

VPN Support on Comet

Supported Features

The VPN client on the Comet is a standards based IPsec VPN client compliant with RFC 2406 for encryption and authentication; RFCs 2407, 2408, 2409, 4109 for key generation and maintenance; RFC's 3947 and 3948 for connection behind NAT devices. Allowing connection to most VPN gateways.

IP Encapsulating Security Payload (ESP) with authentication provide encryption and authentication services, ensuring confidentiality and integrity of data. Confidentiality is provided by a set of encryption algorithms including Null encryption, DES, 3DES, AES 128, AES 192 and AES 256. Integrity/authentication is provided by MD5, SHA-1 and SHA-2¹. Encryption and authentication keys can either be provided as static pre-shared keys or dynamic keys negotiated via Internet Key Exchange (IKE).

Under IKE, Main Mode (also called Identity Protection Mode) and Aggressive Mode are supported for the generation of ISAKMP Security Associations during Phase 1 negotiations. After Phase 1 a pair of encryption and authentication (excluding Null) algorithms are selected to protect Phase 2 of the negotiation. Phase 2 is conducted using Quick Mode resulting in a pair of IKE Security Associations between the VPN peers, detailing encryption, authentication algorithms and keys for the IP ESP traffic. Part of the negotiation includes defining lifetimes of both the ISAKMP and IKE Security Associations, the Comet VPN client will re-negotiate both types of Security Associations before they expire, ensuring continuous connection to the VPN.

Perfect Forward Secrecy (PFS) is provided using Diffie-Hellman groups 1 and 2² as the source of the key material. PFS ensures that if the keys established in Phase 1 are compromised, the security of the data protected by the Phase 2 keys, the ESP traffic, is not effected.

Dynamic IP Address assignment is supported using Mode Config. XAuth is an extension of Mode Config and will be used to further authenticate the user if it is required by the VPN peer. Presently, only simple user and password verification is supported, any prompting will take place after Phase 1 and before Phase 2. Should any Phase 1 re-keying take place and the other IKE peer request user and password, the Comet VPN client will again prompt for user and password.

Connection of a VPN enabled Comet behind a NAT is supported with NAT Traversal (NAT-T). The presence of the NAT is automatically detected by the VPN client and the use of NAT-T is completely transparent.

Both Transport and Tunnel Mode ESP connections are supported. The most commonly used is Tunnel Mode and is required when ESP is implemented in a secure gateway.

Preparing for Configuration

Before commencing with any configuration some preparatory work is required. The following may be needed:

- Determine whether static keys or IKE is to be used. For static keys you will need the inbound and outbound pre-shared keys for the encryption and authentication algorithms. You will also need to determine which algorithms are to be used.

1 Null, DES and MD5 algorithms are considered “weak” and are not proposed by default.

2 Diffie-Hellman group 1 is considered “weak” and is not proposed by default.

- Is the Comet likely to be behind a NAT? This is not directly configured but some of the configuration options are affected by this. Specifically, the use of Main Mode and Identification via IP Address is not supported with a NAT router. Aggressive mode must be configured when behind a NAT.
- Determine which method of identification is to be used, for example Key Identifier or Email Address and gather the relevant Id values.
- Determine the pre-shared secret relevant to the identifier previously chosen. Pre-shared secret is the only method of authentication supported.
- Is the connection via a VPN gateway? Then it will be connected in Tunnel Mode. The IP address of the VPN gateway is required, and if dynamic IP assignment is not used then the fixed IP address of the Comet is required.
- Is the user to be separately verified using XAuth?
- Is Aggressive mode to be used during Phase 1? If so, the encryption algorithm, authentication algorithm and PFS (Perfect Forward Secrecy) Group need to be determined. If any of the encryption or authentication algorithms are considered weak, then weak algorithms will need to be enabled during the configuration process.

Configuring Comet for IKE/IPsec

The following is a run down of the questions asked by the the IPsec configuration wizard. To navigate forward through the wizard simply answer the question and the wizard will guide you through the configuration steps. To correct a mistake or go back to a previous question, press the **ESC** key. Any previous configuration information will be displayed, with the exception of the pre-shared key. Dependent on previous answers, some questions may be skipped.

- Access the *Main* menu by pressing **Stop-M**.
- From the *Main* menu access the *Security* menu.
- From the *Security* menu access the *IPSec* menu.
- To start the configuration wizard, select *Configure IPSec*.
 - The wizard asks “*Enable weak crypto algorithms for enhanced compatibility?*”. Null encryption, DES, MD5 and Diffie-Hellman group 1 are considered weak and are not proposed by default. If any of these algorithms are required, respond select **Yes**.
 - The wizard asks “*Select IPSec Keying Mode*”. Select **IKE**. Static keys are not covered by this document.
 - The wizard asks “*Select IPSec Mode*”. Both Tunnel and Transport mode are supported. If the connection is to a VPN gateway, then select **Tunnel**. Only under very rare circumstances will Transport mode be used.
 - The wizard asks “*Select Phase 1 Mode*”. Phase 1 negotiation determines how the traffic is protected for negotiation of the ESP Security Associations. There are two options **Main** and **Aggressive**. In Main Mode the Comet sends a selection of security proposals to the VPN gateway, the gateway will then select the most appropriate. The set of proposals sent includes most permutations of encryption, hash and Diffie-Hellman algorithms supported by the Comet, it is this proposal set which may or may not include the “*weak crypto algorithms*”.

If **Main** mode is selected the wizard will ask: “**Using Main mode is incompatible with NAT. Do you really want to use this option?**”. When the Comet is behind a NAT device, **Main** mode will fail to negotiate keys. If the Comet is behind a NAT or there is any uncertainty select **Aggressive** mode, the Comet will auto-detect the presence or absence of the NAT.

In **Aggressive Mode** knowledge is required of the configuration of the VPN gateway, specifically, which algorithms the gateway is configured to accept. The Comet will send a single proposal with the given algorithms. **Aggressive Mode** requires more configuration effort but provides more control, there are occasions when the wizard will force **Aggressive Mode**, dependent on answers to previous questions. When **Aggressive** is selected the wizard continues with:

- The wizard asks “*Select Device Id Type*”. Select one of the four options to determine how the Comet identifies itself to the VPN gateway. The identification is typically used as an identifier to select the pre-shared key in the VPN gateway, most commonly used are **IP Address** and **Key Identifier**. Should **IP Address** be selected a warning will be given “**Using the IP address as identifier is incompatible with NAT. Do you really want to use this option?**”. If the Comet is behind a NAT device, NAT precludes the use of **IP Address** as an identifier. You will need to use another option and configure your VPN gateway accordingly.
- The wizard may ask “*Enter Device Id (1-63 chars)*”. Enter the identifier used to select the pre-share key in the VPN gateway.
- “*Select Encryption*”. The list of available encryption algorithms displayed may include “*weak crypto algorithms*”, if previously requested. The complete list is: DES-CBS (considered weak), 3DES-CBC, AES-128, 192 and 256. Select one.
- “*Select Authentication*”. The list of available authentication algorithms displayed may include “*weak crypto algorithms*”, if previously requested. The complete list is SHA1, SHA2-256 and MD5 (considered weak). Select one.
- “*Select DH Group*”, The list of available Diffie-Hellman groups displayed may include “*weak crypto algorithms*”, if previously requested. The complete list is Group 1 (MODP 768) – considered weak, and Group 2 (MODP 1024). Select one.
- The wizard asks “*Does the VPN gateway use username and password authentication (XAuth)?*”. Respond **Yes** if the user is required to authenticate themselves with the VPN gateway. If the response to this does not match the VPN gateway's configuration then the Comet will not connect to the VPN.
- The wizard asks “*Enter Pre-shared Key (6-64 chars/hex digits)*”. The Comet currently only supports pre-shared keys as the method for authentication, the pre-shared key entered here must match that on the VPN gateway. The key can be ASCII characters or, by prefixing with **0x**, hex digits. This is the seed to the creation of the dynamic keys, if this does match the gateway then the Comet will fail to connect to the VPN gateway.
- The wizard asks “*Enter VPN Client IP Address*”. If the Comet has been assigned a fixed IP address within the VPN then enter it here. Leave the address empty to force the Comet to use Mode Config and request an IP address from the VPN gateway.

- The wizard asks “*Enter VPN Server IP Address*”. Enter the public address of the VPN gateway here.
- The wizard asks “*Save Changes?*”. Respond **Yes** to save the configuration to the Comet's flash memory. Press **ESC** to go back and make any revisions. At this point the Comet has an IPSec configuration saved, but it is not enabled.
- The wizard will exit and the *IPSec* menu will be displayed. When IPSec is not active there will an option to *Enable IPSec* and when IPSec is active the option is *Disable IPSec*. Enabling or disabling IPSec does not effect the saved configuration.

Exit out of the menu system and the Comet will reboot to activate the changes.

Configuration Example

An example configuration session, defining a connection to a Cisco PIX VPN gateway. The Comet will propose to use 3DES-CBC, SHA1 and Diffie-Hellman group 2 during Phase 1 of the IKE negotiation. This set of algorithms will be used to protect phase 2. In Phase 2 the Comet will negotiate the final encryption and authentication algorithms used by ESP to protect application traffic. This configuration will work with or without a NAT device.

Starting from the first question in the wizard:

<i>Wizard Question</i>	<i>Reply</i>
<i>Enable weak crypto algorithms for enhanced compatibility?</i>	No
<i>Select IPSec Keying Mode</i>	IKE
<i>Select IPSec Mode</i>	Tunnel
<i>Select Phase 1 Mode</i>	Aggressive
<i>Select Device Id Type</i>	Key Identifier
<i>Enter Device Id (1-63 chars)</i>	tadpole
<i>Select Encryption</i>	3DES-CBC
<i>Select Authentication</i>	SHA1
<i>Does the VPN gateway use username and password authentication (XAuth)?</i>	Yes
<i>Enter Pre-shared Key (6-64 chars/hex digits)</i>	tadpoleskey
<i>Enter VPN Client IP Address</i>	<return>
<i>Enter VPN Server IP Address</i>	192.168.128.2
<i>Save Changes?</i>	Yes