

Configuration de l'authentification des utilisateurs entrants par proxy d'authentification (Pare-feu Cisco IOS, pas NAT)

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Conventions](#)

[Configurez](#)

[Diagramme du réseau](#)

[Configuration](#)

[Vérifiez](#)

[Dépannez](#)

[Informations connexes](#)

[Introduction](#)

Les blocs de cette configuration d'échantillon au commencement trafiquent des hôtes externes à tous les périphériques sur le réseau interne jusqu'à ce que l'authentification du navigateur soit exécutée avec l'utilisation du Seveur mandataire d'authentification. La liste d'accès passée vers le bas du serveur (**TCP d'autorisation|IP|l'ICMP tout**) en ajoute la POST-autorisation d'entrées dynamiques à la liste d'accès 115 qui permettent temporairement l'accès du PC externe au réseau interne.

[Conditions préalables](#)

[Conditions requises](#)

Aucune spécification déterminée n'est requise pour ce document.

[Composants utilisés](#)

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Version de logiciel 12.0.7.T de Cisco IOS®
- Routeur de Cisco 3640

Remarque: La commande de **proxy d'authentification d'IP** est introduite dans la version du logiciel

Cisco IOS 12.0.5.T. Cette configuration a été testée avec la version du logiciel Cisco IOS 12.0.7.T.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à [Conventions relatives aux conseils techniques Cisco](#).

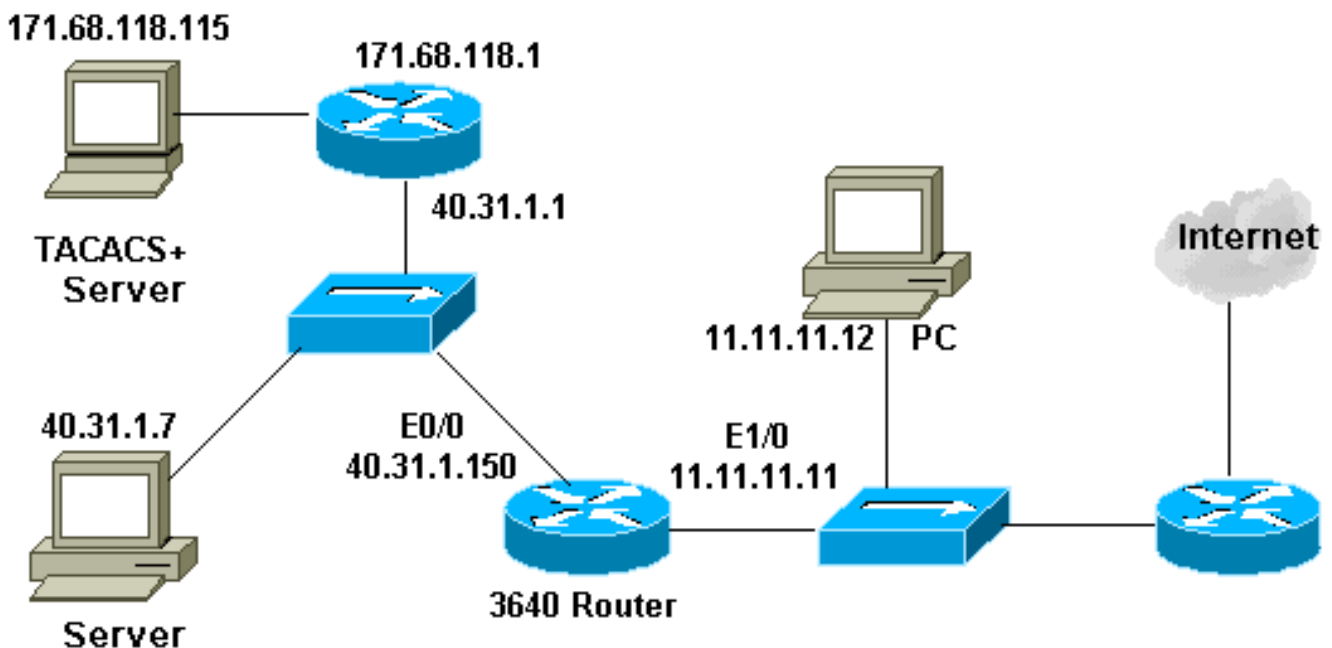
Configurez

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Remarque: Utilisez l'outil [Command Lookup Tool](#) (clients [enregistrés](#) seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



Configuration

Ce document utilise la configuration suivante :

```
Router 3640
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$z9bu5HMy4NTtjstvIhltGT0 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

```

[Vérifiez](#)

Aucune procédure de vérification n'est disponible pour cette configuration.

[Dépannez](#)

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Pour ces commandes, avec l'autre information de dépannage, référez-vous au [Seueur mandataire d'authentification de dépannage](#).

Remarque: Reportez-vous à [Informations importantes sur les commandes de débogage](#) avant d'émettre des commandes **debug**.

[Informations connexes](#)

- [Page de support pour le pare-feu d'IOS](#)
- [Page de support TACACS/TACACS+](#)
- [TACACS+ dans la documentation d'IOS](#)
- [Page d'assistance RADIUS](#)
- [Demandes de commentaires \(RFC\)](#)
- [Support et documentation techniques - Cisco Systems](#)