nuagenetworks
From Nokia

VIRTUALIZED SECURITY SERVICES

Nuage Networks Virtualized Security Services (VSS) is a software-defined security solution for data centers and wide area network (WAN) environments. It is based on the Nuage Networks Virtualized Services Platform (VSP) to help address protection, detection, and operational security challenges in cloud environments driven by emerging security threats and multi-tenancy. VSS is the industry's first distributed, end-to-end (cloud, datacenter, and branch) software-defined network security, visibility, and automation solution.

VSS extends Nuage Networks VSP, a software-defined networking (SDN) platform, with value-added security capabilities that provide contextual traffic visibility and security monitoring, as well as dynamic security automation for rapid incident response. VSS delivers these features in addition to inherent VSP capabilities to provide secure microsegmentation, policy automation, and policy enforcement.

Nuage Networks VSS Highlights

- End-to-End security across enterprise minimizes risks
  - Security spanning branch, datacenter and cloud
- Unified policy and visibility provides better security and manageability
  - Security across containers, multi-hypervisor VMs and bare-metal
- Dynamic security automation enables faster response to mitigate threats
  - Automates policy action in the network based on analytics
- Simplified deployment and management
  - No agents needed on guest OS

Cloud security challenges

Current network security models across datacenter and branch environments cannot effectively address new requirements driven by the move to cloud and an evolving threat landscape. VSS is designed to overcome critical obstacles to cloud security:

- **Lack of sufficient network segmentation inside the datacenter, as well as between remote branch sites and datacenters**
  Current perimeter-centric approaches to securing datacenters are proving to be insufficient to prevent new and emerging attacks that move laterally between workloads within a datacenter. In addition, a lack of sufficient end-to-end segmentation across the WAN poses additional security risks where an attacker can use the branch as an entry point to access applications and data inside the datacenter.
- **Lack of visibility of traffic inside the datacenter and across the WAN**
  Organizations lack the visibility and tools to detect advanced security threats across the datacenter, cloud, and branch networks. Based on a recent security survey, it takes, on average, several months from initial compromise to when an attack is actually detected.
- **Lack of automation**
  Current network security operations are largely manual and device-centric. It can take weeks to provision or modify security policies, including configuring network devices, firewalls, and security protocols for a new application or branch service. Incident response to suspected or identified attacks is manual and slow. The lack of automation for security tasks makes it difficult to deploy new applications and services on-demand, in minutes, on the most efficient resources as cloud architectures strive for.

- **Location-independent security policies and cloud mobility**
  A key requirement for cloud architectures is that applications and services be completely location independent, able to migrate freely to the most efficient resources on any server at any site in the cloud, without introducing dependencies in the application. Traditional security approaches cannot easily support location-independent workloads because security policies are defined by location of security devices or rigid network topologies. The traditional perimeter-centric network security model cannot effectively address security and visibility for east-west traffic inside the datacenter or traffic from WAN networks.

Key VSS features

As described above, security concerns can be a major challenge to cloud-readiness and the adoption of cloud architectures. The multi-tenant nature of cloud on shared or public cloud resources, coupled with manual security processes hinder on-demand deployments and scalability.

VSS supports a three-pronged security methodology with separate components and features to address each step in the security lifecycle:

1. **Prevent** security incidents by minimizing the attack surface with software-defined microsegmentation and policy enforcement across the cloud, datacenter, and WAN.

2. **Detect** security threats and monitor compliance with contextual network visibility and security analytics in real-time.

3. **Respond** faster to security incidents and breaches by automating remediation processes, such as quarantining suspicious applications or engaging deeper analysis tools.

To align with each of these security phases, the three-pronged VSS architecture comprises VSS Prevent, VSS Detect, and VSS Respond.

1. VSS Prevent: Segmentation, distributed security policy enforcement and centralized security policy management
VSS Prevent capabilities enable software-defined, end-to-end network segmentation. This minimizes the attack surface and prevents the spread of lateral malware by enabling microsegmentation for any workload (virtual machines, containers, and bare-metal workloads) within the datacenter, as well as by controlling user access from branch or WAN locations.

- **Software-defined segmentation and distributed security policy enforcement**
  Within the datacenter, VSS provides enforcement of fine-grained, application-specific security policies, also known as microsegmentation, for any workload. Microsegmentation effectively provides a “whitelist” approach to all traffic within the cloud network, blocking all connections between all applications except those that are explicitly allowed. This much more thorough approach to security policy management has been called a “Zero Trust” policy by Forrester Research, and is a rapidly emerging requirement for multi-tenant cloud networks.

  VSS includes a Layer 4 distributed firewall and enforces Layer 4 stateful Access Control Lists (ACL), as well as forwarding and service chaining policies for re-directing traffic to advanced security appliances, such as next generation firewalls (NGFWs) and intrusion prevention systems (IPS). Layer 4 ingress/egress ACLs can be centrally defined based on flexible groupings of end-points based on policy groups in Nuage Networks VSP.

Beyond the datacenter, VSS also provides software defined end-to-end segmentation and policy enforcement based on a common policy model across the enterprise WAN and datacenters. Layer 4 stateful ACLs can be used for better security at the branch perimeter to restrict user access to cloud applications. For example, access to the corporate network can be restricted to guest users.

The Nuage Networks Layer 4 distributed firewall, using Layer 4 stateful ACLs, has also been validated by independent PCI auditors for network segmentation in a PCI-compliant environment across datacenter and branch locations. Organizations can trust that VSS can be an effective tool to help meet compliance requirements in a payment card environment.

- **Simplified security management based on templates**
  VSS enables network security administrators to simplify security policy management across multiple virtual networks and automate compliance enforcement based on ACL templates. Security administrators can centrally define and manage network-wide security policies based on a template defined for specific applications or tenants.

  For example, the network security team can block the spread of a new worm or virus across enterprise networks. This can be done by making a template-level ACL change to block network communication based on a specific port or protocol used by the worm or virus. The resulting policy change quickly and automatically propagates to all relevant application or overlay networks, as needed.

- **Multi-layer security policy management**
  The multi-layer security policy management capability enables multiple teams, (such as the network security and application teams) to manage different aspects of the overall security policy. To ensure compliance, the network security team can control network-wide security policies, while providing application teams the ability to specify application-specific whitelist policies for microsegmentation between application tiers as dictated by the application design.

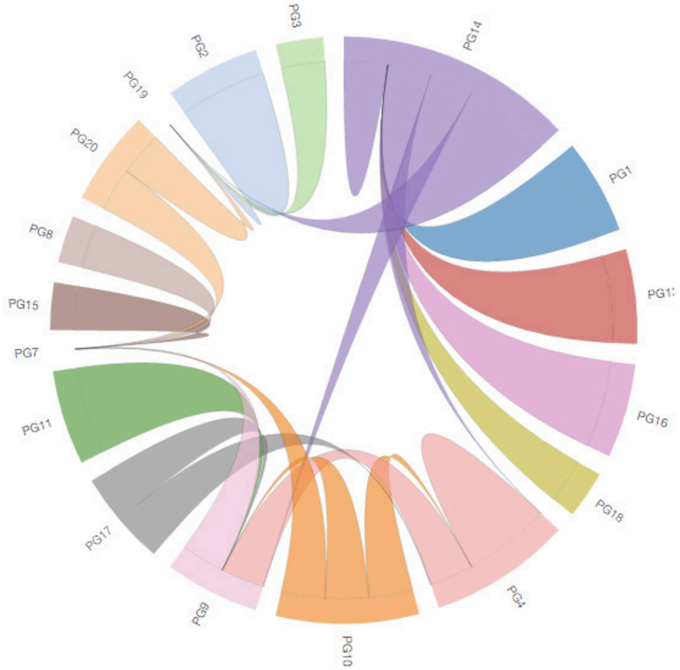
  This is achieved using an ACL sandwich, which is composed of the top, middle, and bottom layers of ACL entries. Network security teams can define the top and bottom layers as a part of the ACL template to specify all traffic that should never reach any of the end-points or deny traffic that isn't explicitly allowed by a matching ACL.

  Top and bottom layer ACLs from the template are combined with application-specific whitelist policies. ACLs, defined per domain instance in the middle layer to form an ACL sandwich, provide fine-grained policy for microsegmentation while ensuring compliance with overall network security policies.

2. VSS Detect: Visibility, security monitoring and analytics (requires VSS license for full functionality in addition to the Nuage Networks VSP)
VSS Detect provides security operations and auditors with contextual visibility of traffic flows, near real-time security alerts, and a dashboard of their virtual network across the datacenter and WAN.

- **Contextual flow visualization**
  For compliance validation, network security administrators and auditors can visualize traffic flows with context (e.g., policy group, and domain), both within the datacenter as well as between datacenters and branch networks. In addition, application flow mapping based on contextual flow visualization (e.g., Layer 4 protocol/ports information used by flows between application components or policy groups) enables auditing and definition of whitelist security policies for microsegmentation.

FIGURE 1. Flows per Domain



- **Virtualized network monitoring and security analytics**
  Network security and operations teams can get insight into network security events with near real-time security alerts, security dashboards, and reports based on ACL allow/deny hits and security events, as well as traffic analytics. Examples of security reports include:

- ACL deny/allow count vs. time within a domain or the entire enterprise
- Security events by source/destination policy groups, or within a domain
- Top source policy groups causing ACL denies within a domain.

FIGURE 2. VSS Enterprise ACL Deny vs Time

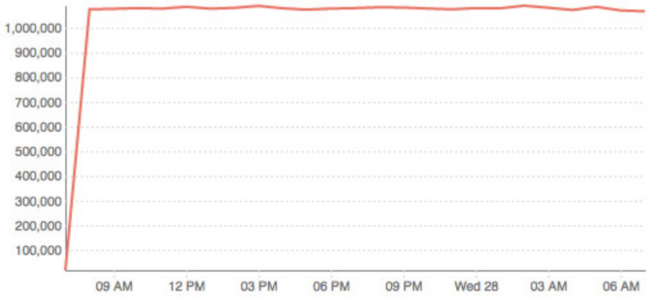


FIGURE 3. Count of Security Events by Source Policy Group

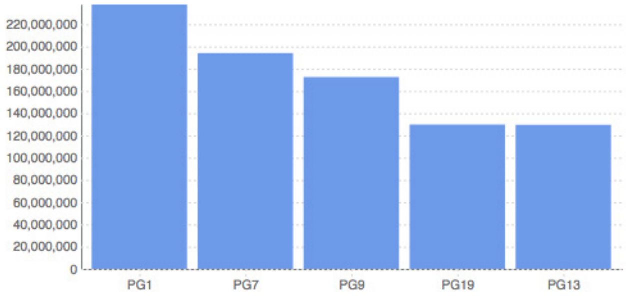
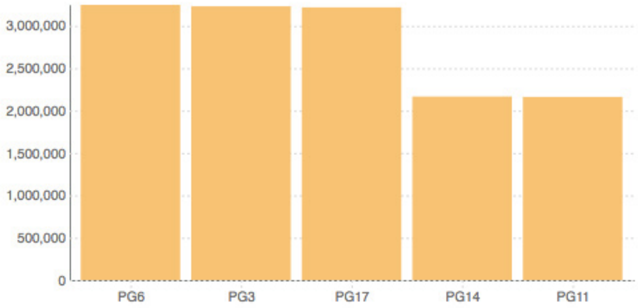


FIGURE 4. Top Destination Policy Groups by Count



- **Policy-based mirroring**
  Policy-based mirroring enables select traffic that matches an ACL entry to be mirrored to security analytics/traffic analyzers for more advanced threat analytics, business intelligence, or troubleshooting. Only traffic that matches a defined policy will be mirrored, so users can be selective about what they choose to analyze and not overwhelm the system. For example, users can choose to mirror suspicious traffic based on anomalous behavior that matches unusual ingress/egress ACL policies.

3. VSS Respond: Dynamic Security Automation (requires VSS license for full functionality, in addition to relevant VSP licenses)

VSS Respond enables rapid response to a security event or an incident by dynamically automating security policies and remediation steps to mitigate the attack in near real-time.

- **Alarm filtering with deeper analytics**
  For example, a threshold crossing alert can be defined based on a metric, such as ACL deny count (at the zone, policy group, vPort or subnet level). If the ACL deny count exceeds a threshold, the end point can be put into a suspect category and be more closely monitored by:

- Inserting advanced security services for traffic from suspicious end points (e.g., sending traffic to an NGFW or IPS)
- Mirroring select traffic from suspicious end points

Alerts with automated actions can be defined based on various metrics at particular vPort/policy group/zone/subnet levels, including Packets in/out, Bytes in/out, Dropped packets in/out, Anti-spoof packet count, ACL deny event count, and Anti-spoof event count.

- **Automated quarantine of affected end points**
  Another use case is to quarantine an infected end-point by dynamically re-assigning the infected end-point to a quarantine policy group to enforce a more stringent security policy and restrict communication from the quarantined end-point. This can be triggered by a security analysis from an external system such as a SIEM (security incident event manager) as a part of the incident response workflow.

VSS solution components

VSS requires the Nuage Networks VSP solution, (including the VSD and VSC SDN controller components). In addition, the VSS solution requires VRS for policy enforcement and flow visibility in the datacenter or private clouds, as well as NSG for branch environment.

Key features and benefits summary

CATEGORY	FEATURE	FEATURE DESCRIPTION	BENEFITS
VSS PREVENT			
	Layer 4 stateful, distributed firewall	■ Layer 4 ingress/egress ACLs can be centrally defined based on flexible grouping of end points at the Policy Group, Zone, Subnet levels. ■ Layer 4 forwarding ACLs can be defined to selectively steer traffic to re-direction targets such as NGFW or IPS. ■ Layer 4 security policies can be enforced using Nuage VRS as host for VM, containers as well as bare-metal, and at branch with the Nuage NSG. ■ Layer 4 distributed firewall was validated by independent PCI auditors for network segmentation in a PCI compliant environment.	■ Minimizes attack surface with microsegmentation and policy enforcement for east-west traffic inside the datacenter, as well as perimeter security in WAN environments. ■ Service chaining for advanced insertion of external security appliances (e.g., NGFW, IPS) inside the datacenter, as well as at branch locations. ■ Protects bare-metal, virtual machine, and container workloads seamlessly.
	Simplified security management based on ACL templates	Layer 4 stateful security policies (ingress/egress/forwarding ACLs) can be defined as a part of the template and automatically inherited for any domain that is instantiated based on the template.	Enables network security admin to automate compliance enforcement. Admins can centrally define and automate enforcement of Layer 4 security policies enterprise/tenant-wide across multiple virtual networks.
	Multi-layer security policy management using ACL sandwich	■ Top and bottom ACLs can be defined as a part of the template to specify all traffic that should never reach any of the end points or deny traffic that isn't explicitly allowed by a matching instance ACL. ■ Top and bottom ACLs are combined with application-specific whitelist policies/ACLs defined per domain instance in the middle layer to form an ACL sandwich that is both fine-grained policy for microsegmentation and compliant with overall network security policy.	Multi-layer security policy management capability using ACL sandwich feature enables multiple teams (network security and application team) to manage different aspects of security policies. It enables network security team to control network-wide security policies to ensure compliance while providing application teams the ability to specify application-specific whitelist policies for microsegmentation.
VSS DETECT			
	Contextual flow visualization	■ Visualize traffic flows between groups of end points (policy groups) within a domain. ■ Select a flow between policy groups and get details on flow (src ip/dst ip/src port/dst port/proto, bytes/packets) for each collection time-interval.	Provides contextual visibility to east-west traffic between VMs, containers and bare-metal workloads inside the datacenter, as well as traffic crossing the branch perimeter to validate compliance with policy.
	ACL analytics and alerts	Reports based on: ■ ACL allow/deny hits vs. time ■ ACL allow/deny hits by destination PG ■ ACL allow/deny hits by source PG Ability to define TCAs based on ACL metrics at PG/zone/subnet/vPort level.	Monitor and alert on ACL policy violations for compliance and early threat detection.
	Traffic analytics and alerts	Reports based on: ■ TCP conn vs. time ■ UDP traffic vs. time ■ ICMP vs. time Ability to define alerts based on traffic metrics (bytes) at PG/zone/subnet/vPort level	Enables detection of security attacks based on abnormal spike in network traffic (e.g., during DDoS attack).

	Security event analytics	Reports based on: ■ Security events by event type (ACL Deny, TCA alert event) ■ Security events by source PG	Provides a dashboard view into various security events happening in the SDN/SD-WAN environment for compliance monitoring.
	Policy based mirroring	Policy based mirroring provides mirroring of select allowed traffic matching an ACL entry.	Enables detection of advanced security attacks by selectively mirroring traffic to security analyzer for traffic that requires full packet inspection.
VSS RESPOND			
	Alerts with automated action	■ Threshold crossing alerts can be defined based on metric (average or absolute) exceeding a specific threshold value over a time period. ■ An automated action can be associated on a TCA event to move the end point/vPort to a new policy group. ■ Metrics include: Packets in/out, Bytes in/out, Dropped packets in/out, Anti-spoof packets count, ACL deny event count, and Anti-spoof event count.	Automates responses while the attack is happening by taking dynamic policy action (e.g., insertion of advanced security services/mirroring of traffic).
	APIs to automate incident response	Incident response systems can automate quarantine of an infected end point by using VSP APIs.	Shortens remediation process

VSS licensing

VSS capabilities are enabled with a feature license on existing VSD, VRS, and NSG components for software-defined security across datacenter and branch deployments.

- VSS license per VSD Analytics/Stats node enables Layer 4 flow collection, security analytics, as well as alerts with automated policy action.
- VSS license per VRS and NSG enables VRS and NSG to function as a security event and flow data source, providing near real-time information on Layer-4 flows, as well as security events.

nuagenetworks
From Nokia