Cohesive Networks

VNS3 IPsec Configuration
VNS3 to Cisco ASA ASDM 9.2
IPsec protocol allows you to securely connect two sites together over the public internet using cryptographically secured services. IPsec ensure private and secure communication between two devices. This type of VPN has many use-cases. We will focus on the Site-to-Site or LAN-to-LAN setup most often used with VNS3 to build Hybrid Clouds.

- Many network hardware devices support IPsec tunneling functionality. Check your device's data sheet to see if it is compatible with VNS3. The requirements are:
  - IKE1 or IKE2
  - AES256 or AES128 or 3DES
  - SHA1 or MD5
  - NAT-Traversal capability (some clouds require NAT-Traversal encapsulation - AWS Generic EC2, Microsoft Azure, etc.)

A diagram of the typical secure hybrid cloud setup using VNS3 is provided on the right. The IPsec tunnel provides secure and encrypted connectivity between the office subnet (192.168.3.0/24) and the VNS3 Overlay Network (172.31.1.0/24).

This guide will provide steps to setup the Cisco ASA side of the IPsec configuration.

The most important thing in any IPsec configuration is to make sure all settings match on both devices that are going to connect to each other. Mismatches are the primary cause for tunnel failure or instability.
Use the Cisco VPN Wizard - Site-to-Site

Unless you are familiar with the Cisco ASA CLI or ASDM, the configuration wizards are the easiest way to configure an IPsec tunnel.

From the Cisco ASDM menu click Wizards>VPN Wizards>Site-to-site VPN Wizard.
The first page of the Site-to-site VPN Connection Setup Wizard provides a diagram (similar to the one on page 2 of this document) and a link to a video that explains the configuration process.

Click **Next**.
The first step in setting up an IPsec tunnel is to let the Cisco ASA know where it will be negotiating the tunnel via Public IP address.

Enter the **VNS3 Manager's Public IP** address in the Peer IP Address field.

Choose **outside** as the **VPN Access Interface** as this tunnel will be negotiated out via the public Internet.

Click **Next**.
Once the ASA knows where the other device is located that it will be building the IPsec to with, the next step is to configure what traffic will be allowed to pass over the tunnel. This is done by entering in network ranges: one range for the local (what is available "behind" the Cisco ASA) and one range for the remote (what is available "behind" the VNS3 instance).

**NOTE:** Use CIDR notation ([CIDR Subnet Calculator](https://www.cis证券投资.com/cidr-calculator)) here and avoid using the network group objects (see page 13). If you need to advertise more than one subnet range simply enter them in a comma separated list (e.g 172.31.1.0/25, 172.31.1.128/25).

Enter your **Local Subnet** in the Local Network field.

Enter the **VNS3 Overlay Subnet/Unencrypted VLAN** in the Remote Network field.

Click **Next**.

*If you are unsure which network to use for the remote network, contact our support team.*
VNS3 supports IPsec tunnel authentication using a pre-shared key (PSK). A PSK is a shared secret between the two connecting parties (in this case owner of the Cisco and the owner of the ASA). Even if a VPN IPsec connection is encrypted, the PSK confirms the peer or device you are establishing connection with is the one you intend to use. Encryption provides confidentiality in the connection and PSK ensures that only you and the other party can provide the required authentication.

VNS3 does not currently support certificate based authentication. If this is a requirement for your deployment contact our support team.

Enter a PSK that will be used for both sides of the connection in the Pre-shared Key field. In our VNS3 Configuration PDF we use test.

**NOTE:** There may be more fields than displayed to the left for IKEv2. Enter in the same PSK for each field.

Click **IKE Version** and select **IKE Version 1**.*

*IKE Version 2 is supported in 3.5+ versions of VNS3. To ensure the highest interop, use IKE v1.
The next step in setting up the security profile for an IPsec configuration is to choose the encryption algorithms that will be used to encapsulate the traffic moving through the tunnel. The settings must match on both sides of the tunnel configuration. Policies are made of an algorithm, hashing and potentially Diffie-Hellman Group.

Click Encryption Algorithms from the Custom Configuration pane menu.

Select the IKE (Phase1) policy and enter it into the IKE Policy field.

NOTE: the IKE Policy is a ASA global setting and is shared with all connections. If you change this, you may experience problems with other existing connections.

Select the IPsec SA (Phase2) policy and enter it into the IPsec Proposal field.

PFS ensures you never regenerate the same key that will be used in encapsulating IPsec VPN traffic. Enabling PFS significantly limits the what a malicious third party can do/see if they compromise a key. Cohesive recommends enabling PFS as best practice.

Click Perfect Forward Secrecy from the Custom Configuration pane menu.

Click the PFS check box and choose a PFS Diffie-Hellman Group from the drop down menu.

Click Next.
The NAT Exempt setting simply tells the ASA not to translate the traffic associated with the tunnel. Source and destination traffic retain the untranslated version of their subnets. In a standard/traditional configuration, NAT Exempt should be checked.

NOTE: If the local subnet (address range "behind" the ASA) is not the actual range and you are using Network Address Translation, this box will need to be left uncheck. For this example we will assume the Traffic configuration on page 6 is using the actual subnet ranges.

Check the **NAT Exempt Box**.

Click **Next**.
Review the IPsec tunnel configuration parameters to make sure everything is entered as expected and matches the VNS3 configuration.

Click Finish.
Once the tunnel has been established, you can monitor the tunnel session information for any issues.

Click **Monitoring** on the ASDM top menu.

Click **VPN** from the bottom left menu.

Click **VPN Statistics>Sessions** from the VPN left column menu pane.

Select the **Connection Profile** and click **Details**.
Troubleshooting
Cisco Network Group Objects allow more than one tunnel/subnet/sa be included in a single ACL line. Cisco Network Group Objects create interoperability problems with VNS3 (and other manufactures) and are NOT SUPPORTED.

```plaintext
access-list VPN_ACL extended permit ip object-group REMOTE object-group LOCAL

object-group network REMOTE
network-object 172.31.0.0 255.255.255.0
network-object 172.21.1.0 255.255.255.0

object-group network LOCAL
network-object 192.168.0.0 255.255.255.0
```

It is recommend that you use the non-grouped ACL syntax with specific address statements.

```plaintext
access-list VPN_ACL-1 line 1 extended permit ip 192.168.0.0 255.255.255.0 172.31.0.0 255.255.255.0
access-list VPN_ACL-1 line 1 extended permit ip 192.168.0.0 255.255.255.0 172.31.1.0 255.255.255.0
```
Interesting Traffic

The first step in initiating the IPsec negotiation process with a Cisco device is sending Interesting Traffic. Interesting traffic as defined by Cisco:

Determining what type of traffic is deemed interesting is part of formulating a security policy for use of a VPN. The policy is then implemented in the configuration interface for each particular IPSec peer. For example, in Cisco routers and PIX Firewalls, access lists are used to determine the traffic to encrypt. The access lists are assigned to a crypto policy such that permit statements indicate that the selected traffic must be encrypted, and deny statements can be used to indicate that the selected traffic must be sent unencrypted. With the Cisco Secure VPN Client, you use menu windows to select connections to be secured by IPsec. When interesting traffic is generated or transits the IPsec client, the client initiates the next step in the process, negotiating an IKE phase one exchange.

Interesting traffic is tunnel traffic that has a source/destination that fits with the tunnel definition/ACLs that were created as part of the IPsec configuration.

It is recommended that a continuous ping is setup on both sides of the tunnel during configuration to ensure interesting traffic is present to begin the IPsec negotiation process.
VPN Idle Timeout is a Cisco setting that will terminate an IPsec connection if there is no communication activity on the connection in the period defined.

Terminated IPsec connections can alarm operations teams and require a specific direction of interesting traffic to re-build/re-negotiate the tunnel. This can be at best a nuisance for production systems. It is recommended this setting is turned off or setting the idle timeout to Unlimited.

To turn off the vpn-idle-timeout via ASDM, click Configuration>Site-to-Site VPN>Group Policies then on the Group Policy created for your tunnel. The resulting page will have a Idle Timeout checkbox, make sure it is set to Unlimited.

To turn vpn-idle-timeout off via the CLI use the following under the Group Policy associated with the tunnel:

```
vpn-idle-timeout none
OR
no vpn-idle-timeout
```

NOTE: when setting up your IPsec configuration via the Site-to-site VPN Wizard, the setting for vpn-idle-timeout will be inherited from your Default Group Policy as configured out your ASA. Double check to make sure it is disabled after tunnel configuration.
VNS3 Configuration Instructions (Free & Lite Editions | BYOL)
Instructions and screenshots for configuring a VNS3 Controller in a single or multiple Controller topology. Specific steps include, initializing a new Controller, generating clientpack keys, setting up peering, building IPsec tunnels, and connecting client servers to the Overlay Network.

VNS3 Administration Document
Covers the administration and operation of a configured VNS3 Controller. Additional detail is provided around the VNS3 Firewall, all administration menu items, upgrade licenses, other routes and SNMP traps.

VNS3 Troubleshooting
Troubleshooting document that provides explanation issues that are more commonly experienced with VNS3.