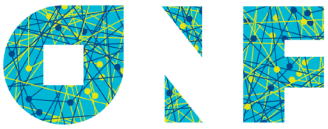


OPEN NETWORKING
FOUNDATION

SDN Security Considerations in the Data Center

ONF Solution Brief
October 8, 2013

Table of Contents

2 Executive Summary
3 SDN Overview
4 Network Security Challenges
6 The Implications of SDN on Network Security
6 Business Application Implications
7 SDN Control Layer Implications
7 SDN Security Use Case: Automated Malware Quarantine
10 SDN Benefits and Best Practices
12 Conclusion
12 Contributors

Executive Summary

Virtualizing and provisioning the network to provide per-tenant, on demand, intelligent security is challenging with today's networks. Numerous security solutions, protocols, and appliances have been deployed in the data center to address a myriad of security threats. Today's security solutions are, however, difficult to manage, expensive, complex, inflexible, and highly proprietary.

Secure networks are critical to all businesses, especially with their increased migration to the cloud and the wave of innovation being unleashed by Software-Defined Networking (SDN). SDN provides a centralized intelligence and control model that is well suited to provide much-needed flexibility to network security deployments.

OpenFlow™ — the first SDN standard — manipulates the network path based on traffic analysis and statistics provided by the SDN controller, in a multi-tenant environment. The flow-based paradigm is particularly well suited to protect traffic on each virtual network slice, or for each virtual tenant.

Along with many benefits, SDN poses new threats, particularly with the emergence of cloud, BYOD (Bring Your Own Device), and virtualized environments. It is critical to consider threats, risk exposure, operational impact, performance, scale, and compliance in the SDN-based data center of the future.

To illustrate how SDN can be used to improve network security, we present a use case for automated malware quarantine (AMQ). AMQ detects and isolates network devices that have become compromised before they can negatively affect the network. This solution brief examines how SDN can be applied in an AMQ implementation, then summarizes its benefits.

SDN Overview

Software Defined Networking is a new architecture that has been designed to enable more agile and cost-effective networks. The Open Networking Foundation (ONF) is taking the lead in SDN standardization, and has defined an SDN architecture model as depicted in Figure 1.

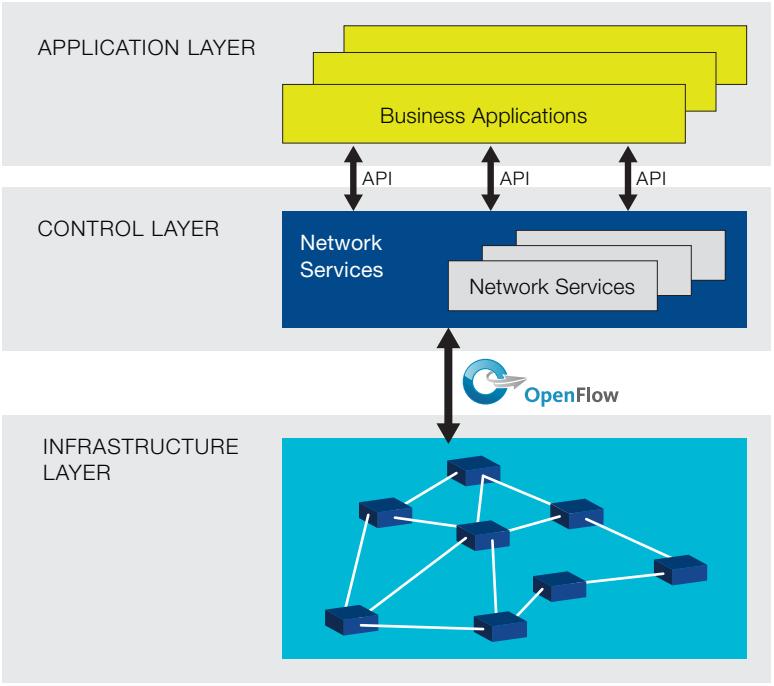


FIGURE 1
ONF/SDN architecture

The ONF/SDN architecture consists of three distinct layers that are accessible through open APIs:

- **The Application Layer** consists of the end-user business applications that consume the SDN communications services. The boundary between the Application Layer and the Control Layer is traversed by the northbound API.
- **The Control Layer** provides the consolidated control functionality that supervises the network forwarding behavior through an open interface.
- **The Infrastructure Layer** consists of the network elements (NE) and devices that provide packet switching and forwarding.

According to this model, an SDN architecture is characterized by three key attributes:

- **Logically centralized intelligence.** In an SDN architecture, network control is distributed from forwarding using a standardized southbound interface: OpenFlow. By centralizing network intelligence, decision-making is facilitated based on a

global (or domain) view of the network, as opposed to today's networks, which are built on an autonomous system view where nodes are unaware of the overall state of the network.

- **Programmability.** SDN networks are inherently controlled by software functionality, which may be provided by vendors or the network operators themselves. Such programmability enables the management paradigm to be replaced by automation, influenced by rapid adoption of the cloud. By providing open APIs for applications to interact with the network, SDN networks can achieve unprecedented innovation and differentiation.
- **Abstraction.** In an SDN network, the business applications that consume SDN services are abstracted from the underlying network technologies. Network devices are also abstracted from the SDN Control Layer to ensure portability and future-proofing of investments in network services, the network software resident in the Control Layer.

Network Security Challenges

IT infrastructure is rapidly moving to the cloud, creating a dramatic technology shift in the data center. This shift has significantly influenced user behavior: end users now expect anytime, anywhere access to all their data. Additionally, network operations are being transformed from operator-intensive management towards greater automation.

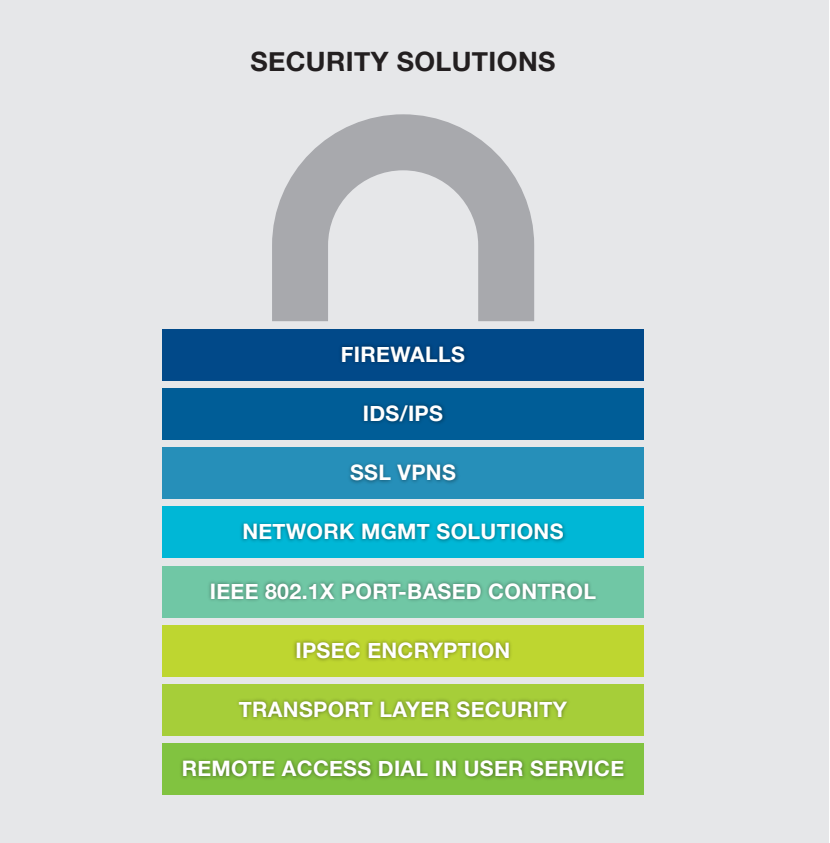
The data center of the future is emerging as a highly virtualized environment that must address a diverse set of user needs, including anytime, anywhere access to their data, the consumerization of IT (BYOD) and increased reliance on cloud services.

Security concerns are consistently identified as a major barrier to this data center transformation. While protecting user data is of paramount importance, mobility and virtualization pose new threats that must be understood and secured. And the human factor continues to lead to unnecessary downtime, expense, and unauthorized intrusion.

Throughout the enterprise, end devices and data center resources including hypervisors, storage devices, servers, switches, and routers must be secured. Despite the diverse threats, existing security strategies can be successful at minimizing many of the security risks in the data center (see Figure 2).

Currently available security solutions are, however, difficult to deploy, manage, program, scale, and secure. Policies are tightly coupled to physical resources as opposed to services and applications. Security solutions struggle to provide quick and automated threat mitigation across equipment from multiple vendors. Consistent security policies are difficult to administer across compute, storage, and network domains, and multiple data centers. No solutions today allow for complete security orchestration across data center networks.

FIGURE 2
Security Solutions



Today's security solutions include:

- Firewalls for perimeter defense and internal domain control.
- Intrusion detection and prevention systems that monitor network activities for malicious activities or policy violations and attempt to prevent attacks.
- Secure Sockets Layer virtual private networks (SSL VPNs), which provide the ability to securely separate customers and domains.
- Network management solutions that attempt to centrally manage many of these security functions via a console.
- IEEE 802.1X port-based network authentication and access control.
- IPsec for end-to-end authentication and encryption of the IP packets in a communication session.
- Transport Layer Security (TLS) for Application Layer communication encryption security at the Transport Layer.
- The Remote Access Dial In User Service (RADIUS) networking protocol, which offers centralized authentication, authorization, and accounting (AAA) management for end devices to use a network service.

The Implications of SDN on Network Security

OpenFlow-based SDN offers a number of attributes that are particularly well suited for implementing a highly secure and manageable environment:

- The flow paradigm is ideal for security processing because it offers an end-to-end, service-oriented connectivity model that is not bound by traditional routing constraints.
- Logically centralized control allows for effective performance and threat monitoring across the entire network.
- Granular policy management can be based on application, service, organization, and geographical criteria rather than physical configuration.
- Resource-based security policies enable consolidated management of diverse devices with various threat risks, from highly secure firewalls and security appliances to access devices.
- Dynamic and flexible adjustment of security policy is provided under programmatic control.
- Flexible path management achieves rapid containment and isolation of intrusions without impacting other network users.

By blending historical and real-time network state and performance data, SDN facilitates intelligent decision-making, achieving flexibility, operational simplicity, and improved security across a common infrastructure.

Business Application Implications

In the ONF SDN architecture model (see Figure 1), business applications are the consumer of SDN communication services. Network services (residing in the Control Layer) expose the SDN communication services through a series of northbound APIs and directly control the forwarding behavior of the underlying network devices that reside in the Infrastructure Layer (through OpenFlow).

Business applications are vulnerable to potential threats because of the powerful SDN programming model. Multiple SDN network services may interfere with one another, compromising the forwarding behavior of the network; such conflicts must be avoided. Security policies may be compromised at the controller, at one or more network devices, and/or at other places. As a result, security policies must be validated, along with the network configuration and behavior and performance.

The benefits of SDN far outweigh these potential threats. SDN security solutions will continue to evolve to minimize risks from this new network paradigm.

SDN Control Layer Implications

While the SDN centralized control model offers significant benefits to the network and to security management, there are tradeoffs. Logically centralized (and typically physically distributed) SDN controllers are potentially subject to a different set of risks and threats compared to conventional network architectures.

- The centralized controller emerges as a potential single point of attack and failure that must be protected from threats.
- The southbound interface between the controller and underlying networking devices (that is, OpenFlow), is vulnerable to threats that could degrade the availability, performance, and integrity of the network. OpenFlow specifies the use of TLS or UDP/DTLS, either of which supports authentication using certificates and encryption to secure the connection. Additional security measures may be needed in case this authentication fails.
- The underlying network infrastructure must be capable of enduring occasional periods where the SDN controller is unavailable, yet ensure that any new flows will be synchronized once the devices resume communications with the controller.

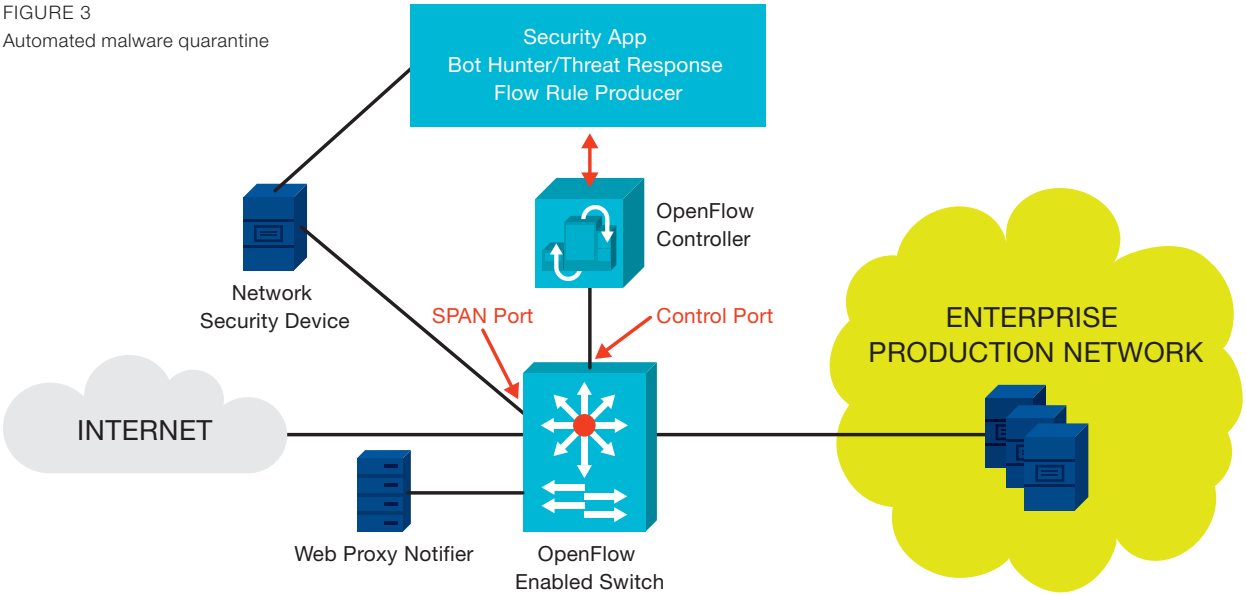
SDN Security Use Case: Automated Malware Quarantine

In this section, we will examine a particular use case to illustrate the implications of the SDN architecture on the implementation of a security function.

Automated malware quarantine (AMQ) detects and isolates insecure network devices before they can negatively affect the network. Upon discovering a potential threat, AMQ identifies the problem and automatically downloads the necessary patches to resolve it. After the threat has been contained, AMQ software automatically allows the device to rejoin the network. This active approach contains and eliminates security threats that could not normally be handled by any single portion of the network.

Today, AMQ is typically deployed as a proprietary solution where each device performs its specified function autonomously with limited awareness of other devices in the network. Such approaches are designed for static traffic flows, and must be capable of monitoring in real-time ingress traffic. This closed approach is inflexible, especially for the data center where server workloads are virtualized, traffic flows are highly dynamic, and multiple simultaneous policies must be maintained. Deploying higher-speed links (40G, 100G, etc.) makes this environment even more difficult.

FIGURE 3
Automated malware quarantine



OpenFlow-based SDN enables a more flexible approach for AMQ, as illustrated in Figure 3. AMQ functionality is centralized in the SDN controller, where it provides efficient security processing. Only suspicious flows will be isolated and monitored.

The flow-based paradigm is particularly well suited for AMQ, because it can manage granular policies and provide efficient service-chaining coordination. In addition, AMQ could benefit from the elasticity achieved through SDN.

EXAMPLE AMQ IMPLEMENTATION

Let's consider a typical AMQ implementation using SDN. In this example, there are two primary security Network Services Modules (NSMs) hosted on the controller that provide the AMQ function:

- The Bot Hunter NSM monitors the network and detects a malware-infested host in real time.
- The Threat Responder NSM directs the controller to initiate the quarantine procedure to isolate the threat from the network in the event of a malware attack.

When a host is quarantined, the Web Proxy Notifier is activated to inform the user on the infected host that security has been compromised.

This example AMQ scenario consists of two stages:

- **Infection**. The end user clicks on a URL or attachment that downloads a rootkit that embeds itself into the user's host machine.
- **Security breach**. The rootkit begins executing a series of procedures to seek additional hosts on the production network and to call home to the botnet control network.

The AMQ application would proactively respond to this malware attack as follows:

- **Observe**. The Bot Hunter NSM observes the traffic pattern from the rootkit to the outside hosts. This pattern includes the stream of port scans performed on the production network from the rootkit application on the infected host.
- **Detect**. Based on the traffic profile (by analyzing what was communicated and to whom) the Bot Hunter NSM detects that there is active malware on the infected hosts.
- **React**. The Bot Hunter NSM creates an infection profile, along with detailed forensics, that generates a high enough score to initiate a quarantine directive to the controller.
- **Respond**. The quarantine directive is translated by the SDN controller as a set of OpenFlow rules that is pushed down to the OpenFlow-enabled switch. These rules cut off the infected host from the production network.
- **Redirect**. All the DNS and web traffic is redirected by the OpenFlow switch to the Web Proxy Notifier, which displays a web page to the end user with the corrective actions to be performed along with the URL to download the software patch to mitigate the attack.
- **Readmit**. Once the corrective actions have been performed, the rules are changed to allow the end host back into the production network.

AMQ transparently and dynamically applies policies to an individual switched port based on the device or user accessing the port. The automatic reconfiguration reduces the response time to security threats and removes the need to have a network engineer create and apply a policy (VLAN, ACL) to manage network access. This approach minimizes the need for manual configuration and application of network user policies.

AMQ does not require any additional network software or hardware beyond the basic OpenFlow-enabled switch or network element, so it is fully interoperable across vendor implementations. AMQ has the potential to reduce operating expenses, automate configuration of edge-port security parameters, and allow for mobility of users at the edge of the network.

SDN Benefits and Best Practices

The AMQ use case illustrates the benefits of SDN for a single security application. Because security is an inherently broad area with many diverse applications, OpenFlow-enabled SDN offers a wide range of benefits for security implementation and management:

- Fine-grained enforcement and control of multiple simultaneous security policies throughout the data center.
- Rapid response to threats, with the ability to rapidly steer or quarantine flows and VMs based on real-time network conditions.
- Validation of security policies, and quick identification and resolution of any policy conflicts that arise.
- Efficient authentication of flow rule producers through the use of digital signatures.
- Incorporation of a trust model with live rule-conflict detection and resolution at the controller layer.
- Synchronization of distributed policy insertion and removal.
- Optimization of secure flow routing in a highly dynamic environment.
- Dynamic assertion of extensions to the security policy when new threats are detected.
- Provision of a mechanism for auditing and audit trails.

AMQ BENEFITS

Besides its overall benefits, OpenFlow-based SDN offers specific advantages when used for automated malware quarantine.

Security Challenges	Autonomous Approach (Today)	SDN-based Approach	Benefits of SDN
New security threats	Security signature is identified. User is located with available tools within the system. User is denied network access. AMQ does not understand the denial. Malicious user moves to another port, continuing to spread the virus.	End-to-end network visibility is derived from centralized configuration and network state. Coarse- or fine-grained controls implement countermeasures in real time.	Operations staff can continuously experiment (out-of-band) to constantly refine AMQ behavior (path management, signatures, traffic management, etc.). Significantly reduce the platform resources required for security processing, thereby reducing CapEx, especially for higher-speed interfaces.
Perimeter security	Perimeter is defined through physical objects (ports, subnets, etc.). Each device must be statically configured individually, typically via CLI. Each device operates autonomously. All traffic for each physical object must be monitored, typically using a single policy.	Perimeter is defined through application-layer concepts (groups, type of device, etc.) Traffic sourced by more vulnerable devices (that is, sources external to the company) can be scrutinized more intensely than traffic from the more secure devices internal to the company. Traffic can be monitored independently of the physical location of the source. Low-touch configuration is possible for all security devices in each domain.	Policy is decoupled from the physical perimeter to better align security processing with the threats. Policies can be granularly applied based on application-layer attributes, not just physical attributes such as ports. Security complexity does not increase in proportion to changes in the physical and logical perimeter, improving protection for the increasing number of mobile users. Coordinated, multi-layer oversight achieves more comprehensive security coverage across the 7-layer stack.
New feature velocity **Proactive patch management**	Difficult to achieve in a consistent manner due to finite resource availability in the embedded device.	Continuous, zero-touch centralized patch management and new feature deployment are possible through centralized control to respond rapidly to new threats.	Simpler to introduce enhanced features; streamlined operations alleviate the need to configure individual devices. Enables a virtual execution environment (VEE) to rapidly analyze and respond to ever-changing threats without the need to patch each individual networking device. VEE allows for near real-time prototyping, testing, and deployment to rapidly respond to new threats. Significantly simpler operation lowers cost.
High scalability	Requires proportional increase in hardware to ensure coverage at the physical perimeter.	Virtualized security processing reduces hardware demands (and management complexity).	Increases security processing capacity along with the scope of the network and additional security processing. Improves utilization because capacity increases can be provided on a temporary basis.

Conclusion

Secure networks are vital to the increased migration to the cloud and to SDN innovation. However, network security is consistently difficult to manage and deploy. This challenge is particularly relevant within the data center, where new services such as cloud computing and the consumerization of IT raise additional security challenges.

OpenFlow-based SDN offers an effective alternative to operate highly secure networks in the rapidly evolving data center. Key benefits of SDN include:

- A flow-based paradigm that untethers policies from the physical perimeter.
- Highly granular policy management and enforcement, for diverse, multi-tenant environments.
- Efficient traffic steering and path management to accelerate detection and isolation of threats.
- Programmability, which enables automation and adaption to mitigate risks.
- Open interfaces to foster multi-vendor interoperability.

As shown in the automated malware quarantine use case, SDN can enable a cost-effective yet robust implementation offering significant operational advantages. Such benefits can also be realized for many other security applications, which must continue to adapt to the ever-changing threat profile of the data center of the future.

Contributors

Mike McBride, Editor
Marc Cohn
Smita Deshpande
Meenakshi Kaushik
Mat Mathews
Shaji Nathan

Open Networking Foundation / www.opennetworking.org

The Open Networking Foundation is a nonprofit organization founded in 2011, whose goal is to accelerate the adoption of open SDN. ONF emphasizes the interests of end-users throughout the Data Center, Enterprise, and Carrier network environments.