Firewalls and VPNs

Raj Jain
Washington University in Saint Louis
Saint Louis, MO 63130
Jain@cse.wustl.edu

Audio/Video recordings of this lecture are available at:
http://www.cse.wustl.edu/~jain/cse571-17/

Overview

1. What is a Firewall?
2. Types of Firewalls
3. Proxy Servers
4. Firewall Location and Configuration
5. Virtual Private Networks

These slides are based on Lawrie Brown’s slides supplied with William Stalling’s

What is a Firewall?

- Interconnects networks with differing trust
  - Only authorized traffic is allowed
- Auditing and controlling access
  - Can implement alarms for abnormal behavior
- Provides network address translation (NAT) and usage monitoring
- Implements VPNs

Firewall Limitations

- Cannot protect from attacks bypassing it
  - E.g., sneaker net, utility modems, trusted organisations, trusted services (e.g., SSL/SSH)
- Cannot protect against internal threats
  - E.g., disgruntled or colluding employees
- Cannot protect against access via Wireless LAN
  - If improperly secured against external use, e.g., personal hot spots
- Cannot protect against malware imported via laptops, PDAs, and storage infected outside
Firewalls – Packet Filters

- Examine each IP packet (no context) and permit or deny according to rules

```
+------------------+
| Application      |
| Transport        |
| Internet         |
| Network access   |
| Physical         |
+------------------+
```

Attacks on Packet Filters

- IP address spoofing: Add filters on router to block
- Source routing attacks: Attacker sets a route other than default
  - Block source routed packets
- Tiny fragment attacks: Split header info over several tiny packets ⇒ Either discard or reassemble before check

Firewalls – Stateful Packet Filters

- Examine each IP packet in context
  - Keep track of client-server sessions
- May even inspect limited application data
Proxy Servers

- Specialized server programs
- Take user's request and forward them to real servers
- Take server's responses and forward them to users
- Enforce site security policy ⇒ Refuse some requests.
- Also known as application-level gateways
- With special "Proxy client" programs, proxy servers are almost transparent

Circuit Level Gateway

- Relays two TCP connections
- Imposes security by limiting which such connections are allowed
- Once created usually relays traffic without examining contents
- Typically used when trust internal users by allowing general outbound connections
- Socket Secure (SOCKS) is commonly used
## Bastion Host

- Highly secure host system
- Runs circuit/application level gateways
- Provides externally accessible services
- Potentially exposed to "hostile" elements
  - Hardened O/S, essential services, extra auth
- May support 2 or more net connections
- May be trusted to enforce policy of trusted separation between these net connections

![Bastion Host Diagram](image)

## Host-Based Firewalls

- S/W module used to secure individual host
  - Available in many operating systems or an add-on package
- Mostly on servers.
- Advantages:
  - Can tailor filtering rules to host environment
  - Protection is provided independent of topology
  - Provides an additional layer of protection

## Personal Firewalls

- Controls traffic between PC/workstation and Internet or enterprise network
- A software module on personal computer or in home/office DSL/cable/ISP router
- Typically much less complex than other firewalls
- Primarily to deny unauthorized remote access to the computer and monitor outgoing activity for malware

![Personal Firewall](image)
Firewall Configurations

(a) Screened host firewall system (single-homed bastion host)

(b) Screened host firewall system (dual-homed bastion host)

Firewall Configurations (Cont)

(c) Screened-subnet firewall system

DMZ Networks

- Demilitarized Zone
**Distributed Firewalls**

- Internet
- External DMZ network
- Internal DMZ network
- Web servers
- Email server
- DNS server
- Internal protected network
- Application and database servers
- Workstations
- Internet access

**Virtual Private Networks**

**What is a VPN?**

- Private Network: Uses leased lines
- **Virtual** Private Network: Uses public Internet

- Internet Service Provider

**Layer 2 VPNs**

- Customers' Layer 2 packets are encapsulated and delivered at the other end
- Looks like the two ends are on the same LAN or same wire
- Provides Ethernet connectivity
- Works for all Layer 3 protocols
- Virtual Private Wire Service (VPWS)
- Virtual Private LAN Service (VPLS)
Layer 3 VPN

- Provides Layer 3 connectivity
- Looks like the two customer routers are connected
- Usually designed for IP packets

VPN Tunneling Protocols

- GRE: Generic Routing Encapsulation (RFC 1701/2)
- PPTP: Point-to-point Tunneling Protocol
- L2TP: Layer 2 Tunneling protocol
- IPsec: Secure IP
- MPLS: Multiprotocol Label Switching

GRE

- Delivery Header
- GRE Header
- Payload

- Generic Routing Encapsulation (RFC 1701/1702)
- Generic $\Rightarrow$ X over Y for any X or Y
- Optional Checksum, Loose/strict Source Routing, Key
- Key is used to authenticate the source
- Over IPv4, GRE packets use a protocol type of 47
- Allows router visibility into application-level header
- Restricted to a single provider network $\Rightarrow$ end-to-end

PPTP

- PPTP = Point-to-point Tunneling Protocol
- Developed jointly by Microsoft, Ascend, USR, 3Com and ECI Telematics
- PPTP server for NT4 and clients for NT/95/98
### PPTP Packets

- **Private Network**
- **PPTP Server**
- **Internet**
- **Network Access Server**
- **Client**

#### PPTP Packets

- **PPP**
- **IP**
- **GRE**
- **PPP**

#### Data

- **IP/IPX/NetBEUI**

#### Internal IP Addressing

- **Encrypted**

### L2TP

- **Layer 2 Tunneling Protocol**
- **L2F = Layer 2 Forwarding (From CISCO)**
- **L2TP = L2F + PPTP**
  - Combines the best features of L2F and PPTP
  - Easy upgrade from L2F or PPTP
  - Allows PPP frames to be sent over non-IP (Frame relay, ATM) networks also (PPTP works on IP only)
  - Allows multiple (different QoS) tunnels between the same end-points. Better header compression. Supports flow control


### L2TPv3

- Allows service providers to offer L2 VPN over IP network.
- L2TPv2 was for tunneling PPP over packet switched data networks (PSDN)
- V3 generalizes it for other protocols over PSDN ⇒ PPP specific header removed
- Can handle HDLC (High-Level Data Link Control), Ethernet, 802.1Q VLANs, Frame relay, packet over SONET (Synchronous Optical Network)

### OpenVPN

- Most popular open source VPN software for client and servers.
- Can be implemented in firmware, e.g., DD-WRT, OpenWRT, …
- Available on most operating systems, e.g., Windows, Linux, Mac, IoS, Android, …
- Many routers come with OpenVPN support
- Does not use IKE, IPSec, PPTP, L2TP
- Uses OpenSSL library for SSL/TLS on TCP/UDP
- Provides all encryption/authentication methods in OpenSSL, e.g., pre-shared key, certificates, username/password, …
- OpenSSL allows servers to issue certificates to clients
- Extendable using modular plugins
- Uses a single TCP/UDP port ⇒ can traverse NAT/firewalls

Ref: [https://en.wikipedia.org/wiki/OpenVPN](https://en.wikipedia.org/wiki/OpenVPN)
Summary

1. Firewalls separate networks of different trust levels
2. Some traffic, such as, laptops, smart phones, and wireless can bypass firewall
3. Firewall can be a simple packet filter or an application level proxy
4. Servers for external public are often placed in DMZ that separates two networks of differing trusts
5. Firewall locations: single bastion inline, single bastion T, double bastion inline, double bastion T, distributed
6. PPTP and L2TP are layer 2 VPN protocols. IPSec provides Layer 3 VPN. OpenVPN is an implementation using SSL.

Lab 23: Tor

- Read about Tor (The Onion Router) from: [https://en.wikipedia.org/wiki/Tor_(anonymity_network)]
- Download and install Tor browser from: [https://www.torproject.org/projects/torbrowser.html.en]
- Open both Tor browser and your regular browser (Firefox or Internet Explorer, etc.)
- Browse to “WhatIsMyIP.com” on both browsers and capture the results.
- Repeat the previous step on both browsers and capture the results.
- Browse to [http://thehiddenwiki.org/2013/08/23/list-of-onion](http://thehiddenwiki.org/2013/08/23/list-of-onion) (Hidden Wiki | Tor .onion urls directories » How to access the Deep Web) on both browsers and capture the results.

Acronyms

- ACK: Acknowledgement
- DMZ: Demilitarized Zone
- DNS: Domain Name System
- DSL: Digital Subscriber Line
- FTP: File Transfer Protocol
- HD: High Definition
- IM: Instant messaging
- IKE: Internet Key Exchange
- IP: Internet Protocol
- IPSec: Secure IP
- ISP: Internet Service Provider
- LAN: Local Area Network
- L2F: Layer 2 Forwarding
- L2TP: Layer 2 Tunneling Protocol
- NAT: Network Address Translator
- PPTP: Point-to-Point Tunneling Protocol
- OS: Operating System
- PC: Personal Computer
- PDA: Personal Digital Assistant
- RFC: Request for Comments
- SIPS: Secure Session Initiation Protocol
- SMTP: Simple Mail Transfer Protocol
- SOCKS: Secure Socket
- SOHO: office/home office
- SSH: Secure Shell
- SSL: Secure Socket Layer
- TCP: Transmission Control Protocol
- Tor: The Onion Router
- UDP: User Datagram Protocol
- VPN: Virtual Private Network
- WAN: Wide Area Network
- WLAN: Wireless Local Area Network