A summary of the DNS control and threat prevention mechanisms supported by the Palo Alto Networks next-generation security platform.

- Accurately identify, control and inspect DNS traffic.
- Block DNS queries to malicious domains as a means of breaking the C2 channel.
- Identify compromised hosts on your network through DNS sinkholing.

DNS is a very necessary and ubiquitous application, as such, it is a very commonly abused protocol for command-and-control and data exfiltration. This tech brief summarizes the DNS classification, inspection and protection capabilities supported by our next-generation security platform, which includes:

1. Malformed DNS messages (symptomatic of vulnerability exploitation attack).
2. DNS responses with suspicious composition (abused query types, DNS-based denial of service attacks).
3. DNS queries for known malicious domains.

Our ability to prevent threats from hiding within DNS is best highlighted by describing our overall approach to preventing threats which begins with the accurate classification of DNS (App-ID™) and our positive security model, and then describing the specific DNS threat prevention capabilities.

Accurately Classifying DNS
First off, App-ID is our traffic classification engine that uses up to four mechanisms (signatures, application and protocol decoders, heuristics) to determine the identity of the traffic. In order for DNS to traverse our device, it will be sent through the DNS decoder within App-ID to ensure that it is indeed DNS and then it can be allowed by policy. Our next-generation security platform allows you to create a policy using App-ID that allows the DNS application only over port 53. By creating a policy with that application specified in the policy, you ensure that only DNS traverses over 53, and not proprietary C2 traffic. Even if a C2 protocol piggybacks on legitimate DNS (i.e. tcp-over-dns, or any number of tools that leverage TXT records and recursive queries), these types of traffic will fall out of the DNS decoder and into another type of application, which would then be denied based on your security policy. With this positive security (whitelist) model, we need not create an IPS signature for each type of DNS abuse we see. We simply allow the known good DNS usage patterns, while blocking everything else. As a means of enforcing additional security-best practices, the firewall policy can also be configured to:

- Block traffic from unauthorized source addresses to enforce that DNS traffic from clients only go to the local DNS resolver, and that the only DNS that leaves/enters the network is from/to the local DNS resolver.
- Identify, alert, and block DNS traffic on a non-standard port or going to unexpected hosts. This is an integral capability of App-ID, our full stack classification engine.
- Detect non-DNS traffic on port 53 by identifying and logging every session at the application layer with App-ID to determine if the traffic on port 53 is legitimate DNS, or if it is identified as something else, such as a known DNS tunneling application or even simply “unknown”. This traffic can proactively be blocked using App-ID and a positive security model, or blocked using a search-and-destroy negative model, or simply alerted in logs to bring it to the administrator’s attention.
Inspecting DNS Traffic
After the traffic passes the application-level allow/block decision, our threat prevention engine analyzes the traffic to look for known malicious, high risk, or suspicious content and block it based on policy. In the case of DNS, this can mean many things, such as: suspicious query types such as zone transfers or “any” queries (information leak); DNS amplification attacks from either the intermediary or the ultimate victim (DDOS); DNS cache spoofing attempts; and queries for known malicious domains determined via Domain Generation Algorithms (DGA) analysis, malware sandboxing, or our global passive DNS network.

Blocking Known Malicious Domains
Our DNS-based threat detection allows you to block DNS queries to malicious domains as a means of breaking the command-and-control channel while also alerting the administrator of the compromised machine. The DNS intelligence we use to execute this function comes from several sources:

• Reverse engineering and automatic “fast forwarding” of Domain Generation Algorithms that we see being used in malware.

• Malware received by WildFire™ is dynamically analyzed in a virtual machine environment to detect domains queried for C2 purposes. The results are delivered to your device in the form of scheduled content updates.

Discovering Malicious Domains with Passive DNS and WildFire
The passive DNS network feature allows you to opt-in to share anonymized DNS query and response data with our global passive DNS network. The data is continuously mined to discover malicious domains that are then added to the PAN-OS DNS signature set that is delivered daily, enabling timely detection of compromised hosts within the network and the disruption of command-and-control channels that rely on name resolution. Data from the passive DNS network is used to “predict” malicious domains; rather than rely solely on direct observations of malware querying domains in a sandbox, we can see if a domain that is queried on a customer network is related to known malicious domains by any number of indicators, such as shared records, name servers, or other heuristics on the domain name itself.

WildFire complements the passive DNS feature by performing malicious domain and command-and-control traffic analysis through sandbox execution of potentially malicious files to find previously undetected malware (APTs). If malware is present, a signature is delivered to all WildFire customers and additional malicious domain and C2 protection mechanisms are then delivered via scheduled device updates.

Controlling Malicious DNS Traffic with DNS Sinkholing
When compromised hosts on the network query DNS to resolve their command-and-control servers, you can alert, block, or sinkhole the query using the DNS sinkholing feature. Sinkholing refers to the ability of the firewall to send a forged response to temporarily poison local DNS cache to cause the malicious domain to resolve to an IP address of your choosing. This can be used to quickly identify compromised hosts on the network using DNS data by discovering which hosts have attempted to initiate sessions to the sinkhole IP. This feature can also be used to route malicious traffic to an internal analysis environment such as a honeypot or other analysis platform to perform packet captures or interact with the compromised host to gather intelligence.