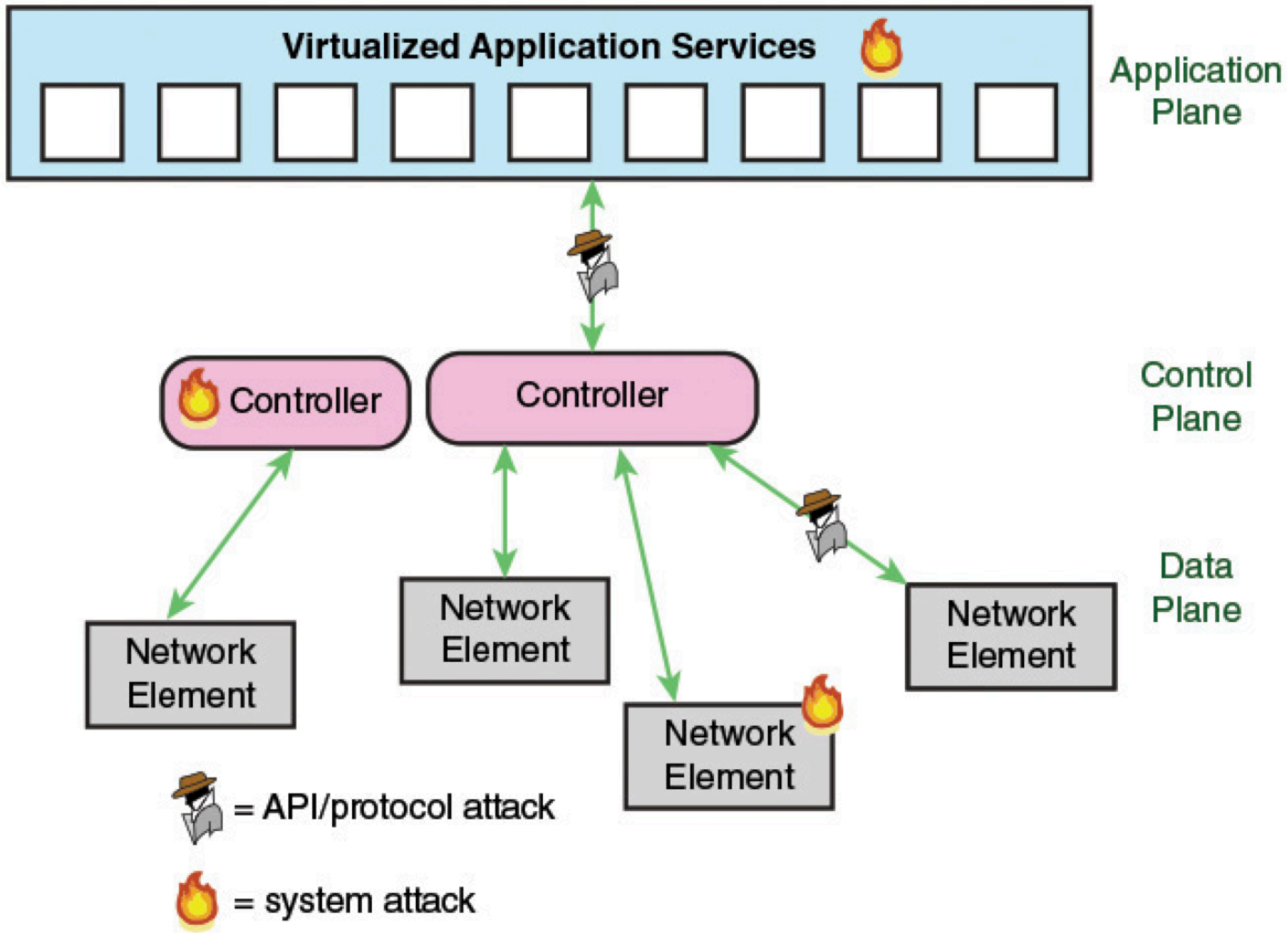
Data-centric security in software-defined networks

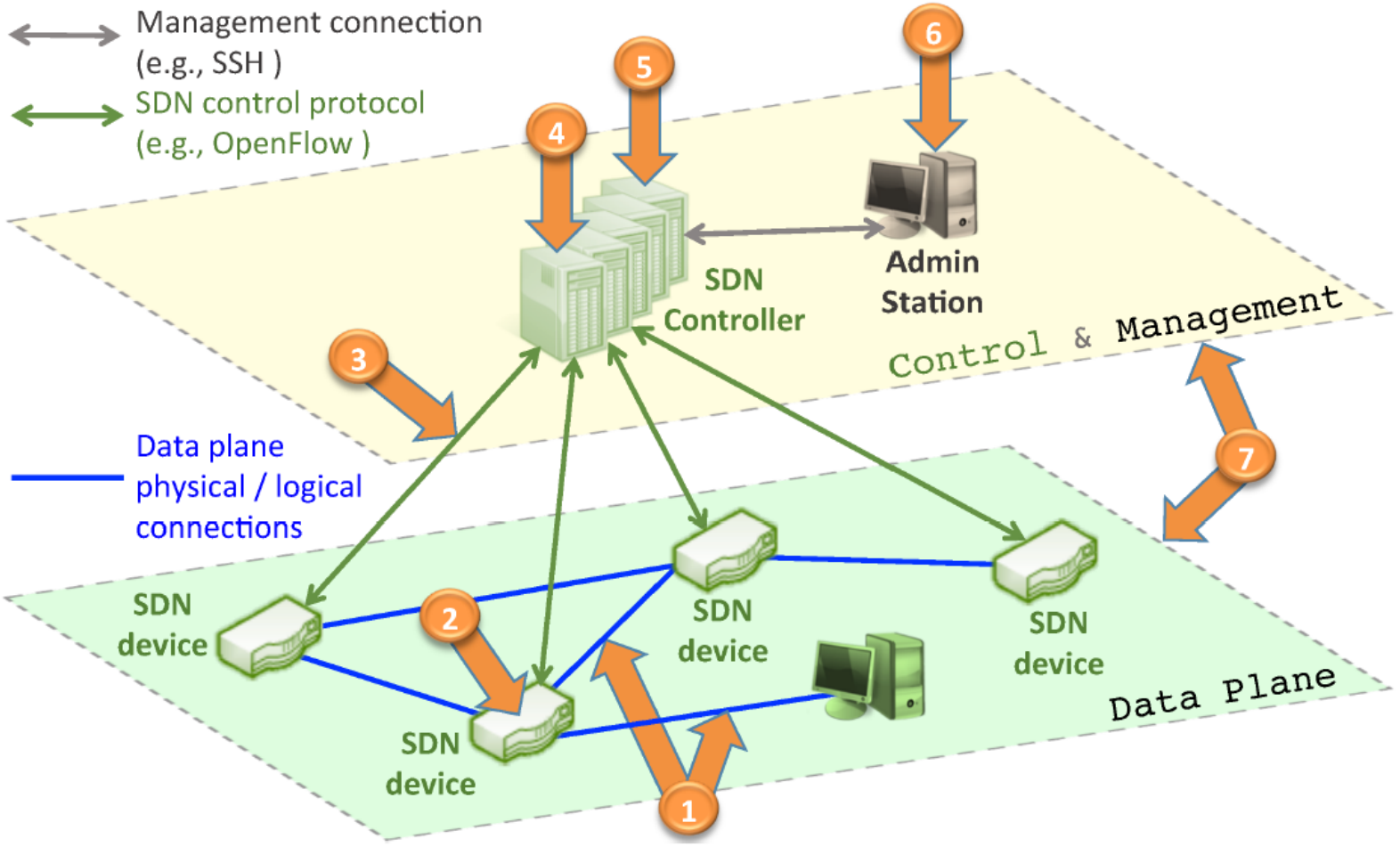
Dr.-Ing. Konrad Wrona

Lecture 3:
Security challenges in software-defined networks

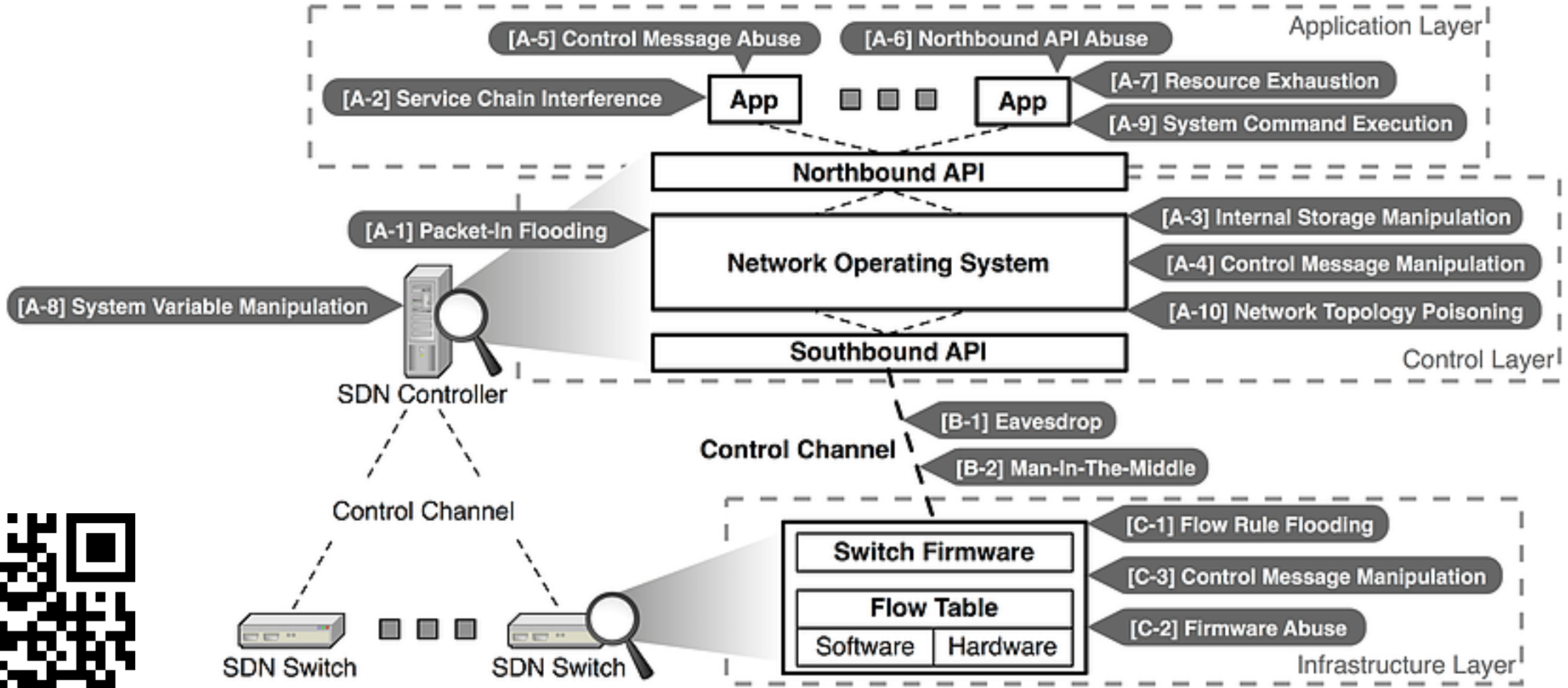
Attack surface in SDN



Security of SDN: Attack vectors



Security of SDN: Attack vectors



Security of SDN: Threats

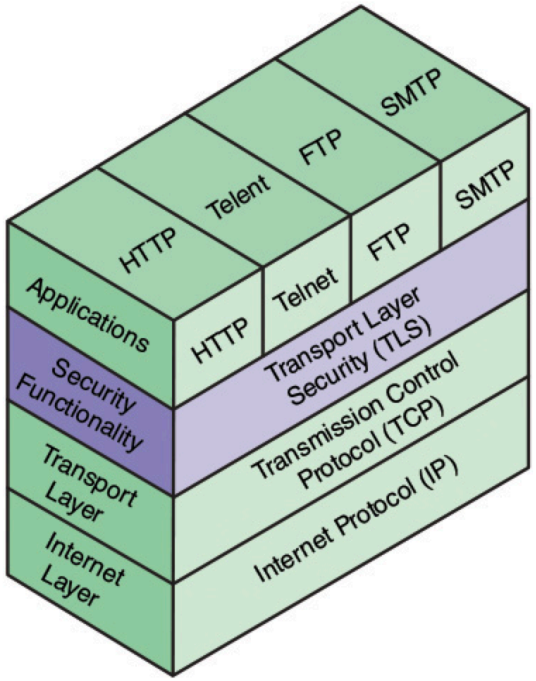
Security Issue/Attack	SDN Layer Affected or Targeted				
	Application Layer	App-Ctl Interface	Control Layer	Ctl-Data Interface	Data Layer
Unauthorized Access e.g.					
Unauthorized Controller Access			✓	✓	✓
Unauthenticated Application	✓	✓	✓		
Data Leakage e.g.					
Flow Rule Discovery (Side Channel Attack on Input Buffer)					✓
Forwarding Policy Discovery (Packet Processing Timing Analysis)					✓
Data Modification e.g.					
Flow Rule Modification to Modify Packets			✓	✓	✓
Malicious Applications e.g.					
Fraudulent Rule Insertion	✓	✓	✓		
Controller Hijacking			✓	✓	✓
Denial of Service e.g.					
Controller-Switch Communication Flood			✓	✓	✓
Switch Flow Table Flooding					✓
Configuration Issues e.g.					
Lack of TLS (or other Authentication Technique) Adoption			✓	✓	✓
Policy Enforcement	✓	✓	✓		

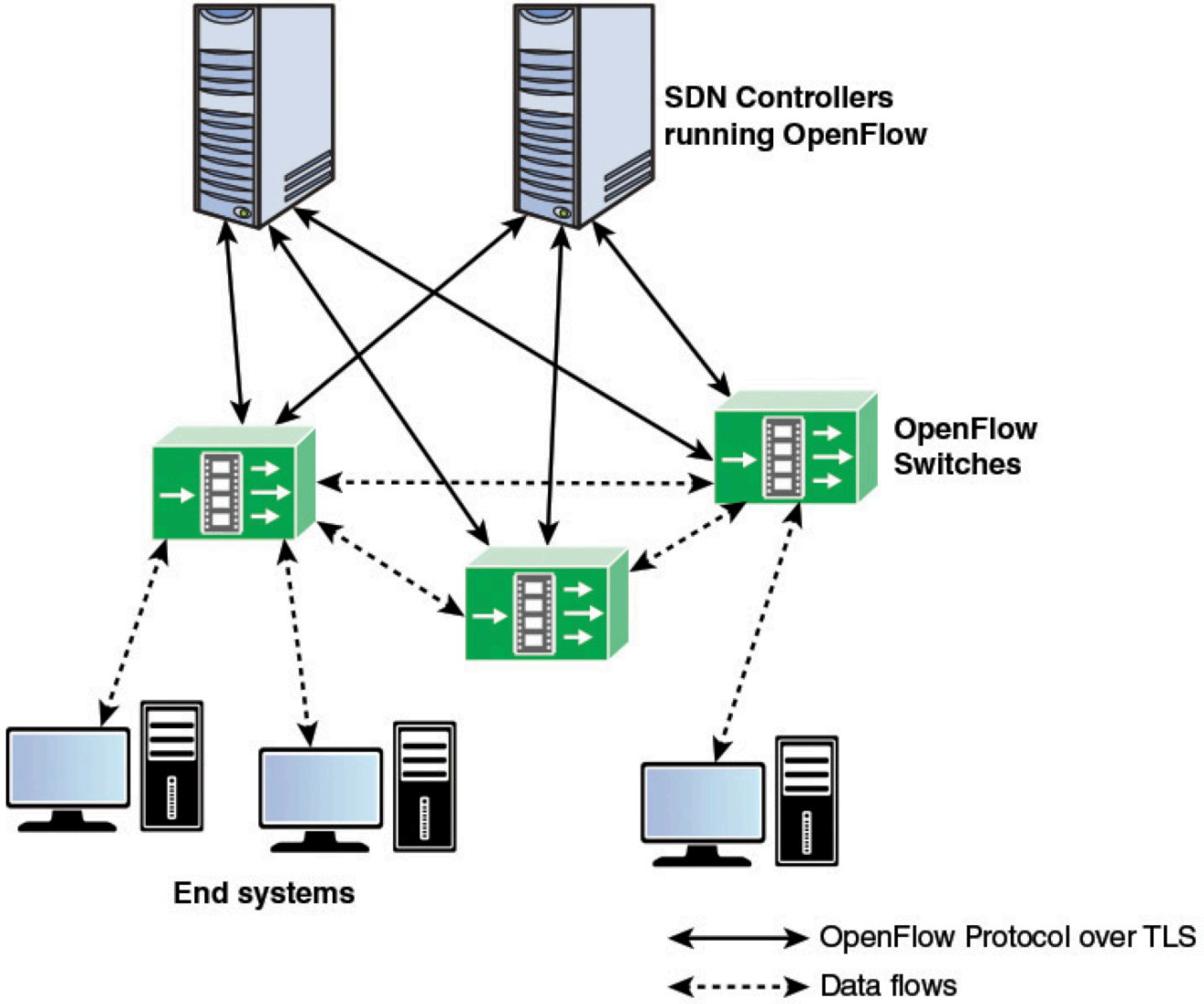
Security of SDN:
Control channel requirements

- Communication between controller and data plane requires provision of standard security features
  - Confidentiality
  - Integrity
  - Availability

  - Accountability
  - Authentication

Secure southbound communication channel





Security of SDN: Optional recommendation in OpenFlow 1.5.1 Specification?

- The switch and controller may communicate through a TLS connection to provide authentication and encryption of the connection. The switch and the controller should use a secure version of TLS ; at the time of publication we recommend using TLS version 1.2 or greater.
- The switch and controller mutually authenticate by exchanging certificates signed by a site-specific private key (recommended). Each switch must be user-configurable with its own certificate and a site-specific public certificate which is used for authenticating the controller. Additionally, the switch may optionally support the configuration of multiple CA certificates as well as maintain Certificate Revocation Lists (CRLs) when establishing connections with multiple controllers. It is recommended to configure and manage all related security credentials (cipher settings, keys, and certificates) using a switch management protocol, such as the OpenFlow Configuration protocol.
- Alternatively, for certain deployments, the switch can also support self-signed controller certificates or use pre-shared key exchange to authenticate the entities (not recommended).
- Plain TCP can be used for non-encrypted communication (not recommended), or to implement an alternate security mechanism, such as using IPsec, VPN or a separate physical network, the detail of such configuration is outside the specification.
- When using plain TCP, it is recommended to use alternative security measures to prevent eavesdropping, controller impersonation or other attacks on the OpenFlow channel.

Security of SDN: Denial-of-Service (DoS) attacks

- Control plane:
  - centralized control plane is vulnerable to flooding with requests
- Data plane:
  - fake flow requests can produce useless flow rules that need to be held by the data plane, thus preventing storage of flow rules for normal network flows
  - too frequent referrals to controller can cause buffer overflow due to waiting flows

Security of SDN:
Consistency and correctness assurance

- Consistency of distributed security policies is vital, but might be too complex for human
  - policies from multiple applications or installed across multiple devices
- Correctness of applications deployed in controller is critical
- Use of model checking, formal methods and symbolic execution may be required (e.g. Frenetic)
- Need for well-defined security patterns and system administration guidance

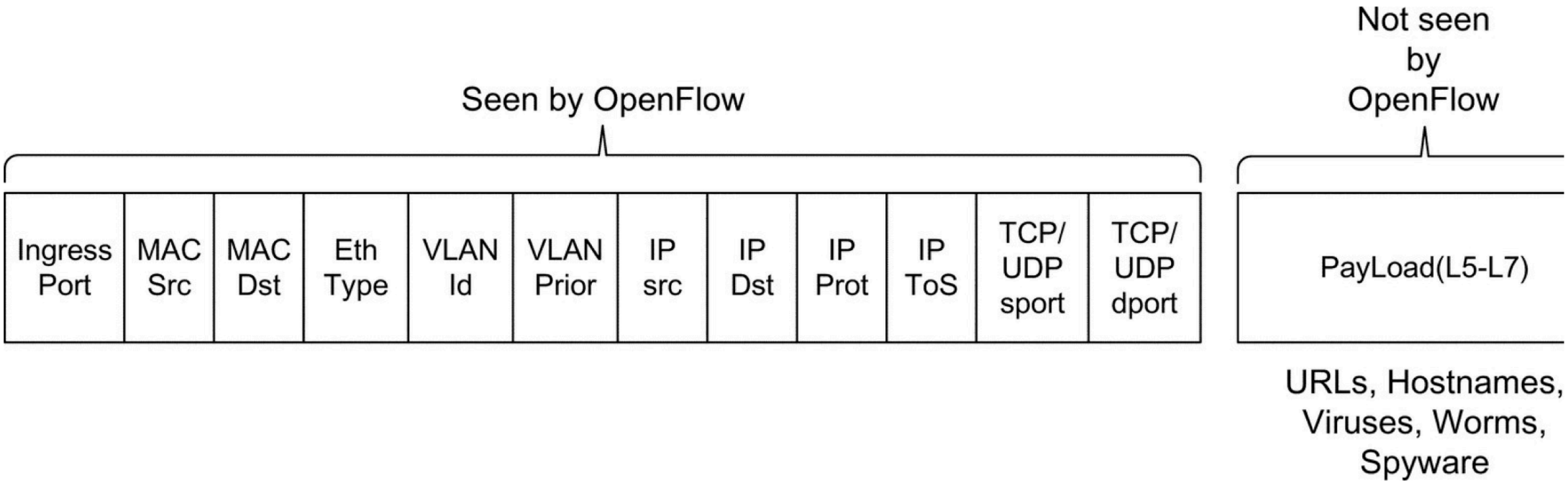
Security of SDN: Ecosystem of network apps

- Objective: moving control and data plane to commodity hardware
  - Big Iron switches to remain specialized hardware for high performance use
  - Non-core routers and firewalls use commodity systems
- Result: a platform and “SDN Apps” stores, similar to iOS, Android, and Windows
- Challenge: we do not have a good security model for existing app stores – how to solve it for SDN?

Security applications of SDN

- Dynamic control of network flow
- Dynamic composition of security services
- Cyber defence in data plane
- Cyber defence in control plane
- Moving target defence
- Traffic confidentiality
- Simplifying security administration

What an OpenFlow switch can inspect?



Security applications of SDN: Flow control

- SDN replaces VLANs, one of the elements of standard network security, provides basic ACLs
- Replacing a full firewall may be currently challenging - network processor needs to capable of deep packet inspection
- But SDN enables better load balancing for security middleboxes
  - Regular switch + controller can efficiently steer traffic towards right middle boxes
  - Implementing load balancing algorithms in network
  - Routing around failed and overloaded middleboxes

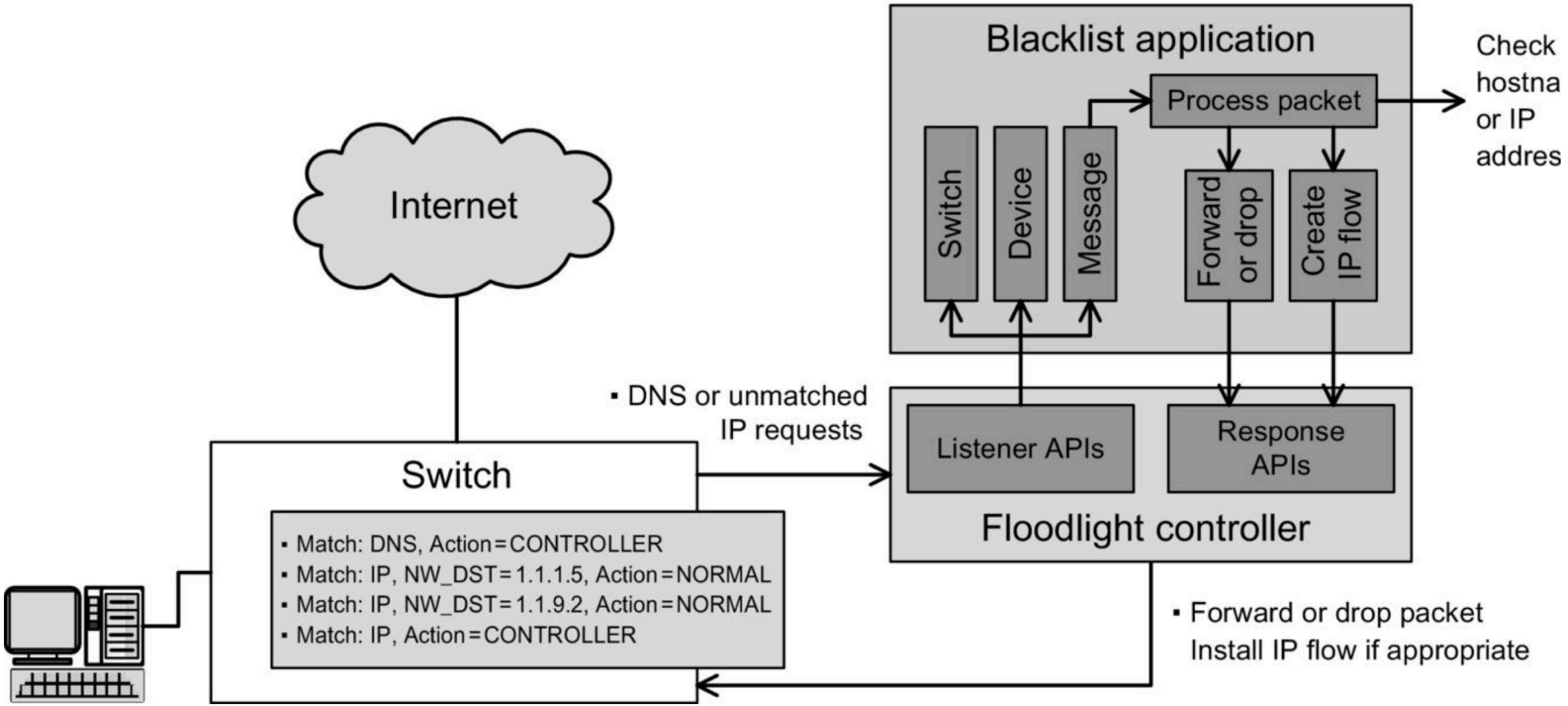
Security applications of SDN: Security service composition

- Packets typically need to go through a sequence of middleboxes
  - e.g., firewall -> IDS -> proxy
- SDN can eliminate the need to plan static placement or routes to enforce such sequences
- Deploying complex sequencing rules can lead to inefficient use of the available switch resources and to incorrect forwarding decisions
  - Thousands of rules
  - Universal processing sequences
  - Middleboxes modify headers, change session behaviour

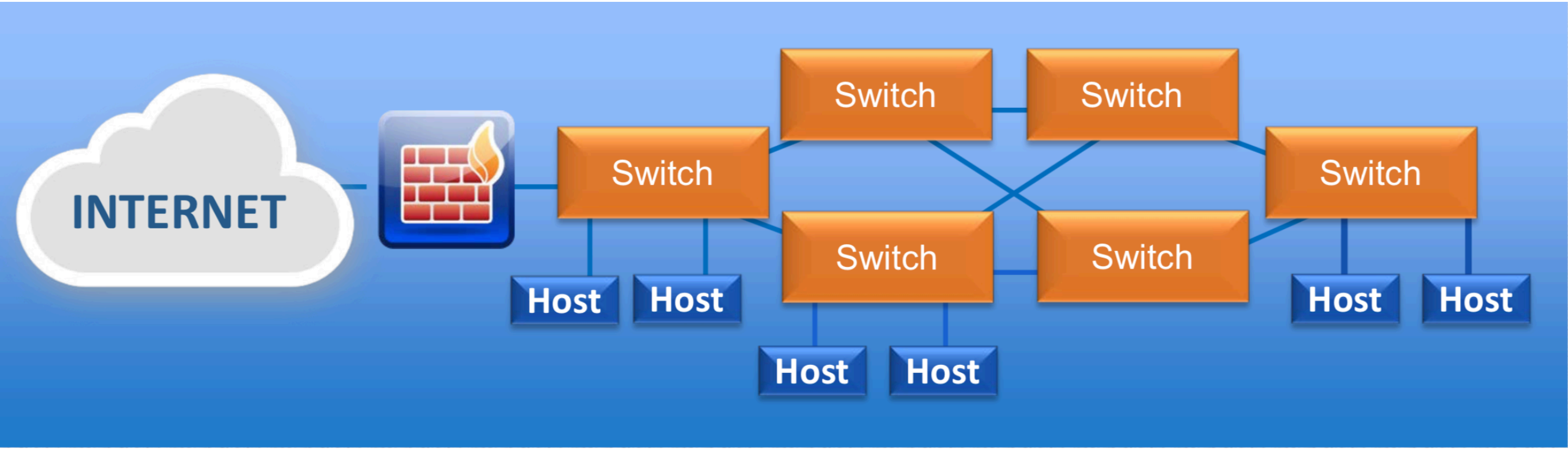
Security applications of SDN: Cyber defence in data plane

- Can help to identify attacks
  - distributed monitoring of the flows
  - identifying abnormal patterns
- Can distribute firewall/IPS/IDS functionality along the path/on a customer basis
  - instead of forcing all traffic to pass through a single specialized middlebox
- Allows fine-grained filtering of malicious traffic
- Filtering capabilities can be employed to duplicate traffic for legal and forensic purposes

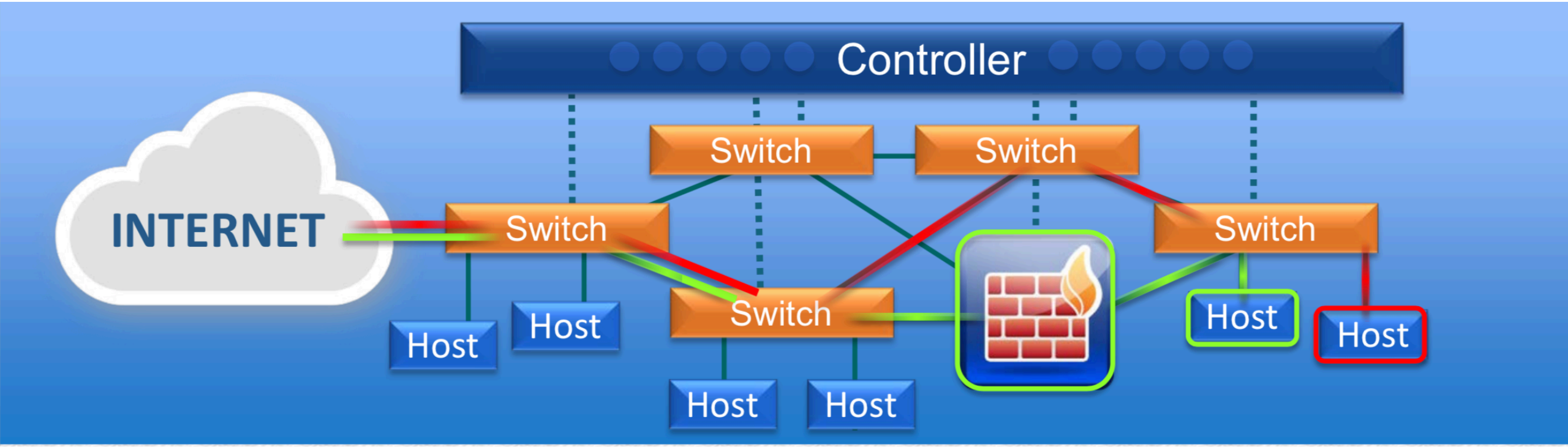
Blacklisting malicious hostnames or IPs



Software-defined perimeter



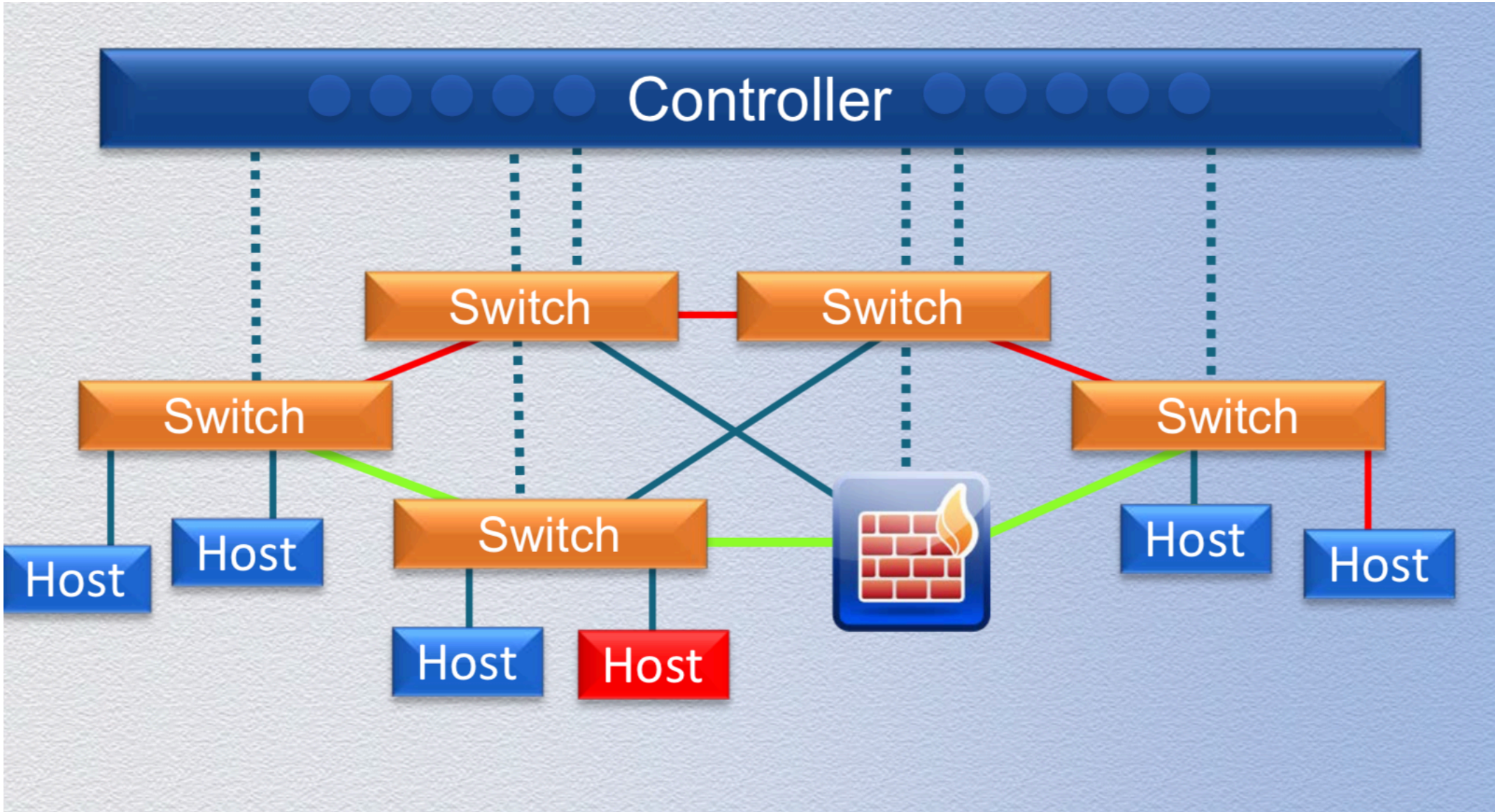
Software-defined perimeter



Security applications of SDN: Cyber defence support by controller

- Central controller enables a highly reactive security monitoring, analysis and response
  - Traffic analysis or anomaly-detection information transferred from data plane
- Applications running at the controller analyse and correlate the data from the complete network
- Updated security policy can be propagated across the network in the form of flow rules

Isolation of compromised hosts



Security applications of SDN: Moving target defence

- Malicious reconnaissance:
  Attackers use scanning techniques to discover vulnerable targets in the network

- Moving target defence:
  Use of random virtual IP addresses
  - OpenFlow controller can manage a pool of virtual IP addresses, which are assigned to hosts within the network, hiding the real IP addresses from the outside world

Security applications of SDN: Traffic confidentiality and administration

- Traffic confidentiality: Traffic shaping and packet re-writting/buffering/insertion can be used to provide countermeasures against traffic analysis

- Separation of concerns: Allows administrators to focus on required content of security policy without worrying about where it is enforced

- Consistent configuration updates: atomic changes to distributed security policies in the network

Protected Core Networking (PCN): Capabilities supported by SDN

1. Highly reliable
   - Protected against random failure and directed cyber attacks
2. Sharing of infrastructure
   - Between both classifications and nations
   - Better utilization and control
3. Seamless relocation of CCs
   - Automatic configuration on connection
4. Converged network
5. Federated
   - Interconnection of communications infrastructures
6. Utilization of all available communications links





Protected Core Networking (PCN): Capabilities supported by SDN

7. Implementation independent
   - Must meet requirements according to the PCN ISpec
8. Resource management
   - Service level agreements (SLAs) regulate usage
9. Federated management
   - Defined management exchanges between PCSs
10. Automated risk assessment
    - Assist operators in maintaining high availability
11. Integrated network management and cyber defence

Conclusions: SDN and PCN

- Clear conceptual compatibility
- E-nodes can be implemented as SDN nodes
- Controllers can manage and coordinate enforcement of single security policy within PCore
- SDN and CCN can support dynamic content-aware flow configuration within Pcore
- Intelligent “specialized” e-node middleboxes can be arranged in service cascades for content processing
- Content can be cashed near to interest areas