Auth-proxy 認証着信（Cisco IOS Firewall - ルータ/スイッチおよび NAT）の設定例

目次

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。 許可後、サーバから渡されるアクセス リスト（permit tcp|ip|icmp any any）は、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するアクセス リスト 116 にダイナミック エントリを追加します。 |IP|

注: この資料で使用される AAA設定は Cisco IOS ® ソフトウェアを実行する Catalyst スイッチにまた適当です。

前提条件

要件

このドキュメントに関する固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くものです。

- Cisco IOS ソフトウェア リリース 12.2.23
- Cisco 3640 ルータ

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たものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始して

います。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分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。

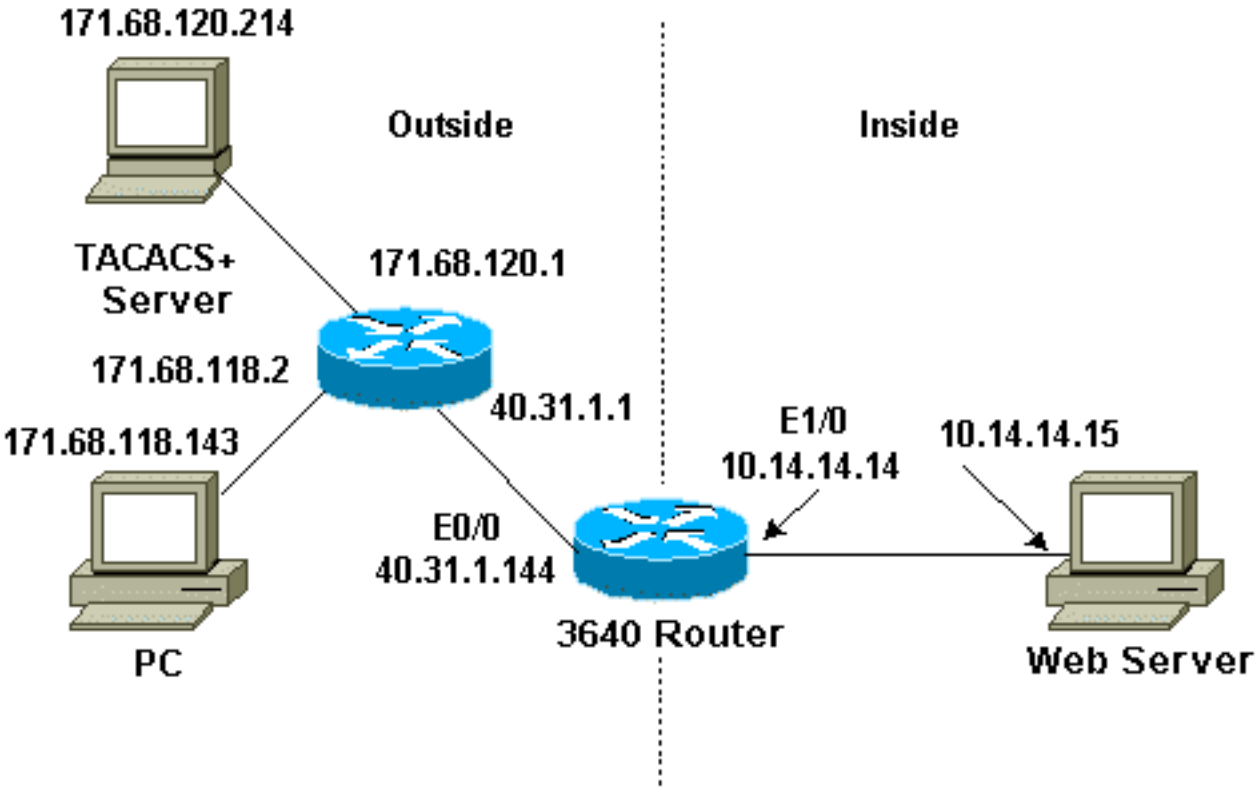
設定

この項では、このドキュメントで説明する機能の設定に必要な情報を提供します。

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）を使用してください。

ネットワーク図

このドキュメントでは、次のネットワーク構成を使用しています。



設定

このドキュメントでは次の設定を使用しています。

- Cisco 3640 ルータ

Cisco 3640 ルータ
Current configuration: ! version 12.2 service timestamps debug uptime

```
service timestamps log uptime
no service password-encryption
!
hostname sec-3640
!
aaa new-model aaa group server tacacs+ RTP server
171.68.120.214 ! aaa authentication login default group
RTP none aaa authorization exec default group RTP none
aaa authorization auth-proxy default group RTP enable
secret 5 $1$pqRI$3TDNFT9FdYT8Sd/q3S0VU1 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 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 ! interface
Ethernet0/0 ip address 40.31.1.144 255.255.255.0 ip
access-group 116 in ip nat outside ip auth-proxy list_a
no ip route-cache no ip mroute-cache speed auto half-
duplex no mop enabled ! interface Ethernet1/0 ip address
10.14.14.14 255.255.255.0 ip nat inside ip inspect myfw
in speed auto half-duplex ! !--- Interfaces deleted. !
nat pool outsidepool 40.31.1.50 40.31.1.60 netmask
255.255.255.0 ip nat inside source list 1 pool
outsidepool ip nat inside source static 10.14.14.15
40.31.1.77 ip classless ip route 0.0.0.0 0.0.0.0
40.31.1.1 ip route 171.68.118.0 255.255.255.0 40.31.1.1
ip route 171.68.120.0 255.255.255.0 40.31.1.1 no ip http
server ! access-list 116 permit tcp host 171.68.118.143
host 40.31.1.144 eq www access-list 116 deny tcp host
171.68.118.143 any access-list 116 deny udp host
171.68.118.143 any access-list 116 deny icmp host
171.68.118.143 any access-list 116 permit icmp any any
access-list 116 permit tcp any any access-list 116
permit udp any any dialer-list 1 protocol ip permit
dialer-list 1 protocol ipx permit ! tacacs-server host
171.68.120.214 tacacs-server key cisco ! line con 0
transport input none line aux 0 line vty 0 4 password ww
! end
```

確認

debug コマンドを使用する前に、『**debug コマンドの重要な情報**』を参照してください。

コマンドとトラブルシューティングの詳細については、『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。

トラブルシューティング

現在のところ、この設定に関する特定のトラブルシューティング情報はありません。

関連情報

- Cisco IOS ファイアウォール
- セキュリティと VPN テクノロジーに関するサポート
- テクニカルサポートとドキュメント - Cisco Systems