CatOS ソフトウェアが稼働する Cisco Catalyst 6000/6500 を使った、詳細トラフィック分析用 VACL キャプチャ

目次

概要
前提条件
要件
使用するコンポーネント
関連製品
表記法
背景説明
VLANベース SPAN
VLAN ACL
VSPAN ではなく VACL を使用する利点
設定
ネットワーク図
VLAN-based SPAN を使用する場合の設定
VACL を使用する場合の設定
確認
トラブルシューティング
関連情報

概要

このドキュメントでは、より細かくネットワーク トラフィックを分析するために VLAN アクセス コントロール リスト（ACL）（VACL）キャプチャ ポート機能を使用する設定例を紹介します。このドキュメントでは、VLAN ベースのスイッチド ポート アナライザ（SPAN）（VSPAN）と比較した場合の VACL キャプチャ ポートを使用する利点についても説明します。

VACL を設定するためにポート機能 on Cisco Catalyst 6000/6500 を Cisco IOS® ソフトウェアを実行する、参照します Cisco IOSソフトウェアを実行する Cisco Catalyst 6000/6500 との粒状のトラフィック交通解析のための VACL キャプチャをキャプチャ して下さい。

前提条件

要件

この設定を行う前に、次の要件が満たされていることを確認します。

- バーチャルLAN —参照して下さいバーチャル LAN/VLAN トランキング プロトコル（ VLAN/VTP ）-詳細については概要。
- アクセス リスト—詳細についてはアクセスコントロールの設定を参照して下さい。

使用するコンポーネント

この文書に記載されている情報は Cisco Catalyst 6506 シリーズに切り替えますこと実行 Catalyst OSリリース 8.1(2) 基づいています。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

関連製品

この設定も Cisco Catalyst 6000/6500 シリーズ スイッチによってその実行 Catalyst OSリリース 6.3 およびそれ以降使用することができます。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

背景説明

VLANベース SPAN

SPAN はあらゆる VLAN の 1つ以上の送信元ポートまたは 1つ以上の VLAN から分析のための宛先ポートにトラフィックをコピーします。 ローカル SPAN は、同じ Catalyst 6500 シリーズ スイッチ上の送信元ポート、送信元 VLAN、および宛先ポートをサポートします。

送信元ポートは、ネットワーク トラフィック分析のためにモニタ対象になるポートです。 送信元 VLAN は、ネットワーク トラフィック分析のためにモニタ対象になる VLAN です。 VLANベース SPAN （ VSPAN ）は 1つ以上の VLAN のネットワークトラフィックの分析です。 入力スパンか、出力 スパン、またはその両方で VSPAN を設定できます。 ソースVLAN のすべてのポートは VSPAN セッションのための稼動ソース ポートになります。 管理用送信元 VLAN の何れかに属すれば、宛先ポートは操作上出典から除かれます。 管理用送信元 VLAN からポートを追加するか、または取除く場合、操作上出典はそれに応じて修正されます。

VSPAN セッションのためのガイドライン:

- トランク ポートは VSPAN セッションのための送信元ポートとして含まれていますが、これらの VLAN がトランクのためにアクティブである場合 Admin Source リストにある VLAN だけ監視されます。
- 入力および出力 スパン両方が設定されている VSPAN セッションに関してはシステムは次のものを持っている Supervisor Engine の種類に基づいて動作します:WS-X6K-SUP1A-PFC、WS-X6K-SUP1A-MSFC、WS-X6K-S1A-MSFC2、WS-X6K-S2-PFC2、WS-X6K-S1A-MSFC2、WS-SUP720、WS-SUP32-GE-3B —パケットが同じ VLAN でスイッチされる場合 2 つのパケットはスパンの終点 ポートによって転送されます。WS-X6K-SUP1-2GE、WS-

X6K-SUP1A-2GE — 1 パケットだけスパンの終点 ポートによって転送されます。
- インバンド ポートは VSPAN セッションにおける操作上出典として含まれていません。
- VLAN はクリアされるとき、VSPAN セッションのためのソースリストから取除かれます。
- VSPAN セッションは Admin Source VLAN リストが空である場合無効です。
- 非アクティブ VLAN は VSPAN 設定のために許可されません。
- VSPAN セッションはソースVLAN のうちのどれかが RSPAN VLAN になる場合非アクティブになります。

ソースVLAN に関する詳細についてはソースVLAN の特性を参照して下さい。

VLAN ACL

VACL はアクセスコントロールすべてのトラフィックできます。 または VLAN からルーティングされるか、または VLAN の内で繋がれるすべてのパケットに適用するためにスイッチの VACL を設定できます。 VACL はセキュリティ パケットフィルタリングのためトラフィック特定の物理的な スイッチポートへのリダイレクト厳しくであり。 Cisco IOS ACL とは違って、VACL は方向によって定義されません (入力か出力) 。

IP および IPX のためのレイヤ3 アドレスの VACL を設定できます。 他のプロトコルはすべて MAC アドレスによっておよび MAC VACL を使用して EtherType 制御されるアクセスです。 IP トラフィックおよび IPXトラフィックは MAC VACL によって制御されるアクセスではないです。 他のトラフィックタイプすべて (AppleTalk、DECnet、等) は MAC トラフィックとして分類されます。 MAC VACL はアクセスコントロールにこのトラフィック使用されます。

VACL でサポートされる ACE

VACL はアクセス制御エントリ (ACE) の規則正しく並べられたリストが含まれています。 各 VACL は 1 つの型だけの ACE が含まれている場合があります。 各 ACE はパケットのコンテンツと一致するいくつかのフィールドが含まれています。 各フィールドはどのビットが関連しているか示す関連するビット マスクがある場合があります。 操作は記述する各 ACE と一致が発生するときシステムがパケットとする必要があるものを関連付けられます。 操作は機能依存です。 Catalyst 6500 シリーズ スイッチは 3 つのタイプのハードウェアの ACE をサポートします:

- IP ACE
- IPX ACE
- イーサネット ACE

この表は各 ACE 型と関連付けられるパラメータをリストしたものです:

ACE 型	TCP か UDP	ICMP	他の IP	IPX	イーサネット
レイヤ4 パラメータ	送信元ポート	-	-	-	-
	送信元ポート オペレータ	-	-	-	-
	宛先ポート	-	-	-	-
	宛先ポート オペレータ	ICMP コード	-	-	-
	N/A	ICMP タ	N/A	-	-

		イプ			
レイヤ3パラメータ	IP TOS バイト	IP TOS バイト	IP TOS バイト	-	-
	IPソースアドレス	IPソースアドレス	IPソースアドレス	IPX ソースネットワーク	-
	IP宛先アドレス	IP宛先アドレス	IP宛先アドレス	IP目的地ネットワーク	-
	-	-	-	IP目的地ノード	-
	TCP か UDP	ICMP	他のプロトコル	IPX パケットタイプ	-
レイヤ2パラメータ	-	-	-	-	EtherType
	-	-	-	-	イーサネット送信元アドレス
	-	-	-	-	イーサネット宛先アドレス

VSPAN ではなく VACL を使用する利点

トラフィックの分析に VSPAN を使用する場合は、いくつかの制約があります。

- 対象の VLAN 内を流れるすべてのレイヤ 2 トラフィックがキャプチャされます。 そのため、分析するデータ量が増大します。
- Catalyst 6500 シリーズ スイッチに設定できる SPAN セッション数に制限があります。 詳細については機能要約および制限を参照して下さい。
- 宛先ポートは、モニタ対象になっているすべての送信元ポートの送受信トラフィックのコピーを受け取ります。 宛先ポートがオーバーサブスクライブされている場合、輻輳状態になる可能性があります。 この輻輳により、1 つ以上の送信元ポートのトラフィックの転送が影響を受ける可能性があります。

VACL キャプチャ ポート機能は、これらの制限の克服に役立ちます。 VACL は主に トラフィックをモニタするように設計されていません。 ただし、トラフィックを分類する機能の広範囲とキャプチャ ポート機能はネットワークトラフィック交通解析が大いにより簡単になることができるように導入されました。 VSPAN ではなく VACL キャプチャ ポートを使用する利点は、次のとおりです。

- きめ細かなトラフィック分析VACL では、送信元 IP アドレス、宛先 IP アドレス、レイヤ 4 プロトコル タイプ、送信元と宛先のレイヤ 4 ポートなどの情報に基づいて照合できます。 この機能により、VACL はきめ細かなトラフィックの識別とフィルタリングに効果を発揮します。
- セッションの数VACL はハードウェアで実施されます。 作成することができる ACE の数は

スイッチで利用可能 な TCAM に左右されます。
- 宛先ポートのオーバーサブスクリプションきめ細かなトラフィックの識別によって宛先ポートに転送されるフレームの数が減少するため、オーバーサブスクリプションの可能性が軽減されます。
- パフォーマンスVACL はハードウェアで実施されます。 VACL のアプリケーションのためのパフォーマンスペナルティは Cisco Catalyst 6500 シリーズ スイッチの VLAN へありません。

設定

この項では、このドキュメントで説明する機能の設定に必要な情報を提供します。

このドキュメントでは、次の設定を使用します。

- VLAN-based SPAN を使用する場合の設定
- VACL を使用する場合の設定

注: このセクションで使用されているコマンドの詳細を調べるには、Command Lookup Tool（登録ユーザ専用）を使用してください。

ネットワーク図

このドキュメントでは、次のネットワーク構成を使用しています。

VLAN-based SPAN を使用する場合の設定

この設定例が VLAN 11 および VLAN 12 のフローがネットワーク アナライザ デバイスにおよびそれらを送信 するすべてのレイヤ2 トラフィックをキャプチャ するために必要なステップをリストします。

1. 対象トラフィックを指定します。この例では、VLAN 100 および VLAN 200 でフローするそれはトラフィックです。`6K-CatOS> (enable) **set span** *11-12 3/24 !--- where **11-12** specifies the range of source VLANs and **3/24** specify the destination port.* 2007 Jul 12 21:45:43 %SYS-5-SPAN_CFGSTATECHG:local span session inactive for des tination port 3/24 Destination : Port 3/24 Admin Source : VLAN 11-12 Oper Source : Port 3/11-12,16/1 Direction : transmit/receive Incoming Packets: disabled Learning : enabled Multicast : enabled Filter : - Status : active 6K-CatOS> (enable) 2007 Jul 12 21:45:43 %SYS-5-SPAN_CFGSTATECHG:local span sessi on active for destination port 3/24` VLAN 11 および VLAN 12 に属するこれによって、すべてのレイヤ2 トラフィックはポート 3/24 にコピーされ、送信 されます。
2. **show span** の SPAN設定を**すべての**コマンド確認して下さい。`6K-CatOS> (enable) **show span all** Destination : Port 3/24 Admin Source : VLAN 11-12 Oper Source : Port 3/11-12,16/1 Direction : transmit/receive Incoming Packets: disabled Learning : enabled Multicast : enabled Filter : - Status : active Total local span sessions: 1 No remote span session configured 6K-CatOS> (enable)`

VACL を使用する場合の設定

この設定例では、ネットワーク管理者から次のような要件が提示されています。

- 仕様サーバへの VLAN 12 のホスト（10.12.12.128/25）の範囲からの HTTPトラフィック（10.11.11.100） VLAN 11 でキャプチャ される必要があります。

- グループ アドレス 239.0.0.100 に向かう伝送 方向のマルチキャスト User Datagram Protocol（UDP; ユーザ データグラム プロトコル）トラフィックは VLAN 11 からキャプチャ される必要があります。

1. セキュリティ ACL を使用して関連 トラフィックを定義して下さい。 定義されるすべての ACE のためのキーワード **キャプチャを**述べることを忘れないようにして下さい。`6K-CatOS> (enable) **set security acl ip** *HttpUdp_Acl* **permit tcp** *10.12.12.128 0.0.0.127* **host** *10.11.11.100* **eq** *www* **capture** *!--- Command wrapped to the second line.* HttpUdp_Acl editbuffer modified. Use 'commit' command to apply changes. 6K-CatOS> (enable) **set security acl ip** *HttpUdp_Acl* **permit udp any host** *239.0.0.100* **capture** HttpUdp_Acl editbuffer modified. Use 'commit' command to apply changes.`
2. ACE 設定が正しく、適切な順序でかどうか確認して下さい。`6K-CatOS> (enable) **show security acl info** *HttpUdp_Acl* **editbuffer** set security acl ip HttpUdp_Acl ---------- ---------- 1. permit tcp 10.12.12.128 0.0.0.127 host 10.11.11.100 eq 80 capture 2. permit udp any host 239.0.0.100 capture ACL HttpUdp_Acl Status: **Not Committed** 6K-CatOS> (enable)`
3. ハードウェアに ACL を託して下さい。`6K-CatOS> (enable) **commit security acl** *HttpUdp_Acl* ACL commit in progress. ACL 'HttpUdp_Acl' successfully committed. 6K-CatOS> (enable)`
4. ACL のステータスを確認して下さい。`6K-CatOS> (enable) **show security acl info** *HttpUdp_Acl* **editbuffer** set security acl ip HttpUdp_Acl ---------- --- 1. permit tcp 10.12.12.128 0.0.0.127 host 10.11.11.100 eq 80 capture 2. permit udp any host 239.0.0.100 capture ACL HttpUdp_Acl Status: **Committed** 6K-CatOS> (enable)`
5. VLAN アクセス マップを適切な VLAN にマッピングします。`6K-CatOS> (enable) **set security acl map** *HttpUdp_Acl* **?** <vlans> Vlan(s) to be mapped to ACL 6K-CatOS> (enable) **set security acl map** *HttpUdp_Acl 11* Mapping in progress. ACL HttpUdp_Acl successfully mapped to VLAN 11. 6K-CatOS> (enable)`
6. VLAN マッピングに ACL を確認して下さい。`6K-CatOS> (enable) **show security acl map** *HttpUdp_Acl* ACL HttpUdp_Acl is mapped to VLANs: 11 6K-CatOS> (enable)`
7. キャプチャ ポートを設定して下さい。`6K-CatOS> (enable) **set vlan** *11 3/24* VLAN Mod/Ports ---- ---------- 11 3/11,3/24 6K-CatOS> (enable) 6K-CatOS> (enable) **set security acl capture-ports** *3/24* Successfully set 3/24 to capture ACL traffic. 6K-CatOS> (enable)` **注**: ACL が複数 の VLAN にマッピング される場合、キャプチャ ポートはすべてのそれらの VLAN に設定する必要があります。 キャプチャ ポートに複数 の VLAN を許可し、ポートをトランクで設定し、ACL にマッピング される VLAN だけ許可させます。 たとえば ACL が VLAN 11 および 12 にマッピング されたら、設定を完了して下さい。`6K-CatOS> (enable) **clear trunk** *3/24 1-10,13-1005,1025-4094* 6K-CatOS> (enable) **set trunk** *3/24 on dot1q 11-12* 6K-CatOS> (enable) **set security acl capture-ports** *3/24*`
8. キャプチャ ポートコンフィギュレーションを確認して下さい。`6K-CatOS> (enable) **show security acl capture-ports** ACL Capture Ports: 3/24 6K-CatOS> (enable)`

確認

ここでは、設定が正常に動作していることを確認します。

Output Interpreter Tool（OIT）（登録ユーザ専用）では、特定の **show** コマンドがサポートされています。 OIT を使用して、**show** コマンド出力の解析を表示できます。

- **show security ACL ヒント**— NVRAM およびハードウェアに現在設定されるか、または最後に託される VACL のコンテンツを表示する。`6K-CatOS> (enable) **show security acl info** *HttpUdp_Acl* set security acl ip HttpUdp_Acl ---------- --- 1. permit tcp 10.12.12.128 0.0.0.127 host 10.11.11.100 eq 80 capture 2. permit udp any host 239.0.0.100 capture 6K-CatOS> (enable)`
- **show security ACL は map** —特定の ACL、ポート、または VLAN のための ACL に VLAN か ACL にポート マッピングを表示する。`6K-CatOS> (enable) **show security acl map all** ACL Name`

```
Type Vlans ------------------------------- ---- ----- HttpUdp_Acl IP 11 6K-CatOS> (enable)
```

- **show security ACL キャプチャ ポート**—キャプチャ ポートのリストを表示する。`6K-CatOS> (enable) show security acl capture-ports ACL Capture Ports: 3/24 6K-CatOS> (enable)`

トラブルシューティング

現在のところ、この設定に関する特定のトラブルシューティング情報はありません。

関連情報

- Cisco IOS ソフトウェアが稼働する Cisco Catalyst 6000/6500 による詳細なトラフィック分析用 VACL キャプチャ
- アクセスコントロールの設定- Catalyst 6500 シリーズ ソフトウェア コンフィギュレーション ガイド、8.6
- LAN 製品に関するサポート ページ
- LAN スイッチングに関するサポート ページ
- テクニカルサポートとドキュメント - Cisco Systems