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

# Sommario

Introduzione **Prerequisiti** Requisiti Componenti usati Configurazione Esempio di rete Configurazione Passaggio 1. Cambiare il SGT degli switch da Sconosciuto a Dispositivi TrustSec. Passaggio 2. Disabilitare l'applicazione basata sui ruoli CTS. Passaggio 3. Mappatura IP-SGT sugli switch per bordi e bordi con modello DNAC. Passaggio 4. SGACL di fallback con modello DNAC. Passaggio 5. Abilitare il modello Allow-List (Default Deny) nella matrice TrustSec. Passaggio 6. Creare SGT per endpoint/utenti. Passaggio 7. Creare SGACL per endpoint/utenti (per il traffico di sovrapposizione produzione). Verifica SGT dispositivo di rete Applicazione sulle porte uplink Mapping IP-SGT locale SGACL FALLBACK locale Abilitazione Allow-List (Default Deny) sugli switch Fabric SGACL per endpoint connesso all'infrastruttura Verifica contratto creato da DNAC Sottoporre il contatore SGACL sugli switch fabric Risoluzione dei problemi Problema 1. Nel caso in cui entrambi i nodi ISE siano inattivi. Problema 2. Voce unidirezionale per IP Phone o nessuna voce. Problema 3. L'endpoint VLAN critico non ha accesso alla rete. Problema 4. VLAN critica di drop-in del pacchetto. Ulteriori informazioni

# 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

Network Device Authorization Define the Network Device Authorization Policy by ass	gning SGTs to network devices. Drag and drop rules to change the	he order.
🖌 🗹 🔹 Defait	If no rules defined or no match	ther TrustSec_Devices

#### 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-andmanagement/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 Directional :
Source SGT : Domain Users (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**.

	RFC_	Access	
Name" RFC_Access		Implicit Action Deny	~
Description (Optio	onal)		
Action	Part/Protocol		
Action	Port/Protocol drs (TCP/UDP 53,5353)	Add   Edit	Delete *
Action PERMIT PERMIT	PersProtecel drs (TCP/UCP 53,5353) dhop (JCP 47,68)	Add   Edit   Add   Edit	Delete * Delete
Action PERMIT PERMIT PERMIT	PertiProtecol           dns (TCP/UDP 53,5353)           dhop (UDP 47,68)           http-alt (TCP/UDP 591,8008,8000)	Add   Edit   Add   Edit   Add   Edit	Delete * Delete Delete
Action PERMIT PERMIT PERMIT	PersProtecel           dns (TCP/UCP 53,5353)           dhcp (UCP 47,68)           http-ait (TCP/UCP 591,8008,8080)           ntp (UCP 123)	Add   Edit   Add   Edit   Add   Edit   Add   Edit   Add   Edit	Delete Delete Delete
Action PORMIT PORMIT PORMIT PORMIT	Pert/Protecol           dris (TCP/UDP 53,5353)           dricp (UDP 67,68)           http://uDP 591,8008,8080)           ntp (UDP 123)           echo (TCP/UDP 7)	Add   Edit   Add   Edit   Add   Edit   Add   Edit   Add   Edit   Add   Edit	Delete Delete Delete Delete Delete

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.

CISCO -	INA I	NUMBER OF STREET	POLICY	PROVIDEDS AND	URANES	= *	0 0							
Destloyerd	Vitasi I	lativorit.	Policy Admit	riatration Contract	cts Registry									
Grave-Based Assess Carthol Fabric) IP-(Issael Access Control (Non-Fabric) Application Publicies Traffic Capp Publicies														
Create Policy by selecting Source, Destination, and applying a Contract														
Pulcy Name* Description (Dystonal) Dortract* Description														
<ul> <li>Enable Pro Available Tex</li> </ul>	iliy O En	nie III-drech	unal O	,	Source Scriptiv-Groups	_								
$\{(Q_{i})^{(i)}(i)\}$														
AG	*0	AD	*	~	Dag projet here									
ACL, Ser vice, Ap	40,7m 1,6m,	ACL, My 3, Same -	Admin	Authors										
	CA	00	00	00	Everification Scolective Decept									
8400	Gamaro	Gara, G america	Gamman	Density: an										
05	00	80		œ	Diag gragai here									
Develop ment_R	Dector	006	Crophyse	luem										
н	•	-	۲	u			I							

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.

low or/Sectoration	Oceanie Rome	Research Nachara	P-Physics	West- testimen	mineran	Real States of States	IC, Interest	000,8eta	NUK	000, Manuaran K	80.110	Tester Deter	(Selection)
Rectaginal Process											WG_Acces		

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

have, Destation	Domain Joan	Complex Monthlese	#.0xxx	Tabo- tanhanas	-	Rate, Metanole, Section	01,5alleven	007,944r	NUK	ODC, Ressures	#10.84	Trusture Destant	University
Burnals Starts											WE, Annual		
Durate Waltons											91,A000		
P-Pass											Value, Ausona		
View Conference											Value_Auson		
											197, Acces		
Ball, Network, Bordon													
DC,balant													
BOL, MAN													
OC,Acouter													
NU/K													
1000	WC, Asses	WC, August	Taken, Assess	Tata Assess	WC, Asses								
Thankon (Induse													
internet .													
torbait								Sec. 2					

Color	Contract
	Deny IP
	Permit IP
	SGACL

# Verifica

## SGT dispositivo di rete

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



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 rolebased sgt-map all** 

SDAFabricEdge#sh cts r Active IPv4-SGT Bindin	ole-base gs Infor	d sgt-map all mation
IP Address	SGT	Source
10. DNACIP	1102	CLI
10. ISE IP	1102	CLI
10. OTT Wireless Infra IP Range	1102	CLI
10 . Monitoring Server IP	1102	CLI
10 . Critical Services IP	1102	CLI
10. OTT AP Subnet Range	2	CLI
10 . Self IP	2	INTERNAL
10. Underlay IP subnet Range	2	CLI
10. Self IP	2	INTERNAL
10. Self IP	2	INTERNAL
10. Self IP	2	INTERNAL
IP-SGT Active Bindings	Summary	
Total number of CLI	bindi	ngs = 7
fotal number of INTERN	AL bindi	ngs = 4
Total number of active	bindi	ngs = 11

### SGACL FALLBACK locale

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

-	Test#sh cts role-based permissions	
IPv4	Role-based permissions from group 3999 to group Unknown (configured) FALLBACK	:
CPv4	Role-based permissions from group 2 to group 2 (configured): FALLBACK	
CPv4	Role-based permissions from group 1102 to group 2 (configured): FALLBACK	
[Pv9	Role-based permissions from group 2 to group 1102 (configured): FALLBACK	
IPve	Role-based permissions from group Unknown to group 3999 (configured) FALLBACK	1
RBACI	Monitor All for Dynamic Policies : FALSE	
RBACL	Monitor All for Configured Policies : FALSE	

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** 



### SGACL per endpoint connesso all'infrastruttura

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

SDAF	bricEdge∎sh cts role-ba	seed permiss	sions to 101
IPv4	Role-based permissions	from group	Unknown to group 101;
	Permit IP-00		
IPvi	Role-based permissions	from group	2:TrustSec_Devices to group 101: Domain_Deers:
	Permit IP-00		
IEvi	Role-based permissions	from group	19:RFC1910 to group 101: Domain_Domain_Osers:
	RFC_Access-00		
IPvs	Role-based permissions	from group	101: Domain Users to group 101: Domain Users:
	Permit IP-00		
IEv4	Role-based permissions	from group	1101:00 Same Commiss Directores to group 101:000 Domain Domain Domain
	Permit IP-00		
IP74	Role-based permissions	from group	1102: Own.Never.Sevies to group 101:36T_TechM_Domain_Users:
	Permit TP+00		

#### 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 ds	t eq d	lomain	
20 permit	udp ds	t eq 5	353	
30 permit	tcp ds	t eq d	lomain	
40 permit	tcp ds	t eq 5	353	
50 permit	udp ds	t eq b	ootps	
60 permit	udp ds	t eq b	ootpc	
70 permit	tcp ds	t eq 5	91	
80 permit	tcp ds	t eq 8	008	
90 permit	tcp ds	t eq 8	080	
100 permi	t udp d	st eq	591	
110 permi	t udp d	st eq	8008	
120 permi	t udp d	st eq	8080	
130 permi	t udp d	st eq	ntp	
140 permi	t udp d	st eq	echo	
150 permi	t top d	st eq	echo	
160 permi	t top d	st eq	443	
170 permi	t udp d	st eq	443	
180 deny	ip			

Security Groups ACLs List > RFG Security Group ACLs	C_Access					
* Name	RFC_Access					
Description	APIC_EM Created Sgacl					
IP Version	○ IPv4 ○ IPv6 ● Agnostic					
* Security Group ACL content	permit udp dst eq 53 permit udp dst eq 5353 permit tcp dst eq 5353 permit tcp dst eq 5353 permit udp dst eq 67 permit udp dst eq 68 permit tcp dst eq 591 permit tcp dst eq 8008 permit udp dst eq 8080 permit udp dst eq 8080 permit udp dst eq 8080 permit udp dst eq 123 permit udp dst eq 7 permit tcp dst eq 7 permit tcp dst eq 443 permit udp dst eq 443	I				

## Sottoporre il contatore SGACL sugli switch fabric

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

Role-bas	ed IPv4	counters					
From	То	SW-Denied	HW-Denied	SW-Permitt	HW-Permitt	SW-Monitor	HW-Monitor
*							0
2	2			1644843			0
1101	2						0
1102							0
101	101						0
1101	101				57647		0
1102	101				12541		0
1103	101				25		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
1
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.