ASA 8.3: Estabelecer e solucionar problemas de conectividade por meio do Cisco Security Appliance

Contents

Introduction

Quando um Cisco Adaptive Security Appliance (ASA) é configurado inicialmente, ele tem uma política de segurança padrão na qual todos no interior podem sair e ninguém de fora pode entrar. Se sua instalação exige uma política de segurança diferente, você pode permitir que os usuários externos se conectem a seu servidor de web com o ASA.

Depois de estabelecer a conectividade básica através do Cisco ASA, você pode fazer alterações na configuração do firewall. Verifique se todas as alterações de configuração feitas no ASA estão em conformidade com sua política de segurança do site.

Consulte o PIX/ASA: Estabeleça e solucione problemas de conectividade por meio do Cisco Security Appliance para a configuração idêntica no Cisco ASA com versões 8.2 e anteriores.

Prerequisites

Requirements

Este documento pressupõe que algumas configurações básicas já foram concluídas no Cisco ASA. Consulte estes documentos para obter exemplos de uma configuração inicial do ASA:

- ASA 8.3(x): Conectar uma única rede interna à Internet
- Configurando o cliente PPPoE em um Cisco Adaptive Security Appliance (ASA)

Componentes Utilizados

As informações neste documento são baseadas em um Cisco Adaptive Security Appliance (ASA) que executa a versão 8.3 e posterior.

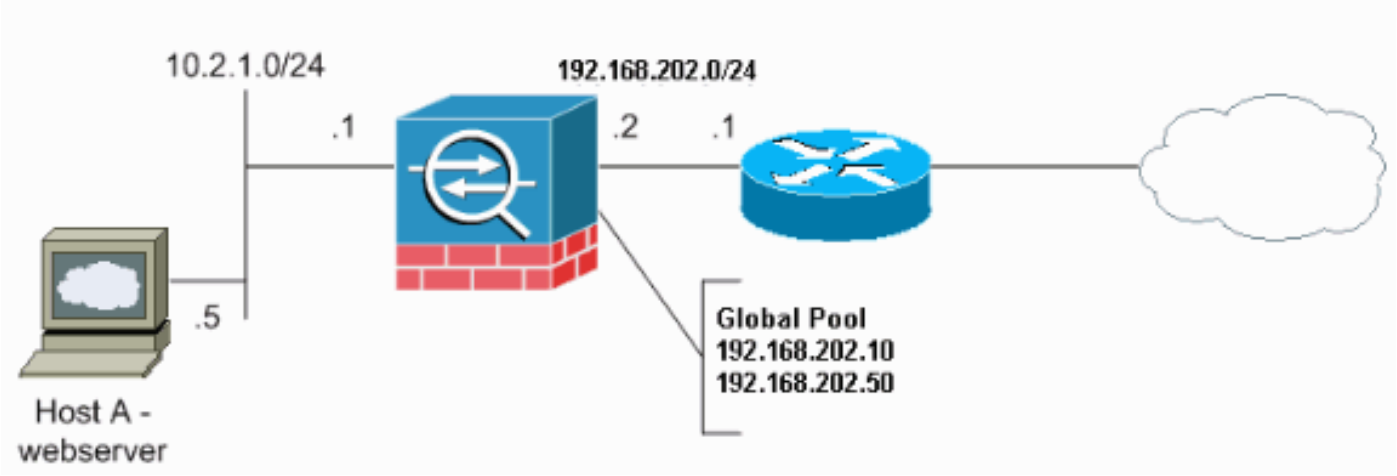
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

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

Como funciona a conectividade por meio do ASA

Nessa rede, o host A é o servidor da Web com o endereço interno 10.2.1.5. O servidor Web recebe um endereço externo (traduzido) de 192.168.202.5. Os usuários da Internet devem apontar para 192.168.202.5 para acessar o Servidor Web. A entrada DNS para o servidor Web precisa ser esse endereço. Nenhuma outra conexão é permitida a partir da Internet.



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

Configurar a conectividade por meio do Cisco ASA

Conclua estes passos para configurar a conectividade através do ASA:

1. Crie um objeto de rede que defina a sub-rede interna e outro objeto de rede para o intervalo do pool IP. Configure o NAT usando estes objetos de rede:

```
object network inside-net
subnet 0.0.0.0 0.0.0.0
```

```
object network outside-pat-pool
range 192.168.202.10 192.168.202.50
nat (inside,outside) source dynamic inside-net  outside-pat-pool
```

2. Atribua um endereço estático traduzido para o host interno ao qual os usuários da Internet têm acesso.

```
object network obj-10.2.1.5
  host 10.2.1.5
  nat (inside,outside) static 192.168.202.5
```

3. Use o comando **access-list** para permitir usuários externos através do Cisco ASA. Use sempre o endereço convertido no comando access-list.

```
access-list 101 permit tcp any host 192.168.202.5 eq www
  access-group 101 in interface outside
```

Permitir tráfego de broadcast ARP

O Security Appliance conecta a mesma rede em suas interfaces internas e externas. Como o firewall não é um salto roteado, você pode facilmente introduzir um firewall transparente em uma rede existente. O endereçamento IP novamente não é necessário. O tráfego IPv4 é permitido pelo firewall transparente automaticamente de uma interface de segurança mais alta para uma interface de segurança mais baixa, sem uma lista de acesso. Os ARPs (Address Resolution Protocols, Protocolos de Resolução de Endereços) são permitidos por meio do firewall transparente em ambas as direções sem uma lista de acesso. O tráfego ARP pode ser controlado pela inspeção ARP. Para o tráfego de Camada 3 que viaja de uma interface de baixo para uma de alta segurança, é necessária uma lista de acesso estendida.

Observação: o aplicativo de segurança de modo transparente não passa pacotes do Cisco Discovery Protocol (CDP) ou pacotes IPv6, ou pacotes que não têm um EtherType válido maior ou igual a 0x600. Por exemplo, você não pode passar pacotes IS-IS. É feita uma exceção para BPDUs (Bridge Protocol Data Units, unidades de dados de protocolo de ponte), que são suportadas.

Endereços MAC permitidos

Esses endereços MAC de destino são permitidos por meio do firewall transparente. Os endereços MAC que não estão nessa lista são descartados:

- Endereço MAC destino de broadcast TRUE igual a FFFF.FFFF.FFFF
- Endereços MAC multicast IPv4 de 0100.5E00.0000 a 0100.5EFE.FFFF
- Endereços MAC multicast IPv6 de 333.0000.0000 a 3333.FFFF.FFFF
- Endereço multicast BPDU igual a 0100.0CCC.CCCD
- Endereços MAC multicast Appletalk de 0900.0700.0000 a 0900.07FF.FFFF

Tráfego não permitido para passagem no modo de roteador

No modo de roteador, alguns tipos de tráfego não podem passar pelo Security Appliance mesmo

que você o permita em uma lista de acesso. O firewall transparente, no entanto, pode permitir quase todo o tráfego usando uma lista de acesso estendida (para tráfego IP) ou uma lista de acesso EtherType (para tráfego não IP).

Por exemplo, você pode estabelecer adjacências de protocolo de roteamento por meio de um firewall transparente. Você pode permitir o tráfego Open Shortest Path First (OSPF), Routing Information Protocol (RIP), Enhanced Interior Gateway Routing Protocol (EIGRP) ou Border Gateway Protocol (BGP) por meio de uma lista de acesso estendida. Da mesma forma, protocolos como o Hot Standby Router Protocol (HSRP) ou o Virtual Router Redundancy Protocol (VRRP) podem passar pelo Security Appliance.

O tráfego não IP (por exemplo, AppleTalk, IPX, BPDUs e MPLS) pode ser configurado para passar usando uma lista de acesso EtherType.

Para recursos que não são suportados diretamente no firewall transparente, você pode permitir a passagem de tráfego para que os roteadores upstream e downstream possam suportar a funcionalidade. Por exemplo, usando uma lista de acesso estendida, você pode permitir o tráfego do Dynamic Host Configuration Protocol (DHCP) (em vez do recurso de retransmissão de DHCP não suportado) ou o tráfego multicast como o criado por IP/TV.

Solucionar problemas de conectividade

Se os usuários da Internet não puderem acessar seu site, faça o seguinte:

1. Verifique se você inseriu os endereços de configuração corretamente:Endereço externo válidoEndereço interno corretoO DNS externo traduziu o endereço
2. Verifique se há erros na interface externa.O Cisco Security Appliance é pré-configurado para detectar automaticamente as configurações de velocidade e duplex em uma interface. No entanto, existem várias situações que podem fazer com que o processo de autonegociação falhe. Isso resulta em incompatibilidades de velocidade ou duplex (e problemas de desempenho). Para infraestrutura de rede de missão crítica, a Cisco codifica manualmente a velocidade e o duplex em cada interface para que não haja chance de erro. Esses dispositivos geralmente não se movem. Portanto, se você configurá-los corretamente, não precisará alterá-los.**Exemplo:**
   ```
   asa(config)#interface ethernet 0/0
   asa(config-if)#duplex full
   asa(config-if)#speed 100
   asa(config-if)#exit
   ```

   Em algumas situações, a codificação da velocidade e das configurações duplex leva à geração de erros. Portanto, você precisa configurar a interface para a configuração padrão do modo de detecção automática como mostrado neste exemplo:**Exemplo:**
   ```
   asa(config)#interface ethernet 0/0
   asa(config-if)#duplex auto
   asa(config-if)#speed auto
   asa(config-if)#exit
   ```

3. Se o tráfego não enviar ou receber através da interface do ASA ou do roteador de ponto inicial, tente limpar as estatísticas ARP.
   ```
   asa#clear arp
   ```

4. Use os comandos **show run object** e **show run static** para verificar se a tradução estática está habilitada.**Exemplo:**

```
object service www
service tcp source eq www
object network 192.168.202.2
host 192.168.202.2
object network 10.2.1.5
host 10.2.1.5
object service 1025
service tcp source eq 1025
nat (inside,outside) source static 10.2.1.5 192.168.202.2 service 1025 www
```

   Neste cenário, o endereço IP externo é usado como o endereço IP mapeado para o servidor Web.

```
nat (inside,outside) source dynamic 10.2.1.5 interface service 1025 www
```

5. Verifique se a rota padrão no servidor Web aponta para a interface interna do ASA.
6. Verifique a tabela de tradução usando o comando **show xlate** para ver se a tradução foi criada.
7. Use o comando **logging buffered** para verificar os arquivos de log para ver se há negações. (Procure o endereço traduzido e veja se você vê alguma negação.)
8. Use o comando **capture**:

```
access-list webtraffic permit tcp any host 192.168.202.5

capture capture1 access-list webtraffic interface outside
```

   Observação: esse comando gera uma quantidade significativa de saída. Pode fazer com que um roteador trave ou recarregue sob cargas de tráfego intensas.
9. Se os pacotes chegarem ao ASA, certifique-se de que sua rota para o servidor Web do ASA esteja correta. (Verifique os comandos **route** em sua configuração do ASA.)
10. Verifique se o proxy ARP está desabilitado. Emita o comando **show running-config sysopt** no ASA 8.3.Aqui, o proxy ARP é desativado pelo comando **sysopt noproxyarp outside**:

```
ciscoasa#show running-config sysopt
no sysopt connection timewait
sysopt connection tcpmss 1380
sysopt connection tcpmss minimum 0
no sysopt nodnsalias inbound
no sysopt nodnsalias outbound
no sysopt radius ignore-secret
sysopt noproxyarp outside
sysopt connection permit-vpn
```

    Para reativar o proxy ARP, insira este comando no modo de configuração global:

```
ciscoasa(config)#no sysopt noproxyarp outside
```

    Quando um host envia tráfego IP para outro dispositivo na mesma rede Ethernet, o host precisa saber o endereço MAC do dispositivo. O ARP é um protocolo da camada 2 que resolve um endereço IP para um endereço MAC. Um host envia uma solicitação ARP e pergunta "Quem é esse endereço IP?". O dispositivo proprietário do endereço IP responde: "Eu possuo esse endereço IP; aqui está meu endereço MAC."O Proxy ARP permite que o Security Appliance responda a uma solicitação ARP em nome dos hosts por trás dele. Ele

faz isso respondendo às solicitações ARP para os endereços mapeados estáticos desses hosts. O Security Appliance responde à solicitação com seu próprio endereço MAC e, em seguida, encaminha os pacotes IP para o host interno apropriado.Por exemplo, no diagrama neste documento, quando uma solicitação ARP é feita para o endereço IP global do servidor web, 192.168.202.5, o Security Appliance responde com seu próprio endereço MAC. Se o proxy ARP não estiver habilitado nessa situação, os hosts na rede externa do Security Appliance não poderão acessar o Servidor Web emitindo uma solicitação ARP para o endereço 192.168.202.5. Consulte a referência de comando para obter mais informações sobre o comando **sysopt**.

11. Se tudo parecer estar correto e os usuários ainda não puderem acessar o Servidor Web, abra um caso no Suporte Técnico da Cisco.

Mensagem de erro - %ASA-4-407001:

Alguns hosts não podem se conectar à Internet e à `Mensagem de Erro - %ASA-4-407001: Negar tráfego para local-host interface_name:inside_address, o limite de número excedido` mensagem de erro é recebido no syslog. Como solucionar esse erro?

Este mensagem de erro é recebida quando o número de usuários excede o limite de licenças utilizadas. Para resolver esse erro, atualize a licença para um número maior de usuários. Pode ser 50, 100 ou licença de usuário ilimitada, conforme necessário.

Informações Relacionadas

- Dispositivos de segurança adaptáveis Cisco ASA 5500 Series
- Avisos de campo de produtos de segurança (incluindo Cisco Adaptive Security Appliance (ASA))
- Solicitações de Comentários (RFCs)
- Suporte Técnico e Documentação - Cisco Systems