Configurazione di TrustSec SXP tra ISE e ASAv

Sommario

Introduzione

In questo documento viene descritto come configurare una connessione SXP (Security Group Exchange Protocol) tra ISE (Identity Services Engine) e ASAv (Virtual Adaptive Security Appliance).

SXP è il protocollo SGT (Security Group Tag) Exchange utilizzato da TrustSec per propagare i mapping IP-SGT ai dispositivi TrustSec. SXP è stato sviluppato per consentire alle reti, inclusi i dispositivi di terze parti o i dispositivi Cisco legacy che non supportano il tagging in linea SGT, di avere funzionalità TrustSec. SXP è un protocollo peer, un dispositivo funge da altoparlante e l'altro da listener. Il diffusore SXP è responsabile dell'invio dei binding IP-SGT e il listener è responsabile della raccolta di tali binding. La connessione SXP utilizza la porta TCP 64999 come protocollo di trasporto sottostante e MD5 per l'integrità/autenticità dei messaggi.

SXP è stato pubblicato come bozza IETF al seguente collegamento:

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

Prerequisiti

Requisiti

Matrice di compatibilità TrustSec:

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

Componenti usati
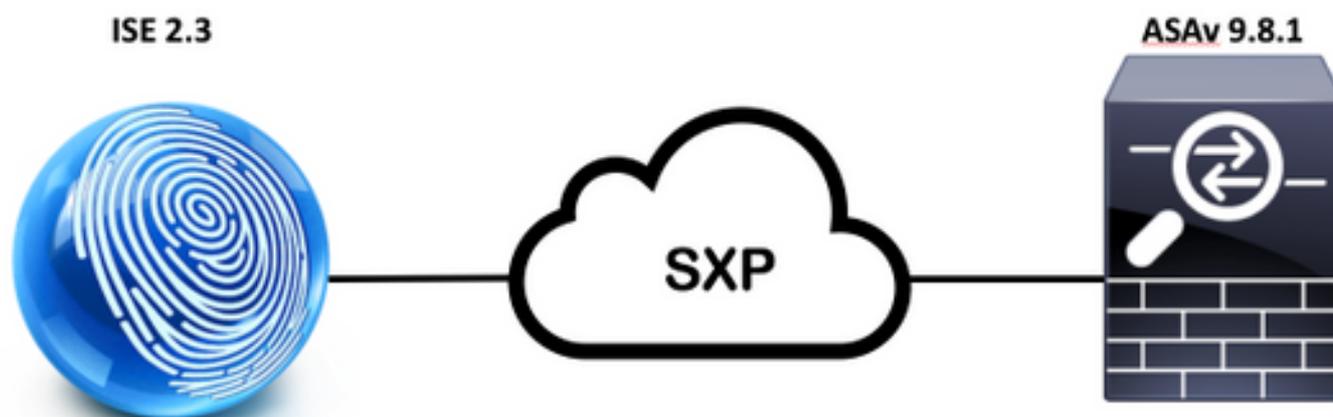
ISE 2.3

ASA v 9.8.1

ASDM 7.8.1.150

Esempio di rete

Indirizzi IP

ISE: 14.36.143.223

ASAv: 14.36.143.30

Configurazione iniziale

dispositivi di rete ISE

Registrazione di un'appliance ASA come dispositivo di rete

Centri di lavoro > TrutSec > Componenti > Dispositivi di rete > **Aggiungi**

Genera PAC fuori banda (OOB) (Credenziale di accesso protetto) e scarica

Configurazione server ASDM AAA

Crea gruppo server AAA

Configurazione > Firewall > Identity by TrustSec > Impostazione gruppo server > **Gestisci...**

Gruppi di server AAA > **Aggiungi**

- Gruppo server AAA: **<Nome gruppo>**
- **Abilita autorizzazione dinamica**

AAA Server Group: 14.36.143.223

Protocol: RADIUS

Realm-id: 1

Accounting Mode: ○ Simultaneous ● Single

Reactivation Mode: ● Depletion ○ Timed

Dead Time: 10 minutes

Max Failed Attempts: 3

☐ Enable interim accounting update

☐ Update Interval: 24 Hours

☐ Enable Active Directory Agent mode

ISE Policy Enforcement

☑ Enable dynamic authorization

Dynamic Authorization Port: 1700

☐ 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

Help   Cancel   OK

Aggiungi server al gruppo di server

Server nel gruppo selezionato > **Aggiungi**

- Nome server o indirizzo IP: **<ISE IP address>**
- Porta di autenticazione server: **1812**
- Porta accounting server: **1813**
- Chiave privata server: **Cisco 1023**
- Password comune: **Cisco 1023**

Importazione PAC scaricata da ISE

Configurazione > Firewall > Identity by TrustSec > Impostazione gruppo server > **Importa PAC...**
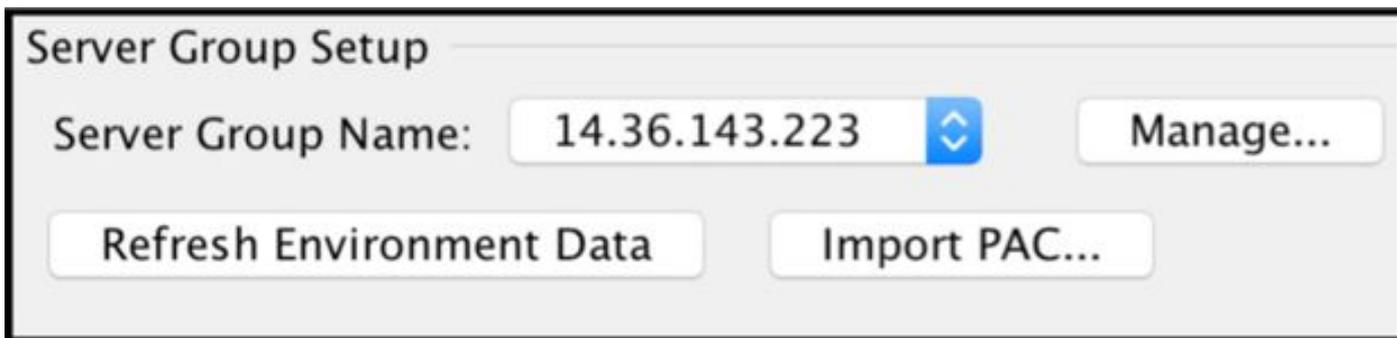
- Password: **Cisco 1023**
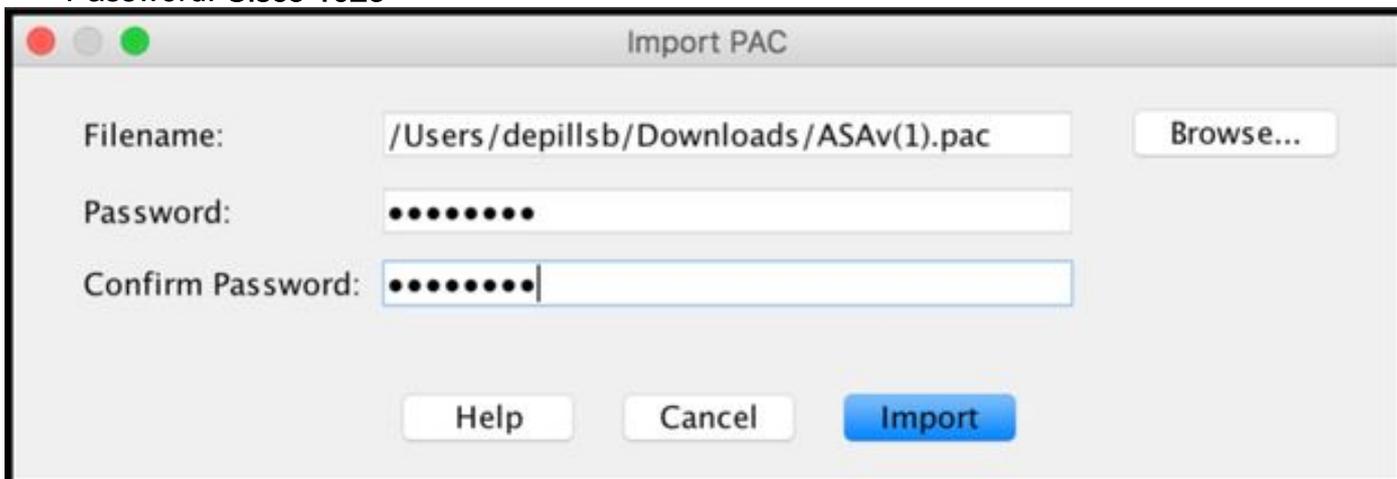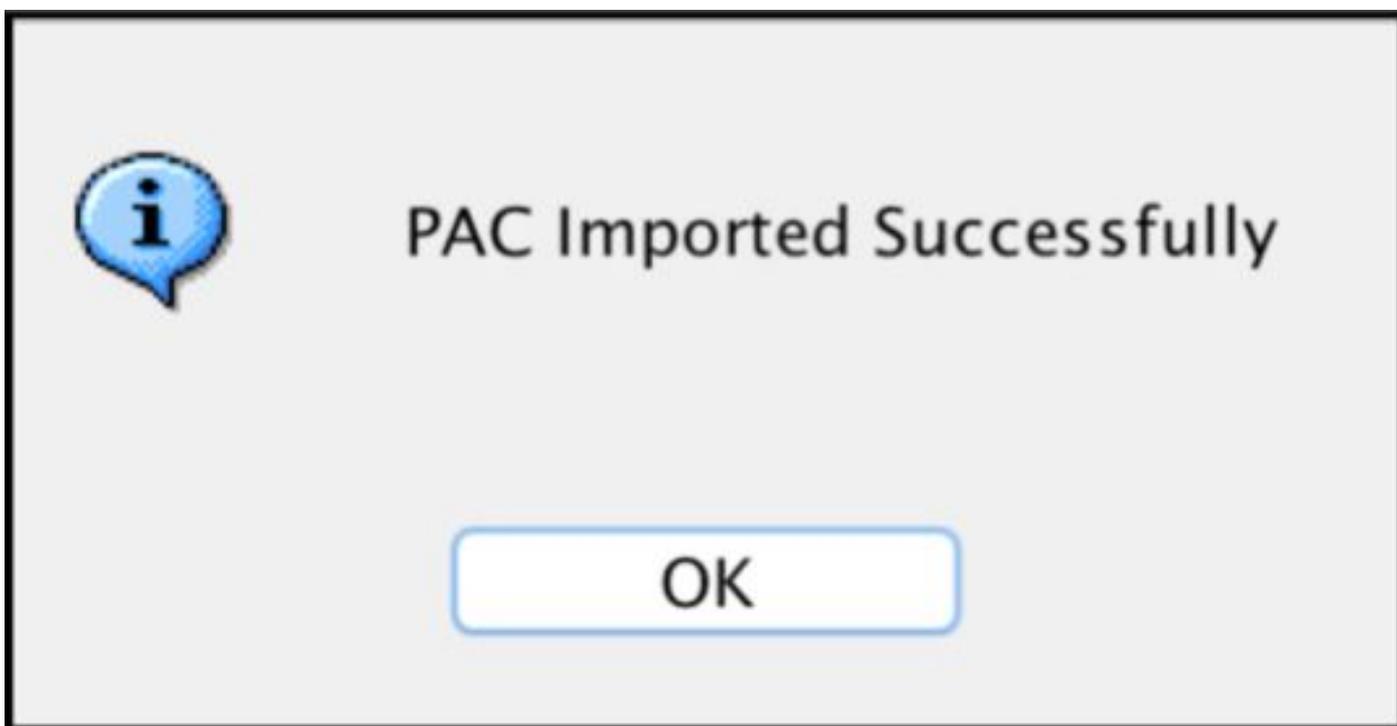
Aggiorna dati ambiente

Configurazione > Firewall > Identity by TrustSec > Impostazione gruppo server > **Aggiorna dati ambiente**

Verifica

log ISE in tempo reale

Operazioni > RADIUS > **Registri attivi**

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:0e248fdff2I7TiOfK10NeCx1yRhjPAO8_ssZ9U9VVy/o3dfT_tk
Class	CACS:0e248fdff2I7TiOfK10NeCx1yRhjPAO8_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:0e248fdfc4PVaU72zvhHwsT3F4qpdgq4rMsifPkqEcQiG4O_YZw
Class	CACS:0e248fdfc4PVaU72zvhHwsT3F4qpdgq4rMsifPkqEcQiG4O_YZw:ISE23/29 0687604/10
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

Gruppi di sicurezza ISE

Centri di lavoro > TrustSec > Componenti > **Gruppi di sicurezza**

Security Groups
For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

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

PAC ASDM

Monitoraggio > Proprietà > Identità per TrustSec > **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
9b76fdbc1216d1d14e689ebb36d7344a5166247e950bbf62a370ea8fc941fa1d6c4ce5
9f438e787052db75a4e45ff2f0ab8488dfdd887a02119cc0c4174fc234f33d9ee9f9d4
dad759e9c8

Dati di ambiente e gruppi di sicurezza ASDM

Monitoraggio > Proprietà > Identità per TrustSec > **Dati 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

Configurazione ASDM SXP

Attiva SXP

Configurazione > Firewall > Identity by TrustSec > **Abilita SGT Exchange Protocol (SXP)**

✓ Enable SGT Exchange Protocol (SXP)

Impostare l'indirizzo IP di origine SXP predefinito e la password SXP predefinita

Configurazione > Firewall > Identity by TrustSec > **Peer di connessione**

Default Source:	14.36.143.30
Default Password:	●●●●●●●●
Confirm Password:	●●●●●●●●

Aggiungi peer SXP

Configurazione > Firewall > Identity by TrustSec > Peer di connessione > **Aggiungi**

Connection Peers
Filter: Peer IP Address   [ ]   Filter   Clear

Peer IP Address	Source IP Address	Password	Mode	Role		
					Add	
					Edit	
					Delete	

- Indirizzo IP peer: **<Indirizzo IP ISE>**

Peer IP Address:	14.36.143.223
Password:	Default
Mode:	Local
Role:	Listener

Configurazione ISE SXP

Impostazione password SXP globale

Centri di lavoro > TrustSec > Impostazioni > **Impostazioni SXP**

- Password globale: **Cisco 1023**

Aggiungi dispositivo SXP

Centri di lavoro > TrustSec > SXP > Dispositivi SXP > **Aggiungi**

Verifica SXP

Verifica ISE SXP

Centri di lavoro > TrustSec > SXP > **Dispositivi SXP**

Mapping ISE SXP

Centri di lavoro > TrustSec > SXP > **Tutti i mapping SXP**

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

Verifica ASDM SXP

Monitoraggio > Proprietà > Identity by TrustSec > **Connessioni 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                                              ...   Filter   Clear

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
```

ASDM ha appreso i mapping da IP SXP a SGT

Monitoraggio > Proprietà > Identità per TrustSec > **Mapping 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

Acquisizione del pacchetto effettuata ad 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