Remote Access VPN's, a basic look

Let us start out by explaining Virtual Private Networks (VPN) so everyone can understand, even managers (it's going to be hard, but I think I am up to the challenge). Most of us have at least heard of VPN's, but not many actually know what they do. My goal is to make the analogy between how VPN's work, with ordering and picking up a pizza. Sound crazy? You ain't heard nothing yet!

It is a Sunday afternoon and you are sitting at home watching football, when all of a sudden your stomach starts to grumble. There is approximately 30 minutes until halftime. This is just enough time to order a pizza, pick it up by halftime, and be back in your lazy boy before the second half starts.

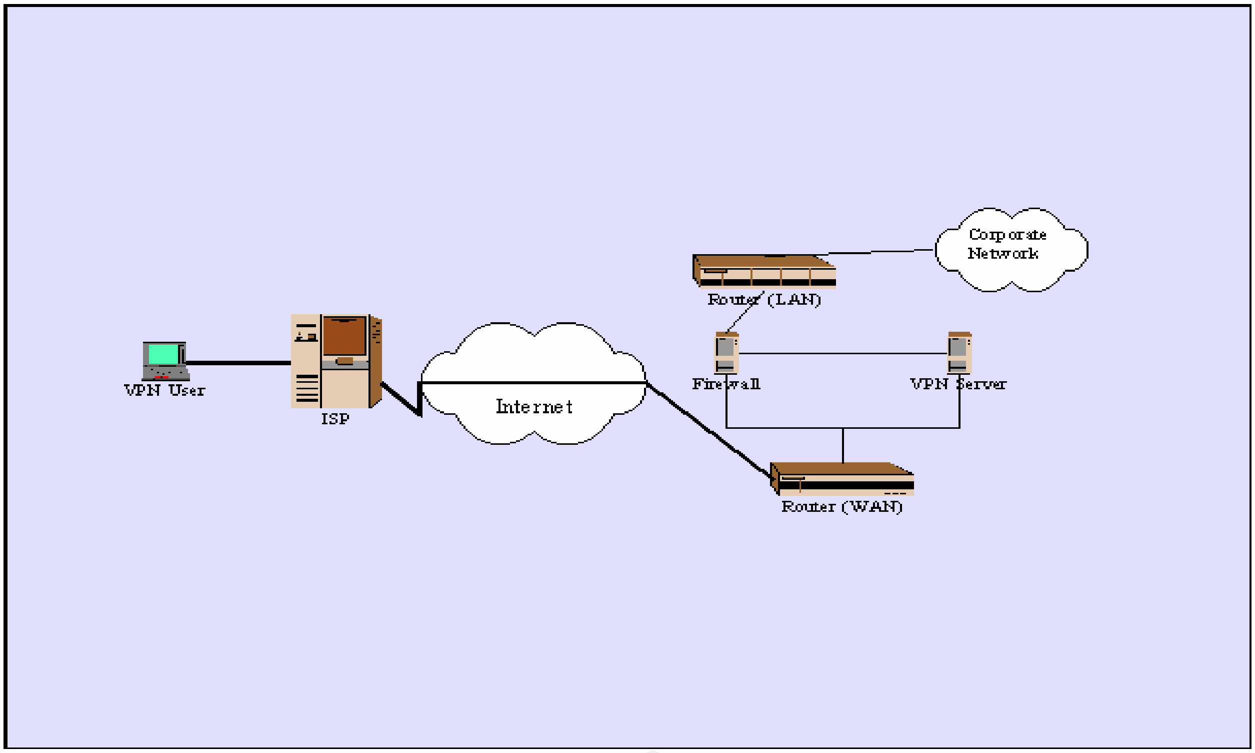
You pick up the phone and call Vinnie's Pizza Emporium and order the Happy Roman Delight with extra cheese. While on the phone the counter help asks for your name and number. Thirty minutes go by and now it is halftime. You get in your car and head down the road to pick up the pizza. You park the car, walk up to the counter and ask for your food. The employee asks your name, gets your pie, pay $10 and you head back to watch the rest of the game.

I am sure by now you are thinking to yourself, "What the heck is this guy talking about, has he lost his mind?" To answer your question, no I have not lost my mind, I just have an over active imagination.

By comparing, steps for ordering and picking up a pizza, with a virtual private network the processes start to take shape.

Decision to order a pizza.	User has a need to access the corporate network.
Vinnie's is on the other side of the city.	The city represents the Internet.
Place the order.	VPN tunnel indicator communicates with the VPN tunnel terminator.
You give Vinnie's your name.	The two VPN gateways agree on an encryption scheme.
Vinnie's asks for your number.	The VPN gateway authenticates user.
You get in your car.	The package is encrypted and encapsulated in an IP (Internet Protocol) packet.
You drive down the road.	The road represents the virtual tunnel.
You arrive at Vinnie's and get out of the car.	VPN tunnel terminator strips out the IP information.
Vinnie's asks your name and verifies your phone number.	The packet is authenticated and decrypted.
You get your pizza and head home.	The packet is sent to the remote access server or router and delivers it to the final destination.

Ok, I will admit, this may be a bit of a stretch, paralleling VPN's and ordering a pizza, but the basic concept is there. In this example, the VPN process is oversimplified but at a very high level, the description is close.



(Figure 1)

The VPN uses the Internet to make a private connection between two machines. Before this can be accomplished there are a few concerns that have to be addressed. The VPN client, through an Internet Service Provider (ISP) to a VPN gateway initiates this connection or "virtual tunnel". The packet is then received by the VPN gateway and the two agree on the encryption and authentication scheme. Once this is worked out the VPN tunnel initiator encapsulates the entire package in an IP packet. When the packet is received by the VPN gateway the IP information is removed, content is decrypted and routed to its final destination.

VPN Client

The Virtual Private Network client can be broken down into four different categories:

1) Tunneling
2) Authentication
3) Access Control
4) Data Integrity and Confidentiality

Tunneling

Tunneling can be defined as the encapsulation of a certain data packet (the original or inner packet) into another data packet (the encapsulation or out packet) so that the inner packet is opaque to the network over which the outer packet is routed. (Virtual Private Networks, Technologies and Solutions, pg. 13)

Tunneling is crucial for two primary reasons. First, to transport multiple protocols over a single protocol network and second, it can be used to hide both source and destination addresses. Typically the tunnel should be encrypted for security reasons.

There are several algorithms that can be used for encryption. Data Encryption Standard (DES), Triple Data Encryption Standard (3DES), International Data Encryption Algorithm (IDEA), symmetric encryption algorithm by C. Adams and S. Tavares (CAST) and Ron's Cipher #4 symmetric encryption algorithm (RC4) are the most predominant in the industry. Encryption will hide your data from prying eyes. After all, if encryption isn't important, why does the Kama-Sutra name it 45th in the list of skills a woman should know (makes you wonder about the preceding 44 doesn't it).

Tunneling can be done at any layer of the Open System Interconnection (OSI), seven-layer architecture for data communication over an IP backbone. Based on this the two most common layers used for tunneling are layer 2 (link layer) and layer 3 (network layer).

Layer 2 Tunneling

- Point-to-Point Tunneling Protocol (PPTP)
- Layer Two Forwarding Protocol (L2F)
- Layer Two Tunneling Protocol (L2TP)

Layer 3 Tunneling

- Multiprotocol Label Switching (MPLS)
- Internet Protocol Security (IPsec)

Any one of the tunneling mechanisms could be a "practical." I am going to focus on the Internet Protocol Security (IPsec). IPsec is an extremely versatile protocol. It can be used for an encryption scheme for any of the layer 2 protocols (L2TP or PPTP) or for a tunneling solution for the VPN. IPsec is a combination of two protocols wrapped into one, Authentication Header (AH) and Encapsulation Security Payload (ESP). AH provides data integrity and data authentication. The AH is formatted into six fields. They are:

- Next Header – This identifies the type of protocol header that follows the AH.
- Payload Len – This field gives the specific length of the AH.
- Reserved – Reserved for future use, it must be set to zero.
- Security Parameter Index – Used to uniquely identify the Security Association (SA) with the destination IP address for the particular packet.
- Sequence Number – This field holds a number that is increase monotonically for sequencing the IP packets.
- Authentication Data – Contains the Integrity Check Value (ICV) for the particular packet.

<table>
<tr><td>Next Header (8 bits)</td><td>Payload Len (8 bits)</td><td>Reserved (16 bits)</td></tr>
<tr><td colspan="3">Security Parameter Index (32 bits)</td></tr>
<tr><td colspan="3">Sequence Number (32 bits)</td></tr>
<tr><td colspan="3">Authentication Data (variable)</td></tr>
</table>

authentication, data confidentiality through encryption and protecting the IP packets from replay. All three of the ESP's features are optional, but generally speaking either authentication or encryption are employed. Otherwise there would be no value added from the protocol.

Before moving on to authentication, I will give a brief description of the tunnel negotiation between the VPN client and the VPN gateway. IPsec uses the Internet Key Exchange (IKE) to exchange secure encryption keys over the Internet. This is a three-phase negotiation:

1) Initiator (VPN client) sends multiple Security Associations (SA) proposals to the responder (VPN gateway). The responder picks one proposal and sends it back to the initiator.
2) The two exchange their key exchange parameters and random use-once values (nonces).
3) The exchange information is authenticated.

Authentication

Authentication can be very simply defined as the process of identity verification. The purpose of authentication is to ensure the data is coming from the source it claims to be. Authentication can be broken into two broad categories: two-party and trusted third-party authentication. The three most common authentication options are:

- Shared Secret Password
- Remote Authentication Dial In User Service (RADIUS)
- Digital Certificates

Two – Party Authentication

- Password – This is where the user and peer work out a secret phrase or word.
- Challenge / Response – This is where the peer asks a question and the user must respond back correctly.
- One-time Password – The password is good for only one authentication session.
- Token Cards – A device picks a one-time password per session.

Trusted Third – Party Authentication

Trusted third party adds a third party to aid in the authentication process. As the name suggests the third party can vouch or provide additional information to be used in authentication. Some of the more popular third party solutions are:

- Kerberos – Network authentication system that provides a means of verifying the identities of entities on an open, unprotected network using a trusted third party.
- Public Key Infrastructure (PKI) – Provides authentication across networks using public key cryptography.
- Pretty Good Privacy (PGP) – Is based on a web of trust approach to authentication.

Access Control

Access control is the set of policies and mechanisms that permit authorized parties access to restricted resources. It also protects resources from being accessed, either maliciously or accidentally, by users not authorized to access them. The client sends the users identity, attributes and requested operations to the server. Since the majority of the access control is done on the server side it will be discussed later during VPN gateways.

Data Integrity and Confidentially

Data integrity is ensuring that the packets will not be modified without detection. Confidentiality is the protection of information being exchanged between communicating parties. This is accomplished using secret key cryptography and public key cryptography. Generally speaking, the three technologies used to ensure data integrity are:

1) One-way hash – This function takes a variable length input file into a fixed output value. Examples of a hash algorithm are MD5, SHA-1 and RIPE-MD-160.
2) Message Authentication Codes (MAC) – MAC is a hash function with a key.
3) Digital Signature – Digital signature is an electronic "handwritten" signature that is legally binding. The sender signing a document with their private key and the receiver authenticating the signature with the sender's public key accomplishes the signature.

VPN Gateway

The VPN gateway has two distinct roles:

1) The gateway allows desired traffic in and out of the Private network.
2) VPN gateway keeps undesired traffic out of the Private network while containing unintentional traffic from leaving.

The VPN client and VPN gateway share the same basic functions:

- Tunneling
- Authentication
- Access Control
- Data Integrity and Confidentiality

Authentication

Three out of four functions were covered previously in the VPN client section. The VPN client's role in access control is limited. Since the restricted resources are in the corporate network additional policies need to be in place. These policies and procedures can be broken down into three areas:

1) Access Control Policy
2) Access Control Mechanisms
3) Access Control Policy

Access Control Policy

Access control policies are the rules and conditions that define the protection of resources. These policies are categorized into discretionary and mandatory. Discretionary access control lets the owner of the resource determine what the access level is and who can access it. Mandatory access control is based on a hierarchy of access that is determined by the organization.

Access Control Mechanisms

Access control mechanisms are how the rules are enforced. Two methods to specify these conditions are access control lists (ACL) and capabilities lists (C-lists). An access control list is a list of what resources users can access and the level of access to the resources. Capabilities lists are specific to each user. C-lists take the stance of deny all until explicitly authorized.

Access Control Policy Management

Access control policy management is the maintaining, distributing and creating the access control polices. Either a distributed policy management or centralized policy management can handle the management. Distributed policy manager, use a policy administrator by sending policies to the policy manager to the enforcement points. Centralized policy management has only one policy manager and a centralized policy repository the access control points connected to.

Advanced Functions

Some of the more advanced functions of the VPN gateway include:

- Quality of service (QoS) – Meeting up to a specified level of service on the network.
- Redundant fail-over and load balancing – If the VPN gateway fails, another gateway will pick up and assume the role.
- Hardware acceleration – Needed for algorithm computations for the encryption operation.

Conclusion

This paper has really only scratched the surface of all the options and pitfalls of the device. As mentioned earlier any one of the sub-topics could be a “practical” in itself. To quote, Virtual Private Networks, Technologies and Solutions by Timothy Strayer and Ruixi Yuan (pg. 281), “Internet access is quickly becoming the vehicle where all kinds of communication services are carried. Therefore, expectations are evolving far beyond that of simple connectivity. The development of virtual Private networks is one step in that evolution.”

Bibliography

Stallion Technologies, "What is Internet-based Virtual Private Networking?" (25/2/01)
http://www.stallion.com/html/solutions/vpn-overview.html

Lee Chae, Article, “Virtual Private Networks” (10/01/98)
http://www.networkmagazine.com/article/NMG20000727S0029/2

Jeff Tyson, Technical Paper, “How Virtual Private Networks Work” (2001)
http://www.howstuffworks.com/vpn.htm

Andrew Brandt and Alexandra Krasne, Article, “How It Works: Encryption” (14/02/00)
http://www.pcworld.com/hereshow/article/0,aid,15230,00.asp

Robert Moskowitz, Article – "What is a Virtual Private Network?" 23/02/01
http://www.networkcomputing.com/905/905colmoskowitz.html

Ruixi Yaun and W. Timothy Strayer, Virtual Private Networks, Technologies and Solutions (2001)

Harold F. Tipton and Micki Krause, Information Security Management, (2000)

Networking Working Group, A Framework for IP Based Virtual Private Network, (2000)