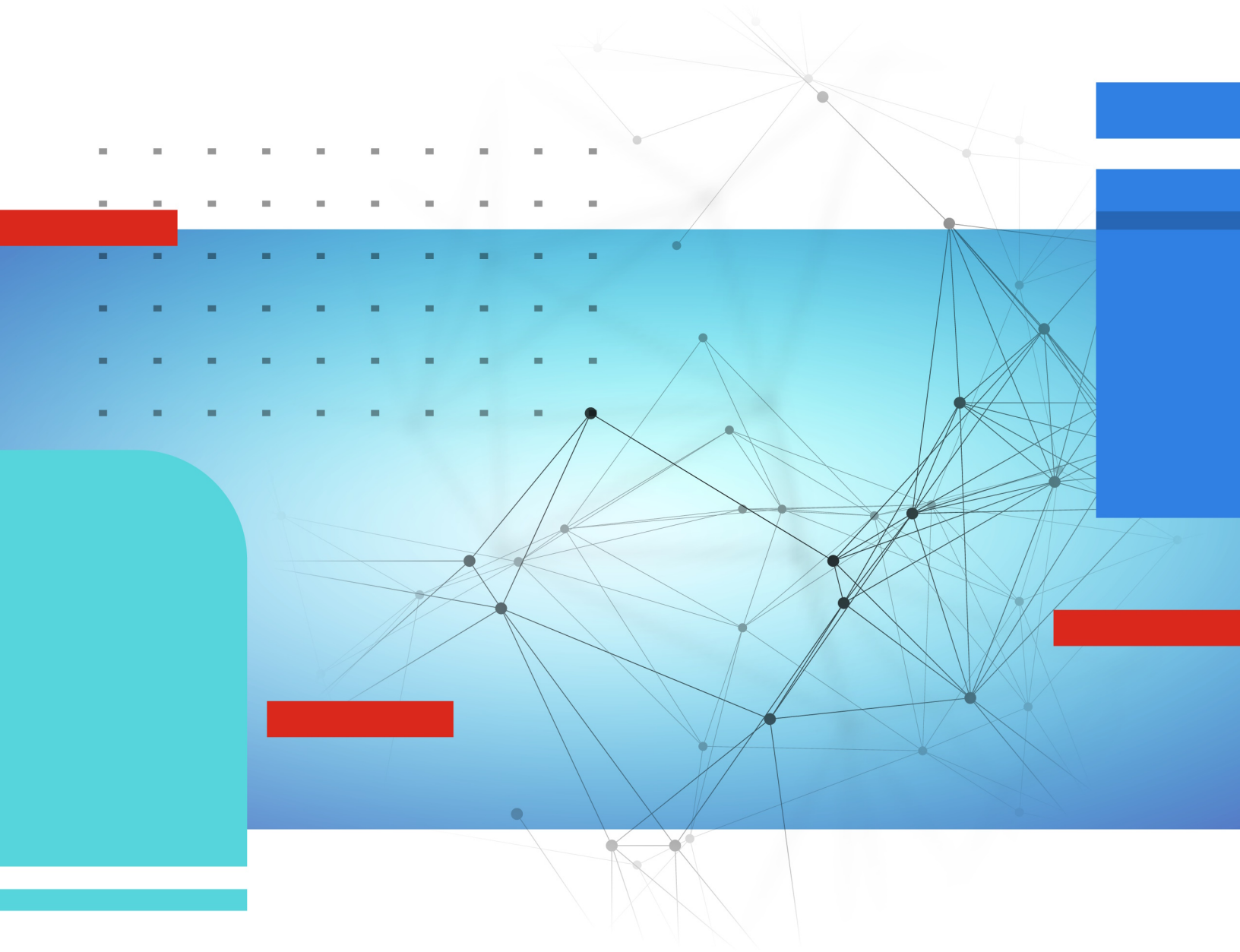
Supported RFCs

FortiProxy 7.6



FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO LIBRARY
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

FORTINET TRAINING INSTITUTE
https://training.fortinet.com

FORTIGUARD LABS
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

November 18, 2024
FortiProxy 7.6 Supported RFCs
45-760-1100093-20241118

TABLE OF CONTENTS

Change Log

Date	Change Description
2024-11-18	Initial document release.

Supported RFCs

FortiOS supports the following RFCs:

Cryptography	IPv6	SSH
DHCP	LDAP	SSL
DNS	NAT	TCP
ICMP	PPP	TLS
IP	RADIUS	VPN
IPsec	SFTP	Other protocols
IPv4	SNMP	Miscellaneous

Cryptography

- 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 6954: Using the Elliptic Curve Cryptography (ECC) Brainpool Curves 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

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

DNS

- RFC 8310: Usage Profiles for DNS over (D)TLS
- 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

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

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 7761: Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised)
- 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 4389: Neighbor Discovery Proxies (ND Proxy)
- RFC 4213: Basic Transition Mechanisms for IPv6 Hosts and Routers
- 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
- RFC 8200: Internet Protocol, Version 6 (IPv6) Specification
- RFC 8201: Path MTU Discovery for IP version 6

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 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)

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

SFTP

- draft-ietf-secsh-filexfer-00: SSH File Transfer Protocol
- draft-ietf-secsh-filexfer-01: SSH File Transfer Protocol
- draft-ietf-secsh-filexfer-02: SSH File Transfer Protocol
- draft-ietf-secsh-filexfer-03: SSH File Transfer Protocol
- draft-ietf-secsh-filexfer-04: SSH File Transfer Protocol
- draft-ietf-secsh-filexfer-05: SSH File Transfer Protocol
- draft-ietf-secsh-filexfer-06: SSH File Transfer Protocol
- draft-ietf-secsh-filexfer-07: SSH File Transfer Protocol
- draft-ietf-secsh-filexfer-08: SSH File Transfer Protocol
- draft-ietf-secsh-filexfer-09: SSH File Transfer Protocol
- draft-ietf-secsh-filexfer-10: SSH File Transfer Protocol
- draft-ietf-secsh-filexfer-11: SSH File Transfer Protocol
- draft-ietf-secsh-filexfer-12: SSH File Transfer Protocol
- draft-ietf-secsh-filexfer-13: SSH File Transfer 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)
- 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 1006: ISO Transport Service on top of the TCP Version: 3
- 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 5246: The Transport Layer Security (TLS) Protocol Version 1.2

VPN

- RFC 3715: IPsec-Network Address Translation (NAT) Compatibility Requirements

Other protocols

- RFC 8484: DNS Queries over HTTPS (DoH)
- RFC 7541: HPACK: Header Compression for HTTP/2
- RFC 7540: Hypertext Transfer Protocol Version 2 (HTTP/2)
- RFC 5424: The Syslog Protocol
- RFC 5357: A Two-Way Active Measurement Protocol (TWAMP)
- RFC 5214: Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)
- 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 2033: Local Mail Transfer Protocol
- RFC 1928: SOCKS Protocol Version 5.
  Supported when explicit proxy is implemented.
- 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 862: Echo Protocol
- RFC 783: The TFTP Protocol (Revision 2)
- RFC 768: User Datagram Protocol
- The TACACS+ Protocol

Miscellaneous

- RFC 8555: Automatic Certificate Management Environment (ACME)
  Supported only as a client.
- RFC 7348: Virtual eXtensible Local Area Network (VXLAN): A Framework for Overlaying Virtualized Layer 2 Networks over Layer 3 Networks
- RFC 4470: Minimally Covering NSEC Records and DNSSEC On-line Signing
- 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 905: ISO Transport Protocol Specification ISO DP 8073
- RFC 894: A Standard for the Transmission of IP Datagrams over Ethernet Networks

www.fortinet.com