Entrada de autenticação do proxy de autenticação - Nenhuma Cisco IOS Firewall ou configuração de NAT

Índice

Introdução

Esta configuração de exemplo obstrui inicialmente o tráfego de um dispositivo host (em 11.11.11.12) na rede externa a todos os dispositivos na rede interna até que você execute a autenticação de navegador com o uso do Proxy de autenticação. Lista de acesso passada adiante a partir do servidor (permit tcp|ip|o ICMP todo o algum) adiciona as entradas dinâmica pós-autorização à lista de acessos 115 que permitem temporariamente o acesso do dispositivo host à rede interna.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Software Cisco® IOS versão 12.0.7.T
- Cisco 3640 Router

Nota: O comando ip auth-proxy foi adotado no Cisco IOS Software versão 12.0.5.T. Esta configuração foi testada com Cisco IOS Software Release 12.0.7.T.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Configurar

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Nota: Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:

Configurações

Este documento utiliza esta configuração:

3640 Router

```
Current configuration:
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname security-3640
!
!--- Turn on authentication. aaa new-model !--- Define
the server group and servers for TACACS+ or RADIUS. aaa
group server tacacs+|radius RTP server 171.68.118.115 !
!--- Define what you need to authenticate. 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 ! !--- You want the router name to appear as
banner. ip auth-proxy auth-proxy-banner !--- You want
the access-list entries to timeout after 10 minutes. ip
auth-proxy auth-cache-time 10 !--- You define the list-
name to be associated with the interface. 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 no ip directed-broadcast no mop enabled !
interface FastEthernet1/0 ip address 11.11.11.11
255.255.255.0 !--- Apply the access-list to the
```

```
interface. ip access-group 115 in no ip directed-
broadcast !--- Apply the auth-proxy list-name. ip auth-
proxy list_a ! ip classless ip route 171.68.118.0
255.255.255.0 40.31.1.1 !--- Turn on the http server and
authentication. ip http server ip http authentication
aaa ! !--- This is our access-list for auth-proxy
testing - !--- it denies only one host, 11.11.11.12,
access - to minimize disruption !--- to the network
during testing. access-list 115 permit tcp host
11.11.11.12 host 11.11.11.11 eq www access-list 115 deny
icmp host 11.11.11.12 any access-list 115 deny tcp host
11.11.11.12 any access-list 115 deny udp host
11.11.11.12 any access-list 115 permit udp any any
access-list 115 permit tcp any any access-list 115
permit icmp any any dialer-list 1 protocol ip permit
dialer-list 1 protocol ipx permit ! !--- Define the
server(s). 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
```

Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

Troubleshooting

Esta seção fornece a informação que você pode se usar a fim pesquisar defeitos sua configuração.

Para estes comandos, junto com a outra informação de Troubleshooting, refira pesquisando defeitos o Proxy de autenticação.

Nota: Consulte Informações Importantes sobre Comandos de Debugação antes de usar comandos **debug**.

Informações Relacionadas

- Página de suporte de firewall do IOS
- Página de Suporte do TACACS/TACACS+
- TACACS+ na Documentação do IOS
- Página de suporte RADIUS
- Solicitações de Comentários (RFCs)
- Suporte Técnico e Documentação - Cisco Systems