PIX/ASA 7.x: Permita/comunicação do desabilitação entre relações

Índice

Introdução

Este documento fornece uma configuração de exemplo para várias formas de comunicação entre as interfaces no mecanismo de segurança ASA/PIX.

Pré-requisitos

Requisitos

Certifique-se de atender a estes requisitos antes de tentar esta configuração:

- Endereços IP de Um ou Mais Servidores Cisco ICM NT e atribuição do gateway padrão
- Conectividade da rede física entre dispositivos
- Número da porta de comunicação identificada para o serviço implementado.

Componentes Utilizados

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

- Adaptive Security Appliance com software versão 7.x ou posterior
- Windows 2003 server
- Estações de trabalho de Windows XP

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.

Produtos Relacionados

Esta configuração também pode ser utilizada com estas versões de hardware e software:

- PIX 500 Series Firewalls com software versão 7.x ou posterior

Convenções

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

Informações de Apoio

Este documento esboça os passos requerido para permitir que uma comunicação flua entre relações diferentes. Os formulários de uma comunicação tais como estes são discutidos:

1. Uma comunicação dos anfitriões que são ficados situados na parte externa que exige o acesso ao recurso localizou no DMZ
2. Uma comunicação dos anfitriões na rede interna que exigem o acesso aos recursos localizou no DMZ
3. Uma comunicação dos anfitriões no interior e a rede do DMZ que exijam o acesso aos recursos na parte externa

NAT

Em nosso exemplo, nós usamos o Network Address Translation (NAT) e a tradução de endereço de porta (PAT) em nossa configuração. A tradução de endereços substitui o endereço real (local) em um pacote com um endereço traçado que (global) seja roteável na rede de destino. O NAT é compreendido de duas etapas: o processo em que um endereço real é traduzido em um endereço traçado e o processo para desabotoar então a tradução para o tráfego que retorna. Há dois formulários da tradução de endereços que nós usamos neste manual de configuração: Estático e dinâmico.

As traduções dinâmica permitem que cada host use um endereço ou uma porta diferente para cada tradução subsequente. As traduções dinâmica podem ser usadas quando os host locais compartilham ou “esconda atrás” de uns ou vários endereços globais comuns. Neste modo, um endereço local não pode permanentemente reservar um endereço global para a tradução. Em lugar de, a tradução de endereços ocorre na muito-a-um ou muito-à-muito base, e as entradas de tradução são criadas somente enquanto são precisadas. Assim que uma entrada de tradução

estiver livre do uso, está suprimido e feito disponível a outros host locais. Este tipo de tradução é o mais útil para as conexões externas, em que host internos estão atribuídos um endereço dinâmico ou um número de porta somente enquanto as conexões são feitas. Há dois formulários da tradução de endereço dinâmico:

- NAT dinâmico - Os endereços locais são traduzidos no endereço global disponível seguinte em um pool. A tradução ocorre em uma base de um para um, assim que é possível esgotar o conjunto de endereço global se um número maior de host locais exige a tradução em um dado momento.
- Sobrecarga NAT (PANCADINHA) - Os endereços locais são traduzidos em um único endereço global; cada conexão está feita original quando o número de porta disponível seguinte da alta ordem do endereço global é atribuído como a fonte da conexão. A tradução ocorre na muito--um à base porque muitos host locais compartilham de um endereço global comum.

A conversão estática cria uma conversão fixa dos endereços reais para os endereços mapeados. Uma configuração do NAT estático traça o mesmo endereço para cada conexão por um host e é uma regra de tradução persistente. As traduções de endereço estático são usadas quando um interno ou um host local precisam de ter o mesmo endereço global para cada conexão. A tradução de endereços ocorre em uma base de um para um. As traduções estáticas podem ser definidas para um host único ou para todos os endereços contidos em uma sub-rede IP.

O principal diferença entre o NAT dinâmico e um intervalo de endereço para o NAT estático é que o NAT estático permite que um host remoto inicie uma conexão a um host traduzido (se há uma lista de acessos que o permita), quando o NAT dinâmico não fizer. Você igualmente precisa um número igual de endereços traçados com NAT estático.

A ferramenta de segurança traduz um endereço quando uma regra NAT combina o tráfego. Se nenhum fósforo da regra NAT, processando para o pacote continua. A exceção é quando você permite o controle NAT. O controle NAT exige que os pacotes que transversal de uma interface de segurança mais elevada (para dentro) a um fósforo mais baixo do nível de segurança (fora) uma regra NAT, ou então o processamento para o pacote param. A fim ver a informação de configuração comum, refira o documento PIX/ASA 7.x NAT e de PANCADINHA. Para obter informações mais detalhadas sobre o funcionamento do NAT, consulte o guia Como o NAT Funciona.

Dica: Sempre que você muda a configuração de NAT, recomenda-se que você cancela traduções de NAT atual. Você pode cancelar a tabela de tradução com o **comando clear xlate**. **Contudo, cuidado da tomada quando você fizer este** desde que cancelar a tabela de tradução desliga todas as conexões atual que usam traduções. O alternativo cancelando a tabela de tradução é esperar traduções atual para cronometrar para fora, mas este não está recomendado porque o comportamento inesperado pode resultar enquanto as novas conexões são criadas com as regras novas.

Níveis de segurança

Os controles de valor do nível de segurança como os anfitriões/dispositivos nas relações diferentes interagem um com o otro. À revelia, os anfitriões/dispositivos conectados às relações com os níveis de segurança mais elevados podem alcançar os anfitriões/dispositivos conectados para conectar com os níveis da baixo-Segurança. Os anfitriões/dispositivos conectados às relações com as interfaces de segurança mais baixa não podem alcançar anfitriões/dispositivos conectam às relações com as interfaces de segurança mais elevada sem a permissão das Listas

de acesso.

O comando do **nível de segurança** é novo à versão 7.0 e substitui a parcela do **comando nameif** que atribuiu o nível de segurança para uma relação. Duas relações, “o interior” e a “parte externa” conectam, têm níveis de segurança do padrão, mas estes podem ser cancelados com o comando do **nível de segurança**. Se você nomeia uma relação “para dentro,” está dada um nível de segurança do padrão de 100; uma relação nomeada “parte externa” é dada a um nível de segurança do padrão de 0. Todas relações recentemente adicionadas restantes recebem um nível de segurança do padrão de 0. a fim atribuir um nível de segurança novo a uma relação, usam o comando do **nível de segurança no** modo de comando interface. Os níveis de segurança variam de 1-100.

Nota: Os níveis de segurança são usados para determinar somente como o Firewall inspeciona e segura o tráfego. Por exemplo, trafique que as passagens de uma interface de segurança mais elevada para mais baixa estão enviadas com políticas padrão menos estritas do que o tráfego que vem de uma interface de segurança mais baixa para uma segurança mais elevada uma. Para obter mais informações sobre os níveis de segurança, consulte o Guia de Referência de Comandos do ASA/PIX 7.x.

ASA/PIX 7.x igualmente introduziu a capacidade para configurar interfaces múltiplas com o mesmo nível de segurança. Por exemplo, as interfaces múltiplas conectaram aos Parceiros ou outros DMZ podem tudo ser dados um nível de segurança dos 50 pés. À revelia, estas mesmas interfaces de segurança não podem comunicar-se um com o outro. A fim trabalhar em torno disto, o comando da inter-**relação da licença do same-security-traffic** foi introduzido. Este comando permite uma comunicação entre relações do mesmo nível de segurança. Para obter mais informações sobre da mesmo-Segurança entre relações, refira os parâmetros guideConfiguring da relação da referência de comandos, e veja este exemplo.

ACL

As listas de controle de acesso consistem tipicamente nas entradas de controle de acesso (ACE) múltiplas organizadas internamente pela ferramenta de segurança em uma lista vinculada. Os ACE descrevem um grupo de tráfego tal como aquele de um host ou de uma rede e alistam uma ação para aplicar-se a esse tráfego, geralmente permit or deny. Quando um pacote é sujeitado ao controle da lista de acessos, o dispositivo do Cisco Security procura esta lista vinculada dos ACE a fim encontrar um que combina o pacote. **O primeiro ACE que combina a ferramenta de segurança é esse que é aplicado ao pacote.** Uma vez que o fósforo é encontrado, a ação nesse ACE (permit or deny) está aplicada ao pacote.

Somente uma lista de acessos é permitida pela relação, pelo sentido. Isto significa que você pode somente ter uma lista de acessos que se aplica para traficar de entrada em uma relação e uma lista de acessos que se aplica para traficar de partida em uma relação. As Listas de acesso que não são aplicadas às relações, tais como NAT ACL, são ilimitadas.

Nota: À revelia, todas as listas de acesso têm um ACE implícito na extremidade que nega todo o tráfego, tão todo o tráfego que não combina nenhum ACE que você incorporar à lista de acessos combina o implícito nega na extremidade e é deixado cair. Você deve ter pelo menos uma indicação da licença em uma lista de acessos da relação para que o tráfego flua. Sem uma indicação da licença, todo o tráfego é negado.

Nota: A lista de acessos é executada com os **comandos access-list e access-group**. Esses comandos são usados em vez dos comandos **conduit** e **outbound** usados nas versões anteriores

do PIX Firewall Software. Para obter mais informações sobre ACLs, consulte Configurando Listas de Acesso de IP.

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 usa esta instalação de rede:

Configuração inicial

Este documento utiliza as seguintes configurações:

- Com esta configuração de firewall básica, não há atualmente nenhuma indicação NAT/STATIC.
- Nenhuma ACL é aplicada. Assim, a ACE implícita deny any any é usada.

Nome de dispositivo 1
ASA-AIP-CLI(config)#**show running-config** ASA Version 7.2(2) ! hostname ASA-AIP-CLI domain-name corp.com enable password WwXYvtKrnjXqGbu1 encrypted names ! interface Ethernet0/0 nameif Outside security-level 0 ip address 172.22.1.163 255.255.255.0 ! interface Ethernet0/1 nameif inside security-level 100 ip address 172.20.1.1 255.255.255.0 ! interface Ethernet0/2 nameif DMZ security-level 50 ip address 192.168.1.1 255.255.255.0 ! interface Ethernet0/3 nameif DMZ-2-testing security-level 50 ip address 192.168.10.1 255.255.255.0 ! interface Management0/0 shutdown no nameif no security-level no ip address ! passwd 2KFQnbNIdI.2KYOU encrypted ftp mode passive dns server-group DefaultDNS domain-name corp.com pager lines 24 mtu inside 1500 mtu Outside 1500 mtu DMZ 1500 no failover icmp unreachable rate-limit 1 burst-size 1 no asdm history enable arp timeout 14400 nat-control route Outside 0.0.0.0 0.0.0.0 172.22.1.1 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 mgcp-pat 0:05:00 timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 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 ! ! policy-map type inspect dns preset_dns_map parameters message-length maximum 512 policy-map global_policy class inspection_default inspect dns preset_dns_map 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 ! service-
policy global_policy global prompt hostname context
Cryptochecksum:4b2f54134e685d11b274ee159e5ed009 : end
ASA-AIP-CLI(config)#
```

DMZ ao interior

A fim permitir uma comunicação do DMZ aos anfitriões da rede interna, use estes comandos. Neste exemplo, um servidor de Web no DMZ precisa de alcançar um AD e um servidor DNS no interior.

1. Crie uma entrada NAT estática para o server AD/DNS no DMZ. O NAT estático cria uma tradução fixa de um endereço real a um endereço traçado. Este endereço traçado é um endereço que os anfitriões DMZ possam usar para alcançar o server no interior sem a necessidade de conhecer o endereço real do server. Este comando traça o endereço 192.168.2.20 DMZ ao endereço interno real 172.20.1.5.`Netmask estático 255.255.255.255 ASA-AIP-CLI(config)# (para dentro, DMZ) 192.168.2.20 172.20.1.5`
2. Os ACL são exigidos para permitir que uma relação com um nível de segurança mais baixo tenha o acesso a um nível de segurança mais elevado. Neste exemplo, nós damos o servidor de Web que se senta no acesso DMZ (50 pés da Segurança) ao server AD/DNS no interior (Segurança 100) com estas portas específicas do serviço: DNS, Kerberos, e LDAP.`Domínio estendido DMZtoInside do eq de 192.168.2.20 do host de 192.168.1.10 do host UDP da licença da lista de acesso ASA-AIP-CLI(config)#Eq estendido DMZtoInside 88 de 192.168.2.20 do host de 192.168.1.10 do host tcp da licença da lista de acesso ASA-AIP-CLI(config)#Eq estendido DMZtoInside 389 de 192.168.2.20 do host de 192.168.1.10 do host UDP da licença da lista de acesso ASA-AIP-CLI(config)#`**Nota:** O acesso da licença ACL ao endereço traçado do server AD/DNS que foi criado neste exemplo e não no endereço interno real.
3. Nesta etapa, você aplica o ACL à relação DMZ na direção de entrada com este comando:`ASA-AIP-CLI(config)# acesso-grupo DMZtoInside na relação DMZ`**Nota:** Se você quer obstruir ou desabilitar a porta 88, o tráfego do DMZ a para dentro, por exemplo, usa este:`ASA-AIP-CLI(config)# no access-list DMZtoInside extended permit tcp host 192.168.1.10 host 192.168.2.20 eq 88`**Dica:** Sempre que você muda a configuração de NAT, recomenda-se que você cancela traduções de NAT atual. Você pode cancelar a tabela de tradução com o **comando clear xlate**. **Exercite o cuidado quando você faz este** desde que cancelar a tabela de tradução desliga todas as conexões atual que usam traduções. O alternativo cancelando a tabela de tradução é esperar as traduções atual para cronometrar para fora, mas este não está recomendado porque o comportamento inesperado pode resultar enquanto as novas conexões são criadas com as regras novas.Outras configurações comum incluem estes:Server do correio no DMZO SSH alcança para dentro e foraSessões de Área de Trabalho Remota permitidas via dispositivos PIX/ASAOutras soluções de DNS usadas na DMZ

Internet ao DMZ

A fim permitir uma comunicação dos usuários no Internet, ou a interface externa (Segurança 0), a um servidor de Web que seja ficado situado no DMZ (50 pés da Segurança), usa estes comandos:

1. Crie uma tradução estática para o servidor de Web no DMZ à parte externa. O NAT estático cria uma tradução fixa de um endereço real a um endereço traçado. Este endereço traçado é um endereço que os anfitriões no Internet possam usar para alcançar o servidor de Web no DMZ sem a necessidade de conhecer o endereço real do server. Este comando traça o endereço exterior 172.22.1.25 ao endereço real 192.168.1.10 DMZ.`Netmask estático 255.255.255.255 ASA-AIP-CLI(config)# (DMZ, fora) 172.22.1.25 192.168.1.10`
2. Crie um ACL que permita que os usuários da parte externa alcancem o servidor de Web através do endereço traçado. Note que o servidor de Web igualmente hospeda o FTP.`ASA-AIP-CLI(config)# a lista de acesso OutsidetoDMZ estendeu a licença tcp todo o eq WWW de 172.22.1.25 do hostASA-AIP-CLI(config)# a lista de acesso OutsidetoDMZ estendeu a licença tcp todo o ftp do eq de 172.22.1.25 do host`
3. A última etapa nesta configuração é aplicar o ACL à interface externa para o tráfego na direção de entrada.`ASA-AIP-CLI(config)# acesso-grupo OutsidetoDMZ na relação fora`**Nota:** Recorde, você pode somente aplicar uma lista de acessos pela relação, pelo sentido. Se você já tem um ACL de entrada aplicado à interface externa, você não pode aplicar-lhe este exemplo ACL. Em lugar de adicionar os ACE neste exemplo no ACL atual que é aplicado à relação.**Nota:** Se você quer obstruir ou desabilitar o tráfego FTP do Internet ao DMZ, por exemplo, usa esta:`ASA-AIP-CLI(config)# no access-list OutsidetoDMZ extended permit tcp any host 172.22.1.25 eq ftp`**Dica:** Sempre que você muda a configuração de NAT, recomenda-se que você cancela traduções de NAT atual. Você pode cancelar a tabela de tradução com o **comando clear xlate**. **Exercite o cuidado quando você faz este** desde que cancelar a tabela de tradução desliga todas as conexões atual que usam traduções. O alternativo cancelando a tabela de tradução é esperar traduções atual para cronometrar para fora, mas este não está recomendado porque o comportamento inesperado pode resultar enquanto as novas conexões são criadas com as regras novas.

Inside/DMZ ao Internet

Nesta encenação, os anfitriões situados na interface interna (Segurança 100) da ferramenta de segurança são fornecidos com o acesso ao Internet na interface externa (Segurança 0). Isto é conseguido com a sobrecarga da PANCADINHA, ou NAT, formulário do NAT dinâmico. Ao contrário das outras encenações, um ACL não é exigido neste caso porque os anfitriões em uma relação da segurança elevada alcançam anfitriões em uma relação da baixo-Segurança.

1. Especifique as origens do tráfego que devem ser convertidas. A regra número **1** NAT é definida aqui, e todo o tráfego do interior e anfitriões DMZ é permitido.`ASA-AIP-CLI(config)# (para dentro) 1 172.20.1.0 nat 255.255.255.0ASA-AIP-CLI(config)# (para dentro) 1 192.168.1.0 nat 255.255.255.0`
2. Especifique que endereço, o conjunto de endereços, ou conecta o tráfego do NATed deve se usar quando alcançar a interface externa. Neste caso, a PANCADINHA é executada com o endereço de interface externa. Isto é especialmente útil quando o endereço de interface externa não é sabido de antemão, como dentro uma configuração de DHCP. Aqui, o comando global é emitido com o mesmo ID do NAT de **1**, que o amarra às regras NAT do mesmo ID.`(Fora) 1 relação ASA-AIP-CLI(config)# global`

Dica: Sempre que você muda a configuração de NAT, recomenda-se que você cancela traduções de NAT atual. Você pode cancelar a tabela de tradução com o **comando clear xlate**. **Exercite o cuidado quando você faz este** desde que cancelar a tabela de tradução desliga todas as conexões atual que usam traduções. O alternativo cancelando a tabela de tradução é esperar traduções atual para cronometrar para fora, mas este não está recomendado porque o

comportamento inesperado pode resultar enquanto as novas conexões são criadas com as regras novas.

Nota: Se você quer obstruir o tráfego da zona de segurança mais elevada (para dentro) à zona de Segurança mais baixa (internet/DMZ), crie um ACL e aplique-o à interface interna do PIX/ASA como de entrada.

Nota: Exemplo: Para bloquear o tráfego da porta 80 do host 172.20.1.100 da rede interna para a Internet, execute:

```
ASA-AIP-CLI(config)#access-list InsidetoOutside extended deny tcp host 172.20.1.100 any eq www
ASA-AIP-CLI(config)#access-list InsidetoOutside extended permit tcp any any
ASA-AIP-CLI(config)#access-group InsidetoOutside in interface inside
```

A mesma comunicação do nível de segurança

A configuração inicial mostra que as relações “DMZ” e "DMZ-2-testing" estão configuradas com nível de segurança (50 pés); à revelia, estas duas relações não podem falar. Aqui nós permitimos que estas relações falem com este comando:

```
Inter-relação da licença do same-security-traffic ASA-AIP-CLI(config)#
```

Nota: Mesmo que da “a inter-relação da licença do tráfego mesmo-Segurança” seja configurada para as mesmas relações do nível de segurança (“DMZ” e "DMZ-2-testing"), ainda precisa uma regra de tradução (estática/dinâmica) alcançar os recursos colocados naquelas relações.

Troubleshooting

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

- Troubleshooting de conexões via PIX e ASA
- NAT ConfigurationsVerify NAT e Troubleshooting

Informações Relacionadas

- Referência de comandos de Cisco ASA
- Referência de comando PIX de Cisco
- Erro de Cisco ASA e mensagens de sistemas
- Erro de Cisco PIX e mensagens de sistemas
- Suporte Técnico e Documentação - Cisco Systems