

VIRTUAL PRIVATE NETWORK OVERVIEW

ExSTARS BRIEFING MERRIMACK, NEW HAMPSHIRE October 21, 1999

What is a Virtual Private Network?

A Virtual Private Network (VPN) allows an exchange of data between two computers in a **secure** manner over a shared **public** network, typically the Internet. The name “Virtual Private Network” comes from the fact that the data exchange happens almost as if the two computers were exchanging data using a private network.

Why is the IRS considering using a Virtual Private Network as the method for accepting *ExSTARS* information reports?

Two important factors are being considered relative to using a VPN and the Internet. The first factor is the need to provide a **secure** means for transporting information reports to the IRS. The second factor is the need to provide a **low cost** solution for electronic filing of this data.

Other relevant factors include:

- Access for stakeholders from virtually any location
- Scalability; the VPN capacity can be sized to meet varying demands
- A simple network architecture

What will it take for a VPN to meet *ExSTARS* information report filing needs?

A Virtual Private Network requires several components to be successful. The key components to be provided by the IRS are:

- **Performance and Quality** - A VPN must deliver, at a minimum, a predictable level of service over the secure tunnels that interconnect the VPN sites.
- **Security** - It is important to ensure that data is kept private and secure while it is transported. Technologies such as secure sockets layer and private communications technology are examples of transport level security that guarantee privacy. In addition, it is important to address Web client security, Web server security, and operating system security.
- **Management** – Virtual Private Networks must be managed and monitored. Tightly integrated tools will be used to manage routing and quality of service. Other management functions include fault management, performance monitoring, and network capacity planning.
- **Carefully Integrated Hardware and Software** – It is important to properly integrate Web Server, Client, firewall and database hardware and software components.

How does a VPN Work?

A VPN is implemented using a technique called tunneling. Tunneling is used to secure information across the Internet by limiting a connection to just one entry and one exit point. The name tunneling is very descriptive because it describes how one protocol (set of rules that govern the transmission of data through a network) is placed inside another protocol, which is placed inside a third protocol. The innermost protocol creates a *tunnel* through the outermost protocol.

Data encryption and data compression are negotiated when the tunnel is created. The information report filer creates a virtual dedicated link for the time needed to complete the data transfer. As soon as the transaction is complete, the link is returned to the public network.

Users of the VPN must be authenticated. Authentication is a process of identifying who is logged on to the VPN and verifying their identity. The first step in authentication is identification. There are potential security problems if only a user name and password are used for identification. For example, passwords can be stolen, guessed by hackers or shared with unauthorized people. It is therefore important to invoke a more secure means of authenticating *ExSTARS* users. Digital Certificates are one of the most secure authentication methods available today. Digital Certificates and other authentication methodologies are being evaluated for use with *ExSTARS*.

The following diagram represents a solution that may be used to implement electronic filing of *ExSTARS* information reports over the Internet. Using this example, the filer would connect to the Internet using an Internet Service Provider. Once connected to the Internet Service Provider, the procedure would be as follows:

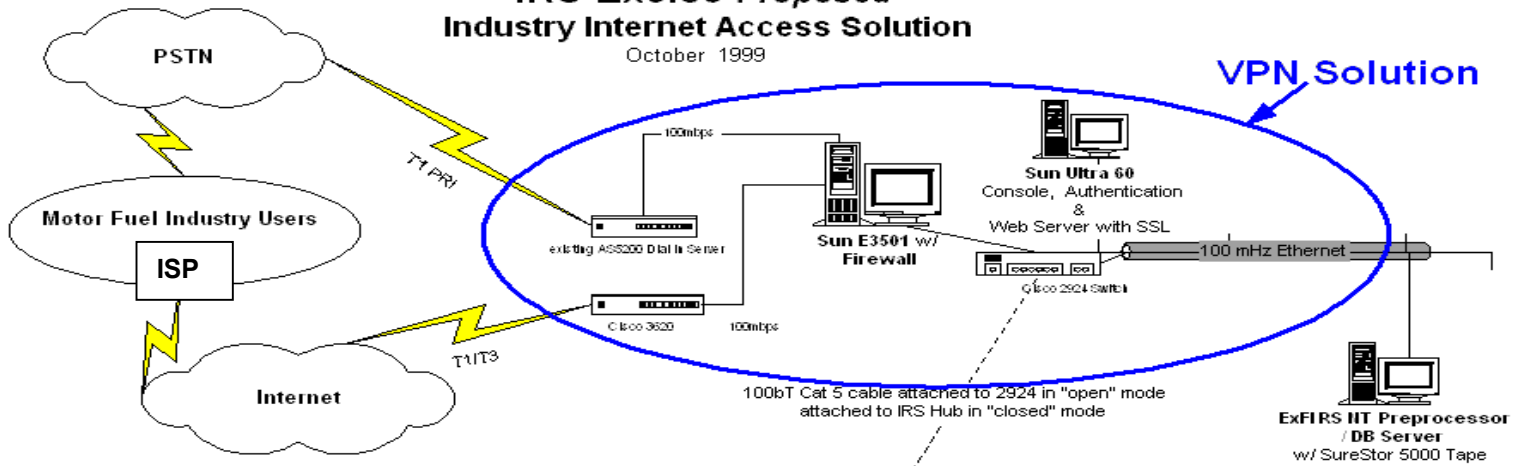
- Issue a request to connect to *ExSTARS* – this will result in the filer getting a connection to a router at the IRS.
- The router will pass the request to the firewall.
- Software on the firewall will filter incoming traffic and pass the request to the Web Server.
- The Web Server checks to see if the user has been authenticated.
- If the user has NOT been authenticated, the user is passed to the “Security Services System” for authentication.
- The authenticated user is passed back to the Web Server.
- The authenticated user submits an EDI file to the *ExSTARS* Translator/Preprocessor.
- The session can then be terminated.

Following the initial processing on the *ExSTARS* Preprocessor, the EDI translator will acknowledge receipt of the EDI file if it is submitted in correct form. The translator will reject the file if it is not in correct form.

The internal firewall is used to partition, isolate, and control access between the *ExSTARS* Preprocessor and internal IRS systems.

IRS Excise *Proposed* Industry Internet Access Solution

October 1999



IRS Firewall

Physical Separation
-ie Switch between
IRS and ExVPN

ExFIRS
Integrated
System

