School of Computing Science and Engineering

Program: B.Tech CSE Hons With Specialization in CNCS

Course Code: CSCN4020

Course Name: Antivirus and Malware Analysis

Course Outcomes :

CO1	Students with a specialist understanding of the nature of malware, its capabilities, and how it is combated through detection and classification
CO2	Students will be able to apply the tools and methodologies used to perform static and dynamic analysis on unknown executables
CO3	Students will have an intimate understanding of executable formats, Windows internals and API, and analysis techniques.
CO4	Students will able to apply techniques and concepts to unpack, extract, decrypt, or bypass new anti-analysis techniques in future malware samples.
CO5	Students will understand what are the underlying scientific and logical limitations on society's ability to combat malware?
CO6	Students would have a broad understanding of the social, economic, and historical context in which malware occurs

Course Prerequisites

Basic knowledge of Computer Networks and various types of attacks

GALGOTIAS UNIVERSITY

School of Computing Science and Engineering

Course Code : Course Name:

Syllabus

UNIT I: Introduction **6 lecture hours**

Introduction and Firewalls - Firewall basics, advanced firewalls, Types of firewall configurations, Intrusion Detection and Prevention - Detection Methods, Intrusion Detection Systems, Intrusion Prevention Systems, Honeypots

UNIT II: Basics of Malware **6 lecture hours**

Introduction to malware, OS security concepts, malware threats, evolution of malware, malware types- viruses, worms, root kits, Trojans, bots, spyware, adware, logic bombs, malware analysis, static malware analysis, dynamic malware analysis

UNIT III: Malware Functionality **7 lecture hours**

Downloader, Backdoors, Credential Stealers, Persistence Mechanisms, Privilege Escalation, Covert malware launching- Launchers, Process Injection, Process Replacement, Hook Injection, Detours, APC injection

UNIT IV: Detection and Prevention Tools/Techniques **7 lecture hours**

Detection and Prevention tools - Anti-Virus/Anti-Malware, Snort, HIDs and HIPs, Splunk, Splunk and Security.

Malware Detection Techniques: Signature-based techniques: malware signatures, packed malware signature, metamorphic and polymorphic malware signature Non-signature based techniques: similarity-based techniques, machine-learning methods, invariant inferences.

UNIT V: Malware Case Study **7 lecture hours**

Android Malware: Malware Characterization, Case Studies – Plankton, DroidKungFu, AnserverBot, Smartphone (Apps) Security

Attacks are Inevitable - Case Study - Attacks are inevitable, Before the Attack, During the Attack, After the Attack, Real World Attacks

Understanding detection and mitigation - How data breaches are exposed

Unit VI: Advances and the Latest Trends **7 Lecture hours**

The advances and the latest trends in the course as well as the latest applications of the areas covered in the course.

The latest research conducted in the areas covered in the course.

Discussion of some latest papers published in IEEE transactions and ACM transactions, Web of Science and SCOPUS indexed journals as well as high impact factor conferences as well as symposiums.

Discussion on some of the latest products available in the market based on the areas covered in the course and patents filed in the areas covered in the course

Program Name: Program Code:

Recommended Books

Reference Book

1. Practical malware analysis The Hands-On Guide to Dissecting Malicious Software by Michael Sikorski and Andrew Honig ISBN-10: 159327-290-1, ISBN-13: 978-1-59327-290-6, 2012 2

2. Computer viruses: from theory to applications by Filiol, Eric Springer Science & Business Media, 2006

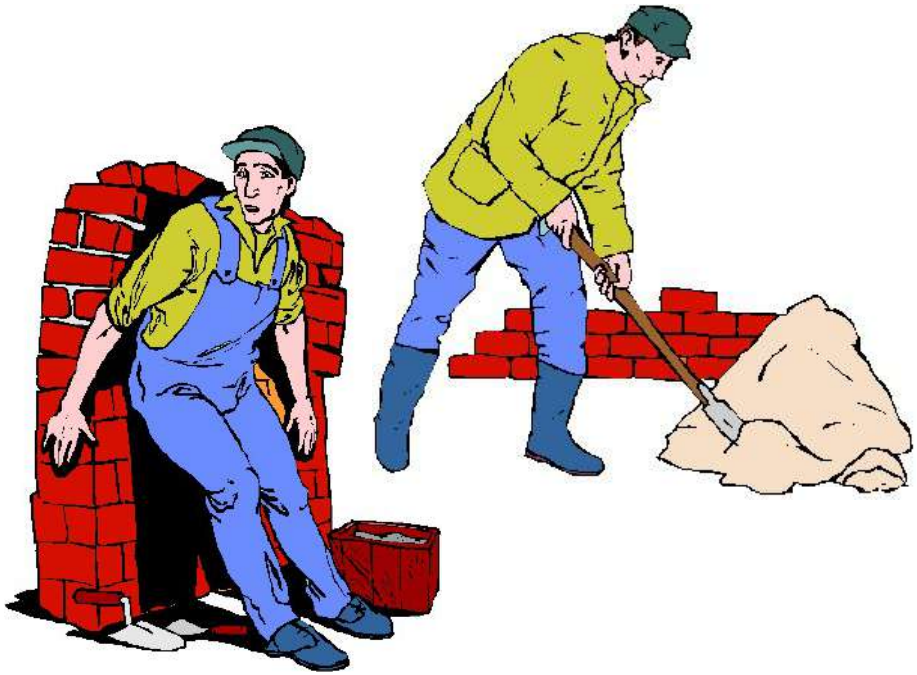
3. Android Malware by Xuxian Jiang and Yajin Zhou, Springer ISBN 978-1-4614-7393-0, 2005

4. Hacking exposed™ malware & rootkits: malware & rootkits security secrets & Solutions by Michael Davis, Sean Bodmer, Aaron Lemasters, McGraw-Hill, ISBN: 978-0-07-159119-5, 2010

5. Windows Malware Analysis Essentials by Victor Marak, Packt Publishing, 2015


Thank You

Firewall Essentials



Welcome to Introduction to Firewall Essentials

This course is intended to provide you with an understanding of key concepts and theories associated with firewalls, security policies and attacks directed toward your network.

Course Objectives

- Understand firewall basics, including the definition of a firewall, firewall functions and the need for firewalls
- Understand firewall technologies, including TCP/IP basics, routers and application-level gateways (proxies)

Course Objectives (cont.)

- Understand security hazards
- Understand cryptography, including the need for encryption and virtual private networks (VPNs)

Course Map

- Firewall Essentials
  - What is a Firewall?
  - Types of Firewalls
  - How Firewalls Work

Course Map

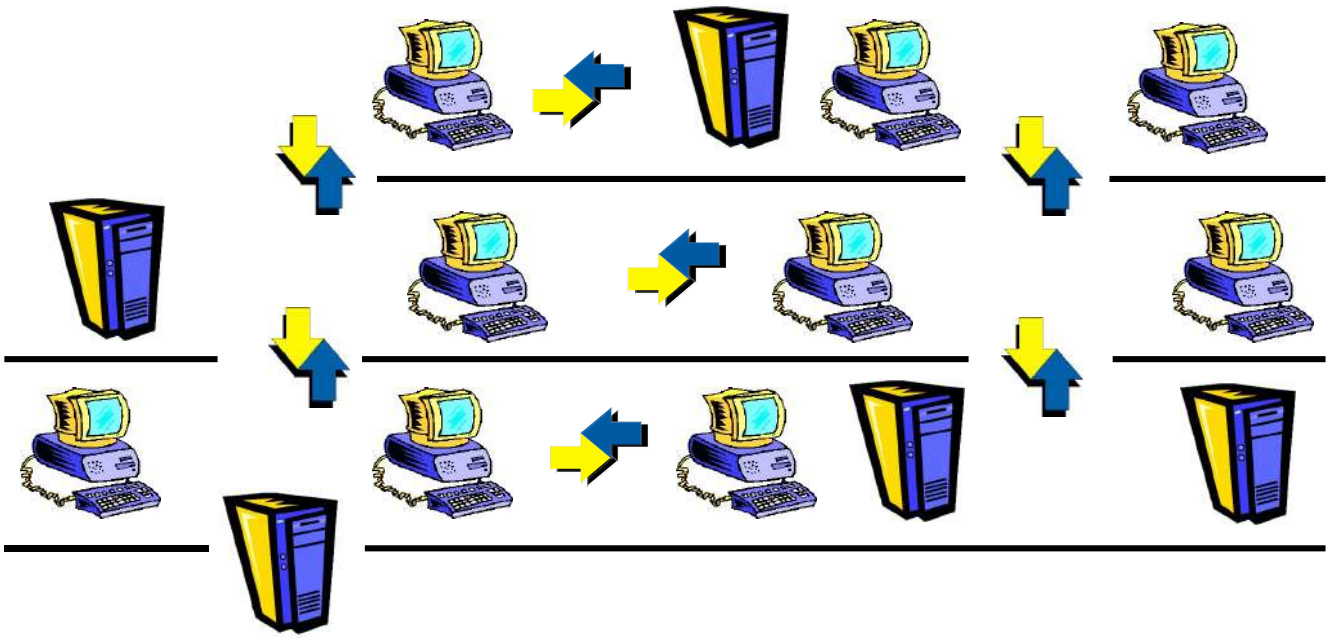
- Firewall Essentials
  - The Need for a Firewall
  - Security Hazards

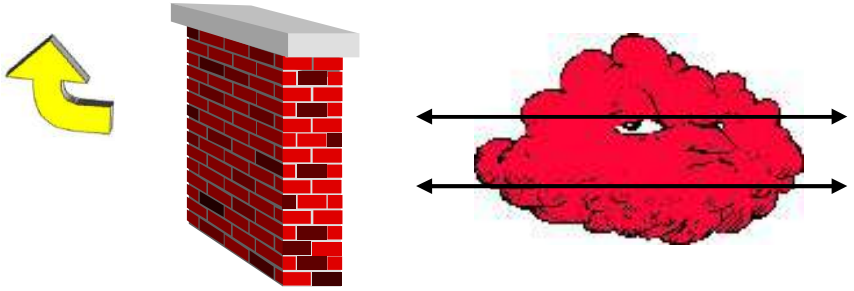
Course Map

- Firewall Essentials
  - Firewall Features
  - Security Policies

What is a Firewall?

Securing a Network



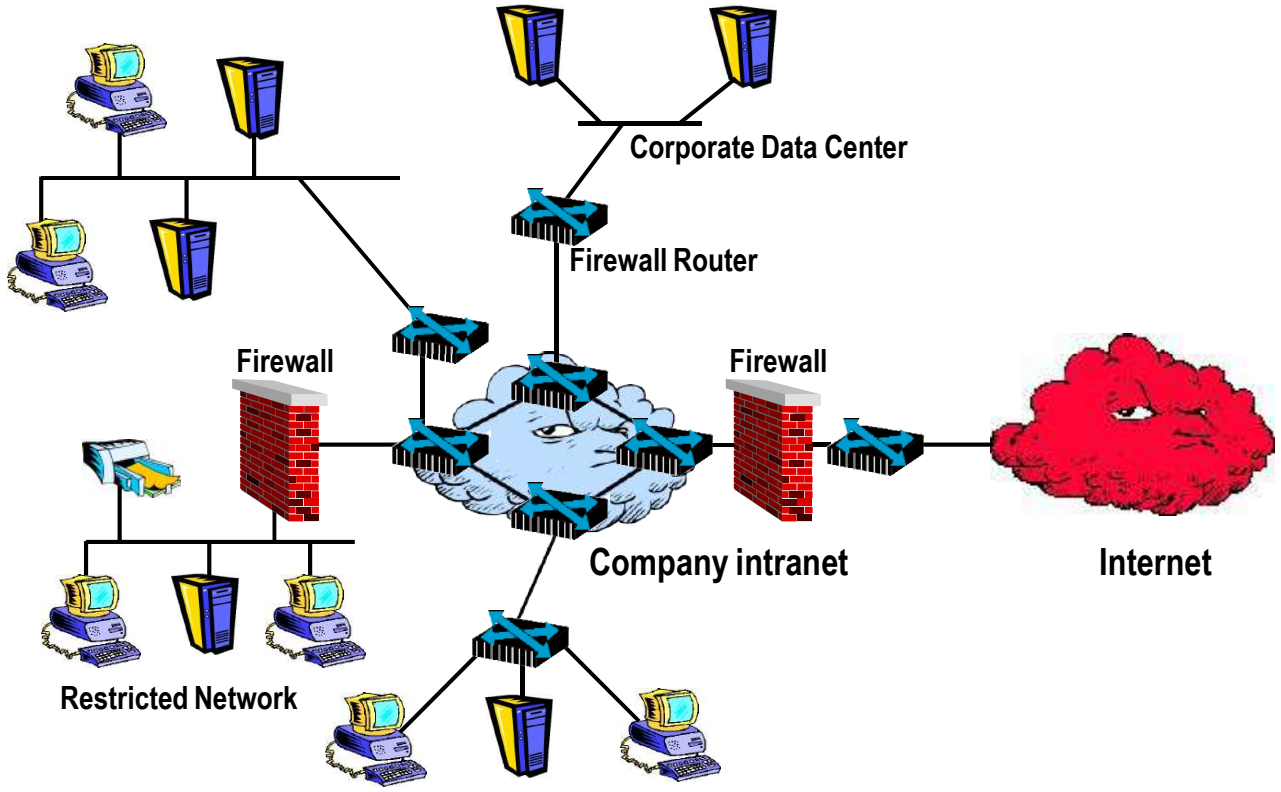


Firewall Visiting Packets

Firewall Location

- Placed at the entrance to an organization's intranet
- Placed inside an internal network
- Placed between RAS and internal network
- It is the check point for communication to an outside network

Firewall Location



Communicating Across a

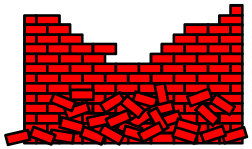
Network

- Network packet (level 3)
- Network session (level 7)

Network Packet

- Contains all the information required to route it to the final destination
- Contains the information to deliver it to the correct application on the destination system
- Requires five specific pieces of information for routing

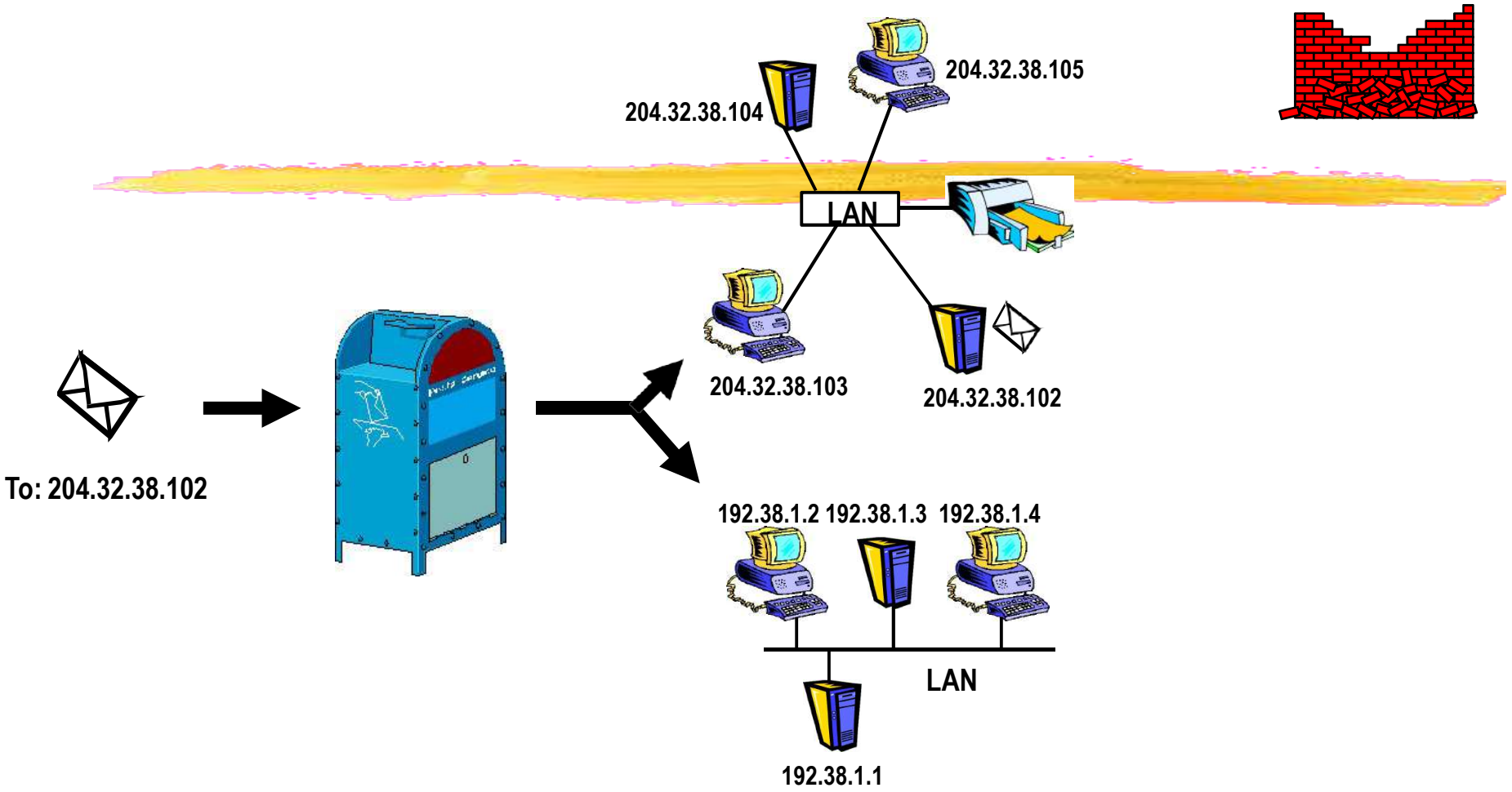
Comparing IP Packet with a Letter Address



IP Packet Components	U. S. Mail Address Components	Comments
Destination IP address	Street address and zip code	Each host on an IP Internet or intranet must have a unique IP address
Protocol	Organization name	The standard protocols above IP are TCP and UDP
Destination port number	Recipient name	Identifies the network application to receive the packet
Source IP address	Sender's return address	So the application knows where to send replies
Source port number	Sender's name	To identify the application of the sending host for return packets

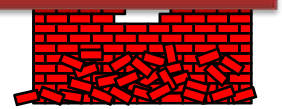
Division of IP Address

- Network - similar to a zip code, the primary information used by routers to deliver the packet to the correct LAN
- Host - similar to a letter address, directs the packet to the correct host on the LAN



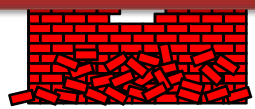
“Mailing” a Letter

Network Session



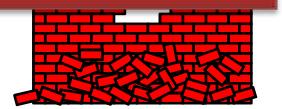
- The total data sent between an initial request and the completion of that request
- Evident at the user or application level of the protocol stack

Standard Firewall Services



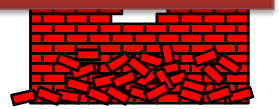
- Access Control
- Authentication
- Activity Logging
- Other Firewall Services

Access Control

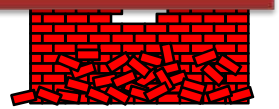


- Allows the firewall to consider the network interface where the packet enters
- Prevents or limits IP spoofing
- “Don’t talk to me unless I talk to you first”

Authentication



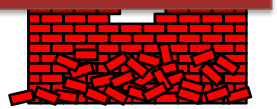
- Standards have usually relied on passwords or smartcards or token
- No based on IP address but user level



Activity Logging

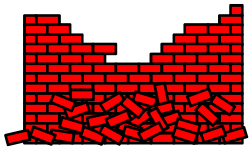
- Allows the firewall to record information concerning all successful and failed session attempts
- Referred to as an audit log

Other Firewall Services



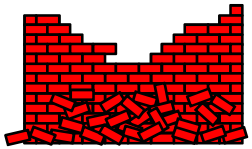
- Proxy Applications
- Virus Scanning
- Address Mapping
- Virtual Private Networks (VPN)

Firewall Administration Interfaces



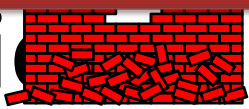
- Three classes of firewall administrator interfaces:
  - Text-file based administration
  - Text-menu based administration
  - GUI-based administration

Text-File Based Administration



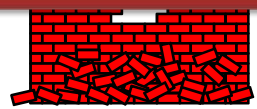
- Popular in routers and homegrown firewalls
- Interface of choice for UNIX administrators
- Easier to make errors

Text-Menu Based Administrati



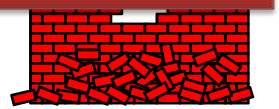
- Reduces likelihood of errors
- Less flexibility of control
- Limited visual feedback to changes made

GUI-Based Administration

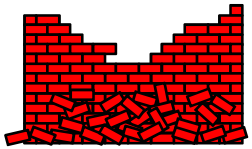


- Most prominent
- Easier to use
- Less prone to errors

Actual Security Provided

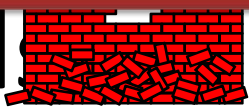


- A firewall can reduce the vulnerabilities on a network, not eliminate them
- Firewalls act as filters



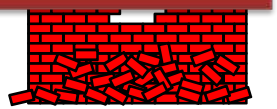
Types of Firewalls

Three Basic Types of Firewall



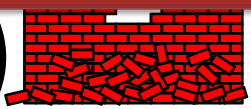
- Packet Filter
- Application-Level Gateway
- Stateful Inspection

Packet Filter Firewall



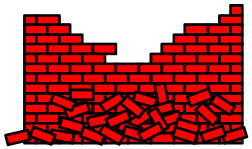
- Referred to as filtering routers with a set of simple rules
- Determines whether a packet should pass based on the source and destination information within the packet
- Process is performed at the kernel level

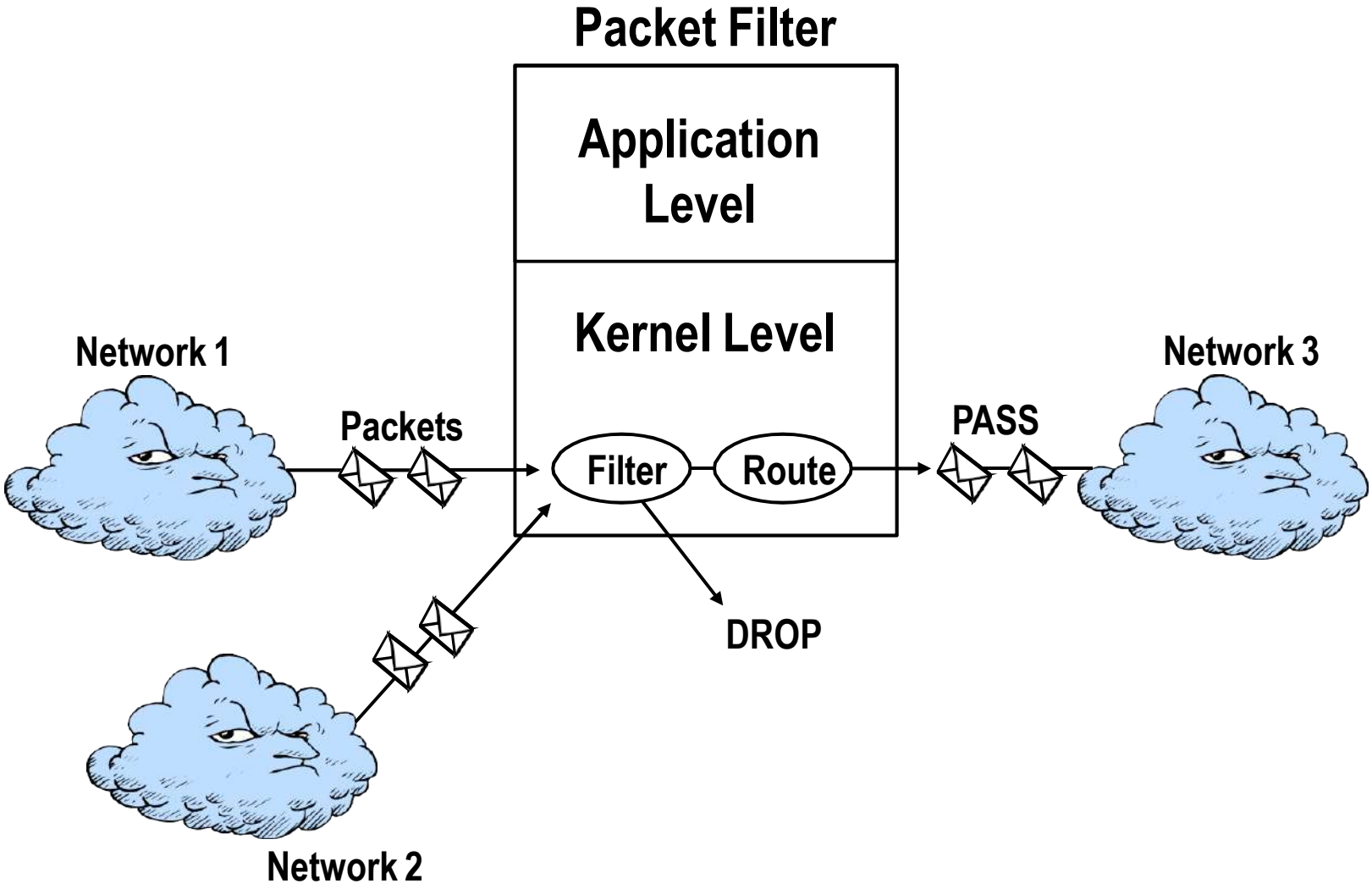
Packet Filter Firewall (cont.)



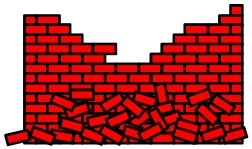
- Less secure than application-level gateway firewalls

Packet Filtering Firewall

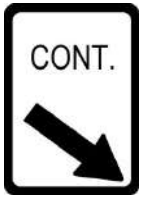




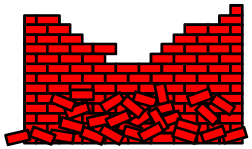
Application-level Gateway Firewall



- Does not allow packets to pass directly between networks
- Original connections are made to a proxy on the firewall

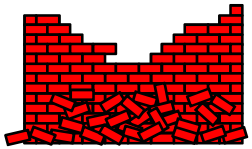


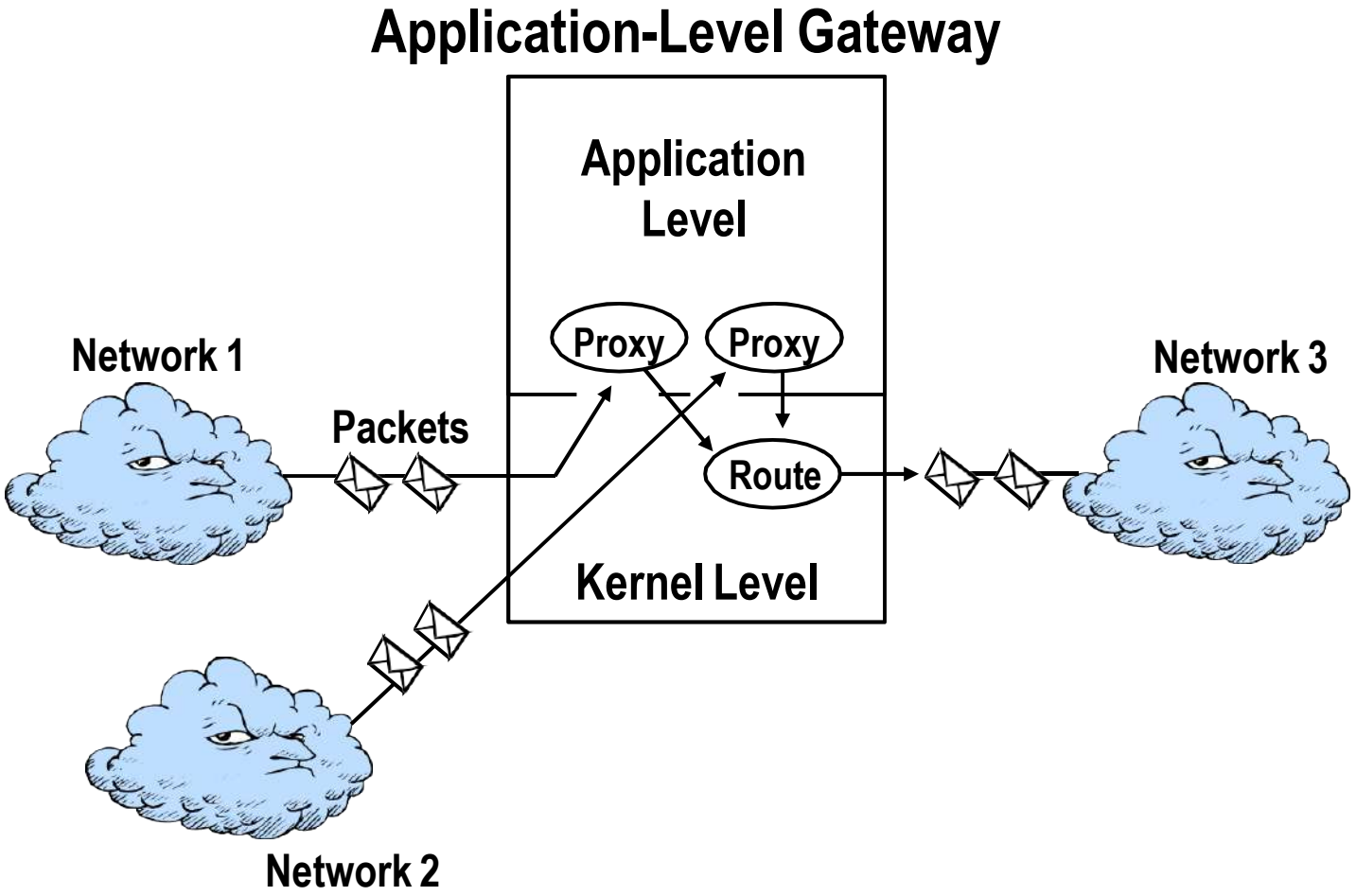
Application-level Gateway Firewall (cont.)



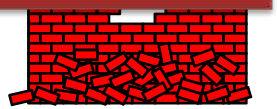
- Requires a separate application for each network service
  - TELNET
  - FTP
  - E-mail
  - WWW

Application-level Gateway Firewall



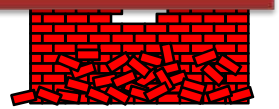


Stateful Packet Filtering



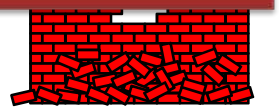
- Ensures the highest level of firewall security by performing the following functions:
  - Accessing, analyzing and utilizing communication information
  - Communication-derived state
  - Application-derived state
  - Information Manipulation

Stateful Inspection



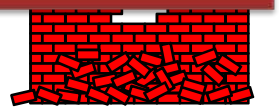
- Communication information
  - Information from all seven layers of the packet

Stateful Inspection



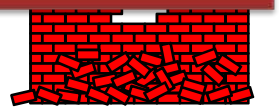
- Communication-derived state
  - State information derived from previous communications

Stateful Inspection



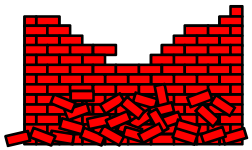
- Application-derived state
  - State information derived from other applications

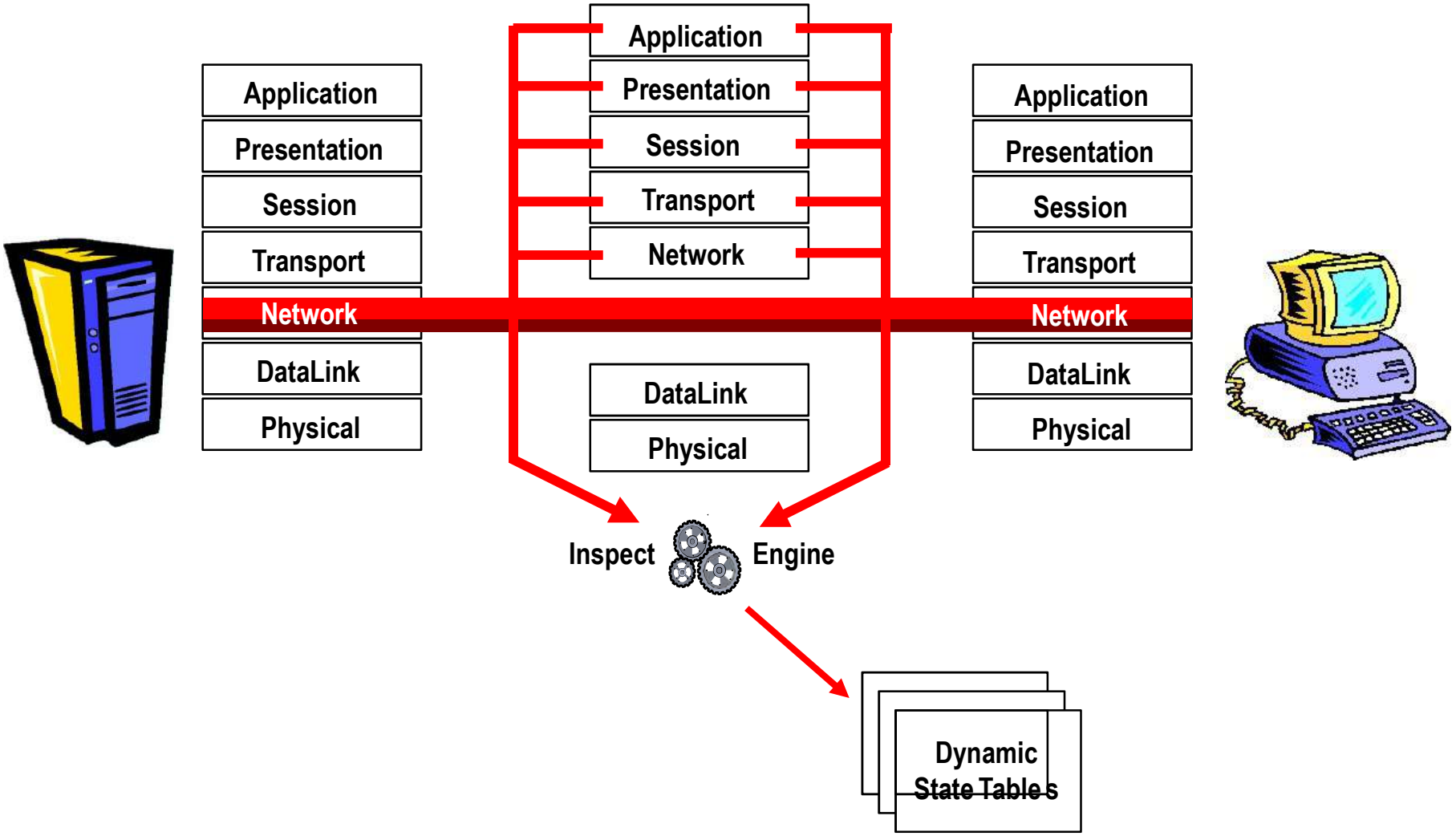
Stateful Inspection



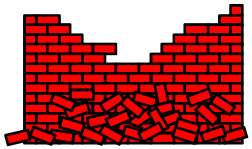
- Information manipulation
  - Evaluation of flexible expressions based on the following:
    - communication information
    - communication-derived state
    - application-derived state

Check Point's FireWall-1 Stateful Inspection

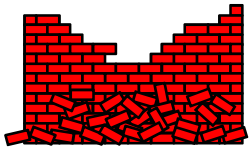




Comparison of Firewall Architecture

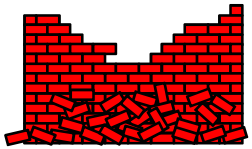


Firewall Capability	Packet Filters	Application Level Gateways	Stateful Inspection
Communication information	Partial	Partial	Yes
Communication-derived state	No	Partial	Yes
Application-derived state	No	Yes	Yes
Information manipulation	Partial	Yes	Yes



How Firewalls Work

How Firewalls Work: Objectives



- Identify the packet processing locations on a firewall
- Describe packet filtering and its limitations
- Describe proxy applications and their limitations
- Identify user authentication
- Describe firewall auditing