# DNS SECURITY SERVICE

## Apply predictive analytics to disrupt attacks that use DNS for command and control or data theft

**Benefits**

- Predict and block new malicious domains with machine learning
- Neutralize DNS-based tunneling
- Simplify security with automation and replace stand-alone tools

The Domain Name System (DNS) is wide open for attackers. According to Palo Alto Networks Unit 42 threat research team, almost 80 percent of malware uses DNS to initiate command-and-control (C2) procedures. Unfortunately, security teams lack basic visibility into how threats use DNS to maintain control of infected devices.

It's impossible to keep up with the high volume of malicious domains, let alone advanced tactics like DNS tunneling for stealthy data theft. Current approaches lack automation—requiring changes to DNS infrastructure—or drown you in uncoordinated data from independent tools. It's time to take back control of your DNS traffic.

### DNS Security Service

Palo Alto Networks DNS Security service applies predictive analytics to disrupt attacks that use DNS for C2 or data theft. Tight integration with Palo Alto Networks next-generation firewalls gives you automated protection and eliminates the need for independent tools. Threats hidden in DNS traffic are rapidly identified with shared threat intelligence and machine learning. Cloud-based protections scale infinitely and are always up to date, giving your organization a critical new control point to stop attacks that use DNS.

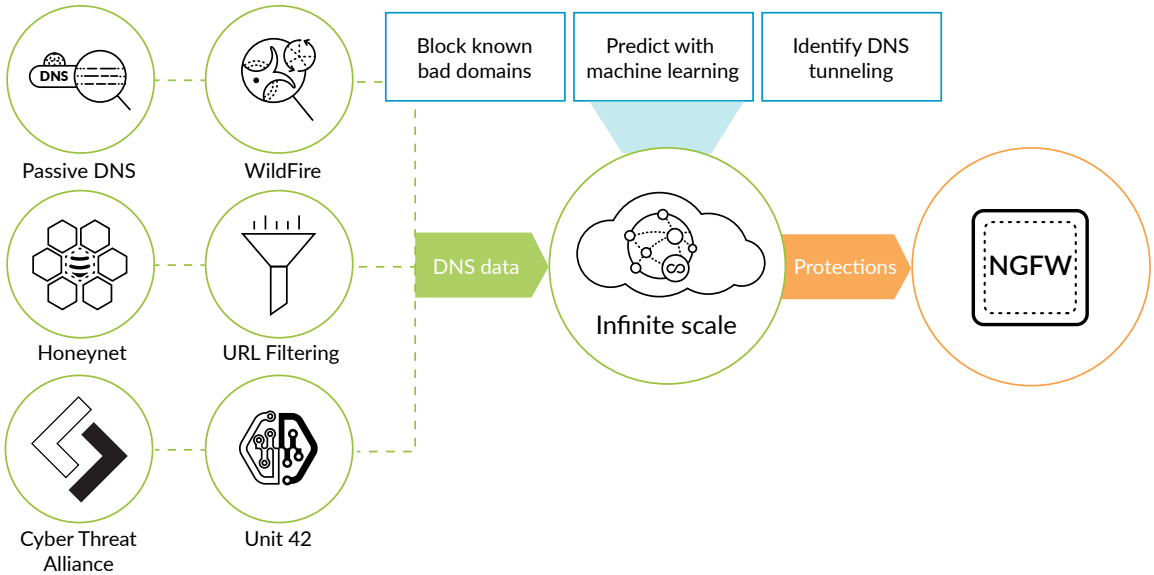


**Figure 1:** Rich DNS data powers machine learning for protection

### Predict and Block New Malicious Domains

DNS is a massive and often overlooked attack surface present in every organization. Adversaries take advantage of the ubiquitous nature of DNS to abuse it at multiple points of an attack, including reliable C2. Security teams struggle to keep up with new malicious domains and enforce consistent protections for millions of emerging domains at once.

The DNS Security service takes a different approach to predicting and blocking malicious domains, giving the advantage back to overwhelmed network defenders. Now, your Palo Alto Networks next-generation firewalls can:

- Automatically protect you against tens of millions of malicious domains identified with real-time analysis and continuously growing, global threat intelligence. Your protection continues to grow with data from a large, expanding threat intelligence sharing community. Our malicious domain database has been gathered over years, with sources including:
  - WildFire® malware prevention service to find new C2 domains, file download source domains, and domains in malicious email links.
  - URL Filtering to continuously crawl newfound or uncategorized sites for threat indicators.
  - Passive DNS and device telemetry to understand domain resolution history seen from thousands of deployed next-generation firewalls, generating petabytes of data per day.
  - Unit 42 threat research to provide human-driven adversary tracking and malware reverse engineering, including insight from globally deployed honeypots.
  - More than 30 third-party sources of threat intelligence to enrich our understanding.
- Predict and stop malicious domains from domain generation algorithm-based malware with instant enforcement. Malware's use of domain generation algorithms (DGA) continues to grow, limiting the effectiveness of blocking known malicious domains alone. DGA malware uses a list of randomly generated domains for C2, which can overwhelm the signature capability of traditional security approaches. DNS Security deals with DGA malware by using:
  - Machine learning to detect new and never-before-seen DGA domains by analyzing DNS queries as they are performed.
  - Easy-to-set policy for dynamic action to block DGA domains or sinkhole DNS queries.
  - Threat attribution and context to identify the malware family with machine learning for faster investigation efforts.
- Provide limitless protection against malicious domains with a cloud-based database for infinite scale. Your protections are always up to date, whether 10,000 or 100,000,000 new malicious domains are created in a single day. As part of the cloud-based service, all DNS queries are checked against our infinitely scalable, cloud-based database in real time to determine appropriate enforcement action. DNS Security service removes one of the most effective and widely used methods by which attackers establish C2, and its protection scales infinitely, ensuring your next-generation firewall can get ahead of new malicious domains before they cause harm.

### Neutralize DNS Tunneling

Advanced attackers use DNS tunneling to hide data theft or C2 in standard DNS traffic. The sheer volume of DNS traffic often means defenders simply lack the visibility or resources to universally inspect it for threats. Our DNS Security service lets you:

- Use machine learning to quickly detect C2 or data theft hidden in DNS tunneling. With historical and real-time shared threat intelligence, our algorithms observe the features of DNS queries, including query rate and patterns, entropy, and n-gram frequency analysis of the domains to accurately detect tunneling behavior.
- Extend PAN-OS® signature-based protection to identify advanced tunneling attempts. DNS Security expands the next-generation firewall's native ability to detect and prevent DNS tunneling. Protections are scalable and evasion-resistant, covering known and unknown variants of DNS tunneling.
- Rapidly neutralize DNS tunneling with automated policy action. DNS tunneling is automatically stopped with the combination of easy-to-set policy actions on the next-generation firewall and blocking the parent domain for all customers.

#### Unit 42 Threat Research on OilRig

OilRig is an active, organized threat group first discovered by Unit 42. Operating primarily in the Middle East, OilRig carefully targets organizations to further its regional strategic goals across multiple industries, including supply chain-based attacks. As part of its adversary playbook, the group employs sophisticated, custom DNS tunneling for C2 and data exfiltration. The use of tunneling includes:

- ALMA Communicator Trojan, which uses DNS tunneling to receive commands from the adversary and exfiltrate data. The malware employs specially crafted subdomains to send data to the C2 server and specific IPv4 addresses to transmit data from the C2 to the Trojan over DNS requests.
- Helminth PowerShell-based Trojan, which can obtain files from a C2 server using a series of DNS TXT queries repeated every 50 milliseconds, essentially building malware on victim systems through hard-to-detect increments sent over DNS.

OilRig's use of DNS tunneling allows the group to establish reliable C2 that can potentially evade existing defenses to carry out further stages of the attack. Get the full details on OilRig from Unit 42's blog post series or the interactive Playbook Viewer.

### Simplify Security with Automation and Replace Stand-Alone Tools

Security teams need integrated innovations that extend the value of their existing security investments without complicating operations. DNS Security takes advantage of the next-generation firewall platform to stop attacks using DNS, with full automation to reduce manual effort.

- Eliminate the need for independent DNS security tools or changes to DNS routing with next-generation firewall integration. Tight integration with the next-generation firewall platform provides a critical new control point to stop attacks that use DNS, extending your existing investment. The service ensures you have one device to deploy, with a single set of policies to manage. Alerts are coordinated across your entire security stack, including firewall policy violations, IPS/IDS, web security, and malware analysis.
- Automate dynamic response to find infected machines and quickly respond in policy. When attacks using DNS are identified, security administrators can automate the process of sinkholing malicious domains on the firewall to cut off C2 and rapidly identify infected users on the network. Combining malicious domain sinkholing, Dynamic Address Groups, and Logging Actions automates detection and response workflows, saving analysts time by removing slow and manual processes.
- Seamlessly take advantage of the latest DNS security innovations through our extensible, cloud-based architecture. The DNS Security service is built on a modular, cloud-based architecture to seamlessly add new detection, prevention, and analytics capabilities with zero customer impact. We will continue to use our rich shared threat intelligence and native enforcement capabilities to deliver new innovations against attacks using DNS.

### Protection Without Performance Impact

Advanced security is seamlessly applied to DNS queries in real time with no business impact. The service is hosted on our global security service delivery network to provide the low latency and high performance necessary to minimize impact to DNS traffic on customer networks.

### Trust and Privacy

Palo Alto Networks DNS Security service has strict privacy and security controls in place to prevent unauthorized access to sensitive or personally identifiable information. We apply industry-standard best practices for security and confidentiality. You can find further information in our privacy datasheets.

### DNS Security Requirements

To use Palo Alto Networks DNS Security service, you will need:

- Palo Alto Networks next-generation firewalls running PAN-OS® 9.0 or later
- Palo Alto Networks Threat Prevention license

### Licensing Information

The DNS Security license is available as an integrated, cloud-based service for the Palo Alto Networks next-generation firewall platform. It is also available as part of the Palo Alto Networks Subscription ELA or VM-Series ELA.

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com