ASA 8.2.X TCP 상태 우회 기능 컨피그레이션 예

목차

소개

이 문서에서는 TCP 상태 우회 기능을 구성하는 방법에 대해 설명합니다. 이 기능을 사용하면 별도의 Cisco ASA 5500 Series Adaptive Security Appliances를 통해 아웃바운드 및 인바운드 플로우를 수행할 수 있습니다.

사전 요구 사항

라이센스 요구 사항

Cisco ASA 5500 Series Adaptive Security Appliance에는 최소 기본 라이센스가 있어야 합니다.

사용되는 구성 요소

이 문서의 정보는 버전 8.2(1) 이상의 Cisco ASA(Adaptive Security Appliance)를 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.

TCP 상태 우회

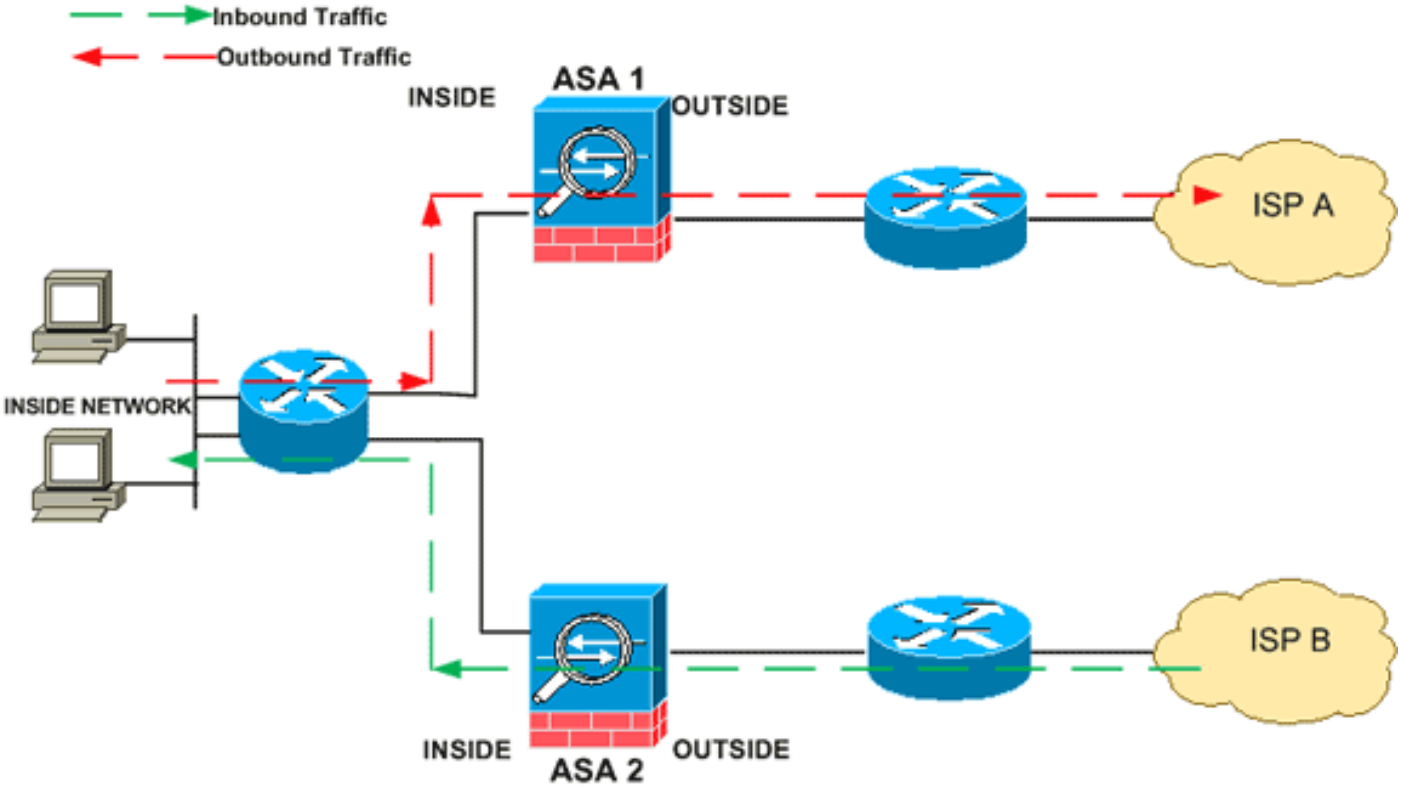
기본적으로 Cisco ASA(Adaptive Security Appliance)를 통과하는 모든 트래픽은 ASA(Adaptive Security Algorithm)를 사용하여 검사되며 보안 정책에 따라 통과 또는 삭제됩니다. 방화벽 성능을 최대화하기 위해 ASA는 각 패킷의 상태(예: 새 연결인가 또는 설정된 연결인가)를 확인하고 세션 관리 경로(새 연결 SYN 패킷), 빠른 경로(설정된 연결) 또는 컨트롤 플레인 경로(고급 검사)에 할당합니다.

빠른 경로의 기존 연결과 일치하는 TCP 패킷은 보안 정책의 모든 측면을 다시 확인하지 않고 Adaptive Security Appliance를 통과할 수 있습니다. 이 기능은 성능을 극대화합니다. 그러나 빠른 경로(SYN 패킷을 사용)에서 세션을 설정하는 데 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 우회를 구성할 수 있습니다. TCP 상태 우회는 빠른 경로에서 세션이 설정되는 방법을 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 패킷은 세션 관리 경로를 통해 빠른 경로에 연결을 설정합니다. 빠른 경로에서 트래픽은 빠른 경로 검사를 우회합니다.

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



참고: Cisco ASA 5500 Series Adaptive Security Appliance에서는 기본적으로 TCP 상태 우회 기능이 비활성화됩니다.

지원 정보

이 섹션에서는 TCP 상태 우회 기능에 대한 지원 정보를 제공합니다.

- 컨텍스트 모드 - 단일 및 다중 컨텍스트 모드에서 지원됩니다.
- 방화벽 모드 - 라우팅 및 투명 모드에서 지원됩니다.
- Failover - 장애 조치를 지원합니다.

다음 기능은 TCP 상태 우회를 사용할 때 지원되지 않습니다.

- 애플리케이션 검사 - 애플리케이션 검사를 수행하려면 인바운드 트래픽과 아웃바운드 트래픽이 모두 동일한 ASA를 통과해야 하므로 애플리케이션 검사는 TCP 상태 우회에서 지원되지 않습니다.
- AAA authenticated sessions(AAA 인증 세션) - 사용자가 하나의 ASA로 인증하면 다른 ASA를 통해 반환되는 트래픽이 거부됩니다. 이는 사용자가 해당 ASA로 인증하지 않았기 때문입니다.
- TCP Intercept, 최대 원시 연결 제한, TCP 시퀀스 번호 임의 설정 - ASA가 연결 상태를 추적하지 않으므로 이러한 기능이 적용되지 않습니다.
- TCP 정규화 - TCP 노멀라이저가 비활성화되어 있습니다.
- SSM 및 SSC 기능 - TCP 상태 우회 및 IPS 또는 CSC와 같은 SSM 또는 SSC에서 실행 중인 애플리케이션을 사용할 수 없습니다.

NAT 지침: 변환 세션이 각 ASA에 대해 별도로 설정되므로 두 ASA에서 모두 TCP 상태 우회 트래픽에 대해 고정 NAT를 구성해야 합니다. 동적 NAT를 사용하는 경우 *ASA 1*에서 세션에 대해 선택한 주소가 *ASA 2*에서 세션에 대해 선택한 주소와 *다릅니다*.

구성

이 섹션에서는 Cisco ASA 5500 Series ASA(Adaptive Security Appliance)에서 TCP 상태 우회 기능을 구성하는 방법에 대해 설명합니다.

TCP 상태 바이패스 기능 컨피그레이션

Cisco ASA 5500 Series Adaptive Security Appliance에서 TCP 상태 우회 기능을 구성하려면 다음 단계를 완료하십시오.

1. *클래스 맵*을 생성하려면 class-map class_map_**name** 명령을 사용합니다. 클래스 맵은 상태 기반 방화벽 검사를 비활성화할 트래픽을 식별하는 데 사용됩니다. 이 예에서 사용되는 클래스 맵은 *tcp_bypass입니다*.
   ```
   ASA(config)#class-map tcp_bypass
   ```

2. 클래스 맵에서 흥미로운 트래픽을 **지정하려면 match parameter** 명령을 사용합니다. Modular Policy Framework를 사용할 때 액세스 목록을 사용하여 작업을 적용할 트래픽을 식별하려면 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
   ```

   *tcp_bypass*는 이 예에서 사용되는 access-list의 이름입니다. 흥미로운 트래픽 지정에 대한 자세한 내용은 트래픽 식별(레이어 3/4 클래스 맵)을 참조하십시오.
3. 이미 지정된 클래스 맵 트래픽과 함께 수행할 작업을 설정하는 정책 맵을 추가하거나(이미 있

는) 정책 맵을 편집하려면 **policy-map name 명령**을 사용합니다. Modular Policy Framework를 사용할 때 Layer 3/4 클래스 맵(class-map 또는 class-map type management 명령)으로 식별한 트래픽에 작업을 할당하려면 전역 컨피그레이션 모드에서 policy-map 명령(type 키워드 없음)을 사용합니다. 이 예에서 정책 맵은 *tcp_bypass_policy입니다*.

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

4. 이미 생성된 클래스 맵(tcp_bypass_policy)을 정책 맵(*tcp_bypass_policy*)에 할당하려면 정책 맵 컨피그레이션 모드에서 class 명령**을** 사용합니다. 여기서 클래스 맵 트래픽에 작업을 할당할 수 있습니다. 이 예에서 클래스 맵은 *tcp_bypass입니다*.

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

5. TCP **상태 우회 기능을 활성화하려면 클래스 컨피그레이션 모드**에서 set connection advanced-options tcp-state-bypass 명령을 사용합니다. 이 명령은 버전 8.2(1)에서 도입되었습니다. 클래스 컨피그레이션 모드는 다음 예와 같이 policy-map 컨피그레이션 모드에서 액세스할 수 있습니다.

```
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 policy map_name [global 사용 모든 인터페이스 또는 대상 인터페이스에서 정책 맵을 전역적으로 활성화하려면 글로벌 컨피그레이션 모드에서 **| interface *intf*] 명령을** 사용합니다. 서비스 정책을 비활성화하려면 이 명령의 **no** 형식을 사용합니다. 인터페이스에서 정책 집합을 활성화하려면 **service-policy** 명령을 사용합니다. **global**은 모든 인터페이스에 정책 맵을 적용하고 **인터페이스**는 하나의 인터페이스에 정책을 적용합니다. 하나의 전역 정책만 허용됩니다. 해당 인터페이스에 서비스 정책을 적용하여 인터페이스에서 전역 정책을 재정의할 수 있습니다. 각 인터페이스에 정책 맵을 하나만 적용할 수 있습니다.

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

다음은 TCP 상태 우회를 위한 샘플 컨피그레이션입니다.

```
!--- 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

다음을 확인합니다.

show conn 명령은 활성 TCP 및 UDP 연결 수를 표시하고 다양한 유형의 연결에 대한 정보를 제공합니다. 지정된 연결 유형에 대한 연결 상태를 표시하려면 특권 EXEC 모드에서 show conn 명령을 사용합니다. 이 명령은 IPv4 및 IPv6 주소를 지원합니다. **TCP 상태 우회를** 사용하는 연결에 대한 출력 표시에는 플래그 **b가** 포함됩니다.

문제 해결

오류 메시지

TCP-state-bypass 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
```

보안 어플라이언스에 이미 전달된 유효한 에코 요청 없이 ICMP 에코 응답 또는 보안 어플라이언스에 이미 설정된 TCP, UDP 또는 ICMP 세션과 관련 없는 ICMP 오류 메시지 중 하나인 상태 저장 ICMP 기능에 의해 추가된 보안 검사 때문에 ICMP 패킷이 보안 어플라이언스에 의해 삭제되었습니다.

ASA는 이 기능을 비활성화하는 경우(즉, 연결 테이블의 Type 3에 대한 ICMP 반환 항목 확인)가 불가능하므로 TCP 상태 우회가 활성화된 경우에도 이 로그를 표시합니다. 그러나 TCP 상태 우회 기능이 올바르게 작동합니다.

다음 메시지가 표시되지 않도록 하려면 이 명령을 사용합니다.

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

관련 정보

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