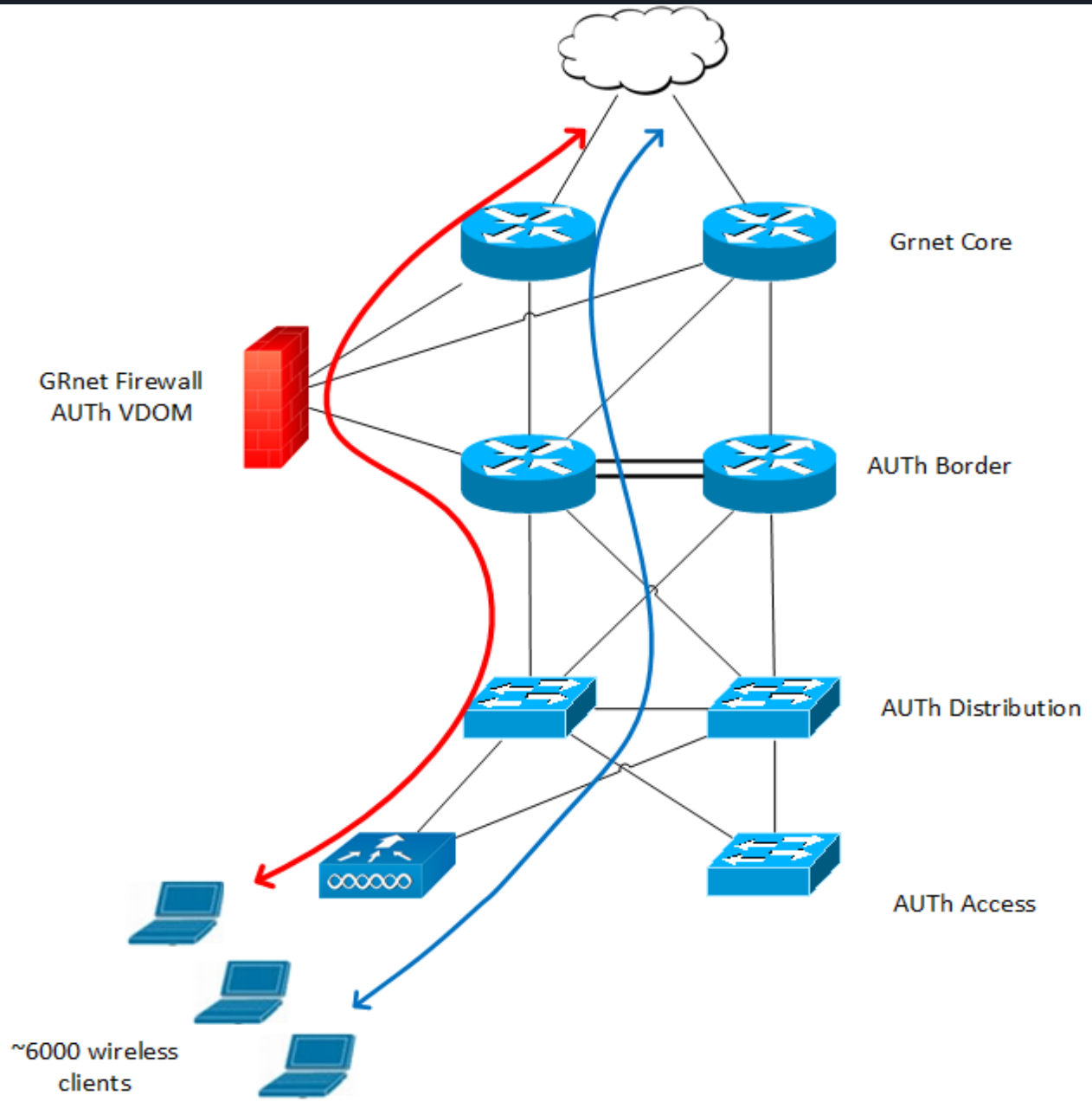
Firewall as a Service - Εφαρμογή στο ΑΠΘ

Γεώργιος Φωτιάδης
Κέντρο Ηλεκτρονικής Διακυβέρνησης ΑΠΘ

Agenda

- Υλοποίηση Firewall as a Service
- Δυνατότητες ρύθμισης
- Παρακολούθηση / αποτελέσματα
- Επόμενα βήματα

Τοπολογία


Grnet Core
GRnet Firewall
AUTh VDOM
AUTh Border
AUTh Distribution
AUTh Access
~6000 wireless
clients

Τοπολογία

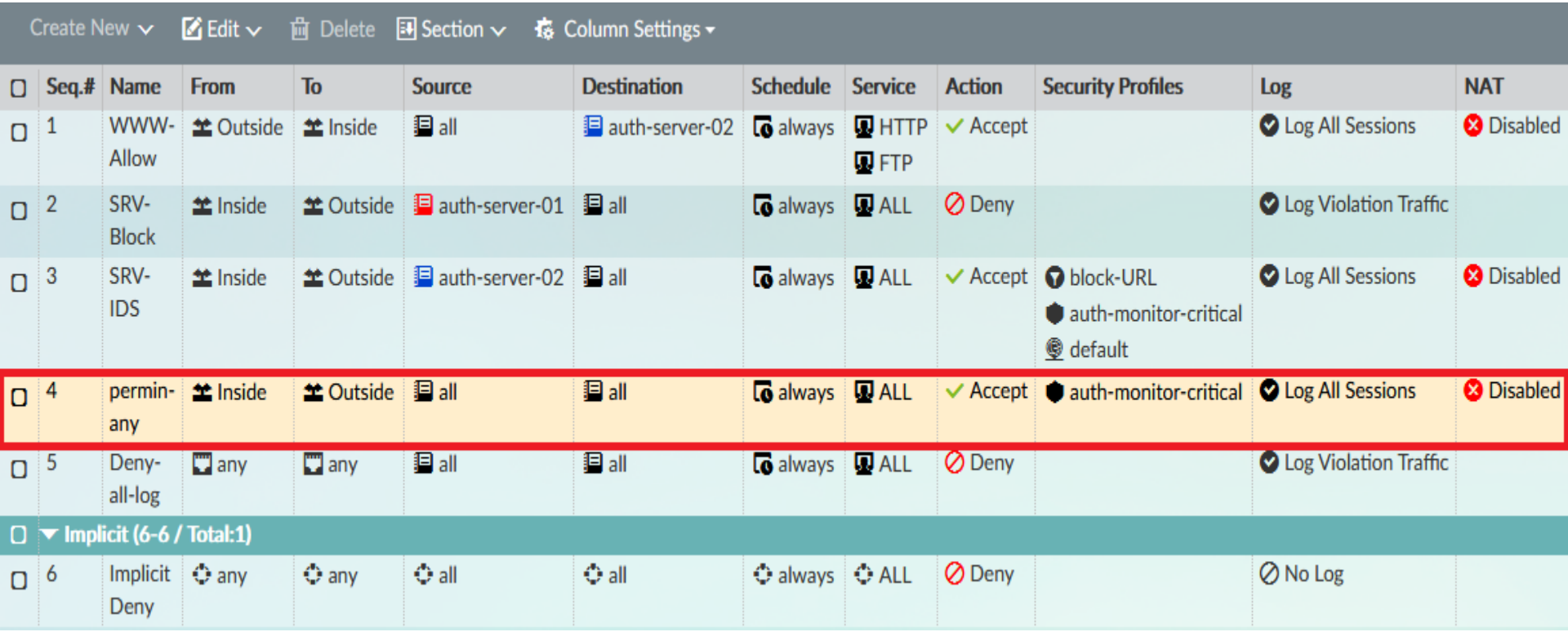
- Υλοποίηση:
  - Ένα νέο **L2VPN** το οποίο για τη σύνδεση του VDOM ΑΠΘ και του in-campus εξοπλισμού
  - **Policy-based routing** (ή dynamic routing) για δρομολόγηση της κίνησης προς το VDOM, μέσω του L2VPN
  - Ένα νέο **BGP peering** μεταξύ του Firewall VDOM ΑΠΘ (στο EIE) και του ΕΔΕΤ

Πλεονασμός (redundancy)

- Αξιοποίηση **2ου VDOM** και εφαρμογή configuration και στα δύο VDOMs
- Δημιουργία **2ου L2VPN** ή χρήση VPLS
- Αντικατάσταση policy-based routing με **dynamic routing**
- Redistribute ‘firewalled’ routes στο BGP του VDOM για ανακοίνωση στο ΕΔΕΤ

Βασικές ρυθμίσεις

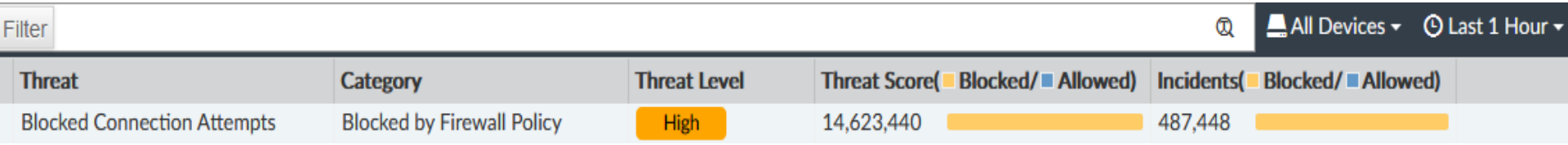
- Ρύθμιση μέσω **GUI** (Forti-Manager)



Seq.#	Name	From	To	Source	Destination	Schedule	Service	Action	Security Profiles	Log	NAT
1	WWW-Allow	Outside	Inside	all	auth-server-02	always	HTTP FTP	Accept		Log All Sessions	Disabled
2	SRV-Block	Inside	Outside	auth-server-01	all	always	ALL	Deny		Log Violation Traffic	
3	SRV-IDS	Inside	Outside	auth-server-02	all	always	ALL	Accept	block-URL auth-monitor-critical default	Log All Sessions	Disabled
4	permin-any	Inside	Outside	all	all	always	ALL	Accept	auth-monitor-critical	Log All Sessions	Disabled
5	Deny-all-log	any	any	all	all	always	ALL	Deny		Log Violation Traffic	
Implicit (6-6 / Total:1)											
6	Implicit Deny	any	any	all	all	always	ALL	Deny		No Log	

Εποπτεία συμβάντων

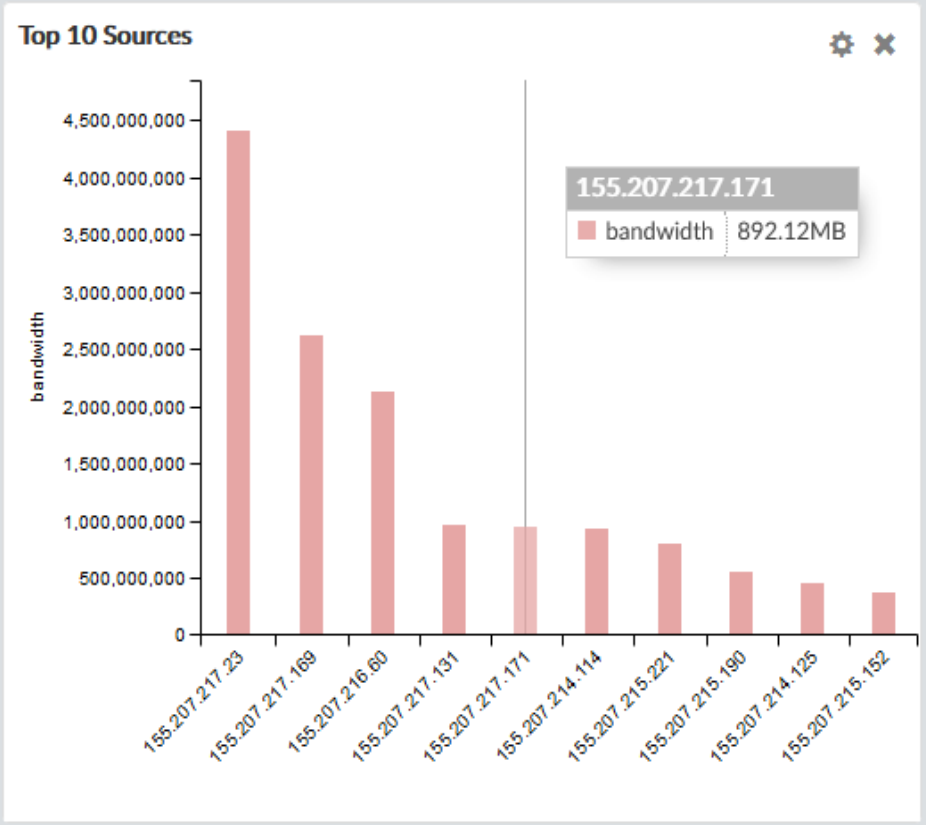
- Η εποπτεία γίνεται μέσω **GUI** (Forti-Analyzer)
  - Fortiview: Dashboard / εποπτικά διαγράμματα
  - Logview: Λεπτομερής ανάλυση περιστατικών
  - Reports: Δημιουργία reports

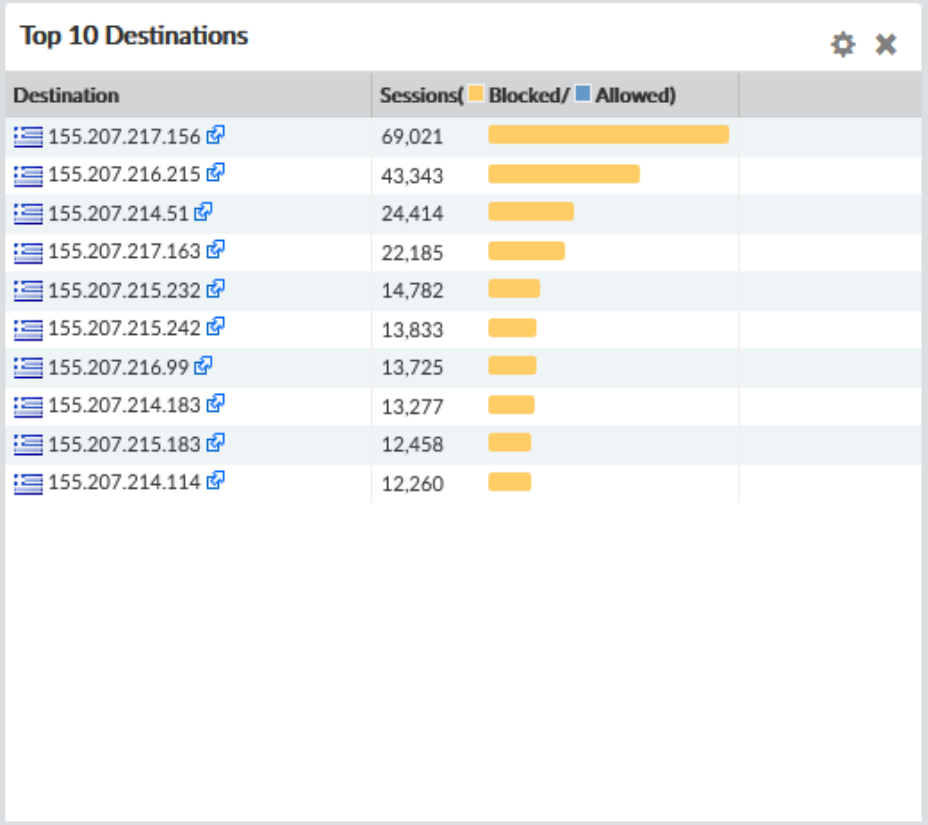


- Απαγόρευση συνδέσεων προς το δίκτυο του ΑΠΘ από κανόνες του firewall
- Καταγραφή **αποτυχημένων** συνδέσεων

Απεικόνιση συνδέσεων/κίνησης

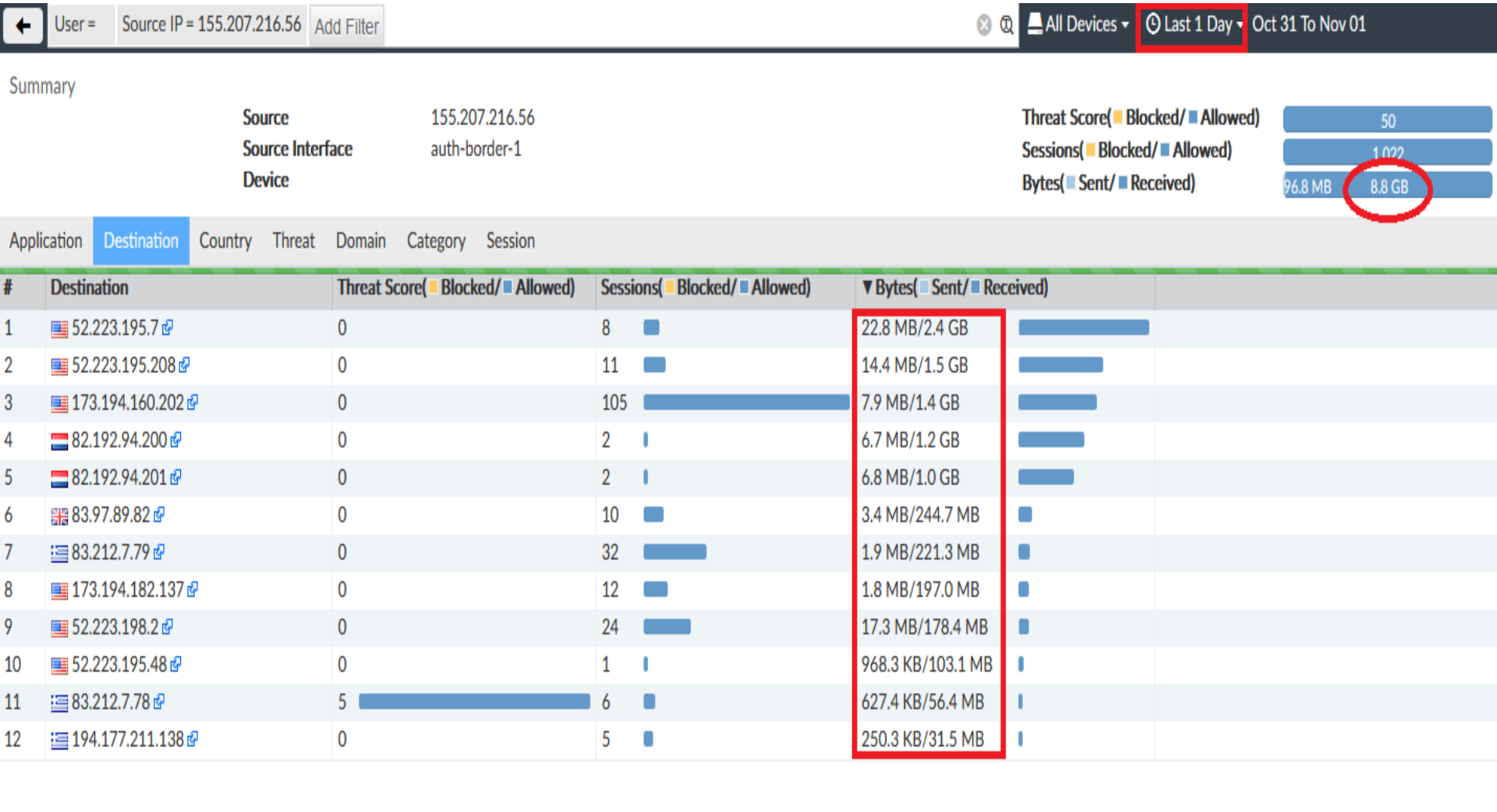
- Ευέλικτη κατηγοριοποίηση **βάση πολλαπλών κριτηρίων**:
  - Μεμονωμένων IP διευθύνσεων (source/destination)
  - Πλήθους συνδέσεων ή όγκου κίνησης
  - Τύπου εφαρμογής
  - Χώρας προέλευσης





Ανάλυση αποτελεσμάτων

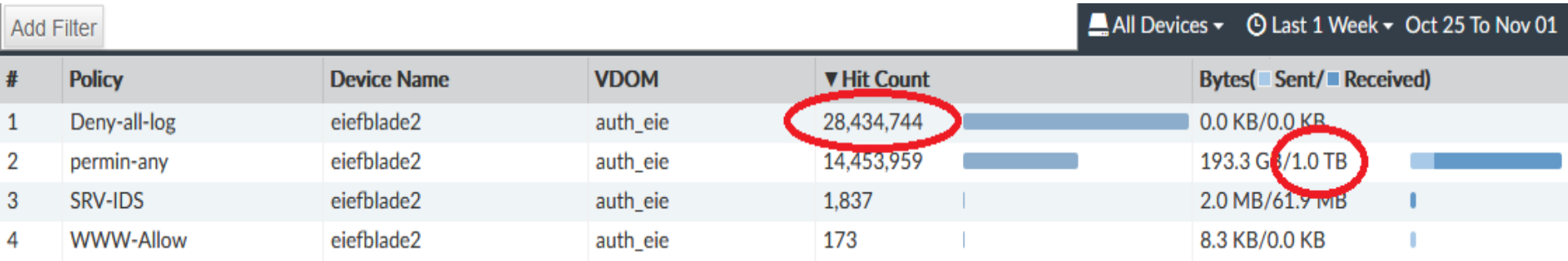
- **Ευέλικτη** και **γρήγορη** ανάλυση συμβάντων



#	Destination	Threat Score(Blocked/ Allowed)	Sessions(Blocked/ Allowed)	▼Bytes(Sent/ Received)
1	52.223.195.7	0	8	22.8 MB/2.4 GB
2	52.223.195.208	0	11	14.4 MB/1.5 GB
3	173.194.160.202	0	105	7.9 MB/1.4 GB
4	82.192.94.200	0	2	6.7 MB/1.2 GB
5	82.192.94.201	0	2	6.8 MB/1.0 GB
6	83.97.89.82	0	10	3.4 MB/244.7 MB
7	83.212.7.79	0	32	1.9 MB/221.3 MB
8	173.194.182.137	0	12	1.8 MB/197.0 MB
9	52.223.198.2	0	24	17.3 MB/178.4 MB
10	52.223.195.48	0	1	968.3 KB/103.1 MB
11	83.212.7.78	5	6	627.4 KB/56.4 MB
12	194.177.211.138	0	5	250.3 KB/31.5 MB

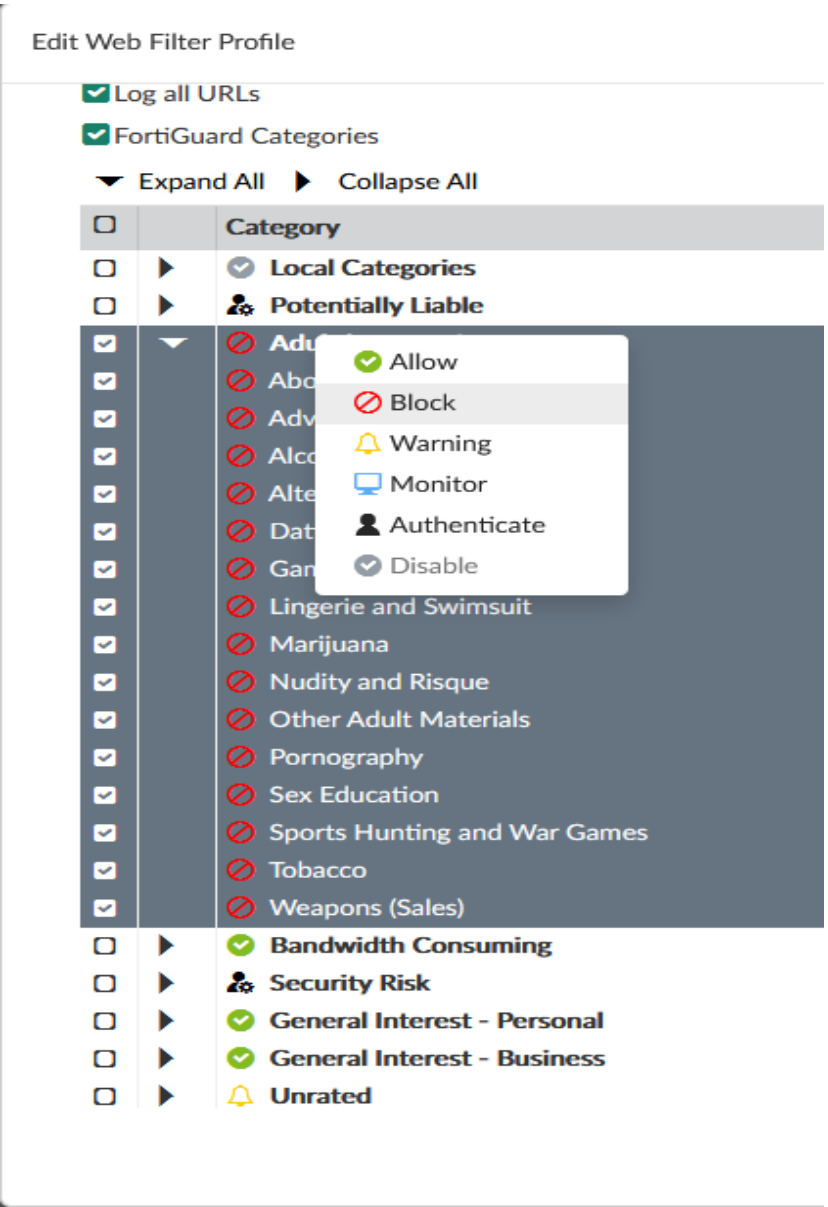
Εποπτεία κανόνων firewall

- Δυνατότητα εποπτείας των κανόνων του firewall, για καλύτερο **έλεγχο** και **troubleshooting**

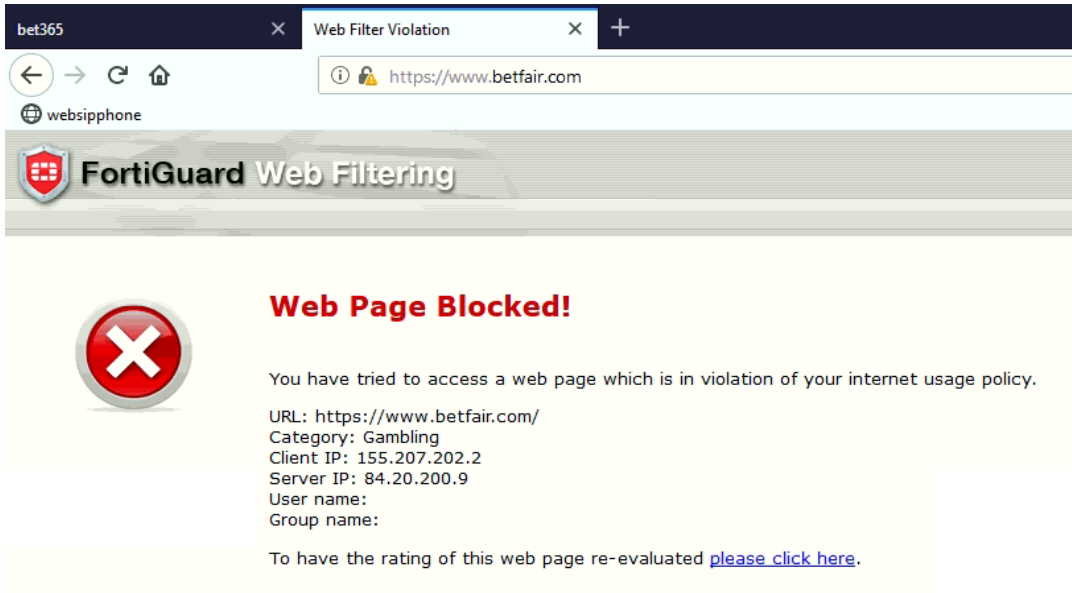


#	Policy	Device Name	VDOM	▼Hit Count	Bytes(Sent/ Received)
1	Deny-all-log	eiefblade2	auth_eie	28,434,744	0.0 KB/0.0 KB
2	permin-any	eiefblade2	auth_eie	14,453,959	193.3 GB/1.0 TB
3	SRV-IDS	eiefblade2	auth_eie	1,837	2.0 MB/61.9 MB
4	WWW-Allow	eiefblade2	auth_eie	173	8.3 KB/0.0 KB

URL filtering

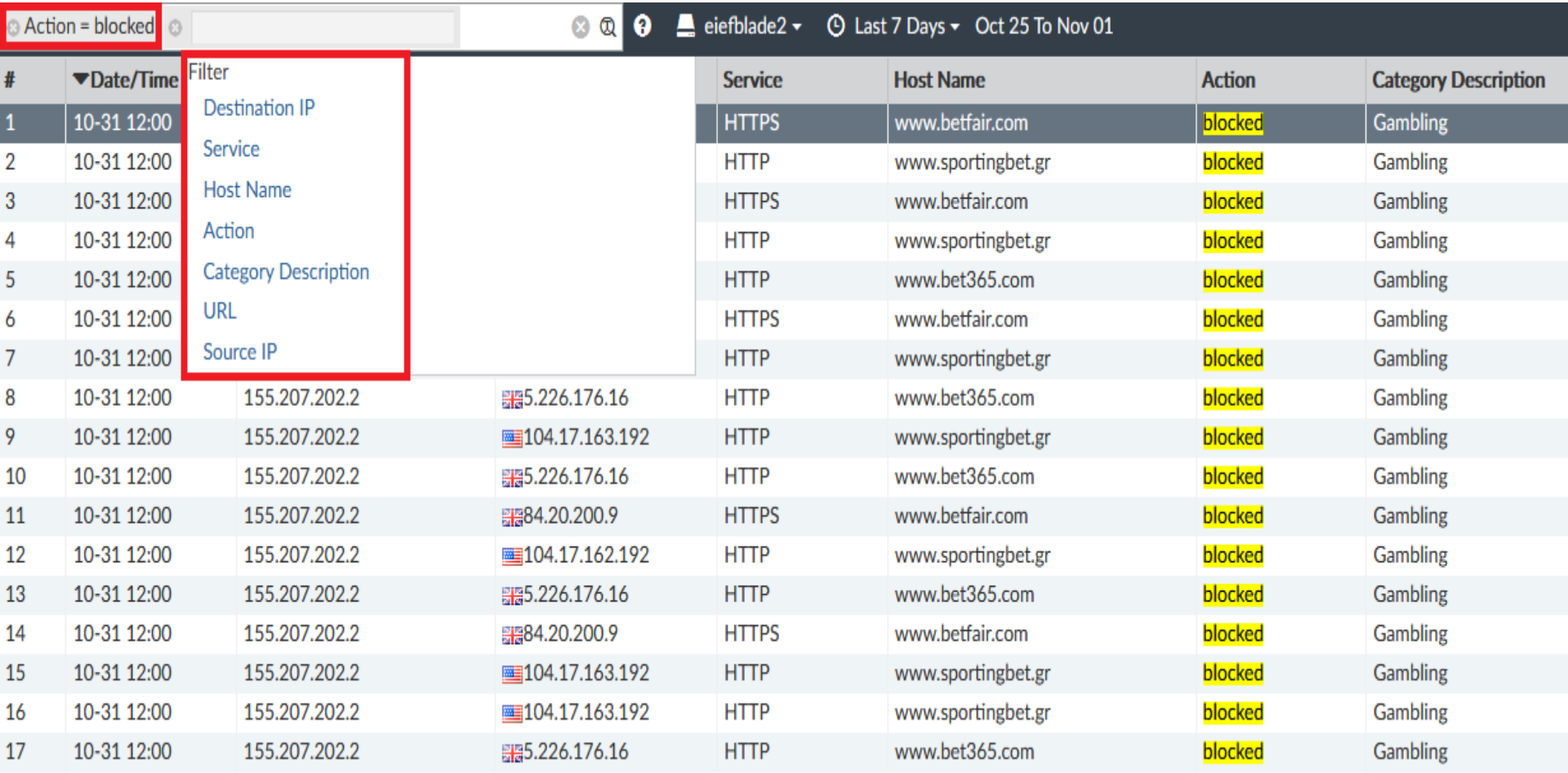


- Εφαρμογή:
  - Με βάση κατηγορία (category-based)
  - Σε συγκεκριμένους κανόνες firewall
  - Σε http και https κίνηση



URL filtering

- Επιβεβαίωση και παρακολούθηση μέσω του Forti-Analyzer



#	Date/Time			Service	Host Name	Action	Category Description
1	10-31 12:00			HTTPS	www.betfair.com	blocked	Gambling
2	10-31 12:00			HTTP	www.sportingbet.gr	blocked	Gambling
3	10-31 12:00			HTTPS	www.betfair.com	blocked	Gambling
4	10-31 12:00			HTTP	www.sportingbet.gr	blocked	Gambling
5	10-31 12:00			HTTP	www.bet365.com	blocked	Gambling
6	10-31 12:00			HTTPS	www.betfair.com	blocked	Gambling
7	10-31 12:00			HTTP	www.sportingbet.gr	blocked	Gambling
8	10-31 12:00	155.207.202.2	5.226.176.16	HTTP	www.bet365.com	blocked	Gambling
9	10-31 12:00	155.207.202.2	104.17.163.192	HTTP	www.sportingbet.gr	blocked	Gambling
10	10-31 12:00	155.207.202.2	5.226.176.16	HTTP	www.bet365.com	blocked	Gambling
11	10-31 12:00	155.207.202.2	84.20.200.9	HTTPS	www.betfair.com	blocked	Gambling
12	10-31 12:00	155.207.202.2	104.17.162.192	HTTP	www.sportingbet.gr	blocked	Gambling
13	10-31 12:00	155.207.202.2	5.226.176.16	HTTP	www.bet365.com	blocked	Gambling
14	10-31 12:00	155.207.202.2	84.20.200.9	HTTPS	www.betfair.com	blocked	Gambling
15	10-31 12:00	155.207.202.2	104.17.163.192	HTTP	www.sportingbet.gr	blocked	Gambling
16	10-31 12:00	155.207.202.2	104.17.163.192	HTTP	www.sportingbet.gr	blocked	Gambling
17	10-31 12:00	155.207.202.2	5.226.176.16	HTTP	www.bet365.com	blocked	Gambling

IDS / IPS

- Δυνατότητα για **signature-based deep packet inspection** (DPI)
  - Περισσότερες από **11.000** υπογραφές
- **Rated-based** filtering
- Ενέργειες
  - Allow
  - Block
  - Monitor
  - Reset

IDS / IPS

- **Low Severity**
  - TCP Overlapping Fragments (SSL – TCP/443)
  - TCP Out Of Range Timestamp (SSL – TCP/443)
- **Medium Severity**
  - TCP Split Handshake
  - Generic JavaScript Cryptocurrency Mining Script (HTTPS)
- **High Severity**
  - MS SMB Server Trans Peeking Data Information Disclosure (TCP/445)
  - HTTP URI SQL Injection (TCP/80)
- **Critical Severity**
  - Gozi Botnet (TCP/80,8000)
  - Andromeda Botnet (TCP/80)
  - Backdoor DoublePulsar (TCP/445)

Severity = critical | Destination IP = 155.207.215.239 | Add Filter | eiefblade2 | Last 7 Days | Oct 25 To Nov 01

#	Date/Time	Severity	Source	Destination IP	Action	Service
1	10-30 14:31	critical	37.187.31.189	155.207.215.239	detected	HTTP
2	10-30 12:29	critical	93.190.138.98	155.207.215.239	detected	HTTP
3	10-30 12:28	critical	80.93.90.27	155.207.215.239	detected	HTTP
4	10-30 10:39	critical	176.7.163.83	155.207.215.239	detected	HTTP
5	10-30 10:39	critical	93.190.138.56	155.207.215.239	detected	HTTP
6	10-30 10:39	critical	148.251.42.49	155.207.215.239	detected	HTTP
7	10-30 10:16	critical	109.238.12.28	155.207.215.239	detected	HTTP

Total logs for analytics: 2 days 11 hours. More | 50 Items per page | « ‹ 1 › | 0.013 Second

Security
- Level: alert
- Threat Level: critical
- Threat Score: 50

Source
- Device ID: FG-5KD3915800057
- Device Name: eiefblade2
- Source: 37.187.31.189
- Source Country: France
- Source IP: 37.187.31.189
- Source Interface: auth-border-1
- Source Port: 8000

Action
- Action: detected
- Policy ID: 1

Threat
- Attack ID: 25304
- Attack Name: Gozi.Botnet
- Incident Serial No.: 431871451
- Reference: https://fortiguard.com/encyclopedia/ips/25304
- Severity: critical

Others

General
- Direction: incoming
- Log ID: 0419016384
- Message: backdoor: Gozi.Botnet,
- Session ID: 404421272
- Time Stamp: 2018-10-30 14:31:48
- Virtual Domain: auth_eie

Destination
- Destination IP: 155.207.215.239
- Destination Interface: link-to-eier
- Destination Port: 49282

Application
- Profile: auth-monitor-critical
- Protocol: 6
- Service: HTTP

Type
- Event Type: signature
- Sub Type: ips
- Type: utm

The big picture

Add Filter

All Devices | Last 1 Day

#	Threat	Category	Threat Level	Threat Score(Blocked/ Allowed)	Incidents(Blocked/ Allowed)
1	Andromeda.Botnet	IPS	Critical	14,250	285
2	Mazben.Botnet	IPS	Critical	300	6
3	Blocked Connection Attempts	Blocked by Firewall Policy	High	70,135,650	2,337,855
4	www.sportingbet.gr	Gambling	High	3,810	127
5	www.bet365.com	Gambling	High	1,440	48
6	www.betfair.com	Gambling	High	1,350	45
7	Generic.JavaScript.Cryptocurrency.Mining.Script	IPS	Medium	100	10
8	TCP.Split.Handshake	IPS	Medium	80	8
9	Failed Connection Attempts	Failed Connection Attempts	Low	664,380	132,876
10	Traceroute	IPS: CVE-1999-0525	Low	86,075	17,215
11	TCP.Out.Of.Range.Timestamp	IPS: CVE-2005-0356	Low	2,990	598
12	TCP.Overlapping.Fragments	IPS	Low	2,540	508
13	UDP.PORT0	IPS	Low	600	120
14	IMAP.Unknown.Reply	IPS	Low	110	22
15	TCP.Stealth.Activity	IPS	Low	40	8
16	HTTP.Null.Session	IPS	Low	5	1

Επόμενα βήματα για το ΑΠΘ

- Αυτή τη στιγμή δρομολογούνται **650 wireless clients** με όγκο κίνησης **150 Mbps**

- Στόχος η δρομολόγηση κίνησης **6.000 wireless clients** με όγκο κίνησης **~1 Gbps**
  - Εφαρμογή **NAT** για τους wireless clients
- **Αυτοματοποίηση** αποτελεσμάτων IDS και αυτόματη **ειδοποίηση χρηστών**
- Υλοποίηση **πλεονασμού** στην τοπολογία

Συμπεράσματα

- **Day-1** deployment
- Ευκολία στην **παραμετροποίηση** και **διαχείριση**
- Δυνατότητα **πιλοτικής εφαρμογής**, μέσω επιλεκτικής δρομολόγησης της κίνησης
- Δυνατότητα **πλεονασμού** (redundancy) στην τοπολογία
- Μεγάλες δυνατότητες **εποπτείας** και **εξαγωγής ποιοτικών/ποσοτικών αποτελεσμάτων**

- Τέλος -

Ευχαριστώ!