I2NSF Data Center Use Cases

draft-zarny-i2nsf-data-center-use-cases-00

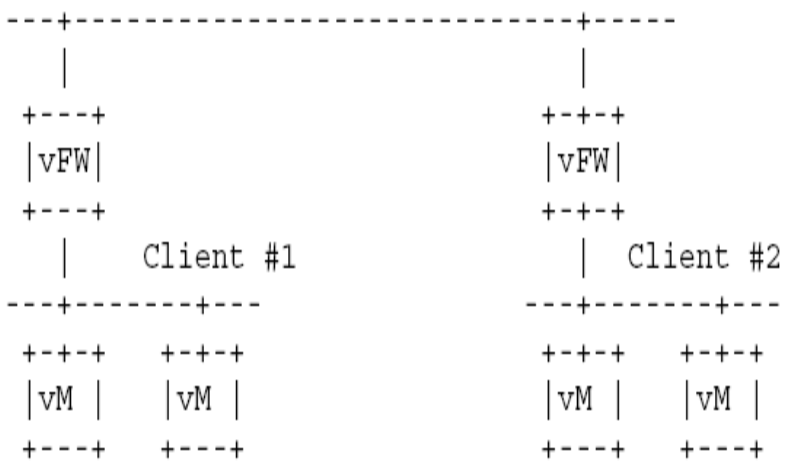
M. Zarny: Goldman Sachs

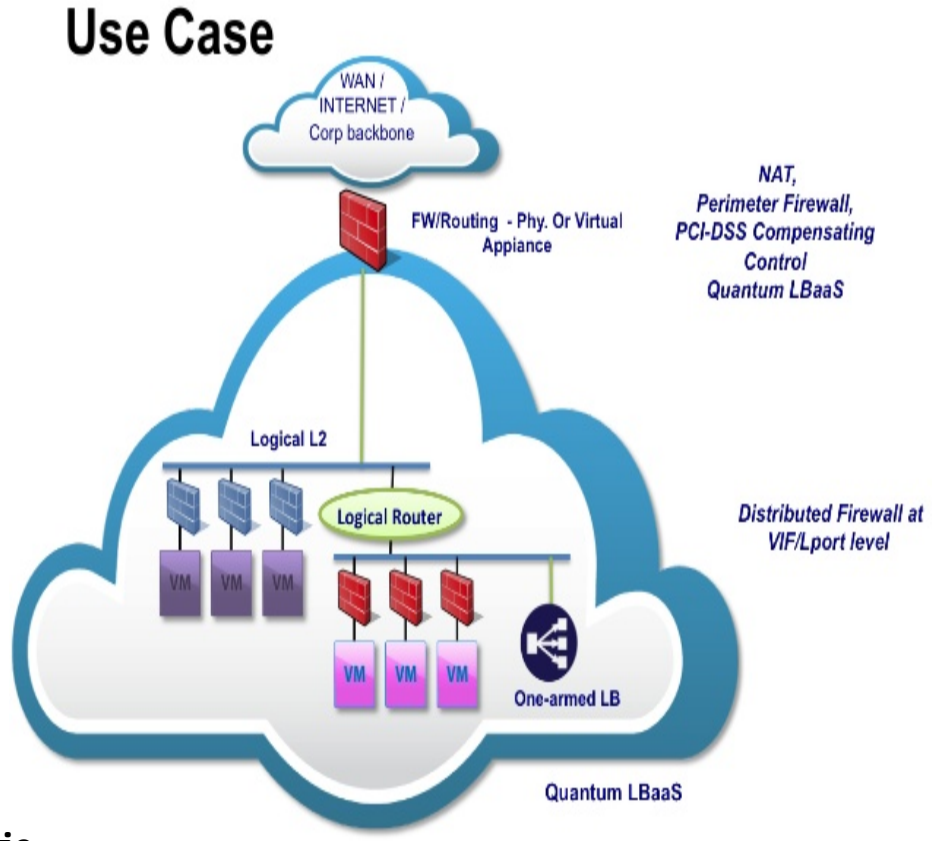
S. Magee: F5 networks

N. Leymann: Deutsche Telecom

L. Dunbar: Huawei

On-demand, elastic FWs





Different types of customers/clients, e.g.

- **residential with (very) limited/no control**
- **business with full control on fw**
- **Internal/infrastructure driven, e.g. automatic updates driven by information from probes**

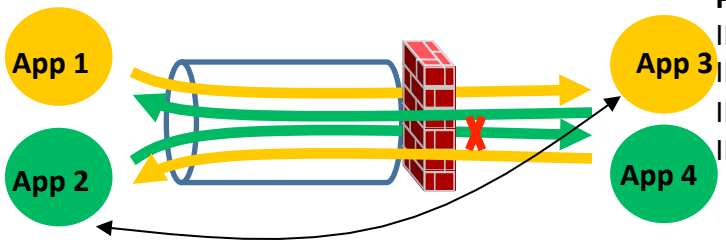
Client Specific Security Policies

Zones:
Yellow zone
Green zone
…

Security Policy:
Yellow===>Yellow, Green
Green ===> Green
•**Prohibited**
Green=X=>Yellow

Config 1:

App 1=IP1
App 2=IP2
App 3=IP3
App 4=IP4
…

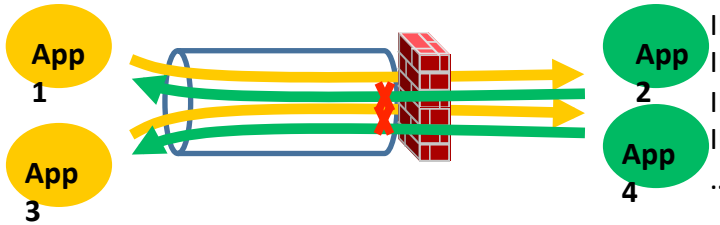


Policies for Firewall

IP1===>IP3
IP1===>IP4
IP2=X=>IP3
IP2===>IP4
IP3 ===>IP1
IP3 ===>IP2
IP4=X=>IP1
IP4 ===>IP2

Config 2:

App 1=IP11
App 2=IP12
App 3=IP13
App 4=IP14
…

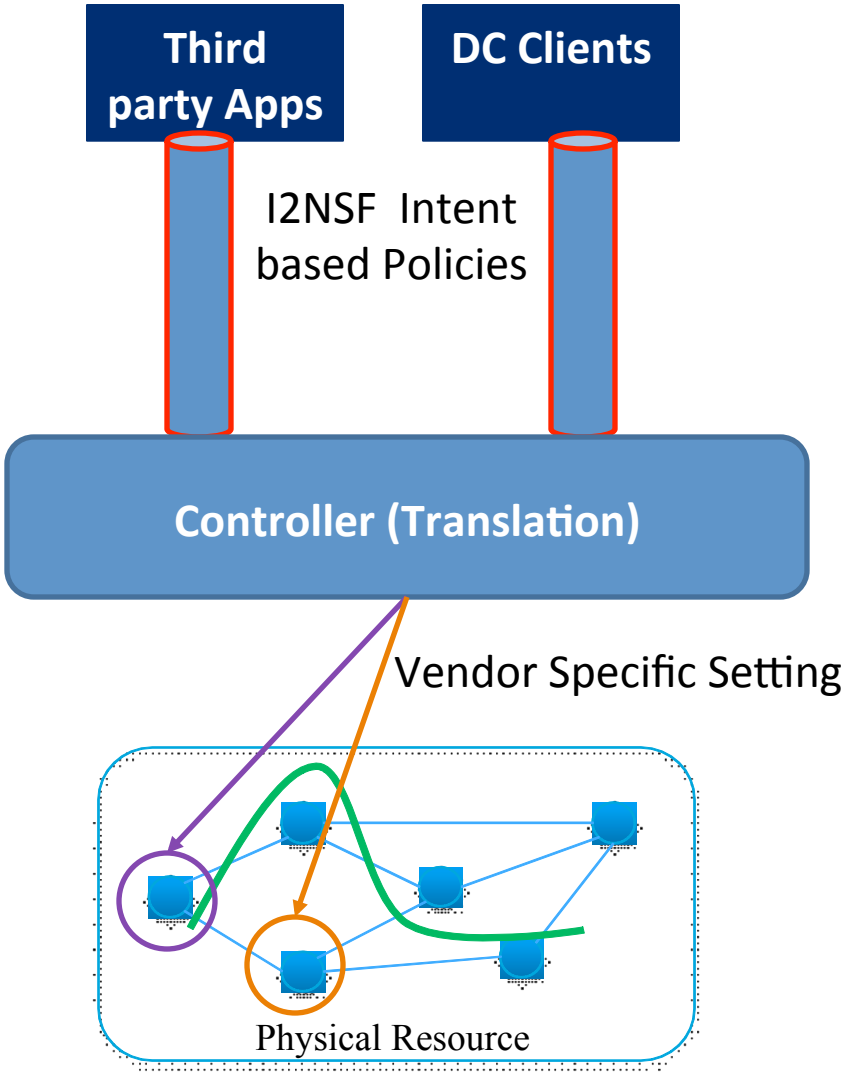


Change of the policies:

IP11===>IP12
IP11===>IP14
IP13===>IP12
IP13===>IP14
…
IP12=X=>IP11
IP12=X=>IP13
IP14=X=>I1P1
IP14 =X=>IP13
…

Role of I2NSF

- Intent Driven Network Security policies for clients



Key Requirement (1 of 2)

- Dynamic creation, enablement, disablement, and removal of network security applications;
- Policy-driven placement of new service instances in the right administrative domain;
- Attachment of appropriate security and traffic policies to the service instances
- Management of deployed instances in terms of fault monitoring, utilization monitoring, event logging, inventory, etc.
- Support of distributed architectures/deployments

Key Requirement (2 of 2)

- Translation of security policies into functional tasks.
  - Security policies may be carried out by one or more security service functions. For example, a security policy may be translated into an IDS/IPS policy and a firewall policy for a given application type.
- Translation of functional tasks into vendor-specific configuration sets.
  - For example, a firewall policy needs to be converted to vendor-specific configurations.
- Retrieval of information such as configuration, utilization, status, etc.
  - Such information may be used for monitoring, auditing, troubleshooting purposes. The above functions should be available in single- or multi-tenant environments as well as on premise or off-premise clouds.