Informazioni sui contatori ACL di crittografia nei tunnel VPN basati su criteri

Sommario

Introduzione

Prerequisiti

- Requisiti
- Componenti usati

Topologia

Scenari

- Scenario 1: Traffico avviato dal router1 mentre il tunnel VPN è inattivo
- Scenario 2: Traffico avviato dal router2 mentre il tunnel VPN è attivo

Configurazione

- Configurazione della crittografia sul router1
- Configurazione della crittografia sul router2

Analisi comportamentale dei contatori della lista di controllo dell'accesso crittografica nei tunnel VPN

- Scenario 1: Traffico avviato dal router1 mentre il tunnel VPN è inattivo
- Scenario due: traffico avviato dal router2 mentre il tunnel VPN è attivo

Conclusione:

Soluzioni chiave:

Introduzione

In questo documento viene descritto il comportamento dei contatori ACL (Access Control List) crittografici all'interno dei tunnel VPN basati su criteri.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- VPN da sito a sito basata su criteri su piattaforma Cisco IOS® /Cisco IOS® XE
- Access Control List su piattaforma Cisco IOS/Cisco IOS XE

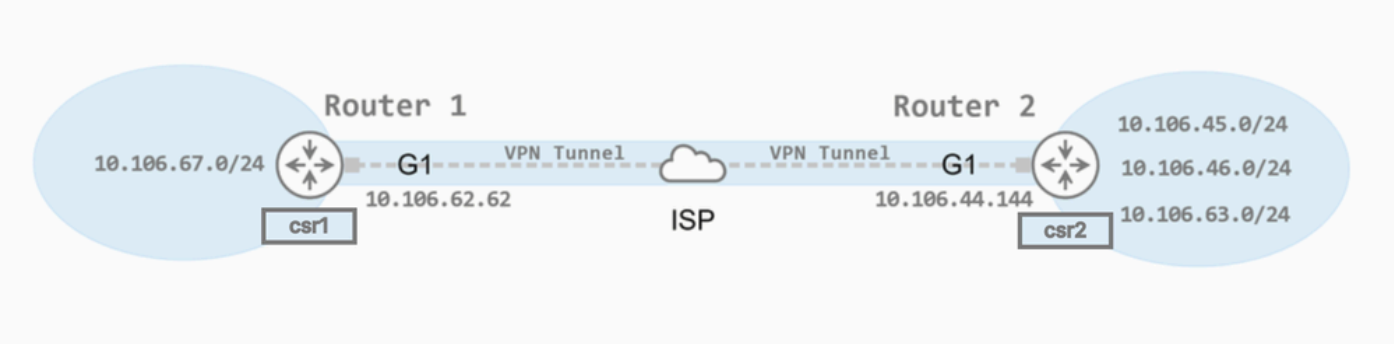
Componenti usati

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

- Cisco C8kv, versione 17.12.04(MD)

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.

Topologia



Topologia

Scenari

Esaminando due scenari distinti, desideriamo capire come i conteggi degli accessi vengono influenzati quando il traffico viene iniziato da peer diversi e quando i tunnel vengono reimpostati.

1. Scenario 1: Traffico avviato dal router1 mentre il tunnel VPN è inattivo

   In questo scenario, le modifiche nei conteggi visite ACL vengono analizzate quando il tunnel VPN è inizialmente inattivo e il traffico viene iniziato dal router1. Questa analisi aiuta a comprendere la configurazione iniziale e come i contatori ACL crittografici reagiscono al primo tentativo di flusso del traffico.

2. Scenario 2: Traffico avviato dal router2 mentre il tunnel VPN è attivo

   In questo scenario, il tunnel VPN è già stato stabilito e il traffico proveniente dal router2 viene avviato. In questo scenario viene illustrato il comportamento dei contatori ACL quando il tunnel è attivo e il traffico viene introdotto da un peer diverso.

Confrontando questi scenari, possiamo ottenere una comprensione completa delle dinamiche dei contatori ACL nei tunnel VPN in condizioni diverse.

Configurazione

È stato configurato un tunnel VPN da sito a sito basato su criteri tra due router Cisco C8kv, designati come peer. Il nome del router1 è "csr1" e il nome del router2 è "csr2".

Configurazione della crittografia sul router1

```
csr1#sh ip int br
Interface              IP-Address      OK?   Method   Status  Protocol
GigabitEthernet1       10.106.62.62    YES   NVRAM    up      up
GigabitEthernet2       10.106.67.27    YES   NVRAM    up      up
```

```
csr1#sh run | sec crypto map
crypto map nigarapa_map 100 ipsec-isakmp
   set peer 10.106.44.144
   set transform-set new_ts
   set ikev2-profile new_profile
   match address new_acl
```

```
csr1#sh ip access-lists new_acl
Extended IP access list new_acl
   10 permit ip 10.106.67.0 0.0.0.255 10.106.45.0 0.0.0.255 log
   20 permit ip 10.106.67.0 0.0.0.255 10.106.46.0 0.0.0.255
   30 permit ip 10.106.67.0 0.0.0.255 10.106.63.0 0.0.0.255 log
```

```
csr1#sh run int GigabitEthernet1
Building configuration...

Current configuration : 162 bytes
!
interface GigabitEthernet1
ip address 10.106.62.62 255.255.255.0
ip nat outside
negotiation auto
no mop enabled
no mop sysid
crypto map nigarapa_map
end
```

Configurazione della crittografia sul router2

```
csr2#sh ip int br
Interface              IP-Address        OK?     Method       Status     Protocol
GigabitEthernet1       10.106.44.144     YES     NVRAM        up         up
GigabitEthernet2       10.106.45.145     YES     NVRAM        up         up
GigabitEthernet3       10.106.46.146     YES     NVRAM        up         up
GigabitEthernet4       10.106.63.13      YES     NVRAM        up         up
```

```
csr2#sh run | sec crypto map
crypto map nigarapa_map 100 ipsec-isakmp
   set peer 10.106.62.62
   set transform-set new_ts
   set ikev2-profile new_profile
   match address new_acl
```

```
csr2#sh ip access-lists new_acl
Extended IP access list new_acl
   10 permit ip 10.106.45.0 0.0.0.255 10.106.67.0 0.0.0.255
   20 permit ip 10.106.46.0 0.0.0.255 10.106.67.0 0.0.0.255
   30 permit ip 10.106.63.0 0.0.0.255 10.106.67.0 0.0.0.255
```

```
csr2#sh run int GigabitEthernet1
Building configuration...

Current configuration : 163 bytes
!
interface GigabitEthernet1
ip address 10.106.44.144 255.255.255.0
ip nat outside
negotiation auto
no mop enabled
no mop sysid
crypto map nigarapa_map
end
```

Analisi comportamentale dei contatori della lista di controllo dell'accesso crittografica nei tunnel VPN

Inizialmente, entrambi i dispositivi hanno un numero di accessi ACL pari a zero nei rispettivi elenchi degli accessi crittografati.

Il numero di accessi della lista di controllo dell'accesso è zero nei rispettivi elenchi degli accessi crittografici su entrambi i dispositivi peer.

Scenario 1: Traffico avviato dal router1 mentre il tunnel VPN è inattivo

Stato iniziale:

Il tunnel VPN che connette il router1 (IP: 10.106.67.27) e router2 (IP: 10.106.45.145) è attualmente inattivo.

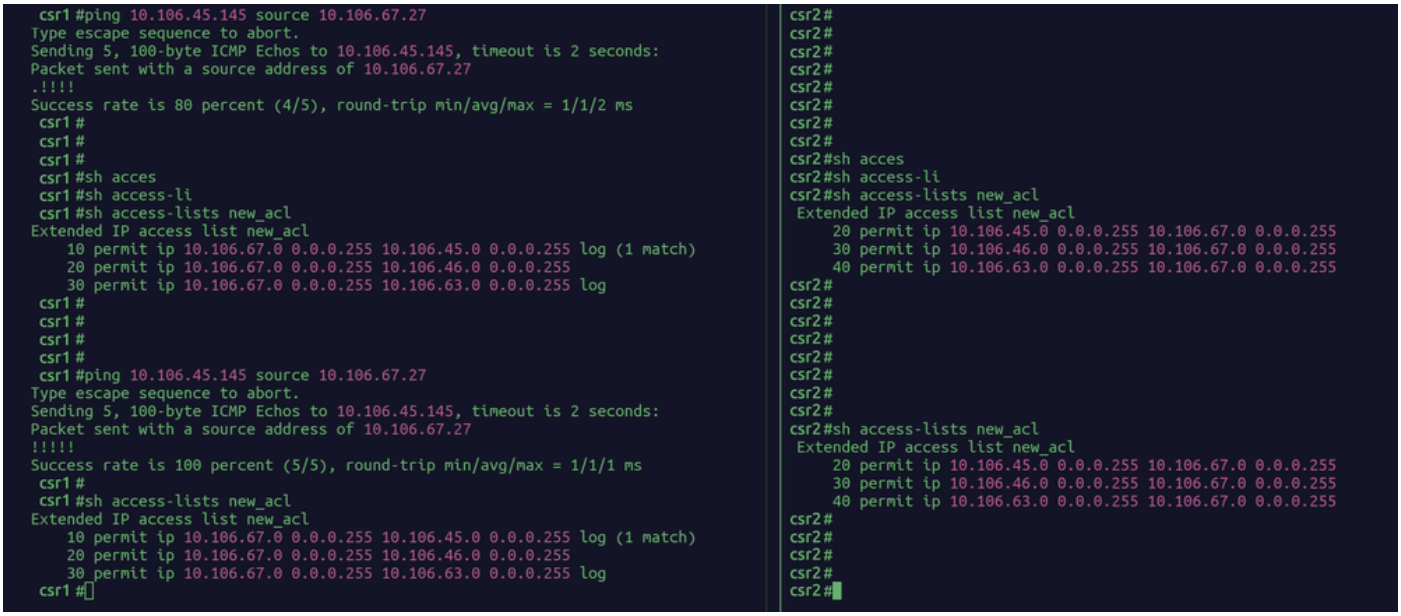
Azione intrapresa:

Il traffico viene avviato da Router1 per stabilire una comunicazione con Router2.

Osservazioni:

1. Comportamento contatore ACL:
   r. Quando si avvia il traffico proveniente dal router1, si verifica un aumento notevole nel contatore dell'elenco di controllo di accesso (ACL) sul router1. Questo aumento si verifica solo una volta nel momento in cui il tunnel tenta di stabilire.
   b. L'aumento del contatore ACL viene osservato solo sul router che avvia il sistema, in questo scenario è il router1. In questa fase, il router2 non riflette alcuna modifica nel contatore ACL.
2. Creazione tunnel:
   r. Dopo l'incremento iniziale corrispondente all'inizio del traffico, il tunnel tra il primo router e il router2 viene stabilito correttamente.
   b. Dopo la creazione del tunnel, il contatore ACL sul router1 si stabilizza e non mostra ulteriori incrementi, indicando che la regola ACL è stata soddisfatta e che ora il traffico viene autorizzato in modo costante attraverso il tunnel stabilito.
3. Riavvio tunnel:
   Il contatore ACL sul router1 subisce un altro incremento solo se il tunnel viene interrotto e deve essere ristabilito. Ciò suggerisce che la regola ACL venga attivata dall'inizio del traffico iniziale che tenta di stabilire il tunnel, piuttosto che dal trasferimento di dati in corso una volta che il tunnel è attivo.

In sintesi, questo scenario dimostra che il contatore ACL sul router1 è sensibile ai tentativi di traffico iniziali per la creazione del tunnel, ma rimane statico una volta che il tunnel VPN è attivo e operativo.



Scenaria 1

Scenario due: traffico avviato dal router2 mentre il tunnel VPN è attivo

Stato iniziale:

Il tunnel VPN che connette il router1 (IP: 10.106.67.27) e router2 (IP: 10.106.45.145) è attualmente attiva e operativa.

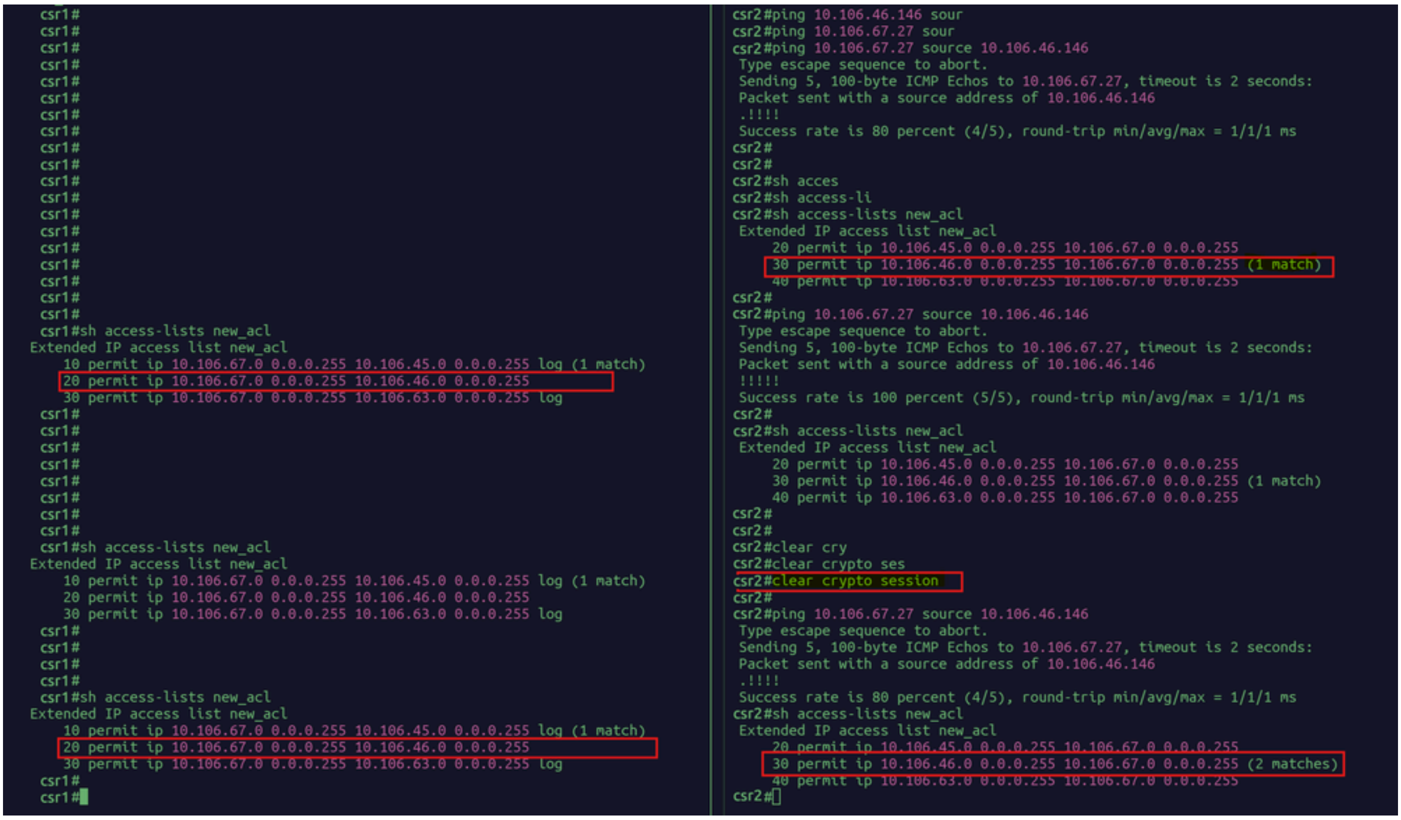
Azione intrapresa:

1. Il traffico viene avviato dal router2 verso il router1 mentre il tunnel è attivo.
2. Successivamente, il tunnel viene deliberatamente cancellato (o ripristinato).
3. Dopo aver cancellato il tunnel, il router2 riavvia il traffico per ristabilire la connessione.

Osservazioni:

1. Inizio traffico iniziale:
   r. Quando il traffico viene avviato per la prima volta dal router2 mentre il tunnel è già stato stabilito, non vi sono modifiche immediate nel contatore dell'elenco di controllo di accesso (ACL).
   b. Ciò indica che il traffico in corso all'interno di un tunnel già stabilito non attiva l'incremento del contatore ACL.
2. Cancellazione e riavvio del tunnel:
   r. Dopo aver cancellato il tunnel, la connessione stabilita tra il primo router e il router2 viene temporaneamente interrotta. Ciò richiede un processo di ristabilimento per qualsiasi traffico successivo.
   b. Quando il traffico viene riavviato dal router2 dopo che il tunnel è stato svuotato, si verifica un incremento osservabile nel contatore ACL sul router2. Questo incremento indica che le regole ACL vengono applicate ancora una volta per facilitare la creazione del tunnel.
3. Specificità contatore ACL:
   L'incremento del contatore ACL si verifica solo sul lato che inizia il traffico, nel caso specifico il router2. Questo comportamento evidenzia il ruolo dell'ACL nel monitoraggio e nel controllo dei processi di inizio del traffico sul lato di origine, mentre il contatore ACL del router1 rimane invariato in questa fase.

In sintesi, in questo scenario viene mostrato che il contatore ACL sul router2 risponde all'avvio del traffico quando si ristabilisce un tunnel VPN. Il contatore non aumenta con il flusso regolare del traffico all'interno di un tunnel attivo, ma reagisce all'esigenza di ristabilire il tunnel, garantendo una tracciatura precisa degli eventi di avvio del tunnel.



Scenario 2

Conclusione:

Il comportamento dei contatori ACL crittografici rivela che registrano i conteggi degli accessi esclusivamente durante la fase di avvio del tunnel VPN.

Incremento specifico iniziatore: Quando il tunnel viene avviato dal router1, l'aumento del numero di accessi viene osservato solo sul router1. Analogamente, se l'avvio viene eseguito dal router2, il numero di accessi viene aumentato solo sul router2. Ciò evidenzia il ruolo dell'ACL nel monitoraggio del processo di avvio del traffico all'origine.

Stabilità post-istituzione: Una volta stabilito il tunnel, i contatori ACL su entrambi i peer rimangono invariati, indicando che non ci sono altri accessi. Questa stabilità persiste fino a quando il tunnel non viene cancellato o reimpostato e viene eseguito un nuovo tentativo di avvio del traffico. Questo comportamento sottolinea la funzionalità degli Access Control List nel tracciare e controllare la fase iniziale di creazione del tunnel, assicurando che il successivo flusso di dati all'interno del tunnel stabilito non influisca sul numero di accessi.

Soluzioni chiave:

Comportamento contatore ACL: I contatori ACL registrano gli incrementi esclusivamente sul lato iniziatore durante il processo di avvio del tunnel. Vale a dire che i contatori sono progettati per monitorare il traffico iniziale che attiva la definizione del tunnel.

Contatori statici successivi all'istituzione: Dopo aver attivato e stabilito il tunnel, i contatori ACL rimangono invariati. e non riflettono altre attività a meno che il tunnel non venga reimpostato e non

debba essere riavviato, sottolineando l'importanza degli eventi iniziali del traffico.

Specificità avvio traffico: Il numero di accessi ACL è specifico del peer che avvia il tunnel. Questa specificità assicura un tracciamento preciso di quale parte è responsabile dell'inizializzazione della connessione VPN, consentendo un monitoraggio e un controllo accurati.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).