Virtual private network essay sample

Technology, Internet

Virtual. Virtual means not real or in a different state of being. In a VPN, private communication between two or more devices is achieved through a public network the Internet. Therefore, the communication is virtually but not physically there. Private. Private means to keep something a secret from the general public. Although those two devices are communicating with each other in a public environment, there is no third party who can interrupt this communication or receive any data that is exchanged between them. Network. A network consists of two or more devices that can freely and electronically communicate with each other via cables and wire. A VPN is a network. It can transmit information over long distances effectively and efficiently. The term VPN has been associated in the past with such remote connectivity services as the (PSTN), Public Switched Telephone Network but VPN networks have finally started to be linked with IP-based data networking. Before IP based networking corporations had expended considerable amounts of time and resources, to set up complex private networks, now commonly called Intranets. These networks were installed using costly leased line services, Frame Relay, and ATM to incorporate remote users.

For the smaller sites and mobile workers on the remote end, companies supplemented their networks with remote access servers or ISDN. Small to medium-sized companies, who could not afford dedicated leased lines, used low-speed switched services. As the Internet became more and more accessible and bandwidth capacities grew, companies began to put their Intranets onto the web and create what are now known as Extranets to link internal and external users. However, as cost-effective and quick-to-deploy as the Internet is, there is one fundamental problem – security. Today’s VPN solutions overcome the security factor using special tunneling protocols and complex encryption procedures, data integrity and privacy is achieved, and the new connection produces what seems to be a dedicated point-to point connection.

And, because these operations occur over a public network, VPNs can cost significantly less to implement than privately owned or leased services. Although early VPNs required extensive expertise to implement, technology has matured to a level where deployment can be a simple and affordable solution for businesses of all sizes. Virtual Simply put, a VPN, Virtual Private Network, is defined as a network that uses public network paths but maintains the security and protection of private networks. For example, Delta Company has two locations, one in Los Angeles, CA (A) and Las Vegas, Nevada (B). In order for both locations to communicate efficiently, Delta Company has the choice to set up private lines between the two locations. Although private lines would restrict public access and extend the use of their bandwidth, it will cost Delta Company a great deal of money since they would have to purchase the communication lines per mile. The more viable option is to implement a VPN. Delta Company can hook their communication lines with a local ISP in both cities. The ISP would act as a middleman, connecting the two locations. This would create an affordable small area network for Delta Company.

VPNs were are broken into 4 categories-

1)Trusted VPN: A customer “ trusted” the leased circuits of a service provider and used it to communicate without interruption. Although it is “ trusted” it is not secured. 2)Secure VPN: With security becoming more of an issue for users, encryption and decryption was used on both ends to safeguard the information passed to and fro. This ensured the security needed to satisfy corporations, customers, and providers. 3)Hybrid VPN: A mix of a secure and trusted VPN. A customer controls the secure parts of the VPN while the provider, such as an ISP, guarantees the trusted aspect. 4)Provider-provisioned VPN: A VPN that is administered by a service provider.

VPN Topology

Next we will look at how a VPN works internally:
To begin using a VPN, an Internet connection is needed; the Internet connection can be leased from an ISP and range from a dial up connection for home users to faster connections for businesses. A specially designed router or switch is then connected to each Internet access circuit to provide access from the origin networks to the VPN. The VPN devices create PVCs (Permanent Virtual Circuit- a virtual circuit that resembles a leased line because it can be dedicated to a single user) through tunnels allowing senders to encapsulate their data in IP packets that hide the underlying routing and switching infrastructure of the Internet from both the senders and receivers.

The VPN device at the sending facility takes the outgoing packet or frame and encapsulates it to move through the VPN tunnel across the Internet to the receiving end. The process of moving the packet using VPN is transparent to both the users, Internet Service Providers and the Internet as a whole. When the packet arrives on the receiving end, another device will strip off the VPN frame and deliver the original packet to the destination network.

VPNs operate at either layer 2 or layer 3 of the OSI model (Open Systems Interconnection). Layer-2 VPN uses the layer 2 frame such as the Ethernet while layer-3 uses layer 3 packets such as IP. Layer-3 VPN starts at layer 3, where it discards the incoming layer-2 frame and generates a new layer-2 frame at the destination. Two of the most widely used protocols for creating layer-2 VPNs over the Internet are: layer-2 tunneling protocol (L2TP) and point-to-point tunneling protocol (PPTP). The newly emerged protocol, called Multiprotocol Label Switching (MPLS) is used exclusively in layer-3 VPNs. See Figure 1

Figure 1. Defined VPN

Note: From A Primer for implementing a Cisco Virtual Private Network © 1999 Cisco systems, Inc All rights Reserved

Types of VPNs

There are currently three types of VPN in use: remote access VPN, intranet VPN, extranet VPN. Remote access VPNs (see figure 2), enables mobile users to establish a connection to an organization server by using the infrastructure provided by an ISP (Internet Services Provider). Remote access VPN allows users to connect to their corporate intranets or extranets wherever or whenever is needed. Users have access to all the resources on the organization’s network as if they are physically located in organization.

The user connects to a local ISP that supports VPN using plain old telephone services (POTS), integrated services digital network (ISDN), digital subscriber line (DSL), etc. The VPN device at the ISP accepts the user's login, then establishes the tunnel to the VPN device at the organization's office and finally begins forwarding packets over the Internet. Remote access VPN offers advantages such as: •Reduced capital costs associated with modem and terminal server equipment •Greater scalability and easy to add new users

•Reduced long-distance telecommunications costs, nationwide toll-free 800 number is no longer needed to connect to the organization's modems

Figure 2. Remote Access VPNs

A Primer for implementing a Cisco Virtual Private Network

© 1999 Cisco systems, Inc All rights Reserved

Intranet VPNs, provides virtual circuits between organization offices over the Internet (see figure 3). They are built using the Internet, service provider IP, Frame Relay, or ATM networks. An IP WAN infrastructure uses IPSec or GRE to create secure traffic tunnels across the network. Benefits of an intranet VPN include the following: •Reduced WAN bandwidth costs, efficient use of WAN bandwidth •Flexible topologies

•Congestion avoidance with the use of bandwidth management traffic shaping

Figure 3. Intranet VPNs

A Primer for implementing a Cisco Virtual Private Network

© 1999 Cisco systems, Inc All rights Reserved

The concept of setting up extranet VPNs are the same as intranet VPN. The only difference is the users. Extranet VPN are built for users such as customers, suppliers, or different organizations over the Internet. See Figure 4

Figure 4. Extranet VPNs

A Primer for implementing a Cisco Virtual Private Network

© 1999 Cisco systems, Inc All rights Reserved

Components of the VPN

In order for a VPN to be beneficial a VPN platform needs to be reliable, manageable across the enterprise and secure from intrusion. The VPN solution also needs to have Platform Scalability – the ability to adapt the VPN to meet increasing requirements ranging from small office configuration to large enterprise implementations. A key decision the enterprise should make before starting their implementation is to consider how the VPN will grow to meet the requirement of the enterprise network and if VPN will be compatible with the legacy networks already in place. 1. Security – Companies need to keep their VPNs secure from tampering and unauthorized users. Some examples of technologies that VPN’s use are; IP Security (IPSec), Point-to-Point Tunneling Protocol (PPTP), Layer 2 Tunneling Protocol and Multiprotocol Label Switching (MPLS) along with Data Encryption Standard (DES), and others to manage security. A further description of these technologies is detailed next. PPTP uses Point-to-Point Protocol (PPP) to provide remote access that can be tunneled through the Internet to a desired site. Tunneling allows senders to encapsulate their data in IP packets that hide the routing and switching infrastructure of the Internet from both senders and receivers to ensure data security against unwanted viewers, or hackers.

PPTP can also handle Internet packet exchange (IPX) and network basic input/output system extended user interface (NetBEUI). PPTP is designed to run on the Network layer of the Open systems interconnection (OSI). It uses a voluntary tunneling method, where connection is only established when the individual user request to logon to the server. PPTP tunnels are transparent to the service provider and there is no advance configuration required by the Network Access Server, this allows PPTP to use multiple service providers without any explicit configuration. For example, the client dials up to the ISP and makes a PPP session. Then, the client dials again to the same PPP session, to contact with the destination remote access server (RAS). After contact is made with the RAS, packets are then tunneled through the new connection and the client is now connected to the corporate server virtually.

Layer Two Tunneling Protocol (L2TP) exists at the data link layer of the OSI model. L2TP is a combination of the PPTP and Layer two Forwarding (L2F). (Layer two forwarding was also designed for traffic tunneling from mobile users to their corporate server. L2F is able to work with media such as frame relay or asynchronous transfer mode (ATM) because it does not dependent on IP. L2F also uses PPP authentication methods for dial up users, and it also allows a tunnel to support more than one connection.) L2TP uses a compulsory tunneling method, where a tunnel is created without any action from the user, and without allowing the user to choose a tunnel. A L2TP tunnel is dynamically established to a predetermined end-point based on the Network Access Server (NAS) negotiation with a policy server and the configured profile. L2TP also uses IPSec for computer-level encryption and data authentication. IPSec uses data encryption standard (DES) and other algorithms for encrypting data, public-key cryptography to guarantee the identities of the two parties to avoid man-in-the-middle attack, and digital certificates for validating public keys.

IPSec is focused on Web applications, but it can be used with a variety of application-layer protocols. It sits between IP at the network layer and TCP/UDP at the transport layer. Both parties negotiated the encryption technique and the key before data is transferred. IPSec can operate in either transport mode or tunnel mode. •In tunnel model, intruders can only see where the end points of the tunnel are, but not the destinations of the packet and the sources. IPSec encrypts the whole packet and adds a new IP packet that contains the encrypted packet. The new IP packet only identifies the destination’s encryption agent. When the IPSec packet arrives at the encryption agent, the new encrypted packet is stripped and the original packet continues to its destination. • In Transport mode IPSec leaves the IP packet header unchanged and only encrypts the IP payload to ease the transmission through the Internet. IPSec here adds an encapsulating security payload at the start of the IP packet for security through the Internet. The payload header provides the source and destination addresses and control information.

Multiprotocol Label Switching (MPLS) uses a label swapping forwarding structure. It is a hybrid architecture which attempts to combine the use of network layer routing structures and per-packet switching, and link-layer circuits and per-flow switching. MPLS operates by making the inter-switch transport infrastructure visible to routing and it can also be operated as a peer VPN model for switching a variety of link-layer and layer 2 switching environments. When the packets enter the MPLS, it is assigned a local label and an outbound interface based on the local forwarding decision. The forwarding decision is based on the incoming label, where it determines the next interface and next hop label. The MPLS uses a look up table to create end-to-end transmission pathway through the network for each packet.

Packet authentication prevents data from being viewed, intercepted, or modified by unauthorized users. Packet authentication applies header to the IP packet to ensure its integrity. When the receiving end gets the packet, it needs to check for the header for matching packet and to see if the packet has any error.

User authentication is used to determine authorized users and unauthorized users. It is necessary to verify the identity of users that are trying to access resources from the enterprise network before they are given the access. User authentication also determines the access levels; data retrieved or viewed by the users, and grant permission to certain areas of the resources from the enterprise. 2. Appliances – intrusion detection firewalls

Firewalls monitors traffic crossing network parameter, and protect enterprises from unauthorized access. The organization should design a network that has a firewall in place on every network connection between the organization and the Internet. Two commonly used types of firewalls are packet-level firewalls and application-level firewalls. Packet-level firewall checks the source and destination address of every packet that is trying to passes through the network. Packet-level firewall only lets the user in and out of the organization’s network only if the users have an acceptable packet with the correspondent source and destination address.

The packet is checked individually through their TCP port ID and IP address, so that it knows where the packet is heading. Disadvantage of packet-level firewall is that it does not check the packet contents, or why they are being transmitted, and resources that are not disabled are available to all users. Application-level firewall acts as a host computer between the organization’s network and the Internet. Users who want to access the organization’s network must first log in to the application-level firewall and only allow the information they are authorized for. Advantages for using application-level firewall are: users access level control, and resources authorization level. Only resources that are authorized are accessible. In contrast, the user will have to remember extra set of passwords when they try to login through the Internet.

3. Management – managing security policies, access allowances, and traffic management VPN’s need to be flexible to a companies management, some companies chooses to manage all deployment and daily operation of their VPN, while others might choose to outsource it to service providers. In our

next section we will discuss how businesses might benefit from a productive VPN and the cost benefits of implementing a VPN.

Productivity and Cost Benefit

In terms of productivity VPN’s have come a long way. In the past, concerns over security and manageability overshadowed the benefits of mobility. Smaller organizations had to consider the additional time and cost associated with providing IT support to employees on the move. Larger companies worried, with good cause, about the possibility that providing mobile workers with remote network access would inadvertently provide hackers with a “ back door” entry to corporate information resources. But as end-user technologies like personal digital assistants (PDAs) and cell phones have made mobility more compelling for employees, technology advances on the networking side have helped address IT concerns as we saw in the previous section. With these advancements in technology comes better productivity. VPN’s have become increasingly important because they enable companies to create economical, temporary, secure communications channels across the public Internet so that mobile workers can connect to the corporate LAN.

VPN’s Benefit a company in the following ways

•Extends Geographic Connectivity- a VPN connects remote workers to central resources, making it easier to set up global operations. •Boosts Employee Productivity- A VPN solution enables telecommuters to boost their productivity by 22% – 45% (Gallup Organization and Opinion Research) by eliminating time-consuming commutes and by creating uninterrupted time for focused work. •Improves Internet Security – An always-on broadband connection to the Internet makes a network vulnerable to hacker attacks. Many VPN solutions include additional security measures, such as firewalls and anti-virus checks to counteract the different types of network security threats. •Scales Easily – A VPN allows companies to utilize the remote access infrastructure within ISPs. Therefore, companies are able to add a virtually unlimited amount of capacity without adding significant infrastructure.

Even though VPN’s are a cheaper way of having remote users connect to a company’s network over the Internet there are still costs associated with implementing the VPN. Some of the typical costs include hardware, ISP subscription fees, network upgrading costs and end user support costs. These costs aren’t standard they vary depending on many factors, some of which include, size or corporation, number of remote users, type of network systems already in place and Internet Service Provider source. When it comes to decision making time IT managers or Executive officers should take these costs into consideration. Also these decision makers must decide whether to develop their VPN solution in house or to outsource to a total service provider.

There are a few ways to approach this topic; 1. In House Implementation- companies decide that for their needs an in-house solution is all they need. These companies would rather set up individual tunnels and devices one at a time and once this is established the company can have their own IT staff take care of the monitoring and upkeep. 2. Outsourced Implementation- companies can choose to outsource if they are large scaled or lack the IT staff to fully implement an in house VPN. When a company outsources the service provider usually designs the VPN and manages it on the company’s behalf. 3. Middle Ground Implementation- Some companies would rather have a service provider install the VPN but have their IT staff monitor the specifics such as tunnel traffic. This type of implementation is a compromise between a company and the service provider. After Implementation the company must make sure that it has adequate support for its end users. That’s where quality of service comes in.

Quality of Service (QOS)

Users of a widely scattered VPN do not usually care about the network topology or the high level of security/encryption or firewalls that handle their traffic. They don’t care if the network implementers have incorporated IPSec tunnels or GRE tunnels. What they care about is something more fundamental, such as:

“ Do I get acceptable response times when I access my mission critical applications from a remote office?”

Acceptance levels for delays vary. While a user would be willing to put up with a few additional seconds for a file transfer to complete, the same user would have less tolerance for similar delays when accessing a database or when running voice over an IP data network. QoS (Quality of Service) aims to ensure that your mission critical traffic has acceptable performance. In the real world where bandwidth is limited and diverse applications from videoconferencing to ERP database lookups must all strive for scarce resources, QoS becomes a vital tool to ensure that all applications can coexist and function at acceptable levels of performance. Quality of Service (QOS) is a key component of any VPN service. In MPLS/BGP VPNs, existing L3 QoS capabilities can be applied to labeled packets through the use of the " experimental" bits in the header, or, where ATM is used as the backbone, through the use of ATM QoS capabilities. The traffic engineering work discussed in is also directly applicable to MPLS/BGP VPNs. Traffic engineering could even be used to establish LSPs with particular QoS characteristics between particular pairs of sites, if that is desirable. Where an MPLS/BGP VPN spans multiple SPs, the architecture described may be useful. An SP may apply either intserv or diffserv capabilities to a particular VPN, as appropriate.

The Future of VPN

As more and more businesses demand a higher level of network access, the business is migrating from a private network environment to a new model in which information is distributed throughout the enterprise network. Thus, expanding their network in the near future and actually seeing the benefits of using the Internet as the backbone to create Virtual Private Networks (VPN). VPN is designed to meet the demands for information access in a secure, cost-effective environment.

Multi-vendor interoperability for VPN is crucial in today's networking environment due to the nature of business successes, the need to extend corporate networks to contractors and partners, and the diverse equipment within company networks. The Microsoft Windows operating system has integrated VPN technology that helps provide secure, low-cost remote access and branch office connectivity over the internet.

The future is in integrated VPNs which depend on how VPNs industry will improve their unique qualities that will enable consumers to communicate effectively with other consumers. Therefore, a VPN creates a large, multi-site, company-wide data network which allows for every device to be uniquely addressed from anywhere on the network. This means that central resources can be accessed from any site in the organization or from any Internet-connected location around the world. The technical problems involved in connecting hundreds of remote sites to a central network are extensive. It often involves the purchase of very expensive high-density backbone routers or the use of costly frame-relay services. These systems are seldom easy to support and often require specialist skills. Also, it depends on the ability of intranets and extranets to deliver on their promises. First of all VPN companies must consider to cost saving for servicing of VPNs. Generally speaking the more the companies supply cheaper cost of services, the more products or demands increase for them on the markets. Therefore, they will earn high profit then spend a lot of money for developing much higher quality VPN. Here is a diagram for U. S. companies with IP VPN.

Table 1. Companies with VPN

Source: IDC’s 2001 U. S. WAN Manager Survey, IDC #26462, February 2002

According to IDC’s 2001 U. S. WAN manager survey as table 1, approximately fifty percents of companies in U. S. have been adopted IP VPN in their companies. Demand for VPN has been increasing even though economy is going down and especially IT business companies have not succeeded at present. More then 20 percents of companies will plan to have IP VPN services in the future so those in near future more than 70 percents of companies are going to use IP VPN services. More companies will adopt IP VPN services and increasing more demand in the U. S. Also many companies have been using IP VPN for remote access as LAN.

The companies for servicing VPN will consider meeting consumer's demands that is voice over IP and other VPN as VOIP VPN. Currently very a few companies have been using this VPN and a few companies will plan to use it in the future. However, contrary to their demands, most produces are standing on difficult situation for improving VOIP VPN because the voice is a kind of special requirement of low latency and jitter. Most of people will continue to use voice communication by telephone that is successfully improving with low costs.

The 21st century invites new ways of viewing the communication networks. Companies that previously managed their own communications requirements are uniting with service providers that can help build up, improve, and manage their networks on a global scale. This opens up opportunities for continued growth, increased profitability, and the greatest achievement for both service providers and subscribers. In the past, service providers drew attention to lower-level transport, such as leased lines and frame relay. Nowadays, service providers team with business customers to meet their networking requirements through virtual private networks (VPNs).

VPNs are the source of future services. When properly implemented, they can simplify network operations while reducing capital expenses. For most companies, the starting point is to connect widely separated workgroups in an efficient, moneymaking manner. From there, service providers can influence the main technology as a foundation for offering additional services such as application hosting, videoconferencing, and packet telephony.

VPN help service providers build customer loyalties while delivering network services that are valuable to their customers' business operations. This indicates an opportunity to capture new customers, as companies switch from yesterday's data communications strategies to today's more comprehensive at hand solutions.

Conclusion

VPN is an emerging technology that has come a long way. From an insecure break off of Public Telephone networks to a powerful business aid that uses the Internet as its gateway. VPN's technology is still developing, and this is a great advantage to businesses, which need to have technology that is able to scale and grow along with them. With VPN businesses now have alternative benefits to offer to their employees, employees can work from home, take care of children while still doing productive, and have access work related information at anytime. VPN will also help to make the possibility of a business expanding its services over long distances and globally, more of a reality.

Bibliography

A primer for Implementing a Cisco Virtual Private Network. (1999). Cisco Systems. Retrieved October 5, 2002, from http://www. cisco. com/warp/public/cc/so/neso/vpn/vpne/vpn21_rg. htm

A Technology Guide from ADTRAN. (2001, September). Understanding Virtual Private Networking. ADTRAN. Retrieved October 25, 2002, from http://www. adtran. com/all/Doc/0/DTCGA3HEJ3B139RK038BE81ID8/EN286. pdf

Connolly, P. J., (2002, January 21). Taming the VPN. Computerworld. Retrieved September 18, 2002, from http://www. computerworld. com/networkingtopics/networking/story/0, 10801, 67396, 00. html

Dix, John. (2001, April 9). Is an integrated VPN in your future? Network World. Retrieved October 1, 2002, from http://www. itworld. com/Net/2553/NWW010409edit/

Ferguson & Huston. (1998, April). What is a VPN? Retrieved September 19, 2002, from http://www. employees. org/~ferguson/vpn. pdf

Internetworking Technologies Handbook, Virtual Private Networks. Cisco Systems. Retrieved September 22, 2002, from http://www. cisco. com/univercd/cc/td/doc/cisintwk/ito_doc/

Introduction to VPN: VPNs utilize special-purpose network protocols. Computer Networking. Retrieved September 14, 2002, from http://www. compnetworking. about. com/library/weekly/aa010701d. htm

Next-Generation Networking: The Future of Greater Performance and Flexibility. (2002, July). IDC Analyze the Future. Retrieved September 28, 2002, from http://www. business. att. com/content/whitepaper/next_generation. pdf

Remote Access VPN Solutions. (2001, June). Check Point Software Technologies Ltd. Retrieved September 20, 2002, from http://www. checkpoint. com/products/downloads/vpn-1_remote_access. pdf

Salamone, Salvatore. (1998, December). VPN Implementation Calls For A Tunnel Trip. Internet Week. Retrieved October 30, 2002, from http://www. internetwk. com/VPN/paper-5. htm

Sandick, H., Nair, R., Rajagopalan, B., Crawley, E., (1998, August). A Framework for QoS-based Routing in the Internet. Retrieved October 1, 2002, from ftp://ftp. isi. edu/in-notes/rfc2386. txt

Sweeney, T., (2000, April 3). Businesses Lock In On VPN Outsourcing Options Providers of virtual private network services put a new spin on the outsourcing spiel. InformationWeek. Retrieved September 20, 2002, from http://www. informationweek. com/780/vpn. htm

Using Point-to Point Tunneling Protocol. (2001, July). Microsoft. Retrieved September 20, 2002, from http://www. microsoft. com/ntserver/techresources/commnet/PPTP/pptpwp. asp

Virtual Private Networks (VPNs). International Engineering Consortium. Retrieved October 19, 2002, from http://www. iec. org/online/tutorials/vpn/index. html

VPN Technologies: Definitions and Requirements. International Engineering Consortium. Retrieved October 19, 2002, from http://www. iec. org/online/tutorials/vpn/topic02. html

Questions

1. What is VPN?

2. What is tunneling?

3. What is the difference between outsourcing and in-house development, and middle-ground implementation? 4. What are the difference between remote access VPNs, Intranet VPNs, and Extranet VPNs? 5. What are the benefits of remote access VPNs?