Lesson Proper for Week 5

FIREWALL

is a security device — computer hardware or software — that can help protect your network by filtering traffic and blocking outsiders from gaining unauthorized access to the private data on your computer.

§ A firewall acts as a gatekeeper. It monitors attempts to gain access to your operating system and blocks unwanted traffic or unrecognized sources.

§ A firewall acts as a barrier or filter between your computer and another network such as the internet. It helps to protect your network and information by managing your network traffic. This includes

blocking unsolicited incoming network traffic and validating access by assessing network traffic for anything malicious like hackers and malware.

<u>FIREWALL HISTORY</u>

Firewalls have certainly evolved over the years and become more advanced since the technology first entered the scene. Getting their start as a basic packet-filtering system in the late 1980's, firewalls monitored packets sent between computers. They now offer more advanced protection and technology, as highlighted in this timeline.

v In late 1980, first generation firewalls developed as attacks on personal computers drove anti-virus products.

v In mid-1990, internet attacks on networks led to the advent of the second generation firewall; the first stateful inspection firewall was introduced in 1993.

v In early 2000, third generation firewalls addressed vulnerability exploits at the application layer, leading to Intrusion Prevention Systems Products (IPS).

v In 2010, increases in targeted attacks instigated anti-bot and sandboxing products.

v In 2017, larger scale attacks drove even more advanced protection.

How does a firewall work?

To start, a firewalled system analyzes network traffic based on rules. A firewall only welcomes those incoming connections that it has been configured to accept. It does this by allowing or blocking specific data packets — units of communication you send over digital networks — based on pre-established security rules.

A firewall works like a traffic guard at your computer's entry point, or port. Only trusted sources, or IP addresses, are allowed in. IP addresses are important because they identify a computer or source, just like your postal address identifies where you live.

BASIC PURPOSE OF A FIREWALL

Basically, a firewall does three things to protect your network:

- It blocks incoming data that might contain a hacker attack.

- It hides information about the network by making it seem that all outgoing traffic originates from the firewall rather than the network. This is called Network Address Translation (NAT).

- It screens outgoing traffic to limit Internet use and/or access to remote sites.

FIREWALL SCREENING LEVELS

A firewall can screen both incoming and outgoing traffic. Because incoming traffic poses a greater threat to the network, it's usually screened more closely than outgoing traffic.

When you are looking at firewall hardware or software products, you'll probably hear about three types of screening that firewalls perform:

- Screening that blocks any incoming data not specifically ordered by a user on the network

- Screening by the address of the sender

- Screening by the contents of the communication

HARWARE AND SOFTWARE FIREWALLS

Firewalls can be either hardware or software. In addition to limiting access to a protected computer and network, a firewall can log all traffic coming into or leaving a network, and manage remote access to a private network through secure authentication certificates and logins.

Hardware firewalls: These firewalls are released either as standalone products for corporate use, or more often, as a built-in component of a router or other networking device. They are considered an essential part of any traditional security system and network configuration. Hardware firewalls will almost always come with a minimum of four network ports that allow connections to multiple systems. For larger networks, a more expansive networking firewall solution is available.

Software firewalls: These are installed on a computer, or provided by an OS or network device manufacturer. They can be customized, and provide a smaller level of control over functions and protection features. A software firewall can protect a system from standard control and access attempts, but have trouble with more sophisticated network breaches.

TYPES OF FIREWALL

There are a number of major firewall types that prevent harmful information from passing through the network:

1. Application-layer Firewalls: This is a hardware appliance, software filter, or server plug-in. It layers security mechanisms on top of defined applications, such as FTP servers, and defines rules for HTTP connections. These rules are built for each application, to help identify and block attacks to a network.

2. Packet Filtering Firewalls: This filter examines every packet that passes through the network – and then accepts or denies it as defined by rules set by the user. Packet filtering can be very helpful, but it can be challenging to properly configure.

3. Circuit-level Firewalls: This firewall type applies a variety of security mechanisms once a UDP or TCP connection has been made. Once the connection is established, packets are exchanged directly between hosts without further oversight or filtering.

4. Proxy Server Firewalls: This version will check all messages that enter or leave a network, and then hide the real network addresses from any external inspection.

5. Next Generation Firewalls (NGFW): These work by filtering traffic moving through a network – the filtering is determined by the applications or traffic types and the ports they are assigned to. These features comprise a blend of a standard firewall with additional functionality, to help with greater, more self-sufficient network inspection.

6. Stateful Firewalls: Sometimes referred to as third generation firewall technology, stateful filtering accomplishes two things: traffic classification based on the destination port, and packet tracking of every interaction between internal connections. These newer technologies increase usability and assist in expanding access control granularity

– interactions are no longer defined by port and protocol. A packet's history in the state table is also measured.

7. Virtual firewalls: A virtual firewall is an appliance used in a cloud-based system, both private and public. This type of firewall is used to assess and manage internet traffic over both physical and virtual networks.

8. Network address translation (NAT) firewalls: A NAT firewall is able to assess internet traffic and block unsolicited communications. In other words, it only accepts inbound web traffic if a device on your private network solicited it.

All of these network firewall types are useful for power users, and many firewalls will allow for two or more of these techniques to be used in tandem with one another.

◀ Preliminary Activity for Week 5

Jump to...

Analysis, Application, and Exploration for Week 5 ▶

Navigation

Home
Dashboard
Site pages
My courses
Capstone Project 1
Multimedia
Network Attacks: Detection, Analysis & Counter...
Participants
General
03 Internal Vulnerability Scanning
04 Open Source Custom Router Firmware
05 Firewalls
Preliminary Activity for Week 5
Lesson Proper for Week 5
Analysis, Application, and Exploration for Week 5
Generalization for Week 5
Evaluation for Week 5
Assignment for Week 5
Ojt/Practicum 1
Social And Professional Issues
System Integration And Architecture 2
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.

Activities

- Assignments
- Forums
- Quizzes
- Resources

Bestlink College of the Philippines
College Department

Powered byeLearning Commons