Using Domain Ownership History to Secure Next-Gen Firewall Estates

Posted on January 23, 2020

Firewalls are an essential pillar of any enterprise network security strategy. They sift traffic coming in and going out of corporate networks, offering round-the-clock perimeter protection.

Even better are today's next-generation firewalls (NGFWs), which bring interoperability and contextualization into the mix. These hybrid firewalls provide a more effective layer of protection as they combine both traditional firewalls with newer types.

Unfortunately, NGFWs and older versions for that matter are not the "be-all and end-all" of enterprise network security. They serve as a good starting point, but they also need to be appropriately configured to work — along with the right data feeds, which can include WHOIS history data, as this post will suggest.

That is why experts recommend taking a phased approach to high-end firewall deployment. Otherwise, compatibility issues may arise, which could expose the network to computer viruses, or worse still, advanced persistent threats (APTs).

NGFW Implementation Recommendations

As with any technical innovation, NGFWs have their limitations too. For instance, unknown traffic passing through them needs to meet a threshold for it to establish a connection between applications. Another example is their overreliance on match conditions. It's essential to find the sweet spot between advantages and disadvantages, bearing in mind to supplement controls during the transition.

Here are some best practices that we have adapted from the National Institute of Standards and Technology (NIST). We found that the guidelines in this well-referenced document still apply in today's NGFWs environment.

Slowly roll out NGFWs in priority segments

Organizations don’t have to replace all firewalls in their endpoints and perimeters as it’s impractical and labor-intensive. However, they can save on costs in the long run by slowly implementing NGFWs in zones or systems that store sensitive data for regulated industries. High-risk segments such as banking and healthcare can derive the most value from NGFWs.

Set up a testing environment

Running the firewall solution in a lab before launching it in a production environment can spare engineers unnecessary headaches. Testing the appliance in a lab helps them determine whether it is fit for current configurations or if it has to be modified to avoid problems down the line.

Introduce new application rulesets in stages

Modifying your firewall controls and policies at once can spell disaster for your organization. To prevent data leakage, seek out protocol-related vulnerabilities and misconfigurations before adding new firewall rulesets. Ensure that all issues are resolved before deployment and continue to monitor the product after that.

How Domain Ownership History Aids NGFW Protection

Over the past two decades, security professionals have seen the concept of threat intelligence find its footing in the cybersecurity industry. More significant volumes of cyberattacks have driven the need for threat data among organizations, and a source that has proved invaluable to analysts is

WHOIS.

WHOIS records and tools provide cybersecurity researchers with actionable intelligence. In NGFW environments, they can aid security engineers in fine-tuning strategies and application controls by providing more profound insights into attack surfaces. Described below are some functionalities where domain history data can help.

Note that the said data is available when using our Domain Research Suite dashboard for manual investigations, our bestwhois command-line tool, as well as programmatically using WHOIS History API.

- **Deep packet inspection (DPI):** This enables enterprises to catch vulnerabilities and threats at the network layer and prevent lateral movement. With accurate domain data, administrators can more easily block domains, IP addresses, and countries that are sending their network unnecessary traffic. They can also enhance the quality of their inbound and outbound traffic and promptly respond to downtimes.

- **Data enrichment:** Detailed historical domain information help users transform events into meaningful intelligence. It allows penetration testers and cyberforensic analysts to isolate threats from raw logs and add more context to them. Domain data, which includes ownership timelines, registrants, and locations, allows cyber investigators to profile threat actors should they hit a dead end.

- **Incident response and mitigation:** Threat actors often use a collection of newly registered domains to deliver the payloads for their malicious campaigns. Incident responders can review the WHOIS records of domains that communicate with their networks for blocking, additional research, or documentation.

- **Access control management (ACM):** Domain data can be used to verify the identities of people who use software and applications within your network. After identifying domains through their IP addresses, security analysts can run these through a WHOIS lookup tool. Then they can apply access restrictions by port or application based on specific user attributes.

- **IP whitelisting and blocking:** WHOIS records give network security specialists an idea of how reputable a domain is, based on its ownership history, registrar, and violations. Our WHOIS history database and WHOIS History Search tool contain information on millions of generic top-level domains (gTLDs) and country-code top-level domains (ccTLDs) that users can reference for accurate IP address analysis. They can then configure their firewall rules to whitelist or blacklist specific IP addresses or netblocks.

As more organizations deploy NGFWs, it's crucial for the security professionals managing them to stay abreast of firewall deployment and threat intelligence trends. **Domain ownership history** records and similar forms of shared intelligence can provide engineers with expert insights into threats that could affect their networks.