

# 认证代理认证出站(Cisco IOS防火墙和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内部网络上的主机设备（地址为 10.31.1.47）到 Internet 上的所有设备的流量。从服务器传递的访问列表(`permit tcp|ip|icmp any any`)将授权后的动态条目添加到访问列表116，该列表暂时允许从该设备访问Internet。

## 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 12.2.23
- Cisco 3640 路由器

**注意：**在Cisco IOS软件版本12.0.5.T中引入了ip auth-proxy命令。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

有关文档约定的更多信息，请参考 [Cisco 技术提示约定](#)。

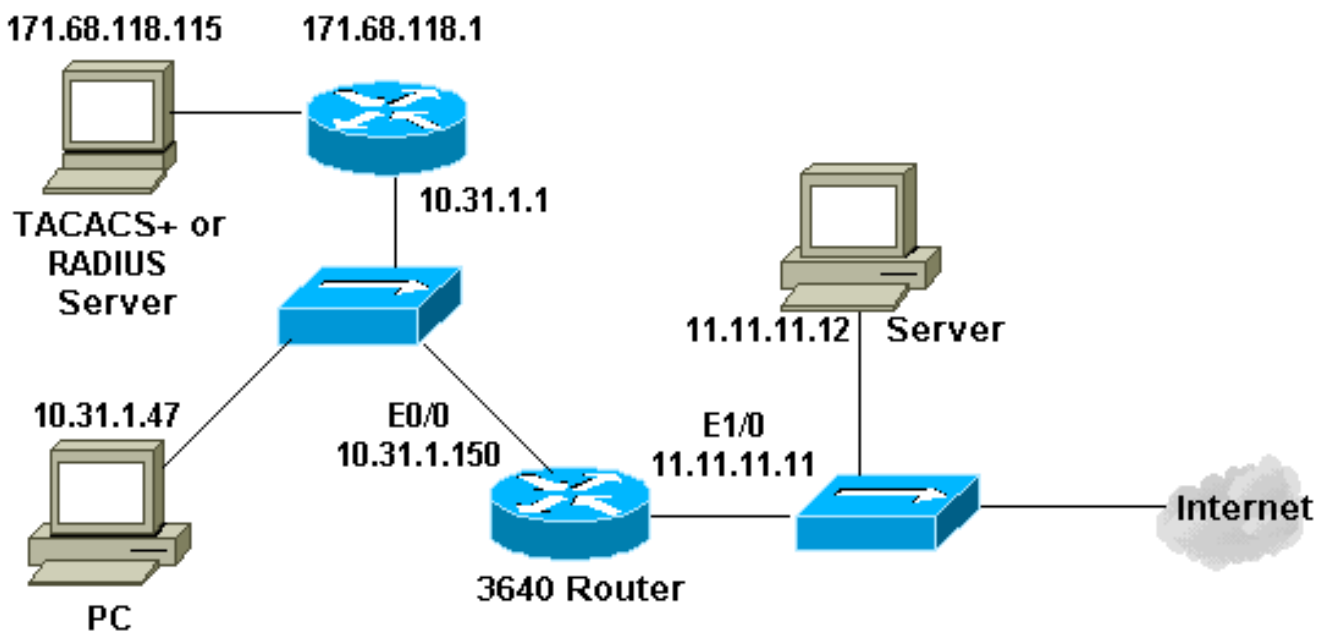
## 配置

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](#)(仅限注册客户)可获取有关本节中使用的命令的详细信息。

## 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 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname security-3640
!
aaa new-model
aaa group server tacacs+ RTP
  server 171.68.118.115
!
aaa authentication login default local group RTP none
aaa authorization exec default group RTP none
aaa authorization auth-proxy default group RTP
enable secret 5 $1$vCfr$rkuU6HLmpbNgLTg/JNM6e1
```

```
enable password ww
!
username john password 0 doe
!
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
!
process-max-time 200
!
interface Ethernet0/0
 ip address 10.31.1.150 255.255.255.0
 ip access-group 116 in
 ip nat inside
 ip inspect myfw in
 ip auth-proxy list_a
 no ip route-cache
 no ip mroute-cache
!
interface Ethernet1/0
 ip address 11.11.11.11 255.255.255.0
 ip access-group 101 in
 ip nat outside
!
ip nat pool outsidepool 11.11.11.20 11.11.11.30 netmask
255.255.255.0
ip nat inside source list 1 pool outsidepool
ip classless
ip route 0.0.0.0 0.0.0.0 11.11.11.1
ip route 171.68.118.0 255.255.255.0 10.31.1.1
ip http server
ip http authentication aaa
!
access-list 1 permit 10.31.1.0 0.0.0.255
access-list 101 deny ip 10.31.1.0 0.0.0.255 any
access-list 101 deny ip 127.0.0.0 0.255.255.255 any
access-list 101 permit icmp any 11.11.11.0 0.0.0.255
unreachable
access-list 101 permit icmp any 11.11.11.0 0.0.0.255
echo-reply
access-list 101 permit icmp any 11.11.11.0 0.0.0.255
packet-too-big
access-list 101 permit icmp any 11.11.11.0 0.0.0.255
time-exceeded
access-list 101 permit icmp any 11.11.11.0 0.0.0.255
traceroute
access-list 101 permit icmp any 11.11.11.0 0.0.0.255
administratively-prohibited
```

```
access-list 101 permit icmp any 11.11.11.0 0.0.0.255
echo
access-list 116 permit tcp host 10.31.1.47 host
10.31.1.150 eq www
access-list 116 deny tcp host 10.31.1.47 any
access-list 116 deny udp host 10.31.1.47 any
access-list 116 deny icmp host 10.31.1.47 any
access-list 116 permit tcp 10.31.1.0 0.0.0.255 any
access-list 116 permit udp 10.31.1.0 0.0.0.255 any
access-list 116 permit icmp 10.31.1.0 0.0.0.255 any
access-list 116 permit icmp 171.68.118.0 0.0.0.255 any
access-list 116 permit tcp 171.68.118.0 0.0.0.255 any
access-list 116 permit udp 171.68.118.0 0.0.0.255 any
dialer-list 1 protocol ip permit
dialer-list 1 protocol ipx permit
!
tacacs-server host 171.68.118.115
tacacs-server key cisco
radius-server host 171.68.118.115 auth-port 1646 acct-
port 1646
radius-server key cisco
!
line con 0
transport input none
line aux 0
line vty 0 4
exec-timeout 0 0
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。

有关debug命令及其他故障排除信息，请参阅“Troubleshooting Authentication Proxy”。

**注意：**在发出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](#)