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

Sommario

Introduzione

In questo documento viene fornita una configurazione di esempio per l'uso della funzione VLAN ACL (VACL) Capture Port per l'analisi del traffico di rete in modo più granulare. In questo documento viene descritto anche il vantaggio dell'uso della porta di acquisizione VACL rispetto all'uso della VSPAN (VLAN-based SPAN).

Per configurare la funzione VACL capture-port su Cisco Catalyst 6000/6500 con software Catalyst OS, fare riferimento a VACL Capture for Granular Traffic Analysis (Acquisizione VACL per analisi del traffico granulare) con Cisco Catalyst 6000/6500 con software CatOS.

Prerequisiti

Requisiti

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

- Elenchi di accesso IP: per ulteriori informazioni, fare riferimento a Configurazione degli elenchi di accesso IP.
- LAN virtuale: per ulteriori informazioni, fare riferimento a Virtual LAN/VLAN Trunking Protocol (VLAN/VTP) - Introduzione.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware: Switch Cisco Catalyst serie 6506 con software Cisco IOS® versione 12.2(18)SXF8.

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 software Cisco IOS versione 12.1(13)E e successive.

Convenzioni

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

Premesse

SPAN basato su VLAN

SPAN (Switched Port Analyzer) 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 VLAN di origine è una VLAN monitorata per l'analisi del traffico di rete. La VSPAN (VLAN-based SPAN) utilizza una VLAN come origine dello SPAN. Tutte le porte nelle VLAN di origine diventano porte di origine. Una porta di origine è una porta monitorata per l'analisi del traffico di rete. Le porte trunk possono essere configurate come porte di origine e combinate con porte di origine non trunk, ma SPAN non copia l'incapsulamento da una porta trunk di origine.

Per le sessioni VSPAN con entrambe le configurazioni di entrata e uscita, due pacchetti vengono inoltrati dalla porta di destinazione se i pacchetti vengono attivati sulla stessa VLAN (uno come traffico in entrata dalla porta di entrata e uno come traffico in uscita dalla porta di uscita).

VSPAN monitora solo il traffico che entra o esce dalle porte di livello 2 nella VLAN.

- Se si configura una VLAN come origine in entrata e il traffico viene instradato alla VLAN monitorata, il traffico instradato non viene monitorato in quanto non viene mai visualizzato come traffico in entrata su una porta di layer 2 della VLAN.
- Se si configura una VLAN come origine di uscita e il traffico viene indirizzato dalla VLAN

monitorata, il traffico indirizzato non viene monitorato perché non viene mai visualizzato come traffico in uscita che lascia una porta di layer 2 nella VLAN.

Per ulteriori informazioni sulle VLAN di origine, consultare il documento sulle caratteristiche della VLAN di origine.

ACL VLAN

I VACL possono fornire il controllo dell'accesso per tutti i pacchetti di cui è stato eseguito il bridging all'interno di una VLAN o che sono instradati verso o da una VLAN o un'interfaccia WAN per l'acquisizione dei VACL. A differenza degli ACL standard o estesi Cisco IOS che sono configurati solo sulle interfacce del router e vengono applicati solo ai pacchetti indirizzati, i VACL si applicano a tutti i pacchetti e possono essere applicati a qualsiasi interfaccia VLAN o WAN. I VACL vengono elaborati nell'hardware. I VACL utilizzano ACL Cisco IOS. I VACL ignorano i campi ACL di Cisco IOS non supportati nell'hardware.

È possibile configurare i VACL per il traffico IP, IPX e MAC-Layer. I VACL applicati alle interfacce WAN supportano solo il traffico IP per l'acquisizione dei VACL.

Quando si configura un VACL e lo si applica a una VLAN, tutti i pacchetti che entrano nella VLAN vengono controllati rispetto a questo VACL. Se si applica un VACL alla VLAN e un ACL a un'interfaccia instradata nella VLAN, un pacchetto che entra nella VLAN viene prima controllato rispetto al VACL e, se autorizzato, viene quindi confrontato con l'ACL di input prima di essere gestito dall'interfaccia instradata. Quando il pacchetto viene indirizzato a un'altra VLAN, viene prima verificato rispetto all'ACL di output applicato all'interfaccia indirizzata e, se autorizzato, viene applicato il VACL configurato per la VLAN di destinazione. Se un VACL è configurato per un tipo di pacchetto e un pacchetto di questo tipo non corrisponde al VACL, l'azione predefinita è Nega. Linee guida per l'opzione di acquisizione in VACL.

- La porta di acquisizione non può essere una porta ATM.
- La porta di acquisizione deve essere nello stato di inoltro Spanning-Tree per la VLAN.
- Lo switch non ha restrizioni sul numero di porte di acquisizione.
- La porta di acquisizione acquisisce solo i pacchetti consentiti dall'ACL configurato.
- Le porte di acquisizione trasmettono solo il traffico che appartiene alla VLAN della porta di acquisizione. Configurare la porta di acquisizione come trunk che trasporta le VLAN richieste in modo da acquisire il traffico diretto a molte VLAN.

Attenzione: una combinazione errata di ACL può interrompere il flusso del traffico. Prestare particolare attenzione quando si configurano gli ACL nel dispositivo.

Nota: VACL non è supportato con IPv6 su uno switch Catalyst serie 6000. In altre parole, il reindirizzamento degli ACL VLAN e l'IPv6 non sono compatibili, pertanto non è possibile utilizzare gli ACL per la corrispondenza con il traffico IPv6.

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

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

- Tutto il traffico di layer 2 che scorre su una VLAN viene acquisito. 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 Limiti di sessioni SPAN e RSPAN locali.

- 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, ma, con un'ampia gamma di funzionalità per classificare il traffico, è stata introdotta la funzionalità Porta di acquisizione in modo che l'analisi del traffico di rete possa diventare molto più semplice. 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 voci di controllo di accesso (ACE, Access Control Entries) che è possibile creare dipende dal TCAM disponibile sugli 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

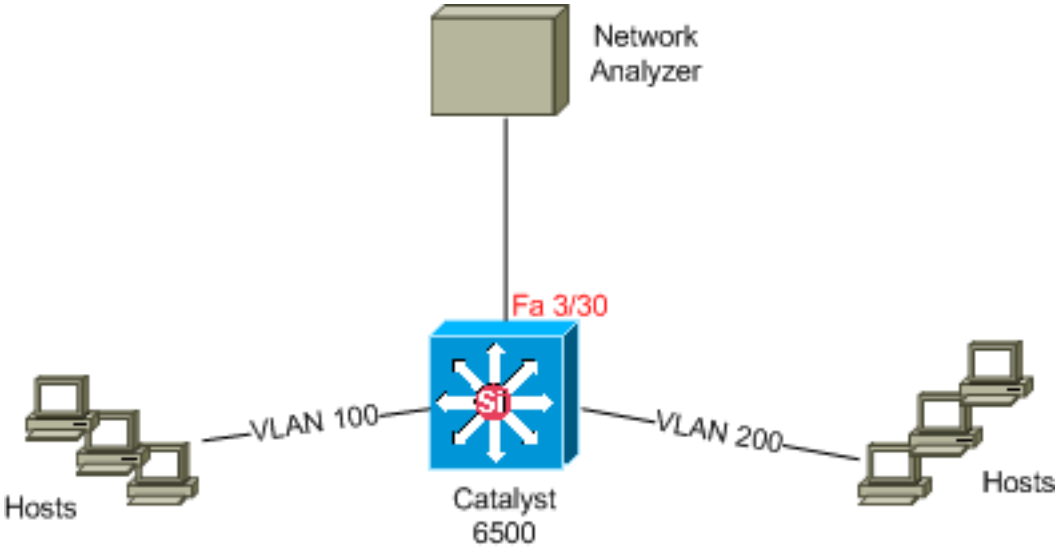
In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

- Configurazione con SPAN basato su VLAN
- Configurazione con VACL

Nota: per ulteriori informazioni sui comandi menzionati in questo documento, 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 100 e nella VLAN 200 e inviarlo al dispositivo Network Analyzer.

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

```
Cat6K-IOS#conf t
Cat6K-IOS(config)#monitor session 50 source vlan 100 , 200 ?
  ,     Specify another range of VLANs
  -     Specify a range of VLANs
  both  Monitor received and transmitted traffic
  rx    Monitor received traffic only
  tx    Monitor transmitted traffic only
  <cr>

 !--- Default is to monitor both received and transmitted traffic

Cat6K-IOS(config)#monitor session 50 source vlan 100 , 200
Cat6K-IOS(config)#
```

2. Specificare la porta di destinazione per il traffico acquisito.

```
Cat6K-IOS(config)#monitor session 50 destination interface Fa3/30
Cat6K-IOS(config)#
```

In questo modo, tutto il traffico di layer 2 che appartiene alla VLAN 100 e alla VLAN 200 viene copiato e inviato alla porta Fa3/30. Se la porta di destinazione fa parte della stessa VLAN di cui viene monitorato il traffico, il traffico che esce dalla porta di destinazione non viene acquisito.

Verificare la configurazione SPAN con il comando **show monitor**.

```
Cat6K-IOS#show monitor detail
Session 50
----------
Type               : Local Session
Source Ports       :
    RX Only        : None
    TX Only        : None
    Both           : None
Source VLANs       :
    RX Only        : None
```

```
    TX Only       : None
    Both          : 100,200
Source RSPAN VLAN : None
Destination Ports : Fa3/30
Filter VLANs      : None
Dest RSPAN VLAN   : None
```

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 (10.20.20.128/25) nella VLAN 200 a un server specifico (10.10.10.101) nella VLAN 100.
- 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 100.

1. Definire il traffico interessante da acquisire e inviare all'analisi.
```
Cat6K-IOS(config)#ip access-list extended HTTP_UDP_TRAFFIC
Cat6K-IOS(config-ext-nacl)#permit tcp 10.20.20.128 0.0.0.127 host 10.10.10.101 eq www
Cat6K-IOS(config-ext-nacl)#permit udp any host 239.0.0.100
Cat6K-IOS(config-ext-nacl)#exit
```
2. Definire un ACL con più numeri per mappare tutto il resto del traffico.
```
Cat6K-IOS(config)#ip access-list extended ALL_TRAFFIC
Cat6K-IOS(config-ext-nacl)#permit ip any any
Cat6K-IOS(config-ext-nacl)#exit
```
3. Definire la mappa di accesso alla VLAN.
```
Cat6K-IOS(config)#vlan access-map HTTP_UDP_MAP 10
Cat6K-IOS(config-access-map)#match ip address HTTP_UDP_TRAFFIC
Cat6K-IOS(config-access-map)#action forward capture
Cat6K-IOS(config)#vlan access-map HTTP_UDP_MAP 20
Cat6K-IOS(config-access-map)#match ip address ALL_TRAFFIC
Cat6K-IOS(config-access-map)#action forward
Cat6K-IOS(config-access-map)#exit
```
4. Applicare la mappa di accesso VLAN alle VLAN appropriate.
```
Cat6K-IOS(config)#vlan filter HTTP_UDP_MAP vlan-list 100
!--- Here 100 is the ID of VLAN on which the VACL is applied.
```
5. Configurare la porta di acquisizione.
```
Cat6K-IOS(config)#int fa3/30
Cat6K-IOS(config-if)#switchport capture allowed vlan ?
  WORD    VLAN IDs of the allowed VLANs when this po
  add     add VLANs to the current list
  all     all VLANs
  except  all VLANs except the following
  remove  remove VLANs from the current list

Cat6K-IOS(config-if)#switchport capture allowed vlan 100
Cat6K-IOS(config-if)#switchport capture
Cat6K-IOS(config-if)#exit
```

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 vlan access-map**: visualizza il contenuto delle mappe di accesso VLAN.

```
Cat6K-IOS#show vlan access-map HTTP_UDP_MAP
Vlan access-map "HTTP_UDP_MAP"  10
        match: ip address HTTP_UDP_TRAFFIC
        action: forward capture
Vlan access-map "HTTP_UDP_MAP"  20
        match: ip address ALL_TRAFFIC
        action: forward
```

- **show vlan filter**: visualizza le informazioni sui filtri VLAN.

```
Cat6K-IOS#show vlan filter
VLAN Map HTTP_UDP_MAP:
        Configured on VLANs:  100
            Active on VLANs:  100
```

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 CatOS
- Cisco Catalyst serie 6500 Switch supportati
- Supporto dei prodotti LAN
- Supporto della tecnologia di switching LAN
- Documentazione e supporto tecnico – Cisco Systems