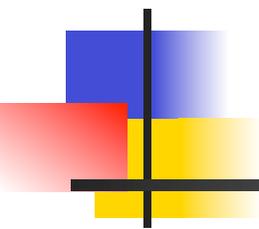
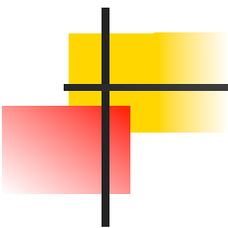


# Security Requirements for Software Defined Networks



---

Internet Area WG  
IETF 85: Atlanta  
November 4, 2012  
Margaret Wasserman  
[mrw@painless-security.com](mailto:mrw@painless-security.com)



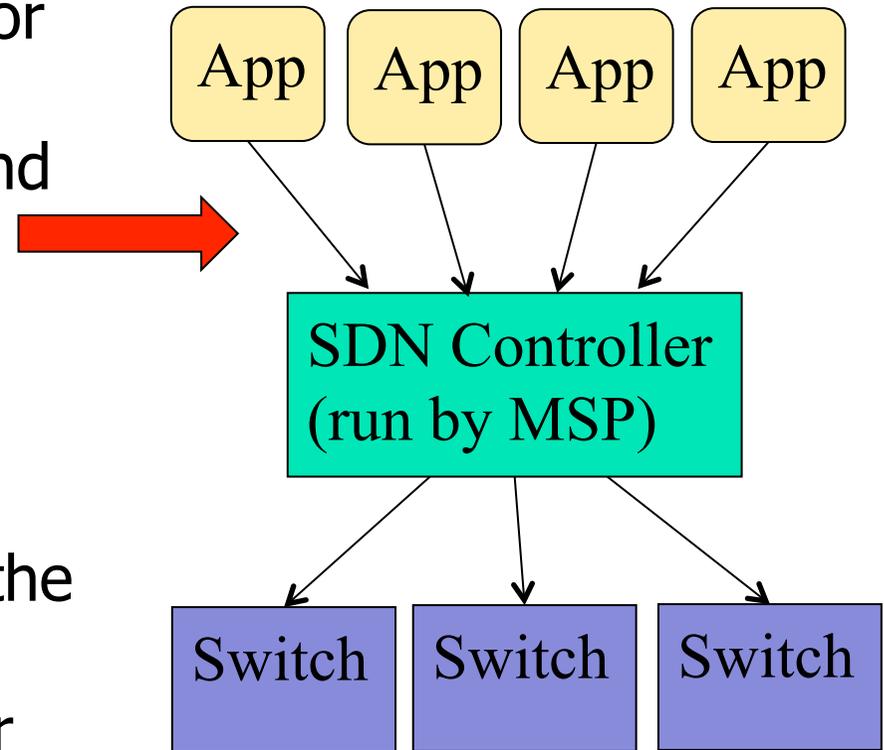
# SDN Security Requirements Draft

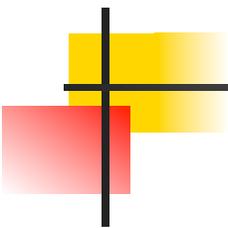
---

- Security Requirements in the SDN Model
  - <http://tools.ietf.org/html/draft-hartman-sdnsec-requirements-00>
- Currently individual work, not tied to any WG
  - Feedback to authors, discussion on saag@ietf.org

# Security Requirements for SDN

- Discusses requirements for an SDN protocol running between “applications” and an SDN controller
- Describes security requirements for three classes of applications
- Apps may not be run by the same organization as the Managed Service Provider (MSP)

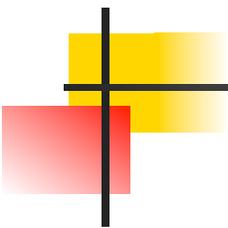




# Three Classes of Applications (1)

---

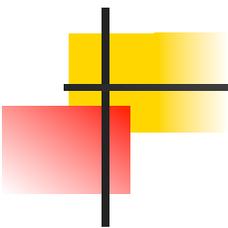
- Class 1: Network Sensitive Applications
- Applications that require particular network characteristics
  - Needs access to ports in particular VLAN
  - Requires specific path characteristics
    - Traffic stays within a specific jurisdiction
    - Traffic travels only over certain equipment
  - Wants to monitor costs of traffic/flows
  - May want to reject or accept certain flows



# Three Classes of Applications (2)

---

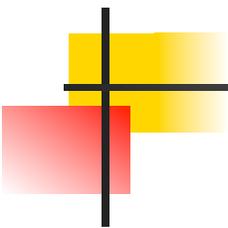
- Class 2: Services for the Network
- Application provides a service for the network
  - e.g. Firewall, content inspection or intrusion detection



# Three Classes of Applications (3)

---

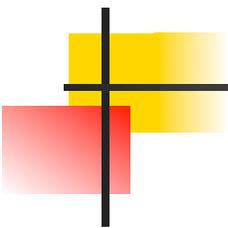
- Class 3: Packaged Network Services
- Combines previous two classes
  - e.g. Application of Class 1 that wishes for all traffic to be sent through a border firewall service
- Application is requesting instantiation of another application as a virtual element in the network
- Permits abstraction and re-use of network applications



# Authentication & Authorization

---

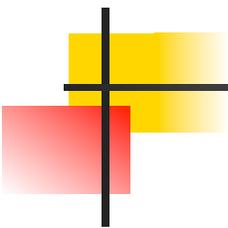
- Need for authentication and authorization across multiple organizations



# Security Requirements (1)

---

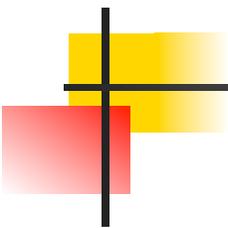
- REQ1: Authentication is REQUIRED to the controller. Authentication SHOULD support existing credentials that are likely to be used in the datacenter.
- REQ2: The interface to the SDN controller MUST support authorizing specific network resources to applications and manipulating the authorizations of applications.
- REQ3: The SDN controller MUST provide facilities to isolate one application from another.



# Security Requirements (2)

---

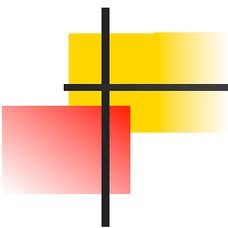
- REQ 4: The SDN controller interface **MUST** support a controller acting as a proxy on behalf of applications.
  - REQ 4a: The SDN interface **SHOULD** support a way of associating an audit ID or other tracking ID so that requests can be correlated with an original application when a proxy acts on behalf of an application.
- REQ 5: The SDN controller interface **MUST** provide mechanisms for operators and applications to enforce privacy.



# Security Requirements (3)

---

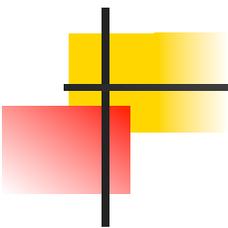
- REQ 6: The SDN controller interface **MUST** support delegating access to a subset of resources; as part of delegation new authorization and privacy constraints **MAY** be supplied. This supports the security needs of the debugging use case, aspects of the nested application use case, and facilitates other inter-organization uses.



# Nested Application Security (1)

---

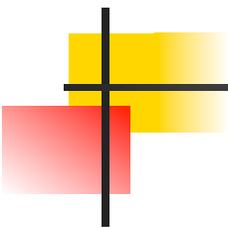
- REQ N1: The SDN controller interface **MUST** support controlling authorization for what nested applications an outer application can nest.
- REQ N2: The controller **MUST** separate authorizations held by one instance of a nested application from authorizations held by other instances of the same nested application.



## Nested Application Security (2)

---

- REQ N3: The SDN controller interface SHOULD provide outer applications a way to learn a nested application's policy for sharing information between instances.
- REQ N4: Nested applications MUST be able to authenticate on behalf of a specific outer application. This facilitates authorization, accounting and auditing.



# Nested Application Security (3)

---

- REQ N5: Nested applications **MUST** be able to specify privacy policy for what resources are visible to the outer application.
- REQ N6: Outer applications **MUST** be able to specify privacy policy and authorizations with regard to what outer resources the nested application can interact with.

# Questions? Feedback?

---

- Send questions of feedback to the draft authors
  - Sam Hartman <hartmans@painless-security.com>
  - Margaret Wasserman [mrw@painless-security.com](mailto:mrw@painless-security.com)
  - Dacheng Zhang [zhangdacheng@huawei.com](mailto:zhangdacheng@huawei.com)
- Or, discuss these drafts on [saag@ietf.org](mailto:saag@ietf.org)