

# インバウンドの Auth-proxy 認証 ( Cisco IOS Firewall、NAT なし ) の設定

## 内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[設定](#)

[ネットワーク図](#)

[コンフィギュレーション](#)

[確認](#)

[トラブルシュート](#)

[関連情報](#)

## 概要

この設定例では、認証プロキシを使用してブラウザの認証が実行されるまで、内部ネットワークのすべてのデバイスに対する外部ホストからのトラフィックをブロックします。サーバから渡されたアクセスリスト(`permit tcp|ip|icmp any any`)は、許可後にダイナミックエントリをアクセスリスト115に追加し、外部PCから内部ネットワークへのアクセスを一時的に許可します。

## 前提条件

### 要件

このドキュメントに特有の要件はありません。

### 使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco IOS(R) ソフトウェア リリース 12.0.7.T
- Cisco 3640 ルータ

注 : `ip auth-proxy` コマンドは、Cisco IOSソフトウェアリリース12.0.5.Tで導入されました。この設定は、Cisco IOSソフトウェアリリース12.0.7.Tでテストされています。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期 ( デフォルト ) 設定の状態から起動しています。対象のネットワークが稼働中である場合には、どのようなコマンドについても、その潜在的

な影響について確実に理解しておく必要があります。

## 表記法

ドキュメント表記の詳細については、『[シスコテクニカルティップスの表記法](#)』を参照してください。

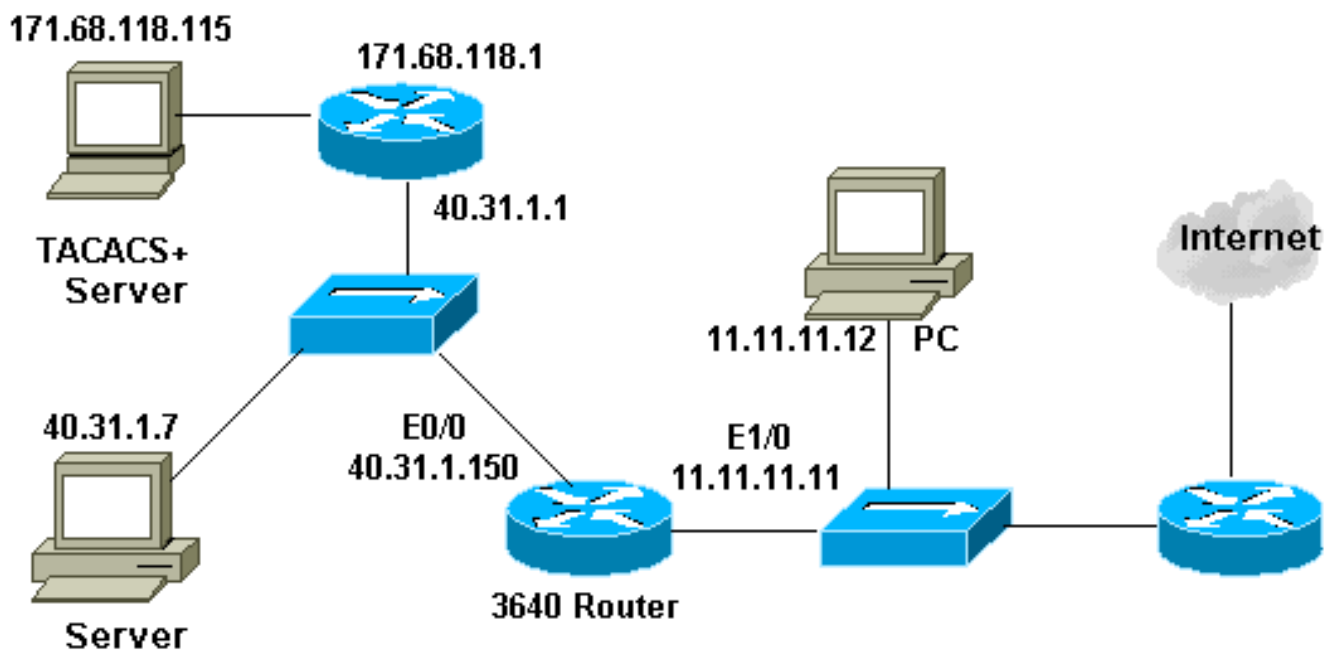
## 設定

このセクションでは、このドキュメントで説明する機能を設定するために必要な情報を提供しています。

注：このセクションで使用されているコマンドの詳細を調べるには、Command Lookup Tool (登録ユーザ専用)を参照してください。一部ツールについては、ゲスト登録のお客様にはアクセスできない場合がありますことをご了承ください。

## ネットワーク図

このドキュメントでは、次のネットワーク セットアップを使用します。



## コンフィギュレーション

このドキュメントでは、次の設定を使用しています。

### 3640 Router

```
Current configuration:
!
version 12.0
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 group RTP none
aaa authorization exec default group RTP none
aaa authorization auth-proxy default group RTP
enable secret 5 $1$H9zZ$z9bu5HMy4NTtjsvIhltGT0
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 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
cns event-service server
!
process-max-time 200
!
interface FastEthernet0/0
  ip address 40.31.1.150 255.255.255.0
  ip access-group 101 in
  no ip directed-broadcast
  ip inspect myfw in
  no mop enabled
!
interface FastEthernet1/0
  ip address 11.11.11.11 255.255.255.0
  ip access-group 115 in
  no ip directed-broadcast
  ip auth-proxy list_a
!
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 40.31.1.1
ip http server
ip http authentication aaa
!
access-list 101 permit icmp 40.31.1.0 0.0.0.255 any
access-list 101 permit tcp 40.31.1.0 0.0.0.255 any
access-list 101 permit udp 40.31.1.0 0.0.0.255 any
access-list 101 permit icmp 171.68.118.0 0.0.0.255 any
access-list 101 permit tcp 171.68.118.0 0.0.0.255 any
access-list 101 permit udp 171.68.118.0 0.0.0.255 any
access-list 115 permit tcp host 11.11.11.12 host
11.11.11.11 eq www
access-list 115 deny tcp any any
access-list 115 deny udp any any
access-list 115 permit icmp any 40.31.1.0 0.0.0.255 echo
```

```
access-list 115 permit icmp any 40.31.1.0 0.0.0.255
echo-reply
access-list 115 permit icmp any 40.31.1.0 0.0.0.255
packet-too-big
access-list 115 permit icmp any 40.31.1.0 0.0.0.255
time-exceeded
access-list 115 permit icmp any 40.31.1.0 0.0.0.255
traceroute
access-list 115 permit icmp any 40.31.1.0 0.0.0.255
unreachable
access-list 115 permit icmp any 40.31.1.0 0.0.0.255
administratively-prohibited
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
radius-server key cisco

!
line con 0
  transport input none
line aux 0
line vty 0 4
  password ww
!
!
end
```

## 確認

現在、この設定に使用できる確認手順はありません。

## トラブルシューティング

ここでは、設定のトラブルシューティングに使用できる情報を示します。

[これらのコマンド、およびその他のトラブルシューティング情報については、認証プロキシのトラブルシューティングを参照してください。](#)

注：debugコマンドを発行する前に、[『debugコマンドの重要な情報』](#)を参照してください。

## 関連情報

- [IOS ファイアウォールのサポート ページ](#)
- [TACACS/TACACS+ サポート ページ](#)
- [IOS での TACACS+ に関するドキュメント](#)
- [RADIUS に関するサポート ページ](#)
- [Requests for Comments \(RFCs\)](#)
- [テクニカル サポートとドキュメント - Cisco Systems](#)