FortiOS™ 6.4 is Fortinet’s most advanced security operating system, offering over 300 new features and capabilities. FortiOS also powers the Fortinet Security Fabric: a comprehensive, broad, integrated, and automated cybersecurity platform that addresses cybersecurity risks and effectively enables organizations to achieve their digital innovations outcomes without compromise. Every element of the Fortinet Security Fabric—from next-generation firewalls to access points and switches to NAC solutions—is driven by the same FortiOS™ code, which delivers a seamless experience under a single console. The Fortinet Security Fabric also integrates with an ecosystem of over 250 technology alliance partners.

Powered by FortiOS™ 6.4, the Fortinet Security Fabric delivers:

**Security-Driven Networking**
Secure and accelerate network and user experiences

**Zero-Trust Network Access**
Identify and secures users and devices, on-/off-network

**Dynamic Cloud Security**
Secure and control cloud infrastructures and applications with agility and automation

**AI-Driven Security Operations**
Automatically prevent, detect, and respond to cyber threats

---

**Highlights — What’s New**
- Consolidate IPv4 and IPv6 policy configuration
- Improved SD-WAN GUI and monitoring capabilities
- SD-WAN support on OCVPN
- SD-WAN zones
- ADVPN Hole Punching and monitoring
- Wireless spectrum analysis GUI Support
- IoT security service support
- Integration with Cloud-based IPAM service
- Matching multiple parameters on application control signatures
Overview

Introducing FortiOS™ 6.4

Digital Innovation

Digital innovation is a disruptive force that is transforming every single industry and allowing organizations to accelerate their businesses, reduce costs, improve efficiencies, and provide better customer experiences. However, this disruption also brings increased security risks as organizations cope with the expanding attack surface, advanced threats, increased ecosystem complexity, and an expanding regulatory compliance landscape. Organizations need to deploy a cybersecurity platform that delivers:

- **Broad** visibility of the entire digital attack surface to better manage risk
- **Integrated** solutions that reduce the complexity of supporting multiple point products
- **Automated** workflows to increase speed of operations and response

To address today’s risks and deliver the industry’s most comprehensive cybersecurity platform that enables digital innovation, Fortinet continues to enhance the Fortinet Security Fabric with the latest version of its operating system, FortiOS™ 6.4 with over 300 new features and capabilities.

The Fortinet Security Fabric is the result of almost 20 years of innovation, organically built from the ground up to be broad, integrated, and automated.

Fortinet’s security technologies have earned the most independent certifications for security effectiveness and performance in the industry. The Fortinet Security Fabric closes gaps left by legacy point products and platforms by providing the broad, powerful, and automated protection that today’s organizations require across their physical and virtual environments, from an endpoint to the cloud.
## Highlights

### FortiOS™ 6.4 Anatomy

<table>
<thead>
<tr>
<th>Feature</th>
<th>Highlights</th>
<th>Fortinet Advantage</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Configuration</strong></td>
<td>Policy Modes, Log &amp; Report, Diagnostics, Monitoring</td>
<td>Operation Integration, Central Mgmt. and Provisioning, Cloud &amp; SDN Integration</td>
</tr>
<tr>
<td><strong>Firewall</strong></td>
<td>Policy and Control</td>
<td>Systems Integration, Visibility, Automation</td>
</tr>
<tr>
<td><strong>VPN</strong></td>
<td>Security</td>
<td>Security Fabric</td>
</tr>
<tr>
<td><strong>SD WAN</strong></td>
<td>Security</td>
<td>Advanced Threat Protection (ATP)</td>
</tr>
<tr>
<td><strong>Routing/NAT</strong></td>
<td>Networking</td>
<td>Wireless Controller, Switch Controller, WAN Interface Manager</td>
</tr>
<tr>
<td><strong>Physical Appliance (+SPU)</strong></td>
<td>Platform Support</td>
<td>Cloud</td>
</tr>
</tbody>
</table>

**Note:** Feature availability may vary by model

### Security Fabric

<table>
<thead>
<tr>
<th>Feature</th>
<th>Highlights</th>
<th>Fortinet Advantage</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>System Integration</strong></td>
<td>Native integration with Fortinet products via quick setup GUI connectors, Standard-based data exchange APIs support with third-party solutions, Standard-based monitoring output – SNMP Netflow/ SFlow and Syslog support to external/third-party SIEM, SOAR and logging systems, Endpoint/Identity infrastructure integrations, External threat feeds integrations</td>
<td>Ability to reuse organization’s existing systems to lower TCO and streamline processes, Expand security and operational capabilities by seamlessly integrating with external solutions</td>
</tr>
<tr>
<td><strong>Central Management and provisioning</strong></td>
<td>Fortinet/third-party automation and portal services support via APIs and CLI scripts, Rapid deployment features including cloud-based provisioning solutions, Developer community platform access and professional service options for complex integrations, Extensive integration resources for Ansible and Terraform</td>
<td>Extensive APIs and CLI commands offering feature-rich service enhancements, Comprehensive rapid deployment options to save time and costs, Fortinet Developer Network (FNDN) empowers large service providers and enterprises with shared implementation/customization/integration knowledge</td>
</tr>
<tr>
<td><strong>Cloud and SDN Integration</strong></td>
<td>Multi-cloud support using Cloud and SDN connectors for AWS, Microsoft Azure, GCP, OCCI, AliCloud, VMware ESXi, NSX, OpenStack, Cisco ACI and Nuage Virtualized Service Platforms, Kubernetes connectors for private and public clouds</td>
<td>Robust and comprehensive SDN integration capabilities that allow organizations to implement cloud solutions securely without compromising agility</td>
</tr>
</tbody>
</table>
## Highlights

<table>
<thead>
<tr>
<th>Feature</th>
<th>Highlights</th>
<th>Fortinet Advantage</th>
</tr>
</thead>
</table>
| **Visibility**        | - Interactive drill-down and topology viewers that illustrate real-time and historical threat status and network usage with comprehensive contextual information  
                        - Aggregated data views provided by fabric devices                                                                                                                                            | - One-click remediation against listed sources/destinations that offers accurate and quick protection against threats and abuses  
                        - Unique threat score system, correlating weighted threats with particular users to prioritize investigations  
                        - Fabric-wide views expand visibility beyond a single security entity, allowing organizations to quickly spot problems and address them |
| **Automation**        | - Wizard-based automation workflow that performs appropriate actions based on triggers defined, across the Fortinet Security Fabric  
                        - Automatically quarantine compromised hosts using FortiClient via EMS or connections via FortiSwitch and FortiAP  
                        - NEW: Slack automation action                                                                                                               | - Reducing risk exposure and replacing manual security processes with automation to help address the organizational challenges of tighter budgets and a skilled staffing shortage |
| **NAC**               | - Interface with FortiAuthenticator and a wide variety of external identity management systems to facilitate user authentication processes  
                        - Wide-ranging single sign-on identity acquisition methods, including Windows AD, terminal servers, access portals, and mail services  
                        - Built-in token server to manage both physical and mobile tokens for use with various FortiOS authentication requirements such as VPN access and FortiGate administration  
                        - Endpoint enforcement using posture checking dynamic user groups based on tags                                                                                                               | - FortiOS integrates with a wide variety of AAA services to facilitate user admission control from various entry points, giving users a simplified experience while implementing greater security  
                        - Easily implement two-factor authentication for user and administrator access at little cost  
                        - Simplified mobile user security enforcement by easily distributing and updating clients’ security profiles that are consistent with gateway protection |
| **Compliance & Security Rating** | - Periodic system configuration checks on fabric devices using a pre-defined checklist to reveal security posture status updates; the data is kept to produce historical trending charts  
                        - Audit setups against PCI compliance requirements  
                        - Security rating ranking are benchmarked against peers                                                                                                                                        | - Automates compliance auditing, which frees up administration resources  
                        - Quickly verify the status and health of your setup and connected devices within the Fabric and identify any gaps that can potentially leave you at greater risk |
| **Advance Threat Protection (ATP)** | - Local file quarantine (for models with storage)  
                        - Anti-bot capabilities using IP reputation DB to terminate botnet communication to C&C servers  
                        - Receive dynamic remediation (malicious file checksum and URLs) DB updates and detail analysis reports from external Fortinet file analysis solutions (FortiSandbox)  
                        - Endpoint vulnerability views that present ranked vulnerable clients with details  
                        - IOC service integration displays IOC detection data from FortiAnalyzer onto FortiView and topology maps                                                                                   | - Supported by proven and industry-validated AV research services.  
                        - Ability to adopt a robust ATP framework that reaches mobile users and branch offices, detecting and preventing advanced attacks that may bypass traditional defenses by examining files from various vectors, including encrypted files  
                        - Easily identify vulnerable hosts across the fabric  
                        - Administrators can easily identify suspicious hosts and quickly or automatically quarantine them |
### Highlights

<table>
<thead>
<tr>
<th>Feature</th>
<th>Highlights</th>
<th>Fortinet Advantage</th>
</tr>
</thead>
</table>
| **Wireless Controller**  | - Integrated wireless controller for Fortinet’s wide range of AP form factors, including indoor, outdoor, and remote models, with no additional license or component fees  
- Enterprise-class wireless management functionality, including rogue AP protection, wireless security, monitoring, and reporting  
- Supports 802.3az WAVE2 APs  
- NEW: spectrum analysis GUI Support | - The wireless controller integrates into the FortiGate console providing a true single-pane-of-glass management for ease-of-use and lower TCO |
| **Switch Controller**    | - Integrated switch controller for Fortinet access switches with no additional license or component fees                                                                 | - Expands security to the access level to stop threats and protect terminals from one another          |
| **WAN Interface Manager** | - Supports LTE connectivity via integrated modem, USB port or the FortiExtender                                                                 | - Allows organizations to use or add 3G/4G connectivity for WAN connections while maintaining access control and defining the usage for those links |

### Operations

<table>
<thead>
<tr>
<th>Feature</th>
<th>Highlights</th>
<th>Fortinet Advantage</th>
</tr>
</thead>
</table>
| **Configuration** | - Wide variety of configuration tools — iOS app, Web UI and CLI  
- Ease of use with intuitive, state-of-the-art GUI and wizards  
- One-click access and actions between log viewers, dashboard widgets, policy tables, and more  
- Intelligent object panel for policy setups and edits | - Unique FortiExplorer configuration tool allows administrators to quickly access configurations, including via mobile phones and tablets  
- VPN wizards facilitate easy setup, including popular mobile clients and other vendors’ VPN gateways  
- Useful one-click access and actions bring administrators to the next steps quickly and accurately to swiftly mitigate threats or resolve problems |
| **Log & Reports** | - Detailed logs and out-of-the-box reports that are essential for compliance, audits, and diagnostic purposes  
- Real-time logging to FortiAnalyzer, FortiAnalyzer Cloud, and FortiGate Cloud  
- Common Event Format (CEF) support  
- Logging consolidation within Security Fabric | - Includes deep contextual information, including source device details and strong audit trail  
- GUI Report Editor offering highly customizable reports  
- Managing logs holistically simplifies configuration and guarantees that critical information from every FortiGate is centrally collected and available for analysis. This closes any gaps in intelligence |
| **Diagnostics** | - Diagnostic CLI commands, session tracer, and packet capture for troubleshooting hardware, system, and network issues  
- Hardware testing suite on CLI  
- Policy and routing GUI tracer | - Comprehensive diagnostic tools help organizations quickly remediate problems and investigate abnormal situations |
## Highlights

<table>
<thead>
<tr>
<th>Feature</th>
<th>Highlights</th>
<th>Fortinet Advantage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitoring</td>
<td>- Real-time monitors&lt;br&gt; - NOC Dashboard&lt;br&gt; - IOS push notification via FortiExplorer app</td>
<td>- Dashboard NOC view allows you to keep mission-critical information in view at all times. Interactive and drill-down widgets avoid dead-ends during your investigations, keeping analysis moving quickly and smoothly.</td>
</tr>
</tbody>
</table>

### Policy & Control

<table>
<thead>
<tr>
<th>Feature</th>
<th>Highlights</th>
<th>Fortinet Advantage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy Modes</td>
<td>- Easy-to-use policy management with unique Section or Global view options&lt;br&gt; - NGFW Policy-based and Policy-based modes&lt;br&gt; - <strong>IMPROVED</strong>: Consolidated IPv4 and IPv6 policies</td>
<td>- Flexible policy setup with various control systems assist organizations in implementing effective network security that is relevant to their networks.</td>
</tr>
<tr>
<td>Device Identification</td>
<td>- Identification of different types of devices present on the network&lt;br&gt; - MAC address policy source objects&lt;br&gt; - <strong>NEW</strong>: IoT security service allowing FortiGates to query FortiGuard servers for more information about a device</td>
<td>- Empowers organizations to add critical security to today’s BYOD environment by identifying personal devices.</td>
</tr>
<tr>
<td>SSL Inspection</td>
<td>- Effectively examine SSL-encrypted traffic with various security controls, such as AV and content filtering&lt;br&gt; - High-performance SSL inspection with content processors&lt;br&gt; - Reputable sites database for exemptions</td>
<td>- Identify and block threats hidden within encrypted traffic without significantly impacting performance.</td>
</tr>
</tbody>
</table>

### Network Security

<table>
<thead>
<tr>
<th>Feature</th>
<th>Highlights</th>
<th>Fortinet Advantage</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPN</td>
<td>- Comprehensive enterprise-class features for various types of VPN setups&lt;br&gt; - SSL and IPsec VPN wizards&lt;br&gt; - Cloud-assisted Overlay Controller VPN that supports, Full Mesh, Hub &amp; Spoke topology with ADVPN options</td>
<td>- The FortiGate’s unmatched performance for VPN allows organizations to establish secure communications and data privacy between multiple networks and hosts by leveraging custom security processors (SPUs) to accelerate encryption and decryption of network traffic.</td>
</tr>
</tbody>
</table>
### Highlights

<table>
<thead>
<tr>
<th>Feature</th>
<th>Highlights</th>
<th>Fortinet Advantage</th>
</tr>
</thead>
</table>
| IPS & DoS    | • Regular and rate-based signatures, supported by zero-day threat protection and research for effective, IPS implementation  
• Integrated DoS protection defends against abnormal traffic behaviors  
• CVE reference for IPS signatures                                                                                                                                 | • Proven quality protection with “NSS Recommended” award for superior coverage and cost/performance  
• Adapts to enterprise needs with full IPS features and NGIPS capabilities, such as contextual visibility  
• Supports various network deployment requirements, such as sniffer mode, and compatible with active-bypass FortiBridge or built-in bypass ports for a selected model |
| Web Filtering| • Enterprise-class URL filtering solution that includes quotas, user overrides, transparent safe search, and search engine keyword logging  
• Superior coverage with URL ratings of over 70 languages and identifies redirected (cached and translated) sites                                                                                                                                 | • Multi-layered anti-proxy avoidance capabilities with integrated application control and IPS allow organizations to implement air-tight web usage controls |
| Email Filtering | • Highly effective, multilayered spam filters with low false positives                                                                                                                                                                                                 | • Cost-efficient anti-spam solution for small organizations or branch offices without requiring investment in an additional system |
| Firewall     | • High-performance firewall within a SPU-powered appliance  
• Implement security policies that use a combination of source objects, IPs, users, and/or devices  
• Automatically or manually quarantine users/attackers  
• Directs registered FortiClient to host quarantines                                                                                                                                 | • Industry’s top firewall appliance with a superior cost-performance ratio |
| Application Control | • Detects and acts against traffic-based on applications while providing visibility on network usage  
• Fine-grained control on popular cloud applications, such as SalesForce, Google Docs, and Dropbox  
• **NEW:** Matching multiple parameters on application control signatures                                                                                                                                 | • Superior coverage, including both desktop and mobile applications, enabling better management of network access policies  
• Applies deeper application inspections for better control and visibility as more enterprises rely on public cloud services |
| Anti-Malware | • Flow- and proxy-based AV options for choices between protection and performance  
• Anti-bot capability using IP reputation DB to terminates botnet communication to C&C servers  
• Receive dynamic remediation (malicious file checksum and URLs) DB updates and detail analysis reports from external Fortinet file analysis solutions (FortiSandbox)  
• Virus Outbreak Protection as an additional layer of proactive protection targeted at new malware; comparing and detecting threats using a real-time FortiGuard checksum database  
• Content Disarm and Reconstruction (CDR) removes exploitable content before reaching users                                                                                                                                 | • Supported by proven and industry-validated AV research services  
• Ability to adopt robust ATP framework that reaches mobile users and branch offices, detecting and preventing advanced attacks that may bypass traditional defenses by examining files from various vectors, including encrypted files |
## Highlights

<table>
<thead>
<tr>
<th>Feature</th>
<th>Highlights</th>
<th>Fortinet Advantage</th>
</tr>
</thead>
</table>
| **SD-WAN**    | - Intelligent WAN path control with the ability to direct traffic among WAN links based on over 3,000 applications and users/user groups  
- Measure application transactions such as latency, jitter, and packet-loss plus built-in automatic fail-over to determine preferred paths and maintain the optimal application performance of business-critical applications  
- Use QoS, Traffic Shaping and policy routing for bandwidth management  
- Peer to peer and remote user WAN optimization and byte caching technologies  
- **IMPROVED:** SD-WAN GUI and monitoring capabilities                                                                                                                                                                                                                     | - Broad coverage of application visibility and first packet classification for efficient SD-WAN adoption  
- Integrated NGFW and SD-WAN on the same appliance further reduces TCO and complexity  
- WAN Path Controller automation continues to provide high application performance  
- Industry’s highest IPsec VPN performance  
- Zero Touch Deployment of SD-WAN Edge                                                                                                                                                                                                                                                                                      |
| **Explicit Proxy** | - Explicit HTTP and HTTPS, FTP over HTTP, or SOCKS proxying of IPv4 and IPv6 traffic on one or more interfaces  
- Transparent web proxy                                                                                                                                                                                                                                                                                                         | - Broad coverage of application visibility and first packet classification for efficient SD-WAN adoption  
- Integrated NGFW and SD-WAN on the same appliance further reduces TCO and complexity  
- WAN Path Controller automation continues to provide high application performance  
- Industry’s highest IPsec VPN performance  
- Zero Touch Deployment of SD-WAN Edge                                                                                                                                                                                                                                                                                      |
| **IPv6**      | - Comprehensive IPv6 support for routing, NAT, security policies, and more                                                                                                                                                                                                                                                                                                                              | - Operating mode options provide flexibility when deploying into existing or new networks, reducing network change requirements                                                                                                                                                                                                                                                                     |
| **High Availability** | - Support for industry-standard VRRP and various proprietary solutions, with ability to combine more than one high availability solution into a single configuration                                                                                                                                                                                                                                  | - Flexible high availability offerings allow organizations to pick the most suitable solutions based on their network environments and SLA requirements                                                                                                                                                                                                                      |
| **Routing/NAT** | - Comprehensive routing protocols and NAT support  
- Traffic redirection with ICAP and WCCP support                                                                                                                                                                                                                                                                                                                                                     | - Wide-ranging routing features that meet carrier and enterprise resilience networking requirements                                                                                                                                                                                                                                                                                                          |
| **L2/Switching** | - Ability to craft software switches or emulate VLAN switches from interfaces  
- Support SPAN ports and port aggregation with multiple interfaces.  
- Implement admission control modes on interfaces such as 802.1x or captive portal  
- Comprehensive WiFi and WAN interface configuration options  
- VXLAN and EMAC VLAN Support                                                                                                                                                                                                                                                                                          | - Flexible interface configurations offer various setup possibilities that best suit an organization’s network requirements while providing optional access security                                                                                                                                                                                                                       |
## Highlights

<table>
<thead>
<tr>
<th>Feature</th>
<th>Highlights</th>
<th>Fortinet Advantage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Offline Inspection</td>
<td>§ Sniffer mode allows threat and usage monitoring of network activities offline</td>
<td>§ Wide-ranging routing features that meet carrier and enterprise resilience networking requirements</td>
</tr>
<tr>
<td>Essential Network Services</td>
<td>§ A wealth of networking services such as DHCP, DNS server, NTP server and more</td>
<td>§ Built-in, out-of-the-box capabilities let organizations quickly provide necessary network services to internal terminals or to integrate with other network devices</td>
</tr>
</tbody>
</table>

## Platform Support

<table>
<thead>
<tr>
<th>Feature</th>
<th>Highlights</th>
<th>Fortinet Advantage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical Appliance (+SPU)</td>
<td>§ Integration with proprietary hardware architecture that includes acceleration components (SPU) and multicore processors</td>
<td>§ Superior software and hardware integration ensures the optimal use of hardware components, yielding the highest cost/ performance for customers</td>
</tr>
<tr>
<td>Virtual System</td>
<td>§ Virtual Domains (VDOMs): Virtualized FortiOS components to multiple logical systems on a single virtual or physical appliance. § Global security profiles § Support Virtual routing and forwarding (VRF) that allows multiple instances of a routing table to exist and work simultaneously § Support for Split-Task VDOM</td>
<td>§ Built-in, out-of-the-box capabilities let organizations quickly provide necessary network services to internal terminals or to integrate with other network devices</td>
</tr>
<tr>
<td>Hypervisor</td>
<td>§ Support for popular hypervisor platforms, including VMware vSphere, Citrix and open source Xen, KVM, and MS Hyper-V</td>
<td>§ Consistent management and features between physical and virtual appliances reduces management cost and simplifies deployments</td>
</tr>
<tr>
<td>Cloud</td>
<td>§ Support for public cloud services: Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP), Oracle Cloud Infrastructure (OCI) and AliCloud</td>
<td>§ Consistent management and features between on-premises and cloud platforms reduces management cost and simplifies deployments</td>
</tr>
</tbody>
</table>
## Specifications

### Security Fabric

**SYSTEM INTEGRATION**
- Security Fabric Logging:
  - Synchronized logging to FortiAnalyzer configurations among FortiGates
  - Data exchange and information such as topology and device asset tags with FortiAnalyzer
- Virtualization, Security Information and Event Management (SIEM), Systems Integration, Testing and Training, and Wireless markets

**AUTOMATION**
- Interactive and graphical visualizer for user, device, network, and security activities (FortiView):
  - A variety of GUI consoles that display current and historical status using different perspectives such as sources, destinations, applications, and threats etc.
  - Threat and VPN map
  - Data view options: table, bubble chart, or world map if applicable
- Statistics and system information about the connected fabric device
  - Accelerated session indication
  - WHOIS Lookup for Public IP addresses within FortiView and log tables

**VISIBILITY**
- Physical and logical topology viewers that illustrate:
  - location of hosts within the security fabric network
  - one-click access to quarantine, IP ban, or access detailed contextual information of hosts
  - connections between security fabric entities
  - SD-WAN related information such as link usage

**CENTRAL MANAGEMENT AND PROVISIONING**
- Central management support: FortiManager, FortiCloud hosted service, web service APIs
  - Rapid deployment: Install wizards, USB auto-install, local and remote script execution

**CLOUD AND SDN INTEGRATION**
- Integration via connectors with:
  - Public Cloud: AWS, MS Azure, GCP, O3, AllCloud and IBM Cloud
  - Private SDN: Kubernetes, VMware ESXi and NSX, OpenStack, Cisco ACI and Nuage Networks

**NETWORK ACCESS CONTROL (NAC)**
- Local user database and remote user authentication service support: LDAP, Radius and TACACS+, native FortiClient and FortiNAC user integration and two-factor authentication
  - SAML SSO support within a fabric network allows an administrator to move between Fabric devices without logging in again
  - PKI and certificates: X.509 certificates, SGCP support, Certificate Signing Request (CSR) creation, auto-renewal of certificates before expiry, OCSP support

**COMPLIANCE AND SECURITY RATING**
- Run a series of system configuration compliance check against PCI requirements
  - Security Fabric Rating: audit components within the fabric against best practices, provide results and recommendations, then allow users to easily apply remediations for some items

**ADVANCE THREAT PROTECTION (ATP)**
- Display list of vulnerable hosts and their vulnerabilities via telemetry with FortiAnalyzer
  - Display list of compromised hosts via information provided by FortiAnalyzer

---

**WIRELESS CONTROLLER**
- Supports integrated external captive portal, 802.1x, pre-shared keys
  - Multiple PSK for WPA Personal

**SWITCH CONTROLLER**
- Supports integrated external captive portal, 802.1x, pre-shared keys
  - Enables scalability and redundancy in a switch stack with VLAN pooling (Round-Robin/Hash Load balancing)

**WAN INTERFACE MANAGER**
- Support USB 3G/4G Wireless WAN modems and modem extender (FortiExtender)

**3G/4G modem settings:**
- Actions: assignment to VLAN and application of port specific settings
  - Device attributes conditions: MAC address, hardware vendor, device type, operating system
  - Port security policies:
    - 802.1x Port-based and MAC-based mode
  - Port mirroring
  - Port security policies:
    - 802.1x Port-based and MAC-based mode

**CAPWAP-like communication known as FortiLink**
- Switch Topologies:
  - Single/Stack of switch units
  - HA-mode FortiGate with single/Stack of switch units
  - HA-mode FortiGate with two-tier switch units (Optional: with access rings)
  - Dual-homed servers connected to a pair of switch units using an MCLAG
  - Standalone/HA-mode FortiGate unit with dual-homed FortiSwitch access
  - Multi-tiered MCLAG with HA-mode FortiGate units

**Switch port Features:**
- PoE settings
  - DHCP blocking and IGMP snooping
  - STP (status, BPDU, root guard)
  - LLDP, IGMP, sFlow and Dynamic ACP Inspection (DA)
  - Port mirroring

**External cloud-based or on-premise file analysis (CS sandbox) integration:**
- External cloud-based or on-premise file analysis (CS sandbox) integration:
  - File submission (with option to select types)
  - Receive file analysis reports
  - Receive dynamic signature updates from file analysis system (file checksum and malicious URL DB)

**Support for external block lists for domain names, web filtering URLs, IP addresses and malware hashes**

**SUPPORT FOR EXTERNAL BLOCK LISTS FOR DOMAIN NAMES, WEB FILTERING URLS, IP ADDRESSES AND MALWARE HASHES**
- Provides URL filtering capabilities for critical websites and domains
  - Categories include phishing, malicious, and suspicious domains
  - Customizable block list settings for specific regions or environments

**INTEGRATION VIA CONNECTORS WITH:**
- CAPWAP data channel security: DTLS and IPsec VPN option
- WiFi Security: Rogue AP suppression, wireless IDS, monitor and suppress phishing SSIDs
  - 802.1x Port-based and MAC-based mode
  - MAC authentication bypass

**Extended logging information in key areas to help WiFi troubleshooting:**
- Association, authentication, DHCP, and DNS

**WIRELESS SECURITY: Rogue AP suppression, wireless IDS, monitor and suppress phishing SSIDs**
- WiFi troubleshooting tools, spectrum analysis and location map

**Rapid deployment:**
- Install wizards, USB auto-install, local and remote script execution

**Wildfire**
- © 2014 Fortinet, Inc. All rights reserved. Fortinet Confidential.
Operations

**CONFIGURATION**
- Management access: HTTPS via web browser, SSH, telnet, console
- Management client on OS: platforms
- Ease-of-use by using USB connectivity
- Provides mobile notification (as part of automation feature)
- Feature store: log files, CLI component display
- GUI configuration:
- One-click access that quickly transfers administrators to next step panels
- Dynamic object selectors and predictive search queries
- GUI language support: English, Spanish, French, Portuguese, Japanese, Simplified Chinese, Traditional Chinese, Korean

**LOG & REPORT**
- Logging facilities support: Local memory & storage (if available), multiple syslog servers, multiple FortiAnalyze jobs, Telnet servers, FortiCloud hosted service
- Reliable syslog based on RFC 3164/FTP/POP3/SMTP
- Encrypted logging & log integrity with FortiAnalyzer
- Scheduled batch log uploading, real-time logging or queue locally until external system is available
- Detailed traffic logs: forwarded, forwarded sessions, local traffic, invalid packets
- Comprehensive event log: systems & network activity audits, routing & networking, VPN, user authentications, activity related events
- Detailed info logs: for systems & users activity audits
- IP and service port name resolution option

**DIAGNOSTICS**
- Diagnostics CLI commands, session tracer, and packet capture for troubleshooting hardware, system, and network issues
- Packet flow CLI tracer
- Hardware testing suite on CLI

**MONITORING**
- SNMP System Monitoring:
  - SNMP v1 and v2c support
  - SNMP v3 implementation includes support for queries, traps, authentication, and privacy
- IP traffic log traffic events and a full log disk or a detected virus
- Traffic Monitoring:
  - SNORT version 5
  - Netflow 5.0 and PFR, may be extended to managed FortiSwitches
  - Egress traffic monitoring, auto-summary, traffic log by specific port
- Dashboard: custom widgets and layout

**Policy and Control**

**POLICY MODES**
- Policy objects: predefined, custom and object grouping
- Address objects: subnet, IP, IP range, GeoIP (Geography), FQDN, Dynamic (based on received tags from external systems) and MAC address
- Internet Service DB: Dynamically updated DB that provides a list of popular applications with their vital information that can be used for policy setup, routing and link load-balancing configurations
- User notifications: customizable replacement message for block sites and attachments
- User quarantine:
  - Manually assigned with perpetual or customizable duration
  - Automatically when triggered by automation configuration

**DEVICE IDENTIFICATION**
- Device Identification: Cloud-based query DB service, device and OS fingerprinting, automatic classification, inventory management
- Device inventory for visibility
- Device L2 lookup resolution
- Switch controller: LLDP-MED Voice detection

**SSL INSPECTION**
- Impact SSL encrypted traffic option for IPS, application control, antivirus, web filtering, and DLP
- SSL: MDM Mirroring
- SSL: Inspection Method options: SSL certificate inspection or full SSL inspection
- SSL inspection exemption by site reputation DB, web categories, and/or policy addresses

**Security**

**ANTI-MALWARE**
- Botnet server IP blocking with global IP reputation database
- Virus protection check-block applications selected on non-default ports
- Protocol enforcement: set networking services to defined ports. A violation can be set to block
- Content download and Reconstruction option:
  - AV Engine removes all active content in real time before passing to user
  - Forward original file to sandbox for further analysis, quarantine or discarded
- AV Inspected protocols and file types:
  - Support for HTTP, FTP, IMAP, POP3, SMTP, MAPI, CIFS and SSH
  - Scan encrypted traffic with SSL inspection
  - (Password-protected) archive files
  - Grayware and mobile malware
- Option to treat Windows executables in email attachments as viruses
- File quarantine (local storage required) and infected host ban

**IPS AND DOS**
- IPS engine: 11,000+ up-to-date signatures, protocol anomaly detection, rate-based detection, custom signatures, manual, automatic pull or push signature update, threat encyclopedia integration
- IPS & DOS: IP-based protection (models) with high-powered signing engines for TCP SYN flood, TCP/UDP/SCTP port scan, ICMP sweep, TCP/UDP/SCTP/KMP session flooding (source/destination)
- IPS & DOS: filter mode

**APPLICATION CONTROL**
- Detects thousands of applications in 18 categories: Business, Cloud/IT, Collaboration, Email, Game, General Interest, Mobile, Network Service, P2P, Proxy, Remote Access, Social Media, Storage/Backup, Update, Video/Audio, VOA, Web Chat and Industrial
- Support for HTTP, HTTPS, FTP, IMAP, POP3, SMTP, MAPI, CIFS and SSH
- Support detection for traffic using HTTP/2 protocol and able to block QUIC protocol
- Multiple parameter support on some signatures
- Actions: block, reset, quarantine attackers IP with expiry time
- IPS Action: default, monitor, block, reset, or quarantine attackers IP with expiry time
- IPS engine: 11,000+ up-to-date signatures, protocol anomaly detection, rate-based detection, custom signatures, manual, automatic pull or push signature update, threat encyclopedia integration
- IPS & DOS: filter mode
- IPS quarantine (local storage required) and infected host ban
- Content download and Reconstruction option:
  - AV Engine removes all active content in real time before passing to user
  - Forward original file to sandbox for further analysis, quarantine or discarded
- AV Inspected protocols and file types:
  - Support for HTTP, FTP, IMAP, POP3, SMTP, MAPI, CIFS and SSH
  - Scan encrypted traffic with SSL inspection
  - (Password-protected) archive files
  - Grayware and mobile malware
- Option to treat Windows executables in email attachments as viruses
- File quarantine (local storage required) and infected host ban

**WEB FILTERING**
- Web filtering inspection mode support: Proxy-based, flow-based, and DNS
- Manually-defined web filtering based on URL, web content and MIE header
- Dynamic web filtering with cloud-based real-time categorization database:
  - Over 250 million URLs rated into 78 categories, in 70 languages
- Pre-configured category-based filter: "G", "PG-13", "R" and custom
- Safe Search enforcement: transparently inserts Safe Search parameter to queries. Supports Google, Yahoo!, Bing and Yandex, defines YouTube Education Filter
- Proxy avoidance prevention: Proxy site category blocking, rate URLs by domain & IP address, block redirects from cache & translation sites, proxy avoidance application blocking (application control), proxy behavior blocking (IPs)
- Artifacts: Google, CloudView, only
DATA SHEET | FortiOS™ 6.4

---

**IPsec VPN Configuration options:** Route-based or policy based

- Auto Discovery VPN (ADVPN): Dynamically establish direct tunnels (called shortcuts) between the spokes of a traditional Hub and Spoke architecture
- UDP hole punching for spokes behind NAT

**Other VPN support:** L2TP client (on selected models) and server mode, L2TP over IPSec, PPTP, GRE over IPEC

---

**EMAIL FILTERING**

Mail protocol support: (MAPS), POP3(S), and SMTP(S)

- Anti-Spam DB query: IP address check, URL check, and email checksum
- Local Spam Filtering: HELO DNS Lookup, return email DNS check, and Black/White list

---

**Networking**

**ROUTING / NAT**

- Static and policy routing
- Dynamic routing protocols: RIP v1 and v2, OSPF v2 and v3, ISIS, BGP4

**Content routing:** WILC and IA

- NAT configuration: Per policy based and central NAT Table
- NAT support: NAT44, NAT64, static NAT, dynamic NAT, PAT, Full Cone NAT, STUN

---

**IPsec VPN**

- Support for remote clients to securely access on-premises resources
- IPsec VPN Configuration options: Route-based or policy based
- Auto Discovery VPN (ADVPN): Dynamically establish direct tunnels (called shortcuts) between the spokes of a traditional Hub and Spoke architecture
- UDP hole punching for spokes behind NAT

**Other VPN support:** L2TP client (on selected models) and server mode, L2TP over IPSec, PPTP, GRE over IPEC

---

**SD WAN**

**WAN load balancing (weighted) algorithms:** by volume, sessions, source-destination IP, Source IP, and referrer

**WAN link checks for SLA:** Ping or HTTP probes

- Monitoring criteria including latency, jitter, and packet loss
- Configurable check interval, failure and fail-back thresholds
- Cloud-based SD-WAN bandwidth monitoring service

---

**Traffic shaping Policies:** Assigns traffic shaping profile according to matching policy based on source, destination, service, application, application category, and/or URL category

**DSCP support:**
- DSCP match in SD-WAN rules
- DSCP tagging of forwarded packets based on identified applications

**Traffic shaping Policies:** Assigns traffic shaping profile according to matching policy based on source, destination, service, application, application category, and/or URL category

**DSCP support:**
- DSCP match in SD-WAN rules
- DSCP tagging of forwarded packets based on identified applications

**Traffic shaping Policies:** Assigns traffic shaping profile according to matching policy based on source, destination, service, application, application category, and/or URL category

**Cloud-assisted One-Click VPN/VPN Overlay Controller:** easily configures

- hub-and-spoke VPN (with ADVPN option)
- Mesh VPN (with ADVPN option)
- SD-WAN configuration integration
- Support VPN client connection to hub

**Cloud-assisted One-Click VPN/VPN Overlay Controller:** easily configures

- hub-and-spoke VPN (with ADVPN option)
- Mesh VPN (with ADVPN option)
- SD-WAN configuration integration
- Support VPN client connection to hub

**Traffic shaping Policies:** Assigns traffic shaping profile according to matching policy based on source, destination, service, application, application category, and/or URL category

**DSCP support:**
- DSCP match in SD-WAN rules
- DSCP tagging of forwarded packets based on identified applications

**Traffic shaping Policies:** Assigns traffic shaping profile according to matching policy based on source, destination, service, application, application category, and/or URL category

**DSCP support:**
- DSCP match in SD-WAN rules
- DSCP tagging of forwarded packets based on identified applications

**Traffic shaping Policies:** Assigns traffic shaping profile according to matching policy based on source, destination, service, application, application category, and/or URL category

**DSCP support:**
- DSCP match in SD-WAN rules
- DSCP tagging of forwarded packets based on identified applications

**Traffic shaping Policies:** Assigns traffic shaping profile according to matching policy based on source, destination, service, application, application category, and/or URL category

---

**Additional features offered by proxy-based web filtering:**

- Filter Java Applet, Activex, and/or cookie
- Block HTTP Post
- Log search keywords
- Rate images by URL
- Block HTTP redirects by rating
- Exempt scanning encrypted connections on certain categories for privacy
- Web Browsing quotas by categories

---

**Virtual Wire Pair:**

- Option to implement wildcard VLANs setup

**Available on both transparent and NAT route Mode**

- Option to implement wildcard VLANs setup

**DSCP tagging of forwarded packets based on identified applications**

**Traffic shaping Policies:** Assigns traffic shaping profile according to matching policy based on source, destination, service, application, application category, and/or URL category

**DSCP support:**
- DSCP match in SD-WAN rules
- DSCP tagging of forwarded packets based on identified applications

**Traffic shaping Policies:** Assigns traffic shaping profile according to matching policy based on source, destination, service, application, application category, and/or URL category

**DSCP support:**
- DSCP match in SD-WAN rules
- DSCP tagging of forwarded packets based on identified applications

**Traffic shaping Policies:** Assigns traffic shaping profile according to matching policy based on source, destination, service, application, application category, and/or URL category

**DSCP support:**
- DSCP match in SD-WAN rules
- DSCP tagging of forwarded packets based on identified applications

**Traffic shaping Policies:** Assigns traffic shaping profile according to matching policy based on source, destination, service, application, application category, and/or URL category

**DSCP support:**
- DSCP match in SD-WAN rules
- DSCP tagging of forwarded packets based on identified applications

**Traffic shaping Policies:** Assigns traffic shaping profile according to matching policy based on source, destination, service, application, application category, and/or URL category

**DSCP support:**
- DSCP match in SD-WAN rules
- DSCP tagging of forwarded packets based on identified applications
Platform Support

VIRTUAL SYSTEMS

Virtual Systems (FortiOS Virtual Domains) divide a single FortiGate unit into two or more virtual instances of FortiOS that function separately and can be managed independently.

- Configurable virtual systems resource limiting and management such as maximum/guaranteed ‘active sessions’ and log disk quotas
- VDOM operating modes: NAT/Route or Transparent
- Split-Task VDOM: Separate VDOMs for management and data paths

HYPERSVISOR

Support for popular hypervisor platform, including VMware vSphere, Citrix and open source Xen, KVM, and MS hyper-V

CLOUD

- Amazon AWS: auto-scaling, native HA with ELB, crossing AZ HA, Guard Duty integration, IAM, topology and CVE integration
- Microsoft Azure: auto-scaling, native HA (Azure LS), Azure Security Center integration
- Azure Stack: Active-Passive HA
- Google Cloud Platform: auto-scaling, HA between zones
- Oracle Cloud Infrastructure: Native and para-virtualized modes, IAM integration
- Alibaba Cloud: auto-scaling, native HA

Others

- Web Application Firewall:
  - Signature based, URL constraints and HTTP method policy
  - Server load balancing: traffic can be distributed across multiple backend servers
  - Based on multiple methods including static (failover), round robin, weighted or based on round trip time, number of connections.
  - Supports HTTP, HTTPS, MAPS, POP3S, SMTPS, SSL or generic TCP/UDP or IP protocols.
  - Session persistence is supported based on the SSL session ID or based on an injected HTTP cookie.
  - Credential Stuffing Defense: scans user names and passwords in submission traffic to external URLs against the sensitive corporate network credentials stored in the corporate domain controller

- DLP message filter:
  - Protocol supported: HTTP-POST, SMTP-POP3, MAP MAP, NTTP
  - Actions: Log only, block, quarantine user/IP/Interface
  - Pre-defined filter: Credit card number, Social Security ID

- DLP file filter:
  - Protocols supported: HTTP-POST, HTTP=GET,SMTP-POP3, MAP MAP, NTTP, FTP
  - Filters options: size, file type, watermark, content, if encrypted

- DLP watermarking: Allows filter rules that pass through the FortiGate unit and contain a corporate identifier (a text string) and a sensitivity level (Critical, Private, and Warning) hidden in a watermark in a support Windows

- DLP fingerprinting: Generates a checksum fingerprint from intercepted files and compares it to those in the fingerprint database

- DLP archiving: Records full content in email, FTP, IM, NNTP, and web traffic

- Others:
  - Built-in DHCP, NTP, DNS server, and DNS proxy
  - FortiGuard NTP, DNS, and DNS service

- Physical Appliance (+SPU)

  Integrates with SPU components for traffic processing acceleration.