ASA CLI에서 명령 문제 해결

목차

소개

이 문서에서는 ASA CLI에서 문제 해결 명령을 사용하는 방법에 대해 설명합니다.

개요

IPSEC IKEv2 터널을 사용하여 Cisco Umbrella SIG 데이터 센터 및 Secure Web Gateway에 연결하기 위해 Cisco ASA 방화벽을 구축하려면 다음 단계를 사용하십시오.
https://docs.umbrella.com/deployment-umbrella/v1.0.6/docs/add-cisco-asa-tunnel

문제 해결 및 지원 케이스 제기

Cisco ASA 구축에 문제가 있는 경우 umbrella-support@cisco.com으로 지원 케이스를 [제기하십시오](#). 케이스를 제기할 때 다음을 제공하십시오. 문제에 대한 설명, 명령의 출력(여기에 표시) 및 관련 ASDM 스크린샷. Cisco ASA CLI를 통해 명령을 실행하십시오.

- show version(ASA 소프트웨어 버전 표시)
- show tech(ASA 하드웨어 정보 표시)
- show run(실행 중인 컨피그레이션을 표시합니다.)
- Show crypto ikev2 sa(1단계 보안 연결 SA의 상태 표시)
- show crypto ipsec sa detail 2단계 SA의 상태를 표시합니다.

특정 소스 IP 주소 및 포트, 특정 목적지 IP 주소 및 포트를 사용하여 내부 인터페이스에서 패킷을 시뮬레이션하려면 이 명령을 사용합니다. 응답은 패킷이 터널을 통과하는지 여부를 나타냅니다.

이 예에서는 10.0.0.1에서 72.163.4.161로의 HTTP 트래픽을 시뮬레이션합니다. 이는 터널을 통해 통신할 수 있는 호스트입니다. 작동하지 않고 SA가 형성되지 않은 경우 1단계는 집중하기 좋은 단계입니다.

명령 형식:

```
packet-tracer input [src_int] [protocol] [src_addr] [src_port] [dest_addr]  [dest_port] detailed
```

ciscoasa#

```
packet-tracer input inside tcp 10.70.134.11 34500  72.163.4.161 443 detailed
```

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.