Cisco TrustSec SGT キャッシング

Cisco TrustSec SGT キャッシング 機能は、セキュリティグループタグ（SGT）の移動性を柔軟にする Cisco TrustSec の機能を強化します。この機能は、IP-SGT バインドを特定し、対応する SGT をキャッシュすることで、通常のディープ パケット インスペクションを処理するすべてのネットワーク サービスを通じて、またパケットが該当する SGT で再度タグ付けされるサービス出力ポイントにおいて、ネットワーク パケットを転送します。

Cisco TrustSec SGT キャッシング の制約事項

グローバルなセキュリティ グループ タグ（SGT）キャッシング設定と、インターフェイス固有の入力設定は相互に排他的です。次のシナリオでは、SGT キャッシングをグローバルおよびインターフェイス上の両方で構成しようとした場合に、警告メッセージが表示されます。

- **cts role-based sgt-cache ingress** コマンドをインターフェイス設定モードで使用して、インターフェイスが入力 SGT キャッシングを有効にし、**cts role-based sgt-caching** コマンドを使用してグローバル設定を試行した場合、次の例が示すような警告メッセージが表示されます。

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitEthernet0/0
Device(config-if)# cts role-based sgt-cache ingress
Device(config-if)# exit
Device(config)# cts role-based sgt-caching

There is at least one interface that has ingress sgt caching configured. Please
remove all interface ingress sgt caching configuration(s) before attempting global
enable.
```

- **cts role-based sgt-caching** コマンドを使用してグローバル設定を有効化し、インターフェイス設定モードで **cts role-based sgt-cache ingress** コマンドを使用してインターフェイス設定を試行した場合、次の例が示すような警告メッセージが表示されます。

```
Device> enable
Device# configure terminal
Device(config)# cts role-based sgt-caching
Device(config)# interface gigabitEthernet0/0
Device(config-if)# cts role-based sgt-cache ingress

Note that ingress sgt caching is already active on this interface due to global
sgt-caching enable.
```

- V4 トランスポートを介した IPv6 パケットおよび V6 トランスポートを介した IPv4 パケットのトンネリングの SGT キャッシングは、サポートされていません。
- ルーティング プラットフォームでの IPv6 SGACL ポリシーのハイアベイラビリティおよび同期は、IPv6-SGT キャッシングではサポートされません。
- SGT キャッシングは、ISR4K ベースのプラットフォームにおいて ESP ヘッダーで SGT タグを伝送する IPSec パケットではサポートされません。
- SGT キャッシングは、リンクローカル IPv6 送信元アドレスに対して実行されません。

  リンクローカルアドレスとは、ホストが接続されているネットワークセグメント（リンク）またはブロードキャストドメイン内の通信にのみ有効なネットワークアドレスです。リンクローカルアドレスは、単一のネットワークセグメントを超えて一意であるとは限りません。そのため、ルータは、リンクローカルアドレスを持つパケットを転送しません。リンクローカルアドレスは一意ではないため、送信元がリンクローカル IPv6 アドレスであるパケットの SGT タグは割り当てられません。
- SGT キャッシングは、IVRF が設定された IPsec を持つトンネルインターフェイスではサポートされません。
- 仮想テンプレート インターフェイスでの SGT キャッシングの設定は、Cisco ASR 1000 プラットフォームではサポートされていません。

Cisco TrustSec SGT キャッシングの詳細

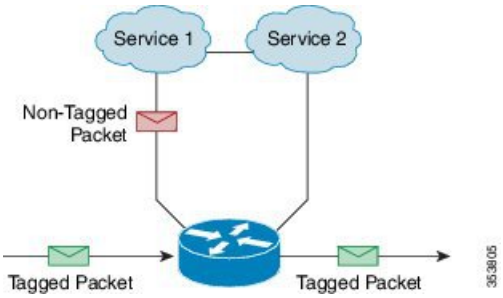
SGT キャッシングを使用した SGT の特定と再適用

Cisco TrustSec は、セキュリティ グループ タグ（SGT）キャッシングを使用して、SGT でタグ付けされたトラフィックを、SGT を認識していないサービスを通じても渡すことができるようにします。SGT を伝播できないサービスには、WAN の高速化または最適化、侵入防御システム（IPS）、およびアップストリーム ファイアウォールがあります。ワンアーム モードでは、SGT でタグ付けされたパケットはデバイス（タグがキャッシュされた場所）に入力され、サービスにリダイレクトされます。そのサービスが完了した後、パケットはデバイスに戻される

か、別のデバイスにリダイレクトされます（図を参照）。このようなシナリオでは、次のようになります。

1. Cisco TrustSec SGT キャッシング機能により、デバイスは、着信パケットからの IP-SGT バインド情報を特定し、この情報をキャッシュします。
2. デバイスは、SGT を伝播できないサービスにパケットをリダイレクトします。
3. サービスが完了した後、パケットはデバイスに返されます。
4. サービスの出力ポイントで、適切な SGT がパケットに再適用されます。
5. サービスからデバイスに返されたパケットには、ロールベースの強制が適用されます。
6. SGT のパケットは、他の Cisco TrustSec 対応デバイスのダウンストリームに転送されます。

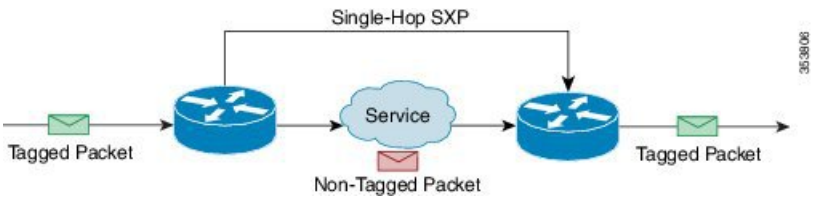
図 *1* : ワンアーム モードでの *SGT* キャッシング



特定のインスタンスでは、Bump-In-The-Wire（BITW）トポロジに導入されるサービスがあります。このようなシナリオでは、次のようになります。

1. サービスを通過するパケットはデバイスに返されません。
2. シングルホップ SGT Exchange Protocol（SXP）を使用して、IP-SGT バインドを特定し、特定されたバインドをエクスポートします。
3. ネットワーク内のアップストリームデバイスは、SXP を通じて IP-SGT バインドを特定し、適切なタグを再適用するか、それらを SGT ベース強制に使用します。出力キャッシング中、元のネットワーク アドレス移動（NAT）前の送信元 IP アドレスは、特定された IP-SGT バインド情報の一部としてキャッシュされます。
4. 300 秒間トラフィックを受信しない IP-SGT バインドは、キャッシュから削除されます。

図 *2* : *Bump-In-The-Wire*（*BITW*）トポロジでの *SGT* キャッシング



IPv6 トラフィックの SGT キャッシング

IPv6 トラフィックの SGT キャッシングに関する考慮事項は次のとおりです。

- **グローバルユニキャスト IPv6 パケット**：IPv6-SGT キャッシングは、IPv6 パケットの入力方向および出力方向で着信するトラフィックに対して実行されます。SGT タグは、パケット（イーサネットヘッダー、IPSec ヘッダー、GRE ヘッダー）にインラインで含まれます。ただし、IPSec パケットのタグの SGT キャッシングは、ISR4K ベースのプラットフォームではサポートされていません。
- **マルチキャスト IPv6 アドレス**：SGT キャッシングは、IPv6 マルチキャストトラフィックおよびリンクローカル IPv6 アドレスではサポートされません。
- **キャッシュされた IPv6-SGT バインディングの SXP を介したエクスポート**：データプレーンで学習された IPv6-SGT バインディングは、IOS の RBM（ロールベースマネージャ）データベースに通知されます。その後、これらのバインディングは、SXP を使用して他の TrustSec デバイスにエクスポートできます。

Cisco TrustSec SGT キャッシングの設定方法

SGT キャッシングのグローバル設定

手順の概要

1. **enable**
2. **configure terminal**
3. **cts role-based sgt-caching**
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# 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。
ステップ 3	**cts role-based sgt-caching** 例：	すべてのインターフェイスに対して、入力方向の SGT キャッシングを有効化します。

	コマンドまたはアクション	目的
	`Device(config)# cts role-based sgt-caching`	
ステップ 4	**end** 例： `Device(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

インターフェイスでの SGT キャッシシングの設定

インターフェイスが Virtual Routing and Forwarding（VRF）ネットワーク上に設定された場合、そのインターフェイス上で特定された IP-SGT バインドは特定の VRF 以下に追加されます。（対応する VRF 上で特定されたバインドを表示するには、**show cts role-based sgt-map vrf** *vrf-name* **all** コマンドを使用します。）

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type slot/port*
4. **cts role-based sgt-cache** [**ingress** | **egress**]
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# 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。
ステップ 3	**interface** *type slot/port* 例： `Device(config)# interface gigabitEthernet 0/1/0`	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**cts role-based sgt-cache** [**ingress**	**egress**] 例：	特定のインターフェイスでSGTキャッシングを設定します。

	コマンドまたはアクション	目的
	`Device(config-if)# cts role-based sgt-cache ingress`	• ingress：特定のインターフェイスを開始するトラフィック（インバウンドトラフィック）に対して SGT キャッシングを有効化します。 • egress：特定のインターフェイスを終了するトラフィック（アウトバウンドトラフィック）に対して SGT キャッシングを有効化します。
ステップ 5	**end** 例： `Device(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

Cisco TrustSec SGT キャッシング の確認

手順の概要

1. **enable**
2. **show cts**
3. **show cts interface**
4. **show cts interface brief**
5. **show cts role-based sgt-map all ipv4**
6. **show cts role-based sgt-map vrf**

手順の詳細

ステップ 1 enable

特権 EXEC モードを有効にします。パスワードを入力します（要求された場合）。

例：

```
Device> enable
```

ステップ 2 show cts

Cisco TrustSec 接続とグローバル SGT キャッシングのステータスを表示します。

例：

```
Device# show cts

Global Dot1x feature: Disabled
CTS device identity: ""
CTS caching support: disabled
CTS sgt-caching global: Enabled
Number of CTS interfaces in DOT1X mode:  0,    MANUAL mode: 0
```

```
Number of CTS interfaces in LAYER3 TrustSec mode: 0
Number of CTS interfaces in corresponding IFC state
  INIT            state:  0
  AUTHENTICATING  state:  0
  AUTHORIZING     state:  0
  SAP_NEGOTIATING state:  0
  OPEN            state:  0
  HELD            state:  0
  DISCONNECTING   state:  0
  INVALID         state:  0
CTS events statistics:
  authentication success: 0
  authentication reject : 0
  authentication failure: 0
  authentication logoff : 0
  authentication no resp: 0
  authorization success : 0
  authorization failure : 0
  sap success           : 0
  sap failure           : 0
  port auth failure     : 0
```

ステップ 3 show cts interface

モード詳細（入力または出力）を使用した、インターフェイスと SGT キャッシング情報についての Cisco TrustSec 設定の統計情報を表示します。

例：

```
Device# show cts interface GigabitEthernet0/1

Interface GigabitEthernet0/1
    CTS sgt-caching Ingress:  Enabled
    CTS sgt-caching Egress :  Disabled
    CTS is enabled, mode:     MANUAL
      Propagate SGT:          Enabled
      Static Ingress SGT Policy:
        Peer SGT:             200
        Peer SGT assignment:  Trusted

    L2-SGT Statistics
        Pkts In                     : 16298041
        Pkts (policy SGT assigned)  : 0
        Pkts Out                    : 5
        Pkts Drop (malformed packet): 0
        Pkts Drop (invalid SGT)     : 0
```

ステップ 4 show cts interface brief

すべてのインターフェイスについて、モード詳細（入力または出力）を使用してSGTキャッシング情報を表示します。

例：

```
Device# show cts interface brief

Interface GigabitEthernet0/0
    CTS sgt-caching Ingress:  Enabled
    CTS sgt-caching Egress :  Disabled
    CTS is disabled
```

```
Interface GigabitEthernet0/1
    CTS sgt-caching Ingress:  Enabled
    CTS sgt-caching Egress :  Disabled
    CTS is enabled, mode:     MANUAL
      Propagate SGT:          Enabled
      Static Ingress SGT Policy:
        Peer SGT:             200
        Peer SGT assignment:  Trusted

Interface GigabitEthernet0/2
    CTS sgt-caching Ingress:  Enabled
    CTS sgt-caching Egress :  Disabled
    CTS is enabled, mode:     MANUAL
      Propagate SGT:          Enabled
      Static Ingress SGT Policy:
        Peer SGT:             0
        Peer SGT assignment:  Untrusted

Interface GigabitEthernet0/3
    CTS sgt-caching Ingress:  Enabled
    CTS sgt-caching Egress :  Disabled
    CTS is disabled

Interface Backplane-GigabitEthernet0/4
    CTS sgt-caching Ingress:  Enabled
    CTS sgt-caching Egress :  Disabled
    CTS is disabled

Interface RG-AR-IF-INPUT1
    CTS sgt-caching Ingress:  Enabled
    CTS sgt-caching Egress :  Disabled
    CTS is disabled
```

ステップ 5 show cts role-based sgt-map all ipv4

すべての SGT-IPv4 バインドを表示します。

例：

```
Device# show cts role-based sgt-map all ipv4

Active IPv4-SGT Bindings Information

IP Address              SGT     Source
============================================
192.0.2.1               50      CACHED
192.0.2.2               50      CACHED
192.0.2.3               50      CACHED
192.0.2.4               50      CACHED
192.0.2.5               3900    INTERNAL
192.0.2.6               3900    INTERNAL
192.0.2.7               3900    INTERNAL

IP-SGT Active Bindings Summary
============================================
Total number of CACHED   bindings = 20
Total number of INTERNAL bindings = 3
Total number of active   bindings = 23
```

ステップ 6 show cts role-based sgt-map vrf

特定の Virtual Routing and Forwarding（VRF）インターフェイスに対する SGT-IP バインドをすべて表示します。

例：

```
Device# show cts role-based sgt-map vrf

%IPv6 protocol is not enabled in VRF RED
Active IPv4-SGT Bindings Information

IP Address              SGT     Source
============================================
192.0.2.1                50      CACHED
192.0.2.2                2007    CACHED
192.0.2.3                50      CACHED
192.0.2.4                50      CACHED
```

IP と SGT のバインドの確認

データプレーンで学習された IP と SGT のバインドを表示します。

```
Device# show cts role-based sgt-map all
Active IPv4-SGT Bindings Information

IP Address              SGT     Source
============================================
10.104.33.219           300     INTERNAL

IP-SGT Active Bindings Summary
============================================
Total number of INTERNAL bindings = 1
Total number of active   bindings = 1

Active IPv6-SGT Bindings Information

IP Address                                  SGT     Source
============================================================
100::/64                                    124     CLI
200::2                                      300     INTERNAL
300::1                                      300     INTERNAL
1000::2                                     300     INTERNAL

IP-SGT Active Bindings Summary
============================================
Total number of CLI      bindings = 1
Total number of INTERNAL bindings = 3
Total number of active   bindings = 4
```

設定例 Cisco TrustSec SGT キャッシング

例：SGT キャッシングのグローバル設定

```
Device> enable
Device# configure terminal
Device(config)# cts role-based sgt-caching
Device(config)# end
```

例：インターフェイスの SGT キャッシシングの設定

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitEthernet 0/1/0
Device(config-if)# cts role-based sgt-cache ingress
Device(config-if)# end
```

例：インターフェイスでの SGT キャッシシングの無効化

次の例は、キャッシングがグローバルに有効だがインターフェイスでは無効な場合に、インターフェイスで SGT キャッシングを無効化し、インターフェイスの SGT キャッシングの状態を表示する方法を示します。

```
Device> enable
Device# configure terminal
Device(config)# cts role-based sgt-caching
Device(config)# interface gigabitEthernet 0/1
Device(config-if)# no cts role-based sgt-cache ingress
Device(config-if)# end
Device# show cts interface GigabitEthernet0/1

Interface GigabitEthernet0/1
    CTS sgt-caching Ingress:  Disabled
    CTS sgt-caching Egress :  Disabled
    CTS is enabled, mode:     MANUAL
      Propagate SGT:          Enabled
      Static Ingress SGT Policy:
        Peer SGT:             200
        Peer SGT assignment:  Trusted

    L2-SGT Statistics
        Pkts In                     : 200890684
        Pkts (policy SGT assigned)  : 0
        Pkts Out                    : 14
        Pkts Drop (malformed packet): 0
```

```
                Pkts Drop (invalid SGT)     : 0
```

に関する追加情報 Cisco TrustSec SGT キャッシング

関連資料

関連項目	マニュアル タイトル
Cisco IOS セキュリティ コマンド	• 『Cisco IOS Security Command Reference: Commands A to C』[英語] • 『Cisco IOS Security Command Reference: Commands D to L』[英語] • 『Cisco IOS Security Command Reference: Commands M to R』[英語] • 『Cisco IOS Security Command Reference: Commands S to Z』[英語]
Cisco TrustSec の設定	『*Cisco TrustSec Configuration Guide*』の「Cisco TrustSec Support for IOS」の章
Cisco TrustSec の概要	『Overview of TrustSec』
Cisco TrustSec ソリューション	『Cisco TrustSec Security Solution』

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

Cisco TrustSec SGT キャッシング 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 : Cisco TrustSec SGT* キャッシング の機能情報

機能名	リリース	機能情報
Cisco TrustSec SGT キャッシング		Cisco TrustSec SGT キャッシング 機能は、セキュリティ グループタグ（SGT）の移動性を柔軟にする Cisco TrustSec の機能を強化します。この機能は、IP-SGT バインドを特定し、対応する SGT をキャッシュすることで、通常のディープ パケット インスペクションを処理するすべてのネットワーク サービスを通じて、またパケットが該当する SGT で再度タグ付けされるサービス出力ポイントにおいて、ネットワーク パケットを転送します。 次のコマンドが導入または変更されました。**cts role-based sgt-caching**、**cts role-based sgt-cache** [**ingress**	**egress**]。

機能名	リリース	機能情報
IPv6の有効化：SGT キャッシング	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。