

Configurar TrustSec SXP entre o ISE e o ASAv

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Diagrama de Rede](#)

[Endereços IP](#)

[Configuração inicial](#)

[Dispositivo de rede ISE](#)

[Registro ASA como um dispositivo de rede](#)

[Gerencia fora da faixa \(OOB\) PAC \(credenciais protegidas do acesso\) e transfira](#)

[Configuração do servidor AAA ASDM](#)

[Crie o Grupo de servidores AAA](#)

[Adicionar o server ao grupo de servidor](#)

[Importe o PAC transferido do ISE](#)

[Refresque dados do ambiente](#)

[Verificação](#)

[Logs vivos ISE](#)

[Grupos de segurança ISE](#)

[ASDM PAC](#)

[Dados e grupos de segurança do ambiente ASDM](#)

[Configuração ASDM SXP](#)

[Permita SXP](#)

[Ajuste a senha do endereço IP de origem do padrão SXP e do padrão SXP](#)

[Adicionar o par SXP](#)

[Configuração ISE SXP](#)

[Configuração de senha global SXP](#)

[Adicionar o dispositivo SXP](#)

[Verificação SXP](#)

[Verificação ISE SXP](#)

[Mapeamentos ISE SXP](#)

[Verificação ASDM SXP](#)

[IP instruído ASDM SXP aos mapeamentos SGT](#)

[Captura de pacote de informação tomada no ISE](#)

Introdução

Este documento descreve como configurar uma conexão SXP (protocolo de intercâmbio do grupo de segurança) entre ISE (Identity Services Engine) e um ASAv (ferramenta de segurança adaptável virtual).

SXP é o protocolo de intercâmbio SGT (etiqueta do grupo de segurança) usado por TrustSec para propagar o IP aos mapeamentos SGT aos dispositivos de TrustSec. SXP foi desenvolvido para permitir as redes que incluem os dispositivos de terceira parte ou os dispositivos Cisco do legado que não apoiam a colocação de etiquetas inline SGT para ter capacidades de TrustSec. SXP é um peering protocol, um dispositivo atuará como um orador e o outro como um ouvinte. O orador SXP é responsável por enviar os emperramentos IP-SGT e o ouvinte é responsável por recolher estes emperramentos. A conexão SXP usa a porta TCP 64999 como o protocolo de transporte subjacente e o MD5 para a integridade de mensagem/autenticidade.

SXP foi publicado como um esboço de IETF no seguinte link:

<https://datatracker.ietf.org/doc/draft-smith-kandula-sxp/>

Pré-requisitos

Requisitos

Matriz de compatibilidade de TrustSec:

<http://www.cisco.com/c/en/us/solutions/enterprise-networks/trustsec/solution-overview-listing.html>

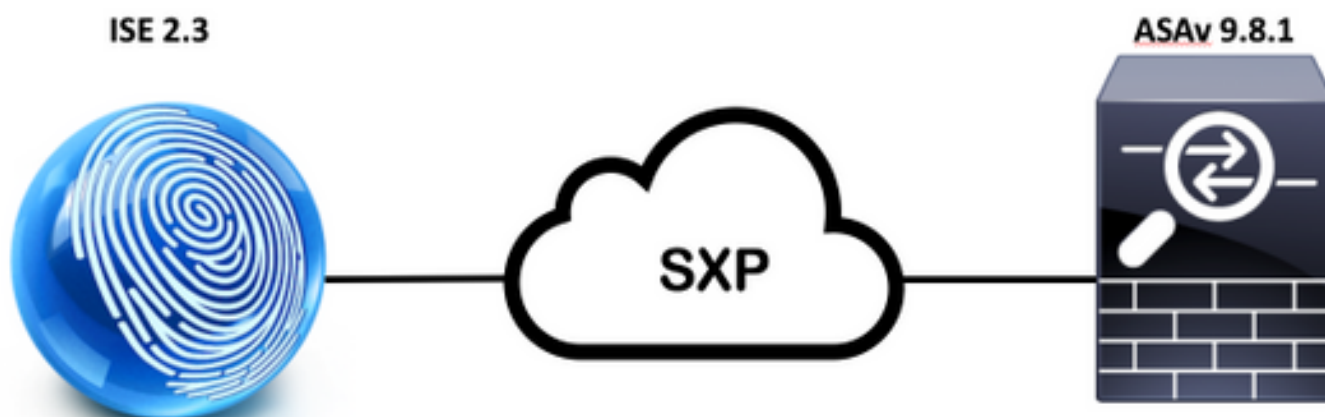
Componentes Utilizados

ISE 2.3

ASAv 9.8.1

ASDM 7.8.1.150

Diagrama de Rede



Endereços IP

ISE: 14.36.143.223

ASAv: 14.36.143.30

Configuração inicial

Dispositivo de rede ISE

Registro ASA como um dispositivo de rede

>Add de WorkCenters > de TrutSec > de componentes > de dispositivos de rede

Network Devices List > **New Network Device**

Network Devices

* Name

Description

IP Address /

RADIUS Authentication Settings

RADIUS UDP Settings

Protocol **RADIUS**

* Shared Secret

CoA Port

Advanced TrustSec Settings

▼ **Device Authentication Settings**

Use Device ID for TrustSec

Identification

Device Id

* Password

▼ **TrustSec Notifications and Updates**

* Download environment data every

* Download peer authorization policy every

* Reauthentication every ⓘ

* Download SGACL lists every

Other TrustSec devices to trust this device

Send configuration changes to device Using CoA CLI (SSH)

Ssh Key

Gerencia fora da faixa (OOB) PAC (credenciais protegidas do acesso) e transfira

▼ **Out Of Band (OOB) TrustSec PAC**

Issue Date

Expiration Date

Issued By

Generate PAC

The Identity field specifies the username or machine name presented as the "inner username" by the EAP-FAST protocol. If the Identity string entered here does not match that username, authentication will fail.

* Identity


* Encryption Key

* PAC Time to Live

Expiration Date 29 Jan 2018 22:47:42 GMT

Opening ASAv.pac

You have chosen to open:

 **ASAv.pac**
which is: **Binary File**
from: **https://14.36.143.223**

Would you like to save this file?

Configuração do servidor AAA ASDM

Crie o Grupo de servidores AAA

A configuração > o Firewall > a identidade por TrustSec > por grupo de servidor Setup > controlam...

Server Group Setup


Server Group Name:

>Add dos Grupos de servidores AAA

| AAA Server Groups | | | | | | | Add |
|-------------------|----------|-----------------|-------------------|-----------|---------------------|----------|--------|
| Server Group | Protocol | Accounting Mode | Reactivation Mode | Dead Time | Max Failed Attempts | Realm Id | |
| LOCAL | LOCAL | | | | | | Edit |
| | | | | | | | Delete |

- Grupo de servidores AAA: <Group Name>
- Permita a autorização dinâmica

AAA Server Group:

Protocol: 

Realm-id:

Accounting Mode: Simultaneous Single

Reactivation Mode: Depletion Timed

Dead Time: minutes

Max Failed Attempts:

Enable interim accounting update

Update Interval: Hours


Enable Active Directory Agent mode

ISE Policy Enforcement

Enable dynamic authorization

Dynamic Authorization Port:

Use authorization only mode (no common password configuration required)

VPN3K Compatibility Option 

Specify whether a downloadable ACL received from RADIUS should be merged with a Cisco AV-Pair ACL.

Do not merge

Place the downloadable ACL after Cisco AV-Pair ACL

Place the downloadable ACL before Cisco AV-Pair ACL

Adicionar o server ao grupo de servidor

Server no > Add selecionado do grupo

| Servers in the Selected Group | | |
|-------------------------------|-----------|---------|
| Server Name or IP Address | Interface | Timeout |
| | | |

Add

Edit

Delete

Move Up

Move Down

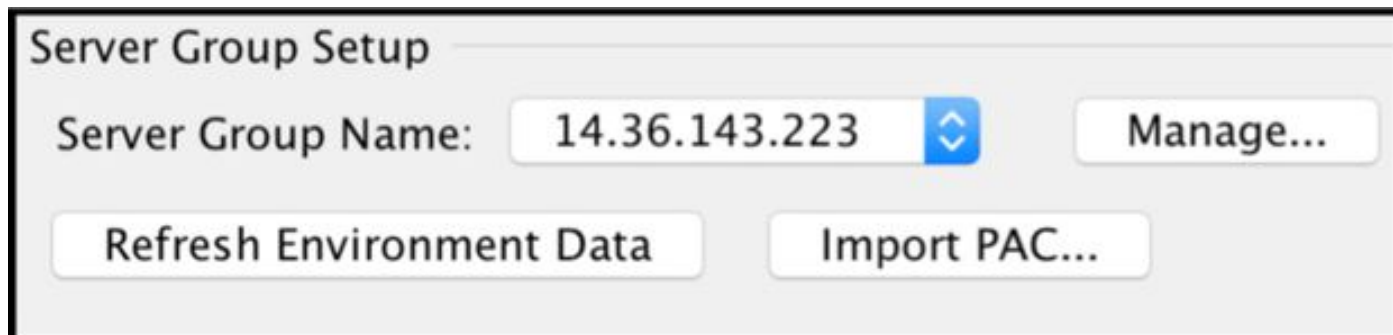
Test

- Nome do servidor ou endereço IP de Um ou Mais Servidores Cisco ICM NT: **Endereço IP de Um ou Mais Servidores Cisco ICM NT <ISE >**
- Porta da autenticação de servidor: **1812**
- Porta de relatório do server: **1813**
- Chave do segredo de servidor: **Cisc0123**
- Senha comum: **Cisc0123**

| | |
|-----------------------------|-------------------------------------|
| Server Group: | 14.36.143.223 |
| Interface Name: | outside |
| Server Name or IP Address: | 14.36.143.223 |
| Timeout: | 10 seconds |
| RADIUS Parameters | |
| Server Authentication Port: | 1812 |
| Server Accounting Port: | 1813 |
| Retry Interval: | 10 seconds |
| Server Secret Key: | •••••••• |
| Common Password: | •••••••• |
| ACL Netmask Convert: | Standard |
| Microsoft CHAPv2 Capable: | <input checked="" type="checkbox"/> |
| SDI Messages | |
| Message Table | |

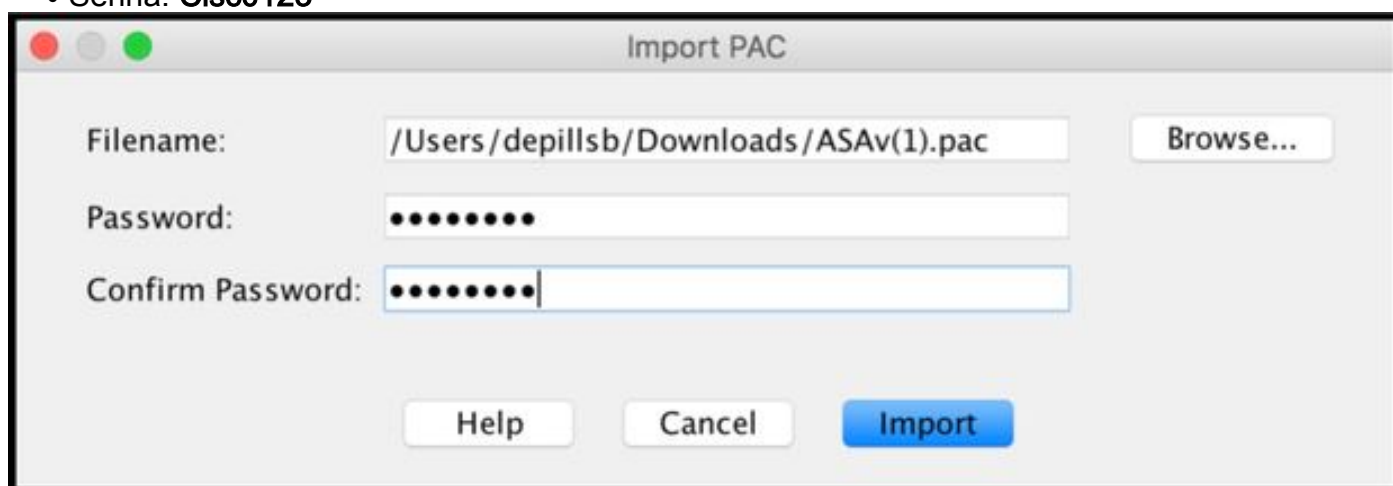
Importação PAC transferida do ISE

Configuração > Firewall > identidade por TrustSec > por grupo de servidor Setup > importação PAC...

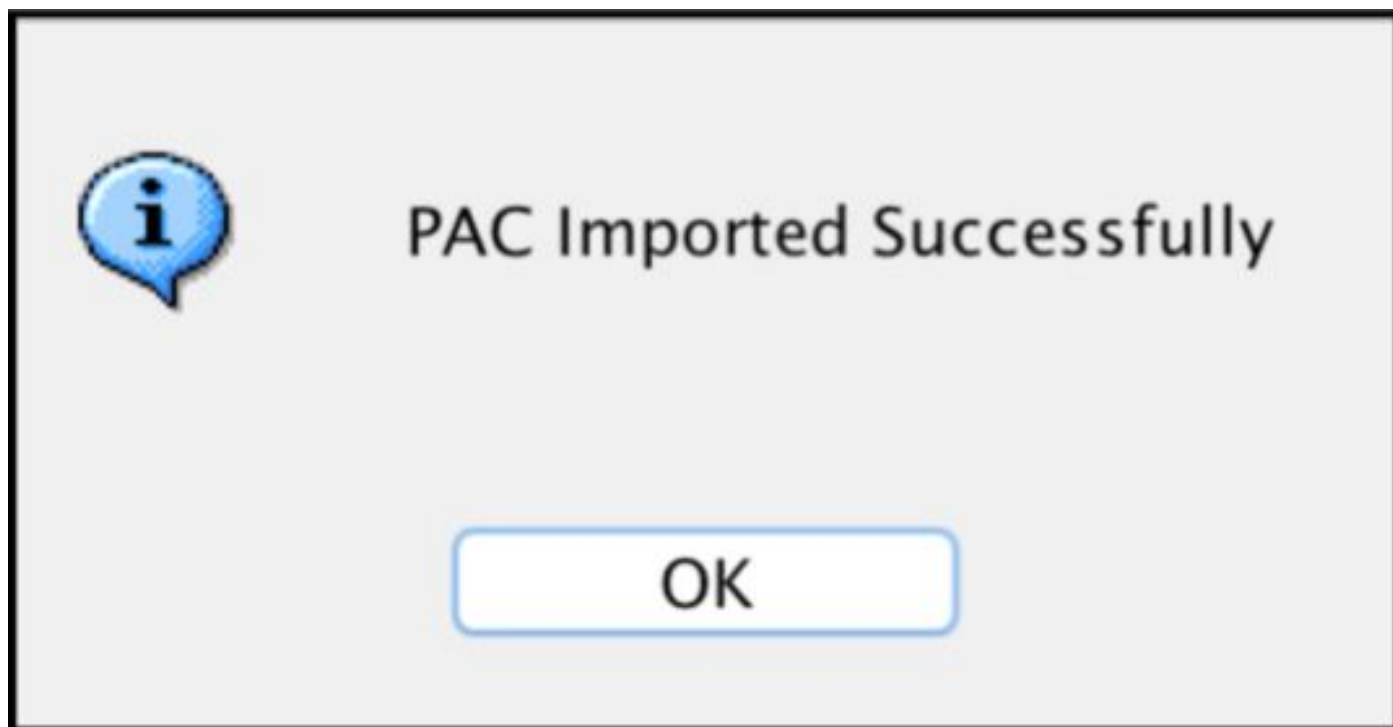


The screenshot shows the 'Server Group Setup' dialog box. It features a text field for 'Server Group Name' containing the IP address '14.36.143.223'. To the right of this field is a 'Manage...' button. Below the text field are two buttons: 'Refresh Environment Data' and 'Import PAC...'. The dialog has a title bar with the text 'Server Group Setup'.

- Senha: Cisc0123



The screenshot shows the 'Import PAC' dialog box. It has a title bar with the text 'Import PAC'. The dialog contains three input fields: 'Filename:' with the path '/Users/depillsb/Downloads/ASAv(1).pac' and a 'Browse...' button; 'Password:' with a masked field of ten dots; and 'Confirm Password:' with a masked field of ten dots. At the bottom, there are three buttons: 'Help', 'Cancel', and 'Import'.



Refresque dados do ambiente

A configuração > o Firewall > a identidade por TrustSec > por grupo de servidor Setup >

refrescam dados do ambiente

Server Group Setup

Server Group Name: 

Verificação

Logs vivos ISE

Operações > RAIO > logs vivos

| | | | | |
|---|---|------|--------------|------------------------------------|
|  |  | ASAv | #CTSREQUEST# | |
|  |  | ASAv | #CTSREQUEST# | NetworkDeviceAuthorization >> NDAC |

Authentication Details

| | |
|--------------------|---------------------------------------|
| Source Timestamp | 2017-07-30 00:05:53.432 |
| Received Timestamp | 2017-07-30 00:05:53.433 |
| Policy Server | ISE23 |
| Event | 5233 TrustSec Data Download Succeeded |
| Username | #CTSREQUEST# |
| Network Device | ASAv |
| Device Type | All Device Types |
| Location | All Locations |
| NAS IPv4 Address | 14.36.143.30 |
| NAS Port Type | Virtual |
| Security Group | TrustSec_Devices |
| Response Time | 33 milliseconds |

CiscoAVPair

```
cts-environment-data=ASAv,  
cts-environment-version=1,  
cts-device-capability=env-data-fragment,  
cts-pac-opaque=****,  
coa-push=true
```

Result

| | |
|---------------|--|
| State | ReauthSession:0e248dff2f27TfOfK10NeCx1yRhjPAO8_ssZ9U9VVy/o3dFT_tk |
| Class | CACS:0e248dff2f27TfOfK10NeCx1yRhjPAO8_ssZ9U9VVy/o3dFT_tk:ISE23/290687604/9 |
| cisco-av-pair | cts:server-list=CTSServerList1-0001 |
| cisco-av-pair | cts:security-group-tag=0002-02 |
| cisco-av-pair | cts:environment-data-expiry=86400 |
| cisco-av-pair | cts:security-group-table=0001-18 |

CiscoAVPair

cts-security-group-table=0001,
cts-pac-opaque=****,
coa-push=true

Result

| | |
|---------------|---|
| State | ReauthSession:0e248fdcf4PVaU72zvhHwsT3F4qpdgq4rMsifPkqEcQiG4O_YZw |
| Class | CACS:0e248fdcf4PVaU72zvhHwsT3F4qpdgq4rMsifPkqEcQiG4O_YZw:ISE23/290687604/10 |
| cisco-av-pair | cts:security-group-table=0001-18 |
| cisco-av-pair | cts:security-group-info=0-0-00-Unknown |
| cisco-av-pair | cts:security-group-info=ffff-1-00-ANY |
| cisco-av-pair | cts:security-group-info=9-0-00-Auditors |
| cisco-av-pair | cts:security-group-info=f-0-00-BYOD |
| cisco-av-pair | cts:security-group-info=5-0-00-Contractors |
| cisco-av-pair | cts:security-group-info=8-0-00-Developers |
| cisco-av-pair | cts:security-group-info=c-0-00-Development_Servers |
| cisco-av-pair | cts:security-group-info=4-0-00-Employees |
| cisco-av-pair | cts:security-group-info=6-2-00-Guests |
| cisco-av-pair | cts:security-group-info=3-0-00-Network_Services |
| cisco-av-pair | cts:security-group-info=e-0-00-PCI_Servers |
| cisco-av-pair | cts:security-group-info=a-0-00-Point_of_Sale_Systems |
| cisco-av-pair | cts:security-group-info=b-0-00-Production_Servers |
| cisco-av-pair | cts:security-group-info=7-0-00-Production_Users |
| cisco-av-pair | cts:security-group-info=ff-0-00-Quarantined_Systems |
| cisco-av-pair | cts:security-group-info=d-0-00-Test_Servers |
| cisco-av-pair | cts:security-group-info=2-2-00-TrustSec_Devices |
| cisco-av-pair | cts:security-group-info=10-0-00-Tester |


















Grupos de segurança ISE

Grupos do > segurança dos centros de trabalho > do TrustSec > dos componentes

Security Groups

For Policy Export go to [Administration > System > Backup & Restore > Policy Export Page](#)

 Edit  Add  Import  Export  Trash  Push

| <input type="checkbox"/> | Icon | Name  | SGT (Dec / Hex) | Description |
|--------------------------|---|--|-----------------|------------------------------------|
| <input type="checkbox"/> |  | Auditors | 9/0009 | Auditor Security Group |
| <input type="checkbox"/> |  | BYOD | 15/000F | BYOD Security Group |
| <input type="checkbox"/> |  | Contractors | 5/0005 | Contractor Security Group |
| <input type="checkbox"/> |  | Developers | 8/0008 | Developer Security Group |
| <input type="checkbox"/> |  | Development_Servers | 12/000C | Development Servers Security Group |
| <input type="checkbox"/> |  | Employees | 4/0004 | Employee Security Group |
| <input type="checkbox"/> |  | Guests | 6/0006 | Guest Security Group |
| <input type="checkbox"/> |  | Network_Services | 3/0003 | Network Services Security Group |
| <input type="checkbox"/> |  | PCI_Servers | 14/000E | PCI Servers Security Group |
| <input type="checkbox"/> |  | Point_of_Sale_Systems | 10/000A | Point of Sale Security Group |
| <input type="checkbox"/> |  | Production_Servers | 11/000B | Production Servers Security Group |
| <input type="checkbox"/> |  | Production_Users | 7/0007 | Production User Security Group |
| <input type="checkbox"/> |  | Quarantined_Systems | 255/00FF | Quarantine Security Group |
| <input type="checkbox"/> |  | Tester | 16/0010 | |
| <input type="checkbox"/> |  | Test_Servers | 13/000D | Test Servers Security Group |
| <input type="checkbox"/> |  | TrustSec_Devices | 2/0002 | TrustSec Devices Security Group |

ASDM PAC

Monitoração > propriedades > identidade por TrustSec > por PAC

PAC Information:

Valid until: **Jan 30 2018 05:46:44**
AID: 6f5719523570b8d229f23073404e2d37
I-ID: ASAv
A-ID-Info: ISE 2.2p1
PAC-type: Cisco Trustsec

PAC Opaque:

```
000200b000030001000400106f5719523570b8d229f23073404e2d3700060094000301  
00359249c4dd61484890f29bbe81859edb00000013597a55c100093a803f883e4ddafa  
d162ae02fac03da08f9424cb323fa8aaeae44c6d6d7db3659516132f71b25aa5be3f38  
9b76fdbbc1216d1d14e689ebb36d7344a5166247e950bbf62a370ea8fc941fa1d6c4ce5  
9f438e787052db75a4e45ff2f0ab8488dfdd887a02119cc0c4174fc234f33d9ee9f9d4  
dad759e9c8
```

Dados e grupos de segurança do ambiente ASDM

Monitoração > propriedades > identidade por TrustSec > por dados do ambiente

Environment Data:

Status: Active
Last download attempt: Successful
Environment Data Lifetime: 86400 secs
Last update time: 21:07:01 UTC Jul 29 2017
Env-data expires in: 0:21:39:07 (dd:hr:mm:sec)
Env-data refreshes in: 0:21:29:07 (dd:hr:mm:sec)

Security Group Table:

Valid until: 21:07:01 UTC Jul 30 2017
Total entries: 18

| Name | Tag | Type |
|-----------------------|-------|---------|
| ANY | 65535 | unicast |
| Auditors | 9 | unicast |
| BYOD | 15 | unicast |
| Contractors | 5 | unicast |
| Developers | 8 | unicast |
| Development_Servers | 12 | unicast |
| Employees | 4 | unicast |
| Guests | 6 | unicast |
| Network_Services | 3 | unicast |
| PCI_Servers | 14 | unicast |
| Point_of_Sale_Systems | 10 | unicast |
| Production_Servers | 11 | unicast |
| Production_Users | 7 | unicast |
| Quarantined_Systems | 255 | unicast |
| Test_Servers | 13 | unicast |
| Tester | 16 | unicast |
| TrustSec_Devices | 2 | unicast |
| Unknown | 0 | unicast |

Configuração ASDM SXP

Permita SXP

A configuração > o Firewall > a identidade por TrustSec > permitem o protocolo de intercâmbio SGT (SXP)

Enable SGT Exchange Protocol (SXP)

Ajuste a senha do endereço IP de origem do padrão SXP e do padrão SXP

Configuração > Firewall > identidade por TrustSec > por pares da conexão

| | |
|-------------------|---|
| Default Source: | <input type="text" value="14.36.143.30"/> |
| Default Password: | <input type="password" value="●●●●●●●●"/> |
| Confirm Password: | <input type="password" value="●●●●●●●●"/> |

Adicionar o par SXP

A configuração > o Firewall > a identidade por TrustSec > por conexão espreitam > Add

| Connection Peers | | | | |
|------------------|-------------------|----------|------|------|
| Peer IP Address | Source IP Address | Password | Mode | Role |
| | | | | |

Filter: Peer IP Address Filter Clear

Add Edit Delete

- Endereço IP do peer: **Endereço IP de Um ou Mais Servidores Cisco ICM NT <ISE >**

| | |
|------------------|--|
| Peer IP Address: | <input type="text" value="14.36.143.223"/> |
| Password: | <input type="text" value="Default"/> |
| Mode: | <input type="text" value="Local"/> |
| Role: | <input type="text" value="Listener"/> |

Configuração ISE SXP

Configuração de senha global SXP

WorkCenters > TrustSec > ajustes > ajustes SXP

- Senha global: Cisc0123

SXP Settings

- Publish SXP bindings on PxGrid
- Add radius mappings into SXP IP SGT mapping table

Global Password

Global Password

This global password will be overridden by the device specific password

Adicionar o dispositivo SXP

WorkCenters > TrustSec > Dispositivos > Adicionar SXP > SXP

▼ Add Single Device

Input fields marked with an asterisk (*) are required.

name

IP Address *

Peer Role *

Connected PSNs *

SXP Domain *

Status *

Password Type *

Password

Version *

► Advanced Settings

Verificação SXP

Verificação ISE SXP

WorkCenters > TrustSec > dispositivos SXP > SXP

SXP Devices

0 Selected Rows/Page / 1 Total Rows

| <input type="checkbox"/> | Name | IP Address | Status | Peer Role | Pass... | Negoti... | SX... | Connected To | Duration [d... | SXP Domain |
|--------------------------|------|--------------|--------|-----------|---------|-----------|-------|--------------|----------------|------------|
| <input type="checkbox"/> | ASAv | 14.36.143.30 | ON | LISTENER | DEFAULT | V3 | V4 | ISE23 | 00:00:00:02 | default |

Mapeamentos ISE SXP

WorkCenters > TrustSec > SXP > todos os mapeamentos SXP

Refresh Add SXP Domain filter Manage SXP Domain filters

| IP Address | SGT | Learned From | Learned By | SXP Domain | PSNs Involved |
|-------------------|---------------------------|---------------|------------|------------|---------------|
| 10.122.158.253/32 | Guests (6/0006) | 14.36.143.223 | Local | default | ISE23 |
| 10.122.160.93/32 | Guests (6/0006) | 14.36.143.223 | Local | default | ISE23 |
| 10.122.165.49/32 | Employees (4/0004) | 14.36.143.223 | Local | default | ISE23 |
| 10.122.165.58/32 | Guests (6/0006) | 14.36.143.223 | Local | default | ISE23 |
| 14.0.69.220/32 | Guests (6/0006) | 14.36.143.223 | Local | default | ISE23 |
| 14.36.143.99/32 | Employees (4/0004) | 14.36.143.223 | Local | default | ISE23 |
| 14.36.143.105/32 | TrustSec_Devices (2/0002) | 14.36.143.223 | Local | default | ISE23 |
| 14.36.147.70/32 | Employees (4/0004) | 14.36.143.223 | Local | default | ISE23 |
| 172.18.250.123/32 | Employees (4/0004) | 14.36.143.223 | Local | default | ISE23 |
| 192.168.1.0/24 | Contractors (5/0005) | 14.36.143.223 | Local | default | ISE23 |

Verificação ASDM SXP

Monitoração > propriedades > identidade por TrustSec > por conexões SXP

SGT Exchange Protocol (SXP) Connections:

SXP: Enabled
 Highest version: 3
 Default password: Set
 Default local IP: 14.36.143.30
 Reconcile period: 120 secs
 Retry open period: 120 secs
 Retry open timer: Not Running
 Total number of SXP connections: 1
 Total number of SXP connections shown: 1

Peer Connection Status:

Filter: Peer IP Address ...

| Peer | Source | Status | Version | Role | Instance # | Password | Reconcile Timer | Delete Hold-down Timer | Last Changed |
|---------------|--------------|--------|---------|----------|------------|----------|-----------------|------------------------|--------------------------|
| 14.36.143.223 | 14.36.143.30 | On | 3 | Listener | 1 | Default | Not Running | Not Running | 0:00:22:56 (dd:hr:mm:se) |

IP instruído ASDM SXP aos mapeamentos SGT

Monitoração > propriedades > identidade por TrustSec > por mapeamentos IP

Security Group IP Mapping Table:

Total number of Security Group IP Mappings: 10

Total number of Security Group IP Mappings shown: 10

Filter:

TAG



| Tag | Name | IP Address |
|-----|------------------|----------------|
| 4 | Employees | 14.36.143.99 |
| 6 | Guests | 10.122.158.253 |
| 6 | Guests | 10.122.160.93 |
| 4 | Employees | 14.36.147.70 |
| 2 | TrustSec_Devices | 14.36.143.105 |
| 4 | Employees | 172.18.250.123 |
| 4 | Employees | 10.122.165.49 |
| 6 | Guests | 14.0.69.220 |
| 6 | Guests | 10.122.165.58 |
| 5 | Contractors | 192.168.1.0/24 |

Captura de pacote de informação tomada no ISE

| | | | | | | | | | | | | | | | | |
|------|----------|---------------|---------------|------|-----|-------|---|-------|-----------------------|--------|-----------|-----------|-------|----------|-------------|------|
| 2060 | 0.000000 | 14.36.143.223 | 14.36.143.30 | TCP | 86 | 25982 | - | 64999 | [SYN] | Seq=0 | Win=29200 | Len=0 | MD5 | MSS=1460 | SACK_PERM=1 | WS=1 |
| 2061 | 0.000782 | 14.36.143.30 | 14.36.143.223 | TCP | 78 | 64999 | - | 25982 | [SYN, ACK] | Seq=0 | Ack=1 | Win=32768 | Len=0 | MSS=1460 | MD5 | |
| 2062 | 0.000039 | 14.36.143.223 | 14.36.143.30 | TCP | 74 | 25982 | - | 64999 | [ACK] | Seq=1 | Ack=1 | Win=29200 | Len=0 | MD5 | | |
| 2074 | 0.039078 | 14.36.143.223 | 14.36.143.30 | SMPP | 102 | | | | SMPP Bind_receiver | | | | | | | |
| 2075 | 0.000522 | 14.36.143.30 | 14.36.143.223 | TCP | 74 | 64999 | - | 25982 | [ACK] | Seq=1 | Ack=29 | Win=32768 | Len=0 | MD5 | | |
| 2076 | 0.000212 | 14.36.143.30 | 14.36.143.223 | SMPP | 90 | | | | SMPP Bind_transmitter | | | | | | | |
| 2077 | 0.000024 | 14.36.143.223 | 14.36.143.30 | TCP | 74 | 25982 | - | 64999 | [ACK] | Seq=29 | Ack=17 | Win=29200 | Len=0 | MD5 | | |
| 2085 | 0.008444 | 14.36.143.223 | 14.36.143.30 | SMPP | 311 | | | | SMPP Query_sm | | | | | | | |
| 2086 | 0.000529 | 14.36.143.30 | 14.36.143.223 | TCP | 74 | 64999 | - | 25982 | [ACK] | Seq=17 | Ack=266 | Win=32768 | Len=0 | MD5 | | |