Alanata TALKS

UNIKÁTNE VLASTNOSTI FIREWALLOV PALO ALTO

Juraj Nemeček

Vedúci oddelenie sieťovej bezpečnosti

Alanata

Technology Meets Business

Na čo ..... ?

Ako ..... ?

Čo ..... ?

Na čo nám je firewall?

Alanata

Technology Meets Business

Alanata
Technology Meets Business

Potrebujeme firewall ?

- V dobe mikrosegmentácie a kontajnerizácie ?
- V dobe rozmachu _**aaS** prostredí ?
- V dobe hybridnej práce ?

Alanata
Technology Meets Business

Potrebujeme firewall ?

- V dobe mikrosegmentácie a kontajnerizácie ?
  Ochrana dátového centra

- V dobe rozmachu _**aaS** prostredí ?
  Ochrana cloud prostredí

- V dobe hybridnej práce ?
  Vzdialený prístup

Ako sa má firewall používať?

Alanata

Technology Meets Business

Alanata
Technology Meets Business

Nástroj

Firewall je **nástroj**

- Umožňuje kontrolu
- Poskytuje “náhľad“ do aktuálneho stavu
- Dáva nám šancu reagovať

Alanata
Technology Meets Business

Bezpečnostná politika

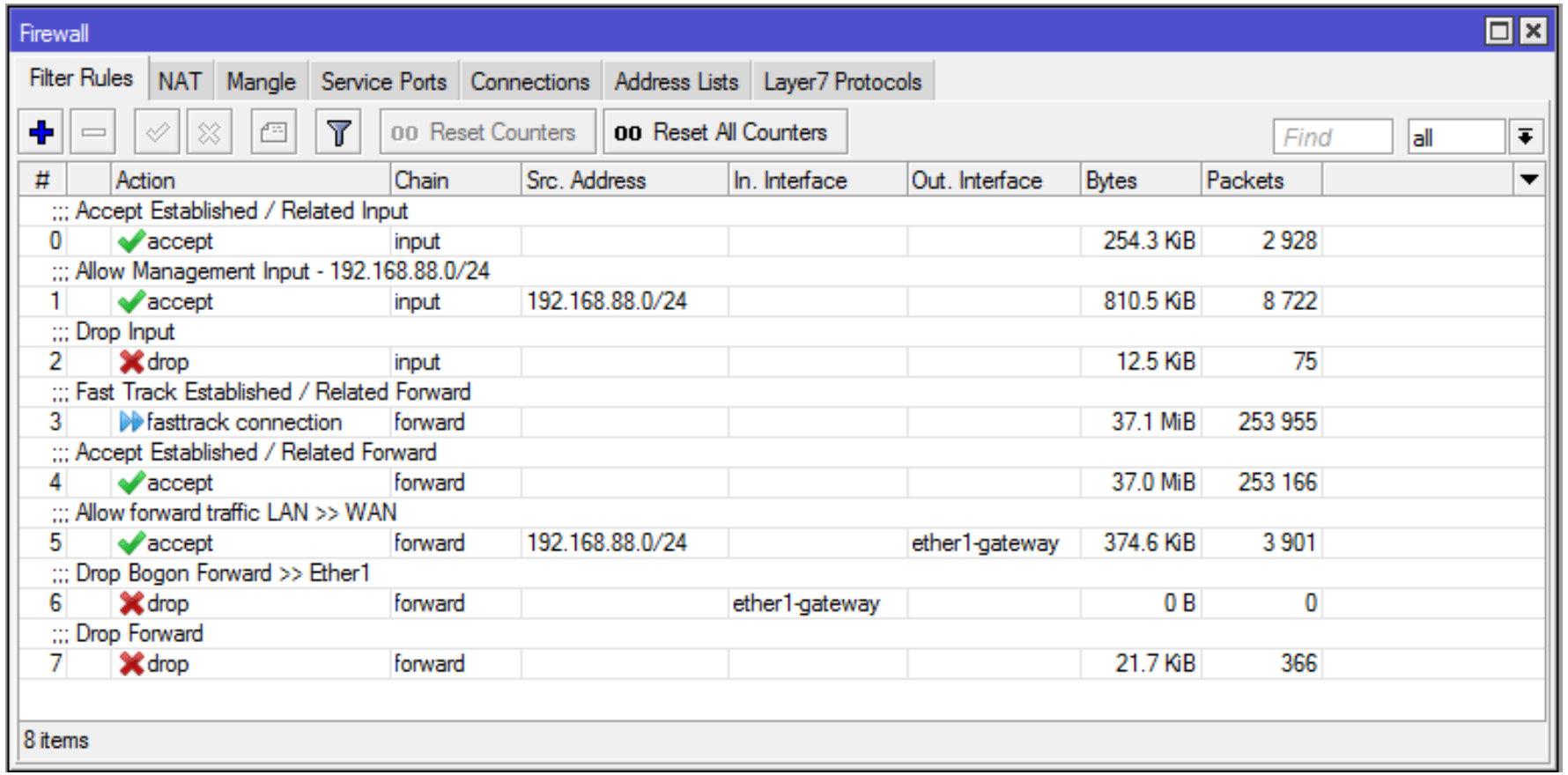
```
root@Raspberry ~ # iptables -L -v
Chain INPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
  172 13541 ACCEPT     all  --  any    any     anywhere             anywhere             ctstate ESTABLISHED
    0     0 ACCEPT     all  --  lo     any     anywhere             anywhere
    0     0 ACCEPT     tcp  --  any    any     anywhere             anywhere             tcp dpt:http
    0     0 ACCEPT     tcp  --  any    any     192.168.1.10         anywhere             tcp dpt:ssh

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 17 packets, 1772 bytes)
 pkts bytes target     prot opt in     out     source               destination
root@Raspberry ~ #
```

Alanata
Technology Meets Business

Bezpečnostná politika



#	Action	Chain	Src. Address	In. Interface	Out. Interface	Bytes	Packets
;;; Accept Established / Related Input							
0	accept	input				254.3 KiB	2 928
;;; Allow Management Input - 192.168.88.0/24							
1	accept	input	192.168.88.0/24			810.5 KiB	8 722
;;; Drop Input							
2	drop	input				12.5 KiB	75
;;; Fast Track Established / Related Forward							
3	fasttrack connection	forward				37.1 MiB	253 955
;;; Accept Established / Related Forward							
4	accept	forward				37.0 MiB	253 166
;;; Allow forward traffic LAN >> WAN							
5	accept	forward	192.168.88.0/24		ether1-gateway	374.6 KiB	3 901
;;; Drop Bogon Forward >> Ether1							
6	drop	forward		ether1-gateway		0 B	0
;;; Drop Forward							
7	drop	forward				21.7 KiB	366

Alanata
Technology Meets Business

Bezpečnostná politika

			Source				Destination						
	NAME	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATI...	SERVICE	ACTION	PROFILE
1	Allow Internet direct	universal	trust	any	Local_office_users	any	untrust	any	any	any	service-https	Allow	none
2	intrazone-default	intrazone	any	any	any	any	(intrazone)	any	any	any	any	Allow	none
3	interzone-default	interzone	any	any	any	any	any	any	any	any	any	Deny	none

Alanata
Technology Meets Business

Bezpečnostná politika

- **Základ** každého firewallu
- Zdoj mnohých frustrácií
- Dobrá politika = dobrý firewall

Čo stojí za zmienku?

Alanata

Technology Meets Business

Alanata
Technology Meets Business

Firewally Palo Alto

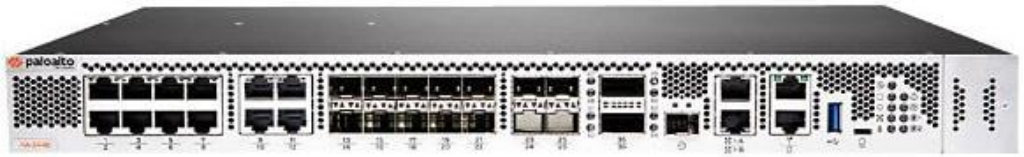
- **PA-410**

	PA-410
Firewall throughput (appmix)*	1.4 Gbps
Threat Prevention throughput (appmix)†	0.8 Gbps
IPsec VPN throughput‡	0.65 Gbps
Max concurrent sessions§	64,000
New sessions per second‖	11,000
Virtual systems (base/max)#	1/1

Alanata
Technology Meets Business

Firewally Palo Alto

- PA-3440



	PA-3440
Firewall throughput (appmix)*	35 Gbps
Threat Prevention throughput (appmix)†	20 Gbps
IPsec VPN throughput‡	14.5 Gbps
Max concurrent sessions§	3M
New sessions per second‖	268,000
Virtual systems (base/max)#	1/11

Alanata
Technology Meets Business

Firewally Palo Alto

- PA-7500

	PA-7500*
Firewall throughput (appmix)†	1,500 Gbps
Threat Prevention throughput (appmix)‡	1,440 Gbps
Max concurrent sessions§	440M
IPsec VPN throughput‖	407 Gbps
New sessions per second#	7.2M
Virtual systems (base/max)**	25/225

Alanata
Technology Meets Business

Unikátne vlastnosti

App-ID a **Content-ID**

- Identifikuje aplikáciu čisto na základe dát zo 7. vrstvy RM OSI
- Umožňuje vytvoriť bezpečnostnú politiku postavenú na aplikáciách
- Robustná podpora pre dešifrovanie
  - Pre protokoly HTTPS, HTTP/2 a SSH
- Rozšírená podpora pre vnorené a tunelované protokoly
- Policy optimizer
- Možnosť aplikovať behaviorálnu analýzu
- Nové signatúry cca. raz za mesiac

Alanata
Technology Meets Business

Unikátne vlastnosti

App-ID Cloud Engine

- Identifikácia cloudových služieb pre web traffic
- Používa machine learning
- Dopĺňa statické signatúry pre App-ID

Alanata
Technology Meets Business

Unikátne vlastnosti

Device-ID

- Možnosť aplikovať bezpečnostnú politiku podľa zariadenia
  - Výrobca
  - Operačný systém a jeho verzia
  - Model
  - Kategória
- Zamerané na ochranu IoT zariadení

Alanata
Technology Meets Business

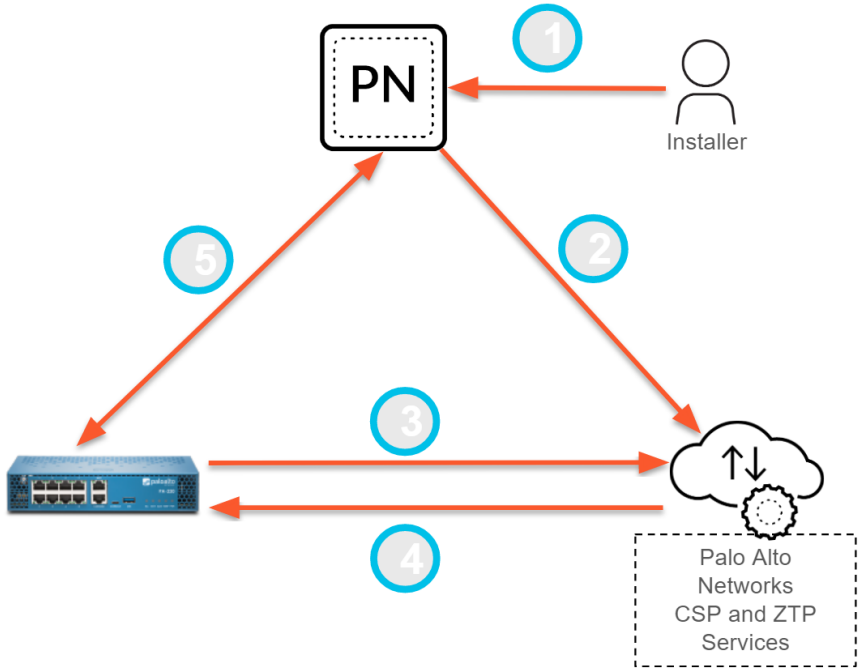
Unikátne vlastnosti

- **Cloud Identity Engine**
  - Cloud-native autentifikačný engine
  - On-premise agent pre integráciu s lokálnym AD
    - SAML 2.0
    - TLS certifikát
    - Okta
    - Google
    - A iné

Firewally Palo Alto

Zero-Touch provisioning

- Možnosť automatizovanej konfigurácie zariadení bez potreby ich ručnej konfigurácie
- Vhodné pri nasadzovaní väčšieho počtu zariadení



Otázky ?

ĎAKUJEM ZA POZORNOSŤ

Alanata

Technology Meets Business

Alanata

Technology Meets Business

Alanata a.s.
Einsteinova Business Center
Krasovského 14
851 01 Bratislava 5
Slovenská republika

www.alanata.sk