DNS Doctoring no exemplo de configuração ASA

Índice

Introdução
Pré-requisitos
Requisitos
Componentes Utilizados
Convenções
Exemplos do DNS Doctoring
Servidor DNS no interior do ASA
Servidor DNS na parte externa do ASA
VPN NAT e DNS Doctoring
Informações Relacionadas

Introdução

Este documento mostra como o DNS Doctoring é usado na ferramenta de segurança adaptável (ASA) para mudar os endereços IP incorporados em respostas do Domain Name System (DNS) de modo que os clientes possam conectar ao endereço IP de Um ou Mais Servidores Cisco ICM NT correto dos server.

Pré-requisitos

Requisitos

O DNS Doctoring exige a configuração do Network Address Translation (NAT) no ASA, assim como a habilitação da inspeção DNS.

Componentes Utilizados

A informação neste documento é baseada na ferramenta de segurança adaptável.

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.

Exemplos do DNS Doctoring

Servidor DNS no interior do ASA

Figura 1 `nat (inside,outside) source static 10.1.1.100 198.51.100.100 dns`

```
!
policy-map global_policy
  class inspection_default
    inspect dns
```

Em figura 1, o servidor DNS é controlado pelo administrador local. O servidor DNS deve distribuir um endereço IP privado, que seja o *endereço IP real* atribuído ao server de aplicativo. Isto permite que o cliente local conecte diretamente ao server de aplicativo.

Infelizmente, o cliente remoto não pode alcançar o server de aplicativo com o endereço privado. Em consequência, o DNS Doctoring é configurado no ASA para mudar o endereço IP incorporado dentro do pacote da resposta de DNS. Isto assegura-se de que quando o cliente remoto faz um pedido DNS para www.abc.com, a resposta que obtêm seja para o endereço traduzido do server de aplicativo. Sem a palavra-chave DNS na declaração NAT, o cliente remoto tenta conectar a 10.1.1.100, que não trabalha porque esse endereço não pode ser distribuído no Internet.

Servidor DNS na parte externa do ASA

Figura 2 `nat (inside,outside) source static 10.1.1.100 198.51.100.100 dns`

```
!
policy-map global_policy
  class inspection_default
    inspect dns
```

Em figura 2, o servidor DNS é controlado pelo ISP ou pelo provedor de serviços similar. O servidor DNS deve distribuir o endereço IP público, isto é, o endereço IP de Um ou Mais Servidores Cisco ICM NT *traduzido do* server de aplicativo. Isto permite que todos os usuários do Internet alcancem o server de aplicativo através do Internet.

Infelizmente, o cliente local não pode alcançar o server de aplicativo com o endereço público. Em consequência, o DNS Doctoring é configurado no ASA para mudar o endereço IP incorporado dentro do pacote da resposta de DNS. Isto assegura-se de que quando o cliente local faz um pedido DNS para www.abc.com, a resposta recebida seja o endereço real do server de aplicativo. Sem a palavra-chave DNS na declaração NAT, o cliente local tenta conectar a 198.51.100.100. Isto não trabalha porque este pacote é enviado ao ASA, que deixa cair o pacote.

VPN NAT e DNS Doctoring

Figura 3

Considere uma situação onde haja as redes que sobrepõem. Nesta circunstância, o endereço 10.1.1.100 vive no lado remoto e no lado local. Em consequência, você precisa de executar o NAT no servidor local de modo que o cliente remoto possa ainda o alcançar com o endereço IP 192.1.1.100. A fim conseguir isto trabalhar corretamente, o DNS Doctoring é exigido.

O DNS Doctoring não pode ser executado nesta função. A palavra-chave DNS pode somente ser adicionada ao fim de um objeto NAT ou da fonte NAT. Duas vezes O NAT não apoia a palavra-chave DNS. Há duas possíveis configurações e ambas falha.

Configuração falhada 1: Se você configura a linha inferior, traduz 10.1.1.1 a 192.1.1.1, não

somente para o cliente remoto, mas para todos no Internet. Desde que 192.1.1.1 não é roteável pelo internet, ninguém no Internet pode alcançar o servidor local.

```
nat (inside,outside) source static 10.1.1.100 192.168.1.100 dns
nat (inside,outside) source static 10.1.1.100 192.168.1.100 destination
   REMOTE_CLIENT REMOTE_CLIENT
```

Configuração falhada 2: Se você configura a linha do DNS Doctoring NAT após duas vezes a linha necessária NAT, esta causa uma situação onde o DNS Doctoring nunca trabalhe. Em consequência, o cliente remoto tenta alcançar www.abc.com com o endereço IP 10.1.1.100, que não trabalha.

```
nat (inside,outside) source static 10.1.1.100 192.168.1.100 destination
   REMOTE_CLIENT REMOTE_CLIENT
nat (inside,outside) source static 10.1.1.100 64.1.1.100 dns
```

Informações Relacionadas

- Cisco ASA 5500 Series Adaptive Security Appliances
- Dispositivos de segurança adaptáveis Cisco ASA série 5500 > downloads do software
- Suporte Técnico e Documentação - Cisco Systems