Application Note

Feature

Matrix NAVAN's Virtual Private Network (VPN) feature used for secure exchange of Voice and Data over Public Network.

Products

Matrix NAVAN CNX200

Introduction

For those businesses which are expanding globally, it is necessary that the employees of each branch offices can access data from the main office; that too securely. In such cases, when the remote employee or business partner wants to have an access to a computer or network of computers from a remote location; using Virtual Private Network is the best solution.

Matrix NAVAN CNX200 provides Virtual Private Network (VPN) for secured data transfer. VPN is a private network, which uses the public network to connect the two computers or two networks or remote offices/users located at remote sites on the network to share or access data securely; appearing as if they are in the same network. A Virtual Private Network, '*virtually*' connects its remote sites/users and transfers the data that are tunneled through WAN using encryption and security protocols resulting into the transfer of data 'privately' on the public network.

The main purpose of a VPN is to give the organization the same capabilities as private leased lines at much lower cost by using the shared public infrastructure.

A VPN is composed of two parts: VPN Server and VPN Client.

VPN Server: It is a machine (host) that accepts connections from VPN client. A VPN Server provides remote access connections or router-to-router (Site-to-Site) VPN connections.

VPN Client: Any remote user, who wants to connect to the VPN Server to access its network, becomes its VPN Client. A VPN Client requires either a dial-in modem or a dedicated connection to the internet.

Matrix NAVAN serves as **both** VPN Server as well as VPN Client.

Matrix NAVAN will always serve as only VPN Client in Site-to-Site VPN (as it sends request) and will serve as only VPN Server in Remote Access VPN. Remote access VPN is a connection between a remote computer and the internet, whereas; Site-to-Site VPN is a connection between two networks (between two NAVAN).

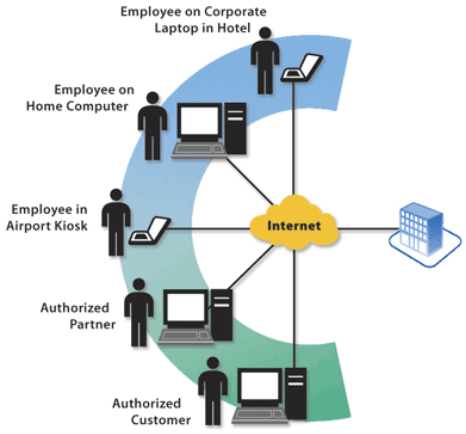
Pre-Requisites for VPN Connection

For VPN Server – Matrix NAVAN CNX200 and for VPN Client – PC, Laptop, Tablet or Smart Phone containing VPN settings and NAVAN or 3rd party router can also be used containing VPN settings.

Types of VPN – Application Based

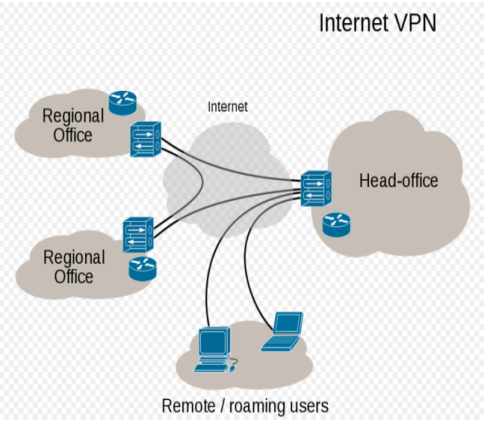
There are two types of VPN: **Remote Access VPN and Site-to-Site VPN.** The VPN client either uses Remote or Site-to-Site type of connection as per their usage.

Remote Access VPN



Remote Access VPN is a connection between a remote computer and the Internet. This type of VPN is a user-to-LAN connection and it is used when any main office has remote employees or users who need to be connected to the private network (main office) to access their email, files and other resources at work from various remote locations. With this type of VPN, you can provide highly secure and flexible remote access to anyone, anywhere and anytime. Remote-access VPNs permit secure, encrypted connections between a company's private network and remote users through a third-party service provider.

Site-to-Site VPN



Site-to-Site VPN connection is a connection between two networks, which usually is done between two routers; connecting multiple sites (offices) securely over a public network (Internet) but appearing as a local connection. Site-to-Site VPN extends the company's network and its resources to branch offices, business partners or customer sites. Thus, this enables both the sites to share resources such as documents and other types of data over the VPN link.

Site-to-Site VPN is further categorized into **Intranet** and **Extranet.**

- **Intranet:** This type of Site-to-Site VPN is a set up between multiple branch offices of the same company located at remote locations. Using this type of set-up, each separate LAN (a single private network) can be connected to a single WAN (public network).
- **Extranet:** This type of Site-to-Site VPN is a set up when the business partners and/or customers located at remote locations are to be connected with the main office. Using this type of set-up, you can get connected with business partners'/customers'/suppliers' LANs securely, at the same time preventing access to their respective intranets.

Matrix NAVAN CNX200 – Security Protocols Supported

A well designed VPN includes data encryption, tunneling, data integration and authentication processes. To perform all these processes, VPN can be created using security protocols, as below:

- Internet Protocol Security (IPSec)
- Layer Two Tunneling Protocol (L2TP)
- Secure Sockets Layer (SSL)
- Point-to-Point Tunneling Protocol (PPTP)

IP security (IPSec): IPSec is used to secure Internet communications and can operate in two modes. Transport mode only encrypts the data packet message itself while Tunneling mode encrypts the entire data packet. This protocol can also be used in tandem with other protocols to increase their combined level of security.

Layer 2 Tunneling Protocol (L2TP)/IPsec: The L2TP and IPsec protocols combine their best individual features to create a highly secure VPN client. Since L2TP isn't capable of encryption, it instead generates the tunnel while the IPSec protocol handles encryption, channel security, and data integrity checks to ensure all of the packets have arrived and that the channel has not been compromised.

Secure Sockets Layer (SSL) and Transport Layer Security (TLS): SSL and TLS are used extensively in the security of online retailers and service providers. These protocols operate using a handshake method. A HTTP-based SSL connection is always initiated by the client using a URL starting with https:// instead of with http://. At the beginning of an SSL session, an SSL handshake is performed. This handshake produces the cryptographic parameters of the session. These parameters, typically digital certificates, are the means by which the two systems exchange encryption keys, authenticate the session, and create the secure connection.

Point-to-Point Tunneling Protocol (PPTP): PPTP simply tunnels and encapsulates the data packet. PPTP uses a control channel over TCP (Transmission Control Protocol) and a MPPE (Microsoft Point-to-Point Encryption) tunnel operating to encapsulate PPP (Point-to-Point Protocol) packets and data security for PPTP connection between VPN server and VPN client.

Advantages of Matrix NAVAN CNX200 – Virtual Private Network

NAVAN's VPN provides your business with the following benefits:

- Provides the flexibility to the remote offices or individual users/employees to access your organization's network through public network (Internet).
- Extended geographical connections without usage of any Leased Lines.
- Maximum security of data exchange, including the authentication of the packets received as well as ensuring that the contents of the data does not change during transition.
- Reduces the cost and time of travelling for the remote users.
- Data Confidentiality.
- Reliability of connection with no hindrance as well as receiving the same quality, even during maximum simultaneous connections.

Document Type	Virtual Private Network Feature of Matrix NAVAN
Compatible Software Version	NAVAN CNX200 V1R1 onwards
Release Date	25-Dec-15
Version	V1R1

 Rel. V1R1 Dec'15