

# 身份驗證代理身份驗證入站 — 無Cisco IOS防火牆或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外部網路上的主機裝置(11.11.11.12)到內部網路上所有裝置的流量，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115，該清單臨時允許從主機裝置訪問內部網路。

## 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12.0.7.T
- 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。

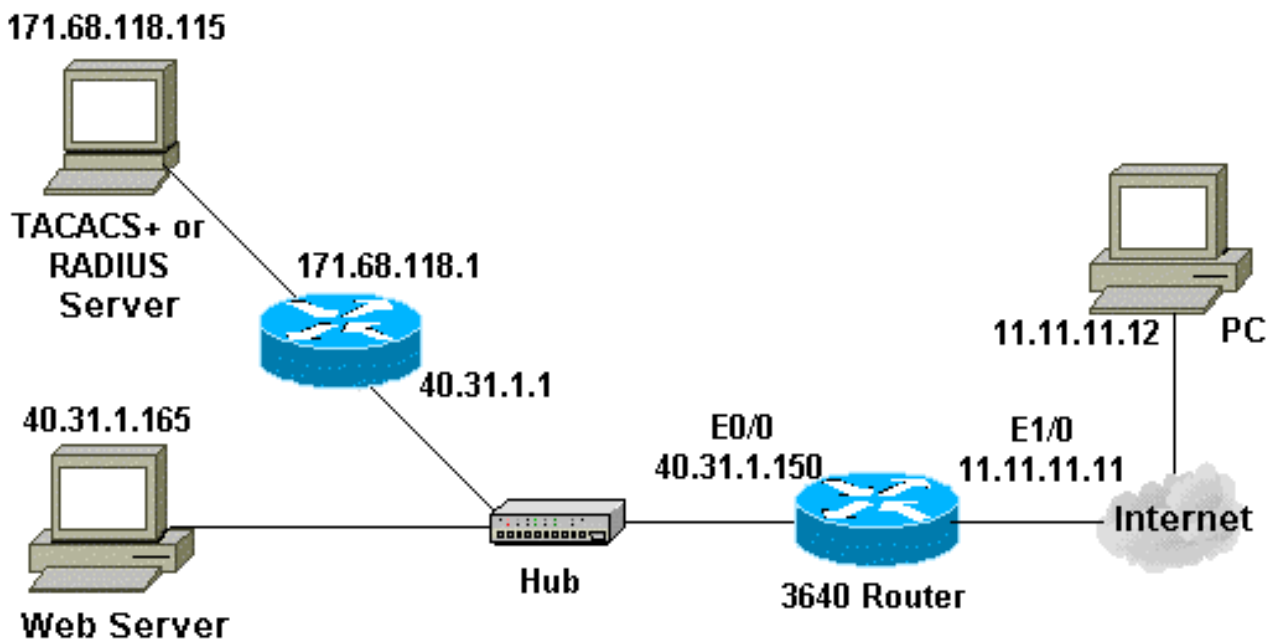
## 設定

本節提供用於設定本文件中所述功能的資訊。

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 12.0
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

## 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。

如需這些命令以及其他疑難排解資訊，請參閱[驗證代理疑難排解](#)。

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](#)