SDN & IBN Assignment

CMIT 495: Current Trends and Projects in Computer Networks and Security

[BART BARTLETT]

By:

[ALVIN SARKADI]

Introduction to software-defined networking (SDN)

SDN is widely used and adopted for organizations with a significant network architecture. SDN provides seamless security and management through defined policies and uses software applications that are intended to automate the process of network security, management, configuration, and optimization.

During the initial steps of deploying SDN to your network infrastructure, the SDN controller and application layer is separated but used together to maintain a high network security posture. The SDN controller enforces policies that should be defined and configured in the application layer. These policies can be anything from update ring policies, user policies, group policies, security, firewall policies and more.

The application layer in SDN is often referred to the software used in the network topology that defines the configuration policies for the SDN controller. In the application layer, policies will be defined. The purpose of the application layer is to manage future interactions with the controller. Once the application layer configures and defines policies, the application layer and controller

layer work together. The controller layer and application layer are used for logical network management and ensuring optimized security.

Introduction to intent based networking IBN

Sometimes people confuse IBN and SDN networking because of its similarities. However, there are key differences in IBN that SDN networks do not introduce. The key aspect of IBN networking is ‘intent.’ Intent in an IBN network infrastructure is defined by the desired outcomes made in all policies in the organization. IBN uses machine learning and artificial intelligence to cover the intent over the network. Intent can be seen as a way of implementing automated security. However, users and administrators of the organization must set the ‘intent’ / the organization’s desire of the policy. Once an ML algorithm knows the intent of each policy configured by an end user, administrator, cloud engineer, etc. Network automation, awareness, and optimization can be delivered through using an IBN network infrastructure. According to several sources, an IBN infrastructure offers real time network status for whichever systems are included in the network and have a defined specific intent. Additionally, for optimization, the network validates whether the set intent by the organization is being met and can make actions to deliver optimization over the network. (Lerner, 2017). “One common misnomer is that the network, or infrastructure, must be intelligent enough to interpret intent. This is false. The infrastructure needs to be able to consume intent, not interpret or define it. Intent is already understood in business logic. The infrastructure should be able to consume that and automate configuration based on that business logic intent.” (Joe, 2018). Since Intent based networking uses machine learning to enhance the overall network security posture, there is a common misconception of how it can be used effectively. In order for these machine learning algorithms

to work, set principles, in this case ‘intents’ in policies must be created to have an optimized and postured network security.

Discussion on how virtualizing the desktop and now back-end infrastructure are complementary and related

Virtualization in a back-end infrastructure environment has many benefits that an organization would consider significant. One of the obvious benefits is cost savings, by using virtualization for the back-end servers, there are no physical costs for physical servers, server racks, cabling, cable management, transportation of physical hardware to designated server regions and more. Platforms such as AWS offer the creation of EC2 instances. EC2 instances are made to be virtual servers and desktops, an end user can choose from a variety of server operating systems.

When virtualizing both desktops and the back-end infrastructure, an organization can achieve unified management across the network. This is especially important for pushing updates, monitoring the network, and device and user activity. Furthermore, this also reduces the need for administrators to manually check network security, push updates to devices and more. Using centralized management, more automation can be deployed across the existing network infrastructure.

When virtualizing the back-end servers, better disaster recovery efforts can be made. For example, when using virtualization in AWS, vast amounts of ability zones are available so there is no single point of failure. Virtualized servers and desktops such as EC2 instances can be made available over several zones, making disaster recovery unnecessary. AWS also offers ‘Amazon Machine Images’ within EC2. This creates a second copy of the instance with the same

configuration settings, in case the original EC2 instance is unobtainable. It is evident that virtualization for both the desktop environment and server environment can be effective and provide efficiency to the organization.

How SDN and IBN are related.

One of the key relations between the two is that both can be used to achieve an organization's intended network needs. IBN doesn't use physical hardware, instead it relies on an existing network infrastructure. IBN can be applied and integrated with SDN network infrastructures to create a more secure network environment.

Another key relation they share when integrated is efficiency. The SDN's application and controller layer reduces manual configuration once policies are enforced, IBN furthers automation processes made by intents set in the policies.

Within a large organization, implementing both network methods can enforce network security, create a more seamless management experience, and create crucial backup methods in instances of natural disasters, network, cyber-attacks, internal attacks, virtual hardware failures or human errors. I also believe a company should adopt a zero-trust concept when creating policies within the network. This will ensure that the IBN will detect such instances in an automated manner, making the organization less prone to attacks across all devices and the network.

References

Lerner, A. (2017, February 7). Intent-based networking [Blog post].

https://blogs.gartner.com/andrew-lerner/2017/02/07/intent-based-networking/

Joe, O. (2018). Intent-Driven Architectures: What Is Intent? - CMIT 495 6393 Cybersecurity Technology Capstone (2248). Umgc.edu.

https://learn.umgc.edu/d2l/le/content/1327469/viewContent/33534659/View

Taimur, B. (2017). Intent-Based Approach CMIT 495 6393 Cybersecurity Technology Capstone (2248). Umgc.edu

https://learn.umgc.edu/d2l/le/content/1327469/viewContent/33534658/View

Acadia Technology Group. (2019). *How to Build a Next Gen SDN & IBN*. Acadia Technology Group. https://www.acadiatech.com/blog/build-sdn-ibn-network/

Amazon(2024). Machine Images in Amazon EC2 - Amazon Elastic Compute Cloud.

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/AMIs.html

