Auth-proxy 認証発信（Cisco IOS Firewall と NAT）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](#)
[設定](#)
[確認](#)
[トラブルシュート](#)
[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、内部ネットワーク上の（10.31.1.47 にある）ホスト デバイスからインターネット上のすべてのデバイスへ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116に追加し、そのデバイスからインターネット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 12.2.23
- 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実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。

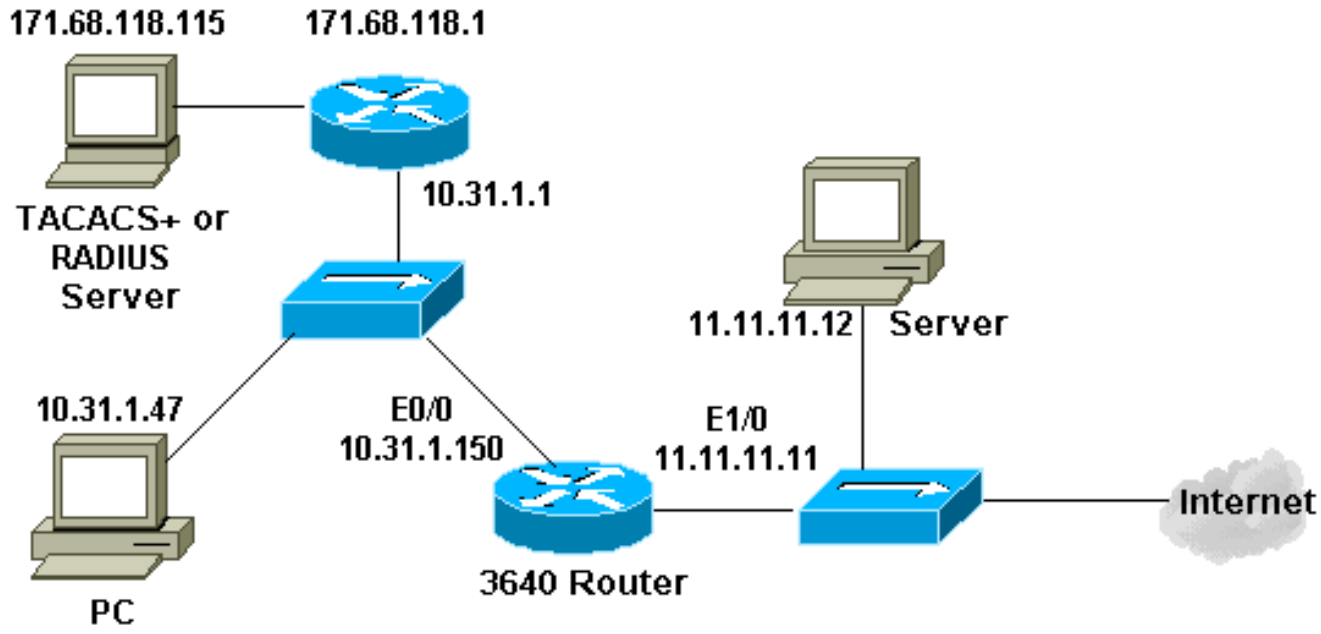
設定

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 12.2 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$rkuU6HLmpbNgLTg/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 1645 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
```

確認

現在、この設定に使用できる確認手順はありません。

トラブルシュート

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。

debugコマンドと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