INTEL NETWORKING CASE STUDY

Captus Networks Helps Prevent Denial of Service Attacks with Intel® PRO/1000 Network Adapters for Multi-gigabit Scalability

Network Security Company Chooses Intel® PRO/1000 Fiber Server Adapters for Innovative Policy-based Prevention of Denial of Service Attacks

CASE HIGHLIGHTS

Profiled Organization: Captus Networks Corporation

Challenge: Stop Denial of Service (DoS) attacks without adding latency or CPU utilization, using an innovative security technology that uses anomaly-based detection and prevention.

Solution: The Intel® PRO/1000 Fiber Server Adapter, which provides Gigabit throughput over fiber optic cabling with low CPU overhead, allows the Captus Networks CaptIO* device to rapidly track and profile network traffic flows, applying policies to prevent DoS attacks.

Benefits: The CaptIO network security device introduces minimum latency to the customer's network because the Intel PRO/1000 Fiber Server Adapter processes data at near-Gigabit speeds. CaptIO is thus able to stop DoS attacks in seconds.

SUMMARY

As businesses grow increasingly dependent on the Internet, they grow more vulnerable to hackers. In several high profile cases, hackers devised cunning ways to send tidal waves of phony traffic to targeted Web sites, drowning company Web servers in sham requests. Such Denial of Service (DoS) attacks cripple a Web site and destroy its ability to respond to customers. And in e-Business, 24x7 availability is everything. When customers can't get online, they take their business elsewhere, as the competition is just a click away.

Network security startup Captus Networks has an answer. Its CaptIO network security device provides immediate and automatic protection from DoS attacks through inline policy-based monitoring of network traffic. Because it sits inline with network traffic rather than offline, everything about CaptIO has to be fast. Captus Networks selected the Intel® PRO/1000 Fiber Server Adapter to integrate Gigabit speeds over fiber optic cabling into its solution.

CHALLENGE: Move Data at Gigabit Speeds

Unlike passive network monitoring solutions, which sit offline and merely provide notification of an attack, the CaptIO is a proactive, inline solution that stops DoS (and Distributed Denial of Service – DDoS) attacks before they damage business-critical networks. The CaptIO uses Captus Networks' Traffic Limiting Intrusion Detection System (TLIDS*), which identifies a DoS attack and automatically implements policy-based rules based on specific information in the header or a packet. This information can be source and destination addresses, port numbers, or protocols. This allows CaptIO to surgically stop the attack while allowing legitimate traffic to get through.

If the traffic surge is determined to be an attack, the CaptIO can be configured to alarm, throttle, redirect, or stop the traffic flow automatically within seconds, mitigating any damages. The ability to distinguish between legitimate surges in traffic versus real DoS attacks is a huge competitive advantage for Captus Networks.

"We looked at half a dozen Gigabit NICs. The Intel® PRO/1000 Fiber Server Adapter had the best throughput with the lowest overhead to the CPU."

Michael Nadler,
Chief Technology Architect,
Captus Networks

"When customers hear that our device sits inline, they're immediately concerned about adding latency to the network," explains Michael Nadler, Chief Technology Architect at Captus Networks. "We need a network adapter that provides the highest possible throughput, allowing customers to take full advantage of their Gigabit networks."

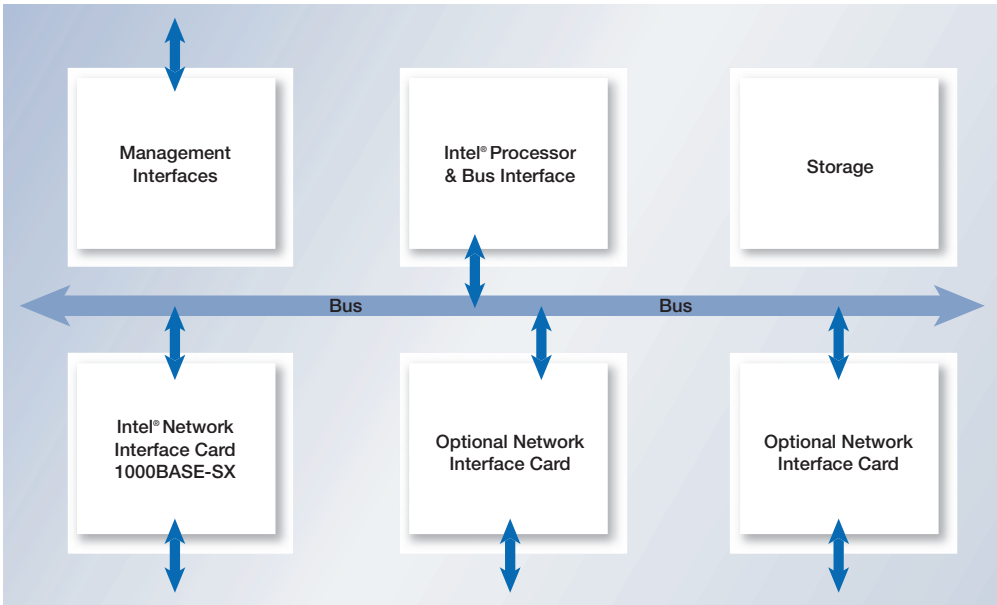
PROCESS: Faster Performance with the Intel® PRO/1000 Fiber Server Adapter

The original CaptIO device was a 12-port 100 BaseT (Fast Ethernet) switch that could dynamically adjust the firewall to significantly reduce the risk of DoS attacks. As Gigabit Ethernet heated up, Captus Networks set out to design a Gigabit device and needed a high-speed network interface card (NIC) to move traffic with only minimal latency.

"We looked at half a dozen Gigabit NICs, and Intel's offering was far and away the best," Nadler says. "The Intel PRO/1000 Fiber Server Adapter had the best throughput with the lowest overhead to the CPU."

SOLUTION: Immediate and Automatic Attack Mitigation

The CaptIO device sits right in the line of fire and examines every bit of traffic traveling across a company's network – originating inside and outside the company. If a retailer launches a successful ad campaign, Web traffic will surge. The CaptIO device needs to determine whether the surge is legitimate or a dangerous Denial of Service attack. When it sees the surge, CaptIO implements a throttle rule that slows all traffic for a few seconds and requests an acknowledgement, using the basic rules of TCP/IP. Legitimate traffic complies with this request, but hacker traffic will not. CaptIO can thus single out bogus DoS traffic within seconds and shut it down, without impacting legitimate traffic.



"The Intel® PRO/1000 Fiber Server Adapter is critical to our ability to deliver sub-second DoS attack prevention, thanks to its super high throughput. We have to have a fast NIC to deliver a high-performance solution to our customers."

Michael Nadler,
Chief Technology Architect,
Captus Networks

What's more, the CaptIO does not adhere to the "trusted" versus "untrusted" network model and effectively redefines the DMZ. Its policies protect companies from inbound floods of traffic as well as from outbound attacks launched from infected "zombie" computers in their own networks.

Captus Networks depends on the Intel PRO/1000 Fiber Server Adapter to deliver a high-performing, Gigabit Ethernet solution over fiber optic cabling. Wide driver support, Intel® SingleDriver™ technology, and the Intel® PROSet Utility also make this adapter one of the easiest and most versatile Gigabit connections available for fiber optic networks. Included software makes it possible to team multiple Intel® PRO Server Adapters together in a server, reducing server bottlenecks and increasing availability by managing fault-tolerant connections and intelligently balancing adapter traffic across multiple NICs.

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.

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.

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 policies characterize normal network traffic patterns and the CaptIO monitors for anomalies in the traffic.

Captus Networks uses the Intel® 21554 PCI-PCI Bridge Chip to extend the PCI bus from the motherboard across the three adapter cards in each system (Captus achieves 12 ports on its backplane by using three NICs with four ports each). “At the time we were designing our system, Intel was the only company that had such a chip, and it did exactly what we needed,” Nadler says.

Captus Networks uses the CaptIO to guard its own network. “Hackers know us as the DoS killers, so they’re after us all the time,” Nadler says. “We get attacked three or four times a week. CaptIO catches them all and refuses them. Our administrator sees the report logs, but no one even knows when they’re happening. Our business proceeds without any interruption.”

BENEFIT: Intel® PRO Server Adapter Critical to High Performance

Since introducing CaptIO in 2000, Captus Networks has become the leader in protecting e-Business from the impact of DoS and Distributed DoS attacks. “Tremendous performance is the key to our success with CaptIO’s inline design,” Nadler says. “The Intel PRO/1000 Fiber Server Adapter is critical to our ability to deliver sub-second DoS attack prevention, thanks to its super high throughput. We have to have a fast NIC to deliver a high-performance solution to our customers.”

“Hackers are here to stay,” Nadler concludes. “But with CaptIO on your network, they’ll give up within minutes and take their attacks somewhere else. Thanks to the Intel PRO/1000 Fiber Server Adapter, we’re every bit as fast as they are.”

0502/HB/LM/PDF Please Recycle. NP2068