Nuage Networks
Product Architecture

White Paper
# Table of Contents

Abstract .................................................................................................................. 3

Networking from the Application’s Perspective .............................................. 4
  Design Principles ............................................................................................. 4
  Architecture ................................................................................................... 4
  Integrating Bare Metal Resources .................................................................. 6

Overlaying WAN Environments ........................................................................... 7
  Software Defined WAN ................................................................................. 7
  Last Mile Flexibility ....................................................................................... 7

Policy-Based Automation ...................................................................................... 8
  Declarative Policies ......................................................................................... 8
  Intelligent Endpoint Interpretation ................................................................. 8
  Topology Modeling ......................................................................................... 9
  Service Chaining ............................................................................................ 9

Security .................................................................................................................. 10
  Microsegmentation ......................................................................................... 10
  Zero Trust Security Model .............................................................................. 11
  Consistent across hypervisors, containers, and bare metal ......................... 11
  “Bump in the Wire” Extensibility ................................................................. 11
  Auditing and Compliance .............................................................................. 11

Summary .............................................................................................................. 12

About ................................................................................................................... 13
Abstract

This White Paper describes the architecture and operation of Nuage Networks Software Defined Networking (SDN) product line.

The intent of this information is to provide insights into the underlying design philosophy, interoperation, and capabilities from both a high level (such as how it fits into a cloud ecosystem) and a detailed level (such as communications protocols).
Networking from the Application’s Perspective

Design Principles
The typical enterprise application is multi-tiered, consisting of front-end, business logic and database tiers. A cloud application cannot be delivered until the compute, storage and networking requirements for the service design have all been turned up. Network connectivity between application tiers is critical, with the understanding that each of the tiers has specific requirements in terms of access, visibility and resiliency.

The Nuage Networks SDN approach applies principles that have proven effective in scaling operations for the world’s largest wireless and IP networks. Technologies conceived for addressing dynamic mobility of wireless devices or secure service delivery to millions of subscribers can be elegantly applied to scaling cloud datacenter networks and addressing the challenges of networking dynamic application resources.

By extending the Popek-Goldberg virtualization theorems to the network, we created a new type of distributed network hypervisor that both enables nested overlays and bridges the performance gaps between overlays and underlays. These capabilities yield an efficient, reliable and elastic Compute Service Fabric.

Architecture
The Nuage Networks Virtualized Services Platform (VSP) Architecture is composed of three major layers. Each layer has its own form factor.

Cloud Service Management Plane – Virtualized Services Directory (VSD)

The Nuage Networks Virtualized Services Directory (VSD) is a policy & business logic engine that simplifies the definition of network services in an application-friendly context. It provides enterprise administrators the freedom to outline the networking requirements of their cloud applications in familiar IT constructs, and establishes policies that ensure the proper scope, security and integrity of application consumption in a manner consistent with enterprise guidelines.

Datacenter / WAN Control Plane – Virtualized Services Controller (VSC)

A Virtualized Services Controller (VSC) maintains the full view of per-tenant network and service topologies and instantiates network service templates defined through the VSD. Through the Nuage Networks VSC, distributed
virtual routing & switching constructs are established that incorporate hypervisors as direct extensions.

Leveraging an operating system that has proven its resiliency, scaling and performance over a decade of operating in the world’s largest Ethernet and IP networks, the Nuage Networks VSC is uniquely capable of driving comprehensive (L2-L4) network virtualization across thousands of tenant slices in a heterogeneous environment.

The VSC uses standard protocols to peer with existing networks, allowing it to discover full network topology and reachability. Through Openflow, it distributes relevant switching and routing information to hypervisors within the virtualized datacenter network.

To facilitate hybrid cloud deployments, the Nuage Networks VSC ensures seamless interconnection with business VPN services (L2 or L3), extending the virtualized datacenter environment to securely include enterprise locations.

Through federation of controllers, the Nuage Networks VSC scales elegantly and seamlessly to meet the expectations of the world’s largest and most demanding datacenter operators and cloud service providers.

Datacenter / WAN Data Plane – Virtualized Routing and Switching (VRS)

With the Nuage Networks solution, the network can react instantaneously, and in a manner consistent with policies, as virtual machines are turned up or removed. Nuage Networks Virtual Routing & Switching (VRS) extensions provide control of network interfaces across leading hypervisor platforms including VMware, KVM, and Xen.
**Integrating Bare Metal Resources**

Understanding that not all of the elements of today’s datacenter are currently virtualized, Nuage Networks also provides an elegant mechanism to integrate “bare-metal” assets such as non-virtualized servers and appliances through a comprehensive set of gateway solutions. For low volume deployments the software based VRS Gateway (VRS-G) module incorporates bare metal as virtualized extensions to the datacenter. For large scale and high traffic volume environments, the Nuage Networks 7850 VSG provides industry leading gateway functionality with native support for 1GE, 10GE and 40GE connections.
Overlaying WAN Environments

Software Defined WAN
By adding a Network Services Gateway (physical or logical) as an endpoint, MPLS WANs become part of the unified network fabric managed by Nuage Networks VNP. Nuage Networks VNS is based on an overlay model that uses any IP network to provide connectivity between sites.

Policy-driven Network Services

Figure 2. Network Services delivered over MPLS WANs are seamlessly delivered and managed

Last Mile Flexibility
This architecture provides maximum flexibility and the support of multiple access/last-mile technologies including copper, fiber or mobile broadband. Available networks from multiple providers can be mixed and matched as well as any available access technologies.
Policy-Based Automation

Declarative Policies
Network policies are defined in business terms using declarative policies (such as “You MUST use HTTP Authentication when accessing this application”) rather than rigid controls based on ever-changing IP addresses.

Intelligent Endpoint Interpretation
Each endpoint (e.g. hypervisor, router, and gateway device) intelligently interprets the declarative policy. In this fashion, a single policy stored in the VSD can be leveraged across private cloud, public cloud, datacenters, and WAN environments.

Policy-Based Automation for the Datacenter and the WAN

Figure 3. A single policy is intelligently and consistently executed across the entire network
Topology Modeling
Using the built-in User Interface or leveraging the REST API, even the most complex physical network topology can be modeled as shown in Figure 4. For convenience, the topology can also be defined in templates for use by other network teams or by application programmers.

Service Chaining
Leveraging the topology model, Service Chaining automation enables even the most complex automations to be performed. In the example shown in Figure 4, there are tiers of cascading firewalls for allowing the web interface to communicate with an application server running business logic (BL) that in turn communicates with a database server (DB). FW1 protects the datacenter from outside traffic while FW2 protects against successful intrusions within the datacenter. Since this topology is cumbersome to set up and maintain manually, service chaining automation is a key enabler for both sophisticated application topologies and cloud architectures.

Topology Modeling and Service Chaining

Figure 4. Even the most complex tasks can be automated – within and across clouds
Security

Microsegmentation
As shown in Figure 5, the Virtual Services Controller (VSC) provides control plane coordination (as indicated by the dotted line) among one-to-many Virtual Routing and Switching (VRS) components. The VRS data plane component includes both an embedded virtual switch (vSwitch) and a firewall.

This architecture enables full microsegmentation of Virtual Machine, Docker Container (not shown), and bare metal server-based application communications. Further, security protection begins at the initial connection to the network, thereby minimizing the overall security exposure surface.

Filling Security Gaps within the Datacenter

Figure 5. Providing consistent security starting at the first network attachment point.
Zero Trust Security Model
Networks by default are set up to facilitate communication. This mode is often referred to as “Full Trust” from a security perspective. Nuage Networks VSP, however, defaults to a “Zero Trust” security model by default. Any communications must be explicitly allowed by a policy. This enables any security model to be implemented — from micro-segmentation at the VM level all the way up to application-level controls. Since it prevents many default communications paths, it also minimizes the impact of manual errors upon security.

Consistent across hypervisors, containers, and bare metal
By leveraging the same architecture across multiple hypervisors, Docker Containers, and bare metal servers, Nuage Networks VSP provides not only high but also consistent levels of security across the entire network.

“Bump in the Wire” Extensibility
Nuage Networks VSP provides “bump in the wire” extensibility. Multiple partner products (e.g. firewalls and other security approaches) can inspect and operate on network traffic down to the packet level.

Auditing and Compliance
Every network event, including changes to security policies, is collected and stored in a robust Apache™ Hadoop® datastore (part of the Nuage Networks VSD). Auditing, threat detection and problem investigation are possible, effective and efficient with this granularity of logging.
Summary

Nuage Networks makes the entire network infrastructure as readily consumable as its compute resources. With the capabilities described in this White Paper, the network transforms into a powerful, highly automated and scalable fabric that instantaneously responds to the dynamic demands of workloads and applications.
About

Nuage Networks (www.nuagenetworks.net) brings a unique combination of groundbreaking technologies and unmatched networking expertise to the enterprise and telecommunications industries. The Silicon Valley-based start-up has applied radically new thinking to the problem of delivering massively scalable and highly programmable SDN solutions with the security and availability required by business-critical environments. Nuage Networks, backed by the rapidly growing IP division of Alcatel-Lucent (Euronext Paris and NYSE: ALU), has the pedigree to serve the needs of the world’s biggest clouds. The cloud has made promises – the mission of Nuage Networks is to help you realize them.