BBM 465

INFORMATION SECURITY LABORATORY | Assignment 4

Ip Tables/Firewall

Group Id:50

**What is Ip Tables?**

iptables has defined a chain for the packets coming to the server where the source code is decoded. These chains are called "INPUT, OUTPUT, and FORWARD. Iptables allow you to add rules to these chains and take certain actions if the inspected package follows one of these rules. The package leaves the chain with the first rule it matches in a chain. When the package is matched, it either jumps to another zinc or by the user. DROP or ACCEPT is obtained.

Don't mess with any rule in a packet chain, the default action of that chain to the packet. the default action can be ACCEPT or DROP. For example, if a server whose default action is DROP and only TCP - 22 port is allowed is TCP - 80, ie HTTP request, a DROP action will be applied by the kernel to the packet that does not match any rules in the INPUT chain. In systems where security is at the forefront, the default action is DROP with the default DROP concept, and it is returned with rules ending with ACCEPT.

In systems where usability is prioritized, the default ACCEPT action is determined and blocked with the default ACCEPT concept.

**What is Firewall?**

A firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules.  
 Firewalls have been a first line of defence in network security for over 25 years. They establish a barrier between secured and controlled internal networks that can be trusted and untrusted outside networks, such as the Internet. A firewall can be hardware, software, or both.

**Types of Firewalls;**  
 **Proxy firewall**

An early type of firewall device, a proxy firewall serves as the gateway from one network to another for a specific application. Proxy servers can provide additional functionality such as content caching and security by preventing direct connections from outside the network. However, this also may impact throughput capabilities and the applications they can support.

**Stateful inspection firewall**

Now thought of as a “traditional” firewall, a stateful inspection firewall allows or blocks traffic based on state, port, and protocol. It monitors all activity from the opening of a connection until it is closed. Filtering decisions are made based on both administrator-defined rules as well as context, which refers to using information from previous connections and packets belonging to the same connection.

**Unified threat management (UTM) firewall**

A UTM device typically combines, in a loosely coupled way, the functions of a stateful inspection firewall with intrusion prevention and antivirus. It may also include additional services and often cloud management. UTMs focus on simplicity and ease of use.

**Virtual firewall**

A virtual firewall is typically deployed as a virtual appliance in a private cloud (VMware ESXi, Microsoft Hyper-V, KVM) or public cloud (AWS, Azure, Google, Oracle) to monitor and secure traffic across physical and virtual networks. A virtual firewall is often a key component in software-defined networks (SDN).

**Ip Tables Common Rules**

* **-A**: Append this rule to a rule chain. Valid chains for what we're doing are INPUT, FORWARD and OUTPUT, but we mostly deal with INPUT in this tutorial, which affects only incoming traffic.
* **-L**: List the current filter rules.
* **-m conntrack**: Allow filter rules to match based on connection state. Permits the use of the --ctstate option.
* **--ctstate**: Define the list of states for the rule to match on. Valid states are:
* **NEW**: The connection has not yet been seen.
* **RELATED**: The connection is new but is related to another connection already permitted.
* **ESTABLISHED**: The connection is already established.
* **INVALID**: The traffic could not be identified for some reason.
* **-m limit**: Require the rule to match only a limited number of times. Allows the use of the --limit option. Useful for limiting logging rules.
* **--limit**: The maximum matching rate, given as a number followed by "/second", "/minute", "/hour", or "/day" depending on how often you want the rule to match. If this option is not used and -m limit is used, the default is "3/hour".
* **-p**: The connection protocol used.
* **--dport**: The destination port(s) required for this rule. A single port may be given, or a range may be given as start: end, which will match all ports from start to end, inclusive.
* **-j**: Jump to the specified target. By default, iptables allows four targets:
* **ACCEPT:** Accept the packet and stop processing rules in this chain.
* **REJECT**: Reject the packet and notify the sender that we did so and stop processing rules in this chain.
* **DROP**: Silently ignore the packet and stop processing rules in this chain.
* **LOG**: Log the packet and continue processing more rules in this chain. Allows the use of the --log-prefix and --log-level options.
* **--log-prefix**: When logging, put this text before the log message. Use double quotes around the text to use.
* **--log-level**: Log using the specified syslog level. 7 is a good choice unless you specifically need something else.
* **-i**: Only match if the packet is coming in on the specified interface.
* **-I**: Inserts a rule. Takes two options, the chain to insert the rule into, and the rule number it should be.
* **-I INPUT 5:** would insert the rule into the INPUT chain and make it the 5th rule in the list.
* **-v**: Display more information in the output. Useful for if you have rules that look similar without using -v.
* **-s –source**: address[/mask] source specification
* **-d –destination:** address[/mask] destination specification
* **-o --out-interface**: output name[+] network interface name ([+] for wildcard)

**Explain Our Solutions**

* **Question 1**For first question, we firstly wrote flush rule which will reset iptables configs, then we wrote default policy as DROP, that rule will drop any package does not match with a rule. After that we allow loopback connection on Firewall. After that rule, we allow established and related incoming and ESTABLISHED outgoing connections on firewall. Lan1(Computer Engineering) Packages Sending and Lan2(Electronic Engineering) Packages Sending rules wrote in order. Finally, we write the rule that save new iptables rules.
* **Question 2**For first question, we firstly wrote flush rule which will reset iptables configs, then we wrote default policy as DROP, that rule will drop any package does not match with a rule. After that we allow loopback connection on Firewall. After that rule, we allow established and related incoming and ESTABLISHED outgoing connections on firewall. Lan1, Lan2, Lan3 Packages Sending Twitter via HTTP/HTTPS and Lan1, Lan2, Lan3 Packages Sending Facebook via HTTP/HTTPS rules wrote in order. Finally, we write the rule that save new iptables rules.
* **Question 3**For first question, we firstly wrote flush rule which will reset iptables configs, then we wrote default policy as DROP, that rule will drop any package does not match with a rule. After that we allow loopback connection on Firewall. After that rule, we allow established and related incoming and ESTABLISHED outgoing connections on firewall. Web Server Packages Sending HTTP/HTTPS Config for accepting, Web Server Packages Sending IMAP/SMTP/POP3 Config for rejecting, E-Mail Server Packages Sending SMTP Config for accepting, E-Mail Server Packages Sending HTTP/HTTPS/IMAP/POP3 Config for rejecting rules wrote in an order. Finally, we write the rule that save new iptables rules.
* **Question 4**For first question, we firstly wrote flush rule which will reset iptables configs, then we wrote default policy as DROP, that rule will drop any package does not match with a rule. After that we allow loopback connection on Firewall. After that rule, we allow established and related incoming and ESTABLISHED outgoing connections on firewall. E-Mail Server Packages Sending IMAP/POP3 Config for Lan1, E-Mail Server Packages Sending IMAP/POP3 Config for Lan2, E-Mail Server Packages Sending IMAP/POP3 Config for Lan3 rules wrote for accept. Finally, we write the rule that save new iptables rules.
* **Question 5**For first question, we firstly wrote flush rule which will reset iptables configs, then we wrote default policy as DROP, that rule will drop any package does not match with a rule. After that we allow loopback connection on Firewall. After that rule, we allow established and related incoming and ESTABLISHED outgoing connections on firewall. Remote Computer Ping Sending Config For Lan1, Remote Computer Ping Sending Config For Lan2, Remote Computer Ping Sending Config For Lan3 are wrote in for accept ping. Finally, we write the rule that save new iptables rules.
* **Question 6**For first question, we firstly wrote flush rule which will reset iptables configs, then we wrote default policy as DROP, that rule will drop any package does not match with a rule. After that we allow loopback connection on Firewall. After that rule, we allow established and related incoming and ESTABLISHED outgoing connections on firewall. Firewall HTTPS Config For All Connections rules wrote for rejecting. Finally, we write the rule that save new iptables rules.

**References**

* <https://phoenixnap.com/kb/iptables-tutorial-linux-firewall>
* <https://medium.com/@gokhansengun/iptables-nedir-nas%C4%B1l-ve-nerelerde-kullan%C4%B1l%C4%B1r-1-7c081a9512c0>
* <https://www.youtube.com/watch?v=XKfhOQWrUVw&ab_channel=ComputerandNetworkSecurity>
* <https://www.tecmint.com/linux-iptables-firewall-rules-examples-commands/#:~:text=Iptables%20is%20a%20Linux%20command,in%20or%20user%20defined%20rules>.
* <https://www.digitalocean.com/community/tutorials/iptables-essentials-common-firewall-rules-and-commands>
* <https://www.thegeekstuff.com/2011/06/iptables-rules-examples/>
* <https://www.cyberciti.biz/tips/linux-iptables-examples.html>