Server-Based Security

Total Security with Distributed Hardware Firewalls

Introduction

With several high profile security breaches in the news over the past year alone, there is now broad awareness among security and IT professionals of the constant threat to their enterprise and cloud data centers. It is safe to assume that all network attached resources are under constant attack from known and unknown assailants that target business-critical applications and sensitive data. The most notable breaches succeeded in bypassing data center edge security, and gained access to the largely unprotected internal networks. Such attacks focus the spotlight on network server security, where a severe lack of protective measures can explain, at least in part, the ease in which data is compromised once the exterior edge is breached.

The Network Security Imperative

There are a number of IT market dynamics that support the case for server-based security in conjunction with or instead of using dedicated and expensive security devices at the edge. These dynamics include scalability concerns with the shift to cloud computing, virtualized network security, network traffic growth and the use of data analytics. This trend is supported by advances in software-defined networking and the availability of intelligent/automated security remediation.

Enterprises are increasingly dependent on network accessible resources, and are therefore actively collecting, processing, and analyzing network data for cyber security investigations. This activity will become increasingly more difficult as network bandwidth in the data center increases from 10Gbps, to 40Gbs, 100Gbps and beyond. In this context, server-based network security capabilities can play a critical role for extremely high-speed packet capture/processing, time stamping, and routing packet information to analytics engines.

Most organizations are using public and private cloud services and are planning to expand such usage over time. As IT shifts in this direction, cloud service providers will need the ability to customize network security/monitoring controls for individual organizations and various classes of workloads. It will thus be optimal to leverage server-based network security solutions not only to support such requirements but also to provide high-speed network I/O, which allows cloud providers to meet their SLAs.

As software-defined networking (SDN) helps abstract the network control plane, network security controls will become virtual, dynamic, and automated. Whether the specific network architecture being deployed is SDN based or not, server network security solutions can adopt SDN mechanisms through centralized control of distributed packet capture and packet processing capabilities for network/security monitoring. Furthermore, servers can act as policy enforcement points for different applications or workloads.

Increasing network bandwidth and traffic for a multitude of applications have also resulted in greater malware volume, sophistication, and variety. To address security problems on this scale, enterprise and cloud organizations have to automate network security remediation activities as they receive new threat intelligence. Intelligent network I/O platforms will help enable this model. When intelligence feeds uncover a potential network threat vector, server network security components can adjust controls at an extremely granular level to protect virtual workloads regardless of their current location.

Server-based Security Requirements

Server-based network security can be used to protect business applications and sensitive data against a variety of internal and external threats by enabling network monitoring to capture, process, and analyze network traffic. At a top-level, there are two types of requirements that drive the need for server-based network security.

Enterprise data center managers require greater network visibility to optimize application and network performance, ensure corporate compliance, detect security threats and prevent data loss. In order to do this, they require more network taps with 10/40 Gbps line rate packet capture to provide detailed visibility into network conditions without the exorbitant expense of specialized appliances that could also compromise performance.

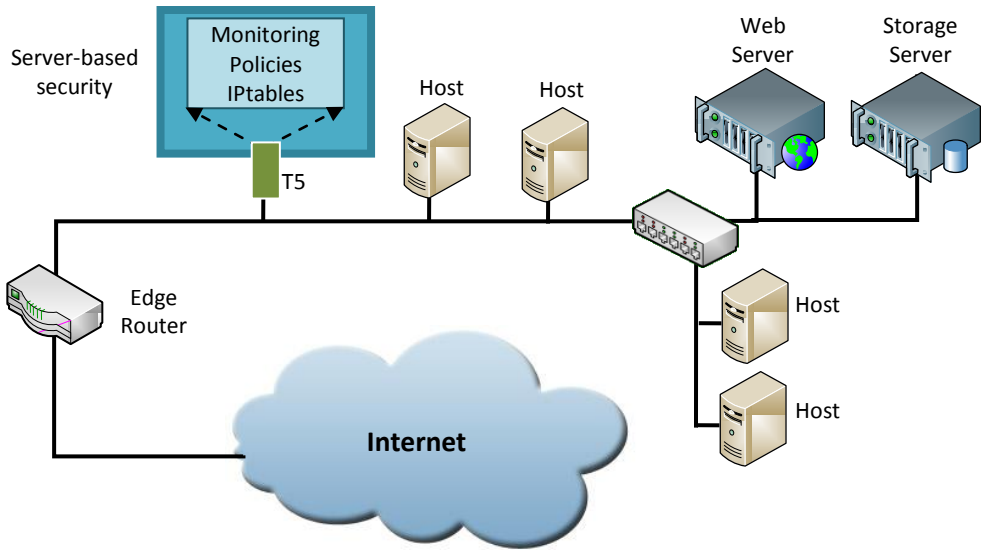

Figure 1 – Server-based security

Cloud service providers who must deliver application and tenant-level isolation and security, network performance and uptime; require network monitoring and security tools perhaps even more crucially than enterprise organizations. The escalating need for capture, processing, and analysis of network data means there is going to be robust growth of server facilities for performing these operations.

The increasing use of server virtualization and cloud computing platforms also introduces the need for blocking attacks from within the servers before they affect the OS or impact the

applications running on the server. There is also great need for filtering, blocking, rate limiting and issuing alerts on bad traffic at the source of traffic. Such functionality needs to be integrated with customers' policy management tools and rule sets, plus third-party threat intelligence data services.

In addition to detecting bad traffic at either end (source or destination), it is required that server network-based security absorbs attacks longer without degradation of good traffic, and that it scales as servers are added, while permitting increased headroom and responsiveness in the face of Denial of Service (DoS) attacks. Denial of service (DoS) or Distributed Denial of Service (DDoS) attacks represent a growing trend in network security, and succeed by making a machine, service, or network resource unavailable to its intended users by exhausting network resources. One common method of attack involves saturating the target machine with external communication requests, so much so that it cannot respond to legitimate traffic or responds so slowly that it is rendered essentially unavailable.

T5 Solution Overview

At the core of Chelsio Terminator ASIC's security capabilities is the Packet Filtering engine. The Terminator Packet Filtering capability is a built-in feature of Chelsio T5-based adapters and blocks attacks before they penetrate the OS or impact the application running on the server. It filters, blocks, rate limits and alerts on malicious traffic and includes APIs that enable integration with customers' policy management tools and SDN-based network security services. Hardware-level integration with FPGAs that implement application-level security capabilities is also supported.

Because Terminator Packet Filtering works to offload the host filtering tables in hardware, it is highly efficient and has minimal performance load for normal traffic. For example, Chelsio's T5 based T520-LL-CR adapter delivers line rate performance at minimum packet size across 2x10Gbps ports, in receive as well as in the demanding bidirectional RFC2544 tests.

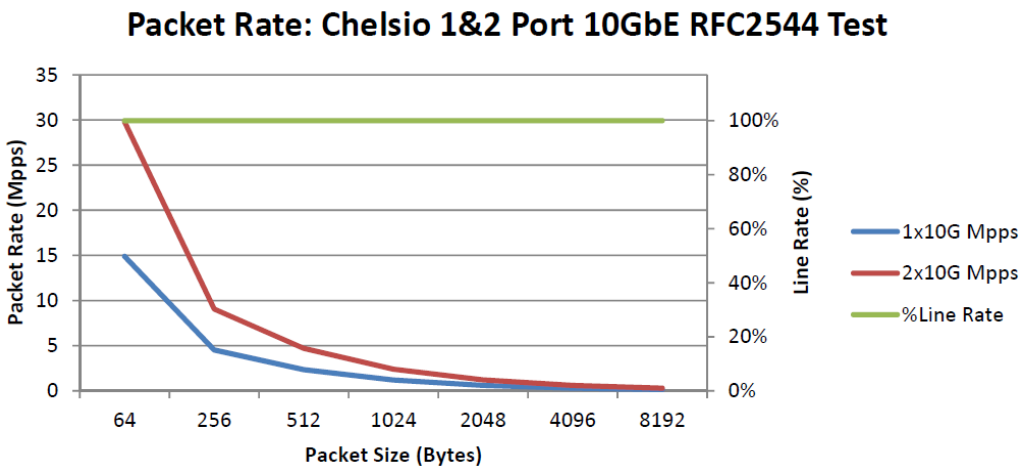

Figure 2 – Packet Rate vs. I/O size

The Packet Filtering feature also enables traffic monitoring through *WD-Sniffer* and *WD-Trace* capabilities. These utilities allow bi-directional packet tracing, packet sniffing and packet filtering at line rates up to 40 Gbps by bypassing the host OS kernel and I/O stack and going directly to user space, where packet capture applications like *tcpdump*, *wireshark*, *snort*, and *suricata* can be used. Traced packets carry hardware packet timestamps with a high 1.5nsec resolution. Additionally, *WD-Trace* allows concurrent normal networking operation, i.e. trace traffic travels on a separate path through the NIC, and goes to a dedicated DMA queue that's handled by a dedicated core without disrupting the regular ingress traffic.

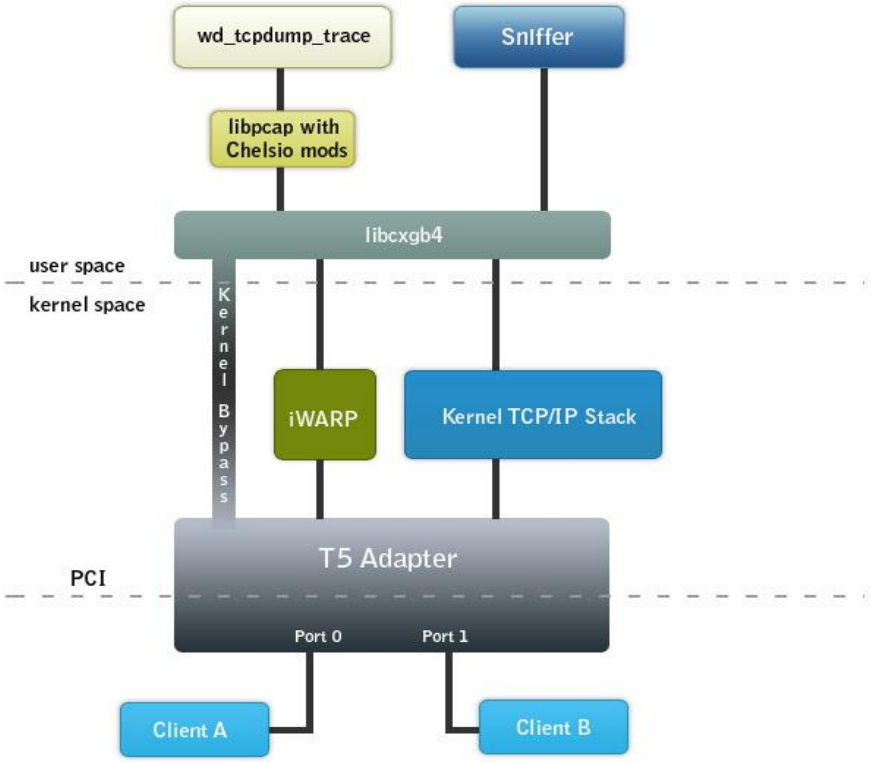

Figure 3 – Terminator traffic monitoring

Use Cases

The Terminator Packet Filtering capability enables a range of use cases for flexible, high-performance server-based security and traffic monitoring, including integration with SDN controllers for automated control on traffic filtering and management, integration with Linux *iptable* firewall capability for support of host-based security policies and integration with virtualization management platforms such as VMware vSphere and Microsoft Hyper-V for v-switch offload, ACL and security features.

Data center security teams can make use of software-defined networking (SDN) as the means for automating the detection and mitigation of a variety of attacks seen today. Through integration within an SDN framework, Terminator Packet Filtering can aid SDN controllers in traffic monitoring, analysis and management through acting as data path software-defined

monitoring (SDM) and enforcement (SDE) devices. For example, SDN-enabled Terminator 10/40 GbE adapters can utilize Packet Filtering to act as a first line of defense in the identification of particular patterns and thresholds of packet volume from a single source or multiple sources within a given timeframe. These adapters can then drop the traffic or redirect it. Conversely, the adapters can act as last line of defense against external attacks.

Terminator Packet Filtering also supports integration with Linux iptables firewall capability. Such support provides a way to configure the Terminator Packet Filtering firewall automatically such that a subset of iptables rules will be enforced by the Chelsio Terminator adapters, which are capable of significantly higher processing rates than software stacks. Such support can also allow administrators to place limits on which flows are allowed through the Packet Filtering capability. Iptables integration provides a very low overhead packet discard path which allows the Packet Filtering feature to excel at server defense when under DDoS attack, while continuing to efficiently handle "good" traffic.

Terminator Packet Filtering also supports integration with server and network virtualization tools, such as VMware vSphere Network I/O Control (NIOC) suite, to ensure that network I/O resources are always available for virtualized business-critical applications. Packet Filtering monitor capability enables NIOC to monitor server networking using a low-overhead means even for high-performance 10/40 GbE connections. On seeing congestion, Packet Filtering can shift resources to highest-priority applications as defined by NIOC-based rules.

Conclusion

With line rate performance and hardware based packet filtering, time-stamping, tracing and sniffing capabilities, Chelsio's T5 adapter-based Packet Filtering capability meets the requirements for providing server-based security for advanced threats and DDoS attacks. It detects bad traffic at the source, or blocks it at the destination, absorbs attacks longer without degradation of good traffic and scales as servers are added to the environment. It also increases headroom and responsiveness in the face of sustained attacks.

Related Links

The Chelsio Terminator 5 ASIC
Packet Rate Performance Report
High Frequency Trading Report
STAC-N1 Benchmark For TCP Traffic
STAC-N1 Benchmark For UDP Traffic