Solucionar problemas de agotamiento de puertos al utilizar la traducción de direcciones de puerto con componentes de Umbrella

Contenido

Introducción

Este documento describe a los clientes de Umbrella que utilizan clientes de roaming y/o dispositivos virtuales y que encuentran problemas con el agotamiento de puertos en los firewalls que utilizan la traducción de direcciones de puerto. Esto es más probable en entornos que tienen un gran número de clientes de roaming y/o un alto volumen de tráfico que circula a través de los VA. Los síntomas pueden incluir consultas de DNS que retornan lentamente o que agotan el tiempo de espera.

Causas

Ni los clientes de roaming ni los appliances virtuales almacenan en caché las respuestas a las consultas DNS. Además, los clientes de roaming envían solicitudes DNS de "sondeo" frecuentes para analizar el entorno de red y realizar comprobaciones de estado.

Recomendaciones

- Asegúrese de que los dominios internos están correctamente configurados en Domain Management en el panel de Umbrella. Deben contener su zona de Active Directory (y/u otras zonas internas) para reducir el volumen de consultas de alta frecuencia.
- Revise algunos de los parámetros de PAT en el firewall:
    - Un tiempo de espera de sesión UDP largo puede ser un problema. Por lo general, recomendamos tiempos de espera de sesión UDP de aproximadamente 15 segundos. Sin embargo, tenga en cuenta que si otras aplicaciones de la red utilizan mucho UDP, pueden tener tiempos de espera más largos que debe tener en cuenta.
    - Dependiendo de su firewall, es posible aumentar el tamaño de su conjunto PAT para aumentar el número de conexiones simultáneas.
- Si tiene una dirección IP que pueda dedicar a los VA, utilice NAT 1:1 en lugar de PAT en el firewall. Nota: "NAT 1:1" se denomina a veces "NAT directa", pero es un nombre incorrecto;

el término técnico correcto es "NAT 1:1".
- Revise los límites de conexión por IP. A menudo, una política que no se espera que se aplique al dispositivo en cuestión está aplicando efectivamente un límite. Consulte la siguiente sección para obtener información sobre cómo confirmar.

Comprobar los límites de conexión por IP en un ASA

Siga estos pasos:

- Configure el ASA con una captura para ver por qué el firewall descarta paquetes:

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

- Busque los paquetes que se descartan para la IP en cuestión. Un motivo de límite de conexión aparece como "Drop-reason: (conn-limit)"
- Examine el límite de conexión del host mediante el comando:

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

    - ¿Este número está estático en un cierto límite (es decir, 999) y nunca aumenta? Si es así, esto indica un límite de conexión.
- Verifique si existe una política de servicio que aplique esto; si lo encuentra, consulte su policy-map:

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

    - Si encuentra un policy-map "NAME" que establece el límite de conexión por host en 1000 (por ejemplo), esto hace que cualquier paquete DNS nuevo del dispositivo se descarte hasta que haya más conexiones disponibles. UDP no tiene información de estado y no se vuelve a intentar.
- Para resolverlo, quite esa política de servicio (no service-policy NAME inside). Las conexiones deben empezar a superar el límite de 1 K (como muestra nuestro ejemplo). Esto ocurre más rápidamente para un VA que para un cliente de roaming.

Otras recomendaciones

Si estas recomendaciones no ayudan, una posible solución alternativa sería:

1. Utilice el informe Panel de paraguas —> Informes —> Destinos principales para identificar uno o más dominios que han recibido un gran número de solicitudes en las últimas 24 horas.
2. En el panel de Umbrella —> Configuration —> Domain Management, agregue uno o más dominios de gran volumen a la lista y establezca "Applies to" (Se aplica a) en "All Appliances

and Devices" (Todos los dispositivos y dispositivos).
3. Después de eso, las consultas de esos dominios son reenviadas por los VAs al DNS local. Idealmente, el DNS local debe configurarse para reenviar al DNS de paraguas en 208.67.220.220/208.67.222.222, pero se puede configurar para reenviar a cualquier DNS externo.
4. El DNS local gestiona las consultas de los dominios para los que tiene autoridad.
5. Suponiendo que el DNS local no acepta consultas para dominios no locales, las consultas para esos otros dominios se reenvían al DNS externo.

Esto se debe a que el DNS local puede almacenar en caché los resultados del DNS, mientras que los clientes de roaming y los dispositivos virtuales no se almacenan en caché. Tenga en cuenta que el uso de esta solución alternativa genera más tráfico y una carga más pesada en el DNS interno, por lo que debe supervisarlos cuidadosamente para asegurarse de que no se sobrecargan.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).