

인증 프록시 인증 인바운드 - Cisco IOS 방화벽 또는 NAT 컨피그레이션 없음

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 인증 프록시를 사용하여 브라우저 인증을 수행할 때까지 외부 네트워크의 호스트 디바이스(11.11.11.12)에서 내부 네트워크의 모든 디바이스로 트래픽을 초기에 차단합니다. 서버에서 전달된 액세스 목록(**permit tcp|ip|icmp any any**)은 호스트 디바이스에서 내부 네트워크로 일시적으로 액세스를 허용하는 액세스 목록 115에 동적 엔트리를 추가합니다.

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® 소프트웨어 릴리스 12.0.7.T
- Cisco 3640 라우터

참고: **ip auth-proxy** 명령은 Cisco IOS Software 릴리스 12.0.5.T에서 도입되었습니다. 이 구성은 Cisco IOS Software 릴리스 12.0.7.T에서 테스트되었습니다.

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 규칙](#)을 참조하십시오.

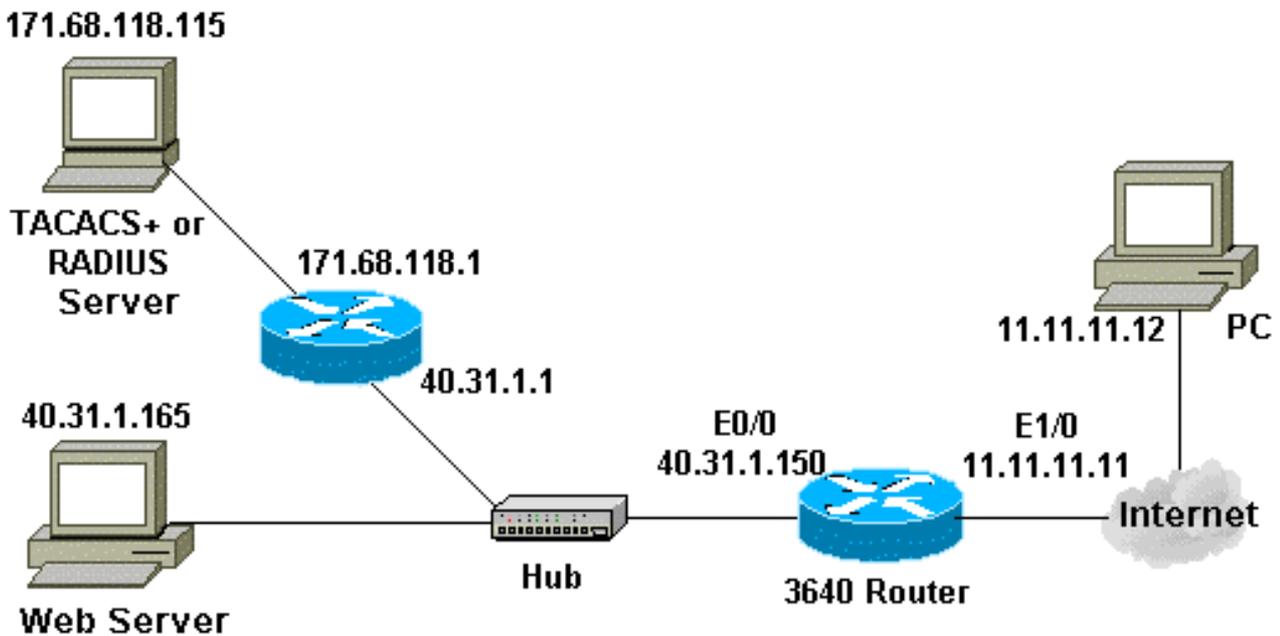
구성

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.

3640 라우터

```
Current configuration:
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname security-3640
!
!---- Turn on authentication. aaa new-model
!---- Define the server group and servers for TACACS+ or
RADIUS. aaa group server tacacs+|radius RTP
server 171.68.118.115
```

```
!  
!--- Define what you need to authenticate. aaa  
authentication login default group RTP none  
aaa authorization exec default group RTP none  
aaa authorization auth-proxy default group RTP  
enable secret 5 $1$H9zZ$z9bu5HMy4NTtjsvIhltGT0  
enable password ww  
!  
ip subnet-zero  
!  
!--- You want the router name to appear as banner. ip  
auth-proxy auth-proxy-banner  
!--- You want the access-list entries to timeout after  
10 minutes. ip auth-proxy auth-cache-time 10  
!--- You define the list-name to be associated with the  
interface. ip auth-proxy name list_a http  
ip audit notify log  
ip audit po max-events 100  
cns event-service server  
!  
process-max-time 200  
!  
interface FastEthernet0/0  
 ip address 40.31.1.150 255.255.255.0  
 no ip directed-broadcast  
 no mop enabled  
!  
interface FastEthernet1/0  
 ip address 11.11.11.11 255.255.255.0  
!--- Apply the access-list to the interface. ip access-  
group 115 in  
 no ip directed-broadcast  
!--- Apply the auth-proxy list-name. ip auth-proxy  
list_a  
!  
ip classless  
ip route 171.68.118.0 255.255.255.0 40.31.1.1  
!--- Turn on the http server and authentication. ip http  
server  
ip http authentication aaa  
!  
!--- This is our access-list for auth-proxy testing - !-  
-- it denies only one host, 11.11.11.12, access - to  
minimize disruption !--- to the network during testing.  
access-list 115 permit tcp host 11.11.11.12 host  
11.11.11.11 eq www  
access-list 115 deny icmp host 11.11.11.12 any  
access-list 115 deny tcp host 11.11.11.12 any  
access-list 115 deny udp host 11.11.11.12 any  
access-list 115 permit udp any any  
access-list 115 permit tcp any any  
access-list 115 permit icmp any any  
dialer-list 1 protocol ip permit  
dialer-list 1 protocol ipx permit  
!  
!--- Define the server(s). tacacs-server host  
171.68.118.115  
tacacs-server key cisco  
radius-server host 171.68.118.115  
radius-server key cisco  
!  
line con 0  
 transport input none  
line aux 0
```

```
line vty 0 4
 password ww
 !
 !
end
```

다음을 확인합니다.

현재 이 구성에 대해 사용 가능한 확인 절차가 없습니다.

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

이러한 명령과 다른 문제 해결 정보는 [인증 프록시 문제 해결](#)을 참조하십시오.

참고: 디버그 명령을 [실행하기 전에 디버그 명령](#)에 대한 중요 정보를 참조하십시오.

관련 정보

- [IOS 방화벽 지원 페이지](#)
- [TACACS/TACACS+ 지원 페이지](#)
- [IOS 설명서의 TACACS+](#)
- [RADIUS 지원 페이지](#)
- [RFC\(Request for Comments\)](#)
- [기술 지원 및 문서 - Cisco Systems](#)