

SoftRemote FAQ

Q- What is a VPN?

A- A Virtual Private Network (VPN) is a way to use a public network, such as the Internet, to provide remote offices or individual users with secure access to their organization's network.

A VPN works by using the Internet for communication while maintaining privacy through security procedures and tunneling protocols such as the Layer Two Tunneling Protocol (L2TP) or IPsec. In effect, private data, encrypted at the sending end and decrypted at the receiving end, is sent through a "tunnel" that cannot be "entered" by any other data.

Q- What makes IPsec so strong?

A- IPsec (Internet Protocol Security) provides security services at the IP layer by enabling a system to select required security protocols, determine the algorithm(s) to use for the service(s), and put in place any cryptographic keys required to provide the requested services.

The IPsec architecture is described in the RFC-4301 (<http://www.rfc-editor.org/rfc/rfc4301.txt>). IPsec has been selected to be embedded in IPv6. IPsec was specifically designed to be strong and to replace some older methods of security, such as PPTP.

Today, IPsec is the most secure way to access a corporate network from the Internet. Here are several reasons why:

- Strong encryption mechanisms, such as Encapsulated Security Payload (ESP) using DES (supported for backward compatibility reasons), 3DES, AES with long key length (e.g. 128, 192, 256)
- Strong authentication of parties identity with the use of XAUTH and Certificate with long key length (e. g. 1536, 2048)
- Use of Internet Key Exchange (IKE) and Internet Security Association and Key Management Protocol (ISAKMP) to automatically exchange keys and perform mutual authentication
- Protection against Denial Of Service (DOS) attacks. The IPsec protocols use a sliding window. Packets are numbered and only accepted if they fit the window.
- Use of SafeNet iKey™ USB Token in conjunction with IPsec client software to protect identity/authentication information and VPN configurations - SafeNet-specific feature

Q- What is NAT Traversal and does SoftRemote support it?

A- Network Address Translation (NAT) is designed to decrease IT manager frustration for scarce public IP addresses. A NAT device takes a packet's originating private IP address, translates it into a public IP address, and then sends the packet across the Internet to its destination. NAT devices use an internal table to keep track of translated addresses, but the packet's original IP header is manipulated, impacting IPsec ability to function. The IETF (Internet Engineering Task Force) worked out a solution called NAT Traversal (NAT-T RFC-3193) that is now widely implemented in routers and appliances.

SafeNet SoftRemote does support NAT-T.

Q- Pre-shared key versus Certificates ?

Computer authentication by IPsec is performed by using pre-shared keys or computer certificates. A pre-shared key identifies one party during the authentication phase. By definition, "pre-shared" means you have to share it with another party

before you can establish a secure VPN tunnel.

The strongest method of authentication is the use of a PKI and certificates. PKI and digital certificates use asymmetric cryptography for strong authentication. SafeNet SoftRemote IPsec VPN Client supports both modes.

Q- What is DPD ?

A- DPD or "Dead Peer Detection" is an Internet Key Exchange (IKE) extension (i.e., RFC3706) for detecting a dead IKE peer. This mechanism is used by the Redundant Gateway feature.

"SafeNet SoftRemote IPsec VPN Client Software"

Q- What is the latest version of SafeNet SoftRemote?

A- SafeNet SoftRemote Version 11.1.1.

Q- Which Windows Versions are supported?

A- Microsoft Windows XP (32-bit).

Microsoft Windows Vista [Home Premium, Business, Enterprise, Ultimate] (32-bit and 64-bit)

Q- Can a single installation package can be used on both versions (32 Bit and 64 bit) the Windows operating system?

A- No, there are separate installation packages for both versions of the operating system.

Q- Does version 11.1.1 supports Microsoft Vista Service Pack -1?

A – Yes, however, version 11.1.0 was not supported on Windows Vista SP1.

Q- Does version 11.1.1 supports silent installation?

A- When installing the client software on Vista platforms, the user will encounter several prompts requiring interaction. Please select 'Continue' or 'Install' when prompted. Due to this anomaly, silent installations are currently not supported on Vista platforms.

Q- How do I upgrade to SoftRemote version 10.X to version 11.1.1?

A- There is no upgrade method for that. You need to install version 11.1.1 separately.

Q – I have created a policy in Security Policy Editor, however, I am not able to see any connection name under the Connect button.

A – You must click on the reload button before attempting to connect using any policy. To reload, right-click on SoftRemote icon (appears on task bar) → Go to policy → click on Reload.

Q- Can we use SoftRemote version 11.1.1 and any other VPN client on a single machine?

A- Yes, you can. However, this was not possible with SoftRemote version 10.X.

Q- Does SoftRemote version 11.1.1 support IKEV2?

A – Yes, it does support IKE V2; however, we edit policy file manually to add this feature.

Q- How do I import/export security policy in version 11.1.1?

A- You can copy the .xml policy file from the directory where SoftRemote installation

files are installed. When adding a new connection using Security Policy Editor, all of the settings are automatically updated in the .xml file.

Q- Which gateways/firewalls are supported by SoftRemote?

A- SoftRemote will work with any gateway or firewall that follows IPsec RFC standards. Currently tested gateways are –

SafeNet SafeEnterprise HA2000
Netscreen
Netgear
Watchguard
Cisco VPN3000

Q- What is the format of the policy file in SoftRemote Version 11.X?

A- The Policy file is in .xml format.

Q – Can we use an old (SoftRemote version 10.X, .spd) policy file with a new version of the client software?

A- Yes. To convert an old policy file to a new policy file, please follow the steps below.

1. Open a command prompt with administrative privileges and navigate to the client installation folder.
2. Copy the legacy SPD file to this folder.
3. Enter > SPDConverter.exe [policy.spd] quicksec.xml
Where [policy.spd] is the name of the legacy SPD file.
4. Reload the policy via SoftRemote tray icon.

Q- Which ports are needed by SafeNet SoftRemote VPN Client?

A- UDP port 500 and UDP port 4500 must be open, and ESP protocol (protocol number 50); AH protocol (protocol number 51) must be allowed. Since Version 11.1 can co-exist with other VPN clients, if port 500 is occupied by that client then Version 11.1 runs on port 1500, 1800 for NAT-T.

Q – Can we define IP address range under remote party addresses?

A- Yes, for that we have to edit the policy file manually. This is not provided in GUI.

Steps –

Step1 - Open the quicksec.xml policy file with any text editor. (Default location - C:\Program Files\SafeNet\SoftRemote)

Step2 - Select the connection for which you want to specify an IP address range. Edit the destination for <rule to-tunnel> and source for <rule from-tunnel> as shown in below example.

For example – We have created “connection1” using user interface. Now we want to specify IP address range 10.10.10.1-10.10.10.20.

How to achieve this –

```
<rule to-tunnel="Connection 1" id="SPE48899" display="Connection 1">
<src>ipv4(0.0.0.0/0)</src>
      <dst>ipv4(10.10.10.1-10.10.10.20)</dst>
      <local-stack direction="from"/>
</rule>
<rule from-tunnel="Connection1" id="SPE37656" display="Connection1">
<src>ipv4(10.10.10.1-10.10.10.20)</src>
```

```
<dst>ipv4(0.0.0.0/0)</dst>
<local-stack direction="to"/>
</rule>
```

Step3- Save the quicksec.xml file.

Step4- Reload the policy from tray icon.

“TROUBLESHOOTING VPN CONNECTION USING LOG VIEWER”

Q – Why is Log Viewer used?

A- Log viewer displays the messages that are shared between two communication parties, client and gateway.

Q- « PAYLOAD MALFORMED » error (wrong Phase 1 [SA])

A- If you have a « PAYLOAD MALFORMED » error you might have a wrong Phase 1 [SA]. Check if the encryption algorithms are the same on each side of the VPN tunnel.

Q- « INVALID COOKIE » error.

If you have an « INVALID COOKIE » error, it means that one of the endpoints is using a SA that is no longer in use. Reset the VPN connection on each side.

Q - « INVALID ID INFORMATION » error.

If you have an « INVALID ID INFORMATION » error, check if « Phase 2 » ID (local address and network address) is correct and matches what is expected by the remote endpoint. Check the VPN Router SA monitor to verify if a previous SA is still alive.

Q - The VPN tunnel is up but I can't ping!

- 1- Check Phase 2 settings: VPN Client address and Remote LAN address. Usually, VPN Client IP address should not belong to the remote LAN subnet.
- 2- Once the VPN tunnel is up, packets are sent with ESP protocol. This protocol can be blocked by a firewall. Check that every device between the client and the VPN server does accept ESP.
- 3- Check your VPN server logs. Packets can be dropped by one of its firewall rules.
- 4- Check that your ISP supports ESP.
- 5- If you still cannot ping, follow ICMP traffic on the VPN server LAN interface and on the LAN computer interface (with Ethereal, for example). You will have an indication that encryption works.
- 6- Check the “default gateway” value in VPN Server LAN. A target on your remote LAN can receive pings but does not answer because there is a no “Default gateway” setting.
- 7- You cannot access computers in the LAN by their name. You must specify their IP address inside the LAN.

Technical Support Contact Information:

E-mail: support@safenet-inc.com

Phone: 800-545-6608, Phone: +1-410-931-7520