Troubleshoot Port Exhaustion when Using Port Address Translation with Umbrella Components

Contents

Introduction

This document describes Umbrella customers using Roaming Clients and/or Virtual Appliances and encountering issues with port exhaustion in firewalls that use Port Address Translation. This is most likely in environments that have a large number of Roaming Clients and/or a high volume of traffic running through the VAs. Symptoms can include DNS queries returning slowly or timing out.

Causes

Neither Roaming Clients nor Virtual Appliances cache answers to DNS queries. Furthermore, Roaming Clients send frequent "probe" DNS requests to analyze the networking environment and as health checks.

Recommendations

- Ensure that your Internal Domains are properly configured within Domain Management on your Umbrella dashboard. They must contain your Active Directory zone (and/or other internal zones) in order to reduce the volume of high-frequency queries.
- Review some of the PAT settings on the firewall:
  - A long UDP session timeout can be an issue. We typically recommend UDP session timeouts of about 15 seconds. However, please note that if UDP is used heavily by other applications on your network, they can have longer timeouts which you must take into account.
  - Depending on your firewall, it is possible to increase the size of its PAT pool in order to increase the number of simultaneous connections.
- If you have an IP addresses that you can dedicate to the VAs, use 1:1 NAT instead of PAT on the firewall. Note: "1:1 NAT" is sometimes referred to as "Direct NAT", but this is a misnomer; the correct technical term is "1:1 NAT".
- Review your per-IP connection limits. Often, a policy not expected to apply to the device in question is indeed applying a limit. See the next section for how to confirm.

Check for per-IP connection limits on an ASA

Use the steps below:

- Configure the ASA with a capture to see why packets were being dropped by the firewall:

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

- Look for packets being dropped for the IP in question. A connection limit reason appears as "Drop-reason: (conn-limit)"
- Examine the host connection limit by using the command:

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

  - Is this number static at a certain limit (that is 999) and never increasing? If so, this indicates a connection limit.
- Check for a service-policy that is applying this; if you find it, check its policy-map:

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

  - If you find a policy-map "NAME" that sets the per-host connection limit to 1000 (for example), this causes any new DNS packets from the device to be dropped until more connections are available. UDP is stateless and does not retry.
- To resolve, remove that service-policy (no service-policy NAME inside). Connections must start going over the 1K limit (from our example). This occurs more quickly for a VA than a roaming client.

Further Recommendations

If these recommendations do not help, then a possible workaround would be:

1. Use the Umbrella dashboard --> Reporting --> Top Destinations report to identify one or more domains that have a large number of requests within the last 24 hours.
2. In the Umbrella dashboard --> Configuration --> Domain Management, add one or more of the high-volume domains to the list, setting "Applies to" to "All Appliances and Devices".
3. After that, queries for those domains are forwarded by the VAs to the local DNS. Ideally, the local DNS must be configured to forward to the Umbrella DNS at 208.67.220.220/208.67.222.222, but they could be configured to forward to any external DNS.
4. The local DNS handles queries for any domains they are authoritative for.
5. Presuming the local DNS does accept queries for non-local domains, queries for those other domains are forwarded to the external DNS.

This is because the local DNS can cache DNS results, while the Roaming Clients and Virtual Appliances do not cache. Please note that using this workaround results in more traffic and a heavier load on the internal DNS, so monitor them carefully to ensure they are not overloaded.