

Exemple de configuration d'authentification des utilisateurs entrants par proxy d'authentification (pare-feu Cisco IOS - Routeurs/Commutateurs et NAT)

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Conventions](#)

[Configuration](#)

[Diagramme du réseau](#)

[Configurations](#)

[Vérification](#)

[Dépannage](#)

[Informations connexes](#)

[Introduction](#)

Cet exemple de configuration bloque initialement le trafic des hôtes externes vers tous les périphériques du réseau interne jusqu'à ce que l'authentification du navigateur soit effectuée à l'aide du proxy d'authentification. Après autorisation, la liste d'accès transmise depuis le serveur (**permit tcp|ip|icmp any any**) ajoute des entrées dynamiques à la liste d'accès 116 qui permettent temporairement l'accès du PC externe au réseau interne.

Remarque : La configuration AAA utilisée dans ce document s'applique également aux commutateurs Catalyst qui exécutent le logiciel Cisco IOS[®].

[Conditions préalables](#)

[Conditions requises](#)

Aucune spécification déterminée n'est requise pour ce document.

[Components Used](#)

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

- Logiciel Cisco IOS Version 12.2.23
- Routeur Cisco 3640

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

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

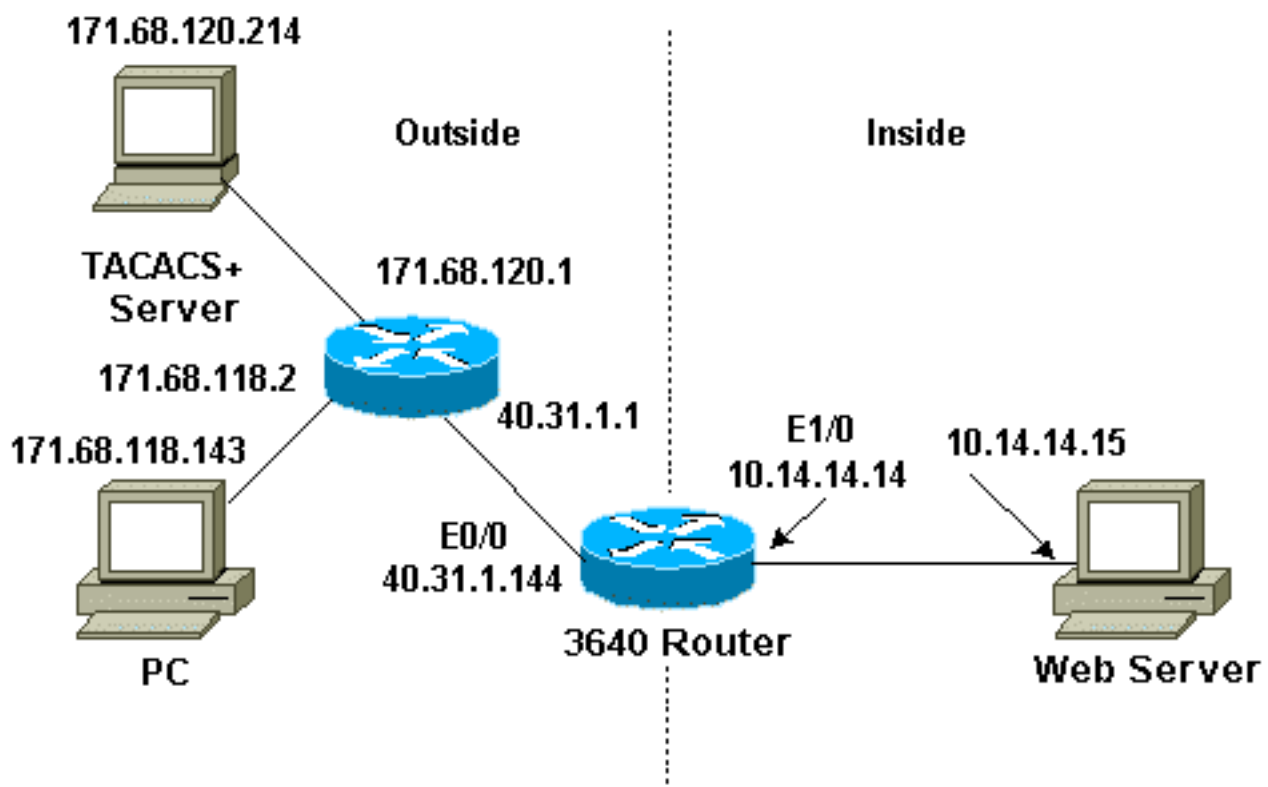
Configuration

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

Remarque : utilisez l'[outil de recherche de commandes](#) (clients [enregistrés](#) uniquement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



Configurations

Ce document utilise la configuration suivante :

- Routeur Cisco 3640

Routeur Cisco 3640

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
```

Vérification

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

Référez-vous à [Dépannage du proxy d'authentification](#) pour obtenir des informations de commande et de dépannage.

Dépannage

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

Informations connexes

- [Cisco IOS Firewall](#)
- [Prise en charge de la sécurité et des technologies VPN](#)
- [Support et documentation techniques - Cisco Systems](#)