SGACL モニタモードおよび SGACL ロギングの設定

SGACL モニタモードおよび SGACL ロギングは、Cisco IOS リリース 15.2(8)E 以降の IE 4000、IE 4010、および IE 5000 シリーズ スイッチでサポートされています。

セキュリティグループベースのアクセスコントロールは Cisco TrustSec セキュリティアーキテクチャのコンポートで、信頼できるネットワークデバイスのドメインを確立することによってセキュアネットワークを構築します。TrustSec の前提条件、ガイドラインと制限事項、設定手順など、TrustSec に関する包括的な情報については、『Cisco TrustSec Switch Configuration Guide』を参照してください。SGT 交換プロトコル over TCP（SXP）およびレイヤ 3 トランスポートの設定については、SGT 交換プロトコル over TCP（SXP）およびレイヤ 3 トランスポートの設定（285 ページ）を参照してください。

SGACL モニタ モード

Cisco TrustSec の事前導入段階で、モニタモードを使用して、ポリシーが意図したとおりに機能することを確認するために、セキュリティポリシーを適用しない状態でテストすることができます。セキュリティポリシーが意図したとおりに機能しない場合、モニタモードでそのことが特定され、セキュリティ グループ アクセス コントロール リスト（SGACL）の適用をイネーブルにする前にポリシーを修正できます。ポリシーを適用する前にポリシーアクションの結果を確認することで、対象のポリシーがセキュリティ要件を満たしている（ユーザが認証されなければリソースへのアクセスは拒否される）ことを確認できます。

モニタリング機能は、SGT-DGT ペア レベルで提供されます。SGACL モニタ モード機能を有効にすると、拒否アクションがライン カード上の ACL 許可として実装されます。これにより、SGACL カウンタおよびロギングでは、接続が SGACL ポリシーによりどう処理されているかを表示できます。すべてのモニタ対象トラフィックが許可されるため、SGACL モニタモードでは、SGACL によるサービスの中断はありません。

SGACL モニタモードを有効にするには、IPServices ライセンスが必要です。

SGACL モニタモードの設定 - CLI

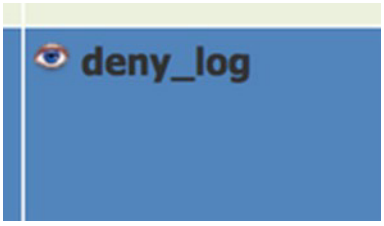
CLI を使用して SGACL モニタモードを設定するには、次の手順を実行します。

	コマンド	目的
1.	`Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
2.	`Switch(config)#cts role-based monitor enable`	モニタモードを有効にします。
3.	`Switch(config)# cts role-based monitor permissions from { sgt_num } to { dgt_num } ipv4`	IPv4 RBACL（SGT-DGT ペア）のモニタモードを有効にします。
4.	`Switch(config)# exit`	コンフィギュレーション モードを終了します。
5.	`Switch# show cts role-based permissions from { sgt_num } to { dgt_num } ipv4 [ details ]`	（任意）SGACL ポリシーとペアごとのモニタモード機能に関する詳細を表示します。<SGT-DGT> ペアでセルごとのモニタモードが有効になっている場合、コマンド出力には「モニタ対象」が表示されます。

SGACL モニタモードの設定 - Radius（ISE）

Cisco Identity Services Engine（ISE）GUI を使用して SGACL モニタモードを有効にするには、次のように [モニタ（Monitor）] を選択します。

目のアイコンは、モニタモードが有効であることを示します。



ポリシーマトリックスの変更は、マトリックスの上部にある展開機能を使用してネットワークデバイスにプッシュされる必要があります。これは、RADIUS CoA を使用して、変更が行われたことをデバイスに通知します。

更新がスイッチにダウンロードされたら、**show cts role-based Permissions** コマンドを使用して設定を確認します。ポリシーの権限は、「モニタ対象」という用語を追加することで、モニタモードの特定のポリシーを示します。

設定の確認

次に、**show cts role-based Permissions** コマンドと **show cts role-based counters** コマンドの出力例を示します。これらのコマンドを使用して、SGACL モニタモードのステータスを表示できます。

```
Switch#show cts role-based permissions
IPv4 Role-based permissions default:
        Permit IP-00
IPv4 Role-based permissions from group 18:HVAC to group 14:PCI_Servers (monitored):
        deny_log-10
RBACL Monitor All for Dynamic Policies : FALSE
RBACL Monitor All for Configured Policies : FALSE
```

show cts role-based カウンタの HW-Monitor カラムには、ハードウェアでモニタされているが実際には適用されていない適用イベントの数が表示されます。

```
Switch#show cts role-based counters
Role-based IPv4 counters
From    To      SW-Denied  HW-Denied  SW-Permitt HW-Permitt SW-Monitor HW-Monitor
*       *       0          0          5378613    6291011    0          0
18      14      0          0          0          0          0          84
```

SGACL ロギング

cts の **log** オプションは個々の ACE に適用され、ACE に一致するパケットがログに記録されます。**log** キーワードで記録された最初のパケットは、syslog メッセージを生成します。

SGACL ロギングは、Cisco ACE アプリケーション コントロール エンジンに **logging** キーワードがある場合にのみトリガーされます。

SGACL でロギングが有効になっている場合、スイッチは次の情報を記録します。

- 送信元セキュリティグループタグ（SGT）および宛先 SGT
- SGACL ポリシー名
- パケットプロトコルタイプ
- パケットで実行されるアクション

Cisco TrustSec ロールベース（セキュリティグループ）アクセスコントロール適用を有効にするには、グローバル コンフィギュレーション モードで **cts role-based enforcement** コマンドを使用します。SGACL のロギング間隔を設定するには、次のように入力します。

cts role-based enforcement [**logging-interval** *interval*]

interval 引数の有効な値は 5 ～ 86400 秒です。デフォルトは 300 秒です。

ロギングを有効にするには、SGACL 構成の ACE 定義の前に **log** キーワードを使用します。たとえば、**permit ip log** などです。

次に、送信元と宛先の SGT、ACE の一致（拒否アクション）を表示するサンプルログを示します。**logging rate-limit** コマンドを使用して、1 秒あたりに記録されるメッセージのレートを制限できます。

```
Switch(config)# cts role-based enforcement logging-interval 90
Switch(config)# logging rate-limit

May 27 10:19:21.509: %RBM-6-SGACLHIT:
ingress_interface='GigabitEthernet1/0/2' sgacl_name='sgacl2' action='Deny'
protocol='icmp' src-ip='16.16.1.3' src-port='8' dest-ip='17.17.1.2' dest-port='0'
sgt = '101' dgt = '202' logging_interval_hits = '5'
```