



Firmware Release Note

P-335U

Release 3.60(AMB.1)C0

Date: Nov 14, 2006
Author: Hubert Jin

ZyXEL P-335U Standard Version release 3.60(AMB.1)C0 Release Note

Date: Nov 14, 2006

Supported Platforms:

ZyXEL P-335U

Versions:

ZyNOS Version: V3.60(AMB.1) | 11/14/2006 13:43:20

Bootbase Version: V1.05 | 04/20/2004 10:36:26

Notes:

1. MSN Video ALG only support with MSN 7.0 above and the default port (1863) should not be changed.
2. Bit Torrent ALG support following tools: BitComet 0.58, BitSpirit v3.1.0, BitLord 1.1, G3 Torrent v0.9999, Aeureus 2.3.0.4, BitTornado T-0.3.12

Known Issues:

1. Allow NetBIOS traffic between WAN & LAN works on limited situations.
2. Even though trigger port rule is removed, these rule still work until time out.
3. MAP doesn't support for this model.
4. WPA-PSK with short RTS/fragment will lead to disassociation
5. STA can't associate with DUT anymore after failed authentication with WPA\WPA2(TTLS-CHAP)
6. 802.11a:RTS/CTS can't work when RTS/CTS value is smaller than the fragmentation threshold value
7. STA with odyssey client using wrong password and CA can still pass the WPA2 authentication once STA passed the WPA2 authentication before.
8. Complex reconfiguration by SPT-GEN may fail in some cases
9. VoIP(SIP) failed on enable Bandwidth MGMT.
10. "SMTP authentication" works failed with some mail servers.
11. Restrict Web Features (including ActiveX, Java, Cookies and Web Proxy) of Content Filter can't work as setting.
12. UPnP whiteboard does not work if you don't choose "Allow users to make configuration changes through UPnP".
13. When server on LAN multicast cannot work until you reboot the device.

CI Command List:

Features:

Modification in 3.60(AMB.1)C0 | 11/14/2006

1. Change to FCS.

Modification in 3.60(AMB.1)b3 | 11/06/2006

2. [BUG FIX]
SPR: 061026960
Symptom: After DHCP off, change device's LAN IP lead to crash .
Condition:
Step1: Default Romfile.
Step2: Off DHCP,then config LAN IP "192.168.1.2" click apply leads to crash

Modification in 3.60(AMB.1)b2 | 10/20/2006

3. [BUG FIX]
SPR: 061009274
Symptom: Content Filter can not block key words which you filled.
Condition:
Content Filter can not block key words which you filled.
4. [BUG FIX]
SPR: 061023725
Symptom: Content filter schedule can not work correctly as you set.
Condition:
Step1: The website will be blocked when you choose "every day to block"
Step2: When you cancel every day to block it still block website, the schedule cannot work as you set.The day to block has the same issue.

Modification in 3.60(AMB.1)b1 | 09/29/2006

1. First Firmware Release Basing On 3.60(AMB.0)C0
2. [FEATURE ENHANCEMENT]
Add VPN Feature

Annex A CI Command List

Last Updated: 2002/11/26

Command Class List Table		
System Related Command	Exit Command	Device Related Command
Ethernet Related Command	POE Related Command	PPTP Related Command
Configuration Related Command	IP Related Command	IPSec Related Command
Firewall Related Command	Wireless LAN Related Command	Bridge Related Command
Radius Related Command	802.1x Related Command	Auto WLAN Security Delivery Command

System Related Command

[Home](#)

Command				Description
sys				
	adjtime			retrive date and time from Internet
	callhist			
	display			display call history
	remove	<index>		remove entry from call history
	countrycode	[countrycode]		set country code
	date	[year month date]		set/display date
	domainname			display domain name
	edit	<filename>		edit a text file
	extraphnum			maintain extra phone numbers for outcalls
	add	<set 1-3> <1 st phone num> [2 nd phone num]		add extra phone numbers
	display			display extra phone numbers
	node	<num>		set all extend phone number to remote node <num>
	remove	<set 1-3>		remove extra phone numbers
	reset			reset flag and mask
	feature			display feature bit
	hostname	[hostname]		display system hostname
	logs			
	category			
		access [0:none/1:log/2:alert/3:both]		record the access control logs
		attack [0:none/1:log/2:alert/3:both]		record and alert the firewall attack logs
		display		display the category setting
		error [0:none/1:log/2:alert/3:both]		record and alert the system error logs
		ipsec [0:none/1:log/2:alert/3:both]		record the access control logs
		ike [0:none/1:log/2:alert/3:both]		record the access control logs
		javablocked [0:none/1:log]		record the java etc. blocked logs
		mten [0:none/1:log]		record the system maintenance logs
		upnp [0:none/1:log]		record upnp logs
		urlblocked [0:none/1:log/2:alert/3:both]		record and alert the web blocked logs
		urlforward [0:none/1:log]		record web forward logs
	clear			clear log
	display	[access attack error ipsec ike javablocked mten urlblocked urlforward]		display all logs or specify category logs
	errlog			
		clear		display log error
		disp		clear log error
		online		turn on/off error log online display
	load			load the log setting buffer

	mail		
		alertAddr [mail address]	send alerts to this mail address
		display	display mail setting
		logAddr [mail address]	send logs to this mail address
		schedule display	display mail schedule
		schedule hour [0-23]	hour time to send the logs
		schedule minute [0-59]	minute time to send the logs
		schedule policy [0:full/1:hourly/2:daily/3:weekly/4:none]	mail schedule policy
		schedule week [0:sun/1:mon/2:tue/3:wed/4:thu/5:fri/6:sat]	weekly time to send the logs
		server [domainName/IP]	mail server to send the logs
		subject [mail subject]	mail subject
	save		save the log setting buffer
	syslog		
		active [0:no/1:yes]	active to enable unix syslog
		display	display syslog setting
		facility [Local ID(1-7)]	log the messages to different files
		server [domainName/IP]	syslog server to send the logs
log			
	clear		clear log error
	disp		display log error
	online	[on off]	turn on/off error log online display
	resolve		Resolve mail server and syslog server address
mbuf			
	link	link	list system mbuf link
	pool	<id> [type]	list system mbuf pool
	status		display system mbuf status
	disp	<address>	display mbuf status
	cnt		
		disp	display system mbuf count
		clear	clear system mbuf count
	debug	[on off]	
pwderrtm		[minute]	Set or display the password error blocking timeout value.
rn			
	load	<entry no.>	load remote node information
	disp	<entry no.>(0:working buffer)	display remote node information
	nat	<none sua full_feature>	config remote node nat
	nailup	<no yes>	config remote node nailup
	mtu	<value>	set remote node mtu
	save	[entry no.]	save remote node information
smt			not support in this product
stdio		[minute]	change terminal timeout value
time		[hour [min [sec]]]	display/set system time
trcdisp			monitor packets
trclog			
trcpacket			
syslog			
	server	[destIP]	set syslog server IP address
	facility	<FacilityNo>	set syslog facility
	type	[type]	set/display syslog type flag

ZyXEL Confidential

	mode	[on/off]	set syslog mode
version			display RAS code and driver version
view		<filename>	view a text file
wdog			
	switch	[on/off]	set on/off wdog
	cnt	[value]	display watchdog counts value: 0-34463
romreset			restore default romfile
server			
	access	<telnet ftp web icmp snmp dns> <value>	set server access type
	load		load server information
	disp		display server information
	port	<telnet ftp web snmp> <port>	set server port
	save		save server information
	secureip	<telnet ftp web icmp snmp dns> <ip>	set server secure ip addr
fwnotify			
	load		load fwnotify entry from spt
	save		save fwnotify entry to spt
	url	<url>	set fwnotify url
	days	<days>	set fwnotify days
	active	<flag>	turn on/off fwnotify flag
	disp		display firmware notify information
	check		check firmware notify event
	debug	<flag>	turn on/off firmware notify debug flag
cmgr			
	trace		
		disp <ch-name>	show the connection trace of this channel
		clear <ch-name>	clear the connection trace of this channel
	cnt	<ch-name>	show channel connection related counter
socket			display system socket information
filter			
	netbios		
roadrunner			
	debug	<level>	enable/disable roadrunner service 0: diable <default> 1: enable
	display	<iface name>	display roadrunner information iface-name: enif0, wanif0
	restart	<iface name>	restart roadrunner
ddns			
	debug	<level>	enable/disable ddns service
	display	<iface name>	display ddns information
	restart	<iface name>	restart ddns
	logout	<iface name>	logout ddns
cpu			
	display		display CPU utilization
filter			
	netbios		
upnp			
	active	[0:no/1:yes]	Activate or deactivate the saved upnp settings
	config	[0:deny/1:permit]	Allow users to make configuration changes. through UPnP
	display		display upnp information
	firewall	[0:deny/1:pass]	Allow UPnP to pass through Firewall.
	load		save upnp information

		save		save upnp information
--	--	------	--	-----------------------

Exit Command

[Home](#)

Command				Description
exit				exit smt menu

Device Related Command

[Home](#)

Command				Description
dev				
	channel			
		drop	<channel_name>	drop channel
	dial		<node#>	dial to remote node

Ethernet Related Command

[Home](#)

Command				Description
ether				
	config			display LAN configuration information
	driver			
		cnt		
			disp <name>	display ether driver counters
			ioctl <ch_name>	Useless in this stage.
			status <ch_name>	see LAN status
	version			see ethernet device type
	pkttest			
			disp	
			packet <level>	set ether test packet display level
			event <ch> [on/off]	turn on/off ether test event display
		sap	[ch_name]	send sap packet
		arp	<ch_name> <ip-addr>	send arp packet to ip-addr
	debug			
			disp <ch_name>	display ethernet debug information
			level <ch_name> <level>	set the ethernet debug level level 0: disable debug log level 1:enable debug log (default)
	edit			
			load <ether no.>	load ether data from spt
			mtu <value>	set ether data mtu
			accessblock <0:disable 1:enable>	block internet access
			save	save ether data to spt

POE Related Command

[Home](#)

Command				Description
poe				
	status		[ch_name]	see poe status
	dial		<node>	dial a remote node
	drop		<node>	drop a pppoe call
	ether		[rfc 3com]	set /display pppoe ether type

PPTP Related Command

[Home](#)

Command				Description
pptp				
	dial		<rn-name>	dial a remote node
	drop		<rn-name>	drop a remote node call
	tunnel		<tunnel id>	display pptp tunnel information

Configuration Related Command

[Home](#)

Command				Description
config				The parameters of config are listed below.
edit	firewall	active <yes no>		Activate or deactivate the saved firewall settings
retrieve	firewall			Retrieve current saved firewall settings
save	firewall			Save the current firewall settings
display	firewall			Displays all the firewall settings
		set <set#>		Display current entries of a set configuration; including timeout values, name, default-permit, and number of rules in the set.
		set <set#>	rule <rule#>	Display current entries of a rule in a set.
		attack		Display all the attack alert settings in PNC
		e-mail		Display all the e-mail settings in PNC
		?		Display all the available sub commands
		e-mail	mail-server <mail server IP>	Edit the mail server IP to send the alert
			return-addr <e-mail address>	Edit the mail address for returning an email alert
			e-mail-to <e-mail address>	Edit the mail address to send the alert
			policy <full hourly daily weekly>	Edit email schedule when log is full or per hour, day, week.
			day <sunday monday tuesday wednesday thursday friday saturday>	Edit the day to send the log when the email policy is set to Weekly
			hour <0~23>	Edit the hour to send the log when the email policy is set to daily or weekly
			minute <0~59>	Edit the minute to send to log when the email policy is set to daily or weekly
			Subject <mail subject>	Edit the email subject
		attack	send-alert <yes no>	Activate or deactivate the firewall DoS attacks notification emails
			block <yes no>	Yes: Block the traffic when exceeds the tcp-max-incomplete threshold
				No: Delete the oldest half-open session when exceeds the tcp-max-incomplete threshold
			block-minute <0~255>	Only valid when sets 'Block' to yes. The unit is minute
			minute-high <0~255>	The threshold to start to delete the old half-opened sessions to minute-low
			minute-low <0~255>	The threshold to stop deleting the old half-opened session
			max-incomplete-high <0~255>	The threshold to start to delete the old half-opened sessions to max-incomplete-low
			max-incomplete-low <0~255>	The threshold to stop deleting the half-opened session
			tcp-max-incomplete <0~255>	The threshold to start executing the block field

		set <set#>	name <desired name>		Edit the name for a set
			default-permit <forward block>		Edit whether a packet is dropped or allowed when it does not match the default set
			icmp-timeout <seconds>		Edit the timeout for an idle ICMP session before it is terminated
			udp-idle-timeout <seconds>		Edit the timeout for an idle UDP session before it is terminated
			connection-timeout <seconds>		Edit the wait time for the SYN TCP sessions before it is terminated
			fin-wait-timeout <seconds>		Edit the wait time for FIN in concluding a TCP session before it is terminated
			tcp-idle-timeout <seconds>		Edit the timeout for an idle TCP session before it is terminated
			pnc <yes no>		PNC is allowed when 'yes' is set even there is a rule to block PNC
			log <yes no>		Switch on/off sending the log for matching the default permit
			rule <rule#>	permit <forward block>	Edit whether a packet is dropped or allowed when it matches this rule
				active <yes no>	Edit whether a rule is enabled or not
				protocol <0~255>	Edit the protocol number for a rule. 1=ICMP, 6=TCP, 17=UDP...
				log <none match not-match both>	Sending a log for a rule when the packet none matches not match both the rule
				alert <yes no>	Activate or deactivate the notification when a DoS attack occurs or there is a violation of any alert settings. In case of such instances, the function will send an email to the SMTP destination address and log an alert.
				srcaddr-single <ip address>	Select and edit a source address of a packet which complies to this rule
				srcaddr-subnet <ip address> <subnet mask>	Select and edit a source address and subnet mask if a packet which complies to this rule.
				srcaddr-range <start ip address> <end ip address>	Select and edit a source address range of a packet which complies to this rule.
				destaddr-single <ip address>	Select and edit a destination address of a packet which complies to this rule
				destaddr-subnet <ip address> <subnet mask>	Select and edit a destination address and subnet mask if a packet which complies to this rule.
				destaddr-range <start ip address> <end ip address>	Select and edit a destination address range of a packet which complies to this rule.
				tcp destport-single <port#>	Select and edit the destination port of a packet which comply to this rule. For non-consecutive port numbers, the user may repeat this command line to enter the multiple port numbers.
				tcp destport-range <start port#> <end port#>	Select and edit a destination port range of a packet which comply to this rule.
				udp destport-single <port#>	Select and edit the destination port of a packet which comply to this rule. For non-consecutive port numbers, users may repeat this command line to enter the multiple port numbers.
				udp destport-range <start port#> <end port#>	Select and edit a destination port range of a packet which comply to this rule.

ZyXEL Confidential

				desport-custom <desired custom port name>	Type in the desired custom port name
delete	firewall	e-mail			Remove all email alert settings
		attack			Reset all alert settings to defaults
		set <set#>			Remove a specified set from the firewall configuration
		set <set#>	rule <rule#>		Remove a specified rule in a set from the firewall configuration
insert	firewall	e-mail			Insert email alert settings
		attack			Insert attack alert settings
		set <set#>			Insert a specified rule set to the firewall configuration
		set <set#>	rule <rule#>		Insert a specified rule in a set to the firewall configuration
cli					Display the choices of command list.
debug	<1 0>				Turn on/off trace for firewall debug information.

Wireless LAN Related Command

[Home](#)

Command				Description
wlan				
	active		[on off]	set on/off wlan
	association			display association list
	chid		[channel id]	set channel
	diagnose			self-diagnostics
	essid		[ess id]	set ESS ID
	version			display WLAN version information

Bridge Related Command

[Home](#)

Command				Description
Bridge				
	cnt			related to bridge routing statistic table
		Disp		display bridge route counter
		Clear		clear bridge route counter
	stat			related to bridge packet statistic table
		Disp		display bridge route packet counter
		Clear		clear bridge route packet counter

Radius Related Command

[Home](#)

Command				Description
Radius				
	auth			show current radius authentication server configuration
	acct			show current radius accounting server configuration

802.1x Related Command

[Home](#)

Command				Description
8021x				
	debug	Level	[debug level]	set ieee802.1x debug message level
		Trace		show all supplications in the supplication table
		User	[username]	show the specified user status in the supplicant table

IP Related Command

[Home](#)

Command			Description
ip			
	address	[addr]	display host ip address
	alias	<iface>	alias iface
	aliasdis	<0 1>	disable alias
	arp		
		status	<iface>
			display ip arp status
	dhcp		
		client	
			release
			release DHCP client IP
			renew
			renew DHCP client IP
		status	[option]
			show dhcp status
	dns		
		query	
		server	<primary> [secondary] [third]
			set dns server
		stats	
			clear
			clear dns statistics
			disp
			display dns statistics
	httpd		
	icmp		
		status	
			display icmp statistic counter
		discovery	<iface> [on off]
			set icmp router discovery flag
	ifconfig		[iface] [ipaddr] [broadcast <addr> mtu <value>dynamic]
			configure network interface
	ping		<hostid>
			ping remote host
	route		
		status	[if]
			display routing table
		add	<dest_addr default>[/<bits>] <gateway> [<metric>]
			add route
		addiface	<dest_addr default>[/<bits>] <gateway> [<metric>]
			add an entry to the routing table to iface
		addprivate	<dest_addr default>[/<bits>] <gateway> [<metric>]
			add private route
		drop	<host addr> [/<bits>]
			drop a route
	smtp		
	status		
			display ip statistic counters
	stroute		
		display	[rule # buf]
			display rule index or detail message in rule.
		load	<rule #>
			load static route rule in buffer
		save	
			save rule from buffer to spt.
		config	
			name <site name>
			set name for static route.
			destination <dest addr>[/<bits>] <gateway> [<metric>]
			set static route destination address and gateway.
			mask <IP subnet mask>
			set static route subnet mask.
			gateway <IP address>
			set static route gateway address.
			metric <metric #>
			set static route metric number.
			private <yes no>
			set private mode.
			active <yes no>
			set static route rule enable or disable.
	traceroute		<host> [ttl] [wait] [queries]
			send probes to trace route of a remote host
	xparent		
		join	<iface1> [<iface2>]
			join iface2 to iface1 group
		break	<iface>
			break iface to leave ipxparent group
	ave		
			anti-virus enforce

ZyXEL Confidential

	urlfilter			
		reginfo		
			display	display urlfilter registration information
			name	set urlfilter registration name
			eMail <size>	set urlfilter registration email addr
			country <size>	set urlfilter registration country
			clearAll	clear urlfilter register information
		category		
			display	display urlfilter category
			webFeature [block/nonblock] [activex/java/cookei/webproxy]	block or unblock webfeature
			logAndBlock [log/logAndBlock]	set log only or log and block
			blockCategory [block/nonblock] [all/type(1-14)]	block or unblock type
			timeOfDay [always/hh:mm] [hh:mm]	set block time
			clearAll	clear all category information
		listUpdate		
			display	display listupdate status
			actionFlags [yes/no]	set listupdate or not
			scheduleFlag [pending]	set schedule flag
			dayFlag [pending]	set day flag
			time [pending]	set time
			clearAll	clear all listupdate information
		exemptZone		
			display	display exemptzone information
			actionFlags [type(1-3)][enable/disable]	set action flags
			add [ip1] [ip2]	add exempt range
			delete [ip1] [ip2]	delete exempt range
			clearAll	clear exemptzone information
		customize		
			display	display customize action flags
			actionFlags[filterList/disableAllExceptTrusted/unblockRWFTtoTrusted/keywordBlock/fullPath/caseInsensitive/fileName][enable/disable]	set action flags
			logFlags [type(1-3)][enable/disable]	set log flags
			add [string] [trust/untrust/keyword]	add url string
			delete [string] [trust/untrust/keyword]	delete url string
			clearAll	clear all information
		logDisplay		display cyber log
		ftplist		update cyber list data
		listServerIP	<ipaddr>	set list server ip
		listServerName	<name>	set list server name
	treidir			
		failcount	<count>	set treidir failcount
		partner	<ipaddr>	set treidir partner
		target	<ipaddr>	set treidir target
		timeout	<timeout>	set treidir timeout
		checktime	<period>	set treidir checktime
		active	<on/off>	set treidir active
		save		save treidir information
		disp		display treidir information

	debug	<value>	set tredir debug value
nat			
	server		
		disp	display nat server table
		load <set id>	load nat server information from ROM
		save	save nat server information to ROM
		clear <set id>	clear nat server information
		edit active <yes no>	set nat server edit active flag
		edit svrport <start port> [end port]	set nat server server port
		edit intport <start port> [end port]	set nat server forward port
		edit remotehost <start ip> [end ip]	set nat server remote host ip
		edit leasetime [time]	set nat server lease time
		edit rulename [name]	set nat server rule name
		edit forwardip [ip]	set nat server server ip
		edit protocol [protocol id]	set nat server protocol
		edit clear	clear one rule in the set
	service		
		irc [on off]	turn on/off irc flag
	resetport		reset all nat server table entries
	incikeport	[on off]	turn on/off increase ike port flag
igmp			
	debug	[level]	set igmp debug level
	forwardall	[on off]	turn on/off igmp forward to all interfaces flag
	querier	[on off]	turn on/off igmp stop query flag
	iface		
		<iface> grouptm <timeout>	set igmp group timeout
		<iface> interval <interval>	set igmp query interval
		<iface> join <group>	join a group on iface
		<iface> leave <group>	leave a group on iface
		<iface> query	send query on iface
		<iface> rsptime [time]	set igmp response time
		<iface> start	turn on of igmp on iface
		<iface> stop	turn off of igmp on iface
		<iface> ttl <threshold>	set ttl threshold
		<iface> v1compat [on off]	turn on/off v1compat on iface
	robustness	<num>	set igmp robustness variable
	status		dump igmp status
pr			

IPSec Related Command

[Home](#)

Command			Description
ipsec	debug	<1 0>	turn on/off trace for IPsec debug information
	ipsec_log_disp		show IPsec log, same as menu 27.3
	route	lan	<on off>
			After a packet is IPsec processed and will be sent to LAN side, this switch is to control if this packet can be applied IPsec again.
			Remark: Command available since 3.50(WA.3)
		wan	<on off>
			After a packet is IPsec processed and will be sent to WAN side, this switch is to control if this packet can be applied IPsec again.
			Remark: Command available since 3.50(WA.3)
	show_runtime	sa	display runtime phase 1 and phase 2 SA information

		spd		When a dynamic rule accepts a request and a tunnel is established, a runtime SPD is created according to peer local IP address. This command is to show these runtime SPD.
	switch	<on/off>		As long as there exists one active IPsec rule, all packets will run into IPsec process to check SPD. This switch is to control if a packet should do this. If it is turned on, even there exists active IPsec rules, packets will not run IPsec process.
	timer	chk_my_ip	<1~3600>	- Adjust timer to check if WAN IP in menu is changed - Interval is in seconds - Default is 10 seconds - 0 is not a valid value
		chk_conn.	<0~255>	- Adjust auto-timer to check if any IPsec connection has no traffic for certain period. If yes, system will disconnect it. - Interval is in minutes - Default is 2 minutes - 0 means never timeout
		update_peer	<0~255>	- Adjust auto-timer to update IPsec rules which use domain name as the secure gateway IP. - Interval is in minutes - Default is 30 minutes - 0 means never update
	updatePeerIp			Remark: Command available since 3.50(WA.3) Force system to update IPsec rules which use domain name as the secure gateway IP right away.
	dial	<rule #>		Remark: Command available since 3.50(WA.3) Initiate IPsec rule <#> from ZyWALL box
	display	<rule #>		Remark: Command available since 3.50(WA.3) Display IPsec rule #
	remote	key	<string>	I add a secured remote access tunnel with pre-shared key. It is a dynamic rule with local: the route's WAN IP. The algorithms with it are fixed to phase1: DES+MD5, DH1 and SA lifetime 28800 seconds; phase2: DES+MD5, PFS off, no anti-replay and SA lifetime 28800 seconds. The length of pre-shared key is between 8 to 31 ASCII characters.
		switch	<on/off>	Activate or de-activate the secured remote access tunnel.
	keep_alive	<rule #>	<on/off>	Set ipsec keep_alive flag
	load	<rule #>		Load ipsec rule
	save			Save ipsec rules
	config	netbios	active <on/off>	Set netbios active flag
			group <group index1, group index2...>	Set netbios group
		name	<string>	Set rule name
		name	<string>	Set rule name
		keyAlive	<Yes No>	Set keep alive or not
		lclDType	<0:IP 1:DNS 2:Email>	Set local ID type
		lclDContent	<string>	Set local ID content
		myIpAddr	<IP address>	Set my IP address

	peerIdType	<0:IP 1:DNS 2:Email>	Set peer ID type
	peerIdContent	<string>	Set peer ID content
	secureGwAddr	<IP address Domain name>	Set secure gateway address or domain name
	protocol	<1:ICMP 6:TCP 17:UDP>	Set protocol
	lcAddrType	<0:single 1:range 2:subnet>	Set local address type
	lcAddrStart	<IP>	Set local start address
	lcAddrEndMask	<IP>	Set local end address or mask
	lcPortStart	<port>	Set local start port
	lcPortEnd	<port>	Set local end port
	rmAddrType	<0:single 1:range 2:subnet>	Set remote address type
	rmAddrStart	<IP>	Set remote start address
	rmAddrEndMask	<IP>	Set remote end address or mask
	rmPortStart	<port>	Set remote start port
	rmPortEnd	<port>	Set remote end port
	antiReplay	<Yes No>	Set antireplay or not
	keyManage	<0:IKE 1:Manual>	Set key manage
	ike	negotiationMode <0:Main 1:Aggressive>	Set negotiation mode in phase 1 in IKE
		preShareKey <string>	Set pre shared key in phase 1 in IKE
		p1EncryAlgo <0:DES 1:3DES>	Set encryption algorithm in phase 1 in IKE
		p1AuthAlgo <0:MD5 1:SHA1>	Set authentication algorithm in phase 1 in IKE
		p1SaLifeTime <seconds>	Set sa life time in phase 1 in IKE
		p1KeyGroup <0:DH1 1:DH2>	Set key group in phase 1 in IKE
		activeProtocol <0:AH 1:ESP>	Set active protocol in phase 2 in IKE
		p2EncryAlgo <0:Null 1:DES 2:3DES>	Set encryption algorithm in phase 2 in IKE
		p2AuthAlgo <0:MD5 1:SHA1>	Set authentication algorithm in phase 2 in IKE
		p2SaLifeTime <seconds>	Set sa life time in phase 2 in IKE
		encap <0:Tunnel 1:Transport>	set encapsulation in phase 2 in IKE
		pfs <0:None 1:DH1 2:DH2>	set pfs in phase 2 in IKE
	manual	activeProtocol <0:AH 1:ESP>	Set active protocol in manual
	manual ah	encap <0:Tunnel 1:Transport>	Set encapsulation in ah in manual
		spi <decimal>	Set spi in ah in manual
		authAlgo <0:MD5 1:SHA1>	Set authentication algorithm in ah in manual
		authKey <string>	Set authentication key in ah in manual
	manual esp	encap <0:Tunnel 1:Transport>	Set encapsulation in esp in manual
		spi <decimal>	Set spi in esp in manual
		encryAlgo <0:Null 1:DES 2:3DES>	Set encryption algorithm in esp in manual
		encryKey <string>	Set encryption key in esp in manual
		authAlgo <0:MD5 1:SHA1>	Set authentication algorithm in esp in manual
		authKey <string>	Set authentication key in esp in manual

Firewall Related Command

[Home](#)

Command			Description
sys	Firewall		
		acl	
		disp	Display specific ACL set # rule #, or all ACLs.
		active	<yes no> Active firewall or deactivate firewall
		clear	Clear firewall log
		cnt	
		disp	Display firewall log type and count.
		clear	Clear firewall log count.

		disp		Display firewall log
		online		Set firewall log online.
		pktdump		Dump the 64 bytes of dropped packet by firewall
		update		Update firewall
		dynamicrule		
		tcprst		
			rst	Set TCP reset sending on/off.
			rst113	Set TCP reset sending for port 113 on/off.
			display	Display TCP reset sending setting.
		icmp		
		dos		
			smtp	Set SMTP DoS defender on/off
			display	Display SMTP DoS defender setting.
			ignore	Set if firewall ignore DoS in lan/wan/dmz/wlan
		ignore		
			dos	Set if firewall ignore DoS in lan/wan/dmz/wlan
			triangle	Set if firewall ignore triangle route in lan/wan/dmz/wlan

Annex A CI Command List Auto WLAN Security Delivery Related Command

[Home](#)

Command		Description	
autoSec	Start		Start the process of WLAN configuration delivery
	Duration		Set the delivery process duration time in seconds
	Port		Set the communication port
	key		Set the communication encryption key