Esempio di configurazione del router ASA/PIX/IOS in modalità shun/blocco su IPS

Sommario

Introduzione

Questo documento descrive come configurare il shun su un router PIX/ASA/Cisco IOS con l'aiuto di Cisco IPS. ARC, l'applicazione che blocca il sensore, avvia e arresta i blocchi sui router, sugli switch Cisco serie 5000 RSM e Catalyst serie 6500, sui PIX Firewall, su FWSM e su ASA. L'ARC invia un blocco o una shun al dispositivo gestito per l'indirizzo IP dannoso. L'ARC invia lo stesso blocco a tutti i dispositivi gestiti dal sensore. Se è stato configurato un sensore di blocco primario, il blocco viene inoltrato ed emesso da questo dispositivo. ARC controlla l'ora del blocco e rimuove il blocco alla scadenza dell'ora.

Quando si usa IPS 5.1, prestare particolare attenzione quando si esegue lo shun sui firewall in modalità a più contesti, in quanto con la richiesta shun non vengono inviate informazioni VLAN.

> **Nota:** Blocco non supportato nel contesto di amministrazione di un modulo FWSM a più contesti.

Esistono tre tipi di blocchi:

- Blocco host: blocca tutto il traffico proveniente da un determinato indirizzo IP.
- Blocco connessione: blocca il traffico proveniente da un determinato indirizzo IP di origine e diretto a un determinato indirizzo IP di destinazione e porta di destinazione. Più blocchi di connessione dallo stesso indirizzo IP di origine a un indirizzo IP di destinazione o a una porta di destinazione differente passano automaticamente il blocco da un blocco di connessione a un blocco host.**Nota:** I blocchi di connessione non sono supportati dalle appliance di sicurezza. Le appliance di sicurezza supportano solo blocchi host con informazioni opzionali su porte e protocolli.

- Blocco di rete - Blocca tutto il traffico proveniente da una determinata rete. È possibile avviare i blocchi host e di connessione manualmente o automaticamente quando viene attivata una firma. I blocchi di rete possono essere avviati solo manualmente.

Per i blocchi automatici, è necessario scegliere Request Block Host o Request Block Connection come azione evento per determinate firme, in modo che SensorApp invii una richiesta di blocco ad ARC quando viene attivata la firma. Una volta che ARC riceve la richiesta di blocco da SensorApp, aggiorna le configurazioni del dispositivo per bloccare l'host o la connessione. Fare riferimento a Assegnazione di azioni alle firme, pagina 5-22 per ulteriori informazioni sulla procedura per aggiungere alla firma le azioni evento Host blocco richieste o Connessione blocco richieste. Fare riferimento a Configurazione delle sostituzioni delle azioni evento, pagine 7-15 per ulteriori informazioni sulla procedura per la configurazione delle sostituzioni che aggiungono le azioni evento Host blocco richiesta o Connessione blocco richiesta agli allarmi di una classificazione di rischio specifica.

Sui router Cisco e gli switch Catalyst serie 6500, ARC crea blocchi applicando ACL o VACL. Gli ACL e i VACL applicano filtri alle interfacce, che includono rispettivamente direzione e VLAN, per autorizzare o bloccare il traffico. . PIX Firewall, FWSM e ASA non utilizzano ACL o VACL. Vengono utilizzati il comando **shun** incorporato e **no shun**.

Queste informazioni sono obbligatorie per la configurazione di ARC:

- ID utente di accesso, se il dispositivo è configurato con AAA
- Password di accesso
- Abilita password, che non è necessaria se l'utente dispone di privilegi di abilitazione
- Interfacce da gestire, ad esempio ethernet0, vlan100
- Eventuali informazioni ACL o VACL esistenti che si desidera applicare all'inizio (ACL pre-blocco o VACL) o alla fine (ACL post-blocco o VACL) dell'ACL o del VACL creato. Ciò non si applica a PIX Firewall, FWSM o ASA perché non usano ACL o VACL per bloccare.
- Uso eventuale di Telnet o SSH per comunicare con il dispositivo
- Indirizzi IP (host o intervallo di host) che non si desidera mai bloccare
- Durata dei blocchi

Prerequisiti

Requisiti

Prima di configurare ARC per il blocco o la limitazione della velocità, è necessario completare le seguenti attività:

- Analizzare la topologia di rete per individuare i dispositivi da bloccare e gli indirizzi da bloccare.
- Raccogliere i nomi utente, le password dei dispositivi, le password di abilitazione e i tipi di connessione (Telnet o SSH) necessari per accedere a ciascun dispositivo.
- Conoscere i nomi delle interfacce sui dispositivi.
- Conoscere i nomi dell'ACL o del VACL pre-blocco e dell'ACL o del VACL post-blocco, se necessario.
- Comprendere quali interfacce devono e non devono essere bloccate e in quale direzione (in o out).

Componenti usati

Le informazioni fornite in questo documento si basano su Cisco Intrusion Prevention System 5.1 e versioni successive.

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.

> **Nota:** Per impostazione predefinita, ARC è configurato per un limite di 250 voci di blocco. Per ulteriori informazioni sull'elenco dei dispositivi di blocco supportati da ARC, fare riferimento a Dispositivi supportati.

Convenzioni

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

Premesse

Utilizzare la pagina Blocco per configurare le impostazioni di base necessarie per abilitare il blocco e la limitazione della velocità.

L'ARC controlla le azioni di blocco e limitazione della velocità sui dispositivi gestiti.

Ènecessario regolare il sensore per identificare gli host e le reti che non devono essere bloccati. È possibile che il traffico di un dispositivo attendibile generi una firma. Se questa firma è configurata per bloccare l'autore dell'attacco, il traffico di rete legittimo può essere interessato. L'indirizzo IP del dispositivo può essere elencato nell'elenco Mai bloccare per evitare questo scenario.

Una maschera di rete specificata in una voce Non bloccare viene applicata all'indirizzo Non bloccare mai. Se non viene specificata alcuna maschera di rete, viene applicata una maschera /32 predefinita.

> **Nota:** Per impostazione predefinita, al sensore non è consentito emettere un blocco per il proprio indirizzo IP in quanto ciò interferisce con la comunicazione tra il sensore e il dispositivo di blocco. Tuttavia, questa opzione è configurabile dall'utente.

Se l'ARC è stato configurato per la gestione di un dispositivo di blocco, gli shun e gli ACL/VACL del dispositivo di blocco utilizzati per il blocco non devono essere modificati manualmente. Ciò può causare un'interruzione del servizio ARC e può comportare la mancata emissione di blocchi futuri.

> **Nota:** Per impostazione predefinita, sui dispositivi Cisco IOS è supportato solo il blocco. È possibile ignorare il valore predefinito di blocco se si sceglie la limitazione di velocità o il blocco più la limitazione di velocità.

Per rilasciare o modificare i blocchi, l'utente IPS deve disporre del ruolo Administrator o Operator.

Configurazione del sensore per la gestione dei router Cisco

In questa sezione viene descritto come configurare il sensore per gestire i router Cisco. Contiene gli argomenti seguenti:

Configura profili utente

Il sensore gestisce gli altri dispositivi con il comando **user-profiles** *nome_profilo* per impostare i profili utente. I profili utente contengono le informazioni relative all'ID utente, alla password e all'abilitazione della password. Ad esempio, i router che condividono tutte le stesse password e gli stessi nomi utente possono trovarsi in un unico profilo utente.

> **Nota:** È **necessario** creare un profilo utente prima di configurare il dispositivo di blocco.

Per impostare i profili utente, completare i seguenti passaggi:

1. Accedere alla CLI con un account con privilegi di amministratore.
2. Accedere alla modalità di accesso alla rete.
```
sensor#configure terminal
sensor(config)#service network-access
sensor(config-net)#
```
3. Creare il nome del profilo utente.
```
sensor(config-net)#user-profiles PROFILE1
```
4. Digitare il nome utente per il profilo utente.
```
sensor(config-net-use)#username username
```
5. Specificare la password per l'utente.
```
sensor(config-net-use)# password
Enter password[]: ********
Re-enter password ********
```
6. Specificare la password di abilitazione per l'utente.
```
sensor(config-net-use)# enable-password
Enter enable-password[]: ********
Re-enter enable-password ********
```
7. Verificare le impostazioni.
```
sensor(config-net-use)#show settings
   profile-name: PROFILE1
   -----------------------------------------------
      enable-password: <hidden>
      password: <hidden>
      username: jsmith default:
   -----------------------------------------------
sensor(config-net-use)#
```
8. Uscire dalla modalità secondaria di accesso alla rete.

```
sensor(config-net-use)#exit
sensor(config-net)#exit
Apply Changes:?[yes]:
```

9. Premere **Invio** per applicare le modifiche o immettere no per ignorarle.

Router e ACL

Se l'ARC è configurato con un dispositivo di blocco che usa gli ACL, gli ACL sono composti nel modo seguente:

1. Una riga di autorizzazione con l'indirizzo IP del sensore o, se specificato, l'indirizzo NAT del sensore**Nota:** Se si permette al sensore di essere bloccato, questa riga non viene visualizzata nell'ACL.
2. ACL pre-blocco (se specificato): Questo ACL deve esistere già nel dispositivo.**Nota:** ARC legge le righe nell'ACL preconfigurato e le copia all'inizio dell'ACL di blocco.
3. Qualsiasi blocco attivo
4. Selezionare **ACL post-blocco** o **permettere ip any**:**ACL post-blocco** (se specificato):Questo ACL deve esistere già nel dispositivo.**Nota:** ARC legge le righe nell'ACL e le copia alla fine dell'ACL.**Nota:** Se si desidera che tutti i pacchetti non corrispondenti siano autorizzati, verificare che l'ultima riga dell'ACL sia allow ip any.**allow ip any any** (non utilizzato se è specificato un ACL post-blocco)

   Nota: Gli ACL creati da ARC non devono essere modificati dall'utente o da altri sistemi. Questi ACL sono temporanei e il sensore crea costantemente nuovi ACL. Le uniche modifiche che è possibile apportare sono agli ACL pre-blocco e post-blocco.

Per modificare l'ACL pre-blocco o post-blocco, attenersi alla seguente procedura:

1. Disattivare il blocco sul sensore.
2. Apportare le modifiche alla configurazione del dispositivo.
3. Riattivare il blocco sul sensore.

Quando il blocco viene riattivato, il sensore legge la nuova configurazione del dispositivo.

Nota: Un singolo sensore può gestire più dispositivi, ma più sensori non possono gestire un singolo dispositivo. Nel caso in cui i blocchi emessi da più sensori siano destinati a un unico dispositivo di blocco, un sensore di blocco primario deve essere incorporato nel progetto. Un sensore di blocco primario riceve richieste di blocco da più sensori e invia tutte le richieste di blocco al dispositivo di blocco.

Gli ACL pre-blocco e post-blocco vengono creati e salvati nella configurazione del router. Questi ACL devono essere ACL IP estesi, con nome o numero. Per ulteriori informazioni su come creare gli ACL, consultare la documentazione del router.

Nota: Gli ACL pre-blocco e post-blocco non si applicano alla limitazione della velocità.

Gli ACL vengono valutati dall'alto verso il basso e viene eseguita la prima corrispondenza. L'ACL pre-blocco può contenere un'autorizzazione che ha la precedenza su una negazione risultante da un blocco.

L'ACL post-blocco viene usato per tenere conto di tutte le condizioni non gestite dagli ACL o dai blocchi pre-blocco. Se sull'interfaccia è presente un ACL nella direzione di emissione dei blocchi, è possibile usare tale ACL come ACL post-blocco. Se non si dispone di un ACL post-blocco, il sensore inserisce un indirizzo ip any alla fine del nuovo ACL.

Quando il sensore si avvia, legge il contenuto dei due ACL. Viene creato un terzo ACL con queste voci:

- Una riga di autorizzazione per l'indirizzo IP del sensore
- Copie di tutte le righe di configurazione dell'ACL pre-blocco
- Riga di rifiuto per ogni indirizzo bloccato dal sensore
- Copie di tutte le righe di configurazione dell'ACL post-blocco

Il sensore applica il nuovo ACL all'interfaccia e alla direzione specificate.

> **Nota:** Quando il nuovo ACL di blocco viene applicato a un'interfaccia del router, in una particolare direzione, sostituisce qualsiasi ACL preesistente su quell'interfaccia nella direzione specificata.

Configurazione dei router Cisco tramite CLI

Per configurare un sensore in modo da gestire un router Cisco per eseguire il blocco e la limitazione della velocità, completare la procedura seguente:

1. Accedere alla CLI con un account con privilegi di amministratore.
2. Accedere alla modalità secondaria di accesso alla rete.
   ```
   sensor#configure terminal
   sensor(config)#service network-access
   sensor(config-net)#
   ```
3. Specificare l'indirizzo IP del router controllato da ARC.
   ```
   sensor(config-net)#router-devices ip_address
   ```
4. Immettere il nome della periferica logica creata durante la configurazione del profilo utente.
   ```
   sensor(config-net-rou)#profile-name user_profile_name
   ```
   Nota: L'ARC accetta tutto ciò che viene immesso. Non verifica se il profilo utente esiste.
5. Specificare il metodo utilizzato per accedere al sensore.
   ```
   sensor(config-net-rou)# communication {telnet | ssh-des | ssh-3des}
   ```

   Se non si specifica un valore, viene utilizzato SSH 3DES.**Nota:** Se si usa DES o 3DES, è necessario usare il comando **ssh host-key ip_address** per accettare la chiave SSH dal dispositivo.
6. Specificare l'indirizzo NAT del sensore.
   ```
   sensor(config-net-rou)#nat-address nat_address
   ```
   Nota: In questo modo l'indirizzo IP nella prima riga dell'ACL viene modificato dall'indirizzo del sensore all'indirizzo NAT. L'indirizzo NAT è l'indirizzo del sensore, post-NAT, tradotto da un dispositivo intermedio, situato tra il sensore e il dispositivo di blocco.
7. Specificare se il router esegue il blocco, la limitazione della velocità o entrambi.**Nota:** Il valore predefinito è blocking. Se si desidera che il router esegua solo il blocco, non è necessario configurare le funzionalità di risposta.Solo limitazione della velocità
   ```
   sensor(config-net-rou)#response-capabilities rate-limit
   ```

Blocco e limitazione della velocità
```
sensor(config-net-rou)#response-capabilities block|rate-limit
```

8. Specificare il nome e la direzione dell'interfaccia.
```
sensor(config-net-rou)#block-interfaces interface_name {in | out}
```

Nota: Il nome dell'interfaccia deve essere un'abbreviazione riconosciuta dal router quando viene utilizzata dopo il comando **interface**.

9. (Facoltativo) Aggiungere il nome pre-ACL (solo blocco).
```
sensor(config-net-rou-blo)#pre-acl-name pre_acl_name
```
10. (Facoltativo) Aggiungere il nome dell'ACL successivo (solo blocco).
```
sensor(config-net-rou-blo)#post-acl-name post_acl_name
```
11. Verificare le impostazioni.
```
sensor(config-net-rou-blo)#exit

sensor(config-net-rou)#show settings

   ip-address: 10.89.127.97
   -----------------------------------------------
      communication: ssh-3des default: ssh-3des
      nat-address: 19.89.149.219 default: 0.0.0.0
      profile-name: PROFILE1
      block-interfaces (min: 0, max: 100, current: 1)
      -----------------------------------------------
         interface-name: GigabitEthernet0/1
         direction: in
         -----------------------------------------------
            pre-acl-name: <defaulted>
            post-acl-name: <defaulted>
         -----------------------------------------------
      -----------------------------------------------
      response-capabilities: block|rate-limit default: block
   -----------------------------------------------
sensor(config-net-rou)#
```
12. Uscire dalla modalità secondaria di accesso alla rete.
```
sensor(config-net-rou)#exit
sensor(config-net)#exit
sensor(config)#exit
Apply Changes:?[yes]:
```
13. Premere **Invio** per applicare le modifiche o immettere **no** per ignorarle.

Configurazione del sensore per la gestione dei firewall Cisco

Per configurare il sensore in modo da gestire i firewall Cisco, completare i seguenti passaggi:

1. Accedere alla CLI con un account con privilegi di amministratore.
2. Accedere alla modalità secondaria di accesso alla rete.
```
sensor#configure terminal
sensor(config)#service network-access
sensor(config-net)#
```
3. Specificare l'indirizzo IP del firewall controllato da ARC.
```
sensor(config-net)#firewall-devices ip_address
```
4. Immettere il nome del profilo utente creato durante la configurazione del profilo utente.
```
sensor(config-net-fir)#profile-name user_profile_name
```
Nota: ARC accetta tutto ciò che viene digitato. Non verifica se il dispositivo logico esiste.
5. Specificare il metodo utilizzato per accedere al sensore.

```
sensor(config-net-fir)#communication {telnet | ssh-des | ssh-3des}
```

Se non si specifica un valore, viene utilizzato SSH 3DES.**Nota:** Se si usa DES o 3DES, è necessario usare il comando **ssh host-key ip_address** per accettare la chiave o l'ARC non può connettersi al dispositivo.

6. Specificare l'indirizzo NAT del sensore.
   ```
   sensor(config-net-fir)#nat-address nat_address
   ```
   Nota: In questo modo l'indirizzo IP nella prima riga dell'ACL viene modificato dall'indirizzo IP del sensore all'indirizzo NAT. L'indirizzo NAT è l'indirizzo del sensore, post-NAT, tradotto da un dispositivo intermedio, situato tra il sensore e il dispositivo di blocco.
7. Uscire dalla modalità secondaria di accesso alla rete.
   ```
   sensor(config-net-fir)#exit
   sensor(config-net)#exit
   sensor(config)#exit
   Apply Changes:?[yes]:
   ```
8. Premere **Invio** per applicare le modifiche o immettere **no** per ignorarle.

Blocco con SHUN in PIX/ASA

L'esecuzione del comando **shun** blocca le connessioni da un host in attacco. I pacchetti che corrispondono ai valori del comando vengono eliminati e registrati fino alla rimozione della funzione di blocco. La **condivisione** viene applicata indipendentemente dal fatto che sia attiva una connessione con l'indirizzo host specificato.

Se si specificano l'indirizzo di destinazione, le porte di origine e di destinazione e il protocollo, la condivisione verrà limitata alle connessioni che corrispondono a tali parametri. È possibile avere un solo comando **shun** per ogni indirizzo IP di origine.

Poiché il comando **shun** viene utilizzato per bloccare gli attacchi in modo dinamico, non viene visualizzato nella configurazione dell'accessorio di protezione.

Ogni volta che si rimuove un'interfaccia, vengono rimossi anche tutti gli shun collegati a tale interfaccia.

Nell'esempio viene mostrato come l'host che ha commesso l'errore (10.1.1.27) stabilisca una connessione con la vittima (10.2.2.89) sul protocollo TCP. Il collegamento nella tabella dei collegamenti dell'accessorio di protezione è il seguente:

```
TCP outside:10.1.1.27/555 inside:10.2.2.89/666
```

Per bloccare le connessioni da un host attaccante, utilizzare il comando **shun** in modalità di esecuzione privilegiata. Applicare il comando **shun** con queste opzioni:

```
hostname#shun 10.1.1.27 10.2.2.89 555 666 tcp
```

Il comando elimina la connessione dalla tabella di connessione dell'appliance di sicurezza e impedisce ai pacchetti da 10.1.1.27:55 a 10.2.2.89:666 (TCP) di passare attraverso l'appliance di sicurezza.

Informazioni correlate

- Configurazione del sensore per la gestione di switch Catalyst serie 6500 e router Cisco serie 7600
- Documentazione e supporto tecnico – Cisco Systems