cohesivenetworks

White Paper

Cloud Security Best Practices

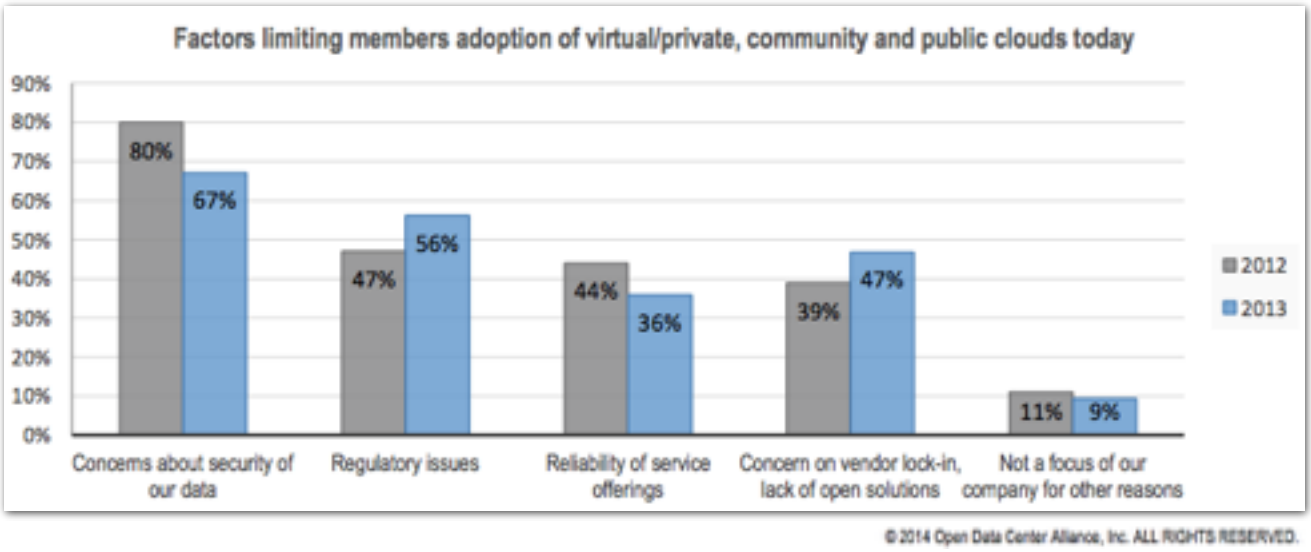
Part 1: Using VNS3 Overlay Network with Private, Public and Hybrid Clouds

October 2014

Introduction

Public cloud offers elastic, scalable, highly available and accessible infrastructure for enterprises of all sizes. The 2014 Gartner Magic Quadrant notes that Amazon's cloud (AWS) has more than five times the IaaS compute capacity than the next 14 providers listed, combined. No business can match that capacity for the same price as on-demand IaaS offerings, but is it safe?

The undisputed largest barrier to business cloud migration is security. According to the 2013 ODCA membership study, 40 percent of respondents cited security as the number one inhibitor to using cloud services. Yet, 79 percent of ODCA member companies said they run about 20 percent of operations using external cloud services.



Cloud IaaS offers an affordable data center extension, yet application-layer security is very different in cloud. Security is largely up to users. Gartner analyst Lydia Leong writes,

> *"IT managers purchasing cloud IaaS should remain aware that many aspects of security operations remain their responsibility, not the cloud provider's. Critically, the customer often retains security responsibility for everything above the hypervisor."*

Essentially, providers manage Layers 0 - 3 while end users must secure the hypervisor up through application. Concerns and pain points such as network encryption in third party environments, role-based access control, and intrusion detection must be fully controlled by the enterprise.

Security, customization and control were the conceptual backdrop to the creation of Cohesive's overlay networking product, VNS3. As Cohesive began to put its own computing systems into the cloud, we were uncomfortable with the loss of control of our network infrastructure. Our cloud migration project allowed us to begin assessing what critical capabilities network virtualization needed to provide to our enterprise customers.

VNS3 is the only application-centric networking product that offers highly available overlay networks connectivity with end-to-end encryption. VNS3 combined with Docker container-based network features allows users to build network functions into a single, secure network. "security lattice" as a similar if not better security strategy than in the traditional enterprise data center. Data-in-motion encryption ensures application owners maintain highly segmented and secure overlay networks.

VNS3 Solution Cases

European mobile application provider improve quality, speed and scale by running dev/test environments in the cloud.

The mobile app provider needed to connect multiple cloud-based dev/test topologies to their existing data center assets while guaranteeing encryption for all data in motion.

The firm uses VNS3 to launch potentially unlimited identical dev/test topologies and connect those topologies to their existing data centers for integration between internal and cloud version control.

European clothing designer scales and controls capacity expansion to the cloud.

A global fashion retailer, designer, and wholesaler created a fashion social networking site with the ability to scale up and down with demand while ensuring secure, encrypted data in motion between the application and the data center.

The VNS3 solution provides controls to accommodate internal corporate security requirements normally not available with public cloud infrastructure.

Sports association scales up to public cloud during championship series.

During international events the sports league needed extra capacity, stability and security for increased website traffic, event applications and nimble data analytics but did not want to manage infrastructure.

VNS3 gives the association the ability to scale in a variety of cloud regions while providing end-to-end encrypted access to their database servers running in their corporate data center.

Large ERP vendor shift data center complexities away from clients to reinvent their subscription SaaS business model.

The ERP vendor wanted to turn a traditional software solution into a cloud-based, subscription SaaS offering. They needed security, connectivity and flexibility when migrating from customer on-premise installations to public cloud.

VNS3 allows the ERP vendor to gain multi-tenancy without re-architecting their application. The vendor guarantees secure customer data and maintains control with integrated NOC services across clouds.

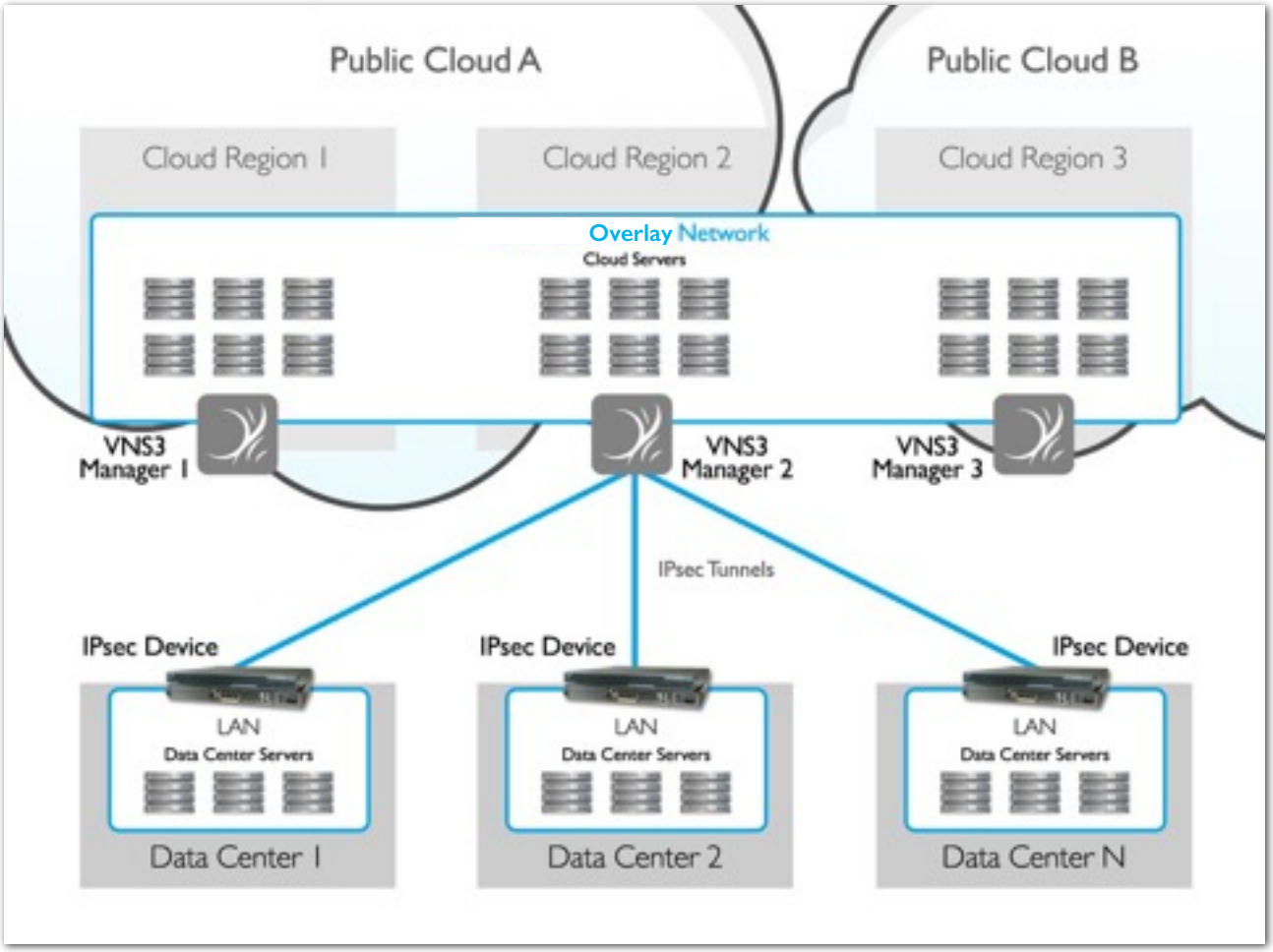
VNS3 Overview

What is VNS3?

VNS3 is a cloud-based networking solution, delivered as a virtual machine for any cloud environment. Since its launch in 2008, VNS3 has secured hundreds of millions of customer device hours in public, private and hybrid clouds.

VNS3 functions as a hybrid virtual networking device. VNS3 provides network control and security at layer 4-7 using the Docker container system. With over 1,000 connected customers in more than 20 countries, VNS3 offers customers enhanced network services on top of the cloud platform network. Common use cases include VLAN peering, encryption for data in motion, multicast support and multi-region or multi-cloud SSL termination, and intrusion/extrusion detection.

Customers benefit from secure, connect and integrated cloud networks by using VNS3. It is delivered as software in a virtual machine, and can easily integrate with existing networking equipment. Because it uses all the same standards as traditional networking solutions, VNS3 does not require additional work to implement.



Extend Your Network to the Cloud

VNS3 lets customers extend data centers into the cloud, making it easy for users to capitalize on public cloud benefits, support IT innovation and control every aspect of enterprise-to-cloud connectivity.

Public cloud environments are controlled by a third party where application owners have no insight, visibility or control over the underlying systems and hardware. Users can overlay networks on top of the cloud network to extend data center networks into the cloud with VNS3. Users can run cloud topologies as required, pass internal and industry audits and attest that a cloud deployment is in the control of the internal IT organization.

VNS3 Best Practices

Run key business computing topologies in the cloud with the required secure access to the corporate data center. VNS3 creates secure and encrypted VPN connections to cloud deployments using standard IPsec tunnels and data-in-motion encryption in the cloud.

Control: Regain control of addressing, protocols and encrypted communications in third party controlled cloud environments. VNS3 uses encrypted overlay networks to assign IPs and use cloud disabled protocols (e.g. UDP Multicast) as required for deployment.

Secure: Encrypt data in motion to, from, and in the cloud.

Extend: Achieve cloud network mobility and agility by extending connectivity to a cloud VNS3 deployment or multiple VNS3 deployments across disparate clouds.

Federate: Configure VNS3 managers in a mesh to eliminate vendor lock-in and allow for high availability, geographic distribution, and cloud federation.

Reuse: Integrate VNS3 with existing edge and DMZ equipment like IPSsec extranet, intrusion prevention, IDS and stateful inspection devices. VNS3 requires no new knowledge or training to implement.

Comply: Meet compliance requirements by confidently attesting to security and control measures the application owner implemented and managed.

Configure: Dynamically launch and configure a software-defined network (SDN) to deploy in minutes using a REST API or web-based interface.

What Makes VNS3 Unique?

We've changed the cloud networking game with the latest VNS3 with Docker container integration. Cloud users can now load applications into a single VNS3 Manager instead of building separate, costly virtual machines (VMs). Customers can build custom functionality such as load balancing, proxy, and network intrusion detection (NIDS), into their VNS3 Manager instance to match their networking use case. Each containerized VNS3 network saves VM run times, simplifies network management, and bundles applications functions in the same VM instance as VNS3.

Unlike hardware solutions, VNS3 customers can control cloud-based projects using their own software. Enterprise cloud users can guarantee secure access between corporate data centers and cloud-based systems using end-to-end encryption and federated multi-cloud overlay networks.

VNS3 is different from other networking products because it creates a customer-controlled network on top of underlying cloud networks. This "overlay network" opens up cloud computing for even more possibilities, including ways to connect and secure data centers and businesses not allowed in public cloud networks.

Previously, security and networking solutions could not guarantee the level of access and accountability enterprises need to attest to industry and regulatory specifications. Plus, VNS3 is provider, vendor, application, OS and script neutral. This eliminates the risky and painful "re-architect everything" attitude typical of many cloud computing solutions. Built using industry standards, VNS3 allows users to reuse existing network infrastructure and expertise. VNS3 is the only overlay networking product that offers both a highly available overlay network and end-to-end encryption.

VNS3 Availability

VNS3 is available in all major public/private clouds that all image import:
Amazon EC2 and VPC, IBM Softlayer, Google Compute Platform, HP Helion, Verizon Cloud and Terremark, Interoute, Abiquo, Rackspace, Flexiant, ElasticHosts, and CloudSigma.

VNS3 is available in the following virtual formats: OVF, VMware, KVM, Xen, OpenStack, Eucalyptus, and VMware (all formats).

Additional clouds without image import functionality can use VNS3 but Cohesive Networks would need to build the VNS3 Image in the customer's account for an additional fee. Contact sales@cohesive.net for custom image questions.

Learn More

Cloud Security Best Practices Part II: Layers of Security

Part II of the Cloud Security Best Practices White Paper will explore the layers of control in public, private and hybrid clouds and how users can create an effective "security lattice" strategy.
Download the PDF here.

Contact for Additional Information or Demo - contactme@cohesive.net

Our solution architects are available to provide additional information about VNS3 or schedule a demo of the features, functions, and common solution cases.

Contact for Overview of Services - services@cohesive.net

Enterprises looking to leverage the potential benefits of Cloud Computing are faced with a wide range of hurdles during their migration. Cohesive Networks is an award winning market leader in cloud networking. Through our delivered cloud migration engagements we have designed many Overlay Network architecture ranging in complexity. Cohesive provides a range of cloud and virtualization specific professional services to help enterprises achieve their cloud-based goals.

View our VNS3 Use Cases Webinar series - www.cohesive.net/webinars

Cohesive Senior Solution Architect, Sam Mitchell, is presenting a three part webinar series on VNS3. Recordings of all webinars will be made available after the original air date.

- VNS3 Best Practices - Part 1 of 3
  The VNS3 Webinar series will begin by introducing VNS3. Sam walks through the history of VNS3, working with VNS3, the compatibility with public clouds, and a preview of the next 2 webinar use cases.

- VNS3 Solution Cases - Part 2 of 3
  This webinar will begin by reviewing some of the topics covered in the VNS3 Best Practices webinar. Sam will then walk through VNS3 technical features and use cases, diagram how we use overlay networks to solve cloud security issues, and preview the next webinar's specific use cases.

- VNS3 Life in the Cloud - Part 3 of 3
  VNS3 has helped businesses migrate to the cloud, connect securely to data centers or across clouds and ensure secure connectivity. With specific case studies, Sam will explore the real-life uses of VNS3 with enterprise IT Cloud scenarios. We will wrap up the 3-part series and a preview the next series, "VNS3 Everywhere."

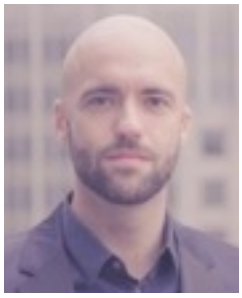
About the Authors

Patrick Kerpan, CEO

Mr. Kerpan is responsible for directing product, technology and sales strategy. Mr. Kerpan brings more than 20 years of software experience to the role of CEO and was one of Cohesive's founders in 2006. Previously he was the CTO of Borland Software Corp which he joined in 2000 through the acquisition of Bedouin, Inc., a company that he founded. Mr. Kerpan was also the vice president and general manager of the Developer Services Platform group at Borland, where he was instrumental in leading the Borland acquisition of StarBase in 2003. Before founding Bedouin, Inc., Mr. Kerpan was a managing director responsible for derivatives technology at multiple global investment banks.

Chris Swan, CTO

Chris Swan is CTO at Cohesive, where he focuses on product development and product delivery. Chris was previously at UBS where he was CTO for Client Experience working on strategy and architecture for web and mobile offerings across all regions and business divisions. At UBS Chris was co-head of Security CTO focussing on identity management, access control and data security. Chris represented UBS as Director on the Steering Committee of Open Data Center Alliance (ODCA), an industry association focussed on enterprise cloud adoption.
Before joining UBS he was CTO at a London based technology investment banking boutique. Chris previously held various senior R&D, architecture and engineering positions at Credit Suisse, which included networks, security, data centre automation and introduction of new application platforms. Before moving to the world of financial services Chris was a Combat Systems Engineering Officer in the Royal Navy. He has an MBA from OUBS and a BEng from the University of York.



Sam Mitchell, Senior Cloud Solutions Architect

As Senior Cloud Solutions Architect, Sam Mitchell leads all technical elements of the global sales cycle. Mitchell runs demos, technical qualification, technical account management, proof of concepts, technical and competitive positioning, RFI/RFP responses and proposals.
Before Cohesive, Mitchell was a Cloud Solution Architect at Platform Computing, which was recently acquired by IBM. He was also a Lead Architect at SITA, where he headed up OSS BSS Architecture, Design and Deployment activities on SITA's cloud offerings.

Referenced Works

Open Data Center Alliance (ODCA). 2013 annual ODCA membership survey. 18 March, 2014. http://www.opendatacenteralliance.org/docs/ODCA_2013MemberSurvey_FINAL.pdf

Leong, Lydia; Toombs, Douglas; Gill Bob; Petri, Gregor; Haynes, Tiny. Magic Quadrant for Cloud Infrastructure as a Service. 28 May 2014. http://www.gartner.com/technology/reprints.do?id=1-1UKQQA6&ct=140528&st=sb

Leong, Lydia. Gartner Research - Gartner for Business Leaders. Research Roundup for Cloud Infrastructure as a Service, 2012. 19 July 2012 http://my.gartner.com/portal/server.pt?open=512&objID=256&mode=2&PageID=2350940&resId=2086515&ref=QuickSearch&sthkw=hybrid+cloud+security

Cearley, David and Heiser, Jay. Gartner Research - Gartner for Business Leaders. Hype Cycle for Cloud Security, 2012. 27 Jul. 2012 http://my.gartner.com/portal/server.pt?open=512&objID=256&mode=2&PageID=2350940&resId=2096517&ref=g_portalfromdoc&content=html%23f-N66498