ΥΠΗΡΕΣΙΕΣ ΑΣΦΑΛΕΙΑΣ ΔΙΚΤΥΟΥ

Τάσος Καραλιώτας – ΕΔΕΤ

Agenda

- Υπηρεσίες δικτυακής ασφάλειας παρεχόμενες από το ΕΔΕΤ
- Persistent firewall
  - Τυπικό στιγμιότυπο χρήσης
  - Χαρακτηριστικά
  - Υποδομή
  - Ωριμότητα
- Dynamic incident mitigation
  - Firewall on demand – FoD
  - FoD – next generation
    - Concept
    - Δομικά στοιχεία

Υπηρεσίες Ασφάλειας

- Παροχή υπηρεσιών ασφάλειας από το ΕΔΕΤ στους φορείς του
- Δύο κατηγορίες αναγκών
  1. Μόνιμο firewalling + threat protection για τους φορείς
  2. Dynamic incident mitigation για την αντιμετώπιση περιστατικών ασφάλειας – εστιασμένες σε επιθέσεις denial of service (dos).

Αντίστοιχα δύο διαφορετικά flavors

- Persistent firewall
- Dynamic Firewall

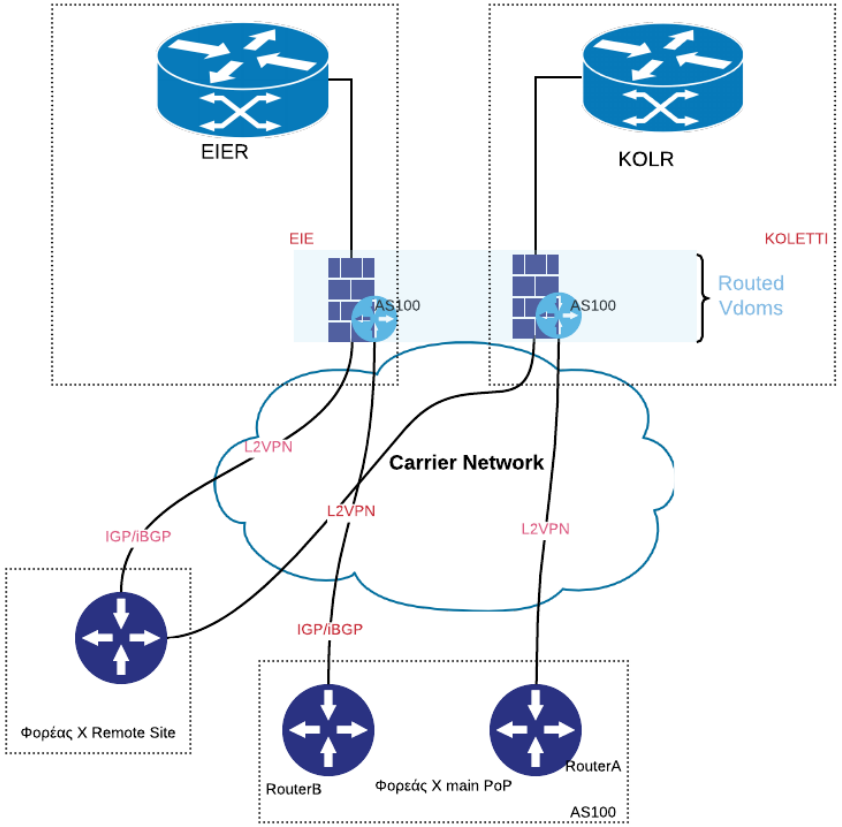
Persistent Firewall ...in alpha testing

Σκοπός: κάλυψη αναγκών των φορέων σε υπηρεσίες ασφαλείας για την κίνηση τους με τον έξω κόσμο

Βασικά στοιχεία

- Virtual firewall instances (vendor's parlance: vdom)
- In line με την κίνηση του φορέα
  - Προσοχή στην ασύμμετρη κίνηση!
- Ενταγμένο στο routing domain του φορέα
  - Με χρήση VPN υπηρεσιών του carrier δικτύου
  - Ενδεχόμενη μεταφορά των peerings με το ΕΔΕΤ στα virtual firewalls
- Εφαρμογή από πριν συγκεκριμένων κανόνων ασφάλειας
- Εξαγωγή στατιστικών χρήσης

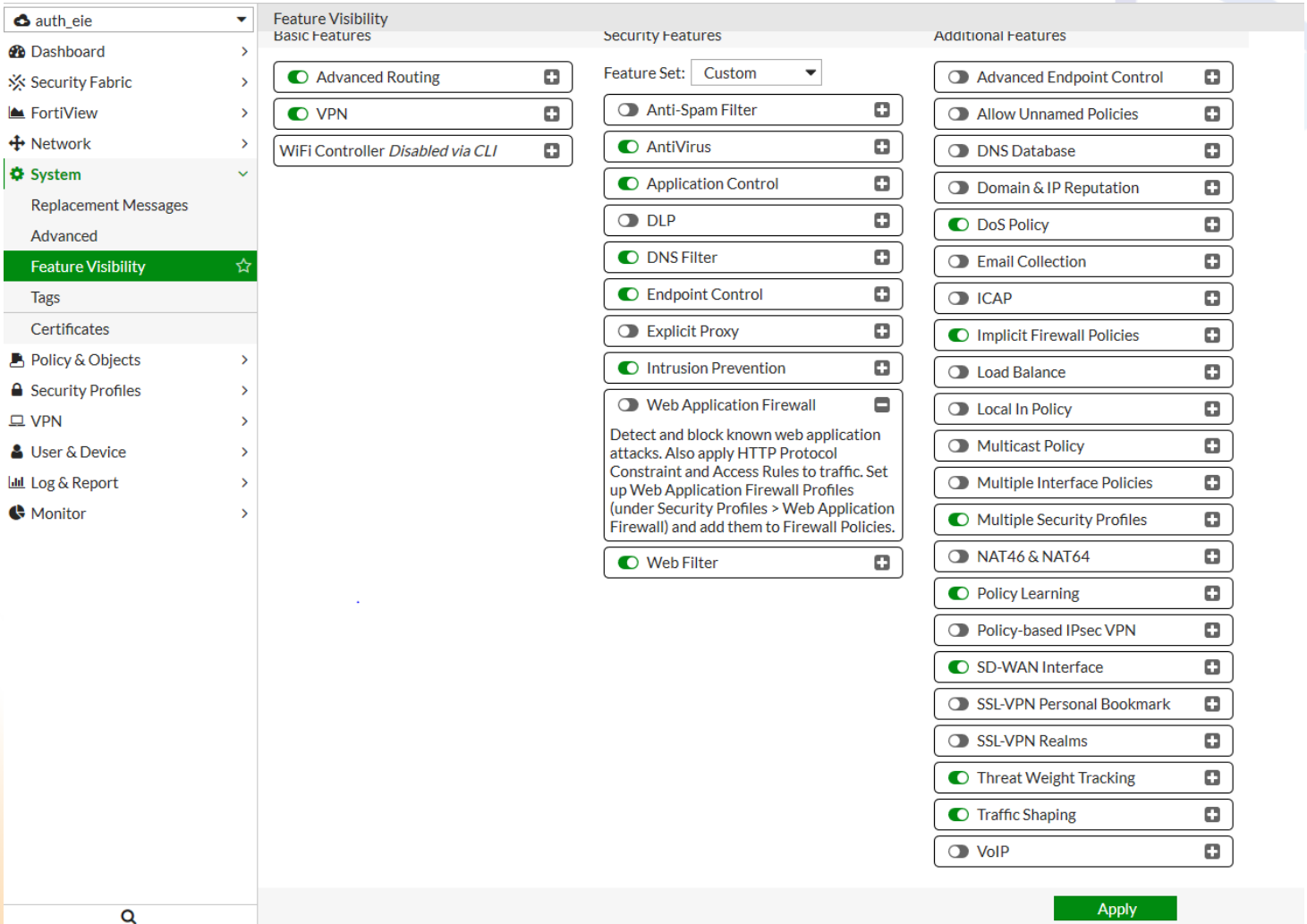
Typical service instance



Χαρακτηριστικά

- 2 modes λειτουργίας για τα virtual firewalls
  - Routed / NAT. Το firewall είναι ένα στοιχείο επιπέδου 3 (recommended)
  - Transparent. Το firewall εξομοιώνει λειτουργικά ένα καλώδιο
    - Έως 2 Interfaces
    - Bad scaling για φορείς με πολλαπλά sites
- Security features
  - Statefull firewalling
  - IPS
  - Antivirus
  - Web Filtering
  - Inspection mode
    - Flow-based
    - Proxy

Features supported



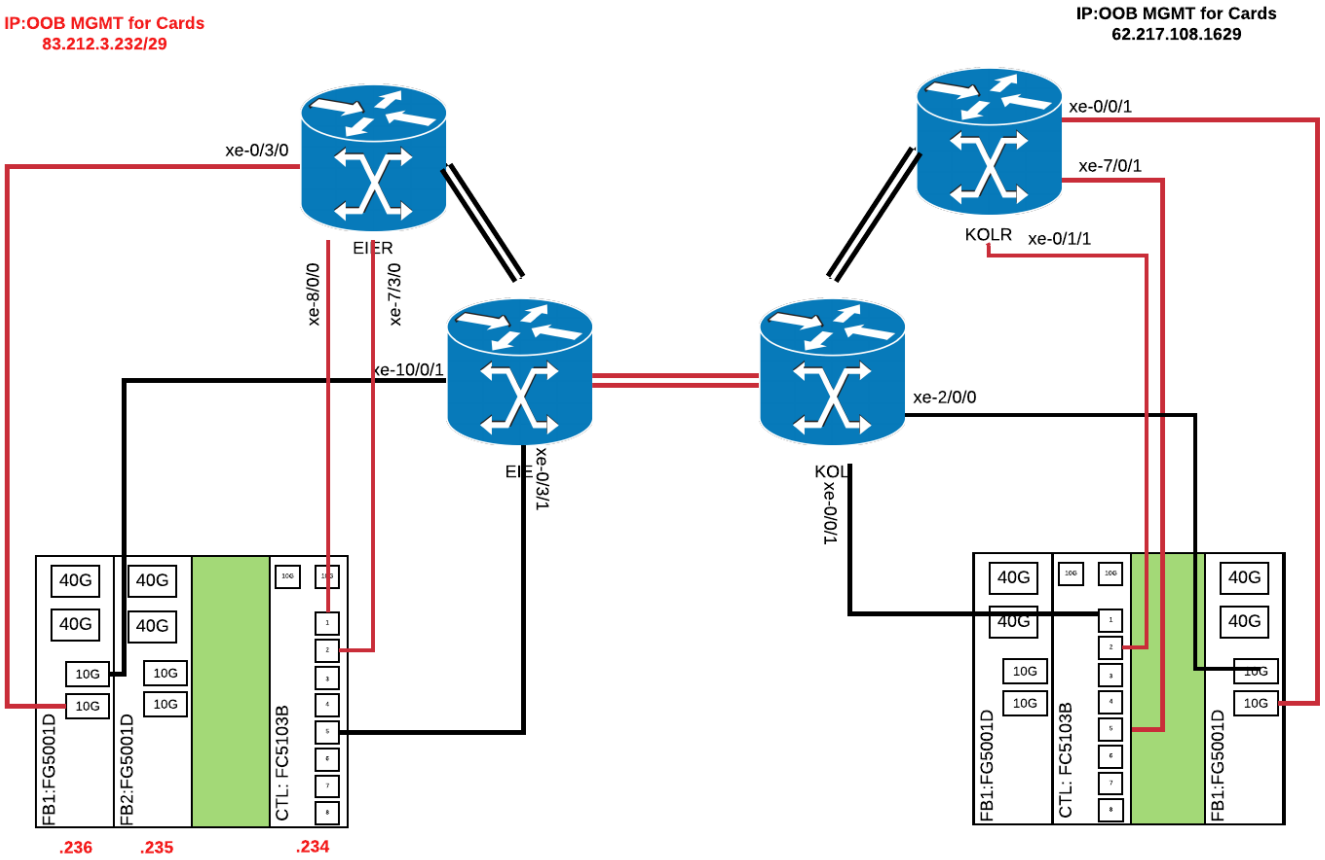
Χαρακτηριστικά

- Πολλαπλοί τρόποι πρόσβασης
  - Fortimanager
    - Multitenant Web console for managing lots of Vdoms
  - CLI
  - HW web GUI
- Security Console
  - Fortianalyzer
- Authentication/Authorization
  - LDAP ...work in progress...
  - Radius/Proxy Radius
- Resource exhaustion protection
  - Ορισμός Quota ανά instance – to be tested more με stresstesting

Υποδομή

- Διαστασιολόγηση
  - 4 blades in total – κατανεμημένα σε 2 chassis
  - 40Gbps firewalling throughput / blade
  - 23M concurrent sessions / blade
  - IPS throughput :13Gbps / blade
  - NGFW throughput: 10Gbps
  - 25 Vdom licenses per blade = total 100 service instances
    - Soft limit, supported vdom number can be increased
  - Subscriptions μέχρι και 2020

Υποδομή


IP:OOB MGMT for Cards
83.212.3.232/29
IP:OOB MGMT for Cards
62.217.108.1629
xe-0/3/0
xe-8/0/0
xe-7/3/0
xe-10/0/1
xe-0/3/1
xe-2/0/0
xe-0/0/1
xe-7/0/1
xe-0/1/1
KOLR
xe-0/0/1
40G
10G
FB1:FG5001D
FB2:FG5001D
CTL: FC5103B
.236
.235
.234

Ωριμότητα

- Alpha testing
- Δοκιμαστικές υλοποιήσεις με
  - ΑΠΘ
  - Πανεπιστήμιο Αιγαίου
  - Πανεπιστήμιο Κρήτης
  - Γρ. ΕΔΕΤ
- Work in progress…
  - Ολοκλήρωση & δοκιμές του σχήματος πιστοποίησης
  - Σχεδιασμός και δοκιμή High Availability Setup (session syncing)
  - Διαστασιολόγηση των απαιτούμενων licenses και προμήθεια (ανάλογα με την αποδοχή)
  - Ανάπτυξη «ΕΔΕΤ» user interface
  - Feedback από τις δοκιμαστικές υλοποιήσεις και ενσωμάτωση
- Δηλώστε ενδιαφέρον!
  - Επικοινωνήστε μαζί μου είτε με τον Αντρέα Πολυράκη (ΑΜ)

Ανίχνευση & Αντιμετώπιση περιστατικών ασφαλείας

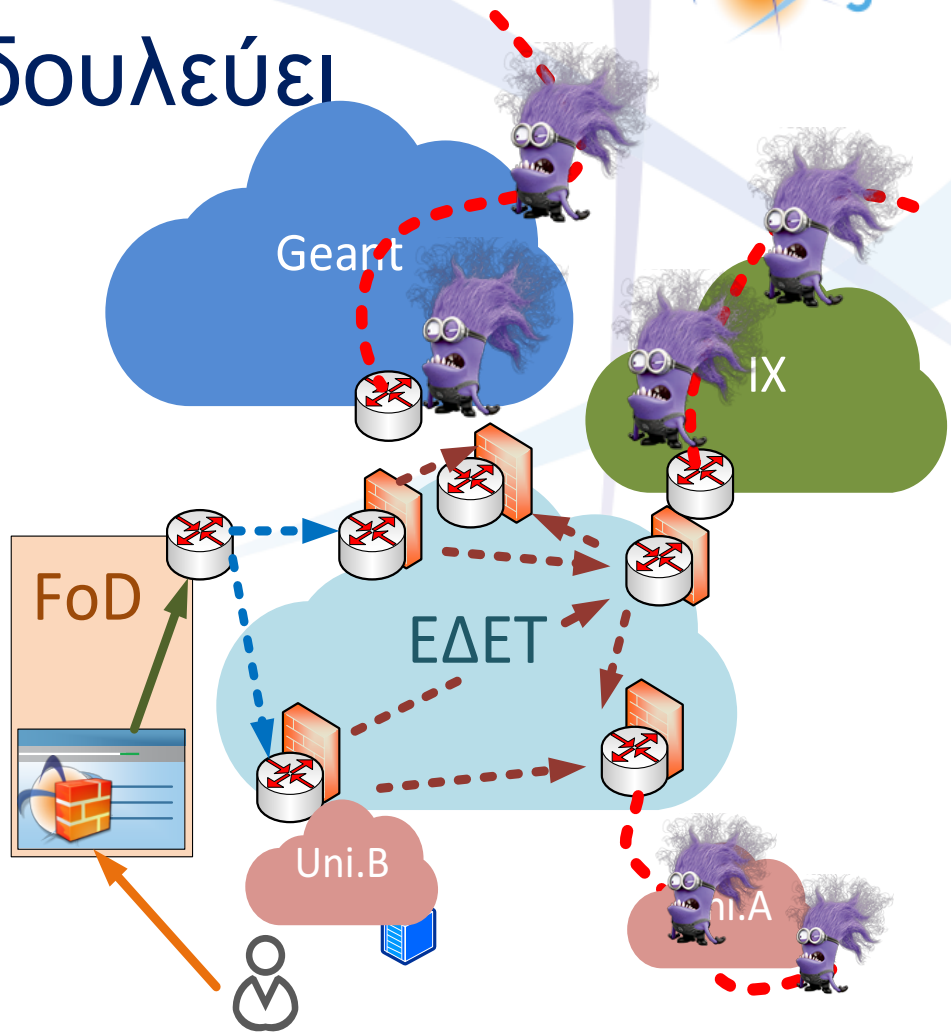
- Στόχος: Η παροχή δυναμικών εργαλείων στους φορείς του ΕΔΕΤ ώστε να ανιχνεύουν και να αντιμετωπίζουν επιθέσεις άρνησης υπηρεσίας (Denial of service)
- Αρχικά ως προσπάθεια για την ανάπτυξη εσωτερικών εργαλείων
- Ανίχνευση
  - flow collector & nfdump
  - home made tools that detected anomalies
    - rady (github.com/grnet/rady) – στατιστική ανάλυση των rrd αρχείων
  - **Netscout's Arbor PeakFlow SP**
  - Δοκιμές άλλων επιλογών flow monitoring (kentik)

Firewall on Demand

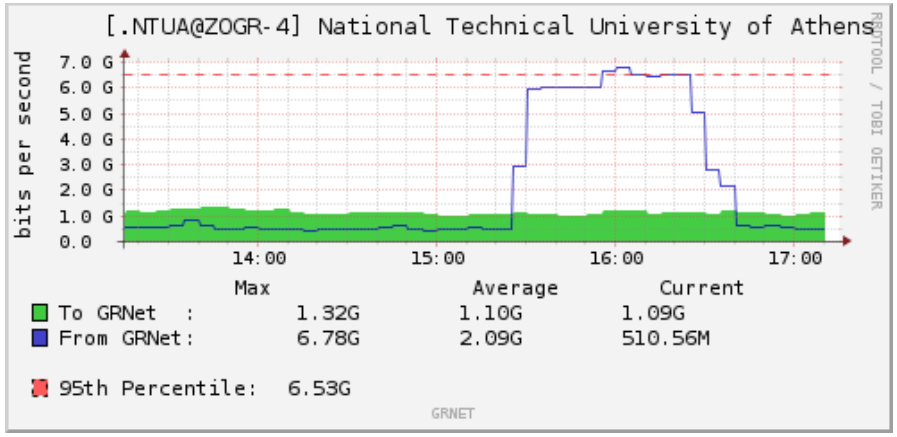
- Πρόσβαση μέσω του https://fod.grnet.gr
- Υπηρεσία σε παραγωγή από το 2011
- Πιστοποίηση δύο επιπέδων
  - Μέσω της ομοσπονδίας ΕΔΕΤ ➔ Specific attribute
  - Manual authorization
- Ο φορέας εισάγει κανόνες που αφορούν (destination) το ip space που του ανήκει
  - action: discard or rate-limit
- Dissemination flow rules over BGP
  - (BGP flowspec – RFC5575 & RFC7674)

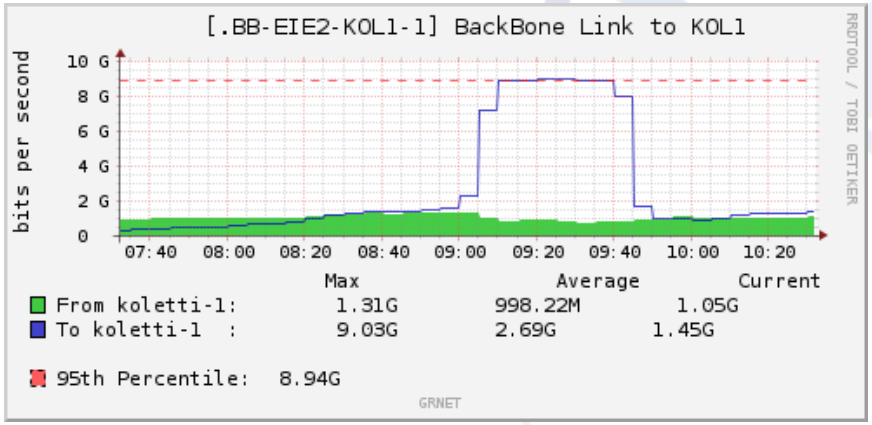
Πώς δουλεύει

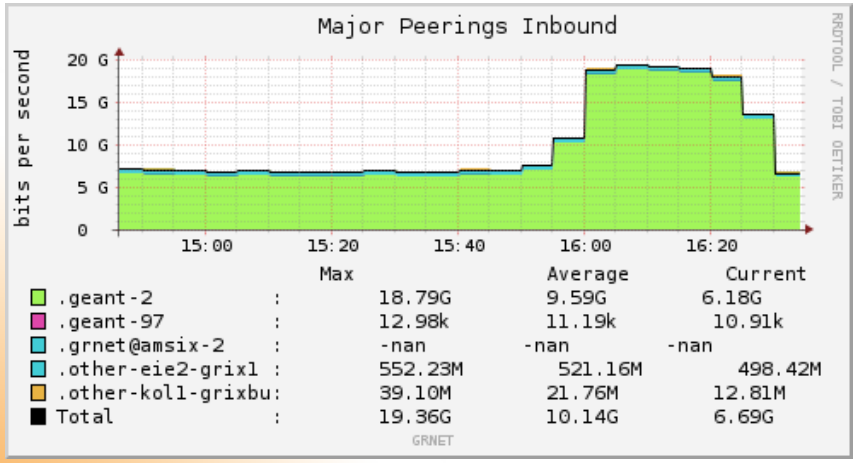
- Το NOC του φορέα εισέρχεται στο fod.grnet.gr & περιγράφει flows και actions
- Destination address ελέγχεται σε σχέση με το IP space του φορέα
- Το flow rule διαφημίζεται από ειδικό δρομολογητή
- Δυναμικά firewall filters εφαρμόζονται σε όλους τους δρομολογητές
- Η επίθεση αντιμετωπίζεται στην είσοδο του δικτύου
- Με το τέλος της επίθεσης: Είτε τα rules "κατεβαίνουν" μέσω του εργαλείου είτε αφήνονται να εκπνεύσουν

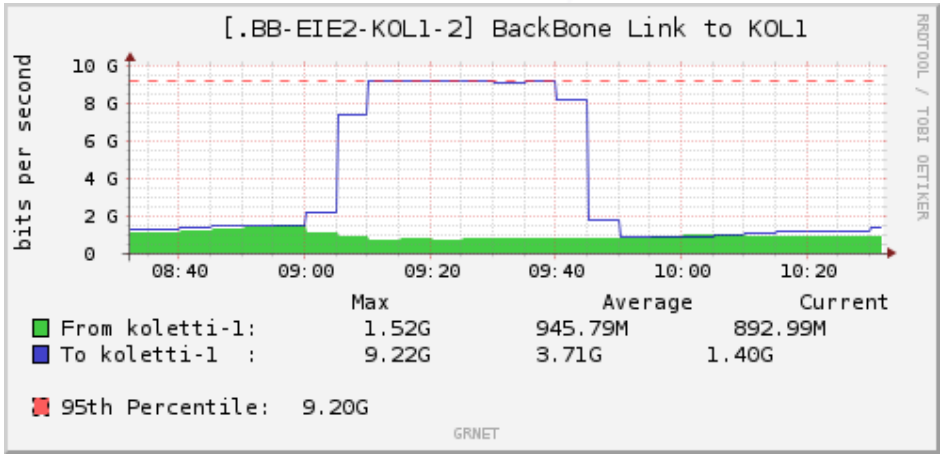


Δουλεύει!


[.NTUA@ZOGR-4] National Technical University of Athens
bits per second
7.0 G
6.0 G
5.0 G
4.0 G
3.0 G
2.0 G
1.0 G
0.0
14:00
15:00
16:00
17:00
Max
Average
Current
To GRNet : 1.32G 1.10G 1.09G
From GRNet: 6.78G 2.09G 510.56M
95th Percentile: 6.53G
GRNET
RRDTOOL / TOBI OETIKER


[.BB-EIE2-KOL1-1] BackBone Link to KOL1
bits per second
10 G
8 G
6 G
4 G
2 G
0
07:40
08:00
08:20
08:40
09:00
09:20
09:40
10:00
10:20
Max
Average
Current
From koletti-1: 1.31G 998.22M 1.05G
To koletti-1 : 9.03G 2.69G 1.45G
95th Percentile: 8.94G
GRNET
RRDTOOL / TOBI OETIKER


Major Peerings Inbound
bits per second
20 G
15 G
10 G
5 G
0
15:00
15:20
15:40
16:00
16:20
Max
Average
Current
.geant-2 : 18.79G 9.59G 6.18G
.geant-97 : 12.98k 11.19k 10.91k
.grnet@amsix-2 : -nan -nan -nan
.other-eie2-grix1 : 552.23M 521.16M 498.42M
.other-kol1-grixbu: 39.10M 21.76M 12.81M
Total : 19.36G 10.14G 6.69G
GRNET
RRDTOOL / TOBI OETIKER


[.BB-EIE2-KOL1-2] BackBone Link to KOL1
bits per second
10 G
8 G
6 G
4 G
2 G
0
08:40
09:00
09:20
09:40
10:00
10:20
Max
Average
Current
From koletti-1: 1.52G 945.79M 892.99M
To koletti-1 : 9.22G 3.71G 1.40G
95th Percentile: 9.20G
GRNET
RRDTOOL / TOBI OETIKER

FoD NG

- Ιδέα: Αντί να επιβάλεις μια συγκεκριμένη πράξη σε όλη την κίνηση (malicious or normal) που αφορά ένα subnet ή ένα tuple (subnet + port) αναδρομολόγησε (off ramp) την «ύποπτη κίνηση» μέσα από μια έξυπνη συσκευή ώστε να εφαρμοστούν εργαλεία ανίχνευσης (IDS) και καταστολής της «κακής» κίνησης
- Συνεργασία με εργαλείο ανίχνευσης επιθέσεων
- Η «καθαρή κίνηση» = «ύποπτη» – «κακή» επιστρέφει στο δίκτυο ώστε να δρομολογηθεί πίσω στον προορισμό της (on ramp)
- User initiated and configured

Δομικά στοιχεία

- Ανίχνευση
  - Arbor Peakflow or similar tool that may detect network anomalies
    - Network anomaly = network behavior that deviates a pre-calculated profile
- Αλληλεπίδραση με τον χρήστη
  - Ενημέρωση του φορέα (alerting)
  - Ο φορέας ενεργοποιεί την διαδικασία αντιμετώπισης
  - Scrubber box
    - Κονσόλα εφαρμογής κανόνων
    - Κονσόλα εμφάνισης της επεξεργασίας των logs
- Back Office
  - Χρήση δικτυακού αυτοματισμού (ansible)
    - Ανά-δρομολόγηση ύποπτης κίνησης
    - Δρομολόγηση της «καθαρισμένης» κίνησης στον τελικό προορισμό
  - Χρήση device & NMS APIs
    - Δυναμική δημιουργία short-lived virtual firewalls

Δομικά στοιχεία

- Ανίχνευση
  - Arbor Peakflow or similar tool that may detect net… anomalies
    - Network anomaly = network behavior that d… -calculated profile
- Αλληλεπίδραση με τον χρήστη
  - Ενημέρωση του φορέα (alerting)
  - Ο φορέας ενεργοποιεί την διαδ… ωπισης
  - Scrubber box
    - Κονσόλα εφαρμο…
    - Κονσόλα εμ… εργασίας των logs
- Back Office
  - Χρήση … οματισμού (ansible)
    - Ανα… γηση ύποπτης κίνησης
    - Δρομο… γηση της «καθαρισμένης» κίνησης στον τελικό προορισμό
  - Χρήση device & NMS APIs
    - Δυναμική δημιουργία short-lived virtual firewalls

Technology pilot
some components have been implemented but there is NOT a full working prototype yet

20 ΧΡΟΝΙΑ ΕΔΕΤ

grnet

ΗΦΑΙΣΤΟΣ

Σας ευχαριστώ! Ερωτήσεις?

Ευρωπαϊκή Ένωση
Ευρωπαϊκό Ταμείο Περιφερειακής Ανάπτυξης

ΕΠΑνΕΚ 2014-2020
ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
ΑΝΤΑΓΩΝΙΣΤΙΚΟΤΗΤΑ • ΕΠΙΧΕΙΡΗΜΑΤΙΚΟΤΗΤΑ • ΚΑΙΝΟΤΟΜΙΑ

ΕΣΠΑ 2014-2020
ανάπτυξη - εργασία - αλληλεγγύη

Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης