CLOUDFLARE
AREA 1 SECURITY

FORTINET

Fortinet and Cloudflare Area 1 Security

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

Challenge

Email is the most widely adopted and frequently attacked cloud application. Even the best conventional security defenses are unable to preempt phishing attacks, which are the root cause of about 90% 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.
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.

Solution

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.

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.

Benefits

Protects across all attack vectors: network, web, and email traffic

Stops web-based phishing, such as credential harvesting and dropper attacks

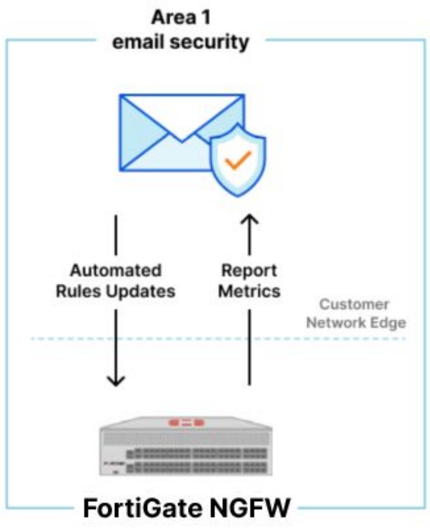
Thwarts network phishing activity including attacker lateral movement, command-and-control traffic, and data exfiltration

Integrates seamlessly in minutes

Facilitates security orchestration with automated updates

Integration overview

Fortified enterprise firewall phishing protection and easy deployment of the FortiGate-Area 1 email security solution:



Joint Use Cases

Phishing attack vectors

Attacks can trick victims into unknowingly downloading malwares that are 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 solution can not only detect but also block threats across all attack vectors, including email, web, and 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. FortiGate-Area 1 can detect the dynamic nature of such phishing sites to initiate prevention and remediation measures, even before the attacks are fully launched.

FortiGate-Area 1 email security solution components

- Cloudflare Area 1 email security
- Fortinet FortiGate NGFW