VPN Client Split Tunneling Issues to Consider

Here are a couple links relating to Split Tunneling and issues associated with it.

Nevermind the fact that this centers around ISA/IAS server VPNs as this applies to all VPN Client connections.

Remote Access VPN and a Twist on the Dangers of Split Tunneling

VPN Client Security Part 1: Split Tunneling Issues

VPN Client Security Part 2: Forcing Firewall Policy on VPN Clients

---------

Wikipedia - Split Tunneling

VPN Clients and Split Tunneling

---------
Split Tunneling Overview
The Contivity Extranet Switch allows the Nortel IPSec Extranet Access Client to operate in two modes - Mandatory and Split Tunnelled mode. While a client tunnel is established in mandatory mode, all client traffic is tunneled through the Switch by default. Split Tunneling allows you to configure specific network routes that are downloaded to the client. Only traffic destined for these network routes are then tunneled and sent to the client's Extranet adapter; any other traffic goes to the local PC Ethernet or Dialup adapter interface. Split tunneling allows you to access the Internet or print locally, for example, even while you are tunneled into the Switch.

Figure 1. Sample Split Tunneling Environment

In the previous example figure, Split Tunneling is enabled and the split tunnel network IP addresses 10.2.3.4 and 10.10.0.5 are configured. When a client establishes an IPSec tunnel these addresses are loaded into the client application.

The remote user, for example, then downloads his/her email from the Mail Server at 10.10.0.5, and downloads a document from the Archive at 10.2.3.4. Next, without exiting the tunnel, the remote user can print the document through the PC's local network interface 192.19.2.32 to the Printer at 192.19.2.33. The remote user also has the capability of browsing the Internet without taking the tunnel down.

The Switch administrator designates which network routes to tunnel through the Switch. This is done on a per-group basis by associating specific split tunnel network routes to specific groups on the switch.
**Security**

The Switch takes precautions against violators' potentially hacking tunneled information when the Switch is operating in Split Tunnel mode.

Security risks and concerns must be completely analyzed and taken into consideration prior to enabling split tunneling. Mandatory tunneling will ensure only access to the private network, making it less likely that the user will be an active conduit for malicious information by downloading sensitive information or uploading malicious files.

The switch's primary precaution is to drop packets that do not have the IP address that is assigned to the tunnel connection as its source address. For example, let's say you have a PPP dial-up connection to the Internet with an IP address of 192.168.21.3. Then you set up a tunneled connection to a Switch and you are assigned a tunnel IP address of 192.192.192.192. Then, any packets that attempt to pass through the tunnel connection with a source IP address of 192.168.21.3 (or any address other than 192.192.192.192) will be dropped.

Furthermore, you can enable filters on the Switch to limit the protocol types that can pass through a tunneled connection. There is a clear distinction between switch filters and client policies, however. While filtering at the switch will allow you to drop certain packets, client policy extends that to the desktop and gives you an additional level of control.

Filtering is the mechanism that controls fine-grained access to specific hosts and services. Each user has a specific filter profile based on their group's profile that describes which resources on the network they can access. The filters are defined by:

- Protocol ID
- Direction
- Source, destination IP addresses
- Source, destination port
- TCP connection establishment

A filter profile consists of a list of rules that you create to perform precisely the action that you want. These rules are tested in order until the first match is found. Therefore, the order of the rules is very important. The filtering mechanism works such that if no rule matches then the packet is discarded (denied). This means that no traffic is transmitted or received unless it is specifically permitted.

**Client Policy**
Client Policy helps prevent potential security violations that could occur when you are using the split-tunneling feature. Split tunneling allows client data to travel either through a tunnel to the enterprise network or directly to the Internet. Although a powerful feature, split tunneling could allow an application on the client to maliciously forward packets from the Internet to the enterprise network.

Potentially malicious threats could be associated with unauthorized software code (such as a java applet or a daemon) that resides on your workstation unbeknownst to you. This code could potentially download documents from the private network through the tunnel to a workstation, and then send those documents to a network system without you knowing. Even though the Extranet Access Client will not route packets into or out of a tunnel, a shrewd rogue application could send the information back out to the Internet through a separate connection. These threats probably have a very, very low probability - the more serious threats are active things users do like install Wingate or other proxy servers to facilitate access from other home network machines, a clear risk if they don't know what they're doing.

Client Policy allows you to determine which network applications and associated protocols and ports a remote user can have active on his workstation while tunneled into the Switch. Limiting certain types of network applications from executing while using the split-tunneling feature eliminates some security threats.

Client Policy, in effect, will shut down a tunnel if a disallowed application is launched on a client machine. And since the Client Policy feature is downloaded when the client attempts to establish a tunnel connection, no remote user intervention is required.

Split Tunneling is disabled by default. Therefore, all traffic to and from the workstation is forced through the tunnel and is subject to the security policy enforced by the Switch's filters, and any corporate firewall that filters traffic to and from the Internet.

The client receives a list of allowed services just after authentication but prior to a tunnel being established. If the client discovers an active application has a TCP or UDP port open that is not permitted, it disconnects the tunnel.

The Client Policy list contains information on the protocols, ports, and application types (client or server) that are permissible during tunneling.

- Configurable protocols include TCP and UDP.
- Configurable ports include the list of ports allowed to be open while the tunnel is active.
• Application types or direction specifies whether the open port is a source (client) or destination (server) port. For example, specifying Client as the application type allows the client to run an FTP client session, but not an FTP server session.

Be careful when choosing the list of network ports that your client can use while using split tunneling because you might prevent acceptable applications from running.

For example, to allow only WEB browsing, POP3 Email and Telnet sessions the switch administrator would set up the following filters:

• For WEB browsing - Client port 80 for the TCP protocol
• For POP Email (POP3 Server) - Client port 110 for the TCP protocol
• For Telnet sessions - Client port 23 for the TCP protocol.

Note: all applications in this example are client based since they are initiated from the client's workstation. Server based applications would typically be listening for and opening sessions with other clients on the network.

When establishing a tunnel, if the client has any network ports open that are not part of the Client Policy list, the tunnel connection is not established and the remote user is notified. A message is also logged on the Switch as to which open port or protocol violated the Client Policy.

Network traffic on a client system is inspected for source/destination address as well as protocol port number to make sure no policy violations occur after the tunnel is established. This way, if a rogue application should start after the client connection has already been established, it is recognized immediately and the tunnel is terminated.

Client Policy is currently implemented for those applications that are defined in terms of using well-known port numbers. Applications that deploy random port numbers are not well suited for use with client policies since there is no mechanism in place today that allows the switch to be configured with a range of port numbers for a specific protocol. This would require that all possible port numbers be configured in the client policy and would make policy administration quite tedious and difficult to manage. There are many applications in use today that implement random port numbers, therefore, the administrator needs to have a good understanding of the applications in use and what port numbers are being opened. For example, FTP Client uses port number 21 to establish a session, but can open a random port number to receive data traffic. Allowing just client port number 21 for the TCP protocol would not suffice to allow FTP traffic through the tunnel.
Careful consideration must be taken for using split tunneling with and without client policies since there are potential security risks involved with using this feature. For those users who are extremely security conscious, split tunneling may not be a desirable option.

**Split Tunneling and Upgraded Switch Versions**

If you upgrade the Switch to Version 2.50 and enable Split Tunneling, then a user who establishes a tunnel with a Version 1.00 or 1.50 Extranet Access Client might not be able to access hosts outside the corporate network through the tunnel.

This problem occurs because Version 1.00 and 1.50 clients only allowed mandatory tunneling (when a tunnel was up, all traffic goes through it). Version 2.50 with Split Tunneling has an additional security measure. Incoming tunnel traffic is checked against the Split Tunnel networks list. Traffic that is not destined for a Split Tunnel network is routed to the Internet.