Security for the Cloud Data Center

Security Challenges

Advanced security threats are now more targeted and stealthy. They no longer focus on denial of service alone, but on the valuable data residing in the data center.

Intrusions, DDoS attacks, APTs, undetectable back-door break-ins, complex multi-phase targeted attacks, are often nearly impossible to detect.

Defending Against Attacks

Actionable intelligence and normal base lining are critical to defend enterprises of all types against attacks and data loss.

Detecting attack patterns early and responding to risks through automated approaches is vital to modern cyber-defense and loss mitigation strategy.

Solution Elements

Establishing active monitoring policy and active response plans provides the best defense against targeted attacks using:

- Multi-tenant access and cross-tenant protection in virtualized cloud networks
- Continuous monitoring for data loss and threat protection using Arista DANZ
- Streamlined scalability and services integration with SDN triggers and automation
- DirectFlow Acceleration to provide cloud-scale >100Gbps performance with next generation firewalls

Many organizations today are embracing cloud-based approaches in their data center, including in-depth virtualization of resources to enable better agility and lower costs, greater network bandwidths to harness the power of dense virtualization, and embracing the information profusion brought on by big data through advanced analytics. The complexity of providing secure access, protecting critical data and end-user privacy, and assuring business continuity in these hyper-dynamic, high-performance compute and data management infrastructures is leading to a demand for a new approach in network and data security.

New Data Center Security Requirements

Whether for government, service provider, or enterprise organizations a new trend toward targeted cyber-attacks has changed the landscape for defense strategies. Stealthy and dangerous multi-phase incursions are prevalent today, using combinations of Denial of Service (DoS), unauthorized access, insertion of malware, and widespread data theft. These advanced attacks are often led by cyber-criminals intent on gaining access to or destroying key data assets without detection.

Fortune 500 enterprises have been losing the war against cyber-criminal forces, according to the 2013 State of Cybercrime Survey from PwC and CSO magazine* which included responses from 500 U.S. executives, security experts, and others from both private and public sectors. These organizations are turning to the latest and best tools for self-defense while trying to determine what economic impact fighting cyber-crime will have on their organizations.

It is widely agreed that no single tool can provide protection against the myriad of attack modes and exploits extant today, while broader strategies can seem economically prohibitive at access speeds of 10Gbps and more. However, organizations with valuable data assets to protect can have high-fidelity threat intelligence that collectively and cost effectively scales to provide a clearer picture of the threat landscape while providing active defenses, by including:

- Distributed perimeter-less protection within the virtualized cloud
- Continuous end-to-end holistic network & system monitoring
- Detection, ranking and correlation of all potential threat activity
- Automated activation of controls and deeper inspection when needed
- Better management of in-placement and overall security cost

A comprehensive approach to deployment of multiple complementary tools to deal with security threats is referred to as 'defense-in-depth' strategy, and is vitally important to today's enterprise and service provider data centers. This paper outlines such an approach.

Security Imperatives in the Modern Software Defined Data Center

Exploding operation complexities have led to many of the key situational factors causing unpreparedness in IT and Security operations to deal with key requirements. In fact, conflicting needs between network and security operations teams have led to high profile breaches in security and data protection. It is imperative that current data center IT and Security operations teams work together to address:

- service assurance and continuity with limited resources
- protection for valuable data assets and customer privacy
- immediate response to mitigate attacks before loss of assets or service occurs
- maximizing the ROI of security investments while migrating from 1/10Gbps to 40/100Gps

In modern data center environments, the concept of 'secure the perimeter' has become effectively irrelevant. East-west traffic patterns dominate the data center while distributed application tiers with a variety of interaction models make it difficult to isolate and protect resources. It is no longer sufficient to insert protections around a secure perimeter to protect the data center. An

integrated approach to tool insertion, threat detection and active mitigation are vital.

Tiered services providing machine-to-machine communications to provide a complete application add another layer of complexity to detecting and mitigating issues in today's data center. These application architectures can increase the dependency on high-volumes of east-west traffic to build scalable application services for the end-user. Furthermore, the integration of each tier with its corresponding clients through network based APIs can open a new realm for threat propagation that needs to be protected. Cross-tier application-centric visibility, as well as visibility into all east-west and inter-VM traffic, are increasingly becoming critical issues in securing and managing the data center workspace.

Where to Insert Security?
Protection of modern data centers from advanced targeted threats requires improved visibility and better security tool integration with the network itself.

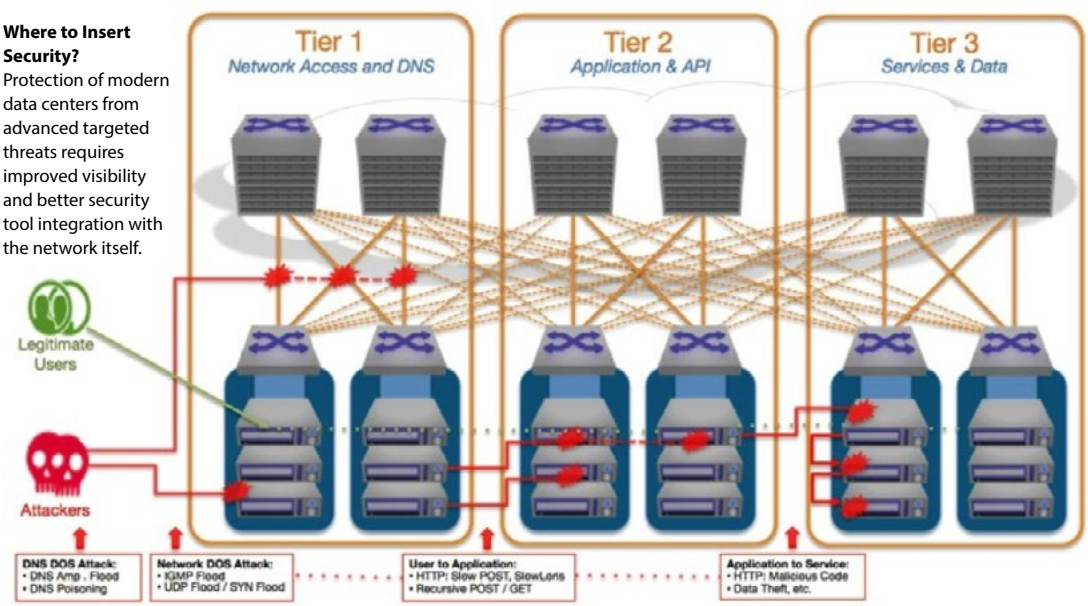

Figure 1: The east-west traffic pattern in cloud data centers creates new security challenges

Additionally, a key factor complicating security decisions for the software defined data center is the impact of compute, storage and network virtualization on visibility of east-west traffic. Inter-VM traffic is increasing, as is the importance of isolating and protecting different tenants within the same data center from each other. The impact on data center architectures and deployment of security tools can be profound.

Where to Start

With comprehensive visibility, active path mitigation, and flexible placement of advanced IT operational intelligence tools an IT organization can effectively defend against the emerging threat landscape even at cloud data center scale and with extensive virtualization. By using a flexible data center architecture based on Arista's Software Driven Cloud Networking, IT and security operations teams are provided with software driven visibility and control that encompasses all in-band and out-of-band requirements for network and application visibility and can provide the automation, services and comprehensive visibility needed to:

- allow actionable re-distribution of traffic when critical resources are compromised
- provide a critical role in responding to and recording attacks programmatically
- inspect all traffic according to profiled attack patterns and redirect it to tools for analysis
- track what information is being sent to outside recipients (exfiltration)
- maintain next-generation firewall security for at-risk traffic in-line while maintaining load balancing and HA

Comprehensive Visibility

Defense-in-depth threat protection strategy starts with a solid internal risk assessment and requires visibility into external actions and traffic patterns that could indicate that an attack is in progress. To detect and understand threat vectors effectively it is critical to first understand what is 'normal' by establishing effective monitoring and profiling of all network traffic.

Network access speeds above 10Gbps are causing scale issues for many tools designed to monitor traffic in the data center at lower speeds. Application Performance Management (APM), Network Performance Management (NPM) and security tool vendors have addressed the need for increasingly speedy network capture and analysis with faster and larger platforms, but the cost of comprehensive monitoring can still seem prohibitively high.

Arista offers a new approach to monitoring aggregation that delivers high density, non-blocking 10/40/100GbE networks powered by award-winning Arista EOS® software to deliver an order of magnitude improvement in the economics of building cloud-scale monitoring. The Arista Data ANalyZer (DANZ) solution delivers scalable end-to-end network and application monitoring with exceptional flexibility and precision, while enabling existing third-party monitoring tools to integrate directly and cost effectively with captured data while scaling to support 10/40/100Gbps.

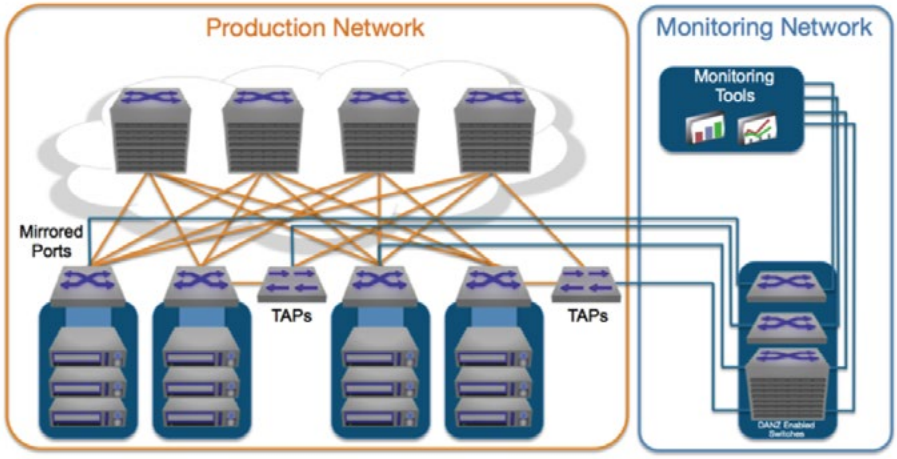

Figure 2: DANZ - Access any traffic for real-time analysis

While raw packet data provides the best and most detailed source of insight for monitoring of security, performance, and troubleshooting information, there are other information sources that can also be valuable. These include coarse-grained flow-analysis data from sFlow, internal network operational data from machine logs and network event mechanisms made available through Splunk, and precision data such as LANZ queue analysis from Arista switches.

The Arista DANZ feature set delivers fundamentally new capabilities with Arista's data center class switches:

- High density, non-blocking, wire-speed packet capture with advanced traffic management capabilities so all network traffic can be monitored without loss
- Software Defined Networking (SDN) support, enabled by the programmability of Arista EOS, makes it possible to directly steer specific network flows to the desired analysis tools
- Symmetric per-flow load balancing permits in-line security and monitoring tools to scale to support terabit speeds without loss of per-session awareness
- The Latency ANalyZer (LANZ) feature enables detection of microbursts and congestion at tool ports so network operators can take appropriate action to maintain network visibility under heavy loads and assure security oversight with 100% fidelity

- Support for emerging network virtualization models (e.g., vMotion, VXLAN, NVGRE) to maintain visibility of any workload in hyper-dynamic virtualized public and private clouds

Triggers and automated actions are supported via direct APIs to the network infrastructure. Log monitoring, and packet capture can allow staff to respond quickly by alerting team members by email, and by automatically redirecting suspicious traffic and event logs to the SIEM and traffic recording tools so that responders have the fingerprints of the attackers and the details of the developing attack scenario immediately.

Adding Active Mitigation to Security Monitoring with DANZ

Typically, the tools that consume raw packet data from packet capture and monitoring architectures like DANZ are focused on providing performance analytics, identifying problems (troubleshooting), and detecting anomalies in complex cross-tier applications. However, a new approach to active mitigation of attacks using the intelligence of these tools now uses programmability of the network through Software Defined Networking (SDN) APIs to provide rapid active mitigation.

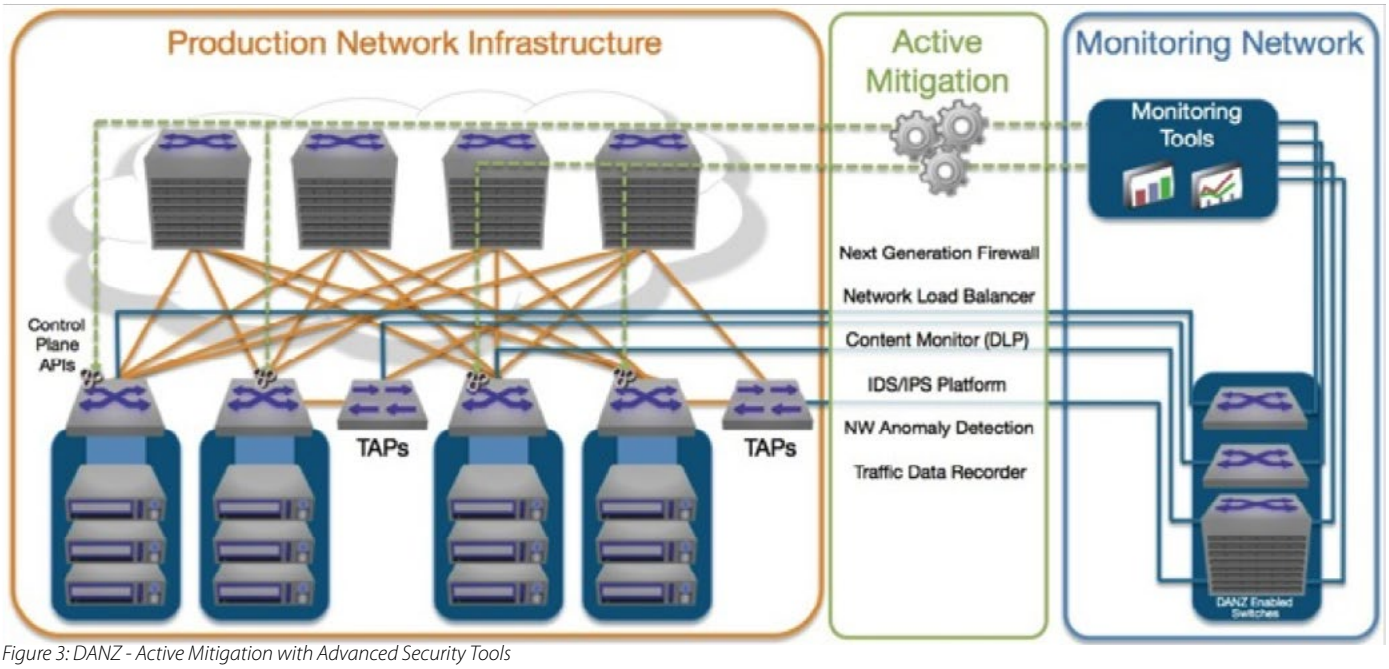

Figure 3: DANZ - Active Mitigation with Advanced Security Tools

Modern network monitoring architectures like DANZ use advanced network hardware capabilities to provide access to specific targeted data on the network for each tool and to condition the traffic before arrival at the tool for greatest efficiency. Out-of-band monitoring can complement in-line mitigation solutions where in-line security devices may otherwise increase latency and slow down overall network performance efficiency.

Choosing the Right Security Tools for Defense-In-Depth

In reality, no singular security tool or vendor can make the claim that their products are an InfoSec panacea nor should they. Most will make valid claims about the ineffectiveness of widely used security techniques, for example, the many flaws of signature-based or statistical-based approaches to threat detection. Actual solutions require a well thought out combination of knowledge, products and/or services to baseline normal behavior, and mitigation solutions to combat the increasingly skilled adversaries targeting businesses. Currently there are wide varieties of technologies available to allow teams to respond effectively to the mounting pressure to intercept attacks.

Table 1: Security Technologies - Perceived Strengths and Weaknesses		
Security Technology	**Strengths**	**Weaknesses**
Network Traffic Monitors (Sniffers, IDS, IPS, Packet Recorders, Data Analytics)	Can provide insights on both normal and abnormal network traffic flows with adequate analysis. Traffic recorders can also be very valuable as forensic tools.	Unable to monitor secure data streams (IPSEC, HTTPS, encrypted tunnels), and poor resolution of security risks unless combined with SIEM data.
Active Network Scanners (Application Probes, Port Probes, to Identify Resources and exposed Personally Identifiable Information (PII))	Continuous probing and monitoring improves situational awareness and historical trail of when assets were in-placed on the network.	Can be expensive to deploy in a dynamic high performance segmented cloud. Storing and securing massive amounts of data is slow and complex analytics can prevent timely insight.
In-line Firewalls and Gateways (Stateful filtering, email monitoring, content scanning, anti-virus, etc.)	Only option to capture and block unknown zero-day exploits from outside sources. Less effective at capture inter-tenant vulnerabilities or those brought into the network by hosts.	Virtualized gateways and firewalls in the cloud are trivial to detect and evade with malware, and zero-day exploits can bypass signature-based gateways.
Security Information and Event Analytics (SIEM)	Provides integration and analytics on macro (log) data from various tools, platforms, etc. Easiest way to manage a defense in depth strategy.	Cannot operate alone and needs variety of other tools deployed to detect actual threat conditions and events. Consider this a complement to other tools.

The best chance of a successful security strategy is to continually adapt to the arms race between emerging attack tools and best-in-class defenses, bringing together expertise with complementary devices and techniques that have proven themselves most capable in their respective arenas. By using a variety of tools to discover and baseline network and application behaviors, organizations can identify risks and focus areas that may indicate an actual active threat in progress.

In addition, detecting normal traffic patterns aids in the real-time and forensic discovery of attacks and probing that can precede attacks and allows actionable insights to be used in preparation of automated policies and triggers that can defend against an unknown or unexpected attacker. Broader use of IT operational intelligence capabilities, based on a variety of monitoring capabilities, has been shown to provide insight into new and emerging threats such as zero-day attacks and APTs better than monolithic monitoring architectures alone.

Scaling Next Generation Security with an Arista SDN

By following SDN principles and techniques, requirements to insert tools in-line, such as for firewalls, can be accommodated while providing global visibility through out-of-band analytics. The SDN capabilities of Arista EOS network operating system include controller-independent architectures using DirectFlow and OpenFlow APIs, automated cloud integration with OpenStack and leading network and compute virtualization platforms such as VMware vSphere/NSX and Microsoft HyperV.

Further, security continuity in hyper-dynamic virtualized cloud environments can be assured through binding of security services with Arista's VM-aware architecture dynamically. Whenever the virtualized network, virtualized compute and storage infrastructure changes to accommodate in-motion workloads, the relevant policies and tool configurations can be dynamically configured through network automation scripts. This model provides persistent visibility in any dynamic cloud environment. Providing active defense using continuous real-time monitoring, VM-aware visibility using Arista VMtracer and provision of trip-wires at all possible attack points are possible at scale.

Example of Dynamic Defense-In-Depth with Arista DirectFlow Assist (DFA)

DirectFlow Assist (DFA) is an EOS extension that runs on an Arista switch to dynamically insert flow table entries via Arista's DirectFlow API, in order to offload or assist an attached in-line or out-of-band security platform such as a firewall. By providing integrated control over network forwarding to the firewall, DFA allows dynamic security policies to be applied in the network based on intelligence derived from out-of-band monitoring, deep packet inspection (DPI), and other analysis technologies.

The scaling and performance benefits of DFA integration allow security platforms to scale performance up to 10-50x over static in-line deployments and provide a scaling model that can be applied in any virtualized or cloud based environment. Use cases for the DFA solution include DDoS attack mitigation and offload for next generation firewalls, content inspection platforms, and IDS/IPS among others.

- DDoS Attack Mitigation, selectively blocking packets in-flow based on DoS detection in attached analytic platforms
- Elephant Flow Offload, inserting a flow entry to bypass the firewall for trusted application traffic such as backups
- Firewall Scaling, providing flow-by-flow bypass and filtering based on firewall DPI discovery and classification
- Redirection of target traffic to a 'honeypot' or decoy platform for both profiling and prosecution

A firewall web console, user program using Arista EOS APIs, or the Arista CLI can be used to configure the policies that will be used to insert network traffic flows of interest using DFA. For the DDoS attack mitigation case, a DDoS Protection Policy will be created and attack volume thresholds and load profiles specified on the firewall.

What happens in DFA during an attack?

When an attack happens, an application can instruct the network comprised of SDN-capable switches to or drop the attack traffic flows in hardware without affecting the performance of the system or network.

Alternatively, suspect traffic may be redirected for deeper analysis by next-generation firewalls, IDS/IPS platforms, or other security solutions. Traffic manipulation that can be commanded with active mitigation can include:

- Bypass or block target flows in the network
- Capture and recording of suspect traffic for later analysis and prosecution of attackers
- Explicit traffic redirection to a target (such as a honeypot or traffic recorder)
- Other user-defined actions such as triggering alarms or other platforms to perform additional functions

---

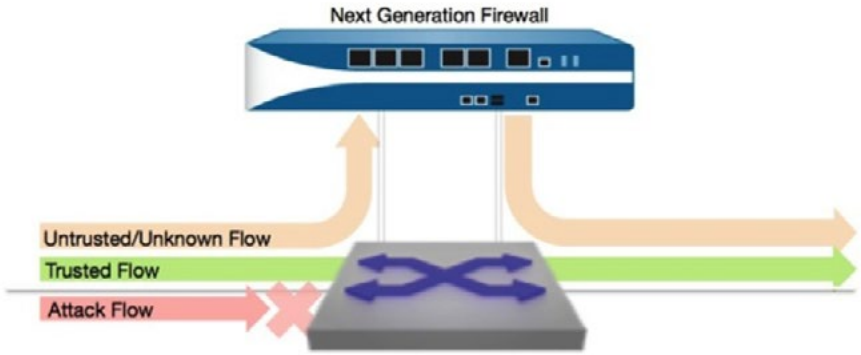

Figure 4: Using SDN Firewall Insertion with DFA

When DFA receives a flow-classification message from the firewall it validates the message and then parses out a "DFA Flow Specification". The Flow Specification includes a unique flow name, match criteria, desired action, priority and lifetime. Match criteria may include source and destination IP addresses, source and destination layer-4 ports and protocol (ICMP, TCP or UDP) depending on the type of flow and custom configuration file settings. The action on the switch will either be to drop packets in the flow or to output packets to a specific switch port in order to bypass the firewall or provide further analysis.

For bypassed flows, an additional Flow Specification is automatically created for the reverse direction return traffic flow to provide symmetry. Flow entries can use aging where EOS will delete the flow entry after a specified lifetime interval, or flows can be explicitly removed by the firewall.

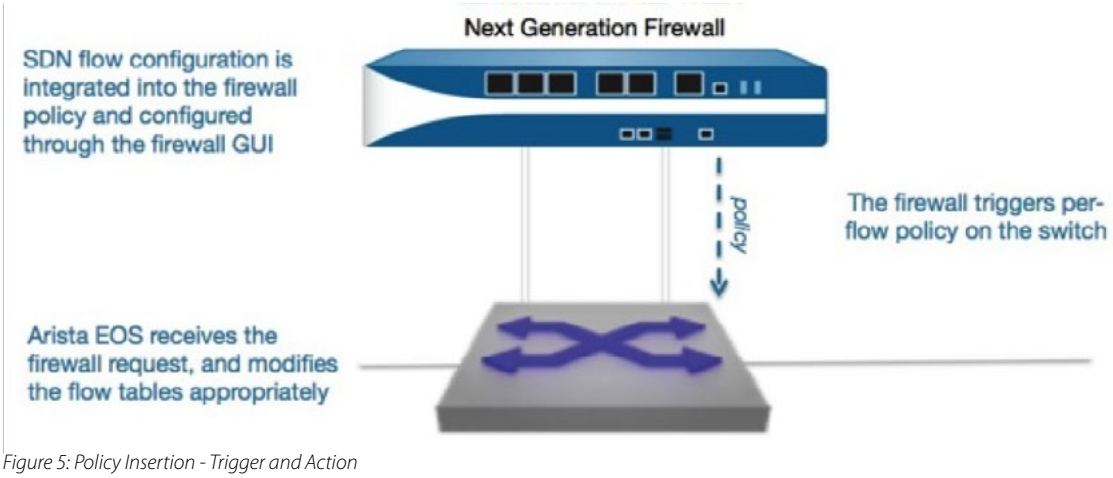

Figure 5: Policy Insertion - Trigger and Action

From the Flow Specification DFA generates a sequence of EOS DirectFlow API configuration commands to create the flow table entry. It then uses eAPI to send this configuration command sequence to EOS. DFA includes a command line shell with various commands for monitoring currently active flows, deleting flows as well as starting and stopping the DirectFlow Assist process.

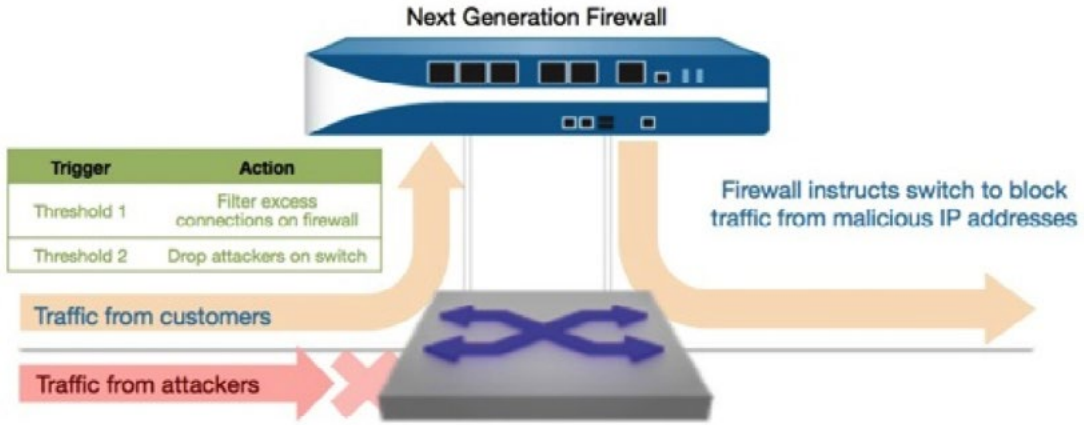

Figure 6: Policy Execution - DoS Mitigation Example

DFA is an example of the flexibility of Arista's Software Driven Cloud Networking (SDCN) capabilities and uses a small subset of the capabilities of the Arista EOS operating system and its APIs. Arista SDCN combines the principles that have made cloud computing the unstoppable force that it is: automation, self service provisioning, and linear scaling of both performance and economics, coupled with network virtualization, custom programmability, simplified architectures, and extreme efficiency.

Conclusion

The combination of cloud features of the Arista EOS software platform for SDN programmability, DANZ for advanced network visibility, and DirectFlow Assist (DFA) create a unique, open, and best-in-class software foundation for maximizing the security of the network to both the enterprise and service provider data center: a new architecture for the most mission-critical location within the IT infrastructure that simplifies management and provisioning, speeds up service delivery, lowers costs while creating opportunities for service differentiation and placing control and visibility back into the hands of the network, security and systems administrators.

Arista's SDCN, in combination with our security partners, provides a comprehensive solution to the conundrum of scaling and integrating effective security in the modern cloud data center. These solutions are available today and address the growing need for defense-in-depth.

According to a 2013 study by Ponemon Institute, cyber-attacks, which target specific servers, caused 18% of data center outages in 2013, up from just 2% in 2010. These attacks have increased dramatically as commercially available attack tools have improved and network speeds have increased, making it easier to generate massive amounts of dummy traffic and overwhelm in-line defenses. Dealing with these attacks often requires specialized techniques, using advanced analytics and forensic expertise according to Ponemon.

*2013 State of Cybercrime Survey courtesy of PwC, CSO magazine, the U.S. Secret Service and the Software Engineering Institute CERT Program at Carnegie Mellon University

Santa Clara—Corporate Headquarters
5453 Great America Parkway,
Santa Clara, CA 95054

Phone: +1-408-547-5500
Fax: +1-408-538-8920
Email: info@arista.com

Ireland—International Headquarters
3130 Atlantic Avenue
Westpark Business Campus
Shannon, Co. Clare
Ireland

Vancouver—R&D Office
9200 Glenlyon Pkwy, Unit 300
Burnaby, British Columbia
Canada V5J 5J8

San Francisco—R&D and Sales Office
1390 Market Street, Suite 800
San Francisco, CA 94102

India—R&D Office
Global Tech Park, Tower A & B, 11th Floor
Marathahalli Outer Ring Road
Devarabeesanahalli Village, Varthur Hobli
Bangalore, India 560103

Singapore—APAC Administrative Office
9 Temasek Boulevard
#29-01, Suntec Tower Two
Singapore 038989

Nashua—R&D Office
10 Tara Boulevard
Nashua, NH 03062