

# Auth-proxy Authentication Outbound ( Cisco IOS防火牆和NAT ) 配置

## 目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[慣例](#)

[設定](#)

[網路圖表](#)

[組態](#)

[驗證](#)

[疑難排解](#)

[相關資訊](#)

## 簡介

此示例配置最初阻止從內部網路上的主機裝置(10.31.1.47)到Internet上所有裝置的流量，直到您使用身份驗證代理執行瀏覽器身份驗證。從伺服器向下傳遞的訪問清單(`permit tcp|ip|icmp any any`)將授權後動態條目新增到訪問清單116，該清單臨時允許從該裝置訪問網際網路。

## 必要條件

### 需求

本文件沒有特定需求。

### 採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco IOS®軟體版本12.2.23
- 思科3640路由器

**注意：** `ip auth-proxy`指令是在Cisco IOS軟體版本12.0.5中匯入，此配置已使用Cisco IOS軟體版本12.0.7進行測試。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

### 慣例

請參閱[思科技術提示慣例](#)以瞭解更多有關文件慣例的資訊。

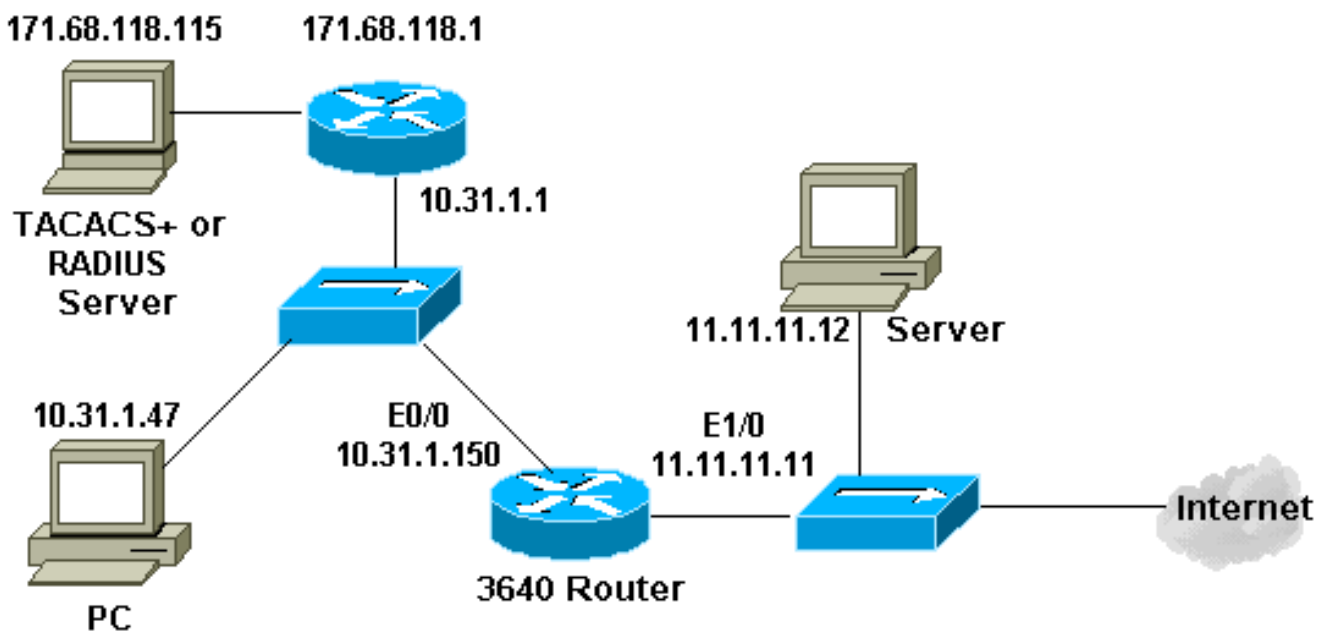
## 設定

本節提供用於設定本文中所述功能的資訊。

**註：**使用[Command Lookup Tool](#)([僅供已註冊客戶使用](#))可獲取本節中使用的命令的詳細資訊。

## 網路圖表

本檔案會使用以下網路設定：



## 組態

本檔案會使用以下設定：

### 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$rrkuU6HLmpbNgLTg/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
```

## 驗證

目前沒有適用於此組態的驗證程序。

## 疑難排解

本節提供的資訊可用於對組態進行疑難排解。

有關debug命令以及其他故障排除資訊，請參閱[驗證代理故障排除](#)。

註：發出debug指令之前，請先參閱有關Debug指令的**重要**資訊。

## 相關資訊

- [IOS防火牆支援頁面](#)
- [TACACS/TACACS+ 支援頁面](#)
- [IOS 文件中的 TACACS+](#)
- [RADIUS 支援頁面](#)
- [要求建議 \(RFC\)](#)
- [技術支援與文件 - Cisco Systems](#)