Solucione problemas de esgotamento de porta ao usar a conversão de endereço de porta com componentes Umbrella

Contents

Introdução

Causas

Recomendações

Verificar os limites de conexão por IP em um ASA

Outras recomendações

Introdução

Este documento descreve os clientes Umbrella que usam clientes de roaming e/ou dispositivos virtuais e encontram problemas com esgotamento de portas em firewalls que usam a conversão de endereço de porta. Isso é mais provável em ambientes que têm um grande número de clientes de roaming e/ou um alto volume de tráfego em execução através dos VAs. Os sintomas podem incluir consultas de DNS que retornam lentamente ou que atingem o tempo limite.

Causas

Nem os clientes móveis nem os aplicativos virtuais armazenam em cache as respostas às consultas DNS. Além disso, os clientes de roaming enviam frequentes solicitações de DNS de "sondagem" para analisar o ambiente de rede e como verificações de integridade.

Recomendações

- Verifique se os Domínios internos estão configurados corretamente no Gerenciamento de domínio no painel do Umbrella. Eles devem conter a zona do Ative Diretory (e/ou outras zonas internas) para reduzir o volume de consultas de alta frequência.
- Revise algumas das configurações de PAT no firewall:
    - Um tempo limite longo de sessão UDP pode ser um problema. Geralmente, recomendamos tempos limite de sessão UDP de aproximadamente 15 segundos. No entanto, observe que se o UDP for usado pesadamente por outros aplicativos em sua rede, eles poderão ter tempos limite maiores, o que você deve levar em conta.
    - Dependendo do firewall, é possível aumentar o tamanho do pool PAT para aumentar o número de conexões simultâneas.
- Se você tiver um endereço IP que possa dedicar aos VAs, use NAT 1:1 em vez de PAT no firewall. Note: "NAT 1:1" às vezes é chamado de "NAT direto", mas esse é um termo incorreto; o termo técnico correto é "NAT 1:1".

- Revise seus limites de conexão por IP. Muitas vezes, uma política que não se espera que seja aplicada ao dispositivo em questão está, de fato, aplicando um limite. Consulte a próxima seção para saber como confirmar.

Verificar os limites de conexão por IP em um ASA

Siga as etapas abaixo:

- Configure o ASA com uma captura para ver por que os pacotes estavam sendo descartados pelo firewall:

```
capture asp type asp-drop all match ip any host 208.67.222.222
```

- Procure pacotes sendo descartados para o IP em questão. Um motivo de limite de conexão é exibido como "Motivo da queda: (conn-limit)"
- Examine o limite de conexões de host usando o comando:

```
show local-host detail | begin <IP Address of VA or roaming client>
```

    - Esse número é estático em um certo limite (ou seja, 999) e nunca aumenta? Em caso afirmativo, isso indica um limite de conexão.
- Verificar uma política de serviço que esteja aplicando isso; se você encontrá-lo, verifique seu mapa de políticas:

```
show run service-policy, show policy-map NAME
```

    - Se você encontrar um "NAME" do mapa de políticas que defina o limite de conexão por host como 1000 (por exemplo), isso fará com que todos os novos pacotes DNS do dispositivo sejam descartados até que mais conexões estejam disponíveis. O UDP é stateless e não tenta novamente.
- Para resolver, remova essa política de serviço (nenhum NOME de política de serviço dentro). As conexões devem começar a ultrapassar o limite de 1K (no nosso exemplo). Isso ocorre mais rapidamente para um VA do que um cliente de roaming.

Outras recomendações

Se essas recomendações não ajudassem, uma possível solução alternativa seria:

1. Use o relatório Umbrella dashboard —> Reporting —> Top Destinations para identificar um ou mais domínios que tenham um grande número de solicitações nas últimas 24 horas.
2. No painel Umbrella —> Configuration —> Domain Management, adicione um ou mais domínios de alto volume à lista, definindo "Aplica-se a" para "Todos os dispositivos".
3. Depois disso, as consultas para esses domínios são encaminhadas pelos VAs para o DNS

local. Idealmente, o DNS local deve ser configurado para encaminhar para o DNS Umbrella em 208.67.220.220/208.67.222.222, mas pode ser configurado para encaminhar para qualquer DNS externo.
4. O DNS local trata as consultas de todos os domínios para os quais são autoritativos.
5. Presumindo que o DNS local não aceita consultas para domínios não locais, as consultas para esses outros domínios são encaminhadas para o DNS externo.

Isso ocorre porque o DNS local pode armazenar em cache os resultados do DNS, enquanto os clientes de roaming e os dispositivos virtuais não armazenam em cache. Observe que o uso dessa solução alternativa resulta em mais tráfego e uma carga maior no DNS interno, portanto, monitore-os cuidadosamente para garantir que não sejam sobrecarregados.

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.