Volume 5, Issue 9, September 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Network Virtualization & Modeling of VPN Security

Mehzabul Hoque Nahid
Lecture, department of MIS, American International University,
Bangladesh (AIUB)

Abstract*— A virtual private network (VPN) is a method for the extension of a private network across a public network, such as the Internet. It enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network, and thus are benefiting from the functionality, security and management policies of the private network. A VPN is created by establishing a virtual point-to-point connection through the use of dedicated connections, virtual tunneling protocols, or traffic encryption. A VPN spanning the Internet is similar to a wide area network (WAN). From a user perspective, the extended network resources are accessed in the same way as resources available within the private network. Traditional VPNs are characterized by a point-to-point topology, and they do not tend to support or connect broadcast domains. Therefore, communication, software, and networking, which are based on OSI layer 2 and broadcast packets, such as NetBIOS used in Windows networking, may not be fully supported or work exactly as they would on a local area network (LAN). VPN variants, such as Virtual Private LAN Service (VPLS), and layer 2 tunneling protocols, are designed to overcome this limitation. Our main objective is design VPN network and explain it.

Keywords*— VPN, ISP, Network, QOS, DSL.

I. INTRODUCTION

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 tunnelling protocol and security procedures. A virtual private network can be contrasted with a system of owned or leased lines that can only be used by one company. 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. Phone companies have provided private shared resources for voice messages for over a decade. A virtual private network makes it possible to have the same protected sharing of public resources for data. Companies today are looking at using a private virtual network for both extranets and wide-area intranets. Before the Internet became nearly-universal, a virtual private network consisted of one or more circuits leased from a communications provider. Each leased circuit acted like a single wire in a network that was controlled by customer [1]. The communications vendor would sometimes also help manage the customer's network, but the basic idea was that a customer could use these leased circuits in the same way that they used physical cables in their local network. The privacy afforded by these legacy VPNs was only that the communications provider assured the customer that no one else would use the same circuit. This allowed customers to have their own IP addressing and their own security policies [2]. A leased circuit ran through one or more communications switches, any of which could be compromised by someone wanting to observe the network traffic. The VPN customer trusted the VPN provider to maintain the integrity of the circuits and to use the best available business practices to avoid snooping of the network traffic. As the Internet became more popular as a corporate communications medium, security became much more of a pressing issue for both customers and providers. Seeing that 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. Networks that are constructed using encryption. More recently, service providers have begun to offer a new type of trusted VPNs, this time using the Internet instead of the raw telephone system as the substrate for communications. These new trusted VPNs still do not offer security, but they give customers a way to easily create network segments for wide area networks (WANs). In addition, trusted VPN segments can be controlled from a single place, and often come with guaranteed quality-of-service (QoS) from the provider. A secure VPN can be run as part of a trusted VPN, creating a third type of VPN that is very new on the market: hybrid VPNs. The secure parts of a hybrid VPN might be controlled by the customer (such as by using secure VPN equipment on their sites) or by the same provider that provides the trusted part of the hybrid VPN. Sometimes an entire hybrid VPN is secured with the secure VPN, but more commonly, only a part of a hybrid VPN is secure.

VPNs allow employees to securely access the corporate intranet while traveling outside the office. Similarly, VPNs securely connect geographically separated offices of an organization, creating one cohesive network [3]. VPN technology is also used by individual Internet users to secure their wireless transactions, to circumvent geo restrictions and censorship, and to connect to proxy servers for the purpose of protecting personal identity and location.

II. TYPES OF VPN

Early data networks allowed VPN-style remote connectivity through dial-up modems or through leased line connections utilizing Frame Relay and Asynchronous Transfer Mode (ATM) virtual circuits, provisioned through a network owned and operated by telecommunication carriers. These networks are not considered true VPNs because they passively secure the data being transmitted by the creation of logical data streams. They have been replaced by VPNs based on IP and IP/Multiprotocol Label Switching (MPLS) Networks, due to significant cost-reductions and increased bandwidth provided by new technologies such as Digital Subscriber Line (DSL) and fibre-optic networks [4].

VPNs can be either remote-access or site-to-site. In a corporate setting, remote-access VPNs allow employees to access their company's intranet from home or while traveling outside the office, and site-to-site VPNs allow employees in geographically disparate offices to share one cohesive virtual network. A VPN can also be used to interconnect two similar networks over a dissimilar middle network; for example, two IPv6 networks over an IPv4 network.

VPN systems may be classified by:

- The protocols used to tunnel the traffic
- The tunnel's termination point location, e.g., on the customer edge or network-provider edge
- Whether they offer site-to-site or network-to-network connectivity
- The levels of security provided
- The OSI layer they present to the connecting network, such as Layer 2 circuits or Layer 3 network connectivity
- The OSI model has seven layers

III. SECURITY MECHANISM

VPNs cannot make online connections completely anonymous, but they can usually increase privacy and security. To prevent disclosure of private information, VPNs typically allow only authenticated remote access and make use of encryption techniques. VPNs provide security by the use of tunnelling protocols and often through procedures such as encryption. The VPN security model provides: information security [5].

- Confidentiality such that even if the network traffic is sniffed at the packet level an attacker would only see encrypted data
- Sender authentication to prevent unauthorized users from accessing the VPN
- Message integrity to detect any instances of tampering with transmitted messages

Secure VPN protocols include the following:

- Internet Protocol Security (IPsec) as initially developed by the Internet Engineering Task Force (IETF) for IPv6, which was required in all standards-compliant implementations of IPv6 before RFC 6434 made it only a recommendation. This standards-based security protocol is also widely used with IPv4 and the Layer 2 Tunnelling Protocol. Its design meets most security goals: authentication, integrity, and confidentiality. IPsec uses encryption, encapsulating an IP packet inside an IPsec packet [6]. De-encapsulation happens at the end of the tunnel, where the original IP packet is decrypted and forwarded to its intended destination.
- Transport Layer Security (SSL/TLS) can tunnel an entire network's traffic or secure an individual connection. A number of vendors provide remote-access VPN capabilities through SSL. An SSL VPN can connect from locations where IPsec runs into trouble with Network Address Translation and firewall rules.
- Datagram Transport Layer Security (DTLS) - used in Cisco Any Connect VPN and in Open Connect VPN to solve the issues SSL/TLS has with tunnelling over UDP.
- Microsoft Point-to-Point Encryption (MPPE) works with the Point-to-Point Tunnelling Protocol and in several compatible implementations on other platforms.
- Microsoft Secure Socket Tunnelling Protocol (SSTP) tunnels Point-to-Point Protocol (PPP) or Layer 2 Tunnelling Protocol traffic through an SSL 3.0 channel.
- Multi Path Virtual Private Network (MPVPN). Regular Systems Development Company owns the registered trademark "MPVPN".
- Secure Shell (SSH) VPN – Open SSH offers VPN tunnelling to secure remote connections to a network or to inter-network links. Open SSH server provides a limited number of concurrent tunnels. The VPN feature itself does not support personal authentication [7].

IV. TROUBLESHOOT VPN CONNECTION

Troubleshooting VPN connection issues typically involves contacting internet service provider (ISP), your VPN server administrator, or your router or firewall manufacturer. When try to connect to VPN server, it may not be able to connect, and may receive an error message that resembles the following:

678: The remote computer did not respond.

930: The authentication server did not respond to authentication requests in a timely fashion.

800: Unable to establish the VPN connection.

623: The system could not find the phone book entry for this connection.

720: A connection to the remote computer could not be established.

To resolve this issue, use one of the following methods:

- Verify that connected to the Internet before try to connect to the VPN server.
  314067 How to troubleshoot TCP/IP connectivity with Windows XP
  314095 How to troubleshoot possible causes of Internet connection problems in Windows XP
- If someone can connect to the Internet but still cannot establish a connection to the VPN server, and you receive error 623, see the following Microsoft Knowledge Base article:
  227391 Error message: "Error 623 the system could not find the phone book entry for this connection" when making a VPN connection
- If someone can connect to the Internet but still cannot establish a connection to the VPN server, and you receive error 720, see the following Microsoft Knowledge Base article:
  314869 Error 720: No PPP control protocols configured
- If someone still cannot connect to the VPN server, the VPN server may not be configured correctly. Contact your VPN server administrator.
  308208 How to install and configure a virtual private network server in Windows 2000
  162847 Troubleshooting PPTP connectivity issues in Windows NT 4.0
  299684 Error message: Error 930; the authentication server did not respond to authentication requests in a timely fashion.

V. VPN ON ROUTER

With the increasing use of VPNs, many have started deploying VPN connectivity on routers for additional security and encryption of data transmission by using various cryptographic techniques. Setting up VPN services on a router will allow any connected device(s) to use the VPN network while it is enabled [8]. This also makes it easy to set up VPNs on devices that do not have native VPN clients such as Smart-TVs, Gaming Consoles etc. Provisioning VPN on the routers will also help in cost savings and network scalability.

Many router manufacturers like Cisco Linksys, Asus and Net gear supply their routers with built-in VPN clients. Since these routers do not support all the major VPN protocols, such as Open VPN, many tend to flash their routers with alternative open source firm wares such as DD-WRT, Openwork and Tomato which support multiple VPN protocols such as PPTP and Open VPN [9].

VI. DESIGN & MODELLING

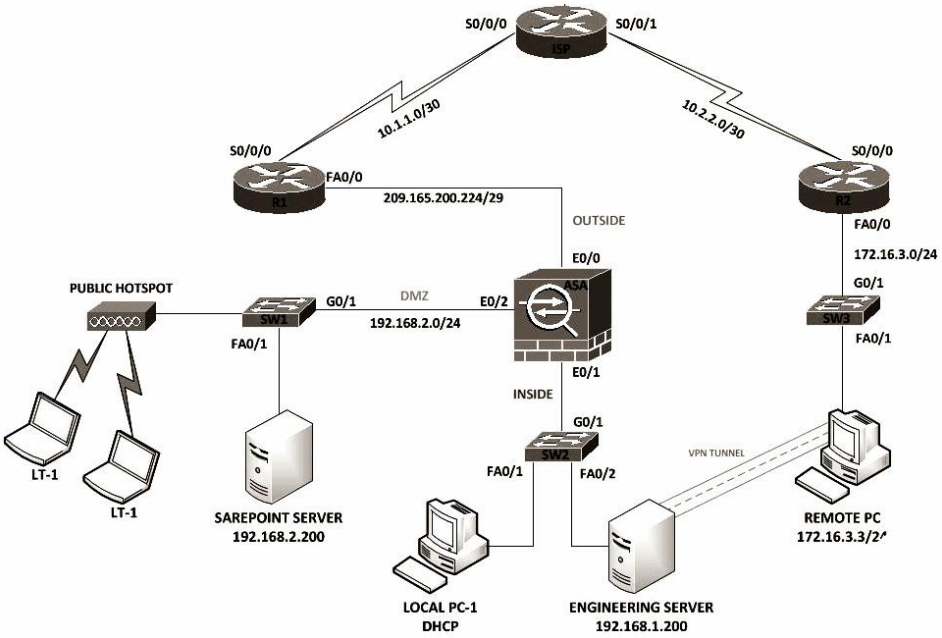

Figure 1: ASA VPN Design

The ASA 5500 series VPN Edition offers the growing list of Any Connect industry-leading Secure Mobility features and the simplicity and ubiquity of clientless secure access. The ASA – Any Connect Secure Mobility solution is easy to deploy and simple to use. Its client and clientless options respond securely and dynamically to today's wide array of fixed and mobile endpoint requirements by offering granular access controls and robust endpoint security. As a result, it maintains the integrity of confidential information to solve the unique challenges associated with diverse user groups and endpoints accessing the enterprise network. The Any Connect Secure Mobility solution also offers integrated web security protection via the Any Connect client. By seamlessly redirecting select traffic to either an on premise appliance, or to a cloud-based service for off-VPN web traffic protection, the Any Connect client provides consistent policy and security without having to backhaul public Internet-bound traffic.

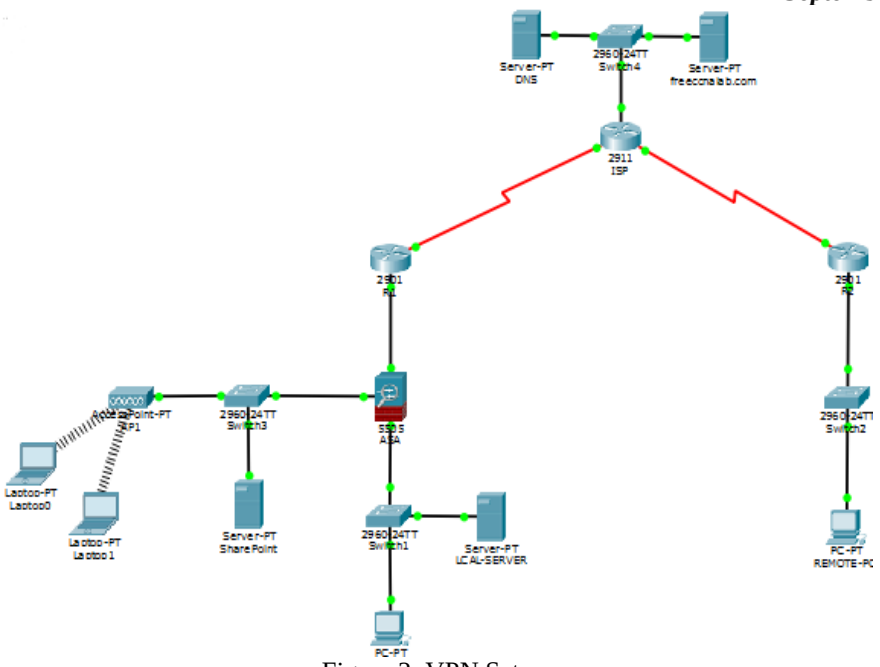

Figure 2: VPN Setup

When setting up incoming PPTP VPN connections in Windows, must configure network router to forward VPN traffic to the Windows computer we want to access remotely. We can do this by logging in to the router's control panel consult the manufacturer's instructions on how to do this and configuring the port-forwarding or virtual-server settings to forward port 1723 to the IP address of the computer you wish to access. In addition, PPTP or VPN pass-through options need to be enabled in the firewall settings, but usually they're switched on by default.

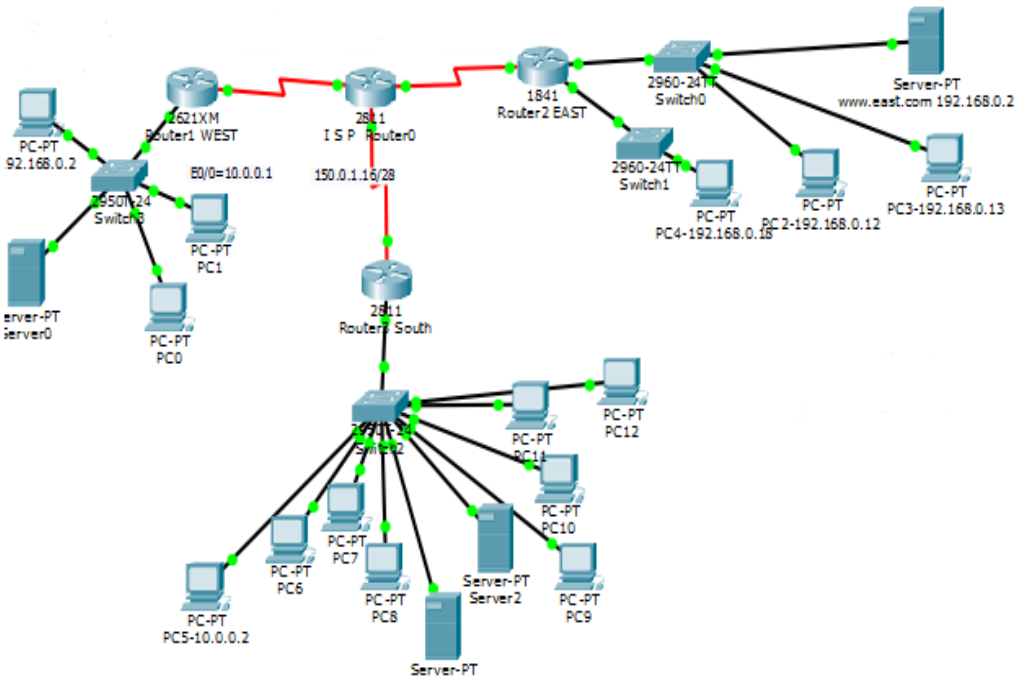

Figure 3: ISP VPN

ISP will only see encrypted information. A VPN is a great way to prevent marketers or ISP from tracking history and online activity. Our ISP may attempt to limit your bandwidth, and having a VPN that provides them with only encrypted information can help us avoid bandwidth limits from ISP. Marketers who would track activity to target for particular advertisements will also be thwarted in their efforts because we will surf using a new IP address every time connect to our servers, and we can even change your server location. Hackers who would look to steal your information are also stopped by Octane VPN. Our information is encrypted and hidden behind our service so hackers cannot gain access to usernames, passwords, emails, and other sensitive information they may use to steal identity, place unauthorized purchases, or harm in other ways. Those who use public connections such as Wi-Fi hotspots in airports, coffee shops, and more, such as frequent travellers, may find this added security beneficial.

Our own hardware versus paying a VPN provider like Tunnel Bear to provide us with VPN service and a convenient app. We could host our own VPN server with a web hosting provider, and this may actually be a few bucks cheaper a month

than going with a dedicated VPN provider. We will pay the hosting provider for server hosting and install a VPN server on the server they've provided to us. Depending on the hosting provider we've chosen, this can be a quick point-and-click process where we add the VPN server software and get a control panel to manage it, or it may require pulling up a command-line to install and configure everything from scratch.

Be sure to configure our VPN server securely. We will want strong security so no one else can connect to VPN. Even a strong password might not be ideal an Open VPN server with a key file that need to connect would be strong authentication, for example.

VII. IP CONFIGURATION

```
ASA Version 8.4(1)
!
hostname ASA
names
!
interface Ethernet0/0
 switchport access vlan 2
!
interface Ethernet0/1
 switchport access vlan 1
!
interface Ethernet0/2
 switchport access vlan 3
!
interface Ethernet0/3
 switchport access vlan 1
!
interface Ethernet0/4
 switchport access vlan 1
!
interface Ethernet0/5
 switchport access vlan 1
!
interface Ethernet0/6
 switchport access vlan 1
!
interface Ethernet0/7
 switchport access vlan 1
!
interface Vlan1
 nameif inside
 security-level 100
 ip address 192.168.1.1 255.255.255.0
!
interface Vlan2
 nameif outside
 security-level 0
 ip address 209.165.200.226 255.255.255.248
!
interface Vlan3
 no forward interface Vlan1
 nameif dmz
 security-level 50
 ip address 192.168.2.1 255.255.255.0
!
webvpn
 enable outside
object network dmz-subnet
 subnet 192.168.2.0 255.255.255.0
object network inside-subnet
 subnet 192.168.1.0 255.255.255.0
!
route outside 0.0.0.0 0.0.0.0 209.165.200.225 1
object network dmz-subnet
```



```
 nat (dmz,outside) dynamic interface
object network inside-subnet
 nat (inside,outside) dynamic interface
!
group-policy remote_users internal
group-policy remote_users attributes
 vpn-tunnel-protocol ssl-clientless
 webvpn
  url-list value Engineering
username client password 4IncP7vTjpaba2aF encrypted
username client attributes
 Vpn-group-policy remote users
!
class-map global-class
 match default-inspection-traffic
!
policy-map global-policy
 class global-class
  inspect dns
  inspect ftp
  inspect h323
  inspect http
  inspect icmp
  inspect tftp
!
Service-policy global-policy global
!
Telnet timeout 5
ssh timeout 5
!
dhcpd address 192.168.1.1-192.168.1.99 inside
dhcpd dns 209.165.200.10 interface inside
dhcpd enable inside
!
dhcpd auto_config outside
!
dhcpd address 192.168.2.10-192.168.2.100 dmz
dhcpd dns 209.165.200.10 interface dmz
dhcpd enable dmz
!
Tunnel-group Client-Profile type remote-access
Tunnel-group Client-Profile general-attributes
 Default-group-policy remote users
```

VIII. CONCLUSIONS

A VPN is also a great service for those who wish to access websites not available in their home country or the country in which they are currently traveling. Some websites restrict access to certain users in particular countries, or prevent users in particular countries from access. A VPN allows you to change your location to that of another country that may be able to access the website. This is particularly beneficial to travellers who wish to continue to access websites from their home country. VPN may even be beneficial to those who wish to bypass their company's firewall security. Employers may place firewalls to prevent their employees from accessing certain websites while they are at work. A VPN will allow you to get around this and other attempts at censorship. Not every router compatible with open source firmware which depends on the built-in flash memory and processor. Firm wares like DD-WRT require a minimum of 2 MB flash memory and Broadcom chipsets. Setting up VPN services on a router requires a deeper knowledge of network security and careful installation. Minor misconfiguration of VPN connections can leave the network vulnerable. Performance will vary depending on the ISP and their reliability.

ACKNOWLEDGMENT

The author gratefully wishes to acknowledge Ahmed Abdullah, lecturer, Royal University of Dhaka, for his assistance configuring IP with Packet Tracer version 6.2 which has been used in designing and modelling of VPN security in this paper.

REFERENCES

[1] Lewis, Mark (2006). Comparing, designing, and deploying VPNs (1st print. Ed.). Indianapolis, Ind.: Cisco Press. pp. 5–6. ISBN 1587051796.
[2] Glyn M Burton: RFC 3378 Ether IP with FreeBSD, 03 February 2011
[3] net-security.org news: Multi-protocol Soft Ether VPN becomes open source, January 2014
[4] Address Allocation for Private Internets, RFC 1918, Y. Rekhter *et al.*, and February 1996
[5] Cisco Systems, Inc. (2004). Internetworking Technologies Handbook. Networking Technology Series (4 Ed.). Cisco Press. p. 233. ISBN 9781587051197. Retrieved 2013-02-15.
[6] Layer Two Tunneling Protocol "L2TP", RFC 2661, W. Townsley et al., August 1999
[7] IP Based Virtual Private Networks, RFC 2341, A. Valencia et al., and May 1998
[8] Point-to-Point Tunneling Protocol (PPTP), RFC 2637, K. Hamzeh et al., July 1999
[9] Phifer, Lisa. "Mobile VPN: Closing the Gap", SearchMobileComputing.com, July 16, 2006.

