Virtual Adaptor FAQ

The Virtual Adapter (VA) is a method to present to the local client machine an interface using remote access service (RAS) or dial-up networking (DUN). It appears to the operating system as another adapter. It is considered a “virtual” adapter since the packets never actually leave the client machine through that adapter. Rather they are intercepted by the IPSec component and sent via a real, physical adapter (e.g. modem, Ethernet, etc.).

What is the purpose of the VA?
The VA is used primarily for two reasons: Client IP address assignment and assignment of network parameters such as WINS and DNS.

There are many scenarios in which the client PC needs to use a “private” address (e.g. 10.0.0.50) from the corporate network. This is often assigned to the client from the IPSec gateway at the edge of the network. One way in which the client machine can manifest that assigned private IP address is by using a virtual adapter with that as its configured IP.

Similarly, many networks have private network values for DNS and WINS addresses. These can be communicated to the client as it connects to the IPSec gateway.

What version includes the VA?
Version 6.1.0 of SoftRemote is the first version that includes the VA functionality.

What IPSec gateways does VA work with?
The VA functionality should work with any IPSec gateway that uses Mode Config to assign an IP address to the client. It can also be used with gateways that don’t do Mode Config by setting the Internal Network IP Address within the client.

When would the VA be used?
There are three primary reasons that the VA would be used:
a)When the IPSec gateway performs assignment of the WINS address via Mode Configuration protocol. Without the VA, the client can accept a private IP address / mask and DNS address, but not WINS.
b)When the client is on a Windows 2000 Operating System and the IPsec gateway assigns DNS address via Mode Config. Due to changes in the operating system, the client supports DNS assignment via Mode Config on other operating systems but not Windows 2000 unless a VA is used.
c)When there is a requirement that the assigned address be visible to user applications on the client system. When the VA is not used, the source address of each IP packet is automatically changed prior to leaving the client machine (similar to NAT). This can cause problems for certain applications that use the IP address.

How is VA configured?
In the “My Identity” section of each connection there is a setting for the Virtual Adapter. Available values are: Disabled, Preferred, and Required.

What’s the difference between VA Preferred and VA Required?
When the policy is configured to have VA Preferred, the policy allows for fallback to the “address substitution” method of address assignment should be VA adapter already be in use or otherwise unavailable (e.g. not installed). If the policy is configured to have VA Required, such unavailability will lead to abandonment of the IKE negotiation.

How long are the assigned values in effect?
When the client receives an IP address, DNS, and/or WINS address, it is only retained for the duration of that VPN connection to that gateway. When the connection is terminated, the VA is brought down and the configured values no longer used.

How does the client get its private IP address?
The client supports three methods for assignment of its private IP address:
·User entered: if enabled on the Global Policy Settings screen, the user can enter their Internal Network IP Address value in the “My Identity” section of the policy.
·Gateway assigned via Mode Config: Many gateways support the Mode Configuration internet draft. During

the IKE session establishment, the IPSec gateway sends the private IP address to the client.
·L2TP: Many gateways use L2TP to configure the client's IP address. During the L2TP session establishment, the L2TP Network Server (LNS) assigns the IP address to the client. The SoftRemote client is configured to secure the L2TP packets using IPsec.

Are L2TP and VA similar?
Yes, in some respects. Both use an adapter to allow the operating system and higher-level applications gain knowledge of the client's private IP address. Both use RAS / DUN when bringing up the L2TP / VA adapter. This means that RAS / DUN must be installed and operational (even though the connection isn't physically using a dial-up connection).

Are VA and "address substitution" similar?
Yes, and no. Yes, in that they both present a "virtual" address to the peer that is distinct from any physical interface on the client machine. No, in these ways:

1) The manner in which the address is manifested on the local machine is different. VA address assigments are visible to user apps on the client machine. "Address substitution" or VRS processing is done "in-the-pipe", and so is transparent to the user apps (as well as to the IP routing table).

2) Because the virtual adapter is an actual system resource, support for multiple VA-supported connections is limited. In contrast, VRS-supported connections are not subject to this limitation.

3) Because VRS-supported connections are transparent to the OS, the use of VRS has minimal impact on packet routing. In contrast, configurations of VA-supported connections must take into considerations the impact of the virtual adapter interface on the routing table.

Does VA cause a change in the client's routing table?
Yes, when the VA is initiated during IKE session establishment, the routing table is updated as a result of the new "dial-up" interface being added. The routing changes are very similar to those made when a dial-up connection is made to an ISP as the operating system's RAS / DUN processing automatically updates the routing table.

Depending on the address of the IPsec gateway, the client might also add a route to the IPsec gateway out it's physical interface. This prevents a packet from getting stuck in the VA and never leaving the machine.

What packets are routed to the VA?
The client's routing table determines what packets are sent via the VA. The operating system automatically updates the routing table to send packets to the VA at time of VA establishment. Note that many of the routing table changes are controlled within the operating system, such as the routing of an entire subnet to the VA. The actual subnet routed to the VA is dependent on the client IP address assigned by the gateway. For example, if the client is assigned a 10.0.0.5 address, the entire 10.0.0.0 class A network is routed to the VA. Whereas, if the client is assigned a 192.168.168.5 address, the 192.168.0.0 class B network.

Once the VA and IKE connection are established, what packets are secured?
To determine which packets are secured, think of it as an intersection of what the client's routing table sends to the VA and the IPsec policy in the client. If the routing table directs packets to the VA and the IPsec policy in the client defines that packets for a given subnet are to be secure, then the packets will be tunneled using IPsec to the gateway.

What happens to packets sent to the VA but not secured?
If the routing table sends packets to the VA but the IPsec policy is not configured to secure those packets, they are discarded. This is a method to prohibit "split tunneling". For example, by using the "use default gateway" option on the VA, (almost) all of the outbound packets can be directed to the VA. But if the IPsec policy is configured to secure only a subset (typically a subnet) of this address space, packets with ther destination addresses will be swallowed up by the VA and not exit the machine.

What is the RAS / DUN connection for?
After the VA has been used once, the user will notice a DUN connection called "SafeNet Virtual Adapter Interface". During session establishment, the client will programmatically access this connection and use

certain settings. If the connection is not present (e.g. first use of VA on a machine), it will be programmatically created with default values. There are a number of properties for the connection, some of which should not be changed; others that can be used to effect operation of the client. Information on some of the more relavent parameters:
Host Name or IP address / phone # : This is set to 000 and should not be changed. This indicates the connection will be used for a VA as opposed to an L2TP connection to an LNS.
IP address : Server assigned should be checked. The client will programmatically set the VA IP address based on the value sent from the IPsec gateway or entered locally in the “my identity” section.
DNS / WIN addresses: Any values entered here will be programmatically overwritten by those sent from the IPsec gateway.
Default gateway: Affects the routing table changes on the client machine that determines which packets are directed to the VA. This value (checked or not checked) can be changed by the user.

Is the “use default gateway” option configurable?
Yes. There is a “use default gateway on remote network” checkbox available under the TCP/IP setting for RAS / DUN connections. By default, when the SafeNet VA is first initialized, it will configure that option as “checked”. However the user has the ability to modify the phone book entry for the VA and uncheck this option. This will effect how the operating system changes the routing tables when the VA is launched. It can be very useful in determining what is (and is not) directed to the VA.