

# 採用SDA的Cisco ISE TrustSec允許清單模型 ( 預設拒絕IP )

## 目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[設定](#)

[網路圖表](#)

[組態](#)

[步驟1.將交換機SGT從Unknown更改為TrustSec裝置。](#)

[步驟2.禁用CTS基於角色的實施。](#)

[步驟3.使用DNAC模板的邊界交換機和邊緣交換機上的IP-SGT對映。](#)

[步驟4.使用DNAC模板回退SGACL。](#)

[步驟5.在TrustSec矩陣中啟用允許清單模型 \( 預設拒絕 \) 。](#)

[步驟6.為終端/使用者建立SGT。](#)

[步驟7.為終端/使用者建立SGACL \( 用於生產重疊流量 \) 。](#)

[驗證](#)

[網路裝置SGT](#)

[上行鏈路埠上的實施](#)

[本地IP-SGT對映](#)

[本地後援SGACL](#)

[交換矩陣交換機上的允許清單 \( 預設拒絕 \) 啟用](#)

[連線到交換矩陣的終端的SGACL](#)

[驗證DNAC建立的合約](#)

[交換矩陣交換機上的底層SGACL計數器](#)

[疑難排解](#)

[問題1：以防兩個ISE節點都關閉。](#)

[問題2. IP-Phone單向語音或無語音。](#)

[問題3.關鍵VLAN端點沒有網路訪問許可權。](#)

[問題4.資料包丟棄關鍵VLAN。](#)

[其他資訊](#)

## 簡介

本檔案介紹如何在軟體定義存取(SDA)中啟用TrustSec的允許清單 ( 預設拒絕IP ) 模式。本文涉及多個技術和元件，包括身分識別服務引擎(ISE)、數位網路架構中心(DNAC)和交換器 ( 邊界和邊緣 )。

有兩種可用的Trustsec模型：

- Deny-List模型 ( 預設允許IP )：在此模型中，預設操作是Permit IP，應使用Security Group

Access Lists(SGACL)顯式配置任何限制。這通常在您對其網路中的流量流沒有完全瞭解時使用。這種模型易於實現。

- Allow-List Model ( 預設拒絕IP ) : 在此模型中，預設操作是Deny IP，因此應使用SGACL明確允許所需的流量。這通常在客戶對其網路中的流量型別有公正瞭解時使用。此模型需要詳細研究控制平面流量，並且一旦啟用，它就有可能阻止ALL流量。

## 必要條件

### 需求

思科建議您瞭解以下主題：

- Dot1x/MAB驗證
- Cisco TrustSec(CTS)
- 安全交換通訊協定(SXP)
- Web代理
- 防火牆概念
- DNAC

### 採用元件

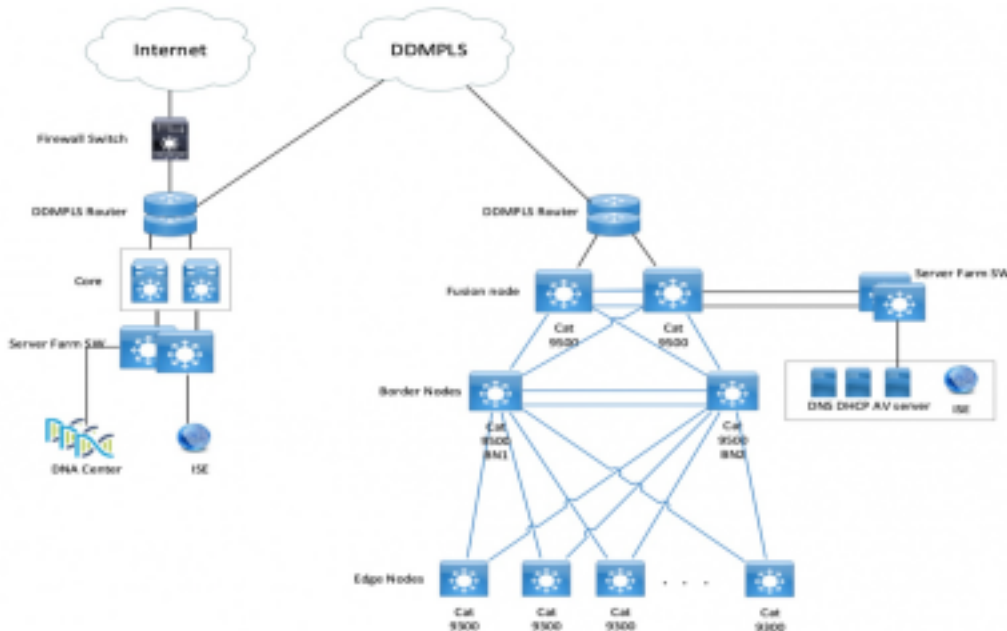
本文中的資訊係根據以下軟體和硬體版本：

- 採用IOS 16.9.3的9300邊緣和9500邊界節點 ( 交換器 )
- DNAC 1.3.0.5
- ISE 2.6補丁3 ( 兩個節點 — 冗餘部署 )
- DNAC和ISE已整合
- 邊界和邊緣節點由DNAC調配
- SXP隧道建立從ISE ( 揚聲器 ) 到兩個邊界節點 ( 監聽器 )
- 將IP地址池新增到主機自註冊

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除 ( 預設 ) 的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

## 設定

### 網路圖表



## 組態

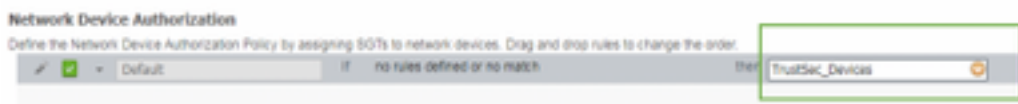
以下是啟用允許清單模式 ( 預設拒絕IP ) 的步驟：

1. 將交換機SGT從未知裝置更改為TrustSec裝置。
2. 禁用CTS基於角色的實施。
3. 使用DNAC模板的邊界交換機和邊緣交換機上的IP-SGT對映。
4. 使用DNAC模板的回退SGACL。
5. 在trustsec Matrix中啟用Allow-List ( 預設拒絕IP ) 。
6. 為終端/使用者建立SGT。
7. 為終端/使用者建立SGACL ( 用於生產重疊流量 ) 。

### 步驟1.將交換機SGT從Unknown更改為TrustSec裝置。

預設情況下，為網路裝置授權配置了未知的安全組標籤(SGT)。將其更改為TrustSec裝置SGT可提供更多可視性，並有助於建立特定於交換機發起流量的SGACL。

導航到工作中心> TrustSec > Trustsec Policy > Network Device Authorization，然後將其從Unknown更改為Trustsec\_Devices



### 步驟2.禁用CTS基於角色的實施。

- 一旦Allow-List模型 ( 預設拒絕 ) 就位，交換矩陣中的所有流量都會遭到封鎖，包括底層多點傳送和廣播流量，例如中間系統到中間系統(IS-IS)、雙向轉發檢測(BFD)、Secure Shell(SSh)流量。
- 連線到交換矩陣邊緣以及邊框的所有TenGig埠都應使用此處的命令進行配置。有了此功能，從此介面發起並進入此介面的流量就無需強制執行。

```
Interface tengigabitethernet 1/0/1  
  
no cts role-based enforcement
```

**附註：**為簡單起見，可以使用DNAC中的範圍模板來完成此操作。否則，對於每台交換機，在調配過程中都需要手動完成。以下代碼段顯示如何通過DNAC模板進行操作。

```
interface range $uplink1  
  
no cts role-based enforcement
```

有關DNAC模板的詳細資訊，請參閱文檔的此URL。

[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](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)

### 步驟3.使用DNAC模板的邊界交換機和邊緣交換機上的IP-SGT對映。

其理念是即使所有ISE都關閉，本地IP-SGT對映也可在交換機上使用。這可以確保Underlay已建立，並且與關鍵資源的連線完好。

第一步是將關鍵服務繫結到SGT（例如 — Basic\_Network\_Services/1000）。這些服務包括：

- 底層/ISIS子網
- ISE/DNAC
- 監控工具
- AP的子網（針對OTT）
- 終端伺服器
- 關鍵服務 — Ex:IP電話

範例：

```
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
```

### 步驟4.使用DNAC模板回退SGACL。

SGT對映只有在使用SGT建立相關SGACL之後才有用，因此我們的下一步是建立一個在ISE節點關閉時充當本地回退的SGACL（當ISE服務關閉時，SXP隧道關閉，因此SGACL和IP SGT對映不會動態下載）。

此配置將推送到所有邊緣和邊界節點。

回退基於角色的ACL/合約:

```
ip access-list role-based FALLBACK
```

```
permit ip
```

TrustSec裝置到TrustSec裝置 :

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

高於SGACL確保交換矩陣交換機和底層IP之間的通訊

TrustSec裝置至SGT 1000:

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

Above SGACL確保交換機和存取點與ISE、DNAC、WLC和監控工具的通訊

SGT 1000到TrustSec裝置 :

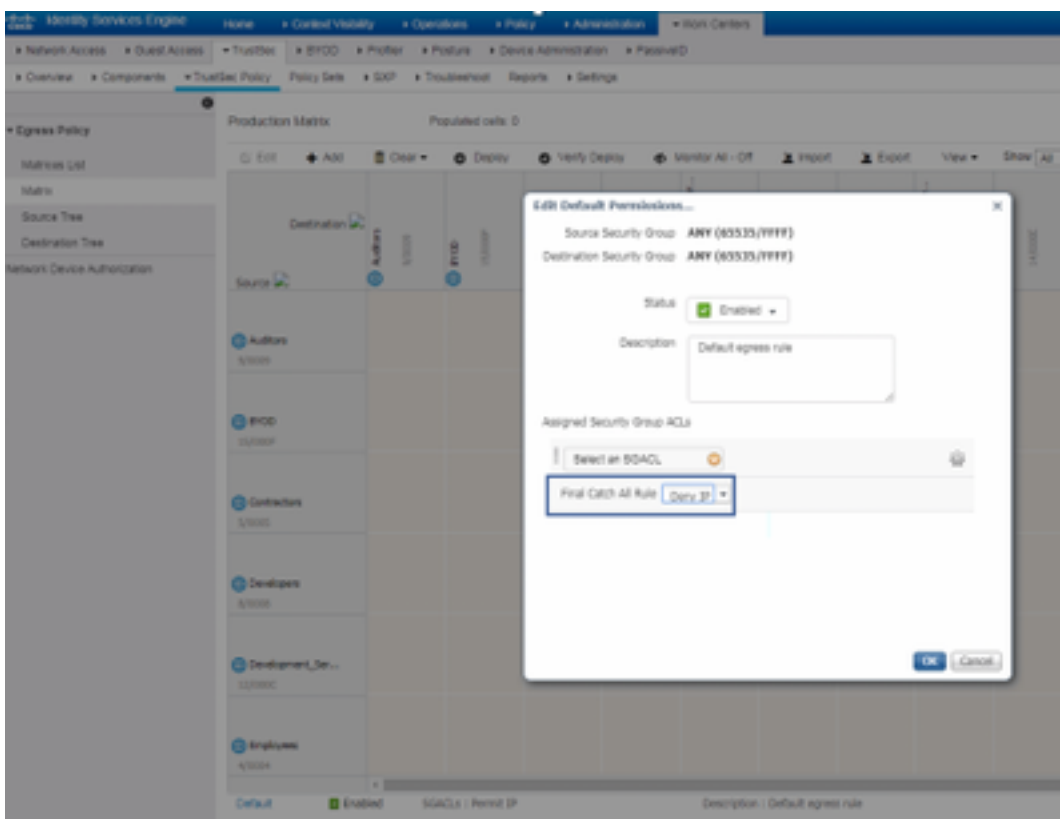
```
cts role-based permissions from 1000 to 2 FALLBACK
```

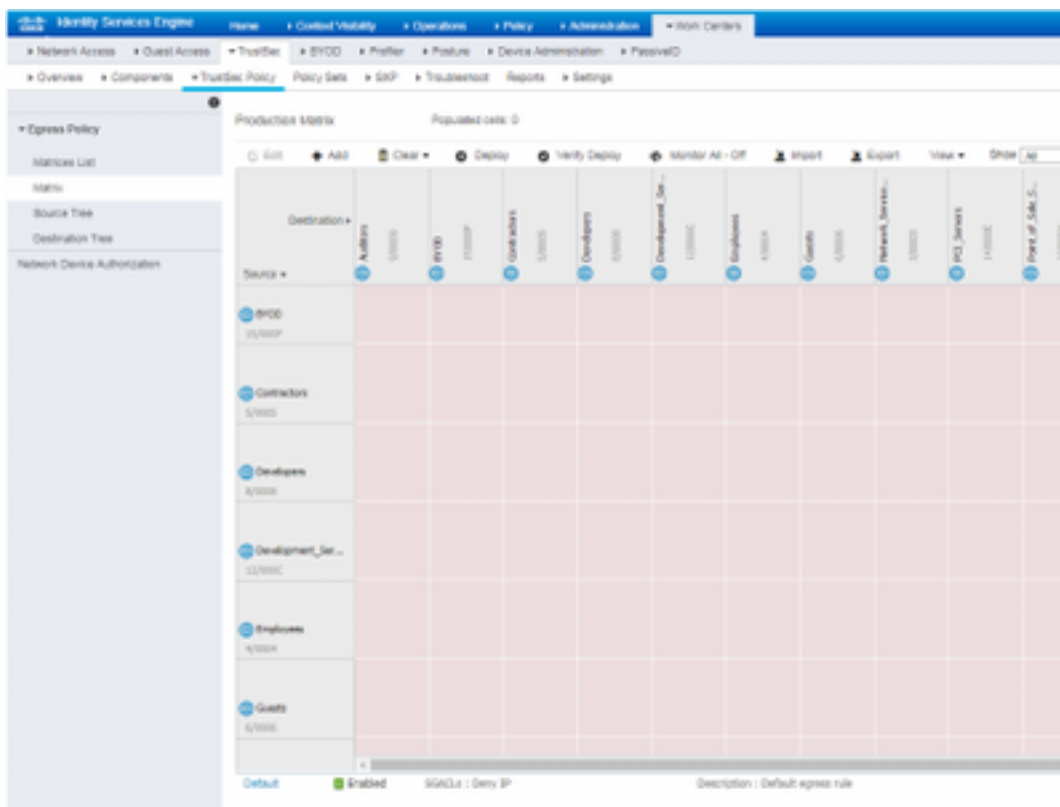
Above SGACL確保從接入點到ISE、DNAC、WLC和監控工具到交換機的通訊

**步驟5.在TrustSec矩陣中啟用允許清單模型 ( 預設拒絕 ) 。**

要求是拒絕網路中的大部分流量，並允許較小的範圍。如果對顯式允許規則使用預設的deny，則需要的策略會更少。

導航到工作中心(Work Centers)> Trustsec > TrustSec Policy > Matrix > Default，然後在最終捕獲規則中將其更改為Deny All。



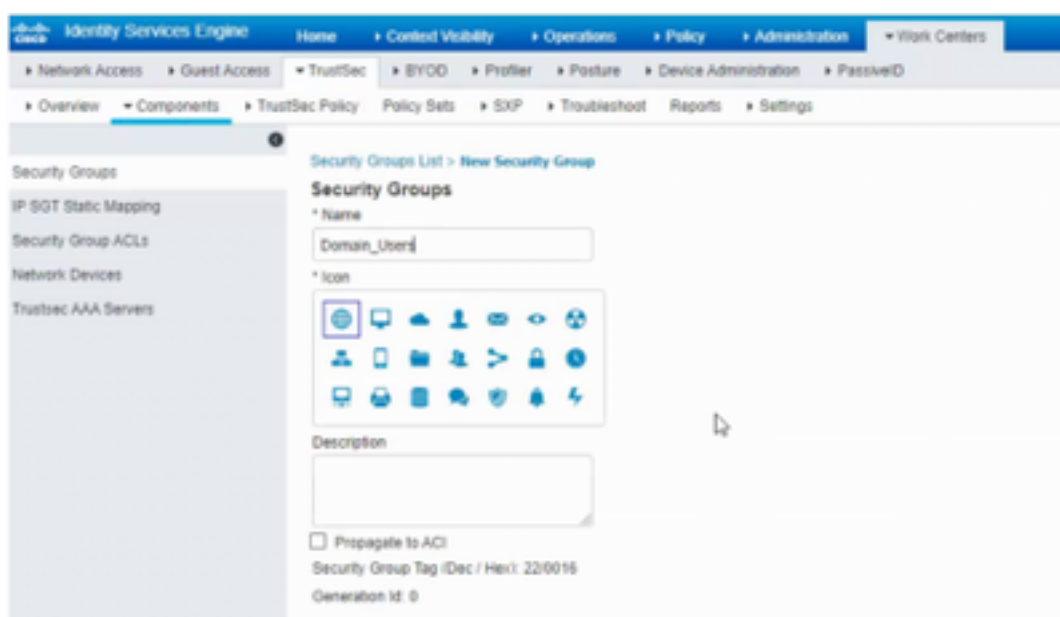


附註：此映像表示（預設情況下，所有列都顯示為紅色）、已啟用預設拒絕，且建立 SGACL 後只能允許選擇性流量。

## 步驟6. 為終端/使用者建立SGT。

在SDA環境中，只能從DNAC GUI建立新的SGT，因為由於ISE/DNAC中的SGT資料庫不匹配，資料庫損壞的情況很多。

若要建立SGT，請登入到DNAC > Policy > Group-Based Access Control > Scalable Groups > Add Groups，頁面將您重定向到ISE Scalable Group，按一下Add，輸入SGT名稱並儲存。



同樣的SGT通過PxGrid整合反映在DNAC中。對於所有未來SGT的建立而言，此過程相同。

## 步驟7.為終端/使用者建立SGACL (用於生產重疊流量)。

在SDA環境中，只能從DNAC GUI建立新的SGT。

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)

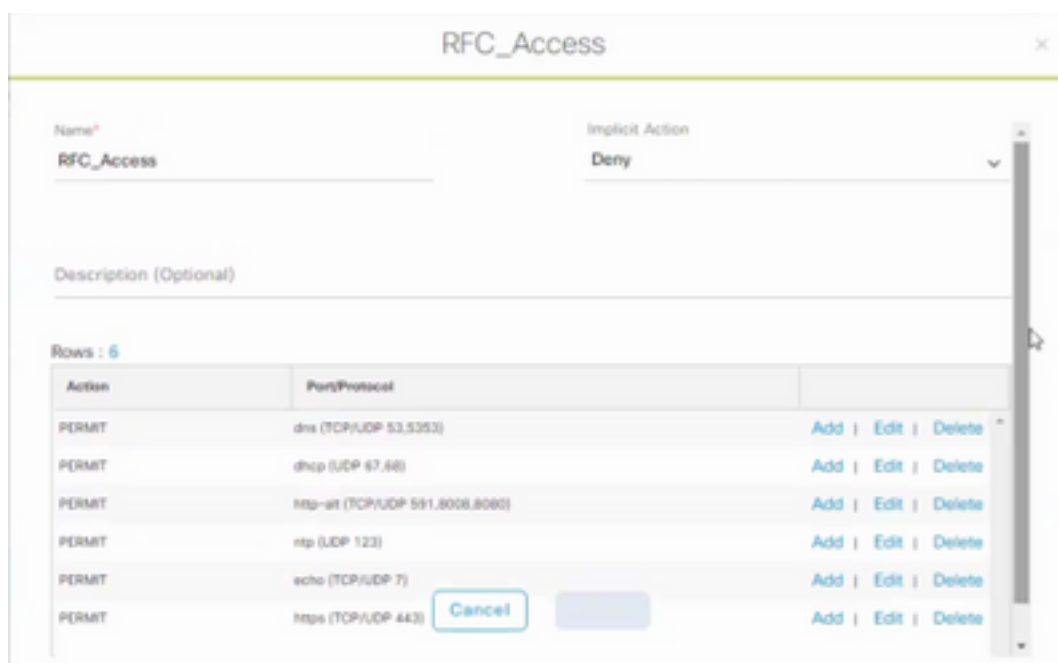
Enable Policy :

Enable Bi-Directional :

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

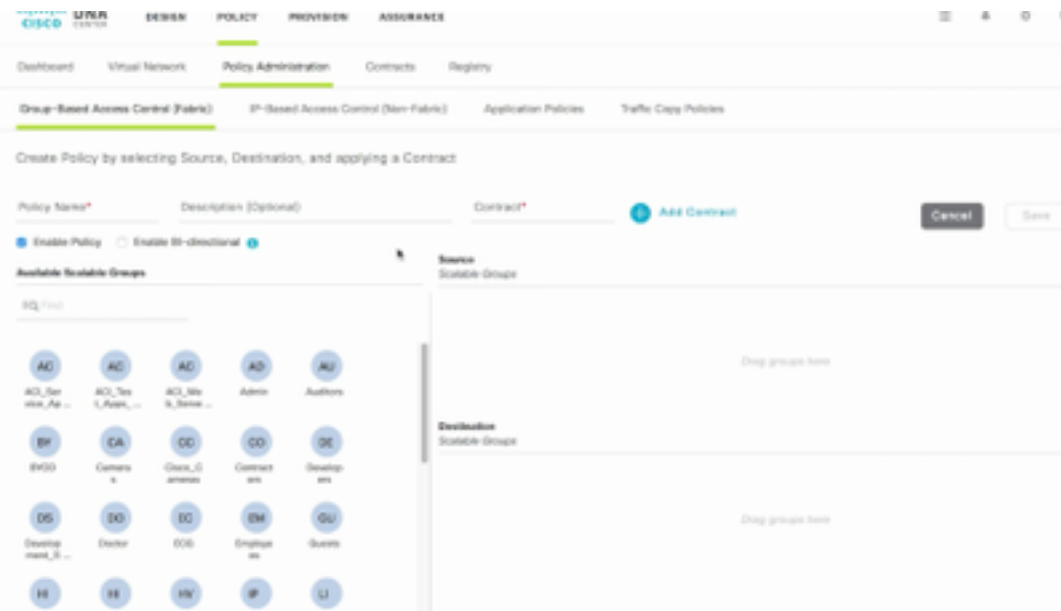
Destination SGT: RFC1918 (Drag from Available Security Group)

若要建立Contract，請登入DNAC，然後導覽至Policy > Contracts > Add Contracts > Add required protocol，然後按一下Save。



Action	Port/Protocol	
PERMIT	dns (TCP/UDP 53,5353)	Add   Edit   Delete
PERMIT	dhcp (UDP 67,68)	Add   Edit   Delete
PERMIT	ntp-wt (TCP/UDP 591,8008,8080)	Add   Edit   Delete
PERMIT	ntp (UDP 123)	Add   Edit   Delete
PERMIT	echo (TCP/UDP 7)	Add   Edit   Delete
PERMIT	https (TCP/UDP 443)	Add   Edit   Delete

要建立合約，請登入到DNAC，然後導航到Policy > Group-Based Access-Policies > Add Policies > Create policy (包含給定資訊)，現在按一下Save，然後Deploy。



從DNAC配置

SGACL/Contract後，它會在ISE中自動反射。下面是單向matrix檢視的示例。

Source/Description	Domain Users	Domain Machines	IP Phones	Video-Conference	Infocenters	Back_Network_Servers	DC_Authen	SQL_Servers	SQL_MC	SQL_Replicas	WCS/WSA	TrustSec Endpoints	Unknown
Example/Desc	Green	Red	Red	Red	Red	Green	Green	Red	Red	Red	Blue	Red	Green

SGACL矩陣 (如下圖所示)

是允許清單 (預設拒絕) 模型的示例檢視。

Source/Description	Domain Users	Domain Machines	IP Phones	Video-Conference	Infocenters	Back_Network_Servers	DC_Authen	SQL_Servers	SQL_MC	SQL_Replicas	WCS/WSA	TrustSec Endpoints	Unknown
Domain Users	Green	Red	Red	Red	Red	Green	Green	Red	Red	Red	Blue	Red	Green
Domain Machines	Red	Green	Red	Red	Red	Green	Green	Red	Red	Red	Blue	Red	Green
IP Phones	Red	Red	Green	Red	Red	Green	Green	Red	Red	Red	Blue	Red	Green
Video-Conference	Red	Red	Red	Green	Red	Green	Green	Red	Red	Red	Blue	Red	Green
Infocenters	Red	Red	Red	Red	Green	Green	Green	Red	Red	Red	Blue	Red	Green
Back_Network_Servers	Green	Red	Red	Red	Red	Green	Green	Red	Red	Red	Blue	Red	Green
DC_Authen	Red	Red	Red	Red	Red	Green	Green	Red	Red	Red	Blue	Red	Green
SQL_Servers	Red	Red	Red	Red	Red	Green	Green	Red	Red	Red	Blue	Red	Green
SQL_MC	Red	Red	Red	Red	Red	Green	Green	Red	Red	Red	Blue	Red	Green
SQL_Replicas	Blue	Blue	Blue	Blue	Blue	Green	Green	Red	Red	Red	Blue	Red	Green
WCS/WSA	Blue	Blue	Blue	Blue	Blue	Green	Green	Red	Red	Red	Blue	Red	Green
TrustSec Endpoints	Green	Red	Red	Red	Red	Green	Green	Red	Red	Red	Blue	Red	Green
Unknown	Green	Red	Red	Red	Red	Green	Green	Red	Red	Red	Blue	Red	Green
Default	Red	Red	Red	Red	Red	Red	Red	Red	Red	Red	Red	Red	Red

Color	Contract
Red	Deny IP
Green	Permit IP
Blue	SGACL

驗證



## 網路裝置SGT

要驗證ISE接收的交換機SGT，請運行以下命令：`show cts environmental-data`

```
SDAFabricEdge#sh cts environmental-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: 10.10.10.10, port 1812, A-ID B6220695C1B21F6F3554E3C5F57B9D6E
    Status = ALIVE
    auto-test = FALSE, keywrap-enable = FALSE, idle-time = 60 mins, deadtime = 20 secs
  Server: 10.10.10.10, port 1812, A-ID B6220695C1B21F6F3554E3C5F57B9D6E
    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
```

## 上行鏈路埠上的實施

若要驗證上行鏈路介面上的強制實施，請運行以下命令：

- `show run interface <uplink>`
- `show cts interface <uplink interface>`

```
SDAFabricEdge#sh run int ten1/1/2
Building configuration...

Current configuration : 328 bytes

interface TenGigabitEthernet1/1/2
description Fabric Physical Link
no switchport
dampening
ip address 10.10.10.10 255.255.255.254
ip pim sparse-mode
ip router isis
load interval 30
no cts role-based enforcement
bfd interval 100 min_rx 100 multiplier 3
no bfd echo
cls mtu 1400
isis network point-to-point
end

SDAFabricEdge#sh cts interface tenGigabitEthernet 1/1/2
interface TenGigabitEthernet1/1/2:
CTS is disabled.

L3 IPM: disabled.
```

## 本地IP-SGT對映

若要驗證本地配置的IP-SGT對映，請運行以下命令：`sh cts role-based sgt-map all`

```
SDAFabricEdge#sh cts role-based sgt-map all
Active IPv4-SGT Bindings Information
```

IP Address	SGT	Source
DNAC IP	1102	CLI
ISE IP	1102	CLI
OTT Wireless Infra IP Range	1102	CLI
Monitoring Server IP	1102	CLI
Critical Services IP	1102	CLI
OTT AP Subnet Range	2	CLI
Self IP	2	INTERNAL
Underlay IP subnet Range	2	CLI
Self IP	2	INTERNAL
Self IP	2	INTERNAL
Self IP	2	INTERNAL

```
IP-SGT Active Bindings Summary
```

```
=====
Total number of CLI bindings = 7
Total number of INTERNAL bindings = 4
Total number of active bindings = 11
```

## 本地後援SGACL

若要驗證回退SGACL，請運行以下命令：`sh cts role-based permission`

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

附註：ISE推送的SGACL的優先順序高於本地SGACL。

## 交換矩陣交換機上的允許清單（預設拒絕）啟用

若要驗證允許清單（預設拒絕）模型，請運行以下命令：`sh cts role-based permission`

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

## 連線到交換矩陣的終端的SGACL

若要驗證從ISE下載的SGACL，請運行以下命令：`sh cts role-based permission`

```
SDAFabricEdge#sh cts role-based permissions to 101
IPv4 Role-based permissions from group Unknown to group 101:SGT_TechM_Domain_Users:
  Permit IP-00
IPv4 Role-based permissions from group 2:TrustSec_Devices to group 101:SGT_TechM_Domain_Users:
  Permit IP-00
IPv4 Role-based permissions from group 19:RFC1918 to group 101:SGT_TechM_Domain_Users:
  RFC_Access-00
IPv4 Role-based permissions from group 101:SGT_TechM_Domain_Users to group 101:SGT_TechM_Domain_Users:
  Permit IP-00
IPv4 Role-based permissions from group 1101:SGT_TechM_Domain_Services to group 101:SGT_TechM_Domain_Users:
  Permit IP-00
IPv4 Role-based permissions from group 1102:SGT_TechM_Domain_Services to group 101:SGT_TechM_Domain_Users:
  Permit IP-00
```

## 驗證DNAC建立的合約

若要驗證從ISE下載的SGACL，請運行以下命令：`show access-list <ACL/Contract Name>`

```
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
```

Security Groups ACLs List > RFC\_Access

### Security Group ACLs

\* Name

Description

IP Version  IPv4  IPv6  Agnostic

\* Security Group ACL content

```

permit udp dst eq 53
permit udp dst eq 5353
permit tcp dst eq 53
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 tcp dst eq 8080
permit udp dst eq 591
permit udp dst eq 8008
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
deny ip

```

## 交換矩陣交換機上的底層SGACL計數器

若要驗證SGACL策略命中，請運行以下命令：**Show cts role-based counter**

```

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

```

## 疑難排解

### 問題1：以防兩個ISE節點都關閉。

如果兩個ISE節點都關閉，ISE接收的IP到SGT對映將被刪除，所有DGT都標籤為未知，所有存在的使用者會話將在5-6分鐘後停止。

**附註：**只有當sgt(xxxx)-> unknown(0)SGACL訪問僅限於DHCP、DNS和Web代理埠時，此問題才適用。

解決方案：

1. 建立了SGT(例如RFC(1918))。
2. 將RFC私有IP範圍推送到兩個邊界。
3. 限制從sgt(xxxx)—> RFC1918訪問DHCP、DNS和Web代理
4. 建立/修改sgacl sgt(xxxx)—> unknown，帶允許IP合約。

現在，如果兩個ise節點都關閉，則SGACL sgt—>未知命中，且存在的會話將保持不變。

## 問題2. IP-Phone單向語音或無語音。

在SIP上進行IP轉換擴展，在IP到IP之間通過RTP進行實際語音通訊。CUCM和語音網關已新增到DGT\_Voice。

解決方案：

1. 通過允許來自IP\_Phone —> IP\_Phone的流量，可以啟用相同的位置或東西語音通訊。
2. DGT RFC1918中的「允許RTP協定」範圍可允許該位置的其餘部分。IP\_Phone —> Unknown可允許相同範圍。

## 問題3.關鍵VLAN端點沒有網路訪問許可權。

DNAC為資料調配具有關鍵VLAN的交換機，根據配置，在ISE中斷期間所有新連線都將獲得關鍵VLAN和SGT 3999。Trustsec中的預設拒絕策略限制新連線訪問任何網路資源。

解決方案：

使用DNAC模板為所有邊緣和邊界交換機上的關鍵SGT推送SGACL

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

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

這些命令將新增到配置部分。

**附註：**所有命令可以合併到一個模板中，並在調配過程中推送。

## 問題4.資料包丟棄關鍵VLAN。

由於ISE節點關閉，電腦進入關鍵VLAN後，對於關鍵VLAN中的所有端點，每3-4分鐘會出現一次資料包丟棄（觀察到10個最大丟包）。

意見：當伺服器為DEAD時，身份驗證計數器增加。當伺服器被標籤為DEAD時，客戶端嘗試使用PSN進行身份驗證。

解決方案/解決方法：

理想情況下，如果ISE PSN節點關閉，則不應從終端發出任何身份驗證請求。

將此命令推入具有DNAC的radius伺服器下：

```
automate-tester username auto-test probe-on
```

透過交換器中的此命令，它會定期向RADIUS伺服器傳送測試驗證訊息。它從伺服器查詢RADIUS響應。不需要顯示成功消息 — 身份驗證失敗就足夠了，因為它顯示伺服器處於活動狀態。

## 其他資訊

DNAC最終模板：

```
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
```

**附註：**邊緣節點中的所有上行鏈路介面都未強制配置，並且假設上行鏈路僅連線到邊界節點。在Border節點上，通向邊緣節點的上行鏈路介面需要配置，無需強制執行，並且必須手動完成。