Wrong DNS Server used by random clients

Problem

Fortigate VPN users reporting that they cannot connect to internal resources anymore.
When you check the client the internal host is reachable by IP but it appears that windows isn't using the internal DNS server to resolve the host name. A check with nslookup was working when testing this on the VPN client.

Solution

the clients having issues were using IPV6 and learned about this feature in Windows call "Smart Multi-Homed Name Resolution". It sounds like Windows will forward a DNS query to both the IPV6 and IPV4 DNS servers and use the first response.

Adding a regkey to disable the parallel queries and the issue cleared.

Go to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Dnscache\Parameters

- If the Dword value DisableParallelAandAAAA exists already, make sure its value is set to 1.
- If the value does not exist, right-click on Parameters, and select New > Dword (32-bit) Value.
- Name it DisableParallelAandAAAA.
- Set the value of the Dword to 1. You can turn the feature back on by setting the value to 0, or by deleting the value.

Link

https://forum.fortinet.com/tm.aspx?m=190334

Revision #2
Created 18 November 2020 07:34:04
Updated 20 May 2021 13:58:47