Use TraceRT for WAN Optimization

Author: Felicia King

This article is about how to find the best DNS servers to use for the WAN DNS for your perimeter security appliance.

The DNS server settings discussed here are NOT the DNS server settings that would be delivered to end users via DHCP.

WAN DNS concepts

What is WAN DNS used for?

Perimeter security appliances use WAN DNS in order to look up content in real time as well as on a scheduled basis. To best understand this, think about web content filtering. Every time one of your users looks up a website, a web content filtering lookup is made to the web content lookup database. That database is hosted in the cloud and found by the perimeter security appliance via DNS. You can imagine that this is a lot of lookups for the average company on an average day. Even for a small office of 5 people, their aggregated web browsing can result in tens of thousands of DNS lookups per day.

Any inefficiency in the DNS lookup process that does not increase security is simply wasted time. There are valid reasons for using things like DNS proxies or WAN DNS hosts that can provide additional security, such as OpenDNS. But using OpenDNS for DNS lookups for the security services portion of your appliance adds no value. What does add value is to find the closest, yet reliable DNS server that is accessible from ALL of your WAN interfaces.

Use WAN DNS accessible from both ISPs

Many networks use multiWAN. That means the network has two ISPs. The proper use of multiWAN is to use policy-based routing, load balancing, and automatic failover. Link status monitoring is a topic for another article, but realize that whatever the DNS is that is used for the WAN functions of the security appliance must be accessible from BOTH WAN connections. Otherwise a situation can result where WAN DNS lookups for services can fail because the DNS server is not accessible from the remaining WAN link.

Use TraceRT to select best DNS

TraceRT

Tracert.exe is a trace routing command line tool. The syntax for usability is:

```
Tracert.exe [ip address]
```

Trace route will show how many network hops away from the WAN connection is the WAN DNS server. The more hops, the worse the network performance.

Check a few WAN DNS servers for hop count

Check Google's ever popular and probably way over utilized DNS server. 16 hops is very slow network performance.

```
C:\>tracert 8.8.8.8

Tracing route to google-public-dns-a.google.com [8.8.8.8]
over a maximum of 30 hops:

  1     1 ms    <1 ms    <1 ms  10[redacted]
  2     1 ms    <1 ms    <1 ms  192.168.0.1
  3     8 ms     8 ms     8 ms  142.254.153.81
  4    23 ms    20 ms    22 ms  ae63.kenowibl01h.midwest.rr.com [24.164.241.97]
  5    13 ms    14 ms    14 ms  be31.milzwift01r.midwest.rr.com [65.31.113.40]
  6    15 ms    14 ms    15 ms  bu-ether18.chctilwc00w-bcr00.tbone.rr.com [66.109.6.206]
  7    19 ms    14 ms    14 ms  bu-ether11.chcgildt87w-bcr00.tbone.rr.com [66.109.6.20]
  8    13 ms    13 ms    12 ms  0.ae0.pr1.chi10.tbone.rr.com [107.14.17.192]
  9    15 ms    13 ms    13 ms  ix-ae-27-0.tcore2.ct8-chicago.as6453.net [64.86.79.97]
 10    22 ms    25 ms    25 ms  72.14.219.82
 11    13 ms    13 ms    24 ms  209.85.143.190
 12    13 ms    15 ms    13 ms  72.14.238.89
 13    24 ms    22 ms    31 ms  216.239.47.121
 14    30 ms    22 ms    22 ms  216.239.46.191
 15     *        *        *     Request timed out.
 16    23 ms    23 ms    23 ms  google-public-dns-a.google.com [8.8.8.8]

Trace complete.
```

Check OpenDNS. Find that DNS server is 12 hops away.

```
C:\>tracert 208.67.222.222

Tracing route to resolver1.opendns.com [208.67.222.222]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  1[redacted]
  2     1 ms    <1 ms     1 ms  192.168.0.1
  3    73 ms    44 ms    46 ms  142.254.153.81
  4    27 ms    21 ms    22 ms  ae63.kenowibl01h.midwest.rr.com [24.164.241.97]
  5    14 ms    19 ms    43 ms  be31.milzwift01r.midwest.rr.com [65.31.113.40]
  6    17 ms    19 ms    50 ms  bu-ether18.chctilwc00w-bcr00.tbone.rr.com [66.109.6.206]
  7    14 ms    13 ms    13 ms  0.ae1.pr0.chi30.tbone.rr.com [66.109.1.78]
  8     *       14 ms    15 ms  lag-12.ear2.chicago2.level3.net [4.68.111.17]
  9   184 ms   219 ms    14 ms  ae-21-52.car1.chicago1.level3.net [4.69.138.35]
 10    14 ms    14 ms    14 ms  ae-21-52.car1.chicago1.level3.net [4.69.138.35]
 11    14 ms    16 ms    14 ms  open-dns-in.car1.chicago1.level3.net [4.28.56.10]
 12    14 ms    13 ms    14 ms  resolver1.opendns.com [208.67.222.222]

Trace complete.
```

Check Dyn.com DNS server. Find that it is 11 hops away.

```
C:\>tracert 216.146.35.35

Tracing route to resolver1.dyndnsinternetguide.com [216.146.35.35]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  10.[redacted]
  2     1 ms    <1 ms    <1 ms  192.168.0.1
  3     9 ms     8 ms     8 ms  142.254.153.81
  4    20 ms    15 ms    22 ms  ae63.kenowibl01h.midwest.rr.com [24.164.241.97]
  5    14 ms    13 ms    18 ms  be31.milzwift01r.midwest.rr.com [65.31.113.40]
  6    17 ms    15 ms    15 ms  bu-ether18.chctilwc00w-bcr00.tbone.rr.com [66.109.6.206]
  7    21 ms    14 ms    14 ms  bu-ether11.chcgildt87w-bcr00.tbone.rr.com [66.109.6.20]
  8    14 ms    12 ms    12 ms  0.ae2.pr1.chi10.tbone.rr.com [107.14.17.196]
  9    12 ms    12 ms    13 ms  ix-ae-27-0.tcore2.ct8-chicago.as6453.net [64.86.79.97]
 10    13 ms    12 ms    13 ms  64.86.79.94
 11    13 ms    13 ms    14 ms  resolver1.dyndnsinternetguide.com [216.146.35.35]

Trace complete.
```

Check Time Warner Cable DNS. While it is very close, if you have multiWAN, you should not use the ISP DNS because it is probably not accessible from both WAN connections. If you don't have multiWAN, than this DNS server would be the best primary option, but use Dyn.com as the secondary.

```
C:\>tracert 209.18.47.61

Tracing route to dns-cac-lb-01.rr.com [209.18.47.61]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  10.[redacted]
  2     1 ms    <1 ms     4 ms  192.168.0.1
  3     8 ms     8 ms     8 ms  142.254.153.81
  4    26 ms    21 ms    21 ms  ae63.kenowibl01h.midwest.rr.com [24.164.241.97]
  5    13 ms    15 ms    14 ms  be31.milzwift01r.midwest.rr.com [65.31.113.40]
  6    27 ms    24 ms    27 ms  be40.clmkohpe01r.midwest.rr.com [65.25.137.109]
  7    55 ms    35 ms    33 ms  agg1.clmkohpe38r.midwest.rr.com [65.29.1.247]
  8    24 ms    23 ms    23 ms  dns-cac-lb-01.rr.com [209.18.47.61]

Trace complete.
```

Decision

For singleWAN, use the ISP DNS as primary DNS and Dyn.com as secondary.

For multiWAN, use Dyn.com as primary and OpenDNS as secondary.

In my testing, I found that the reduction in hops had the most noticeable results in slow connections such as satellite, microwave, or DSL. This strategy still applies to most internet connections.

Depending upon what your network's ISP is, you will need to find out what that ISP's DNS servers are and do your own testing. If you are on the west coast of the United States, you may find that 8.8.8.8 has a less hops tracert response than my results.