ISOM 5280
Protection Tools

Prof. Weiyin Hong

Department of ISOM, HKUST Business School

Fall 2024

Organization View of Cybersecurity

Table of Contents (Protection)

- End-point protection (Antivirus/Antimalware/Patches/Upgrades)

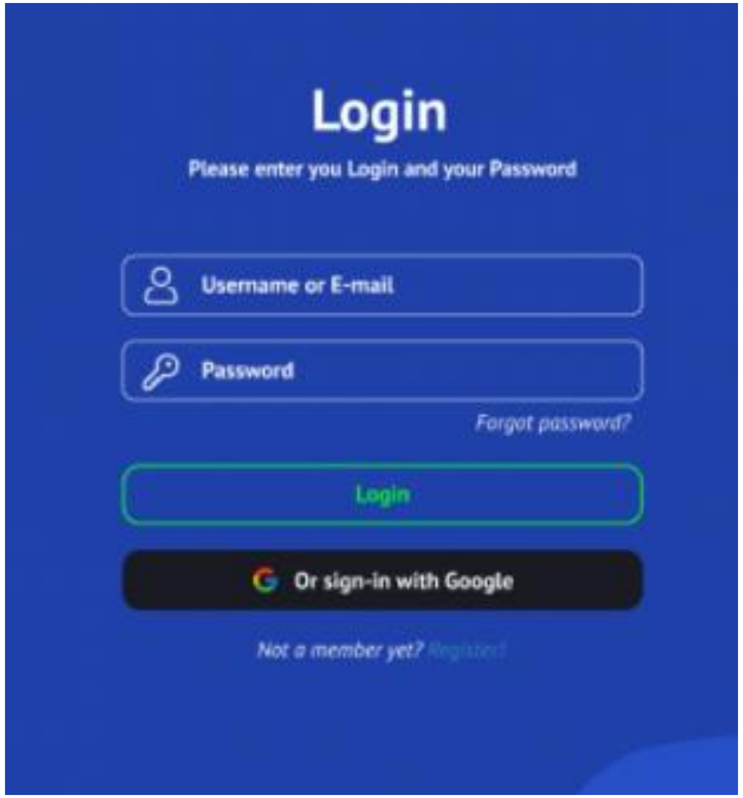
1. Authentication method (access control)
2. Firewall
3. IDPS
4. Honeypots
5. VPN

- Cryptography

Reading

- [WM] – Chapters 8 and 9

1. Does Authentication Work?



- 63% of network intrusions are the result of compromised **user passwords and usernames**. (Microsoft)
- 91% of people know the risks of reusing passwords across their online accounts, which inherently leads to a higher risk of password theft and credential misuse. Despite this, 66% do it anyway. (LastPass Psychology of Passwords)

1. Authentication Methods

- Something you know
  - Password, security questions

** What is the name of your high school?*

- Something you have
  - Token, SMS, ID card

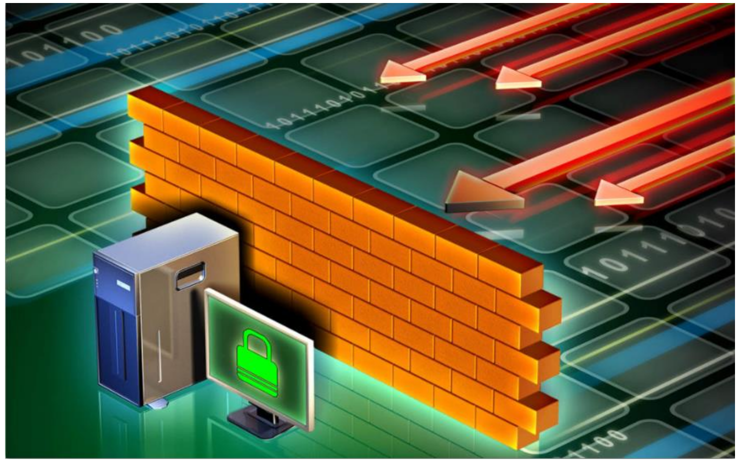
- Something you are or can produce
  - Signature, retina scan, facial recognition, voice

- What's the most effective way to construct two-factor authentication using the above pieces of information? – combine methods across categories.

故宮博物院

2. Firewall

- A specific type of computing facility to control network traffic, and keep your organization's internal network (or other devices, data, applications, etc.) safe from outside threats
  - Plays the role of a "gatekeeper" to segment corporate networks from the Internet
  - Regulates all inbound traffics, outbound traffics
  - Can be implemented as hardware or software



Firewall Architecture

- Single Bastion Hosts
- Dual-homed Bastion Host
- Screened Subnet
- Screened Subnet with DMZ (Demilitarized Zone)

Single Bastion Hosts

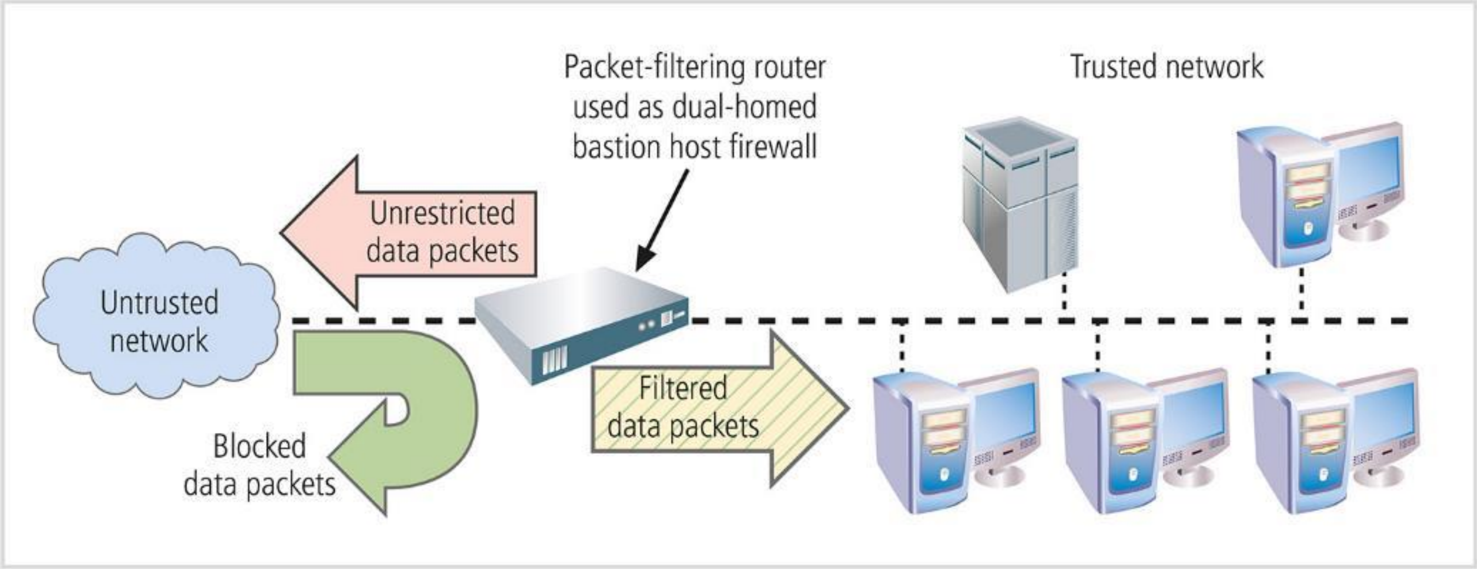

Packet-filtering router used as dual-homed bastion host firewall
Trusted network
Unrestricted data packets
Untrusted network
Blocked data packets
Filtered data packets

Figure 8-10 **Packet-filtering router**

Dual-Homed Bastion Host firewall

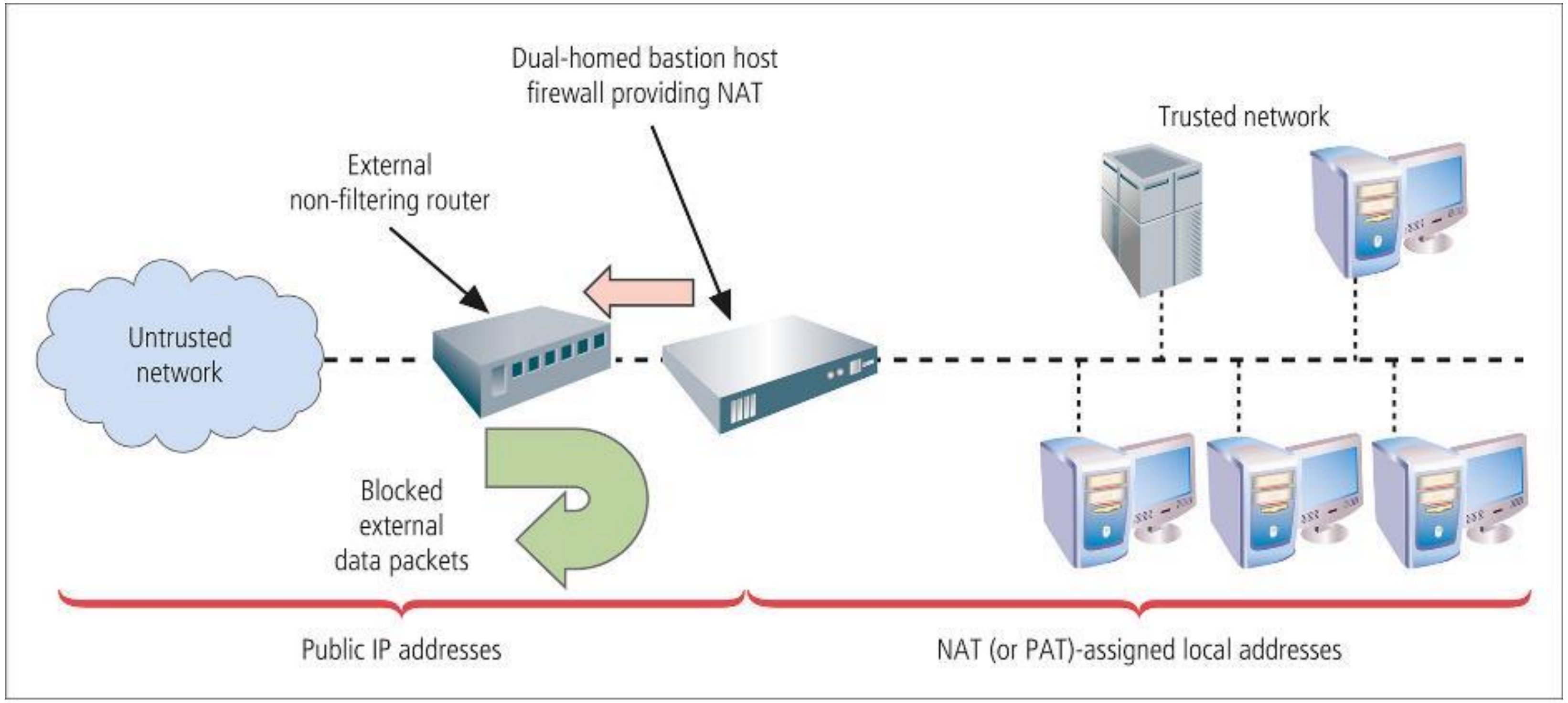

Dual-homed bastion host firewall providing NAT
Trusted network
External non-filtering router
Untrusted network
Blocked external data packets
Public IP addresses
NAT (or PAT)-assigned local addresses

Figure 8-12 **Dual-homed bastion host firewall architecture**

Screened Subnet Architecture

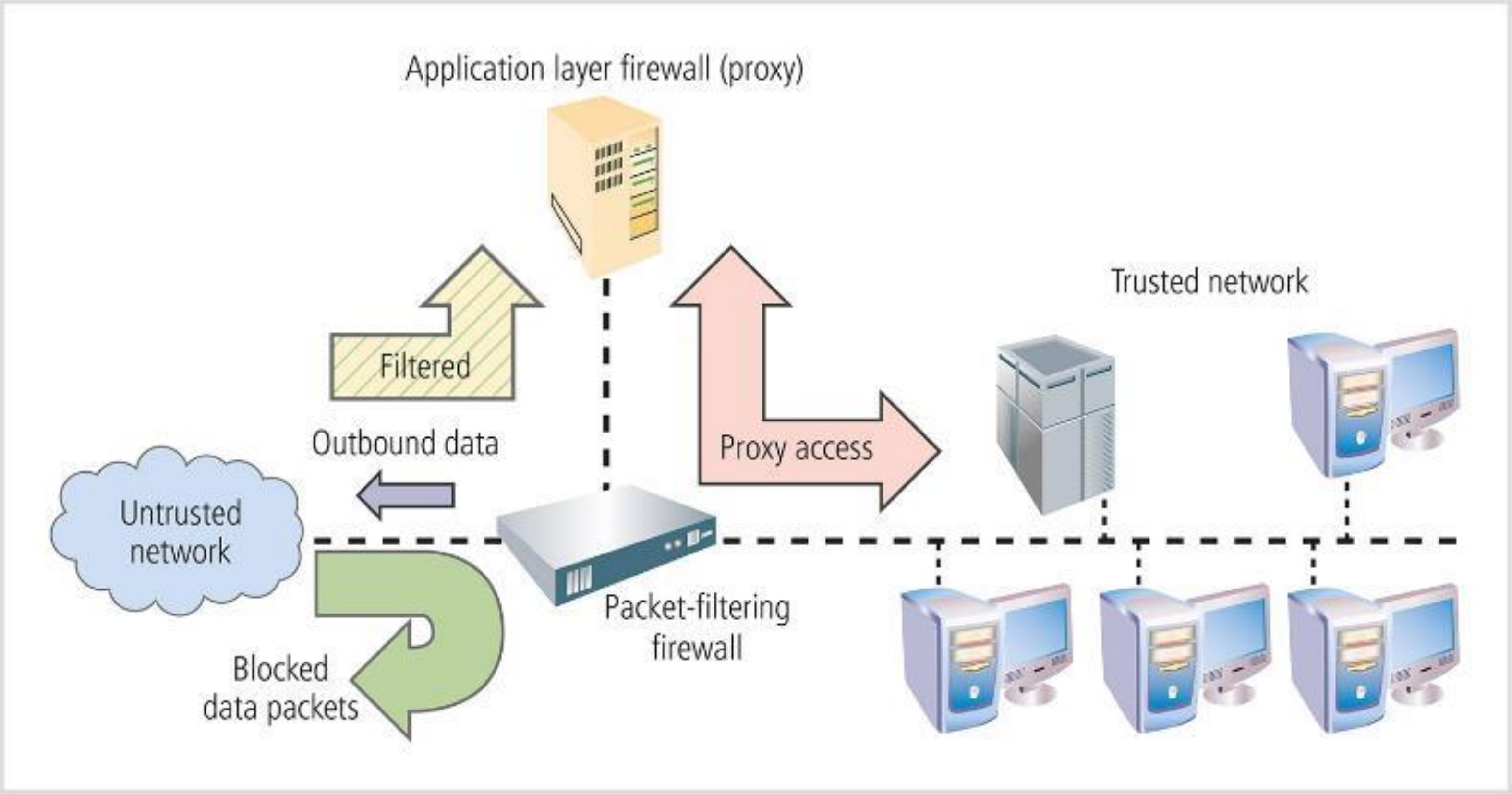
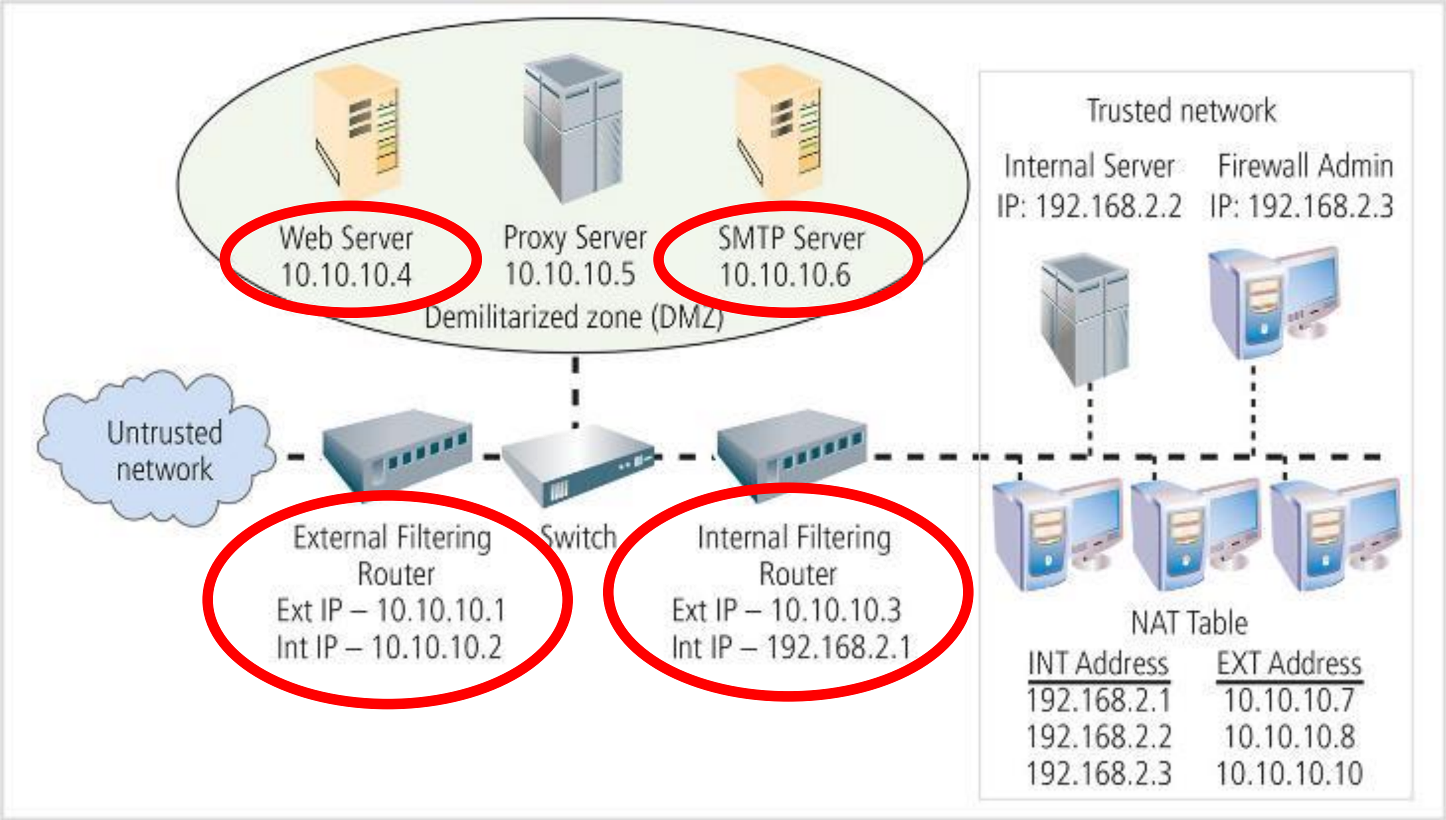


Figure 8-13 **Screened host firewall architecture**

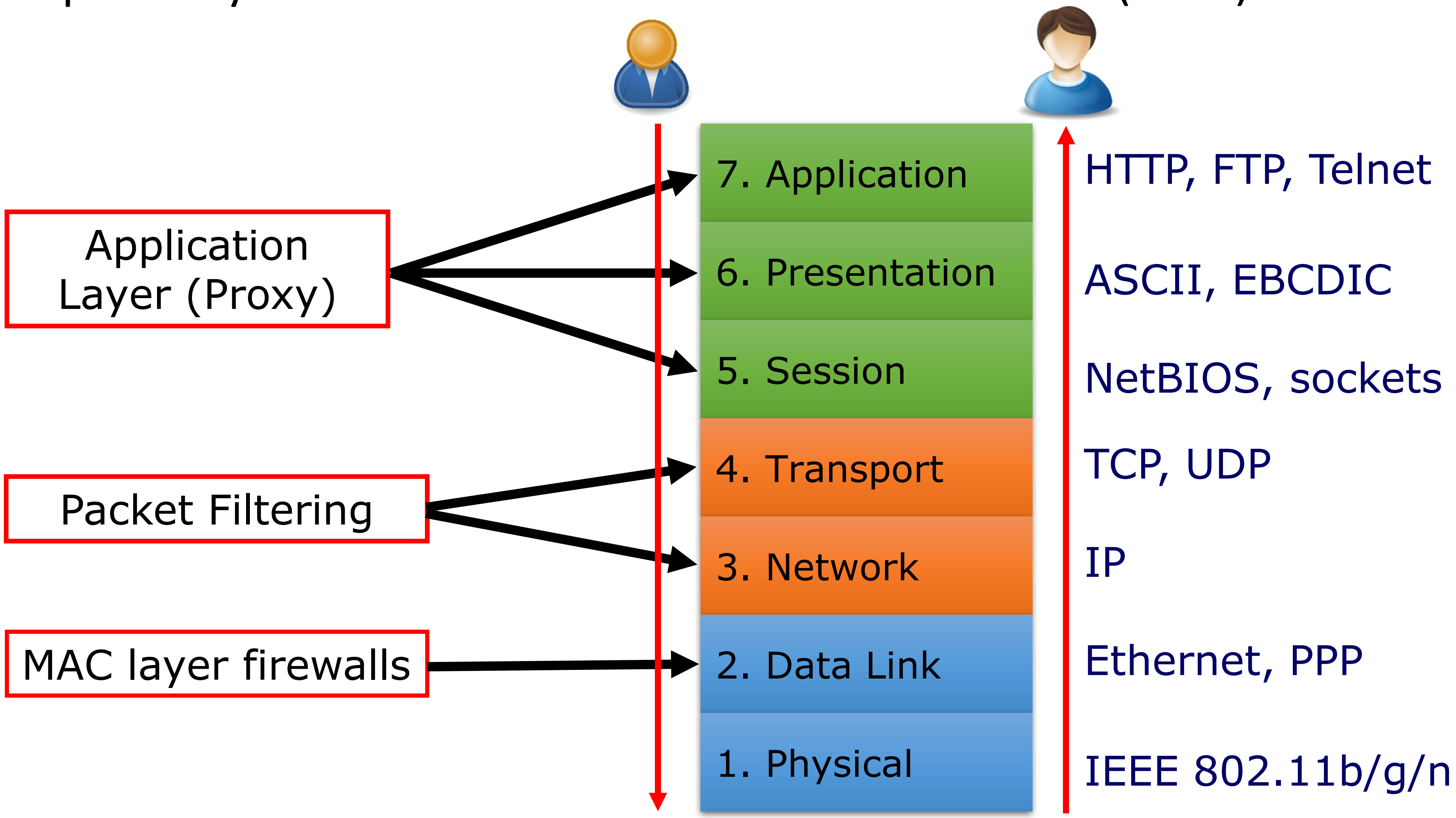
Screened Subnet with DMZ



INT Address	EXT Address
192.168.2.1	10.10.10.7
192.168.2.2	10.10.10.8
192.168.2.3	10.10.10.10

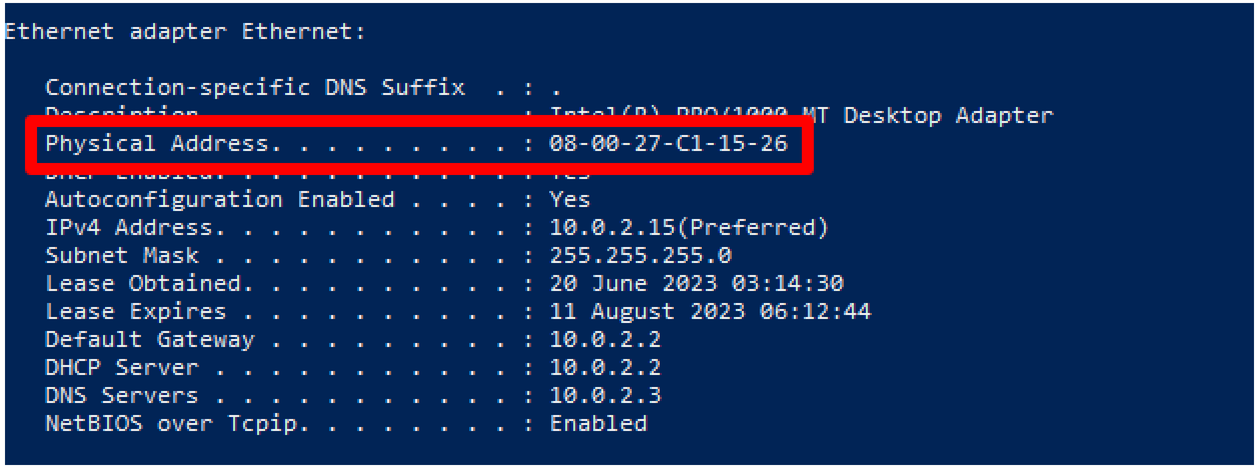
Figure 8-15 Second example of screened subnet with DMZ

Open System Interconnection Model (OSI)



Application Layer (Proxy)	7. Application	HTTP, FTP, Telnet
	6. Presentation	ASCII, EBCDIC
	5. Session	NetBIOS, sockets
Packet Filtering	4. Transport	TCP, UDP
	3. Network	IP
MAC layer firewalls	2. Data Link	Ethernet, PPP
	1. Physical	IEEE 802.11b/g/n

MAC Layer Firewall (Media Access Control)



```
Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : .
   Description . . . . . . . . . . . : Intel(R) PRO/1000 MT Desktop Adapter
   Physical Address. . . . . . . . . : 08-00-27-C1-15-26
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 10.0.2.15(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : 20 June 2023 03:14:30
   Lease Expires . . . . . . . . . . : 11 August 2023 06:12:44
   Default Gateway . . . . . . . . . : 10.0.2.2
   DHCP Server . . . . . . . . . . . : 10.0.2.2
   DNS Servers . . . . . . . . . . . : 10.0.2.3
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

A **MAC address**, or **Media Access Control address**, is a unique identifier assigned to a network interface controller (NIC) for use as a network address in communications within a network segment.

Packet Filtering Firewalls

ISOM 5280

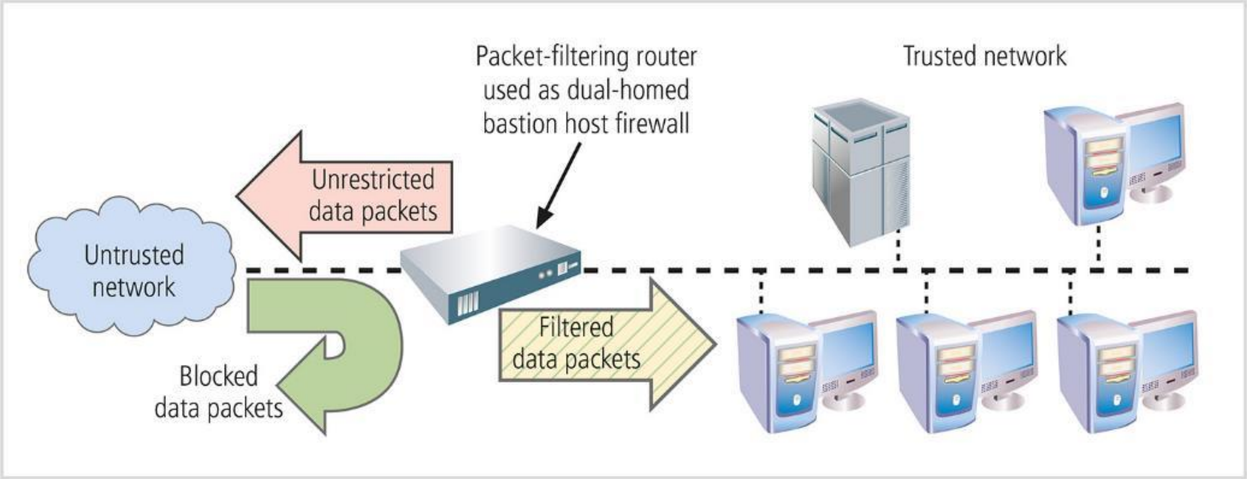
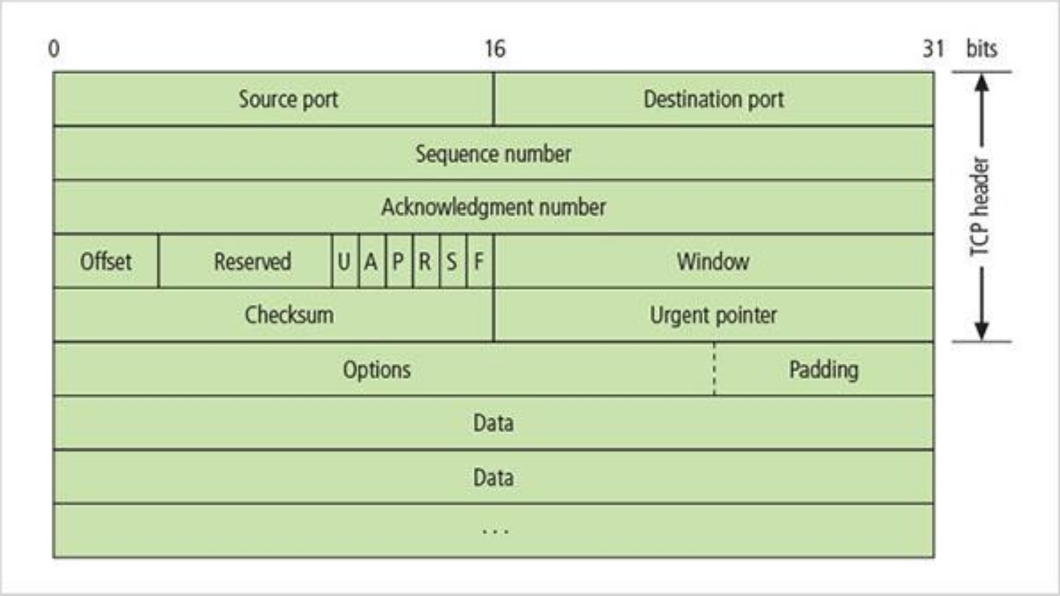

Packet-filtering router used as dual-homed bastion host firewall
Trusted network
Unrestricted data packets
Untrusted network
Filtered data packets
Blocked data packets

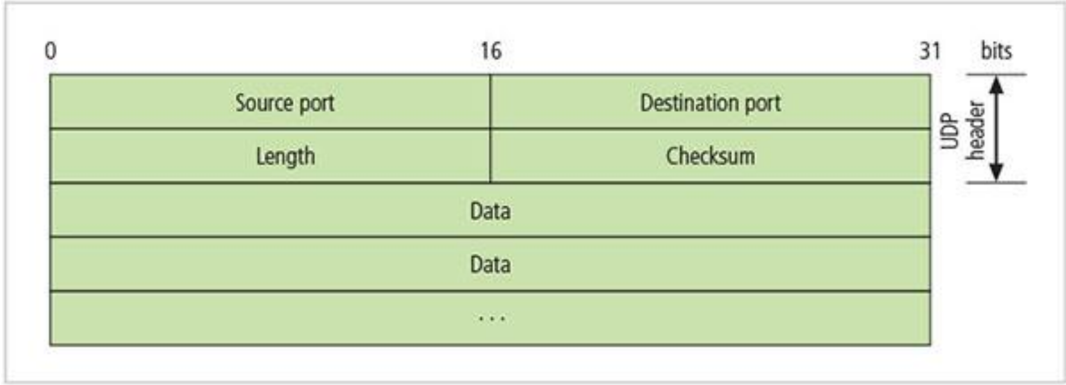
Figure 8-10 Packet-filtering router

Packet Structure



<table>
<tr><th colspan="8">0 … 16</th><th>… 31 bits</th></tr>
<tr><td colspan="8">Source port</td><td>Destination port</td></tr>
<tr><td colspan="9">Sequence number</td></tr>
<tr><td colspan="9">Acknowledgment number</td></tr>
<tr><td>Offset</td><td>Reserved</td><td>U</td><td>A</td><td>P</td><td>R</td><td>S</td><td>F</td><td>Window</td></tr>
<tr><td colspan="8">Checksum</td><td>Urgent pointer</td></tr>
<tr><td colspan="8">Options</td><td>Padding</td></tr>
<tr><td colspan="9">Data</td></tr>
<tr><td colspan="9">Data</td></tr>
<tr><td colspan="9">. . .</td></tr>
</table>

TCP/IP



0 … 16	… 31 bits
Source port	Destination port
Length	Checksum
Data	
Data	
. . .	

UDP

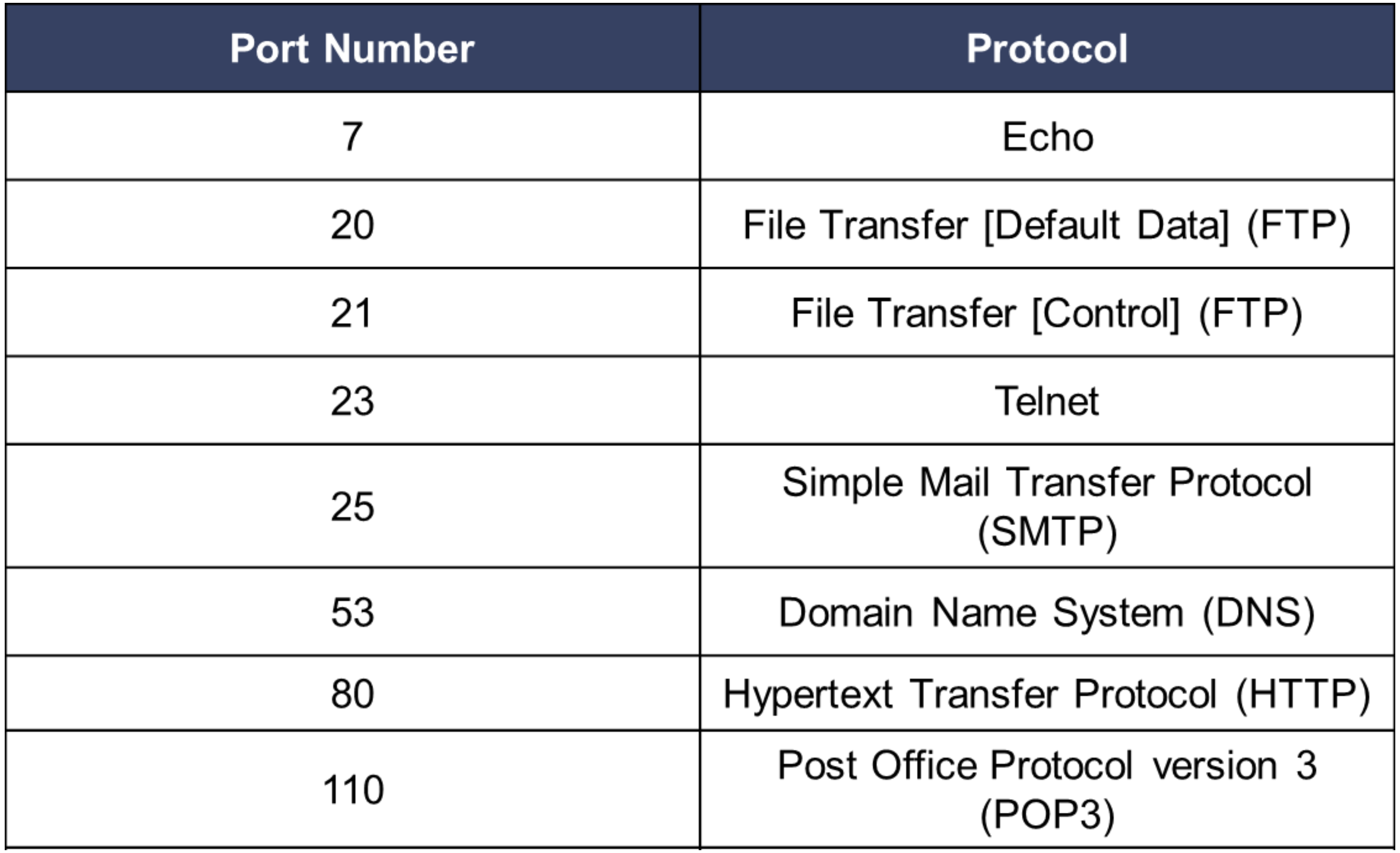
Stateless Firewall (Static Packet Filtering)

- Most basic form of firewall protection
- Accept/reject data packets based on the packets’ header information
  - Source and destination IP addresses via an access control list (ACL) (i.e., firewall rule set)
- Efficient and low cost as it only examines header information of packets
- No concept of “state” of packets, which makes it less secure
- Has no way of knowing if any given packet is part of an existing connection, is trying to establish a new connection or is just a rogue packet

Static Packet Filtering - Rules

Source Address	Source Port	Destination Address	Destination Port	Action
Any	Any	10.10.10.x	>1023	Allow
Any	Any	10.10.10.1	Any	Deny
10.10.10.x	Any	Any	Any	Allow
Any	Any	10.10.10.6	25	Allow
Any	Any	10.10.10.x	7	Deny
10.10.10.x	Any	10.10.10.x	23	Allow
Any	Any	10.10.10.x	23	Deny
Any	Any	10.10.10.4	80	Allow
10.10.10.4	Any	10.10.10.8	80	Allow
Any	Any	Any	Any	Deny

Common Port Numbers



Port Number	Protocol
7	Echo
20	File Transfer [Default Data] (FTP)
21	File Transfer [Control] (FTP)
23	Telnet
25	Simple Mail Transfer Protocol (SMTP)
53	Domain Name System (DNS)
80	Hypertext Transfer Protocol (HTTP)
110	Post Office Protocol version 3 (POP3)

Static Packet Filtering - Rules

Source Address	Source Port	Destination Address	Destination Port	Action	
Any	Any	10.10.10.x	>1023	Allow	Response to internal requests are allowed
Any	Any	10.10.10.1	Any	Deny	The firewall device is never accessible directly from the public network
10.10.10.x	Any	Any	Any	Allow	All traffic from the trusted network is allowed out
Any	Any	10.10.10.6	25	Allow	All email traffic allowed to the SMTP server but only at port 25
Any	Any	10.10.10.x	7	Deny	All ICMP (i.e., ping) requests should be denied.
10.10.10.x	Any	10.10.10.x	23	Allow	Telnet connections allowed among internal devices
Any	Any	10.10.10.x	23	Deny	Telnet requests from external to internal devices denied.
Any	Any	10.10.10.4	80	Allow	All HTTP requests are allowed to web/proxy servers in DMZ
10.10.10.4	Any	10.10.10.8	80	Allow	Then web/proxy servers in DMZ are allowed to reach internal network
Any	Any	Any	Any	Deny	All other types of traffic denied

Menti.com

- Does encrypted traffic affect how firewall works? - no

- How many rules do you think there will be? – from a few hundreds to a few thousands and even more, depending on the size of the organization

- Will inbound rules be different from outbound rules? - yes

- What should be the last rule? – deny all

- Subject to what type of attack? – spoofing attack

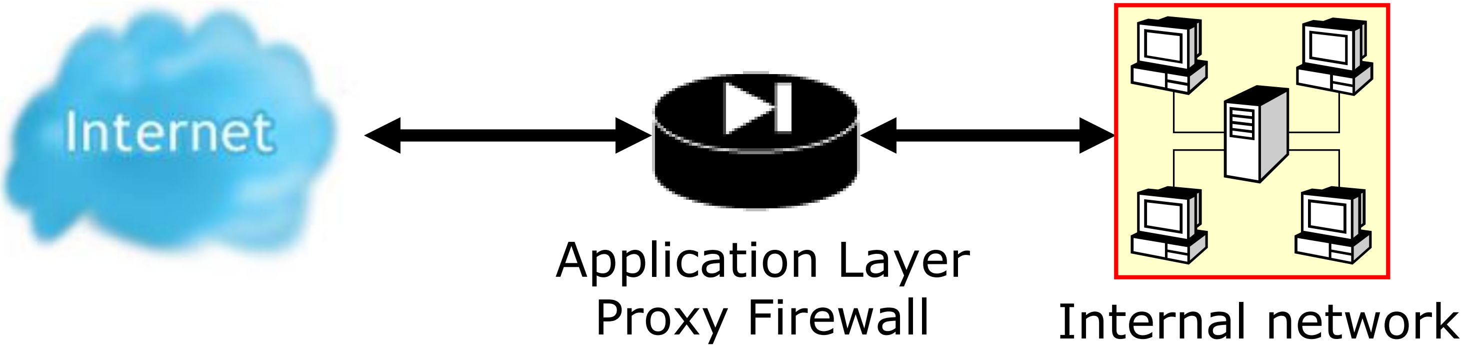
Stateful Firewall (Dynamic Packet Filtering)

- Keep track of connection status using a state table and a firewall ruleset
  - Accept traffic from the outside that matches an existing entry in the dynamic state table
  - Could be slower than packet filtering firewall
  - Far more secure than packet filtering firewall
  - Additional processing cost in order to maintain the state table

Source address	Destination address	Destination port	Time remaining	Total time	Protocol
192.168.2.5	10.10.10.7	80	2275	3600	TCP

Application Layer (Proxy) Firewall

- Sits between the internal network and the outside servers and gateways; serves as an intermediary that allows two systems to communicate indirectly; Hides internal network configuration
- Typically installed in a dedicated computer separate from the filtering router
- Allow or deny incoming traffic related to applications or services, such as web or FTP
- Checks IPs; validates TCP handshakes; deep packet and stateful inspections; audit and logging; user authentication



Firewall Prices

	Cisco ASA 5500-X	SonicWall TZ	Fortinet FortiGate	pfSense	Cisco Firepower	Cisco Meraki MX
trScore	8.0 (15+ Ratings)	9.4 (30+ Ratings)	8.7 (140+ Ratings)	9.0 (35+ Ratings)	8.4 (10+ Ratings)	9.0 (90+ Ratings)
Additional services included in pricing?	Yes	No	Yes	No	Yes	No
Small-Scale(<1 Gbps Throughput)	~$400	$300-600	$250-2,000	$179	~$500	$595-5,000
Mid-Range(1-4 Gbps Throughput)	$1,500-20,000	$800-1,500	$2,000-20,000	$199-699	$2,000-15,000	$9,995
Campus/Enterprise(5+ Gbps Throughput)	N/A	$1,600-2,300	$30,000-300,000	$899-2,649	$22,000-200,000	$19,995

Food for thought:

- Can firewalls (as introduced in today’s lecture) be used to stop a DDoS attack? And why?

Table of Contents (Continues…)

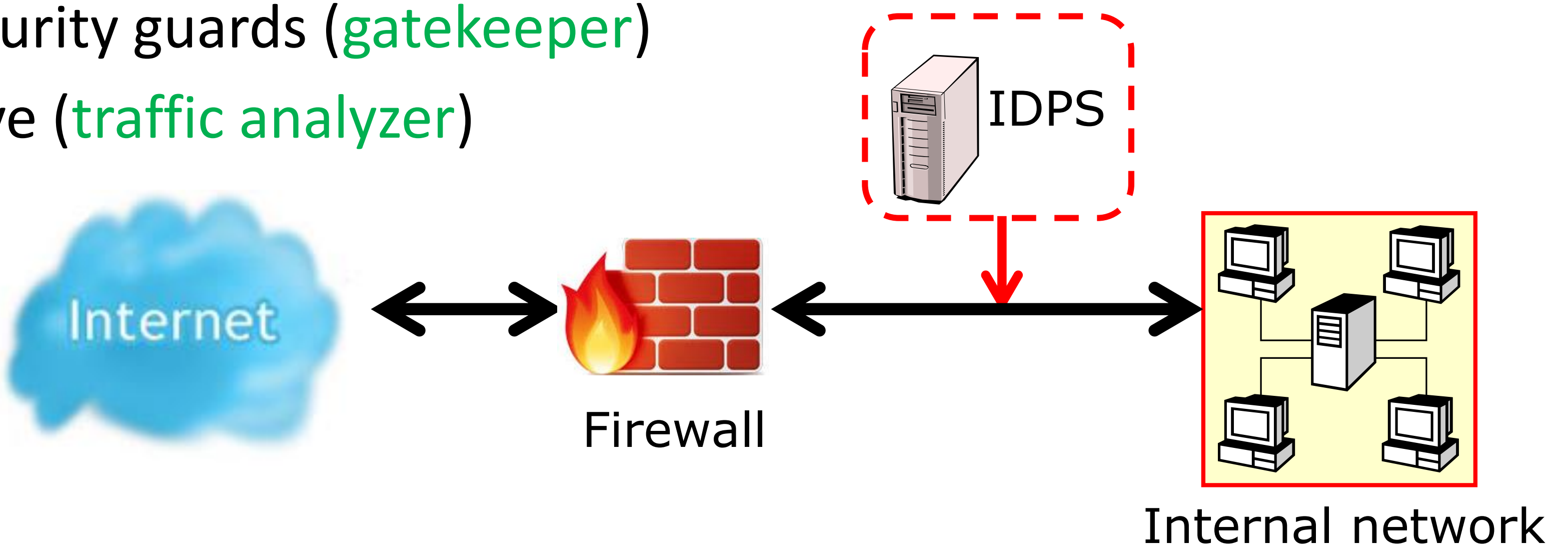
- Antivirus/Antimalware/Patches/Upgrades

1. Authentication method
2. Firewall
3. IDPS
4. Honeypots
5. VPN

- Cryptography

3. Intrusion Detection

- Intrusion detection (prevention) system – detection, reaction, correction, and prevention
- How does IDS differ from a firewall?
  - Firewall: security guards (gatekeeper)
  - IDS: detective (traffic analyzer)



Stateful Protocol Analysis (SPA)

- Stores and uses relevant data detected in a session to identify intrusions involving multiple requests/responses and allows IDPS to better detect specialized, multisession attacks (also called deep packet inspection).
- Drawbacks are analytical complexity, heavy processing overhead, and failure to detect intrusion unless protocol violates fundamental behavior.

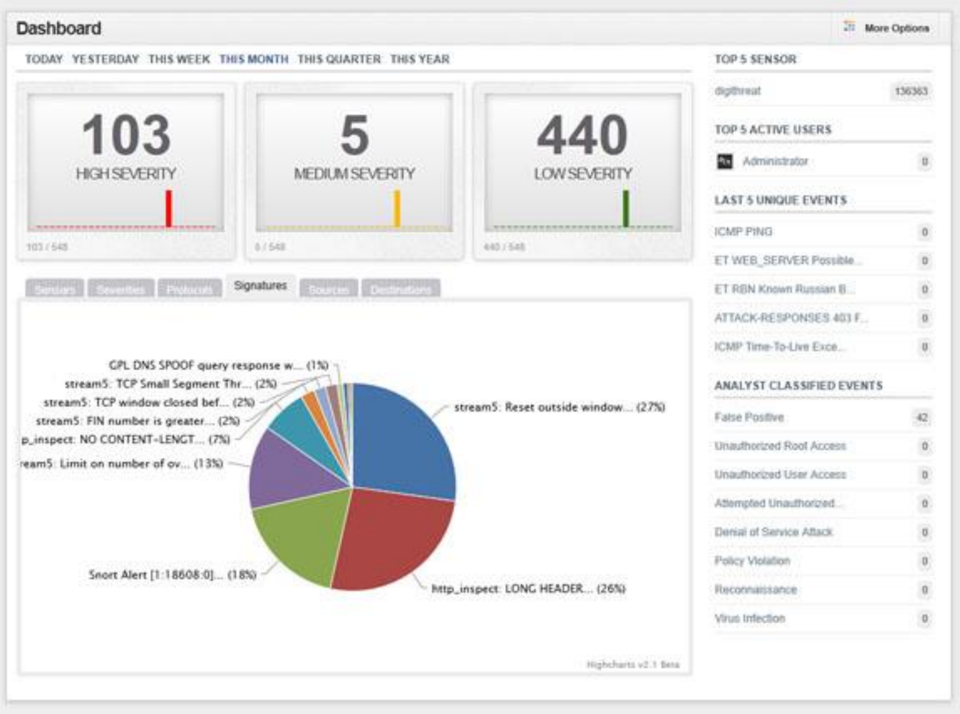
Differences Between Firewall and IDPS

- Only examines header
- Sits at perimeter of a network
- Block packets by IP/port
- Rule-based
- Like a doorman
- Easier to implement

- Examines header and payload
- Sits between firewall and trusted network
- Analyze packets, signal alarm and take actions (drop, alert, or clean)
- Rule-based or anomaly-based
- Like a patrol or a bodyguard
- More complex configuration

Detection Methods

- Signature-based – match traffic or data patterns with pre-defined or known attack (suspicious) patterns
- Statistical anomaly-based – sample network activities and compare them with “normal” baselines



Dashboard

More Options
TODAY
YESTERDAY
THIS WEEK
THIS MONTH
THIS QUARTER
THIS YEAR
Sensors
Severities
Protocols
Signatures
Sources
Destinations
GPL DNS SPOOF query response w... (1%)
stream5: TCP Small Segment Thr... (2%)
stream5: TCP window closed bef... (2%)
stream5: FIN number is greater... (2%)
p_inspect: NO CONTENT-LENGT... (7%)
ream5: Limit on number of ov... (13%)
Snort Alert [1:18608:0]... (18%)
stream5: Reset outside window... (27%)
http_inspect: LONG HEADER... (26%)
Highcharts v2.1 Beta

103 HIGH SEVERITY 103 / 548

5 MEDIUM SEVERITY 5 / 548

440 LOW SEVERITY 440 / 548

TOP 5 SENSOR	
digithreat	136363

TOP 5 ACTIVE USERS	
Administrator	0

LAST 5 UNIQUE EVENTS	
ICMP PING	0
ET WEB_SERVER Possible...	0
ET RBN Known Russian B...	0
ATTACK-RESPONSES 403 F...	0
ICMP Time-To-Live Exce...	0

ANALYST CLASSIFIED EVENTS	
False Positive	42
Unauthorized Root Access	0
Unauthorized User Access	0
Attempted Unauthorized...	0
Denial of Service Attack	0
Policy Violation	0
Reconnaissance	0
Virus Infection	0

Which one triggers more alarms?

- Statistical anomaly-based

IDS Modes

Passive

- Analyze and report the information/problem (i.e., generate alarms) that it has collected
- Does not interfere with the traffic itself
- Wait for administrator’s actions

Active

- Automatically initiate responses when alerts are triggered
- e.g., collect and archive additional information, modify the environment, take action against the intruders, etc.

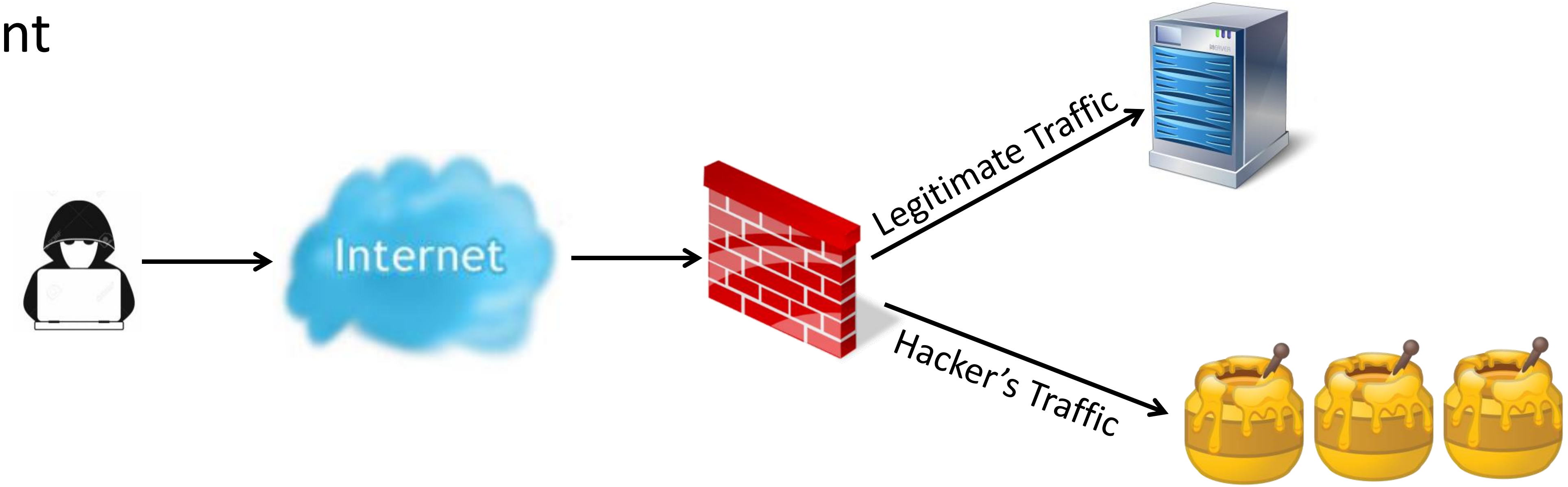
About IDPS…

- What if the traffic is encrypted? – greatly affects the IDPS’s ability to identify malware
- What if there is heavy network traffic? – IDPS can cause network congestion and negatively impact the network’s performance

Solution Name	Features	Pricing	Toolbox Comments
AirMagnet Enterprise	Its AirWISE engine analyzes wireless network activity using frame inspection, stateful pattern analysis, statistical modeling, radio-frequency analysis, and anomaly detection.	Pricing for the solution is approximately $10,325.	AirMagnet is a reliable tool for compliance purposes, but it may not be as sophisticated as solutions with AI and advanced automation.
Amazon Web Services (AWS) GuardDuty	It is built using ML, which means it adapts to your enterprise environment and becomes incrementally more effective with time.	Pricing starts at $0.80 per one million events or $1.00 per GB (region-specific).	GuardDuty is easy to deploy and has a one-click deployment process. However, it supports very little customization and does not allow users to maintain their own rules.
Azure Firewall Premium IDPS	It is constantly updated, with 20-40 new intrusion detection rules released every day.	Pricing starts at $1.75 per deployment hour and $0.016 per GB processed.	Microsoft offers scalable and easy-to-configure IDPS. However, it protects only Azure-based networks and requires cloud expertise.
Blumira	It claims to be 5X faster than the industry average, aided by intrusion evidence stacking, automatic prioritization, and correlation.	Pricing for Blumira is undisclosed.	Blumira is a compliant and comprehensive IDPS solution. However, the dashboards aren't configurable and can generate only CSV reports without any visualizations.
Cisco Secure IPS (NGIPS)	It offers flexible deployment at the enterprise perimeter, in your data center, or behind a firewall.	Pricing starts at $35,000.	Cisco Secure IPS is ideal for large enterprises. However, the documentation is insufficient, and fine-tuning the policies can be time-consuming.
Darktrace Enterprise Immune System	Darktrace is powered by cutting-edge AI technology that self-learns and acts autonomously.	Pricing will depend on the deployment environment – e.g., it costs $30,000 annually on AWS.	Darktrace detects abnormal activities even if they are imperceptible. However, it may result in false positives and slow down systems.
IBM Intrusion Detection and Prevention System (IDPS) Management	IBM can protect highly complex IT environments by incorporating human expertise and threat intelligence services.	Pricing for IBM IDPS Management is undisclosed.	The tool is a good fit for companies with heterogeneous environments. However, it does not come with pre-built configurations and rules.
Meraki MX Advanced Security Edition	It is designed for SD-WAN environments, uses ML, and can be deployed in just three clicks.	Pricing for the software license starts at approximately $4,600.	SD-WAN users can consider Meraki, but the tool may not be flexible enough for complex environments. Also, users have noted that the quality of support has deteriorated in recent years.
NSFocus Next-Generation Intrusion Prevention System	It uses multi-stage AI analysis to visualize the attack chain accurately.	Pricing for this solution is undisclosed.	The tool's multiple detection engines drive reliable and comprehensive coverage. However, the documentation is insufficient, and customers have reported the absence of SSL protection.

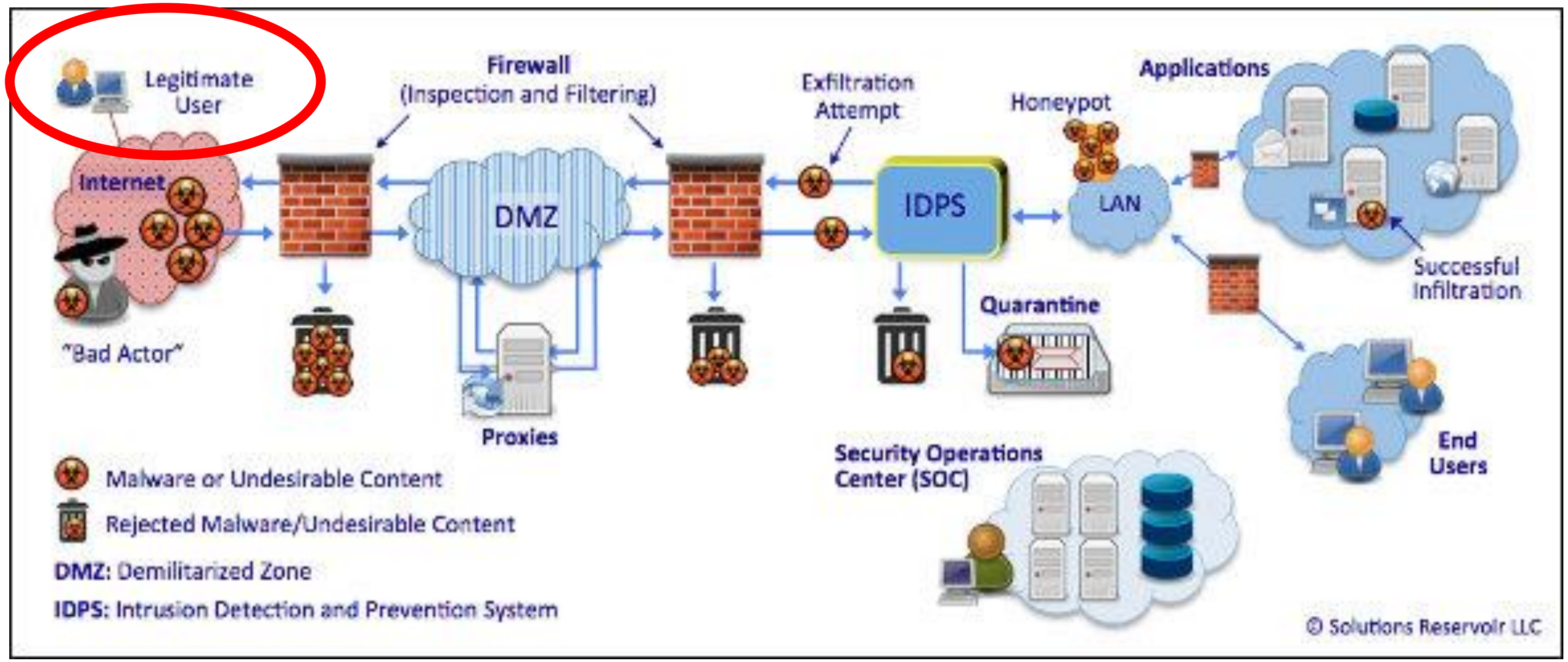
4. Honeypots and Honeynets

- Honeypots: decoy systems designed to lure potential attackers away from critical systems
- Honeynets: several honeypots connected together on a network segment



Honeypots and Honeynets

- Honeypots are designed to:
  - Divert an attacker from accessing critical systems
  - Collect information about the attacker’s activity
  - Encourage the attacker to stay on a system long enough for administrators to document the event and perhaps respond
- Potential issues:
  - Legal implications unclear
  - Attackers may get angrier and launch more serious attacks
  - High level of expertise required for admin


Legitimate User
Firewall (Inspection and Filtering)
Exfiltration Attempt
Honeypot
Applications
Internet
DMZ
IDPS
LAN
"Bad Actor"
Successful Infiltration
Quarantine
Proxies
Security Operations Center (SOC)
End Users
Malware or Undesirable Content
Rejected Malware/Undesirable Content
DMZ: Demilitarized Zone
IDPS: Intrusion Detection and Prevention System
© Solutions Reservoir LLC

WORK
AT HOME

5. Virtual Private Network (VPN)

- Extends an organization’s internal network to remote locations
- Provide private and secure network connection between systems
- VPN must accomplish (CIA):
  - Confidentiality: the carrier network will route the data, but unable to decrypt it (through encryption).
  - Integrity: messages transported across the network cannot be changed easily while they are in transport (through encapsulation).
  - Authentication: users from both ends need to authenticate themselves, to be able to use the network (through passwords, keys, digital signatures, etc.).

Virtual Private Network (VPN)

- Tunnel mode
  - Establishes two perimeter tunnel servers to encrypt all traffic that will traverse an unsecured network
  - Entire client package encrypted and added as data portion of a packet from one tunneling server to another

Tunnel Mode VPN

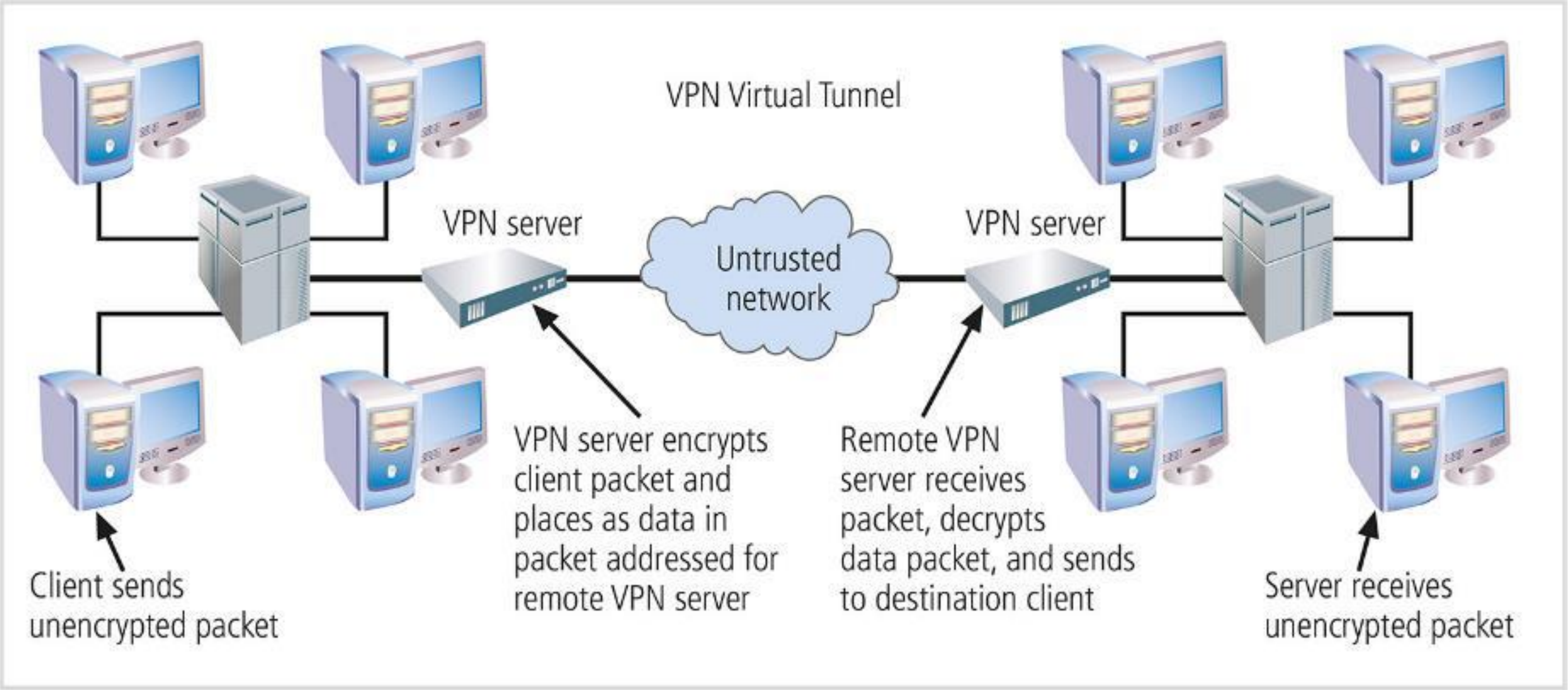
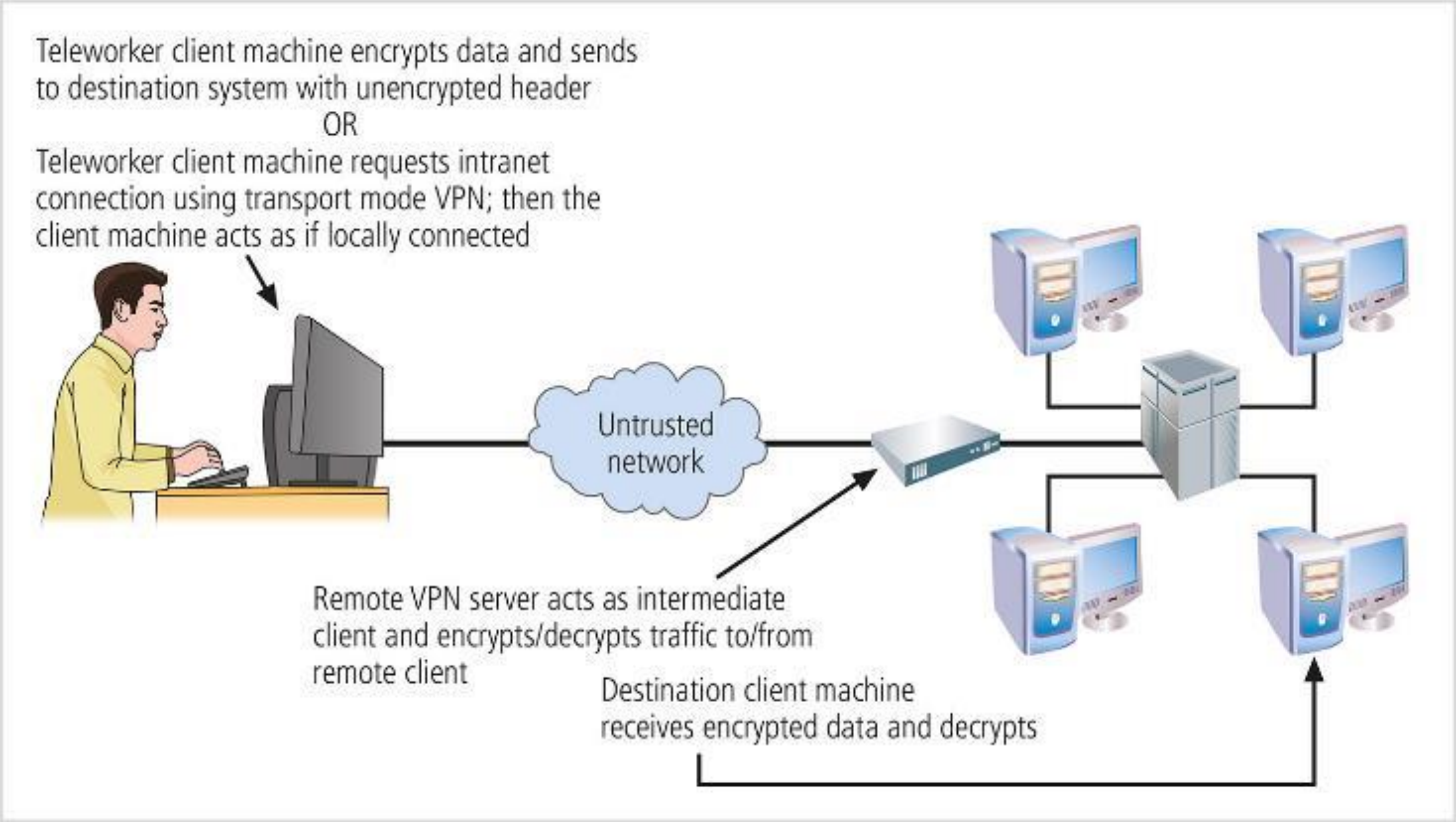

VPN Virtual Tunnel
VPN server
Untrusted network
VPN server
VPN server encrypts client packet and places as data in packet addressed for remote VPN server
Remote VPN server receives packet, decrypts data packet, and sends to destination client
Client sends unencrypted packet
Server receives unencrypted packet

Figure 8-20 Tunnel mode VPN

Virtual Private Network (VPN)

- Transport mode
  - Data within IP packet are encrypted, but header information is not
  - Allows user to establish secure link directly with remote host, encrypting only data contents of packet
  - Two popular uses:
    - End-to-end transport of encrypted data
    - Remote access worker connects to an office network over Internet by connecting to a VPN server on the perimeter

Transport Mode VPN



Teleworker client machine encrypts data and sends to destination system with unencrypted header

OR

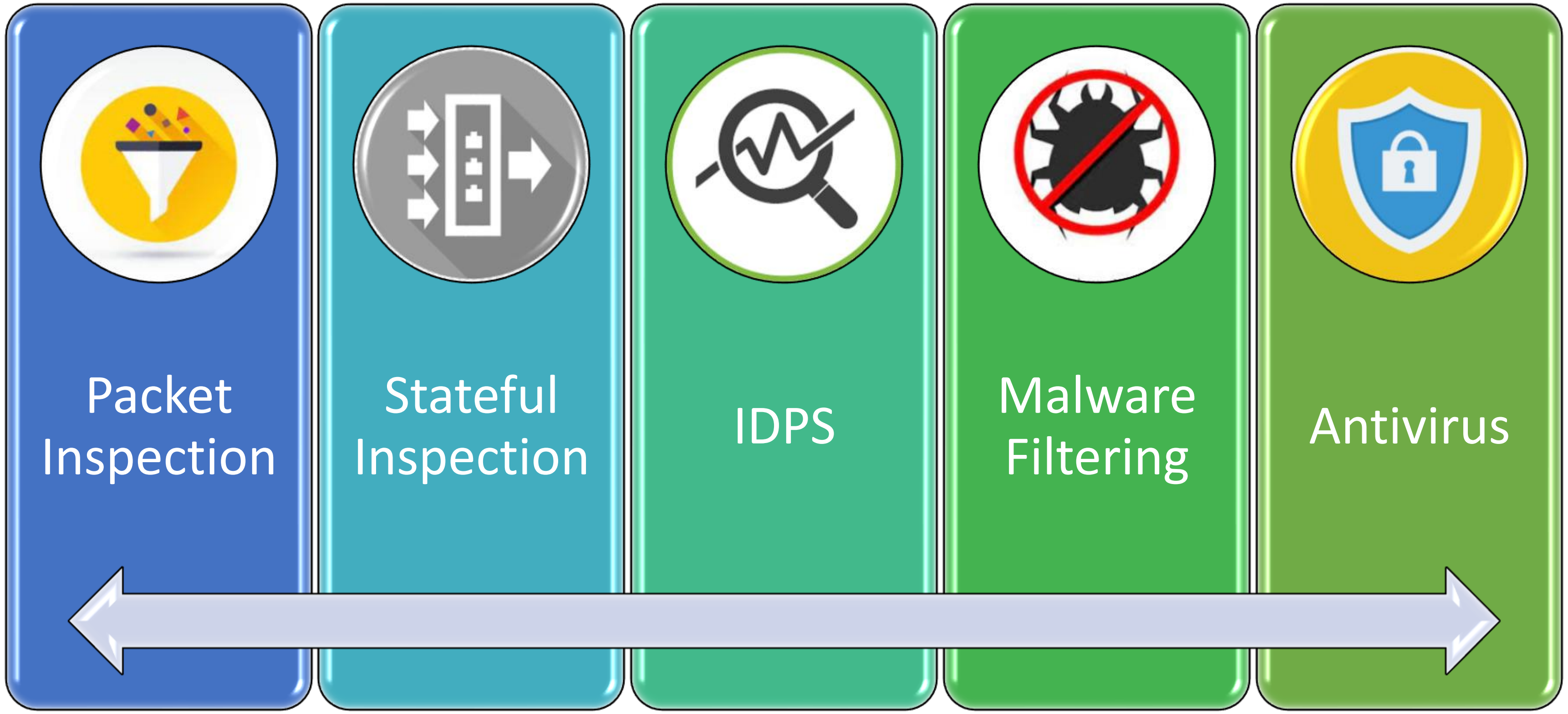
Teleworker client machine requests intranet connection using transport mode VPN; then the client machine acts as if locally connected

Remote VPN server acts as intermediate client and encrypts/decrypts traffic to/from remote client

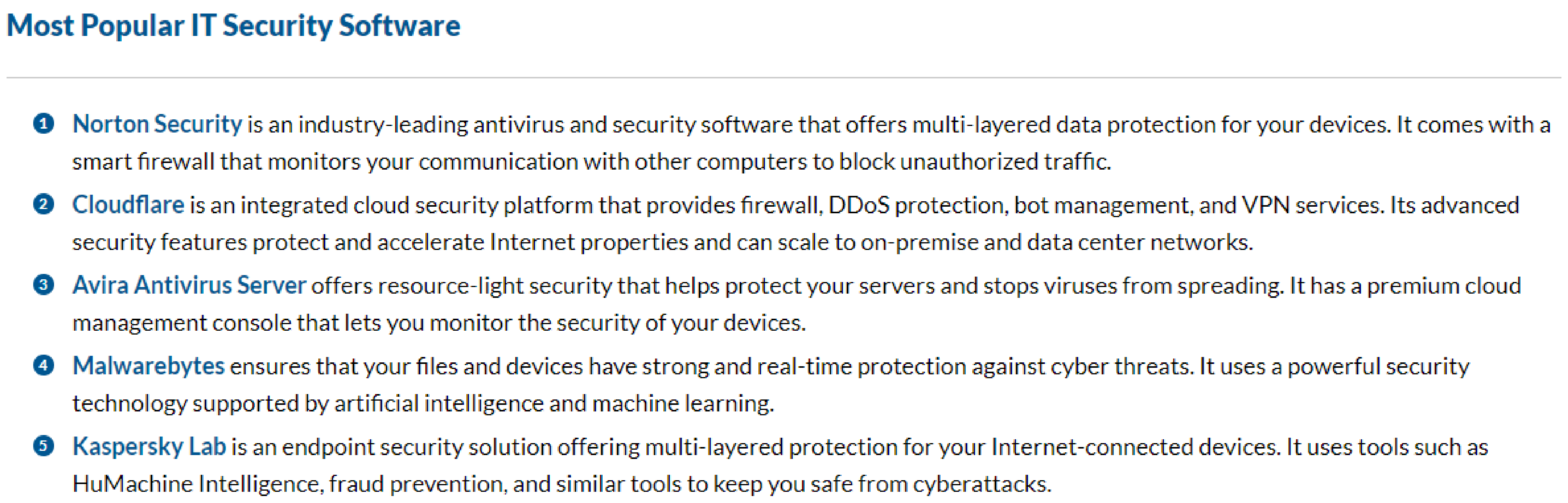
Destination client machine receives encrypted data and decrypts

Figure 8-19 Transport mode VPN

Next Generation Firewall



Popular IT Security Software



Most Popular IT Security Software

1. Norton Security is an industry-leading antivirus and security software that offers multi-layered data protection for your devices. It comes with a smart firewall that monitors your communication with other computers to block unauthorized traffic.
2. Cloudflare is an integrated cloud security platform that provides firewall, DDoS protection, bot management, and VPN services. Its advanced security features protect and accelerate Internet properties and can scale to on-premise and data center networks.
3. Avira Antivirus Server offers resource-light security that helps protect your servers and stops viruses from spreading. It has a premium cloud management console that lets you monitor the security of your devices.
4. Malwarebytes ensures that your files and devices have strong and real-time protection against cyber threats. It uses a powerful security technology supported by artificial intelligence and machine learning.
5. Kaspersky Lab is an endpoint security solution offering multi-layered protection for your Internet-connected devices. It uses tools such as HuMachine Intelligence, fraud prevention, and similar tools to keep you safe from cyberattacks.

Source: https://financesonline.com/cybersecurity-statistics/