Cisco TrustSec SGT キャッシング

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。

IPv4 SGT キャッシングのみがサポートされます。ハイアベイラビリティは SGT キャッシングでサポートされています。

Cisco TrustSec SGT キャッシングの制約事項

グローバルな 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 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、こ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 gigabitEthernet 1/0/1
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.
```

この制限は、レイヤ 3 ルーテッドポートインターフェイスにのみ適用されます。また、SGT キャッシングが機能するには、ポートが信頼できるポートである必要があります。

- SGT キャッシングは内部的に NetFlow TCAM（Ternary Content Addressable Memory）スペースを使用するため、インターフェイス上ではいつでも Flexible NetFlow または SGT キャッシングのどちらかを特定の方向で有効にできます。
- **cts role-based sgt-caching** コマンドを使用してグローバル コンフィギュレーションを有効にし、インターフェイス コンフィギュレーション 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 コンフィギュレーションを試行すると、次の例に示すように、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 gigabitEthernet 1/0/1
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.
```

- IPv6 SGT キャッシングはサポートされていません。
- 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できません。

  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。したがって、デバイス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が一意ではないため、送信元がリンクローカル IPv6 アドレスであるパケットには SGT タグは割り当てられません。
- SGT キャッシングは、Application Visibility and Control（AVC）、有線デバイス AVC（WDAVC）、暗号化トラフィック分析（ETTA）、または NetFlow/Flexible NetFlow 機能が設定されているポートインターフェイス上で共存できません。SGT キャッシングとこれらの機能のいずれかが同じインターフェイス上で設定されている場合、エラーメッセージがコンソールに表示されます。

  上記の機能のいずれかとともに SGT キャッシングが有効になっている場合、次のエラーメッセージがコンソールに表示されます。*SGT* キャッシングは設定できません。設定を削除します。ただし、SGT キャッシング機能が **show running-config** コマンドの出力に表示されます。共存できない機能を削除した後、SGT キャッシングを手動で削除して再設定する必要があります。
- 出力 SGT キャッシングと L2 SGT キャッシングは、Cisco Catalyst 9500 シリーズ スイッチの C9500-32C、C9500-32QC、C9500-48Y4C、および C9500-24Y4C モデルではサポートされていません。

Cisco TrustSec SGT キャッシングに関する情報

SGT キャッシングを使用した SGT の特定と再適用

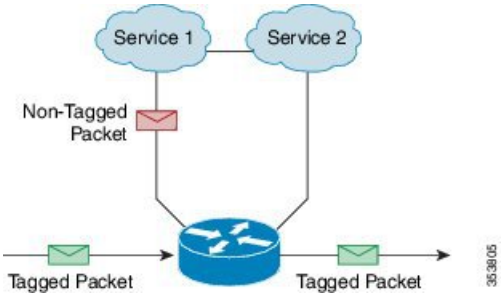
Cisco TrustSec は、セキュリティグループタグ（SGT）キャッシングを使用して、SGT でタグ付けされたトラフィックを、SGT を認識していないサービスを通じても渡すことができるようにします。SGT を伝播できないサービスには、WAN の高速化または最適化、侵入防御システム（IPS）、およびアップストリーム ファイアウォールがあります。

VLAN で SGACL キャッシングを設定するには、対応するポートおよび VLAN で SGT キャッシングを有効にする必要があります。

ワンアームモード（下の図を参照）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。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



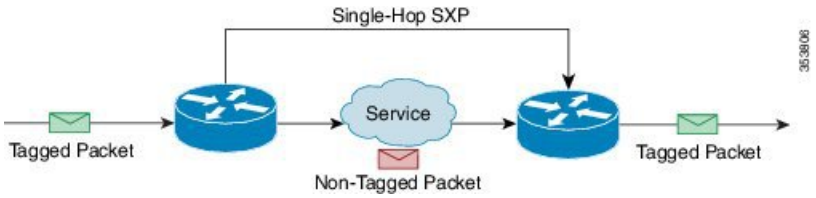
特定のインスタンスでは、Bump-In-The-Wire（BITW）トポロジに導入されるサービスがあります（上の図を参照）。このようなシナリオでは、次のようになります。

1. 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



Cisco TrustSec SGT キャッシングの設定方法

このセクションでは、SGTキャッシングをグローバルにインターフェイス上で設定する方法について説明します。

SGT キャッシングのグローバル設定

始める前に

SGTキャッシングを有効にする前に、情報交換のためにセキュリティ交換プロトコル（SXP）を確立する必要があります。

手順

	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： `Device(config)# cts role-based sgt-caching`	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
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。）SGT キャッシングは、VRF ごとに設定することもできます。

手順

	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 1/0/1`	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： `Device(config-if)# cts role-based sgt-cache ingress`	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。 • **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。 • **ingress**：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。

	コマンドまたはアクション	目的
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

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 GigabitEthernet 1/0/1

Interface GigabitEthernet1/0/1
    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 GigabitEthernet1/0/1
    CTS sgt-caching Ingress:  Enabled
    CTS sgt-caching Egress :  Disabled
    CTS is disabled

Interface GigabitEthernet1/0/1
    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 GigabitEthernet1/0/2
    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 GigabitEthernet1/0/3
    CTS sgt-caching Ingress:  Enabled
    CTS sgt-caching Egress :  Disabled
```

```
    CTS is disabled

Interface Backplane-GigabitEthernet1/0/4
    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 *vrf-name* all ipv4

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 vrf1 all ipv4

%IPv6 protocol is not enabled in VRF vrf1
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
```

ステップ 7 SGT キャッシュエントリは、ポートのシャットダウンまたは SGT キャッシュのタイムアウト後に削除されます。

Cisco TrustSec キャッシングの設定例

例：SGT キャッシングのグローバル設定

次に、SGT キャッシングをグローバルに設定する例を示します。

```
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

次に、インターフェイスの SGT キャッシングを設定する例を示します。

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

Interface GigabitEthernet1/0/1
    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
```

Cisco TrustSec SGT キャッシングの機能の履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Fuji 16.9.2	Cisco TrustSec SGT キャッシング	Cisco TrustSec SGT キャッシング機能は、SGT の移動性を柔軟にする Cisco TrustSec の機能を強化します。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。