captus NETWORKS™

The Leader in Denial of Service Prevention

CaptIO™ Policy-Based Security Device

The CaptIO Policy-Based Security Device automatically detects, identifies, validates, and stops Denial of Service attacks in seconds.

- **Automatic, Immediate DoS Mitigation**
- **Ingress & Egress Traffic Protection**
- **Prevention of Firewall Overload and IDS "False Positives"**
- **Ensurance of Server Availability**
- **Detection and Identification of Network Traffic Anomalies**

Denial of Service Prevention

In today's e-business economy, network security is a mission-critical function. A secure, highly-available network is critical to protecting e-commerce brands. Recent malicious Denial of Service (DoS) attacks on some of the Internet's largest Web sites underscore the need for comprehensive security solutions.

Presently, network administrators attempt to decrease the impact of DoS attacks with a patchwork of equipment. They may install firewalls, IDS systems, and configure their IP routers to drop packets of a given type or particular source and destination address. Unfortunately, these solutions are not well integrated, reduce network performance, and fail to stop DoS attacks prior to network impact.

The key is to stop a DoS or distributed DoS (DDoS) attack before it slows down or shuts down your network. Reactive solutions let your network control you. Preventive solutions allow you to be in control of your network.

The CaptIO Network Security Device

The CaptIO uses anomaly-based network security policies to detect, identify, and stop Denial of Service attacks within seconds of detection. Patent-pending technologies provide the capability to distinguish between legitimate spikes in network traffic and malicious DoS attacks. This allows you to surgically shut down an attack without disrupting legitimate traffic to your business.

CaptIO Architecture

The CaptIO system architecture is comprised of major security components that provide ingress and egress traffic management, comprehensive traffic profiling, and policy-based intrusion detection and response.

Redefining the DMZ

Ingress and Egress Traffic Management

Because there is no "trusted" side of the network with the CaptIO, unique policies can be applied to both ingress and egress traffic. This means that all traffic passing through the device, whether inbound "ingress" or outbound "egress", is tracked for security policy violations. Each interface of a CaptIO can be configured as a discrete network having its own policies.

Ingress and egress traffic management on the CaptIO includes source filtering and reciprocal firewall technology. Source filtering helps insure that private IP addresses are not allowed to propagate across the public Internet. Reciprocal firewall technology enforces security policies regardless of traffic direction. The CaptIO only passes traffic that has been explicitly defined by the user and immediately denies any other network traffic. This network model eliminates the secondary DoS threat of worm/viruses, such as in Code Red and Nimda.

Patent-Pending Technologies

The core security component of the CaptIO device is the policy-based intrusion detection and response system. Two patent-pending technologies specifically address the ability of the device to automatically detect, identify, and validate DoS attacks.

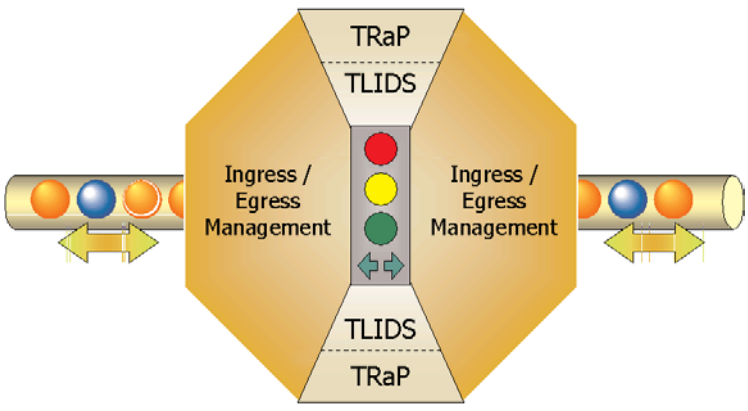
TRaP Technology™

Traffic Restriction and Profiling (TRaP) Technology allows the CaptIO to track and profile all traffic flows through the device. Network traffic is tracked by any combination of source and destination IP addresses, source and destination ports, and protocol. Flows can be tracked separately or as an aggregate of matching traffic.

TLIDS™ Technology

The CaptIO device also utilizes an innovative Traffic Limiting Intrusion Detection System (TLIDS), which monitors network traffic to identify and validate a DoS attack. TLIDS policies are determined by the network administrator and are specific to the network being protected.

The CaptIO system architecture is comprised of major security components that provide ingress and egress traffic management, comprehensive traffic profiling, and policy-based intrusion detection and response.



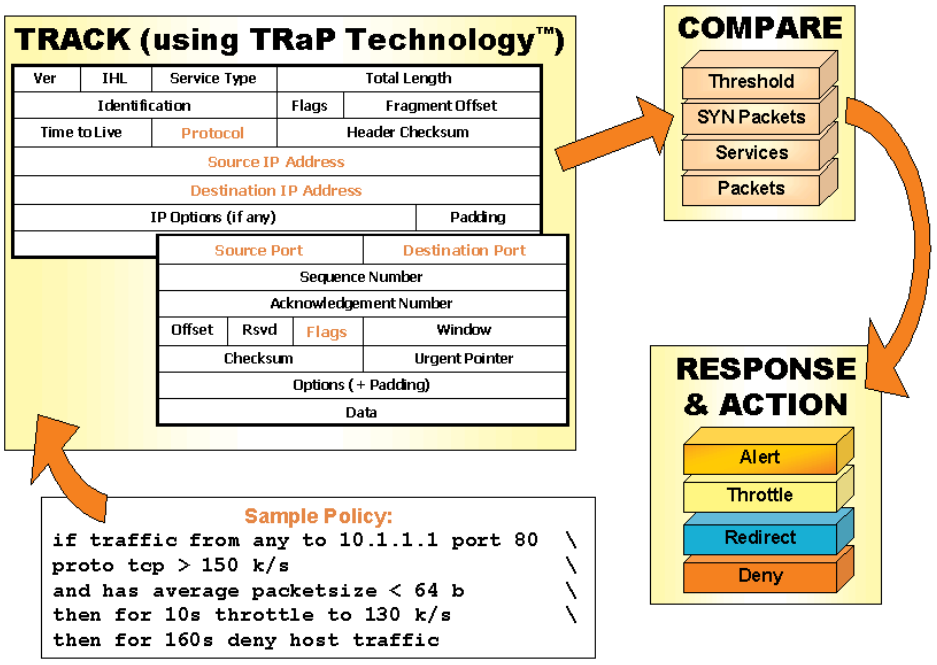
DoS Prevention Technology

Inside TLIDS Technology

TLIDS policies characterize normal network traffic patterns and the CaptIO monitors for anomalies in traffic. When network traffic violates a TLIDS policy, the CaptIO device dynamically takes action to notify, throttle, redirect, or deny traffic between the two specific offending hosts. This capability allows the CaptIO to surgically stop the attack while allowing legitimate traffic to continue through. If an attack is detected, the policies determine what action is automatically taken by the CaptIO to mitigate any damages from the attack. When an attack subsides, the filters invoked by the TLIDS policies are automatically removed and network traffic continues to be monitored for anomalies.

Policy-based Security

Policies can be set against all IP protocol types and are independently configured for each CaptIO interface. Policy thresholds can be based on the total data flow, packet flow, average packet size, TCP SYN traffic, and service scans. Packet and data buckets allow for protocols that are naturally bursty, such as HTTP, to occasionally reach high traffic rates without triggering a policy action.



In addition to stopping DDoS attacks, the CaptIO can also stop port scans. A potential attacker uses a port scan to see what services on a host or hosts on a network are available. This attacker can then use this information to launch a DDoS or other attack.

The sample policy shown above is set to track HTTP traffic, inspecting for anomalies such as that generated by a malicious flood of traffic to a Web server. In this example, the CaptIO will monitor all HTTP traffic passing through the device.

Layered Security

Today's Layered Approach to Securing E-business

Yesterday's security framework, otherwise known as the DMZ, consisted of a firewall and an IDS system. Today's security framework includes a Denial of Service component.

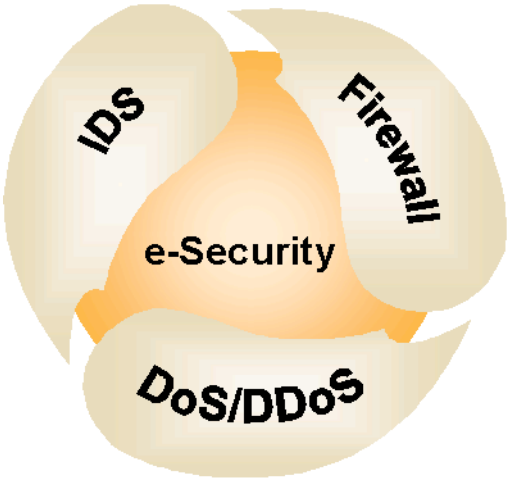
The firewall, in its purest form, is a secure gateway that connects a company's network with the Internet. It protects the company's network from unauthorized access. Firewalls manage traffic flow and can block data that does not meet the standards of the company's security policy.

An IDS is primarily an advisory system. IDS systems endeavor to identify and record attempts to compromise the security of a network.

IDS's, whether host- or network-based, use databases of "attack scenarios", drawing from previous experience, to indicate incoming intrusion attempts.

Because companies are facing new challenges to protect infrastructure and information assets from cyber attacks, a new component has been added to the security suite, the Captus Networks DoS security device. The CaptIO device is able to distinguish good from bad traffic, and provides ingress/egress filtering. By offloading packet filtering and DoS mitigation to a CaptIO, firewall, router, and IDS resources can be more effectively utilized, enhancing overall network performance.

This suite of security technologies allows you to implement state-of-the-art prevention, detection, response, and forensic procedures to mitigate ongoing risk in a digital economy.

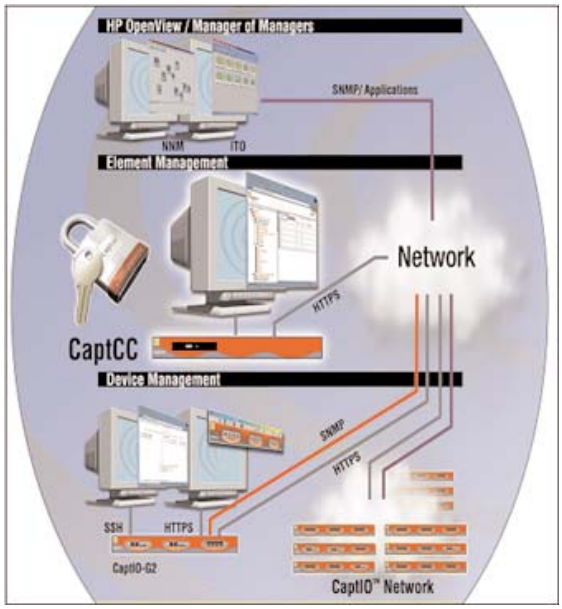


Companies are facing new challenges to protect infrastructure and information assets. Today's comprehensive e-security suite includes an intrusion detection system, a firewall, and a Denial of Service prevention component.

Attack Name	Type	Stopped by CaptIO?
PING flood	ICMP flood	Yes
UDP flood	UDP flood	Yes
SYN flood	TCP flood	Yes
Trin00	UDP flood	Yes
smurf	ICMP echo/reply (broadcast)	Yes
fraggle	UDP echo (broadcast)	Yes
TFN	UDP, SYN, ICMP floods	Yes
TFN2K	UDP, SYN, ICMP floods	Yes
stacheldraht	UDP, SYN, ICMP floods	Yes
Ping of Death	ICMP oversized packet	Yes
nmap	Port scanning	Yes
Code Red	Buffer overflow attack	Yes

Some "named" attacks that can be stopped by the CaptIO device are listed above. The CaptIO detects traffic anomalies, takes action based on policies, and stops any network attack, whether it is well-known or has just been introduced.

Management and Support



Captus Networks provides multi-level FCAPS management solutions for the device, element, and network level.

- **Network Management / Manager of Managers**
  - Support for V1/V2 SNMP
  - SNMP Gets and Traps on CaptIO
- **Element Management**
  - CaptCC™ Centralized Management for up to 25 CaptIO Devices
  - New Windows-based Report Viewer
- **Device Management**
  - CaptIO Web Management Interface allows secure, remote access using HTTPS
  - CLI access via SSH

Comprehensive Management

There are three levels of management solutions for the CaptIO. First, any SNMP-based "Manager of Managers" platform, like HP OpenView®, can be used to remotely monitor CaptIO devices through the use of SNMP gets and traps. Second, the CaptCC Global Administrator serves as an Element Management System for CaptIO devices. Finally, the CaptIO includes both a secure Command Line Interface (CLI) with terminal access using SSH, and a Web Management Interface (WMI) that can be launched via any standard Web browser for configuration and management. In addition, the CaptIO has the added feature of supporting Network Time Protocol (NTP) as server/client for the network.

Exceptional Support

Captus provides technical and product support to its customers through a 24x7 call center service. Captus Networks includes call-center support, field replacement, and minor software updates as part of the first 90 days warranty. Additional services—including priority access, extended support, and database privileges—can be added/extended on a yearly basis as part of the Premium Support offering.

Corporate Headquarters
Captus Networks
1680 Tide Court, Suite B
Woodland, CA 95776
Toll Free: 877-9CAPTUS
(877-922-7887)
Phone: (530) 406-3500
Fax: (530) 406-3406
e-mail: info@captusnetworks.com
web: www.captusnetworks.com

CaptIO Specifications

Detected Attack Types

Floods TCP (SYN, ACK), ICMP, UDP, IGMP multicast

Other ICMP oversized packet (Ping of Death), Invalid IP packet types, Invalid IP fragmentation, port scanning

Policy Enforcement

Actions Alert, Throttle, Reroute, Deny non-conforming traffic

Notification

Types SNMP (V1, V2) gets & traps, local syslog, remote syslog

Management

Interface Encrypted SSH (V2) CLI, SSL Web Browser, NTP client/server

Connectivity

Ethernet Interfaces

10Base-T/100Base-TX: Half/Full Duplex Autosense, RJ45 connectors

1000Base-SX: Multi-mode Fiber (62.5-50µm), SC duplex connector

Management

One 10Base-T/100Base-TX Autosense, RJ45 connector

One RS-232 Serial, DB9 connector

Local Console: SVGA (DB15) & Keyboard (PS/2-style)

Power & Environmental Requirements

Input 100-240V AC, 50/60 Hz, 2A

Temperature 40-105 °F (5-40 °C)

Relative Humidity 5-90% non-condensing

Altitude 0-9843 ft. (3000 m)

Dimensions and Weight

Height 1.75 in. (1RU)

Width 17.00 in.

Depth 22.00 in.

Weight 19 lbs.

Certifications

Safety CSA, UL, CE

EMI CFR 47 Part 15, Subpart B, Class A (FCC)

Ordering Options

Model	Number of Interfaces		
	Fast Ethernet (10/100BASE-TX)	Gigabit Ethernet (1000BASE-SX)	Management (10/100BASE-TX)
CaptIO (0x4)	4	-	1
CaptIO-G (1x4)	4	1	1
CaptIO-G2 (2x4)	4	2	1

Ordering Information

The CaptIO, CaptIO-G™, and CaptIO-G2™ support various configurations of Gigabit Ethernet and Fast Ethernet interfaces, depending on network connectivity requirements. Each network interface can be individually configured with unique security policies. All CaptIO devices are one rack-unit high (1.75 inches) and mount in a standard 19" equipment rack.

A CaptIO device can be configured as a hot standby to an active device in high availability (HA) network environments. Using unique fault-management software and redundant device synchronization, the CaptIO HA solution delivers seamless fail-over for mission-critical network security.