DNS Firewalls Importance in Enterprise Security

The reason traditional firewalls are inadequate against today's threats is because they leave a huge pathway into your enterprise completely unprotected. Cyber criminals use that pathway to infiltrate your network hence the need for another firewall.

Introducing the DNS Firewall

Focus now moves from firewalls and IDS/IPS solutions to DNS resolvers that function as firewalls for DNS to combat advanced persistent threats (APT) and other malware that circumvent traditional perimeter defenses.

Extensive use of network security measures has not slowed down attackers who exploit unprotected DNS-based Internet infrastructure to infiltrate and exfiltrate valuable information without detection. Use of DNS firewalls would have prevented most of these attacks.

What is a DNS Firewall?

Apart from preventing the entire enterprise from malicious internet locations, the enterprise security teams rely on DNS firewall to provide immediate feedback about potential compromises like botnets and APTs on their networks. An enterprise can use DNS gateway to ensure its employees and IT systems are not routed to malicious destinations arising from the addition of malicious domains or hostname to the configuration of the DNS resolver server.

Availability of the current DNS resolver infrastructure as a foundation is another advantage of a DNS firewall because you don't have to install hardware, perform software upgrades or reconfigure networks. In days or hours, a DNS firewall can be deployed via vendor solutions, or with a few scripts, some good data sources, and help from DNS administrator. Vendor solutions are the most preferred amongst enterprises but the trick is in how comprehensive, timely, and accurate your threat data is and how sure you are of your implementation.

Why a DNS Firewall is so Important

A connection of an enterprise to a malicious location through the resolver jeopardizes security. Enterprises are unable to identify malicious locations and protect enterprise users because the DNS resolver they use today is susceptible to various direct attacks and lacks a built-in security layer.

Spear phishing attacks also effectively drop malware since they appear to come from trusted sources. Such malware uses hostnames, or an algorithm for generating those hostnames on the fly, rather than hard-coded IP addresses when determining where to find its C&C server. Enterprises know almost all malware attacks by their DNS communications patterns and can prevent attacks with properly maintained DNS firewall that blocks access to information by preventing the connection and/or diverting traffic from any infected computers to a safe server for inspection.

Driving DNS Firewall Adoption

A DNS firewall in place offers protection from breaches resulting from hostnames the security community was already aware of or became aware of well before the companies hit by them found out via traditional methods. Despite not being a new technology and several companies offering “clean” DNS, the consumer-focused solutions are not widely implemented, and often don’t work well in an enterprise environment.

Traditional firewalls are great but the industry needs to protect the DNS layer from increased attacks by criminals and hackers who are aware of existing holes in the security of the Internet’s infrastructure.