Risoluzione dei problemi di configurazione di Cisco IOS Firewall

Sommario

Introduzione

In questo documento vengono fornite informazioni che permettono di risolvere i problemi relativi alle configurazioni di Cisco IOS® Firewall.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Convenzioni

Fare riferimento a Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti.

Risoluzione dei problemi

Nota: consultare le informazioni importanti sui comandi di debug prima di usare i comandi di **debug**.

- Per invertire (rimuovere) un elenco degli accessi, specificare "no" davanti al comando **access-group** in modalità di configurazione interfaccia:

```
int
```

- Se viene rifiutato un volume troppo elevato di traffico, riesaminare la logica dell'elenco e cercare di definire un elenco più ampio, quindi applicarlo. Ad esempio:

```
access-list # permit tcp any any
access-list # permit udp any any
access-list # permit icmp any any
int
```

- Il comando **show ip access-lists** mostra gli elenchi degli accessi applicati e il traffico da essi negato. Se si controlla il numero di pacchetti negati prima e dopo l'operazione non riuscita con l'indirizzo IP di origine e di destinazione, questo numero aumenta se l'elenco degli accessi blocca il traffico.
- Se il router non è caricato molto, il debug può essere eseguito a livello di pacchetto sull'elenco degli accessi esteso o ip inspect. Se il router è molto carico, il traffico sul router è rallentato. Utilizzare la discrezione con i comandi di debug.Aggiungere temporaneamente il comando **no ip route-cache** all'interfaccia:

```
int
```

Quindi, in modalità abilitazione (ma non config):

```
term mon
debug ip packet # det
```

produce un output simile al seguente:

```
*Mar 1 04:38:28.078: IP: s=10.31.1.161 (Serial0), d=171.68.118.100 (Ethernet0),
   g=10.31.1.21, len 100, forward
*Mar 1 04:38:28.086: IP: s=171.68.118.100 (Ethernet0), d=9.9.9.9 (Serial0), g=9.9.9.9,
   len 100, forward
```

- Gli elenchi degli accessi estesi possono essere utilizzati anche con l'opzione "log" alla fine delle varie istruzioni:

```
access-list 101 deny ip host 171.68.118.100 host 10.31.1.161 log
access-list 101 permit ip any any
```

Sullo schermo vengono quindi visualizzati messaggi relativi al traffico autorizzato e non autorizzato:

```
*Mar 1 04:44:19.446: %SEC-6-IPACCESSLOGDP: list 111 permitted icmp 171.68.118.100
   -> 10.31.1.161 (0/0), 15 packets
*Mar  1 03:27:13.295: %SEC-6-IPACCESSLOGP: list 118 denied tcp 171.68.118.100(0)
   -> 10.31.1.161(0), 1 packet
```

- Se l'elenco ip inspect è sospetto, il comando **debug ip inspect <tipo_traffico>**restituisce un output come questo:

```
Feb 14 12:41:17 10.31.1.52 56: 3d05h: CBAC* sis 258488 pak 16D0DC TCP P ack 3195751223
   seq 3659219376(2) (10.31.1.5:11109) => (12.34.56.79:23)
Feb 14 12:41:17 10.31.1.52 57: 3d05h: CBAC* sis 258488 pak 17CE30 TCP P ack 3659219378
   seq 3195751223(12) (10.31.1.5:11109) <= (12.34.56.79:23)
```

Per questi comandi e altre informazioni sulla risoluzione dei problemi, consultare il documento sulla risoluzione dei problemi del proxy di autenticazione.

Informazioni correlate

- Supporto dei prodotti Cisco IOS Firewall
- Documentazione e supporto tecnico – Cisco Systems