

# Auth-proxy Authentication Inbound(Cisco IOS Firewall - 라우터/스위치 및 NAT) 컨피그레이션 예

## 목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[표기 규칙](#)

[구성](#)

[네트워크 다이어그램](#)

[구성](#)

[다음을 확인합니다.](#)

[문제 해결](#)

[관련 정보](#)

## 소개

이 샘플 컨피그레이션은 처음에는 인증 프록시를 사용하여 브라우저 인증이 수행될 때까지 외부 호스트에서 내부 네트워크의 모든 디바이스로 이동하는 트래픽을 차단합니다. 권한 부여 후 서버에서 전달된 액세스 목록(`permit tcp|ip|icmp any any`)은 외부 PC에서 내부 네트워크로 일시적으로 액세스를 허용하는 액세스 목록 116에 동적 항목을 추가합니다.

**참고:** 이 문서에 사용된 AAA 컨피그레이션은 Cisco IOS® 소프트웨어를 실행하는 Catalyst 스위치에도 적용됩니다.

## 사전 요구 사항

### 요구 사항

이 문서에 대한 특정 요건이 없습니다.

### 사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco IOS Software 릴리스 12.2.23
- Cisco 3640 라우터

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바

이스는 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 규칙](#)을 참조하십시오.

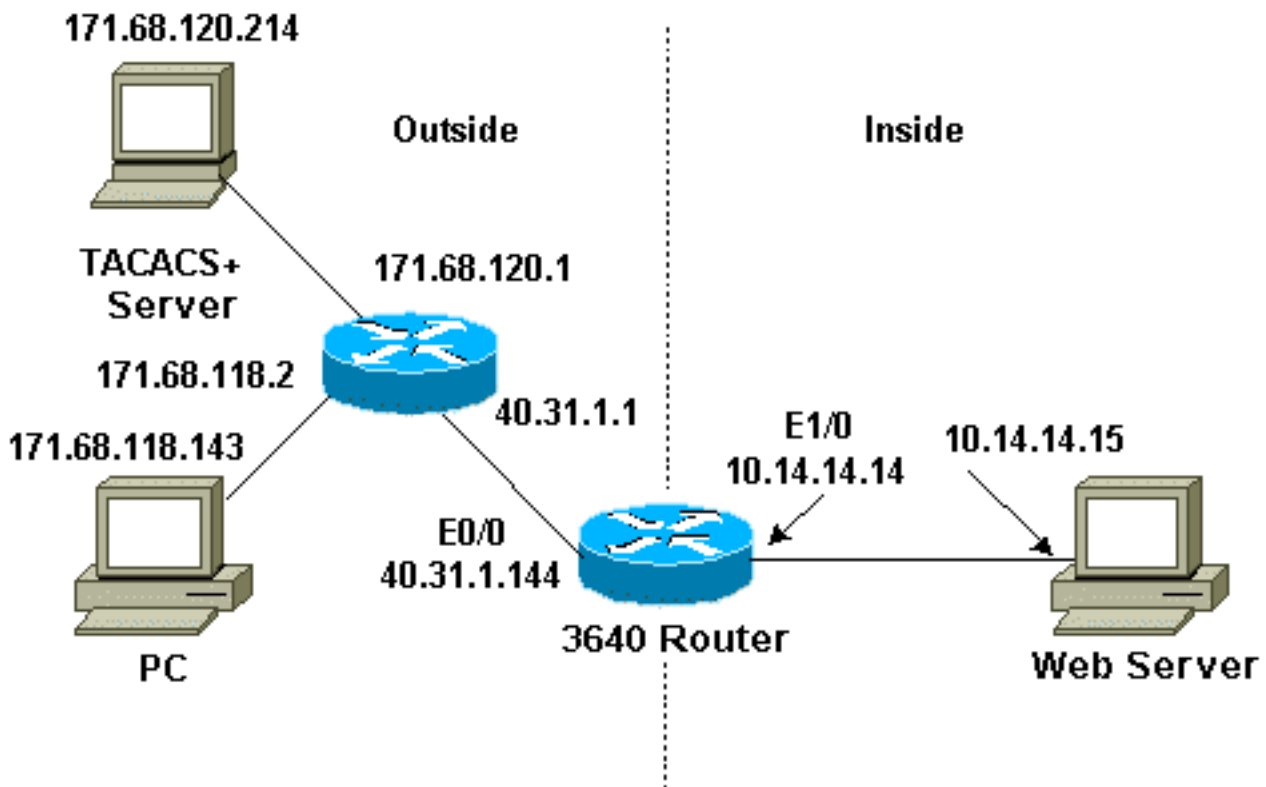
## 구성

이 섹션에는 이 문서에서 설명하는 기능을 구성하기 위한 정보가 표시됩니다.

**참고:** [명령 조회 도구](#)([등록된](#) 고객만 해당)를 사용하여 이 섹션에 사용된 명령에 대한 자세한 내용을 확인하십시오.

## 네트워크 다이어그램

이 문서에서는 다음 네트워크 설정을 사용합니다.



## 구성

이 문서에서는 다음 구성을 사용합니다.

- Cisco 3640 Router

Cisco 3640 Router
Current configuration: ! version 12.2

```
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname sec-3640
!
aaa new-model
aaa group server tacacs+ RTP
  server 171.68.120.214
!
aaa authentication login default group RTP none
aaa authorization exec default group RTP none
aaa authorization auth-proxy default group RTP
enable secret 5 $1$pqRI$3TDNFT9FdYT8Sd/q3S0VU1
enable password ww
!
ip subnet-zero
!
ip inspect name myfw cuseeme timeout 3600
ip inspect name myfw ftp timeout 3600
ip inspect name myfw http timeout 3600
ip inspect name myfw rcmd timeout 3600
ip inspect name myfw realaudio timeout 3600
ip inspect name myfw smtp timeout 3600
ip inspect name myfw sqlnet timeout 3600
ip inspect name myfw streamworks timeout 3600
ip inspect name myfw tftp timeout 30
ip inspect name myfw udp timeout 15
ip inspect name myfw tcp timeout 3600
ip inspect name myfw vdolive

ip auth-proxy auth-proxy-banner
ip auth-proxy auth-cache-time 10
ip auth-proxy name list_a http
ip audit notify log
ip audit po max-events 100
!
interface Ethernet0/0
  ip address 40.31.1.144 255.255.255.0

ip access-group 116 in
  ip nat outside

ip auth-proxy list_a
  no ip route-cache
  no ip mroute-cache
  speed auto
  half-duplex
  no mop enabled
!
interface Ethernet1/0
  ip address 10.14.14.14 255.255.255.0
  ip nat inside
  ip inspect myfw in
  speed auto
  half-duplex
!
!--- Interfaces deleted. ! nat pool outsidepool
40.31.1.50 40.31.1.60 netmask 255.255.255.0 ip nat
inside source list 1 pool outsidepool ip nat inside
source static 10.14.14.15 40.31.1.77 ip classless ip
route 0.0.0.0 0.0.0.0 40.31.1.1 ip route 171.68.118.0
```

```
255.255.255.0 40.31.1.1 ip route 171.68.120.0
255.255.255.0 40.31.1.1 no ip http server !
access-list 116 permit tcp host 171.68.118.143 host
40.31.1.144 eq www
access-list 116 deny tcp host 171.68.118.143 any
access-list 116 deny udp host 171.68.118.143 any
access-list 116 deny icmp host 171.68.118.143 any
access-list 116 permit icmp any any
access-list 116 permit tcp any any
access-list 116 permit udp any any
dialer-list 1 protocol ip permit
dialer-list 1 protocol ipx permit
!
tacacs-server host 171.68.120.214
tacacs-server key cisco
!
line con 0
 transport input none
line aux 0
line vty 0 4
 password ww
!
end
```

## 다음을 확인합니다.

[debug 명령을 실행하기 전에 디버그 명령에 대한 중요 정보](#)를 참조하십시오.

명령 및 문제 해결 정보는 [인증 프록시 문제 해결](#)을 참조하십시오.

## 문제 해결

현재 이 컨피그레이션에 사용할 수 있는 특정 문제 해결 정보가 없습니다.

## 관련 정보

- [Cisco IOS Firewall](#)
- [보안 및 VPN 기술 지원](#)
- [기술 지원 및 문서 - Cisco Systems](#)