Acquisizione VACL per l'analisi granulare del traffico con Cisco Catalyst 6000/6500 con software CatOS

Sommario

[Introduzione](#)
[Prerequisiti](#)
[Requisiti](#)
[Componenti usati](#)
[Prodotti correlati](#)
[Convenzioni](#)
[Premesse](#)
[SPAN basato su VLAN](#)
[ACL VLAN](#)
[Vantaggi dell'utilizzo di VACL rispetto all'utilizzo di VSPAN](#)
[Configurazione](#)
[Esempio di rete](#)
[Configurazione con SPAN basato su VLAN](#)
[Configurazione con VACL](#)
[Verifica](#)
[Risoluzione dei problemi](#)
[Informazioni correlate](#)

Introduzione

In questo documento viene fornita una configurazione di esempio per usare la funzionalità VACL (VLAN Access Control List) per analizzare in modo più granulare il traffico della rete. In questo documento viene descritto anche il vantaggio dell'uso delle porte di acquisizione VACL rispetto all'uso delle VSPAN (Switched Port Analyzer) basate su VLAN.

Per configurare la funzione VACL Capture Port su Cisco Catalyst 6000/6500 con software Cisco IOS®, fare riferimento a VACL Capture for Granular Traffic Analysis con Cisco Catalyst 6000/6500 con software Cisco IOS.

Prerequisiti

Requisiti

Prima di provare questa configurazione, accertarsi di soddisfare i seguenti requisiti:

- LAN virtuale: per ulteriori informazioni, fare riferimento a LAN virtuali/VLAN Trunking Protocol (VLAN/VTP).
- Elenchi di accesso: per ulteriori informazioni, fare riferimento a Configurazione del controllo di accesso.

Componenti usati

Per la stesura del documento, sono stati usati switch Cisco Catalyst serie 6506 con software Catalyst OS versione 8.1(2).

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Prodotti correlati

Questa configurazione può essere utilizzata anche con gli switch Cisco Catalyst serie 6000/6500 con Catalyst OS versione 6.3 e successive.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Premesse

SPAN basato su VLAN

Lo SPAN copia il traffico da una o più porte di origine in una VLAN o da una o più VLAN a una porta di destinazione per l'analisi. Lo SPAN locale supporta porte di origine, VLAN di origine e porte di destinazione sullo stesso switch Catalyst serie 6500.

Una porta di origine è una porta monitorata per l'analisi del traffico di rete. Una VLAN di origine è una VLAN monitorata per l'analisi del traffico di rete. La VSPAN (VLAN-based SPAN) è un'analisi del traffico di rete in una o più VLAN. È possibile configurare VSPAN come Ingress SPAN, Ingress SPAN o entrambi. Tutte le porte nelle VLAN di origine diventano le porte di origine operative per la sessione VSPAN. Le porte di destinazione, se appartengono a una delle VLAN di origine amministrativa, vengono escluse dall'origine operativa. Se si aggiungono o rimuovono le porte dalle VLAN di origine amministrativa, le origini operative vengono modificate di conseguenza.

Linee guida per le sessioni VSPAN:

- Le porte trunk sono incluse come porte di origine per le sessioni VSPAN, ma solo le VLAN presenti nell'elenco di origine Admin vengono monitorate se queste VLAN sono attive per il trunk.
- Per le sessioni VSPAN con SPAN in entrata e in uscita configurate, il sistema funziona in base al tipo di supervisor engine di cui si dispone: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: due pacchetti vengono inoltrati dalla porta di destinazione SPAN se i pacchetti vengono scambiati sulla stessa VLAN.WS-X6K-SUP1-2GE, WS-X6K-SUP1A-2GE: solo un pacchetto viene inoltrato dalla porta di destinazione SPAN.

- Una porta in banda non è inclusa come origine operativa per le sessioni VSPAN.
- Quando una VLAN viene cancellata, viene rimossa dall'elenco di origine delle sessioni VSPAN.
- Una sessione VSPAN viene disabilitata se l'elenco delle VLAN di origine dell'amministratore è vuoto.
- Le VLAN inattive non sono consentite per la configurazione VSPAN.
- Una sessione VSPAN viene disattivata se una delle VLAN di origine diventa una VLAN RSPAN.

Per ulteriori informazioni sulle VLAN di origine, fare riferimento a Caratteristiche della VLAN di origine.

ACL VLAN

I VACL possono controllare tutto il traffico. È possibile configurare i VACL sullo switch in modo che vengano applicati a tutti i pacchetti in entrata o in uscita da una VLAN o che sono collegati tramite bridge all'interno di una VLAN. I VACL sono destinati esclusivamente al filtro dei pacchetti di sicurezza e al reindirizzamento del traffico a porte di switch fisiche specifiche. A differenza degli ACL di Cisco IOS, i VACL non sono definiti in base alla direzione (input o output).

È possibile configurare i VACL sugli indirizzi di layer 3 per IP e IPX. Tutti gli altri protocolli sono controllati tramite gli indirizzi MAC e EtherType usando i VACL MAC. Il traffico IP e il traffico IPX non sono controllati dai VACL MAC. Tutti gli altri tipi di traffico (AppleTalk, DECnet e così via) sono classificati come traffico MAC. I VACL MAC vengono utilizzati per controllare questo traffico.

ACE supportati nei VACL

VACL contiene un elenco ordinato di voci di controllo di accesso (ACE). Ogni VACL può contenere ACE di un solo tipo. Ogni voce ACE contiene un numero di campi che vengono confrontati con il contenuto di un pacchetto. A ogni campo può essere associata una maschera di bit per indicare i bit rilevanti. A ogni voce ACE è associata un'azione che descrive le operazioni che il sistema deve eseguire sul pacchetto quando si verifica una corrispondenza. L'azione dipende dalla feature. Gli switch Catalyst serie 6500 supportano tre tipi di ACE nell'hardware:

- ACE IP
- ACE IPX
- ACE Ethernet

In questa tabella vengono elencati i parametri associati a ogni tipo ACE:

Tipo ACE	TCP o UDP	ICMP	Altro IP	IPX	Ethernet
Parametri layer 4	Porta di origine	-	-	-	-
	Source Port Operator	-	-	-	-
	Porta di destinazio	-	-	-	-

	ne				
	Operatore porta di destinazione	Codice ICMP	-	-	-
	N/D	Tipo ICMP	N/D	-	-
Parametri livello 3	Byte IP ToS	Byte IP ToS	Byte IP ToS	-	-
	Indirizzo origine IP	Indirizzo origine IP	Indirizzo origine IP	Rete di origine IPX	-
	Indirizzo di destinazione IP	Indirizzo di destinazione IP	Indirizzo di destinazione IP	Rete di destinazione IP	-
	-	-	-	Nodo destinazione IP	-
	TCP o UDP	ICMP	Altro protocollo	Tipo di pacchetto IPX	-
Parametri livello 2	-	-	-	-	EtherType
	-	-	-	-	Indirizzo origine Ethernet
	-	-	-	-	Indirizzo di destinazione Ethernet

Vantaggi dell'utilizzo di VACL rispetto all'utilizzo di VSPAN

L'utilizzo di VSPAN per l'analisi del traffico presenta diverse limitazioni:

- Viene acquisito tutto il traffico di layer 2 in una VLAN. In questo modo aumenta la quantità di dati da analizzare.
- Il numero di sessioni SPAN che possono essere configurate sugli switch Catalyst serie 6500 è limitato. per ulteriori informazioni, fare riferimento a Riepilogo delle feature e limitazioni.
- Una porta di destinazione riceve copie del traffico inviato e ricevuto per tutte le porte di origine monitorate. Se una porta di destinazione ha una sottoscrizione eccessiva, potrebbe diventare congestionata. Questa congestione può influire sull'inoltro del traffico su una o più porte di origine.

La funzione VACL Capture Port consente di superare alcune di queste limitazioni. I VACL non sono progettati principalmente per monitorare il traffico. Tuttavia, con una vasta gamma di funzionalità per la classificazione del traffico, è stata introdotta la funzione Capture Port che consente di semplificare l'analisi del traffico di rete. Di seguito sono riportati i vantaggi dell'utilizzo della porta di acquisizione VACL rispetto a VSPAN:

- Analisi granulare del traffico
  I VACL possono corrispondere in base all'indirizzo IP di origine, all'indirizzo IP di destinazione, al tipo di protocollo di livello 4, alle porte di origine e di destinazione di livello 4 e ad altre informazioni. Questa funzionalità rende i VACL molto utili per l'identificazione e il filtraggio granulari del traffico.
- Numero di sessioni
  I VACL vengono applicati nell'hardware. Il numero di ACE che è possibile creare dipende dal TCAM disponibile negli switch.
- Sovrascrittura porta di destinazione
  L'identificazione granulare del traffico riduce il numero di frame da inoltrare alla porta di destinazione e, di conseguenza, riduce al minimo la probabilità di una sovrascrittura.
- Prestazioni
  I VACL vengono applicati nell'hardware. L'applicazione dei VACL a una VLAN sugli switch Cisco Catalyst serie 6500 non comporta alcuna riduzione delle prestazioni.

Configurazione

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

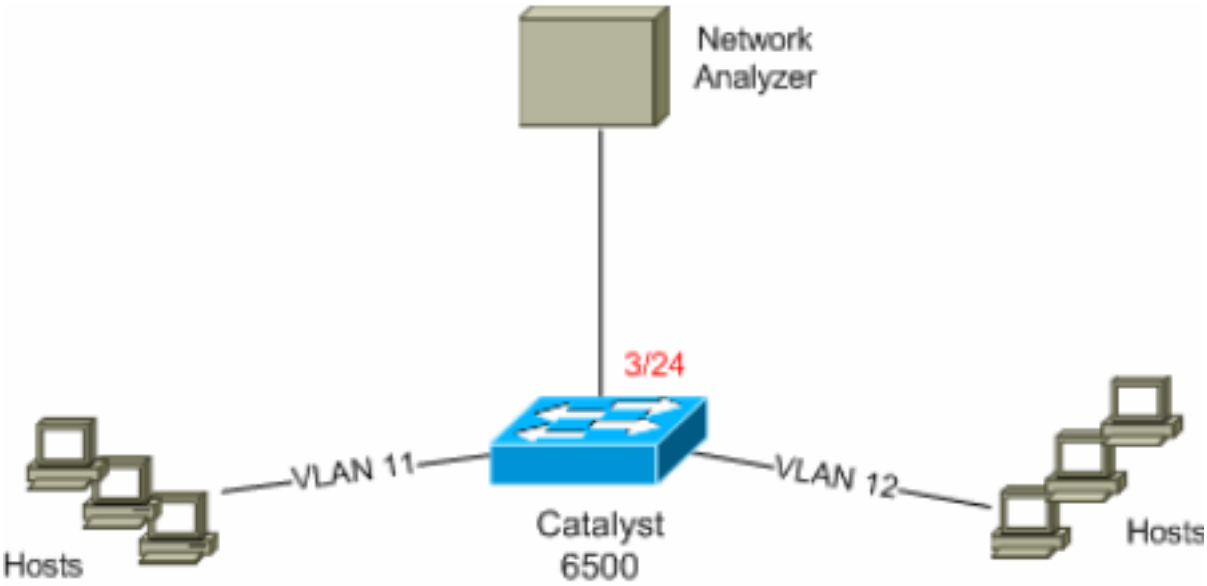
Nel documento vengono usate queste configurazioni:

- Configurazione con SPAN basato su VLAN
- Configurazione con VACL

Nota: per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo strumento di ricerca dei comandi (solo utenti registrati).

Esempio di rete

Nel documento viene usata questa impostazione di rete:



Configurazione con SPAN basato su VLAN

In questo esempio di configurazione vengono elencati i passaggi necessari per acquisire tutto il traffico di layer 2 che scorre nella VLAN 11 e nella VLAN 12 e inviarlo al dispositivo Network Analyzer.

1. Specificare il traffico interessante.Nell'esempio, il traffico viene trasmesso sulla VLAN 100 e sulla VLAN 200.

```
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
```

   Con questo comando, tutto il traffico di layer 2 che appartiene alla VLAN 1 e alla VLAN 12 viene copiato e inviato alla porta 3/24.
2. Verificare la configurazione SPAN con il comando **show span all**.

```
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)
```

Configurazione con VACL

In questo esempio di configurazione l'amministratore di rete deve soddisfare diversi requisiti:

- Ènecessario acquisire il traffico HTTP da un intervallo di host (10.12.12.128/25) nella VLAN 12 a un server specifico (10.11.11.100) nella VLAN 11.
- Il traffico UDP (Multicast User Datagram Protocol) nella direzione di trasmissione destinata all'indirizzo di gruppo 239.0.0.100 deve essere acquisito dalla VLAN 11.

1. Definire il traffico interessante utilizzando gli ACL di sicurezza. Ricordarsi di menzionare l'**acquisizione** della parola chiave per tutte le ACE definite.

```
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. Verificare che la configurazione ACE sia corretta e nell'ordine corretto.

```
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. Eseguire il commit dell'ACL nell'hardware.

```
6K-CatOS> (enable) commit security acl HttpUdp_Acl
ACL commit in progress.

ACL 'HttpUdp_Acl' successfully committed.
6K-CatOS> (enable)
```

4. Verificare lo stato dell'ACL.

```
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. Applicare la mappa di accesso VLAN alle VLAN appropriate.

```
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. Verificare il mapping tra ACL e VLAN.

```
6K-CatOS> (enable) show security acl map HttpUdp_Acl
ACL HttpUdp_Acl is mapped to VLANs:
11
6K-CatOS> (enable)
```

7. Configurare la porta di acquisizione.

```
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)
```

Nota: se un ACL è mappato a più VLAN, la porta di acquisizione deve essere configurata su tutte le VLAN. Per fare in modo che la porta di acquisizione consenta più VLAN, configurare la porta come trunk e consentire solo le VLAN mappate all'ACL. Ad esempio, se l'ACL è mappato alle VLAN 1 e 12, completare la configurazione.

```
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. Verificare la configurazione della porta di acquisizione.

```
6K-CatOS> (enable) show security acl capture-ports
ACL Capture Ports: 3/24
6K-CatOS> (enable)
```

Verifica

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

Lo strumento Output Interpreter (solo utenti registrati) (OIT) supporta alcuni comandi **show**. Usare l'OIT per visualizzare un'analisi dell'output del comando **show**.

- **show security acl info**: visualizza il contenuto del VACL attualmente configurato o di cui è stato eseguito l'ultimo commit nella NVRAM e nell'hardware.

```
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 map**: visualizza il mapping tra ACL e VLAN o tra ACL e porta per un ACL, una porta o una VLAN specifica.

```
6K-CatOS> (enable) show security acl map all
ACL Name                        Type Vlans
------------------------------- ---- -----
HttpUdp_Acl                        IP   11
6K-CatOS> (enable)
```

- **show security acl capture-ports**: visualizza l'elenco delle porte di acquisizione.

```
6K-CatOS> (enable) show security acl capture-ports
ACL Capture Ports: 3/24
6K-CatOS> (enable)
```

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.

Informazioni correlate

- Acquisizione VACL per l'analisi granulare del traffico con Cisco Catalyst 6000/6500 con software Cisco IOS
- Configurazione del controllo di accesso - Guida alla configurazione del software Catalyst serie 6500, 8.6
- Pagine di supporto dei prodotti LAN
- Pagina di supporto dello switching LAN
- Documentazione e supporto tecnico – Cisco Systems