IPv6 csomagszűrés

Kadlecsik József
KFKI RMKI
kadlec@sunserv.kfki.hu

2007.05.14.

Tartalom

- IPv6 és ICMPv6
- Egyszerű csomagszűrés
- Állapottartó tűzfalak, komplex protokollok
- NAT
- netfilter/ip6tables
- essence

IPv6 címek

- Méret: 128 bit
- Típusok:
  - unicast
    - loopback: ::1 (0000::/8)
    - link-local: FE80::/10
    - global: 2000::/3
  - anycast
  - multicast: FF00::/8

IPv6 csomagok

- IPv6-os fejléc:
  - version (4), traffic class (8), flow label (20)
  - payload length (16), next hdr (8), hop limit (8)
  - src (128)
  - dst (128)
- Kiterjesztés-fejlécek (extension headers)
  - Hop-by-Hop, Routing, Fragment, Destination Options, Authentication, Encapsulating Security Payload
- Protokoll-fejléc: TCP, UDP, ICMPv6, SCTP

ICMPv6 I.

- ICMPv6: nem segéd-protokoll
  - type: 8bit, 0-255
    - type <= 127: error
    - type > 127: information
  - code: 8bit
- Hibaüzenetek:
  - Destination Unreachable
  - Packet Too Big
  - Time Exceeded
  - Parameter Problem

ICMPv6 II.

- Szerteágazó feladatok:
  - Neighbor Discovery, Duplicate Address Detection, Neigbor Unreachability Discovery:
    - Neighbor, Router Solicitation (NS, RS)
    - Neigbor, Router Advertisement (NA, RA)
  - Stateless Autoconfiguration
  - Path MTU Discovery
  - Multicast Router Advertisement, Solicitation
  - Mobile IPv6 support ...

ICMPv6 III.

- ICMPv6 tűzfalon való szűrése:
  - RFC 4890: E. Davies, J. Mohácsi, Recommendations for Filtering ICMPv6 Messages in Firewalls

Egyszerű csomagszűrés

- Forrás és célcím: típus, scope, subnet, stb.
- Interfész
- Csomagméret
- Extension header és tartalma
- Extension header-ek sorrendje
- Felsőbb protokoll típusa és szokásos paraméterei

Állapottartó tűzfalak

- A csomagok nem függetlenek egymástól: stream, session
  - ICMPv6
    - information: kérdés-válasz
    - error: előző csomaghoz kapcsolódik
  - TCP, UDP, SCTP

Komplex protokollok

- Kontroll (parancs) csatornán keresztül adják meg a segéd-csatornák paramétereit
  - FTP, IRC, TFTP, H.323, SIP, stb

NAT

- Címfordítás (feltételezett) előnyei
  - biztonság, anonimitás
  - “virtuális” IP címek
  - debuggolás
- Hátrányok
  - end-to-end
  - elérhetőség
  - dinamikus címek

Netfilter/ip6tables

- Netfilter keretrendszer fölött:
  - IPv4-es tűzfal: iptables
  - IPv6-os tűzfal: ip6tables
- “Majdnem” csak cím és parancsnév-csere

```
ip6tables -A FORWARD -d DEAD:BEEF::1
    -p tcp --dport 80 -j ACCEPT
```

ip6tables I.

- táblák: raw, mangle, filter
- targetek: ACCEPT, DROP, QUEUE, RETURN
- szokásos egyezések: src, dst IPv6 cím, interfészek, felsőbb protokollok
- közös egyezések: limit, mac, mark, condition, length; ah, esp, policy (IPsec)
- IPv6 specifikus egyezések: dst, eui64, frag, hbh, hl, mh, rt; ipv6header

ip6tables II.

- Közös targetek: LOG, MARK, NFQUEUE, REJECT, TCPMSS; SECMARK, CONNSECMARK (SELinux)
- IPv6 specifikus targetek: HL

ip6tables III.

- Kapcsolatnyomkövető: state
- IPv6 fölött támogatott komplex protokollok:
  - FTP, TFTP, Amanda, H.323, SIP
  - Kernel modul neve: nf_conntrack_ftp, stb.

ip6tables III.

- Kapcsolatnyomkövető: state match!
  - nf_conntrack
- IPv6 fölött támogatott komplex protokollok:
  - FTP, TFTP, Amanda, H.323, SIP
  - Kernel modul neve: nf_conntrack_ftp, stb.

essence I.

- SecureFilter:
  - tűzfal számára optimalizált i386-os kernel
  - LIDS-el megerősített Debian
  - essence tűzfal-konfiguráló eszköz
  - dinamikus routing protokollok támogatása (quagga)
  - http://www.kfki.hu/cnc/projekt/securefilter

essence II.

- Egyszerű nyelv tűzfal-szabályokhoz
  - IPv4: raw, mangle, nat, filter
  - IPv6: raw, mangle, filter
  - automatikus IPv4/IPv6 spoofing elleni védelem
- perl és shell script

essence III.

```
filter = webserver
  IP = 10.1.1.1, DEAD:BEEF:1
  service = http, https
  service = ssh
    allow = 10.254.1.0/24
    deny = 10.254.1.1
  [client = domain, ftp, http]
```

essence IV.

- RFC4890-et megelőző draft ajánlásait tartalmazza

Köszönöm a figyelmet!