



A

- Access Control List (ACL)** ACL's act as a basic method of limiting access to the network. They constitute sequential lists of permit and deny conditions. The lists define the connections permitted to pass through a device, usually a router.
- Analysis Module** This module is active during the Guard Protection mode of operation. When no DDoS attack signs are indicated the Guard directs the diverted Zone traffic to flow through this module. The analysis module lets the Zone traffic flow unobstructed. The module analyzes the flows, allowing the recognition module to sample them.
- Anti-Spoofing** A security feature designed to prevent unauthorized access to a network through the technique known as IP spoofing. See *IP spoofing*.
- ARP Redirect Attack** An attack on a local subnet using the ARP protocol. Begin the definition with a capital letter, and end the definition with a period.

B

- Bandwidth Saturation Flood** A flood of simple HTTP requests for static content targeted towards Web servers; stresses routers, firewalls, IDS, and load balancers. A failure in any of these nodes constitutes network's susceptibility.
- block-unauthenticated** A policy action that directs traffic to an anti-spoofing mechanism that deals with unauthenticated traffic.
- Bypass filter** A filter designed to enable the user to direct desired traffic flows to bypass the Detector's detection mechanisms. Thus, the user can better adopt the Detector to its detection policy.

C

- Client attack** Attacks from legitimate sources, which open half connections causing a server to exhaust.
- Combination attack** Multi-platform DoS attack, which integrates BONK, JOLT, LAND, Nestea, Netear, SynDrop, and Winnuke - all into one attack. It is targeted at any/all network nodes (such as routers, firewalls, web servers, IDS systems).
- Command Line Interface (CLI)** A prompt line interface from which the user performs its operations.

D

- DDoS** See Distributed Denial of Service.
- Denial of Service Attack (DoS)** Forms of computer network communication sabotage via exploitation of computer communication protocols. The purpose of the attack is overwhelming the target with spurious data in order to prevent legitimate connection attempts from succeeding. DoS attacks do not reveal sensitive data to the attacker in contrast to attacks whose purpose is to penetrate the target system. In these kinds of attacks, the skillful attacker tries to choke down networks and servers in vital network junctions. A successful attack may cause considerable revenue and resources loss. Examples of DoS attacks are SYN Flood, Tribal Flood Network (TFN), and ping of death.
- Detector event log** A log file containing the Detector activities, current events, performed actions and the measures it undertook.
- Detection Policy** The Detector policies are the mechanisms that measure a particular traffic flow and take an action as a result of a threshold violation. A policy may, for example, direct the Detector to produce a Dynamic filter that range from merely notifying to activating a remote Guard or Guards to protect the Zone against the DDoS attack.

Detector User community (privilege domain)	The Detector enables access domains to several groups of users (Show, Dynamic, Configuration, and Administrator). These are classified by their authority and hence their ability to perform a scope of operations. The highest and utmost privileged is the Administrator and the least privileged is the Show user level.
Distributed Denial of Service (DDoS) Attack	A Denial of Service attack against a site or server launched from multiple sources. This is sometimes carried out by concealed exploiting servers to function as agents for transmitting the attacks. In many cases, the attacker will place client software on a number of unsuspecting remote computers and then use these computers to launch the attack. A Distributed Denial of Service attack is more effective than a simple Denial of Service attack, as the volume of traffic is considerably higher, and is more difficult to prevent. Examples of DDoS attacks are Syn flood, Smurf attack and Targa attack.
dns_tcp	A policy template that produces a group of policies related to DNS-TCP protocol traffic.
dns_udp	A policy template that produces a group of policies related to DNS-UDP protocol traffic.
DNS Attack	Flood of DNS requests causing a DNS server to saturate.
Dynamic filter	Dynamic filters are created by the Detector as the result of analysis of traffic flow. They are used to detect DDoS attacks and take an action accordingly. This set of filters is continuously adapted to the Zone traffic and the type of the DDoS attack.

F

404 File Not Found Flood	Flood of valid HTTP requests for invalid content or files targeted directly at Web servers; used to validate both security policy and quantify effect on an end user.
Filters	The filters are the mechanism that directs the diverted traffic to the required detection modules. The Detector enables the user to set its preferred filter configurations and thus design a variety of possibilities for customized traffic direction and DDoS attack detection mechanisms.

FIN Flood	Flood of connection resets from an invalid source to a targeted node; consumes network resources of an intended target. A FIN flood is also used to validate correct firewall/router policies.
Flex filter	The Flex filter is a Berkley Packet filter that facilitates the user with extremely flexible filtering capabilities such as filtering according to fields in the IP and TCP headers and filtering according to content bytes. It enables to use complex Boolean expressions. The Flex filter is used to count a specified packet flow.
Fraggle Attack	Sends UDP requests to a directed broadcast address. The forged source address of the request is the target of the attack. The recipients of the directed broadcast request respond to the request and flood the target's network. It is similar to the Smurf attack, but rather than ICMP uses UDP to broadcast address for amplification.
fragments	A policy template that produces a group of policies related to fragmented traffic.
Fragmentation Attack	See IP Fragmentation Attack.

G

Guard	A system designed to protect network elements against DDoS attacks.
GUI	Graphical user interface.

H

http	A policy template that produces a group of policies related to HTTP traffic flowing (by default) through port 80 (or other user-configured ports).
-------------	--

HTTP Connection Flood	Flood of HTTP half-requests targeted at the Web server connection resources. Also used to validate correct firewall policies (that is, limit connections per source). A Web server or OS network-level failure, also seen as connection failures on a client-side, constitutes network's susceptibility.
https	(Hypertext Transfer Protocol over Secure Socket Layer, or HTTP over SSL) is a Web protocol, developed by Netscape, built into browsers, that encrypts and decrypts user page requests as well as the pages that are returned by the Web server. HTTPS is the use of Secure Socket Layer (SSL) as a sub-layer under its regular HTTP application layering. (HTTPS uses port 443 instead of HTTP port 80 in its interactions with the lower layer, TCP/IP.)
<hr/>	
ICMP Redirect Attack	ICMP redirects can cause data overload to the system being targeted.
ICMP Unreachable Attack	The attacker sends ICMP unreachable packets from a spoofed address to a host. This causes all legitimate TCP connections on the host to the spoofed address to be torn down. This causes the TCP session to retry and as more ICMP unreachables are sent, a DoS condition occurs.
Interactive	A Zone detection mode in which the user will activate the dynamic filters in an interactive manner. The Dynamic filters that the policies recommend will appear as recommendations, and the user will specify the action to be taken for each filter.
ip_scan	A policy template that produces a group of policies relating to IP scanning (A situation in which a source IP tries to access many destination IPs on the Zone). See IP scanning.
IP Fragmentation Attack	Flood of valid but heavily fragmented HTTP requests targeted at a Web server; stresses IDS. Used to quantify resilience and scalability of IDS systems.

- IP Scanning** The act of sending systematic queries to hosts in a network in attempt to find hosts (IP addresses) through which an attacker can pass traffic. IP scanning is often used to find vulnerable targets for attack on the Internet.
- IRDP Attack** ICMP Router Discovery Protocol can be spoofed and cause fake routing entries to be entered into a Windows machine. IRDP has no authentication. Upon startup, a system running MS Windows95/98 will always send 3 ICMP Router Solicitation packets to the 224.0.0.2 multicast address. If the machine is NOT configured as a DHCP client, it ignores any Router Advertisements sent back to the host. However, if the Windows machine is configured as a DHCP client, any Router Advertisements sent to the machine will be accepted and processed.

L

- Land Attack** The sent packets have the same Source and destination IP addresses causing a response to loop.
- Looping UDP Ports Attack** The attack uses two UDP services. Chargen (port 19) and echo (port 7), that can be spoofed into sending data to each other.

M

- Maximum Transfer Unit (MTU)** The largest frame size that can be transmitted over the network. Messages longer than the MTU must be divided into smaller frames.

N

- Network Time Protocol (NTP)** A protocol for synchronizing the Detector with a Time Synchronization Server.
- notify** A policy action that notifies the user of a policy threshold violation.

O

- Open/close Attack** The open/close attack opens and closes connections at a high rate to any port serviced by an external service through inetd. The number of connections allowed is hard-coded inside inetd.
- other_protocols** A policy template that produces a group of policies relating to non TCP or UDP protocols.

P

- Pending Dynamic filters** The pending dynamic are dynamic filters the user has not yet defined the action for (accept or ignore). Pending Dynamic filters are created only if the Zone is in interactive detection mode. A group of pending Dynamic filters constitute a recommendation. See Recommendations.
- Ping Flood** Flood of ICMP echo requests; stresses routers, firewalls, load balancers, and Web servers. Poor end-user response time or failure to connect constitutes susceptibility.
- Ping of death** ICMP packets greater than 65536. A ping of death attack can bring down a system.
- Policy Construction Phase** In this phase the Detector, based on the Zone traffic characteristics, produces the detection policies with the aid of the Policy Templates. This phase consists of traffic flowing transparently through the Detector, enabling it to discover which services are used by the Zone.
- Policy Operational Parameters** This is a set of parameters that relate to the policy operations. This set consists of the following: Threshold, Proxy-threshold, Timeout, and Action.
- Policy Templates** The policy templates are a collection of policy constructing guiding rules and the output of each template after concluding the Policy Construction phase is a group of policies. The Policy Templates user-configured parameters are the Minimum Threshold and Maximum Services.

port_scan A policy template that produces a group of policies relating to port scanning (A situation in which a source IP tries to access many ports on the Zone). See Port scanning.

Port Scanning The act of sending systematic queries to hosts in an attempt to find open ports through which an attacker can pass traffic. Port scanning is often used to find vulnerable targets for attack on the Internet.

R

Recommendations Recommendations are a mechanism that enables the user to decide on the activation of the filters the policies launch. They are created when a Zone is configured in interactive mode. The recommendations are a summary of the pending dynamic filters aggregated according to the policies that produced them.

S

Secured Shell (SSH) Management The user may access the Detector via Secured Shell (SSH) to enable controlling the Detector from any network.

Smurf Flood ICMP (Internet Control Message Protocol) ping requests to a directed broadcast address. The forged source address of the request is the target of the attack. The recipients of the directed broadcast ping request respond to the request and flood the target's network.

Snapshots A Detector mechanism used to verify the learning process outcome.

Spoofed attack	A DDoS attack technique that inserts a false sender IP address into an Internet transmission in order to gain unauthorized access to a computer system. To the computer system the request will seem as though it came from a trusted source, although the packet cannot be routed back to the initial source. IP spoofing presents potential for unnecessary network congestion and possible denial of service.
SYN Flood	Flood of connection requests from an invalid source to a targeted node; consumes network resources of an intended target. Used also to validate correct firewall/router policies.

T

Targa Attack	Floods of invalid ICMP-, UDP- and TCP- packets.
tcp_connections	A policy template that produces a group of policies related to TCP connection characteristics.
TCP_NO_PROXY policy templates	A template designed for a Zone for which no proxy is to be used. This template may be used if the Zone is moderated according to IP addresses such as an Internet Relay Chat (IRC) server-type Zone.
tcp_not_auth	A policy template that produces a group of policies related to TCP connections that haven't been authenticated by the Guard's anti-spoofing mechanisms.
tcp_outgoing	This policy template produces sets of policies related to TCP connections initiated by the Zone.
tcp_ratio	This policy template produces sets of policies related to ratios between different types of TCP packets (e.g. SYN packets versus FIN/RST packets).
tcp_services	A policy template that produces a group of policies related to TCP services on ports other than HTTP-related (such as ports 80, 8080, etc.).
TCP flood	When TCP communicates, each TCP allocates some resources to each connection. By repeatedly establishing a TCP connection and then abandoning it, a malicious host can tie up significant resources on a server.

TCP Segmentation	Flood of heavily segmented TCP packets targeted at a Web server or application server. This attack stresses both IDS and the target machine's TCP stack.
Teardrop Attack	Sends overlapping IP fragments.
Threshold Tuning Phase	This is the stage in which the Guard further analyses the Zone traffic and defines threshold for the policies constructed in the Policy Construction phase. In this phase, the policies are tuned to fit the Zone services traffic rates.
to-user-filters	An action (configured for a policy or a dynamic filter) that directs traffic to the user filters.

U

UDP Flood Attack	Flood of large numbers of raw UDP (User Datagram Protocol) packets targeted at routers, firewalls, load balancers, and IDS systems. The attack ties up network resources.
udp_services	A template that produces a group of policies related to UDP services.
UDP Reflectors Attack	All Web servers, DNS servers, and routers are reflectors, since they will return SYN acks or RSTs in response to SYN or other TCP packets; query replies in response to query requests; or ICMP Time Exceeded or Host Unreachable in response to particular IP packets. By spoofing IP addresses from slaves—a massive DDoS attack can be carried out.
URL attacks	URL attacks attempt to overload an http server via various methods: http bombing; continuous requests for the same homepage or large web page; requesting the page with REFRESH so as to bypass any proxy server. Many of these attacks are not zombie attacks but rather human executed, by hundreds simultaneously.

W

WBM	See Web Based Management.
Web Based Management	A GUI over HTTP Detector interface that enables the user to manage the Detector detection and Zones (excluding Detector configuration procedures) via the web using a browser.

Z

Zombie	A device that acts as an unaware participant in a distributed Denial of Service (DDoS) attack.
Zombie attack	A zombie attack is a type of attack that uses unaware participant machines to launch a DDoS attack. The attacker first spreads a Trojan to unsuspecting users, that are not the final target, and may later instruct this Trojan to perform “legitimate” connections to the Zone.
Zone	The Detector-detected network element. Also, a Detector file with all data relating to the detected Zone (configurations, policies, filters, etc.).

