PIX/ASA: Execute o DNS Doctoring com o comando static e o exemplo de configuração de duas relações NAT

Índice

Introdução

Este documento fornece uma configuração de exemplo para executar o Domain Name System (DNS) que medica na ferramenta de segurança adaptável do 5500 Series ASA ou na ferramenta de segurança da série PIX 500 usando indicações da tradução de endereço da rede estática (NAT). Medicar DNS permite que a ferramenta de segurança reescreva Um-registros DNS.

A reescrita DNS executa duas funções:

- Traduz um endereço público (o roteável ou o endereço traçado) em uma resposta DNS a um endereço privado (o endereço real) quando o cliente de DNS está em uma interface confidencial.
- Traduz um endereço privado a um endereço público quando o cliente de DNS está na

interface pública.

Nota: A configuração neste documento contém duas relações NAT; para dentro e fora. Para um exemplo do DNS que medica com estatísticas e três relações NAT (para dentro, exterior e dmz), refira o PIX/ASA: Execute o DNS Doctoring com o comando static e o exemplo de configuração de três relações NAT.

Refira PIX/ASA 7.x NAT e indicações e utilização nat, globais, estáticas, conduíte, e comandos access-list e redirecionamento de porta da PANCADINHA (transmissão) no PIX para obter mais informações sobre de como usar o NAT em uma ferramenta de segurança.

Pré-requisitos

Requisitos

A inspeção DNS deve ser permitida a fim executar o DNS que medica na ferramenta de segurança. A inspeção DNS está ligada à revelia. Se foi desligada, veja a seção da inspeção configurar DNS mais atrasada neste documento re-para permiti-lo. Quando a inspeção DNS é permitida, a ferramenta de segurança executa estas tarefas:

- Traduz o registro DNS baseado na configuração terminada usando a **estática** e os **comandos nat** (reescrita DNS). A tradução aplica-se somente ao Um-registro na resposta DNS. Consequentemente, consultas reversas, que pedem o registro PTR, não são afetados pela reescrita DNS.**Nota:** A reescrita DNS não é compatível com tradução de endereço da porta estática (PANCADINHA) porque as regras múltiplas da PANCADINHA são aplicáveis para cada Um-registro, e a regra da PANCADINHA a usar-se é ambígua.
- Reforça o tamanho da mensagem do máximo DNS (o padrão é 512 bytes e o comprimento máximo é 65535 bytes). A remontagem é executada como necessário para verificar que o comprimento do pacote é menos do que o comprimento máximo configurado. O pacote é deixado cair se excede o comprimento máximo.**Nota:** Se você emite o comando **dns da inspeção** sem a opção do comprimento máximo, o tamanho de pacote de DNS não está verificado.
- Reforça um comprimento do Domain Name de 255 bytes e um comprimento da etiqueta de 63 bytes.
- Verifica a integridade do Domain Name referido pelo ponteiro se os ponteiros da compressão são encontrados na mensagem DNS.
- Verifica para ver se um laço do ponteiro da compressão existe.

Componentes Utilizados

A informação neste documento é baseada no 5500 Series ferramenta de segurança ASA, versão 7.2(1).

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 a ferramenta de segurança da série do Cisco PIX 500, versão 6.2 ou mais recente.

Nota: A configuração do Cisco Adaptive Security Device Manager (ASDM) é aplicável à versão 7.x somente.

Convenções

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

Informações de Apoio

Em uma troca típica DNS um cliente envia uma URL ou um hostname a um servidor DNS a fim determinar o endereço IP de Um ou Mais Servidores Cisco ICM NT desse host. O servidor DNS recebe o pedido, olha acima o mapeamento do nome-à-IP-endereço para esse host, e fornece então o Um-registro o endereço IP de Um ou Mais Servidores Cisco ICM NT ao cliente. Quando este procedimento trabalhar bem em muitas situações, os problemas podem ocorrer. Estes problemas podem ocorrer quando o cliente e o host que o cliente tenta alcançar são ambos na mesma rede privada atrás do NAT, mas o servidor DNS usado pelo cliente está em uma outra rede pública.

Encenação: Duas relações NAT (para dentro, fora)

Topologia

Nesta encenação, o cliente e o servidor WWW que o cliente tenta alcançar são ambos situados na interface interna do ASA. A PANCADINHA dinâmica é configurada para permitir o acesso do cliente ao Internet. O NAT estático com uma lista de acesso é configurado para permitir o acesso de servidor ao Internet, assim como permite que os host de Internet alcancem o servidor WWW.

Este diagrama é um exemplo desta situação. Neste caso, o cliente em 192.168.100.2 quer usar **server.example.com** URL para alcançar o servidor WWW em 192.168.100.10. 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, conhece o endereço traçado servidor WWW de 172.20.1.10. Assim, o servidor DNS contém o mapeamento do IP-endereço-à-nome de **server.example.com a 172.20.1.10**.

Problema: O cliente não pode alcançar o servidor WWW

Sem medicar DNS ou uma outra solução permitido nesta situação, se o cliente envia um pedido DNS para o endereço IP de Um ou Mais Servidores Cisco ICM NT de server.example.com, é incapaz de alcançar o servidor WWW. Isto é porque o cliente recebe um Um-registro que contenha o endereço público traçado: 172.20.1.10 do servidor WWW. Quando o cliente tenta alcançar este endereço IP de Um ou Mais Servidores Cisco ICM NT, a ferramenta de segurança deixa cair os pacotes porque não permite o redirecionamento de pacote na mesma relação. É aqui o que a parcela NAT da configuração olha como quando medicar DNS não é permitido:

```
ciscoasa(config)#show running-config : Saved : ASA Version 7.2(1) ! hostname ciscoasa !---
```

```
Output suppressed. access-list OUTSIDE extended permit tcp any host 172.20.1.10 eq www !---
Output suppressed. global (outside) 1 interface nat (inside) 1 192.168.100.0 255.255.255.0
static (inside,outside) 172.20.1.10 192.168.100.10 netmask 255.255.255.255 access-group OUTSIDE
in interface outside !--- Output suppressed.
```

Este é o que a configuração olha como no ASDM quando medicar DNS não é permitido:

Está aqui uma captura de pacote de informação dos eventos quando medicar DNS não é permitido:

1. O cliente envia a pergunta DNS.No. Time Source Destination Protocol Info
   1 0.000000 **192.168.100.2 172.22.1.161 DNS Standard query A server.example.com** Frame 1 (78 bytes on wire, 78 bytes captured) Ethernet II, Src: Cisco_c8:e4:00 (00:04:c0:c8:e4:00), Dst: Cisco_9c:c6:1f (00:0a:b8:9c:c6:1f) Internet Protocol, Src: 192.168.100.2 (192.168.100.2), Dst: 172.22.1.161 (172.22.1.161) User Datagram Protocol, Src Port: 50879 (50879), Dst Port: domain (53) Domain Name System (query) [Response In: 2] Transaction ID: 0x0004 Flags: 0x0100 (Standard query) Questions: 1 Answer RRs: 0 Authority RRs: 0 Additional RRs: 0 **Queries server.example.com: type A, class IN Name: server.example.com Type: A (Host address) Class: IN (0x0001)**
2. A PANCADINHA é executada na pergunta DNS pelo ASA e a pergunta é enviada. Note que o endereço de origem do pacote mudou à interface externa do ASA.No. Time Source Destination Protocol Info
   1 0.000000 **172.20.1.2** 172.22.1.161 DNS Standard query A server.example.com Frame 1 (78 bytes on wire, 78 bytes captured) Ethernet II, Src: Cisco_9c:c6:1e (00:0a:b8:9c:c6:1e), Dst: Cisco_01:f1:22 (00:30:94:01:f1:22) Internet Protocol, Src: 172.20.1.2 (172.20.1.2), Dst: 172.22.1.161 (172.22.1.161) User Datagram Protocol, Src Port: 1044 (1044), Dst Port: domain (53) Domain Name System (query) [Response In: 2] Transaction ID: 0x0004 Flags: 0x0100 (Standard query) Questions: 1 Answer RRs: 0 Authority RRs: 0 Additional RRs: 0 Queries server.example.com: type A, class IN Name: server.example.com Type: A (Host address) Class: IN (0x0001)
3. O servidor DNS responde com o endereço traçado do servidor WWW.No. Time Source Destination Protocol Info
   2 0.005005 **172.22.1.161 172.20.1.2 DNS Standard query response A 172.20.1.10** Frame 2 (94 bytes on wire, 94 bytes captured) Ethernet II, Src: Cisco_01:f1:22 (00:30:94:01:f1:22), Dst: Cisco_9c:c6:1e (00:0a:b8:9c:c6:1e) Internet Protocol, Src: 172.22.1.161 (172.22.1.161), Dst: 172.20.1.2 (172.20.1.2) User Datagram Protocol, Src Port: domain (53), Dst Port: 1044 (1044) Domain Name System (response) [Request In: 1] [Time: 0.005005000 seconds] Transaction ID: 0x0004 Flags: 0x8580 (Standard query response, No error) Questions: 1 Answer RRs: 1 Authority RRs: 0 Additional RRs: 0 Queries server.example.com: type A, class IN Name: server.example.com Type: A (Host address) Class: IN (0x0001) **Answers server.example.com: type A, class IN, addr 172.20.1.10 Name: server.example.com Type: A (Host address) Class: IN (0x0001) Time to live: 1 hour Data length: 4 Addr: 172.20.1.10**
4. O ASA desabotoa a tradução do endereço de destino da resposta de DNS e para a frente do pacote ao cliente. Note que sem medicar DNS permitido, o **ADDR na** resposta é ainda o endereço traçado do servidor WWW.No. Time Source Destination Protocol Info
   2 0.005264 172.22.1.161 **192.168.100.2** DNS Standard query response A 172.20.1.10 Frame 2 (94 bytes on wire, 94 bytes captured) Ethernet II, Src: Cisco_9c:c6:1f (00:0a:b8:9c:c6:1f), Dst: Cisco_c8:e4:00 (00:04:c0:c8:e4:00) Internet Protocol, Src: 172.22.1.161 (172.22.1.161), Dst: 192.168.100.2 (192.168.100.2) User Datagram Protocol, Src Port: domain (53), Dst Port: 50879 (50879) Domain Name System (response) [Request In: 1] [Time: 0.005264000 seconds] Transaction ID: 0x0004 Flags: 0x8580 (Standard query response, No error) Questions: 1 Answer RRs: 1 Authority RRs: 0 Additional RRs: 0 Queries server.example.com: type A, class IN Name: server.example.com Type: A (Host address) Class: IN (0x0001) **Answers server.example.com: type A, class IN, addr 172.20.1.10 Name: server.example.com Type: A (Host address) Class: IN (0x0001) Time to live: 1 hour Data length: 4 Addr: 172.20.1.10**
5. Neste momento, o cliente tenta alcançar o servidor WWW em 172.20.1.10. O ASA cria uma entrada de conexão para esta comunicação. Contudo, porque não permite que o tráfego flua

do interior à parte externa a para dentro, o tempo de conexão para fora. Os logs ASA mostram este:

```
%ASA-6-302013: Built outbound TCP connection 54175 for
outside:172.20.1.10/80 (172.20.1.10/80) to inside:192.168.100.2/11001
(172.20.1.2/1024)

%ASA-6-302014: Teardown TCP connection 54175 for outside:172.20.1.10/80 to
inside:192.168.100.2/11001 duration 0:00:30 bytes 0 SYN Timeout
```

Solução: palavra-chave “dns”

DNS Doctoring com a palavra-chave “dns”

O DNS que medica com a palavra-chave **dns** dá à ferramenta de segurança a capacidade para interceptar e para reescrever os índices do servidor DNS responde ao cliente. Quando configurada corretamente, a ferramenta de segurança pode alterar o Um-registro para permitir o cliente em tal encenação como discutido no problema: O cliente não pode alcançar a seção do servidor WWW para conectar. Nesta situação, com medicar DNS permitido, a ferramenta de segurança reescreve o Um-registro para dirigir o cliente a **192.168.100.10**, em vez de **172.20.1.10**. Medicar DNS é permitido quando você adiciona a palavra-chave **dns a uma** indicação do NAT estático. É aqui o que a parcela NAT da configuração olha como quando medicar DNS é permitido:

```
ciscoasa(config)#show run : Saved : ASA Version 7.2(1) ! hostname ciscoasa !--- Output
suppressed. access-list OUTSIDE extended permit tcp any host 172.20.1.10 eq www !--- Output
suppressed. global (outside) 1 interface nat (inside) 1 192.168.100.0 255.255.255.0 static
(inside,outside) 172.20.1.10 192.168.100.10 netmask 255.255.255.255 dns !--- The "dns" keyword
is added to instruct the security appliance to modify !--- DNS records related to this entry.
access-group OUTSIDE in interface outside !--- Output suppressed.
```

Termine estas etapas a fim configurar o DNS que medica no ASDM:

1. Navegue à **configuração > ao NAT** e escolha a regra do NAT estático a ser alterada. O clique **edita**.
2. **Opções NAT do** clique**….**
3. Verificam a **tradução DNS respondem esse fósforo a** caixa de verificação da **regra de tradução**.
4. **APROVAÇÃO do** clique para deixar o indicador das opções NAT. Clique a **APROVAÇÃO** para deixar o indicador da regra do NAT estático da edição. O clique **aplica-se** para enviar sua configuração à ferramenta de segurança.

Está aqui uma captura de pacote de informação dos eventos quando medicar DNS é permitido:

1. O cliente envia a pergunta DNS.

```
No.     Time       Source           Destination
Protocol Info
1       0.000000   192.168.100.2 172.22.1.161 DNS Standard query A server.example.com Frame
1 (78 bytes on wire, 78 bytes captured) Ethernet II, Src: Cisco_c8:e4:00
(00:04:c0:c8:e4:00), Dst: Cisco_9c:c6:1f (00:0a:b8:9c:c6:1f) Internet Protocol, Src:
192.168.100.2 (192.168.100.2), Dst: 172.22.1.161 (172.22.1.161) User Datagram Protocol, Src
Port: 52985 (52985), Dst Port: domain (53) Domain Name System (query) [Response In: 2]
Transaction ID: 0x000c Flags: 0x0100 (Standard query) Questions: 1 Answer RRs: 0 Authority
RRs: 0 Additional RRs: 0 Queries server.example.com: type A, class IN Name:
server.example.com Type: A (Host address) Class: IN (0x0001)
```

2. A PANCADINHA é executada na pergunta DNS pelo ASA e a pergunta é enviada. Note que o endereço de origem do pacote mudou à interface externa do ASA.

```
No.     Time       Source
Destination         Protocol Info
1       0.000000   172.20.1.2 172.22.1.161 DNS Standard query A server.example.com Frame 1
```

(78 bytes on wire, 78 bytes captured) Ethernet II, Src: Cisco_9c:c6:1e (00:0a:b8:9c:c6:1e), Dst: Cisco_01:f1:22 (00:30:94:01:f1:22) Internet Protocol, Src: 172.20.1.2 (172.20.1.2), Dst: 172.22.1.161 (172.22.1.161) User Datagram Protocol, Src Port: 1035 (1035), Dst Port: domain (53) Domain Name System (query) [Response In: 2] Transaction ID: 0x000c Flags: 0x0100 (Standard query) Questions: 1 Answer RRs: 0 Authority RRs: 0 Additional RRs: 0 Queries server.example.com: type A, class IN Name: server.example.com Type: A (Host address) Class: IN (0x0001)

3. O servidor DNS responde com o endereço traçado do servidor WWW.No. Time Source Destination Protocol Info
2 0.000992 **172.22.1.161 172.20.1.2 DNS Standard query response A 172.20.1.10** Frame 2 (94 bytes on wire, 94 bytes captured) Ethernet II, Src: Cisco_01:f1:22 (00:30:94:01:f1:22), Dst: Cisco_9c:c6:1e (00:0a:b8:9c:c6:1e) Internet Protocol, Src: 172.22.1.161 (172.22.1.161), Dst: 172.20.1.2 (172.20.1.2) User Datagram Protocol, Src Port: domain (53), Dst Port: 1035 (1035) Domain Name System (response) [Request In: 1] [Time: 0.000992000 seconds] Transaction ID: 0x000c Flags: 0x8580 (Standard query response, No error) Questions: 1 Answer RRs: 1 Authority RRs: 0 Additional RRs: 0 Queries server.example.com: type A, class IN Name: server.example.com Type: A (Host address) Class: IN (0x0001) **Answers server.example.com: type A, class IN, addr 172.20.1.10 Name: server.example.com Type: A (Host address) Class: IN (0x0001) Time to live: 1 hour Data length: 4 Addr: 172.20.1.10**
4. O ASA desabotoa a tradução do endereço de destino da resposta de DNS e para a frente do pacote ao cliente. Note que com medicar DNS permitido, o **ADDR na** resposta está reescrito para ser o endereço real do servidor WWW.No. Time Source Destination Protocol Info
2 0.001251 **172.22.1.161 192.168.100.2 DNS Standard query response A 192.168.100.10** Frame 2 (94 bytes on wire, 94 bytes captured) Ethernet II, Src: Cisco_9c:c6:1f (00:0a:b8:9c:c6:1f), Dst: Cisco_c8:e4:00 (00:04:c0:c8:e4:00) Internet Protocol, Src: 172.22.1.161 (172.22.1.161), Dst: 192.168.100.2 (192.168.100.2) User Datagram Protocol, Src Port: domain (53), Dst Port: 52985 (52985) Domain Name System (response) [Request In: 1] [Time: 0.001251000 seconds] Transaction ID: 0x000c Flags: 0x8580 (Standard query response, No error) Questions: 1 Answer RRs: 1 Authority RRs: 0 Additional RRs: 0 Queries server.example.com: type A, class IN Name: server.example.com Type: A (Host address) Class: IN (0x0001) **Answers server.example.com: type A, class IN, addr 192.168.100.10 Name: server.example.com Type: A (Host address) Class: IN (0x0001) Time to live: 1 hour Data length: 4 Addr: 192.168.100.10** *!--- 172.20.1.10 has been rewritten to be 192.168.100.10.*
5. Neste momento, o cliente tenta alcançar o servidor WWW em 192.168.100.10. A conexão sucede. O sem tráfego é capturado no ASA porque o cliente e servidor está na mesma sub-rede.

Configuração final com a palavra-chave “dns”

Esta é a configuração final do ASA para executar o DNS que medica com a palavra-chave **dns** e as duas relações NAT.

Configuração final ASA 7.2(1)
ciscoasa(config)#**show running-config** : Saved : ASA Version 7.2(1) ! hostname ciscoasa enable password 9jNfZuG3TC5tCVH0 encrypted names dns-guard ! interface Ethernet0/0 nameif outside security-level 0 ip address 172.20.1.2 255.255.255.0 ! interface Ethernet0/1 nameif inside security-level 100 ip address 192.168.100.1 255.255.255.0 ! interface Ethernet0/2 shutdown no nameif no security-level no ip address ! interface Management0/0 shutdown no nameif no security-level no ip address management-only ! passwd 2KFQnbNIdI.2KYOU encrypted ftp mode passive **access-list OUTSIDE extended permit tcp any host 172.20.1.10 eq www** *!--- Simple access-list that permits HTTP access to the mapped !--- address of the WWW server.* pager lines 24 logging enable logging buffered debugging mtu outside 1500 mtu inside

```
1500 asdm image disk0:/asdm512-k8.bin no asdm history
enable arp timeout 14400 global (outside) 1 interface
nat (inside) 1 192.168.100.0 255.255.255.0 static
(inside,outside) 172.20.1.10 192.168.100.10 netmask
255.255.255.255 dns !--- PAT and static NAT
configuration. The DNS keyword instructs !--- the
security appliance to rewrite DNS records related to
this entry. access-group OUTSIDE in interface outside !-
-- The Access Control List (ACL) that permits HTTP
access !--- to the WWW server is applied to the outside
interface. route outside 0.0.0.0 0.0.0.0 172.20.1.1 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
username cisco password ffIRPGpDSOJh9YLq encrypted http
server enable 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 MY_DNS_INSPECT_MAP parameters message-length maximum
512 !--- DNS inspection map. policy-map global_policy
class inspection_default inspect ftp inspect h323 h225
inspect h323 ras inspect rsh inspect rtsp inspect esmtp
inspect sqlnet inspect skinny inspect sunrpc inspect
xdmcp inspect sip inspect netbios inspect tftp inspect
dns MY_DNS_INSPECT_MAP !--- DNS inspection is enabled
using the configured map. inspect icmp policy-map type
inspect dns migrated_dns_map_1 parameters message-length
maximum 512 ! service-policy global_policy global prompt
hostname context
Cryptochecksum:a4a38088109887c3ceb481efab3dcf32 : end
```

Solução alternativa: Hairpinning

Hairpinning com NAT estático

Cuidado: O hairpinning com NAT estático envolve enviar todo o tráfego entre o cliente e o servidor WWW através da ferramenta de segurança. Considere com cuidado a quantidade de tráfego prevista e as capacidades de sua ferramenta de segurança antes que você execute esta solução.

O hairpinning é o processo por que o tráfego é enviado para trás para fora à mesma relação em que chegou. Esta característica foi introduzida na versão de software 7.0 da ferramenta de segurança. Para versões mais cedo de 7.2(1), exige-se que pelo menos um braço do tráfego hairpinned (de entrada ou de partida) esteja cifrado. De 7.2(1) e mais atrasado, esta exigência é já não no lugar. O tráfego de entrada e o tráfego de partida puderam ser unencrypted quando você o uso 7.2(1).

O hairpinning, conjuntamente com uma indicação do NAT estático, pode ser usado para conseguir o mesmo efeito que medicar DNS. Este método não muda os índices do Um-registro DNS que é retornado do servidor DNS ao cliente. Em lugar de, quando o hairpinning é usado, como na encenação discutida neste documento, o cliente pode usar o endereço de **172.20.1.10** que é retornado pelo servidor DNS a fim conectar.

Éaqui o que a porção relevante da configuração olha como quando você usa o hairpinning e o

NAT estático para conseguir um efeito medicando DNS. Os comandos em corajoso são explicados em maiores detalhes na extremidade desta saída:

```
ciscoasa(config)#show run : Saved : ASA Version 7.2(1) ! hostname ciscoasa !--- Output
suppressed. same-security-traffic permit intra-interface !--- Enable hairpinning. global
(outside) 1 interface !--- Global statement for client access to the Internet. global (inside) 1
interface !--- Global statment for hairpinned client access through !--- the security appliance.
nat (inside) 1 192.168.100.0 255.255.255.0 !--- The NAT statement defines which traffic should
be natted. !--- The whole inside subnet in this case. static (inside,outside) 172.20.1.10
192.168.100.10 netmask 255.255.255.255 !--- Static NAT statement mapping the WWW server's real
address to a !--- public address on the outside interface. static (inside,inside) 172.20.1.10
192.168.100.10 netmask 255.255.255.255 !--- Static NAT statment mapping requests for the public
IP address of !--- the WWW server that appear on the inside interface to the WWW server's !---
real address of 192.168.100.10.
```

- **same-security-traffic** — Este comando permite o tráfego do mesmo nível de segurança de transitar pela ferramenta de segurança. As palavras-chaves da intra-**relação da licença** concedem que same-security-traffic incorporar e deixar a mesma relação, assim o hairpinning é permitido.**Nota:** Refira o same-security-traffic para obter mais informações sobre do hairpinning e do **comando same-security-traffic**.
- **(para dentro) 1 relação global** — Todo o tráfego que cruza a ferramenta de segurança deve se submeter ao NAT. Este comando usa o endereço da interface interna da ferramenta de segurança a fim permitir o tráfego que incorpora a interface interna para se submeter à PANCADINHA enquanto hairpinned para trás para fora a interface interna.
- **(para dentro, para dentro) netmask estático 255.255.255.255 de 172.20.1.10 192.168.100.10** — esta entrada NAT estática cria um segundo mapeamento para o endereço IP público do servidor WWW. Contudo, ao contrário da primeira entrada NAT estática, esta vez o endereço 172.20.1.10 é traçado à interface interna da ferramenta de segurança. Isto permite que a ferramenta de segurança responda aos pedidos que vê para este endereço na interface interna. Então, reorienta aqueles pedidos ao endereço real do servidor WWW com se.

Termine estas etapas a fim configurar o hairpinning com o NAT estático no ASDM:

1. Navegue ao **configuração > interfaces**.
2. Na parte inferior do indicador, verifique o **tráfego da possibilidade entre dois ou mais anfitriões conectados à mesma** caixa de **verificação de interface**.
3. Clique em Apply.
4. Navegue à **configuração > ao NAT** e escolha **adicionam a regra do NAT estático do > Add….**
5. Preenchem a configuração para a tradução estática nova.Povoe a área do **endereço real** com a informação do servidor WWW.Povoe a área da **tradução estática** com o endereço e a relação a que você quer traçar o servidor WWW.Neste caso, a interface interna é escolhida permitir que os anfitriões na interface interna alcancem o servidor WWW através do endereço traçado 172.20.1.10.
6. Clique a **APROVAÇÃO** para deixar o indicador da regra do NAT estático adicionar.
7. Escolha a tradução dinâmica existente da PANCADINHA e o clique **edita**.
8. Escolha **para dentro da** caixa do pulldown da relação.
9. Clique em Add.
10. Escolha a **tradução de endereço de porta (PAT)** marcada botão de rádio **usando o endereço IP de Um ou Mais Servidores Cisco ICM NT da relação**. Clique em Add.
11. Clique a **APROVAÇÃO** para deixar o indicador do conjunto de endereço global adicionar. **APROVAÇÃO do** clique para deixar à edição o indicador dinâmico da regra NAT. O clique **aplica-se** para enviar sua configuração à ferramenta de segurança.

Está aqui a sequência de evento que ocorre quando o hairpinning é configurado. Supõe que o

cliente tem perguntado o servidor DNS e tem recebido já uma resposta de **172.20.1.10** para o endereço do servidor WWW:

1. O cliente tenta contactar o servidor WWW em 172.20.1.10.`%ASA-7-609001: Built local-host inside:192.168.100.2`
2. A ferramenta de segurança vê o pedido e reconhece que o servidor WWW está em 192.168.100.10.`%ASA-7-609001: Built local-host inside:192.168.100.10`
3. A ferramenta de segurança cria uma tradução dinâmica da PANCADINHA para o cliente. A fonte do tráfego do cliente é agora a interface interna da ferramenta de segurança: 192.168.100.1.`%ASA-6-305011: Built dynamic TCP translation from inside:192.168.100.2/11012 to inside:`**`192.168.100.1/1026`**
4. A ferramenta de segurança cria uma conexão de TCP entre o cliente e o servidor WWW com se. Note os endereços traçados de cada host entre parênteses.`%ASA-6-302013: Built inbound TCP connection 67399 for inside:192.168.100.2/11012` **`(192.168.100.1/1026)`** `to inside:192.168.100.10/80` **`(172.20.1.10/80)`**
5. **O comando show xlate na** ferramenta de segurança verifica que o tráfego do cliente traduz através da ferramenta de segurança.`ciscoasa(config)#`**`show xlate`** `3 in use, 9 most used Global 172.20.1.10 Local 192.168.100.10 Global 172.20.1.10 Local 192.168.100.10` **`PAT Global 192.168.100.1(1027) Local 192.168.100.2(11013)`**
6. **O comando show conn na** ferramenta de segurança verifica que a conexão sucedeu entre a ferramenta de segurança e o servidor WWW em nome do cliente. Note o endereço real do cliente entre parênteses.`ciscoasa#`**`show conn`** `TCP out 192.168.100.1`**`(192.168.100.2)`**`:11019 in 192.168.100.10:80 idle 0:00:03 bytes 1120 flags UIOB`

Configuração final com hairpinning e NAT estático

Esta é a configuração final do ASA que usa o hairpinning e o NAT estático para conseguir um efeito medicando DNS com duas relações NAT.

Configuração final ASA 7.2(1)

```
ciscoasa(config-if)#show running-config : Saved : ASA
Version 7.2(1) ! hostname ciscoasa enable password
9jNfZuG3TC5tCVH0 encrypted names dns-guard ! interface
Ethernet0/0 nameif outside security-level 0 ip address
172.20.1.2 255.255.255.0 ! interface Ethernet0/1 nameif
inside security-level 100 ip address 192.168.100.1
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 management-only ! passwd 2KFQnbNIdI.2KYOU
encrypted ftp mode passive same-security-traffic permit
intra-interface access-list OUTSIDE extended permit tcp
any host 172.20.1.10 eq www !--- Simple access-list that
permits HTTP access to the mapped !--- address of the
WWW server. pager lines 24 logging enable logging
buffered debugging mtu outside 1500 mtu inside 1500 asdm
image disk0:/asdm512-k8.bin no asdm history enable arp
timeout 14400 global (outside) 1 interface !--- Global
statement for client access to the Internet. global
(inside) 1 interface !--- Global statment for hairpinned
client access through !--- the security appliance. nat
(inside) 1 192.168.100.0 255.255.255.0 !--- The NAT
statement defines which traffic should be natted. !---
The whole inside subnet in this case. static
(inside,outside) 172.20.1.10 192.168.100.10 netmask
```

```
255.255.255.255 !--- Static NAT statement mapping the
WWW server's real address to a public !--- address on
the outside interface. static (inside,inside)
172.20.1.10 192.168.100.10 netmask 255.255.255.255 !---
Static NAT statement mapping requests for the public IP
address of the !--- WWW server that appear on the inside
interface to the WWW server's real address !--- of
192.168.100.10. access-group OUTSIDE in interface
outside !--- The ACL that permits HTTP access to the WWW
server is applied !--- to the outside interface. route
outside 0.0.0.0 0.0.0.0 172.20.1.1 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
username cisco password ffIRPGpDSOJh9YLq encrypted http
server enable 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 MY_DNS_INSPECT_MAP parameters message-length maximum
512 policy-map global_policy class inspection_default
inspect ftp inspect h323 h225 inspect h323 ras inspect
rsh inspect rtsp inspect esmtp inspect sqlnet inspect
skinny inspect sunrpc inspect xdmcp inspect sip inspect
netbios inspect tftp inspect dns MY_DNS_INSPECT_MAP
inspect icmp policy-map type inspect dns
migrated_dns_map_1 parameters message-length maximum 512
! service-policy global_policy global prompt hostname
context Cryptochecksum:7c9b4e3aff085ba90ee194e079111e1d
: end
```

Nota: Refira este vídeo, Hair-Pinning em Cisco ASA (clientes registrados somente), para obter mais informações sobre das encenações diferentes onde o Hair-Pinning poderia ser usado.

Configurar a inspeção DNS

A fim permitir a inspeção DNS (se tem sido desabilitada previamente), execute estas etapas. Neste exemplo, a inspeção DNS é adicionada à política global da inspeção do padrão, que é aplicada globalmente por um **comando service-policy** como se o ASA começou com uma configuração padrão. Refira a utilização da estrutura de política modular para obter mais informações sobre das políticas de serviços e da inspeção.

1. Crie um mapa de política da inspeção para o DNS.`ciscoasa(config)#`**`policy-map type inspect dns MY_DNS_INSPECT_MAP`**
2. Do modo da configuração de mapa de política, entre no modo da configuração de parâmetro para especificar parâmetros para o motor da inspeção.`ciscoasa(config-pmap)#`**`parameters`**
3. No modo da configuração de parâmetro do mapa de política, especifique o tamanho da mensagem do maxiumum para que as mensagens DNS sejam 512.`ciscoasa(config-pmap-p)#`**`message-length maximum 512`**
4. Retire fora do modo da configuração de parâmetro do mapa de política e do modo da configuração de mapa de política.`ciscoasa(config-pmap-p)#`**`exit`** `ciscoasa(config-pmap)#`**`exit`**
5. Confirme que o mapa de política da inspeção esteve criado como desejado.`ciscoasa(config)#`**`show run policy-map type inspect dns`** `! policy-map type inspect dns MY_DNS_INSPECT_MAP parameters message-length maximum 512 !`

6. Entre no modo da configuração de mapa de política para o **global_policy**.`ciscoasa(config)#policy-map global_policy ciscoasa(config-pmap)#`
7. No modo da configuração de mapa de política, especifique o mapa da classe da camada 3/4 do padrão, **inspection_default**.`ciscoasa(config-pmap)#class inspection_default ciscoasa(config-pmap-c)#`
8. No modo de configuração de classe do mapa de política, especifique que o DNS deve ser inspecionado usando o mapa de política da inspeção criado nas etapas 1-3.`ciscoasa(config-pmap-c)#inspect dns MY_DNS_INSPECT_MAP`
9. Retire fora do modo de configuração de classe do mapa de política e do modo da configuração de mapa de política.`ciscoasa(config-pmap-c)#exit ciscoasa(config-pmap)#exit`
10. Verifique que o mapa de política do **global_policy** está configurado como desejado.`ciscoasa(config)#show run policy-map ! !--- The configured DNS inspection policy map. policy-map type inspect dns MY_DNS_INSPECT_MAP parameters message-length maximum 512 policy-map global_policy class inspection_default inspect ftp inspect h323 h225 inspect h323 ras inspect rsh inspect rtsp inspect esmtp inspect sqlnet inspect skinny inspect sunrpc inspect xdmcp inspect sip inspect netbios inspect tftp inspect dns MY_DNS_INSPECT_MAP !--- DNS application inspection enabled. !`
11. Verifique que o global_policy está aplicado globalmente por uma serviço-política.`ciscoasa(config)#show run service-policy service-policy global_policy global`

Configuração do DNS em divisão

Emita o **DNS em divisão** comandam no modo de configuração da grupo-política a fim incorporar uma lista de domínios a ser resolvidos através do túnel em divisão. Não use ***nenhum*** formulário deste comando a fim suprimir de uma lista.

Quando não há nenhuma lista de domínios do Split Tunneling, os usuários herdam alguns que existirem na política do grupo padrão. Emita o **comando none do DNS em divisão** a fim impedir a herança de listas de domínios do Split Tunneling.

Use um espaço único a fim separar cada entrada na lista de domínios. Não há nenhum limite no número de entradas, mas a corda inteira pode ser já não do que 255 caráteres. Você pode usar somente caráteres alfanuméricos, hífens (-), e períodos (.). **Nenhum DNS em divisão** comanda, quando usado sem argumentos, suprime de todos os valores atual, que inclui um valor nulo criado quando você emite o **comando none do DNS em divisão**.

Este exemplo mostra como configurar os domínios Domain1, Domain2, Domain3 e Domain4 a fim ser resolvido com o Split Tunneling para a política do grupo nomeada FirstGroup:

```
hostname(config)#group-policy FirstGroup attributes hostname(config-group-policy)#split-dns
value Domain1 Domain2 Domain3 Domain4
```

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

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.

Capture o tráfego DNS

Um método para verificar que os registros das reescritas DNS da ferramenta de segurança são corretamente capturar os pacotes na pergunta, como discutido no exemplo anterior. Termine estas etapas a fim capturar o tráfego no ASA:

1. Crie uma lista de acessos para cada exemplo que da captação você quer criar.O ACL deve especificar o tráfego que você quer capturar. Neste exemplo, dois ACL foram criados.O ACL para o tráfego na interface externa:`access-list DNSOUTCAP extended permit ip host 172.22.1.161 host 172.20.1.2`
   `!--- All traffic between the DNS server and the ASA.` `access-list DNSOUTCAP extended permit ip host 172.20.1.2 host 172.22.1.161` `!--- All traffic between the ASA and the DNS server.`O ACL para o tráfego na interface interna:`access-list DNSINCAP extended permit ip host 192.168.100.2 host 172.22.1.161`
   `!--- All traffic between the client and the DNS server.` `access-list DNSINCAP extended permit ip host 172.22.1.161 host 192.168.100.2` `!--- All traffic between the DNS server and the client.`
2. Crie os exemplos da captação:`ciscoasa#`**`capture DNSOUTSIDE access-list DNSOUTCAP interface outside`** `!--- This capture collects traffic on the outside interface that matches !--- the ACL DNSOUTCAP.` `ciscoasa#`**`capture DNSINSIDE access-list DNSINCAP interface inside`** `!--- This capture collects traffic on the inside interface that matches !--- the ACL DNSINCAP.`
3. Veja as captações.É aqui o que as captações do exemplo olham como depois que algum tráfego DNS foi passado:`ciscoasa#`**`show capture DNSOUTSIDE`** `2 packets captured 1: 14:07:21.347195 172.20.1.2.1025 > 172.22.1.161.53: udp 36 2: 14:07:21.352093 172.22.1.161.53 > 172.20.1.2.1025: udp 93 2 packets shown ciscoasa#`**`show capture DNSINSIDE`** `2 packets captured 1: 14:07:21.346951 192.168.100.2.57225 > 172.22.1.161.53: udp 36 2: 14:07:21.352124 172.22.1.161.53 > 192.168.100.2.57225: udp 93 2 packets shown`
4. (Opcional) copie as captações a um servidor TFTP no formato do pcap para a análise em um outro aplicativo.Os aplicativos que podem analisar gramaticalmente o formato do pcap podem mostrar detalhes adicionais tais como o nome e o endereço IP de Um ou Mais Servidores Cisco ICM NT em Um-registros DNS.`ciscoasa#`**`copy /pcap capture:DNSINSIDE tftp`** `... ciscoasa#`**`copy /pcap capture:DNSOUTSIDE tftp`**

Troubleshooting

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

A reescrita DNS não é executada

Certifique-se de que você tem a inspeção DNS configurada na ferramenta de segurança. Veja a seção da inspeção configurar DNS.

Criação da tradução falhada

Se uma conexão não pode ser criada entre o cliente e o servidor WWW, pôde ser devido a um misconfiguration NAT. Verifique os logs da ferramenta de segurança para ver se há mensagens que indicam que um protocolo não criou uma tradução através da ferramenta de segurança. Se tais mensagens aparecem, verifique que o NAT esteve configurado para o tráfego desejado e que nenhum endereço está incorreto.

```
%ASA-3-305006: portmap translation creation failed for tcp src
inside:192.168.100.2/11000 dst dmz:10.10.10.10/23
```

Cancele as entradas do xlate, e então remova e reaplique as declarações NAT a fim resolver este

erro.

Deixe cair a resposta UDP DNS

Épossível que você recebe este Mensagem de Erro devido à gota do pacote de DNS:

```
 %PIX|ASA-4-410001: UDP DNS request from source_interface:source_address/source_port
to dest_interface:dest_address/dest_port; (label length | domain-name length)
52 bytes exceeds remaining packet length of 44 bytes.
```

Aumente o comprimento do pacote de DNS entre 512-65535 a fim resolver esta edição.

Exemplo:

```
ciscoasa(config)#policy-map type inspect dns MY_DNS_INSPECT_MAP ciscoasa(config-pmap)#parameters
ciscoasa(config-pmap-p)#message-length maximum <512-65535>
```

Informações Relacionadas

- Cisco PIX Firewall Software
- Referências do comando Cisco Secure PIX Firewall
- Field Notice de produto de segurança
- Request For Comments (RFC)
- Hair pinning em Cisco ASA
- Cisco ASA 5500 Series Adaptive Security Appliances
- Suporte Técnico e Documentação - Cisco Systems