LAN-Cell Mobile Gateway

Firmware Release Notes

Release 3.62(XF.3)

Proxicast, LLC
312 Sunnyfield Drive, Suite 200
Pittsburgh, PA 15116

1-877-77PROXI
1-877-777-7694
1-412-213-2477

Fax: 1-412-492-9386

E-Mail: support@proxicast.com.
Internet: www.proxicast.com.

Date:	**June 10, 2005**
Author:	**Tim Tseng**
Project Leader:	**Neil Cheng**

Proxicast LAN-Cell Mobile Gateway
Release 3.62(XF.3)
Release Notes

Date: Jun 10, 2005

Supported Platforms:

Proxicast LAN-Cell Mobile Gateway – all models

Versions:

ProxiOS F/W Version: V3.62(XF.3) | 06/10/2005
BootBase: V1.07 | 04/16/2004

Notes:

1. Loading firmware causes Restore to Factory Defaults Settings = **No**.
2. The setting of ignore triangle route is on in default ROMFILE. Triangle route network topology has potential security crisis. If you are not clear about it, please refer to Appendix for the triangle route issue.
3. IKE process in phase 2 will check ID information between system and the peer. If you found that the IPSEC connection is failed, please check your settings.
4. Using Web to configure VPN, the phase 1 algorithms have been fixed to DES + MD5. If other algorithms are preferred, please use ADVANCE page to configure them.
5. When firewall turns from "off" to "on", the firewall initialization procedure will disconnect all connections running through the LAN-Cell.
6. SUA/NAT address loopback feature was enabled on LAN-Cell by default; however, if users do not need it, a C/I command "ip nat loopback off" could turn it off.

Known Issues:

1. eWC→WAN IP has bugs when WAN→ISP is PPPoE or PPTP. Leaving some values in remote IP or remote masks for WAN→IP and then switch to dynamic IP, LAN-Cell cannot dial anymore.
2. The DHCP client in LAN-Cell LAN side may get an IP which is reserved by static DHCP. The situation will disappear if the client releases the IP and requests again.
3. Symptom: When turning on to many web sites at same time, it may cause content filter fail.
   Condition: When turning on browser to access a lot of websites (for example, 30 sites) at same time may cause content filter fail.

4. When you use MSN messenger, sometimes you fail to open special applications, such as whiteboard, file transfer and video etc. You have to wait more than 3 minutes and retry these applications.
5. In web MAIN MENU->SYSTEM->General page, the IP addresses of "System DNS Servers" fields are empty when gateway connects to Internet using dial backup.
6. You cannot change Cellular Modem IP from dynamic to static by telnet or SSH.
7. Symptom: Responder will jump to wrong VPN rule when current rule's phase 2 parameter is wrong.
   Condition:
   Initiator ----------NAT router ---------- Responder

   1). Initiator has one VPN rule in which NAT traversal is on.
   2). In responder, there are two VPN rules.
   - Rule 1: NAT traversal is off, and phase 2 parameters are wrong.
   - Rule 2: NAT traversal is off, and all other parameters are correct.
   3). Trigger tunnel from initiator and responder will use rule 1 to negotiate.
   4). When phase 2 negotiation starts, responder found rule 1's parameters are wrong, and will jump to rule 2.
   5). Negotiation will keep going and tunnel will be up.
8. Can't block ActiveX in some case.
9. System may need to reboot when changing the SNMP port number.

Change History:

Modifications in V 3.62(XF.3) | 06/10/2005
Modify for formal release

Modifications in V 3.62(XF.3)b1 | 06/06/2005
1. [ENHANCEMENT]
Add a CI command "sys restart [timer|daily|display]" to set a timer to restart device. You can also add this CI command into autoexec.net.

Modifications in V 3.62(XF.2) | 10/15/2004
Modify for formal release.

Modifications in V 3.62(XF.2)b1 | 10/13/2004
1. [ENHANCEMENT]
   The "AT Command Initial String" length of eWC->WAN->Cellular Modem page extends from 31 to 71.
2. [BUG FIX]
   Symptom: Sometimes the LAN-Cell reboots by software watchdog.
   Condition:
   1. Put the LAN-Cell on the network for a long time.
   2. Sometimes the LAN-Cell will reboot by software watchdog.

Modifications in V 3.62(XF.1) | 07/08/2004

1. Modify for formal release.

Modifications in V 3.62(XF.1)b2 | 07/06/2004

1. [BUG FIX] Symptom: Trigger port will disappear after system reboot.
   Condition:
   (1) Configure Trigger port rule.
   (2) System reboot.
   (3) The configured Trigger port rule disappear.

2. [BUG FIX] Symptom: In eWC->SYSTEM->Time and Date->Synchronize Now page, the message should be “The LAN-Cell is attempting to synchronize with ...”
   Condition:
   (1) Goto eWC->->SYSTEM->Time and Date->Synchronize Now.
   (2) the message should be “The LAN-Cell is attempting to synchronize with ...”.

3. [BUG FIX] Symptom: The link of help page is wrong.
   Condition:
   (1) Goto eWC->->SYSTEM->Time and Date->Synchronize Now.
   (2) The “HELP” link is assigned with a incorrect URL.
4. [BUG FIX] Symptom: The wording is error in eWC->MAIN MENU page.
   Condition: In eWC->MAIN MENU page, the message should be “Welcome to the Proxicast”.

Modifications in V 3.62(XF.1)b1 | 06/30/2004

1. [ENHANCEMENT] In eWC>SYSTEM>Time and Date,
   (1) The original page is separated into three parts
      1. Current Time and Date only displays the information about the system time and date and it's read-only.
      2. Time and Date Setup includes:
         1) Manual (None,use no time protocol)
         2) Get from Time Server (Use protocol Daytime,Time or NTP)
         3)Time Zone Setup: users can configure the time zone and the daylight saving.
   (2) After pressing 'Synchronize Now' button, the gateway not only synchronizes with time server immediately but also stores the configurations. After pressing the synchronize button, a warning screen will appear.
   (3) There are two different behaviors when configuring the date and time.
      1. If users only change the time zone and daylight saving but don't change the original time and date. The new time and date will be updated based on the new time zone and if it is in the daylight saving period.
      2. If users change the time or date, no matter if users change the time zone and daylight saving, the gateway will store the new date and time directly, regardless of the time zone and daylight saving which were configured by the user.

2. [BUG FIX] Symptom: There are error wordings in SMT's DDNS page .
   Condition:
   (1) Goto SMT DDNS page.

(2) Some wordings are not identical with eWC->WAN->DDNS.

3. [ENHANCEMENT] Add SMTP authentication feature in eWC->LOGS->Log Settings page.

Modifications in V 3.62(XF.0) | 05/17/2004
Modify for formal release.

Modifications in V 3.62(XF.0)b1 | 04/16/2004
1. [FEATURE CHANGE]
   Formal release.

Appendix 1: System Restart Command

The new CI command to force a scheduled system restart command has the following syntax:

`SYS RESTART DISPLAY`

Shows the current System Restart Timer settings

`SYS RESTART TIMER n`

Set the System Restart countdown timer to N minutes from now. N can be any number of minutes from 0 to 2^{32}. Common values are:

60 = 1 hour
240 = 4 hours
480 = 8 hours
720 = 12 hours
1440 = 24 hours
10080 = 7 days
43200 = 30 days

`SYS RESTART DAILY n`

Set the System Restart to occur at N hour. N must be a whole number between 1 and 24 (midnight). The LAN-Cell uses its internal system clock to determine when to perform the System Restart, so check the current system time with the `SYS DATE TIME` command.

The SYS RESTART command can be added to the AUTOEXEC.NET system startup batch file to create a regularly scheduled system restart (e.g. every day, every N minutes, etc).

Appendix 2: Packet filter for "NetBIOS over TCP/IP" (NBT)

The new CI command is under "sys filter netbios" sub-command. Default values of any direction are “Forward”, and trigger dial is “Disabled”.

There are two CI commands:
(1) "sys filter netbios disp": It will display the current filter mode.

Example output:

```
============== NetBIOS Filter Status ==============
        LAN to WAN:         Block
        WAN to LAN:         Forward
        IPSec Packets:      Forward
        Trigger Dial:       Disabled
```

(2) "sys filter netbios config <type> {on|off}": To configure the filter mode for each type.

Current filter types and their description are:

Type	Description	Default mode
0	LAN to WAN	Forward
1	WAN to LAN	Forward
6	IPSec pass through	Forward
7	Trigger dial	Disabled

Example commands:
sys filter netbios config 0 on => block LAN to WAN NBT packets
sys filter netbios config 1 on => block WAN to LAN NBT packets
sys filter netbios config 6 on => block IPSec NBT packets
sys filter netbios config 7 off => disable trigger dial

Appendix 3: IPSec FQDN support

LAN-Cell A----------Router C (with NAT) ----------LAN-Cell B
(WAN) (WAN) (LAN) (WAN)

If LAN-Cell A wants to build a VPN tunnel with LAN-Cell B by passing through Router C with NAT, A can not see B. It has to secure gateway as C. However, LAN-Cell B will send it packet with its own IP and its ID to LAN-Cell A. The IP will be NATed by Router C, but the ID will remain as LAN-Cell B sent.

In FQDN design, all three types, IP, DNS, E-Mail, can set ID content. For ID type is DNS or E-mail, the behavior is simple. LAN-Cell A and LAN-Cell B only checks the ID contents are consistent and they can connect.

Basically the story is the same when ID type is IP. If user configures ID content, then LAN-Cell will use it as a check. So the ID content also has to match each other. For example, ID type and ID content of incoming packets must match “Peer ID Type” and “Peer ID content”. Or LAN-Cell will reject the connection.

However, user can leave “ID content” blank if the ID type is IP. LAN-Cell will put proper value in it during IKE negotiation. This appendix describes all combinations and behaviors of LAN-Cell.

We can put all combinations in to these two tables:

(Local ID Type is IP):

Configuration		**Run-time status	
My IP Addr	Local ID Content	My IP Addr	Local ID Content
0.0.0.0	*blank or 0.0.0.0	My WAN IP	My WAN IP
0.0.0.0	a.b.c.d (NOT 0.0.0.0)	My WAN IP	a.b.c.d
a.b.c.d (not 0.0.0.0)	*blank or 0.0.0.0	a.b.c.d	a.b.c.d
a.b.c.d (not 0.0.0.0)	e.f.g.h (NOT 0.0.0.0)	a.b.c.d	e.f.g.h

*Blank: User can leave this field as empty, doesn’t put anything here.
**Runtime status: During IKE negotiation, LAN-Cell will use “My IP Addr” field as source IP of IKE packets, and put “Local ID Content” in the ID payload.

(Peer ID Type is IP):

Configuration		*Run-time check
Secure Gateway Addr	Peer ID Content	
0.0.0.0	Blank or 0.0.0.0	Just check ID types of incoming packet and machine’s peer ID type. If the peer’s ID is

		IP, then we accept it.
0.0.0.0	a.b.c.d (NOT 0.0.0.0)	System checks both type and content
a.b.c.d	Blank	1. System will check the ID type and the content. 2. The contents will match only if the ID content of coming packet is a.b.c.d because system will put Secure Gateway Address as Peer ID content.
a.b.c.d	e.f.g.h	1. System will check the ID type and the content. 2. The contents will match only if the ID content of coming packet is e.f.g.h.

*Runtime Check: During IKE negotiation, we will check ID of incoming packet and see if it matches our setting of “Peer ID Type” and “Peer ID Content”.

Summary:

1. When Local ID Content is blank or 0.0.0.0, during IKE negotiation, my ID content will be “My IP Addr” (if it’s not 0.0.0.0) or local’s WAN IP.
2. When “Peer ID Content” is not blank or 0.0.0.0, ID of incoming packet has to match our setting. Or the connection request will be rejected.
3. When “Secure Gateway IP Addr” is 0.0.0.0 and “Peer ID Content” is blank or 0.0.0.0, system can only check ID type. This is a kind of “dynamic rule” which means it accepts incoming request from any IP, and these requests’ ID type is IP. So if user put such a kind of rule in top of rule list, it may be matched first. To avoid this problem, we will enhance it in the future.

Appendix 4: DNS servers for IPSec VPN Note

DNS Domain Names

DNS (Domain Name System), a system for naming computers and network services that is organized into hierarchy of domain. DNS services provided by the DNS server can resolve the name to other information associated with the name, such as an IP address. The LAN-Cell can be configured as a DHCP server. For most cases, your computer connected to the LAN of the LAN-Cell can get IP settings (IP address, network mask, gateway address and DNS server address) from the LAN-Cell DHCP server automatically.

There are three ways the LAN-Cell's DHCP server assigns DNS servers addressed to its DHCP client computers.

(1) If the administrator has setup DNS servers on the LAN-Cell's DHCP setting, the LAN-Cell will tell the client those DNS server addresses.
(2) If the DNS server has not been setup on the LAN-Cell DHCP server, but the LAN-Cell has gotten the public DNS servers from the ISP; the LAN-Cell will assign those public DNS servers address.
(3) The LAN-Cell gives its own LAN IP address and acts as a DNS server proxy.

But the above are not enough for IPSec VPN applications.

How to access the private network by using domain names

On the IPSec VPN application, the user on the LAN of the LAN-Cell, wants to access remote private networks. He must use the IP address to identify the remote site he wants to access. But at the modern intranet applications, we still want to have the DNS service for private network access. For example, there is a private Web server installed at the headquarters of your computer. You can access this Web server inside your company, or from your home by way of the LAN-Cell's IPSec tunnel. The IP address of the private Web server is also private. You can't use the Internet public DNS servers to resolve those domain names that belong to your company's private network. You must setup those private DNS servers on your computer manually if you want to access the private network by using domain names.

LAN-Cell DNS Servers for IPSec VPN

The LAN-Cell has added DNS Server on each IPSec policy setup. When you setup the IPSec rule, you can give the DNS server if there exists a DNS Server that provides DNS service for this private network. The DHCP client (on LAN-Cell's LAN) requests the IP information from your LAN-Cell, the LAN-Cell assigns additional DNS servers for IPSec VPN to the client, if the assigned IP address belongs to the range of local addresses of the IPSec rule.

Appendix 5: CI Command List

Command Class List Table		
System Related Command	Exit Command	Ethernet Related Command
IP Related Command	IPSec Related Command	Firewall Related Command

System Related Command

Command				Description
sys				
	adjtime			retrive date and time from Internet
			display	display cbuf static
	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> <1st phone num> [2nd 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]	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]	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
			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		display all 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
	pwderrtm		[minute]	Set or display the password error blocking timeout value.
	reboot			Performs an immediate system reboot
	restart			
		display		Display current sys restart timer settings
		daily	[1 to 24]	Hour at which to restart device
		timer	[0 to 2^32]	Number of minutes from now to restart
	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
	stdio		[second]	change terminal timeout value
	time		[hour [min [sec]]]	display/set system time
	trcdisp			monitor packets
	trclog			
	trcpacket			
	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
	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		

Exit Command

Command				Description
exit				exit smt menu

Ethernet Related Command

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
	edit			
		load	<ether no.>	load ether data from spt
		mtu	<value>	set ether data mtu
		speed	[auto|100/full|100/half|10/full|10/half]	change Ethernet speed
		save		save ether data to spt

IP Related Command

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
		attpret	<on|off>	switch to avoid IP spoofing ARP attack
	dhcp		<iface>	
		client		
			release	release DHCP client IP
			renew	renew DHCP client IP
		status	[option]	show dhcp status
	dns			
		query		
		stats		
		system		
			edit	edit system DNS status
			display	show system DNS status
		lan		
			edit	edit LAN DNS status
			display	show LAN DNS status
			clear	clear dns statistics
			disp	display dns statistics
		default	<ip>	Set default DNS server
	httpd			
		debug	[on|off]	set http debug flag
	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>]	add route

			<gateway> [<metric>]	
		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.
	udp			
		status		display udp status
	rip			
	tcp			
		status	[tcb] [<interval>]	display TCP statistic counters
	telnet		<host> [port]	execute telnet clinet command
	tftp			
	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
	urlfilter			
		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 [act(1-6)][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
	tredir			
		failcount	<count>	set tredir failcount
		partner	<ipaddr>	set tredir partner
		target	<ipaddr>	set tredir target
		timeout	<timeout>	set tredir timeout
		checktime	<period>	set tredir checktime
		active	<on|off>	set tredir active
		save		save tredir information
		disp		display tredir information
		debug	<value>	set tredir debug value
	rpt			

		start		start report
		stop		stop report
		url	[num]	top url hit list
		ip	[num]	top ip addr list
		srv	[num]	top service port list
	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

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
		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 minuets
				- 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
				Remark: Command available since 3.50(WA.3)
	updatePeerIp			Force system to update IPSec rules which use domain name as the secure gateway IP right away.
				Remark: Command available since 3.50(WA.3)
	dial	<rule #>		Initiate IPSec rule <#> from LAN-Cell box
				Remark: Command available since 3.50(WA.3)
	display	<rule #>		Display IPSec rule #
	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
		active	<Yes | No>	Set active or not
		keeyAlive	<Yes| No>	Set keep alive or not
		natTraversal	<Yes| No>	Enable NAT traversal or not.
		lcIdType	<0:IP | 1:DNS | 2:Email>	Set local ID type
		lcIdContent	<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 anitreplay 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
		name	<string>	Set rule name

Firewall Related Command

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