Firewall MikroTik, IPS, IDS

Wykonali: Wojciech Bernaś, Jan Książek oraz Paweł Wójcik

Zasada działania firewalli

Główne domeny pracy firewalla to 3 i 4 warstwa sieciowa modelu ISO/OSI. Na warstwie 2 mamy możliwość analizy jedynie źródłowego adresu MAC i priorytetu w nagłówku VLAN, natomiast zaawansowane funkcje poniżej warstwy 3 dostępne są poprzez inne mechanizmy: reguły filtrowania

Firewall warstwy 7

Firewall pozwala także na filtrację pakietów w warstwie aplikacji poprzez wyszukiwanie wzorców w strumieniach protokołów ICMP/TCP/UDP (funkcja layer7-protocol). Wzorce do filtrowania stosowane przez RouterOS są kompatybilne z projektem l7-filter.

Protocols

The pattern *name* is what you must use when issuing l7-filter commands. The names below link to the pattern files. Select column headings to sort.

bad third line in replaytv-ivs.pat

wiki	name	speed	quality	group	notes	description
W	100bao	○ ◑	■			100bao - a Chinese P2P protocol/program - http://www.100bao.com
W	aim	● ◑	■	$		AIM - AOL instant messenger (OSCAR and TOC)
W	aimwebcontent	◑ ◑	■	$		AIM web content - ads/news content downloaded by AOL Instant Messenger
W	applejuice	○ ○	■			Apple Juice - P2P filesharing - http://www.applejuicenet.de
W	ares	○ ○	■		−	Ares - P2P filesharing - http://aresgalaxy.sf.net
W	armagetron	● ◑	■			Armagetron Advanced - open source Tron/snake based multiplayer game
W	battlefield1942	○ ○	■	$		Battlefield 1942 - An EA game
W	battlefield2	● ◑	■	$		Battlefield 2 - An EA game.
W	battlefield2142	◑ ○	■	$		Battlefield 2142 - An EA game.
W	bgp	○ ○	■			BGP - Border Gateway Protocol - RFC 1771
W	biff	◑ ○	■		− +	Biff - new mail notification
W	bittorrent	● ◑	■		−	Bittorrent - P2P filesharing / publishing tool - http://www.bittorrent.com
W	chikka	◑ ○	■	$		Chikka - SMS service which can be used without phones - http://chikka.com
W	cimd	◑ ◑	■	$		Computer Interface to Message Distribution, an SMSC protocol by Nokia
W	ciscovpn	○ ○	■	$		Cisco VPN - VPN client software to a Cisco VPN server
W	citrix	◑ ◑	■	$		Citrix ICA - proprietary remote desktop application - http://citrix.com
W	counterstrike-source	○ ○	■	$		Counterstrike (using the new "Source" engine) - network game
W	cvs	○ ○	■			CVS - Concurrent Versions System
W	dayofdefeat-source	○ ○	■	$		Day of Defeat: Source - game (Half-Life 2 mod) - http://www.valvesoftware.com
W	dazhihui	◑ ○	■			Dazhihui - stock analysis and trading; Chinese - http://www.gw.com.cn
W	dhcp	○ ○	■			DHCP - Dynamic Host Configuration Protocol - RFC 1541

Podstawowa konfiguracja reguł

Funkcja IDS

IDS (Intrusion Detection Systems) systemy wykrywania intruzów, jak sama nazwa wskazuje, zajmują się wykrywaniem prób uzyskania dostępu do systemu. Ich zadaniem jest wykrycie takiego zdarzenia i poinformowanie o tym odpowiednich osób. Działanie takich systemów jest podobne do alarmu chroniącego dom przed włamywaczami.

IDS często są używane razem z firewallami, nie należy jednak mylić tych pojęć - zapory sieciowe służą wyłącznie do ochrony systemu przed niepowołanymi osobami. IDS są wykorzystywane do uzupełnienia całości dobrze zorganizowanego systemu bezpieczeństwa, na który oprócz nich powinny się składać m.in:

- polityka bezpieczeństwa
- szyfrowanie danych
- weryfikacja użytkowników
- kontrola dostępu
- zapory sieciowe

Funkcja IDS c.d. Przykładowe systemy

Darmowe:

- Snort (NIDS), ACID (analiza), Snortalog (analiza)
- Bro IDS (NIDS)
- Snort-Prelude (NIDS), Prelude-lml (HIDS), Prewikka (analiza)
- OSSEC (HIDS)
- GesWall
- Suricata

Komercyjne:

- IBM ISS Proventia (NIDS), Proventia Server (HIDS), Site Protector (zbieranie i analiza zdarzeń)
- 3COM Tipping Point
- Juniper IDP
- DefenseWall HIPS (dostępny także w polskiej wersji)
- Safe'n'Sec Pro (+Rootkit Detector)

Funkcja IPS

- **Czym są IPS?**
- IPS (Intrusion Prevention Systems) to sprzętowe bądź programowe rozwiązania, których zadaniem jest wykrywanie ataków na system komputerowy z wewnątrz jak i od zewnątrz systemu oraz uniemożliwianie przeprowadzenia takich ataków. Od strony technicznej systemy IPS to mniej więcej połączenie zapory sieciowej i systemu IDS. W dalszej części prezentacji omówionych zostanie kilka różnych sposobów implementacji systemów ochrony przed intruzami.

Przykładowa konfirguracja IPS w MikroTik'u

Mikrotik IPS IDS

Regarding a Forum post by "slech", [1] you can enable Mikrotik Router to work with Snort [2] IDS system.

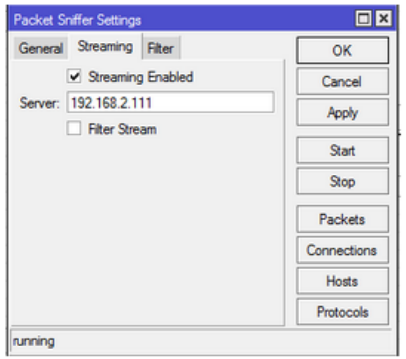
Snort already has developed Subscribed and Free service for attack signature update and mechanism for attack detection and alerting.

As Tap of main Internet line is not ideal solution for some cases, like with redundant routers connected with VRRP, it is great to have solution based only on Mikrotik Sniffing Stream.

IDS Solution

To install IDS Snort solution, you need computer running Linux OS. Download and install Snort following OS Specific manual, or compile it from source if there is no binary for your OS. Snort Installation Procedures ([3]) After full installation, follow configuration parameters to setup Snort. Subscribe to Snort site, to get latest Regular User rules with attack signatures and set them like in manual.

To setup Mikrotik, you need to install Calea package and opet Sniffing Tool. Set Sniffer to listed all Interfaces, and uncheck Only Headers box. Open Streaming tab, and enter IP address of Linux server, check Streaming Enabled, and uncheck Filter Stream. Start your sniffing.



https://wiki.mikrotik.com/wiki/Mikrotik_IPS_IDS