Software Defined Networking

SDN and Cloud Security

Aziz Al-Qwati | Cybersecurity Engineer

Agenda

- Introduction
- Traditional vs. SDN Architecture
- How SDN Works
- SDN in Virtual and Cloud Environments
- SDN Use Cases
- SDN and Cloud Security
- Summary and Q&A

Software defined networking (SDN)

- is an approach to network management that enables dynamic, programmatically efficient network configuration to improve network performance and monitoring.

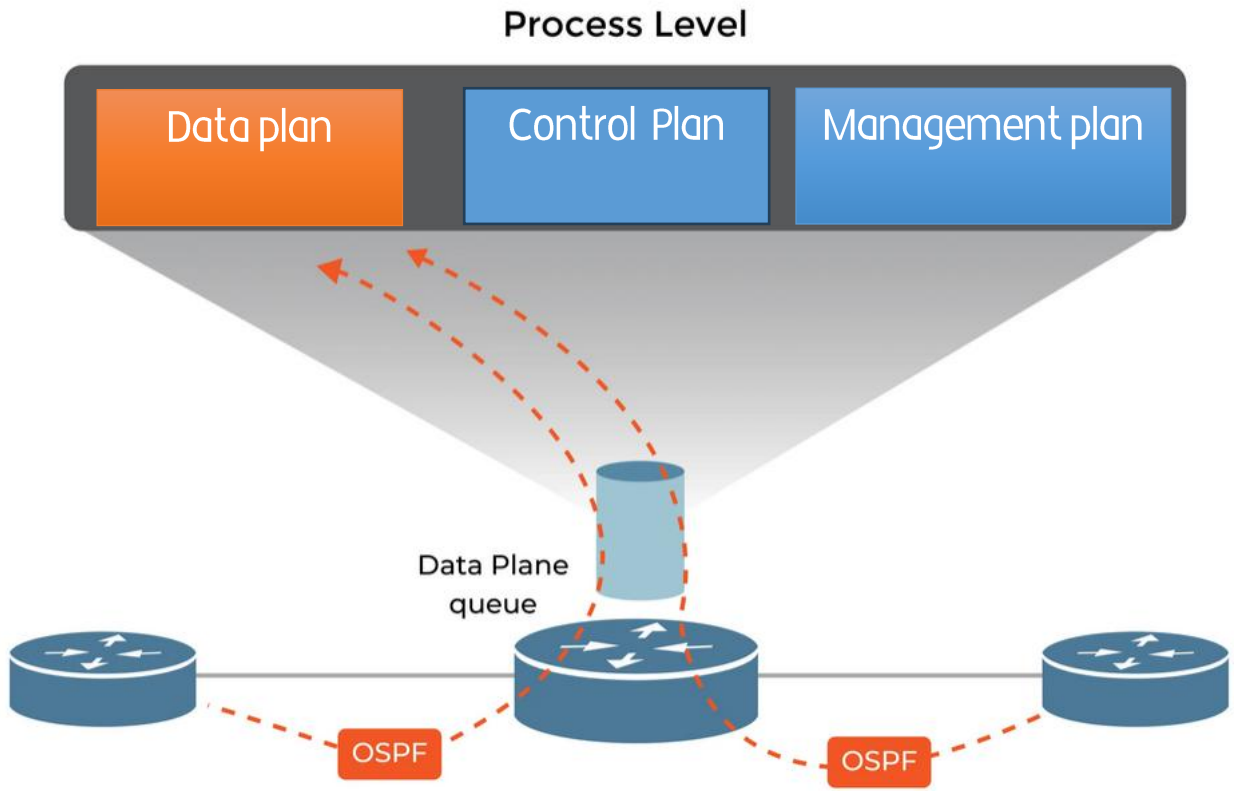
  Use Cases:
  - Data center networks
  - Network automation and orchestration
  - Traffic engineering
  - Network slicing in 5G
  - Enhanced security via dynamic flow rules

- But, How?!!!

Traditional networks (Internal operations)

- The hardware (like routers and switches) decides how data moves through the network.

- Each switch/router has its own control logic (firmware).
- Configuration is done **manually** per device using CLI.
- Hardware **dictates** behavior — it's static and vendor-locked.



Traditional networks (Internal operations

In a traditional network, each switch has its own control plane and data plane. Switches exchange topology information to build a forwarding table that decides where to send data packets

Tight coupling of control and data plane limits flexibility

Manual configuration leads to high operational overhead

Difficult to scale in large, dynamic environments

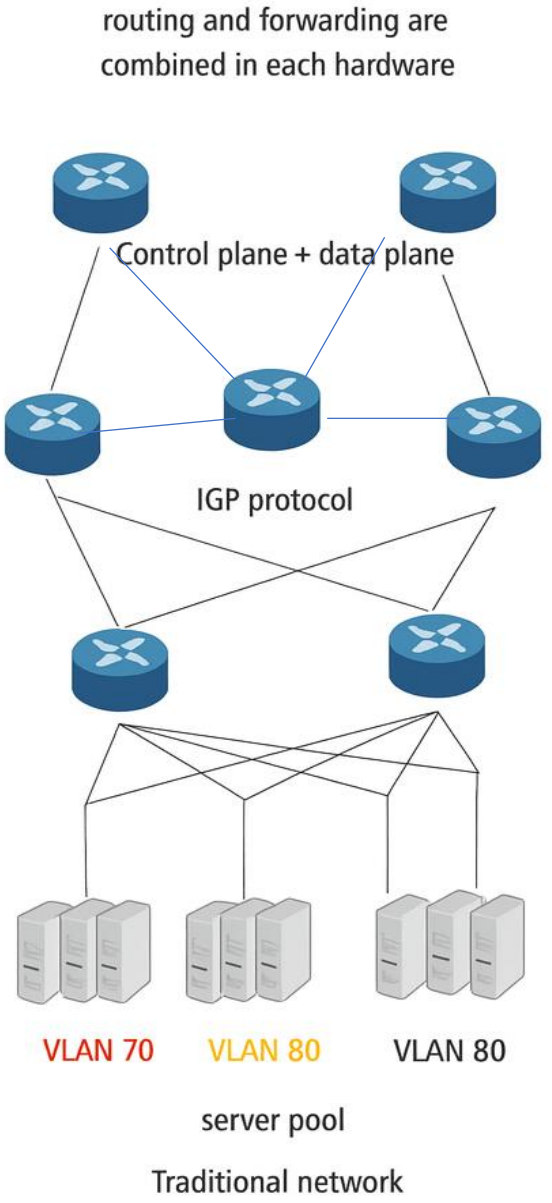
Lack of centralized control makes automation hard

Slower response to network changes or failures

Limited programmability and innovation

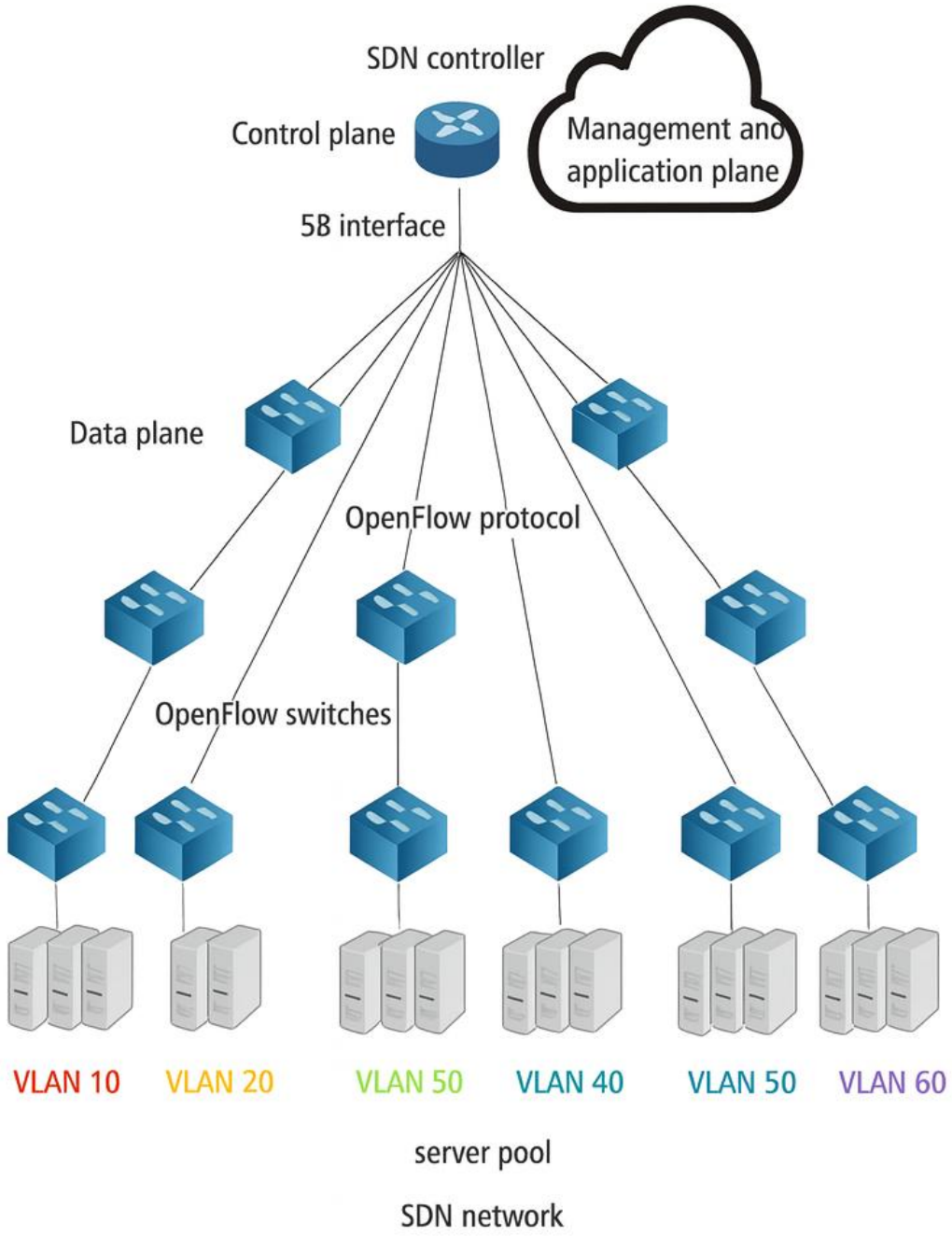
Vendor lock-in due to proprietary hardware/software

Troubleshooting is complex and distributed



SDN

- Control logic is moved to a central controller. (software).
- Switches and routers are simplified to just forward packets (data plane).
- Network behavior (routing, security, QoS, etc.) is defined via software APIs.



SDN–In short

Why is it called "Software-Defined" Networking (SDN)?

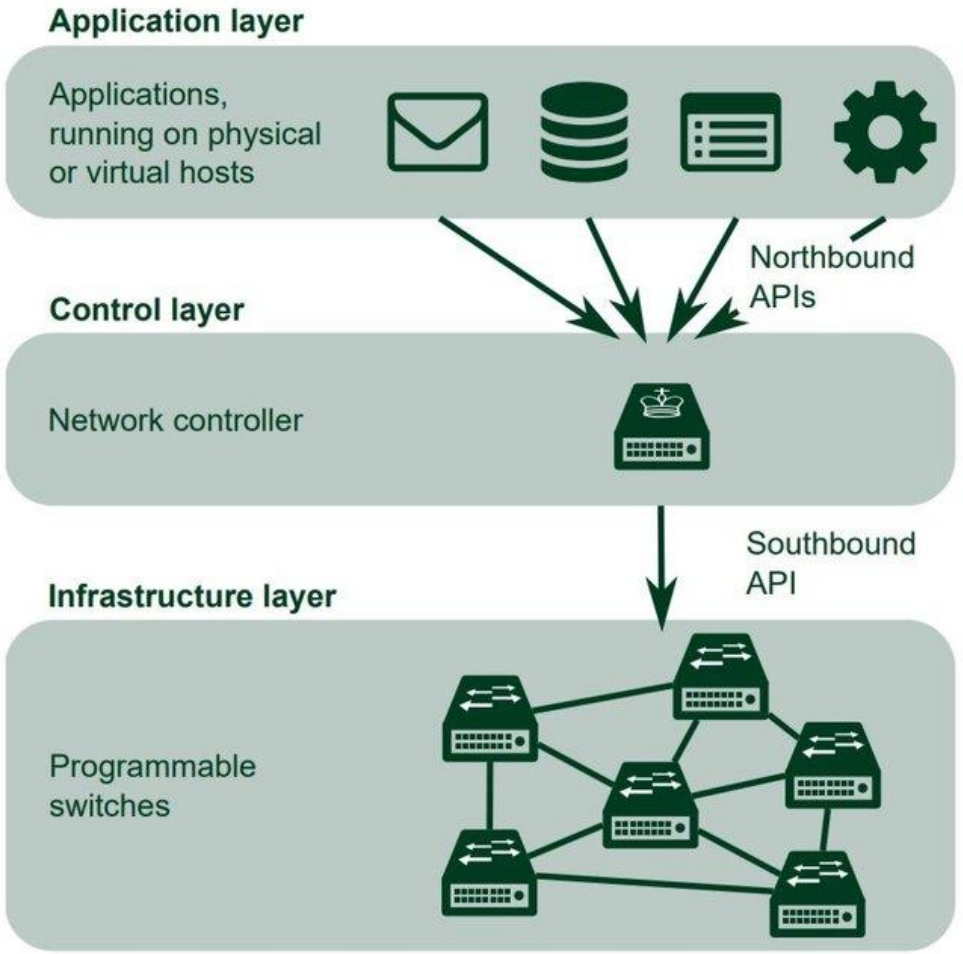
- Because in SDN, the behavior of the network is defined and controlled by **software**, rather than being hardcoded into hardware devices like traditional routers and switches.

"Software-Defined" Means:

- You can program the network dynamically using code.
- You use software controllers to tell the network what to do.
- Decisions (e.g., how to route traffic) come from a central, software-managed brain, not scattered hardware.

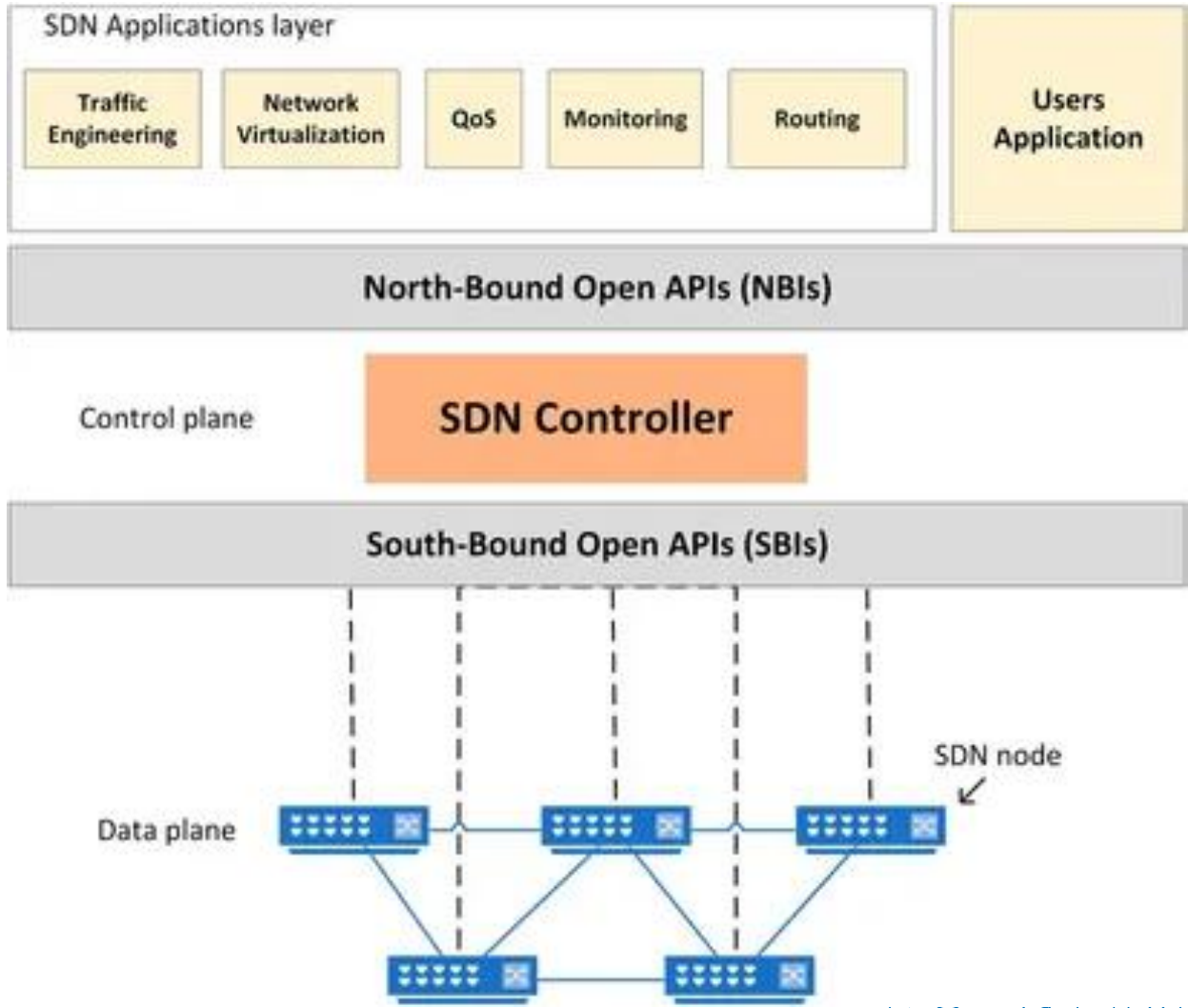
A typical SDN architecture consists of three layers.

- **Application Layer:** It contains the typical network applications like intrusion detection, firewall, and load balancing.
- **Control Layer:** It consists of the SDN controller which acts as the brain of the network. It also allows hardware abstraction to the applications written on top of it.
- **Infrastructure Layer:** This consists of physical switches which form the data plane and carries out the actual movement of data packets.



SDN – Benefits

Centralized control and visibility	Simplified network management	Easy automation and orchestration
Switch hardware becomes cheaper	Enhanced scalability for large environments	Consistent policy enforcement across the network
Improved network programmability via APIs	Easier integration with cloud and virtualization platforms	**Enhanced Security**

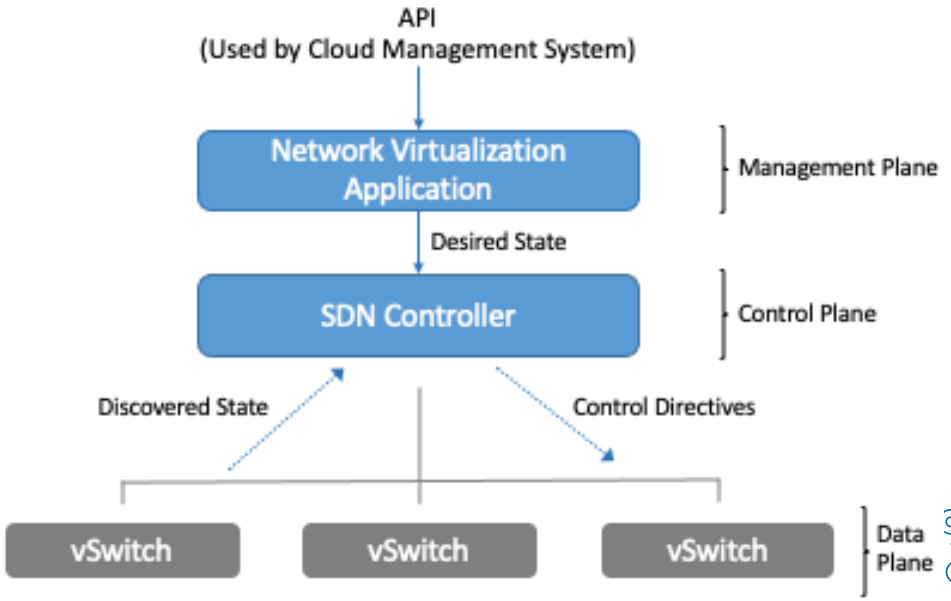


SDN in Virtual and cloud Environments

As data centers and cloud computing evolved, traditional networking couldn't keep up with the dynamic, multi-tenant, virtualized world. Specifically:

- Virtual Machines (VMs) could move between physical servers (live migration), but network configurations were static.
- Manual configuration of switches and routers couldn't support rapid scaling or automation.
- Networking became a bottleneck for automation in cloud environments like OpenStack or VMware.

To solve this, Software-Defined Networking (SDN) was introduced to bring the same **flexibility** to the network layer that virtualization brought to compute and storage.

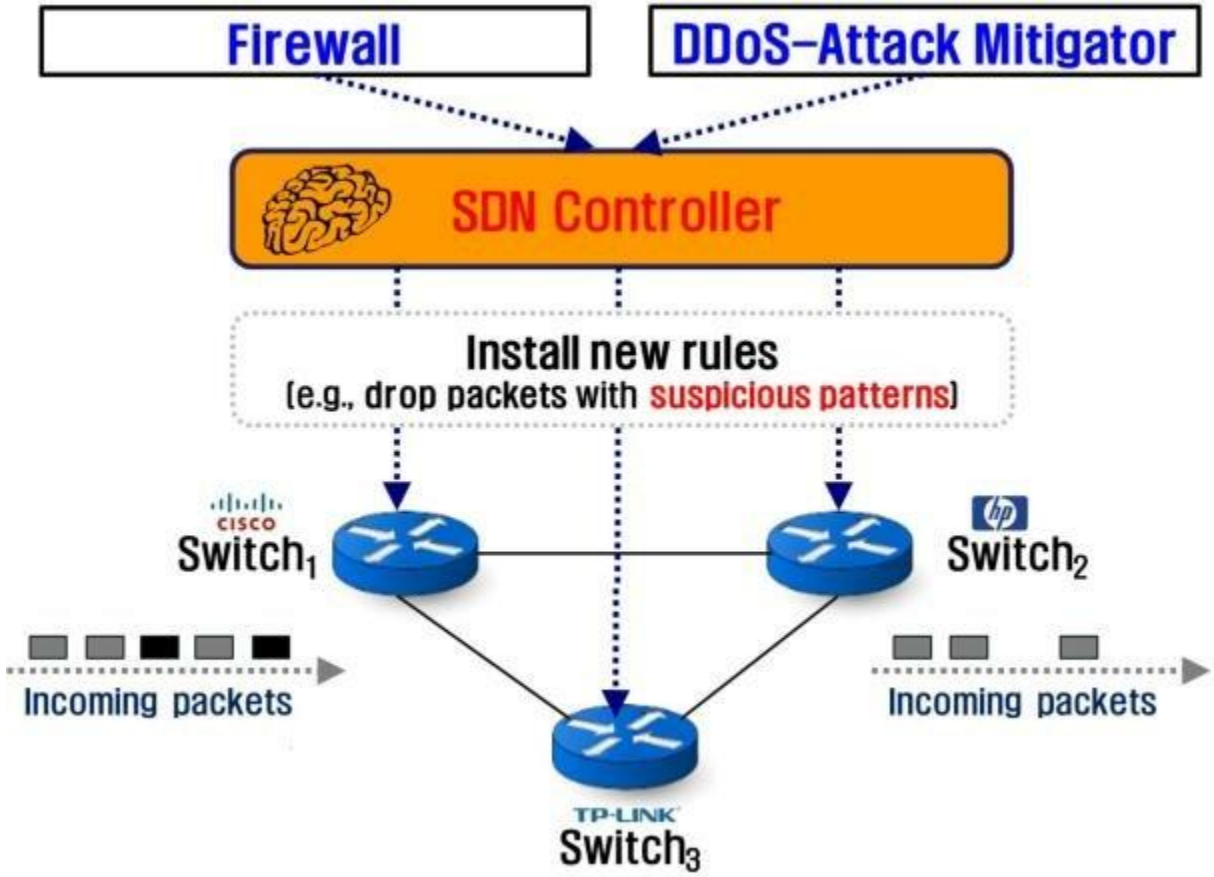


How SDN Works in Virtual and cloud Environments

1. Centralized Control via SDN Controllers
   - Example controllers: OpenDaylight, ONOS, VMware NSX, Cisco ACI
   - They manage routing, firewalls, load balancing—all from software
2. Programmable APIs
   - Cloud orchestration tools (e.g., OpenStack Neutron) use northbound APIs to request networking services from the SDN controller.
   - The controller pushes flow rules via southbound protocols (like OpenFlow) to physical/virtual switches.
3. Network Virtualization
   - Networks are abstracted into virtual switches, routers, and firewalls
   - This enables multi-tenancy, dynamic scaling, and on-demand provisioning

SDN And Cloud security

- Software-Defined Networking (SDN) enhances cloud security by centralizing control, enabling dynamic response, and increasing visibility over the entire virtual network.



SDN And Cloud security

1. Centralized Security Policies	• ACLs, firewall rules, segmentation are defined **once** at the SDN. • Reduces human error and misconfiguration.
2. Dynamic Flow Control	• Suspicious traffic can be **rerouted** to (IDS) or honeypots in real–time.
3. Microsegmentation	• SDN enables **isolation of workloads** (e.g., VM–to–VM).
4. Real–Time Threat Detection and Response	• Controllers can **monitor traffic patterns** and react instantly: • Block IPs
5. Automated Security Policy Updates	• Policies can be updated or rolled back **automatically** through APIs or orchestration tools.
6. Visibility and Auditing	• SDN provides full visibility of the network via telemetry. • Every flow is logged, enabling deep forensic analysis and **audit trails**.
7. Security as a Service (SECaaS)	• SDN offering security features like **DDoS protection**, **firewalling**, and **VPNs** as scalable cloud–native services.

Thanks


سُحبكم
sohobcom
سُحبكم لتقنية المعلومات والحلول الرقمية
Sohobcom for Information Technology and Digital Solutions