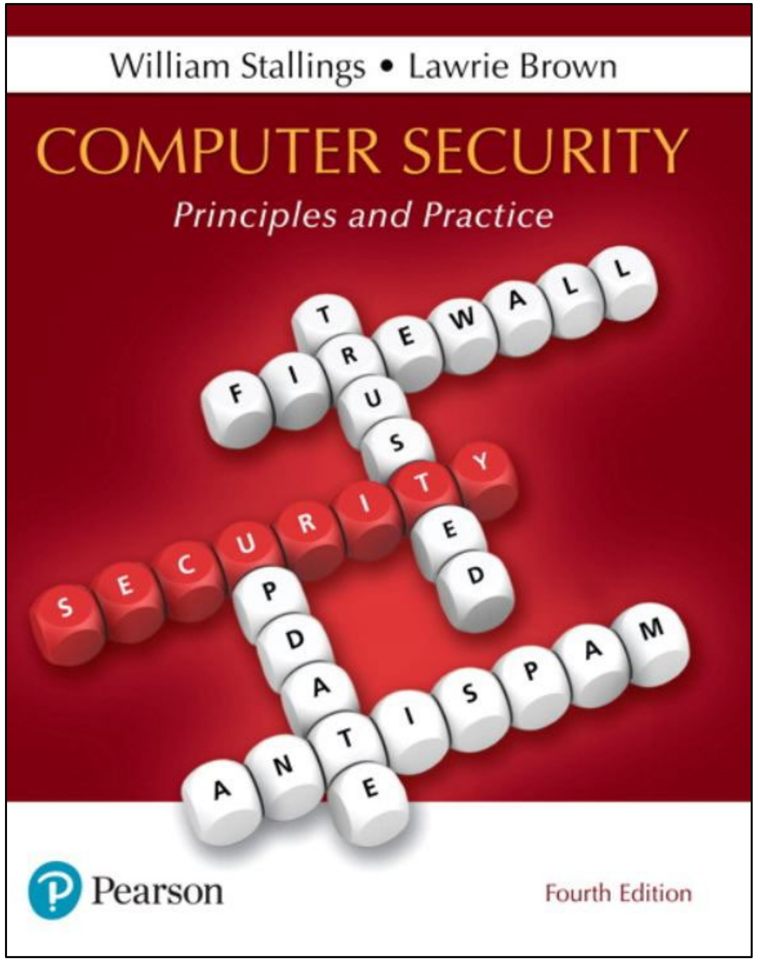
Firewalls

CalPolyPomona

Computer Security: Principles and Practice



- **Chapter 9**

- Firewalls and Intrusion Prevention Systems

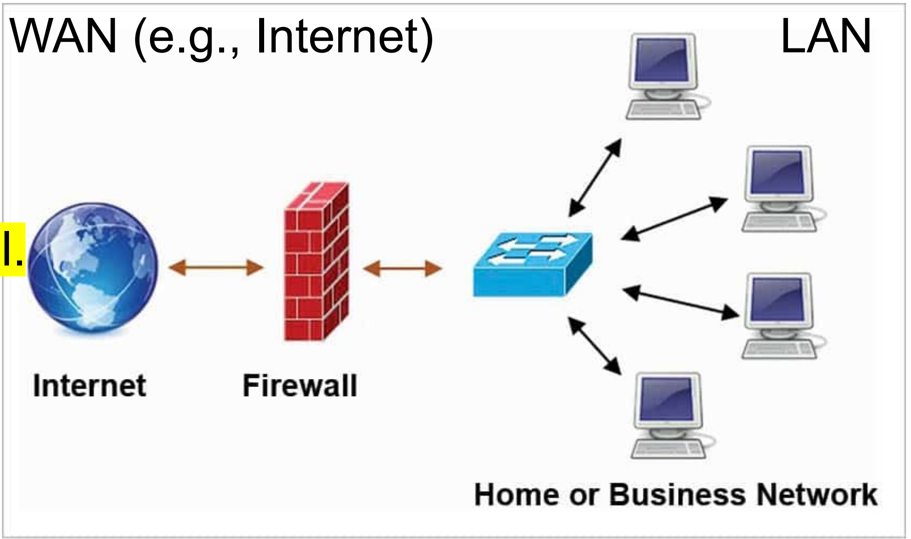
The Need For Firewalls

- Firewalls are a category of systems that protect computers from attacks that come from the network
- They are extremely critical if computers are connected to the Internet since machines are reachable from anywhere
- The initial model of a firewall was a device able to protect a LAN
- Inserted between the premises network and the Internet to establish a controlled link
  - Can be a single computer system or a set of two or more systems working together
- Used as a perimeter defense
  - Single choke point to impose security and auditing
  - Insulates the internal systems from external networks

OBSERVATION: The initial model of dividing the world in external is untrusted Vs. internal is trusted, is no longer a reliable assumption.
Shadow IT, Insiders and BYOD are examples that threaten the model.
Firewalls are still an important solution, but not enough anymore, since the **attack surface is not physically delimited by the border of a LAN.**

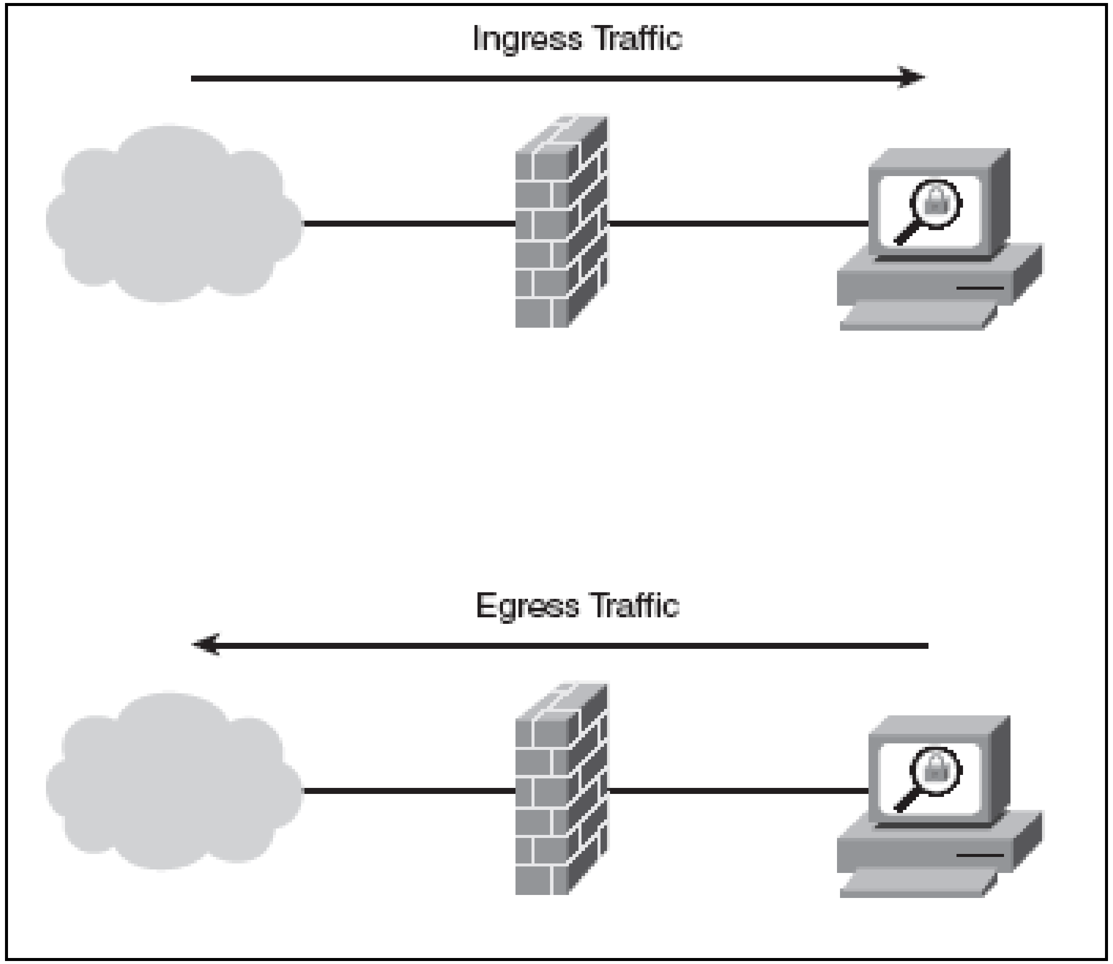
“untrusted”
WAN (e.g., Internet)

“trusted”
LAN



Firewall Characteristics

- **Design goals**
  - All traffic from inside to outside (egress traffic), and vice versa (ingress traffic), must pass through the firewall
  - Only authorized traffic as defined by the local security policy will be allowed to pass
  - The firewall itself is immune to penetration



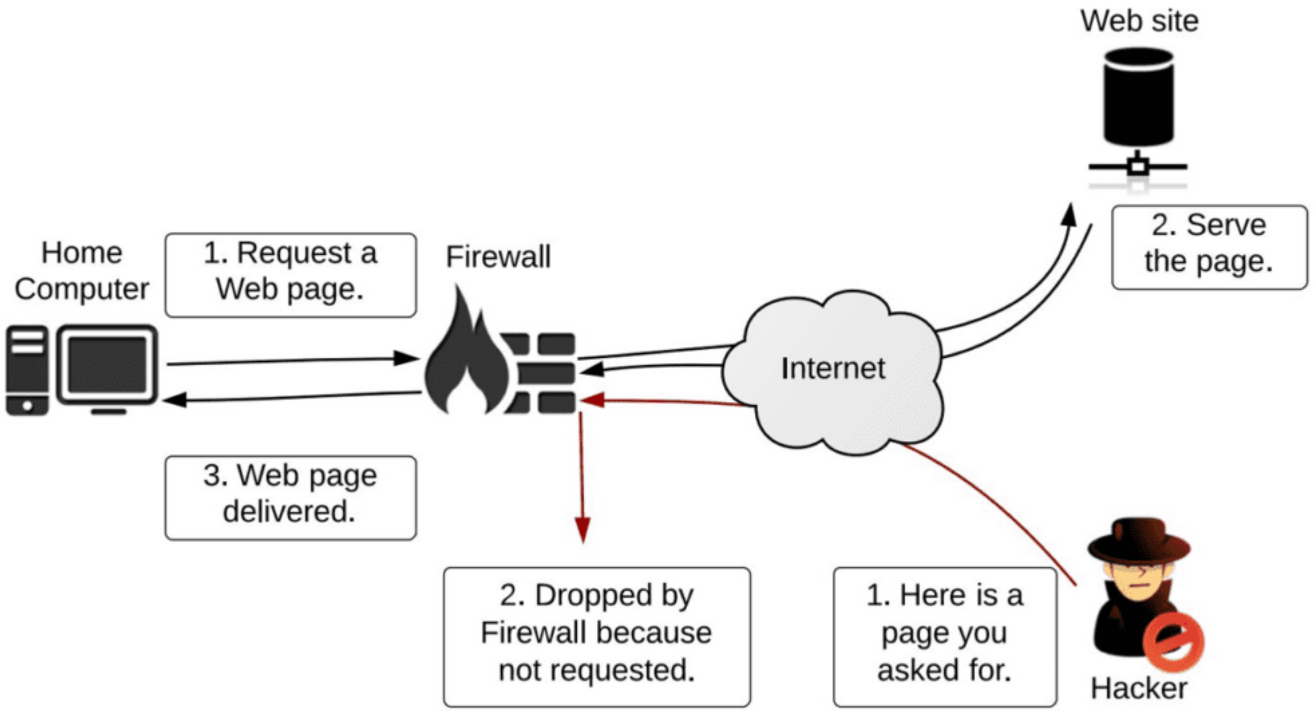
Why do we need a firewall?

- Ingress filtering – controlling traffic into a network
  - Can help to prevent some attacks:
    - DDoS traffic from spoofed IPs
    - Some weird combinations of packet fields
    - Direct access to services from outside
- Egress filtering – controlling of traffic leaving from a network
  - Can help to prevent some attacks, for example:
    - Spoofing from inside the network
    - Some exfiltration attacks

- Note: firewalls are a small but important tool to orchestrate defense from attacks.
  In general, more techniques have to be combined to stop some of these attacks

Firewall Access Policy/List (ACL)

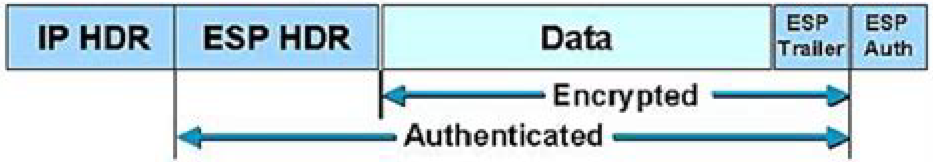
- Security admins need to establish the access policy for ingress/egress traffic
  - This lists the types of traffic authorized to pass through the firewall
  - Includes address ranges, protocols, applications and content types



General mechanisms to define access policies of traffic in a firewall

- Network/Transmission-level filtering: IP address and protocol values
  - This type of filtering is used by packet filter and stateful inspection firewalls
  - Typically used to limit access to specific services
- Application-level filtering: Application protocol
  - This type of filtering is used by an application-level gateway that relays and monitors the exchange of information for specific application protocols
- User identity
  - Typically for inside users who identify themselves using some form of secure authentication technology
  - Example, IPSec, a protocol which allows authentication of IP packets and it's used to create VPNs

ESP is the header in IPSec protocol

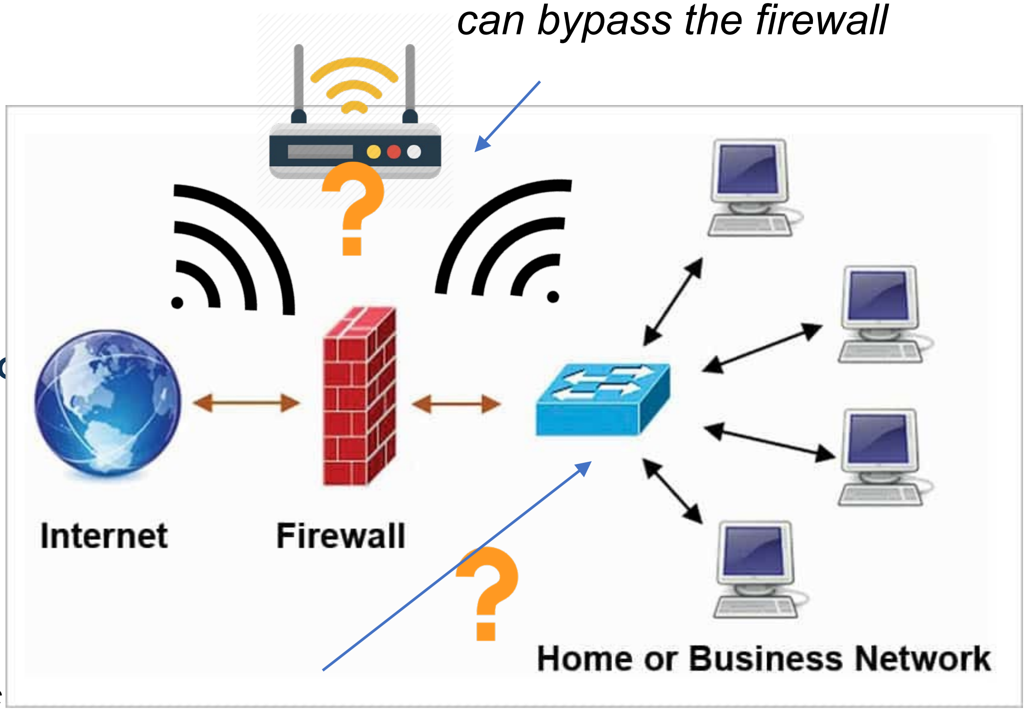


- Network activity
  - Controls access based on considerations such as the time or request, rate of requests, or other activity patterns

Firewall Capabilities and Limits

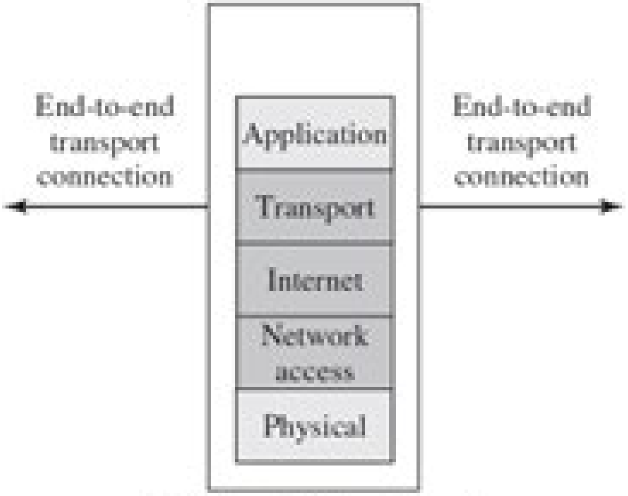
- **Capabilities:**
  - Defines a single choke point
  - Provides a location for monitoring security events (however, only events in the firewall location)
  - Convenient platform for several Internet functions that are not security related (NAT: network address translation or PAT: port address translation)
  - Can serve as the platform for IPSec (network layer VPN)
- **Limitations:**
  - Cannot protect against attacks bypassing firewall with physical signal sent out from a different path
  - May not protect fully against internal threats
  - Improperly secured wireless LAN can be accessed from outside the organization
  - Laptop, PDA, or portable storage device may be infected outside the corporate network then used internally
  - Cannot protect from attacks that are not visible in communications, e.g., against vulnerabilities in software

Wifi traffic or unsecured wifi *can bypass the firewall*



Internal traffic *(i.e., generated and received within the network) is not protected by the firewall*

Packet filter firewall


End-to-end transport connection
Application
Transport
Internet
Network access
Physical
End-to-end transport connection

(b) Packet filtering firewall

- Applies rules to each incoming and outgoing IP packet
  - Typically, a list of rules based on matches in the IP or TCP header
  - Forwards or discards the packet based on rules match

- Filtering rules are based on information contained in a network packet
  - **Source IP address:** e.g., specific 10.1.0.122, or network 10.1.0.0/24
  - **Destination IP address: :** e.g., specific 10.1.0.122, or network 10.1.0.0/24
  - **Source and destination transport-level port**: e.g., port 25, 53
  - **Transport protocol field:** e.g., TCP, UDP, ARP, ICMP
  - **Interface:** e.g., eth0, eth2, whatever is used in the firewall

- Two default policies:
  - **Discard** - prohibit unless expressly permitted
    - More conservative, controlled, visible to users
  - **Forward** - permit unless expressly prohibited
    - Easier to manage and use but less secure

Packet-Filtering: Example rules

Rule	Direction	Src address	Dest addresss	Protocol	Dest port	Action
1	In	External	Internal	TCP	25	Permit
2	Out	Internal	External	TCP	>1023	Permit
3	Out	Internal	External	TCP	25	Permit
4	In	External	Internal	TCP	>1023	Permit
5	Either	Any	Any	Any	Any	Deny

Access to the internal email server from out (SMTP port 25)

Reply to the request from out

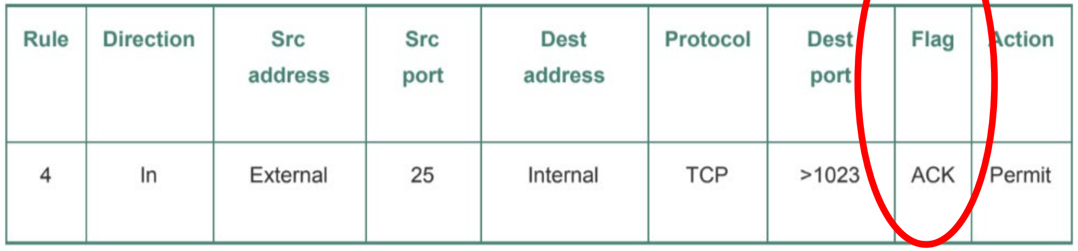
Access to the external email server from in (SMTP port 25)

Reply to the request from in

Deny anything else

Problem 1: Rule 4, what if the attacker sends a send a TCP message to an open port in the internal network (E.g., 8080, a web server for internal use) ?
There is no way to stop it from going in.
Fix 1 (not great though): rather than just saying >1023, you can specify source ports in the rule, hence limiting which ports are used.

Problem 2: Rule 3 and 4 consider that the external server SMTP is listening on port 25. What if that port is used for malicious purposes in an external machine? E.g., the malicious host might declare to use source port 25, hence waiting for the replies on that port.

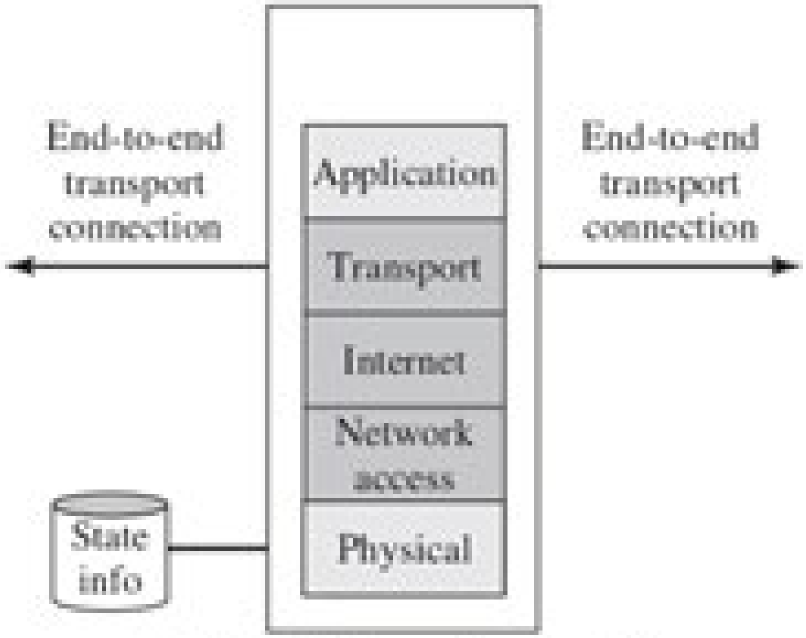


Rule	Direction	Src address	Src port	Dest address	Protocol	Dest port	Flag	Action
4	In	External	25	Internal	TCP	>1023	ACK	Permit

Packet Filter Advantages And Weaknesses

- Advantages
  - Simplicity: simple mechanisms
  - Typically, transparent to users and are very fast
- Weaknesses
  - Cannot prevent attacks that employ application specific vulnerabilities or functions: the payload at application level might target a vulnerability in an internal server, but will never be caught by the firewall
  - Limited logging functionality: only information available is related to the rules matched by a packet
  - Do not support advanced user authentication: if a packet passes the filter, there is no way to check where it comes from
  - Vulnerable to attacks on TCP/IP protocol bugs: if the attack is not targeting an anomaly in the protocol, rather in the implementation (e.g., IP spoofing with external spoofed address), no way to catch it.
  - Improper configuration can lead to breaches: easily can lead to error during the configuration

Stateful packet firewall


End-to-end transport connection
Application
Transport
Internet
Network access
Physical
End-to-end transport connection
State info

(c) Stateful inspection firewall

- Tightens rules for TCP traffic by creating a directory of outbound TCP connections
  - There is an entry for each currently established connection
  - Packet filter allows incoming traffic to high numbered ports only for those packets that fit the profile of one of the entries in this directory
- Reviews packet information but also records information about TCP connections
  - Keeps track of TCP sequence numbers to prevent attacks that depend on the sequence number
  - Inspects data for protocols like FTP, IM and SIPS commands

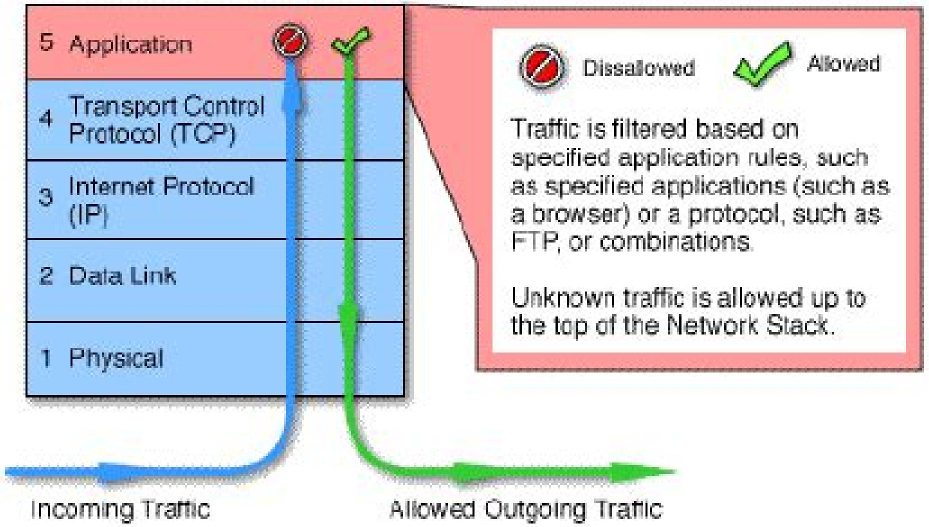
Example Stateful Firewall Connection State Table

Records IP addresses and status of connection
to allow packets to pass.
Any packets in the step can bypass the network

Source Address	Source Port	Destination Address	Destination Port	Connection State
192.168.1.100	1030	210.9.88.29	80	Established
192.168.1.102	1031	216.32.42.123	80	Established
192.168.1.101	1033	173.66.32.122	25	Established
192.168.1.106	1035	177.231.32.12	79	Established
223.43.21.231	1990	192.168.1.6	80	Established
219.22.123.32	2112	192.168.1.6	80	Established
210.99.212.18	3321	192.168.1.6	80	Established
24.102.32.23	1025	192.168.1.6	80	Established
223.21.22.12	1046	192.168.1.6	80	Established

Application-Level Gateway

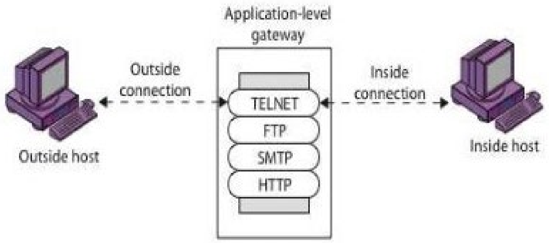
- Also called an **application proxy**
- Acts as a relay of application-level traffic
  - User contacts gateway using a TCP/IP application
  - User is authenticated
  - Gateway contacts application on remote host and rela TCP segments between server and user
- Advantages:
  - Filter application specific commands, e.g., http post/get with specific parameters etc.
  - Inspect the entire packet
  - Tend to be more secure than packet filters
- Disadvantages:
  - additional processing overhead on each connection
  - Vendors must update for new protocols and updates of protocols



Traffic is filtered based on specified application rules, such as specified applications (such as a browser) or a protocol, such as FTP, or combinations.

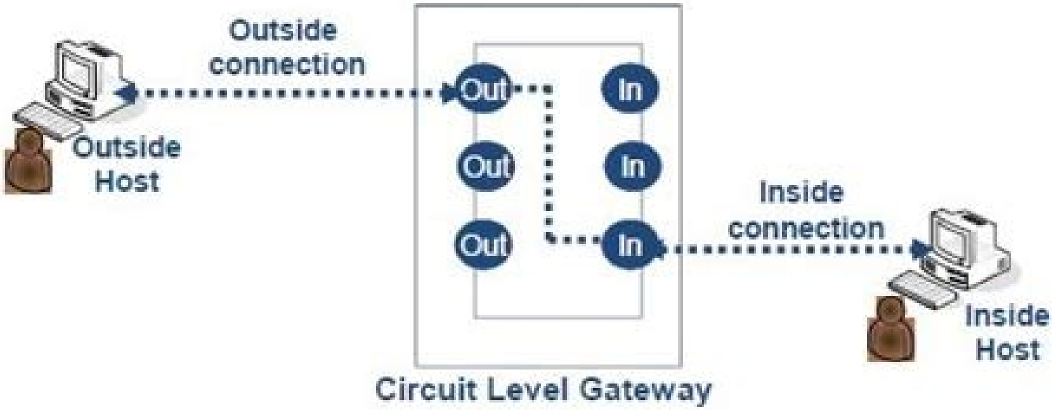
Unknown traffic is allowed up to the top of the Network Stack.

Application level gateway

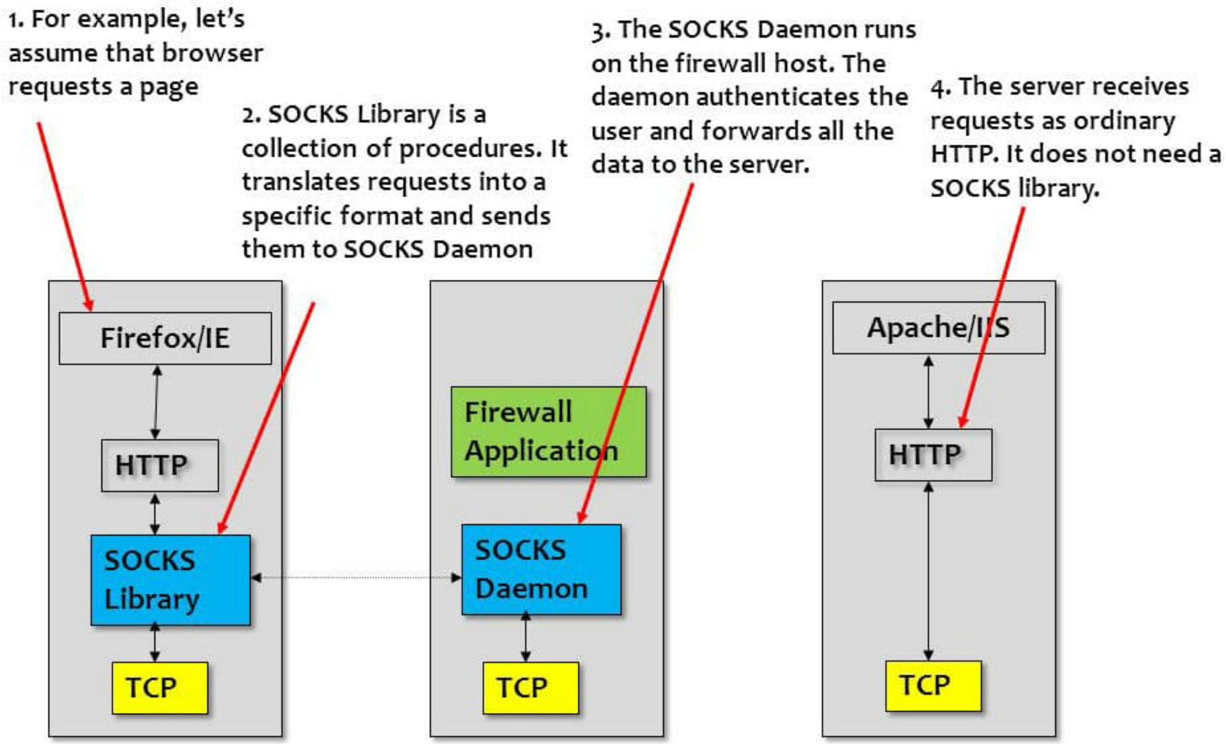


(b) Application-level gateway

Circuit-Level Gateway



- **Circuit level proxy**
  - Sets up **two TCP connections:**
    - one between itself and a TCP user on an inner host
    - one on an outside host
  - **Relays TCP segments** from one connection to the other **without examining contents**
  - Security function consists of determining which connections will be allowed
- **Typically used when inside users are trusted**
  - May use application-level gateway inbound and circuit-level gateway outbound
  - Lower overheads



1. For example, let's assume that browser requests a page

2. SOCKS Library is a collection of procedures. It translates requests into a specific format and sends them to SOCKS Daemon

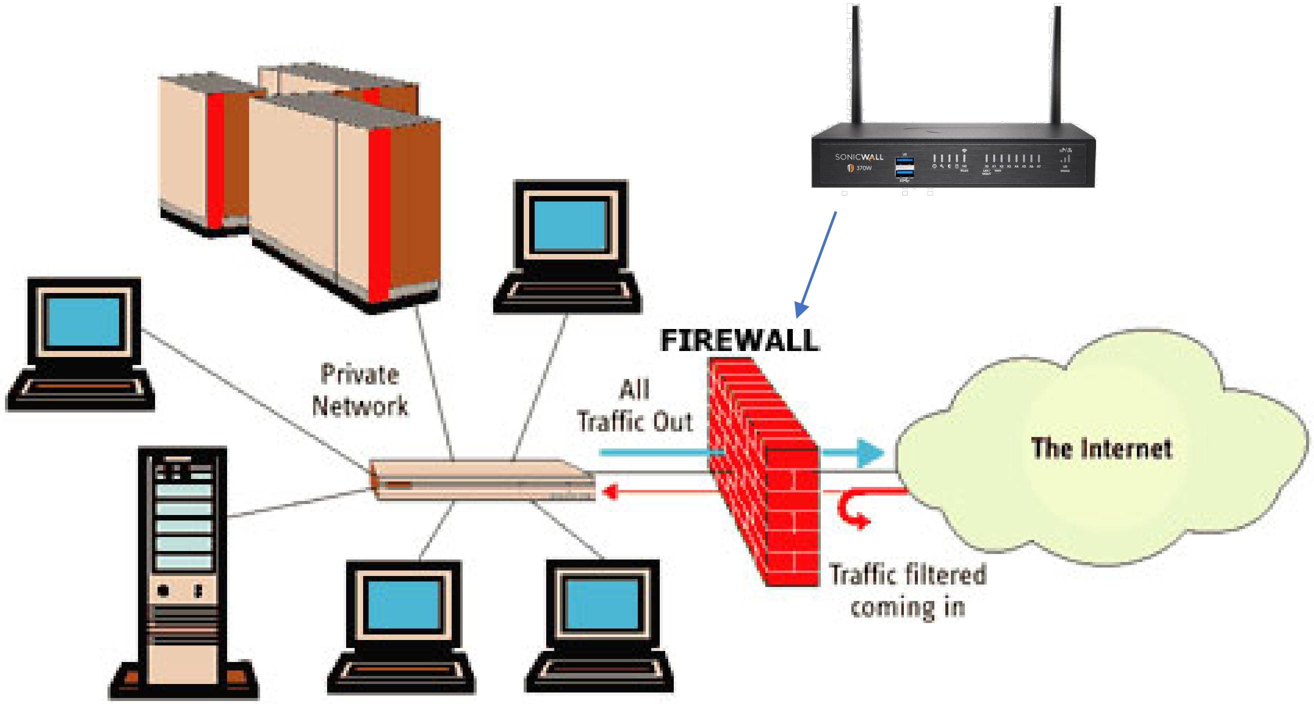
3. The SOCKS Daemon runs on the firewall host. The daemon authenticates the user and forwards all the data to the server.

4. The server receives requests as ordinary HTTP. It does not need a SOCKS library.

Example of Circuit-level Gateway: **SOCKS protocol**

Uses of firewalls

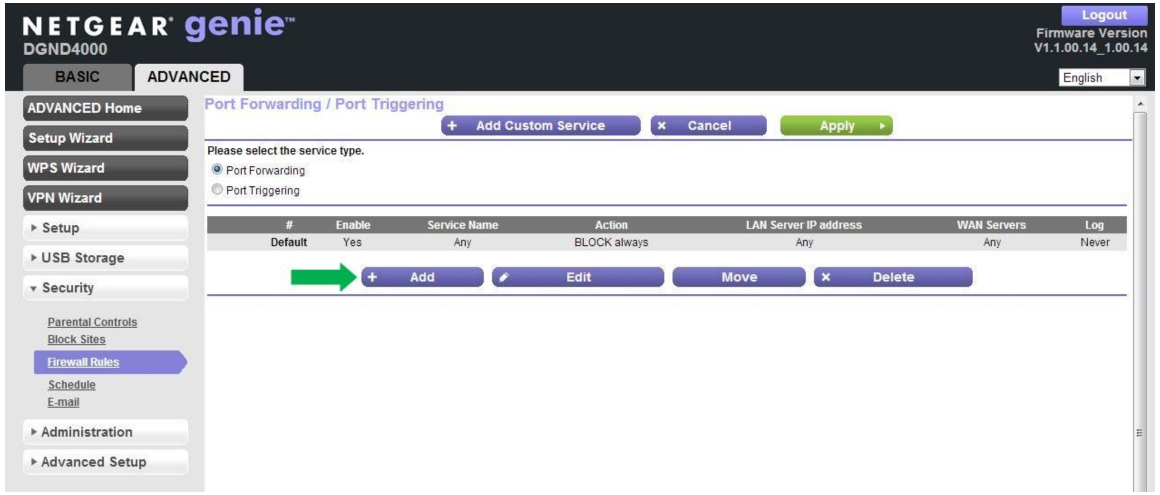
Firewall Case: Network device firewall



**Most often, even home routers have the possibility
to be configured with a network firewall functionality.**

In general, they are devices installed before the home/office router.

If implementing stateless or stateful packet filters are also known as **Screening router.**



Please select the service type.

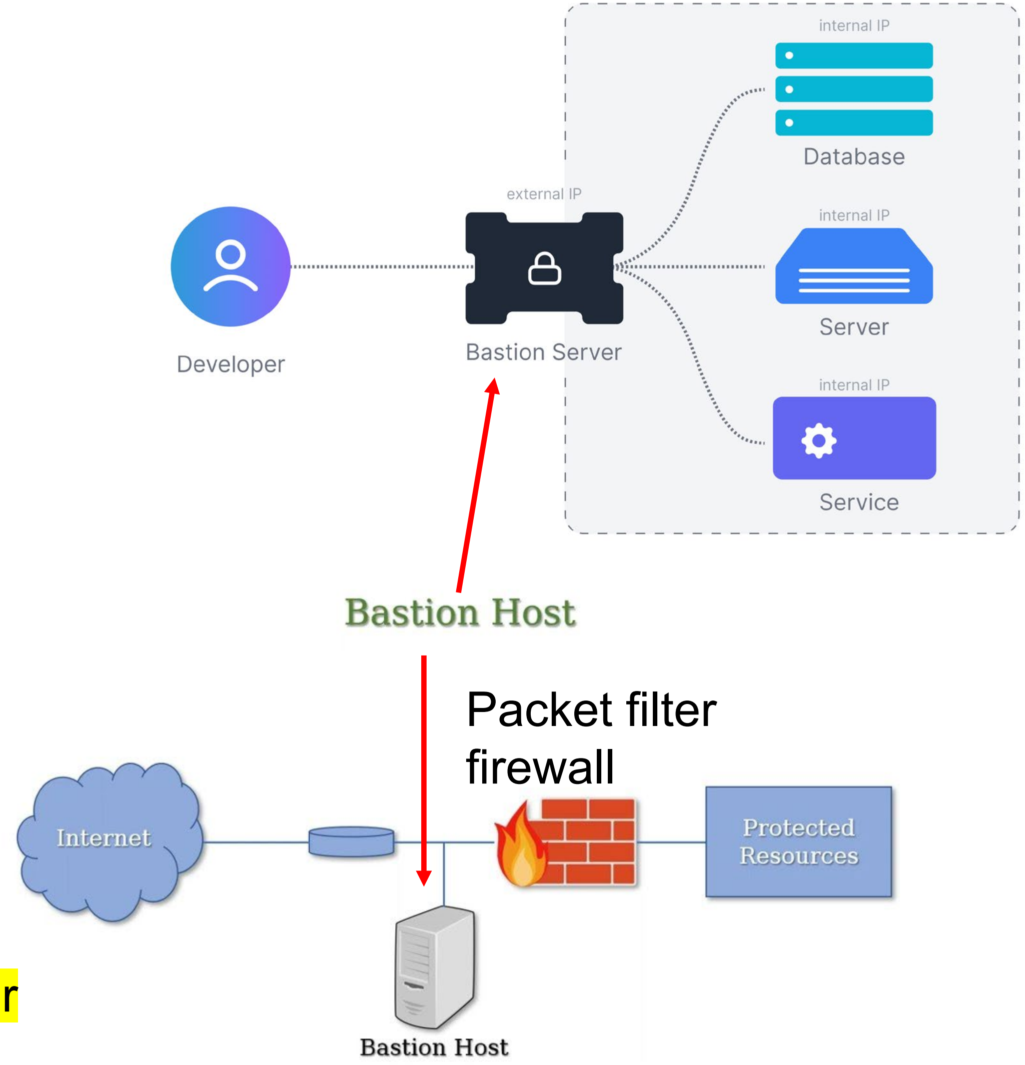
● Port Forwarding

○ Port Triggering

#	Enable	Service Name	Action	LAN Server IP address	WAN Servers	Log
Default	Yes	Any	BLOCK always	Any	Any	Never

Firewall case: Bastion Host + Packet filter

- System identified as a critical strong point in the network's security: It is the most exposed host to the Internet, hence most attacked
- Serves as a platform for an **application-level or circuit-level gateway:**
  - Usually only a very limited set of applications are protected by the Bastion host
- Common characteristics:
  - Runs secure O/S, only essential services
  - May require user authentication to access proxy or host
  - Each proxy can restrict features, hosts accessed
  - Each proxy is small, simple, checked for security
  - Each proxy is independent, non-privileged
  - Limited disk use, hence read-only code



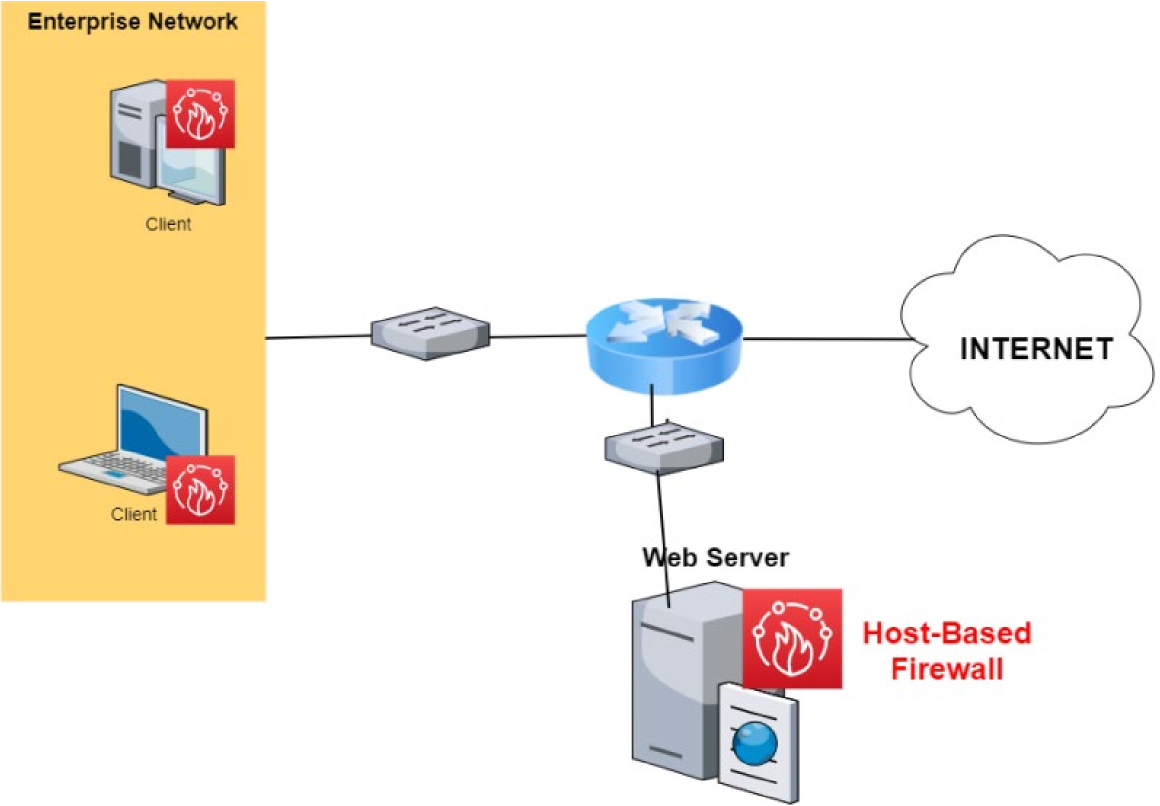
Usually, the bastion host is located in between two firewalls or outside the internal firewall

The Security Buddy
https://www.thesecuritybuddy.com/

Firewall case: Host-Based Firewalls

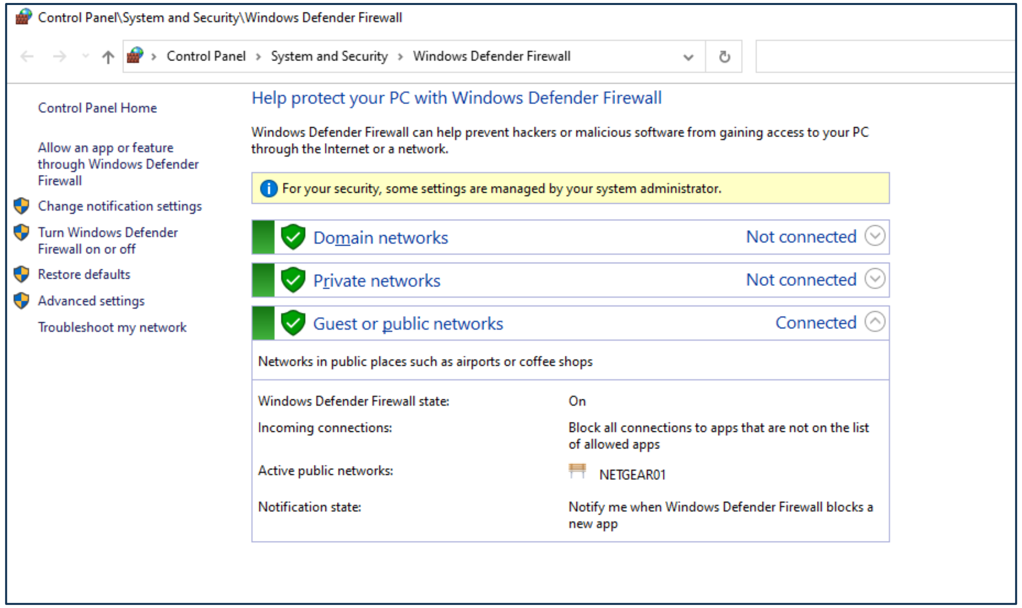
- Used to secure an individual host
- Available in operating systems or can be provided as an add-on package
- Filter and restrict packet flows
- **Common location is a server**

- Advantages:
  - Filtering rules can be tailored to the host environment
  - Protection is provided independent of topology
  - Provides an additional layer of protection



Firewall case: Personal Firewall

- **Similar to Host-based firewall, but related to each Personal computers, not servers**
  - **E.g., your MacOS, Windows laptop or smartphone might have one installed.**
- Controls traffic between a personal computer or workstation and the Internet or enterprise network
- Can be housed in a router that connects all of the home computers to a DSL, cable modem, or other Internet interface
- Typically, much less complex than server-based or stand-alone firewalls
- Primary role is to deny unauthorized remote access
- May also monitor outgoing traffic to detect and block worms and malware activity


Control Panel\System and Security\Windows Defender Firewall
Control Panel › System and Security › Windows Defender Firewall
Control Panel Home
Allow an app or feature through Windows Defender Firewall
Change notification settings
Turn Windows Defender Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network

Help protect your PC with Windows Defender Firewall

Windows Defender Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.

For your security, some settings are managed by your system administrator.

Domain networks — Not connected

Private networks — Not connected

Guest or public networks — Connected

Networks in public places such as airports or coffee shops

Windows Defender Firewall state:	On
Incoming connections:	Block all connections to apps that are not on the list of allowed apps
Active public networks:	NETGEAR01
Notification state:	Notify me when Windows Defender Firewall blocks a new app

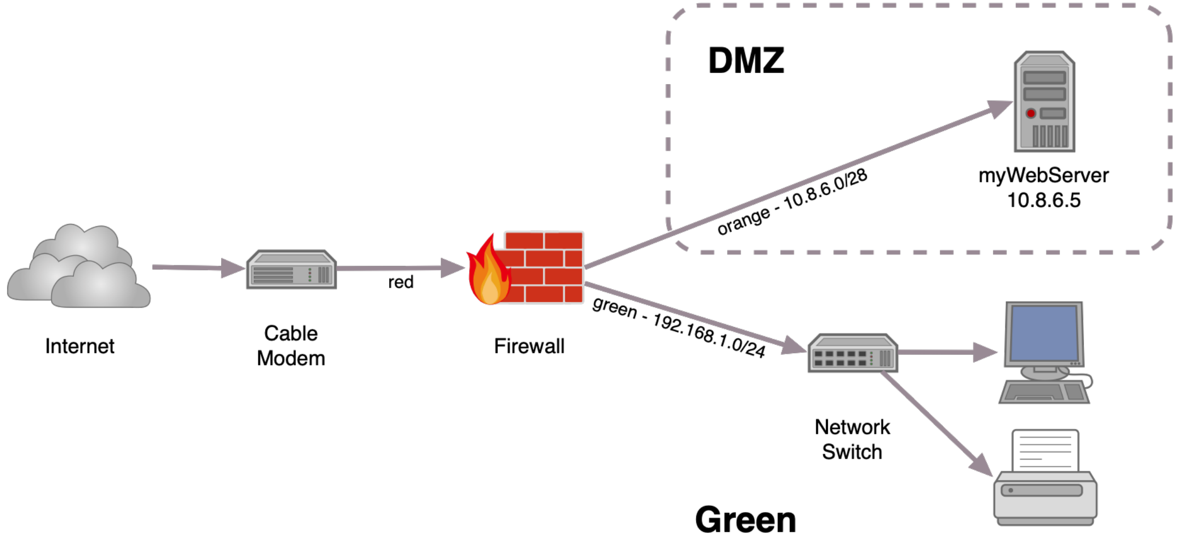
e.g., Windows Firewall

Firewall location and configurations

CalPolyPomona

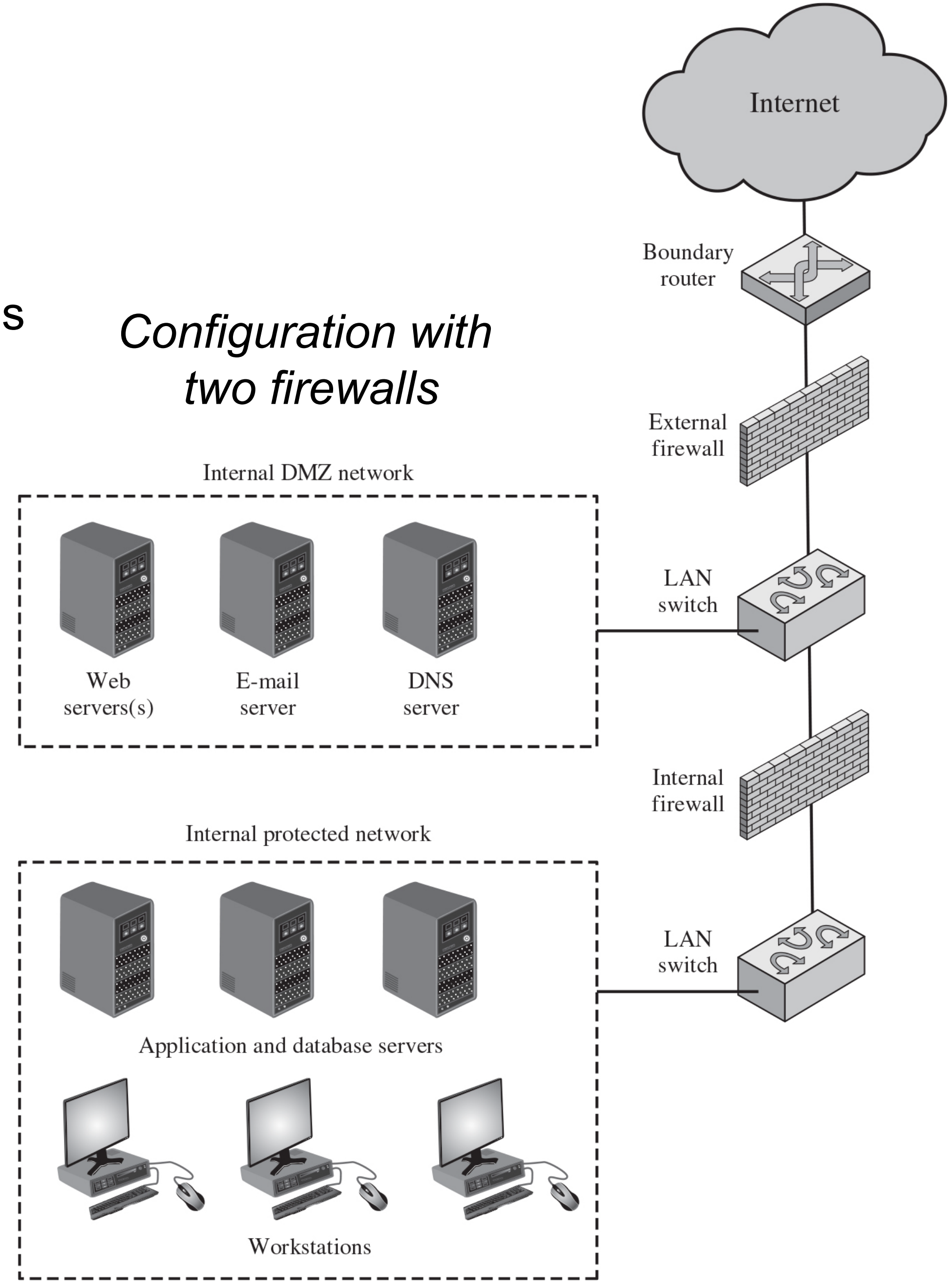
DMZ: Demilitarized Zone

A DMZ is in between internal and external network to expose services accessible from outside (public) and from inside (private) a LAN.
It has a separate network segment wrt
the LAN network and subnetworks.



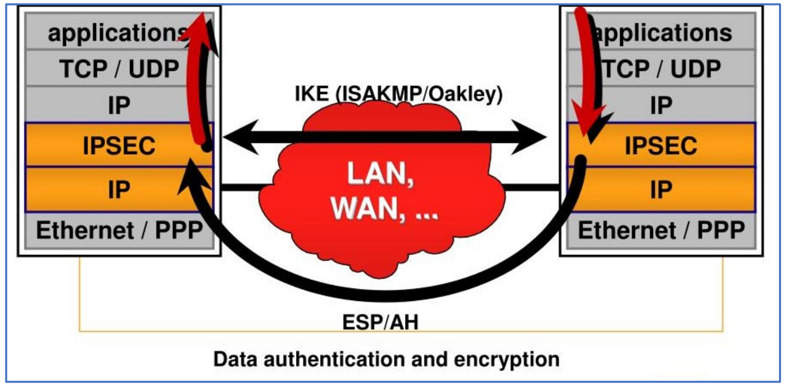
Configuration with single firewall

Configuration with two firewalls



VPN Firewall

Network-level VPN: A Firewall with IPSec is meant to **encapsulate** IP packets that follow an authentication process between two special routers (the IPSec firewalls, indeed).



IPSec is another protocol that will contain an entire IP packet: This is a **"Tunnel"**

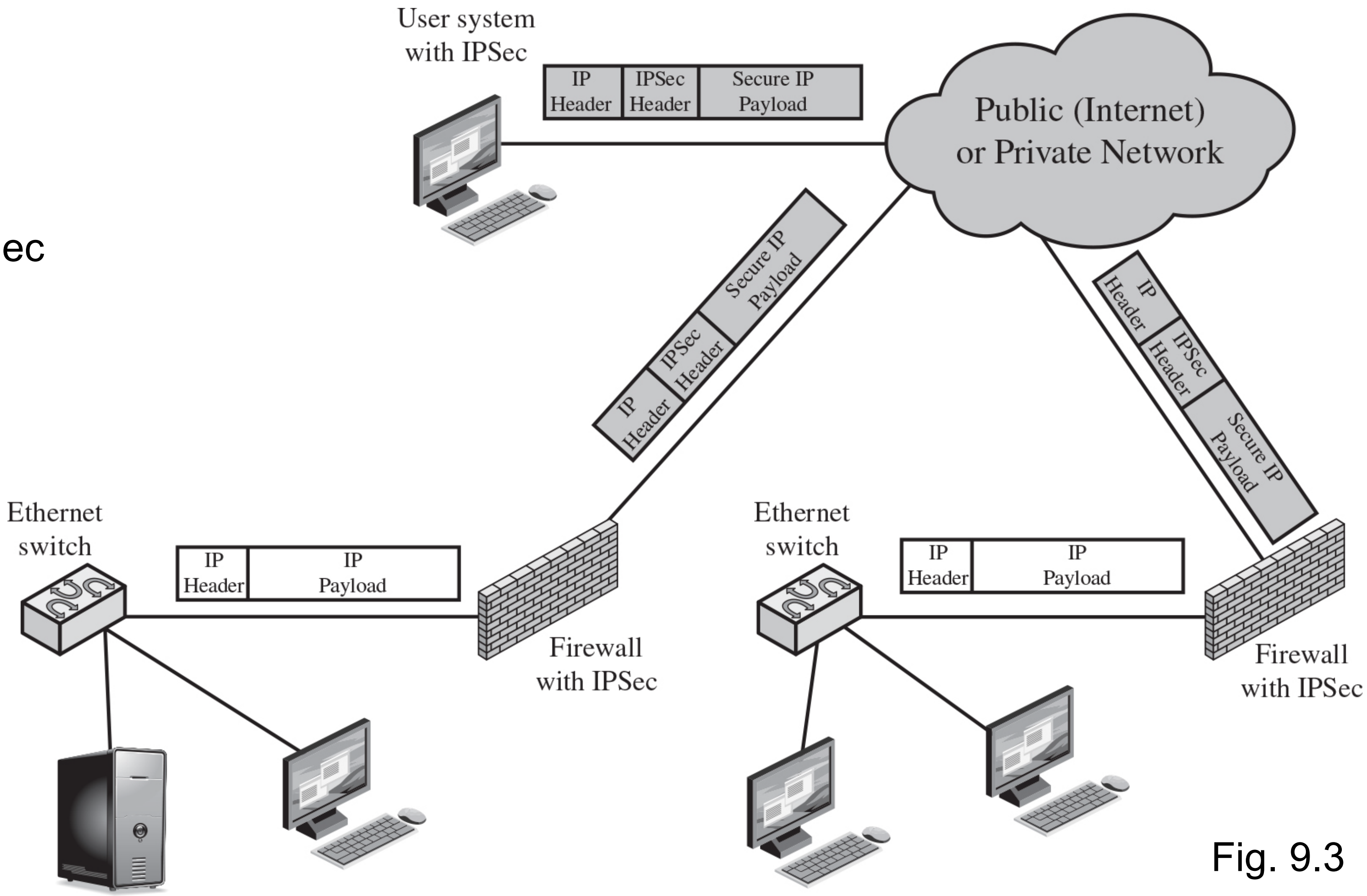
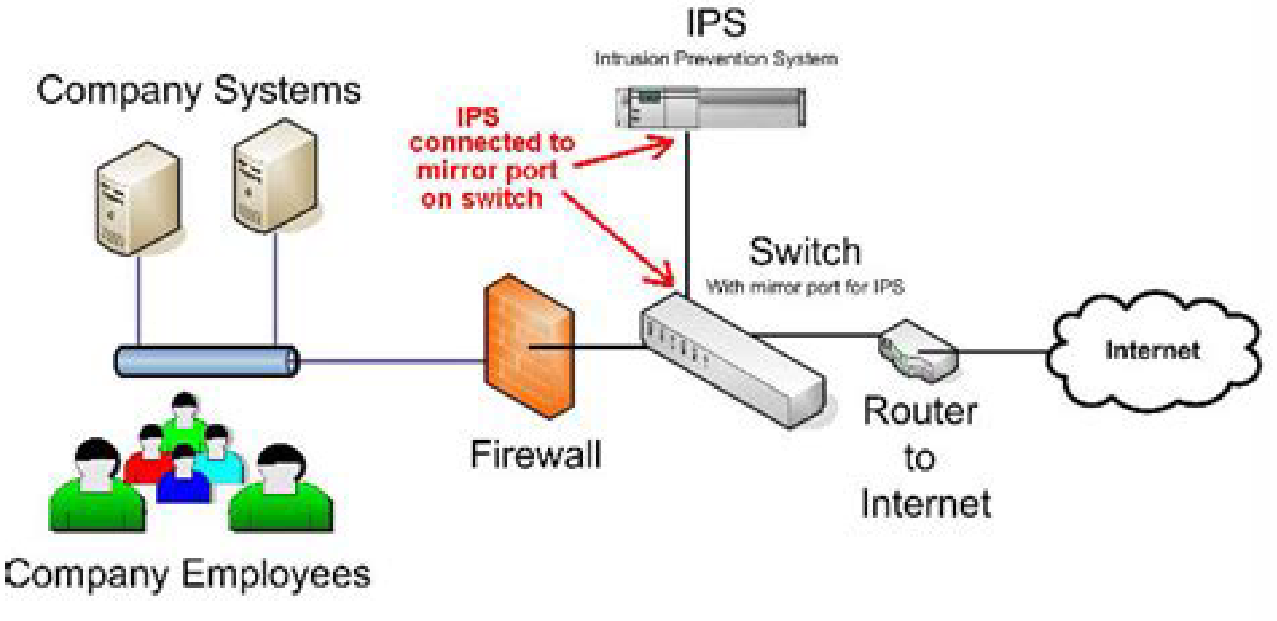


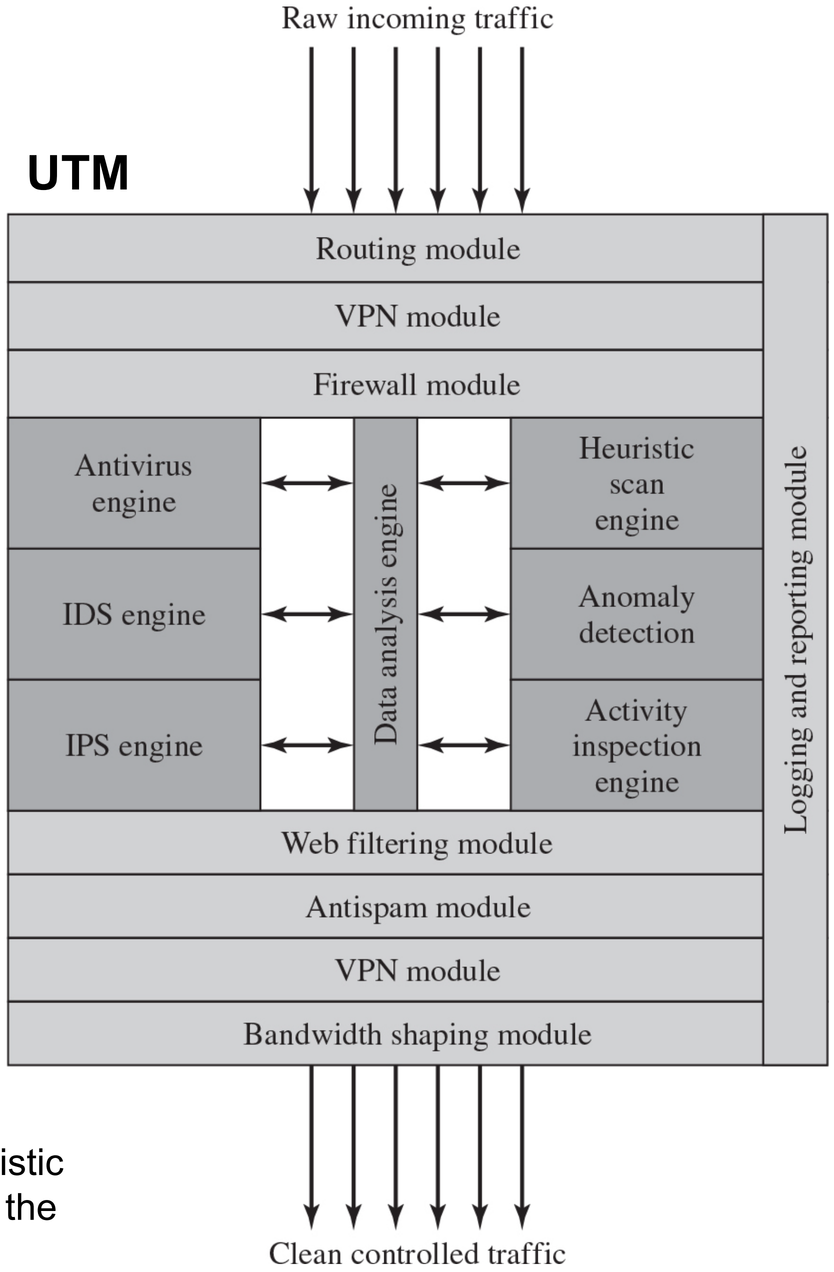
Fig. 9.3

Observation: VPN can be achieved also from Transport level, using SSL/TSL

Advanced Firewall Deployments: Intrusion Prevention Systems (IPS) and Unified Threat Management (UTM)



UTM



Also known as Intrusion Detection and Prevention System (IDPS):

- Is an extension of an IDS that includes the capability to attempt to block or prevent detected malicious activity
- Can be host-based, network-based, or distributed/hybrid
- Can use anomaly detection to identify behavior that is not that of legitimate users, or signature/heuristic detection to identify known malicious behavior can block traffic as a firewall does, but makes use of the types of algorithms developed for IDSs to determine when to do so

Network segmentation

- Is the process of dividing a LAN in Segments, each with different kind of users, hosts, servers, risks and exposure to externals.
- Each segment might be separated by the others using router firewalls.
- A notable segmentation model for Industrial Control Systems is called *Purdue model*

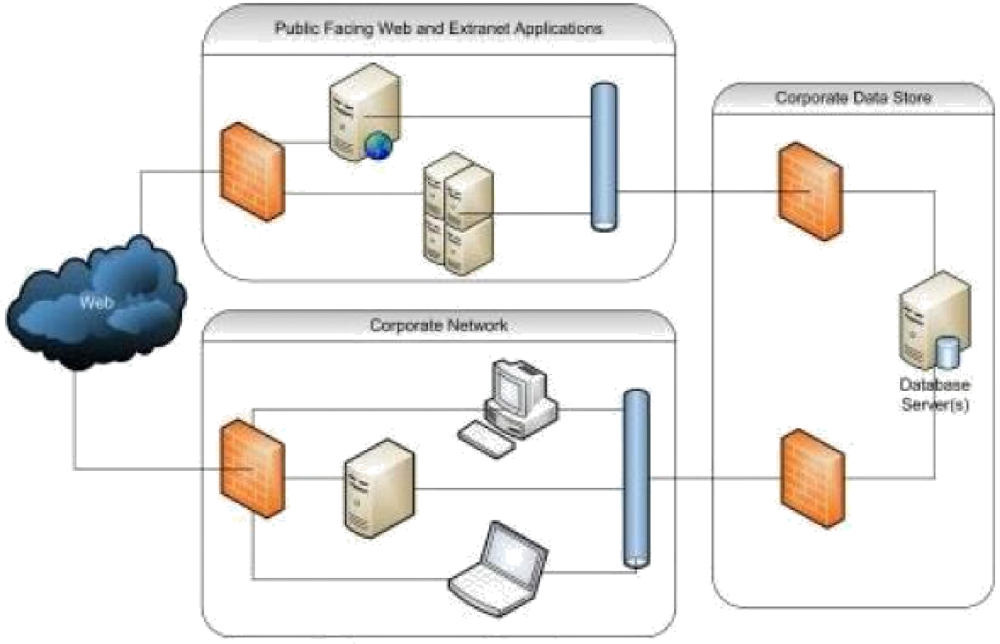
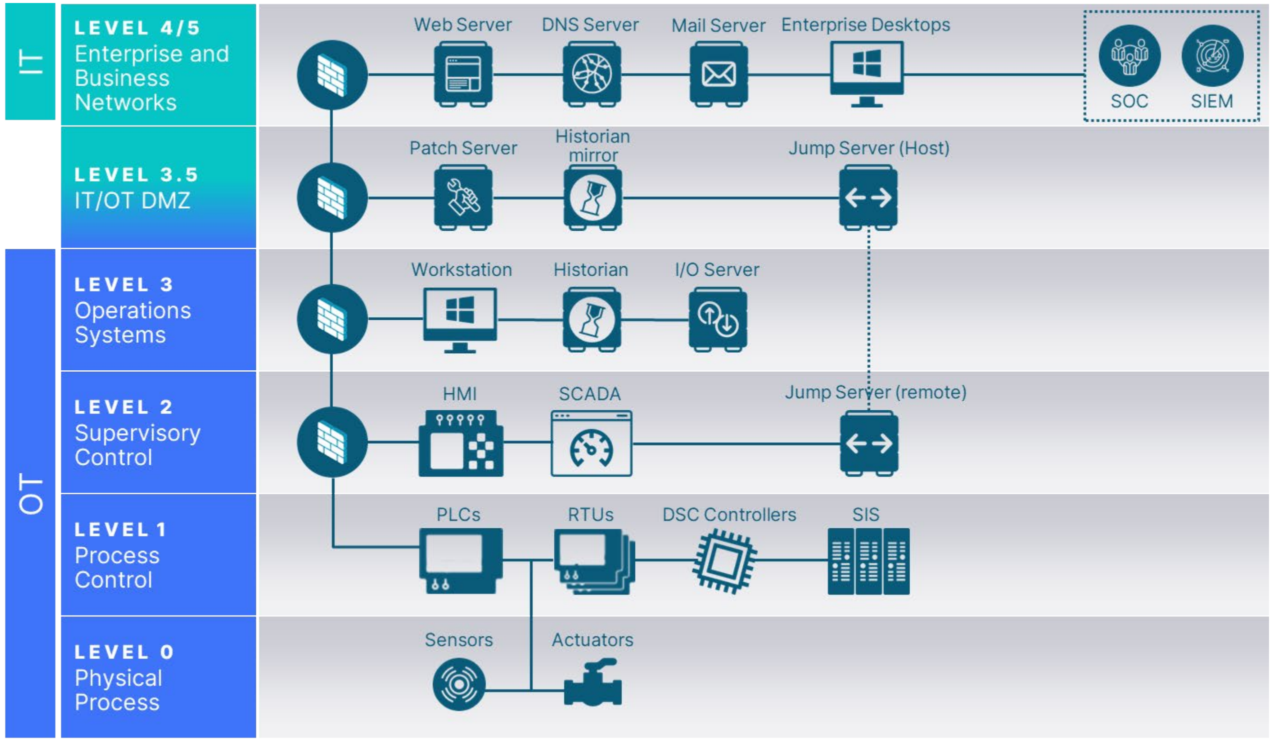


Figure 1: A secure network segmentation

Purdue model



IT
LEVEL 4/5
Enterprise and Business Networks
Web Server
DNS Server
Mail Server
Enterprise Desktops
SOC
SIEM
LEVEL 3.5
IT/OT DMZ
Patch Server
Historian mirror
Jump Server (Host)
OT
LEVEL 3
Operations Systems
Workstation
Historian
I/O Server
LEVEL 2
Supervisory Control
HMI
SCADA
Jump Server (remote)
LEVEL 1
Process Control
PLCs
RTUs
DSC Controllers
SIS
LEVEL 0
Physical Process
Sensors
Actuators