ASDM을 사용하는 ASA에서 특정 트래픽에 대한 연결 시간 초과 구성

목차

소개

이 문서에서는 HTTP, HTTPS, FTP 또는 기타 프로토콜과 같은 특정 애플리케이션 프로토콜에 대해 ASA 및 ASDM에서 연결 시간 제한을 구성하는 방법에 대해 설명합니다. Connection timeout(연결 시간 제한)은 리소스를 확보하고 보안을 강화하기 위해 방화벽 또는 네트워크 디바이스가 유휴 연결을 종료한 이후의 비활성 기간입니다. 먼저 첫 번째 질문은 이 구성에 대한 요구 사항은 무엇입니까? 애플리케이션에 적절한 TCP 킵얼라이브 설정이 있는 경우 방화벽에서 연결 시간 제한을 구성하지 않아도 되는 경우가 많습니다. 그러나 애플리케이션이 적절한 keepalive 설정 또는 시간 초과 구성이 부족한 경우, 방화벽에서 연결 시간 초과를 구성하는 것은 리소스 관리, 보안 강화, 네트워크 성능 향상, 규정 준수 보장, 사용자 환경 최적화에 매우 중요합니다.

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- ACL(Access Control List)

- 서비스 정책
- 연결 시간 초과

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- ASA 9.17(1)
- ASDM 7.17(1)

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

기본값

참고: 기본 시간 초과

기본 원시 시간 제한은 30초입니다.

기본 절반이 닫힌 유휴 시간 제한은 10분입니다.

기본 dcd max_retries 값은 5입니다.

기본 dcd retry_interval 값은 15초입니다.

기본 tcp 유휴 시간 제한은 1시간입니다.

기본 udp 유휴 시간 제한은 2분입니다.

기본 icmp 유휴 시간 제한은 2초입니다.

기본 sip 유휴 시간 제한은 30분입니다.

기본 sip_media 유휴 시간 제한은 2분입니다.

기본 esp 및 ha 유휴 시간 제한은 30초입니다.

다른 모든 프로토콜의 경우 기본 유휴 시간 제한은 2분입니다.

시간 초과를 방지하려면 0:0:0을 입력합니다.

연결 시간 초과 구성

ASDM

특정 트래픽에 연결 테이블이 있는 경우 특정 유휴 시간 제한이 적용됩니다. 예를 들어, 이 문서에서는 DNS 트래픽에 대한 연결 시간 제한을 변경합니다.

이 트래픽의 네트워크 다이어그램을 고려하여 특정 트래픽에 대한 연결 시간 제한을 구성하는 옵션

은 다음과 같습니다.

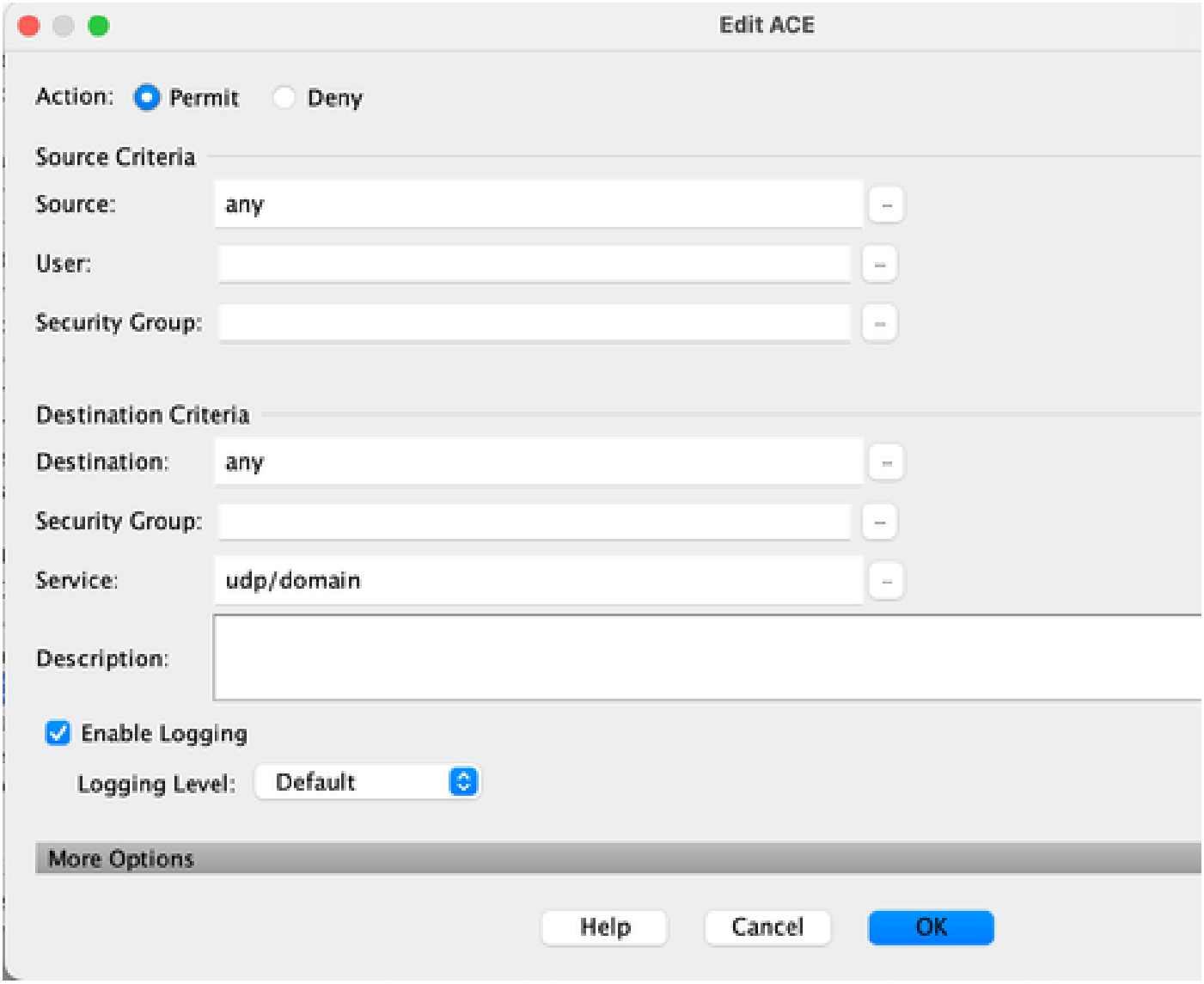
클라이언트 ----- [인터페이스: MNG] 방화벽 [인터페이스: OUT] ----- 서버

인터페이스에 ACL을 할당할 수 있습니다.

1단계: ACL 생성

Source, Destination 또는 Service를

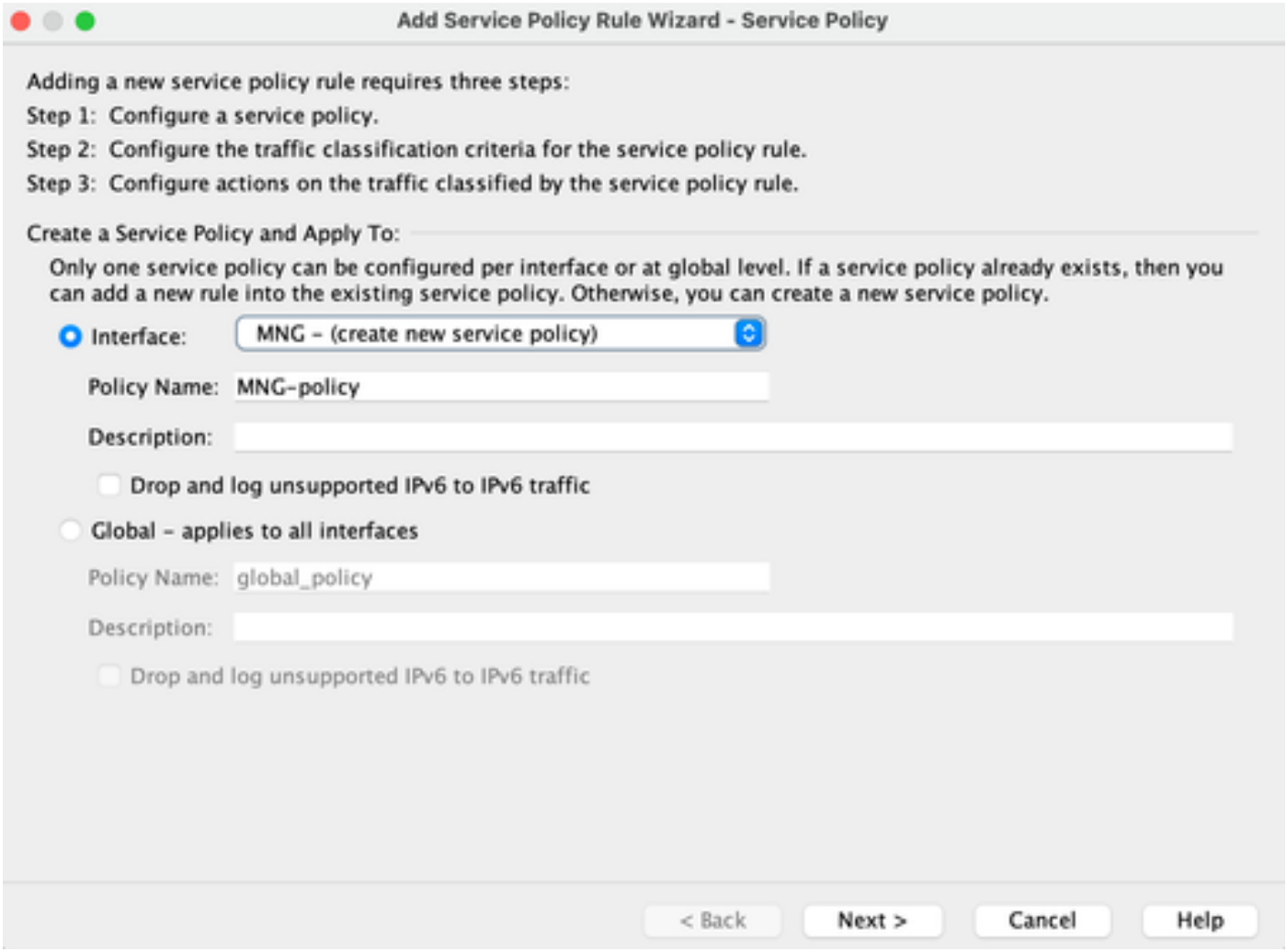
ASDM > Configuration > Firewall > Advanced > ACL Manager



2단계: 서비스 정책 규칙 생성

ACL이 이미 있는 경우 마지막 단계를 건너뛸 수 있으며, 이러한 매개변수 중 하나(소스, 대상 또는 서비스)를 인터페이스에 서비스 정책에 할당할 수 있습니다.

ASDM > Configuration > Firewall > Service Policy rules

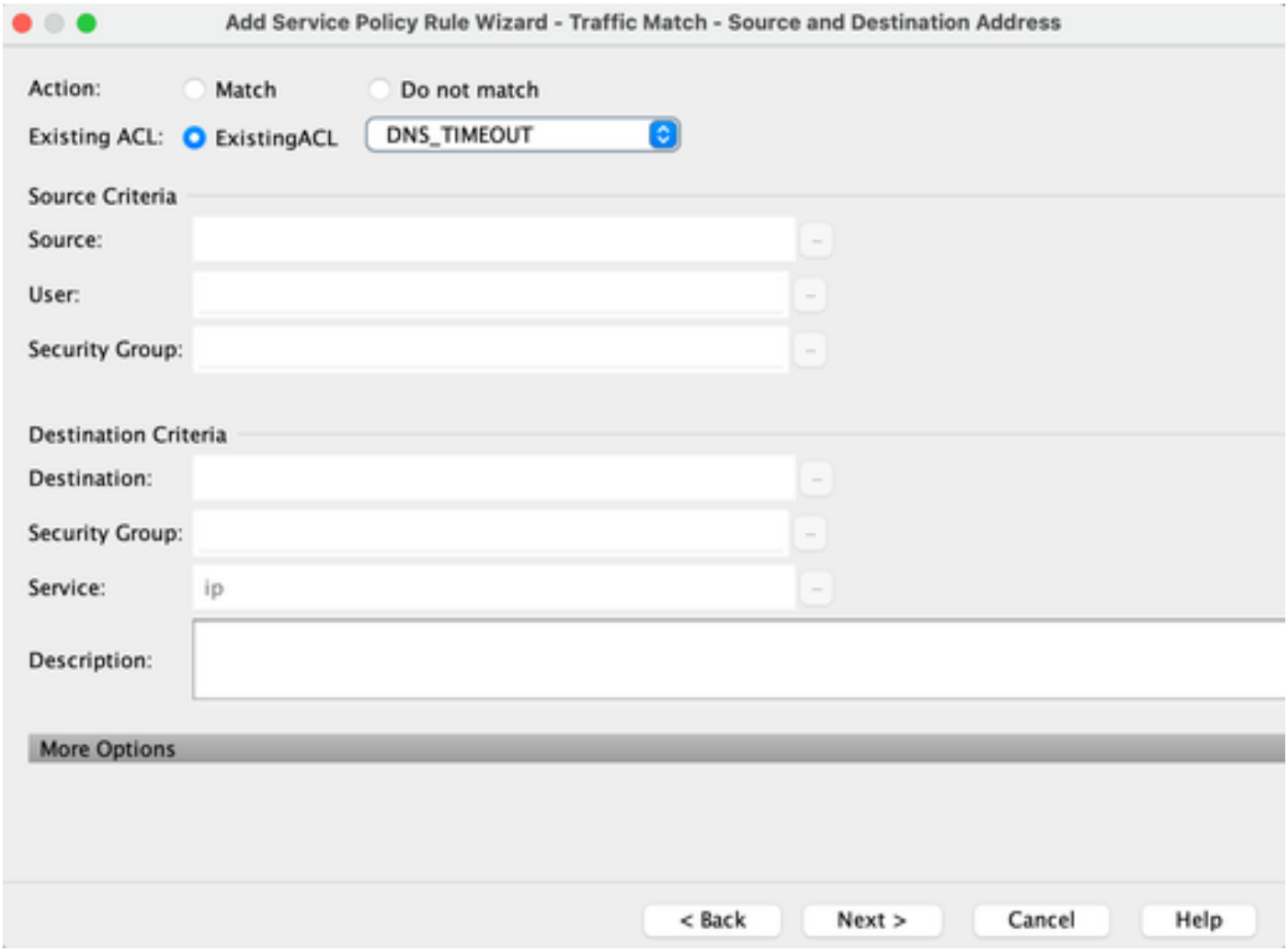


3단계: 트래픽 클래스 생성

Source and Destination IP Address(소스 및 대상 IP 주소)를 선택할 수 있습니다(ACL 사용)

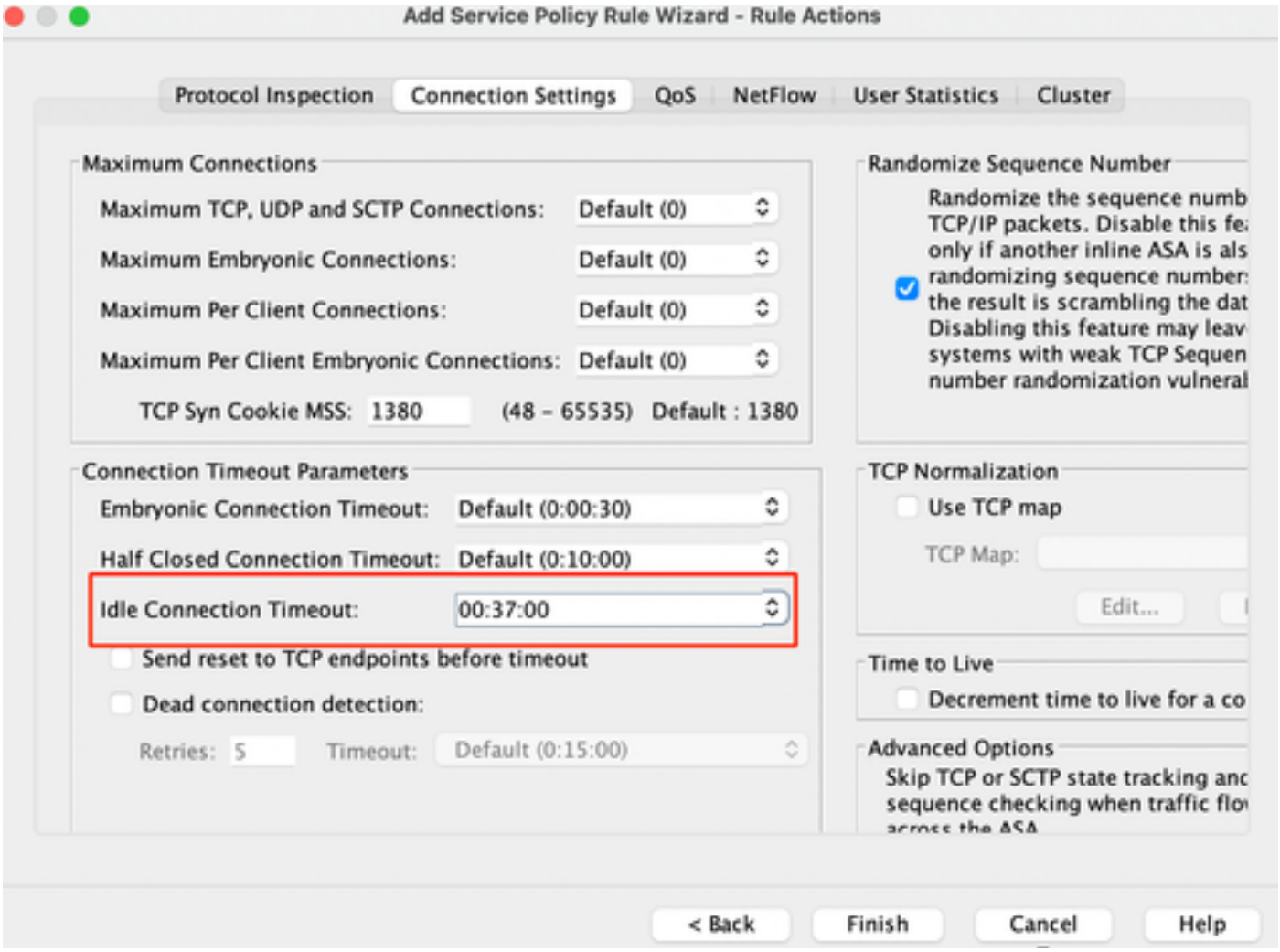
4단계: ACL 할당

이 단계에서는 기존 ACL을 할당하거나 일치 조건(소스, 대상 또는 서비스)을 선택할 수 있습니다



5단계: 유휴 시간 제한 매개변수 구성

유효한 형식 HH:MM:SS에 따라 유휴 시간 제한을 구성합니다.



해당 특정 트래픽에 대한 연결을 지웁니다.

#clear 주소IP 주소 또는 IP 주소 범위를 입력합니다

#clear 프로토콜SCP/TCP/UDP conn만 지우려면 이 키워드를 입력합니다

ASA CLI

CLI를 통해 이 모든 설정을 구성할 수 있습니다.

ACL:

access-list DNS_TIMEOUT extended permit udp any eq domain

클래스 맵:

class-map MNG-class
match access-list DNS_TIMEOUT

정책 맵:

```
정책 맵 MNG-policy
MNG 클래스
연결 시간 제한 유휴 설정 0:37:00

인터페이스에 정책 맵을 적용합니다.

service-policy MNG-policy interface MNG
```

다음을 확인합니다.

팁: 이 명령을 실행하면 DNS 트래픽의 연결 시간 초과를 확인할 수 있습니다.

ASA CLI > enable mode > show conn long

예: show conn long address 192.168.1.1

```
UDP MNG: 192.168.1.1/53 (192.168.1.1/53) OUT: 10.10.10.30/63327 (10.10.10.30/63327), flags - , idle 17s, uptime 17s, timeout 2m0s, bytes 36

UDP MNG: 192.168.1.1/53 (192.168.1.1/53) OUT: 10.10.10.30/62558 (10.10.10.30/62558), flags - , idle 40s, uptime 40s, timeout 2m0s, bytes 36
```

그런 다음 컨피그레이션 후 유휴 시간 제한 컨피그레이션을 확인할 수 있습니다.

예: show conn long address 192.168.1.1

```
UDP MNG: 192.168.1.1/53 (192.168.1.1/53) OUT: 10.10.10.30/63044 (10.10.10.30/63044), flags - , idle 8s, uptime 8s, timeout 37m0s, bytes 37

UDP MNG: 192.168.1.1/53 (192.168.1.1/53) OUT: 10.10.10.30/63589 (10.10.10.30/63589), flags - , idle 5s, uptime 5s, timeout 37m0s, bytes 41
```

참조

연결 설정이란?

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.