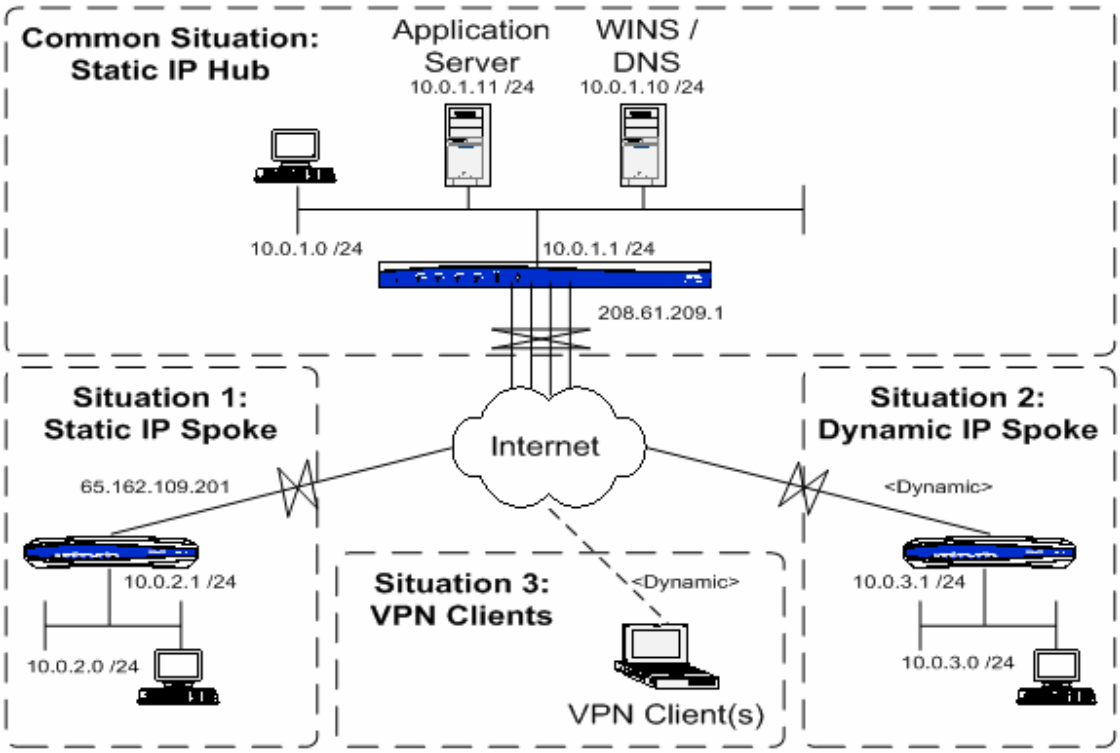
June 2008

Quick Configuration Guide
Configuring a Hub & Spoke VPN in AOS

Configuring a Hub & Spoke VPN in AOS



Introduction

The traditional VPN connection is used to connect two private subnets using a virtual link over a public network. If multiple sites need to communicate with one another, it requires that either (1) a VPN connection must be made from each site to each site also called a Full Mesh, or (2) the sites must be allowed to communicate through a central site, called a Hub & Spoke, which this document will cover.

Hardware/Software Requirements

- Unit must be operating on Enhanced firmware (EFP), which is an optional upgrade on most Netvanta models. Other models are only sold with the EFP.
- Network IP addressing must follow a logical, sequential pattern to allow for the super-netting process explained later.

Overview

Configuring the Hub & Spoke network requires the following steps to be taken:

- Proper IP Addressing
- Standard VPN Settings / Considerations
- Hub Configuration Based Upon Scenario
    - Static IP
    - Dynamic IP
    - VPN Client
- Spoke Configuration Based Upon Scenario
    - Static IP
        - Static IP behind NAT
    - Dynamic IP
    - VPN Client
    - Dual Internet (Fail-over, not Load-Sharing)
- Addendum
    - Firewall Settings
    - VPN Keep-Alive

Proper IP Addressing

Regardless of the type of Spoke scenario, the most important aspect of any Hub & Spoke VPN is logical, sequential private IP addressing to allow for super-netting. Within the VPN configuration the traffic type and range must be specified, resulting in only the configured traffic being allowed to traverse the tunnel. If multiple ranges, called selectors in AOS, are defined, it results in multiple tunnels to the same peer. The key, therefore, is to reduce the selectors to a single entry.

A single selector is possible if every subnet in the network can be selected by a single range that encompasses only those networks. To illustrate this point, consider the following example:

Site	IP Subnet	IP Subnet Mask
Hub	10.0.1.0	255.255.255.0
Spoke 1	10.0.2.0	255.255.255.0
Spoke 2	10.0.3.0	255.255.255.0
…	…	…
Spoke 253	10.0.253.0	255.255.255.0
Clients	10.0.254.0	255.255.255.0

In this example, all of the subnets can be combined, or super-netted, into a single range:

Site	IP Subnet	IP Subnet Mask
All	10.0.0.0	255.255.0.0

To illustrate an incorrect IP configuration, consider the following example:

Site	IP Subnet	IP Subnet Mask
Hub	10.0.1.0	255.255.255.0
Spoke 1	172.16.0.0	255.255.255.0
Spoke 2	192.168.1.0	255.255.255.0

In this example of an incorrect IP configuration, the only selector that can encompass all of the various subnets would have to match every IP address, and would interfere with Internet traffic:

Site	IP Subnet	IP Subnet Mask
All	0.0.0.0	0.0.0.0

If this selector was used, traffic to www.google.com would go through the VPN tunnel, for instance.

Standard VPN Settings / Considerations

In every VPN setup, there a several settings that must be configured, each having a different impact on the security and throughput of the tunnel.

- Phase 1 (referred to as IKE) Tunnel Mode:
  - The mode types are Main & Aggressive.
    - Main mode is the most secure type, but it requires that IP Address ID type is used, which is usually only feasible if the VPN peer has a static IP.
    - Aggressive mode does not allow for negotiation of settings, but a properly configured VPN should not have to negotiate settings. This tunnel type is usually used when a VPN peer is on a dynamic IP, or if IP Address ID type cannot be used.
- ID Type / Value:
  - The allowable ID types are: IP Address, FQDN, User-FQDN, and ASN-DN.
    - IP Address is a four-octet number representing an IP address. The IP address sent by default is the current primary IP of the outgoing (egress) interface. Until 17.01 firmware, this was the only address that could be sent when using the IP Address type. After 17.01 firmware, any address configured can be sent. This is the address type used with Main mode tunnels.

        - FQDN is an acronym for Fully-Qualified Domain Name. Contrary to what one might think, there is no DNS or third-party lookup involved. This is simply a string of characters that must match on both sides. The FQDN sent does not have to be a real domain name. This is the address type used with Aggressive mode tunnels.
        - User-FQDN is another way of saying Email Address. The same rules that apply to the FQDN ID-type apply to the User-FQDN type.
        - ASN-DN is in its own special class because it is only used if certificates are used, so this will not be covered in this document.
- IKE Hashing:
    - The hashing function is used to ensure authenticity & integrity of the VPN packet sent to the VPN peer.
    - The Netvanta series supports MD5 & SHA-1.
        - MD5 is a 128-bit hash output.
        - SHA-1 is a 160-bit hash output, and is more secure and slightly slower because of it.
- IKE Encryption:
    - The encryption function is used to protect the VPN payload.
    - The Netvanta series supports DES, 3DES, & AES-128/192/256 encryption. A higher bit number yields a more secure connection.
        - DES is a 56-bit encryption and is only supported for legacy devices.
        - 3DES is a 168-bit encryption and is the de-facto standard in use at this time.
        - AES-128/192/256 is a 128-bit / 192-bit / 256-bit encryption, depending on the mode of AES chosen. AES is a modern encryption function which was designed with hardware in mind to achieve adequate encryption with adequate throughput capability.
- IKE Diffie-Hellman Key Group:
    - The key group is used in the key exchange process that protects the negotiation of the actual encryption keys.
    - All Netvanta units support groups 1 & 2. Support for group 5 was added in 15.01 firmware.
    - The higher the group, the higher the security, but the more processor-intensive the key exchange.
- IKE Authentication:
    - Authentication is how VPN peers ensure the device they are negotiating with is authorized to connect.
    - This is performed by using the defined key with the hashing function described above.
    - Netvanta units support Pre-Shared Keys and Certificates.
        - Pre-Shared keys require less overhead and configuration, and will be described in this document.
        - Certificates require setting up a certificate server, or paying a public service such as VeriSign. This type will not be covered.

- IKE Lifetime:
  - Lifetime is defined in seconds and determines the amount of time between negotiations. The default value is 28800 seconds, or 8 hours.
  - Each negotiation creates a new encryption key so that anyone attempting to break the previous key has to start again.
- Phase 2 (referred to as IPSEC) Tunnel Mode:
  - The tunnel types are Transport & Tunnel.
  - Netvanta units only support Tunnel mode.
    - Any Transport mode tunnel can also operate in Tunnel mode.
- IPSEC Hashing:
  - Same function as IKE Hashing, and is usually set to the same value.
- IPSEC Encryption:
  - Same function as IKE Encryption, and is usually set to the same value
- IPSEC Perfect Forward Secrecy (PFS) Key Group (Optional):
  - If the IPSEC lifetime is set to less than the IKE lifetime, PFS should be used.
  - If PFS is not used, the same key negotiated in IKE will be used again.
- IPSEC Life Type / Value:
  - The life types are defined in seconds, kilobytes, or both.
  - The lifetime should always be defined in seconds, or both seconds & kilobytes. If both are defined, the first one to reach the limit causes a re-negotiation.
  - The lifetime should be less than or equal to the lifetime of IKE.

Hub Settings

The Hub will be creating a connection to each Spoke, and will allow traffic between Spokes. Since the traffic that is allowed to traverse a VPN tunnel must be specified, the destination network will be the Spoke's IP subnet and the source network will be the super-netted subnet. This will allow any network within that super-net to converse with the Spoke's IP subnet.

Each Spoke will have an individual Remote-ID & IPSEC policy. The IKE policy will be the same for each Spoke with a dynamic IP, and will have an individual policy for each Spoke with a static IP. This means that the Hub will be able to initiate a tunnel to any Spoke with a static IP, but each Spoke with a dynamic IP must initiate the tunnel to the Hub.

The Hub, and each static IP Spoke, will use the IP Address ID-Type, with the value being their respective static IP. They will use Main mode. Both the Hub and the Spoke will be capable of initiating the tunnel.

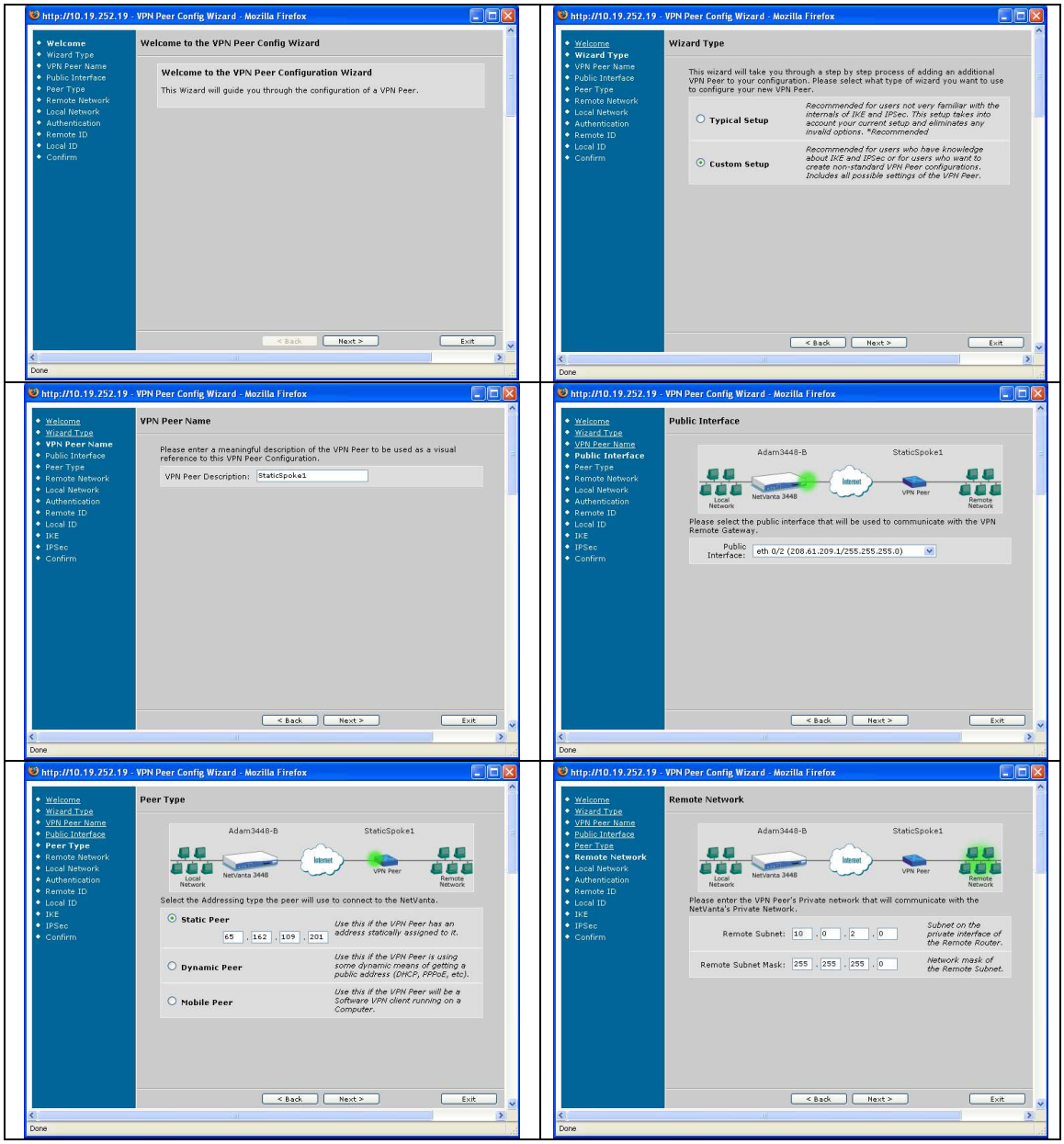
Each dynamic Spoke & each VPN Client will need to use either FQDN or User-FQDN ID-Type. They will use Aggressive mode. Only the Spoke or VPN Client will be capable of initiating the tunnel.

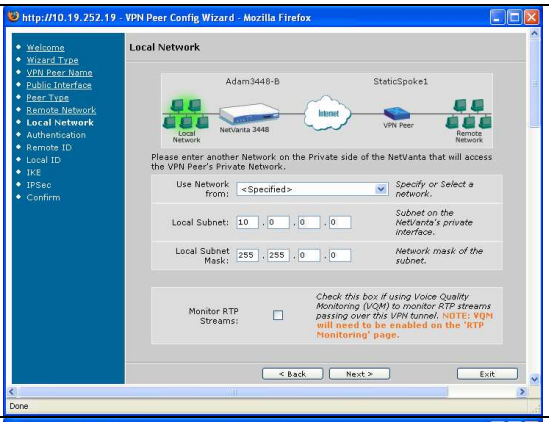
Scenario 1: Hub Configuration for a Static IP Spoke

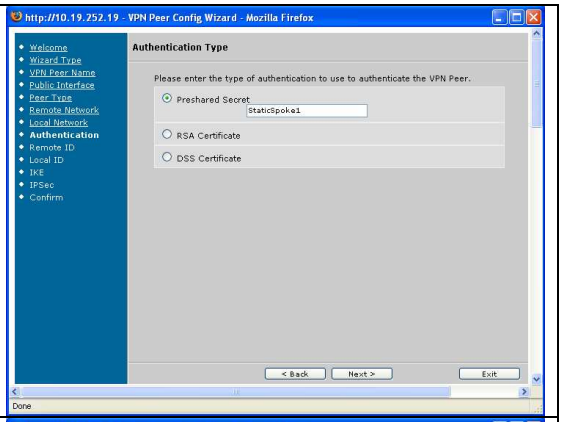
To setup a static IP Spoke through the CLI, the configuration will look similar to the example below. Each static IP Spoke will have its own IKE policy.

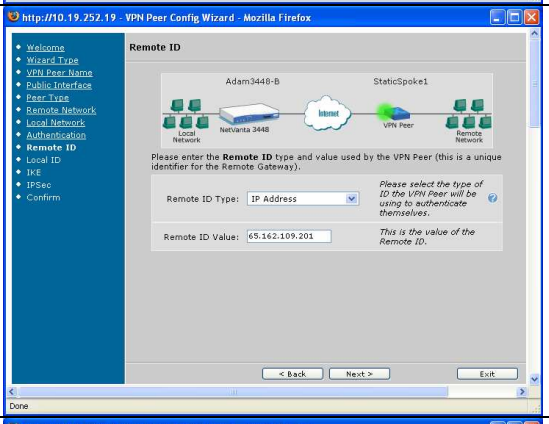
```
ip crypto

crypto ike policy 2
  initiate main
  respond main
  local-id address 208.61.209.1
  peer 65.162.109.201
  attribute 1
    hash md5
    encryption 3des
    authentication pre-share
    group 1
    lifetime 28800

crypto ike remote-id address 65.162.109.201 preshared-key StaticSpoke1
ike-policy 2 crypto map VPN 2 no-mode-config no-xauth

crypto ipsec transform-set 3DES-MD5 esp-3des esp-md5-hmac
  mode tunnel

crypto map VPN 2
  match address VPN-2-Selectors
  set transform-set 3DES-MD5
  set security-association lifetime seconds 28800
  peer 65.162.109.201
  ike-policy 2

ip access-list extended VPN-2-Selectors
  permit ip 10.0.0.0 0.0.255.255 10.0.2.0 0.0.0.255

interface ppp 1
  access-policy Public
  crypto map VPN
```

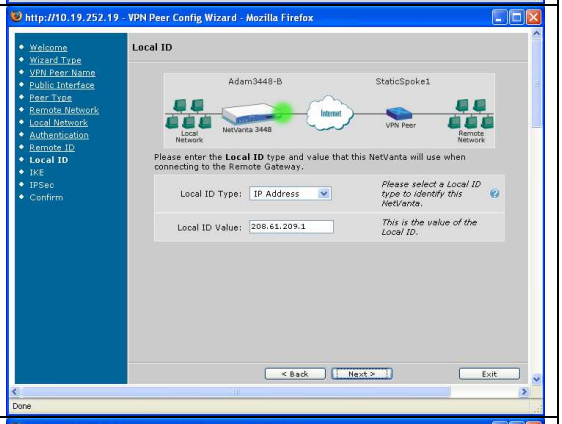
To setup a static IP Spoke through the GUI, the VPN wizard will be used, custom mode:

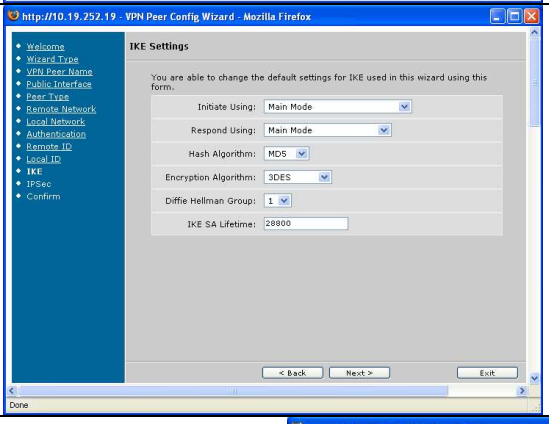


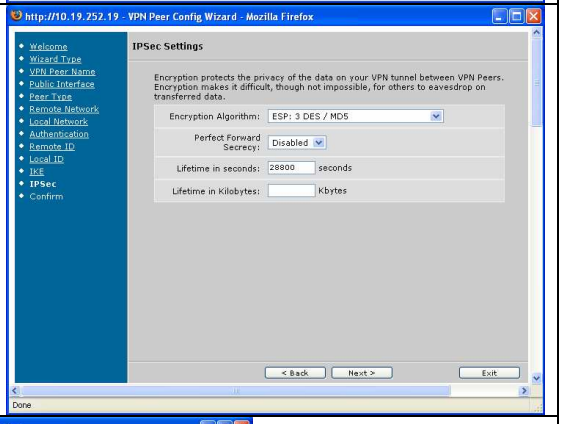

http://10.19.252.19 - VPN Peer Config Wizard - Mozilla Firefox
Welcome
Wizard Type
VPN Peer Name
Public Interface
Peer Type
Remote Network
Local Network
Authentication
Remote ID
Local ID
IKE
IPSec
Confirm
Local Network
Adam3448-B
StaticSpoke1
Internet
NetVanta 3448
VPN Peer
Please enter another Network on the Private side of the NetVanta that will access the VPN Peer's Private Network.
Use Network from:
<Specified>
Specify or Select a network.
Local Subnet:
10 . 0 . 0 . 0
Subnet on the NetVanta's private interface.
Local Subnet Mask:
255 . 255 . 0 . 0
Network mask of the subnet.
Monitor RTP Streams:
Check this box if using Voice Quality Monitoring (VQM) to monitor RTP streams passing over this VPN tunnel. NOTE: VQM will need to be enabled on the 'RTP Monitoring' page.
< Back
Next >
Exit
Done

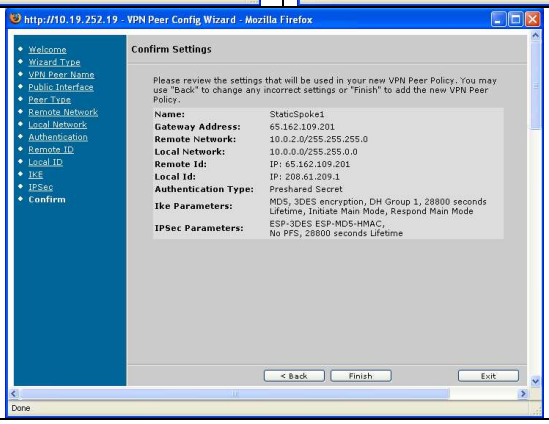

http://10.19.252.19 - VPN Peer Config Wizard - Mozilla Firefox
Welcome
Wizard Type
VPN Peer Name
Public Interface
Peer Type
Remote Network
Local Network
Authentication
Remote ID
Local ID
IKE
IPSec
Confirm
Authentication Type
Please enter the type of authentication to use to authenticate the VPN Peer.
Preshared Secret
StaticSpoke1
RSA Certificate
DSS Certificate
< Back
Next >
Exit
Done


http://10.19.252.19 - VPN Peer Config Wizard - Mozilla Firefox
Welcome
Wizard Type
VPN Peer Name
Public Interface
Peer Type
Remote Network
Local Network
Authentication
Remote ID
Local ID
IKE
IPSec
Confirm
Remote ID
Adam3448-B
StaticSpoke1
Internet
NetVanta 3448
VPN Peer
Please enter the Remote ID type and value used by the VPN Peer (this is a unique identifier for the Remote Gateway).
Remote ID Type:
IP Address
Please select the type of ID the VPN Peer will be using to authenticate themselves.
Remote ID Value:
65.162.109.201
This is the value of the Remote ID.
< Back
Next >
Exit
Done


http://10.19.252.19 - VPN Peer Config Wizard - Mozilla Firefox
Welcome
Wizard Type
VPN Peer Name
Public Interface
Peer Type
Remote Network
Local Network
Authentication
Remote ID
Local ID
IKE
IPSec
Confirm
Local ID
Adam3448-B
StaticSpoke1
Internet
NetVanta 3448
VPN Peer
Please enter the Local ID type and value that this NetVanta will use when connecting to the Remote Gateway.
Local ID Type:
IP Address
Please select a Local ID type to identify this NetVanta.
Local ID Value:
208.61.209.1
This is the value of the Local ID.
< Back
Next >
Exit
Done


http://10.19.252.19 - VPN Peer Config Wizard - Mozilla Firefox
Welcome
Wizard Type
VPN Peer Name
Public Interface
Peer Type
Remote Network
Local Network
Authentication
Remote ID
Local ID
IKE
IPSec
Confirm
IKE Settings
You are able to change the default settings for IKE used in this wizard using this form.
Initiate Using:
Main Mode
Respond Using:
Main Mode
Hash Algorithm:
MD5
Encryption Algorithm:
3DES
Diffie Hellman Group:
1
IKE SA Lifetime:
28800
< Back
Next >
Exit
Done


http://10.19.252.19 - VPN Peer Config Wizard - Mozilla Firefox
Welcome
Wizard Type
VPN Peer Name
Public Interface
Peer Type
Remote Network
Local Network
Authentication
Remote ID
Local ID
IKE
IPSec
Confirm
IPSec Settings
Encryption protects the privacy of the data on your VPN tunnel between VPN Peers. Encryption makes it difficult, though not impossible, for others to eavesdrop on transferred data.
Encryption Algorithm:
ESP: 3 DES / MD5
Perfect Forward Secrecy:
Disabled
Lifetime in seconds:
28800
seconds
Lifetime in Kilobytes:
Kbytes
< Back
Next >
Exit
Done

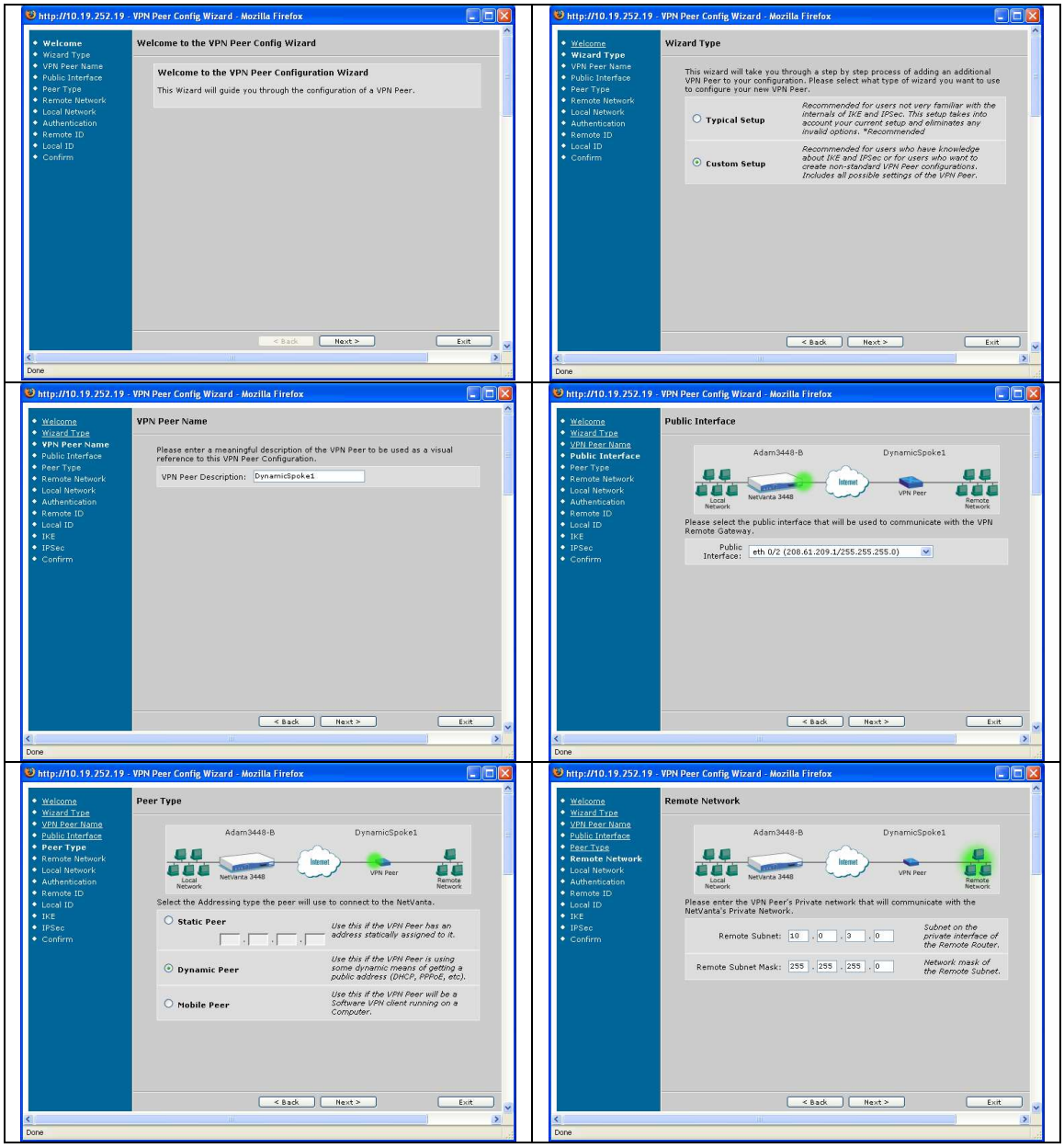

http://10.19.252.19 - VPN Peer Config Wizard - Mozilla Firefox
Welcome
Wizard Type
VPN Peer Name
Public Interface
Peer Type
Remote Network
Local Network
Authentication
Remote ID
Local ID
IKE
IPSec
Confirm
Confirm Settings
Please review the settings that will be used in your new VPN Peer Policy. You may use "Back" to change any incorrect settings or "Finish" to add the new VPN Peer Policy.
Name: StaticSpoke1
Gateway Address: 65.162.109.201
Remote Network: 10.0.2.0/255.255.255.0
Local Network: 10.0.0.0/255.255.0.0
Remote Id: IP: 65.162.109.201
Local Id: IP: 208.61.209.1
Authentication Type: Preshared Secret
Ike Parameters: MD5, 3DES encryption, DH Group 1, 28800 seconds Lifetime, Initiate Main Mode, Respond Main Mode
IPSec Parameters: ESP-3DES ESP-MD5-HMAC, No PFS, 28800 seconds Lifetime
< Back
Finish
Exit
Done

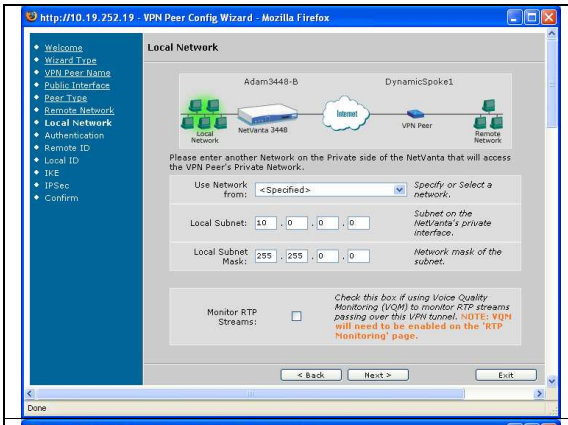
Scenario 2: Hub Configuration for a Dynamic IP Spoke

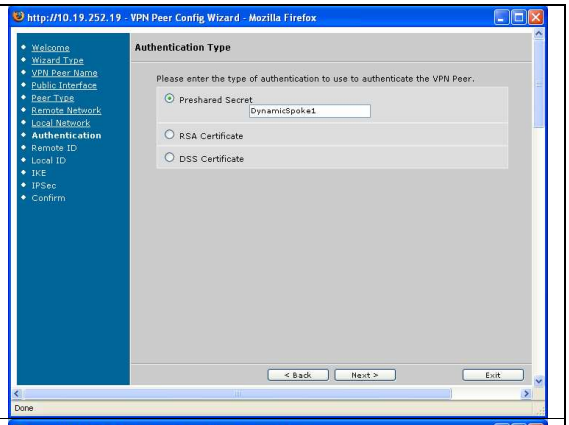
To setup a dynamic IP Spoke through the CLI, the configuration will look similar to the example below. Every dynamic IP Spoke will share the same IKE policy.

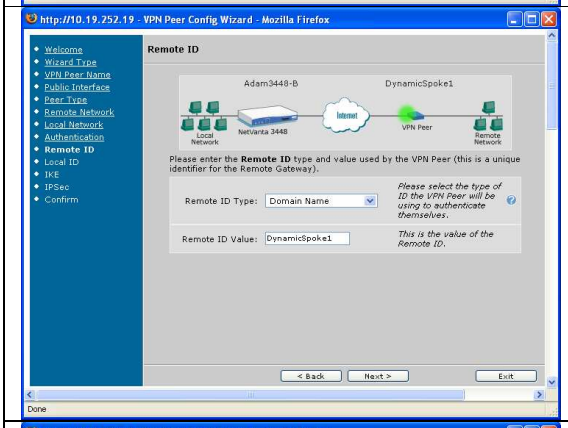
```
ip crypto

crypto ike policy 1
  no initiate
  respond aggressive
  local-id address 208.61.209.1
  peer any
  attribute 1
    hash md5
    encryption 3des
    authentication pre-share
    group 1
    lifetime 28800

crypto ike remote-id fqdn DynamicSpoke1 preshared-key DynamicSpoke1
ike-policy 1 crypto map VPN 3 no-mode-config no-xauth

crypto ipsec transform-set 3DES-MD5 esp-3des esp-md5-hmac
  mode tunnel

crypto map VPN 3
  match address VPN-3-Selectors
  set transform-set 3DES-MD5
  set security-association lifetime seconds 28800
  ike-policy 1

ip access-list extended VPN-3-Selectors
  permit ip 10.0.0.0 0.0.255.255 10.0.3.0 0.0.0.255

interface ppp 1
  access-policy Public
  crypto map VPN
```

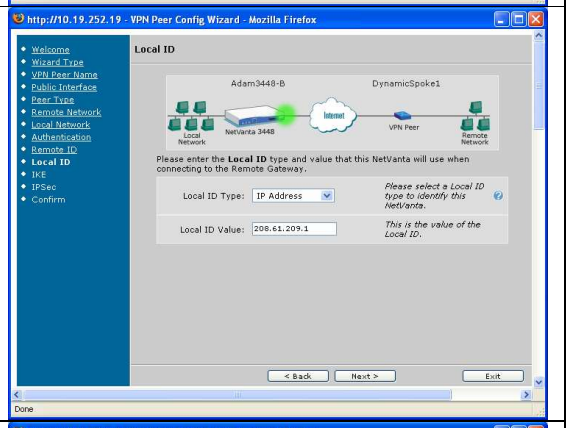
To setup a dynamic IP Spoke through the GUI, the VPN wizard will be used, custom mode:

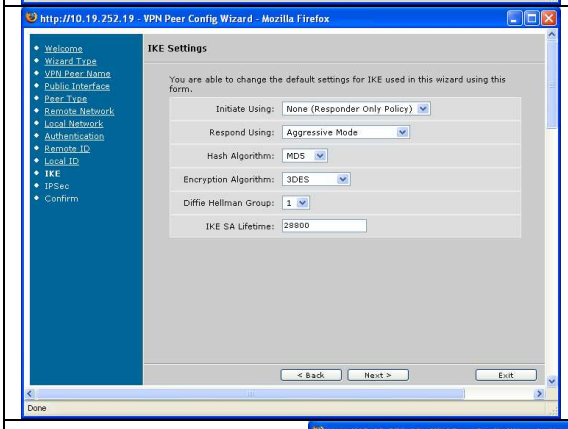


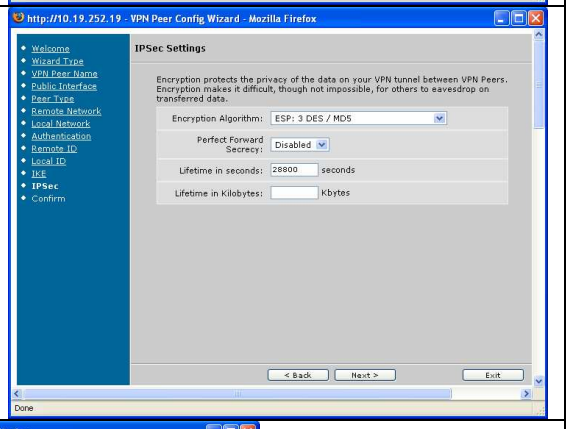

http://10.19.252.19 - VPN Peer Config Wizard - Mozilla Firefox
Welcome
Wizard Type
VPN Peer Name
Public Interface
Peer Type
Remote Network
Local Network
Authentication
Remote ID
Local ID
IKE
IPSec
Confirm
Local Network
Adam3448-B
DynamicSpoke1
Internet
NetVanta 3448
VPN Peer
Local Network
Remote Network
Please enter another Network on the Private side of the NetVanta that will access the VPN Peer's Private Network.
Use Network from:
<Specified>
Specify or Select a network.
Local Subnet:
10 . 0 . 0 . 0
Subnet on the NetVanta's private interface.
Local Subnet Mask:
255 . 255 . 0 . 0
Network mask of the subnet.
Monitor RTP Streams:
Check this box if using Voice Quality Monitoring (VQM) to monitor RTP streams passing over this VPN tunnel. NOTE: VQM will need to be enabled on the 'RTP Monitoring' page.
< Back
Next >
Exit
Done

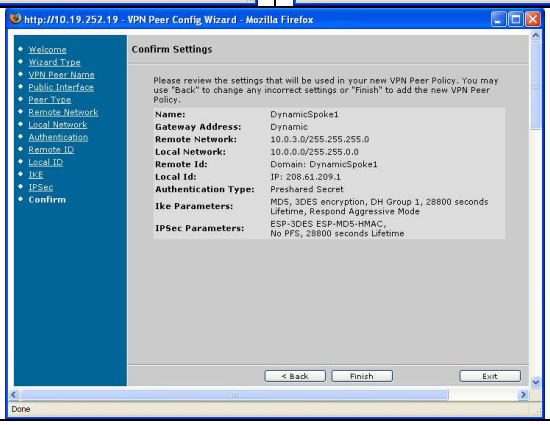

http://10.19.252.19 - VPN Peer Config Wizard - Mozilla Firefox
Welcome
Wizard Type
VPN Peer Name
Public Interface
Peer Type
Remote Network
Local Network
Authentication
Remote ID
Local ID
IKE
IPSec
Confirm
Authentication Type
Please enter the type of authentication to use to authenticate the VPN Peer.
Preshared Secret
DynamicSpoke1
RSA Certificate
DSS Certificate
< Back
Next >
Exit
Done


http://10.19.252.19 - VPN Peer Config Wizard - Mozilla Firefox
Welcome
Wizard Type
VPN Peer Name
Public Interface
Peer Type
Remote Network
Local Network
Authentication
Remote ID
Local ID
IKE
IPSec
Confirm
Remote ID
Adam3448-B
DynamicSpoke1
Internet
NetVanta 3448
VPN Peer
Local Network
Remote Network
Please enter the Remote ID type and value used by the VPN Peer (this is a unique identifier for the Remote Gateway).
Remote ID Type:
Domain Name
Please select the type of ID the VPN Peer will be using to authenticate themselves.
Remote ID Value:
DynamicSpoke1
This is the value of the Remote ID.
< Back
Next >
Exit
Done


http://10.19.252.19 - VPN Peer Config Wizard - Mozilla Firefox
Welcome
Wizard Type
VPN Peer Name
Public Interface
Peer Type
Remote Network
Local Network
Authentication
Remote ID
Local ID
IKE
IPSec
Confirm
Local ID
Adam3448-B
DynamicSpoke1
Internet
NetVanta 3448
VPN Peer
Local Network
Remote Network
Please enter the Local ID type and value that this NetVanta will use when connecting to the Remote Gateway.
Local ID Type:
IP Address
Please select a Local ID type to identify this NetVanta.
Local ID Value:
208.61.209.1
This is the value of the Local ID.
< Back
Next >
Exit
Done


http://10.19.252.19 - VPN Peer Config Wizard - Mozilla Firefox
Welcome
Wizard Type
VPN Peer Name
Public Interface
Peer Type
Remote Network
Local Network
Authentication
Remote ID
Local ID
IKE
IPSec
Confirm
IKE Settings
You are able to change the default settings for IKE used in this wizard using this form.
Initiate Using:
None (Responder Only Policy)
Respond Using:
Aggressive Mode
Hash Algorithm:
MD5
Encryption Algorithm:
3DES
Diffie Hellman Group:
1
IKE SA Lifetime:
28800
< Back
Next >
Exit
Done


http://10.19.252.19 - VPN Peer Config Wizard - Mozilla Firefox
Welcome
Wizard Type
VPN Peer Name
Public Interface
Peer Type
Remote Network
Local Network
Authentication
Remote ID
Local ID
IKE
IPSec
Confirm
IPSec Settings
Encryption protects the privacy of the data on your VPN tunnel between VPN Peers. Encryption makes it difficult, though not impossible, for others to eavesdrop on transferred data.
Encryption Algorithm:
ESP: 3 DES / MD5
Perfect Forward Secrecy:
Disabled
Lifetime in seconds:
28800
seconds
Lifetime in Kilobytes:
Kbytes
< Back
Next >
Exit
Done


http://10.19.252.19 - VPN Peer Config Wizard - Mozilla Firefox
Welcome
Wizard Type
VPN Peer Name
Public Interface
Peer Type
Remote Network
Local Network
Authentication
Remote ID
Local ID
IKE
IPSec
Confirm
Confirm Settings
Please review the settings that will be used in your new VPN Peer Policy. You may use "Back" to change any incorrect settings or "Finish" to add the new VPN Peer Policy.
Name: DynamicSpoke1
Gateway Address: Dynamic
Remote Network: 10.0.3.0/255.255.255.0
Local Network: 10.0.0.0/255.255.0.0
Remote Id: Domain: DynamicSpoke1
Local Id: IP: 208.61.209.1
Authentication Type: Preshared Secret
Ike Parameters: MD5, 3DES encryption, DH Group 1, 28800 seconds Lifetime, Respond Aggressive Mode
IPSec Parameters: ESP-3DES ESP-MD5-HMAC, No PFS, 28800 seconds Lifetime
< Back
Finish
Exit
Done

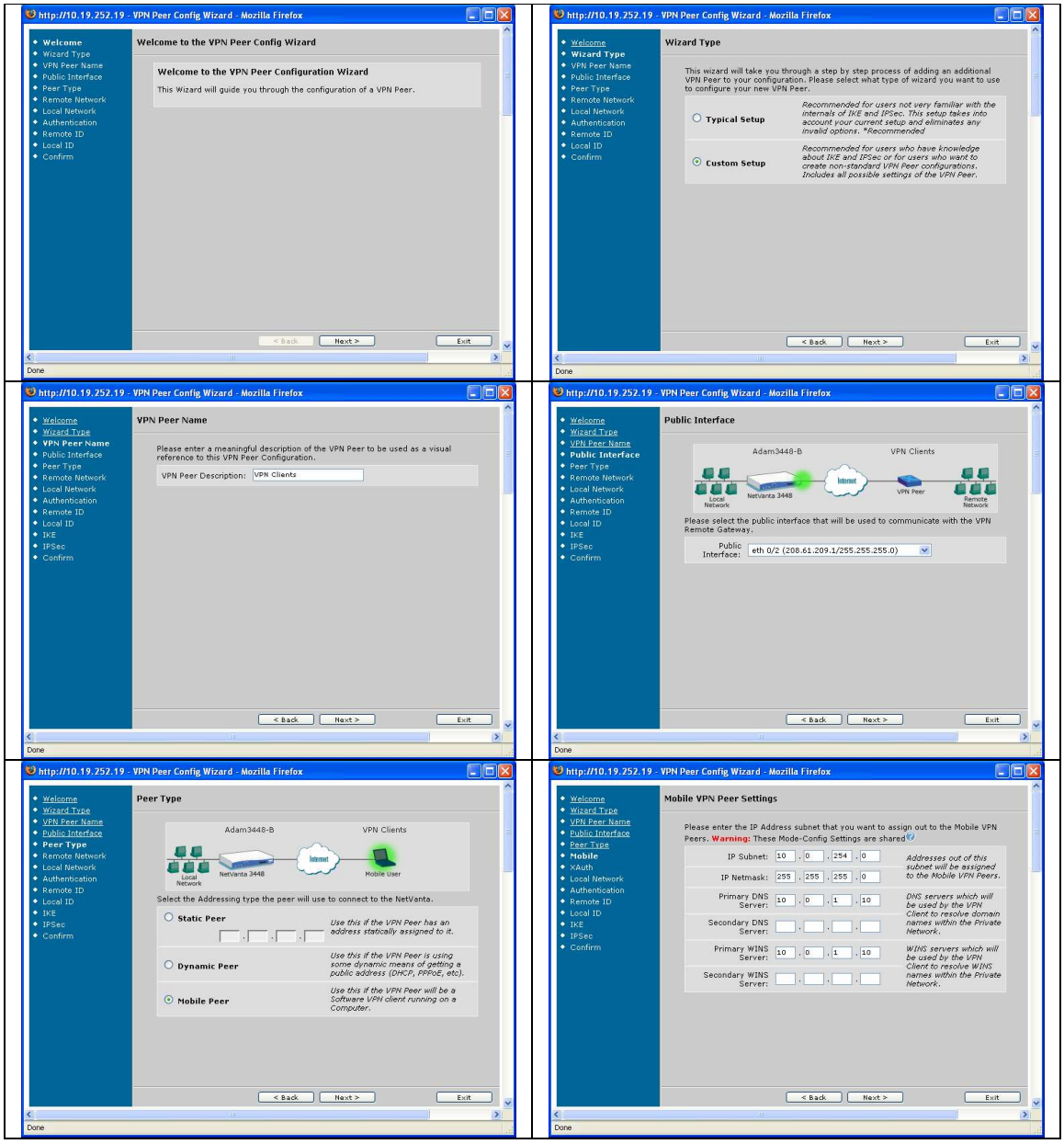
Scenario 3: Hub Configuration for VPN Clients

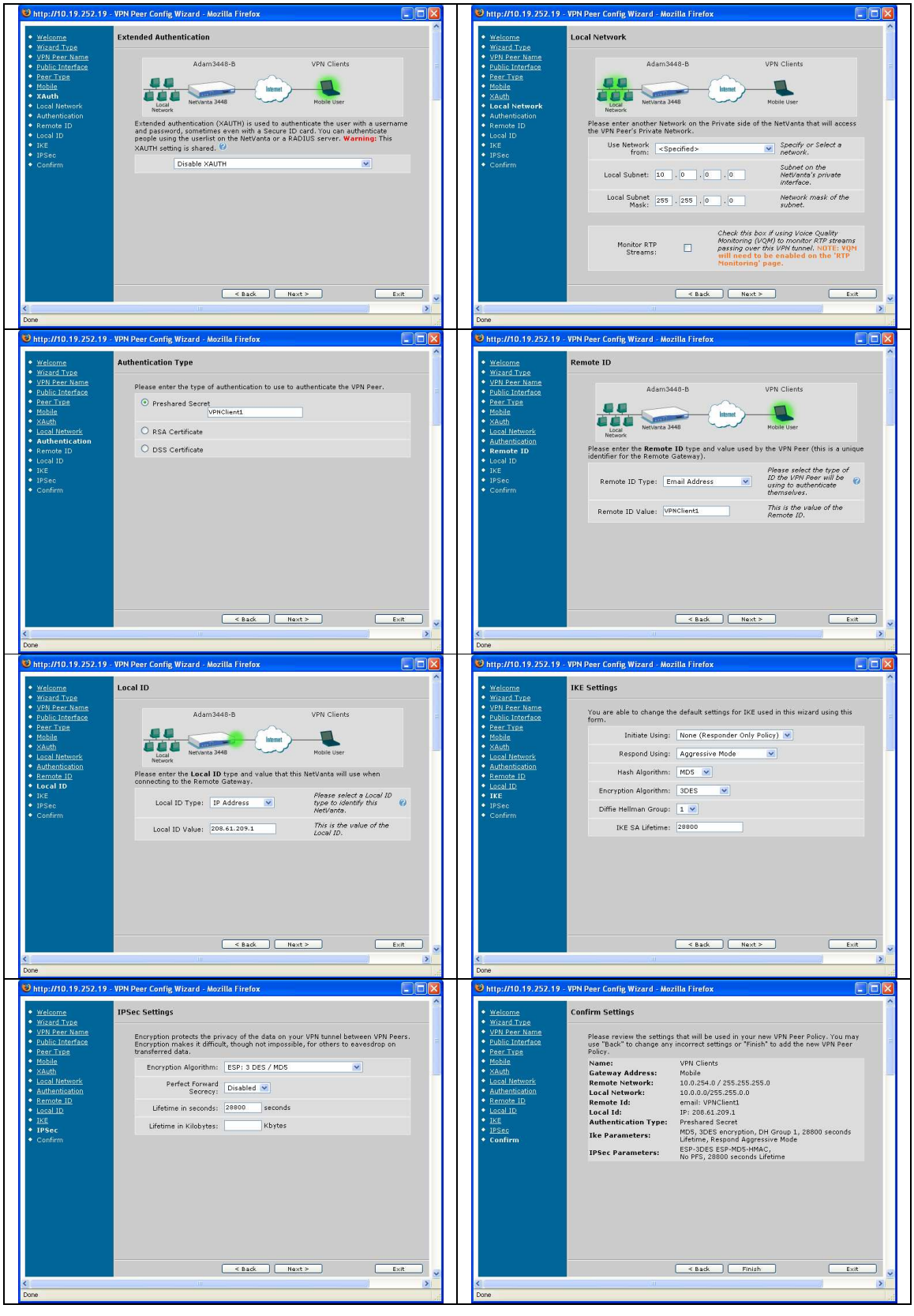
To setup a VPN Client through the CLI, the configuration will look similar to the example below. The VPN Client will share the same IKE policy as the dynamic Spokes. Additions in bold made to the IKE policy only affect the VPN Clients, because their use is controlled by the remote-ID statement:

- No-Mode-Config
  - Disables handing out of an IP from the Client Configuration Pool.
- No-Xauth
  - Disables prompting for an additional username & password. This function will not be covered in this article.

```
ip crypto

crypto ike client configuration pool “VPN Clients”
  ip-range              10.0.254.1   10.0.254.1
  dns-server            10.0.1.10
  netbios-name-server   10.0.1.10

crypto ike policy 1
  no initiate
  respond aggressive
  local-id address 208.61.209.1
  peer any
  client configuration pool “VPN Clients”
  attribute 1
    hash md5
    encryption 3des
    authentication pre-share
    group 1
    lifetime 28800

crypto ike remote-id user-fqdn VPNClient1 preshared-key VPNClient1 ike-
policy 1 crypto map VPN 254 no-xauth

crypto ipsec transform-set 3DES-MD5 esp-3des esp-md5-hmac
  mode tunnel

crypto map VPN 254
  match address VPN-254-Selectors
  set transform-set 3DES-MD5
  set security-association lifetime seconds 28800
  ike-policy 1
  mobile

ip access-list extended VPN-254-Selectors
  permit ip 10.0.0.0 0.0.255.255 10.0.254.0 0.0.0.255

interface ppp 1
  access-policy Public
  crypto map VPN
```

To setup a VPN Client through the GUI, the VPN wizard will be used, custom mode:




http://10.19.252.19 - VPN Peer Config Wizard - Mozilla Firefox
Welcome
Wizard Type
VPN Peer Name
Public Interface
Peer Type
Mobile
XAuth
Local Network
Authentication
Remote ID
Local ID
IKE
IPSec
Confirm
Extended Authentication
Adam3448-B
VPN Clients
Local Network
NetVanta 3448
Internet
Mobile User
Extended authentication (XAUTH) is used to authenticate the user with a username and password, sometimes even with a Secure ID card. You can authenticate people using the userlist on the NetVanta or a RADIUS server. Warning: This XAUTH setting is shared.
Disable XAUTH
< Back
Next >
Exit
Done
Local Network
Please enter another Network on the Private side of the NetVanta that will access the VPN Peer's Private Network.
Use Network from:
<Specified>
Specify or Select a network.
Local Subnet:
10 . 0 . 0 . 0
Subnet on the NetVanta's private interface.
Local Subnet Mask:
255 . 255 . 0 . 0
Network mask of the subnet.
Monitor RTP Streams:
Check this box if using Voice Quality Monitoring (VQM) to monitor RTP streams passing over this VPN tunnel. NOTE: VQM will need to be enabled on the 'RTP Monitoring' page.
Authentication Type
Please enter the type of authentication to use to authenticate the VPN Peer.
Preshared Secret
VPNClient1
RSA Certificate
DSS Certificate
Remote ID
Please enter the Remote ID type and value used by the VPN Peer (this is a unique identifier for the Remote Gateway).
Remote ID Type:
Email Address
Please select the type of ID the VPN Peer will be using to authenticate themselves.
Remote ID Value:
VPNClient1
This is the value of the Remote ID.
Local ID
Please enter the Local ID type and value that this NetVanta will use when connecting to the Remote Gateway.
Local ID Type:
IP Address
Please select a Local ID type to identify this NetVanta.
Local ID Value:
208.61.209.1
This is the value of the Local ID.
IKE Settings
You are able to change the default settings for IKE used in this wizard using this form.
Initiate Using:
None (Responder Only Policy)
Respond Using:
Aggressive Mode
Hash Algorithm:
MD5
Encryption Algorithm:
3DES
Diffie Hellman Group:
1
IKE SA Lifetime:
28800
IPSec Settings
Encryption protects the privacy of the data on your VPN tunnel between VPN Peers. Encryption makes it difficult, though not impossible, for others to eavesdrop on transferred data.
Encryption Algorithm:
ESP: 3 DES / MD5
Perfect Forward Secrecy:
Disabled
Lifetime in seconds:
28800
seconds
Lifetime in Kilobytes:
Kbytes
Confirm Settings
Please review the settings that will be used in your new VPN Peer Policy. You may use "Back" to change any incorrect settings or "Finish" to add the new VPN Peer Policy.
Name: VPN Clients
Gateway Address: Mobile
Remote Network: 10.0.254.0 / 255.255.255.0
Local Network: 10.0.0.0/255.255.0.0
Remote Id: email: VPNClient1
Local Id: IP: 208.61.209.1
Authentication Type: Preshared Secret
Ike Parameters: MD5, 3DES encryption, DH Group 1, 28800 seconds Lifetime, Respond Aggressive Mode
IPSec Parameters: ESP-3DES ESP-MD5-HMAC, No PFS, 28800 seconds Lifetime
Finish

Spoke Settings

The Spokes will be, in most cases, initiating the tunnel, as the reason for a VPN tunnel is usually for the remote sites to connect back to the main. The tunnels, once up, allow for the main site to connect to the remotes, if the need arises. The setup described in this document also allows for communication between Spokes through the Hub.

The Spoke's selector statement will specify the Spoke's local subnet as the source subnet, and the super-netted address as the destination subnet. Since the only router the Spoke will be connecting to is the Hub router, there will only be one VPN policy required.

Scenario 1: Spoke Configuration for a Static IP Spoke

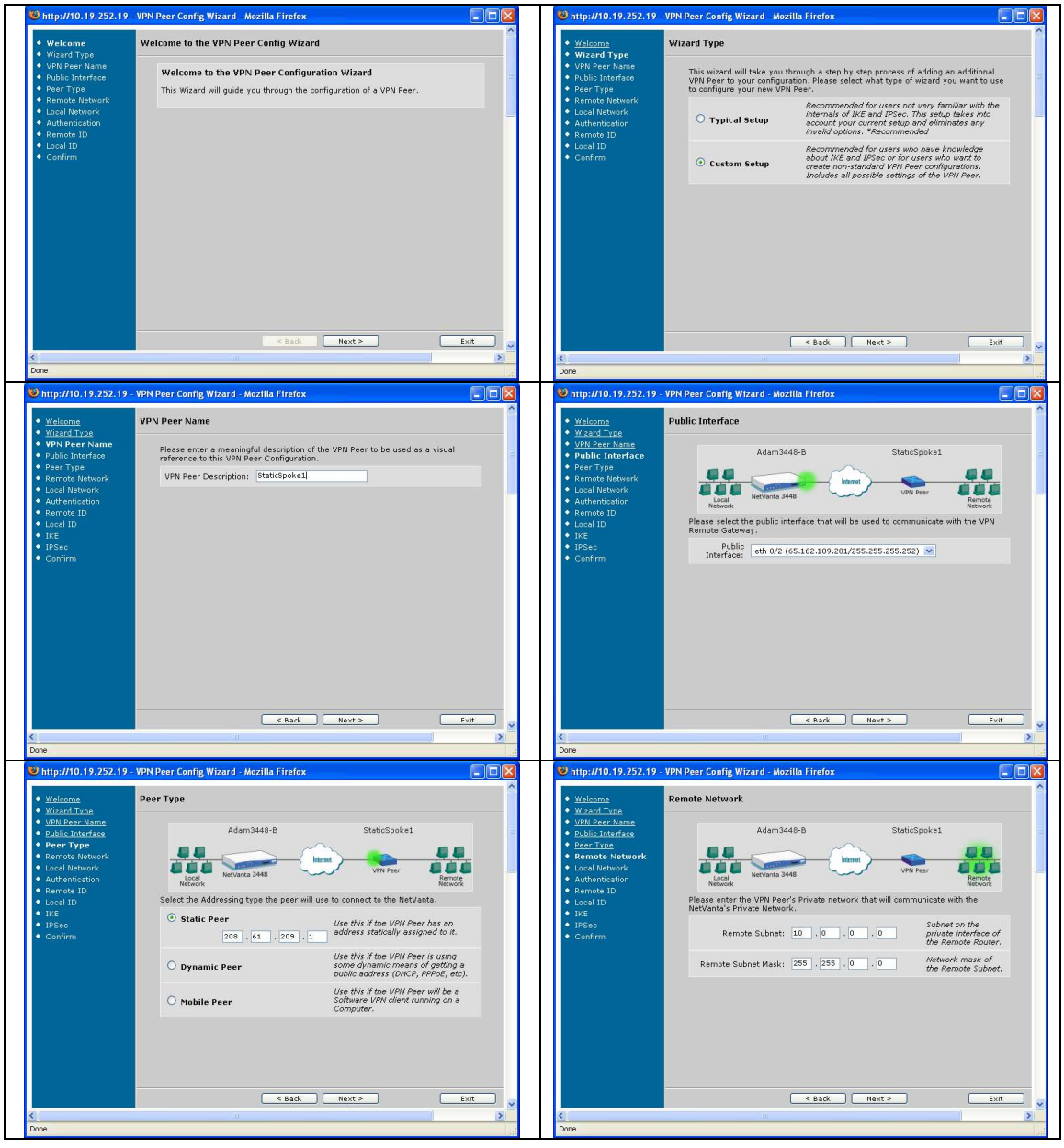
A static IP Spoke is the preferred solution for many reasons, but mainly for the reasons that Main mode is more secure than Aggressive mode, and that the Hub can initiate the connection to the Spoke, allowing for connection-on-demand.

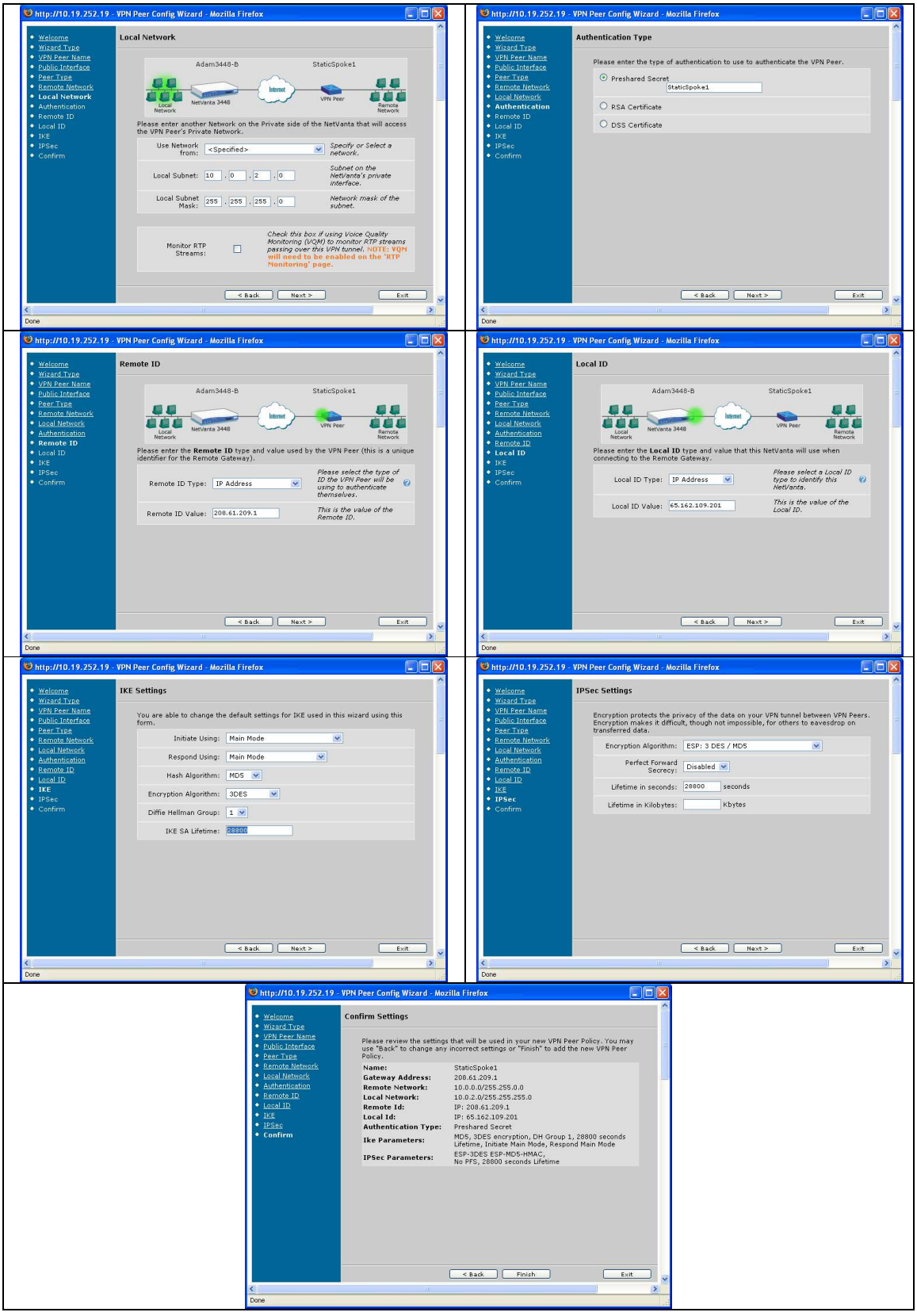
To setup a static IP Spoke through the CLI, the configuration will look similar to the example below:

```
ip crypto

crypto ike policy 2
  initiate main
  respond main
  local-id address 65.162.109.201
  peer 208.61.209.1
  attribute 1
    hash md5
    encryption 3des
    authentication pre-share
    group 1
    lifetime 28800

crypto ike remote-id address 208.61.209.1 preshared-key StaticSpoke1
ike-policy 2 crypto map VPN 2 no-mode-config no-xauth

crypto ipsec transform-set 3DES-MD5 esp-3des esp-md5-hmac
  mode tunnel

crypto map VPN 2
  match address VPN-2-Selectors
  set transform-set 3DES-MD5
  set security-association lifetime seconds 28800
  peer 208.61.209.1
  ike-policy 2

ip access-list extended VPN-2-Selectors
  permit ip 10.0.2.0 0.0.0.255 10.0.0.0 0.0.255.255
```

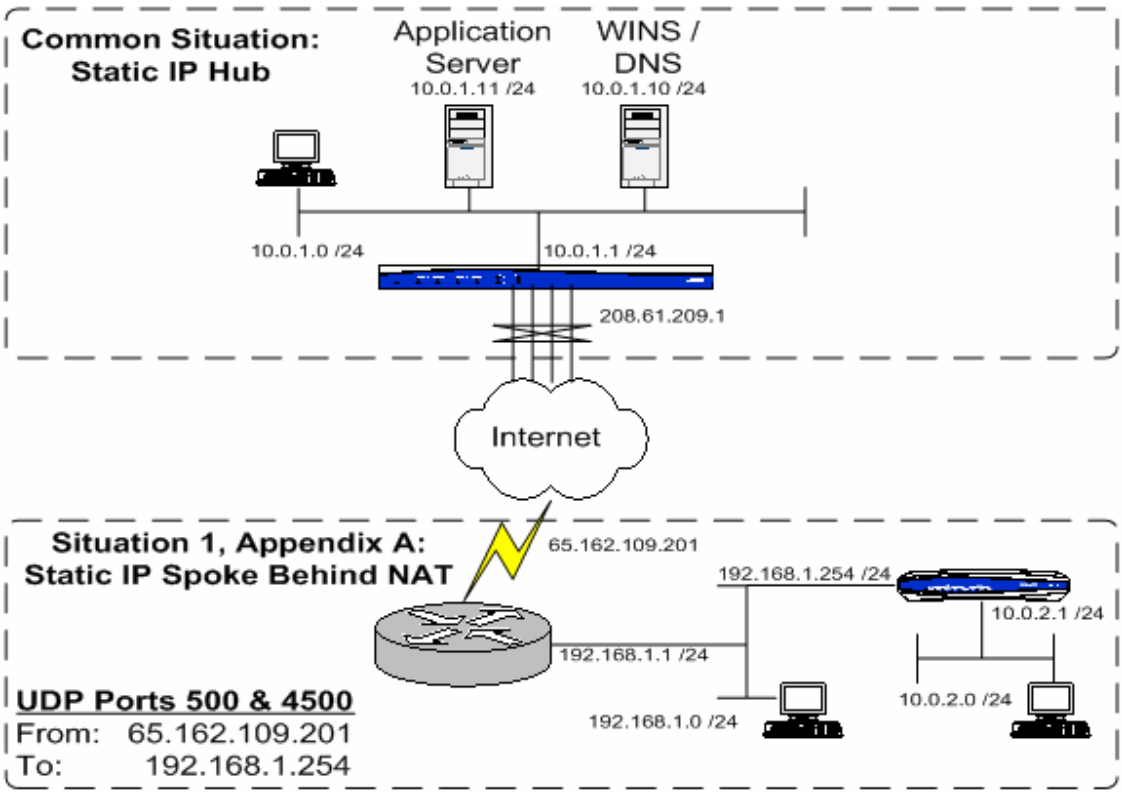
```
interface ppp 1
  access-policy Public
  crypto map VPN
```

To setup a static IP Spoke through the GUI, the VPN wizard will be used, custom mode:




http://10.19.252.19 - VPN Peer Config Wizard - Mozilla Firefox
Welcome
Wizard Type
VPN Peer Name
Public Interface
Peer Type
Remote Network
Local Network
Authentication
Remote ID
Local ID
IKE
IPSec
Confirm
Local Network
Adam3448-B
StaticSpoke1
Internet
NetVanta 3448
VPN Peer
Local Network
Remote Network
Please enter another Network on the Private side of the NetVanta that will access the VPN Peer's Private Network.
Use Network from:
<Specified>
Specify or Select a network.
Local Subnet:
10 . 0 . 2 . 0
Subnet on the NetVanta's private interface.
Local Subnet Mask:
255 . 255 . 255 . 0
Network mask of the subnet.
Monitor RTP Streams:
Check this box if using Voice Quality Monitoring (VQM) to monitor RTP streams passing over this VPN tunnel. NOTE: VQM will need to be enabled on the 'RTP Monitoring' page.
< Back
Next >
Exit
Done
Authentication Type
Please enter the type of authentication to use to authenticate the VPN Peer.
Preshared Secret
StaticSpoke1
RSA Certificate
DSS Certificate
Remote ID
Please enter the Remote ID type and value used by the VPN Peer (this is a unique identifier for the Remote Gateway).
Remote ID Type:
IP Address
Please select the type of ID the VPN Peer will be using to authenticate themselves.
Remote ID Value:
208.61.209.1
This is the value of the Remote ID.
Local ID
Please enter the Local ID type and value that this NetVanta will use when connecting to the Remote Gateway.
Local ID Type:
IP Address
Please select a Local ID type to identify this NetVanta.
Local ID Value:
65.162.109.201
This is the value of the Local ID.
IKE Settings
You are able to change the default settings for IKE used in this wizard using this form.
Initiate Using:
Main Mode
Respond Using:
Main Mode
Hash Algorithm:
MD5
Encryption Algorithm:
3DES
Diffie Hellman Group:
1
IKE SA Lifetime:
28800
IPSec Settings
Encryption protects the privacy of the data on your VPN tunnel between VPN Peers. Encryption makes it difficult, though not impossible, for others to eavesdrop on transferred data.
Encryption Algorithm:
ESP: 3 DES / MD5
Perfect Forward Secrecy:
Disabled
Lifetime in seconds:
28800
seconds
Lifetime in Kilobytes:
Kbytes
Confirm Settings
Please review the settings that will be used in your new VPN Peer Policy. You may use "Back" to change any incorrect settings or "Finish" to add the new VPN Peer Policy.
Name: StaticSpoke1
Gateway Address: 208.61.209.1
Remote Network: 10.0.0.0/255.255.0.0
Local Network: 10.0.2.0/255.255.255.0
Remote Id: IP: 208.61.209.1
Local Id: IP: 65.162.109.201
Authentication Type: Preshared Secret
Ike Parameters: MD5, 3DES encryption, DH Group 1, 28800 seconds Lifetime, Initiate Main Mode, Respond Main Mode
IPSec Parameters: ESP-3DES ESP-MD5-HMAC, No PFS, 28800 seconds Lifetime
Finish

Scenario 1, Appendix A: Spoke Configuration for a Spoke Behind NAT



When the VPN peer is behind a NAT process, special considerations must be made to allow for inbound, uninitiated VPN negotiations to occur properly. The Netvanta must be given a static or sticky IP address, and have ports UDP 500 and UDP 4500 forwarded to it from the NAT device. Devices on the subnet between the NAT device and the Netvanta will not be allowed to communicate through the tunnel, only devices behind the Netvanta.

If the Netvanta in question is running previous to 17.01 firmware, it will not be allowed to send the Public IP it is being NAT'd to as its Local-ID. This requires the Hub router be configured to accept the Private IP Local-ID that will have to be sent. In 17.01 firmware, any IP Address Local-ID can be sent, irregardless of whether or not the Netvanta is configured with that IP address. If this is not the preferred solution, Aggressive mode can be used to utilize non-IP Address IDs, while still preserving the ability for the Hub site to initiate the connection.

Note: If the hub does not have a need to initiate the connection, then this can be treated in the same manner as a dynamic IP Spoke, discussed in the next section.

The configuration and setup will be identical, unless Aggressive mode is being used.

Scenario 2: Spoke Configuration for a Dynamic IP Spoke

Static IP addresses are not always feasible or affordable, so dynamic IP spoke configuration is supported to allow for those situations. The downside is that these type of VPN configurations are slightly more susceptible to attacks, Denial of Service (DoS) in particular, because Aggressive mode is required and connections must be accepted from any IP address.

A dynamic IP Spoke will be configured the same way irregardless of whether or not a NAT process is taking place before reaching the Hub router. Since the Spokes will always be initiating the connection, the remotes must be connected before the Hub or any other Spoke can communicate with it.

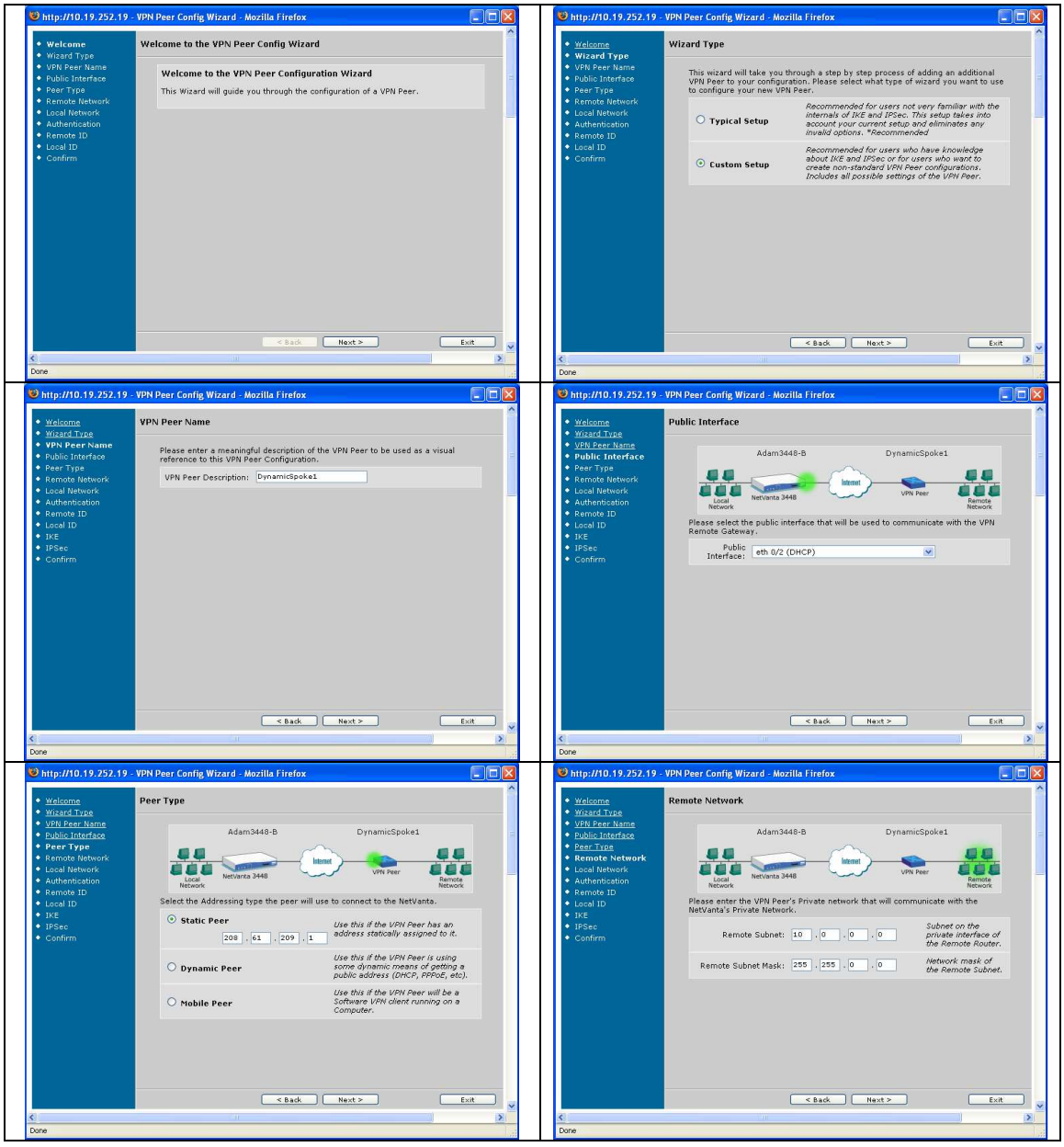
FQDN or Email Address Local-IDs are usually used in these cases, since the IP address cannot be known. Remember that there is no DNS or third-party lookup in this process. The IDs are strings of characters that must match both in type and value on both sides of the tunnel.

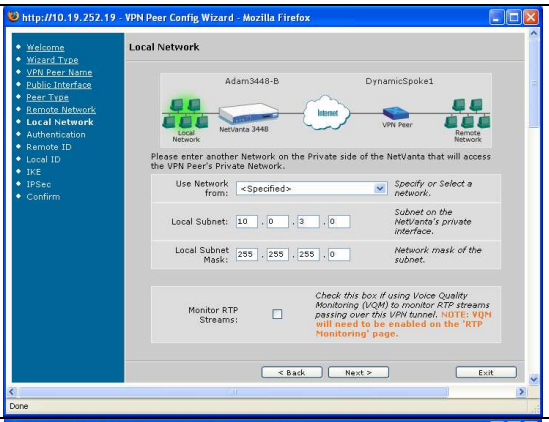
The configuration for a dynamic IP Spoke though the CLI will look similar to the example below:

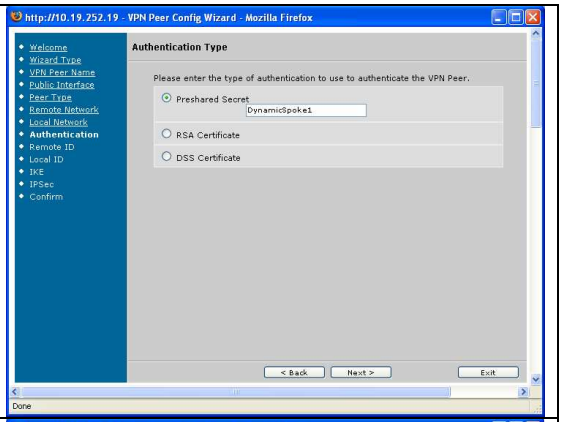
```
ip crypto

crypto ike policy 3
  initiate aggressive
  respond aggressive
  local-id fqdn DynamicSpoke1
  peer 208.61.209.1
  attribute 1
    hash md5
    encryption 3des
    authentication pre-share
    group 1
    lifetime 28800

crypto ike remote-id address 208.61.209.1 preshared-key StaticSpoke1
ike-policy 3 crypto map VPN 3 no-mode-config no-xauth

crypto ipsec transform-set 3DES-MD5 esp-3des esp-md5-hmac
  mode tunnel

crypto map VPN 3
  match address VPN-3-Selectors
  set transform-set 3DES-MD5
  set security-association lifetime seconds 28800
  peer 208.61.209.1
  ike-policy 3

ip access-list extended VPN-3-Selectors
  permit ip 10.0.3.0 0.0.0.255 10.0.0.0 0.0.255.255
```

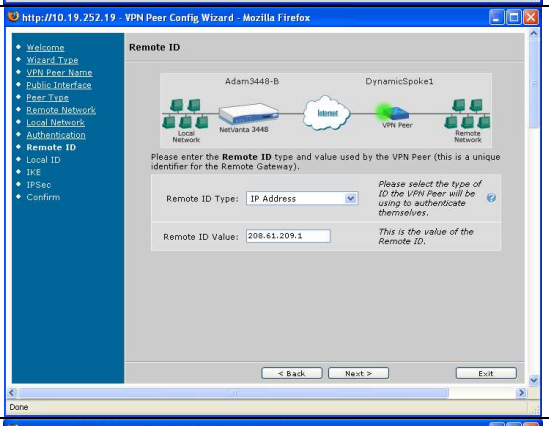
```
interface ppp 1
  access-policy Public
  crypto map VPN
```

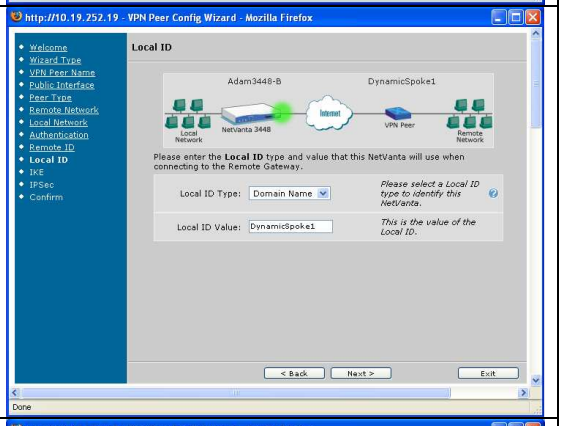
To setup a dynamic IP Spoke through the GUI, the VPN wizard will be used, custom mode:

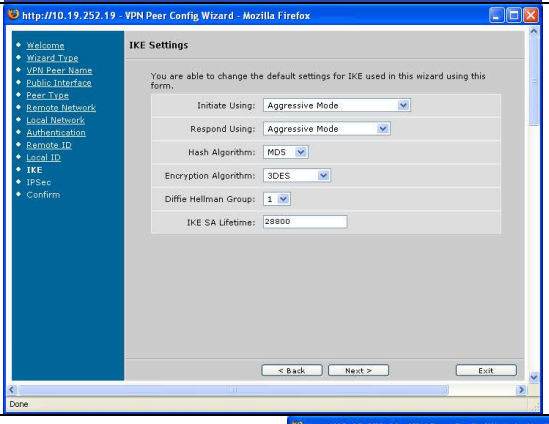


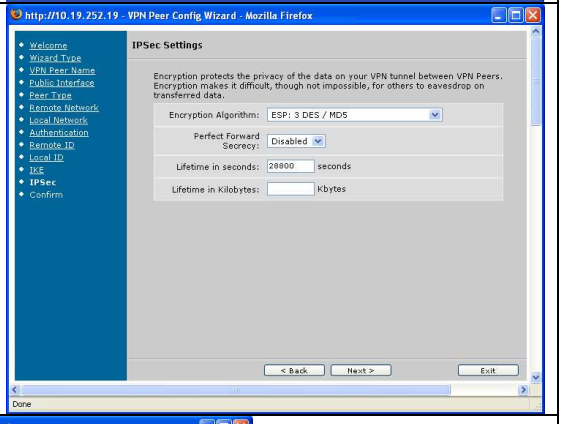

http://10.19.252.19 - VPN Peer Config Wizard - Mozilla Firefox
Welcome
Wizard Type
VPN Peer Name
Public Interface
Peer Type
Remote Network
Local Network
Authentication
Remote ID
Local ID
IKE
IPSec
Confirm
Local Network
Adam3448-B
DynamicSpoke1
Internet
NetVanta 3448
VPN Peer
Local Network
Remote Network
Please enter another Network on the Private side of the NetVanta that will access the VPN Peer's Private Network.
Use Network from:
<Specified>
Specify or Select a network.
Local Subnet:
10 . 0 . 3 . 0
Subnet on the NetVanta's private interface.
Local Subnet Mask:
255 . 255 . 255 . 0
Network mask of the subnet.
Monitor RTP Streams:
Check this box if using Voice Quality Monitoring (VQM) to monitor RTP streams passing over this VPN tunnel. NOTE: VQM will need to be enabled on the 'RTP Monitoring' page.
< Back
Next >
Exit
Done

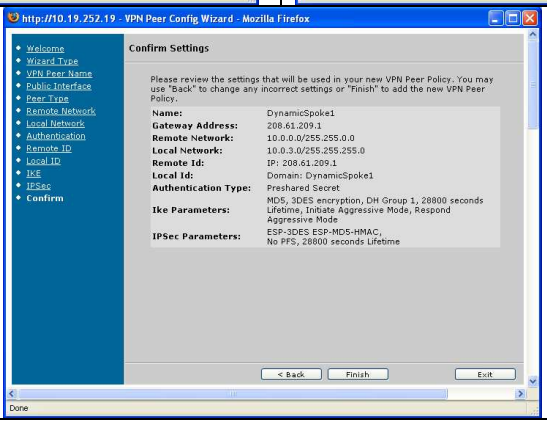

http://10.19.252.19 - VPN Peer Config Wizard - Mozilla Firefox
Welcome
Wizard Type
VPN Peer Name
Public Interface
Peer Type
Remote Network
Local Network
Authentication
Remote ID
Local ID
IKE
IPSec
Confirm
Authentication Type
Please enter the type of authentication to use to authenticate the VPN Peer.
Preshared Secret
DynamicSpoke1
RSA Certificate
DSS Certificate
< Back
Next >
Exit
Done


http://10.19.252.19 - VPN Peer Config Wizard - Mozilla Firefox
Welcome
Wizard Type
VPN Peer Name
Public Interface
Peer Type
Remote Network
Local Network
Authentication
Remote ID
Local ID
IKE
IPSec
Confirm
Remote ID
Adam3448-B
DynamicSpoke1
Internet
NetVanta 3448
VPN Peer
Local Network
Remote Network
Please enter the Remote ID type and value used by the VPN Peer (this is a unique identifier for the Remote Gateway).
Remote ID Type:
IP Address
Please select the type of ID the VPN Peer will be using to authenticate themselves.
Remote ID Value:
208.61.209.1
This is the value of the Remote ID.
< Back
Next >
Exit
Done


http://10.19.252.19 - VPN Peer Config Wizard - Mozilla Firefox
Welcome
Wizard Type
VPN Peer Name
Public Interface
Peer Type
Remote Network
Local Network
Authentication
Remote ID
Local ID
IKE
IPSec
Confirm
Local ID
Adam3448-B
DynamicSpoke1
Internet
NetVanta 3448
VPN Peer
Local Network
Remote Network
Please enter the Local ID type and value that this NetVanta will use when connecting to the Remote Gateway.
Local ID Type:
Domain Name
Please select a Local ID type to identify this NetVanta.
Local ID Value:
DynamicSpoke1
This is the value of the Local ID.
< Back
Next >
Exit
Done

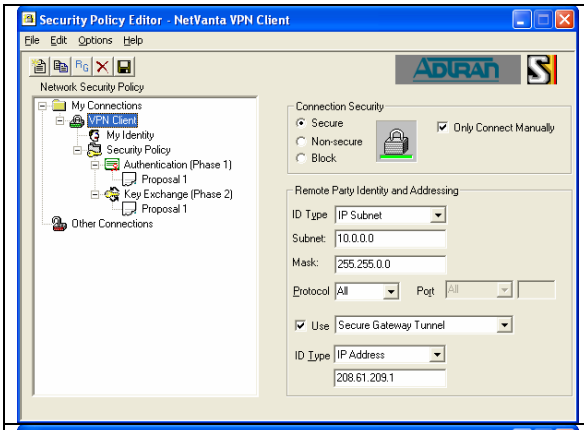

http://10.19.252.19 - VPN Peer Config Wizard - Mozilla Firefox
Welcome
Wizard Type
VPN Peer Name
Public Interface
Peer Type
Remote Network
Local Network
Authentication
Remote ID
Local ID
IKE
IPSec
Confirm
IKE Settings
You are able to change the default settings for IKE used in this wizard using this form.
Initiate Using:
Aggressive Mode
Respond Using:
Aggressive Mode
Hash Algorithm:
MD5
Encryption Algorithm:
3DES
Diffie Hellman Group:
1
IKE SA Lifetime:
28800
< Back
Next >
Exit
Done


http://10.19.252.19 - VPN Peer Config Wizard - Mozilla Firefox
Welcome
Wizard Type
VPN Peer Name
Public Interface
Peer Type
Remote Network
Local Network
Authentication
Remote ID
Local ID
IKE
IPSec
Confirm
IPSec Settings
Encryption protects the privacy of the data on your VPN tunnel between VPN Peers. Encryption makes it difficult, though not impossible, for others to eavesdrop on transferred data.
Encryption Algorithm:
ESP: 3 DES / MD5
Perfect Forward Secrecy:
Disabled
Lifetime in seconds:
28800
seconds
Lifetime in Kilobytes:
Kbytes
< Back
Next >
Exit
Done

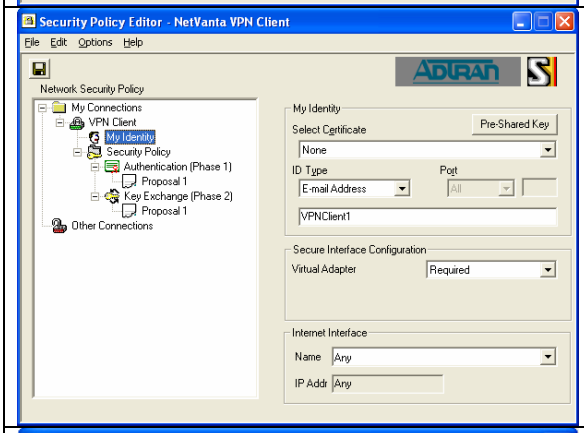

http://10.19.252.19 - VPN Peer Config Wizard - Mozilla Firefox
Welcome
Wizard Type
VPN Peer Name
Public Interface
Peer Type
Remote Network
Local Network
Authentication
Remote ID
Local ID
IKE
IPSec
Confirm
Confirm Settings
Please review the settings that will be used in your new VPN Peer Policy. You may use "Back" to change any incorrect settings or "Finish" to add the new VPN Peer Policy.
Name: DynamicSpoke1
Gateway Address: 208.61.209.1
Remote Network: 10.0.0.0/255.255.0.0
Local Network: 10.0.3.0/255.255.255.0
Remote Id: IP: 208.61.209.1
Local Id: Domain: DynamicSpoke1
Authentication Type: Preshared Secret
Ike Parameters: MD5, 3DES encryption, DH Group 1, 28800 seconds Lifetime, Initiate Aggressive Mode, Respond Aggressive Mode
IPSec Parameters: ESP-3DES ESP-MD5-HMAC, No PFS, 28800 seconds Lifetime
< Back
Finish
Exit
Done

Scenario 3: Netvanta VPN Client Configuration for VPN Clients

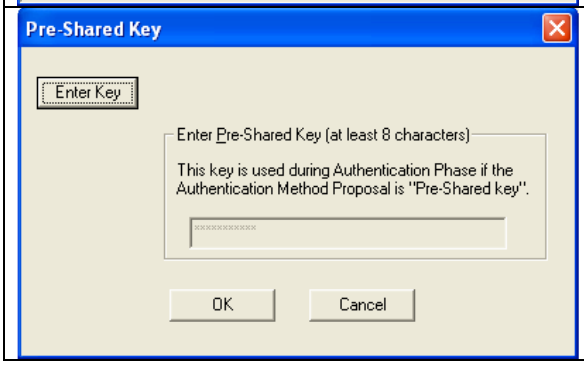
VPN client connections allow for mobile or home users without a hardware VPN unit to connect to the VPN network from a single computer anywhere on the Internet. This guide will cover the configuration of the Netvanta VPN Client for use with the example scenario.



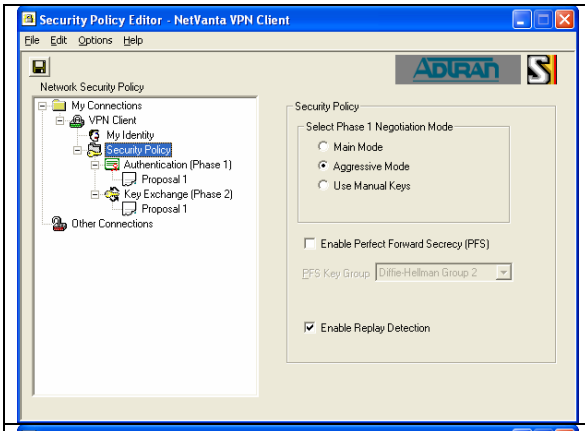
1. **Specify the Remote Subnet.**
   a. This is the network the client is connecting to.
2. **Specify the Security Gateway.**
   a. This is the IP address of the router the client is connecting to.



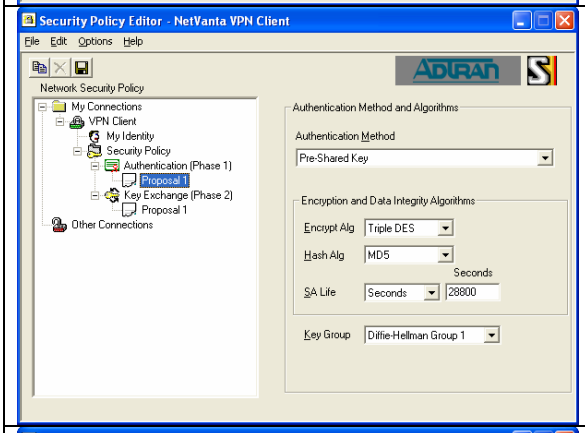
3. **Specify the ID Type.**
4. **Specify the ID Value.**
5. **Set the Virtual Adapter to 'Preferred' or 'Required'.**
   a. The Virtual Adapter is where the address the router hands out will be installed.
6. **Set the Internet Interface to 'Any'.**



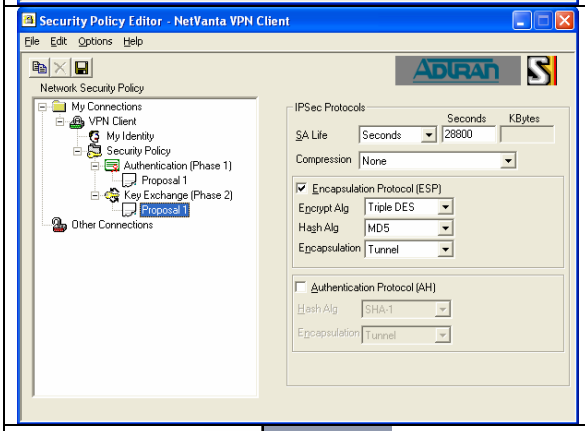
7. **Enter the Pre-Shared Key.**
   a. The key must be at least eight (8) characters.



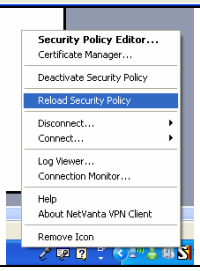
8. **Set the Negotiation Mode to 'Aggressive'.**
9. **Enable Perfect Forward Secrecy (Optional).**
   a. Not used in this scenario.



10. **Set the Authentication Method to 'Pre-Shared Key'.**
11. **Specify the Encryption.**
12. **Specify the Hashing.**
13. **Specify the Lifetime value.**
14. **Specify the Key Group.**



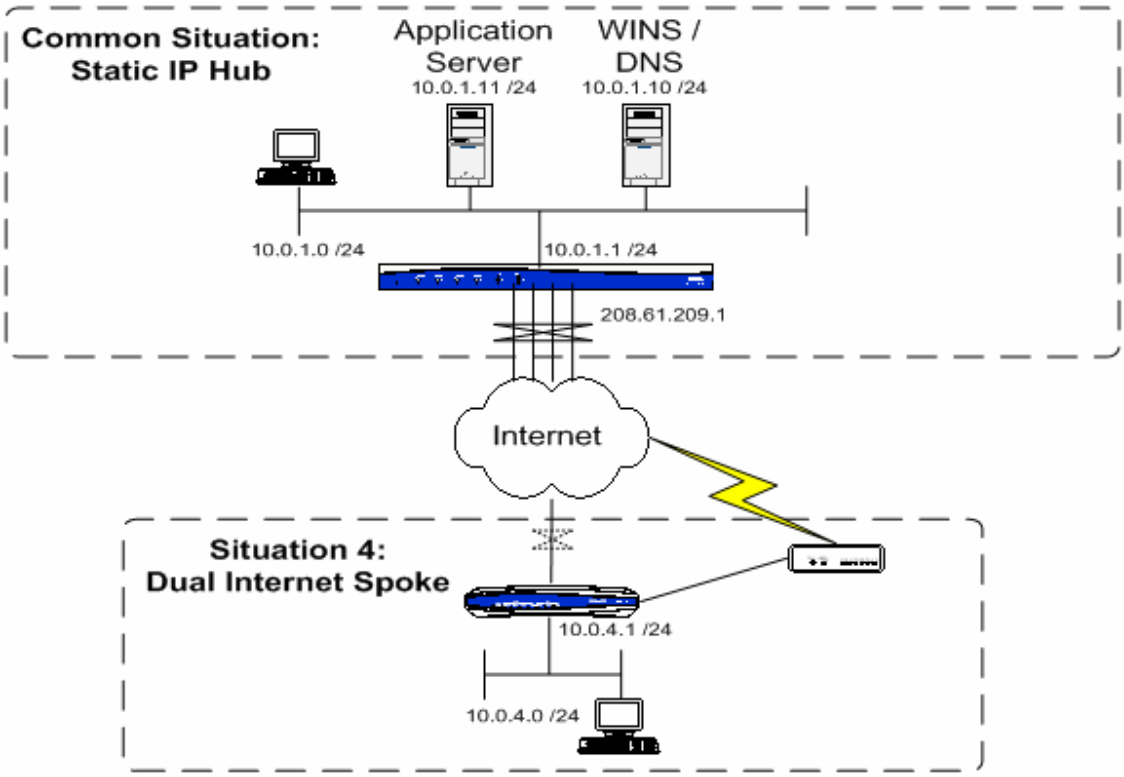
15. **Specify the Lifetime Type and Value.**
    a. Can be specified in seconds, kilobytes or both.
    b. Recommended to use seconds or both. Kilobytes alone are not recommended.
16. **Specify the Encryption.**
17. **Specify the Hashing.**
18. **Set the Encapsulation Mode to 'Tunnel'.**



19. **Save the Policy.**
20. **Reload the Policy Editor.**

Scenario 4: Spoke Configuration for a Dual Internet Spoke

(Fail-Over, not Load-Sharing)



Spokes that possess multiple Internet connections for a fail-over scenario will be treated as a dynamic Spoke. This document will only cover the VPN-related configuration. To learn how to setup the Internet & routing failover, refer to KB article #2311.

There is also another, more complicated, configuration that explains how to create a Main mode tunnel fail-over scenario, allowing for the Hub site to connect to the Spoke site, assuming that all the connections involved have static IPs. This configuration is described in KB article #2306.

All of the configuration for this setup must be done from the CLI, and only consists of two lines of configuration changes:

1. Crypto Fast-Failover must be enabled.
    a. This allows the router to tear down any existing tunnels that may be currently up using the primary connection when a default route change is detected. This forces the tunnel to re-negotiate using the backup connection.
2. The Crypto Map must be applied to both the primary & backup WAN interfaces.
    a. A VPN can only be initiated or received on an interface with a crypto map applied. The routing engine will control which Crypto Map is used based upon which interface the default route is pointing out.

The configuration for a dual Internet connection Spoke though the CLI will look similar to the example below. The changes that need to be made through the CLI are in bold.

```
ip crypto
ip crypto fast-failover

crypto ike policy 4
  initiate aggressive
  respond aggressive
  local-id fqdn DualInternetSpoke1
  peer 208.61.209.1
  attribute 1
    hash md5
    encryption 3des
    authentication pre-share
    group 1
    lifetime 28800

crypto ike remote-id address 208.61.209.1 preshared-key
DualInternetSpoke1 ike-policy 4 crypto map VPN 4 no-mode-config no-
xauth

crypto ipsec transform-set 3DES-MD5 esp-3des esp-md5-hmac
  mode tunnel

crypto map VPN 4
  match address VPN-4-Selectors
  set transform-set 3DES-MD5
  set security-association lifetime seconds 28800
  peer 208.61.209.1
  ike-policy 4

ip access-list extended VPN-4-Selectors
  permit ip 10.0.4.0 0.0.0.255 10.0.0.0 0.0.255.255

interface ppp 1
  access-policy Public
  crypto map VPN

interface eth 0/1
  access-policy Public-Backup
  crypto map VPN
```

Addendum

Firewall Settings

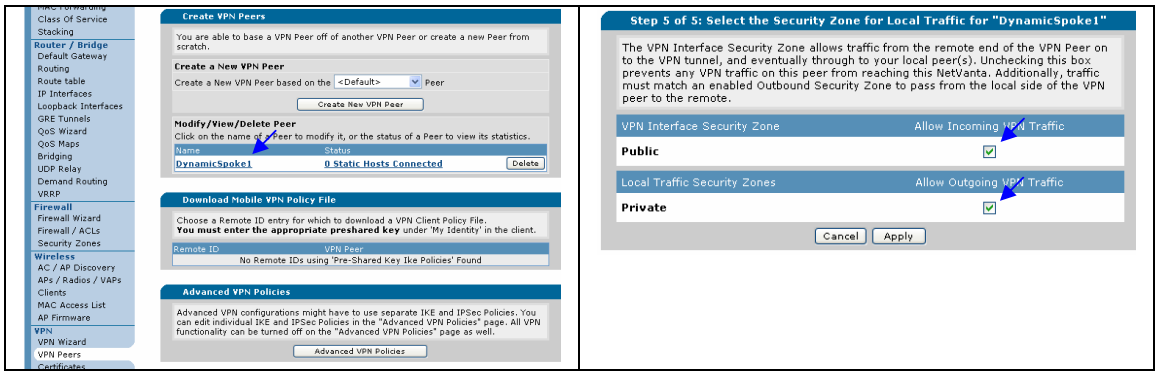
The firewall, if being used, must have the appropriate statements to allow traffic through the firewall. In most cases, the VPN selector statements can be referenced.

If the Netvanta in question is running 12.01 firmware or later, the ‘stateless’ keyword should be used. Stateless processing bypasses virtually all of the firewall checks, so that the VPN traffic is allowed through the router with the lowest possibility of being blocked.

A configuration in this manner would look similar to the following:

```
interface ppp 1
  access-policy Public
  crypto map VPN

interface eth 0/1
  access-policy Private

ip access-list extended VPN-2-Selectors
  permit ip 10.0.2.0 0.0.0.255 10.0.0.0 0.0.255.255

ip policy-class Public
  allow reverse list VPN-2-Selectors stateless
  <Admin Access>

ip policy-class Private
  allow list VPN-2-Selectors stateless
  <Admin Access>
  <NAT to Internet>
```

This can also be setup in the GUI, using the VPN Peers page:



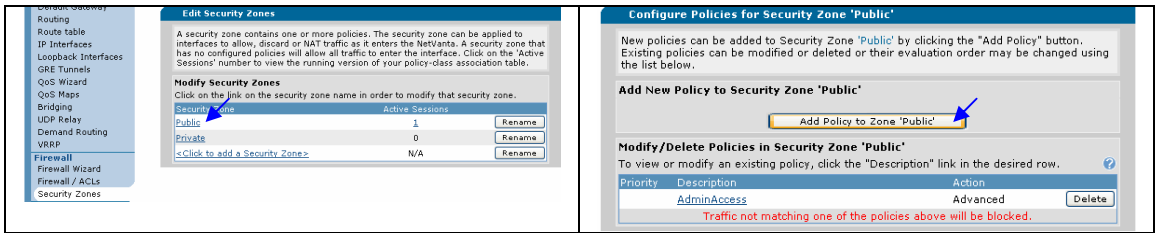
This type of firewall setup works for every Spoke. However, when the router has numerous VPN tunnels, there would be a firewall entry in each policy-class (Security Zone in GUI terminology) for each tunnel.

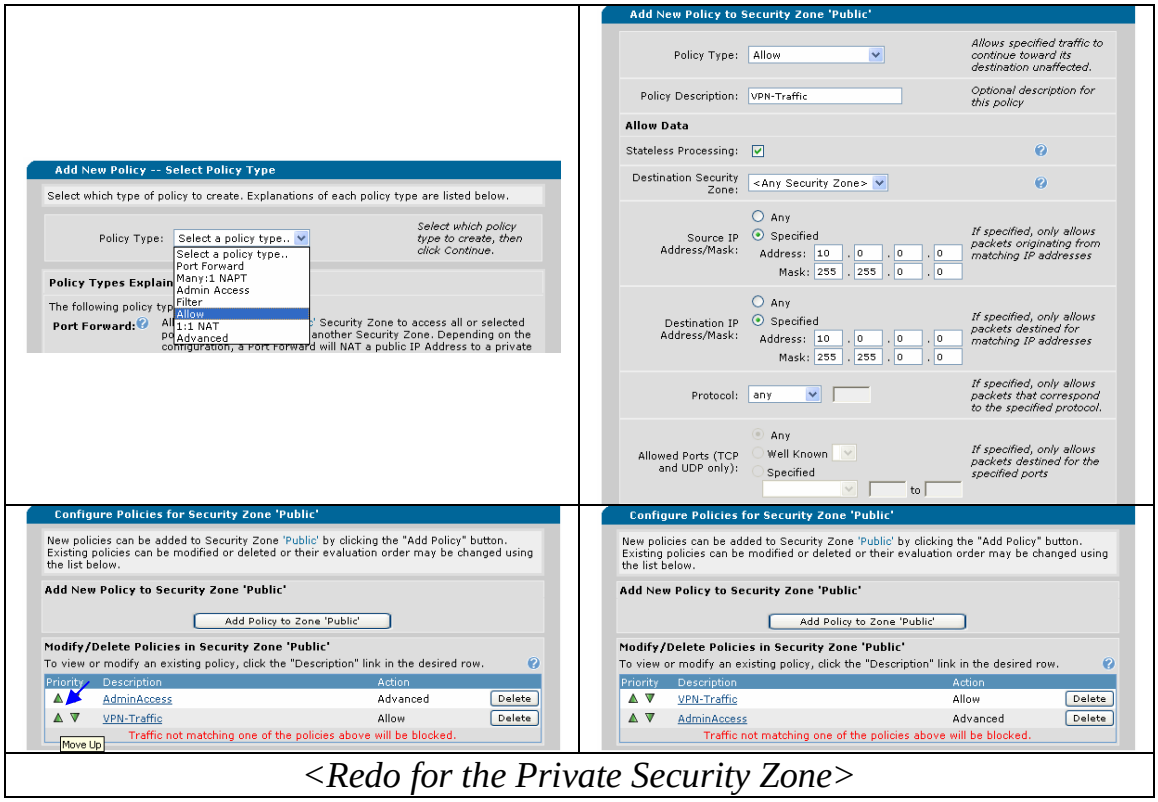
In the Hub configuration, the firewall will make use of the super-netted address used to select all private subnets at once. This will allow all VPN traffic to be selected with a single firewall policy.

A configuration in this manner would look similar to the following:

```
interface ppp 1
  access-policy Public
  crypto map VPN

interface eth 0/1
  access-policy Private

ip access-list extended VPN-Traffic
  permit ip 10.0.0.0 0.0.255.255 10.0.0.0 0.0.255.255

ip policy-class Public
  allow list VPN-Traffic stateless
  <Admin Access>

ip policy-class Private
  allow list VPN-Traffic stateless
  <Admin Access>
  <NAT to Internet>
```

This can also be setup in the GUI, using the VPN Peers page:





<Redo for the Private Security Zone>

VPN Keep-Alive

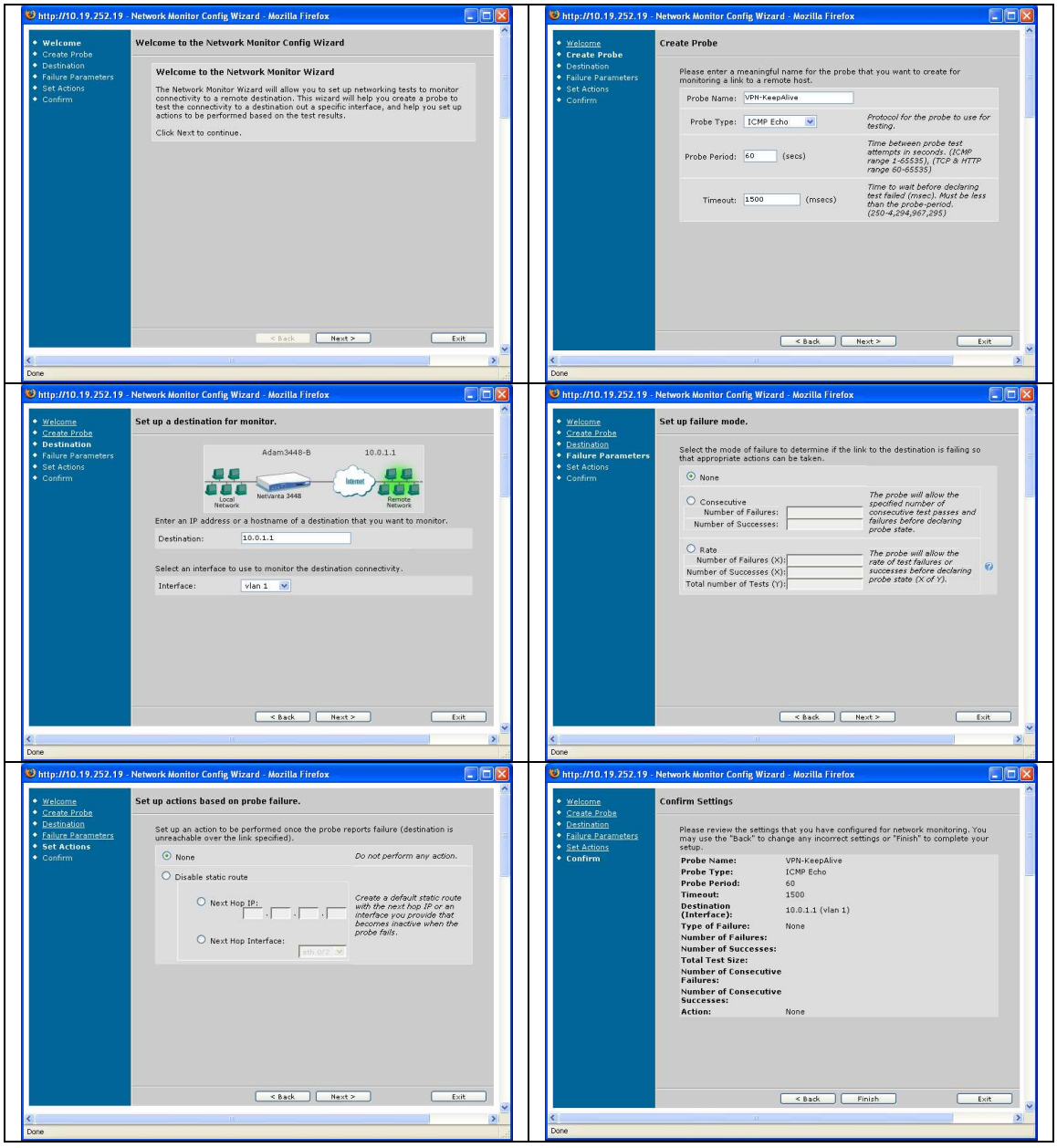
Note: This functionality requires the Netvanta in question to support Network Monitor and run at least 13.1 firmware.

This setting is optional, but necessary if the main site must be able to reach a remote site that it cannot initiate a VPN connection to. This will be setup on the initiating side. By creating a probe that matches the selector statement, 'interesting' traffic is always created at specified intervals. A sample CLI configuration is shown here:

```
probe VPN-KeepAlive icmp-echo
destination <Router's LAN IP Address>
source-address <Peer Router's LAN IP Address>
period 60
no shutdown
```

In this case, the keep-alive is sent every 60 seconds. The interval is user-definable and should be set according to your site's needs. It only needs to create traffic at a rate faster than the lifetime of the VPN tunnel. However, if a tunnel should drop for any reason, it should be set to the amount of time the remote site can be 'down' from any connection initiations from the main site.

This can also be setup in the GUI using the Network Monitor Wizard:


http://10.19.252.19 - Network Monitor Config Wizard - Mozilla Firefox
Welcome
Create Probe
Destination
Failure Parameters
Set Actions
Confirm
Welcome to the Network Monitor Config Wizard
Welcome to the Network Monitor Wizard
The Network Monitor Wizard will allow you to set up networking tests to monitor connectivity to a remote destination. This wizard will help you create a probe to test the connectivity to a destination out a specific interface, and help you set up actions to be performed based on the test results.
Click Next to continue.
< Back
Next >
Exit
Done
Create Probe
Please enter a meaningful name for the probe that you want to create for monitoring a link to a remote host.
Probe Name: VPN-KeepAlive
Probe Type: ICMP Echo
Protocol for the probe to use for testing.
Probe Period: 60 (secs)
Time between probe test attempts in seconds. (ICMP range 1-65535), (TCP & HTTP range 60-65535)
Timeout: 1500 (msecs)
Time to wait before declaring test failed (msec). Must be less than the probe-period. (250-4,294,967,295)
Set up a destination for monitor.
Adam3448-B
10.0.1.1
Internet
Local Network
NetVanta 3448
Remote Network
Enter an IP address or a hostname of a destination that you want to monitor.
Destination: 10.0.1.1
Select an interface to use to monitor the destination connectivity.
Interface: vlan 1
Set up failure mode.
Select the mode of failure to determine if the link to the destination is failing so that appropriate actions can be taken.
None
Consecutive
Number of Failures:
Number of Successes:
The probe will allow the specified number of consecutive test passes and failures before declaring probe state.
Rate
Number of Failures (X):
Number of Successes (X):
Total number of Tests (Y):
The probe will allow the rate of test failures or successes before declaring probe state (X of Y).
Set up actions based on probe failure.
Set up an action to be performed once the probe reports failure (destination is unreachable over the link specified).
None
Do not perform any action.
Disable static route
Next Hop IP:
Next Hop Interface:
Create a default static route with the next hop IP or an interface you provide that becomes inactive when the probe fails.
Confirm Settings
Please review the settings that you have configured for network monitoring. You may use the "Back" to change any incorrect settings or "Finish" to complete your setup.
Probe Name: VPN-KeepAlive
Probe Type: ICMP Echo
Probe Period: 60
Timeout: 1500
Destination (Interface): 10.0.1.1 (vlan 1)
Type of Failure: None
Number of Failures:
Number of Successes:
Total Test Size:
Number of Consecutive Failures:
Number of Consecutive Successes:
Action: None
Finish