**Firewally (IPTABLES)**

Firewall slouží k oddělení sítí s různým stupněm zabezpečení. Zpravidla oddělujeme vnitřní (lokální) síť od internetu. Vytváří zabezpečenou zónu důvěryhodné sítě a slouží jako komunikační uzel mezi těmito sítěmi. Provoz mezi sítěmi je pak na firewallu filtrován podle předem daných bezpečnostních pravidel.

**Podle principu činnosti můžeme firewally rozdělit na:**

* paketové filtry (nestavové stateless)
* stavové firewally (statefull)
* aplikační firewally

**Paketové filtry**

Filtrují provoz na základě ip adres a portů. Firewall sleduje procházející pakety a zkoumá zdrojové a cílové adresy a porty, které porovnává s nastavenými bezpečnostními pravidly. Pokud paket vyhoví určitému pravidlu, je s ním provedena nadefinovaná operace (propuštění, odmítnutí, zahození). Pracují především na prvních 3 vrstvách modelu OSI, 4. vrstvu používají pro zjišťování adres portů.

**Stavové firewally**

Princip je podobný jako u stateless firewallů, ale navíc provádí za pomoci 4. vrstvy OSI modelu inspekci paketu (SPI – statefull packet inspection) a sleduje všechna spojení. Na základě získaných informací je schopen vyhodnotit, jestli průchozí paket je počátkem nového spojení, patří k již existujícímu spojení nebo nepatří k žádnému spojení).

**Aplikační brány**

Pracují na 7. (aplikační vrstvě OSI modelu), "rozumí" některým aplikačním protokolům, jako je např. (http, FTP, DNS), je schopen detekovat, jestli se někdo nesnaží zneužít aplikačního protokolu a obejít tak definovaná bezpečnostní pravidla.

**Proxy servery**

Jsou určeny pro konkrétní aplikaci nebo protokol, zpracovávají požadavky klienta a vzhledem ke vzdálenému počítači (nebo serveru) se samy chovají jako klient. Požadavky klienta zpracují a předají je na vzdálený počítač, vrácenou odezvu opět zpracují a předají zpět klientovi. Můžou měnit obsah probíhající komunikace.

**NAT (IPv4)**

**Stavové a nestavové firewally zároveň implementují dvě funkce:**

NAT (network address translation) – překlad (záměnu) ip adres z adresního prostotu jedné sítě (veřejného adresního prostoru) do adresního prostoru druhé sítě (soukromého adresního prostoru).

Typy NATu:

* 1:1 – statická konfigurace 1 veřejné IP na jednu privátní IP
* N:N – dynamická konfigurace, každé jedné privátní IP je dynamicky přidělená veřejná IP
* PAT (port address translation) – mapuje více privátních IP na jednu veřejnou (NAT overload)

Funkce NAT slouží většinou k oddělení veřejného a privátního adresního prostoru mezi veřejnou a privátní sítí, byl vyvinut především pro úsporu IP adres v adresním prostoru IPv4. Umožňuje pomocí jedné veřejné IP adresy připojit celou vnitřní síť s mnoha adresami.

**Netfilter**

Linuxový paketový filtr, který je implementovaný přímo v jádru systému. Může být nakonfigurován jako nestavový i jako stavový firewall. Základem netfiltru jsou tabulky obsahující řetězce (chains) pravidel, podle kterých probíhá síťová komunikace mezi sítí a počítačem nebo mezi síťovými rozhraními.

Tabulek s pravidly je v současné době 5 a jsou spravované pomocí příkazu **iptables**.

**Tabulky:**

* filter
* nat
* mangle
* raw
* security

**Filter** – provádí filtrování paketů na základě pravidel, obsahují řetězce **INPUT** (pakety na vstupu), **FORWARD** (předávání paketů mezi rozhraními), **OTPUT** (pakety na výstupu).

**NAT** – provádí překlad portů a adres v paketech, obsahují řetězce **PREROUTING** (změna na vstupu), **OTPUT** (změna lokálně generovaných paketů před routováním) a **POSTROUTING** (změna odchozích paketů).

**Mangle** – mění další informace v paketech jako je TTL apod. Obsahují řetězce **INPUT**, **OUTPUT**, **FORWARD**, **PREROUTING**, **POSTROUTING**.

**Raw** – značí pakety, které nemají být jádrem sledovány (connection tracking), obsahují řetězce **PREROUTING** a **OUTPUT**.

**Security** – značkování paketů pomocí SECMARK a CONSECMARK pro aplikaci mandatorního způsobu zabezpečení MAC (založeném na bezpečnostních politikách). Pro tento účel je využíván modul SELINUX.

**Řetězec** – sada (seznam) pravidel v určité tabulce. Paket prochází řetězcem od prvního pravidla k poslednímu, dokud nenarazí na pravidlo, kterému vyhovuje. Pak je sním provedena příslušná akce definovaná u tohoto pravidla. Pokud nevyhoví žádnému pravidlu, je na něj aplikována výchozí bezpečnostní politika.

**Politiky se definují pro:**

* INPUT
* OUTPUT
* FORWARD

Výchozími akcemi jsou buď **ACCEPT** (propustit dál) nebo **DROP** (zahodit).

**Příkaz iptables**

Iptables –P směr politika *(definice politiky)*  
iptables –A směr –t tabulka (výchozí je filter) protokol zdroj cíl akce *(přidání pravidla)*  
iptables –F –t tabulka *(vymazání tabulky nebo politiky)*iptables –X *(vymazání řetezců)*  
iptables –N název\_řetězce *(definice řetězce)*  
iptables –L *(výpis tabulek)*  
iptables –D pravidlo (řetězec) – *(vymazání řetězce nebo pravidla)*

**Argumenty:**

**-t název\_tabulky (filter, nat, mangle, raw, security)  
-p** – protokol (vše, co je v /etc/protocols (většinou tcp, udp, icmp, all) nebo číslo protokolu  
**-i** –bod vstupu (rozhraní)  
**-s --source** (zdrojová adresa)  
**--sport** - zdrojový port  
**-m mac --mac-source** MAC adresa  
**-o** – bod výstupu (rozhraní)  
**-d --destination** (cílová adresa)  
**--dport** – cílový port  
**-m state --state (ESTABLISHED,RELATED)** – související spojení, může být ještě **NEW** (nové) nebo **INVALID** (neplatné – nesouvisející ani nové)  
**!** – negace hodnoty

**-j AKCE**

**Akce:**

**ACCEPT** – přijmout, propustit dál  
**DROP** – tiše zahodit  
**REJECT** – odmítnutí, informuje odesílatele  
**DNAT** --to-destination – adresa:cílový port při NATu  
**SNAT** --to source – věřejná IP  
**MASQUERADE** - jako SNAT, ale pro dynamickou adresu na výstupu   
**REDIRECT** --to-ports port – přesměrování portů  
**LOG** --log-prefix "návěští: " --log-level 7 (úroveň) – zápis do syslogu

**Konfigurace IPTABLES**

Konfiguraci iptables vytváříme v **shellovém .sh skriptu**, který pak vložíme do **/etc/network/if-pre-up.d**.

Na začátek vložíme interpretr a proměnné s adresami sítí, rozhraní atd.

#!/bin/bash  
#seznam proměnných ……

**#Konfigurace jádra**

**#neodpovídat na ICMP broadcasty**

echo 1 > /proc/sys/net/ipv4/icmp\_eccho\_ignore\_broadcasts

**#vypnout zdrojové směrování**

echo 0 > /proc/sys/net/ipv4/conf/all/accept\_source\_route  
echo 0 > /proc/sys/net/ipv4/conf/all/send\_redirects  
echo 0 > /proc/sys/net/ipv4/conf/all/accept\_redirects  
echo 1 > /proc/sys/net/ipv4/icmp\_ignore\_bogus\_error\_responses

**#zapnutí routování**

echo 1 > /proc/sys/net/ipv4/ip\_forward

**#Marťani**

echo 1 > /proc/sys/net/ipv4/conf/all/log\_martians

**#Výmaz stávajících pravidel**

iptables - F  
iptables –F –t nat  
iptables –F –t filter  
iptables –F –t mangle  
iptables -X

**#Definice výchozí politiky**

iptables –P INPUT DROP  
iptables –P FORWARD DROP  
iptables –P OUTPUT ACCEPT  
  
**#NATovaní paketů přicházejících zvenku**

iptables –A PREROUTING –t nat –p tcp –i vstupni\_rozhrani --dport port –j DNAT --to-destination cílová\_ip:port

**#NATování z lokální sítě směrem ven (do internetu)**

iptables –A POSTROUTING –t nat –o odchozí\_síťovka –j SNAT --to-source výstupní\_ip

**#Povolení provozu na localhost**

iptables –A INPUT –i lo –s adresa\_lo –j ACCEPT

**#Pakety přicházející na místní PC**

iptables –N icmp\_in  
iptables –N udp\_in  
iptables –N tcp\_in

iptables –A icmp\_in –p icmp --icmp-type 0 (3, 5, 8,11) –j ACCEPT  
iptables –A icmp\_in –p icmp –j DROP

iptables –A udp\_in –m state --state ESTABILISHED,RELATED –j ACCEPT  
iptables –A udp\_in –p udp –j DROP

iptables –A tcp\_in –p tcp –i vstupní\_rozhraní –s ip\_zdroje –d cilova\_ip --dport cilovy\_port –j ACCEPT  
iptables –A tcp\_in –m state –state ESTABLISHED,RELATED –j ACCEPT  
iptables –A tcp\_in –p tcp –j DROP

**#Třídění příchozích paketů**

iptables –A INPUT –p icmp –j icmp\_in  
iptables –A INPUT –p tcp –j tcp\_in  
iptables –A INPUT –p udp –j udp\_in

**#Pakety procházející přes firewall**

iptables –N icmp\_fw\_in  
iptables –N udp\_fw\_in  
iptables –N tcp\_fw\_in

iptables –A icmp\_fw\_in –p icmp --icmp-type 0 (3, 5, 8,11) –j ACCEPT  
iptables –A icmp\_fw\_in –p icmp –j DROP

iptables –A udp\_fw\_in –m state --state ESTABLISHED,RELATED –j ACCEPT  
iptables –A udp\_fw\_in –p udp –j DROP

iptables –A tcp\_fw\_in –p tcp –i vstupní\_rozhraní –s ip\_zdroje –d cilova\_ip --dport cilovy\_port –j ACCEPT  
iptables –A tcp\_fw\_in –m state –state ESTABLISHED,RELATED –j ACCEPT  
iptables –A tcp\_fw\_in –p tcp –j DROP

**#Třídění paketů procházejících přes firewall**

iptables –A FORWARD –p icmp –i vstupni\_rozhrani –o vystupni\_tozhrani ! –s lokalni\_sit –d lokalni\_sit –j icmp\_fw\_in  
iptables –A FORWARD –p tcp –i vstupni\_rozhrani –o vystupni\_tozhrani ! –s lokalni\_sit –d lokalni\_sit –j tcp\_fw\_in

iptables –A FORWARD –p udp –i vstupni\_rozhrani –o vystupni\_tozhrani ! –s lokalni\_sit –d lokalni\_sit –j udp\_fw\_i**n**

**#Odchozí pakety procházející přes firewall**

Iptables –A FORWARD –p all –i vstupni\_rozhrani –o vystupni\_rozhrani –s lokalni\_sit ! –d lokalni\_sit –j ACCEPT