Verifica della configurazione e della funzionalità di rilevamento delle minacce ASA

Sommario

Introduzione

Questo documento descrive i tre componenti principali della funzionalità e della configurazione per il rilevamento delle minacce.

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.

Premesse

In questo documento viene descritta la funzionalità e la configurazione di base della funzione di rilevamento delle minacce di Cisco Adaptive Security Appliance (ASA). Threat Detection fornisce agli amministratori del firewall gli strumenti necessari per identificare, comprendere e arrestare gli attacchi prima che raggiungano l'infrastruttura di rete interna. A tal fine, la funzione si basa su una serie di trigger e statistiche differenti, che sono descritti in dettaglio in queste sezioni.

Threat Detection può essere usato su qualsiasi firewall ASA con software versione 8.0(2) o successive. Anche se il rilevamento delle minacce non può sostituire una soluzione IDS/IPS dedicata, può essere utilizzato in ambienti in cui non è disponibile un IPS per fornire un ulteriore livello di protezione alle funzionalità principali dell'appliance ASA.

Funzionalità di rilevamento minacce

La funzione di rilevamento delle minacce è composta da tre componenti principali:

1. Rilevamento di base delle minacce
2. Rilevamento avanzato delle minacce
3. Rilevamento delle minacce durante la scansione

Ognuno di questi componenti è descritto in dettaglio in queste sezioni.

Rilevamento di base delle minacce (velocità a livello di sistema)

Il rilevamento delle minacce di base è abilitato per impostazione predefinita su tutte le appliance ASA con 8.0(2) e versioni successive.

Il rilevamento base delle minacce monitora la frequenza con cui i pacchetti vengono scartati dall'appliance ASA nel suo insieme per vari motivi. Ciò significa che le statistiche generate dal rilevamento di base delle minacce si applicano solo all'intero accessorio e non sono generalmente abbastanza granulari da fornire informazioni sulla fonte o sulla natura specifica della minaccia. Al contrario, l'ASA monitora i pacchetti ignorati per questi eventi:

- Drop ACL (acl-drop) - I pacchetti vengono negati dagli elenchi degli accessi.
- Pacchetti errati (bad-packet-drop) - Formati di pacchetto non validi, che includono le intestazioni L3 e L4 non conformi agli standard RFC.
- Conn Limit (conn-limit-drop) - Pacchetti che superano un limite di connessione configurato o globale.
- Attacco DoS (dos-drop) - Attacchi DoS (Denial of Service).
- Firewall (fw-drop) - Controlli di sicurezza firewall di base.
- Attacco ICMP (icmp-drop) - Pacchetti ICMP sospetti.
- Inspect (inspect-drop) - Rifiuto mediante ispezione dell'applicazione.
- Interface (interface-drop) - Pacchetti scartati dai controlli dell'interfaccia.
- Scanning (scanning-threat) - Attacchi di scansione di rete/host.
- Attacco SYN (attacco SYN) - Attacchi di sessione incompleti, che includono attacchi SYN TCP e sessioni UDP unidirezionali senza dati di ritorno.

Ognuno di questi eventi ha una serie specifica di trigger che vengono utilizzati per identificare la minaccia. La maggior parte dei trigger è legata a specifici motivi di perdita ASP, sebbene vengano presi in considerazione anche alcuni syslog e azioni di ispezione. Alcuni trigger sono monitorati da più categorie di minacce. In questa tabella vengono descritti alcuni dei trigger più comuni, anche se non si tratta di un elenco

esaustivo:

Minaccia di base	Trigger/i / Motivo/i rilascio ASP
acl-drop	acl-drop
bad-packet-drop	invalid-tcp-hdr-length invalid-ip-header inspect-dns-pak-troppo lungo inspect-dns-id-not-matched
conn-limit-drop	conn-limit
dos-drop	sp-security-failed
fw-drop	inspect-icmp-seq-num-not-matched inspect-dns-pak-troppo lungo inspect-dns-id-not-matched sp-security-failed acl-drop
icmp-drop	inspect-icmp-seq-num-not-matched
inspect-drop	Cadute di fotogrammi attivate da un motore di ispezione
interface-drop	sp-security-failed nessun percorso
minaccia di scansione	tcp-3whs-failed tcp-not-syn sp-security-failed acl-drop inspect-icmp-seq-num-not-matched inspect-dns-pak-troppo lungo inspect-dns-id-not-matched
syn-attack	%ASA-6-302014 syslog con motivo di disinstallazione di "SYN Timeout"

Per ogni evento, il rilevamento di base delle minacce misura la frequenza con cui queste cadute si verificano in un periodo di tempo configurato. Questo periodo di tempo viene definito intervallo ARI (Average Rate Interval) e può variare da 600 secondi a 30 giorni. Se il numero di eventi che si verificano nell'ARI supera le soglie configurate per la velocità, l'ASA considera questi eventi una minaccia.

Il rilevamento di base delle minacce ha due soglie configurabili per quando considera gli eventi una minaccia: il tasso medio e il tasso burst. La velocità media è semplicemente il numero medio di cadute al secondo nel periodo di tempo dell'ARI configurato. Ad esempio, se la soglia della velocità media per le perdite degli ACL è configurata per 400 con un'ARI di 600 secondi, l'ASA calcola il numero medio di pacchetti ignorati dagli ACL negli ultimi 600 secondi. Se il numero è superiore a 400 al secondo, l'ASA registra una minaccia.

Analogamente, la velocità di burst è molto simile, ma considera periodi più piccoli di dati snapshot, denominati BRI (burst rate interval). L'BRI è sempre più piccolo dell'ARI. Ad esempio, basandosi sull'esempio precedente, l'ARI per le perdite ACL è ancora 600 secondi e ora ha una velocità di burst di 800. Con questi valori, l'ASA calcola il numero medio di pacchetti scartati dagli ACL in 20 secondi, dove 20 secondi è l'BRI. Se il valore calcolato supera le 800 cadute al secondo, viene registrata una minaccia. Per determinare l'uso della funzione BRI, l'ASA calcola il valore di 1/30 dell'ARI. Pertanto, nell'esempio utilizzato in precedenza, 1/30 di 600 secondi è 20 secondi. Tuttavia, il rilevamento delle minacce ha un BRI minimo di 10 secondi, quindi se 1/30 dell'ARI è inferiore a 10, l'ASA usa ancora 10 secondi come BRI. Inoltre, è importante notare che questo comportamento era diverso nelle versioni precedenti all'8.2(1), che utilizzavano un valore di 1/60 dell'ARI, invece di 1/30 dell'ARI. Il valore BRI minimo di 10 secondi è lo stesso per tutte le versioni del software.

Quando viene rilevata una minaccia di base, l'ASA genera semplicemente il syslog %ASA-4-733100 per avvisare l'amministratore che è stata identificata una minaccia potenziale. Il numero medio, corrente e totale di eventi per ciascuna categoria di minaccia può essere visualizzato con il comando **show threat-detection rate**. Il numero totale di eventi cumulativi è la somma del numero di eventi visualizzati negli ultimi 30 esempi BRI.

La velocità di burst in syslog viene calcolata in base al numero di pacchetti scartati finora nell'attuale BRI. Il calcolo viene eseguito periodicamente in un BRI. Quando si verifica una violazione, viene generato un syslog. È limitato il fatto che in un BRI venga generato un solo syslog. La velocità di burst in "show threat-detection rate" viene calcolata in base al numero di pacchetti scartati nell'ultimo BRI. La differenza sta nel fatto che syslog è sensibile al fattore tempo, quindi se si verifica una violazione nell'attuale BRI, potrebbe essere acquisita. "show threat-detection rate" è meno sensibile al tempo, quindi viene utilizzato il numero dell'ultimo BRI.

Il rilevamento di base delle minacce non intraprende alcuna azione per arrestare il traffico deviato o prevenire futuri attacchi. In questo senso, il rilevamento delle minacce di base è puramente informativo e può essere utilizzato come meccanismo di monitoraggio o di segnalazione.

Rilevamento avanzato delle minacce (statistiche a livello di oggetto e primi N)

A differenza del rilevamento delle minacce di base, il rilevamento avanzato delle minacce può essere utilizzato per tenere traccia delle statistiche relative a oggetti più granulari. L'ASA supporta il rilevamento delle statistiche per IP, porte, protocolli, ACL e server host protetti da TCP intercept. Il rilevamento avanzato delle minacce è abilitato solo per impostazione predefinita per le statistiche ACL.

Per gli oggetti host, porte e protocolli, il rilevamento delle minacce tiene traccia del numero di pacchetti, byte e perdite inviati e ricevuti dall'oggetto entro un periodo di tempo specifico. Per gli ACL, il processo di rilevamento delle minacce tiene traccia delle 10 ACE (autorizzazioni e rifiuti) più colpite in un determinato periodo di tempo.

I periodi di tempo rilevati in tutti questi casi sono 20 minuti, 1 ora, 8 ore e 24 ore. Anche se i periodi di tempo non sono configurabili, il numero di periodi tracciati per oggetto può essere regolato con la parola chiave 'number-of-rate'. Per ulteriori informazioni, vedere la sezione Configurazione. Ad esempio, se 'number-of-rate' è impostato su 2, verranno visualizzate tutte le statistiche relative a 20 minuti, 1 ora e 8 ore. Se 'number-of-rate' è impostato su 1, verranno visualizzate tutte le statistiche relative a 20 minuti, 1 ora. Indipendentemente da ciò, viene sempre visualizzata la frequenza di 20 minuti.

Quando TCP intercept è abilitato, Threat Detection è in grado di tenere traccia dei primi 10 server considerati sotto attacco e protetti da TCP intercept. Le statistiche per l'intercettazione TCP sono simili a quelle per il rilevamento delle minacce di base, nel senso che l'utente può configurare l'intervallo di velocità misurato insieme alle velocità medie (ARI) e burst (BRI) specifiche. Le statistiche di rilevamento avanzato delle minacce per l'intercettazione TCP sono disponibili solo in ASA 8.0(4) e versioni successive.

Le statistiche Advanced Threat Detection vengono visualizzate tramite il comando **show threat-detection statistics** e **show threat-detection statistics**. Questa è anche la funzione responsabile della compilazione dei grafici "in alto" sul dashboard del firewall di ASDM. Gli unici syslog generati dal rilevamento avanzato delle minacce sono %ASA-4-733104 e %ASA-4-733105, che vengono attivati quando le velocità media e burst (rispettivamente) vengono superate per le statistiche dell'intercettazione TCP.

Analogamente al rilevamento delle minacce di base, il rilevamento avanzato delle minacce è puramente informativo. Non viene intrapresa alcuna azione per bloccare il traffico in base alle statistiche di Rilevamento avanzato minacce.

Rilevamento delle minacce durante la scansione

La scansione del rilevamento delle minacce viene utilizzata per tenere traccia dei possibili attacchi che creano connessioni a troppi host in una subnet o a molte porte in un host o in una subnet. L'analisi del rilevamento delle minacce è disattivata per impostazione predefinita.

La funzionalità di rilevamento delle minacce di scansione si basa sul concetto di rilevamento delle minacce di base, che definisce già una categoria di minaccia per un attacco di scansione. Pertanto, le impostazioni dell'intervallo di velocità, della velocità media (ARI) e della velocità di burst (BRI) sono condivise tra Basic e Scanning Threat Detection. La differenza tra le due funzionalità consiste nel fatto che, mentre il rilevamento delle minacce di base indica esclusivamente il superamento delle soglie della velocità media o burst, il rilevamento delle minacce di scansione mantiene un database di indirizzi IP di utenti non autorizzati e di destinazione che può contribuire a fornire più contesto intorno agli host coinvolti nell'analisi. Inoltre, solo il traffico effettivamente ricevuto dall'host o dalla subnet di destinazione viene preso in considerazione dalla funzione di rilevamento delle minacce. La funzione Basic Threat Detection può ancora attivare una minaccia di scansione anche se il traffico viene scartato da un ACL.

La scansione di Threat Detection può opzionalmente reagire a un attacco evitando l'IP dell'utente malintenzionato. In questo modo, la funzione di rilevamento delle minacce è l'unico sottoinsieme della funzione di rilevamento delle minacce in grado di influenzare attivamente le connessioni tramite l'appliance ASA.

Quando il rilevamento delle minacce rileva un attacco, viene registrato %ASA-4-733101 per l'autore dell'attacco e/o gli IP di destinazione. Se la funzionalità è configurata per evitare l'autore dell'attacco, %ASA-4-733102 viene registrato quando l'analisi del rilevamento delle minacce genera un'esclusione. %ASA-4-733103 viene registrato quando si rimuove lo shun. è possibile usare il comando **show threat-detection scanning-threat** per visualizzare l'intero database delle minacce da scansione.

Limitazioni

- il rilevamento delle minacce è disponibile solo in ASA versione 8.0(2) e successive. Non è supportato

sulla piattaforma ASA 1000V.
- Il rilevamento delle minacce è supportato solo in modalità contesto singolo.
- Vengono rilevate solo le minacce "through-the-box". Il traffico inviato all'appliance ASA non viene preso in considerazione dal rilevamento delle minacce.
- I tentativi di connessione TCP reimpostati dal server di destinazione non vengono conteggiati come attacco SYN o minaccia di scansione.

Configurazione

Rilevamento di base delle minacce

Il rilevamento di base delle minacce è abilitato con il comando **threat-detection basic-threat**.

<#root>

```
ciscoasa(config)#
```

```
threat-detection basic-threat
```

Le velocità predefinite possono essere visualizzate con il comando **show run all threat-detection**.

<#root>

```
ciscoasa(config)#
```

```
show run all threat-detection
```

```
threat-detection rate dos-drop rate-interval 600 average-rate 100 burst-rate 400
threat-detection rate dos-drop rate-interval 3600 average-rate 80 burst-rate 320
threat-detection rate bad-packet-drop rate-interval 600 average-rate 100 burst-rate 400
threat-detection rate bad-packet-drop rate-interval 3600 average-rate 80 burst-rate 320
threat-detection rate acl-drop rate-interval 600 average-rate 400 burst-rate 800
threat-detection rate acl-drop rate-interval 3600 average-rate 320 burst-rate 640
threat-detection rate conn-limit-drop rate-interval 600 average-rate 100 burst-rate 400
threat-detection rate conn-limit-drop rate-interval 3600 average-rate 80 burst-rate 320
threat-detection rate icmp-drop rate-interval 600 average-rate 100 burst-rate 400
threat-detection rate icmp-drop rate-interval 3600 average-rate 80 burst-rate 320
threat-detection rate scanning-threat rate-interval 600 average-rate 5 burst-rate 10
threat-detection rate scanning-threat rate-interval 3600 average-rate 4 burst-rate 8
threat-detection rate syn-attack rate-interval 600 average-rate 100 burst-rate 200
threat-detection rate syn-attack rate-interval 3600 average-rate 80 burst-rate 160
threat-detection rate fw-drop rate-interval 600 average-rate 400 burst-rate 1600
threat-detection rate fw-drop rate-interval 3600 average-rate 320 burst-rate 1280
threat-detection rate inspect-drop rate-interval 600 average-rate 400 burst-rate 1600
threat-detection rate inspect-drop rate-interval 3600 average-rate 320 burst-rate 1280
threat-detection rate interface-drop rate-interval 600 average-rate 2000 burst-rate 8000
threat-detection rate interface-drop rate-interval 3600 average-rate 1600 burst-rate 6400
```

Per regolare queste velocità con valori personalizzati, è sufficiente riconfigurare il comando **threat-detection rate** per la categoria di minacce appropriata.

<#root>

```
ciscoasa(config)#
```

```
threat-detection rate acl-drop rate-interval 1200 average-rate 250 burst-rate 550
```

Per ogni categoria di minaccia è possibile definire un massimo di 3 velocità diverse (con ID di velocità 1, 2 e 3). Nel syslog %ASA-4-733100 viene fatto riferimento all'ID tariffa specificato superato.

Nell'esempio precedente, il rilevamento di minacce crea syslog 73100 solo quando il numero di cadute ACL supera 250 cadute/secondo in 1200 secondi o 550 cadute/secondo in 40 secondi.

Rilevamento avanzato delle minacce

Usare il comando **threat-detection statistics** per abilitare Advanced Threat Detection. Se non viene specificata alcuna parola chiave specifica, il comando attiva il rilevamento per tutte le statistiche.

<#root>

```
ciscoasa(config)#
```

```
threat-detection statistics ?
```

```
configure mode commands/options:
 access-list      Keyword to specify access-list statistics
 host            Keyword to specify IP statistics
 port            Keyword to specify port statistics
 protocol       Keyword to specify protocol statistics
 tcp-intercept   Trace tcp intercept statistics
 <cr>
```

Per configurare il numero di intervalli di velocità rilevati per le statistiche di host, porte, protocolli o ACL, usare la parola chiave **number-of-rate**.

<#root>

```
ciscoasa(config)#
```

```
threat-detection statistics host number-of-rate 2
```

La parola chiave number-of-rate configura il rilevamento delle minacce in modo da tenere traccia solo del numero *n* di intervalli più breve.

Per abilitare le statistiche di intercettazione TCP, usare il comando **threat-detection statistics tcp-intercept**.

<#root>

```
ciscoasa(config)#
```

```
threat-detection statistics tcp-intercept
```

Per configurare velocità personalizzate per le statistiche dell'intercettazione TCP, usare le parole chiave **rate-interval**, **average-rate** e **burst-rate**.

```
<#root>

ciscoasa(config)#

threat-detection statistics tcp-intercept rate-interval 45 burst-rate 400 average-rate 100
```

Rilevamento delle minacce durante la scansione

Per abilitare il rilevamento delle minacce mediante scansione, usare il comando **threat-detection scanning-threat**.

```
<#root>

ciscoasa(config)#

threat-detection scanning-threat
```

Per regolare le velocità di una minaccia di scansione, usare lo stesso comando **threat-detection rate** usato dal Basic Threat Detection.

```
<#root>

ciscoasa(config)#

threat-detection rate scanning-threat rate-interval 1200 average-rate 250 burst-rate 550
```

Per consentire all'ASA di eliminare un indirizzo IP di un utente malintenzionato a livello di scansione, aggiungere la parola chiave **shun** al comando **threat-detection scanning-threat**.

```
<#root>

ciscoasa(config)#

threat-detection scanning-threat shun
```

In questo modo, la funzionalità Rilevamento minacce di digitalizzazione consente all'utente malintenzionato di risparmiare un'ora. Per regolare la durata dello shun, usare il comando **threat-detection scanning-threat shun duration**.

```
<#root>

ciscoasa(config)#

threat-detection scanning-threat shun duration 1000
```

In alcuni casi, è possibile evitare che l'appliance ASA ignori determinati IP. A tale scopo, creare un'eccezione con il comando **threat-detection scanning-threat shun except**.

<#root>

```
ciscoasa(config)#
```

```
threat-detection scanning-threat shun except ip-address 10.1.1.1 255.255.255.255
```

```
ciscoasa(config)#
```

```
threat-detection scanning-threat shun except object-group no-shun
```

Prestazioni

Il rilevamento delle minacce di base ha un impatto molto limitato sulle prestazioni dell'appliance ASA. Le funzioni di rilevamento avanzato e di scansione delle minacce richiedono molte più risorse in quanto devono tenere traccia di varie statistiche in memoria. Solo la funzionalità di rilevamento delle minacce attivata con la funzione shun può avere un impatto attivo sul traffico che altrimenti sarebbe stato autorizzato.

Con l'avanzare delle versioni del software ASA, l'utilizzo della memoria per il rilevamento delle minacce è stato notevolmente ottimizzato. Tuttavia, è necessario monitorare l'utilizzo della memoria da parte dell'ASA prima e dopo l'abilitazione del rilevamento delle minacce. In alcuni casi, è preferibile attivare solo temporaneamente alcune statistiche (ad esempio, le statistiche host) durante la risoluzione attiva di un problema specifico.

Per una visualizzazione più dettagliata dell'utilizzo della memoria per il rilevamento delle minacce, eseguire il comando **show memory app-cache threat-detection [detail]**.

Azioni consigliate

Nelle sezioni seguenti vengono forniti alcuni consigli generali sulle azioni da eseguire quando si verificano vari eventi correlati al rilevamento delle minacce.

Quando viene superata una frequenza di rilascio di base e viene generato %ASA-4-733100

Determinare la categoria di minaccia specifica menzionata nel syslog %ASA-4-733100 e correlarla all'output di show threat-detection rate . Con queste informazioni, controllare l'output di show asp drop per stabilire i motivi della riduzione del traffico.

Per una visualizzazione più dettagliata del traffico che viene scartato per un motivo specifico, utilizzare un'acquisizione drop ASP con il motivo in questione per visualizzare tutti i pacchetti scartati. Ad esempio, se vengono registrate minacce di eliminazione ACL, acquisire il motivo di eliminazione ASP di acl-drop :

<#root>

```
ciscoasa#
```

```
capture drop type asp-drop acl-drop
```

```
ciscoasa#
```

show capture drop

```
1 packet captured

   1: 18:03:00.205189 10.10.10.10.60670 > 192.168.1.100.53:  udp 34 Drop-reason:
 (acl-drop) Flow is denied by configured rule
```

L'acquisizione mostra che il pacchetto scartato è un pacchetto UDP/53 compreso tra 10.10.10.10 e 192.168.1.100.

Se %ASA-4-73100 segnala una minaccia di analisi, può essere utile abilitare temporaneamente il rilevamento delle minacce di analisi. Questo consente all'ASA di tenere traccia degli IP di origine e di destinazione coinvolti nell'attacco.

Poiché la funzionalità Basic Threat Detection monitora principalmente il traffico che è già stato interrotto dall'ASP, non è necessaria alcuna azione diretta per interrompere una minaccia potenziale. Fanno eccezione gli attacchi SYN e le minacce di scansione, che riguardano il traffico che attraversa l'appliance ASA.

Se le cadute rilevate nell'acquisizione delle cadute ASP sono legittime e/o previste per l'ambiente di rete, regolare gli intervalli di frequenza di base su un valore più appropriato.

Se le cadute mostrano traffico non legittimo, è necessario agire per bloccare o limitare il traffico prima che raggiunga l'appliance ASA. tra cui ACL e QoS sui dispositivi upstream.

Per gli attacchi SYN, il traffico può essere bloccato in un ACL sull'appliance ASA. L'intercettazione TCP potrebbe essere configurata anche per proteggere i server di destinazione, ma potrebbe semplicemente causare una minaccia Conn Limit registrata.

Per analizzare le minacce, il traffico può essere bloccato in un ACL sull'appliance ASA. Scansione del rilevamento delle minacce con shunQuesta opzione può essere abilitata per consentire all'ASA di bloccare proattivamente tutti i pacchetti provenienti dall'autore dell'attacco per un periodo di tempo definito.

Quando viene rilevata una minaccia di scansione e %ASA-4-733101 è registrato

%ASA-4-73101 deve elencare l'host/subnet di destinazione o l'indirizzo IP dell'autore dell'attacco. Per l'elenco completo di bersagli e aggressori, controllare l'output di show threat-detection scanning-threat.

Anche le acquisizioni dei pacchetti sulle interfacce ASA che devono affrontare l'attacco e/o le destinazioni possono aiutare a chiarire la natura dell'attacco.

Se l'analisi rilevata non è prevista, è necessario agire per bloccare o limitare la velocità del traffico prima che raggiunga l'appliance ASA. tra cui ACL e QoS sui dispositivi upstream. Quando il shunQuesta opzione viene aggiunta alla configurazione di Rilevamento minacce di scansione e può permettere all'ASA di eliminare proattivamente tutti i pacchetti dall'IP dell'utente malintenzionato per un periodo di tempo definito. Come ultima risorsa, il traffico può essere bloccato manualmente sull'appliance ASA tramite un criterio di intercettazione ACL o TCP.

Se l'analisi rilevata è un falso positivo, regolare gli intervalli di velocità delle minacce di scansione su un valore più appropriato per l'ambiente di rete.

Quando un utente malintenzionato viene escluso e %ASA-4-733102 registrato

%ASA-4-73102 elenca l'indirizzo IP dell'utente non autorizzato. Utilizzare il show threat-detection shun per visualizzare un elenco completo degli aggressori esclusi in modo specifico dal Threat Detection. Utilizzare il show shun per visualizzare l'elenco completo di tutti gli IP esclusi dall'appliance ASA (compresi quelli provenienti da fonti diverse dal rilevamento delle minacce).

Se lo shun fa parte di un attacco legittimo, non è necessaria alcuna ulteriore azione. Tuttavia, sarebbe utile bloccare manualmente il traffico dell'aggressore il più a monte possibile verso la sorgente. Questa operazione può essere eseguita tramite ACL e QoS. Ciò garantisce che i dispositivi intermedi non debbano sprecare risorse in caso di traffico illecito.

Se la minaccia di scansione che ha attivato lo shun è un falso positivo, rimuovere manualmente lo shun con lo clear threat-detection shun [IP_address]

Quando %ASA-4-73104 e/o %ASA-4-733105 è registrato

%ASA-4-733104 e %ASA-4-733105 elencano l'host interessato dall'attacco attualmente protetto da TCP intercept. Per ulteriori dettagli sulle percentuali di attacco e sui server protetti, vedere l'output di show threat-detection statistics top tcp-intercept .

<#root>

```
ciscoasa#
```

```
show threat-detection statistics top tcp-intercept
```

```
Top 10 protected servers under attack (sorted by average rate)
Monitoring window size: 30 mins    Sampling interval: 30 secs
------------------------------------------------------------------------------
1    192.168.1.2:5000 inside 1249 9503 2249245  Last: 10.0.0.3 (0 secs ago)
2    192.168.1.3:5000 inside 10 10 6080 10.0.0.200 (0 secs ago)
3    192.168.1.4:5000 inside 2 6 560 10.0.0.200 (59 secs ago)
4    192.168.1.5:5000 inside 1 5 560 10.0.0.200 (59 secs ago)
5    192.168.1.6:5000 inside 1 4 560 10.0.0.200 (59 secs ago)
6    192.168.1.7:5000 inside 0 3 560 10.0.0.200 (59 secs ago)
7    192.168.1.8:5000 inside 0 2 560 10.0.0.200 (59 secs ago)
8    192.168.1.9:5000 inside 0 1 560 10.0.0.200 (59 secs ago)
9    192.168.1.10:5000 inside 0 0 550 10.0.0.200 (2 mins ago)
10   192.168.1.11:5000 inside 0 0 550 10.0.0.200 (5 mins ago)
```

Quando Advanced Threat Detection rileva un attacco di questo tipo, l'ASA protegge già il server interessato tramite TCP intercept. Verificare i limiti di connessione configurati per assicurarsi che forniscano una protezione adeguata per la natura e la velocità dell'attacco. Inoltre, sarebbe utile bloccare manualmente il traffico dell'aggressore il più possibile a monte verso la sorgente. Questa operazione può essere eseguita tramite ACL e QoS. Ciò garantisce che i dispositivi intermedi non debbano sprecare risorse in caso di traffico illecito.

Se l'attacco rilevato è un falso positivo, regolare le velocità per un attacco di intercettazione TCP su un valore più appropriato con threat-detection statistics tcp-intercept

Come attivare manualmente una minaccia

Per eseguire il test e la risoluzione dei problemi, può essere utile attivare manualmente varie minacce. In questa sezione vengono forniti suggerimenti per l'attivazione di alcuni tipi di minacce comuni.

Minaccia di base - Rilascio di ACL, firewall e scansione

Per attivare una particolare minaccia di base, fare riferimento alla tabella riportata nella sezione precedente Funzionalità. Scegliere un motivo di rilascio ASP specifico e inviare il traffico attraverso l'appliance ASA che verrebbe scartato in base al motivo di rilascio ASP appropriato.

Ad esempio, le minacce ACL Drop, Firewall e Scanning prendono in considerazione tutte la frequenza dei pacchetti scartati da acl-drop. Completare questa procedura per attivare simultaneamente le seguenti minacce:

1. Creare un ACL sull'interfaccia esterna dell'ASA che scarti esplicitamente tutti i pacchetti TCP inviati a un server di destinazione all'interno dell'ASA (10.11.11.11):

```
access-list outside_in extended line 1 deny tcp any host 10.11.11.11
access-list outside_in extended permit ip any any
access-group outside_in in interface outside
```

2. Da un utente malintenzionato all'esterno dell'appliance ASA (10.10.10.10), usare nmap per eseguire una scansione SYN di TCP su tutte le porte del server di destinazione:

```
nmap -sS -T5 -p1-65535 -Pn 10.11.11.11
```

> **Nota**: T5 configura nmap per eseguire l'analisi il più rapidamente possibile. In base alle risorse del PC autore dell'attacco, questa operazione non è ancora abbastanza veloce da attivare alcune delle tariffe predefinite. In questo caso, è sufficiente ridurre le velocità configurate per la minaccia che si desidera visualizzare. Quando si imposta ARI e BRI su 0, il rilevamento delle minacce di base attiva sempre la minaccia indipendentemente dalla frequenza.

---

3. Si noti che vengono rilevate minacce di base per le minacce ACL Drop, Firewall e Scansione:

```
%ASA-1-733100: [ Scanning] drop rate-1 exceeded. Current burst rate is 19 per second,
 max configured rate is 10; Current average rate is 9 per second,
 max configured rate is 5; Cumulative total count is 5538
%ASA-1-733100: [ ACL drop] drop rate-1 exceeded. Current burst rate is 19 per second,
 max configured rate is 0; Current average rate is 2 per second,
 max configured rate is 0; Cumulative total count is 1472
%ASA-1-733100: [ Firewall] drop rate-1 exceeded. Current burst rate is 18 per second,
 max configured rate is 0; Current average rate is 2 per second,
 max configured rate is 0; Cumulative total count is 1483
```

> **Nota**: nell'esempio, l'ARI e l'BRI del firewall che vengono scartati dall'ACL sono stati impostati su 0, in modo che attivino sempre una minaccia. Per questo motivo le velocità configurate massime sono elencate come 0.

Advanced Threat - TCP Intercept

1. Creare un ACL sull'interfaccia esterna che autorizzi tutti i pacchetti TCP inviati a un server di destinazione all'interno dell'ASA (10.11.11.11):

```
access-list outside_in extended line 1 permit tcp any host 10.11.11.11
access-group outside_in in interface outside
```

2. Se il server di destinazione non esiste effettivamente o se ripristina i tentativi di connessione dell'utente malintenzionato, configurare una voce ARP falsa sull'appliance ASA in modo da bloccare il traffico di attacco verso l'interfaccia interna:

```
arp inside 10.11.11.11 dead.dead.dead
```

3. Creare un criterio TCP intercept semplice sull'appliance ASA:

```
access-list tcp extended permit tcp any any
class-map tcp
  match access-list tcp
policy-map global_policy
  class tcp
    set connection conn-max 2
service-policy global_policy global
```

Da un utente malintenzionato all'esterno dell'appliance ASA (10.10.10.10), usare nmap per eseguire una scansione SYN di TCP su tutte le porte del server di destinazione:

```
nmap -sS -T5 -p1-65535 -Pn 10.11.11.11
```

Notare che Threat Detection tiene traccia del server protetto:

<#root>

```
ciscoasa(config)#
```

show threat-detection statistics top tcp-intercept

```
Top 10 protected servers under attack (sorted by average rate)
Monitoring window size: 30 mins    Sampling interval: 30 secs

------------------------------------------------------------------------------
1    10.11.11.11:18589 outside 0 0 1 10.10.10.10 (36 secs ago)
2    10.11.11.11:47724 outside 0 0 1 10.10.10.10 (36 secs ago)
3    10.11.11.11:46126 outside 0 0 1  Last: 10.10.10.10 (6 secs ago)
4    10.11.11.11:3695 outside 0 0 1  Last: 10.10.10.10 (6 secs ago)
```

Minaccia di scansione

1. Creare un ACL sull'interfaccia esterna che autorizzi tutti i pacchetti TCP inviati a un server di destinazione all'interno dell'ASA (10.11.11.11):

```
access-list outside_in extended line 1 permit tcp any host 10.11.11.11
access-group outside_in in interface outside
```

> **Nota**: per consentire alla funzionalità Scanning Threat Detection di tenere traccia degli IP di destinazione e degli utenti non autorizzati, il traffico deve essere autorizzato tramite l'appliance ASA.

2. Se il server di destinazione non esiste effettivamente o se ripristina i tentativi di connessione dell'utente malintenzionato, configurare una voce ARP falsa sull'appliance ASA in modo da bloccare il traffico di attacco verso l'interfaccia interna:

```
arp inside 10.11.11.11 dead.dead.dead
```

> **Nota**: le connessioni reimpostate dal server di destinazione non vengono considerate come parte della minaccia.

3. Da un utente malintenzionato all'esterno dell'appliance ASA (10.10.10.10), usare nmap per eseguire una scansione SYN di TCP su tutte le porte del server di destinazione:

```
nmap -sS -T5 -p1-65535 -Pn 10.11.11.11
```

> **Nota**: T5 configura nmap per eseguire l'analisi il più rapidamente possibile. In base alle risorse del PC autore dell'attacco, questa operazione non è ancora abbastanza veloce da attivare alcune delle tariffe predefinite. In questo caso, è sufficiente ridurre le velocità configurate per la minaccia che si desidera visualizzare. Quando si imposta ARI e BRI su 0, il rilevamento delle minacce di base attiva sempre la minaccia indipendentemente dalla frequenza.

4. Si noti che viene rilevata una minaccia di scansione, che l'indirizzo IP dell'utente non autorizzato viene rilevato e che l'utente non autorizzato viene escluso:

```
%ASA-1-733100: [ Scanning] drop rate-1 exceeded. Current burst rate is 17 per second,
max configured rate is 10; Current average rate is 0 per second,
 max configured rate is 5; Cumulative total count is 404
%ASA-4-733101: Host 10.10.10.10 is attacking. Current burst rate is 17 per second,
 max configured rate is 10; Current average rate is 0 per second,
 max configured rate is 5; Cumulative total count is 700
%ASA-4-733102: Threat-detection adds host 10.10.10.10 to shun list
```

Informazioni correlate

- **Guida alla configurazione dell'ASA**
- **Guida di riferimento ai comandi ASA**
- **Messaggi syslog Cisco Secure Firewall serie ASA**
- **Supporto tecnico e download Cisco**

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).