Fortinet and Noviflow Security Solution

Security services optimized and scaled in a high throughput programmable SDN networking environment

Challenges

Recent years have seen tremendous and accelerating increases in demand for data networking capacity with carriers and in enterprises. The multiplication of mobile and connected devices, the proliferation of streaming video-based applications, and now the internet of things (IoT) will only increase the challenge of delivering capacity and ensuring quality as data moves from web to mobile to machines. The challenge is even greater for companies seeking to protect data, infrastructure and identities by cost effectively inspecting, analyzing and mitigating cyber threats in an age of social networks, state-sponsored cyberterrorism, automated BOT networks, and machine learning driven malware.

In partnership with Fortinet, NoviFlow integrates Software Defined Networking (SDN) capabilities with Fortinet Security Fabric, effectively moving the services onto the SDN enabled network, while reducing total customer network CAPEX and OPEX. The Fortinet Security Fabric is designed around a series of open application programming interfaces (APIs), open authentication technology, and standardized telemetry data that also enables NoviFlow CyberMapper to link Fortinet's security services and appliances directly into NoviFlow's programmable fabric and provide end-to-end broad, automated and integrated security.

Key Benefits

- Higher bandwidth and cost-effective dynamic scaling to address large data flows and on-demand capacity.
- NoviFlow CyberMapper provides line-rate traffic filtering, steering, load balancing and security mitigation services.

FORTINET Fabric-Ready

Noviflow Noviware and Cybermapper

NoviWare and CyberMapper deliver on the promise of SDN by offering forwarding plane solutions that can handle complex flow processing, massive throughput, and scalability, making it possible for Fortinet Security Fabric users to stay ahead of today's exponentially growing demand and ever-expanding threat horizon. NoviFlow combines filtering and load balancing functions into a single cost effective white box appliance that can handle up to 6.5T of throughput (using the Barefoot Tofino networking chip). It would take a number of traditional load balancing appliances to address the level of traffic managed by a single NoviFlow appliance.

Combined Solution Description

In conjunction with Fortinet security services and appliances, NoviFlow reduces latency and operating costs, and increases reliability by significantly simplifying network architectures. NoviFlow solutions also support elastic scaling of Fortinet security solutions – at line rate – up to Terabits of throughput at a fraction of the cost seen by other solutions.

NoviFlow's CyberMapper enables NoviWare™ compatible switches to deliver packet filtering, threat mitigation and load balancing directly in the network fabric in a simple, scalable pizza-box form factor, and at a fraction of the price of conventional threat mitigation solutions.

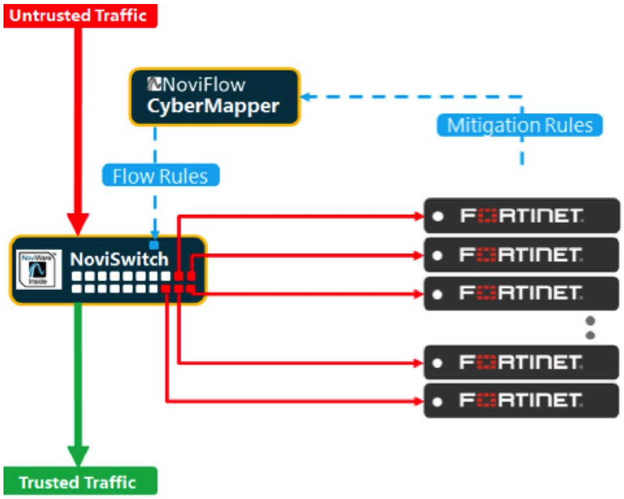
CyberMapper implements fine grain mapping of cyber mitigation events including reputation filtering and load balancing into a DPI security cluster. Combined with NoviSwitches, CyberMapper delivers a high-performance forwarding plane ideal for use in a Threat Intelligence Gateway. CyberMapper leverages the power and flexibility of the SDN match-action pipeline to map cyber-mitigation functions into rules sets used by Noviflow's NoviWare to provision and control high-performance programmable data planes forwarding up to 6.5 Tbps in a single switch, and using open standard interfaces such as OpenFlow, gRPC and P4Runtime. Flows can be identified and managed using any information in the header at full line rate.

CyberMapper changes the equation on the cost, performance and scalability of delivering cybersecurity by leveraging the power of SDN to implement cybersecurity as a forwarding plane function!

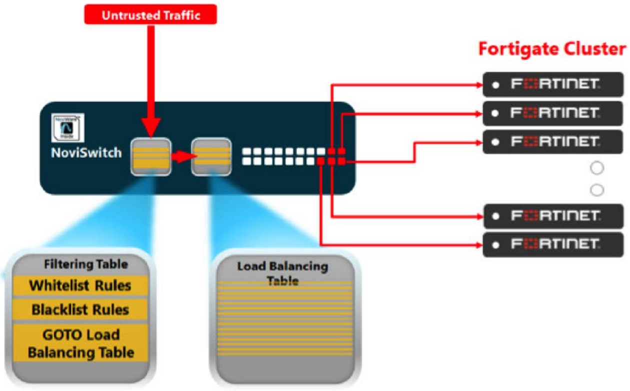
The combined solution allows Fortinet and NoviFlow to address larger scale deployments and get involved in scaling the highest throughput use cases. By implementing security functions in the forwarding plane, traffic directed to each security hdevice is highly reduced and optimized so that security functions are more efficiently utilized.

This allows stacking of Virtual Network Functions and appliances to achieve total throughput capability in the Terabit range. It also significantly reduces periodic loss of security capacity due to rehashing and restoring of state when right sizing or replacing downed security devices. Another benefit of the NoviFlow/Fortinet solution is all traffic types experience lower latency as traffic is filtered and load-balanced at line-rate in the switch. CyberMapper even provides a feedback channel enabling Fortinet cybersecurity applications to adjust network behavior in real-time.

Diagrams of Joint Solution



- Scale-out of the Fortinet Security Services
- Accelerate performance with off-load services
- Protect “State” in Fail-over or Dynamic Scaling processes
- Replaces high-end, expensive load balancers
- Increase throughput of existing Fortinet cluster



- Programmable Match Action Pipeline
- Customizable switch for specific security needs
- Match and act on anything in Header
- Implement Powerful Mitigation policies
- Steer flows where you want and how you want
- Integrate load balancing

Fortinet Security Fabric

The Fortinet Security Fabric is an architectural approach that unifies the security technologies deployed across the digital network, including multi-cloud, endpoints, email and web applications, and network access points, into a single security system integrated through a combination of open standards and a common operating system. These solutions are then enhanced through the inhtegration of advanced threat protection technologies and a unified correlation, management, orchestration, and analysis system.

About Noviflow

NoviFlow provides high-performance OpenFlow-based switching solutions to network carriers, data center operators, government agencies and enterprises seeking greater control, security and flexibility over their networks. NoviFlow has offices in Montreal, Boston, Sunnyvale and Seattle, and representatives in Asia Pacific, Europe and the Middle East.

www.fortinet.com

February 6, 2019 9:14 PM

Mac:Users:susiehwang:Desktop:Egnyte:Egnyte:Shared:Creative Services:Team:Susie-Hwang:Egnyte:Shared:CREATIVE SERVICES:Team:Susie-Hwang:2018:Collateral-Refresh-2018:Solution-Brief-Template:sb-template-gray Folder:sb-template-gray