# ArcTiv™ Network Optimizer

Operation Manual

**Table of Contents**

## Chapter 1 Introduction

This document introduces the security features and system structure of the ArcTiv Network Optimizer (to be referenced as 'Optimizer' in this document) and the details about the Graphic User Interface (GUI) that is used for operating and controlling the network appliance. The Optimizer is an in-line network security appliance which utilizes a 100% hardware-based solution for adaptive traffic bandwidth management, network attack mitigation and network access control - all without packet forwarding delays. Typical applications include:

- Adaptive traffic bandwidth controls
- DDoS attack detection and mitigation
- Full layer network visibility for continuous traffic monitoring
- User-defined pattern matching

### System Structure

The Optimizer is an in-line network security appliance that provides functions for network attack mitigation, network access control, and adaptive traffic bandwidth management. Depending on the security policy configurations, the appliance performs adaptive operation on network traffic providing real-time visibility on both network layer and application layers.

The Optimizer also maintains system-level security by checking user authentication, system integrity, system record audit, and real-time traffic monitoring. Purpose-built proprietary network security boards with 10 Gbps interfaces are used to keep the wire-speed performance for all network security features applied to live traffic. This security board utilizes both FPGA and DRAM memory to realize the functions that are categorized into multiple subsystems. The physical boundaries of the system elements are between the security board and system motherboard where the system Operating System and software runs – as shown below.

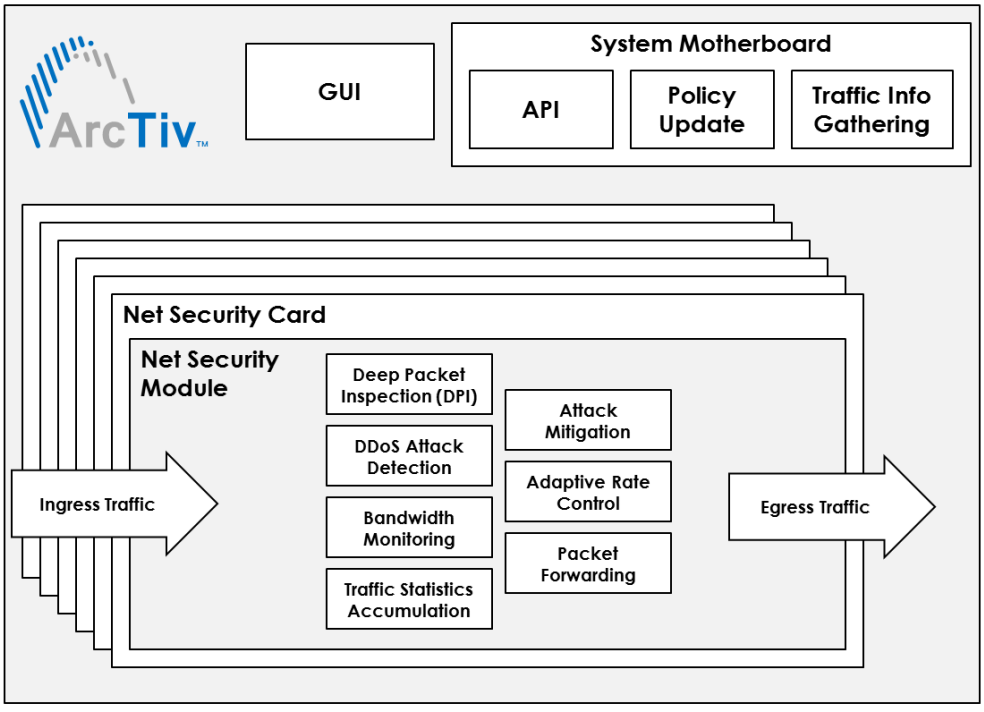



**Figure 1. Optimizer Physical boundaries**

**Subsystems**

The Optimizer provides network security features to protect data transmitted over the network in both directions. Functional elements of the appliance are composed of the following subsystems:

- Receive Module
- Packet Filtering
- DDoS Mitigation
- IPS
- Transmit Module
- Engine Control
- Security Management
- User Authentication
- Common Module
- Virtual Group
- Application

**Notes:**

- Each attack mitigation option can be activated individually.
- Multiple attack mitigation options can be activated and run simultaneously for attack detections from incoming and outgoing packets.
- User authentication, security management and application subsystems are software-based and run on the CPU via the motherboard.
- Other subsystems are performed using the FPGA and connected DRAM memory and run on the security board.
- Security related features, traffic statistics raw information gathering, and bandwidth control features run in the FPGA, where the CPU is not involved in attack mitigation functions.

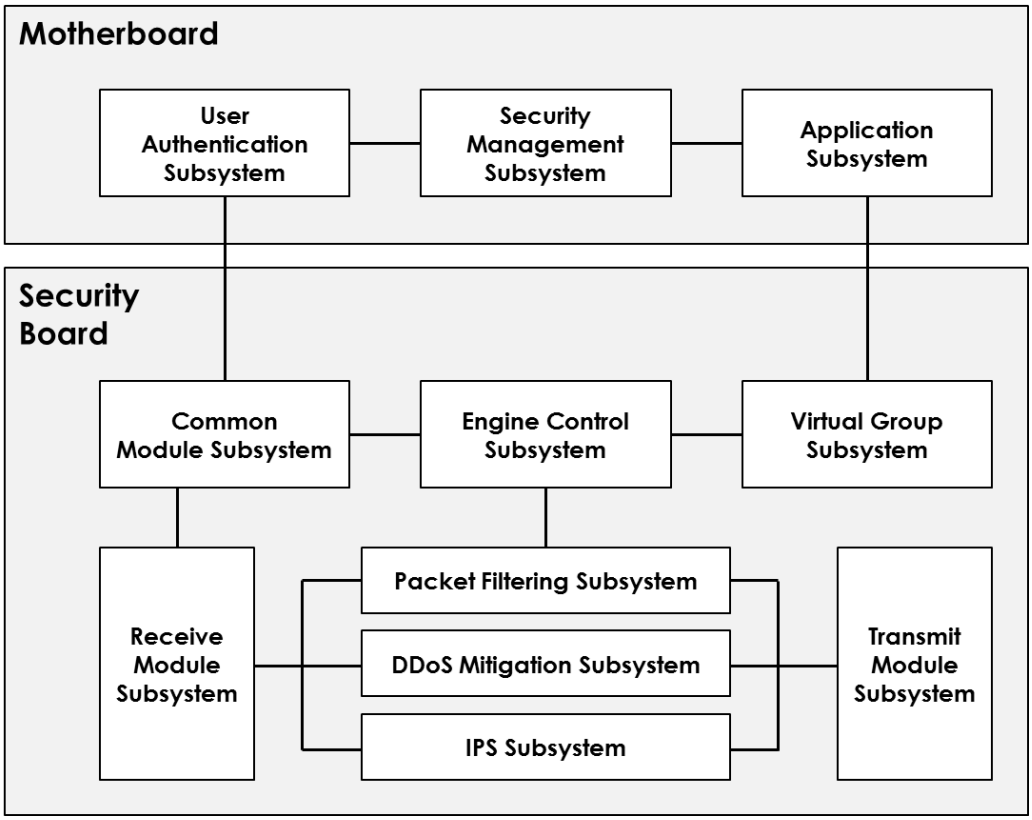



**Figure 2. Subsystems of Optimizer**

**Subsystem Functions**

The main functions of each subsystem are realized by using dedicated functional modules. Key functions of each subsystem are identified in Table 1.

**Table 1. Subsystem Functions**

| Subsystem | Functions |
|---|---|
| Receive Module | - Temporary packet storage before packet filtering<br>- Packet header parsing |
| Packet Filtering | - Full layer packet header information parallel processing<br>- Packet identification number assignment for per packet level mitigation purpose<br>- Potential attack packet check for all attack types and virtual group IP addresses<br>- IP address and port number based access control<br>- White List check<br>- Black List check |
| DDoS Mitigation | - DDoS attack detection and prevention<br>- Flood attack detection and prevention<br>- Application layer attack detection and prevention<br>- Volumetric attack detection and prevention |
| IPS | - Deep Packet Inspection<br>  - User configurable detection rules<br>  ▪ Direction<br>  ▪ IP version<br>  ▪ IP flags<br>  ▪ Protocol<br>  ▪ Source IP address<br>  ▪ Destination IP address<br>  ▪ TCP flags<br>  ▪ Configurable pattern 1<br>  ▪ Configurable pattern 2<br>  ▪ Configurable pattern 3<br>- Detected packet capturing |
| Transmit Module | - Attack detection result compilation<br>  - Log<br>  - Rate limit<br>  - Block the packets for a configured duration<br>- Transmission buffer control<br>- Packet capture |
| Engine Control | - Controlling the subsystems<br>  - Receive Module Subsystem<br>  - Packet Filtering Subsystem<br>  - DDoS Mitigation Subsystem<br>  - Transmit Module Subsystem<br>- Traffic statistics selection<br>- Detection parameter updates<br>  - Detection count<br>  - Detection duration in seconds<br>  - Detection policy application duration |
| Security Management | - System operation<br>- Policy update<br>- GUI operation<br>- Detection parameter configuration per each attack definition<br>- Traffic statistics information processing |

| | | |
|---|---|---|
| User Authentication | - | User authentication<br>Command Line Interface(CLI)<br>Graphic User Interface(GUI) |
| Common Module | - | Packet buffering for packet parsing and packet transmit<br>Packet header and payload parsing |
| Virtual Group | - | Attack mitigation based on protected server IP address group<br>Traffic statistics gathering per server IP address group |
| Application | - | Security data processing<br>API control<br>Data interface with security board<br>Security configuration to security board<br>Network traffic statistics from security board<br>Attack mitigation results from security board<br>System management<br>System control<br>System interface for control network devices |

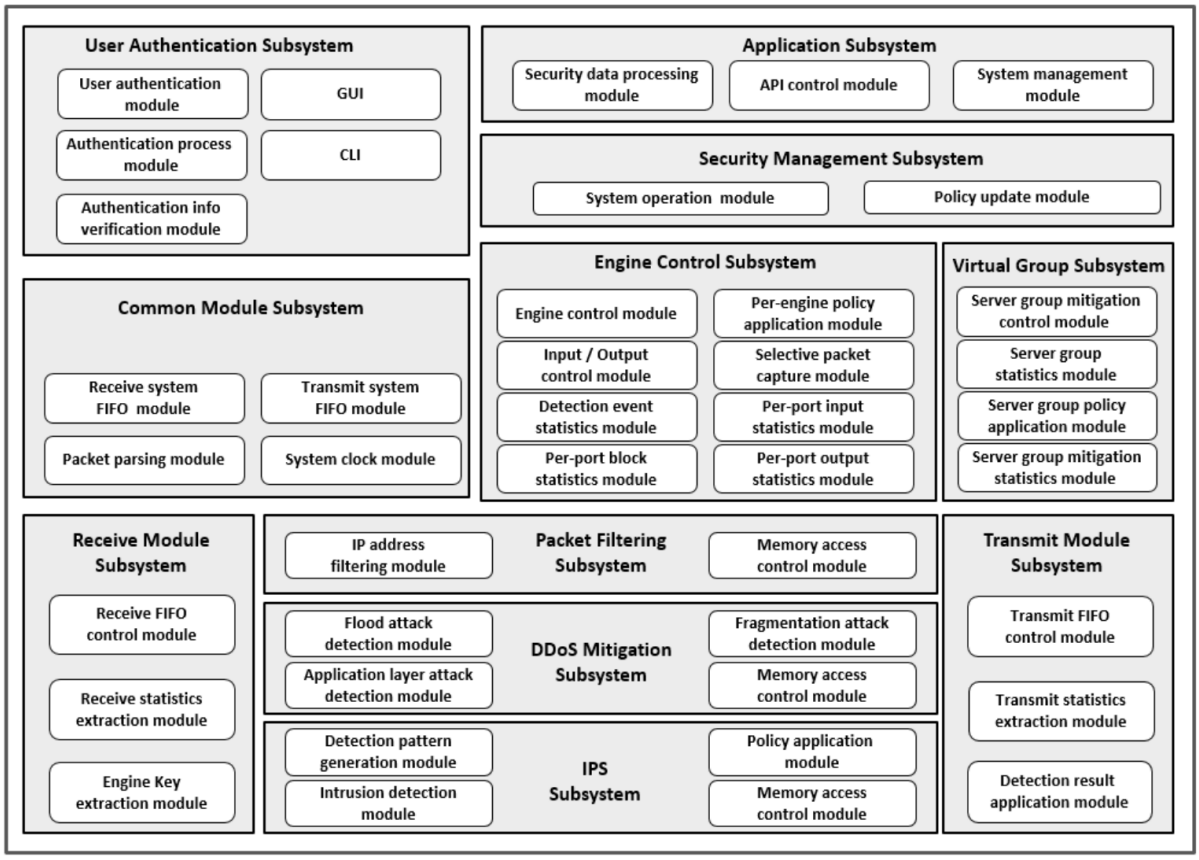



**Figure 3. Subsystem Interfaces and Modules**

## Chapter 2. NETWORK CONFIGURATION AND FEATURES

### Network Application

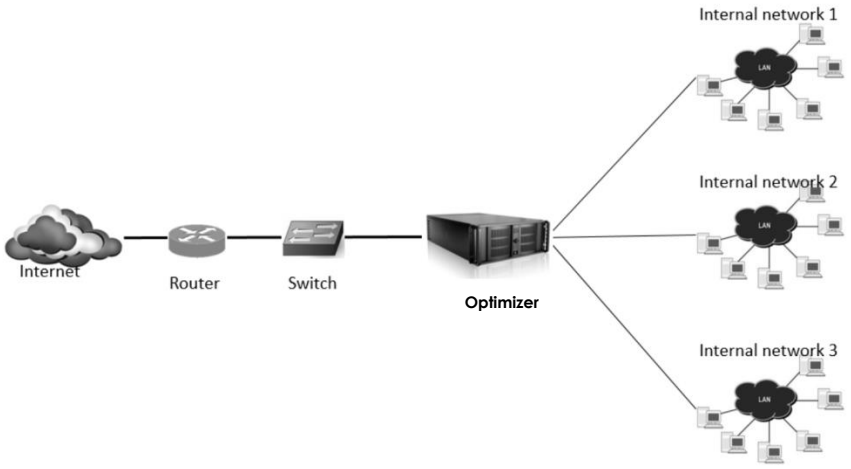



**Figure 4. Optimizer In-Line Network Application**

### Major Features

The main features of the Optimizer are summarized as follows:

- A pure hardware solution for monitoring and mitigation of network security threats by providing DDoS attack mitigation, full layer network visibility and user-configurable pattern matching
- Full wire-speed performance before, during and after attacks at a network, protocol and application layer.
- Field-programmable to monitor, detect and process network threat information.
- Network traffic monitoring, analysis and intelligent bandwidth management without packet forwarding delays. Its innovative deep packet inspection (DPI) technology provides flow visibility for Layer 7 applications, resulting in industry-leading traffic handling speed.
- L3 and L4, L7 Flooding, fragmentation, application-layer attack detection, blocking, functions are implemented on each Security board that is applied on the motherboard PCI express slots. Board level scalability is provided by the appliance.
- Real-time network traffic monitoring via GUI dashboard. Specific traffic statistics monitoring such as for TCP flag and protocol types are also provided.
- Generates audit record of the actions related to the security of the system through the security audit function. Generates a warning message when the limit of storage space to store audit records is exceeded while also providing logical search and query filtering using the GUI.
- Performs identification and authentication of the administrator through the encrypted identification and authentication process. Operated by the administrator who is identified and authenticated successfully by the system.
- Ensures DDoS attack detection and prevention feature run at wire-speed against flooding attacks and application layer attacks with no system latency for normal packets.
- Provides server IP address specific attack mitigations features.

## Chapter 3. SYSTEM TEST ENVIRONMENT

A simple test environment to measure the Optimizer performance of can be configured using the following devices.

- 10 GbE Testing Equipment Chassis
- 10 GbE LAN service modules with SFP+ interface: 2 modules
- PC or Laptop with10 GbE testing equipment control S/W
- Optimizer test unit
- Monitor for GUI

Using the 10 GbE testing equipment, test packets can be generated with the combination of normal and attack traffic.

The Optimizer can be configured with the traffic monitoring and mitigation parameters via the web-based GUI interface either locally or remotely. The status of device and the information gathered from monitoring and attack mitigation is stored and shown on GUI in real-time as described in the following sections.

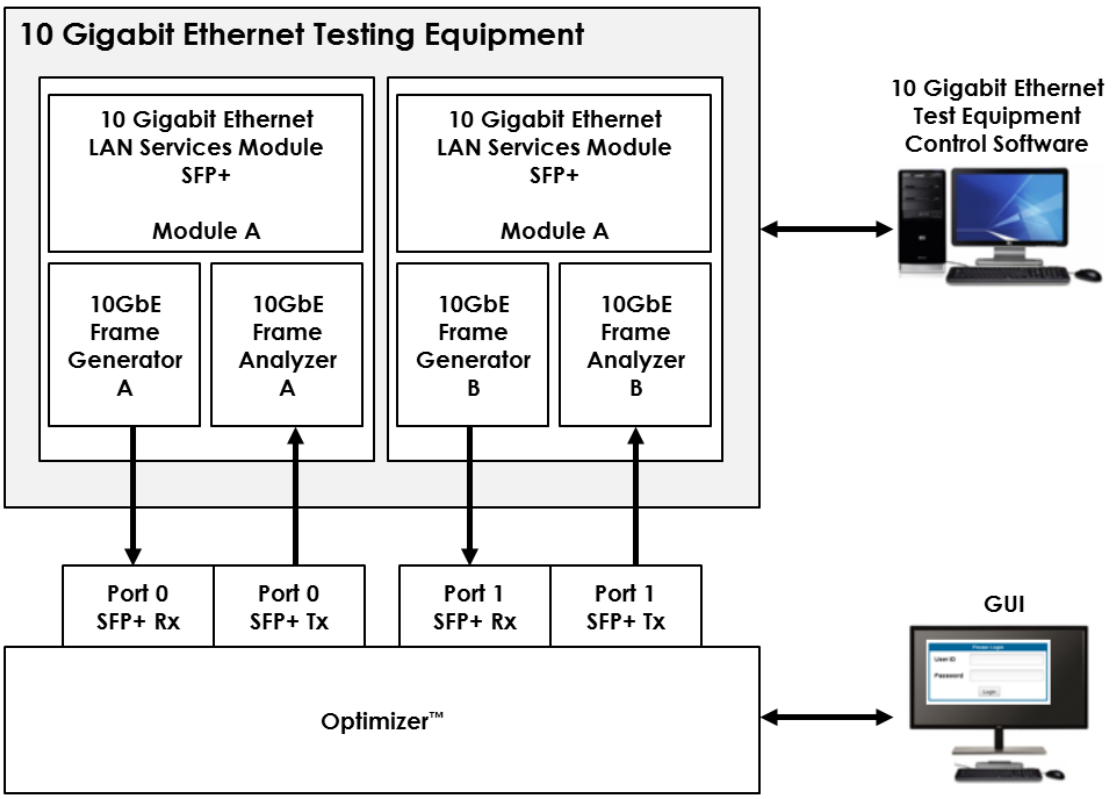



**Figure 5. Simplified Test Environment for the Optimizer**

## CHAPTER 4. GUI USER GUIDE

The basic operations of the GUI are described in this chapter.

### Login & Logout

After typing in the URL of the system (or https://localhost when accessed locally), you are landing on the login page.

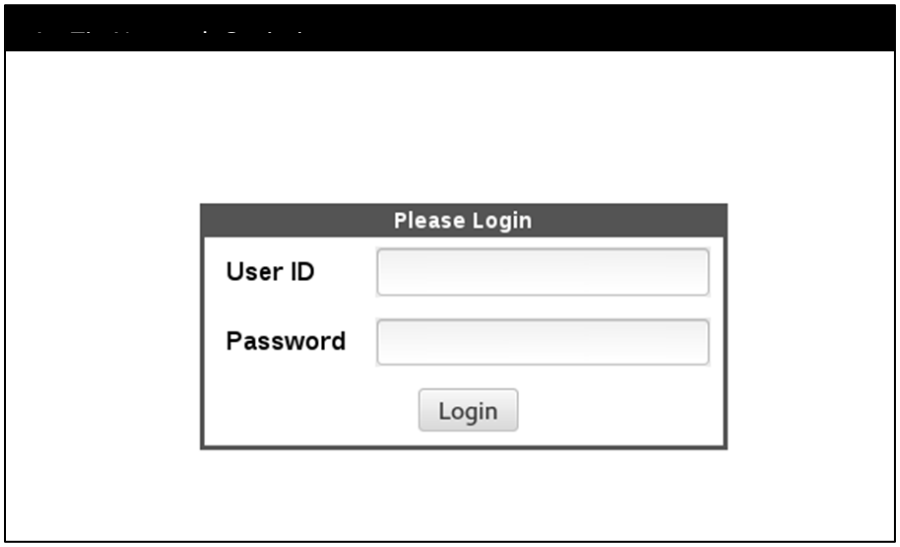



**Figure 6. Optimizer Login Page**

By entering the user ID and password, and clicking Login button, you are brought to Dashboard Operation page. Please note while the system allows two administrator user ID's, only one user at a time can login to the system.

To log out of the system, click Logout button at the right bottom of the window.

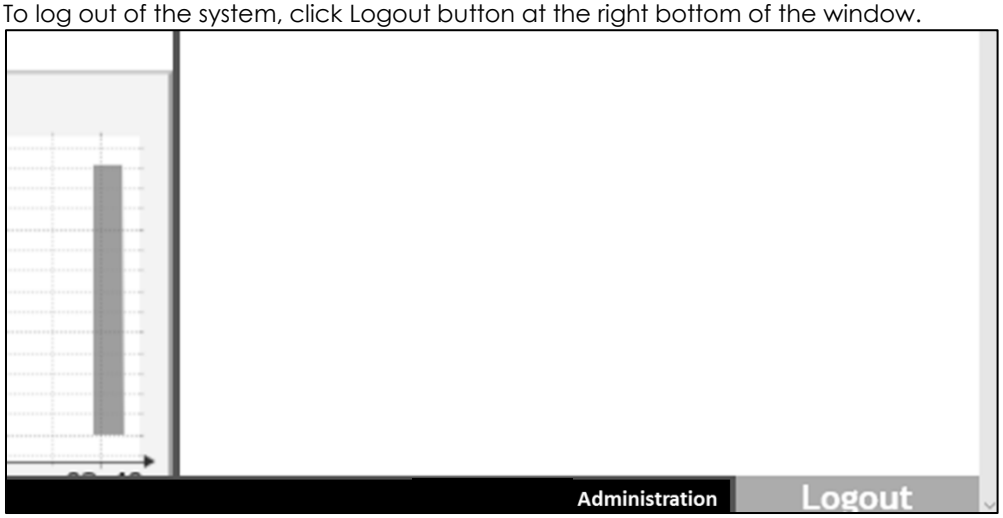



**Figure 7. Logout Button**

In order to prevent unauthorized access, the user will be logged out if inactive for more than 5 minutes.

### Top Tabs

The top tabs panel provides quick access to different functions of the system.


**Figure 8. Top Tabs**

**Table 2. Top Tabs Description**

| Item | Description |
|---|---|
| Dashboard Operation | Presents summarized system information which enables administrators to routinely check system status at a glance. |
| Operation Statistics | Presents various operation statistics in detail |
| ACL Operation | Provides configuration interfaces for white list and black list |
| Attack Mitigation | Provides interface to configure attack mitigation rules for layer 3, layer 4, layer 7. |
| Port Status | Shows the port status report and provides the interface to manually assess the port status. |
| Administration | Provides access to system administration related configurations, information, and utilities. |

## CHAPTER 5. DASHBOARD OPERATION

The Dashboard Operation tab provides summarized system information which enables administrators to routinely check system status at a glance.

### Dashboard Operation

Dashboard operation window provides the control of data update rate of this tab.


**Figure 9. Dashboard Operation Window**

**Table 3. Dashboard Operation Description**

| Item | Description |
|---|---|
| Refresh Dashboard automatically | Check the checkbox to enable periodical automatic refresh. The refresh rate, can be set to 1, 2, 4, 6, 8, or 10 seconds, and is selectable from the drop-down menu. Automatic refresh every 1 second is enabled by default. |
| Refresh Dashboard | Enabled when the checkbox is unchecked. The user can manually refresh the data in this tab by clicking this button. |
| Attack Detected. Please investigate immediately! | The blinking warning message appears to prompt human intervention only when attack is detected. |

### Attack Status

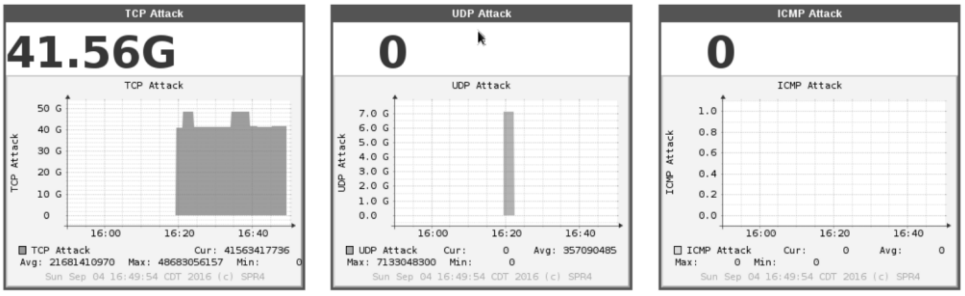


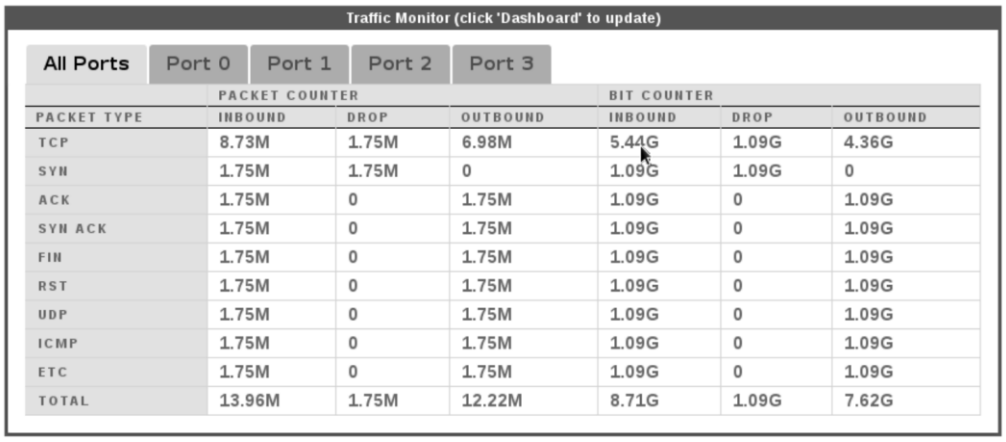

**Figure 10. Attack Status Windows**

**Table 4. Attack Status Description**

| Item | Description |
|---|---|
| TCP Attack | Visualizes the total volume of TCP attack in the last 60 minutes. |
| UDP Attack | Visualizes the total volume of UDP attack in the last 60 minutes. |
| ICMP Attack | Visualizes the total volume of ICMP attack in the last 60 minutes. |

### Traffic Monitor

This window comprises of the packet and bit count of each type.




| | PACKET COUNTER | | | BIT COUNTER | | |
|---|---|---|---|---|---|---|
| PACKET TYPE | INBOUND | DROP | OUTBOUND | INBOUND | DROP | OUTBOUND |
| TCP | 8.73M | 1.75M | 6.98M | 5.44G | 1.09G | 4.36G |
| SYN | 1.75M | 1.75M | 0 | 1.09G | 1.09G | 0 |
| ACK | 1.75M | 0 | 1.75M | 1.09G | 0 | 1.09G |
| SYN ACK | 1.75M | 0 | 1.75M | 1.09G | 0 | 1.09G |
| FIN | 1.75M | 0 | 1.75M | 1.09G | 0 | 1.09G |
| RST | 1.75M | 0 | 1.75M | 1.09G | 0 | 1.09G |
| UDP | 1.75M | 0 | 1.75M | 1.09G | 0 | 1.09G |
| ICMP | 1.75M | 0 | 1.75M | 1.09G | 0 | 1.09G |
| ETC | 1.75M | 0 | 1.75M | 1.09G | 0 | 1.09G |
| TOTAL | 13.96M | 1.75M | 12.22M | 8.71G | 1.09G | 7.62G |

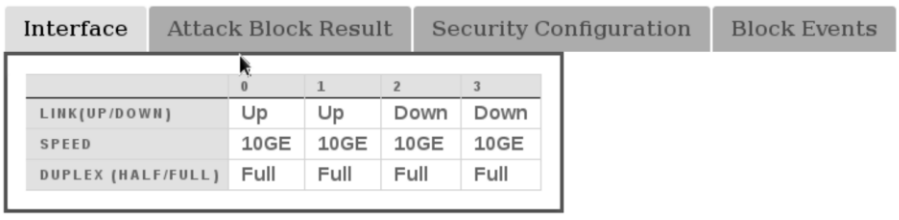
**Figure 11. Traffic Monitor Window**

**Table 5. Traffic Monitor Description**

| Item | Description |
|---|---|
| All Ports (Tab) | Combines the packet and bit count statistics of all ports |
| Port 0 (Tab) | Shows traffic statics in Port 0. |
| Port 1(Tab) | Shows traffic statics in Port 1. |
| Port 2 (Tab) | Shows traffic statics in Port 2. |
| Port 3 (Tab) | Shows traffic statics in Port 3. |
| Packet Counter | Traffic statistics in terms of packet count. |
| Bit Counter | Traffic statistics in terms of number of bits. |
| Packet Type | Classifies packets into TCP, SYN, ACK, SYN ACK, RST, UDP, ICMP and ETC. Total counts are listed in the last row. |
| Inbound | Statistics of inbound traffic. |
| Drop | Statistics of packets dropped by the system. |
| Outbound | Statistics of outbound traffic. |

### Interface

This tab of the window displays the current status of each port.




| | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| LINK(UP/DOWN) | Up | Up | Down | Down |
| SPEED | 10GE | 10GE | 10GE | 10GE |
| DUPLEX (HALF/FULL) | Full | Full | Full | Full |

**Figure 12. Interface Tab**

**Table 6. Interface Description**

| Item | Description |
|---|---|
| Link | This row shows whether the link of each port is Up (with active connection) or Down (inactive). |
| Speed | This row indicates the link speed of each port. |
| Duplex (Half/Full) | This row indicates the duplex mode, Full (full-duplex) or Half (half-duplex) of each port. |

### Attack Block Result

This tab shows the result of attacks have been blocked by the system in tabulated format.


**Figure 13. Attack Block Result Tab**

**Table 7. Attack Block Result Description**

| Item | Description |
|---|---|
| Show Entries | Select how many entries in the list are displayed per page. |
| Search | Filter the list below by entering search keyword. |
| Date and Time | The date and time when the attack occurred. |
| IP Protocol | The IP protocol involved in the attack. |
| Source IP Address | The source IP address involved in the attack. |
| Source Port Number | The source port number involved in the attack. |
| Destination IP Address | The destination IP address involved in the attack. |
| Destination Port Number | The destination port number involved in the attack. |
| Type of Attack | The type of attack identified by the system. |
| Detected Attack Count | The number of attacks got detected. |
| Mitigated Attack Count | The number of attacks got mitigated. |
| Showing Entries | Indicates how many entries out of the total number of entries are displayed in the current view. |
| First | Click to jump to the first page. |
| Previous | Click to jump to the previous page. |
| Next | Click to jump to the next page. |
| Last | Click to jump to the last page. |

### Security Configuration

This tab provides a summarized list of the current security configurations.

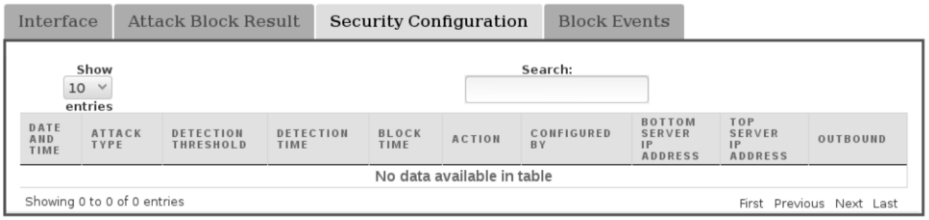



**Figure 14. Security Configuration Tab**

**Table 8. Security Configuration Description**

| Item | Description |
|---|---|
| Show Entries | Select how many entries in the list are displayed per page. |
| Search | Enter the search keyword to filter the keyword in the list below. |
| Date and Time | The date and time when the security configuration is registered. |
| Attack Type | The type of attack the system identifies. |
| Detection Threshold | The min number of packets matching the security configuration entry within the detection time to trigger the system to take action. |
| Detection Time | The duration the system should accumulate the occurrence count of packets matching the security configuration entry to trigger the system to take action. |
| Block Time | The duration the system should block the packets matching the security configuration entry. |
| Mitigation Action | The action the system should take after detection. |
| Configured By | The user ID who set up this security configuration entry. |
| Bottom Server IP Address | The lowest server IP address involved in this security configuration entry. |
| Top Server IP Address | The highest server IP address involved in this security configuration entry. |
| Outbound | Whether the packet is outbound or not. |
| Showing Entries | Indicates how many entries out of the total number of entries are displayed in the current view. |
| First | Click to jump to the first page. |
| Previous | Click to jump to the previous page. |
| Next | Click to jump to the next page. |
| Last | Click to jump to the last page. |

**Block Events**

This tab presents the summarized block event list of each port.

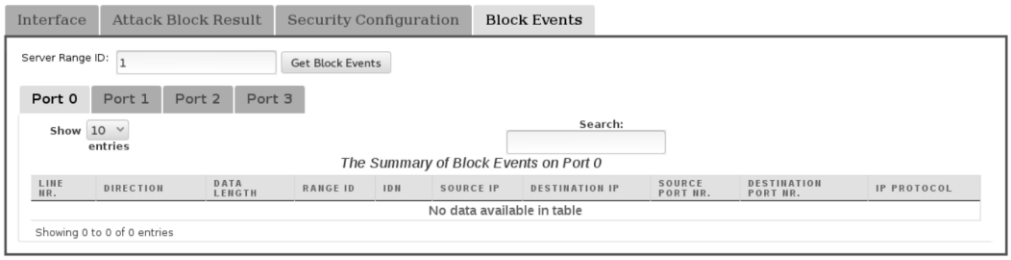



**Figure 15. Block Events Tab.**

**Table 9. Block Events Description**

| Item | Description |
|---|---|
| Server Range ID | The number identifies the server range. |
| Get Block Events | By clicking this button, the block event list relevant to the entered server range ID is displayed below. |
| Port 0 | Tab shows the list of block events occurring at port 0. |
| Port 1 | Tab shows the list of block events occurring at port 1. |
| Port 2 | Tab shows the list of block events occurring at port 2. |
| Port 3 | Tab shows the list of block events occurring at port 3. |
| Show Entries | Select how many entries in the list are displayed per page. |
| Search | By entering search keyword in this text box, the list below is filtered by the keyword. |
| Line Number | The number identifies the entry of the block event. |
| Direction | The direction of the blocker packet. |
| Data Length | The data length of the blocked packet. |
| Range ID | The number identifies a predefined server IP address range. |
| IDN | The number identifies the attack type which was blocked. |
| Source IP Address | The source IP address of the blocked packet. |
| Destination IP Address | The destination IP address of the blocked packet. |
| Source Port Number | The source port number of the blocked packet. |
| Destination Port Number | The destination port number of the blocked packet. |

**Detection Result**

This window shows the summary of packet and bit counter of detection result per IDN number.

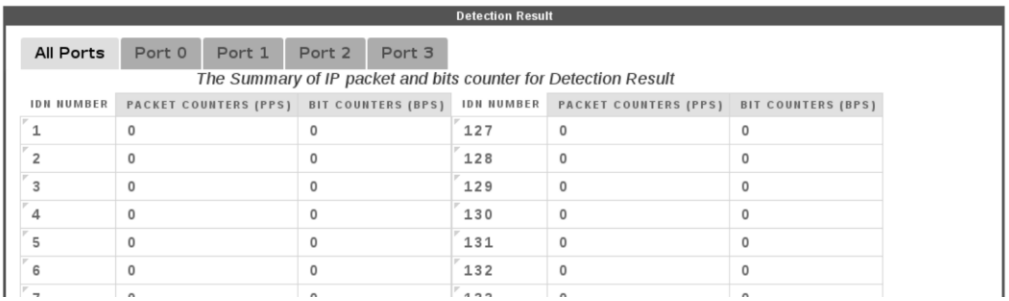



**Figure 16. Detection Result Window**

**Table 10. Detection Result Description**

| Item | Description |
|---|---|
| All Ports | Tab shows the detection results of all port combined. |
| Port 0 | Tab shows the detection results occurring at Port 0. |
| Port 1 | Tab shows the detection results occurring at Port 1. |
| Port 2 | Tab shows the detection results occurring at Port 2. |
| Port 3 | Tab shows the detection results occurring at Port 3. |
| IDN Number | The number identifies the attack type which was detected. |
| Packet Counters | The total number of blocked packets of the IDN number. |
| Bit Counters | The total volume (in bits) of blocked packets of the IDN number. |

## CHAPTER 6. OPERATION STATISTICS

In this tab, system administrators can review varies operation statistics in detail.

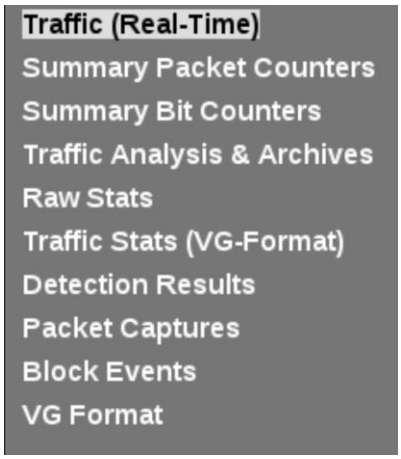



**Figure 17. Left Panel Sub-Tabs in Operation Statistics Tab**

### Traffic (Real-Time)


**Figure 18. Overall Traffic Statistics Window**

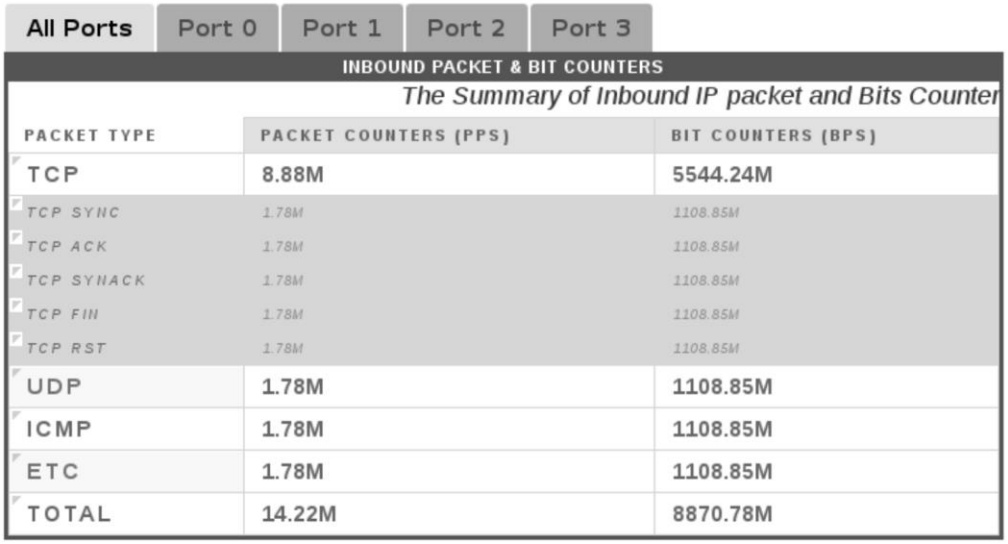
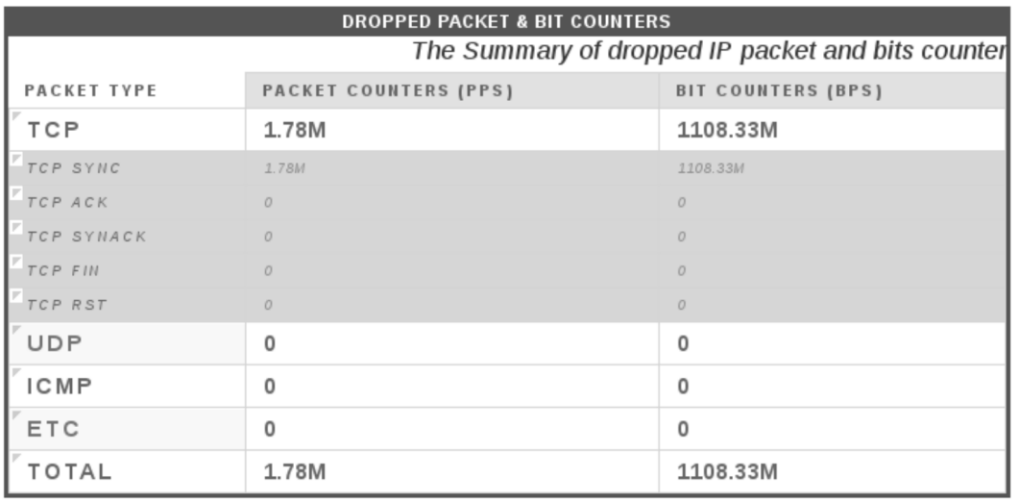



**Figure 19. Inbound Packet & Bit Counters Table with Port Selection Tabs**

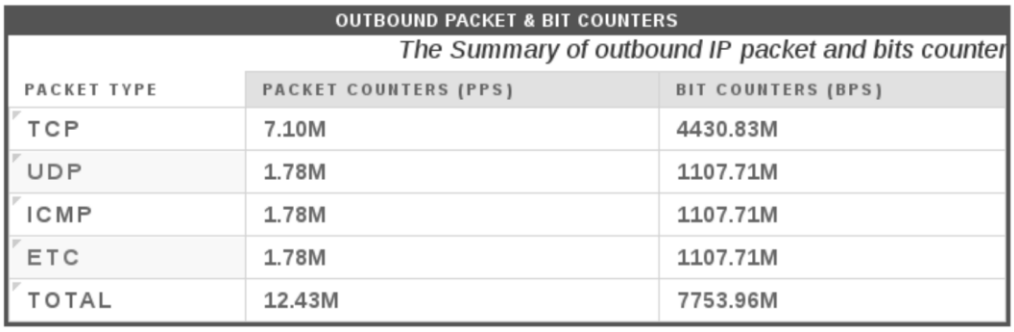


DROPPED PACKET & BIT COUNTERS

*The Summary of dropped IP packet and bits counter*

| PACKET TYPE | PACKET COUNTERS (PPS) | BIT COUNTERS (BPS) |
|---|---|---|
| TCP | 1.78M | 1108.33M |
| TCP SYNC | 1.78M | 1108.33M |
| TCP ACK | 0 | 0 |
| TCP SYNACK | 0 | 0 |
| TCP FIN | 0 | 0 |
| TCP RST | 0 | 0 |
| UDP | 0 | 0 |
| ICMP | 0 | 0 |
| ETC | 0 | 0 |
| TOTAL | 1.78M | 1108.33M |

**Figure 20. Dropped Packet & Bit Counters Table**



OUTBOUND PACKET & BIT COUNTERS

*The Summary of outbound IP packet and bits counter*

| PACKET TYPE | PACKET COUNTERS (PPS) | BIT COUNTERS (BPS) |
|---|---|---|
| TCP | 7.10M | 4430.83M |
| UDP | 1.78M | 1107.71M |
| ICMP | 1.78M | 1107.71M |
| ETC | 1.78M | 1107.71M |
| TOTAL | 12.43M | 7753.96M |

**Figure 21. Outbound Packet & Bit Counters Table**

**Table 11 Traffic (Real-Time) description**

| Item | Description |
|---|---|
| Stop Collecting Data | Stops continuous traffic data collection. This button is available only when the traffic data is actively collected and displayed. Traffic data collection is automatically started when loaded. |
| Resume Collecting Data | Click to resume continuous traffic data collection. This button is available only when traffic data collection is stopped. |
| Data Collection Started at | The date and time the current traffic data collection session began. |
| All Ports | Shows real-time traffic statistics of all ports combine. |
| Port 0 | Shows real-time traffic statistics of Port 0 |
| Port 1 | Shows real-time traffic statistics of Port 1 |
| Port 2 | Shows real-time traffic statistics of Port 2 |
| Port 3 | Shows real-time traffic statistics of Port 3 |
| Inbound Packet and Bit Counters | This window shows the inbound traffic statistics of all types of packets in terms of packets per second (pps) and bits per second (bps). |

| | |
|---|---|
| Dropped Packet and Bit Counters | This window shows the dropped traffic statistics of all types of packets in terms of pps and bps. |
| Outbound Packet and Bit Counters | This window shows the outbound traffic statistics of all types of packets in terms of pps and bits per second bps. |

**Summary Packet Counters**

This tab shows diagrams which show how traffic statistics of all protocols and types change over time in terms of packet count.

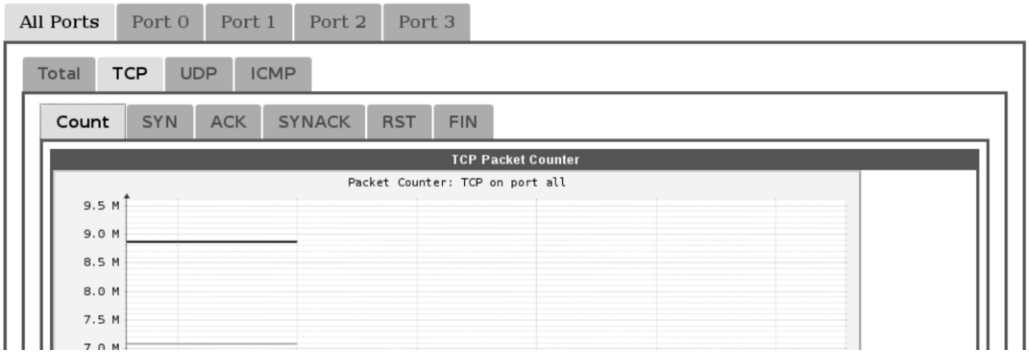



**Figure 22. Summary Packet Counter Window**

**Table 12. Summary Packet Counter Description**

| Item | Description |
|---|---|
| All Ports | Shows the traffic statistics line chart of all ports combine. |
| Port 0 | Shows the traffic statistics line chart of port 0. |
| Port 1 | Shows the traffic statistics line chart of port 1. |
| Port 2 | Shows the traffic statistics line chart of port 2. |
| Port 3 | Shows the traffic statistics line chart of port 3. |
| Total | Shows the total packet counter line chart of all protocols. |
| TCP | Shows various packet counter line charts of TCP packets only. |
| UDP | Shows the packet counter line chart of UDP packets only. |
| ICMP | Shows the packet counter line chart of ICMP packets only. |
| Count | Only available when TCP tab is selected. Shows the total packet counter line chart of all TCP packets combine. |
| SYN | Only available when TCP tab is selected. Shows the packet counter line chart of TCP SYN packets. |
| ACK | Only available when TCP tab is selected. Shows the packet counter line chart of TCP ACK packets. |
| SYNACK | Only available when TCP tab is selected. Shows the packet counter line chart of TCP SYNACK packets. |
| RST | Only available when TCP tab is selected. Shows the packet counter line chart of TCP RST packets. |

| | |
|---|---|
| FIN | Only available when TCP tab is selected. Shows the packet counter line chart of TCP FIN packets. |
| Specify time frame for displaying real-time traffic | This window provides the time scale control of the line charts rendered above. The time window can be selected from the drop-down menu from 3 minutes to 2 days. |

**Summary Bit Counters**

This tab shows diagrams which show how traffic statistics of all protocols and types change over time in terms of bit count.

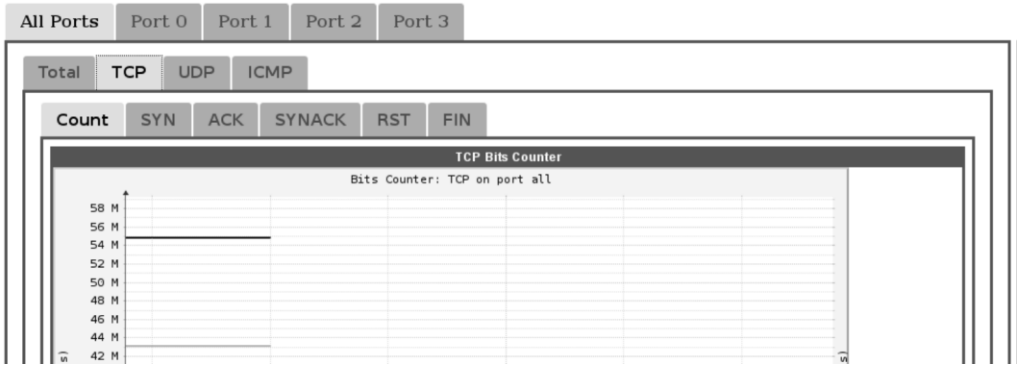



**Figure 23. Summary Bit Counter Window**

**Table 13. Summary Bit Counter Description**

| Item | Description |
|---|---|
| All Ports | Traffic statistics line chart of all ports. |
| Port 0 | Traffic statistics line chart of port 0. |
| Port 1 | Traffic statistics line chart of port 1. |
| Port 2 | Traffic statistics line chart of port 2. |
| Port 3 | Traffic statistics line chart of port 3. |
| Total | Total bit counter line chart of all protocols. |
| TCP | Packet counter line charts of TCP packets. |
| UDP | Bit counter line chart of UDP packets. |
| ICMP | Bit counter line chart of ICMP packets. |
| Count | Available when TCP tab is selected. Shows the total bit counter line chart of all TCP packets. |
| SYN | Available when TCP tab is selected. Shows the bit counter line chart of TCP SYN packets. |
| ACK | Available when TCP tab is selected. Shows the bit counter line chart of TCP ACK packets. |
| SYNACK | Available when TCP tab is selected. Shows the bit counter line chart of TCP SYNACK packets. |

| | |
|---|---|
| RST | Available when TCP tab is selected. Shows the bit counter line chart of TCP RST packets. |
| FIN | Available when TCP tab is selected. Shows the bit counter line chart of TCP FIN packets. |
| Specify time frame for displaying real time traffic | Provides the time scale control of the line charts rendered above. The time window can be selected from the drop-down menu from 3 minutes to 2 days. |

**Traffic Analysis and Archives**

In this tab, system administrators can retrieve historic traffic statistics and visualize into diagrams.

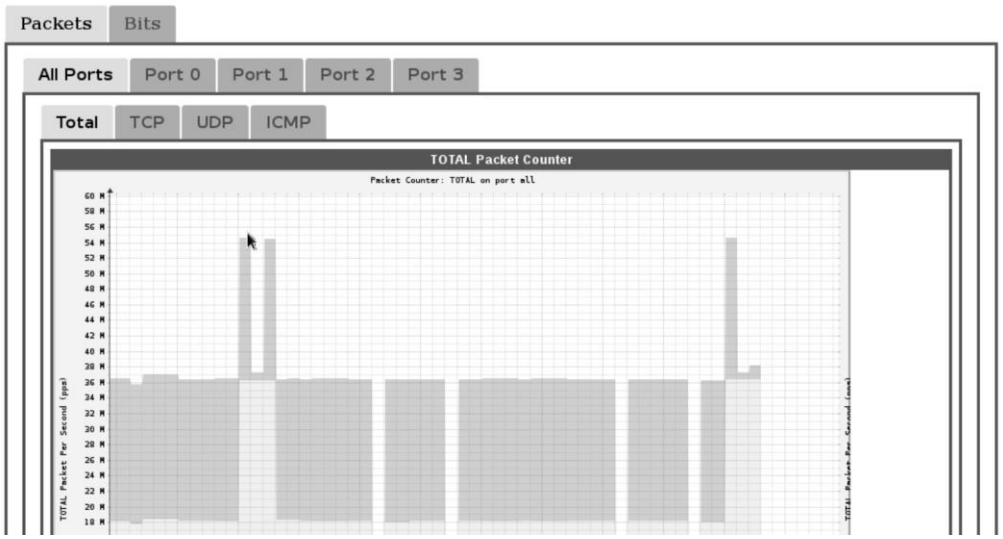



**Figure 24. Traffic Statistics Diagram Window**

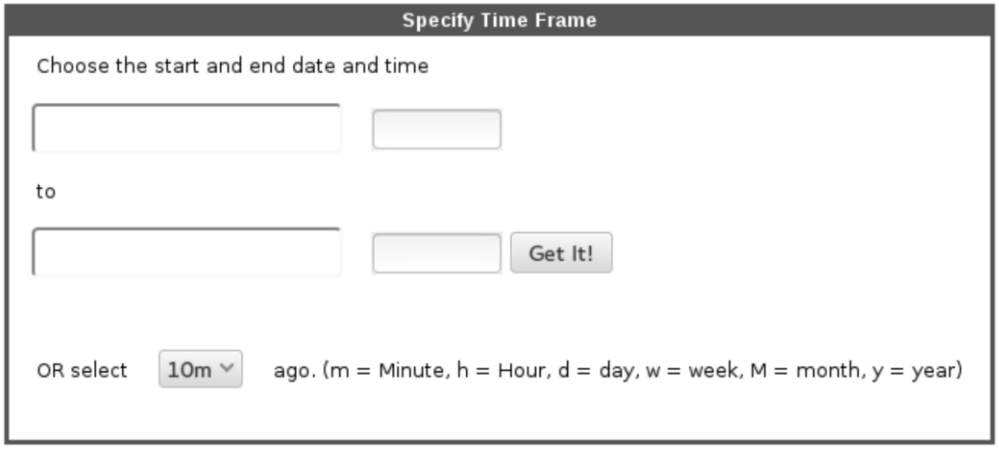



**Figure 25. Specify Time Frame Window**

**Table 14. Traffic Analysis and Archive Description**

| Item | Description |
|---|---|
| Packets | Select this tab to show traffic statistics diagrams in terms of packet count. |
| Bits | Select this tab to show traffic statistics diagrams in terms of bit count. |
| All Ports | Traffic statistics line chart of all ports. |
| Port 0 | Traffic statistics line chart of port 0. |
| Port 1 | Traffic statistics line chart of port 1. |
| Port 2 | Traffic statistics line chart of port 2. |
| Port 3 | Traffic statistics line chart of port 3. |
| Total | Total packet or bit counter line chart of all protocols during the selected time window. |
| TCP | Packet or bit counter line charts of TCP packets during the selected time window. |
| UDP | Packet or bit counter line charts of UDP packets during the selected time window. |
| ICMP | Packet or bit counter line charts of ICMP packets during the selected time window. |
| Count | Available when TCP tab is selected. Shows the total packet or bit counter chart of all TCP packets during the selected time window. |
| SYN | Available when TCP tab is selected. Shows the packet or bit counter chart of TCP SYN packets during the selected time window. |
| ACK | Available when TCP tab is selected. Shows the packet or bit counter chart of TCP ACK packets during the selected time window. |
| SYNACK | Available when TCP tab is selected. Shows the packet or bit counter chart of TCP SYACK packets during the selected time window. |
| RST | Available when TCP tab is selected. Shows the packet or bit counter chart of TCP RST packets during the selected time window. |
| FIN | Available when TCP tab is selected. Shows the packet or bit counter chart of TCP FIN packets during the selected time window. |
| Count | Available when TCP tab is selected. Shows the total packet or bit counter chart of all TCP packets during the selected time window. |
| Specify Time Frame | Provides the control of time window applying to the above diagrams. |
| Choose the start and end date time | The first and second rows set the starting time and end times. A selectable calendar pops up when clicking the first columns to generate formatted dates, while a drop-down menu pops up when clicking the second columns to generate formatted times. |
| Get it! | By clicking this button, the selected time window is applied to the above diagrams. |
| Or select…ago | The system administrator can also select the length of the most recent time window from 10 minutes to 3 years. |

### Raw Statistics

This tab provides the utility to show raw traffic statistics in real time. It is used mainly for testing.

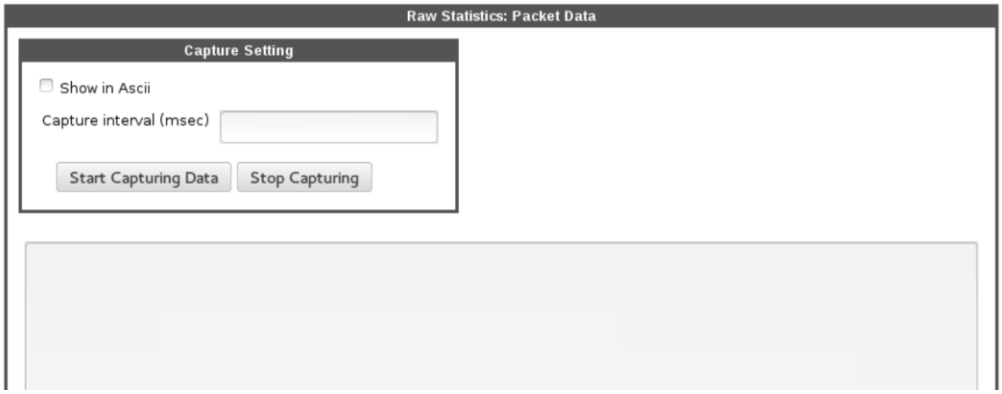



**Figure 26. Raw Statistics: Packet Data window**

**Table 15. Raw Stats description**

| Item | Description |
|---|---|
| Raw Statistics: Packet Data | The main window of this tab shows the raw traffic statistics in terms of packet. |
| Capture Setting | This sub window comprises the control of capturing raw traffic statistics. |
| Show in ASCII | Click to view the results in ASCII code. |
| Capture Interval | Enter a number in the text box to assign the capture interval in millisecond. |
| Start Capturing Data | Click to capture results in the box below. |
| Stop Capturing | Click to stop data capturing. |

### Traffic Statistics (VG-Format)

This tab presents traffic statistics aggregated per server range ID.

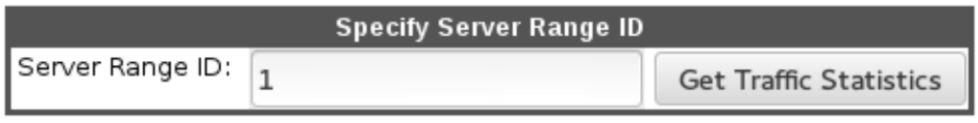



**Figure 27. Specify Server Range ID Window**

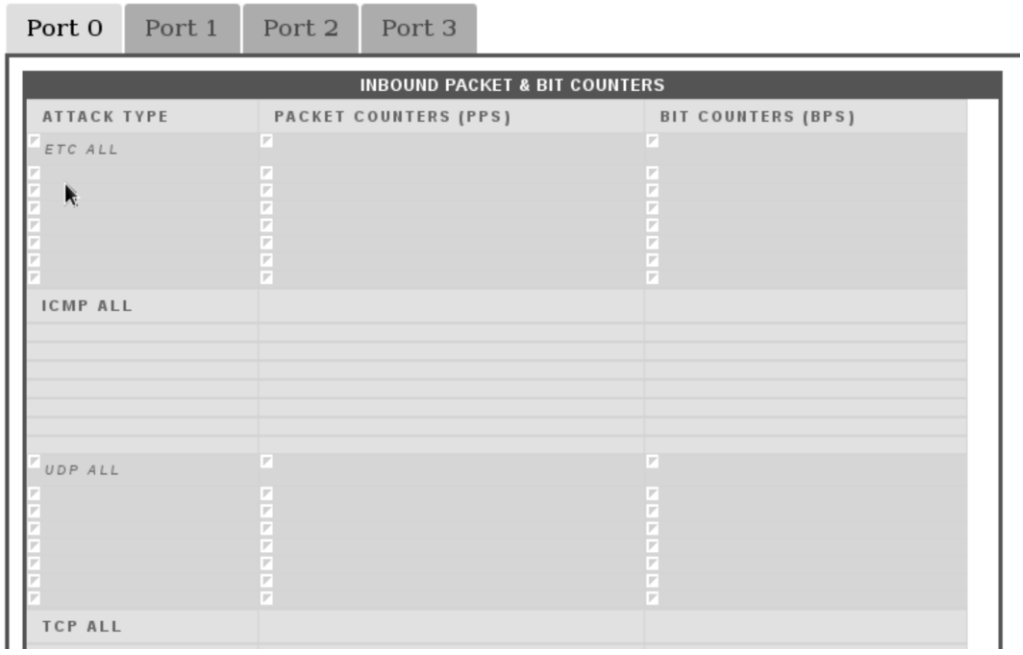



**Figure 28. Inbound Packet & Bit Counters Table**

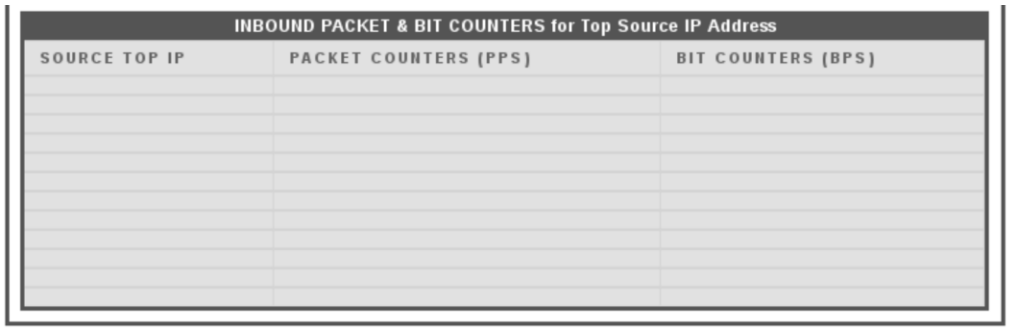



**Figure 29. Inbound Packet & Bit Counters for Top Source IP Address List**

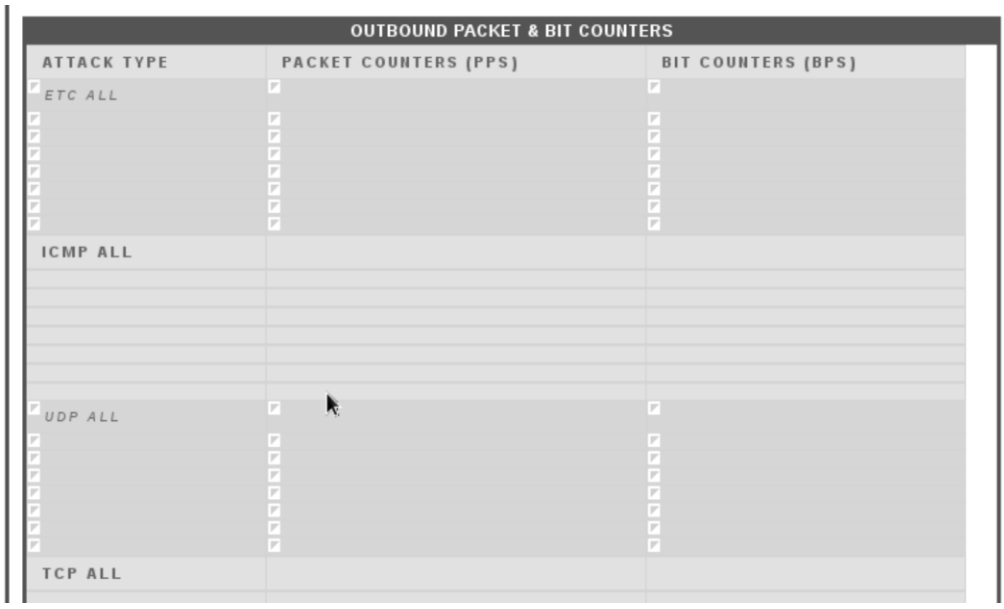



**Figure 30. Outbound Packet & Bit Counters Table**

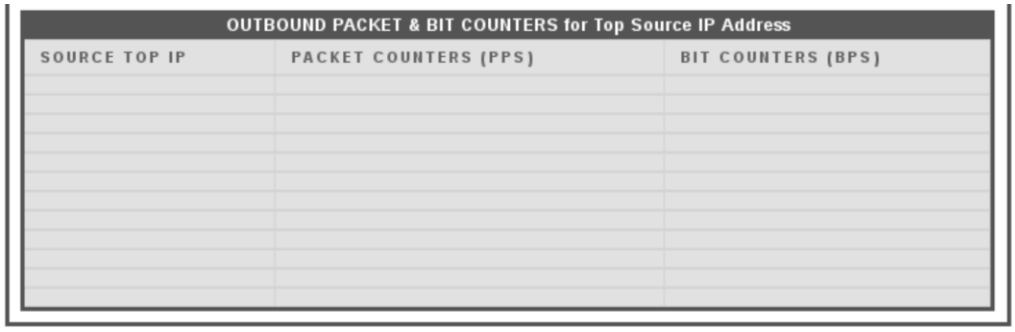



**Figure 31. Outbound Packet & Bit Counters for Top Source IP Address List**

**Table 16. Traffic Stat's (VG-Format) Description**

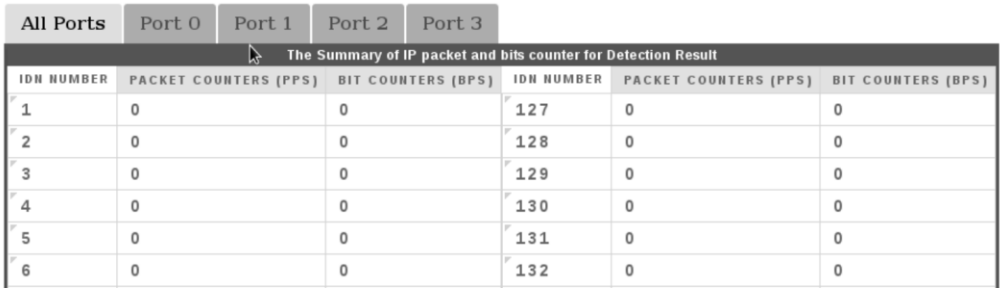
| Item | Description |
|---|---|
| Specify Server Range ID | Enter to identify the predefined server range. |
| Get Traffic Statistics | Click to show the aggregated traffic statistics. |
| Inbound Packet and Bit Counters | List of inbound packet and bit counter for each attack type. |
| Attack Type | Supported attack types. |
| Packet Counter | Packet count statistics |
| Bit Counters | Bit count statistics. |
| Outbound Packet and Bit Counters | List of outbound packet and bit counter for each attack type. |
| Inbound Packet and Bit Counters for Top-Source IP Address | List of source IP addresses sorted by inbound packet and bit counts. |

| | |
|---|---|
| Outbound Packet and Bit Counters for Top-Source IP Address | List of source IP addresses sorted by outbound packet and bit counts. |

### Detection Results

This tab presents the detection results aggregated by server range ID.


**Figure 32. Specify Server ID Window**




| IDN NUMBER | PACKET COUNTERS (PPS) | BIT COUNTERS (BPS) | IDN NUMBER | PACKET COUNTERS (PPS) | BIT COUNTERS (BPS) |
|---|---|---|---|---|---|
| 1 | 0 | 0 | 127 | 0 | 0 |
| 2 | 0 | 0 | 128 | 0 | 0 |
| 3 | 0 | 0 | 129 | 0 | 0 |
| 4 | 0 | 0 | 130 | 0 | 0 |
| 5 | 0 | 0 | 131 | 0 | 0 |
| 6 | 0 | 0 | 132 | 0 | 0 |

**Figure 33. The Summary of IP Packet and Bit Counter for Detection Result**

**Table 17. Detection Results Description**

| Item | Description |
|---|---|
| Specify Server Range ID | Comprises the control of server range ID. |
| Server Range ID | Enter to identify the predefined server range. |
| Get Detection Result | Displays the detection results of the selected server range. |
| The Summary of IP Packet and Bits Counter for Detection Result | List of detection results. Each entry presents an IDN and the corresponding packet and bit counters. |
| IDN Number | Presents the attack type; ranging from 0 to 252. |
| Packet Counters | Packet count of the detected IDN. |
| Bit Counters | Bit count of the detected IDN. |

**Packet Captures**

This tab presents the packet capture summary per server range ID.

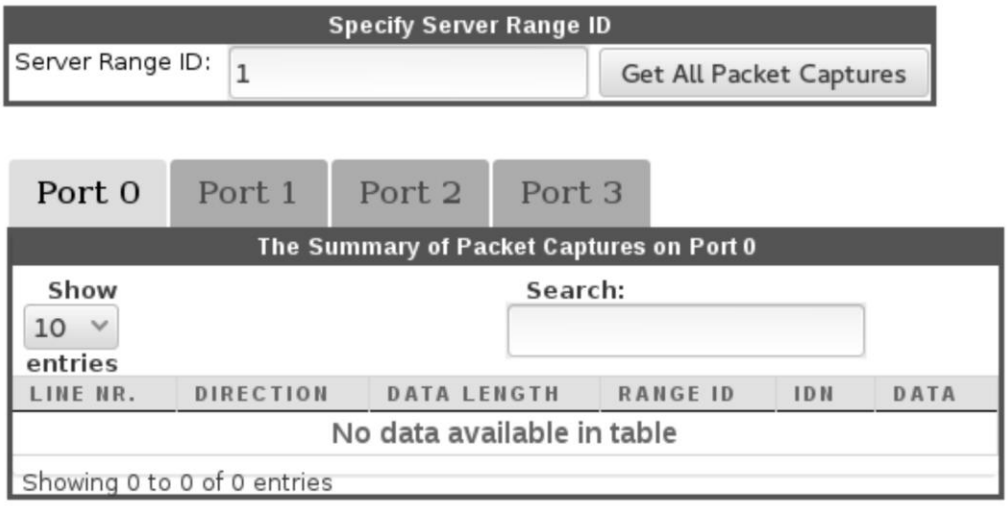



**Figure 34. Control Windows in Packet Captures Tab**

**Table 18. Packet Captures Description**

| Item | Description |
|---|---|
| Specify Server Range ID | Provides the control of server range ID selection. |
| Server Range ID | Enter to identify the predefined server range. |
| Get All Packet Captures | Click after the server range ID is entered to update the packet capture summary listed below. |
| Show Entries | Select how many entries in the list are displayed per page. |
| Search | Filter the list below by entering search keyword. |
| Line Number | The line number in the main list of all capture results. |
| Direction | Defines the packet direction, outbound or inbound. |
| Data Length | Defines the length of captured data. |
| Range ID | Defines the range ID associating |
| IDN | Presents the attack type |
| Data | The captured data content. |

### Block Events

This tab presents the list of block events per port per server range ID.

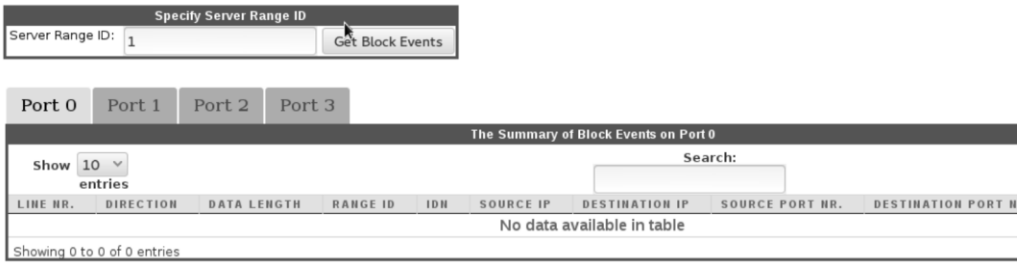



**Figure 35. Control Windows in Block Events Tab**

**Table 19. Block Events Description**

| Item | Description |
|---|---|
| Specify Server Range ID | Provides the control of server range ID selection. |
| Server Range ID | Enter to identify the predefined server range. |
| Get Block Events | Select after the server range ID is entered to update the block event summary lists below. |
| Port 0 ~ Port 3 | Select the block event summary list of Port 0 to Port 3. |
| Show Entries | Select the number of entries in the list are displayed |
| Search | Enter the search keyword |
| Line Number | Line number in the main list of all block events |
| Direction | The packet direction, outbound or inbound, of the block event. |
| Data Length | The length of blocked packet. |
| Range ID | The range ID associating with this entry. |
| IDN | The IDN, presenting the attack type, associating to this entry. |
| Source IP Address | The source IP address of the blocked packet. |
| Destination IP Address | The destination IP address of the blocked packet. |
| Source Port Number | The source port number of the blocked packet. |
| Destination Port Number | The destination port number of the blocked packet. |
| IP Protocol | The IP protocol of the blocked packet. |

### VG Format

This tab provides an integral presentation of VG (Virtual Group) format data.

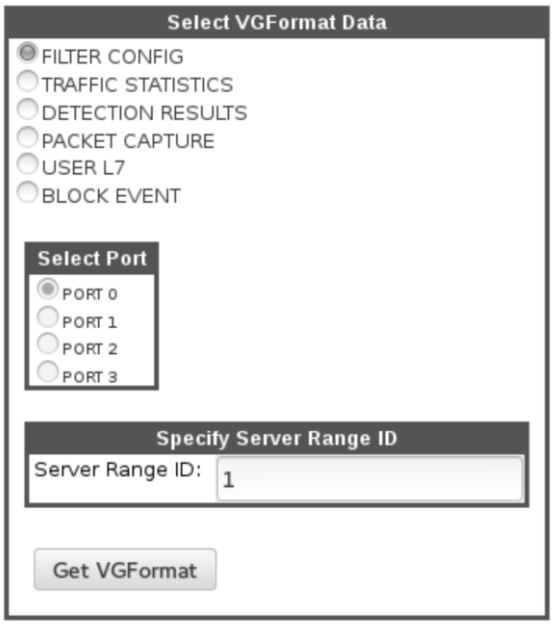



**Figure 36. Select VG Format Data Window**

**Table 20. VG Format Description**

| Item | Description |
|---|---|
| Select VG Format Data | The window comprises the main controls of VG format data presentation. |
| Filter Configuration | Showing the filter configuration per server range ID. |
| Traffic Statistics | Showing the traffic statistic data per server range ID. |
| Detection Results | Showing the detection results per server range ID. |
| Packet Capture | Showing the packet capture result per port per server range ID. |
| User L7 | Showing the L7 user configuration per server range ID. |
| Block Event | Showing the block events per port per server range ID. |
| Select Port | Selecting the port to present port-specific VG format data. The port selections are only available when packet capture or block event is selected above. |
| Specify Server Range ID | This sub window highlights the server range ID selection. |
| Server Range ID | Enter the number identifies the predefined server range. |
| Get VG Format | After data type and/or port number is selected and the server range ID is entered, click this button to update the VG format data below. |

This tab provides configuration interfaces for white list and black list.

### White List

This tab provides the configuration interface to the white list.

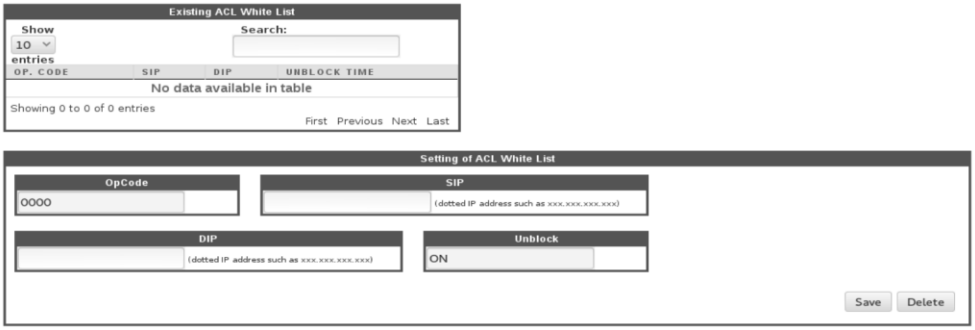



**Figure 37. White List Configuration Windows**

**Table 21. White List Description**

| Item | Description |
|---|---|
| Existing ACL White List | This window shows the existing white list. |
| Show Entries | Select how many entries in the list are displayed per page. |
| Search | Enter the search keyword in this text box. |
| Operation Code | The hex code identifies the operation of the white list entry. |
| Source IP Address | The source IP address of the white list entry. |
| Destination IP Address | The destination IP address of the white list entry. |
| Unblock | Grant packets matching the entry unblock privilege. |
| Showing Entries | Indicates how many entries out of the total number of entries are displayed in the current view. |
| First | Click to jump to the first page. |
| Previous | Click to jump to the previous page. |
| Next | Click to jump to the next page. |
| Last | Click to jump to the last page. |
| Setting ACL White List | The window comprises the setting form of an ACL entry. The form fields are filled with current settings of the white list entry select from the table above for modification. |
| Save | A new entry is added after it is created from scratch after clicking. For entry modification, the entry selected from the above table is updated after clicking this button. |
| Delete | The entry selected from the above table is removed from the white list after clicking this button. |

**Black List**

This tab provides the configuration interface to the black list.

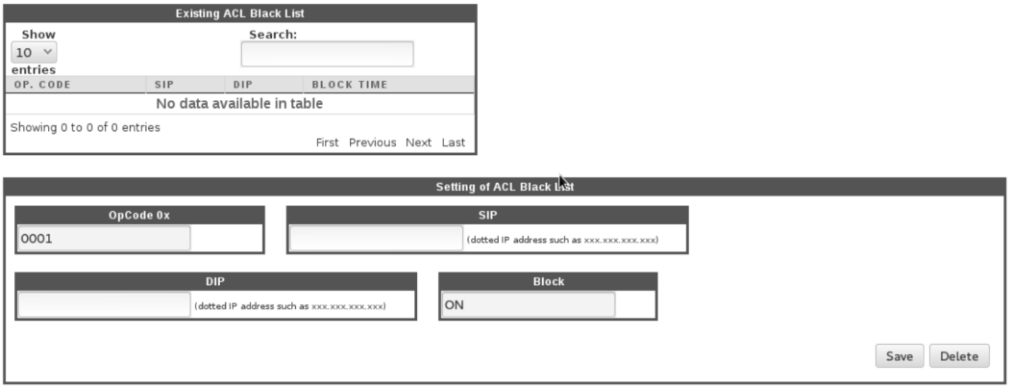



**Figure 38. Black List Configuration Windows**

**Table 22. Black List Description**

| Item | Description |
|---|---|
| Existing ACL Black List | This window shows the existing black list. |
| Show Entries | Select how many entries in the list are displayed per page. |
| Search | Enter the search keyword in this text box. |
| Operation Code | The hex code identifies the operation of the black list entry. |
| Source IP Address | The source IP address of the black list entry. |
| Destination IP Address | The destination IP address of the black list entry. |
| Block | Enable blocking packets matching the entry. |
| Showing Entries | Indicates how many entries out of the total number of entries are displayed in the current view. |
| First | Click to jump to the first page. |
| Previous | Click to jump to the previous page. |
| Next | Click to jump to the next page. |
| Last | Click to jump to the last page. |
| Setting ACL Black List | The window comprises the setting form of an ACL entry. The form fields are filled with current settings of the black list entry select from the table above for modification. |
| Save | A new entry is added after it is created from scratch after clicking. For entry modification, the entry selected from the above table is updated after clicking this button. |
| Delete | The entry selected from the above table is removed from the white list after clicking this button. |

This tab provides interface to configure attack mitigation rules for layer 3, layer 4, and layer 7.


**Figure 39. Layer Selection Tabs**

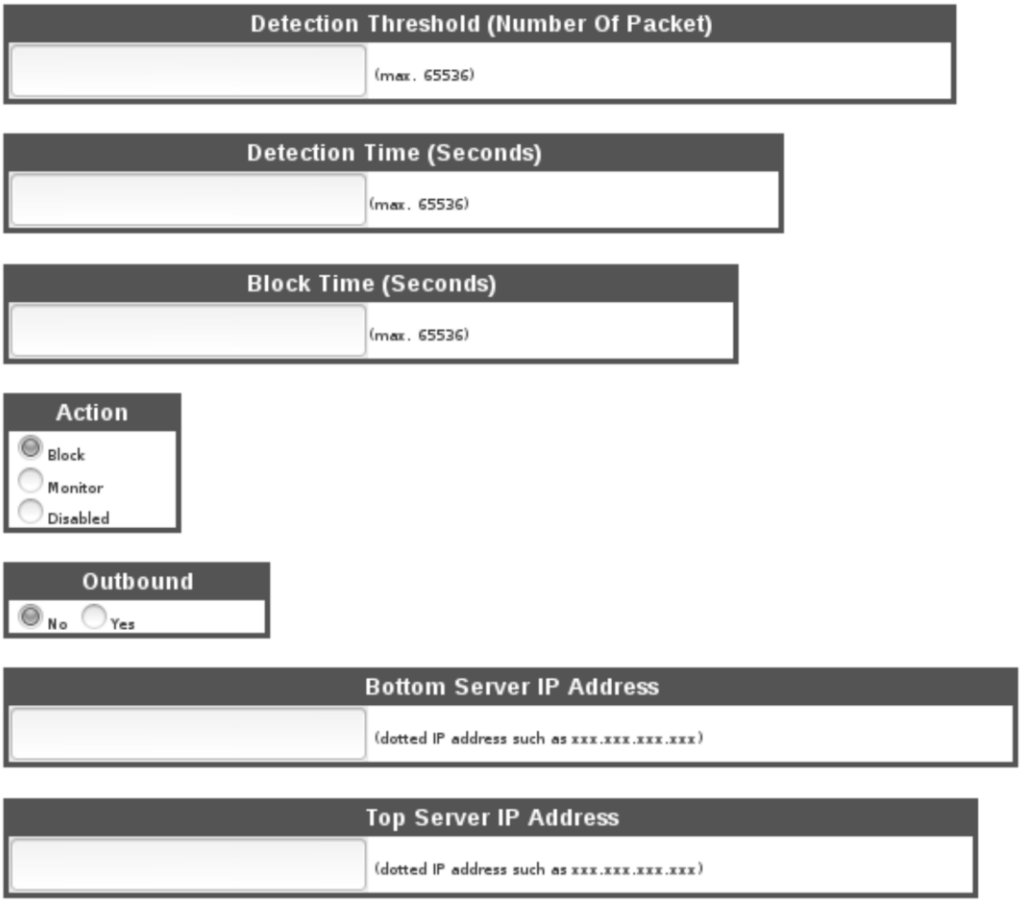



**Figure 40. Common Input Fields Across All Layers**

**Table 23. Common Input Fields Across All Layers in Attack Mitigation Tab**

| Item | Description |
|---|---|
| Detection Threshold (Number of Packets) | Define the minimum number of packets matching the rule within the detection time (defined below) to actualize a detection of the rule. |
| Detection Time | Define the time window in seconds. |
| Block Time (Seconds) | Define how long the subsequent packets matching the rule should be blocked after a detection is actualized, if the mitigation action is Block. |

| | |
|---|---|
| Action | The action to be taken to mitigate the detected attack. Administrators can choose Block (blocking the subsequent packets of the attack for a while), Monitor (only monitoring the packets matching the rule after the detection without touching the traffic), or Disable (disabling the rule until it is reactivated by setting to Block or Monitor). |
| Outbound | Define the rule to detect only outbound packets. |
| Bottom Server IP Address | Define the lowest server IP address the rule matches. |
| Top Server IP Address | Define the highest server IP address the rule matches. |
| Save | A new entry is added after it is created from scratch after clicking this button. For entry modification, the entry selected from the existing settings table is updated after clicking this button. |
| Delete | The entry selected from the existing settings table is removed from the list after clicking this button. |

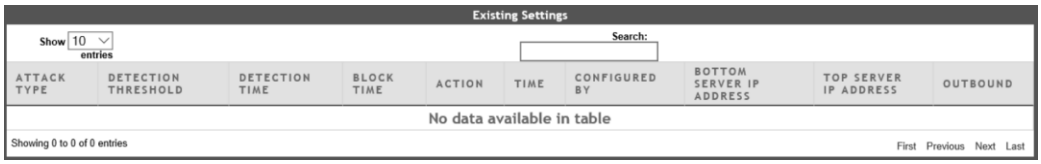



**Figure 41. Existing Settings Table**

**Table 24. Existing Settings Fields Description**

| Item | Description |
|---|---|
| Attack Type | Attack type of the rule entry. |
| Detection Threshold | The minimum number of packets matching the rule within the detection time to actualize a detection of the rule. |
| Detection Time | The time window in seconds. |
| Block Time | How long the subsequent packets matching the rule should be blocked after a detection is actualized. |
| Action | The value can be Block, Monitor, or Disable. |
| Time | The time when the rule was created. |
| Configured By | The user ID who created this rule. |
| Bottom Server IP Address | The lowest server IP address the rule matches. |
| Top Server IP Address | The highest server IP address the rule matches. |
| Outbound | The value is Yes when the rule detects only outbound packets - otherwise it is No. |
| Showing Entries | Indicates how many entries out of the total number of entries are displayed in the current view. |
| First | Click to jump to the first page. |

| | |
|---|---|
| Previous | Click to jump to the previous page. |
| Next | Click to jump to the next page. |
| Last | Click to jump to the last page. |

**Mitigation Settings For Layer 3**

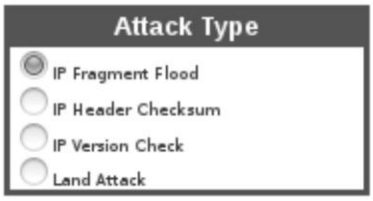



**Figure 42. Layer 3 Attack Type Selection Window**

**Table 25. Attack Type Selections for Layer 3**

| Item | Description |
|---|---|
| Attack Type | One of the four layer 3 attack types could be selected to define an attack mitigation rule entry including IP Fragment Flood, IP Header Checksum, IP Version Check, and Land Attack. |

**Mitigation Settings for Layer 4**

The attack type selections specific for layer 4 mitigation settings.

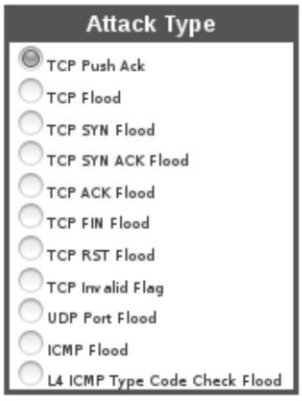



**Figure 43. Layer 4 Attack Type Selection Window**

**Table 26. Attack Type Selections for Layer 4**

| Item | Description |
|---|---|
| Attack Type | One of the eleven layer 4 attack types could be selected to define an attack mitigation rule entry including TCP Push ACK, TCP Flood, TCP SYN Flood, TCP SYN ACK Flood, TCP ACK Flood, TCP FIN Flood, TCP RST Flood, TCP invalid Flag, UDP Port Flood, ICMP Flood, and L4 ICMP Type Code Check Flood. |

### Mitigation Settings for Layer 7

The attack type selections specific for layer 7 mitigation settings.


**Figure 44. Layer 7 Attack Type Selection Window**

**Table 27. Attack Type Selections for Layer 7**

| Item | Description |
|---|---|
| Attack Type | One of the three layer 7 attack types could be selected to define an attack mitigation rule entry including L7 CC Cache Control Attack, GET Flood, and DNS Flood. |

## Port Configuration

This window shows the port status report and provides the interface to manually assess the port status.

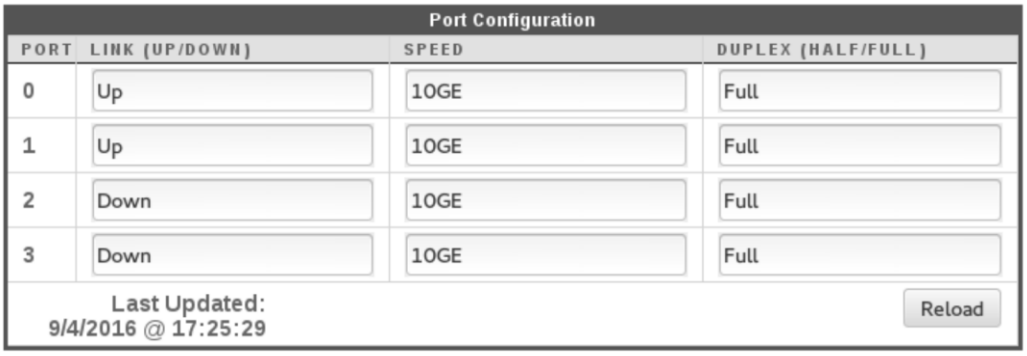



**Figure 45. Port Configuration Window**

**Table 28. Port Status Indication**

| Item | Description |
|---|---|
| Port | The port number. |
| Link (Up/Down) | This row shows whether the link of each port is Up (with active connection) or Down (inactive). |
| Speed | This row indicates the link speed of each port. |
| Duplex (Half/Full) | This row indicates the duplex mode, Full (full-duplex) or Half (half-duplex) of each port. |
| Last Updated | The date and time the port status was assessed. |
| Reload | The port status is assessed and updated by clicking this button |

## CHAPTER 10 ADMINISTRATION

Administration tab provides access to system administration related configurations, information, and utilities.

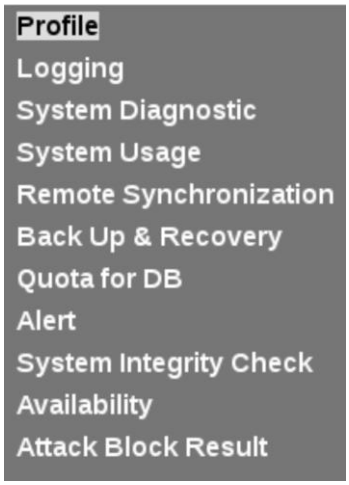



**Figure 46. Left Panel Sub-Tabs in Administration Tab**

### Profile

In Profile tab, system administrators can check their encrypted password, change the password, change the email address used to receive notifications, set the IP address allowed for remote access, and set the system name.

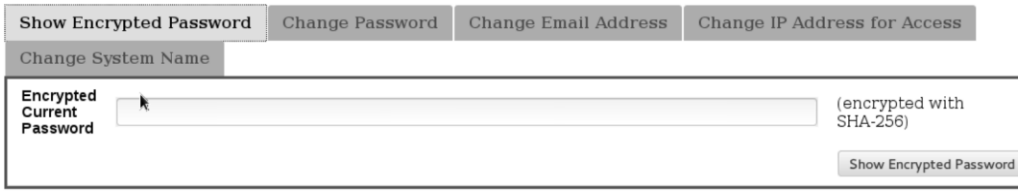



**Figure 47. Show Encrypted Password Tab of Profile Window**

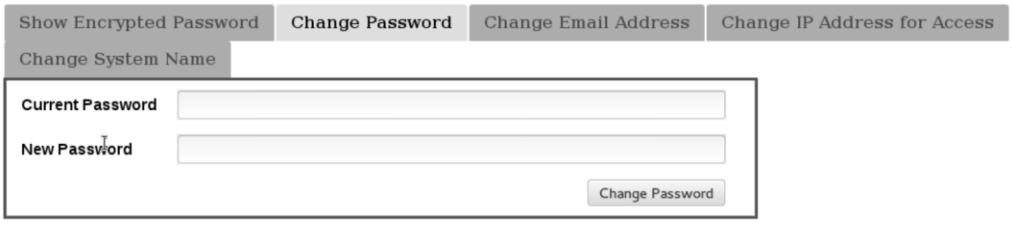



**Figure 48. Change Password Tab of Profile Window**

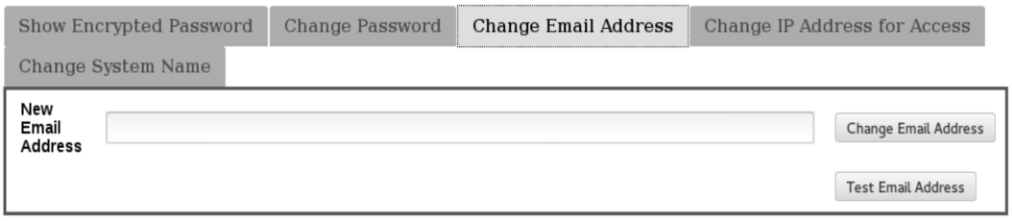



**Figure 49. Change Email Address Tab of Profile Window**

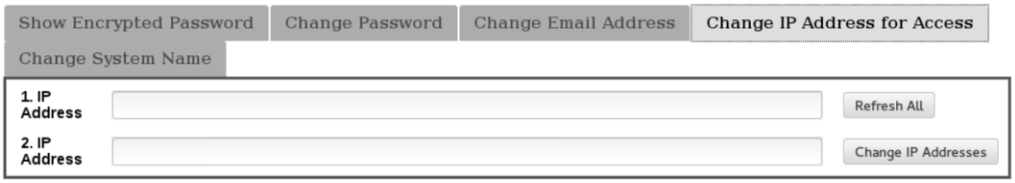



**Figure 50. Change IP Address for Access Tab of Profile Window**


**Figure 51. Change System Name Tab of Profile Window**

**Table 29. Profile Window Description**

| Category | Button | Description |
|---|---|---|
| Show Encrypted Password | Show Encrypted Password | By clicking, the current password encrypted with SHA-256 is displayed in the above text box. The encrypted password cannot be used to retrieve the original password in plain text and is useful to check whether the password is shared with other systems. |
| Change Password | Current Password | Enter the current password in this text box. |
| | New Password | Enter the new password in this text box. The password requirement hint will be shown when typing. |
| | Change Password | Once the current password entered is correct and the new password entered meets the requirement, the password is changed after clicking this button. |
| Change Email Address | New Email Address | Enter the new email address for receiving system notifications in this text box. |
| | Change Email Address | By clicking, the new email address will be registered in the system replacing the previous one. |
| | Test Email Address | A test email will be sent to the email address entered above when clicking. User can check whether emails sent from the system can be delivered properly. |

| | | |
|---|---|---|
| Change IP Address for Access | IP Address | User can set up to two IP addresses to access the system. Please remember that localhost (127.0.0.1) is not granted to access the system until it is set. |
| | Refresh All | The current IP addresses to access the system are shown in the IP address text boxes after click this button. |
| | Change IP Addresses | The IP addresses entered in both text boxes are registered in the system by clicking. |
| Change System Name | System Name | Enter the new system name in this text box. |
| | Update System Name | The system name is replaced by the name entered in the text box after clicking this button. |

**Logging**

In logging tab, the user can review the system and configuration logs in tabulated format.


**Figure 52. System Log Window**

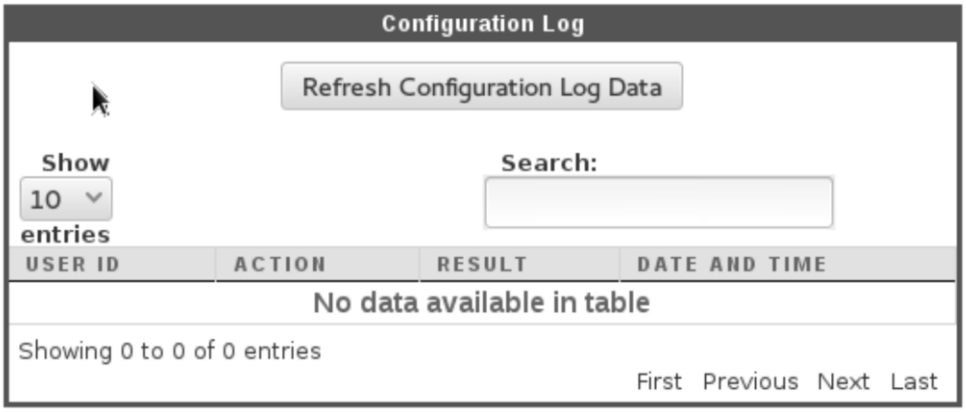



**Figure 53. Configuration Log Window**


**Figure 54. Administrator Log Window**

**Table 30. Logging Tab Description**

| Tab | Description |
|---|---|
| System Log | Shows the system related event log such as failed login attempts. |
| Refresh System Log Data | Tabulated system log is populated after clicking. |
| Show Entries | Select how many entries in the log are displayed per page. |
| Search | Enter the search keyword in this text box. |
| USER ID | The user ID who triggered or was involved in the event. |
| Action | The action which triggered or was involved in the event. |
| Result | The result of the action in the event. |
| Date and Time | The date and time when the event occurred. |
| Configuration Log | The box shows configuration event log like setting new layer 3, 4, 7 attack mitigation rules. |
| Refresh Configuration Log Data | Tabulated configuration log is populated after clicking. |
| Administration Log | Shows administration event log like setting new IP addresses to access the system. |
| Refresh Administration Log | Tabulated administrator log is populated after clicking. |

**System Diagnostic**

This tab provides an interface to access the self-test subroutine. In case of observing erroneous behavior of the system, this tool displays summarized subsystem status which implies where the troubleshooting should begin with.

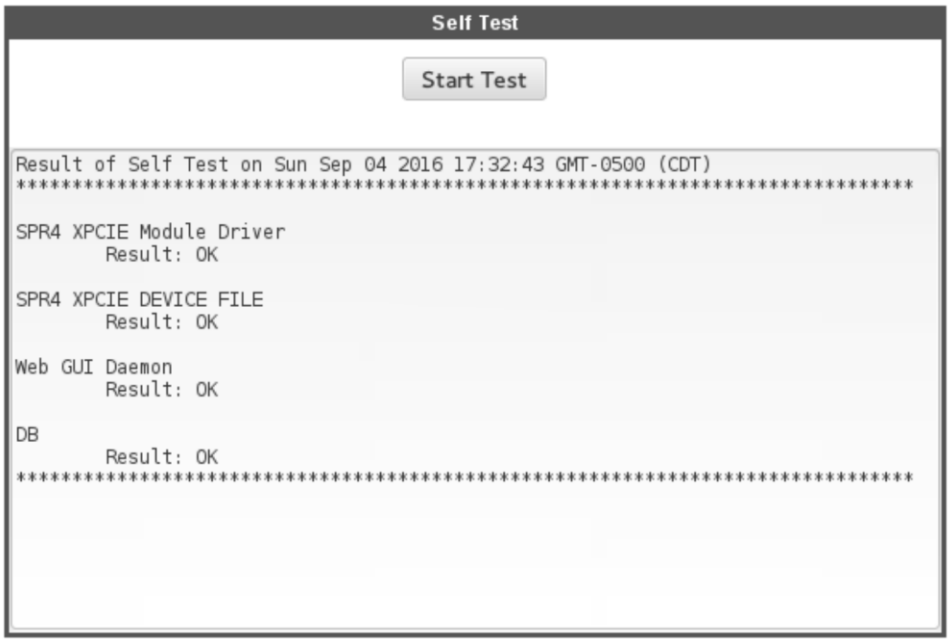



**Figure 55. Self Test Window**

**Table 31. Self Test Description**

| Item | Description |
|---|---|
| Self Test | This window is the interface to the underlying self-test subroutine. |
| Start Test | Launches the self-test subroutine, displaying the result in the text box. |

### System Usage

System usage tab shows system usage information in terms of blocked and active users.


**Figure 56. Blocked Users and Active Users Windows**

**Table 32. System Usage Description**

| Item | Description |
|---|---|
| Blocked Users | This window shows the list of blocked users. |
| Refresh | By clicking both blocked and active users' lists are refreshed and displayed. |

| | |
|---|---|
| Unblock | By selecting a user in the list and clicking this button, the selected user is unblocked from the system. |
| Show Entries | Select how many entries in the list are displayed per page. |
| Search | By entering search keyword in this text box, the list below is filtered by the keyword right away. |
| USER ID | The user which is blocked or active in the list. |
| Status | The user's status. |
| Last Login | The time when the user logged in last time. |
| Active Users | The window shows the list of active users. |
| Purge | By selecting an active user from the list and clicking this button, the selected user gets kicked out from the system. |

**Remote Synchronization**

This tab facilitates synchronizing configuration with remote host.

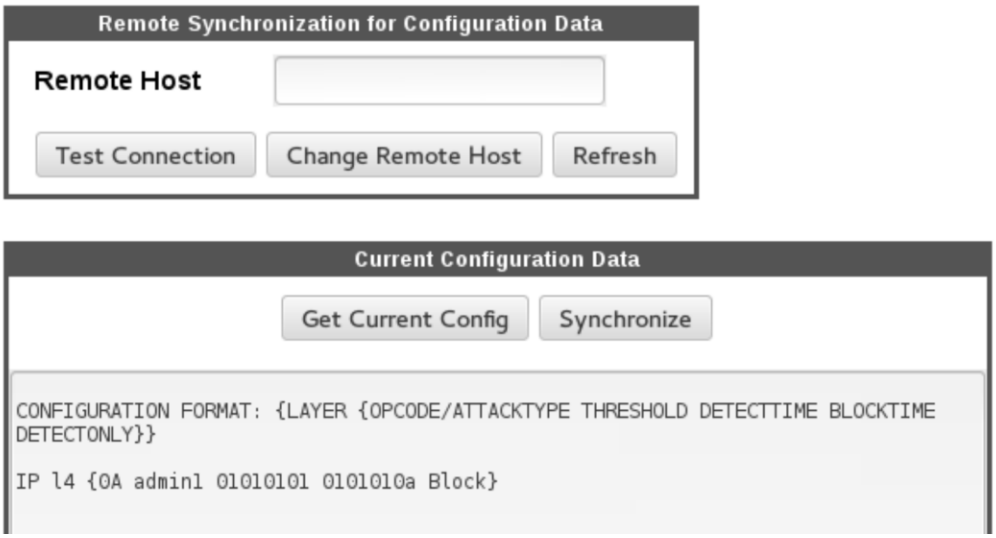



**Figure 57. Remote Synchronization for Configuration Data and Current Configuration Data Windows**

**Table 33. Remote Synchronization Description**

| Item | Description |
|---|---|
| Remote Synchronization for Configuration Data | This window provides the control of synchronization connectivity. |
| Remote Host | The address of the remote host. |
| Test Connection | The connectivity to the remote host as entered in the text box is tested when clicking this button. |
| Change Remote Host | By editing the remote host text box and clicking this button, the new remote host address is registered to the system. |

| | |
|---|---|
| Refresh | The current remote host address is displayed in the text box after clicking this button. |
| Current Configuration Data | This window provides the control of configuration data to be synchronized. |
| Get Current Configuration | The configuration data is displayed in the text box below after clicking this button. |
| Synchronize | The configuration data is synchronized with the remote host set in the window above by clicking this button. |

**Backup & Recovery**

In this tab, the user can manage configuration data backup and recovery of the system.


**Figure 58. Configuration Data Backup Window**


**Figure 59. Recovery Window**


**Figure 60. Content of the Backup Window**

**Table 34. Backup & Recovery Description**

| Item | Description |
|---|---|
| Configuration Data Backup | This window provides the interface to create a backup of the configuration data of the system. |
| Name of Backup | The user can optionally enter a name to identify the backup to be created. |
| Backup | By clicking this button, a backup of the configuration data is created. If the name is entered in the text box, the backup is created with the customized name. |
| Recovery | The window provides the user the interface to recover the configuration data of the system from the previous created backup. |
| Refresh | The list of the backups stored in the system is populated in the box below by clicking this button. |
| Recovery | By selecting a backup from the list and clicking this button, the configuration data of the system is recovered from the selected backup. |
| Delete | By selecting a backup from the list and clicking this button, the selected backup is deleted from the list. |
| Show Entries | Select how many entries in the list are displayed per page. |
| Search | By entering search keyword in this text box, the list below is filtered by the keyword right away. |
| Name | The name of the backup. |
| Date/Time | The date and time the backup was created. |
| Backed Up By | The user ID of who created the backup. |
| Content of the Backup | This window displays the content of a selected backup. |
| Display Content | By selecting a backup from the above window and clicking this button, the configuration data in the backup is displayed in the box below. |

### Quota for DB

This tab provides the control of how much hard drive space allowed for the system database.

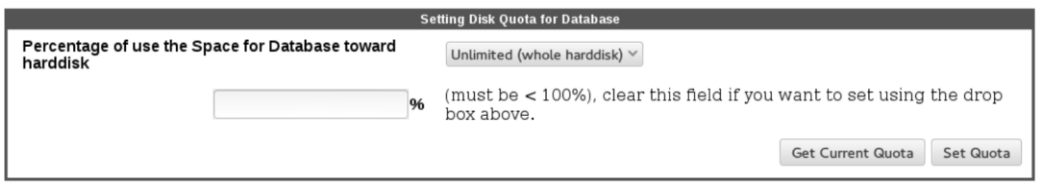



**Figure 61. Setting Disk Quota for Database Window**

**Table 35. Quota for DB Description**

| Item | Description |
|---|---|
| Setting Disk Quota for Database | This window contains the hard drive usage control of the database. |
| Percentage of Use of the Space for Database Toward Hard-disk | Two ways to control the usage percentage of the database. The user can either select unlimited (allowing using the whole hard drive), 30%, 20%, or 10% of the hard drive space from the drop-down menu, or fill in the desired percentage in the input text box. Please note that the input text box is prioritized over the drop-down menu. Thus the user has to clear the input text box if the value selected from the drop-down menu is desired. |

### Alert

Users can configure the threshold of sending alert by email in this tab.


**Figure 62. Set Threshold to Alert Window**

**Table 36. Alert Description**

| Item | Description |
|---|---|
| Set Threshold to Alert | This window provides the control of the alert threshold. |
| Number of Attack Detections Before Sending Alert | The threshold value can be entered into this text box. |
| Get Current Threshold Value | By clicking this button, the current threshold in use is displayed in the text box above. |
| Set Alert Threshold | By entering a threshold value in the text box above and clicking this button, the alert threshold value is updated. The system only sends alert emails when the number of attack detections exceeds the threshold, which prevents the user's inbox gets clogged by sporadic attack detections. |

### System Integrity Check

This tab includes a system integrity check tool to ensure the integrity of system software and data structures.


**Figure 63. Initiate System Integrity Check Window**

**Table 37. System Integrity Check Description**

| Item | Description |
|---|---|
| Initiate System Integrity Check | This window comprises the control of the system integrity check tool. |
| Backup | By checking this box, the backups are included in the integrity check subroutine. |
| Config | By checking this box, the configuration of the system is included in the integrity check subroutine. |
| Archives & Historical Data | By checking this box, the archives and historic data is included in the integrity check subroutine. |
| Executables | By checking this box, the software executables are included in the integrity check subroutine. |
| Integrity Check Period | The user can select periodic system integrity check of every day, 2 days, 3 days, 1 week, 2 weeks, or 1 month, or disable the periodic check by selecting none, in the drop-down list. |
| Save | By clicking the button, the configuration of periodic system integrity check is registered to the system. |
| Check Now | Users can also click this button to manually initiate an iteration of system integrity check of all types right away. The result of each type is shown underneath. |

**Availability**

This tab provides the control of periodic database and web server processes status check.


**Figure 64. Process Check Window**

**Table 38. Availability Description**

| Item | Description |
|---|---|
| Process Check | This window provides the input and output of process status check period settings. |
| Database and Web Server Check | Users can choose performing hourly, weekly, or monthly process status check, or disabling it through this dropdown menu. |
| Set | By selecting the period of process status check from the drop-down menu and clicking this button, the process check configuration is registered to the system. |
| Refresh | The current process status check configuration is updated to the drop-down menu by clicking this button. |

### Attack Block Results

The attack block result of user selectable time frame is shown in this tab.

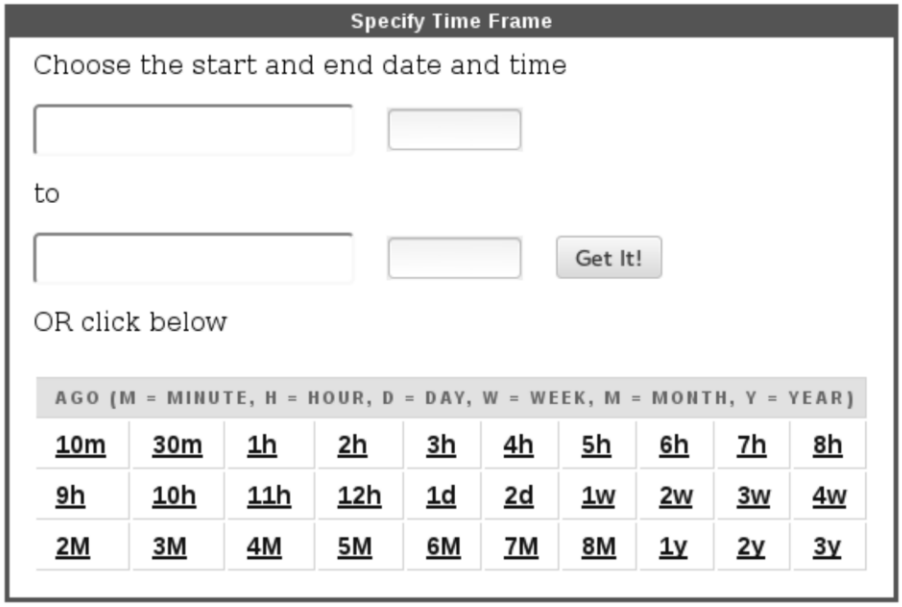



**Figure 65. Specify Time Frame Window**

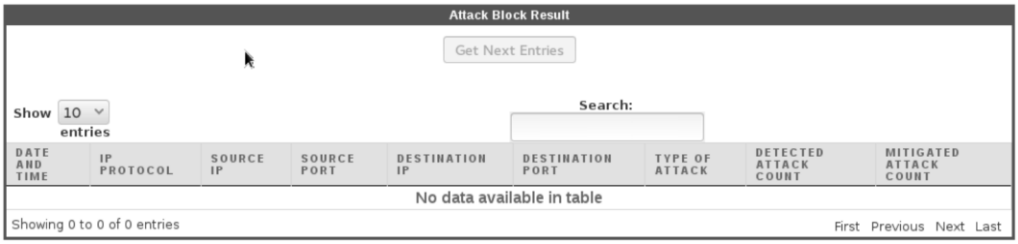



**Figure 66. Attack Block Result Window**

**Table 39. Attack Block Result Description**

| Tab | Description |
|---|---|
| Specify Time Frame | This window provides the time frame control of the blocked attack event listing. |
| Choose the Start and End Data and Time | The first and second rows set the starting time and end time, respectively. A selectable calendar pops up when clicking the first columns to generate formatted dates, while a drop-down menu pops up when clicking the second columns to generate formatted times. |
| Get It! | By clicking this button, the attack block result list is displayed in the window below. |
| Or Click Below | If it is the most recent time frame interests the user, the user can also select the length of the time frame from the menu below. The attack block result list is updated right after the time frame length is clicked. |
| Attack Block Result | This window displays the attack block result list of the time frame selected in the window above. |
| Show Entries | Select how many entries in the list are displayed per page. |
| Search | By entering search keyword in this text box, the list below is filtered by the keyword right away. |
| Date and Time | The date and time when the attack occurred. |
| IP Protocol | The IP protocol involved in the attack. |
| Source IP Address | The source IP address involved in the attack. |
| Source Port Number | The source port number involved in the attack. |
| Destination IP Address | The destination IP address involved in the attack. |
| Destination Port Number | The destination port number involved in the attack. |
| Type of Attack | The type of attack identified by the system |
| Detected Attack Count | The number of attacks detected. |
| Mitigated Attack Count | The number of attacks mitigated. |