

# 认证代理认证入局-没有Cisco IOS防火墙或NAT配置

## 目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[规则](#)

[配置](#)

[网络图](#)

[配置](#)

[验证](#)

[故障排除](#)

[相关信息](#)

## 简介

在使用认证代理执行浏览器身份验证之前，此配置示例最初会阻塞从外部网络上的主机设备（地址为 11.11.11.12）到内部网络上的所有设备的流量。从服务器通过的下来访问列表(`permit tcp|ip|icmp any any`) 会将动态条目后授权添加到暂时允许主机设备访问内部网络的访问列表 115 中。

## 先决条件

### 要求

本文档没有任何特定的要求。

### 使用的组件

本文档中的信息基于以下软件和硬件版本：

- Cisco IOS®软件版本12.0.7.T
- Cisco 3640路由器

**注意：** `ip auth-proxy`指令在Cisco IOS软件版本12.0.5.T.被引入此配置测试了Cisco IOS软件版本12.0.7.T。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

## 规则

有关文档规则的详细信息，请参阅 [Cisco 技术提示规则](#)。

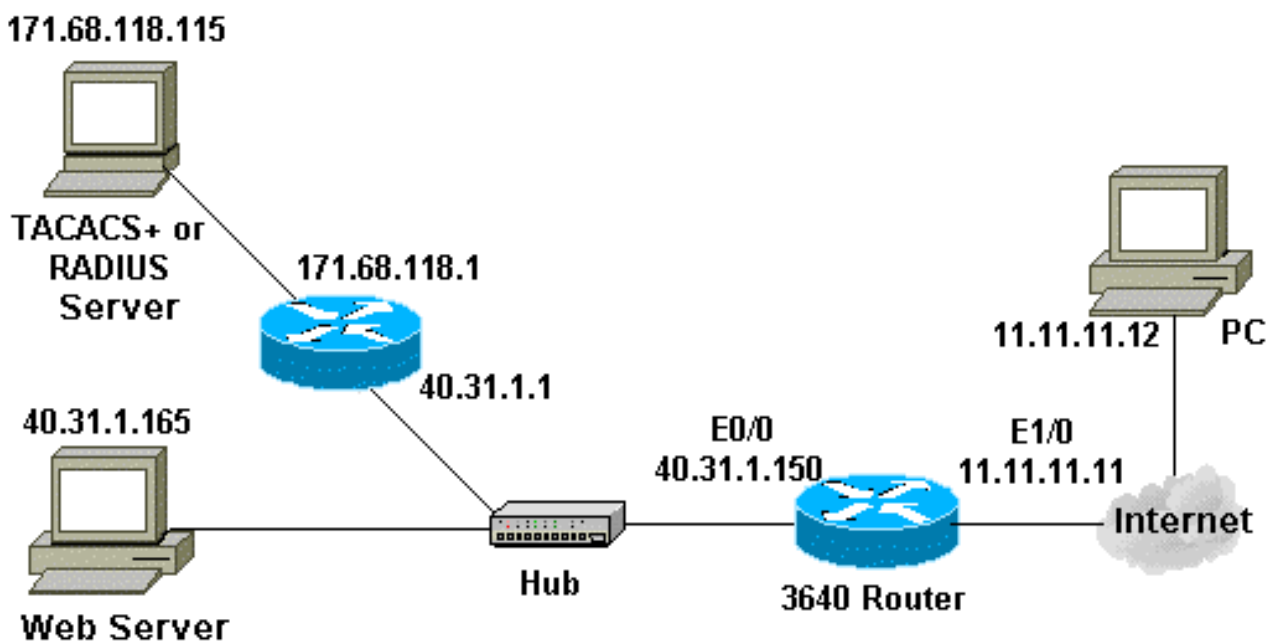
## 配置

本部分提供有关如何配置本文档所述功能的信息。

**注意：** 使用 [命令查找工具](#) ( [仅限注册用户](#) ) 可获取有关本部分所使用命令的详细信息。

## 网络图

本文档使用以下网络设置：



## 配置

本文档使用以下配置：

### 3640路由器

```
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$z9bu5HMy4NTtjstvIhltGT0 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
```

## 验证

当前没有可用于此配置的验证过程。

## 故障排除

本部分提供了可用于对配置进行故障排除的信息。

对于这些指令和其他故障排除信息，请参见[排错认证代理](#)。

**注意：**发出 `debug` 命令之前，请参阅[有关 Debug 命令的重要信息](#)。

## 相关信息

- [IOS防火墙支持页面](#)
- [TACACS/TACACS+支持页面](#)
- [IOS 文档中的 TACACS+](#)
- [RADIUS 支持页](#)
- [请求注解 \(RFC\)](#)
- [技术支持和文档 - Cisco Systems](#)