Supervisor Engine 2T 搭載 Cisco Catalyst 6500 シリーズ: Cisco TrustSec の有効化による投資保護の実現

このドキュメントの内容

このホワイト ペーパーでは、Cisco TrustSec® ネットワークを有効化した Supervisor Engine 2T 搭載の Cisco® Catalyst® 6500 シリーズ向けに設計された 2 つの動作モードについて説明します。この 2 つの動作モードにより、異なる世代のラインカードを混在させて使用するワイヤリング クローゼットおよびアグリゲーション レイヤ展開に対する投資の保護を実現できます。

このホワイト ペーパーでは、Cisco TrustSec ソリューションについての基礎的な知識があることを前提としています。Cisco TrustSec についての詳細は、Web サイト http://www.cisco.com/web/JP/index.html を参照してください。

概要

Cisco TrustSec は、ポリシーベースのアクセス制御、ID 認識型のネットワーキング、およびデータ整合性と機密性のサービスにより、ネットワークおよびネットワーク リソースへのセキュアなアクセスを可能にします。また、Cisco TrustSec により、コンプライアンスの改善、セキュリティの強化、および運用効率の向上を実現することができます。ネットワークが拡張され、デバイス、アプリケーション、ユーザが追加されても、Cisco TrustSec ソリューションは、信頼性、一貫性、効率性を備えた ID ベースのビジネス サービスとアプリケーションをいつでも、どこでも、誰にでも提供します。シスコとパートナーは、ポリシーの見直し、分析、および設計の専門知識によって、Cisco TrustSec ソリューションをネットワークに展開する準備をするためのスマートでパーソナライズされたプロフェッショナル サービスを提供します。これらのサービスは、最先端のプラクティスを活用しながら、より迅速かつコスト効率に優れた方法で完全な認証およびアクセスのソリューションを展開するよう支援すると同時に、継続的な運用効率に関する知識を提供します。

Supervisor Engine 2T および 6900 シリーズ ラインカード搭載の Cisco Catalyst 6500 は、Cisco TrustSec ネットワークの実装をフル サポートするハードウェアとソフトウェアです。表 1 に、Supervisor Engine 2T および 6900 シリーズ ラインカード搭載の Cisco Catalyst 6500 で最初から利用可能な主な Cisco TrustSec 関連の機能を示します。

表 1 Supervisor Engine 2T および 6900 シリーズ ラインカードで利用可能な機能

TrustSec 機能	Supervisor Engine 2T/6900 シリーズ ラインカード	Supervisor Engine 720 ベースのシステム
ポリシーベースの SGACL の適用	可	不可
IEEE 802.1AE Media Access Control（MAC; メディア アクセス コントロール）セキュリティ	可	不可
Cisco TrustSec レイヤ 3 トランスポート フォワーディング	可	不可
Cisco TrustSec Security Group Tag Exchange Protocol（SXP）	可	可
Network Device Admission Control（NDAC）	可	可

Cisco Catalyst 6500 に Supervisor Engine 2T および 6900 シリーズ ラインカードを構成すると、Cisco TrustSec サービスの提供に関する制限とは無関係に、システムをフルに利用できます。Cisco TrustSec を有効化したシステムの フォワーディング パフォーマンスは、Security Group Tag（SGT; セキュリティ グループ タグ）付けの有無にかかわらず Cisco TrustSec が構成されていないシステムと一致しています。

Supervisor Engine 2T および Cisco TrustSec とのラインカードの互換性

従来、Cisco Catalyst 6500 は、ワイヤリング クローゼット、WAN エッジ、データ センター、および中規模から大規模の企業のディストリビューション、コアおよびコアの環境を含む、企業ネットワークにおいてエンドツーエンドで展開されてきました。

Supervisor Engine 2T を使用した Cisco TrustSec ネットワークに移行しても、既存の Cisco Catalyst 6500 スイッチおよびラインカードを引き続き使用したいというお客様の要望が多数ありました。このため、シスコでは Cisco TrustSec ネットワークでの展開時に特定の既存のラインカードと互換性を持つよう、Supervisor Engine 2T を開発しました。

ワイヤ速度での SGT および IEEE 802.1AE MACsec のリンク暗号化などの新しい Cisco TrustSec 機能をサポートするため、新しい Supervisor Engine 2T と 6900 シリーズ ラインカードには専用の Application Specific Integrated Circuit（ASIC; 特定用途向け集積回路）が使用されています。また、この機能では内部のフォワーディング決定プロセスの変更も必要となります。このため、既存のラインカードとの互換性を実現するには、既存または旧世代のラインカードとの互換性を保持するために設計された 2 つの新しい動作モードを使用する必要があります。Cisco TrustSec ネットワークの展開において Cisco Catalyst 6500 がどのように投資保護を実現するかの詳細のを説明する前に、ラインカードおよび各ラインカードにおける異なるレベルの Cisco TrustSec サポートの定義から見て行きましょう。

イーサネット LAN ラインカードについて、Supervisor Engine 2T は次をサポートしています。

- すべての WS-X6148 シリーズ ラインカード
- Centralized Forwarding Card（CFC; 集中型フォワーディング カード）を備えたすべての 6700 シリーズ ラインカード
- Distributed Forwarding Card Version 4（DFC4; 分散型フォワーディング カード バージョン 4）を備えたすべての WS-X6700 シリーズ ラインカード
  （WS-X6800 シリーズ ラインカードは、基本的に DFC4 を備えた 6700 ラインカードであることに注意してください）
- すべての WS-X6900 シリーズ モジュール

表 2 は、Supervisor Engine 2T と Cisco TrustSec をサポートする Cisco Catalyst 6500 ラインカードについて説明しています。

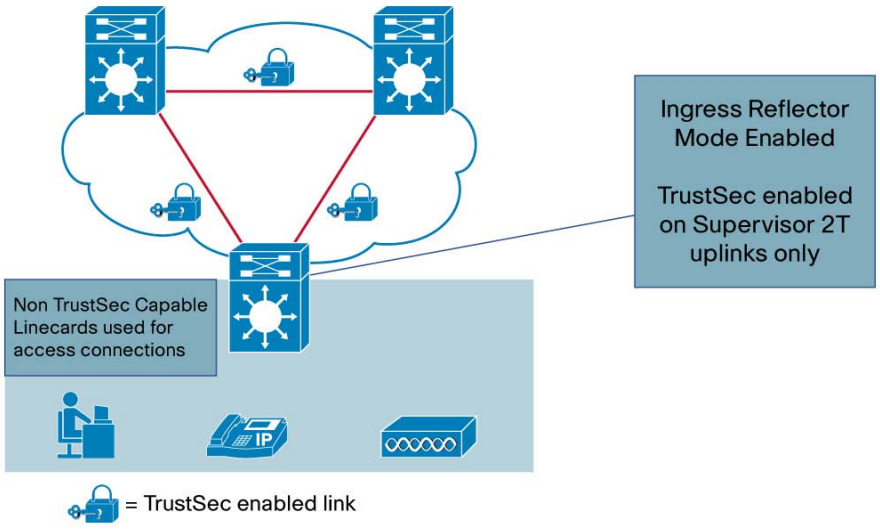
表 2　Cisco Catalyst 6500 ラインカードの Cisco TrustSec のサポートレベル

Cisco TrustSec のサポート レベル	説明	ラインカード
Cisco TrustSec を使用できる	セキュリティ グループ タグの付与および IEEE 802.1AE MACsec のハードウェア アクセラレーションにより、完全な Cisco TrustSec をサポート	Supervisor Engine 2T、およびすべての 6900 シリーズ ラインカード
Cisco TrustSec に対応している	セキュリティ グループ タグの付与または IEEE 802.1AE MACsec をサポートしていませんが、これらのラインカードはセキュリティ グループ タグ情報を含むフォワーディング決定を解釈できます。このため、Cisco TrustSec が使用できるラインカードでの出力用にトラフィックを転送することができます。	WS-X6816-10G-4C/XL WS-X6816-10T-4C/XL
Cisco TrustSec を使用できない	セキュリティ グループ タグの付与または IEEE 802.1AE MACsec をサポートしていません。また、セキュリティ グループ タグ情報を使用したフォワーディング決定を解釈しません。	WS-X6724-SFP WS-X6748-SFP WS-X6748-GE-TX WS-X6704-10G WS-X6824-SFP WS-X6848-SFP WS-X6848-GETX WS-X6148 シリーズ（すべて）

Ingress Reflector モード

Ingress Reflector モードは、Cisco TrustSec を使用できないラインカードと Cisco TrustSec を有効化した Supervisor Engine 2T アップリンクとの間の互換性を提供します。目的は、ワイヤリング クローゼットまたはアクセス レイヤの実装を行うためです。Ingress Reflector モードでは集中型フォワーディングのみがサポートされているため、パケット フォワーディング（ルックアップ決定）はすべて Supervisor Engine 2T PFC 上で発生することになります。6148 シリーズ、または 6748-GE-TX ラインカードなどファブリック対応の CFC ラインカードのみがサポートされています。Ingress Reflector モードを有効化した場合、DFC を備えたラインカードまたは 10 ギガビット イーサネット ラインカードはサポートされません。サポートされていないラインカードは、Ingress Reflector モードが構成された状態では電源を投入しても起動しません（図 1 を参照）。

図 1　Ingress Reflector モードの使用例



Ingress Reflector モードは、グローバル コンフィギュレーション コマンドを使用して有効化され、システムのリロードを必要とします。

図 2 に、必要な CLI を示します。システムのリロードを実行する前に、必ず実行コンフィギュレーションをスタートアップ コンフィギュレーションに保存してください。

図 2　Ingress Reflector モードを有効にする CLI の例

```
6513E.SUP2T.SA.2(config)#platform cts ?
  egress   Platform Hardware CTS egress
  ingress  Platform Hardware CTS ingress

6513E.SUP2T.SA.2(config)#platform cts ingress
CTS Ingress reflector will be active only on next system reboot.
Please reboot the system for CTS Ingress reflector to be active.

6513E.SUP2T.SA.2(config)#
```

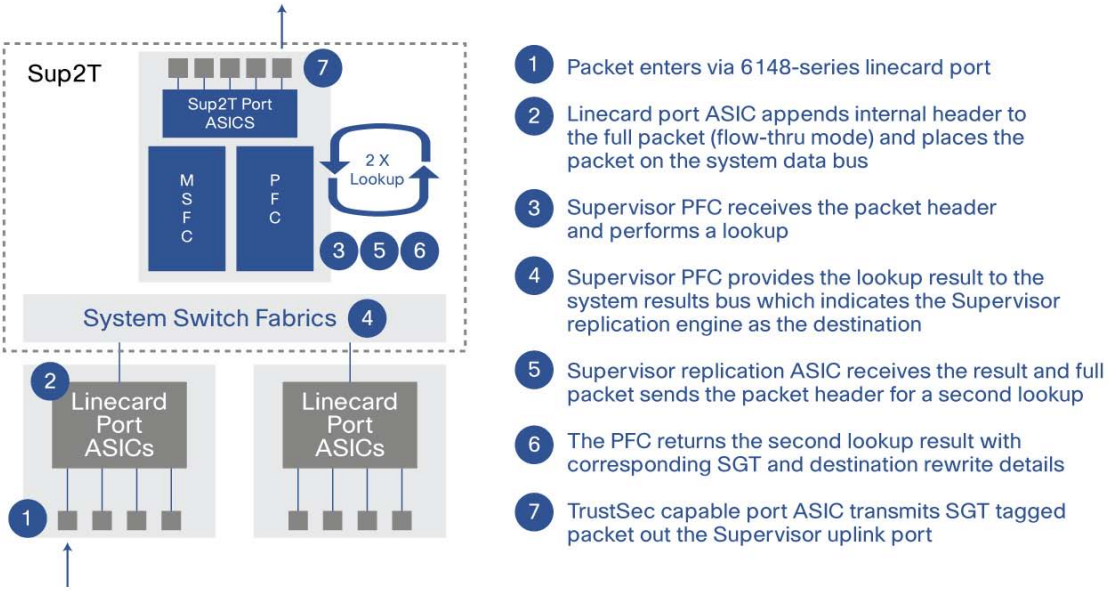
前述のように、Ingress Reflector モードはクラシック バス [1]および CEF 720 アーキテクチャ [2] に構築されたラインカードとの互換性を提供することを目的としています。この場合の課題は、これらのラインカードには、ソース SGT と共に提供されるフォワーディング結果を解釈できるハードウェアが搭載されていないことです。このため、Ingress Reflector モードを有効化すると、システムは Supervisor Engine 2T PFC に組み込まれたパケット レプリケーション ASIC を使用して、追加のフォワーディング ルックアップ サイクルのパケットを反映(複製)します。2 番目のフォワーディング結果は、結果を SGT 情報と併せて処理することが可能なレプリケーション ASIC レプリケーションによって処理されます。

Ingress Reflector モードでの動作

最も数多く設置されているアクセス レイヤ ラインカードとの互換性を提供することが主な利点ですが、Ingress Reflector モードを使用するときに生じるパフォーマンスと制限について理解することも重要です。Ingress Reflector モードがどのように機能するかをよりよく理解するために図 3 にハイレベル パケット ウォークの例を示します。

この例では、パケットはステップ 1 でラインカード ポートを使用してシステムに進入し、ラインカード ポート ASIC が内部システム ヘッダーをパケット全体に付加し、パケットを転送するためにパケットを共有システム バスに入れます。この場合、PFC がスーパーバイザ エンジン上のレプリケーション ASIC にパケットを振り分けるフォワーディング決定を実行します。次にレプリケーション ASIC は PFC にパケット ヘッダーを送信することによって、2 番目のフォワーディング決定を初期化します。これは、この特定のフレームの PFC フォワーディング プロセスの 2 番目のサイクルであることに注意してください。このフォワーディング決定により、SGT タグ情報と、必要な関連パケット上書き情報が生成されます。この場合、レプリケーション ASIC は、SGT タグ情報を含むルックアップ決定を処理でき、スーパーバイザ エンジン アップリンクを使用してパケットを転送します。さらに、トラフィック統計は PFC の最初のパスでは更新されず、PFC の 2 番目および最後のパスでのみ更新されることにも注意してください。

図 3 Ingress Reflector モードのパケット フォワーディングの例



フォワーディング決定サイクルを追加すると、システム全体のパフォーマンスが低下しますが、フォワーディング プロセスはフルにハードウェア アクセラレーションされた状態になります。6148 シリーズ ラインカードを使用したシステ

[1] クラシック バス ラインカードは、32 Gbps 共有バス スイッチ ファブリックを使用するラインカードです。6148 シリーズ ラインカードは、Supervisor Engine 2T でサポートされている唯一のクラシック バス シリーズ ラインカードです。

[2] CEF 720 ラインカードは、モジュール内トラフィックにファブリック間のスイッチ ファブリック、集中型フォワーディング決定にクラシック バスを使用するラインカードです。ラインカードには分散型フォワーディング ドーター カードは取り付けられていません。

ムの場合、集約フォワーディングのパフォーマンスは約 7.5 Mpps です。6700 シリーズなどのすべてのファブリックで有効化されたラインカードを使用したシステムの場合、パフォーマンスは約 24 Mpps です。

表 3 に、さまざまな方向の可能性および関連する最大フォワーディング パフォーマンスの概要を示します。

表 3 Ingress Reflector モードのパフォーマンス

トラフィックの方向	最大スループット	入力例
Cisco TrustSec を使用できない 6100 シリーズ ラインカードから Supervisor Engine 2T へのアップリンク	15 Mpps	WS-X6148-GETX から Supervisor Engine 2T へのアップリンク
Cisco TrustSec を使用できない 6100 シリーズ ラインカードから Cisco TrustSec を使用できない他のラインカードへ	7.5 Mpps	WS-X6148GETX から WS-X6148-GETX
Cisco TrustSec を使用できない 6100 シリーズから WS-X6908 へ	7.5 Mpps	WS-X6148GETX から WS-X6908-10G
Cisco TrustSec を使用できない 6700 シリーズまたは 6800 シリーズのラインカードから Supervisor Engine 2T へのアップリンク	24 Mpps（CFC を使用したシステム全体の集中型フォワーディング）	WS-X6748-SFP から Supervisor Engine 2T へのアップリンク（CFC） WS-X6848-SFP から Supervisor Engine 2T へのアップリンク（DFC）
Cisco TrustSec を使用できない 6700 シリーズまたは 6800 シリーズのラインカードから Cisco TrustSec を使用できない他のラインカードへ	WS-X6148 シリーズに対して 7.5 ～ 15 Mpps 24 Mpps（CFC を使用したシステム全体の集中型フォワーディング） ラインカードあたり 24 Mpps（DFC4 を使用）	WS-X6748 から WS-X6148-GETX WS-X6748 から WS-X6748（CFC）
Cisco TrustSec を使用できない 6700 シリーズまたは 6800 シリーズのラインカードから WS-X6908 へ	24 Mpps（CFC を使用したシステム全体の集中型フォワーディング）	WS-X6748 から WS-X6908（CFC）
Cisco TrustSec を認識する DFC4 ラインカードから Supervisor Engine 2T へのアップリンク	ラインカードあたり 48 Mpps	WS-X6716 から Supervisor Engine 2T へのアップリンク
6900 シリーズから 6900 シリーズへ	60 Mpps	WS-X6908 から WS-X6908

Ingress Reflector モードの概要：

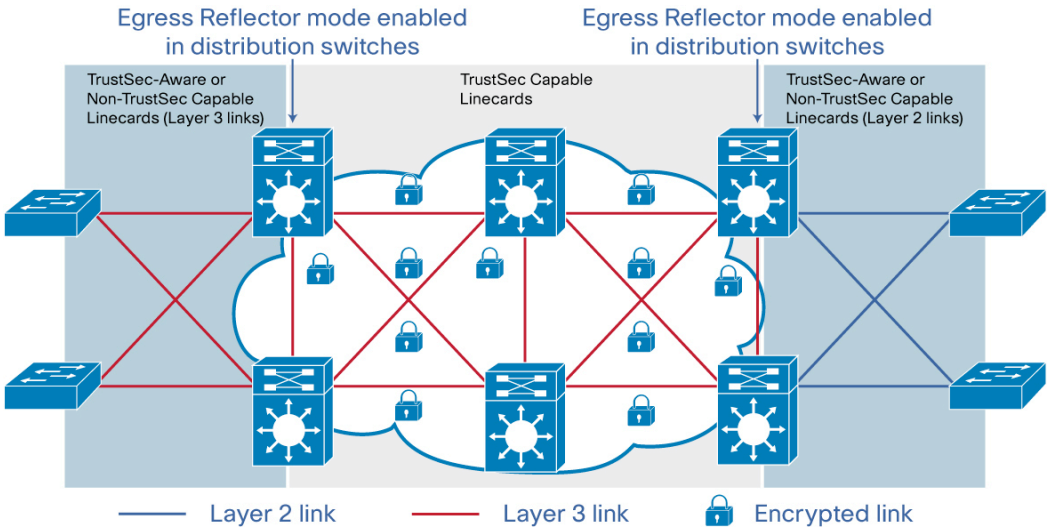
- ワイヤリング クローゼットまたはアクセス レイヤの実装を目的としている
- 6148 シリーズと 6700 シリーズ ラインカードを提供します。Cisco TrustSec SGT タグの伝播は、Supervisor Engine 2T アップリンク ポート（アクティブとスタンバイ のアップリンクの両方をサポート）または WS-X6908-10G ポートでのみ有効となります。
- DFC ドーター カードは、WS-X6908-10G および WS-6816-10G ラインカードでのみサポートされます [3]。フロースルー スイッチング モードでの集約フォワーディング パフォーマンスは 7.5 Mpps（クラシック ライン カード）です。
- コンパクト スイッチング モードでの集約フォワーディングのパフォーマンスは 24 Mpps（6700 シリーズ ライン カード）です。
- サービス モジュールは、Ingress Reflector モードではサポートされていません。

Egress Reflector モード

Egress Reflector モードは、システムレベルの動作モードで、Cisco TrustSec が既存ラインカードとの下位互換性を提供した状態で、Supervisor Engine 2T および 6900 シリーズ ラインカードで有効化されるようにします。目的は、ディストリビューション レイヤなどにあるネットワークのアグリゲーション ポイントのためです。Egress Reflector モードにより、お客様はスーパーバイザ エンジン モジュールおよび DFC をアップグレードし、既存のラインカードを引き続き使用することができます（図 4 を参照）。

[3] WS-X6816-10G ラインカードは、基本的に DFC4 がインストールされている WS-X6716-10GE ラインカードです。

図 4　Egress Reflector モードの使用例



Egress Reflector モードでの動作

Egress Reflector モードは、2 番目のパケット フォワーディング決定を開始する組み込みパケット レプリケーション ASIC のフォワーディング エンジンを使用して、レガシー ラインカードとの互換性を提供します。2 番目のフォワーディング決定は、Cisco TrustSec SGT 情報を取得するために使用されます。

Egress Reflector モードは、グローバル コンフィギュレーション コマンドを使用して有効化され、システムのリロードを必要とします。

図 5 に、必要な CLI を示します。システムのリロードを実行する前に、必ず実行コンフィギュレーションをスタートアップ コンフィギュレーションに保存してください。

図 5　Egress Reflector モードを有効にする CLI の例

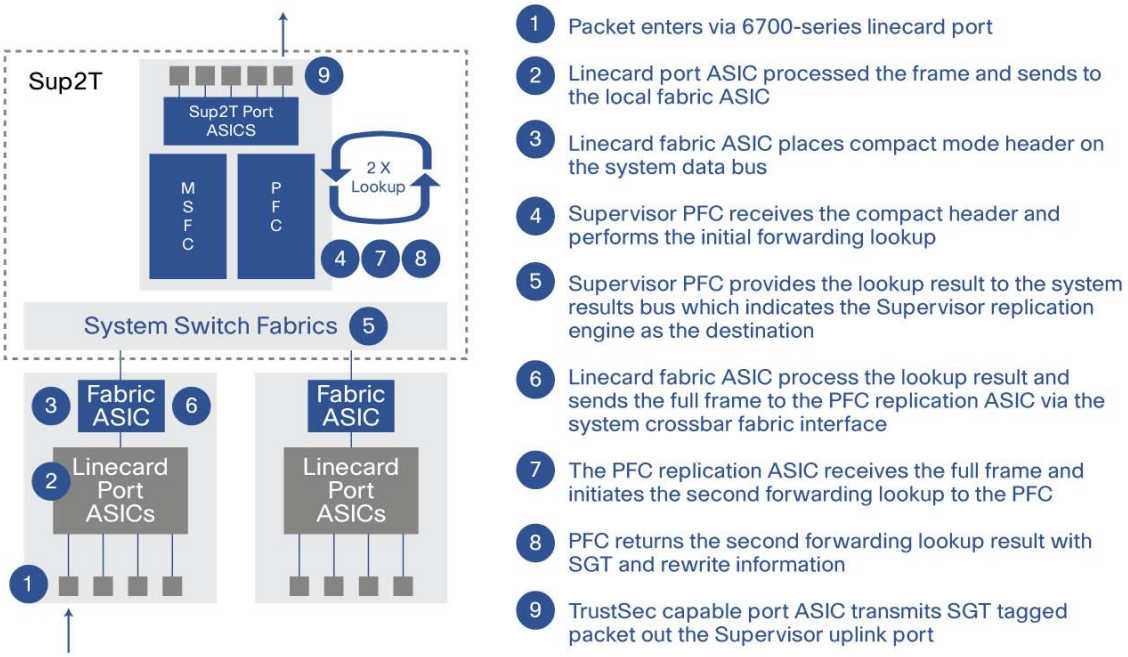
```
6513E.SUP2T.SA.2(config)#platform cts ?
  egress    Platform Hardware CTS egress
  ingress   Platform Hardware CTS ingress

6513E.SUP2T.SA.2(config)#platform cts egress
CTS Egress reflector will be active only on next system reboot.
Please reboot the system for CTS Egress reflector to be active.

6513E.SUP2T.SA.2(config)#
```

Egress Reflector モードが機能する方法をよりよく理解するため、Cisco TrustSec を使用できないラインカード と Supervisor Engine 2T アップリンク ポートの間でのパケット フォワーディング プロセスの概要を 図 5 に示します。この例では出力インターフェイスが Supervisor Engine 2T のインターフェイスと示されていますが、出力インターフェイスは 6900 シリーズ ラインカードの任意のルーテッド インターフェイスになる場合もあります。出力インターフェイスが 6900 シリーズ ラインカード上にある場合、フレームの反映には、スーパーバイザ エンジン PFC ではなく、カード上のレプリケーション ASIC が使用されます。

最初のステップで、パケットは 6700 シリーズ ラインカードのポートからスイッチに進入します。ラインカードはローカル ポートとファブリック ASIC を使用して、標準的なレイヤ 2 およびレイヤ 3 のフォワーディング プロセスを実行します。出力レプリケーション モードが設定されているため、結果の PFC フォワーディング ルックアップ決定はスーパーバイザ エンジン PFC 上のレプリケーション ASIC の宛先インデックスを示します。ラインカード ファブリックは、クロスバー スイッチ ファブリック インターフェイス を使用してフレーム全体を PFC レプリケーション ASIC に送信します。PFC レプリケーションは、フレームを反映（複製）し、2 番目のフォワーディング ルックアップ決定を開始します。

2 番目のルックアップ決定の結果は、SGT 情報およびパケット上書き情報を含みます。次に、PFC レプリケーション エンジンは、適切な SGT でスーパーバイザ エンジン アップリンク ポートに全体のフレームを転送します。さらに、トラフィック統計は PFC の最初のパスでは更新されず、PFC の 2 番目および最後のパスでのみ更新されることにも注意してください（図 6 を参照）。

図 6　Egress Reflector モードでのパケット フォワーディングの例



Egress Reflector モードの主な利点は、旧世代のラインカードとの互換性を提供することです。SGT 伝播がレイヤ 3 ルーテッド ポートでのみ有効にすることができるという要件などの、若干の制限があります。Cisco TrustSec はラインカードを認識し、Cisco TrustSec を使用できないラインカードは、レイヤ 2 またはレイヤ 3 を使用して、システムでダウンリンクとしてサポートされます。ダウンリンク インターフェイスは、たとえば、ネットワーク デバイス アドミッション制御の実装に構成されている場合、ソフトウェアベースの Cisco TrustSec 構成で引き続き使用されます。

表 4 に、さまざまな方向の可能性および関連する最大フォワーディング パフォーマンスの概要を示します。

表 4　Egress Reflector モードのパフォーマンス

トラフィックの方向	最大スループット	入力例
Cisco TrustSec を使用できない 6100 シリーズ ラインカードから Supervisor Engine 2T へのアップリンク	15 Mpps（システム全体の集中型フォワーディング）	WS-X6148-GETX から Supervisor Engine 2T へのアップリンク
Cisco TrustSec を使用できない 6100 シリーズ ラインカードから Cisco TrustSec を使用できない他のラインカードへ	15 Mpps（システム全体の集中型フォワーディング）	WS-X6148GETX から WS-X6148-GETX
Cisco TrustSec を使用できない 6100 シリーズから WS-X6908 へ	15 Mpps（システム全体の集中型フォワーディング）	WS-X6148GETX から WS-X6908-10G
Cisco TrustSec を使用できない 6700 シリーズまたは 6800 シリーズのラインカードから Supervisor Engine 2T へのアップリンク	30 Mpps（CFC を使用したシステム全体の集中型フォワーディング） ラインカードあたり 30 Mpps（DFC4 を使用）	WS-X6748-SFP から Supervisor Engine 2T へのアップリンク（CFC） WS-X6848-SFP から Supervisor Engine 2T へのアップリンク（DFC）
Cisco TrustSec を使用できない 6700 シリーズまたは 6800 シリーズのラインカードから Cisco TrustSec を使用できない他のラインカードへ	WS-X6148 シリーズに対して 15 Mpps 30 Mpps（CFC を使用したシステム全体の集中型フォワーディング） ラインカードあたり 30 Mpps（DFC4 を使用）	WS-X6748 から WS-X6148-GETX WS-X6748 から WS-X6748（CFC） WS-X6748 から WS-X6848（DFC）
Cisco TrustSec を使用できない 6700 シリーズまたは 6800 シリーズのラインカードから WS-X6908 へ	30 Mpps（CFC を使用したシステム全体の集中型フォワーディング） ラインカードあたり 30 Mpps（DFC4 を使用）	WS-X6748 から WS-X6908（CFC） WS-X6748 から WS-X6908（DFC4）

トラフィックの方向	最大スループット	入力例
Cisco TrustSec を認識する DFC4 ラインカードから Supervisor Engine 2T へのアップリンク	ラインカードあたり 48 Mpps	WS-X6716 から Supervisor Engine 2T へのアップリンク
6900 シリーズから 6900 シリーズへ	60 Mpps	WS-X6908 から WS-X6908

Egress Reflector モードには次の制限が適用されます。

- SGT の伝播に構成されるすべてのポートは、レイヤ 3 ルーテッド ポートまたはレイヤ 3 ルーテッド EtherChannel インターフェイスである必要があります（レイヤ 2 スイッチポートはサポートされていません）。
- Cisco TrustSec SGT により有効化されたすべてのポートにインターバル システム VLAN が割り当てられます。
- Egress Reflector モードではサービス モジュールがサポートされていませんが、以降のソフトウェア リリースでは変更される可能性があります。

まとめ

Cisco Catalyst 6500 は Supervisor Engine 2T および 6900 シリーズ ラインカードのリリースとともに進化を続けていきます。Cisco Catalyst 6500 には大規模なインストール ベースおよび多彩な展開オプションがあるため、Cisco Catalyst 6500 が Cisco TrustSec のフル スイートをサポートすることが特に重要です。Cisco Catalyst 6500 が Cisco TrustSec をサポートすることで、真のエンドツーエンドの展開が可能になります。

ポリシーの見直し、分析および専門知識を提供するシスコとパートナーのスマートでパーソナライズされたプロフェッショナル サービスを利用して、ネットワークに Cisco TrustSec ソリューションを展開する準備をしてください。これらのサービスは、最先端のプラクティスを活用しながら、より迅速かつコスト効率に優れた方法で完全な認証およびアクセスのソリューションを展開するよう支援すると同時に、継続的な運用効率に関する知識を提供します。

そして、Supervisor Engine 2T および 6900 シリーズ ラインカードを使用した Cisco Catalyst 6500 システムを選択したお客様は、Cisco TrustSec のフル スイートの機能および利点を活用することができます。また、このホワイトペーパーで説明した Ingress Reflector モードおよび Egress Reflector モードを利用することにより、既存のラインカードのインストール ベースを Cisco TrustSec ネットワークで使用することも選べます。したがって、お客様はニーズに応じて、Cisco TrustSec ネットワークに移行していただくことが可能になります。

お問い合わせ先

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先:シスコ コンタクトセンター
0120-092-255(フリーコール、携帯・PHS含む)
電話受付時間:平日10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

11.07