

Telecommunication -- Firewalls -- VPN

- ❖ *DigitalSherlock.com | SafeHack.com*
- ❖ *Date: 2005/05/27*
- ❖ *Document Name: telecommunication_firewalls_vpn.pdf*
- ❖ *GNU Free Documentation License*
- ❖ *Version 1.00, 2005-05-27*
- ❖ *Copyright © 2005 Adonis, MSc, Eng, CISSP, Security+, CEH, GSec, MCSE, etc.*
- ❖ *Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.2 or any later version published by the Free Software Foundation.*

❖ Firewall Types

➤ Packet Filtering

- **First Generation**
- **Called Screening router**
- **It use Access Control Lists ACL**
- **Operates at the Network layer (3)**
- **Examines both the source and destination addresses of the incoming packet**
- **Look at the data packet to get information about source and destination**
- **Sometime used to manage access to DMZ**
- **PRO and CONS**
 - Provide scalability
 - Provide high performance
 - Provide application independence
 - Protects against standard generic external attacks
 - But it provide low security and no protection above the network layer
 - ACLs can be manually difficult to maintain
 - It lacks strong user authentication
 - Does not look into the packet past the header information
 - Does not keep track of the state of a connection
 - The most common and oldest firewall

➤ Application Level Proxy

- **Second Generation**
- **Often called a Proxy Server**
- **Proxy Server is the middleman in communication**
- **It transfer a copy of each accepted data packet from one net to another**
- **Operates at Application layer (7)**
- **Application VS. Circuit Level Proxy**
 - Application Level Proxy
 - ♦ Inspect the entire packet and make access decisions
 - ♦ Is aware of the protocols, services, and commands being used
 - ♦ Transfer a copy of each accepted data packet from one network to another
 - ♦ Different proxy is required for each service allowed
 - ♦ Hides internal computer information and IP address
 - ♦ Provide more control than Circuit level proxy
 - ♦ Reduces network performance
 - Circuit Level Proxy
 - ♦ Creates a circuit between the client and the server
 - ♦ It knows the source and destination addresses and makes access decisions
 - ♦ Do not provide the detailed control that an application proxy provides
 - ♦ Provides security for a wider range of protocols

- ♦ Are easier to maintain than full application proxy firewalls.
 - ♦ Circuit level proxy that does not require server resource overhead
- **PRO and CONS**
 - Looks at the information within a packet all the way up to the application layer
 - Provide better security than packet filtering
 - Is aware of the protocols, services, and commands being used
 - Limited to what applications it can support
 - Degrades traffic performance
 - Poor scalability
 - Breaks client/server model
- **Stateful Inspection**
 - **Third Generation**
 - **Packets are captured by the inspection engine**
 - **Operate at Network layer (3) analyse packet at all OSI level**
 - **PRO and CONS**
 - Maintains a state table that tracks each communication
 - Offer better performance than proxy firewalls
 - It is scalable and transparent to users
 - Help track connection less UDP and RPC
 - Is aware of the protocols, services, and commands being used
- **Dynamic Packet Filtering**
 - **Fourth Generation**
 - **Enables the modification of the firewall security rule**
 - **Makes informed decisions on the ACL's to apply**
 - **Used to provide limited support to UDP**
- **Kernel Proxy**
 - **Fifth Generation**
 - **Very specialized architecture that provides modular kernel-based**
 - **Multi-layer session evaluation and runs in the NT executive space**
 - **Use dynamic and custom TCP/IP based stacks to inspect packets**

❖ **Firewall Architectures**

- **Dynamic Packet Filtering**
 - **Fourth Generation**
 - **Enables the modification of the firewall security rule**
 - **Makes informed decisions on the ACL's to apply**
 - **Used to provide limited support to UDP**
- **Screened Host**
 - **Screened host is between the border router and the LAN**
 - **Use both Packet filter router and Bastion host**
 - **Sometime we call Bastion host "Sacrificial Host"**
 - **Provide both Network layer (packet filter) and application layer services (proxy)**
- **Screened Subnet with DMZ**
 - **Is sandwiched between two routers**
 - **One of the most secure**
 - **It use 2 packet filtering routers and a bastion host**

- Provide both Network layer (packet filter) and application layer services (proxy)
- **Dual-homed host**
 - Very common
 - Single computer with two Nics
 - Can translate between two network access layer protocols
- **Socks**
 - Socks Work on Application Layer (7)
 - Provides authentication and encryption similar to VPN.
 - It is not considered as VPN
 - A socks client is required on every client
 - Can be resource intensive

❖ VPN

- **Introduction**
 - Created by dynamically building a secure communication link between nodes using a secret Encapsulation method
 - This link is called "Secure Encrypted Tunnel"
 - VPN - Private data network that makes use of the public telecommunication infrastructure
 - VPN - use tunneling protocol to provide a secure network link
 - VPN - use PPTP, L2F, L2TP, IPSec
 - VPN - Encrypt data before sending
 - **§ Tunneling**
 - A protocol or set of communication rules
 - Create a virtual private network (VPN) through "tunnels" over the Internet
 - Tunneling protocols move frames from one network to another by placing them inside of routable encapsulated frames
 - **Encapsulation tunnel Created using methods such**
 - Installing software or hardware agents on the client
 - Implementing various user or node authentication systems
 - Implementing key and certificate exchange systems
 - **NAT is an important part of VPN**
 - **§ Network Address Translation**
 - Translation of an Internet Protocol address (IP address) to a different IP
 - Private addresses are not easily routable. This is the reason of using NAT
 - One network is designated the inside
 - One network is designated the outside
 - NAT is included as part of a router
 - Often part of a corporate firewall
 - NAT reduces the need for a large amount of publicly known IP
 - NAT use these reserved IP's
 - ◆ 10.0.0.0 - 10.255.255.255
 - ◆ 172.16.0.0 - 172.31.255.255
 - ◆ 192.168.0.0 - 192.168.255.255
- **VPN Protocol Standards**
 - **PPTP**
 - Point To Point Tunneling Protocol
 - Work at the Data Link Layer

- Enable ONLY one single point-to-point connection per session
- Use PPP authentication and encryption services
- Use PAP or CHAP
- It is asynchronous
- **L2TP**
 - Combination of PPTP and earlier Layer 2 forwarding Protocol
 - Dial-up VPN use this standard
 - Designed for Single Point-To-Point client to server Like PPTP
 - Multiple protocol can be encapsulated within L2TP tunnel
 - Work on Data Link Layer
- **IPSec**
 - Work at the Network Layer
 - They are installed on a network perimeter and encrypt traffic by creating a secure tunnel
 - They work only with IP they are NOT multi-protocol
 - Enable multiple and simultaneous tunnels
 - IPSec has 2 modes
 - ◆ Tunnel mode - encrypt payload and header information
 - ◆ Transport mode - Encrypt only the payload
 - Ensures confidentiality and integrity to IP packets
 - Authenticate and encrypt IP data
 - Focus more on Network-To-Network connectivity
- **VPN Devices**
 - **Non-IPSec Compatible**
 - Socks
 - ◆ Socks based systems contain Authentication and Encryption similar to VPN
 - ◆ Socks Work on Application Layer 7
 - PTP
 - ◆ Multiprotocol used in Win9x and NT
 - ◆ Use PAP or CHAP for End-To-End Encryption
 - ◆ Commonly used by ISP's
 - SSH
 - ◆ Secure Shell SSH-2 is not a VPN product but it can be used as such
 - ◆ SSH open a secure encrypted shell session from the internet through a firewall
 - **Firewall based VPN**
 - Frequently available on Thrid generation of firewall (Statful Inspection)
 - Use VPN that integrate to the firewall and often it is proprietary and non-standard
 - Work on Application Layer 7 in tunnel mode