FIREWALL - IPTABLES

1. Co je to firewall?

Firewall je bezpečný a důvěryhodný počítač zapojený mezi privátní a veřejnou sítí. Firewallový systém má nastavena pravidla udávající, jaký síťový provoz může propouštět a jaký má být zablokován nebo odmítnut. V některých velkých organizacích se firewally používají i uvnitř sítě jako ochrana citlivých oddělení organizace od ostatních zaměstnanců.

Firewally je možné konstruovat různými metodami. Nejpokročilejší metoda používá několik samostatných systémů a rozděluje síť na různě zabezpečené úrovně. Dva počítače fungují jako filtry umožňují průchod pouze přesně definovaným typům provozu a mezi nimi jsou umístěny síťové servery jako například poštovní brána, WWW server, a podobně. Takováto konfigurace může být velmi bezpečná a umožňuje snadno nastavit kdo se může připojit zvenčí dovnitř a zevnitř ven. Tento typ ochrany se používá obvykle ve velkých společnostech.

Typičtěji je firewall jediným počítačem, který zajišťuje vše. Jedná se o méně bezpečné řešení, protože pokud bude v samotném firewallu chyba, která umožní neautorizovaný přístup k němu, může být narušena celá bezpečnost sítě.

2. NETFILTER a IPTABLES

Nástroj iptables je součástí zdrojového balíku netfilter. Tento balík vznikl jako důsledek snahy o zjednodušení mechanismu filtrování datagramů ve firewallovém jádře. V linuxu se používá od verze jádra 2.4. Netfilter na rozdíl od předcházejících ipchans řeší jak složitost, tak neobratnost tím, že v jádře implementuje obecnou platformu, která zjednodušuje proces zpracování datagramů a zároveň umožňuje modifikovat filtrační politiky bez nutnosti modifikovat jádro. V implementaci IP Chains se třída input vztahuje na všechny datagramy přijaté počítačem, bez ohledu na to, zda jsou určeny pro něj, nebo zda je má pouze směrovat. V implementaci netfilter se třída input vztahuje pouze na datagramy určené lokálnímu hostiteli, třída forward pak pouze na datagramy určené jinému hostiteli. Analogicky se v IP chains třída output vstahuje na všechny odeslané datagramy bez ohledu na to, zda je odesílá lokální systém, nebo zda je směřuje jinému hostiteli. V netfilter se třída output vztahuje pouze na datagramy generované lokálním systémem a netýká se datagramů směrovaných jinému hostiteli.

Program **iptables** slouží k nastavení filtračních pravidel mechanismu netfilter. Jeho syntaxe je odvozena od ipchains, liší se v jednom podstatném rysu: je rozšiřitelná. Znamená to, že funkce programu je možné doplnit bez nutnosti jeho nového přeložení. Toto je realizovéno pomocí sdílených knihoven. Příkaz iptables slouží k nastavení filtrace a k nastavení filtrace adres. Zajišťují to dvě tabulky pravidel filter a nat. Tabulka filter se nahravá automaticky, pokud neuvedeme prametr –t. Kromě toho systém obsahuje pět vestavěných tříd. Třídy

INPUT a FORWARD se týkají tabulky filter, třídy PREROUTING a POSTROUTING tabulky nat a třída OUTPUT obou tabulek. Obecná syntaxe příkazu iptables je:

iptables *příkaz specifikace_pravidel rozšíření*

Příkazy
K nastavení firewallů se vztahují následující příkazy :

-A *třída* Přidá na konec třídy jedno nebo více pravidel

-I *třída č_prav* Přidá jedno nebo více pravidel na začátek třídy.

-D *třída* Vymaže ze třídy jedno nebo více pravidel, která odpovídají následující specifikaci.
-D třída č_prav Vymaže ze třídy pravidlo na pozici *č_prav*. Pravidla jsou číslovány od jedničky.
-R *třída č_prav* Nahradí pravidlo na pozici *č_pravidlo* novým pravidlem.

-C *třída*

-L *[třída]* Vypíše pravidla dané třídy, případně všech tříd, pokud není třída zadána.
-F [*třída*] Vymaže pravidla dané třídy, případně všech tříd, není-li zadána třída.

-Z [*třída*] Vynuluje počítadla datagramů dané třídy nebo všech tříd.

-N *třída* Vytvoří novou třídu se zadaným názvem. Třída zadaného jména nesmí existovat. Tímto příkazem se vytvářejí uživatelem definované třídy.
-X [*třída*] Vymaže třídu definovanou uživatelem, případě všechny uživatelem definované třídy.
-P *třída politika* Nastavuje implicitní politiku dané třídy.

Specifikace pravidel
Program iptables má celou řadu parametrů sloužících k definici pravidel. Kdykoliv se zadává pravidlo, používají se všechny následující parametry. Pokud některý z parametrů není zadán, použije se jeho implicitní hodnota.

-p *[!] protokol* Udává protokol, který pravidlu vyhovuje. Platné názvy protokolů jsou tcp, udp, icmp nebo číselná hodnota protokolu. Je-li uveden !, pravidlo je negováno a budou mu vyhovovat všechny protokoly kromě zadaného.

-s *[!] adresa[/maska]*
Udává zdrojovou adresu datagramu, který pravidlu vyhovuje. Adresa může být zadána názvem počítače, názvem sítě nebo IP adresou. Nepovinný údaj *maska*, představuje síťovou masku a může být zadán buď v tradiční podobě (např. /255.255.255.0) nebo v moderní podobě (např. /24).

-d *[!] adresa[/maska]*
Udává cílovou adresu datagramu, který pravidlu vyhovuje. Parametr se používá stejně jako –s.

-j *cíl* Definuje akci, která se má provést, jestliže diagram pravidlu vyhovuje.

Tento parametr můžete chápat jako příkaz „běž na“. Platné cílové hodnoty jsou ACCEPT, DROP a REJECT.

-i *[!] název_rozhraní*

Definuje rozhraní, na němž je datagram přijat. Symbol ! opět neguje význam pravidla. Pokud název rozhraní končí symbolem +, vyhovují všechna rozhraní začínající zadaným řetězcem. Například –i ppp+ definuje všechny rozhranií PPP, -i ! eth+ definuje všechna rozhraní kromě ethernetových rozhraní.

-o *[!] název_rozhraní*

Definuje rozhraní, na němž je datagram odesílán. Použití je stejné jako u parametru -i.

[!] -f

Udává, že pravidlo platí pro všechno kromě prvního fragmentu fragmentovaného datagramu.

Volby

Následující volby příkazu iptable jsou obecné. Některé z nich slouží k nastavení specifických nuancí systému netfilter.

-v

Zapne „výřečný “ výstup programu iptables. Program bude sdělovat více informací.

-n

Způsobí, že iptables bude vypisovat IP adresy a porty jako čísla a nebude se pokoušet o jejich převod na názvy.

-x

Všechna čísla ve výstupu programu iptables budou uvedena přesně, bez zaokrouhlování.

- - line – numbers

Při výpisu pravidel jednotlivých tříd budou řádky číslovány. Čísla řádků odpovídají pořadí pravidla ve třídě.

Rozšíření

Iptables je rozšiřitelný pomocí modulů sdílených knihoven. Existuje několik standardních rozšíření, která implementují funkce programu ipchains. Abychom mohli rozšíření použít, musíme jeho název sdělit programu iptables parametrem *–m název*. Následující seznam obsahuje parametry –m a –p, které nastavují kontext rozšíření, společně s parametry, které rozšíření poskytuje.

Rozšíření TCP : -m tcp -p tcp

-sport [!] [port [:port]]

Definuje zdrojový port datagramu, z nějž musí datagram pocházet, aby pravidlu vyhovoval. Je možno specifikovat i rozsahy portů zadáním spodní a horní meze oddělených dvojtečkou. Například 20:25 znamená porty od 20(včetně) po 25 (včetně). Znakem ! je možno význam pravidel negovat.

-port [!] [port [:port]]

Definuje cílový port diagramu, na němž musí být datagram určen, aby pravidlu vyhovoval. Použití parametru je stejné jako u –sport.

-tcp – flags [!] maska comp

Pravidlu budou vyhovovat ty TCP datagramy, jejichž příznaky odpovídají podmínkám specifikovaným parametry *maska* a *comp*.

maska je čárkami oddělený seznam příznaků, které mají být do testování zahrnuty, *comp* je čárkami oddělený seznam testovaných příznaků, které musí být nastaveny. Platnými příznaky jsou SYN, ACK, FIN, URG, PSH, ALL, a NONE. Symbolem ! je možné význam pravidla negovat.

Rozšíření UDP : -m udp -p udp

-sport [!] [port [:port]]

Definuje zdrojový port datagramu, z nějž musí datagram procházet, aby pravidlu vyhovoval. Je možné specifikovat i rozsahy portů zadáním spodní a horní meze oddělených dvojtečkou. Znakem ! je možné význam pravidla negovat.

-dport [!] [port [:port]]

Definuje cílový port datagramu, na nějž musí být datagram určen, aby pravidlu vyhovoval. Použití parametru je stejné jako u *-sport.*

Rozšíření ICMP : -m icmp -p icmp

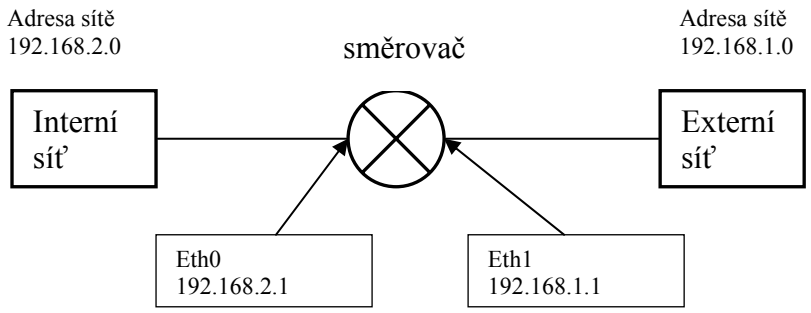
-icmp-type [!] typ Udává typ ICMP zprávy, která bude pravidlu vyhovovat. Typ je možné zadat číslem názvem. Některé platné názvy jsou: *echo-request, echo-reply, source-quench, time-exceeded, destination-unreachable, network-unreachable, host-unreachable, protocol-unreachablea a port-unreachable.*

Rozšíření MAC : -m mac

-mac-source [!] adresa

Udává ethernetovou adresu hostitele, který datagram vyslal. Tento parametr má význam pouze ve třídách input a forward, protože u všech dataramů ve třídě output jsme odesílatelem my.

4. Nastavení směrovače



Při nastavení směrovače postupujeme následujícím způsobem

1. nastavení ip adres síťových rozhraní směrovače. Každé rozhraní náleží jedné ze síťových karet.

ifconfig eth0 192.168.2.1 netmask 255.255.255.0
ifconfig eth1 192.168.1.1 netmask 255.255.255.0

2. dále potřebujeme nastavit, aby směrovač předával informace z interní do externí sítě a naopak. Toto se nastavuje v souboru /proc/sys/net/ipv4/id_forward. Pro zjištění jakou hodnotu tento soubor obsahuje.

   more /proc/sys/net/ipv4/id_forward

   Pro zapnutí směrování, musíme v tomto souboru nastavit hodnotu na 1. Příkaz pro zapnutí směrování použijeme příkaz

   echo “1” > /proc/sys/net/ipv4/id_forward

5. Příklady

Pozn : Při propouštění nějaké služby přes firewall, kdy nechceme, aby dosáhla na lokální počítač, budou nám stačit dvě pravidla : obě ve třídě forward, jedno pro směr „tam“ a druhé pro směr „zpět“.

Příklad 1. **Nastavení počátečních politik**

/sbin/iptables -X
/sbin/iptables -F INPUT
/sbin/iptables -F OUTPUT
/sbin/iptables -F FORWARD

Příklad 2. **Povolení localhostu**

/sbin/iptables -A INPUT -i lo -j ACCEPT
/sbin/iptables -A OUTPUT -o lo -j ACCEPT

Příklad 3. **Povolení pro eth1** – uživatel je schopen z eth1 provádět operace

/sbin/iptables -A INPUT -i eth1 -j ACCEPT
/sbin/iptables -A OUTPUT -o eth1 -j ACCEPT

Příklad 4. **Povolení pro eth0**

/sbin/iptables -A INPUT -i eth0 -j ACCEPT
/sbin/iptables -A OUTPUT -o eth0 -j ACCEPT¨

Příklad 5.**WWW pro obě strany**

/sbin/iptables -A FORWARD -p tcp -s 0/0 -d 0/0 --dport 80 -j ACCEPT
/sbin/iptables -A FORWARD -p tcp -d 0/0 -s 0/0 --sport 80 -j ACCEPT

Příklad 6. **FTP** – z vnější sítě se není nikdo schopen přihlásit na ftp, ale z sítě 192.168.2.0 se můžem přihlásit kamkoliv

/sbin/iptables -A FORWARD -p tcp -s 192.168.2.0/24 -d 0/0 --dport 20 -j ACCEPT
/sbin/iptables -A FORWARD -p tcp -s 192.168.2.0/24 -d 0/0 --dport 21 -j ACCEPT
/sbin/iptables -A FORWARD -p tcp -d 192.168.2.0/24 -s 0/0 --sport 20 -j ACCEPT
/sbin/iptables -A FORWARD -p tcp -d 192.168.2.0/24 -s 0/0 --sport 21 -j ACCEPT

Příklad 7. **ICMP** – povolení icmp pro lokalní sít (např. jsem schopný se pingnout na stroje za Firewallem)

/sbin/iptables -A FORWARD -p icmp -j ACCEPT

Příklad 8. **ICMP** – povolení icmp na router (např. jsem schopný pingnout interface routeru)

/sbin/iptables -A INPUT -p ICMP -j ACCEPT
/sbin/iptables -A OUTPUT -p ICMP -j ACCEPT

6. Reference

1. Linus Torvalds, “Linux dokumentační projekt”,
2. AbcLinuxu s.r.o., “www.abclinuxu.cz”