Cisco IOS Classic Firewall/IPS: Configurazione del controllo degli accessi basato sul contesto (CBAC) per la protezione dalla negazione del servizio

Sommario

Introduzione

In questo documento viene descritta la procedura di ottimizzazione per i parametri DoS (Denial of Service) nel Cisco IOS® Classic Firewall con CBAC.

La funzione CBAC offre funzionalità avanzate di filtro del traffico e può essere utilizzata come parte integrante del firewall di rete.

DoS in genere si riferisce all'attività di rete che, intenzionalmente o meno, sovraccarica le risorse di rete, come la larghezza di banda del collegamento WAN, le tabelle di connessione del firewall, la memoria dell'host finale, la CPU o le funzionalità dei servizi. Nello scenario peggiore, l'attività DoS sovraccarica la risorsa vulnerabile (o destinata) al punto che la risorsa non è più disponibile e impedisce la connettività WAN o l'accesso ai servizi per gli utenti legittimi.

Cisco IOS Firewall può contribuire a mitigare l'attività del servizio DoS se mantiene contatori del numero di connessioni TCP "half-open", nonché la velocità totale di connessione attraverso il firewall e il software di prevenzione delle intrusioni sia nel Classic Firewall (**ip inspect**) che nel Zone-Based Policy Firewall.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

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

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

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

Premesse

Le connessioni half-open sono connessioni TCP che non hanno completato l'handshake SYN-SYN/ACK-ACK a tre vie sempre utilizzato dai peer TCP per negoziare i parametri della connessione reciproca. Un numero elevato di connessioni half-open può indicare attività dannose, ad esempio attacchi DoS o DDoS (Distributed-Denial-of-Service). Un esempio di un tipo di attacco DoS è condotto da software dannoso sviluppato intenzionalmente, come worm o virus che infettano più host su Internet e tentano di sopraffare specifici server Internet con attacchi SYN, dove un gran numero di connessioni SYN vengono inviate a un server da più host su Internet o all'interno della rete privata di un'organizzazione. Gli attacchi SYN rappresentano un pericolo per i server Internet in quanto le tabelle di connessione dei server possono essere caricate con tentativi di connessione SYN "falsi" che arrivano più rapidamente di quanto il server possa gestire le nuove connessioni. Si tratta di un tipo di attacco DoS perché il numero elevato di connessioni nell'elenco delle connessioni TCP del server vittima impedisce l'accesso legittimo dell'utente ai server Internet vittime.

Cisco IOS Firewall inoltre considera "half-open" le sessioni UDP (User Datagram Protocol) con traffico in una sola direzione, in quanto molte applicazioni che utilizzano UDP per il trasporto riconoscono la ricezione dei dati. Le sessioni UDP senza traffico di ritorno sono probabilmente indicative dell'attività DoS o dei tentativi di connessione tra due host, in cui uno degli host non risponde. Molti tipi di traffico UDP, ad esempio i messaggi di log, il traffico di gestione della rete SNMP, lo streaming dei supporti voce e video e il traffico di segnalazione, utilizzano il traffico in una sola direzione per trasportare il traffico. Molti di questi tipi di traffico applicano funzionalità di intelligence specifiche dell'applicazione per impedire che i modelli di traffico unidirezionale influiscano negativamente sul comportamento del firewall e del DoS IPS.

Nelle versioni software Cisco IOS versione 12.4(11)T e 12.4(10), Cisco IOS Stateful Packet Inspection offre protezione dagli attacchi DoS come impostazione predefinita quando viene applicata una regola di ispezione. Le versioni 12.4(11)T e 12.4(10) del software Cisco IOS hanno modificato le impostazioni DoS predefinite in modo che la protezione DoS non venga applicata automaticamente, ma i contatori delle attività di connessione siano ancora attivi. Quando la protezione DoS è attiva, ovvero quando si utilizzano i valori predefiniti in versioni software meno recenti o i valori sono stati modificati in base all'intervallo che influisce sul traffico, la protezione

DoS viene attivata sull'interfaccia in cui viene applicato il controllo, nella direzione in cui viene applicato il firewall, in modo che i protocolli di configurazione dei criteri del firewall possano analizzarla. La protezione DoS è abilitata sul traffico di rete solo se il traffico entra o esce da un'interfaccia con ispezione applicata nella stessa direzione del traffico iniziale (pacchetto SYN o primo pacchetto UDP) per una connessione TCP o una sessione UDP.

L'ispezione di Cisco IOS Firewall fornisce diversi valori regolabili per proteggere dagli attacchi DoS. Le versioni software Cisco IOS precedenti alla 12.4(11)T e alla 12.4(10) hanno valori DoS predefiniti che possono interferire con il corretto funzionamento della rete se non sono configurate per il livello appropriato di attività di rete in reti in cui la velocità di connessione supera i valori predefiniti. Questi parametri consentono di configurare i punti in cui la protezione DoS del router firewall inizia a diventare effettiva. Quando i contatori DoS del router superano i valori predefiniti o configurati, il router ripristina una vecchia connessione half-open per ogni nuova connessione che superi i valori configurati max-incomplete o max-high di un minuto finché il numero di sessioni half-open non scende al di sotto dei valori massimi incompleti. Il router invia un messaggio syslog se la registrazione è abilitata e se sul router è configurato un IPS (Intrusion Prevention System), il router del firewall invia un messaggio di firma DoS tramite lo SDEE (Security Device Event Exchange). Se i parametri DoS non vengono regolati in base al comportamento normale della rete, la normale attività di rete può attivare il meccanismo di protezione DoS, che causa errori dell'applicazione, prestazioni di rete inadeguate e un elevato utilizzo della CPU sul router del firewall Cisco IOS.

Configurazione

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

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

Tuning della negazione del servizio per il software Cisco IOS Classic (IP Inspect) Firewall e sistema di prevenzione delle intrusioni

Il firewall Cisco IOS classico gestisce un insieme globale di contatori DoS per il router e tutte le sessioni del firewall per tutti i criteri del firewall su tutte le interfacce vengono applicate al set globale di contatori del firewall.

Per impostazione predefinita, Cisco IOS Classic Firewall Inspection fornisce protezione dagli attacchi DoS quando viene applicato un firewall classico. La protezione DoS è abilitata su tutte le interfacce a cui viene applicata l'ispezione, nella direzione in cui viene applicato il firewall, per ogni servizio o protocollo che il criterio firewall è configurato per ispezionare. Il firewall classico fornisce diversi valori regolabili per la protezione dagli attacchi DoS. Le impostazioni predefinite legacy (dalle immagini software precedenti alla release 12.4(11)T) mostrate nella tabella 1 possono interferire con il corretto funzionamento della rete se non sono configurate per il livello appropriato di attività di rete nelle reti in cui le velocità di connessione superano i valori predefiniti. Le impostazioni DoS possono essere visualizzate con il comando exec **show ip inspect config** e sono incluse nell'output di **sh ip inspect all**.

La funzione CBAC utilizza i timeout e le soglie per stabilire per quanto tempo gestire le informazioni sullo stato di una sessione e per stabilire quando eliminare le sessioni che non vengono completamente stabilite. Questi timeout e soglie vengono applicati globalmente a tutte le sessioni.

Tabella 1: limiti di protezione DoS predefiniti del firewall classico		
Valore protezione DoS	Prima della versione 12.4(11)T/12.4(10)	12.4(11)T/12.4(10) e successive
valore massimo incompleto	500	Illimitato
valore minimo max incompleto	400	Illimitato
valore massimo di un minuto	500	Illimitato
valore minimo di un minuto	400	Illimitato
valore host tcp max-incomplete	50	Illimitato

I router configurati per applicare Cisco IOS VRF-Aware Firewall mantengono un set di contatori per ciascun VRF.

Il contatore tra "ip inspect one-minute high" e "ip inspect one-minute low" mantiene la somma di tutti i tentativi di connessione TCP, UDP e Internet Control Message Protocol (ICMP) eseguiti nel minuto precedente al funzionamento del router, indipendentemente dal fatto che le connessioni siano state completate o meno. Un aumento della velocità di connessione può indicare un'infezione da worm su una rete privata o un tentativo di attacco DoS contro un server.

Sebbene non sia possibile "disattivare" la protezione DoS del firewall, è possibile regolare la protezione DoS in modo che non abbia effetto a meno che nella tabella delle sessioni del router firewall non sia presente un numero elevato di connessioni half-open.

Protezione firewall DoS

Attenersi alla procedura seguente per ottimizzare la protezione DoS del firewall all'attività della rete:

1. Accertarsi che la rete non sia infetta da virus o worm che potrebbero causare valori di connessione half-open o tentativi di connessione errati. Se la rete non è pulita, non è possibile regolare correttamente la protezione DoS del firewall. È necessario osservare l'attività della rete in un periodo di attività tipica. Se si sintonizzano le impostazioni di protezione DoS della rete in un periodo di attività di rete bassa o inattiva, i livelli di attività normali probabilmente superano le impostazioni di protezione DoS.
2. Impostare i valori massimi incompleti su valori molto alti:

   ```
   ip inspect max-incomplete high 20000000
   ip inspect one-minute high 100000000
   ip inspect tcp max-incomplete host 100000 block-time 0
   ```

   In questo modo il router non potrà fornire la protezione DoS mentre si osservano i modelli di connessione della rete. Se si desidera lasciare disabilitata la protezione DoS, interrompere subito la procedura.**Nota:** se il router esegue il software Cisco IOS versione 12.4(11)T o

successive o la versione 12.4(10) o successive, non è necessario aumentare i valori predefiniti di Protezione DoS; per impostazione predefinita sono già impostati sui limiti massimi.**Nota:** per abilitare la prevenzione della negazione del servizio più aggressiva specifica dell'host TCP, che include il blocco dell'avvio della connessione a un host, è necessario impostare il tempo di blocco specificato nel comando **ip inspect tcp max-complete host**

3. Cancellare le statistiche di Cisco IOS Firewall con questo comando:

```
show ip inspect statistics reset
```

4. Lasciare il router configurato in questo stato per un certo periodo di tempo, probabilmente da 24 a 48 ore, in modo da poter osservare il modello di rete in almeno un giorno intero del tipico ciclo di attività della rete.**Nota:** anche se i valori sono impostati su livelli molto elevati, la rete non beneficia della protezione Cisco IOS Firewall o IPS DoS.
5. Dopo il periodo di osservazione, controllare i contatori DoS con questo comando:

```
show ip inspect statistics
```

I parametri da osservare per ottimizzare la protezione DoS sono evidenziati in **grassetto**:

```
Packet inspection statistics
   [process switch:fast switch]
  tcp packets: [218314:7878692]
  udp packets: [501498:65322]
   packets: [376676:80455]
   packets: [5738:4042411]
  smtp packets: [11:11077]
  ftp packets: [2291:0]
Interfaces configured for inspection 2
Session creations since subsystem
   startup or last reset 688030
Current session counts
   (estab/half-open/terminating) [0:0:0]
Maxever session counts
   (estab/half-open/terminating) [207:56:35]
Last session created 00:00:05
Last statistic reset never
Last session creation rate 1
Maxever session creation rate 330
Last half-open session total 0
TCP reassembly statistics
  received 46591 packets out-of-order; dropped 16454
  peak memory usage 48 KB; current usage: 0 KB
  peak queue length 16
```

6. Configurare **ip inspect max-complete high** su un valore superiore del 25% al valore half-open del numero di sessioni maxever indicato sul router. Un moltiplicatore 1,25 offre un margine di crescita del 25% rispetto al comportamento osservato, ad esempio:

```
Maxever session counts
   (estab/half-open/terminating) [207:56:35]
56 * 1.25 = 70
```

Configurazione:

```
router(config)
   #ip inspect max-incomplete high 70
```

Nota: questo documento descrive l'uso di un moltiplicatore di 1,25 volte l'attività tipica della rete per impostare i limiti per attivare la protezione DoS. Se si osserva la rete entro i picchi

tipici delle attività di rete, lo spazio di manovra deve essere sufficiente per evitare l'attivazione della protezione DoS del router in tutte le circostanze tranne quelle atipiche. Se la rete rileva periodicamente picchi di attività legittime superiori a questo valore, il router attiva le funzionalità di protezione DoS, che possono avere un impatto negativo su parte del traffico di rete. È necessario monitorare i registri del router per rilevare eventuali attività DoS e modificare i limiti **massimo incompleti di ip inspect** e/o **ip inspect di un minuto** per evitare di attivare DoS, dopo aver determinato che i limiti sono stati rilevati come risultato di un'attività di rete legittima. È possibile riconoscere l'applicazione di protezione DoS dalla presenza di messaggi di registro come il seguente:

7. Configurare **ip inspect max-complete low** sul valore visualizzato dal router per il valore half-open del numero di sessioni maxever, ad esempio:
   ```
   Maxever session counts
      (estab/half-open/terminating) [207:56:35]
   ```
   Configurazione:
   ```
   router(config)
      #ip inspect max-incomplete low 56
   ```
8. Il contatore per **ip inspect da un minuto in più** e da **un minuto in meno** mantiene la somma di tutti i tentativi di connessione TCP, UDP e Internet Control Message Protocol (ICMP) eseguiti nel minuto precedente del funzionamento del router, anche se le connessioni sono state completate correttamente. Un aumento della velocità di connessione può indicare un'infezione da worm su una rete privata o un tentativo di attacco DoS contro un server. Un'ulteriore statistica di ispezione è stata aggiunta all'output delle **statistiche show ip inspect** in 12.4(11)T e 12.4(10) per rivelare il limite massimo per la velocità di creazione della sessione. Se si esegue un software Cisco IOS con versione precedente alla 12.4(11)T o alla 12.4(10), le statistiche relative al controllo non contengono la seguente riga:
   ```
   Maxever session creation rate [value]
   ```
   Nelle versioni software Cisco IOS precedenti alla 12.4(11)T e alla 12.4(10), non viene mantenuto un valore per l'ispezione della frequenza di connessione massima di un minuto; pertanto, è necessario calcolare il valore applicato in base ai valori osservati per il "conteggio massimo di sessioni". Le osservazioni di diverse reti che utilizzano l'ispezione stateful di Cisco IOS Firewall versione 12.4(11)T in produzione hanno mostrato che le velocità di creazione di sessioni Maxever tendono a superare la somma dei tre valori (stabilito, semi-aperto e terminante) nel "conteggio di sessioni maxever" di circa il 10%. Per calcolare il valore minimo di un minuto di ip inspect, moltiplicare il valore "stabilito" indicato per 1,1, ad esempio:
   ```
   Maxever session counts
      (estab/half-open/terminating) [207:56:35]
   (207 + 56 + 35) * 1.1 = 328
   ```

   Configurazione:
   ```
   ip inspect one-minute low 328
   ```
   Se il router esegue il software Cisco IOS versione 12.4(11)T o successive o la versione 12.4(10) o successive, è possibile applicare semplicemente il valore mostrato nella statistica di ispezione della "velocità di creazione di sessioni Maxever":
   ```
   Maxever session creation rate 330
   ```
   Configurazione:
   ```
   ip inspect one-minute low 330
   ```
9. Calcolare e configurare **ip inspect con un'altezza di un minuto**. Il valore massimo di un minuto per ip inspect deve essere maggiore del 25% del valore minimo calcolato di un minuto, ad esempio:
   ```
   ip inspect one-minute low (330) * 1.25 = 413
   ```

Configurazione:

```
ip inspect one-minute high 413
```

Nota: questo documento descrive l'uso di un moltiplicatore di 1,25 volte l'attività tipica della rete per impostare i limiti per attivare la protezione DoS. Se si osserva la rete entro i picchi tipici delle attività di rete, lo spazio di manovra deve essere sufficiente per evitare l'attivazione della protezione DoS del router in tutte le circostanze tranne quelle atipiche. Se la rete rileva periodicamente picchi di attività legittime superiori a questo valore, il router attiva le funzionalità di protezione DoS, che possono avere un impatto negativo su parte del traffico di rete. È necessario monitorare i registri del router per rilevare eventuali attività DoS e modificare i limiti **massimo incompleti di ip inspect** e/o **ip inspect di un minuto** per evitare di attivare DoS, dopo aver determinato che i limiti sono stati rilevati come risultato di un'attività di rete legittima. È possibile riconoscere l'applicazione di protezione DoS dalla presenza di messaggi di registro come il seguente:

10. Ènecessario definire un valore per **ip inspect tcp max-complete host** in base alla conoscenza delle funzionalità dei server. Questo documento non può fornire linee guida per la configurazione della protezione DoS per host in quanto questo valore varia ampiamente in base alle prestazioni hardware e software dell'host finale. In caso di dubbi sui limiti appropriati da configurare per la protezione DoS, sono disponibili due opzioni per definire i limiti DoS:L'opzione preferibile è configurare la protezione DoS basata su router per host su un valore elevato (inferiore o uguale al valore massimo di 4.294.967.295) e applicare la protezione specifica dell'host offerta dal sistema operativo di ciascun host o da un sistema di protezione dalle intrusioni basato su host esterno, ad esempio Cisco Security Agent (CSA).Esaminare i registri di attività e prestazioni sugli host di rete e determinare la velocità massima di connessione sostenibile. Poiché il firewall classico offre un solo contatore globale, è necessario applicare il valore massimo determinato dopo aver controllato la velocità massima di connessione di tutti gli host di rete. È comunque consigliabile utilizzare limiti di attività specifici del sistema operativo e un IPS basato su host come CSA.**Nota:** Cisco IOS Firewall offre una protezione limitata dagli attacchi diretti a vulnerabilità specifiche del sistema operativo e delle applicazioni. La protezione DoS di Cisco IOS Firewall non offre alcuna garanzia di protezione da compromessi sui servizi dell'host finale esposti ad ambienti potenzialmente ostili.
11. Monitorare l'attività di protezione DoS della rete. In teoria, è necessario utilizzare un server syslog o, preferibilmente, una stazione di monitoraggio e reporting (MARS) Cisco per registrare le occorrenze del rilevamento di attacchi DoS. Se il rilevamento avviene molto di frequente, è necessario monitorare e regolare i parametri di protezione DoS.Per ulteriori informazioni sugli attacchi DoS TCP SYN, vedere Definizione delle strategie di protezione dagli attacchi Denial of Service TCP SYN.

Verifica

Attualmente non è disponibile una procedura di verifica per questa configurazione.

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

Risoluzione dei problemi

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

Informazioni correlate

- Software Cisco PIX Firewall
- Riferimenti per i comandi di Cisco Secure PIX Firewall
- Avvisi sui prodotti per la sicurezza (inclusi PIX)
- RFC (Requests for Comments)
- Documentazione e supporto tecnico – Cisco Systems