

インバウンドのプロキシ認証 - Cisco IOS Firewall や NAT のない設定

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](#)

[設定](#)

[確認](#)

[トラブルシューティング](#)

[関連情報](#)

概要

この設定例は、認証プロキシを使用してブラウザの認証が行われるまで、外部ネットワーク上の (11.11.11.12 にある) ホスト デバイスから内部ネットワーク上のすべてのデバイスへのトラフィックを最初にブロックします。サーバから渡されたアクセスリスト (`permit tcp|ip|icmp any any`) は、許可後に動的エントリをアクセスリスト115に追加し、ホストデバイス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。

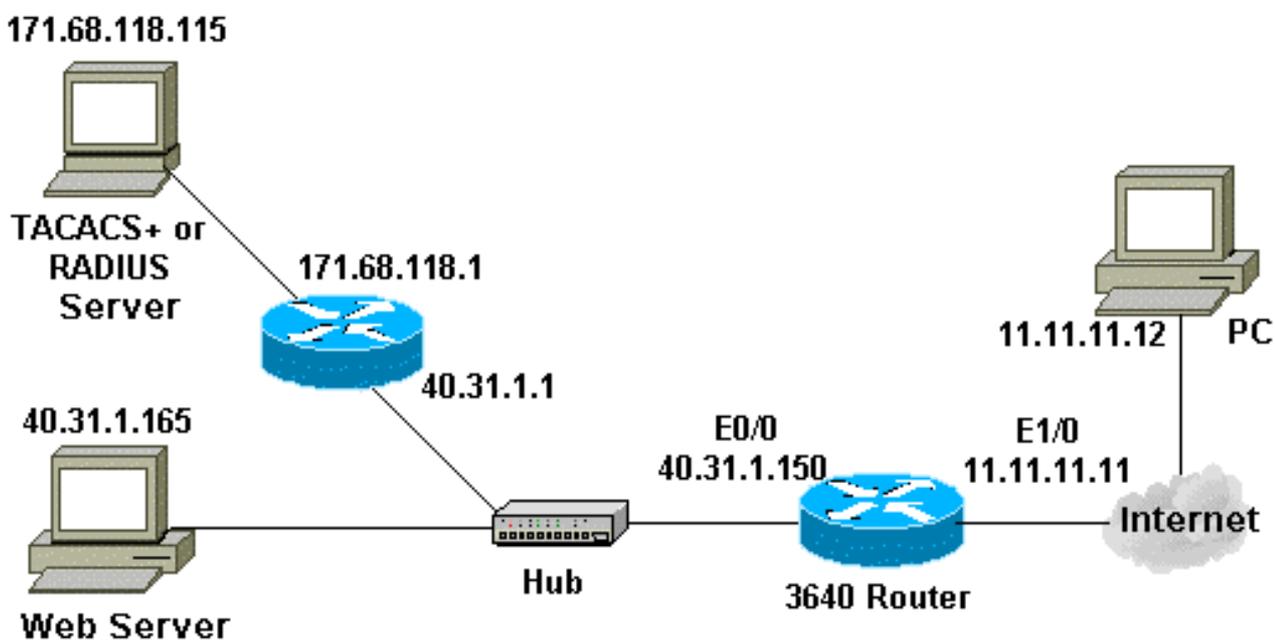
設定

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。



設定

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
!
!--- 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$z9bu5HMy4NTtjsvIhltGT0
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
```

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](#)