FIREWALL RULES

Firewalls operate by examining a data packet and performing a comparison with some predetermined logical rules. The logic is based on a set of guidelines programmed in by a firewall administrator, or created dynamically and based on outgoing requests for information. This logical set is most commonly referred to as firewall rules, rule base, or firewall logic.

Most firewalls use packet header information to determine whether a specific packet should be allowed to pass through or should be dropped. In order to better understand more complex rules, it is important to be able to create simple rules and understand how they interact.

For the purpose of this discussion, assume a network configuration as illustrated in Fig 6-14, with an internal and an external filtering firewall. In the exercise, the rules for both firewalls will be discussed, and a recap at the end of the exercise will show the complete rule sets for each filtering firewall.

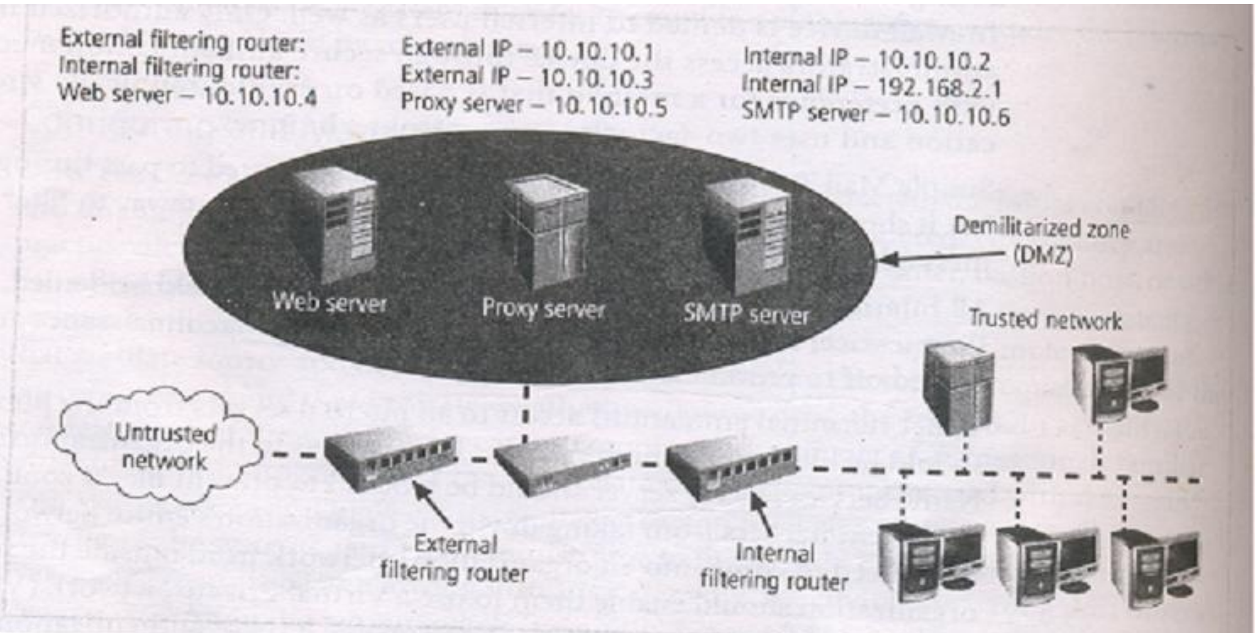

FIGURE 6-14 Example Network Configuration

Some firewalls can filter packets by the name of a particular protocol as opposed to the protocol‘s usual port numbers. For instance, Telnet protocol packets usually go to TCP port 23, but can sometimes be directed to another much higher port number in an attempt to conceal the activity. The System or well-known ports are those from 0 through 1023, User or registered ports are those from 1024 through 49151, and Dynamic or Private Ports are those from 49152 through 65535.

The following example uses the port numbers associated with several well-known protocols to build a rule base. The port numbers to be used are listed in Table 6-5. Note that this is not an exhaustive list.

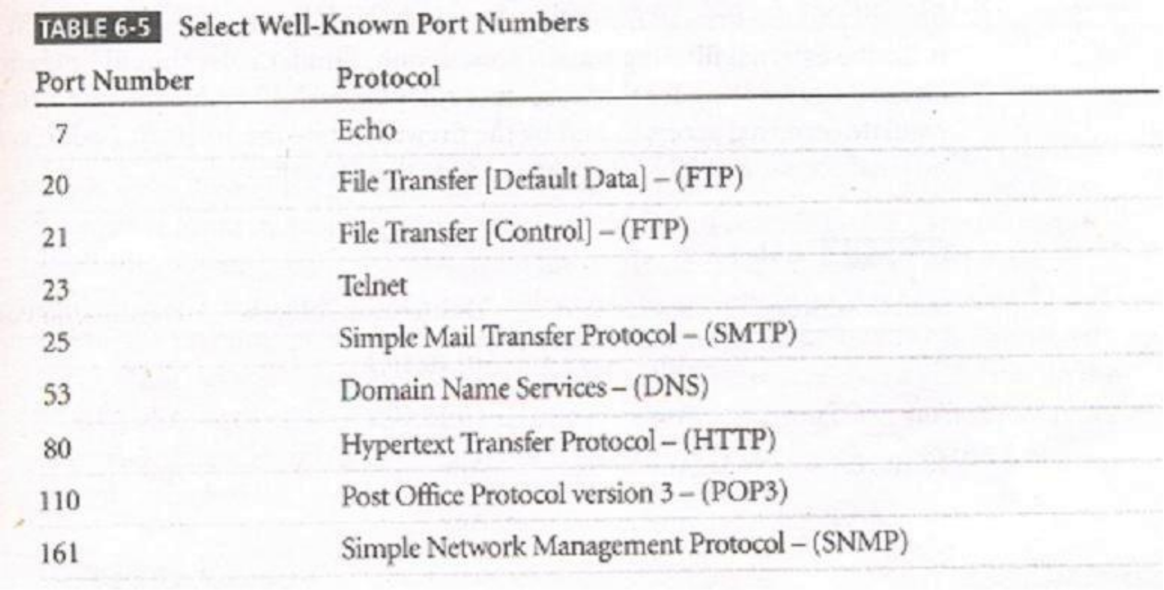

TABLE 6-5 Select Well-Known Port Numbers

Port Number	Protocol
7	Echo
20	File Transfer [Default Data] – (FTP)
21	File Transfer [Control] – (FTP)
23	Telnet
25	Simple Mail Transfer Protocol – (SMTP)
53	Domain Name Services – (DNS)
80	Hypertext Transfer Protocol – (HTTP)
110	Post Office Protocol version 3 – (POP3)
161	Simple Network Management Protocol – (SNMP)

Rule Set-1: Responses to internal requests are allowed. In most firewall implementations, it is desirable to allow a response to an internal request for information. In dynamic or stateful firewalls, this is most easily accomplished by matching the incoming traffic to an outgoing request in a state table. In simple packet filtering, this can be accomplished with the following rule for the External Filtering Router. (Note that the network address for the destination ends with .0; some firewalls use a notation of .X instead.)

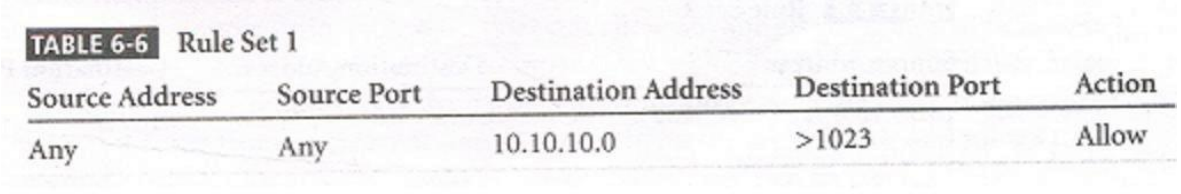

TABLE 6-6 Rule Set 1

Source Address	Source Port	Destination Address	Destination Port	Action
Any	Any	10.10.10.0	>1023	Allow

From Table 6-6, you can see that this rule states that any incoming packet (with any source address and from any source port) that is destined for the internal network (whose destination address is 10.10.10.0) and for a destination port greater than 1023 (that is , any port out of the number range for the well-known ports) is allowed to enter. Why allow all such packets? While outgoing communications request information from a specific port (i.e a port 80 request for a Web page), the response is assigned a number outside the well-known port range. If multiple browser windows are open at the same time, each window can request a packet from a Web site, and the response is directed to a specific destination port, allowing the browser and Web server to keep each conversation separate. While this rule is sufficient for the external router (firewall), it is dangerous simply to allow any traffic in just because it is destined to a high port range. A better solution is to have the internal firewall router use state tables that track connections and prevent dangerous packets from entering this upper port range.

Rule set-2: The firewall device is never accessible directly from the public network. If hackers can directly access the firewall, they may be able to modify or delete rules and allow unwanted traffic through. For the same reason, the firewall itself should never be allowed to access other network devices directly. If hackers compromise the firewall and then use its permissions to access other servers or clients, they may cause additional damage or mischief. The rules shown in Table 6-7 prohibit anyone from directly accessing the firewall and the firewall from directly accessing any other devices. Note that this example is for the external filtering router/firewall only. Similar rules should be crafted for the internal router. Why are there separate rules for each IP addresses? The 10.10.10.1 address regulates external access to and by the firewall, while the 10.10.10.2 address regulates internal access. Not all hackers are outside the firewall!

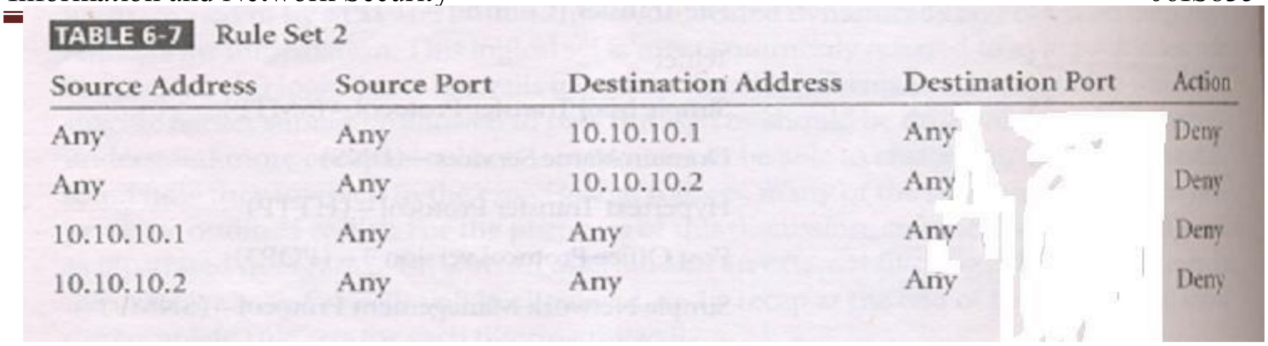

TABLE 6-7 Rule Set 2

Source Address	Source Port	Destination Address	Destination Port	Action
Any	Any	10.10.10.1	Any	Deny
Any	Any	10.10.10.2	Any	Deny
10.10.10.1	Any	Any	Any	Deny
10.10.10.2	Any	Any	Any	Deny

Rule set-3: All traffic from the trusted network is allowed out. As a general rule it is wise not to restrict outgoing traffic, unless a separate router is configured to handle this traffic. Assuming most of the potentially dangerous traffic is inbound, screening outgoing traffic is just more work for the firewalls. This level of trust is fine for most organizations. If the organization wants control over outbound traffic, it should use a separate router. The rule shown in Table 6-8 allows internal communications out.

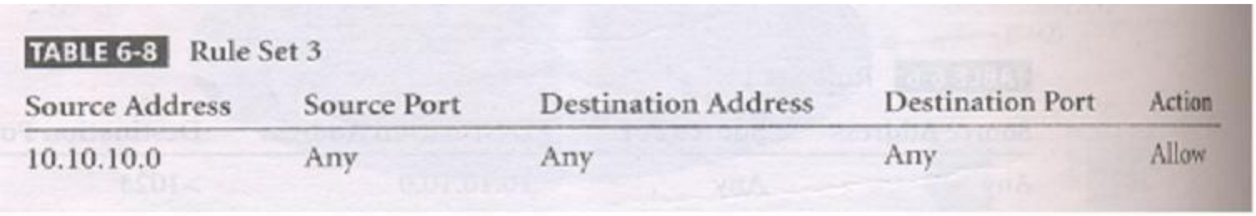

TABLE 6-8 Rule Set 3

Source Address	Source Port	Destination Address	Destination Port	Action
10.10.10.0	Any	Any	Any	Allow

Why should rule set-3 come after rule set-1 and 2? It makes sense to allow the rules that unambiguously impact the most traffic to be earlier in the list. The more rules a firewall must process to find one that applies to the current packet, the slower the firewall will run. Therefore, most widely applicable rules should come first since the first rule that applies to any given packet will be applied.

Rule set-4: The rule set for the Simple mail Transport Protocol (SMTP) data is shown in Table 6-9. As shown, the packets governed by this rule are allowed to pass through the firewall, but are all routed to a well-configured SMTP gateway. It is important that e-mail traffic reach your e-mail server, and only your e-mail server. Some hackers try to disguise dangerous packets as e-mail traffic to fool a firewall. If such packets can reach only the e-mail server, and the e-mail server has been properly configured, the rest of the network ought to be safe.

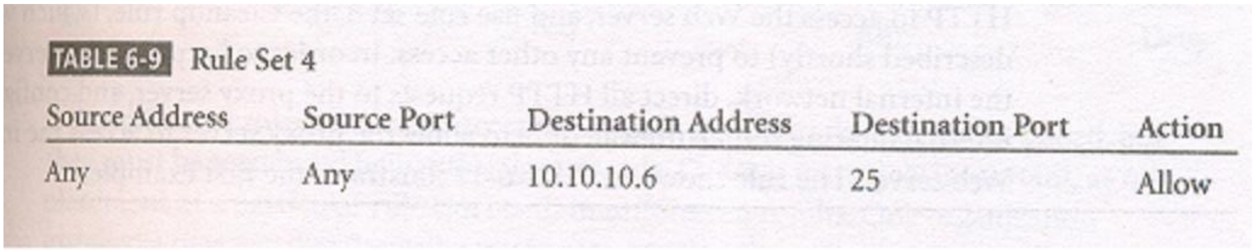

TABLE 6-9 Rule Set 4

Source Address	Source Port	Destination Address	Destination Port	Action
Any	Any	10.10.10.6	25	Allow

Rule set 5: All Internet Control Message Protocol (ICMP) data should be denied. Pings, formally known as ICMP echo requests, are used by internal systems administrators to ensure that clients and servers can reach and communicate. There is virtually no legitimate use for ICMP outside the network, except to test the perimeter routers. ICPM uses port 7 to request a response to a query (eg ―Are you there?”) and can be the first indicator of a malicious attack. It‘s best to make all directly connected networking devices ―black holes” to external probes. Traceroute uses a variation on the ICMP Echo requests, so restricting this one port provides protection against two types of probes. Allowing internal users to use ICMP requires configuring two rules, as shown in Table 6-10.

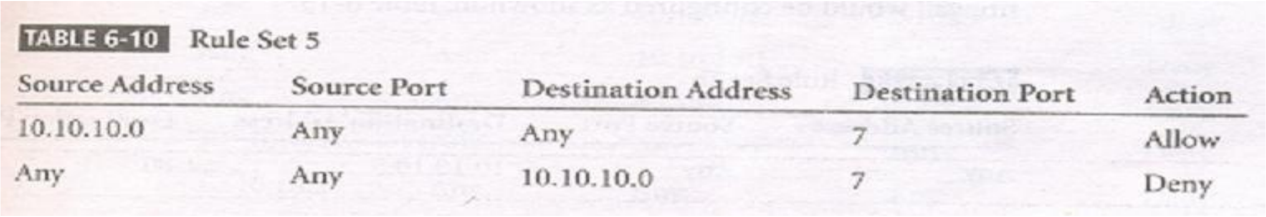

TABLE 6-10 Rule Set 5

Source Address	Source Port	Destination Address	Destination Port	Action
10.10.10.0	Any	Any	7	Allow
Any	Any	10.10.10.0	7	Deny

The first of these two rules allows internal administrators (and users) to use Ping. Note that this rule is unnecessary if internal permissions rules like those in rule set 2 is used. The second rule in Table 6-10 does not allow anyone else to use Ping. Remember that rules are processed in order. If an internal user needs to Ping an internal or external address, the firewall allows the packet and stops processing the rules. If the request does not come from an internal source, then it bypasses the first rule and moves to the second.

Rule set 6: Telnet (Terminal emulation) access to all internal servers from the public networks should be blocked. Though not used much in Windows environments, Telnet is still useful to systems administrators on Unix/Linux systems. But the presence of external requests for Telnet services can indicate a potential attack. Allowing internal use of Telnet requires the same type of initial permission rule you use with Ping. See Table 6-11. Note that this rule is unnecessary if internal permissions rules like those in rule set 2 are used.

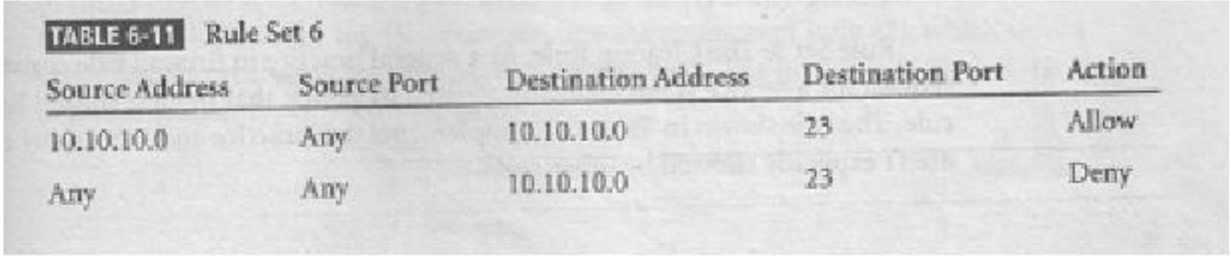

TABLE 6-11 Rule Set 6

Source Address	Source Port	Destination Address	Destination Port	Action
10.10.10.0	Any	10.10.10.0	23	Allow
Any	Any	10.10.10.0	23	Deny

Rule set 7: when Web services are offered outside the firewall, HTTP traffic should be denied from reaching the internal networks through the use of some form of proxy access or DMZ architecture. With a Web server in the DMZ you simply allow HTTP to access the Web server, and use rule set 8, the Clean Up rule to prevent any other access. In order to keep the Web server inside the internal network, direct all HTTP requests to the proxy server, and configure the internal filtering router/firewall only to allow the proxy server to access the internal Web server. The rule shown in Table 6-12 illustrates the first example.

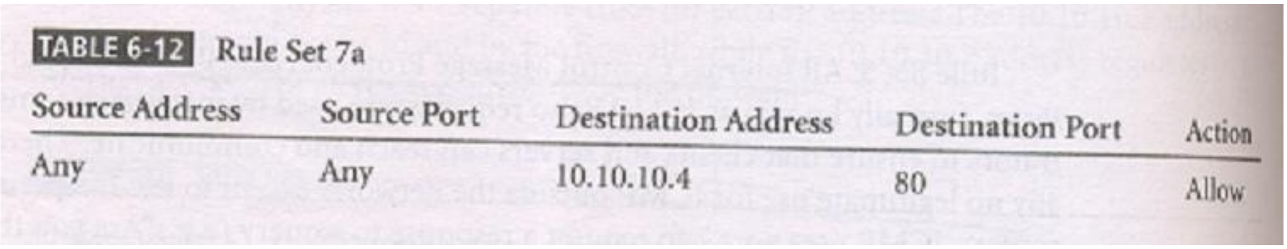

TABLE 6-12 Rule Set 7a

Source Address	Source Port	Destination Address	Destination Port	Action
Any	Any	10.10.10.4	80	Allow

This rule accomplishes two things: It allows HTTP traffic to reach the Web server, and it prevents non-HTTP traffic from reaching the Web server. It does the latter through the Clean Up rule (Rule 8). If someone tries to access theWeb server with non-HTTP traffic (other than port 80), then the firewall skips this rule and goes to the next.

Proxy server rules allow an organization to restrict all access to a device. The external firewall would be configured as shown in Table 6-13.

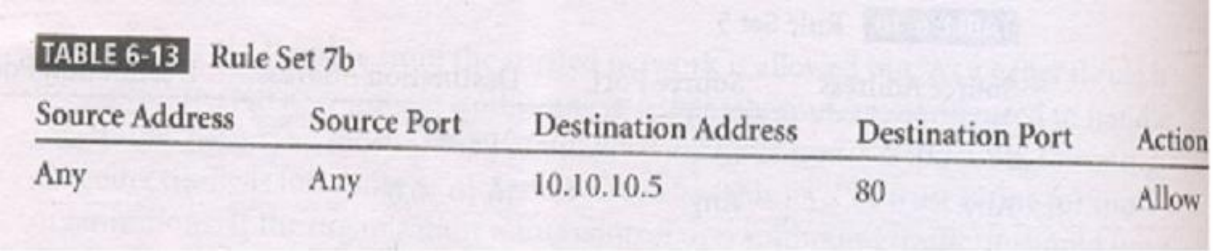

TABLE 6-13 Rule Set 7b

Source Address	Source Port	Destination Address	Destination Port	Action
Any	Any	10.10.10.5	80	Allow

The effective use of as proxy server of course requires the DNS entries to be configured as if the proxy server were the Web server. The proxy server would then be configured to repackage any HTTP request packets into a new packet and retransmit to the Web server inside the firewall. Allowing for the retransmission of the repackaged request requires the rule shown in Table 6-14 to enable the proxy server at 10.10.10.5 to send to the internal router, presuming the IP address for the internal Web server is 192.168.2.4

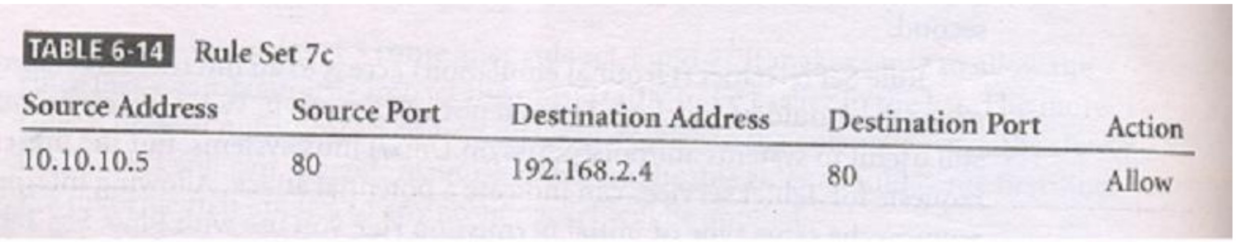

TABLE 6-14 Rule Set 7c

Source Address	Source Port	Destination Address	Destination Port	Action
10.10.10.5	80	192.168.2.4	80	Allow

The restriction on the source address then prevents anyone else from accessing the Web server from outside the internal filtering router/firewall.

Rule set 8: The Clean up rule: As a general practice in firewall rule construction, if a request for a service is not explicitly allowed by policy, that request should be denied by a rule. The rule shown in Table 6-15 implements this practice and blocks any requests that aren‘t explicitly allowed by other rules.

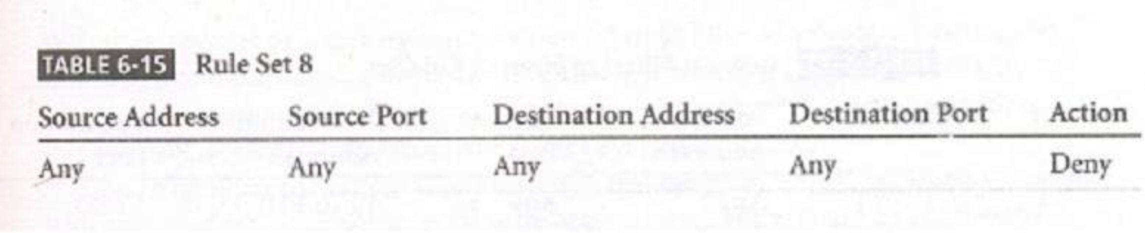

TABLE 6-15 Rule Set 8

Source Address	Source Port	Destination Address	Destination Port	Action
Any	Any	Any	Any	Deny

Additional rules restricting access to specific servers or devices can be added, but they must be sequenced before the clean up rule. Order is extremely important, as misplacement of a particular rule can result in unforeseen results.

Tables 6-16 and 6-17 show the rule sets, in their proper sequences, for both external and internal firewalls.

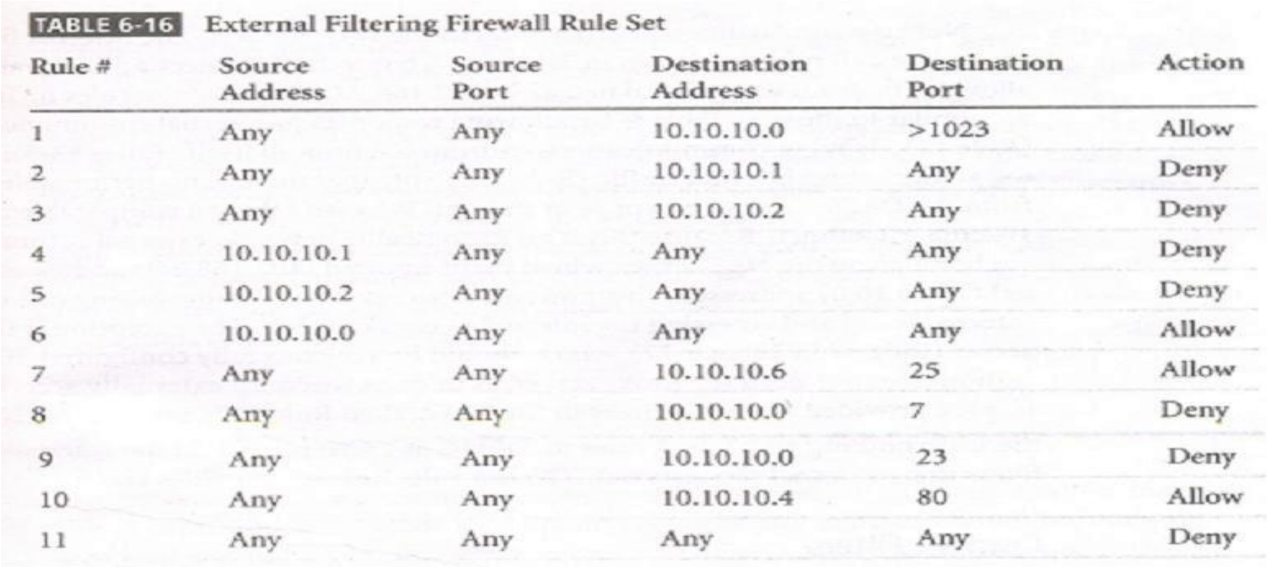

TABLE 6-16 External Filtering Firewall Rule Set

Rule #	Source Address	Source Port	Destination Address	Destination Port	Action
1	Any	Any	10.10.10.0	>1023	Allow
2	Any	Any	10.10.10.1	Any	Deny
3	Any	Any	10.10.10.2	Any	Deny
4	10.10.10.1	Any	Any	Any	Deny
5	10.10.10.2	Any	Any	Any	Deny
6	10.10.10.0	Any	Any	Any	Allow
7	Any	Any	10.10.10.6	25	Allow
8	Any	Any	10.10.10.0	7	Deny
9	Any	Any	10.10.10.0	23	Deny
10	Any	Any	10.10.10.4	80	Allow
11	Any	Any	Any	Any	Deny

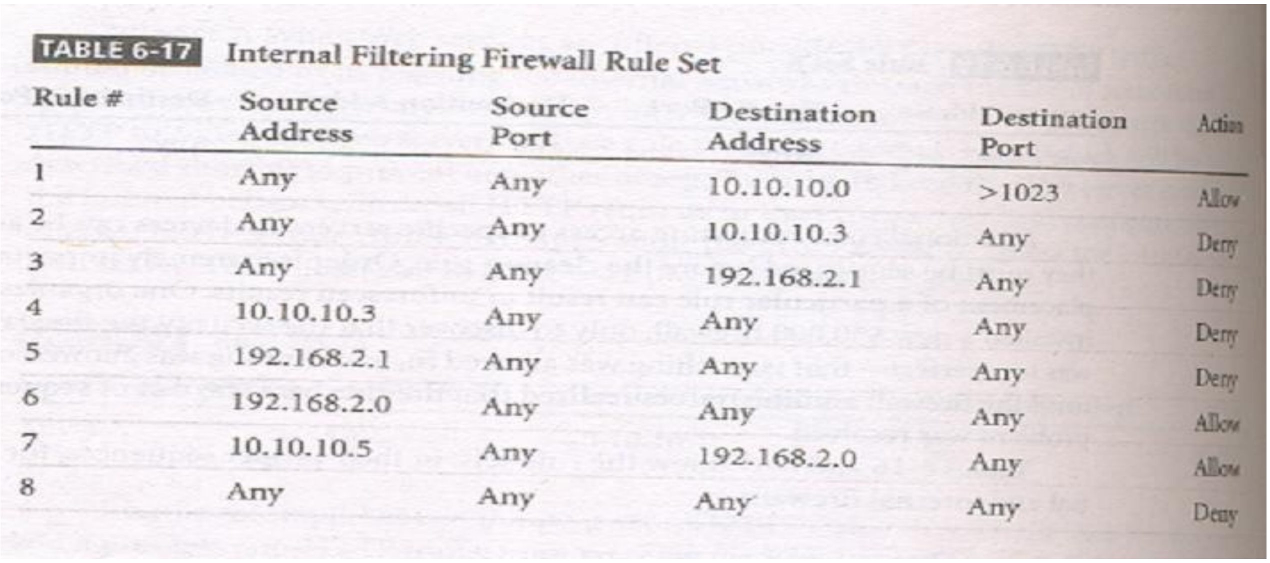

TABLE 6-17 Internal Filtering Firewall Rule Set

Rule #	Source Address	Source Port	Destination Address	Destination Port	Action
1	Any	Any	10.10.10.0	>1023	Allow
2	Any	Any	10.10.10.3	Any	Deny
3	Any	Any	192.168.2.1	Any	Deny
4	10.10.10.3	Any	Any	Any	Deny
5	192.168.2.1	Any	Any	Any	Deny
6	192.168.2.0	Any	Any	Any	Allow
7	10.10.10.5	Any	192.168.2.0	Any	Allow
8	Any	Any	Any	Any	Deny

Note that the rule allowing responses to internal communications comes first (appearing in Table 6-16 as Rule #1), followed by the four rules prohibiting direct communications to or from the firewall (Rules #2-5 in Table 6-16). After this comes the rule stating that all outgoing internal communications are allowed, followed by the rules governing access to the SMTP server, and denial of Ping, Telnet access, and access to the HTTP server. If heavy traffic to the HTTP server is expected, move the HTTP server rule closer to the top (For example, into the position of Rule #2), which would expedite rule processing for external communications. The final rule in Table 6-16 denies any other types of communications.

Note the similarities and differences in the two rule sets. The internal filtering router/firewall rule set, shown in Table 6-17, has to both protect against traffic to and allow traffic from the internal network (192.168.2.0). Most of the rules in Table 6-17 are similar to those in Table 6-16: allowing responses to internal communications (Rule #1); denying communications to/from the firewall itself (rule # 2-5); and allowing all outbound internal traffic (Rule #6). Note that there is no permissible traffic from the DMZ systems, except as in Rule #1.

Why isn‘t there a comparable rule for the 192.168.2.1 subnet? Because this is an unrouteable network, external communications are handled by the NAT server, which maps internal (192.168.2.0) addresses to external (10.10.10.0) addresses. This prevents a hacker from compromising one of the internal boxes and accessing the internal network with it. The exception is the proxy server (Rule #7 in Table 6-17), which should be very carefully configured. If the organization does not need the proxy server, as in cases where all externally accessible services are provided from machines in the DMZ, tehn rule #7 is not needed. Note that there are no Ping and Telnet rules in Table 6-17. This is because the external firewall filters these external requests out. The last rule, rule#8 provides cleanup.

Source : http://elearningatria.files.wordpress.com/2013/10/ise-viii-information-and-network-security-06is835-notes.pdf