Specifications	Description	USG2110F/FW/AW/AGW V300R001	USG2160/W V300R001	USG2230 V300R001	USG2260 V300R001	USG5120 V300R001	USG5150 V300R001
Memory		512M	512M	2G	2G	2G	2G
Flash		32M	32M	64M	64M	64M	64M
SD card		Not Supported	2G	2G	2G	2G	2G
Fixed interface	WAN	2FE/2FE/1FE+1ADSL	1FE	2GE Combo	2GE Combo	2GE Combo+2GE	4GE Combo
	LAN	8FE	8FE	Not Supported	Not Supported	Not Supported	Not Supported
	Wi-Fi	Not Supported/Supported/Supported	Not Supported/Supported	Not Supported	Not Supported	Not Supported	Not Supported
	USB port	1	1	2	2	2	2
	Console interface	1	1	1	1	1	1
Number of slots	Number of slots supported by the device	Not Supported	2 MIC (1 DMIC)	4 MIC (2 DMIC)+2 FIC (1 DFIC)	4 MIC (2 DMIC)+2 FIC (1 DFIC)	4 MIC (2 DMIC)+2 FIC (1 DFIC)+2 DFIC	4 MIC (2 DMIC)+2 FIC+4 DFIC
Types of interface cards	Types of extension cards supported by the device	USB expansion: WCDMA 3G, CDMA2000 3G, and TD-SCDMA 3G	MIC: 1FE, 5FSW, 1E1, 1CE1, 1Wi-Fi, 1SA, 2SA, 1ADSL2+, 4G.SHDSL.bis, 2G.SHDSL.bis, 1G.SHDSL.bis, 3G-WCDMA, 3G-CDMA2000, 3G-TD-SCDMA DMIC: 8FE2GE FIC: 2E1, 2CE1, 4E1, 4CE1, 8E1, 8CE1, 2FE+2FE Combo, 1GE, 4GE, 16FXS, 1GPONot Supported DFIC: 18FE+2SFP, 16GE+4SFP USB expansion: WCDMA 3G, CDMA2000 3G, TD-SCDMA 3G				
Maximum number of interfaces	Number of interfaces in full configuration	10 FE	17 FE+2 GE	26 GE+16 FE	26 GE+16 FE	68 GE+16 FE	108 GE+16 FE
Dimensions (H x W x D)	Including the frame and exterior	35 mm x 280 mm x 190 mm	43.6 mm x 420 mm x 255 mm	43.6 mm x 442 mm x 414 mm	43.6 mm x 442 mm x 414 mm	86.1 mm x 442 mm x 414 mm	130.5 mm x 442 mm x 414 mm
Weight	Device weight	< 2.0 kg	5 kg	Bare machine: 5.4 kg, full configuration ≤ 8 kg	Bare machine: 5.4 kg, full configuration ≤ 8 kg	Bare machine: 6.5 kg, full configuration ≤ 13.5 kg	Bare machine: 8.3 kg, full configuration ≤ 18 kg
Power supply	AC power supply, voltage, and current	100 V to 240V	100 V to 240 V	85 V to 264 V	85 V to 264 V	100 V to 240 V	100 V to 240 V
	DC power supply	Not Supported	Not Supported	Not Supported	–48 V to –60 V	–48 V to –60 V	–48 V to –60 V
	Power supply	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported	Supported
Power	Power of the power supply and the maximum power	< 18 W	Power for typical empty configuration: 15 W, maximum power: 35 W	100 W	100 W	210 W	300 W
Ambient temperature	Long-term operating, short-term operating, and storage temperatures	0 to 40	0 to 40	0 to 45 (long-term), –5 to 55 (short-term)	0 to 45 (long-term), –5 to 55 (short-term)	0 to 45 (long-term), –5 to 55 (short-term)	0 to 45 (long-term), –5 to 55 (short-term)
Ambient humidity	Operating humidity and storage humidity	10% to 90%, non-condensing	10% to 90%, non-condensing	5% to 95%, non-condensing	5% to 95%, non-condensing	5% to 95%, non-condensing	5% to 95%, non-condensing
Hot swappable module	Including the fan and power supply	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported	The power supply and fan are hot swappable.
MTBF/MTTR	Mean Time Between Failures Mean Time To Repair	MTBF: 12.67 years MTTR: 0.5 hours	MTBF: 12.67 years MTTR: 0.5 hours	MTBF: 12.67 years MTTR: 0.5 hours	MTBF: 12.67 years MTTR: 0.5 hours	MTBF: 12.67 years MTTR: 0.5 hours	MTBF: 12.67 years MTTR: 0.5 hours
Hardware certification							
	Chinese wireless model standards			Supported	Supported	Supported	Supported
	CE-CERTI	Supported	Supported	Supported	Supported	Supported	Supported
	CB-Aoc-HW-TUVPS	Supported					
	CB-TUVPS	Supported	Supported	Supported	Supported	Supported	Supported
	CE EMC-Aoc-HW-TUVPS	Supported	Supported	Supported	Supported	Supported	Supported
	CE LVD-Aoc-HW-TUVPS	Supported	Supported	Supported	Supported	Supported	Supported
	UL	Supported	Supported	Supported	Supported	Supported	Supported
	FCC-PART15	Supported	Supported	Supported	Supported	Supported	Supported
	FCC-DOC	Supported	Supported	Supported	Supported	Supported	Supported
	IC-SDOC	Supported	Supported	Supported	Supported	Supported	Supported
	VCCI	Supported	Supported	Supported	Supported	Supported	Supported
	C-TICK	Supported	Supported	Supported	Supported	Supported	Supported
	RoHS	Supported	Supported	Supported	Supported	Supported	Supported
	CCC	Supported	Supported	Supported	Supported	Supported	Supported
	REACH	Supported	Supported	Supported	Supported	Supported	Supported
	WEEE	Supported	Supported	Supported	Supported	Supported	Supported
Software certification							
	Ministry of Information Industry	Supported	Supported	Supported	Supported	Supported	Supported
	ICSA authentication(4.1x)	Supported	Supported	Supported	Supported	Supported	Supported
	ISCCC	Supported	Supported	Supported	Supported	Supported	Supported
	Wi-Fi	Supported	Supported	Supported	Supported	Supported	Supported

Specifications	Description	USG2110F/FW/AW/AGW V300R001	USG2160/W V300R001	USG2230 V300R001	USG2260 V300R001	USG5120 V300R001	USG5150 V300R001
Built-in interface		2110F/FW: 2 FE (WAN)+8 FE (LAN) 2110AW/AGW:1 FE (WAN)+1 ADSL+8 FE (LAN)	1 FE (WAN)+8 FE (LAN)	2 GE Combo	2 GE Combo	2 GE+2 GE Combo	4 GE Combo
Number of slots		Not Supported	1 MIC	4 MIC+2 FIC	4 MIC+2 FIC	4 MIC+2 FIC+2 DFIC	4 MIC+2 FIC+4 DFIC
MIC interface card							
MIC-1E1	1-port E1 & Fractional E1 interface card	Not Supported	Supported	Supported	Supported	Supported	Supported
MIC-1CE1	1-port channelized E1 interface card	Not Supported	Supported	Supported	Supported	Supported	Supported
MIC-1ADSL2+	1-port ADSL interface card	Not Supported	Supported	Supported	Supported	Supported	Supported
MIC-1FE	1-port 100M interface card	Not Supported	Supported	Supported	Supported	Supported	Supported
MIC-5ESW[1]	5-port 100M switching interface card (old)	Not Supported	Supported	Supported	Supported	Supported	Supported
MIC-5FSW	5-port 100M switching interface card	Not Supported	Supported	Supported	Supported	Supported	Supported
MIC-1SA	1-port synchronous/asynchronous interface card	Not Supported	Supported	Supported	Supported	Supported	Supported
MIC-2SA	2-port synchronous/asynchronous interface card	Not Supported	Supported	Supported	Supported	Supported	Supported
MIC-4G.SHDSL.bis	4-port G.SHDSL interface card	Not Supported	Supported	Supported	Supported	Supported	Supported
MIC-2G.SHDSL.bis	2-port G.SHDSL interface card	Not Supported	Supported	Supported	Supported	Supported	Supported
MIC-1G.SHDSL.bis	1-port G.SHDSL interface card	Not Supported	Supported	Supported	Supported	Supported	Supported
MIC-3G	WCDMA, CDMA2000, and TD-SCDMA	Not Supported	Supported	Supported	Supported	Supported	Supported
MIC-1Wi-Fi	1-port Wi-Fi interface card	Not Supported	Not Supported	Supported	Supported	Supported	Supported
DMIC-8FE2GE		Not Supported	Supported	Supported	Supported	Supported	Supported
Interface card exclusiveness	Each 3G or Wi-Fi model of integrated devices supports only one card.						
FIC interface card							
FIC-2E1	2-port unchannelized E1 interface card	Not Supported	Not Supported	Supported	Supported	Supported	Supported
FIC-2CE1	2-port channelized E1 interface card	Not Supported	Not Supported	Supported	Supported	Supported	Supported
FIC-4E1	4-port unchannelized E1 interface card	Not Supported	Not Supported	Supported	Supported	Supported	Supported
FIC-4CE1	4-port channelized E1 interface card	Not Supported	Not Supported	Supported	Supported	Supported	Supported
FIC-8E1	8-port unchannelized E1 interface card	Not Supported	Not Supported	Supported	Supported	Supported	Supported
FIC-8CE1	8-port channelized E1 interface card	Not Supported	Not Supported	Supported	Supported	Supported	Supported
FIC-1GE	1-port Gigabit interface card	Not Supported	Not Supported	Supported	Supported	Supported	Supported
FIC-4GE	2-port Gigabit interface card	Not Supported	Not Supported	Supported	Supported	Supported	Supported
FIC-2FE+2FE Combo	2-port 100M+2-port 100M optical/electrical (mutually exclusive) interface card	Not Supported	Not Supported	Supported	Supported	Supported	Supported
FIC-4GE bypass		Not Supported	Not Supported	Not Supported	Not Supported	Supported	Supported
DFIC interface card							
DFIC-18FE+2SFP		Not Supported	Not Supported	Supported	Supported	Supported	Supported
DFIC-16GE+4SFP		Not Supported	Not Supported	Supported	Supported	Supported	Supported
Interface card exclusiveness	The USG5150 has limitations on slots.						Slots FIC9 and FIC10 do not support the FIC-1GE, FIC-4GE, and DFIC cards.
USB							
USB-Key		Supported	Supported	Supported	Supported	Supported	Supported
USB-3G-WCDMA	WCDMA format USB-3G	Supported	Supported	Supported	Supported	Supported	Supported
USB-3G-TD-CDMA	TD-CDMA format USB-3G	Supported	Supported	Supported	Supported	Supported	Supported
USG-3G-CDMA2000	CDMA2000 format USB-3G	Supported	Supported	Supported	Supported	Supported	Supported
Interface card exclusiveness	Each model of integrated devices supports only one 3G card.						

Note:
1. Compared with the MIC-5FSW card, the MIC-5ESW supports less VLANs, and does not support Layer-2 features such as QoS and mirroring.

Primary Specifications	Secondary Specifications	Description	Note	USG2110F/FW/AW/AGW V3R1	USG2160/W V3R1	USG2230/USG2260 V3R1	USG5120/USG5150 V3R1
Vlanif sub-interface				Supported	Supported	Supported	Supported
	Basic function						
		Adding Layer-2 Eth-Trunk interfaces to the Vlanif interface		Supported	Supported	Supported	Supported
		VRRP		Supported	Supported	Supported	Supported
		Unicast routing protocol	BGP, OSPF, IS-IS, and RIP	Supported	Supported	Supported	Supported
		LDP signal		Supported	Supported	Supported	Supported
		Access CE	PEs including Layer-3 MPLS/BGP VPN	Supported	Supported	Supported	Supported
		IPv4/IPv6/MPLS forwarding		Supported	Supported	Supported	Supported
		Static ARP	The command specifies the actual physical interface or Trunk ID.	Supported	Supported	Supported	Supported
		Serving as the outbound interface of policy-based routes		Supported	Supported	Supported	Supported
		NetStream		Supported	Supported	Supported	Supported
			Supports the enabling of NetStream on the physical interface based on configurations.	Supported	Supported	Supported	Supported
			Netstream supports traffic aggregation based on global VLANs.	Supported	Supported	Supported	Supported
		Traffic statistics	Supports traffic statistics based on VLANs.	Supported	Supported	Supported	Supported
		Number of Vlanif interfaces for the integrated device		15	15	1024	1024
		MTU range	46 to 9600	328 to 1500	328 to 1500	328 to 1500	328 to 1500
VLAN sub-interface				Supported	Supported	Supported	Supported
	Basic protocol						
		802.1q encapsulation		Supported	Supported	Supported	Supported
		Inter-VLAN forwarding	Configures the sub-interfaces for a physical interface to enable communications among VLANs. Packets are forwarded at Layer 3.	Supported	Supported	Supported	Supported
		Layer-3 VPN access		Supported	Supported	Supported	Supported
		Layer-2 switching cannot be directly performed between the VLAN sub-interface and the global VLAN interface.	Except Layer-2 VPN cases covering VPLS, VLL, and V-SWITCH	Supported	Supported	Supported	Supported
		URPF		Supported	Supported	Supported	Supported
		Traffic classification	Supports both the incoming and outgoing directions.	Supported	Supported	Supported	Supported
		Upper layer protocols	Unless otherwise specified, upper-layer protocols supported by the VLAN sub-interface are the same as those supported by the Ethernet WAN interface.	Supported	Supported	Supported	Supported
		sub-interface statistics		Supported	Supported	Supported	Supported
Eth-Trunk							
	Manual aggregation						
		Creation of Layer-2 aggregation interfaces				Supported	Supported
		Adding Layer-2 Ethernet interfaces as members of the Eth-Trunk interface				Supported	Supported
		In-board binding				Supported	Supported
		Cross-board binding				Supported (not supported in Layer-2 aggregation)	Supported (not supported in Layer-2 aggregation)
		Binding between LANs and between WANs				Supported	Supported
		Binding of ports with different rates	Supports the binding between FE and GE interfaces			Supported The total weights of member ports cannot exceed the number of member ports of the Eth-Trunk interface.	Supported The total weights of member ports cannot exceed the number of member ports of the Eth-Trunk interface.
		Member interface				Supported	Supported
		IP/MAC binding				Supported	Supported
		Maximum number of Eth-Trunks				16	16
		Maximum number of members of an Eth-Trunk interface				8	8
	Static LACP						
		Setting of system priority and port priority	Range, priority, and default value			Supported	Supported
		LACPDU packet forwarding				Supported	Supported
		Link aggregation group switchover				Supported	Supported
		LACP preemption	Supports LACP preemption based on priority. You need to configure the function on devices on both ends to enable the function.			Supported	Supported
		Setting of the LACP active mode and passive mode				Supported	Supported
		Setting of LACP packet timeout				Supported	Supported
		Preemption of the active LACP ports with a higher priority	The preemption delay can be configured			Supported	Supported
		Selection of LACP active port based on port rate LACP				Supported	Supported
		Selection of LACP active port based on port priority				Supported	Supported
	Dynamic LACP						
		Enabling LACP				Supported	Supported
		Automatic creation of port aggregation				Supported	Supported
	Load-balancing of unicast packets					Supported	
	Load-balancing of multicast packets					Supported	
	Internal rapid switchover		When a port in the Trunk group turns down, traffic is rapidly switched to another port in the group. The switchover duration varies with the fault detection speed.			Supported (Supports Phycheck scheduled detection, but not interruption sensing or BFD detection. The switchover duration is longer.)	
	Active/Standby port		You can configure the active and standby ports. During the active/standby switchover, sessions do not change. The non-preemption mode is provided.			Supported	
	Setting of load-balancing weights of the member ports					Supported	
		Tunnel transversal over the private network for remote access L3VPN		Supported	Supported	Supported	Supported
		Bearing BGP VPN (L3VPN)		Supported	Supported	Supported	Supported
		Tunnel detection in LinkAlive mode		Supported	Supported	Supported	Supported
		Multicast		Supported	Supported	Supported	Supported
		LDP		Supported	Supported	Supported	Supported
		IPv6		Supported	Supported	Supported	Supported
		Tunnel nesting		Supported	Supported	Supported	Supported
		Checksum		Supported	Supported	Supported	Supported
Console port				Supported	Supported	Supported	Supported
	Port type	RS232		RS232	RS232	RS232	RS232
	Baud rate	Default value and configurable range		The interface rate ranges from 9600 bps to 115,200 bps. The default value is 9600 bps.	The interface rate ranges from 9600 bps to 115,200 bps. The default value is 9600 bps.	The interface rate ranges from 9600 bps to 115,200 bps. The default value is 9600 bps.	The interface rate ranges from 9600 bps to 115,200 bps. The default value is 9600 bps.
	Xmodem	Upgrade through Xmodem		Supported	Supported	Supported	Supported
Ethernet				Supported	Supported	Supported	Supported
	Physical-layer protocol	Supported protocols including IEEE 802.3 (standard Ethernet), IEEE802.3u (FE), IEEE802.3x (GE), and IEEE802.3ab (GE).		FE	FE	FE and GE	FE and GE

	Data link-layer protocol	Supported packet formats (including 802.3 and EthII). If a format is not supported, explain the processing mode such as discarding and transparent transmission.		ETHERNot SupportedET_II	ETHERNot SupportedET_II	ETHERNot SupportedET_II	ETHERNot SupportedET_II
	MTU	Range and default value		328 to 1500, 1500 by default	328 to 1500, 1500 by default	FE: 328 to 1500 GE: 328 to 1500	FE: 328 to 1500 GE: 328 to 1500
	Jumbo frame			Not Supported	Not Supported (Switching interface 5FE only)	Not Supported (Switching interfaces 5FE/18FE/16GE only)	Not Supported (Switching interfaces 5FE/18FE/16GE only)
	Port negotiation	Attributes including the duplex, rate, and cable type		10/100M/AUTO Full-duplex/half-duplex/auto-negotiation	10/100M/AUTO Full-duplex/half-duplex/auto-negotiation	FE: 10/100M/AUTO Full-duplex/half-duplex/auto-negotiation GE: 10/100M/1000/AUTO Full-duplex/half-duplex/auto-negotiation	FE: 10/100M/AUTO Full-duplex/half-duplex/auto-negotiation GE: 10/100M/1000/AUTO Full-duplex/half-duplex/auto-negotiation
	Port type	FE, GE, and 10GE		FE	FE	FE and GE	FE and GE
	Port statistics	Query and clearing of port statistics covering the rate and optical module		Supported	Supported	Supported	Supported
	Port control	Attributes including the duplex, rate, enabling, and traffic control (GE)		10/100M/AUTO Full-duplex/half-duplex/auto-negotiation	10/100M/AUTO Full-duplex/half-duplex/auto-negotiation	10/100M/1000/AUTO Full-duplex/half-duplex/auto-negotiation	10/100M/1000/AUTO Full-duplex/half-duplex/auto-negotiation
	Port mirroring			Supported (Supported by the WANot Supported interface, but not the LANot Supported interface)	Supported	Supported	Supported
	Loopback test			Supported	Supported	Supported	Supported
E1 interface				Not Supported	Supported	Supported	Supported
	Clock mode			Not Supported	Supported	Supported	Supported
		Line clock (default value)	Configuration command: clock slave	Not Supported	Supported	Supported	Supported
		Internal clock	Configuration command: clock master	Not Supported	Supported	Supported	Supported
	E1 frame format			Not Supported	Supported	Supported	Supported
		4-bit CRC verification	Configuration command: frame-format crc4	Not Supported	Supported	Supported	Supported
		Non-CRC verification	Configuration command: frame-format no-crc4	Not Supported	Supported	Supported	Supported
	E1 line code			Not Supported	Supported	Supported	Supported
		AMI code	Configuration command: code ami	Not Supported	Supported	Supported	Supported
		HDB3 code	Configuration command: code hdb3	Not Supported	Supported	Supported	Supported
	E1 power cable mode			Not Supported	Supported	Supported	Supported
		Long power cable mode	Configuration command: cable long	Not Supported	Supported	Supported	Supported
		Short power cable mode	Configuration command: cable short	Not Supported	Supported	Supported	Supported
	E1 and channelized E1 (CE1)			Not Supported	Supported	Supported	Supported
		E1 working mode	Configuration command: using e1	Not Supported	Supported	Supported	Supported
		CE1 working mode	Configuration command: using ce1	Not Supported	Supported	Supported	Supported
	Loopback test			Not Supported	Supported	Supported	Supported
		Local loopback	Configuration command: loopback local	Not Supported	Supported	Supported	Supported
		External payload loopback	Configuration command: loopback payload	Not Supported	Supported	Supported	Supported
		External remote loopback	Configuration command: loopback remote	Not Supported	Supported	Supported	Supported
	Indicator			Not Supported	Supported	Supported	Supported
		LINK	If the indicator is off, the link is disconnected. If the indicator is on, the link is connected.	Not Supported	Supported	Supported	Supported
		ACT	If the indicator is off, no data is being transmitted. If the indicator is blinking, data is being transmitted.	Not Supported	Supported	Supported	Supported
	Information statistics			Not Supported	Supported	Supported	Supported
		Traffic statistics	Collects statistics on traffic per second based on the numbers of the received and sent packets and bytes. Data is collected every five minutes.	Not Supported	Supported	Supported	Supported
		Sending and receiving statistics	Collects statistics on the numbers of the received and sent packets and bytes, covering the numbers of the correctly received and sent packets and bytes.	Not Supported	Supported	Supported	Supported
		Error statistics	Collects statistics on the numbers of the received and sent packets of various error types. Errors: runts, giants, CRC, overruns, aborts, and underruns	Not Supported	Supported	Supported	Supported
		Information clearing	Supports the clearing of statistics Configuration command: reset counter	Not Supported	Supported	Supported	Supported
	MTU		300 to 1500 bytes. The default value is 1500.	Not Supported	328 to 1500	328 to 1500	328 to 1500
	Incoming frame filtering		Hardware filtering on undersize packets and oversized packets	Not Supported	Supported	Supported	Supported
		CRC	Filtering on CRC error packets (that is, FCS) The error packets are filtered out at the bottom layer, but not forwarded.	Not Supported	Supported	Supported	Supported
		Undersize packet	The error packets are filtered out at the bottom layer, but not forwarded. (The undersize packet is smaller than or equal to 38 bytes.)	Not Supported	Supported	Supported	Supported
		Oversize packet	The error packets are filtered out at the bottom layer, but not forwarded. (The oversized packet is larger than 1600 bytes.)	Not Supported	Supported	Supported	Supported
	E1 bandwidth			Not Supported	Supported	Supported	Supported
		Minimum bandwidth	64000 bps	Not Supported	Supported	Supported	Supported
		Maximum bandwidth	2048000 bps	Not Supported	Supported	Supported	Supported
		Bandwidth range	CE1: n*64000 bps E1: 2048000 bps	Not Supported	Supported	Supported	Supported
	Testability			Not Supported	Supported	Supported	Supported
		LED test		Not Supported	Supported	Supported	Supported
		Key chip self-check		Not Supported	Supported	Supported	Supported
		EEPROM test		Not Supported	Supported	Supported	Supported
		Memory test		Not Supported	Not Supported/A	Not Supported/A	Not Supported/A
		Offline self-test: internal loopback test of data		Not Supported	Supported	Supported	Supported
		Offline self-test: external loopback test of data		Not Supported	Supported	Supported	Supported
		Offline self-test: chip loopback test		Not Supported	Supported	Supported	Supported
		Register test		Not Supported	Supported	Supported	Supported
		Clock test		Not Supported	Not Supported	Not Supported	Not Supported
	Alarm for remote signal loss		CE1 is supported and E1 is not supported.	Not Supported	Supported	Supported	Supported
SA serial port				Not Supported	Supported	Supported	Supported
		Standards: V.24, V.35, X.21, EIA/TIA-449, and EIA-530		Not Supported	Supported	Supported	Supported
	Number of ports			Not Supported	1	1 or 2	1 or 2
	Port rate			Not Supported			
		V.24	2400 bps to 64 kbps	Not Supported	2400 bps to 64 kbps	2400 bps to 64 kbps	2400 bps to 64 kbps
		V.35	2400 bps to 2048 kbps	Not Supported	2400 bps to 2048 kbps	2400 bps to 2048 kbps	2400 bps to 2048 kbps
		V.21	2400 bps to 2048 kbps	Not Supported	2400 bps to 2048 kbps	2400 bps to 2048 kbps	2400 bps to 2048 kbps
		RS449	2400 bps to 2048 kbps	Not Supported	2400 bps to 2048 kbps	2400 bps to 2048 kbps	2400 bps to 2048 kbps
		RS530	2400 bps to 2048 kbps	Not Supported	2400 bps to 2048 kbps	2400 bps to 2048 kbps	2400 bps to 2048 kbps
	Port feature			Not Supported			
			Working modes including V.35 (DTE and DCE), V.24 (DTE and DCE), X.21 (DTE and DCE), RS449 (DTE and DCE), RS530 (DTE) V35, V24, X.21, RS449, and RS530 Automatic identification of power cables	Not Supported	Working modes including V.35 (DTE and DCE), V.24 (DTE and DCE), X.21 (DTE and DCE), RS449 (DTE and DCE), RS530 (DTE) V35, V24, X.21, RS449, and RS530 Automatic identification of power cables	Working modes including V.35 (DTE and DCE), V.24 (DTE and DCE), X.21 (DTE and DCE), RS449 (DTE and DCE), RS530 (DTE) V35, V24, X.21, RS449, and RS530 Automatic identification of power cables	Working modes including V.35 (DTE and DCE), V.24 (DTE and DCE), X.21 (DTE and DCE), RS449 (DTE and DCE), RS530 (DTE) V35, V24, X.21, RS449, and RS530 Automatic identification of power cables

	Port type	DB28 connector		Not Supported	DB28 connector	DB28 connector	DB28 connector
	Transmission distance	V.24		Not Supported	15 m	15 m	15 m
		V.35		Not Supported	15 m	15 m	15 m
	Code type	NRZ and NRZI		Not Supported	Not SupportedRZ and Not SupportedRZI	Not SupportedRZ and Not SupportedRZI	Not SupportedRZ and Not SupportedRZI
	Service support	The interface supports data link-layer protocols such as PPP and HDLC.		Not Supported	The interface supports data link-layer protocols such as PPP and HDLC.	The interface supports data link-layer protocols such as PPP and HDLC.	The interface supports data link-layer protocols such as PPP and HDLC.
	System interface	The PCIE connects to the RPU through the backplane.		Not Supported	The PCIE connects to the RPU through the backplane.	The system interface complies with the PCI bus 2.1 standard (33 MHz/32 bits), and connects to the RPU through the backplane.	The system interface complies with the PCI bus 2.1 standard (33 MHz/32 bits), and connects to the RPU through the backplane.
	User interface			Not Supported			
		LINK		Not Supported	Supported	Supported	Supported
		ACT		Not Supported	Supported	Supported	Supported
	Working mode of local loopback			Not Supported	Supported	Supported	Supported
	Port management						
		Switchover of the synchronous/asynchronous serial port	1. By default, the synchronous/asynchronous serial port works in synchronous mode. You need to configure the port to work in asynchronous mode if required. 2. The serial port can be switched from synchronous to asynchronous when the port works in protocol mode.	Not Supported	Supported	Supported	Supported
		Enabling and disabling of ports	1. Configuration command: shutdown 2. Configuration command: undo shutdown. The command is executed by default.	Not Supported	Supported	Supported	Supported
		Setting of the link establishment mode	Supported asynchronous modes: 1. Protocol mode. This mode is configured by default. 2. Flow mode	Not Supported	Supported	Supported	Supported
	Telnet redirection		Asynchronous mode				
		Enabling and disabling of redirection	Disabling by default	Not Supported	Supported	Supported	Supported
		Setting of the idle timeout of Telnet		Not Supported	Supported	Supported	Supported
Wi-Fi				Supported	Supported	Supported	Supported
	Working mode			Supported	Supported	Supported	Supported
		802.11a		Supported	Supported	Supported	Supported
		802.11n		Supported	Supported	Supported	Supported
		802.11b		Supported	Supported	Supported	Supported
		802.11g		Supported	Supported	Supported	Supported
		Composite mode		Supported	Supported	Supported	Supported
	Data rate			Supported	Supported	Supported	Supported
		802.11a data rate	6, 9, 12, 18, 24, 36, 48 and 54 Mbps	Supported	Supported	Supported	Supported
		802.11b data rate	1, 2, 5.5 and 11 Mbps	Supported	Supported	Supported	Supported
		802.11g data rate	6, 9, 12, 18, 24, 36, 48 and 54 Mbps	Supported	Supported	Supported	Supported
		802.11n data rate	20 MHz channel: 1Nss: 65 Mbps @ 800GI, 72.2 Mbps @ 400GI 2Nss: 130 Mbps @ 800GI, 144.4 Mbps @ 400GI 40 MHz channel: 1Nss: 135 Mbps @ 800GI, 150 Mbps @ 400GI 2Nss: 270 Mbps @ 800GI, 300 Mbps @ 400GI	Supported	Supported	Supported	Supported
	Wi-Fi security policy						
		Wi-Fi encryption transmission	Supports 64-bit and 128-bit WEP encryption, TKIP, AES encryption; supports WPA-PSK and WPA2-PSK	Supported	Supported	Supported	Supported
		Authentication mode setting	Supports shared, WPA, WPA2, and WPA+WPA2	Supported	Supported	Supported	Supported
		802.1X authentication (RADIUS)	WPA-Enterprise and WPA2-Enterprise	Supported	Supported	Supported	Supported
		MAC address filtering	Blacklist and whitelist filtering Each of the blacklist and whitelist supports a maximum of 64 entries. A maximum of 256 entries can be supported.	Supported	Supported	Supported	Supported
	SSID management			Supported	Supported	Supported	Supported
		Multiple SSIDs		16	16	16	16
		SSID-VLAN binding		Supported	Supported	Supported	Supported
		Enabling and disabling of SSID broadcast		Supported	Supported	Supported	Supported
	Wi-Fi management						
		Setting of the AP isolation switch		Supported	Supported	Supported	Supported
		Setting of the country code		Supported	Supported	Supported	Supported
		Battery saving mode		Supported	Supported	Supported	Supported
		Configurable channel		Supported	Supported	Supported	Supported
ADSL				Supported	Supported	Supported	Supported
	Mode standard						
		auto		Supported	Supported	Supported	Supported
		g.lite	If g.lite is not configured at the peer end, use the auto mode.	Supported	Supported	Supported	Supported
		g.dmt		Supported	Supported	Supported	Supported
		t1.413		Supported	Supported	Supported	Supported
	Performance	Interface type RJ-11 Interface ADSL standard: ANSI T1.413 Issue 2 ITU G.992.1 (G.dmt) Annex A ITU G.992.2 (G.lite) Annex A ITU G.994.1 (G.hs) ADSL2 standard: ITU G.992.3 (G.dmt.bis) Annex A ITU G.992.4 (G.lite.bis) Annex A ADSL2+ standard: ITU G.992.5 Annex A Data transmission rate G.dmt in full speed: The downstream data flow rate is 8 Mbit/s, and the upstream data flow rate is 896 kbit/s. G.lite: The downstream data flow rate is 1.5 Mbit/s, and the upstream data flow rate is 512 kbit/s. T1.413: The downstream data flow rate is 8 Mbit/s, and the upstream data flow rate is 896 kbit/s. G.992.5 (ADSL2+): The downstream data flow rate is 24 Mbit/s, and the upstream data flow rate is 1.2 Mbit/s.		Supported	Supported	Supported	Supported
	Number of PVCs		The old card supports only one PVC. The new card supports eight PVCs. Seven of the PVCs can be configured on the host, one PVC is reserved.	8	8	8	8
	PVC encapsulation mode						
		bridge-llc		Supported	Supported	Supported	Supported
		bridge-vcmux		Supported	Supported	Supported	Supported
G.SHDSL				Not Supported	Supported	Supported	Supported
	Encapsulation mode						
		IPoEoA		Not Supported	Supported	Supported	Supported

		PPPoEoA		Not Supported	Supported	Supported	Supported
	Port binding			Not Supported	Supported	Supported	Supported
	Standard						
		G.991.2		Not Supported	Supported	Supported	Supported
		ETSI TS 101524		Not Supported	Supported	Supported	Supported
		Annex A, applicable to networks in North America		Not Supported	Supported	Supported	Supported
		Annex B, applicable to networks in Europe		Not Supported	Supported	Supported	Supported
	Cable			Not Supported			
		RJ11 connector, single-pair line		Not Supported	Supported	Supported	Supported
	Rate						
		192 kbps to 5696 kbps. If the value is set to 64 kbps, only the client mode is supported; that is, only the auto-negotiation rate mode is supported.		Not Supported	Supported	Supported	Supported
	Distance						
		6 km		Not Supported	Supported	Supported	Supported
3G					Supported	Supported	Supported
	Dual-SIM card			Supported (Only the model available to the fixed 3G card supports this feature.)	Not Supported	Not Supported	Not Supported
	Huawei ET128						
		Format	TD-SCDMA/EDGE/GPRS/GSM	Not Supported	Supported	Supported	Supported
		Frequency	TD-SCDMA: 2010 MHz to 2025 MHz GSM/GPRS/EDGE: 900MHz/1800MHz/1900MHz	Not Supported	Supported	Supported	Supported
		Maximum upstream rate	384 kbit/s	Not Supported	Supported	Supported	Supported
		Maximum downstream rate	2.8 Mbit/s	Not Supported	Supported	Supported	Supported
	Huawei E180						
		Format	HSUPA/HSDPA/UMTS/EDGE/GPRS/GSM	Supported	Supported	Supported	Supported
		Frequency	HSUPA/HSDPA/UMTS: 2100/900MHz EDGE/GPRS/GSM: 1900/1800/900/850MHz	Supported	Supported	Supported	Supported
		HSUPA maximum rate	The peak value of HSUPA is 2.0 Mbps (Standalone).	Supported	Supported	Supported	Supported
		HSDPA maximum rate	The peak value of HSDPA is 7.2 Mbps (Standalone).	Supported	Supported	Supported	Supported
	Huawei EC169						
		Format	1. CDMA2000 1x 2. CDMA2000 1x EV-DO Rev.0 3. CDMA2000 1x EV-DO Rev.A	Supported	Supported	Supported	Supported
		Frequency	800M/1900M	Supported	Supported	Supported	Supported
		Maximum upstream rate	1.8 Mbit/s	Supported	Supported	Supported	Supported
		Maximum downstream rate	3.1 Mbit/s	Supported	Supported	Supported	Supported
	Data service						
		PS attachment	Manual/automatic PS attachment and unattachment	Supported	Supported	Supported	Supported
		PDP activation and deactivation	Manual activation and deactivation of PDP Context	Supported	Supported	Supported	Supported
		PDP parameter modification	PDP Context modification	Supported	Supported	Supported	Supported
		PDP parameter query	PDP Context query	Supported	Supported	Supported	Supported
		APN parameter setting	APN parameter setting	Supported	Supported	Supported	Supported
		Sending traffic statistics	Statistics on accumulated sending traffic and sending failure times	Supported	Supported	Supported	Supported
		Receiving traffic statistics	Statistics on accumulated receiving traffic and error packets	Supported	Supported	Supported	Supported
		Connection time statistics	Time statistics on dial-up connections	Supported	Supported	Supported	Supported
		Current sending rate	Query of the current sending rate	Supported	Supported	Supported	Supported
		Current receiving rate	Query of the current receiving rate	Supported	Supported	Supported	Supported
	Network search						
		Selection of network search modes	Selection of the manual or automatic network search mode	Supported	Supported	Supported	Supported
		Priority selection of the network search access technology	Network search based on the priority of the access technology	Supported	Supported	Supported	Supported
		Frequency band selection	Selection of the frequency band supported by the board	Supported	Supported	Supported	Supported
		Selection of the network access domain	Selection of the network access domain	Supported	Supported	Supported	Supported
		Automatic network search and registration	Automatic network search and registration	Supported	Supported	Supported	Supported
		Manual registration of the specified network	After the manual network search is complete, you can select a network from the obtained network list for registration.	Supported	Supported	Supported	Supported
		Signal strength query	Signal strength query	Supported	Supported	Supported	Supported
		Query and report of the current service status	Query and report of the current service status	Supported	Supported	Supported	Supported
		Query of the current roaming status	Query of the current roaming status	Supported	Supported	Supported	Supported
		Query of the current service domain	Query of the current service domain	Supported	Supported	Supported	Supported
		Communications mode query	Communications modes that can be queried: GSM/GPRS/EDGE, WCDMA, HSDPA, and HSUPA.	Supported	Supported	Supported	Supported
	Expansion function						
		Query of the board version of the 3G module	Query of the hardware version of the 3G module	Supported	Supported	Supported	Supported
		Query of the board information of the 3G module	Query of the IMEI, IMSI, and SN of the 3G module	Supported	Supported	Supported	Supported
	Device management						
		Alarm report	Alarm report to the host end	Supported	Supported	Supported	Supported
		Error indication	Error indication through indicators	Supported	Supported	Supported	Supported
USB port				Supported	Supported	Supported	Supported
	Port type	USB2.0, compatible with 1.1, and does not support high rate		Supported	Supported	Supported	Supported
	Baud rate	12M at the highest value		Supported	Supported	Supported	Supported
	USB 3G			Supported	Supported	Supported	Supported
	USB key			Supported	Supported	Supported	Supported

Primary Specification	Secondary Specification	USG2110F/FW/AW/AGW V300R001	USG2160/W V300R001	USG2230 V300R001	USG2260 V300R001	USG5120 V300R001	USG5150 V300R001
Security							
Maximum throughput of the integrated device (bps)		180 Mbit/s	200 Mbit/s	900 Mbit/s	2 Gbit/s	2.5 Gbit/s	3.9 Gbit/s
Packet forwarding rate (pps)		120 kpps	160 kpps	360 kpps	490 kpps	950 kpps	1500 kpps
Number of new connections per second		2000	3000	20000	20000	40000	40000
Maximum number of concurrent connections		100000	200000	1000000	1000000	1200000	1200000
Working mode							
	Routing mode	Supported	Supported	Supported	Supported	Supported	Supported
	Transparent mode	Supported	Supported	Supported	Supported	Supported	Supported
	Composite mode	Supported	Supported	Supported	Supported	Supported	Supported
Security domain							
	Number of default security domains	4	4	4	4	4	4
	Number of security domains	Root firewall: 16 (4 fixed firewalls and 12 user-defined firewalls)	Root firewall: 16 (4 fixed firewalls and 12 user-defined firewalls) Virtual firewall: 8 (4 fixed firewalls and 4 user-defined firewalls)	Root firewall: 16 (4 fixed firewalls and 12 user-defined firewalls) Virtual firewall: 8 (4 fixed firewalls and 4 user-defined firewalls)	Root firewall: 16 (4 fixed firewalls and 12 user-defined firewalls) Virtual firewall: 8 (4 fixed firewalls and 4 user-defined firewalls)	Root firewall: 16 (4 fixed firewalls and 12 user-defined firewalls) Virtual firewall: 8 (4 fixed firewalls and 4 user-defined firewalls)	Root firewall: 16 (4 fixed firewalls and 12 user-defined firewalls) Virtual firewall: 8 (4 fixed firewalls and 4 user-defined firewalls)
	Range for the configuration of user-defined security domain precedence	1–100	1–100	1–100	1–100	1–100	1–100
	Number of the interfaces that can be added in the domain	1024	1024	1024	1024	1024	1024
Virtual firewall		Not Supported	Supported	Supported	Supported	Supported	Supported
	Maximum number of virtual firewalls	0	10	100	100	100	100
	Number of interfaces supported by the virtual firewall		100	100	100	100	100
	Forwarding across different virtual firewalls in the routing mode		Supported	Supported	Supported	Supported	Supported
	Configuration multi-instance		Supported	Supported	Supported	Supported	Supported
	Security domain multi-instance		Supported	Supported	Supported	Supported	Supported
	ACL multi-instance		Supported	Supported	Supported	Supported	Supported
	Address group multi-instance		Supported	Supported	Supported	Supported	Supported
	Service set multi-instance		Supported	Supported	Supported	Supported	Supported
	Session multi-instance		Supported	Supported	Supported	Supported	Supported
	Servermap multi-instance		Supported	Supported	Supported	Supported	Supported
	Blacklist multi-instance		Supported	Supported	Supported	Supported	Supported
	Virtual routing and forwarding (VRF)		Supported	Supported	Supported	Supported	Supported
	NAT multi-instance		Supported	Supported	Supported	Supported	Supported
	IPSEC VPN multi-instance		Supported	Supported	Supported	Supported	Supported
	L2TP VPN multi-instance		Supported	Supported	Supported	Supported	Supported
	GRE VPN multi-instance		Supported	Supported	Supported	Supported	Supported
	When IPv4 over IPv6 tunneling is used, multiple VPN instances can be bound.		Supported (When IPv4 over IPv6 tunneling is used, a VPN instance can be bound.)	Supported (When IPv4 over IPv6 tunneling is used, a VPN instance can be bound.)	Supported (When IPv4 over IPv6 tunneling is used, a VPN instance can be bound.)	Supported (When IPv4 over IPv6 tunneling is used, a VPN instance can be bound.)	Supported (When IPv4 over IPv6 tunneling is used, a VPN instance can be bound.)
	Network Time Protocol (NTP) multi-instance		Supported	Supported	Supported	Supported	Supported
	WEB multi-instance		Supported	Supported	Supported	Supported	Supported
	SLB multi-instance		Supported	Supported	Supported	Supported	Supported
	Network management multi-instance		Supported	Supported	Supported	Supported	Supported
	Management of virtual system users		Supported	Supported	Supported	Supported	Supported
	Multi-instance of virtual system user login log		Supported	Supported	Supported	Supported	Supported
	Multi-instance of virtual system user operation log		Supported	Supported	Supported	Supported	Supported
	Management of the virtual system by the system users with Telnet		Supported	Supported	Supported	Supported	Supported
	Management of the virtual system by the system users with SSH		Supported	Supported	Supported	Supported	Supported
	Management of the virtual system by the system users with WEB		Supported	Supported	Supported	Supported	Supported
Blacklist		Supported	Supported	Supported	Supported	Supported	Supported
	Number of static blacklist entries	256	256	256	256	256	256
	Number of dynamic blacklist entries	1024	1024	1024	1024	1024	1024
Packet filtering							
	Independent ACL rule in each inter-domain inbound direction	Supported	Supported	Supported	Supported	Supported	Supported
	Independent ACL rule in each inter-domain outbound direction	Supported	Supported	Supported	Supported	Supported	Supported
	Default filtering rule of the firewall	Supported	Supported	Supported	Supported	Supported	Supported
	Unique default rule based on inter-domain	Supported	Supported	Supported	Supported	Supported	Supported
	MAC address-based access rule configured on the interface	Supported	Supported	Supported	Supported	Supported	Supported
	Setting of the packet filtering functions in the designated domain	Supported	Supported	Supported	Supported	Supported	Supported
Access Control List (ACL)							
	Layer-2 ACL						
	Filtering based on the COS	Supported	Supported	Supported	Supported	Supported	Supported
	Filtering based on the destination MAC address	Supported	Supported	Supported	Supported	Supported	Supported
	Filtering based on the source MAC address and source mask	Supported	Supported	Supported	Supported	Supported	Supported
	Filtering based on the type code and type wildcard	Supported	Supported	Supported	Supported	Supported	Supported
	Layer-3 ACL						
	Filtering of the source address of IP packets	Supported	Supported	Supported	Supported	Supported	Supported
	Filtering of the destination address of IP packets	Supported	Supported	Supported	Supported	Supported	Supported
	Filtering of ICMP message types	Supported	Supported	Supported	Supported	Supported	Supported
	Filtering of ICMP message codes	Supported	Supported	Supported	Supported	Supported	Supported
	Filtering of the source and destination port numbers of TCP packets	Supported	Supported	Supported	Supported	Supported	Supported
	Filtering of the source and destination port numbers of UDP packets	Supported	Supported	Supported	Supported	Supported	Supported
	Packet precedence filtering	Supported (Support the filtering for TOS/Precedence.)	Supported (Support the filtering for TOS/Precedence.)	Supported (Support the filtering for TOS/Precedence.)	Supported (Support the filtering for TOS/Precedence.)	Supported (Support the filtering for TOS/Precedence.)	Supported (Support the filtering for TOS/Precedence.)
	Use of time range-based ACL rules	Supported (The time range-based ACL does not apply the IPSec Policy.)	Supported (The time range-based ACL does not apply the IPSec Policy.)	Supported (The time range-based ACL does not apply the IPSec Policy.)	Supported (The time range-based ACL does not apply the IPSec Policy.)	Supported (The time range-based ACL does not apply the IPSec Policy.)	Supported (The time range-based ACL does not apply the IPSec Policy.)
	Address group	Supported	Supported	Supported	Supported	Supported	Supported
	Mask	Supported	Supported	Supported	Supported	Supported	Supported
	Wildcard mask	Supported	Supported	Supported	Supported	Supported	Supported
	Nesting of address group	Supported	Supported	Supported	Supported	Supported	Supported
	Address object	Supported (The address group of object type)	Supported (The address group of object type)	Supported (The address group of object type)	Supported (The address group of object type)	Supported (The address group of object type)	Supported (The address group of object type)
	Number of items in the address set	2,048	2,048	10,000	10,000	10,000	10,000
	Maximum number of address groups	32 (Group-address-set address group)	32(Group-address-set address group)	512 (Group-address-set address group)	512 (Group-address-set address group)	512 (Group-address-set address group)	512 (Group-address-set address group)
	Number of the addresses of each address group	256	256	256	256	256	256
	Maximum number of the address group elements			100,000	100,000	100,000	100,000
	Service set	Supported	Supported	Supported	Supported	Supported	Supported
	Number of service objects	64 (Service object can define the protocol for data flow, source port, and destination port. Service object is included in the service set.)	64 (Service object can define the protocol for data flow, source port, and destination port. Service object is included in the service set.)	1024 (Service object can define the protocol for data flow, source port, and destination port. Service object is included in the service set.)	1024 (Service object can define the protocol for data flow, source port, and destination port. Service object is included in the service set.)	1024 (Service object can define the protocol for data flow, source port, and destination port. Service object is included in the service set.)	1024 (Service object can define the protocol for data flow, source port, and destination port. Service object is included in the service set.)
	Service set nesting	Supported	Supported	Supported	Supported	Supported	Supported
	Number of service groups	16	16	512	512	512	512
	Number of predefined service objects	64	64	256	256	256	256
	Number of items in the service	1,024	1,024	10,000	10,000	10,000	10,000
	ACL acceleration	Supported	Supported	Supported	Supported	Supported	Supported
	After the ACL rules are changed, the service using the ACL takes effect automatically.	Supported	Supported	Supported	Supported	Supported	Supported
	Counting of the hits of the rule	Supported	Supported	Supported	Supported	Supported	Supported
	The ACL supports field description.	Supported	Supported	Supported	Supported	Supported	Supported
	The rule supports field description.	Supported	Supported	Supported	Supported	Supported	Supported
	Basic ACL groups marked with numerals	2000~2999	2000~2999	2000~2999	2000~2999	2000~2999	2000~2999
	Advanced ACL groups marked with numerals	3000~3999	3000~3999	3000~3999	3000~3999	3000~3999	3000~3999
	Number of ACL rules in each ACL group	2048	2048	20000	20000	20000	20000
	Number of ACL rules with logs	2048	2048	2048	2048	2048	2048
	Maximum number of definable ACLs	3000	3000	20000	20000	20000	20000
Time range							
	Absolute time ranges	Supported	Supported	Supported	Supported	Supported	Supported
	Periodical time ranges	Supported	Supported	Supported	Supported	Supported	Supported
	Number of configurable time ranges	255	255	255	255	255	255
	Maximum number of absolute times allowed in each time range	12	12	12	12	12	12
	Maximum number of cycle times allowed in each time range	32	32	32	32	32	32
Application Specific Packet Filter (ASPF)		Supported	Supported	Supported	Supported	Supported	Supported
	General TCP/UDP application	Supported	Supported	Supported	Supported	Supported	Supported
	FTP-based state detection	Supported	Supported	Supported	Supported	Supported	Supported
	RTSP-based state detection	Supported	Supported	Supported	Supported	Supported	Supported
	H323-based state detection	Supported	Supported	Supported	Supported	Supported	Supported

	SIP-based state detection	Supported (Support both UDP-based and TCP-based state detections, but the TCP-based state detection is not verified.)	Supported (Support both UDP-based and TCP-based state detections, but the TCP-based state detection is not verified.)	Supported (Support both UDP-based and TCP-based state detections, but the TCP-based state detection is not verified.)	Supported (Support both UDP-based and TCP-based state detections, but the TCP-based state detection is not verified.)	Supported (Support both UDP-based and TCP-based state detections, but the TCP-based state detection is not verified.)	Supported (Support both UDP-based and TCP-based state detections, but the TCP-based state detection is not verified.)
	MGCP-based state detection	Supported	Supported	Supported	Supported	Supported	Supported
	QQ-based state detection	Supported	Supported	Supported	Supported	Supported	Supported
	MSN-based state detection	Supported	Supported	Supported	Supported	Supported	Supported
	PPTP-based state detection	Supported	Supported	Supported	Supported	Supported	Supported
	SQL.NET-based state detection	Supported	Supported	Supported	Supported	Supported	Supported
	MMS-based state detection	Supported	Supported	Supported	Supported	Supported	Supported
	DNS-based state detection	Not Supported	Not Supported	Not Supported	Not Supported	Supported	Supported
	Java/ActiveX blocking	Supported	Supported	Supported	Supported	Supported	Supported
	User-defined port detection	Supported	Supported	Supported	Supported	Supported	Supported
	NetBIOS-based state detection	Supported	Supported	Supported	Supported	Supported	Supported
	ILS-based state detection	Supported	Supported	Supported	Supported	Supported	Supported
IP-MAC binding		Supported	Supported	Supported	Supported	Supported	Supported
	Number of entries	256	256	1000	1000	1000	1000
	Replacing ARP entry with the IP-MAC binding	Supported	Supported	Supported	Supported	Supported	Supported
	Filtering the packets of which the MAC addresses are not corresponding to the IP address	Supported	Supported	Supported	Supported	Supported	Supported
	Detecting the ARP automatically and binding IP addresses to MAC addresses	Supported	Supported	Supported	Supported	Supported	Supported
Defense		Supported	Supported	Supported	Supported	Supported	Supported
SYN flood defense		Supported	Supported	Supported	Supported	Supported	Supported
	TCP Proxy functions	Supported	Supported	Supported	Supported	Supported	Supported
	SYN Flood defense types detected based on the source IP address	Supported	Supported	Supported	Supported	Supported	Supported
	SYN flood defense for all the hosts in the designated security domain	Supported	Supported	Supported	Supported	Supported	Supported
	SYN flood defense for the destination hosts of the packets with designated inbound interfaces	Supported	Supported	Supported	Supported	Supported	Supported
	SYN Flood defense types based on the source security domain	Supported	Supported	Supported	Supported	Supported	Supported
	SYN flood defense for the designated destination IP addresses and ports	Supported	Supported	Supported	Supported	Supported	Supported
UDP flood defense		Supported	Supported	Supported	Supported	Supported	Supported
	UDP flood defense based on pattern matching	Supported	Supported	Supported	Supported	Supported	Supported
	UDP flood defense for all the hosts in the designated security domain	Supported	Supported	Supported	Supported	Supported	Supported
	UDP flood defense for the destination hosts of the packets with designated inbound interfaces	Supported	Supported	Supported	Supported	Supported	Supported
	Flow-based UDP flood defense	Supported	Supported	Supported	Supported	Supported	Supported
ICMP flood defense		Supported	Supported	Supported	Supported	Supported	Supported
	ICMP flood defense for all the hosts in the designated security domain	Supported	Supported	Supported	Supported	Supported	Supported
	ICMP flood defense for the destination hosts of the packets with designated inbound interfaces	Supported	Supported	Supported	Supported	Supported	Supported
	Flow-based ICMP flood defense	Supported	Supported	Supported	Supported	Supported	Supported
IP Spoofing		Supported	Supported	Supported	Supported	Supported	Supported
LAND attack		Supported	Supported	Supported	Supported	Supported	Supported
Smurf attack		Supported	Supported	Supported	Supported	Supported	Supported
Fraggle attack		Supported	Supported	Supported	Supported	Supported	Supported
Winnuke		Supported	Supported	Supported	Supported	Supported	Supported
Ping of Death		Supported	Supported	Supported	Supported	Supported	Supported
Tear Drop		Supported	Supported	Supported	Supported	Supported	Supported
Address scanning		Supported	Supported	Supported	Supported	Supported	Supported
Port scanning		Supported	Supported	Supported	Supported	Supported	Supported
Control of IP Option		Supported	Supported	Supported	Supported	Supported	Supported
Control of IP packet fragments		Supported	Supported	Supported	Supported	Supported	Supported
Inspection on the validity of TCP marks		Supported	Supported	Supported	Supported	Supported	Supported
Control of ultra-large ICMP packet		Supported	Supported	Supported	Supported	Supported	Supported
Control of ICMP redirection packet		Supported	Supported	Supported	Supported	Supported	Supported
Control of ICMP destination unreachable packet		Supported	Supported	Supported	Supported	Supported	Supported
Control of TRACERT packet		Supported	Supported	Supported	Supported	Supported	Supported
SYN inspection on the first TCP packet		Supported	Supported	Supported	Supported	Supported	Supported
Packet sequence test		Supported	Supported	Supported	Supported	Supported	Supported
http GET flood defense		Supported	Supported	Supported	Supported	Supported	Supported
Address Resolution Protocol (ARP) spoofing defense							
	Verification of ARP packet validity	Supported	Supported	Supported	Supported	Supported	Supported
	ARP request spoofing attack	Supported	Supported	Supported	Supported	Supported	Supported
	ARP response spoofing attack	Supported	Supported	Supported	Supported	Supported	Supported
	Reverse ARP	Supported	Supported	Supported	Supported	Supported	Supported
ARP flood defense		Supported	Supported	Supported	Supported	Supported	Supported
	ARP flood attack defense based on the ARP rate limit at the interface	Supported	Supported	Supported	Supported	Supported	Supported
	ARP flood defense over the designated interfaces	Supported	Supported	Supported	Supported	Supported	Supported
	Configuration of ARP attack rate threshold	Supported	Supported	Supported	Supported	Supported	Supported
Bandwidth management/Traffic control							
	Traffic control based on the interface	Supported	Supported	Supported	Supported	Supported	Supported
	IP-based control of traffic and connections	Supported	Supported	Supported	Supported	Supported	Supported
	Segment-based control of traffic and connections	Supported	Supported	Supported	Supported	Supported	Supported
	User-based control of traffic and connections	Supported	Supported	Supported	Supported	Supported	Supported
	User group-based control of traffic and connections	Supported	Supported	Supported	Supported	Supported	Supported
	Application protocol-based control of traffic and connections	Supported	Supported	Supported	Supported	Supported	Supported
	Time-based control of traffic and connections	Supported	Supported	Supported	Supported	Supported	Supported
	Data upload-based and download-based traffic control	Supported	Supported	Supported	Supported	Supported	Supported
	User- or IP-based assured bandwidth	Supported	Supported	Supported	Supported	Supported	Supported
	User- or IP-based limited bandwidth	Supported	Supported	Supported	Supported	Supported	Supported
	Bandwidth multiplexing during idle time	Supported	Supported	Supported	Supported	Supported	Supported
	Point-to-point (P2P) control	Supported	Supported	Supported	Supported	Supported	Supported
	Number of traffic classes	8	8	8	8	8	8
	Number of concurrent connection classes	8	8	8	8	8	8
	Configurable time range	Supported	Supported	Supported	Supported	Supported	Supported
	Signature database update	Supported	Supported	Supported	Supported	Supported	Supported
Network Address Translation (NAT)		Supported	Supported	Supported	Supported	Supported	Supported
	Address translation mode						
	Address translation in NO-PAT mode	Supported	Supported	Supported	Supported	Supported	Supported
	Address translation in PAT mode	Supported	Supported	Supported	Supported	Supported	Supported
	NAT extended function	Supported	Supported	Supported	Supported	Supported	Supported
	Address translation in address pool mode	Supported	Supported	Supported	Supported	Supported	Supported
	Number of address pools	32	32	1024	1024	1024	1024
	Length of the address pool	256	256	256	256	256	256
	Control of address translation by using ACLs	Supported	Supported	Supported	Supported	Supported	Supported
	Translation of the address by directly using the port IP address (Easy IP)	Supported	Supported	Supported	Supported	Supported	Supported
	Policy-based destination NAT	Supported	Supported	Supported	Supported	Supported	Supported
	Number of policy-based destination NATs	256	256	256	256	256	256
	Bidirectional NAT	Supported	Supported	Supported	Supported	Supported	Supported
	Bidirectional NAT ALG	Supported	Supported	Supported	Supported	Supported	Supported
	Intra-domain NAT and ALG	Supported	Supported	Supported	Supported	Supported	Supported
	NAT server	Supported	Supported	Supported	Supported	Supported	Supported
	Mapping of the IP addresses from Internet to Intranet	Supported	Supported	Supported	Supported	Supported	Supported
	Mapping of the IP addresses and interface number from Internet to Intranet	Supported	Supported	Supported	Supported	Supported	Supported
	Mapping of multiple Internet addresses to a server of the Intranet	Supported	Supported	Supported	Supported	Supported	Supported
	Mapping of NAT Server in the domain	Supported	Supported	Supported	Supported	Supported	Supported
	NAT server without reversing table	Supported	Supported	Supported	Supported	Supported	Supported
	Mapping of the Internet addresses which are domain names	Supported	Supported	Supported	Supported	Supported	Supported
	Interface-based configuration of Internet addresses	Supported	Supported	Supported	Supported	Supported	Supported
	NAT ALG	Supported	Supported	Supported	Supported	Supported	Supported
	FTP ALG	Supported	Supported	Supported	Supported	Supported	Supported
	H323 (including T.120) ALG	Supported	Supported	Supported	Supported	Supported	Supported
	RAS ALG	Supported	Supported	Supported	Supported	Supported	Supported
	SIP ALG	Supported	Supported	Supported	Supported	Supported	Supported

	MGCP ALG	Supported	Supported	Supported	Supported	Supported	Supported
	ICMP ALG	Supported	Supported	Supported	Supported	Supported	Supported
	RTSP	Supported	Supported	Supported	Supported	Supported	Supported
	NetBios ALG	Supported	Supported	Supported	Supported	Supported	Supported
	DNS ALG	Supported	Supported	Supported	Supported	Supported	Supported
	ILS ALG	Supported	Supported	Supported	Supported	Supported	Supported
	PPTP ALG	Supported	Supported	Supported	Supported	Supported	Supported
	QQ ALG	Supported	Supported	Supported	Supported	Supported	Supported
	MSN ALG	Supported	Supported	Supported	Supported	Supported	Supported
	User define ALG	Supported	Supported	Supported	Supported	Supported	Supported
	SQL.NET ALG	Supported	Supported	Supported	Supported	Supported	Supported
	MMS ALG	Supported	Supported	Supported	Supported	Supported	Supported
	ICQ ALG	Supported	Supported	Supported	Supported	Supported	Supported
	Internal server	Supported	Supported	Supported	Supported	Supported	Supported
	Number of internal servers	4096	4096	4096	4096	4096	4096
Server Load Balance (SLB)		Supported	Supported	Supported	Supported	Supported	Supported
	Port translation between the real server and the virtual server	Supported	Supported	Supported	Supported	Supported	Supported
	Source Hashing Scheduling	Supported	Supported	Supported	Supported	Supported	Supported
	Round Robin	Supported	Supported	Supported	Supported	Supported	Supported
	Weighted round robin	Supported	Supported	Supported	Supported	Supported	Supported
	Server survivability detection	Supported	Supported	Supported	Supported	Supported	Supported
	ALG	Supported	Supported	Supported	Supported	Supported	Supported
	FTP ALG	Supported	Supported	Supported	Supported	Supported	Supported
	Number of virtual servers	64	64	64	64	64	64
	Number of real servers supported by each virtual server	4	4	4	4	4	4
	Total number of the real servers	128	128	128	128	128	128
Virtual private network (VPN)		Supported	Supported	Supported	Supported	Supported	Supported
	Layer 2 Tunneling Protocol (L2TP)	Supported	Supported	Supported	Supported	Supported	Supported
	Number of L2TP VPN tunnels	64	64	2000	2000	4000	4000
	L2TP VPN performance	40 Mbit/s	50 Mbit/s	300 Mbit/s	500 Mbit/s	1 Gbit/s	2 Gbit/s
	L2TP access concentrator (LAC)	Supported	Supported	Supported	Supported	Supported	Supported
	Independent dial-up LAC	Supported	Supported	Supported	Supported	Supported	Supported
	L2TP network server (LNS)	Supported	Supported	Supported	Supported	Supported	Supported
	Optional tunneling verification functions: Implementation of optional Challenge Handshake Authentication Protocol (CHAP) authentication for the server LAC of the service port.	Supported	Supported	Supported	Supported	Supported	Supported
	The LAC of the service port supporting the pre-negotiation of PAP mode	Supported	Supported	Supported	Supported	Supported	Supported
	The LAC of the service port supporting the pre-negotiation of CHAP mode	Supported	Supported	Supported	Supported	Supported	Supported
	Forcible implementation of the CHAP verification on local port with the Client	Supported	Supported	Supported	Supported	Supported	Supported
	Implementation of LCP pre-negotiation with the Client again.	Supported	Supported	Supported	Supported	Supported	Supported
	Forcible disabling of the channel	Supported	Supported	Supported	Supported	Supported	Supported
	Supporting multiple trigger modes of L2TP to build channels	Supported	Supported	Supported	Supported	Supported	Supported
	LNS backup	Supported	Supported	Supported	Supported	Supported	Supported
	Configuration of the loopback port on the LAC as the source port of the tunnel	Supported	Supported	Supported	Supported	Supported	Supported
	GRE	Supported	Supported	Supported	Supported	Supported	Supported
	Number of GRE tunnels	64	64	1000	1000	1000	1000
	GRE performance	40 Mbit/s	50 Mbit/s	300 Mbit/s	500 Mbit/s	1 Gbit/s	2 Gbit/s
	Basic function of GRE encapsulation	Supported	Supported	Supported	Supported	Supported	Supported
	Display of the source tunnel address by the port name	Supported	Supported	Supported	Supported	Supported	Supported
	Use of the configured key to ensure security	Supported	Supported	Supported	Supported	Supported	Supported
	Verification of packets	Supported	Supported	Supported	Supported	Supported	Supported
	Periodical check on the tunnel interface state	Supported	Supported	Supported	Supported	Supported	Supported
	TUNNEL port supporting the MTU settings	Supported	Supported	Supported	Supported	Supported	Supported
	BGP routing protocol	Supported	Supported	Supported	Supported	Supported	Supported
	OSPF routing protocol	Supported	Supported	Supported	Supported	Supported	Supported
	RIP routing protocol	Supported	Supported	Supported	Supported	Supported	Supported
	Capacity of bearing MPLS packets	Supported	Supported	Supported	Supported	Supported	Supported
	Fragment and reassembly	Supported	Supported	Supported	Supported	Supported	Supported
	Maximum number of tunnels	256	256	256	256	256	256
	Forwarding of IPv6 packets by the GRE tunnel	Supported	Supported	Supported	Supported	Supported	Supported
	GRE tunnel supporting DDNS	Supported	Supported	Supported	Supported	Supported	Supported
	Multiprotocol Label Switching (MPLS)	Supported	Supported	Supported	Supported	Supported	Supported
	Number of L3 VPN LSPs	1,000	1,000	10,000	10,000	10,000	10,000
	MPLS forwarding (support label push, pop, and swap.)	Supported	Supported	Supported	Supported	Supported	Supported
	MPLS L3 VPN	Supported	Supported	Supported	Supported	Supported	Supported
	Policy-based routing to the label switched path (LSP)	Supported	Supported	Supported	Supported	Supported	Supported
	Forwarding table	Supported	Supported	Supported	Supported	Supported	Supported
	GRE tunnel	Supported	Supported	Supported	Supported	Supported	Supported
	IP packet fragments	Supported	Supported	Supported	Supported	Supported	Supported
	Mapping of the IP to the MPLS TTL	Supported	Supported	Supported	Supported	Supported	Supported
	Handling of Reserve labels	Supported	Supported	Supported	Supported	Supported	Supported
	POP, PUSH, SWAP	Supported	Supported	Supported	Supported	Supported	Supported
	LSP accounting	Supported	Supported	Supported	Supported	Supported	Supported
	Label Distribution Protocol (LDP)	Supported	Supported	Supported	Supported	Supported	Supported
	MTU signaling	Supported	Supported	Supported	Supported	Supported	Supported
	LDP MIB	Supported	Supported	Supported	Supported	Supported	Supported
	UP processing of LDP sessions	Supported	Supported	Supported	Supported	Supported	Supported
	DOWN processing of LDP sessions	Supported	Supported	Supported	Supported	Supported	Supported
	Multilink processing	Supported	Supported	Supported	Supported	Supported	Supported
	LSPM	Supported	Supported	Supported	Supported	Supported	Supported
	LSP	Supported	Supported	Supported	Supported	Supported	Supported
	LSR	Supported	Supported	Supported	Supported	Supported	Supported
	Cross-domain building	Supported	Supported	Supported	Supported	Supported	Supported
	MPLS Ping	Supported	Supported	Supported	Supported	Supported	Supported
	MPLS Tracereute	Supported	Supported	Supported	Supported	Supported	Supported
	L2TP access MPLS VPN	Supported	Supported	Supported	Supported	Supported	Supported
	IPSec access MPLS VPN	Supported	Supported	Supported	Supported	Supported	Supported
	IPSec VPN borne by MPLS	Supported	Supported	Supported	Supported	Supported	Supported
	MPLS VPN supported by GRE	Supported	Supported	Supported	Supported	Supported	Supported
	IPSec	Supported	Supported	Supported	Supported	Supported	Supported
	Number of IPSec VPN tunnels	64	64	2000	2000	4000	4000
	IPSec performance(site-to-site, client-to-site)	40 Mbit/s	50 Mbit/s	300 Mbit/s	500 Mbit/s	1 Gbit/s	2 Gbit/s
	Hardware encryption	Supported	Supported	Supported	Supported	Supported	Supported
	Number of IKE policies	64	64	100	100	100	100
	Number of IPSec policies	64	64	100	100	100	100
	Number of Security Associations (SAs)	128	128	4000	4000	8000	8000
	Implementation of IP security architecture	Supported	Supported	Supported	Supported	Supported	Supported
	Authentication Header (AH) Protocol	Supported	Supported	Supported	Supported	Supported	Supported
	Encapsulating Security Payload (ESP) Protocol	Supported	Supported	Supported	Supported	Supported	Supported
	AH and ESP Protocols	Supported	Supported	Supported	Supported	Supported	Supported
	Data Encryption Standard (DES) encryption	Supported	Supported	Supported	Supported	Supported	Supported
	Triple Data Encryption Standard (3DES) encryption	Supported	Supported	Supported	Supported	Supported	Supported
	Advanced Encryption Standard (AES) encryption algorithm	Supported	Supported	Supported	Supported	Supported	Supported
	AES-128 encryption algorithm	Supported	Supported	Supported	Supported	Supported	Supported
	AES-192 encryption algorithm	Supported	Supported	Supported	Supported	Supported	Supported
	AES-256 encryption algorithm	Supported	Supported	Supported	Supported	Supported	Supported
	ESP_NULL encryption	Supported	Supported	Supported	Supported	Supported	Supported
	HMAC-MD5-96 authentication algorithm	Supported	Supported	Supported	Supported	Supported	Supported
	HMAC-SHA1-96 authentication algorithm	Supported	Supported	Supported	Supported	Supported	Supported
	ESP non-authentication	Supported	Supported	Supported	Supported	Supported	Supported
	Manual establishment of SAs	Supported	Supported	Supported	Supported	Supported	Supported
	Establishment of SAs by using Internet Key Exchange (IKE) negotiation	Supported	Supported	Supported	Supported	Supported	Supported
	Transfer mode	Supported	Supported	Supported	Supported	Supported	Supported
	Tunnel mode	Supported	Supported	Supported	Supported	Supported	Supported
	Data flow classification	Supported	Supported	Supported	Supported	Supported	Supported
	Anti-replay	Supported	Supported	Supported	Supported	Supported	Supported
	Number of anti-replay windows	1024	1024	1024	1024	1024	1024
	Updating of SAs regularly	Supported	Supported	Supported	Supported	Supported	Supported
	Updating cycle	480-604,800s	480-604,800s	480-604,800s	480-604,800s	480-604,800s	480-604,800s
	Updating of SAs by consuming a certain amount of traffic	Supported	Supported	Supported	Supported	Supported	Supported
	Traffic	8000-4,194,303 KB	8000-4,194,303 KB	8000-4,194,303 KB	8000-4,194,303 KB	8000-4,194,303 KB	8000-4,194,303 KB
	Dynamic security policy	Supported	Supported	Supported	Supported	Supported	Supported
	Number of templates	100	100	2048	2048	2048	2048
	Dynamic random number mixing pool	Supported	Supported	Supported	Supported	Supported	Supported
	Manual security policy supports assignment of cipher key in character strings for the algorithm.	Supported	Supported	Supported	Supported	Supported	Supported
	Length of the character string	1–127	1–127	1–127	1–127	1–127	1–127

	Manual security policy supports assignment of cipher key in hexadecimal mode for the algorithm.	Supported	Supported	Supported	Supported	Supported	Supported
	Hexadecimal length (MD5)	16	16	16	16	16	16
	Hexadecimal length (SHA1)	20	20	20	20	20	20
	IPSec encryption for L2TP and GRE packets	Supported	Supported	Supported	Supported	Supported	Supported
	Tunnel nesting and implementation of the IPSEC processing to the nonlocal UDP 500/4500 packets	Supported	Supported	Supported	Supported	Supported	Supported
	Transparent NAT traversal of IPSec packets by using UDP packet encapsulation	Supported	Supported	Supported	Supported	Supported	Supported
	Fragment and reassembly	Supported	Supported	Supported	Supported	Supported	Supported
	IPSEC tunneling	Supported	Supported	Supported	Supported	Supported	Supported
	IKEv1	Supported	Supported	Supported	Supported	Supported	Supported
	Switch of aggressive mode	Supported	Supported	Supported	Supported	Supported	Supported
	Switch of main mode	Supported	Supported	Supported	Supported	Supported	Supported
	Switch of fast mode	Supported	Supported	Supported	Supported	Supported	Supported
	Diffie-Hellman (DH) switch	Supported	Supported	Supported	Supported	Supported	Supported
	Perfect forward secrecy (PFS) features	Supported	Supported	Supported	Supported	Supported	Supported
	Use of address range to configure and verify peer ID	Supported	Supported	Supported	Supported	Supported	Supported
	Information packets	Supported	Supported	Supported	Supported	Supported	Supported
	Dead peer detection (DPD)	Supported	Supported	Supported	Supported	Supported	Supported
	Heartbeat packets	Supported	Supported	Supported	Supported	Supported	Supported
	Regular updating of SAs	Supported	Supported	Supported	Supported	Supported	Supported
	Management of IPSEC SA by using the IKE	Supported	Supported	Supported	Supported	Supported	Supported
	IKE supporting DES encryption algorithm	Supported	Supported	Supported	Supported	Supported	Supported
	IKE supporting 3DES encryption algorithm	Supported	Supported	Supported	Supported	Supported	Supported
	IKE supporting AES encryption	Supported	Supported	Supported	Supported	Supported	Supported
	Default IKE security proposal	Supported	Supported	Supported	Supported	Supported	Supported
	NAT traversal of IPSec by using IKE negotiation	Supported	Supported	Supported	Supported	Supported	Supported
	Negotiation by means of the RAS encrypting the nonce	Supported	Supported	Supported	Supported	Supported	Supported
	Negotiation by means of certificate-based signature	Supported	Supported	Supported	Supported	Supported	Supported
	Negotiation by means of Pre-share Key	Supported	Supported	Supported	Supported	Supported	Supported
	Mode of RSA check word	Supported	Supported	Supported	Supported	Supported	Supported
	IKEv2	Supported	Supported	Supported	Supported	Supported	Supported
	DH switch	Supported	Supported	Supported	Supported	Supported	Supported
	PFS features	Supported	Supported	Supported	Supported	Supported	Supported
	INITIAL switch	Supported	Supported	Supported	Supported	Supported	Supported
	CREATE_CHILD_SA switch	Supported	Supported	Supported	Supported	Supported	Supported
	Switch of Information mode	Supported	Supported	Supported	Supported	Supported	Supported
	Repeated authentication	Supported	Supported	Supported	Supported	Supported	Supported
	DPD	Supported	Supported	Supported	Supported	Supported	Supported
	Traffic selectors support narrowing	Supported	Supported	Supported	Supported	Supported	Supported
	Rekey of IKE_SA and CHILD_SA.	Supported	Supported	Supported	Supported	Supported	Supported
	Stateless COOKIE-based anti-DOS protection	Supported	Supported	Supported	Supported	Supported	Supported
	Management of IPSEC SA by using IKEv2	Supported	Supported	Supported	Supported	Supported	Supported
	Integrity algorithm of MD5, SHA1, and AES-XCBC	Supported	Supported	Supported	Supported	Supported	Supported
	IKE supporting DES encryption algorithm	Supported	Supported	Supported	Supported	Supported	Supported
	IKE supporting 3DES encryption algorithm	Supported	Supported	Supported	Supported	Supported	Supported
	IKE supporting AES encryption algorithm	Supported	Supported	Supported	Supported	Supported	Supported
	NAT traversal of IPSec by using IKEv2 negotiation	Supported	Supported	Supported	Supported	Supported	Supported
	Negotiation by means of certificate-based signature	Supported	Supported	Supported	Supported	Supported	Supported
	Negotiation by means of Pre-share Key	Supported	Supported	Supported	Supported	Supported	Supported
	Extensible Authentication Protocol (EAP) authentication (as the NAS equipment)	Supported	Supported	Supported	Supported	Supported	Supported
	Public key infrastructure (PKI)	Supported	Supported	Supported	Supported	Supported	Supported
	Obtaining the CA certificate on line	Supported	Supported	Supported	Supported	Supported	Supported
	Registering certificates on line	Supported (SCEP)	Supported (SCEP)	Supported (SCEP)	Supported (SCEP)	Supported (SCEP)	Supported (SCEP)
	Certificate query	Supported	Supported	Supported	Supported	Supported	Supported
	Obtaining the certificate revocation list (CRL) on line	Supported (SECP, LDAP, HTTP)	Supported (SECP, LDAP, HTTP)	Supported (SECP, LDAP, HTTP)	Supported (SECP, LDAP, HTTP)	Supported (SECP, LDAP, HTTP)	Supported (SECP, LDAP, HTTP)
	Loading the certificate and CRL into the file system	Supported	Supported	Supported	Supported	Supported	Supported
	Providing certificate exchange when building IKE channels	Supported	Supported	Supported	Supported	Supported	Supported
	PKCS#7 encryption standard	Supported	Supported	Supported	Supported	Supported	Supported
	Registering certificates in the out-of-band mode	Supported	Supported	Supported	Supported	Supported	Supported
	Import of certificates and files	Supported	Supported	Supported	Supported	Supported	Supported
	X509 and X509V3 certificate standard	Supported	Supported	Supported	Supported	Supported	Supported
	Multi-level CA	Supported	Supported	Supported	Supported	Supported	Supported
	The certificate chain of peer end can be imported into the local certificate chain so that multiple chains appear during the certificate authentication.	Supported	Supported	Supported	Supported	Supported	Supported
	Cross-authentication	Supported	Supported	Supported	Supported	Supported	Supported
	Certificate backup name	Supported	Supported	Supported	Supported	Supported	Supported
	Certificate DN type	Supported	Supported	Supported	Supported	Supported	Supported
	CA server	Supported	Only support X509 certificate server.	Only support X509 certificate server.	Only support X509 certificate server.	Only support X509 certificate server.	Only support X509 certificate server.
	Number of domains supported	5	5	5	5	5	5
	Maximum number of local certificates supported	5	5	5	5	5	5
	Maximum number of CA certificates supported	32	32	32	32	32	32
	Maximum number of CRLs supported	32	32	32	32	32	32
	Authentication type supported by the Lightweight Directory Access Protocol (LDAP)	Supported	Supported	Supported	Supported	Supported	Supported
	Frequency of automatic CRL updating	Supported	Supported	Supported	Supported	Supported	Supported
	Pending interval for certificate registration	Supported	Supported	Supported	Supported	Supported	Supported
	Times of continuous pending	Supported	Supported	Supported	Supported	Supported	Supported
	Online Certificate Status Protocol (OCSP)	Supported	Supported	Supported	Supported	Supported	Supported
	Lightweight Directory Access Protocol (LDAP)	Supported	Supported	Supported	Supported	Supported	Supported
	Simple Certificate Enrollment Protocol (SCEP)	Supported	Supported	Supported	Supported	Supported	Supported
	Number of simultaneously registering certificates supported	2	2	2	2	2	2
	Automatic updating of SCEP real certificates	Supported	Supported	Supported	Supported	Supported	Supported
	PKI dual-system hot backup	Supported	Supported	Supported	Supported	Supported	Supported
	Real-time backup	Supported	Supported	Supported	Supported	Supported	Supported
	Batch backup	Supported	Supported	Supported	Supported	Supported	Supported
	Secure Sockets Layer (SSL)	Supported	Supported	Supported	Supported	Supported	Supported
	Number of SSL VPN users	20	50	100	100	150	200
	SSL VPN performance	5 Mbps	5 Mbps	10 Mbps	10 Mbps	10 Mbps	10 Mbps
	TLS1.0	Supported	Supported	Supported	Supported	Supported	Supported
	TLS1.0 + SSL3.0	Supported	Supported	Supported	Supported	Supported	Supported
	TLS1.0 + SSL3.0 + SSL2.0	Supported	Supported	Supported	Supported	Supported	Supported
	DES/3DES	Supported	Supported	Supported	Supported	Supported	Supported
	AES	Supported	Supported	Supported	Supported	Supported	Supported
	Length of AES key	128/256	128/256	128/256	128/256	128/256	128/256
	Rivest Cipher 4 (RC4)	Supported	Supported	Supported	Supported	Supported	Supported
	Length of RC4 key	128	128	128	128	128	128
	Configurable session aging time	1–1440 min. Or it can be set as never aging.	1–1440 min. Or it can be set as never aging.	1–1440 min. Or it can be set as never aging.	1–1440 min. Or it can be set as never aging.	1–1440 min. Or it can be set as never aging.	1–1440 min. Or it can be set as never aging.
	Configurable life cycle	60–2880 min. Or it can be set as never overdue.	60–2880 min. Or it can be set as never overdue.	60–2880 min. Or it can be set as never overdue.	60–2880 min. Or it can be set as never overdue.	60–2880 min. Or it can be set as never overdue.	60–2880 min. Or it can be set as never overdue.
	New SSL VPN users per second (person/second)	2	2	2	2	2	2
	New SSL connections per second (time/second)	5	5	5	5	5	5
	Maximum number of the policy rules that can be defined by SSL VPN users (piece)	Maximum number of user policies and user group policies configured by a virtual gateway: 16 Number of various policies made effective by a user: 16 Maximum number of virtual gateway source IP policies configured by a virtual gateway: 256	Maximum number of user policies and user group policies configured by a virtual gateway: 16 Number of various policies made effective by a user: 16 Maximum number of virtual gateway source IP policies configured by a virtual gateway: 256	Maximum number of user policies and user group policies configured by a virtual gateway: 16 Number of various policies made effective by a user: 16 Maximum number of virtual gateway source IP policies configured by a virtual gateway: 256	Maximum number of user policies and user group policies configured by a virtual gateway: 16 Number of various policies made effective by a user: 16 Maximum number of virtual gateway source IP policies configured by a virtual gateway: 256	Maximum number of user policies and user group policies configured by a virtual gateway: 16 Number of various policies made effective by a user: 16 Maximum number of virtual gateway source IP policies configured by a virtual gateway: 256	Maximum number of user policies and user group policies configured by a virtual gateway: 16 Number of various policies made effective by a user: 16 Maximum number of virtual gateway source IP policies configured by a virtual gateway: 256
	Maximum provision of virtual gateway (piece)	4	4	4	4	4	4
	Maximum number of SSL VPN resource items (item)	1024	1024	1024	1024	1024	1024
	Number of manageable SSL VPN VPNDB users (person)	1000	1000	1000	1000	1000	1000
	Number of groups for the SSL VPN single virtual gateway (group)	64	64	64	64	64	64
	Explorer type						
	Internet Explorer	Supported. IE 5.5 version and later ones	Supported. IE 5.5 version and later ones	Supported. IE 5.5 version and later ones	Supported. IE 5.5 version and later ones	Supported. IE 5.5 version and later ones	Supported. IE 5.5 version and later ones

	Maxthon Browser	Supported. Maxthon1.6.3 version and later ones	Supported. Maxthon1.6.3 version and later ones	Supported. Maxthon1.6.3 version and later ones	Supported. Maxthon1.6.3 version and later ones	Supported. Maxthon1.6.3 version and later ones	Supported. Maxthon1.6.3 version and later ones
	Firefox Browser	Supported. Versions between Firefox 3.0 and Firefox 4.0	Supported. Versions between Firefox 3.0 and Firefox 4.0	Supported. Versions between Firefox 3.0 and Firefox 4.0	Supported. Versions between Firefox 3.0 and Firefox 4.0	Supported. Versions between Firefox 3.0 and Firefox 4.0	Supported. Versions between Firefox 3.0 and Firefox 4.0
	System type						
	Windows2000 Professional (32 bits)	Supported	Supported	Supported	Supported	Supported	Supported
	Windows server 2000 (32 bits)	Supported	Supported	Supported	Supported	Supported	Supported
	Windows server 2003 (32 bits)	Supported	Supported	Supported	Supported	Supported	Supported
	Windows XP (32 bits)	Supported	Supported	Supported	Supported	Supported	Supported
	Windows vista (32 bits)	Supported	Supported	Supported	Supported	Supported	Supported
	Windows 7 (32 bits)	Supported	Supported	Supported	Supported	Supported	Supported
	Windows server 2008 (32 bits)	Supported	Supported	Supported	Supported	Supported	Supported
	WEB proxy	Supported	Supported	Supported	Supported	Supported	Supported
	HTTP web proxy	Supported	Supported	Supported	Supported	Supported	Supported
	HTTPS web proxy	Supported	Supported	Supported	Supported	Supported	Supported
	Access by using the proxy server	Supported	Supported	Supported	Supported	Supported	Supported
	File sharing	Supported	Supported	Supported	Supported	Supported	Supported
	CIFS/SMB	Supported	Supported	Supported	Supported	Supported	Supported
	File Server of windows operating system	Supported (Only support Server Message Block (SMB))	Supported (Only support SMB)	Supported (Only support SMB)	Supported (Only support SMB)	Supported (Only support SMB)	Supported (Only support SMB)
	NTLM0.12 dialect	Supported (Only support SMB)	Supported (Only support SMB)	Supported (Only support SMB)	Supported (Only support SMB)	Supported (Only support SMB)	Supported (Only support SMB)
	Network file system (NFS)	Supported	Supported	Supported	Supported	Supported	Supported
	NFSV3	Supported	Supported	Supported	Supported	Supported	Supported
	UID and GID verification of Unix	Supported	Supported	Supported	Supported	Supported	Supported
	NFS v3: UDP-based NFS file sharing	Supported	Supported	Supported	Supported	Supported	Supported
	Portmap V2 mapping of the NFS interface	Supported	Supported	Supported	Supported	Supported	Supported
	NFS bearing the protocol RPC V2	Supported	Supported	Supported	Supported	Supported	Supported
	Read and write control permission	Supported	Supported	Supported	Supported	Supported	Supported
	Interface forwarding	Supported	Supported	Supported	Supported	Supported	Supported
	Application based on the Transmission Control Protocol (TCP)	Supported	Supported	Supported	Supported	Supported	Supported
	Telnet	Supported	Supported	Supported	Supported	Supported	Supported
	Microsoft remote desktop	Supported	Supported	Supported	Supported	Supported	Supported
	Secure shell protocol (SSH)	Supported	Supported	Supported	Supported	Supported	Supported
	Virtual Network Computing (VNC)	Supported	Supported	Supported	Supported	Supported	Supported
	Notes application	Supported	Supported	Supported	Supported	Supported	Supported
	Outlook e-mail application	Supported	Supported	Supported	Supported	Supported	Supported
	Passive mode of FTP	Supported	Supported	Supported	Supported	Supported	Supported
	Oracle	Supported	Supported	Supported	Supported	Supported	Supported
	Access by using the proxy server	Supported	Supported	Supported	Supported	Supported	Supported
	Network expansion	Supported	Supported	Supported	Supported	Supported	Supported
	Point-to-point communication in the network extension	Supported	Supported	Supported	Supported	Supported	Supported
	Distribution of the designated virtual addresses to users	Supported	Supported	Supported	Supported	Supported	Supported
	Bidirectional NAT translation with the Intranet server	Supported	Supported	Supported	Supported	Supported	Supported
	Access control based on the destination IP and PORT	Supported	Supported	Supported	Supported	Supported	Supported
	Virtual gateway	Supported	Supported	Supported	Supported	Supported	Supported
	Security features	Supported	Supported	Supported	Supported	Supported	Supported
	VPND8 authentication and authorization	Supported	Supported	Supported	Supported	Supported	Supported
	Password change by users	Supported	Supported	Supported	Supported	Supported	Supported
	Reminder for regular password change	Supported	Supported	Supported	Supported	Supported	Supported
	Setting of password strength	Supported	Supported	Supported	Supported	Supported	Supported
	Setting of requiring changing the password for the first login	Supported	Supported	Supported	Supported	Supported	Supported
	Public account	Supported	Supported	Supported	Supported	Supported	Supported
	RADIUS authentication and authorization	Supported	Supported	Supported	Supported	Supported	Supported
	RADIUS authentication supporting PAP mode	Supported	Supported	Supported	Supported	Supported	Supported
	Configuration of the timeout, number of retransmissions, server address, port, and key	Supported	Supported	Supported	Supported	Supported	Supported
	Under the same virtual gateway, the same authentication mode supports configuring a main server and a standby one.	Supported	Supported	Supported	Supported	Supported	Supported
	LDAP authentication and authorization	Supported	Supported	Supported	Supported	Supported	Supported
	Plaintext authentication of LDAP protocol	Supported	Supported	Supported	Supported	Supported	Supported
	Configuration of the server address port, BaseDN, filter, and the DN and password of the administrator	Supported	Supported	Supported	Supported	Supported	Supported
	Under the same virtual gateway, the same authentication mode supports configuring a main server and a standby one.	Supported	Supported	Supported	Supported	Supported	Supported
	x.509 digital certificate authentication	Supported	Supported	Supported	Supported	Supported	Supported
	Anonymous authentication of certificates	Supported	Supported	Supported	Supported	Supported	Supported
	Challenge authentication of certificates	Supported	Supported	Supported	Supported	Supported	Supported
	Verification of client certificates	Supported	Supported	Supported	Supported	Supported	Supported
	Maximum number of the CA certificates supported by the system	40	40	40	40	40	40
	Check mode for the client certificate status – CRL	Supported	Supported	Supported	Supported	Supported	Supported
	The way to obtain CRL distribution point (CDP) – from CA certificates	Supported	Supported	Supported	Supported	Supported	Supported
	The way to obtain CDP– from client certificates	Supported	Supported	Supported	Supported	Supported	Supported
	The way to obtain CDP–manual configuration	Supported	Supported	Supported	Supported	Supported	Supported
	The way to obtain CDP–not obtain	Supported	Supported	Supported	Supported	Supported	Supported
	Download of CRL by using web	Supported	Supported	Supported	Supported	Supported	Supported
	Download of CRL by using LDAP	Supported	Supported	Supported	Supported	Supported	Supported
	Manual download of CRL	Supported	Supported	Supported	Supported	Supported	Supported
	Regular download of CRL	Supported	Supported	Supported	Supported	Supported	Supported
	Limitation on the CRL file size	Less than 50KB	Less than 50KB	Less than 50KB	Less than 50KB	Less than 50KB	Less than 50KB
	Limitation on the number of the CRL file	Support 40 CRL files to the maximum.	Support 40 CRL files to the maximum.	Support 40 CRL files to the maximum.	Support 40 CRL files to the maximum.	Support 40 CRL files to the maximum.	Support 40 CRL files to the maximum.
	Limitation on the size of a certificate	Not more than 3072B	Not more than 3072B	Not more than 3072B	Not more than 3072B	Not more than 3072B	Not more than 3072B
	Import of single certificate files	Supported	Supported	Supported	Supported	Supported	Supported
	Import of certificate chain files	Supported	Supported	Supported	Supported	Supported	Supported
	Levels of certificate chains	<=10 levels	<=10 levels	<=10 levels	<=10 levels	<=10 levels	<=10 levels
	Manual import of equipment certificate	Supported	Supported	Supported	Supported	Supported	Supported
	Import of the certificate for the issuer of equipment certificate	Supported	Supported	Supported	Supported	Supported	Supported
	Filtering certificates according to effective start and end dates and issuers	Supported	Supported	Supported	Supported	Supported	Supported
	USBKEY + digital certificate	Supported	Supported	Supported	Supported	Supported	Supported
	Hierarchical authentication and authorization	Supported, Three levels to the maximum	Supported, Three levels to the maximum	Supported, Three levels to the maximum	Supported; A maximum of three levels	Supported; A maximum of three levels	Supported; A maximum of three levels
	Public account	Supported	Supported	Supported	Supported	Supported	Supported
	Access control	Supported	Supported	Supported	Supported	Supported	Supported
	Based on the source address	Supported	Supported	Supported	Supported	Supported	Supported
	Based on the destination IP address and interface	Supported	Supported	Supported	Supported	Supported	Supported
	URL control	Supported	Supported	Supported	Supported	Supported	Supported
	Automatic sequencing of the policy rules of the same nature	Supported	Supported	Supported	Supported	Supported	Supported
Authentication, Authorization and Accounting (AAA)		Supported	Supported	Supported	Supported	Supported	Supported
	Authentication functions						
	Local authentication	Supported	Supported	Supported	Supported	Supported	Supported
	Password change by users	Supported	Supported	Supported	Supported	Supported	Supported
	Setting of password strength	Supported	Supported	Supported	Supported	Supported	Supported
	Setting of requiring changing the password for the first login	Supported	Supported	Supported	Supported	Supported	Supported
	RADIUS authentication	Supported	Supported	Supported	Supported	Supported	Supported
	Standard RADIUS protocol	Supported	Supported	Supported	Supported	Supported	Supported
	RADIUS + 1.1 protocol	Supported	Supported	Supported	Supported	Supported	Supported
	Huawei extended RADIUS protocol	Supported	Supported	Supported	Supported	Supported	Supported
	Huawei RADIUS + protocol V.1.1	Supported	Supported	Supported	Supported	Supported	Supported
	CHAP mode	Supported	Supported	Supported	Supported	Supported	Supported
	PAP mode	Support part of the mode and only support shiva.	Support part of the mode and only support shiva.	Support part of the mode and only support shiva.	Support part of the mode and only support shiva.	Support part of the mode and only support shiva.	Support part of the mode and only support shiva.
	RADIUS authentication and authorization, and access challenge	Support part of them and only support radius authorization.	Support part of them and only support radius authorization.	Support part of them and only support radius authorization.	Support part of them and only support radius authorization.	Support part of them and only support radius authorization.	Support part of them and only support radius authorization.
	Configuration of the timeout, number of retransmissions, server address, port, and key	Supported	Supported	Supported	Supported	Supported	Supported
	HWTACACS authentication	Supported	Supported	Supported	Supported	Supported	Supported
	LDAP authentication	Supported	Supported	Supported	Supported	Supported	Supported
	Plaintext authentication of LDAP protocol	Supported	Supported	Supported	Supported	Supported	Supported
	Configuration of the server address port, BaseDN, filter, and the DN and password of the administrator	Supported	Supported	Supported	Supported	Supported	Supported
	AD authentication	Supported	Supported	Supported	Supported	Supported	Supported
	Kerberos-based authentication	Supported	Supported	Supported	Supported	Supported	Supported
	Password change by Kerberos-based users	Supported	Supported	Supported	Supported	Supported	Supported

	Authentication of x.509 digital certificates	Supported	Supported	Supported	Supported	Supported	Supported
	Online Certificate Status Protocol (OCSP)	Supported	Supported	Supported	Supported	Supported	Supported
	CRL	Supported	Supported	Supported	Supported	Supported	Supported
	Manual import of certificates	Supported	Supported	Supported	Supported	Supported	Supported
	Multilevel certificate chain	Supported	Supported	Supported	Supported	Supported	Supported
	Authentication management	Supported	Supported	Supported	Supported	Supported	Supported
	Authorization functions					Supported	Supported
	Local authorization	Supported	Supported	Supported	Supported	Supported	Supported
	HWTACACS authorization	Supported	Supported	Supported	Supported	Supported	Supported
	Authorization after being authenticated on the RADIUS server	Supported	Supported	Supported	Supported	Supported	Supported
	Authorization plan management	Supported	Supported	Supported	Supported	Supported	Supported
	Charging functions	Supported	Supported	Supported	Supported	Supported	Supported
	Remote accounting in RADIUS mode	Supported	Supported	Supported	Supported	Supported	Supported
	Remote accounting in HWTACACS mode	Supported	Supported	Supported	Supported	Supported	Supported
User management		Supported	Supported	Supported	Supported	Supported	Supported
	Local user management	Supported	Supported	Supported	Supported	Supported	Supported
	Online user management	Supported	Supported	Supported	Supported	Supported	Supported
	Maximum number of users	500	500	2,000	2,000	6,000	6,000
	Maximum number of user groups	50	50	200	200	600	600
	Maximum subordination layers of users	7	7	7	7	7	7
	Number of user groups to which a single user belongs	3	3	3	3	3	3
	Duplication of user group name	Supported	Supported	Supported	Supported	Supported	Supported
	Creating, deleting, and modifying users or user groups locally	Supported	Supported	Supported	Supported	Supported	Supported
	Description about configuration of users and user groups	Supported	Supported	Supported	Supported	Supported	Supported
	Import of the information about users and user groups from the remote authentication server	Supported	Supported	Supported	Supported	Supported	Supported
	Import of the information about users and user groups from the remote authentication server needs a supporting organization.	Supported	Supported	Supported	Supported	Supported	Supported
	Management on the validity duration of the local users	Supported	Supported	Supported	Supported	Supported	Supported
	Static configuration of user status	Supported	Supported	Supported	Supported	Supported	Supported
	Password change by users	Supported	Supported	Supported	Supported	Supported	Supported
	Import and export functions of users and user groups	Supported	Supported	Supported	Supported	Supported	Supported
	Dual-system hot backup and switchover of information about users and user groups	Supported	Supported	Supported	Supported	Supported	Supported
	Online check of user information	Supported	Supported	Supported	Supported	Supported	Supported
	Management operation on the online users by administrator	Supported	Supported	Supported	Supported	Supported	Supported
File Transfer Protocol (FTP) filtering		Not Supported	Not Supported	Supported	Supported	Supported	Supported
	Supported modes			Supported	Supported	Supported	Supported
	FTP active mode			Supported	Supported	Supported	Supported
	FTP passive mode			Supported	Supported	Supported	Supported
	FTP command filtering			Supported	Supported	Supported	Supported
	FTP PUT command filtering			Supported	Supported	Supported	Supported
	FTP GET command filtering			Supported	Supported	Supported	Supported
	FTP Delete command filtering			Supported	Supported	Supported	Supported
	FTP file filtering			Supported	Supported	Supported	Supported
	Filtering based on the names of uploading and downloading files			Supported	Supported	Supported	Supported
	Filtering based on the suffix of uploading and downloading files			Supported	Supported	Supported	Supported
	File size filtering			Supported	Supported	Supported	Supported
Secure shell protocol (SSH)							
	SSH1.5 protocol	Supported	Supported	Supported	Supported	Supported	Supported
	SSH2.0 protocol	Supported	Supported	Supported	Supported	Supported	Supported
	SSH2 Server	Supported	Supported	Supported	Supported	Supported	Supported
	Different encryption algorithms can be used for entering and exiting the SSH2 server.	Supported	Supported	Supported	Supported	Supported	Supported
	Different Mac algorithms can be used for entering and exiting the SSH2 server.	Supported	Supported	Supported	Supported	Supported	Supported
	SSH2 server supporting 3DES-CBC, DES, and AES128 encryption algorithm negotiation	Supported	Supported	Supported	Supported	Supported	Supported
	SSH2 server supporting hmac-sha1 verification algorithm negotiation	Supported	Supported	Supported	Supported	Supported	Supported
	SSH2 server supporting diffie-hellman-group1-sha1 Diffie-Hellman negotiation	Supported	Supported	Supported	Supported	Supported	Supported
	SSH2 server supporting Key Re-Exchange	Supported	Supported	Supported	Supported	Supported	Supported
	SSH2 server supporting Password	Supported	Supported	Supported	Supported	Supported	Supported
	SSH2 server supporting RSA verification	Supported	Supported	Supported	Supported	Supported	Supported
	SSH2 server supporting the processing of IPv6 connections	Supported	Supported	Supported	Supported	Supported	Supported
	Enabling and disabling of the SSH TELNET server functions	Supported	Supported	Supported	Supported	Supported	Supported
	Enabling and disabling of the SFTP server functions	Supported	Supported	Supported	Supported	Supported	Supported
	Setting of the default directory for users to access SFTP	Supported	Supported	Supported	Supported	Supported	Supported
	SSH server supporting the listening of the interface number	Supported	Supported	Supported	Supported	Supported	Supported
	SSH2 server timeout detection	Supported	Supported	Supported	Supported	Supported	Supported
	SFTP service subsystem supporting the file uploading	Supported	Supported	Supported	Supported	Supported	Supported
	SFTP service subsystem supporting the file downloading	Supported	Supported	Supported	Supported	Supported	Supported
	SFTP service subsystem supporting the change of file names	Supported	Supported	Supported	Supported	Supported	Supported
	SFTP service subsystem supporting file deletion	Supported	Supported	Supported	Supported	Supported	Supported
	SFTP service subsystem supporting building new directories	Supported	Supported	Supported	Supported	Supported	Supported
	SFTP service subsystem supporting deleting directories	Supported	Supported	Supported	Supported	Supported	Supported
	SFTP service subsystem supporting changing the operation path	Supported	Supported	Supported	Supported	Supported	Supported
	SFTP service subsystem supporting displaying the file list under the designated directory.	Supported	Supported	Supported	Supported	Supported	Supported
	SFTP service subsystem supporting displaying the current working directory of the user.	Supported	Supported	Supported	Supported	Supported	Supported
	Maximum number of the users supported by the SSH2 FTP server	5	5	5	5	5	5
	Maximum number of the users supported by the SSH2 TELNET server	15	15	15	15	15	15
	SSH2 FTP server and SSH2 TELNET server supporting 15 users to the maximum	15	15	15	15	15	15
	Rate of SFTP uploading and downloading reaching 30% of that of the FTP	Supported	Supported	Supported	Supported	Supported	Supported
	The SSH server port number can be configured as 22 and 1025-55535.	Supported	Supported	Supported	Supported	Supported	Supported
	Maximum number of SSH users supported by the SSH server	200	200	200	200	200	200
	Providing the command to debug and diagnose the SSH state machine (providing different switches for different users and configuration parameters.)	Supported	Supported	Supported	Supported	Supported	Supported
	SSH key information and abnormal log information	Supported	Supported	Supported	Supported	Supported	Supported
	Providing command to query the users who log in to the SSH server	Supported	Supported	Supported	Supported	Supported	Supported
	Providing command to query the users who configure the SSH server	Supported	Supported	Supported	Supported	Supported	Supported
	Providing command to query SSH server information	Supported	Supported	Supported	Supported	Supported	Supported
	SSH Client	Supported	Supported	Supported	Supported	Supported	Supported
	First authentication of the SSH2 client	Supported	Supported	Supported	Supported	Supported	Supported
	Basic functions of the SSH2 Telnet client	Supported	Supported	Supported	Supported	Supported	Supported
	Different encryption algorithms can be used for entering and exiting the SSH2 Telnet client.	Supported	Supported	Supported	Supported	Supported	Supported
	Different Mac algorithms can be used for entering and exiting the SSH2 Telnet client.	Supported	Supported	Supported	Supported	Supported	Supported
	SSH2 Telnet client suppoting diffie-hellman-group1-sha1 Diffie-Hellman negotiation	Supported	Supported	Supported	Supported	Supported	Supported
	SSH2 Telnet client suppoting Key Re-Exchange	Supported	Supported	Supported	Supported	Supported	Supported
	SSH2 Telnet client suppoting 3DES-CBC, DES, and AES128 encryption algorithm negotiation	Supported	Supported	Supported	Supported	Supported	Supported
	SSH2 Telnet client suppoting hmac-sha1 verification algorithm negotiation.	Supported	Supported	Supported	Supported	Supported	Supported

	SSH2 Telnet client supporting Public key and Password.	Supported	Supported	Supported	Supported	Supported	Supported
	SSH2 Telnet client supporting the designated source IP address.	Supported	Supported	Supported	Supported	Supported	Supported
	SSH2 Telnet client supporting the access to private networks.	Supported	Supported	Supported	Supported	Supported	Supported
	SSH2 Telnet client supporting the access of other interfaces numbers.	Supported	Supported	Supported	Supported	Supported	Supported
	SSH2 Telnet client supporting the processing of the IPv6 address.	Supported	Supported	Supported	Supported	Supported	Supported
	Basic functions of the SFTP client	Supported	Supported	Supported	Supported	Supported	Supported
	Different encryption algorithms can be used for entering and exiting the SFTP client.	Supported	Supported	Supported	Supported	Supported	Supported
	Different Mac algorithms can be used for entering and exiting the SFTP client.	Supported	Supported	Supported	Supported	Supported	Supported
	SFTP client supporting diffie-hellman-group1-sha1 Diffie-Hellman negotiation	Supported	Supported	Supported	Supported	Supported	Supported
	SFTP client supporting Key Re-Exchange	Supported	Supported	Supported	Supported	Supported	Supported
	SFTP client supporting 3DES-CBC, DES, and AES128 encryption algorithm negotiation	Supported	Supported	Supported	Supported	Supported	Supported
	SFTP client supporting hmac-sha1 verification algorithm negotiation	Supported	Supported	Supported	Supported	Supported	Supported
	SFTP client supporting Public key and Password	Supported	Supported	Supported	Supported	Supported	Supported
	SFTP client supporting the designated source IP address	Supported	Supported	Supported	Supported	Supported	Supported
	SFTP client supporting the access to private networks	Supported	Supported	Supported	Supported	Supported	Supported
	SFTP client supporting the access of other interfaces numbers	Supported	Supported	Supported	Supported	Supported	Supported
	SFTP client supporting the processing of the IPv6 address	Supported	Supported	Supported	Supported	Supported	Supported
	SFTP client supporting the file uploading	Supported	Supported	Supported	Supported	Supported	Supported
	SFTP client supporting the file downloading	Supported	Supported	Supported	Supported	Supported	Supported
	SFTP client supporting the change of file names	Supported	Supported	Supported	Supported	Supported	Supported
	SFTP client supporting file deletion	Supported	Supported	Supported	Supported	Supported	Supported
	SFTP client supporting building new directories	Supported	Supported	Supported	Supported	Supported	Supported
	SFTP client supporting deleting directories	Supported	Supported	Supported	Supported	Supported	Supported
	SFTP client supporting changing the operation path	Supported	Supported	Supported	Supported	Supported	Supported
	SFTP client supporting displaying the file list under the designated directory	Supported	Supported	Supported	Supported	Supported	Supported
	SFTP client supports displaying the current working directory of the user.	Supported	Supported	Supported	Supported	Supported	Supported
	SSH2 TELNET client port number can be configured as 22 and 1025–55535.	Supported	Supported	Supported	Supported	Supported	Supported
	SFTP client port number can be configured as 22 and 1025–55535.	Supported	Supported	Supported	Supported	Supported	Supported
	Twenty servers can be bound to the SSH client to the maximum.	20	20	20	20	20	20
	Command to query the information of the server related to the SSH client	Supported	Supported	Supported	Supported	Supported	Supported
	Interworking with ME, H3COM, and Cisco products	Supported	Supported	Supported	Supported	Supported	Supported
	RSA algorithm	Supported	Supported	Supported	Supported	Supported	Supported
	Length of the RSA key pair	512-2048 bits	512-2048 bits	512-2048 bits	512-2048 bits	512-2048 bits	512-2048 bits
IDS cooperation		Only support NIP at present.	Only support NIP at present.	Only support NIP at present.	Only support NIP at present.	Only support NIP at present.	Only support NIP at present.
License		Supported	Supported	Supported	Supported	Supported	Supported
	Control of the number of virtual firewalls by using the License	Supported	Supported	Supported	Supported	Supported	Supported
	Control of the number of SSL VPN concurrent users by using the License	Supported	Supported	Supported	Supported	Supported	Supported
	Control of the IPS update services by using the License	Supported	Supported	Supported	Supported	Supported	Supported
	Control of the AV update services by using the License	Supported	Supported	Supported	Supported	Supported	Supported
	Control of the anti-spam update services by using the License	Supported	Supported	Supported	Supported	Supported	Supported
	Control of the URL filtering update services by using the License	Supported	Supported	Supported	Supported	Supported	Supported
	Control of the UTM function update services by using the License	Supported	Supported	Supported	Supported	Supported	Supported

Primary Specification	Secondary Specification	USG2110F/FW/AW/AGW V300R001	USG2160/W V300R001	USG2230 V300R001	USG2260 V300R001	USG5120 V300R001	USG5150 V300R001	Remarks
Network								
Link layer protocol								
	ETHERNET	Support	Support	Support	Support	Support	Support	
	Virtual Local Area Network (VLAN)	Support	Support	Support	Support	Support	Support	
	802.1Q	Support	Support	Support	Support	Support	Support	
	Number of VLANs supported	15	15	4094	4094	4094	4094	
	Configurable scope of VLAN ID	1–4094	1–4094	1–4094	1–4094	1–4094	1–4094	
	STP/MSTP/RSTP	Support	Support	Support	Support	Support	Support	
	Point-to-Point Protocol (PPP)	Support	Support	Support	Support	Support	Support	
	Point-to-Point Protocol over Ethernet (PPPoE)	Support	Support	Support	Support	Support	Support	
	PPPoE Server	Support	Support	Support	Support	Support	Support	
	Maximum connections	256	256	2048	2048	2048	2048	
	PPPOE Client	Support	Support	Support	Support	Support	Support	
	Address Resolution Protocol (ARP)	Support	Support	Support	Support	Support	Support	
	Static ARP	Support	Support	Support	Support	Support	Support	
	Number of static ARPs	256	256	2000	2000	2000	2000	
	Dynamic ARP	Support	Support	Support	Support	Support	Support	
	Number of dynamic learning ARPs	512	512	Overall unit: 64K. Each interface: 4K.	Overall unit: 64K. Each interface: 4K.	Overall unit: 64K. Each interface: 4K.	Overall unit: 64K. Each interface: 4K.	
	ARP proxy	Support	Support	Support	Support	Support	Support	
	ARP aging time	Default: 20 minutes. Configurable scope: 60–1200s	Default: 20 minutes. Configurable scope: 60–1200s	Default: 20 minutes. Configurable scope: 60–1200s	Default: 20 minutes. Configurable scope: 60–1200s	Default: 20 minutes. Configurable scope: 60–1200s	Default: 20 minutes. Configurable scope: 60–1200s	
	Gratuitous ARP	Support	Support	Support	Support	Support	Support	
	Strom control	Support	Support	Support	Support	Support	Support	
	Unicast storm control	Support	Support	Support	Support	Support	Support	
	Broadcast storm control	Support	Support	Support	Support	Support	Support	
	Multicast storm control	Support	Support	Support	Support	Support	Support	
	Link Aggregation Control Protocol (LACP)	Not support	Not support	Support	Support	Support	Support	
	Static LACP	Not support	Not support	Support	Support	Support	Support	
	Link Layer Discovery Protocol (LLDP)	Support	Support	Support	Support	Support	Support	
	Data Communication Channel (DCC)	Support	Support	Support	Support	Support	Support	
	Rotating DCC	Support	Support	Support	Support	Support	Support	
	Number of Tunnel interfaces	256	256	256	256	256	256	
	Number of Dialer interfaces	64	1024	1024	1024	1024	1024	
	Number of VT interfaces	64	1024	1024	1024	1024	1024	
	Number of Loopback interfaces	64	1024	1024	1024	1024	1024	
	Total number of the interfaces (including the physical interfaces and the logical interfaces)	1024	2048	2048	2048	2048	2048	
Port binding								
	Eth-Trunk	Support	Support	Support	Support	Support	Support	
	Number of Eth-Trunk interfaces	16	16	64	64	64	64	
	Number of members supported by each Eth-Trunk interface	8	8	8	8	8	8	
	Eth-Trunk interface can be bound to various ports and can balance the traffic according to the weight of the Trunk member.	Support	Support	Support	Support	Support	Support	
	Eth-Trunk balance the load of the unicast packet.	Support	Support	Support	Support	Support	Support	
	Eth-Trunk balance the load of the multicast packet.	Support	Support	Support	Support	Support	Support	
Network layer protocol								
	IP forwarding	Support	Support	Support	Support	Support	Support	
	Number of fragments for a single packet during caching	8	8	32	32	32	32	
	Fragment reassembly timeout	30s	30s	Default: 5s. Configurable scope: 1–40,000s.	Default: 5s. Configurable scope: 1–40,000s.	Default: 5s. Configurable scope: 1–40,000s.	Default: 5s. Configurable scope: 1–40,000s.	
	Fragment reassembly queue length	1000	1000	1000	1000	1000	1000	
	Number of the fragment reassembly queues	400	400	400	400	400	400	
	Primary and secondary addresses number of the interfaces	Primary address: 1. Secondary address: 31.	Primary address: 1. Secondary address: 31.	Primary address: 1. Secondary address: 31.	Primary address: 1. Secondary address: 31.	Primary address: 1. Secondary address: 31.	Primary address: 1. Secondary address: 31.	
	IP options	Support	Support	Support	Support	Support	Support	
	Strict source record route	Support	Support	Support	Support	Support	Support	
	Loose source record route	Support	Support	Support	Support	Support	Support	
	Time stamp	Support	Support	Support	Support	Support	Support	
	Route Alert options	Support	Support	Support	Support	Support	Support	
	Option length	Maximum: 40 bytes	Maximum: 40 bytes	Maximum: 40 bytes	Maximum: 40 bytes	Maximum: 40 bytes	Maximum: 40 bytes	
	Internet Control Messages Protocol (ICMP) protocol	Support	Support	Support	Support	Support	Support	
	TRACERT	Support	Support	Support	Support	Support	Support	
	FIB table	Support	Support	Support	Support	Support	Support	
	Transmission Control Protocol (TCP)	Support	Support	Support	Support	Support	Support	
	User Datagram Protocol (UDP)	Support	Support	Support	Support	Support	Support	
	SOCKET	Support	Support	Support	Support	Support	Support	
	PING	Support	Support	Support	Support	Support	Support	
	ARP	Support	Support	Support	Support	Support	Support	
	IP address unnumbered	Support	Support	Support	Support	Support	Support	
	Interface for PPP encapsulation uses IP address unnumbered	Support	Support	Support	Support	Support	Support	
	Interface for HDLC encapsulation uses IP address unnumbered	Support	Support	Support	Support	Support	Support	
	Interface for Tunnel uses IP address unnumbered	Support	Support	Support	Support	Support	Support	
	Interface for Virtual Template uses IP address unnumbered	Support	Support	Support	Support	Support	Support	
	Dynamic host configuration protocol (DHCP)	Support	Support	Support	Support	Support	Support	
	DHCP SERVER	Support	Support	Support	Support	Support	Support	
	Global address pool	Support	Support	Support	Support	Support	Support	
	Interface binding IP+MAC	Support	Support	Support	Support	Support	Support	
	Forbidden entry	Support	Support	Support	Support	Support	Support	
	Number of IP leases	1024	1024	8*1024	8*1024	8*1024	8*1024	
	Maximum DHCP packet processing rate	100/s	100/s	500/s	500/s	500/s	500/s	
	DHCP Client	Support	Support	Support	Support	Support	Support	
	Maximum interfaces which enable the DHCP Client	16	16	16	16	16	16	
	DHCP Relay	Support	Support	Support	Support	Support	Support	
	DHCP Snooping	Support	Support	Support	Support	Support	Support	

	Domain Name Server (DNS)	Support	Support	Support	Support	Support	Support	
	Protocol over the DNS	UDP	UDP	UDP	UDP	UDP	UDP	
	DNS Server	Not support	Not support	Not support	Not support	Not support	Not support	
	DNS Client	Support	Support	Support	Support	Support	Support	
	DNS Proxy/Relay	Support	Support	Support	Support	Support	Support	
	Dynamic Domain Name Server (DDNS)	Support	Support	Support	Support	Support	Support	
	Unicast reverse path forwarding(URPF)	Support	Support	Support	Support	Support	Support	
	Path maximum transmission unit(MTU)	328 to 1500	328 to 1500	328 to 1500	328 to 1500	328 to 1500	328 to 1500	
Unicast routing								
	Static routing	Support	Support	Support	Support	Support	Support	
	Static routing entry	5000	5000	5000	5000	5000	5000	
	Policy-based routing	Support	Support	Support	Support	Support	Support	
	Routing policy	Support	Support	Support	Support	Support	Support	
	Number of the routing policies	1000	1000	1000	1000	1000	1000	
	Number of nodes of each policy-based routing	20	20	20	20	20	20	
	Routing iteration	Support	Support	Support	Support	Support	Support	
	Routing management	Support	Support	Support	Support	Support	Support	
	Equal-cost multipath(ECMP)	Support	Support	Support	Support	Support	Support	
	Entry of the equal-cost routing	8	8	8	8	8	8	
	Packet-based ECMP	Support	Support	Support	Support	Support	Support	
	Flow-based ECMP	Support	Support	Support	Support	Support	Support	
	WCMP	Support	Support	Support	Support	Support	Support	
	Packet-based WCMP	Support	Support	Support	Support	Support	Support	
	Flow-based WCMP	Support	Support	Support	Support	Support	Support	
	ISP intelligent routing	Support	Support	Support	Support	Support	Support	
	Dynamic routing	Support	Support	Support	Support	Support	Support	
	Maximum number of the dynamic routing entries	10000	10000	16000	16000	16000	16000	
	RIPv1/v2	Support	Support	Support	Support	Support	Support	
	Open Shortest Path First Interior Gateway Protocol (OSPF)	Support	Support	Support	Support	Support	Support	
	Number of the OSPF instances supported	100	100	100	100	100	100	
	Number of the AREAs supported by each OSPF instance	50	50	50	50	50	50	
	Number of the LSDBs supported by each OSPF instance	100,000	100,000	100,000	100,000	100,000	100,000	
	Number of the external LSAs supported by each OSPF instance	100,000	100,000	100,000	100,000	100,000	100,000	
	Number of the instances imported into the routing protocol	99	99	99	99	99	99	
	ISIS	Support	Support	Support	Support	Support	Support	
	BGP	Support	Support	Support	Support	Support	Support	
	Number of the BGPs instances supported	100	100	100	100	100	100	
	Number of the PEERs supported	100	100	100	100	100	100	
Multicast characteristic								
	Static multicast	Support	Support	Support	Support	Support	Support	
	Internet Group Management Protocol (IGMP)	Not Support	Support	Support	Support	Support	Support	
	IGMP Proxy	Not Support	Support	Support	Support	Support	Support	
	IGMP Snooping	Not Support	Support	Support	Support	Support	Support	
	Multicast Source Discovery Protocol (MSDP)	Support	Support	Support	Support	Support	Support	
	Protocol Independent Multicast-Dense Mode (PIM-DM)	Support	Support	Support	Support	Support	Support	
	Protocol Independent Multicast-Sparse Mode (PIM-SM)	Support	Support	Support	Support	Support	Support	
Intelligent routing								
	Intelligent routing based on the users	Support	Support	Support	Support	Support	Support	
	Intelligent routing based on the user groups	Support	Support	Support	Support	Support	Support	
	Intelligent routing based on the application protocols	Support	Support	Support	Support	Support	Support	
	Intelligent routing based on the weight	Support	Support	Support	Support	Support	Support	
	Intelligent routing based on the interface load	Not support	Not support	Not support	Not support	Not support	Not support	
	The same uplink and downlink routes with different outbound interfaces	Not support	Not support	Not support	Not support	Not support	Not support	
QOS								
	Interface-based CAR	Support	Support	Support	Support	Support	Support	
	FIFO	Support	Support	Support	Support	Support	Support	
	Length of the FIFO queue	Range: 1–1024. Default: 256	Range: 1–1024. Default: 256	Range: 1–1024. Default: 256	Range: 1–1024. Default: 256	Range: 1–1024. Default: 256	Range: 1–1024. Default: 256	
	PQ	Support	Support	Support	Support	Support	Support	
	Default length of the HIGH queue	300	300	300	300	300	300	
	Default length of the MEDIUM queue	400	400	400	400	400	400	
	Default length of the NORMAL queue	500	500	500	500	500	500	
	Default length of the LOW queue	600	600	600	600	600	600	
	Maximum length of the queues	1024	1024	1024	1024	1024	1024	
	Number of the PQL rule groups	16	16	16	16	16	16	
	Maximum number of traffic classification rules for each PQL	100	100	100	100	100	100	
	CQ	Support	Support	Support	Support	Support	Support	
	Default length of the CQ queue	100	100	100	100	100	100	
	Maximum length of the queues	1024	1024	1024	1024	1024	1024	
	Number of the CQL rule groups	16	16	16	16	16	16	
	Maximum number of nodes for each CQL	100	100	100	100	100	100	
	WFQ	Support	Support	Support	Support	Support	Support	
	Number scope of the WFQ queue	16-4096	16-4096	16-4096	16-4096	16-4096	16-4096	
	Default length of the WFQ queue	64	64	64	64	64	64	
	Maximum length of the WFQ queue	1024	1024	1024	1024	1024	1024	
	WRR	Support	Support	Support	Support	Support	Support	
	CQC	Support	Support	Support	Support	Support	Support	
	CBWFQ	Support	Support	Support	Support	Support	Support	
	CBQ	Support	Support	Support	Support	Support	Support	
	EF	Support	Support	Support	Support	Support	Support	
	AF	Support	Support	Support	Support	Support	Support	
	WFQ	Support	Support	Support	Support	Support	Support	
	CIR	Support	Support	Support	Support	Support	Support	
	RTPQ	Support	Support	Support	Support	Support	Support	
	WRED	Support	Support	Support	Support	Support	Support	
	LR	Support	Support	Support	Support	Support	Support	
	GTS	Support	Support	Support	Support	Support	Support	
	HQOS	Support	Support	Support	Support	Support	Support	
	Constraint on full rate of the HQoS interface	Support	Support	Support	Support	Support	Support	
	User-level queue scheduling	Support	Support	Support	Support	Support	Support	
	Service-level queue scheduling	Support	Support	Support	Support	Support	Support	

Item	Functions	USG2110F/FW/AW/AGW V300R001	USG2160/W V300R001	USG2230 V300R001	USG2260 V300R001	USG5120 V300R001	USG5150 V300R001	Remarks
Unified Threat Management (UTM)								
	IPS	Supported	Supported	Supported	Supported	Supported	Supported	
	Antivirus	Supported	Supported	Supported	Supported	Supported	Supported	
	URL filtering	Supported	Supported	Supported	Supported	Supported	Supported	
	Anti-spam	Supported	Supported	Supported	Supported	Supported	Supported	The RBL is supported.
	UTM performance(IPS, AV, URL filtering, AS)	24M	24M	370M	370M	725M	725M	Use Spirent WebAvalanche
Performance								
IPS performance								
	Data throughput (HTTP)	24M	24M	370M	370M	770M	770M	Use Spirent WebAvalanche
	Capacity of the signature repository	500+	500+	2000+	2,000+	2,000+	2,000+	
Anti-Virus performance(proxy-based)								
	Data throughput (HTTP)	31.4M	31.4M	500M	500M	725M	725M	Use Spirent WebAvalanche
	Capacity of the anti-virus library	30000	30000	100000	100000	100000	100000	
	Virus that can be detected	1,000,000+	1,000,000+	7,000,000+	7,000,000+	7,000,000+	7,000,000+	
Uniform Resource Locater(URL) performance								
	URL category			130	130	130	130	
	Number of the URL entries			65000000	65000000	65000000	65000000	
IPS Intrusion Prevention								
	Deployment mode	Supported	Supported	Supported	Supported	Supported	Supported	
	Protection mode	Supported	Supported	Supported	Supported	Supported	Supported	
	Alarm mode	Supported	Supported	Supported	Supported	Supported	Supported	
	Capacity of the signature repository	500 plus	500 plus	2000 plus	2000 plus	2000 plus	2000 plus	
	Fragment reassembly	Supported	Supported	Supported	Supported	Supported	Supported	
	Flow reassembly	Supported	Supported	Supported	Supported	Supported	Supported	
	Feature-based intrusion prevention	Supported	Supported	Supported	Supported	Supported	Supported	
	Protocol anomaly detection	Supported	Supported	Supported	Supported	Supported	Supported	
	Protocol identification	Supported	Supported	Supported	Supported	Supported	Supported	
	User-defined IPS signature	Supported	Supported	Supported	Supported	Supported	Supported	
	Global IPS enabling switch	Supported	Supported	Supported	Supported	Supported	Supported	
	Setting category-based response modes	Supported	Supported	Supported	Supported	Supported	Supported	
	Setting response modes based on a single signature forcibly	Supported	Supported	Supported	Supported	Supported	Supported	
	Applied in the interdomain (either inbound or outbound) and intradomain	Not Supported	Not Supported	Supported	Supported	Supported	Supported	
	Setting privileged IPS: specifying a certain existing IPS policy as a privileged policy	Supported	Supported	Supported	Supported	Supported	Supported	
	IPS virtualization	Not Supported	Not Supported	Supported	Supported	Supported	Supported	
	Virtual firewall detected by IPS	Not Supported	Not Supported	Supported	Supported	Supported	Supported	
	IPS detects the transmission packets of each virtual firewall.	Not Supported	Not Supported	Supported	Supported	Supported	Supported	
	Number of the IPS policies supported by the virtual firewall	Not Supported	Not Supported	2 global IPS policies	2 global IPS policies	2 global IPS policies	2 global IPS policies	
	Provision of the IPS policies template	Supported	Supported	Supported	Supported	Supported	Supported	
	Display of the signatures according to different categories	Supported	Supported	Supported	Supported	Supported	Supported	
	Query of signatures	Supported	Supported	Supported	Supported	Supported	Supported	
	Signature repository upgrade	Supported	Supported	Supported	Supported	Supported	Supported	
	Automatic upgrade	Supported	Supported	Supported	Supported	Supported	Supported	
	Manual upgrade	Supported	Supported	Supported	Supported	Supported	Supported	
	Local upgrade	Supported	Supported	Supported	Supported	Supported	Supported	
	Version rollback	Supported	Supported	Supported	Supported	Supported	Supported	
Anti-Virus								
	Global antivirus enabling switch	Supported	Supported	Supported	Supported	Supported	Supported	
	Grade setting for the virus scanning	Level 1 to level 3	Level 1 to level 3	Level 1 to level 3	Level 1 to level 3	Level 1 to level 3	Level 1 to level 3	
	Scanning files uploaded or downloaded through HTTP	Supported	Supported	Supported	Supported	Supported	Supported	
	Scanning files uploaded or downloaded through FTP	Not Supported	Not Supported	Supported	Supported	Supported	Supported	
	Scanning SMTP mail attachments	Supported	Supported	Supported	Supported	Supported	Supported	
	Scanning POP3 mail attachments	Supported	Supported	Supported	Supported	Supported	Supported	
	Scanning compressed files	Supported (the maximum number of files to be scanned is 100)	Supported (the maximum number of files to be scanned is 100)	Supported (the maximum number of files to be scanned is 100)	Supported (the maximum number of files to be scanned is 100)	Supported (the maximum number of files to be scanned is 100)	Supported (the maximum number of files to be scanned is 100)	
	Compressed file types	Compressed formats supported: Mac binary, Apple Single, ZIP, OLESS -- Structured Storage (MS Office documents), OLE1 (not the same as OLESS), GZIP, LHA, RAR, ARJ, TNEF, LZ, AMG, TAR, RTF, BZIP2, PDF, and TEXT (MIME, BinHex, UUE, MBOX)	Compressing formats supported: Mac binary, Apple Single, ZIP, OLESS -- Structured Storage (MS Office documents), OLE1 (not the same as OLESS), GZIP, LHA, RAR, ARJ, TNEF, LZ, AMG, TAR, RTF, BZIP2, PDF, and TEXT (MIME, BinHex, UUE, MBOX)	Compressing formats supported: Mac binary, Apple Single, ZIP, OLESS -- Structured Storage (MS Office documents), OLE1 (not the same as OLESS), GZIP, LHA, RAR, ARJ, TNEF, LZ, AMG, TAR, RTF, BZIP2, PDF, and TEXT (MIME, BinHex, UUE, MBOX)	Compressing formats supported: Mac binary, Apple Single, ZIP, OLESS -- Structured Storage (MS Office documents), OLE1 (not the same as OLESS), GZIP, LHA, RAR, ARJ, TNEF, LZ, AMG, TAR, RTF, BZIP2, PDF, and TEXT (MIME, BinHex, UUE, MBOX)	Compressing formats supported: Mac binary, Apple Single, ZIP, OLESS -- Structured Storage (MS Office documents), OLE1 (not the same as OLESS), GZIP, LHA, RAR, ARJ, TNEF, LZ, AMG, TAR, RTF, BZIP2, PDF, and TEXT (MIME, BinHex, UUE, MBOX)	Compressing formats supported: Mac binary, Apple Single, ZIP, OLESS -- Structured Storage (MS Office documents), OLE1 (not the same as OLESS), GZIP, LHA, RAR, ARJ, TNEF, LZ, AMG, TAR, RTF, BZIP2, PDF, and TEXT (MIME, BinHex, UUE, MBOX)	
	Setting of decompressed layer	1–4 layer	1–4 layer	2–20 layer	2–20 layer	2–20 layer	2–20 layer	
	Scanning packed viruses	Supported	Supported	Supported	Supported	Supported	Supported	
	Setting refined virus scanning policies of HTTP	Supported	Supported	Supported	Supported	Supported	Supported	
	Setting refined virus scanning policies of SMTP protocol	Supported	Supported	Supported	Supported	Supported	Supported	
	Setting refined virus scanning policies of POP3 protocol	Supported	Supported	Supported	Supported	Supported	Supported	
	Common configurations for policies	Supported	Supported	Supported	Supported	Supported	Supported	
	The policy is applied in the interdomain in inbound or outbound direction.	Supported	Supported	Supported	Supported	Supported	Supported	
	The user can query the virus list of the current signature files.	Supported	Supported	Supported	Supported	Supported	Supported	
	Virus URL collection	Supported	Supported	Supported	Supported	Supported	Supported	
	AV virtualization	Not Supported	Not Supported	Supported	Supported	Supported	Supported	

	Virtual firewall detected by AV	Not Supported	Not Supported	Supported	Supported	Supported	Supported	
	AV detects the transmission packets of each virtual firewall.	Not Supported	Not Supported	Supported	Supported	Supported	Supported	
	Number of the AV policies supported by the virtual firewall	Not Supported	Not Supported	3 global AV policies	3 global AV policies	3 global AV policies	3 global AV policies	
	Configuration of the AV policy within the root firewall and application of that within the virtual firewall instance	Not Supported	Not Supported	Supported	Supported	Supported	Supported	
	Anti virus database and anti-virus engine upgrade	Supported	Supported	Supported	Supported	Supported	Supported	
	Automatic upgrade	Supported	Supported	Supported	Supported	Supported	Supported	
	Manual upgrade	Supported	Supported	Supported	Supported	Supported	Supported	
	Local upgrade	Supported	Supported	Supported	Supported	Supported	Supported	
	Version rollback	Supported	Supported	Supported	Supported	Supported	Supported	
WEB filtering								
	URL filtering	Not Supported	Not Supported	Supported	Supported	Supported	Supported	
	URL standardization	Not Supported	Not Supported	Supported	Supported	Supported	Supported	
	Classification filtering based on remote URL	Not Supported	Not Supported	Supported	Supported	Supported	Supported	
	Classification filtering based on local URL	Not Supported	Not Supported	Supported	Supported	Supported	Supported	
	URL keyword filtering	Not Supported	Not Supported	Supported	Supported	Supported	Supported	
	Providing URL blacklist and whitelist	Not Supported	Not Supported	Supported	Supported	Supported	Supported	
	Providing global URL filtering configuration	Not Supported	Not Supported	Supported	Supported	Supported	Supported	
	Providing inter-domain switch of the global URL filtering	Not Supported	Not Supported	Supported	Supported	Supported	Supported	
	Providing default processing action configuration of the URL policies	Not Supported	Not Supported	Supported	Supported	Supported	Supported	
	Providing configuration for the content of the push page	Not Supported	Not Supported	Supported	Supported	Supported	Supported	
	Providing URL filtering policies setting of the fine grain	Not Supported	Not Supported	Supported	Supported	Supported	Supported	
	Number of the URL polices of the fine grain	Not Supported	Not Supported	100	100	100	100	
	Configuration parameters of the URL filtering policies at least comprises: on/off for each sub-function and action of classification.	Not Supported	Not Supported	Supported	Supported	Supported	Supported	
	Both prohibition and permission of the response mode are available. In the prohibition mode, the page push is available.	Not Supported	Not Supported	Supported	Supported	Supported	Supported	
	Application in the web policies	Not Supported	Not Supported	Supported	Supported	Supported	Supported	
	Default action configuration	Not Supported	Not Supported	Supported	Supported	Supported	Supported	
	Adjustment of the user-defined classification priority	Not Supported	Not Supported	Supported	Supported	Supported	Supported	
	URL visiting design	Not Supported	Not Supported	Supported	Supported	Supported	Supported	
	URL hot library	Not Supported	Not Supported	Supported	Supported	Supported	Supported	
	URL filtering virtualization	Not Supported	Not Supported	Supported	Supported	Supported	Supported	
	WEB filtering	Not Supported	Not Supported	Supported	Supported	Supported	Supported	
	WEB content and keyword filtering	Not Supported	Not Supported	Supported	Supported	Supported	Supported	
	Keyword of the search engine filtering	Not Supported	Not Supported	Supported, Google, Yahoo, Bing, and Baidu	Supported, Google, Yahoo, Bing, and Baidu	Supported, Google, Yahoo, Bing, and Baidu	Supported, Google, Yahoo, Bing, and Baidu	
email filtering								
	Blacklist and whitelist filtering based on the local IP(SMTP)	Not Supported	Not Supported	Supported	Supported	Supported	Supported	
	SMTP supports filtering of the local IP whitelist.	Not Supported	Not Supported	Supported	Supported	Supported	Supported	
	Number of the whitelists	Not Supported	Not Supported	128	128	128	128	
	SMTP supports filtering of the local IP blacklist.	Not Supported	Not Supported	Supported	Supported	Supported	Supported	
	Number of the blacklists	Not Supported	Not Supported	128	128	128	128	
	Whitelist shall prevail when an IP simultaneously appears in the blacklist and whitelist.	Not Supported	Not Supported	Supported	Supported	Supported	Supported	
	Anti-Spam filtering based on the remote RBL(SMTP)	Not Supported	Not Supported	Supported	Supported	Supported	Supported	
	Response action setting	Not Supported	Not Supported	Blocking, alarming, and discharging	Blocking, alarming, and discharging	Blocking, alarming, and discharging	Blocking, alarming, and discharging	
	Email content filtering	Not Supported	Not Supported	Supported	Supported	Supported	Supported	
	Email type	Not Supported	Not Supported	webmail (163/Yahoo), smtp, and POP3	webmail (163/Yahoo), smtp, and POP3	webmail (163/Yahoo), smtp, and POP3	webmail (163/Yahoo), smtp, and POP3	
	Receiver/sender keyword filtering	Not Supported	Not Supported	Supported	Supported	Supported	Supported	
	Keyword filtering of the email subject and content	Not Supported	Not Supported	Supported	Supported	Supported	Supported	
	Attachment files name/capacities/extensions/number of attachments shall be filtered according to users.	Not Supported	Not Supported	Supported	Supported	Supported	Supported	
	Response mode	Not Supported	Not Supported	SMTP response mode: return the blocking answer-back code and reason; POP4 response mode: write a new email to replace the blocked email for the receiver; Webmail response mode: discharging and blocking	SMTP response mode: return the blocking answer-back code and reason; POP5 response mode: write a new email to replace the blocked email for the receiver; Webmail response mode: discharging and blocking	SMTP response mode: return the blocking answer-back code and reason; POP5 response mode: write a new email to replace the blocked email for the receiver; Webmail response mode: discharging and blocking	SMTP response mode: return the blocking answer-back code and reason; POP5 response mode: write a new email to replace the blocked email for the receiver; Webmail response mode: discharging and blocking	
	Email filtering virtualization	Not Supported	Not Supported	Supported	Supported	Supported	Supported	

Primary Specification	Secondary Specification	USG2100 V300R001	USG2200/USG5100 V300R001	Remarks
IPv6 Basic				
	Protocol processing	Supported	Supported	
	Unicast forwarding processing	Supported	Supported	
	IPv6 MIB	Supported	Supported	
	Interfaces supported by IPv6	Eth, VlanIF, Tunnel, Dialer, Eth-Trunk, Loopback, and Subinterface	Eth, GE, VlanIF, Tunnel, Dialer, Eth-Trunk, Loopback, and Subinterface	
	ICMPv6			
	Computing the ICMP6 checksum	Supported	Supported	
	ICMPv6 error message reported to the application layer by using RawIPv6 module	Supported	Supported	
	Sending of ICMPv6 error packet type to the TCP6 or UDP6	Supported	Supported	
	Proper processing the ICMPv6 notification	Supported	Supported	
	Precise processing the notification according to the ICMP6	Supported	Supported	
	Sending of the ICMP error message and notification	Supported	Supported	
	Sending of redirection message	Supported	Supported	
	IPv6 address management	Supported	Supported	
	Manual configuration of the local address of links	Supported	Supported	
	Stateless address auto-configuration of link-local address	Supported	Supported	
	All-state address auto-configuration of Global unicast address	Supported	Supported	
	Stateless address auto-configuration of global unicast address	Supported	Supported	
	Manual configuration of global unicast address	Supported	Supported	
	Configuration of global unicast address interface identifier according to the IEEE EUI-64 format	Supported	Supported	
	Query of unicast and multicast IPv6 addresses	Supported	Supported	
	Executing DAD for the unicast IPv6 address	Supported	Supported	
	ND	Supported	Supported	
	Receiving and responding to router solicitation	Supported	Supported	
	Periodical sending of router advertisement	Supported	Supported	
	Receiving and confirming router advertisement	Supported	Supported	
	Sending of RA packet when changing interface status, local link address or Routing Area (RA) parameters	Supported	Supported	
	Receiving neighbor advertisement and sending response	Supported	Supported	
	Receiving neighbor advertisement and refreshing neighbor buffer	Supported	Supported	
	The node sends neighbor advertisement for address.	Supported	Supported	
	Sending of neighbor advertisement for address DAD	Supported	Supported	
	Configuration of RA parameters	Supported	Supported	
	Automatical generation of prefix options of the RA when adding IPv6 address to the interface	Supported	Supported	
	Query of neighbor items by using the IPv6 address	Supported	Supported	
	Number of neighbor items	(4096 dynamic + 1024 static)/interface	(4096 dynamic + 1024 static)/interface	
	Periodical refreshing neighbor items and deleting unreachable neighbors	Supported	Supported	
	Configuration of static neighbor items	Supported	Supported	
	Display of neighbor items content	Supported	Supported	
	ND-RA	Supported	Supported	
	Disabling/enabling sending of RS packets	Supported	Supported	
	Configuration of default route according to RA packets	Supported	Supported	
	Configuration of interface address according to RA packets	Supported	Supported	
	Obtaining the information of DNS server and DNS Domain according to RA packets	Supported	Supported	
	Update of interface MTU according to RA packets	Supported	Supported	
	Specifications of ND RA	Each interface supports a maximum of 10 prefix entries. The overall unit supports a maximum of 10 default routes. The overall unit supports a maximum of 16 stateless auto-configured interfaces. The overall unit supports a maximum of 20 DNS server addresses. The overall unit supports a maximum of 20 DNS domains.	Each interface supports a maximum of 10 prefix entries. The overall unit supports a maximum of 10 default routes. The overall unit supports a maximum of 16 stateless auto-configured interfaces. The overall unit supports a maximum of 20 DNS server addresses. The overall unit supports a maximum of 20 DNS domains.	
	CGA	Supported	Supported	
	SEND	Supported	Supported	
	Configuration of the CGA address by using the interface	Supported	Supported	
	Communication between the interface and other nodes by using the CGA address	Supported	Supported	
	Setting timestamp parameters for the interface and discarding packets with unauthorized timestamps	Supported	Supported	
	running the interface under the full-secure mode and discarding neighbor packets without security options	Supported	Supported	
	Sending of NS, NA, RA, and Redirect packets by means of the CGA address	Supported	Supported	
	Verification of SEND-type packets and discard of unauthorized packets.	Supported	Supported	
	Router authentication and correct RA and CPA response to the RS and CPS requests from the host so as to configure the correct network parameters	Supported	Supported	
	Interface types supported by SEND	Eth, VlanIF, Eth-Trunk, and Subinterfaces	GE, Eth, VlanIF, Eth-Trunk, and Subinterfaces	
	The node sends neighbor advertisement for address resolution.	Supported	Supported	
	PMTU	Supported	Supported	

	Configuration and display of PMTU aging time based on a destination address or global default address	Supported	Supported	
	Configuration and display of PMTU based on a destination address	Supported	Supported	
	The PMTU items are maintained by using two hashes. The keys of the hashes are destination address and immediate number, and socket number and immediate number.	Supported	Supported	
	Sending of a notification packet when PMTU changes and is removed from the socket	Supported	Supported	
	PMTU items in a total size of 1 kilobyte can be saved, or else the least-used item is deleted.	Supported (1024)	Supported (1024)	
	Analyzing and processing ultra-large ICMP packets	Supported	Supported	
	PMTU aging is implemented by timer mechanism on the main control board.	Supported	Supported	
	The ultra-large ICMP packets are processed on the main control board.	Supported	Supported	
	IPv6 unicast reverse path forwarding (URPF)	Supported	Supported	
IPv6 Extension				
	Ethernet Link Layer	Supported	Supported	
	ACL IPv6	Supported	Supported	
	Basic ACL	Supported	Supported	
	Packet filtering based on the source address	Supported	Supported	
	Packet filtering based on the time range	Supported	Supported	
	Advanced ACL	Supported	Supported	
	Packet filtering based on the source address, destination address, source interface, destination interface, and protocol	Supported	Supported	
	Packet filtering based on the time range	Supported	Supported	
	Packet filtering based on the TOS field	Supported	Supported	
	Packet filtering based on the priority	Supported	Supported	
	Number of the rules available for the configuration of the overall unit	3,000	10,000	
	Number of the rules for each ACL rule group	2,048	10,000	
	Policy 6	Supported	Supported	
	Maximum number of address object	256	256	
	Maximum number of address group	256	256	
	In the address object, configure the IPv6 addresses or address ranges as members. Maximum number of members.	1024	1024	
	In the address group, IPv6 addresses and address ranges are configured as members, or other address objects and address groups are used as members. Maximum number of members.	1024	1024	
	Maximum number of service objects	1024	1024	
	Maximum number of service groups	512	512	
	For the service object, one or several of protocols, source interfaces, and destination interfaces are configured as one service, which functions as a member of the service object. Maximum number of members.	256	256	
	In the service group, service objects and service groups are configured as members. Maximum number of members.	256	256	
	Number of Policy IDs in the overall system	3,000	20,000	
	Upper limit for use of each ipv6 address set	512	512	
	Upper limit for use of each service set	512	512	
	ACL6 acceleration	Supported	Supported	
	Enabling/disabling ACL6 acceleration	Supported	Supported	
	ACL6 acceleration query	Supported	Supported	
	Basic ACL6 rule acceleration	Supported	Supported	
	Advanced ACL6 rule acceleration	Supported	Supported	
	Policy6 rule acceleration	Supported	Supported	
	NAT64 policy rule acceleration	Supported	Supported	
	Ping6	Supported	Supported	
	DNS6			
	DNS static configuration	Supported	Supported	
	Number of DNS static configuration entries	For static host: up to 50 For suffix of domain name: up to 10	For static host: up to 50 For suffix of domain name: up to 10	
	DNS local buffer	Supported	Supported	
	DNS buffer timeout	Supported	Supported	
	DNS6 Proxy	Not Supported	Supported	
	Receiving/sending type-A query requests		Supported	
	Receiving/sending type-AAAA query requests		Supported	
	Receiving/resolving query request packets		Supported	
	Receiving/resolving query response packets		Supported	
	Static domain name search		Supported	
	Dynamic buffer		Supported	
	Buffer auto-aging		Supported	
	TraceRT			
	Telnet	Supported	Supported	
	DHCP6			
	DHCP6 client	Supported	Supported	
	DHCP6 Server	Supported	Supported	
	Interface type supported	Vlanif, Ethernet, Eth-runk, and Subinterface	GE, Vlanif, Ethernet, Eth-runk, and Subinterface	
	Configuration of quick options	Supported	Supported	
	Configuration of interface bound address pool	Supported	Supported	
	Number of IPv6 addresses assigned to each client	1	1	
	Lease management of IPv6 address	Supported	Supported	
	Recycle of addresses released by clients.	Supported	Supported	

	Disabling/enabling address pool or certain address prefix	Supported	Supported	
	The stateless PHCPv6 is supported, in which the client obtains IPv6 address by using stateless address allocation and other configuration information from the Server.	Supported	Supported	
	Lifetime preferred-lifetime, priority time	Supported	Supported	
	Lifetime valid-lifetime, valid time	Supported	Supported	
	The renew-time-percent is configured, which is the percentage of the priority time divided by the IPv6 address pool renew time (T1).	Supported	Supported	
	The rebind-time-percent is configured, which is the percentage of the priority time divided by the IPv6 address pool rebind time (T2).	Supported	Supported	
	Number of client end	25,000	25,000	
	DHCP6 OPTION	Supported	Supported	
	The IPv6 prefix pool includes the local prefix pool and Delegation prefix pool.	Supported	Supported	
	The IPv6 address pool stands as a single type.	Supported	Supported	
	Generation mode of DUID	Creation of DUID by LL mode.	Creation of DUID by LL mode.	
	Number of DNS servers available for client configuration	2	2	
	Number of domain names available for client configuration	1	1	
	Maximum number of Client-DUIDs and prefix bindings available in the delegation prefix pool	1024	1024	
	IPv6 prefixes are allocated by Relay.	Supported	Supported	
	DHCP6 Server Relay			
	Configuration of DHCPv6 server address and outbound interface	Supported	Supported	
	DHCP interaction information between the relay server and the client	Supported	Supported	
	DHCP interaction information between relays	Supported	Supported	
	DHCP interaction information between the relay and the server	Supported	Supported	
	Relay information to one or multiple relays or servers.	Supported	Supported	
	The client-sent DHCP packets is relayed to the destination DHCP server across different network segments. Number of the network segments.	Support level 4 relay	Support level 4 relay	
	Number of next hop destinations (IP or outbound interface) available for each relay interface	4	4	
	Prefix proxy			
	Configuration of prefix address pool	Supported	Supported	
	FW simultaneously implements client and server functions when acting as a Requesting-Router.	Supported	Supported	
	FW implements server function when acting as a Delegating-Router.	Supported	Supported	
	Requesting-Router applies for address prefix and other address information and imports them in the local address pool.	Supported	Supported	
	Address prefix lease of Requesting-Router and update of local address pool	Supported	Supported	
	Validity check for DHCPV6 Request packets	Supported	Supported	
	Statistics of DHCPV6 packets received	Supported	Supported	
	Statistics of DHCPV6 packets discarded	Supported	Supported	
	The configuration of address pool is checked.	Supported	Supported	
	The allocation of address pool is checked.	Supported	Supported	
	Printing of the interactive debug information of DHCPv6	Supported	Supported	
	Log for address allocation success and failure information is output.	Supported	Supported	
	Log for prefix allocation success and failure information is printed.	Supported	Supported	
	Diagnosis log information in the key procedures during address application and allocation is printed.	Supported	Supported	
	Authentication type	Non-authentication, local authentication, and Radius authentication are supported.	Non-authentication, local authentication, and Radius authentication are supported.	
	PPPoE6 Client			
IPv6 transition technology				
	IPv4 over IPv6 tunnel	Supported	Supported	
	IPv4 over IPv6 manual tunnel	Supported	Supported	
	IPv6 over IPv4 tunnel			
	IPv6 over IPv4 manual tunnel	Supported	Supported	
	IPv6 over IPv4 automatic tunnel	Supported	Supported	
	IPv6 over IPv4 GRE tunnel	Supported	Supported	
	IPv6 over IPv4 6to4 tunnel	Supported	Supported	
	ISATAP tunnel	Supported	Supported	
	6RD tunnel	Supported	Supported	
	Tunnel seal type is 6RD.	Supported	Supported	
	Configuration of IPv6 prefix.	Supported, Range: 1-63 BIT	Supported, Range: 1-63 BIT	
	Configuration of the 6RD entrust prefix (IPv4 address mask length)	Supported, Range: 0-31 BIT	Supported, Range: 0-31 BIT	
	Configuration of the source address of the IPv6 tunnel	Supported	Supported	
	Manual configuration of the BR address	Supported	Supported	
	URPF under 6RD tunnel	Supported	Supported	
	Automatic generation of the entrusted prefix of IPv6	Supported	Supported	
	Fragmentation and reassembly.	Supported	Supported	
	NAT64	Not supported	Supported	
	Configuration of IPv4 public network address pool		Supported	
	Configuration of IPv6 prefix and address format		Supported	
	Translation of TCP/UDP/ICMP packets		Supported	
	PMTU processing		Supported	
	ALG includes FTP, RTSP, and ICMP.		Supported	
	Configurable aging time for Session (TCP/UDP)		Supported	
	Triplet session		Supported	

	Packet fragmentation		Supported	
	Translation of packet fragments		Supported	
	Out-of-sequence processing for packet fragments		Supported	
	PAT mode		Supported	
IPv6 ASPF&ALG				
	IPv6 ASPF			
	FTPv6	Supported	Supported	
	Status detection for RTSP protocol	Supported	Supported	
	IPv6 ALG			
	FTPv6 ALG	Supported	Supported	
	RTSP ALG	Supported	Supported	
IPv6 forwarding				
	IPv6 stream forwarding	Supported	Supported	
	Number of IPv6 session tables		1,000,000 for FW mode; 100,000 for UTM mode	
	Number of fragment session tables	64 x 1024	64 x 1024	
	Fragment cache	Supported	Supported	
	Fragment transparent transmission	Supported	Supported	
	Session entry query	Supported	Supported	
	Keyword filtering	Supported	Supported	
	Number of IPv6 ServerMap entries	Supported	Supported	
	FTP extension command	Supported	Supported	
	Interfaces supported by IPv6	Eth, vlanIf, Eth-Trunk, subinterface, Tunnel, and Dialer	GE, Eth, vlanIf, Eth-Trunk, subinterface, Tunnel, and Dialer	
IPv6 route				
	Static route			
	Number of IPv6 static routes	1000	1000	
	Policy-based routing			
	Configuration of interface type of policy-based routing	Vlanif, Ethernet, Eth-runk, and Subinterface	GE, Vlanif, Ethernet, Eth-runk, and Subinterface	
	Policy-based routing is used for packets received at designated interfaces.	Supported	Supported	
	Control and execution of the policy-based routing by ACL6	Supported	Supported	
	Number of policy-based routings	100	100	
	Number of nodes for each policy-based routing	20	20	
	Equal-cost route under the next hop of policy-based routing	Supported	Supported	
	Routing policy			
	Number of IPV6 address prefixes supported by the overall unit	5,000	5,000	
	Number of nodes supported by each routing policy	128	128	
	Number of routing policy supported by the overall unit	64	64	
	Number of nodes supported by the overall unit	128 x 64	128 x 64	
	Routing iteration	Supported	Supported	
	RIPng			
	Sending of RIPng response	Supported	Supported	
	Receiving RIPng response	Supported	Supported	
	Sending of RIPng request	Supported	Supported	
	Receiving RIPng request	Supported	Supported	
	Trigger update.	Supported	Supported	
	Next-Hop	Supported	Supported	
	Routing Tag	Supported	Supported	
	Subnet mask	Supported	Supported	
	Validity certification for packets	Supported	Supported	
	Neighbor source address check	Supported	Supported	
	Disable MBZ domain check	Supported	Supported	
	Withdrawal of distributed route	Supported	Supported	
	Setting Update timer and time interval	Supported	Supported	
	Setting Age timer and time interval	Supported	Supported	
	Setting Garbage Collection timer and time interval	Supported	Supported	
	Setting Suppress timer and time interval	Supported	Supported	
	Enabling/disabling RIPng on the interface	Supported	Supported	
	Sending of default route on the interface	Supported	Supported	
	Metric value is added when sending route upgrades on the interface.	Supported	Supported	
	Metric value is added when receiving route upgrades on the interface.	Supported	Supported	
	Configuration of route summarization on the interface	Supported	Supported	
	Configuration of split horizon on the interface	Supported	Supported	
	Configuration of poison reverse on the interface	Supported	Supported	
	Equal-cost route	Supported	Supported	
	Control of the maximum number of equal-cost routes	Supported	Supported	
	Multi-threaded process with its number restricted by the License	Supported	Supported	
	Import of direct routing	Supported	Supported	
	Import of static routing	Supported	Supported	
	Import of OSPFv3 routing	Supported	Supported	
	Import of ISIS routing	Supported	Supported	
	Import of RIPng routing	Supported	Supported	
	Import of BGP routing	Supported	Supported	
	Routing policy is applied when importing a route.	Supported	Supported	
	Route filtering is implemented when receiving a route.	Supported	Supported	
	Route filtering is implemented when distributing a route.	Supported	Supported	
	Number of PEERs supported	100	100	
	Number of routes supported by RIPng	10,000	10,000	

	Number of processes supported by RIPng		100	
	Maximum number of interfaces supported by each process		256	
	OSPFv3			
	Area division	Supported	Supported	
	Configuration of default cost value in the area	Supported	Supported	
	Stub area	Supported	Supported	
	Total Stub area.	Supported	Supported	
	Route summarization on ABR	Supported	Supported	
	Route summarization not-advertise on ABR.	Supported	Supported	
	Enabling/disabling OSPFv3 on the interface	Supported	Supported	
	Silent interface	Supported	Supported	
	Configuration of cost value on the interface	Supported	Supported	
	Configuration of DR priority on the interface	Supported	Supported	
	Configuration of Ignore MTU check on the interface	Supported	Supported	
	Configuration of transfer delay on the interface	Supported	Supported	
	Configuration of Hello time interval on the interface	Supported	Supported	
	Configuration of Dead time interval on the interface	Supported	Supported	
	Configuration of retransmission time interval on the interface	Supported	Supported	
	Multi-threaded process	Supported	Supported	
	Designated Router ID	Supported	Supported	
	Configuration of the cost value of the default route	Supported	Supported	
	Hello imitation	Supported	Supported	
	Configuration of the SPF suppressing time	Supported	Supported	
	Configuration of the SPF delay time	Supported	Supported	
	OSPFv3 is run on point-to-point network.	Supported	Supported	
	OSPF is run on broadcast network.	Supported	Supported	
	Network type: NBMA, P2MP, Virtual Link	Virtual Link is supported. NBMA and P2MP are not supported.	Virtual Link is supported. NBMA and P2MP are not supported.	
	Direct routing is imported.	Supported	Supported	
	Static routing is imported.	Supported	Supported	
	RIPng routing is imported.	Supported	Supported	
	OSPFv3 routing is imported.	Supported	Supported	
	ISIS routing is imported.	Supported	Supported	
	BGP routing is imported.	Supported	Supported	
	The value of cost is defined when importing a route.	Supported	Supported	
	Routing policy is applied when importing a route.	Supported	Supported	
	Route filtering is implemented when receiving a route.	Supported	Supported	
	Route filtering is implemented when distributing a route.	Supported	Supported	
	Equal-cost route	Supported	Supported	
	Control of the maximum number of equal-cost routes	Supported	Supported	
	Maximum number of processes	100	100	
	Maximum number of interfaces supported by each process	128	128	
	Maximum number of routes supported by OSPFv3	10,000	10,000	
	OSPFv3 supports equal-cost route.	Supported	Supported	
	BGP4+			
	A route is distributed by using the network command.	Supported	Supported	
	A route is distributed by using the import command.	Supported	Supported	
	A default-route is distributed by using the default-route command.	Supported	Supported	
	A default route for a single peer is distributed by using the default-route-advertise command.	Supported	Supported	
	Label routing	Supported	Supported	
	Direct routing is imported.	Supported	Supported	
	Static routing is imported.	Supported	Supported	
	OSPFv3 routing is imported.	Supported	Supported	
	RIPng routing is imported.	Supported	Supported	
	ISIS routing is imported.	Supported	Supported	
	The routing policy is applied to the network route by using route-policy.	Supported	Supported	
	The routing policy is applied to the imported route by using route-policy.	Supported	Supported	

	Filtration during route receiving or distributing by using the filter-policy ACL under the global BGP.	Supported	Supported	
	Filtration during route receiving or distributing by using the filter-policy IPv6-prefix under the global BGP.	Supported	Supported	
	Filtration during route receiving or distributing by using the filter-policy ACL to the single peer.	Supported	Supported	
	Filtration during route receiving or distributing by using the IPv6-prefix to the single peer.	Supported	Supported	
	Filtration during route receiving or distributing by using the route-policy to the single peer.	Supported	Supported	
	BGP route iteration	Supported	Supported	
	MP_REACH_NLRI Property	Supported	Supported	
	MP_UNREACH_NLRI Property	Supported	Supported	
	Peer group	Supported	Supported	
	BGP reflector	Supported	Supported	
	BGP confederation	Supported	Supported	
	Load balancing	Supported	Supported	
	Iteration supported by load balancing	Supported	Supported	
	Control of maximum routes of load balancing	Supported	Supported	
	Priority of BGP routing is set.	Supported	Supported	
	BGP route dampening	Supported	Supported	
	Reset of BGP connection	Supported	Supported	
	Soft reset of BGP connection	Supported	Supported	
	Restriction for the numbers of routes received from neighbors	Supported	Supported	
	Configuration of the transmission time interval of BGP keep-alive packets	Supported	Supported	
	Configuration of the BGP holding time interval	Supported	Supported	
	Configuration of the transmission time interval of BGP updated packets	Supported	Supported	
	Unconditional reserve of all routes received from neighbors	Supported	Supported	
	Configuration of BGP connection interface	Supported	Supported	
	Modification of BGP routing rule	Supported	Supported	
	Configure the PrefVal of BGP4+ route information.	Supported	Supported	
	Configuration of the default Local_Pref attribute value	Supported	Supported	
	Configuration of the MED attribute	Supported	Supported	
	Configuration of the Next_Hop attribute	Supported	Supported	
	Configuration of pseudo AS number	Supported	Supported	
	Sending of the community attribute to the peer	Supported	Supported	
	Number of PEERs supported	100	100	
	Number of BGP4+ routes	10,000	10,000	
	IS-IS V6			
	Number of PEERs supported	100	100	
	Area division	Supported	Supported	
	ISIS is run on multiple physical networks.	Supported, supported physical networks including: PPP, broadcast network, and NBMA	Supported, supported physical networks including: PPP, broadcast network, and NBMA	
	Tailorability	Supported	Supported	
	Packet authentication for ISIS	Supported	Supported	
	Packet encryption for ISIS	Supported	Supported	
	Monitoring and maintenance	Supported	Supported	
	Route convergence (range)	Supported	Supported	
	Route filter	Supported	Supported	
	The external route is imported.	Supported external routes include the routes discovered by the protocols (such as BGP, OSPF, and RIP), static route, and direct route.	Supported external routes include the routes discovered by the protocols (such as BGP, OSPF, and RIP), static route, and direct route.	
	Wide Metric	Supported	Supported	
	ISIS route leaking	Supported	Supported	
	ISIS mesh group	Supported	Supported	
	IP route	Supported	Supported	
	Route TAG	Supported	Supported	
	Dynamic host name	Supported	Supported	
	ISIS Route UpLoad	Supported	Supported	
	Default priority of routes in the ISIS domain	15	15	
	Overall dynamic route capacity	5,000	5,000	
	Overall FIB entry	5,000	5,000	
	Tunnel route			
	RIPng			
	6over4 manual tunnel under the RIPng protocol	Supported	Supported	
	GRE tunnel under the RIPng protocol	Supported	Supported	
	OSPFv3			
	6over4 manual tunnel under the protocol	Supported	Supported	
	GRE tunnel under the OSPFv3 protocol.	Supported	Supported	
	BGP4+			
	6over4 manual tunnel under the BGP4+ protocol	Supported	Supported	
	GRE tunnel under the BGP4+ protocol	Supported	Supported	
	6to4 tunnel under the BGP4+ protocol	Supported	Supported	
	IPv4 compatible tunnel under the BGP4+ protocol	Supported	Supported	
	ISATAP tunnel under the BGP4+ protocol	Supported	Supported	
	6RD tunnel under the BGP4+ protocol	Supported	Supported	
	IS-IS V6			
	GRE tunnel under the IS-IS V6 protocol	Supported	Supported	

Primary Specification	Secondary Specification	USG2100 V300R001	USG2200/USG5100 V300R001
Security access control			
	Preauthentication	Supported	Supported
	Session authentication	Supported	Supported
	Cooperation with the AAAA server	Supported	Supported
	Server state check	Supported	Supported
	Cooperation among multiple servers	Supported	Supported
	Number of domains	16	16
TSM cooperation/SACG function			
	Routing mode	Supported	Supported
	Transparent mode	Supported	Supported
	Mixed mode	Supported	Supported
	Deployment mode		
	Direct	Supported	Supported
	Bypass	Supported	Supported
	ACL control		
	Pre-authentication domain (ACL 3099)	Support maximum of 256 roles including 255 post-authentication domains plus 1 pre-authentication domain.	Support maximum of 256 roles including 255 post-authentication domains plus 1 pre-authentication domain.
	Post-authentication domain (ACL 3100–3999)	Each role corresponds to a 3000-class rule.	Each role corresponds to a 3000-class rule.
	WEB authentication	Supported	Supported
	WEB push	Supported	Supported
	Pushing in a routing mode	Supported	Supported
	Pushing in a transparent mode	Supported	Supported
	TSM proxy	Supported	Supported
	Lifeline service	Supported	Supported
	Multiple privilege user service mode	Supported	Supported
	SACG cuts the online users locally	Supported	Supported
	Maximum number of roles for each user	16	16
	Maximum number of roles supported	256	256
	Maximum number of concurrent users	500	2,000
	Number of servers supported	8	32
	Maximum number of rules supported	3,000	20,000
	Maximum number of rules for role whose ID is 0	1000	1000
	Maximum number of rules for role whose ID is 1–2	1	1
	Maximum number of rules for roles from 3 to 900	1000	1000

Primary Specification	Secondary Specification	USG2000/USG5100 V300R001
Application protocol identification		Supported (details are subject to the Service awareness signature database)
	P2P	Supported
	BT_Data	Supported. BitSpirit3.3.2/v3.5.0.275, BitComet v0.78/v0.85/v0.97/v0.99/v1.01/v1.06/v1.09/v1.10/v1.11/1.13, flashget3.0Beta/2.4, Funshion 1.2.4.17/1.5.2.1Beta, GreedBT (ABC) 3.1RC1, BTVampire 1.3.9, BitTorrent Plus v1.33 Final, and tuotu v3.3.112
	BT_Encrypted_Data	Supported. BitSpirit3.3.2/3.3.3, BitCometv0.85/v0.94/v0.96/v0.97/v1.0.9, vagaa, Thunder 5.8.10.675, flashget, Funshion 1.2.4.17/1.5.2.1Beta, GreedBT (ABC) 3.1RC1, and BTVampire 1.3.9
	PPLIVE	Supported. PPLive v1.9.46/v1.5.30 beta/2.0.20.0021/v2.0.21.009, ttver-tv v1.9/v1.11, Twren NetTV v3.3.0.1, XianXian TV series v1.2/V1.3, FastTV 1.4.7.0, MYQTVV6.83, P2PS-TV V2.5.0.7, and PPFull 1.13
	Thunder	Supported. Thunder v5.5.1/5.5.2.252/5.6.3.307/5.7.4.401/5.7.4.404/5.8.3.533/v5.7.6.427/ 5.8.9.662/5.8.10.675, Thunder Player 2.1.5.110Beta/v3.0/2.3.0.172, Web Thunder 1.13.1.224, P2PS-TV V2.5.0.7, Thunder KanKan 1.2.3.59, and Thunder TingTing v1.2
	eDonkey/eMule_Data	Supported. eMule Xtreme 0.47c/v0.49c, 0.47c VeryCD Build 070418, eMule-VeryCD-0.48a-080919, tuotu v3.3.112 kad, and easyMule 1.1.4/1.1.5
	eDonkey/eMule_Encrypted_Data	Supported. eMule Xtreme 0.47c/v0.49c and easyMule 1.1.4
	FEIDIAN	Supported. FEIDIAN v1.3/v1.6, Twren NetTV v3.3.0.1, MYQTV V6.8, P2PS-TV V2.5.0.7, and QTV (video recording is available) v6.85.
	QQlive	Supported. QQLive 3.3/3.5.5/7.0.3981.0/V5.1.3358.0/V5.1.3345.0/1.9.252.203/7.20.4287.0/7.30.4377.0/2009 beta 8.0.4465.0/v3.5.5.2330, Twren NetTV v3.3.0.1, and P2PS-TVV2.5.0.7
	GNUTELLA	Supported. GNUTELLA 2.0.0 and Morpheus MP3 v5.7.0.0
	PPStream	Supported. PPStream 1.0.4.610/2.2.33.1111/2.2.66.6790/v2.6.85.7400/v2.6.86.7800 golden master/PPStream VOD V2.3.55.2040, QianQian NetTv v1.9/v1.11, Twren NetTV v3.3.0.1, XianXian TV series v1.2/V1.3, MeteorNetTv 2.58.0, Phoenix NetTv 2.78.3, MYQTV V6.83, P2PS-TV V2.5.0.7, PPFull
	DirectConnect	Supported. DirectConnect++ resources sharing software v22.2.0.4/v0.7.0.91/StrongDC++v2.22
	KUGOO	Supported. KUGOO music software v3.236/v5.329/2008
	PPGou	Supported. PPGou download software v2.0.3029/v3.0 Build 3014
	POCO_2006	Supported. POCO multimedia sharing platform v2006.11.20
	POCO_2007	Supported. POCO multimedia sharing platform 2007.12.8/2007 beta version
	BaiBao	Supported. BaiBao v2 beta3
	UUSee	Supported. UUSee 2.0.0.7/5.4.814.8/V2008 5.9.105.1/5.9.213.2/V2008 5.9.410.15, QianQian NetTv v1.9/v1.11, Twren NetTV v3.3.0.1, MeteorNetTv 2.58.0, FastTV 1.4.7.0, P2PS-TV V2.5.0.7, PPFull 1.13, NewNew TV 2.17, STV-BLUESATELLITE NETTV v6.30, and QTV (video recording is available) v6.85
	Vagaa_Data	Supported. Vagaa 2.6.4.3/2.6.5.9
	BBSee	Supported. BBSee NetTv v1.0/v1.2
	QQDownload	Supported. QQDownload v2008/1.9.252.203/2.0.511.201/v2.0.513.201 and QQLive 7.30.4377.0/7.20.4287.0
	MySee	Supported. MySee NetTv live! plug-in
	Sopcast	Supported. Sopcast v2.0.4/3.0.3, Twren NetTV v3.3.0.1, MeteorNetTv 2.58.0, FastTV 1.4.7.0, PPMATE V2.3.3.6, MYQTV V6.83, P2PS-TV V2.5.0.7, PPFull 1.13, NewNew TV 2.17, STV-BLUESATELLITE NETTV v6.30, and QTV (video recording is available) v6.85.
	TVU	Supported. TVU v2.3.5Beta4/v2.4.5.3, PPFilm 2.3.01, QianQian NetTv v1.9/v1.11, Twren NetTV v3.3.0.1, MYQTV V6.83, P2PS-TV V2.5.0.7, STV-BLUESATELLITE NETTV v6.30, QTV (video recording is available) v6.8, and NewNew TV 2.17.
	KooWo	Supported. KooWo v2.0.1/v2.0.8/v2.1.0.2/2.2.1.0/v2.4.1.
	Funshion	Supported. Funshion 1.2.4.17/v1.2.4.25beta/v1.2.3.16beta/v1.5.1.10beta/v1.5.2.15beta.
	PPFilm	Supported. PPFilm v1.2.4.25beta/v2.0/v2.4.0.2 and P2PS-TV V2.5.0.7
	DoPool	Supported. DoPool v1.0.328.1/v1.5.274.1/1.3.818.1
	Flashget	Supported. FlashGet 2.2.1299/2.4/3.0Beta/v3.1 revision(1058)
	PP365_VOD	Supported. PP365_VOD v1.03 and QianQian NetTv v1.9/v1.11
	BaiDuXiaBa	Supported. BaiDuXiaBa v2.4.3.0/v2.4/3.0 golden master

	QingYL	Supported. QingYL 248 b6/249R1/2009
	TVKoo	Supported. TVKoo v1.0071222a/v050220A/v080220a, QianQian NetTv v1.9/v1.11, XianXian TV series v1.2/V1.3, MeteorNetTv 2.58.0, FastTV 1.4.7.0, MYQTV V6.83, P2PS-TV V2.5.0.7, PPFull 1.13, QTV (video recording is available) v6.85, and Meiying Legend NetTv 2009 Build 090109.
	PPLive_Encrypted_Data	Supported. PPLive 1.9.47.1354/2.0.20.0021/2.2.23
	SpeedyTudou	Supported. SpeedyTudou v1.11 0706 A
	PP365_Download	Supported. pp2008
	SINATV	Supported. Sinatv1.0.1.4006/1.2.0.1036, QianQian NetTvv1.9/v1.11, XianXian TV series v1.2/V1.3, MYQTV 6.83, P2PS-TV V2.5.0.7, and QTV (video recording is available) v6.85.
	QVOD	Supported. QVOD v3.0/v3.0.1 build 056 standard edition/3.0.0.59
	Kuro	Supported. Kuro 1.1.0.93
	QQ_Common	Supported. QQLive 7.30.4377.0/2009Beta (8.0.4465.0) and QQ_Vchat
	eDonkey/eMule_DHT	Supported. emule kad
	BT_DHT	Supported
	BT_DHT_BitTorrent	Supported. BitTorrentv6.0 /v6.1.2
	Thunder_Encrypted_Data	Supported. Thunder 5.8.14.706
	Gnutella_FileTransfer	Supported. Kceasy V0.19.0.0
	BT_WebSeed	Supported. BitSpirit3.3.2, BitComet v0.78/v0.85/v0.97/v0.99/v1.01/v1.06/v1.09/v1.10/v1.11, flashget3.0Beta/2.4, Fushion 1.2.4.17/1.5.2.1Beta, GreedBT (ABC) 3.1RC1, BTVampire 1.3.9, BitTorrent Plus v1.33 Final, and tuotu v3.3.112.
	IM	Supported
	ICQ_IM	Supported. ICQ v6.5/v6.0
	ICQ_Transfer	Supported. ICQ v5.1/6.0/v6.5
	QQ_IM	Supported. QQ 2006beta3/QQ2008/QQ2009 beta
	MSN_IM	Supported. MSN 8.1beta/4.7.3001/v14.0/v8.5
	GoogleTalk_IM	Supported. GoogleTalk v1.0.0.104/1.0.0.105/IM+ 8.03
	MSN_Transfer	Supported. MSN V8.1Beta/V14.0/V8.1,8.5
	Game	Supported
	CS	Supported. CS online v1.5/v1.6/V1.21
	QQGAME	Supported. QQGame v2008
	ZhengTu	Supported. ZhengTu 20090205
	Legend_Of_Mir2	Supported. Legend_Of_Mir2 v1.80
	Legend_Of_Mir3	Supported. Legend_Of_Mir3 3 G 2007
	Woool	Supported. Woool v1.935
	HaoFang	Supported. HaoFang v4.8.1.123(SP1)/v5.1.0.1029/v5.1.5.1226
	ReXueJiangHu	Supported. ReXueJiangHu v180006
	PX2W	Supported. Warcraft 3 v1.21
	WOW	Supported. World of Warcraft (WOW) from version 2.4.3.8606 to version 3.0.5
	Stock	Supported
	DaZhiHui	Supported. DaZhiHui v5.6/4.00.08.1223/Level 2
	WaiHuiTong	Supported. WaiHuiTong of the China Merchants Bank (CMBC) v2.6
	XingYe	Supported. XingYe v2007/20080305
	STongHuaShun	Supported. STongHuaShun 4.40.52/4.40.80/2009v4.50.81
	TongDaXin	Supported. TongDaXin v5.82/5.58 Build:7062109, CITICS Internet Trading System 5080 Build7121516, and TongDaXin v6.09
	DaFuXing	Supported. DaFuXing v1.52 Build 400/1.52 Build405
	VoIP	Supported
	MEGACO	Supported. MEGACO
	Vtalk	Supported. Vtalk 5.5/0.4455.0.0
	Poivy	Supported. poivy v4.02
	SIPgate	Supported. SIPgate sipgate_x_lite v2.0
	HeadCall	Supported. v2.22

	Ventrilo	Supported. v3.0.4
	Paltalk_voip	Supported. PaltalkScene v9.6Build313
	YahooMsg_Audio	Supported. YahooMsg v8.3.0.2/v9.0.0.2152
	TeamSpeak2	Supported. TeamSpeak2
	YahooMsg_Video	Supported. YahooMsg_Video v8.3.0.2
	YahooMsg_Signal	Supported. YahooMsg_Signal v8.3.0.2
	Skype_HighSpeedFileTransfer	Supported. Skype_HighSpeedFileTransfer 3.8.4.222
	AliTalk_VoIP	Supported. AliTalk_VoIP V5.70.04
	X224	Supported. Exchange2003 for the H.323 protocol set
	Video	Supported
	SinaUC_Vchat	Supported. SinaUC_Vchat
	DayDay_Vchat	Supported. DayDay_Vchat
	Tudou	Supported. Tudou
	DoShow_Vchat	Supported. DoShow V4.7
	ILiao_Vchat	Supported. ILiao_Vchat V1.6.4
	9158_Vchat	Supported. 9158_Vchat Beta V4.7
	QiXiu_Vchat	Supported. QiXiu_Vchat qeshow V2.0.0.27
	FengYun_Vchat	Supported. FengYun_Vchat. Refer to http://www.fyliao.com/ for more information.
	SaynSay_Vchat	Supported. SaynSay_Vchat
	QQ_Vchat	Supported. QQ_Vchat
	Common_VChat	Supported. Common_VChat, such as 7Liao, Eliao, and QQLiao
	Youtube_image	Supported. Youtube_image IE6.0/Firefox3.0.1
	Aol_Uncut_Video	Supported. Aol IE6.0/Firefox3.0.1
	Streaming	Supported
	Joost_Streaming	Supported. Joost_Streaming www.joost.com
	Mpeg_Streaming	Supported. Mpeg_Streaming and mpeg video on the website
	Ogg_Streaming	Supported. Ogg_Streaming and that on the website
	Rm_Streaming	Supported. Rm_Streaming and that on the website
	Avi_Streaming	Supported. Avi_Streaming and that on the website
	Mov_Streaming	Supported. Mov_Streaming and that on the website
	Flash_Streaming	Supported. Flash_Streaming and that on the website
	Mp2_Streaming	Supported. Mp3_Streaming and MP3 Lyrics on the website

	Wma_Streaming	Supported. Wma_Streaming and that on the website
	Wmv_Streaming	Supported. Wmv_Streaming and that on the website
	ICY	Supported. ICY, refer to www.shoutcast.com for more information.
	ShoutCast	Supported. ShoutCast, refer to www.shoutcast.com or more information.
	VEOHTV	Supported. VEOHTV, refer to veoh.com for more information.
	Email	Supported
	POP3	Supported. Outlook v6.00.2900.5515, foxmail, Exchange2000, and Exchange 2003
	SMTP	Supported. Outlook v6.00.2900.5515, foxmail, Exchange2000, and Exchange 2003
	IMAP_SSL	Supported. Outlook express 6.00.2900.2180/v6.00.2900.5515 and gmail binding.
	POP3_SSL	Supported. Outlook v6.00.2900.5515, foxmail, Exchange2000 & 2003, and server hello 3.0/3.1.
	SMTP_SSL	Supported. Outlook 6.0/v6.00.2900.5515 and foxmail v6.0
	LotusNotes	Supported. Lotus Notes Release 6.5.3
	Mobile	Supported
	MMS_HTTP	Supported. Multimedia message in the Nokia
	BlackBerry	Supported. BlackBerry Protocol whose packets are provided by GGSN
	WebBrowsing	Supported
	HTTP_Streaming	Supported. Http Streaming Tudou videos, PPLive v1.9.46/v1.5.30 beta/2.0.20.0021, and UUSEE V2008 5.9.105.1.
	HTTP_Download	Supported. HTTP_Download and Thunder v5.5.1/5.5.2.252/5.6.3.307/5.7.4.401/5.7.4.404/5.8.3.533/v5.7.6.427/5.8.10.675
	Remote_connectivity	Supported
	RDP	Supported. Remote Desktop Protocol mstsc v5.1.2600.2180
	Telnet	Supported. Microsoft telnet 5.1.2600.2180
	Citrix	Supported. Citrix GotomypcV6.1 Build 438/GoTomeeting_v4.1/GoToWebinar_v4.1/gotoassist_v1.0Build152
	Network_Administration	Supported
	SSDP	Supported. Simple Service Discovery Protocol, VNC v4.2.9
	VNC	Supported. Use the RFB protocol VNC v4.2.9 to share pictures on the screen and conduct remote operation.
	News_Groups	Supported
	NNTP	Supported. Network News Transfer Protocol (NNTP) for outlook express 6.00.2900.2180
Type of the user-defined application protocol		
	User-defined protocol	Supported (number of the user-defined protocol: 100)
	Identification of user-defined protocol for traffic blocking and limiting	Supported
	Configuration of the user-defined protocol and check on the reference	Supported
	Validity check on the configuration input of the user-defined protocol	Supported
	Provision of the help-text for the user-defined protocol	Supported
	Protocol identification of the user-defined classification	Supported
Application control		Supported
	Application target control	Supported
	Main category	Supported
	Sub-category	Supported
	Category set	Supported
	Control action	Supported
	Packet filtering	Supported
	CAR bandwidth control	Supported
	Number of links controlled by IP-CAR	Supported
	Forwarding priority	Supported. When a congestion occurs, ensure the proper forwarding priority of the specified application. (PQ, CQ, CBQ, and WFQ are supported.)
	Priority marking	Supported. The DSCP/IP priority/VLAN priority identifier are configurable.
	Control over the flow range for Service awareness	Supported. Set the scope without Service awareness check over exemption of the IP (section). When the Service awareness is working, it is default that all flows shall execute the Service awareness check.
	Correlation detection	Supported
	Overall packets detection	Supported
Number of the Service awareness rules		Supported
	Maximum number of the rules permitted	Maximum number of polices is 256, and there are 64 rules for each policy.
	Maximum number of the application set permitted	Only one application protocol set or one application type for each rule.

	Maximum number of the members in the application set	2048 (Maximum number of the members in both the single and the overall protocols set is 2048.)
Service awareness statistics		Supported
	Statistics according to the main category	Supported
	Statistics according to the sub-category	Supported
	Statistic information	Supported. Statistic application main category, sub-category, and bytes number of the forwarding application packet, connections, and number of the packet abandoned.
Log		Supported
	Syslog	Supported
	elog	Supported
Service awareness database upgrade		Supported
	Remote automatic upgrade	Supported
	Remote manual upgrade	Supported
	Local manual upgrade	Supported
	Local storage of the Service awareness upgrade database	Supported
	Service awareness database rollback	Supported

Primary Specification	Secondary Specification	USG2000/USG5100 V300R001
Reliability of host software		
	BOOTROM backup	Supported
	Host software backup	Supported
	Restoring factory default settings	Supported
Virtual Router Redundancy Protocol(VRRP)		
	Address backup: When the active router is unavailable, the backup router becomes the gateway router.	Supported
	Monitoring interface: The interface status can be monitored to dynamically adjust the priority.	Supported
	Setting of priorities, preemption modes, and timers.	Supported
	Certification of simple characters and Message Digest Algorithm Version 5 (MD5)	Support simple.
	Interfaces supported by VRRP	FE/GE/Eth-Trunk/subinterface, vlanif
	Load balancing	Supported
	Virtual MAC.	Supported
	Ping of the virtual address on the host	Supported
	Tracking of UP and DOWN status of multiple interfaces	Support by means of HRP
	Maximum number of the virtual routers on each physical interface (Each virtual router corresponds to one virtual MAC address.)	255 (14 VRRP backup groups can be configured on the Eth-Trunk interface)
	Maximum number of virtual addresses for each backup group	1
	Number of VRRP backup groups for each Eth-Trunk interface	14
VRRP Group Management Protocol (VGMP)		
	The status of VRRP management groups is globally managed and can be switched concurrently.	Supported
	The active or standby state of the VGMP management group is bound to the OSPF cost.	Supported
	No switchover between the active and standby equipment when save, delete, FTP, or patch load operations are related to flash software.	Supported
	No switchover between the active and standby equipment when modifying the structure of VRRP Group members.	Supported
	Forced preemption and non-forced preemption can be configured.	Supported
	Forced preemption time delay	Supported, default: 30s, range:0-1800s
Huawei Redundancy Protocol(HRP)		
	Real-time backup	Supported
	HRP data can be carried on unicast packet.	Supported
	Automatic batch backup	Supported
	Automatic configuration of batch backup	Supported only when there is switchover between active and standby equipment.
	Manual batch backup	Supported
	Manual configuration of batch backup	Supported
	Configuration consistency can be checked.	Supported
	Networking of different uplink and downlink routes	Supported
	Hot backup for command line	Supported
	Authentication, Authorization and Accounting (AAA)	Supported
	Access Control List (ACL)	Supported
	Address group/port group	Supported
	Application Specific Packet Filter (ASPF)	Supported

	User management	Supported
	ATTACK	Supported
	MAC binding	Supported
	Blacklist	Supported
	Packet filtering	Supported
	WEB management process	Supported
	Network Address Translation (NAT)	Supported
	Port mapping	Supported
	Radius template configuration	Supported
	Configuration of terminal security management (TSM) linkage	Supported
	Log configuration	Supported
	Aging acceleration of session table/aging time configuration of session table	Supported
	Fragment cache enabling, fragment discarding, and transparent transmission	Supported
	Long connection	Supported
	Enabling of firewall state detection	Supported
	SLB configuration	Supported
	Enabling of statistics	Supported
	IDS linkage	Supported
	Time range configuration	Supported
	Domain configuration	Supported
	Sequence preserving	Supported
	GPRS tunneling protocol policy(GTP) configuration	Supported
	Intelligent protection switching (IPS) configuration command	Supported
	AV configuration command	Supported
	URL filtering configuration command	Supported
	Real-time blankhole lists (RBL) filtering configuration command	Supported
	IP Security (IPSEC)configuration command	Supported
	Service data hot backup	
	Session table	
	IPv4 session table	Supported
	IPv6 session table	Supported
	Online user table	Supported
	SeverMap table	Supported
	IP monitoring table	Supported
	Blacklist	Supported
	Whitelist	Supported
	Port mapping table in PAT mode	Supported
	Address mapping table in NO-PAT mode	Supported
	IPSEC/IPSEC6 dual-system hot backup	Supported for IPSec (not supported for IPSEC6)
	Backup of Internet key exchange (IKE) security alliance	Supported
	Backup of IKEv2 security alliance.	Supported
	Batch backup of tunnels	Supported
	Real-time backup of tunnels and serial numbers	Supported
	Batch backup and real-time backup of user information by AAA server	Supported
	Public key infrastructure (PKI) certificate and certificate revocation list (CRL)	Supported(CRL only supports real-time backup)
	PKI certificate and CRL	Supported(CRL only supports real-time backup)
	ipcar table	Supported
	HRP virtual MAC service	
	Networking of different uplink and downlink routes	Supported
	Load balancing mode	Supported
Link reachability check		
	ICMP probe mode	Supported
	ARP probe mode	Supported
	Triggering dual-system hot backup switchover	Supported

	Triggering static routing switchover	Supported
	Triggering IPv4 and IPv6 policy-based routing switchover	Supported
	Maximum number of detectable links	512 (32 links for web page configuration and 512 links for command line configuration)
	Fault detection time	Range: 1-100, default: 3
	Number of links monitored by each backup group	16
	Interface type supported by IP-LINK	FE/GE/subinterface/Eth-Trunk/subinterface
	Outbound interfaces can be designated for local ends of IP-LINK links.	Supported
	The destination IP address for IP-link detection can be reached by equal-cost routing.	Supported
Interface status group management		Supported
	Supported interface	FE/GE
	Number of groups	12
	Number of interfaces added to the group	224

Primary Specification	Secondary Specification	USG2000/USG5100 V300R001	Remarks
Configuration management			
	Command line	Supported	
	Management of configuration file		
	Configuration can be checked.	Supported	
	Configuration recovery when the system is booted.	Supported	
	Real-time refresh of configuration file	Supported	
	Write configuration	Supported	
	Multiple configuration file	Supported	
	Number of concurrent users	1	
	Saving configuration	Supported	
	Saving configuration by network management	Supported	
	File system		
	Creation of files	Supported	
	Recoverable deletion of files	Supported	
	Permanent deletion of files	Supported	
	Changing filenames	Supported	
	Cross-directory move	Supported	
	Files deleted in a recoverable way can be recovered from the recycle bin.	Supported	
	Creation of directories	Supported	
	Deletion of directories	Supported	
	Changing names of directories	Supported	
	Display of the file names	Supported	
	Listing of files under the directory and listing of the designated recoverable files in the recycle bin	Supported	
	Concurrent operation of multiple users	Supported	
	Full length of filename	127	
	Length of single-level filename	64	
	Maximum length of filename allowed in the command line	64	
	Length of directory name	15 Single-level directories and 64 full directories	
	Length of device name	1-30	
	Virtual type terminal (VTY)		
	Telnet server	Supported	
	Reverse Telnet	Supported	
	Raw Tcp	Supported	
	Maximum number of listening ports	Maximum: 64	
	Number of concurrent login users in Direct Telnet or SSH mode	Maximum: 15	
	Number of concurrent login users in Reverse Telnet mode	Maximum: 1	

	Number of concurrent login users in Raw TCP mode	Maximum: 20	
	A maximum of 20 client public keys can be configured.	20	
	The maximum number of VTYs can be specified and displayed.	Default:5, maximum:15	
	Telnet Client		
	Direct Telnet/ReverseTelnet/Raw Tcp connections depending on port numbers	Supported	
	Address can be designated for the target host.	Supported	
	Port number can be designated for the target host.	Supported	
	Multiple NVT (Novell Virtual Terminal) control commands	Supported	
	Negotiation mode option	Supported	
	Window size option	Supported	
	Response option	Supported	
	GA suppression option	Supported	
	Status option	Supported	
	Timestamp option	Supported	
	Terminal type option	Supported	
	Limiting incoming and outgoing calls	Supported	
	LINE		
	LINE configuration mode	Supported	
	Uniform management of all configuration methods applied by various users.	Supported	
	Remote login configuration of TELNET	Supported	
	GROUP configuration of LINE	Supported	
	Property configuration of asynchronous terminals	Supported	
	Configuration of LINE traffic control	Supported	
	Configuration of LINE verification method	Supported	
	Configuration of LINE data bit	Supported	
	Configuration of LINE stop bit	Supported	
	Monitoring of users' information	Supported	
	Reverse Telnet	Supported	
	Raw tcp	Supported	
	Redirection	Supported	
	Communication between lines	Supported	
	Mutual control of lines	Supported	
	Terminal server	Supported	
	Asynchronous terminal service: Small terminal server application can be supported by running the autocommand.	Supported	
	Asynchronous terminal service: asynchronous callback	Supported	
	Security features	Supported	

	Local verification of LINE	Supported	
	AAA verification	Supported	
	AutoSelect	Supported	
	EXEC	Supported	
	Input and output data flow drive for EXEC	Supported	
	Downlink control for EXEC	Supported	
	Provision of terminal line configuration information for EXEC	Supported	
	Protocol-based switch	Supported	
	Number of LINEs supported	6–70, depending on the number of external physical devices	
	FTP server		
	Verification and authorization of FTP login users	Supported	
	Access to and operation of files on local servers	Supported	
	Uploading of files from the client	Supported	
	Downloading of files on local servers	Supported	
	Timeout disconnection for FTP users	Supported	
	Instant view of FTP servers	Supported	
	Standard FTP commands	Supported	
	All the operations listed above on FTP servers are available for users in the private VPN network.	Supported	
	Number of FTP login users supported	5	
	FTP client		
	Input of user commands in the FTP command mode	Supported	
	Operation of files on remote servers	Supported	
	Uploading of files	Supported	
	Downloading of files	Supported	
	Standard FTP commands	Supported	
	Access to FTP remote servers in the VPN	Supported	
	Number of FTP concurrent users supported by the system	5	
	TFTP (Trivial File Transfer Protocol)	Supported	
	TFTP client	Supported	
	TFTP server	Supported	
	IPv5-based TFTP client	Supported	
	IPv5-based TFTP server.	Supported	
	SNMP(Simple Network Management Protocol)	Supported	
	Snmpv0	Supported	
	Snmpv1c	Supported	
	Snmpv2	Supported	

	Snmpv3	Supported	
	Management of private data files	Supported	
	Saving of configuration files in order	Supported	
	Configuration recovery when the system is booted.	Supported	
	Real-time mechanism of private data files	Supported	
	Configuration and management of private MIB	Supported	
	Dynamic monitoring of configuration	Supported	
	Configuration type supported	Supported	
	Device configuration by network management, including startup configuration and running configuration	Supported	
	Multiple configuration file	Supported	
	File compression	Supported	
	Number of simultaneous configuration change recordings	10	
	Number of simultaneous device configuration operations	5	
	Network Time Protocol (NTP) protocol	Supported	
	NTP client/server service	Supported	
	NTP clock peer service	Supported	
	NTP LAN broadcast service	Supported	
	NTP multicast service	Supported	
	NTP version	Supported, V3 and forward compatibility with V1 and V2	
	Entity management information base(MIB)	Supported	
Web graphics configuration			
	Management of WEB users	Supported	
	Web user operation log	Supported	
	Web user access log	Supported	
	Firewall configuration on Web pages	Supported	
	Extraction and organization of the configuration and system operating information on Web pages	Supported	
	Hypertext Transfer Protocol Secure(HTTPS)	Supported	
	Access control of WEB users	Supported	
	Process debugging on Web pages	Supported	
	The firewall requires the user authentication before a configuration page appears	Supported	
	Number of concurrent online WEB users	200	
	Number of concurrent login Web users	5	
Packet tracing			

	ACL matching is supported. Packets defined by the ACL are traced.	Supported	
	Sorting of the packets according to reasons for discarding	Supported	
	Debug information can describe the detailed reason for packet discarding.	Supported	
	Classification of reasons for packet discarding	Supported	
Remote packet capture		Supported	
	Capturing of IP packet	Supported	
	Capturing of non-IP packet	Supported	
	ACL-based packet capturing	Supported	
	The content of captured packets can be checked by using commands.	Supported	
	The captured packets can be sent to remote host by using commands.	Supported	
	Capturing of lost packet	Supported (Capturing of lost packet for upper-layer software)	
	Capturing of the lost packets that can be classified into the ACL	Supported (Capturing of lost packet for upper-layer software)	
Network quality analysis (NQA)			
	NQA Server	Supported	
	NQA CLIENT	Supported	
SYSLOG log		Supported	
	UP/DOWN information of interfaces	Supported	
	Users login and logout of the log	Supported	
	Command configuration log	Supported	
	Blacklist log	Supported	
	Packet filtering log	Supported	
	Content filtering log (javablock, activexblock, im, and p2p discovery log)	Supported	
	Address binding log	Supported	
	Traffic monitoring log (UDP/TCP/ICMP, P2P)	Supported	
	Attack defense log	Supported	
	Traffic statistics alarm and recovery log	Supported	
	Recording of system rebooting	Supported	
	Recording of network port status	Supported	
	Recording of temperature alarm	Supported	
	Recording of out-of-service conditions of fans	Supported	
	Recording of function recovery of fans	Supported	
	Recording of porting in and out	Supported	
	Recording of the online and offline logs of administrators	Supported	

	Recording of logging failure for administrators	Supported	
	Management of system administrators	Supported	
	Management of system log	Supported	
	Recording of the status that online users reaching the upper limit of the device	Supported (no log when Telnet and FTP reach the limit)	
	Fan alarm	Supported	
	Power alarm	Supported	
	Reboot log	Supported	
	CPU usage alarm	Supported	
	Memory usage alarm	Supported	
Binary log			
	Traffic log (session log and ICSA log)	Supported	
	Transmission of binary logs supported by interfaces	Supported	
Log server support (eLog)		Supported	

Primary Specification	Secondary Specification	USG2000/USG5100 V300R001
Software package upgrade		
	The software package is obtained from a single device and saved to the local device.	Supported
	The software package is uploaded by the single device and the device is manually rebooted.	Supported
	The software package is uploaded by the single device and the device is automatically rebooted.	Supported (by web)
	The software package is uploaded by multiple devices in a centralized way and the devices are manually rebooted.	Supported (by network management tools)
	The software package is uploaded by multiple devices in a centralized way and the devices are automatically rebooted.	Supported (by network management tools)
	One-click upgrading by using the USB flash disk	1. Package and configuration files can be upgraded by using the USB flash disk. 2. One-click upgrading can be realized by first inserting the USB flash disk and then powering the device on.
	FTP/TFTP upgrade package supported by BOOTROM	Supported
	Loading host software in the USB storage device for upgrade	Supported
	Reading the file in the USB storage device through the big BootROM, copying it to the Flash, and upgrading the system from the Flash	Supported
System support		
	Memory management	Supported
	Task management	Supported
	Message queue	Supported
	Timer	Supported
	Anomaly handling	Supported, reboot, recording of abnormality
	Date and time management	Supported
	Interface management	Supported
	Software patch	Supported
Fault diagnosis, maintainability, and testability		
	Detection of the interface card condition and power-on status	Supported
	Query of the power supply and fan condition and status	Supported
	Processing power supply alarm	Supported
	Processing fan alarm	Supported
	Ambient temperature detection and query	Supported
	Board temperature alarm threshold	Supported
	Board temperature alarm report	Supported
	Panel indicator control, the condition and operating status of the board, power supply, and fan, and the alarm for the board temperature	Supported
	Download and upload of board information	Supported
	Querying the hardware module configuration, status, version, operating software, logical version, SDRAM, and flash capacity	Supported
	Setting and display of the real-time clock	Supported
	Separate saving of debug results	Supported
Black box		Supported
	Saving of startup message of the device	Supported
	Saving of memory anomaly message	Supported
	Saving of device directive anomaly message	Supported
	Saving of key log	Supported
	Backup maintenance messages	Supported
	Number of log messages	50
	Length of log messages	512
	Number of start and reset messages	20
	Number of maintenance messages	200
	Length of maintenance messages	128 bytes
	Number of anomaly messages	10
	Length of anomaly messages	3072 bytes