CTS SGACL のサポート

CTS SGACL のサポート機能は、IP アドレスではなく、セキュリティ アソシエーションまたはセキュリティ グループ タグ値に基づいたステートレスのアクセス制御メカニズムを提供します。

CTS SGACL サポートの前提条件

CTS SGACL サポートについては、Protected Access Credential（PAC）と環境データのダウンロードが、ダイナミック SGACL のデバイスで設定されていること。

CTS SGACL サポートの制約事項

- プラットフォームあたりでサポートされている TrustSec 機能のリストおよび IOS リリースの最小要件については、次の URL の Cisco TrustSec プラットフォーム サポート マトリックス [英語] を参照してください：http://www.cisco.com/en/US/solutions/ns170/ns896/ns1051/trustsec_matrix.html
- SGACL の適用は、管理インターフェイスではサポートされていません。
- ダイナミック SGACL のダウンロード サイズは、6 KB に制限されています。
- Port-Channel インターフェイスの SGACL 適用は検証されていません。

- VRF aware SGT 設定では、Cisco IOS XE Denali 16.3 は、VRF 管理インターフェイスではありませんが、ISE 通信をサポートしています。管理インターフェイスを通じた ISE 通信はサポートされていません。
- 6 KB の拡張制限は、ダイナミック SGACL のみです。スタティック SGACL は、256*256 マトリックスのような高い拡張性をサポートできます。
- SGACL の適用は、リンクローカル IPv6 送信元/宛先アドレスを持つ IPv6 パケットについてはバイパスされます。
- IPv6 マルチキャストトラフィックの SGACL 適用はバイパスされます。
- Cisco IOS XE Bengaluru 17.4.1 以降では、VRF を認識するように自動テスターを設定できます。**automate-tester** コマンドで **vrf** キーワードを使用すると、デフォルト以外の VRF の自動テスト機能を有効化します。

（注） VRF 対応の自動テスターを機能させるには、**global config ipv4/ipv6 source interface** *interface-name* **vrf** *vrf-name* コマンドを設定する必要があります。

CTS SGACL サポートに関する情報

CTS SGACL のサポート

セキュリティ グループ アクセス コントロール リスト（SGACL）はポリシーの適用です。これによって管理者は、セキュリティグループの割り当てと宛先リソースに基づいてユーザが実行する操作を制御できます。Cisco TrustSec ドメイン内のポリシーの適用は、軸の 1 つが送信元セキュリティ グループ番号、もう 1 つの軸が宛先セキュリティ グループ番号である、アクセス許可マトリックスで表示されます。マトリックス内の各セルには、SGACL の番号付きリストが含まれます。ここでは、送信元セキュリティ グループに属し宛先セキュリティ グループに属する宛先 IP を持つ、IP から送信されるパケットに適用される必要があるアクセス権限を指定します。

SGACL は、IP アドレスではなく、セキュリティ アソシエーションまたはセキュリティ グループ タグ値に基づいたステートレスのアクセス制御メカニズムを提供し、一致クラスに基づいてトラフィックをフィルタリングします。SGACL ポリシーをプロビジョニングするには、次の 3 つの方法があります。

- スタティック ポリシー プロビジョニング：**cts role-based permission** コマンドを使用して、ユーザーが SGACL ポリシーを定義します。
- ダイナミック ポリシー プロビジョニング：SGACL ポリシーの設定は、Cisco Secure ACS または Cisco Identity Services Engine の主にポリシー管理機能によって実行する必要があります。後者については『Cisco Identity Services Engine User Guide』を参照してください。

- 認可変更（CoA）：更新されたポリシーは、SGACL ポリシーが ISE で変更され、CoA が CTS デバイスにプッシュされるとダウンロードされます。

SGACL モニター モード

Cisco TrustSec の事前導入段階で、管理者は、モニターモードを使用して、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します。セキュリティポリシーが意図したとおり機能しない場合には、モニターモードが、その問題を識別するための便利なメカニズムと、SGACL の適用を有効にする前にポリシーを修正する機会を提供します。これにより、管理者は、ポリシーを適用する前にポリシーアクションの結果をより可視的に確認でき、対象のポリシーがセキュリティ要件を満たしている（ユーザー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 モニター 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。すべてのモニター対象トラフィックが許可されるため、SGACLモニターモードでは、SGACL によるサービスの中断はありません。

CTS SGACL サポートの設定方法

SGACL ポリシーの適用のグローバルな有効化

Cisco TrustSec 対応ルーテッドインターフェイスの SGACL ポリシーの強制を有効化するには、次のタスクを実行します。

```
enable
configure terminal
cts role-based enforcement
```

インターフェイスあたりの SGACL ポリシーの適用の有効化

cts role-based enforcement コマンドを使用すると、SGACL のグローバルな適用を有効にして、特定のインターフェイスでは無効にすることができます。また、SGACL の適用は、グローバルで有効化しなくても、特定のインターフェイスで有効化できます。

インターフェイスでの SGACL ポリシーの適用を有効化するには、次のタスクを実行します。

```
enable
configure terminal
interface GigabitEthernet 0/1/1
cts role-based enforcement
```

IPv6 SGACL アクセス制御エントリの設定

SGACL は、次のコマンドを使用して、拡張名前付き ACL と同様に定義されます。

```
Device(config)#ipv6 access-list role-based sgacl1
IPV6 Role-based Access List Configuration commands:
  default   Set a command to its defaults
  deny      Specify packets to reject
  exit      Exit from access-list configuration mode
  no        Negate a command or set its defaults
  permit    Specify packets to forward
  remark    Access list entry comment
  sequence  Sequence number for this entry
```

権限マトリックスセルへの SGACL のアタッチ

```
Device(config)#cts role-based permissions from 100 to 200
  WORD  Role-based Access-list name
  ipv4  Protocol Version - IPv4
  ipv6  Protocol Version - IPv6
```

このコマンドは、特定 <SGT, DGT> ペアの RBACL のリストを定義、置換、または削除します。このポリシーは、同じ SGT、DGT に対するダイナミックなポリシーがない場合に有効になります。デフォルトでは、IPv4 タイプの RBACL のみをアタッチできます。IPv6 SGACL を追加するには、**ipv6** を明示的に指定します。

SGACL ポリシーの手動設定

SGACL ポリシーを手動で設定するには、次のタスクを実行します。

```
enable
configure terminal
ip access-list role-based allow_webtraff
10 permit tcp dst eq 80
20 permit tcp dst eq 443
cts role-based permissions from 55 to 66 allow_webtraff
end
```

ダウンロードされた SGACL ポリシーのリフレッシュ

ダウンロードされた SGACL ポリシーを更新するには、次のタスクを実行します。

```
enable
cts refresh policy
```

または

```
enable
```

```
cts refresh policy sgt 10
```

SGACL モニター モードの設定

SGACL モニターモードを設定する前に、Cisco TrustSec が有効になっていることを確認してください。

（注） デバイスレベルのモニターモードは、いずれかの設定が適用されないかぎり、デフォルトでは有効になりません。ISE からダウンロードされた SGACL の場合、ISE からのモニターモードの状態が常に優先されます。これは、セルごとのモニターモードと、すべてのセルに適用されるグローバルモニターモードの両方に適用されます。

```
configure terminal
cts role-based monitor enable
cts role-based monitor permissions from 2 to 3 ipv4
show cts role-based permissions from 2 to 3 ipv4
show cts role-based counters ipv4
```

IPv6 SGACL ACE の設定

IPv6 SGACL のアクセス制御エントリ（ACE）を定義するには、次の CLI が使用されます。

```
Device(config)#ipv6 access-list role-based sgacl1
Device(config-ipv6rb-acl)#permit ipv6
Device(config-ipv6rb-acl)#exit
Device(config)#cts role-based permissions from 100 to 200 ipv6 sgacl1
```

（注） IPv6 ACL 設定はスタティック SGACL 用であり、ダイナミック SGACL の場合は、ACE が ISE で設定されます。

CTS SGACL サポートの設定例

例：CTS SGACL のサポート

次に、show cts role-based permissions コマンドの出力例を示します。

```
Router# show cts role-based permissions

IPv4 Role-based permissions default:
        default_sgacl-02
```

```
        Permit IP-00
IPv4 Role-based permissions from group 55:SGT_55 to group 66:SGT_66 (configured):
        allow_webtraff
RBACL Monitor All for Dynamic Policies : FALSE
RBACL Monitor All for Configured Policies : FALSE


Router#sh cts role-based permissions ipv6
IPv6 Role-based permissions from group 2103:Cisco_UC_Servers to group
2104:Exchange_Servers:
        SGACL_5-10-ipv6
RBACL Monitor All for Dynamic Policies : FALSE
RBACL Monitor All for Configured Policies : FALSE
```

次に、ダイナミック SGACL にのみ適用される show cts policy sgt コマンドの出力例を示します。

```
Router# show cts policy sgt

CTS SGT Policy
==============
RBACL Monitor All : FALSE
RBACL IP Version Supported: IPv4
SGT: 0-02:Unknown
SGT Policy Flag: 0xc1408801
RBACL Source List: Empty
RBACL Destination List: Not exist
RBACL Multicast List: Not exist
RBACL Policy Lifetime = 1800 secs
RBACL Policy Last update time = 20:58:28 IST Wed Jul 13 2016
Policy expires in 0:00:24:05 (dd:hr:mm:sec)
Policy refreshes in 0:00:24:05 (dd:hr:mm:sec)
Cache data applied = NONE

SGT: 65535-46:ANY
SGT Policy Flag: 0x41400001
RBACL Source List:
  Source SGT: 65535-46:ANY-0, Destination SGT: 65535-46:ANY-0
  rbacl_type = 80
  rbacl_index = 1
  name   = default_sgacl-02
  IP protocol version = IPV4
  refcnt = 1
  flag   = 0x40000000
  stale  = FALSE
  RBACL ACEs:
    permit icmp
    permit ip
  Source SGT: 65535-46:ANY-0, Destination SGT: 65535-46:ANY-0
  rbacl_type = 80
  rbacl_index = 2
  name   = Permit IP-00
  IP protocol version = IPV4
  refcnt = 1
  flag   = 0x40000000
  stale  = FALSE
  RBACL ACEs:
    permit ip
RBACL Destination List: Not exist
RBACL Multicast List: Not exist
RBACL Policy Lifetime = 1800 secs
```

```
RBACL Policy Last update time = 20:58:28 IST Wed Jul 13 2016
Policy expires in 0:00:24:05 (dd:hr:mm:sec)
Policy refreshes in 0:00:24:05 (dd:hr:mm:sec)
Cache data applied = NONE
```

次に、ダイナミック SGACL にのみ適用される show cts rbacl コマンドの出力例を示します。

```
Router# show cts rbacl

CTS RBACL Policy
================
RBACL IP Version Supported: IPv4 & IPv6
  name   =multple_ace-16
  IP protocol version = IPV4
  refcnt = 4
  flag = 0x40000000
  stale = FALSE
  RBACL ACEs:
      permit icmp
      deny tcp

  name   =default_sgacl-02
  IP protocol version = IPV4
  refcnt = 2
  flag = 0x40000000
  stale = FALSE
  RBACL ACEs:
      permit icmp
      permit ip

  name   =SGACL_256_ACE-71
  IP protocol version = IPV4
```

例：SGACL モニターモードの設定

次に、SGACL モニターモードの設定例を示します。

```
Device# configure terminal
Device(config)# cts role-based monitor enable
Device(config)# cts role-based permissions from 2 to 3 ipv4
Device# show cts role-based permissions from 2 to 3 ipv4

        IPv4 Role-based permissions from group 2:sgt2 to group 3:sgt3 (monitored):
        denytcpudpicmp-10
        Deny IP-00

Device# show cts role-based permissions from 2 to 3 ipv4 details

        IPv4 Role-based permissions from group 2:sgt2 to group 3:sgt3 (monitored):
        denytcpudpicmp-10
        Deny IP-00
        Details:
        Role-based IP access list denytcpudpicmp-10 (downloaded)
        10 deny tcp
```

```
        20 deny udp
        30 deny icmp
        Role-based IP access list Permit IP-00 (downloaded)
        10 permit ip
Device# show cts role-based permissions ipv6
IPv6 Role-based permissions from group 201 to group 22 (configured):
        g6
IPv6 Role-based permissions from group 100 to group 200 (configured):
        sgacl1
RBACL Monitor All for Dynamic Policies : FALSE
RBACL Monitor All for Configured Policies : FALSE

Device# show cts role-based counters ipv4
Role-based IPv4 counters
From    To      SW-Denied  HW-Denied  SW-Permitt HW-Permitt SW-Monitor HW-Monitor
100     200     0          0          0          0          0          0
101     201     0          0          0          0          0          0

Device# show cts role-based counters ipv6
Role-based IPv6 counters
From    To      SW-Denied  HW-Denied  SW-Permitt HW-Permitt SW-Monitor HW-Monitor
201     22      0          0          0          0          0          0
100     200     0          0          0          0          0          0
```

例：ダウンロードされた SGACL ポリシーのリフレッシュ

次に、ダウンロードした SGACL ポリシーをリフレッシュするための設定例を示します。このコマンドは特権 EXEC モードで実行されます。

```
Router#cts refresh policy
Router#cts refresh policy sgt
```

CTS SGACL サポートに関する追加情報

関連資料

MIB

MIB	MIB のリンク
CISCO-MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

CTS SGACL サポートの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *1 : CTS SGACL* サポートの機能情報

機能名	リリース	機能情報
CTS SGACL のサポート	Cisco IOS Release 16.3	CTS SGACL のサポート機能は、IP アドレスではなく、セキュリティ アソシエーションまたはセキュリティ グループ タグ値に基づいたステートレスのアクセス制御メカニズムを提供します。 Cisco IOS リリース 16.3 では、この機能は、シスコ アグリゲーション サービス ルータ 1000 シリーズとサービス統合型ルータ 4000 シリーズに導入されました。 この機能により、次のコマンドが導入されました。**cts role-based enforcement, ip access-list role-based, cts role-based permissions, show cts role-based permissions, show cts rbacl**。

機能名	リリース	機能情報
TrustSec SGACL モニターモード	Cisco IOS XE Everest 16.4.1	TrustSec SGACL モニターモード機能は、ポリシーが意図したとおりに機能することを強制することなく、セキュリティポリシーをモニターします。モニターモードは、機能しないセキュリティポリシーを識別するための便利なメカニズムと、SGACL の適用を有効にする前にポリシーを修正する機会を提供します。 この機能により、次のコマンドが導入されました。**cts role-based monitor enable, cts role-based monitor permissions**。
IPv6 の有効化：SGACL の適用	Cisco IOS XE Fuji 16.8.1	IPv6 のサポートが導入されました。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。