Virtual Elastic Security Appliance Data Sheet

Virtualization has become a real game changer in the data center. Network Function Virtualization (NFV) and Software Defined Networks (SDN) are revolutionizing data center architectures. But, in the stampede to virtualize, security seems to be the forgotten stepchild in the virtualization build out. All current security solutions have critical deficiencies in a virtualized environment: Physical firewalls require traffic to be routed to the physical appliance and back again. This complicates network topology and impacts performance. It also fails to protect workloads that move dynamically using vMotion. Virtual firewalls can be deployed near workloads but they also fail to protect workloads that move dynamically. Furthermore, virtual security appliances cannot scale when workloads require high burst rates and dynamic allocation of resources. Hypervisor based firewalls solve the vMotion problem but it must severely constrain the functionality and performance of security solutions to avoid impacting the performance and stability of the hypervisor.

Hillstone's Virtual Elastic Security Appliance (vESA) solves all of these problems. It virtualizes firewalls components into separate security, control, and data planes that are all managed by a centralized cloud orchestration platform. It allows critical components to scale up or down "elastically" as demand increases and subsides. Components can be deployed close to workloads that need protection and they maintain state when workloads move insuring uninterrupted protection. Components are also deployed in pairs to insure high availability and redundancy. Only Hillstone's Virtual Elastic Security Appliance provides the agility, flexibility, and elasticity required to meet the modern data center's need to protect north-south and east-west traffic.

Product Highlights

Flexible Scaling

Hillstone's vESA offers multi-tenant flexibility and scalability much like our physical appliance but without the physical limitations of the chassis. In the physical world each tenant has his or her own virtual System (vSYS) firewall. Resources are dynamically deployed to meet the instantaneous demands of each tenant, as long as excess capacity is available. When more capacity is needed cards can be installed up to the physical limits of the chassis. A single manager manages all tenants and each tenant manages their own management domain.

Hillstone's vESA operates in the same conceptual way but it does not have the constraints of a physical chassis. All components of the appliance have been turned into virtual machines (VMs) and can be deployed across the virtualized data center. When demand increases additional VMs can be deployed close to the tenant workloads. When the demand is reduced the VMs can be retired. And since they are all conceptually tied to the same appliance they are managed by one management interface.

Dynamic Allocation of Resources

As with NFV, Hillstone has virtualized the functionality of its intelligent Next Generation Firewall (iNGFW). It virtualizes the firewall components into separate control planes, data planes, and security planes:

- The control plane is represented by the virtual Security Control Module (vSCM). It interfaces to the cloud orchestration software via the RESTful API and is responsible for configuring, scaling, and monitoring the security services on the network.
- The security plane is represented by the virtual Security Service Module (vSSM). It handles policy lookup, keeps firewall state and handles other advanced security functions. These modules can be placed close to the workloads to reduce latency.
- The data plane is represented by the virtual Input/Output Module (vIOM). It handles north/south and east/west data traffic and can scale to insure there are no traffic bottlenecks.

The beauty of separate security and data planes is that each can scale

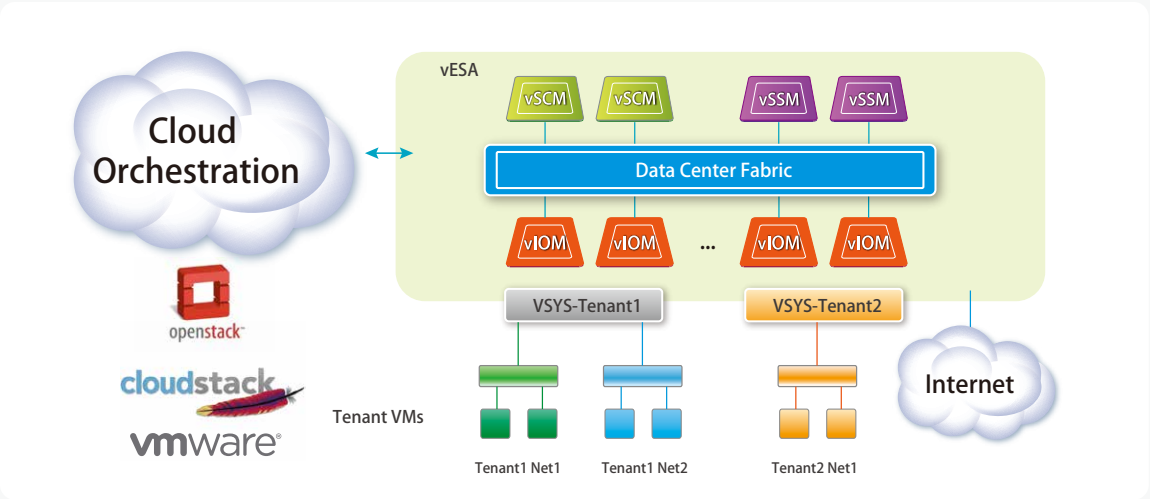
independently, insuring that the right resources are deployed when and where they are needed. Another important feature is that these modules are deployed in pairs for high availability and redundancy.

Manageability

The entire vESA interface can be managed as if it were a single firewall appliance. The virtual Security Control Module (vSCM) acts as the central security configuration manager, integrating tightly with datacenter orchestration via the RESTful API. Administrators can also manage vESA through a WebUI and CLI.

vESA supports multiple tenants through virtual systems (vSYS) and each tenant is automatically given their own management domain. When a new tenant is added to Openstack a corresponding vSYS is created in the vESA configuration.

Another important feature is Hillstone's "dynamic address book." Normally, address books contain static IP addresses. However, in a cloud environment, VMs can be moved easily from one network address to another, making it difficult to associate a VM to an IP address. In StoneOS an administrator can create a dynamic address entry that includes the VM name and/or VM metadata to define an address entry. The IP addresses of all VMs, that have names or metadata, will automatically update whenever they move.



Features

Cloud Management Platform

- OpenStack
- Interface: RESTful API, CLI, WebUI
- Hypervisor Compatibility: VMware, KVM

Network Services

- Static and Policy routing
- Built-in DHCP, NTP, DNS Server and DNS proxy
- Interface modes: port aggregated, loopback, VLANs (802.1Q and Trunking)
- L3 routing

Firewall

- Stateful inspection
- Operating Modes: L3 NAT/route and L2 transparent
- Policy objects
  - Predefined, custom and object grouping
  - Dynamic address book: IP addresses auto update when named VMs move
- NAT support: SNAT, DNAT, PAT, Full Cone NAT, STUN
- NAT configuration: per policy and central NAT table
- Schedules: one-time and recurring
- Virtual Systems: Up to 1000 vSYS

User and Device Identity

- Local user database
- User and device-based policies

Attack Protection

- Protection from: malformed packets, DoS/DDoS, DNS Query Flood, SYNFlood and ARP attacks

Application Control

- Over 3,000 applications that can be filtered by name, category, subcategory, technology and risk
- Each application contains a description, risk factors, dependencies, typical ports used, and URLs for additional reference
- Actions: block, reset session, monitor, traffic shaping

High Availability

- Redundant heartbeat interfaces
- vSSM: Active/Active
- vIOM: Active/Active
- vSCM: Active/Passive
- Failover:
  - Port, local & remote link monitoring
  - Stateful failover
  - Sub-second failover
  - Failure notification
- ISSU – In Service Software Upgrades

Administration

- Management access: HTTP/HTTPS, SSH, telnet, console
- System Integration: SNMP, syslog, alliance partnerships
- Dynamic real-time dashboard status and drill-in monitoring widgets
- Language support: English

Logs & Reporting

- Logging facilities: local memory and storage (if available), multiple syslog servers and multiple Hillstone Security Audit (HSA) platforms
- Reliable logging using TCP option (RFC 3195)
- Detailed traffic logs: forwarded, violated sessions, local traffic, invalid packets
- Comprehensive event logs: system and administrative activity audits, routing & networking, VPN, user authentications, WiFi related events
- IP and service port name resolution option
- Brief traffic log format option

vESA Capacities

- Max number of vIOM plus vSSM: 50
- Max number of policies – 60,000
- Max number of address objects
  - Addresses – 1,024,000
  - Address book – 16,381
- Max sessions – 3,400,000 per vSSM
- Max new sessions/sec – 9k
- Max mac table entries – 64k

Performance

- vIOM Forwarding Performance
  - 1500 byte packets – 10 Gbps

Unless specified otherwise, all performance, capacity and functionality are based on StoneOS 5.5R1. Results may vary based on StoneOS® version and deployment.