Sodobna požarna pregrada in Layer 7

ko potrebujemo več,
kot prepoznavo aplikacije

Zgodovina

(Legacy Firewalls)

- V 80-ih letih se pojavijo prvi zametki fil
  1989 -Jeff Mogul iz DEC zasnuje prvo g
- V zgodnih 90-ih se pojavijo IP usmerjev
  podporo osnovnih možnosti filtriranja p
- 1992 pride na trg DEC Seal - prva komer
  pregrada, hibridna pregrada sestavljena
  proxijev in paketnih filtrov
- 1994 se pojavi prvi „Stateful firewall“
  CheckPoint ustvari pojem „Stateful Inspection“ *(20 let)*

Zgodovina

(Sodobne požarne pregrade)

- 2004 IDC skuje izraz UTM (Unified Threat Management) izraz posvojijo številni ponudniki, ki v eni napravi nudijo več različnih varnostnih funkcij *(15 let)*
- 2009 Gartner in Palo Alto Networks definirata pojem „Next-Generation Firewall“ *(10 let)*

LCD vs. LED vs. Smart…

What‘s the difference?

Kaj pa danes…?

- Srečujemo se z vsemi variantami p.p. od stateful do požarnih pregrad naslednje generacije
- Delitev gre vse bolj v smeri SOHO / SME / Enterprise rešitev
- Na SOHO področju še vedno (pre)močno prevladujejo „Routerji“ brez varnostnih funkcij
- Kritično pomanjkanje znanja zlasti v SME

SME vs. Enterprise rešitve?

- Ločnica med njima je vse bolj zabrisana
- Enterprise rešitve predvsem tekmujejo z vse bolj zmogljivim HW (bitka za datacenter)
- Enterprise rešitve pogosto ne nudijo opcij, za katere se v teh okoljih uporablja specializirane rešitve (npr. filtriranje elektronske pošte)
- SME rešitve tekmujejo z prilagojenostjo posebnim zahtevam, katera imajo SME okolja (pomanjkanje kadrov, resursov, znanja,…)

Smeri razvoja SME rešitev

- SME rešitve se danes razvijajo predvsem v dve smeri:
  a) **Poenostavljanje**, s katerim se prilagaja pomanjkanju kadra s specializiranem znanjem
  b) **Višja specializacija** in napredne **SME funkcionalnost**i za „eksperte“, zlasti za **MSSP** področje (storitve upravljanja varnosti)

SME v Sloveniji

REPUBLIKA SLOVENIJA
STATISTIČNI URAD RS

Podatkovni portal SI-STAT » Ekonomsko področje » Seznam tabel » Dimenzije in kategorije / Izbor podatkov

Podjetja po dejavnosti (SKD 2008) in velikosti glede na število oseb, ki delajo, Slovenija, letno

Informacije Opombe Statistična znamenja

Dimenzije in kategorije / Izbor podatkov

Urejanje in preračuni | Shrani tabelo kot...

Podjetja po dejavnosti (SKD 2008) in velikosti po: SKD, LETO, MERITVE , RAZREDI OSEB, KI DELAJO. Prikazano po: število/število/1000 EUR , Deleži.

		2017						
		Število podjetij						
		Razredi oseb, ki delajo - Skupaj	Mikro podjetje (0-9) - Skupaj	Mikro podjetje (0-1)	Mikro podjetje (2-9)	Majhno podjetje (10-49)	Srednje podjetje (50-249)	Veliko podjetje (250+)
število/število/1000 EUR	SKD 2008 - Skupaj	195756	185997	144101	41896	7329	2084	346
Deleži	SKD 2008 - Skupaj	100,00	95,02	73,61	21,40	3,74	1,07	0,18

81,1% 14,2% 4,0% **0,7%**

99,3%

Opombe:
Vir: Statistični urad Republike Slovenije.

Enota opazovanja
Enota opazovanja je podjetje, registrirano kot pravna ali fizična oseba, ki je med letom opazovanja izkazala prihodek ali zaposlene osebe ali investicije.

Uporabljena statistična znamenja:
z podatek zaradi zaupnosti ni objavljen

Časovne vrste podatkov po SKD 2002 so objavljeni v tabeli Število podjetij .

MERITVE
Število podjetij
Je število registriranih pravnih ali fizičnih oseb, ki so med letom opazovanja izkazale prihodek ali zaposlene osebe ali investicije.

Vir: https://pxweb.stat.si/pxweb/Database/Ekonomsko/14_poslovni_subjekti/01_14188_podjetja/01_14188_podjetja.asp

Težave SME okolja

- Mikro podjetja (81% !) nimajo usposobljenega kadra, ki bi znal izbrati primerno varnostno rešitev. Podobno mala podjetja (14%)
- Vzdrževanje omrežja izvaja zunanji izvajalec
- Kupujejo se neoptimalne rešitve
- Konfiguracije so ‚bazične‘
- Rednega nadzora nad dogajanjem ni
- Pomanjkanje specialistov MSSP in njihove akceptance (podjetja hočejo one-stop shop)

Rešitve, ki v praksi delujejo?

1) Za varovanje omrežja potrebujemo podatke

TRAFFIC | ALARM | EVENT | DIAGNOSTIC | STATISTIC | ALL | SEARCH | ACTIONS

View 1 - 25 of 346,547 Page 1 of 13,862 25

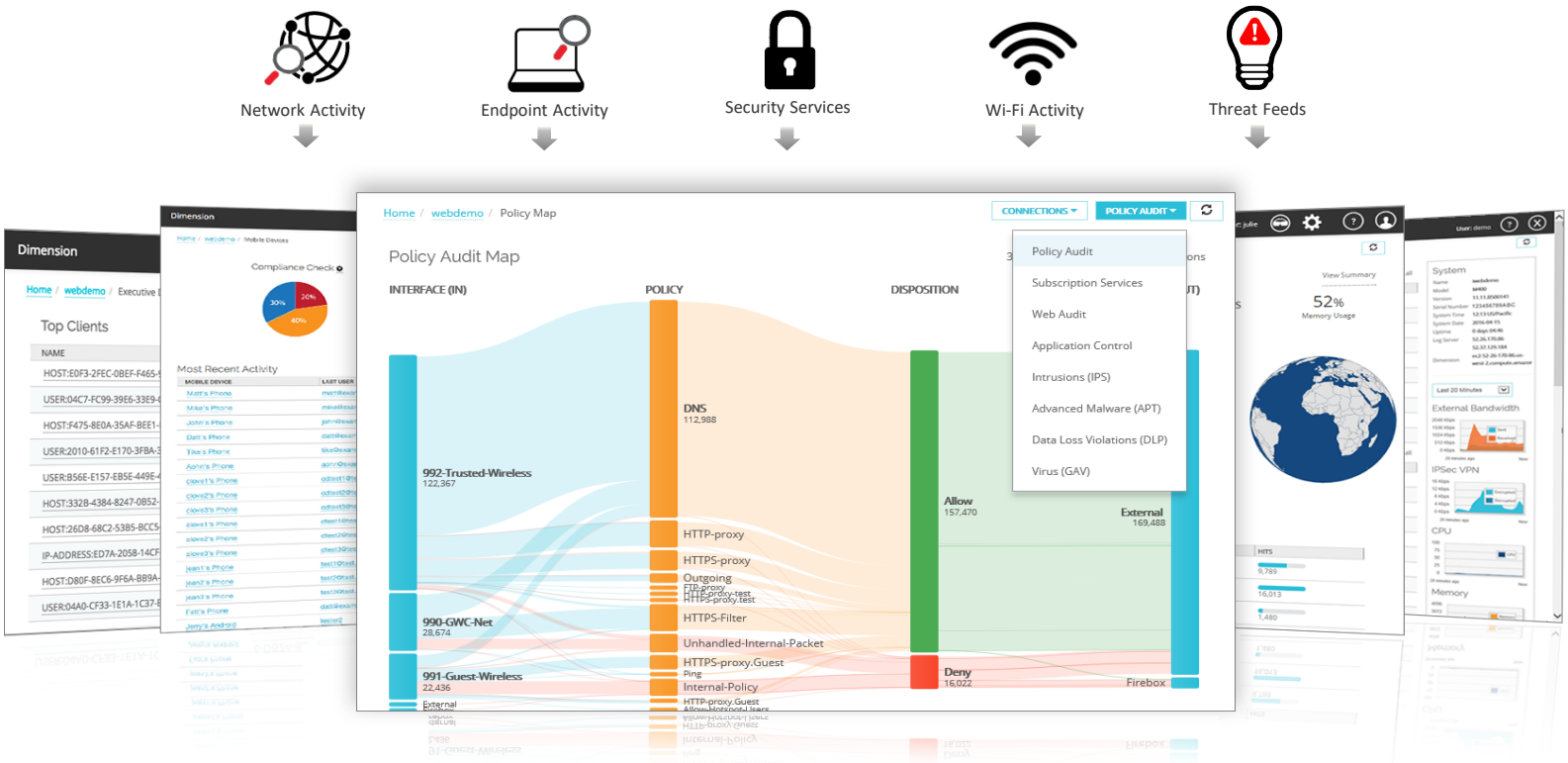
DISPOSITION	DATE-TIME	SOURCE	INTERFACE	DESTINATION	PORT	INTERFACE	PROTOCOL	POLICY
FWAllowEnd	2019-03-01 00:00:27	10.0.2.102	2-Servers	4.2.2.2	53	0-External	dns/udp	DNS-00
ProxyAllow	2019-03-01 00:00:36	10.0.2.102	2-Servers	naproduction.excelsior.service.consul	443	0-External	https/tcp	HTTPS-proxy.Guest-00
ProxyHTTPSReq	2019-03-01 00:00:36	10.0.2.102	2-Servers	34.210.36.119	443	0-External	https/tcp	HTTPS-proxy.Guest-00
Allow	2019-03-01 00:00:37	10.0.2.102	2-Servers	4.2.2.2	53	0-External	dns/udp	DNS-00
Allow	2019-03-01 00:00:37	10.0.2.102	2-Servers	34.210.36.119	443	0-External	https/tcp	HTTPS-proxy.Guest-00
FWAllowEnd	2019-03-01 00:01:07	10.0.2.102	2-Servers	4.2.2.2	53	0-External	dns/udp	DNS-00
ProxyAllow	2019-03-01 00:01:07	10.0.2.102	2-Servers	naproduction.excelsior.service.consul	443	0-External	https/tcp	HTTPS-proxy.Guest-00
ProxyHTTPSReq	2019-03-01 00:01:07	10.0.2.102	2-Servers	34.210.118.12	443	0-External	https/tcp	HTTPS-proxy.Guest-00
Allow	2019-03-01 00:01:08	10.0.2.102	2-Servers	4.2.2.2	53	0-External	dns/udp	DNS-00
Allow	2019-03-01 00:01:08	10.0.2.102	2-Servers	34.210.118.12	443	0-External	https/tcp	HTTPS-proxy.Guest-00
ProxyAllow	2019-03-01 00:01:38	10.0.2.102	2-Servers	naproduction.excelsior.service.consul	443	0-External	https/tcp	HTTPS-proxy.Guest-00
ProxyHTTPSReq	2019-03-01 00:01:38	10.0.2.102	2-Servers	35.162.108.47	443	0-External	https/tcp	HTTPS-proxy.Guest-00
FWAllowEnd	2019-03-01 00:01:38	10.0.2.102	2-Servers	4.2.2.2	53	0-External	dns/udp	DNS-00
Allow	2019-03-01 00:01:38	10.0.2.102	2-Servers	4.2.2.2	53	0-External	dns/udp	DNS-00
Allow	2019-03-01 00:01:38	10.0.2.102	2-Servers	35.162.108.47	443	0-External	https/tcp	HTTPS-proxy.Guest-00

Rešitve, ki v praksi delujejo?

2) Za generiranje podatkov potrebujemo „senzorje“

Rešitve, ki v praksi delujejo?

3) Podatke moramo predelati v informacije



Požarne pregrade kot senzor

Tipična konfiguracija požarne pregrade:

Order	Action	Policy Name	Policy Type	From	To	Port
1	✗	Ping.INcoming	Ping	Any-External	Any	ICMP (type: 8, code: 255)
2	✓	Ping	Ping	Any-Trusted, Any-Optional	Any	ICMP (type: 8, code: 255)
3	✓	FTP	FTP	Any-Trusted, Any-Optional	Any-External	tcp:21
4	✓	HTTP-proxy	HTTP-proxy	Sales (Any)	Any-External	tcp:80
5	✓	WatchGuard Authentication	WG-Auth	Any-Trusted, Any-Optional	Firebox	tcp:4100
6	✓	WatchGuard Web UI	WG-Fireware-XTM-WebUI	Any-External, Any-Trusted, Any-Optiona	Firebox	tcp:8080
7	✓	WatchGuard	WG-Firebox-Mgmt	Any-External, Any-Trusted, Any-Optiona	Firebox	tcp:4105 tcp:4117 tcp:41...
8	✗	Outgoing	TCP-UDP	Any-Trusted, Any-Optional	Any-External	tcp:0 (Any) udp:0 (Any)

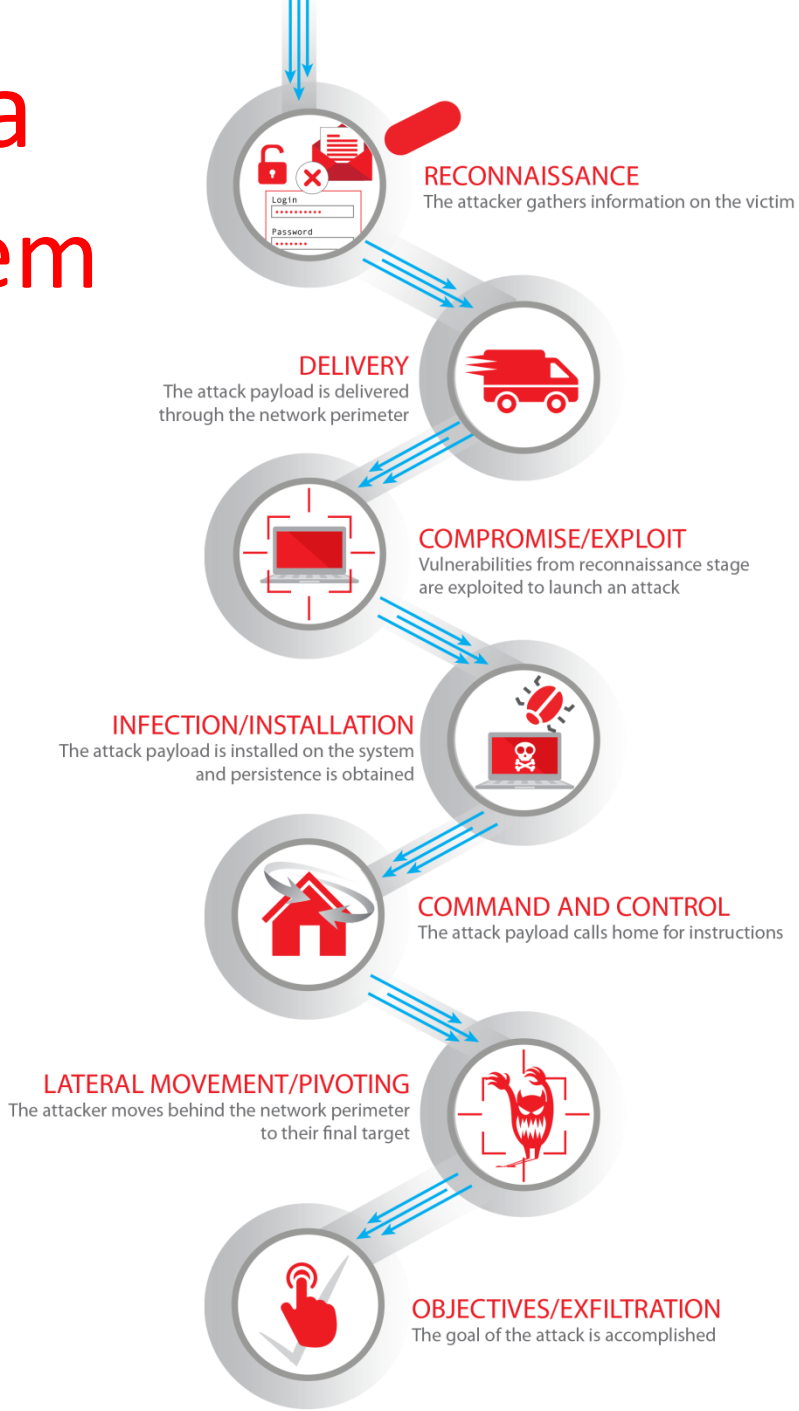
Večnivojska obramba za večnivojski problem

Na desni prikazani Cyber Kill Chain® ponazarja tipično zaporedje, po katerem se zgodijo omrežni varnostni incidenti.

Napredne požarne pregrade ga poskušajo zaznati in zaustaviti na vsaki stopnji.

V ta namen se poslužujejo večnivojske obrambe.

Da pa bi ta lahko bila maksimalno učinkovita, potrebujemo tudi ustrezno konfiguracijo požarne pregrade.



Drop vs. Block

- Tipično požarne pregrade izvedejo zgolj ***Drop***, kadar neka povezava ne ustreza zadanim pravilom
- V logih dobimo en zapis, ki običajno sam po sebi ne bo pritegnil pozornosti
- Če namesto drop izvorni IP naslov uvrstimo na „Blacklisto“, govorimo o ***Block*** akciji
- Taka blokada IP naslova bo povzročila *drop* za vse, tudi sicer dovoljene povezave tega naslova
- V logih dobimo več zapisov, pojavijo se opazna odstopanja, ki pritegnejo pozornost

Security Dashboard

(GDPR anonimizacija vključena)

WatchGuard Dimension

User: demo

2019-03-01 00:00 — 2019-03-02 00:00

Home / webdemo / Security Dashboard

Top Blocked Advanced Malware (APT)

View All

NAME	HITS
/d/CZ8SVw2r/770629/CoolGameMod.exe, /d/d1HMiibK/886895/ScreenSaver.exe, /d/sROJPAe6/7040...	3
/download.php?file_id:4088847256755021092 1&t:4088847256755021092100123	1

Top Blocked Clients

View All

NAME	BYTES	HITS
USER:4786-B632-73B5-C78D-9CB6-0372-4935-375A-F5D2-A8BF-7C72-00...	23	7
IP-ADDRESS:B70D-1379-A78B-7824-08C9-AB6C-AD80-24C5-A1F8-F534-C...	0	5,222
HOST:3FA7-0ABE-1547-61D2-C074-0B65-F958-FC70-0967-22BA-D2F5-2E...	0	2,372
IP-ADDRESS:6C09-DD2E-24B8-A5A0-1810-083B-AC4B-06C6-34C8-2FCC-...	0	994
USER:59A9-353C-A458-A480-44B1-D4B2-038F-9AA0-7D92-5442-B15A-61...	0	853
HOST:6A11-001B-5F4F-6E0F-939B-F1DE-5CD3-F7AF-AB0B-24F3-4150-1C...	0	813
HOST:FB25-AEF7-8357-E6E6-74AE-3D05-0494-A6C6-C2D1-51B9-83A6-C1...	0	654
IP-ADDRESS:9F4A-8F4F-CB7B-E0B6-55B5-7B7D-8671-BC4C-EC07-2279-3...	0	531
USER:EA4A-16DA-589E-330D-6280-EF48-68E0-2FCB-89B2-7963-ADA4-CE...	0	226
IP-ADDRESS:97E2-EBD7-B72D-5326-7EC3-12A6-B3F9-E470-36DB-74C1-1...	0	171

Top Blocked Destinations

View All

NAME	BYTES	HITS
52.200.252.136	23	1
10.99.1.255	0	2,545
4.2.2.2	0	1,783
255.255.255.255	0	765
23.209.11.156	0	588
192.168.130.80	0	241
63.232.60.117	0	215
192.168.130.81	0	207
216.115.208.230	0	110
172.25.1.100	0	94

Top Blocked URL Categories

View All

NAME	HITS
Sex	106
Suspicious Content	2

Top Blocked Applications

View All

NAME	HITS
XBOX	618
HTTP Proxy Server	118
LogMeIn	63
Valve Steam	2
Glype	1

Top Blocked Application Categories

View All

NAME	HITS
Games	620
Bypass Proxies and Tunnels	182

Security Dashboard

(Anonimizacija izključena)

WatchGuard Dimension User: demo

2019-03-01 00:00 — 2019-03-02 00:00

Home / webdemo / Security Dashboard

Top Blocked Advanced Malware (APT)

View All

NAME	HITS
/d/CZ8SVw2r/770629/CoolGameMod.exe, /d/d1HMiibK/886895/ScreenSaver.exe, /d/sROJP...	3
/download.php?file_id:4088847256755021092100123	1

Top Blocked Clients

View All

NAME	BYTES	HITS
Hannah@example.com	23	7
10.99.1.103	0	5,222
AP200_20AP0579063FF	0	2,372
10.99.1.101	0	994
Rex@example.com	0	853
AP300_30AP02BB6AF40	0	813
guest-icfcq	0	654
10.99.1.100	0	531
Jessie@example.com	0	226
10.99.2.100	0	171

Top Blocked Destinations

View All

NAME	BYTES	HITS
52.200.252.136	23	1
10.99.1.255	0	2,545
4.2.2.2	0	1,783
255.255.255.255	0	765
23.209.11.156	0	588
192.168.130.80	0	241
63.232.60.117	0	215
192.168.130.81	0	207
216.115.208.230	0	110
172.25.1.100	0	94

Top Blocked URL Categories

View All

NAME	HITS
Sex	106
Suspicious Content	2

Top Blocked Applications

View All

NAME	HITS
XBOX	618
HTTP Proxy Server	118

Top Blocked Application Categories

View All

NAME	HITS
Games	620
Bypass Proxies and Tunnels	182

Security Dashboard

(Anonimizacija izključena)

WatchGuard Dimension User: demo

2019-03-01 00:00 — 2019-03-02 00:00

Home / webdemo / Security Dashboard / Top Blocked Clients

Top Blocked Clients

View All

NAME	BYTES	HITS
Hannah@example.com	23	7
10.99.1.103	0	5,222
AP200_20AP0579063FF	0	2,372
10.99.1.101	0	994
Rex@example.com	0	853
AP300_30AP02BB6AF40	0	813
guest-icfcq	0	654
10.99.1.100	0	531
Jessie@example.com	0	226
10.99.2.100	0	171
guest-grwug	0	89
fred@example.com	0	70
guest-16kyu	0	29
10.99.2.102	0	28
10.99.1.102	0	19
Sid@example.com	0	15
10.99.2.101	0	10
10.99.2.104	0	7
10.99.2.254	0	6
10.99.0.254	0	4
192.168.43.115	0	2
10.99.2.103	0	2
165.254.96.118	0	1

Security Dashboard

(**Realen** primer – tedenski pregled - Anonimizacija vključena)

WatchGuard Dimension User: Bojan

2019-03-27 00:00 — 2019-04-03 15:09

Home / / Security Dashboard

Top Blocked Botnet Sites

View All

NAME	HITS
69.16.175.10	90
104.193.88.123	84
69.16.175.42	83
104.193.88.77	60
52.164.206.56	34
104.215.95.187	31
66.240.205.34	19
80.82.77.139	16
185.25.204.80	10
80.82.77.33	10

Top Blocked Clients

View All

NAME	BYTES	HITS
IP-ADDRESS:1D45-E51F-A40A-B320-53D5-AA1E-67BE-37DB-3FE8-A139-7...	8 MB	2,954
IP-ADDRESS:2313-4099-FB21-29F7-83F6-3CF9-D91D-68D6-F777-28A8-4C...	7 MB	3,635
IP-ADDRESS:DE68-B8CE-3EC3-1F12-E659-ECB5-74B4-475F-4681-1982-05...	5 MB	1,641
IP-ADDRESS:FE0A-8DBD-0ED7-8717-A060-9F95-5EFA-ECA9-6688-B42E-B...	2 MB	847
IP-ADDRESS:9216-87B6-0F65-691B-A715-66E9-2BBC-FB2A-50C6-17AD-F...	2 MB	488
IP-ADDRESS:83F9-EC62-DD85-8C01-5294-93A1-43C5-8235-AAEA-9A8D-3...	1 MB	868
IP-ADDRESS:331C-9A23-21F5-5A1E-D458-E455-9823-4BD5-7D5D-4BD4-6...	1 MB	466
IP-ADDRESS:3DE1-5086-E090-5F5C-7216-C1F3-ABB4-ABA4-CA9A-20C8-1...	1 MB	603
IP-ADDRESS:0841-3629-BD8E-7B7C-26D9-A064-4C87-7F5C-66F6-B932-9...	938 KB	365
IP-ADDRESS:6287-A577-BD0A-5E06-92F5-CA43-EEA4-C49D-7743-498E-F...	638 KB	679

Top Blocked Destinations

View All

NAME	BYTES	HITS
init.itunes.apple.com	10 MB	3,353
api.gameanalytics.com	8 MB	2,824
service.supercell.net	3 MB	1,786
bag.itunes.apple.com	1 MB	410
inbox.brawlstars.com	1007 KB	330
fbdownldr.net	950 KB	324
itunes.apple.com	835 KB	270
video-edge-ebf6a2.sjc02.hls.ttvnw.net	628 KB	212
maps.nepremicnine.link	580 KB	200
css.enetscores.com	489 KB	184

Top Blocked URL Categories

View All

NAME	HITS
Games	2,839
Media File Download	2,336
Gambling	419
Newly Registered Websites	166
Peer-to-Peer File Sharing	120
Elevated Exposure	100
Sex	40
Adult Content	31
Potentially Unwanted Software	6
Compromised Websites	4

Top Blocked Applications

View All

NAME	HITS
BitTorrent Series	4,819
HTTP Proxy Server	113
HotspotShield	13

Top Blocked Application Categories

View All

NAME	HITS
Peer-to-peer networks	4,819
Tunneling and proxy services	126

Security Dashboard

(Realen primer – tedenski pregled pt.2- Anonimizacija vključena)

WatchGuard Dimension User: Bojan

bag.itunes.apple.com	1 MB	410
inbox.brawlstars.com	1007 KB	330
fbdownldr.net	950 KB	324
itunes.apple.com	835 KB	270
video-edge-ebf6a2.sjc02.hls.ttvnw.net	628 KB	212
maps.nepremicnine.link	580 KB	200
css.enetscores.com	489 KB	184

Newly Registered Websites	166
Peer-to-Peer File Sharing	120
Elevated Exposure	100
Sex	40
Adult Content	31
Potentially Unwanted Software	6
Compromised Websites	4

Top Blocked Applications

View All

NAME	HITS
BitTorrent Series	4,819
HTTP Proxy Server	113
HotspotShield	13

Top Blocked Application Categories

View All

NAME	HITS
Peer-to-peer networks	4,819
Tunneling and proxy services	126

Top Blocked Protocols

View All

NAME	BYTES	HITS
https/tcp	31 MB	12,239
5678/udp	0	54,213
62976/udp	0	21,698
icmp	0	16,089
igmp	0	12,797
telnet/tcp	0	10,404
http/tcp	0	6,355
56760/udp	0	3,240
sip/udp	0	1,920
ssh/tcp	0	1,606

Top Blocked Malware

View All

NAME	HITS
Exploit.CVE-2017-11882.Gen	91
Exploit.SpamMalware-RAR.Gen	21
Exploit.MathType-Obfs.Gen	12
Gen:Variant.Strictor.189011	7
Gen:Variant.Ulise.33544	7
VB:Trojan.VBA.Agent.AGW	6
Gen:Variant.Ursu.414797	6
Gen:Variant.Ulise.34126	6
Trojan.GenericKD.41155170	3
Trojan.GenericKD.31811606	2

Security Dashboard

(Realen primer – Exploit.CVE-2017-11882.Gen - Anonimizacija vključena)

WatchGuard Dimension User: Bojan

2019-03-27 00:00 — 2019-04-03 15:09

Home / ..... / Security Dashboard / Exploit.CVE-2017-11882.Gen

Top Blocked Clients

View All

NAME	HITS
IP-ADDRESS:3048-12E9-2134-E2F4-2945-953B-2D14-16FF-A5AF-96D8-72D5-8564	19
IP-ADDRESS:AD0E-E874-9D51-BCDE-0CAC-07F2-FE17-00BB-35A0-DCF8-A5BB-0E48	15
IP-ADDRESS:4C0D-98BB-354D-BDA1-1184-2B6A-64FE-CA0A-3285-C3C7-E955-F880	14
IP-ADDRESS:3DE1-5086-E090-5F5C-7216-C1F3-ABB4-ABA4-CA9A-20C8-147A-0F3F	14
IP-ADDRESS:AE82-58DF-9A58-79C7-32D9-F797-3C1D-BFCD-FF97-4791-4AF2-C4E0	14
IP-ADDRESS:0EAE-6B66-ADE6-B241-D2CB-6BA3-C6EF-C959-3920-C12F-BCFE-6A87	8
IP-ADDRESS:87BA-872B-467C-4255-1531-F475-AD45-891E-1669-BFC1-B22C-D2C2	5
IP-ADDRESS:E994-96AC-0454-B0C3-76F8-9C9D-B2BD-5C69-62D8-7623-602B-8340	1
IP-ADDRESS:A560-FA70-FB9B-5F1A-A396-C69C-A12B-D33C-8B31-E072-2464-91C8	1

Top Blocked Destinations

View All

NAME	HITS
91.185.212.109	91

Top Blocked Protocols

View All

NAME	HITS
pop3/tcp	91

Blokirajmo več za več informacij!

- Da bi pridobili čim bolj uporabno statistiko moramo zaznati čim več *kršitev* pravil
- Pomagamo si z
  - Dinamično blocklisto
  - Spremembo privzete obravnave
  - Block akcijo v pravilih
  - Block akcijami v Proxy nastavitvah
  - Block akcijami v varnostnih storitvah

Dinamična Blocklista

Z njeno pomočjo:

- Prekinemo povezave, ki so bile zaznane kot potencialno nevarne
- Prekinemo obstoječe sicer dovoljene povezave do problematičnega naslova
- Začasno onemogočimo VSE povezave do problematičnega naslova
- Blokado podaljšujemo, če v tem času zaznamo ponovne poskuse vzpostavitve potencialno nevarnih povezav

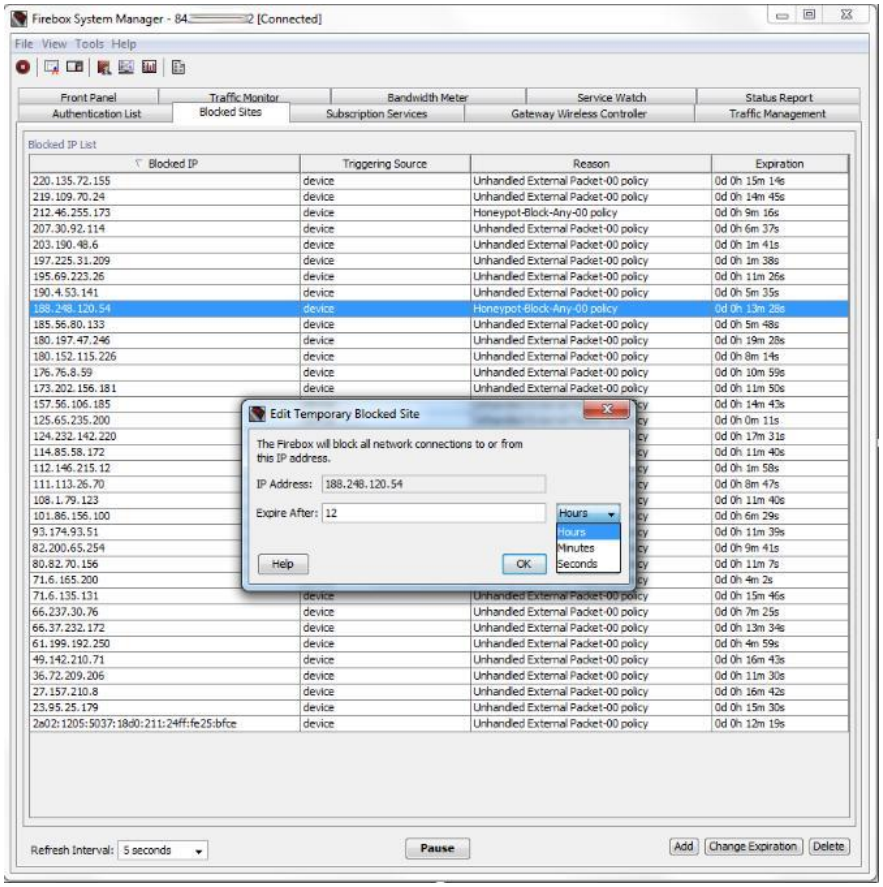
Dinamična Blocklista

IP naslove vpisujemo in brišemo v/z blockliste:

a) Ročno

b) Samodejno

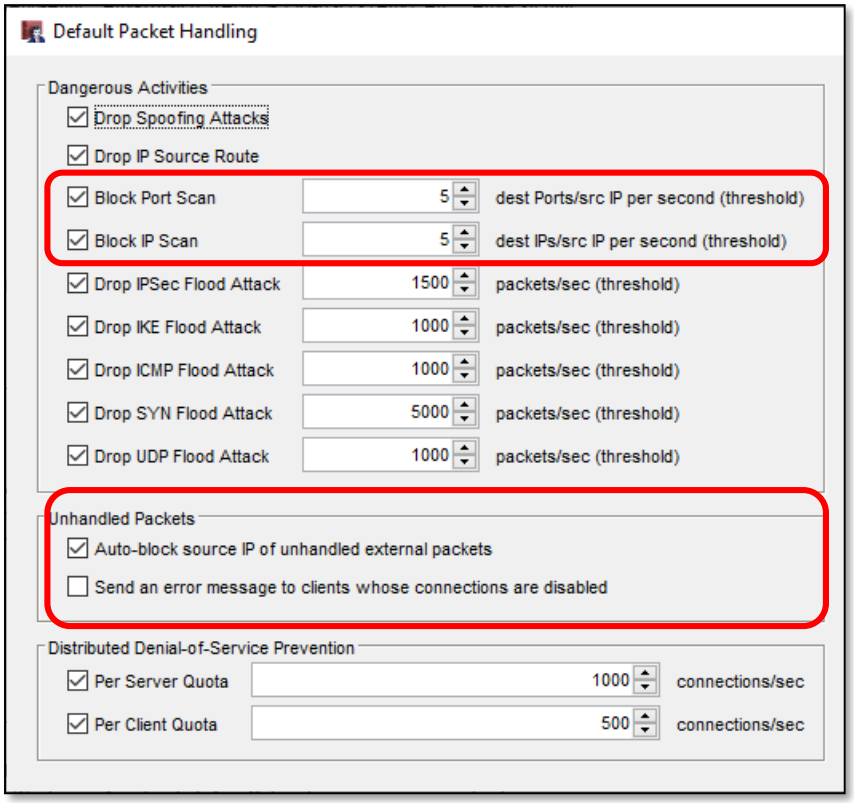
Privzeta blokada traja 20 minut



Samodejno dodajanje - Autoblock

(Sprememba sistemske privzete obravnave)

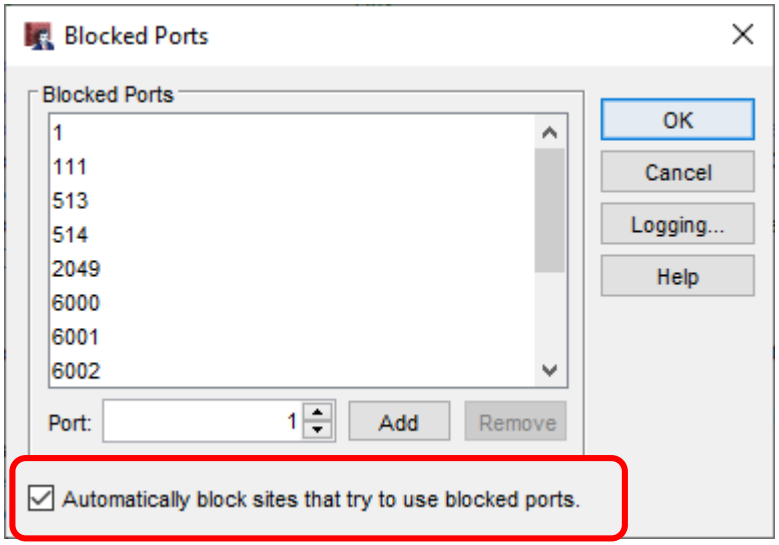
- IP in Port Scan blokada
- blokada za ves „nedefiniran promet“



Samodejno dodajanje - Autoblock

(Sprememba sistemske privzete obravnave)

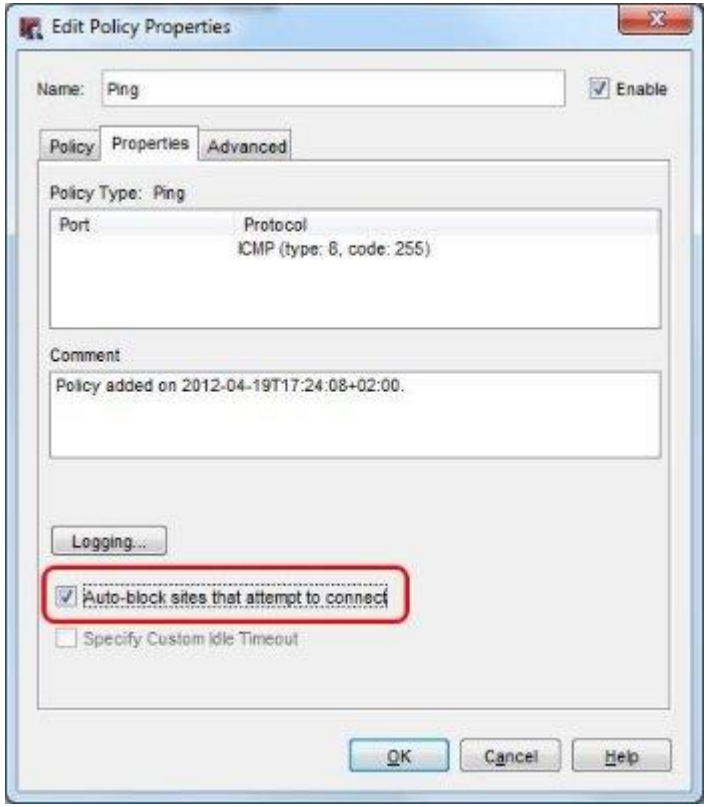
- Privzeti blokirani porti



Samodejno dodajanje - Autoblock

(Block akcija v pravilih)

- V vseh **DENY** pravilih požarne pregrade imamo možnost določiti, da se izvorni IP vpiše v blocklisto

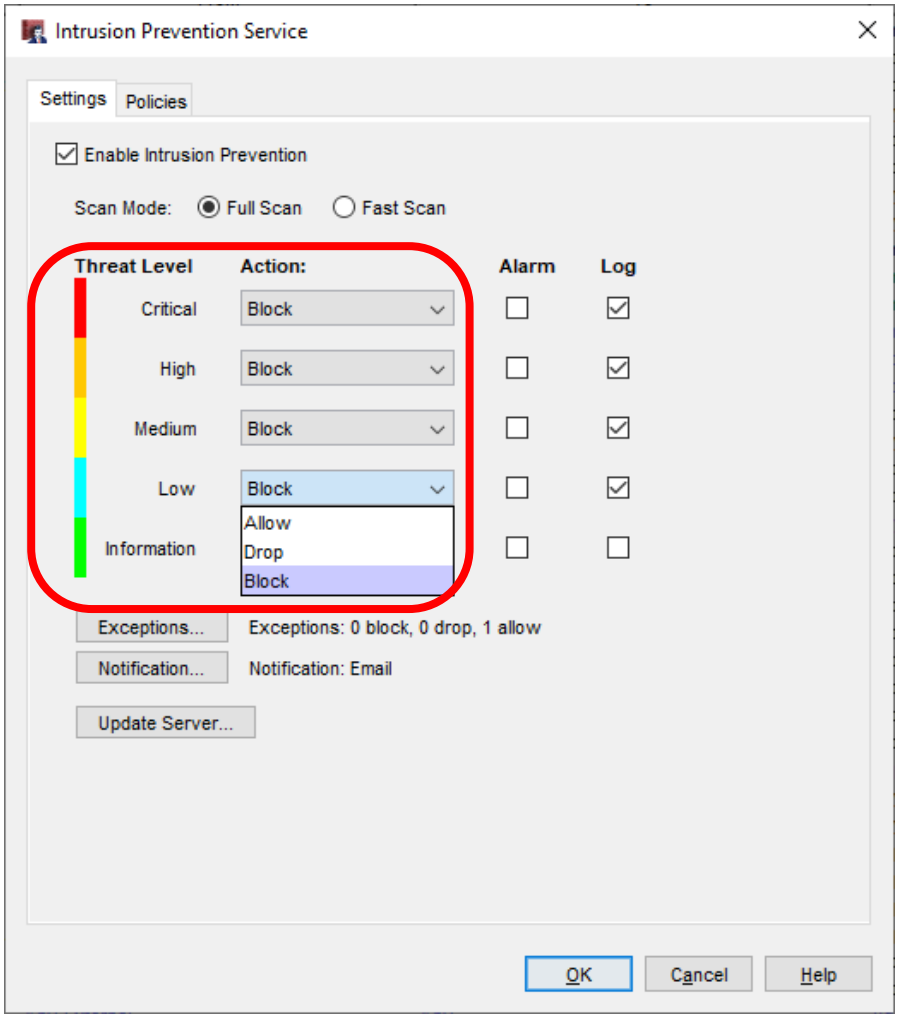


Samodejno dodajanje - Autoblock

(Block akcija v varnostnih storitvah)

- IPS zaznava grožnje

  Z določenim IP naslovom prekinemo ***vso*** *komunikacijo, ne le povezavo, ki je sprožila alarm!*

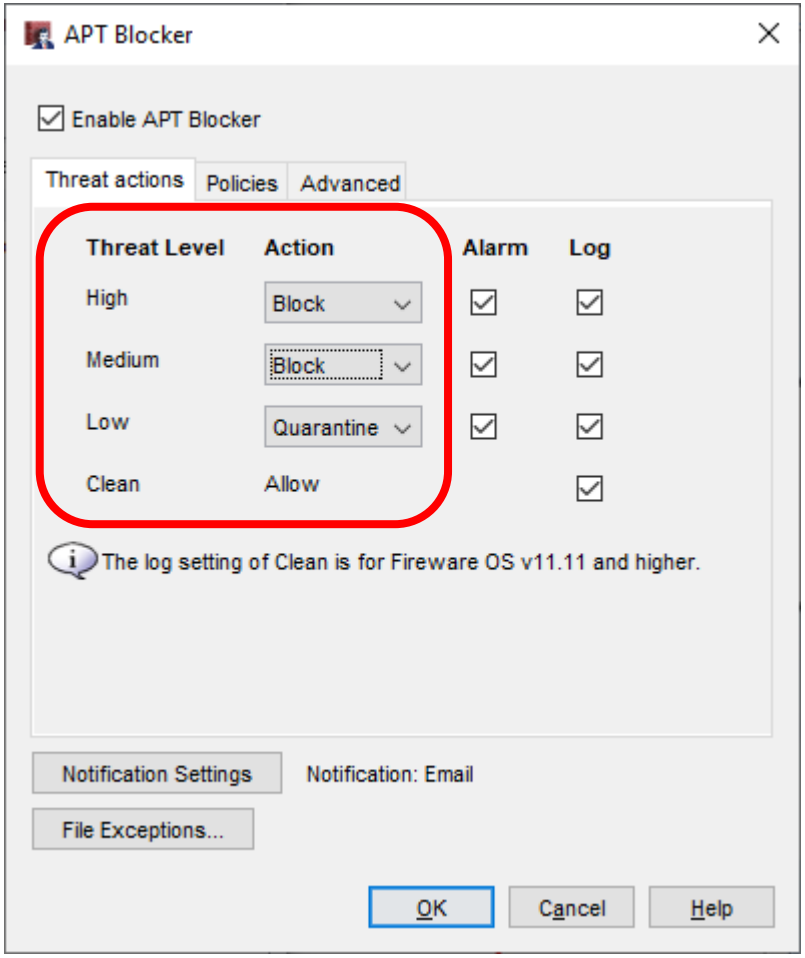


Samodejno dodajanje - Autoblock

(Block akcija v varnostnih storitvah)

- APT Blocker (sandbox analitika)

  Z določenim IP naslovom prekinemo ***vso*** *komunikacijo, ne le povezavo, ki je sprožila alarm!*



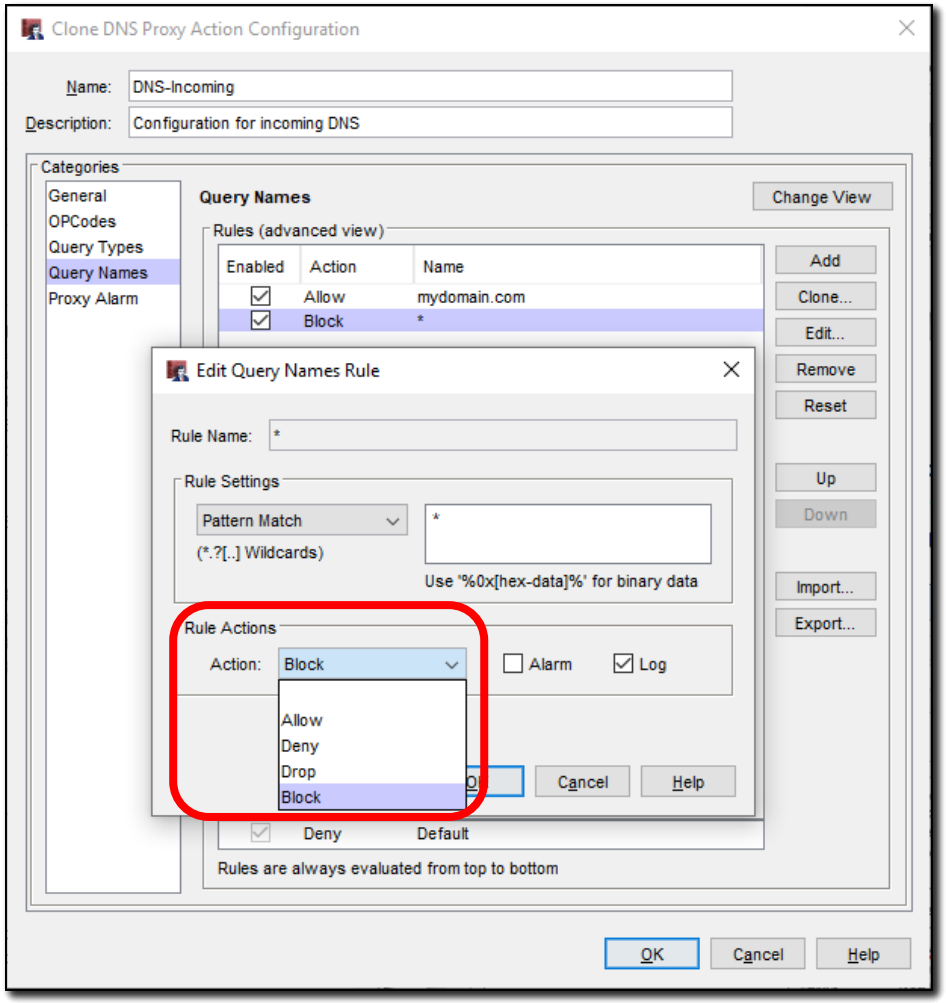
Blokiranje v Proxy pravilih

- Proxiji in ALG-ji pregledujejo promet na aplikativnem nivoju - DPI
- Velike razlike med proizvajalci – **testiraj!**
- Odkrivajo protokolske anomalije
- Omejujejo kritične aplikacijske parametre
- Preprečujejo posledice napak v konfiguraciji zalednih sistemov (DNS, WWW, SMTP,…)
- Dekriptirajo SSL promet za IPS in AV preverjanje

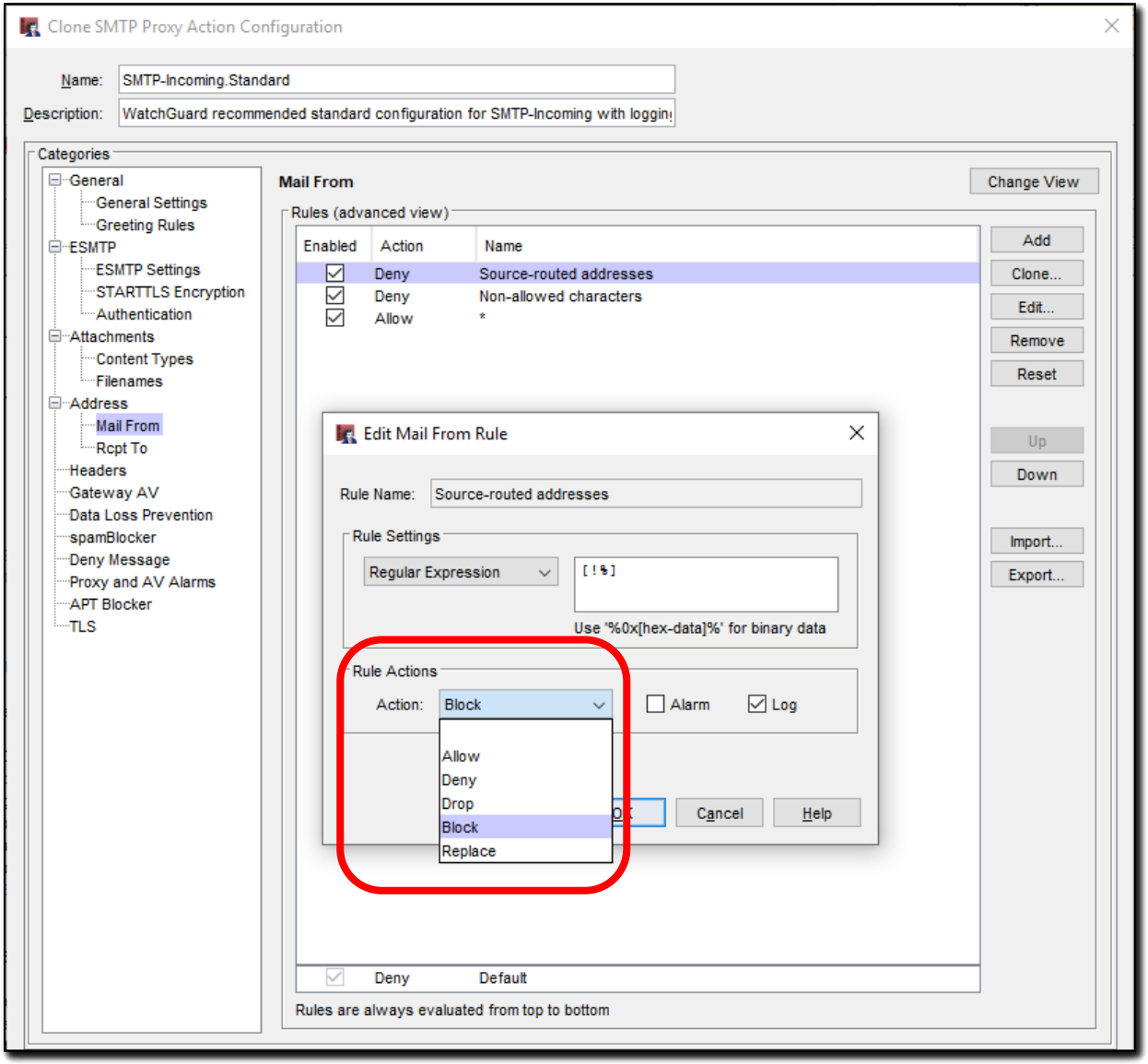
Blokiranje v Proxy pravilih

(DNS proxy)

- Varujemo lokalni DNS strežnik
- Varujemo DNS odjemalce
- Varujemo omrežje pred zlorabo DNS protokola



Blokiranje v Proxy pravilih



Blokiranje v Proxy pravilih

Clone SMTP Proxy Action Configuration

Name: SMTP-Incoming.Standard

Description: WatchGuard recommended standard configuration for SMTP-Incoming with loggin

Categories

- General
  - General Settings
  - Greeting Rules
- ESMTP
  - ESMTP Settings
  - STARTTLS Encryption
  - Authentication
- Attachments
  - Content Types
  - Filenames
- Address
  - Mail From
  - Rcpt To
- Headers
- Gateway AV
- Data Loss Prevention
- spamBlocker
- Deny Message
- Proxy and AV Alarms
- APT Blocker
- TLS

Gateway AV

Gateway AntiVirus settings are applied only when AV Scan is selected in the Action drop-down lists on the Content Types and Filenames rulesets.

☑ Enable Gateway AntiVirus

Actions

When a virus is detected

Quarantine: quarantine the email — ☐ Alarm ☑ Log this action

When a scan error occurs:

Lock: lock message content — ☐ Alarm ☑ Log this action

When content exceeds scan size limit (Fireware OS v12.0.1 and higher):

Allow: allow the email — ☐ Alarm ☑ Log this action

When content is encrypted (Fireware OS v12.0.1 and higher):

Allow: allow the email — ☐ Alarm ☑ Log this action

- **Allow:** allow the email
- **Lock:** lock message content
- **Remove:** remove message parts
- **Quarantine:** quarantine the email
- **Deny:** deny the email (Fireware OS v12.2.1 and higher)
- **Drop:** drop the connection immediately
- **Block:** drop the connection and auto-block the source

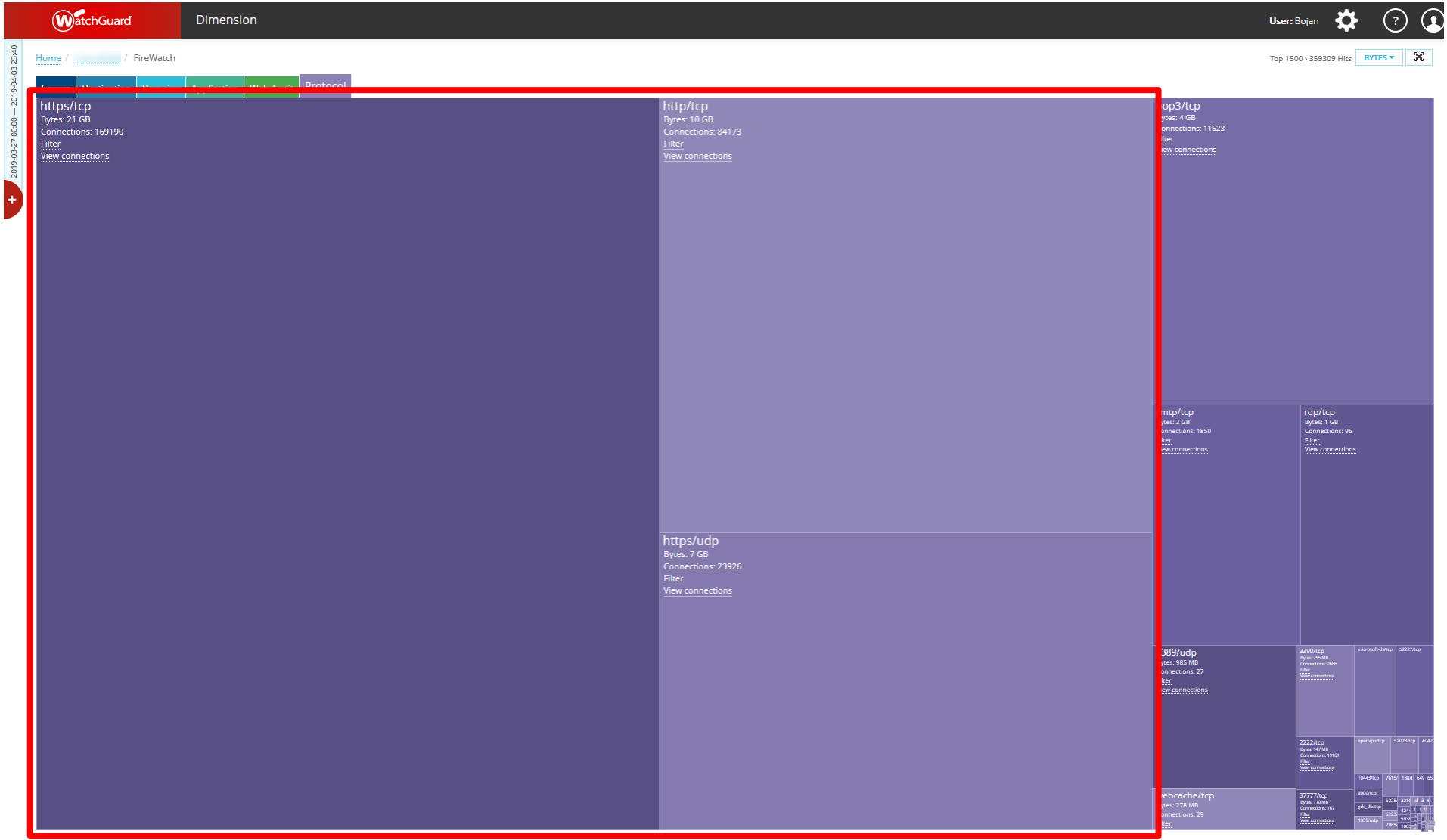
by APT Blocker. If you set the Gateway AntiVirus
to 10 MB in size.

Blokiranje v Proxy pravilih

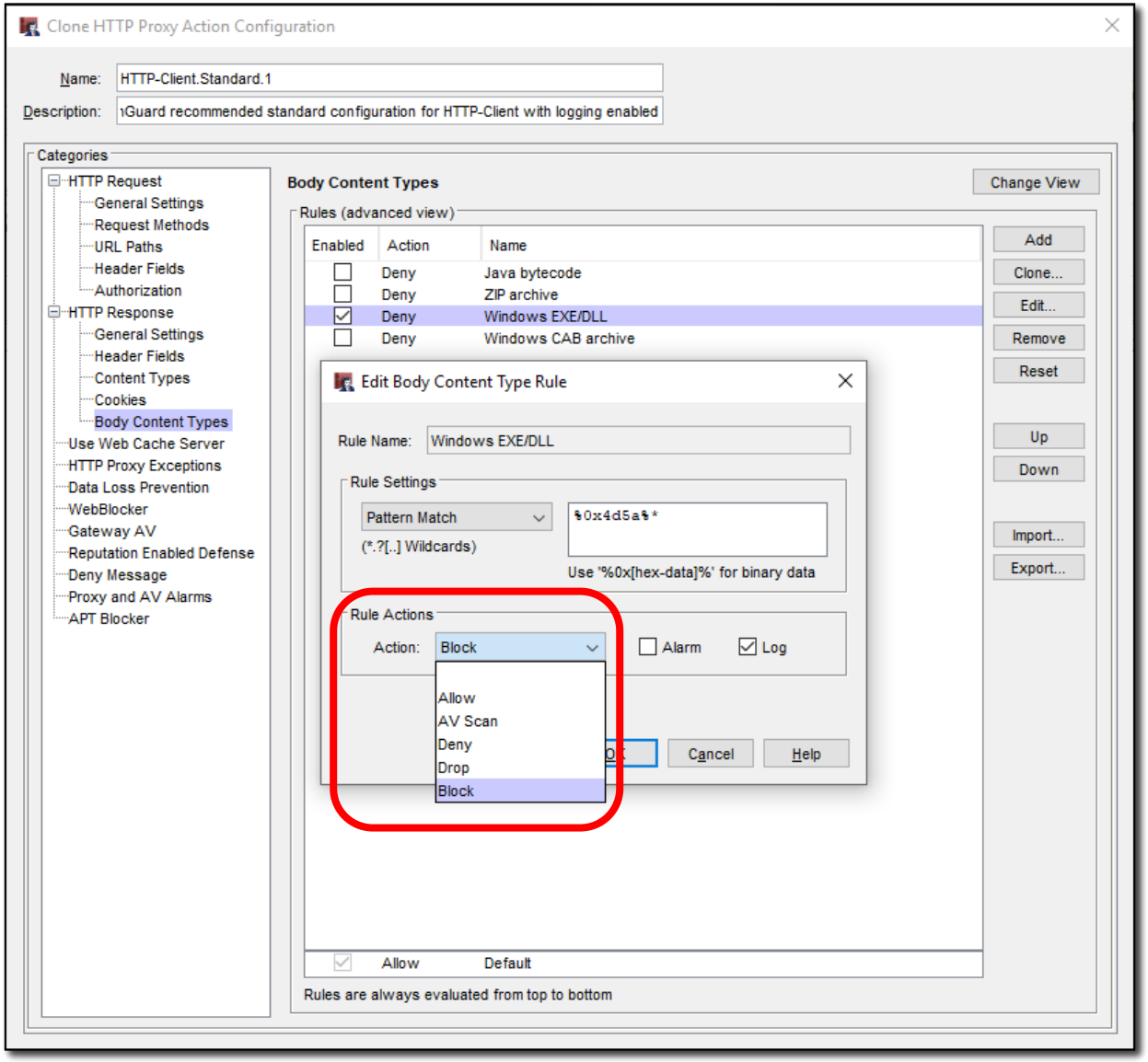
- Podobno kot varujemo lastni mail strežnik, varujemo tudi odhodne SMTP povezave
- Zelo podobno kot SMTP nadziramo tudi:
  - Pop3
  - Pop3(s)
  - Imap
  - Imap(s)

Blokiranje v Proxy pravilih

(HTTP proxy)



Blokiranje v Proxy pravilih



Blokiranje v Proxy pravilih

- Aplikacijski proxiji so na voljo za:
  - **DNS** (odjemalec & strežnik)
  - **HTTP(s)** (odjemalec & strežnik)
  - **SMTP** (odjemalec & strežnik)
  - **Pop3(s)** (odjemalec & strežnik)
  - **Imap(s)** (odjemalec & strežnik)
  - **FTP** (odjemalec & strežnik)
  - **SIP** (odjemalec)
  - **H.323** (odjemalec)

Rezultat

(Dimension Security Dashboard)

WatchGuard Dimension User: demo

2019-03-01 00:00 — 2019-03-02 00:00

Home / webdemo / Security Dashboard

Top Blocked Advanced Malware (APT)

View All

NAME	HITS
/d/CZ8SVw2r/770629/CoolGameMod.exe, /d/d1HMiibK/886895/ScreenSaver.exe, /d/sROJP...	3
/download.php?file_id:4088847256755021092100123&t:4088847256755021092100123	1

Top Blocked Clients

View All

NAME	BYTES	HITS
Hannah@example.com	23	7
10.99.1.103	0	5,222
AP200_20AP0579063FF	0	2,372
10.99.1.101	0	994
Rex@example.com	0	853
AP300_30AP02BB6AF40	0	813
guest-icfcq	0	654
10.99.1.100	0	531
Jessie@example.com	0	226
10.99.2.100	0	171

Top Blocked Destinations

View All

NAME	BYTES	HITS
52.200.252.136	23	1
10.99.1.255	0	2,545
4.2.2.2	0	1,783
255.255.255.255	0	765
23.209.11.156	0	588
192.168.130.80	0	241
63.232.60.117	0	215
192.168.130.81	0	207
216.115.208.230	0	110
172.25.1.100	0	94

Top Blocked URL Categories

View All

NAME	HITS
Sex	106
Suspicious Content	2

Top Blocked Applications

View All

NAME	HITS
XBOX	618
HTTP Proxy Server	118

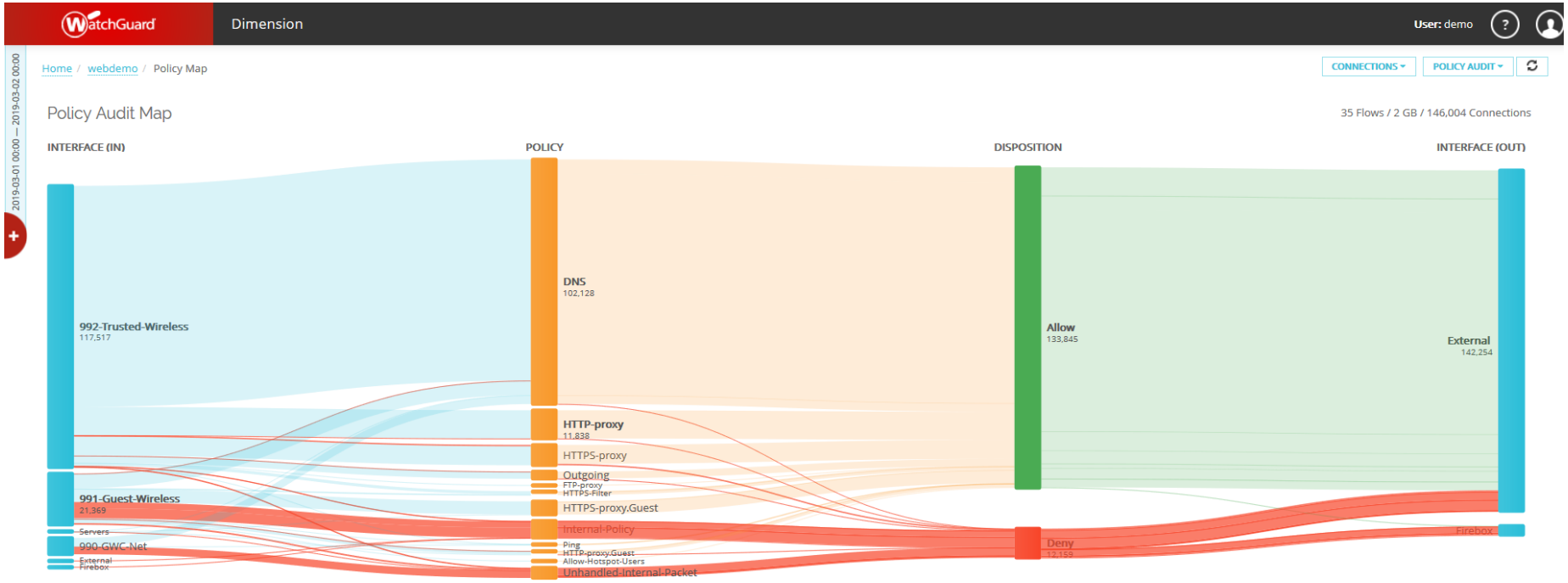
Top Blocked Application Categories

View All

NAME	HITS
Games	620
Bypass Proxies and Tunnels	182

Rezultat - grafično

(Dimension Policy Map)



Anonimizirani demo: https://demo-anon.watchguard.com

De-Anonimizirani demo: https://demo.watchguard.com

User: **demo** Password: **visibility**

Zaključek

- Večina proizvajalcev požarnih pregrad je aplikacijske proxije opustila pred leti ali jih nikoli ni uvedla
- Proxiji so pri večini proizvajalcev doživeli povratek z SSL dekripcijo (visoka degradacija performans, zelo omejene zmogljivosti)
- Čeprav prikazano temelji na WatchGuard rešitvi, to ne pomeni, da se ni možno prikazanemu pristopu približati tudi z drugimi rešitvami oz. kombinacijo njih.