Technical sciences

UDC 004.7:004.62:004.77

Slabovych Volodymyr
Student of the
Taras Shevchenko National University of Kyiv

Marianovskyi Vitalii
Candidate of Technical Sciences (PhD), Assistant Lecturer,
Head of the ICC Network Department
Taras Shevchenko National University of Kyiv

Boyko Yuriy
Candidate of Physical and Mathematical Sciences (PhD), Associate Professor,
Head of the Department of Computer Engineering
Taras Shevchenko National University of Kyiv

Boretskyi Oleksandr
Candidate of Technical Sciences (PhD), Assistant Lecturer,
Chief Engineer of the ICC
Taras Shevchenko National University of Kyiv

ADVANCED NETWORK PROTECTION AND ADMISSION CONTROL BY DNS FILTERING

Summary. *The aim of this work is to propose an effective and scalable approach to network traffic filtering by utilizing open-source technologies, specifically the PowerDNS software for DNS resolution and filtering. The proposed model involves defining filtering rules using the DNS Firewall, which can block or redirect DNS queries based on various criteria.The proposed automated solution involves a script that reads a list of domains from a file and creates a new DNS zone for each domain.The handling of HTTPS traffic requires* *special attention to ensure proper functionality and security, as the filtering software may need to intercept and modify the SSL certificate verification process to display the blocking page. However, this can pose a security risk if not implemented correctly. It is also important to consider the issue of allowing users to specify their own DNS servers, as blocking such requests may create difficulties for users who require static DNS server settings. This may result in network engineers having to identify and resolve issues in the network. Overall, the proposed PowerDNS-based filtering solution provides a cost-effective and customizable approach to network traffic filtering, which can improve an organization's security and performance.*

Key words: *DNS, network, traffic filtering, network filtering, online privacy, online security.*

Introduction. Network traffic filtering has become an critical component of network infrastructure and businesses security strategies to prevent cyber threats and ensure high network availability and performance. The filtering system identifies and blocks malicious traffic while allowing legitimate traffic to pass through, thus reducing the risk of cyberattacks, such as DDoS attacks, malware, and phishing. Additionally, it optimizes network performance by reducing latency and improving response times.

PowerDNS-based traffic filtering system is gaining popularity as it provides a reliable and scalable solution for DNS management. PowerDNS enables advanced technologies such as RPZ, DNSSEC, and DNS-over-HTTPS (DoH) to enhance security and protect against threats [1].

One of the significant advantages of a PowerDNS-based traffic filtering system is its effectiveness against DDoS attacks, which are a prevalent type of cyber threat. The system filters out traffic that does not match defined criteria, reducing the risk of DDoS attacks. Additionally, PowerDNS's advanced load-balancing capabilities enable the efficient distribution of DNS queries, further improving network performance.

Another advantage of a PowerDNS-based traffic filtering system is its ease of management. The open-source PowerDNS software is relatively easy to set up and configure, and the DNS Firewall plugin allows for the straightforward definition of filtering rules. The solution is customizable and can be tailored to meet the specific needs of an organization.

In conclusion, a PowerDNS-based traffic filtering system offers several advantages over traditional DNS solutions, including enhanced security, improved network performance, increased reliability, compliance, and cost savings. It provides an effective and scalable approach to network traffic filtering and can be customized to an organization's specific needs, making it an attractive option for businesses and organizations seeking to enhance their security posture.

Benefits of DNS Traffic Filtering Systems Based on PowerDNS

DNS traffic filtering systems based on PowerDNS offer a range of benefits over traditional DNS solutions. Some of the key advantages include:

Enhanced Security: DNS traffic filtering systems can help prevent cyberattacks such as DNS spoofing, cache poisoning, and DNS tunneling by identifying and blocking malicious DNS traffic. With PowerDNS, organizations can leverage advanced technologies such as Response Policy Zones (RPZ), DNS Security Extensions (DNSSEC), and DNS-over-HTTPS (DoH) to further enhance security and protect against threats.
RPZ is a DNS zone that contains policies for domain name resolution. With RPZ, organizations can block or redirect traffic from known malicious domains, phishing sites, and other threats.

DNSSEC is a protocol that provides a secure way to authenticate DNS records and prevent DNS spoofing attacks. PowerDNS supports DNSSEC validation and signing for increased security.

DoH is a protocol that encrypts DNS queries to prevent eavesdropping and man-in-the-middle attacks. PowerDNS supports DoH for secure DNS resolution.

Improved Network Performance: DNS filtering can help optimize network performance by reducing latency and improving response times. PowerDNS can also enable organizations to distribute DNS queries more efficiently by leveraging its advanced load-balancing capabilities [2].

PowerDNS supports multiple load-balancing algorithms such as Round Robin, Random, and Geographical, allowing organizations to distribute DNS queries based on location, server availability, and other criteria. With PowerDNS, organizations can also implement caching to improve performance by storing frequently requested DNS records locally.

Increased Reliability: By filtering DNS traffic and redirecting queries to the appropriate server, PowerDNS can help ensure a more stable and reliable DNS service. This is especially important for organizations that require high availability for their critical applications.

PowerDNS supports advanced failover capabilities such as DNS-based Service Discovery (DNS-SD) and health checks, allowing organizations to automatically switch to a backup server in case of a failure. PowerDNS also supports multi-master replication, enabling organizations to maintain multiple copies of their DNS zones for increased redundancy.

Compliance: Many industries are subject to regulatory compliance requirements that mandate the monitoring and control of DNS traffic. DNS filtering systems based on PowerDNS can help organizations meet these requirements more effectively and efficiently.

PowerDNS supports logging and auditing features that allow organizations to monitor DNS traffic and generate reports for compliance purposes.PowerDNS also supports integration with third-party security tools such as SIEMs and threat intelligence platforms for enhanced visibility and threat detection.

Cost Savings: PowerDNS can help reduce costs by providing a scalable and flexible solution that can be deployed on-premises or in the cloud. It also offers a range of features that can help streamline DNS management and reduce administrative overhead.

PowerDNS supports containerization and virtualization, allowing organizations to deploy it on various platforms and infrastructure. With PowerDNS, organizations can also automate DNS management tasks such as zone creation, record updates, and DNSSEC key rotation, reducing administrative overhead and operational costs.

Filtered Encrypted Data: As encryption usage for data transmission increases, filtering encrypted traffic has become a challenge. PowerDNS-based DNS traffic filtering systems can filter encrypted data without decryption. This feature improves the DNS security of organizations by enabling efficient encrypted traffic filtering. It is especially essential for industries subject to regulatory compliance requirements mandating DNS traffic monitoring and control.

PowerDNS-based DNS filtering can also help ensure a more stable and reliable DNS service. By filtering DNS traffic and redirecting queries to the appropriate server, organizations can help ensure that their DNS service remains available and functioning properly. This is particularly important for organizations that require high availability for their critical applications, such as financial institutions, healthcare providers, and government agencies.

According to the above benefits of DNS traffic filtering systems based on PowerDNS, it becomes clear that such systems offer a range of advantages that can significantly improve an organization's DNS infrastructure. By implementing a PowerDNS-based DNS traffic filtering system, organizations can enhance their DNS security, ensuring that malicious traffic is identified and blocked before it can cause harm. This is particularly important in today's cybersecurity landscape, where cyber threats are becoming increasingly sophisticated and frequent.

In addition to improving security, PowerDNS-based DNS filtering can also optimize network performance by reducing latency and improving response times. This is particularly important for organizations that require reliable and fast DNS resolution for their critical applications. By leveraging PowerDNS's advanced load-balancing capabilities, organizations can distribute DNS queries more efficiently and ensure that their network is operating at peak performance.

Moreover, PowerDNS-based DNS filtering systems can help organizations meet regulatory compliance requirements related to DNS traffic monitoring and control. This is particularly important for industries such as finance, healthcare, and government, which are subject to strict compliance regulations. By providing a reliable and scalable solution for DNS traffic filtering, organizations can meet these requirements more effectively and efficiently.

Ultimately, implementing DNS filtering with PowerDNS can result in cost savings by offering a scalable and adaptable solution that can be deployed either on-premises or in the cloud. By doing so, organizations can minimize infrastructure and administrative expenses, while at the same time improving the reliability and efficiency of their DNS infrastructure. In general, deploying PowerDNS-based DNS filtering systems can provide various advantages that can greatly enhance an organization's DNS security, performance, reliability, compliance, and cost-effectiveness.

Proposed approach

Based on the reviewed literature and available technologies for network traffic filtering, a model for implementing a PowerDNS-based filtering solution can be proposed. The proposed model utilizes the open-source PowerDNS software for DNS resolution and filtering, which has been shown to be a reliable and scalable solution for DNS management. The filtering rules can be defined using the DNS Firewall plugin, which allows for the blocking or redirecting of DNS queries based on various criteria, such as domain names, IP addresses, or DNS record types [3].

To validate the proposed model, a testbed environment can be set up, which includes a number of client machines generating network traffic and a PowerDNS server instance with the DNS Firewall plugin enabled. The effectiveness of the filtering rules can be evaluated by analyzing the network traffic logs and comparing them to the expected results based on the defined filtering rules [4].

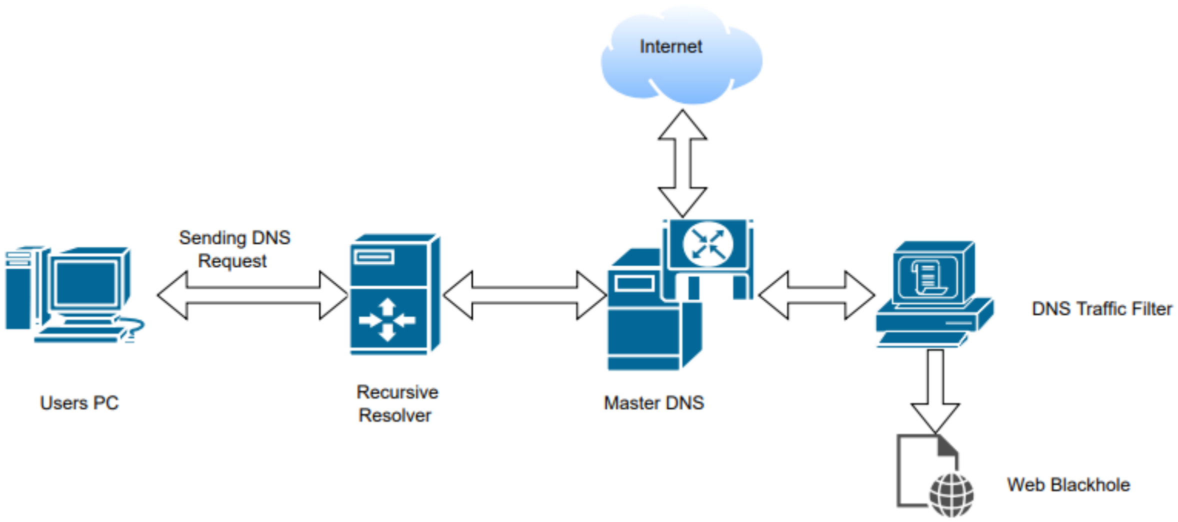
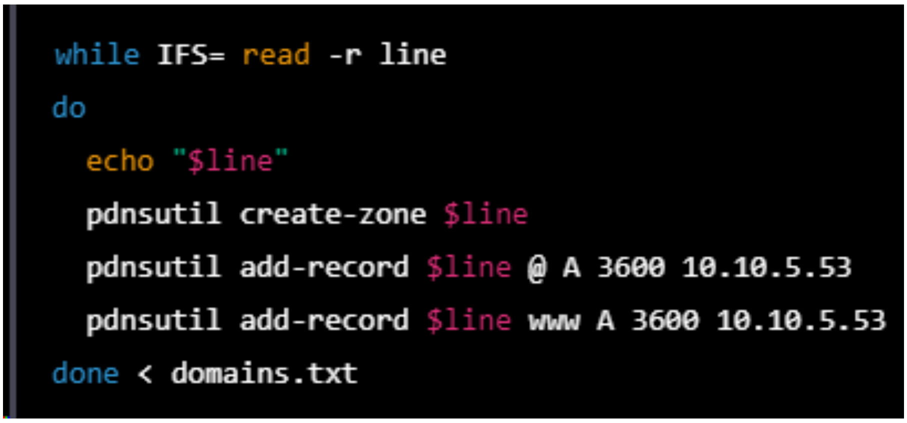


Fig. 1. Sending DNS request and filtering

Overall, the proposed PowerDNS-based filtering solution provides an effective and scalable approach to network traffic filtering, which can be customized to the specific needs of an organization. By leveraging open-source technologies, the solution can be implemented at a relatively low cost, while providing high performance and security.

Proposed model

The script is a Bash script that reads a list of domains from a file called "domains.txt" and performs three actions for each domain:



```
while IFS= read -r line
do
  echo "$line"
  pdnsutil create-zone $line
  pdnsutil add-record $line @ A 3600 10.10.5.53
  pdnsutil add-record $line www A 3600 10.10.5.53
done < domains.txt
```

Fig. 2. Building a DNS Zone Filtering System

Creates a new DNS zone for the domain using the "pdnsutil create-zone" command.

Adds an A record for the domain using the "pdnsutil add-record" command with the domain name, IP address, and TTL (time-to-live) values.

Adds a CNAME record for the "www" subdomain using the "pdnsutil add-record" command with the "www" subdomain, IP address, and TTL values.

The "while IFS= read -r line" command reads each line in the "domains.txt" file and assigns it to the "line" variable. The "echo "$line"" command simply prints the domain name to the console for tracking purposes.

The "pdnsutil" commands are part of the PowerDNS utility suite, which is used to manage DNS zones and records. The "create-zone" command creates a new DNS zone for the domain, and the "add-record" command adds a new record to the zone. In this case, the script adds an A record for the domain and a CNAME record for the "www" subdomain.

The TTL value specifies how long the record should be cached by other DNS servers before it needs to be refreshed. The TTL value of 3600 seconds (1 hour) is commonly used for A records.

After traffic filtering, if a website is blocked, a web page is displayed indicating that the resource is blocked. When describing this component, special attention should be paid to HTTPS resources. The problem is that it requires lifting the website's certificate, which can have a number of negative consequences. Therefore, a warning message may be displayed to the user indicating that the website's certificate cannot be trusted. This message is displayed because the certificate is either self-signed, expired, or has not been issued by a trusted certificate authority.

This is because the SSL certificate for a site needs to be verified before the connection can be established, and if the certificate cannot be verified, the connection will fail. In the case of a blocked website, the filtering software may attempt to display the blocking page before the certificate verification process can be completed, causing the connection to fail and the user to receive an error message instead of the intended blocking page.

To avoid this problem, the filtering software should be able to intercept and modify the SSL certificate verification process to allow the blocking page to be displayed. This requires special handling of HTTPS traffic and can pose a security risk if not implemented correctly.

Overall, while DNS filtering can be an effective way to improve an organization's security, the handling of HTTPS traffic requires special attention to ensure proper functionality and security.

In the context of this work, it's important to consider the issue of allowing users to specify their own DNS servers. If such requests are blocked, it may create difficulties for users who are in networks that require static DNS server settings. When these users move their device to the network of the company being discussed, they will lose Internet access, and they may not be able to identify or fix the problem on their own. This, in turn, adds work for network engineers who have to identify and resolve issues in the network.

One solution to this problem is to use Policy-Based Routing (PBR) and Destination NAT (DNAT) technologies to transform requests to any global caching DNS server into a local DNS server request. For example, requests to socket X.X.X.X:53, where X.X.X.X is an arbitrary destination IP address, can be redirected to Y.Y.Y.Y:53, where Y.Y.Y.Y is the internal recursive DNS server of the company. This solution allows users to continue using their preferred DNS servers while still maintaining connectivity when they connect to the company's network.

It is worth noting that there are some limitations to the use of the proposed approach. When using DNS over TLS and DNS over HTTPS, a user can successfully bypass network traffic filtering by reaching out to external DNS servers [3]. However, in cases where the ability to use a secure connection is unavailable, most operating systems and software automatically switch to using an insecure connection. As such, the effectiveness of the proposed approach may be limited when a user cannot use a secure connection. Definitive conclusions can only be drawn after further research on this issue.

Overall, this script automates the process of creating new DNS zones and records for multiple domains, which can save a significant amount of time and effort for system administrators managing large numbers of domains.

Overall. The article discusses the benefits of DNS traffic filtering systems based on PowerDNS, which provide an effective and scalable approach to network traffic filtering, allowing organizations to enhance their security posture. PowerDNS enables advanced technologies such as RPZ, DNSSEC, and DNS-over-HTTPS (DoH) to enhance security and protect against threats while optimizing network performance by reducing latency and improving response times. The open-source PowerDNS software is relatively easy to set up and configure and can be customized to meet an organization's specific needs. Additionally, PowerDNS-based DNS filtering systems offer improved reliability, compliance, cost savings, and can filter encrypted data without decryption. Overall, PowerDNS-based DNS traffic filtering systems offer a range of benefits that can significantly improve an organization's DNS infrastructure.

References

1. Mens J. P. Alternative DNS Servers: Choice and Deployment, and Optional SQL/LDAP Back-Ends. UIT Cambridge Ltd.; Illustrated edition. 2009. P. 113.
2. Grigorik I. High Performance Browser Networking. O'Reilly Media, Inc. 2013. P.10.
3. Hoang N. P., Polychronakis M., Gill Ph. Measuring the Accessibility of Domain Name Encryption and Its Impact on Internet Filtering. URL: https://storage.googleapis.com/pub-tools-public-publication-data/pdf/d1cc0cc9b507a8d9ef71c90c35caa9919b95a077.pdf (date of application: 04.04.2023).
4. Sanders Ch. Practical packet analysis : using Wireshark to solve real-world network problems. 2007. P. 2.