

Configuração de Encaminhamento DNS do Balanceador de Carga F5 para Acesso Seguro

Contents

Problema

A resolução DNS não estava funcionando ao usar um balanceador de carga F5 como servidor DNS do cliente durante a migração do Umbrella to Secure Access. Quando as solicitações DNS atingem o VIP (IP Virtual), o balanceador de carga F5 encaminha com êxito pacotes para encaminhadores DNS de back-end, mas os nomes de host não estavam sendo resolvidos em máquinas de ponto de extremidade. A resolução DNS funcionou bem ao usar um dispositivo virtual diretamente como o servidor DNS do cliente, indicando que o problema era específico à configuração do balanceador de carga F5.

As capturas de pacotes revelaram que as respostas DNS estavam usando o endereço IP do dispositivo virtual em vez do endereço VIP F5 esperado. O computador cliente esperava respostas DNS do endereço VIP F5 , mas recebeu respostas do endereço IP do dispositivo virtual back-end.

Ambiente

- Cisco Umbrella para ambiente de migração de acesso seguro
- Balanceador de carga F5 com VIP de balanceamento de carga DNS configurado
- Vários encaminhadores DNS como servidores back-end
- Dispositivos virtuais que servem como servidores DNS
- Pontos de extremidade do cliente que requerem resolução DNS através do balanceador de carga

Resolução

O problema foi resolvido com a configuração do balanceador de carga F5 para atuar corretamente como um proxy entre os computadores cliente e os dispositivos virtuais. A principal alteração de configuração envolveu a habilitação da conversão de endereço de rede de origem (SNAT) com a funcionalidade de mapeamento automático.

Etapas de Diagnóstico Realizadas

Passo 1: Verificar o comportamento da resolução DNS

A resolução DNS foi testada usando o VIP do balanceador de carga F5 e conexões diretas do dispositivo virtual para isolar o problema.

Passo 2: Capturar e analisar o tráfego DNS

Capturas de pacotes foram realizadas para analisar a solicitação DNS e o fluxo de resposta através do balanceador de carga F5.

Passo 3: Identificar incompatibilidade de endereço de origem

A análise revelou que as respostas DNS continham o endereço IP do dispositivo virtual em vez do endereço VIP F5, causando confusão ao cliente.

Alteração de configuração

Passo 1: Acessar configuração de balanceador de carga F5

Navegue até a interface de gerenciamento do balanceador de carga F5 para modificar a configuração DNS VIP.

Passo 2: Habilitar mapeamento automático de SNAT

Configure a SNAT (Conversão de Endereço de Rede de Origem) para mapear automaticamente no balanceador de carga F5. Isso garante que o dispositivo F5 processe corretamente as solicitações e respostas DNS entre os clientes e os servidores DNS de back-end.

Passo 3: Verifique a configuração

Após implementar a configuração de mapeamento automático de SNAT, a resolução DNS começou a funcionar corretamente através do balanceador de carga F5.

Causa

A causa raiz foi uma configuração SNAT (Conversão de Endereço de Rede de Origem) incorreta no balanceador de carga F5. Sem o mapa automático de SNAT habilitado, o dispositivo F5 não estava atuando corretamente como um proxy para o tráfego DNS. Isso fez com que as respostas de DNS fossem enviadas diretamente dos dispositivos virtuais de back-end para os computadores cliente, usando o endereço IP do dispositivo virtual como origem em vez do endereço VIP F5 esperado. Os computadores clientes esperavam que as respostas DNS se originassem do mesmo endereço IP para o qual enviaram suas solicitações (o F5 VIP), mas estavam recebendo respostas de diferentes endereços IP (os servidores back-end), causando falhas de resolução DNS.

Conteúdo relacionado

- [Configurar o balanceamento de carga GTM F5](#)
- [Suporte técnico e downloads da Cisco](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.