوقيعه مع ال CA قالب (ISE-PXGRID) صحيح، واستوردته من جديد.

أيضا، بالنسبة إلى "شهادة إدارة ISE" و"شهادة ISE PxGrid"، قم باستيراد شهادة CA (لضمان شهادة PxGrid المقدمة من ISE):

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 shows 'Identity Services Engine 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

[Edit Settings...](#)

الخطوة 3. إختبار اتصال ISE

أخترت شبكة < Identity Services Engine in order to اختبرت التوصيل إلى 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.

الخطوة 4. ملفات تعريف ISE

أختر مدير أمان الويب < ملفات تعريف لإضافة ملف تعريف جديد ل ISE. للحصول على التعرف والمصادقة "أستخدم تعريف المستخدمين ب ISE بشفافية.

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 displays a table of "Client / User Identification Profiles".

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	

Buttons: Add Identification Profile... (top left), Edit Order... (bottom left)

الخطوة 5. الوصول إلى السياسة القائمة على علامة الرقيب

أختر مدير أمان الويب < سياسات الوصول لإضافة سياسة جديدة. تستخدم العضوية ملف تعريف 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>	

بالنسبة للمجموعات المحددة والمستخدمين، ستتم إضافة العلامة 2 الخاصة بالرقيب (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"/>

وتحرم هذه السياسة المستخدمين التابعين لرقبب تكنولوجيا المعلومات من الوصول إلى كافة المواقع الرياضية:

Access Policies

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

[Add Policy...](#)

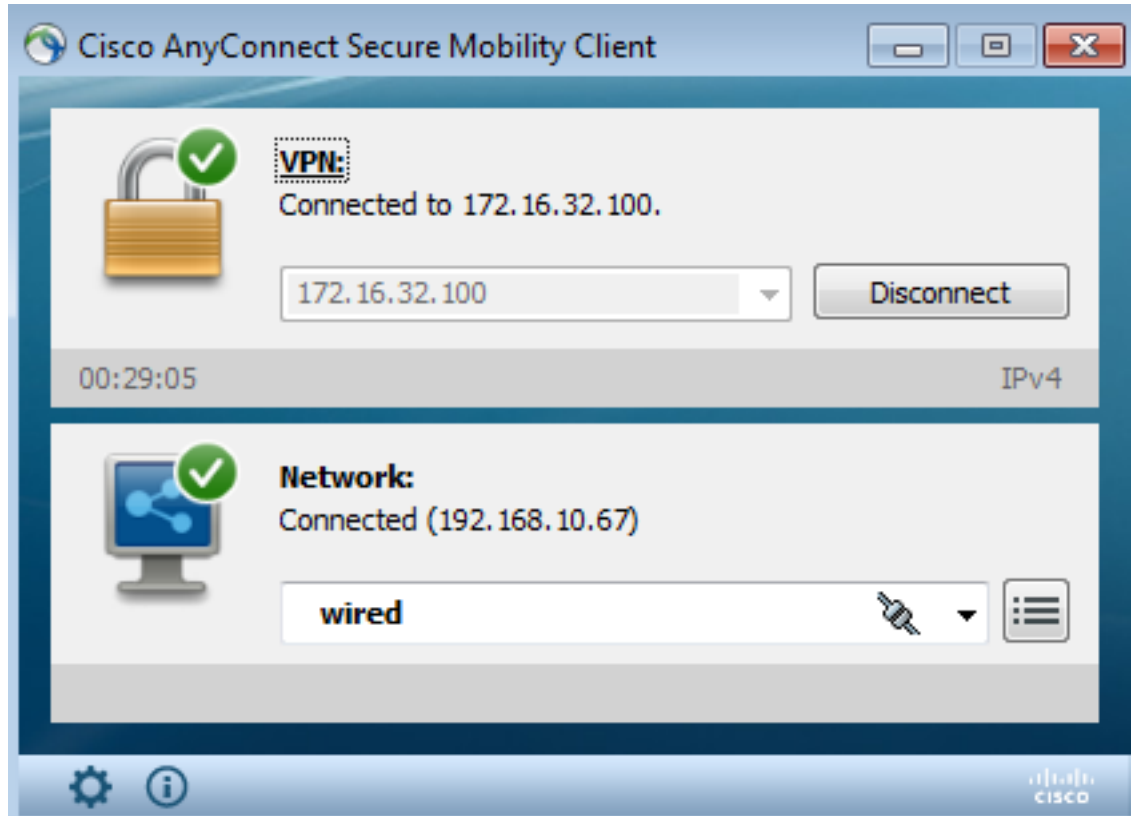
[Edit Policy Order...](#)

التحقق من الصحة

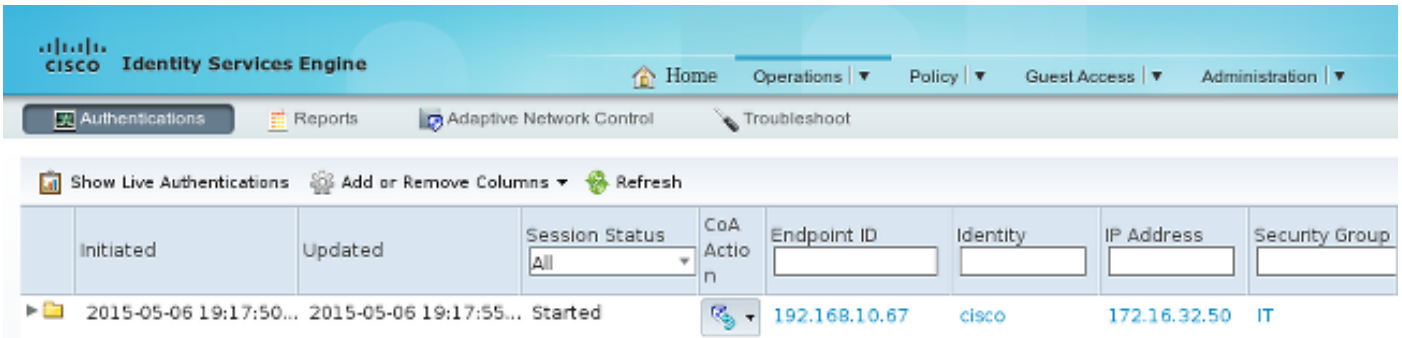
استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

الخطوة 1. جلسة شبكة VPN

يقوم مستخدم شبكة VPN بتهيئة جلسة VPN تجاه ASA-VPN:



يستخدم ASA-VPN ISE للمصادقة. يقوم نظام التشغيل ISE بإنشاء جلسة عمل ويعين فيها العلامة 2 للرقيب (IT):

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes "Home", "Operations", "Policy", "Guest Access", and "Administration". Below the navigation bar, there are tabs for "Authentications", "Reports", "Adaptive Network Control", and "Troubleshoot". The main content area displays "Show Live Authentications" with options to "Add or Remove Columns" and "Refresh". A table of live authentications is shown with the following columns: "Initiated", "Updated", "Session Status", "CoA Action", "Endpoint ID", "Identity", "IP Address", and "Security Group". The table contains one row of data: "2015-05-06 19:17:50...", "2015-05-06 19:17:55...", "Started", "None", "192.168.10.67", "cisco", "172.16.32.50", and "IT".

بعد المصادقة الناجحة، يقوم ASA-VPN بإنشاء جلسة VPN باستخدام علامة الرقيب 2 (التي تم إرجاعها في تقنية الوصول إلى RADIUS بزوج Cisco-av):

```
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

بما أن الارتباط بين ASA-VPN و ASA-FW ليس تمكين TrustSec، يرسل ASA-VPN الإطارات غير المميزة لحركة المرور تلك (لن يكون قادرا على تكوين إطارات الإيثرنت GRE باستخدام حقل CMD/TrustSec الذي تم حقه).

الخطوة 2. تم إستراداد معلومات جلسة العمل بواسطة WSA

في هذه المرحلة، يجب أن يتلقى WSA التخطيط بين عنوان IP واسم المستخدم والرقب (عبر بروتوكول 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
[ ]> █
```

الخطوة 3. إعادة توجيه حركة المرور إلى WSA

يقوم مستخدم شبكة VPN ببدء اتصال ب Sport.pl، والذي يتم اعتراضه بواسطة 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
```

وإنشاء قنوات في GRE إلى WSA (لاحظ أن WCCP Router-id هو أعلى عنوان IP تم تكوينه):

```
asa-fw# show capture
[capture CAP type raw-data interface inside [Capturing - 70065 bytes
match gre any any
```

```
asa-fw# show capture CAP
```

```
packets captured 525
```

```
ip-proto-47, length 60 :172.16.32.204 < 172.16.33.110 03:21:45.035657 :1
ip-proto-47, length 48 :172.16.32.204 < 172.16.33.110 03:21:45.038709 :2
ip-proto-47, length 640 :172.16.32.204 < 172.16.33.110 03:21:45.039960 :3
```

يوصل WSA مصافحة TCP ويعالج طلب GET. ونتيجة لذلك، تم الوصول إلى النهج المسمى PolicyForIT وتم حظر حركة المرور:

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

وهذا ما يؤكدته تقرير رابطة محترفات الحرب:

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)		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.

لاحظ أن ISE يعرض اسم المستخدم.

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

شهادات غير صحيحة

في حالة عدم تهيئة (شهادات) WSA بشكل صحيح، يجب اختبار فشل اتصال 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.

يلغ ISE pxgrid-cm.log :

```
[2015-05-06T16:26:51Z] [INFO ] [cm-1.jabber-172-16-31-202]
TCPSocketStream::_doSSLHandshake] [] Failure performing SSL handshake: 1]
وبوسعنا أن نرى السبب وراء هذا الفشل مع فيرسهارك:
```

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, Descrip

▷ 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)

بالنسبة لجلسة SSL المستخدمة لحماية تبادل بروتوكول التواجد والمراسلة الممتدة (XMPP) (المستخدم من قبل pxGrid)، يبلغ العميل عن فشل SSL بسبب سلسلة شهادات غير معروفة مقدمة من الخادم.

تصحيح السيناريو

للسيناريو الصحيح، يتم تسجيل الدخول إلى ISE pxgrid-controller.log :

INFO [Thread-7] [] cisco.pxgrid.controller.sasl.SaslWatcher 18:40:09,153 2015-05-06

Handling authentication for user name wsa.example.com-test_client -:::-

كما تقدم واجهة المستخدم الرسومية (GUI) لنظام التشغيل WSA كمشارك بالإمكانات الصحيحة:

The screenshot shows the Cisco Identity Services Engine (ISE) GUI. The top navigation bar includes 'Home', 'Operations', 'Policy', 'Quest Access', and 'Administration'. Below the navigation bar, there are tabs for 'System', 'Identity Management', 'Network Resources', 'Device Portal Management', 'pxGrid Services', 'Fixed Services', and 'pxGrid Identity Mapping'. The main content area is titled 'Clients' and 'Live Log'. It features a table of clients with columns: Client Name, Client Description, Capabilities, Status, Client Group, and Log. The table lists three clients: 'ise-admin-ise14', 'ise-mnt-ise14', and 'ironport.example.com-pxgr...'. A 'Capability Detail' pop-up window is open, showing a table of capabilities with columns: Capability Name, Capability Version, Messaging Role, and Message Filter. The capabilities listed are 'SessionDirectory' and 'TrustSecMetadata', both with version 1.0 and role Sub.

معلومات ذات صلة

- [ASA الإصدار 9.2.1 VPN Posture مع مثال تكوين ISE](#)
- [دليل مستخدمي WSA 8.7](#)
- [مثال تكوين ASA و Catalyst 3750X Series Switch TrustSec ودليل أكتشاف الأخطاء وإصلاحها](#)
- [دليل تكوين محول Cisco TrustSec: فهم Cisco TrustSec](#)
- [تكوين خادم خارجي لتفويض مستخدم جهاز الأمان](#)
- [دليل تكوين واجهة سطر الأوامر Cisco ASA Series VPN الإصدار 9.1](#)
- [دليل مستخدم محرك خدمات الهوية من Cisco، إصدار 1.2](#)
- [الدعم التقني والمستندات - Cisco Systems](#)

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن تسم ل اذ ه Cisco ت مچرت
م ل اء ان ا ع مچ ي ف ن م دخت س م ل م عد و ت م م م دقت ل ة يرش ب ل و
امك ة ق ي ق د ن و ك ت ن ل ة ل آل ة مچرت ل ض ف ا ن ا ة ظ ح ال م ي ج ر ي . ة ص ا خ ل م ه ت غ ل ب
Cisco ي ل خ ت . ف ر ت م م مچرت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ال ا ة مچرت ل ا ع م ل ا ح ل ا و ه
ل ا ا م ا د ع و ج ر ل ا ب ي ص و ت و ت ا مچرت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Systems
(ر ف و ت م ط ب ا ر ل ا) ي ل ص ا ل ا ي ز ي ل ج ن ا ل ا دن ت س م ل ا