NIC VPN SERVICE

Introduction

NIC-VPN Service was launched to securely update web sites hosted in NICNET and also for accessing the Intranet.

What is VPN?

A **virtual private network** (VPN) is a private data network that makes use of the public telecommunication infrastructure, maintaining privacy through the use of a tunneling protocol and security procedures. VPN creates a virtual "tunnel" connecting two endpoints by encrypting end to end communication and protecting the data from unauthorized access or interception. The main purpose of a VPN is to give the company the same capabilities as private leased lines at much lower cost by using the shared public infrastructure.

The VPN Service provides a secure communication channel for updating the websites through different updating methods like SFTP, SSH or SCP. From the logs of Radius accounting and Authentication one can be held responsible for any change in any web site that is getting updated.

A user with a VPN client connects and receives an IP address from the Internet service provider (ISP). This is then replaced by an IP address from the IP pool defined on the VPN server. Users who are not running the client can connect to the web server using the address provided by the static assignment. Traffic of inside users does not go through the IPSec tunnel when the user connects to the Internet. Each user is made to access to the particular web server for updating his page.

There are 3 types of VPN technologies: Trusted VPNs, Secure VPNs, and Hybrid VPNs. NIC is providing Secure VPN service.

Secure VPN

Networks that are constructed using encryption are called secure VPNs. Trusted VPNs offered no real security, vendors started to create protocols that would allow traffic to be encrypted at the edge of one network or at the originating computer, moved over the Internet like any other data, and then decrypted when it reached the corporate network or a receiving computer. This encrypted traffic acts like it is in a tunnel between the two networks: even if an attacker can see the traffic, they cannot read it, and they cannot change the traffic without the changes being seen by the receiving party and therefore rejected.

Secure VPN technologies

- **IPsec with encryption** in either tunnel and transport modes. The security associations can be set up either manually or using IKE with either certificates or preshared secrets.
- **IPsec inside of L2TP** has significant deployment for client-server remote access secure VPNs.

VPN account is valid for 2 years and can be extended on request by users forwarded by respective HOD/ NIC Coordinator. VPN connection will be provided to only authorized and approved users and server farms / projects/ network.

NIC VPN division will not be responsible of any activities done in the server / site even if the connection is established through VPN. The server administrator should take necessary action to secure the application/ server.