ASA 8.3: Estabeleça e pesquise defeitos a Conectividade através do dispositivo do Cisco Security

Índice

Introdução

Quando uma ferramenta de segurança adaptável de Cisco (ASA) é configurada inicialmente, tem uma política de segurança padrão onde todos no interior possa sair, e ninguém da parte externa possa obter dentro. 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.

Uma vez que você estabelece a conectividade básica através de Cisco ASA, você pode fazer alterações de configuração ao Firewall. Certifique-se que todas as alterações de configuração que você fizer ao ASA seja em conformidade com sua política de segurança do local.

Refira o PIX/ASA: Estabeleça e pesquise defeitos a Conectividade através do dispositivo do Cisco Security para a configuração idêntica em Cisco ASA com versões 8.2 e anterior.

Pré-requisitos

Requisitos

Este documento supõe que algumas configurações básicas têm sido terminadas já em Cisco ASA. Refira estes documentos para exemplos de uma configuração inicial ASA:

- ASA 8.3(x): Conecte uma única rede interna ao Internet
- Configurando o PPPoE Client em uma ferramenta de segurança adaptável de Cisco (ASA)

Componentes Utilizados

A informação neste documento é baseada em uma ferramenta de segurança adaptável de Cisco (ASA) essa versão 8.3 e mais recente das corridas.

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.

Como a Conectividade com o ASA trabalha

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

Nota: Os esquemas de endereçamento IP usados nesta configuração não são legalmente roteáveis na Internet. São os endereços da RFC1918 que foram usados em um ambiente de laboratório.

Configurar a Conectividade através de Cisco ASA

Termine estas etapas a fim configurar a Conectividade com o ASA:

1. Crie um objeto de rede que defina a sub-rede interna e um outro objeto de rede para a escala do IP pool. Configurar 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 traduzido estático para o host interno a que os usuários do Internet têm o 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** permitir usuários externos através de 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
   ```

Permita o tráfego de broadcast ARP

A ferramenta de segurança conecta a mesma rede em suas interfaces internas e externas.

Porque o Firewall não é um salto roteado, você pode facilmente introduzir um Firewall transparente a uma rede existente. O re-endereçamento IP não é necessário. O tráfego do IPv4 é permitido com o Firewall transparente automaticamente de uma interface de segurança mais elevada a uma interface de segurança mais baixa, sem uma lista de acessos. Os protocolos Protocolo de resolución de la dirección (ARP) (ARP) são permitidos com o Firewall transparente nos ambos sentidos sem uma lista de acessos. O tráfego ARP pode ser controlado pela inspeção ARP. Para o tráfego da camada 3 que viaja de um ponto baixo a uma relação da segurança elevada, uma lista de acesso extendida é exigida.

Nota: A ferramenta de segurança do modo transparente não passa pacotes do Cisco Discovery Protocol (CDP) ou pacotes do IPv6, ou nenhuns pacotes que não têm Ethertype superior ou igual a um 0x600 válidos. Por exemplo, você não pode passar pacotes IS-IS. Uma exceção é feita para o bridge protocol data units (BPDU), que são apoiadas.

Endereços permitidos MAC

Estes endereços MAC de destino são permitidos com o Firewall transparente. Os endereços MAC não nesta lista são deixados cair:

- RETIFIQUE o endereço MAC de destino da transmissão igual ao FFFF.FFFF.FFFF
- Endereços MAC de transmissão múltipla do IPv4 de 0100.5E00.0000 a 0100.5EFE.FFFF
- Endereços do Multicast IPv6 MAC de 3333.0000.0000 a 3333.FFFF.FFFF
- Endereço de multicast BPDU igual a 0100.0CCC.CCCD
- Endereços MAC de transmissão múltipla do APPLETALK de 0900.0700.0000 a 0900.07FF.FFFF

Tráfego não permitido passar no modo do roteador

No modo do roteador, alguns tipos de tráfego não podem passar através da ferramenta de segurança mesmo se você a permite em uma lista de acessos. O Firewall transparente, contudo, pode permitir quase todo o tráfego com da utilização de uma lista de acesso extendida (para o tráfego IP) ou de uma lista de acessos de Ethertype (para o tráfego não-IP).

Por exemplo, você pode estabelecer adjacências do protocolo de roteamento com um Firewall transparente. Você pode permitir o tráfego do Open Shortest Path First (OSPF), do Routing Information Protocol (RIP), do Enhanced Interior Gateway Routing Protocol (EIGRP), ou do Border Gateway Protocol (BGP) baseado completamente em uma lista de acesso extendida. Similarmente, os protocolos tais como o Hot Standby Router Protocol (HSRP) ou o Virtual Router Redundancy Protocol (VRRP) podem passar através da ferramenta de segurança.

O tráfego não-IP (por exemplo, APPLETALK, IPX, BPDU, e MPLS) pode ser configurado para atravessar a utilização de uma lista de acessos de Ethertype.

Para as características que não são apoiadas diretamente no Firewall transparente, você pode permitir que o tráfego passe completamente de modo que o Roteadores do fluxo acima e fluxo abaixo possa apoiar a funcionalidade. Por exemplo, usando uma lista de acesso extendida, você pode permitir o tráfego do protocolo de configuração dinâmica host (DHCP) (em vez dos recursos de Frame Relay DHCP unsupported) ou o tráfego multicast tal como isso criado pelo IP/TV.

Solucionar problemas de conectividade

Se os usuários do Internet não podem alcançar seu Web site, termine estas etapas:

1. Certifique-se de você ter incorporado corretamente endereços de configuração:Endereço externo válidoEndereço interno corretoO DNS externo traduziu o endereço
2. Verifique a interface externa para ver se há erros.O dispositivo do Cisco Security preconfigured auto-para detectar os ajustes da velocidade e duplexação em uma relação. Contudo, diversas situações existem que podem fazer com que o processo de auto-negociação falhe. Isto conduz à velocidade ou as incompatibilidades duplex (bidirecional) (e os problemas de desempenho). Para a infraestrutura de rede de missão crítica, Cisco não codifica manualmente a velocidade e duplexação em cada relação tão lá é nenhuma possibilidade para o erro. Estes dispositivos geralmente não se movem ao redor. Consequentemente, se você os configura corretamente, você não deve precisar de mudá-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, codificar os ajustes da velocidade e duplexação conduz à geração de erros. Consequentemente, você precisa de configurar a relação à configuração padrão de auto-detecta o modo enquanto este exemplo mostra:**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 envia nem recebe através da relação do ASA ou do roteador do fim do cabeçalho, tente cancelar as estatísticas ARP.`asa#clear arp`
4. Use o **objeto da corrida da mostra** e **mostre comandos static da corrida** a fim certificar-se de que a tradução estática está permitida.**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` Nesta encenação, o endereço IP externo é usado como o endereço IP de Um ou Mais Servidores Cisco ICM NT traçado para o servidor de Web.
   `nat (inside,outside) source dynamic 10.2.1.5 interface service 1025 www`
5. Verifique para ver que a rota padrão no servidor de Web aponta à interface interna do ASA.
6. Verifique a tabela de tradução usando o comando show xlate a fim ver se a tradução foi criada.
7. Use o comando logging buffered a fim verificar os arquivos de registro para ver se nega ocorrem. (Procure o endereço traduzido e veja se você vê alguns nega.)
8. Use o comando capture:
   `access-list webtraffic permit tcp any host 192.168.202.5 capture capture1 access-list webtraffic interface outside` **Nota:** Este comando gerencie uma quantidade significativa de saída. Pode fazer com que um roteador pendure ou recarregue sob cargas de tráfego pesado.
9. Se os pacotes o fazem ao ASA, certifique-se que sua rota ao servidor de Web do ASA está correta. (Verifique os comandos route em sua configuração ASA.)
10. Verifique para ver se o proxy ARP é desabilitado. Emita o comando show running-config sysopt em ASA 8.3.Aqui, o proxy ARP é desabilitado pelo **noproxyarp do sysopt fora do** comando:`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` A fim re-permitir o proxy ARP, incorpore este comando ao modo de configuração global:`ciscoasa(config)#no sysopt noproxyarp outside` Quando um host enviar o tráfego IP a um outro dispositivo na mesma rede Ethernet, as necessidades do host de conhecer o MAC address do dispositivo. O ARP é um protocolo da camada 2 que resolva um endereço IP de Um ou Mais Servidores Cisco ICM NT a um MAC address. Um host

envia uma requisição ARP e pede-a “quem é este endereço IP de Um ou Mais Servidores Cisco ICM NT?”. O dispositivo que possui o endereço IP de Um ou Mais Servidores Cisco ICM NT responde, “eu possuo esse endereço IP de Um ou Mais Servidores Cisco ICM NT; está aqui meu MAC address.”O proxy ARP permite que a ferramenta de segurança responda a uma requisição ARP em nome dos anfitriões atrás dele. Faz este respondendo às requisições ARP para os endereços traçados estática daqueles anfitriões. A ferramenta de segurança responde ao pedido com seu próprio MAC address, então para a frente os pacotes IP ao host interno apropriado.Por exemplo, no diagrama neste documento, quando uma requisição ARP é feita para o endereço IP global do servidor de Web, 192.168.202.5, a ferramenta de segurança responde com seu próprio MAC address. Se o proxy ARP não é permitido nesta situação, os anfitriões na rede externa da ferramenta de segurança não podem alcançar o servidor de Web emitindo uma requisição ARP para o endereço 192.168.202.5. Refira a referência de comandos para obter mais informações sobre do comando sysopt.

11. Se tudo parece estar correto, e os usuários ainda não podem alcançar o servidor de Web, abra um caso com Suporte técnico de Cisco.

Mensagem de Erro - %ASA-4-407001:

Alguns anfitriões não podem conectar ao Internet e ao `Mensagem de Erro - %ASA-4-407001: Negue o tráfego para o local-host interface_name: os inside_address, limite da licença de` Mensagem de Erro `excedido número` são recebidos no Syslog. Como solucionar esse erro?

Este mensagem de erro é recebida quando o número de usuários excede o limite de licenças utilizadas. A fim resolver este erro, promova a licença a um número mais alto de usuários. Esta pode ser 50 pés, 100, ou licença do usuário ilimitado como necessário.

Informações Relacionadas

- Cisco ASA 5500 Series Adaptive Security Appliances
- Field Notice de produto de segurança (que incluem a ferramenta de segurança adaptável de Cisco (ASA))
- Solicitações de Comentários (RFCs)
- Suporte Técnico e Documentação - Cisco Systems