

# 认证代理认证进站(Cisco IOS防火墙-路由器或Switches和NAT)配置示例

## 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

此示例配置最初阻断从外部主机(在10.31.1.47)到内部网络上的所有设备之间的数据流,直到使用认证代理进行了浏览器认证。授权后,从服务器传递的访问列表(`permit tcp|ip|icmp any any`)向访问列表116添加动态条目,该列表暂时允许从外部PC访问内部网络。

**注意:** 本文档中使用的AAA配置也适用于运行Cisco IOS®软件的Catalyst交换机。

## 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

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](#)。

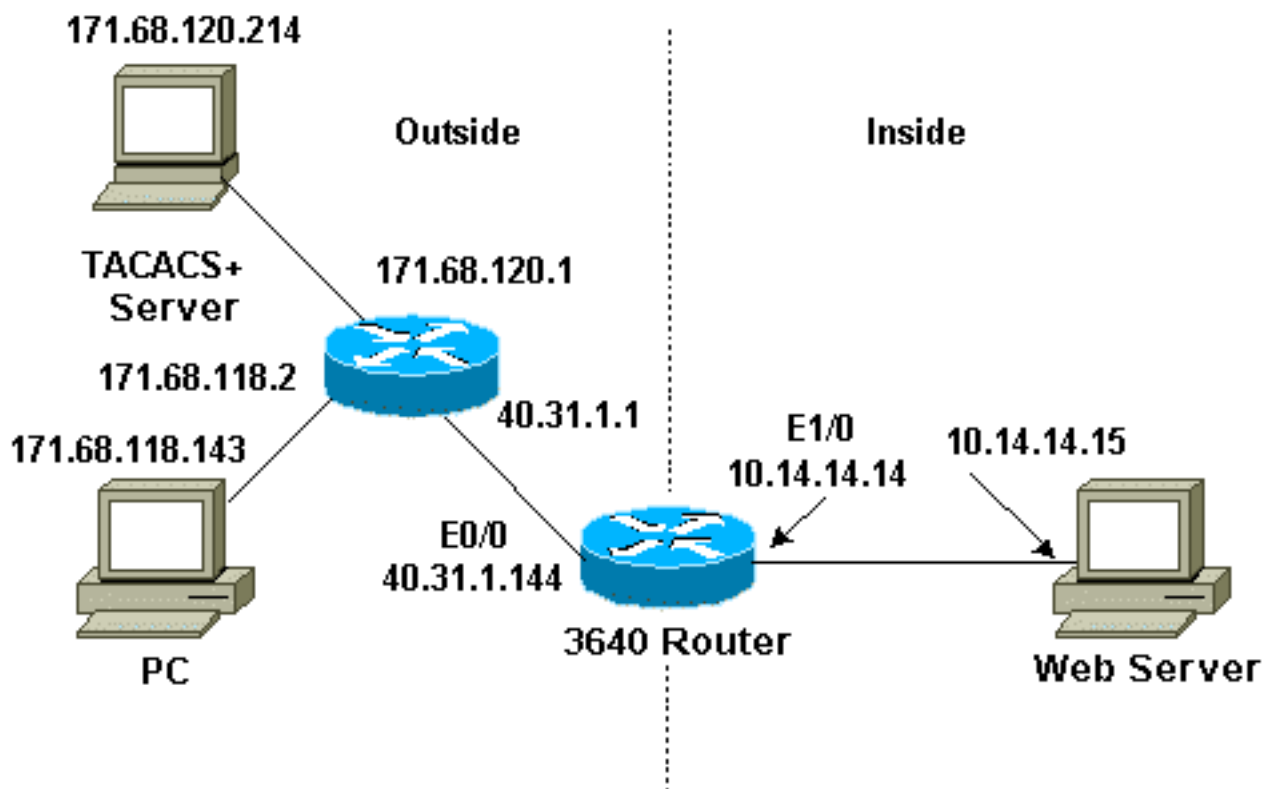
## 配置

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：

- Cisco 3640 路由器

### Cisco 3640 路由器

```
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 $1$pgRI$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
```

## [验证](#)

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

有关命令和[故障排除信息](#)，请参阅身份验证代理故障排除。

## [故障排除](#)

目前没有针对此配置的故障排除信息。

## [相关信息](#)

- [Cisco IOS 防火墙](#)
- [安全和VPN技术支持](#)
- [技术支持和文档 - Cisco Systems](#)