Configuring Attack Defense

To configure Attack Defense, take the following steps:

1. On the Navigation pane, click **Configure** > **Security** > **Attack Defense** to visit the Attack Defense page.
2. Select a security zone for Attack Defense from the **Zone** drop-down list.
3. To enable all the Attack Defense functions for the security zone, select the **Enable all** check box, and also select an action from the **Action** drop-down list. To enable an individual defense function, select its corresponding check box.
4. Configure parameters for the selected functions.
5. Click **OK** to save the changes.

Options for Attack Defense are described in detail as follows:

Select a zone

Zone: Select a security zone for Attack Defense from the **Zone** list.

Select all

Enable all: Select this check box to enable all the Attack Defense functions for the security zone.

Action: Specifies an action for all the Attack Defense functions, i.e., the defense measure the system will take if any attack has been detected.

- **Drop** - Drops packets. This is the default action.
- **Alarm** - Gives an alarm but still permits packets to pass through.

Flood defense

ICMP flood: Select this check box to enable ICMP flood defense for the security zone.

- **Threshold** - Specifies a threshold for inbound ICMP packets. If the number of inbound ICMP packets destined to one single

IP address per second exceeds the threshold, system will identify the traffic as an ICMP flood and take the specified action. The value range is 1 to 50000. The default value is 1500.

- **Action -** Specifies an action for ICMP flood attacks. If the default action **Drop** is selected, system will only permit the specified number (threshold) of IMCP packets to pass through during the current and the next second, and also give an alarm. All the excessive packets of the same type will be dropped during this period.

UDP flood: Select this check box to enable UDP flood defense for the security zone.

- **Src threshold -** Specifies a threshold for outbound UDP packets. If the number of outbound UDP packets originating from one single source IP address per second exceeds the threshold, system will identify the traffic as a UDP flood and take the specified action. The value range is 1 to 50000. The default value is 1500.

- **Dst threshold** - Specifies a threshold for inbound UDP packets. If the number of inbound UDP packets destined to one single port of one single destination IP address per second exceeds the threshold, system will identify the traffic as a UDP flood and take the specified action. The value range is 1 to 50000. The default value is 1500.
- **Action** - Specifies an action for UDP flood attacks. If the default action **Drop** is selected, system will only permit the specified number (threshold) of UDP packets to pass through during the current and the next second, and also give an alarm. All the excessive packets of the same type will be dropped during this period.

ARP spoofing: Select this check box to enable ARP spoofing defense for the security zone.

- **Max IP number per MAC** - Specifies whether system will check the IP number per MAC in ARP table. If the parameter is set to 0, system will not check the IP number; if set to a value other than 0, system will check the IP number, and if the IP number per MAC is

larger than the parameter value, system will take the specified action. The value range is 0 to 1024.

- **Reverse query** - Select this check box to enable Reverse query. When system receives an ARP request, it will log the IP address and reply with another ARP request; and then system will check if any packet with a different MAC address will be returned, or if the MAC address of the returned packet is the same as that of the ARP request packet.
- **Gratuitous ARP send rate** - Specifies if system will send gratuitous ARP packet(s). If the parameter is set to 0 (the default value), system will not send any gratuitous ARP packet; if set to a value other than 0, system will send gratuitous ARP packet(s), and the number sent per second is the specified parameter value. The value range is 0 to 10.

SYN flood: Select this check box to enable SYN flood defense for the security zone.

- **Src threshold** - Specifies a threshold for outbound SYN packets (ignoring the

destination IP address and port number). If the number of outbound SYN packets originating from one single source IP address per second exceeds the threshold, system will identify the traffic as a SYN flood. The value range is 0 to 50000. The default value is 1500. The value of 0 indicates the Src threshold is void.

- **Dst threshold** - Specifies a threshold for inbound SYN packets. If the number of inbound SYN packets destined to one single destination IP address per second exceeds the threshold, system will identify the traffic as a SYN flood. The value range is 0 to 50000. The default value is 1500. The value of 0 indicates the Dst threshold is void.
- **Action** - Specifies an action for SYN flood attacks. If the default action **Drop** is selected, system will only permit the specified number (threshold) of SYN packets to pass through during the current and the next second, and also give an alarm. All the excessive packets of the same type will be dropped during this period. Besides if Src threshold and Dst threshold are also configured, system will first

detect if the traffic is a destination SYN flood attack: if so, system will drop the packets and give an alarm, if not, system will continue to detect if the traffic is a source SYN attack; if so, system will drop the packets and give an alarm.

MS-Windows defense

WinNuke attack: Select this check box to enable WinNuke attack defense for the security zone. If any WinNuke attack has been detected, system will drop the packets and give an alarm.

Scan/spoof defense

IP address spoof: Select this check box to enable IP address spoof defense for the security zone. If any IP address spoof attack has been detected, system will drop the packets and give an alarm.

IP address sweep: Select this check box to enable IP address sweep defense for the security zone.

- **Threshold** - Specifies a time threshold for IP address sweep. If over 10 ICMP packets from one single source IP address are sent to

different hosts within the period specified by the threshold, system will identify them as an IP address sweep attack. The value range is 1 to 5000 milliseconds. The default value is 1.

- **Action -** Specifies an action for IP address sweep attacks. If the default action **Drop** is selected, system will only permit 10 IMCP packets originating from one single source IP address while destined to different hosts to pass through during the specified period (threshold), and also give an alarm. All the excessive packets of the same type will be dropped during this period.

Port scan: Select this check box to enable port scan defense for the security zone.

- **Threshold** - Specifies a time threshold for port scan. If over 10 TCP SYN packets are sent to different ports of one single destination address within the period specified by the threshold, system will identify them as a port scan attack. The value range is 1 to 5000 milliseconds. The default value is 1.

- **Action** - Specifies an action for port scan attacks. If the default action **Drop** is selected, system will only permit 10 TCP SYN packets destined to different ports of one single destination address to pass through, and also give an alarm. All the excessive packets of the same type will be dropped during this period.

Denial of service defense

Ping of Death attack: Select this check box to enable Ping of Death attack defense for the security zone. If any Ping of Death attack has been attacked, system will drop the attacking packets, and also give an alarm.

Teardrop attack: Select this check box to enable Teardrop attack defense for the security zone. If any Teardrop attack has been attacked, system will drop the attacking packets, and also give an alarm.

IP fragment: Select this check box to enable IP fragment defense for the security zone.

- **Action** - Specifies an action for IP fragment attacks. The default action is **Drop**.

IP option: Select this check box to enable IP option attack defense for the security zone. system will defend against the following types of IP options: Security, Loose Source Route, Record Route, Stream ID, Strict Source Route and Timestamp.

- **Action** - Specifies an action for IP option attacks. The default action is **Drop**.

Smurf or fraggle attack: Select this check box to enable Smurf or fraggle attack defense for the security zone.

- **Action** - Specifies an action for Smurf or fraggle attacks. The default action is **Drop**.

Land attack: Select this check box to enable Land attack defense for the security zone.

- **Action** - Specifies an action for Land attacks. The default action is **Drop**.

Large ICMP packet: Select this check box to enable large ICMP packet defense for the security zone.

- **Threshold** - Specifies a size threshold for ICMP packets. If the size of any inbound

ICMP packet is larger than the threshold, system will identify it as a large ICMP packet and take the specified action. The value range is 1 to 50000 bytes. The default value is 1024.

- **Action -** Specifies an action for large ICMP packet attacks. The default action is **Drop**.

Proxy

SYN proxy: Select this check box to enable SYN proxy for the security zone. SYN proxy is designed to defend against SYN flood attacks in combination with SYN flood defense. When both SYN flood defense and SYN proxy are enabled, SYN proxy will act on the packets that have already passed detections for SYN flood attacks.

- **Proxy trigger rate -** Specifies a min number for SYN packets that will trigger SYN proxy or SYN-Cookie (if the **Cookie** check box is selected). If the number of inbound SYN packets destined to one single port of one single destination IP address per second exceeds the specified value, system will trigger SYN proxy or SYN-Cookie. The value

range is 1 to 50000. The default value is 1000.

- **Cookie** - Select this check box to enable SYN-Cookie. SYN-Cookie is a stateless SYN proxy mechanism that enables system to enhance its capacity of processing multiple SYN packets. Therefore, you are advised to expand the range between "Proxy trigger rate" and "Max SYN packet rate" appropriately.
- **Max SYN packet rate** - Specifies a max number for SYN packets that are permitted to pass through per second by SYN proxy or SYN-Cookie (if the **Cookie** check box is selected). If the number of inbound SYN packets destined to one single port of one single destination IP address per second exceeds the specified value, system will only permit the specified number of SYN packets to pass through during the current and the next second. All the excessive packets of the same type will be dropped during this period. The value range is 1 to 1500000. The default value is 3000.

- **Timeout** - Specifies a timeout for half-open connections. The half-open connections will be dropped after timeout. The value range is 1 to 180 seconds. The default value is 30.

Protocol anomaly report

TCP option anomaly: Select this check box to enable TCP option anomaly defense for the security zone.

- **Action** - Specifies an action for TCP option anomaly attacks. The default action is **Drop**.

DNS query flood

DNS query flood: Select this check box to enable DNS query flood defense for the security zone.

- **Threshold** - Specifies a threshold for inbound DNS query packets. If the number of inbound DNS query packets destined to one single port of one single IP address per second exceeds the threshold, system will identify the traffic as a DNS query flood and

take the specified action. The value range is 1 to 50000. The default value is 1500.

- **Action** - Specifies an action for DNS query flood attacks. If the default action **Drop** is selected, system will only permit the specified number (threshold) of DNS query packets to pass through during the current and next second, and also give an alarm. All the excessive packets of the same type will be dropped during this period; if **Alarm** is selected, system will give an alarm but still permit the DNS query packets to pass through.

Recursive DNS query flood: Select this check box to enable recursive DNS query flood defense for the security zone.

- **Threshold** - Specifies a threshold for inbound recursive DNS query packets. If the number of inbound recursive DNS query packets destined to one single port of one single IP address per second exceeds the threshold, system will identify the traffic as a recursive DNS query flood and take the specified action. The value range is 0 to

50000. The default value is 1000. The value of 0 indicates no recursive DNS query packet is permitted.

- **Action** - Specifies an action for recursive DNS query flood attacks. If the default action **Drop** is selected, system will only permit the specified number (threshold) of recursive DNS query packets to pass through during the current and next second, and also give an alarm. All the excessive packets of the same type will be dropped during this period; if **Alarm** is selected, system will give an alarm but still permit the recursive DNS query packets to pass through.

Related Topics:

- Land Attack Defense Configuration Example
- Layer 2 IP Address Spoof Defense Configuration Example