



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.



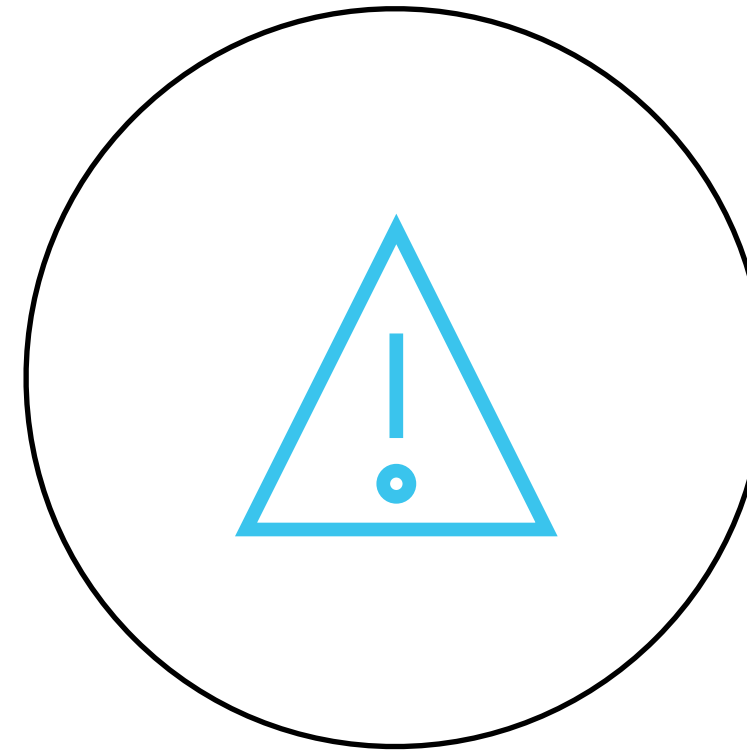
2000+ customers in 20+ countries across all industry verticals and sectors



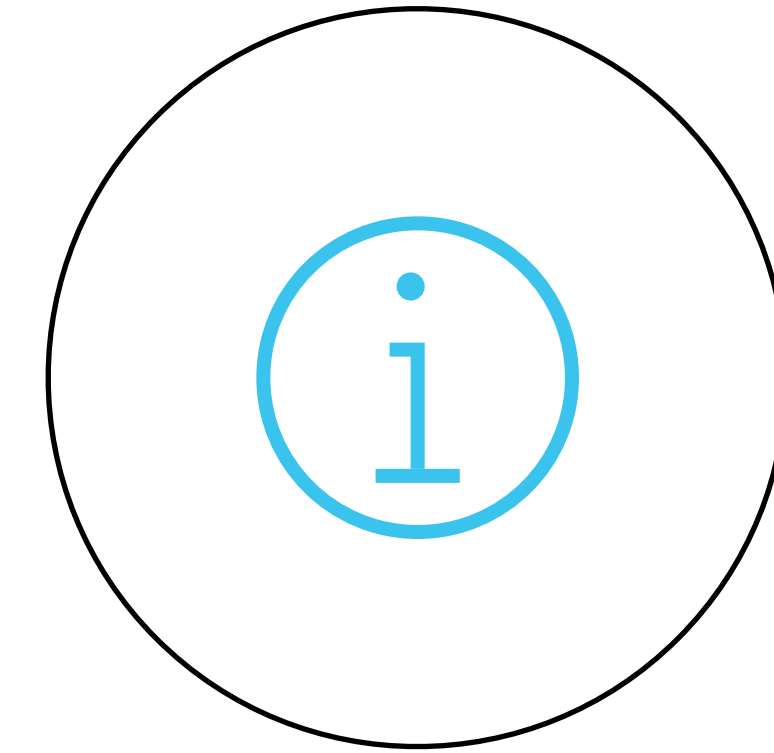
New realities of cybersecurity



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



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

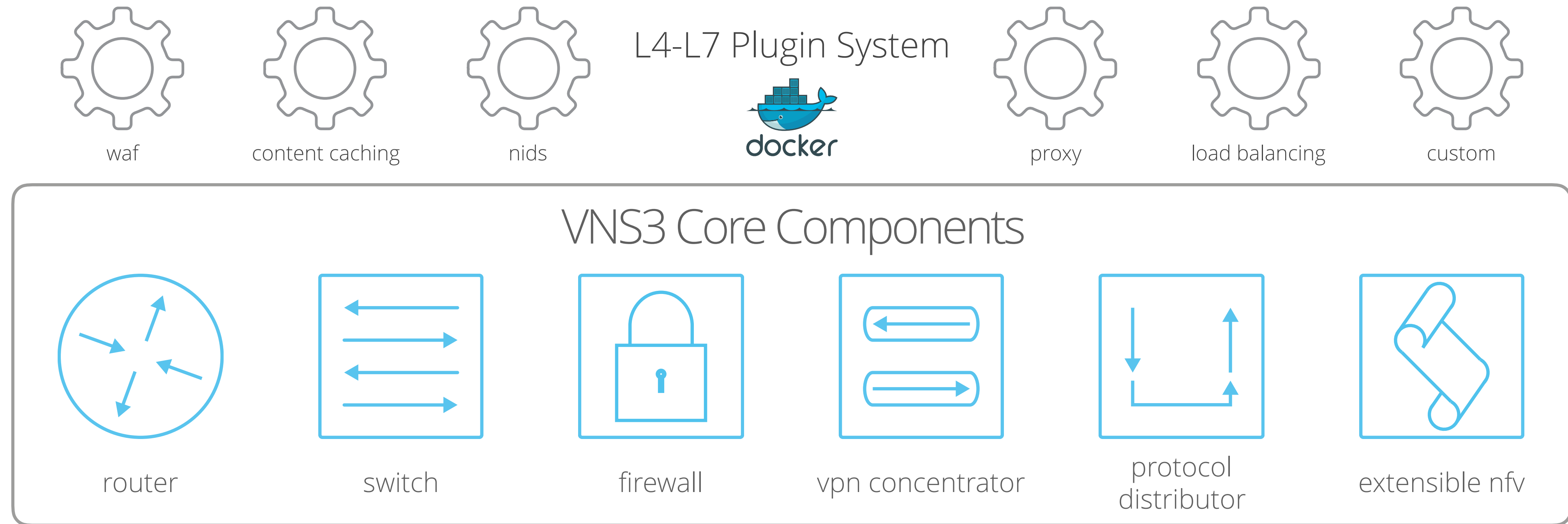


Regulatory implementation and reporting demands are increasing.

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

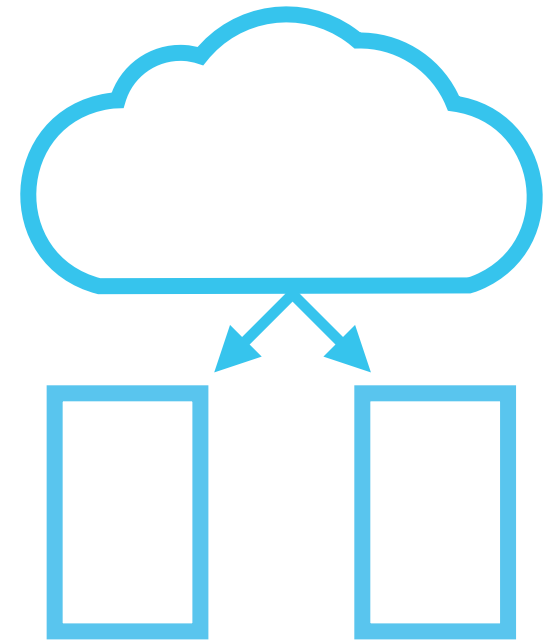


VNS3 provides connectivity and security + L4-L7 plug-in system

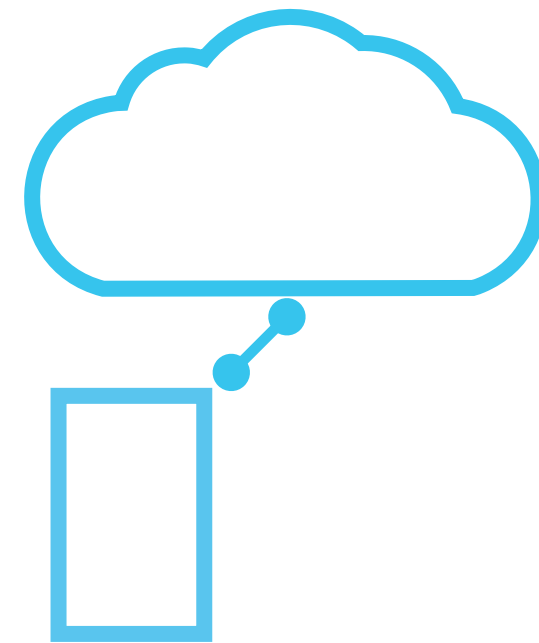


VNS3 is a **software-only virtual appliance** you deploy in your cloud/virtual infra to bring all the the connectivity and security controls normally available at the data center edge to your application edge. With the option Overlay Network, you can also **encrypt all data-in-transit** to, from and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

VNS3 enables production cloud use-cases



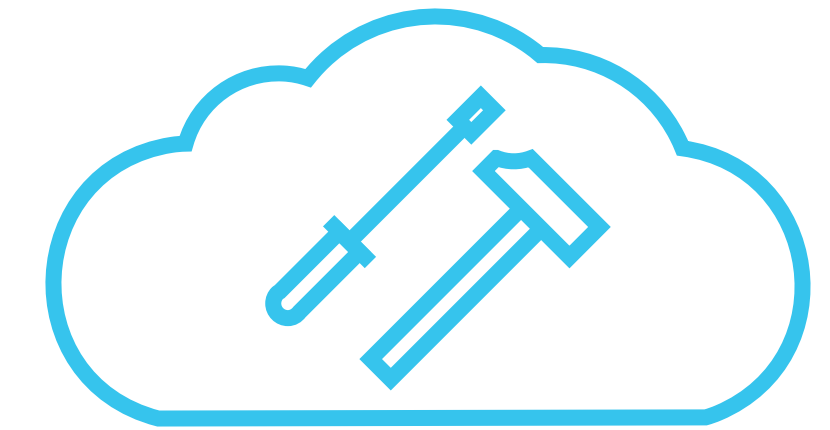
Partner/Customer Networks



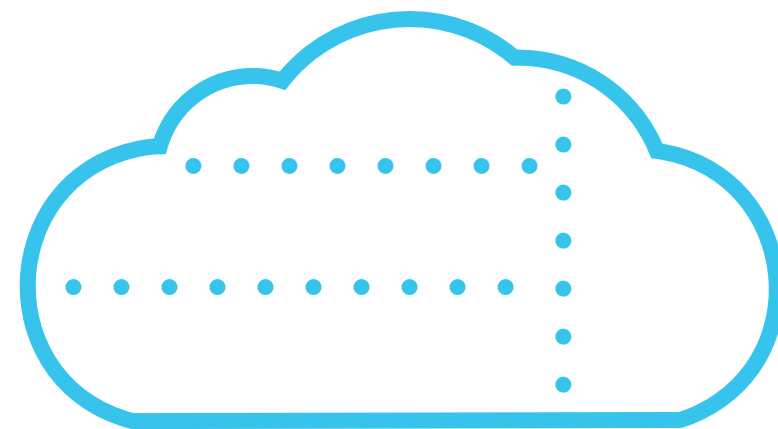
Cloud VPN



Security & Compliance



Rapid Dev/Test



App Segmentation

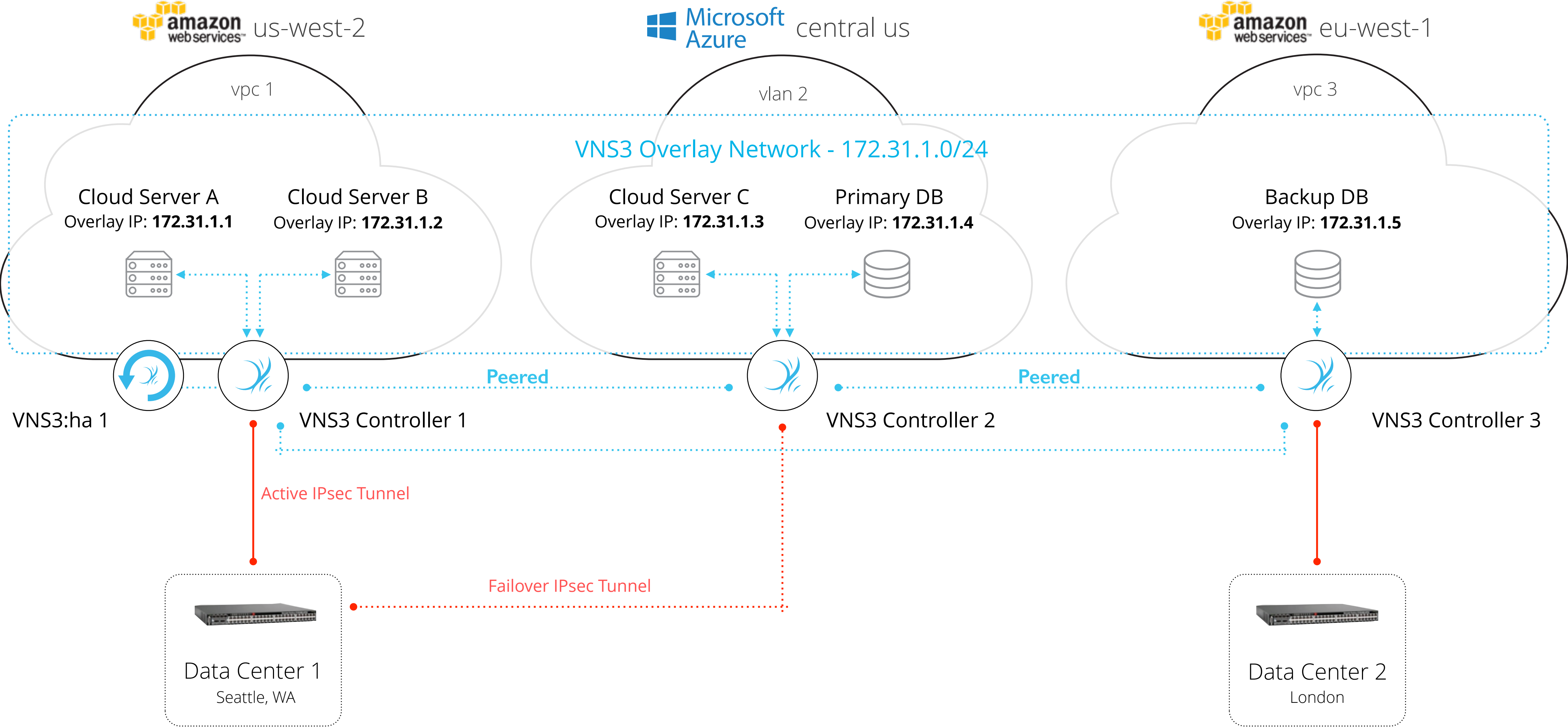


Private Cloud



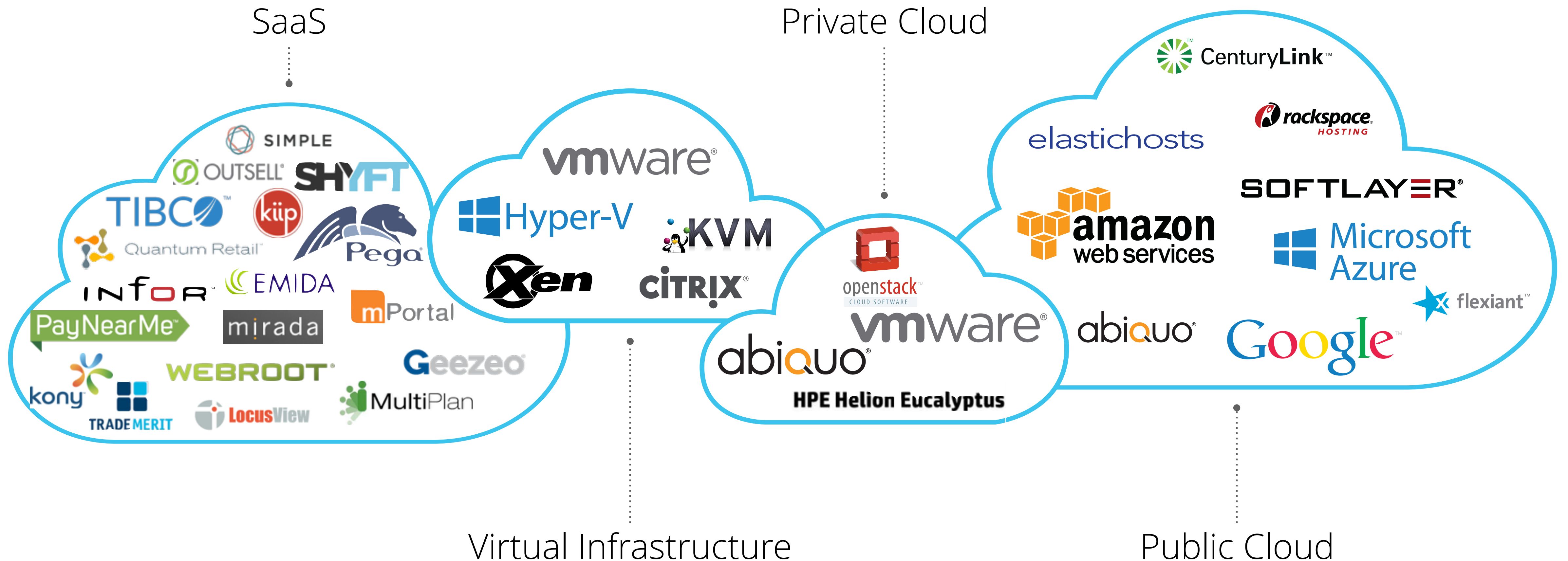
Cloud DR

VNS3 allows topology control

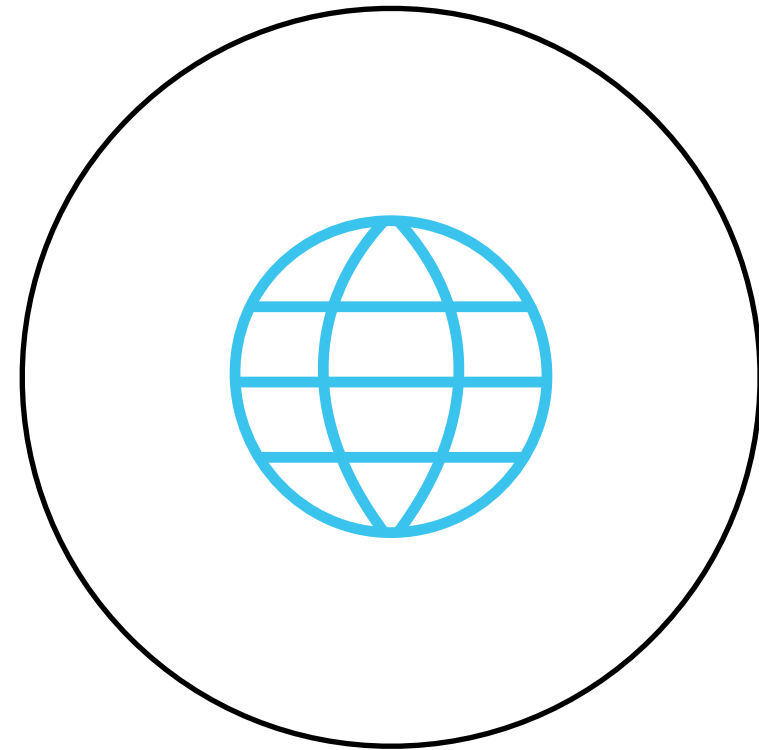


VNS3 is available everywhere

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

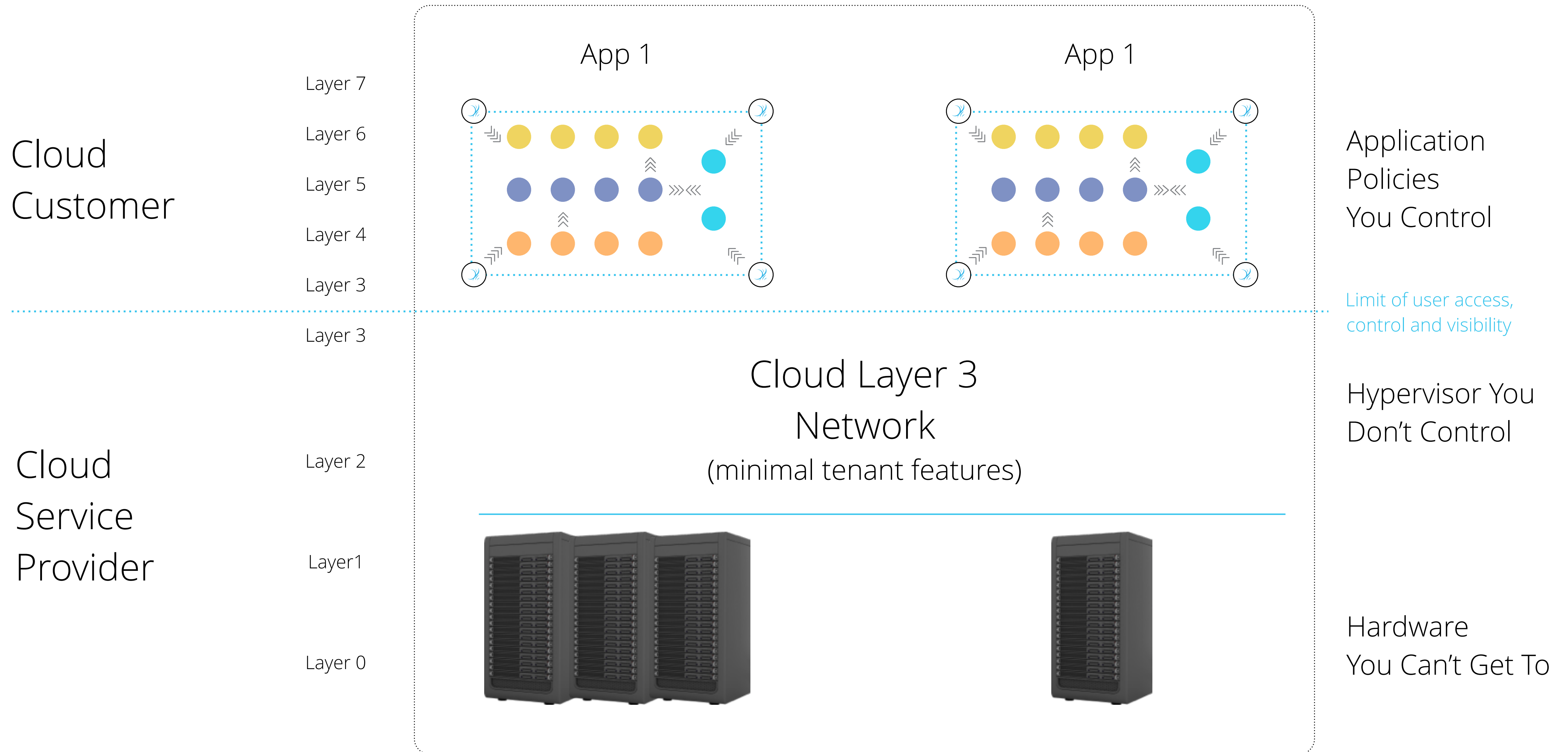
IPsec Site-to-Site

- 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

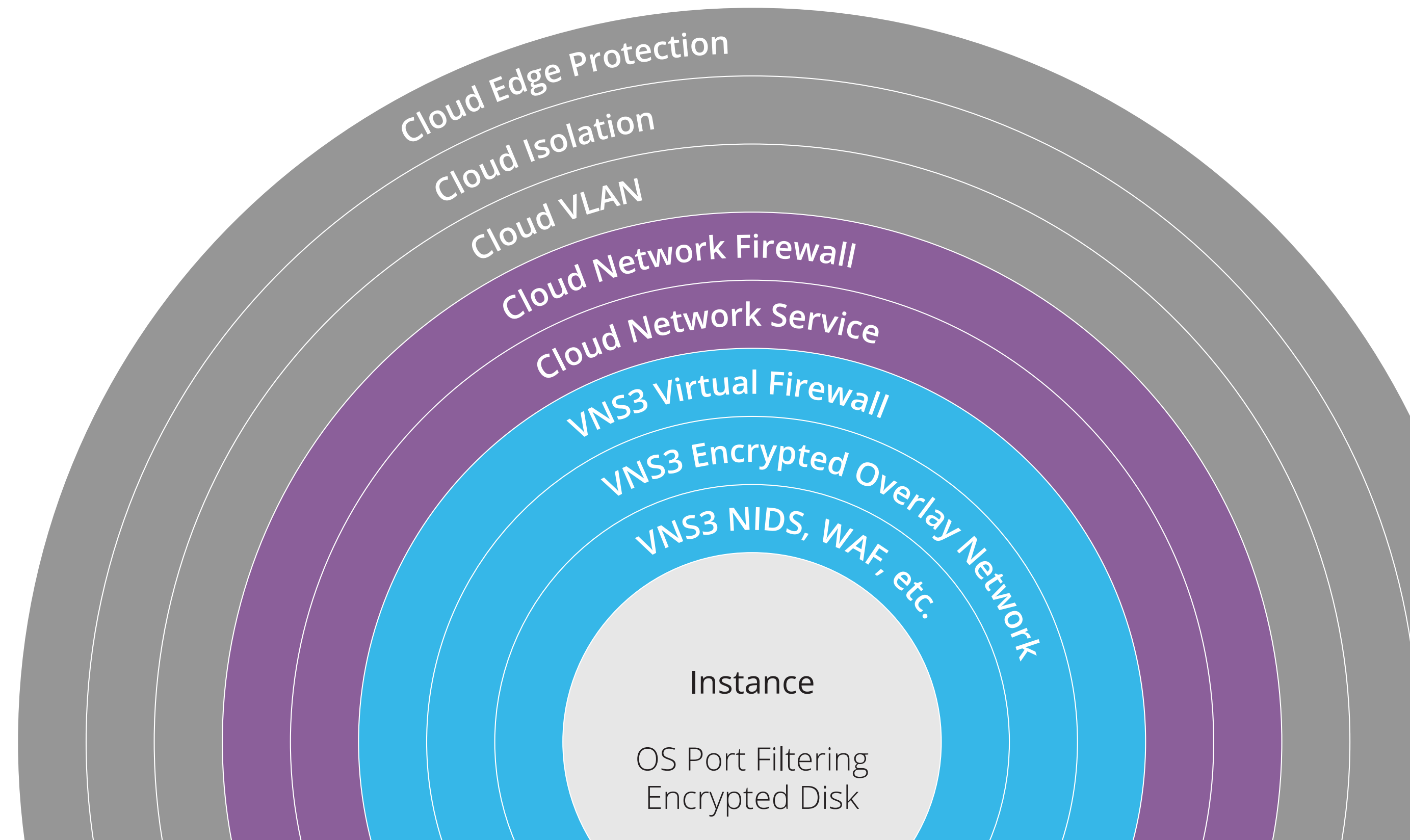


Build layers of control and access

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

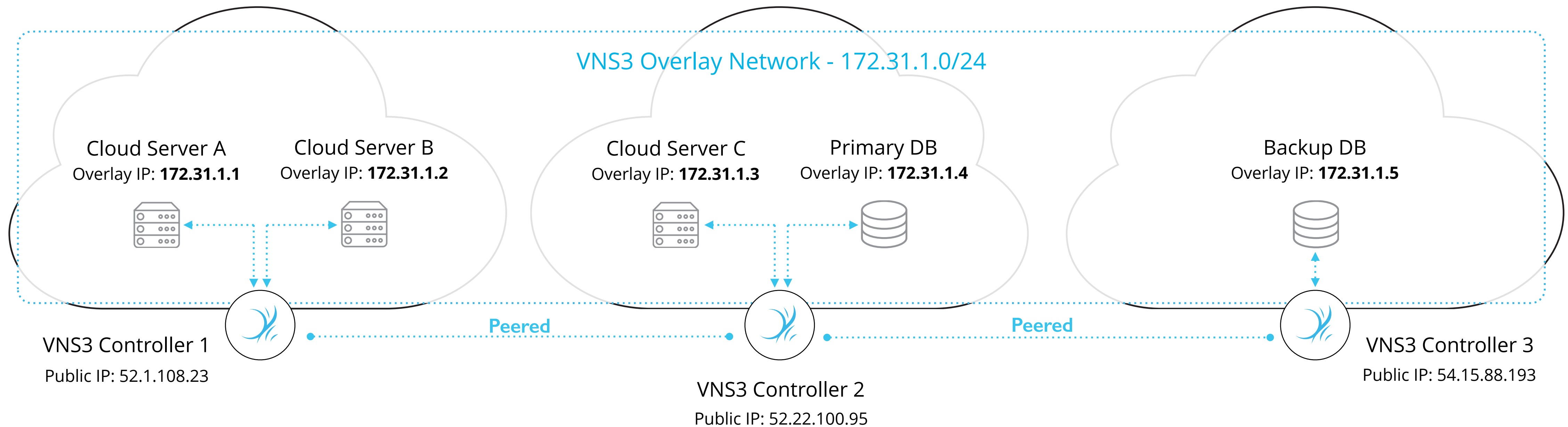
Taking advantage of the additional isolation and network controls of VPC VLAN is a critical piece of the overall security strategy for deploying cloud applications.

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.

The screenshot displays the VNS3.ms web interface. The top navigation bar shows 'VNS3.ms' and the user 'admin'. The left sidebar contains a navigation menu with options like 'Dashboard', 'New Virtual Network', and a tree view for 'Cohesive Networks' including 'Internal Production', 'Internal VLAN', and sub-regions 'us-east-1' and 'eu-central-1'. The main content area is titled 'Cloud VLAN Component us-east-1'. It features a 'General Information' section with the following details: Name: us-east-1, Cloud VLAN: Internal VLAN, Owner: admin, Description: Internal Production, Credentials: EC2, Cloud Type: EC2, Region: us-east-1, and VLAN component ID: vpc-6c3bd300. Below this is a 'VLAN information for us-east-1' section showing a table of subnets for the vpc-6c3bd300 component. At the bottom, there is an 'Addresses' table listing various IP addresses and their statuses.

Name	Private IP	Public IP	Status	Location	Action
Archive ES *** DO NOT DELETE ***	172.31.1.71		stopped	us-east-1b	Details
VNS3.ms 1.2.0 production	172.31.1.86	xx.xx.xx.xx	running	us-east-1b	Details
CN Infra - Jenkins	172.31.1.96	xx.xx.xx.xx	running	us-east-1b	Details
cohesiveft.com website - 301 redirect (TEMP)	172.31.1.103	xx.xx.xx.xx	running	us-east-1b	Details
pi - es-builder1	172.31.1.98	xx.xx.xx.xx	running	us-east-1b	Details

Use the encrypted TLS tunneled Overlay Network



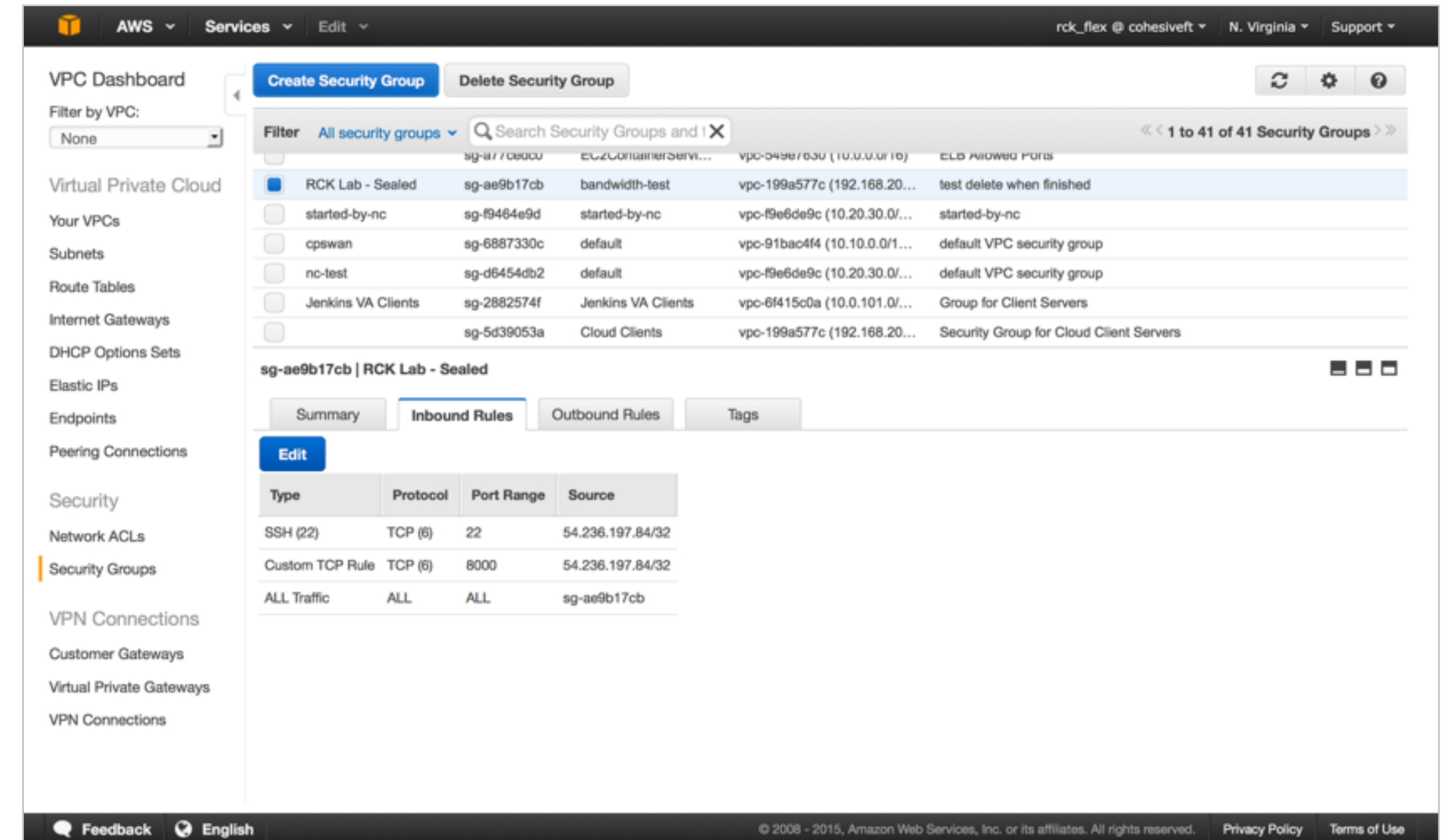
Cloud servers use a unique X.509 credential that is associated with an Overlay IP address plus a tunneling agent (e.g. OpenVPN) to create a secure TLS VPN tunnel to a VNS3 Controller instance. The VNS3 Controller instance acts as a switch, router, firewall, and protocol redistributor. **All data in motion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



The screenshot shows the AWS Management Console interface for Security Groups. The left sidebar contains navigation options like VPC Dashboard, Virtual Private Cloud, Your VPCs, Subnets, Route Tables, Internet Gateways, DHCP Options Sets, Elastic IPs, Endpoints, Peering Connections, Security, Network ACLs, Security Groups, VPN Connections, Customer Gateways, Virtual Private Gateways, and VPN Connections. The main content area shows a list of security groups, with 'RCK Lab - Sealed' (sg-ae9b17cb) selected. Below the list, the 'Inbound Rules' tab is active, displaying a table of rules:

Type	Protocol	Port Range	Source
SSH (22)	TCP (6)	22	54.236.197.84/32
Custom TCP Rule	TCP (6)	8000	54.236.197.84/32
ALL Traffic	ALL	ALL	sg-ae9b17cb

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.

Step 2: Choose an Instance Type

Currently selected: m3.medium (3 ECUs, 1 vCPUs, 2.5 GHz, Intel Xeon E5-2670v2, 3.75 GiB memory, 1 x 4 GiB Storage Capacity)

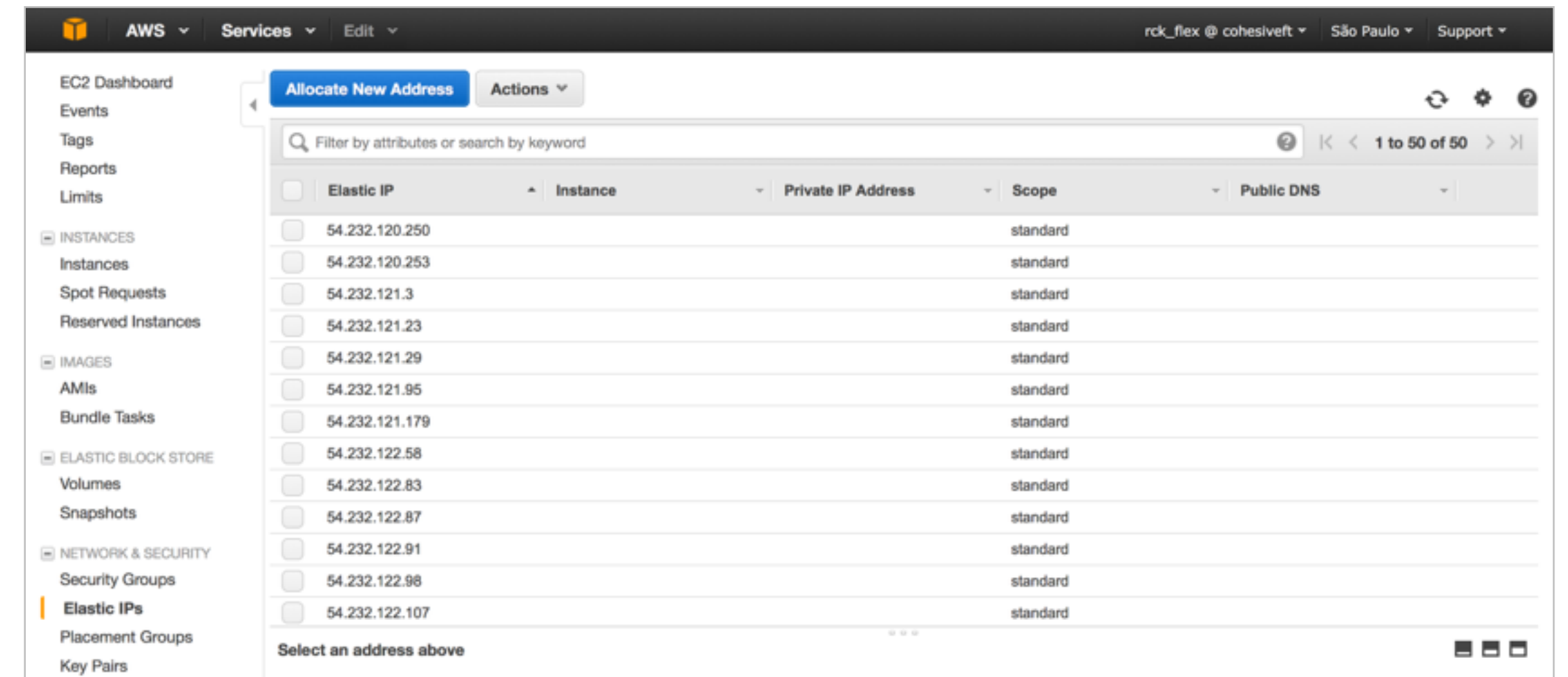
	Family	Type	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance
<input type="checkbox"/>	General purpose	t2.micro Free tier eligible	1	1	EBS only	-	Low to Moderate
<input type="checkbox"/>	General purpose	t2.small	1	2	EBS only	-	Low to Moderate
<input type="checkbox"/>	General purpose	t2.medium	2	4	EBS only	-	Low to Moderate
<input type="checkbox"/>	General purpose	t2.large	2	8	EBS only	-	Low to Moderate
<input type="checkbox"/>	General purpose	m4.large	2	8	EBS only	Yes	Moderate
<input type="checkbox"/>	General purpose	m4.xlarge	4	16	EBS only	Yes	High
<input type="checkbox"/>	General purpose	m4.2xlarge	8	32	EBS only	Yes	High
<input type="checkbox"/>	General purpose	m4.4xlarge	16	64	EBS only	Yes	High
<input type="checkbox"/>	General purpose	m4.10xlarge	40	160	EBS only	Yes	10 Gigabit
<input checked="" type="checkbox"/>	General purpose	m3.medium	1	3.75	1 x 4 (SSD)	-	Moderate
<input type="checkbox"/>	General purpose	m3.large	2	7.5	1 x 32 (SSD)	-	Moderate

Cancel Previous **Review and Launch** Next: Configure Instance Details

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
```

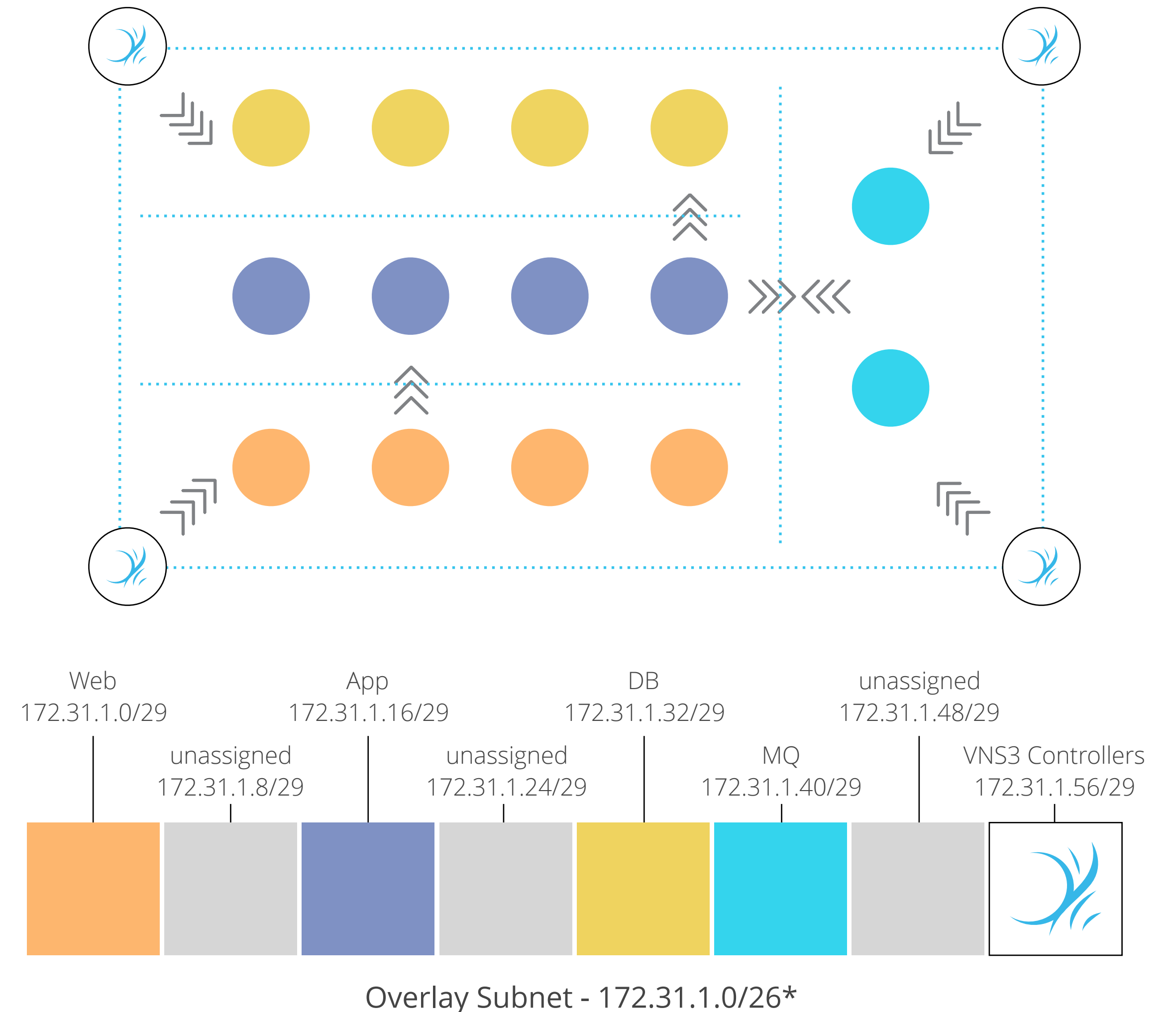
Links to Other Managers					
Remote Manager ID	Remote Manager IP	Local Endpoint	Local Process Running?	Direct Link Status	Remote Manager Reachable?
2	ec2-54-174-31-169.compute-1.amazonaws.com	server	running	up	reachable

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.

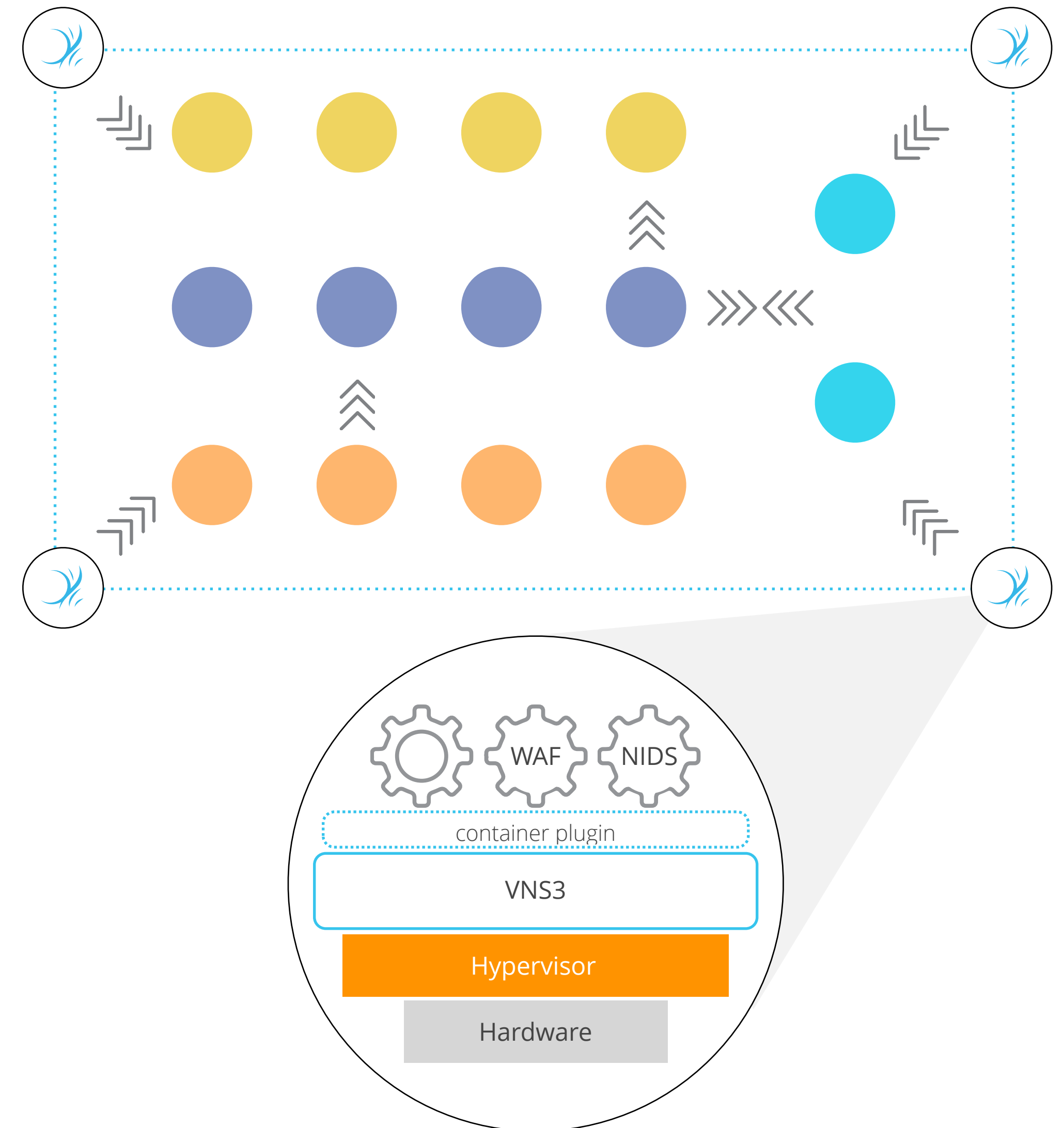
*This is an example Overlay Network Addressing scheme with a /26 subnet size. Overlay Network subnet sizes can be anything from a /28 to a /16. It's not recommended to configure an Overlay Network with a bit block larger than 16 bits.



Monitor traffic with VNS3 NIDS/WAF Containers

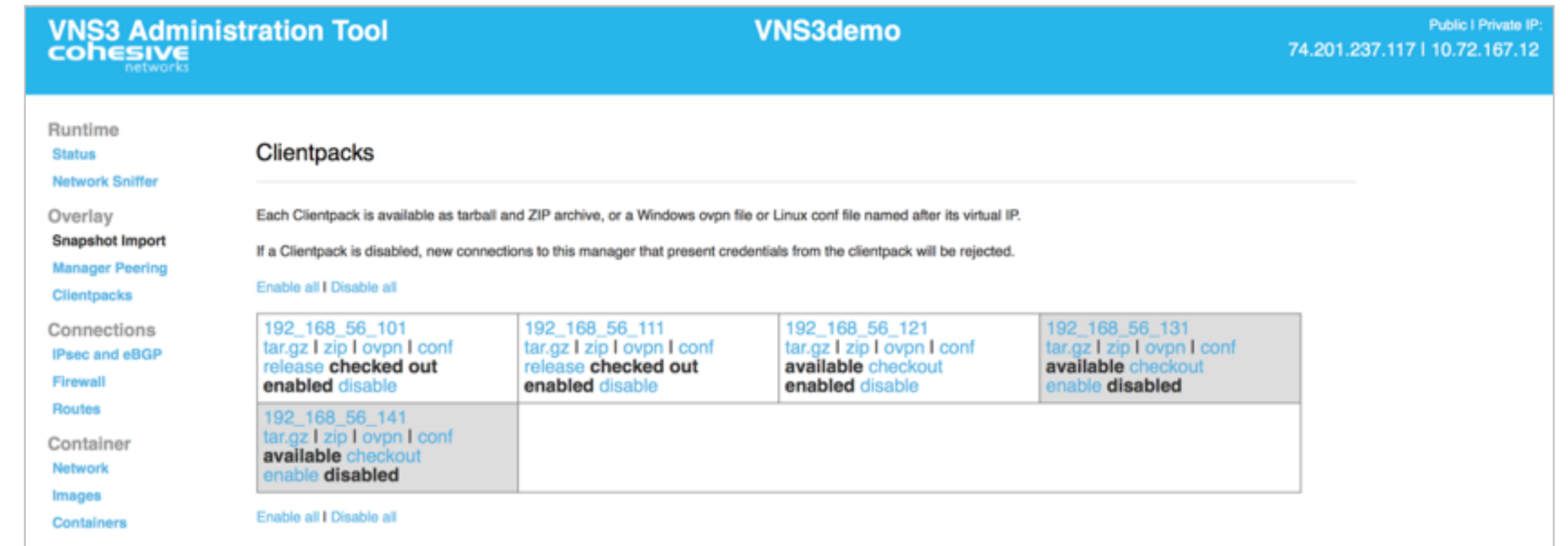
All the traffic coming into, going out of and moving within the VNS3 Overlay Network pass through the VNS3 controllers.

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.



The screenshot shows the VNS3 Administration Tool interface for the 'VNS3demo' instance. The page title is 'Clientpacks'. Below the title, there is a note: 'Each Clientpack is available as tarball and ZIP archive, or a Windows ovpn file or Linux conf file named after its virtual IP. If a Clientpack is disabled, new connections to this manager that present credentials from the clientpack will be rejected.' There are links for 'Enable all' and 'Disable all'. A table lists four clientpacks with their respective file formats and status.

Clientpack ID	File Formats	Status
192_168_56_101	tar.gz zip ovpn conf	release checked out enabled disable
192_168_56_111	tar.gz zip ovpn conf	release checked out enabled disable
192_168_56_121	tar.gz zip ovpn conf	available checkout enabled disable
192_168_56_131	tar.gz zip ovpn conf	available checkout enable disabled

Below the table, there is a link for 'Enable all' and 'Disable all'.

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.

VNS3 Administration Tool VNS3demo Public | Private IP: 74.201.237.117 | 10.72.167.12

Manager Status

Server date & time: 2015-07-07 19:00:35 +0000
Topology checksum: 06c28224ba3a26d828b22aadfd2f13bea969e629
Keyset checksum: 97b059b010af38409cb7b4a3f02cbe45f3e30425
Client download username/password: clientpack:92a20ec3b9a0359f16b2af0c2db15629d51afa77
Manager ID: 2
Manager Overlay IP: 192.168.56.252
Manager VIP: 192.168.56.250
Manager Subnet: 192.168.56.0/24

Peers and Clients

Links to Other Managers

Remote Manager ID	Remote Manager IP	Local Endpoint	Local Process Running?	Direct Link Status	Remote Manager Reachable?
1	8.22.9.95	client	running	up	reachable
3	64.15.188.193	server	running	up	reachable

Connected Clients

Client Virtual IP	Connected to Manager ID	Physical IP	Actions
Database Server (192.168.56.101)	3	10.123.171.12 (cached)	
AppServer (192.168.56.102)	2 (this manager)	10.72.167.13	Reset
192.168.56.103			Reset

Clientpack Details: 192_168_56_101

Status: **connected**

Log: No entries found.

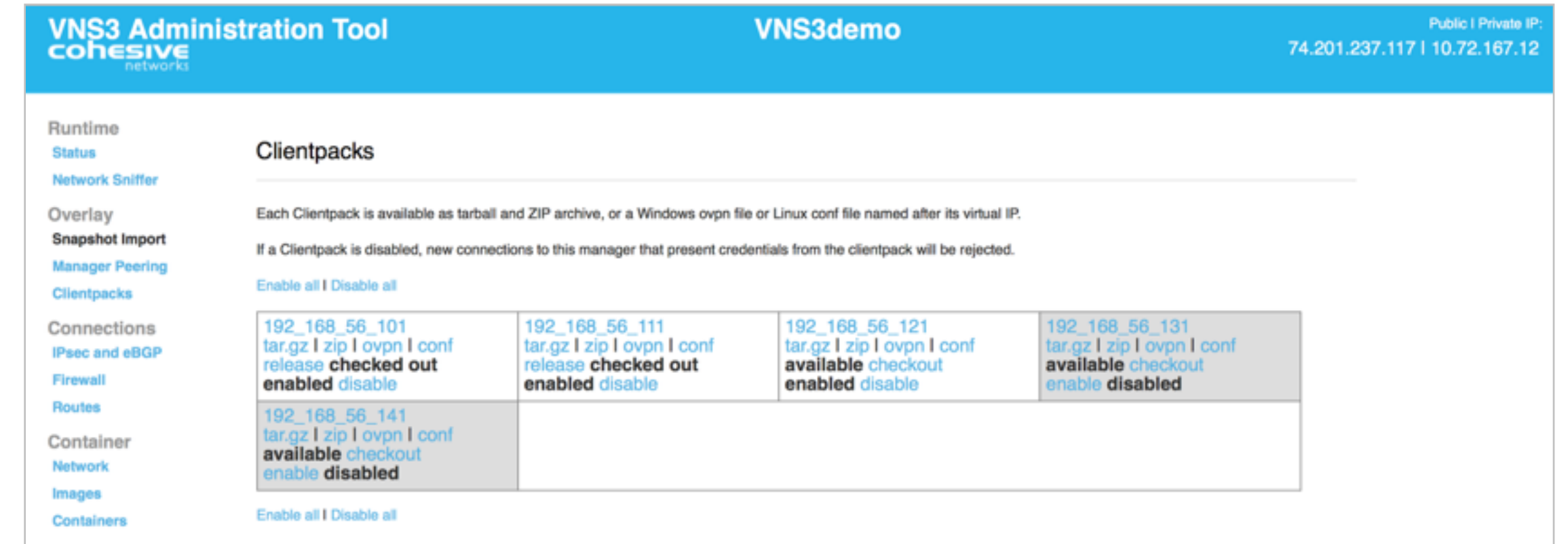
Tags: name = Database Server [x]

=

[Regenerate clientpack](#)

Disable unused clientpacks

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



The screenshot shows the VNS3 Administration Tool interface for 'VNS3demo'. The page title is 'Clientpacks'. Below the title, there is explanatory text: 'Each Clientpack is available as tarball and ZIP archive, or a Windows ovpn file or Linux conf file named after its virtual IP.' and 'If a Clientpack is disabled, new connections to this manager that present credentials from the clientpack will be rejected.' There are links for 'Enable all' and 'Disable all'. A table lists clientpacks with their virtual IP, file formats, and status. The table has four columns. The first column shows IP 192.168.56.101 with status 'checked out' and 'disabled'. The second column shows IP 192.168.56.111 with status 'checked out' and 'disabled'. The third column shows IP 192.168.56.121 with status 'available' and 'disabled'. The fourth column shows IP 192.168.56.131 with status 'available' and 'disabled'. A fifth row shows IP 192.168.56.141 with status 'available' and 'disabled'. There are also links for 'Enable all' and 'Disable all' at the bottom of the table.

Virtual IP	File Formats	Status
192.168.56.101	tar.gz zip ovpn conf	release checked out enabled disabled
192.168.56.111	tar.gz zip ovpn conf	release checked out enabled disabled
192.168.56.121	tar.gz zip ovpn conf	available checkout enabled disabled
192.168.56.131	tar.gz zip ovpn conf	available checkout enable disabled
192.168.56.141	tar.gz zip ovpn conf	available checkout enable disabled

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 inaccessible, 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.

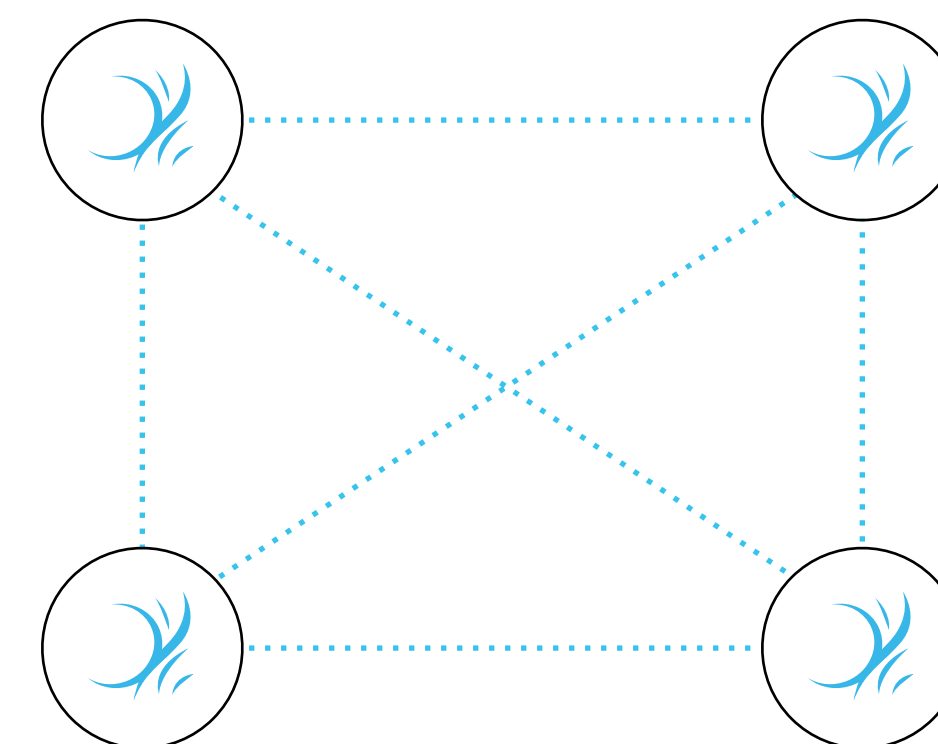


The screenshot shows the 'VNS3 Administration Tool' interface for 'CLDemoPriDBTier'. The 'Peering Setup' section includes fields for 'Manager #1 this instance', 'Manager #2' (74.201.237.117), 'Manager #3' (64.15.188.193), and 'Manager #4' (not set). A 'Save changes' button is visible at the bottom.



The screenshot shows the 'Peers and Clients' section with a table titled 'Links to Other Managers'.

Remote Manager ID	Remote Manager IP	Local Endpoint	Local Process Running?	Direct Link Status	Remote Manager Reachable?
2	74.201.237.117	server	running	up	reachable
3	64.15.188.193	server	running	up	reachable



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 Authentication 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.

The screenshot shows the VNS3 Administration Tool interface for editing a remote endpoint. The page title is "VNS3 Administration Tool" with the Cohesive Networks logo. The user is logged in as "VNS3demo" with public and private IP addresses: 74.201.237.117 and 10.72.167.12. The left sidebar contains navigation menus for Runtime, Overlay, Connections, Container, Maintenance, License Upgrade, Remote Support, and Admin. The main content area is titled "IPsec: Edit Remote Endpoint" and includes the following fields and options:

- Enter name (human readable description) for this endpoint:** VNS3demoFrontEnd
- Enter Internet IP address for this endpoint:** 206.142.241.56
- Enter PSK (Preshared Key) twice for confirmation:** ****
- If the Remote Endpoint is not directly connected to the Internet (i.e., is behind NAT), please enter its private IP address below. This is often referred to as IKE ID or PEER ID of the Remote Endpoint. If unsure, leave this blank.** 192.50.2.254
- Enable PFS (Perfect Forward Secrecy). If not sure, leave checked (enabled).
- Enable GRE over IPsec. If not sure, leave unchecked (disabled).
- Extra configuration parameters (if advised by CohesiveFT Technical Support). If not sure, leave blank.**

```
phase1=aes256-sha1-dh5
phase2=aes256-sha1
pfsgroup=dh5
phase1-lifetime=3600s
phase2-lifetime=28800s
dpdaction=restart
dpddelay=30s
dpdtimeout=90s
```

At the bottom of the form are "Save" and "Cancel" buttons.

Recommended IPsec Parameters

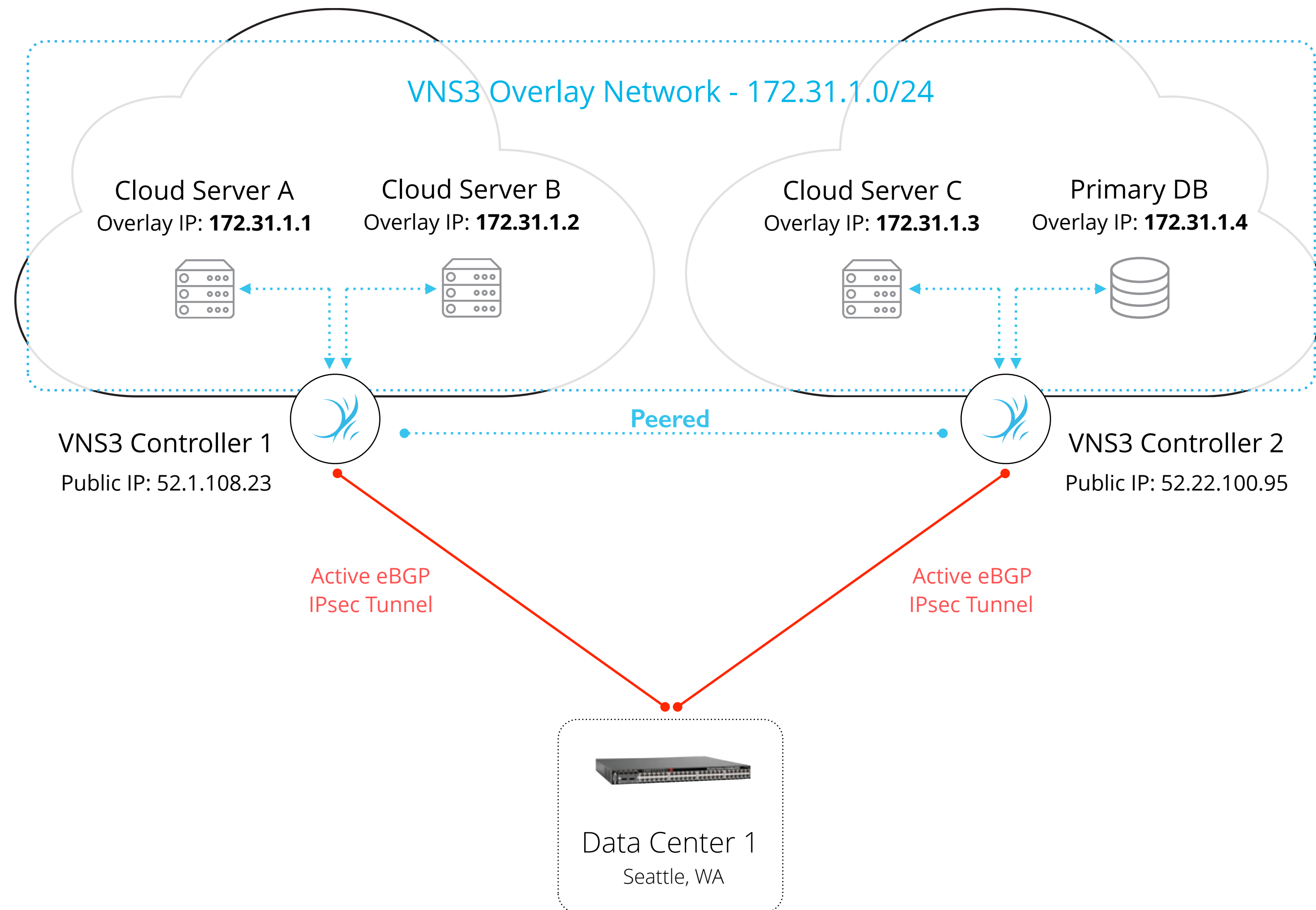
Based on experience connecting thousands of partner and customer devices we recommend the following IPsec tunnel settings:

- 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

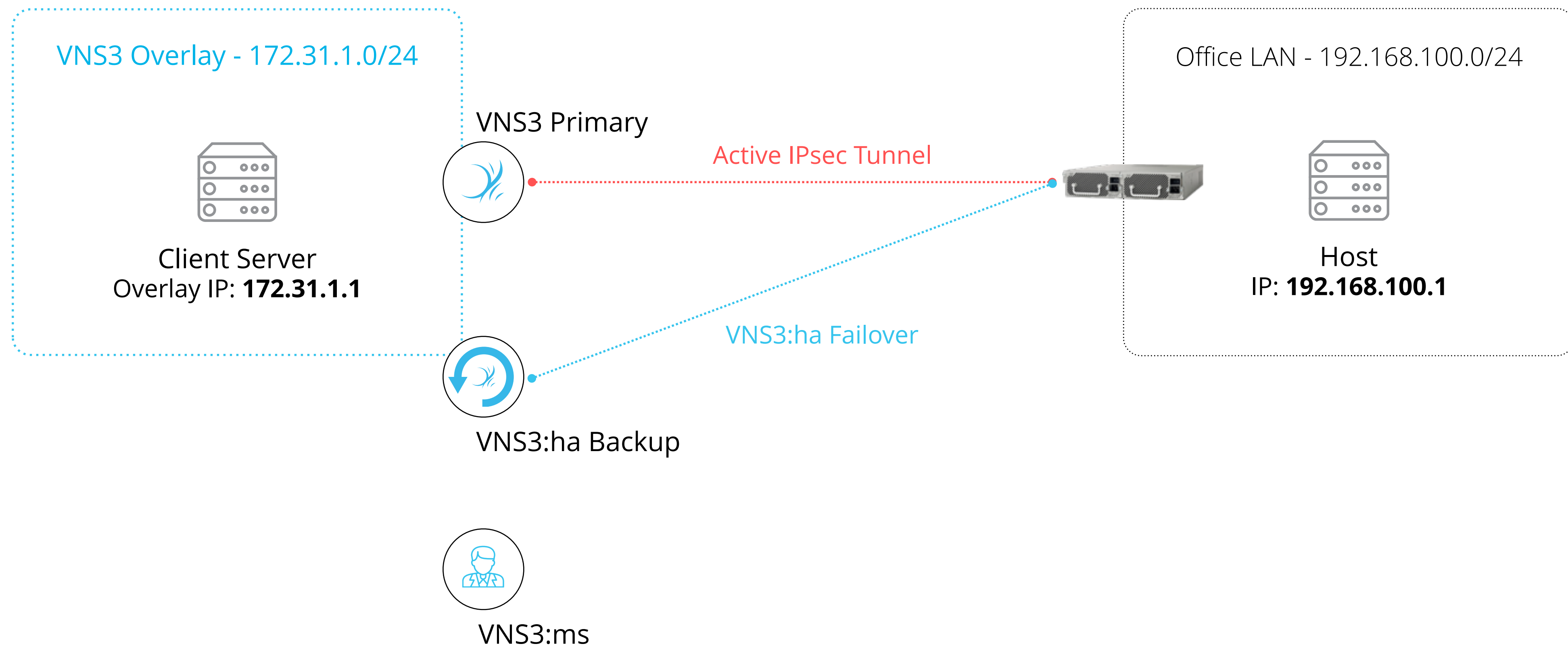
IPsec HA can be achieved using VNS3 Peered mesh and IPsec BGP tunnels that decide the quickest path.

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

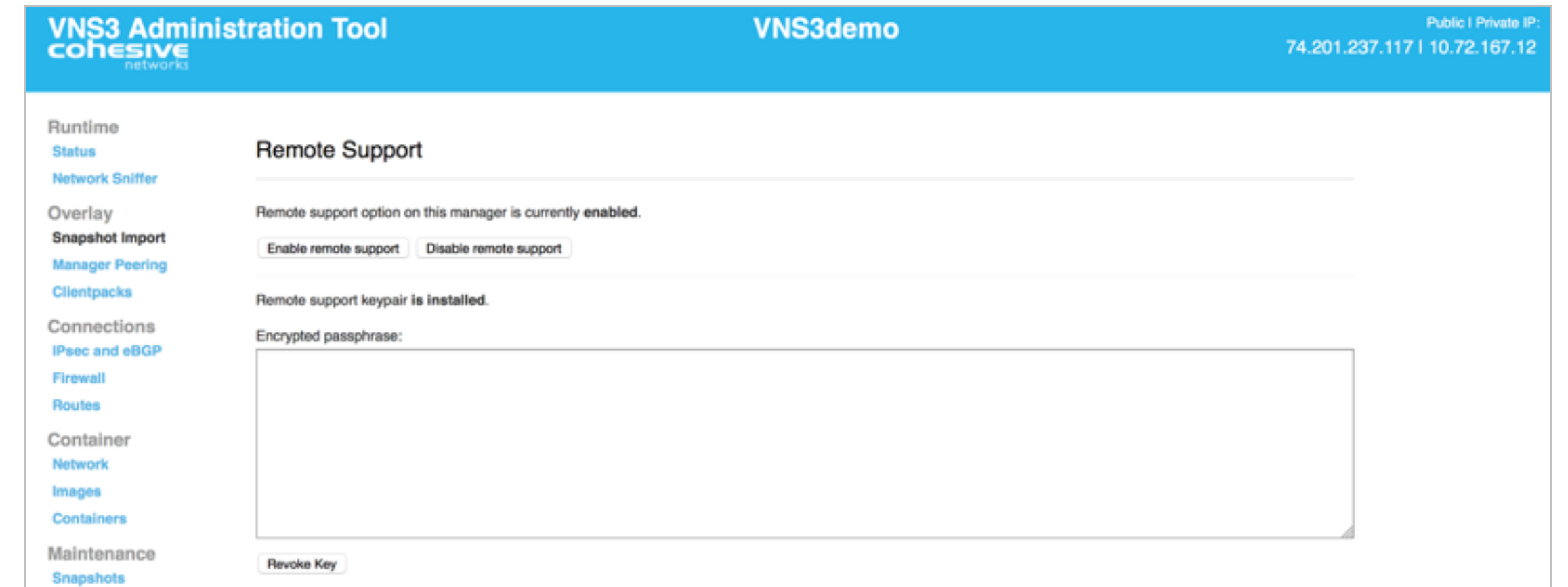
Many regulated industries have to follow best practices like changing default username and passwords. Having different access credentials for people and programs and a logical extension.

The screenshot displays the VNS3 Administration Tool interface. The top navigation bar is blue and contains the logo for 'cohesive networks', the text 'VNS3 Administration Tool', 'VNS3demo', and 'Public | Private IP: 74.201.237.117 | 10.72.167.12'. On the left side, there is a vertical menu with categories: Runtime (Status, Network Sniffer), Overlay (Snapshot Import, Manager Peering, Clientpacks), Connections (IPsec and eBGP, Firewall, Routes), Container (Network, Images, Containers), Maintenance (Snapshots, License Upgrade, Remote Support), and Admin (Topology Name, Admin Username, Admin & API Passwords, Reboot). The main content area is titled 'Change Username and/or Password' and contains the following text: 'Change VNS3 Web admin password for user "vns3ubed" and VNS3 API password. New passwords will take effect immediately and you will be asked to re-authenticate using your new password once you submit the form below. To leave a password unchanged, leave it blank.' Below this text are four input fields: 'Type new VNS3 Web admin password:', 'Re-type new VNS3 Web admin password:', 'Type new API password:', and 'Re-type new API password:'. A 'Change password(s)' button is located at the bottom of the form.

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.



The screenshot displays the VNS3 Administration Tool interface. The top navigation bar is blue and contains the text "VNS3 Administration Tool" on the left, "VNS3demo" in the center, and "Public | Private IP: 74.201.237.117 | 10.72.167.12" on the right. Below the navigation bar is a sidebar menu with the following items: "Runtime" (selected), "Status", "Network Sniffer", "Overlay", "Snapshot Import", "Manager Peering", "Clientpacks", "Connections", "IPsec and eBGP", "Firewall", and "Routes". The main content area is titled "Runtime Snapshots" and contains a section for "Available Snapshots" with two entries: "snapshot_20150707_1436296252_74.201.237.117 (created on 2015-07-07 19:10:52 +0000) [x]" and "snapshot_20150707_1436275822_74.201.237.117 (created on 2015-07-07 13:30:23 +0000) [x]". Below this is a "Create Snapshot" section with a button labeled "Take New Snapshot Now".

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.)

