TXOne Edge Series Product

Command-Line Interface Manual

(For EdgeIPS v1.3/EdgeIPS Pro v1.2/EdgeFire v1.2)

2021-11-01

Trend Micro Incorporated reserves the right to make changes to this document and to the product described herein without notice. Before installing and using the product, review the readme files, release notes, and/or the latest version of the applicable documentation, which are available from the Trend Micro website at:

http://docs.trendmicro.com/en-us/home.aspx

This documentation introduces the main features of the product and/or provides installation instructions for a production environment. Read through the documentation before installing or using the product.

Detailed information about how to use specific features within the product may be available at the Trend Micro Online Help Center and/or the Trend Micro Knowledge Base.

Table of Contents

Getting Started

This chapter describes Edge series and how to get started with configuring Command-Line Interface (CLI) settings. Edge series which currently supports CLI commands is included EdgeIPS, EdgeIPS Pro and EdgeFire.

Opening the CLI Management Console

Edge series provide a built-in management CLI management interface that you can use to configure and manage the product(s). Operate the CLI management interface with Telnet or SSH terminal software.

Note: Before you access the CLI management interface, please go to "Administration > System Management" and enable "Telnet" or "SSH" in Management Method plane.

Procedure

1. In a telnet or SSH terminal software, type the address of Edge series in the following format: https://192.168.127.254

Note: Edge series use an automatically-generated self-signed SSL certificate to encrypt communications between the client and the device. Given that the certificate is self-signed, most SSH terminal software will not trust the certificate and will give a warning that the certificate being used is not signed by a known authority.

The logon screen will appear.

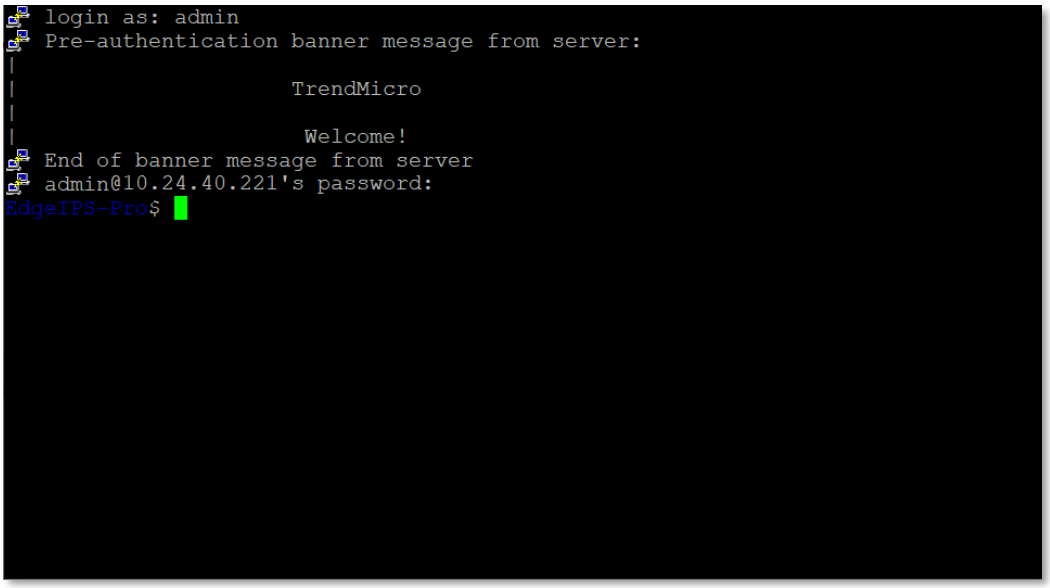
Note: The default IP address of Edge series is 192.168.127.254 with subnet 255.255.255.0. Before connecting a PC/laptop to Edge series, the PC's IP address should be set to an IP address that is able to access to the default IP address. After that, connect the PC and Edge series with an Ethernet cable.

2. Input the logon credentials (user ID and password).

   Use the default administrator logon credentials when logging on for the first time:

   - User ID: `admin`
   - Password: `txone`

3. Click Log On.



How to Operate the CLI Management Console

The CLI management interface include several modes and tips that help you configure Edge series.

Entering the View Mode

1. Log on to the CLI management console.
2. Input the below commands.

   EdgeIPS-Pro$ enable

   EdgeIPS-Pro#

3. When the prompt character "$" becomes to "#", you can press tab key to list out the commands you use to list the function status, set the system time, sync ntp server, reboot the device or switch the firmware partition.

```
EdgeIPS-Pro$ enable
EdgeIPS-Pro#
set configure
set system time
sync ntp-server
reboot
power off
switch partition
show acl
show device
show network
show remote-access
show ip-objects
show service-objects
show policy-enforcement-rulesets
show antivirus-profiles
show antivirus-exceptions
show port-security
show partition
show bandwidth-management
show snmp-settings
show snmp-trap-settings
show odc-server
show ntp-server
show timezone
show system
exit
EdgeIPS-Pro#
```

Entering the Edit Mode

1. Log on to the CLI management console.
2. Input the below commands.

> **EdgeIPS-Pro$** enable
>
> **EdgeIPS-Pro#** set configure
>
> **EdgeIPS-Pro(set configure)#**

3. When the prompt character "$" becomes to "#", you can press tab key to list out the commands you use to edit the function. A path indicator in "()" shows the current function location that you are located for configuration.

```
EdgeIPS-Pro# set configure
EdgeIPS-Pro(set configure)#
edit device
edit network
edit remote-access
edit ip-objects
edit policy-enforcement-ruleset
edit bandwidth-management
edit service-objects
edit port-security
edit snmp-trap-settings
edit odc-server
edit ntp-server
edit snmp-settings
edit timezone
edit antivirus-profiles
edit antivirus-exception-file
edit acl
edit remote-access
exit
EdgeIPS-Pro(set configure)#
```

System Information

Monitor your basic system information, including System Boot Time, System Time, Device Name, Model Name, Firmware Version, Firmware Build Time, Serial Number, IPS/Antivirus Pattern Version and ODC Sync Status.

Procedure (For EdgeIPS / EdgeIPS Pro / EdgeFire)

1. Log on to the CLI management console.
2. Input the below commands.

```
EdgeIPS-Pro$ enable
EdgeIPS-Pro# show system
```

3. The output displays the system information below.

```
EdgeIPS-Pro# show system

        System Boot Time:        2021-09-21T16:46:52+08:00
        System Time:             2021-09-24T19:18:58+08:00
        Device Name:             EdgeIPS-Pro
        Model Name:              IPS-Pro-2096-BP-TM
        Firmware Version:        IPSP_T01_1.2.10
        Firmware Build Time:     2021-09-10T18:02:47+08:00
        Serial Number:           TMP01990000002

        IPS Pattern Version:             TM_IPSP_210909_14
        Antivirus Pattern Version:       2.004

        ODC Sync status:         connected
EdgeIPS-Pro#
```

```
EdgeFire# show system

        System Boot Time:        2021-10-26T14:44:06+08:00
        System Time:             2021-10-26T19:15:20+08:00
        Device Name:             EdgeFire
        Model Name:              IEF-1012-TM
        Firmware Version:        IEF_T01_1.2.1
        Firmware Build Time:     2021-10-22T18:30:12+08:00
        Serial Number:           TMF02200000949
        Operation Mode:          gateway

        IPS Pattern Version:     TM_210927_14

        ODC Sync status:         connected
        Independent MGMT IP:     -       status: disabled
EdgeFire#
```

System Information	Description
System Boot Time	The time and the date the system was initialized and booted up.
System Time	The current time and date.
Device Name	The name of the Edge-series device.

Model Name	The model name of the Edge-series device.
Firmware Version	The firmware version of the Edge-series device in the active partition.
Firmware Build Time	The time and the date the firmware was compiled and built as an image.
Serial Number	The serial number of the Edge-series device.
Operation Mode	The operation mode of EdgeFire. Note: Only EdgeFire supports this system information.
IPS Pattern Version	The IPS pattern version of the Edge-series device.
Antivirus Pattern Version	The antivirus pattern version of the Edge-series device. Note: Only EdgeIPS Pro supports this system information
ODC Sync status	The connection status between the Edge-series device and OT Defense Console (ODC).
Independent MGMT IP	The IP address and the connection status of the Independent MGMT Port. Note: Only EdgeFire supports this system information

The Device Tab

This chapter describes how to set up the network settings and port configuration for the device.

Configuring Network Settings

Procedure (For EdgeIPS / EdgeIPS Pro)

1. Log on to the CLI management console.
2. Input the below commands.

```
EdgeIPS-Pro$ enable

EdgeIPS-Pro# set configure

EdgeIPS-Pro# edit network
```

3. The output displays the system information below. Now you are already in the editor mode to configure network. You can input the command lines to configure the network settings.

```
EdgeIPS-Pro(set configure)# edit network

    Network Setting:
        IP 192.168.1.115 mask 255.255.255.0 gateway 192.168.1.1
        DNS 192.168.1.1
        no VLAN
        LLDP disabled

EdgeIPS-Pro(cfg-edit network)#
```

Command Line	Description
set ip <addr> <mask> <gateway>	Configure the IP address, network mask and gateway address of the device.
set dns <ip>	Configure the DNS server IP address of the device.
set vlan tag <id>	Enable VLAN Tag and configure the VLAN ID of the device.
set vlan untag	Disable the VLAN Tag of the device.
set lldp <enabled | disabled>	Enable or disable LLDP function
preview	List the preview settings.
save	Save the current settings.
exit	Return to the upper layer of the command lines.

4. Once you decide to save the configuration, input "save" and press enter.
5. Input "exit" and press enter to leave the current function settings.

Note: Only EdgeIPS and EdgeIPS Pro support Network Interface settings.

The Network Tab

This chapter describes how to set up the network interface settings, operation mode settings for EdgeFire.

Viewing Network Interface Settings

Procedure (For EdgeFire, Gateway Mode)

1. Log on to the CLI management console.
2. Input the below commands.

   EdgeFire$ enable

   EdgeFire# show network-interface

3. The output displays the system information below.

```
EdgeFire41# show network-interface

                    Interface:              WAN1
                    Status:                 enabled
                    Connection Type :       Static IP
                    IP address:             10.24.7.41
                    Mask:                   255.255.0.0
                    VLAN-ID:                0
                    Description:            test

                    Interface:              LAN1
                    Status:                 enabled
                    Connection Type :       DHCP Server
                    IP address:             192.168.127.254
                    Mask:                   255.255.255.0
                    VLAN-ID:                0
                    Description:

                    Interface:              LAN2
                    Status:                 enabled
                    Connection Type :       DHCP Server
                    IP address:             192.168.2.254
                    Mask:                   255.255.255.0
                    VLAN-ID:                0
                    Description:

                    Interface:              DMZ
                    Status:                 enabled
                    Connection Type :       DHCP Server
                    IP address:             192.168.253.254
                    Mask:                   255.255.255.0
                    VLAN-ID:                0
                    Description:            192.168.253.254

EdgeFire41#
```

Note: Only EdgeFire (in Gateway mode) supports Network Interface settings.

Configuring Network Interface Settings

Procedure (For EdgeFire, Gateway Mode)

1. Log on to the CLI management console.
2. Input the below commands.

```
EdgeFire$ enable

EdgeFire# set configure

EdgeFire# edit network-interface
```

3. The output displays the system information below. Now you are already in the editor mode to configure network. You can input the command lines to configure the network interface settings.

```
EdgeFire(set configure)# edit network-interface

                Interface:          WAN1
                Status:             enabled
                Connection Type :   Static IP
                IP address:         10.24.7.41
                Mask:               255.255.0.0
                VLAN-ID:            0
                Description:        test

                Interface:          LAN1
                Status:             enabled
                Connection Type :   DHCP Server
                IP address:         192.168.127.254
                Mask:               255.255.255.0
                VLAN-ID:            0
                Description:

                Interface:          LAN2
                Status:             enabled
                Connection Type :   DHCP Server
                IP address:         192.168.2.254
                Mask:               255.255.255.0
                VLAN-ID:            0
                Description:

                Interface:          DMZ
                Status:             enabled
                Connection Type :   DHCP Server
                IP address:         192.168.253.254
                Mask:               255.255.255.0
                VLAN-ID:            0
                Description:        192.168.253.254

EdgeFire(cfg-edit network-interface)#
```

Command Line	Description
edit <wan1 | lan1 | lan2 | dmz>	Configure the IP address, network mask and gateway address of the device.
preview	List the preview settings.
save	Save the current settings.
exit	Return to the upper layer of the command lines.
save force	Save the current settings without displaying prompt for confirmation
exit force	Return to the upper layer of the command lines without displaying prompt for confirmation

4. If you already choose the specific connection type in WAN1 to edit, input the below command lines.

Command Line	Description
set enabled < true | false >	Set the WAN1 interface to be enabled or disabled.
set description <description>	Input the description of the WAN1 interface.
set vlan tag <id>	Enable VLAN tag and set the VLAN ID on the WAN1 interface.
set vlan untag	Disable VLAN tag on the WAN1 interface.
set connection-type < static_ip | dhcp_client >	Set the connection type to static IP or DHCP client.
set ip <addr> <mask> <gateway>	Set the IP address, the network mask address and the gateway address on the WAN1 interface.
set dns [<ip>,<ip>]	Set the primary and secondary DNS addresses.
preview	List the preview settings.
done	Keep current settings (the configuration has not yet been saved).
exit	Return to the upper layer of the command lines.
done force	Keep current settings (the configuration has not yet been saved) without displaying prompt for confirmation.
exit force	Return to the upper layer of the command lines without displaying prompt for confirmation.

5. If you already choose LAN1/LAN2/DMZ to edit, input the below command lines.

Command Line	Description
set enabled < true | false >	Set LAN1/LAN2/DMZ interface(s) to be enabled or disabled.
set description <description>	Input the description of LAN1/LAN2/DMZ interface(s).
set vlan tag <id>	Enable VLAN tag and set the VLAN ID on LAN1/LAN2/DMZ interface(s).
set vlan untag	Disable VLAN tag on LAN1/LAN2/DMZ interface(s).
set lan-ip	Set the LAN IP address on tLAN1/LAN2/DMZ interface(s).
set mask <mask>	Set the network mask address on LAN1/LAN2/DMZ interface(s).
set dhcp enabled < server | relay >	Enable the DHCP service and set it as DHCP server or DHCP relay.
set ip-range <start-ip> <end-ip>	Set the starting IP and ending IP for the IP range on LAN1/LAN2/DMZ interface(s).
set gateway <ip-addr>	Set the gateway IP address on LAN1/LAN2/DMZ interface(s).
set lease-time <number>	Set the DHCP lease time for DHCP server.
set dns [<ip1>, <ip2>]	Set the primary and secondary DNS addresses on LAN1/LAN2/DMZ interface(s).

set dhcp disabled	Disable DHCP service.
preview	List the preview settings.
done	Keep current settings (the configuration has not yet been saved).
exit	Return to the upper layer of the command lines.
done force	Keep current settings (the configuration has not yet been saved) without displaying prompt for confirmation.
exit force	Return to the upper layer of the command lines without displaying prompt for confirmation.

6. Once you decide to save the configuration, input "save" and press enter.
7. Input "exit" and press enter to leave the current function settings.

Note: Only EdgeFire (in Gateway mode) supports Network Interface settings.

Viewing Operation Mode Settings

Procedure (For EdgeFire)

1. Log on to the CLI management console.
2. Input the below commands.

```
EdgeFire$ enable
EdgeFire# show operation-mode
```

3. The output displays the system information below.

```
EdgeFire41# show operation-mode
        Operation Mode: gateway
EdgeFire41#
```

Note: Only EdgeFire supports Operation Mode.

Configuring Operation Mode Settings

Procedure (For EdgeFire)

1. Log on to the CLI management console.
2. Input the below commands.

```
EdgeFire$ enable
EdgeFire# set configure
EdgeFire# edit operation-mode
```

3. The output displays the system information below. Now you are already in the editor mode to configure network. You can input the command lines to configure the operation mode settings.

```
EdgeFire(cfg-edit operation-mode)#
set operation-mode
preview
save
exit
EdgeFire(cfg-edit operation-mode)# exit
```

Command Line	Description
set operation-mode <gateway | bridge>	Set the operation mode to gateway mode or bridge mode.
preview	List the preview settings.
save	Save current settings.
exit	Return to the upper layer of the command lines.
save force	Save current settings without displaying prompt for confirmation.
exit force	Return to the upper layer of the command lines without displaying prompt for confirmation.

4. If you already choose to set the operation mode to gateway mode, input the below command lines.

Command Line	Description
set operation-mode <gateway | bridge>	Set the operation mode to gateway mode or bridge mode.
preview	List the preview settings.
save	Save current settings.
exit	Return to the upper layer of the command lines.
save force	Save current settings without displaying prompt for confirmation.
exit force	Return to the upper layer of the command lines without displaying prompt for confirmation.

5. If you already choose to set the operation mode to bridge mode, input the below command lines.

Command Line	Description
set operation-mode <gateway | bridge>	Set the operation mode to gateway mode or bridge mode.
set management-interface <bridge-port | independent-MGMT-port>	Set bridge port or independent MGMT port as the management interface.
set ip <addr> <mask> <gateway>	Set the IP address, network mask and gateway address of the management interface.
set dns (optional) <ip>	Set the DNS address of the management interface.
set vlan tag <id>	Enable VLAN tag and set the VLAN ID of the management interface
set vlan untag	Disable VLAN tag on the management interface.
set stp enabled	Enable STP (Spanning Tree Protocol) for all network interfaces or ports on EdgeFire. EdgeFire can detect the loop and disable the network interfaces or ports that cause the loop.
set stp disabled	Disable STP (Spanning Tree Protocol) for all network interfaces or ports on EdgeFire.
preview	List the preview settings.
save	Save current settings.
exit	Return to the upper layer of the command lines.
save force	Save current settings without displaying prompt for confirmation.
exit force	Return to the upper layer of the command lines without displaying prompt for confirmation.

6. Once you decide to save the configuration, input "save" and press enter.
7. Input "yes" and press enter to write the configuration.
8. Input "yes" and press enter to switch the operation mode. The system will reboot.

Note:	When EdgeFire is switched from gateway mode to bridge mode, the features of Network Interface, NAT Rules, ALG, and Static Route will not operate and not be configurable.
Note:	When the operation mode is set to gateway mode, the LAN1 network settings / LAN1 DHCP Service for Gateway mode is not editable and for previewing only.
Note:	The configuration of the policy enforcement rule is not compatible between Gateway mode and Bridge mode. Therefore, the policy enforcement rule needs to be reconfigured after switching from Gateway mode to Bridge mode.

The NAT Tab

Use the NAT (Network Address Translation) tab to view and configure NAT rules on EdgeFire.

NAT Rule

Use the NAT tab to configure the following:

- 1 to 1 network address translation for incoming traffic on the specific interface
- Multiple 1 to 1 network address translation for incoming traffic on the specific interface
- Port forwarding address translation for incoming traffic on the specific interface

The following table describes the tasks you can perform in NAT Rule function in CLI mode.

Task	Description
Add a NAT rule	Create a new NAT rule.
Edit a NAT rule	Edit the NAT rule settings.
Delete a NAT rule	Select one or multiple NAT rules to delete.

Viewing NAT Rule List

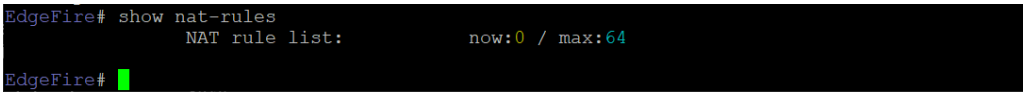
Procedure (For EdgeFire, Gateway Mode)

1. Log on to the CLI management console.
2. Input the below commands.

   EdgeFire$ enable

   EdgeFire# show nat-rules

3. The output displays the system information below.



Note: Only EdgeFire (in Gateway mode) supports NAT Rule settings.

Configuring NAT Rule

Procedure (For EdgeFire, Gateway Mode)

1. Log on to the CLI management console.
2. Input the below commands.

   EdgeFire$ enable

   EdgeFire# set configure

   EdgeFire# edit nat-rules

3. The output displays the system information below. Now you are already in the editor mode to configure the network. The default NAT type in a new NAT rule is 1-to-1 NAT. If you already set a NAT type to 1-to-1 NAT in the NAT rule, input the below command lines.

```
EdgeFire(set configure)# edit nat-rules

        NAT rule list:        now:1 / max:64

            Index: 1      Name: test     Status: enabled
            Type: 1 to 1 NAT
            Original ip: 10.10.10.10
            Mapped ip: 192.168.2.10

EdgeFire(cfg-edit nat-rules)#
```

Command Line	Description
set name <new-name>	Set the name of the NAT rule.
set description <description>	Set the description of the NAT rule.
set enabled <true | false>	Eanble or disable the NAT rule.
set nat-loopback <enabled | disabled>	Eanble or disable the NAT loopback feature in the NAT rule.
set incoming-interface <WAN1 | LAN1 | LAN2 | DMZ >	Set the following interfaces of the NAT rule. - WAN1 - LAN1 - LAN2 - DMZ
set type <1-to-1-nat | multi-1-to-1-nat-ip-range | multi-1-to-1-nat-cidr | port-forward>	Set the NAT type in the NAT rule. - 1 to 1 NAT - Multiple 1 to 1 NAT (Define the rule with IP range) - Multiple 1 to 1 NAT (Define the rule with CIDR) - Port forward
set original-ip <ip>	Set the original IP address in the NAT rule. (for 1 to 1 NAT).
set mapped-ip <ip>	Set the mapped IP address in the NAT rule. (for 1 to 1 NAT).
preview	List the preview settings.
done	Keep current settings (the configuration has not yet been saved).
exit	Return to the upper layer of the command lines.
done force	Keep current settings without displaying prompt for confirmation (the configuration has not yet been saved).
exit force	Return to the upper layer of the command lines without displaying prompt for confirmation.

4. If you already set a NAT type to multi 1-to-1 NAT (IP range) in the NAT rule, input the below command lines.

Command Line	Description
set name <new-name>	Set the name of the NAT rule.
set description <description>	Set the description of the NAT rule.
set enabled <true | false>	Eanble or disable the NAT rule.

set nat-loopback <enabled | disabled>	Eanble or disable the NAT loopback feature in the NAT rule.
set incoming-interface <WAN1 | LAN1 | LAN2 | DMZ >	Set the following interfaces of the NAT rule. - WAN1 - LAN1 - LAN2 - DMZ
set type <1-to-1-nat | multi-1-to-1-nat-ip-range | multi-1-to-1-nat-cidr | port-forward>	Set the NAT type in the NAT rule. - 1 to 1 NAT - Multiple 1 to 1 NAT (Define the rule with IP range) - Multiple 1 to 1 NAT (Define the rule with CIDR) - Port forward
set ip-range <original-ip-range-start> < original-ip-range-end> <mapped-ip-range-start> <mapped--ip-range-end>	Set the original IP starting/ending address and the mapping IP starting/ending address in the NAT rule. (for multiple 1 to 1 NAT).
preview	List the preview settings.
done	Keep current settings (the configuration has not yet been saved).
exit	Return to the upper layer of the command lines.
done force	Keep current settings without displaying prompt for confirmation (the configuration has not yet been saved).
exit force	Return to the upper layer of the command lines without displaying prompt for confirmation.

5. If you already set a NAT type to multi 1-to-1 NAT (CIDR, Classless Inter-Domain Routing) in the NAT rule, input the below command lines.

Command Line	Description
set name <new-name>	Set the name of the NAT rule.
set description <description>	Set the description of the NAT rule.
set enabled <true | false>	Eanble or disable the NAT rule.
set nat-loopback <enabled | disabled>	Eanble or disable the NAT loopback feature in the NAT rule.
set incoming-interface <WAN1 | LAN1 | LAN2 | DMZ >	Set the following interfaces of the NAT rule. - WAN1 - LAN1 - LAN2 - DMZ
set type <1-to-1-nat | multi-1-to-1-nat-ip-range | multi-1-to-1-nat-cidr | port-forward>	Set the NAT type in the NAT rule. - 1 to 1 NAT - Multiple 1 to 1 NAT (Define the rule with IP range) - Multiple 1 to 1 NAT (Define the rule with CIDR) - Port forward
set ip-cidr <original-ip> <mapped-ip> <cidr>	Set the original IP starting/ending address and the mapping IP starting/ending address in NAT rule via CIDR format. (For multiple 1 to 1 NAT)
preview	List the preview settings.
done	Keep current settings (the configuration has not yet been saved).
exit	Return to the upper layer of the command lines.

done force	Keep current settings without displaying prompt for confirmation (the configuration has not yet been saved).
exit force	Return to the upper layer of the command lines without displaying prompt for confirmation.

6. If you already set a NAT type to port-forward in the NAT rule, input the below command lines.

Command Line	Description
set name <new-name>	Set the name of the NAT rule.
set description <description>	Set the description of the NAT rule.
set enabled <true | false>	Eanble or disable the NAT rule.
set nat-loopback <enabled | disabled>	Eanble or disable the NAT loopback feature in the NAT rule.
set incoming-interface <WAN1 | LAN1 | LAN2 | DMZ >	Set following interfaces of the NAT rule. - WAN1 - LAN1 - LAN2 - DMZ
set type <1-to-1-nat | multi-1-to-1-nat-ip-range | multi-1-to-1-nat-cidr | port-forward>	Set the NAT type in the NAT rule. - 1 to 1 NAT - Multiple 1 to 1 NAT (Define the rule with IP range) - Multiple 1 to 1 NAT (Define the rule with CIDR) - Port forward
set protocol <tcp | udp | tcp/udp>	Set the protocol type in the port forwarding rule. - TCP - UDP - TCP/UDP (Both)
set original-port <start-port> <end-port>	Set the orginal starting port and the orginal ending port in the port forwarding rule.
set mapped-ip <ip>	Set the mapped IP addess in the port forwarding rule.
set mapped-port <start-port> <end-port>	Set the mapped starting port and the mapped ending port in the port forwarding rule.
preview	List the preview settings.
done	Keep current settings (the configuration has not yet been saved).
exit	Return to the upper layer of the command lines.
done force	Keep current settings without displaying prompt for confirmation (the configuration has not yet been saved).
exit force	Return to the upper layer of the command lines without displaying prompt for confirmation.

7. Once you decide to save the configuration, input "save" and press enter.
8. Input "yes" and press enter to write the configuration.

The Routing Tab

Static Route

Static routes are generally used when no appropriate dynamic route is present, or when you want the traffic to follow the static route you specify as opposed to following the dynamic route that is automatically learned and generated by the device.

Use the [Static Route] tab to view a list of current static routes on the device and configure their settings.

The following table describes the tasks you can perform in NAT Rule function in CLI mode.

Task	Description
Add a static route	create a new static route rule.
Edit a static route	edit the existing static route rule.
Delete a static route	delete the existing static route rule.

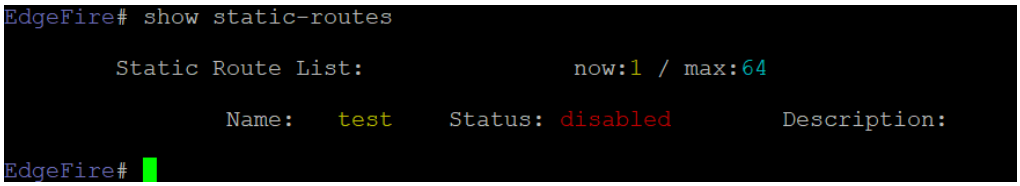
Viewing Static Route

Procedure (For EdgeFire, Gateway Mode)

1. Log on to the CLI management console.
2. Input the below commands.

```
EdgeIPS-Pro$ enable
EdgeIPS-Pro# show static-routes
```

3. The output displays the system information below.



Configuring Static Route

Procedure (For EdgeFire, Gateway Mode)

1. Log on to the CLI management console.
2. Input the below commands.

```
EdgeFire$ enable
EdgeFire# set configure
EdgeFire# edit static-routes
```

3. The output displays the system information below. Now you are already in the editor mode to configure the network.

```
EdgeFire(set configure)# edit static-routes

    Static Route List:          now:1 / max:64

        Name:  test   Status: disabled      Description:

EdgeFire(cfg-edit static-routes)#
```

4. Input the below command lines to create/edit/delete the static route rule.

Command Line	Description
edit <route-name>	Create a new static route rule or edit an existing static router rule.
delete <route-name>	Delete the existing static route rule.
preview	List the preview settings.
done	Keep current settings (the configuration has not yet been saved).
exit	Return to the upper layer of the command lines.
done force	Keep current settings without displaying prompt for confirmation (the configuration has not yet been saved).
exit force	Return to the upper layer of the command lines without displaying prompt for confirmation.

5. If you already create a static route rule for editing, input the below command lines.

Command Line	Description
set enabled <true | false>	Enable or disable the static route rule.
set name <new-name>	Set the name of the static route rule.
set description <description>	Set the description of the static route rule.
set destination-ip <ip-addr> <mask>	Set the destination IP address and network mask of the static route rule.
set gateway-ip <ip-addr>	Set the gateway IP address and network mask of the static route rule.
set interface <name>	Set the intergateway IP address and the network mask of the static route rule.
set metric <number>	Set the metric value as the weight value for routing. (Value: 1~15).
preview	List the preview settings.
done	Keep current settings (the configuration has not yet been saved).
exit	Return to the upper layer of the command lines.
done force	Keep current settings without displaying prompt for confirmation (the configuration has not yet been saved).
exit force	Return to the upper layer of the command lines without displaying prompt for confirmation.

The Object Profiles Tab

Object profiles simplify policy management by storing configurations that can be used by Edge series.

You can configure the following types of object profiles for this device in CLI management console:

- **IP Object Profile**: Contains the IP addresses that you can apply to a policy rule.
- **Service Object Profile**: Contains the service definitions that you can apply to a policy rule. TCP port range, UDP port range, ICMP, and custom protocol number are defined here.
- **Antivirus Profile**: Contains the settings of antivirus profile that you can apply to a policy rule.

Viewing IP Object Profiles

Procedure (For EdgeIPS / EdgeIPS Pro / EdgeFire)

4. Log on to the CLI management console.
5. Input the below commands.

```
EdgeIPS-Pro$ enable
EdgeIPS-Pro# show ip-objects
```

6. The output displays the IP object profiles below.

```
EdgeIPS-Pro# show ip-objects
        IP Object Profile List:                 now:1 / max:256
                Name:   All             Description:
EdgeIPS-Pro#
```

Configuring IP Object Profiles

You can configure the IP address in an IP object profile, which can be used by other policy rules.

The types of IP addresses you can assign to are:

- Single IP address
  For example: `192.168.1.1`
- IP ranges
  For example: from `192.168.1.1` to `192.168.1.20`
- IP subnets
  For example: `192.168.1.0/24`

Procedure (For EdgeIPS / EdgeIPS Pro / EdgeFire)

1. Log on to the CLI management console.

2. Input the below commands.

```
EdgeIPS-Pro$ enable
EdgeIPS-Pro# set configure
EdgeIPS-Pro# edit ip-objects
```

3. The output displays the system information below. Now you are already in the editor mode to configure the network.

```
EdgeIPS-Pro(set configure)# edit ip-objects
    IP Object Profile List:                    now:0 / max: 32
EdgeIPS-Pro(cfg-edit ip-objects)#
```

4. Input the command lines. to create a new profile "test".

```
EdgeIPS-Pro(cfg-edit ip-objects)# edit test
    IP Object Profile:
        Name:   test
        Description:
        IP object list:          now:0 / max:8
EdgeIPS-Pro(cfg-edit ip-objects)#
```

5. Input the command lines.to configure the network settings.

Command Line	Description
set ip <ip address>	Set the IP address of the device.
set dns <ip address>	Set the DNS address of the device.
set vlan tag <vlanId>	Enable VLAN and set the VLAN tag.
set vlan untag	Disable VLAN ID.
set lldp <enabled | disabled>	Enable / Disable LLDP function. Transmit via LLDP (Link Layer Discovery Protocol), allowing Edge series to advertise its identity and capabilities on the network.
save	Save the profile configuration.
preview	List the preview settings.
done	Keep current settings (the configuration has not yet been saved).
exit	Return to the upper layer of the command lines.
done force	Keep current settings without displaying prompt for confirmation (the configuration has not yet been saved). Note: The command is avaiable in EdgeFire 1.2.
exit force	Return to the upper layer of the command lines without displaying prompt for confirmation. Note: The command is avaiable in EdgeFire 1.2.

6. Input the command lines. to keep and save profile settings.

```
EdgeIPS-Pro(cfg-edit ip-objects)# done
EdgeIPS-Pro(cfg-edit ip-objects)# save
```

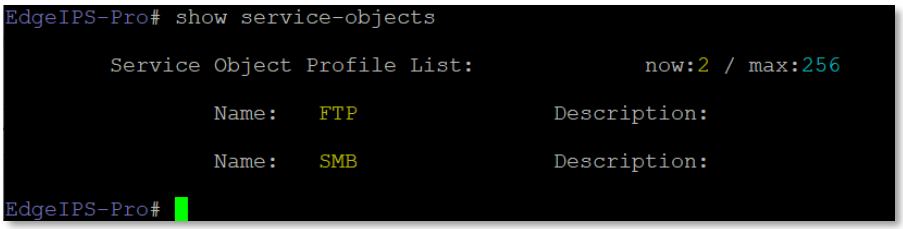
Viewing Service Object Profiles

Procedure (For EdgeIPS / EdgeIPS Pro / EdgeFire)

1. Log on to the CLI management console.
2. Input the below commands.

```
EdgeIPS-Pro$ enable
EdgeIPS-Pro# show service-objects
```

3. The output displays the service object profiles below.



Configuring Service Object Profiles

In a service object profile, you can define the following:

- TCP protocol port range
  For example: TCP port 100 ~ 120
- UDP protocol port range
  For example: UDP port 100 ~ 120
- ICMP protocol type and code
  For example: ICMP type 8 code 0
- Custom protocol with specified protocol number
  For example: protocol number = 6 and service ports range from 100 to 120

Note: The term 'protocol number' refers to the protocol number defined in the internet protocol suite.

Procedure (For EdgeIPS / EdgeIPS Pro / EdgeFire)

1. Log on to the CLI management console.
2. Input the below commands.

```
EdgeIPS-Pro$ enable
EdgeIPS-Pro# set configure
EdgeIPS-Pro# edit service-objects
```

3. The output displays the system information below. Now you are already in the editor mode to configure network.

```
EdgeIPS-Pro(set configure)# edit service-objects
    Service Object Profile List:                now:0 / max: 32
EdgeIPS-Pro(cfg-edit service-objects)#
```

4. Input the command lines to create a new profile "test".

```
EdgeIPS-Pro(cfg-edit service-objects)# edit test

    Service Object Profile:

        Name:   test

        Description:

        Service object list:          now:0 / max:8

EdgeIPS-Pro(cfg-edit service-objects)#
```

5. Input the command lines below to configure the network settings.

Command Line	Description
set name <new-name>	Set the profile name of the service object.
set description <description>	Set the profile description of the service object.
append tcp <start-port> <end-port>	Set the port range of TCP protocol.
append ucp <start-port> <end-port>	Set the port range of UDP protocol.
append icmp <type> <code>	Set the type and code of ICMP protocol.
append custom <type> <code>	Set the type and code of the custom protocol.
remove <index>	Remove the service profile in the desginated index.
save	Save the profile configuration.
preview	List the preview settings.
done	Keep current settings (the configuration has not yet been saved).
exit	Return to the upper layer of the command lines.
done force	Keep current settings without displaying prompt for confirmation (the configuration has not yet been saved). Note: The command is avaiable in EdgeFire 1.2.
exit force	Return to the upper layer of the command lines without displaying prompt for confirmation. Note: The command is avaiable in EdgeFire 1.2.

6. Input the command lines below to keep and save the profile settings.

```
EdgeIPS-Pro(cfg-edit service-objects)# done

EdgeIPS-Pro(cfg-edit service-objects)# save
```

Viewing Antivirus Profiles

Procedure (For EdgeIPS Pro)

1. Log on to the CLI management console.
2. Input the below commands.

```
EdgeIPS-Pro$ enable
EdgeIPS-Pro# show antivirus-profiles
```

3. The output displays the service object profiles below.

```
EdgeIPS-Pro# show antivirus-profiles
       Antivirus Profile List:                  now:2 / max:256
       Name:   default          Description:
       Name:   All              Description:
EdgeIPS-Pro#
```

Note: Only EdgeIPS Pro supports antivirus feature.

Configuring Antivirus Profiles

Antivirus is a stream-based design. The Antivirus Profiles are available to configure and view HTTP and FTP protocols and the advanced settings which include the file size limitation setting and compressed file scanning, allowing you to create or edit profiles to apply to a policy rule.

In a profile, you can define the following:

- Protocol settings: include HTTP and FTP
  Advanced settings: include the file size limitation and compressed file scanning

Procedure (For EdgeIPS Pro)

1. Log on to the CLI management console.
2. Input the below commands.

```
EdgeIPS-Pro$ enable
EdgeIPS-Pro# set configure
EdgeIPS-Pro# edit antivirus-profiles
```

3. The output displays the system information below. Now you are already in the editor mode to configure the file size limitation network.

```
EdgeIPS-Pro(set configure)# edit antivirus-profiles
      Antivirus Profile List:                  now:0 / max: 256
EdgeIPS-Pro(cfg-edit antivirus-profiles)#
```

4. Input the command lines below to create a new profile “test”.

```
EdgeIPS-Pro(cfg-edit antivirus-profiles)# edit test

    Antivirus Profile:

        Name:  test

        Description:

EdgeIPS-Pro(cfg-edit antivirus-profiles)#
```

5. Input the command lines below to configure the antivirus profile.

Command Line	Description
Set name <new-name>	Profile name of antivirus profile.
Set description <description>	Profile description of antivirus profile.
edit protocol-settings	Enter and edit the protocol settings in the antivirus profile.
set file-size-settings enabled <maximum-file-size> <if-drop-over-size>	Enable maximum file size for scanning: the file size range is 1~10MB and the oversized file will be skipped.
set file-size-settings disabled	Disable maximum file size for scanning.
set compressed-file-settings enabled <if-drop-password-protected-file> <if-drop-malformed>	Enable scanning for compressed file and activate the action of "Deny password protected file" and "Destroy file cannot be Decompressed" if needed. The scanning only support ZIP and GZIP file format.
set compressed-file-settings disabled	Disable scanning for compressed file.
remove <index>	Remove the antivirus profile in the desginated index.
save	Save the profile configuration.
preview	List the preview settings.
done	Keep current settings (the configuration has not yet been saved).
exit	Return to the upper layer of the command lines.

6. If you need to edit the protocol settings in the antivirus profile, input the command line to keep and save the profile settings.

```
EdgeIPS-Pro(cfg-edit antivirus-profiles)# edit protocol-settings
```

   a. If you need to edit the protocol settings in the antivirus profile, input the command lines to keep and save the profile settings.

Command Line	Description
set http enabled <accept | deny>	Enable the file scanning via http protocol and the action when matched, including Accept and Log, Deny and Log.
set http disabled	Disable the file scanning via HTTP protocol.
set ftp enabled <accept | deny>	Enable/Disable the file scanning via FTP protocol and the action when matched, including 'Accept and Log' and 'Deny and Log.'
set ftp disabled	Disable the file scanning via ftp protocol.
preview	List the protocol setings.
done	Keep current settings (the configuration has not yet been saved).
exit	Return to the upper layer of the command lines.

   b. Input the command lines to keep and save the profile settings.

```
EdgeIPS-Pro(cfg-edit antivirus-profiles)# done
EdgeIPS-Pro(cfg-edit antivirus-profiles)# save
```

7. If you need to edit the protocol settings in the antivirus profile, input the command lines below to keep and save the profile settings.

```
EdgeIPS-Pro(cfg-edit antivirus-profiles)# done
EdgeIPS-Pro(cfg-edit antivirus-profiles)# save
```

Note: The supported archive file formats include zip and gzip files.

The Security Tab

This chapter describes the general settings for security, including cyber security, policy enforcement, policy rule auto-learning and suspicious objects.

Policy Enforcement

Policy enforcement allows you to define a custom protocol that matches to an industrial protocol, and then allow or block activities that matches to the custom protocol in your network environment.

Note: For rule checking, the device rule list is of higher priority than the master rule list.

Note: Only the device rule list is configurable on CLI management console.

Viewing Policy Enforcement Rule Set(s)

Procedure (For EdgeIPS Pro)

1. Log on to the CLI management console.
2. Input the below commands.

```
EdgeIPS-Pro$ enable
EdgeIPS-Pro# show policy-enforcement-rulesets
```

3. The output displays the policy enforcement rule set(s) below.

```
EdgeIPS-Pro# show policy-enforcement-rulesets
        Policy Enforcement RuleSet List:                now:3 / max:64
                Name:   All             Description:        Last update:    2021-09-09T14:16:15+08:00
                Name:   OnlyIPS         Description:        Last update:    2021-08-19T22:52:01+08:00
                Name:   AV              Description:        Last update:    2021-09-06T18:27:17+08:00
```

Note: Only EdgeIPS Pro supports policy enforcement rule set(s).

Configuring Policy Enforcement Rule Set(s)

Procedure (For EdgeIPS Pro)

1. Log on to the CLI management console.
2. Input the below commands.

```
EdgeIPS-Pro$ enable
EdgeIPS-Pro# set configure
EdgeIPS-Pro# edit policy-enforcement-ruleset
```

3. The output displays the system information below. Now you are already in the editor mode to configure the network.

```
EdgeIPS-Pro(set configure)# edit policy-enforcement-rulesets
    Policy Enforcement RuleSet List:                    now:0 / max: 64
EdgeIPS-Pro(cfg-edit policy-enforcement-ruleset)#
```

4. Input the command lines to create a new ruleset "test".

```
EdgeIPS-Pro(cfg-edit policy-enforcement-ruleset)# edit test
    Policy Enforcement RuleSet:
        Name:  test
        Description:
EdgeIPS-Pro(cfg-edit policy-enforcement-ruleset)#
```

5. Input the command lines to configure policy enforcement rule set(s).

Command Line	Description
set name <new-name>	Set the name of the policy enforcement rule set.
set description <description>	Set the description of the policy enforcement rule set.
set default-action <accept | accept-log | deny-log>	Set the default-action of the policy enforcement rule set.
edit <rule-name>	Edit or create the policy enforcement rule set.
remove <rule-name>	Remove the policy enforcement rule set.
move <rule-name> <priority>	Move the policy enforcement rule set to the designated order.
preview	Preview the policy enforcement rule set.
done	Keep current settings (the configuration has not yet been saved).
Exit	Return to the upper layer of the command lines.

6. Once you decide to save the configuration, input "save" and press enter.
7. Input "exit" and press enter to leave the current function settings.

Note: Only EdgeIPS Pro supports policy enforcement rule set(s).

Viewing Policy Enforcement Rule(s)

Procedure (For EdgeIPS Pro)

1. Log on to the CLI management console.
2. Type the below commands (e.g. enter the name set "All")

```
EdgeIPS-Pro$ enable
EdgeIPS-Pro# edit policy-enforcement-rulesets
EdgeIPS-Pro(cfg-edit policy-enforcement-ruleset)# edit all
EdgeIPS-Pro(cfg-edit policy-enforcement-ruleset-all)# preview
```

3. The output displays the service object profile below.

```
EdgeIPS-Pro(cfg-policyEnforce-all)# preview

        Policy Enforcement Rule Settings:
                Name:           All
                Description:
                Default action: deny
                Rule list:                now:3 / max:2048

                        Priority: 1     Name:   ftp     Status: enabled

                        Priority: 2     Name:   smb     Status: enabled

                        Priority: 3     Name:   Adv.    Status: enabled
```

Procedure (For EdgeIPS)

1. Log on to the CLI management console.
2. Type the below commands

EdgeIPS$ enable **EdgeIPS#** show policy-enforcement

3. The output displays the service object profile below.

```
EdgeIPS# show policy-enforcement

        Policy Enforcement Rule Settings:       enabled
                Operation Mode:                  monitor
                Default Rule Action:             deny
                Rule List:              now:4 / max:512

                                Priority: 1     Name:   ftp     Status: enabled Description:

                                Priority: 2     Name:   smb     Status: enabled Description:

                                Priority: 3     Name:   Adv.    Status: enabled Description:

                                Priority: 4     Name:   ip      Status: disabled        Description:

EdgeIPS#
```

Procedure (For EdgeFire)

1. Log on to the CLI management console.
2. Type the below commands

EdgeFire$ enable **EdgeFire#** show policy-enforcement

3. The output displays the service object profile below.

```
EdgeFire# show policy-enforcement

        Policy Enforcement Rule Settings:       enabled
                Operation Mode:                  monitor
                Default Rule Action:             deny
                Rule List:              now:3 / max:512

                                Priority: 1     Name:   ftp     Status: enabled Description:

                                Priority: 2     Name:   smb     Status: enabled Description:

                                Priority: 3     Name:   Adv     Status: enabled Description:

EdgeFire#
```

Configuring Policy Enforcement Rule(s)

Procedure (For EdgeIPS Pro)

1. Log on to the CLI management console.
2. Input the below commands.

```
EdgeIPS-Pro$ enable
EdgeIPS-Pro# set configure
EdgeIPS-Pro(set configure) # edit policy-enforcement-ruleset
```

3. The output displays the system information below. Now you are already in the editor mode to configure the network.

```
EdgeIPS-Pro(set configure)# edit policy-enforcement-rulesets
    Policy Enforcement RuleSet List:                    now:0 / max: 64
EdgeIPS-Pro(cfg-edit policy-enforcement-ruleset)#
```

4. Input the command lines to create a new ruleset "test".

```
EdgeIPS-Pro(cfg-edit policy-enforcement-ruleset)# edit test
    Policy Enforcement RuleSet:
        Name:  test
        Description:
EdgeIPS-Pro(cfg-edit policy-enforcement-ruleset-test)#
```

5. Input the command lines to create a new rule "default".

```
EdgeIPS-Pro(cfg-policyEnforce-all)# edit default
    Policy Enforcement Rule:
        Name:  default      Status: enabled
        Description:
        Source IP Object:     any
        Destination IP object:  any
        Service Object:       any
        Vlan IDs:             disabled
        Action:               accept

        Protocol filter profile: disabled
        IPS profile:          disabled
        File filter profile:    disabled
        Antivirus profile:     disabled
EdgeIPS-Pro(cfg-policyEnforce-default)#
```

6. Input the command lines to configure the policy enforcement rule(s).

Command Line	Description
set name <new-name>	Set the name of policy enforcement rule.
set description <description>	Set the description of policy enforcement rule.
set enabled <true | false>	Enable or disable the policy enforcement rule.
set source-ip any	Set the source IP address to ANY.
set source-ip single <ip address>	Set the source IP address to the specific IP Address.
set source-ip range <start-ip address> <end-ip address>	Set the source IP address to the specific IP range.
set source-ip subnet <ip subnet> <cidr value>	Set the source IP address to the specific IP subnet.
set source-ip object <up-object-name>	Apply the specific IP object to the source IP address.
set destination-ip any	Set the destination IP address to ANY.
set destination-ip single <ip address>	Set the destination IP address to the specific IP Address.
set destination-ip range <start-ip address> <end-ip address>	Set the destination IP address to the specific IP range.
set destination-ip subnet <ip subnet> <cidr value>	Set the destination IP address to the specific IP subnet.
set destination-ip object <up-object-name>	Apply the specific IP object to the destination IP address.
set service any	Set the service port to ANY.
set service tcp <start-port> <end-port>	Set the service port to the specific TCP port range.

set service udp <start-port> <end-port>	Set the service port to the specific UCP port range.
set service icmp <type> <code>	Set the service port to the specific ICMP type and code.
set service custom <protocol-number>	Set the service port to be the custom protocol number.
set service object <service-object-name>	Apply the specific service object to the service port.
set vlan-id any	Set the VLAN ID to ANY.
set vlan-id [<vlan-id-1>, <vlan-id-2>, ...]	Set the VLAN ID to [<vlan-id-1>, <vlan-id-2>, ...]. The maximum number of VLAN ID for one policy enforcement is 5.
set action <accept | accept-log | deny-log>	Set the action to accept, accept & log or deny & log. Note: if you set the action to "deny-log", you cannot configure "ips-profile", "file-filter-profile" and "antivirus-profile" via the commands.
set protocol-filter-profile <profile-name>	Enable the protocol filter profile and import the designated profile.
set protocol-filter-profile disabled	Disable the protocol filter profile.
set ips-profile <profile-name>	Enable the IPS profile and import the designated profile.
set ips-profile disabled	Disable the IPS profile.
set file-filter-profile <profile-name>	Enable the file filter profile and import the designated profile.
set file-filter-profile disabled	Disable the file filter profile.
set antivirus-profile <profile-name>	Enable the antivirus profile and import the designated profile.
set antivirus-profile disabled	Disable the antivirus profile.
preview	List the preview settings.
done	Keep current settings (the configuration has not yet been saved).
exit	Return to the upper layer of the command lines.

7. Once you decide to save the configuration, input "save" and press enter.
8. Input "exit" and press enter to leave the current function settings.

Procedure (For EdgeIPS)

1. Log on to the CLI management console.
2. Input the below commands.

```
EdgeIPS$ enable

EdgeIPS# set configure

EdgeIPS(set configure) # edit policy-enforcement
```

3. The output displays the system information below. Now you are already in the editor mode to configure the policy enforcement. You can input the command lines to configure the policy enforcement settings.

EdgeIPS(set configure)# edit policy-enforcement

Policy Enforcement Rule: now:0 / max: 512

EdgeIPS(cfg-edit policy-enforcement)#

Command Line	Description
set enabled <true | false>	Enable or disable the policy enforcement settings.
set operation-mode <prevention | monitor>	Set the operation mode of policy enforcement to "prevention" mode or "monitor" mode.
set default-action <accept | accept-log | deny-log>	Set the default-action of the policy enforcement ruleset.
edit <rule-name>	Enter and edit the policy enforcement rule. For details, please refer to the information in step 4 and 5.
remove <rule-name>	Remove the policy enforcement rule in the desginated index.
move <rule-name> <priority>	Move the policy enforcement rule to the specific index.
preview	List the policy enforcement rule settings.
save	Save the profile configuration.
exit	Return to the upper layer of the command lines.

4. Input the command lines to create a new rule "default".

EdgeIPS(cfg-policyEnforce)# edit default

Policy Enforcement Rule:

Name: default Status: enabled

Description:

Source IP Object: any

Destination IP object: any

Service Object: any

Vlan IDs: disabled

Action: accept

Protocol filter profile: disabled

IPS profile: disabled

File filter profile: disabled

EdgeIPS(cfg-policyEnforce-default)#

5. Input the command lines below to configure the policy enforcement rule(s).

Command Line	Description
set name <new-name>	Set the name of the policy enforcement rule.
set description <description>	Set the description of the policy enforcement rule.
set enabled <true | false>	Enable or disable the policy enforcement rule.

set source-ip any	Set the source IP address to ANY.
set source-ip single <ip address>	Set the source IP address to the specific IP Address.
set source-ip range <start-ip address> <end-ip address>	Set the source IP address to the specific IP range.
set source-ip subnet <ip subnet> <cidr value>	Set the source IP address to the specific IP subnet.
set source-ip object <up-object-name>	Apply the specific IP object to the source IP address.
set destination-ip any	Set the destination IP address to ANY.
set destination-ip single <ip address>	Set the destination IP address to the specific IP Address.
set destination-ip range <start-ip address> <end-ip address>	Set the destination IP address to the specific IP range.
set destination-ip subnet <ip subnet> <cidr value>	Set the destination IP address to the specific IP subnet.
set destination-ip object <up-object-name>	Apply the specific IP object to the destination IP address.
set service any	Set the service port to ANY.
Set service tcp <start-port> <end-port>	Set the service port to the specific TCP port range.
set service udp <start-port> <end-port>	Set the service port to the specific UCP port range.
set service icmp <type> <code>	Set the service port to the specific ICMP type and code.
set service custom <protocol-number>	Set the service port to be the custom protocol-number.
set service object <service-object-name>	Apply the specific service object to the service port.
set vlan-id any	Set the VLAN ID to ANY.
set vlan-id [<vlan-id-1>, <vlan-id-2>, ...]	Set the VLAN ID to [<vlan-id-1>, <vlan-id-2>, ...]. The maximum number of VLAN ID for one policy enforcement is 5.
set action <accept | accept-log | deny-log>	Set the action to accept, accept & log or deny & log. Note: if you set the action to "deny-log", you cannot configure "ips-profile", "protocol-filter-profile" and "file-filter-profile" via the commands.
set protocol-filter-profile <profile-name>	Enable the protocol filter profile and import the designated profile.
set protocol-filter-profile disabled	Disable the protocol filter profile.
set ips-profile <profile-name>	Enable the IPS profile and import the designated profile.
set ips-profile disabled	Disable the IPS profile.
set file-filter-profile <profile-name>	Enable the file filter profile and import the designated profile.
set file-filter-profile disabled	Disable the file filter profile.
preview	List the preview settings.
done	Keep current settings (the configuration has not yet been saved).
exit	Return to the upper layer of the command lines.

6. Once you decide to save the configuration, input "save" and press enter.

7. Input "exit" and press enter to leave the current function settings.

Procedure (For EdgeFire, Gateway Mode)

1. Log on to the CLI management console.
2. Input the below commands.

```
EdgeFire$ enable
EdgeFire# set configure
EdgeFire(set configure) # edit policy-enforcement
```

3. The output displays the system information below. Now you are already in the editor mode to configure the policy enforcement. You can input the the command lines to configure the policy enforcement settings.

```
EdgeFire(set configure)# edit policy-enforcement
    Policy Enforcement Rule:                now:0 / max: 512
EdgeFire(cfg-edit policy-enforcement)#
```

Command Line	Description
set enabled <true | false>	Enable or disable the policy enforcement settings.
set operation-mode <prevention | monitor>	Set the operation mode of policy enforcement to "prevention" mode or "monitor" mode.
set default-action <accept | accept-log | deny-log>	Set the default-action of the policy enforcement ruleset.
edit <rule-name>	Enter and edit the policy enforcement rule. For details, please refer to the information in step 4 and 5.
remove <rule-name>	Remove the policy enforcement rule in the desginated index.
move <rule-name> <priority>	Move the policy enforcement rule to the specific index.
preview	List the policy enforcement rule settings.
save	Save the profile configuration.
exit	Return to the upper layer of the command lines.
save force	Save the profile configuration without displaying prompt for confirmation.
exit force	Return to the upper layer of the command lines without displaying prompt for confirmation.

4. Input the the command lines to create a new rule "default".

```
EdgeFire(cfg-edit policy-enforcement)# edit default
    Policy Enforcement Rule:
        Name:  default      Status: enabled
        Description:
        Source IP Object:     any
        Destination IP object:  any
        Service Object:       any
        Interface Direction:   any
        Action:            accept

        Protocol filter profile: disabled
        IPS profile:         disabled
        File filter profile:   disabled
EdgeFire(cfg-policyEnforcement-default)#
```

5. Input the command lines below to configure the policy enforcement rule(s).

Command Line	Description
set name <new-name>	Set the name of the policy enforcement rule.
set description <description>	Set the description of the policy enforcement rule.
set enabled <true | false>	Enable or disable the policy enforcement rule.
set source-ip any	Set the source IP address to ANY.
set source-ip single <ip address>	Set the source IP address to the specific IP Address.
set source-ip range <start-ip address> <end-ip address>	Set the source IP address to the specific IP range.
set source-ip subnet <ip subnet> <cidr value>	Set the source IP address to the specific IP subnet.
set source-ip object <up-object-name>	Apply the specific IP object to the source IP address.
set destination-ip any	Set the destination IP address to ANY.
set destination-ip single <ip address>	Set the destination IP address to the specific IP Address.
set destination-ip range <start-ip address> <end-ip address>	Set the destination IP address to the specific IP range.
set destination-ip subnet <ip subnet> <cidr value>	Set the destination IP address to the specific IP subnet.
set destination-ip object <up-object-name>	Apply the specific IP object to the destination IP address.
set service any	Set the service port to ANY.
Set service tcp <start-port> <end-port>	Set the service port to the specific TCP port range.
set service udp <start-port> <end-port>	Set the service port to the specific UCP port range.

set service icmp <type> <code>	Set the service port to the specific ICMP type and code.
set service custom <protocol-number>	Set the service port to be the custom protocol-number.
set service object <service-object-name>	Apply the specific service object to the service port.
set interface-direction <any | wan-to-lan | lan-to-wan | wan-to-dmz | dmz-to-wan | lan-to-dmz | dmz-to-lan | lan-to-lan >	Set the interface direction to check the connection traffic in the policy enforcement rule(s). - **any:** no restriction on direction. EdgeFire checks all the connection traffic from any network interfaces. - **wan-to-lan:** EdgeFire checks the connection traffic from the WAN interface to the LAN interface. - **lan-to-wan:** EdgeFire checks the connection traffic from the LAN interface to the WAN interface. - **wan-to-dmz:** EdgeFire checks the connection traffic from the WAN interface to the DMZ interface. - **dmz-to-wan:** EdgeFire checks the connection traffic from the DMZ interface to the WAN interface. - **lan-to-dmz:** EdgeFire checks the connection traffic from the LAN interface to the DMZ interface. - **dmz-to-lan:** EdgeFire checks the connection traffic from the DMZ interface to the LAN interface. - **lan-to-lan:** EdgeFire checks the connection traffic from the LAN interface to another LAN interface. e.g. **set interface-direction wan-to-lan**
set action <accept | accept-log | deny-log>	Set the action to accept, accept & log or deny & log. Note: if you set the action to "deny-log", you cannot configure "ips-profile", "protocol-filter-profile" and "file-filter-profile" via the commands.
set protocol-filter-profile <profile-name>	Enable the protocol filter profile and import the designated profile.
set protocol-filter-profile disabled	Disable the protocol filter profile.
set ips-profile <profile-name>	Enable the IPS profile and import the designated profile.
set ips-profile disabled	Disable the IPS profile.
set file-filter-profile <profile-name>	Enable the file filter profile and import the designated profile.
set file-filter-profile disabled	Disable the file filter profile.
preview	List the preview settings.
done	Keep current settings (the configuration has not yet been saved).

exit	Return to the upper layer of the command lines.
done force	Keep current settings without displaying prompt for confirmation (the configuration has not yet been saved).
exit force	Return to the upper layer of the command lines without displaying prompt for confirmation.

6. Once you decide to save the configuration, input "save" and press enter.
7. Input "exit" and press enter to leave the current function settings.

Procedure (For EdgeFire, Bridge Mode)

1. Log on to the CLI management console.
2. Input the below commands.

```
EdgeFire$ enable
EdgeFire# set configure
EdgeFire(set configure) # edit policy-enforcement
```

3. The output displays the system information below. Now you are already in the editor mode to configure policy enforcement. You can input the command lines to configure policy enforcement settings.

```
EdgeFire(set configure)# edit policy-enforcement
    Policy Enforcement Rule:                now:0 / max: 512
EdgeFire(cfg-edit policy-enforcement)#
```

Command Line	Description
set enabled <true | false>	Enable or disable the policy enforcement settings.
set operation-mode <prevention | monitor>	Set the operation mode of policy enforcement to "prevention" mode or "monitor" mode.
set default-action <accept | accept-log | deny-log>	Set the default-action of policy enforcement ruleset.
edit <rule-name>	Enter and edit the policy enforcement rule. For details, please refer to the information in step 4 and 5.
remove <rule-name>	Remove the policy enforcement rule in the desginated index.
move <rule-name> <priority>	Move the policy enforcement rule to the specific index
preview	List the policy enforcement rule settings.
save	Save the profile configuration.
exit	Return to the upper layer of the command lines.
save force	Save the profile configuration without displaying prompt for confirmation.
exit force	Return to the upper layer of the command lines without displaying prompt for confirmation.

4. Input the command lines to create a new rule "default".

```
EdgeFire(cfg-edit policy-enforcement)# edit default

    Policy Enforcement Rule:

        Name:   default                    Status: enabled

        Description:

        Source IP Object:       any

        Destination IP object:  any

        Service Object:         any

        Vlan IDs:               disabled

        Action:                 accept


        Protocol filter profile:  disabled

        IPS profile:              disabled

        File filter profile:      disabled

EdgeFire(cfg-policyEnforcement-default)#
```

5. Input the command lines below to configure policy enforcement rule(s).

Command Line	Description
set name <new-name>	Set the name of policy enforcement rule.
set description <description>	Set the description of policy enforcement rule.
set enabled <true | false>	Enable or disable the policy enforcement rule.
set source-ip any	Set the source IP address to ANY.
set source-ip single <ip address>	Set the source IP address to the specific IP Address.
set source-ip range <start-ip address> <end-ip address>	Set the source IP address to the specific IP range.
set source-ip subnet <ip subnet> <cidr value>	Set the source IP address to the specific IP subnet.
set source-ip object <up-object-name>	Apply the specific IP object to the source IP address.
set destination-ip any	Set the destination IP address to ANY.
set destination-ip single <ip address>	Set the destination IP address to the specific IP Address.
set destination-ip range <start-ip address> <end-ip address>	Set the destination IP address to the specific IP range.
set destination-ip subnet <ip subnet> <cidr value>	Set the destination IP address to the specific IP subnet.
set destination-ip object <up-object-name>	Apply the specific IP object to the destination IP address.
set service any	Set the service port to ANY.
Set service tcp <start-port> <end-port>	Set the service port to the specific TCP port range.
set service udp <start-port> <end-port>	Set the service port to the specific UCP port range.

set service icmp <type> <code>	Set the service port to the specific ICMP type and code.
set service custom <protocol-number>	Set the service port to be the custom protocol-number.
set service object <service-object-name>	Apply the specific service object to the service port.
set vlan-id any	Set the VLAN ID to ANY.
set vlan-id [<vlan-id-1>, <vlan-id-2>, ...]	Set the VLAN ID to [<vlan-id-1>, <vlan-id-2>, ...]. The maximum number of VLAN ID for one policy enforcement is 5.
set action <accept | accept-log | deny-log>	Set the action to accept, accept & log or deny & log. Note: if you set the action to "deny-log", you cannot configure "ips-profile", "protocol-filter-profile" and "file-filter-profile" via the commands.
set protocol-filter-profile <profile-name>	Enable the protocol filter profile and import the designated profile.
set protocol-filter-profile disabled	Disable the protocol filter profile.
set ips-profile <profile-name>	Enable the IPS profile and import the designated profile.
set ips-profile disabled	Disable the IPS profile.
set file-filter-profile <profile-name>	Enable the file filter profile and import the designated profile.
set file-filter-profile disabled	Disable the file filter profile.
preview	List the preview settings.
done	Keep current settings (the configuration has not yet been saved).
exit	Return to the upper layer of the command lines.
done force	Keep current settings without displaying prompt for confirmation (the configuration has not yet been saved).
exit force	Return to the upper layer of the command lines without displaying prompt for confirmation.

6. Once you decide to save the configuration, input "save" and press enter.
7. Input "exit" and press enter to leave the current function settings.

Port Security Settings

This feature allows the network user to configure security settings for each port interface in EdgeIPS Pro. When port security is configured for each interface, related actions will be performed, applying to the security profiles and settings.

Viewing Port Security

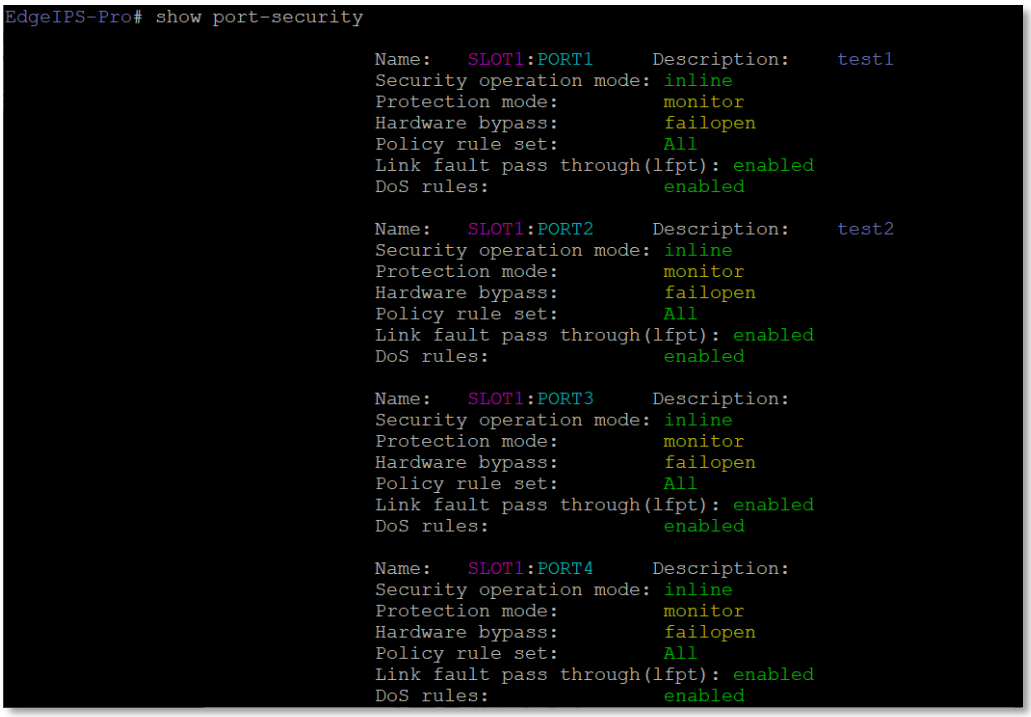
Procedure (For EdgeIPS Pro)

1. Log on to the CLI management console.
2. Input the below commands.

```
EdgeIPS-Pro$ enable

EdgeIPS-Pro# show port-security
```

3. The output displays the service object profiles below.



Note: Only EdgeIPS Pro supports Port Security.

Configuring Port Security

Procedure (For EdgeIPS Pro)

1. Log on to the CLI management console.
2. Input the below commands.

```
EdgeIPS-Pro$ enable
EdgeIPS-Pro$ set configure
EdgeIPS-Pro(set configure)# edit port-security
```

3. The output displays the system information below. Now you are already in the editor mode. You can input the command lines below to configure port security settings.

4. Input the command lines to configure the designated port or designated multiple ports.

```
EdgeIPS-Pro(set configure)# edit port-security
                    Name:  SLOT1:PORT1   Description:   test1
                    Security operation mode: inline
                    Protection mode:       monitor
                    Hardware bypass:       failopen
                    Policy rule set:       All
                    Link fault pass through(lfpt): enabled
                    DoS rules:             enabled

                    Name:  SLOT1:PORT2   Description:   test2
                    Security operation mode: inline
                    Protection mode:       monitor
                    Hardware bypass:       failopen
                    Policy rule set:       All
                    Link fault pass through(lfpt): enabled
                    DoS rules:             enabled
                                           .
                                           .
                                           .
EdgeIPS-Pro(cfg-edit port-security)#
```

Command Line	Description
edit <slot name> <port name>	Edit the designated port and slot for configuration. For example, edit slot1:port1.
clone <source slot name> <source port name> <target slot name> <target port name>	Clone the port security settings from the referred port and slot to the designated port and slot. For example, clone slot1:port1 slot2:port1 Note: Once the designated odd/even port is applied to the new configuration, the mapped odd/even port is also updated. For example, if the user clones the port security configuration of port 1 in slot 1 to port 1 in slot 3, port 2 in slot 3 will also be updated with the same configuration. Port 1 and port 2 in slot 3 are considered one pair connecting to the OT asset and the upper layer management switch in OT operation.
preview	List the preview settings.
save	Save the current settings.
exit	Return to the upper layer of the command lines.

5. Once you decide to configure the designated port or multiple ports, input the the command lines to configure the port security.

Command Line	Description
set description <description> set security-operation-mode <inline | offline>	Set the description of the designated port or multiple ports.
set protection-mode <prevention | monitor>	Set the mode to "prevention" mode or "monitor" mode.
set hardware-bypass <fail-open | fail-close | force-open>	Set the hardware bypass mode to the port(s). • fail-open: the port is set to bypass the traffic when EdgeIPS Pro is failed to operate.

	• fail-close: the port is set to block the traffic when EdgeIPS Pro is failed to operate. • force-open: enforce the port to bypass the traffic.
set lfpt <enabled | disabled>	Enable or disable the Link Fault Pass Through (LFPT) function to the designated port(s).
set policy-enforcement enabled <ruleset-name>	Apply the designated policy enforcement ruleset to the port(s).
set policy-enforcement disabled	Disable the policy enforcement rule function in the port(s).
set dos <enabled | disabled>	Enable or disable Denial of Service Prevention (DOS) function in the port(s).
set dos-rule enabled <rule-name> <threshold>	Enable the rule of Denial of Service Prevention (DOS) function and set the threshold. • TCP_SYN_Flood (threshold: 10000) • TCP_Port_FIN_Scan (threshold: 10000) • TCP_Port_Xmas_Scan (threshold: 10000) • UDP_Flood (threshold: 10000) • ICMP_Flood (threshold: 250) • IGMP_Flood (threshold: 1800) • UDP_Port_Scan (threshold: 1800) • TCP_Port_SYN_Scan (threshold: 1800) • TCP_Port_NULL_Scan (threshold: 1800)
set dos-rule disabled <rule-name>	Disable the rule of Denial of Service Prevention (DOS) function. • TCP_SYN_Flood • TCP_Port_FIN_Scan • TCP_Port_Xmas_Scan • UDP_Flood • ICMP_Flood • IGMP_Flood • UDP_Port_Scan • TCP_Port_SYN_Scan • TCP_Port_NULL_Scan
preview	List the preview settings.
done	Keep current settings (the configuration has not yet been saved).
exit	Return to the upper layer of the command lines.

6. Once you decide to save the configuration, input "save" and press enter.
7. Input "exit" and press enter to leave the current function settings.

The QoS Tab

The QoS (Quality of Service) guarantee technology in Edge series allows the network administrator to manage, monitor and allocate bandwidth for the production-critical network traffic of each pair's egress port in real-time.

Viewing Bandwidth MGMT

Procedure (For EdgeIPS Pro)

1. Log on to the CLI management console.
2. Input the below commands.

```
EdgeIPS-Pro$ enable
EdgeIPS-Pro# show bandwidth-management
```

3. The output displays the service object profiles below.

```
EdgeIPS-Pro# show bandwidth-management

                        Name:           SLOT1:PORT1
                        Enabled:        disabled
                        Egress rate:    1000
                        Description:

                        Name:           SLOT1:PORT2
                        Enabled:        disabled
                        Egress rate:    1000
                        Description:
```

Note: Only EdgeIPS Pro supports bandwidth MGMT.

Configuring Bandwidth MGMT

Procedure (For EdgeIPS Pro)

1. Log on to the CLI management console.
2. Input the below commands.

```
EdgeIPS-Pro$ enable
EdgeIPS-Pro# set configure
EdgeIPS-Pro# edit bandwidth-management
```

3. The output displays the system information below. Now you are already in the editor mode. You can input the command lines to configure bandwidth MGMT.

```
EdgeIPS-Pro(set configure)# edit bandwidth-management
                Name:         SLOT1:PORT1
                Enabled:      disabled
                Egress rate:  1000
                Description:

                Name:         SLOT1:PORT2
                Enabled:      disabled
                Egress rate:  1000
                Description:
                              .
                              .
                              .
EdgeIPS-Pro(cfg-edit bandwidth-management)#
```

Command Line	Description
edit <slot name> <port name>	Edit the designated slot and the port.
preview	List the preview settings.
save	Save current settings.
exit	Return to the upper layer of the command lines.

4. Once you decide to configure the designated port or multiple ports, input the command lines to configure the port security. After editing the bandwidth management settings, input "done" and "exit" to the upper layer of the command lines.

```
EdgeIPS-Pro(cfg-edit bandwidth-management)# edit SLOT1 PORT1
                Name:         SLOT1:PORT1
                Enabled:      disabled
                Egress rate:  1000
                Description:
EdgeIPS-Pro(cfg-edit bandwidth-management)#
```

Command Line	Description
set enabled <true | false>	Enable or disable the bandwidth MGMT for the port.
set egress-rate-limit <egress rate>	Set the egress rate. (range: 1-1000 unit: MB)
set description	Set the description of bandwidth MGMT for the port.
preview	List the preview settings.

done	Keep current settings (the configuration has not yet been saved).
exit	Return to the upper layer of the command lines.

5. Once you decide to save the configuration, input “save” and press enter.
6. Input “exit” and press enter to leave the current function settings.

The Administration Tab

This chapter describes the available administrative settings for Edge series.

Configuring Device Name and Device Location Information

Procedure (For EdgeIPS / EdgeIPS Pro / EdgeFire)

1. Log on to the CLI management console.
2. Input the below commands.

```
EdgeIPS-Pro$ enable
EdgeIPS-Pro# set configure
EdgeIPS-Pro(set configure)# edit device
```

3. The output displays the system information below. Now you are already in the editor mode. You can input the command lines to configure device settings.

```
EdgeIPS-Pro(set configure)# edit device

        Host name:    EdgeIPS-Pro        Location:

EdgeIPS-Pro(cfg-edit device)#
```

Command Line	Description
set hostname	Set the hostname of the device.
set location	Set the location description of the device.
preview	List the preview settings.
save	Save current settings.
exit	Return to the upper layer of the command lines.
save force	Save current settings without displaying prompt for confirmation. Note: This command supports only in EdgeFire 1.2.
exit force	Return to the upper layer of the command lines without displaying prompt for confirmation. Note: This command supports only in EdgeFire 1.2.

4. Once you decide to save the configuration, input "save" and press enter.
5. Input "exit" and press enter to leave the current function settings.

Configuring Management Protocols and Ports

Procedure (For EdgeIPS / EdgeIPS Pro / EdgeFire)

1. Log on to the CLI management console.

2. Input the below commands.

```
EdgeIPS-Pro$ enable
EdgeIPS-Pro# set configure
EdgeIPS-Pro(set configure)# edit remote-access
```

3. The output displays the system information below. Now you are already in the editor mode. You can input the command lines to configure the management protocol/port settings.

```
EdgeIPS-Pro(set configure)# edit remote-access

                HTTP port:      80      disabled
                HTTPS port:     443     enabled
                SSH port:       22      enabled
                Telnet port:    23      disabled

EdgeIPS-Pro(cfg-edit remote-access)#
```

Command Line	Description
set http enabled <port-number>	Enable HTTP protocol for the login of web management console and set the port number. Note: when HTTP protocol is enabled, HTTPS protocol will be disabled.
set https enabled <port-number>	Enable HTTPS protocol for the login of web management console and set the port number. Note: when HTTPS protocol is enabled, HTTP protocol will be disabled.
set ssh enabled <port-number>	Enable SSH protocol for the login of SSH client and set the port number.
set ssh disabled	Disable SSH protocol for the login of SSH client.
set telnet enabled <port-number>	Enable TELNET protocol for the login of TELNET client and set the port number.
set telnet disabled	Disable TELNET protocol for the login of TELNET client.
preview	List the preview settings.
save	Save current settings.
exit	Return to the upper layer of the command lines.
save force	Save current settings without displaying prompt for confirmation. Note: This command supports only in EdgeFire 1.2.
exit force	Return to the upper layer of the command lines without displaying prompt for confirmation. Note: This command supports only in EdgeFire 1.2.

4. Once you decide to save the configuration, input "save" and press enter.
5. Input "exit" and press enter to leave the current function settings.

Viewing Access Control List

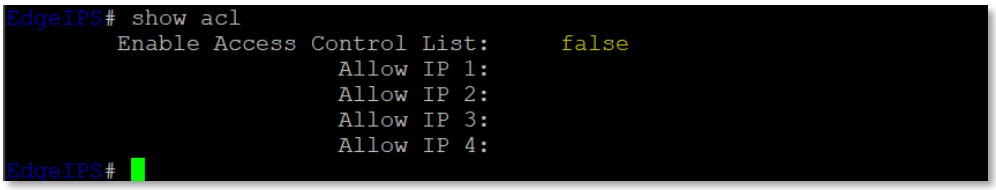
Procedure (For EdgeIPS / EdgeIPS Pro / EdgeFire)

1. Log on to the CLI management console.

2. Input the below commands.

```
EdgeIPS-Pro$ enable
EdgeIPS-Pro# show acl
```

3. The output displays the access control list below.



Configuring Access Control List

Procedure (For EdgeIPS / EdgeIPS Pro / EdgeFire)

1. Log on to the CLI management console.
2. Input the below commands.

```
EdgeIPS-Pro$ enable
EdgeIPS-Pro# set configure
EdgeIPS-Pro(set configure)# edit acl
```

3. The output displays the system information below. Now you are already in the editor mode. You can input the command lines to configure the Access Control List settings.

```
EdgeIPS-Pro(set configure)# edit acl

        Enable Access Control List:    false
                        Allow IP 1:
                        Allow IP 2:
                        Allow IP 3:
                        Allow IP 4:

EdgeIPS-Pro(cfg-edit acl)#
```

```
EdgeFire(set configure)# edit acl

        Access from WAN:       enabled

        Enable Access Control List:    false
                        Allow IP 1:
                        Allow IP 2:
                        Allow IP 3:
                        Allow IP 4:
```

Command Line	Description
set enabled <true | false>	Enable or disable the access control list function.
set ip [ip1,ip2,ip3,ip4]	Add/update the IP address(es) into the access control list.

set access-wan <enabled | disabled>	Enable or disable the access from the WAN interface Note: Only EdgeFire supports this command.
preview	List the preview settings.
save	Save current settings.
exit	Return to the upper layer of the command lines.
save force	Save current settings without displaying prompt for confirmation. Note: This command supports only in EdgeFire 1.2.
exit force	Return to the upper layer of the command lines without displaying prompt for confirmation. Note: This command supports only in EdgeFire 1.2.

4. Once you decide to save the configuration, input "save" and press enter.
5. Input "exit" and press enter to leave the current function settings.

Display ODC Sync Settings

Procedure (For EdgeIPS / EdgeIPS Pro / EdgeFire)

1. Log on to the CLI management console.
2. Input the below commands.

```
EdgeIPS-Pro$ enable
EdgeIPS-Pro# show odc-server
```

3. The output displays the access control list below.

```
EdgeIPS# show odc-server
                Name:    10.24.7.45                    Status: enabled
EdgeIPS#
```

Configuring ODC Sync Settings

Procedure (For EdgeIPS / EdgeIPS Pro / EdgeFire)

1. Log on to the CLI management console.
2. Input the below commands.

```
EdgeIPS-Pro$ enable
EdgeIPS-Pro# set configure
EdgeIPS-Pro(set configure)# edit odc-server
```

3. The output displays the system information below. Now you are already in the editor mode. You can input the command lines to configure the ODC sync settings.

```
EdgeIPS(set configure)# edit odc-server

        Name:   10.24.7.45          Status: enabled

EdgeIPS(cfg-edit odc-server)#
```

Command Line	Description
set enabled <true | false>	Enable or disable the ODC sync settings.

set address <ip-address | domain-name>	Edit the IP address of domain name of ODC server.
preview	List the preview settings.
save	Save current settings.
exit	Return to the upper layer of command line.
save force	Save current settings without displaying prompt for confirmation. Note: This command supports only in EdgeFire 1.2.
exit force	Return to the upper layer of the command lines without displaying prompt for confirmation. Note: This command supports only in EdgeFire 1.2.

4. Once you decide to save the configuration, input "save" and press enter.
5. Input "exit" and press enter to leave the current function settings.

Viewing SNMP

Procedure (For EdgeIPS / EdgeIPS Pro / EdgeFire)

1. Log on to the CLI management console.
2. Input the below commands.

```
EdgeIPS-Pro$ enable
EdgeIPS-Pro# show snmp-settings
EdgeIPS-Pro# show snmp-trap-settings
```

3. The output displays the service object profiles below.

```
EdgeIPS# show snmp-settings

        Status:         disabled
        Port:           161
        v1/v2c Settings:
        v3 Settings:
EdgeIPS#
```

```
EdgeIPS# show snmp-trap-settings

        Snmp Trap Receivers:            now:0 / max:5

EdgeIPS#
```

Configuring SNMP Settings

Procedure (For EdgeIPS / EdgeIPS Pro / EdgeFire)

1. Log on to the CLI management console.
2. Input the below commands.

```
EdgeIPS-Pro$ enable
EdgeIPS-Pro# set configure
EdgeIPS-Pro# edit snmp-settings
```

3. The output displays the system information below. Now you are already in the editor mode. You can input the command lines to configure SNMP settings.

```
EdgeIPS-Pro(set configure)# edit snmp-settings
    Status:       disabled
    Port:         161
    v1/v2c Settings:
    v3 Settings:
EdgeIPS-Pro(cfg-edit snmp-settings)#
```

Command Line	Description
set enabled <true | false>	Enable or disable SNMP settings.
set port <port-number>	Set the SNMP port. The default setting is Port 161.
edit community <community-name>	Set the community name.
remove community <community-name>	Remove the community name.
edit usm-user <user-name>	Add and configure a USM user.
remove usm-user <user-name>	Remove an existing USM user.
preview	List the preview settings.
save	Save current settings.
exit	Return to the upper layer of the command lines.
save force	Save current settings without displaying prompt for confirmation. Note: This command supports only in EdgeFire 1.2.
exit force	Return to the upper layer of the command lines without displaying prompt for confirmation. Note: This command supports only in EdgeFire 1.2.

4. If you want to create a new community name or edit an existing community name, you can input the command lines to configure SNMP settings (e.g. users create a new community "**test**"). After editing the community name, input "done" and "exit" to the upper layer of the command lines.

```
EdgeIPS-Pro(set configure)# edit snmp-settings
    Status:       disabled
    Port:         161
    v1/v2c Settings:
    v3 Settings:
EdgeIPS-Pro(cfg-edit snmp-settings)# edit community test
```

Command Line	Description
set name <new-name>	Edit the name of the community.
append trusted-address <<ip>|<ip> <cidr>>	To add the trusted IP address, you can add one single IP address (e.g. append trusted-address 1.1.1.1) or a sub network (e.g. append trusted-address 2.2.2.2 30).

remove <index>	Remove the trusted address in the designated index of priority.
preview	List the preview settings.
done	Keep current settings (the configuration has not yet been saved).
exit	Return to the upper layer of the command lines.
done force	Keep current settings without displaying prompt for confirmation (the configuration has not yet been saved). Note: This command supports only in EdgeFire 1.2.
exit force	Return to the upper layer of the command lines without displaying prompt for confirmation. Note: This command supports only in EdgeFire 1.2.

5. If you want to create a new USM user or edit an existing USM user, you can input the command lines to configure USM user settings. (e.g., user create a new USM user "**test**"). After editing the USM user settings, input "done" and "exit" to the upper layer of the command lines.

```
EdgeIPS-Pro(set configure)# edit snmp-settings
    Status:      disabled
    Port:        161
    v1/v2c Settings:
    v3 Settings:
EdgeIPS-Pro(cfg-edit snmp-settings)# edit usm-user test
```

Command Line	Description
set name <new-name>	Set the name of a USM user.
set security-level <no-auth-no-priv | auth-no-priv | auth-and-priv>	Set the security level to one of the three options. - no authentication/private key required - need authentication but no private key - need authentication and private key
set auth-key-protocol <SHA | MD5>	Set the hash format for the authentication key. - SHA - MD5
set auth-key <auth-key>	Set the value of the authentication key.
set priv-key-protocol <DES | AES>	Set the encryption method for the authentication key. - DES - AES
set priv-key <priv-key>	Set the value of the private key.
preview	List the preview settings.
done	Keep current settings (the configuration has not yet been saved).
exit	Return to the upper layer of the command lines.
done force	Keep current settings without displaying prompt for confirmation (the configuration has) . Note: This command supports only in EdgeFire 1.2.
exit force	Return to the upper layer of the command lines without displaying prompt for confirmation. Note: This command supports only in EdgeFire 1.2.

6. Once you decide to save the configuration, input "save" and press enter.

7. Input "exit" and press enter to leave the current function settings.

Configuring SNMP Trap Settings

Procedure (For EdgeIPS / EdgeIPS Pro / EdgeFire)

1. Log on to the CLI management console.
2. Input the below commands.

```
EdgeIPS-Pro$ enable
EdgeIPS-Pro# set configure
EdgeIPS-Pro (set configure)# edit snmp-trap-settings
```

3. The output displays the system information below. Now you are already in the editor mode. You can input the command lines to configure the SNMP trap settings.

Command Line	Description
edit <name>	Set the profile name of SNMP trap
delete <name>	Delete the profile of SNMP trap
preview	List the preview settings.
save	Save current settings.
exit	Return to the upper layer of the command lines.
save force	Save current settings without displaying prompt for confirmation. Note: This command supports only in EdgeFire 1.2.
exit force	Return to the upper layer of the command lines without displaying prompt for confirmation. Note: This command supports only in EdgeFire 1.2.

4. If you want to create or edit the designated SNMP trap profile, input the command lines to configure the SNMP trap profile. (e.g., users create a new SNMP trap profile, "**test**"). After editing the SNMP trap settings, input "done" and "exit" to the upper layer of the command lines.

```
EdgeIPS-Pro (cfg-edit snmp-trap-settings)# edit test
                    Name:  test                          Status: enabled
                    Description:
                    Version:       v1
                    Address:       10.10.10.10           Port: 162
                    Community:     security
                    Type: trap                           Retries: -
                    High CPU usage:                      disabled
                    High memory usage:                   disabled
                    Log storage is low:                  disabled
                    Interface IP address changed:        disabled
                    Network interface link up:           disabled
                    Network interface link down:         disabled
                    HA heartbeat failed:                 disabled
EdgeIPS-Pro (cfg-edit snmp-trap-settings)#
```

Command Line	Description
set name <new-name>	Set the profile name of the SNMP trap.
set enabled <true | false>	Enable or disable the SNMP trap profile.

set description <description>	Set the description of the SNMP trap profile.
set address <address>	Set the server IP address.
set port <port-number>	Set the server port.
set community <community>	Set the trap communty name.
set version v1	Set the SNMP version to SNMPv1
set version v2c <trap>|<inform> <retry-times>	Set the SNMP version to SNMPv2c, the message type and the retry times: - Trap - InformRequest
set event-notification enabled [<all | cpu-usage-high | memory-usage-high | disk-usage-high | ip-address-changed | link-up | link-down | ha-heartbeat-failed>]	Set the event notification to enable the below message(s). - All of the messages - High CPU Usage - High Memory Usage - Log Storage is Low - Interface IP Address Changed - Network Interface Link Up - Network Interface Link Down - High Availability heartbeat is failed (Only EdgeIPS Pro supports this message option.)
set event-notification disabled [<all | cpu-usage-high | memory-usage-high | disk-usage-high | ip-address-changed | link-up | link-down | ha-heartbeat-failed>]	Set the event notification to disable the below message(s). - All of the messages - High CPU Usage - High Memory Usage - Log Storage is Low - Interface IP Address Changed - Network Interface Link Up - Network Interface Link Down - High Availability heartbeat is failed (Only EdgeIPS Pro supports this message option)
preview	List the preview settings.
done	Keep current settings (the configuration has not yet been saved).
exit	Return to the upper layer of the command lines.
done force	Keep current settings without displaying prompt for confirmation (the configuration has) . Note: This command supports only in EdgeFire 1.2.
exit force	Return to the upper layer of the command lines without displaying prompt for confirmation. Note: This command supports only in EdgeFire 1.2.

5. Once you decide to save the configuration, input “save” and press enter.
6. Input “exit” and press enter to leave the current function settings.

Viewing NTP Settings

Procedure (For EdgeIPS / EdgeIPS Pro / EdgeFire)

1. Log on to the CLI management console.
2. Input the below commands.

```
EdgeIPS-Pro$ enable
EdgeIPS-Pro# show ntp-server
```

3. The output displays the access control list below.

```
EdgeIPS-Pro# show ntp-server
                Name:    10.24.7.45                    Status: enabled
EdgeIPS-Pro#
```

Configuring NTP Settings

Procedure (For EdgeIPS / EdgeIPS Pro / EdgeFire)

1. Log on to the CLI management console.
2. Input the below commands.

```
EdgeIPS-Pro$ enable
EdgeIPS-Pro# set configure
EdgeIPS-Pro(set configure)# edit ntp-server
```

3. The output displays the system information below. Now you are already in the editor mode. You can input the command lines to configure the ODC sync settings.

```
EdgeIPS(set configure)# edit ntp-server

        Name:   10.24.7.45              Status: enabled

EdgeIPS(cfg-edit ntp-server)#
```

Command Line	Description
set enabled <true | false>	Enable or disable the NTP server settings. Note: when the device is connected to ODC server, the NTP setting is not configurable.
set address <ip-address | domain-name>	Edit the IP address or domain name of NTP server.
preview	List the preview settings.
save	Save current settings.
exit	Return to the upper layer of the command lines.
save force	Save current settings without displaying prompt for confirmation. Note: This command supports only in EdgeFire 1.2.
exit force	Return to the upper layer of the command lines without displaying prompt for confirmation. Note: This command supports only in EdgeFire 1.2.

4. Once you decide to save the configuration, input "save" and press enter.
5. Input "exit" and press enter to leave the current function settings.

Note: ODC system synchronizes the system time with its managed instances.

Viewing Time Zone Settings

Procedure (For EdgeIPS / EdgeIPS Pro / EdgeFire)

1. Log on to the CLI management console.
2. Input the below commands.

```
EdgeIPS-Pro$ enable
EdgeIPS-Pro# show timezone
```

3. The output displays the access control list below.

```
EdgeIPS-Pro# show timezone
name: (GMT+08:00) Asia/Taipei   timeZoneID: Asia/Taipei
        offset: 28800

EdgeIPS-Pro#
```

Configuring Time Zone Settings

Procedure (For EdgeIPS / EdgeIPS Pro / EdgeFire)

1. Log on to the CLI management console.
2. Input the below commands.

```
EdgeIPS-Pro$ enable
EdgeIPS-Pro# set configure
EdgeIPS-Pro(set configure)# edit timezone
```

3. The output displays the system information below. Now you are already in the editor mode. You can input the command lines to configure the ODC sync settings.

```
EdgeIPS(set configure)# edit timezone

name: (GMT+08:00) Asia/Taipei   timeZoneID: Asia/Taipei
      offset: 28800

EdgeIPS(cfg-edit ntp-server)#
```

Command Line	Description
set zone <zone-id>	Set the time zone.
preview	List the preview settings.
save	Save current settings.
exit	Return to the upper layer of the command lines.
save force	Save current settings without displaying prompt for confirmation. Note: This command supports only in EdgeFire 1.2.
exit force	Return to the upper layer of the command lines without displaying prompt for confirmation. Note: This command supports only in EdgeFire 1.2.

4. Once you decide to save the configuration, input "save" and press enter.

5. Input "exit" and press enter to leave the current function settings.

Configuring System Time Settings

Procedure (For EdgeIPS / EdgeIPS Pro / EdgeFire)

1. Log on to the CLI management console.
2. Input the below commands.

```
EdgeIPS-Pro$ enable
```

3. You can input the command line to configure ~~the~~ ODC sync settings.

Command Line	Description
set system time <YYYY-MM-DDTHH:mm:ssZ>	Set the system time in UTC format. • YYYY - year • MM - month number (2-digit) • DD - day of month (2-digit) • HH - hours (2-digit, 24-hour format) • mm - minutes (2-digit) • ss - seconds (2-digit) • Z - UTC offset (1-digit) For example, set the system time to 2021-10-17T12:19:438 and the system time will display in the format of "2021-10-17T12:19:43+08:00".

4. Input "exit" and press enter to leave the current function settings.

Syncing NTP Time Settings

Procedure (For EdgeIPS / EdgeIPS Pro / EdgeFire)

1. Log on to the CLI management console.
2. Input the below commands.

```
EdgeIPS-Pro$ enable
```

3. You can input the command line to configure the ODC sync settings.

Command Line	Description
sync ntp-server	Sync up with the NTP server.

4. Input "exit" and press enter to leave the current function settings.

System Reboot

Procedure (For EdgeIPS / EdgeIPS Pro / EdgeFire)

1. Log on to the CLI management console.
2. Input the below commands.

```
EdgeIPS-Pro$ enable
```

3. You can input the command line to configure the ODC sync settings.

Command Line	Description
reboot	Reboot the device

4. After input "reboot" and press enter. The system will display the prompt for confirmation.

```
EdgeIPS-Pro$ reboot
Are you sure you want to reboot?: yes/no
```

5. Input "yes" and press enter. The device will reboot automatically.

System Power Off

Procedure (For EdgeIPS / EdgeIPS Pro / EdgeFire)

1. Log on to the CLI management console.
2. Input the below commands.

```
EdgeIPS-Pro$ enable
```

3. You can input the command line to configure the ODC sync settings.

Command Line	Description
power off	Power off the device

4. After input "power off" and press enter. The system will display the prompt for confirmation.

```
EdgeIPS-Pro$ power off
Are you sure you want to poweroff device?: yes/no
```

5. Input "yes" and press enter. The device will be powered off automatically.

Note: Once the device is powered off, hardware bypass will start to operate. To power on the device, user needs to unplug and plug in the terminal block or the power adapter again.

Viewing Device Firmware Information

Procedure (For EdgeIPS / EdgeIPS Pro / EdgeFire)

1. Log on to the CLI management console.
2. Input the below commands.

```
EdgeIPS-Pro$ enable
```

3. You can input the command line to view the firmware partition settings.

Command Line	Description
show partition	Display the partition firmware information.

4. After inputting "show partition" and pressing enter, the system will display the firmware partition information.

```
EdgeIPS-Pro$ show partition

                partition name: boot1   status: running
                firmware version: IPSP_T01_1.2.10
                firmware build time: 2021-09-10T18:02:47+08:00

                partition name: boot2   status: standby
                firmware version: IPSP_T01_1.1.15
                firmware build time: 2021-04-06T11:00:40+08:00

EdgeIPS-Pro$
```

Note: Edge series can have up to two versions of firmware installed. Each firmware is installed in its own individual partition. At any given point of time, one partition is in the [Running] status that indicates the currently running and active firmware. The other partition will be in the [Standby] status that indicates an alternative or standby firmware.

Switching Firmware Partition

To switch firmware partition from the [Standby] partition to the [Running] partition, a user may need to boot the [Standby] partition and load the firmware from there.

Procedure (For EdgeIPS / EdgeIPS Pro / EdgeFire)

1. Log on to the CLI management console.
2. Input the below commands.

```
EdgeIPS-Pro$ enable
```

3. You can input the command line to view the firmware partition settings.

Command Line	Description
switch partition	Display the partition firmware information.

4. After inputting "show partition" and pressing enter, the system will display the firmware partition information.

```
EdgeIPS-Pro$ switch partition
This operation will switch to standby partition after reboot! Are you sure you
want to switch partition?: yes/no exit
```

5. Input "yes" and press enter. The device will reboot the [standby] partition automatically.