SDAを使用したCisco ISE TrustSec許可リストモデル（デフォルトの拒否IP）

内容

概要

このドキュメントでは、ソフトウェア定義アクセス(SDA)でTrustSecの許可リスト（デフォルトの拒否IP）モデルを有効にする方法について説明します。 このドキュメントには、Identity Services Engine(ISE)、Digital Network Architecture Center(DNAC)、およびスイッチ（ボーダーとエッジ）を含む複数のテクノロジーとコンポーネントが含まれています。

使用可能なTrustsecモデルは2種類あります。

- 拒否リストモデル（デフォルトの許可IP）:このモデルでは、デフォルトのアクションは[Permit IP]で、セキュリティグループアクセスリスト(SGACL)を使用して制限を明示的に設定する必要があります。 これは、一般に、ネットワーク内のトラフィックフローを完全に理解していない場合に使用されます。このモデルは実装が非常に簡単です。

- 許可リストモデル（デフォルトの拒否IP）:このモデルでは、デフォルトアクションはDeny IPであるため、SGACLを使用して必要なトラフィックを明示的に許可する必要があります。これは通常、顧客がネットワーク内のトラフィックフローの種類を十分に理解している場合に使用されます。このモデルでは、コントロールプレーントラフィックの詳細な調査が必要です。また、有効になった時点ですべてのトラフィックをブロックする可能性があります。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Dot1x/MAB認証
- Cisco TrustSec（CTS）
- Security Exchange Protocol(SXP)
- Webプロキシ
- ファイアウォールの概念
- DNAC

使用するコンポーネント

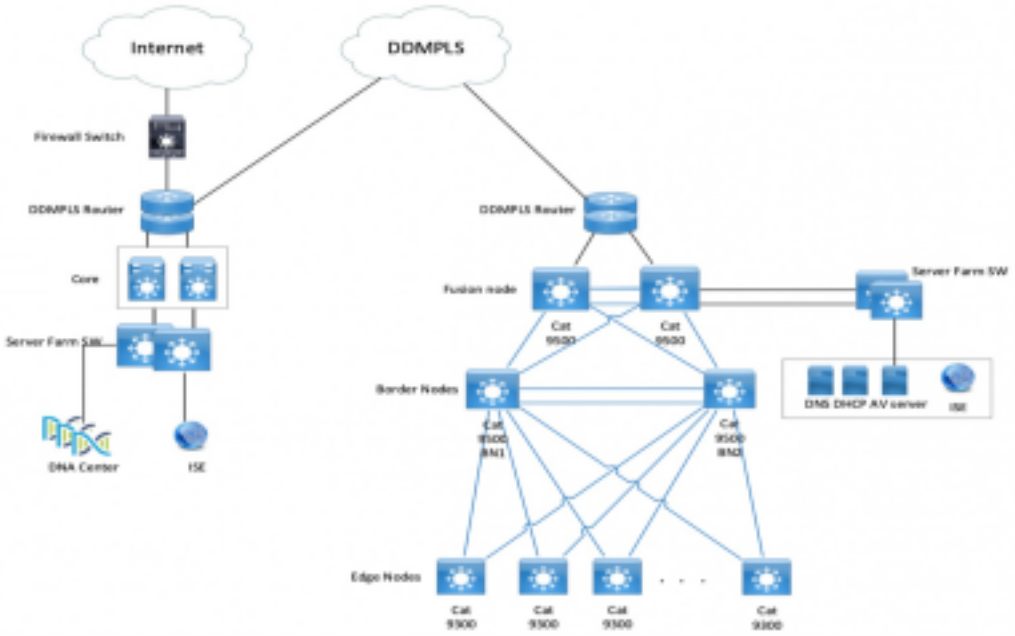
このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- IOS 16.9.3を使用した9300エッジおよび9500ボーダーノード（スイッチ）
- DNAC 1.3.0.5
- ISE 2.6パッチ3（2ノード – 冗長展開）
- DNACとISEを統合
- ボーダーノードとエッジノードは、DNACによってプロビジョニングされます
- SXPトンネルは、ISE（スピーカ）から両方の境界ノード（リスナー）に確立されます
- IPアドレスプールがホストオンボーディングに追加される

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

設定

ネットワーク図



コンフィギュレーション

許可リストモデル（デフォルトの拒否IP）を有効にする手順は、次のとおりです。

1. スイッチのSGTを[Unknown]から[TrustSec Devices]に変更します。
2. CTSロールベースの適用を無効にします。
3. DNACテンプレートを使用したボーダースイッチとエッジスイッチでのIP-SGTマッピング。
4. DNACテンプレートを使用したフォールバックSGACL。
5. Trustsec MatrixでAllow-List（デフォルトの拒否IP）を有効にします。
6. エンドポイント/ユーザのSGTを作成します。
7. エンドポイント/ユーザ用のSGACLの作成（実稼働オーバーレイトラフィック用）

ステップ1：スイッチSGTを[Unknown]から[TrustSec Devices]に変更します。

既定では、不明なセキュリティグループタグ(SGT)がネットワークデバイスの許可に設定されています。これをTrustSecデバイスSGTに変更すると、可視性が向上し、スイッチが開始するトラフィックに固有のSGACLを作成できます。

[Work Centers] > [TrustSec] > [Trustsec Policy] > [Network Device Authorization]に移動し、[Trustsec_Devices from Unknown]に変更します

ステップ2:CTSロールベースの適用を無効にします。

- 許可リストモデル（デフォルトの拒否）が設定されると、アンダーレイマルチキャストおよびブロードキャストトラフィック(Intermediate System-to-Intermediate System(IS-IS)、Bidirectional Forwarding Detection(BFD)、Secure Shell(SSH)トラフィックなど)がファブリック内でブロックされます。

- ファブリックエッジおよびボーダーに接続するすべてのTenGigポートは、次のコマンドで設定する必要があります。この場所では、このインターフェイスから開始され、このインターフェイスに着信するトラフィックは適用されません。

```
Interface tengigabitethernet 1/0/1

no cts role-based enforcement
```

注：これは、DNACで範囲テンプレートを使用して簡単に行うことができます。それ以外の場合は、すべてのスイッチについて、プロビジョニング中に手動で行う必要があります。次のスニペットは、DNACテンプレートを使用して行う方法を示しています。

```
interface range $uplink1

no cts role-based enforcement
```

DNACテンプレートの詳細については、*このドキュメント*のURLを参照してください。

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

ステップ3:DNACテンプレートを使用したボーダースイッチとエッジスイッチのIP-SGTマッピング。

ローカルIP-SGTマッピングは、すべてのISEがダウンした場合でもスイッチで使用できます。これにより、アンダーレイが起動し、重要なリソースへの接続が維持されます

最初のステップは、重要なサービスをSGT（例：Basic_Network_Services/1000）にバインドすることです。 これらのサービスには、次のものがあります。

- アンダーレイ/ISISサブネット
- ISE/DNAC
- モニタリングツール
- OTTの場合のAPのサブネット
- ターミナルサーバ
- 重要なサービス：例：IP フォン

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
```

ステップ4:DNACテンプレートを使用したSGACLのフォールバック。

SGTマッピングは、関連するSGACLがSGTを使用して作成されるまでは使用されないため、次のステップは、ISEノードがダウンした場合にローカルフォールバックとして機能するSGACLを作成することです（ISEサービスがダウンし、SGACLとIP SGTマッピングがががをダウンロードダウンロードされない））。

この設定は、すべてのエッジノードと境界ノードにプッシュされます。

フォールバックロールベースACL/コントラクト:

```
ip access-list role-based FALLBACK

permit ip
```

TrustSecデバイスからTrustSecデバイス：

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

SGACLの上ファブリックスイッチとアンダーレイIP内の通信を保証

SGT 1000へのTrustSecデバイス：

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

SGACLの上：スイッチとアクセスポイントからISE、DNAC、WLC、モニタリングツールへの通信を保証

SGT 1000からTrustSecデバイス：

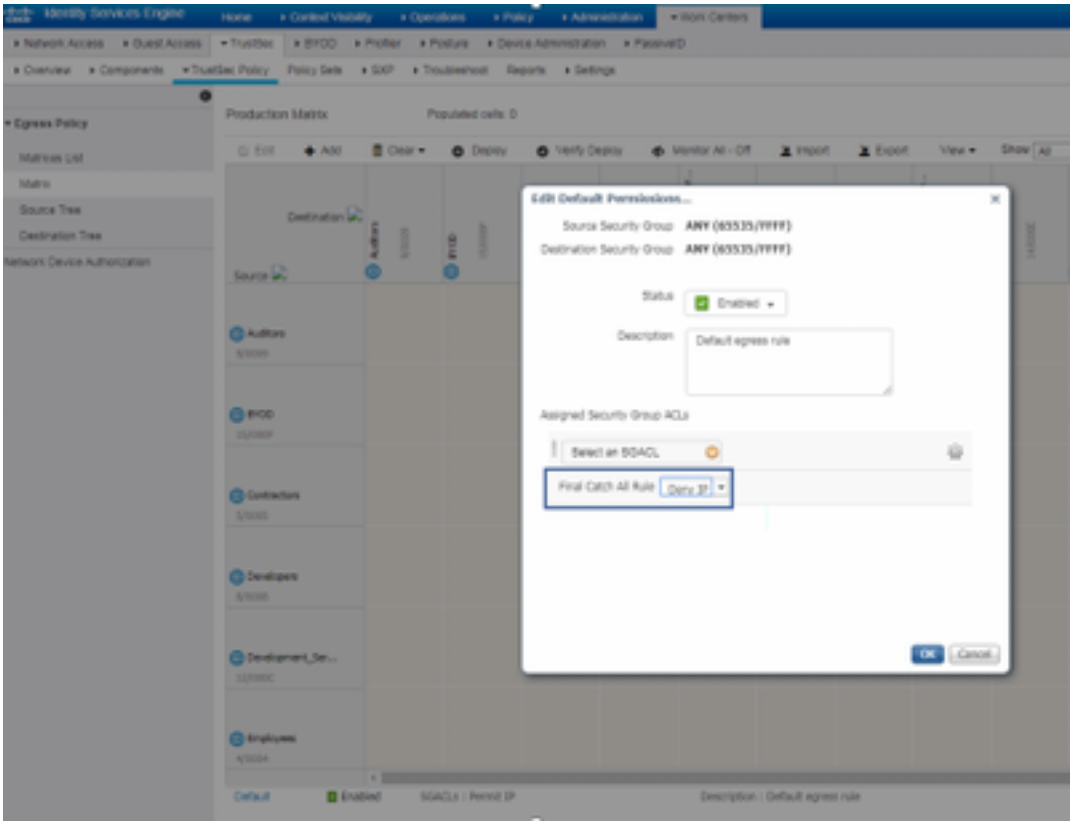
```
cts role-based permissions from 1000 to 2 FALLBACK
```

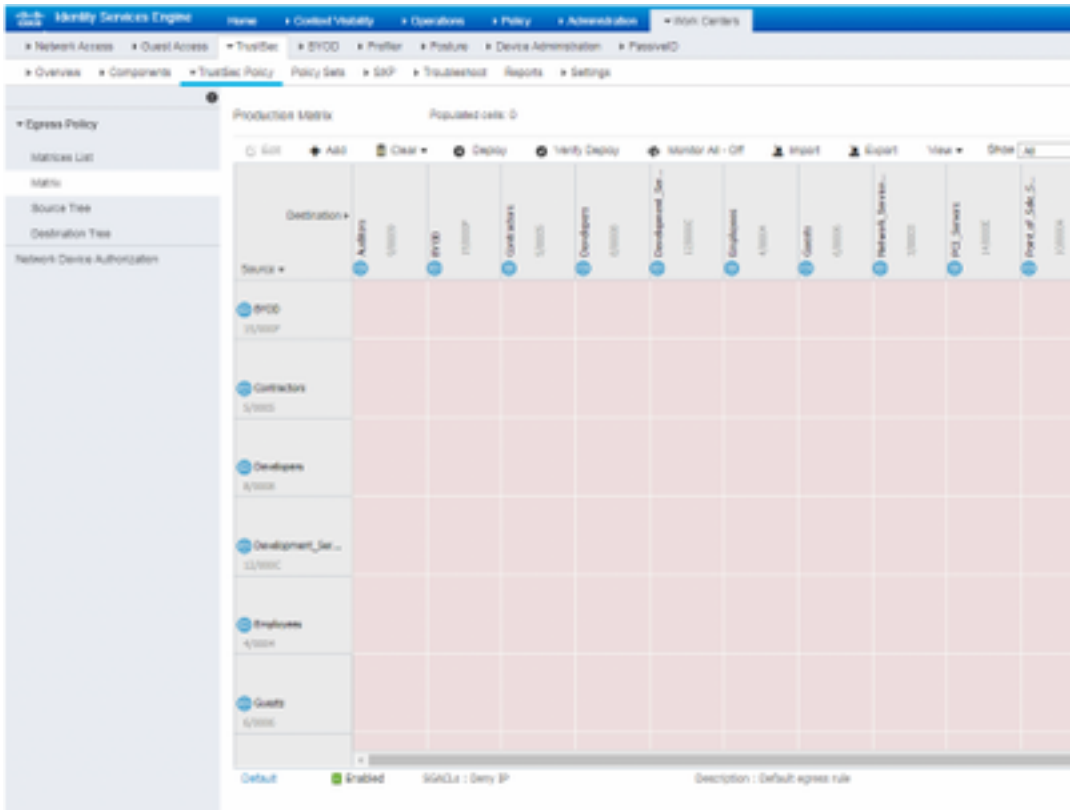
上記のSGACLアクセスポイントからISE、DNAC、WLC、およびモニタリングツールへのスイッチへの通信を保証

ステップ5:TrustSecマトリクスで許可リストモデル（デフォルトの拒否）を有効にします。

ネットワーク上のほとんどのトラフィックを拒否し、許可する範囲を小さくすることが要件です。明示的な許可ルールでdefault denyを使用すると、必要なポリシーが少なくなります。

[ワークセンター] > [Trustsec] > [TrustSecポリシー] > [マトリックス] > [デフォルト]に移動し、最終キャッチルールで[すべて]を拒否]に変更します。





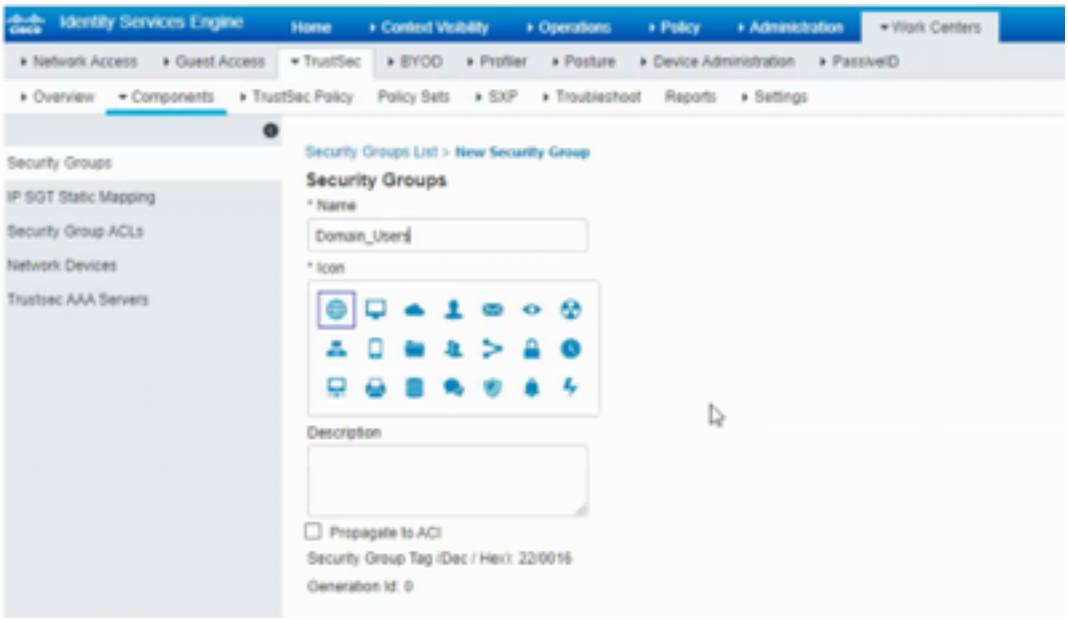
注：この図は（デフォルトでは、すべての列が赤で表示されます）、デフォルト拒否が有効になっており、SGACL作成後に許可できる選択的トラフィックのみ許可されます。

ステップ6：エンドポイント/ユーザのSGTを作成します。

SDA環境では、新しいSGTはDNAC GUIからのみ作成する必要があります。これは、ISE/DNACでのSGTデータベースの不一致が原因でデータベースが破損するケースが多数あるた

めです。

SGTを作成するには、[DNAC] > [Policy] > [Group-Based Access Control] > [Scalable Groups] > [Add Groups]にログインします。ページが[ISE Scalable Group]にリダイレクトされ、[Add]をクリックし、SGT名を入力して保存します。



同じSGTがPxGrid統合を通じてDNACに反映されます。これは、将来のすべてのSGTの作成で同じ手順です。

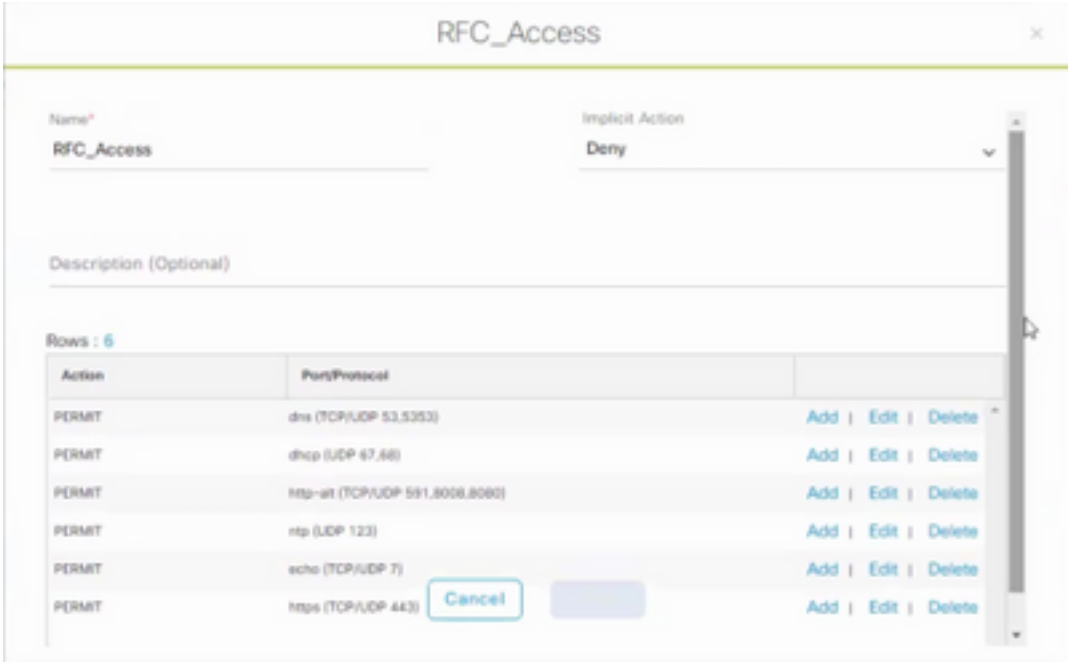
ステップ7：エンドポイント/ユーザのSGACLを作成します（実稼働オーバーレイトラフィック用）。

SDA環境では、新しいSGTはDNAC GUIからのみ作成する必要があります。

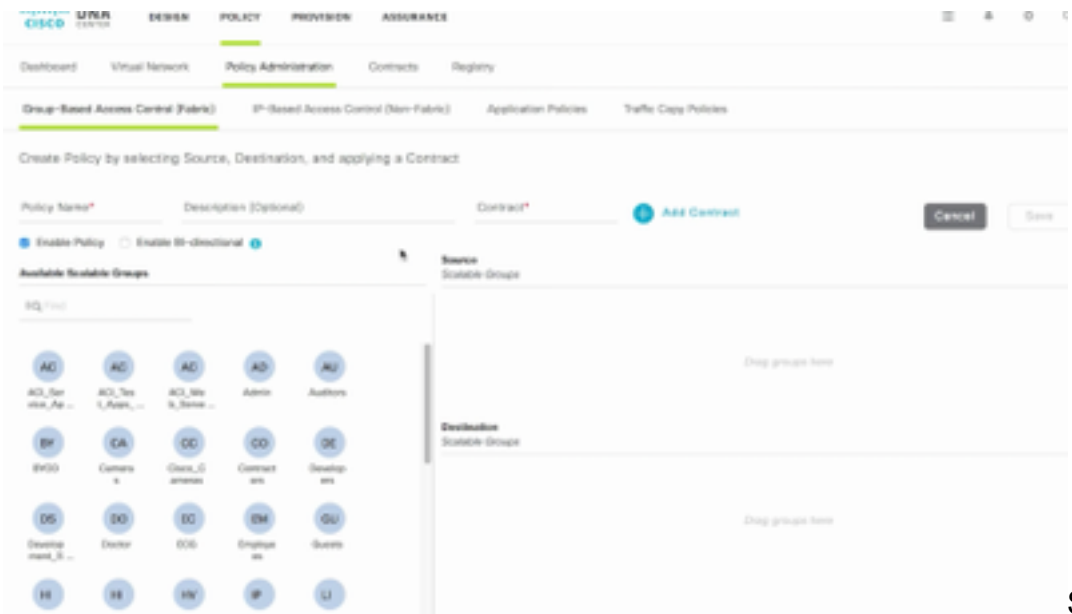
```
Policy Name: Domain_Users_Access

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)
```

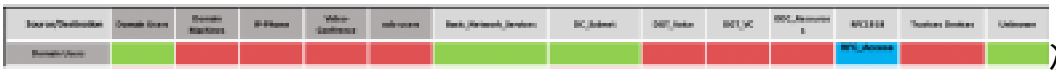
契約を作成するには、**DNACにログインし、[Policy] > [Contracts] > [Add Contracts] > [Add required protocol]**に移動し、[Save]をクリックします。



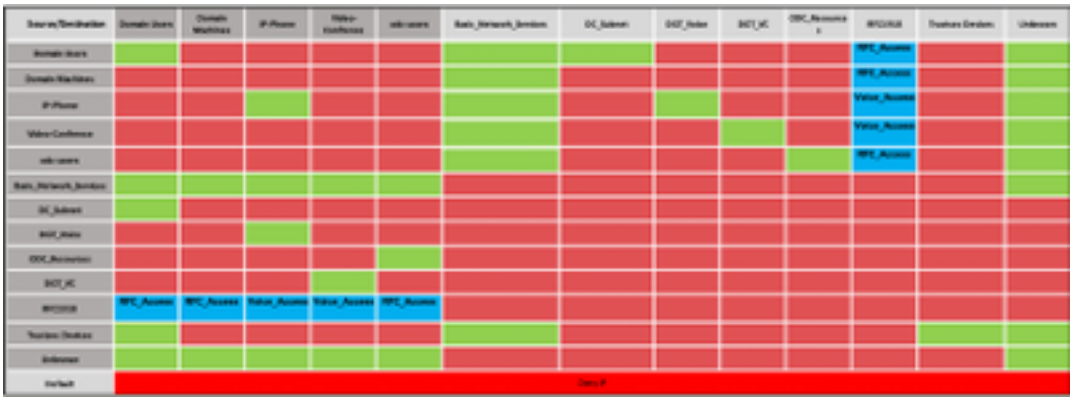
契約を作成するには、**DNACにログインし、[Policy] > [Group-Based Access Control] > [Group-Based-Access-Policies] > [Add Policies] > [Create policy（指定された情報を使用して）]**に移動し、[**Save** and **Deploy**].

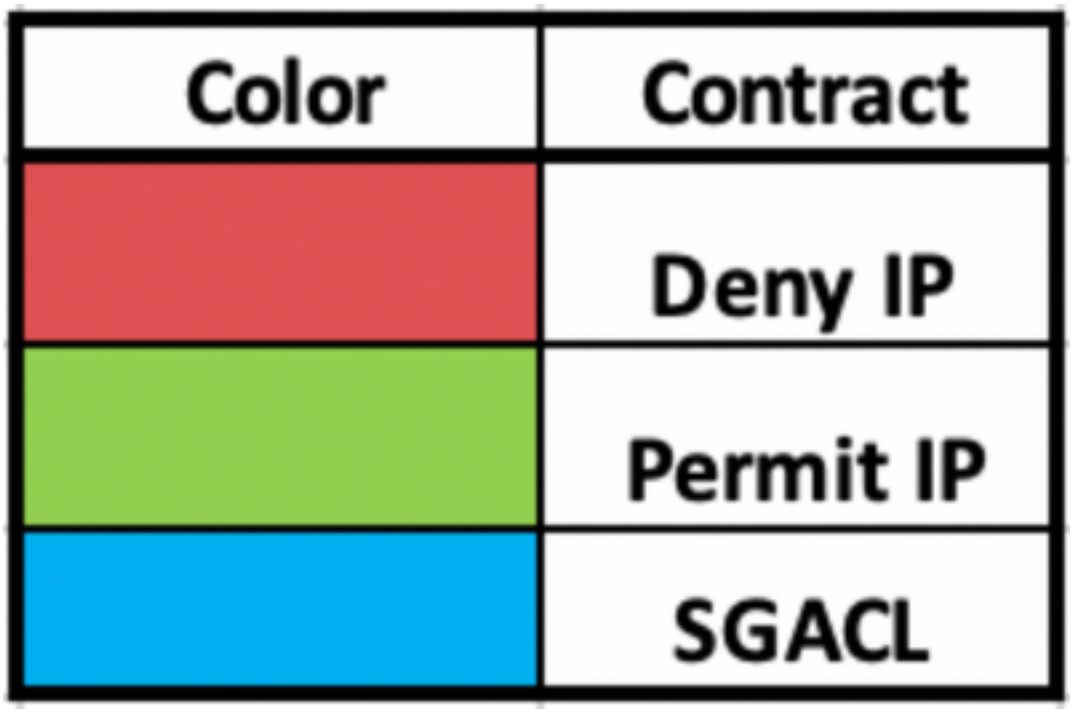


SGACL/コントラクトがDNACから設定されると、自動的にISEに反映されます。次に、sgtに対する一方向のmatrxビューの例を示します。



次の図に示すように、SGACL MatrixはAllow-list（デフォルトの拒否）モデルのビューの例です。





確認

ネットワークデバイスSGT

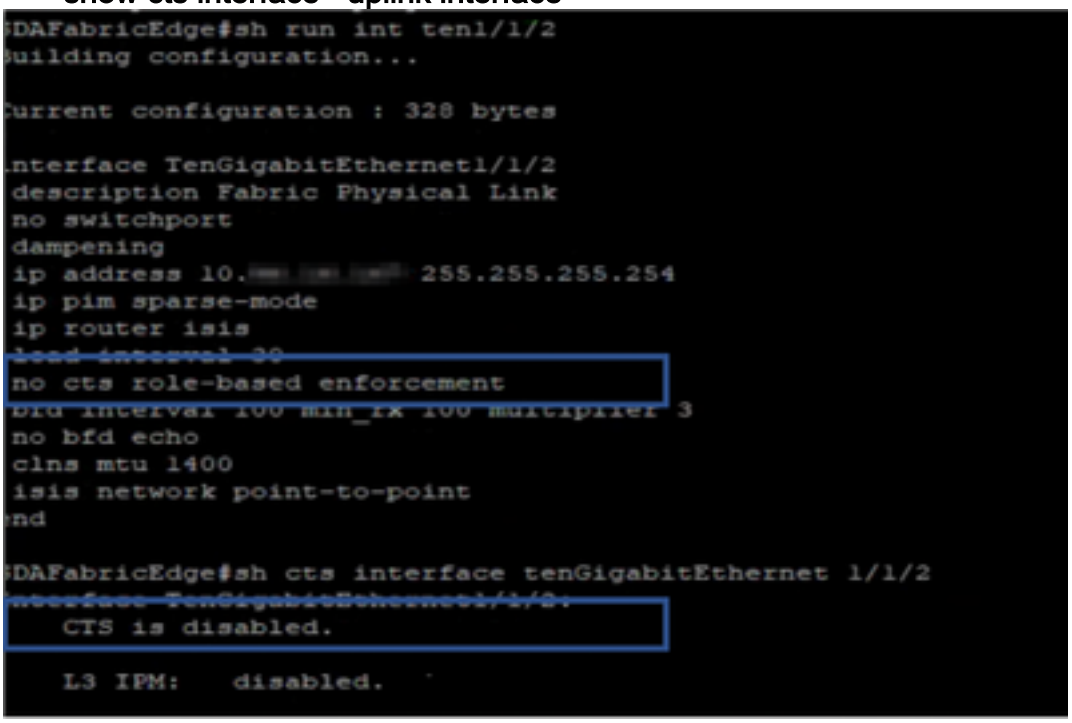
ISEが受信したスイッチのSGTを確認するには、次のコマンドを実行します。**show cts environmental-data**

```
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
```

アップリンクポートでの適用

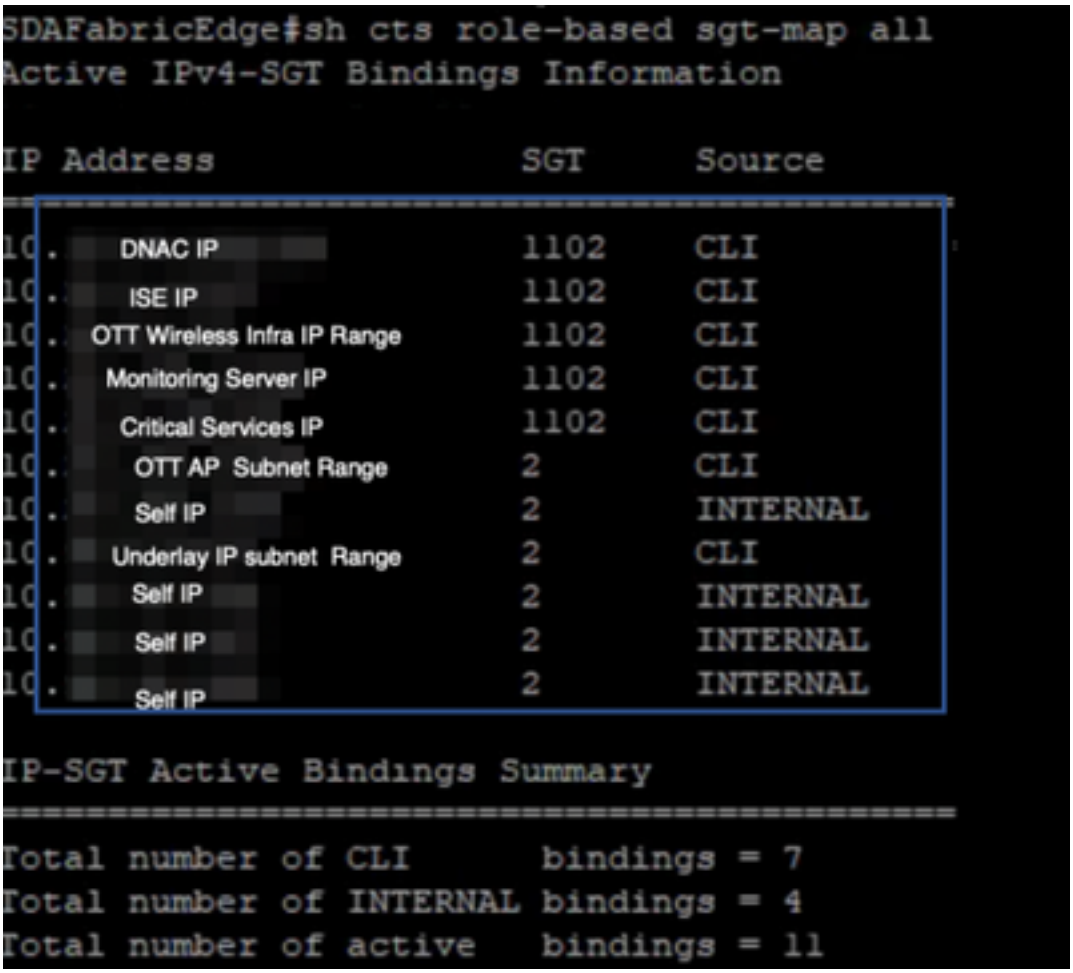
アップリンクインターフェイスでの適用を確認するには、次のコマンドを実行します。

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



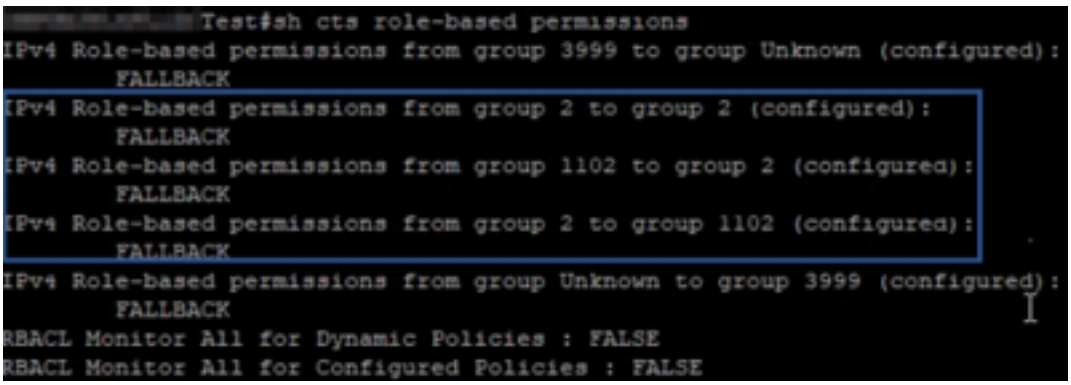
ローカルIP-SGTマッピング

ローカルに設定されたIP-SGTマッピングを確認するには、sh cts role-based sgt-map all



ローカルフォールバックSGACL

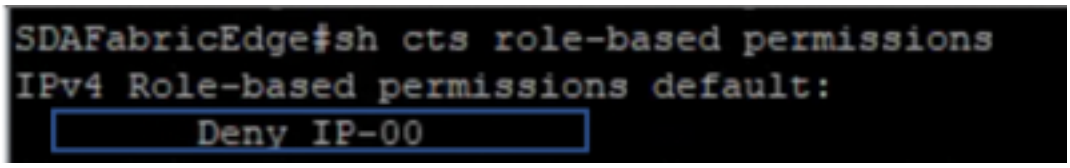
フォールバックSGACLを確認するには、sh cts role-based permission



注：ISEによってプッシュされるSGACLは、ローカルSGACLよりも優先されます。

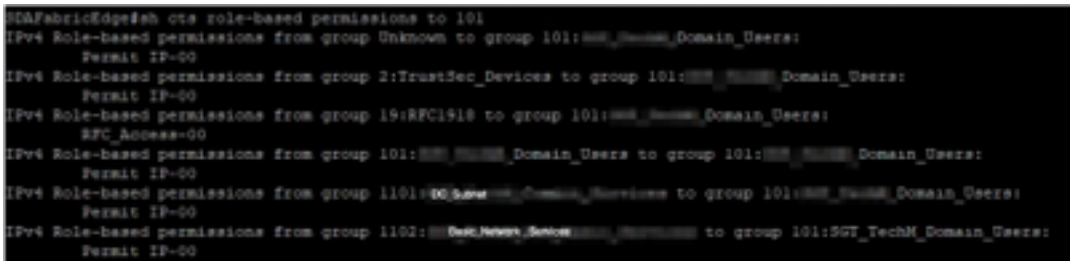
ファブリックスイッチでの許可リスト（デフォルトの拒否）の有効化

許可リスト（デフォルトの拒否）モデルを確認するには、sh cts role-based permission



ファブリックに接続されたエンドポイントのSGACL

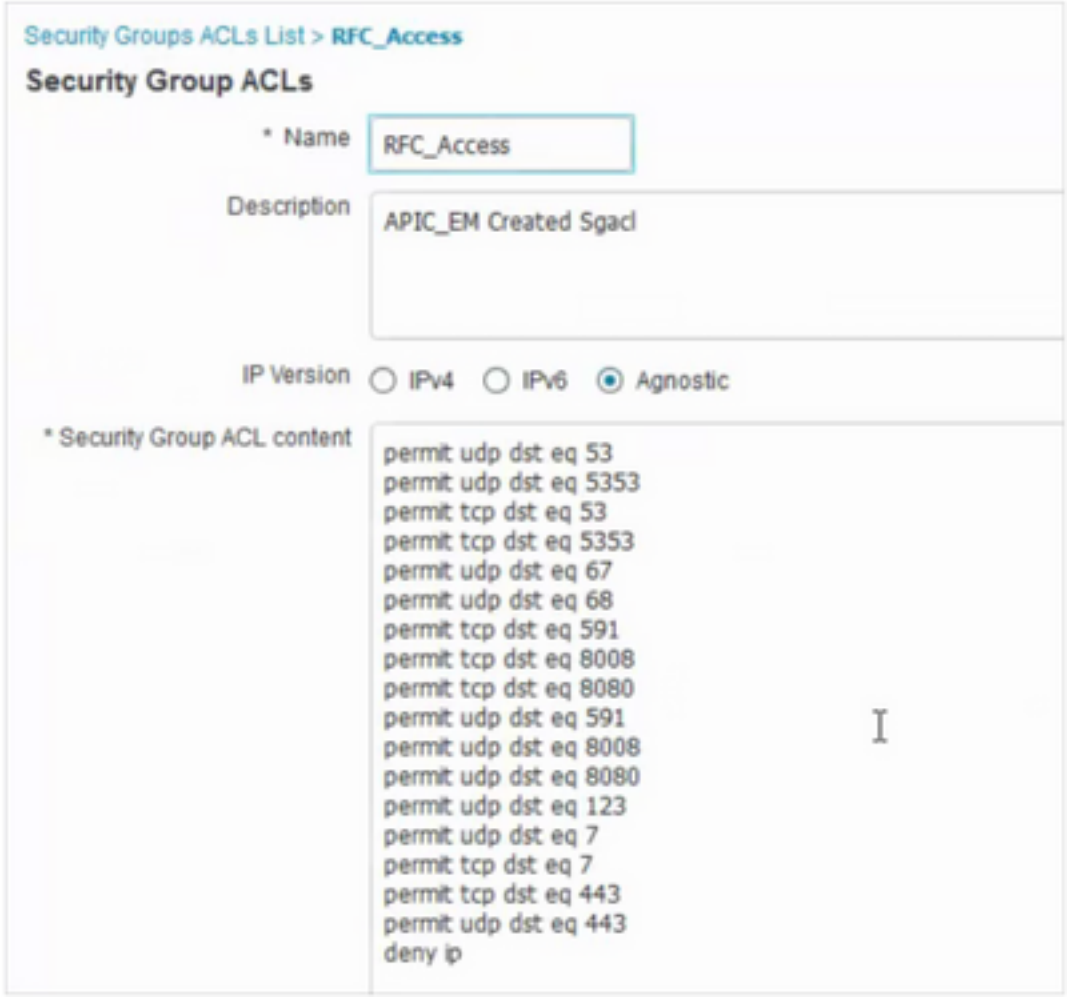
ISEからダウンロードしたSGACLを確認するには、sh cts role-based permission



DNACによって作成された契約の確認

ISEからダウンロードしたSGACLを確認するには、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
```



ファブリックスイッチのアンダーレイSGACLカウンタ

SGACLポリシーのヒットを確認するには、次のコマンドを実行します： **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
```

トラブルシュート

問題1：両方のISEノードがダウンした場合。

両方のISEノードがダウンした場合、ISEが受信したIP-to-SGTマッピングが削除され、すべてのDGTが不明としてタグ付けされ、存在するすべてのユーザセッションが5 ~ 6分後に停止します。

> **注**：この問題は、sgt (xxxx) -> unknown (0) SGACLアクセスがDHCP、DNS、およびWebプロキシポートに制限されている場合にのみ適用されます。

ソリューション：

1. SGTの作成(例：RFC1918)。
2. RFCプライベートIP範囲を両方の境界にプッシュします。
3. sgt(xxxx) —> RFC1918からのDHCP、DNS、およびWebプロキシへのアクセスを制限します
4. sgacl sgt(xxxx) —>不明を作成/変更し、Permit IP契約を伴います。

これで、両方のiseノードがダウンした場合、SGACL sgt—>unknown hitsが発生し、存在するセッションはそのまま残ります。

問題2:IP Phoneの片通話または音声なし

SIPで内線番号からIPへの変換が行われ、IPからIPへのRTP経由で実際の音声通信が行われます。CUCMと音声ゲートウェイが**DGT_Voice**に追加さ**れました**。

ソリューション：

1. IP_Phone —> IP_Phoneからのトラフィックを許可することで、同じ場所または水平方向の音声通信を有効にできます。
2. 残りの場所は、DGT RFC1918のAllowing RTP protocol rangeで許可できます。同じ範囲はIP_Phone —> Unknownで許可できます。

問題3：重要なVLANエンドポイントにネットワークアクセスがない。

DNACは、データ用の重要なVLANでスイッチをプロビジョニングし、設定に従って、ISEの停止中のすべての新しい接続が重要なVLANとSGT 3999を取得します。Default Deny in trustsecポリシーは、ネットワークリソースにアクセスするための新しい接続を制限します。

ソリューション：

DNACテンプレートを使用して、すべてのエッジスイッチおよびボーダースイッチの重要なSGTにSGACLをプッシュ

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

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

これらのコマンドは、設定セクションに追加されています。

> **注**：すべてのコマンドを1つのテンプレートに組み合わせて、プロビジョニング中にプッシュできます。

問題4：パケットドロップインクリティカルVLAN

ISEノードのダウンによりマシンが重要なVLANに入ると、重要なVLANのすべてのエンドポイントに対して3 ~ 4分ごとにパケットがドロップされます（最大10個のドロップが観察されます）。

観察:サーバがDEADになると、認証カウンタが増加します。サーバがDEADとマークされたときに、クライアントはPSNで認証を試みます。

ソリューションと回避策：

理想的には、ISE PSNノードがダウンしている場合は、エンドポイントからの認証要求を行う必要はありません。

DNACを使用するradiusサーバで次のコマンドをプッシュします。

automate-tester username auto-test probe-on

スイッチでこのコマンドを使用すると、定期的にテスト認証メッセージがRADIUSサーバに送信されます。サーバからのRADIUS応答を検索します。成功メッセージは必要ありません。サーバが動作していることを示すため、認証に失敗しても十分です。

追加情報

DNAC最終テンプレート：

```
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
```

注：エッジノード内のすべてのアップリンクインターフェイスは強制なしで設定され、アップリンクはボーダーノードのみに接続すると仮定されます。ボーダーノードでは、エッジノードへのアップリンクインターフェイスを強制なしで設定する必要があり、手動で設定する必要があります。