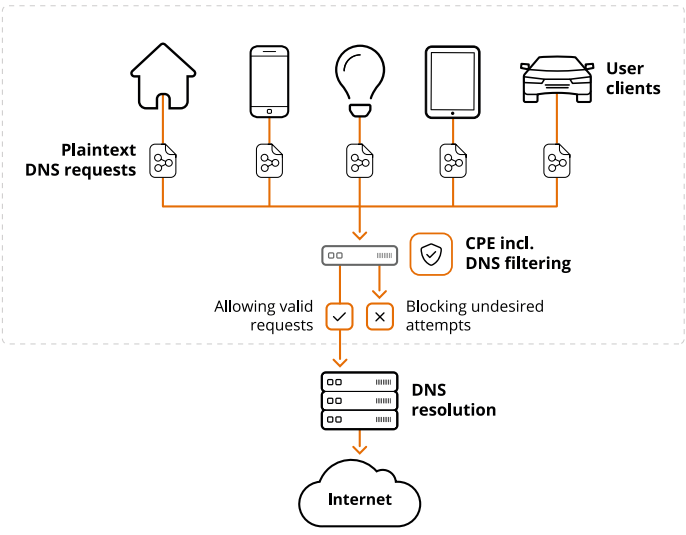
POWERDNS

DNS Encryption
For CPE-based Security

Keeping Users Secure with CPE-based Protection

DNS acts as the address book of the internet and is a key element in making services accessible by providing human-readable domain names for internet services. For consumers, any action on the internet starts with the client looking up the IP addresses of the service using the domain name system. These lookups are sent from the client (computer, phone, or other device in a house) to the Customer Premise Equipment (CPE[1]). This box is often referred to as 'the Internet Service Provider (ISP) router' or modem, which facilitates the connection to the ISP.



[1] The CPE often consists of a modem and router in one. This device acts as the connection point between a user's home network (via Wi-Fi or UTP cables in the house) and the internet provider's network (via DSL, cable, or fiber connections).

Because the CPE is the initial gateway into a user's network, ISPs like to use it to provide users with security and protection measures. This can include, for example, protection against malware, phishing, and other malicious activities, as well as parental control options. In addition, attacks such as Botnet activation and other Distributed Denial of Service (DDoS) attacks can be blocked on the CPE before they can harm the operator's network. To achieve this, ISPs, hardware manufacturers and security providers place security solutions on the CPE, which filter DNS traffic and block any malicious content before it reaches a user's connected devices.

As a result, devices that connect to the internet through the CPE can be secured from the network, which potentially complements or replaces any on-device protection.

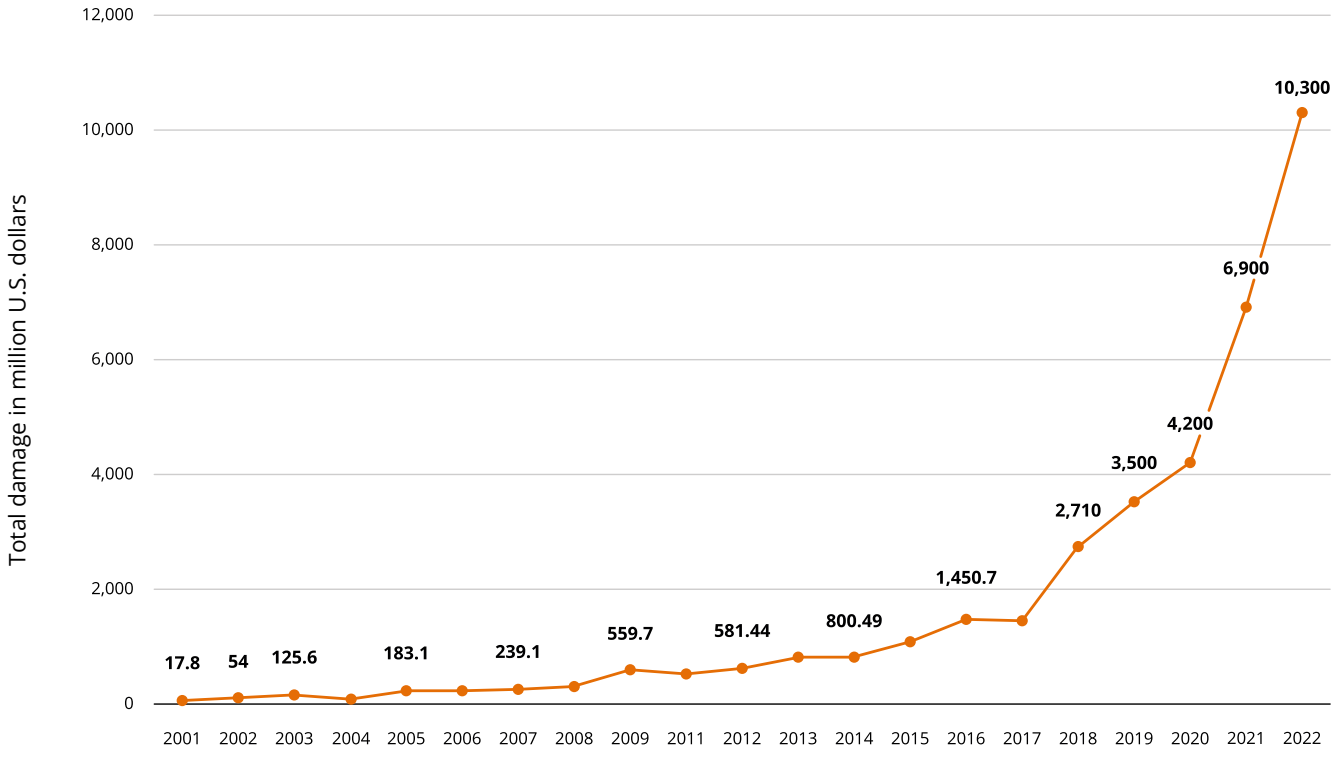
The importance of CPE-based filtering and other network security solutions is undisputed. The number of attacks, the methods used and the monetary damage caused by successful attacks have been increasing disproportionately for years[2].

In addition to increasing attacks on mobile devices, a rise in banking trojans and gaming scams, there has also been a noticeable increase in attacks targeting home and business routers, including the traffic passing this 'front door' into a user's network of connected devices[3]. Therefore, filtering of DNS traffic on CPE has an important part to play reducing the risks users are exposed to online.

[2] https://www.statista.com/statistics/267132/total-damage-caused-by-by-cyber-crime-in-the-us/

[3] https://info.allot.com/CyberThreatReportQ22022_ContentDownloadLP.html

Amount of monetary damage caused by reported cyber crime to the IC3 from 2001 to 2022 (in million U.S. dollars)



Additional Information: Worldwide; IC3; FBI; 2001 to 2022, excluding 2010; Cybercrime reported to IC3

Sources: FBI; IC3 ©Statista 2023

Ability to Analyze Internet Traffic

For this to work, the security solutions on the CPE must be able to analyze incoming DNS requests. Until recently, this was the case, because the requests consisted of plaintext DNS, which CPE-based security solutions were able to filter, block and so could be used to provide protection.

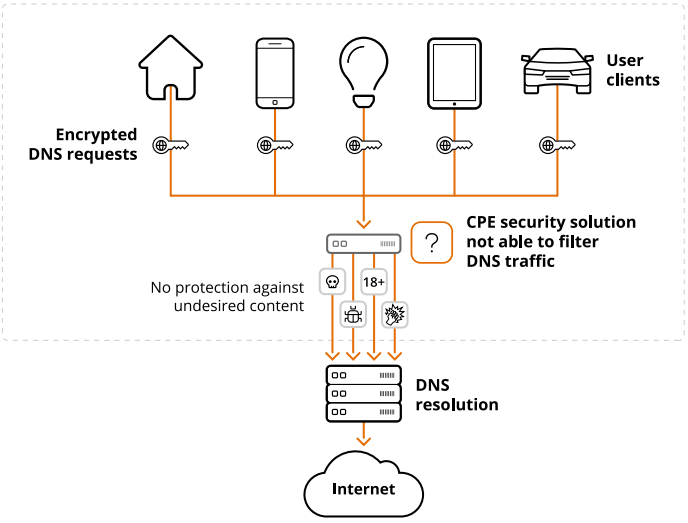
However, because DNS forms such a critical control point on the internet – and given that it was the last major unencrypted internet protocol – operators, browser vendors, operating system manufacturers and others are increasingly routing the transmission of queries over the internet as encrypted HTTPS traffic to provide end-user data privacy.

Complications From Increased Encryption of DNS

The increased awareness around privacy from internet providers led to huge interest for DNS encryption in the recent past, resulting in an increased use of encrypted DNS with DNS over TLS (DoT), DNS over HTTPS (DoH), DNS over QUIC (DoQ) and DNS over HTTP/3 (DoH3) protocols.

Due to this encryption of DNS requests, however, security solutions are no longer able to analyze the internet traffic, and therefore no longer provide adequate protection. This significantly reduces options for ISPs to provide security based on filtering DNS traffic. This also applies to security solutions placed on the CPE.

If they cannot handle encrypted DNS, they are no longer able to identify malicious traffic and protect users as usual.



DNSdist Enables Encrypted DNS on CPE

PowerDNS recognized the demand for additional privacy and started offering DoH and DoT to enable encrypted DNS for ISPs back in 2020, followed by the introduction of DoQ and DoH3 in 2024. In addition, PowerDNS understands the challenge of CPE-based security solutions and therefore extended the DNS encryption capabilities by providing a solution for CPEs.

DNSdist brings DNS encryption with Dot, DoH, DoQ and DoH3 to CPEs and therefore allows for the protection of the confidentiality and integrity of traffic in the first mile of internet access.

Given the limitations of CPEs with their very few resources, in order to allow DNSdist to run on this hardware, the memory usage and CPU consumption of DNSdist was reduced significantly for the typical 'in-house' use-case. DNsdist works effectively with OpenWrt's native configuration format (Unified Configuration Interface), so that it is easy to set up DNSdist via the usual interfaces, including the OpenWrt Web UI. In addition, DNSdist provides DHCP integration, so that it can learn about devices on the local network and provide native DNS resolution.

DNSdist also implements the ability to process queries and responses in an asynchronous way by suspending the query processing. Together with some further improvements, this provides the necessary mechanisms for an agent on the CPE to enable decision making for this specific query, thus allowing for filtering on the CPE.

At PowerDNS, we are very excited about this development and the possibilities it opens up. We believe that with this, DNSdist is an invaluable tool to have on routers, which will also help further drive the adoption of encrypted DNS while keeping security solutions and protection of user viable.

CPE manufacturers and solution providers are now able to offer security and encrypted DNS functionality on the router, close to the end-user.

powerdns.com | info@powerdns.com

POWERDNS