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

Índice

Introdução

Esta configuração de exemplo demonstra como configurar o ASA Security Appliance para acesso a um servidor de e-mail (SMTP) situado na rede interna.

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) na configuração de rede externa Exampleto estabelece a ferramenta de segurança ASA para o acesso a um server mail/SMTP situado na rede externa.

Refira PIX/ASA 7.x e mais tarde: Envie o acesso de servidor (S TP) no exemplo de configuração da rede interna para mais informação da 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 liberação 12.4(20)T do Cisco IOS ® Software

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.

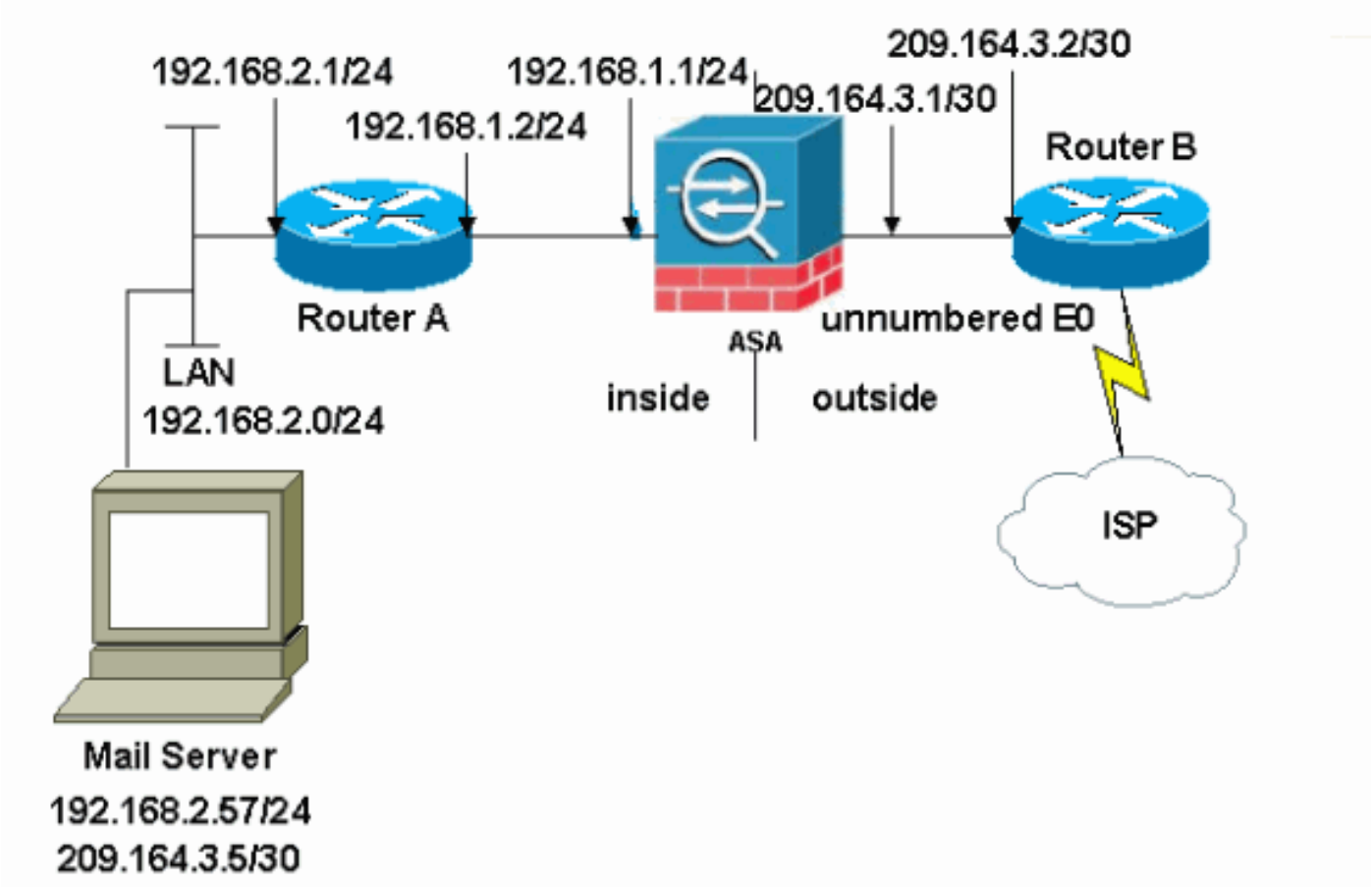
Configurar

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 (192.168.1.0/24) e a rede externa (209.164.3.0/30). O mail server com endereço IP 209.64.3.5 é ficado situado na rede interna.

Configurações

Este documento utiliza as seguintes configurações:

- ASA
- 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 ! !--- Define the IP
address for the inside interface. interface Ethernet3
nameif inside security-level 100 ip address 192.168.1.1
255.255.255.0 ! !--- Define the IP address for the
outside interface. interface Ethernet4 nameif outside
security-level 0 ip address 209.164.3.1 255.255.255.252
! interface Ethernet5 shutdown no nameif no security-
level no ip address ! passwd 2KFQnbNIdI.2KYOU encrypted
```

```
ftp mode passive !--- Create an access list that permits Simple !--- Mail Transfer Protocol (SMTP) traffic from anywhere !--- to the host at 209.164.3.5 (our server). The name of this list is !--- smtp. Add additional lines to this access list as required. !--- Note: There is one and only one access list allowed per !--- interface per direction, for example, inbound on the outside interface. !--- Because of limitation, any additional lines that need placement in !--- the access list need to be specified here. If the server !--- in question is not SMTP, replace the occurrences of SMTP with !--- www, DNS, POP3, or whatever else is required. access-list smtp extended permit tcp any host 209.164.3.5 eq smtp pager lines 24 mtu inside 1500 mtu outside 1500 no failover no asdm history enable arp timeout 14400 !--- Specify that any traffic that originates inside from the !--- 192.168.2.x network NATs (PAT) to 209.164.3.129 if !--- such traffic passes through the outside interface. object network obj-192.168.2.0 subnet 192.168.2.0 255.255.255.0 nat (inside,outside) dynamic 209.164.3.129 !--- Define a static translation between 192.168.2.57 on the inside and !--- 209.164.3.5 on the outside. These are the addresses to be used by !--- the server located inside the ASA. object network obj-192.168.2.57 host 192.168.2.57 nat (inside,outside) static 209.164.3.5 !--- Apply the access list named smtp inbound on the outside interface. access-group smtp in interface outside !--- Instruct the ASA to hand any traffic destined for 192.168.x.x !--- to the router at 192.168.1.2. route inside 192.168.0.0 255.255.0.0 192.168.1.2 1 !--- Set the default route to 209.164.3.2. !--- The ASA assumes that this address is a router address. route outside 0.0.0.0 0.0.0.0 209.164.3.2 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 as "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 netbios inspect rsh inspect rtsp inspect skinny inspect esmtp inspect sqlnet inspect sunrpc inspect tftp inspect sip inspect xdmcp ! !--- SMTP/ESMTP is inspected as "inspect esmtp" is included in the map. service-policy global_policy global Cryptochecksum:f96eaf0268573bd1af005e1db9391284 : end
```

roteador B

```
Current configuration:
 !
 version 12.4
 service timestamps debug uptime
 service timestamps log uptime
 no service password-encryption
 !
 hostname 2522-R5
 !
 enable secret 5 $1$N0F3$XE2aJhJlCbLWYloDwNvcV.
 !
```

```
 ip subnet-zero
 !
 !
 !
 !
 !
 interface Ethernet0

!--- Sets the IP address of the Ethernet interface to
209.164.3.2. ip address 209.164.3.2 255.255.255.252 !
interface Serial0 !--- Instructs the serial interface to
use !--- the address of the Ethernet interface when the
need arises. ip unnumbered ethernet 0 ! interface
Serial1 no ip address no ip directed-broadcast ! ip
classless !--- Instructs the router to send all traffic
!--- destined for 209.164.3.x to 209.164.3.1. ip route
209.164.3.0 255.255.255.0 209.164.3.1 !--- Instructs the
router to send !--- all other remote traffic out serial
0. ip route 0.0.0.0 0.0.0.0 serial 0 ! ! line con 0
transport input none line aux 0 autoselect during-login
line vty 0 4 exec-timeout 5 0 password ww login ! end
```

Nota: A configuração de roteador A não é adicionada. Você somente tem que dar os endereços IP de Um ou Mais Servidores Cisco ICM NT nas relações e ajustar o gateway padrão a 192.168.1.1, que é a interface interna do ASA.

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
```

Nota: Na versão ASA 8.0.3 e mais atrasado, o comando permitir-**TLS** está disponível para permitir o email TLS com inspeciona o esmtp permitido como mostrado:

```
policy-map type inspect esmtp tls-esmtp
parameters
allow-tls
inspect esmtp tls-esmtp
```

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