

Configurar a integração WSA com o ISE para serviços clientes de TrustSec

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Configurar](#)

[Diagrama da rede e fluxo de tráfego](#)

[ASA-VPN](#)

[ASA-FW](#)

[ISE](#)

[Etapa 1. SGT para o TI e o outro grupo](#)

[Etapa 2. Regra da autorização para o acesso VPN que atribui SGT = 2 \(a TI\)](#)

[Etapa 3. Adicionar o dispositivo de rede e gerencia o arquivo PAC para ASA-VPN](#)

[Etapa 4. Permita o papel do pxGrid](#)

[Etapa 5. Gerencia o certificado para a administração e o papel do pxGrid](#)

[Registro automático do pxGrid de etapa 6.](#)

[WSA](#)

[Etapa 1. Modo transparente e reorientação](#)

[Etapa 2. Geração do certificado](#)

[Etapa 3. Teste a Conectividade ISE](#)

[Etapa 4. Perfis da identificação ISE](#)

[Etapa 5. Alcance a política baseada na etiqueta SGT](#)

[Verificar](#)

[Etapa 1. Sessão de VPN](#)

[Etapa 2. Informação de sessão recuperada pelo WSA](#)

[Etapa 3. Reorientação do tráfego ao WSA](#)

[Troubleshooting](#)

[Certificados incorretos](#)

[Encenação correta](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve como integrar a ferramenta de segurança da Web (WSA) com Identity Services Engine (ISE). A versão 1.3 ISE apoia um pxGrid chamado API novo. Estes suportes de protocolo modernos e flexíveis autenticação, criptografia, e privilégios (grupos) que permite a fácil

integração com outras soluções da Segurança.

A versão 8.7 WSA apoia o protocolo do pxGrid e pode recuperar a informação de identidade do contexto do ISE. Em consequência, WSA permite que você construa as políticas baseadas nos grupos da etiqueta do grupo de segurança de TrustSec (SGT) recuperados do ISE.

Pré-requisitos

Requisitos

Cisco recomenda que você tem a experiência com configuração de Cisco ISE e conhecimento básico destes assuntos:

- Disposições e configuração de autorização ISE
- Configuração de CLI adaptável da ferramenta de segurança (ASA) para o acesso de TrustSec e VPN
- Configuração WSA
- Compreensão básica de disposições de TrustSec

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Microsoft Windows 7
- Versão de software 1.3 de Cisco ISE e mais atrasado
- Versão 3.1 e mais recente do Mobile Security de Cisco AnyConnect
- Versão ASA 9.3.1 de Cisco e mais atrasado
- Versão 8.7 e mais recente de Cisco WSA

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Configurar

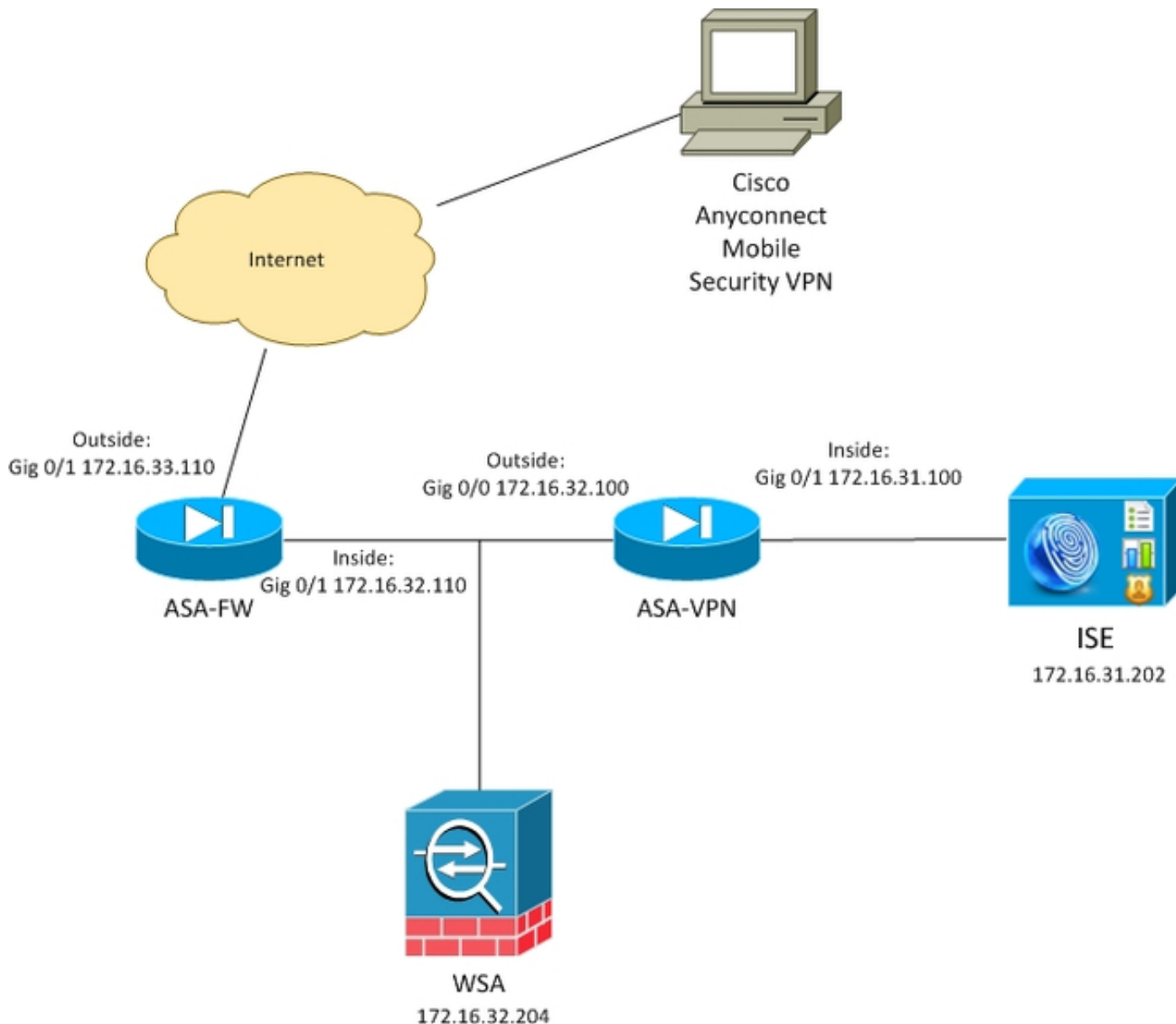
Note: Use a [Command Lookup Tool](#) ([somente clientes registrados](#)) para obter mais informações sobre os comandos usados nesta seção.

Diagrama da rede e fluxo de tráfego

As etiquetas de TrustSec SGT são atribuídas pelo ISE usado como um Authentication Server para todos os tipos de usuários que alcançam a rede corporativa. Isto envolve prendido/usuários Wireless que autenticam através dos portais do 802.1x ou do convidado ISE. Também, usuários remotos VPN que usam o ISE para a autenticação.

Para WSA, não importa como o usuário alcançou a rede.

Este exemplo apresenta os usuários remotos VPN que terminam a sessão no ASA-VPN. Aqueles usuários foram atribuídos uma etiqueta específica SGT. Todo o tráfego de HTTP ao Internet será interceptado pelo ASA-FW (Firewall) e reorientado ao WSA para a inspeção. O WSA usa o perfil da identidade que permite que classifique os usuários baseados na etiqueta SGT e construa o acesso ou as políticas de descryptografia baseado naquele.



O fluxo detalhado é:

1. O usuário de AnyConnect VPN termina a sessão do secure sockets layer (SSL) no ASA-VPN. O ASA-VPN é configurado para TrustSec e usa o ISE para a autenticação de usuários do VPN. O usuário autenticado é atribuído um valor da etiqueta SGT = 2 (name= a TI). O usuário recebe um endereço IP de Um ou Mais Servidores Cisco ICM NT da rede 172.16.32.0/24 (172.16.32.50 neste exemplo).
2. O usuário tenta alcançar o página da web no Internet. O ASA-FW é configurado para o Protocolo de Comunicação de Cache da Web (WCCP) que reorienta o tráfego ao WSA.
3. O WSA é configurado para a integração ISE. Usa o pxGrid a fim transferir a informação do ISE: o IP address 172.16.32.50 do usuário foi atribuído a etiqueta 2. SGT.

4. O WSA processa o pedido do HTTP do usuário e bate a política de acesso PolicyForIT. Que a política está configurada para obstruir o tráfego aos locais dos esportes. Todos usuários restantes (que não pertencem a SGT 2) batem a política de acesso do padrão e têm o acesso direto aos locais dos esportes.

ASA-VPN

Este é um gateway de VPN configurado para TrustSec. A configuração detalhada é fora do espaço deste documento. Refira estes exemplos:

- [O ASA e o exemplo de configuração de TrustSec do Catalyst 3750X Series Switch e pesquisam defeitos o guia](#)
- [Exemplo de configuração da classificação e da aplicação da versão ASA 9.2 VPN SGT](#)

ASA-FW

O Firewall ASA é responsável para o redirecionamento de WCCP ao WSA. Este dispositivo não está ciente 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

O ISE é um ponto central no desenvolvimento de TrustSec. Atribui etiquetas SGT a todos os usuários que alcançam e autenticam à rede. As etapas exigidas para a configuração básica são alistadas nesta seção.

Etapa 1. SGT para o TI e o outro grupo

Escolha **grupos do > segurança do acesso do grupo do > segurança da política > dos resultados** e crie o SGT:

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

Etapa 2. Regra da autorização para o acesso VPN que atribui SGT = 2 (a TI)

Escolha a política > a autorização e crie uma regra para o acesso remoto VPN. Todas as conexões de VPN estabelecidas através de ASA-VPN obterão o acesso direto (PermitAccess) e serão atribuídas a etiqueta 2 SGT (a TI).

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

Etapa 3. Adicionar o dispositivo de rede e gerencia o arquivo PAC para ASA-VPN

A fim adicionar o ASA-VPN ao domínio de TrustSec, é necessário gerar arquivo da configuração do proxy o auto (PAC) manualmente. Esse arquivo será importado no ASA.

Isso pode ser configurado da **administração > dos dispositivos de rede**. Depois que o ASA é adicionado, enrole para baixo ajustes de TrustSec e gerencia o arquivo PAC. Os detalhes para aquele são descritos em um documento (provido) separado.

Etapa 4. Permita o papel do pxGrid

Escolha a **administração > o desenvolvimento** a fim permitir o papel do pxGrid.

The screenshot displays the Cisco Identity Services Engine (ISE) Administration web interface. The top navigation bar includes 'Home', 'Operations', 'Policy', 'Guest Access', and 'Administration'. Below this, a secondary navigation bar lists various services like '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 a specific node. The 'General Settings' tab is active, displaying fields for Hostname (ise14), FQDN (ise14.example.com), IP Address (172.16.31.202), and Node Type (Identity Services Engine (ISE)). Below these fields, the 'Personas' section is expanded, showing a list of roles with checkboxes and role dropdown menus. The 'Administration' role is checked and set to 'STANDALONE'. The 'Monitoring' role is checked and set to 'PRIMARY'. The 'Policy Service' role is checked, with 'Enable Session Services' and 'Enable Profiling Service' sub-options checked. At the bottom of the list, the 'pxGrid' checkbox is also checked.

Etapa 5. Gerencia o certificado para a administração e o papel do pxGrid

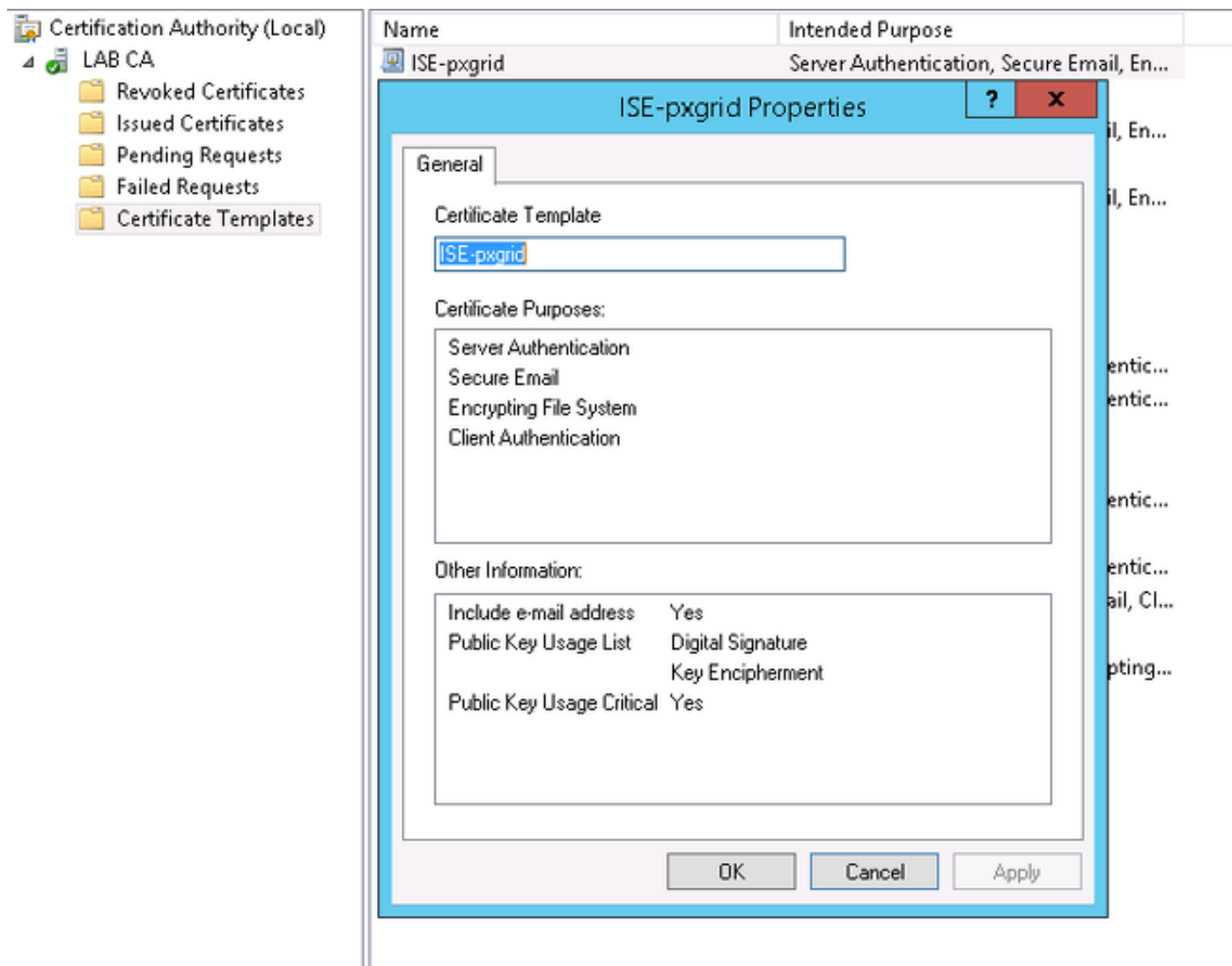
O protocolo do pxGrid usa o certificado de autenticação para o cliente e o server. É muito importante configurar os Certificados corretos para o ISE e o WSA. Ambos os Certificados devem incluir o nome de domínio totalmente qualificado (FQDN) no assunto e os Ramais x509 para a autenticação do cliente e a autenticação de servidor. Também, certifique-se que o registro correto DNS A está criado para o ISE e o WSA e combina o FQDN correspondente.

Se ambos os Certificados são assinados por um Certificate Authority (CA) diferente, é importante incluir aqueles CA na loja confiada.

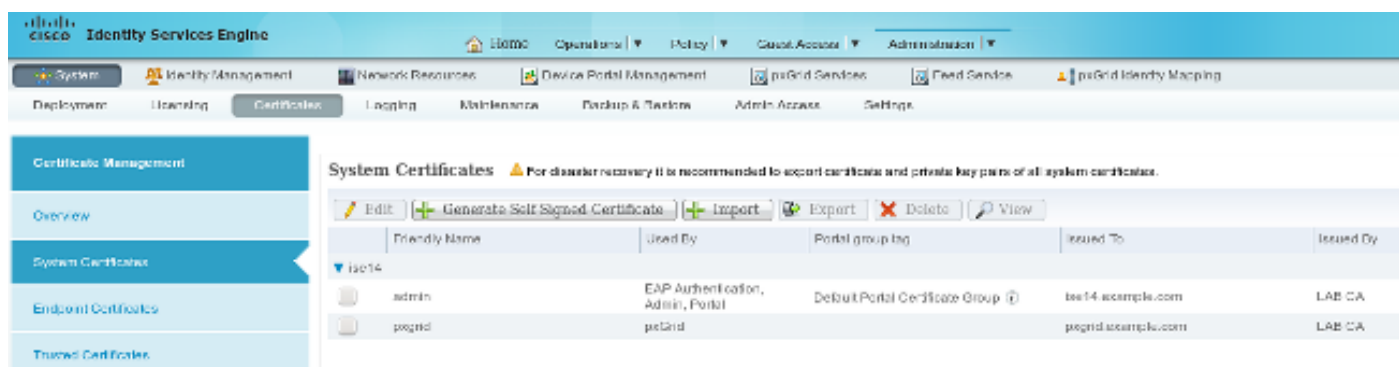
A fim configurar Certificados, escolha a **administração > Certificados**.

O ISE pode gerar uma solicitação de assinatura de certificado (CSR) para cada papel. Para o papel do pxGrid, a exportação e assina o CSR com CA externo.

Neste exemplo, Microsoft CA foi usado com este molde:



O resultado final pôde olhar como:



Não esqueça criar os registros DNS A para `ise14.example.com` e `pxgrid.example.com` que apontam a `172.16.31.202`.

Registro automático do pxGrid de etapa 6.

À revelia, o ISE não registrará automaticamente assinantes do pxGrid. Isso deve manualmente ser aprovado pelo administrador. Esse ajuste deve ser mudado para a integração WSA.

Escolha **serviços da administração** > do pxGrid e o grupo **permite o registro automático**.

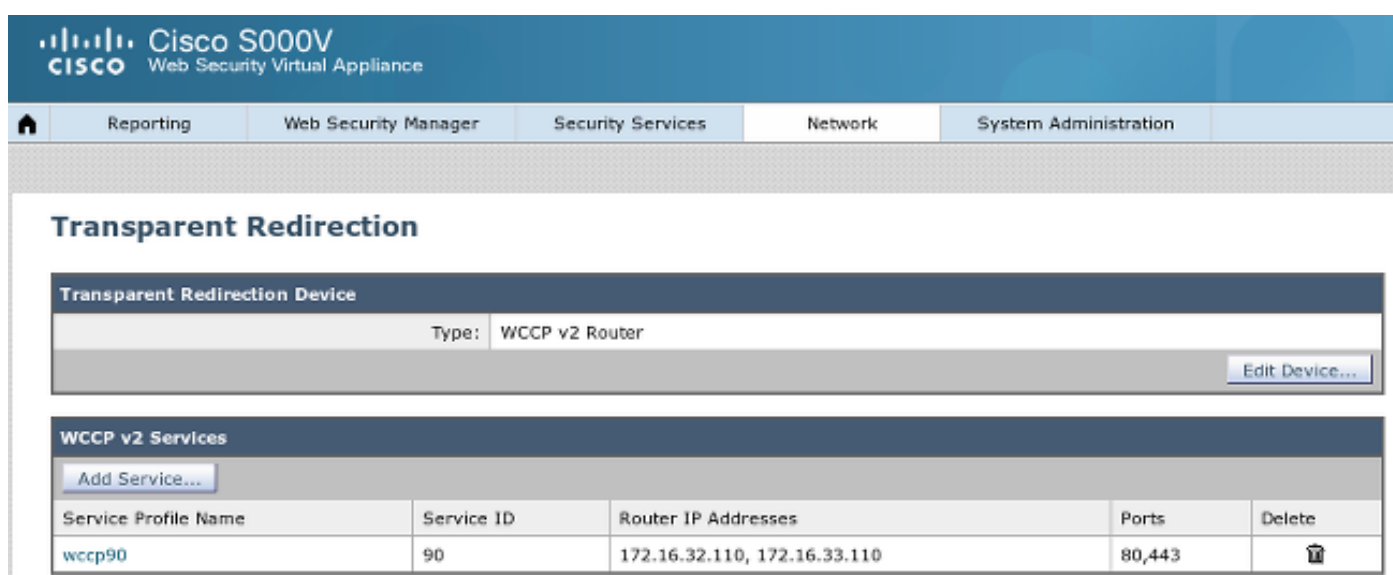
[View By Capabilities](#)

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

WSA

Etapa 1. Modo transparente e reorientação

Neste exemplo, o WSA é configurado com apenas a interface de gerenciamento, o modo transparente, e a reorientação do 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	

Etapa 2. Geração do certificado

O WSA precisa de confiar CA para assinar todos os Certificados. Escolha o > **gerenciamento de certificado da rede** a fim adicionar um certificado de CA:

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

É igualmente necessário gerar um certificado que o WSA se usará a fim autenticar ao pxGrid. Escolha a rede > o Identity Services Engine > o certificado de cliente WSA a fim gerar o CSR, assine-o com o molde correto de CA (ISE-pxgrid), e importe-o para trás.

Também, para “o certificado ISE Admin” e “o certificado do pxGrid ISE”, importe o certificado de CA (a fim confiar o certificado do pxGrid apresentado pelo 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...

Etapa 3. Teste a Conectividade ISE

Escolha a rede > o Identity Services Engine a fim testar a conexão ao 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.

Etapa 4. Perfis da identificação ISE

Escolha perfis do gerenciador de segurança > da identificação da Web a fim adicionar um perfil novo para o ISE. Para da "" o uso "identificação e da autenticação identifique transparentemente usuários com ISE".

The screenshot shows the Cisco S000V Web Security Virtual Appliance interface. The top navigation bar includes 'Reporting', 'Web Security Manager', 'Security Services', 'Network', and 'System Administration'. The main content area is titled 'Identification Profiles' and contains a table of 'Client / User Identification Profiles'. The table has five columns: 'Order', 'Transaction Criteria', 'Authentication / Identification Decision', 'End-User Acknowledgement', and 'Delete'. There are two rows: one for the 'ISE' profile and one for the 'Global Identification Profile'.

Order	Transaction Criteria	Authentication / Identification Decision	End-User Acknowledgement	Delete
1	ISE Protocols: HTTP/HTTPS	Identify Users Transparently: Identity Services Engine Guest privileges for users falling transparent user identification	(global profile)	
	Global Identification Profile	Exempt from Authentication / User Identification	Not Available	

Etapa 5. Alcance a política baseada na etiqueta SGT

Escolha o gerenciador de segurança > as políticas de acesso da Web a fim adicionar uma política nova. A sociedade usa o perfil 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>	

Para grupos e usuários selecionados a etiqueta 2 SGT será adicionada (a TI):

Access Policies: Policy "PolicyForIT": Edit Secure Group Tags

Authorized Secure Group Tags

Use the search function below to add Secure Group Tags. To remove Secure Group Tags from this policy, use the Delete option.

1 Secure Group Tag(s) currently included in this policy.

Secure Group Tag Name	SGT Number	SGT Description	Delete
IT	2	__NONE__	<input type="checkbox"/>

[Delete](#)

Secure Group Tag Search

Enter any text to search for a Secure Group Tag name, number, or description. Select one or more Secure Group Tags from the list and use the Add button to add to this policy.

Search x

0 Secure Group Tag(s) selected for Add

[Add](#)

Secure Group Tag Name	SGT Number	SGT Description	Select
Unknown	0	Unknown Security Group	<input type="checkbox"/>
Marketing	3	__NONE__	<input type="checkbox"/>
IT	2	__NONE__	<input checked="" type="checkbox"/>
ANY	65535	Any Security Group	<input type="checkbox"/>

A política nega o acesso a todos os locais dos esportes para os usuários que pertencem a SGT A TI:

Access Policies

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

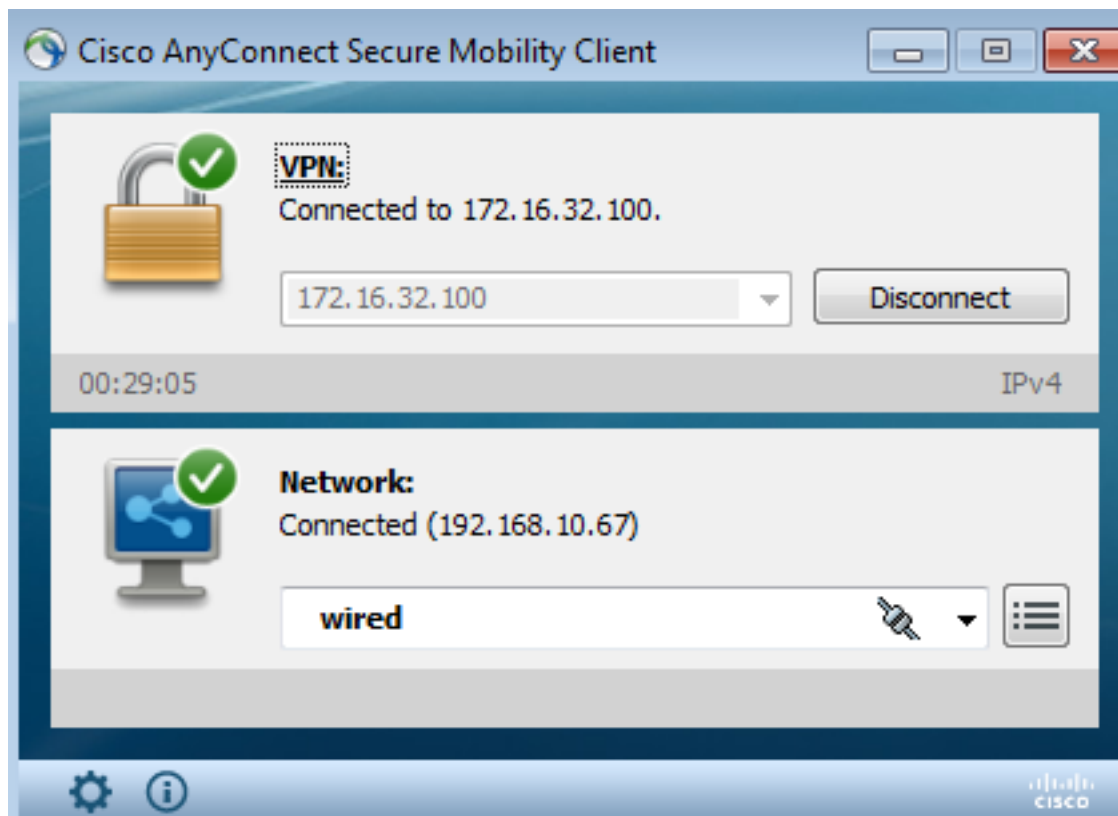
[Edit Policy Order...](#)

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

Etapa 1. Sessão de VPN

O usuário VPN inicia uma sessão de VPN para o ASA-VPN:



O ASA-VPN usa o ISE para a autenticação. O ISE cria uma sessão e atribui a etiqueta 2 SGT (a TI):

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 "Refresh" button. Below this is a table with 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", a dropdown menu, "192.168.10.67", "cisco", "172.16.32.50", and "IT".

Após a autenticação bem sucedida, o ASA-VPN cria uma sessão de VPN com a etiqueta 2 SGT (retornada na aceitação de acesso do raio no 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
```

Desde que o link entre o ASA-VPN e o ASA-FW não é TrustSec permitido, o ASA-VPN envia frames sem etiqueta para esse tráfego (não possa ao GRE encapsulam frames da Ethernet com o campo CMD/TrustSec injetado).

Etapa 2. Informação de sessão recuperada pelo WSA

Nesta fase, o WSA deve receber o mapeamento entre o endereço IP de Um ou Mais Servidores Cisco ICM NT, o username, e o SGT (através do protocolo do 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
[ ]> █
```

Etapa 3. Reorientação do tráfego ao WSA

O usuário VPN inicia uma conexão a sport.pl, que é interceptado pelo 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 escavado um túnel no GRE ao WSA (observação que a roteador-identificação WCCP é o endereço IP de Um ou Mais Servidores Cisco ICM NT o mais alto configurado):

```
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
```

O WSA continua o cumprimento de TCP e processa o pedido GET. Em consequência, a política nomeada PolicyForIT é bater e o tráfego é obstruído:

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

Isso é confirmado pelo relatório 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.

Observe que o ISE indica o username.

Troubleshooting

Esta seção fornece a informação que você pode se usar a fim pesquisar defeitos sua configuração.

Certificados incorretos

Quando o WSA não estiver inicializado corretamente (Certificados), teste para a falha de conexão 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.
```

Os relatórios ISE pxgrid-cm.log:

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

A razão para a falha pode ser considerada com 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)

Para uma sessão de SSL usada para proteger a troca elástico do protocolo da Mensagem e da presença (XMPP) (usada pelo pxGrid), a falha dos relatórios SSL do cliente devido a um certificate chain desconhecido apresentado pelo server.

Encenação correta

Para a encenação correta, os logs ISE pxgrid-controller.log:

```
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
```

Também, o ISE GUI apresenta o WSA como um subscritor com as capacidades corretas:

Client Name	Client Description	Capabilities	Status	Client Group	Log
ise-admin-ise14		Capabilities(2 Pub, 1 Sub)	Online	Administrator	View
ise-mn1-ise14		Capabilities(2 Pub, 0 Sub)	Online	Administrator	View
Ironport.example.com-pxgr...	pxGrid Connection from WSA	Capabilities(0 Pub, 2 Sub)	Online	Session	View

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

wsa.example.com-test_client	pxGrid Connection from WSA	Capabilities(0 Pub, 0 Sub)	Offline	Session	View
-----------------------------	----------------------------	----------------------------	---------	---------	----------------------

Informações Relacionadas

- [Postura da versão ASA 9.2.1 VPN com exemplo de configuração ISE](#)
- [Guia de usuários WSA 8.7](#)
- [O ASA e o exemplo de configuração de TrustSec do Catalyst 3750X Series Switch e pesquisam defeitos o guia](#)
- [Guia de configuração de switch de Cisco TrustSec: Compreendendo Cisco TrustSec](#)
- [Configurando um servidor interno para a autorização de usuário da ferramenta de segurança](#)
- [Guia de configuração de CLI da série VPN de Cisco ASA, 9.1](#)
- [Guia do Usuário do Cisco Identity Services Engine, liberação 1.2](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)