Nominee: Cohesive Networks' VNS3

Nomination title: Software Defined Networking Tackles Security - Cohesive Networks' VNS3

VNS3 is different from other SDN and network function virtualisation (NFV) solutions by creating a customer-controlled overlay network on top of the underlying network backbone. VNS3 users can distribute networks across multiple data centres and cloud networks to create one logical group of federated resource, while managing servers as if they are running on-premises.

The software-defined networking (SDN) features of VNS3 give users access, visibility and control from the application layer. VNS3 is a hybrid of five devices in one: a router, switch, firewall, IPsec/SSL VPN concentrator, protocol redistributor and dynamic and scriptable SDN. It can be configured "in a mesh," so it can extend to multiple sites at once. VNS3 separates network location and network identity, which translates into agility and mobility for cloud users. Encrypted data-in-motion and site-to-site IPsec connectivity allow users to extend an existing data centre network to any cloud environment.

VNS3 also includes Docker container integration. Docker is a open-source virtualisation platform that allows VNS3 users to run application as a lightweight container inside VNS3 virtual machines (VMs). With container plugins, VNS3 users can load network functions into a single VNS3 device instead of building separate, costly VMs. Production customers use Nginx reverse proxy, Snort Network intrusion detection (NIDS) and HAProxy load balancers.

VNS3 provides SDN capabilities that give control over IP addressing to create IP address for cloud servers, network topology to assign (and move) IPs to any server on any cloud, protocols to enable and disable protocols such as UDP Multicast, and encrypted communications to secure all data in motion, to, from and within the cloud.

VNS3 is completely unique in that it is provider, vendor, application, OS and script neutral. VNS3 is the only overlay SDN product that offers both a highly available overlay network and site-to-site IPsec connectivity with end-to-end data in motion encryption.

Over 2000 customers use VNS3 to built highly available overlay networks to partner and customer with site-to-site IPsec connectivity and end-to-end data in motion encryption. Other cloud network routing and security appliances are typically hardware or virtual appliances that don't allow customers access or customisation.

Since launch, VNS3 has secured over 200M virtual device hours in data centres, private clouds and public cloud. VNS3 is available in most major public clouds including Amazon, Google, IBM Softlayer, ElasticHosts, Flexiant, and Rackspace. VNS3 also runs production workloads in virtual Infrastructures including VMWare, Citrix, Xen, and KVM data centres.

VNS3 provides overlay software defined networking (SDN) capabilities in both data centre and cloud environments.

Users are able to create one logical group of federated resource across multiple data centres and cloud networks, while managing servers as if on-premises.

SDN capabilities give control over IP addressing, protocols such as UDP Multicast, end-to-end encryption for all data in transit.

Container plugins load functions into one VNS3 device for additional network capabilities such as reverse proxy, Network intrusion detection (NIDS) and load balancers.

VNS3 is the only overlay SDN product that offers both a highly available network and site-to-site IPsec connectivity.

Why nominee should win

- 96% of VNS3 customers renew each year

VNS3 users typically grow their business by more than 50% annually

- VNS3 secures and connects critical enterprise data in any network, in any cloud, using any networking device.

- A software-only network appliance adds security at the application layer.

- VNS3 virtualises critical network security functions, including routing, switching, firewalls and SSL VPNs.

- VNS3 works as a hybrid device to connect virtual networks across data centres and clouds.