cohesivenetworks

Your applications secured

10 Ways VNS3 Enhances your VPC

VNS3 and Amazon Web Services VPC

Want to do more with your AWS Virtual Private Cloud (VPC)? We have 10 ways you can enhance VPC for your more complex, important, and larger cloud networks with our virtual appliance, VNS3.

1. Encrypt ALL data-in-motion

   Traffic in AWS EC2 and VPC traverses an untrusted, 3rd party controlled network in plain text. VNS3 encrypts all your data to, from, and within the cloud using unique keys only you control.

2. Monitor all your virtual networks from a single network console

   VNS3 provides a dashboard to manage and monitor your VNS3 network and VPN connections as well as all your VPC network components (CIDR, subnets, route tables, ACLs, security groups, etc.).

3. Add IPsec interoperability and flexibility

   The only AWS VPC encryption algorithm for IPsec VPN connections is AES-128. VNS3 supports a wide range of encryption algorithms to accommodate industry regulations (like HIPAA, PCI, FIPS, etc.), internal requirements or the demands of connecting parties.

4. Connect across Availability Zones, Regions, and into other clouds

   VPC Peering limits you by the number of VPCs you can peer, and is only available for intra-region networks. VNS3 subnets can span across Availability Zones, Regions and even into other clouds.

5. Reduce your bill

   Separate NAT AMIs and VPC IPsec services run up your EC2 bill. VNS3 provides IPsec and NAT capabilities in one virtual instance.

6. Manage network address overlap

   VNS3 can map network address ranges, so you can connect both overlapping VPC subnets and remote subnets that are advertised via IPsec tunnels.

7. Eliminate Public IP Address Conflict

   The Amazon VPC VPN system globally only allows a single VPC per region to connect to any public IP address. VNS3 can connect to any number of IPsec endpoints and even handle address overlap, so you don't get locked out of mission-critical connections.

8. IPsec with NAT-Traversal encapsulation or GRE over IPsec

   VPC only supports native IPsec. VNS3 can negotiate tunnels with native IPsec, NAT-T IPsec or GRE over IPsec.

9. Use Multicast

   AWS 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.

10. Extensibility

    Add SSL termination, proxy server, load balancing, content caching or other network services directly to the VNS3 instance using Docker containers.

Chicago | London | Palo Alto
contactme@cohesive.net

US toll-free: +1 888 444 3932
UK: +44 208 144 015
www.cohesive.net/vpc

cohesive networks