Cisco ACL vs IPTables

Úvod

V tomto článku bych rád porovnal možnosti dvou částečně konkurenčních produktů, Cisco ACL a IPTables.
Cisco ACL (*Access Control List*) je součástí propritálního OS (*Operačního systému*) Cisco IOS (*Internetwork Operating systém*), je to seznam pravidel, která řídí přístup k nějakému objektu. Nejčastější použití je pro řízení (omezování) siťového provozu tzv. p*acket filtering*.
IPTables je opensource nástroj na vytváření pravidel pro Netfilter, který poskytuje řadu možností, jak ovlivnit síťový provoz.
Ve srovnání se budu zaměřovat především na 3. a vyšší síťové vrstvy ISO modelu.

Cisco ACL

Nalezneme je ve všech novějších verzích Cisco IOS. Zahrnuje v sobě jak nástroj na tvorbu pravidel, tak i samotný engine uplatňování těchto pravidel. Dělí se na dva typy, IP ACL a Ethernet (MAC) ACL. Zaměřme se na IP ACL, které filtrují provoz IPv4. ACL se používá především jako základní síťová bezpečnost, k blokování nebo povolení provozu.
ACL je sekvenční seznam pravidel permit a deny, těmto pravidlům se říká ACE (*Access Control Entries*). Můžeme je identifikovat číslem nebo jménem. Nová pravidla se přidávají vždy na konec seznamu. Průchod pravidly je tzv.*first-fit*, tedy průchod pravidli jde od začátku seznamu a při první shodě se uplatní dané pravidlo a dále se seznam neprochází. Každý seznam má defaultní politiku *deny any*, tedy zakaž vše. Pokud se paket vyhodnotí deny, tak se odešle ICMP zpráva *host unreacheable*.
U ACL se nepoužívají klasické síťové masky, ale tzv.*wildcard mask*y. Jedná se o inverzní masku. Například pro masku 255.255.255.0 je to 0.0.0.255.
ACL se dělí do dvou skupin, standard ACL a extended ACL.
Standard ACL je starší a jednodušší verze, má méně možností konfigurace. Používají se číselná označení 1-99 a 1300-1999. Filtruje pouze zdrojové adresy, většinou se používá jako odchozí filtr.
Extended ACL používá označení 100-199 a 2000-2699. Dokáže filtrovat IP adresu zdroje i cíle, kontroluje řadu položek v hlavičce 3. a 4.síťové vrstvy (protokol, ToS(*Type of Service*), v TCP porty a protokoly, v UDP porty).
Syntaxe výtváření pravidel:
Standard ACL
#access-list cislo {deny|permit} {host|source source-wildcard|any} [log]

Extended ACL
#access-list cislo {deny|permit} protokol {host|source source-wildcard|any} [port] {host| destination destination-wildcar|any} [port]

Vytvořený ACL se aplikuje na zvolené rozhraní a směr. ACL se dá aplikovat pouze na směr dovnitř (*in*) nebo ven (*out*)
Syntaxe: #ip access-group cislo {in|out}

IPTables

IPTables je Linuxový opensource nástroj pro editaci pravidel pro NetFilter. V Linuxu se používá pro jádra řady 2.4 a 2.6. Jedná se tedy jen o editor pravidel, samotné uplatňování pravidel má na starosti NetFilter. IPTables jsou ve vývoji od r.1998. Pomocí IPTables můžeme vytvářet packet filter pravidla, ale také měnit hlavičky paketů (např. u NATu).
Pravidla můžeme vytvářet ve třech tabulkách (filter, nat a mangle). V každé tabulce je několik

tzv.*chain*ů, což jsou „řetězy“ pravidel. Průchod pravidly viz. zdroj [6]. V IPTables můžeme také používat různé rozšíření pro NetFilter, která nám dávají další možnosti při psaní pravidel. Můžeme vytvářet pravidla závislá nebo proměnná v čase. Buď pravidlo platí v určitý časový úsek nebo je omezeno na X akcí v nějakém čase (např. 10 paketů za hodinu).
Pravidla v IPTables se píší přímo na interface a aplikují se v momentě potvrzení příkazu, který pravidlo vytvoří. Výchozí politika je povolit všechno, ale dá se změnit.

Shrnutí

IPTables nám dávají mnohem větší možnosti při vytváření pravidel než ACL. Je to dáno enginem, který pravidla zpracovává. IPTables používá více tabulek a několik *chainů*, ACL rozděluje tok pouze na *in* a *out*. Na NetFilter, který je opensource, se mohou dopisovat různá rozšíření a tím i rozšiřovat možnosti pravidel IPTables. IPTables nám také dovolují psát pravidla, který manipulují s hlavičkami paketů, dá se proto udělat přesměrování portů, záměna IP adresy (NATy) apod.
Pro psaní základní bezpečnostní politiky je Cisco ACL dostačující. Pokud chceme více funkcí určitě se nám vyplatí sáhnout po IPTables.

Michal Heczko

Použité zdroje

[1] článek o Cisco ACL - http://www.samuraj-cz.com/clanek/cisco-ios-8-access-control-list/
[2] seriál o iptables - http://www.root.cz/serialy/vse-o-iptables/
[3] Easy Firewall Generator for IPTables - http://easyfwgen.morizot.net/gen/
[4] OSI model - http://en.wikipedia.org/wiki/OSI_model
[5] IPTables - http://en.wikipedia.org/wiki/Iptables
[6] Průchod tabulkamy a chainy - http://www.jollycom.ca/iptables-tutorial/images/tables_traverse.jpg