Software Defined Environment

A View for the Security Practitioner

Brian S. Rodgers

East Carolina University

4 Dec 2018

ABSTRACT

Exploring and understanding software defined services, hosted locally or off premise in a cloud provider's data center, is a critical task demands the Information Security (InfoSec) practitioner's attention. A strong password and sturdy door locks may have once been adequate to secure business computing environments. The modern enterprise network, assailed by threats from many different avenues, demands a more sophisticated approach to security. Many networks have evolved from simple flat networks to complex instantiations including virtual machines, multiple sites, and diversified strata of information; each demanding different protections. Much of the literature reviewed for this effort was focused on either vendor specific offerings or pure academic works. This work will provide a foundation of cloud and software defined services from a vendor neutral position that abstracts details. Further research is required to evolve the body of knowledge for the security implications from the software defined environment and its elastic characteristics.

Keywords: software defined, cloud, information security, networking

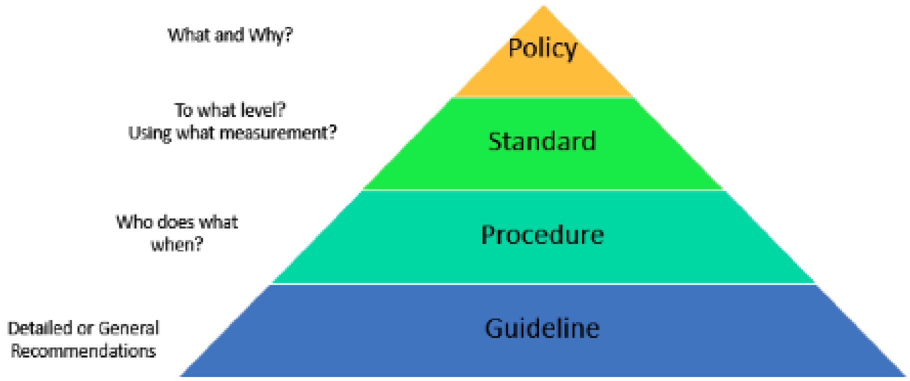
INTRODUCTION

The modern enterprise is faced with multiple decisions when determining its approach to cloud support to business practices. Exploring and understanding software defined services, hosted locally or off premise in a cloud provider's data center, is a critical task demands the Information Security (InfoSec) practitioner's attention. Security controls, honed over years of refinement as best practices for on premise enterprise networks, may not be appropriate for cloud instantiations be they in the local or vendor provided cloud. This work will begin with a high level framework and refresher of enterprise security followed by a primer of cloud based services. Throughout the reader is as challenged to continually assess responsibility and accountability for enterprise security activities in the modern Software Defined Environment (SDE).

A Review of Information Security in the Enterprise

Leadership may be expressed in the corporate environment via the governance and management domains. This paradigm applies to the security and risk management of the organization as well as other more traditional business domains. The board of directors or chief officers provide the governance leadership and the managers and staff execute. (NIST SP 800-100, 2006, p. 14) This process is implemented via Policy, Standards, Procedures, and Guidelines.

Figure 2 - Hierarchy of Guidance



MITRE recommends answering the following questions when developing or reviewing policies:

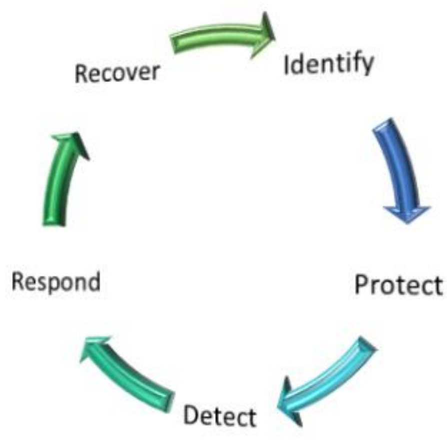
Table 1 - MITRE Policy Questions

What decisions must be made to ensure the effective management and use of IT?	What are the desired outcomes?
Who should make these decisions?	Who is accountable and responsible?
How will these decisions be made and monitored?	How should the process work?

Designing the IT Governance process should be done after the organization has identified its desired outcomes. (MITRE, 2019, p. 60) (MITRE, 2019, p. 60) Each organization should determine the appropriate policies for their situation. Minimally policies should be reviewed annually or after any major incident. ([NIST SP 800-39], 2011) SANS Institute provides templates for nearly thirty policies free of charge. (SANS, 2019) Wholesale adoption of all policies is not recommended regardless of the source. The organization develops its guidance through the evaluation of and desired security posture, threat, and vulnerabilities.

The National Institute of Standards and Technology's (NIST) Cyber Security Framework is provided free of charge as a top level approach to managing information security risk. The Cyber Security framework defines the processes and is supported by numerous special publications that provide implementation details. . Figure three depicts the continual NIST process.

Figure 3 - NIST 5-Step Cybersecurity Process



The adoption of software defined services creates a more complex landscape for this process. The process is more straight forward in conventional enterprise networks, where hardware, software, and networks are on often premise. Additionally decades of application of extensive control matrices such as those in NIST SP800-53r4 or ISO 27001 are well understood. The organization must carefully assess who is responsible for which decisions, actions, and ultimately who is accountable for application of controls in the SDE. The enterprise team must identify, as aligned to the first step of the NIST process, determining what is, what should, and what should not be located in a cloud service.

NIST has been woefully behind in adapting the controls of 800-53r4 to include the cloud. In fact the last update of the NIST Cloud Security Definitions nearly a decade from the date of this paper. Fortunately the Cloud Security Alliance provides its Cloud Controls Matrix as a start point for organizations. The CCM has 13 domains and over 130 controls. (Cloud Security Alliance, 2019) However, after a review of the CCM there are opportunities for Information

Security professionals to contribute more controls and best practices from their body of knowledge.

One proposed method to determine the appropriate controls is via the use of threat modeling. Threat modeling, a discipline within itself, invokes a great deal of debate of the "right method." A commonly accepted approach to threat modeling is the STRIDE method developed at Microsoft by Loren Kohnfelder and Praerit Garg. (MICROSOFT, 2007) STRIDE is an acronym composed of:

- Spoofing
- Tampering
- Repudiation
- Information Disclosure
- Denial of Service
- Escalation of privilege

InfoSec professionals may use STRIDE to evaluate virtual and physical system components. The STRIDE process assists in selection of controls, prioritization of monitoring resources, and should align to the aforementioned policy guidance as part of a holistic enterprise risk management program. Contract enforcement is an additional control if the necessary specifications, responsibilities, and actions are clearly stated. The reader is challenged to keep the NIST process as well as STRIDE model in mind during the remaining treatment of "cloud" and Software Defined Environments. Is there a STRIDE threat vector to the chosen service? If so, who should be responsible and accountable for its mitigation? How and who should and will monitor, respond and recover the service?

Cloud Computing Definitions

First in any discussion is the agreement on terms and concepts that will remain common throughout this discussion. Technical personnel and marketing professionals are equally as guilty of using multiple terms in an attempt to differentiate various solutions. This initial discussion shall do quite the opposite and group like items into broad categories of characteristics then provide a more detailed treatment of current SDN implementations.

The characteristics of cloud systems will aide in conceptualizing and assisting in the selection of cloud services and controls. NIST SP 800-145 lists-five characteristics of cloud computing. All attempts to paraphrase the characteristics induced a loss of specificity, clarity, and impact. The five services verbatim are:

On-demand self-service	A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider
Broad Network Access	Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).
Resource Pooling	The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be

	able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, and network bandwidth.
Rapid Elasticity	Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.
Measured Service	Cloud systems automatically control and optimize resource use by leveraging a metering capability1 at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service

(NIST, 2011, p. 2)

Remaining consistent with NIST's lexicon are three service models. It is posited that additional services are required; such as Security As A Service. However, this author recognizes that opinions on what degree of abstraction is likely different amongst all practitioners. NIST SP800-145 three service abstraction models are paraphrased bellow.

Software As A Service (SAAS) is a model where customers access software operated by a provider. This is generally via a web browser or an application program interface. In the SAAS service model the consumer does not own and operate the underlying support infrastructure for the program. (NIST, 2011, p. 2)

The Platform As A Service (PAAS) model allows the customer to deploy applications and services in the provider's cloud. This is normally done using provider owned and maintained libraries and application programming interfaces. The underlying infrastructure is owned, operated, and maintained by the provider. The customer is likely responsible for maintenance of the deployed applications. (NIST, 2011, p. 2)

The Infrastructure As A Service (IAAS) model allows the customer to deploy infrastructure such as servers, hosts, and applications in a virtualized environment. Traditionally, the customer is responsible for installation, operation, and maintenance of deployed systems. The provider is maintains the underlying virtualization environment. (NIST, 2011, p. 3)

NIST SP 800-145 additionally defines four deployment methodologies. First, a private cloud that is for the exclusive use of one organization or tenant. Second, a community cloud where multiple tenants share the cloud and its resources. Third, the public cloud where the general public may provision necessary resources. Finally, a hybrid cloud that is a composition of more than one cloud. (NIST, 2011, p. 3) The InfoSec professional quickly begins to detect blurring trust boundaries, complex topologies, and convoluted information flows depending on the deployment methodologies.

NIST's SP800-145 "Definition of Cloud Computing" was last updated in September 2011. The document, although likely requiring update, provides an approach to extend the foundational concepts. A likely extension to the cloud offerings of IAAS, PAAS, and SAAS is Software Defined Networking SDN. Discussions on the internet abound debating if SDN is a component of IAAS or is domain of its own. As previously mentioned one may observe the adoption of cloud and software defined capabilities in part or whole to create software defined environments.

Software Defined Networking

SDN is focused on separating the control plane of the networking devices from the forwarding plane. Additionally, SDN is flow based vice packet based with software determining the delivery of data to nodes. SDN promises scalability, micro-segmentation, elasticity and potentially greater security by separating the forwarding, control, and management planes. (Krishnan, Duttagupta, & Achutan, 2019)

SDN Characteristics

The IBM Software Defined Environment lists five benefits of software defined networking.

SDN is:

- **Directly Programmable**

The network is programmable as the forwarding and control are decoupled as opposed to tightly coupled as they are in traditional network devices.

- **Agile**

The network can be adjusted based on flows network wide to meet network scaling issues.

- **Centrally Managed**

The network appears as a single unified system to the SDN controllers ensuring a global view and holistic configuration.

- **Programmatically Configured**

Network managers access and configure the network via application programming interfaces to SDN programs vice directly to the network hardware be it virtualized or physical.

- **Open Standards Based and Vendor Neutral**

Open Standards are readily available and embraced by vendors. This allows a multi-vendor instating of the network yet remain configured from the central controller

(Quintero, et al., 2015)

SDN Objects

SDN may be thought of as virtual or physical objects that either control or forward network traffic. These objects are controlled in "planes" which are collections of functions. Finally, abstraction layers provide the access between the various interfaces. A brief definition of each is provided below with a final graphical depiction in figure four.

RFC 7426 provides concepts for the grouping of what this treatment discusses as objects.

SDN Objects

Network Device	Physical or virtual device that performs one or more packet manipulation or forwarding tasks
Interface	Point of interaction that may be implemented via Application Programming Interface (API), Inter-Process Communication (IPC), or a network protocol
Application	A standalone piece of software that although parameterized does NOT expose interfaces to other applications or services
Services	Software that performs functions to support forwarding or control via exposed interfaces or APIs.

SDN Planes

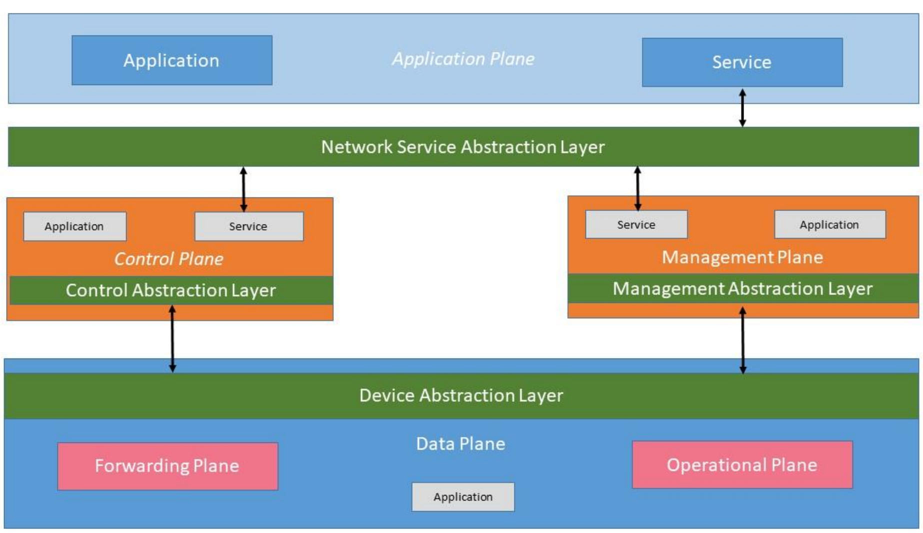
Forwarding Plane	All resources across all network devices that forward traffic

Control Plane	All functions across all network devices that instruct those devices how to process and forward traffic
Operational Plane	The resources responsible for the operation of the network devices such as active and inactive states
Management Plane	Functions responsible for the configuration, operation, and maintenance of the network device
Application Plane	The entirety of the applications and resources that program network behavior.

SDN Abstraction Layers

Device Abstraction Layer	Abstraction of network devices
Control Abstraction Layer	Provides access down or “southbound” from the Control Layer to the Device Abstraction Layer
Management Abstraction layer	Provides access down or “southbound” from the Management Layer to the Device Abstraction Layer
Network Abstraction and Services Layer	Provides high level abstraction to top level applications and services obfuscation network operations

Figure 4- SDN Architecture as per SP 800-145



(RFC 7426, 2015)

The separation of the control and forwarding plane has the advantage of using a controller that manages and the configuration of networking devices be they completely virtualized in software or SDN enabled hardware. However, this centralization imposes a responsibility to adequately protect and monitor the controller. Configuration interfaces, often exposed as web portals, suffer the same threats as other web applications. Multiple vendors may have various objects, services, all expected to operate in harmony with other vendor implementations. This implied trust between vendors must be enforced with controls as exposed in the earlier STRIDE analysis.

The use of a cloud service provider's Intrusion Detection system is akin to stepping on an airplane; one has limited knowledge of conditions and even less control. If a hybrid deployment with both on and off premise services the network is only as secure as the most vulnerable surface. NIDS and HIDS must be carefully planned in the cloud much as in a fully on premise solution. Complicating the issue is who configures, what the alerting processes are, and what actions re taken when. It may be posited the contracts with cloud service and software defined providers may be one of the most important security documents in the enterprise. The contracts, level of investment, and risk profile must match the initial guidance as discussed in the opening of this paper. A cloud instantiation of an IPS/IDS is beyond the scope of this paper. However cloud IDS/IPS in likely next area of examination in the exploration of the Software Defined Environment in a cloud environment. The placement of sensors in an SDN as well as protocol selection create a complex challenge for InfoSec professionals. Is Security As a Service far on the horizon or near?

CONCLUSION

This short treatment of software and cloud resources forces on enterprise security provides only a basic exposure to a more complex problem set faced by the modern InfoSec practitioner and corporate leadership. Through literature review there are gaps in the update of various NIST documents. It is recommended that cloud controls and risk be integrated into NIST documents vice separate documentation. It is unlikely that wholesale adoption of any framework will create security. It is the underlying analysis and actions that result in security. The analysis will likely be enforced as a security control via contracts and service level agreements. Tools such as STRIDE, implemented in accordance with a framework of continual improvement, and a deeper understanding of how technology supports business goals that InfoSec practitioners will improve their enterprise.

Recommendations for further research:

- Software Defined Networking protocols and their vulnerabilites
- Optimization of Intrusion Detection System sensors in SDEs
- Establishing trust between SDN enclaves with public key encryption
- Impacts of block-chain technology on trust in the SDE
- Best practices in contracting service agreements with cloud service providers

Works Cited

[NIST Cybersecurity Framework]; NIST. (2018, February 12). [NIST Cybersecurity Framework]. *Framework for Improving Critical Infrastructure Cybersecurity*. National Instiitute of Standards and Technology.

[NIST SP 800-53] NIST. (2013). *Recommended Security Controls for Federal Information Systems and Organizations*. National Institute of Standards and Technology. Retrieved from http://csrc.nist.gov/publications/PubsSPs.html

Abdou, A., Van Oorschot, P., & Wan, T. (2018). Comparative Analysis of Control Plane Security of SDN and Conventional Networks. *IEEE Communications Surveys and Tutorials*, 3343-3559.

Cloud Security Alliance. (2019 , July 30). *Cloud Controls Matrix.* Retrieved from Cloud Security Alliance: https://cloudsecurityalliance.org/research/cloud-controls-matrix/

Haleplidis, E., Denazis , S., Pentikousis, K., Salim, J., Meyer, D., & Koufplavlou, O. (2014, September 4). IETF DRAFT - SDN Layers and Architecture Terminology.

Internet Engineering Task Force. (2015, January). RFC 7426. *Software-Defined Networking (SDN): Layers and Architecture Terminology*. Internet Engineering Task Force.

Krishnan, P., Duttagupta, S., & Achutan, K. (2019). VARMAN: Multi-plane security framework for software defined networks. *Computer Communications*, 215-239.

MICROSOFT. (2007, Sep 11). *Stride Chart.* Retrieved from Microsoft Security: https://www.microsoft.com/security/blog/2007/09/11/stride-chart/

MITRE. (2019). *Systems Engineering Guide.* Bedford, MA: MITRE.

NIST. (2006, October). [NIST SP 800-100]. *Information Security Hanbook a Guidebook for Managers*. Washington, DC: National Institute of Standards and Technology.

NIST. (2011, September 2011). NIST SP800-145. *NIST Definition of Cloud Computing* . Gaithersburg, MD: National Institute of Science and Technology.

NIST. (2018, February). NIST Special Publication 500-322. *Evaluation of Cloud Computing Services Based on NIST SP 800-145*. National Instiitute of Technology.

Open Networking Foundation. (2014, November). SDN Architecture Overview. Palo Alto, California: Open Networking Foundation.

Quintero, D., Genovese, W., Kim, K., Li, M., Martins, F., Nainwal, A., . . . Tiwary, A. (2015). *IBM Software Defined Environment (RedBooks).* Poughkeepsie, NY: IBM.

SANS. (2019, Nov 3). *Information Security Policy Templates*. Retrieved from SANS: https://www.sans.org/security-resources/policies/general#acceptable-encryption-policy