Asian Journal of Computer Science and Technology
ISSN: 2249-0701 (P) Vol.7 No.2, 2018, pp.30-33
© The Research Publication, www.trp.org.in
DOI: https://doi.org/10.51983/ajcst-2018.7.2.1886

Cisco Secured Virtual Private Networks: A Review

Yusera Farooq Khan
Computer Science and Engineering, School of Engineering and Technology,
Baba Ghulam Shah Badshah University, Rajouri, Jammu and Kashmir, India
E-Mail: yusrakhan.205@gmail.com

(Received 30 May 2018; Revised 20 June 2018; Accepted 10 July 2018; Available online 17 July 2018)

***Abstract* - Now-a-days the significance of security has been greater than before because of the fact that data has been accessed and transferred through public network. The data which has been transferred could be sniffed which may be a loss for us. When data is transferred in to public network we need confidentiality, integration and authentication. In this review paper we will discuss all these factors that keep our data safe enough. In order to provide this factor a site-to-site virtual private network has been designed which provide more security to data and made the public network into private network. The virtual private network hides the source and destination address as well as it also hides the internal network so that our network would be safe enough.**

***Keywords:* confidentiality, authentication, hashing, security, sniffed**

I. INTRODUCTION

In this day and age networks are everywhere, especially in the form of internet. The internet, the ultimate network is itself is an enormous network which has revolutionized the world. In this discussion of networking, it is very useful to take a look at the networking from a higher level. A network is simply a collection of computers and other hardware device that are connected to each other either physically or logically , using special hard ware and soft ware that allows the devices to exchange information . networks connects computers and their users through LANs, MANs and WANs. One of the most important use of networking is sharing of data.

A. Routing

Routing is the process of selecting path for traffic across a network or multiple networks from one host to another [5] . Packets are the fundamental units of information transported in computer networks and other communication networks. Routing is a key feature of the internet.

B. Routing protocol

Specifies how routers communicate with each other, distributing information that enables them to select routes between any two nodes on a computer network. Routing algorithms determine the specific choice of route. Each router has a prior knowledge only of networks attached to it directly.

A routing protocol shares this information first among immediate neighbours, and then throughout the network[5]. This way, routers gain knowledge of the topology of the network.

The specific characteristics of routing protocols include the manner in which they avoid routing loops, the manner in which they select preferred routes, using information about hop costs, their scalability, and other factors [6].

II. VIRTUAL PRIVATE NETWORK

Virtual private networks (VPN) extends a private network across a public network and enable users to send and receive data across shared or public networks as if their computing devices were directly connected to private network. In simple terms [1], it creates a secure, encrypted connection which can be thought of a tunnel , between a computer and server operated by VPN service .

Formally we can define Virtual Private Network (VPN) as follows:
“A network is formed by applying virtualization on public physical network infrastructure in such a way that the users are able to use it as a private or user-owned 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 available from the public internet can provide some of the benefits of wide area networks.

A. Types of VPN

VPN can be either remote Access (connecting a computer to a network or site-to-site (connecting two networks). In a corporate setting, remote access VPN allows employees to access their companies intranet from home or while travelling outside the office and in site-to-site VPNs allow employees in geographically disparate offices to share one cohesive virtual network.

B. VPN Security Mechanism

VPNs cannot make online connection completely anonymous, but they can usually increase privacy and security. To prevent disclosure of private information, VPNs typically allow authenticated remote access using tunneling protocols and encryption techniques[12] . The VPN security model provides:

1. Confidentiality

Such that even if the network traffic is sniffed in 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.

2. Authentication

Tunnel end points must b authenticated before secure VPN tunnel can be established. User created remote access VPNs may use password , biometrics , two factors authentication or other cryptographic methods .

3. *Network*

To network tunnels often use passwords or digital certificates. They permanently store the key to allow tunnel to establish automatically, without intervention from the administrator.

4. Routing

VPN routing provides a way of controlling how VPN traffic is directed. VPN routing can be implemented with security gateway modules and remote access clients.

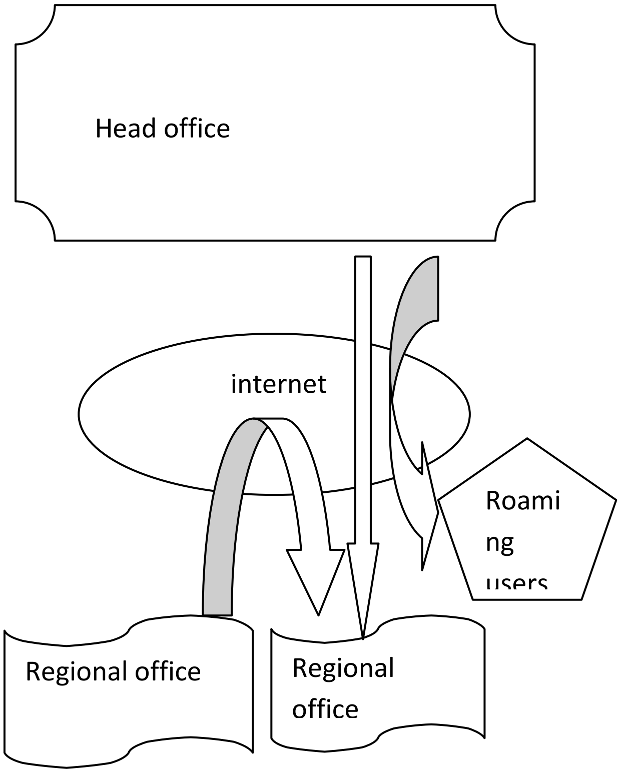

Fig. 1 Internet VPN

III. CISCO ASA REMOTE ACCESS VPN

The Cisco IOS (network operating system) is a command line interface used by current Cisco routers and catalyst switches .This IOS provides the mechanism to configure all layer 2 and layer 3 functions on Cisco devices. The IOS is structured into several modes, which contain set of commands specific to the function of that mode.

The remote user requires the Cisco VPN client Software on his/her computer , once the connection is established the user will receive a private IP address from the ASA(adaptive Security Appliances) and has access to the network. the Cisco VPN client is end-of-life and has been replaced by the Cisco any connect secure mobility client. The ASA has two interfaces inside and outside.

A. Configuration

1.VPN pool

First configure a pool with IP address that will be assigned to remote VPN users and then user IP address for our VPN users. We need to tell ASA that we will use local pool for remote VPN users.

2. NAT Exemption

If we have NAT enabled on the ASA them we need to make sure that traffic between the local network and our remote VPN user does not get translated . To accomplish this we will configure NAT exemption.

3. Group policy

When the remote user has established the VPN , they will b unable to access anything ion the internet , only the remote network is reachable . for security reasons this is a good practice as it forces you to send all traffic through ASA . if you do not want this then you can enable split tunneling. with split tunneling enables , we will use the VPN only for access to remote network .

IV. INTERESTING TRAFFIC INITIATES THE IPSEC PROCESS

IPSec involves many component technologies and encryption methods. IPSec operation is breakdown into five main steps [25]. Traffic is deemed interesting when the IPSec security policy configures in the IPSec peers starts the IKE(internet key Exchange) process [25]. Internet Key Exchange is the protocol used to set up a security association (SA) in the IPsec protocol suite.

IKE phase 1: IKE authenticates IPSec peers and negotiates IKE SAs during this phase, setting up a secure channel for negotiating IPSec SAs in phase 2.

IKE phase 2: IKE negotiates IPSec SA parameters and sets up matching IPSec SAs in the peers.

Data transfer: Data is transferred between IPSec peers based on the IPSec parameters and keys stored in the SA database.

IPSec tunnel termination: IPSec SAs terminate through deletion or by timing out.

Step 1: Defining Interesting Traffic

What type of traffic is deemed *interesting* is determined as part of formulating a security policy for use of a VPN. The policy is then implemented in the configuration interface for each particular IPSec peer. For example, in Cisco routers and PIX Firewalls, access lists are used to determine the traffic to encrypt. The access lists are assigned to a cryptography policy; the policy's *permit statements* indicate that the selected traffic must be encrypted, and *deny statements* indicate that the selected traffic must be sent unencrypted. With the Cisco Secure VPN Client, you use menu windows to select connections to be secured by IPSec [26].

When interesting traffic is generated or transits the IPSec client, the client initiates the next step in the process, negotiating an IKE phase 1 exchange.

Step 2: IKE Phase 1

The basic purpose of IKE phase 1 is to authenticate the IPSec peers and to set up a secure channel between the peers to enable IKE exchanges. IKE phase 1 performs the following functions:

1. Authenticates and protects the identities of the IPSec peers
2. Negotiates a matching IKE SA policy between peers to protect the IKE exchange
3. Performs an authenticated Diffie-Hellman exchange with the end result of having matching shared secret keys
4. Sets up a secure tunnel to negotiate IKE phase 2 parameters

IKE phase 1 occurs in two modes: main mode and aggressive mode. These modes are described in the following sections.

Main Mode: It has three two-way exchanges between the initiator and the receiver.

1. First exchange: The algorithms and hashes used to secure the IKE communications are agreed upon in matching IKE SAs in each peer.
2. Second exchange: Uses a Diffie-Hellman exchange to generate shared secret keying material used to generate shared secret keys and to pass nonces—random numbers sent to the other party and then signed and returned to prove their identity.
3. Third exchange: Verifies the other side's identity. The identity value is the IPSec peer's IP address in encrypted form. The main outcome of main mode is matching IKE SAs between peers to provide a protected pipe for subsequent protected ISAKMP exchanges between the IKE peers. The IKE SA specifies values for the IKE exchange: the authentication method used, the encryption and hash algorithms, the Diffie-Hellman group used, the lifetime of the IKE SA in seconds or kilobytes, and the shared secret key values for the encryption algorithms. The IKE SA in each peer is bi-directional

Aggressive Mode: In aggressive mode, fewer exchanges are made, and with fewer packets. On the first exchange, almost everything is squeezed into the proposed IKE SA values: the Diffie-Hellman public key; a nonce that the other party signs; and an identity packet, which can be used to verify identity via a third party[22]. The receiver sends everything back that is needed to complete the exchange. The only thing left is for the initiator to confirm the exchange. The weakness of using the aggressive mode is that both sides have exchanged information before there's a secure channel. Therefore, it's possible to "sniff" the wire and discover who formed the new SA. However, it is faster than main mode.

Step 3: IKE Phase 2

The purpose of IKE phase 2 is to negotiate IPSec SAs to set up the IPSec tunnel. IKE phase 2 performs the following functions:

1. Negotiates IPSec SA parameters protected by an existing IKE SA
2. Establishes IPSec security associations
3. Periodically renegotiates IPSec SAs to ensure security
4. Optionally performs an additional Diffie-Hellman exchange

IKE phase 2 has one mode, called quick mode. Quick mode occurs after IKE has established the secure tunnel in phase 1. It negotiates a shared IPSec policy, derives shared secret keying material used for the IPSec security algorithms, and establishes IPSec SAs. Quick mode exchanges nonces that provide replay protection. The nonces are used to generate new shared secret key material and prevent replay attacks from generating bogus SAs.

Step 4: IPSec Encrypted Tunnel

After IKE phase 2 is complete and quick mode has established IPSec SAs, information is exchanged via an IPSec tunnel. Packets are encrypted and decrypted using the encryption specified in the IPSec SA.

Step 5: Tunnel Termination

IPSec SAs terminate through deletion or by timing out . An SA can time out when a specified number of seconds have elapsed or when a specified number of bytes have passed through the tunnel. When the SAs terminate, the keys are also discarded. When subsequent IPSec SAs are needed for a flow, IKE performs a new phase 2 and, if necessary, a new phase 1 negotiation. A successful negotiation results in new SAs and new keys [23]. New SAs can be established before the existing SAs expire, so that a given flow can continue uninterrupted.

V. CONCLUSION

With the recent accessibility of high-speed Internet connections to the home and the continued move of workers out of central office locations (whether for travel, or branch office expansion), virtual private networks (VPNs) have become a significant part of commercial network architectures. VPNs use highly developed encryption and tunnelling to permit our association to establish secure, end-to-end, private network connections over third-party networks, such as the Internet. This new networking standard not only adds to the effectiveness of the corporate workforce, but save money by leveraging third-party networks and allows us to scale our networks with greater ease. Cisco Secure Virtual Private Networks provides a complete solution for designing, implementing, and managing VPN networks and help us to make the most efficient use of your VPN.

REFERENCES

[1] M. Erwin, C. Scott and Wolfe, "*Virtual Private Networks*", Sebastopol CA: O'Rielly & Associates Inc. 1999.

[2] J. H Carmouche, "*IPsec Virtual Prive Network Fundamentals*" Indianapolis: Cisco Press , 2007.

[3] J. S. Tiller, "*A technical Guide to IPSec Virtual Private Networks*" New York: Auerbach Publications, 2001.

[4] V. C. Perta, M. V. Barbera, G. Tyson, H. Haddadi and A. Mei, "A Glance through the VPN Looking Glass: IPv6 Leakage and DNS Hijacking in Commercial VPN Clients", *PETS*, 2015.

[5] D. Waitzman, C. Partridge and S. Deering, "Distance Vector Multicast Routing Protocol", RFC1075, November, 1988.

[6] S. Hanks, T. Li, D. Farinacci and P. Traina, "*Generic Routing Encapsulation*", RFC1701, October 1994.

[7] Baohong He, Tianhui, "*Technology of IPSec VPN [M]*", Beijing: Posts & Telecom press, 2008, 7.

[8] C. Metz, "The Latest in Virtual Private Networks: Part II," *IEEE Internet Computing*, May – June, 2004.

[9] K.Kompella, Ed., and Y. Rekhter Ed., "Routing Extensions in Support of Generalized Multi-Protocol Label Switching (GMPLS)", *IETF L1VPN RFC 4202*, October 2005.

[10] H. Ould-Brahim and Y. Rekhter, "GVPN Services: Generalized VPN Services Using BGP and GMPLS Toolkit", *IETF L1VPN Internet draft*, February 2005

[11] S. Kent and R. Atkinson, "Security architecture for the Internet Protocol", *RFC (Standards Track) 2401*, 1998

[12] Venkateswaran, "Virtual private networks", *IEEE Potentials Magazine*, Vol. 20, No. 1, Feb-Mar 2001.

[13] H. Ould-Brahim and Y. Rekhter, "GVPN Services: Generalized VPN Services Using BGP and GMPLS Toolkit", *IETF L1VPN Internet draft*, February 2005

[14] http://www.zlin.ba.ttu.edu/doc/vpn-rsvp.ppt

[15] http://www.ijarcsse.com/../V2I900209.pdf

[16] http://www.engpaper.net/vpn-research-paper

[17] http://www.csun.edu/~vcact00f/311/termprojects/330class/vpnpresentation.ppt

[18] National Institute of Standards and Technology: Guide to IPSec VPNs (www.http://csrc.nist.gov/publications/nistpubs/800-77/sp800-77.pdf)

[19] CISCO VPN and VPN technologies, (www.ciscopress.com/articles/article.asp?p=24833&seqNum=6)

[20] CISCO SSL VPN, (http://www.cisco.com/en/US/docs/ios/12_4t/12_4t11/htwebvpn.html)

[21] IPSec and SSL decision Criteria, (http://www.cadincweb.com/wordpress/wpcontent/uploads/2010/11/JuniperIPSec-vs-SSL-VPN.pdf)

[22] White Paper, "Virtual Private Networks: Improving Network Security for a diverse user community". (http://www.pdfio.net/k7234709.html).

[23] L. Phifer, Tunnel Vission: Choosing a VPN-SSL VPN vs IPsec VPN. (http://searchsecurity.techtarget.com/feature/Tunnel-VisionChoosing-a-VPN-SSL-VPN-vs-IP sec-VPN), 2003

[24] A. Hassan Pathan and M. Irshad, "IP Based Virtual Private Network Implementation on Financial Institution and Banking System", pp. 30-34, 2014.

[25] Root, Don and R. Rissler, "IPsec and SSL VPN Decision Criteria A Technology White Paper by Juniper Networks", May, 1-13, 2006.

[26] P.K. Singh and P.P. Singh, "A Novel approach for the Analysis & Issues of IPsec VPN", *International Journal of Sciences and Research*,Vol. 2, No. 7, pp. 187-89, 2013.