ASA 8.3 이상:MPF 컨피그레이션 예를 사용하여 SSH/텔넷/HTTP 연결 시간 초과 설정

목차

소개

이 문서에서는 모든 애플리케이션에 적용되는 것과 달리 SSH/Telnet/HTTP와 같은 특정 애플리케이션에 특정한 시간 제한의 버전 8.3(1) 이상을 지원하는 Cisco ASA(Adaptive Security Appliance)에 대한 샘플 컨피그레이션을 제공합니다.이 컨피그레이션 예에서는 Cisco ASA(Adaptive Security Appliance) 버전 7.0에 도입된 MPF(Modular Policy Framework)를 사용합니다. 자세한 내용은 Modular Policy Framework 사용을 참조하십시오.

이 샘플 컨피그레이션에서는 워크스테이션(10.77.241.129)이 라우터 뒤에 있는 원격 서버(10.1.1.1)에 텔넷/SSH/HTTP를 허용하도록 Cisco ASA가 구성됩니다.텔넷/SSH/HTTP 트래픽에 대한 별도의 연결 시간 초과도 구성됩니다.다른 모든 TCP 트래픽은 계속해서 timeout conn **1:00:00**과 연결된 정상적인 연결 시간 제한 값**을 갖습니다**.

PIX/ASA 7.x 이상/FWSM 참조:버전 8.2 이하의 Cisco ASA에서 동일한 컨피그레이션에 대해 MPF 컨피그레이션 예를 사용하여 SSH/텔넷/HTTP 연결 시간 제한을 설정합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 Cisco ASA Security Appliance Software 버전 8.3(1)과 ASDM(Adaptive Security

Device Manager) 6.3을 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.

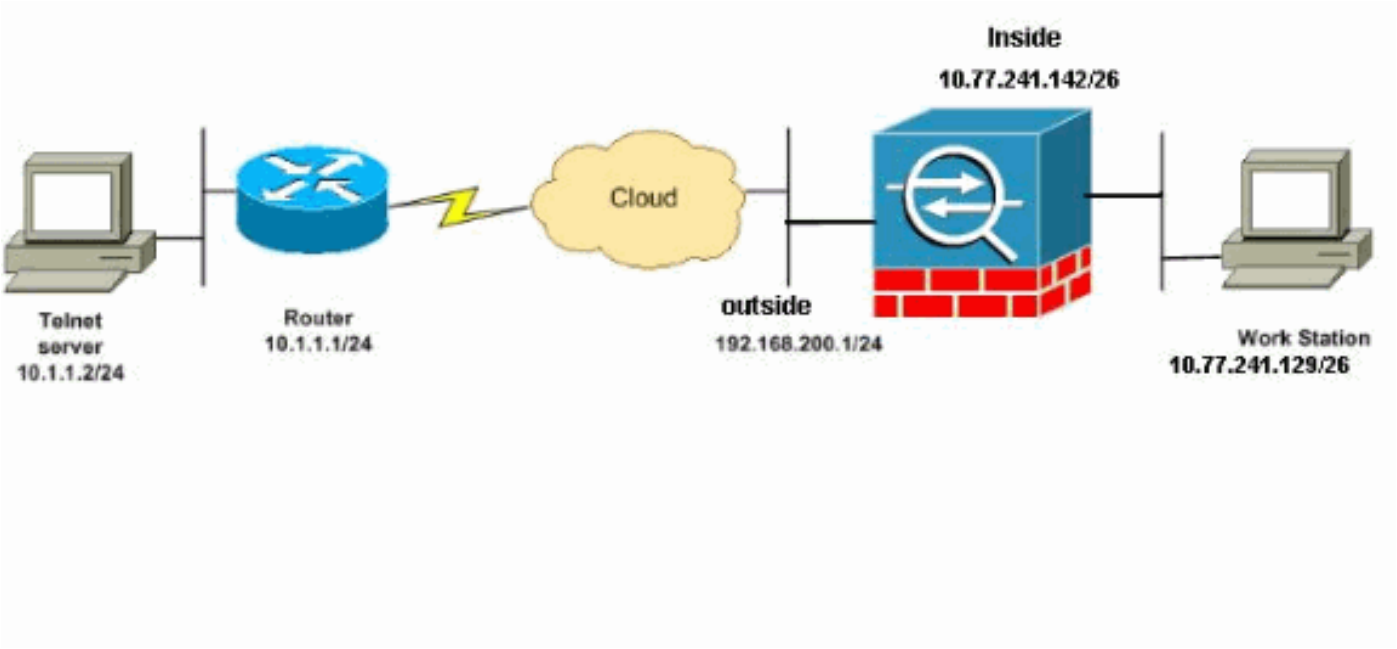
구성

이 섹션에서는 이 문서에 설명된 기능을 구성하는 정보를 제공합니다.

참고: 이 섹션에 사용된 명령에 대한 자세한 내용을 보려면 명령 조회 도구(등록된 고객만 해당)를 사용하십시오.

네트워크 다이어그램

이 문서에서는 다음 네트워크 설정을 사용합니다.



참고: 이 구성에 사용된 IP 주소 지정 체계는 인터넷에서 합법적으로 라우팅할 수 없습니다.실습 환경에서 사용된 RFC 1918 주소입니다.

구성

이 문서에서는 다음 구성을 사용합니다.

- CLI 컨피그레이션
- ASDM 컨피그레이션

참고: 이러한 CLI 및 ASDM 구성은 FWSM(Firewall Service Module)에 적용됩니다.

CLI 컨피그레이션

ASA 8.3(1) 컨피그레이션

```
ASA Version 8.3(1)
!
hostname ASA
domain-name nantes-port.fr
enable password S39lgaewi/JM5WyY level 3 encrypted
enable password 2KFQnbNIdI.2KYOU encrypted
passwd 1mZfSd48bl0UdPgP encrypted
no names

dns-guard
!
interface Ethernet0/0
 nameif outside
 security-level 0
 ip address 192.168.200.1 255.255.255.0
!
interface Ethernet0/1
 nameif inside
 security-level 100
ip address 10.77.241.142 255.255.255.0


boot system disk0:/asa831-k8.bin
ftp mode passive
dns domain-lookup outside

!--- Creates an object called DM_INLINE_TCP_1. This
defines the traffic !--- that has to be matched in the
class map. object-group service DM_INLINE_TCP_1 tcp
 port-object eq www
 port-object eq ssh
 port-object eq telnet

access-list outside_mpc extended permit tcp host
10.77.241.129 any object-group DM_INLINE_TCP_1


pager lines 24
mtu inside 1500
mtu outside 1500
no failover
no asdm history enable
arp timeout 14400
nat (inside) 0 access-list inside_nat0_outbound
access-group 101 in interface outside

route outside 0.0.0.0 0.0.0.0 192.168.200.2 1
timeout xlate 3:00:00

!--- The default connection timeout value of one hour is
applicable to !--- all other TCP applications. timeout
conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp
0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp
0:05:00
timeout mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
```

```
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup
linkdown coldstart
telnet timeout 5
ssh timeout 5
console timeout 0
!

!--- Define the class map Cisco-class in order !--- to
classify Telnet/ssh/http traffic when you use Modular
Policy Framework !--- to configure a security feature.
!--- Assign the parameters to be matched by class map.


class-map Cisco-class
 match access-list outside_mpc

class-map inspection_default
 match default-inspection-traffic
!
!
policy-map global_policy
 class inspection_default
  inspect dns maximum-length 512
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp

!--- Use the pre-defined class map Cisco-class in the
policy map.


policy-map Cisco-policy

!--- Set the connection timeout under the class mode
where !--- the idle TCP (Telnet/ssh/http) connection is
disconnected. !--- There is a set value of ten minutes
in this example. !--- The minimum possible value is five
minutes. class Cisco-class
  set connection timeout idle 0:10:00 reset
!
!
service-policy global_policy global

!--- Apply the policy-map Cisco-policy on the interface.
!--- You can apply the service-policy command to any
interface that !--- can be defined by the nameif
command.

service-policy Cisco-policy interface outside
end
```

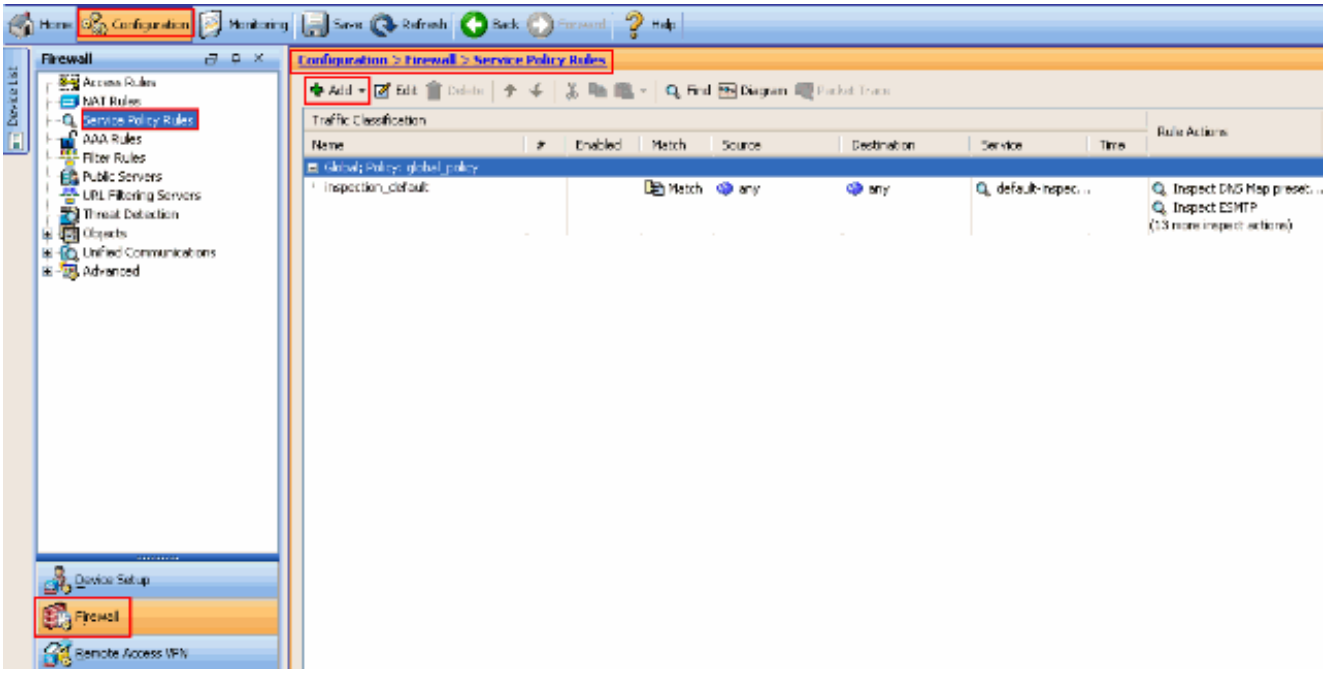
ASDM 컨피그레이션

표시된 대로 ASDM을 사용하여 텔넷, SSH 및 HTTP 트래픽에 대한 TCP 연결 시간 제한을 설정하려면 다음 단계를 완료합니다.

참고: ASDM을 통해 PIX/ASA에 액세스하려면 ASDM에 대한 HTTPS 액세스 허용을 참조하십시오.

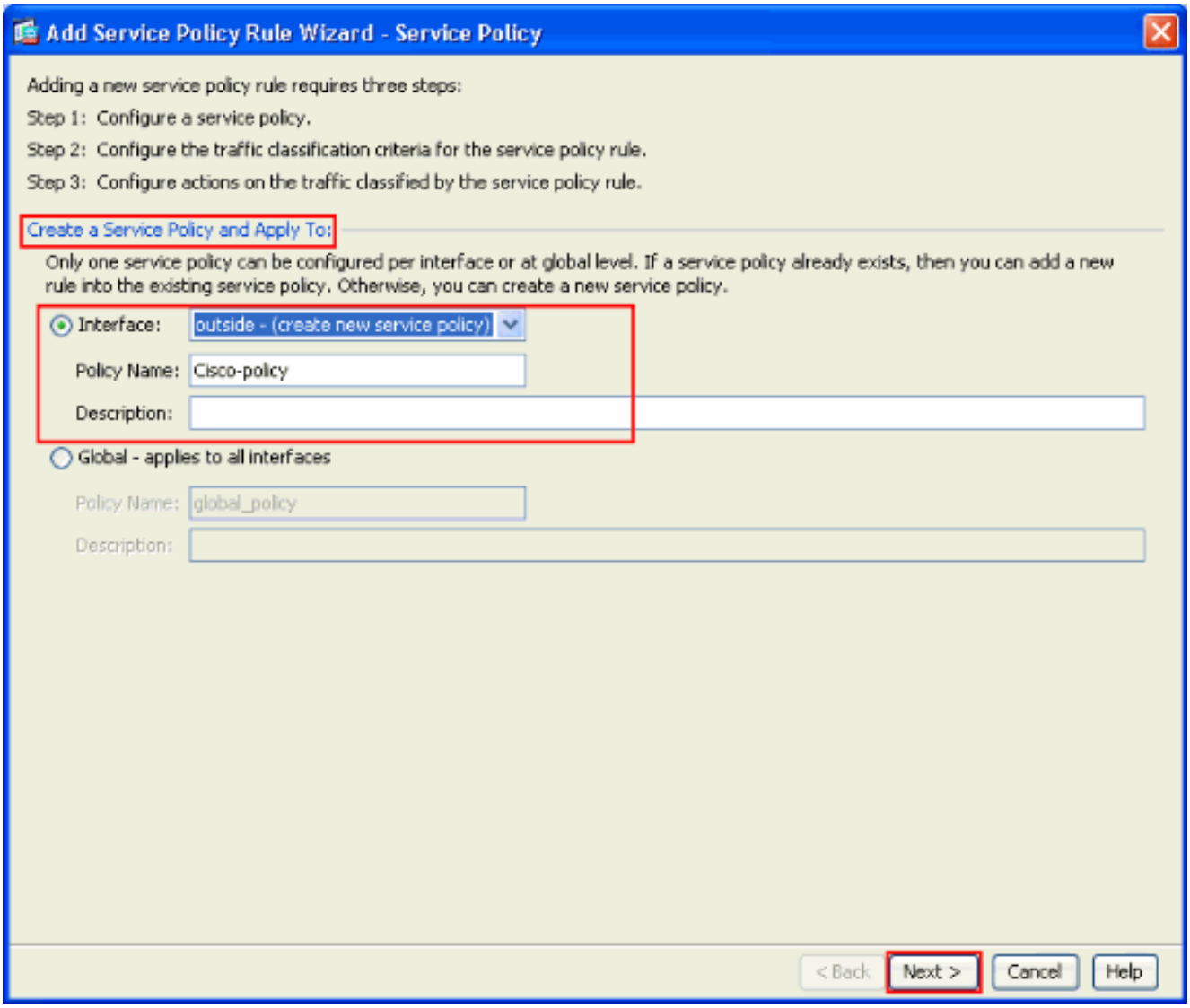
1. Configuration(**컨피그레이션) > Firewall(방화벽) > Service Policy Rules(서비스 정책 규칙)**를 선택하고 **Add(추가)**를 클릭하여 서비스 정책 규칙을 그림과 같이 구성합니다

.

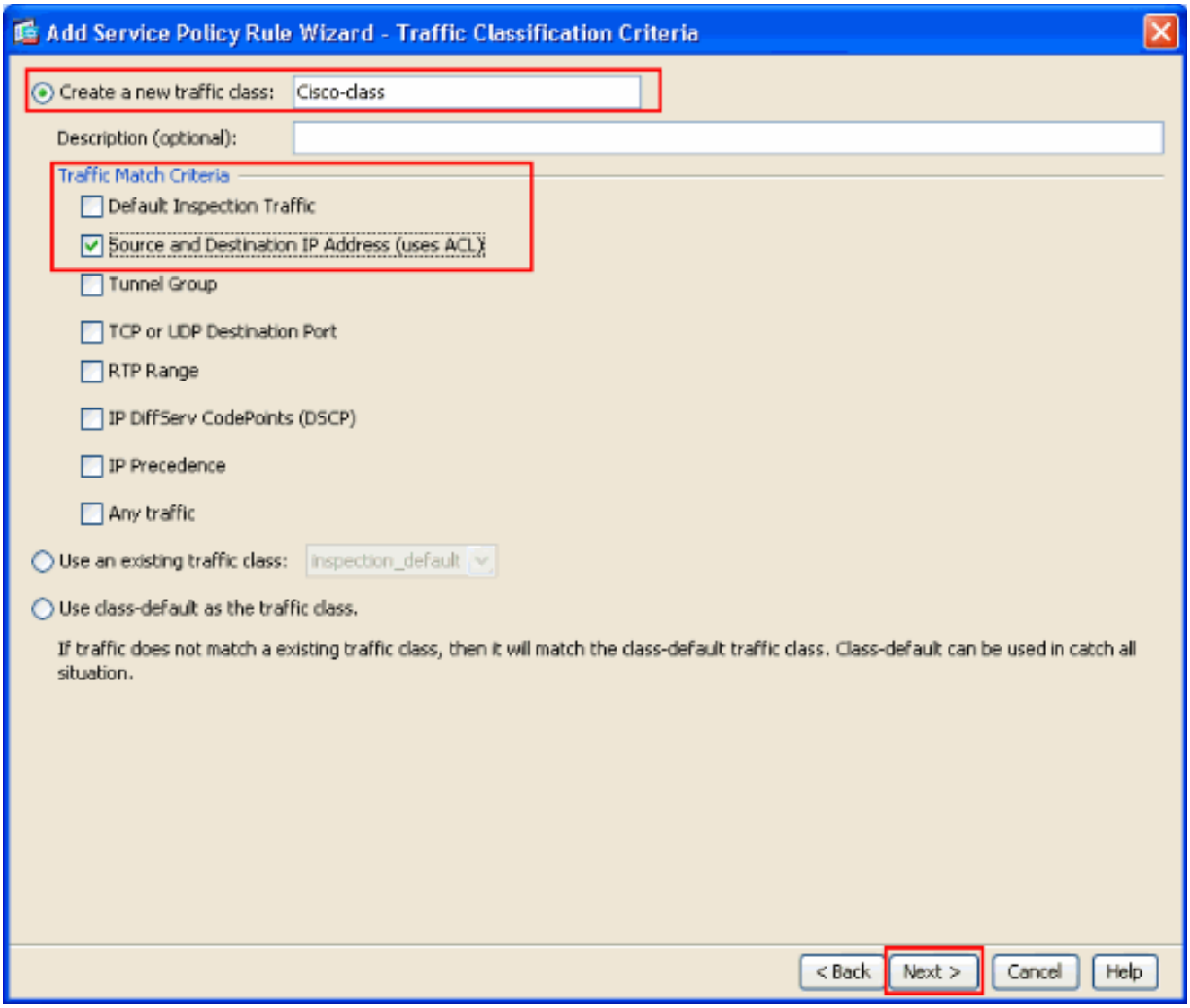


2. Add **Service Policy Rule Wizard - Service Policy(서비스 정책 추가 마법사 - 서비스 정책)** 창에서 Create a Service Policy and Apply To(**서비스 정책 생성 및 적용 대상)** 섹션의 **Interface(인터페이스) 옆의** 라디오 버튼을 선택합니다.이제 드롭다운 목록에서 원하는 인터페이스를 선택하고 **정책 이름**을 **입력합니다**.이 예에서 사용되는 정책 이름은 **Cisco-policy입니다**.그런 다음 **다음**을 클릭합니다

.

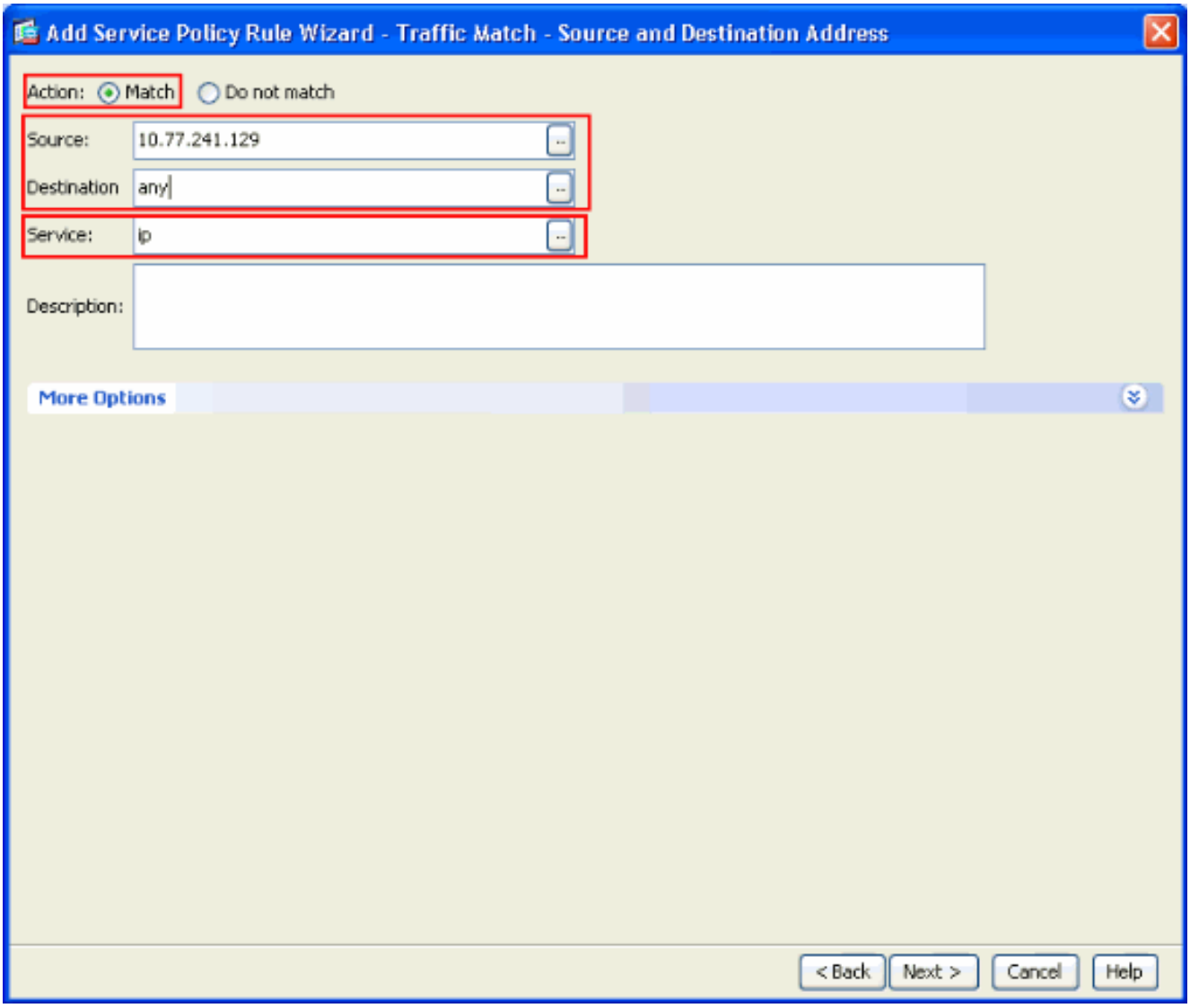


3. 클래스 맵 이름을 **Cisco-class**로 만들고 Traffic Match Criteria(트래픽 일치 기준)에서 Source and Destination IP address (uses **ACL)** 확인란을 선택합니다.그런 다음 **다음**을 클릭합니다 .

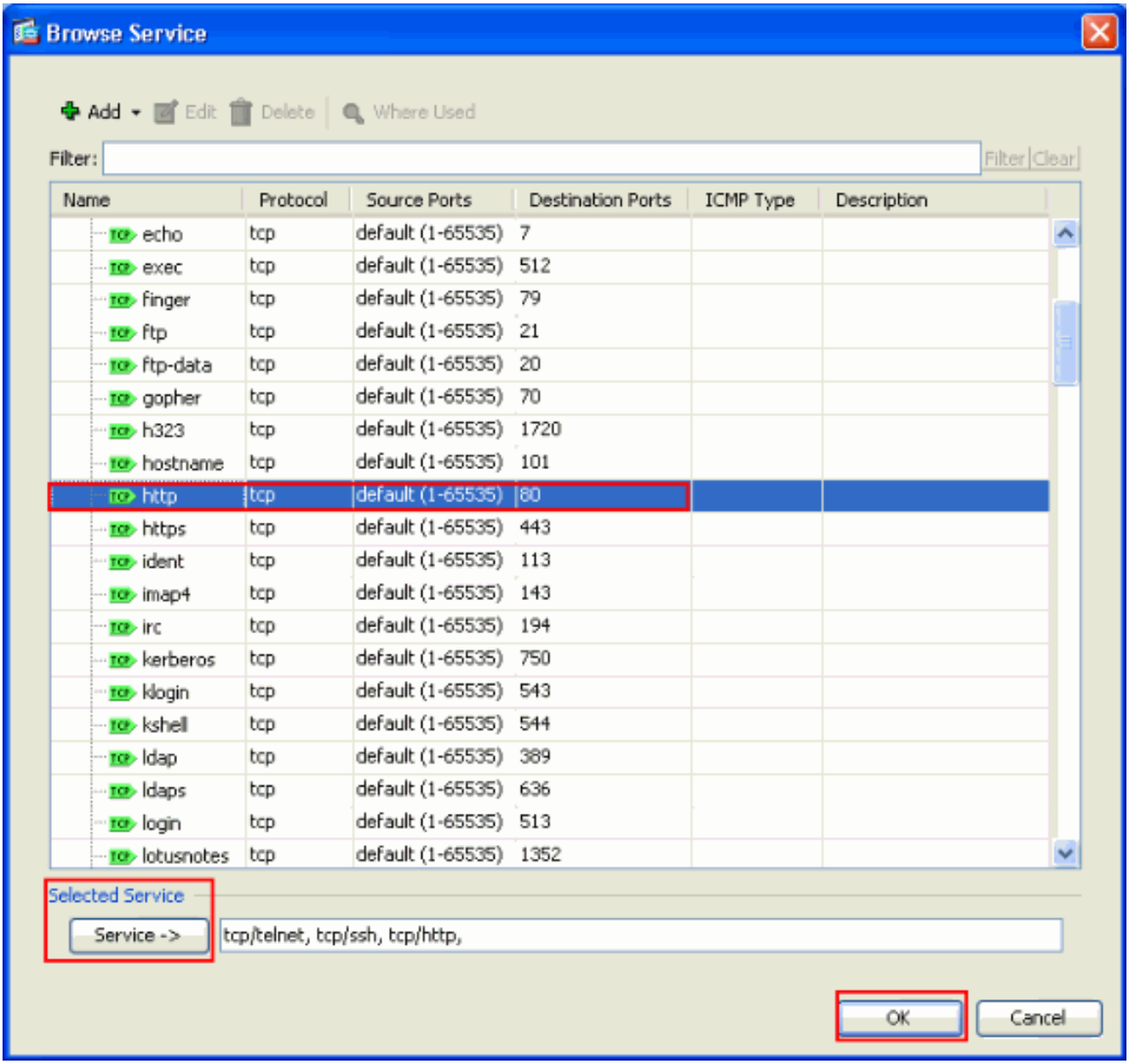


4. Add **Service Policy Rule Wizard - Traffic Match - Source and Destination Address(서비스 정책 규칙 추가 마법사 - 트래픽 일치 - 소스 및 대상 주소)** 창에서 Match(**일치**) 옆의 라디오 버튼을 선택한 다음 표시된 대로 소스 및 대상 주소를 제공합니다.**서비스** 옆의 드롭다운 버튼을 클릭하여 필요한 서비스를 선택합니다

.

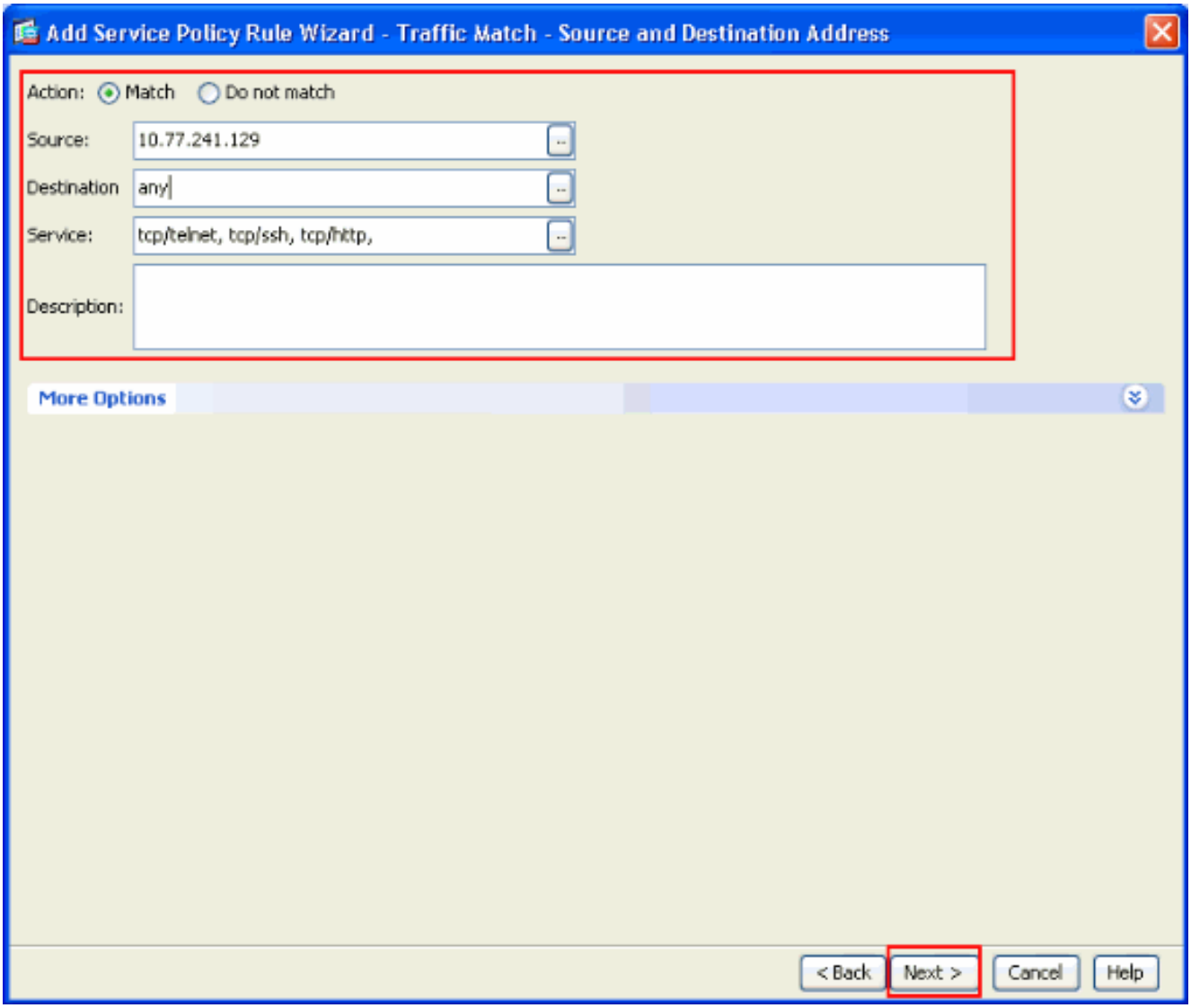


5. **텔넷**, **ssh** 및 **http**와 같은 필수 서비스를 **선택합니다**.그런 다음 **확인**을 클릭합니다
.

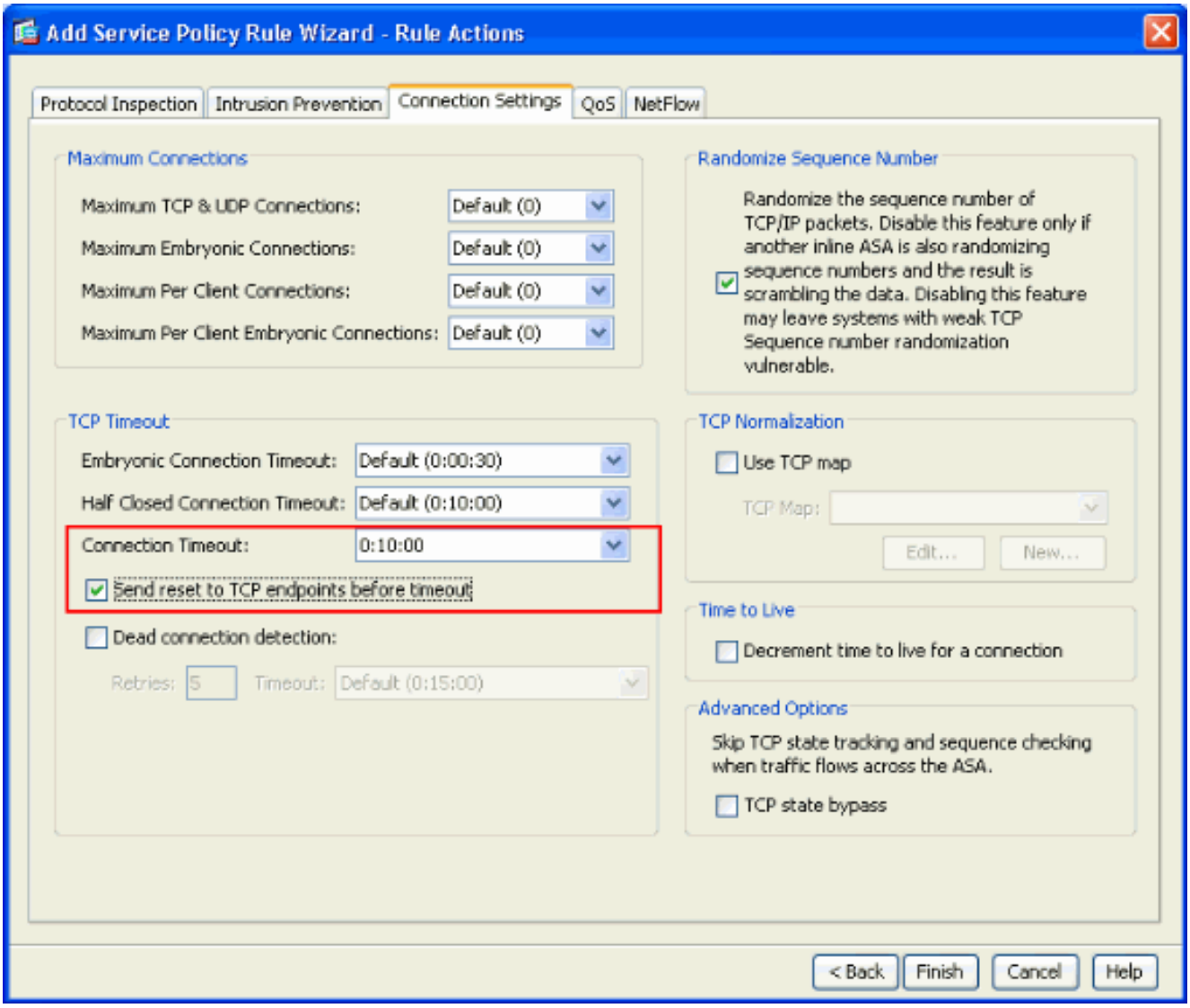


6. 시간 제한을 구성합니다.Next(다음)를 클릭합니다

.

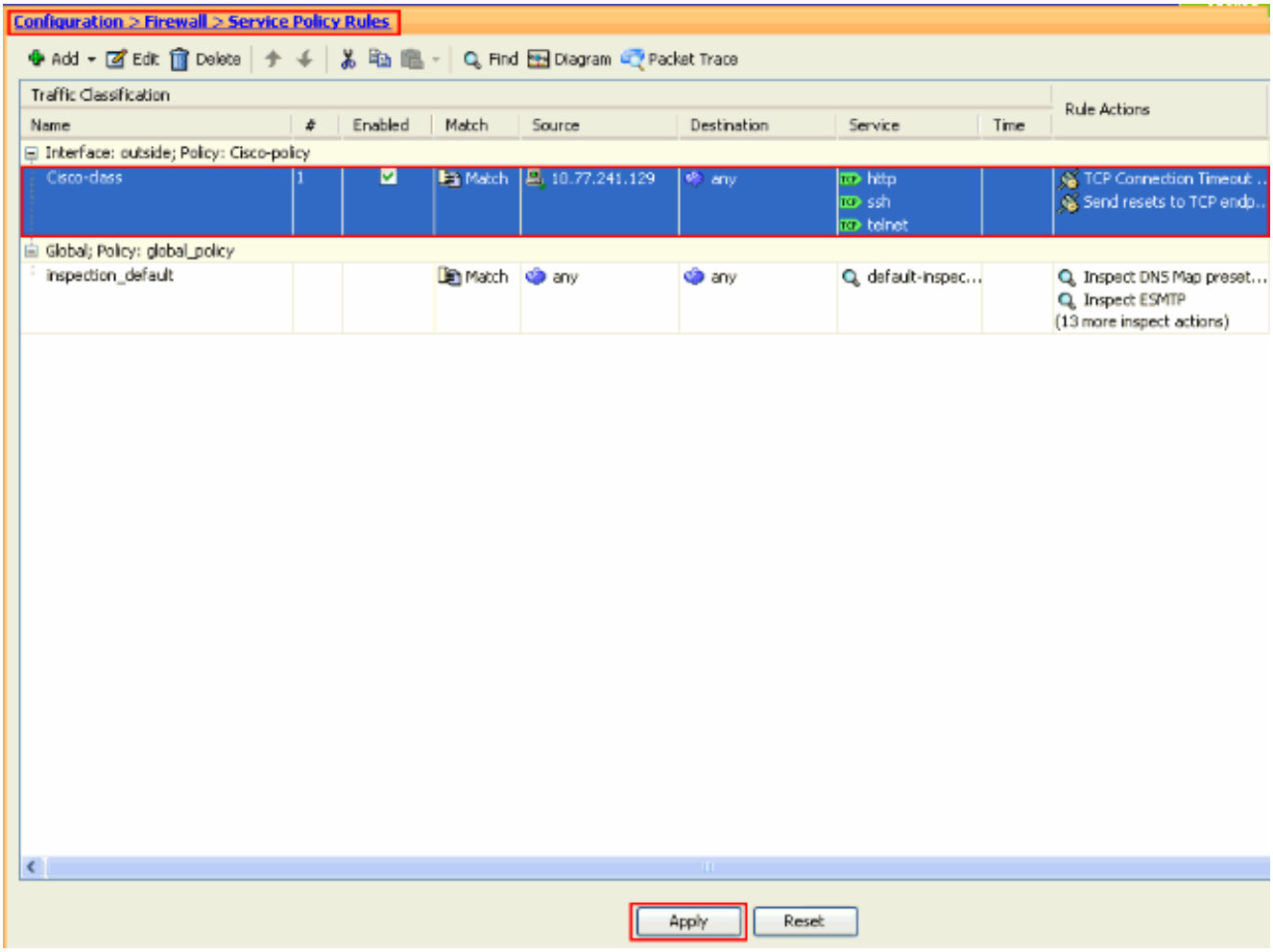


7. TCP 연결 시간 제한을 10분으로 설정하려면 Connection Settings(연결 설정)를 선택합니다.또한 Send reset to **TCP endpoints before timeout** 확인란**을** 선택합니다.**마침**을 **클릭합니다**
.



8. Apply(**적용**)를 클릭하여 컨피그레이션을 보안 어플라이언스에 적용합니다.이렇게 하면 컨피그레이션이 완료됩니다

.



ebryonic 시간 초과

원시 연결은 절반이 열려 있거나, 예를 들어 3방향 핸드셰이크가 완료되지 않은 연결입니다.ASA에서 SYN 시간 초과로 정의됩니다.기본적으로 ASA의 SYN 시간 제한은 30초입니다.다음은 원시 시간 제한을 구성하는 방법입니다.

```
access-list emb_map extended permit tcp any any

class-map emb_map
match access-list emb_map

policy-map global_policy
class emb_map
set connection timeout embryonic 0:02:00

service-policy global_policy global
```

문제 해결

연결 시간 제한이 MPF에서 작동하지 않는 경우 TCP 시작 연결을 확인합니다.이 문제는 소스 및 대상 IP 주소의 취소이거나, 액세스 목록의 잘못 구성된 IP 주소가 MPF에서 일치하지 않아 새 시간 초과 값을 설정하거나 애플리케이션의 기본 시간 제한을 변경할 수 있습니다.MPF로 연결 시간 제한을 설정하려면 연결 시작에 따라 액세스 목록 항목(소스 및 대상)을 생성합니다.

관련 정보

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