Configurazione della prevenzione degli attacchi basata sulla velocità con filtro Snort 3 Rate su Secure FTD

Problema

L'attenzione è posta su come strutturare le regole per coprire più subnet, comprendere le best practice per l'implementazione e determinare i valori di soglia appropriati (conteggi al secondo) per la segnalazione o il blocco, in particolare nel contesto della prevenzione degli attacchi di tipo SYN.

Ambiente

- Cisco Secure Firewall Firepower con FTD 7.4.2.4
- Piattaforma hardware Firepower 2110
- Gestito da Firepower Management Center (FMC) 7.6.2.1
- Snort 3 Intrusion Prevention System con rate_filter Inspector abilitato
- Più subnet interne che richiedono protezione da allagamenti SYN
- Non sono presenti guasti attivi; guida alla configurazione per la difesa proattiva

Risoluzione

Questi passaggi descrivono in dettaglio come configurare e implementare la prevenzione degli attacchi basati sulla velocità utilizzando la funzione di ispezione Snort 3 rate_filter su Cisco Secure Firewall FTD, con una spiegazione della struttura delle regole per più subnet e suggerimenti sulle best-practice. Queste azioni sono progettate per aiutare a stabilire le linee di base per il traffico normale e per abilitare il rilevamento o il blocco efficace degli attacchi di tipo flood SYN.

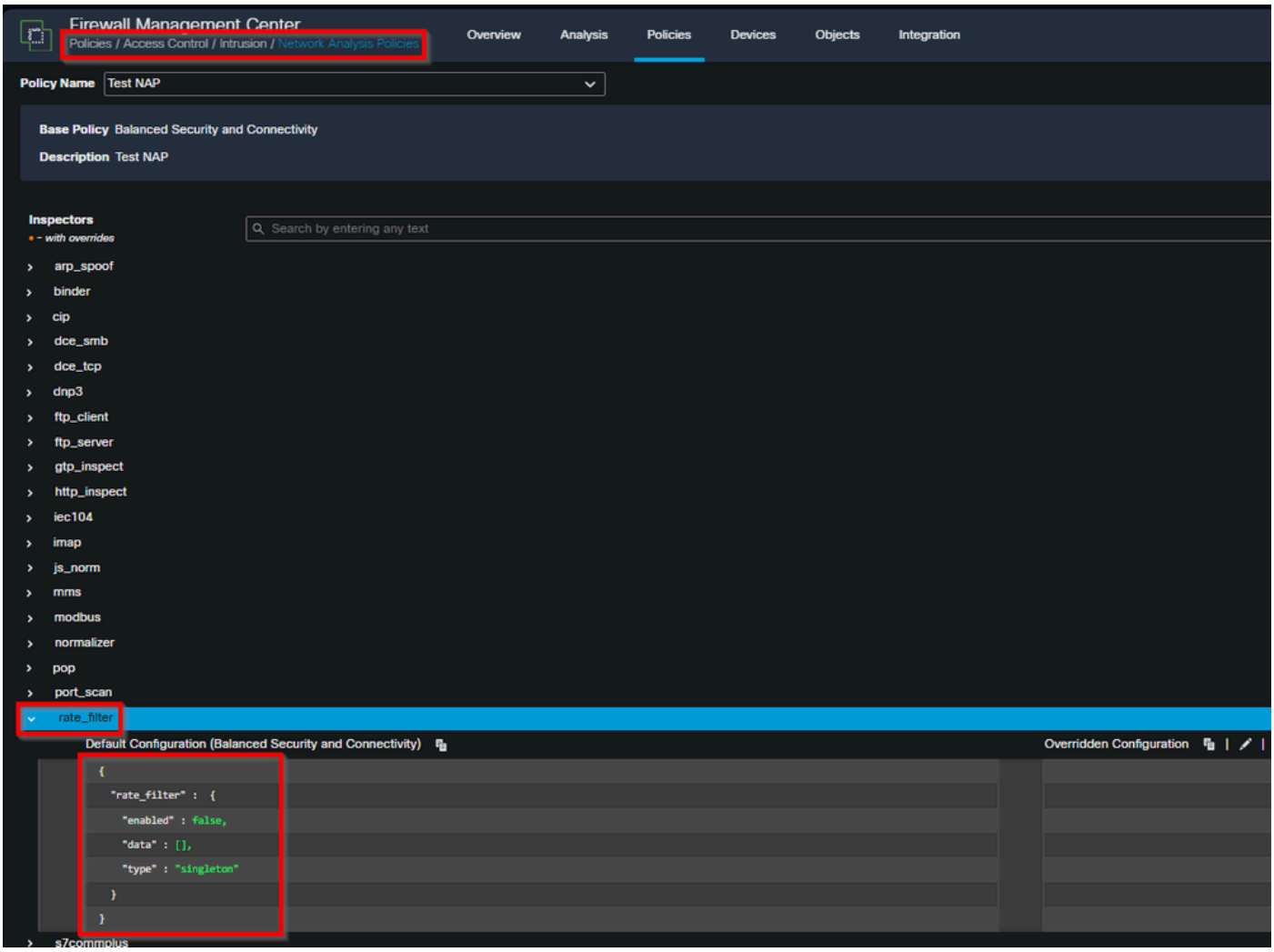
Nota: Non rientra nell'ambito di lavoro TAC suggerire o consigliare valori specifici per questi filtri delle regole. Ogni ambiente è diverso e richiede un'analisi approfondita dei

---

modelli di traffico e della progettazione della rete per determinare i valori migliori per questi filtri.

1: Passare al filtro rate_snort 3

Questi filtri sono configurati in Criteri > Controllo di accesso: Intrusione > Criteri di analisi di rete facendo clic su Snort 3 Version per il criterio Protezione accesso alla rete e quindi facendo clic sull'elenco a discesa rate_filter nel pannello a sinistra.



inline_image_0.png

2: Informazioni sulla struttura della regola di filtro Snort 3 Rate

La finestra di ispezione rate_filter nello Strumento 3 consente di definire le regole che controllano tipi specifici di traffico (ad esempio i pacchetti SYN) e di eseguire azioni (alert o drop) quando viene superata una determinata soglia. Queste regole possono essere applicate a più subnet.

Esempio di configurazione rate_filter per più subnet:

```
{
  "rate_filter": {
    "data": [
      {
        "apply_to": ["10.1.2.0/24", "10.1.3.0/24"],
        "count": 5,
        "gid": 135,
        "sid": 1,
        "new_action": "alert",
        "seconds": 10,
        "timeout": 15,
        "track": "by_src"
      }
    ],
    "enabled": true,
    "type": "singleton"
  }
}
```

Spiegazione dei parametri:

- apply_to: Elenco di indirizzi IP o di subnet a cui si applica il filtro (supporta più subnet).
- count + seconds: soglia per l'evento, ad esempio 5 pacchetti SYN entro 10 secondi.
- gid / sid: identifica l'evento Snort (ad esempio GID 135, SID 1 per il rilevamento di flood SYN).
- new_action: azione da eseguire quando viene superata la soglia, ad esempio alert, drop.
- timeout: durata precedente all'attivazione di un nuovo avviso/azione per la stessa condizione.
- track: modalità di rilevamento (ad esempio, by_src per IP di origine, by_dst per IP di destinazione).

3: Best practice per l'ottimizzazione delle soglie e l'implementazione delle policy

- Inizia in modalità di avviso: impostare new_action su alert e utilizzare soglie conservative (ad esempio, conteggio più elevato e secondi) per evitare falsi positivi.
- Traffico di rete di base: monitorare gli eventi generati per comprendere l'aspetto delle normali frequenze SYN per l'ambiente e le subnet.
- Sintonizzazione iterativa dei parametri: regolazione del conteggio, dei secondi e del timeout in base ai modelli di traffico osservati e alle esigenze operative.

- Passare al blocco: una volta accertato che le soglie riflettono accuratamente un comportamento anomalo, modificare new_action da alert a drop o equivalente a bloccare attivamente gli attacchi.
- Filtri separati in base alle esigenze: considerare limiti di velocità diversi per segmenti o ruoli diversi (ad esempio, server e subnet utente) se i modelli di traffico variano.
- Monitoraggio continuo: gestione di avvisi e monitoraggio sugli eventi rate_filter per identificare rapidamente i problemi di tuning o le minacce attive.

Causa

Nessuna. La configurazione è stata richiesta per motivi di sicurezza proattiva e come guida a causa di un precedente evento flood SYN.

Contenuto correlato

- Riferimento ispettore Snort 3: Filtro tasso
- Guida alla configurazione dei dispositivi di Cisco Secure Firewall Management Center, 7.4: Prevenzione degli attacchi basati sulla velocità
- Supporto tecnico Cisco e download

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).