ΣΤΗΡΙΖΩ | Υποστήριξη Ψηφιακού Σχολείου και νέες υπηρεσίες Πανελλήνιου Σχολικού Δικτύου

Επιχειρησιακό Πρόγραμμα: «ΕΚΠΑΙΔΕΥΣΗ ΚΑΙ ΔΙΑ ΒΙΟΥ ΜΑΘΗΣΗ» 2007-2013

ΠΡΑΞΗ: «ΣΤΗΡΙΖΩ – Οριζόντιο Έργο Υποστήριξης Σχολείων, Εκπαιδευτικών και Μαθητών στο Δρόμο για το ΨΗΦΙΑΚΟ ΣΧΟΛΕΙΟ, νέες υπηρεσίες Πανελλήνιου Σχολικού Δικτύου και Στήριξη του ΨΗΦΙΑΚΟΥ ΣΧΟΛΕΙΟΥ (ΟΡΙΖΟΝΤΙΑ ΔΡΑΣΗ)»

ΔΡΑΣΗ Α2: Βασικές (κρίσιμες) υπηρεσίες ΠΣΔ

εσίας
ού

Κατάσταση Έκδοσης	**Υπό έγκριση από ΙΤΥΕ**
Ημερομηνία	**30/7/2012**
Περιγραφή Αρχείου	
Συμπράττων Φορέας	**ΕΠΙΣΕΥ**
Υπεύθυνος Παραδοτέου	**Δρ. Βασίλειος Χατζηγιαννάκης**
Αριθμός Σελίδων	
Ημ/νια παραλαβής από Φορέα	**30/7/2012**
Ημ/νια παραλαβής από ΙΤΥΕ	

Ινστιτούτο Τεχνολογίας Υπολογιστών και Εκδόσεων «Διόφαντος» (ΙΤΥΕ)

ΙΤΥΕ "ΔΙΟΦΑΝΤΟΣ" Ινστιτούτο Τεχνολογίας Υπολογιστών & Εκδόσεων

Ευρωπαϊκή Ένωση Ευρωπαϊκό Κοινωνικό Ταμείο

ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΕΚΠΑΙΔΕΥΣΗ ΚΑΙ ΔΙΑ ΒΙΟΥ ΜΑΘΗΣΗ
επένδυση στην κοινωνία της γνώσης
ΥΠΟΥΡΓΕΙΟ ΠΑΙΔΕΙΑΣ & ΘΡΗΣΚΕΥΜΑΤΩΝ, ΠΟΛΙΤΙΣΜΟΥ & ΑΘΛΗΤΙΣΜΟΥ
ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

ΕΣΠΑ 2007-2013 Πρόγραμμα για την ανάπτυξη ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΩΝΙΚΟ ΤΑΜΕΙΟ

Ομαδα Εκπονησης Παραδοτεου

1. **Καθ. Ευσταθιος Συκας**
2. **Δρ. Δημητριος Καλογερας**
3. **Δρ. Βασιλειος Χατζηγιαννακης**
4. **Παναγιωτης Χριστιας**

1. ΓΕΝΙΚΗ ΠΕΡΙΓΡΑΦΗ

Η υπηρεσία ελέγχου περιεχομένου του Πανελλήνιου Σχολικού Δικτύου (ΠΣΔ) έχει σκοπό την προστασία των ανήλικων χρηστών από σελίδες με ακατάλληλο περιεχόμενο απαγορεύοντας την πρόσβαση σε αυτές. Η απαγόρευση της πρόσβασης γίνεται σε κεντρικό σημείο του δικτύου, εφαρμόζεται για όλους συνολικά τους χρήστες του ΠΣΔ και αφορά σελίδες με περιεχόμενο όπως πορνογραφία, βία, ναρκωτικά, τυχερά παιγνίδια κλπ. Το σύνολο των ακατάλληλων σελίδων διατηρείται σε βάση δεδομένων και επικαιροποιείται τακτικά τόσο από ανάλογες βάσεις δεδομένων που διατίθενται δωρεάν στο διαδίκτυο, όσο και από τους ίδιους τους χρήστες του ΠΣΔ.

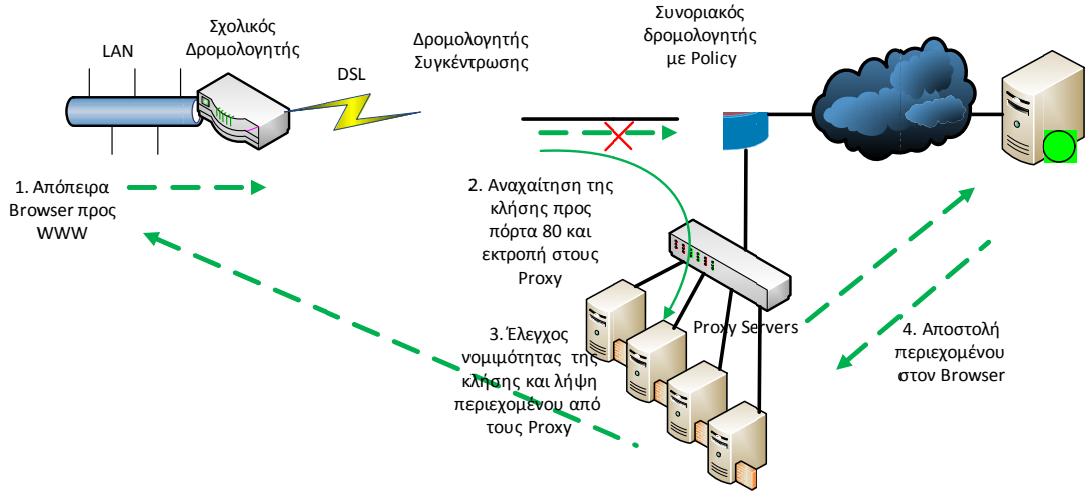
Η παρούσα μελέτη εξετάζει την τρέχουσα μορφή της υπηρεσίας και προτείνει βελτιώσεις και αναβαθμίσεις που μπορούν να γίνουν σε αυτήν στα πλαίσια του έργου «ΣΤΗΡΙΖΩ».

2. ΠΕΡΙΓΡΑΦΗ ΤΡΕΧΟΥΣΑΣ ΜΟΡΦΗΣ ΥΠΗΡΕΣΙΑΣ

Η τρέχουσα μορφή της υπηρεσίας περιεχομένου υλοποιείται στον κεντρικό κόμβο λειτουργίας του ΠΣΔ στην Αθήνα. Εκεί βρίσκεται ο συνοριακός δρομολογητής του ΠΣΔ, η σύνδεση του ΠΣΔ με τον πάροχό του (ΕΔΕΤ) και καταλήγουν όλες οι γραμμές κορμού του.

Ο συνοριακός δρομολογητής αναδρομολογεί αυτομάτως τις αιτήσεις HTTP των χρηστών του ΠΣΔ σε μια συστοιχία εξυπηρετητών με τη χρήση της τεχνολογίας Cisco IP policy. Στους εξυπηρετητές λειτουργεί το λογισμικό Squid ως transparent proxy server αναχαιτίζοντας με διαφανή τρόπο τις αιτήσεις των χρηστών. Οι χρήστες, δηλαδή, του ΠΣΔ δεν αντιλαμβάνονται την ύπαρξη του proxy server, ούτε χρειάζεται να προχωρήσουν σε ρύθμισή του στους φυλλομετρητές τους (web browsers). Η καταλληλότητα ή όχι του περιεχομένου που ζητούν οι χρήστες κρίνεται από το λογισμικό SquidGuard, το οποίο διατηρεί βάση δεδομένων με ακατάλληλους ιστότοπους και ιστοσελίδες. Σε περίπτωση που το αίτημα κριθεί ακατάλληλο ο χρήστης ανακατευθύνεται σε μια ενημερωτική σελίδα, αλλιώς το Squid αναλαμβάνει να εξυπηρετήσει το αίτημα, φέρνοντας το σχετικό αντικείμενο από το διαδίκτυο.

Μια γενική εικόνα της διαδικασίας που ακολουθείται περιγράφεται στο ακόλουθο σχήμα:



Εικόνα 1 Διαδικασία αναδρομολόγης κίνησης HTTP

Ακολουθεί ανάλυση των υπομερών της υπηρεσίας:

2.1 ΣΥΣΤΟΙΧΙΑ ΕΞΥΠΗΡΕΤΗΤΩΝ

Για την εξυπηρέτηση των αναγκών της υπηρεσίας έγινε προμήθεια 16 υπολογιστικών συστημάτων HP ProLiant DL380 G5 στα πλαίσια του έργου e-datacenter. Από αυτά, 8 χρησιμοποιούνται από την υπηρεσία, 2 χρησιμοποιούνται ως εφεδρικά και για δοκιμές, ενώ τα υπόλοιπα 6 έχουν δανειστεί σε άλλες υπηρεσίες του ΠΣΔ για την κάλυψη επειγουσών αναγκών. Κάθε ένα από τα συστήματα αυτά περιλαμβάνει ένα επεξεργαστή Intel Xeon E5420, 2 GB κεντρικής μνήμης, 3 δίσκους SAS σε διάταξη RAID1 (mirror) + hot spare και διπλό υποσύστημα τροφοδοσίας. Η εγκατάσταση των συγκεκριμένων συστημάτων έγινε στις αρχές του έτους 2010.

Στα συστήματα που χρησιμοποιούνται από την υπηρεσία έχει εγκατασταθεί η έκδοση 7.3 του λειτουργικού συστήματος FreeBSD και έχει παραμετροποιηθεί σύμφωνα με τα πρότυπα του Κέντρου Δικτύων του ΕΜΠ. Έχει ληφθεί ιδιαίτερη μέριμνα ώστε όλα τα συστήματα να είναι παραμετροποιημένα με τον ίδιο ακριβώς αυτοματοποιημένο τρόπο και να διαφέρουν μόνο σε συγκεκριμένες παραμέτρους που αφορούν το καθένα από αυτά, όπως διεύθυνση IP((Internet Protocol address), hostname κλπ. Με τον τρόπο αυτό εξασφαλίζεται η ομοιόμορφη συμπεριφορά τους, επιτυγχάνεται η διατήρηση του διαχειριστικού κόστους τους σε χαμηλά επίπεδα ασχέτως του πλήθους των μηχανών, δίνεται η δυνατότητα εύκολης και γρήγορης προσθήκης επιπλέον μηχανών όποτε αυτό θεωρηθεί σκόπιμο για τις ανάγκες της υπηρεσίας και δεν είναι αναγκαία η λήψη αντιγράφων ασφαλείας (backup) για κάθε σύστημα ξεχωριστά.

Πλέον του λειτουργικού συστήματος, έχουν εγκατασταθεί και χρησιμοποιούνται τα πακέτα λογισμικού Squid (έκδοση 2.7), SquidGuard (έκδοση 1.4) και Nginx (έκδοση 1.2).

Το Squid λειτουργεί ως διαμεσολαβητής (proxy server) για την εξυπηρέτηση των αιτημάτων HTTP των χρηστών του ΠΣΔ. Τα αιτήματα των χρηστών προωθούνται στη συστοιχία από τον κεντρικό δρομολογητή ως ροές πακέτων (packet flows) πρωτοκόλλου TCP με διευθύνσεις IP προορισμού εκτός ΠΣΔ και θύρα προορισμού 80. Το υποσύστημα δικτύου σε κάθε εξυπηρετητή είναι ρυθμισμένο καταλλήλως ώστε να αναγνωρίζει τις συγκεκριμένες ροές και να τις προωθεί στη διεργασία του Squid για τον περαιτέρω χειρισμό. Οι ρυθμίσεις

αυτές περιλαμβάνουν την εγκατάσταση πυρήνα με ενεργοποιημένη την επιλογή IPFIREWALL_FORWARD (βλ. /usr/src/sys/amd64/conf/SCH) και ενεργοποίηση του ipfw με κατάλληλες παραμέτρους για την προώθηση των ροών HTTP στην θύρα 80 του loopback interface lo0 όπου «ακούει» η διεργασία του Squid (βλ. /etc/rc.conf και /etc/firewall.conf). Καθώς σε ώρες αιχμής κάθε εξυπηρετητής μπορεί να κληθεί να εξυπηρετήσει έως και μερικές εκατοντάδες αιτήματα HTTP το δευτερόλεπτο, η διεργασία του Squid έχει ρυθμιστεί έτσι ώστε να μην διατηρεί αντίγραφα των αιτημάτων (σελίδες HTML, εικόνες κλπ.) στον τοπικό δίσκο. Το παραπάνω κρίθηκε σκόπιμο, γιατί σε τέτοιους ρυθμούς η διαδικασία εγγραφής, αναζήτησης και ανάγνωσης από το δίσκο δημιουργούσε φαινόμενα κορεσμού και προσκαλούσε σοβαρές καθυστερήσεις στην εξυπηρέτηση των αιτημάτων. Εξάλλου, το εύρος ζώνης (bandwidth) των συνδέσεων του ΠΣΔ με το πάροχό του (ΕΔΕΤ) και στη συνέχεια με το διαδίκτυο είναι πλέον τόσο που τα οφέλη από τη λειτουργία του Squid ως caching proxy είναι μηδαμινά.

Το SquidGuard, που λειτουργεί σαν υποδιεργασία του Squid, διατηρεί τη βάση δεδομένων με τις ακατάλληλες σελίδες και αναλαμβάνει το ρόλο του διαιτητή επιτρέποντας ή μη την πρόσβαση στις σελίδες που ζητούν οι χρήστες. Η βάση δεδομένων είναι πανομοιότυπη για όλους τους εξυπηρετητές της συστοιχίας. Ο κάθε εξυπηρετητής διατηρεί το δικό του τοπικό αντίγραφο που ανανεώνεται αυτομάτως από κεντρικό σημείο. Η βάση περιλαμβάνει ανά κατηγορία ακατάλληλου περιεχομένου:

1. λίστα ονομάτων δικτυακών τόπων (hostnames, διευθύνσεις IP, domain names) που περιέχουν αποκλειστικά ακατάλληλο περιεχόμενο,
2. λίστα διευθύνσεων ιστοσελίδων (URLs) με ακατάλληλο περιεχόμενο που όμως φιλοξενούνται σε δικτυακούς τόπους που δεν περιλαμβάνουν αποκλειστικά ακατάλληλο περιεχόμενο,
3. λίστα με λέξεις κλειδιά και κανονικές εκφράσεις (regular expressions) που θεωρούνται ακατάλληλες και μπορεί να εμφανιστούν σε οποιοδήποτε σημείο της διεύθυνσης μιας ιστοσελίδας.

Η διαδικασία αξιολόγησης της καταλληλότητας ενός δικτυακού τόπου ή μιας ιστοσελίδας γίνεται από τους συντάκτες των παραπάνω λιστών. Η υπηρεσία ελέγχου περιεχομένου του

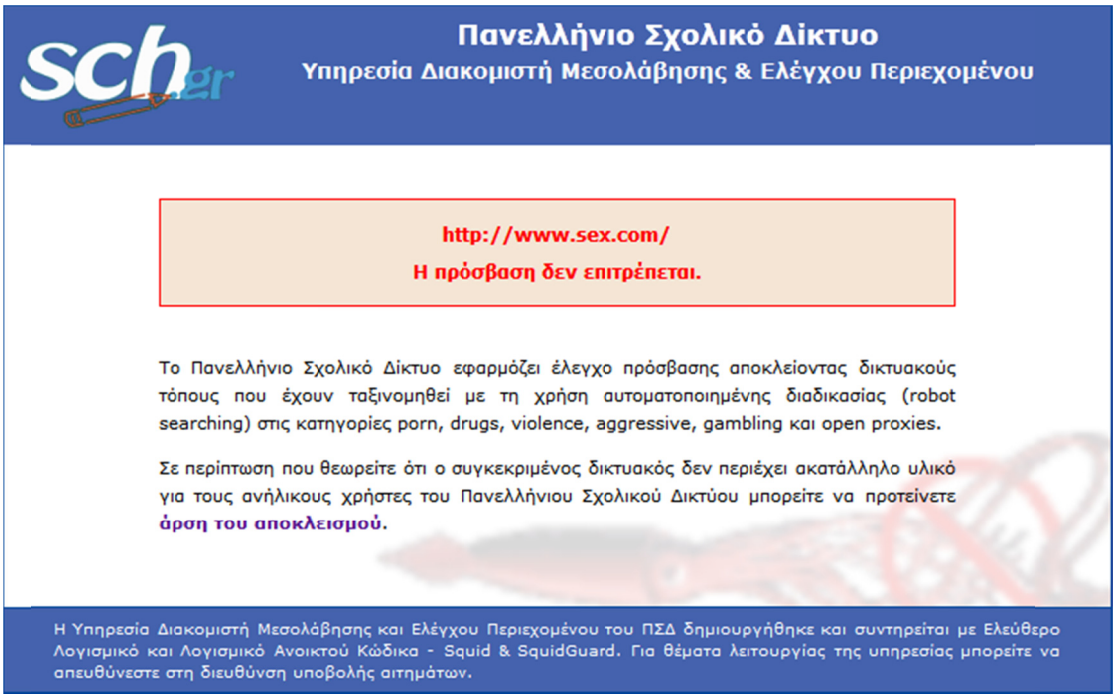
ΠΣΔ χρησιμοποιεί αντίγραφα των συγκεκριμένων λιστών για ελέγξει την καταλληλότητα των σελίδων που ζητούν οι χρήστες του, ελέγχοντας σε πραγματικό χρόνο αν κάποιο από τα hostname, διεύθυνση IP, domain name ή URL της σελίδας ταυτίζεται με εγγραφή στη βάση. Σε καμία περίπτωση δεν γίνεται έλεγχος του περιεχομένου των σελίδων και των λοιπών αντικειμένων, όπως εικόνες, που ζητούν οι χρήστες και προσπάθεια αξιολόγησης της καταλληλότητάς τους. Κάτι τέτοιο θα απαιτούσε πιθανώς πολλαπλάσιους υπολογιστικούς πόρους και εξελιγμένο λογισμικό που δεν είναι διαθέσιμο προς χρήση, τουλάχιστον με άδεια open source και χωρίς επιπλέον κόστος.

Επίσης, στη βάση διατηρούνται ορισμένες επιπλέον κατηγορίες περιεχομένου που δεν εμπίπτουν άμεσα σε αυτήν της ακατάλληλης για ανηλίκους. Οι κατηγορίες αυτές είναι:

1. Εξυπηρετητές στο διαδίκτυο που λειτουργούν ως open proxies και θα μπορούσαν να χρησιμοποιηθούν από τους χρήστες του ΠΣΔ για την παράκαμψη της υπηρεσίας ελέγχου περιεχομένου.
2. Παραβιασμένοι ιστότοποι ή ιστοσελίδες που έχουν μολυνθεί από επιτηδείους, φιλοξενούν επικίνδυνο υλικό (viruses, malware κλπ.) και τυχόν επίσκεψη σε αυτές θα μπορούσε να οδηγήσει σε μαζική μόλυνση υπολογιστών του ΠΣΔ.
3. Ιστότοποι ή ιστοσελίδες με ακατάλληλο υλικό που περιλαμβάνονται σε κάποια από όλες τις προηγούμενες κατηγορίες, αλλά προς το παρόν ακόμα δεν περιέχονται σε κάποια από τις λίστες που χρησιμοποιεί η υπηρεσία. Τέτοιες περιπτώσεις συνήθως αναφέρονται από τους χρήστες του ΠΣΔ και προστίθενται στη συγκεκριμένη ξεχωριστή κατηγορία.
4. Ιστότοποι ή ιστοσελίδες που κακώς αναφέρονται ως ακατάλληλες στις λίστες που χρησιμοποιεί η υπηρεσία. Τέτοιες περιπτώσεις συνήθως αναφέρονται από τους χρήστες του ΠΣΔ και προστίθενται στη συγκεκριμένη ξεχωριστή κατηγορία ώστε να εξαιρεθούν από τον αποκλεισμό.

Το Nginx λειτουργεί ως απλός εξυπηρετητής WWW στον οποίο καταλήγουν οι χρήστες όταν ζητούν να επισκεφτούν κάποια ακατάλληλη σελίδα. Φιλοξενεί μόνο μια στατική σελίδα που ενημερώνει το χρήστη για τους λόγους που δεν έχει πρόσβαση στην ιστοσελίδα που αρχικώς ζήτησε. Επιπλέον του παρέχει οδηγίες για τη διαδικασία που μπορεί να ακολουθήσει

στην περίπτωση που θεωρεί ότι η αρχική ιστοσελίδα έχει κακώς κριθεί ακατάλληλη και επιθυμεί να αιτηθεί την άρση του περιορισμού. Η χρήση του λογισμικού Nginx σε σχέση με άλλα πιο δημοφιλή, όπως ο Apache HTTPd, κρίθηκε σκόπιμη για εξοικονόμηση πόρων του συστήματος.



Εικόνα 2 Ενημερωτική σελίδα για ακατάλληλο ιστότοπο

Για την αποδοτικότερη λειτουργία της υπηρεσίας σε κάθε σύστημα λειτουργεί ξεχωριστός εξυπηρετητής ονοματολογίας (recursive caching name server), ο οποίος εξυπηρετεί αποκλειστικά τα αιτήματα του ίδιου του συστήματος, ως επί τω πλείστον προερχόμενα από το Squid. Χρησιμοποιείται το λογισμικό ISC BIND όπως διατίθεται προεγκατεστημένο από το λειτουργικό σύστημα.

2.2 Ρυθμισεις ανακατευθυνσης κινησης στο συνοριακο δρομολογητη

Ο συνοριακός δρομολογητής του ΠΣΔ είναι ένας Cisco 7604. Ανάμεσα στα υπόλοιπα χαρακτηριστικά του είναι και η υποστήριξη της τεχνολογίας IP Policy, που επιτρέπει το

χειρισμό μέρος της κίνησης που δρομολογείται μέσω της συσκευής με διαφορετικό τρόπο (από την συνήθη δρομολόγηση με βάση το πεδίου της διεύθυνσης προορισμού) εφόσον πληροί συγκεκριμένα κριτήρια που ορίζονται από το διαχειριστή της.

Η συγκεκριμένη τεχνολογία χρησιμοποιείται από την υπηρεσία ελέγχου περιεχομένου ως μηχανισμός διαφανούς ανακατεύθυνσης των αιτημάτων HTTP των χρηστών του ΠΣΔ που προορίζονται προς το διαδίκτυο. Συγκεκριμένα, οι ροές πακέτων που ικανοποιούν όλες οι ακόλουθες συνθήκες:

1. πρωτόκολλο TCP,
2. διεύθυνση (IP) αφετηρίας από το δίκτυο του ΠΣΔ,
3. διεύθυνση (IP) προορισμού εκτός δικτύου ΠΣΔ,
4. θύρα (port) προορισμού ίσο με 80

αντί να δρομολογηθούν προς το διαδίκτυο, δρομολογούνται προς τη συστοιχία των εξυπηρετητών της υπηρεσίας ελέγχου περιεχομένου. Η κατανομή των αιτημάτων μεταξύ των οκτώ εξυπηρετητών της συστοιχίας γίνεται με βάση τα τρία τελευταία bits της διεύθυνσης IP προορισμού, δηλαδή του ιστοτόπου που φιλοξενεί τη σελίδα που ζητά ο χρήστης. Με τον τρόπο αυτό κάθε ιστότοπος, εφόσον χρησιμοποιεί μία μόνο διεύθυνση IP θα εξυπηρετείται πάντα από τον ίδιο εξυπηρετητή της συστοιχίας. Η συγκεκριμένη συμπεριφορά είναι χρήσιμη στις περιπτώσεις που εμφανίζεται κάποιο πρόβλημα και απαιτείται αποσφαλμάτωση (debugging).

Τελικά, ο υπολογιστής του χρήστη καταλήγει, εν αγνοία του, να συνάπτει μία σύνδεση TCP με έναν από τους εξυπηρετητές της συστοιχίας, αντί με τον εξυπηρετητή της ιστοσελίδας που ζήτησε.

Για τις περιπτώσεις εξαιρέσεων, στις παραπάνω συνθήκες προστίθεται άλλη μία με την μορφή access list. Εάν η διεύθυνση (IP) προορισμού ταιριάζει με μία εγγραφή της συγκεκριμένης access list, τότε ακόμα και εάν ικανοποιεί τις αρχικές τέσσερις συνθήκες δεν ανακατευθύνεται. Οι περιπτώσεις εξαιρέσεων που περιλαμβάνονται στη συγκεκριμένη access list χωρίζονται σε δύο κατηγορίες:

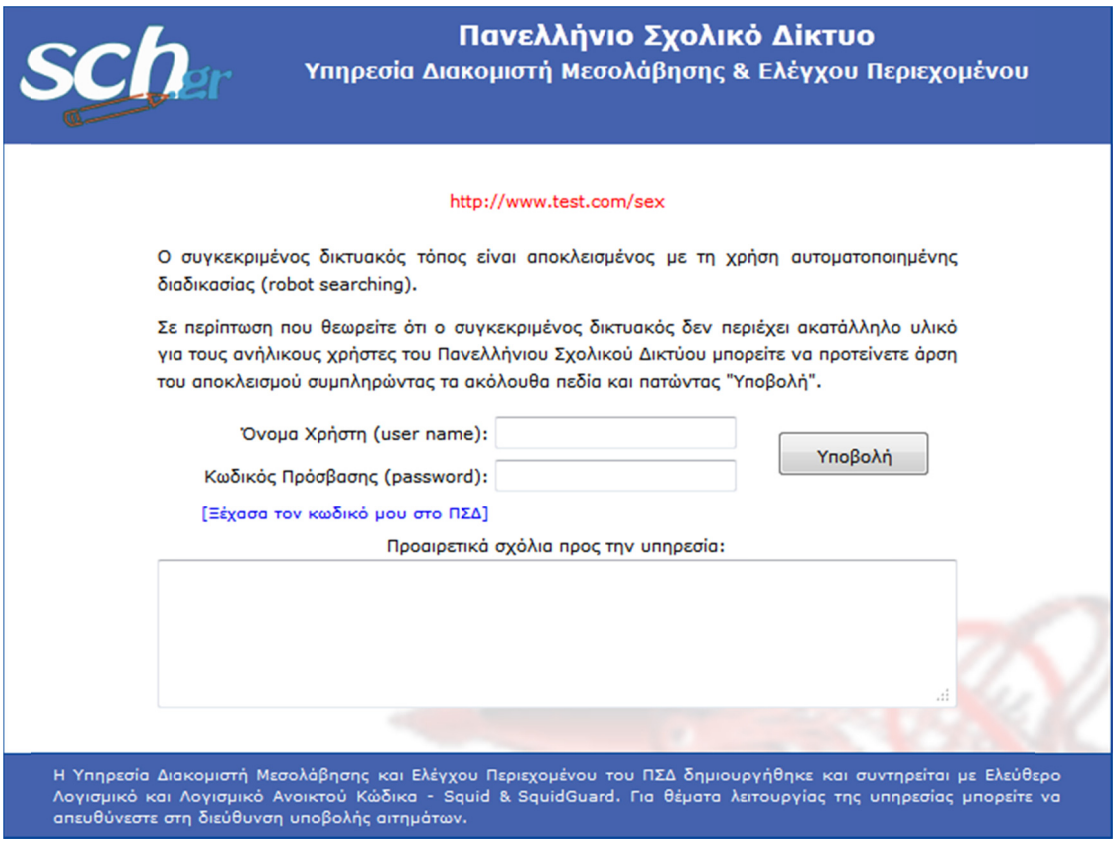
1. Δίκτυα που δεν περιέχουν ακατάλληλο περιεχόμενο, εξ ορισμού ή κατόπιν ελέγχου και είναι ιδιαίτερα δημοφιλή στους χρήστες. Για παράδειγμα, ελληνικά ή διεθνή ακαδημαϊκά ή ερευνητικά δίκτυα, υπηρεσίες του Υπουργείου Παιδείας και του Ελληνικού Κράτους, δίκτυα που προσφέρουν ενημερώσεις για λειτουργικά συστήματα (Microsoft updates) ή για «αντιβιοτικά» (antivirus updates) κλπ. Η εξαίρεση τέτοιων περιπτώσεων γίνεται για την εξοικονόμηση πόρων της υπηρεσίας.
2. Συγκεκριμένοι δημοφιλείς ιστότοποι, με κατάλληλο περιεχόμενο, οι οποίοι θεωρούν τον αυξημένο αριθμό κλήσεων που δέχονται από τους εξυπηρετητές της υπηρεσίας ελέγχου περιεχομένου ως ένδειξη κακής χρήσης και απαγορεύουν την πρόσβαση από αυτούς. Αθροιστικά πρόκειται για μερικές δεκάδες περιπτώσεις που αυξάνονται με αργούς ρυθμούς με την πάροδο του χρόνου. Αρχικά, γινόταν προσπάθεια επικοινωνίας με τους διαχειριστές του κάθε ιστότοπου για την επίλυση της κάθε περίπτωσης. Το κόστος όμως σε ανθρώπινους πόρους από την πλευρά της υπηρεσίας ελέγχου περιεχομένου ήταν υπερβολικά υψηλό και συνεπώς ασύμφορο, οπότε και επιλέχθηκε η τρέχουσα λύση της παροδικής ή μόνιμης εξαίρεσης.

Το τρέχον σύστημα ανακατεύθυνσης και κατανομής της κίνησης HTTP επιλέχθηκε καθώς δεν κατέστει δυνατή η υλοποίηση της λύσης που περιελάμβανε τη χρήση ενός εξειδικευμένου μεταγωγέα επιπέδου 4/7 (Layer 4/7 switch). Η λύση του μεταγωγέα επιπέδου 4/7 θα προσέφερε δυνατότητα καλύτερης κατανομής του φορτίου της υπηρεσίας στους εξυπηρετητές της συστοιχίας, ασχέτως του πλήθους τους και δυνατότητα αυτόματης αναδρομολόγησης της κίνησης ενός εξυπηρετητή στους υπόλοιπους σε περίπτωση αστοχίας του. Όμως, η συγκεκριμένη λύση απαιτούσε και συγκεκριμένη δικτυακή τοπολογία εντός του ΠΣΔ, με ξεχωριστό δρομολογητή σε ρόλο αποκλειστικά συνοριακού (border router), κεντρικό δρομολογητή (core router) με τις συνδέσεις κορμού να καταλήγουν σε αυτόν και διασύνδεση των δύο μέσω του μεταγωγέα επιπέδου 4/7 με συνδέσεις ικανής χωρητικότητας ανάλογης αυτής της σύνδεσης με το διαδίκτυο (10 Gbps ή πολλαπλά 1 Gbps).

2.2.1 Σύστημα λογισμικού εξυπηρέτησης αιτημάτων χρηστών

Για την εξυπηρέτηση των αιτημάτων των χρηστών της υπηρεσίας έχει υλοποιηθεί σύστημα λογισμικού προσβάσιμο μέσω WWW. Αποτελείτε από δύο μέρη, ένα για τους τελικούς χρήστες και ένα για τους διαχειριστές της υπηρεσίας.

Το υποσύστημα που απευθύνεται στους τελικούς χρήστες είναι προσπελάσιμο από τη σελίδα που τους ενημερώνει ότι κάποιος δικτυακός τόπος δεν είναι διαθέσιμος λόγω ακατάλληλου περιεχομένου. Τους προσφέρει τη δυνατότητα να αιτηθούν την επανεξέταση της απαγόρευσης. Για την αποφυγή υποβολής άσκοπων αιτημάτων οι χρήστες καλούνται να ταυτοποιηθούν με username και password.



Εικόνα 3 Φόρμα υποβολής αιτήματος άρσης απαγόρευσης πρόσβασης

Το υποσύστημα για τους διαχειριστές της υπηρεσίας προσφέρει τη δυνατότητα εξυπηρέτησης των αιτημάτων των χρηστών. Καλύπτει τις περιπτώσεις αποχαρακτηρισμού ως ακατάλληλης μιας ολόκληρης δικτυακής περιοχής (π.χ. **d**omain.com), ενός

συγκεκριμένου δικτυακού τόπου (π.χ. hostname.domain.com) ή μιας μεμονωμένης ιστοσελίδας (π.χ. http://hostname.domain.com/path/page.html). Αντιστρόφως, καλύπτει και τις ανάλογες περιπτώσεις χαρακτηρισμού περιοχών, τόπων και σελίδων ως ακατάλληλες. Επίσης, έχει τη δυνατότητα μαζικής εισαγωγής εγγραφών, καθώς και ελέγχου υποψήφιων εγγραφών. Οι νέες εγγραφές προωθούνται σε τακτά χρονικά διαστήματα αυτομάτως στους εξυπηρετητές της υπηρεσίας.

Εικόνα 4 Διαχειριστικό περιβάλλον υπηρεσίας ελέγχου περιεχομένου

Προς το παρόν φιλοξενείται σε υποδομή του Κέντρου Δικτύων ΕΜΠ. Στα πλαίσια του έργου «Στηρίζω» θα μπορούσε να μεταστεγαστεί σε υποδομές του ΠΣΔ. Επιπλέον, θα μπορούσε να αναπτυχθεί περαιτέρω καλύπτοντας και τις λειτουργίες που θα αναπτυχθούν, όπως την υποστήριξη για IPv6, τον μηχανισμό ελέγχου περιεχομένου μέσω DNS, τη διαχείριση τις λίστας εξαιρέσεων PROXY-BYPASS, κλπ.

2.3 ΣΥΣΤΗΜΑ ΛΟΓΙΣΜΙΚΟΥ ΕΛΕΓΧΟΥ ΚΑΛΗΣ ΛΕΙΤΟΥΡΓΙΑΣ ΥΠΗΡΕΣΙΑΣ

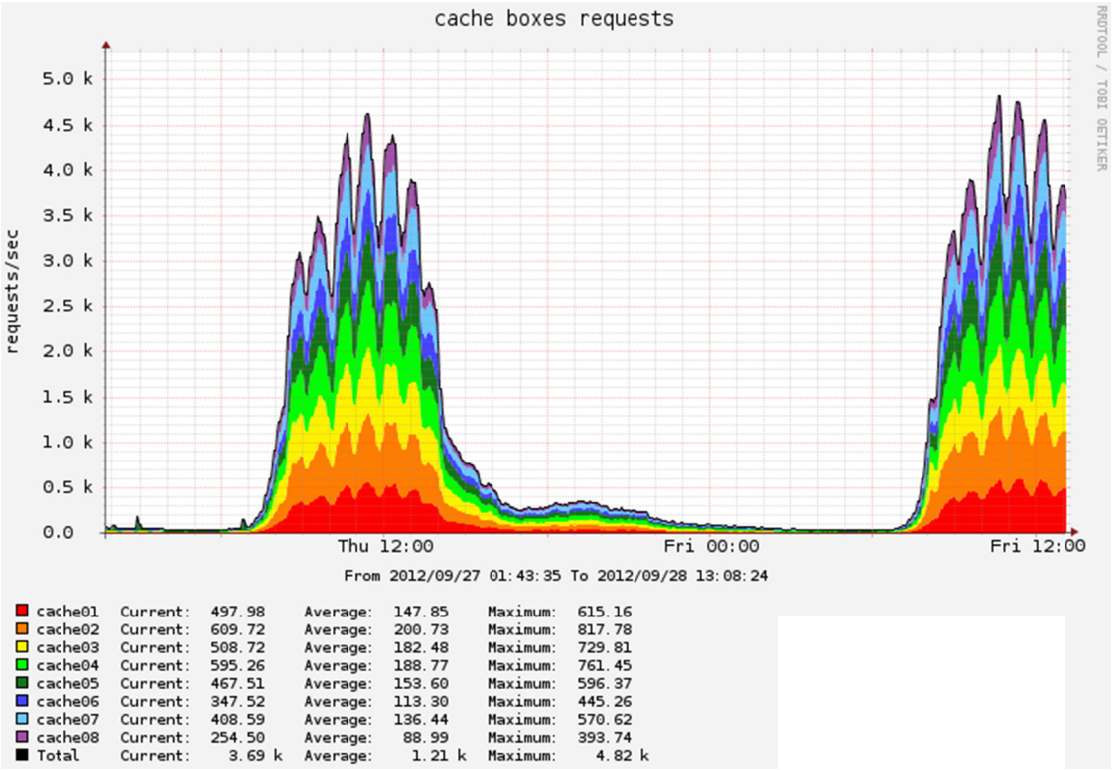
Για τον έλεγχο της καλής λειτουργίας της υπηρεσίας και την παρακολούθηση διαφόρων παραμέτρων της χρησιμοποιείται η σχετική υποδομή του Κέντρου Δικτύων του ΕΜΠ. Η υποδομή αυτή περιλαμβάνει τα ακόλουθα μέρη:

1. Λογισμικό Nagios για την παρακολούθηση της καλής λειτουργίας των εξυπηρετητών (υλικό, λειτουργικό σύστημα, λογισμικό Squid, δικτυακή σύνδεση κλπ.) και την άμεση ενημέρωση των διαχειριστών της υπηρεσίας μέσω ηλεκτρονικού ταχυδρομείου σε περίπτωση δυσλειτουργίας.
2. Λογισμικό Cacti για την παρακολούθηση διαφόρων παραμέτρων των εξυπηρετητών και την αποτύπωσή τους σε γραφήματα (ημερήσια, εβδομαδιαία, μηνιαία, ετήσια) διαθέσιμα online.

Οι συγκεκριμένες λειτουργίες θα μπορούσαν να μεταφερθούν σε διαθέσιμες υποδομές του ΠΣΔ σε συνεργασία με τους υπεύθυνους για αυτές.

3. ΑΝΑΒΑΘΜΙΣΗ ΣΥΣΤΗΜΑΤΟΣ ΑΝΑΔΡΟΜΟΛΟΓΗΣΗΣ ΜΕ ΧΡΗΣΗ ΠΡΩΤΟΚΟΛΛΟΥ WCCP

Όπως αναφέρθηκε σε προηγούμενο κεφάλαιο, η αυτόματη αναδρομολόγηση των αιτημάτων HTTP των χρηστών του ΠΣΔ γίνεται με τη χρήση του μηχανισμού του IP policy στο συνοριακό δρομολογητή. Η συγκεκριμένη μέθοδος λειτουργεί απρόσκοπτα καλύπτοντας τις αυξημένες απαιτήσεις της υπηρεσίας χωρίς προβλήματα ή ιδιαίτερη επιβάρυνση του συνοριακού δρομολογητή. Επιπλέον, παρέχει ευέλικτο μηχανισμό εξαιρέσεων μέσω της access list PROXY-BYPASS. Η μέθοδος κατανομής του φορτιού των αιτημάτων στους οκτώ εξυπηρετητές της υπηρεσίας έχει ικανοποιητικά αποτελέσματα, αλλά όχι βέλτιστα, καθώς ορισμένοι από τους εξυπηρετητές αναλαμβάνουν σε σταθερή βάση την εξυπηρέτηση έως και υποδιπλασιάσου αριθμού αιτημάτων από τους υπόλοιπους (βλ. σχετικό διάγραμμα).



Εικόνα 5 Κατανομή αιτημάτων HTTP ανά εξυπηρετητή

Το σοβαρότερο μειονέκτημα της μεθόδου του IP policy είναι ότι δεν προσφέρει μηχανισμούς για αυτόματη αντιμετώπιση προβλημάτων αστοχίας ενός ή περισσοτέρων εξυπηρετητών της

υπηρεσίας. Στο τρέχον σχήμα, εάν κάποιος από τους εξυπηρετητές παρουσιάσει βλάβη (στο υλικό ή στο λογισμικό του) η κίνηση HTTP που του αναλογεί θα συνεχίσει να ανακατευθύνεται σε αυτόν χωρίς όμως να είναι δυνατή η εξυπηρέτησή της. Το αποτέλεσμα για τους τελικούς χρήστες είναι ότι δεν έχουν πρόσβαση στο συγκεκριμένο υποσύνολο του παγκόσμιου ιστού (WWW) μέχρι είτε να διορθωθεί η βλάβη, είτε να παρακαμφθεί ο συγκεκριμένος εξυπηρετητής. Τόσο η αντιμετώπιση της βλάβης, όσο και η παράκαμψη του συγκεκριμένου εξυπηρετητή γίνεται με παρέμβαση του διαχειριστή της υπηρεσίας στις ρυθμίσεις του συνοριακού δρομολογητή. Η ίδια διαδικασία ακολουθείται και σε κάθε περίπτωση προγραμματισμένης διακοπής για εργασίες στους εξυπηρετητές, π.χ. για αναβαθμίσεις.

Για την αντιμετώπιση του προβλήματος εξετάστηκε στο παρελθόν η λύση της χρήσης ενός μεταγωγέα επιπέδων 4/7 (Layer 4/7 switch). Ο μεταγωγέας θα αναλάμβανε τις λειτουργίες της ανακατεύθυνσης της κίνησης, της κατανομής της με καλύτερο τρόπο στους εξυπηρετητές και της αντιμετώπισης αστοχιών με αυτόματη ανακατανομή της κίνησης του προβληματικού κόμβου στους υπόλοιπους. Όμως, η δικτυακή τοπολογία (κεντρικός δρομολογητής – μεταγωγέας επιπέδων 4/7 – συνοριακός δρομολογητής) που απαιτούσε η συγκεκριμένη λύση δεν μπόρεσε να υλοποιήθηκε για διάφορους τεχνικούς και οικονομικούς λόγους.

Εναλλακτική λύση που είναι πλέον διαθέσιμη και προσφέρει τα ίδια πλεονεκτήματα είναι η χρήση του πρωτοκόλλου Web Cache Communication Protocol (WCCP). Το συγκριμένο πρωτόκολλο προτάθηκε και υλοποιήθηκε αρχικώς από την εταιρία Cisco, στη συνέχεια προτυποποιήθηκε (βλ. http://tools.ietf.org/html/draft-mclaggan-wccp-v2rev1-00) και πλέον είναι διαθέσιμο σε συσκευές και λογισμικά τρίτων κατασκευαστών.

Σκοπός του πρωτοκόλλου WCCP είναι να προσφέρει μέσα από το ίδιο το λειτουργικό σύστημα της Cisco (IOS) λειτουργίες και δυνατότητες που αρχικά ήταν διαθέσιμες μόνο από εξειδικευμένες συσκευές, όπως οι μεταγωγείς επιπέδων 4/7. Έτσι από την έκδοση 12.1 και έπειτα του Cisco IOS, οι εκδόσεις 1 και 2 του πρωτοκόλλου WCCP είναι διαθέσιμες στις συσκευές της Cisco (δρομολογητές και μεταγωγείς).

Η έκδοση 1 του πρωτοκόλλου WCCP, υποστηρίζει αποκλειστικά την εξυπηρέτηση κίνησης HTTP (θύρα 80) από ένα δρομολογητή και ένα ή περισσότερους εξυπηρετητές.

Η έκδοση 2 υποστηρίζει:

1. έως 32 δρομολογητές σε διάταξη cluster,
2. οποιοδήποτε πρωτόκολλο IP (TCP ή UDP)
3. έως 255 διαφορετικές υπηρεσίες ταυτόχρονα,
4. ταυτοποίηση των συμμετεχόντων μερών με χρήση MD5 shared secret security.

Μία λύση που στηρίζεται στο πρωτόκολλο WCCP αποτελείτε από τα ακόλουθα μέρη:

1. Τον πελάτη WCCP (WCCP client ή WCCP engine), ρόλο που αναλαμβάνει ένας ή περισσότεροι εξυπηρετητές που τρέχουν λογισμικού proxy caching (όπως το Squid). Οι πελάτες αρχικά καταχωρούν την ύπαρξή τους και τις δυνατότητές τους, δηλαδή τις υπηρεσίες που είναι σε θέση να εξυπηρετήσουν (HTTP κλπ.) και σε τακτικά χρονικά διαστήματα ανακοινώνουν τη διαθεσιμότητά τους (μηνύματα «Here I Am»).
2. Τον εξυπηρετητή WCCP (WCCP server), ρόλο που αναλαμβάνει ένας ή περισσότεροι δρομολογητές ή μεταγωγείς. Καταχωρεί σε ομάδες ανά υπηρεσία τους πελάτες WCCP που έχουν ανακοινώσει την ύπαρξή τους, παρακολουθεί τη διαθεσιμότητά τους (από τα μηνύματα που λαμβάνει) και αναλόγως αναδρομολογεί με ομοιόμορφο τρόπο την κίνηση στους διαθέσιμους πελάτες. Στους δρομολογητές η αναδρομολογούμενη κίνηση από τον εξυπηρετητή WCCP προς τους πελάτες WCCP διοχετεύεται μέσω πρωτοκόλλου GRE (tunneling) ώστε το περιεχόμενο των αρχικών πακέτων IP να παραμείνει αναλλοίωτο. Στους μεταγωγείς υποστηρίζεται μηχανισμός αναδρομολόγησης επιπέδου 2 (Layer 2 redirection) αντί του καναλιού GRE.

1.1.1 Παραμετροποίηση πρωτοκόλλου WCCP στο συνοριακό δρομολογητή

Στον τρέχοντα συνοριακό δρομολογητή του ΠΣΔ είναι εγκαταστημένη η έκδοση 12.2(18)SXF15 του λειτουργικού συστήματος IOS, η οποία υποστηρίζει τις εκδόσεις 1 και 2 του πρωτοκόλλου WCCP. Εξ ορισμού, εφόσον ενεργοποιηθεί, χρησιμοποιείται η έκδοση 2.

Η παραμετροποίηση του συνοριακού δρομολογητή του ΠΣΔ για την ενεργοποίηση του πρωτοκόλλου WCCP είναι:

```
! enable WCCP v2
ip wccp version 2

! set WCCP server/client password
ip wccp web-cache password secret-pass

! access list 10 contains the cache boxes address space
ip wccp web-cache group-list 10

! cache01.att.sch.gr
access-list 10 permit host 194.63.239.231
! cache02.att.sch.gr
access-list 10 permit host 194.63.239.232
! cache03.att.sch.gr
access-list 10 permit host 194.63.239.233
! cache04.att.sch.gr
access-list 10 permit host 194.63.239.234
! cache05.att.sch.gr
access-list 10 permit host 194.63.239.235
! cache06.att.sch.gr
access-list 10 permit host 194.63.239.236
! cache07.att.sch.gr
access-list 10 permit host 194.63.239.237
! cache08.att.sch.gr
access-list 10 permit host 194.63.239.238
! cache09.att.sch.gr
access-list 10 permit host 194.63.239.239
! cache10.att.sch.gr
access-list 10 permit host 194.63.239.210

! address space defined in PROXY-BYPASS access list
! should not be redirected
ip wccp web-cache redirect-list PROXY-BYPASS-2
```

```
! enable traffic redirection on every SCH.gr user interface
interface Vlan9
  ip wccp web-cache redirect in
interface Vlan10
  ip wccp web-cache redirect in
interface Vlan11
  ip wccp web-cache redirect in
interface Vlan12
  ip wccp web-cache redirect in
interface Vlan13
  ip wccp web-cache redirect in
interface Vlan14
  ip wccp web-cache redirect in
interface Vlan15
  ip wccp web-cache redirect in
interface Vlan16
  ip wccp web-cache redirect in
interface Vlan17
  ip wccp web-cache redirect in
interface Vlan100
  ip wccp web-cache redirect in
interface Vlan101
  ip wccp web-cache redirect in
interface Vlan202
  ip wccp web-cache redirect in
interface Vlan204
  ip wccp web-cache redirect in
interface Vlan205
  ip wccp web-cache redirect in
interface Vlan206
  ip wccp web-cache redirect in
interface Vlan207
  ip wccp web-cache redirect in
interface Vlan210
```

```
  ip wccp web-cache redirect in
interface Vlan212
  ip wccp web-cache redirect in
interface Vlan213
  ip wccp web-cache redirect in
interface Vlan214
  ip wccp web-cache redirect in
interface Vlan215
  ip wccp web-cache redirect in
interface Vlan216
  ip wccp web-cache redirect in
interface Vlan218
  ip wccp web-cache redirect in
interface Vlan334
  ip wccp web-cache redirect in
interface Vlan550
  ip wccp web-cache redirect in
interface Tunnel11
  ip wccp web-cache redirect in
```

Οι παραπάνω ρυθμίσεις περιλαμβάνουν:

1. την ενεργοποίηση του πρωτοκόλλου WCCP,
2. τον ορισμό ενός κοινού συνθηματικού MD5,
3. τον ορισμό των διευθύνσεων IP των εξυπηρετητών της υπηρεσίας,
4. τον ορισμό των εξαιρέσεων από το σχήμα αναδρομολόγησης μέσω της λίστας PROXY-BYPASS-2, η οποία είναι η «αντίστροφη» της λίστας PROXY-BYPASS, δηλαδή περιλαμβάνει ακριβώς τις ίδιες εγγραφές, αλλά έχει εντολές `permit` στη θέση των εντολών `deny` και το ανάποδο, λόγω του τρόπου υλοποίησης της εντολής `ip wccp web-cache redirect-list`,
5. τον ορισμό της αναδρομολόγησης της κίνησης στις θύρες (interfaces) του εξυπηρετούν τους χρήστες του ΠΣΔ.

Για τον έλεγχο της λειτουργίας και την αποσφαλμάτωση του πρωτοκόλλου WCCP στο δρομολογητή μπορούν να χρησιμοποιηθούν οι εντολές:

```
show ip wccp
show ip wccp web-cache detail
debug ip wccp events
debug ip wccp packets
```

Από τους χρήστες δρομολογητών Cisco, αλλά και από την ίδια την εταιρία, αναφέρονται περιπτώσεις ασυμβατότητας μεταξύ του μηχανισμού αναδρομολόγησης και άλλων λειτουργιών όταν είναι ταυτόχρονα ενεργοποιημένες στην ίδια θύρα. Θα πρέπει να εξεταστεί ανά περίπτωση σε συνεργασία με την ομάδα διαχείρισης του δικτύου κορμού του ΠΣΔ.

Η υποστήριξη της αναδρομολόγησης κίνησης IPv6 μέσω του πρωτοκόλλου WCCP αναφέρεται σε πλέον πρόσφατες εκδόσεις του λειτουργικού συστήματος IOS, το οποίο πιθανώς να μην είναι διαθέσιμο για το συνοριακό δρομολογητή του ΠΣΔ. Θα πρέπει να εξεταστεί και αυτό σε συνεργασία με την ομάδα διαχείρισης του δικτύου κορμού του ΠΣΔ. Σε περίπτωση που δεν βρεθεί λύση για υποστήριξη της κίνησης IPv6 από το πρωτόκολλο WCCP, τότε το συγκεκριμένο είδος κίνησης θα συνεχίσει να εξυπηρετείται από το μηχανισμό του IP policy.

Περισσότερες πληροφορίες για τον συνδυασμό IPv6 και WCCP είναι διαθέσιμες στη σελίδα http://www.cisco.com/en/US/docs/ios-xml/ios/ipapp/configuration/15-2mt/iap-wccp-v2-ipv6.html.

3.1 ΠΑΡΑΜΕΤΡΟΠΟΙΗΣΗ ΠΡΩΤΟΚΟΛΛΟΥ WCCP ΣΤΟΥΣ ΕΞΥΠΗΡΕΤΗΤΕΣ

Στους εξυπηρετητές της υπηρεσίας για την υποστήριξη του πρωτοκόλλου WCCP απαιτούνται ρυθμίσεις στο λειτουργικό σύστημα και στο λογισμικό Squid.

3.1.1 Παραμετροποίηση πρωτοκόλλου WCCP στο λειτουργικό σύστημα

Συγκεκριμένα, στο λειτουργικό σύστημα πρέπει να γίνει η παραμετροποίηση του καναλιού GRE για να είναι δυνατή η λήψη της αναδρομολογούμενης κίνησης από το δρομολογητή. Το λειτουργικό σύστημα FreeBSD από την έκδοση 6.0 και έπειτα υποστηρίζει εγγενώς στον πυρήνα του το πρωτόκολλο GRE. Ο ορισμός του καναλιού γίνεται με τις εντολές:

```
# create interface
```

```
ifconfig gre0 create

# set link2 parameter (for WCCPv2)
ifconfig gre0 link2

# create tunnel between server and router
ifconfig gre0 tunnel SERVER_IP ROUTER_IP
```

Η διαδικασία αναδρομολόγησης των πακέτων IP, εσωτερικά στον εξυπηρετητή, στη διεργασία του λογισμικού Squid εξακολουθεί να γίνεται με την ίδια μέθοδο που ακολουθείται και τώρα, δηλαδή με τη χρήση του module IPFW του πυρήνα:

```
# do not touch outgoing traffic
ipfw add 48 allow tcp from SERVER_IP to any

# do not touch incoming traffic destined to SERVER_IP:80
ipfw add 49 allow tcp from any to SERVER_IP 80

# redirect any other web traffic to squid listening in localhost:80
ipfw add 50 fwd 127.0.0.1,80 tcp from any to any 80
```

3.1.2 Παραμετροποίηση πρωτοκόλλου WCCP στο λογισμικό Squid

Στο λογισμικό Squid πρέπει να προστεθούν οι ακόλουθες παράμετροι στο αρχείο ρυθμίσεών του για την υποστήριξη της έκδοσης 2 του πρωτοκόλλου WCCP:

```
# this is our WCCP router
wccp2_router ROUTER_IP

# WCCP internal version
wccp2_version 4

# set to 1 for GRE tunnel setup
wccp2_forwarding_method 1

# set to 1 for GRE tunnel setup
wccp2_return_method 1

#set to 0 for standard HTTP redirection
wccp2_service standard 0 password=secret-pass
```

Επίσης, το λογισμικό Squid θα πρέπει να έχει μεταγλωττιστεί με την παράμετρο `--enable-wccpv2` για να υποστηρίζει εγγενώς το πρωτόκολλο WCCP v2.

4. ΥΠΟΣΤΗΡΙΞΗ ΠΡΩΤΟΚΟΛΛΟΥ IPv6

Το πρωτόκολλο IPv6 είναι η νέα έκδοση διαδικτυακής τεχνολογίας στο επίπεδο δικτύου, η οποία προέκυψε από την έλλειψη επαρκούς αριθμού δημόσιων διευθύνσεων για τους χρήστες του διαδικτύου. Το ΠΣΔ τα τελευταία χρόνια έχει υιοθετήσει την τεχνολογία στο δίκτυο κορμού και πλέον έχει επικεντρωθεί στη ενσωμάτωση της τεχνολογίας στο δίκτυο πρόσβασης και στις βασικές υπηρεσίες του. Η υπηρεσία ελέγχου περιεχομένου δεν θα μπορούσε να μείνει εκτός μετάβασης για το νέο πρωτόκολλο διαφορετικά οι χρήστες θα μπορούσαν να αποκτήσουν ανέλεγκτη πρόσβαση σε δικτυακούς κόμβους με χρήση του νέου πρωτοκόλλου.

Δεδομένου ότι τα βασικά συστατικά στοιχεία της υπηρεσίας ελέγχου περιεχομένου είναι:

- Η ενεργοποίηση και διευθυνσιοδότηση IPv6 στους εξυπηρετητές της υπηρεσίας
- Η δρομολόγηση με βάση το πεδίο του πρωτοκόλλου (πολιτική δρομολόγησης)
- Το υποσύστημα λογισμικού Squid
- Το υποσύστημα λογισμικού Squidguard

Χρειάζεται να εντοπίσουμε τις αλλαγές που χρειάζεται να γίνουν στα παραπάνω υποσυστήματα με την προϋπόθεση ότι έχουν εγκατασταθεί οι κατάλληλες εκδόσεις για την υποστήριξη του πρωτοκόλλου IPv6.

4.1 ΕΝΕΡΓΟΠΟΙΗΣΗ IPv6 ΚΑΙ ΔΙΕΥΘΥΝΣΙΟΔΟΤΗΣΗ ΣΤΟΥΣ PROXY-CACHE

Στο λειτουργικό σύστημα FreeBSD από την έκδοση 6.X και έπειτα ο πυρήνας του λειτουργικού συστήματος περιέχει τις απαραίτητες δομές (INET6) για την λειτουργία του πρωτοκόλλου IPv6 με αποτέλεσμα η ενεργοποίηση του να είναι ρύθμιση ορισμένων αρχείων. Επιπλέον επειδή είναι επιθυμητό η αριθμοδότηση των proxy να είναι σταθερή επιλέγεται να προστεθεί στο αρχείο /etc/rc.conf σταθερά τα:

```
ipv6_enable="YES"
ipv6_ifconfig_fxp0="2001:648:2302:FC02::231"
ipv6_defaultrouter="2001:648:2302:FC02::1"
```

όπου η πρώτη γραμμή ενεργοποιεί την στίβα IPv6 , η δεύτερη γραμμή ρυθμίζει την διεύθυνση του μηχανήματος και η 3η γραμμή ρυθμίζει την διεύθυνση του δρομολογητή. Στην συνέχεια εκτελούμε:

```
$ /etc/rc.d/network_ipv6 restart
```

Και ο έλεγχος για την διευθυνσιοδότηση γίνεται με

```
$                                                                    ifconfig
$ ifconfig | grep inet6
```

Ο έλεγχος για την σωστή δρομολόγηση γίνεται εκτελώντας εντολές:

```
$ ping6 ipv6.google.com

$ traceroute6 ipv6.google.com
```

Και λαμβάνοντας σαν αποτέλεσμα κάτι σαν:

```
 1?: [LOCALHOST]
 1 grnetRouter.sch.access-link.grnet.gr (2001:648:2FFD:8248:1::1) 0 msec 0 msec 0 msec
 2 eie2-to-koletti1.backbone.grnet.gr (2001:648:2FFF:311::2) 0 msec 0 msec 4 msec
 3 grnet.rt1.ath2.gr.geant2.net (2001:798:19:10AA::1) 0 msec 0 msec 0 msec
 4 so-4-2-0.rt1.mil.it.geant2.net (2001:798:CC:1901:1E01::2) 36 msec 32 msec 32 msec
 5 as0.rt1.gen.ch.geant2.net (2001:798:CC:1201:1E01::1) 40 msec 44 msec 40 msec
 6 so-4-0-0.rt1.fra.de.geant2.net (2001:798:CC:1401:2201::9) 152 msec 48 msec 48 msec
 7 google-gw.rt1.fra.de.geant2.net (2001:798:14:10AA::E) 48 msec 52 msec 48 msec
 8 2001:4860::1:0:11 48 msec 72 msec
   2001:4860::1:0:10 48 msec
 9 2001:4860::8:0:3015 52 msec 52 msec 48 msec
10 2001:4860::1:0:336C 60 msec 56 msec 56 msec
11 2001:4860:0:1::535 60 msec 56 msec 60 msec
12 2A00:1450:8000:1E::E 60 msec 60 msec 60 msec
```

4.2 ΕΝΕΡΓΟΠΟΙΗΣΗ IPv6 ΣΤΗΝ ΠΟΛΙΤΙΚΗ ΔΡΟΜΟΛΟΓΗΣΗΣ ΑΝΑΚΑΤΕΥΘΥΝΣΗΣ

Όπως αναφέρθηκε προηγουμένως η πολιτική δρομολόγησης είναι προγραμματισμένη στο συνοριακό δρομολογητή του ΠΣΔ με το ΕΔΕΤ. Η τυπική συγκρότηση γίνεται με τον ορισμό της πολιτικής και στην συνέχεια με την ενεργοποίηση της πολιτικής στις πόρτες του

δρομολογητή που μεταφέρουν κίνηση που παράγεται από σχολεία. Συνοπτικά η πολιτική δρομολόγησης όπως έχει εξηγηθεί παραπάνω είναι:

```
route-map proxy-redirect deny 10
!exclude Cache IP address, heavy loaded sites i.e. MSN, google etc
 match ip address PROXY-BYPASS
!
route-map proxy-redirect permit 20
 match ip address PROXY-REDIRECT-CACHE1
 set ip next-hop 194.63.239.231
!
route-map proxy-redirect permit 30
 match ip address PROXY-REDIRECT-CACHE2
 set ip next-hop 194.63.239.232
!
route-map proxy-redirect permit 40
 match ip address PROXY-REDIRECT-CACHE3
 set ip next-hop 194.63.239.233
!
route-map proxy-redirect permit 50
 match ip address PROXY-REDIRECT-CACHE4
 set ip next-hop 194.63.239.234
!
route-map proxy-redirect permit 60
 match ip address PROXY-REDIRECT-CACHE5
 set ip next-hop 194.63.239.235
!
route-map proxy-redirect permit 70
 match ip address PROXY-REDIRECT-CACHE6
 set ip next-hop 194.63.239.236
!
route-map proxy-redirect permit 80
 match ip address PROXY-REDIRECT-CACHE7
 set ip next-hop 194.63.239.237
!
route-map proxy-redirect permit 90
```

```
 match ip address PROXY-REDIRECT-CACHE8
 set ip next-hop 194.63.239.238
!
ip access-list extended PROXY-REDIRECT-CACHE1
 deny   tcp any any neq www
 deny   tcp any 194.63.239.224 0.0.0.31
 permit tcp any 0.0.0.0 255.255.255.248
ip access-list extended PROXY-REDIRECT-CACHE2
 deny   tcp any any neq www
deny   tcp any 194.63.239.224 0.0.0.31
 permit tcp any 0.0.0.1 255.255.255.248
ip access-list extended PROXY-REDIRECT-CACHE3
 deny   tcp any any neq www
 deny   tcp any 194.63.239.224 0.0.0.31
 permit tcp any 0.0.0.2 255.255.255.248
ip access-list extended PROXY-REDIRECT-CACHE4
 deny   tcp any any neq www
deny   tcp any 194.63.239.224 0.0.0.31
 permit tcp any 0.0.0.3 255.255.255.248
ip access-list extended PROXY-REDIRECT-CACHE5
 deny   tcp any any neq www
deny   tcp any 194.63.239.224 0.0.0.31
 permit tcp any 0.0.0.4 255.255.255.248
ip access-list extended PROXY-REDIRECT-CACHE6
 deny   tcp any any neq www
deny   tcp any 194.63.239.224 0.0.0.31
 permit tcp any 0.0.0.5 255.255.255.248
ip access-list extended PROXY-REDIRECT-CACHE7
 deny   tcp any any neq www
deny   tcp any 194.63.239.224 0.0.0.31
 permit tcp any 0.0.0.6 255.255.255.248
ip access-list extended PROXY-REDIRECT-CACHE8
 deny   tcp any any neq www
deny   tcp any 194.63.239.224 0.0.0.31
 permit tcp any 0.0.0.7 255.255.255.248
```

Ο συνδυασμός του route-map και ACL χωρίζει τις δ/σης σε 8 ομάδες και προωθεί την κάθε ομάδα σε ένα proxy. Δεδομένου ότι σε αρχικό στάδιο η κίνηση IPv6 δεν εκτιμάται να είναι μεγάλη προτείνεται να υπάρχει ένας μόνο εξυπηρετητής και στην συνέχεια να ενεργοποιούνται 2, 4 μέχρι 8. Ως εκ τούτου η αρχική τροποποίηση των παραπάνω δομών σε IPv6 μπορεί να είναι η ακόλουθη:

```
route-map proxy-v6-redirect-init deny 10
!exclude Cache IP address heavy loaded sites
 match ipv6 address PROXY-BYPASS-v6
!
route-map proxy-v6-redirect-init permit 20
 match ipv6 address PROXY-REDIRECT-v6-CACHE
!random IPv6 address since no real IPv6 address delegation has been made
 set ipv6 next-hop 2001:648:2302:FC02::231
!
ipv6 access-list PROXY-REDIRECT-v6-CACHE
 deny   tcp any any neq www
! exclude WWW originated trafic from servers
! i.e. exclude schdb.sch.gr—deny tcp any host …
! i.e. exclude the LAN of Proxy servers
deny tcp any 2001:648:2302:FC02::/64
 permit tcp any any
!
!
ipv6 access-list PROVY-BYPASS-v6
! permit tcp from SCH vlan
! permit tcp from VPN
! permit tcp from moodle – bbb server
! permit tcp server LANS
! permit tcp any callmanager
permit tcp any 2001:648:2302::/48
! permit tcp any KASPERSY-LABS
! permit tcp any Miscrosoft GLOBAL NET
!permit tcp any CAN
!permit tcp any limelightnetworks
```

4.3 ΕΝΕΡΓΟΠΟΙΗΣΗ IPV6 ΣΤΟ SQUID

Το λογισμικό Squid υποστηρίζει πλήρως το IPv6 από την έκδοση 3.1 Δεν θα χρειαστεί τίποτα το ιδιαίτερο για την ρύθμιση σε περιβάλλον native IPv6. Σχετικές πληροφορίες μπορεί να βρεθούν στο σύνδεσμο http://wiki.squid-cache.org/Features/IPv6.

4.4 ΕΝΕΡΓΟΠΟΙΗΣΗ IPV6 ΣΤΟ SQUIDGUARD (SG)

Το λογισμικό Squidguard είναι το αποθετήριο των απαγορευμένων διευθύνσεων προορισμού του ΠΣΔ. Το SG λειτουργεί ως εξωτερική βοηθητική μονάδα (external authentication). Η ενσωμάτωση της λειτουργικότητας για το IPv6 έρχεται από ένα ανεξάρτητο προγραμματιστή στο σύνδεσμο:

https://github.com/andihofmeister/squidGuard

Ειδικότερα αυτό που ενδιαφέρει είναι η λίστα προορισμών που περιγράφεται με το "in-addr" π.χ. http://[2a02:2e0:3fe:100::7]. Η χρήση διευθύνσεων IPv6 εντός των URL επιτρέπει αρκετές δυνατότητες και ως εκ τούτου η μετάφραση τους στην κανονική μορφή δεν είναι πάντα εφικτή. Για αυτές τις περιπτώσεις προτείνεται να αποκόπτονται ολόκληρα τα μπλόκ των διευθύνσεων.

5. ΠΑΡΟΧΗ ΥΠΗΡΕΣΙΑΣ ΕΛΕΓΧΟΥ ΠΕΡΙΕΧΟΜΕΝΟΥ ΣΕ ΤΡΙΤΟΥΣ ΜΕΣΩ DNS

5.1 ΠΕΡΙΓΡΑΦΗ ΠΡΟΒΛΗΜΑΤΟΣ ΚΑΙ ΒΑΣΙΚΕΣ ΑΠΑΙΤΗΣΕΙΣ

Στους χρήστες που βρίσκονται εντός του ΠΣΔ εφαρμόζεται κεντρικά έλεγχος περιεχομένου για την εμπόδιση πρόσβασης σε σελίδες με ακατάλληλο ή επικίνδυνο περιεχόμενο. Το σύνολο των ακατάλληλων σελίδων διατηρείται σε ειδικά διαμορφωμένη βάση δεδομένων. Στόχος είναι η δυνατότητα χρησιμοποίησης της βάσης δεδομένων από τρίτους που δεν βρίσκονται εντός του ΠΣΔ, για παράδειγμα από γονείς σε οικιακές συνδέσεις.

Στο ΠΣΔ έχουν αναπτυχθεί διαδικασίες για την συντήρηση και επικαιροποίηση της βάσης δεδομένων. Οι διαδικασίες αυτές αποτελούνται από αυτόματες ενημερώσεις από άλλες γνωστές και ευρέως χρησιμοποιούμενες βάσεις στο Διαδίκτυο, αλλά και από χειροκίνητες εισαγωγές (ή αντίθετα εξαιρέσεις) ύστερα από αιτήματα των χρηστών. Συνεπώς, προκειμένου η νέα υπηρεσία να έχει όσο το δυνατόν λιγότερο διαχειριστικό κόστος, είναι απαραίτητο να χρησιμοποιηθεί η υπάρχουσα βάση δεδομένων από την υπηρεσία ελέγχου περιεχομένου εντός του ΠΣΔ.

Εντός του ΠΣΔ, ο έλεγχος περιεχομένου βασίζεται στην αυτόματη αναδρομολόγηση των αιτήσεων HTTP των χρηστών του ΠΣΔ σε μια συστοιχία εξυπηρετητών proxy. Επειδή δεν υπάρχει αντίστοιχος τρόπος για αυτόματη δρομολόγηση αιτήσεων από χρήστες που βρίσκονται σε διαφορετικά δίκτυα, προτείνεται η χρήση της υπηρεσίας ονοματολογίας (DNS).

Στο Διαδίκτυο το κατανεμημένο σύστημα ονοματολογίας που ονομάζεται Domain Naming System (DNS) επιτρέπει την αναφορά σε κόμβους του δικτύου όχι με την IP διεύθυνσή τους (Internet Protocol address) αλλά με μνημονικά ονόματα (hostnames). Οι πληροφορίες ονοματολογίας καταχωρούν και διαχωρίζουν τα ονόματα σε διαφορετικές ζώνες οι οποίες γίνονται διακριτές στα ονόματα από την ύπαρξη της τελείας (.) Για παράδειγμα το όνομα www.sch.gr δηλώνει την ύπαρξη 3 ζωνών (.sch, .gr και της έμμεσα δηλωμένης ζώνης ρίζας (.))που αποθηκεύονται σε διαφορετικούς εξυπηρετητές. Ο εξυπηρετητής Ονοματολογίας που είναι υπεύθυνος για κάποια συγκεκριμένη ζώνη, αυτός δηλαδή που διατηρεί την πρωτογενώς καταχωρημένη πληροφορία, ονομάζεται authoritative nameserver. Ο εξυπηρετητής ο οποίος

αναλαμβάνει την εύρεση της IP διεύθυνσης ενός hostname αναζητώντας τον κατάλληλο authoritative nameserver, ονομάζεται recursive/caching name server.

Ο στόχος είναι η εκμετάλλευση του πρωτοκόλλου DNS ώστε όταν κάποια αίτηση περιέχει hostname το οποίο θεωρείται ακατάλληλο (βρίσκεται δηλαδή στη βάση δεδομένων της υπηρεσίας ελέγχου περιεχομένου του ΠΣΔ), αντί να επιστρέφεται από τον εξυπηρετητή ονοματολογίας η πραγματική IP διεύθυνση του hostname, να επιστρέφεται η διεύθυνση εξυπηρετητή του σχολικού δικτύου. Με τον τρόπο αυτό, ο χρήστης θα οδηγείται σε ειδική σελίδα και θα ενημερώνεται ότι ο δικτυακός τόπος που θέλει να επισκεφθεί είναι ακατάλληλος.

Για την εφαρμογή της παραπάνω διαδικασίας χρειάζεται:

- Διαχωρισμός των εξυπηρετητών ονοματολογίας του ΠΣΔ σε authoritative και recursive
- Δημιουργία και παραμετροποίηση ειδικού λογισμικού το οποίο θα λειτουργεί ως recursive/caching nameserver, το οποίο πριν επιστρέψει την πραγματική διεύθυνση ενός hostname θα ελέγχει αν ανήκει στη βάση δεδομένων της υπηρεσίας ελέγχου περιεχομένου.
- Κάθε χρήστης που θέλει να χρησιμοποιήσει την υπηρεσία, να ορίζει χειροκίνητα στον υπολογιστή του, ως εξυπηρετητές ονοματολογίας, τους ειδικά διαμορφωμένους εξυπηρετητές που θα στηθούν για την νέα υπηρεσία. Για τις περιπτώσεις οικιακών δικτυακών συνδέσεων (π.χ. συνδέσεις ADSL) ο ορισμός του εξυπηρετητή ονοματολογίας μπορεί να οριστεί κεντρικά στο δρομολογητή της σύνδεσης (ADSL modem/router). Με τον τρόπο αυτό καλύπτονται όλες οι συσκευές στο σπίτι που χρησιμοποιούν τη συγκεκριμένη σύνδεση.

Καθώς θα χρησιμοποιηθεί η υπηρεσία ονοματολογίας για το φιλτράρισμα του περιεχομένου, από τις διαθέσιμες λίστες που βρίσκονται στη βάση δεδομένων του ΠΣΔ για τον έλεγχο περιεχομένου είναι δυνατό να χρησιμοποιηθεί μονάχα η λίστα ονομάτων ιστοτόπων (hostnames, διευθύνσεις IP, domain names) που περιέχουν αποκλειστικά ακατάλληλο περιεχόμενο.

Για λόγους καλής λειτουργίας των recursive/caching nameserver και προκειμένου να μπορούν να αντεπεξέρθουν στο φορτίο, συνήθως αυτοί ρυθμίζονται έτσι ώστε να δέχονται αιτήσεις μονάχα από υπολογιστές που ανήκουν στο δίκτυό τους. Στην περίπτωση της υπηρεσίας αυτής, οι nameserver που θα στηθούν θα πρέπει να είναι «ανοιχτοί» σε αιτήματα από εξωτερικά δίκτυα. Ανάλογα με το πόσο δημοφιλής μπορεί να γίνει η υπηρεσία, μπορεί να αυξηθεί αρκετά το φορτίο στα μηχανήματα αυτά. Συνεπώς, θα πρέπει:

- Να προβλεφθεί κατά τη μελέτη και ανάπτυξη της υπηρεσίας η χρήση λογισμικού το οποίο θα μπορεί να υποστεί μεγάλο φορτίο.
- Να διαχωριστεί η νέα υπηρεσία ονοματολογίας από την υπάρχουσα, ώστε να μην επηρεαστεί η ποιότητα υπηρεσίας εντός του ΠΣΔ.
- Να εξεταστεί κατά πόσο είναι δυνατόν να περιοριστεί η πρόσβαση σε κόμβους που ανήκουν σε συγκεκριμένα δίκτυα (π.χ. σε δίκτυα μονάχα στην Ελλάδα).

5.2 ΠΑΡΟΜΟΙΕΣ ΥΠΗΡΕΣΙΕΣ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

Υπηρεσία παρόμοια με αυτή που προτείνεται στο υπάρχον κείμενο προσφέρεται από τον οργανισμό openDNS (http://www.opendns.com/). Πέρα από τη βασική και κρίσιμη μετάφραση ονομάτων (name resolution), το OpenDNS προσφέρει και κάποια άλλα πράγματα. Π.χ.:

- Διορθώνει λάθη πληκτρολόγησης. Αν για παράδειγμα ο χρήστης πληκτρολογήσει κατά λάθος το όνομα exemple.com αντί για το example.com, επιστρέφεται τελικά στο χρήστη μια σελίδα με προτάσεις ή με το σύνδεσμο για το δικτυακό τόπο τον οποίο ήθελε να επισκεφθεί ο χρήστης. Για τη λειτουργία αυτή χρειάζεται η συνεργασία ανάμεσα σε name server και web server. Στη πράξη, η λειτουργία αυτή προσφέρεται ήδη από διάφορους browser (για παράδειγμα τον chrome σε συνεργασία με το google search engine)
- Με την αξιοποίηση δεδομένων που συλλέγει ειδικό λογισμικό ασφαλείας, προστατεύει κατά του «phishing» (phishing: κακόβουλοι ιστότοποι που συστήνονται ως κάτι άλλο απ' αυτό που είναι, με σκοπό συνήθως να αποσπάσουν προσωπικά

ευαίσθητα δεδομένα των χρηστών, όπως για παράδειγμα στοιχεία πιστωτικών καρτών).

Η υπηρεσία αυτή παρέχεται δωρεάν σε οικιακούς χρήστες, και επί πληρωμή σε μεγαλύτερους ή πολύ μεγάλους πελάτες, μαζί με την προσφορά επιπλέον χαρακτηριστικών, όπως ο γονικός έλεγχος (parental control) που ενδιαφέρει και στην περίπτωση που εξετάζεται.

Παρόμοια υπηρεσία προσφέρεται και από τη Norton. Πιο συγκεκριμένα, η υπηρεσία που ονομάζεται Norton DNS (https://dns.norton.com/dnsweb/) προσφέρει δημόσιους name servers με την παρακάτω πολιτική:

- Πολιτική 1 - Ασφάλεια: Αυτή η πολιτική εμποδίζει όλους τους τόπους που φιλοξενούν malware, phishing, και γενικότερα ιστοσελίδες με μη ασφαλές περιεχόμενο.
- Πολιτική 2 - Ασφάλεια + Πορνογραφία: Εκτός από τον αποκλεισμό των μη ασφαλών δικτυακών τόπων, αυτή η πολιτική εμποδίζει την πρόσβαση σε ιστοσελίδες που περιέχουν υλικό σεξουαλικού περιεχομένου.
- Πολιτική 3 - Ασφάλεια, Πορνογραφία και μη φιλικές προς οικογένειες ιστοσελίδες (non-Family Friendly). Η πολιτική αυτή απευθύνεται σε οικογένειες με μικρά παιδιά. Εκτός από τον αποκλεισμό των μη ασφαλών ιστοσελίδων και των ιστοσελίδων με πορνογραφία, αυτή η πολιτική εμποδίζει την πρόσβαση σε ιστοσελίδες που διαθέτουν περιεχόμενο που απευθύνεται σε ενήλικες, με θέματα όπως το αλκοόλ, το έγκλημα, τα ναρκωτικά, τα τυχερά παιχνίδια, το κάπνισμα ή τη βία.

Σε κάθε διαφορετική πολιτική, διατίθεται ξεχωριστό ζεύγος από Name server.

5.3 ΠΕΡΙΓΡΑΦΗ ΛΥΣΗΣ

Για την κάλυψη των απαιτήσεων που περιγράφηκαν στην προηγούμενη ενότητα, προτείνεται το λογισμικό BIND σε συνδυασμό με τη χρήση της τεχνολογίας Response Policy Zones (RPZ).

Το BIND είναι το μακράν πιο ευρέως χρησιμοποιούμενο λογισμικό DNS στο Διαδίκτυο. Είναι λογισμικό ανοιχτού κώδικα που υλοποιεί τα πρωτόκολλα του Domain Name System για το Διαδίκτυο. Είναι μια εφαρμογή αναφοράς για τα πρωτόκολλα αυτά, αλλά είναι επίσης λογισμικό που χρησιμοποιείται ευρέως σε συστήματα παραγωγής, καθώς είναι κατάλληλο για χρήση σε μεγάλου όγκου και υψηλής αξιοπιστίας συστήματα.

Η έκδοση BIND 9.8.1 περιλαμβάνει το Response Policy Zone (RPZ) Rewriting, έναν μηχανισμό τροποποίησης των DNS απαντήσεων για αναδρομικές αιτήσεις (requerive queries), παρόμοιο σε λειτουργία με τις anti-spam DNS Blacklists. Με το μηχανισμό αυτό, η απάντηση σε κάποιο αίτημα ονοματολογίας μπορεί να αλλάξει και αντί για την επιστροφή της διεύθυνσης IP του hostname που ζητήθηκε, ο εξυπηρετητής ονοματολογίας είτε να αρνηθεί την ύπαρξη της δικτυακής υποπεριοχής (NXDOMAIN), είτε να αρνηθεί την ύπαρξη διευθύνσεων IP για τον συγκεκριμένο δικτυακό τόπο (NODATA), ή να επιστρέψει άλλη IP διεύθυνση.

Οι ζώνες RPZ είναι κοινές ζώνες DNS που περιέχουν εγγραφές DNS (RRsets) που θα μπορούσαν να χρησιμοποιηθούν σε οποιαδήποτε άλλη ζώνη ονοματολογίας. Προκειμένου να ενεργοποιηθεί ο μηχανισμός τροποποίησης, οι ζώνες αυτές ορίζονται με τη επιλογή response-policy option στο αρχείο ρυθμίσεων του BIND.

Υπάρχουν τέσσερα είδη εγγραφών στις ζώνες RPZ: QNAME, IP, NSIP, και NSDNAME. Από τα παραπάνω είδη, στην περίπτωσή που ενδιαφέρει την παρούσα μελέτη, μπορούν να χρησιμοποιηθούν οι εγγραφές IP και QNAME (που αφορούν ερωτήσεις A, AAAA και CNAME).

Συνεπώς, τα βήματα που χρειάζεται να γίνουν για την εγκατάσταση της υπηρεσίας είναι τα ακόλουθα:

- Εγκατάσταση σε κατάλληλους εξυπηρετητές του λογισμικού BIND 9.8.1 ή νεότερου με δυνατότητα χρήσης RPZ με παράλληλη ρύθμιση για αποδοχή αναδρομικών αιτημάτων από εξωτερικά δίκτυα (εκτός ΠΣΔ). Τα δίκτυα από τα οποία θα επιτρέπεται να δρομολογηθούν αιτήματα ονοματολογίας προς τους εξυπηρετητές

αυτούς μπορούν να περιοριστούν στον ελληνικό χώρο (ΠΣΔ,ΕΔΕΤ,GRIX), ρυθμίζοντας κατάλληλες access lists στους συνοριακούς δρομολογητές του ΠΣΔ.

- Δημιουργία ενός προγράμματος (script) που θα τρέχει περιοδικά, σε χρόνους που αντιστοιχούν στο χρονοδιάγραμμα αυτόματης ανανέωσης της βάσης δεδομένων της υπηρεσίας ελέγχου περιεχομένου του ΠΣΔ, το οποίο θα συλλέγει τα hostname που φιλοξενούν ακατάλληλες ιστοσελίδες και θα εισάγει αντίστοιχες εγγραφές (A,AAAA,CNAME) σε μια ειδική ζώνη ονοματολογίας.
- Η ζώνη ονοματολογίας θα προσφέρεται από τους εξυπηρετητές ονοματολογίας της υπηρεσίας και θα επαναφορτώνεται αυτόματα μετά από κάθε εκτέλεση του script.
- Λειτουργία web server στον οποίο θα ανακατευθύνονται μέσω DNS/RPZ οι χρήστες που έχουν ορίζει ως name server τους εξυπηρετητές της νέας υπηρεσίας, ο οποίος θα προσφέρει ειδική σελίδα που θα ενημερώνει το χρήστη ότι προσπάθησε να προσπελάσει ακατάλληλο ή επικίνδυνο περιεχόμενο. Αντίστοιχη υπηρεσία χρησιμοποιείται είδη για τον έλεγχο περιεχομένου εκτός του ΠΣΔ.

5.4 ΠΑΡΑΔΕΙΓΜΑ ΠΑΡΑΜΕΤΡΟΠΟΙΗΣΗΣ ΤΟΥ BIND9 ΓΙΑ ΤΗ ΧΡΗΣΗ RPZ

Στο αρχείο ρυθμίσεων named.conf του BIND, στις κεντρικές ρυθμίσεις:

```
response-policy { zone "blockedhosts"; };
```

Στο τμήμα ορισμού των ζωνών τις οποίες σερβίρει ο εξυπηρετητής:

```
zone " blockedhosts " {type master; file "master/badlist"; allow-query {none;}; };
```

Ενδεικτικά τα περιεχόμενα της ζώνης blockedhosts:

```
$TTL 1H
@                                       SOA LOCALHOST. ns1.sch.gr (1 1h 15m 30d 2h)
                                        NS LOCALHOST.


; QNAME policy records.
nxdomain.domain.com             CNAME .                 ; NXDOMAIN policy
nodata.domain.com               CNAME *.                ; NODATA policy
bad.domain.com                  A 10.0.0.1              ; redirect to a walled garden
```

```
                                        AAAA 2001:2::1

                                        CNAME garden.sch.gr


; do not rewrite (PASSTHRU) OK.DOMAIN.COM

ok.domain.com                   CNAME ok.domain.com.
```

Στο παραπάνω αρχείο υπάρχουν οι εξής περιπτώσεις λειτουργίας:

- Ερωτήσεις για το domain nxdomain.domain.com, επιστρέφουν απάντηση NXDOMAIN.
- Ερωτήσεις για το domain nodata.domain.com, επιστρέφουν απάντηση NODATA.
- Ερωτήσεις τύπου A,AAAA,CNAME για το bad.domain.com, προκαλούν ανακατεύθυνση σε μηχάνημα της επιλογής του διαχειριστή. Στη συγκεκριμένη περίπτωση, πρόκειται για το μηχάνημα garden.sch.gr , με διευθύνσεις 10.0.0.1 και 2001:2::1.
- Το domain ok.domain.com δεν υπόκειται σε ανακατεύθυνση (PASSTHROU).

Οι εγγραφές έχουν χρόνο ζωής (Time to Live - TTL) μία ώρα, ώστε να μην κρατούνται πάνω από μια ώρα στη λανθάνουσα μνήμη των υπολογιστών-πελατών, και να είναι σχετικά άμεση η διόρθωση σε περίπτωση λανθασμένης εισαγωγής κάποιου δικτυακού τόπου στη βάση δεδομένων και κατ' επέκταση στη ζώνη RPZ. Περισσότερες λεπτομέρειες είναι διαθέσιμες στο εγχειρίδιο χρήσης του λογισμικού BIND (BIND9 Reference – http://ftp.isc.org/isc/bind9/cur/9.8/doc/arm/Bv9ARM.pdf).

6. ΥΛΟΠΟΙΗΣΗ ΥΠΗΡΕΣΙΑΣ ΓΙΑ ΤΟ ΠΡΩΤΟΚΟΛΛΟ HTTPS

Η τρέχουσα έκδοση της υπηρεσίας ελέγχου περιεχομένου του ΠΣΔ αναδρομολογεί τις κλήσεις που γίνονται μέσω του πρωτοκόλλου HTTP (θύρα TCP 80). Οι κλήσεις που γίνονται μέσω του πρωτοκόλλου HTTPS (Secure HTTP – θύρα TCP 433), όπως και τυχόν κλήσεις μέσω πρωτοκόλλου HTTP σε θύρες διαφορετικές της 80 δεν αναδρομολογούνται και κατά συνέπεια δεν ελέγχονται για ακατάλληλο περιεχόμενο.

Η συγκεκριμένη προσέγγιση, μέχρι στιγμής δεν έχει δημιουργήσει παράπονα από τους χρήστες του ΠΣΔ καθώς δεν έχουν εμφανιστεί περιπτώσεις ιστοσελίδων με ακατάλληλο περιεχόμενο που να διατίθενται μέσω θυρών διαφορετικών της 80. Εξαίρεση στον κανόνα αποτελούν οι ιστότοποι κοινωνικής δικτύωσης, όπως το Facebook, το Google+ κλπ., οι οποίοι πλέον σε μία προσπάθεια να διασφαλίσουν το απόρρητο της επικοινωνίας και των δεδομένων των χρηστών τους διαθέτουν τις υπηρεσίες μέσω του πρωτοκόλλου HTTPS. Οι συγκεκριμένες υπηρεσίες, κατόπιν απόφασης του ΠΣΔ, δεν είναι διαθέσιμες στους μαθητές των Δημοτικών σχολείων (παιδιά ηλικίας μικρότερης των 13 ετών). Ο συγκεκριμένος περιορισμός δεν έχει εφαρμοστεί μέσω της υπηρεσίας ελέγχου περιεχομένου καθώς όλες οι εκπαιδευτικές μονάδες, ανεξαρτήτου βαθμίδας, λαμβάνουν διευθύνσεις IP από κοινό χώρο διευθύνσεων και συνεπώς δεν είναι δυνατό να διαχωριστούν σε Δημοτικά σχολεία και λοιπά. Αντί αυτού, προτιμήθηκε η επιλεκτική εφαρμογή access list στους δρομολογητές των Δημοτικών σχολείων με αυτοματοποιημένο τρόπου μέσω της υπηρεσία Radius.

Η εκτίμηση που επικρατεί είναι πως και στο μέλλον δεν πρόκειται να εμφανιστούν σοβαρές περιπτώσεις ιστοτόπων με ακατάλληλο περιεχόμενο που να διατίθενται μέσω πρωτοκόλλου HTTPS ή άλλης θύρας διαφορετικής της 80. Σε κάθε περίπτωση όμως, η υπηρεσία ελέγχου περιεχομένου του ΠΣΔ θα πρέπει να είναι σε θέση να αντιμετωπίσει τέτοιες περιπτώσεις, είτε στα πλαίσια της τυπικής λειτουργίας της, είτε με εναλλακτικούς τρόπους.

6.1 ΤΡΟΠΟΙ ΕΛΕΓΧΟΥ ΚΙΝΗΣΗΣ HTTPS ΜΕΣΩ ΛΟΓΙΣΜΙΚΟΥ SQUID

Η υπηρεσία ελέγχου περιεχομένου, όπως αναφέρθηκε και σε προηγούμενα κεφάλαια λειτουργεί σε μορφή transparent proxy με τους εξυπηρετητές της υπηρεσίας να

παρεμβάλλονται ανάμεσα στους φυλλομετρητές των χρηστών και τους ιστότοπους που ζητούν να επισκεφτούν. Οι συνδέσεις των χρηστών καταλήγουν στους εξυπηρετητές της υπηρεσίας και αυτοί με τη σειρά τους ξεκινούν νέες προς τους ιστότοπους. Όμως, οι συνδέσεις HTTPS έχουν ως βασικό χαρακτηριστικό τους ότι ο φυλλομετρητής του χρήστη δέχεται από τον ιστότοπο υπογεγραμμένο ψηφιακό πιστοποιητικό που αποδεικνύει την αυθεντικότητά του και εξασφαλίζει το απόρρητο της επικοινωνίας και την ακεραιότητα των δεδομένων που διακινούνται.

Σε περίπτωση που παρεμβληθεί ανάμεσα τους κάποιος τρίτος, έστω και οι εξυπηρετητές του ΠΣΔ, τίθενται θέματα εμπιστευτικότητας και παραβίασης απορρήτου επικοινωνιών και ως εκ τούτου θεωρείται κακή πρακτική (man in the middle attack). Από την κοινότητα του λογισμικού Squid έχουν αναπτυχθεί ορισμένες τεχνολογίες που επιτρέπουν την αναδρομολόγηση συνδέσεων HTTPS σε περιβάλλον transparent proxy όπως η τεχνολογία «Squid-in-the-middle SSL Bump» (βλ. http://wiki.squid-cache.org/Features/SslBump). Στην περίπτωση αυτή, το λογισμικό Squid παρουσιάζει στο χρήστη ένα δικό του ψηφιακό πιστοποιητικό και στη συνέχεια ξεκινάει νέα σύνδεση HTTPS με το ζητούμενο ιστότοπο. Το μειονέκτημα της συγκεκριμένης μεθόδου είναι ότι το ψηφιακό πιστοποιητικό του Squid δεν ταιριάζει με το όνομα του ιστότοπου που ζητάει ο χρήστης και στις περισσότερες περιπτώσεις κάθε σύγχρονος φυλλομετρητής θα παρουσιάσει μία ή περισσότερες προειδοποιήσεις (warnings) στο χρήστη, τις οποίες ο χρήστης θα κληθεί να αγνοήσει. Κάτι τέτοιο είναι εντελώς αντίθετο με την κουλτούρα που προσπαθεί να εμπεδώσει το ΠΣΔ στους νέους χρήστες του διαδικτύου για ασφαλή περιήγηση σε αυτό.

Για την ελαχιστοποίηση των προειδοποιήσεων των φυλλομετρητών αναπτύσσονται από την κοινότητα του λογισμικού Squid οι τεχνολογίες «Dynamic SSL Certificate Generation» (βλ. http://wiki.squid-cache.org/Features/DynamicSslCert) και «SslBump using Bump-Server-First method» (http://wiki.squid-cache.org/Features/BumpSslServerFirst). Η πρώτη είναι διαθέσιμη στην έκδοση 3.2 και επιτρέπει την έκδοση ψηφιακών πιστοποιητικών σε πραγματικό χρόνο από Αρχή Πιστοποίησης που μπορεί διαθέτει εσωτερικά το λογισμικό Squid, αλλά από μόνη της δεν μπορεί να λειτουργήσει σε σχήμα transparent proxy. Η δεύτερη βρίσκεται υπό ανάπτυξη, θα είναι διαθέσιμη στην έκδοση 3.3 και χρησιμοποιείται για

να μεταφέρει σε σχήμα transparent proxy το σωστό όνομα του τελικού ιστότοπου στην Αρχή Πιστοποίησης που θα παραγάγει το προσωρινό πιστοποιητικό.

6.2 ΕΝΑΛΛΑΚΤΙΚΟΙ ΤΡΟΠΟΙ ΕΛΕΓΧΟΥ ΚΙΝΗΣΗΣ HTTPS

Εναλλακτικοί τρόποι αντιμετώπισης ιστότοπων με ακατάλληλο περιεχόμενο σε θύρες διαφορετικές της 80 είναι:

1. Εφαρμογή περιορισμού πρόσβασης στους συγκεκριμένους ιστότοπους με την προθήκη κατάλληλης εγγραφής στην access list που υπάρχει στη σύνδεση του ΠΣΔ - ΕΔΕΤ του συνοριακού δρομολογητή. Η συγκεκριμένη access list μπορεί να δεχτεί δεκάδες, ίσως και εκατοντάδες, νέες εγγραφές, υπεραρκετές για τις λίγες περιπτώσεις που αναμένεται τυχόν να εμφανιστούν.
2. Αξιοποίηση του μηχανισμού ελέγχου περιεχομένου μέσω πρωτοκόλλου DNS, που περιγράφηκε σε προηγούμενο κεφάλαιο, εντός ΠΣΔ με εγκατάστασή του στους εξυπηρετητές ονοματολογίας που χρησιμοποιούν οι τελικοί χρήστες του ΠΣΔ. Με τον τρόπο αυτό, οι χρήστες δεν θα μπορούν να έχουν πρόσβαση στους ιστότοπους που αποκλείονται ασχέτως της θύρας που χρησιμοποιούν αυτοί.

Σημειώνεται ότι οι παραπάνω δύο προτεινόμενοι εναλλακτικοί τρόποι λειτουργούν για ολόκληρους ιστότοπους και όχι για μεμονωμένες ιστοσελίδες, δηλαδή δεν επιτρέπουν τον αποκλεισμό της πρόσβασης αποκλειστικά σε συγκεκριμένες ιστοσελίδες.

7. ΠΛΑΝΟ ΑΝΑΒΑΘΜΙΣΕΩΝ ΚΑΙ ΕΡΓΑΣΙΩΝ

7.1 ΑΝΑΒΑΘΜΙΣΗ ΛΕΙΤΟΥΡΓΙΚΟΥ ΣΥΣΤΗΜΑΤΟΣ ΕΞΥΠΗΡΕΤΗΤΩΝ ΣΤΗΝ ΕΚΔΟΣΗ FREEBSD 9.1

Η συγκεκριμένη έκδοση του λειτουργικού συστήματος FreeBSD αναμένεται να είναι διαθέσιμη προς χρήση εντός του Οκτωβρίου του 2012. Αυτή τη στιγμή είναι διαθέσιμη η πρώτη υποψήφια έκδοσή της (9.1-RC1), η οποία κυκλοφόρησε στις 23/8/2012. Θα υπάρξει μία δεύτερη υποψήφια έκδοση (9.1-RC2), συνήθως 45 ημέρες μετά την πρώτη και στη συνέχεια θα κυκλοφορήσει η τελική έκδοση (9.1-RELEASE). Η έκδοση 9.1 θα έχει το χαρακτηρισμό «Extended» που σημαίνει ότι θα υποστηρίζεται για δύο έτη (βλ. http://www.freebsd.org/security/#sup – Supported FreeBSD Releases), σε αντίθεση με τις εκδόσεις που χαρακτηρίζονται «Normal» και υποστηρίζονται για ένα έτος.

Σε περίπτωση που η έκδοση 9.1 καθυστερήσει πέρα του Οκτωβρίου, μπορεί να χρησιμοποιηθεί η έκδοση 8.3 (Extended με υποστήριξη έως τις 30/4/2014) και αργότερα να γίνει η αναβάθμιση. Σε κάθε περίπτωση η σειρά 9.x είναι προτιμότερη καθώς περιλαμβάνει αρκετά νέα χαρακτηριστικά και θα είναι περισσότερο καιρό υποστηριζόμενη με νέες εκδόσεις.

Για τη δοκιμαστική αναβάθμιση στην έκδοση 9.1 (ή την 8.3) και τον έλεγχο της καλής λειτουργίας της υπηρεσίας σε αυτήν προτείνεται να χρησιμοποιηθούν αρχικά οι εξυπηρετητές cache09.att.sch.gr και cache10.att.sch.gr, οι οποίοι αυτή τη στιγμή δεν χρησιμοποιούνται παραγωγικά και είναι διαθέσιμοι για δοκιμές και ως εφεδρικοί. Όταν είναι έτοιμοι μπορούν να δοκιμαστούν στη θέση κάποιων εκ των cache01 έως cache08, για συγκεκριμένο χρονικό διάστημα, με μια απλή αλλαγή στην παράμετρο ip next-hop των route-map proxy-redirect.

Εφόσον τα αποτελέσματα των δοκιμών είναι ενθαρρυντικά, μπορεί να προχωρήσει η αναβάθμιση των εξυπηρετητών cache01 έως cache08. Η αναβάθμιση μπορεί να γίνει ανά ζεύγος (cache01-cache02, cache03-cache04 κλπ.) με τους cache09 και cache10 να αναλαμβάνουν την εξυπηρέτηση των αιτημάτων τους για όσο χρόνο διαρκεί η διαδικασία αναβάθμισης. Με τον τρόπο αυτό, δεν πρόκειται να υπάρξει διακοπή στην υπηρεσία που

απολαμβάνουν οι χρήστες του ΠΣΔ (downtime), ούτε πίεση για βεβιασμένες αναβαθμίσεις ή για αναβαθμίσεις σε μέρες και ώρες που το δίκτυο υπολειτουργεί.

Το μόνο προαπαιτούμενο για τη συγκεκριμένη ενέργεια είναι η κυκλοφορία της έκδοσης 9.1 του λειτουργικού συστήματος FreeBSD.

7.2 ΑΝΑΒΑΘΜΙΣΗ ΛΟΓΙΣΜΙΚΟΥ SQUID ΣΤΗΝ ΕΚΔΟΣΗ 3.1

Το λογισμικό Squid διαθέτει αυτή τη στιγμή τρεις κύριες εκδόσεις (βλ. http://www.squid-cache.org/Versions/):

1. Την 2.7, με τελευταία υποέκδοση την 2.7.STABLE9 που κυκλοφόρησε στις 31/5/2008. Θεωρείτε από πολλούς ως η πλέον σταθερή και ώριμη έκδοση πριν τη ριζοσπαστική έκδοση 3.0 (κατά την οποία μεγάλο μέρος του κώδικα γράφτηκε ξανά από την αρχή). Χρησιμοποιείται ακόμη σε πολλές εγκαταστάσεις (και στο ΠΣΔ), παρόλο που πλέον δεν υποστηρίζεται.
2. Την 3.1, με τελευταία υποέκδοση την 3.1.20 που κυκλοφόρησε στις 8/7/2012. Είναι η πρώτη από τις εκδόσεις της σειράς 3.x που θεωρείται αρκετά σταθερή και ώριμη για παραγωγική λειτουργία σε περιβάλλοντα υψηλών απαιτήσεων, όπως το ΠΣΔ. Περιλαμβάνει υποστήριξη για όλες τις νέες τεχνολογίες, όπως IPv6 και WCCPv1/v2. Εξακολουθεί να υποστηρίζεται ενεργά με διορθώσεις και προσθήκες νέων χαρακτηριστικών που αναπτύσσονται σε νεότερες εκδόσεις.
3. Την 3.2, με τελευταία υποέκδοση την 3.2.1 που κυκλοφόρησε στις 14/8/2012. Πρόκειται για την πρώτη έκδοση της σειράς 3.2 και χαρακτηρίζεται από τους δημιουργούς της ως σταθερή έκδοση κατάλληλη για παραγωγική χρήση. Το γεγονός όμως ότι πρακτικά δεν έχει δοκιμαστεί ακόμη ευρέως σε περιβάλλοντα παραγωγής με υψηλές απαιτήσεις δεν την καθιστά καλή υποψήφιο για χρήση, προς το παρόν στο ΠΣΔ.

Με βάση τα παραπάνω, κρίνουμε ότι η καταλληλότερη έκδοση του λογισμικού Squid για το ΠΣΔ είναι η 3.1, καθώς καλύπτει τις ανάγκες για εξελιγμένα χαρακτηριστικά και παράλληλα

μπορεί να εγγυηθεί την απρόσκοπτη λειτουργίας της σε ένα περιβάλλον υψηλών απαιτήσεων όπως το ΠΣΔ.

Για την αναβάθμιση του λογισμικού Squid στους εξυπηρετητές της υπηρεσίας ελέγχου περιεχομένου μπορεί να ακολουθηθεί μια προσέγγιση σαν αυτήν που περιγράφεται στο κεφαλαίο για την αναβάθμιση του λειτουργικού συστήματος των εξυπηρετητών. Δηλαδή, αρχικά στα δύο εφεδρικά συστήματα, στη συνέχεια δοκιμή των δύο αυτών συστημάτων στη θέση δύο εν των cache01 – cache08 και τέλος σταδιακή, ανά ζεύγος, αναβάθμιση στα οκτώ συστήματα παραγωγής. Με τον τρόπο αυτό, ούτε στην περίπτωση αυτή θα υπάρξει διακοπή της λειτουργίας της υπηρεσίας.

Η συγκεκριμένη ενέργεια δεν έχει προαπαιτούμενα για την υλοποίησή της, για παράδειγμα δεν επηρεάζεται από την έκδοση του λειτουργικού συστήματος. Συνεπώς, μπορεί να ξεκινήσει το συντομότερο δυνατόν, αξιοποιώντας για παράδειγμα το χρόνο αναμονής για την κυκλοφορία της έκδοσης 9.1 του FreeBSD. Επιμέρους λειτουργίες, όπως υποστήριξη του πρωτοκόλλου IPv6 ή των πρωτοκόλλων ανακατεύθυνσης WCCP v1 και v2 μπορούν να ενεργοποιηθούν αργότερα όταν θα είναι έτοιμα και τα υπόλοιπα υποσυστήματα (λειτουργικό σύστημα εξυπηρετητών και συνοριακός δρομολογητής).

7.3 ΑΝΑΒΑΘΜΙΣΗ ΛΟΓΙΣΜΙΚΟΥ SQUIDGUARD

Η τρέχουσα σταθερή έκδοση του λογισμικού SquidGuard (χρησιμοποιείται και στο ΠΣΔ) είναι η 1.4 που κυκλοφόρησε το 2009. Έκτοτε έχει κυκλοφορήσει η έκδοση 1.5 που χαρακτηρίζεται ως beta. Γενικότερα, η κοινότητα που αναπτύσσει το συγκεκριμένο λογισμικό δεν είναι ιδιαίτερα δραστήρια τα τελευταία χρόνια καθώς αυτό έχει φτάσει σε ένα επίπεδο ωριμότητας που καλύπτει σχεδόν πλήρως τις ανάγκες των χρηστών του.

Η μόνη εκκρεμότητα που είχε μείνει ήταν η υποστήριξη για το πρωτόκολλο IPv6. Η συγκεκριμένη εκκρεμότητα μοιάζει να έχει καλυφθεί μετά από ανακοίνωση στην επίσημη mailing list squidguard@shalla.de ότι είναι πλέον διαθέσιμη μια νέα έκδοση με υποστήριξη για IPv6 στη σελίδα https://github.com/andihofmeister/squidGuard. Η συγκεκριμένη

έκδοση έτυχε ευρείας αποδοχής από τα μέλη της κοινότητας του λογισμικού SquidGuard και κρίνεται κατάλληλη για δοκιμή και χρήση στο ΠΣΔ.

Για την αναβάθμιση του λογισμικού SquidGuard στους εξυπηρετητές της υπηρεσίας ελέγχου περιεχομένου προτείνεται να ακολουθηθεί παρόμοια διαδικασία με αυτήν που περιγράφτηκε στα κεφάλαια για τις αναβαθμίσεις του λειτουργικού συστήματος και του λογισμικού Squid. Στόχος θα είναι πάντα να μην υπάρξει διακοπή της λειτουργίας της υπηρεσίας.

Η αναβάθμιση μπορεί να χωριστεί σε δύο μέρη:

1. Αναβάθμιση του λογισμικού στην νεότερη έκδοση και δοκιμή της καλής λειτουργίας του στις τρέχουσες συνθήκες λειτουργίας της υπηρεσίας.
2. Ενεργοποίηση της υποστήριξης του πρωτοκόλλου IPv6 και δοκιμής του αφού πρώτα ενεργοποιηθεί στα υπόλοιπα υποσυστήματα (κυρίως στο λειτουργικό σύστημα και στο λογισμικό Squid).

Η συγκεκριμένη ενέργεια δεν έχει προαπαιτούμενα από άλλες ενέργειες για τη φάση της αναβάθμισης του λογισμικού. Ως προαπαιτούμενο για την πλήρη ολοκλήρωσή της μπορεί να θεωρηθεί η ενεργοποίηση του πρωτοκόλλου IPv6 στους εξυπηρετητές και στο λογισμικό Squid.

7.4 ΥΠΟΣΤΗΡΙΞΗ ΤΟΥ ΠΡΩΤΟΚΟΛΛΟΥ IPv6

Για την υποστήριξη του πρωτοκόλλου IPv6 στην υπηρεσία ελέγχου περιεχομένου απαιτούνται οι ακόλουθες ενέργειες:

7.4.1 Ενεργοποίηση πρωτοκόλλου IPv6 στο λειτουργικό σύστημα εξυπηρετητών

Προαπαιτούμενα για τη συγκεκριμένη ενέργεια είναι η απόδοση ενός χώρου διευθύνσεων IPv6 στο υποδίκτυο των εξυπηρετών της υπηρεσίας και η ενεργοποίησή του στο δρομολογητή του ΠΣΔ που το δρομολογεί. Στη συνέχεια η ενεργοποίηση του πρωτοκόλλου

IPv6 στο λειτουργικό σύστημα των εξυπηρετητών μπορεί να γίνει οποιαδήποτε στιγμή χωρίς διακοπή της λειτουργίας υπηρεσίας και ασχέτως της προόδου των υπολοίπων ενεργειών.

Σε κάθε εξυπηρετητή θα ανατεθεί μια στατική διεύθυνση IPv6 η οποία για λόγους εύκολης συσχέτισης με τη διεύθυνση IPv4 που χρησιμοποιεί ήδη προτείνεται να χρησιμοποιεί το τελευταίο byte της διεύθυνσης IPv4. Έτσι, για παράδειγμα, αν το υποδίκτυο IPv6 που θα ανατεθεί είναι το 2001:648:2302:FC02::/64, τότε η διεύθυνση IPv6 του cache01.att.sch.gr (με διεύθυνση IPv4 194.63.239.231) θα είναι η 2001:648:2302:FC02::231.

7.4.2 Ενεργοποίηση του πρωτοκόλλου IPv6 στο λογισμικό Squid

Προαπαιτούμενα για τη συγκεκριμένη ενέργεια είναι:

1. Η ενεργοποίηση του πρωτοκόλλου IPv6 στο λειτουργικό σύστημα των εξυπηρετητών της υπηρεσίας.
2. Η αναβάθμιση του λογισμικού Squid στην έκδοση 3.1 που υποστηρίζει το πρωτόκολλο IPv6.
3. Η αναβάθμιση του λογισμικού SquidGuard στην πλέον πρόσφατη έκδοση που υποστηρίζει το πρωτόκολλο IPv6 και η ενεργοποίησή του.

Η καθαυτή ενεργοποίηση του πρωτοκόλλου IPv6 στο λογισμικό Squid είναι απλή υπόθεση και μπορεί να γίνει οποιαδήποτε στιγμή χωρίς διακοπή της λειτουργίας υπηρεσίας.

7.4.3 Ενεργοποίηση του πρωτοκόλλου IPv6 στο λογισμικό SquidGuard.

Η ενεργοποίηση του πρωτοκόλλου IPv6 στο λογισμικό SquidGuard είναι απλή υπόθεση και μπορεί να γίνει οποιαδήποτε στιγμή χωρίς διακοπή της λειτουργίας υπηρεσίας.

Μοναδική προαπαίτηση είναι η εγκατάσταση της πλέον πρόσφατης έκδοσης που υποστηρίζει το πρωτόκολλο IPv6, όπως αναφέρθηκε σε προηγούμενο κεφάλαιο.

7.4.4 Ενεργοποίηση του πρωτοκόλλου IPv6 στο μηχανισμό αναδρομολόγησης IP policy

Προϋπόθεση για την ενεργοποίηση του πρωτοκόλλου IPv6 στο μηχανισμό αναδρομολόγησης IP policy είναι η συνεννόηση με τη διαχειριστική ομάδα δικτύου κορμού του ΠΣΔ αρμοδιότητα της οποίας είναι η λειτουργία του συνοριακού δρομολογητή. Οι συνεργάτες της ομάδας δικτύου κορμού θα εξετάσουν τις αλλαγές στις ρυθμίσεις του δρομολογητή που θα προταθούν από την ομάδα της υπηρεσίας ελέγχου περιεχομένου, θα προτείνουν τυχόν διορθώσεις/βελτιώσεις και κρίνουν αν χρειάζεται κάποια διαφορετική ή νεότερη έκδοση του λειτουργικού συστήματος του δρομολογητή (IOS firmware) για την καλύτερη λειτουργία των προτεινόμενων χαρακτηριστικών. Καθώς το ΠΣΔ δεν διαθέτει εφεδρικό συνοριακό δρομολογητή για δοκιμές, οι αλλαγές θα πρέπει να γίνουν σε προγραμματισμένο παράθυρο συντήρησης και κατά προτίμηση σε μέρα και ώρα που η κίνηση του δικτύου είναι χαμηλή ώστε να μειωθεί στο ελάχιστο η ενόχληση των χρηστών σε περίπτωση που εμφανιστεί κάποια δυσλειτουργία.

Η αρχική ενεργοποίηση μπορεί να συνοδεύεται από μία έκδοση της access list PROXY-BYPASS που θα εξαιρεί όλη την κίνηση IPv6 ώστε να μην υπάρξει πρόβλημα προσβασιμότητας σε ιστότοπους με διευθύνσεις IPv6 σε περίπτωση που η ενεργοποίηση του πρωτοκόλλου IPv6 δεν έχει ολοκληρωθεί στα υπόλοιπα υποσυστήματα (π.χ. εξυπηρετητές, Squid κλπ.). Στη συνέχεια μπορούν να αναδρομολογηθούν δοκιμαστικά συγκεκριμένοι ιστότοποι, ασχέτως περιερχομένου, που διαθέτουν περιεχόμενο μέσω IPv6, π.χ. www.ntua.gr, ώστε να δοκιμαστεί η ορθή λειτουργία του μηχανισμού.

7.4.5 Αναβάθμιση της εφαρμογής διαχείρισης βάσης του SquidGuard για υποστήριξη του πρωτοκόλλου IPv6

Προαπαιτούμενο για την αναβάθμιση της εφαρμογής διαχείρισης είναι η εγκατάσταση της νεότερης έκδοσης του λογισμικού SquidGuard που υποστηρίζει το πρωτόκολλο IPv6 ώστε να δέχεται και να μπορεί να χειριστεί νέες εγγραφές με διευθύνσεις IPv6.

Οι περιπτώσεις για νέες εγγραφές με διευθύνσεις IPv6 αναμένεται, τουλάχιστον τον πρώτο καιρό, να είναι πολύ λίγες και θα μπορούσαν να προστίθενται στη βάση δεδομένων του

λογισμικού SquidGuard με χειροκίνητο τρόπο. Με τον τρόπο αυτό, είναι δυνατή η ενεργοποίηση του πρωτοκόλλου IPv6 στην υπηρεσία πριν την ολοκλήρωση της αναβάθμισης της εφαρμογής διαχείρισης.

7.5 Υλοποιηση μηχανισμου αναδρομολογησης με χρηση πρωτοκολλου WCCP

Προαπαιτούμενα για την υλοποίηση του μηχανισμού αναδρομολόγησης με τη χρήση του πρωτοκόλλου WCCP είναι:

1. Η εγκατάσταση του λειτουργικού συστήματος FreeBSD 9.1 στους εξυπηρετητές της υπηρεσίας.
2. Η αναβάθμιση του λογισμικού Squid στην έκδοση 3.1, ώστε να υπάρχει όσο το δυνατόν καλύτερη υποστήριξη των πρωτοκόλλων WCCP v1 και v2.
3. Η αποκλειστική χρήση των δύο τουλάχιστον εφεδρικών συστημάτων cache09 και cache10 για όσο καιρό χρειαστεί να γίνουν δοκιμές και πειραματισμοί.
4. Η στενή συνεργασία με τη διαχειριστική ομάδα δικτύου κορμού του ΠΣΔ αρμοδιότητα της οποίας είναι η λειτουργία του συνοριακού δρομολογητή και στον οποίο θα χρειαστεί να γίνουν αλλαγές στις ρυθμίσεις, πιθανώς περισσότερο εκτεταμένες από αυτές που θα απαιτηθούν για την υποστήριξη του πρωτοκόλλου IPv6 στο μηχανισμό IP policy.

Καθώς η ενεργοποίηση του πρωτοκόλλου WCCP απαιτεί αλλαγές στις ρυθμίσεις τριών τουλάχιστον υποσυστημάτων (του συνοριακού δρομολογητή, του λειτουργικού των εξυπηρετητών της υπηρεσίας και του λογισμικού Squid), προτείνεται να γίνει σε περίοδο που δεν θα εκτελούνται άλλες εργασίες στα συγκεκριμένα υποσυστήματα. Θα μπορούσε σε πρώτη να γίνουν όλες οι ενέργειες που απαιτούνται για την ενεργοποίηση του πρωτοκόλλου IPv6 και μετά την ολοκλήρωσή τους να ξεκινήσει η υλοποίηση του μηχανισμού αναδρομολόγησης με τη χρήση του πρωτοκόλλου WCCP.

Η δοκιμαστική λειτουργία του πρωτοκόλλου WCCP προτείνεται να γίνει αρχικά με τη συμμετοχή μόνο των δύο εφεδρικών συστημάτων και την ενεργοποίησή του στο συνοριακό

δρομολογητή για σύντομο χρονικό διάστημα σε περίοδο χαμηλής χρήσης του ΠΣΔ, όπως απογευματινές ώρες, με παράλληλη απενεργοποίηση του μηχανισμού IP policy.

Αναλόγως με τα αποτελέσματα, στη συνέχεια, μπορούν να γίνουν δοκιμές με περισσότερους εξυπηρετητές και σε ώρες υψηλότερης χρήσης του δικτύου. Τελικός σκοπός θα είναι να περάσουν όλοι οι εξυπηρετητές στον μηχανισμό του πρωτοκόλλου WCCP. Σε κάθε περίπτωση και στα τρία υποσυστήματα θα παραμείνουν απενεργοποιημένες οι ρυθμίσεις για τον μηχανισμό IP policy, αλλά διαθέσιμες για να αντικαταστήσουν τις ρυθμίσεις του μηχανισμού WCCP όποτε χρειαστεί. Επίσης, ο μηχανισμός WCCP μπορεί αρχικά να ενεργοποιηθεί μόνο για το πρωτόκολλο IPv4, ενώ το πρωτόκολλο IPv6 μπορεί να συνεχίσει να εξυπηρετείται από το μηχανισμό IP policy. Με τη διαδικασία αυτή αναμένεται να υπάρξουν μόνο πολύ σύντομες διακοπές της λειτουργίας της υπηρεσίας και όχι σε ώρες αιχμής.

7.6 Υλοποιηση του υπηρεσιας ελεγχου περιεχομενου σε τριτους μεσω DNS

Η συγκεκριμένη νέα υπηρεσία είναι ανεξάρτητη από την κύρια υπηρεσία ελέγχου του ΠΣΔ και ως τέτοια δεν έχει προαπαιτούμενα από άλλες ενέργειες ή υποσυστήματα που θα αναπτυχθούν ή θα αναβαθμιστούν. Συνεπώς, μπορεί να υλοποιηθεί με ανεξάρτητο χρονοδιάγραμμα και να ξεκινήσει το συντομότερο δυνατόν.

Για την ανάπτυξή της θα χρειαστεί έναν εξυπηρετητή, ο οποίος θα φιλοξενήσει τα πακέτα λογισμικού που θα επιλεχθούν (ISC BIND ή PowerDNS Recursive Server). Ο συγκεκριμένος εξυπηρετητής δεν χρειάζεται να είναι νέο ξεχωριστό φυσικό μηχάνημα. Μπορεί να είναι ένα εικονικό σύστημα, χρησιμοποιώντας την τεχνολογία FreeBSD Jails, σε ένα από τα δύο συστήματα δοκιμών cache09 και cache10.