IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 21, Issue 3, Ser. III (May - June 2019), PP 34-36
www.iosrjournals.org

Comparison between Cisco ASA and Fortinet FortiGate

Mohammed Faizan[1], Sujay S. Hegde[2], Nagaratna V. Yaligar[3*]
[1]Computer Science, KLE Technological University, Hubballi-580021, India
[2] Computer Science, KLE Technological University, Hubballi-580021, India
[3] Computer Science, KLE Technological University, Hubballi-580021, India*
Corresponding Author: Nagaratna V. Yaligar

Abstract *: Network Security is major concern for all organizations. There are different types of network security, that can be implemented on organizations such as application security, network access control, email security to mention a few. A firewall is a type of network security that acts as the gateway between internal and external network. It restricts potential attacks to gain critical information and prevents unauthorized access to the private network. The objective of this paper is to provide information about the architectural features and their benefits of NGFW solutions provided by Cisco's Adaptive Security Appliance (ASA) and Fortinet's FortiGate.*

Keywords: *ASA, FortiGate, NGFW.*

Date of Submission: 10-05-2019 Date of acceptance: 27-05-2019

I. Introduction

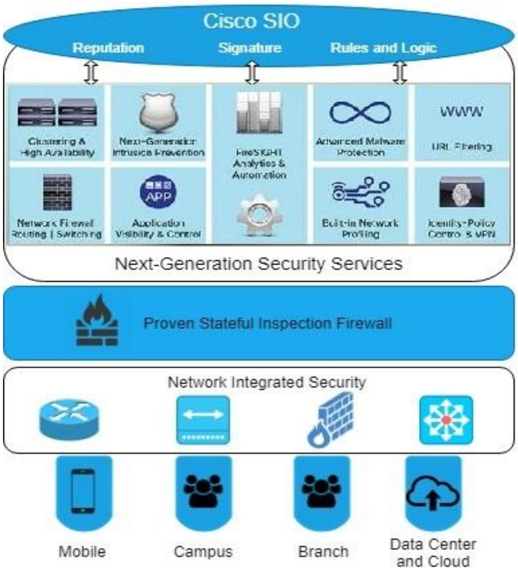
A computer network, is a cluster of computers and devices that are connected together, to carry out the process of communication and information sharing. Over the years there have been significant rise in cyber-attacks against organizations, as a network contains loopholes which is used by hackers to gain unauthorized access into the computer system to steal or damage vital information of an organization. An organization may also be jeopardized if its network gets infected through spyware and virus attacks. Hence firewall is a standard requirement and an essential security tool for companies. There are different types of firewalls used such as the packet-filtering firewall, proxy firewall, circuit-gateway firewall, to mention a few. However, the Next Generation Firewalls (NGFWs) are more advanced versions of firewalls and provide several benefits compared to the traditional firewalls. This paper aims to compare the two leading NGFWs, the Cisco ASA and Fortinet FortiGate. The parameters taken into consideration are throughput, performance, security, configuration & management of the firewalls.

II. Cisco ASA

Cisco ASA is a standalone product that provides firewall features. But when combined with Firepower services, it becomes a NGWF solution which is designed to maintain a balance between performance and modularity. Typically, Cisco ASA software integrated with Firepower service runs on Linux platform and provides a throughput up to 320Gbps. However, higher throughput can be achieved by disabling IPS service for the traffic. The NGFW product is built to work together with the ASA series to provide more than just access control and traffic filtering.

Cisco ASA acts as an interface between the internal network and the internet. The ASA family can be implemented on networks of varying sizes (small, medium, and large). Like any other firewall, Cisco ASA provides a few benefits to enterprises including Intrusion Detection System (IDS), antivirus software, URL filtering and load balancing. However, if integrated with services offering critical security technologies like Firepower, Cisco cloud web security, and Cisco Identity Services Engine (ISE), it will deliver higher performance, next-generation IPS/IDS solution, modularity, and availability.

Cisco ASA's architecture is built upon Cisco SecureX architecture which is comprised of three main components - Cisco TrustSec, Cisco AnyConnect, and Cisco Talos responsible for security, superior connectivity and threat intelligence respectively. The latest Cisco ASA software release 9.0 introduces Cisco Cluster Link Aggregation Control Protocol (cLAP) which enables multiple ASA devices to be clustered and managed as a single entity in order to increase throughput and connectivity. The Suite B cryptographic encryption is included in the architecture as it uses the Eliptic Curve technology necessary to provide remote access and site-to-site connection.


Cisco SIO
Reputation
Signature
Rules and Logic
Clustering & High Availability
Next-Generation Intrusion Prevention
FireSIGHT Analytics & Automation
Advanced Malware Protection
URL Filtering
Network Firewall Routing | Switching
Application Visibility & Control
Built-in Network Profiling
Identity-Policy Control & VPN
Next-Generation Security Services
Proven Stateful Inspection Firewall
Network Integrated Security
Mobile
Campus
Branch
Data Center and Cloud

Cisco ASA Architecture

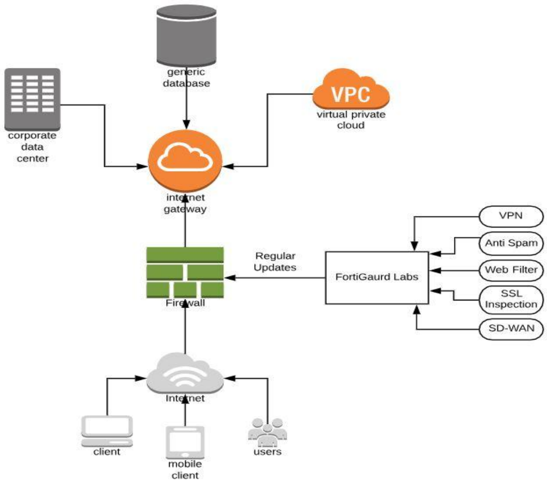
III. Fortinet Fortigate

Fortinet FortiGate’s next generation firewall solution is secure against most external threats to an organisation. The FortiGate firewall is based on Linux kernel running on FortiOS (proprietary). It provides high end performance for almost all types of traffic including encrypted traffic, which is becoming popular recent times. FortiGate’s throughput ranges from 17Gbps to 1Tbps.

FortiGate uses two component architecture enabled with parallel path processing, to optimize the throughput performance. This makes the system data-packet independent. The two components are Content Processor (CP) and Network Processor (NP). The CP series operates outside the traffic flow purview and provides rapid cryptography facility which helps inspect the traffic content. The encryption algorithms used to monitor the traffic include AES (AES-GCM, AES256, AES192, AES128) and DES (3DES, DES). The NP series works with the dedicated operating system (FortiOS) to deliver high-end performance for different internet protocols like IPV4 and IPV6. FortiGate also handles multicast traffic with the least latency (about three microseconds).

FortiGate NGFW provides intent based packet segmentation for granular control over the encrypted traffic. The ability of the NGFW to detect and monitor encrypted traffic depends on the chipset and its capacity to scan SSL encrypted traffic. One such product is the FortiGate 3000E series, which provides 30 to 34 Gbps of SSL inspection (encrypted traffic inspection).

When FortiGate NGFW is coupled with the Fortinet Fabric, which includes Forti Manager, Forti Switch, Forti Web, Forti Token Authentication and other Forti products, it provides management analytics, multi-cloud facility, web application support, advanced threat protection, unified access, open ecosystem and much more.



Fortinet FortiGate Architecture

IV. Comparison Of ASA And Fortigate

Starting with assessing the network size, the ASA firewall can be used in small office and branch office (ASA 5505-5508 series), Internet Edge (ASA 5512-5555 series), and Enterprise Data Center (ASA 5585-X). In comparison, Fortinet has wide variety of products for changing requirements of various organizations. Some of these products are next generation firewalls (D and E series ranging from 30E to 7060E), secure SD-WAN (FortiGate and FortiManager), Crypto VPN's (FortiGate 6300F – FortiGate 30E), Secure web gateways (FortiGate SWG 600E – 3700D, FortiProxy 400E – 4000E), and much more. These standalone products, when bundled together, form FortiGuard services bundle. This helps Fortinet to target different areas of the market and expand their business. Both Cisco ASA and Fortinet Fortigate have variety of solutions in their product inventory.

In order to protect the data, it is necessary to understand what is present inside a network. Since it is difficult to monitor the traffic of growing networks, both Cisco ASA and Fortinet Fortigate provide interactive UI's. The Management Console called Cisco Firepower Management Center provides the network administrator, a dashboard with information about network (operating system, mobile devices, endpoints, servers), application (application and user details, bandwidth utilization, URL visibility), geolocation, malware, intrusion and threat events, and file information. The console has several features but lacks simplicity. The Fortinet management console (called as FortiGuru dashboard) provides a dashboard with features like Network (IPV4 and IPV6 traffic), Config (to configure the NGFW regarding firewall whitelist for allowed connections, open ports, etc.), Admin (to manage all devices connected to the firewall), Monitor (to view traffic throughput, devices connected to the network, the OS they use and the amount of traffic they produce) and many other model specific features. This helps to update security policies and threat detection algorithm with an interactive UI, which in turn enables users to configure complex devices easily. This gives Fortinet a slight edge over Cisco based on features like ease of use and implementation.

The operational capabilities of Cisco's firewall are better than FortiGate because of the Cisco OptiFlow scanning architecture consisting of APIs such as eStreamer, remediation, host API which allows the firewall to be integrated with third-party security solutions and applications. Moreover, Cisco's firewall is a true Distributed Denial of Service (DDoS) because of the integration of Radware DefensePro vDoS container. In comparision, Fortinet FortiGate handles DDoS attacks in its own unique way by using black hole routing (dropping excess data-packets by routing it to the last node of the network). This reduces the requirement of external devices to handle such attacks and removes third party vendor dependency (no integration issues).

In terms of licensing models, with growing enterprise network, additional licenses need to be purchased (the traditional approach). This is followed by Cisco ASA which provides a wide variety of licensing models with a maximum of 160,000 connections per second to the network. In the case of Fortinet Fortigate, the licensing model once bought can be extended to add new connections to the network with more than 400,000 connections per second.

V. Conclusion

By combining stateful inspection and next-generation services, Cisco ASA provides the better solution for enterprises of varying sizes. But, given the requirement of performance and speed for a large enterprise, FortiGate outruns ASA series. Both Cisco ASA and Fortinet FortiGate provide similar features but differ in target audience. Fortinet can provide good service even with its individual products, but tends to bundle with other products to form Fortinet Fabric (combined implementation of all products provided by Fortinet) to provide better performance. Cisco, on the other hand, tends to produce stand alone components that perform optimally when deployed into a network, and can also be combined with other network products for improved efficiencies. Fortinet provides its products at a slightly lower price than what Cisco charges for its products. Fortinet is best suited for low budget network deployment.

Considering these pros and cons of Cisco and Fortinet, we can conclude that although Cisco is an established company in the firewall domain, Fortinet is not far behind. Hence it is a matter of requirement and user choice to select either of the service providers as both Cisco and Fortinet provide the benefits of securing the network.

References

[1]. Tam, K & Salvador, M.H.H. & McAlpine, K & Basile, R & Matsugu, B & More, J. (2012). UTM Security with Fortinet: Mastering FortiOS.

[2]. J. Frahim, O. Santos, A. Ossipov, Cisco ASA all-in-one next-generation firewall, IPS, and VPN services (Indianapolis: Cisco Press, 2014).

[3]. Rosato Fabbri and Fabrizio Volpe, Getting started with FortiGate, (Birmingham, UK: Packt Publishing, 2013).