Cloud Security Best Practices

Cohesive Networks - your applications secured

Our family of **security and connectivity solutions**, VNS3, protects cloud-based applications from exploitation by hackers, criminal gangs, and foreign governments.

2000+ customers in 20+ countries across all industry verticals and sectors

NETWORKcomputing WINNER 2016

amazon web services | Partner Network
TECHNOLOGY PARTNER

Microsoft Azure Certified

CIO Review Top 20 Most Promising Enterprise Security Company 2015

CenturyLink™
Cloud Marketplace Provider

2016 DCS AWARDS

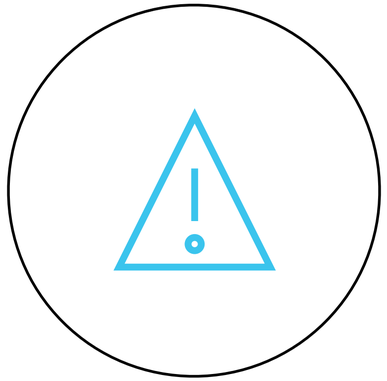
HP Helion Ready

14/15 Cloud INNOVATION WORLD CUP WINNER

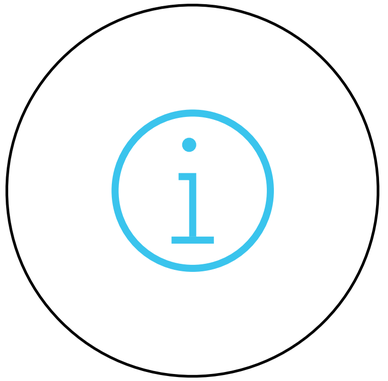
Business Partner IBM™

New realities of cybersecurity

Attacks have become professional: hackers, criminals or foreign governments.



In the post-Sony era, all servers “on a wire” are compromised or targets.



Regulatory implementation and reporting demands are increasing.

Cohesive Networks VNS3 is the "Top of Cloud" network security solution

Cloud Customer

Cloud Service Provider

Layer 7
Layer 6
Layer 5
Layer 4
Layer 3
Layer 3
Layer 2
Layer1
Layer 0

cohesivenetworks VNS3

Cloud Layer 3 Network
(minimal tenant features)

vmware NSX
Open vSwitch An Open Virtual Switch
Juniper Networks OpenContrail
OpenFlow
PLUMgrid
Cisco

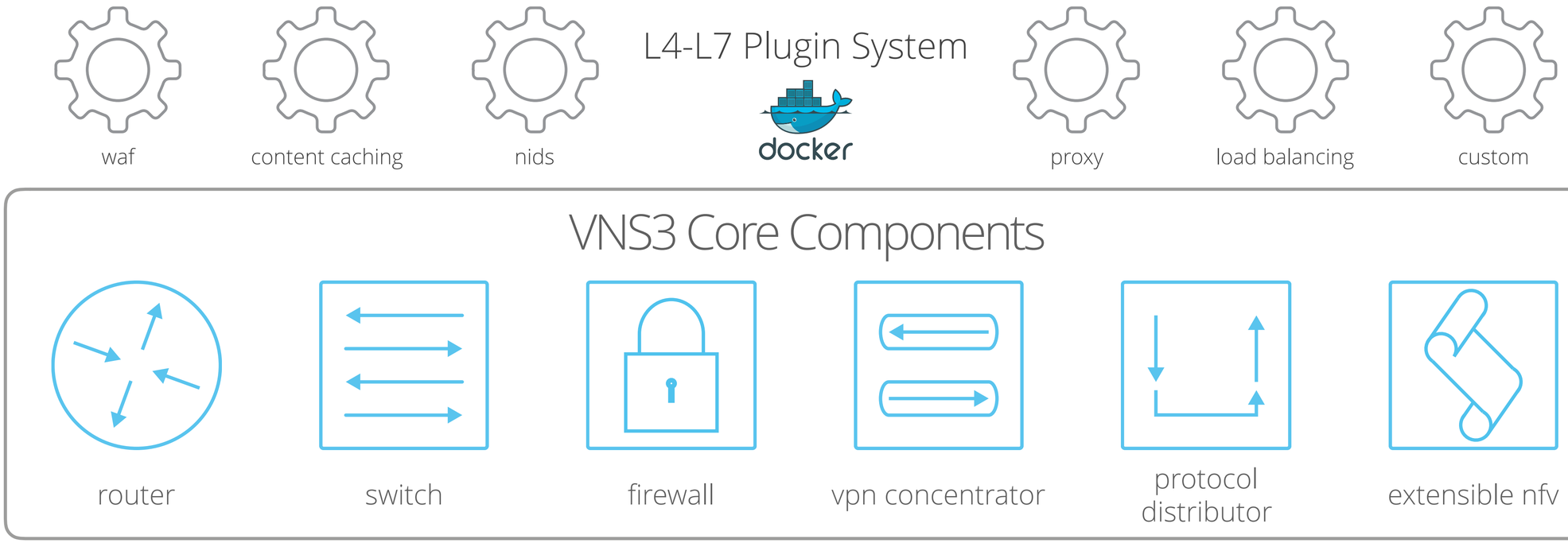
Application Policies You Control

Limit of user access, control and visibility

Hypervisor You Don't Control

Hardware You Can't Get To

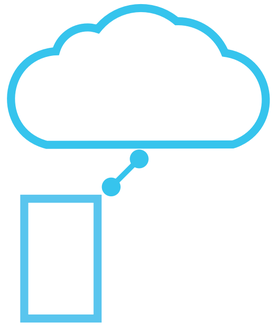
VNS3 provides connectivity and security + L4-L7 plug-in system



VNS3 is a **software-only virtual appliance** you deploy in your cloud/virtual infra to bring all the the connectivity and security controls normally available at the data center edge to your application edge. With the option Overlay Network, you can also **encrypt all data-in-transit** to, from and within your application deployment.

VNS3 enables production cloud use-cases

Partner/Customer Networks



Cloud VPN

Security & Compliance

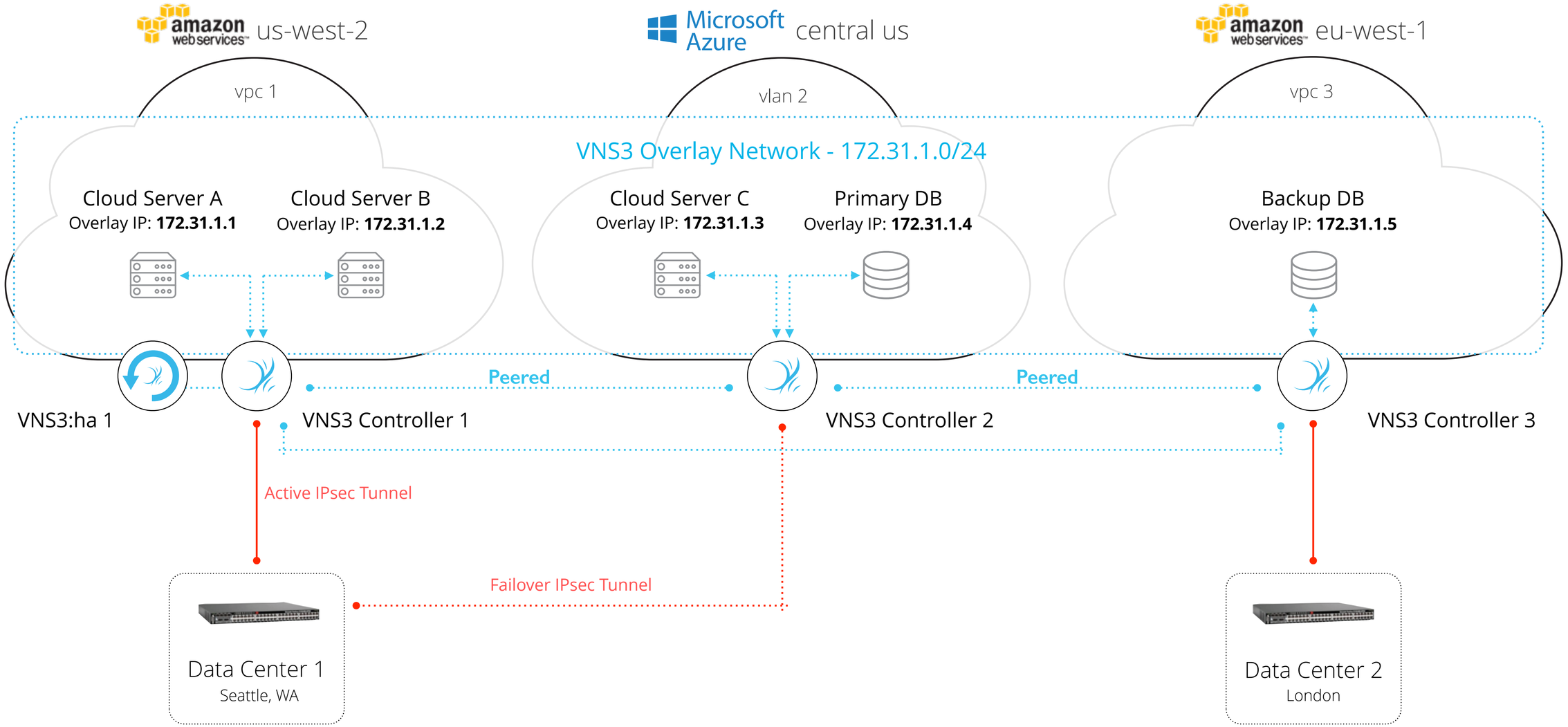
Rapid Dev/Test

App Segmentation

Private Cloud

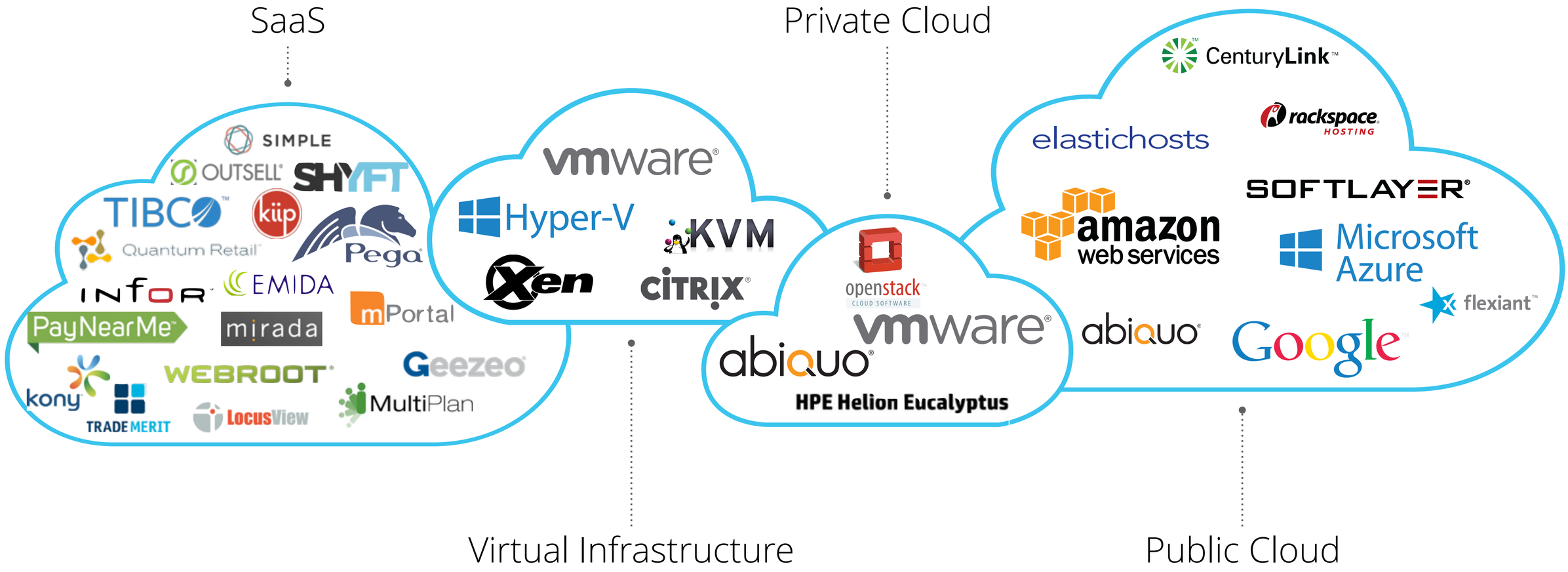
Cloud DR

VNS3 allows topology control

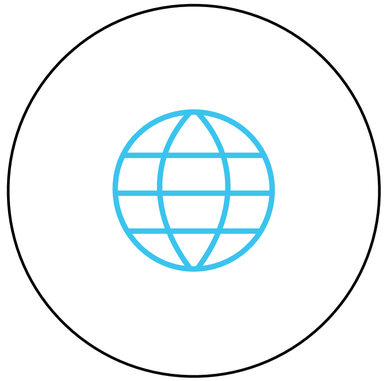


VNS3 is available everywhere

Cohesive is the **critical security and connectivity component**



Cohesive Networks



Our customers can use any product made by any traditional network vendor - and choose us.

Security and connectivity at the top of the public and private cloud is a key B2B growth area.

The cloud is growing all of our businesses. Let's grow together and securely.

Your Applications Connected and Secure

VNS3 Best Practices

Cloud security best practices

Defense in Depth

- Shared Responsibility
- NIDS and WAF
- Virtual Firewall
- Overlay Network

Overlay Network

- Encrypted TLS tunneled Overlay Network
- Lock Down overlay communication to only UDP 1194 in/out
- Check out Clientpacks
- Use Clientpack Name Tag
- Disable unused clientpacks
- Run multiple VNS3 controller instances to provide Overlay HA via VNS3 Peering
- NAT traffic through the VNS3 controller to the public Internet

IPsec Site-to-Site

- Explicitly match all IPsec parameters
- Policy based IPsec VPN
- Algorithms, hashing, DH, PFS, PSK, and lifetimes
- Run multiple VNS3 controller instances to provide IPsec HA

Secure Administration

- Separate UI and API passwords
- Use Static IPs (DNS name resolution where available)
- Use multifactor/multiparty authentication for Remote Support
- Image Size
- Use VNS3 Snapshots
- Use VNS3:ms for management and monitoring

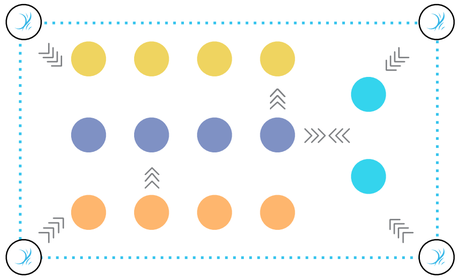
Understand the security shared responsibility model

Cloud Customer

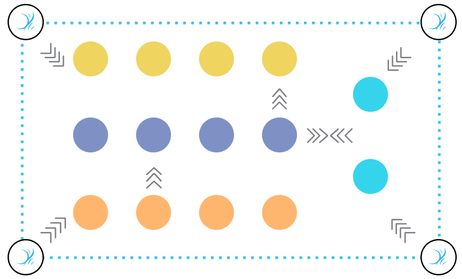
Cloud Service Provider

Layer 7
Layer 6
Layer 5
Layer 4
Layer 3
Layer 3
Layer 2
Layer1
Layer 0

App 1



App 1



Cloud Layer 3 Network
(minimal tenant features)

Application Policies You Control

Limit of user access, control and visibility

Hypervisor You Don't Control

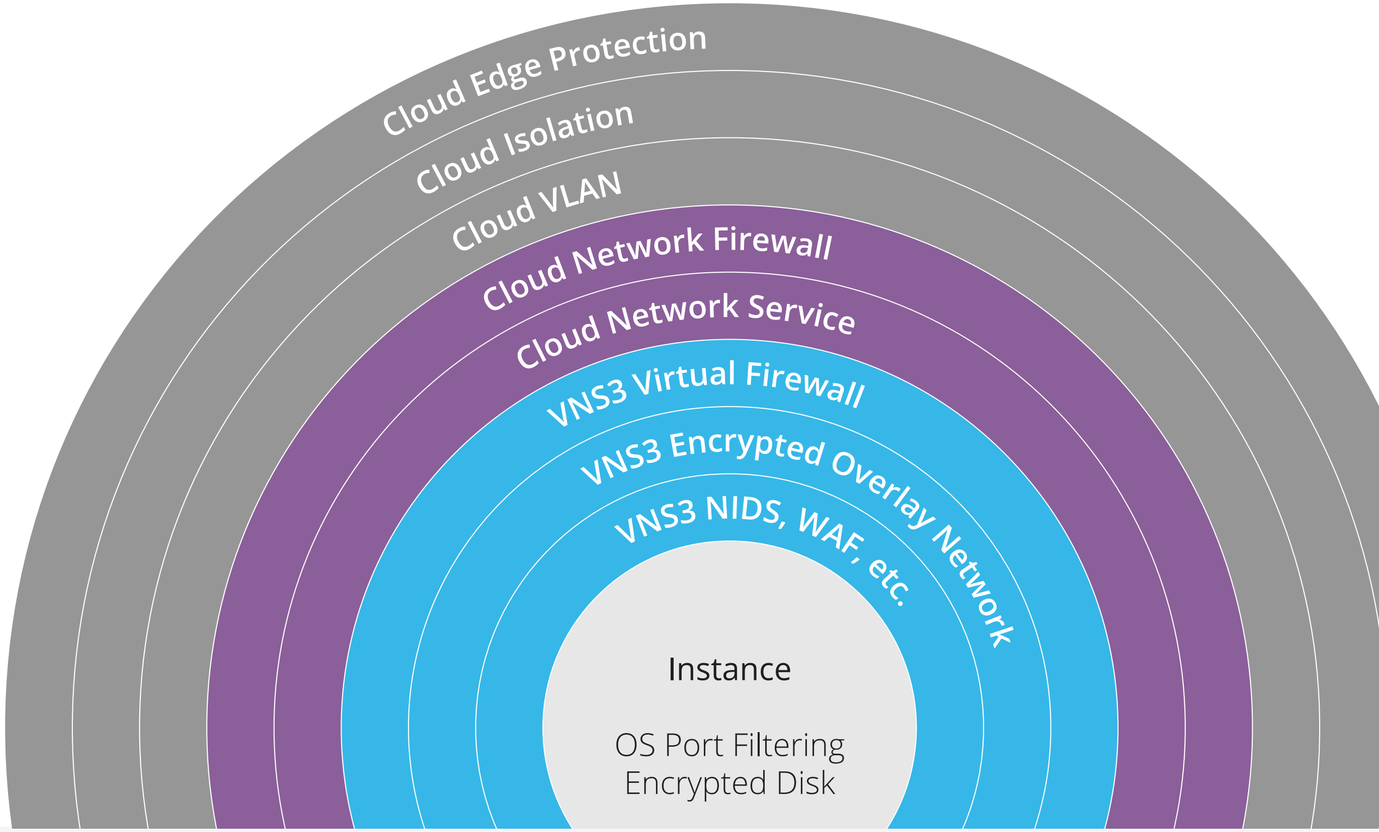
Hardware You Can't Get To

Build layers of control and access

Cloud networks combine with user & provider firewalls and isolation features to create a “security lattice” with layers of security

Key security elements must be controlled by the customer, but separate from the provider.

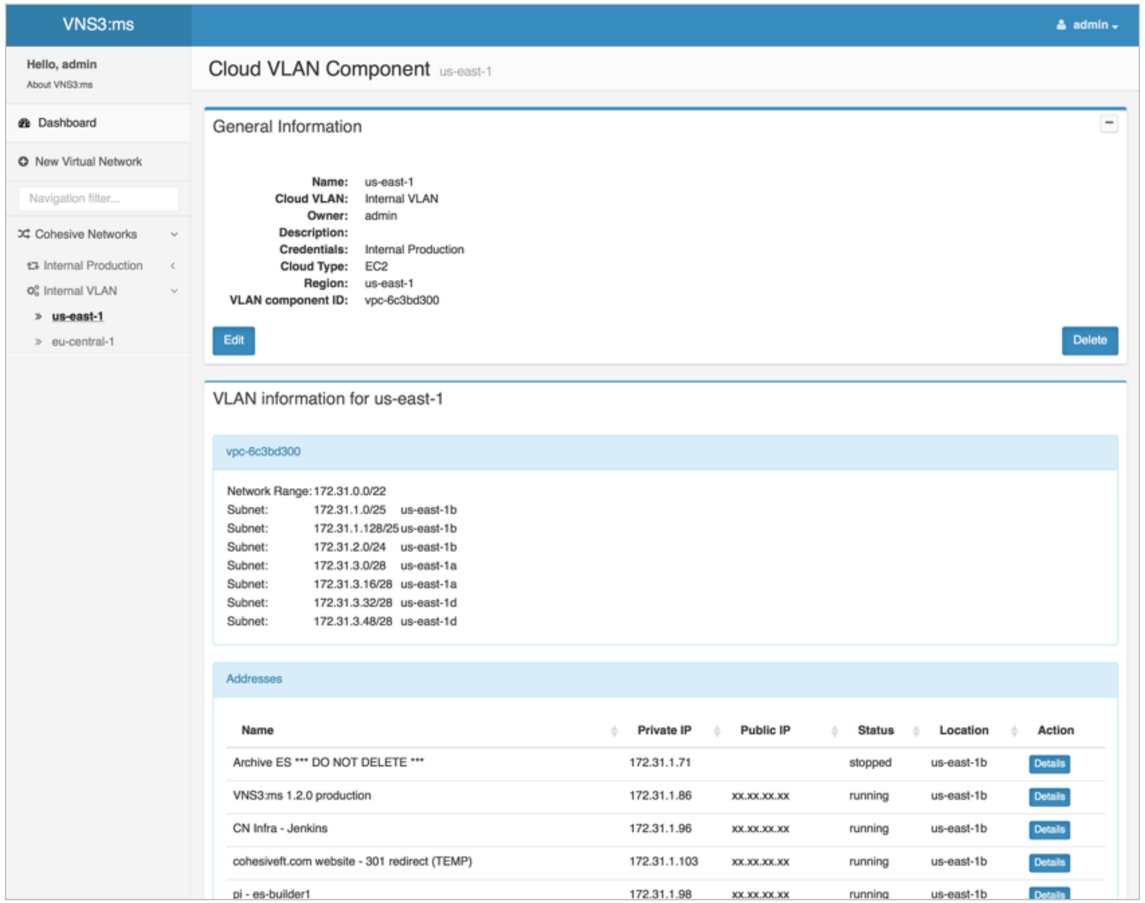
- Provider Owned/Provider Controlled
- Provider Owned/User Controlled
- VNS3 - User Owned/User Controlled
- User Owned/User Controlled



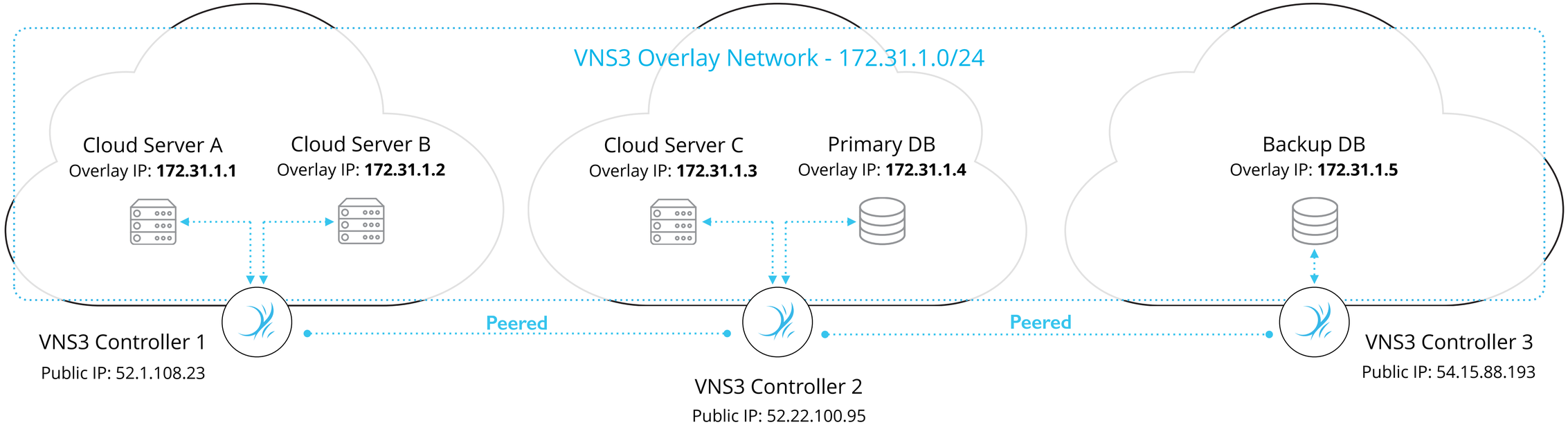
Use VPC

Taking advantage of the additional isolation and network controls of VPC VLAN is a critical piece of the overall security strategy for deploying cloud applications.

It is also recommended to enable DNS resolution and DNS hostnames. This used in combination with Elastic IPs (see page 17) allows shorter DR failover time objectives, increased performance and reduced network transfer costs.



Use the encrypted TLS tunneled Overlay Network



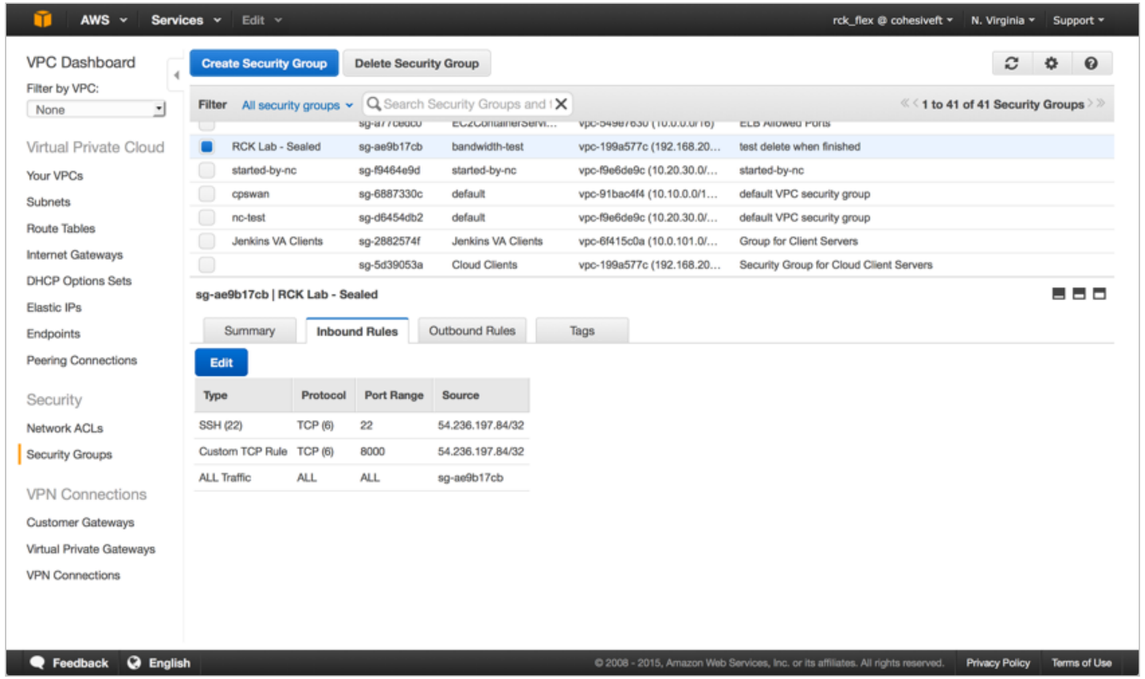
Cloud servers use a unique X.509 credential that is associated with an Overlay IP address plus a tunneling agent (e.g. OpenVPN) to create a secure TLS VPN tunnel to a VNS3 Controller instance. The VNS3 Controller instance acts as a switch, router, firewall, and protocol redistributor. **All data in motion is encrypted end-to-end**.

Lock down the cloud environment

Overlay Network cloud servers communicate to each other and to the remote encrypted domains available via IPsec tunnels through the encrypted switch and router functions of the VNS3 controllers.

The secure connection between a Overlay Network cloud server and VNS3 controller is negotiated via TLS VPN.

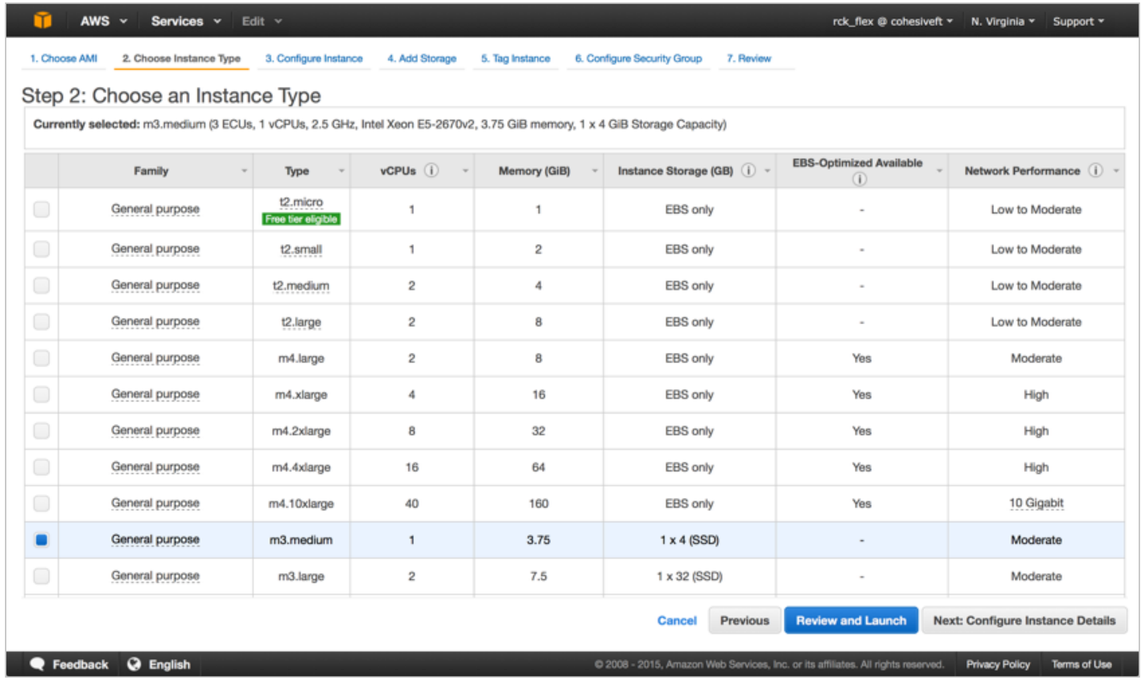
Locking down the intra-cloud communications to only UDP 1194 in/out ensures only the encrypted and tunneled Overlay Network traffic is allowed.



Use an appropriate Instance Size

The instance size required for a use-case is dependent on the total throughput an application deployment needs and how many VNS3 controller instances will be securing that application deployment.

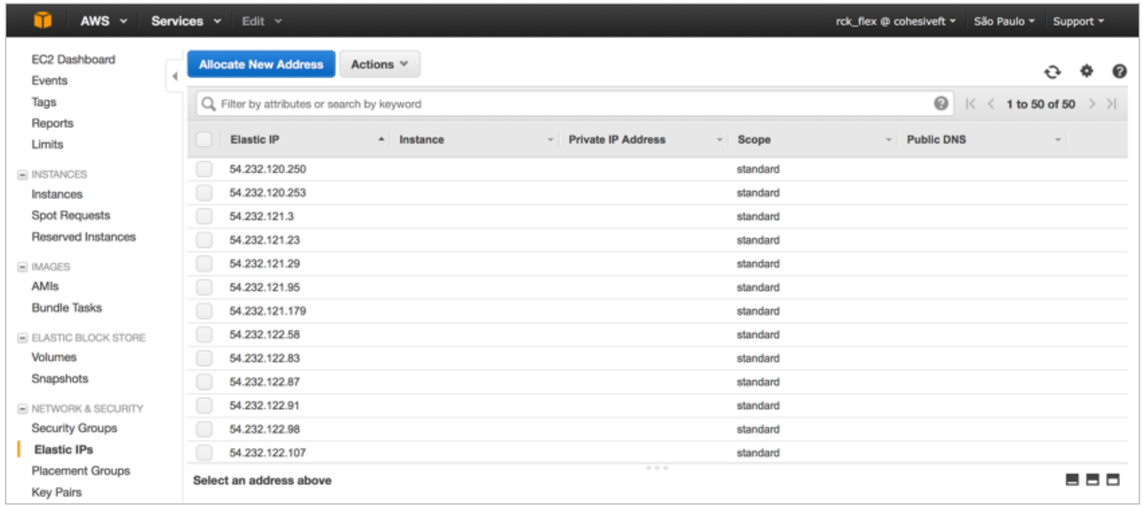
Standard enterprise application network throughput requirements are often accommodated by an instance with 2 virtual CPUs and 4 GB of memory.



Use Static IPs

Using static and assignable public IPs whenever possible allows for fast DR with little to no reconfiguration.

Additionally referencing the DNS hostname in configuration of the Overlay Network connected clients and VNS3 controller peering takes advantage of the AWS private IP resolution when available to keep traffic on the internal AWS network to increase performance and reduce costs.




```
# add remote commands here
remote ec2-52-134-11-19.compute-1.amazonaws.com 1194
remote ec2-50-104-23-221.compute-1.amazonaws.com 1194
remote ec2-54-174-200-57.compute-1.amazonaws.com 1194
remote ec2-54-174-200-103.compute-1.amazonaws.com 1194
```

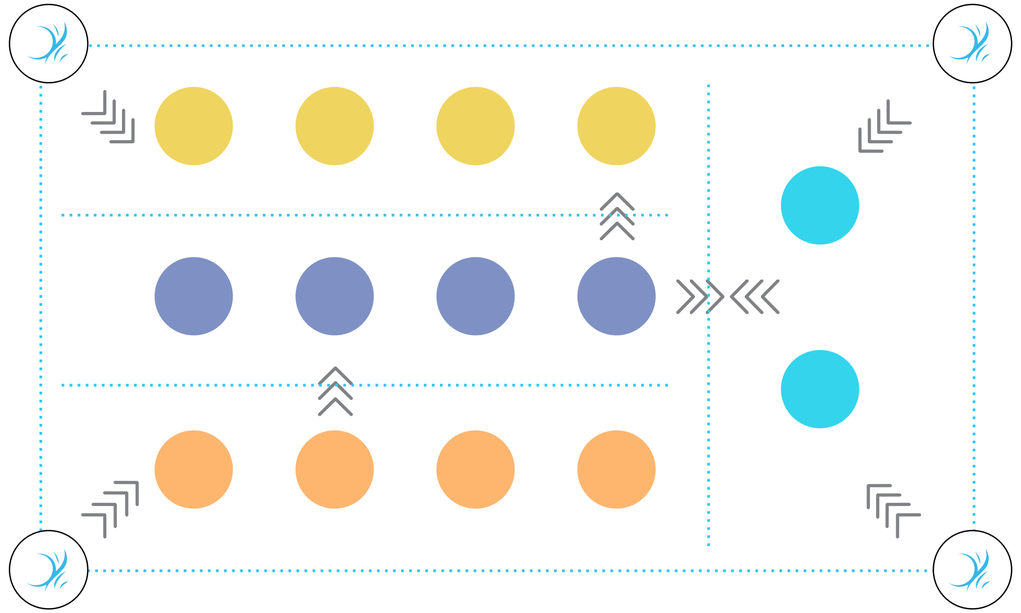
Links to Other Managers

Remote Manager ID	Remote Manager IP	Local Endpoint	Local Process Running?	Direct Link Status	Remote Manager Reachable?
2	ec2-54-174-31-169.compute-1.amazonaws.com	server	running	up	reachable

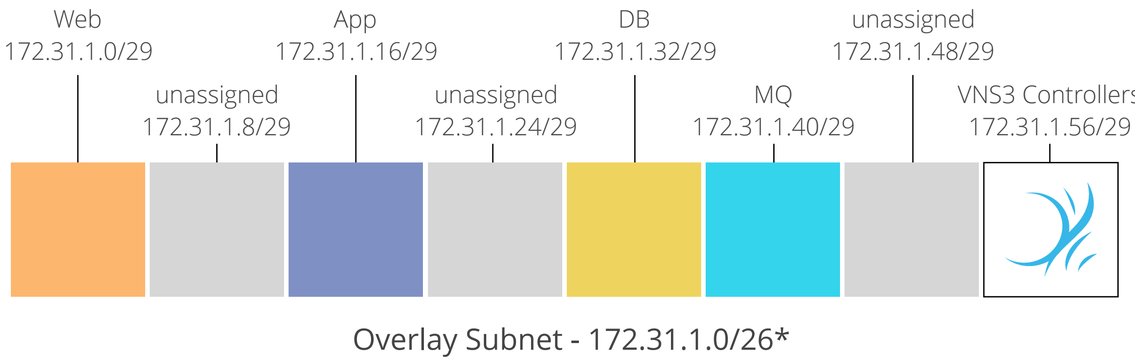
Create Logical Subnets with the VNS3 Firewall

Smaller subnets within the defined Overlay Network CIDR along with VNS3 firewall rules enforce traffic policies to provide segmentation and isolation.

This orthogonal control ensures that the devices are communicating with each other via an encrypted switch and the intra Overlay Network communication is limited to what is necessary.



*This is an example Overlay Network Addressing scheme with a /26 subnet size. Overlay Network subnet sizes can be anything from a /28 to a /16. It's not recommended to configure an Overlay Network with a bit block larger than 16 bits.

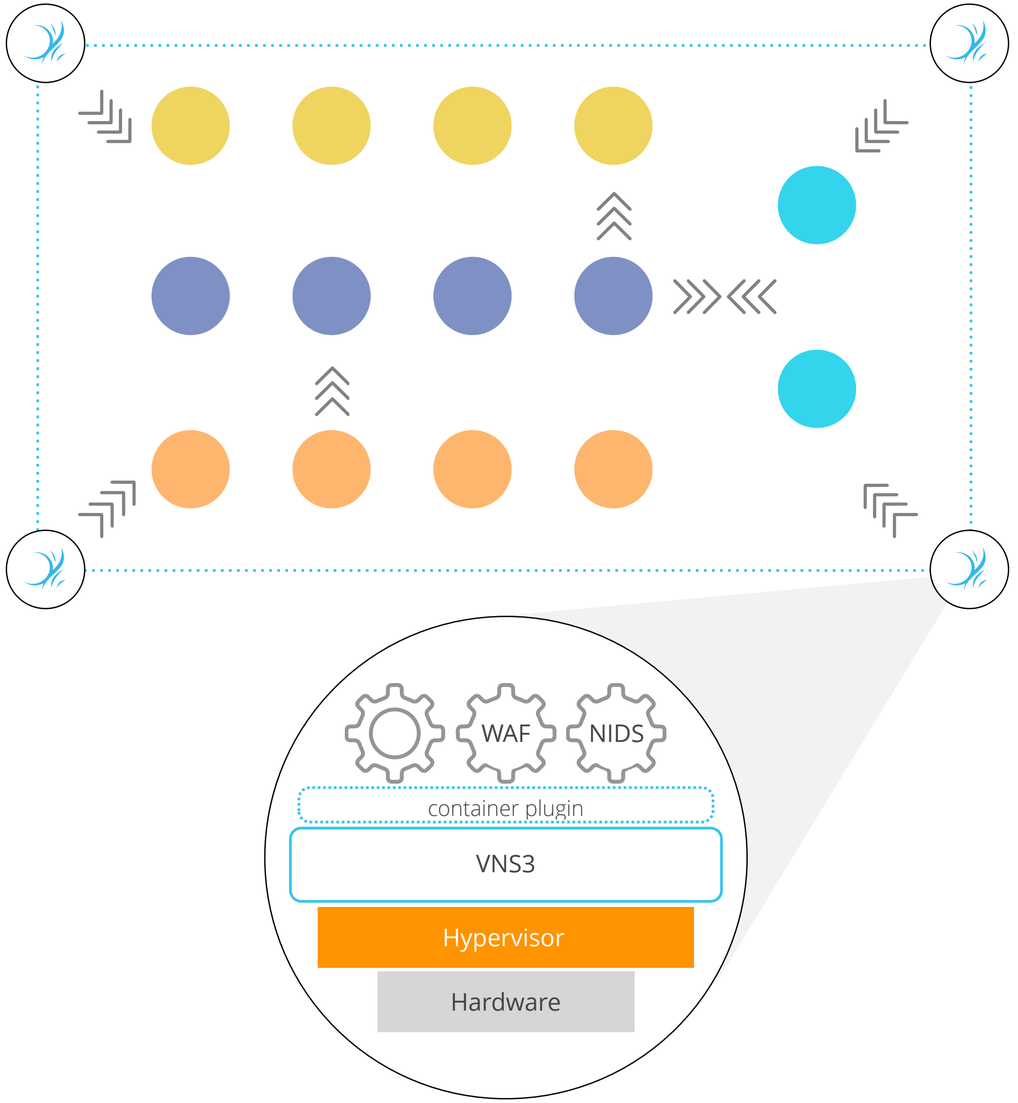


Overlay Subnet - 172.31.1.0/26*

Monitor traffic with VNS3 NIDS/WAF Containers

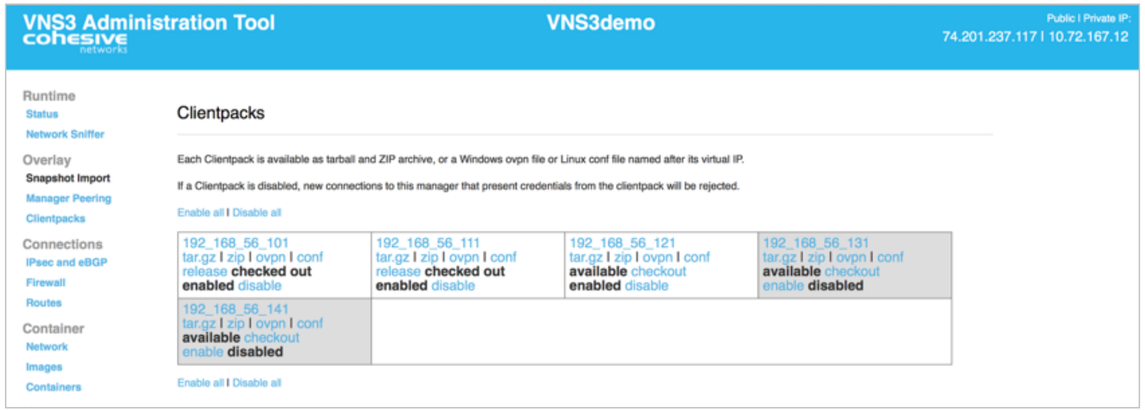
All the traffic coming into, going out of and moving within the VNS3 Overlay Network pass through the VNS3 controllers.

Run traffic management and security services like NIDS and WAF on the VNS3 controllers.



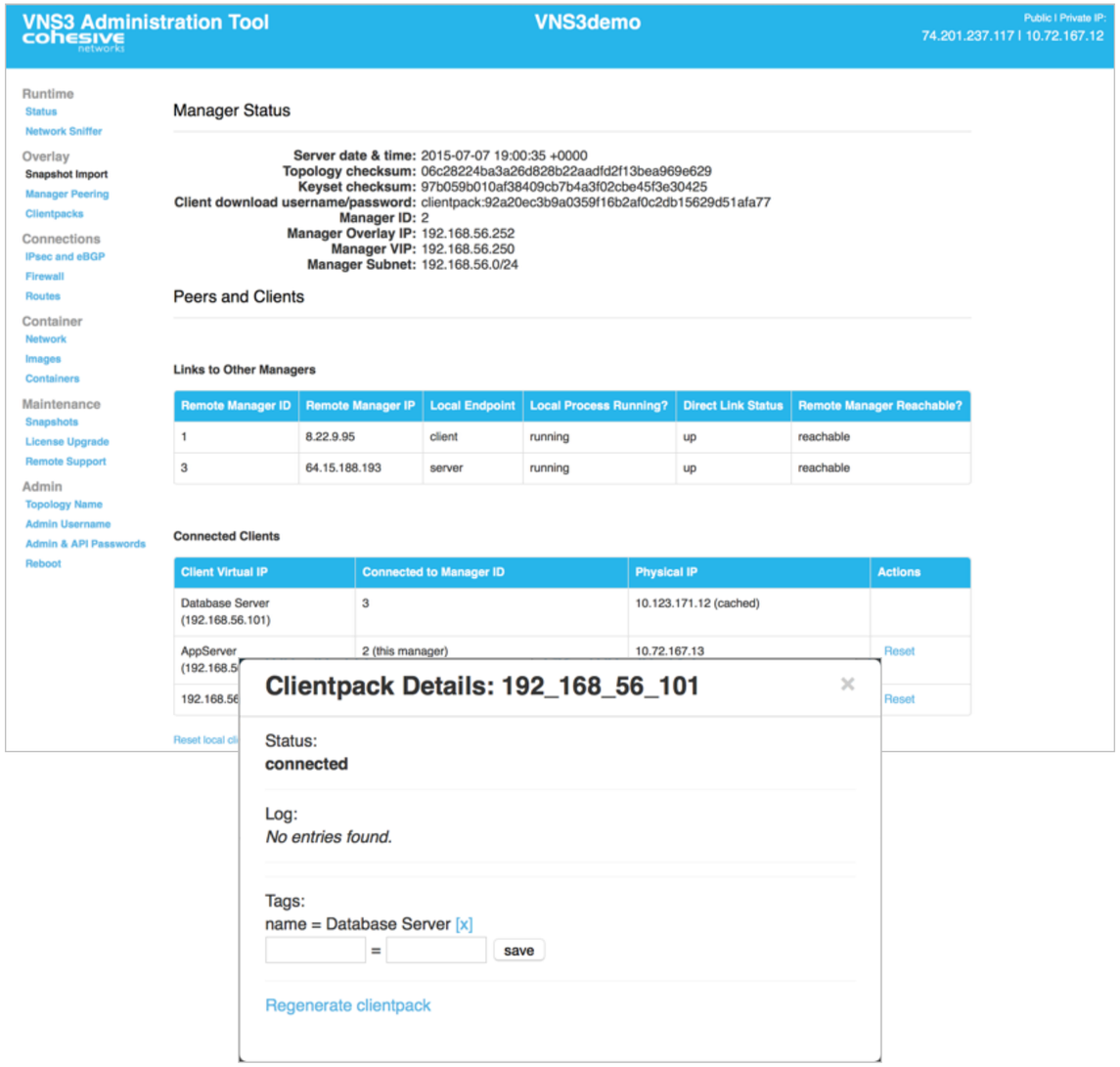
Check out clientpacks

Clientpacks are available to be fetched programmatically via the VNS3 API. Checking out a clientpack makes that credentials unavailable via the API. Mark clientpacks that are currently connected and in use via the check out feature.



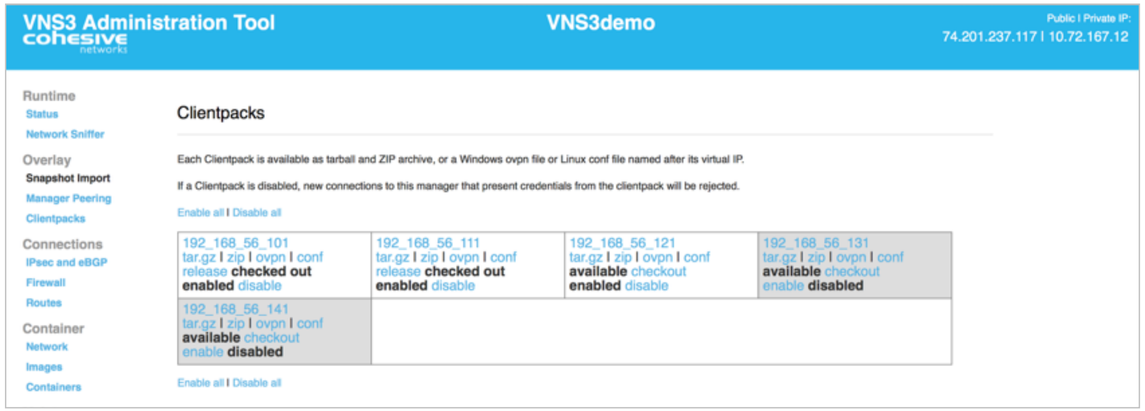
Use clientpack name tag

Tagging each clientpack via the key value tagging system available on VNS3 allows easier tracking and administration of the Overlay connected client servers.



Disable unused clientpacks

Unused clientpacks can be marked as disabled to deny any incoming connections from using that credential.

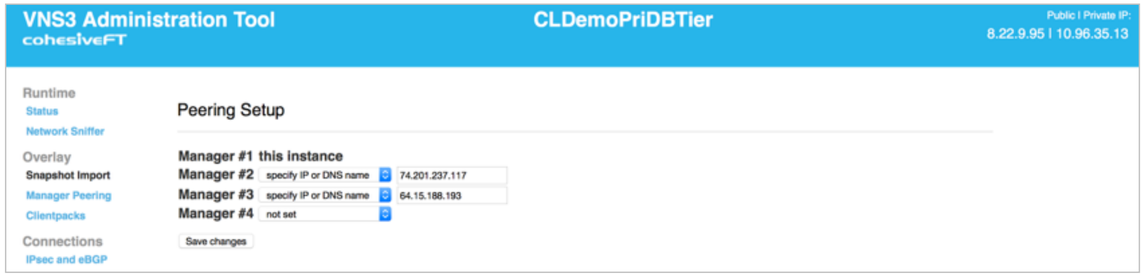


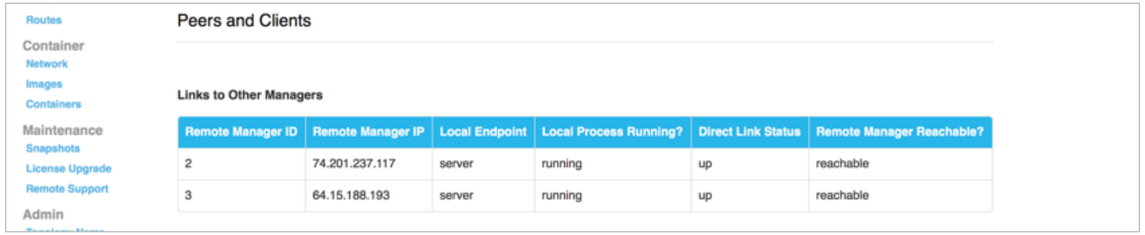
Build a VNS3 Peered mesh network

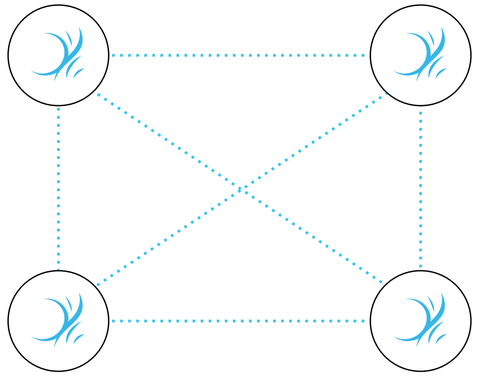
Controllers connect to each other in a process called Peering. Peered Controllers create a redundant, highly available and secure overlay network and share traffic load from the overlay network connected servers.

Connected client servers can specify a list of VNS3 controllers to connect to in order to join the Overlay Network. In the event one controller is in accessible, the connected client server attempts to connect to the next VNS3 controller in the list.

Use Peering if federating any cloud resources across availability zone, data center, region, or cloud provider.







True n-Mesh Peering

IPsec Tunnels

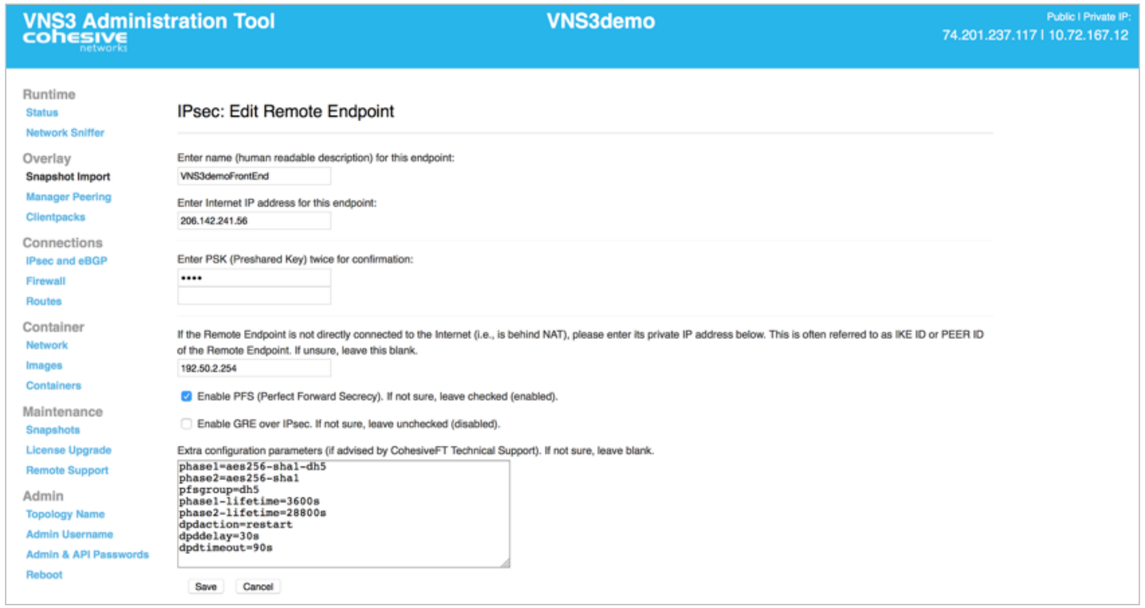
Recommended IPsec tunnels negotiated with VNS3:

- **Policy-based VPN** - encapsulates traffic between two sites as defined by a specific policy or ACL. This is used instead of a Route-based VPN that encapsulates traffic based on routes on both sides which can make it easier to administer but downgrades the security.
- **Encapsulating Security Packet (ESP)** wire level protocol - encrypting and authenticating of the data flowing over the tunnel. This is used instead of Authenication Header (AH) which only authenticates.
- **Tunnel Mode** - encapsulates the entire IP packet for communication over untrusted networks. This is used instead of Transport mode that only encapsulates the IP payload.
- **Internet Key Exchange (IKE)** - protocol used to setup the shared security associations (SA) for the IPsec tunnel. This is used instead of manual key exchange.
- **Main Mode** - used to setup the IPsec tunnel SAs using IKE. This is used instead of Aggressive mode that requires fewer messages to establish the SA but does so in a less secured manner.
- **Preshared Key (PSK)** - used for authentication between two connecting parties. This is used instead of certificates.

Match all tunnel parameters

IPsec devices often have parameter groups and list from which IPsec tunnel definition information is sourced. Often the in-force IPsec parameter information is different from the intended definition.

Specifying the exact parameters required for IPsec negotiation ensures the correct encryption details are used.



Recommended IPsec Parameters

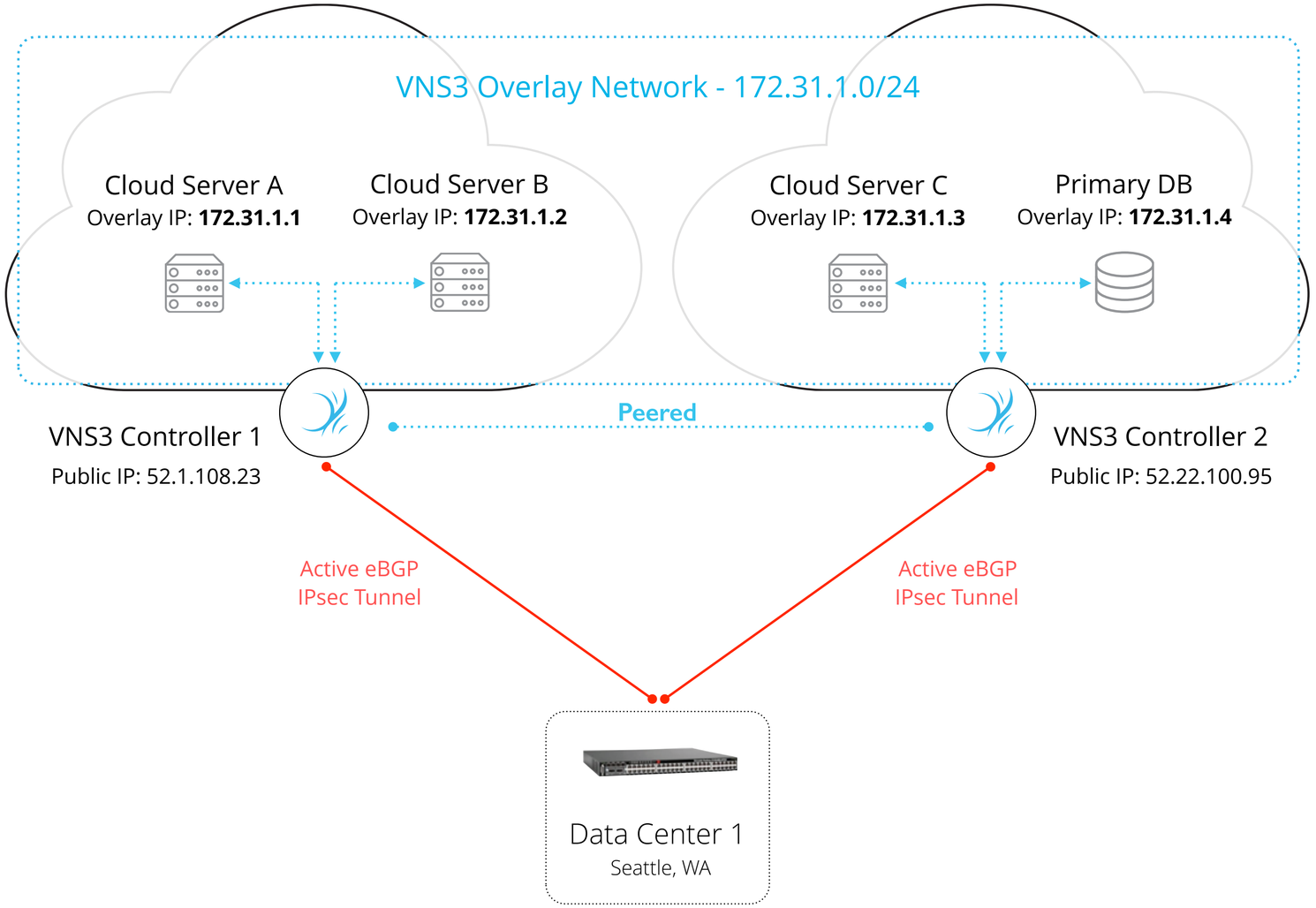
Based on experience connecting thousands of partner and customer devices we recommend the following IPsec tunnel settings:

- AES256 algorithms
- SHA1 (or SHA2 256) authentication hashing
- DH5 or DH14
- Perfect Forward Secrecy
- DPD
- Phase1 Lifetime of 3600s/1h
- Phase2 Lifetime of 28800s/8h

IPsec Failover - BGP

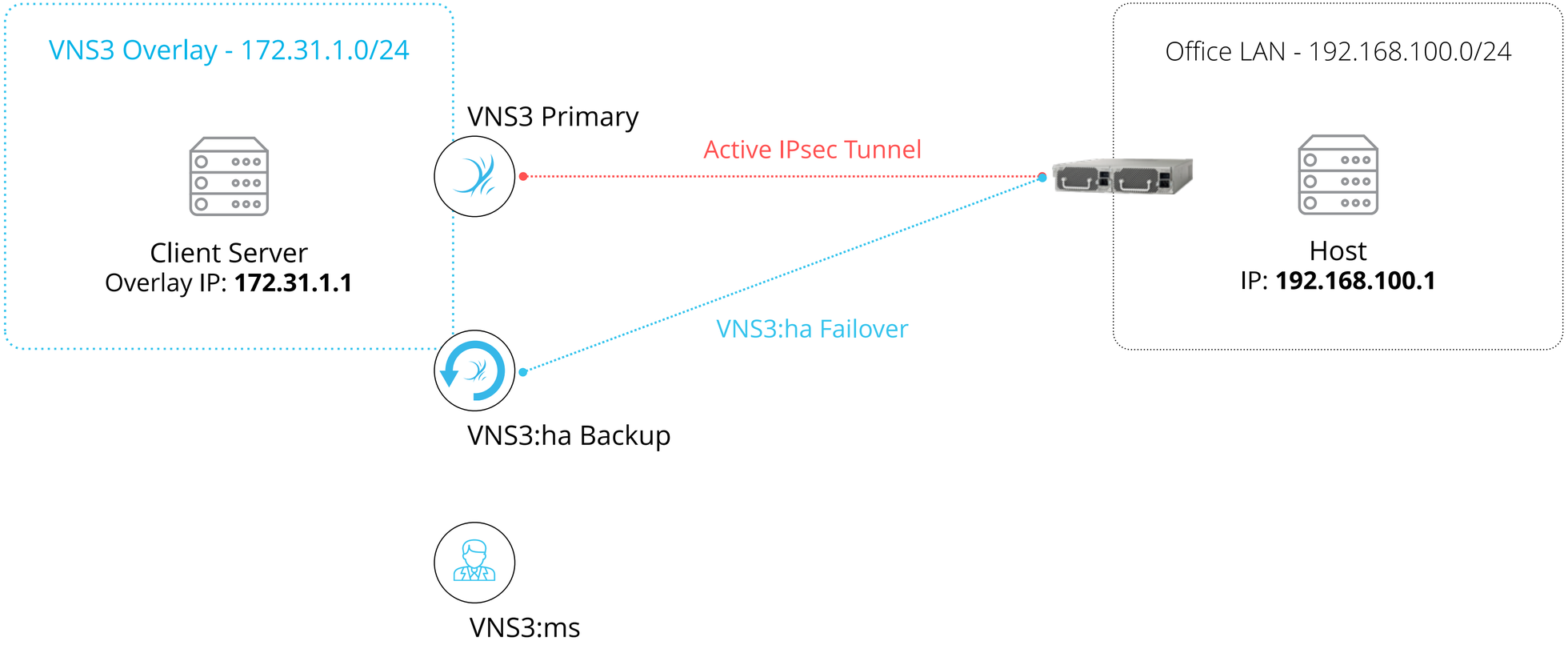
IPsec HA can be achieved using VNS3 Peered mesh and IPsec BGP tunnels that decide the quickest path.

This is completely dependent on the connecting party's hardware and expertise.



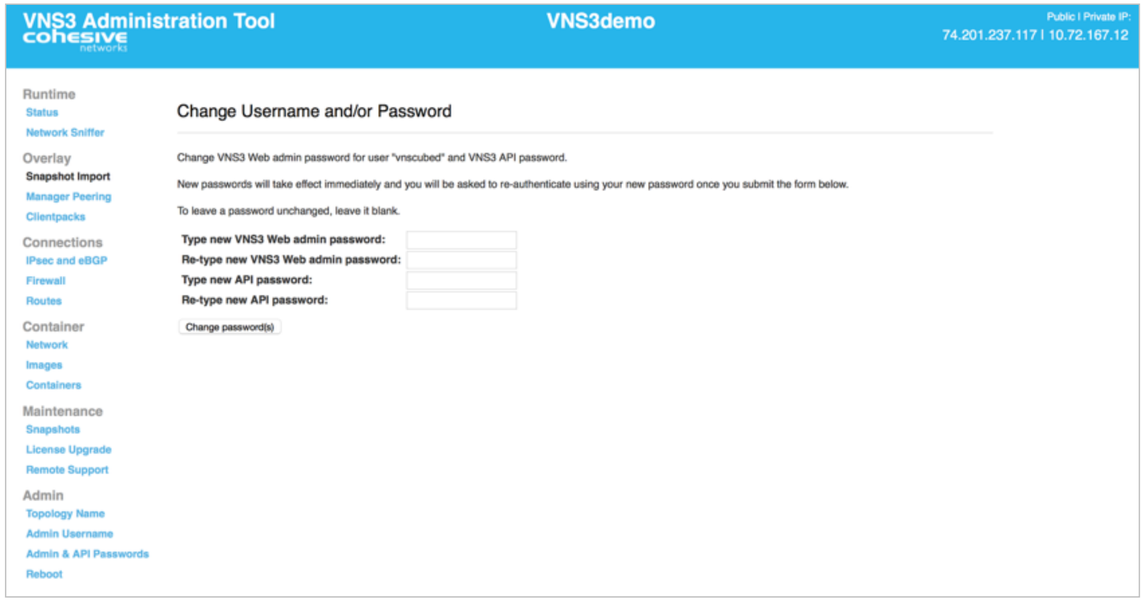
IPsec Failover - Normal IPsec

VNS3 provides an add-on for instance-based automatic IPsec VPN failover solution to reduce RTO in the event of cloud connectivity failure.



Separate UI and API Credentials

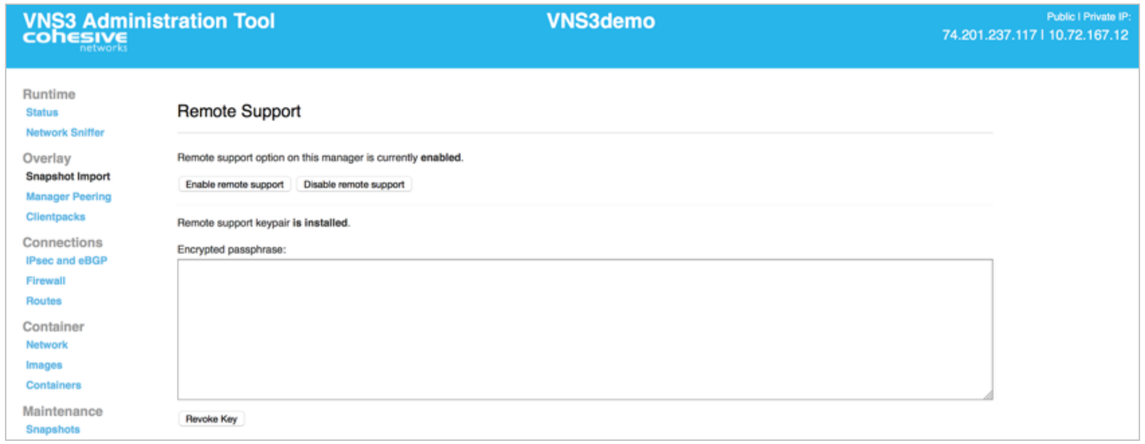
Many regulated industries have to follow best practices like changing default username and passwords. Having different access credentials for people and programs and a logical extension.



Use multi-factor / multi-party authentication

We send an encrypted passphrase to generate a private key used by Cohesive Support staff to access the VNS3 Controller.

Access to the restricted SSH daemon is completely controlled by the user. Once the support ticket has been closed the user can disable remote support access and invalidate the access key.



VNS3 snapshots for DR

VNS3 Snapshots include all the running configuration details.

Use VNS3 snapshots to move configuration state from one VNS3 controller instance to another.

Use VNS3:ms for management and monitoring

A single dashboard to manage and monitor VNS3 networks plus all underlying cloud VLAN network components (CIDR, subnets, route tables, ACLs, security groups, etc.)