Software-Defined Networks: Audit & Compliance

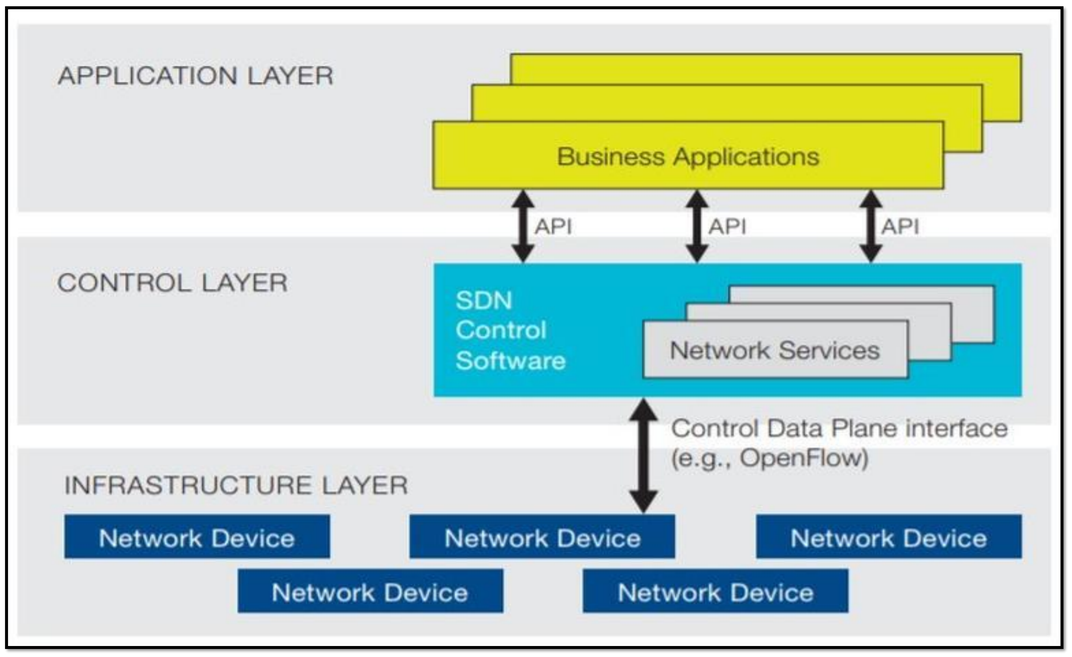
Mohamed Dandachi, Computer Information Systems

Mentor: Dr. Ronald Pike

Kellogg Honors College Capstone Project

What are Software-Defined Networks? (SDN)

SDN is the physical separation of the network control plane from the forwarding plane, and where a control plane controls several devices. This is a type of architecture that aims to make networks agile and flexible. It accomplishes this by having a "controller" at the top of the network infrastructure that allows for central management. This form of central management allows network staff to manage, secure, and optimize network resources via SDN programs that can be written by anyone. Controllers are open standards-based and vendor-neutral, with the main goal of improving network control by enabling business service providers to respond quickly to changing business requirements.



The Importance of Audit & Compliance

For an organization to remain viable in a constantly changing world with new forms of risks, an audit is essential. An audit provides objective insight that is independent and unbiased, giving the ability to find better solutions to business processes. Audits also improve the efficiency of operations by routinely monitoring and reviewing processes, allowing for identification of control recommendations to improve the processes. An audit is vital for an organization to evaluate risks and protect their assets.

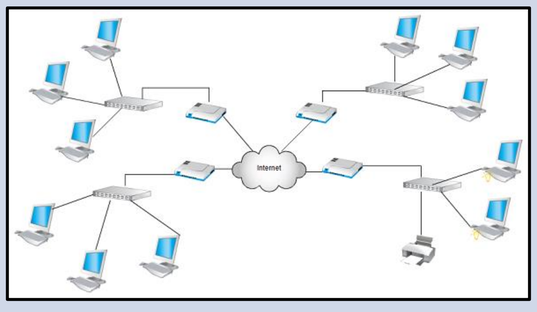
With an audit comes a risk assessment, which evaluates risks and helps to identify any gaps in the process and allow for a remediation plan to take place. An audit will also assess an organization's controls, with the goal of improving the control environment of the company by assessing efficiency and operating effectiveness. The biggest reason organization's undergo audits is to ensure compliance with laws and regulations. Clients and customers trust organizations that have a history of compliance, not to mention that an organization meeting compliance means the avoidance of costly fines that are associated with non-compliance.

Current Benefits of SDN

- Centralized network provisioning
  - Provision both virtual and physical network devices from a central location.
- Flexibility
  - SDN controller assumes most complex functions, so devices don't need to understand how to execute data flow based on different protocols from different vendors.
- More granular security
  - Intelligent response blocks malicious traffic while still allowing normal traffic flows.
- Anomaly detection
  - Diverts suspicious network flows to special enforcement points (firewalls).
- Network modification
  - SDN controller is the brain, so it's much easier to modify the controller than manually reconfigure every network device.

Auditing a Legacy Network

- Auditors would audit all parts of the network that would fall under the compliance scope.
- Auditors work with stakeholders (management and technical team) to determine their amount of access to the network.
- Auditors go through appropriate network equipment to gather evidence and data for their audit.
- Auditors then compile a final report and provide recommendations based on their findings.
- Would take a significant amount of time and money to thoroughly complete an audit.
- Meeting compliance can be incredibly costly and take time especially if a major policy or network overhaul was needed.



Point-in-Time Auditing

- Auditors gather data and information for certain parts of the year at a time.
- Example: First audit is done during June and July for all data that has been gathered between January and May. The audit period would be January – May, which is point-in-time auditing.
- This method of auditing is typically done twice a year.
- Not the best approach, because a control can be fine up until the first audit but have issues right after.
- Example: An issue wouldn't be seen or resolved on an audit until a few months later, putting the organization at risk.
- Can't do real-time auditing with legacy networks as an organization would need an enormous and costly audit staff, which is impractical.

Auditing a Software-Defined Network

- Much more simplified than a legacy network audit.
- No need for auditors to audit the entire or big portions of the physical network.
- With the SDN controller being the brains of the network and making the important decisions, auditors only need to audit the controller.
- Auditing only the SDN controller saves a significant amount of time and money.
- Instead of having to work with physical networks, everything's controlled via software.
- To meet compliance, organizations can define specific rules in the software itself.
- In doing so, organizations are compliant within a few days versus months.

Real-Time Auditing

- Real-time auditing is possible with SDN as it's easier and automated, without the need for extensive staff.
- Real-time auditing allows for continuous improvements and recommendations throughout the year (as opposed to a few times a year under the point-in-time system)
- Provides an increase in security and minimizes company risk.
- Example: Firewall misconfiguration that occurs right after an audit in a point-in-time system could be up for months before being found in the next audit.
- In real-time, the audit and compliance dashboard would be populated with the issue, making it known quickly.

SDN Audit & Compliance Dashboard

- With a more holistic and simplistic way of looking at the network, SDN could make a network audit and compliance dashboard possible.
- Audit & Compliance Dashboard would constantly communicate with the SDN controller to provide real-time data.
- Makes tracking, managing, and monitoring audit data and information in real time more streamlined and easier.
- Helps in automating the audit process with real-time alerts to issues and problems.
- Constantly test network controls 24/7 instead of a few times a year.