

## VPN and RADIUS Implementation

The VPN and RADIUS services have been implemented on the network's ISA server. This has been setup to allow external access for those that have cleared authority to access and view the network accordingly. Through the ISA services we can also monitor and evaluate all accessed into the network to include those that have accessed through the VPN for higher level of watchdog type security.

Access to the VPN is done by remotely by accessing the NSF.IS-A-GEEK.COM or NSF.KICKS-ASS.ORG. Once the users have established a connection a properly logged onto the system from there they can gain outside access to the network and all of the utilities that are needed from the comfort of a foreign location.

Implementation of the VPN started by first installing a Windows 2003 server environment from there the ISA services were installed and properly configured. This is for any intrusion and defense protections.

After which VPN services were setup using the ISA services by enabling the Routing and Remotes Access Service (RRAS) and then configuring the VPN services.

Once the initial setup of has been completed we would then go to the Task tab on the side and enable vpn client access.

Then the select the Radius server and use the Radius services for authentication and logging.

To add the radius services click add radius services add server name, fully qualified domain name (such as fileserver.nsf.inc) then go to the access network tab under VPN properties. Extend the options and go to all networks then static pull. The range of the IP assignments will go from 0.0.0.1 thru 10.0.0.100. Obtain the DHCP/ DNS from the internal network.

Authentication will be MSCHAP V.2, GAP, allow IPSec/L2TP connections. Users will use a pre-shared key of 1234abCD. Then under VPN properties, client access, enable max number of VPN users. Protocols enabled are PPTP, L2TP. Then the Domain name will be NSF.INC.

After which the firewall policies are setup for the VPN/RADIUS services through access roles. These access rolls are through PPTP, IKE, L2TP, IPSEC. Then allow it to monitor sessions through IDS. Once this is completed you will verify the network roles by going through the vpn clients and setting it for destination networks are external.

Once this is done the setup for the VPN services and security is completed. This will assist in production of the workforce even if the user is not presently at work. This will assist in cutting back lost man hours, broken deadlines, lost continuity if a user happens

to miss work. This setup will also assist in secure monitoring and evaluations of the network to assist in keeping unethical events for reaching inside the company virtually.

