SOLUTION BRIEF

Communications Service Providers
Network Security

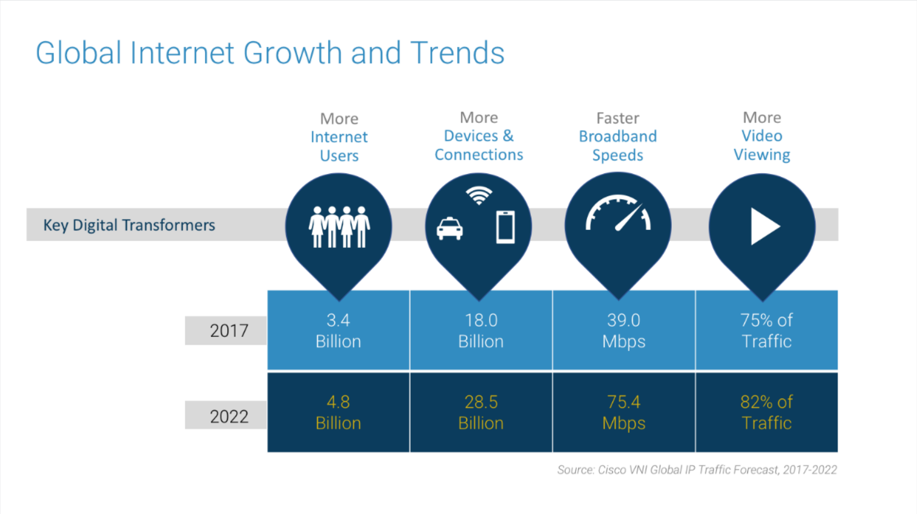
NoviFlow CyberMapper Scales Network Security to Terabit Speed

NoviFlow CyberMapper provides security load balancing and mitigation services for high-throughput networks. The NoviFlow solution utilizes Barefoot Networks Tofino™-based switches rated for up to 6.5 terabit-per-second performance.

Internet data traffic levels are growing significantly, which means communications service providers (CommSPs), data centers, enterprises, government agencies, and other network operators must scale their cybersecurity infrastructure to help keep their networks safe. Load balancing is a proven tool for improving web server performance, and NoviFlow has revolutionized this technology for cybersecurity applications, allowing network operators to scale cyber defenses cost effectively to meet the needs of higher throughput network services.

Ramping Up Cybersecurity to Meet Growing Data Volumes

More devices, more users, more video, and more new applications. Network operators are in a race to expand network capacity to keep up with quickly increasing volumes of network data. Figure 1 shows just some of the contributors to the growth in data consumption according to the Cisco Visual Network Index.



Global Internet Growth and Trends

Key Digital Transformers	More Internet Users	More Devices & Connections	Faster Broadband Speeds	More Video Viewing
2017	3.4 Billion	18.0 Billion	39.0 Mbps	75% of Traffic
2022	4.8 Billion	28.5 Billion	75.4 Mbps	82% of Traffic

Source: Cisco VNI Global IP Traffic Forecast, 2017-2022

Figure 1. Internet data growth trends from the Cisco Visual Network Index[1]

One significant trend is the replacement of fixed-function appliances with more agile and scalable virtualized or containerized network elements. Virtualized services both lower network costs and have advanced lifecycle management for managing data services features, performance, and lifecycle to meet consumer demand. Network operators are also adopting software defined networking (SDN) to add centralized packet forwarding intelligence that improves throughput by making better routing decisions and reducing congestion.

But network operators must ramp up their cybersecurity performance to keep pace with the increased data flows. Protecting data, infrastructure, and personal identities from hacker attacks, malware, cyber terrorism, and other threats while maintaining performance is a new challenge to the performance of these networks. Deep packet inspection (DPI)-based security appliances or virtual network functions (VNFs) can be scaled by upgrading their hardware or by implementing multiple VNF instances. With multiple DPI services, a specialized load balancer must be used to direct the data flow to various server instances in a way that scales with data flows without impacting network performance.

Intel® Network Builders ecosystem partner NoviFlow has developed an SDN-based load balancer to help protect even the highest performance networks. The NoviFlow CyberMapper solution has the performance and specialized features needed for high throughput cybersecurity protection for the scale out of networks.

CyberMapper Utilizes Programmable Switches for High-Speed Cybersecurity

NoviFlow is a networking software company specializing in developing SDN solutions for high-performance networks. The company first developed NoviWare, an SDN-enabled network operating system (NOS) for next-generation programmable white-box switches. This expertise is the basis for the CyberMapper, which is a high-performance security network middleware that creates a security perimeter by providing security redirect services to send data to clusters of DPI-based cybersecurity applications such as firewalls, unified threat management, and other virtualized or appliance-based security functions.

CyberMapper also can provide high-performance security mitigation by identifying known-safe (whitelist) or known-hostile (blacklist) traffic before the packets enter the perimeter. The load balancer drops blacklist traffic and other data that doesn't need further security scrutiny. This mitigation reduces the load on expensive DPI servers.

CyberMapper's affinity load balancing features help protect mission critical deep packet inspection (DPI)-based security content filtering clusters. In the event that one or more of the servers or virtual network functions (VNFs) in the cluster fail, CyberMapper provides non-destructive load balancing to help protect the stateful nature of the security DPI servers. This feature is also helpful for maintaining throughput during server/VNF maintenance events.

As seen in Figure 2, CyberMapper integrates real-time inputs from trusted industry IP reputation feeds and policy enforcement rules as well as mitigation events generated by DPI threat engines. These are all converted into new flow rules that are distributed to all NoviWare-enabled switches managed by CyberMapper.

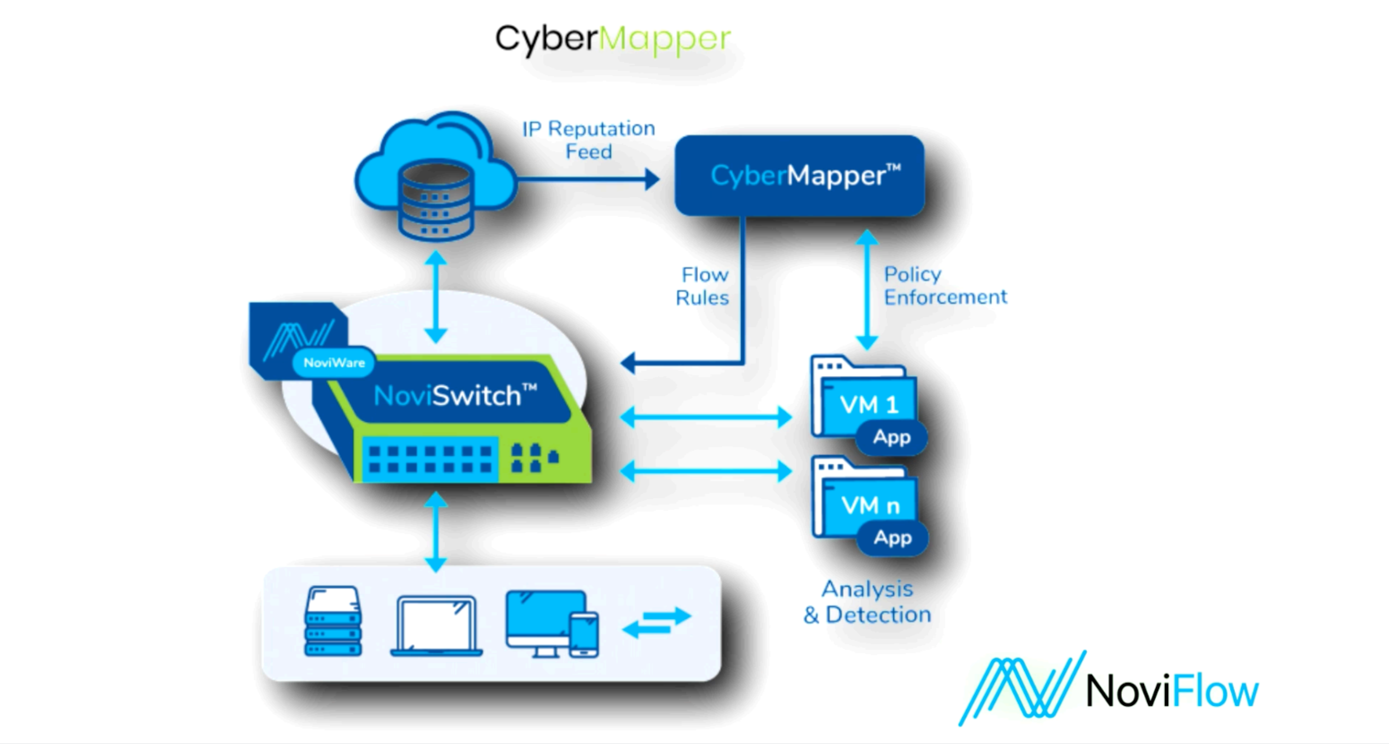


Figure 2. CyberMapper block diagram

CyberMapper Dashboard

CyberMapper also includes a browser-based tool that provides real-time telemetry statistics on each security tool in the security cluster, traffic flow information on the WAN and LAN ports, plus the active status of reputation and mitigation filtering. If an attack is in progress, the dashboard enables real-time mitigation of traffic flows and the results of mitigation, as well as capacity analysis of flow volumes to DPI servers.

High Performance Using Barefoot Tofino™-Based White-Box Switches

CyberMapper runs on white-box servers and controls NoviFlow's NoviWare network operating system (NOS) on white-box switches. The NoviWare NOS specifically addresses the need of programming match-action pipelines optimized for Tofino switching chipsets. NoviWare has been developed as a reliable NOS platform with a rich set of interfaces, including OpenFlow, gRPC, and P4-Runtime interfaces. This allows customers to create, test, and deploy their own application-specific pipelines to fit their application needs.

NoviFlow offers its White-Box Series (WB Series), a line of white-box switches with NoviFlow already integrated. With NoviWare, the Tofino-based switches, which are rated for up to 6.5 Tbps of traffic, can be programmed to take line-rate forwarding actions on a large variety of parameters.

NoviFlow has delivered CyberMapper on switches powered by the Tofino Ethernet switch ASIC from Barefoot Networks, an Intel company. The Tofino switch family is based on Barefoot's Protocol Independent Switch Architecture (PISA) with one switch chip in the family supporting Ethernet interfaces totaling up to 6.5 Tbps. The PISA architecture leverages the P4 programming language for data planes, an open source project managed by the Open Networking Foundation (ONF). With the P4 data plane, Tofino switches forwarding capability can be adapted via software to new needs in the network or to new protocols that are supported by P4. This programmability combined with the centralized SDN control provided by NoviWare provides a very high performance hardware foundation for CyberMapper.

Conclusion

NoviFlow's CyberMapper implements a security network fabric optimized to load balance and mitigate cybersecurity tools that provides network operators the ability to gracefully scale in order to face continually increasing data flows. With its mitigation features, CyberMapper can triage incoming data based on whitelists/blacklists to identify and act on packets that are from trusted or untrusted sources, reducing the load on cybersecurity applications. With its security load balancing services, it maximizes the scalability of a cybersecurity application cluster. Performance is based on the hardware infrastructure, and when implemented on a white-box switch powered by the Barefoot Networks Tofino programmable Ethernet switch, CyberMapper can achieve outstanding performance.

About NoviFlow

NoviFlow Inc. provides open standard-based high-performance SDN networking solutions to network operators, data center operators and enterprises seeking greater performance, flexibility, cost-efficiency, and security over their networks. NoviFlow has offices in Montreal, Sunnyvale, and Seattle, and representatives in Asia Pacific, Europe, and the Middle East. For more information, visit http://noviflow.com/. Follow NoviFlow on Twitter @NoviFlowInc.

About Intel® Network Builders

Intel Network Builders is an ecosystem of infrastructure, software, and technology vendors coming together with communications service providers and end users to accelerate the adoption of solutions based on network functions virtualization (NFV) and software defined networking (SDN) in telecommunications and data center networks. The program offers technical support, matchmaking, and co-marketing opportunities to help facilitate joint collaboration through to the trial and deployment of NFV and SDN solutions. Learn more at http://networkbuilders.intel.com.

[1] Figure provided courtesy of NoviFlow.

Intel technologies may require enabled hardware, software or service activation.
No product or component can be absolutely secure.
Your costs and results may vary.
Intel does not control or audit third-party data. You should consult other sources to evaluate accuracy.