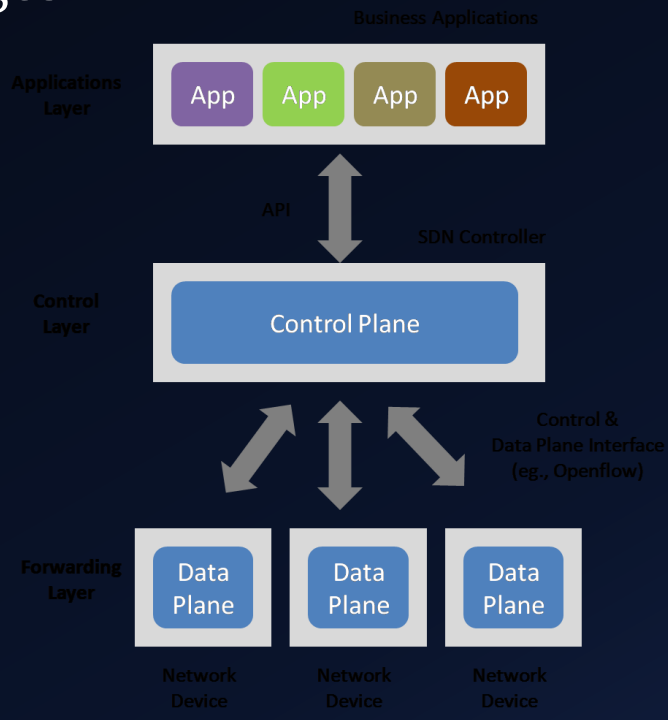
Security in Software Defined Networks using Firewall

JAGRUTI WAGHULDE
3323

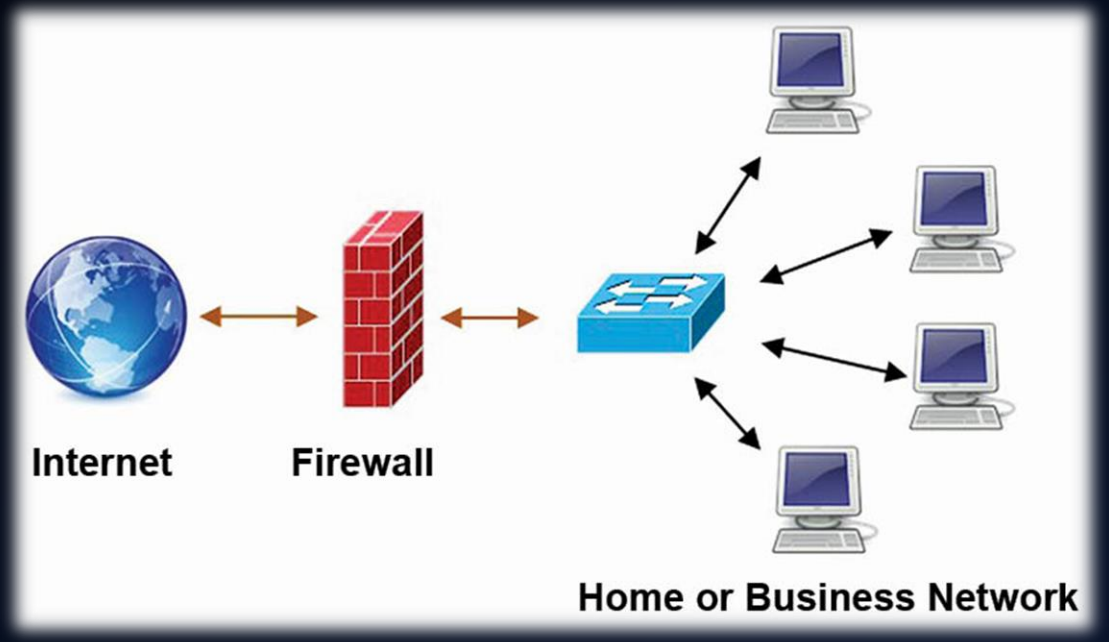
SECURITY CHALLENGES IN SDN :

- SDN is pulling the intelligence away from hardware.
- Separation of the planes opens new security challenges
- Denial of service attacks, man-in middle attack .
- Propagating viruses and worms in the network.



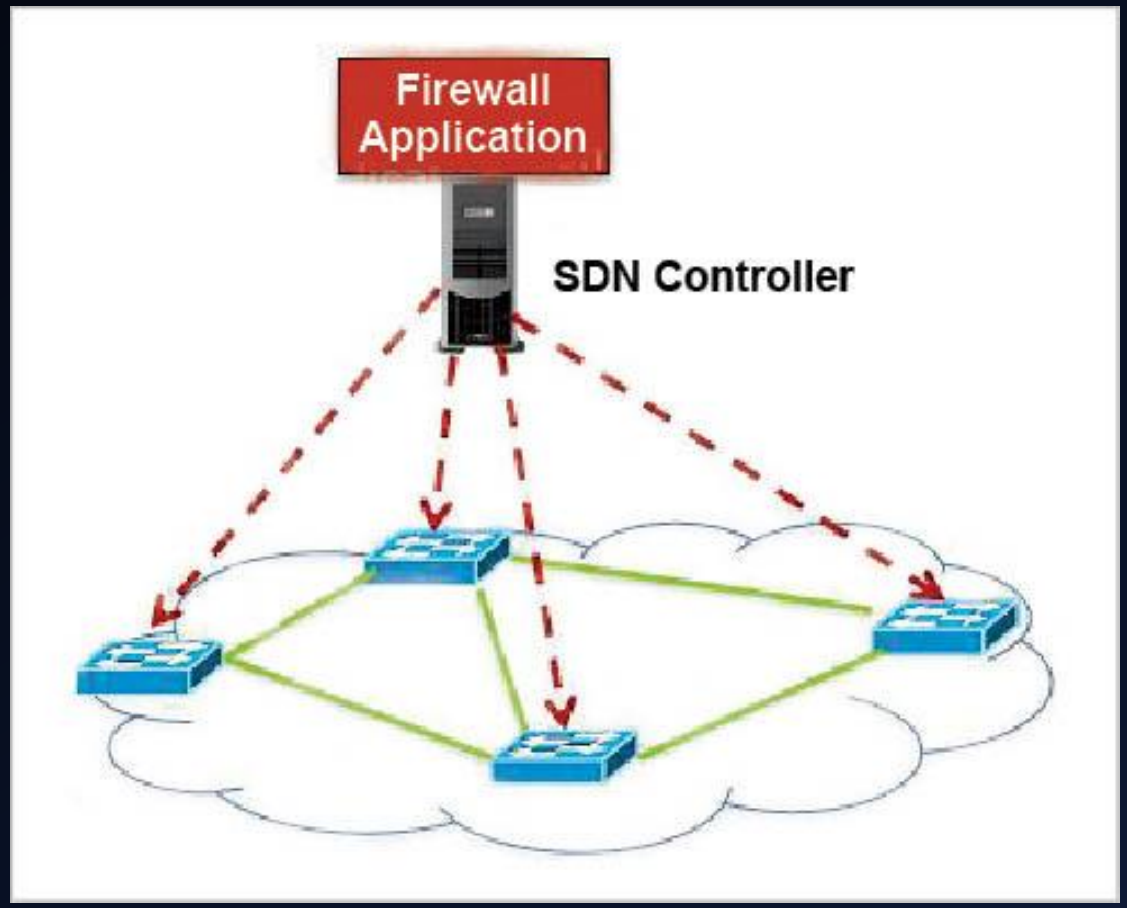
Firewall

- A Firewall is a network security system that is used to control the flow of ingress and egress traffic usually between a more secure local-area network (LAN) and a less secure wide-area network (WAN).

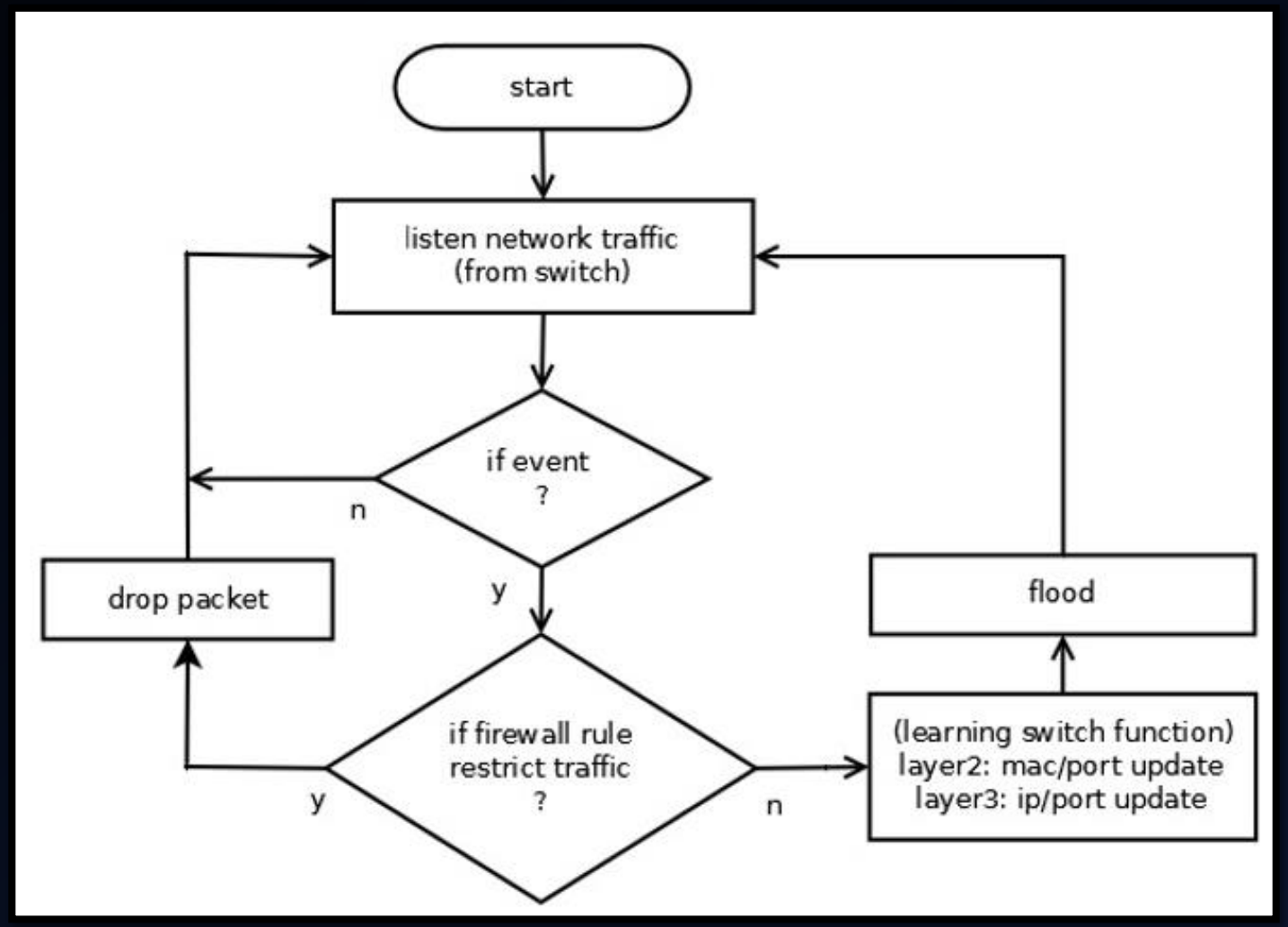


SDN Firewall

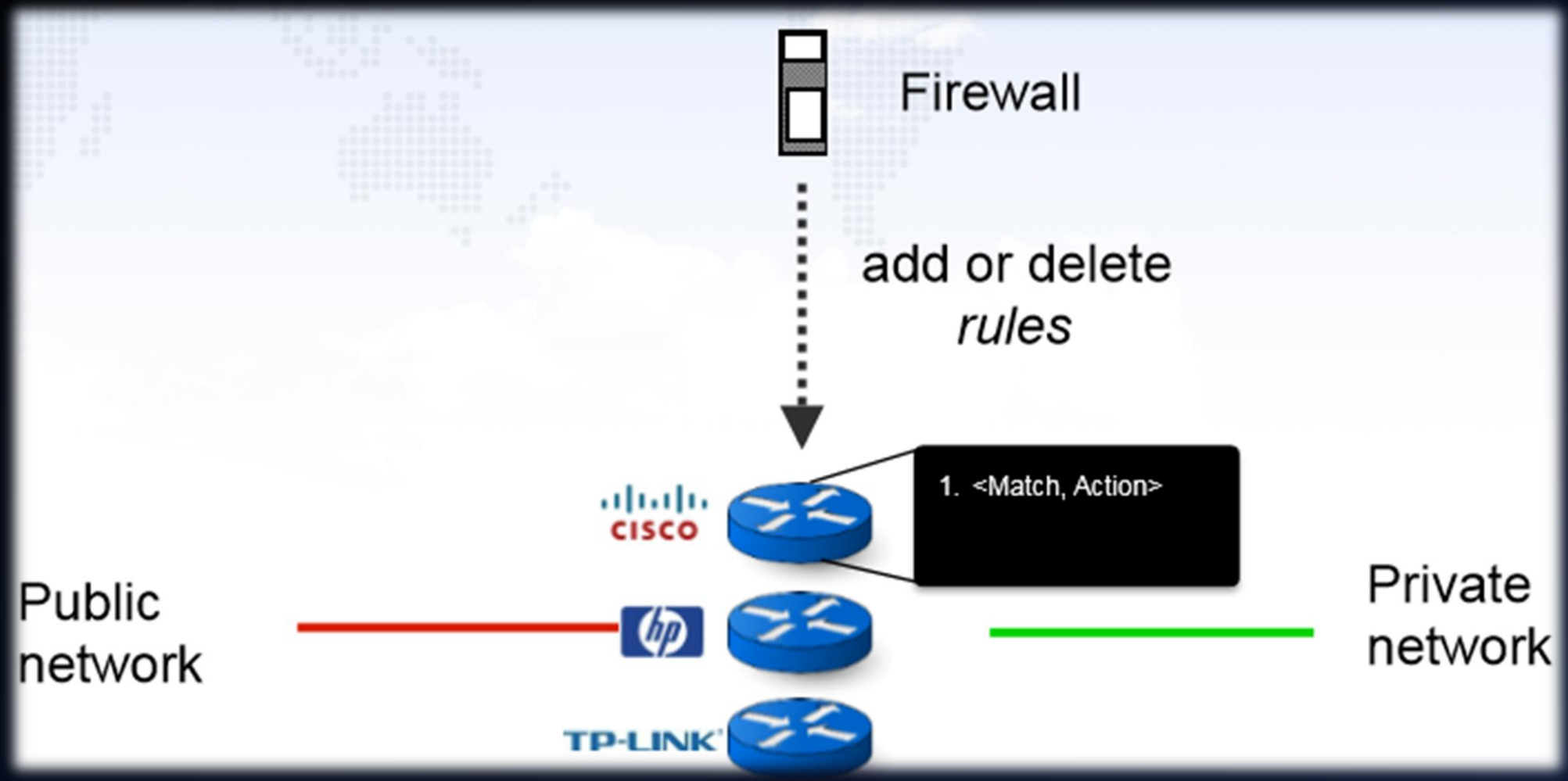
- SDN firewall is writing firewall policies to the central controller to manage, filter and inspect the traffic.
- Internal traffic is not seen and cannot be filtered by a traditional firewall.
- An SDN based firewall works both as a packet filter and a policy checker.
- Firewall rules can be managed flexibly by a centralized server.



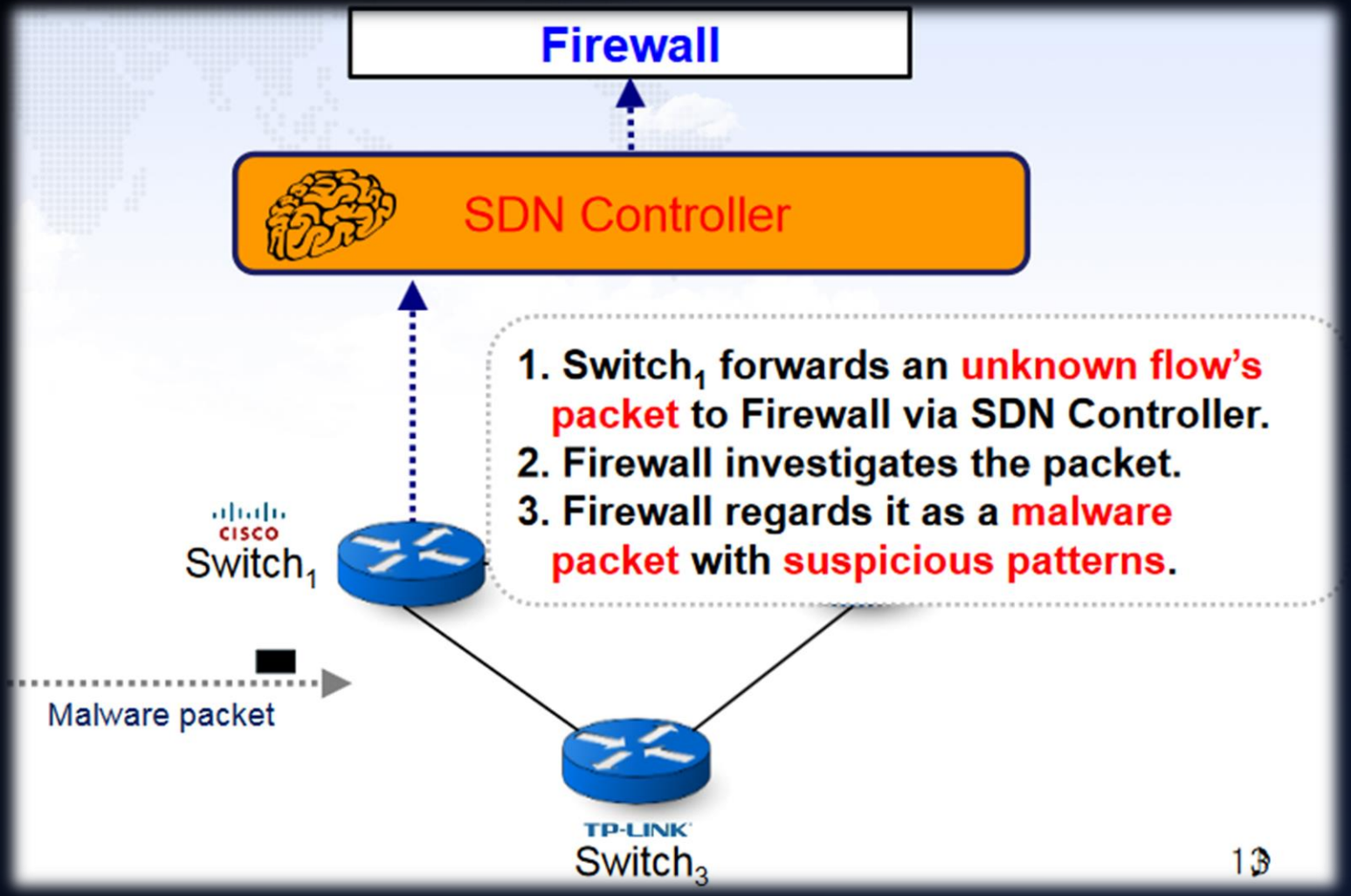
Flow Chart For Implementation Of SDN Firewall :

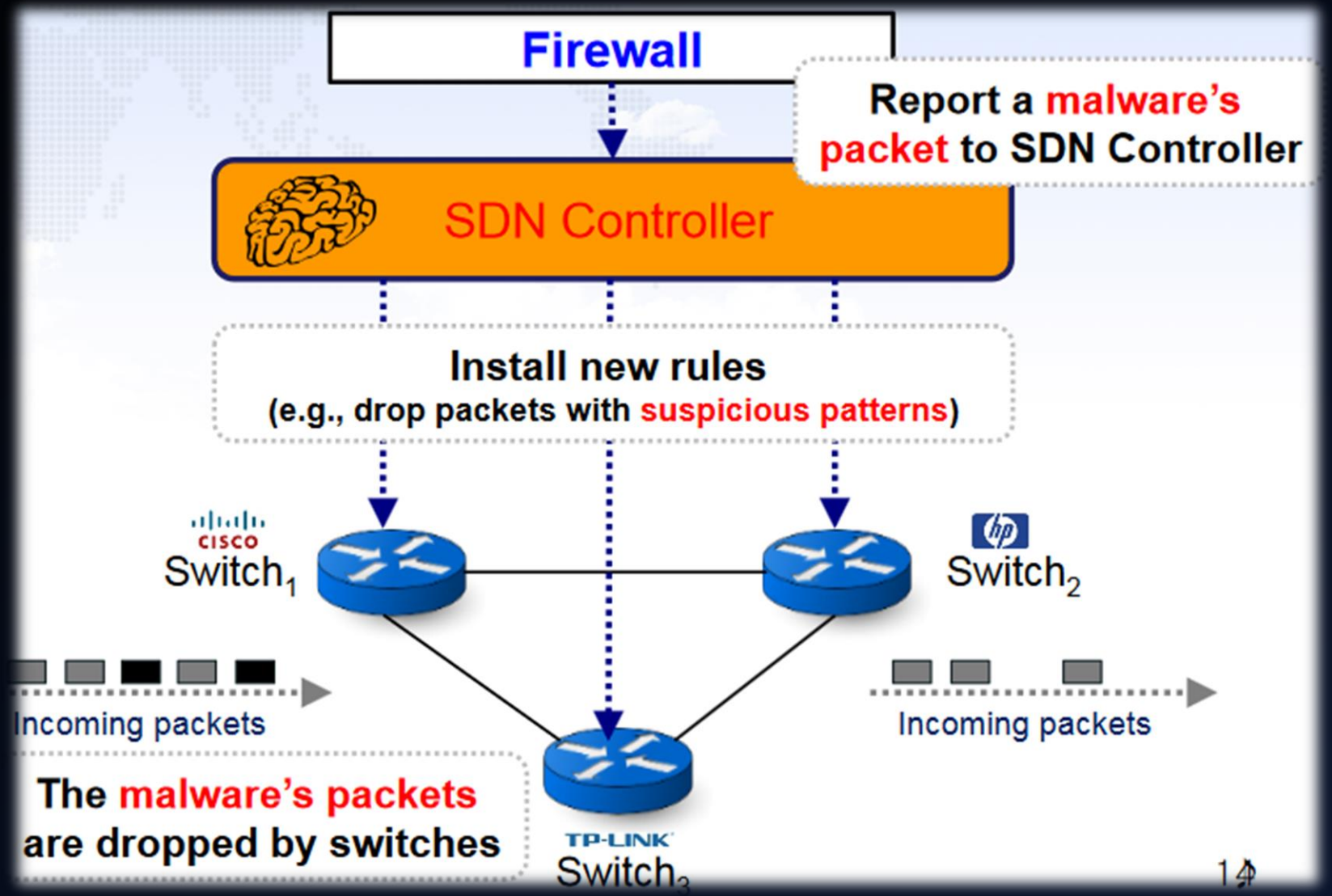


SDN Firewall



Centralized Firewall System




Firewall
Report a malware's packet to SDN Controller
SDN Controller
Install new rules
(e.g., drop packets with suspicious patterns)
Switch1
Switch2
Incoming packets
Incoming packets
The malware's packets are dropped by switches
Switch3
14

Features of SDN based Firewall

- Cost : Ideally, one single firewall is enough
- Performance: Firewalls can adaptively be deployed depending on network conditions.
- Management: Firewall rules can dynamically be added with new attacks
- Policy : Centralized view might be helpful to determine security policies
- Binding : Application level rules can be defined by software.

Difference between traditional and SDN firewall:

PARAMETERS	TRADITIONAL NETWORK FIREWALL	SDN FIREWALL
Stateful Inspection	Track the state of traffic present	Track the state of Layer2 to Layer7
IPS and IDS	The IPS or IDS deployment is done with the help of a separate appliance	IDS and IPS is fully integrated
Internal Traffic	Not seen and filtered	Filtered
Firewall Policy	Enforced at the interface level	Centrally defined and enforced at the controller

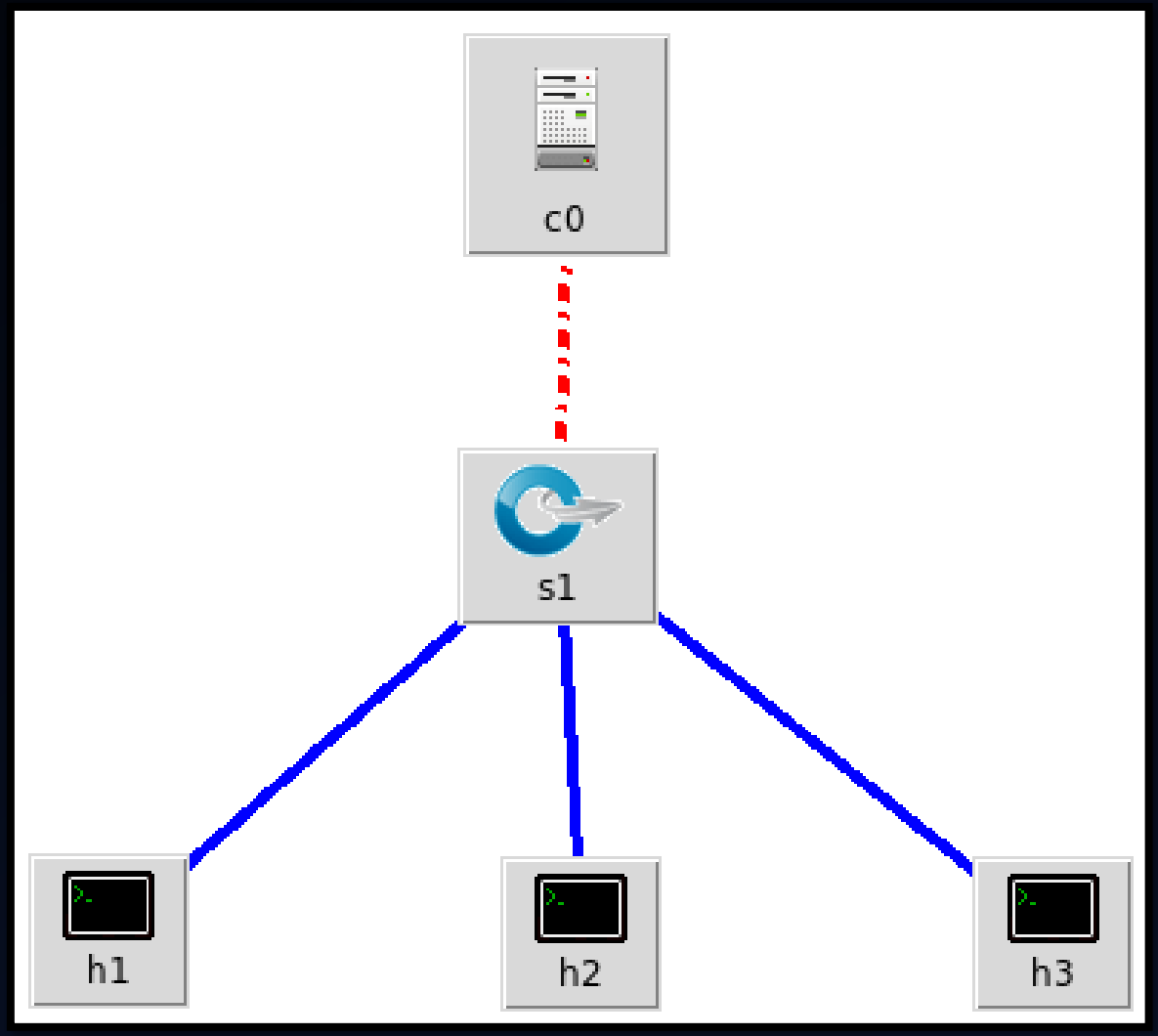
Pre-Requisites for SDN Layer2 Firewall Setup :

- ✓ VirtualBox : provides an environment for virtual network to be formed.

- ✓ Mininet : provides virtual SDN network topology.

- ✓ POX : SDN controller

Tree Topology

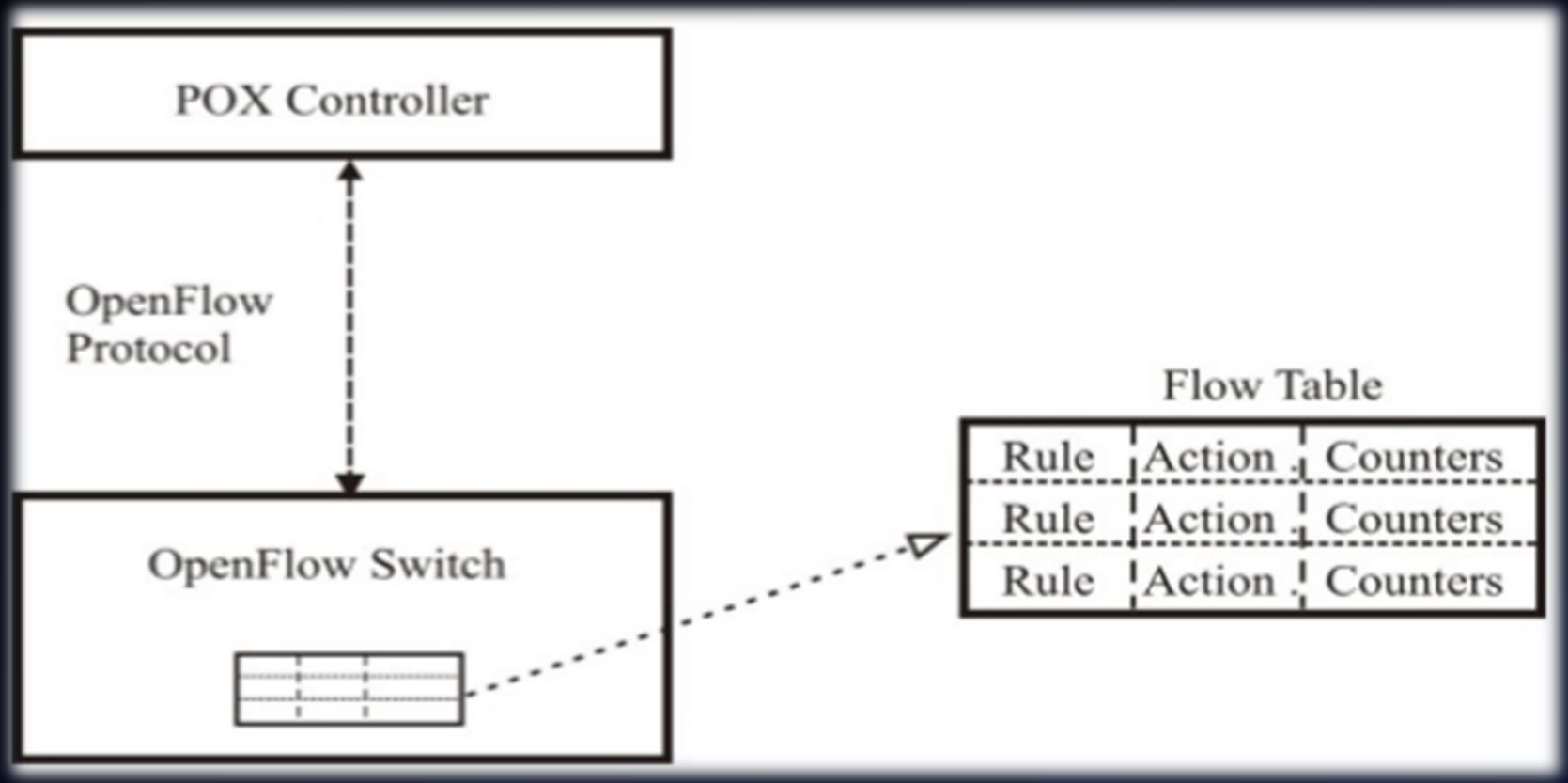


POX Controller & Its Features :

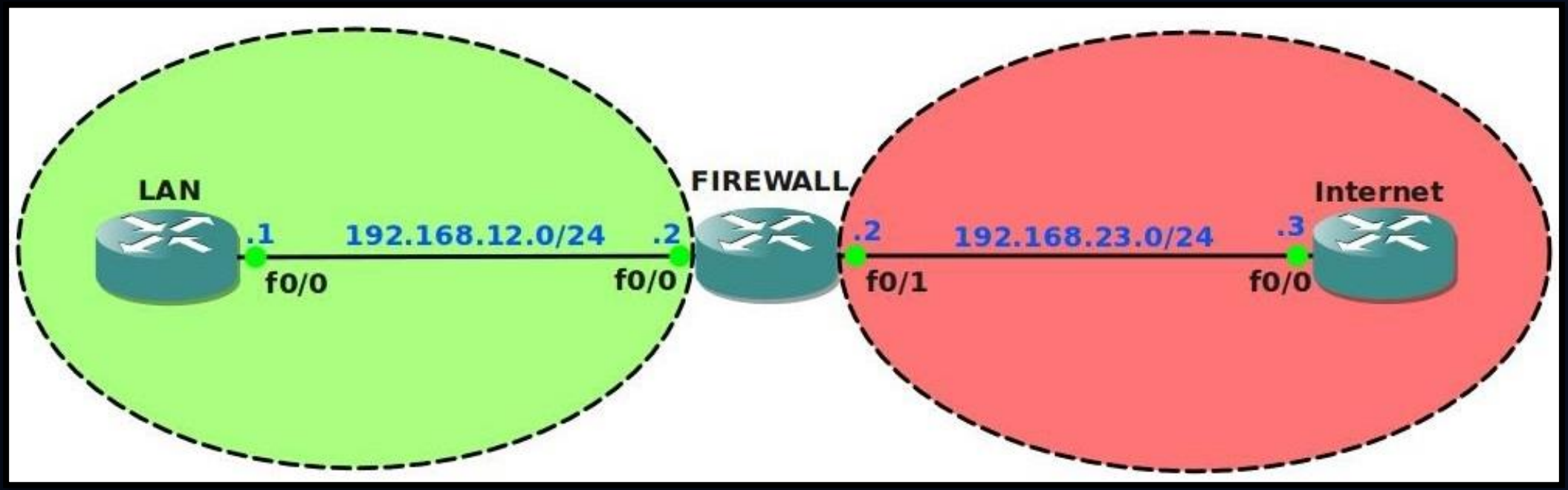
- POX is an open source development platform for Python-based software-defined networking (SDN) control applications, such as OpenFlow SDN controllers.
- POX provides a framework for communicating with SDN switches using the OpenFlow.

- **POX features:**
- “Pythonic” OpenFlow interface(uses openflow v1.0)
- Successor of NOX(based on C++) whereas POX is written in Python.
- Reusable sample components for path selection, topology discovery, etc.
- “Runs anywhere” – Can bundle with install-free PyPy runtime for easy deployment.
- Specifically targets Linux, Mac OS, and Windows.
- Topology discovery.

POX Controller :



Zone Based Firewall :



Features of Zone Based Firewall

- Interfaces are grouped into security “zones,”
- Each interface in a zone has the same security level.
- Packet-filtering policies .
- Interfaces in same zone share the same security level.

Steps In Setting Up a Zone Based Firewall

- Step 1 - Define the Zone Names and create zones
- Step 2 – Put the correct interface in zone
- Step 3- Define the Zone Pairs (direction of traffic flow)
- Step 4 - Create a Policy Maps and class for Zone Pairs
- Step 5- Assign the Policy Map to a Zone Pair
- Step 6-Specify the matching protocols.
- Step 7 – Verification (ping)

Zone Based Firewall Rules:

- Unidirectional policy is applied between zones
- Default policy for inter-zone traffic is DENY ALL
- Multiple traffic classes and actions can be applied per zone-pair
- If two interfaces are not in zones, traffic flows freely between them
- If two interfaces are in two different zones, traffic will not flow between the interfaces until a policy is defined to allow the traffic.

Key Constructs of Zone Based Firewall:

- Class-map
- Policy-map
- Zone-pair
- Service-policy
- Inspect type
- Policy Actions:
  - Inspect
  - Drop
  - Pass

THANK YOU!!