INFOKAVACH
Redefining Security





2

Firewalls



@2021 Infokavach Consulting Private Limited | www.infokavach.com | info@infokavach.com | 05 April 2021 | Article 002 v1.0



This document is part of shot notes /articles/topic by topic series that intends to be supplementary, not a replacement for officially published security study guides and books. I may have added multiple definitions of the same process or procedure due to the varying definitions from different resources. If you encounter any conflicts, please refer to the latest Official security.

This is to benefit others with the knowledge and experienced gained during my study term. I hope this article would benefit those interested in becoming security experts or want to know various security concepts.

Firewalls

Firewall…Firewall is NOT an antivirus scanner! Firewalls are essential tools in managing and controlling network traffic. A firewall is a network device used to filter traffic based on defined 'set of rules', also called "filters" or "access control list". 'Set of rules' are basically set of instructions, used to distinguish authorized traffic from unauthorised and/or malicious traffic. Firewalls are It is typically deployed between a private network and a link to the internet; but it can also be deployed between departments with an organization.

Most firewalls offer extensive logging, auditing, and monitoring capabilities as well as alarms and basic intrusion detection system functions.

Firewalls are typically unable to block/detect virus or malicious code (i.e., firewall do not typically scan traffic as an anti-virus scanner) transmitted through otherwise authorized communication channels prevent unauthorized but accidental or intended disclosure of info by users, prevent attack by malicious users already behind the firewall, or protect data after it passes out of or into the private network. However, you can add these features as a special add-in modules or companion products, such as anti-virus scanners and Intrusion detection system (IDS)

Remember, firewalls are only one part of an overall security solution for an organization. With a firewall, many other security mechanisms are concentrated in one place, and thus a firewall can be a single point of failure. Its always suggested to have layered/Defence in depth approach to protect assets in an organization.

Firewalls provide protection only against traffic that crosses the firewall from one subnet to another and offer no protection against traffic within a subnet.

Purpose of firewalls

- They maintain the routing rules.
- Act as a single choke point (all traffic must pass through the firewall).
- Allow only authorised traffic (accept/ deny rules are applied on both inbound and outbound traffic).
- Enforce immunity against penetration attacks.

Types of Firewalls

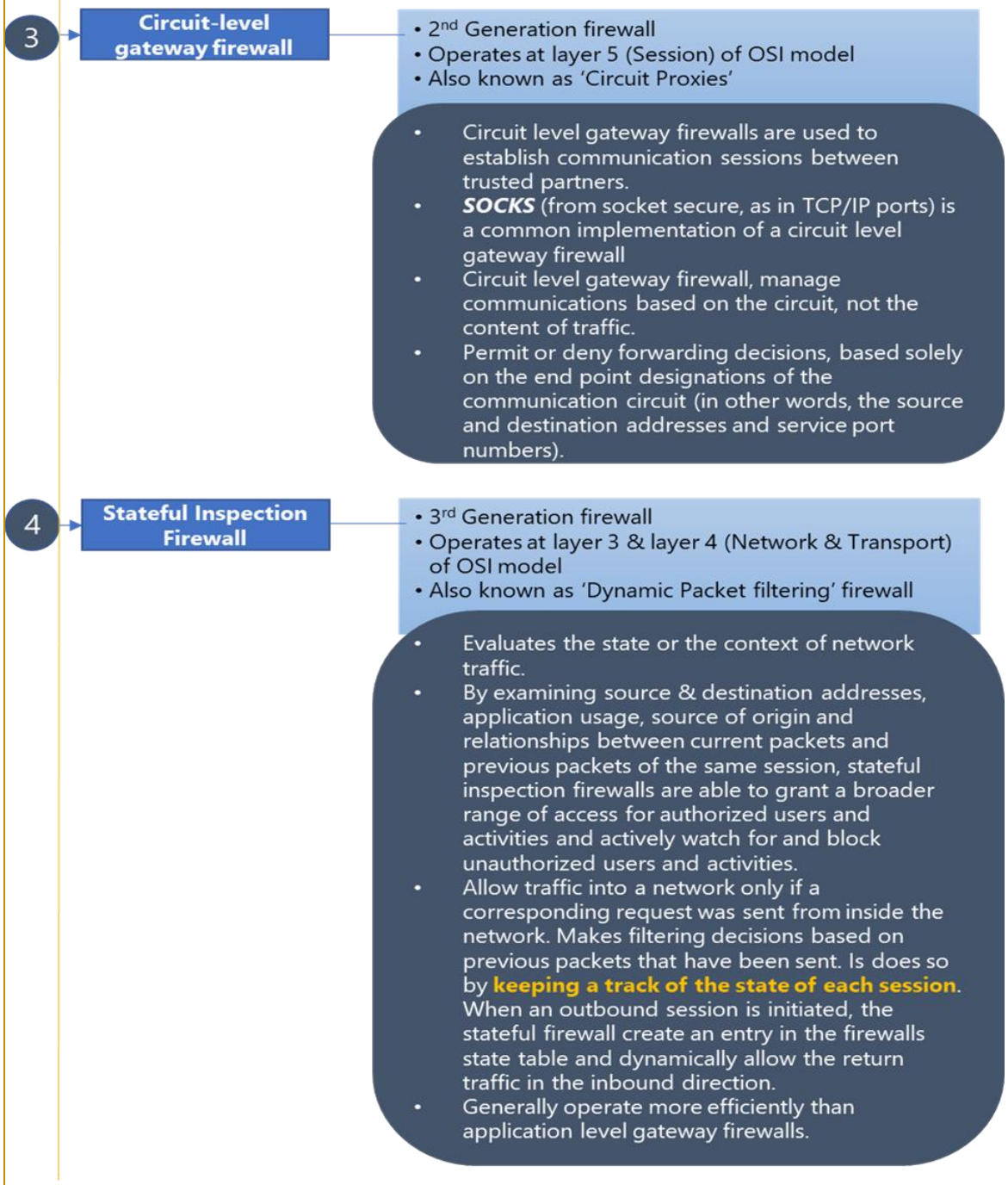
1. **Static packet filtering firewalls**
   - 1st Generation firewall
   - Operates at layer 3 (Network) of OSI model
   - Also known as 'Screening Router'

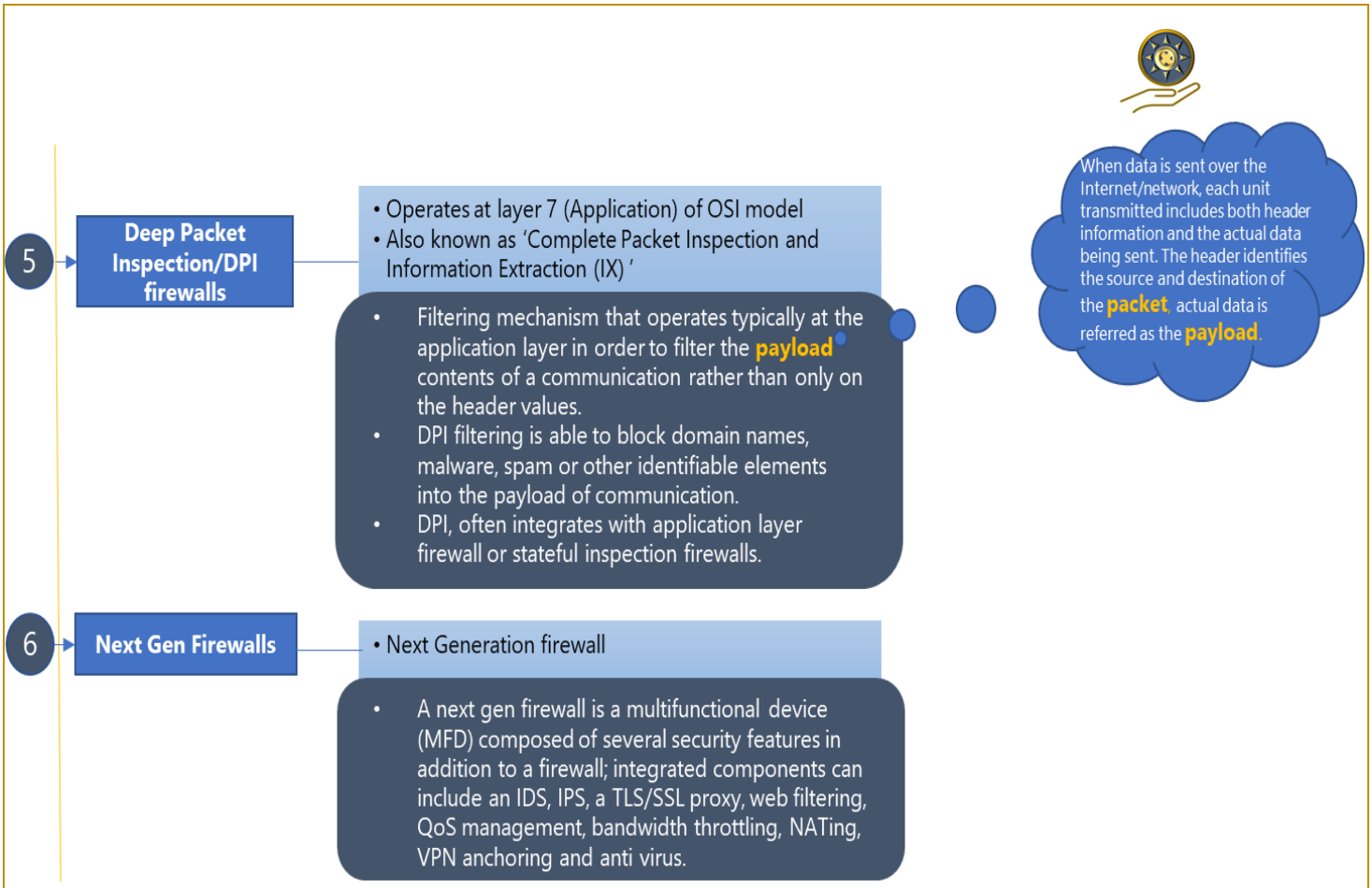
   - Filters traffic by examining data from a message header.
   - Typically, rules are concerned with:
     - ❑ Source
     - ❑ Destination
     - ❑ Port addresses
   - Unable to provide user authentication or to tell if a packet originated from inside or outside the private network, and it is easily fooled with spoofed packets

2. **Application-level gateway firewalls**
   - 2nd Generation firewall
   - Operates at layer 7 (Application) of OSI model
   - Also known as 'Proxy Firewall'

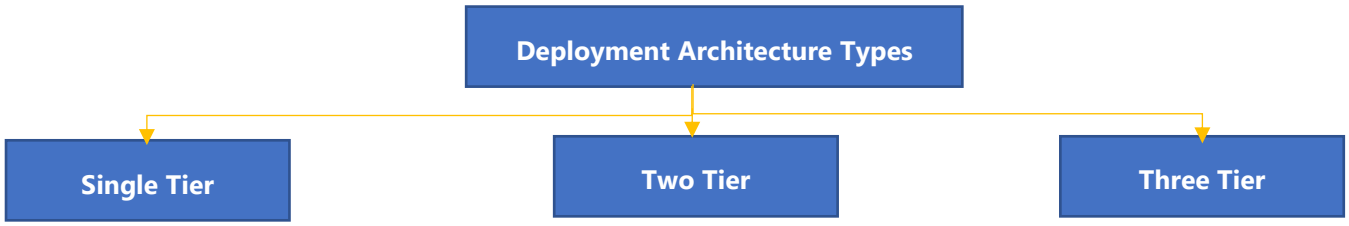
   - Filters traffic based on the internet service (in other words, the application) used to transmit or receive the data. Each type of application must have its own unique proxy server. Thus, an application level gateway firewall comprises numerous individual proxy servers.
   - This type of firewall negatively affects network performance as each packet must be examined and processed as it passes through the firewall.

A **proxy** is a mechanism that copies packets from one network into another; the copy process also change the source and destination address to protect the identity of the internal network.


3
Circuit-level gateway firewall
• 2nd Generation firewall
• Operates at layer 5 (Session) of OSI model
• Also known as 'Circuit Proxies'
• Circuit level gateway firewalls are used to establish communication sessions between trusted partners.
• SOCKS (from socket secure, as in TCP/IP ports) is a common implementation of a circuit level gateway firewall
• Circuit level gateway firewall, manage communications based on the circuit, not the content of traffic.
• Permit or deny forwarding decisions, based solely on the end point designations of the communication circuit (in other words, the source and destination addresses and service port numbers).
4
Stateful Inspection Firewall
• 3rd Generation firewall
• Operates at layer 3 & layer 4 (Network & Transport) of OSI model
• Also known as 'Dynamic Packet filtering' firewall
• Evaluates the state or the context of network traffic.
• By examining source & destination addresses, application usage, source of origin and relationships between current packets and previous packets of the same session, stateful inspection firewalls are able to grant a broader range of access for authorized users and activities and actively watch for and block unauthorized users and activities.
• Allow traffic into a network only if a corresponding request was sent from inside the network. Makes filtering decisions based on previous packets that have been sent. Is does so by keeping a track of the state of each session. When an outbound session is initiated, the stateful firewall create an entry in the firewalls state table and dynamically allow the return traffic in the inbound direction.
• Generally operate more efficiently than application level gateway firewalls.


5
Deep Packet Inspection/DPI firewalls
• Operates at layer 7 (Application) of OSI model
• Also known as 'Complete Packet Inspection and Information Extraction (IX) '
• Filtering mechanism that operates typically at the application layer in order to filter the payload contents of a communication rather than only on the header values.
• DPI filtering is able to block domain names, malware, spam or other identifiable elements into the payload of communication.
• DPI, often integrates with application layer firewall or stateful inspection firewalls.
6
Next Gen Firewalls
• Next Generation firewall
• A next gen firewall is a multifunctional device (MFD) composed of several security features in addition to a firewall; integrated components can include an IDS, IPS, a TLS/SSL proxy, web filtering, QoS management, bandwidth throttling, NATing, VPN anchoring and anti virus.
When data is sent over the Internet/network, each unit transmitted includes both header information and the actual data being sent. The header identifies the source and destination of the packet, actual data is referred as the payload.

Firewall Deployment Architecture



1. **Single Tier Deployment Architecture**

   A single tier deployment architecture places the private network behind a firewall, which is then connected through a router to the internet. Single tier is useful against generic attacks only and offers only minimal protection.

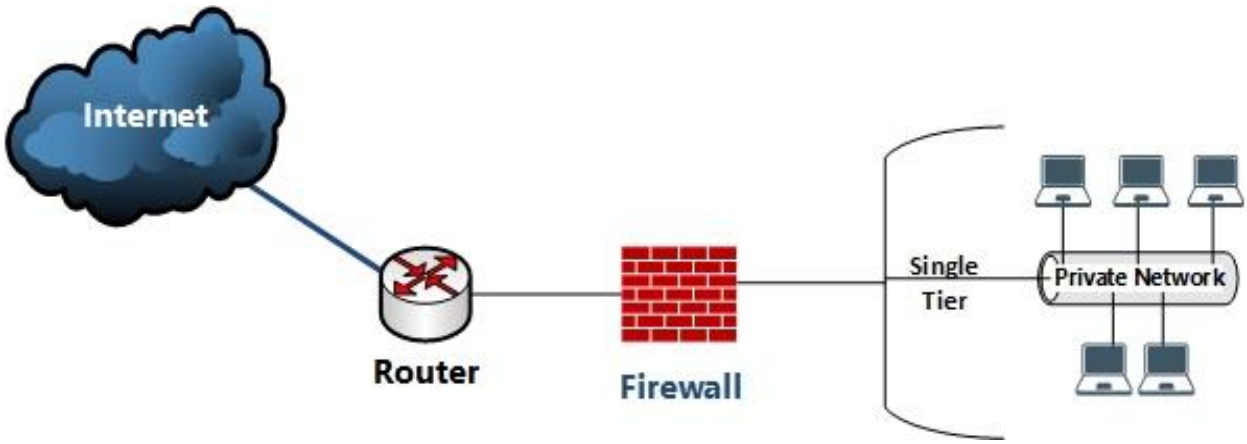


Figure 1: Single Tier Architecture

2. Two Tier Deployment Architecture

Two Tier deployment architecture may be one of the two different designs. One uses a firewall with three or more interfaces. The other used two firewalls in a series.

In the first design, the DMZ is located off one of the interfaces of the primary firewall. While in the second design the DMZ is located between the two serial firewalls.

The DMZ is used to host information server systems to which external users should have access. The firewall routes traffic to the DMZ or the trusted network according to its strict filtering rules. This architecture introduces a moderate level of routing and filtering complexity.

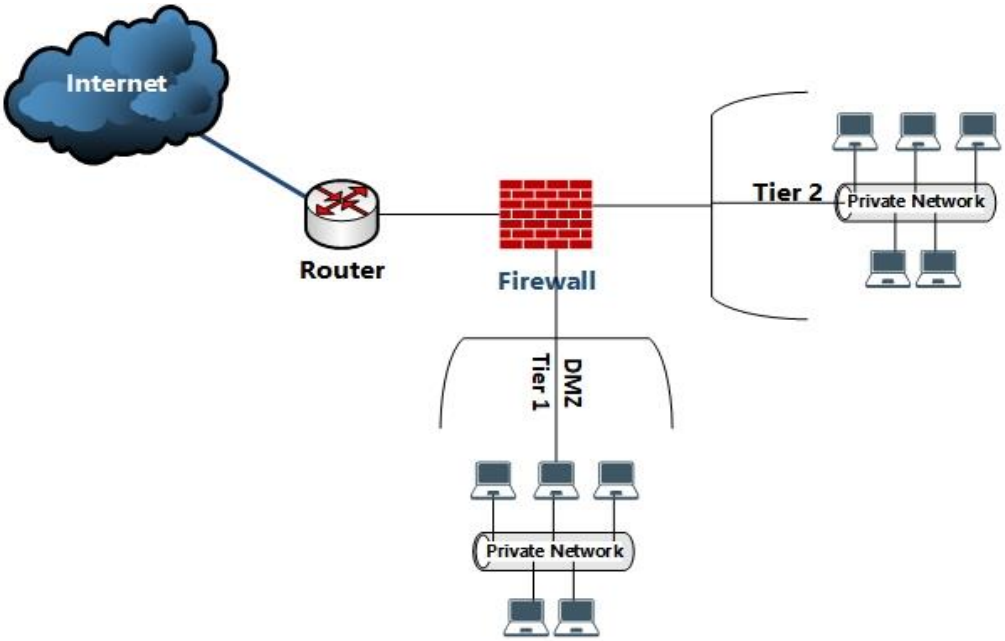


Figure 2: Two Tier Type I

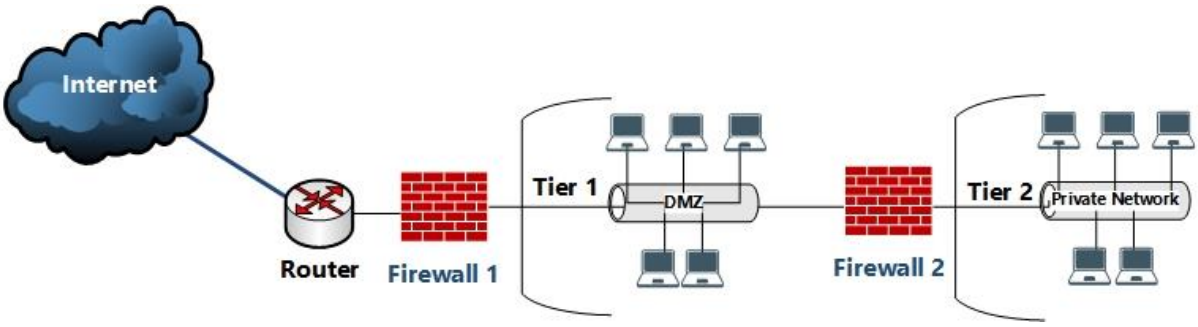


Figure 3: Two Tier Type II

3. Three Tier Deployment Architecture

The three-tier deployment architecture is the deployment of multiple subnets between the private network and the internet separated by firewalls. Each subsequent firewall has more stringent filtering rules to restrict traffic to only trusted sources. The outermost subnet is usually a DMZ. A middle subnet can serve as a 'transaction subnet; where systems needed to support complex web applications in the DMZ reside. The third, or back-end subnet can support the private network. This architecture is the most secure of these options; however, it is also the most complex to design , implement and manage.

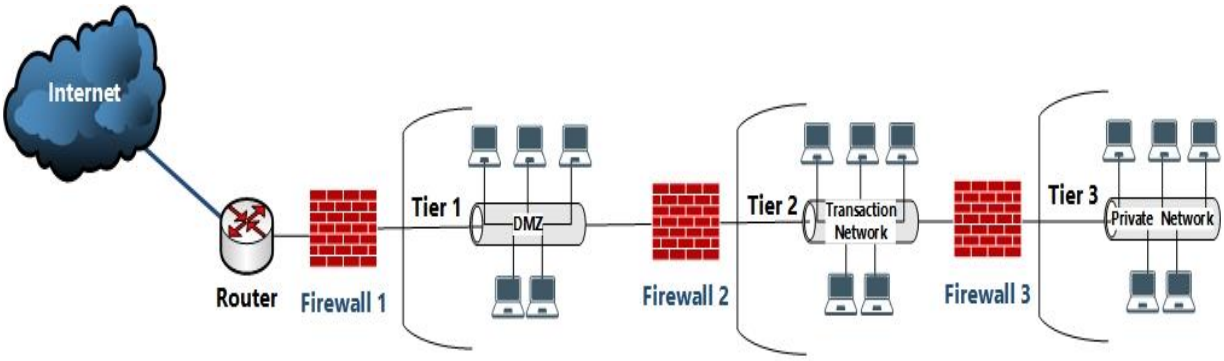


Figure 4: Three Tier Type I

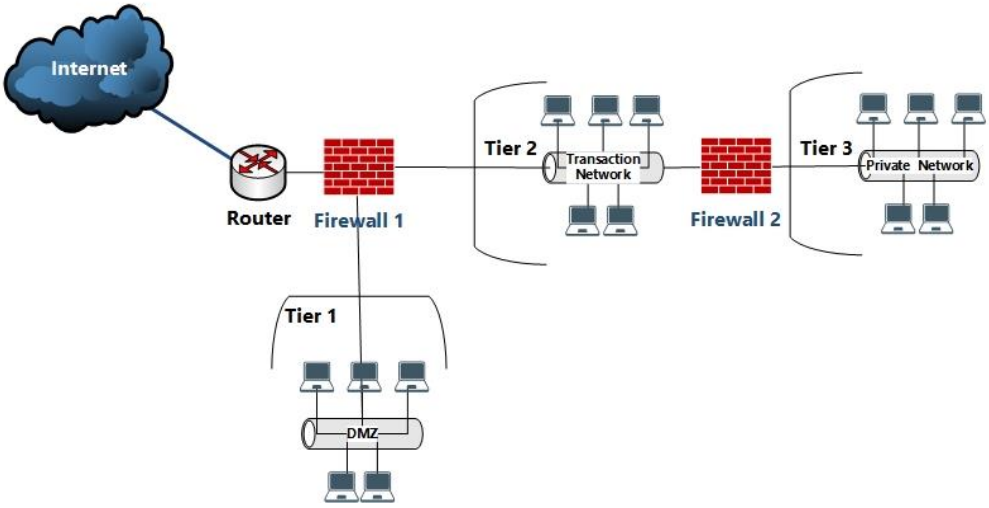


Figure 5: Three Tier Type II

Firewall Rules

A firewall filter traffic based on defined 'set of rules', also called "filters" or "access control list". 'Set of rules' are basically set of instructions, used to distinguish authorized traffic from unauthorised and/or malicious traffic.

Few common sets of rules those are configured in a firewall are as below.

1. Stealth Rule

It is an explicit rule near the of the ***policy denying access to the firewall*** beyond what is requested to manage the device. Stealth rule ensures that rules later defined in the policy do not inadvertently permit to firewall itself. Stealth rules disallow any communication to the firewall itself.

- **Source = ANY**
- **Destination = [Self]**
- **Service/application = ANY**
- **Action = DROP**
- **Logging = Enabled**

2. Explicit Rules

These rules are created for allow or drop traffic. At the top of the rule base, set the most explicit firewall rules. ***Rule bases typically work on a top-down protocol/sequence in which the first rule in the list perform its action first***. This action is done, so that the traffic permitted by the first rule, will never be assessed by the remainder of the rules.

3. Clean up Rule (set explicit drop rule)

The main purpose of firewalls is to drop all traffic that is not explicitly permitted. As a safeguard to stop uninvited traffic from passing through the firewall, place any-any-any drop rule (clean-up rule) at the bottom of each security zone context. This will ***provide a catch all mechanism for capturing traffic***.

- **Source = ANY**
- **Destination = ANY**
- **Service/application = ANY**
- **Action = DROP**
- **Logging = Enabled**

4. **Remove "Accept All" Rules**

5. **Implicit Deny Rule**

If traffic is not explicitly permitted, then it is denied.

Bonus Concepts

This section covers some concepts those would help in real time or while studying security concepts.

1. **Multihomed/Dual homed firewalls**

Some firewalls systems have more than one NIC/Interface and such firewall systems are known as multihomed systems (Please note, any machine/system/server/workstation/firewall or any other device with more than one network interface/NIC can be called as multihomed). A multihomed firewall must have at least two interfaces to filter traffic. All multihomed firewalls should have IP forwarding, which automatically sends traffic to another interface, disabled. This will force the filtering rules to control all traffic rather than allowing a software supported shortcut between one interface and another.

2. **Bastion Host**

Bastion host is a computer/appliance that is exposed to the internet and been hardened by removing all unnecessary elements such as services, programs, protocols, and ports.

3. **Screened Host**

A screened host is a firewall protected system logically positioned just inside a private network. All inbound traffic is routed to the screened host, which in turn acts as a proxy for all the trusted system within the private network. It is a responsible for filtering traffic coming into the private network as well as for protecting the identity of the internal client.

4. Screened Network

A Screened subnet is similar to screened host concept, except a subnet is placed between two routers or firewalls and the baston host(s) is located within that subnet. All inbound traffic is directed to the baston host, and only authorized traffic can pass through the second router/firewall into the private network. This creates a subnet where some external visitors can communicate with the resources offered by the network. This is the concept of DMZ, which is a network area (usually a subnet) that id designed to be accessed by outside visitors but that is still isolated from the private network of the organization. The DMZ is often the host of public web, email, file, and other resource servers.

END