Esempio di configurazione della funzione ASA 8.2.X TCP State Bypass

Sommario

Introduzione

In questo documento viene descritto come configurare la funzione TCP State Bypass. Questa funzione consente flussi in entrata e in uscita attraverso appliance Cisco ASA serie 5500 Adaptive Security separate.

Prerequisiti

Requisiti di licenza

Le appliance Cisco ASA serie 5500 Adaptive Security devono avere almeno la licenza base.

Componenti usati

Il riferimento delle informazioni contenute in questo documento è Cisco Adaptive Security Appliance (ASA) versione 8.2(1) e 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.

Convenzioni

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

Bypass stato TCP

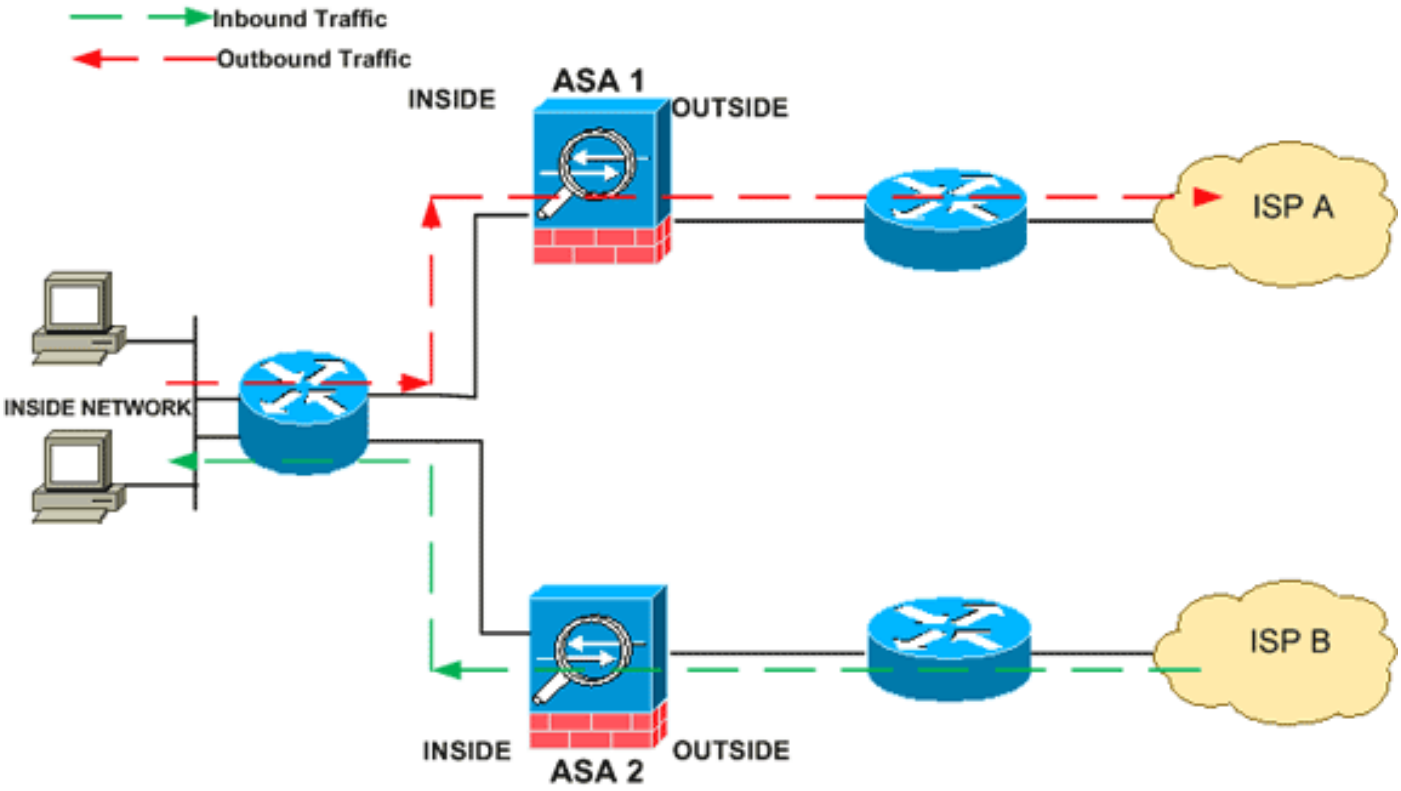
Per impostazione predefinita, tutto il traffico che attraversa Cisco Adaptive Security Appliance (ASA) viene ispezionato utilizzando l'algoritmo di sicurezza adattivo e viene autorizzato o rifiutato in base ai criteri di sicurezza. Per ottimizzare le prestazioni del firewall, l'ASA controlla lo stato di ciascun pacchetto (ad esempio, si tratta di una nuova connessione o di una connessione stabilita?) e lo assegna al percorso di gestione della sessione (un nuovo pacchetto SYN della connessione), al percorso rapido (una connessione stabilita) o al percorso del control plane (ispezione avanzata).

I pacchetti TCP che corrispondono alle connessioni esistenti nel percorso rapido possono passare attraverso l'appliance di sicurezza adattiva senza ricontrollare ogni aspetto del criterio di sicurezza. Questa funzione ottimizza le prestazioni. Tuttavia, il metodo usato per stabilire la sessione nel percorso rapido (che usa il pacchetto SYN) e i controlli che avvengono nel percorso rapido (come il numero di sequenza TCP) possono ostacolare le soluzioni di routing asimmetrico: il flusso in entrata e in uscita di una connessione deve passare attraverso la stessa appliance ASA.

Ad esempio, una nuova connessione viene stabilita con *ASA 1*. Il pacchetto SYN attraversa il percorso di gestione della sessione e una voce per la connessione viene aggiunta alla tabella dei percorsi rapidi. Se i pacchetti successivi di questa connessione passano attraverso l'appliance *ASA 1*, corrisponderanno alla voce nel percorso rapido e verranno passati. Se i pacchetti successivi passano all'*ASA 2*, dove non era presente un pacchetto SYN che ha attraversato il percorso di gestione della sessione, non vi è alcuna voce nel percorso rapido per la connessione e i pacchetti vengono scartati.

Se sui router a monte è configurato il routing asimmetrico e il traffico è alternato tra due appliance ASA, è possibile configurare il bypass dello stato TCP per il traffico specifico. Il bypass dello stato TCP altera il modo in cui le sessioni vengono stabilite nel percorso rapido e disabilita i controlli del percorso rapido. Questa funzione tratta il traffico TCP in modo analogo alla connessione UDP: quando un pacchetto non SYN corrispondente alle reti specificate entra nell'ASA e non è presente un percorso rapido, il pacchetto attraversa il percorso di gestione della sessione per stabilire la connessione nel percorso rapido. Una volta sul percorso rapido, il traffico ignora i controlli del percorso rapido.

Nell'immagine viene mostrato un esempio di routing asimmetrico, in cui il traffico in uscita attraversa un'appliance ASA diversa da quella in entrata:



Nota: per impostazione predefinita, la funzione TCP state bypass è disabilitata sulle appliance Cisco ASA serie 5500 Adaptive Security.

Informazioni di supporto

In questa sezione vengono fornite le informazioni di supporto per la funzione TCP State Bypass.

- Modalità contesto - Supportata in modalità contesto singolo e multiplo.
- Modalità firewall - Supportata in modalità instradata e trasparente.
- Failover: supporta il failover.

Queste funzionalità non sono supportate quando si utilizza il bypass dello stato TCP:

- Ispezione delle applicazioni: per l'ispezione delle applicazioni è necessario che il traffico in entrata e in uscita passi attraverso la stessa ASA, quindi l'ispezione delle applicazioni non è supportata con il bypass dello stato TCP.
- Sessioni autenticate AAA: quando un utente esegue l'autenticazione con un'appliance ASA, il traffico che ritorna attraverso l'altra appliance viene rifiutato in quanto l'utente non ha eseguito l'autenticazione con l'appliance.
- TCP Intercept, maximum embronic connection limit, TCP sequence number randomization: l'ASA non tiene traccia dello stato della connessione, quindi queste funzionalità non vengono applicate.
- Normalizzazione TCP: il normalizzatore TCP è disabilitato.
- Funzionalità SSM e SSC: non è possibile utilizzare il bypass dello stato TCP e le applicazioni in esecuzione su SSM o SSC, ad esempio IPS o CSC.

Linee guida NAT: Poiché la sessione di conversione viene stabilita separatamente per ciascuna ASA, verificare di configurare il protocollo NAT statico su entrambe le ASA per il traffico di bypass dello stato TCP; se si utilizza un NAT dinamico, l'indirizzo scelto per la sessione sull'appliance *ASA 1* sarà diverso dall'indirizzo scelto per la sessione sull'appliance *ASA 2*.

Configurazione

In questa sezione viene descritto come configurare la funzione TCP State Bypass su Cisco ASA serie 5500 Adaptive Security Appliance (ASA).

Configurazione funzionalità TCP State Bypass

Completare questa procedura per configurare la funzione TCP State Bypass su Cisco ASA serie 5500 Adaptive Security Appliance:

1. Per creare una *mappa* delle *classi,* usare il comando class-map_map_name. La mappa delle classi viene utilizzata per identificare il traffico per il quale si desidera disattivare l'ispezione del firewall con stato. La mappa delle classi utilizzata in questo esempio è *tcp_bypass*.
   ```
   ASA(config)#class-map tcp_bypass
   ```

2. Utilizzare il comando match parameter per specificare il traffico interessante nella mappa di classe. Quando si utilizza la struttura dei criteri modulare, utilizzare il comando **match access-list** in modalità di configurazione mappa delle classi per utilizzare un elenco degli accessi per identificare il traffico a cui si desidera applicare le azioni. Di seguito è riportato un esempio di questa configurazione:
   ```
   ASA(config)#class-map tcp_bypass
   ASA(config-cmap)#match access-list tcp_bypass
   ```

   tcp_bypass è il nome dell'elenco degli accessi utilizzato nell'esempio. Per ulteriori informazioni su come specificare il traffico interessante, fare riferimento a Identificazione del traffico (Mappa classi layer 3/4).
3. Utilizzare il comando policy-map name per aggiungere una mappa dei criteri o modificare una mappa dei criteri (già presente) che imposta le azioni da eseguire sul traffico della mappa delle classi già specificato. Quando si utilizza la struttura dei criteri modulare, utilizzare il comando **policy-map** (senza la parola chiave type) in modalità di configurazione globale per assegnare azioni al traffico identificato con una mappa di classe di layer 3/4 (il comando class-map o class-map type management). In questo esempio, la mappa dei criteri è *tcp_bypass_policy*:
   ```
   ASA(config-cmap)#policy-map tcp_bypass_policy
   ```

4. Utilizzare il comando class in modalità di configurazione mappa dei criteri per assegnare la mappa delle classi (*tcp_bypass*) già creata alla mappa dei criteri (*tcp_bypass_policy*) in cui è possibile assegnare azioni al traffico della mappa delle classi. Nell'esempio, la mappa della classe è *tcp_bypass*:
   ```
   ASA(config-cmap)#policy-map tcp_bypass_policy
   ASA(config-pmap)#class tcp_bypass
   ```

5. Per abilitare la funzione TCP state bypass, usare il comando set connection advanced-options-tcp-state-bypass in modalità di configurazione della classe. Questo comando è stato introdotto nella versione 8.2(1). La modalità di configurazione delle classi è accessibile dalla modalità di configurazione della mappa dei criteri, come illustrato nell'esempio seguente:
   ```
   ASA(config-cmap)#policy-map tcp_bypass_policy
   ASA(config-pmap)#class tcp_bypass
   ASA(config-pmap-c)#set connection advanced-options tcp-state-bypass
   ```

6. Utilizzare il criterio servizio policymap_name [global | interface *intf*] in modalità di configurazione globale per attivare una mappa dei criteri a livello globale su tutte le interfacce o su un'interfaccia di destinazione. Per disabilitare i criteri del servizio, utilizzare la forma **no** di questo comando. Utilizzare il comando **service-policy** per abilitare un set di criteri su un'interfaccia.**global** applica la mappa dei criteri a tutte le interfacce e **interface** applica il criterio a un'interfaccia. È consentito un solo criterio globale. È possibile sostituire il criterio globale in un'interfaccia applicando un criterio del servizio a tale interfaccia. È possibile applicare una sola mappa dei criteri a ciascuna interfaccia.
   ```
   ASA(config-pmap-c)#service-policy tcp_bypass_policy outside
   ```

Di seguito è riportata una configurazione di esempio per il bypass dello stato TCP:

```
!--- Configure the access list to specify the TCP traffic !--- that needs to by-pass inspection
to improve the performance. ASA(config)#access-list tcp_bypass extended permit tcp 10.1.1.0
255.255.255.224 any

!--- Configure the class map and specify the match parameter for the !--- class map to match the
interesting traffic. ASA(config)#class-map tcp_bypass
ASA(config-cmap)#description "TCP traffic that bypasses stateful firewall"
ASA(config-cmap)#match access-list tcp_bypass

!--- Configure the policy map and specify the class map !--- inside this policy map for the
class map. ASA(config-cmap)#policy-map tcp_bypass_policy
ASA(config-pmap)#class tcp_bypass
!--- Use the set connection advanced-options tcp-state-bypass !--- command in order to enable
TCP state bypass feature.

ASA(config-pmap-c)#set connection advanced-options tcp-state-bypass
!--- Use the service-policy policymap_name [ global | interface intf ] !--- command in global
configuration mode in order to activate a policy map !--- globally on all interfaces or on a
targeted interface.

ASA(config-pmap-c)#service-policy tcp_bypass_policy outside

ASA(config-pmap-c)#static (inside,outside) 192.168.1.224 10.1.1.0 netmask
255.255.255.224
```

Verifica

Il comando show conn visualizza il numero di connessioni TCP e UDP attive e fornisce informazioni sulle connessioni di vario tipo. Per visualizzare lo stato della connessione per il tipo di connessione designato, utilizzare il comando show conn in modalità di esecuzione privilegiata. Questo comando supporta gli indirizzi IPv4 e IPv6. La visualizzazione dell'output per le connessioni che utilizzano il **bypass dello stato TCP** include il flag **b**.

Risoluzione dei problemi

Messaggio di errore

L'ASA visualizza questo messaggio di errore anche dopo aver abilitato la funzione TCP-state-bypass.

```
%PIX|ASA-4-313004:Denied ICMP type=icmp_type, from source_address oninterface
interface_name to dest_address:no matching session
```

I pacchetti ICMP sono stati scartati dall'appliance di sicurezza a causa dei controlli di sicurezza aggiunti dalla funzionalità ICMP con stato, ossia risposte echo ICMP senza una richiesta echo valida già passata all'appliance di sicurezza o messaggi di errore ICMP non correlati a sessioni TCP, UDP o ICMP già stabilite nell'appliance di sicurezza.

L'ASA visualizza questo registro anche se il bypass dello stato TCP è abilitato perché non è possibile disabilitare questa funzionalità (ossia, controllare le voci restituite ICMP per il tipo 3 nella tabella delle connessioni). Tuttavia, la funzione TCP state bypass funziona correttamente.

Per impedire la visualizzazione dei messaggi seguenti, utilizzare questo comando:

```
hostname(config)#no logging message 313004
```

Informazioni correlate

- Cisco ASA serie 5500 Adaptive Security Appliance
- RFC (Requests for Comments)
- Documentazione e supporto tecnico – Cisco Systems