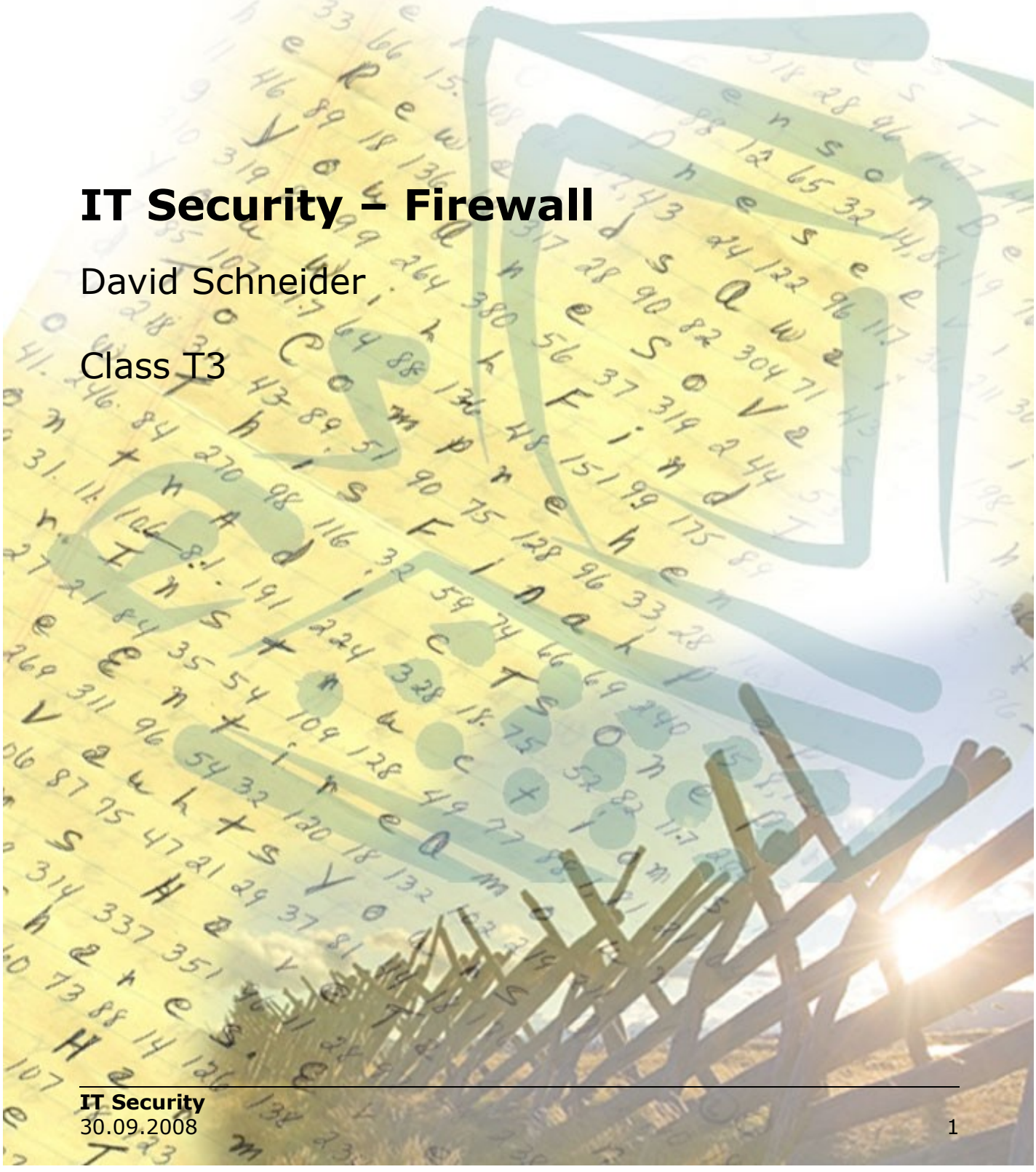
IT Security



IT Security – Firewall

David Schneider

Class T3

Table of content

1 Firewall

A network, specially a corporate network, needs to be secured. This means the the traffic that is allowed to passes from the exterior into the network, and contrariwise, needs to be specified.

Small companies use routers as firewall, larger companies often use perimeter routers before the firewall to provide a better packet inspection which uses also a lot more CPU performance.

The firewall often has tree interfaces to separate the internet, the corporate network and the demilitarized zone. The third contains servers which offers services that are accessible from internet, for example web, file or mail servers or public data bases.

Packet Filtering Firewalls

Packet Filters observe the network traffic on OSI model layer 3 and 4. They are able to deny or permit IP traffic according to source and destination IP addresses or protocol or in the UDP or TCP header by the source or destination port fields.
Cisco Routers do packet filtering with access lists. If sessions like UDP or ICMP needs to be established throw the router, Cisco provides a solution with refexive access-lists.

State full Firewalls

Due to connectionless protocols, unlike TCP, do not provide tracking information, we can't determine if an incoming packet is the response on one of our requests. Therefore does statefull firewalls have to know which packet refers to which session. The firewall just let pass information if the client on the interior of the network has ordered from the exterior system. That means, the firewall can block the traffic even if a session has been established.

The statefull firewall uses for those decision a combination of different fields in the IP and TCP header as destination and source address, protocol field and the TCP flags (SYN, ACK and FIN).

It is also important that the last packet wasn't received to long ago and the session is still established, that the sequence and acknowledgment numbers were increased correctly, and the used ports don't change during the session.

This type of firewalls helps much more to prevent against attacks than usual packet filters.

Proxy Firewalls

Proxy-based firewalls also known as application-layer firewalls check the content of the OSI layer 7. They understand the protocol or service and can figure out if another unwanted service tries to missuse a allowed service.

The content filter allows to deny java applets such as ActiveX or JavaScript elements, block viruses or trojans on websites, filter confident data, block URL's or keywords, deny unwanted application protocoll or check mail transfer for illegal commands.

2 iptables

Show table

```
[root@localhost ~]# iptables -L -n -v -t filter
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
 2161 86504 ACCEPT     all  --  *      *       0.0.0.0/0            0.0.0.0/0           state RELATED,ESTABLISHED
    0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            0.0.0.0/0
 2161  130K ACCEPT     all  --  lo     *       0.0.0.0/0            0.0.0.0/0
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           state NEW tcp dpt:22
  811  134K REJECT     all  --  *      *       0.0.0.0/0            0.0.0.0/0           reject-with icmp-host-prohibited

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 REJECT     all  --  *      *       0.0.0.0/0            0.0.0.0/0           reject-with icmp-host-prohibited

Chain OUTPUT (policy ACCEPT 4333 packets, 219K bytes)
 pkts bytes target     prot opt in     out     source               destination
```

FLUSH table

```
[root@localhost ~]# iptables -F
```

DROP

We choose to drop all the ICMP packets.

```
[root@localhost ~]# iptables -A INPUT -p icmp -j LOG
[root@localhost ~]# iptables -A INPUT -p icmp -j DROP
[root@localhost ~]# iptables -L -n -v -t filter
Chain INPUT (policy ACCEPT 112 packets, 16678 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 LOG        icmp --  *      *       0.0.0.0/0            0.0.0.0/0           LOG flags 0 level 4
    0     0 DROP       icmp --  *      *       0.0.0.0/0            0.0.0.0/0

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 4333 packets, 219K bytes)
 pkts bytes target     prot opt in     out     source               destination
```

We can't ping the destination any more.

```
jerome@LeNotre:~$ ping 160.98.31.6
PING 160.98.31.6 (160.98.31.6) 56(84) bytes of data.
From 160.98.31.6 icmp_seq=1 Destination Port Unreachable
From 160.98.31.6 icmp_seq=2 Destination Port Unreachable
From 160.98.31.6 icmp_seq=3 Destination Port Unreachable
From 160.98.31.6 icmp_seq=4 Destination Port Unreachable
From 160.98.31.6 icmp_seq=5 Destination Port Unreachable
From 160.98.31.6 icmp_seq=6 Destination Port Unreachable
From 160.98.31.6 icmp_seq=7 Destination Port Unreachable
From 160.98.31.6 icmp_seq=8 Destination Port Unreachable
From 160.98.31.6 icmp_seq=9 Destination Port Unreachable
From 160.98.31.6 icmp_seq=10 Destination Port Unreachable
From 160.98.31.6 icmp_seq=11 Destination Port Unreachable

--- 160.98.31.6 ping statistics ---
11 packets transmitted, 0 received, +11 errors, 100% packet loss, time 10000ms
```

REJECT ICMP

Now we changed the policy to reject the ICMP packets.

```
[root@localhost ~]# iptables -F
[root@localhost ~]# iptables -A INPUT -p icmp -j LOG
[root@localhost ~]# iptables -A INPUT -p icmp -j REJECT
[root@localhost ~]# iptables -L -n -v -t filter
Chain INPUT (policy ACCEPT 384 packets, 65367 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 LOG        icmp --  *      *       0.0.0.0/0            0.0.0.0/0           LOG flags 0 level 4
    0     0 REJECT     icmp --  *      *       0.0.0.0/0            0.0.0.0/0           reject-with icmp-port-unreachable

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 4335 packets, 219K bytes)
 pkts bytes target     prot opt in     out     source               destination
```

The packets are now rejected.

```
jerome@LeNotre:~$ ping 160.98.31.6
PING 160.98.31.6 (160.98.31.6) 56(84) bytes of data.
From 160.98.31.6 icmp_seq=1 Destination Net Prohibited
From 160.98.31.6 icmp_seq=2 Destination Net Prohibited
From 160.98.31.6 icmp_seq=3 Destination Net Prohibited
From 160.98.31.6 icmp_seq=4 Destination Net Prohibited
From 160.98.31.6 icmp_seq=5 Destination Net Prohibited
From 160.98.31.6 icmp_seq=6 Destination Net Prohibited
From 160.98.31.6 icmp_seq=7 Destination Net Prohibited
From 160.98.31.6 icmp_seq=8 Destination Net Prohibited
From 160.98.31.6 icmp_seq=9 Destination Net Prohibited

--- 160.98.31.6 ping statistics ---
9 packets transmitted, 0 received, +9 errors, 100% packet loss, time 8003ms
```

ACCEPT only ICMP

```
[root@localhost ~]# iptables -F
[root@localhost ~]# iptables -A INPUT -p icmp -j ACCEPT
[root@localhost ~]# iptables -L -n -v -t filter
Chain INPUT (policy ACCEPT 527 packets, 98047 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            0.0.0.0/0

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 4371 packets, 227K bytes)
 pkts bytes target     prot opt in     out     source               destination
```

We were still able to connect to the SSH server.

```
jerome@LeNotre:~$ ssh root@160.98.31.6
root@160.98.31.6's password:
Permission denied, please try again.
root@160.98.31.6's password:
Last login: Fri Sep 26 12:21:23 2008 from 160.98.158.96
[root@localhost ~]#
```

DENY all, ACCEPT ICMP

```
[root@localhost ~]# iptables -F
[root@localhost ~]# iptables -P INPUT DROP
[root@localhost ~]# iptables -A INPUT -p icmp -j ACCEPT
[root@localhost ~]# iptables -L -n -v -t filter
Chain INPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            0.0.0.0/0

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 4432 packets, 235K bytes)
 pkts bytes target     prot opt in     out     source               destination
```

All the ping passes.

```
jerome@LeNotre:~$ ping 160.98.31.6
PING 160.98.31.6 (160.98.31.6) 56(84) bytes of data.
64 bytes from 160.98.31.6: icmp_seq=1 ttl=64 time=6.49 ms
```

```
64 bytes from 160.98.31.6: icmp_seq=2 ttl=64 time=0.466 ms
64 bytes from 160.98.31.6: icmp_seq=3 ttl=64 time=0.452 ms
64 bytes from 160.98.31.6: icmp_seq=4 ttl=64 time=0.379 ms
64 bytes from 160.98.31.6: icmp_seq=5 ttl=64 time=0.481 ms
64 bytes from 160.98.31.6: icmp_seq=6 ttl=64 time=0.466 ms
64 bytes from 160.98.31.6: icmp_seq=7 ttl=64 time=0.380 ms

--- 160.98.31.6 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6001ms
rtt min/avg/max/mdev = 0.379/1.302/6.496/2.120 ms
```

The SSH connection didn't work.

```
jerome@LeNotre:~$ ssh root@160.98.31.6

jerome@LeNotre:~$
```

REJECT Type

We changed the reject message on the server.

```
[root@localhost ~]# iptables -F
[root@localhost ~]# iptables -A INPUT -p icmp -j REJECT --reject-with icmp-net-prohibited
[root@localhost ~]# iptables -L -n -v -t filter
Chain INPUT (policy DROP 510 packets, 80529 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 REJECT     icmp --  *      *       0.0.0.0/0            0.0.0.0/0           reject-with icmp-net-prohibited

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 4437 packets, 236K bytes)
 pkts bytes target     prot opt in     out     source               destination
```

The message is now „Destination Net Prohibited" instead of „Destination Port Unreachable"

```
jerome@LeNotre:~$ ping 160.98.31.6
PING 160.98.31.6 (160.98.31.6) 56(84) bytes of data.
From 160.98.31.6 icmp_seq=1 Destination Net Prohibited
From 160.98.31.6 icmp_seq=2 Destination Net Prohibited
From 160.98.31.6 icmp_seq=3 Destination Net Prohibited
From 160.98.31.6 icmp_seq=4 Destination Net Prohibited
From 160.98.31.6 icmp_seq=5 Destination Net Prohibited
From 160.98.31.6 icmp_seq=6 Destination Net Prohibited
From 160.98.31.6 icmp_seq=7 Destination Net Prohibited
From 160.98.31.6 icmp_seq=8 Destination Net Prohibited
From 160.98.31.6 icmp_seq=9 Destination Net Prohibited

--- 160.98.31.6 ping statistics ---
9 packets transmitted, 0 received, +9 errors, 100% packet loss, time 8003ms
```

Ordre of filters

```
[root@localhost ~]# iptables -F
[root@localhost ~]# iptables -A INPUT -s 0/0 -d 0/0 -j DROP
[root@localhost ~]# iptables -L -n -v -t filter
Chain INPUT (policy DROP 576 packets, 89457 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 DROP       all  --  *      *       0.0.0.0/0            0.0.0.0/0

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 4457 packets, 237K bytes)
 pkts bytes target     prot opt in     out     source               destination
[root@localhost ~]# iptables -A INPUT -p icmp -j ACCEPT
[root@localhost ~]# iptables -L -n -v -t filter
Chain INPUT (policy DROP 576 packets, 89457 bytes)
 pkts bytes target     prot opt in     out     source               destination
   15  1885 DROP       all  --  *      *       0.0.0.0/0            0.0.0.0/0
    0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            0.0.0.0/0

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 4457 packets, 237K bytes)
 pkts bytes target     prot opt in     out     source               destination
```

With this order the ping won't pass.

```
jerome@LeNotre:~$ ping 160.98.31.6
PING 160.98.31.6 (160.98.31.6) 56(84) bytes of data.
```

```
^X
--- 160.98.31.6 ping statistics ---
6 packets transmitted, 0 received, 100% packet loss, time 5009ms

jerome@LeNotre:~$ ssh root@160.98.31.6

jerome@LeNotre:~$
```

Insert before

```
[root@localhost ~]# iptables -I INPUT -p icmp -j ACCEPT
[root@localhost ~]# iptables -L -n -v -t filter
Chain INPUT (policy DROP 576 packets, 89457 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            0.0.0.0/0
  142 21559 DROP       all  --  *      *       0.0.0.0/0            0.0.0.0/0
    0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            0.0.0.0/0

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 4457 packets, 237K bytes)
 pkts bytes target     prot opt in     out     source               destination
```

With ICMP as first entry the ping passes.

```
jerome@LeNotre:~$ ping 160.98.31.6
PING 160.98.31.6 (160.98.31.6) 56(84) bytes of data.
64 bytes from 160.98.31.6: icmp_seq=1 ttl=64 time=6.49 ms
64 bytes from 160.98.31.6: icmp_seq=2 ttl=64 time=0.466 ms
64 bytes from 160.98.31.6: icmp_seq=3 ttl=64 time=0.452 ms
64 bytes from 160.98.31.6: icmp_seq=4 ttl=64 time=0.379 ms
64 bytes from 160.98.31.6: icmp_seq=5 ttl=64 time=0.481 ms
64 bytes from 160.98.31.6: icmp_seq=6 ttl=64 time=0.466 ms
64 bytes from 160.98.31.6: icmp_seq=7 ttl=64 time=0.380 ms

--- 160.98.31.6 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6001ms
rtt min/avg/max/mdev = 0.379/1.302/6.496/2.120 ms
```

Statefull FW

```
[root@localhost ~]# iptables -F
[root@localhost ~]# iptables -N block
[root@localhost ~]# iptables -A block -m state --state ESTABLISHED,RELATED -j LOG
[root@localhost ~]# iptables -A block -m state --state ESTABLISHED,RELATED -j ACCEPT
[root@localhost ~]# iptables -A block -j DROP
[root@localhost ~]# iptables -A INPUT -j block
[root@localhost ~]# iptables -L -n -v -t filter
Chain INPUT (policy DROP 614 packets, 95202 bytes)
 pkts bytes target     prot opt in     out     source               destination
   40  4483 block      all  --  *      *       0.0.0.0/0            0.0.0.0/0

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 4464 packets, 238K bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain block (1 references)
 pkts bytes target     prot opt in     out     source               destination
    0     0 LOG        all  --  *      *       0.0.0.0/0            0.0.0.0/0           state RELATED,ESTABLISHED LOG flags 0
level 4
    0     0 ACCEPT     all  --  *      *       0.0.0.0/0            0.0.0.0/0           state RELATED,ESTABLISHED
   40  4483 DROP       all  --  *      *       0.0.0.0/0            0.0.0.0/0
```

Didn't work to establish a session.