Open Security Controller Project
Use Cases

Security Orchestration for Software-defined Infrastructure

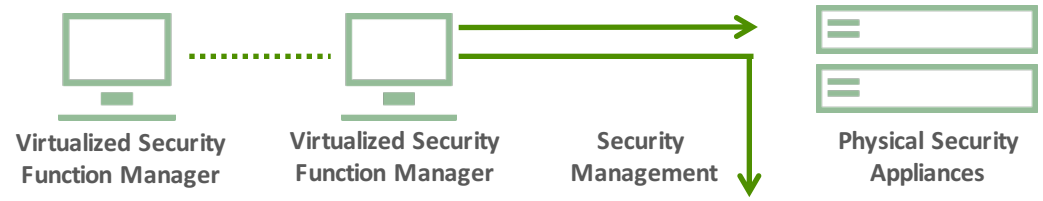
https://www.opensecuritycontroller.org

Conceptual Architecture

Orchestrating security policies with network provisioning across **multiple virtual environments**

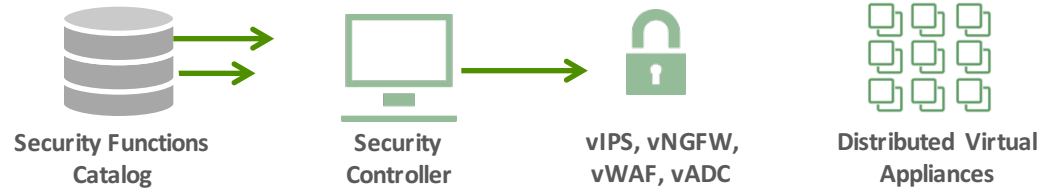
Security Function Manager

Centralized management and separation of duties



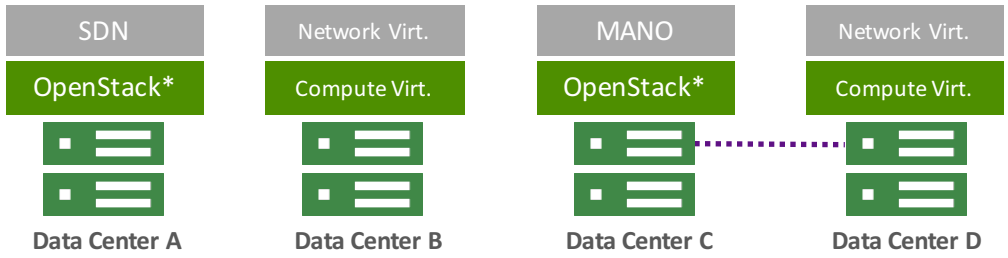
Security Controller

Security service automation and orchestration



Virtualization Infrastructure Management

Abstracts compute, storage, and network

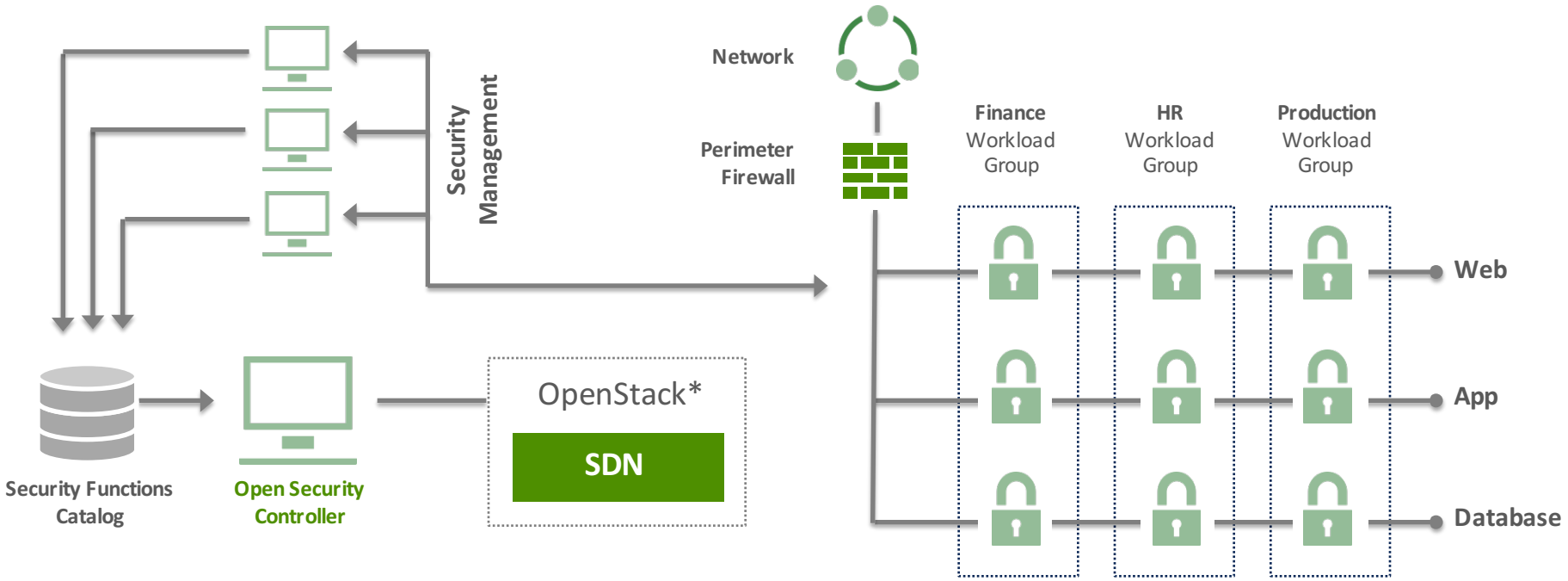


Conceptual Architecture

- A lot of customers run multiple stacks in their data centers, so the security that you need in your data center should not be isolated to a single stack, but uniformly available to all stacks.

- OSC connects with multiple stacks and their SDN controllers and make security available to all of them simultaneously. It does it for one VM as easily as it can be done for hundreds of VMs.

Use Case: **Micro-segmentation**



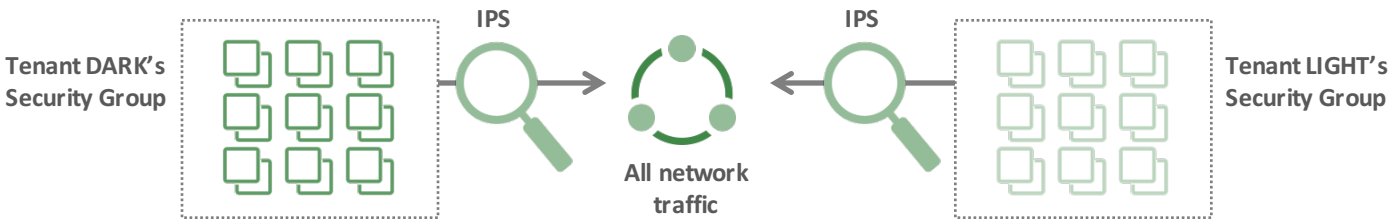
Use Case: **Micro-segmentation**

- Open Security Controller (OSC) enables the grouping of workloads by their security needs and the selective binding of workload-specific security policies to those workloads. It connects with the appliance manager, and through OpenStack, deploys virtual instances. OSC brings micro segmentation to OpenStack security.
- But not only can you use OSC to create logical groups of workloads, it also allows you to deploy VNFs onto different physical hosts. It allows users to share security virtual networking functions (VNFs) across tenants.
- This allows efficiency through security automation and agility in meeting compliance mandates. Data center security administrators no longer need to manually deploy/install and configure hardware or virtual security appliances in series. Applying security policy to VMs is as simple as a few mouse clicks and can be done for one VM as easily as it can be done for hundreds of VMs. Data center administrators can configure VNFs in a faster, more efficient way (instead of taking days or weeks, they can configure virtual functions in minutes or hours).

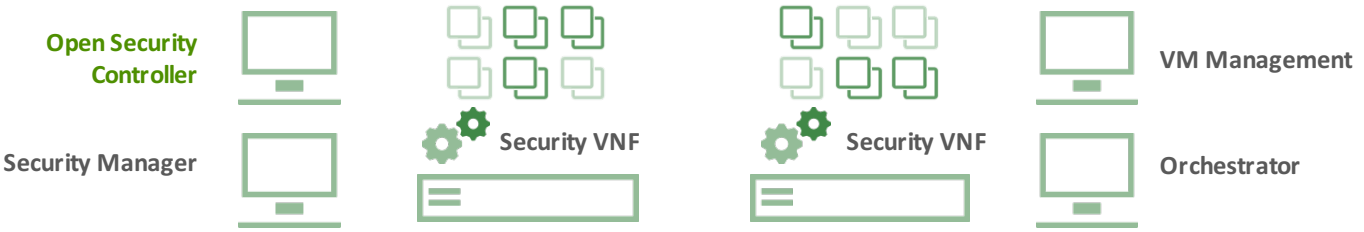
Use Case: **Multi-tenancy** (e.g., MSP)

Tenant Perspective
Must be fully isolated

Logical Perspective
Require IPS inspection at edge



Practical Perspective
Must share resources



Use Case: **Multi-tenancy** (e.g., MSP)

- A popular use case is the separation of tenants by IPS within a multi tenant environment. This may be encountered in the case of a managed hosting or managed services provider, or as separate business units or functions within the same company.
- The desires these cases are the same…From the tenants perspective, they have their VMs or workloads hosted in a secure cloud with IPS protecting the edge of their network or segment. The tenant wants to be fully isolated from any neighbors as if they were the only ones there.
- The service provider or IT needs to provide this isolation and IPS inspection for the segments but needs to used shared resources. Practically and physically, the VMs of both tenants are sharing the same physical hosts and and located all over the place.
- The beauty of micro-segmentation is that it is designed to provide the necessary segmentation isolation and service insertion on the shared infrastructure. From a logical perspective, broad security groups can be created for each tenant with the ability for the tenant to still define subgroups for their own individual needs.
- Physically, the distributed IPS instances are looking at tenant specific policy tags on each packet that inform the IPS which inspection policy to apply. The result is exactly as desired. The tenants are isolated with IPS at their edge and the infrastructure that is securing them is shared.

END