SOLUTION BRIEF

Enable Deep Visibility for Applications, Users, and Devices with FortiGate Next-Generation Firewalls

Executive Summary

Traditional firewalls are typically only able to allow or block connections based on port and protocol. However, network access is now dynamic and contextual, operating under zero-trust principles. In addition, the modern enterprise is hybrid, spanning on-premises data centers, public clouds, corporate branches and campuses, as well as remote sites. Today's IT teams require deep visibility into applications, users, and devices to defend enterprise networks against cyberthreats across the entire environment, but this is often a challenge.

Compounding the visibility problem is that almost all internet traffic is now encrypted. Enterprises are finding large swathes of network blind spots as they shift from expensive hub-and-spoke architectures to distributed models with direct internet access at sites. Malicious actors can exploit these network gaps, hiding threats in encrypted traffic.

Over 95% of internet traffic is now encrypted.[1]

FortiGate Next-Generation Firewalls (NGFWs) deliver the visibility into encrypted traffic and user, application, and device activity necessary to build contextual, evolving network and security policies that secure digital transformation. FortiGate NGFWs can identify and control all users, applications, and devices on the network with advanced data collection and analysis techniques. As the key component of a hybrid mesh firewall (HMF) solution, FortiGate NGFWs integrate this visibility and protection across IT domains, covering the entire network infrastructure.

Application Control

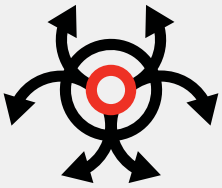
The FortiGuard Application Control Service attaches to FortiGate NGFWs and quickly identifies known and unknown applications traversing the network. It enables easy creation of policies to allow, deny, and restrict access to applications, certain functions within applications, and application categories.

#	Risk	Application	Category	Technology	Users	Bandwidth	Sessions
1	5	Asprox.Botnet	Botnet	Client-Server	1	1.74 MB	587
2	5	Proxy.HTTP	Proxy	Network-Protocol	11	7.10 MB	457
3	5	Onavo.Protect	Proxy	Client-Server	1	1.78 KB	9
4	5	Hotspot.Shield	Proxy	Client-Server	2	203.99 KB	8
5	5	Skyfire	Proxy	Client-Server	3	27.20 KB	3
6	4	Rsh	Remote.Access	Client-Server	67	9.82 GB	302,237
7	4	BitTorrent	P2P	Peer-to-Peer	8	1.79 MB	5,096
8	4	Telnet	Remote.Access	Client-Server	9	37.81 MB	681
9	4	RDP	Remote.Access	Client-Server	14	9.89 MB	48
10	4	TeamViewer	Remote.Access	Client-Server	22	1.13 MB	38

FortiGate NGFWs can identify applications not only by matching their port and protocol but also by the application signature, heuristic behaviors, and other identifying indicators. With a combined look at application signatures and internet service database (ISDB) applications, FortiGate can set over 4,200 application control rules. Below are some ways FortiGate identifies applications beyond Layers 3 and 4.

Application signatures: Allowed network traffic is assigned a signature based on transaction characteristics and whether the application port is default or nonstandard. Traffic is scanned for threats and deep analysis.

Encryption: If FortiGate detects encryption such as secure sockets layer (SSL)/transport layer security (TLS), Hypertext Transfer Protocol Secure (HTTPS), or secure shell (SSH), and a decryption policy rule is in place, the session is decrypted, and application signatures are applied again on the decrypted flow.



"...companies that inspected incoming traffic said that 70% of malware came in over an encrypted connection."[2]

Decoders: If the application protocol is known, it is then used to apply additional context-based signatures to detect other applications that may be tunneling inside of the protocol. Decoders validate that the traffic conforms to the protocol specification and provide support for network address translation (NAT) traversal and opening dynamic pinholes for applications such as session initiation protocol (SIP) and file transfer protocol (FTP).

Heuristics: FortiGate heuristic analysis uses behavioral analytics to determine the identity of evasive applications. This includes applications that use port 80, port 443, or engage in port hopping—for example, Voice over Internet Protocol (VoIP), collaboration, and peer-to-peer (P2P) applications that cannot be identified through advanced signature and protocol analysis.

If the FortiGate is unable to identify an application based on its signature, then it will rely on behavioral characteristics through heuristics, classifying the previously unknown application into an existing application group and applying dynamic filters or policy-based forwarding to achieve the desired result.

Identifying applications can provide meaningful context about the network. FortiGate can reveal information about the inherent function, application ports, protocol, technology, and behavioral characteristics of the application, which enables IT teams to make confident and informed access policies. Once the team understands how an application is being used on the network, a variety of policies and responses beyond allow and block can be applied.

FortiGuard Application Control also allows organizations to build policies and control functions within each application. Examples include:

- Allowing access to Facebook but blocking Facebook Messenger file transfers
- Letting users access Gmail but disabling Google Chat
- Blocking file uploads to Dropbox, Box, or Google Drive
- Filtering unwanted video categories from being viewed on YouTube

FortiOS, the FortiGate operating system, provides extensive visibility into application usage in real time, as well as trends over time through views, visualizations, and reports. Application control keeps malicious, risky, and unwanted applications out of the network through control points at the perimeter, in the data center, and internally between network segments.

User Identification

Identifying users beyond their IP addresses is another critical part of enterprise security. FortiOS can identify users based on a variety of sources and methods, such as Microsoft Active Directory (AD), LDAP servers, syslog, port mapping, and XFF headers.

FortiGate user identification provides better visibility into network activity and detection against malicious or damaging behavior. FortiGate user identification identifies users across operating systems in any location, providing improved visibility into application usage based on users. This gives IT teams a more relevant picture of network activity.

The power of user identification becomes evident when an unfamiliar application is found on the network. Whether using FortiView or application control logs, security teams can discern:

- The application
- The user
- Bandwidth and session consumption
- Source and destination of the application traffic
- Any associated threats

User mapping

FortiGate can create profiles of users on the network and match usernames to the IP addresses in received packets. User information can be mapped to security policies for safer network usage, reserving application access only for those who have a business need. User mapping can enable one set of rules or policies for less risky applications like Salesforce or PowerPoint while at the same time setting more stringent policies for sensitive applications like pen-testing tools or remote desktop controllers.

Group mapping

Defining policy rules based on user groups can simplify IT management, as policies and rules are already in place and do not need to be reconfigured when adding new users to groups. FortiGate can apply these rules and group updates, supporting a variety of directory servers, including Microsoft AD, Novell eDirectory, and Sun ONE Directory Server. After enabling user identification and leveraging group mapping, security policies can be configured for specific users and groups. These include application categories and subcategories, underlying technologies, and application characteristics. Policy rules can be defined to safely enable applications based on users and groups of users, in either outbound or inbound directions.

Examples of user-based and group-based policies include:

- Tools like: SSH, Telnet, and FTP on standard ports are restricted to corporate IT
- Policies like:
  - Allow sales to access Salesforce and Microsoft 365
  - Allow all users to watch YouTube but block specific video categories

User identification helps shape policies that support and protect employees, guests, and other stakeholders. FortiGate can provide deep user insight and automate policy controls.

Device identification

While user identification provides user-based policy, and application identification provides app-based policy, device identification provides policy rules that are based on a device, regardless of changes to its IP address or location. By providing traceability for devices and associating network events with specific devices, device ID delivers context for how events relate to devices. It writes policies that are associated with devices instead of users, locations, or IP addresses, which can change over time. Device ID is important for security, decryption, quality of service (QoS), and authentication policies.

With FortiGate, advanced device policies and prioritization can be categorized by:

- Class, such as secure networked devices
- Critical devices, such as servers and medical devices
- Environmental devices, like badge readers, cameras, and fire alarms
- Internet-of-Things (IoT) devices, like smartwatches and other connected “smart” devices

SSL/TLS 1.3 decryption

Given that malware is regularly hidden in encrypted traffic, it's critical that encrypted traffic is examined. FortiGate NGFWs deliver SSL/TLS 1.3 decryption with no network slowdowns. Further, FortiGates can decrypt specific kinds of traffic and make exclusions based on sites or categories. With Fortinet's high-performance proprietary security processing units, there is no need to choose between security and performance.

Centralized and unified management

Centralized and unified management is the most critical capability of an HMF. If separate domains, such as corporate sites, public and private clouds, and remote workers, require protection via separate dashboards, then IT complexity increases while visibility is greatly reduced.

Centralized management coordinates and unifies disparate security domains into a single enterprise IT security solution—simple, unified, and automated protection that extends from corporate sites to the cloud and remote workers. And because different organizations have different requirements for managing their dispersed network firewalls, all form factors of the centralized management must be supported, including appliances, VMs, SaaS, and managed firewall services.

Centralized management also delivers enormous value in bringing network operations center (NOC) and security operations center (SOC) teams together using a single pane of glass to manage, monitor, and secure the entire attack surface.

FortiGuard AI-Powered Security Services

With over 8 million sensors deployed around the world, FortiGate NGFWs are able to leverage the latest global threat intelligence through FortiGuard AI-Powered Security Services. With real-time, comprehensive security updates, FortiGate can protect the entire network with multilayered security defenses such as URL and DNS filtering, anti-malware and inline sandboxing, as well as hardware-accelerated IPS for high-performance virtual patching. These cybersecurity services protect the enterprise from both known and previously unknown attacks. Independent testing from CyberRatings.org[3] shows that FortiGate NGFWs are 99.88% effective against malicious exploits and evasions.

Conclusion

Identifying applications, users, and devices on the network is an important capability in managing and securing enterprise networks. FortiGate NGFWs are known for their advanced visibility and control over network traffic, as well as unparalleled performance. FortiGate defines and automates policies that ensure appropriate use, stop threats, and reduce the enterprise attack surface. Centralized and unified management integrates the FortiGate appliance with other security form factors, such as virtual firewalls, cloud-native firewalls, and Firewall-as-a-Service, to build a seamless HMF solution across the entire IT environment. The latest FortiGuard AI-Powered Security Services ensure up-to-date defenses from even the newest and most advanced attacks.

[1] "HTTPS encryption on the web," Google Transparency Report, Google, accessed May 15, 2023.

[2] Maria Korolov, "Network Encryption: A Double-edged Sword for Cybersecurity," Datacenter Knowledge, March 8, 2023.

[3] "Fortinet FortiGate 600F," Enterprise Firewall, CyberRatings.org, Q2 2023.

FORTINET

www.fortinet.com

June 7, 2023 3:30 PM
1711466-A-0-EN