PIX/ASA 7.2(1) e mais atrasado: Comunicações Intra-Interface

Índice

Introdução

Este documento ajuda a resolver problemas comuns que ocorrem ao habilitar as comunicações entre interfaces em um Mecanismo de Segurança Adaptável (ASA) ou PIX que opera na versão de software 7.2(1) e mais recente. O Software Release 7.2(1) inclui a capacidade de distribuir dados do texto claro dentro e fora da mesma relação. Para habilitar este recurso, execute o comando **same-security-traffic permit intra-interface**. Este documento supõe que o administrador de rede permitiu estes característica ou planos a no futuro. A configuração e o Troubleshooting são fornecidos usando o comando line interface(cli).

Nota: Este documento centra-se sobre os dados (unencrypted) claros que chegam e saem do ASA. Os dados criptografados não são discutidos.

A fim permitir uma comunicação da intra-relação em ASA/PIX para a configuração IPSec, refira o PIX/ASA e o cliente VPN para os Internet públicas VPN em um exemplo de configuração da vara.

A fim permitir uma comunicação da intra-relação no ASA para a configuração de SSL, refira ASA 7.2(2): Cliente VPN SSL (SVC) para os Internet públicas VPN em um exemplo de configuração da vara.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Listas de acesso
- Roteamento
- Intrusion Prevention System (IPS) do Módulo de serviços da inspeção avançada e da Prevenção-Segurança (AIP-SSM) — o conhecimento deste módulo é somente necessário se o módulo é instalado e operacional.
- Software Release 5.x IPS — O conhecimento do software IPS não é exigido se o AIP-SSM não é dentro uso.

Componentes Utilizados

- ASA 5510 7.2(1) e mais atrasado
- AIP-SSM-10 que opera o software 5.1.1 IPS

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 pode igualmente ser usada com o Cisco 500 Series PIX que executa a versão 7.2(1) e mais recente.

Convenções

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

Informações de Apoio

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.

Esta tabela mostra o ASA que começa a configuração:

ASA
ciscoasa#**show running-config** : Saved : ASA Version 7.2(1) ! hostname ciscoasa enable password 8Ry2YjIyt7RRXU24 encrypted names ! *!--- The IP addressing assigned to interfaces.* interface Ethernet0/0 nameif inside security-level 100 ip address 10.1.1.2 255.255.255.0 ! interface Ethernet0/1 nameif outside security-level 0 ip address 172.22.1.160 255.255.255.0 ! interface Ethernet0/2 shutdown no nameif no security-level no ip address ! interface Management0/0 shutdown no nameif no security-level no ip address ! passwd

```
2KFQnbNIdI.2KYOU encrypted ftp mode passive !--- Notice
that there are no access-lists. pager lines 24 logging
enable logging buffered debugging mtu inside 1500 mtu
outside 1500 no asdm history enable arp timeout 14400 !-
-- There are no network address translation (NAT) rules.
!--- The static routes are added for test purposes.
route inside 10.2.2.0 255.255.255.0 10.1.1.100 1 route
outside 172.16.10.0 255.255.255.0 172.22.1.29 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:
```

Troubleshooting

Estas seções ilustram diversos cenários de configuração, mensagens do syslog relacionados, e saídas do pacote-projétil luminoso com relação às comunicações da intra-relação.

Comunicações da Intra-relação não permitidas

Na configuração ASA, tentativas de 172.22.1.6 do host de sibilar o host 172.16.10.1. O host 172.22.1.6 envia um pacote de requisição de eco ICMP ao gateway padrão (ASA). as comunicações da Intra-relação não foram permitidas no ASA. O ASA deixa cair o pacote de requisição de eco. O sibilo do teste falha. O ASA é usado para pesquisar defeitos o problema.

Este exemplo mostra a saída dos mensagens do syslog e de um pacote-projétil luminoso:

- Este é o mensagem do syslog registrado ao buffer:`ciscoasa(config)#`**`show logging`** *`!--- Output is suppressed.`* `%ASA-3-106014: Deny inbound icmp src outside:172.22.1.6 dst outside:172.16.10.1 (type 8, code 0)`
- Isto é o pacote-projétil luminoso output:`ciscoasa(config)#`**`packet-tracer input outside icmp 172.22.1.6 8 0 172.16.10.1 detailed`** `Phase: 1 Type: FLOW-LOOKUP Subtype: Result: ALLOW Config: Additional Information: Found no matching flow, creating a new flow Phase: 2 Type: ROUTE-LOOKUP Subtype: input Result: ALLOW Config: Additional Information: in 172.16.10.0 255.255.255.0 outside Phase: 3 Type: ACCESS-LIST Subtype:` ***`Result: DROP`*** `Config:` ***`Implicit Rule`*** *`!--- Implicit rule refers to configuration rules not configured !--- by the user. By default, intra-interface communication is not permitted. !--- In this example, the user has not enabled intra-interface communications !--- and therefore the traffic is implicitly denied.`* `Additional Information: Forward Flow based lookup yields rule: in id=0x3bd8480, priority=111, domain=permit, deny=true hits=0, user_data=0x0, cs_id=0x0, flags=0x4000, protocol=0 src ip=0.0.0.0, mask=0.0.0.0, port=0 dst ip=0.0.0.0, mask=0.0.0.0, port=0 Result: input-interface: outside input-status: up input-line-status: up output-interface: outside output-status: up output-line-status: up Action: drop Drop-reason: (acl-drop) Flow is denied by configured rule`

O equivalente dos comandos CLI no ASDM é mostrado nestas figuras:

Passo 1:

Passo 2:

A saída do pacote-projétil luminoso com o **comando intra-interface da licença do same-security-traffic** desabilitado.

A saída do rastreador de pacotes drop...implicit rule sugere que uma opção de configuração padrão está bloqueando o tráfego. O administrador precisa de verificar a configuração running a fim assegurar-se de que comunicações da intra-relação esteja permitida. Neste caso, a configuração ASA precisa comunicações da intra-relação de ser permitida (intra-**relação da licença do same-security-traffic**).

```
ciscoasa#show running-config !--- Output is suppressed. interface Ethernet5 shutdown no nameif
no security-level no ip address ! passwd 2KFQnbNIdI.2KYOU encrypted ftp mode passive same-
security-traffic permit intra-interface !--- When intra-interface communications are enabled,
the line !--- highlighted in bold font appears in the configuration. The configuration line !---
appears after the interface configuration and before !--- any access-list configurations.
access-list... access-list...
```

Comunicações da Intra-relação permitidas

as comunicações da Intra-relação são permitidas agora. O comando **same-security-traffic permit intra-interface** é adicionado à configuração anterior. Tentativas de 172.22.1.6 do host de sibilar o host 172.16.10.1. O host 172.22.1.6 envia um pacote de requisição de eco ICMP ao gateway padrão (ASA). Respostas bem sucedidas dos registros de 172.22.1.6 do host de 172.16.10.1. O ASA passa o tráfego ICMP com sucesso.

Estes exemplos mostram as saídas do mensagem do syslog e do pacote-projétil luminoso ASA:

- Estes são os mensagens do syslog registrados ao buffer:`ciscoasa#show logging !--- Output is suppressed. %PIX-7-609001: Built local-host outside:172.22.1.6 %PIX-7-609001: Built local-host outside:172.16.10.1 %PIX-6-302020: Built ICMP connection for faddr 172.22.1.6/64560 gaddr 172.16.10.1/0 laddr 172.16.10.1/0 %PIX-6-302021: Teardown ICMP connection for faddr 172.22.1.6/64560 gaddr 172.16.10.1/0 laddr 172.16.10.1/0 %PIX-7-609002: Teardown local-host outside:172.22.1.6 duration 0:00:04 %PIX-7-609002: Teardown local-host outside:172.16.10.1 duration 0:00:04`
- Isto é o pacote-projétil luminoso output:`ciscoasa(config)#packet-tracer input outside icmp 172.22.1.6 8 0 172.16.10.1 Phase: 1 Type: FLOW-LOOKUP Subtype: Result: ALLOW Config: Additional Information: Found no matching flow, creating a new flow Phase: 2 Type: ROUTE-LOOKUP Subtype: input Result: ALLOW Config: Additional Information: in 172.16.10.0 255.255.255.0 outside Phase: 3 Type: ACCESS-LIST Subtype: Result: ALLOW Config: Implicit Rule Additional Information: Phase: 4 (Type: IP-OPTIONS Subtype: Result: ALLOW Config: Additional Information: Phase: 5 Type: INSPECT Subtype: np-inspect Result: ALLOW Config: Additional Information: Phase: 6 Type: FLOW-CREATION Subtype: Result: ALLOW Config: Additional Information: New flow created with id 23, packet dispatched to next module Phase: 7 Type: ROUTE-LOOKUP Subtype: output and adjacency Result: ALLOW Config: Additional Information: found next-hop 172.22.1.29 using egress ifc outside adjacency Active next-hop mac address 0030.a377.f854 hits 0 Result: input-interface: outside input-status: up input-line-status: up output-interface: outside output-status: up output-line-status: up Action: allow` O equivalente dos comandos CLI no ASDM é mostrado nestas figuras:**Passo 1:Passo 2:**A saída do pacote-projétil luminoso com o **comando intra-interface da licença do same-security-traffic** permitido.**Nota:** Nenhuma lista de acesso é aplicada à interface externa. Na configuração de exemplo, a interface externa recebe o nível de segurança 0. Por padrão, o firewall não permite o tráfego de uma interface de baixa segurança para uma interface de alta

segurança. Isto pôde conduzir administradores acreditar que o tráfego da intra-relação não está permitido (na relação exterior da baixa Segurança) sem permissão de uma lista de acesso. Contudo, as mesmas passagens do tráfego da relação livremente quando nenhuma lista de acesso for aplicada à relação.

Intra-relação permitida e tráfego passado ao AIP-SSM para a inspeção

o tráfego da Intra-relação pode ser passado ao AIP-SSM para a inspeção. Esta seção supõe que o administrador configurou o ASA para enviar o tráfego ao AIP-SSM e o administrador sabe configurar o software IPS 5.x.

Neste momento a configuração ASA contém a configuração de exemplo precedente, as comunicações da intra-relação são permitidas, e todo o (algum) tráfego é enviado ao AIP-SSM. A assinatura 2004 IPS é alterada para deixar cair o tráfego da requisição de eco. Tentativas de 172.22.1.6 do host de sibilar o host 172.16.10.1. O host 172.22.1.6 envia um pacote de requisição de eco ICMP ao gateway padrão (ASA). O ASA para a frente o pacote de requisição de eco ao AIP-SSM para a inspeção. O AIP-SSM deixa cair o pacote de dados pela configuração IPS.

Estes exemplos mostram o mensagem do syslog e o pacote-projétil luminoso ASA output:

- Este é o mensagem do syslog registrado ao buffer:`ciscoasa(config)#`**`show logging`** *`!--- Output is suppressed.`* `%ASA-4-420002: IPS requested to drop ICMP packet from outside:172.22.1.6/2048 to outside:172.16.10.1/0` *`!--- ASA syslog message records the IPS request !--- to drop the ICMP traffic.`*
- Isto é o pacote-projétil luminoso output:`ciscoasa#`**`packet-tracer input outside icmp 172.22.1.6 8 0 172.16.10.1`** `Phase: 1 Type: FLOW-LOOKUP Subtype: Result: ALLOW Config: Additional Information: Found no matching flow, creating a new flow Phase: 2 Type: ROUTE-LOOKUP Subtype: input Result: ALLOW Config: Additional Information: in 172.16.10.0 255.255.255.0 outside Phase: 3 Type: ACCESS-LIST Subtype: Result: ALLOW Config: Implicit Rule Additional Information: Phase: 4 Type: IP-OPTIONS Subtype: Result: ALLOW Config: Additional Information: Phase: 5 Type: INSPECT Subtype: np-inspect Result: ALLOW Config: Additional Information: Phase: 6 Type: IDS Subtype:` ***`Result: ALLOW`*** `Config:` ***`class-map traffic_for_ips match any policy-map global_policy class traffic_for_ips ips inline fail-open service-policy global_policy global`*** *`!--- The packet-tracer recognizes that traffic is to be sent to the AIP-SSM. !--- The packet-tracer does not have knowledge of how the !--- IPS software handles the traffic.`* `Additional Information: Phase: 7 Type: FLOW-CREATION Subtype: Result: ALLOW Config: Additional Information: New flow created with id 15, packet dispatched to next module Result: input-interface: outside input-status: up input-line-status: up output-interface: outside output-status: up output-line-status: up` ***`Action: allow`*** *`!--- From the packet-tracer perspective the traffic is permitted. !--- The packet-tracer does not interact with the IPS configuration. !--- The packet-tracer indicates traffic is allowed even though the IPS !--- might prevent inspected traffic from passing.`*

Éimportante notar que os administradores devem usar tantas como ferramentas de Troubleshooting como possíveis quando pesquisam um problema. Este exemplo mostra como duas ferramentas de Troubleshooting diferentes podem pintar imagens diferentes. Ambas as ferramentas dizem junto uma história completa. A política da configuração ASA permite o tráfego mas a configuração IPS não faz.

Intra-relação permitida e Listas de acesso aplicadas a uma relação

Esta seção usa a configuração de exemplo original neste documento, em comunicações da intra-relação permitidas, e em uma lista de acesso aplicada à relação testada. Estas linhas são adicionadas à configuração. A lista de acesso é pretendida ser uma representação simples do que pôde ser configurado em um Firewall da produção.

```
ciscoasa(config)#access-list outside_acl permit tcp any host 172.22.1.147 eq 80
ciscoasa(config)#access-group outside_acl in interface outside !--- Production firewalls also
have NAT rules configured. !--- This lab tests intra-interface communications. !--- NAT rules
are not required.
```

Tentativas de 172.22.1.6 do host de sibilar o host 172.16.10.1. O host 172.22.1.6 envia um pacote de requisição de eco ICMP ao gateway padrão (ASA). O ASA deixa cair o pacote de requisição de eco pelas regras da lista de acesso. O sibilo do teste de 172.22.1.6 do host falha.

Estes exemplos mostram o mensagem do syslog e o pacote-projétil luminoso ASA output:

- Este é o mensagem do syslog registrado ao buffer:`ciscoasa(config)#show logging !--- Output is suppressed. %ASA-4-106023: Deny icmp src outside:172.22.1.6 dst outside:172.16.10.1 (type 8, code 0) by access-group "outside_acl" [0xc36b9c78, 0x0]`
- Isto é o pacote-projétil luminoso output:`ciscoasa(config)#packet-tracer input outside icmp 172.22.1.6 8 0 172.16.10.1 detailed Phase: 1 Type: FLOW-LOOKUP Subtype: Result: ALLOW Config: Additional Information: Found no matching flow, creating a new flow Phase: 2 Type: ROUTE-LOOKUP Subtype: input Result: ALLOW Config: Additional Information: in 172.16.10.0 255.255.255.0 outside Phase: 3 Type: ACCESS-LIST Subtype: Result: DROP Config: Implicit Rule !--- The implicit deny all at the end of an access-list prevents !--- intra-interface traffic from passing. Additional Information: Forward Flow based lookup yields rule: in id=0x264f010, priority=11, domain=permit, deny=true hits=0, user_data=0x5, cs_id=0x0, flags=0x0, protocol=0 src ip=0.0.0.0, mask=0.0.0.0, port=0 dst ip=0.0.0.0, mask=0.0.0.0, port=0 Result: input-interface: outside input-status: up input-line-status: up output-interface: outside output-status: up output-line-status: up Action: drop Drop-reason: (acl-drop) Flow is denied by configured rule`

Refira o pacote-projétil luminoso para obter mais informações sobre do comando do pacote-**projétil luminoso**.

Nota: No evento que a lista de acesso aplicada à relação inclui uma instrução de negação, a saída do pacote-projétil luminoso muda. Por exemplo:

```
ciscoasa(config)#access-list outside_acl permit tcp any host 172.22.1.147 eq 80
ciscoasa(config)#access-list outside_acl deny ip any any ciscoasa(config)#access-group
outside_acl in interface outside ciscoasa#packet-tracer input outside icmp 172.22.1.6 8 0
172.16.10.1 detailed !--- Output is suppressed. Phase: 3 Type: ACCESS-LIST Subtype: log Result:
DROP Config: access-group outside_acl in interface outside access-list outside_acl extended deny
ip any any Additional Information: Forward Flow based lookup yields rule:
```

O equivalente dos comandos CLI acima no ASDM é mostrado nestas figuras:

Passo 1:

Passo 2:

A saída do pacote-projétil luminoso com o **comando intra-interface da licença do same-security-traffic** permitido e o **comando deny ip any any estendido outside_acl da lista de acesso** configurado para negar pacotes.

Se as comunicações da intra-relação estão desejadas em uma interface particular e as listas de acesso estão aplicadas à mesma relação, as regras da lista de acesso devem permitir o tráfego da intra-relação. Com o uso dos exemplos nesta seção, a lista de acesso precisa de ser redigida como:

```
ciscoasa(config)#access-list outside_acl permit tcp any host 172.22.1.147 eq 80
ciscoasa(config)#access-list outside_acl permit ip 172.22.1.0 255.255.255.0 172.16.10.0
255.255.255.0 !--- 172.22.1.0 255.255.255.0 represents a locally !--- connected network on the
ASA. !--- 172.16.10.0 255.255.255.0 represents any network that !--- 172.22.1.0/24 needs to
access. ciscoasa(config)#access-list outside_acl deny ip any any ciscoasa(config)#access-group
```

```
outside_acl in interface outside
```
O equivalente dos comandos CLI acima no ASDM é mostrado nestas figuras:

Passo 1:

Passo 2:

A saída do pacote-projétil luminoso com o **comando intra-interface da licença do same-security-traffic** permitido e o **comando deny ip any any estendido outside_acl da lista de acesso** configurado na mesma relação onde o tráfego da intra-relação é desejado.

Refira a lista de acesso estendida e o acesso-grupo para obter mais informações sobre dos **comandos access-list e access-group**.

Intra-relação permitida com estática e NAT

Esta seção explica uma encenação onde um usuário interno esteja tentando alcançar o servidor de Web interno com seu endereço público.

Neste caso, o cliente em 192.168.100.2 quer usar o endereço público do servidor WWW (por exemplo, 172.20.1.10). Os serviços DNS para o cliente são proporcionados pelo servidor DNS externo em 172.22.1.161. Porque o servidor DNS é ficado situado em uma outra rede pública, não conhece o endereço IP privado do servidor WWW. Em lugar de, o servidor DNS conhece o endereço traçado servidor WWW de 172.20.1.10.

Aqui este tráfego da interface interna tem que ser traduzido e redistribuído através da interface interna para alcançar o servidor WWW. Isto é chamado hairpinning. Isto pode ser executado com estes comandos:

```
same-security-traffic permit intra-interface global (inside) 1 interface nat (inside) 1
192.168.100.0 255.255.255.0 static (inside,inside) 172.20.1.10 192.168.100.10 netmask
255.255.255.255
```
Para detalhes de configuração completos e mais informação sobre o hairpinning, refira o hairpinning com uma comunicação da Intra-relação.

Lista de acesso com visão de futuro

Não todas as políticas de acesso do Firewall são as mesmas. Algumas políticas de acesso são mais específicas do que outro. Na intra-relação do evento as comunicações estão permitidas e o Firewall não tem uma lista de acesso aplicada a todas as relações, ele pôde vale adicionando uma lista de acesso então as comunicações da intra-relação são permitidas. A lista de acesso aplicada precisa de permitir comunicações da intra-relação assim como de manter outras exigências da política de acesso.

Este exemplo ilustra este ponto. O ASA conecta uma rede privada (interface interna) ao Internet (interface externa). A interface interna ASA não tem uma lista de acesso aplicada. À revelia, todo o tráfego IP é permitido do interior à parte externa. A sugestão é adicionar uma lista de acesso que olhe qualquer outra coisa semelhante output:

```
access-list inside_acl permit ip <locally connected network> <all other internal networks>
access-list inside_acl permit ip any any access-group inside_acl in interface inside
```

Este grupo de listas de acesso continua a permitir todo o tráfego IP. as linhas da lista de acesso específicas para as comunicações intra-interface lembram aos administradores que as comunicações intra-interface devem ser permitidas por uma lista de acesso aplicada.

Informações Relacionadas

- Referência de comandos do dispositivo do Cisco Security, versão 7.2
- Mensagens de Log de sistema do dispositivo do Cisco Security, versão 7.2
- Cisco PIX Firewall Software
- ASA: Exemplo de Configuração para Envio de Tráfego de Rede do ASA para o AIP-SSM
- Sustentação do produto do Dispositivos de segurança adaptáveis Cisco ASA série 5500
- Suporte Técnico e Documentação - Cisco Systems