



Romel Cabiling ▾



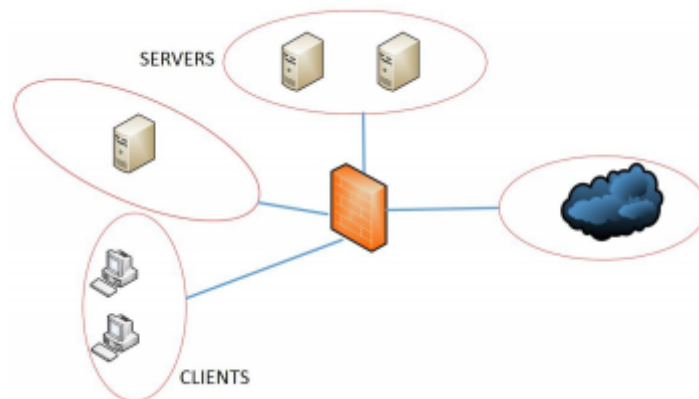
[Home](#)

[Home](#) > [My courses](#) > [121 - ITSP2B](#) > [15 Exploring Firewall Technologies I](#) > [Lesson Proper for Week 15](#)

Lesson Proper for Week 15

EXPLORING FIREWALL TECHNOLOGIES

Firewalls can be defined as any hardware or software that enables the filtering of the packets or controls the flow of traffic. They are generally implemented in a network perimeter. They act as a border for trusted and untrusted zones:



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

But if a company opts for Cisco IOS Firewall, software, instead of hardware, would also have the same kind of security satisfaction. Cisco IOS provides fullfeatured firewall services when it is implanted properly on any Cisco router. It helps a network to break down into several small domains or sub-networks, thereby helping by keeping the possible security breach limited to one domain, if any, and not allowing it to spread to the entire network—that would result in a major loss.

Two crucial apparatuses are used to carry out the functions of the firewall:



- An apparatus to block the traffic
- An apparatus to permit the traffic

Most firewalls would permit traffic from a trusted zone to an untrusted zone without any special configuration. But the reverse has to be configured and must be explicitly permitted, hence anything not configured/explicitly permitted from an untrusted zone to a trusted zone should be implicitly denied. A firewall is not limited to trusted and untrusted zones; there are mid-zones, generally known as **DMZs (Demilitarized Zones, or less trusted zones)**.

Basically, a firewall is a set of programs that can be enabled in a network gateway server that secure the resources of a private network from other external network users.

The following topics will be covered:

- What is a Firewall
- Types of Firewalls

Services offered by the Firewall

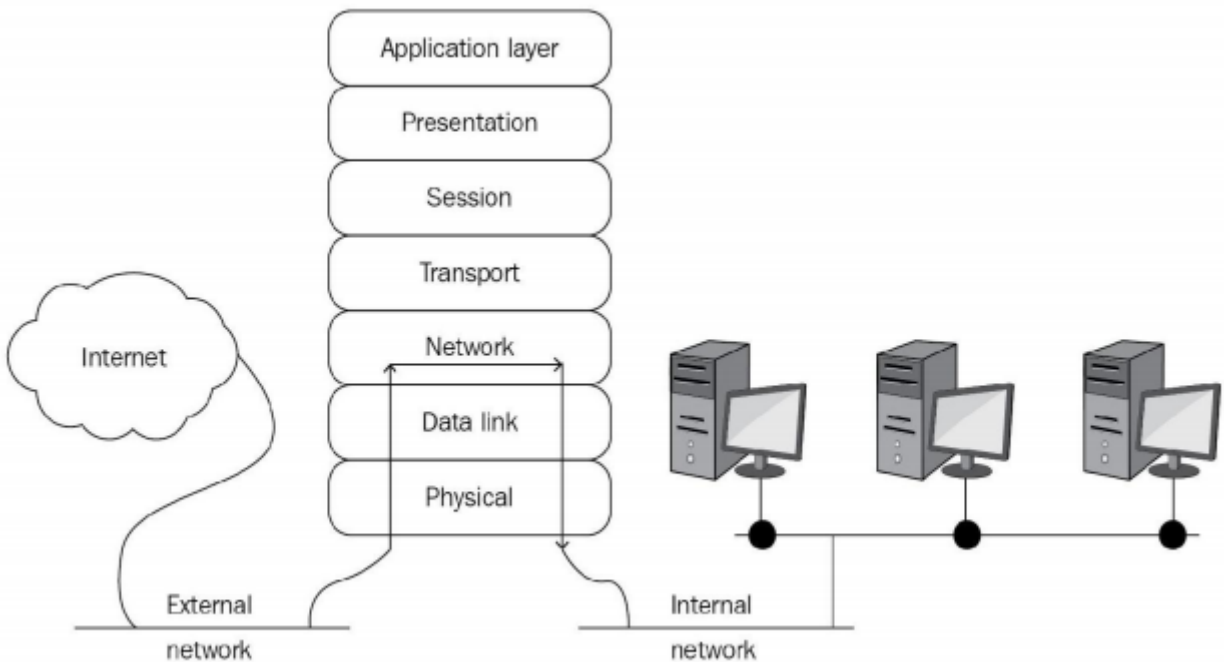
Services offered by the firewall are:

- Static-packet filtering
- Circuit-level firewalls
- Proxy server
- Application server
- NAT
- Stateful packet inspection

1. Static-packet filtering

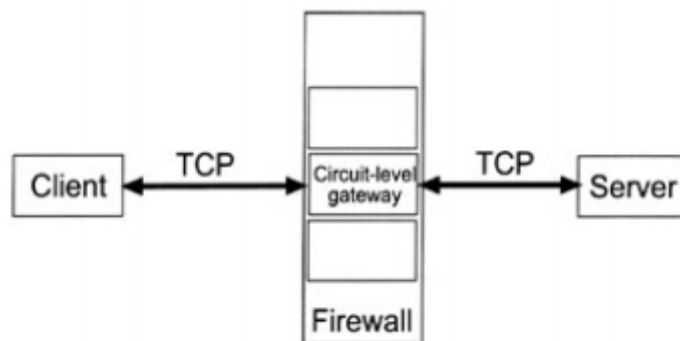
It is a firewall and the routing ability of a device that can filter packets based on fields of the packet and the rules configured by the administrator. The administrator can define rules (ACLs) to manage allowed ports and IP addresses at Layer 3 and Layer 4:





2. Circuit-level firewalls

It is also known as a **transparent proxy firewall**. This firewall cannot change the request or response beyond the authentication and authorization required by the proxy:



3. Proxy Server

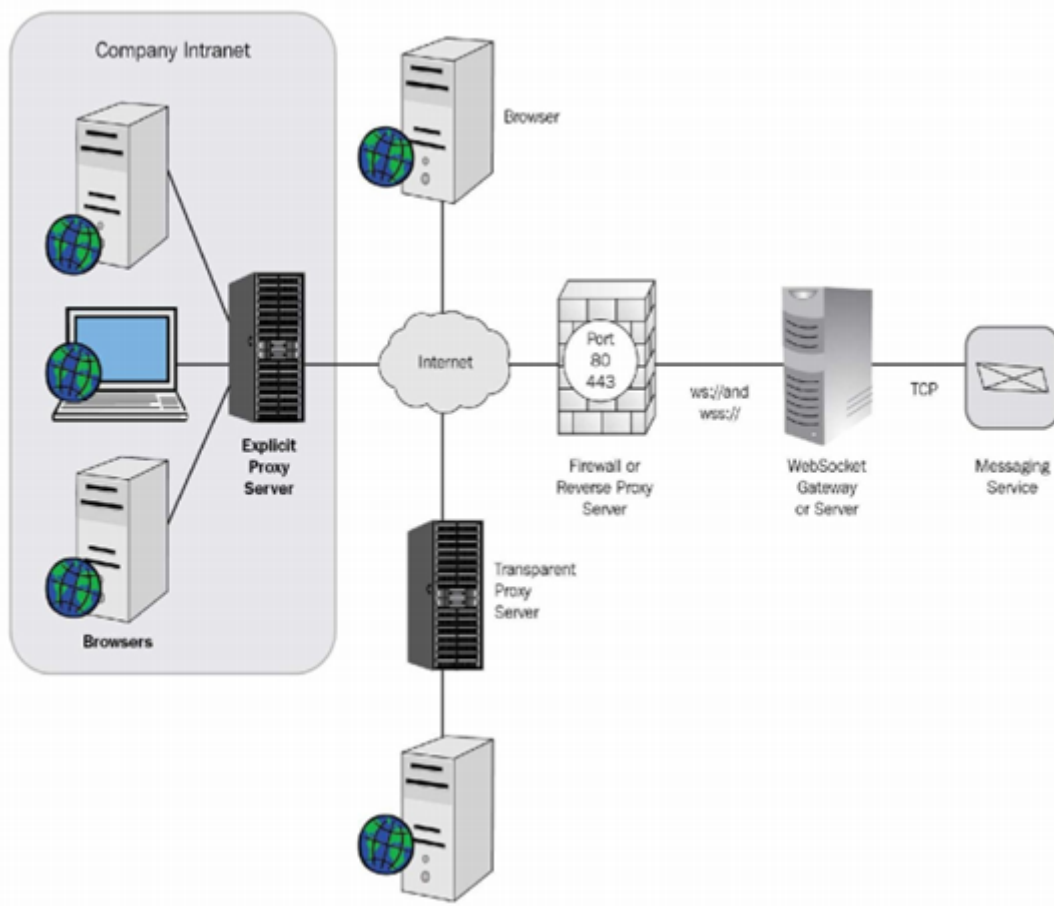
It is a server or a computer that provides indirect access (network connections) to the other network services. When a client requires a connection with the network, the client sends a request and the proxy server serves the requirement from the cache.

There are four different types of proxy servers:

- Transparent proxy
- Anonymous proxy
- Distorting proxy
- High-anonymity proxy

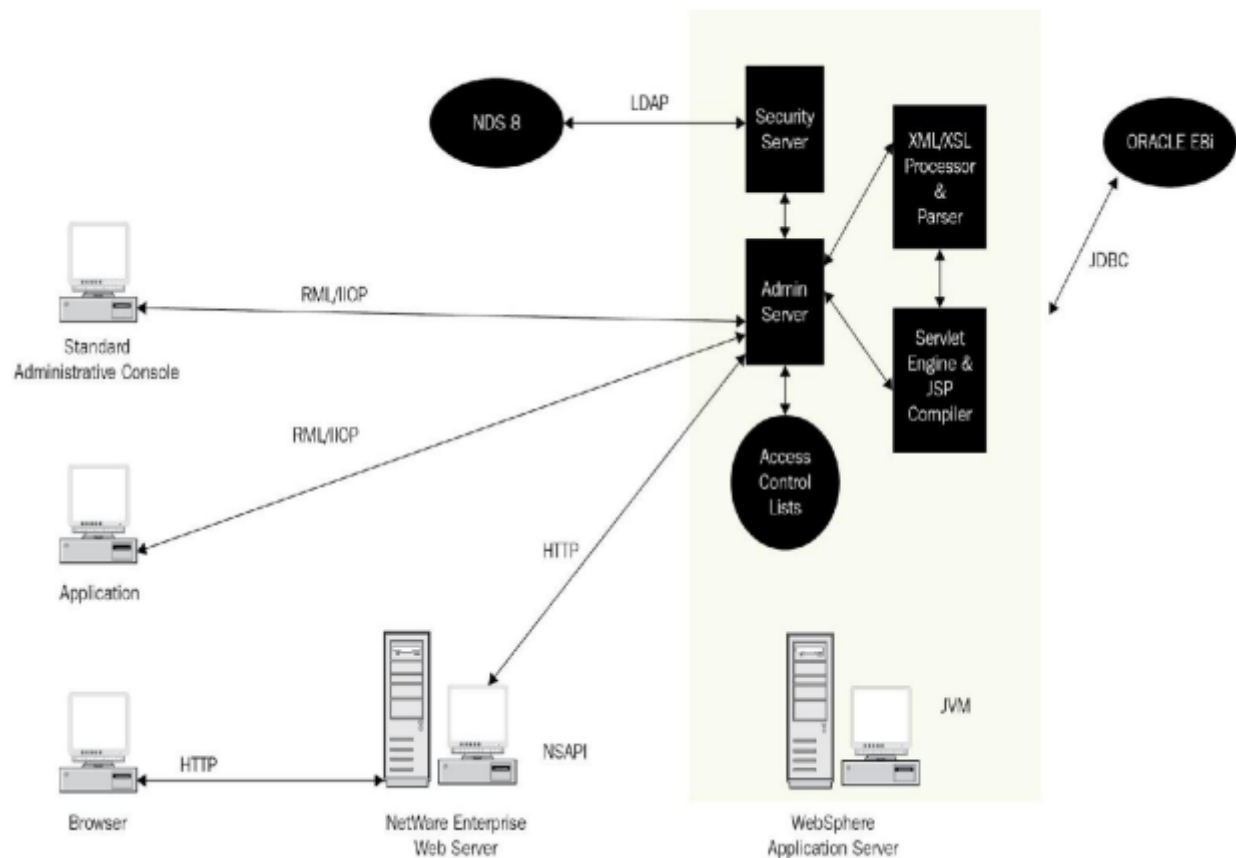
The following graphic displays the appropriate placement of the proxy server:





4. Application Server

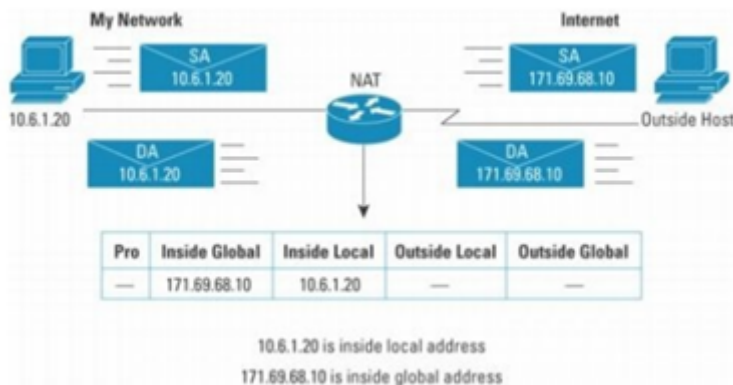
It is a server that provides an environment for arranging and running custom, server-based business applications that can be built and deployed with software applications such as Microsoft .NET Framework 3.0:



5. Network Address Translation

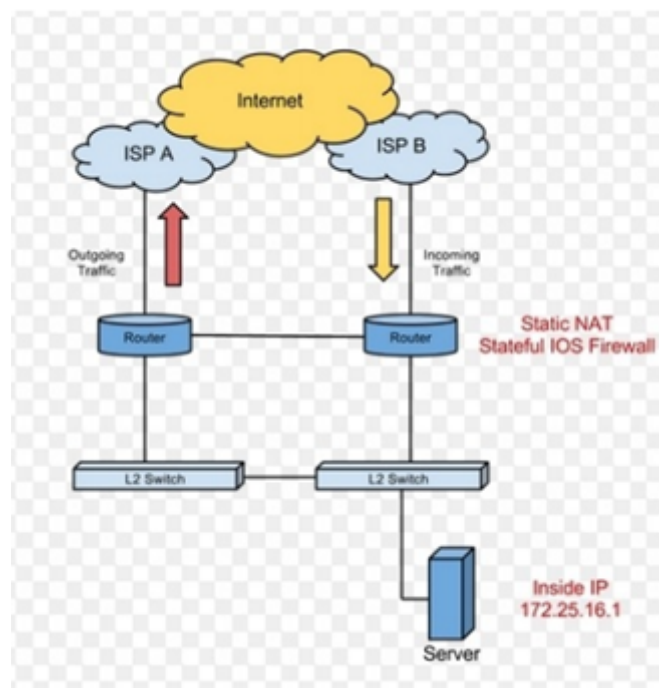
It is a translation method used inside a network with a dissimilar IP address known within another network.

Network Address Translation (NAT) can be performed on a router and it is often called a **corporate firewall**. The Cisco version of NAT enables an administrator to create tables:



6. Stateful Inspection

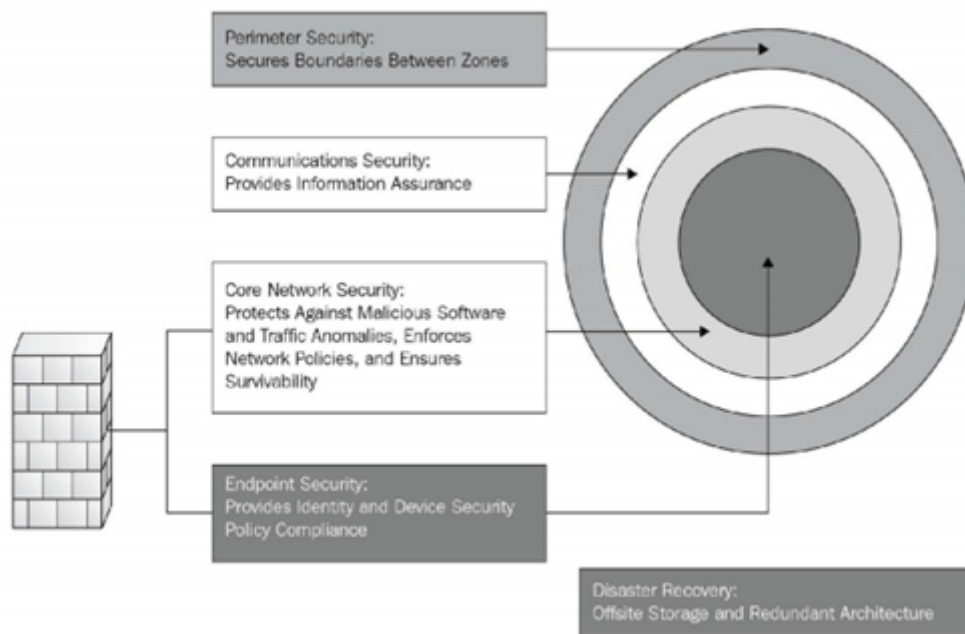
It is also known as dynamic packet filtering. It screens the status of active connections and uses this information to regulate which network packets to permit through the firewall:



FIREWALLS IN A LAYERED DEFENSE STRATEGY

In a layered defense strategy, firewalls provide perimeter security for the entire network and for internal network segments in the core. They can be used on separate VLAN segments. They can be used to separate the internal networks, separating one segment from the rest of the segments:





Several firewalls are used with several layers incorporated in them. Let's understand this process.

When the traffic flows in from an untrusted network, it encounters packet filter on the external router. In the next phase, the traffic steps into either a screened host firewall or a bastion host system. Then this system checks whether there are any suspicious packets, if yes, then it would get discarded. If the packet is not rejected then it would go to the interior screening router. After crossing all these checks, the packet travels to the final destination. This multilayer approach is called **DMZ** or a **screened-subnet configuration**.

To build a complete defense in depth:

- Firewalls don't protect from a large number of intrusions that get injected via the hosts in the network
- Firewalls can't trace the rogue modems in the setup
- Firewalls don't have any planned disaster-recovery mechanisms and they are deployed because of the high CPU utilization and hardware failure

Best practices to guide you in 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 uses of the user and, based on the report, assign those services to them. You need to deploy the least-privilege principle to deny all access to perform one's job smoothly.
- **Deny physical access to the firewall:** It is always a good practice to keep any kind of physical access to the firewall controlled or to deny it completely.
- **Allow only necessary protocols:** It's always good to have a prepared list of protocols that should be allowed and ones that need to be blocked.



- **Use logs and alerts:** You must have a logging strategy that projects the level and type of logging, and you need be sure to monitor all those logs on a regular basis.
- **Segment security zone:** Firewalls are used to protect the internal system from internal misuse and to protect public servers from being accessed by external security threats from the internet.
- **Do not use the firewall as a server:** Firewalls 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 the important ones that need to be removed.
- **Never use a firewall as a workstation:** In general, users' systems depend on a lot of client applications, such as Microsoft and Oracle, that can open a gate to viruses, worms, and so on.
- **Set connection limits:** Enforcing connection limits on the Cisco security appliance firewalls can mitigate worms and the like. Default connection limits can be changed in the global settings.
- **Restrict access to firewalls:** Access to firewalls should be highly restricted. Only an administrator should be allowed to log in with strong passwords assigned to them. You can also use OTP cards for better security.
- **Combine firewall technology:** Packet filtering should not be done only for the line of defense. It can be incorporated with some inspections, such as protocol, stateful, or application.
- **Use firewalls as part of a comprehensive security solution:** Firewalls should be used in juxtaposition with other devices to build a full security solution. They should be integrated with other technologies.
- **Maintain the installation:** Software and patches should be kept updated. Update firewall configurations as application requirements change.

◀ Preliminary Activity for Week 15

Jump to...



Analysis, Application, and Exploration for Week 15 ►



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

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

 Preliminary Activity for Week 15

 **Lesson Proper for Week 15**

 Analysis, Application, and Exploration for Week 15

 Generalization for Week 15

 Evaluation for Week 15

 Assignment for Week 15

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



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

