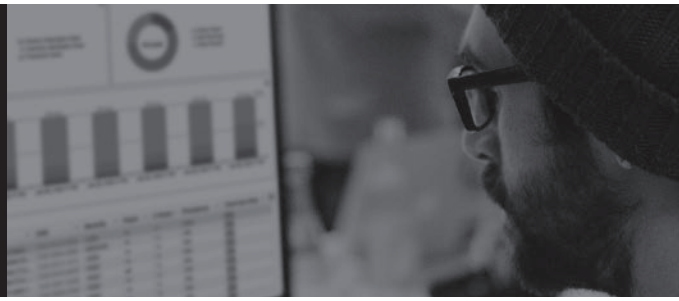
REDSEAL

REDSEAL AND VMWARE NSX



SOLUTION OVERVIEW

VMware NSX enables the creation of entire networks in software. It abstracts the underlying physical hardware and embeds it into the Hypervisor. You can save networks, delete them, restore them – just like virtual machines.

VMware NSX represents a new paradigm in network design, but as the virtual infrastructure grows it often connects to legacy hardware networks as well as private and public clouds. These networks create more access paths within and across the hybrid network; making it difficult to understand what is exposed to the internet, where attackers can go, and what access a given host has.

UNIFY PHYSICAL, VIRTUAL AND CLOUD SECURITY

With RedSeal your physical, virtual and cloud networks become a unified security architecture capable of being modeled, tested and measured. RedSeal easily integrates with VMware NSX giving you the ability to assess the security of your Software Defined Data Center (SDDC) as well as the rest of your hybrid network. It gives you the means to analyze both east-west and north-south traffic and to validate micro-segmentation. RedSeal can also drill-into the Distributed Firewall (DFW) security groups and provide you with the specific rules that apply to individual workloads (hosts). This feature makes it easy for security teams to ensure that only authorized access is allowed.

MODEL, TEST AND MEASURE UNIFIED ARCHITECTURE

RedSeal interoperates with VMware NSX just as it does with your physical devices. It will automatically collect and import the following data:

- Distributed Logical Routers and access rules
- Edge Gateway Routers and access rules
- Load Balancing rules
- Distributed Firewall rules
- Security groups and rules
- Networks
- Workloads (hosts)

BENEFITS

- Unify security architecture across hybrid infrastructure
- See end-to-end access across your hybrid network
- View all workloads (hosts) in a security group
- See the firewall ruleset that applies to an individual workload (host)
- Verify compliance with industry configuration guidelines

WHAT YOU NEED

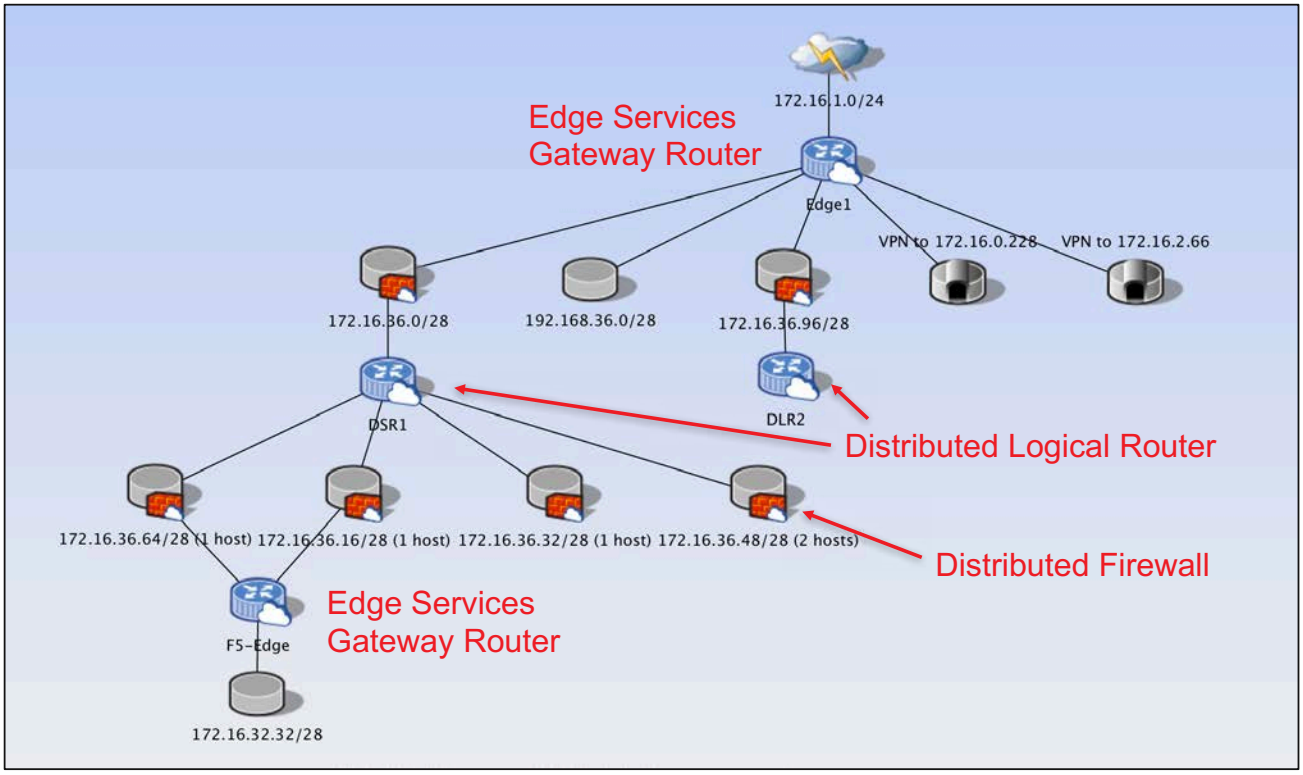
- RedSeal 8.4
- VMWare NSX 6.2.2

REDSEAL AND VMWARE NSX

WHAT'S NEW IN REDSEAL 8.4?

- View all security groups within a SDDC
- View all workloads (hosts) in a security group
- View specific firewall rules that apply to a given workload (host)
- Query subnets and view micro-segmentation policies

RedSeal provides the full feature set to VMware NSX that exists for all RedSeal supported devices. It provides security teams with improved network context so they can see the security posture of their physical, virtual and cloud networks as well as the end-to-end access across their hybrid infrastructure. It accelerates vulnerability management and incident response by prioritizing vulnerabilities and indicators of compromise based on access to untrusted networks and critical assets. And, it validates compliance with industry secure configuration guidelines so security teams can systematically improve the resilience of their hybrid IT environments.



VMware NSX Topology in 8.4

REDSEAL

940 Stewart Drive, Sunnyvale, CA 94085

+1 408 641 2200 | 888 845 8169 | redseal.net