In the Boxing Ring
MAR 2023

Network Box Technical News
from Mark Webb-Johnson
Chief Technology Officer, Network Box

Welcome to the March 2023 edition of In the **Boxing Ring**

This month, Network Box USAs CTO, Pierluigi Stella, is talking about the **Issues with DNS.** If your network is like most companies, you are likely using Active Directory and therefore have Domain Controllers (DCs). Your workstations are likely using these DCs as their DNS servers. The DCs, in turn, have a configuration for DNS forwarders, which are used to resolve public IP addresses. In the majority of cases with our clients, these forwarders are configured to be the DNS servers of their primary ISP. This configuration might have been viable in the past, but today it is not advisable. In fact, it is discouraged. On pages 2 to 3, we discuss why.

In other news, Network Box USA's CTO, Pierluigi Stella, and Channel Leader and Industry Influencer, Len DiCostanzo, hosted an exclusive, in-depth masterclass on the SASE evolution. Additionally, Network Box's Managing Director, Michael Gazely, presented and discussed Gartner's MESH Cybersecurity Architecture concept to members of the HK Computer Society. In this month's global security headlines, security issues were encountered by Reddit, Microsoft, Google, GoDaddy, LastPass, Fortinet, and Cisco.

Mark Webb-Johnson
CTO, Network Box Corporation Ltd.
March 2023

Stay Connected

You can contact us here at Network Box HQ by email: **nbhq@network-box.com**, or drop by our office next time you are in town. You can also keep in touch with us by several social networks:

https://twitter.com/networkbox
https://www.facebook.com/networkbox
https://www.facebook.com/networkboxresponse
https://www.linkedin.com/company/network-box-corporation-limited/
https://www.youtube.com/user/NetworkBox

In this month's issue:

Issues with DNS

(Domain Naming Sytem)

by Pierluigi Stella
Chief Technology Officer
Network Box USA

If your network is like most companies, you are likely using Active Directory and therefore have Domain Controllers (DCs). Your workstations are likely using these DCs as their DNS servers. The DCs, in turn, have a configuration for DNS forwarders, which are used to resolve public IP addresses. In the majority of cases with our clients, these forwarders are configured to be the DNS servers of their primary ISP. This configuration might have been viable in the past, but today it is not advisable. In fact, it is discouraged. And here is why.

The ISP DNS servers are not a public service

They do not respond to DNS queries from the Internet. They respond to your servers because you are using their network. In other words, your public IP is authorized to query those servers. So, what happens when you change ISP? Suddenly, you can't get to the Internet, and you scratch your head thinking, "the new ISP did something wrong," when instead, you have a simple DNS issue - your new public IP address is not authorized to query those servers.

Of course, the first solution you'll think of is to replace those forwarders with the new DNS IP addresses the new ISP provides. But what happens if you have 2 ISPs, in load balance or high availability? Do you change the forwarders every time you fail over to the 'other one'? Or do you configure the DNS servers recommended by both ISPs? If you do that, when you're using the 'secondary' DNS server, you'll see delays, and your users will complain of slow Internet, which is very close to saying that the Internet isn't working.

Consider that a DNS query can take hundreds of milliseconds, and the secondary DNS server is only queried once the primary times out. Then consider how many domain resolutions your browser needs to perform for each web page you're visiting; you'll quickly realize that DNS malfunction is a very likely cause of Internet sluggishness. In my direct experience, DNS issues are by far the most frequent reason why the Internet is slow.

DNS can be attacked

Another very important reason to avoid adopting such forwarders is that DNS can be attacked. Several attacks can be carried against DNS servers, but here I am referring more to DNS spoofing, whereby your workstation ends up requesting DNS from servers that aren't the ones you think you configured. This is a catastrophic attack because now, every query your browser runs gets a reply that will point your browser to the IP the hacker wants you to reach; the results of that can be catastrophic. Protecting your DNS with a DNS proxy is essential because it avoids this attack altogether.

Rate Limiting for Queries

Many bypass the ISP DNS issue by using public DNSs. I see many using 8.8.8.8. While there is nothing wrong in doing so, those IP addresses belong to Google. So the first thing that you need to consider is that you're telling Google every domain you're visiting. Is that something you want? Or did you think that Google has a big heart and is providing you with that service for free? Aside from this 'conspiracy theory,' this IP address (and its companion 8.8.4.4) apply rate limits to how many queries per second or minute they will allow. If you're a small organization, this may not really matter, but it is quite easy to reach that limit - after which they stop responding for a period of time. And again, you'll think there is something wrong with the Internet when it's just your DNS configuration causing you problems instead.

Cloudflare also offers a similar service with their 1.1.1.1 IP address. Many years ago, the DNS of choice was 4.4.4.4 and 4.4.2.2. But then Layer 3 bought the entire 4.4.0.0/16 subnet. The DNS servers are still working, but Layer 3 is not in the business of providing free public services. Before you know it, they might well take those servers down. And again, you'd be stuck with no Internet.

So what is the solution to all these possible issues?

If you are a Network Box client, the solution is to point your forwarders to the local Network Box LAN IP (or DMZ or whatever). We will configure all our devices to run their own secure DNS service (DNS server 127.0.0.1) and use the Internet ROOT DNS servers as the primary forwarders.

There are many reasons why this is a good idea. The ROOT servers are those operated by the registrars, so when you make DNS configuration changes, they are the first to know, and the propagation has to start from here. I have seen cases where 8.8.8.8 took hours to note a DNS change when the root servers had already seen it within minutes of the change being made. The root servers are by far the most reliable. They are run by the registrars and 'know,' which are the authoritative servers for a domain. At the end of the day, every other DNS server ends up querying these servers first to find the IP of the DNS server that is authoritative for that domain. So, why not query them directly? And by using the Network Box LAN IP as your DNS forwarder, you will also avoid the DNS spoofing attack, which is a big thing to consider.

If you are a Network Box client and you are also using a DNS proxy service such as OpenDNS, you may want to reconsider how you're spending your budget. The service they offer is something you already have with Network Box. Why spend the money twice?

Stay safe.

Network Box HIGHLIGHTS

Network Box HK

HK Computer Society - Digital Leadership Development (DLD) Program

As part of the DLD Program, Network Box's Managing Director, Michael Gazely, presented and discussed Gartner's MESH Cybersecurity Architecture concept to members of the HK Computer Society.

Network Box USA

SASE Masterclass

Network Box USA's CTO, Pierluigi Stella, and Channel Leader and Industry Influencer, Len DiCostanzo, hosted an exclusive, in-depth masterclass on the SASE evolution and why you need a SASE networking and cybersecurity stack.

Newsletter Staff

Mark Webb-Johnson
Editor

Michael Gazeley
Kevin Hla
Production Support

Network Box HQ
Network Box USA
Contributors

Subscription

Network Box Corporation
nbhq@network-box.com
or via mail at:

Network Box Corporation
16th Floor, Metro Loft,
38 Kwai Hei Street,
Kwai Chung, Hong Kong

Tel: +852 2736-2083
Fax: +852 2736-2778

www.network-box.com

Copyright © 2023 Network Box Corporation Ltd.

Global Security Headlines

TechCrunch
Reddit says hackers accessed employee data following phishing attack
LINK: https://tcrn.ch/3ZxwUKy

Bleeping Computer
Hackers backdoor Microsoft IIS servers with new Frebniis malware
LINK: https://bit.ly/3YaKmmw

The Hacker News
Hackers Using Google Ads to Spread FatalRAT Malware Disguised as Popular Apps
LINK: https://bit.ly/3JamI5w

SC Magazine
GoDaddy blasted for breach response
LINK: https://bit.ly/3ERkntF

Ars Technica
LastPass says employee's home computer was hacked and corporate vault taken
LINK: https://bit.ly/3ZwtasM

Bleeping Computer
Hackers now exploit critical Fortinet bug to backdoor servers
LINK: https://bit.ly/3kAetGs

Security Week
Cisco Patches Critical Vulnerability in IP Phones
LINK: https://bit.ly/3KOBoIH