MAUSAM, **69**, 1 (January 2018), 97-102

551.501.8 : 55.502 : 551.509.13

Technical study of remote access VPN and its advantages over site to site VPN to analyze the possibility of hybrid setups at radar stations with evolving mobile communication technology

R. BIBRAJ, SUNNY CHUG, SANKAR NATH and S. L. SINGH

India Meteorological Department, New Delhi – 110 003 India

(*Received 28 February 2017, Accepted 17 October 2017*)

e mail : bibraj.r@imd.gov.in

सार – भारत मौसम विज्ञान विभाग ने नए रेडार स्टेशनों को आरंम्भ करते हुए भारतीय उपमहाद्धीप में रेडार के प्रभाव को बढ़ाने की योजना बनाई है। रेडार स्टेशनों से अपरिष्कृत आॉकडों को साइट टू साइट VPN रूटर के माध्यम से नई दिल्ली स्थित केंद्रीय सर्वर को भेजा जाता है। इस कार्य के लिए रेडार स्टेशनों में VPN रूटर हार्डवेयर की आवश्कता होती है संचार तकनीक सुरक्षा और गति में लगातार तीव्र गति से प्रगति कर रही है। इसलिए रेडार स्टेशनों में VPN हार्डवेयर को लगातार उन्नत करने की आवश्कता है। मोबाइल टेक्नोलॉजी ने गति और विश्वस्नीयता में तीव्र गति से कदम बढ़ाया है जिससे तार संचार की अपेक्षा इसके इसके रखरखाव में और उन्नत करने में लागत कमी आने की संभावना बढ़ जाती है। सुदूर स्टेशनों और पर्वतीय क्षेत्रों में VPN कनेक्शन के लिए केबल बिछाने में अत्याधिक पूँजी भी लगती है और उसके ठीक तरीके से काम न कर पाने में अत्यधिक धन लगाने की संभावना भी रहती है, जिससे उसके रखरखाव में धन और समय दोनों लगते है। केबल के काम न कर पाने जैसे मामलों में आंकड़ों का अंतरण आम इंटरनेट के जरिए मोबाइल ब्रॉडबैड मॉडम से किया जाता है जो कि VPN जैसे सुरक्षित नहीं हैं। हालाँकि एक स्थान से दूसरे स्थान वाले VPN संदेश स्विचन स्टेशनों में यह अनिवार्य है। भले ही रेडार स्टेशनों में यह जरूरी नहीं होती है जहाँ पर कि आॉकड़ो का सिंगल प्वाइंट अपलोड और डाउनलोड किया जाता है। सुदूर एसेस VPN बिना किसी अतिरिक्त हार्डवेयर के सिंगल प्वाइंट से सेंट्रल सर्वर तक आॉकड़ों का अंतरण सुरक्षित और विश्वसनीय तरीके से करता है। सुदूर एसेस VPN ग्राहकों का सॉफ्टवेयर मौजूद इंटरनेट आधारभूत संरचना के माध्यम से नई दिल्ली स्थित नेटवर्क एसेस सर्वर तक VPN टनल बनाता है जिससे आंकड़ों का अंतरण सुरक्षित तरीके से होता है। जब इंटरनेट सेवा प्रदान करने वाला अपने संचार माध्यमों के बुनियादी ढाँचे को उन्नत करता है तो रेड़ार स्टेशनों में हार्डवेयर पर कोई निर्भरता नहीं रह जाती है और आंकड़ों को उन्नत इंटरनेट आधारभूत संरचना के जरिए भेजा सकता है। दूरदराज इलाकों मे लगे रेड़ार स्टेशनों जहाँ संचार का साधन मोबाइल ब्रॉडबैड मॉडम के जरिए होता है वहाँ रिमोट एसेस VPN टनल ने आंकडों को सुरक्षित भेजा जा सकता है। इस शोध पत्र में साइट टू साइट VPN पर रिमोट एसेस VPN के लाभ के बारे में विवेचन किया गया है और रेडार स्टेशनों में हाइब्रिड संचार नेटवर्क की संभावना को खोजा गया है।

ABSTRACT. India Meteorological Department (IMD) has planned to increase the radar coverage in the Indian sub-continent by commissioning new radar stations. The raw data are sent from the radar stations to the central server at New Delhi through site to site VPN which requires VPN router hardware in the radar station. The communication technology is continuing to make rapid progress in security and speed which requires constant up gradation of the VPN hardware in the radar stations. Mobile technology has made rapid strides in speed and reliability which opens a possibility of reduced maintenance and up gradation costs compared to wired communication. In remote stations and hilly regions, laying of cables for VPN connection is capital intensive and prone to failures which leads to maintenance costs and downtime. In such cases of cable failure the data transfer is made by mobile broadband modem through public internet which is not as secured as VPN. Though site to site VPN is essential in message switching stations, it may not be necessary in radar stations where single point upload and download of data takes place. Remote access VPN offer secured, reliable data transfer from single point to central server without using any additional VPN hardware. Remote access VPN client side software creates a VPN tunnel to the Network Access server located in New Delhi through existing internet infrastructure and data transfer happens in a secured manner. When the internet service provider upgrades their communication infrastructure there is no hardware dependencies in the radar stations and data can be send through upgraded internet infrastructure. In Remote radar stations where communication is through mobile broadband modem, the data can be send in a secured VPN tunnel by remote access VPN. This paper discusses the advantages of remote access VPN over site to site VPN and explores the possibility of hybrid communication network in the radar stations.

Key words – VPN, Virtual private network, RTH, Radar network, Site to site VPN, Remote access VPN, ISSD.

1. Introduction

Information System and Services Division (ISSD) of India Meteorological Department (IMD) acts as Regional Telecommunication Hub (RTH) in Global perspective and as National Meteorological Telecommunication Centre (NMTC) for national data exchange. The new RTH has file switching capability through FTP (Satellite, RADAR and NWP model), automatic conversion of the received SYNOP and upper air messages to BUFR and their transmission on GTS. The circuits link New Delhi (Palam), Mumbai, Kolkata, Chennai and Guwahati Airport networks with the NMTC New Delhi at high speed through VPN (Virtual Private Network of BSNL). Such VPN facility has been extended to almost all RMCs, MCs, DWRs and other important stations throughout the country as a replacement of T/P links & other high-speed links and it has become the main national network for data exchange within the country.

A virtual private network (VPN) is a technology that creates an encrypted connection over a less secure network. The benefit of using a VPN is that it ensures the appropriate level of security to the connected systems when the underlying network infrastructure alone cannot provide it. The most common types of VPNs are remote-access VPNs and site-to-site VPNs.

Doppler Weather Radars are used to detect process, distribute and display meteorological data over a large area. Doppler technology opened new trends in the field of the radar meteorology and increased the performance of weather radars significantly. Radar data in addition to the now-casting abilities also plays a significant role during Cyclones for tracking and analysis.

2. Overview of existing virtual private network

Virtual private network has different configurations based on the usage. The most common among them are the site to site VPN and remote access VPN. With both the remote access and site-to-site connections, VPNs enable an organization to replace the need for long distance dial-up or leased lines which are cost intensive both in capital and maintenance.

In a site-to-site VPN, hosts do not have any software in the client side; they send and receive normal TCP/IP traffic through a VPN gateway. The VPN gateway is responsible for encapsulating and encrypting outbound traffic, sending it through a VPN tunnel over the Internet, to a peer VPN gateway at the target site. Upon receipt, the peer VPN gateway strips the headers, decrypts the content and relays the packet towards the target host inside its private network. The most common secure

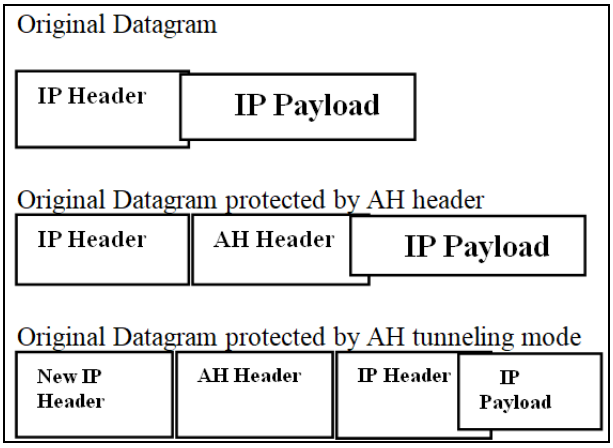

Fig. 1. VPN header format

tunneling protocol used in site-to-site VPN is the IPSec. IPSec standard provides a method to manage authentication and data protection. Another site-to-site VPN protocol is Multi-Protocol Label Switching (MPLS), although MPLS does not provide encryption, it provides reliable and efficient routing. For site-to-site VPN we need a router in central server as well as in destination station to do routing configuration. Each router has definite characteristics of speed it can support, the number of ports and the kind of physical network it can support (Fig. 1).

At present, all DWR stations along with Telecom Division of IMD, New Delhi have been connected by an IP VPN network. At each VPN access point / location, a modem connects to the VPN network provider. Modem is connected with router which acts as a bridge between the VPN network and the local LAN. The router is connected with switch which connects the DWR servers among themselves as well as with the router. Since data from all the DWR stations will come to Telecom Division, New Delhi, so the Telecom Division, New Delhi is connected to VPN network with a higher bandwidth, 8 Mbps link. VPN also facilitates the interconnectivity between two radar stations as all are connected in the same network. The data from the Radar server is encapsulated, encrypted in the router in the radar station. This data is send through the communication infrastructure of the VPN service provider through modem and is received at the router in the central server at New Delhi. At the central server, the data is decrypted and sent to the respective destination address (Fig. 2).

The Router maintenance comes under the purview of IMD and its up gradation is required when the VPN service provider has switched to an advanced communication Infrastructure. The communication

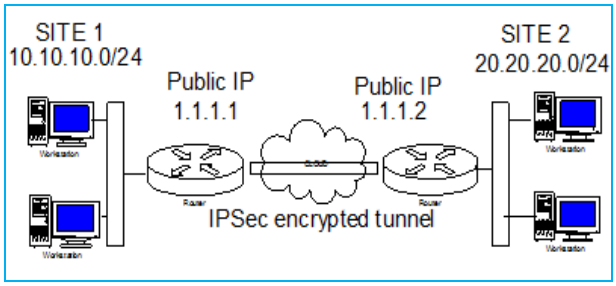

Fig. 2. Site to site VPN presently used in IMD

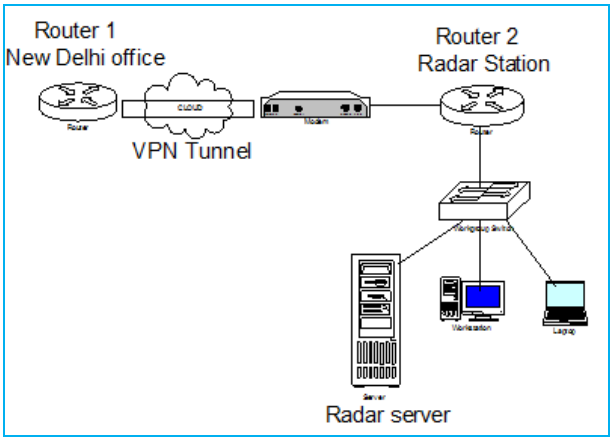

Fig. 3. Present set up of VPN connected to Radar stations

infrastructure is rapidly improving from broadband Ethernet to fiber optic cables. In case of situations wherein a redundant network is necessary which will be useful in the times of disaster and bad weather, a complete router setup with a different VPN network provider is necessary. Site to site VPN is also restricted when we use mobile broadband modem. This paper discuss the configuration of remote access VPN which removes the dependency of router hardware at the client side and also provides flexibility with the network service providers.

3. Remote access VPN

Remote Access VPN also provide a secure and encrypted connection between the organization network (IMD Network in the central server) to the remote machine which is present in the radar station for transmitting the Radar Data. This is done by creating an encrypted IPSec Tunnel through the Internet connection provided by the service provider *(technet.microsoft.com).* This connection consists of a VPN client in the workstation at the radar station and a VPN gateway in the central server at New Delhi. The VPN client initiates the IPSec tunnel from the workstation in the radar site to the VPN gateway at the central server in New Delhi.

The data from the radar server can be transferred to the workstation where the VPN client is present through File Transfer protocol (FTP) by the local LAN network and once the data reaches the workstation, it can be transferred to the central server in a secured way through the VPN. The VPN client initiates the tunnel and is independent of the Internet service provider, it uses only the communication Infrastructure of the service provider whereas the encryption is done by the remote access VPN client software which is present in the workstation, This is different to the site to site VPN where the encryption and encapsulation is done by a VPN router at the client side. A username and password is provided to the Radar station VPN client to access the VPN gateway in the central server. This username and password is configured in the VPN gateway in the central server for Authentication *(sc1.checkpoint.com: 85469)* this prevents unauthorized login to the central server.

The tunnel is created by Internet key exchange (IKE). The data through the VPN tunnel are made secure by encryption from the sender side and decryption in the receiver side, for this to happen both should agree on a common key for the encryption. An IKE negotiation takes place between the VPN client in the radar station and the security gateway in the central server. During the process of negotiation the authentication of the peers are verified. The security gateway verifies the identity of the client in the radar station and the client verifies the identity of the security gateway *(sc1.checkpoint.com: 85469)*. IKE establishes the VPN tunnel by authenticating on either sides and to agree upon the method of encryption and integrity. After the IKE negotiation a Security association (SA) is created. Upon completion of the SA successfully a secured connection is established between the client and the security gateway and all data inside this VPN tunnel is encrypted as per the IPSec Standard. Negotiation and agreement of keys and method of encryption are done in a secured way by having two phases of IKE (*sc1.checkpoint.com : 73680*).

The keys and encryption agreed in the first phase of IKE will be used to transfer information in the next phase of IKE. Diffie hellman Key exchange method where the peers can independently create a shared secret is used to generate the keys in the first phase of IKE *(sc1.checkpoint.com : 73680)* The outcome of first phase of IKE is IKE SA which is an agreement of keys and method of encryption for the second phase of IKE. In the second phase of IKE, the encryption and keys which will be used for the actual data transfer through IPSec is negotiated between the client and the gateway, this

TABLE 1

Technical comparison of site to site VPN vs. Remote access VPN

Site to site VPN	Remote access VPN
Does not require any client software	Requires Client Software
VPN Router is required in the client side	VPN Router is not required
All systems in the client side can be connected to the VPN	Only the system which is provided with remote client can be connected
Encryption is done by the VPN Router	Encryption is done by the remote access client
Username and password is not required for connecting to central server	Username and password is required
Requires a dedicated service provider for VPN communication	Can be connected through any service provider
Connection is through a dedicated VPN channel	Connection is through public Internet
Common protocols used are GRE,MPLS VPN, IPSec	Common Protocols used are PPTP,L2TP, IPsec and SSL VPN
Central server can directly connect to the remote site	Central server cannot directly connect to the remote site
Connection is always present	Connection is initiated and terminated by the remote client

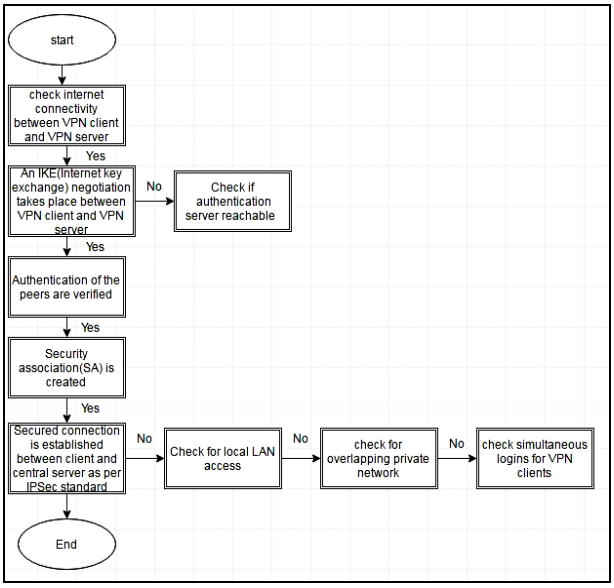

Fig. 4. Flow chart for implementing remote access VPN

agreement is encrypted by the IKE SA which is created in the first phase. The Key material transferred between the peers in second phase is used for creating an IPsec SA which is an agreement of keys and encryption to be used during IPSec data transfer. By having a two phase encryption, the keys and encryption method used for data transfer in the VPN tunnel is secured.

The security gateway has the ability to set access control and policies for different users and groups. These policies are set of rules which define how a client can access to the network through security gateway. The access for a client in radar station can be restricted to the central server machine where the raw data and gif images can be uploaded. This makes it more secure that the client cannot access any another machine in the private network except for which it is expected to connect. Additionally, protocol specific access can be provided in the security gateway like File Transfer protocol for transferring files.

4. Case study

The radar station located in the Kailasagiri Hill, Visakhapatnam can be taken for a case study. There is a service provider exchange on top of the Hill which is connected to another exchange at the base of the hill through underground cables. The connection provided to the radar station is Fiber to the Home (FTTH) where an optical fiber runs from the service provider exchange on top of the hill to the radar station through an overhead cable. A modem is present in the radar station which has an optical fiber at one end and Ethernet ports at the other. The FTTH connection has two points of failure; it could be the overhead cable between exchange at hill top and radar station or underground cables from exchange at base to the exchange at hill top. In case of failure the restoration time is long due to the fact that it is a hilly region and heavy manual work involved. In order to have a backup communication a mobile modem is used whenever the FTTH fails. This mobile modem is used during cyclones and bad weather situations to prevent loss of data transfer to the central server. The mobile modem is wire less and less affected by failures. When using the mobile broadband the data can be sent only through public Internet and not through a secured VPN connection. If a remote access VPN is used the data can be transferred securely through the mobile broadband connection. In Kailasagiri Radar station a Hybrid model can be used where a site to site VPN can be setup through FTTH and a remote access VPN through Mobile broadband connection.

5. Conclusions

Though Site to site VPN provides a secure connection between the central server and the LAN

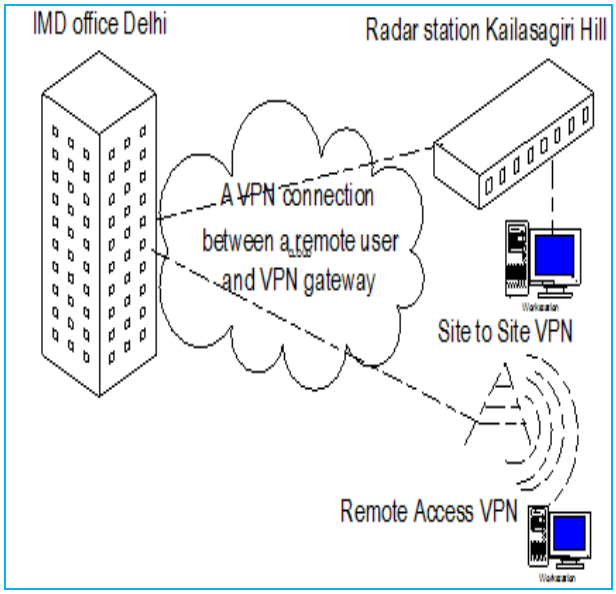

Fig. 5. Proposed hybrid set up for radar station.

network in the radar station, It has dependencies upon the Router hardware in the Radar station which needs to be upgraded every time the speed of the link has to be increased; the VPN connectivity is dependent on the service provider. Usually the Radar stations are connected with only service provider and in case of the failure of services by the service provider the communication is disconnected. It is not possible to use a backup Mobile modem to connect to the internet as site to site VPN. Site to site VPN is of very much use in Regional Meteorological Centre (RMC), Meteorological Centre (MC) and Aviation Meteorological offices where many systems are connected to the central server for uploading and downloading data and it is required that the LAN network of the office needs to be connected to the central server. In radar stations co-located with the RMC and MC, the server of the radar is also present in the LAN network and data transfer can happen through the site to site VPN. But most of the existing radars and proposed ones are situated independently in remote locations where communication still remains a challenge. Radar stations having the need of only a single point option of uploading and downloading the radar data also offers an opportunity to explore Remote access VPN which in turn can be used in mobile modems. Mobile communication speeds have increased steadily and it can be used to send the radar data in a secured manner through remote access VPN. The complete change over from site to site VPN to remote access VPN maybe not be a good solution as significant investments have been involved in the setting up of site to site VPN routers and installation. The current communication system can be modified to a hybrid model where site to site VPN is used as a primary communication with one service provider and remote access VPN as secondary communication with another service provider. This creates a backup communication system in radar stations and also an opportunity for a long time study of reliability, limitations and effectiveness of remote access VPN in radar stations. In proposed radar stations which may be located in remote areas, there could be delays in the setting up the wired communication infrastructure and VPN connectivity. Here remote access VPN can be used as primary communication till the wired communication infrastructure is setup as the process for acquiring a mobile modem and client software installation is much easier. In future, on assessing the performance of remote access VPN and increased coverage of mobile communication, the primary and secondary communication at radar can be made by mobile modems with different service providers. Remote access VPN also has limitations as it provides connectivity only from a single system to the central gateway. A complete LAN network cannot be connected to the central server using a single remote access VPN connection. Usage of mobile communication is dependent on the signal coverage by the respective service providers. In the current scenario, the best option would be to use a hybrid model of both site-to- site and remote access VPN in parallel which utilizes the features of both the configuration and also provides redundancy.

Acknowledgments

Authors are thankful to the Director General of Meteorology, New Delhi, Deputy Director General of Meteorology (UAID) and Deputy Director General of Meteorology (ISSD) for extending their support and providing the facilities to carry out the work. The contents and views expressed in this research paper/article are the views of the authors and do not necessarily reflect the views of India Meteorological Department.

References

A Review on IPsec and SSL VPN Baljot Kaur Chawla, O. P. Gupta, B. K. Sawhney (https://www.ijser.org/researchpaper/A-Review-on-IPsec-and-SSL-VPN.pdf), 2014.

Analysis and Comparison of major mechanisms implementing Virtual Private Networks, Anupriya Shrivastava, M A Rizvi (http://ijarcet.org/wp-content/uploads/IJARCET-VOL-3-ISSUE-7-2374-2381.pdf)

Checkpoint Admin Guide (sc1.checkpoint.com/documents/R77/CP_R77_VPN_AdminGuide/85469).

Checkpoint Admin Guide sc1.checkpoint.com/documents/R77/CP_R77_VPN_AdminGuide/73680.

Defining a VPN (http://scitechconnect.elsevier.com/wp-content/uploads/2013/09/Defining-a-VPN.pdf)

Extending your Business Network through a Virtual Private Network (VPN), Kaleb Fornero (https://www.sans.org/reading-room/whitepapers/vpns/extending-business-network-virtual-private-network-vpn-36985)

Investigation of different VPN Solutions And Comparison of MPLS, IPSec and SSL based VPN Solutions, Sheikh Riaz Ur Rehman(https://www.diva-portal.org/smash/get/diva2:830670/FULLTEXT01.pdf).

Remote Access VPN - Security Concerns and Policy Enforcement, Michael Stines, (https://www.sans.org/reading-room/whitepapers/ vpns/remote-access-vpn-security-concerns-policy-enforcement-881)

Technet library, Remote access VPN **(**Technet.microsoft.com/en-us/library/cc958048).

Virtual Private Networking, A White Paper, Mike Ellsworth (http://stratvantage.com/google/ACNvpnanalysis.pdf)

VPN Scenarios, Configuration and Analysis, Rodoya Takele Degefa (https://publications.theseus.fi/bitstream/handle/10024/98730/RODOYA%20TAKELE.pdf?sequence=1),2015

VPN Security (https://www.infosec.gov.hk/english/technical/files/vpn.pdf)

Wikipedia (https://en.wikipedia.org/wiki/Virtual_private_network)