ASA 5500 Series에서 TCP 상태 우회 기능 구성

목차

소개

이 문서에서는 아웃바운드 및 인바운드 트래픽이 별도의 Cisco ASA 5500 Series ASA(Adaptive Security Appliances)를 통과하도록 허용하는 TCP 상태 우회 기능을 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서에 설명된 컨피그레이션을 계속하려면 Cisco ASA에 최소 기본 라이센스가 설치되어 있어야 합니다.

사용되는 구성 요소

이 문서의 정보는 소프트웨어 버전 9.x를 실행하는 Cisco ASA 5500 Series를 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든

명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 규칙을 참조하십시오.

배경 정보

이 섹션에서는 TCP 상태 우회 기능 및 관련 지원 정보에 대한 개요를 제공합니다.

TCP 상태 바이패스 기능 개요

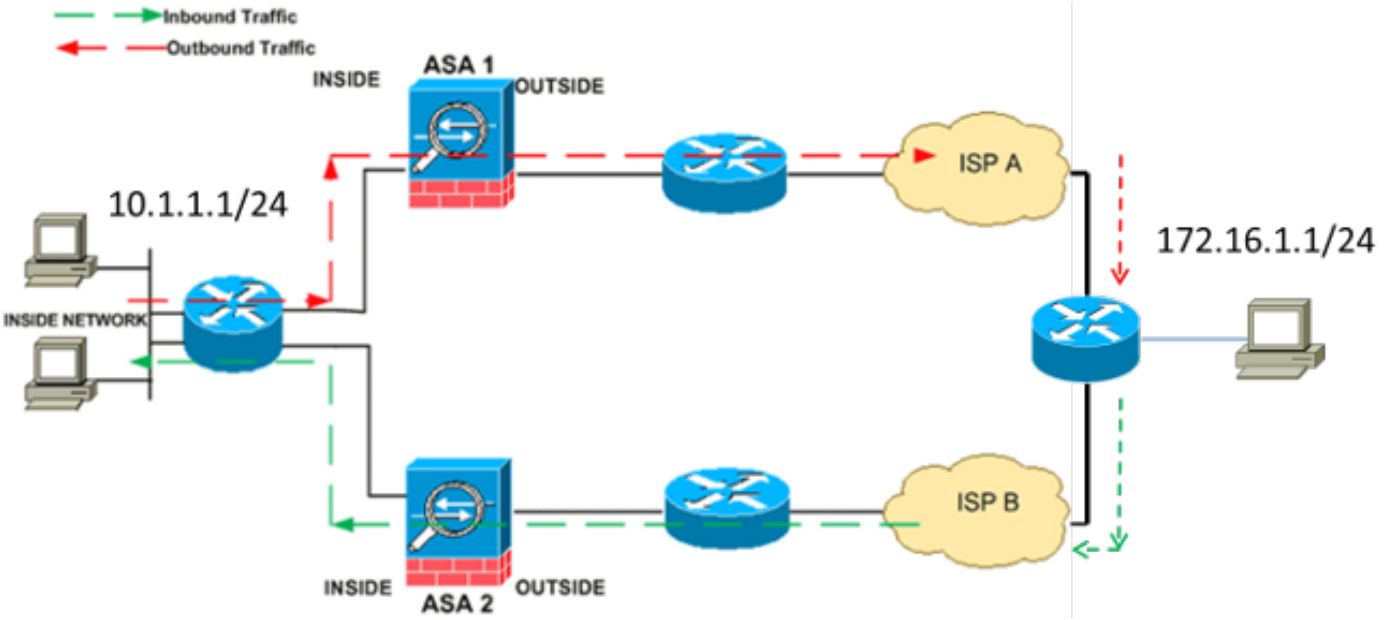
기본적으로 ASA를 통과하는 모든 트래픽은 Adaptive Security Algorithm을 통해 검사되며 보안 정책에 따라 통과하거나 삭제됩니다.방화벽 성능을 최대화하기 위해 ASA는 각 패킷의 상태(예: 새 연결인지 또는 설정된 연결인지 확인)를 확인하고 세션 관리 경로(새 연결 동기화(SYN) 패킷), 빠른 경로(설정된 연결) 또는 컨트롤 플레인 경로(고급 검사)에 할당합니다.

빠른 경로의 현재 연결과 일치하는 TCP 패킷은 보안 정책의 모든 측면을 재확인하지 않고 ASA를 통과할 수 있습니다.이 기능은 성능을 극대화합니다.그러나 빠른 경로(SYN 패킷을 사용)에서 세션을 설정하기 위해 사용되는 방법과 빠른 경로(예: TCP 시퀀스 번호)에서 발생하는 검사는 비대칭 라우팅 솔루션의 방해가 될 수 있습니다.연결의 아웃바운드 및 인바운드 흐름은 모두 동일한 ASA를 통과해야 합니다.

예를 들어, 새 연결은 *ASA 1*로 이동합니다. SYN 패킷은 세션 관리 경로를 통과하며 연결에 대한 항목이 빠른 경로 테이블에 추가됩니다.이 연결의 후속 패킷이 *ASA 1*을 통과하는 경우, 패킷은 빠른 경로의 항목과 일치하고 통과됩니다.후속 패킷이 *ASA 2*로 이동하면 세션 관리 경로를 통과하는 SYN 패킷이 없는 경우 연결의 빠른 경로에 항목이 없으며 패킷이 삭제됩니다.

업스트림 라우터에 비대칭 라우팅이 구성되어 있고 두 ASA 간에 트래픽이 대체되는 경우 특정 트래픽에 대해 TCP 상태 우회 기능을 구성할 수 있습니다.TCP 상태 우회 기능은 빠른 경로에서 세션이 설정되는 방식을 변경하고 빠른 경로 검사를 비활성화합니다.이 기능은 UDP 연결을 처리하는 만큼 TCP 트래픽을 처리합니다.지정된 네트워크와 일치하는 비 SYN 패킷이 ASA에 진입하고 빠른 경로 항목이 없는 경우 패킷이 빠른 경로에서 연결을 설정하기 위해 세션 관리 경로를 거칩니다.빠른 경로에서 트래픽은 빠른 경로 검사를 우회합니다.

이 이미지는 아웃바운드 트래픽이 인바운드 트래픽과 다른 ASA를 통과하는 비대칭 라우팅의 예를 제공합니다.



참고:TCP 상태 우회 기능은 Cisco ASA 5500 Series에서 기본적으로 비활성화되어 있습니다 .또한 TCP 상태 우회 컨피그레이션이 제대로 구현되지 않으면 많은 수의 연결을 일으킬 수 있습니다.

지원 정보

이 섹션에서는 TCP 상태 우회 기능에 대한 지원 정보에 대해 설명합니다.

- **컨텍스트 모드** TCP 상태 우회 기능은 단일 및 다중 컨텍스트 모드에서 지원됩니다.
- **방화벽 모드** TCP 상태 우회 기능은 라우팅 및 투명 모드에서 지원됩니다.
- **장애 조치** TCP 상태 우회 기능은 장애 조치를 지원합니다.

다음 기능은 TCP 상태 우회 기능을 사용할 때 지원되지 않습니다.

- **애플리케이션 검사** 애플리케이션 검사에서는 인바운드 트래픽과 아웃바운드 트래픽이 모두 동일한 ASA를 통과해야 하므로 애플리케이션 검사는 TCP 상태 우회 기능에서 지원되지 않습니다.
- **AAA(Authentication, Authorization, and Accounting) 인증 세션** 사용자가 하나의 ASA로 인증하면 다른 ASA를 통해 반환되는 트래픽은 사용자가 해당 ASA를 인증하지 않았기 때문에 거부됩니다.
- **TCP 가로채기, 최대 원시 연결 제한, TCP 시퀀스 번호 임의 설정** ASA는 연결 상태를 추적하지 않으므로 이러한 기능이 적용되지 않습니다.
- **TCP 정규화** TCP 노멀라이저가 비활성화되어 있습니다.
- **SSM(Security Services Module) 및 SSC(Security Services Card) 기능** SSM 또는 SSC에서 실행되는 애플리케이션(예: IPS 또는 CSC)에서는 TCP 상태 우회 기능을 사용할 수 없습니다.

참고:변환 세션이 각 ASA에 대해 별도로 설정되므로 TCP 상태 우회 트래픽에 대해 두 ASA에

서 고정 NAT(Network Address Translation)를 구성해야 합니다.동적 NAT를 사용하는 경우 *ASA 1*의 세션에 대해 선택한 주소가 *ASA 2*의 세션에 대해 선택된 주소와 *다릅니다*.

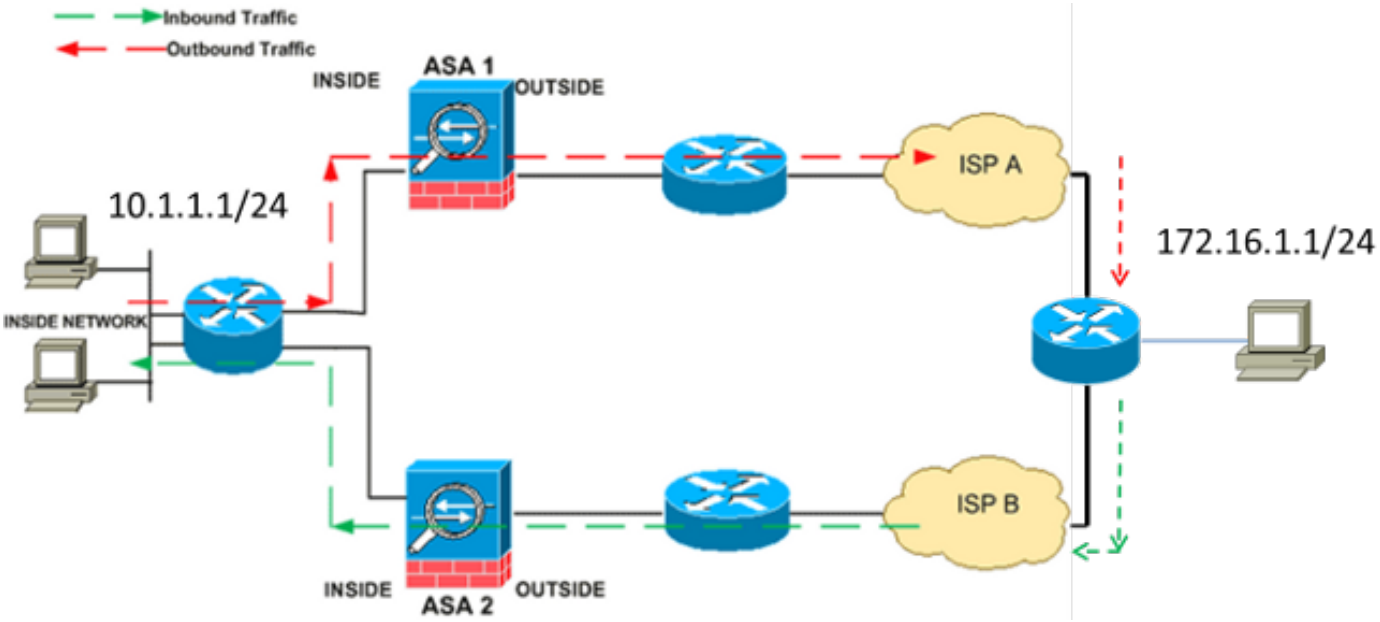
구성

이 섹션에서는 두 가지 시나리오에서 ASA 5500 Series에서 TCP 상태 우회 기능을 구성하는 방법에 대해 설명합니다.

참고:이 섹션에서 사용되는 명령에 대한 자세한 내용을 보려면 Command Lookup Tool(등록된 고객만 해당)을 사용합니다.

시나리오 1

다음은 첫 번째 시나리오에 사용되는 토폴로지입니다.



참고:이 섹션에 설명된 컨피그레이션을 두 ASA에 모두 적용해야 합니다.

TCP 상태 우회 기능을 구성하려면 다음 단계를 완료합니다.

1. *클래스 맵*을 생성하려면 class-map class_map_name 명령을 *입력합니다*.클래스 맵은 상태 기반 방화벽 검사를 비활성화할 트래픽을 식별하는 데 사용됩니다.**참고:**이 예에서 사용되는 클래스 맵은 **tcp_bypass입니다**.
   ```
   ASA(config)#class-map tcp_bypass
   ```
2. 클래스 맵 내에서 관심 있는 트래픽을 지정하려면 match parameter 명령을 입력합니다 .Modular Policy Framework를 사용할 때 작업을 적용할 트래픽을 식별하기 위해 액세스 목록을 사용하려면 *class-map 컨피그레이션* 모드에서 match access-**list** 명령을 사용합니다.다음은 이 구성의 예입니다.

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

```
ASA(config-cmap)#match access-list tcp_bypass
```

참고:tcp_bypass는 이 예에서 사용되는 액세스 목록의 이름입니다.관심의 트래픽을 지정하는 방법에 대한 자세한 내용은 *Cisco ASA 5500 Series Configuration Guide*의 Identifying Traffic (Layer 3/4 Class Map) 섹션을 참조하십시오.

3. 정책 맵을 추가하거나 지정된 클래스 맵 트래픽에 대해 수행할 작업을 할당하는 정책 맵(이미 있음)을 편집하려면 **policy-map name** 명령을 입력합니다.Modular Policy Framework를 사용하는 경우 *전역 컨피그레이션* 모드**에서 policy-map** 명령(type 키워드 없이)을 사용하여 Layer 3/4 클래스 맵(**class-map 또는 class-map type management 명령)으로 식별한 트래픽에 작업을 할당합니다.** 이 예에서 정책 맵은 **tcp_bypass_policy입니다**.

```
ASA(config-cmap)#policy-map tcp_bypass_policy
```

4. 생성된 클래스 맵(tcp_bypass)을 정책 맵(*tcp_bypass_policy*)에 할당하여 클래스 맵 트래픽에 작업을 할당할 수 있도록 정책 맵 *컨피그레이션* 모드에서 class 명령*을* 입력합니다.이 예에서 클래스 맵은 tcp_**bypass입니다**.

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

5. TCP **상태** 우회 기능**을 활성화하려면** *클래스 컨피그레이션* 모드에서 set connection advanced-options tcp-**state-bypass** 명령을 입력합니다.이 명령은 버전 8.2(1)에서 도입되었습니다. *클래스 컨피그레이션* 모드*는 정책 맵 컨피그레이션* 모드에서 액세스할 수 있습니다(다음 예 참조).

```
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. **service-policy**map_name [**global** 입력 | **interface** *intf*는 *전역 컨피그레이션* 모드에서 모든 인터페이스 또는 대상 인터페이스에서 정책 맵을 전역적으로 활성화하려면 명령을 사용합니다.서비스 정책을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.인터페이스에서 정책 집합을 활성화하려면 **service-policy** 명령을 입력합니다.global 키워드는 모든 인터페이스에 정책 맵을 적용하고 **interface** 키워드는 하나의 인터페이스에만 정책 맵을 적용합니다.하나의 전역 정책만 허용됩니다.인터페이스에서 전역 정책을 재정의하려면 해당 인터페이스에 서비스 정책을 적용할 수 있습니다.각 인터페이스에 정책 맵을 하나만 적용할 수 있습니다.예를 들면 다음과 같습니다.

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

*ASA1*에서 TCP 상태 우회 기능에 대한 컨피그레이션의 예는 다음과 같습니다.

```
!--- 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
```

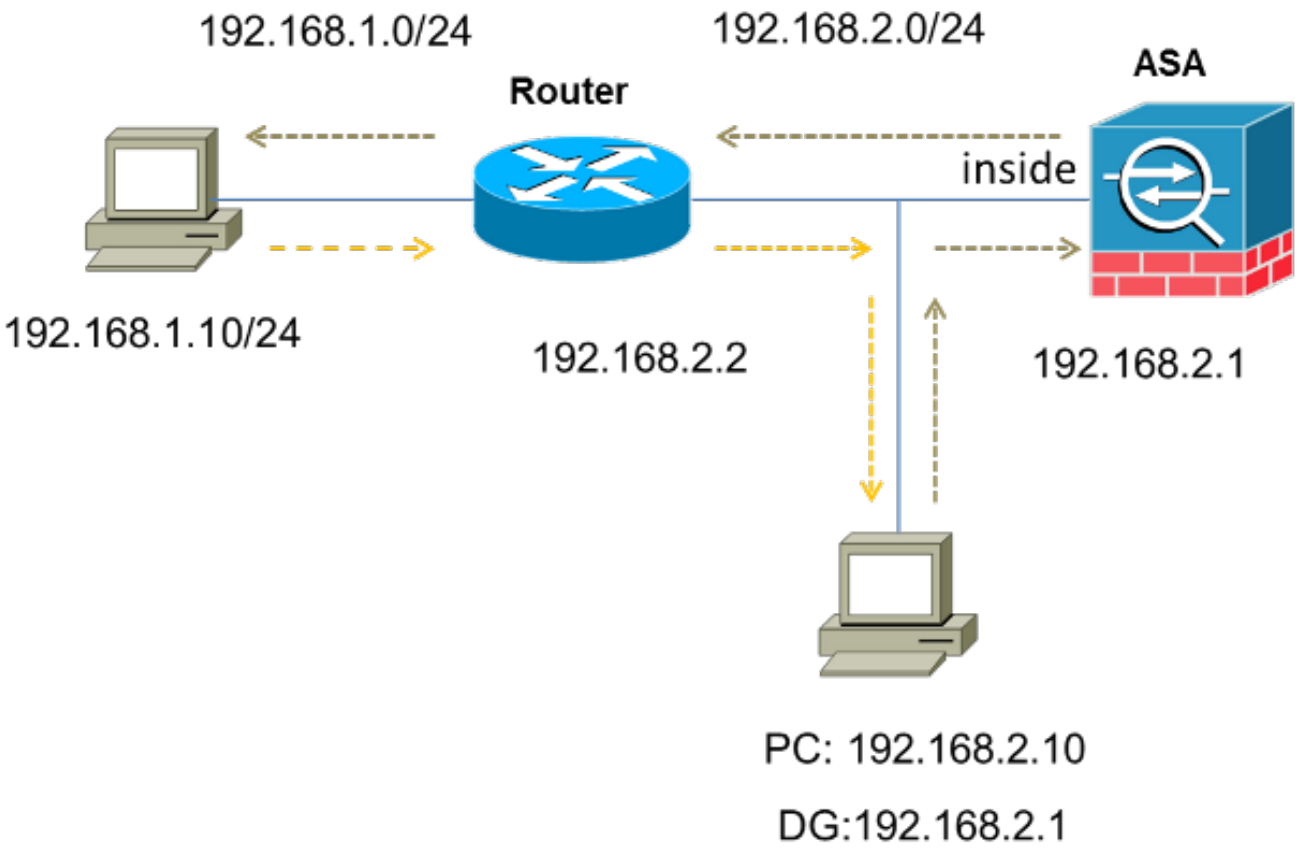
*ASA2*에서 TCP 상태 우회 기능에 대한 컨피그레이션의 예는 다음과 같습니다.

```
!--- 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
```

시나리오 2

이 섹션에서는 트래픽이 동일한 인터페이스(*u-turning*)에서 ASA로 들어오고 나가는 비대칭 라우팅을 사용하는 시나리오에 대해 ASA에서 TCP 상태 우회 기능을 구성하는 방법에 대해 설명합니다.

이 시나리오에서 사용되는 토폴로지는 다음과 같습니다.



TCP 상태 우회 기능을 구성하려면 다음 단계를 완료합니다.

1. TCP 검사를 *우회해야* 하는 트래픽을 매칭하기 위해 access-list를 생성합니다.

   ```
   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. *클래스 맵*을 생성하려면 class-map class_map_name 명령을 *입력합니다*.클래스 맵은 상태 기반 방화벽 검사를 비활성화할 트래픽을 식별하는 데 사용됩니다.**참고:**이 예에서 사용되는 클래스 맵은 **tcp_bypass입니다**.
   ```
   ASA(config)#class-map tcp_bypass
   ```
3. 클래스 맵에 관심 있는 트래픽을 지정하려면 match parameter 명령을 입력합니다.Modular Policy Framework를 사용할 때 작업을 적용할 트래픽을 식별하기 위해 액세스 목록을 사용하려면 클래스 맵 컨피그레이션 모드에서 match access-**list** 명령을 사용합니다.다음은 이 구성의 예입니다.

   ```
   ASA(config)#class-map tcp_bypass
   ASA(config-cmap)#match access-list tcp_bypass
   ```
   참고:tcp_**bypass**는 이 예에서 사용되는 액세스 목록의 이름입니다.관심 있는 트래픽을 지정하는 방법에 대한 자세한 내용은 *Cisco ASA 5500 Series Configuration Guide*의 Identifying Traffic (Layer 3/4 Class Map) 섹션을 참조하십시오.
4. 정책 맵을 추가하거나 지정된 클래스 맵 트래픽에 대해 수행할 작업을 설정하는 정책 맵(이미 있음)을 편집하려면 policy-map name 명령을 입력합니다.Modular Policy Framework를 사용

하는 경우 *전역 컨피그레이션* 모드**에서 policy-map** 명령(type 키워드 없이)을 사용하여 Layer 3/4 클래스 맵(**class-map** 또**는 class-map type management 명령)으로 식별한 트래픽에 작업을 할당합니다.** 이 예에서 정책 맵은 **tcp_bypass_policy입니다**.

```
ASA(config-cmap)#policy-map tcp_bypass_policy
```

5. 생성된 클래스 맵(tcp_bypass)을 정책 맵(*tcp_bypass_policy*)에 할당하여 클래스 맵 트래픽에 작업을 할당할 수 있도록 *policy-map 컨피그레이션* 모드에서 class 명령을 입력합니다.이 예에서 클래스 맵은 **tcp_bypass입니다**.

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

6. TCP 상태 우회 기능**을 활성화하려면** *클래스 컨피그레이션* 모드에서 set connection advanced-options tcp-**state-bypass** 명령을 입력합니다.이 명령은 버전 8.2(1)에서 도입되었습니다. *클래스 컨피그레이션 모드는 정책 맵 컨피그레이션* 모드에서 액세스할 수 있습니다(다음 예 참조).

```
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. service-policymap_name [global 입력 [interface *intf*] *글로벌 컨피그레이션* 모드에서 모든 인터페이스 또는 대상 인터페이스에서 정책 맵을 전역적으로 활성화할 수 있습니다.서비스 정책을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.인터페이스에서 정책 집합을 활성화하려면 **service-policy** 명령을 입력합니다.global 키워드는 모든 인터페이스에 정책 맵을 적용하고 **interface** 키워드는 하나의 인터페이스에만 정책을 적용합니다.하나의 전역 정책만 허용됩니다.인터페이스에서 전역 정책을 재정의하려면 해당 인터페이스에 서비스 정책을 적용할 수 있습니다.각 인터페이스에 정책 맵을 하나만 적용할 수 있습니다.예를 들면 다음과 같습니다.

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

8. ASA의 트래픽에 대해 동일한 보안 수준을 허용합니다.

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

다음은 ASA의 TCP 상태 우회 기능에 대한 컨피그레이션의 예입니다.

```
!--- 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
```

다음을 확인합니다.

다음을 입력합니다. conn 표시 명령을 사용하여 활성 TCP 및 UDP 연결 수와 다양한 유형의 연결에 대한 정보를 볼 수 있습니다.지정된 연결 유형의 연결 상태를 표시하려면 conn 표시 명령(*특권 EXEC* 모드)

> **참고:**이 명령은 IPv4 및 IPv6 주소를 지원합니다.TCP 상태 우회 기능을 사용하는 연결에 대해 표시되는 출력에는 플래그 **b가** 포함됩니다.

다음은 출력의 예입니다.

```
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
```

문제 해결

이 기능에 대한 특정 문제 해결 정보가 없습니다.일반적인 연결 문제 해결 정보는 다음 문서를 참조하십시오.

- CLI 및 ASDM을 사용한 ASA 패킷 캡처 컨피그레이션 예
- ASA 8.2:Cisco ASA 방화벽을 통한 패킷 흐름

  참고:TCP 상태 우회 연결은 장애 조치 쌍의 스탠바이 유닛에 복제되지 않습니다.

오류 메시지

TCP 상태 우회 기능이 활성화된 후에도 ASA에서 이 오류 메시지를 표시합니다.

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

상태 기반 ICMP 기능에 의해 추가된 보안 검사 때문에 ASA에서 ICMP(Internet Control Message Protocol) 패킷을 삭제합니다.이러한 메시지는 일반적으로 ASA를 통해 이미 전달된 유효한 *에코 요청* 없이 ICMP 에코 응답 또는 ASA에 현재 설정된 TCP, UDP 또는 ICMP 세션과 관련이 없는 ICMP

오류 메시지입니다.

이 기능의 비활성화(즉 연결 테이블에서 Type 3에 대한 ICMP *반환* 항목 확인)가 불가능하므로 TCP 상태 우회 기능이 활성화된 경우에도 ASA는 이 로그를 표시합니다.그러나 TCP 상태 우회 기능이 올바르게 작동합니다.

다음 메시지가 표시되지 않도록 하려면 다음 명령을 입력합니다.

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

관련 정보

- Cisco Adaptive Security Device Manager
- Cisco ASA 5500 Series Adaptive Security Appliance
- RFC(Request for Comments)
- 기술 지원 및 문서 – Cisco Systems