ASA 8.3 e mais atrasado: Acesso de servidor do correio (S TP) no exemplo de configuração da rede externa

Índice

Introdução

Esta configuração de exemplo fornece a informação em como estabelecer a ferramenta de segurança adaptável (ASA) para o acesso a um mail server situado na rede externa.

Refira ASA 8.3 e mais atrasado: Envie o acesso de servidor (S TP) no exemplo da configuração DMZ para obter mais informações sobre de como estabelecer a ferramenta de segurança ASA para o acesso a um server mail/SMTP situado na rede do DMZ.

Refira ASA 8.3 e mais atrasado: Envie o acesso de servidor (S TP) no exemplo de configuração da rede interna a fim estabelecer a ferramenta de segurança ASA para o acesso a um server mail/SMTP situado na rede interna.

Refira PIX/ASA 7.x e mais tarde: Envie o acesso de servidor (S TP) no exemplo de configuração da rede externa para a configuração idêntica na ferramenta de segurança adaptável de Cisco (ASA) com versões 8.2 e anterior.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

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

- A ferramenta de segurança adaptável de Cisco (ASA) essa executa a versão 8.3 e mais recente
- Cisco 1841 Router com Software Release 12.4(20)T de Cisco IOS®

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:

Nota: Os esquemas de endereçamento IP usados nesta configuração não são legalmente roteáveis na Internet. São os endereços do RFC 1918 que foram usados em um ambiente de laboratório.

A instalação de rede usada neste exemplo tem o ASA com rede interna (192.168.1.0/30) e a rede externa (209.64.3.0/30). O mail server com endereço IP 209.64.3.6 é ficado situado na rede externa. Configurar a declaração NAT de modo que todo o tráfego da rede 192.168.2.x que passa da interface interna (ethernet0) à interface externa (Ethernet1) traduza a um endereço na escala de 209.64.3.129 com 209.64.3.253. O último endereço disponível (209.64.3.254) é reservado para a tradução de endereço de porta (PAT).

Configurações

Este documento utiliza as seguintes configurações:

- ASA
- Roteador A
- roteador B

ASA

```
ASA#show run : Saved : ASA Version 8.3(1) ! hostname ASA
enable password 8Ry2YjIyt7RRXU24 encrypted passwd
2KFQnbNIdI.2KYOU encrypted names ! interface Ethernet0
shutdown no nameif no security-level no ip address !
interface Ethernet1 shutdown no nameif no security-level
no ip address ! interface Ethernet2 shutdown no nameif
no security-level no ip address ! !--- Configure the
inside interface. ? interface Ethernet3 nameif inside
security-level 100 ip address 192.168.1.1
255.255.255.252 ! !--- Configure the outside interface.
interface Ethernet4 nameif outside security-level 0 ip
address 209.64.3.1 255.255.255.252 ! interface Ethernet5
shutdown no nameif no security-level no ip address !
passwd 2KFQnbNIdI.2KYOU encrypted boot system
disk0:/asa831-k8.bin ftp mode passive pager lines 24 mtu
inside 1500 mtu outside 1500 no failover no asdm history
enable arp timeout 14400 !--- This command states that
any traffic !--- from the 192.168.2.x network that
passes from the inside interface (Ethernet0) !--- to the
outside interface (Ethernet 1) translates into an
address !--- in the range of 209.64.3.129 through
209.64.3.253 and contains a subnet !--- mask of
255.255.255.128. object network obj-
209.64.3.129_209.64.3.253 range 209.64.3.129-
209.64.3.253 !--- This command reserves the last
available address (209.64.3.254) for !--- for Port
Address Translation (PAT). In the previous statement, !-
-- each address inside that requests a connection uses
one !--- of the addresses specified. If all of these
addresses are in use, !--- this statement provides a
failsafe to allow additional inside stations !--- to
establish connections. object network obj-209.64.3.254
host 209.64.3.254 !--- This command indicates that all
addresses in the 192.168.2.x range !--- that pass from
the inside (Ethernet0) to a corresponding global !---
designation are done with NAT. !--- As outbound traffic
is permitted by default on the ASA, no !--- static
commands are needed. object-group network nat-pat-group
network-object object obj-209.64.3.129_209.64.3.253
network-object object obj-209.64.3.254 object network
obj-192.168.2.0 subnet 192.168.2.0 255.255.255.0 nat
(inside,outside) dynamic nat-pat-group !--- Creates a
static route for the 192.168.2.x network with
192.168.1.2. !--- The ASA forwards packets with these
addresses to the router !--- at 192.168.1.2. route
inside 192.168.2.0 255.255.255.0 192.168.1.2 1 !--- Sets
the default route for the ASA Firewall at 209.64.3.2.
route outside 0.0.0.0 0.0.0.0 209.64.3.2 1 timeout xlate
3:00:00 timeout conn 1:00:00 half-closed 0:10:00 udp
0:02:00 icmp 0:00:02 timeout sunrpc 0:10:00 h323 0:05:00
h225 1:00:00 mgcp 0:05:00 timeout mgcp-pat 0:05:00 sip
0:30:00 sip_media 0:02:00 timeout uauth 0:05:00 absolute
no snmp-server location no snmp-server contact snmp-
server enable traps snmp authentication linkup linkdown
coldstart telnet timeout 5 ssh timeout 5 console timeout
0 ! class-map inspection_default match default-
inspection-traffic ! ! !--- SMTP/ESMTP is inspected
since "inspect esmtp" is included in the map. policy-map
global_policy class inspection_default inspect dns
maximum-length 512 inspect ftp inspect h323 h225 inspect
h323 ras inspect rsh inspect rtsp inspect esmtp inspect
sqlnet inspect skinny inspect sunrpc inspect xdmcp
inspect sip inspect netbios inspect tftp ! service-
policy global_policy global
```

```
Cryptochecksum:8a63de5ae2643c541a397c2de7901041 : end
```

Roteador A

```
Current configuration:
  !
  version 12.4
  service timestamps debug uptime
  service timestamps log uptime
  no service password-encryption
  !
  hostname 2522-R4
  !
  enable secret 5 $1$N0F3$XE2aJhJlCbLWYloDwNvcV.
  !
  ip subnet-zero
  !
  !
  !
  !
  !
  interface Ethernet0

!--- Assigns an IP address to the inside Ethernet
interface. ip address 192.168.2.1 255.255.255.0 no ip
directed-broadcast ! interface Ethernet1 !--- Assigns an
IP address to the ASA-facing interface. ip address
192.168.1.2 255.255.255.252 no ip directed-broadcast !
interface Serial0 no ip address no ip directed-broadcast
shutdown ! interface Serial1 no ip address no ip
directed-broadcast shutdown ! ip classless !--- This
route instructs the inside router to forward all !---
non-local packets to the ASA. ip route 0.0.0.0 0.0.0.0
192.168.1.1 ! ! line con 0 transport input none line aux
0 autoselect during-login line vty 0 4 exec-timeout 5 0
password ww login ! end
```

roteador B

```
Current configuration:
  !
  version 12.4
  service timestamps debug uptime
  service timestamps log uptime
  no service password-encryption
  !
  hostname 2522-R4
  !
  enable secret 5 $1$N0F3$XE2aJhJlCbLWYloDwNvcV.
  !
  ip subnet-zero
  !
  !
  !
  !
  interface Ethernet0

!--- Assigns an IP address to the ASA-facing Ethernet
interface. ip address 209.64.3.2 255.255.255.252 no ip
directed-broadcast ! interface Ethernet1 !--- Assigns an
IP address to the server-facing Ethernet interface. ip
address 209.64.3.5 255.255.255.252 no ip directed-
broadcast ! interface Serial0 !--- Assigns an IP address
to the Internet-facing interface. ip address 209.64.3.9
255.255.255.252 no ip directed-broadcast no ip mroute-
cache ! interface Serial1 no ip address no ip directed-
```

```
broadcast ! ip classless !--- All non-local packets are
to be sent out serial 0. In this case, !--- the IP
address on the other end of the serial interface is not
known, !--- or you can specify it here. ip route 0.0.0.0
0.0.0.0 serial 0 ! !--- This statement is required to
direct traffic destined to the !--- 209.64.3.128 network
(the ASA global pool) to the ASA to be translated !---
back to the inside addresses. ip route 209.64.3.128
255.255.255.128 209.64.3.1 ! ! line con 0 transport
input none line aux 0 autoselect during-login line vty 0
4 exec-timeout 5 0 password ww login ! end
```

Configuração ESMTP TLS

Nota: Se você usa a criptografia do Transport Layer Security (TLS) para uma comunicação do email então a característica da inspeção de ESMTP (permitida à revelia) no ASA deixa cair os pacotes. A fim permitir os email com o TLS permitido, desabilite a característica da inspeção de ESMTP como esta saída mostra. Refira a identificação de bug Cisco CSCtn08326 (clientes registrados somente) para mais informação.

```
ciscoasa(config)#policy-map global_policy ciscoasa(config-pmap)#class inspection_default
ciscoasa(config-pmap-c)#no inspect esmtp ciscoasa(config-pmap-c)#exit ciscoasa(config-pmap)#exit
```

Verificar

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

Troubleshooting

A Output Interpreter Tool (apenas para clientes registrados) (OIT) suporta determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

O comando 7 protegido de registro dirige mensagens ao console ASA. Se a Conectividade ao mail server é um problema, examine o console debugam mensagens para encontrar os endereços IP de Um ou Mais Servidores Cisco ICM NT da emissão e das estações de recepção a fim determinar o problema.

Informações Relacionadas

- Cisco ASA 5500 Series Adaptive Security Appliances
- Solicitações de Comentários (RFCs)
- Suporte Técnico e Documentação - Cisco Systems