

SPAN basato sul flusso alternativa all'acquisizione VACL

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Convenzioni](#)

[Procedura](#)

[Restrizioni](#)

[Informazioni correlate](#)

Introduzione

In questo documento viene descritto come usare un FSPAN (Flow-Based Switched Port Analyzer) per acquisire il traffico filtrato sugli switch Cisco Catalyst che non supportano l'acquisizione di VACL (VLAN Access Control List).

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco Catalyst serie 3750-X Switch
- Cisco Catalyst serie 3560-X Switch
- Cisco Catalyst serie 3750-E Switch
- Cisco Catalyst serie 3560-E Switch
- Cisco Catalyst serie 2960-X Switch con licenza Iplite
- Cisco IOS[®] versione 12.2(44)SE e successive

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.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento [Cisco sulle convenzioni nei suggerimenti tecnici](#).

Procedura

gli switch Cisco Catalyst 3750-X, 3560-X, 3750-E, 3560-E e 2960-X (licenza esclusiva) non supportano l'acquisizione VACL; tuttavia, questi switch supportano SPAN basato sul flusso e RSPAN (Flow-Based Remote SPAN), che possono ottenere risultati simili all'acquisizione delle VACL.

L'SPAN basato sul flusso fornisce un meccanismo per utilizzare i filtri specificati al fine di acquisire i dati richiesti tra gli host terminali.

Alla sessione SPAN è possibile allegare tre tipi di elenchi di controllo di accesso (ACL) FSPAN:

- ACL FSPAN IPv4: filtra solo i pacchetti IPv4.
- ACL FSPAN IPv6: filtra solo i pacchetti IPv6.
- ACL MAC FSPAN: filtra solo pacchetti non IP.

Gli ACL di sicurezza hanno una priorità più alta degli ACL FSPAN su uno switch. Se si applicano gli ACL FSPAN e quindi si aggiungono altri ACL di sicurezza che non possono essere contenuti nella memoria hardware, gli ACL FSPAN vengono rimossi dalla memoria in modo da liberare spazio per gli ACL di sicurezza. Un messaggio di sistema informa l'utente di questa azione, denominata scaricamento.

Quando lo spazio è nuovamente disponibile, gli ACL FSPAN vengono aggiunti nuovamente alla memoria hardware dello switch. Un messaggio di sistema informa l'utente di questa azione, denominata ricaricamento.

Gli switch 3750-X supportano fino a due sessioni SPAN e FSPAN non può evitare questo limite. FSPAN utilizza lo stesso ASIC di replica di un normale SPAN.

Questo è un esempio di utilizzo di FSPAN su uno switch 3750-X:

```
3750X(config)#ip access-list extended FILTER
3750X(config-ext-nacl)#permit ip host 192.168.1.1 host 172.16.1.1
3750X(config-ext-nacl)#exit
3750X(config)#monitor session 1 source interface gil/0/1 both3750X
(config)#monitor session 1 destination interface gil/0/2 3750X
(config)#monitor session 1 filter ip access-group FILTER
```

```
3750X(config)##exit3750X#show monitor session
sh mon session 1
Session 1
-----
Type                : Local Session
```

```
Source Ports          :  
  Both               : Gi1/0/1Destination Ports      : Gi1/0/2  
  Encapsulation      : Native  
    Ingress          : Disabled  
IP Access-group      : FILTER
```

Restrizioni

- FSPAN non è supportato sugli switch 3750, 3750G, 2950, 2960 e 2960-S.
- La versione 2960-X con licenza Iplite supporta solo FSPAN.
- È possibile associare gli ACL a una sola sessione SPAN o RSPAN alla volta.
- Quando non sono collegati ACL FSPAN, FSPAN viene disabilitato e tutto il traffico viene copiato sulle porte di destinazione SPAN.
- Quando è collegato almeno un ACL FSPAN, FSPAN è abilitato.
- Quando si collega un ACL FSPAN vuoto a una sessione SPAN, i pacchetti non vengono filtrati e tutto il traffico viene monitorato.
- Le porte Catalyst 3750 possono essere aggiunte come porte di destinazione in una sessione FSPAN.
- Le sessioni FSPAN basate su VLAN non possono essere configurate su uno stack che include gli switch Catalyst 3750.
- EtherChannel non è supportato in una sessione FSPAN.
- Gli ACL FSPAN con flag TCP o la parola chiave **log** non sono supportati.
- Le sessioni FSPAN basate sulla porta possono essere configurate su uno stack che include switch Catalyst 3750 a condizione che la sessione includa solo le porte Catalyst 3750-E come porte di origine. Se la sessione ha porte Catalyst 3750 come porte di origine, il comando FSPAN ACL viene rifiutato.

Informazioni correlate

- [Documentazione e supporto tecnico – Cisco Systems](#)