SOLUTION BRIEF

Fortinet and Cloudflare Area 1 Integrated Email Security Solution

Comprehensive Protection Against Phishing Attacks and Business Email Compromise

Executive Summary

The Fortinet FortiGate Next-Generation Firewall (NGFW) integrates with Cloudflare Area 1 to enhance network and web defenses and protect customers from targeted phishing attacks. Area 1 email security integrates quickly and easily with FortiGate NGFWs, updating them automatically with emerging phishing infrastructure and campaign indicators to enable advanced, effective protection from targeted attacks.

Even the best conventional security defenses are unable to preempt phishing attacks, which are the root cause of the majority of cybersecurity-related data breaches and subsequent financial loss. The fact that the attacks are often multi-vector, hitting email, web, and network traffic, makes finding and defending against them all the more challenging and complex. Sophisticated threats are dynamic, with attackers launching and shutting down phishing sites and payloads within hours. Traditional email security defenses rely on knowledge of yesterday's active attack characteristics, and therefore can't reliably defend against targeted phishing attacks, such as business email compromise (BEC), that continually evolve.

Early visibility into phishing sites and campaigns

What's needed is forward-looking security technology that is aware not only of yesterday's active phishing payloads, websites, and techniques but also provides early insight into phishing sites before campaigns launch and attacks are active.

Fortifying defenses with security technology that hunts for malicious sites before attacks launch—during the weeks and months hackers are establishing or compromising websites to prepare for launching an attack—can provide the early visibility and threat indicators necessary to protect from impending attacks. Arming email, web, and network cyber defenses with early insight into phishing sites and payloads enables these defenses to more effectively detect and block phishing email, malicious web downloads, attacker movement through your network, command-and-control communication, and data exfiltration to external sites. To reduce the risk of cyber breaches, organizations need earlier visibility into phishing sites and payloads before attacks launch.

FortiGate-Area 1 Email Security Solution Components

- Cloudflare Area 1 Security
- Fortinet FortiGate NGFW

Solution Benefits

- Protects across all attack vectors: network, web, and email traffic
- Stops web-based phishing, such as credential harvesting and dropper attacks
- Thwarts network phishing activity, including attacker lateral movement, command-and-control traffic, and data exfiltration
- Integrates seamlessly in minutes
- Facilitates security orchestration with automated updates

The Fortinet and Cloudflare Area 1 Integrated Security Solution

Area 1 anti-phishing service integrates with the FortiGate NGFW to enhance network and web defenses and protect customers from targeted phishing attacks.

Email is the most widely adopted and frequently attacked cloud application. Area 1 removes implicit trust from the this primary cyber-attack vector to preemptively stop phishing and BEC attacks. Through never trusting a sender, all user traffic including email is verified, filtered, inspected, and isolated from internet threats. Area 1 analyzes content, context, and social graphs of email communications to stop "needle in the haystack" email threats, and enforces multiple layers of inbox protection for defense-in-depth.

Area 1 integrates quickly and easily with FortiGate NGFW enterprise firewalls and updates them automatically with emerging phishing infrastructure and campaign indicators. The FortiGate NGFW recognizes the predetermined security rules and acts on the information shared by Area 1. Together, the joint solution offers superior detection and blocking of web-based and network-based phishing activity.

FortiGate-Area 1 Email Security Solution Components

- **Cloudflare Area 1 Security:** Gain early visibility into phishing sites, malware payloads, and compromised email accounts before attacks launch. Area 1's preemptive and comprehensive anti-phishing service detects and blocks phishing threats that traditional secure email gateways and cloud email suites miss.
- **Fortinet FortiGate NGFW:** FortiGate NGFW enterprise firewalls offer flexible deployments from the network edge to the core, data center, internal segment, and the cloud. FortiGate NGFW enterprise firewalls leverage purpose-built security processors (SPUs) that deliver scalable performance of advanced security services like threat protection, SSL inspection, and ultra-low latency for protecting internal segments and mission-critical environments.

Cloudfare Area 1-Fortinet FortiGate NGFW Integration

The FortiGate-Area 1 email security solution offers fortified enterprise firewall phishing protection and easy deployment.

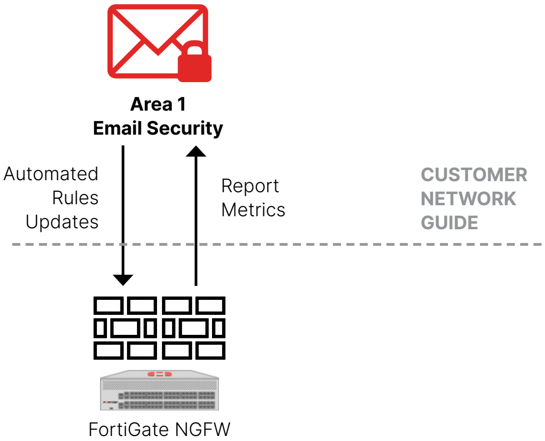

Figure 1: Cloudflare Area 1 and FortiGate NGFW joint integrated solution for advanced phishing defense

Joint Use Cases

Phishing attack vectors

Attacks can trick victims into unknowingly downloading malware that is hidden in email file attachments or on web pages. Once the victim's device is infected, the hacker can gain access to networks and systems and establish communication with external phishing sites to exfiltrate data. To protect from such attacks, the FortiGate-Area 1 email security solution threats across all attack vectors, including email, web, and the network.

Phishing sites and campaigns are dynamic

When executing phishing campaigns, hackers first compromise trusted websites and email servers, or establish imposter websites and email accounts—weeks or even months in advance of a planned attack. After setting up a phishing site, hackers launch and shut down their attacks in a matter of hours. The FortiGate-Area 1 email security solution can detect the dynamic nature of such phishing sites to initiate prevention and remediation measures in real time even before the attacks are fully launched.

About Cloudflare

Cloudflare, Inc. (www.cloudflare.com/@cloudflare) is on a mission to help build a better Internet. Cloudflare's suite of products protect and accelerate any Internet application online without adding hardware, installing software, or changing a line of code. Internet properties powered by Cloudflare have all web traffic routed through its intelligent global network, which gets smarter with every request. As a result, they see significant improvement in performance and a decrease in spam and other attacks.

FORTINET

www.fortinet.com

August 17, 2022 11:21 PM
1701251-0-0-EN