David Thomsen

<table>
<tr><td>Recursive</td><td>A recursive DNS is when one DNS server uses other dns servers to locate and retrieve an IP address.</td></tr>
<tr><td>Iterative</td><td>In an Iterative DNS, the client directly contacts each DNS server that is used with the lookup of the IP.</td></tr>
<tr><td colspan="2">The main difference between these two is that with recursion, the program will loop until the condition (in this case, finding the IP) is met. In this example, the recursive DNS will continue to ping other DNS servers until it finds the IP address it is looking for.
Iterative on the other hand will look at each DNS individually from the client’s device. It will look at each DNS server, and move on to the next one, until the IP address is located.</td></tr>
</table>

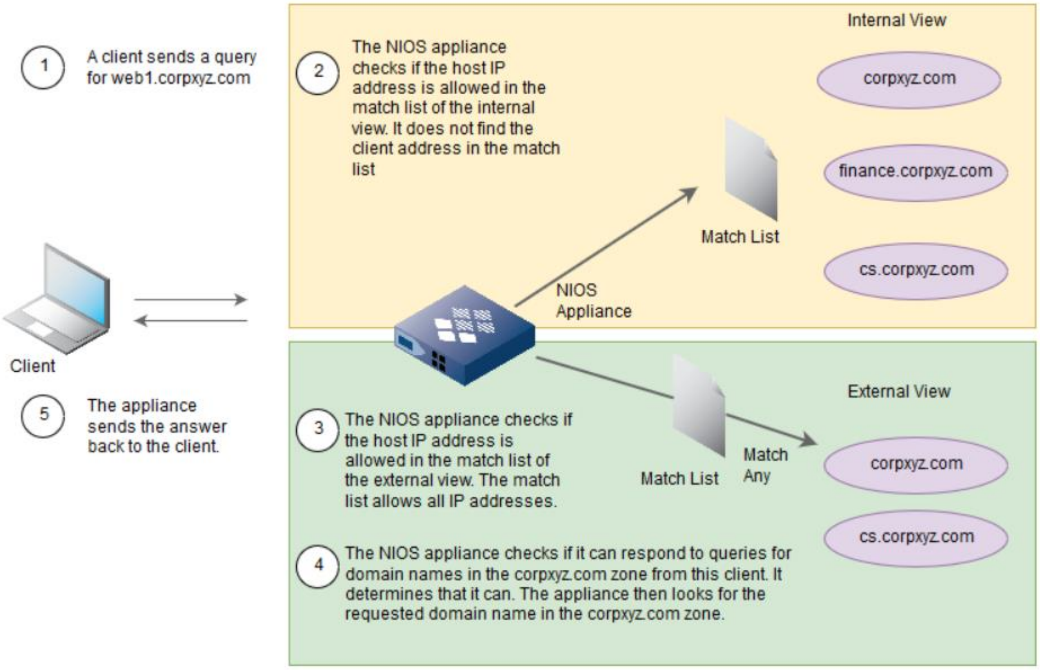
What type of attack can occur as a result of enabling DNS recursion on a DNS server for ANY client on the Internet

a) A DDOS attack is a very common and likely type of attack on a public, recursive DNS. A DDOS, aka a Distributed Denial of Service, is an attack where malicous end users will use public and open DNS servers to flood a whole network with DNS packet traffic. The malicious user will send thousands of fake packets to the DNS server, and the recursion will continue sending them around, massively slowing down, or maybe even shutting down the network.

b) Recursion should be set up in a way that allows recursive DNS to be used by trusted IPs so that while the organization is able to use it, new people being added to the network are not able to. With untrusted/unknown ip addresses on a network using recursive DNS, this allows the possibility of a DDOS attack.

Research "DNS Views" and describe how they work and the benefits they provide.

DNS Views provide the ability to show DNS data to the clients on the server. They are also able to show different versions of the Views to different clients. Depending on the client sending out the DNS query, the DNS server can either show the Internal View or the External View. I have included a screenshot of a diagram that explains the usage more clearly. As seen here, the client sends out a query to the dns, and the DNS decides based on the host IP if it should receive an Internal or External View.



1 A client sends a query for web1.corpxyz.com

2 The NIOS appliance checks if the host IP address is allowed in the match list of the internal view. It does not find the client address in the match list

3 The NIOS appliance checks if the host IP address is allowed in the match list of the external view. The match list allows all IP addresses.

4 The NIOS appliance checks if it can respond to queries for domain names in the corpxyz.com zone from this client. It determines that it can. The appliance then looks for the requested domain name in the corpxyz.com zone.

5 The appliance sends the answer back to the client.

Research IP Address Management and describe what it is and why many organizations are moving in that direction for managing DNS and DHCP.

IPAM, or IP Address Management is a way to Administrate DNS or DHCP services within a network. It allows the admin to track and manage the IP addresses that are used in a network. Organizations are moving to this rather than simply using DHCP or DNS management because by using IPAM, each service will know automatically about the changes made to itself or any other services. This could be the DNS knowing which IP is being given out by the DHCP, or the other way around, the DHCP knowing which IP addresses it cant give out because of the DNS.

CISA. (2013, March 29). *Alert (TA13-088A) DNS Amplification Attacks*. CISA. Retrieved September 25, 2022, from https://www.cisa.gov/uscert/ncas/alerts/TA13-088A.

Cloudflare, Inc. (2022). *What is recursive DNS?* CloudFlare. Retrieved September 25, 2022, from https://www.cloudflare.com/learning/dns/what-is-recursive-dns/

Infoblox. (n.d.). *Chapter 18 DNS Views*. Docs.infoblox.com. Retrieved September 25, 2022, from https://docs.infoblox.com/space/NAG8/22280613/Chapter+18+DNS+Views

Infoblox. (2021, April 27). *What is IPAM (IP Address Management)?* Infoblox.com. Retrieved September 25, 2022, from https://www.infoblox.com/glossary/ipam-ip-address-management/