FORTINET

Product Name: Fortimanager

Main Website: https://www.fortinet.com/

Product Website: https://www.fortinet.com/products/management/fortimanager.html

Product Integration Type

Firewall

Integration Objective

- Integrates with Fortimanager to mitigate malicious IP addresses and web URLs
- Currently only Fortimanager is supported, Fortigate integration is not supported in this release
- Cyphort compiles the list of malicious IP addresses from CNC IP addresses seen in infections and web URLs from network downloads. To avoid false-positives, the reputation of CNC IP addresses and web urls are checked
- As of version 3.5, SmartCore pushes the CNC IP addresses and web URLs automatically to Fortimanager without any need for manual intervention

Customer Value Proposition

Integrates with existing third party infrastructure in the customer's environment to block calls to malicious CNC server IP addresses and bad websites. Integration with Fortimanager makes it easier to push IP addresses and web URLs to multiple Fortigate devices.

Tested Vendor Versions

Fortimanager Version: 5.4

Integration Classification

Blocking: Firewall and Web Proxy

Integration Details

Enterprise. Can work in large environments with a variety of integration points.

Integration Method

Push: SmartCore pushes CNC IP addresses and Web URLs to Fortimanager

Integration Detail Summary (API, CLI)

- CNC IP addresses are pushed to Address Group in Fortimanager
- Mitigated URLs are pushed into a custom web filter profile; necessary action can be taken on this profile
- CNC IP addresses and Web URLs can be added or removed from Fortimanager using Cyphort UI
- User can also specify “expiry days” on the Cyphort Manager UI to automatically remove the CNC IP addresses from Fortimanager after the specified number of days expire
- SmartCore uses Fortimanager’s JSON/REST API to push blocked CNC IP addresses
- FortiManager configures a policy package referencing the address group and web filter profile name created above. Installation targets for the policy package need specified for the Fortigate devices

Cyphort Manager GUI Component

- Yes
- Cyphort Manager configuration: Settings are configured under Settings -> Environmental Settings -> Firewall Mitigation Settings

GUI Operational Use Case

Under the Mitigation tab in the Cyphort Manager, the CNC IP addresses show up under Firewalls. The web URLs show up under Secure Web Gateway. The administrator can push or remove IP addresses/web URLs from the Fortimanager manually. From release 3.5 onwards, CNC IP/web URL addresses can be pushed automatically to Fortimanager without the need for manual intervention.

Threat Score Impact

No

Integration Documentation

N/A

Integration Demo

No

About Cyphort

Cyphort is a privately held cybersecurity company founded in 2011 and based in Santa Clara, CA. The company provides SMB and enterprise customers with the Anti-SIEM, an open, scalable software platform that combines advanced threat detection, analytics, and mitigation capabilities. The solution minimizes the cost and complexity of traditional SIEMs, while delivering immediate, actionable insight into security incidents for fast threat resolution. www.cyphort.com

CYPHORT

5451 Great America Pkwy, Suite 225, Santa Clara, CA 95054 | P 1.408.841.4665 | F 1.408.540.1299 | info@cyphort.com

Sales/Customer Support P 1.855.862.5927 | F 1.408.540.1299 | support@cyphort.com