Cisco ISE TrustSec modello Allow-List (Default Deny IP) con SDA

Sommario

Introduzione

In questo documento viene descritto come abilitare il modello allow-list (Default Deny IP) di TrustSec in SDA (Software Defined Access). Questo documento riguarda diverse tecnologie e componenti, tra cui Identity Services Engine (ISE), Digital Network Architecture Center (DNAC) e switch (Border and Edge).

Sono disponibili due modelli Trustsec:

- Modello elenco indirizzi non consentiti (predefinito): In questo modello, l'azione predefinita è Autorizza IP e qualsiasi restrizione deve essere configurata esplicitamente con l'utilizzo degli elenchi di accesso ai gruppi di sicurezza (SGACL). Questa opzione viene in genere utilizzata quando non si ha una conoscenza completa dei flussi di traffico all'interno della rete. Questo modello è abbastanza semplice da implementare.

- Modello elenco indirizzi consentiti (predefinito Nega IP): In questo modello, l'azione predefinita è Deny IP (Nega IP), quindi il traffico richiesto deve essere autorizzato esplicitamente con l'uso di SGACL. Questa opzione viene in genere utilizzata quando il cliente ha una comprensione adeguata del tipo di traffico all'interno della rete. Questo modello richiede uno studio dettagliato del traffico del control plane e ha la capacità di bloccare TUTTO il traffico nel momento in cui viene attivato.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Autenticazione Dot1x/MAB
- CTS (Cisco TrustSec)
- Protocollo SXP (Security Exchange Protocol)
- Proxy Web
- Concetti sul firewall
- DNAC

Componenti usati

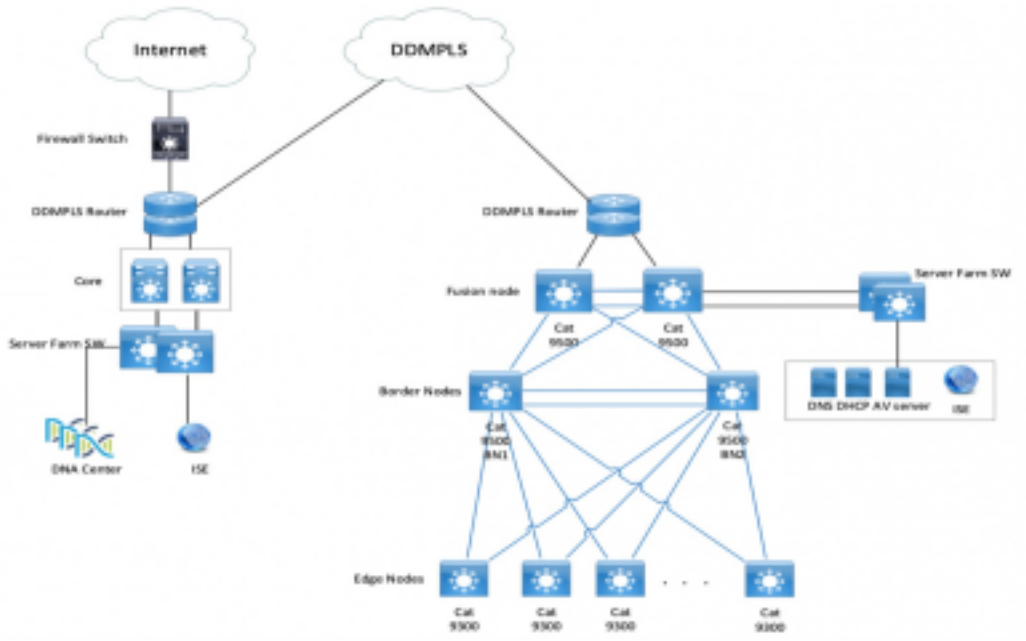
Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Nodi di bordo 9300 Edge e 9500 (switch) con IOS 16.9.3
- DNAC 1.3.0.5
- ISE 2.6 patch 3 (installazione ridondante su due nodi)
- DNAC e ISE sono integrati
- Il provisioning dei nodi Border e Edge viene eseguito da DNAC
- Il tunnel SXP viene stabilito dall'ISE (altoparlante) a entrambi i nodi di confine (listener)
- I pool di indirizzi IP vengono aggiunti all'onboarding dell'host

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

Esempio di rete



Configurazione

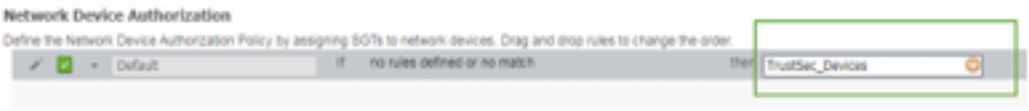
Di seguito viene riportata la procedura per abilitare il modello dell'elenco indirizzi consentiti (IP di negazione predefinito):

1. Cambiare il SGT degli switch da Sconosciuto a Dispositivi TrustSec.
2. Disabilita l'imposizione basata sul ruolo CTS.
3. Mappatura IP-SGT sugli switch Border and Edge con modello DNAC.
4. SGACL di fallback con modello DNAC.
5. Abilitare Allow-List (Default Deny IP) nella matrice trustsec.
6. Creare SGT per endpoint/utenti.
7. Creare SGACL per endpoint/utenti (per il traffico di sovrapposizione produzione).

Passaggio 1. Cambiare il SGT degli switch da Sconosciuto a Dispositivi TrustSec.

Per impostazione predefinita, il tag del gruppo di sicurezza (SGT) sconosciuto è configurato per l'autorizzazione dei dispositivi di rete. Modificandolo in TrustSec Device SGT si ottiene maggiore visibilità e si contribuisce a creare SGACL specifico per il traffico avviato dallo switch.

Passare a **Centri di lavoro > TrustSec > Criteri trustsec > Autorizzazione dispositivo di rete** e quindi modificarlo in Trustsec_Devices da Sconosciuto



Passaggio 2. Disabilitare l'applicazione basata sui ruoli CTS.

- Dopo aver attivato il modello Allow-List (Default Deny), tutto il traffico viene bloccato nell'infrastruttura, inclusi il traffico multicast e broadcast di base, ad esempio il traffico IS-IS (Intermediate System-to-Intermediate System), BFD (Bidirectional Forwarding Detection) e SSH (Secure Shell).

- Tutte le porte TenGig che si connettono al bordo della struttura e al bordo devono essere configurate con il comando qui. A questo punto, il traffico proveniente da questa interfaccia e proveniente da questa interfaccia non sono soggetti a misure di applicazione.

```
Interface tengigabitethernet 1/0/1

no cts role-based enforcement
```

> **Nota:** Per semplificare questa operazione, è possibile utilizzare un modello di intervallo in DNAC. In caso contrario, per ogni switch, l'operazione deve essere eseguita manualmente durante il provisioning. Lo snippet di codice seguente illustra come eseguire questa operazione tramite un modello DNAC.

```
interface range $uplink1

no cts role-based enforcement
```

Per ulteriori informazioni sui modelli DNAC, *fare riferimento a* questo URL per il documento.

https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/1-2-1/user_guide/b_dnac_ug_1_2_1/b_dnac_ug_1_2_chapter_010000.html

Passaggio 3. Mappatura IP-SGT sugli switch per bordi e bordi con modello DNAC.

L'idea è quella di rendere disponibile la mappatura IP-SGT locale sugli switch anche se l'ISE viene disabilitata completamente. Ciò garantisce l'operatività del sottosistema e l'integrità della connettività alle risorse critiche

Il primo passo è quello di associare i servizi critici a un SGT (ad esempio - Basic_Network_Services/1000). Alcuni di questi servizi includono:

- Subnet Underlay/ISIS
- ISE/DNAC
- Strumento di monitoraggio
- Subnet AP in caso di OTT
- Server terminal
- Servizi Critici, Ad Esempio: Telefono IP

Esempio:

```
cts role-based sgt-map <ISE/DNAC Subnet> sgt 1000

cts role-based sgt-map  sgt 2

cts role-based sgt-map <Wireless OTT Infra> sgt 1000

cts role-based sgt-map <Underlay OTT AP Subnet> sgt 2

cts role-based sgt-map <Monitoring Tool IP> sgt 1000

cts role-based sgt-map vrf CORP_VN <Voice Gateway and CUCM Subnet> sgt 1000
```

Passaggio 4. SGACL di fallback con modello DNAC.

Una mappatura SGT non è utile finché non viene creato un SGACL rilevante utilizzando il SGT. Pertanto, il passo successivo consiste nella creazione di un SGACL che agisca come Fallback locale in caso di interruzione dei nodi ISE (quando i servizi ISE sono inattivi, il tunnel SXP si blocca e quindi i SGACL e la mappatura IP SGT non vengono scaricati in modo dinamico).

Push di questa configurazione su tutti i nodi Edge e Border.

ACL/contratto basati su ruoli di fallback:

```
ip access-list role-based FALLBACK

permit ip
```

TrustSec dispositivi per trustSec:

```
cts role-based permissions from 2 to 2 FALLBACK
```

Sopra SGACL Garantire la comunicazione all'interno di switch fabric e IP sottostanti

TrustSec Devices to SGT 1000:

```
cts role-based permissions from 2 to 1000 FALLBACK
```

Sopra SGACL Garantire la comunicazione tra switch e punti di accesso a ISE, DNAC, WLC e strumenti di monitoraggio

Da SGT 1000 a TrustSec Dispositivi:

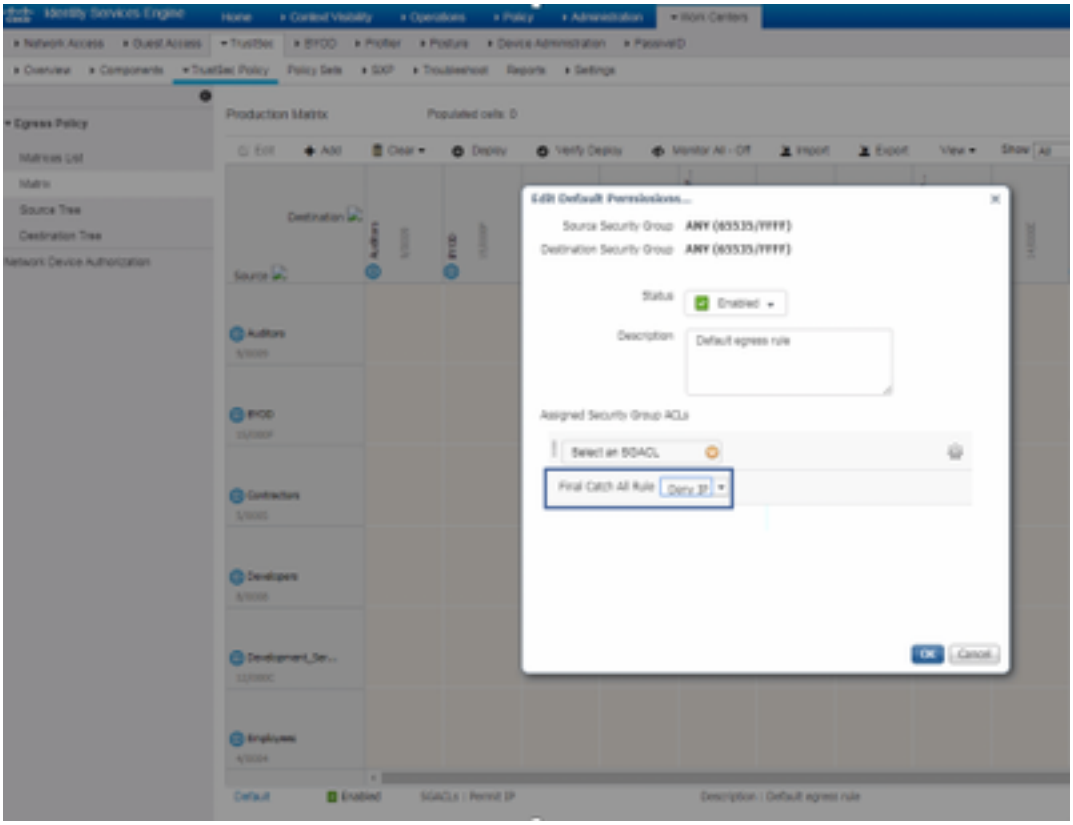
```
cts role-based permissions from 1000 to 2 FALLBACK
```

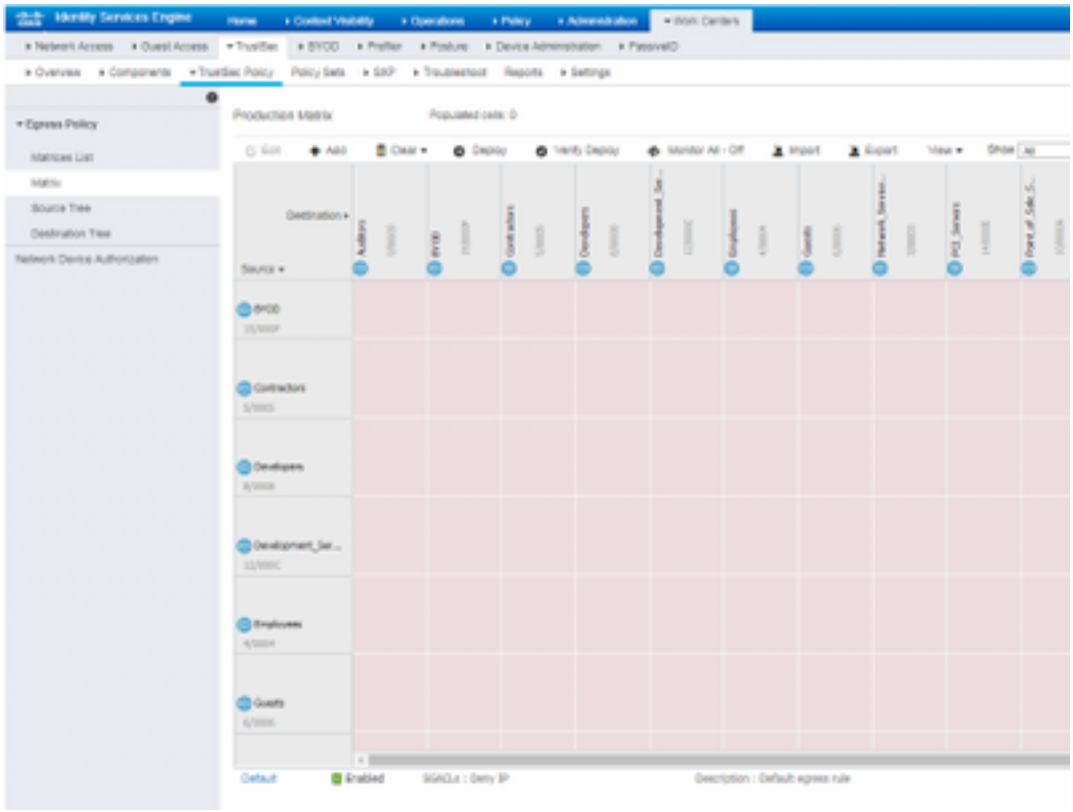
Sopra SGACL Garantire la comunicazione dai punti di accesso agli strumenti ISE, DNAC, WLC e monitoraggio sugli switch

Passaggio 5. Abilitare il modello Allow-List (Default Deny) nella matrice TrustSec.

L'esigenza è quella di negare la maggior parte del traffico sulla rete e permettere una quantità inferiore. Se si utilizza la negazione predefinita con regole di autorizzazione esplicite, è necessario un numero inferiore di criteri.

Passare a **Centri di lavoro > TrustSec > Criteri TrustSec > Matrice > Predefinito** e modificarlo in **Nega tutto** nella regola catch finale.





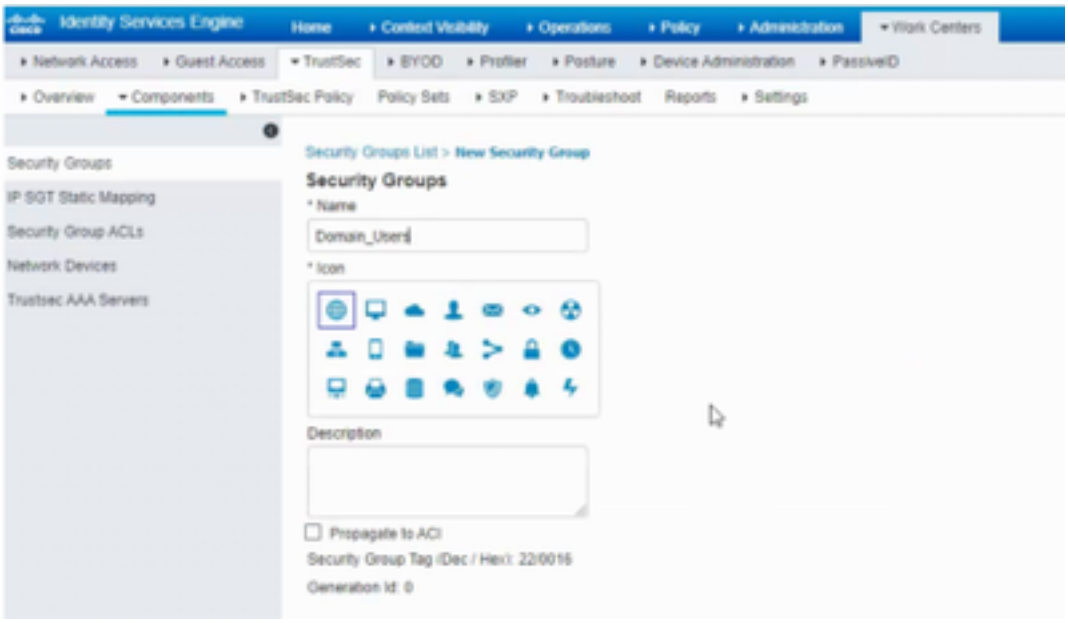
Nota: L'immagine rappresenta (per impostazione predefinita, tutte le colonne sono in rosso), il valore di Rifiuto predefinito è stato abilitato e dopo la creazione di SGACL è possibile autorizzare solo il traffico selettivo.

Passaggio 6. Creare SGT per endpoint/utenti.

In ambiente SDA, il nuovo SGT deve essere creato solo dalla GUI DNAC, poiché si verificano

numerosi casi di danneggiamento del database a causa della mancata corrispondenza del database SGT in ISE/DNAC.

Per creare SGT, accedere a **DNAC > Policy > Group-Based Access Control > Scalable Groups > Add Groups**, una pagina reindirizza l'utente a **ISE Scalable Group**, fare clic su **Add**, immettere il nome SGT e salvarlo.



Lo stesso SGT si riflette in DNAC attraverso l'integrazione PxGrid. Questa è la stessa procedura per la creazione futura di SGT.

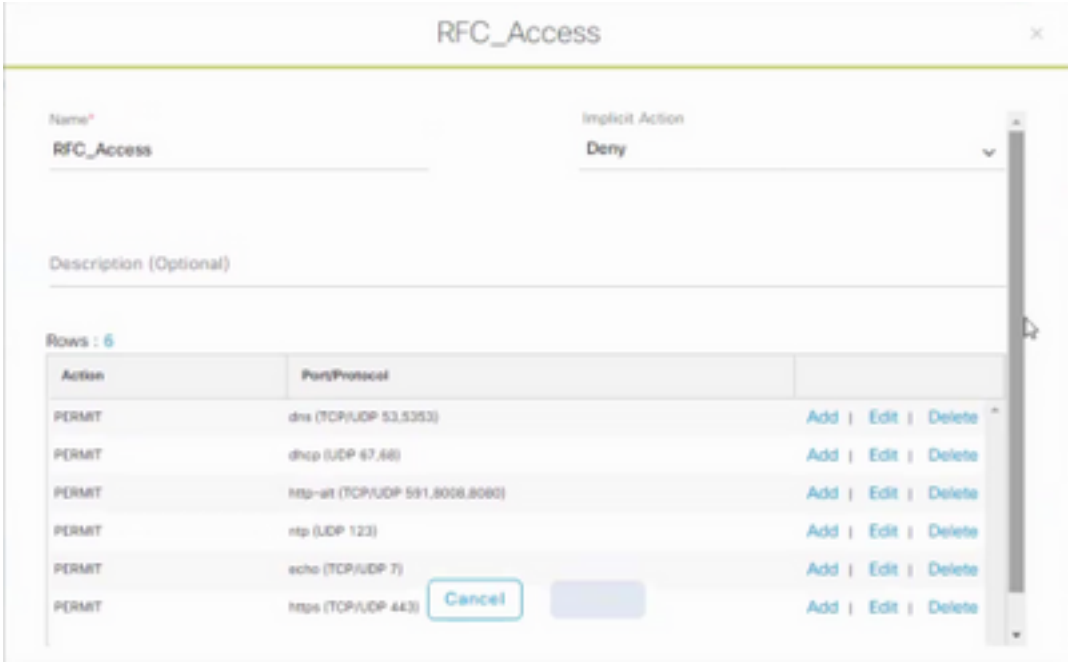
Passaggio 7. Creare SGACL per endpoint/utenti (per il traffico di sovrapposizione produzione).

In ambiente SDA, il nuovo SGT deve essere creato solo dalla GUI DNAC.

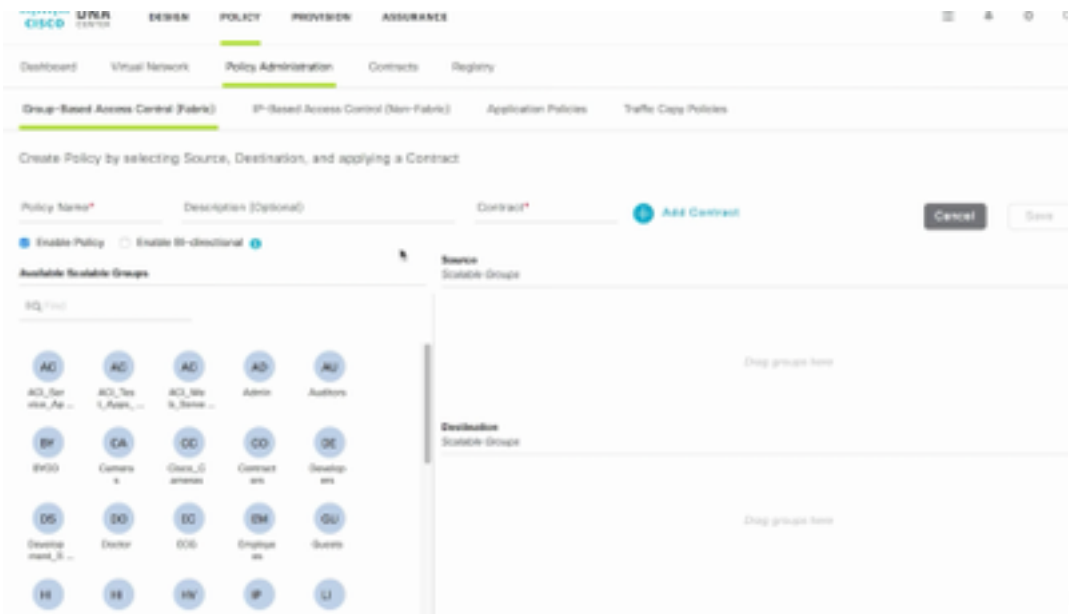
```
Policy Name: Domain_Users_Access

Contract : Permit

Enable Policy :

Enable Bi-Directional :

Source SGT : Domain Users (Drag from Available Security Group)

Destination SGT: Domain_Users, Basic_Network_Services, DC_Subnet, Unknown (Drag from Available
Security Group)


Policy Name: RFC_Access

Contract : RFC_Access (This Contract contains limited ports)

Enable Policy :

Enable Bi-Directional :

Source SGT : Domain Users (Drag from Available Security Group)
```

```
Destination SGT: RFC1918 (Drag from Available Security Group)
```

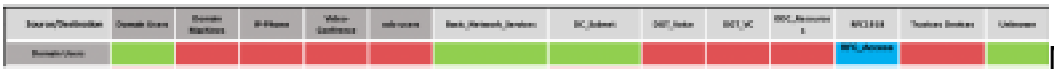
Per creare un **contratto**, accedere a **DNAC** e selezionare **Criteri > Contratti > Aggiungi contratti > Aggiungi protocollo richiesto** e quindi fare clic su **Salva**.



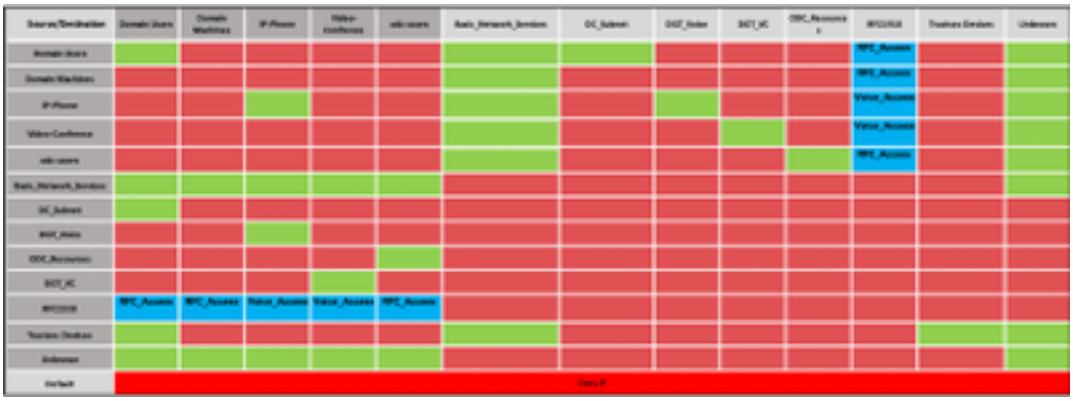
Per creare un contratto, accedere a **DNAC** e selezionare **Criteri > Controllo di accesso basato su gruppo > Criteri di accesso basati su gruppo > Aggiungi criteri > Crea criteri (con le informazioni specificate)**. Fare clic su **Salva** e quindi su **Distribuisci**.

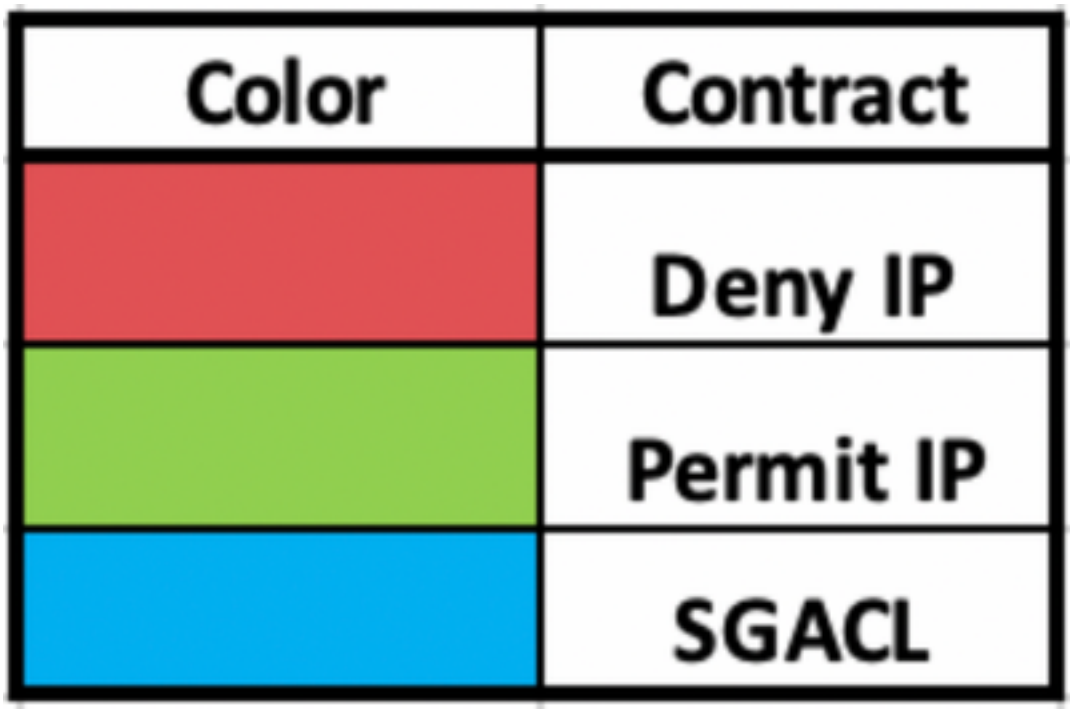


Una volta configurato da DNAC, SGACL/Contract si riflette automaticamente in ISE. Di seguito è riportato un esempio di vista matrice a senso unico per un segmento.



Matrice SGACL, come illustrato nell'immagine seguente, è una visualizzazione di esempio per il modello Allow-list (Default Deny).





Verifica

SGT dispositivo di rete

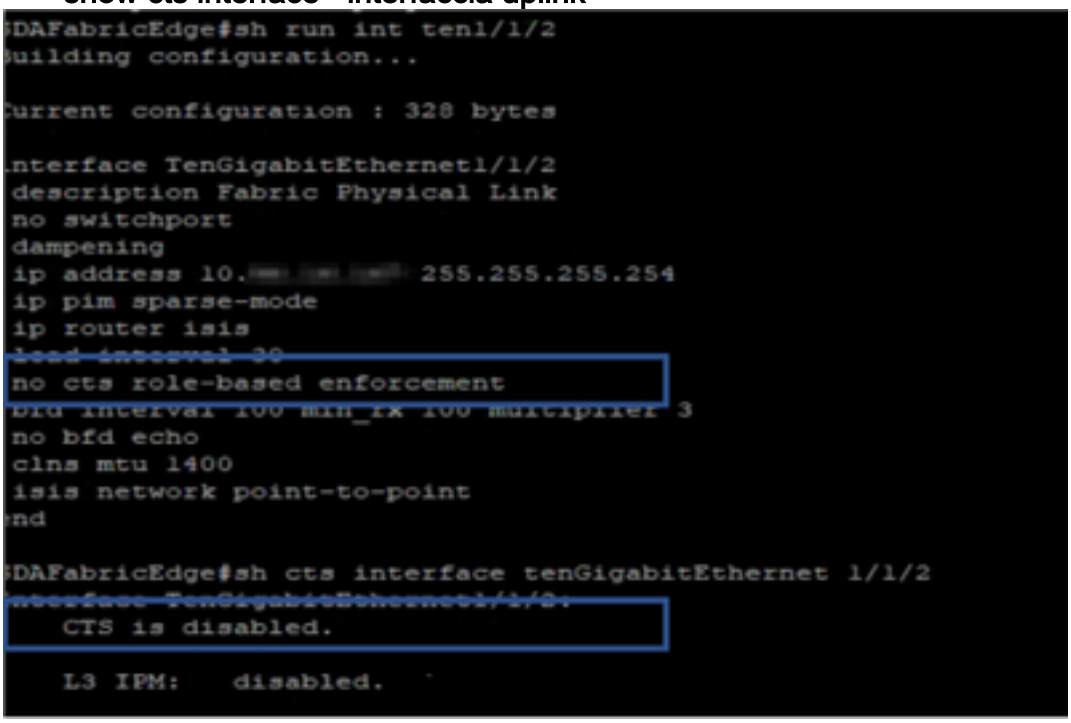
Per verificare lo SGT degli switch ricevuto da ISE, eseguire questo comando: **show cts environment-data**

```
SDAFabricEdge#sh cts environment-data
CTS Environment Data
====================
Current state = COMPLETE
Last status = Successful
Local Device SGT:
  SGT tag = 2-15:TrustSec_Devices
Server List Info:
Installed list: CTSServerList1-0002, 2 server(s):
  Server: 10.[redacted], port 1812, A-ID B6220695C1B21F6F3556E3C5F57B9D6E
          Status = ALIVE
          auto-test = FALSE, keywrap-enable = FALSE, idle-time = 60 mins, deadtime = 20 secs
  Server: 10.[redacted], port 1812, A-ID B6220695C1B21F6F3556E3C5F57B9D6E
          Status = ALIVE
          auto-test = FALSE, keywrap-enable = FALSE, idle-time = 60 mins, deadtime = 20 secs
Security Group Name Table:
    0-00:Unknown
    2-00:TrustSec_Devices
```

Applicazione sulle porte uplink

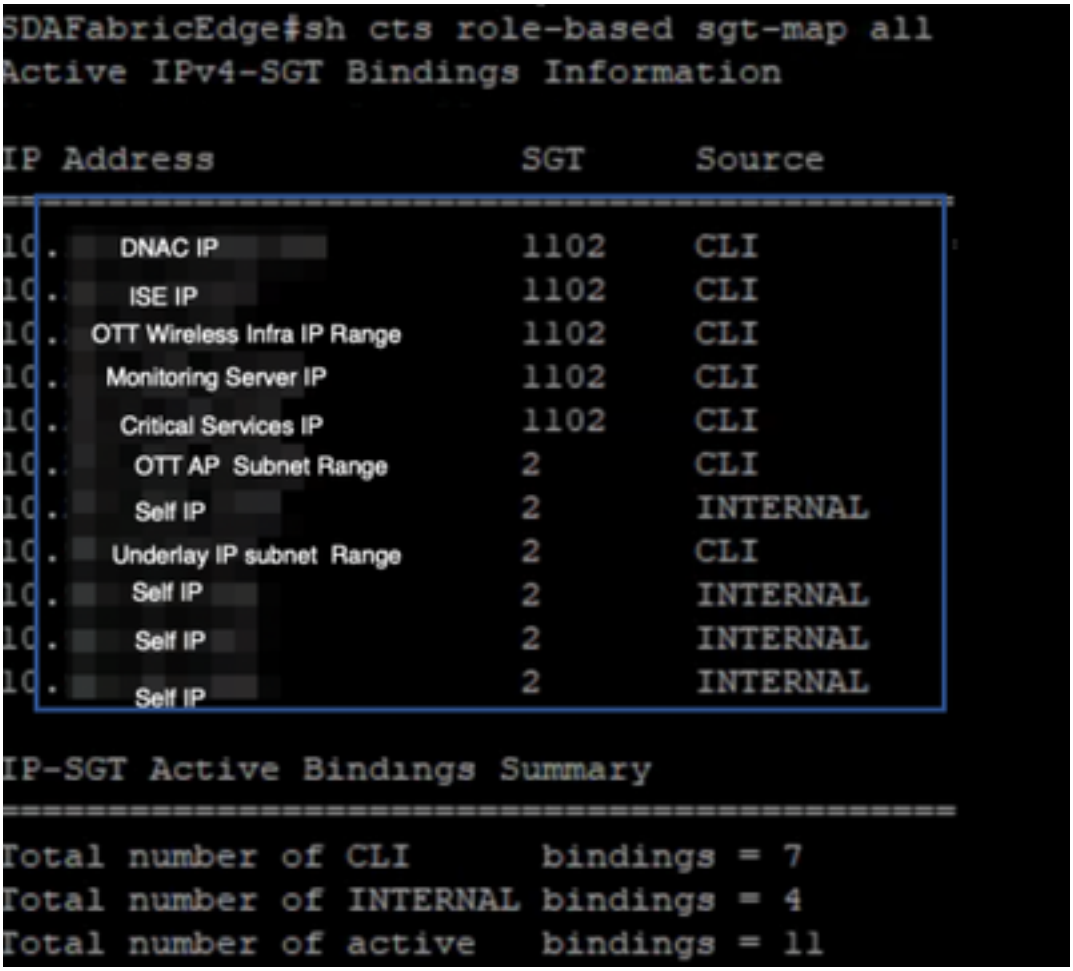
Per verificare l'applicazione sull'interfaccia uplink, eseguire i seguenti comandi:

- **show run interface <uplink>**
- **show cts interface <interfaccia uplink>**



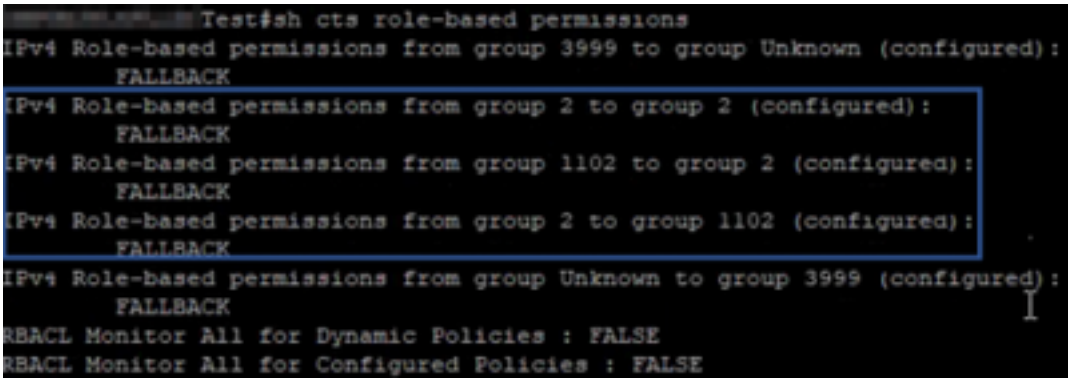
Mapping IP-SGT locale

Per verificare i mapping IP-SGT configurati localmente, eseguire questo comando: **sh cts role-based sgt-map all**



SGACL FALLBACK locale

Per verificare FALLBACK SGACL, eseguire questo comando: **sh cts autorizzazione basata su ruolo**



Nota: Il protocollo SGACL implementato da ISE ha la priorità sul protocollo SGACL locale.

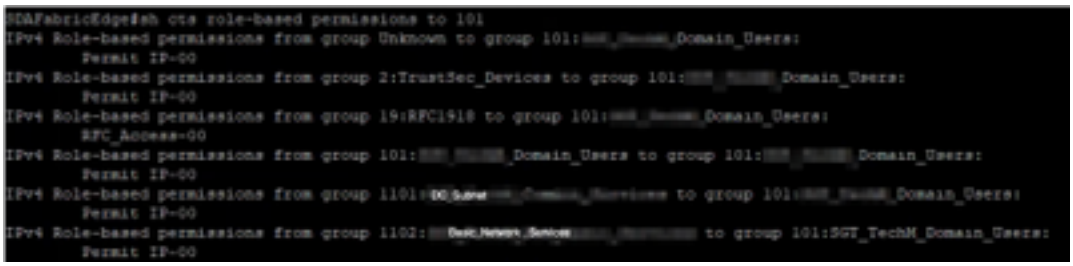
Abilitazione Allow-List (Default Deny) sugli switch Fabric

Per verificare il modello Allow-list (Default Deny), eseguire questo comando: **sh cts autorizzazione basata sul ruolo**

```
SDAFabricEdge#sh cts role-based permissions
IPv4 Role-based permissions default:
        Deny IP-00
```

SGACL per endpoint connesso all'infrastruttura

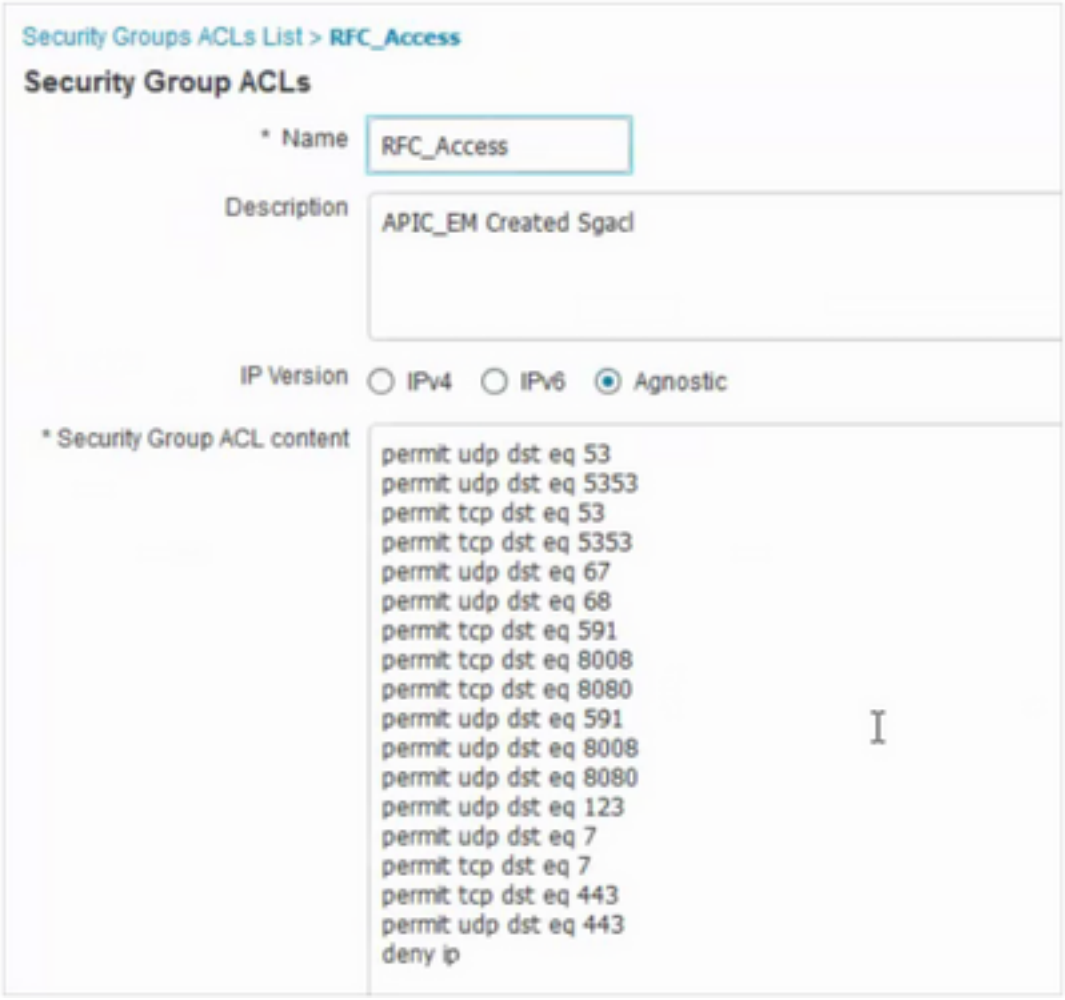
Per verificare lo SGACL scaricato da ISE, eseguire questo comando: **sh cts autorizzazione basata su ruolo**



Verifica contratto creato da DNAC

Per verificare lo SGACL scaricato da ISE, eseguire questo comando: **show access-list <ACL/Nome contratto>**

```
Role-based IP access list RFC_Access-00 (downloaded)
    10 permit udp dst eq domain
    20 permit udp dst eq 5353
    30 permit tcp dst eq domain
    40 permit tcp dst eq 5353
    50 permit udp dst eq bootps
    60 permit udp dst eq bootpc
    70 permit tcp dst eq 591
    80 permit tcp dst eq 8008
    90 permit tcp dst eq 8080
    100 permit udp dst eq 591
    110 permit udp dst eq 8008
    120 permit udp dst eq 8080
    130 permit udp dst eq ntp
    140 permit udp dst eq echo
    150 permit tcp dst eq echo
    160 permit tcp dst eq 443
    170 permit udp dst eq 443
    180 deny ip
```



Sottoporre il contatore SGACL sugli switch fabric

Per verificare gli accessi ai criteri SGACL, eseguire questo comando: **Mostra contatore basato sul ruolo cts**

```
Role-based IPv4 counters
From    To      SW-Denied  HW-Denied  SW-Permitt  HW-Permitt  SW-Monitor  HW-Monitor
*       *       0          0          0           0           0           0
2       2       0          0          1644843     0           0           0
1101    2       0          0          0           0           0           0
1102    2       0          0          0           0           0           0
101     101     0          0          0           0           0           0
1101    101     0          0          0           57647       0           0
1102    101     0          0          0           12541       0           0
1103    101     0          0          0           25          0           0
```

Risoluzione dei problemi

Problema 1. Nel caso in cui entrambi i nodi ISE siano inattivi.

Se entrambi i nodi ISE sono inattivi, la mappatura IP-SGT ricevuta da ISE viene rimossa e tutte le DGT vengono contrassegnate come sconosciute, e tutte le sessioni utente esistenti vengono interrotte dopo 5-6 minuti.

> **Nota:** Questo problema è applicabile solo quando l'accesso SGACL sgt (xxxx) -> unknown (0) è limitato alle porte DHCP, DNS e proxy Web.

Soluzione:

1. Creazione di un SGT (es. RFC 1918).
2. Eseguire il push dell'intervallo IP privato RFC su entrambi i bordi.
3. Limita l'accesso a DHCP, DNS e proxy Web da SFT (xxxx) —> RFC1918
4. Crea/modifica sgacl sgt (xxxx) —> sconosciuto con contratto Permit IP.

Ora, se entrambi i nodi ise si bloccano, SGACL sgt—>accessi sconosciuti e la sessione esistente rimane intatta.

Problema 2. Voce unidirezionale per IP Phone o nessuna voce.

L'estensione alla conversione IP avviene sul SIP e la comunicazione vocale effettiva avviene sul RTP tra IP e IP. CUCM e Voice Gateway sono stati aggiunti a **DGT_Voice**.

Soluzione:

1. Èpossibile abilitare la stessa posizione per la comunicazione vocale est-ovest permettendo il traffico da IP_Phone —> IP_Phone.
2. Il resto del percorso può essere consentito dall'intervallo del protocollo RTP di autorizzazione nella DGT RFC1918. Lo stesso intervallo può essere consentito per IP_Phone —> Unknown.

Problema 3. L'endpoint VLAN critico non ha accesso alla rete.

DNAC fornisce allo switch una VLAN critica per i dati e, in base alla configurazione, tutte le nuove connessioni durante l'interruzione dell'ISE ottengono una VLAN critica e una SGT 3999. Il criterio Deny in trustsec predefinito limita l'accesso della nuova connessione a qualsiasi risorsa di rete.

Soluzione:

Push SGACL per SGT critico su tutti gli switch Edge e Border con modello DNAC

```
cts role-based permissions from 0 to 3999 FALLBACK

cts role-based permissions from 3999 to 0 FALLBACK
```

Questi comandi vengono aggiunti alla sezione di configurazione.

> **Nota:** Tutti i comandi possono essere combinati in un singolo modello e possono essere sottoposti a push durante il provisioning.

Problema 4. VLAN critica di drop-in del pacchetto.

Se il computer si trova in una VLAN critica a causa di nodi ISE inattivi, il pacchetto diminuisce ogni 3-4 minuti (sono state osservate max 10 perdite) per tutti gli endpoint della VLAN critica.

Osservazioni: I contatori di autenticazione aumentano quando i server sono INATTIVI. I client tentano di eseguire l'autenticazione con PSN quando i server sono stati contrassegnati come INATTIVI.

Soluzione:

In teoria, non dovrebbe esserci alcuna richiesta di autenticazione da un endpoint se i nodi PSN ISE sono inattivi.

Eseguire questo comando in Server Radius con DNAC:

automate-tester username auto-test probe-on

Con questo comando nello switch, invia periodicamente messaggi di autenticazione di test al server RADIUS. Cerca una risposta RADIUS dal server. Non è necessario un messaggio di operazione completata. Un'autenticazione non riuscita è sufficiente perché indica che il server è attivo.

Ulteriori informazioni

Modello finale DNAC:

```
interface range $uplink1

no cts role-based enforcement

! .

cts role-based sgt-map <ISE Primary IP> sgt 1102

cts role-based sgt-map <Underlay Subnet> sgt 2

cts role-based sgt-map <Wireless OTT Subnet>sgt 1102

cts role-based sgt-map <DNAC IP> sgt 1102

cts role-based sgt-map <SXP Subnet> sgt 2

cts role-based sgt-map <Network Monitoring Tool IP> sgt 1102

cts role-based sgt-map vrf CORP_VN <Voice Gateway Subnet> sgt 1102

!

ip access-list role-based FALLBACK

permit ip

!

cts role-based permissions from 2 to 1102 FALLBACK

cts role-based permissions from 1102 to 2 FALLBACK

cts role-based permissions from 2 to 2 FALLBACK

cts role-based permissions from 0 to 3999 FALLBACK

cts role-based permissions from 3999 to 0 FALLBACK
```

> **Nota:** Tutte le interfacce uplink nei nodi edge sono configurate senza imposizione e si presume che uplink si connetta solo al nodo border. Sui nodi Border, le interfacce uplink verso i nodi edge devono essere configurate senza imposizione e questa operazione deve

essere eseguita manualmente.