认证代理认证入站(Cisco IOS防火墙，没有NAT)配置

目录

简介

在使用认证代理执行浏览器身份验证之前，此示例配置最初会阻塞从外部主机到内部网络上的所有设备的流量。从服务器通过的下来访问列表(**permit tcp|ip|**icmp any any) 会将动态条目后授权添加到暂时允许从外部 PC 访问内部网络的访问列表 115 中。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Cisco IOS®软件版本12.0.7.T
- Cisco 3640路由器

注意： ip auth-proxy命令在Cisco IOS软件版本12.0.5.T.介绍此配置测试了Cisco IOS软件版本12.0.7.T。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

配置

本部分提供有关如何配置本文档所述功能的信息。

注意： 使用命令查找工具（仅限注册用户）可获取有关本部分所使用命令的详细信息。

网络图

本文档使用以下网络设置：

配置

本文档使用以下配置：

3640路由器

```
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$z9bu5HMy4NTtjsvIhltGT0 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
```

验证

当前没有可用于此配置的验证过程。

故障排除

本部分提供的信息可用于对配置进行故障排除。

对于这些指令和其他故障排除信息，请参见排错认证代理。

注意： 发出 **debug** 命令之前，请参阅有关 Debug 命令的重要信息。

相关信息

- IOS防火墙支持页面
- TACACS/TACACS+支持页面
- IOS 文档中的 TACACS+
- RADIUS 支持页
- 请求注解 (RFC)
- 技术支持和文档 - Cisco Systems