TCPWave IPAM

Approach To Protective DNS (PDNS)

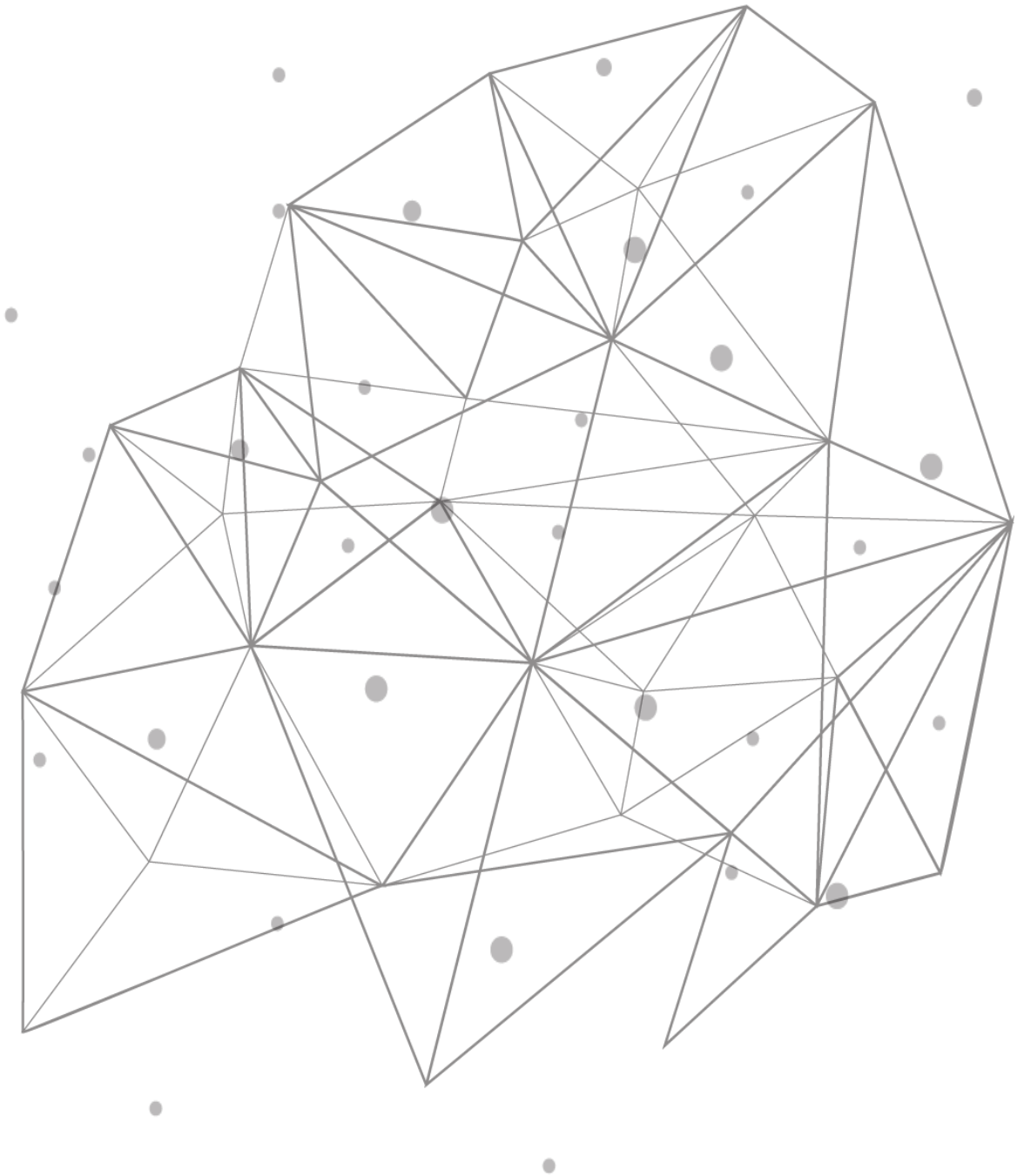


Table of Contents

Introduction

Paul Mockapetris's invention of the Domain Name System (DNS) in 1983 didn't have its security aspect in mind. With the evolution of technology, numerous vulnerabilities within the system were exploited to attack targets using this facility.

Eventually, various security frameworks and standards came into place over the years to defend the vulnerabilities. The Protective DNS (PDNS) solution is one of the recent cybersecurity best practices advised by the **National Security Agency** (NSA) and **Cybersecurity Infrastructure Security Agency** (CISA).

What is PDNS

PDNS is the defensive measure where the system inspects the DNS queries to identify potential threats and take preventive measures as appropriate. It leads to mitigation of possible damages, leveraging the existing DNS protocol & its architecture. PDNS suppresses the use of DNS for malware attacks and operations.

Securing DNS interaction between the client & a server is one of the critical aspects of internet security. Users often mistype domain names while attempting to navigate to a known website and unintentionally go to malicious ones instead of the actual webpage that they were looking at. Malicious actors lace phishing emails with malicious links. A compromised device may listen for remote commands from a control server, resulting in data exfiltration from a compromised system to remote destinations. The domain names associated with harmful content are often spotted quickly, and preventing their resolution protects individual users and enterprises.

Functionality - PDNS

The existing DNS security enhancements, such as Domain Name System Security Extensions (DNSSEC), ensure DNS records' integrity and authenticity from the upstream servers. Web protocols such as DNS over TLS (DoT), DNS over HTTP (DoH) safeguard the privacy of DNS clients. Irrespective of these security enhancements and protocols, there is still no validation of the trustworthiness of the upstream DNS infrastructure that might have been compromised.

To overcome this situation, PDNS plays a crucial role. It uses a recursive DNS resolver policy, and the clients' answers are returned based on the defined policies. The policies are called Response Policy Zones (RPZ).

Response Policy Zones

Using RPZ, the DNS appliance inspects both the DNS query and the returned IP addresses against a list of threat intelligence data. If there are matches, connections to those known or suspected malicious sites are blocked by the DNS appliance. PDNS performs this operation either by redirecting the client to any other non-malicious site or by not returning any IP address for the query done by the client (NXDOMAIN). Thus, the client machine wouldn't communicate to the malicious endpoint since it would not get an IP address to connect or redirect to any known good websites. Besides this, many infrastructures still do not support DNSSEC or support DoT, but many PDNS providers support this additional security extension.

Importance - PDNS

There are various other best practices to secure DNS from being exploited for cyber-attacks.

Example: DNSSEC is the set of specifications that strengthens authentication in DNS using digital signatures based on public-key cryptography. DoT and DoH protects user privacy from eavesdropping, manipulation of DNS data via man-in-the-middle attacks, etc.

However, none of these features can prevent a client machine from resolving a known malicious/look-alike domain on the internet as long as an attacker gives a legitimate posture to them. In this situation, a PDNS service accepts data feeds from known threat intelligence providers worldwide and uses this data to evaluate the legitimacy of a DNS query/response before responding to a recursive DNS query.

The significant benefits of PDNS are as follows:

- A centralized threat management system collecting data inputs from multiple contributors worldwide would escalate an organization's security posture and level.
- Usage of PDNS would mean that malicious queries would get blocked instantly when it gets added to the list.
- To control the outbound DNS traffic based on RPZ policies. An administrator can decide if a DNS server should recurse to find a response to a known malicious domain.

Protective DNS Domain Classification

One of the prime competencies of PDNS is its capacity to categorize domain names based on threat intelligence data. PDNS services typically leverage open source, commercial, and governmental information feeds of known malicious domains. These feeds enable coverage of domain names found at numerous points of the network exploitation lifecycle. Some solutions may also detect new malicious domains based on pattern recognition. The types of domains typically covered by a PDNS server include the following:

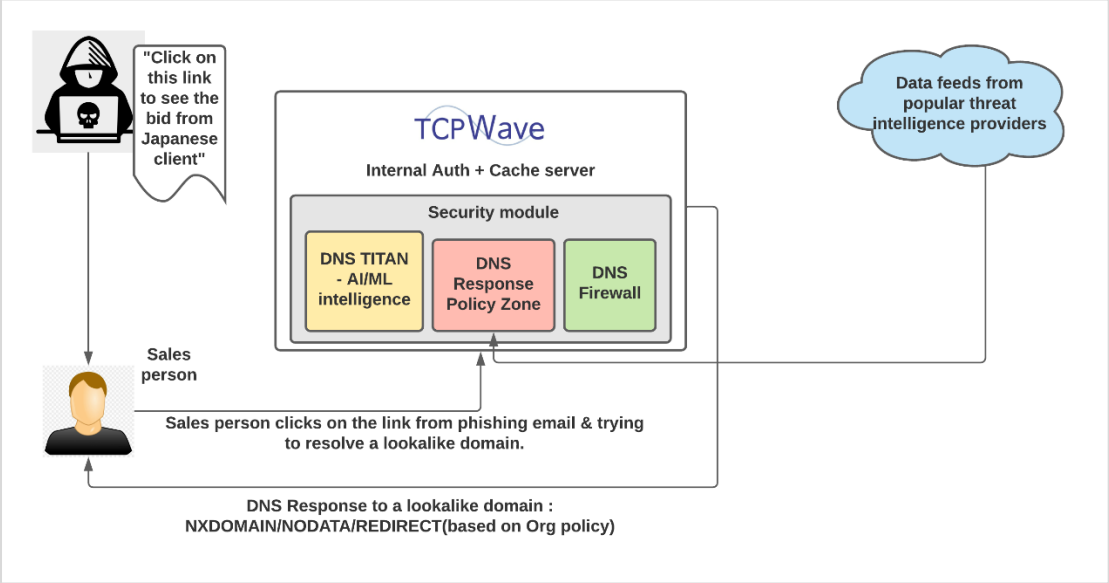
- **Phishing**: The tricky process of obtaining sensitive information, such as usernames and passwords, by masquerading as a reliable entity in communication. Phishing techniques include social engineering, link manipulation, and website forgery. Domains may include typosquats – or look-alikes of common domains. PDNS can protect users from accidentally connecting to a potentially malicious link.
- **Malware Distribution and Command & Control (C2)**: Websites known to host malicious content or are known to be used by attackers to command & control malware.
    - **Example**: It may include websites hosting malicious JavaScript files or domains that host advertisements that collect information for undesired profiling. PDNS can block and alert on known malicious connection attempts.
- **Domain Generation Algorithms (DGA)**: Websites with programmatically generated domain names used by malware to circumvent static blocking. Advanced malware, including some botnets, depend on the ability to communicate with C2 infrastructure. Cyber threat actors use DGAs for malware to bypass static blocking by domain name or IP by programmatically generating domain names. PDNS offers protection from malware DGAs by analyzing every domain's textual attribute and tagging those associated with known DGA attributes, such as high entropy.

- **Content Filtering**: Websites whose content is in specific categories that are against an organization's access policies. Although an ancillary benefit to malware protection, PDNS can categorize various domains' use cases (example: "gambling") and warn or block those deemed a risk for a given environment.

Actions

The actions taken by PDNS servers in response to malicious requests are as follows:

- **NXDOMAIN**: The client doesn't receive an IP address to connect to.
- **NODATA**: The requested name exists, but the type doesn't match.
- **PASSTHROUGH**: Even though the requested domain appears malicious, the DNS server cascades the response back to the client. For some use-cases, administrators may tend to use this policy to meet specific business requirements.
- **REDIRECT**: The client redirects to any other domain, which can also be a warning page indicating the client has been trying to access something malicious in nature.



Protective DNS Solutions from TCPWave

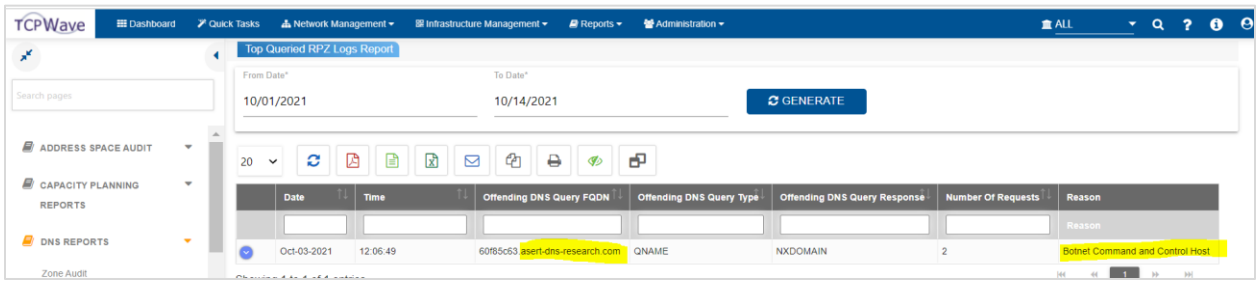
TCPWave IPAM's integration with DNS Response Policy Zones can effectively defend against malware, phishing, ransomware sites, botnets, etc.

- Leveraging the guidelines from DNS RPZ, TCPWave's RPZ offering collects threat intelligence feeds from some of the best-in-class providers such as ThreatSTOP, Spamhaus, etc.
- Using data feeds, possibly supplemented with custom rules, TCPWave's RPZ provides an effective firewall that prevents users from accessing harmful websites. The solution inspects DNS queries to detect and block threats, data exfiltration, phishing, ransomware, and advanced threats such as DGA, look-alike domains, etc.
- To support the processing of logs by Security Information and Event Management (SIEM) and other systems, TCPWave produces audit log files that comply with the Common Event Format (CEF) standard.

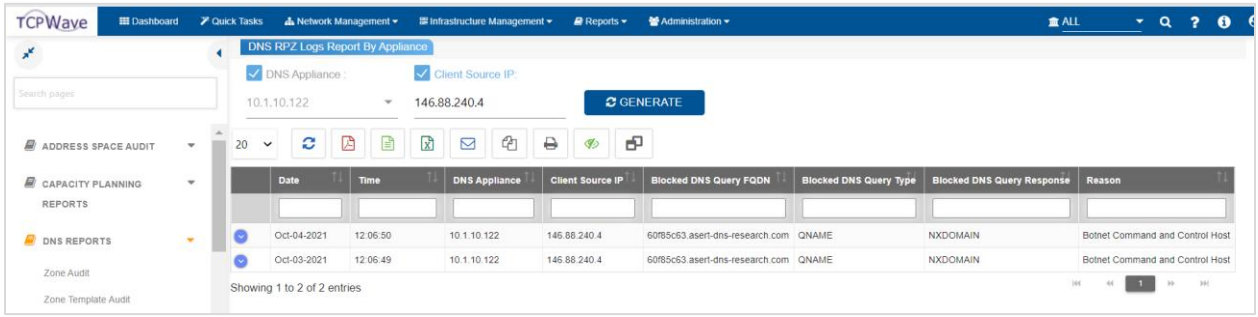
- TCPWave supports forwarding this to IBM QRadar, Splunk, Apache Flume, and others that help security personnel quickly detect and respond to threats.

Report Management

TCPWave IPAM provides reports of blocked DNS queries, which help security personnel and others understand trends in security threats and better protect users. Also, these reports are based on RPZ log files. The Top Queried RPZ Logs Report displays the most frequent DNS queries resolved by RPZ rules. The DNS RPZ Logs Report displays the history of DNS queries that were resolved by RPZ rules. Additionally, you can filter it to see just the queries for a specific appliance or a specific client.



Top Queries RPZ Logs Report



DNS RPZ Logs Report By Appliance

Conclusion

TCPWave's DDI solution helps our customers manage and modernize their enterprise-grade solutions by ensuring they have the most innovative technology with minimal risks.

For a quick demo, contact the TCPWave Sales Team.

References

Thanks to the **National Security Agency** (NSA) and **Cybersecurity Infrastructure Security Agency** (CISA) that has issued an advisory on the expanding need to introduce a protective DNS (PDNS) solution to the enterprise's security footprint.