Network Security Architecture

Firewall, Network Segment, VPN, SASE and Etc

Dr. Tushar, Mosaddek Hossain Kamal
Professor (CSE, DU)

Computer Science and Engineering, University of Dhaka,

Mar, Academic Year: 2025

CSE804: Network and Internet Security

October 11, 2025

Outline

Network Security Components

The Network Security involves lot of security components, Such as,

- Firewall – Fundamental components of the network security
- Segmentation – What can we do using firewalls
- VPN – Virtual Private Network
- SASE – Secure Access Service Edge (Cloud Computing)
- etc

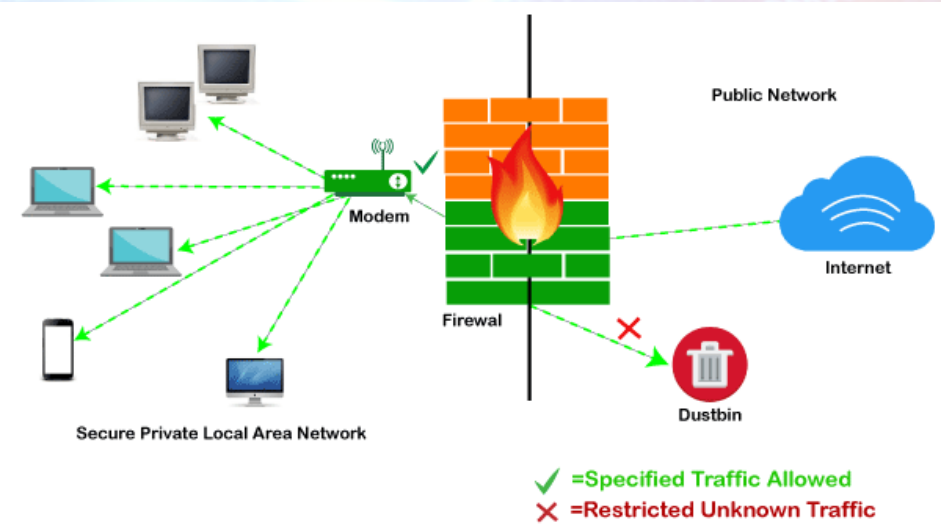
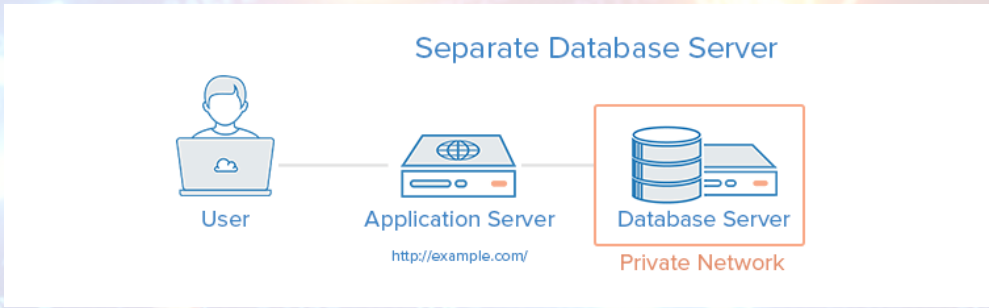


Figure 1: Firewall – Multi-layer

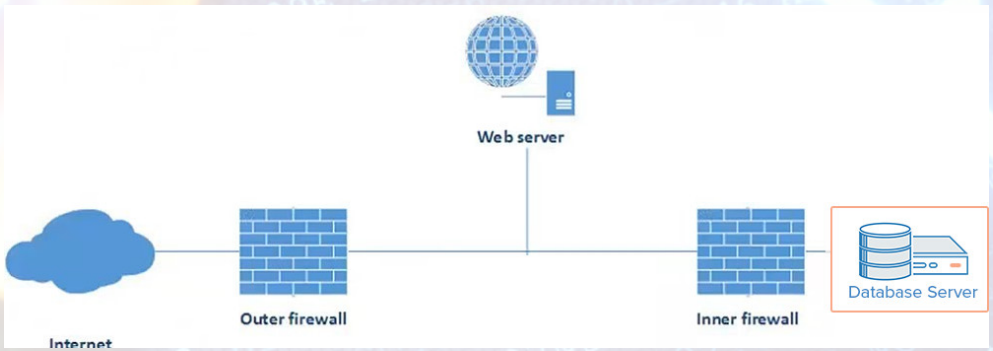
Firewall

Firewall Concepts Coming From the real life scenarios

- Creating Isolation and Protection from a dangerous event
- Take that concept in mind and apply to a network scenario
  - Example: A user workstation hitting a web server, the web-server/application server accessing a database



  - We typically put firewall between user – application server – database as,



Firewall – Operations

The purpose of firewall

- Firewall simply to filtering packet
- packet filtering – examine the packet's various components including content
  - We look into the packet
  - the information sent to user to application/web server
  - firewall examine

SRC Address	DST address	Port	Payload

  - Source address – The user machine or client address
  - Destination Address – Application Server, webserver or other service
  - Port – Service endpoint or TCP/UDP port (80, 443) – kind of traffice
  - Payload – Content or request/command (get/put, etc)
- Firewall can filter based upon the information

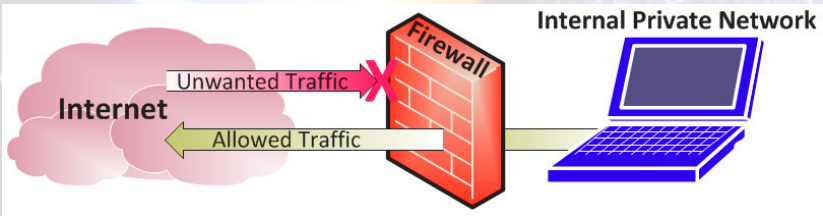
Firewall – operation

Firewall – Allow and match the criteria based on the rule, such as,

- Allow standard port 80 to web server
- Allow encrypted traffic 443
  - SSL/TLS encrypted traffic
- Open the first firewall (external) to allow those traffic

However we can make it more meaningful

- Block/set rule for source address allowed to access
- Why – we want to ensure that somebody is not spoofing
  - from internal or external
  - some time from internal somebody may spoofing
  - suppose a packet coming from the outside
    - claiming it is from inside (using internal address)
- Destination address filtering
  - If the external access tries to access the database – it will not allow



Second – internal Firewall

Internal Firewall

- Allow traffic to database only from web or application server
- Only allow packet from source address of web-server
- Not allow anything came fro the internet or external world
  - The packet must be originated from the application/web server
- The destination is only the database or target application

Thus we can create or assign rule using firewall to allow

- Packet from outside with addresses (allowed) only can access to the web or application server
  - It cannot get anywhere else
- Application/web server only can access to the database server

Basically, applying rules in the firewall to tighten the security

Firewall – Packet filtering

We are basically filtering the packet based on the header

- Source address
- destination address
- Port
- We have not look inside the packet – content

SRC Address	DST address	Port	Payload

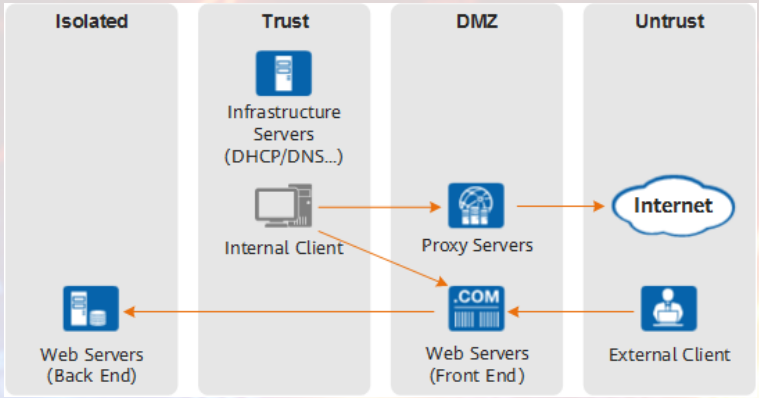
- There is no inspection to the payload
- We can do it in state full packet inspection

Firewall – Statefull

Statefull Packet inspection

- We can inspect packet in full including payload
- application firewall – in more specific
- the data send – make sure it not harmful to us
- In this case firewall open the envelop and like to see
  - Not only the header
  - but we can see the content as well
- It can inspect individual packet in isolation
- known as packet filtering
- Know as first generation firewall

Firewall – Zones/Segmentation



- Many security zones can achieve precise network control and security
- However, it may complicate the management
- The zones are: Untrust, Trust, and DMZ zones
- Untrust – connect the external network
- Trust – Internal Network
- DMZ – connects external and internal network – using certain rules
- Isolated – application server and database server, stores important data and needs to be deployed in the Isolated area
- Devices from different zone – need to configure security policies
- Attackers can access only resources of the zone contains attacked subnet.

DMZ

Defense in Depth – Demilitarized Zone (DMZ)

- Provide a systematic network configuration that include
  - packet filter firewall
  - an application proxy
  - personal firewalls or endpoint protection
  - demilitarized zone, or DMZ

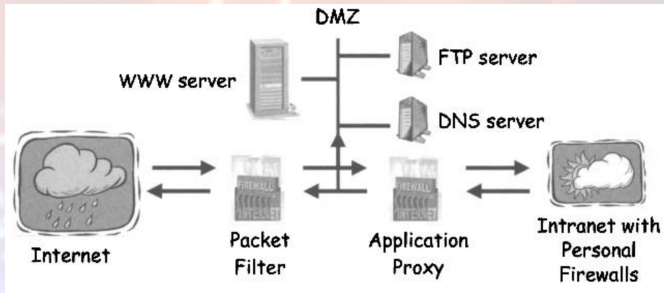


Figure 2: Demilitarized Zone (DMZ)

- System in DMZ must be exposed to the internet – use a packet filter
- System in DMZ must be maintained carefully
- Internal network is using proxy to the network and DMZ
- Fig. 2 if one layer of the defense is breached other layers will protect

Personal Firewall

Personal Firewall

- A personal firewall is used to protect a single host or a small network
  - Home network
- any of the three methods can be used
- generally such firewalls are relatively simple for the sake of efficiency and ease of configuration.
- compared to anti-virus applications, personal firewalls work in the background at the device (link layer) level
  - to protect the integrity of the system from malicious computer code by controlling internet connections

Next Generation Firewall

NGFW

A next-generation firewall (NGFW) is a third generation of firewall technology that implements in either hardware or software and is capable of detecting and blocking sophisticated attacks by enforcing security policies at the application, port and protocol levels.

NGFWs typically feature advanced functions including:

- application awareness; extensive control and visibility of apps, identify using analysis and signature matching
- Signature-based (Cloud based) integrated intrusion prevention systems (IPS);
- identity awareness – user and group control; work as bridged and routed modes
- the ability to use external intelligence sources.
- block malware from engine of the network

Please see: Internet Documents: FortiNet, Checkpoint, Cisco Sophos XG Firewall etc.

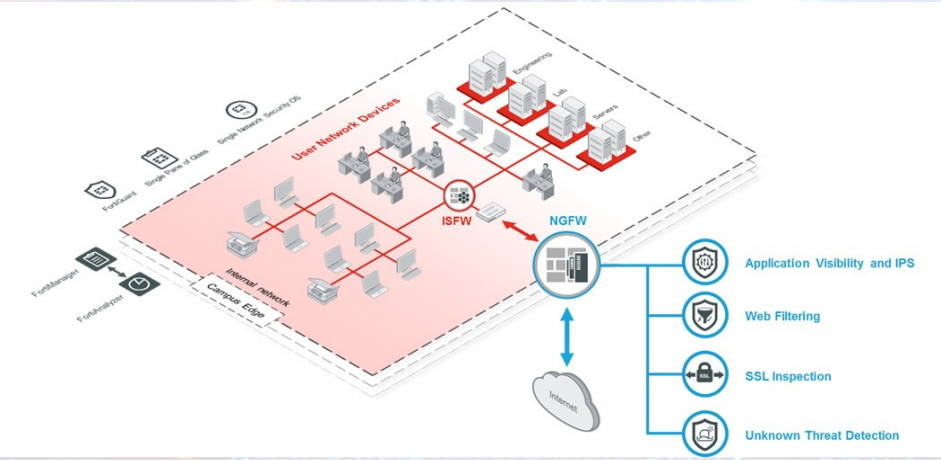
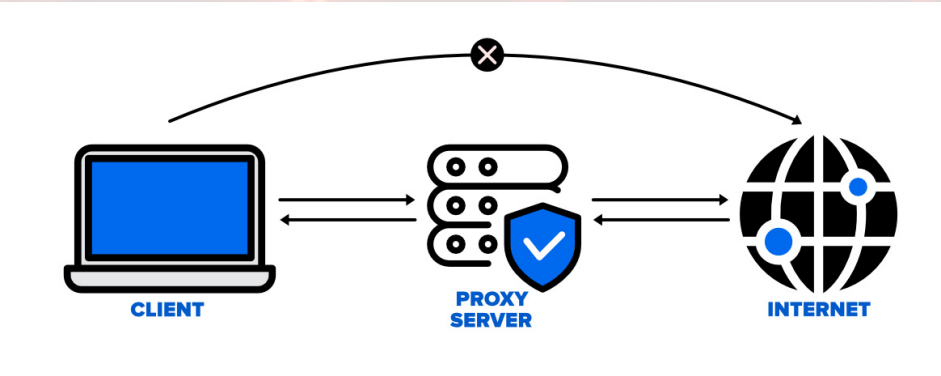


Figure 3

Firewall – Proxy



Proxy work on behalf of some application/services

- In direct connection incoming/outgoing packet travel without filtering
- Proxy breaks the session and inspect the content of the packet
- In proxy configuration
  - Client directly communication with proxy
  - Proxy communicating with the target service
  - Client connect with proxy and proxy communicating with back- end web/application server
  - Client things that it talking to the web server; in fact it talking to the proxy server
  - Proxy talking to the web server
- Now we have a man-in-the middle – but good guy

Proxy – Inspection

Proxy – Inspection

- Now as resides in the middle between client and server
- can inspect based on the rules and drop or allow to access
- Traffic coming from the outside– may be allowed of not
- We can set rule for dropping incoming/outgoing packets if it contains viruses or malware signature
- we can inspect and enforce security policies
- Sometime people put proxy for privacy reason
  - Who is accessing, what services
- Transparent proxy – automatically redirect the packet for certain request
- For transparent proxy client do not need to redirect the packet

1. **Stateless Firewall**
2. **Statefull Firewall**

NAT – Network Address Translation

It added an extra network security which may be interesting to the management

- Some addresses are route able to the Internet – known as public address
- Some address in IPv4 and IPv6 are reserved for private use
- IPv4:

Private IP	Public IP
Used with LAN or Network	Used on Public Network
Not recognized over Internet	Recognized over Internet
Assigned by LAN administrator	Assigned by Service provider / IANA
Unique only in LAN	Unique Globally
Free of charge	Cost associated with using Public IP
Range – Class A -10.0.0.0 to 10.255.255.255 Class B – 172.16.0.0 to 172.31.255.255 Class C – 192.168.0.0 – 192.168.255.255	Range – Class A -1.0.0.0 to 9.255.255.255 11.0.0.0 – 126.255.255.255 Class B -128.0.0.0 to 172.15.255.255 172.32.0.0 to 191.255.255.255 Class C -192.0.0.0 – 192.167.255.255 192.169.0.0 to 223.255.255.255

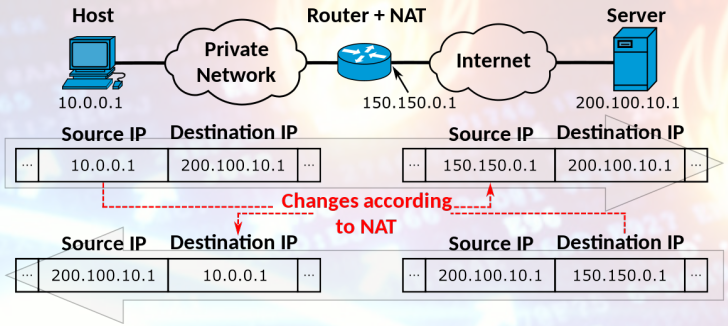
- IPv6:

IPv6 Address Category	Prefix
Unassigned	0::0
Loopback	0::1 or ::1
Link-local	FE80::/64
Unique Local	FC00::/7 (Equivalent to IPv4 Private address)
Multicast	FF00::/8
Global Unicast	2000::/3

NAT

NAT – Network Address Translation

- Private addresses are not routable to Internet
- So it needs some specific rule for internet traffic



- Private network – like Home or corporate office LAN
- Devices can communicate each other in the private network
- However, device needs public IP address to get Internet services
- Usual NAT-Box does the translation and keeps state of the communication
- NAT-firewall or simple NAT maintains a table that,
- Keep the private address to public address and vice-versa with
- Local-IP, Local-Port, Public (Pseudo IP), Peer IP and Peer Port, next

NAT Table

Index	Protocol	Local IP	Local Port	Pseudo IP	Pseudo Port	Peer IP	Peer Port
1	TCP	192.168.2.88	3645	60.49.63.157	55001	84.74.65.229	8080
2	TCP	192.168.2.88	3710	60.49.63.157	55002	84.74.65.229	8080
3	TCP	192.168.2.88	3819	60.49.63.157	55003	84.74.65.229	8080
4	TCP	192.168.2.88	4111	60.49.63.157	55006	84.74.65.229	8080
5	TCP	192.168.2.106	1472	60.49.63.157	55017	221.130.193.25	8080
6	TCP	192.168.2.88	1644	60.49.63.157	55019	84.74.65.229	8080
7	TCP	192.168.2.88	3534	60.49.63.157	55028	218.208.229.174	8080
8	TCP	192.168.2.88	3672	60.49.63.157	55030	218.208.229.174	8080
9	TCP	192.168.2.88	4866	60.49.63.157	55036	84.74.65.229	8080
10	TCP	192.168.2.88	1331	60.49.63.157	55037	84.74.65.229	8080
11	TCP	192.168.2.88	4893	60.49.63.157	4893	97.82.155.198	6881
12	TCP	192.168.2.88	4929	60.49.63.157	4929	68.148.20.210	28932
13	TCP	192.168.2.105	3102	60.49.63.157	3102	208.71.113.218	80
14	TCP	192.168.2.88	4398	60.49.63.157	4398	85.50.77.7	14706

NAT – Security ?

How NAT provides Security

- The local Devices are not accessible from outside of the network
- However, Devices in the local Network can Access the Internet
- Therefore, we can control the internal traffic and external traffic
- Prevent External traffic
- However, we can set NAT rule for external traffic to access certain services – port forwarding
- Protect Local Network Privacy and Provide Security
- Prohibit direct access from the Internet
- This is very common and uses in the Home router

VPN – Virtual Private Network

VPN Provides

- Provides Secure Channel to the untrusted network
- Encrypting information and sending over the network
  - We get confidentiality
  - People cannot see what is in the packet – all they see the encrypted information
  - Look like a pipe or tunnel between devices
  - Bad side – limited inspection capabilities
    - If bad guys using the VPN
    - Someone may putting maleware or viruses in our system
  - Security personnel or system cannot see the packet inside

VPN and ISO Protocol Stack

ISO Seven Layers

- Has different level of concern in each layer
  - Application Layer people concern about the application
  - Network Layer People concentrate their mind for network management
  - One of the layer deploy security will automatically applied for other layers

Application	SSH, SFTP
Presentation	Secure data format
Session Security:	RPC, Session – common token
Transport	TLS/SSL (old)
Network	IPSec
Data Linke	PPTP/L2TP
Physical	Surveillance, Authorized employee

- SSH, SFTP application specific VPN – you can connect secure connection to devices

OSI Layer Security

OSI 7-Layer Security

- Application Layer – encrypted application packet, SSH, SFTP, DNS Security
- Transport Layer Security - TLS/SSL
  - Secure Socket Layer – old name
  - PCIDSS support greater than TLS 1.1 (TLS 1.2+)
  - Web server 443 default
  - Provide certified public key – verifiable
  - Certified authority (CA)
  - Certificate - chain
- TLS provides private-public key end to end secure channel
- IPSec – Provides security between TCP/IP packets
  - All the information in IP packet is encrypted

VPN – Move towards Application

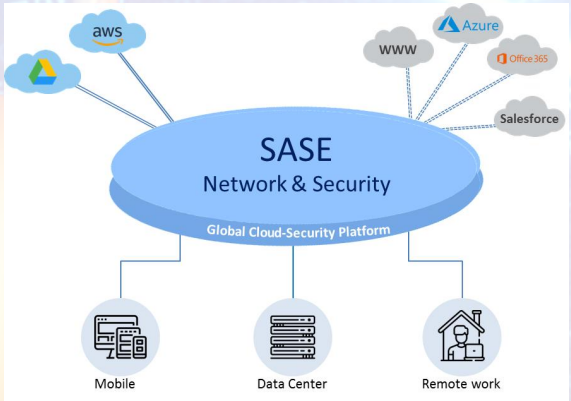
Nowadays Security prefer Application VPN rather Network based VPN

- Network Layer VPN simple and provide security for all
- Network layer VPN provides protection for other layers and for ALL APP
- Application Layer VPN is specific
- Good granularity
- Application Layer VPN: file sharinf, email and so on
- Application layer VPN control all application separately,
  - Therefore, we can shutdown an application if find issues

SASE – Secure Access Service Edge

SASE – Secure Access Service Edge

- Another subject of zero trust
- Micro segmentation
- zones for micro networks
- Create some sort of secure capability that deliver on edge
- SASE – is the intersection of Network, Cloud and Security



SASE

SASE - What is it

- It is WAN and Network Security Delivered from the cloud
- Network Security or NETSEC - contains
  - firewall
  - secure web gateway (application specific firewall)
  - DLP – Data loss prevention
- WAN Specifically, A software defined WAN (SD-WAN)
  - A way creating dynamic network
  - change the boundary of network and provision in real time
  - give more agility and flexibility
- Merging both of them give us scalability, scale up, scale down – elasticity
- Next – Identity Management – Authentication and Authorization

Combine all of this in a single component delivered from Cloud to Edge

SASE – Diagram

SASE – Technologies

Five essential technologies required for SASE deployment

- **FWaaS** – Firewall as a service
  - Cloud-Native next generation firewall
  - Providing advanced Layer 7 inspection,
  - access control
  - threat detection and prevention, and so on.
- **CASB** – Cloud Security Broker
  - Sectioned and unsenctioned SaaS services
  - Malware and threat detection
  - Ensures visibility and control of sensitive data in SaaS repositories – Part of cloud DLP solution
- **ZTNA** – Zero Trust Network Access
  - Enables continuous verification and inspection capabilities
  - delivers identity and application-based policy enforcement
    - Organization sensitive data and application

SASE – Technologies – Contd.

Five essential technologies required for SASE deployment (contd.)

- SD-WAN – Software Defined WAN
  - Provides an overlay network decoupled from the underlying hardware
  - Providing flexible, secure traffic between sites and direct to the internet.