cohesivenetworks
Connect. Federate. Secure.

How VNS3 Enhances Your Azure Cloud

Recover the insight, visibility, and control you lose in third-party-controlled environments. VNS3 allows customers to deliver improved security, connectivity, and compliance while minimizing complexity. Here are some of the highlights of VNS3 when deployed in the Azure cloud:

Encrypt ALL Data-in-Motion

Public cloud should be considered a Zero Trust environment. VNS3 not only encrypts all data-in-motion but it does this while meeting or exceeding many industry standards (like HIPAA, PCI, FIPS, etc.). Utilizing AES-256, 3DES cipher suites, or custom keys, your data is protected to, from, and within cloud networks.

Micro-Perimeters and Network Segmentation

VNS3 allows you to create micro-perimeters at your application edge to isolate and protect your sensitive applications, in and between the cloud and datacenter. Our application-centric firewall further segments application traffic to prevent east-west vulnerabilities in your deployment. VNS3 improves the speed, efficiency, and simplicity of segmenting your entire network.

High Availability and DR

VNS3's IPSec active/active or active/passive failover uses state-of-the-art protocols to minimize connection downtime. Our meshed network can be deployed across multiple availability zones, regions or cloud providers which ensures connectivity is always up. VNS3 instance recovery allows you to meet your MTTR goals, should the worst happen.

Connect and Federate

VNS3 makes it easy to connect any network to another, you can connect overlapping virtual network subnets and remote subnets that are advertised via IPSec tunnels, including the use of public IPs for encryption domains. VNS3 can be deployed in any virtual environment individually or as a meshed network allowing a unified network across multiple regions, availability zones and cloud providers.

Monitor and Troubleshoot Your Cloud Networks

Get increased visibility into your network with improved status information and access to VPN connection logs. VNS3 provides status APIs, SNMP traps, and access to IPSec logs for on device consumption or remote delivery.

Extend and Customize With Network Plugins

Use VNS3’s ever-expanding list of plugins to extend the functionality of your network. Add new network functions such as SSL termination, Web Application Firewall, Network Intrusion Detection/Prevention, proxy, load balancing, content caching, monitoring or other layer 4-7 network services, directly in the VNS3 instance running at the edge of your application

Flexible VPN Configuration Options

VNS3 allows you to support multiple VPN policies, with no capped limits on the number of connections. Mix and match native IPSec and NAT-T within Route and Policy based VPNs with ease.

Reduce Costs and Avoid Vendor Lock-In

As individual cloud services multiply and scale they become expensive, by consolidating VPN, NAT, Peering and others into one VNS3 appliance your deployments remain simple, more cost effective and above cloud, giving you the agility to adapt to change.

Cloud Multicast in Azure

Azure and most other clouds do not offer support for multicast. VNS3 enables multicast in the cloud by redistributing the normally blocked protocol via the Overlay Network.

Simple (not Simplistic) Deployments

VNS3's intuitive interface allows for a user friendly configuration experience or you can launch and configure VNS3 using your current CI/CD pipelines and automation frameworks with our comprehensive API. Should you get stuck our excellent support team will be able to assist.