FortiOS Wireless LAN Controller

Highlights

Support for Wi-Fi6, Wi-Fi6E, and Wi-Fi7 FortiAPs

Scale from 1 to 10,000+ APs

Flexible deployment models for SD-Branch, Campus, Education, Healthcare, and Remote AP

Integrated security and management

Built in NAC services

PCI compliance capabilities for retail stores

Integrated guest access management with captive portal

BYOD device finger printing and control

Integrated WIDS and rogue AP management

Spectrum analysis

End to End Wireless LAN Security with Superior Performance

Today's organizations are facing numerous challenges from the campus to the branch as the network environment evolves with the rapid rise of IoT devices, demanding mobile and remote workforce, and evolving security threats. Fortinet's Secure Wireless LAN Controllers are integrated into FortiOS, a purpose-built network security operating system, which forms the foundation of the FortiGate Network Security Platform. This solution leads to security-driven networking for wireless LANs.

Wi Fi CERTIFIED

FortiOS Highlights

Security Fabric Integration

Fortinet's Security Fabric extends to our Secure Wireless solution providing coordinated security policies to the very edge of the wired/wireless network where there are the most vulnerabilities.

Superior Performance

The latest wireless standards, integrated security at the edge via FortiLink, client band steering, Application control services, and HW based CAPWAP acceleration all combine to deliver the highest level of performance and user experience.

End-to-End Wireless LAN Security

Integrated security services from the controller to the AP secures for the network, the clients, and the applications.

Key Features and Benefits

Scalable and Resilient

Highly scalable and centrally managed enterprise WLAN, with integrated radio resource management to reduce co-channel interference and provide consistent WLAN performance.

Integrated Security Features

Extends wired security features to WLAN, unifying both wired and wireless management into a single console, providing a "Single Pane of Glass" management interface to the network.

Layer-7 Application Visibility

Leverage market leading features with the power of SPU-based deep packet inspection technology to deliver granular application level visibility and control.

A Comprehensive Suite of Security, Wireless, and Networking Services

The need for secure wireless networks with intra-SSID privacy, robust third-party certified security and advanced networking capabilities, is now more important than ever. Delivering the industry's most comprehensive suite of security, wireless and networking services, the FortiOS enterprise-class Wireless LAN Controller is purpose-built to leverage hardware acceleration provided by custom Fortinet Security Processing Units (SPUs) while providing an easy to use enterprise wireless solution, in a single unified platform.

Feature Highlights

Unbeatable Flexibility to Meet all Deployment Needs

A wireless infrastructure must be flexible and scalable. By consolidating security and wireless network capabilities, Fortinet Secure Wireless LAN Controllers significantly reduce network complexity and ultimately TCO. Fortinet's no-VLANs™ approach reduces complex Layer-2 requirements, eliminating the need to propagate VLAN information across the network to simplify and accelerate large, scalable deployments. With a wide range of FortiGate models to choose from, no matter the size of your network, there's a FortiGate solution right for you.

Single Pane-of-Glass Management

Integrating wired and wireless security into a single pane-of-glass lowers operating costs and reduces IT staff workloads by eliminating the complexities of troubleshooting a multivendor network and the need for costly training and certification across multiple vendor products. In addition to reducing operating costs, a single pane of glass provides complete visibility of clients, access points, switches and, security services, ensuring consistent security and control policies are applied across the enterprise.

Sophisticated Application Control

Wireless bandwidth is a precious shared medium and it is critical that business applications receive priority on the wireless LAN. FortiOS Application Control is built-in to the Wireless LAN controller and uses deep Layer-7 inspection with over 4,000 application signatures to provide bandwidth guarantees and prioritization of critical applications. This industry-leading Application Control capability provides the fine-grained application control required to ensure the Wireless LAN is performing at its best and is being utilized for the intended applications.

Industry-Leading Security

FortiOS has its pedigree in Unified Threat Management and Fortinet holds more industry certifications than any other vendor, providing the best-in-class unified protection with an integrated set of security services. From antivirus, web content filtering, application control, network IPS, email filtering and DLP, the same security that is applied to the wired network can now be applied to the wireless LAN.

Advanced WIDS

The Wireless Intrusion Detection System (WIDS) profile with modern capabilities, enabling more comprehensive detection and reporting of diverse security threats and intrusion attempts. See the advanced WIDS options list and description here.

Automated Rogue AP Detection and Suppression

Rogue access points pose a serious network security threat by creating a leakage point where sensitive data such as credit card information can be siphoned off the network. For this reason, the PCI DSS and other data security standards often mandate proactive monitoring and suppression of rogue APs. The FortiGate Rogue AP on-wire detection engine uses various correlation techniques to determine if a Rogue AP is connected to the network. This automated process continuously monitors for unknown APs and automatically suppresses any found to be unauthorized.

Band Steering

Band steering makes more efficient use of your available wireless network by sending clients to the bands where they are most efficiently served. FortiOS allows the user to assign bands to clients based on their capabilities. Without band steering, a dual-band client could associate on whatever band they happen to choose, leading to overcrowding on one band or the other depending on device preferences. With band steering, you can direct some of this traffic to your band of choice. Another example of using band steering is to separate devices by their importance (or the importance of the types of traffic they will be passing on your network). You can leave all clients with low priority profiles on the 2.4 GHz channels (where bandwidth is not a concern) and move clients to the 5 GHz or 6GHz bands when possible to achieve higher data rates.

Automatic Radio Resource Provisioning

FortiOS DARRP (Distributed Automatic Radio Resource Provisioning) technology ensures the wireless infrastructure is always optimized to deliver maximum performance. Fortinet APs enabled with this advanced feature continuously monitor the RF environment for interference, noise, and signals from neighboring APs, enabling the FortiGate WLAN Controller to determine the optimal RF power levels for each AP on the network. When a new AP is provisioned, DARRP also ensures that it chooses the optimal channel, without administrator intervention.

Captive Portal

Browser-based authentication for guest users is also supported via SSL enabled captive portal. This built-in captive portal allows for HTML login page customization as well as guest account provisioning and management via an integrated guest management portal. FortiOS also supports the universal access method (UAM) for integrating with third-party external captive portal servers as well as two-factor authentication with the FortiToken One Time Password (OTP) solution.

NAC Services

Onboard NAC services allows for secure onboarding of devices. Rules can leverage EMS tags, or IoT device fingerprinting to ensure that regardless of the type or capability of the device, it's placed into the correct security posture at the time of connection.

FortiLink NAC Secure Onboarding

Securely onboard devices by leveraging EMS tags, user authentication information or specific device characteristics learned from fingerprinting. Device fingerprinting allows the collection of various attributes about a device connecting to the network. The collected attributes can fully or partially identify individual devices, including the client's OS, device type, and browser being used. This information can be used to create flexible NAC rules to allow for secure onboarding of IoT or OT devices.

Spectrum Analysis

Get detailed RF information to understand what interfering devices are in your area by using an existing AP radio for spectrum analysis. Several graphical depictions are available including Signal Inteferencce, Spectragram, and Interferer list.

Hardware Acceleration

Fortinet leverages custom ASIC based hardware acceleration to offload the processing of our wireless management and control protocol. FortiOS takes advantage of these custom hardware features to take the burden off the main onboard processor. This allows Fortinet appliances running FortiOS to scale the number of APs they manage without having a corresponding impact on FortiGate performance. Both wireless traffic and non-wireless firewall traffic benefits from this offload, allowing FortiOS to deliver superior performance at lower appliance price points.

Layer 3 (L3) Mobility

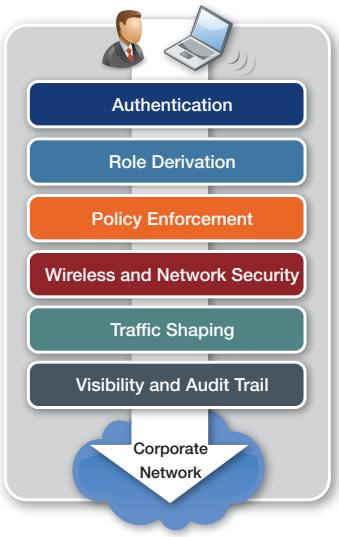
Roaming is an essential component of wireless networks, it allows the mobility and freedom for clients to move from AP to AP without the need to completely rebuild the connection every time. The IEEE standard has allowed mechanisms to allow for roaming within the same network, and accordingly FortiOS maintains a client database that includes important security connection context so that it can facilitate this roaming behavior throughout the network.

Occasionally a client may move not just from one AP to another, but from L3 domain to another (perhaps moving between floors or buildings on a campus). Historically this forced a client to reset network information such as IP address, resulting in a longer roam downtime and human noticeable service interruption for voice and video applications. FortiOS can allow for L3 roaming capabilities in which a client is allowed to roam and keep its original IP address, allowing the user to continue to experience seamless connectivity. FortiOS can support this capability regardless if the L3 roam happened across APs managed by the same FortiGate, or across APs managed by separate FortiGates.

Multi-Pre-Shared Key (MPSK)

It is often the case in Pre-Shared Key networks that IT has a need to assign sperate PSKs to different devices or groups of devices. This functionality (called MPSK) makes it easier for administrators to change keys for only a subset of devices without needing to change all devices. One of the classic use cases for MPSK is when headless IoT devices are in use which can often be difficult and/or time consuming to update a PSK on. FortiOS allows users to batch generate or import MPSK keys as well as dynamically assign VLANs based on used MPSK, and apply an MPSK schedule in the GUI.

Note that MPSK functionality is limited to use with WPA2. When possible it is recommended that users leverage WPA3 for it's enhanced security features. However when this is not a viable option, we recommend implementing additional security for IoT devices leveraging MPSK on WPA2 such as FortiLink NAC, while having all WPA3 capable devices running full WPA3 security.



Complete Secure Wireless LAN Architecture

- Captive Portal, 802.1x, Temporary Guest Access
- User and Device Identification, Authorization
- User and Device based policies, Application Control
- Rogue AP Mitigation, Wireless Intrusion Detection
- User and Application Based Wireless QOS
- Detailed Network and Threat Visibility, Compliance Reporting

Failover Options

Provides multiple options for configuring failover between FortiGates, tailored to different deployment scenarios.

FGCP

A legacy protocol that enables hitless HA failover with full configuration synchronization across FortiGate clusters.

Inter-controller HA

Not optimized for firewall functions, but designed to support distributed wireless deployments by providing backup resilience across different FortiGate models. Commonly recommended for wireless overlay deployments.

Enhanced Accesspoint AC discovery

Well-suited for wireless overlay deployments with configurations managed directly by access points. Supports seamless access point failover between master and slave FortiGates, along with flexible configuration options to adjust failover timers or to manage fallback behavior between FortiGates.

Specifications

WIRELESS CONTROLLER	
Networking	
Bonjour Gateway	Ability to monitor and control Apple's Bonjour Protocol
DHCP	Integrated DHCP server
VLANs	Interface and trunk
	SSID to VLAN mapping
	Dynamic VLAN Support
Routing	Static, dynamic and policy routing
	RIP, OSPF and BGP support
Multicast	PIM Mode
	Multicast to unicast conversion
Data Forwarding	Centralized – Tunneled to FortiGate, no VLANs
	Distributed – Bridged locally
	Split Policy Based – Selective forwarding based on resources, policy
Provisioning and Management	
Management Access	HTTPS via web browser
	SSH, Telnet and console
	SNMP (V1 and V2)
Management Availability	1+1 Support for High Availability (HA)
	Hitless failover in HA mode
Monitoring	Access Point (radio, channel) – Status, usage, utilization
	Client monitoring – Signal strength, SNR, username, IP, device type, firewall policy, bandwidth usage, application visibility
	Rogue AP
	Mesh connectivity hierarchy
	Wireless health monitoring, client trends, overloaded APs, excessive RF errors
	Location information available via API
Centralized Management	Single pane of glass management for wired, wireless and security configuration and monitoring
	Centralized management of thousands of locations via FortiManager
	Centralized reporting, network analytics and trends of thousands of locations via FortiAnalyzer
Troubleshooting	Remote wireless packet capture
Remote AP	
Remote AP (teleworker) Support	Supported on all FAP models
	Enables FAPs to be deployed remotely (over WAN link) to the FortiGate Wireless LAN Controller
	Options to encrypt data traffic
	Split routing – Selective forwarding based on policy
WAN Survivability	Wireless client connectivity is maintained when the wireless controller is unreachable for open and PSK type SSIDs
Troubleshooting	Local FAP diagnostic web portal
Mesh and Bridging	
Topology	Multi-hop mesh
	Support for multiple mesh instances
Mesh Hops	Configurable maximum hop count
Bridging	Point-to-Point bridging
	Point-to-Multipoint bridging for wireless ISP applications
Management	Via FortiGate web interface

WIRELESS CONTROLLER	
Wireless Access and Authentication	
Access – Authentication Methods	IEEE 802.1x (EAP, Cisco-LEAP, PEAP, EAP-TLS, EAP-TTLS, EAP-SIM, EAP-AKA, EAP-TTLS/MSCHAPv2, PEAPv0/EAP-MSCHAPv2, PEAPv1/EAP-GTC, EAP-FAST, EAP-TTLS/PAP)
	RFC 2716 PPP EAP-TLS
	RFC 2865 RADIUS authentication
	RFC 3579 RADIUS support for EAP
	RFC 3580 IEEE 802.1x RADIUS Guidelines
	RFC 3748 Extensible Authentication Protocol
	WEP64 – 64-bit Web Equivalent Privacy
	WEP128 – 128-bit WEP
	WPA (Wi-Fi Protected Access) Personal and Enterprise, including support for Multiple PreShared Keys (M-PSKs)
	WPA3 (Personal and Enterprise) including support for Multiple PreShared Keys (M-PSKs)
	MAC address authentication
	MAC address authentication via RADIUS
	Certificate based authentication for BYOD
Authentication Servers	Internal Database, RADIUS, LDAP, TACACS+, Radsec
	External Authentication Servers – Microsoft Active Directory, Microsoft IAS RADIUS server, Cisco ACS Server, FreeRADIUS , Interlink RADIUS server, Steel Belted Radius
Encryption Protocols	CCMP/AES
	TKIP
	TKIP+AES
	DTLS
	L2TP/IPSec (RFC 3193)
	XAUTH/IPSec
VPN	Support for VPN endpoint and encryption
Captive Portal	Authentication against internal or external authentication server
	Fully customizable look and feel including branding, graphics and language
	Disclaimer page
	Multiple-captive portal pages
	Forward to external captive portal
	Redirect to website after authentication
Guest User Management	Integrated receptionist guest user management portal
	Configurable expiration time
	Configurable start times
	Bulk account creation
	Integration with FortiAuthenticator for self-service captive portal with e-mail login

Specifications

WIRELESS CONTROLLER	
RF and Performance Management	
DAARP (Distributed Automatic Radio Resource Provisioning) DAARP Scheduling	Automated selection of RF channel to achieve consistent optimal performance
	Configurable (enable/disable)
	Enable Multi-profile with the option to exclude time slots
Band Steering	Intelligently balances stations across radios, steering stations to bands for optimal performance and reducing interference
AP Load Balancing	Distribute clients evenly across APs on available channels
Self Healing	Automatically adjust TX power levels to extend coverage to compensate failed APs
Spectrum Analysis	Get insight into the interferers in the environment
Rogue AP Management	
Background Scanning	Background and full-time scanning for rogue APs
On-Wire Correlation	On-Wire correlation to identify malicious APs that are connected to the local network
Rogue Suppression	Configurable options for automatic and/or manual suppression options
	Over-the-air suppression of offending APs and counter measures to prevent clients attempting to connect to an identified rogue AP
Wireless IDS	Detects and logs multiple RF intrusion methods
Event Logging	Syslog of all Rogue AP events
Auditing	Pre-built reported for PCI-DSS compliance generated via FortiAnalyzer
BYOD and Mobility	
Device Identity	Distinguish between corporate assets and employee owned devices
	Identify and classify device types, vendor information, OS types and OS versions
Application Visibility	Layer-7 application detection with support for over 3,000 signatures
	Ability to detect, prioritize or suppress applications
Quality of Service	End-to-end QoS
	Policy based retagging of applications
	Preserve QoS tags across the wired and wireless network
	Prioritize transmission of business critical applications over wireless
Policy Management	Manage and enforce firewall and traffic shaping policies based on device and user identity
Roaming	Layer 3 roaming capable
	802.11i fast-roam back
	802.11i fast-associate in advance
	PMK caching
Presence Detection	Presence detection for presence analytics

WIRELESS CONTROLLER	
IPv6 Support	
Client Support	Support for IPv6 clients
Accesspoint Management	Management over IPv6 — Support for FortiGate to act as IPv6 node
Traffic	Routing protocols, firewall and UTM support
Firewall	ICSA firewall enterprise certification
	ICSA IPv6 certified firewall
	USGv6 certified firewall
Industry Standards	
Wi-Fi Alliance	WPA™ Personal, WPA™ Enterprise, WPA2™ Personal, WPA2™ Enterprise, WPA3™-Enterprise, WPA3™-Personal, WMM™, WMM™ Power Save, Wi-Fi Agile Multiband™, Wi-Fi CERTIFIED 6E™, Wi-Fi CERTIFIED 6™, Wi-Fi CERTIFIED 7, Wi-Fi CERTIFIED™ ac, Wi-Fi CERTIFIED™ a/b/g/n, Wi-Fi Enhanced Open™, Passpoint
IEEE Standard Compliance	802.11a, 802.11b, 802.11d, 802.11be, 802.11e, 802.11g, 802.11h, 802.11i, 802.11j, 802.11k, 802.11n, 802.11r, 802.11v, 802.11ac, 802.11ax, 802.11mc, 802.1X, 802.3ad, 802.3at, 802.3bt, 802.3az, 802.1Q, 802.11u, 802.11w, 802.3bz
Additional RF Technologies	
	Bluetooth beacon enabled
	Supports BLE based third party RTLS solutions
	Electronic Shelf Label (ESL) system support for Hanshow and SES-IMagotag

Specifications

Additional RFCs	
BGP	
RFC 7911	Advertisement of Multiple Paths in BGP
RFC 4724	Graceful Restart Mechanism for BGP
RFC 4456	BGP Route Reflection: An Alternative to Full Mesh Internal BGP (IBGP)
RFC 4360	BGP Extended Communities Attribute
RFC 4271	A Border Gateway Protocol 4 (BGP-4)
RFC 2918	Route Refresh Capability for BGP-4
RFC 2545	Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing
RFC 2439	BGP Route Flap Damping
RFC 1997	BGP Communities Attribute
RFC 1930	Guidelines for creation, selection, and registration of an Autonomous System (AS)
RFC 1772	Application of the Border Gateway Protocol in the Internet

Additional RFCs	
DHCP	
RFC 4361	Node-specific Client Identifiers for Dynamic Host Configuration Protocol Version Four (DHCPv4)
RFC 3736	Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6
RFC 3633	IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6
RFC 3456	Dynamic Host Configuration Protocol (DHCPv4) Configuration of IPsec Tunnel Mode
RFC 3315	Dynamic Host Configuration Protocol for IPv6 (DHCPv6)
RFC 2132	DHCP Options and BOOTP Vendor Extensions
RFC 2131	Dynamic Host Configuration Protocol
Diffserv	
RFC 3260	New Terminology and Clarifications for Diffserv
RFC 2597	Assured Forwarding PHB Group
RFC 2475	An Architecture for Differentiated Services
RFC 2474	Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers

Additional RFCs	
Cryptography	
RFC 6954	Using the Elliptic Curve Cryptography (ECC) Brainpool Curves for the Internet Key Exchange Protocol Version 2 (IKEv2)
RFC 8031	Curve25519 and Curve448 for the Internet Key Exchange Protocol Version 2 (IKEv2) Key Agreement
RFC 7634	ChaCha20, Poly1305, and Their Use in the Internet Key Exchange Protocol (IKE) and IPsec
RFC 7627	Transport Layer Security (TLS) Session Hash and Extended Master Secret Extension
RFC 7539	ChaCha20 and Poly1305 for IETF Protocols
RFC 7427	Signature Authentication in the Internet Key Exchange Version 2 (IKEv2)
RFC 7383	Internet Key Exchange Protocol Version 2 (IKEv2) Message Fragmentation
RFC 7296	Internet Key Exchange Protocol Version 2 (IKEv2)
RFC 7027	Elliptic Curve Cryptography (ECC) Brainpool Curves for Transport Layer Security (TLS)
RFC 6989	Additional Diffie-Hellman Tests for the Internet Key Exchange Protocol Version 2 (IKEv2)
RFC 6290	A Quick Crash Detection Method for the Internet Key Exchange Protocol (IKE)
RFC 6023	A Childless Initiation of the Internet Key Exchange Version 2 (IKEv2) Security Association (SA)
RFC 5723	Internet Key Exchange Protocol Version 2 (IKEv2) Session Resumption
RFC 5282	Using Authenticated Encryption Algorithms with the Encrypted Payload of the Internet Key Exchange version 2 (IKEv2) Protocol
RFC 5280	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
RFC 4754	IKE and IKEv2 Authentication Using the Elliptic Curve Digital Signature Algorithm (ECDSA)
RFC 4635	HMAC SHA TSIG Algorithm Identifiers
RFC 4492	Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS)
RFC 4478	Repeated Authentication in Internet Key Exchange (IKEv2) Protocol
RFC 4106	The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP)
RFC 3947	Negotiation of NAT-Traversal in the IKE
RFC 3602	The AES-CBC Cipher Algorithm and Its Use with IPsec
RFC 3526	More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE)
RFC 2986	PKCS #10: Certification Request Syntax Specification Version 1.7
RFC 2845	Secret Key Transaction Authentication for DNS (TSIG)
RFC 2631	Diffie-Hellman Key Agreement Method
RFC 2451	The ESP CBC-Mode Cipher Algorithms
RFC 2410	The NULL Encryption Algorithm and Its Use With IPsec
RFC 2405	The ESP DES-CBC Cipher Algorithm With Explicit IV
RFC 2404	The Use of HMAC-SHA-1-96 within ESP and AH
RFC 2403	The Use of HMAC-MD5-96 within ESP and AH
RFC 2315	PKCS #7: Cryptographic Message Syntax Version 1.5
RFC 2104	HMAC: Keyed-Hashing for Message Authentication
RFC 2085	HMAC-MD5 IP Authentication with Replay Prevention
RFC 1422	Privacy Enhancement for Internet Electronic Mail: Part II: Certificate-Based Key Management
RFC 1321	The MD5 Message-Digest Algorithm
PKCS #12	PKCS 12 v1: Personal Information Exchange Syntax

Specifications

Additional RFCs	
DNS	
RFC 6895	Domain Name System (DNS) IANA Considerations
RFC 6604	xNAME RCODE and Status Bits Clarification
RFC 6147	DNS64: DNS Extensions for Network Address Translation from IPv6 Clients to IPv4 Servers
RFC 4592	The Role of Wildcards in the Domain Name System
RFC 4035	Protocol Modifications for the DNS Security Extensions
RFC 4034	Resource Records for the DNS Security Extensions
RFC 4033	DNS Security Introduction and Requirements
RFC 3597	Handling of Unknown DNS Resource Record (RR) Types
RFC 3226	DNSSEC and IPv6 A6 aware server/resolver message size requirements
RFC 3007	Secure Domain Name System (DNS) Dynamic Update
RFC 2308	Negative Caching of DNS Queries (DNS NCACHE)
RFC 2181	Clarifications to the DNS Specification
RFC 2136	Dynamic Updates in the Domain Name System (DNS UPDATE)
RFC 1996	A Mechanism for Prompt Notification of Zone Changes (DNS NOTIFY)
RFC 1995	Incremental Zone Transfer in DNS
RFC 1982	Serial Number Arithmetic
RFC 1876	A Means for Expressing Location Information in the Domain Name System
RFC 1706	DNS NSAP Resource Records
RFC 1183	New DNS RR Definitions
RFC 1101	DNS Encoding of Network Names and Other Types
RFC 1035	Domain Names - Implementation and Specification
RFC 1034	Domain Names - Concepts and Facilities
ICMP	
RFC 6918	Formally Deprecating Some ICMPv4 Message Types
RFC 6633	Deprecation of ICMP Source Quench Messages
RFC 4884	Extended ICMP to Support Multi-Part Messages
RFC 4443	Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification
RFC 1191	Path MTU Discovery
RFC 792	Internet Control Message Protocol IP
RFC 5798	Virtual Router Redundancy Protocol (VRRP) Version 3 for IPv4 and IPv6
RFC 4301	Security Architecture for the Internet Protocol
RFC 3272	Overview and Principles of Internet Traffic Engineering
RFC 3168	The Addition of Explicit Congestion Notification (ECN) to IP
RFC 2072	Router Renumbering Guide
RFC 2071	Network Renumbering Overview: Why would I want it and what is it anyway?
RFC 1918	Address Allocation for Private Internets
RFC 1123	Requirements for Internet Hosts -- Application and Support
RFC 1122	Requirements for Internet Hosts -- Communication Layers
RFC 791	Internet Protocol
IP Multicast	
RFC 4604	Using Internet Group Management Protocol Version 3 (IGMPv3 and Multicast Listener Discovery Protocol Version 2 (MLDv2) for Source-Specific Multicast
RFC 3973	Protocol Independent Multicast - Dense Mode (PIM-DM): Protocol Specification (Revised)
RFC 3956	Embedding the Rendezvous Point (RP) Address in an IPv6 Multicast Address
RFC 3306	Unicast-Prefix-based IPv6 Multicast Addresses
RFC 2365	Administratively Scoped IP Multicast
RFC 1112	Host Extensions for IP Multicasting
IPSec	
RFC 4304	Extended Sequence Number (ESN) Addendum to IPsec Domain of Interpretation (DOI) for Internet Security Association and Key Management Protocol (ISAKMP)
RFC 4303	IP Encapsulating Security Payload (ESP)
RFC 3706	A Traffic-Based Method of Detecting Dead Internet Key Exchange (IKE) Peers

Additional RFCs	
IPv4	
RFC 6864	Updated Specification of the IPv4 ID Field
RFC 5177	Network Mobility (NEMO) Extensions for Mobile IPv4
RFC 4632	Classless Inter-domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan
RFC 3927	Dynamic Configuration of IPv4 Link-Local Addresses
RFC 3021	Using 31-Bit Prefixes on IPv4 Point-to-Point Links
RFC 1812	Requirements for IP Version 4 Routers
IPv6	
RFC 6343	Advisory Guidelines for 6to4 Deployment
RFC 5175	IPv6 Router Advertisement Flags Option
RFC 5095	Deprecation of Type 0 Routing Headers in IPv6
RFC 4941	Privacy Extensions for Stateless Address Autoconfiguration in IPv6
RFC 4862	IPv6 Stateless Address Autoconfiguration
RFC 4861	Neighbor Discovery for IP version 6 (IPv6)
RFC 4193	Unique Local IPv6 Unicast Addresses
RFC 4007	IPv6 Scoped Address Architecture
RFC 3971	SEcure Neighbor Discovery (SEND)
RFC 3596	DNS Extensions to Support IP Version 6
RFC 3587	IPv6 Global Unicast Address Format
RFC 3493	Basic Socket Interface Extensions for IPv6
RFC 3056	Connection of IPv6 Domains via IPv4 Clouds
RFC 3053	IPv6 Tunnel Broker
RFC 2894	Router Renumbering for IPv6
RFC 2675	IPv6 Jumbograms
RFC 2464	Transmission of IPv6 Packets over Ethernet Networks
RFC 2185	Routing Aspects Of IPv6 Transition
RFC 1752	The Recommendation for the IP Next Generation Protocol IS-IS
RFC 5310	IS-IS Generic Cryptographic Authentication
RFC 5308	Routing IPv6 with IS-IS
RFC 3359	Reserved Type, Length and Value (TLV) Codepoints in Intermediate System to Intermediate System
RFC 1195	Use of OSI IS-IS for Routing in TCP/IP and Dual Environments
LDAP	
RFC 4513	Lightweight Directory Access Protocol (LDAP): Authentication Methods and Security Mechanisms
RFC 4512	Lightweight Directory Access Protocol (LDAP): Directory Information Models
RFC 4511	Lightweight Directory Access Protocol (LDAP): The Protocol
RFC 3494	Lightweight Directory Access Protocol version 2 (LDAPv2) to Historic Status
NAT	
RFC 7857	Updates to Network Address Translation (NAT) Behavioral Requirements
RFC 6888	Common Requirements for Carrier-Grade NATs (CGNs)
RFC 6146	Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers
RFC 5508	NAT Behavioral Requirements for ICMP
RFC 5382	NAT Behavioral Requirements for TCP
RFC 4966	Reasons to Move the Network Address Translator - Protocol Translator (NAT-PT) to Historic Status
RFC 4787	Network Address Translation (NAT) Behavioral Requirements for Unicast UDP
RFC 4380	Teredo: Tunneling IPv6 over UDP through Network Address Translations (NATs)
RFC 3948	UDP Encapsulation of IPsec ESP Packets
RFC 3022	Traditional IP Network Address Translator (Traditional NAT)

Specifications

Additional RFCs	
OSPF	
RFC 6860	Hiding Transit-Only Networks in OSPF
RFC 6845	OSPF Hybrid Broadcast and Point-to-Multipoint Interface Type
RFC 5340	OSPF for IPv6
RFC 4812	OSPF Restart Signaling
RFC 4811	OSPF Out-of-Band Link State Database (LSDB) Resynchronization
RFC 4203	OSPF Extensions in Support of Generalized Multi-Protocol Label Switching (GMPLS)
RFC 3630	Traffic Engineering (TE) Extensions to OSPF Version 2
RFC 3623	Graceful OSPF Restart
RFC 3509	Alternative Implementations of OSPF Area Border Routers
RFC 3101	The OSPF Not-So-Stubby Area (NSSA) Option
RFC 2328	OSPF Version 2
RFC 1765	OSPF Database Overflow
RFC 1370	Applicability Statement for OSPF
PPP	
RFC 2516	A Method for Transmitting PPP Over Ethernet (PPPoE)
RFC 2364	PPP Over AAL5
RFC 1661	The Point-to-Point Protocol (PPP)
RADIUS	
RFC 5176	Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)
RFC 2866	RADIUS Accounting
RFC 2548	Microsoft Vendor-specific RADIUS Attributes
RIP	
RFC 4822	RIPv2 Cryptographic Authentication
RFC 2453	RIP Version 2
RFC 2080	RIPng for IPv6
RFC 1724	RIP Version 2 MIB Extension
RFC 1058	Routing Information Protocol
SIP	
RFC 3960	Early Media and Ringing Tone Generation in the Session Initiation Protocol (SIP)
RFC 3325	Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks
RFC 3262	Reliability of Provisional Responses in the Session Initiation Protocol (SIP)
RFC 3261	SIP: Session Initiation Protocol
SNMP	
RFC 4293	Management Information Base for the Internet Protocol (IP)
RFC 4273	Definitions of Managed Objects for BGP-4
RFC 4113	Management Information Base for the User Datagram Protocol (UDP)
RFC 4022	Management Information Base for the Transmission Control Protocol (TCP)
RFC 3635	Definitions of Managed Objects for the Ethernet-like Interface Types
RFC 3417	Transport Mappings for the Simple Network Management Protocol (SNMP)
RFC 3416	Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)
RFC 3414	User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)
RFC 3413	Simple Network Management Protocol (SNMP) Applications
RFC 3412	Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)
RFC 3411	An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks
RFC 3410	Introduction and Applicability Statements for Internet Standard Management Framework
RFC 2863	The Interfaces Group MIB
RFC 2578	Structure of Management Information Version 2 (SMIv2)

Additional RFCs	
SNMP	
RFC 1238	CLNS MIB for use with Connectionless Network Protocol (ISO 8473) and End System to Intermediate System (ISO 9542)
RFC 1215	A Convention for Defining Traps for use with the SNMP
RFC 1213	Management Information Base for Network Management of TCP/IP-based internets: MIB-II
RFC 1212	Concise MIB Definitions
RFC 1157	A Simple Network Management Protocol (SNMP)
RFC 1156	Management Information Base for Network Management of TCP/IP-based internets
RFC 1155	Structure and Identification of Management Information for TCP/IP-based Internets SSH
RFC 4254	The Secure Shell (SSH) Connection Protocol
RFC 4253	The Secure Shell (SSH) Transport Layer Protocol
RFC 4252	The Secure Shell (SSH) Authentication Protocol
RFC 4251	The Secure Shell (SSH) Protocol Architecture
RFC 4250	The Secure Shell (SSH) Protocol Assigned Numbers SSL
RFC 6176	Prohibiting Secure Sockets Layer (SSL) Version 2.0
RFC 6101	The Secure Sockets Layer (SSL) Protocol Version 3.0 TCP
RFC 6691	TCP Options and Maximum Segment Size (MSS)
RFC 6298	Computing TCP's Retransmission Timer
RFC 6093	On the Implementation of the TCP Urgent Mechanism
RFC 793	Transmission Control Protocol
TLS	
RFC 8446	The Transport Layer Security (TLS) Protocol Version 1.3
RFC 7858	Specification for DNS over Transport Layer Security (TLS)
RFC 6347	Datagram Transport Layer Security Version 1.2
RFC 6066	Transport Layer Security (TLS) Extensions: Extension Definitions
RFC 5746	Transport Layer Security (TLS) Renegotiation Indication Extension
RFC 5425	Transport Layer Security (TLS) Transport Mapping for Syslog
RFC 5246	The Transport Layer Security (TLS) Protocol Version 1.2
RFC 4681	TLS User Mapping Extension
RFC 4680	TLS Handshake Message for Supplemental Data VPN
RFC 4761	Virtual Private LAN Service (VPLS) Using BGP for Auto-Discovery and Signaling
RFC 4684	Constrained Route Distribution for Border Gateway Protocol/MultiProtocol Label Switching (BGP/MPLS) Internet Protocol (IP) Virtual Private Networks (VPNs)
RFC 4577	SPF as the Provider/Customer Edge Protocol for BGP/MPLS IP Virtual Private Networks (VPNs)
RFC 4364	BGP/MPLS IP Virtual Private Networks (VPNs)
RFC 3715	IPsec-Network Address Translation (NAT) Compatibility Requirements Wireless
RFC 5415	Control and Provisioning of Wireless Access Points (CAPWAP)
RFC 5416	Control and Provisioning of Wireless Access Points (CAPWAP) Protocol Binding for IEEE 802.11
RFC 5417	CAPWAP Access Controller DHCP Option
RFC 8110	Opportunistic Wireless Encryption (OWE)

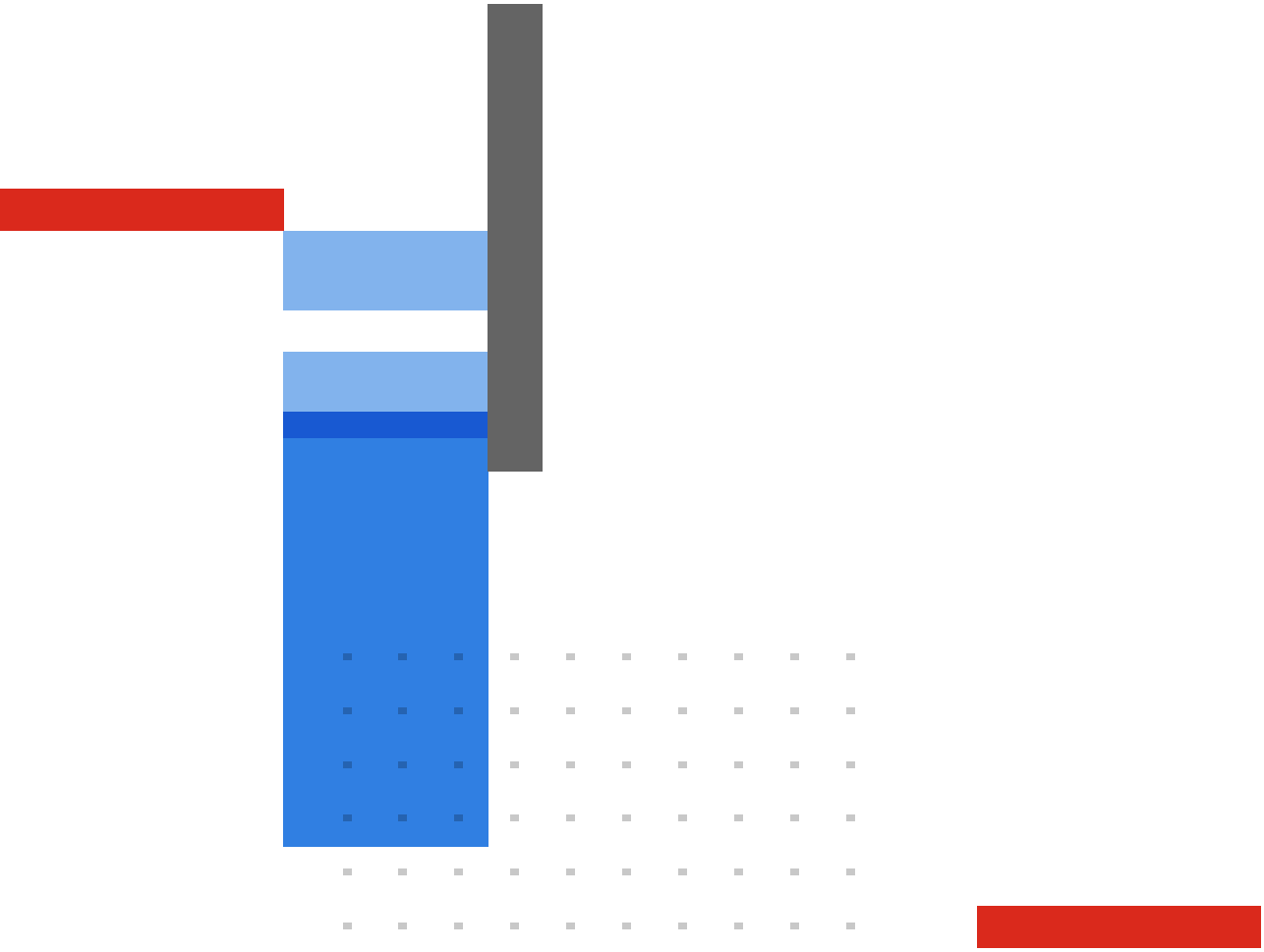
Specifications

Additional RFCs	
Other Protocols	
RFC 7540	Hypertext Transfer Protocol Version 2 (HTTP/2) For RFC 7540, only flow mode is supported; proxy mode is not yet supported.
RFC 5424	The Syslog Protocol
RFC 5357	A Two-Way Active Measurement Protocol (TWAMP)
RFC 5214	Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)
RFC 4960	Stream Control Transmission Protocol
RFC 3435	Media Gateway Control Protocol (MGCP) Version 1.0
RFC 3376	Internet Group Management Protocol, Version 3
RFC 5357	A Two-Way Active Measurement Protocol (TWAMP)
RFC 5214	Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)
RFC 4960	Stream Control Transmission Protocol
RFC 3435	Media Gateway Control Protocol (MGCP) Version 1.0
RFC 3376	Internet Group Management Protocol, Version 3
RFC 2890	Key and Sequence Number Extensions to GRE
RFC 2784	Generic Routing Encapsulation (GRE)
RFC 2661	Layer Two Tunneling Protocol "L2TP"
RFC 2637	Point-to-Point Tunneling Protocol (PPTP)
RFC 2412	The OAKLEY Key Determination Protocol
RFC 2225	Classical IP and ARP over ATM
RFC 2033	Local Mail Transfer Protocol
RFC 1413	Identification Protocol
RFC 1305	Network Time Protocol (Version 3) Specification, Implementation and Analysis
RFC 1011	Official Internet Protocols
RFC 959	File Transfer Protocol (FTP)
RFC 826	Echo Protocol
RFC 783	The TFTP Protocol (Revision 2)
RFC 768	User Datagram Protocol
-	The TACACS+ Protocol

Additional RFCs	
Miscellaneous	
RFC 7348	Virtual eXtensible Local Area Network (VXLAN): A Framework for Overlaying Virtualized Layer 2 Networks over Layer 3 Networks
RFC 4784	Verizon Wireless Dynamic Mobile IP Key Update for cdma2000(R) Networks for cdma2000(R) Networks
RFC 4470	Minimally Covering NSEC Records and DNSSEC On-line Signing
RFC 3985	Pseudo Wire Emulation Edge-to-Edge (PWE3) Architecture
RFC 2979	Behavior of and Requirements for Internet Firewalls
RFC 2827	Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing
RFC 2780	IANA Allocation Guidelines For Values In the Internet Protocol and Related Headers
RFC 2647	Benchmarking Terminology for Firewall Performance
RFC 2644	Changing the Default for Directed Broadcasts in Routers
RFC 2231	MIME Parameter Value and Encoded Word Extensions: Character Sets, Languages, and Continuations
RFC 1945	Hypertext Transfer Protocol -- HTTP/1.0
RFC 950	Internet Standard Subnetting Procedure
RFC 894	A Standard for the Transmission of IP Datagrams over Ethernet Networks

Fortinet Corporate Social Responsibility Policy

Fortinet is committed to driving progress and sustainability for all through cybersecurity, with respect for human rights and ethical business practices, making possible a digital world you can always trust. You represent and warrant to Fortinet that you will not use Fortinet's products and services to engage in, or support in any way, violations or abuses of human rights, including those involving illegal censorship, surveillance, detention, or excessive use of force. Users of Fortinet products are required to comply with the Fortinet EULA and report any suspected violations of the EULA via the procedures outlined in the Fortinet Whistleblower Policy.



FORTINET

www.fortinet.com

September 15, 2025

FOS-WLC-DAT-R9-20250915