



Romel Cabiling ▾



Home

Home > My courses > 121 - ITSP2B > 02 Delving into Security Toolkits > Lesson Proper for Week 2

Lesson Proper for Week 2

For a company that secures the network and data, it will add complexity to the network administrator. The costs of maintaining and implementing such a high level of security, such as e-commerce, intranet, extranet, and email services, are always high, but when compared to the loss that is incurred due to the lack of high-level security, it is considered more important.

But if a company opts for a Cisco firewall, software, instead of hardware, would also have the same kind of security fulfillment. Cisco IOS provides full-featured firewall services when it is implemented properly on any Cisco router. It helps a network to break down into several small domains or sub networks, thereby helping to keep the possible security breach limited to one domain, if any, and preventing it from spreading across the entire network, which would result in a major loss.

There are two important parts of a firewall:

- A part to permit the traffic
- A part to block the traffic

Most firewalls permit traffic from a trusted zone to the untrusted zone without any special configuration. But the traffic flow from the untrusted zone to the trusted zone must be configured and must be explicitly permitted, so anything not configured or permitted from untrusted to trusted should be denied implicitly. A firewall is not limited to trusted and untrusted zones only; it also has a mid-zone called the **DMZ zone (Demilitarized zone or less-trusted zone)**.

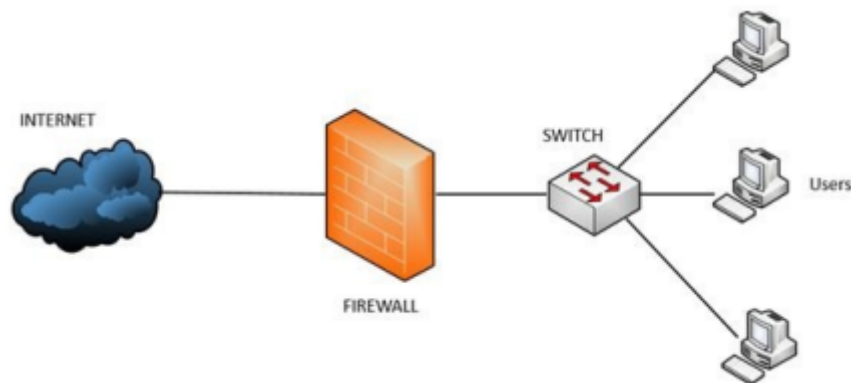
Basically, a firewall is a set of programs that can be enabled in a network gateway server and secures the resources of a private network from other external network users. The firewall operates based on the set of rules and policies defined by the administrator.

Firewalls come in two varieties:

- **Hardware firewall:** Examples are routers with built-in **Access Control List (ACL)**, **Adaptive Security Appliance (ASA)**, and **Personal Internet Exchange (PIX)**
- **Software firewall:** Operating systems with firewall software

All the messages entering inside and moving out from the internet to the intranet pass through the firewall. Thus, a firewall offers a preeminent security solution.

Firewalls are based on rules and policies. The rules configured on the firewall decide what type of connection should be allowed and how it should be allowed. The firewall also decides based on the direction of the packet flow:



Apart from controlling unauthorized access to the network, firewalls also help to allow remote connection to a secure network using authentication mechanisms.

The rules that firewalls use are that nothing but security guidelines that can be configured by a user or a network administrator to permit/deny the traffic to file servers, web servers, FTP servers, and Telnet servers. Firewalls allow administrators to have immense control over the traffic flowing in and out of their systems/networks.

FIREWALL FUNCTIONS

Firewalls primarily have two functions:

- Packet filtering
- Network Address Translation

Most firewalls also perform two other important security services:

- Encrypted authentication
- Encrypted tunnels

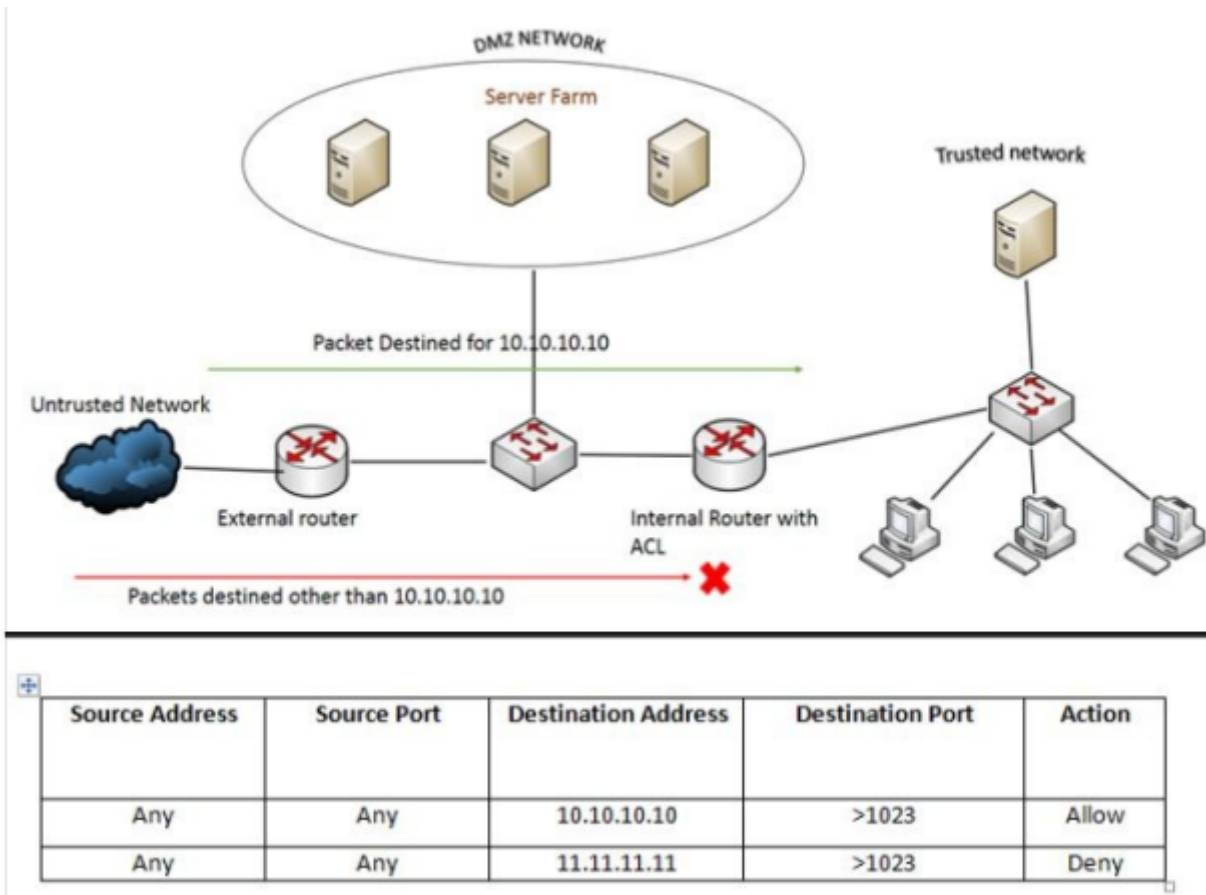
1. Rules of Firewall

The rules of a firewall can be customized depending on our needs, requirements, and threat levels. There are different conditions on which firewall filters work. These are as follows:

- **IP address:** The first condition on which a firewall rule works is on IP address. The decision is based on the range of IP addresses and subnet masks.
- **Domain name:** The second condition on which a firewall works is on domain name. A firewall can be configured to permit or deny access to specified domain names of corporate websites or domain name extensions, such as .org, .tv, or .biz.
- **Protocols and ports:** c a firewall works on is the protocols and its ports. A firewall can be configured to permit or deny some protocols and port numbers, such as SMTP, FTP, UDP, and SNMP. It can also be configured to inspect the traffic passing through the open ports of the server.
- **Keywords:** The fourth condition on which the firewall works is specific keywords. Firewalls can be configured to check some keywords or phrases to decide whether to permit offensive data to flow in the network or not.

The logic is based on a group of guidelines configured either statically or dynamically, based on the requests of information in the network. Most firewalls use the header information of the packet to determine whether it should be allowed or blocked.

Let's assume the following network topology to understand how a firewall uses the configured rules:



The rule in this diagram mentions that any incoming packet (**Source Address —Any and Source Port—Any**) that is intended for the internal network with a **Destination Address** of 10.10.10.10 and a Destination Port of more than 1023 is allowed to enter the network, and all other incoming packets with a destination other than 10.10.10.10 will be blocked.

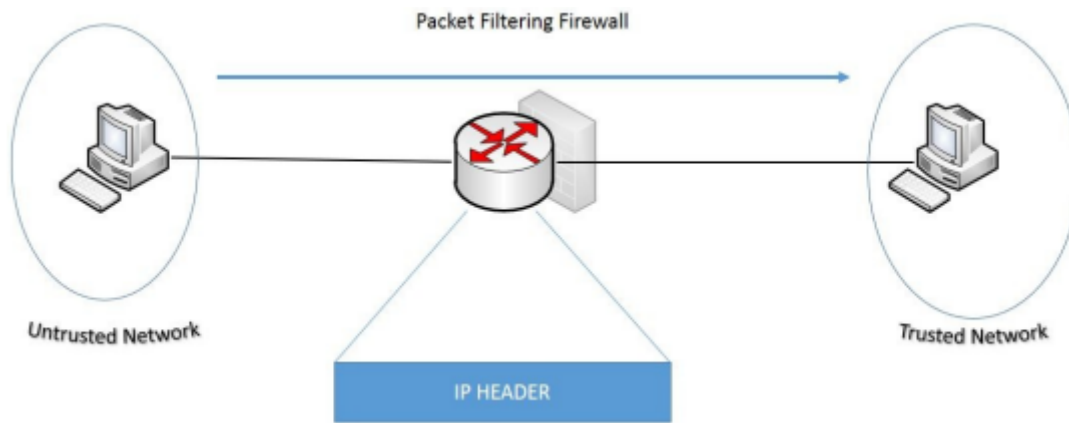
2. Types of Firewall

Firewalls can be classified into the following types, based on their operation and the method used to inspect the packet:

- Packet-filtering firewalls
- Circuit-level gateway firewalls
- Application firewalls
- Zone-based firewalls

A. Packet-filtering firewalls

This type of firewall is nothing but routers that connect the internal network to the external network. Packet-filtering firewalls work on the network layer and the transport layer of the OSI model. Routers configured with an ACL are packet-filtering firewalls. An ACL can be defined based on the IP address, protocols, and packet attributes (IP header), as shown in the following diagram. If a packet does not meet the configured policies and rules, the packet is discarded and the routers will create a log:

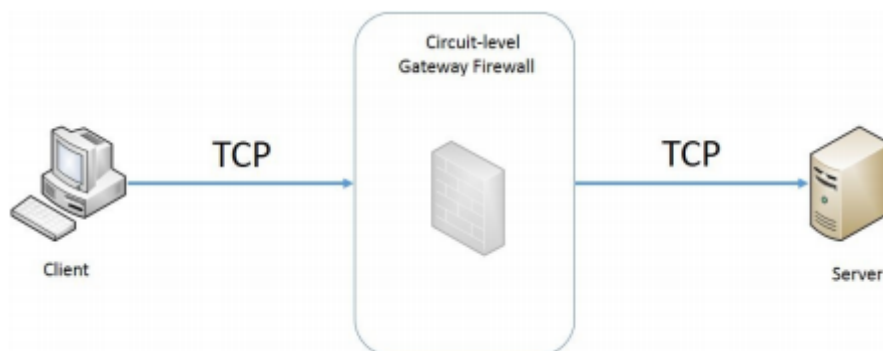


B. Circuit-level gateway firewalls

This is also known as a transparent proxy firewall. The word stateless indicates that the firewall checks the matching criteria and, if matched, forwards the traffic, but the return traffic will once again be inspected as a separate packet.

For example, assume web traffic is going from host **A** to server **B**. If this traffic was allowed by the firewall, the traffic would pass through. However, the return traffic, that is, from server **B** to host **A**, would once again be verified on the outbound interface of the firewall. If the firewall has a policy to block this traffic, then the return traffic gets dropped. This might not be proper policy enforcement on the firewall.

An example of a stateful firewall is **Cisco Adaptive Security Appliance (Cisco ASA)**:



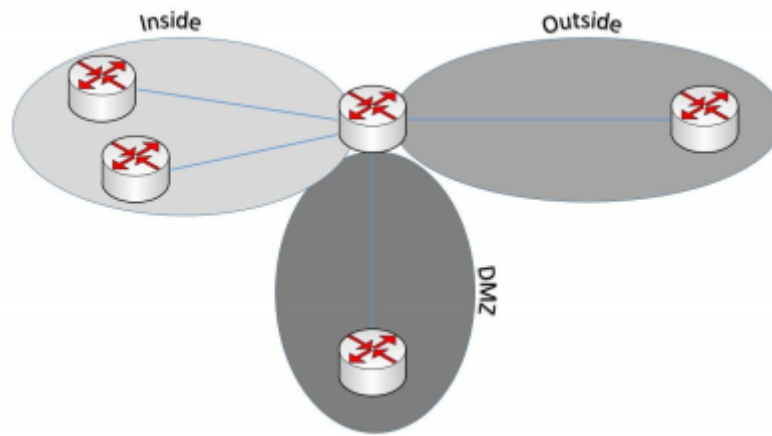
C. Application-layer firewall

It is a Layer-7 firewall that does a deep-packet inspection. The difference between an application-layer firewall and the firewalls mentioned earlier is that the application-layer firewall can check inside the content of the payload.

For example, this type of firewall does more than looking at just the port number, such as port 80 identifying HTTP. It can identify whether the structure of the HTTP payload looks like malicious code and can drop it.

D. Zone-based firewall

This is another layer-7 firewall that can perform deep-packet inspection. But, its added functionality is the capacity of this firewall to bundle some common interfaces under the zone and define a policy for a zone pair:



For example, if there are two LAN and one WAN connections, the firewall could bundle the two local interfaces under a zone called inside zone and map the WAN link to a zone called outside zone. The traffic can be classified using a class map. The policy is defined using a policy map. This policy will then be applied on the zone pair from the inside to outside zone or the outside to inside zone.

Here are the best practices for designing a sound firewall policy:

- Trust no one: It is always advisable to enable all the key services and deny the rest of the traffic. Analyze the privilege levels of the user and, based on the report, assign those services to them. You need to deploy the least privilege principle; this concept gives a user access to only what is needed and nothing more.
- Deny physical access to firewall: It is always a good practice to keep any kind of physical access to a firewall controlled or deny it completely. For example, place the firewall inside a server farm/data center.
- Allow only necessary protocols: It's always good to have a prepared list of protocols, including those that should be allowed and those that need to be blocked.
- Use logs and alerts: A logging strategy must be followed to ensure the level and type of logging, and you need to be sure to monitor all those logs on a regular basis.
- Segment security zone: Create internal zones and explicitly define a policy for incoming traffic from the internet. Create a DMZ if public servers have to be placed.
- Do not use a firewall as a server: A firewall should never be used in server incorporation design. We should always uninstall or disable any unwanted software, as per the company requirement. Management tools are important ones that need to be removed.
- Never use a firewall as a workstation: In general, a user's system depends on a lot of client applications, such as Microsoft and Oracle, which can create vulnerability that viruses and worms may exploit.
- Restrict access to firewalls: Access to firewalls should be highly restricted. Only an administrator should be allowed to log in into strong password assigned to them. This can use OTP cards for better security.
- Combine firewall technologies: Packet filtering should not be done only for the line of defense. It can be incorporated with some inspections using protocols, stateful mechanisms, and applications.

- Use a firewall as part of comprehensive security solutions: A firewall should be positioned facing the internet directly for any incoming network traffic. A firewall should be used with other security appliances and applications to provide a defense in depth strategy.

Maintain the installation: Software and patches should be kept updated. The updating of a firewall configuration, as per application and business requirements, might change.

◀ Preliminary Activity for Week 2

Jump to...



Analysis, Application, and Exploration for Week 2 ▶



Navigation

Home



Dashboard

Site pages

My courses

121 - CC106

121 - BPM101 / DM103

121 - OAELEC2

121 - ITE3

121 - MUL101

121 - ITSP2B

Participants



Grades


General

01 Exploring Security Threats

02 Delving into Security Toolkits

 Preliminary Activity for Week 2

 **Lesson Proper for Week 2**

 Analysis, Application, and Exploration for Week 2

 Generalization for Week 2

 Evaluation for Week 2

 Assignment for Week 2

03 Intrusion Prevention System

04 Understanding Security Policies I

05 Understanding Security Policies II

06 - Preliminary Examination

07 Deep Diving into Cryptography

08 Deep Diving into Cryptography: Types of Cipher

- 09 Implementing the AAA Framework
- 10 Implementing the AAA Framework: Implementing A...
- 11 Securing the Control and Management Planes
- 12 - Midterm Examination
- 13 Protecting Layer 2 Protocols
- 14 Protecting the Switch Infrastructure
- 15 Exploring Firewall Technologies I
- 16 Exploring Firewall Technologies II
- 17 Cisco ASA

121 - WEB101 / CCS3218

Courses

Fair Warning

NOTICE: Please be reminded that it has come to the attention of the Publishing Team of eLearning Commons that learning materials published and intended for ***free use only by students and faculty members within the eLearning Commons network were UNLAWFULLY uploaded in other sites without due and proper permission.***

PROSECUTION: Under Philippine law (Republic Act No. 8293), copyright infringement is punishable by the following: Imprisonment of between 1 to 3 years and a fine of between 50,000 to 150,000 pesos for the first offense. Imprisonment of 3 years and 1 day to six years plus a fine of between 150,000 to 500,000 pesos for the second offense.

COURSE OF ACTION: Whoever has maliciously uploaded these concerned materials are hereby given an ultimatum to take it down within 24-hours. Beyond the 24-hour grace period, our Legal Department shall initiate the proceedings in coordination with the National Bureau of Investigation for IP Address tracking, account owner identification, and filing of cases for prosecution.

2nd Semester Enrollment

A banner for Bestlink College of the Philippines (BCP) featuring a blue-tinted image of a modern building. The text is overlaid on the image. At the top right, it says "visit www.bcp.edu.ph". The main headline in large red letters reads "Enrollment registration is now Ongoing". Below this, in white text on a blue background, it says "For 2nd Semester SY 2021 - 2022". Underneath that, in white text on a dark blue background, it says "We are accepting new students, returnees and transferees." On the right side, there is a quote: "Be trained to be the best, Be linked to success" next to the BCP logo. At the bottom left, there is an email icon and the address "bcp-inquire@bcp.edu.ph". At the bottom right, there is a phone icon and the numbers "(8)442-8601 | (8)518-8050".

visit www.bcp.edu.ph

Enrollment registration is now Ongoing

For 2nd Semester SY 2021 - 2022

We are accepting new students, returnees and transferees.





"Be trained to be the best,
Be linked to success"



 bcp-inquire@bcp.edu.ph

 (8)442-8601 | (8)518-8050

Activities

-  Assignments
-  Forums
-  Quizzes
-  Resources

Bestlink College of the Philippines
College Department

Powered by [eLearning Commons](#)