Configurazione della funzione TCP State Bypass su ASA serie 5500

Sommario

Introduzione

In questo documento viene descritto come configurare la funzione TCP State Bypass, che consente il flusso del traffico in entrata e in uscita attraverso le appliance Cisco ASA serie 5500 Adaptive Security (ASA) separate.

Prerequisiti

Requisiti

Prima di poter procedere con la configurazione descritta in questo documento, Cisco ASA deve avere installato almeno la licenza base.

Componenti usati

Per la stesura del documento, è stato usato Cisco ASA serie 5500 con software versione 9.x.

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

In questa sezione viene fornita una panoramica della funzione di bypass dello stato TCP e delle relative informazioni di supporto.

Panoramica della funzione TCP State Bypass

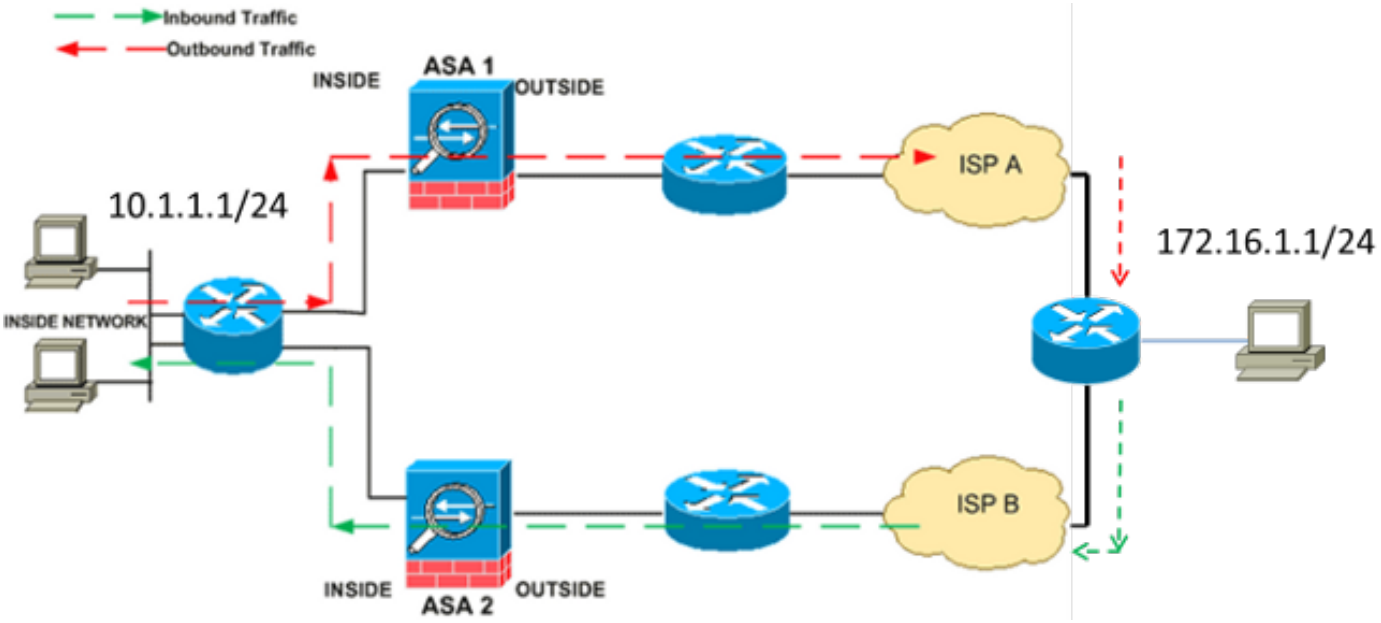
Per impostazione predefinita, tutto il traffico che attraversa l'ASA viene ispezionato tramite l'algoritmo di sicurezza adattivo e può essere attraversato o interrotto in base ai criteri di sicurezza. Per ottimizzare le prestazioni del firewall, l'ASA controlla lo stato di ciascun pacchetto (ad esempio, verifica se si tratta di una nuova connessione o di una connessione stabilita) e lo assegna al percorso di gestione della sessione (un nuovo pacchetto SYN), al percorso rapido (una connessione stabilita) o al percorso del control plane (ispezione avanzata).

I pacchetti TCP che corrispondono alle connessioni correnti nel percorso rapido possono passare attraverso l'ASA senza rivedere 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; i flussi in entrata e in uscita di una connessione devono passare attraverso la stessa 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 su questa connessione passano attraverso l'*ASA 1*, i pacchetti corrispondono alla voce nel percorso rapido e vengono 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 la funzione TCP State Bypass per il traffico specifico. La funzione di 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 che corrisponde alle reti specificate entra nell'ASA e non è presente un percorso rapido, il pacchetto passa attraverso 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: La funzione TCP state bypass è disabilitata per impostazione predefinita su Cisco ASA serie 5500. Inoltre, la configurazione TCP state bypass può causare un numero elevato di connessioni se non è implementata correttamente.

Informazioni di supporto

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

- **Modalità contesto** âÂ La funzione di bypass dello stato TCP è supportata in modalità contesto singolo e multipla.
- **Modalità firewall** âÂ La funzione di bypass dello stato TCP è supportata in modalità instradata e trasparente.
- **Failover**Â La funzione di bypass dello stato TCP supporta il failover.

Queste funzionalità non sono supportate quando si utilizza la funzione di bypass dello stato TCP:

- **L'ispezione delle applicazioni** ÂÂ **richiede** che sia il traffico in entrata che il traffico in uscita passino attraverso la stessa ASA, quindi l'ispezione delle applicazioni non è supportata con la funzione TCP State Bypass.
- **Sessioni di autenticazione, autorizzazione e accounting (AAA)**ÂÂÂ Quando un utente esegue l'autenticazione con un'appliance ASA, il traffico che ritorna attraverso l'altra appliance ASA viene rifiutato in quanto l'utente non ha eseguito l'autenticazione con tale appliance.
- **TCP intercept, maximum embonic connection limit, TCP sequence number randomization** âÂÂ L'ASA non rileva lo stato della connessione, quindi queste funzionalità non vengono applicate.

- **Normalizzazione TCP**Â Il normalizzatore TCP è disabilitato.
- **Funzionalità Security Services Module (SSM) e Security Services Card (SSC)**Â **Non è** possibile utilizzare la funzione TCP State Bypass con qualsiasi applicazione in esecuzione su SSM o SSC, ad esempio IPS o Content Security (CSC).

Nota: Poiché la sessione di conversione viene stabilita separatamente per ciascuna ASA, verificare di configurare il protocollo NAT (Network Address Translation) 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*.

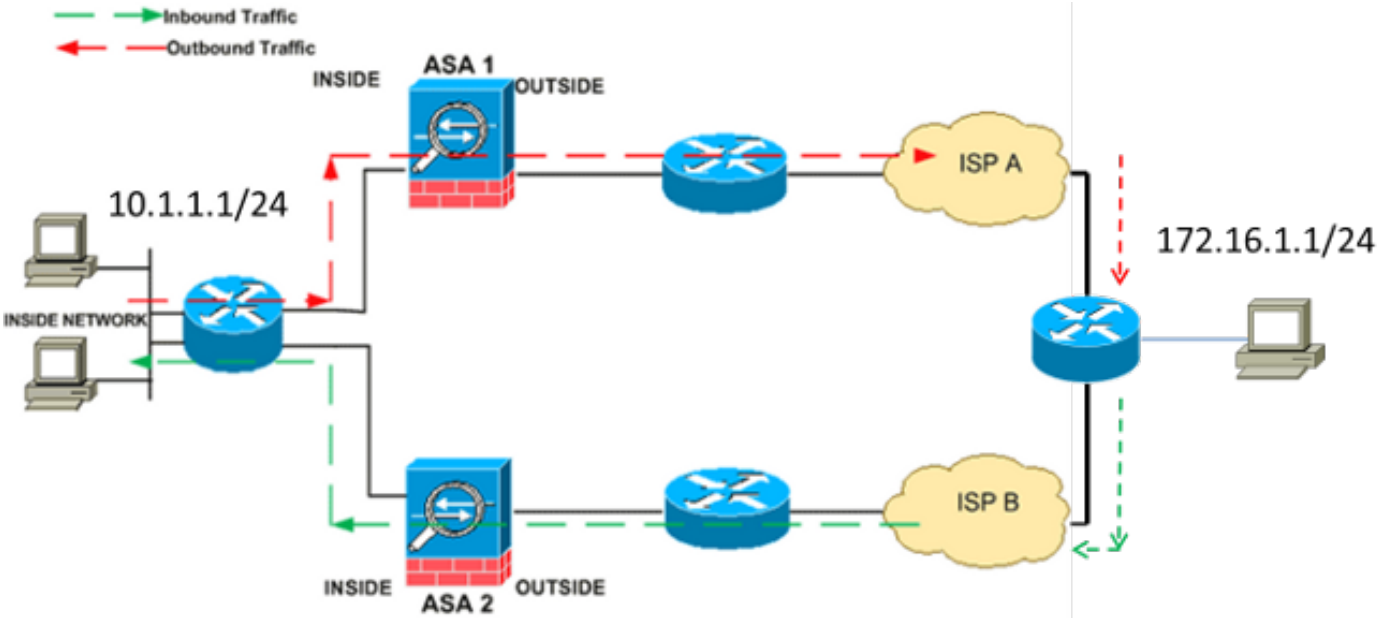
Configurazione

In questa sezione viene descritto come configurare la funzione TCP State Bypass sull'appliance ASA serie 5500 in due scenari diversi.

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

Scenario 1

Questa è la topologia utilizzata per il primo scenario:



Nota: La configurazione descritta in questa sezione deve essere applicata a entrambe le appliance ASA.

Completare questa procedura per configurare la funzione TCP State Bypass:

1. Immettere il comando class-map_map_name per creare una *mappa classi*. La mappa delle classi viene utilizzata per identificare il traffico per cui si desidera disattivare l'ispezione del firewall con stato.**Nota:** La mappa delle classi utilizzata in questo esempio è **tcp_bypass**.
```
ASA(config)#class-map tcp_bypass
```
2. Immettere il comando match parameter per specificare il traffico di interesse all'interno della mappa di classe. Quando si utilizza la struttura dei criteri modulare, utilizzare il comando **match access-list** in modalità di *configurazione class-map* 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
```
Nota: Il valore **tcp_bypass** è il nome dell'elenco degli accessi utilizzato nell'esempio. Per ulteriori informazioni su come specificare il *traffico* di interesse, consultare la sezione Identification Traffic *(*Layer *3/4 Class Map)* della *guida alla configurazione di Cisco ASA serie 5500* dall*'interfaccia CLI 8.2*.
3. Immettere il comando policy-map name per aggiungere una mappa dei criteri o modificare una mappa dei criteri (già presente) che assegna le azioni da eseguire in relazione al traffico della mappa delle classi specificato. Quando si utilizza la struttura dei criteri modulare, utilizzare il comando policy-map (senza la parola chiave *type*) nella modalità di *configurazione globale* per assegnare azioni al traffico identificato con una mappa di classe di layer 3/4 (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. Immettere il comando class in modalità di *configurazione mappa dei criteri* per assegnare la mappa delle classi creata (*tcp_bypass*) alla mappa dei criteri (*tcp_bypass_policy*) in modo da poter assegnare le 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, immettere il comando set connection advanced-options tcp-state-bypass in modalità di *configurazione 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 mostrato 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. Immettere il nome_mappa_criteri dei servizi [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. Immettere il comando **service-policy** per abilitare un set di criteri su un'interfaccia. La parola chiave **global** applica la mappa dei criteri a tutte le interfacce, mentre la parola chiave **interface** applica la mappa dei criteri a una sola interfaccia. È consentito un solo criterio globale. Per eseguire l'override del criterio globale in un'interfaccia, è possibile applicare un criterio servizio a tale interfaccia. È possibile applicare una sola mappa dei criteri a ciascuna interfaccia. Di seguito è riportato un esempio:

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

Di seguito è riportata una configurazione di esempio per la funzione TCP state bypass su *ASA1*:

```
!--- Configure the access list to specify the TCP traffic
!--- that needs to by-pass inspection to improve the performance.

ASA1(config)#access-list tcp_bypass extended permit tcp 10.1.1.0 255.255.255.0
172.16.1.0 255.255.255.0

!--- Configure the class map and specify the match parameter for the
!--- class map to match the interesting traffic.

ASA1(config)#class-map tcp_bypass
ASA1(config-cmap)#description "TCP traffic that bypasses stateful firewall"
ASA1(config-cmap)#match access-list tcp_bypass

!--- Configure the policy map and specify the class map
!--- inside this policy map for the class map.

ASA1(config-cmap)#policy-map tcp_bypass_policy
ASA1(config-pmap)#class tcp_bypass

!--- Use the set connection advanced-options tcp-state-bypass
!--- command in order to enable TCP state bypass feature.

ASA1(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.

ASA1(config-pmap-c)#service-policy tcp_bypass_policy outside

!--- NAT configuration

ASA1(config)#object network obj-10.1.1.0
ASA1(config-network-object)#subnet 10.1.1.0 255.255.255.0
ASA1(config-network-object)#nat(inside,outside) static 192.168.1.0
```

Di seguito è riportata una configurazione di esempio per la funzione TCP state bypass su *ASA2*:

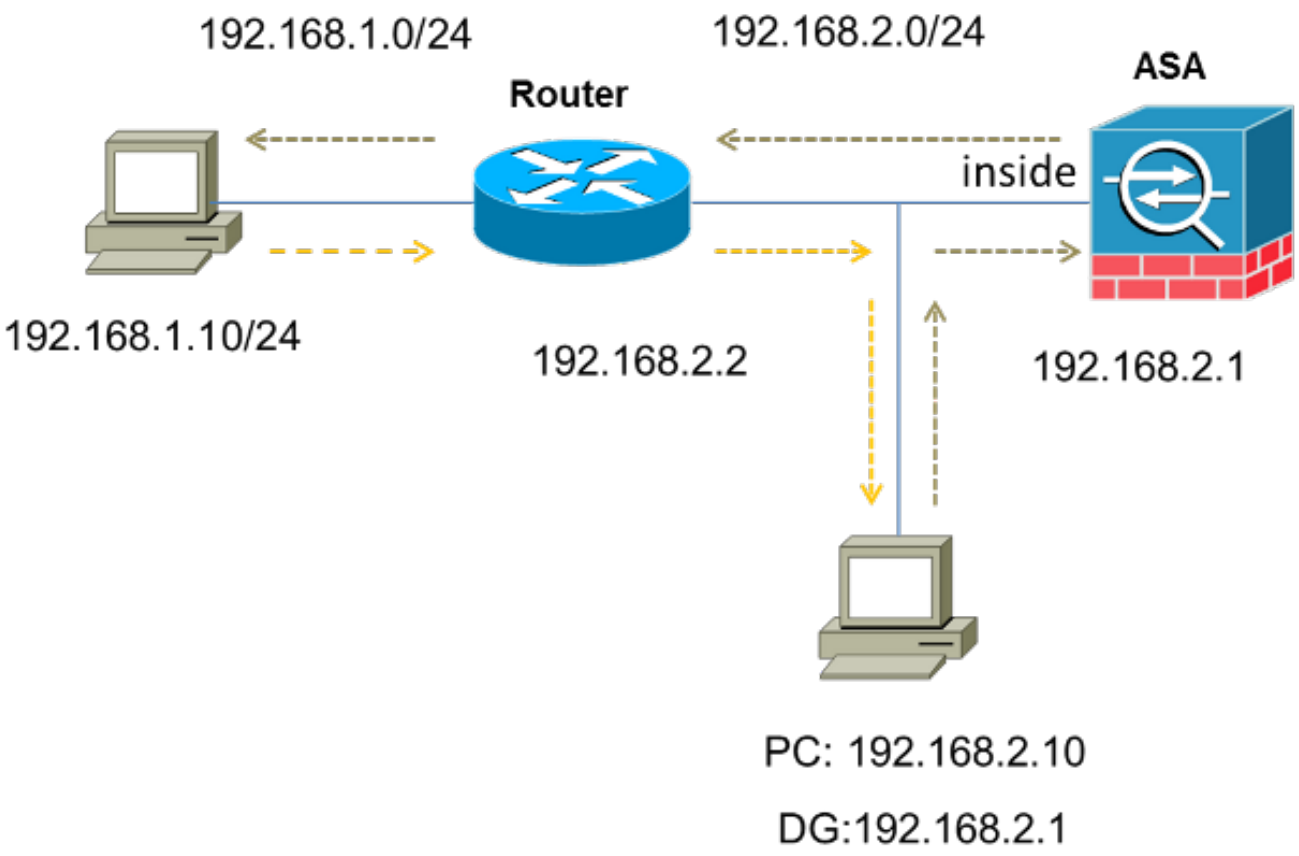
```
!--- Configure the access list to specify the TCP traffic
!--- that needs to by-pass inspection to improve the performance.

ASA2(config)#access-list tcp_bypass extended permit tcp 172.16.1.0 255.255.255.0
10.1.1.0 255.255.255.0

!--- Configure the class map and specify the match parameter for the
!--- class map to match the interesting traffic.

ASA2(config)#class-map tcp_bypass
ASA2(config-cmap)#description "TCP traffic that bypasses stateful firewall"
ASA2(config-cmap)#match access-list tcp_bypass

!--- Configure the policy map and specify the class map
!--- inside this policy map for the class map.
```

```
ASA2(config-cmap)#policy-map tcp_bypass_policy
ASA2(config-pmap)#class tcp_bypass

!--- Use the set connection advanced-options tcp-state-bypass
!--- command in order to enable TCP state bypass feature.

ASA2(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.

ASA2(config-pmap-c)#service-policy tcp_bypass_policy outside

!--- NAT configuration

ASA2(config)#object network obj-10.1.1.0
ASA2(config-network-object)#subnet 10.1.1.0 255.255.255.0
ASA1(config-network-object)#nat(inside,outside) static 192.168.1.0
```

Scenario 2

In questa sezione viene descritto come configurare la funzione di bypass dello stato TCP sull'appliance ASA per scenari che usano il routing asimmetrico, in cui il traffico in entrata e in uscita dall'appliance da una stessa interfaccia (*u-turn*).

Di seguito è riportata la topologia utilizzata in questo scenario:



Completare questa procedura per configurare la funzione TCP State Bypass:

1. Creare un *elenco degli accessi* in modo che corrisponda al traffico che deve ignorare l'ispezione TCP:

```
ASA(config)#access-list tcp_bypass extended permit tcp 192.168.2.0 255.255.255.0
192.168.1.0 255.255.255.0
```

2. Immettere il comando class-map map_name per creare una *mappa classi*. La mappa delle classi viene utilizzata per identificare il traffico per cui si desidera disattivare l'ispezione del firewall con stato.**Nota:** La mappa delle classi utilizzata in questo esempio è **tcp_bypass**.

```
ASA(config)#class-map tcp_bypass
```

3. Immettere il comando match parameter per specificare il traffico di interesse 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
```

Nota: Il valore **tcp_bypass** è il nome dell'elenco degli accessi utilizzato nell'esempio. Per ulteriori informazioni su come specificare il traffico di interesse, consultare la sezione Identificazione del traffico (mappa di classe layer 3/4) della *guida alla configurazione di Cisco ASA serie 5500 dall'interfaccia CLI della versione 8.2*.

4. Immettere 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 in relazione al traffico della mappa delle classi specificato. Quando si utilizza la struttura dei criteri modulare, utilizzare il comando policy-map (senza la parola chiave *type*) nella modalità di *configurazione globale* per assegnare le azioni al traffico identificato con una mappa di classe di layer 3/4 (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
```

5. Immettere il comando class in modalità di *configurazione mappa dei criteri* per assegnare la mappa delle classi creata (*tcp_bypass*) alla mappa dei criteri (*tcp_bypass_policy*) in modo da poter 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
```

6. Per abilitare la funzione TCP state bypass, immettere il comando set connection advanced-options tcp-state-bypass in modalità di *configurazione 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 mostrato 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
```

7. Immettere il nome_mappa_criteri dei servizi [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. Immettere il comando **service-policy** per abilitare un set di criteri su un'interfaccia. La parola chiave **global** applica la mappa dei criteri a tutte le interfacce e la

parola chiave **interface** applica il criterio a una sola interfaccia. È consentito un solo criterio globale. Per eseguire l'override del criterio globale in un'interfaccia, è possibile applicare un criterio servizio a tale interfaccia. È possibile applicare una sola mappa dei criteri a ciascuna interfaccia. Di seguito è riportato un esempio:

```
ASA(config-pmap-c)#service-policy tcp_bypass_policy inside
```

8. Permettere lo stesso livello di sicurezza per il traffico sull'appliance ASA:

```
ASA(config)#same-security-traffic permit intra-interface
```

Di seguito è riportata una configurazione di esempio per la funzione TCP State Bypass sull'appliance ASA:

```
!--- Configure the access list to specify the TCP traffic
!--- that needs to bypass inspection to improve the performance.

ASA(config)#access-list tcp_bypass extended permit tcp 192.168.2.0 255.255.255.0
192.168.1.0 255.255.255.0

!--- 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 inside

!--- Permit same security level traffic on the ASA to support U-turning

ASA(config)#same-security-traffic permit intra-interface
```

Verifica

Immettere il mostra conn per visualizzare il numero di connessioni TCP e UDP attive e le informazioni sulle connessioni dei vari tipi. Per visualizzare lo stato della connessione per il tipo di connessione designato, immettere il mostra conn in modalità *di esecuzione privilegiata*.

Nota: Questo comando supporta gli indirizzi IPv4 e IPv6. L'output visualizzato per le connessioni che utilizzano la funzione di bypass dello stato TCP include il flag **b**.

Di seguito è riportato un esempio di output:

```
ASA(config)show conn
1 in use, 3 most used
TCP tcp 10.1.1.1:49525 tcp 172.16.1.1:21, idle 0:01:10, bytes 230, flags b
```

Risoluzione dei problemi

Non sono disponibili informazioni specifiche sulla risoluzione dei problemi per questa funzionalità. Per informazioni generali sulla risoluzione dei problemi di connettività, consultare i seguenti documenti:

- Esempio di acquisizione di pacchetti ASA con CLI e configurazione ASDM
- ASA 8.2: Flusso di pacchetti attraverso Cisco ASA Firewall

  Nota: Le connessioni TCP di bypass dello stato non vengono replicate nell'unità di standby in una coppia di failover.

Messaggi 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 (Internet Control Message Protocol) vengono scartati dall'appliance ASA a causa dei controlli di sicurezza aggiunti dalla funzionalità ICMP con stato. In genere, si tratta di risposte *echo* ICMP senza una *richiesta echo* valida già passata sull'appliance ASA o di messaggi di errore ICMP non correlati a sessioni TCP, UDP o ICMP attualmente stabilite nell'appliance ASA.

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

Immettere questo comando per evitare che vengano visualizzati questi messaggi:

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

Informazioni correlate

- Cisco Adaptive Security Device Manager
- Cisco ASA serie 5500 Adaptive Security Appliance
- RFC (Requests for Comments)

- Documentazione e supporto tecnico – Cisco Systems