Πανεπιστήμιο Πειραιώς – Τμήμα Πληροφορικής

Πρόγραμμα Μεταπτυχιακών Σπουδών

<<Πληροφορική>>

Μεταπτυχιακή Διατριβή

Τίτλος Διατριβής	**Ασφάλεια Δικτύων: Μελέτη και προσομοίωση πολιτικών και αρχιτεκτονικών ασφαλείας** **Network security: Study and simulation of security policies and architectures**
Ονοματεπώνυμο Σπουδαστή	**Χρήστος Ντίκος**
Πατρώνυμο	**Θωμάς**
Αριθμός Μητρώου	**ΜΠΠΛ 12044**
Επιβλέπων	**Παναγιώτης Κοτζανικολάου, Λέκτορας**

Ημερομηνία Παράδοσης 10/09/2014

Τριμελής Εξεταστική Επιτροπή

Παναγιώτης Κοτζανικολάου	**Χρήστος Δουληγέρης**	**Μιχαήλ Ψαράκης**
Λέκτορας	**Καθηγητής**	**Επίκουρος Καθηγητής**

Ευχαριστώ Θερμά τον Δρ. Κ. Παναγιώτη Κοτζανικολάου
για την σημαντική βοήθεια και την καθοδήγηση του
καθ΄όλη την διάρκεια της συγγραφής της παρούσας
Μεταπτυχιακής διατριβής και την Οικογένεια μου
για την πολύτιμη συμπαράσταση της.

Πίνακας Περιεχομένων

Λίστα εικόνων

Λίστα πινάκων

Περίληψη

Η παρούσα μεταπτυχιακή διατριβή έχει ως στόχο να αναλύσει την έννοια της ασφάλειας σε επίπεδο δικτύου, να μας επισημάνει διάφορες μεθόδους προστασίας Δικτύων που υπάρχουν σήμερα και να μας παρουσιάσει μέσα από λογισμικό προσομοίωσης Δικτύου, διάφορα σενάρια προστασίας Δικτύων στηριζόμενα σε πολιτικές ασφάλειας και ρυθμίσεις των δομικών στοιχείων του Δικτύου (Router's, switches, Firewall's), με σκοπό την αποτροπή των διάφορων μορφών επιθέσεων. Τέλος συνοψίζουμε τα συμπεράσματα μας, σχολιάζοντας τα διάφορα αυτά σενάρια και προτείνοντας Βέλτιστες πρακτικές αυτών των σεναρίων.

Λέξεις κλειδιά: ασφάλεια δικτύου, προστασία δικτύου, μέθοδοι επιθέσεων, πολιτικές ασφαλείας.

Abstract

This Thesis, analyze the concept of security at the Network level and to provide us, various methods of protecting Networks that exist today through simulation open source software, various scenarios of Protection Network's, supported with security policies and settings of Network components (Routers, switches, Firewall's), in order to prevent various types of attacks. Finally we summarize our conclusions, commenting on these different scenarios and suggested best practices.

Keywords: network security, network protection, attack methods, security policies.

Εισαγωγή

Το 1^0 Κεφάλαιο αποτελεί ένα εισαγωγικό κεφάλαιο στα Δίκτυα Υπολογιστών, επισυνάπτοντας τις βασικές τοπολογίες ενός τοπικού Δικτύου και αναλύοντας μεγαλύτερου είδους δίκτυα, όπως τα Μητροπολιτικά Δίκτυα (MAN) και τα Δίκτυα ευρείας λήψης (WAN). Στην συνέχεια γίνετε αναφορά στο βασικό μοντέλο Δικτύου, το πρότυπο O.S.I. , αναλύοντας τα επίπεδα του. Τέλος, γίνετε μία αναφορά στα δομικά στοιχεία από τα οποία αποτελείται ένα Δίκτυο, περιγράφοντας τα βασικά χαρακτηριστικά τους.

Στο 2^0 Κεφάλαιο περιγράφουμε την διεύθυνση της μορφής IPv4, με αναφορά στις κλάσεις της συγκεκριμένης διεύθυνσης και στον τρόπο υπολογισμού της διευθυνσιοδότησης της. Στην συνέχεια γίνετε αναφορά στα είδη των Firewall's που υπάρχουν σήμερα, περιγράφοντας μερικά είδη επιθέσεων. Αναφερόμαστε στην αρχιτεκτονική DMZ και σε συνδέσεις απομακρυσμένης πρόσβασης χρηστών (VPN) αναπτύσσοντας τα πρωτόκολλα VPN. Τέλος, παρουσιάζουμε την τεχνική NAT και γίνετε μία σύντομη επισκόπηση της Διεύθυνσης IPv6, μελετώντας την δομή και τα βασικά χαρακτηριστικά της.

Το 3^0 Κεφάλαιο μας εισάγει στις πολιτικές Ασφάλειας των Δικτύων, που υπάρχουν σήμερα, τον τρόπο καθορισμού τους, τους τρόπους με τους οποίους αναπτύσσεται μία ασφάλεια, και σε πολιτικές ασφάλειας που εφαρμόζονται σε συσκευές δικτύωσης όπως είναι τα Router's, switche's και firewall's.

Στο 4^0 Κεφάλαιο, πραγματοποιείται μία μικρή αναφορά στο περιβάλλον ανοιχτού λογισμικού κώδικα προσομοίωσης δικτύων που είναι το GNS3, παρουσιάζοντας τον τρόπο εγκατάστασης του και αναφέροντας ορισμένα παραδείγματα που έχουν σχέση με τις δυνατότητες πρόσβασης των χρηστών μέσα από λίστες πρόσβασης (ACL), σε ένα εσωτερικό δίκτυο και τον τρόπο με τον οποίο πραγματοποιείται μία VPN σύνδεση με την χρήση IPsec.

Τέλος, πραγματοποιούνται 2 εργαστηριακές μετρήσεις, με την χρήση υπηρεσίων FTP,TELNET,RADIUS,HTTP,MAIL σε δίκτυο με ένα Firewall προστασίας και σε δίκτυο με δύο Firewall προστασίας, παρατηρώντας τον τρόπο με τον οποίο εφαρμόζουν στο δίκτυο και συγκρίνοντας τα μεταξύ τους.

ΚΕΦΑΛΑΙΟ 1 – ΕΙΣΑΓΩΓΗ ΣΤΑ ΔΙΚΤΥΑ Η/Υ - ΤΟΠΟΛΟΓΙΕΣ ΔΙΚΤΥΩΝ

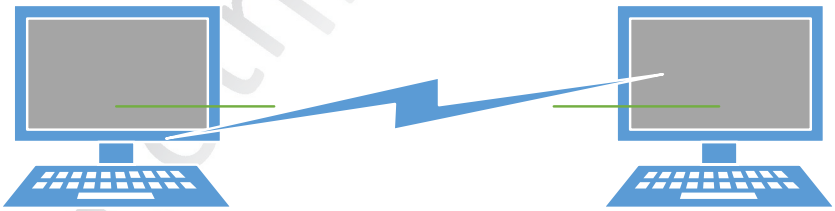
1.1 Εισαγωγή

Σε αυτό το κεφάλαιο θα μιλήσουμε για τις τοπολογίες των δικτύων, οι περισσότεροι των οποίων χαρακτηρίζονται ως Τοπικά Local Area Networks (LAN). Συνήθως σχεδιάζονται μικρά δίκτυα για να μπορούν πολλοί υπολογιστές να μοιράζονται πόρους (π.χ. εκτυπωτές).

Επίσης θα περιγράψουμε τις έννοιες στις οποίες βασίζονται οι τεχνολογίες των τοπικών δικτύων σήμερα, παρουσιάζοντας τις βασικές τοπολογίες των δικτύων.

1.2 Άμεση επικοινωνία σημείου προς σημείο

Στην επικοινωνία σημείου προς σημείου (Point To Point), κάθε κανάλι επικοινωνίας συνδεόταν σε ακριβώς δύο υπολογιστές, και μόνο. Η μέθοδος αυτή, που λέγεται *δίκτυο σημείου προς σημείο* (Point To Point Network) ή *δίκτυο πλέγματος* (Mesh Network), έχει τρεις χρήσιμες ιδιότητες.



Εικόνα 1.1 Σημείο προς Σημείο

Πρώτον, επειδή η κάθε σύνδεση εγκαθίσταται ανεξάρτητα, μπορεί να χρησιμοποιηθεί κατάλληλο υλικό.

Δεύτερον, επειδή οι συνδεδεμένοι υπολογιστές έχουν αποκλειστική πρόσβαση, μπορούν να αποφασίζουν πώς ακριβώς θα στέλνουν τα δεδομένα μέσω της σύνδεσης.

Τρίτον, επειδή μόνο δύο υπολογιστές έχουν πρόσβαση στο κανάλι, είναι εύκολο να εξασφαλιστεί η ασφάλεια και το προσωπικό απόρρητο. Κανένας άλλος υπολογιστής δε χειρίζεται τα δεδομένα, και κανένας άλλος υπολογιστής δεν μπορεί να αποκτήσει πρόσβαση.

Η σύνδεση σημείου προς σημείο εκτός από πλεονεκτήματα προσφέρει και μειονεκτήματα.

Πρώτον, Δεν μπορούν να επικοινωνούν παραπάνω από 2 υπολογιστές μεταξύ τους.

Δεύτερον, ο αριθμός των συνδέσεων αυξάνετε ανάλογα με τον αριθμό των ζευγών των υπολογιστών. Για παράδειγμα για 2 υπολογιστές χρειαζόμαστε 1 σύνδεση, για 4 υπολογιστές χρειαζόμαστε 2 συνδέσεις κοκ.

Τρίτον, όσο αυξάνετε ο αριθμός των υπολογιστών, αυξάνετε και ο αριθμός των συνδέσεων άρα αυξάνετε και το κόστος αυτών.

1.3 Η ανακάλυψη του τοπικού Δικτύου

Για να αντιμετωπιστεί αυτό το φαινόμενο που παρουσιάστηκε με την τοπολογία σημείο προς σημείο, επινοήθηκε μία άλλη μέθοδος γνωστή και ως τοπικά δίκτυα (Local Area Networks).

Ουσιαστικά κάθε τοπικό Δίκτυο αποτελείτε από ένα μέσο μετάδοσης το οποίο χρησιμοποιείτε από όλα τα τερματικά (Υπολογιστές , κινητά, εκτυπωτές κ.α.) για να συνδεθούν σε αυτό. Η πιο συνηθισμένη τεχνική χρησιμοποίησης του μέσου μετάδοσης είναι η χρησιμοποίηση του μέσου από τα τερματικά ο ένας μετά τον άλλον. Ένας ακόμα λόγος που χρησιμοποιούμε ένα κοινό μέσο μετάδοσης είναι λόγο της χαμηλής οικονομικής επιβάρυνσης που έχουμε στο σύστημα με την χρησιμοποίηση ενός κοινού μέσου.

Ο πιο σημαντικός λόγος όμως που χρησιμοποιούμε το Τοπικό δίκτυο σήμερα και έχει μεγάλη ζήτηση είναι γιατί στηρίζετε στην θεμελιώδη αρχή δικτύωσης των υπολογιστών γνωστή και ως **τοπικότητα των αναφορών.**

Η τοπικότητα των αναφορών μας αναφέρει το εξής:

Ότι ένας υπολογιστής είναι πιο πιθανό να μιλάει με άλλους υπολογιστές πιο βρίσκονται πιο κοντά με αυτόν από φυσικής απόψεως σε σχέση με άλλους υπολογιστές που βρίσκονται πιο μακριά από αυτούς.

Επίσης αυτός ο υπολογιστής τυγχάνει να μιλάει με υπολογιστές που έχει μιλήσει κατά το παρελθόν συχνότερα από υπολογιστές που επικοινωνεί για πρώτη φορά.

Η αρχή της τοπικότητας των αναφορών μπορεί να γίνει εύκολα κατανοητή, επειδή ισχύει και για την ανθρώπινη επικοινωνία. Για παράδειγμα, οι άνθρωποι επικοινωνούν πιο συχνά με άλλους που βρίσκονται κοντά από φυσική άποψη (π.χ. εργάζονται μαζί). Ακόμα, αν ένα άτομο επικοινωνήσει με κάποιον, (π.χ. με ένα φίλο ή με ένα μέλος της οικογένειάς του), είναι πιθανό να επικοινωνήσει ξανά με το ίδιο πρόσωπο

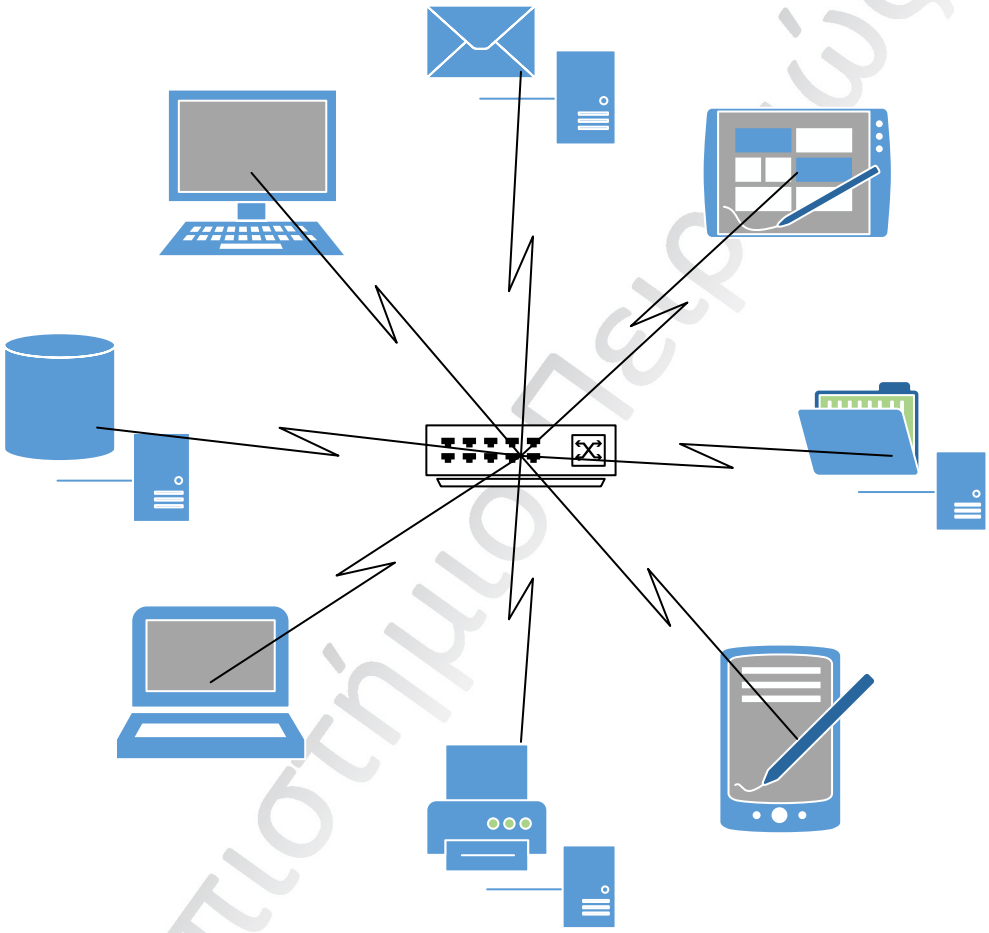
1.3.1 Τοπολογίες Τοπικού Δικτύου

Σε αυτή την ενότητα θα μιλήσουμε για 3 πιο σημαντικές τοπολογίες που χρησιμοποιούνται πιο συχνά στα Τοπικά Δίκτυα και είναι οι εξής :

- Τοπολογία Αστέρα
- Τοπολογία Δακτυλίου
- Τοπολογία Διαύλου

1.3.1.1 Τοπολογία αστέρα

Στην τοπολογία αστέρα όλοι οι υπολογιστές συνδέονται σε ένα κεντρικό σημείο (Κόμβος), όπου από εκεί μπορούν να επικοινωνούν με τους άλλους υπολογιστές όπως και οι άλλοι υπολογιστές να επικοινωνούν με αυτούς.



Εικόνα1.2. Τοπολογία αστέρα

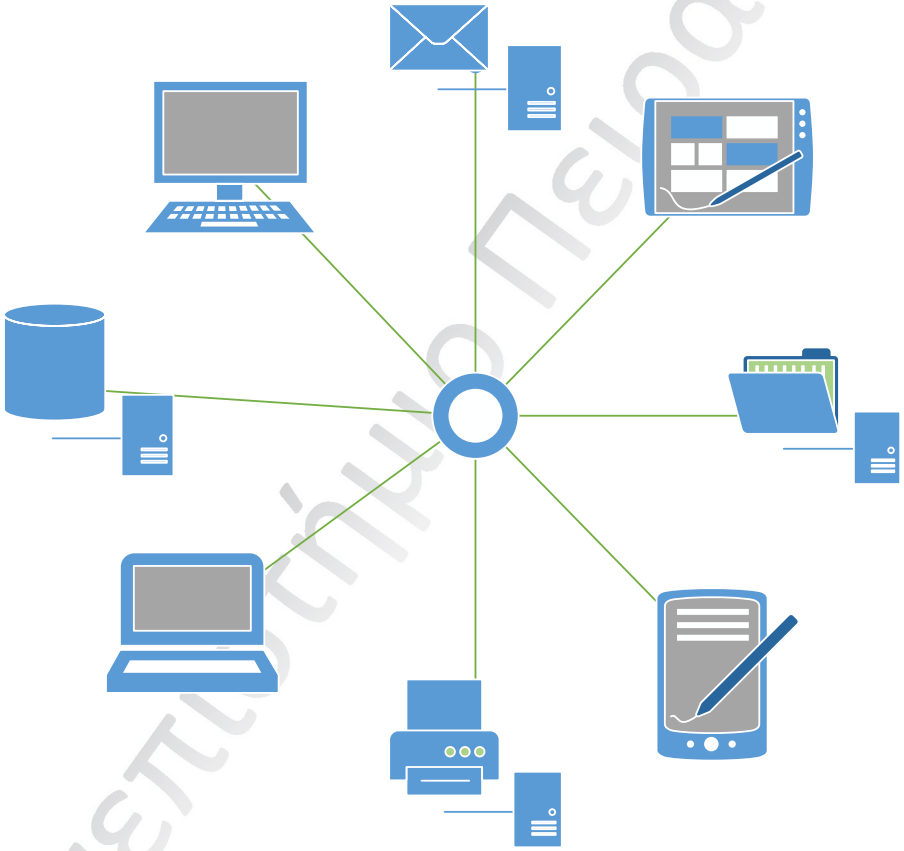
Το κέντρο του δικτύου αυτού συνήθως αποκαλείτε ομφαλός (Hub). Η λειτουργία του ομφαλού είναι κυρίως να δέχεται δεδομένα από τον υπολογιστή αποστολέα και να τα παραδίδει στον κατάλληλο προορισμό.

Στην πράξη τα συγκεκριμένα δίκτυα έχουν συμμετρική απόσταση από τον κόμβο μόνο που ο κόμβος δεν βρίσκετε απαραίτητα στο κέντρο του δικτύου αλλά συνήθως σε κάποιες γωνίες αυτού.

1.3.1.2 Τοπολογία Δακτυλίου

Σε αυτό το δίκτυο όλοι οι υπολογιστές συνδέονται σε ένα κλειστό βρόγχο, εφαρμόζοντας την ακόλουθη συνδεσμολογία. Ο πρώτος υπολογιστής συνδέετε με τον δεύτερο , ο δεύτερος συνδέετε με τον τρίτο ... και ο τελευταίος υπολογιστής συνδέετε με τον πρώτο κλείνοντας τον κύκλο.

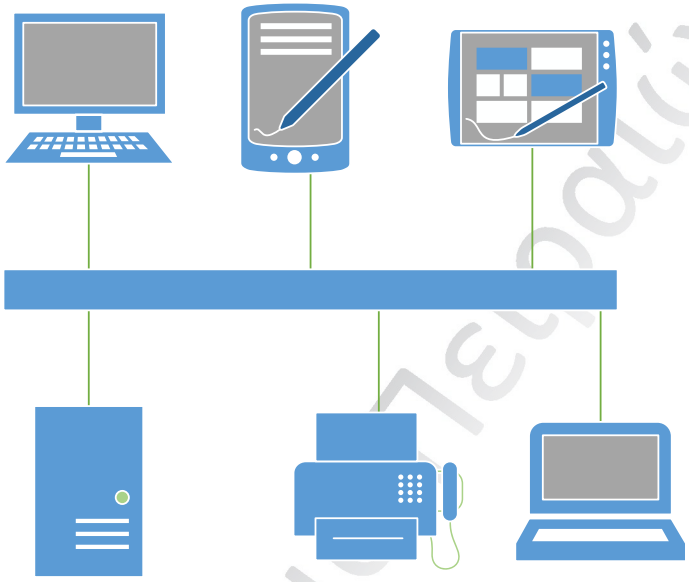
Ο όρος δακτύλιος αναφέρετε στις λογικές συνδέσεις μεταξύ των υπολογιστών και όχι στην φυσική διάταξη τους , δηλαδή δεν χρειάζονται οι υπολογιστές να βρίσκονται απαραίτητα σε κυκλική διάταξη.



Εικόνα 1.3. Τοπολογία δακτυλίου

1.3.1.3 Τοπολογία Διαύλου

Είναι ένα δίκτυο στο οποίο συνδέονται όλοι οι υπολογιστές από ένα κοινό μέσω το οποίο ονομάζουμε **σημείο πρόσβασης στο μέσο** ή αλλιώς **δίαυλος.** Η κύρια λειτουργία του δικτύου είναι οι εξής, όταν κάποιος υπολογιστής ο οποίος είναι συνδεδεμένος στον δίαυλο στείλει ένα σήμα μέσω αυτού του καλωδίου τότε όλοι οι άλλοι οι υπολογιστές που είναι συνδεδεμένοι στο καλώδιο αυτό θα λάβουν αυτό το σήμα.



Εικόνα 1.4. Τοπολογία διαύλου

Σύμφωνα με αυτή την λογική , όπου αναφέρθηκε παραπάνω , οποιοσδήποτε υπολογιστής που έχει πρόσβαση στο μέσο μπορεί να στείλει δεδομένα σε οποιονδήποτε άλλον υπολογιστή. Ο συντονισμός των υπολογιστών είναι ένας σημαντικός παράγοντας για την ομαλή λειτουργία του συγκεκριμένου δικτύου για να εξασφαλίζετε με αυτό τον τρόπο ότι ένας μόνο υπολογιστής θα μπορεί να στέλνει σήμα κάθε δεδομένη χρονική στιγμή αλλιώς θα παρουσιαζόταν το φαινόμενο των συγκρούσεων (collision) το οποίο θα προκαλούσε μεγάλο πρόβλημα στο δίκτυο.

Για την αποφυγή ταυτόχρονης χρήσης του μέσου μεταφοράς χρησιμοποιήθηκε ο εξής τρόπος:

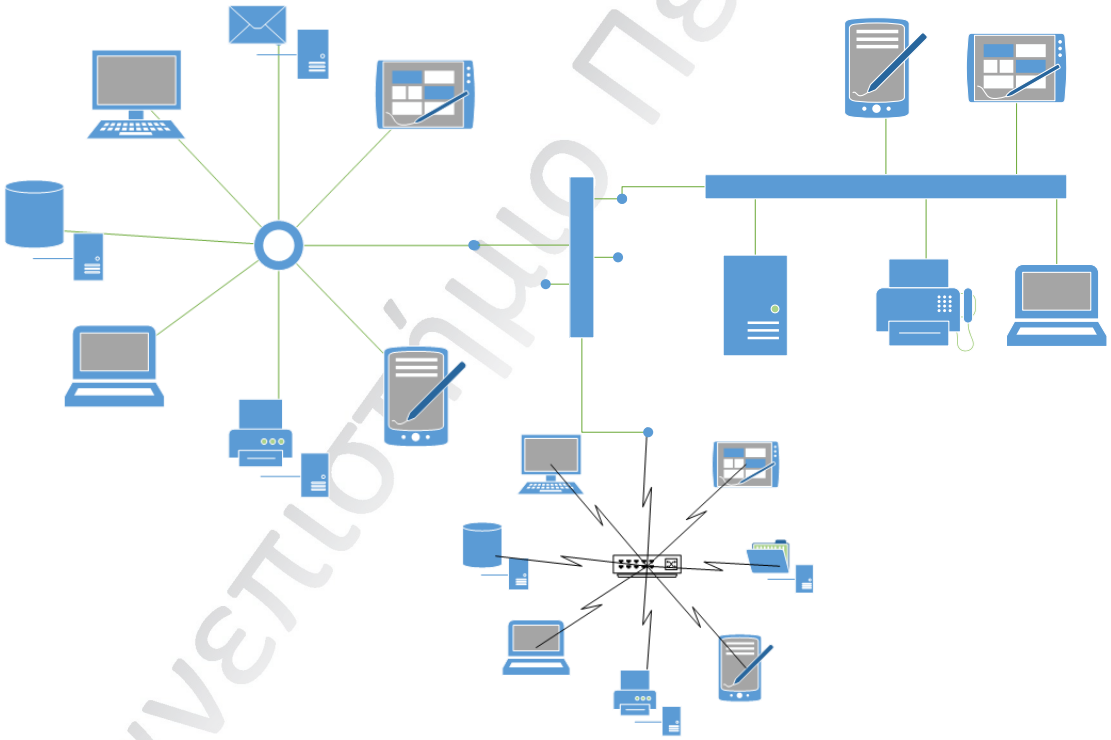
- **Μέθοδος Carrier-sense multiple access (CSMA/CD)**

Σύμφωνα με αυτό το πρωτόκολλο, όλοι οι κόμβοι έχουν ίδια προτεραιότητα και ο έλεγχος δεν είναι κεντρικός. Αυτό αποτελεί και το μεγαλύτερό του πλεονέκτημα, αφού με αυτόν τον τρόπο, όταν κάποιος κόμβος αποτύχει, το υπόλοιπο δίκτυο δεν επηρεάζεται. Ο αλγόριθμος λειτουργίας του πρωτοκόλλου είναι απλός και η περιγραφή του είναι η εξής:

Όταν ένας κόμβος έχει κάποιο πακέτο το οποίο θέλει να μεταδώσει, “ακούει” πρώτα προσεκτικά το μέσο μεταφοράς για να δει αν αυτό είναι άδειο, και μόνο σε αυτή την περίπτωση το αποστέλλει, γιατί διαφορετικά θα μπορούσε να δημιουργηθεί σύγκρουση με κάποιο πακέτο που θα προερχόταν από κάποιο άλλο υπολογιστή.

1.3.1.4 Σύνθετη Τοπολογία

Σύνθετη ή υβριδική τοπολογία, ονομάζουμε κάθε συνδυασμό των παραπάνω μεθόδων που αναφέραμε. Ένα παράδειγμα είναι μια τοπολογία δέντρου η οποία συνδυάζει τα χαρακτηριστικά των γραμμικών τοπολογιών bus και αστέρα. Αποτελείται από ομάδες διαμορφωμένων τερματικών σταθμών που συνδέονται με ένα γραμμικό βασικό καλώδιο bus. Αυτές οι τοπολογίες μπορούν επίσης να αναμιχθούν. Παραδείγματος χάριν, ένα δίκτυο bus - αστέρα αποτελείται από ένα bus υψηλής-εύρους ζώνης, αποκαλούμενο σπονδυλική στήλη, η οποία συνδέει τις συλλογές των τμημάτων αστεριών αργές-εύρους ζώνης.

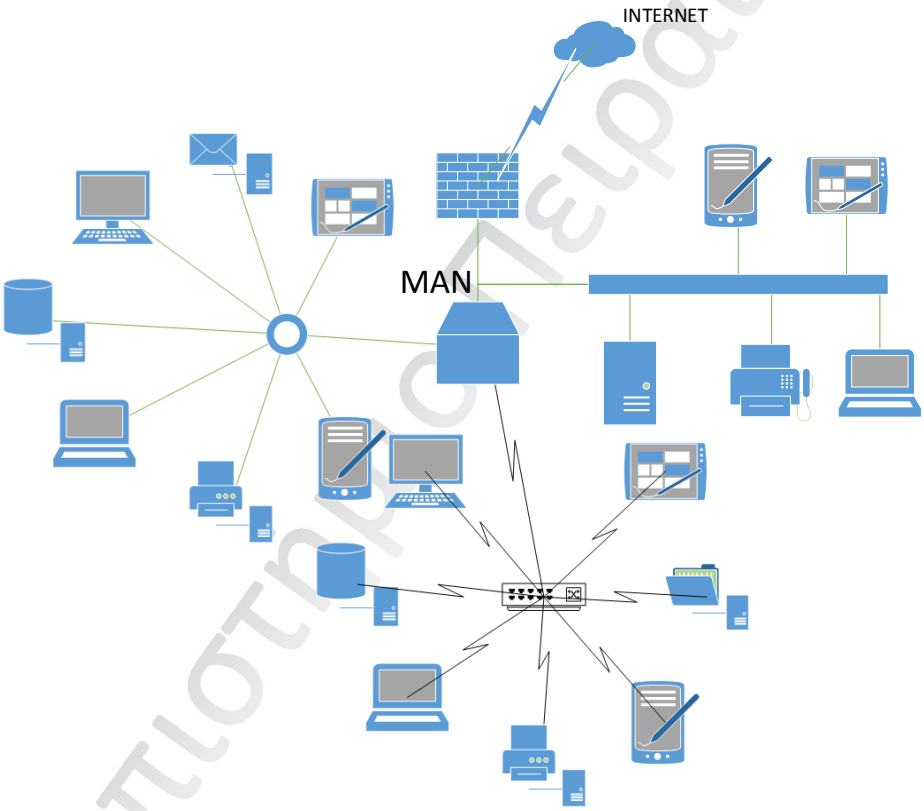


Εικόνα 1.5. Σύνθετη Τοπολογία

1.4 Μητροπολιτικά δίκτυα (MAN)

Το μητροπολιτικό δίκτυο (Metropolitan Area Network) είναι ένα δίκτυο το οποίο η εμβέλεια του είναι όσο μία πόλη ή μία πανεπιστημιακή κοινότητα (Campus). Η ακτίνα εμβέλειας του συγκεκριμένου δικτύου κυμαίνετε από 10 km και φτάνει τα 100 km περίπου. Σκοπός του μητροπολιτικού δικτύου είναι να παραλαμβάνει την κυκλοφορία από το τοπικό ή τοπικά δίκτυα του και να την μεταφέρει σε ένα δίκτυο ευρείας περιοχής ή σε άλλο τοπικό δίκτυο.

Οι τεχνολογίες που μπορεί να χρησιμοποιήσει ένα μητροπολιτικό δίκτυο είναι το SONET/SDH , το ATM και από τεχνολογίες μέσου είναι το Gigabit Ethernet , το Ethernet και το Fast Ethernet.



Εικόνα 1.6. Μητροπολιτικό δίκτυο (MAN)

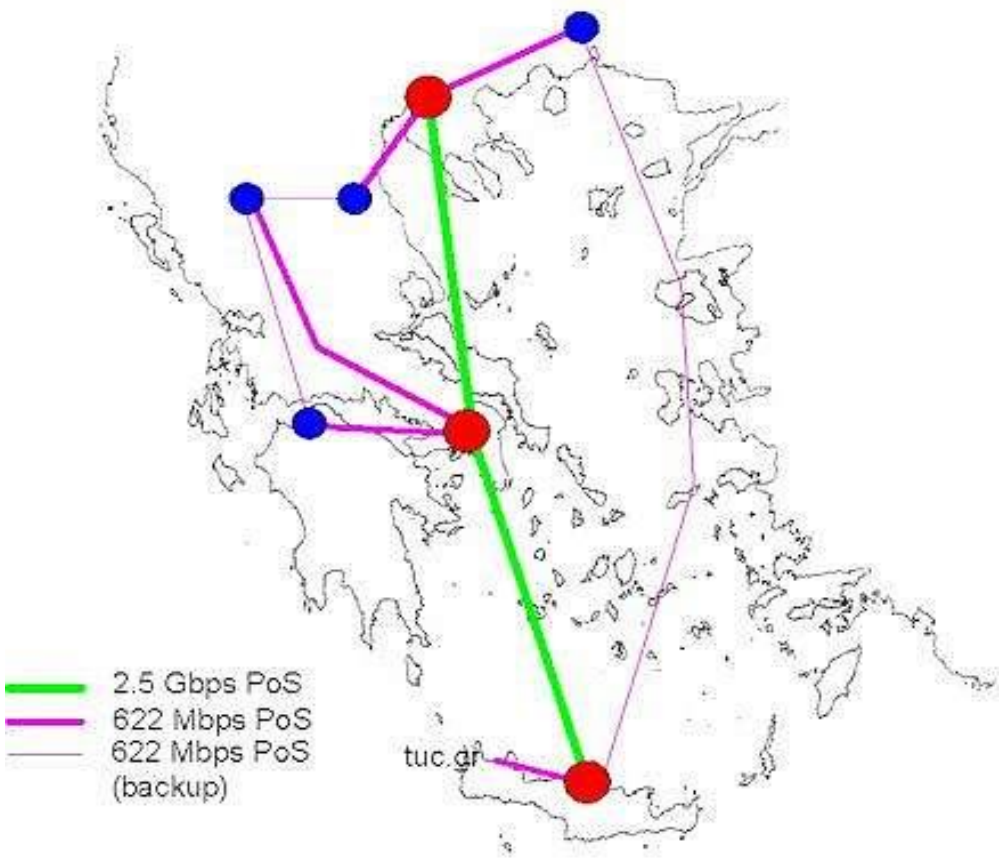
1.5 Δίκτυα ευρείας περιοχής (WAN)

Τα Δίκτυα ευρείας περιοχής (Wide Area Network), είναι ένα δίκτυο το οποίο η εμβέλεια του είναι μεγαλύτερη από μία χώρα ακόμα και από μία ολόκληρη ήπειρο. Σε αυτά τα Δίκτυα μπορούμε να έχουμε την συμμετοχή πολλών τοπικών δικτύων ή ακόμα και άλλων δικτύων ευρείας περιοχής.

Οι ταχύτητες των συγκεκριμένων δικτύων δεν είναι και πάρα πολύ μεγάλες και συνήθως είναι πιο μικρές από αυτές των LAN και MAN. Ο λόγος για τον οποίο υπάρχουν αυτές οι μεγάλες διαφορές είναι εξαιτίας των μεγάλων αποστάσεων που έχουν αυτά τα δίκτυα.

Τα μέσα μετάδοσης που μπορεί κάποιος να συναντήσει σε ένα δίκτυο WAN είναι πολλά και διάφορα (ασύρματα, οπτική ίνα, utp).

Παραδείγματα τέτοιων δικτύων είναι δορυφορικά δίκτυα καθώς και ασύρματα δίκτυα.



Εικόνα 1.7. Δίκτυο ευρείας Περιοχής (WAN)

1.6 Μοντέλα αναφοράς δικτύων

1.6.1 Το Πρότυπο OSI

Το μοντέλο αναφοράς O.S.I. (Open Systems Interconnection) αναπτύχτηκε από τον Διεθνή Οργανισμό Τυποποίησης (I.S.O.) και χρησιμοποιήθηκε κυρίως για την τυποποίηση των πρωτοκόλλων που υπάρχουν στα διάφορα επίπεδα των Δικτύων. Σκοπός του είναι να μπορεί να συνδέσει διαφόρων ειδών συστήματα με άλλα συστήματα επικοινωνίας.

Αποτελείτε από 7 επίπεδα λειτουργίας:

- Φυσικό επίπεδο
- Επίπεδο Ζεύξης δεδομένων
- Επίπεδο δικτύου
- Επίπεδο μεταφοράς
- Επίπεδο συνόδου
- Επίπεδο παρουσίασης
- Επίπεδο εφαρμογής

Φυσικό επίπεδο

Βρίσκεται στο πιο χαμηλό επίπεδο, ολόκληρου του δικτύου επικοινωνίας. Ασχολείται κυρίως με την μετάδοση Bits εντός του καναλιού μετάδοσης δεδομένων.
Χρησιμοποιεί διαφόρων ειδών συσκευές όπως είναι τα HUB , οι repeaters που χρησιμοποιούνται εντός του φυσικού μέσου για ενίσχυση του σήματος σε περίπτωση εξασθένισης του , οι κάρτες δικτύου που χρησιμοποιούνται για την αποστολή και λήψη των δεδομένων κ.α.
Πραγματοποιεί λειτουργίες όπως:

- Έναρξη και τερματισμός ηλεκτρικής σύνδεσης επικοινωνιακής συσκευής
- Συμμετοχή σε διαδικασία πολυπλεξίας
- Διαμόρφωση και αναδιαμόρφωση ψηφιακών δεδομένων κατά την μετάδοση αυτών από άκρο σε άκρο

Επίπεδο Ζεύξης δεδομένων

Βρίσκετε αμέσως μετά από το φυσικό επίπεδο. Παρέχει αξιόπιστη μεταφορά δεδομένων εντός του φυσικού μέσου. Η αξιόπιστη μεταφορά δεδομένων επιτυγχάνετε με το τεμαχισμό ολόκληρου του μηνύματος σε πλαίσια δεδομένων, εργασία όπου αναλαμβάνει να την εκτέλεση ο αποστολέας. Τα πλαίσια αυτά στην συνέχεια μεταφέρονται με ευθύνη του πλαισίου στην συσκευή προορισμού.

Μπορούμε να βρούμε διάφορα παραδείγματα πρωτοκόλλων που βρίσκονται σε αυτό το επίπεδο όπως Ethernet , Token Ring, ISDN, PPP, και Frame Relay.

Επίπεδο δικτύου

Το επίπεδο δικτύου παρέχει συνδεσιμότητα μεταξύ 2 τερματικών συσκευών οι οποίες μπορεί να βρίσκονται ακόμα και σε διαφορετικά δίκτυα. Επίσης είναι υπεύθυνο για την λειτουργία του υποδικτύου. Καθορίζει το δρομολόγιο των πακέτων από την πηγή έως και τον προορισμό του. Ελέγχει την συμφόρηση η οποία μπορεί να παρουσιαστεί εντός του δικτύου λόγω κυκλοφοριακής συμφόρησης πακέτων. Στο συγκεκριμένο δίκτυο ο κάθε χρήστης επιβαρύνετε με απόδοση λογικής διεύθυνσης (IP).
Χαρακτηριστικό παράδειγμα πρωτοκόλλου είναι το IP.

Επίπεδο μεταφοράς

Το επίπεδο μεταφοράς ουσιαστικά εξασφαλίζει την έγκυρη αποστολή των πακέτων από την μεριά του αποστολέα προς τον παραλήπτη. Το σύνηθες κατά την αποστολή των μηνυμάτων είναι ότι τα μηνύματα που στέλνονται , λαμβάνονται με την ίδια σειρά χωρίς ιδιαίτερες αλλαγές σε αυτά (σφάλματα). Όταν πρόκειται η αποστολή των μηνυμάτων να περιλαμβάνει διάφορους προορισμούς , τότε και η σειρά αυτών μπορεί να μην είναι η ίδια αλλά διαφορετική. Παρατηρούμε ότι από αυτό το επίπεδο η επικοινωνία είναι από άκρο σε άκρο και όχι μέσω αλυσιδωτών αντιδράσεων όπως γινόταν στα προηγούμενα 3 επίπεδα.

Επίπεδο συνόδου

Το επίπεδο συνόδου αποτελεί την έναρξη συνδιάλεξης (session) μεταξύ 2 υπολογιστών. Στο επίπεδο συνόδου είναι αυτό στο οποίο λειτουργεί **η ταυτοποίηση του χρήστη**. Για παράδειγμα εάν προσπαθούμε να κάνουμε login για να συνδεθούμε στο mail μας, αυτό αποτελεί μία συνδιάλεξη που πραγματοποιείται με τον server του συστήματος και ταυτόχρονα Ο mail server ταυτοποιεί εάν είμαστε η ίδιοι για να πραγματοποιήσουμε είσοδο στο mail μας και ταυτόχρονα να κάνει και έναρξη του session. Το επίπεδο συνόδου με την ίδια λογική που είναι υπεύθυνο για την έναρξη του session , είναι υπεύθυνο και για τον τερματισμό του.

Επίπεδο παρουσίασης

Το επίπεδο Παρουσίασης (Presentation Layer) αποτελεί το κλειδί για την ασφάλεια των δεδομένων που μεταφέρονται εντός του δικτύου. Είναι αυτό το οποίο αναλαμβάνει να κωδικοποιήσει τα δεδομένα κατά την αποστολή τους εντός του δικτύου. Με λίγα λόγια το επίπεδο αυτό φροντίζει για την καλύτερη αναπαράσταση των δεδομένων.

Επίπεδο εφαρμογής

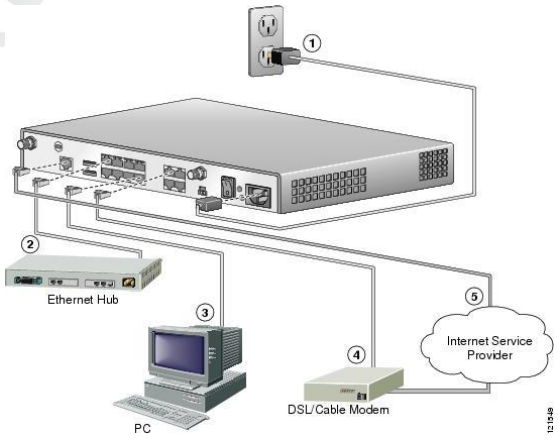
Το επίπεδο εφαρμογής δίνει την δυνατότητα στο χρήστη να πραγματοποιεί είσοδος εντός του δικτύου μέσω κάποιας εφαρμογής που χρησιμοποιεί, για παράδειγμα ο browser του (Mozilla , internet explorer κ.α.).
Τα πρωτόκολλα τα οποία χρησιμοποιεί είναι ποικίλα. Μεταξύ αυτών είναι το HTTP, FTP , TELNET, SMTP κ.α.

1.7 Δομικά στοιχεία Δικτύων

Σε αυτή την ενότητα θα αναφέρουμε στα κύρια μέλη του δικτύου, τα οποία είναι απαραίτητα για την λειτουργία του. Χάρις τα οποία μπορούμε να πραγματοποιούμε σύνδεση εντός αυτού, να αποστέλλουμε, αλλά και να δεχόμαστε πληροφορίες.

1.7.1 Δρομολογητές (Routers)

Οι δρομολογητές είναι υπεύθυνοι για την δρομολόγηση των δεδομένων από τον αποστολέα προς τον παραλήπτη εντός του Lan. Ένα χαρακτηριστικό τους είναι ότι δεν κρατούν κατάσταση για τις συνδέσεις τους, αλλά προωθούν τα πακέτα βάση της διεύθυνσης τερματικού προορισμού που διαθέτουν. Κατά την λήψη πακέτων, και γνωρίζοντας τον προορισμό τους, προωθούν τα πακέτα βάση του πίνακα προώθησης που διαθέτουν. Σε περίπτωση όπου τα πακέτα που λαμβάνονται έχουν γρηγορότερο ρυθμό από αυτά που προωθούνται , τότε εμφανίζετε το φαινόμενο της **Ουράς**. Στην ακριβώς αντίθετη περίπτωση όταν τα πακέτα που πρέπει να προωθηθούν έχουν μεγαλύτερο ρυθμό μετάδοσης από αυτά που προωθούνται τότε ο δρομολογητής μπορεί να τα αποθηκεύσει σε ενταμιευτές (buffers) που διαθέτει γνωρίζοντας με αυτό τον τρόπο την σειρά με την οποία τα **αναμονή πακέτα** πρέπει να μεταδοθούν.

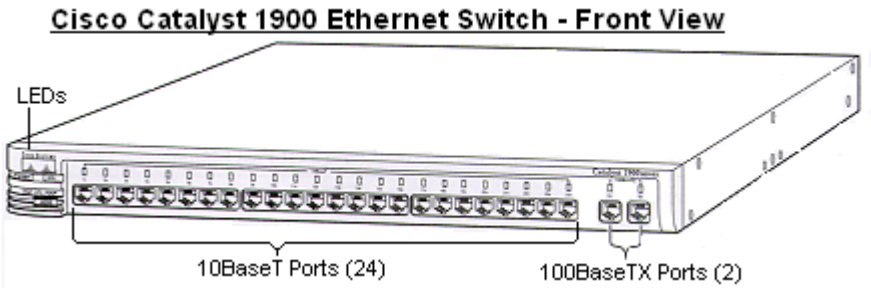


Εικόνα 1.8. Αναλυτική απεικόνιση ενός δρομολογητή

Επίσης παρέχουν συνδεσιμότητα σε WAN δίκτυα. Εντός του Lan δικτύου, οι routers παρέχουν υπηρεσίες όπως είναι τα ARP και μπορούν να χωρίσουν το ήδη υπάρχον δίκτυο σε υποδίκτυα χρησιμοποιώντας την τεχνική Sub netting.
Ανήκουν στο επίπεδο δικτύου του μοντέλου αναφοράς OSI. Κατά την λειτουργία τους για την επιτυχή επικοινωνία, με τους γειτονικούς δρομολογητές χρησιμοποιούν διάφορα πρωτόκολλα δρομολόγησης όπως είναι τα πρωτόκολλα R.I.P. , O.S.P.F. , B.G.P. .

1.7.2 Μεταγωγής (Switches)

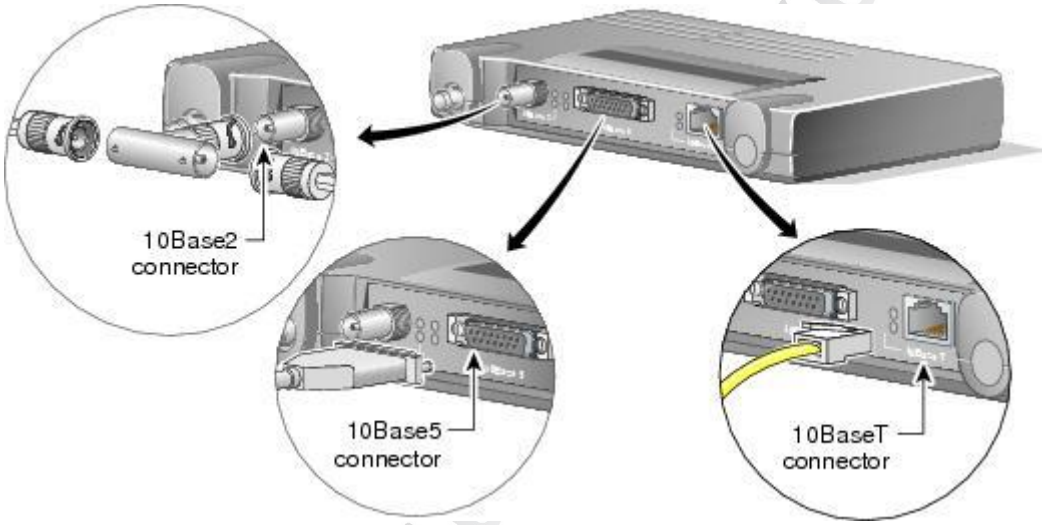
Το switch μπορεί να αναφέρετε και σαν μία συσκευή η οποία είναι μία γέφυρα πολλαπλών πορτών, ο οποίος αυτός ο αριθμός εξαρτάται ανάλογα με πόσα υποδίκτυα (Segments) το συγκεκριμένο δίκτυο έχει. Σε κάθε πόρτα που έχουν μαθαίνουν και αποθηκεύουν σε ένα πίνακα που διαθέτουν με ποιό τερματικό συνδέονται. Έτσι δημιουργούν πίνακες προώθησης των πακέτων αυτών για να καθορίσουν τον προορισμό τους. Σε σύγκριση με τις **Γέφυρες** η μεταγωγής διαθέτουν πολλές πόρτες, περιλαμβάνοντας διάφορα υποδίκτυα και παρέχοντας καλύτερες λύσεις συνδεσιμότητας , βελτιώνοντας την απόδοση του δικτύου (**σε σχέση με την ταχύτητα και το εύρος ζώνης**).



Εικόνα 1.9 Μεταγωγέας Cisco Catalyst 1900 Ethernet

1.7.3 Γέφυρες (Bridges)

Οι γέφυρες είναι συσκευές οι οποίες λειτουργούν με το ίδιο ακριβώς τρόπο με αυτό τον μεταγωγών. Κάνουν χρήση των διευθύνσεων (MAC) των σταθμών εργασίας του τοπικού δικτύου, για να μεταδώσουν τα πλαίσια δεδομένων (*data frames*) μεταξύ των δικτύων που συνδέουν. Η συγκεκριμένη τεχνολογία με το πέρασμα των χρόνων ενσωματώθηκε στους δρομολογητές που υπάρχουν σήμερα.



Εικόνα 1.10 Γέφυρα Cisco Aironet 340 Series Wireless Bridge

Στην παραπάνω εικόνα παρατηρούμε ότι η συγκεκριμένη συσκευή διαθέτει συνδέσεις 3 τύπων

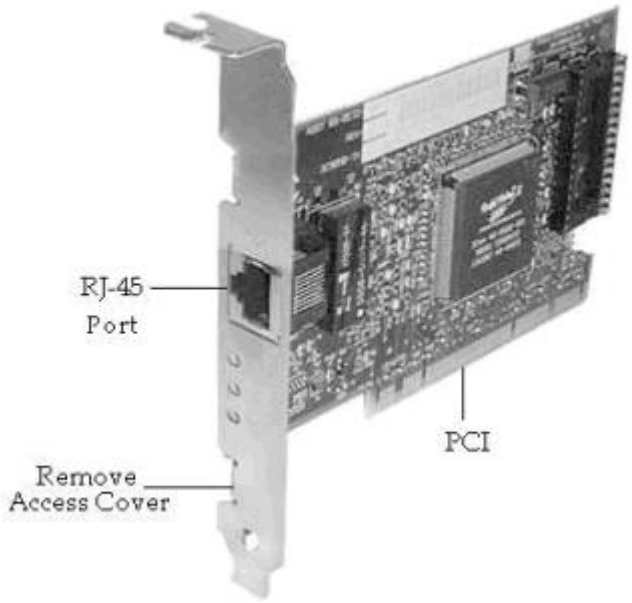
- 10Base2 (Thinnet) σε BNC T-σύνδεσμο
- 10Base5 (Thicknet) σύνδεσμο
- RJ-45 σύνδεσμο σε 10BaseT (Twisted Pair) θύρα

1.7.4 Επαναληπτές (Repeaters)

Είναι συσκευές οι οποίες ενισχύουν το ηλεκτρικό σήμα που μεταφέρετε εντός του δικτύου , ιδιαίτερα όταν οι αποστάσεις ξεπερνούν τα 100 μέτρα (υπολογισμός εξασθένισης του ηλεκτρικού σήματος σε καλώδια τύπου UTP CAT 5).
Στα περισσότερα δίκτυα που χρησιμοποιούν Ethernet καλώδια την θέση του repeater την αναλαμβάνει η συσκευή HUB ή το Switch.

1.7.5 Κάρτες Δικτύου (Network Cards)

Η κάρτα δικτύου είναι το κύκλωμα εκείνο το οποίο παρέχει σύνδεση στο τερματικό εντός του δικτύου. Μπορεί να υπάρχει ενσωματωμένο (τις περισσότερες φορές) εντός της μητρικής πλακέτας. Όταν μία κάρτα δικτύου εγκατασταθεί σε ένα υπολογιστή για την εκτέλεση των υπηρεσιών της, απαιτεί από τον σταθμό εργασίας της, να τις παρέχει ένα (κομμάτι) της CPU , όπως και διευθύνσεις εισόδου/εξόδου και επαρκής χώρο μνήμης για την εκτέλεση των λειτουργιών της.



Εικόνα 1.11 Κάρτα δικτύου τύπου PCI

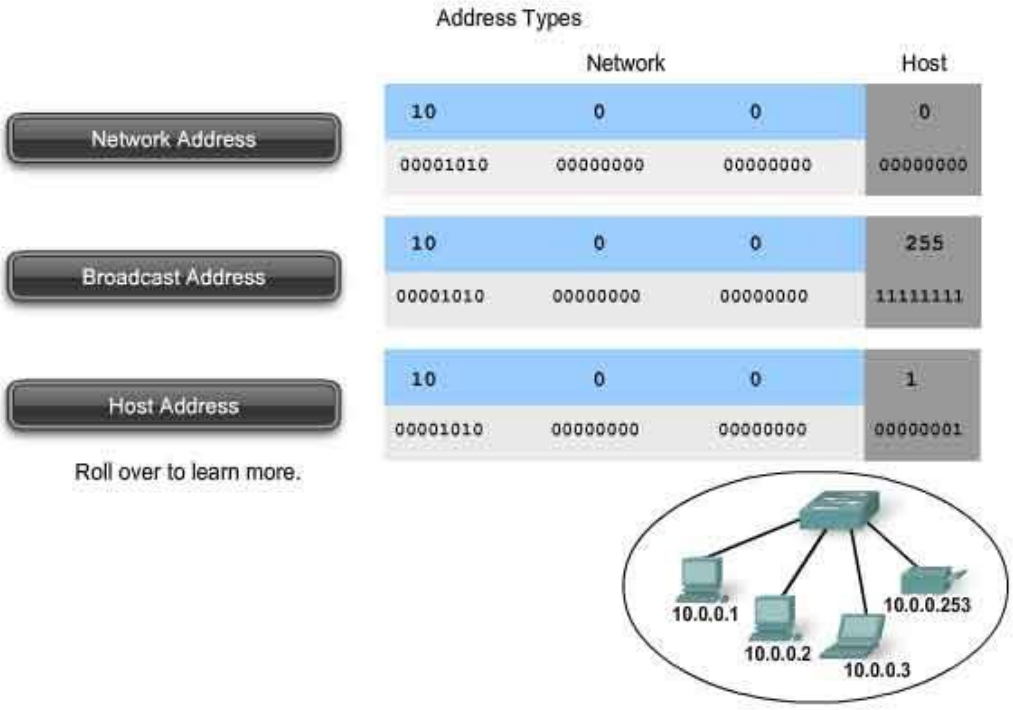
Για την σωστή επιλογή της κάρτας δικτύου πρέπει να γνωρίζουμε τα εξής :

- **Ο τύπος του δικτύου :** ανάλογα με τους τύπους των δικτύων που χρησιμοποιούμε χρησιμοποιούνται και οι κατάλληλες κάρτες δικτύου για αυτές. Επικρατέστερη και πιο χρησιμοποιούμενη θεωρείτε η κάρτα δικτύου για τοπικά δίκτυα (LAN).
- **Ο τύπος του μέσου μετάδοσης :** υπάρχουν διάφοροι τύποι μέσων που χρησιμοποιούνται για την μετάδοση των δεδομένων.
  Μερικοί από αυτούς είναι οι εξής:
  - Ασύρματα
  - Ομοαξονικού τύπου
  - Τύπου καλωδίου συνεστραμμένων ζευγών
  - Οπτικής ίνας

ΚΕΦΑΛΑΙΟ 2 – ΑΣΦΑΛΕΙΑ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

2.1 Η Διεύθυνση IPV4

Η κάθε IPV4 διεύθυνση αποτελείτε από δύο μέρη. Ένα μέρος προσδιορίζει το δίκτυο στο οποίο το σύστημα είναι συνδεδεμένο, και ένα δεύτερο τμήμα προσδιορίζει το συγκεκριμένο σύστημα του δικτύου.



Εικόνα 2.1 Οι βασικές διευθύνσεις του δικτύου

Αυτού του είδους η διεύθυνση, ονομάζεται *ιεραρχική*, επειδή περιέχει διαφορετικά επίπεδα, όπως φαίνεται στο παραπάνω σχήμα. Κάθε οκτάδα (από τις 4), της διεύθυνσης κυμαίνεται από 0 έως 255 .Η κάθε οκτάδα, αναλύεται σε 256 υποομάδες, και αυτές οι ομάδες διασπώνται σε 256 διευθύνσεις η κάθε μία. Μια διεύθυνση IP συνδυάζει αυτά τα δύο αναγνωριστικά σε έναν αριθμό. Ο αριθμός αυτός πρέπει να είναι μοναδικός, επειδή οι διπλές διευθύνσεις δεν επιτρέπονται στο Δίκτυο. **Το πρώτο μέρος** προσδιορίζει τη διεύθυνση δικτύου του συστήματος. **Το δεύτερο μέρος**, μας λέει ποιο συγκεκριμένα σε ποιο δίκτυο ανήκει.
Οι διευθύνσεις IP που δίνονται από τον διαχειριστή του δικτύου, κατασκευάζονται με βάση της ανάγκες που υπάρχουν σε κάθε Δίκτυο.

Οι IP διευθύνσεις χωρίζονται σε πέντε κλάσεις. Αναλόγως με το ποιός αριθμός είναι στην πρώτη οκτάδα (δηλαδή τα πρώτα 8 bits από τα 32 που έχει μία IP) μίας IP διεύθυνσης μπορούμε να καταλάβουμε και σε ποιά κλάση βρίσκεται και συνεπώς πόσα υποδίκτυα και IP διευθύνσεις μπορούμε να έχουμε σε εκείνη την κλάση που βρίσκεται η IP. Πιο συγκεκριμένα έχουμε:

Περιοχή δεκαδικών τιμών της κάθε κλάσης

Class A ——> 0-127

Class B ——> 128-191

Class C ——> 192-223

Class D ——> 224-239

Class E ——> 240-255

Οι κυριότερες κλάσεις είναι οι τρεις πρώτες δηλαδή η A η B και η C καθώς η κλάση D δεσμεύεται για multicasting και η κλάση E είναι δεσμευμένη για testing. Αν λοιπόν έχουμε για παράδειγμα μια IP που ξεκινάει με 15 τότε καταλαβαίνουμε αμέσως ότι είναι κλάσης A.

Κλάση A

Σχεδιάστηκε για να υποστηρίξει μεγάλα σε μέγεθος Δίκτυα. Μια διεύθυνση IP κλάσης A χρησιμοποιεί μόνο την πρώτη οκτάδα για να αναφέρει τη διεύθυνση του δικτύου. Οι υπόλοιπες τρεις οκτάδες χρησιμοποιούνται για διευθύνσεις υποδοχής.

Επειδή χρησιμοποιείται μόνο η πρώτη οκτάδα του σημαίνει ότι ο μέγιστος αριθμός δικτύων που μπορεί να έχει η κλάση αυτή είναι 0 2^7=128 δίκτυα, το οποίο αποτελεί και το πρόθεμα της κλάσης.

Οι υπόλοιπες 3 οκτάδες, χρησιμοποιούνται για να δηλώσουν τον μέγιστο αριθμό των υπολογιστών που μπορεί να αντέξει το κάθε δίκτυο και είναι 2^{24}=16777216, το οποίο αποτελεί και το επίθεμα της κλάσης.

Κλάση B

Η διεύθυνση κλάσης B, σχεδιάστηκε για να υποστηρίξει τις ανάγκες μεγάλου μεγέθους δίκτυα σαφώς μικρότερα όμως από τα δίκτυα κλάσης A.

Μια διεύθυνση IP κλάσης B χρησιμοποιεί δύο από τις τέσσερις οκτάδες για να δείξει την διεύθυνση εργασίας της. Άρα ο μέγιστος αριθμός δικτύων που μπορεί να έχει η κλάση αυτή είναι 2^{14}=16384 δίκτυα, το οποίο αποτελεί και το πρόθεμα της κλάσης.

Οι άλλες δύο οκτάδες καθορίζουν τις διευθύνσεις υποδοχής.
Τα πρώτα 2 bits της πρώτης οκτάδας της διεύθυνσης κλάσης B είναι πάντα 10. Τα υπόλοιπα 6 bits μπορεί να συμπληρωθούν είτε με 1 είτε με 0. Ως εκ τούτου, 0 χαμηλότερος αριθμός που μπορεί να αναπαρασταθεί σε μια διεύθυνση B είναι 10000000 (δεκαδικό 128), και ο μεγαλύτερος αριθμός που μπορεί να παρασταθεί είναι σε δεκαδικό το 191. Κάθε διεύθυνση που ξεκινά με την αξία της τάξεως των 128 - 191 στην οκτάδα είναι μια διεύθυνση κλάσης B. Οι άλλες 2 οκτάδες αποτελούν το επίθεμα της κλάσης. Ο μέγιστος αριθμός υπολογιστών που μπορεί να έχει κάθε δίκτυο από τα 16384 είναι 2^{16}=65536.

Κλάση C

Η διεύθυνση κλάσης C, είναι η πιο συχνά χρησιμοποιούμενη των αρχικών κλάσεων διεύθυνση. Το διάστημα της διεύθυνσης αυτής, προορίζεται να στηρίξει πολλά μικρά δίκτυα.

Μια διεύθυνση κατηγορίας C αρχίζει με δυαδικό 110. Ως εκ τούτου, ο χαμηλότερος αριθμός που μπορεί να εκπροσωπηθεί είναι ο 11000000 (δεκαδικό 192), και ο μεγαλύτερος αριθμός που μπορεί να παρασταθεί είναι ο δεκαδικός 223. Εάν μια διεύθυνση περιέχει έναν αριθμό στο εύρος από 192 έως 223 στην πρώτη οκτάδα, τότε είναι μια διεύθυνση κλάσης C.

Οι 3 πρώτες οκτάδες αποτελούν το πρόθεμα του δικτύου και ο μέγιστος αριθμός δικτύων που μπορεί να έχει αυτή η κλάση είναι 2^{21}=2097152 δίκτυα. Η τελευταία οκτάδα που απομένει θα χρησιμοποιηθεί για την εύρεση του μέγιστου αριθμού υπολογιστών ανά δίκτυο και είναι 2^{8}=256 υπολογιστές.

Κλάση D

Η διεύθυνση κλάσης D, δημιουργήθηκε για να εκπέμπει σε ευρεία μετάδοση (broadcast) μέσα από μία IP. Μία multicast διεύθυνση είναι η μοναδική διεύθυνση του δικτύου που κατευθύνει τα πακέτα που έχουν την διεύθυνση αυτή σε προκαθορισμένες ομάδες του δικτύου. Συνεπώς ένας ενιαίος σταθμός, μπορεί να μεταδώσει ταυτόχρονα σε πολλούς παραλήπτες δεδομένα.
Ο χώρος διεύθυνσης κλάσης D, όπως και τους άλλους χώρους διευθύνσεων, μαθηματικά περιορίζει ότι τα πρώτα 4 bits της διεύθυνσης της κατηγορίας A θα πρέπει να είναι 1110.

Ως εκ τούτου, η πρώτη σειρά οκτάδα για διευθύνσεις D είναι 11100000 - 11101111, ή 224 έως 239. Μια IP διεύθυνση που ξεκινά με μια τιμή στην περιοχή από 224-239 στην πρώτη οκτάδα είναι μια διεύθυνση κατηγορίας D.

Κλάση E

Η διεύθυνση κλάσης E , έχει οριστεί στο διάστημα 240 ως 255. Ωστόσο, η Engineering Task Force Internet (IETF), διατηρεί αυτές τις διευθύνσεις για τη δική του έρευνα. Ως εκ τούτου, δεν υπάρχουν διευθύνσεις της κλάσης E που έχουν κυκλοφορήσει για χρήση στο Διαδίκτυο. Τα πρώτα 4 bits της διεύθυνσης E Class είναι πάντα οριστεί σε 1. Ως εκ τούτου, η πρώτη σειρά οκτάδα για διευθύνσεις της κατηγορίας E είναι 11110000-11111111, ή 240 έως 255.

Από τα παραπάνω προκύπτει ο πίνακας που περιλαμβάνει τον μέγιστο αριθμό των δικτύων καθώς και των μέγιστο αριθμό υπολογιστών που μπορεί να έχει κάθε δίκτυο με βάση την κλάση στην οποία εντάσσετε.

Κλάση διεύθυνσης	Πρόθεμα κλάσης	Μέγιστος αριθμός δικτύων	Επίθεμα κλάσης	Μέγιστος αριθμός υπολογιστών/δίκτυο
A	7	128	24	16777216
B	14	16384	16	65536
C	21	2097152	8	256

Πίνακας 2.1 Οι κλάσεις τις διεύθυνσης IPv4

2.1.1 Ιδιωτικές και δημόσιες διευθύνσεις IP

Οι Δημόσιες διευθύνσεις IP είναι μοναδικές. Δεν υπάρχουν δύο μηχανήματα που να συνδέονται σε ένα δημόσιο δίκτυο, επειδή η δημόσια διεύθυνση IP είναι παγκόσμια και τυποποιημένη. Όλες οι μηχανές που συνδέονται με το Διαδίκτυο συμφωνούν να ενταχθούν στο σύστημα . Οι Δημόσιες διευθύνσεις IP προέρχονται από μια υπηρεσία παροχής Internet (ISP).

Οι ιδιωτικές διευθύνσεις IP χρησιμοποιούνται σε δίκτυα που δεν είναι συνδεδεμένα με το Διαδίκτυο και μπορούν να χρησιμοποιούν οποιαδήποτε έγκυρη διεύθυνση , εφ ‘όσον είναι μοναδικές μέσα στο ιδιωτικό δίκτυο.

2.1.2 Υπολογισμός των διευθύνσεων με κλάσεις

Οι διευθύνσεις IP με κλάσεις, χαρακτηρίζονται ως αναπροσδιοριζόμενες, επειδή η συγκεκριμένη κλάση μπορεί να υπολογιστεί από την ίδια την διεύθυνση.

Ο πίνακας που χρησιμοποιείται για τον υπολογισμό της κλάσης μιας διεύθυνσης είναι ο παρακάτω

Τα bit της διεύθυνσης	Η δεκαδική τους μορφή	Η κλάση της κάθε διεύθυνσης
0000	0	A
0001	1	A
0010	2	A
0011	3	A
0100	4	A
0101	5	A
0110	6	A
0111	7	A
1000	8	B
1001	9	B
1010	10	B
1011	11	B
1100	12	C
1101	13	C
1110	14	D
1111	15	E

Πίνακας 2.2 Υπολογισμός των κλάσεων

Για να είναι εύκολα κατανοητές από τους ανθρώπους χρησιμοποιείται ο *συμβολισμός των δεκαδικών με τελείες*. Όπου κάθε ενότητα αναπαριστάται από 8 bit ενός δεκαδικού αριθμού και ως 32 bit η συνολική δεκαδική τιμή ολόκληρης της διεύθυνσης, (καθώς αποτελείται από 4 ενότητες).

Για παράδειγμα

Η διεύθυνση 129.52.6.0 στο δυαδικό σύστημα γράφετε ως

10000001 . 00110100 . 00000110 . 00000000

(129) . (52) . (6) . (0)

2.1.3 Μάσκες διευθύνσεων

Η μάσκα διευθύνσεων είναι μία διεύθυνση των 32 bit που χρησιμοποιείται για να καθορίσει στο δίκτυο που εφαρμόζετε τον μέγιστο αριθμό υπολογιστών που μπορεί να έχει το δίκτυο αυτό.

Για παράδειγμα , ας υποθέσουμε ότι έχουμε την διεύθυνση δικτύου 192.168.0.0 στο οποίο δίκτυο θέλουμε να τοποθετήσουμε μέχρι 62 υπολογιστές.

Εφαρμόζοντας την δύναμη του 2 για την εύρεση της μάσκας διεύθυνσης έχουμε:

2^6=64 δυνατές διευθύνσεις , από τις οποίες 1 θα χρησιμοποιηθεί ως διεύθυνση δικτύου (επιλέγουμε την 192.168.0.0) και μία θα χρησιμοποιήσουμε ως διεύθυνση ευρείας εκπομπής (επιλέγουμε την 192.168.0.63), επομένως η διευθύνσεις που θα έχουμε θα είναι 62 σύμφωνα με το ζητούμενο.

Η μάσκα διεύθυνσης που προκύπτει στο δυαδικό σύστημα

11111111.11111111.11111111.11000000 (26 bits)

Και εκφράζετε στο δεκαδικό σύστημα

255.255.255.192. επομένως η συγκεκριμένες διευθύνσεις που έχουμε στο συγκεκριμένο δίκτυο είναι από 192.168.0.1 έως 192.168.0.63.

2.2 Τείχος προστασίας (Firewall)

Τα firewalls είναι συσκευές του δικτύου, που επιτρέπουν ACLs (λίστες ελέγχου πρόσβασης), που εφαρμόζονται για τον έλεγχο της πρόσβασης στους χρήστες και εφαρμογές που τρέχουν στους υπολογιστές τους. Τα Firewalls ενισχύουν την ασφάλεια, αν και μπορεί να προκαλέσουν προβλήματα εφαρμογής τους και να επηρεάσουν την απόδοση του δικτύου.

2.2.1 Είδη Firewall

Δύο τύποι firewall που χρησιμοποιούνται σήμερα είναι:

• Οι δρομολογητές όπου το επίπεδο ασφαλείας τους καλύπτεται με 3/4 από ACLs (**ACL Router's**)

• Τα **stateful firewalls**

- ***ACL Router's***

Τα router που χρησιμοποιούν σήμερα τις βασικές εντολές των λιστών πρόσβασης (ACLs), αποτελούν την κινητήρια δύναμη για την ασφάλεια του δικτύου. Αξίζουν να αποκαλούνται Τείχη προστασίας (Firewall's), όπως ακριβώς και μία stateful firewall συσκευή, παρόλο που ίσως να μην έχουν ορισμένα κοινά χαρακτηριστικά με αυτές.
Οι βασικές εντολές ACLs, επιτρέπουν σε έναν διαχειριστή να ελέγχει την ροή της κυκλοφορίας στο επίπεδο δικτύου (Network Layer), καθώς και στο επίπεδο μεταφοράς (Transport Layer).

Ένα παράδειγμα λίστας πρόσβασης, μπορεί να θεωρηθεί το παρακάτω:

Έστω ότι θέλουμε να επιτρέψουμε την κυκλοφορία των TCP πακέτων (θύρα 22), από το δίκτυο 10.1.1.0/24 προς τον χρήστη με διεύθυνση 10.2.3.4

Η εντολή είναι η εξής:

access-list 101 permit tcp 10.1.1.0 0.0.0.255 host 10.2.3.4 eq 22

Επειδή το ACL είναι στατικό και όχι δυναμικό, η ακόλουθη ACL πρέπει να εφαρμοστεί και προς την αντίθετη κατεύθυνση για να είναι όσο το δυνατόν πιο λειτουργική:

access-list 102 permit tcp host 10.2.3.4 eq 22 10.1.1.0 0.0.0.255 established

Επειδή το ACL είναι στατικό, ο δρομολογητής δεν έχει καμία ιδέα για το αν το session SSH είναι ενεργοποιημένο ή όχι. Αυτό οδηγεί στο εξής συμπέρασμα ότι τα ACLs χρησιμοποιούνται επάνω ακριβώς στις διασυνδέσεις για να αποτρέψουν την κυκλοφορία των πακέτων.

Για παράδειγμα ,

access-group 102 in interface FastEthernet 0/0

- ***Statefull Firewalls***

Ένα **Statefull Firewall** παρουσιάζει ίδιες περίπου δυνατότητες, με ένα router που χρησιμοποιεί ACLs. Μία πρόσθετη λειτουργία που έχει το Stateful Firewall, είναι ότι ελέγχει την κατάσταση σύνδεσης που υπάρχει. Στο παράδειγμα, της προηγούμενης λίστας πρόσβασης που εξετάσαμε, παρατηρούμε ότι η δεύτερη εντολή που επιτρέπει την κίνηση επιστροφής (**από τον χρήστη 10.2.3.4 προς το Δίκτυο 10.1.1.0**) δεν είναι απαραίτητη. Το firewall γνωρίζει ότι ένας κεντρικός υπολογιστής στο δίκτυο (**10.1.1.0/24**) ξεκίνησε τη συνεδρία SSH (**θύρα 22**), επιτρέποντας έτσι η κίνηση επιστροφής από τον router με αυτόματο τρόπο. Ως αποτέλεσμα, το Stateful Firewall, παρέχει αυξημένη ασφάλεια, επειδή ο router SSH θα είναι σε θέση να ξεκινήσει επικοινωνία με το δίκτυο (**10.1.1.0/24**), χωρίς την προ εγκατάσταση σύνδεσης. Αν και διαφέρουν σε εφαρμογή, τα Stateful Firewalls παρακολουθούν τις πιο σημαντικές τιμές των πινάκων συνδέσεις:

• Θύρα Πηγή (Source Port)

• Θύρα προορισμού (Destination Port)

• Source IP

• Destination IP

• Sequence Number (αριθμοί ακολουθίας των πακέτων)

Παρακάτω δίνετε ένας πίνακας σύγκρισης των Statefull Firewalls με τους Δρομολογητές, που χρησιμοποιούν λίστες πρόσβασης ως προς τα είδη των επιθέσεων που υπάρχουν.

(Πίνακας από βιβλίο NETWORK SECURITY ARCHITECTURES CISCO PRESS σελ. 146)

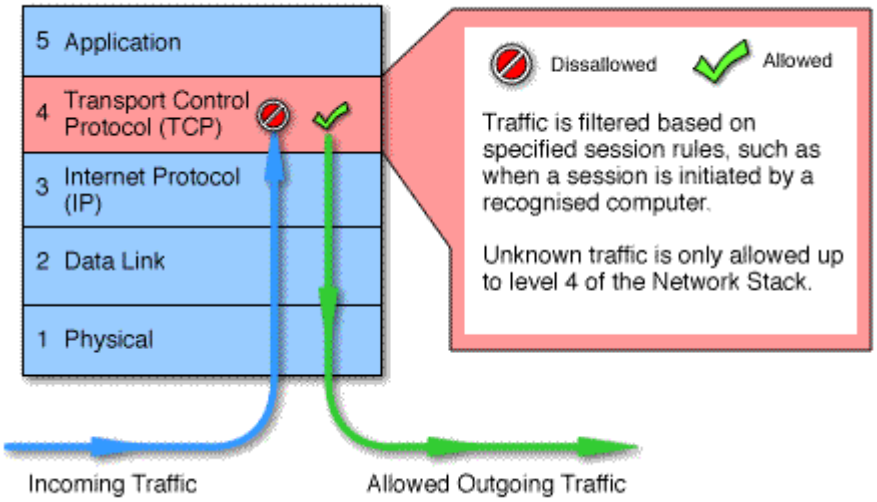
Είδη επιθέσεων	**Δρομολογητής με λίστες πρόσβασης**	**Statefull Firewall**
Αναγνώριση	19.67	19.67
Πρόληψη	123	125
Παράκαμψη	2	4
Ευκολία εφαρμογής τους στο δίκτυο	2	3
Συνέπειες χρηστών	3	4
Διαφάνεια εφαρμογής	2	3
Ωριμότητα εφαρμογής	5	5
Ευκολία διαχείρισης	3	4
Επίδοσης	3	4
Δυνατότητα επέκτασης	3	4
Προσιτό	5	4
Γενικός βαθμός	80	89

Πίνακας 2.3 acl router's vs statefull Firewall's σε διάφορα είδη επιθέσεων

Από τον παραπάνω πίνακα παρατηρούμε, ότι τα Statefull Firewalls , παρουσιάζουν καλύτερα αποτελέσματα σε σύγκριση με τα αποτελέσματα των δρομολογητών. Αυτό συμβαίνει κυρίως, λόγω τις καλύτερης διαχείρισης που έχουν στην ασφάλεια του δικτύου.

- **Circuit – level Gateway's**

Ένας άλλος τύπος δρομολογητών (gateway) που χρησιμοποιούμε για τις εξερχόμενες συνδέσεις είναι το επίπεδο κυκλώματος ή circuit - level. Οι πύλες που είναι επιπέδου κυκλώματος, χρησιμοποιούνται σε TCP συνδέσεις, (στο επίπεδο μεταφορών του μοντέλου O.S.I.). Αυτός που πραγματοποιεί την κλήση, συνδέεται σε μια θύρα TCP στην πύλη του δρομολογητή, η οποία συνδέεται με κάποιο τρόπο στην άλλη πλευρά της πύλης. Κατά τη διάρκεια της κλήσης ο δρομολογητής δημιουργεί ένα αντίγραφο από bytes και η πύλη λειτουργεί όπως ένα απλό καλώδιο.



Εικόνα 2.2 Έλεγχος κυκλοφορίας στο επίπεδο μεταφοράς

Σε ορισμένες περιπτώσεις, η σύνδεση ενός κυκλώματος γίνεται αυτόματα. Για παράδειγμα , υπάρχει ένας χρήστης ο οποίος βρίσκετε εκτός του δικτύου μας, ο οποίος πρέπει να χρησιμοποιήσει έναν εσωτερικό εκτυπωτή. Έχουμε πει στον συγκεκριμένο χρήστη ότι πρέπει να συνδεθεί με μία υπηρεσία εκτύπωσης στην πύλη του δρομολογητή (gateway). Η Πύλη μας είναι ρυθμισμένη για την αναμετάδοση της συγκεκριμένης σύνδεσης με τη θύρα του εκτυπωτή σε μια εσωτερική μηχανή . Χρησιμοποιούμε ένα μηχανισμό ελέγχου πρόσβασης για να διασφαλίσουμε ότι μόνο μία εξωτερική μονάδα μπορεί να συνδεθεί με την υπηρεσία εκτύπωσης της πύλης . Είμαστε επίσης βέβαιοι ότι η συγκεκριμένη σύνδεση δεν θα αποτελεί ένα κενό ασφαλείας που θα θέσει σε κίνδυνο την εξωτερική υποδοχή του δικτύου.

Σε άλλες περιπτώσεις , η υπηρεσία σύνδεσης πρέπει να καθορίσει τον επιθυμητό προορισμό της. Σε αυτή την περίπτωση, πρέπει να καθοριστεί ένα πρωτόκολλο μεταξύ του χρήστη που πραγματοποιεί την κλήση και της πύλης. Αυτό το πρωτόκολλο περιγράφει τον επιθυμητό προορισμό και την επιθυμητή υπηρεσία και η πύλη μπορεί να επιστρέψει πληροφορίες σφάλματος, εάν υπάρχουν. Σε περίπτωση, όπου η σύνδεση θεωρείτε επιτυχής το πρωτόκολλο σύνδεσης ολοκληρώνετε και ξεκινάει η αποστολή bytes.
Οι υπηρεσίες αυτές ελέγχουν το πλήθος των bytes και τον προορισμό της TCP σύνδεσης.

- ***Screening Routers ή Packet Filtering Firewall***

Είναι το Firewall το οποίο εξετάζει την προέλευση του κάθε πακέτου που πρόκειται να εισέλθει στο δίκτυο , μέσω της IP διεύθυνσης του.
Επίσης περιορίζει την πρόσβαση σε υπηρεσίες που προσπαθούν να εισέλθουν στο δίκτυο μέσω τον θυρών.
Υπάρχουν διάφορες επιθέσεις που μπορούν να πραγματοποιηθούν σε packet filtering firewalls.
Μερικά είδη επιθέσεων που μπορούμε να μιλήσουμε γι αυτά είναι τα εξής

- **IP address spoofing**

Με τον όρο IP spoofing εννοούμε, την δημιουργία πακέτων IP με ψεύτικη διεύθυνση προέλευσης ούτως ώστε να συγκαλυφθεί η ταυτότητα του αποστολέα του πακέτου και ο παραλήπτης να νομίζει ότι προήλθε από άλλον υπολογιστή.
Για να καταφέρουμε να αποτρέψουμε αυτού του είδους των επιθέσεων, προτείνετε η εγκατάσταση φίλτρων στον δρομολογητή (Router). Με αυτό τον τρόπο φιλτράρετε η εξερχόμενη κίνηση των πακέτων και μπλοκάρετε η κίνηση των πακέτων από το εσωτερικό δίκτυο καθώς η διεύθυνση πηγής τους δεν υπάρχει στο εσωτερικό δίκτυο.
Για την αποφυγή αυτού του είδους των επιθέσεων , προτείνετε ο σχεδιασμός πρωτοκόλλων ο οποίος δεν βασίζετε στις IP διευθύνσεις για την αυθεντικοποίηση των πακέτων.

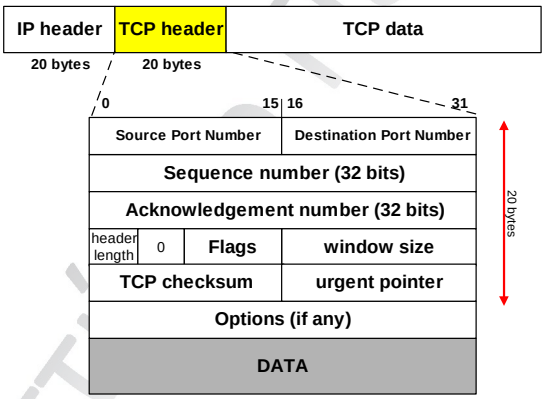
- **Source routing attacks**

Το source route σε IP πακέτα χρησιμοποιείται από το δίκτυο κυρίως για την εύρεση προβλημάτων σε σχέση με την δρομολόγηση των πακέτων και την διευκόλυνση ορισμένων υπηρεσιών.

Τα πακέτα τα οποία φέρουν την επιλογή source route, αγνοούν τις καταχωρήσεις που υπάρχουν για την προώθηση των πακέτων μέσω των δρομολογητών κατά μήκος του δικτύου.
Κατά την μεταφορά τέτοιων πακέτων μέσω του δικτύου, η διεύθυνση πηγής καθώς και η διεύθυνση προορισμού αλλάζουν συνεχώς. Αποτέλεσμα αυτών, είναι ένας επιτιθέμενος να μπορέσει να τροποποιήσει την επιλογή των πακέτων αυτών με την τοποθέτηση ενός δρομολογίου, διαφορετικό από το κανονικό δρομολόγιο, με σκοπό να προκαλέσει σύγχυση στο Δίκτυο.
Μία λύση για την πρόληψη, ως προς τα πακέτα αυτά είναι η απόρριψη τους ή η προώθηση τους εντός του δικτύου και η καταγραφή τους ανάλογα με την διαμόρφωση που έχουν.

- **Tiny fragment attacks**

Πρόκειται για ένα είδος επίθεσης, το οποίο τεμαχίζει την πληροφορία που φέρει, η επικεφαλίδα TCP του πακέτου, έτσι ώστε να μην μπορεί να ανιχνευθεί από τον δρομολογητή ή το firewall του δικτύου.



Εικόνα 2.3 Η δομή της επικεφαλίδας TCP

Ό μόνος τρόπος, που μπορούμε να αποκρούσουμε μία τέτοιου είδους επίθεση, είναι να πραγματοποιείται ανασυγκρότηση της επικεφαλίδας του πακέτου πριν το πέρασμα του, από τα φίλτρα.

2.2.2 θύρες συνδέσεων TCP και UDP

Σύμφωνα με τον διεθνή οργανισμό I.A.N.A. (Internet Assigned Numbers Authority), έχει καθοριστεί σε κάθε θύρα σύνδεσης (TCP και UDP), το πρωτόκολλο με το οποίο θα μπορεί να λειτουργεί η κάθε μία.

Στον παρακάτω πίνακα μπορούμε να δούμε, μερικές από τις επίσημες υπηρεσίες, που πρέπει να χρησιμοποιούν συγκεκριμένες θύρες συνδέσεων .

Ονομασία υπηρεσίας	**Θύρα**	**Πρωτόκολλο μεταφοράς**	**Περιγραφή**
echo	7	TCP,UDP	Error detection
daytime	13	TCP,UDP	Testing protocol
ftp-data	20	TCP,UDP	File transfer protocol
ftp	21	TCP,UDP	File transfer protocol
SSH	22	TCP,UDP	Secure Shell Protocol
telnet	23	UDP	Protocol using virtual terminal connection
SMTP	25	TCP,UDP	Simple Mail Transfer
name	42	TCP,UDP	Host Name Server
domain	53	TCP,UDP	Domain Name Server
TFTP (Trivial File Transfer Protocol)	69	TCP,UDP	Read and write Files in terminal Server
HTTP	80	TCP,UDP	World Wide Web
Kerberos	88	TCP,UDP	Authentication protocol for node communication
hostname	101	TCP,UDP	Translate host name to internet address

author	113	TCP,UDP	Cryptographic Protocol with authenticating entities
SFTP	115	TCP,UDP	Secure transfer protocol extend of secure shell
IMAP	143	TCP,UDP	Internet Message access protocol
SEND	169	TCP,UDP	Security Extension of Neighbour Discovery Protocol in IPV6
SET (Secure Electronic Transaction)	257	TCP,UDP	Communication protocol for securing credit card Transaction
BGMP (Border Gateway Multicast Protocol)	264	TCP,UDP	A routing protocol for the global internet
M.A.N.E.T. Protocol	269	TCP,UDP	A routing protocol for mobile devices
MFTP	349	TCP,UDP	Multicast file transfer protocol
LDAP	389	TCP,UDP	Catalogue/information service over IP network
https	443	TCP,UDP	http protocol over SSL/TLS
tunnel	604	TCP,UDP	Use a protocol ex. IP to 'ship' a foreign protocol across a network

Πίνακας 2.4 Υπηρεσίες θυρών TCP, UDP

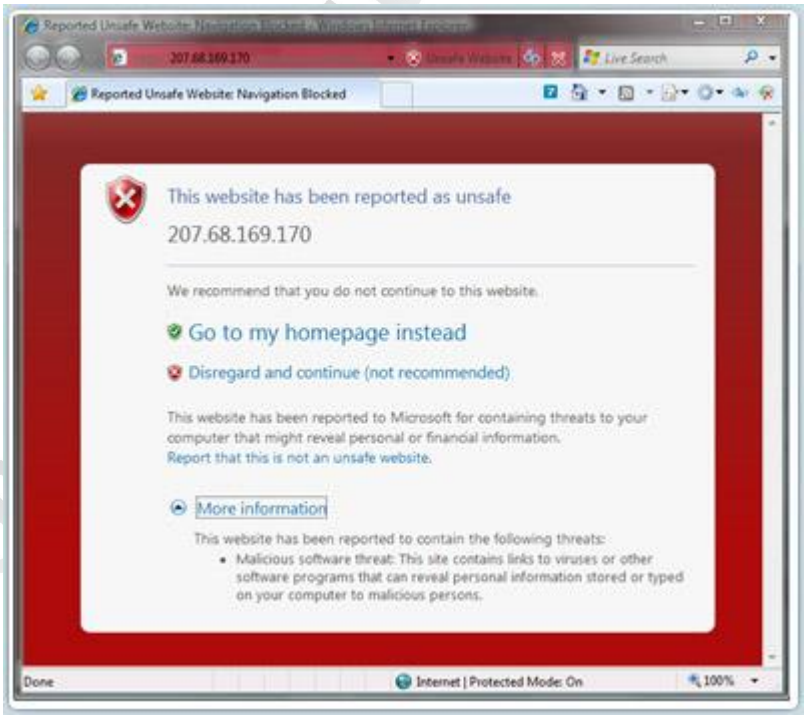
2.3 Content Filtering (φιλτράρισμα περιεχομένου)

Στην συνέχεια της ενότητας, θα αναφερθούμε σε τεχνολογίες όπως web filtering , proxy servers και e-mail filtering. Οι συγκεκριμένες τεχνολογίες αποτελούν την καλύτερη προσθήκη, σε δίκτυα που έχουν Firewall συστήματα και δρουν ως ένα επιπλέον στρώμα προστασίας σε αυτά.

Web filtering

Αποτελεί μία τεχνολογία η οποία έχει σχεδιαστεί για να περιορίσει την πρόσβαση από το δικό μας δίκτυο προς το εξωτερικό. Αυτό πραγματοποιείται μέσω *φιλτραρίσματος διευθύνσεων URL* και *κινητού κώδικα φιλτραρίσματα*.

Το *URL φιλτράρισμα* λειτουργεί με την αποστολή αιτημάτων (requests), προς τον URL – Filtering Server, όπου αυτός στην συνέχεια ελέγχει κάθε αίτημα χωριστά αν υπάρχει ως εγγραφή σε μία βάση δεδομένων που περιέχει τα site που θεωρούνται ασφαλή. Στην περίπτωση, όπου το αίτημα είναι επιτρεπτό, ο server μεταβιβάζει τον χρήστη κατευθείαν στην ιστοσελίδα, ενώ σε περίπτωση όπου το αίτημα δεν είναι επιτρεπτό, στέλνετε προς τον χρήστη ένα μήνυμα προειδοποίησης (Alert message) ή τον κατευθύνει προς μία άλλη σελίδα. Συνοψίζοντας μπορούμε να πούμε ότι το URL Filtering, χρησιμοποιείται για να κατευθύνει τους χρήστες , μόνο σε ασφαλής ιστοσελίδες.



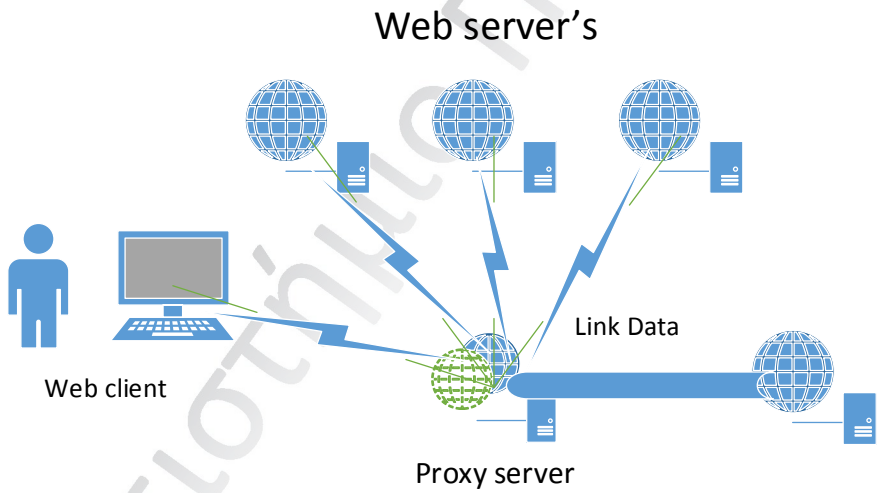
Εικόνα 2.4 Περιορισμός πρόσβασης στην ιστοσελίδα

Το *φιλτράρισμα κινητού κώδικα* είναι η προσπάθεια που πραγματοποιείται από ένα επιτιθέμενο στο να έχει πρόσβαση στο web traffic ενός χρήστη, με σκοπό την εισχώρηση κακόβουλων δεδομένων – κώδικα. Μία περίπτωση αντιμετώπισης μίας τέτοιας επιθέσεις, είναι όλη η κυκλοφορία των δεδομένων να περνάει μέσω proxy server (αναλύετε παρακάτω), και μέσω ενός σαρωτή να ελέγχετε ο κώδικας πριν καν αποσταλεί στον χρήστη.

Η χρησιμοποίηση τέτοιων φίλτρων σε ένα οργανισμό , θα δημιουργήσει προβλήματα και καθυστερήσεις ως προς την απόδοση του δικτύου.

Proxy server

Ο Router μεσολάβησης ή όπως τον λέμε ***Proxy Server,*** λειτουργεί ως ένας ενδιάμεσος δρομολογητής, ο οποίος λαμβάνει τα αιτήματα (request) ενός πελάτη και ενός server.



Εικόνα 2.5 Αρχιτεκτονική Proxy Server

Ο Proxy Server, μπορεί να χρησιμοποιηθεί για να λαμβάνει και να παρακολουθεί όλες τις αλληλεπιδράσεις που πραγματοποιούνται μεταξύ τις σχέσης Client - Server.

Κάποια από τα συγκεκριμένα πρωτόκολλα που μπορεί να παρακολουθήσει είναι τα εξής:

- **Πρωτόκολλα HTTP** που χρησιμοποιούνται σε ιστοσελίδες.
- **Πρωτόκολλα HTTPS** που χρησιμοποιούνται σε ασφαλείς ιστοσελίδες οι οποίες διαθέτουν πιστοποιητικά πρόσβασης.
- **Πρωτόκολλα SMTP** για μηνύματα ηλεκτρονικού ταχυδρομείου.

Οι Proxy Servers είναι πιο αργή σε σχέση με τα Firewalls, καθώς πραγματοποιούν επανεγκατάσταση της κάθε σύνδεσης, για κάθε σύνδεση που υπάρχει.

Έχει παρατηρηθεί, ότι οι Proxy Servers παρουσιάζουν κάποιες δυσκολίες στις συνδέσεις τους με τις εφαρμογές του Δικτύου. Για παράδειγμα όταν μία εφαρμογή μεταφέρετε προς το Διαδίκτυο διαμέσου ενός Proxy Server, ο συγκεκριμένος Router, θα πρέπει να κατανοήσει το συγκεκριμένο πρωτόκολλο για να του επιτρέψει την πρόσβαση.

Μία τεχνική που παρατηρείται στην χρήση αυτού του Router, είναι ότι συνήθως τοποθετείται ακριβώς πίσω από τον Firewall του Δικτύου για να μπορεί να ελέγχει τα εξερχόμενα πακέτα των χρηστών στο Διαδίκτυο. Έτσι το user authentication, το URL filtering , το caching και άλλες τεχνικές θα μπορούν να καταστούν δυνατές για χρησιμοποίηση τους από τους χρήστες. Με αυτό τον τρόπο τα δικαιώματα πρόσβασης εφαρμόζονται στο έπακρο για το σύνολο των χρηστών που θα πρέπει να εφαρμοστούν, επιτρέποντας σε άλλους χρήστες (με βάση την πολιτική ασφάλειας που έχουν), απεριόριστη πρόσβαση στο Internet. Αυτό επίσης δίνει την δυνατότητα στο τείχος προστασίας να απασχοληθεί με τον έλεγχο της κυκλοφορίας στην περίμετρο ασφαλείας, χωρίς να απασχολείται με τα δικαιώματα του χρήστη.

E-mail filtering

Πραγματοποιεί το ίδιο περίπου φιλτράρισμα με αυτό του web filtering. Η gateway του router ελέγχει τα εισερχόμενα και εξερχόμενα μηνύματα για κακόβουλο κώδικα. Τα μηνύματα τα οποία κυρίως σαρώνονται για ιούς, είναι τα συνημμένα μηνύματα τα οποία περιέχουν αρχεία. Το μήνυμα το οποίο περιέχει το μολυσμένο αρχείο διαγράφετε ολοσχερώς ή μόνο το συγκεκριμένο τμήμα που περιέχει το μολυσμένο αρχείο και στην συνέχεια επιστρέφει στον χρήστη ενημερώνοντας των για το μήνυμα αυτό. Όταν αναγνωριστεί ο ιός πραγματοποιείται ενημέρωση του gateway του router με πιο γρήγορο ρυθμό από ότι στο υπόλοιπο δίκτυο.

Πίνακας από cisco security chapter 4 pp.151

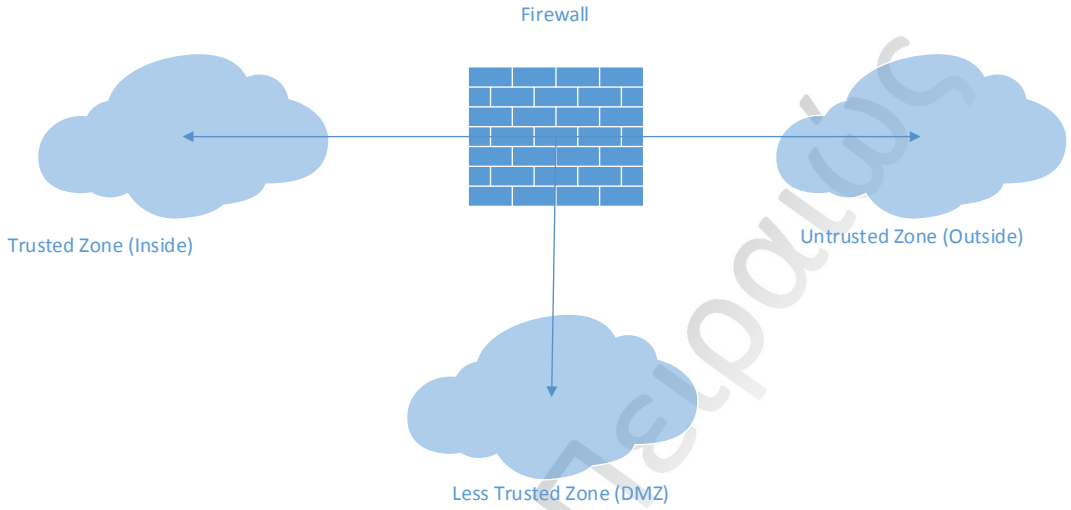
Στην συνέχεια παρουσιάζετε ένας συνοπτικός πίνακας παρουσίασης των τριών παραπάνω τεχνολογιών φιλτραρίσματος στον οποίο συγκρίνονται σε σχέση με διαφορετικά στοιχεία επιθέσεων.

Στοιχείο επίθεσης	**Proxy server**	**Web Filtering**	**E-mail Filtering**
Αναγνώριση	0	0	0
Πρόληψη	39	81	79
Παράκαμψη	3	3	4
Ευκολία εφαρμογής τους στο δίκτυο	4	4	5
Συνέπειες χρηστών	2	1	5
Διαφάνεια εφαρμογής	1	4	4
Ωριμότητα εφαρμογής	4	3	4
Ευκολία διαχείρισης	3	4	4
Επίδοσης	2	1	4
Δυνατότητα επέκτασης	3	1	4
Προσιτό	4	3	3
Γενικός βαθμός	43	53	69

Πίνακας 2.5 Σύγκριση Proxy Server, Web, E-Mail Filtering

2.4 Αντιπυρική ζώνη DMZ

Το DMZ (De Militarized Zone network), αποτελεί την πιο συνηθισμένη μορφή υλοποίησης σε περιβάλλον firewall. είναι μία περιοχή του δικτύου η οποία χαρακτηρίζετε, ως η *λιγότερη περιοχή εμπιστοσύνης,* ανάμεσα στις 3 διαφορετικές περιοχές που υπάρχουν στο δίκτυο.



Εικόνα 2.6 Δομή DMZ

Για να μπορέσουμε να διαχειριστούμε το επίπεδο εμπιστοσύνης που υπάρχει σε κάθε ζώνη του δικτύου, εφαρμόζουμε στις διασυνδέσεις που διατηρεί το firewall με την κάθε περιοχή, security – levels.

Ως περιοχή εμπιστοσύνης χαρακτηρίζετε η περιοχή του δικτύου στην οποία ανήκει το τοπικό δίκτυο (LAN).

Ως περιοχή μη-εμπιστοσύνης χαρακτηρίζετε η περιοχή η οποία δεν ανήκει στο δίκτυο αλλά η ευρύτερη περιοχή του διαδικτύου (internet).

Η κυκλοφορία των δεδομένων από μία περιοχή, η οποία έχει υψηλό δείκτη εμπιστοσύνης προς μία περιοχή με χαμηλότερο δείκτη εμπιστοσύνης, όπως παρουσιάζετε από τις εργαστηριακές μετρήσεις που θα ακολουθήσουν επιτρέπετε, ενώ η κυκλοφορία από μια περιοχή χαμηλής εμπιστοσύνης προς μία υψηλότερη επιτρέπετε, υπό προϋποθέσεις, οι οποίες καθορίζονται από τον διαχειριστή του Δικτύου.

Τα Δίκτυα DMZ, παρέχουν τις υπηρεσίες τους, τόσο στο εξωτερικό Δίκτυο (external network), όσο και στο εσωτερικό Δίκτυο (internal network), με αποτέλεσμα να πρέπει να προστατευτούν τόσο από τους εσωτερικούς χρήστες (internal users) , όσο και από το εξωτερικούς χρήστες (external users).

2.4.1 Η Αρχιτεκτονική DMZ

Η κύρια λειτουργία του DMZ, είναι να προστατεύσει τους κόμβους του Δικτύου οι οποίοι, παρέχουν υπηρεσίες προς το εξωτερικό Δίκτυο, μέσω των Servers του Δικτύου.

- Mal servers
- Web servers
- ftp servers

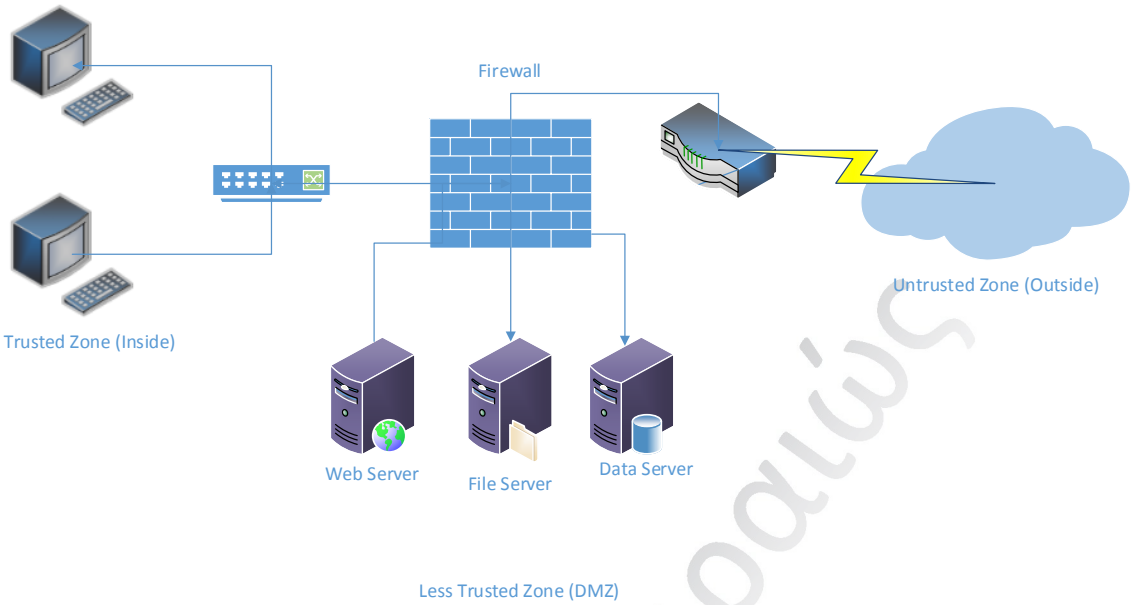
Η περιοχή DMZ χρησιμοποιεί το firewall για τον έλεγχο της πρόσβασης

- Από την περιοχή του internet, προς την περιοχή του DMZ, με σκοπό να προστατεύσει τους servers
- Από την περιοχή DMZ προς το εσωτερικό intranet, με σκοπό να περιορίσει την αμοιβαίες εισχωρήσεις

Οι 2 πιο βασικές αρχιτεκτονικές DMZ, που υπάρχουν σήμερα είναι

- Με την χρησιμοποίηση ενός firewall

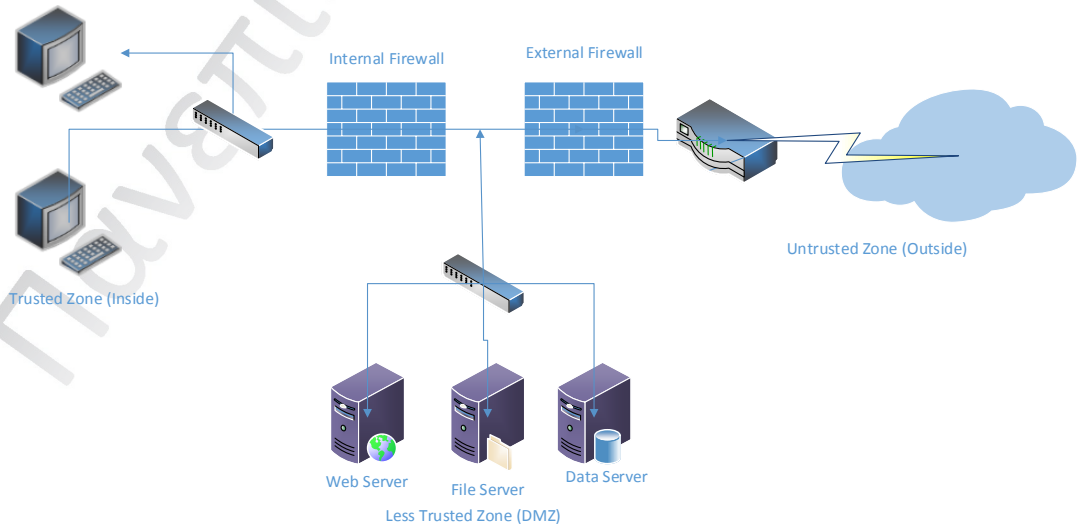
Η πιο συνηθισμένη αρχιτεκτονική με την χρησιμοποίησης ενός firewall είναι η λεγόμενη «service leg» ρύθμιση firewall , όπου το firewall χωρίζετε σε 3 διαφορετικά interfaces. Το πρώτο interface χρησιμοποιείται για το external network. Το δεύτερο interface χρησιμοποιείται για το internal network μέσω κάποιου network switch και το τρίτο interface χρησιμοποιείται για το DMZ Δίκτυο.



Εικόνα 2.7 Αρχιτεκτονική DMZ

Αυτού του είδους η ρύθμιση προσφέρει ένα αυξημένο κίνδυνο των υπηρεσιών που παρέχονται από το DMZ Δίκτυο, στην μορφή επίθεσης Denial Of Service D.O.S. Attacks. Αυτού του είδους η επίθεση κατά πάσα πιθανότητα προσβάλει, μόνο τους συγκεκριμένους πόρους του δικτύου που γίνετε η επίθεση. Την βάρος της ευθύνης το φέρει το ίδιο το firewall σε τέτοιου είδους επιθέσεις καθώς πρέπει να αναλύει, οποιαδήποτε κίνηση, πριν εισέλθουν στο ευαίσθητο τμήμα του Δικτύου.

- Με την χρησιμοποίηση δύο firewall



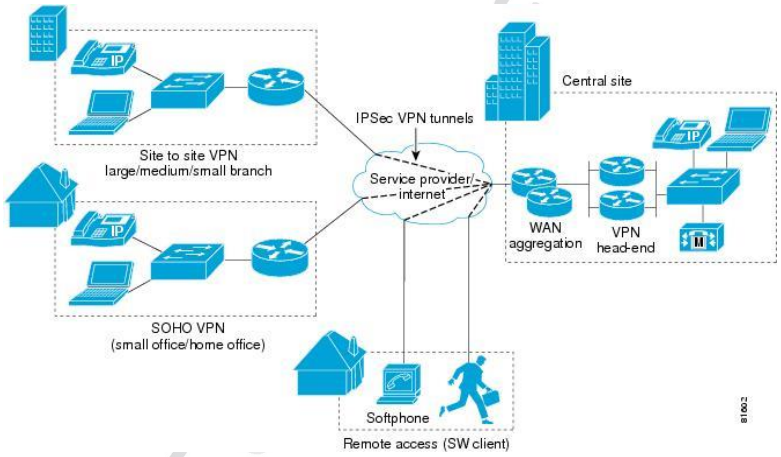
Εικόνα 2.8 Αρχιτεκτονική DMZ με χρησιμοποίηση δύο Firewall

Χρησιμοποιώντας για παράδειγμα 2 firewall στο δίκτυο μας, το ένα από αυτά, θα παρείχε προστασία, για τους servers του Δικτύου και το άλλο θα έλεγχε την πρόσβαση στους server’s σε περίπτωση όπου δεχόντουσαν επίθεση. Σε κάθε περίπτωση όμως και τα 2 firewall’s θα προστάτευαν τόσο από εξωτερικές όσο και από εσωτερικές επιθέσεις. Τα DMZ Δίκτυα σε αυτή την περίπτωση θα τοποθετηθούν, ανάμεσα στα 2 firewall’s του Δικτύου. Για παράδειγμα , σε περίπτωση, όπου χρειάζεται να πραγματοποιηθεί σύνδεση με χρήστες απομακρυσμένης πρόσβασης, για την είσοδο τους στο Δίκτυο, συνηθίζετε να τοποθετούμε τους Remote Access Servers εντός του DMZ Δικτύου, έτσι ώστε σε περίπτωση επίθεσης μέσω απομακρυσμένης πρόσβασης να μπορεί το firewall να ελέγχει, αυτή την κίνηση.

2.4.2 Χρησιμοποίηση Firewall σε Virtual private networks

Μία ακόμα σημαντική χρησιμοποίηση των firewalls σε δίκτυα είναι για τον έλεγχο των VPN δικτύων.

Τα VPN δίκτυα όπως γνωρίζουμε παρέχουν απομακρυσμένη πρόσβαση σε χρήστες οι οποίοι βρίσκονται σε διαφορετικά είδους δίκτυα. Το VPN δίκτυο συνήθως τοποθετείται στην κορυφή του υπάρχοντος δικτύου παρέχοντας πρόσθετα πρωτόκολλα κατά την επικοινωνία τους με τους εξωτερικούς χρήστες του δικτύου χρησιμοποιώντας κρυπτογράφηση στα πρωτόκολλα αυτά. Η κρυπτογράφηση του VPN δικτύου μπορεί να χρησιμοποιηθεί ως επέκταση προστασίας για το εσωτερικό – ευαίσθητο δίκτυο. Με αυτό τον τρόπο το VPN δίκτυο παρέχει διασυνδέσεις με αλλά δίκτυα τα οποία θεωρούνται μη-εμπιστοσύνης. Επίσης δίνετε η δυνατότητα εκμετάλλευσης μίας μόνο σύνδεση ως προς το εξωτερικό δίκτυο και η οποία μπορεί να χρησιμοποιηθεί για να παρέχει απομακρυσμένη πρόσβαση σε διαφορετικά ιδιωτικά δίκτυα και στην εκμετάλλευση των πόρων τους από αυτό. Ο συγκριμένος θεωρείται οικονομικά αποδοτικός για πολλούς οργανισμούς.



Εικόνα 2.9 Η αρχιτεκτονική της VPN μέσω IPsec

Ένα από τα πιο σημαντικά πρωτόκολλα που χρησιμοποιούνται για τα VPN δίκτυα είναι το IPSEC πρωτόκολλο (internet protocol security). Το IPSEC πρωτόκολλο χρησιμοποιείται για IP επικοινωνία αυθεντικοποιώντας κατά την έναρξη της σύνδεσης και κρυπτογραφώντας κάθε IP πακέτο του κατά την περίοδο επικοινωνίας. Αλλά σημαντικά πρωτόκολλα που χρησιμοποιούνται για τα VPN δίκτυα είναι τα PPTP (Point - to - Point Tunneling Protocol), και τα L2TP (Layer 2 Tunneling Protocol)

Η τοποθέτηση των VPN servers γίνετε συνήθως στο σημείο που βρίσκετε το firewall. Η συγκεκριμένη τοποθέτηση θεωρείται η πιο σωστή <<τεχνικά>>, για τον λόγο ότι το VPN server παρέχει κρυπτογραφημένη επικοινωνία (μέσω τον IPSEC και των άλλων πρωτοκόλλων του) και σε περίπτωση τοποθέτησης του πίσω ακριβώς από τον firewall θα δημιουργήσει προβλήματα στην επικοινωνία του καθώς το firewall θα κάνει drop τα κρυπτογραφημένα πακέτα που θα αποστέλλονται και θα λαμβάνονται καθώς δεν θα μπορεί να τα αναγνωρίζει και κατά συνέπεια να μπορεί να τα ελέγξει.

Εξαρτήματα δικτύου hubs και switches

Τα συγκεκριμένα εξαρτήματα αποτελούν ένα σημαντικό κομμάτι στην υποδομή του δικτύου.

Το πιο απλό εξάρτημα που μπορεί να χρησιμοποιηθεί σε δίκτυο είναι το hub. Το hub είναι μία συσκευή η οποία λειτουργεί, όπως αναφέραμε και στο κεφάλαιο 1 , στο φυσικό επίπεδο. Το μόνο που μπορεί να παρέχει είναι φυσική σύνδεση μεταξύ των συσκευών δημιουργώντας μειονεκτήματα κατά την χρήση τους. Το πιο σημαντικό ελάττωμα είναι ότι συνδέουν οποιαδήποτε συσκευή με οποιαδήποτε άλλη καθιστώντας τα απαγορευτικά για την χρησιμοποίηση τους σε DMZ δίκτυα.

Αντίθετα τα switch είναι συσκευές οι οποίες μπορεί να χρησιμοποιηθούν σε DMZ δίκτυα και σε firewall περιβάλλοντα. Λειτουργούν στο επίπεδο διασύνδεσης δεδομένων (data link layer) , παρέχοντας βασική αναγνώριση των διασυνδέσεων που πραγματοποιούνται επάνω σε αυτά.

Όπως έχουμε αναφέρει και σε προηγούμενο κεφάλαιο τα network switches είναι συσκευές οι οποίες αποτελούνται από πολλές θύρες εισόδων/εξόδων μεταφέροντας όλο το εύρος ζώνης του δικτύου σε κάθε θύρα. Ένα πλεονέκτημα που μπορεί να παρουσιάσει αυτή η συσκευή είναι ότι ένα σύστημα το οποίο συνδέετε μέσω του switch δεν μπορεί να υποκλέψει πληροφορίες από μία άλλη σύνδεση καθιστώντας τα χρήσιμα στα DMZ δίκτυα και firewall περιβάλλοντα.

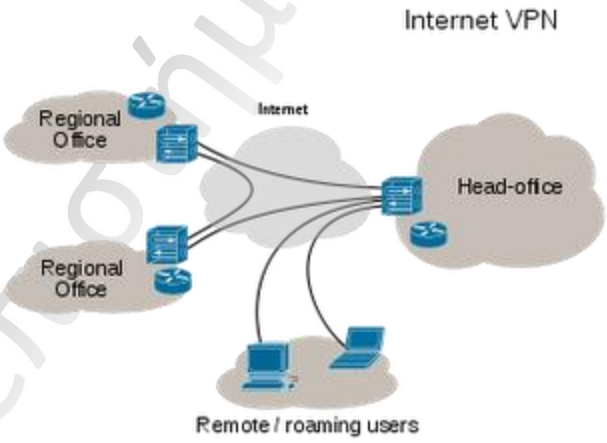
2.5 Εικονικά Ιδιωτικά Δίκτυα (Virtual Private Networks)

Το VPN είναι ένα δίκτυο εικονικών ζεύξεων ανεπτυγμένο σε μία υπάρχουσα δικτυακή υποδομή, με τη ιδιότητα ότι έχει την ίδια ασφάλεια, διαχείριση και υφίσταται την ίδια πολιτική σε όλο το μήκος του σαν να επρόκειτο για ιδιωτικό δίκτυο. Οι απαιτήσεις των VPN's δεν είναι άλλες από αυτές των WAN: υποστήριξη πολλαπλών πρωτοκόλλων, υψηλή αξιοπιστία και εκτεταμένη διαβάθμιση. Ένα VPN μπορεί να αξιοποιήσει τις πιο γνωστές τεχνολογίες μεταφοράς που υπάρχουν σήμερα:

- το δημόσιο Internet (κατά κύριο λόγο),
- τα IP backbones διαφόρων παροχών υπηρεσιών όπως επίσης και
- τα Frame Relay και ATM δίκτυά τους.

Οι δικτυακές εικονικές συνδέσεις που δημιουργούνται μεταξύ του χρήστη και του δικτύου στο οποίο επιθυμεί να έχει πρόσβαση, θεωρούνται ιδεατές καθώς τα πακέτα που αποστέλλονται μπορούν να ακολουθήσουν διαφορετικές διαδρομές μέχρι που να φτάσουν στο δίκτυο και όχι μία συγκεκριμένη διαδρομή όπως θα μπορούσαμε να φανταστούμε.

Ένα Δίκτυο VPN στηρίζετε κυρίως στο πρωτόκολλο IP, όπου η μετάδοση των δεδομένων γίνετε σε πακέτα IP και μεταδίδεται στο IP Δίκτυο.



Εικόνα 2.10 Η αρχιτεκτονική VPN

Ένα IP VPN (η πιο συνηθισμένη περίπτωση Εικονικών Ιδιωτικών Δικτύων) είναι μία δικτυακή σύνδεση η οποία από την πλευρά των χρηστών συμπεριφέρεται σαν να ήταν μία ιδιωτική σύνδεση, παρόλο που χρησιμοποιείται κοινή διαμοιρασμένη δικτυακή υποδομή (shared communication infrastructure) για την πραγματοποίηση της σύνδεσης. Επιπλέον, η υλοποίηση των Εικονικών Ιδιωτικών Δικτύων είναι δυνατόν να βασίζεται στις τεχνολογίες ATM (Asynchronous Transfer Mode), Frame Relay ή MPLS (Multiprotocol Label Switching).

Το MPLS πρωτόκολλο χρησιμοποιήθηκε για την αύξηση της απόδοσης του IP πρωτοκόλλου και για την παροχή νέων υπηρεσιών προς το Διαδίκτυο.

Τα Δίκτυα ATM είναι δίκτυα ασύγχρονου τρόπου μεταφοράς δεδομένων. Μέσα από αυτά τα δίκτυα ο χρήστης μπορεί να μεταδώσει φωνή και δεδομένα με πολύ υψηλές ταχύτητες που μπορεί να φτάσουν και τα 155 Mbps. Η επικοινωνία τους στηρίζετε σε εικονικά τύπου κυκλώματα, όπου κατά την επικοινωνία 2 χρηστών έχουμε δέσμευση πόρων του δικτύου και όλα τα πακέτα που αποστέλλονται ακολουθούν την ίδια διαδρομή σε αντίθεση με τα IP πακέτα όπου δεν ακλουθούν πάντα την ίδια διαδρομή. Η διαδρομή αυτή δεν θεωρείται αποκλειστικής χρήσης και είναι κοινόχρηστη και το κύκλωμα απελευθερώνει την συγκεκριμένη διαδρομή με το τερματισμό της κλήσης.

2.5.1 Αρχιτεκτονικές Εικονικών Ιδιωτικών Δικτύων

Τα Εικονικά Ιδιωτικά Δίκτυα χωρίζονται στις εξής κατηγορίες:

1. **Με βάση την αντιστοιχία τους με τα επίπεδα του μοντέλου αναφοράς OSI**, τα Εικονικά Ιδιωτικά Δίκτυα κατηγοριοποιούνται ως εξής:

a. **Στα Εικονικά Ιδιωτικά Δίκτυα Επιπέδου 3 (Δικτύου)**. Σε αυτήν ανήκουν τα VPN που δομούνται πάνω σε IP δίκτυα και χρησιμοποιούν το πρωτόκολλο IPSec, καθώς και τα VPN που δομούνται πάνω σε MPLS δίκτυα.

b. **Στα Εικονικά Ιδιωτικά Δίκτυα Επιπέδου 2 (Ζεύξης Δεδομένων)**. Σε αυτήν την κατηγορία εμπίπτουν τα VPN στα οποία χρησιμοποιείται κάποιο από τα πρωτόκολλα L2F, PPTP, L2TP. Επίσης VPN επιπέδου 2 μπορούν να αναπτυχθούν πάνω στην τεχνολογία MPLS.

c. **Στα Εικονικά Δίκτυα επιπέδου 4 (Μεταφοράς)**. Σε αυτήν την κατηγορία εμπίπτουν τα VPN στα οποία χρησιμοποιείται το πρωτόκολλο SSL.

2. **Με βάση το είδος της διόδου (tunnel)** που αναπτύσσεται (όπου με τον όρο δίοδο εννοούμε πρακτικά το νοητό κύκλωμα που σχηματίζεται, μέσω του οποίου γίνεται η μετάδοση των δεδομένων στο VPN). Υπάρχουν δύο είδη διόδων που προσδιορίζουν και την αντίστοιχη κατηγορία στην οποία εμπίπτει ένα VPN:

a. οι «αυθόρμητες δίοδοι» (voluntary tunnels),

b. οι «αναγκαστικές» δίοδοι (compulsory ή mandatory tunnels).

3. **Με βάση το ποιοι είναι οι τελικοί χρήστες του VPN** (δηλαδή ποια είναι τα δύο μέρη που συνομιλούν). Έτσι έχουμε:

a. Τα VPN δομής «πελάτης-προς-δίκτυο» (client - to - LAN), όπου στην ουσία ένας απλός χρήστης συνδέεται με τον υπολογιστή του σε ένα τοπικό δίκτυο. Αυτού του είδους τα VPN ονομάζονται επίσης και «**Εικονικά Ιδιωτικά Δίκτυα Απομακρυσμένης Πρόσβασης**»

b. Τα VPN δομής «δίκτυο-προς-δίκτυο» (LAN-to-LAN), όπου η δίοδος μεταφοράς των δεδομένων αναπτύσσεται μεταξύ δύο τοπικών δικτύων.

2.5.2 Εικονικά Ιδιωτικά Δίκτυα βασισμένα στο πρωτόκολλο IPsec

Τα πρωτόκολλα IPSec, παρέχει μηχανισμούς κρυπτογράφησης σε ένα IP πρωτόκολλο και χρησιμοποιείται για την ασφαλή μετάδοση των δεδομένων πάνω από ένα IP Δίκτυο.

Το IPsec σήμερα αποτελεί έναν από τους πιο διαδεδομένους τρόπους υλοποίησης των δικτύων VPN. Ως προς τα επίπεδα του OSI, αντιστοιχίζεται στο επίπεδο 3 (επίπεδο δικτύου).

Τα θέματα ασφάλειας που ανακύπτουν με τη χρησιμοποίηση του Διαδικτύου για τη πραγματοποίηση ιδιωτικών επικοινωνιών είναι τα ακόλουθα:

• ***Απώλεια της Ιδιωτικότητας των Δεδομένων (Loss of Privacy):*** Σ’ αυτήν την περίπτωση ένας μη εξουσιοδοτημένος χρήστης που έχει καταφέρει να εισχωρήσει σε κάποιο δίκτυο έχει τη δυνατότητα να παρακολουθεί εμπιστευτικά δεδομένα κατά τη διακίνησή τους στο Internet.

• ***Απώλεια Ακεραιότητας Δεδομένων (Loss of Data Integrity):*** Σ’ αυτήν την περίπτωση ένας μη εξουσιοδοτημένος χρήστης αλλάζει τα δεδομένα που μεταφέρονται στο δίκτυο (π.χ. τους αριθμούς ενός λογαριασμού καταθέσεων)

• ***Προσποίηση ταυτότητας (Identity Spoofing):*** Σε αυτή την περίπτωση ένας μη εξουσιοδοτημένος χρήστης παριστάνει ότι ένας νόμιμος χρήστης του δικτύου και ζητά πληροφορίες οι οποίες είναι ιδιωτικές.

• ***Άρνηση Υπηρεσιών (Denial - of - Service)*****:** Σ' αυτήν την περίπτωση γίνεται "επίθεση" σε κάποιον server του δικτύου.

Ο βασικός στόχος στην ανάπτυξη του προτύπου IPSec είναι η αντιμετώπιση των παραπάνω απειλών χωρίς να απαιτείται πρόσθετος εξοπλισμός, ούτε να υπάρχει ανάγκη για ένα σύνολο τροποποιήσεων και αλλαγών σε διάφορες εφαρμογές.

Έτσι οι υπηρεσίες που προσφέρει το πρωτόκολλο IPSec είναι:

• **Ακεραιότητα των δεδομένων (Integrity)**, που διασφαλίζει ότι τα πακέτα των δεδομένων κατά την διάρκεια της μεταφοράς τους δεν έχουν αλλοιωθεί ή παραποιηθεί, είτε από «εισβολείς» είτε από τυχόν σφάλματα επικοινωνίας.

• **Εξακρίβωση γνησιότητας της προέλευσης των δεδομένων (Authentication) ή πιστοποίηση ταυτότητας,** που επαληθεύει ότι τα δεδομένα στάλθηκαν πράγματι από το χρήστη που ισχυρίζεται ότι τα έστειλε.

• **Εμπιστευτικότητα (Confidentiality),** που προσφέρει τη δυνατότητα αναγνώρισης και επεξεργασίας των δεδομένων μόνο από εγκεκριμένους χρήστες.

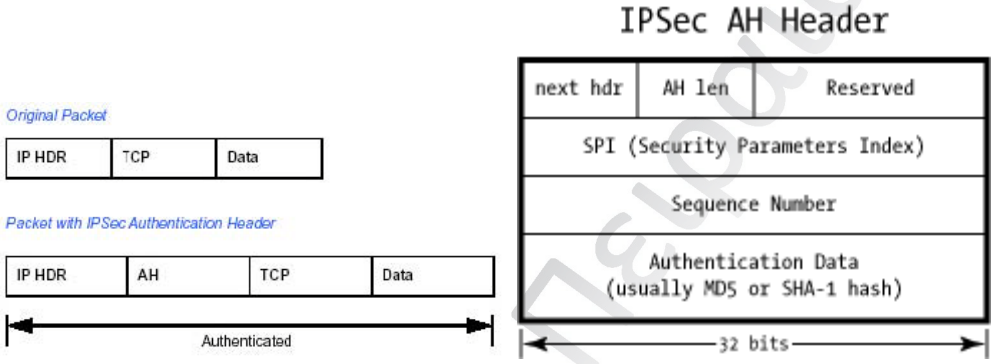
2.5.3 Δομή πρωτοκόλλου IPsec

Το πρωτόκολλο IPsec προσθέτει στο IP πακέτο δύο νέες επικεφαλίδες:

- Μία επικεφαλίδα που χρησιμοποιείται για πιστοποίηση (**Authentication Header - AH**) και
- Μία επικεφαλίδα που χρησιμοποιείται για την ενθυλάκωση της πληροφορίας (**Encapsulating Security Payload – ESP**)

Επικεφαλίδα πιστοποίησης Ταυτότητας

Αυτή η επικεφαλίδα, διασφαλίζει την ακεραιότητα, την πιστοποίηση ταυτότητας των δεδομένων, καθώς και την αποφυγή διπλότυπων πακέτων. Δεν παρέχει ασφάλεια εμπιστευτικότητας. Η ακεραιότητα και η πιστοποίηση πραγματοποιούνται και από τα δύο IPSec μέλη στις άκρες του tunnel εκτελώντας μία συνάρτηση κατακερματισμού στο IP πακέτο χρησιμοποιώντας ένα κοινό κλειδί (Message Authentication Code – MAC). Το αποτέλεσμα του υπολογισμού ο οποίος προκύπτει από τη συνάρτηση κατακερματισμού δεν κρυπτογραφείται και χρησιμοποιείται απλά από το άλλο συμβαλλόμενο μέρος για να ελέγξει ότι τα στοιχεία δεν έχουν τροποποιηθεί.

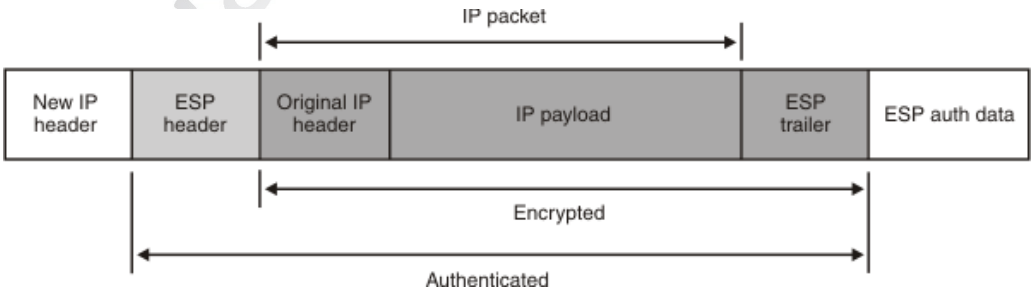


Εικόνα 2.11 Επικεφαλίδα πιστοποίησης ταυτότητας

Το γεγονός αυτό καθ' αυτό της χρησιμοποίησης ενός κοινού μυστικού κλειδιού που είναι γνωστό και στα δύο μέρη (αποστολέας-δέκτης), εγγυάται για την πιστοποίηση της ταυτότητας τους.

Επικεφαλίδα ενθυλάκωσης της πληροφορίας

Αυτή η κεφαλίδα παρέχει υπηρεσίες για την πιστοποίηση και ακεραιότητα των πακέτων IP που διαβιβάζονται μεταξύ δύο IPSec συστημάτων.



Εικόνα 2.12 Επικεφαλίδα ενθυλάκωσης πληροφορίας

Επιπρόσθετα παρέχει εμπιστευτικότητα μέσω μεθόδων κρυπτογράφησης. Η πιστοποίηση και η ακεραιότητα μπορούν να παρασχεθούν με τον ίδιο τρόπο που τα παρέχει και η κεφαλίδα AH. **Το ESP παρέχει εμπιστευτικότητα με την κρυπτογράφησης ενός IP πακέτου**. Το ESP υποστηρίζει ένα μεγάλο αριθμό συμμετρικών αλγορίθμων κρυπτογράφησης, αλλά η εξ ορισμού συνηθισμένη προεπιλογή είναι ο αλγόριθμος AES (128-bit).

Τεχνολογίες κρυπτογράφησης πρωτοκόλλου IPsec

Συνοπτικά αναφέρουμε μερικές από τις τεχνολογίες κρυπτογράφησης όπως:

- Το *κλειδί Diffie-Hellman* για ανταλλαγή μεταξύ δύο σημείων
- Ο αλγόριθμος κρυπτογράφησης DES
- Η ψηφιακή πιστοποίηση Δημοσίων Κλειδιών
- Ο αλγόριθμος Hash

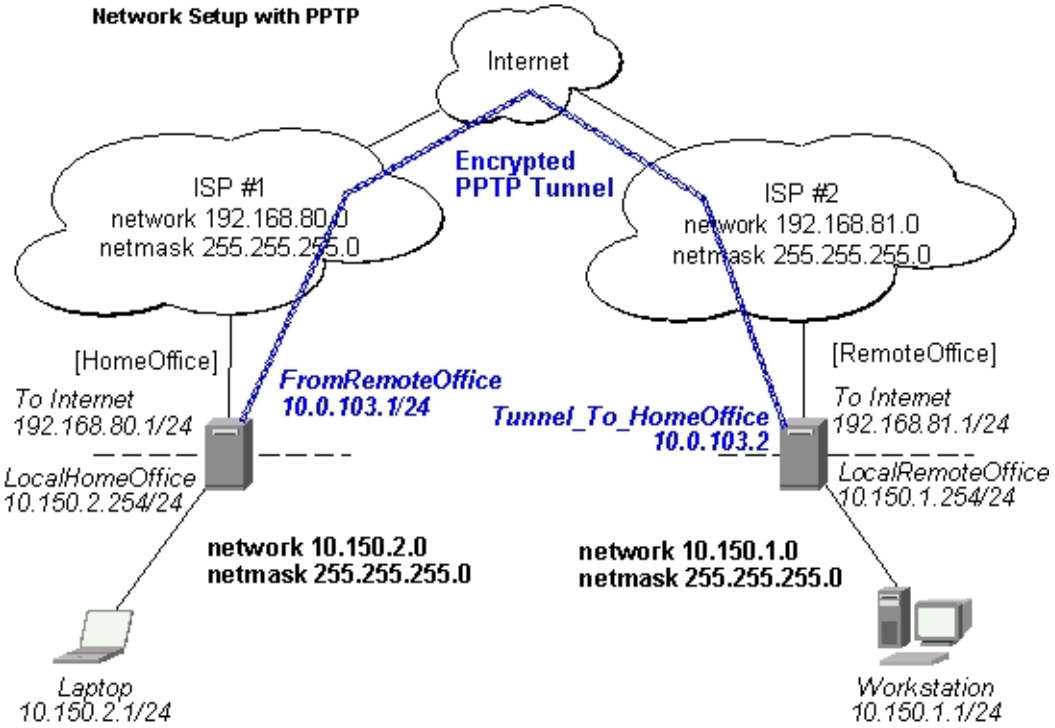
2.5.4 Το πρωτόκολλο PPTP

Ανήκει στην κατηγορία των Ιδιωτικών Εικονικών Δικτύων επιπέδου 2 (Ζεύξης Δεδομένων). Ο σκοπός δημιουργίας του πρωτοκόλλου αυτού, ήταν για την εύκολη και ασφαλή πρόσβαση απομακρυσμένων χρηστών μέσω τοπικού δικτύου ISP.

Όπως είπαμε και προηγουμένως το συγκεκριμένο πρωτόκολλο ανήκει στο δεύτερο επίπεδο ζεύξης δεδομένων του στρώματος O.S.I. και ενθυλακώνει τα κρυπτογραφημένα πακέτα IP μέσω Point To Point πρωτοκόλλων (P.P.P.) πακέτων. Αυτά στην συνέχεια ενθυλακώνονται από ένα ISP Server σε IP πακέτα για την δρομολόγηση τους μέχρι τον προορισμό πάνω από το Διαδίκτυο ή από οποιοδήποτε άλλο δίκτυο στηριζόμενο σε TCP/IP τεχνολογία.

Η πιο συνήθης χρησιμοποίηση του πρωτοκόλλου αυτού είναι για απομακρυσμένη πρόσβαση μέσω ενός τοπικού ISP και η εγκατάσταση μίας PPP σύνδεσης. Στην συνέχεια ξεκινά μία δεύτερη σύνδεση όπου ο στόχος της είναι μία IP διεύθυνση. Αυτή η συγκεκριμένη διεύθυνση ανήκει σε ένα Server PPTP ο οποίος ανήκει μέσα στο δίκτυο με το οποίο θα γίνει η απομακρυσμένη πρόσβαση. Μόλις η σύνδεση επιτευχθεί όλα τα δεδομένα θα ρέουν κρυπτογραφημένα.

Στην παρακάτω εικόνα περιγράφετε αναλυτικά μία επιτυχημένη εγκατάσταση απομακρυσμένης πρόσβασης, του πρωτοκόλλου PPTP που πραγματοποιείτε διαμέσου του διαδικτύου.



Εικόνα 2.13 Εγκατάσταση VPN μέσω πρωτοκόλλου PPTP

Συγκεκριμένα έχουμε ένα φορητό υπολογιστή ο οποίος θέλει να συνδεθεί με το απομακρυσμένο δίκτυο στην δημόσια διεύθυνση **192.168.81.1/24.**

Ο Router του κάθε δικτύου είναι συνδεμένος σε διαφορετικό ISP πάροχο.

Ο Router του πρώτου δικτύου [Home Office] έχει τις εξής διασυνδέσεις:

- Gateway τοπικού δικτύου 10.150.2.254/24
- Gateway με την οποία συνδέετε στο Διαδίκτυο 192.168.80.1/24

Ο Router του Δεύτερου δικτύου [Remote Office] έχει τις εξής διασυνδέσεις:

- Gateway τοπικού δικτύου 10.150.1.254/24
- Gateway με την οποία συνδέετε στο Διαδίκτυο 192.168.81.1/24

Για την δημιουργία μίας ασφαλούς σύνδεσης (Secure Tunnel) προσθέτουμε τον ίδιο κωδικό (user and password) σε ένα group με το όνομα 'ppp' και στους 2 Routers.

Στην συνέχεια δημιουργείτε ένα PPTP TUNNEL μεταξύ των 2 Routers με IP Διευθύνσεις την 10.0.103.1 και την 10.0.103.2 για τον Router [Home Office] και τον Router [Remote Office] αντίστοιχα.

Για την δρομολόγηση των 2 δικτύων μέσω του PPTP TUNNEL χρησιμοποιείται στατική δρομολόγηση μεταξύ τους.

[Home office] > ip route 10.150.1.0 255.255.255.0 10.0.103.2

[Remote office] > ip route 10.150.2.0 255.255.255.0 10.0.103.1

Στην συνέχεια πραγματοποιείται έλεγχος σύνδεσης των 2 Router , μέσω echo πρωτοκόλλου.

[Remote office] > Ping 10.0.103.1 , *ελέγχοντας την PPTP Tunnel σύνδεση*

[Remote office] > Ping 10.150.2.254, *ελέγχοντας την PPTP Tunnel σύνδεση προς την εσωτερική διασύνδεση του Home Office Router.*

2.5.5 Πρωτόκολλο L2F (Cisco Layer 2 Forwarding Protocol)

Είναι ένα πρωτόκολλο, το οποίο παρέχει εικονικές συνδέσεις σε οποιοδήποτε μέρος του διαδικτύου μέσω μη – IP πρωτοκόλλων όπου και εκμεταλλεύεται τα πλεονεκτήματα που του παρέχει το ιντερνέτ.

Οι χρήστες το μόνο που κάνουν είναι να δημιουργήσουν μία PPP σύνδεση (direct σύνδεση), με τον παροχή υπηρεσιών τους και στην συνέχεια να έχουν πρόσβαση στο δίκτυο που θέλουν.

Τα πλεονεκτήματα που μπορούμε να εξάγουμε από το συγκεκριμένο πρωτόκολλο αναλύονται παρακάτω:

- Μπορούν να χρησιμοποιηθούν πρωτόκολλα τα οποία είναι ανεξάρτητα μεταξύ τους όπως
    - Πρωτόκολλα IPX (είναι πρωτόκολλα που χρησιμοποιούνται για την εύρεση της καλύτερης διαδρομής μέσα από ένα IPX δίκτυο, ένα από τα πλεονεκτήματα τους είναι ότι δεν υπάρχει διευθυνσιοδότηση και ορίζονται αυθαίρετα στο δίκτυο)

- Πρωτόκολλα SNA (είναι πρωτόκολλο που δημιουργήθηκε απ0ό την IBM και χρησιμοποιείται για την απομακρυσμένη πρόσβαση)

➢ Πραγματοποιούν Αυθεντικοποίηση των πακέτων

Η διαδικασία αυτή εκτελείται μέσω των

- PPP συνδέσεων
- CHAP πρωτοκόλλων, (ή αλλιώς Challenge Handshake Authentication Protocol), είναι ένα πρωτόκολλο το οποίο χρησιμοποιείται για την αυθεντικοποίηση του χρήστη στο δίκτυο.

Χρησιμοποιείτε κυρίως από τους servers για να πιστοποίηση την αυθεντικότητα των χρηστών που πρόκειται να εισέλθουν στο δίκτυο. Η πιστοποίηση γίνετε με την χρησιμοποίηση της τεχνικής των τριών σημείων χειραψίας (three way handshake).

- TACACS , RADIUS πρωτόκολλα

Είναι πρωτόκολλα που έχουν δημιουργηθεί από την cisco για την προστασία των δικτύων από απομακρυσμένους χρήστες.

Χειρίζονται τις υπηρεσίες authentication, authorization, and accounting services (AAA) = *πιστοποίηση , έγκριση , αυθεντικοποίηση*.

Πιστοποίηση = πραγματοποιείται με την απλή πρόσβαση του χρήστη στο δίκτυο

Έγκριση = είναι η ικανότητα περιορισμού δικτυακών υπηρεσιών ανάλογα με την κατηγορία του χρήστη.

Παρακολούθηση = αποτελεί μία πλήρης παρακολούθηση της κίνησης των χρηστών στο δίκτυο.

TACACS : Terminal Access Controller Access-Control System

Ανήκει στην οικογένεια των πρωτοκόλλων που χρησιμοποιούνται στην απομακρυσμένη πρόσβαση και στον έλεγχο των χρηστών.

Συγκεκριμένα επιτρέπει σε ένα χρήστη να ελέγξει το username και το password του και στην συνέχεια να στείλει ένα query στον TACACS server για πιστοποίηση της αυθεντικότητας του χρήστη.

RADIUS : Remote Authentication Dial In User Service

Είναι ένα πρωτόκολλο το οποίο ανήκει στην ίδια οικογένεια με τα TACACS πρωτόκολλα. Χρησιμοποιείται για πιστοποίηση των χρηστών και αυθεντικοποίηση τους μέσω απομακρυσμένης πρόσβασης.

Η επικοινωνία για την πιστοποίηση της αυθεντικότητας των χρηστών γίνετε από radius clients οι οποίοι επικοινωνούν με radius servers

Radius servers : παρέχουν υπηρεσίες πιστοποίησης και αυθεντικότητας προς radius clients.

Radius clients : είναι στην ουσία NAS (Network Access Server) οι οποίοι χρησιμοποιούν όλες τις θύρες τους , για τον έλεγχο τις πρόσβασης των χρηστών στο δίκτυο.

- Διαχείριση διευθύνσεων
- Δυναμικά και ασφαλή tunnels
- Υπηρεσίες χρέωσης (accounting)
- Έλεγχος ροής (επιβεβαίωση λήψης πακέτων από παραλήπτη, πριν την αποστολή των επόμενων πακέτων)

Συνοψίζοντας, μπορούμε να χωρίζουμε την διαδικασία πιστοποίησης αυτού του πρωτοκόλλου στα εξής σταδία

Πρώτο στάδιο

Ο χρήστης πραγματοποιεί μία PPP σύνδεση με τον ISP πάροχο υπηρεσιών του.

Δεύτερο στάδιο

Ο Network access server ή αλλιώς radius client δημιουργεί ένα tunnel με τον radius server. Για να μπορέσει ο radius server να δώσει IP διεύθυνση στον εξωτερικό χρήστη θα πρέπει να γίνει πιστοποίηση από το σύστημα του, μέσω username και password.

2.5.6 Πρωτόκολλο L2TP (Layer 2 Tunnelling Protocol)

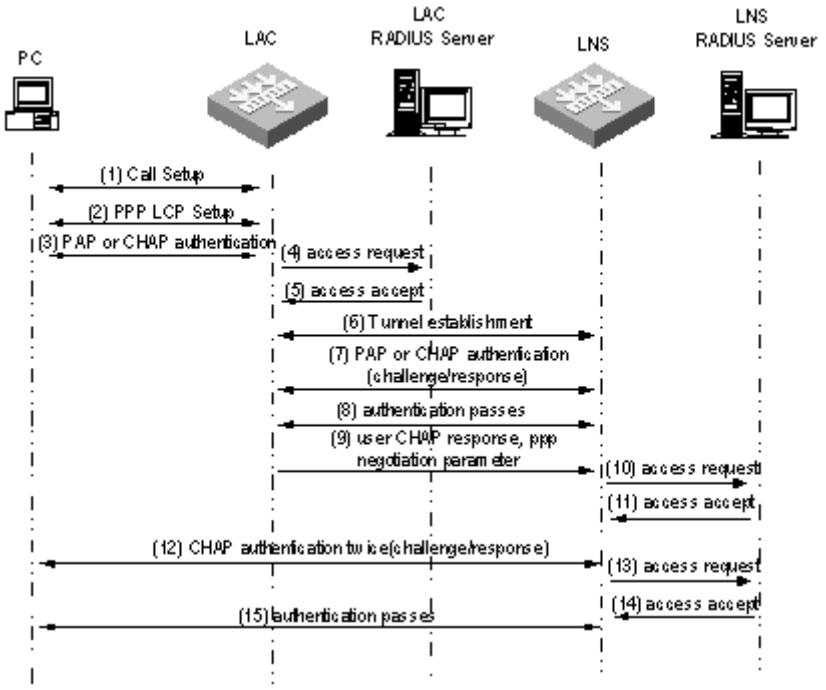
Το L2TP είναι δημιούργημα της ένωσης του PPTP και του L2F. το οποίο ορίστηκε για λόγους συμβατότητας όλων των δικτύων μεταξύ τους. Το L2TP χρησιμοποιεί πολλά χαρακτηριστικά του IPSec για να επιτύχει μεγαλύτερη ασφάλεια. Μπορεί να παρέχει υπηρεσίες δεύτερου (ζεύξης δεδομένων) αλλά και τρίτου (διαδικτύου) επιπέδου. Το L2TP χρησιμοποιεί δύο servers για τη σύνοδο:

• τον **LAC (L2TP Access Concentrator)** – είναι ένας server ο οποίος βρίσκεται στον ISP πάροχο και χρησιμοποιείται για την εγκαθίδρυση μίας διόδου σε ένα δημόσιο δίκτυο το οποίο μπορεί να είναι είτε PSTN, ISDN, τα οποία τερματίζονται στον LNS Server ο οποίος αποτελεί και τον κόμβο προορισμού.

• τον **LNS (L2TP Network Server)** – είναι ένας server ο οποίος βρίσκεται στον κόμβο προορισμό και χρησιμοποιείται για τον τερματισμό του tunnel. Ο LNS είναι ο Server εκείνος, ο οποίος Αναλαμβάνει την αυθεντικοποίηση του χρήστη. Όταν ο LNS λαμβάνει αιτήματα για συνδέσεις, από έναν LAC Server, αυθεντικοποιεί τον κάθε χρήστη και εγκαθιδρύει το tunnel μεταξύ του LAC Server.

Στη δίοδο που δημιουργείται μεταξύ του Access Concentrator (LAC) και του Network Server (LNS), μπορούν να υπάρχουν ταυτόχρονα πολλές σύνοδοι (επικοινωνίες): κάθε σύνοδος έχει ένα δικό της μοναδικό αριθμό Call ID, που υπάρχει στην επικεφαλίδα κάθε L2TP πακέτου. Μπορούν επίσης να υπάρχουν ταυτόχρονα πολλές διαφορετικές δίοδοι μεταξύ του ίδιου Access Concentrator και του Access Server. Η κάθε μία τότε μπορεί να ικανοποιεί διαφορετικό υπηρεσίες Q.O.S. .

Όπως και στο PPTP, η αρχική σύνδεση του χρήστη με τον LAC (ο οποίος παίζει το ρόλο που έχει ο NAS στο PPTP) γίνεται με χρήση του PPP, μέσω του οποίου ενθυλακώνονται διαφόρων ειδών πακέτα (Apple Talk, IP, IPX και NETBEUI) και πραγματοποιείται μία πρώτη αυθεντικοποίηση του χρήστη (με PAP ή CHAP). Μία δεύτερη πιστοποίηση της ταυτότητας του χρήστη λαμβάνει χώρα αμέσως μετά, με χρήση του RADIUS. Επίσης, μία άλλη αναλογία του L2TP με το PPTP είναι τα δύο είδη μηνυμάτων που μπορεί να ανταλλάσσονται: μηνύματα ελέγχου και μηνύματα δεδομένων. Τέλος, όπως και στο PPTP, ένα VPN που υλοποιείται με βάση το L2TP μπορεί να υποστηρίζει τόσο αυθόρμητες (voluntary) όσο και αναγκαστικές (compulsory) διόδους.



Εικόνα 2.14 Στάδια εγκατάστασης L2TP συνόδου

Τα στάδια που ακολουθούνται για τη δημιουργία μίας L2TP διόδου είναι τα ακόλουθα:

Στάδιο 1: Ο απομακρυσμένος χρήστης συνδέεται με τον LAC του ISP με χρήση του πρωτοκόλλου PPP.
Ο LAC αυθεντικοποιεί τον χρήστη, με βάση το user name και password του. Στη συνέχεια, ο LAC προσδιορίζει την IP διεύθυνση του LNS που ανήκει στο LAN για το οποίο ο χρήστης αιτείται σύνδεση. Μεταξύ LAC και LNS, η σύνοδος L2TP ξεκινά.
Στάδιο 2: Μετά την εκκίνηση της L2TP συνόδου, ξεκινά η αυθεντικοποίηση του χρήστη στον LNS. Μπορεί να χρησιμοποιηθεί οποιοσδήποτε τυποποιημένος αλγόριθμος αυθεντικοποίησης, π.χ. CHAP (Challenge Handshake Authentication Protocol). Όπως στα πρωτόκολλα PPTP και L2F, το L2TP δε θέτει περιορισμό για αλγόριθμο αυθεντικοποίησης. Ωστόσο, στην πράξη, έχει προτιμηθεί κυρίως η αυθεντικοποίηση με χρήση του RADIUS.

Στάδιο 3: Μετά από επιτυχή αυθεντικοποίηση, μπορεί να δημιουργηθεί ένα προστατευμένο tunnel μεταξύ LAC και LNS. Το L2TP δεν προσδιορίζει ρητά μεθόδους για την κρυπτογράφηση. Ωστόσο, για διόδους (tunnels) πάνω σε IP δίκτυα, μπορεί να χρησιμοποιηθεί το πρωτόκολλο IPSec.

Τότε το L2TP ενθυλακώνεται σε UDP πακέτα που μεταφέρονται μεταξύ LAC και LNS μέσω IPSec tunnel. Συνήθως η πόρτα που χρησιμοποιείται για την μεταφορά των udp πακέτων είναι η 1701, ωστόσο για λόγους ασφάλειας **Ο Διαχειριστής του δικτύου,** επιβάλετε να αλλάξει την αρίθμηση της συγκεκριμένης πόρτας για να αποφύγει τις default επιθέσεις που πιθανών να υπάρξουν.

Στην αναγκαστική δίοδο, ο χρήστης στέλνει PPP πακέτα στον LAC και η δημιουργία διόδου μεταξύ του LAC και του LNS του απομακρυσμένου δικτύου γίνεται χωρίς την εξουσιοδότηση του χρήστη.

Σε IP δίκτυα, για την μεταφορά των δεδομένων από τον χρήστη στον ISP πάροχο γίνετε μέσω των IPsec πρωτοκόλλων, καθώς αποτελεί την καλύτερη επιλογή για τον χρήστη στέλνοντας κρυπτογραφημένα τα δεδομένα. Το AH προστίθεται από τον LAC του ISP στην επικεφαλίδα των προς αποστολή πακέτων . Η ESP επικεφαλίδα προστίθεται μόνο όταν ο LNS στον προορισμό υποστηρίζει το IPSec πρωτόκολλο. Το κλειδί κρυπτογράφησης που χρησιμοποιείται είναι συμμετρικό (IKE).

Το (IKE), είναι ένα πρωτόκολλο που χρησιμοποιείται για να εγκαταστήσει την σύνδεση μέσω IPsec , αφού πρώτα δημιουργήσει ένα ασφαλές κανάλι μεταξύ των 2 οντοτήτων που πρόκειται να συνδεθούν.

Στην αυθόρμητη δίοδο, το AH εφαρμόζεται κατευθείαν στο πακέτο που στέλνετε από τον χρήστη προς τον ISP πάροχο. Αν ο LNS δεν υποστηρίζει IPSec, τότε το ESP προστατεύει τα δεδομένα μέχρι να φτάσουν στον LNS Server.

2.6 Μετάφραση διευθύνσεων δικτύου (NAT) – (NAPT)

NAT

Για να μπορέσουμε να ικανοποιήσουμε έναν μεγάλο αριθμό συσκευών στο Διαδίκτυο, οι κοινότητα του Διαδικτύου όρισε μία <<Τεχνική>> κατά την οποία η κάθε συσκευή που ανήκει σε μία ομάδα συσκευών που υπάρχουν σε ένα εσωτερικό δίκτυο για την επικοινωνία τους με τα εξωτερικά δίκτυα που ανήκουν στον ευρύτερο χώρο του διαδικτύου, να μπορούν να μπορούν να μοιράζονται μια κοινή διεύθυνση IP μειώνοντας με αυτό τον τρόπο το κόστος χρησιμοποίησης τους.

Η NAT επιτρέπει σε μια τοποθεσία του Internet να έχει μια μοναδική έγκυρη διεύθυνση IP, πολλούς υπολογιστές, και καμία σύγκρουση σε επίπεδο διεύθυνσης. Το μυστικό της τεχνολογίας NAT για την αποφυγή των συγκρούσεων είναι ότι εκχωρεί σε κάθε υπολογιστή μια τοπικά μοναδική διεύθυνση. Οι διευθύνσεις αυτές, λέγονται *ιδιωτικές*, πράγμα που σημαίνει ότι δεν ισχύουν στο internet. Για παράδειγμα, η διεύθυνση 10.0.0.0/8 έχει δεσμευθεί ως ιδιωτική διεύθυνση, επομένως στην τοποθεσία αυτή μπορούν να εκχωρούνται διευθύνσεις από την 10.0.0.0. Επιπλέον, οι δρομολογητές που βρίσκονται στην τοποθεσία είναι διευθετημένοι ώστε να προωθούν τα αυτοδύναμα πακέτα τα οποία περιέχουν τις τοπικές διευθύνσεις. Πριν επιτραπεί σε ένα αυτοδύναμο πακέτο να σταλεί στο Internet, η NAT θα πρέπει να μεταφράσει την ιδιωτική διεύθυνση IP σε μια Δημόσια διεύθυνση IP, η οποία είναι αναγνωρίσιμη από το ιντερνέτ. Με την ίδια λογική, η NAT μεταφράζει τη διεύθυνση προορισμού IP σε κάθε εισερχόμενο αυτοδύναμο πακέτο από τη διεύθυνση που χρησιμοποιείται στο παγκόσμιο Ιστό (ιντερνέτ) σε μια ιδιωτική διεύθυνση που χρησιμοποιείται τοπικά.

Η τεχνολογία NAT χρησιμοποιείται κυρίως σε Routers η οποίοι βρίσκονται στην κορυφή του δικτύου (border routers) και επικοινωνούν απευθείας με το Διαδίκτυο. Οι routers αυτή η οποίοι περιέχουν το λογισμικό NAT λέγονται SOHO Routers και χρησιμοποιούνται σε μικρού όγκου οικιακά κυρίως δίκτυα. Σε μεγαλύτερα Δίκτυα ,όπως για παράδειγμα Δίκτυα επιχειρήσεων χρησιμοποιούνται συσκευές NAT για αυτό το σκοπό.

Η NAT, επεξεργάζεται κάθε πακέτο που εισέρχεται ή εξέρχεται από την τοποθεσία. Για παράδειγμα, μια τοποθεσία έχει την διεύθυνση IP, 128.210.24.6, και χρησιμοποιεί ιδιωτικές διευθύνσεις την 10.0.0.0/8. Αν ένας υπολογιστής στην τοποθεσία με ιδιωτική διεύθυνση 10.0.0.1 στείλει ένα αυτοδύναμο πακέτο στο Internet με προορισμό τη διεύθυνση 128.211.134.4, το αυτοδύναμο πακέτο περνάει από τις εξής τροποποιήσεις:

Διεύθυνση αφετηρίας πακέτου : 10.0.0.1

Διεύθυνση προορισμού : 128.211.134.4

10.0.0.1 --------> (NAT) ---------> 128.210.24.6 ----> (Internet) ----> 128.211.134.4

10.0.0.1 <-------- (NAT) <--------- 128.210.24.6 <---- (Internet) <---- 128.211.134.4

Στο παραπάνω σχήμα η NAT μετατρέπει τη διεύθυνση αφετηρίας (10.0.0.1) στην διεύθυνση (128.210.24.6) και την στέλνει στην διεύθυνση 128.211.134.4. Η NAT πρέπει να ξαναγράψει τη διεύθυνση προορισμού ώστε να αντιστοιχεί στη σωστή ιδιωτική διεύθυνση, πριν προωθήσει το αυτοδύναμο πακέτο στην τοποθεσία. Η ίδια ακριβώς διαδικασία παρατηρείται και στην αντίθετη περίπτωση.

Η NAT για να μπορεί να αναγνωρίζει και να θυμάται όλα τα πακέτα που εισέρχονται και εξέρχονται από το δίκτυο χρησιμοποιεί ένα *πίνακα μετάφρασης*, όπου αποθηκεύει σε αυτόν όλες τις εξερχόμενες και εισερχόμενες κινήσεις.

Κατεύθυνση	**Πεδίο**	**Παλιά τιμή**	**Νέα τιμή**
Εξερχόμενη	Αφετηρία	10.0.0.1	128.10.24.6
Εισερχόμενη	Προορισμός	128.10.24.6	10.0.0.1

Πίνακας 2.6 Πίνακας μετάφρασης διευθύνσεων (NAT)

Συνήθως οι τοποθετήσεις των τιμών πραγματοποιούνται αυτόματα από την ίδια την NAT.

NAPT

Η NAT είναι μία τεχνική η οποία δεν μπορεί να πραγματοποιηθεί όταν στην συγκεκριμένη τοποθεσία ενός εσωτερικού δικτύου 2 ή περισσότεροι υπολογιστές θέλουν να συνδεθούν με μία συγκεκριμένη Ιδιωτική διεύθυνση IP. Το παραπάνω πρόβλημα αντιμετωπίζετε από μια πληρέστερη έκδοση της NAT, η οποία επιτρέπει σε μια τοποθεσία να διαθέτει έναν απεριόριστο αριθμό εφαρμογών που εκτελούνται σε οποιουσδήποτε υπολογιστές, και επικοινωνούν όλες με απεριόριστους προορισμούς στο Internet. Ο μηχανισμός αυτός ονομάζετε NAPT (*μετάφραση δικτυακών διευθύνσεων και Θυρών).*

Εκτός των διευθύνσεων IP η NAPT μετατρέπει και αριθμούς θυρών πρωτοκόλλου. Επειδή καταλαβαίνει τους αριθμούς θυρών, η NAPT μπορεί να συσχετίσει σωστά κάθε αυτοδύναμο πακέτο με μια σύνδεση TCP ή με μια σύνοδο UDP. Δηλαδή, η NAPT λειτουργεί σε επίπεδο συνδέσεων μεμονωμένων μεταφορών και όχι υπολογιστών. Το αποτέλεσμα είναι ότι ο πίνακας μετάφρασης που χρησιμοποιείται από τη NAPT πρέπει να περιέχει τόσο τις διευθύνσεις IP όσο και τους αριθμούς θυρών πρωτοκόλλου.

Για παράδειγμα, σκεφθείτε τον πίνακα μετάφρασης που μπορεί να προκύψει αν ένας browser στον υπολογιστή 10.0.0.1 και ένας browser στον υπολογιστή 10.0.0.2 χρησιμοποιούν ταυτόχρονα την τοπική θύρα 30000, και διαμορφώσουν και οι δύο μια σύνδεση TCP με ένα Server του Παγκόσμιου Ιστού στη θύρα 80 μέσω μιας συσκευής NAPT η οποία χρησιμοποιεί τη διεύθυνση 128.10.19.20. Για να αποφευχθεί η σύγκρουση, η NAPT θα πρέπει να διαλέξει μια εναλλακτική θύρα αφετηρίας TCP για μία από τις δύο συνδέσεις. Μια πιθανή λύση φαίνεται στην παρακάτω Εικόνα.

Κατεύθυνση	**Πεδίο**	**Παλιά τιμή**	**Νέα τιμή**
Προς τα έξω	**ΑΦΕΤ IP: ΑΦΕΤ TCP**	**10.0.0.1 : 30000**	**128.10.19.20:40001**
Προς τα έξω	**ΑΦΕΤ IP: ΑΦΕΤ. TCP**	**10.0.0.2 : 30000**	**128.10.19.20:40002**
Προς τα μέσα	**ΠΡΟΟΡ IP: ΠΡΟΟΡ TCP**	**128.10.19.20:40001**	**10.0.0.1 : 30000**
Προς τα μέσα	**ΠΡΟΟΡ IP: ΠΡΟΟΡ TCP**	**128.10.19.20:40002**	**10.0.0.2 : 30000**

Πίνακας 2.7 Πίνακας μετάφρασης διευθύνσεων (NAPT)

Επειδή η NAPT μπορεί να αντιστοιχίζει αριθμούς θυρών TOP, έχει τη δυνατότητα να επεκταθεί ώστε να υποστηρίζει και *συνένωση TCP*. Με άλλα λόγια, μπορεί να σχεδιαστεί μια συσκευή που αρχικά δημιουργεί δύο διαφορετικές συνδέσεις TCP, τις οποίες και στη συνέχεια συνενώνει μέσω μετάφρασης πρωτοκόλλου. Όταν ένα αυτοδύναμο πακέτο που μεταφέρει ένα τμήμα TCP φτάνει από τη μία σύνδεση, η συσκευή συνένωσης ξαναγράφει τα πεδία της κεφαλίδας και στέλνει το αυτοδύναμο πακέτο με την άλλη σύνδεση. Τα δύο ακραία σημεία της επικοινωνίας αλληλεπιδρούν στέλνοντας δεδομένα και λαμβάνοντας επιβεβαιώσεις, χωρίς να γνωρίζουν ότι ένα ενδιάμεσο σύστημα πραγματοποιεί συνένωση. Για να κάνει τη διασύνδεση διάφανη, μια συσκευή συνένωσης TCP πρέπει να αντιστοιχίζει την ακολουθία του TCP και τις τιμές των επιβεβαιώσεων, όπως επίσης και τους αριθμούς θυρών.

2.7 Η διεύθυνση IPV6

όσο συνεχίζετε η εξάπλωση του Διαδικτύου και η εισχώρηση όλο και περισσότερων ασύρματων συσκευών (tablet's , smartphones, παιχνιδομηχανές , Web T.V.) οι διευθύνσεις IP, οι οποίες καλύπτονται από την τέταρτη έκδοση (IPV4) αρχίζουν ολοένα και λιγοστεύουν με αποτέλεσμα μετά από μερικά χρόνια να υπάρχει έλλειψη σε αυτές.

Εκτός από το πρόβλημα που έχει παρουσιαστεί στις IPV4 διευθύνσεις σε σχέση με το πλήθος τους, υπάρχουν και άλλα σημαντικά προβλήματα στα οποία το συγκεκριμένο είδος διευθύνσεων δεν μπορεί να ανταποκριθεί σε αυτά.

Ενδεικτικά αναφέρουμε μερικά από τα προβλήματα της IPV4 διεύθυνσης

- Δύσκολη διαχείριση
- Μη αποδοτική δρομολόγηση
- Quality of Service
- Ασφάλεια
- Δύσκολη η ταυτόχρονη χρήση περισσότερων της μιας προσθηκών του IPv4 (QoS, IPsec, Mobile IP, etc.)

Μερικές από τις λύσεις που προσφερθήκαν ανά τακτά χρονικά διαστήματα

- IPv4 routing : μεγάλες λίστες στους δρομολογητές
- Subnetting : Χρήση subnet masks
- CIDR: Συνένωση υποδικτύων
- DHCP: Auto configuration, Απαιτεί ρητή αρχικοποίηση DHCP server
- TOS: Πεδίο για παροχή ποιότητας υπηρεσίας
- IPsec : Υλοποίηση μηχανισμών ασφάλειας στο IPv4
- NAT: Ένα Υποδίκτυο δεν δεσμεύει εσωτερικά μοναδικές IP διευθύνσεις, αλλά γίνεται χρήση ενός μεσολαβητή που μεταφράζει τις διευθύνσεις του υποδικτύου σε μοναδικές διευθύνσεις διαδικτύου, επιτρέποντας την έμμεση επικοινωνία με το διαδίκτυο

Η τεχνολογία NAT όμως εκτός από τα πλεονεκτήματα που φαίνονται από πρώτη ματιά , παρουσιάζει και μερικά μειονεκτήματα

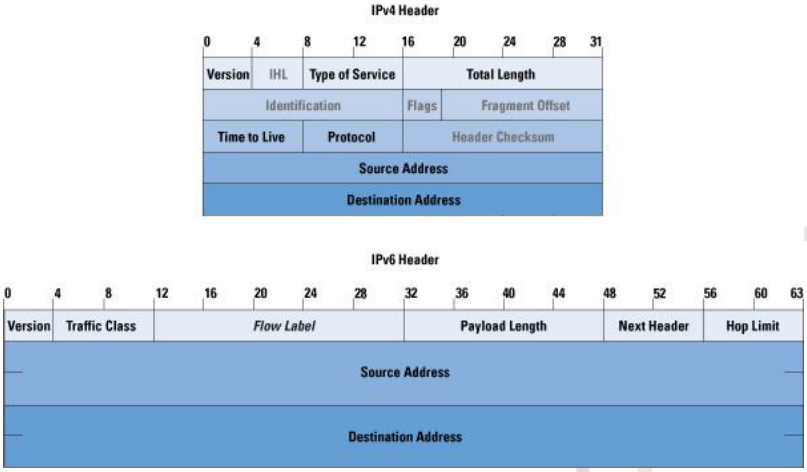
- Προκαλεί μείωση στην απόδοση του NAT δρομολογητή με την συνεχή τροποποίηση των διευθύνσεων
- Δεν λειτουργεί σε πρωτόκολλα ανώτερου επιπέδου τα οποία ο NAT δρομολογητής δεν γνωρίζει ή περιέχουν κρυπτογραφημένα μηνύματα
- Δεν επικοινωνεί με την χρήση back – up δρομολογητή

2.7.1 Πλεονεκτήματα IPV6

Η IPV6 πρόκειται για ένα είδος διεύθυνσης το οποίο έχει σχεδιαστεί έτσι ώστε να καλύπτει τα προβλήματα που έχουν δημιουργηθεί από τον προκάτοχο του (IPV4).

- Ο χώρος των διευθύνσεων αυξάνετε από 32 bit σε 128 , πολλαπλασιάζοντας το πλήθος των χρηστών.
- Η επικεφαλίδα του είναι πιο απλοποιημένη καθώς έχει λιγότερα πεδία , το οποίο βοηθά σημαντικά στο κόστος δρομολόγησης για το κάθε πακέτο και του κόστους σε εύρος ζώνης που καταναλώνετε από κάθε επικεφαλίδα.
- Παρουσιάζει καλύτερες επιλογές ως προς την πληθώρα των επεκτάσεων στην επικεφαλίδα που μπορούν να προστεθούν.
- Έχει την δυνατότητα να μπορεί να ελέγχει την ροή κίνησης για σκοπούς όπως για παράδειγμα την διαχείριση εύρους ζώνης του δικτύου. Η χρήση του ακόμα βρίσκετε σε πειραματικό στάδιο. Το Flow Label πρόκειται στην πραγματικότητα για ένα το οποίο παράγετε για την ιεράρχηση των πακέτων , όπου η πραγματική ιεράρχηση γίνετε στους δρομολογητές κατά την διαδρομή των πακέτων. Ένα από τα μειονεκτήματα αυτού του πεδίου είναι ότι οι δρομολογητές ακόμα δεν το χρησιμοποιούν με αποτέλεσμα το Q.O.S.(Quality Of Service) να είναι το ίδιο με το IPV4.
- Παρουσιάζουν καλύτερες δυνατότητες ασφάλειας όπως Αυθεντικοποίηση και Ιδιωτικότητα (IPsec).
- Δεν υποστηρίζουν την τεχνολογία NAT. Στηρίζονται μόνο στο μοντέλο τον end – to end συνδέσεων.

- Οι IPv6 διευθύνσεις μπορούν να μεταφέρονται μέσω του ήδη υπάρχοντος δικτύου, δηλαδή να μπορούν να ενθυλακώνονται μέσα σε IPv4 διευθύνσεις.



Εικόνα 2.15 Η δομή της IPv4 και της IPv6 διεύθυνσης

2.7.2 Επικεφαλίδες IPV6 διευθύνσεων

Χρησιμοποιούνται κυρίως για να παρακάμψουν την ήδη πολιτική ασφαλείας που εφαρμόζετε στις συγκεκριμένες διευθύνσεις. Διακρίνονται σε:

Επικεφαλίδες επέκτασης

Hop – by Hop Header χρησιμοποιείται από όλους τους στους οποίους περνάει ένα πακέτο κατά την διάρκεια της διαδρομής του. Περιέχει όλες τις πληροφορίες εκείνες που θα πρέπει να εξετάζονται από κάθε κόμβο κατ μήκος της διαδρομής του πακέτου.

Επικεφαλίδες Routing

Οι επικεφαλίδες Routing χρησιμοποιούνται από την πηγή που προέρχεται το πακέτο με σκοπό να τοποθετήσει μία λίστα στην επικεφαλίδα του οι οποία θα αναγράφει τους κόμβους στους οποίους το πακέτο θα πρέπει να περάσει από αυτούς κατά την διαδρομή του.

Επικεφαλίδα κατακερματισμού

Χρησιμοποιείται από την πηγή για να στείλει πακέτα μεγαλύτερα από την μέγιστη μονάδα μετάδοσης ενός μονοπατιού.

Η διάσπαση του πακέτου γίνετε μόνο από την πηγή και όχι από τους δρομολογητές που βρίσκονται πάνω στην διαδρομή. Ο μόνος έλεγχος που πραγματοποιείται από τους δρομολογητές είναι ότι σε περίπτωση όπου τα πακέτα είναι πολύ μεγάλα στέλνουν ICMP πακέτα προς τον χρήστη με την φράση «packet too big».

Επικεφαλίδα προορισμού

Περιέχει προαιρετικές πληροφορίες που εξετάζονται μόνο από τους κόμβους προορισμού.

Επικεφαλίδα Αυθεντικοποίησης

Είναι μία επικεφαλίδα η οποία μπορεί να επιβεβαιώσει την αυθεντικότητα προέλευσης των δεδομένων και να προστατεύση τον προορισμό από τυχόν επαναλήψεις των πακέτων (anti-replay protection)

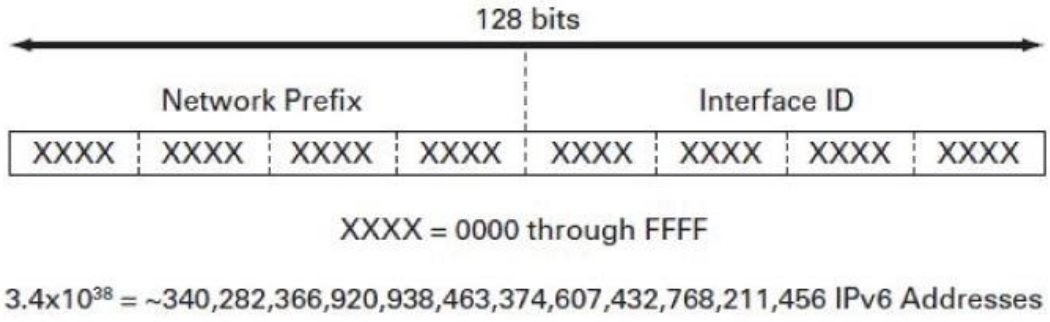
Επικεφαλίδα Κρυπτογράφησης

Παρέχει εμπιστευτικότητα ως προς τα δεδομένα, επιβεβαιώνει την αυθεντικότητα προέλευσης των δεδομένων, προστατεύει από τυχόν επαναλήψεις και παρέχει μία περιορισμένη εμπιστευτικότητα της ροής κίνησης των πακέτων.

2.7.3 Δομή της IPV6 διεύθυνσης

Network Prefix

Το πρώτο μισό μίας διεύθυνσης, δηλαδή τα πρώτα 64 bits, αποτελεί το **Network Prefix**. Είναι το αντίστοιχο του **Network Address του IPv4**.



Εικόνα 2.16 Η δομή της IPv6 διεύθυνσης

Σε αυτό το prefix εφαρμόζονται οι διευθύνσεις:

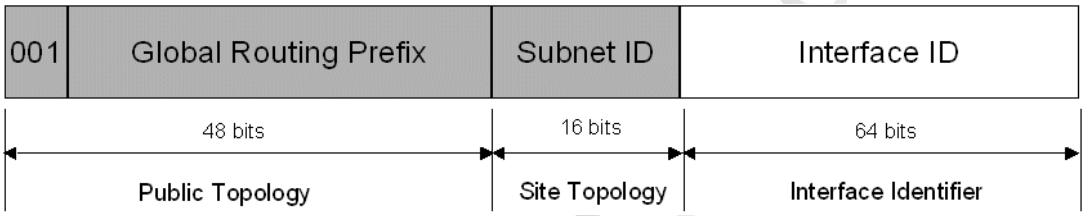
Global unicast,

site - local και

link – local.

Global Unicast Διευθύνσεις

Οι διευθύνσεις Global Unicast, είναι αντίστοιχες Internet διευθύνσεις του IPv4. Είναι οι διευθύνσεις των οποίων τα πρώτα 3 bits είναι τα 001 (εκφρασμένα σε bits και όχι σε δεκαδική μορφή). Οι διευθύνσεις αυτές διανέμονται από τον οργανισμό IANA στους ISPs, τα ιδρύματα και τους οργανισμούς.



Εικόνα 2.17 Η Global Unicast διεύθυνση

Ένας ISP πάροχος υπηρεσιών μπορεί να δώσει μία διεύθυνση με routing global prefix που θα κινείται από /48 εύρος μέχρι /64 εύρος. Η απόφαση για το εύρος που θα δοθεί είναι στην κρίση του κάθε ISP παρόχου. Ανάλογα με τα prefix που θα δοθούν θα έχουμε και ένα εύρος από 0 έως 16 bit για τον καταμερισμό των subnets. Για παράδειγμα να μία διεύθυνση **έχει 0 bit**, τότε θα υπάρχει **μόνο ένα subnet.**

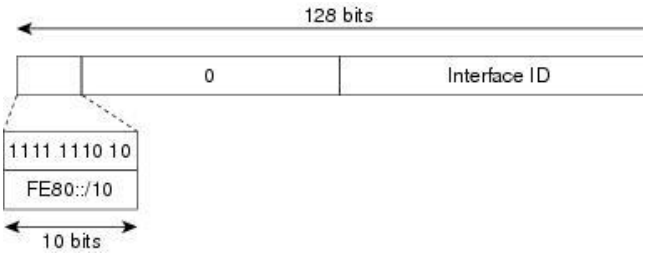
Link-Local Διευθύνσεις

Οι διευθύνσεις που ξεκινούν με **FE** και το τρίτου δεκαεξαδικό ψηφίο **είναι 8 έως το B** ανήκουν στην κατηγορία των link - local διευθύνσεων. Οι διευθύνσεις αυτές έχουν επίσης τοπική σημασία, αλλά δεν μπορούν ποτέ να δρομολογηθούν, ακόμα και μεταξύ ιδιωτικών δικτύων.

Οι link – local διευθύνσεις χρησιμοποιούνται κυρίως για τα τοπικά υποδίκτυα και είναι διευθύνσεις που χρησιμοποιούν την τεχνική του auto – configuration.

Οι router’s δεν προωθούν πακέτα τα οποία περιέχουν link – local διευθύνσεις.

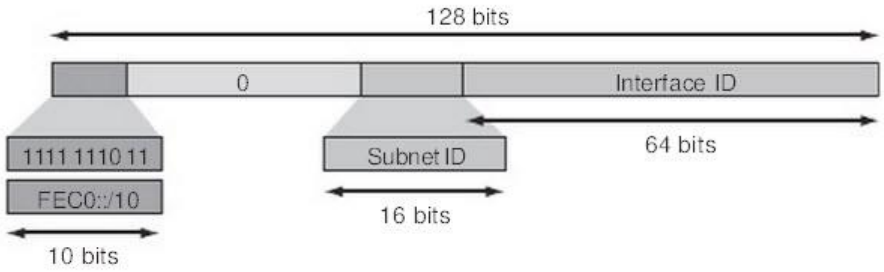
Στις IPv6 διευθύνσεις έχουν καταχωρηθεί με το πρόθεμα **fe80::/10.**



Εικόνα 2.18 Η link local διεύθυνση

Οι site – local Διευθύνσεις

Οι διευθύνσεις site – local, είναι οι διευθύνσεις που ξεκινούν με **FE** και το τρίτου δεκαεξαδικό ψηφίο είναι **C έως το F**. Αποτελούν το ακριβές αντίστοιχο των **Private διευθύνσεων του IPv4**.



Εικόνα 2.18 Η on site local διεύθυνση

Οι διευθύνσεις αυτές εφαρμόζονται στο ίδιο υπόδικτυο, προσδιορίζοντας την διεύθυνση θέσης του χρήστη.

Interface ID

Το υπόλοιπο μισό, δηλαδή τα τελευταία 64 bits αποτελούν το Host ID και προσδιορίζουν μονοσήμαντα έναν host σε ένα δίκτυο.

Απόδοση διευθύνσεων στους Host's

Η απόδοση των IP διευθύνσεων σε έναν host μπορεί να γίνει με 4 διαφορετικούς τρόπους

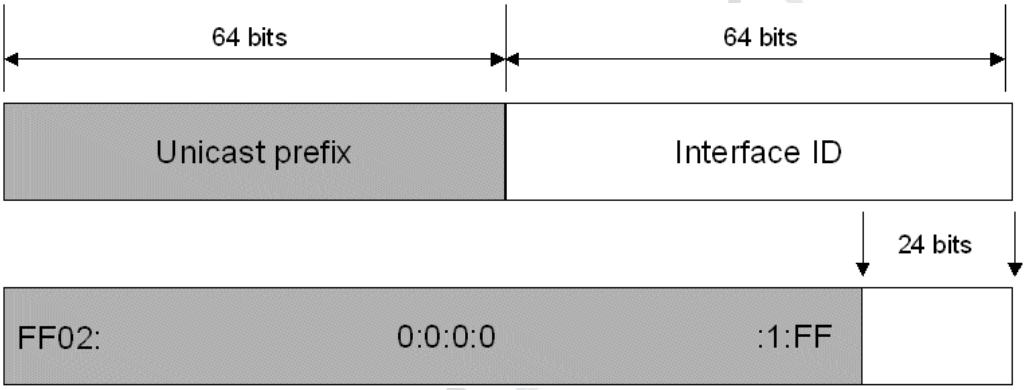
- Πληκτρολογώντας σε κάθε host μία μοναδική στο Δίκτυο Διεύθυνση.
- Χρησιμοποιώντας την τεχνική EUI-64, όπου σε αυτή την περίπτωση εισάγουμε μόνο το network prefix και στην συνέχεια το host ID εξάγετε αυτόματα και συμπληρώνετε με βάση την MAC address του υπολογιστή.

- Χρησιμοποιώντας την State less αυτόματη απόδοση διεύθυνσης.
- Χρησιμοποιώντας ένα DHCPv6 server που θα μοιράζει διευθύνσεις και άλλες ρυθμίσεις (DNS Server, gateways, κλπ) στους hosts του δικτύου.

2.7.4 Διευθυνσιοδότηση σε IPV6

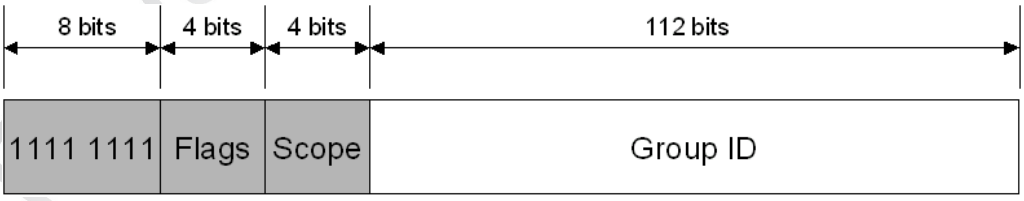
Η διεύθυνση στο IPV6 χωρίζετε σε 3 τύπους διευθύνσεων

- **Unicast :** είναι η διεύθυνση η οποία στηρίζετε στην κλασσική p2p επικοινωνία. Η διεύθυνση αυτή αντιπροσωπεύει ένα **συγκεκριμένο interface**. Ένα πακέτο που στέλνετε σε μία unicast διεύθυνση παραδίδετε στην διεπαφή αυτή προσδιοριζόμενο από αυτή την διεύθυνση.



Εικόνα 2.19 Η Unicast διεύθυνση

- **Multicast:** η διεύθυνση αυτή αντιπροσωπεύει ένα σύνολο από interfaces (**που συνήθως ανήκουν σε διαφορετικούς κόμβους**). Ένα πακέτο που στέλνετε σε μία multicast διεύθυνση παραδίδετε σε όλες τις διεπαφές (**one to many**) που προσδιορίζονται από αυτή την διεύθυνση. Συνήθως χρησιμοποιούνται από host's και router's οι οποίοι τις Data – link διευθύνσεις των γειτονικών τους συσκευών.

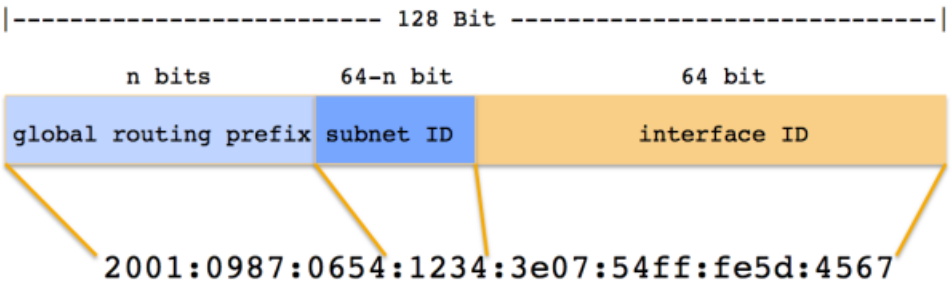


Εικόνα 2.20 Η Multicast διεύθυνση

Flags

- όταν έχει την τιμή 1 πρόκειται για μία παροδική διεύθυνση που δεν είναι μόνιμα καταχωρημένη.
- όταν έχει την τιμή 0 πρόκειται για μία multicast διεύθυνση που απεικονίζετε με μόνιμο τρόπο

➢ **Anycast:** η διεύθυνση αυτή αντιπροσωπεύει ένα σύνολο από interfaces (**που συνήθως ανήκουν σε διαφορετικούς κόμβους**). Ένα πακέτο που στέλνετε σε μία any cast διεύθυνση παραδίδετε σε μία από αυτές τις διευθύνσεις του συνόλου και συγκεκριμένα στην διεύθυνση η οποία είναι «***πλησιέστερη και η καλύτερη***» , σύμφωνα με το πρωτόκολλο δρομολόγησης. Κατανέμονται από τον χώρο τον unicast διευθύνσεων.



Εικόνα 2.21 HAny cast διεύθυνση

Περιγραφή των IPv6 διευθύνσεων

Προτεινόμενη φόρμα

- 3FFE:3600:0:FF:8:800:200C:417A

Συμπιεσμένη φόρμα

- FF01:0:0:0:0:0:0:7 γίνετε FF01::7

Με IPV4 ενσωμάτωση

- 0:0:0:0:0:0:140.113.131.3 ή ::140.113.131.3

Με Prefix Διεύθυνση

Το prefix-μήκος στις IPv6 είναι ισοδύναμο με την μάσκα υποδικτύου στην IPv4 διεύθυνση. Αποτελείτε από ένα ακέραιο αριθμό που ξεκινά από 0 – 128. Για παράδειγμα:

2001:db8:abcd:0012::0/64περιγράφη ένα υποδίκτυο με πλήθος IP διευθύνσεων από:

2001:db8:abcd:0012:0000:0000:0000:0000

Έως και

2001:db8:abcd:0012:ffff:ffff:ffff:ffff.

Ένα interface μπορεί να έχει πολλές διαφορετικές διευθύνσεις. Ο ορισμός των κάθε interfaces, εξαρτάται κάθε φορά από τον διαχειριστή του δικτύου έτσι ώστε να μπορεί να ελέγξει τις συσκευές που θα έχουν πρόσβαση στο Διαδίκτυο ή σε ανάλογες περιοχές.

Κεφάλαιο 3 Πολιτικές Ασφάλειας δικτύων

3.1 Εισαγωγή

Σκοπός των πολιτικών ασφάλειας, είναι να προστατεύετε το δίκτυο από τυχόν απειλές, τόσο από εξωτερικούς παράγοντες, όσο και από εσωτερικούς και παράλληλα να διατηρείτε η απόδοση του σε όσο πιο υψηλά επίπεδα.

Μπορούμε να ορίσουμε την έννοια της πολιτικής ασφάλειας ως εξής:

Ως πολιτική ασφάλειας, καθορίζετε ένα σύνολο κανόνων ασφάλειας που εφαρμόζονται στους υπολογιστές, με το οποίο οι άνθρωποι θα μπορούν να έχουν πρόσβαση στην τεχνολογίας και στις πληροφορίες που αποτελούν περιουσιακά στοιχεία ενός οργανισμού που πρέπει να τηρούν.

Μία πολιτική ασφάλειας αποτελεί ένα χάρτη για τον σχεδιαστή του δικτύου και με αυτό τον τρόπο παρατηρούμε πως λειτουργεί η ασφάλεια εντός αυτού.

Γενικά η πολιτική ασφάλειας σε ένα δίκτυο, μπορεί να καθοριστεί με διάφορους τρόπους:

- Επιβολή της πολιτικής ασφάλειας σε πραγματικό χρόνο
- Παθητική τεχνολογία με την βοήθεια του ελέγχου συμφόρησης
- Μη- τεχνικός έλεγχος συμφόρησης
- Συμβατικός έλεγχος συμφόρησης

Επιβολή της πολιτικής ασφάλειας σε πραγματικό χρόνο

Αποτελεί μία από τις πιο εύκολες μεθόδους ασφάλειας, που μπορούν να χρησιμοποιηθούν στο δίκτυο. Σε αυτή την μέθοδο, χρησιμοποιείται μία συγκεκριμένη τεχνολογία, η οποία διασφαλίζει με επιτυχία και χωρίς παρέμβαση του διαχειριστή, ότι η συγκεκριμένη πολιτική εφαρμόζετε. Για παράδειγμα, ας σκεφτούμε το γεγονός της εφαρμογής μίας πολιτικής ασφάλειας, με την οποία πραγματοποιείται ένα μπλοκάρισμα στις εξερχόμενες προσβάσεις telnet από το δίκτυο μας.

Στην συνέχεια, έχουμε τις εντολές που εφαρμόζουμε στον Router, του δικτύου μας, για την εφαρμογή της συγκεκριμένης πολιτικής.

#access-list 10 deny tcp 172.16.4.0 0.0.0.255 any eq 23

#line vty 0 4

#access-class out 10

Η συγκεκριμένη πολιτική, μολονότι ότι προσφέρει υψηλό βαθμό αξιοπιστίας, δεν μπορεί να χρησιμοποιηθεί σε όλα τα σενάρια ασφάλειας καθώς το κάθε σενάριο, έχει διαφορετική πολιτική.

Παθητική τεχνολογία, με την βοήθεια του ελέγχου συμφόρησης

Σε αυτή την κατηγορία, η πολιτική ασφάλειας που εφαρμόζετε παίζει ένα υποστηρικτικό ρόλο στην ασφάλεια του δικτύου. Η κύρια τεχνολογία που εφαρμόζετε είναι μέσω συστήματος ανίχνευσης εισβολής (IDS), το οποίο ουσιαστικά προειδοποιεί τον διαχειριστή δικτύου για ύποπτη δραστηριότητα που παρατηρείται στην κυκλοφορία των δεδομένων. Τα IDS συστήματα ανίχνευσης εισβολών, εντοπίζουν προσπάθειες παράκαμψης των μηχανισμών ασφάλειας, τόσο από εσωτερικούς χρήστες με περιορισμένα δικαιώματα πρόσβασης, όσο και από εξωτερικούς χρήστες οι οποίοι προσπαθούν να αποκτήσουν πρόσβαση. Εκτός από την προειδοποίηση, τα συγκεκριμένα συστήματα ελέγχουν ανά τα τακτά χρονικά διαστήματα, τους κωδικούς πρόσβασης των χρηστών, προειδοποιώντας τους, για την αδυναμία των κωδικών τους, με κίνδυνο παραβίαση τους.

Μη - τεχνικός έλεγχος συμφόρησης

Χρησιμοποιείται κυρίως από τα ανώτερα στελέχη μίας επιχείρησης ή ενός οργανισμού, πραγματοποιώντας δειγματοληπτικούς ελέγχους και ελέγχοντας την χρήση του δικτύου από τους εργαζομένους.

Συμβατικός έλεγχος συμφόρησης

Απευθύνετε κυρίως στους χρήστες του δικτύου και αποτελεί μία συμφωνία μεταξύ των χρηστών και των διαχειριστών του δικτύου, όπου σε αυτή την συμφωνία, οι χρήστες θα πρέπει να συμμορφωθούν με τους κανόνες των ρόλων που έχουν στο δίκτυο. Σε περίπτωση παραβίασης τους, οι χρήστες θα πρέπει να έχουν επιπτώσεις από την παραβίαση των πολιτικών που έχουν αποδεχτεί.

3.2 Ανάπτυξη συστήματος ασφάλειας

Υπάρχουν τρία σημαντικά βήματα, με τα οποία μπορούμε να αναπτύξουμε ένα σύστημα ασφάλειας, σε ένα οργανισμό.

3.2.1 Εξετάζοντας τον τρόπο εφαρμογής των πολιτικών ασφάλειας

3.2.2 Αναπτύσσοντας την πολιτική ασφάλειας

3.2.3 Σχεδιάζοντας το σύστημα ασφάλειας

3.2.1 Εξετάζοντας τον τρόπο εφαρμογής των πολιτικών ασφάλειας

Η διαδικασία αρχίζει με την εξέταση των δύο βασικών παραγόντων για την δημιουργία της πολιτικής ασφάλειας:

- Τις ανάγκες των επιχειρήσεων
- Την ανάλυση κινδύνου

Οι ανάγκες των επιχειρήσεων

Οι ανάγκες των επιχειρήσεων, ως προς την πολιτική ασφάλειας, χωρίζονται σε δύο κατηγορίες:

- Οι επιχειρηματικοί στόχοι
- Η ανάλυση κινδύνου

Επιχειρηματικοί στόχοι

Είναι οι στόχοι των επιχειρήσεων, οι οποίες μεταφράζονται σε οδηγίες για την κατασκευή πολιτικών ασφάλειας. Όταν οι συγκεκριμένες πολιτικές ασφάλειας, ταιριάζουν με τις ανάγκες των επιχειρήσεων τότε τα πράγματα βαίνουν καλώς.

Ο αρχιτέκτονας ασφάλειας, δέχεται ως είσοδο πληροφορίες με τις ανάγκες των επιχειρήσεων και προσπαθεί να τις μεταφράσει σε πολιτικές. Οι στόχοι θα πρέπει να γνωστοποιούνται επαρκώς έτσι ώστε να μπορούν να γίνουν ορθές αποφάσεις για την ασφάλεια. Από άποψη κόστους ο αρχιτέκτονας ασφάλειας, θα πρέπει να καθορίσει τα κόστη, ανάλογα με τα συμβάντα ασφαλείας που μπορούν να υπάρξουν στο δίκτυο του και χωρίζονται σε 2 κατηγορίες:

- **Ασφάλεια, ως προς την παραβίαση των δεδομένων,** που μπορεί να υπάρξει από ένα επιτιθέμενο.
- **Ασφάλεια, ως προς την απώλεια διαθεσιμότητας του δικτύου,** από διάφορες μορφές επιθέσεων, όπως είναι η άρνηση πρόσβασης υπηρεσιών στο δίκτυο, Denial Of Service (D.O.S.) Attacks.

Ανάλυση Κινδύνου

Παραδοσιακά η ανάλυση κινδύνου, θεωρείτε η εκτίμηση των πιθανών κίνδυνων, σε ένα οργανισμό για να δικαιολογήσει τις πολιτικές ασφάλειας που έχει χρησιμοποιήσει σε αυτό. Αποτελεί επίσης, απαραίτητο συστατικό για την ανάπτυξη των πολιτικών ασφάλειας, διότι εστιάζει το σύστημα ασφάλειας σε μια συγκεκριμένη δέσμη προτεραιοτήτων. Μειονέκτημα της παραδοσιακής ανάλυσης κινδύνου συχνά, είναι οι πολλές πιθανές κατηγορίες απειλών που συχνά παραβλέπονται, επειδή στόχος της ανάλυσης κινδύνου είναι το αποτέλεσμα της επίθεσης.

3.2.2 Αναπτύσσοντας την πολιτική ασφάλειας

Αποτελεί μία από τις πιο σημαντικές ενέργειες, που πρέπει να κάνει ο διαχειριστής ασφάλειας του δικτύου. Μια κακή πολιτική, μπορεί να παρομοιαστεί σαν ένα κακό οδικό χάρτη: μπορούμε να φτάσουμε στον τελικό προορισμό μας, αλλά στην πορεία θα πάρουμε πολλές λάθος διαδρομές. Είναι πιο επιρρεπής σε λάθη, γιατί η αναπτυξιακή πολιτική ασφάλειας, συχνά θεωρείται ως μια επίπονη διαδικασία, η οποία αλλάζει με τον καιρό, ανάλογα με τις ανάγκες των επιχειρήσεων και των κινδύνων που μπορούν να υπάρξουν στα δίκτυα. Γενικά, η πολιτική ασφάλειας μπορεί να παρουσιασθεί, ως μία σειρά ενεργειών όπου κάθε μία, έχει συγκεκριμένη αρχή και ένα συγκεκριμένο τέλος.

Ο ευκολότερος τρόπος για να εξασφαλιστεί μία επιτυχής πολιτική ασφάλειας, είναι να δημιουργήσουμε μία σειρά από μικρότερες, για να μπορούμε να πραγματοποιούμε εύκολα αλλαγές και να τις προσαρμόζουμε ανάλογα με τις συνθήκες που έχουμε να αντιμετωπίσουμε.

Πολιτικές ασφάλειας

Οι Βασικοί τομείς που θα πρέπει να εξετάσουμε είναι οι ακόλουθοι:

- Πολιτικές καθορισμού αποδεκτής χρήσης
- Πολιτικές που διέπουν στις συνδέσεις με απομακρυσμένα δίκτυα
- Πολιτικές που περιγράφουν το επίπεδο ευαισθησίας των διαφόρων τύπων πληροφοριών που πραγματοποιούνται στο πλαίσιο ενός οργανισμού
- Πολιτικές προστασίας της ιδιωτικής ζωής των χρηστών του δικτύου και όλα τα δεδομένα των πελατών
- Πολιτικές που καθορίζουν τις γραμμές ασφάλειας που πρέπει να τηρούνται από τις συσκευές πριν από τη σύνδεσή τους με το δίκτυο

Πολιτικές ασφάλειας και όροι πολιτικής χρήσης

Το πρώτο μέλημα που υπάρχει, είναι ο καθορισμός των βασικών πολιτικών στόχων που πρέπει να εφαρμόσουμε. Κατ 'αρχάς, θα πρέπει να υπάρχει μια **αποδεκτή πολιτική χρήσης (AUP)**. Η πολιτική αυτή καθορίζει τους κανόνες, σύμφωνα με τους οποίους οι χρήστες μπορούν να έχουν πρόσβαση στο δίκτυο. Αυτό θα πρέπει να περιλαμβάνει, όχι μόνο τις κατευθυντήριες γραμμές για την εσωτερική και εξωτερική πρόσβαση στο δίκτυο, αλλά και τους τύπους της κυκλοφορίας που θα πρέπει να επιτρέπονται.

Πολιτικές ασφάλειας στα απομακρυσμένα δίκτυα

Το δεύτερο μέλημα μας, θα πρέπει να είναι οι πολιτικές που διέπουν τις συνδέσεις με τα απομακρυσμένα δίκτυα (VPN), είτε είναι δημόσια, είτε ιδιωτικά. Ορισμένοι οργανισμοί χωρίζουν αυτές τις πολιτικές σε διάφορες κατηγορίες. Οι πολιτικές αυτές θα πρέπει να περιλαμβάνουν απαιτήσεις ασφάλειας κατά την επικοινωνία, όπως εμπιστοσύνη, εχεμύθεια, και πιστοποίηση ταυτότητας για τη σύνδεση με απομακρυσμένους εργαζόμενους, συνεργάτες και πελάτες που θέλουν να επικοινωνήσουν με το δίκτυο, καθώς και το πώς θα πρέπει να ελέγχεται η πρόσβαση στα δίκτυα αυτά, όπως γίνετε με το Internet.

Πολιτικές ασφάλειας στο εσωτερικό δίκτυο

Τρίτο μέλημα μας, θα πρέπει να είναι μια πολιτική που θα περιγράφει πώς πρέπει να αντιμετωπίζονται τα διάφορα είδη των δεδομένων εντός του δικτύου σας. Αυτή η πολιτική καθορίζει σε τι επίπεδο οι επικοινωνίες θα πρέπει να είναι κρυπτογραφημένες και με ποιες μεθόδους κρυπτογράφησης θα είναι αποδεκτές.

Πολιτικές ασφάλειας κατά τον σχεδιασμό

Τέταρτο μέλημα, είναι η πολιτική απορρήτου ενός οργανισμού όσον αφορά τους χρήστες και πελάτες του. Οι πολιτικές αυτές θα πρέπει να καθορίζονται από τις απαιτήσεις για την προστασία των δεδομένων των πελατών, όπως και στην περίπτωση μία ιστοσελίδας που διακινεί εμπορικό περιεχόμενο (e-commerce). Ορισμένες εταιρείες έχουν πολιτικές σύμφωνα με την οποίες κάθε χρήση των πόρων του δικτύου μπορεί να παρακολουθείται από σύστημα IPS. Ο σχεδιαστής του δικτύου, θα πρέπει να γνωρίζει τις πολιτικές του οργανισμού, έτσι ώστε η αρχιτεκτονική ασφάλειας, να συμπίπτει με τους ελέγχους ασφάλειας, όπως έχουν αναπτυχθεί στο δίκτυο.

Οι πολιτικές ασφάλειας χωρίζονται σε 3 κατηγορίες:

- **Γενικές Πολιτικές** – είναι οι Πολιτικές, που αποτελούν τα βασικά στοιχεία της συνολικής πολιτικής για την ασφάλεια του δικτύου και έχουν ευρύτερες επιπτώσεις στη λειτουργία του.
- **Πρότυπα –** καθορίζουν τις ελάχιστες δέσμες ενεργειών που αποτελούν τα κριτήρια για την συγκεκριμένη τεχνολογία. Συχνά αναφέρονται από άλλες πολιτικές. Παραδείγματα είναι, τα πρότυπα κωδικών πρόσβασης, προδιαγραφές για τις ρυθμίσεις ασφάλειας ενός server και άλλα.

- **Κατευθυντήριες γραμμές -** ορίζονται οι πρακτικές ενός οργανισμού. Περιγράφουν τις μεθόδους που πραγματικά προτιμούνται από ένα οργανισμό, χωρίς να είναι απολύτως απαραίτητο αυτό. Παραδείγματα κατευθυντήριων γραμμών είναι η θέσπιση της ζώνης (DMZ), κατά την τοποθέτηση των server ή χαρακτηριστικά ασφάλειας που εφαρμόζονται σε συσκευές που είναι συνδεδεμένες στο δίκτυο.

οι κατευθυντήριες γραμμές μπορεί να εφαρμόζονται στα πλαίσια μιας πολιτικής ή προτύπου.

Ομάδα Πολιτικής Ασφάλειας

Θα πρέπει να αποτελείτε από 2 διαχειριστές. Ο ένας διαχειριστής θα πρέπει να ασχολείται με τις δραστηριότητες του δικτύου (Network Administrator) και ο άλλος ο διαχειριστής θα πρέπει να ασχολείται με τις δραστηριότητες που διέπουν την ασφάλεια του δικτύου (Security Administrator).

Ασφάλεια ενάντια στην πρόσβαση

Κατά τον σχεδιασμό των πολιτικών ασφάλειας, σε περίπτωση όπου οι πολιτικές αυτές θεωρηθούν πολύ περιοριστικές υπάρχει μεγάλος φόβος παραβίασης τους.

Με την πλήρη απαγόρευση των χρηστών προς το Διαδίκτυο, οι χρήστες αναπτύσσουν και προσαρμόζουν τον εαυτό τους χωρίς ρυθμίσεις ασφάλειας. Μέσα από αυτή την ενέργεια οι χρήστες εκτίθενται με μεγαλύτερη πιθανότητα σε επιθέσεις που μπορεί να γίνουν προς το δίκτυο αυτό.

Συνοψίζοντας, μπορούμε να παρατηρήσουμε ότι ένα δίκτυο με τις βέλτιστες πρακτικές ασφάλειας μπορεί να θεωρηθεί πιο ασφαλές από ένα δίκτυο στο οποίο απαγορεύονται όλες οι προσβάσεις προς τα εξωτερικά δίκτυα.

Τελική Αξιολόγηση

Ο αρχιτέκτονας ασφάλειας, θα πρέπει να εξασφαλίσει ότι η ανάπτυξη πολιτικής ασφάλειας είναι και πλήρης και ρεαλιστική. Ιδιαίτερη προσοχή πρέπει να δοθεί στις περιοχές όπου η πολιτική γίνετε με αυτόματο τρόπο και βασίζεται στο δίκτυο. Σε αυτή την περίπτωση θα πρέπει να γίνει μία τροποποίηση της πολιτικής. Όσο λιγότερες πολιτικές ασφάλειας υπάρξουν στο δίκτυο, τόσο η τροποποίηση τους καθώς και ο έλεγχος τους θα μπορεί να γίνει με μεγαλύτερη ευκολία.

3.2.2.1 Παράδειγμα πολιτικής ασφάλειας ανάπτυξης δικτύου

1.0 Σκοπός

Σκοπός αυτής της πολιτικής, είναι η προστασία των δεδομένων που υπάρχουν στο εργαστήριο, οι οποίες δεν θα μπορούν να τεθούν σε κίνδυνο και θα μπορούν να προστατεύονται από εργαστηριακές δραστηριότητες.

2.0 Έκταση

Η συγκεκριμένη πολιτική, θα εφαρμόζετε σε όλες τις συσκευές και σε όλους τους χρήστες του δικτύου. Εκτός από τις υπάρχων συσκευές , όλες οι μελλοντικές συσκευές θα πρέπει να υπακούν στην υπάρχουσα πολιτική, που θα ασκείτε στο δίκτυο.

3.0 Πολιτική

3.1 Ευθύνες ιδιοκτησίας

1. Το εργαστήριο ανήκει εξολοκλήρου στον οργανισμό που υφίσταται. Ο οργανισμός είναι υπεύθυνος για την ανάθεση των εργασιών στους διαχειριστές του δικτύου, την δημιουργία σημείου επαφής (Point Of Contact) μεταξύ των διαχειριστών του δικτύου καθώς και ένα αντίγραφο ασφαλείας (POC), για κάθε εργαστήριο του οργανισμού. Επίσης οι ιδιοκτήτες των εργαστηρίων, θα πρέπει να διατηρούν ενημερωμένες τις (POC) πληροφορίες, οι οποίες θα διακινούνται μέσω των InfoSec ενεργειών (ονομάζουμε τις ενέργειες που γίνονται για την προστασία της πληροφορίας από μη εξουσιοδοτημένη πρόσβαση, χρησιμοποίηση, αλλαγή κ.λπ.), καθώς και την διαχείριση της ομάδας των στελεχών. Οι διαχειριστές των εργαστηρίων καθώς και τα αντίγραφα ασφάλειας, θα πρέπει να είναι άμεσα διαθέσιμα σε περίπτωση έκτακτης ανάγκης, διαφορετικά θα πρέπει να ληφθούν μέτρα προστασίας χωρίς την ύπαρξη τους.

2. Οι διαχειριστές των εργαστηρίων, θα πρέπει να είναι υπεύθυνοι για την ασφάλεια και λειτουργία του εργαστηρίου και για τις επιπτώσεις που θα υπάρξουν από την κίνηση των άλλων εργαστηρίων του οργανισμού. Οι πολιτικές αυτές θα πρέπει να προσδιορίζονται, από τους διαχειριστές του δικτύου, οι οποίοι θα πρέπει να εφαρμόσουν τα καλύτερα μέτρα ασφάλειας για την προστασία του οργανισμού.

3. Οι διαχειριστές των εργαστηρίων, θα πρέπει να είναι υπεύθυνοι για την συμμόρφωση του εργαστηρίου, με όλες τις πολιτικές ασφάλειας που έχουν τεθεί για αυτούς. Μία από τις πιο σημαντικές πολιτικές, είναι ***η πολιτική κωδικού πρόσβασης*** *για ασύρματες συσκευές,* **η πολιτική που**

χρησιμοποιείται στα Anti – Virus και **η προστασία των φυσικών συσκευών** (Hardware, Software, networks, data), από φυσικά φαινόμενα που μπορεί να προκαλέσουν απώλεια ή καταστροφή π.χ. πυρκαγιά, σεισμός, κλοπή, βανδαλισμός, τρομοκρατική επίθεση κ.λπ. .

4. Οι διαχειριστές των εργαστηρίων, θα πρέπει να είναι υπεύθυνοι για τον έλεγχο της πρόσβασης στο εργαστήριο. Η πρόσβαση θα πρέπει να δίνετε μόνο από τον διαχειριστή προς εκείνα τα άτομα που έχουν οριστεί από την εργασία τους, για την χρησιμοποίηση του συγκεκριμένου δικτύου. Αυτό δημιουργεί την ανάγκη, για συνεχόμενη παρακολούθηση της λίστας πρόσβασης του δικτύου και τερματισμός της πρόσβασης σε χρήστες, οι οποίοι δεν διαθέτουν την απαιτούμενη πρόσβαση.

5. Ο οργανισμός θα πρέπει να διαθέτει ένα τείχος προστασίας (firewall), ανάμεσα στο δίκτυο παραγωγής του οργανισμού και στα δίκτυα των εργαστηρίων.

6. Ο οργανισμός θα μπορεί να έχει το δικαίωμα της διακοπής της σύνδεσης των εργαστηρίων, οι οποίες παρεμποδίζουν την λειτουργία του οργανισμού ή αυξάνουν τον κίνδυνο για την ασφάλεια του.

7. Οι IP διευθύνσεις των συσκευών που χρησιμοποιούνται για τα εργαστήρια, θα πρέπει να ανήκουν στο εύρος των διευθύνσεων που έχουν καθοριστεί για αυτά και θα πρέπει να καταχωρούνται σε βάσεις δεδομένων της εταιρείας, οι οποίες θα περιέχουν πρόσφατες πληροφορίες για τις επαφές τους, καθώς και πληροφορίες για το εργαστήριο.

8. Κάθε εργαστήριο που θα πρέπει να παρέχει μία εξωτερική σύνδεση, θα πρέπει να προσδιορίζει τον λόγο για τον οποίο θα πρέπει να παρέχει την σύνδεση αυτή και μετά από την εξέταση του αιτήματος, θα πρέπει να αποφασιστεί ή έγκριση ή η απόρριψη του.

9. Όλοι οι κωδικοί πρόσβασης των χρηστών, θα πρέπει να αναπτύσσονται βάση των πολιτικών ασφάλειας των κωδικών πρόσβασης του οργανισμού. Επιπλέον χρήστες ή συσκευές οι οποίες δεν έχουν άδεια εξουσιοδότησης, θα πρέπει να διαγράφονται εντός τριών ημερών. Οι κωδικοί λογαριασμών των χρηστών θα πρέπει να αλλάζουν κάθε τρείς μήνες τουλάχιστον.

10. Κανένα εργαστήριο δεν θα πρέπει να παρέχει υπηρεσίες παραγωγής. Οι υπηρεσίες παραγωγής ορίζονται, ως κρίσιμες επιχειρηματικές υπηρεσίες που παράγουν έσοδα ή παρέχουν υπηρεσίες προς τους πελάτες.

11. Τα αιτήματα άρσης μη συμμόρφωσης θα αξιολογούνται για κάθε περίπτωση χωριστά και θα γίνονται παρατηρήσεις εφόσον είναι δικαιολογημένες.

3.2 Γενικές ρυθμίσεις απαιτήσεων

1. Όλη η κίνηση του οργανισμού (παραγωγή και δίκτυα εργαστηρίων), θα πρέπει να περνάνε από την δικτυακή υποστήριξη του οργανισμού, η οποία θα βρίσκετε στο Firewall. Οι συσκευές του εργαστηρίου δεν θα πρέπει να διασυνδέονται με τις συσκευές εταιρικής παραγωγής.

2. Οι αρχικές ρυθμίσεις που θα πρέπει να γίνουν στο Firewall, καθώς και οι βελτιώσεις, θα καθορίζονται από την δικτυακή υποστήριξη του οργανισμού.

3. Δραστηριότητες που πρέπει να εφαρμόζονται στα δίκτυα όπως, σαρώσεις θυρών, έλεγχος κυκλοφορίας πακέτων για spam και υπερφόρτωση δικτύου, οι οποίες δρουν αρνητικά στην συνολική απόδοση του δικτύου, θα πρέπει να εφαρμόζονται σε κάθε δίκτυο χωριστά.

4. Οι κινήσεις δεδομένων μεταξύ των εργαστηρίου και του εταιρικού δικτύου, θα πρέπει να επιτρέπονται με βάση της ανάγκες των επιχειρήσεων και όταν οι κινήσεις αυτές δεν θα έχουν αρνητικές επιπτώσεις για την απόδοση του δικτύου. Σε καμία περίπτωση, δεν θα πρέπει να διαφημίζονται υπηρεσίες του δικτύου παραγωγής ή πληροφορίες εμπιστευτικές, οι οποίες μπορούν να θέσουν σε κίνδυνο, ολόκληρη την επιχείρηση.

5. Η δικτυακή υποστήριξη του οργανισμού, θα μπορεί να παρεμβαίνει σε όλα τα δεδομένα, που υπάρχουν στο εργαστήριο και θα μπορεί να παρεμβάλετε ανά πάσα στιγμή.

6. Οι συσκευές των εργαστηρίων θα πρέπει να πληρούν όλες τις προϋποθέσεις του κατασκευαστή, σχετικά με την ασφάλεια του προϊόντος και θα πρέπει να πιστοποιούνται από τους Server's ελέγχου ταυτότητας του δικτύου.

7. Ο κωδικός πρόσβασης για όλες τις συσκευές, που είναι πύλες στο δίκτυο θα πρέπει να είναι διαφορετικός από οποιονδήποτε άλλο κωδικό πρόσβασης του εργαστηρίου. Θα παρέχετε μόνο από τους διαχειριστές του δικτύου.

8. Σε εργαστήρια, όπου δεν υπάρχει πιθανότητα να βρίσκετε μόνιμο προσωπικό (εργαστήρια εκπαίδευσης), οι άμεσες συνδέσεις με το δίκτυο παραγωγής δεν θα επιτρέπονται.

9. Συσκευές υποδομής (όπως IP Phones), που χρειάζονται συνδεσιμότητα με το εταιρικό δίκτυο, θα πρέπει να συμμορφώνονται, με τις πολιτικές που ισχύουν για αυτή την κατηγορία των συσκευών.

10. Οι αιτήσεις των εργαστηρίων για εξωτερικές συνδέσεις, θα πρέπει να εγκρίνονται από την δικτυακή υποστήριξη του οργανισμού. Οι γραμμές αυτές που υπάρχουν για τις εξωτερικές συνδέσεις θα πρέπει να ρυθμιστούν με τέτοιον τρόπο ώστε να δέχονται μόνο ασφαλείς αριθμούς κλήσεων. Ισχυροί κωδικοί θα πρέπει να χρησιμοποιούνται για έλεγχο ταυτότητας.

11. Οι εξωτερικές συνδέσεις με δίκτυα παραγωγής, δεν θα πρέπει να υπάρχουν από οποιοδήποτε εξοπλισμό του δικτύου.

4.0 Επιβολή

Σε περίπτωση που κάποιος εργαζόμενος έχει παραβιάσει την συγκεκριμένη πολιτική ασφάλειας, θα του επιδοθούν κυρώσεις ακόμη και τερματισμό της απασχόλησης του, από αυτήν.

5.0 Ορισμοί

Εσωτερικά - Ένα εργαστήριο το οποίο βρίσκετε σε εταιρικό τείχος προστασίας και συνδέετε σε δίκτυο παραγωγής, θα μπορεί να συμμετέχει στην παραγωγή.

Υποστήριξη δικτύου του οργανισμού - χρησιμοποιείται για την υποστήριξη της διαχείρισης των δικτύων που ανήκουν στον οργανισμό.

Διευθυντής εργαστηρίου - είναι το άτομο που είναι υπεύθυνο για όλες τις δραστηριότητες του εργαστηρίου και του προσωπικού του.

Εργαστήριο – είναι ο χώρος του δικτύου που ασχολείται με την δοκιμή, την επίδειξη και την κατάρτιση του προϊόντος.

Εξωτερικές συνδέσεις – είναι οι συνδέσεις οι οποίες απευθύνονται σε τρίτους, για σύνδεση με το δίκτυο του οργανισμού, χωρίς την μεταφορά των δεδομένων χωρίς έλεγχο. Υποστηρίζονται από ISDN γραμμές και από οποιεσδήποτε άλλες τηλεφωνικές γραμμές.

Εργαστήριο με συσκευή πύλης δικτύου – είναι ένα εργαστήριο, το οποίο διαθέτει μία συσκευή πύλης δικτύου η οποία συνδέει το εργαστήριο με το υπόλοιπο δίκτυο της εταιρείας. Από αυτό το σημείο περνάει και ελέγχετε όλη η κίνηση που υπάρχει μεταξύ του εργαστηρίου και το εταιρικό δίκτυο παραγωγής.

Telco - είναι οι γραμμές, οι οποίες είναι παρόμοιες με τις γραμμές που παρέχονται από φορέα παροχής υπηρεσιών (Service Provider). Οι τηλεφωνικές εταιρείες προσφέρουν συνδεσιμότητα στο δίκτυο του οργανισμού μέσω T1 , T3, DSL, ISDN και άλλων γραμμών.

Κυκλοφορία – αναφέρετε στην μαζική κίνηση δεδομένων, εντός του δικτύου που μπορεί να προκαλέσει συμφόρηση σε αυτό.

Τείχος προστασίας – είναι μία συσκευή, η οποία ελέγχει την πρόσβαση μεταξύ των δικτύων με την οποία συνδέονται. Ως τείχος προστασίας μπορεί να είναι ένα **PIX Firewall**, ένα **Router με λίστες πρόσβασης** ή άλλες παρόμοιες συσκευές.

Extranet – είναι εξωτερικά δίκτυα που απαιτούν πρόσβαση στα ιδιωτικά δίκτυα.

DMZ ζώνη – είναι το τμήμα του δικτύου που συνήθως βρίσκετε εξωτερικά από το εσωτερικό τμήμα (intranet) και διαθέτει υψηλό έλεγχο πρόσβασης σε αντίθεση με το υπόλοιπο δίκτυο.

3.2.3 Σχεδιάζοντας το Σύστημα ασφάλειας

Βέλτιστες πρακτικές

Αποτελεί το τελευταίο βήμα, πριν την εφαρμογή στο δίκτυο. Οι παραπάνω πολιτικές που έχουν διατυπωθεί θα πρέπει να είναι σαφής, για να μπορούν να εφαρμοστούν.

Ένα παράδειγμα που μπορεί αν δοθεί ως εφαρμογή πολιτικής ασφάλειας στο δίκτυο είναι η βασική ρύθμιση των δρομολογητών. Μία τέτοια ενέργεια θεωρείται επίπονη διαδικασία καθώς τέτοιου είδους αλλαγές θα δημιουργήσουν επιπτώσεις στην απόδοση του δικτύου.

Σε αυτή την περίπτωση η λήψη των πολιτικών ασφάλειας, δεν πρέπει να θεωρείται ως η *μόνη* είσοδος σε συστήματα ασφάλειας. Επομένως θα πρέπει να εφαρμοστούν μία σειρά από **βέλτιστες πρακτικές.**

Οι Βέλτιστες πρακτικές διασφαλίζουν ότι οι πολιτικές ασφάλειας που θα χρησιμοποιηθούν, θα εφαρμοστούν με τον καλύτερο δυνατό τρόπο.

Οι βέλτιστες πρακτικές μπορούν να αντληθούν από διάφορα μέρη, όπως:

- Βιβλία
- Ομάδες συζητήσεων (Forums)
- Διάφορες Ιστοσελίδες, που σχετίζονται με την ασφάλεια.

Για την εφαρμογή των βέλτιστων πρακτικών μπορούν να χρησιμοποιηθούν τα εξής βήματα:

Βήμα 1 Σε περίπτωση που μια βέλτιστη πρακτική που περιγράφεται εδώ έχει νόημα και δεν έρχεται σε αντίθεση με τις πολιτικές σας ή με τον τρόπο που ο οργανισμός σας χρησιμοποιεί το δίκτυό, τότε μπορεί να εφαρμοστεί.

Βήμα 2 Σε περίπτωση που μια βέλτιστη πρακτική που περιγράφεται εδώ δεν έχει νόημα, τότε συνεχίζουμε στο επόμενο βήμα.

Βήμα 3 Καθορίζουμε το στοιχείο εκείνο της βέλτιστης πρακτικής που έρχεται σε αντίθεση με την πολιτική που έχουμε θεσπίσει. Μεταφέρουμε το στοιχείο αυτό, πίσω στην ομάδα σχεδιασμού της πολιτικής και καθορίζουμε τις επιπτώσεις, της μη εφαρμογής των πρακτικών αυτών.

Βήμα 4 Αναπτύσσουμε μία λίστα βέλτιστων πρακτικών, κατανοώντας τις συνέπειες που θα υπάρξουν σε περίπτωση μη εφαρμογής τους.

Οι βέλτιστες πρακτικές, συνήθως δεν βρίσκονται άμεσα στις πολιτικές ασφάλειας. Κάθε νέα έκδοση του υλικού και του λογισμικού μπορεί να αλλάξει τον τρόπο με τον οποίο η ασφάλεια μπορεί να υλοποιηθεί, με αποτέλεσμα ορισμένες βέλτιστες πρακτικές να αλλάξουν. Έχοντας τροποποιήσει τις πολιτικές ασφάλειας, κάθε φορά που συμβαίνει αυτό, δεν είναι αποτελεί καλή στρατηγική σχεδιασμού. Τα έγγραφα που πιθανά να προσεγγίζουν αυτό το επίπεδο λεπτομέρειας είναι τα έγγραφα προτύπων ή κατευθυντήριων γραμμών. Χωρίς να περιέχουν όλες τις τεχνικές λεπτομέρειες.

Για παράδειγμα, για την πρόσβαση στο WLAN θα πρέπει να εξασφαλίζεται με την **εμπιστευτικότητα**, την **ακεραιότητα**, και την **επαλήθευση ταυτότητας** παραπέμποντας τον αναγνώστη σε **αποδεκτά πρότυπα κρυπτογράφησης**. Με την εφαρμογή αυτής της πολιτικής, ο χρήστης θα κινηθεί σε ασφαλή επίπεδα κρυπτογράφησης, σύμφωνα με την πολιτική που υπάρχει για την ασφαλή πρόσβαση στο ιντερνέτ.

Κύκλος Ζωής Συστημάτων ασφάλειας

Οι λειτουργίες ασφάλειας είναι η διαδικασία της αναθεώρησης, της προσαρμογής και της αντιμετώπισης συμβάντων ασφάλειας, όπως αυτά συμβαίνουν στο δίκτυο. Μπορούμε να πούμε ότι υπάρχουν, τρεις κύριοι τομείς των λειτουργιών ασφάλειας:

- Παρακολούθηση και συντήρηση του συστήματος
- Τον έλεγχο της συμμόρφωσης
- Αντιμετώπιση περιστατικών

Σύστημα Παρακολούθησης και Συντήρησης

Κατά την δικτύωση, απαιτείται ελάχιστη παρακολούθηση του συστήματος. Συνήθως σε μικρού μεγέθους δίκτυα, η παρακολούθηση του συστήματος μέσω των πινάκων δρομολόγησης του δικτύου συνήθως δεν πραγματοποιείται.

Κατά την παρακολούθηση ενός δικτύου, για να μπορεί να θεωρηθεί επιτυχής η συγκεκριμένη ενέργεια, θα πρέπει να ακολουθήσουμε τις εξής πρακτικές:

- Αναδημιουργία των συστημάτων ασφάλειας που βρίσκονταν σε κίνδυνο και επανεκπαίδευση των διαχειριστών σχετικά με τις πολιτικές συντήρησης του συστήματος.
-

- Εντοπισμός της πηγής της επίθεσης.
- Έλεγχος των servers, για την διασφάλιση τους από μη εξουσιοδοτημένες αλλαγές.
- Εξέταση του ενδεχομένου τροποποίησης της πολιτικής ασφάλειας ανάλογα με την πρόσβαση που υπάρχει από τον server.

Συντήρηση

Είναι μία διαδικασία, που εξασφαλίζει ότι τα συστήματα είναι ενημερωμένα με τις τελευταίες διορθώσεις της ασφάλειας. Η Εφαρμογή συντήρησης των συστημάτων είναι συγκεκριμένη. Τα βασικά βήματα είναι τα εξής:

Βήμα 1 Καθορισμός των διορθώσεων, που θεωρούνται απαραίτητες και τις συχνότητας με την οποία θα πρέπει να εφαρμοστούν.

Βήμα 2 Έλεγχος πριν από την εμφάνιση της εφαρμογής τους, στην παραγωγική διαδικασία.

Βήμα 3 Πιθανές διορθώσεις της εφαρμογής, κατά την εκτέλεση στην παραγωγική διαδικασία.

Έλεγχος της συμμόρφωσης

Ο έλεγχος της συμμόρφωσης είναι η πιο ενδιαφέρουσα τεχνική, στην διάρκεια του κύκλου ζωής της ασφάλειας. Κατά τον έλεγχο αυτό, οι πολιτικές, τα πρότυπα και οι κατευθυντήριες γραμμές ελέγχονται σε πραγματικό περιβάλλον εργασίας.

Μέσα από τον έλεγχο συμμόρφωσης:

- Το σύστημα ασφάλειας, εφαρμόζει τις απαιτήσεις των πολιτικών ασφάλειας, με τον πιο αποτελεσματικό τρόπο.
- Οι Πολιτικές ασφάλειας, αντιμετωπίζουν όλες τις απειλές που μπορούν να υπάρξουν σε ένα πραγματικό περιβάλλον.

Εκτός από την εσωτερική ασφάλεια του δικτύου, είναι χρήσιμο να υπάρχει και μία εξωτερική οντότητα η οποία θα αξιολογεί την ασφάλεια σε τακτική βάση.

Εκτός από τις εσωτερικές δράσεις του δικτύου, είναι πολύ χρήσιμο να έχουμε μια εξωτερική οντότητα (outside entity access), που να αξιολογεί την ασφάλεια τακτικά. Συνήθως, οι πιο αποτελεσματικές εκτιμήσεις, είναι αυτές που πραγματοποιούνται εκτός δικτύου.

Ο στόχος είτε των εσωτερικών ελέγχων είτε των εξωτερικών ελέγχων είναι να προσδιορίσουμε τις περιοχές όπου η πολιτική ασφάλειας, επιτρέπει επιθέσεις που κανονικά δεν θα έπρεπε να επιτρέπει.

Αντιμετώπιση περιστατικών

Είναι μία ενέργεια, που δεν μπορεί να αποφευχθεί σε κανονικές συνθήκες. Λαμβάνει χώρα όταν συμβαίνει μία αποτυχία στις πολιτικές σας, σύστημα ασφάλειας, στις εργασίες της ομάδας ή σε βασικές παραδοχές.

Παρακάτω παρουσιάζονται μερικές από τις καταστάσεις που υπάρχουν για την αντιμετώπιση τέτοιων φαινομένων:

- Το σύστημα ασφάλειας αποτυγχάνει να αντιμετωπίσει ένα συγκεκριμένο είδος επίθεσης και η επίθεση αυτή λαμβάνει χώρα στο σύστημα.
- Ο οργανισμός δεν μπορεί να αναγνωρίσει ένα κρίσιμο τμήμα του συστήματος, με αποτέλεσμα το παραπάνω σύστημα να προσβληθεί.
- Ένα νέο είδος επίθεσης χτυπά το δίκτυο και το υπάρχον σύστημα ασφάλειας που υπάρχει δεν μπορεί να ανταποκριθεί.
- Η πιστοποίηση με την οποία αναγνωρίζονται οι χρήστες είναι λανθασμένη με αποτέλεσμα να έχουμε μία εσωτερική επίθεση στο δίκτυο στην οποία δεν υπάρχει προστασία.
- Οι χρήστες, οι οποίοι δεν ακολουθούν τα πρότυπα ασφάλειας ενός οργανισμού, θέτουν και τον ίδιο τον οργανισμό σε κίνδυνο.

3.3 Πολιτικές ασφαλείας σε συσκευές δικτύωσης

Σήμερα υπάρχουν 3 συσκευές δικτύωσης, μεταξύ άλλων,

- Routers,
- Switches,
- Firewalls.

Η ασφάλεια των συσκευών αυτών είναι αρκετά διαφορετική, η οποία αλλάζει ανάλογα με την ποσότητα της εργασίας που έχει να εκτελέσει. Για την πρόσβαση στις συσκευές χρησιμοποιείται η θύρα κονσόλας. Η θύρα κονσόλας εκτός από την πρόσβαση μπορεί να χρησιμοποιηθεί για την επανάκτηση χαμένων κωδικών πρόσβασης.

3.3.1 Router

Ο Δρομολογητής είναι μία συσκευή η οποία αποτελεί ένα από τα πιο σημαντικά αντικείμενα των επιθέσεων που πραγματοποιούνται στο δίκτυο. Για να μπορέσουμε να διασφαλίσουμε την σωστή λειτουργία τις συσκευής , θα πρέπει να απενεργοποιήσουμε τις περιττές υπηρεσίες και να διασφαλίσουμε ότι οι κωδικοί πρόσβασης κρυπτογραφηθεί όποτε είναι δυνατόν.

- Απενεργοποίηση Domain name System (DNS)

  Router (config) # no ip domain-lookup

- Απενεργοποίηση μικρών Υπηρεσιών που χρησιμοποιούνται κυρίως για διαγνωστικούς σκοπούς, όπως echo μηνύματα καθώς και Finger υπηρεσίες

  Router (config) #no service tcp-small-servers

  Router (config) # no service udp-small-servers

  Router (config) # no service finger

- Απενεργοποίηση της υπηρεσίας BOOTP SERVER, η οποία είναι μια υπηρεσία η οποία παρέχει αντίγραφα των αρχείων ρυθμίσεων IOS σε δικτυακές και μπορούν να χρησιμοποιηθούν για σκοπούς επιθέσεων.

  Router (config) #no ip bootp server

- Απενεργοποίηση της υπηρεσίας IP SOURCE ROUTING, κατά την οποία ο αποστολέας ενός IP πακέτου μπορεί να ελέγξει όλη την διαδρομή που ακολουθεί το πακέτο του, από την πηγή έως και τον προορισμό.

  Router(config)#no ip source-route

- Απενεργοποίηση απευθείας λήψης και αποστολής πακέτων-broadcast προς ένα συγκεκριμένο υποδίκτυο στο οποίο ανήκει ο host.

  Router (config) #no ip directed-broadcast

- Απενεργοποίηση υπηρεσίας Proxy ARP, η οποία χρησιμοποιείται κυρίως για την επέκταση ενός υπάρχοντος δικτύου, με την χρησιμοποίηση διάφορων τμημάτων.

  Router (config) # interface Ethernet 0

  Router (config) # no ip proxy-arp

- Απενεργοποίηση υπηρεσίας ICMP πακέτων, τα ICMP πακέτα χρησιμοποιούνται σε πολύπλοκα δίκτυα, στα οποία θέλουμε να εξασφαλίσουμε και να ελέγξουμε την επιτυχής δρομολόγηση μονοπατιών. Υπάρχουν 3 μορφές ICMP πακέτων:

  - **ICMP REDIRECTS**: χρησιμοποιούνται κυρίως για την πιστοποίηση δρομολόγησης συγκεκριμένης κατεύθυνσης.

    Router(config)#no ip redirect

  - **ICMP Host Unreachable :** αυτά τα πακέτα δεν ανήκουν στις πληροφορίες των πακέτων που ανήκουν στα Routing Table του Router.

    Router(config)#no ip unreachable

  - **ICMP Mask Reply Messages:** είναι ένα είδος μηνυμάτων που απαντά σε address mask requests μεταφέροντας πληροφορίες address mask field και πληροφορίες σχετικά με το υποδίκτυο που ανήκει και σε ποιο δίκτυο.

    Router(config)#no ip mask-reply

Κρυπτογράφηση κωδικών πρόσβασης

Η κρυπτογράφηση των κωδικών πρόσβασης στηρίζονται στο Αλγόριθμο κρυπτογράφησης Vignere, όπου σε αυτόν κρυπτογραφούνται αλγόριθμοι κρυπτογράφησης του καίσαρα.

Router(config)#service password-encryption

Ρυθμίσεις αυθεντικοποίησης

Μερικές από τις αυθεντικοποιήσης που χρησιμοποιούνται στους δρομολογητές είναι οι εξής:

Enable secret

Στηρίζονται σε αλγόριθμους κρυπτογράφησης τύπου MD5, οι οποίοι θεωρούνται πιο ασφαλής από τους default μεθόδους κρυπτογράφησης.

Router(config)#enable secret *password*

Login Banner

Είναι ένα μήνυμα που εμφανίζετε κατά την διαδικασία σύνδεσης των χρηστών με την συσκευή.

Router(config)#banner motd

Line Access

Η παρακάτω μέθοδος χρησιμοποιείται για την προστασία της γραμμής κονσόλας, για την πρόσβαση των χρηστών στην συσκευή

Router(config)# line con 0

Router(config-line)# exec-timeout 5 0

Router(config-line)# password *password*

Router(config-line)#login

Απενεργοποίηση AUX θύρας

Router(config)# line aux 0

Router(config-line)# no exec

Απενεργοποίηση VTY θύρας

Router(config)# line vty 0 3

Router(config-line)# exec-timeout 5 0

Router(config-line)# password *password*

Router(config-line)#login

Router(config-line)#transport input *protocol*

Line vty 0 4

Πρόκειται για τις 5 γραμμές που χρησιμοποιούνται για telnet συνδέσεις, μεταξύ αυτών η line vty 0 που πρόκειται για πρόσβαση μέσω κονσόλας. Σε αυτές τις θύρες, μπορούμε να χρησιμοποιήσουμε access-list οι οποίες θα μας βοηθήσουν για να αποφύγουμε την άρνηση υπηρεσιών κατά την διαδικασία του login, επιτρέποντας μόνο συγκεκριμένες διευθύνσεις για πρόσβαση.

Router (config) # line vty 4

Router (config-line) # exec-timeout 5 0

Router (config-line) # password *password*

Router (config-line) # login

Router (config-line) # transport input *protocol*

Router (config-line) # access-class 99 in Router (config) # access-list 99 permit host *adminIP*

Router (config) # access-list 99 deny any log

Username, passwords

Router (config) # username *username* password *password*

Router (config) # line vty 0 4

Router (config-line) # login local

Ρύθμιση αυθεντικοποίησης μέσω TACACS+

Είναι μια εφαρμογή ασφαλείας που χρησιμοποιείται για αυθεντικοποίηση των χρηστών εκείνων που θέλουν να αποκτήσουν πρόσβαση στο router.

Router (config) # aaa new-model

Ρύθμιση σε ποια τοποθεσία ανήκει ο TACACS SERVER

Router (config) # tacacs-server host *ipaddr*

Καθώς και τους κωδικούς που χρησιμοποιεί

Router (config) # tacacs-server key *password*

Default μορφές αυθεντικοποίησης των TACACS +

Router (config) # aaa authentication login default group tacacs+

Μέθοδος αυθεντικοποίησης για πρόσβαση μέσω θύρα κονσόλας

Router (config) # line vty 0 4

Router (config-line) # login authentication default

Router(config)#line con 0

Router (config-line) # login authentication no-tacacs

Αναλυτική καταγραφή (log) κάθε εντολής που χρησιμοποιήθηκε για την ρύθμιση αυθεντικοποίησης των routers

! καταγραφή του login και του logout στον router

Router (config) # aaa accounting exec default start-stop group tacacs+

! καταγραφή των εντολών που αφορούν την βασική ρύθμισης telnet σύνδεσης

Router (config) # aaa accounting commands 1 default start-stop group tacacs+

! καταγραφή των εντολών που αφορούν το enable mode

Router (config) # aaa accounting commands 15 default start-stop group tacacs+

Ρύθμιση απομακρυσμένης πρόσβασης μέσω Secure Shell (SSH)

Το secure shell (ssh), είναι ένα πρωτόκολλο που χρησιμοποιείται για απομακρυσμένες συνδέσεις. Οι επικοινωνίες μεταξύ client-server πραγματοποιούνται χρησιμοποιώντας είτε SSH VERSION 1 είτε SSH VERSION 2. Ιδιαίτερη βαρύτητα δίνετε σε SSH VERSION 2, λόγω ότι παρέχουν πιο ασφαλείς αλγορίθμους κρυπτογραφίας.

Προϋπόθεση για την χρησιμοποίηση του πρωτοκόλλου αυτού, είναι το IOS image που χρησιμοποιείται να είναι **k9(crypto)**.

Router (config) # hostname *hostname*

Router (config) # ip domain-name *yourdomain.com*

Router (config) # crypto Key generate rsa

Ρύθμιση των VTY – lines να δέχονται μόνο SSH πρωτόκολλα

Router(config)#line vty 0 4

Router(config)#transport input ssh

Διαχείριση πρόσβασης

Περίπτωση πρόσβασης μέσω HTTP

Στην περίπτωση όπου οι χρήστες θα πρέπει να έχουν πρόσβαση σε υπηρεσίες web server θα πρέπει να ρυθμίσουμε τον router, έτσι ώστε να δέχεται συγκεκριμένες διευθύνσεις IP.

Router(config)# ip http access-class 10

Router(config)# access-list 10 permit host *ip-address*

Router(config)# access-list 10 deny aby log

Καλό θα είναι, όταν δεν χρησιμοποιούνται οι υπηρεσίες http να απενεργοποιείτε η ρύθμιση

Router(config)# no ip http server

Αυθεντικοποίηση για πρόσβαση σε http υπηρεσίες

Router(config) # ip http authentication ?

Enable, χρησιμοποιώντας κωδικούς πρόσβασης

Local, χρησιμοποιώντας username και passwords

Tacacs, χρησιμοποιώντας εφαρμογές ασφαλείας tacacs για αυθεντικοποίηση χρηστών

Ασφαλή ρύθμιση του πρωτοκόλλου CDP

Είναι ένα πρωτόκολλο που χρησιμοποιείται για την κοινοποίηση πληροφοριών των γειτονικών routers

Καλό θα είναι, σε περιπτώσεις όπου δεν εμπιστευόμαστε τους γειτονικούς routers να απενεργοποιείτε για λόγους ασφαλείας.

Ολική απενεργοποίηση

Router(config)#no cdp run

Απενεργοποίηση μόνο σε συγκεκριμένες διασυνδέσεις

Router(config-if)#no cdp enable

Ασφαλής ρύθμιση του συστήματος καταγραφής μέσω Syslog

Ενεργοποίηση του συστήματος καταγραφής σε συγκεκριμένους host's με την εφαρμογή χρονοσφραγίδων (timestamps)

Router(config)#service timestamps log datetime localtime msec show-timezone

Router(config)Slogging *syslog- ip -addr*

Αποθήκευση των μηνυμάτων καταγραφής στην buffer μνήμη του router

Router(config)#logging buffered *buffersize*

Ασφαλής ρύθμιση μέσω NTP υπηρεσιών

Για την μέγιστη χρησιμοποίηση των syslog μηνυμάτων, θα συγχρονίσουμε την time-zone που χρησιμοποιούμε στον router με NTP υπηρεσίες.

Router(config)#clock timezone PST -8

Router(config)#clock summer-time PDT recurring

Router(config)#ntp authenticate

Router(config)#ntp authentication-key 1 md5 *password*

Router(config)#ntp trusted-key 1

Router(config)#ntp access-group peer 96

Router(config)#ntp server *ntp-svr-ip* key 1

Router(config)#access-list 96 permit host *ntp-svr-ip*

Router(config)#access-list 96 deny any log

Σε περίπτωση, που δεν χρειαζόμαστε NTP πληροφορίες για την καταγραφή NTP μηνυμάτων θα πρέπει να τις απενεργοποιήσουμε σε ορισμένες διασυνδέσεις που δεν χρειάζονται.

Router(config-if)#ntp disable

3.3.2 Switch

Οι ρυθμίσεις ασφάλειας των switches's είναι παρόμοιες με τις ρυθμίσεις ασφάλειας που χρησιμοποιούνται στα routers τις cisco παραθέτοντας παρακάτω τις πιο σημαντικές

! ενεργοποίηση των NTP υπηρεσιών

set timezone PST -8

set summertime PDT

set summertime recurring

set ntp authentication enable

set ntp key 1 trusted md5 *password*

set ntp server *ntp-svr-ip* key 1

set ntp client enable

! απενεργοποίηση υπηρεσιών που δεν είναι απαραίτητες

set cdp disable

set ip http server disable

! ενεργοποίηση για αυθεντικοποίηση πρόσβασης χρηστών μέσω aaa

set tacacs server *tacacs-ip-addr* primary

set tacacs key *password*

set authentication login tacacs enable telnet

set authentication login local disable telnet

set accounting exec enable start-stop tacacs+

set accounting commands enable all start-stop tacacs+

! ενεργοποίηση passwords και περιορισμών πρόσβασης

set banner motd *

Insert your warning banner here.

set logout 5

set ip permit enable telnet

set ip permit *telnet- ip -addr* 255.255.255.255 telnet I

! εγκατάσταση SSH

set crypto key rsa 1024

set ip permit enable ssh

set ip permit *ssh -client-ips netmask* ssh

3.3.3 Firewall

Όπως έχουμε αναφέρει και σε προηγούμενα κεφάλαια τα firewalls αποτελούν συσκευές οι οποίες παρακολουθούν και ελέγχουν την κίνηση δεδομένων εντός του δικτύου. Είναι συσκευές οι οποίες παρουσιάζουν μεγαλύτερες δυνατότητες ασφάλειας σε σχέση με τις προηγούμενες συσκευές που έχουμε αναφέρει.

Μερικά από τα χαρακτηριστικά ασφαλείας που διαθέτουν είναι τα παρακάτω

- Περιορισμός σε telnet συνδέσεις

pixfirewall(config)# telnet *ip-addr mask interface*

π.χ. (pixfirewall(config)# telnet 192.0.2.55 255.255.255.255 inside)

- ρύθμιση password

pixfirewall(config)# passwd password

- Αυθεντικοποίηση χρηστών μέσω υπηρεσιών TACACS+

pixfirewall(config)# aaa-server telnet-group protocol tacacs+

pixfirewall(config)# aaa-server telnet-group (inside) host tacacs-ip-addr

- Έλεγχος της telnet σύνδεσης για την χρησιμοποίηση του telnet-group

pixfirewall(config)# aaa authentication telnet console telnet-group

- Ενεργοποίηση password

pixfirewall(config)# enable password *password*

- Ρύθμιση του SSH

!προσδιορισμός του hostname και του domain-name

hostname *nsa-pix*

domain-name *yourdomain.com*

! δημιουργία κλειδιού

ca generate rsa key 1024

! αποθήκευση κλειδιού

ca save all

! ενεργοποίηση SSH σε inside διασύνδεση

ssh 192.0.2.0 255.255.255.0 inside

- Ρύθμιση του συστήματος καταγραφής syslog

pixfirewall(config)# logging on

pixfirewall(config)# logging host inside syslog- ip -addr

- Εντολή περιορισμού του επιπέδου καταγραφής για περιορισμό των <<αχρείαστων>> προειδοποιήσεων

pixfirewall(config)# logging trap *error,* όπου (error), αποτελεί το εύρος των επιπέδων 3 έως 7.

3.3.4 Συμπέρασμα

Χρησιμοποιώντας τις παραπάνω συσκευές δικτύωσης με τις κατάλληλες ρυθμίσεις ασφαλείας αυτό που πετυχαίνουμε είναι η μείωση των απειλών που μπορούν να προκύψουν από διάφορες περιπτώσεις επιθέσεων, οι οποίες έχουν ως σκοπό την παραβίαση του δικτύου και την πρόσβαση σε ασφαλή δεδομένα. Για να μπορέσουμε να εξασφαλίσουμε την ασφάλεια αυτή εκτός από τις ξεχωριστές ρυθμίσεις των συσκευών, θα πρέπει να μελετήσουμε και διάφορες μεθόδους επιθέσεων με τις οποίες θα ασχοληθούμε παρακάτω.

Κεφάλαιο 4 Εργαστηριακές μετρήσεις

4.1 Εργαστηριακό περιβάλλον GNS3

4.1.1 Εισαγωγή

Το GNS3 είναι ένα περιβάλλον προσομοίωσης ανοιχτού λογισμικού, μέσω του οποίου μπορούμε να παρατηρήσουμε τον τρόπο λειτουργίας, σε πραγματικές συνθήκες.

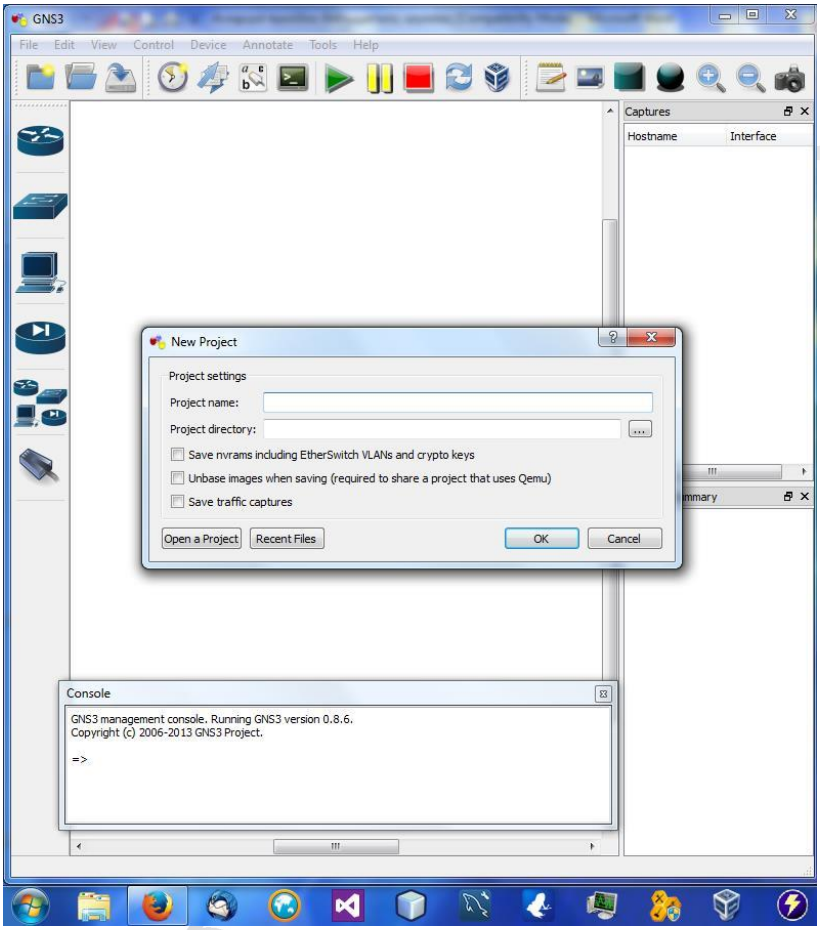
Το λογισμικό παρέχει ένα γραφικό περιβάλλον στο οποίο ο χρήστης θα μπορεί με εύκολο τρόπο να σχεδιάζει δίκτυα.

Μπορεί να εκτελεστεί σε καθημερινούς υπολογιστές και μπορεί να χρησιμοποιεί ως τερματικά, πολλαπλά και διαφορετικά μεταξύ τους λειτουργικά συστήματα (LINUX, WINDOWS SERVER, WINDOWS XP κ.α.).

Προκειμένου να παρέχει πλήρεις και ακριβές προσομοιώσεις το GNS3 χρησιμοποιεί τους ακόλουθους προσομοιωτές για οποιοδήποτε λειτουργικό σύστημα :

- Dynamips είναι ο κλασσικός προσομοιωτής που χρησιμοποιείτε σε μηχανήματα CISCO IOS
- VirtualBox είναι ένας παραδοσιακός προσομοιωτής λειτουργικών συστημάτων, που παρέχετε μέσω της εταιρείας ORACLE
- Qemu είναι ένας ανοιχτού τύπου προσομοιωτής για τα firewall της cisco (cisco asa , pix , ids)

Για να μπορέσουμε να χρησιμοποιήσουμε τα (εικονικά) μηχανήματα της cisco, με σκοπό την προσομοίωση του δικτύου μας, θα πρέπει να αναζητήσουμε **ios images** για **routers**, **switches**, **firewalls** της cisco, πραγματοποιώντας αναζήτηση στο διαδίκτυο και να τα εγκαταστήσουμε στο λογισμικό.



Εικόνα 4.1 Αρχική οθόνη GNS3

Στην συνέχεια, ακολουθείται ένας συγκεκριμένος τρόπος με τον οποίο μπορούμε να εγκαταστήσουμε τα images των συσκευών στην συγκεκριμένη εφαρμογή και τον οποίο θα αναλύσουμε παρακάτω.

4.1.2 Τρόπος εγκατάστασης ενός router σε περιβάλλον GNS3

Παρακάτω θα αναλύσουμε σε μερικά βήματα τον τρόπο εγκατάστασης ενός ios image και συγκεκριμένα του router C7200.

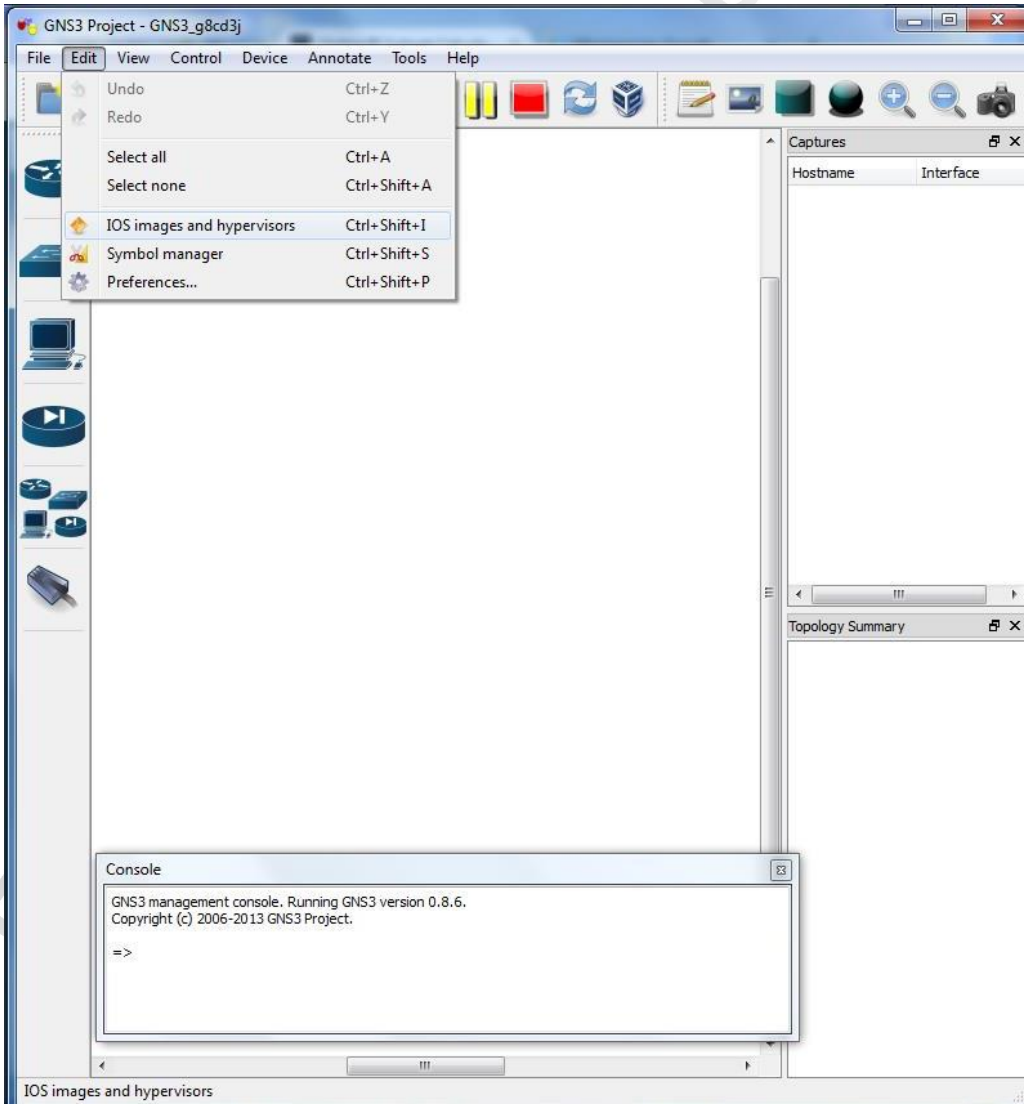
1. Πρώτα πραγματοποιούμε αναζήτηση για το συγκεκριμένο ios image χρησιμοποιώντας λέξεις – κλειδιά :

   ios image,

   router c7200 ios image,

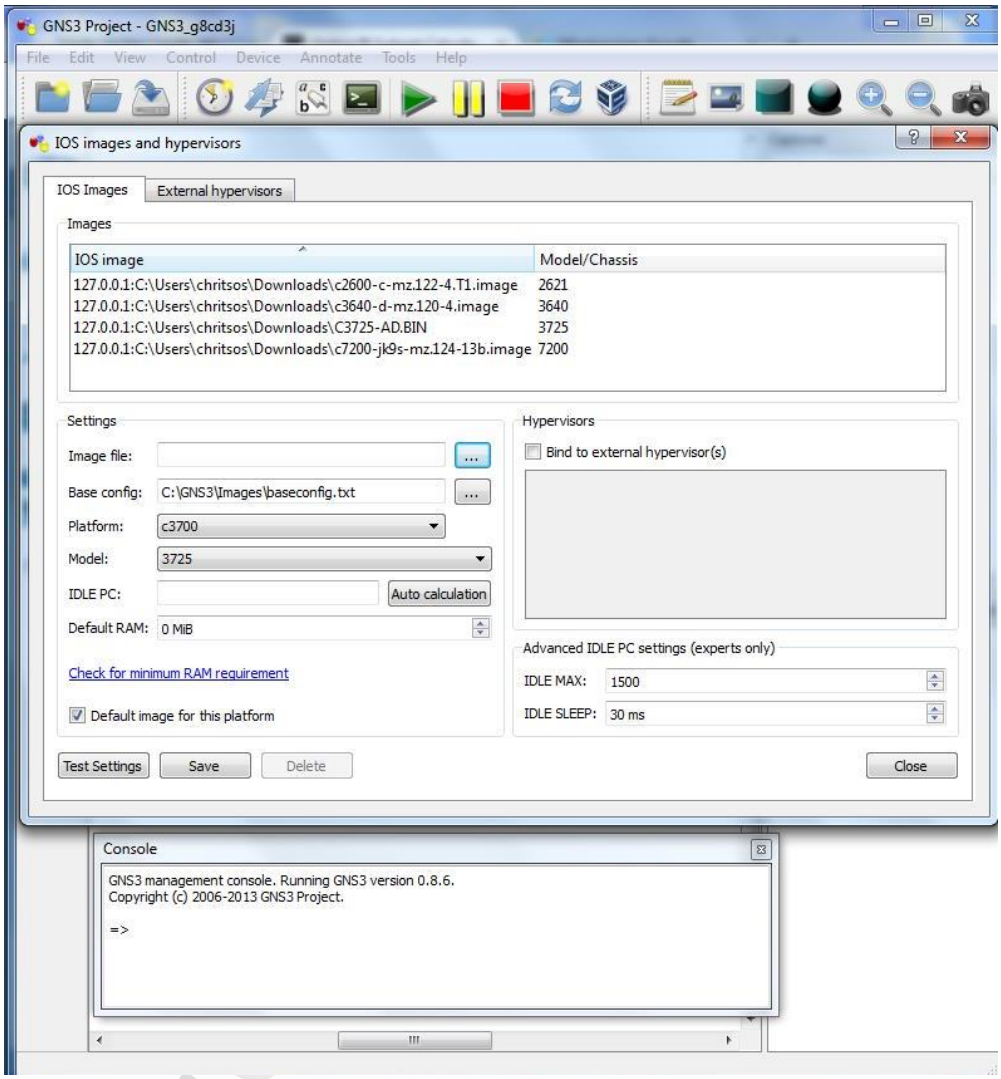
   ios images gns3

2. Αφού βρούμε το ios image που μας ενδιαφέρει , πραγματοποιούμε λήψη στον υπολογιστή μας και εισερχόμαστε στο περιβάλλον του λογισμικού μας.



Εικόνα 4.2 εύρεση του image που θέλουμε να εγκαταστήσουμε

3. Μας εμφανίζετε ένα παράθυρο , όπου από εκεί θα μπορέσουμε να εισάγουμε το image που θέλουμε πηγαίνοντας στο πεδίο ***settings*** και επιλέγοντας το ***image file***



Εικόνα 4.3 Εεπιλογή του συγκεκριμένου image file προς εγκατάσταση

Επιλέγουμε τις ρυθμίσεις που επιθυμούμε επιλέγοντας ***Platform*** , ***Model*** και ***Default RAM*** και τις ελέγχουμε με το ***Test settings***. Στην συνέχεια πατάμε το κουμπί ***Save***.

4.1.3 Τρόπος εγκατάστασης ενός Firewall σε περιβάλλον GNS3

Με την ίδια περίπου λογική πραγματοποιούμε και την εγκατάσταση ενός IOS IMAGE σε firewall συστήματα.

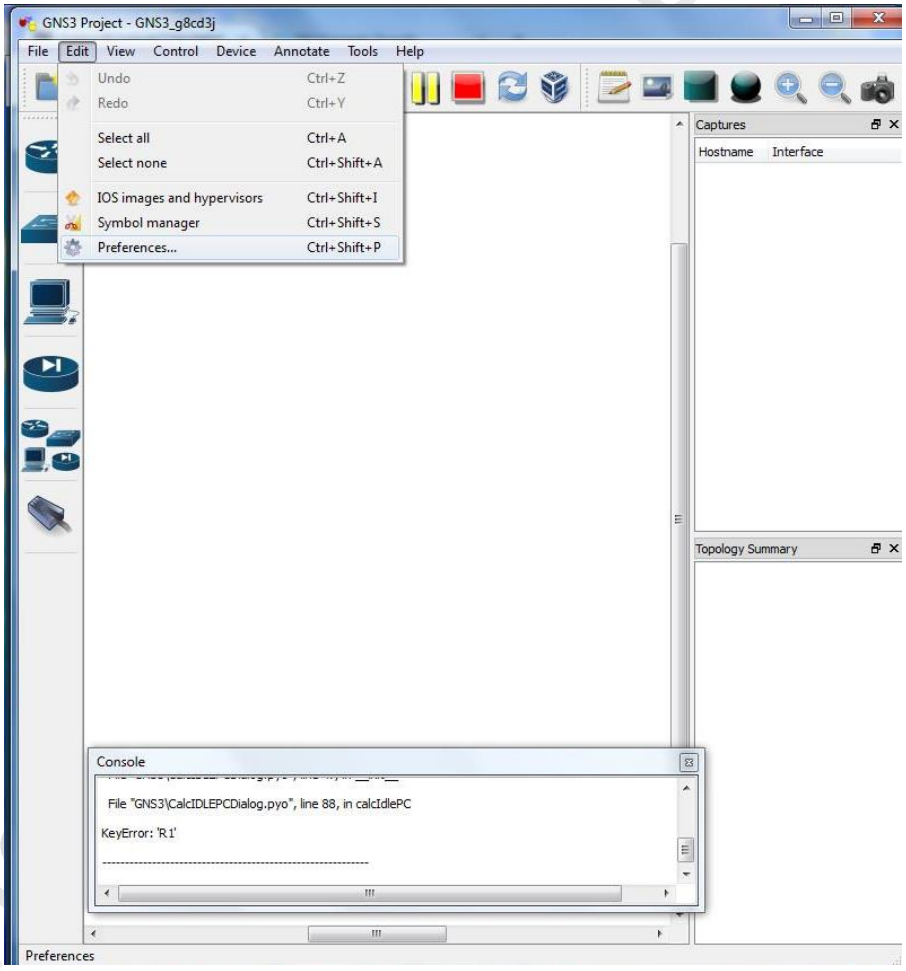
1. Πρώτα πραγματοποιούμε αναζήτηση για το συγκεκριμένο ios image χρησιμοποιώντας λέξεις – κλειδιά :

   ios image,

   pix firewall ios image,

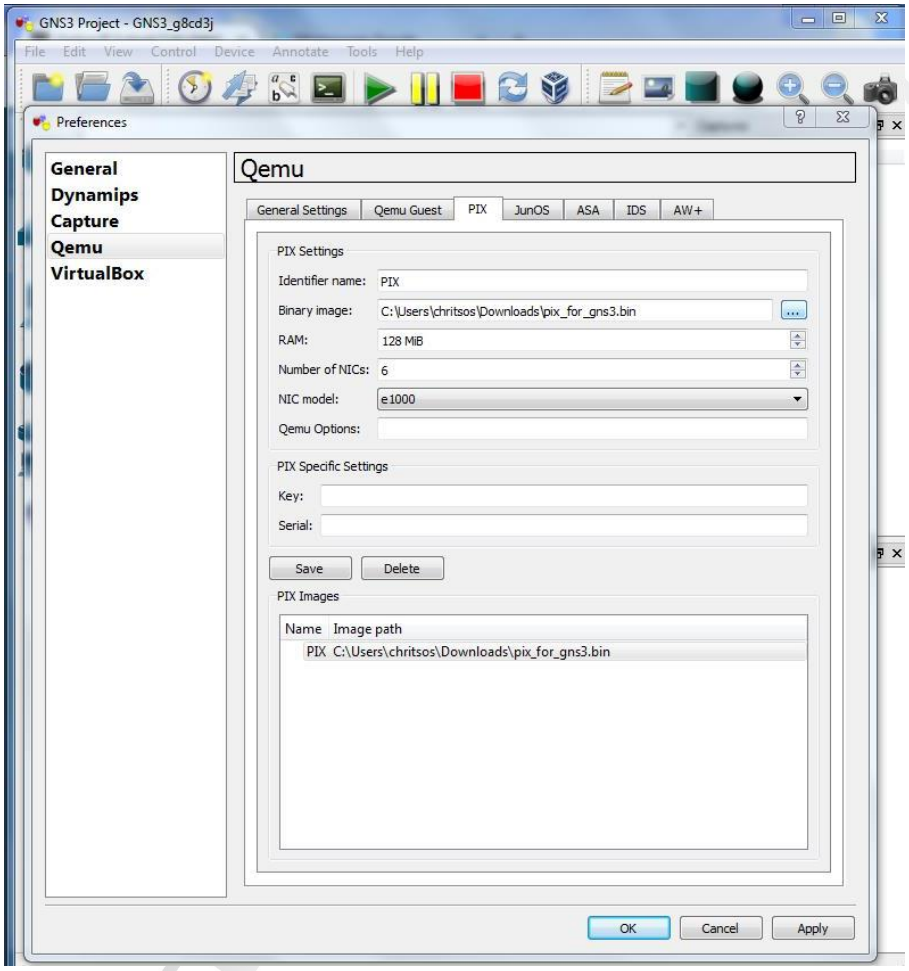
   ios images gns3

2. Αφού βρούμε το ios image που μας ενδιαφέρει , πραγματοποιούμε λήψη στον υπολογιστή μας και εισερχόμαστε στο περιβάλλον του λογισμικού μας.



Εικόνα 4.4 Εύρεση του image που θέλουμε να εγκαταστήσουμε

3. Μας εμφανίζετε ένα παράθυρο , όπου από εκεί θα μπορέσουμε να εισάγουμε το image που θέλουμε πηγαίνοντας στο πεδίο ***Qemu*** και στην συνέχεια στην καρτέλα ***PIX*** και συγκεκριμένα στο ***Binary image*** αναζητώντας το αρχείο με την κατάληξη .bin



Εικόνα 4.5 Βασικές ρυθμίσεις του Firewall

4 Εισάγουμε το όνομα με το οποίο θέλουμε να εμφανίζετε το firewall μας.

5. Εισάγουμε την ποσότητα της RAM που θέλουμε να χρησιμοποιήσουμε για το συγκεκριμένο μηχάνημα (στην δική μας περίπτωση χρησιμοποιούμε 1024 Mbit)

6. Εισάγουμε τον αριθμό των καρτών δικτύου

7. Καθώς και το μοντέλο των καρτών του δικτύου (Στην δική μας περίπτωση e1000)

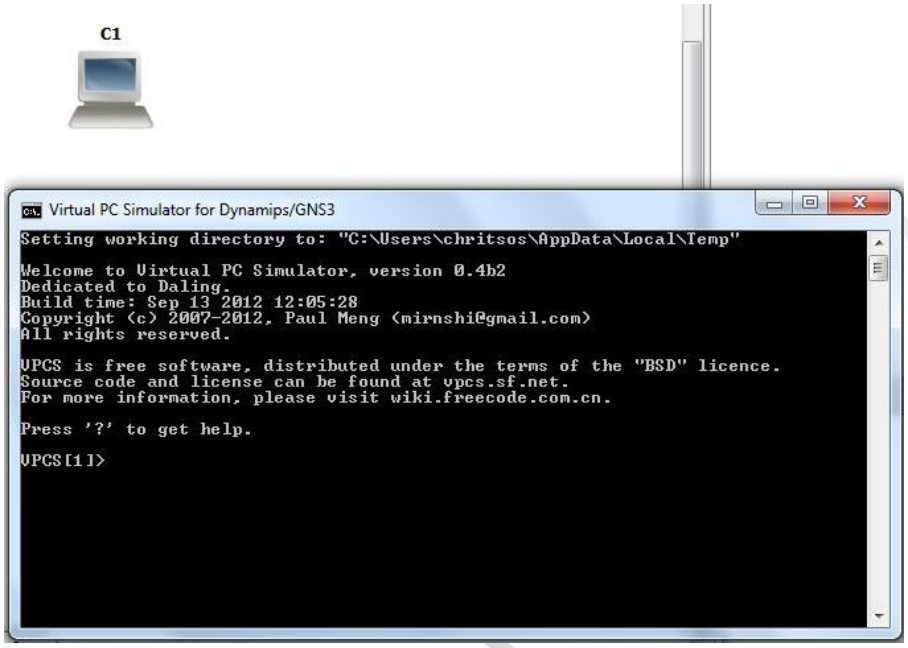
8. Πατώντας το κουμπί Apply και στην συνέχεια το OK αποθηκεύουμε την συγκεκριμένη ρύθμιση και το firewall είναι έτοιμο προς χρήση.

4.1.4 Πρόσθεση Host στην τοπολογία μέσω του Virtual PC Simulator

Περισσότερες πληροφορίες για την πρόσθεση απλών τερματικών συσκευών μπορείτε να βρείτε εδώ.
Το Virtual PC Simulator είναι ένα πρόγραμμα το οποίο μπορεί να εκτελεστεί σε Windows και Linux Περιβάλλον. Χρησιμοποιείται κυρίως για τον έλεγχο σε icmp πακέτα (Ping) και σε Traceroute λειτουργία.
Το πλεονέκτημα που προσφέρει η συγκεκριμένη εφαρμογή είναι ότι με την χρησιμοποίηση της θα μπορούμε να γλυτώσουμε μνήμη και επεξεργασία (CPU) σε σύγκριση με άλλα πιο απαιτητικά τερματικά που χρησιμοποιούνται όπως VirtualBoxes.
Είναι δωρεάν λογισμικό και μπορείτε να το κατεβάσετε από εδώ.
Για τους χρήστες που χρησιμοποιούν λειτουργικό σύστημα Windows, θα αναλύσουμε σε μερικά βήματα τον τρόπο χρησιμοποίησης του.

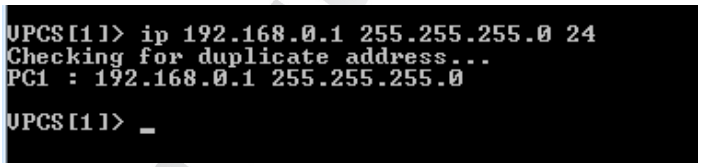
5 Κατεβάζουμε την συγκεκριμένη εφαρμογή από την τοποθεσία http://www.gns3.net/download/. Επιλέγοντας τον τύπο της εφαρμογής που ταιριάζει στα χαρακτηριστικά τα οποία αναζητούμε

6 Μετά την λήψη αυτού που βρίσκετε σε συμπιεσμένη μορφή τον αποσυμπιέζουμε σε μία θέση στον δίσκο και εκτελούμε το vpcs.exe

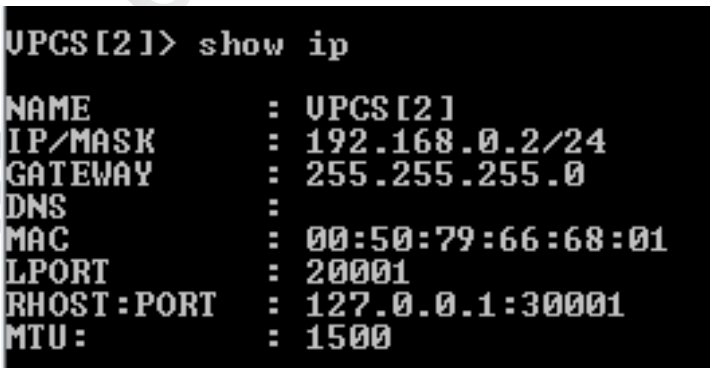


Εικόνα 4.6 Η γραμμή εντολών (cmd) του τερματικού

7 Απόδοση διεύθυνσης στον Host C1



8 Έλεγχος απόδοσης διεύθυνσης



4.2 Διαχείριση της κυκλοφορίας του Δικτύου, με λίστες πρόσβασης (ACL)

Οι λίστες πρόσβασης, ACL's περιγράφουν ένα σύνολο κυκλοφορίας, από ένα κεντρικό υπολογιστή ή δίκτυο και απαριθμούν μια δράση για την εφαρμογή της εν λόγω κίνησης, επιτρέποντας ή απορρίπτοντας. Όταν ένα πακέτο υποβάλλεται σε λίστα ελέγχου πρόσβασης , οι συσκευές Cisco Security Appliance αναζητούν αυτή την συνδεδεμένη λίστα, ώστε να βρεθεί και να ταιριάξει με το πακέτο. Η πρώτη ACL που ταιριάζει με τη συσκευή ασφάλειας είναι αυτή που εφαρμόζεται στο πακέτο.

Μόνο μία λίστα πρόσβασης επιτρέπεται ανά interface , ανά κατεύθυνση . Αυτό σημαίνει ότι μπορεί να υπάρχει μόνο μία λίστα πρόσβασης που ισχύει για την εισερχόμενη κίνηση σε μια διασύνδεση και μία λίστα πρόσβασης που ισχύει για εξερχόμενη κυκλοφορία σε μια διασύνδεση. Λίστες πρόσβασης που δεν εφαρμόζονται με διεπαφές , όπως NAT ACLs , είναι απεριόριστες .

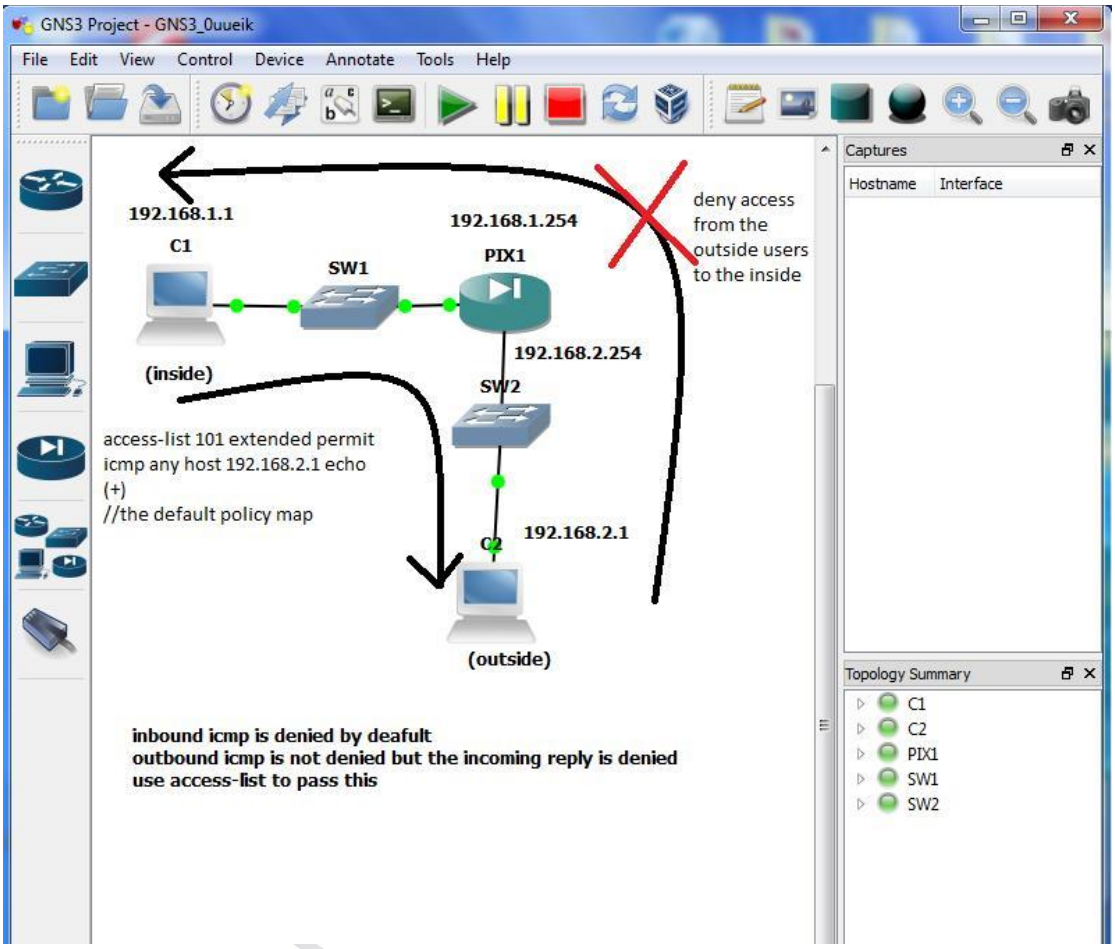
Σημείωση : Από προεπιλογή, όλες οι λίστες πρόσβασης έχουν μια σιωπηρή ACL στο τέλος που αρνείται όλη την κυκλοφορία, έτσι ώστε το σύνολο της κίνησης που δεν ταιριάζει με κανένα ACL που εισάγετε στη λίστα πρόσβασης να ταιριάζει με την σιωπηρή άρνηση στο τέλος και να απορριφτεί. Θα πρέπει να υπάρχει τουλάχιστον μία δήλωση άδειας σε μια λίστα πρόσβασης διεπαφής για την ροή της κυκλοφορίας. Χωρίς μια permit άδεια, όλη η κυκλοφορία θα απορρίπτεται.

Σημείωση : Η Access-list υλοποιείται με την access -list και εντολές πρόσβαση της ομάδας (access-group).

Για να μπορέσουμε να κατανοήσουμε την εφαρμογή της λίστας πρόσβασης σε ένα δίκτυο, θα εφαρμόσουμε ορισμένα σενάρια.

4.2.1 Δυνατότητα πρόσβασης από τους εσωτερικούς χρήστες του δικτύου (inside users), προς τους εξωτερικούς χρήστες του δικτύου (outside users).

Για το συγκεκριμένο σενάριο έχουμε κατασκευάσει το ακόλουθο σχήμα

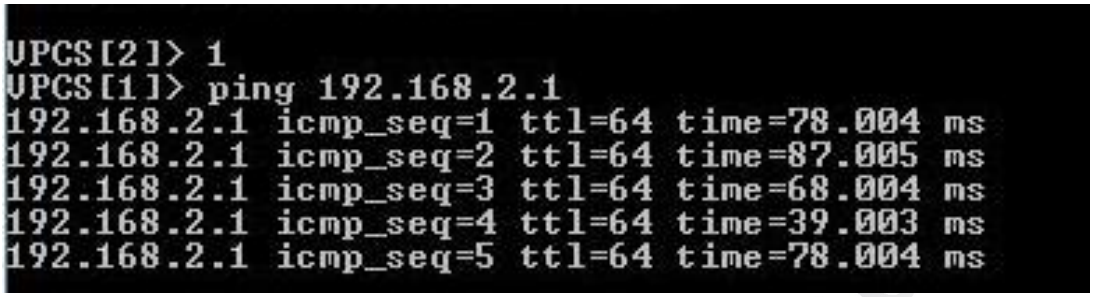


Εικόνα 4.7 Λίστα πρόσβασης από τους εσωτερικούς χρήστες προς τους εξωτερικούς χρήστες

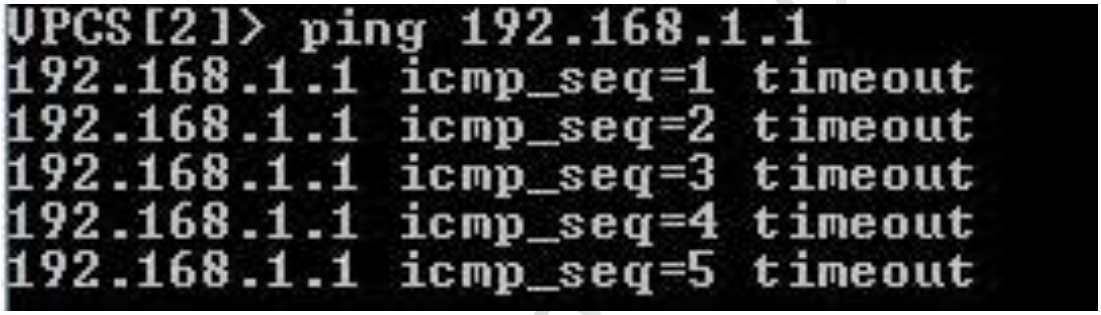
Σε αυτή την περίπτωση, όπως μπορούμε να διακρίνουμε ο εσωτερικός χρήστης του δικτύου, μέσω access-list έχει την δυνατότητα να μπορεί να κάνει ping , δηλαδή να στείλει icmp πακέτα προς τον εξωτερικό χρήστη (outside) του δικτύου.
Από την άλλη πλευρά ο εξωτερικός χρήστης δεν μπορεί να πραγματοποιήσει την ίδια ενέργεια καθώς δεν του έχουμε την δυνατότητα αυτή.

Επιβεβαίωση

1. Από τον εσωτερικό χρήστη προς τον εξωτερικό

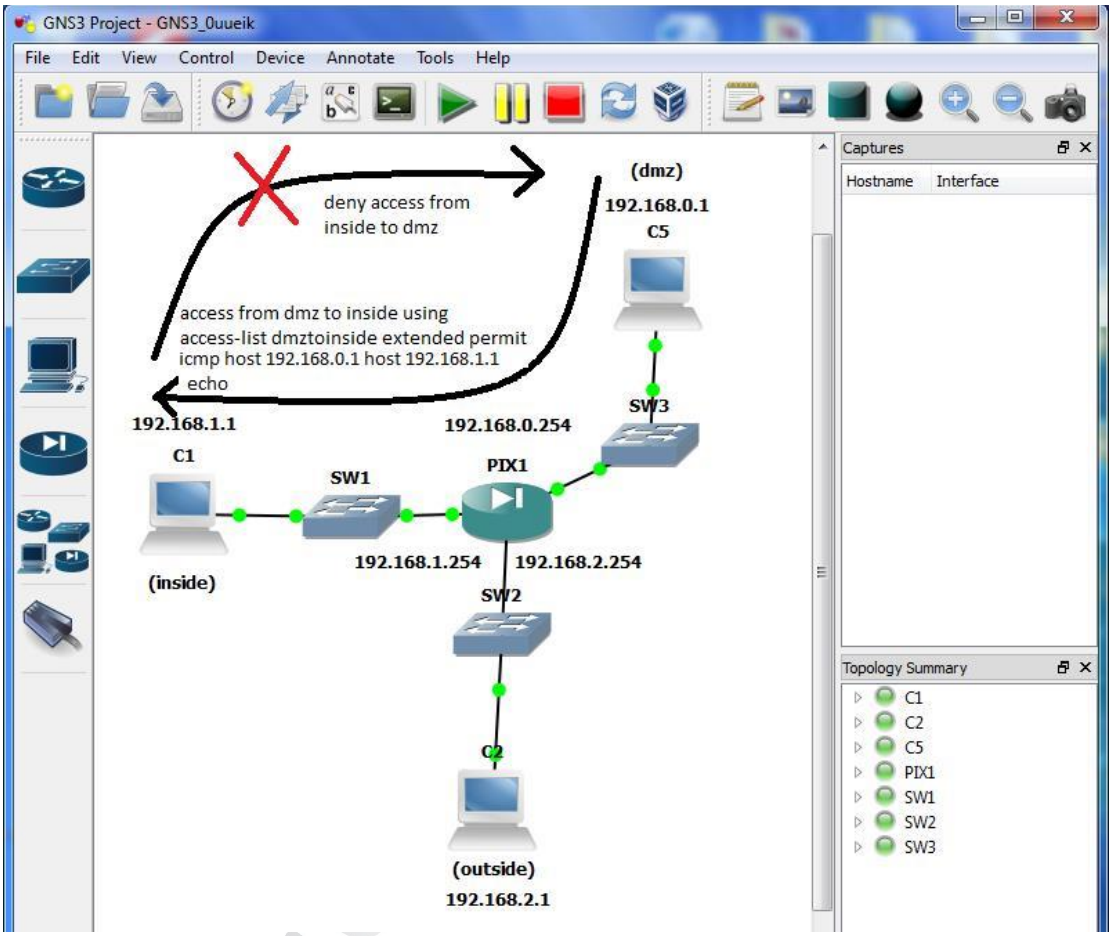


2. Από τον εξωτερικό χρήστη προς τον εσωτερικό



4.2.2 Δυνατότητα πρόσβασης από τους χρήστες του δικτύου (dmz users), προς τους εσωτερικούς χρήστες του δικτύου (inside users).

Για το συγκεκριμένο σενάριο έχουμε κατασκευάσει το ακόλουθο σχήμα



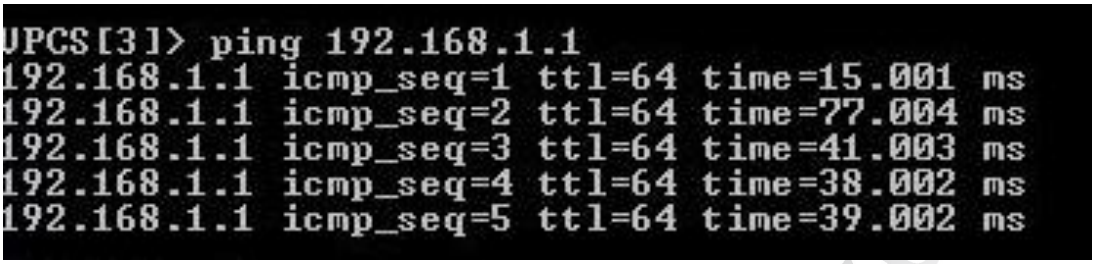
Εικόνα 4.8 Λίστα πρόσβασης από τους χρήστες DMZ προς τους εξωτερικούς χρήστες

Σε αυτή την περίπτωση, όπως μπορούμε να διακρίνουμε ο χρήστης dams του δικτύου , μέσω access-list έχει την δυνατότητα να μπορεί να κάνει ping , δηλαδή να στείλει imp πακέτα προς τον εσωτερικό χρήστη (inside) του δικτύου.

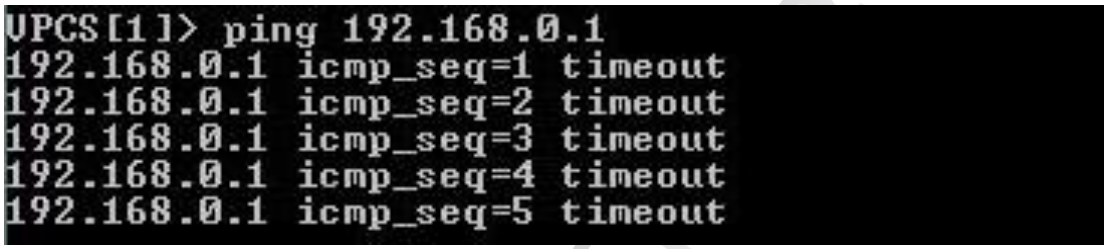
Από την άλλη πλευρά ο εσωτερικός χρήστης δεν μπορεί να πραγματοποιήσει την ίδια ενέργεια καθώς δεν του έχουμε δώσει την δυνατότητα πρόσβασης.

Επιβεβαίωση

1. Από τον χρήστη DMZ προς τον εσωτερικό χρήστη



2. Από τον εσωτερικό χρήστη προς τον DMZ



4.3 Χρησιμοποίηση της τεχνολογίας VPN (Virtual Private Networks), με την χρήση IPsec και με ISAKMP προτύπων.

Το Tunnelling protocol είναι ένα πρωτόκολλο επικοινωνίας, που χρησιμοποιείται για την επίτευξη μίας σύνδεσης μεταξύ ενός VPN δικτύου και ενός χρήστη απομακρυσμένης πρόσβασης. Η επικοινωνία αυτή επιτυγχάνετε πάνω από ένα TCP/IP δίκτυο.
Η συσκευές που χρησιμοποιούνται για την πραγματοποίηση της ασφάλειας (όπως είναι τα router), χρησιμοποιούν τα IPsec και τα ISAKMP πρότυπα. Η διαδικασία με την οποία επιτυγχάνετε η σύνδεση είναι η εξής:

- Η ρύθμιση του tunnel πρωτοκόλλου
- Η εγκαθίδρυση μίας tunnel σύνδεσης
- Η αυθεντικοποίηση των χρηστών και των δεδομένων, που θα αποσταλούν
- Η διαχείριση των ασφαλή κλειδιών
- Η κρυπτογράφηση και η αποκρυπτογράφηση των δεδομένων
- Η διαχείριση του ρυθμού μεταφοράς των δεδομένων μέσω του ασφαλούς καναλιού (tunnel)
- Η διαχείριση του ρυθμού μεταφοράς των δεδομένων, τόσο των εισερχόμενων όσο και των εξερχόμενων.

Κατά την εγκαθίδρυση μίας σύνδεσης ασφαλούς καναλιού (tunnel), οι χρήστες που συμμετέχουν πραγματοποιούν αμοιβαίες ρυθμίσεις. Αυτές οι ρυθμίσεις χωρίζονται σε 2 κατηγορίες:

1. Την εγκαθίδρυση του ασφαλούς καναλιού (IKE SA)
2. Την ασφαλή κυκλοφορία των δεδομένων μέσω του καναλιού αυτού (IPsec SA)

Μέσω του προτύπου IPsec σε LAN – to – LAN συνδέσεις οι συσκευές (router's), που συμμετέχουν μπορούν να χρησιμοποιηθούν και ως αποστολείς αλλά και ως δέκτες.

Σε client – to –LAN συνδέσεις οι συσκευές χρησιμοποιούνται όμως μόνο ως παραλήπτες.

Το ISAKMP πρωτόκολλο, χρησιμοποιείται για την ανταλλαγή κλειδιών πριν την εγκατάσταση της σύνδεσης.

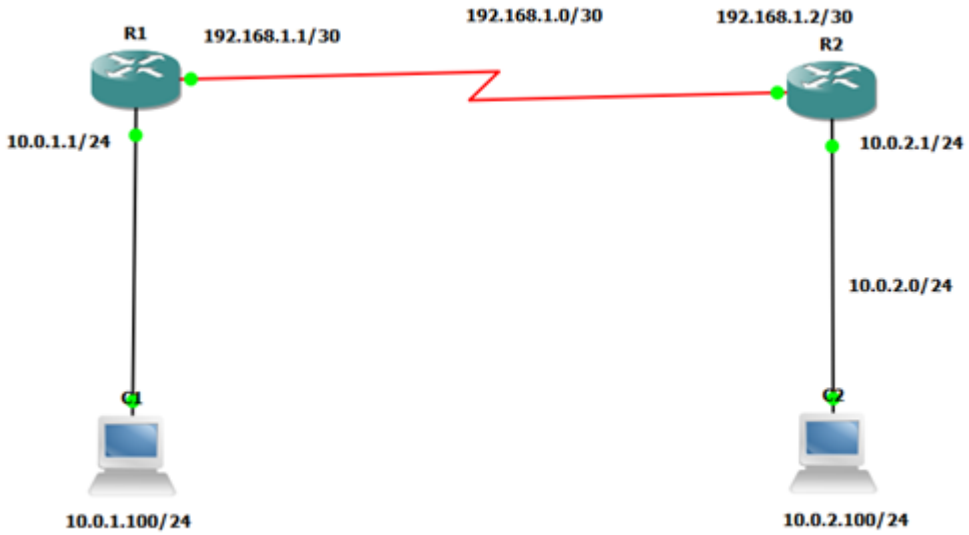
Ο συνδυασμός του πρωτοκόλλου IPsec σε συνδυασμό με το ISAKMP πρωτόκολλο κάνει την VPN σύνδεση ακόμα πιο ασφαλή.

Η εφαρμογή του ISAKMP πρωτοκόλλου, στηρίζετε στην πολιτική που θα εφαρμόσουμε για την λειτουργία του πρωτοκόλλου αυτού η οποία περιλαμβάνει:

- Μέθοδος αυθεντικοποίησης, για την διασφάλιση των αναγνωσιμότητας των χρηστών
- Μέθοδος κρυπτογράφησης για την προστασία των δεδομένων κατά την μετάδοση τους.
- Μέθοδος αυθεντικοποίησης μηνύματος μέσω συνάρτησης κατακερματισμού δεδομένων (hash), HMAC (Hashed Message Authentication Codes), η οποία εκτός από την ταυτοποίηση των χρηστών, πιστοποιεί ότι το μήνυμα που παρελήφθη δεν έχει τροποποιηθεί κατά την διάρκεια μετάδοσης του.
- Χρησιμοποίηση του πρωτοκόλλου Diffie – Hellman για την ασφαλή μετάδοση των κλειδιών.
- Την ρύθμιση (time limit) του χρόνου χρησιμοποίησης των κλειδιών, πριν την αντικατάσταση τους.

4.4 Εφαρμογή της πολιτικής ISAKMP σε περιβάλλον προσομοίωσης GNS3

Έστω ότι έχουμε το ακόλουθο σχήμα, στο οποίο θέλουμε να εφαρμόσουμε την πολιτική ISAKMP, με σκοπό την εγκαθίδρυση μιας VPN σύνδεσης.



Εικόνα 4.9 Εφαρμογή πολιτικής ISAKMP, μεταξύ 2 router

Παρακάτω δίνονται οι ρυθμίσεις IOS που έχουν πραγματοποιηθεί για τον δρομολογητή R1.

Σελίδα (1/3)

```
R1#show run
Building configuration...

Current configuration : 1609 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
no ip icmp rate-limit unreachable
!
!
ip cef
no ip domain lookup
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
ip tcp synwait-time 5
!
!
crypto isakmp policy 10
 encr aes 256
 authentication pre-share
 group 5
```

Εικόνα 4.10 Ρυθμίσεις IOS του δρομολογητή R1 (1/3)

```
 lifetime 3600
crypto isakmp key my_key_preshared address 192.168.1.2
crypto isakmp keepalive 10 periodic
!
!
crypto ipsec transform-set myset esp-aes 256 esp-sha-hmac
!
crypto map r1_to_r2 10 ipsec-isakmp
 set peer 192.168.1.2
 set transform-set myset
 match address 101
!
!
!
!
interface FastEthernet0/0
 ip address 10.0.1.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial1/0
 ip address 192.168.1.1 255.255.255.252
 serial restart-delay 0
 crypto map r1_to_r2
!
interface Serial1/1
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial1/2
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial1/3
 no ip address
 shutdown
 serial restart-delay 0
!
ip route 0.0.0.0 0.0.0.0 192.168.1.2
```

Εικόνα 4.11 Ρυθμίσεις IOS του δρομολογητή R1 (2/3)

```
ip route 10.0.1.0 255.255.255.0 192.168.1.2
!
no ip http server
no ip http secure-server
!
!
access-list 101 permit ip 10.0.2.0 0.0.0.255 10.0.1.0 0.0.0.255
!
!
!
!
control-plane
!
!
!
!
!
!
gatekeeper
 shutdown
!
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line vty 0 4
 login
!
!
end
```

Εικόνα 4.12 Ρυθμίσεις IOS του δρομολογητή R1 (3/3)

Όπως βλέπουμε από τις ρυθμίσεις, η πολιτική ISAKMP έχει τις εξής ρυθμίσεις:

- Κρυπτογράφηση του συγκεκριμένου πρωτοκόλλου, μέσω του αλγορίθμου κρυπτογράφησης AES με συμμετρικό κλειδί 256 bits
- Αυθεντικοποίηση των χρηστών μέσω προ – συμφωνημένων κλειδιών (pre-shared). Τα κλειδιά αυτά αποτελούν μία default διαδικασία, κατάλληλα για μικρά δίκτυα. Για μεγαλύτερα όμως δίκτυα, προτείνετε η χρησιμοποίηση της εντολής **authentication crack**, η οποία παρέχει δυνατότερη αυθεντικοποίηση, των χρηστών και υποστηρίζετε μέσω της χρήσης RADIUS server.
- Η εντολή group, αναφέρετε συγκεκριμένα στο πρωτόκολλο ανταλλαγής κλειδιών Diffie – Hellman, όπου οι 2 IPSec χρήστες χρησιμοποιούν για να μεταδώσουν ένα κοινό μυστικό κλειδί, χωρίς να χρειάζεται να είναι προ – συμφωνημένο. Στην περίπτωση μας, η κρυπτογράφηση AES πρέπει να υποστηρίζετε από Diffie – Hellman group 5.

```
crypto isakmp policy 10
 encr aes 256
 authentication pre-share
 group 5
```

- Η εντολή **crypto isakmp policy lifetime 3600,** καθορίζει τον χρόνο ζωής του πρωτοκόλλου ISAKMP σε 3600 sec. Ο default χρόνος ζωής του πρωτοκόλλου είναι 86400 sec ή 24 ώρες. Όσο μικρότερος είναι ο χρόνος ζωής του πρωτοκόλλου τόσο πιο ασφαλής θεωρείται η κρυπτογράφηση.
- Η εντολή **crypto isakmp key my_key_preshared address 192.168.1.2,** καθορίζει τον κωδικό **my_key_preshared,** που χρησιμοποιεί ο απομακρυσμένος χρήστης, με διεύθυνση 192.168.1.2 για μετάδοση ISAKMP πληροφορίας.
- Η εντολή **crypto isakmp keepalive 10 periodic,** επιτρέπει στην gateway να στέλνει DPD (Dead Peer Detection) μηνύματα προς τον άλλο χρήστη. Έτσι με αυτό τον τρόπο πιστοποιεί την ύπαρξη της ζωντάνιας τις σύνδεσης ανά τακτά χρονικά διαστήματα. Χρησιμοποιείται για τον έγκαιρο εντοπισμό μίας σύνδεσης η οποία πιθανών να μην βρίσκετε σε λειτουργία.

```
 lifetime 3600
crypto isakmp key my_key_preshared address 192.168.1.2
crypto isakmp keepalive 10 periodic
```

Το crypto map αποτελεί μια ρύθμιση του configuration το οποίο εκτελεί 2 βασικές λειτουργίες. Στην πρώτη λειτουργία επιλέγει δεδομένα τα οποία χρειάζονται ασφάλεια. Κατά την δεύτερη λειτουργία, προσδιορίζει τα πολιτική που θα εφαρμόσει στα δεδομένα αυτά, και το τερματικό στο οποίο θα εφαρμόσει την κυκλοφορία.

Το crypto map εφαρμόζετε επάνω σε διασυνδέσεις. Αποτελεί επέκταση της τεχνικής IPsec.

- Η εντολή **crypto ipsec transform-set myset esp-aes 256 esp-sha-hmac,** χρησιμοποιείτε για την μετατροπή των δεδομένων κατά την μετάδοση τους με μέθοδο κρυπτογράφησης και μέθοδο αυθεντικοποίησης. Για παράδειγμα στην συγκεκριμένη εντολή που έχουμε ορίσει η μέθοδος κρυπτογράφησης που χρησιμοποιείται είναι η esp-aes-256 και η μέθοδος αυθεντικοποίησης είναι η esp-sha-hmac, η οποία είναι και η default μέθοδος.
- Η επόμενη εντολή καθορίζει την πολιτική που θα εφαρμοστεί στην **crypto map r1_to_r2** και αυτή είναι η πολιτική **10** εφαρμόζωντας το πρωτόκολλο **ipsec-isakmp**.
- Στην συνέχεια καθορίζουμε τον γειτονικό κόμβο, ο οποίος είναι ο **192.168.1.2**
- Καθορίζουμε το transform-set που θα χρησιμοποιήσουμε με την ονομασία **myset**
- Και τέλος καθορίζουμε την λίστα ελέγχου πρόσβασης που έχουμε θέσει παραπάνω στο configuration του δρομολογητή.

```
crypto ipsec transform-set myset esp-aes 256 esp-sha-hmac
!
crypto map r1_to_r2 10 ipsec-isakmp
 set peer 192.168.1.2
 set transform-set myset
 match address 101
```

Ομοίως έχουν πραγματοποιηθεί ρυθμίσεις IOS αντίστοιχα και στον δρομολογητή R2 του σχήματος.

Για να μπορέσουμε να βεβαιωθούμε ότι, έχει πραγματοποιηθεί σωστά η εγκαθίδρυση και η λειτουργία της IPsec, μέσω ISAKMP πολιτικής, μπορούμε να το ελέγξουμε με τις παρακάτω εντολές.

- **Show crypto isakmp key**: εμφάνιση των κλειδιών που έχουν χρησιμοποιηθεί κατά την εφαρμογή της ISAKMP και εμφάνιση των διασυνδέσεων που υπάρχουν στον Router.

```
R1#show crypto isakmp key
Keyring              Hostname/Address                 Preshared Key

default              192.168.1.2                      my_key_preshared
R1#show ip int brief
Interface                  IP-Address      OK? Method Status                Protocol
FastEthernet0/0            10.0.1.1        YES manual up                    up
FastEthernet0/1            unassigned      YES unset  administratively down down
Serial1/0                  192.168.1.1     YES manual up                    up
Serial1/1                  unassigned      YES unset  administratively down down
Serial1/2                  unassigned      YES unset  administratively down down
Serial1/3                  unassigned      YES unset  administratively down down
```

- **Show crypto ipsec SA**: είναι εντολή που χρησιμοποιείτε για να μπορούμε να ελέγξουμε την επιτυχημένη εγκατάσταση του πρωτοκόλλου ipsec.

```
R1#show crypto ipsec sa

interface: Serial1/0
    Crypto map tag: r1_to_r2, local addr 192.168.1.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (10.0.2.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (10.0.1.0/255.255.255.0/0/0)
   current_peer 192.168.1.2 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
    #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 192.168.1.1, remote crypto endpt.: 192.168.1.2
     path mtu 1500, ip mtu 1500, ip mtu idb Serial1/0
     current outbound spi: 0x0(0)

     inbound esp sas:

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:

     outbound ah sas:

     outbound pcp sas:
```

- **debug crypto isakmp, debug crypto ipsec:** χρησιμοποιούνται για να ελέγξουμε εάν τα πρωτόκολλα isakmp και ipsec, είναι ενεργοποιημένα.

```
R1#debug crypto isakmp
Crypto ISAKMP debugging is on
R1#debug crypto ipsec
Crypto IPSEC debugging is on
```

- **show crypto map:** εμφανίζει το crypto map που υπάρχει στο δίκτυο.

```
R1#show crypto map
Crypto Map "r1_to_r2" 10 ipsec-isakmp
        Peer = 192.168.1.2
        Extended IP access list 101
            access-list 101 permit ip 10.0.2.0 0.0.0.255 10.0.1.0 0.0.0.255
        Current peer: 192.168.1.2
        Security association lifetime: 4608000 kilobytes/3600 seconds
        PFS (Y/N): N
        Transform sets={
                myset,
        }
        Interfaces using crypto map r1_to_r2:
                Serial1/0
```

4.4.1 προσπάθεια σύνδεσης των 2 τερματικών, μέσω icmp πακέτων

Στην συνέχεια θα ελέγξουμε, αν το τερματικό c1 της τοπολογίας, μπορεί να κάνει ping με το τερματικό c2 .

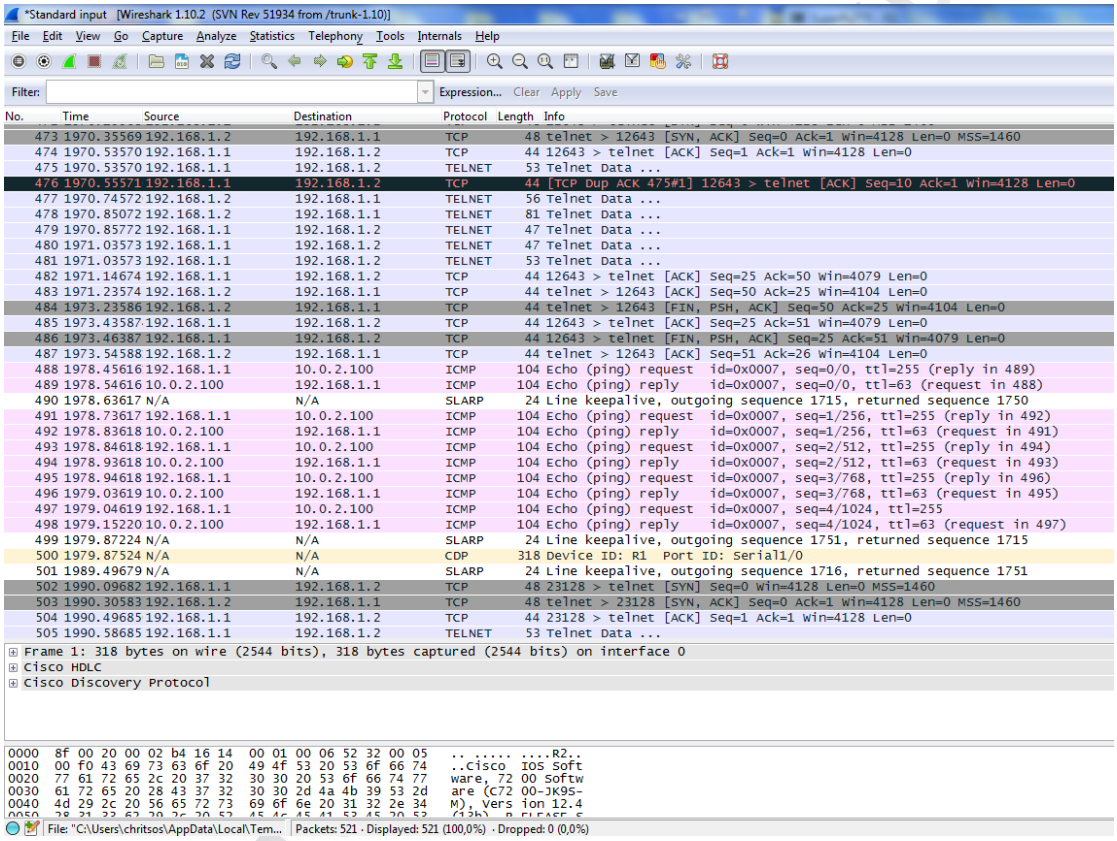
```
VPCS[1]> ping 10.0.2.100
10.0.2.100 icmp_seq=1 ttl=63 time=536.031 ms
10.0.2.100 icmp_seq=2 ttl=63 time=317.018 ms
10.0.2.100 icmp_seq=3 ttl=63 time=486.028 ms
10.0.2.100 icmp_seq=4 ttl=63 time=218.013 ms
10.0.2.100 icmp_seq=5 ttl=63 time=379.022 ms

VPCS[1]> 2
VPCS[2]> ping 10.0.1.100
10.0.1.100 icmp_seq=1 ttl=63 time=399.023 ms
10.0.1.100 icmp_seq=2 ttl=63 time=297.017 ms
10.0.1.100 icmp_seq=3 ttl=63 time=209.012 ms
10.0.1.100 icmp_seq=4 ttl=63 time=305.018 ms
10.0.1.100 icmp_seq=5 ttl=63 time=402.023 ms
```

Παρατηρούμε ότι τα 2 τερματικά μπορούν να επικοινωνήσουν κατευθείαν μέσω των δρομολογητών της τοπολογίας μας και αυτό οφείλετε στην τοπολογία που έχουμε ακολουθήσει κατά την κατασκευή της ISAKMP πολιτικής.

4.4.2 Καταγραφή κίνησης δεδομένων δικτύου με χρήση Wireshark

Για να μπορέσουμε να ελέγξουμε την κίνηση των δεδομένων του δικτύου και να πληροφορήσουμε τον διαχειριστή του για τα είδη των πακέτων που κινούνται μέσα σε αυτό, χρησιμοποιούμε το λογισμικό wireshark, το οποίο είναι εγκατεστημένο στο λογισμικό προσομοίωσης του GNS3.



Εικόνα 4.13 Έλεγχος της κίνησης των δεδομένων μέσω του wireshark

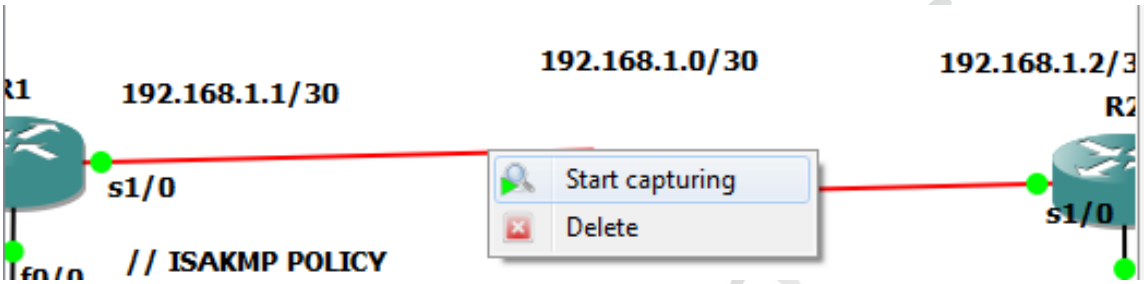
Σύμφωνα με την παραπάνω εικόνα του σχήματος, παρατηρούμε ότι τα είδη των πακέτων που κινούνται στο δίκτυο την δεδομένη χρονική στιγμή είναι τα πακέτα TCP, TELNET, ICMP και SLARP.

Τα SLARP μηνύματα είναι στην ουσία request μηνύματα που στέλνονται από τον router προς τις γειτονικές συσκευές του, ενημερώνοντας με αυτό τον τρόπο την κατάσταση των γειτονικών συσκευών του.

Για να μπορέσουμε να καταγράψουμε την κίνηση των διασυνδέσεων στην τοπολογία μας, κάνουμε τα εξής βήματα:

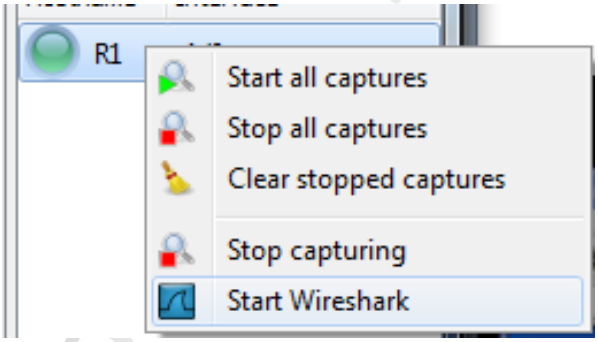
Βήμα No.1

Επιλέγουμε την Διασύνδεση που θέλουμε να παρακολουθήσουμε κάνοντας δεξί κλικ, επάνω σε αυτή.



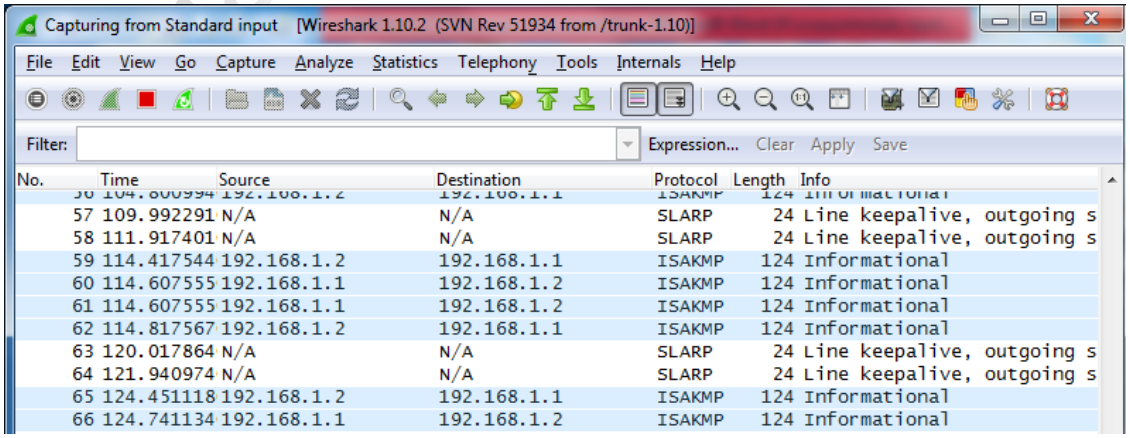
Βήμα No.2

Στην συνέχεια, επιλέγουμε την εκκίνηση της εφαρμογής wireshark.

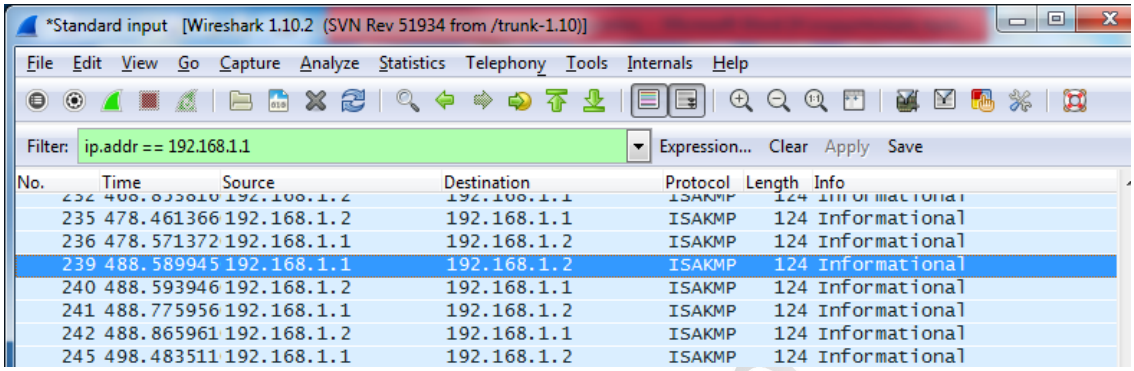


Βήμα No.3

Το wireshark, αρχίζει και καταγράφει την κίνηση των δεδομένων της συγκεκριμένης διασύνδεσης.

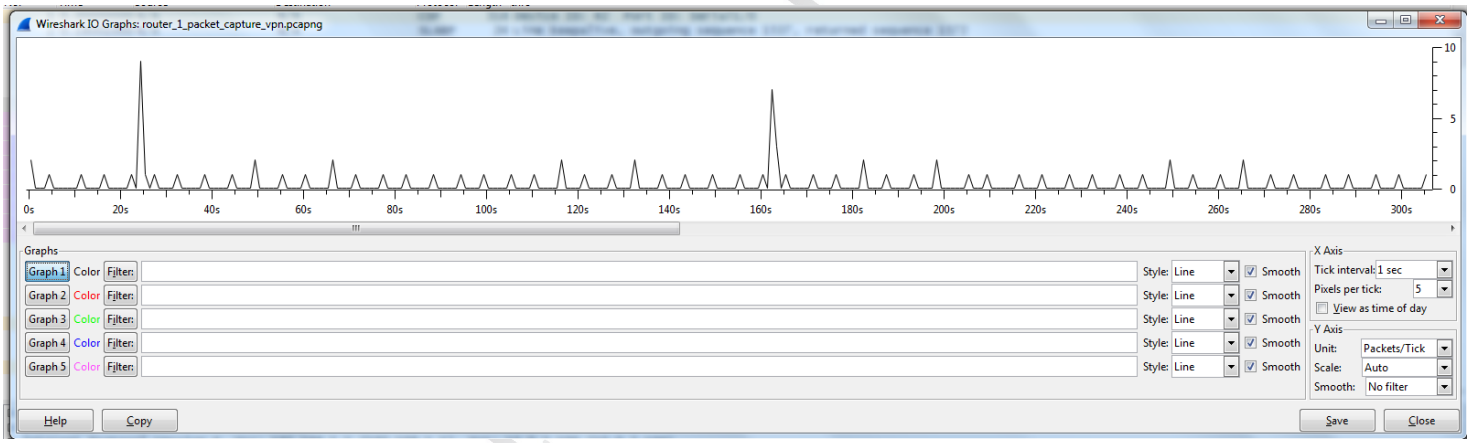


Το wireshark εκτός από την καταγραφή όλης της κίνησης της διασύνδεσης, έχει την δυνατότητα να παρακολουθήσει μία συγκεκριμένη κίνηση που επιθυμεί ο χρήστης. Για παράδειγμα, έστω ότι θέλουμε να καταγράψουμε την κίνηση της διεύθυνσης ip 192.168.1.1.



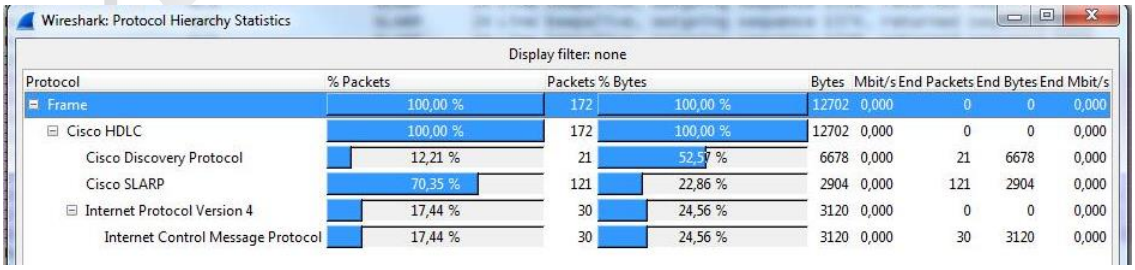
Εικόνα 4.14 Έλεγχος της κίνησης συγκεκριμένης διεύθυνσης IP

Εκτός από την καταγραφή της κίνησης δεομένων, το wireshark μπορεί να μας παρουσιάσει με γραφικό τρόπο την κίνηση του κατά την διάρκεια του χρόνου.



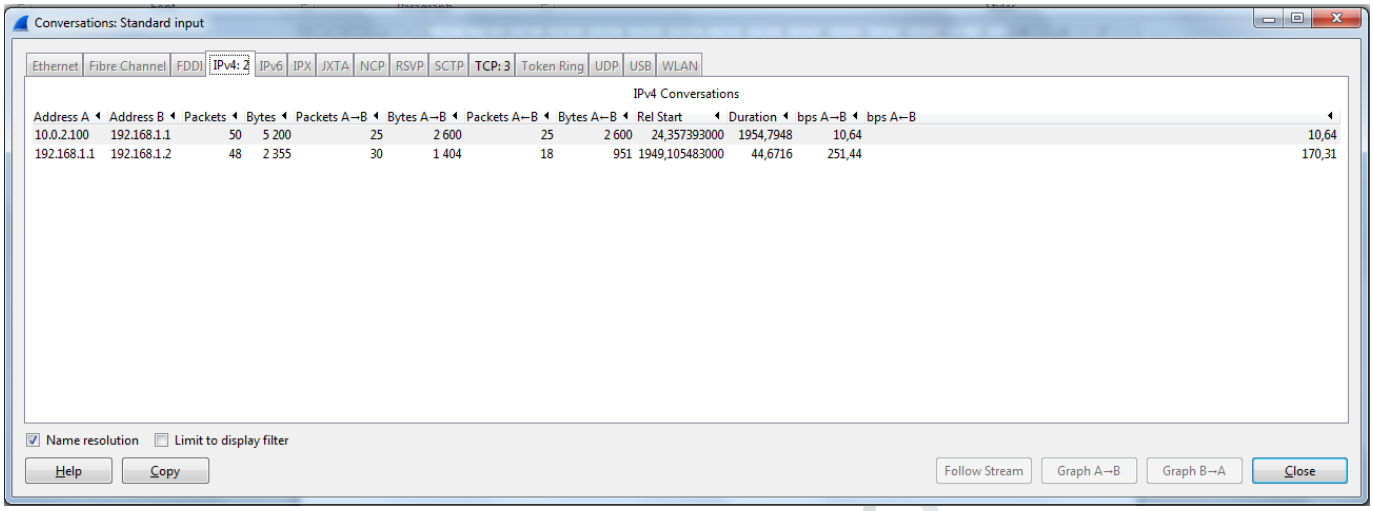
Εικόνα 4.15 Γραφική αναπαράσταση του πλήθους των πακέτων κατά την διάρκεια του χρόνου

Μπορεί να μας δείξει το πλήθος των πρωτοκόλλων που χρησιμοποιήθηκαν καθώς και το ποσοστό χρησιμοποίησης τους.

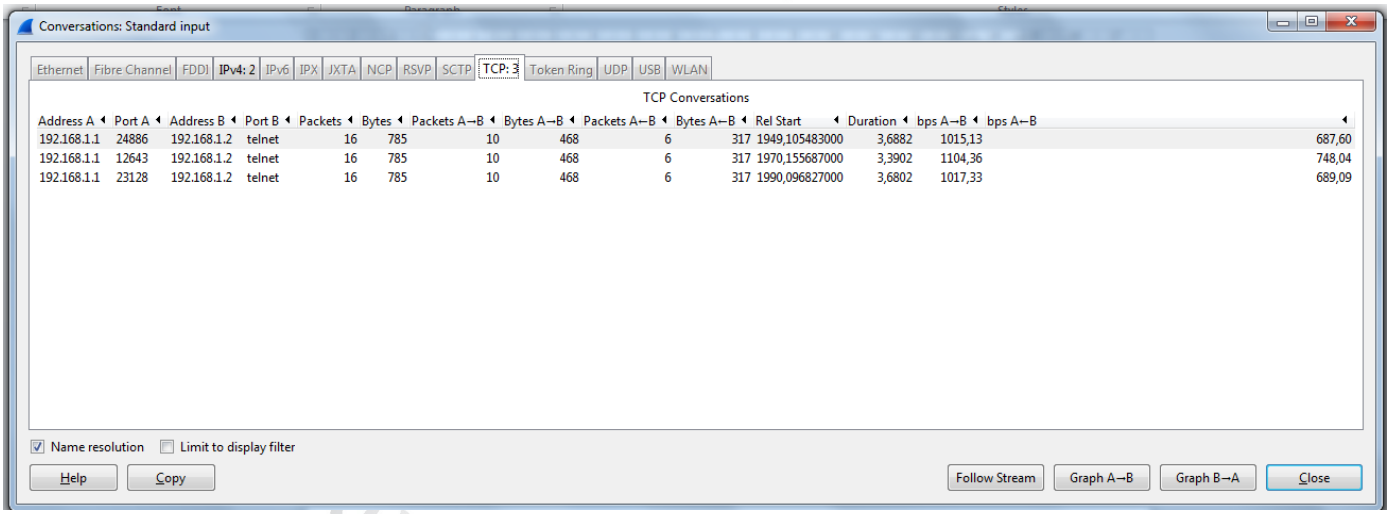


Εικόνα 4.16 καταγραφή πλήθους και ποσοστού χρησιμοποίησης πρωτοκόλλων

Το είδος των πρωτοκόλλων IPV4 που χρησιμοποιήθηκαν στο δίκτυο

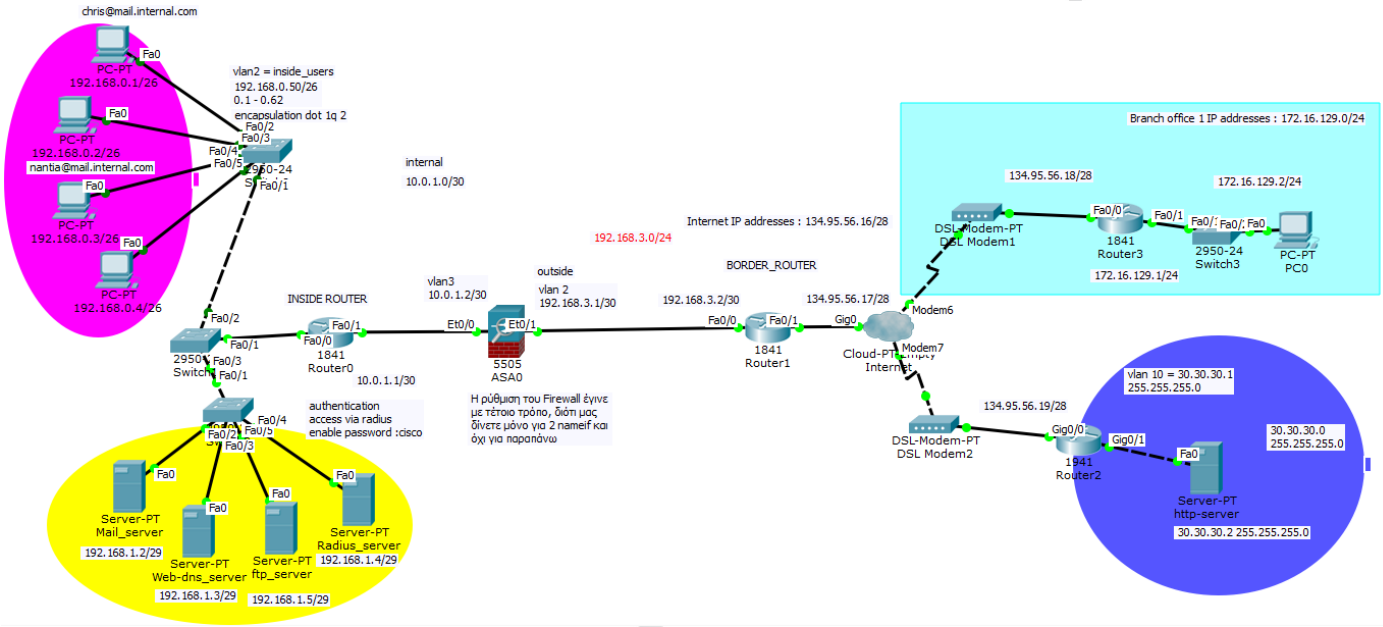


Καθώς και τα πρωτόκολλα TCP



4.5 Εφαρμογή της αρχιτεκτονικής DMZ σε δίκτυο εταιρείας με την χρησιμοποίηση ενός Firewall (Single firewall).

Στο παρακάτω σχήμα παρουσιάζετε ένα δίκτυο εταιρείας, το οποίο χρησιμοποιεί την αρχιτεκτονική DMZ και προστατεύετε με την χρησιμοποίηση ενός firewall.



Εικόνα 4.17 Εφαρμογή της αρχιτεκτονικής DMZ με την χρησιμοποίηση ενός Firewall (Single Firewall)

Περιγραφή δεδομένων

Το συγκεκριμένο δίκτυο, αποτελείται από τα εξής στοιχεία:

- 4 Υπολογιστές, οι οποίοι ανήκουν στο εσωτερικό του δικτύου και έχουν διευθύνσεις IP, από 192.168.0.1 / 26 - 192.168.0.4/26
- 4 Server's, οι οποίοι ανήκουν στο εσωτερικό του δικτύου και επίσης ανήκουν και σε διαφορετικό υποδίκτυο, από αυτόν τον υπολογιστών που ανήκουν στους χρήστες του δικτύου και με διευθύνσεις IP συγκεκριμένα:

  - ✓ Για τον Mail_server με διεύθυνση 192.168.1.2/29
  - ✓ Για τον Web-dns_server με διεύθυνση 192.168.1.3/29
  - ✓ Για τον Ftp_server με διεύθυνση 192.168.1.5/29
  - ✓ Για τον Radius_server με διεύθυνση 192.168.1.4/29

- Ένας εσωτερικός Router (INSIDE ROUTER) , ο οποίος είναι υπεύθυνος για την εσωτερική δρομολόγηση του εσωτερικού δικτύου και ο οποίος αναλύετε παρακάτω

- Ένα τείχος προστασίας (Firewall), ο οποίος βρίσκετε μπροστά από τον εσωτερικό δρομολογητή (INSIDE ROUTER) και ελέγχει την κίνηση των δεδομένων που έρχονται από το εξωτερικό δίκτυο προς το εσωτερικό. Θα πραγματοποιηθεί εκτενέστερη ανάλυση του τείχους προστασίας, παρακάτω.
- Ένας εσωτερικός δρομολογητής (BORDER ROUTER), ο οποίος αποτελεί το τελευταίο στοιχείο του δικτύου και αποτελεί το πρώτο φιλτράρισμα των δεδομένων που εισέρχονται στο δίκτυο. Εκτός από το φιλτράρισμα των δεδομένων πραγματοποιεί και την VPN σύνδεση με ένα δρομολογητή (Router3), ο οποίος βρίσκετε στο εξωτερικό δίκτυο (INTERNET) και επικοινωνεί μαζί του με IPsec.

Από την μεριά του εξωτερικού δικτύου έχουμε τα εξής στοιχεία:

- Τον δρομολογητή (Router3), ο οποίος όπως αναφέραμε προηγουμένως χρησιμοποιείται για την VPN σύνδεση με τον δρομολογητή (BORDER ROUTER).
- Τον δρομολογητή (Router2), ο οποίος χρησιμοποιείται σαν δρομολογητής ενός απομακρυσμένου δικτύου για την εμφάνιση μίας ιστοσελίδας, την οποία έχουμε ονομάσει ως (google.com) με διεύθυνση 30.30.30.2.

Για να μπορούν να επικοινωνούν το εσωτερικό δίκτυο με τον εξωτερικά δίκτυα, τα οποία θεωρούμε, ότι υπάρχουν κάπου στο διαδίκτυο, χρησιμοποιούμε dsl-modem δίνοντας την εικόνα σύνδεσης των 3 αυτών δικτύων στο διαδίκτυο.
Και οι 3 Δρομολογητές, χρησιμοποιούν στατικές διευθύνσεις για την σύνδεση τους.

Αναλυτικά έχουμε:

- BORDER_ROUTER με διεύθυνση 134.95.56.17/28
- Router3 με διεύθυνση 134.95.56.18/28
- Router2 με διεύθυνση 134.95.56.19/28

Οι συγκεκριμένες εργασίες που πρέπει να εφαρμοστούν στο δίκτυο της εικόνας 4.17, είναι οι εξής:

- ✓ Επικοινωνία των 2 χρηστών 192.168.0.1/26 – 192.1168.0.2/26 μέσω ηλεκτρονικού ταχυδρομείου.
- ✓ Πρόσβαση στην εσωτερική ιστοσελίδα του δικτύου, μόνο των χρηστών 192.168.0.1/26 και 192.168.0.2/26.
- ✓ Επικοινωνία των 2 χρηστών 192.168.0.1/26 – 192.1168.0.2/26 με τον ftp server του δικτύου για την μεταφορά και ανταλλαγή αρχείων.
- ✓ Πραγματοποίηση VPN σύνδεσης μεταξύ των 2 δρομολογητών με διευθύνσεις IP 192.168.0.0/29 και 172.16.129.2/24.
- ✓ Όλοι οι χρήστες του δικτύου να έχουν πρόσβαση στην ιστοσελίδα εξωτερικού δικτύου με διεύθυνση 30.30.30.2/24.
- ✓ Ο χρήστης με διεύθυνση 172.16.129.2 να έχει πρόσβαση στην εσωτερική ιστοσελίδα του δικτύου με διεύθυνση 192.168.1.3.

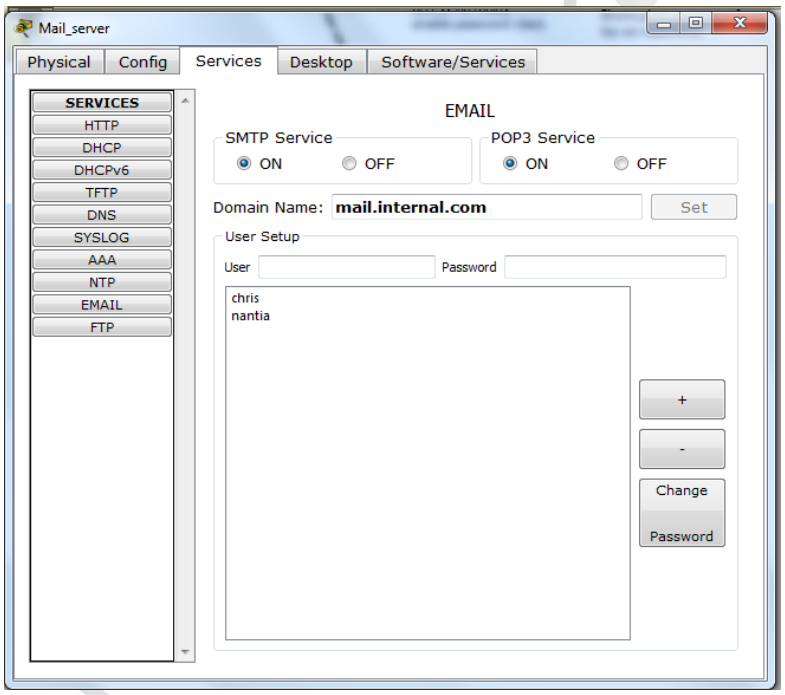
4.5.1 Υπηρεσίες εσωτερικού δικτύου

Για τις ανάγκες του εσωτερικού δικτύου, χρησιμοποιήσαμε τις συγκεκριμένες υπηρεσίες.

- **Υπηρεσία Ηλεκτρονικού Ταχυδρομείου (e-mail)**

- **Mailbox provider**

Χρησιμοποιήθηκε για την αποστολή και λήψη μηνυμάτων ηλεκτρονικού ταχυδρομείου (e-mail), μεταξύ των χρηστών του εσωτερικού δικτύου.
Για τους σκοπούς της εργαστηριακής άσκησης, χρησιμοποιήθηκε το όνομα του e-mail provider : mail.internal.com

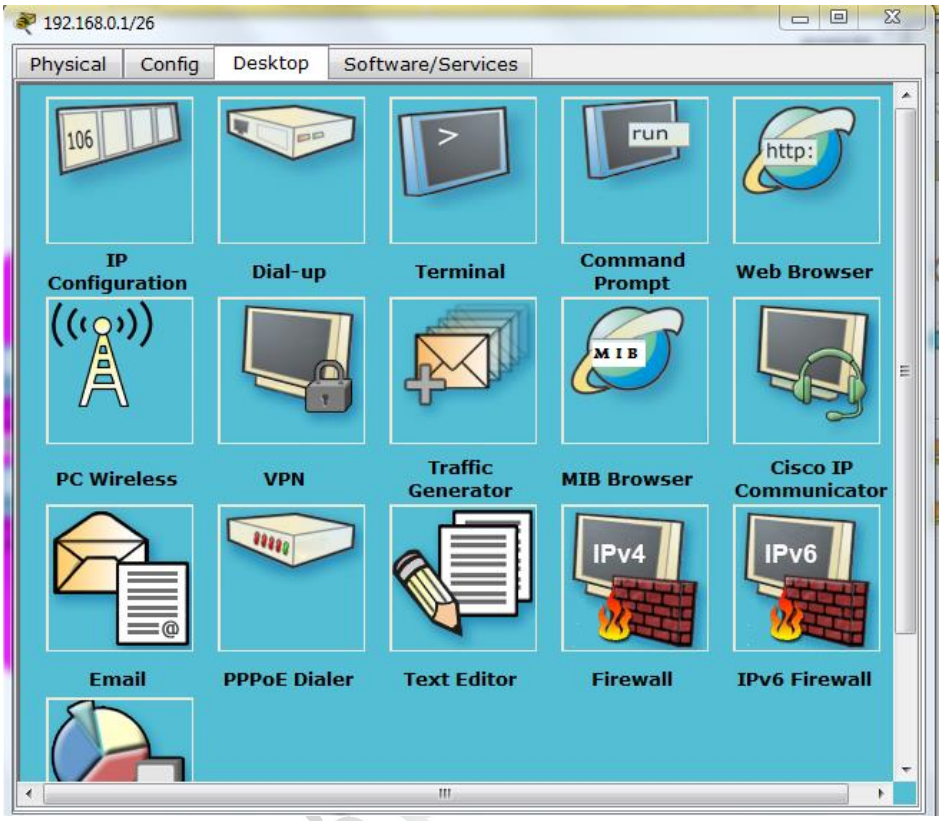


Εικόνα 4.18 Κεντρική οθόνη ρύθμισης του mail server

Στην παραπάνω εικόνα, ορίζουμε την όνομα του e-mail provider, το οποίο όπως αναφέραμε παραπάνω είναι το mail.internal.com. Εκτός από το όνομα ορίζουμε και τους χρήστες (δίνοντας ένα User και ένα Password), οι οποίοι θα μπορούν να χρησιμοποιούν τον mail server.

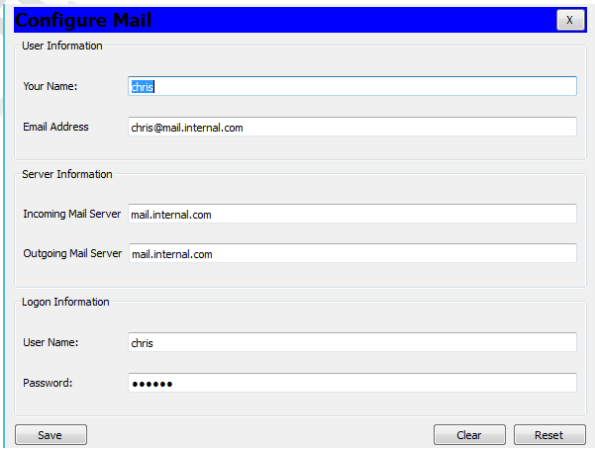
- **Ρύθμιση των e-mail λογαριασμών στους χρήστες**

Οι χρήστες του δικτύου, για να μπορούν να χρησιμοποιήσουν το Ηλεκτρονικό ταχυδρομείο, θα πρέπει να δημιουργήσουν ένα καινούργιο λογαριασμό στον υπολογιστή τους.



Εικόνα 4.19 Κεντρική Καρτέλα <<Desktop>> ρυθμίσεων ενός υπολογιστή.

Στην παραπάνω εικόνα, για να μπορέσουμε να ρυθμίσουμε ένα καινούργιο λογαριασμό επιλέγουμε το εικονίδιο Email. Στην συνέχεια εμφανίζετε μία καρτέλα, όπου θα πρέπει να συμπληρώσουμε τα στοιχεία για την ενεργοποίηση του λογαριασμού.



Εικόνα 4.20 Καρτέλα ενεργοποίησης λογαριασμού e-mail χρηστών.

Μετά την συμπλήρωση των στοιχείων, πατάμε το κουμπί <<save>> και ο λογαριασμός έχει ενεργοποιηθεί. Η ίδια ακριβώς διαδικασία, πραγματοποιείτε και για τους υπόλοιπους χρήστες του δικτύου.

Στο δίκτυο της παραπάνω εικόνας (εικόνα 4.17), οι χρήστες που χρησιμοποιούν το εσωτερικό ηλεκτρονικό ταχυδρομείο είναι 2. Ο χρήστης με διεύθυνση 192.168.0.1/26 και με account : chris@mail.internal.com και ο χρήστης με διεύθυνση 192.168.0.2/26 και με account : nantia@mail.internal.com . Οι υπόλοιποι 2 χρήστες, για λόγους ασφαλείας, δεν θα μπορούν να έχουν πρόσβαση στην υπηρεσία. Για να υλοποιήσουμε την συγκεκριμένη παράμετρο, θα πρέπει να εφαρμόσουμε στον εσωτερικό δρομολογητή (INSIDE ROUTER), μία λίστα πρόσβασης η οποία θα επιτρέπει στους χρήστες με διευθύνσεις 192.168.0.1/26 και 192.168.0.2/26 να έχουν πρόσβαση, σε tcp πρωτόκολλα και συγκεκριμένα στην θύρα 25, η οποία έχει πρόσβαση στην υπηρεσία SMTP (Simple Mail Transfer) και στην θύρα 110 , η οποία έχει πρόσβαση στην υπηρεσία POP3.

```
access-list 110 permit tcp host 192.168.0.1 host 192.168.1.2 eq smtp
access-list 110 permit tcp host 192.168.0.2 host 192.168.1.2 eq smtp

access-list 110 permit tcp host 192.168.0.1 host 192.168.1.2 eq pop3
access-list 110 permit tcp host 192.168.0.2 host 192.168.1.2 eq pop3
```

αποτρέποντας τους άλλους 2 χρήστες:

```
access-list 110 deny ip any any
```

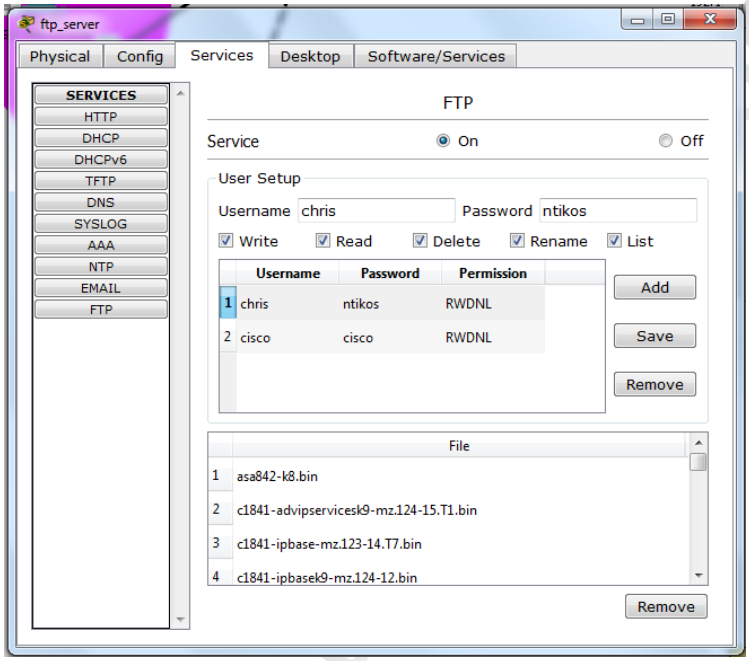
Η συγκεκριμένη λίστα πρόσβασης (access-list 110), εφαρμόζετε επάνω στην διασύνδεση FastEthernet 0/0.2, για την ενεργοποίηση της σε εισερχόμενη κίνηση.

```
interface FastEthernet0/0.2
encapsulation dot1Q 2
ip address 192.168.0.50 255.255.255.192
ip access-group 110 in
```

➢ **Υπηρεσία Απομακρυσμένης μεταφοράς αρχείων, File Transfer Protocol (Ftp)**

- **Ρύθμιση της υπηρεσίας ftp**

Για την ενεργοποίηση της υπηρεσίας χρησιμοποιήσαμε ένα ftp_server με διεύθυνση IP 192.168.1.5/26 και κάναμε τις εξής ρυθμίσεις.



Εικόνα 4.21 Κεντρική οθόνη ρύθμισης του ftp server

Στην παραπάνω εικόνα, για να ενεργοποιήσουμε την συγκεκριμένη υπηρεσία, θα πρέπει να εγγράψουμε χρήστες δίνοντας τους ένα username και ένα password και ενεργοποιώντας τους άδειες επεξεργασίας των αρχείων που ανταλλάσσονται όπως ***write, read, delete, rename, list.***

Στην συνέχεια για να μπορούν οι χρήστες να έχουν πρόσβαση σε αυτή την υπηρεσία θα πρέπει να ρυθμίσουμε τον εσωτερικό δρομολογητή (INSIDE ROUTER), για την μεταφορά των πρωτοκόλλων.

```
ip dhcp pool ftppool
network 192.168.0.0 255.255.255.192
default-router 192.168.0.50
dns-server 192.168.1.3
```

Η εντολή ip dhcp pool ftppool, χρησιμοποιείται για τον καθορισμό του υποδικτύου στον οποίο θα μπορούν οι χρήστες να χρησιμοποιούν την υπηρεσία ftp και των καθορισμό του server στον οποίο θα υπάρχει το domain name για την σύνδεση, όπου και αυτός θα αναλυθεί στις επόμενες παραγράφους.

```
ip dhcp pool ftpserver
network 192.168.1.0 255.255.255.248
default-router 192.168.1.1
dns-server 192.168.1.3
```

Η εντολή ip dhcp pool ftpserver, χρησιμοποιείται για να καθορίσουμε στον δρομολογητή, το υποδίκτυο στο οποίο ανήκει ο server της συγκεκριμένης υπηρεσίας και τον server στον οποίο υπάρχει το domain name για την σύνδεση.

Μετά από αυτές τις ρυθμίσεις, γνωστοποιούμε στον δρομολογητή το username και το password που υπάρχει για την σύνδεση των χρηστών με την ftp υπηρεσία.

```
ip ftp username chris
ip ftp password ntikos
```

Όπως και στην υπηρεσία του ηλεκτρονικού ταχυδρομείου, μόνο οι χρήστες με διευθύνσεις 192.168.0.1/26 και 192.168.0.2/26 θα μπορούν να χρησιμοποιούν την συγκεκριμένη υπηρεσία αποτρέποντας στους άλλους 2 χρήστες (192.168.0.3/26 – 192.168.0.4/26), την χρησιμοποίηση της. Για τον λόγο αυτό στην λίστα πρόσβασης θα προσθέσουμε τους εξής κανόνες.

```
access-list 110 permit ip host 192.168.0.1 host 192.168.1.5
access-list 110 permit ip host 192.168.0.2 host 192.168.1.5
```

Παρατηρούμε ότι στην συγκεκριμένη υπηρεσία, χρησιμοποιήσαμε πλήρης πρόσβαση στον ftp server από τους 2 χρήστες του δικτύου για τον λόγο ότι οι 2 χρήστες θα πρέπει να διαθέτουν πλήρης πρόσβαση στον server.

αποτρέποντας τους άλλους 2 χρήστες:

```
access-list 110 deny ip any any
```

- **Εφαρμογή της υπηρεσίας ftp**

Στο συγκεκριμένο παράδειγμα ο χρήστης με διεύθυνση 192.168.0.1/26 προσπαθεί επιτυχώς, να συνδεθεί με την υπηρεσία ftp του δικτύου, για την μεταφορά ενός αρχείου ergazomeni.txt ο οποίος περιέχει διάφορα στοιχεία των εργαζόμενων.

```
PC>ftp www.ftpserver.com
Trying to connect...www.ftpserver.com
Connected to www.ftpserver.com
220- Welcome to PT Ftp server
Username:chris
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>put ergazomeni.txt

Writing file ergazomeni.txt to www.ftpserver.com:
File transfer in progress...

[Transfer complete - 712 bytes]

712 bytes copied in 0.104 secs (6846 bytes/sec)
ftp>
```

Εικόνα 4.22 Επιτυχής μεταφορά αρχείου στον www.ftpserver.com

Και στην συνέχεια το συγκεκριμένο αρχείο ergazomeni.txt υπάρχει στην λίστα του www.ftpserver.com

```
ftp>dir

Listing /ftp directory from www.ftpserver.com:
0    : asa842-k8.bin                                5571584
1    : c1841-advipservicesk9-mz.124-15.T1.bin       33591768
2    : c1841-ipbase-mz.123-14.T7.bin                13832032
3    : c1841-ipbasek9-mz.124-12.bin                 16599160
4    : c2600-advipservicesk9-mz.124-15.T1.bin       33591768
5    : c2600-i-mz.122-28.bin                        5571584
6    : c2600-ipbasek9-mz.124-8.bin                  13169700
7    : c2800nm-advipservicesk9-mz.124-15.T1.bin     50938004
8    : c2800nm-advipservicesk9-mz.151-4.M4.bin      33591768
9    : c2800nm-ipbase-mz.123-14.T7.bin              5571584
10   : c2800nm-ipbasek9-mz.124-8.bin                15522644
11   : c2950-i6q4l2-mz.121-22.EA4.bin               3058048
12   : c2950-i6q4l2-mz.121-22.EA8.bin               3117390
13   : c2960-lanbase-mz.122-25.FX.bin               4414921
14   : c2960-lanbase-mz.122-25.SEE1.bin             4670455
15   : c2960-lanbasek9-mz.150-2.SE4.bin             4670455
16   : c3560-advipservicesk9-mz.122-37.SE1.bin      8662192
17   : ergazomeni.txt                               712
18   : pt1000-i-mz.122-28.bin                       5571584
19   : pt3000-i6q4l2-mz.121-22.EA4.bin              3117390
ftp>
```

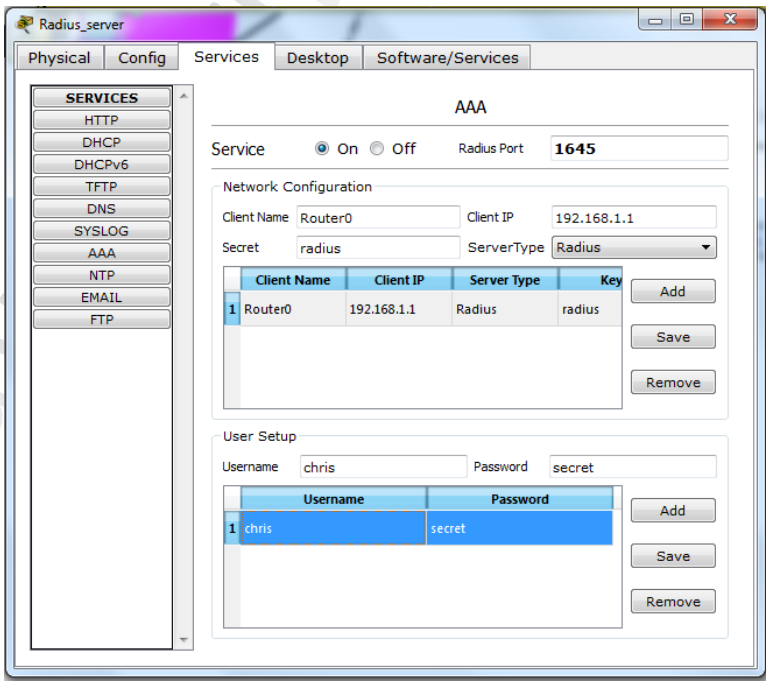
Εικόνα 4.23 Εμφάνιση της λίστας των αρχείων του ftp server

- **Υπηρεσία αυθεντικοποίησης χρηστών για χρήση δικτυακών συσκευών (Radius server)**

Η συγκεκριμένη υπηρεσία θα εφαρμοστεί για την αυθεντικοποίηση των χρηστών οι οποίοι θα θέλουν να έχουν πρόσβαση μέσω telnet στο configuration mode του εσωτερικού δρομολογητή (inside router).
Για να μπορεί ο δρομολογητής να χρησιμοποιήσει την συγκεκριμένη υπηρεσία θα πρέπει να ορίσει κάποιες τροποποιήσεις, που είναι η εξής:

!Δημιουργία νέου μοντέλου aaa (Authentication, Authorization, and Accounting)
Router0 (config)# aaa new-model
!αυθεντικοποίηση χρηστών μέσω Radius
Router0 (config)# aaa authentication login default group radius none
!σύνδεση τους μέσω telnet (teknet-lines)
Router0 (config)# aaa authentication login teknet-lines group radius
!ενεργοποίηση της υπηρεσίας, μέσω telnet
line vty 0 4
login authentication teknet-lines
!ρύθμιση της πόρτας καθώς (1645) και του κωδικού για την επικοινωνία με τον radius_server
radius-server host 192.168.1.4 auth-port 1645 key radius

Στην συνέχεια μεταφερόμαστε στον Radius server, όπου και πραγματοποιούμε τις ρυθμίσεις που εμφανίζονται στην παρακάτω εικόνα.



Εικόνα 4.24 Καρτέλα ρυθμίσεων του radius server

Στο πεδίο network configuration καθορίζουμε το όνομα της συσκευής που θα χρησιμοποιηθεί για την αυθεντικοποίηση της, την διεύθυνση στην οποία ανήκει, καθώς και τον κωδικό που θα χρησιμοποιηθεί για την επικοινωνία της συσκευής με τον server, όπως επίσης και το είδος της αυθεντικοποίησης όπου στην δικιά μας περίπτωση είναι το radius.

Στην συνέχεια στο πεδίο User Setup εισάγουμε το όνομα και τον κωδικό πρόσβασης που θα χρησιμοποιήσουμε για την αυθεντικοποίηση των χρηστών.

```
User Access Verification

Username: chris
Password:
Router0>en
Router0#
```

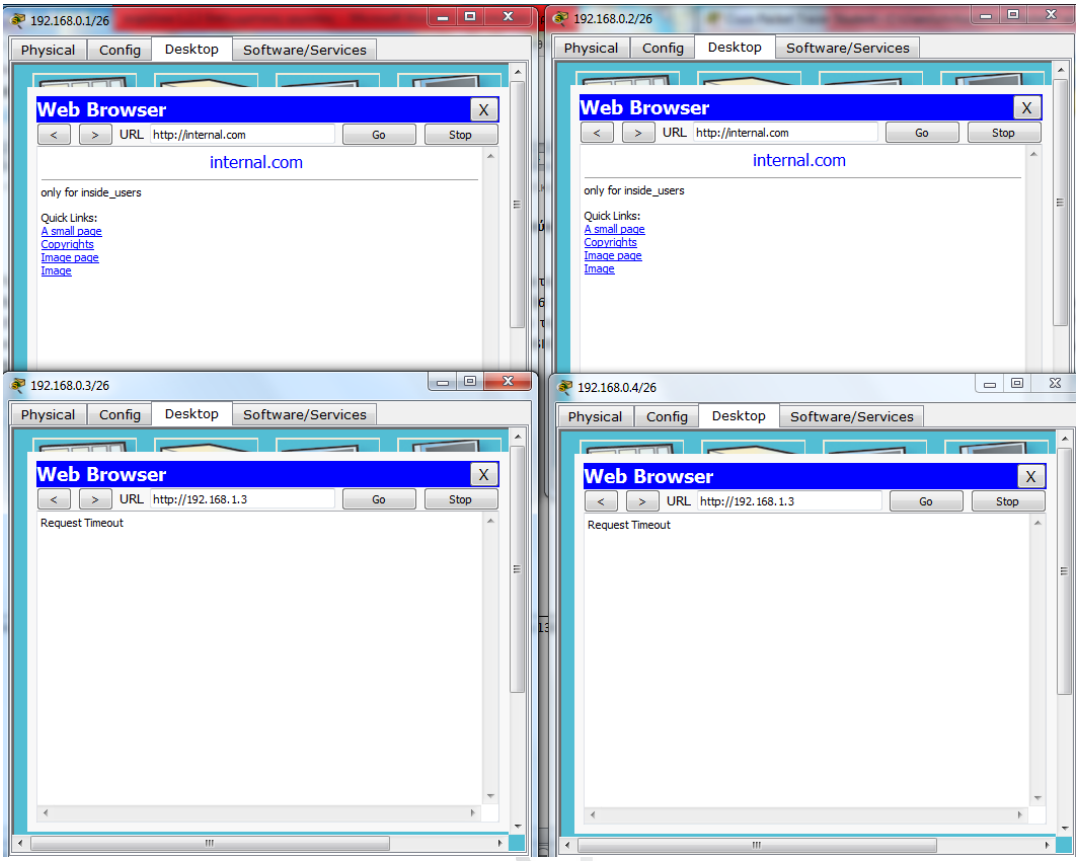
Οι κανόνες που θα εφαρμόσουμε στον εσωτερικό δρομολογητή (INSIDE ROUTER) είναι οι εξής:

```
access-list 110 permit tcp host 192.168.0.1 host 192.168.1.4 eq 1645
access-list 110 permit udp host 192.168.0.1 host 192.168.1.4 eq 1645
```

- **Υπηρεσία πρόσβασης των χρηστών στην εσωτερική ιστοσελίδα του δικτύου (internal.com) καθώς και χρησιμοποίηση της υπηρεσίας domain name**

Για τους σκοπούς της εργαστηριακής άσκησης, πρόσβαση στην εσωτερική ιστοσελίδα του δικτύου θα μπορεί να έχουν μόνο οι χρήστες με τις διευθύνσεις 192.168.0.1/26 – 192.168.0.2/26 και όχι οι άλλοι 2 χρήστες. Επομένως για να τους αποτρέψουμε την σύνδεση, θα προσθέσουμε στην λίστα πρόσβασης του εσωτερικού δρομολογητή (INSIDE ROUTER) άλλους 2 κανόνες που είναι οι εξής :

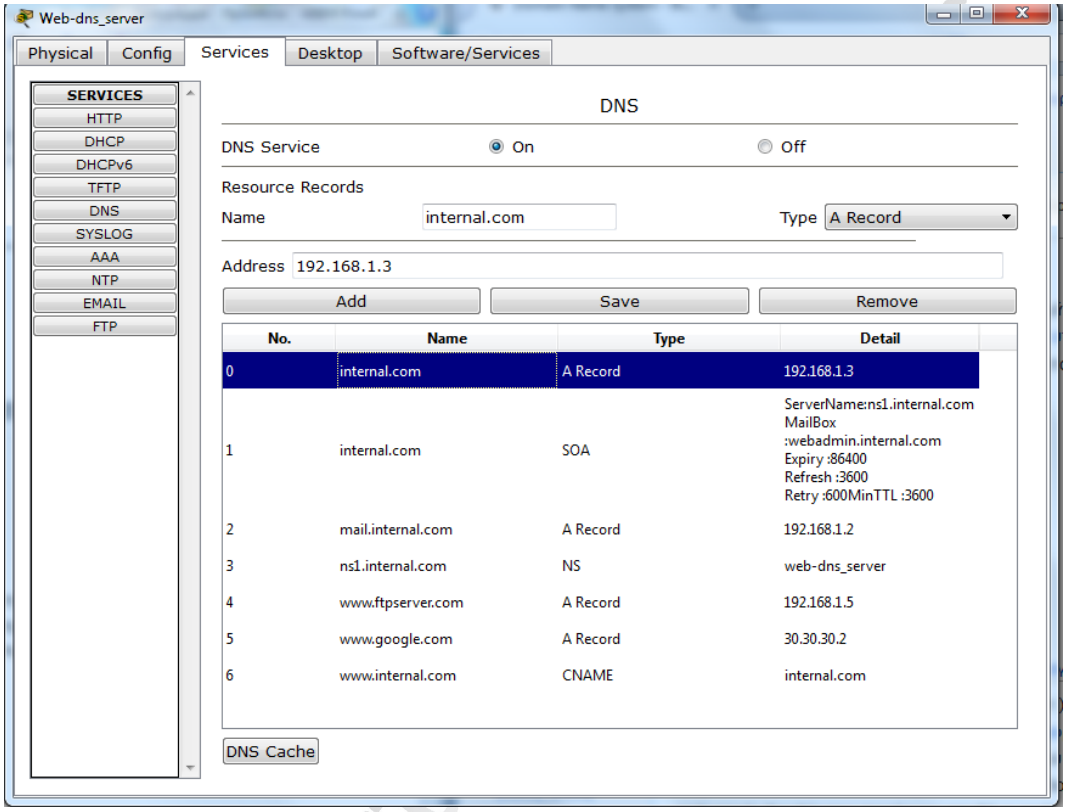
```
access-list 110 permit tcp host 192.168.0.1 host 192.168.1.3 eq www
access-list 110 permit tcp host 192.168.0.2 host 192.168.1.3 eq www
```



Εικόνα 4.25 Εμφάνιση της ιστοσελίδας και στους 4 χρήστες της ιστοσελίδας του εσωτερικού δικτύου

- **Υπηρεσία domain name**

Η υπηρεσία domain name χρησιμοποιείται για την ονοματοδοσία των διευθύνσεων πρωτοκόλλου IP. Έτσι, για όλες τις παραπάνω υπηρεσίες που παρουσιάσαμε έχουμε δώσει ορισμένα ονόματα, για την ευκολότερη χρησιμοποίηση τους και τα οποία είναι τα εξής:



Εικόνα 4.26 Καρτέλα ρυθμίσεων της DNS υπηρεσίας

Στην συνέχεια για να μπορέσει το υποδίκτυο των χρηστών μας 192.168.0.0/26 να χρησιμοποιήσει την domain υπηρεσία θα πρέπει να επιτρέψει την κυκλοφορία, μέσω του εσωτερικού δρομολογητή:

```
access-list 110 permit udp 192.168.0.0 0.0.0.63 host 192.168.1.3 eq domain
```

4.5.2 Configuration file του δρομολογητή (inside router)

```
User Access Verification

Username: chris
Password:
Router0>en
Password:
Router0#show run
Building configuration...

Current configuration : 4058 bytes
!
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Router0
!
enable password cisco
!
ip dhcp pool ftppool
network 192.168.0.0 255.255.255.192
default-router 192.168.0.50
dns-server 192.168.1.3
ip dhcp pool ftpserver
network 192.168.1.0 255.255.255.248
default-router 192.168.1.1
dns-server 192.168.1.3
!
aaa new-model
!
aaa authentication login default group radius none
aaa authentication login teknet-lines group radius
!
ip cef
no ipv6 cef
!
ip ftp username chris
ip ftp password ntikos
ip ssh version 1
!
!
spanning-tree mode pvst
!
```

```
interface FastEthernet0/0
no ip address
duplex auto
speed auto
!
interface FastEthernet0/0.2
encapsulation dot1Q 2
ip address 192.168.0.50 255.255.255.192
ip access-group 110 in
!
interface FastEthernet0/0.3
encapsulation dot1Q 3
ip address 192.168.1.1 255.255.255.248
ip access-group 111 in
!
interface FastEthernet0/1
ip address 10.0.1.1 255.255.255.252
duplex auto
speed auto
ipv6 ospf cost 1
!
interface Vlan1
no ip address
shutdown
!
ip classless
ip route 134.95.56.16 255.255.255.240 10.0.1.2
ip route 192.168.2.0 255.255.255.252 10.0.1.2
ip route 192.168.0.0 255.255.255.192 10.0.1.2
ip route 192.0.2.0 255.255.255.252 10.0.1.2
ip route 192.168.1.0 255.255.255.248 10.0.1.2
ip route 172.16.129.0 255.255.255.0 10.0.1.2
ip route 30.30.30.0 255.255.255.0 10.0.1.2
!
ip flow-export version 9
!
!
access-list 110 permit ip host 192.168.0.1 host 192.168.1.5
access-list 110 permit ip host 192.168.0.2 host 192.168.1.5
access-list 110 permit tcp host 192.168.0.1 host 192.168.1.3 eq www
access-list 110 permit tcp host 192.168.0.2 host 192.168.1.3 eq www
access-list 110 permit tcp host 192.168.0.1 host 192.168.1.2 eq smtp
access-list 110 permit tcp host 192.168.0.2 host 192.168.1.2 eq smtp
access-list 110 permit tcp host 192.168.0.1 host 192.168.1.3 eq 22
access-list 110 permit tcp host 192.168.0.2 host 192.168.1.3 eq 22
access-list 110 permit udp host 192.168.0.1 host 192.168.1.3 eq 22
access-list 110 permit udp host 192.168.0.2 host 192.168.1.3 eq 22
access-list 110 permit tcp host 192.168.0.1 host 192.168.1.2 eq pop3
access-list 110 permit tcp host 192.168.0.2 host 192.168.1.2 eq pop3
```

```
access-list 110 permit tcp 192.168.0.0 0.0.0.63 host 30.30.30.2 eq www
access-list 110 permit udp 192.168.0.0 0.0.0.63 host 192.168.1.3 eq domain
access-list 110 permit tcp host 192.168.0.1 host 192.168.1.4 eq 1645
access-list 110 permit udp host 192.168.0.1 host 192.168.1.4 eq 1645
access-list 110 permit tcp host 192.168.0.1 host 192.168.1.1 eq telnet
access-list 110 deny ip any any
access-list 111 permit udp 192.168.0.0 0.0.0.63 host 192.168.1.3 eq domain
access-list 111 permit tcp host 192.168.0.1 host 192.168.1.2 eq smtp
access-list 111 permit tcp host 192.168.0.2 host 192.168.1.2 eq smtp
access-list 111 permit tcp host 192.168.0.1 host 192.168.1.2 eq pop3
access-list 111 permit tcp host 192.168.0.2 host 192.168.1.2 eq pop3
access-list 111 permit tcp host 192.168.0.1 host 192.168.1.3 eq www
access-list 111 permit tcp host 192.168.0.2 host 192.168.1.3 eq www
access-list 111 permit ip host 192.168.0.1 host 192.168.1.5
access-list 111 permit ip host 192.168.0.2 host 192.168.1.5
access-list 111 permit udp host 192.168.1.1 host 192.168.1.4 eq 1645
access-list 111 permit udp host 192.168.0.1 host 192.168.1.4 eq 1645
access-list 111 permit udp host 192.168.1.4 host 192.168.1.1 eq 1645
access-list 111 permit udp host 192.168.1.3 192.168.0.0 0.0.0.63
access-list 111 permit tcp host 192.168.1.3 192.168.0.0 0.0.0.63
access-list 111 permit tcp host 192.168.1.2 host 192.168.0.1
access-list 111 permit tcp host 192.168.1.2 host 192.168.0.2
access-list 111 permit tcp host 192.168.1.5 host 192.168.0.1
access-list 111 permit tcp host 192.168.1.5 host 192.168.0.2
access-list 111 permit tcp host 192.168.1.3 host 172.16.129.2
access-list 111 deny ip any any
!
!
radius-server host 192.168.1.4 auth-port 1645 key radius
!
!
!
line con 0
!
line aux 0
!
line vty 0 4
login authentication teknet-lines
!
!
!
end
```

4.5.3 Τείχος προστασίας – Firewall (FW-1)

Το τείχος προστασίας, αποτελεί μία συσκευή, η οποία στην ουσία καταγράφει τις κινήσεις των δεδομένων που αποστέλλονται τόσο από το εσωτερικό δίκτυο προς το εξωτερικό, όσο και από το εξωτερικό δίκτυο προς το εσωτερικό.

Για την διευκόλυνση μας ορίσαμε την διασύνδεση η οποία βρίσκετε από την μεριά του εσωτερικού δικτύου ως inside και την διασύνδεση η οποία βρίσκετε από την μεριά του εξωτερικού δικτύου ως outside.

```
interface Ethernet0/0
switchport access vlan 3

!
interface Vlan3
nameif inside
security-level 100
ip address 10.0.1.2 10.0.0.0
!

interface Ethernet0/1
switchport access vlan 2

!
interface Vlan2
nameif outside
security-level 0
ip address 192.168.3.1 255.255.255.252
!
```

Για να μπορούμε να ξεχωρίζουμε εύκολα τις 2 λίστες πρόσβασης που θα χρησιμοποιήσουμε, ονομάσαμε την μία λίστα πρόσβασης insidetooutside και απευθύνετε στα δεδομένα με κατεύθυνση από το εσωτερικό δίκτυο προς το εξωτερικό και την άλλη outsidetoinside με κατεύθυνση από το εξωτερικό δίκτυο προς το εσωτερικό.

```
access-list outsidetoinside extended permit icmp 30.30.30.0 255.255.255.0
192.168.0.0 255.255.255.192
access-list outsidetoinside extended permit tcp host 172.16.129.2 host 192.168.1.3 eq
www
access-list outsidetoinside extended permit tcp host 30.30.30.2 192.168.0.0
255.255.255.192
access-list insidetooutside extended permit icmp 192.168.0.0 255.255.255.192
30.30.30.0 255.255.255.0
access-list insidetooutside extended permit tcp host 192.168.1.3 host 172.16.129.2
access-list insidetooutside extended permit tcp 192.168.0.0 255.255.255.192 host
30.30.30.2 eq www
!
```

Στην συνέχεια, για να μπορούν αυτές οι λίστες να εφαρμοστούν, επάνω στις διασυνδέσεις, χρησιμοποιούμε τις παρακάτω εντολές

access-group outsidetoinside out interface inside
access-group insidetooutside in interface inside

- **Configuration file του τείχους προστασίας (FW-1)**

```
ciscoasa>en
Password:
ciscoasa#show run
: Saved
:
ASA Version 8.4(2)
!
hostname ciscoasa
names
!
interface Ethernet0/0
 switchport access vlan 3
!
interface Ethernet0/1
 switchport access vlan 2
!
interface Ethernet0/2
!
interface Ethernet0/3
!
interface Ethernet0/4
!
interface Ethernet0/5
!
interface Ethernet0/6
!
interface Ethernet0/7
!
interface Vlan1
 no nameif
 no security-level
 no ip address
!
interface Vlan2
 nameif outside
 security-level 0
 ip address 192.168.3.1 255.255.255.252
!
```

```
interface Vlan3
 nameif inside
 security-level 100
 ip address 10.0.1.2 10.0.0.0
!
route inside 192.168.0.0 255.255.255.192 10.0.1.1 1
route inside 192.168.1.0 255.255.255.248 10.0.1.1 1
route outside 172.16.129.0 255.255.255.0 192.168.3.2 1
route outside 30.30.30.0 255.255.255.0 192.168.3.2 1
route outside 134.95.56.16 255.255.255.240 192.168.3.2 1
!
access-list outsidetoinside extended permit icmp 30.30.30.0 255.255.255.0
192.168.0.0 255.255.255.192
access-list outsidetoinside extended permit tcp host 172.16.129.2 host 192.168.1.3 eq
www
access-list outsidetoinside extended permit tcp host 30.30.30.2 192.168.0.0
255.255.255.192
access-list insidetooutside extended permit icmp 192.168.0.0 255.255.255.192
30.30.30.0 255.255.255.0
access-list insidetooutside extended permit tcp host 192.168.1.3 host 172.16.129.2
access-list insidetooutside extended permit tcp 192.168.0.0 255.255.255.192 host
30.30.30.2 eq www
!
!
access-group outsidetoinside out interface inside
access-group insidetooutside in interface inside
!
telnet timeout 5
ssh timeout 5
!
dhcpd enable
!
dhcpd auto_config outside
!

interface Vlan1
no nameif
no security-level
no ip address
!
interface Vlan2
nameif outside
security-level 0
ip address 192.168.3.1 255.255.255.252
!
```

```
interface Vlan3
nameif inside
security-level 100
ip address 10.0.1.2 10.0.0.0
!
!
route inside 192.168.0.0 255.255.255.192 10.0.1.1 1
route inside 192.168.1.0 255.255.255.248 10.0.1.1 1
route outside 172.16.129.0 255.255.255.0 192.168.3.2 1
route outside 30.30.30.0 255.255.255.0 192.168.3.2 1
route outside 134.95.56.16 255.255.255.240 192.168.3.2 1
!
access-list outsidetoinside extended permit icmp 172.16.129.0 255.255.255.0
192.168.0.0 255.255.255.192
access-list outsidetoinside extended permit icmp 30.30.30.0 255.255.255.0
192.168.0.0 255.255.255.192
access-list outsidetoinside extended permit tcp 172.16.129.0 255.255.255.0
192.168.0.0 255.255.255.192
access-list outsidetoinside extended permit tcp 30.30.30.0 255.255.255.0 192.168.0.0
255.255.255.192
access-list outsidetoinside extended permit tcp host 172.16.129.2 host 192.168.1.3 eq
www
access-list insidetooutside extended permit icmp 192.168.0.0 255.255.255.192
172.16.129.0 255.255.255.0
access-list insidetooutside extended permit icmp 192.168.0.0 255.255.255.192
30.30.30.0 255.255.255.0
access-list insidetooutside extended permit tcp host 192.168.1.3 host 172.16.129.2
access-list insidetooutside extended permit tcp 192.168.0.0 255.255.255.192
172.16.129.0 255.255.255.0
access-list insidetooutside extended permit tcp 192.168.0.0 255.255.255.192
30.30.30.0 255.255.255.0 eq www
!
!
access-group outsidetoinside out interface inside
access-group insidetooutside in interface inside
!
telnet timeout 5
ssh timeout 5
!
dhcpd enable
!
dhcpd auto_config outside
!
```

4.5.4 Εσωτερικός δρομολογητής (BORDER ROUTER)

Ο δρομολογητής αυτός, αποτελεί τον <<ακρογωνιαίο λίθο>> του δικτύου, συνδεοντάς μας με τα υπόλοιπα δίκτυα του διαδικτύου. Εκτός από την σύνδεση μας με το διαδίκτυο, αποτελεί το ένα μέλους του ζεύγους (το άλλο είναι το router3), για την VPN σύνδεση που θα εφαρμόσουμε στην συγκεκριμένη εργαστηριακή άσκηση.
Στον συγκεκριμένο δρομολογητή δεν εφαρμόσαμε λίστες πρόσβασης καθώς η όποια κίνηση η οποία θα περάσει από αυτόν θα ελεγχθεί από το τείχος προστασίας το οποίο βρίσκετε ακριβώς πίσω του.

- **Configuration file του εσωτερικού δρομολογητή (BORDER ROUTER)**

```
Router>
Router>en
Router#show run
Building configuration...

Current configuration : 1301 bytes
!
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Router
!
ip cef
no ipv6 cef
!
crypto isakmp policy 10
encr aes 256
authentication pre-share
group 5
!
crypto isakmp key ISAKMP_KEY address 134.95.56.18
!
!
!
crypto ipsec transform-set firstset esp-aes 256 esp-sha-hmac
!
crypto map vpn 10 ipsec-isakmp
set peer 134.95.56.18
set pfs group5
set transform-set firstset
match address 101
!

spanning-tree mode pvst
!
```

```
!
!
!
!
!
interface FastEthernet0/0
ip address 192.168.3.2 255.255.255.252
duplex auto
speed auto
ipv6 ospf cost 1
!
interface FastEthernet0/1
ip address 134.95.56.17 255.255.255.240
duplex auto
speed auto
crypto map vpn
!
interface Vlan1
no ip address
shutdown
!
ip classless
ip route 192.168.0.0 255.255.255.192 192.168.3.1
ip route 172.16.129.0 255.255.255.0 134.95.56.18
ip route 30.30.30.0 255.255.255.0 134.95.56.19
ip route 192.168.1.0 255.255.255.248 192.168.3.1
!
ip flow-export version 9
!
!
access-list 1 permit 192.168.0.0 0.0.0.63
access-list 101 permit tcp 172.16.129.0 0.0.0.255 192.168.1.0 0.0.0.7
access-list 101 permit tcp 192.168.1.0 0.0.0.7 172.16.129.0 0.0.0.255
!
!
!
!
line con 0
!
line aux 0
!
line vty 0 4
login
!
!
!
end
```

4.5.5 VPN σύνδεση site to site μεταξύ των 2 δρομολογητών BORDER ROUTER και Router3

Σκοπός της VPN σύνδεσης μεταξύ 2 σημείων, όπως έχουμε αναφέρει και σε προηγούμενα κεφάλαια, είναι η κρυπτογράφηση και η αυθεντικοποίηση των δεδομένων που διέρχονται από αυτές τις 2 μεριές του δικτύου (μέσω ESP Tunnel), παρέχοντας παράλληλα την ασφάλεια ενός ιδιωτικού δικτύου. Η συγκεκριμένη σύνδεση, αποτελεί την βασική αρχιτεκτονική μίας IPsec λειτουργίας.

Για να μπορέσουμε να εφαρμόσουμε αυτή την τεχνική στους 2 δρομολογητές θα κάνουμε τις εξής ρυθμίσεις:

Για τον BORDER ROUTER έχουμε :

!προσδιορισμός της IKE πολιτικής για την συγκεκριμένη VPN σύνδεση, εδώ παρατηρούμε
!ότι χρησιμοποιήθηκε η AES κρυπτογραφία 256 bit, κλειδιά pre-share και αλγόριθμος
!diffie-hellman group 5. Επίσης χρησιμοποιήθηκε και η κρυπτογραφική function SHA-1
!η οποία επειδή είναι default δεν εμφανίζετε στο configuration file του δρομολογητή.

```
crypto isakmp policy 10
encr aes 256
authentication pre-share
group 5
```

!Προσδιορισμός των pre-share κλειδιών, τα οποία είναι μοναδικά για κάθε ζευγάρι.
!Ας σημειωθεί ότι τα κλειδιά όπως και κάθε κλειδί θα πρέπει να αποτελείται από
!διαφόρων είδη χαρακτήρων (πεζά, κεφαλαία, αριθμούς, σύμβολα)
!δυσκολεύοντας με αυτόν τον τρόπο την αποκωδικοποίηση τους.

```
crypto isakmp key ISAKMP_KEY address 134.95.56.18
```

!το ipsec transform-set είναι ένα πρωτόκολλο επικοινωνίας μεταξύ των 2 συσκευών το
!οποίο στην συγκεκριμένη περίπτωση μας πραγματοποιεί κρυπτογράφηση των δεδομένων
μέσω aes μήκους !256 bit και χρησιμοποιεί την sha-1 για την ακεραιότητα των δεδομένων.

```
crypto ipsec transform-set firstset esp-aes 256 esp-sha-hmac
```

!το κάθε ζεύγος που χρησιμοποιείται για την vpn σύνδεση έχει το δικό του crypto map το
!οποίο εφαρμόζετε επάνω στην διασύνδεση του κάθε δρομολογητή και σε αυτόν
!καθορίζετε η συσκευή η οποία αποτελεί το άλλο μέλος του ζεύγους, το <<pfs>> το οποίο
!μας σιγουρεύει ότι τα κλειδιά τα οποία έχουν παραχθεί για αυτή την σύνδεση μετά το
!τέλος της διάρκειας δεν θα είναι σε θέση να ξανά παραχθούν και ότι η κυκλοφορία των
!δεδομένων θα είναι σε συμφωνία με την λίστα πρόσβασης 101

```
crypto map vpn 10 ipsec-isakmp
set peer 134.95.56.18
set pfs group5
set transform-set firstset
match address 101
```

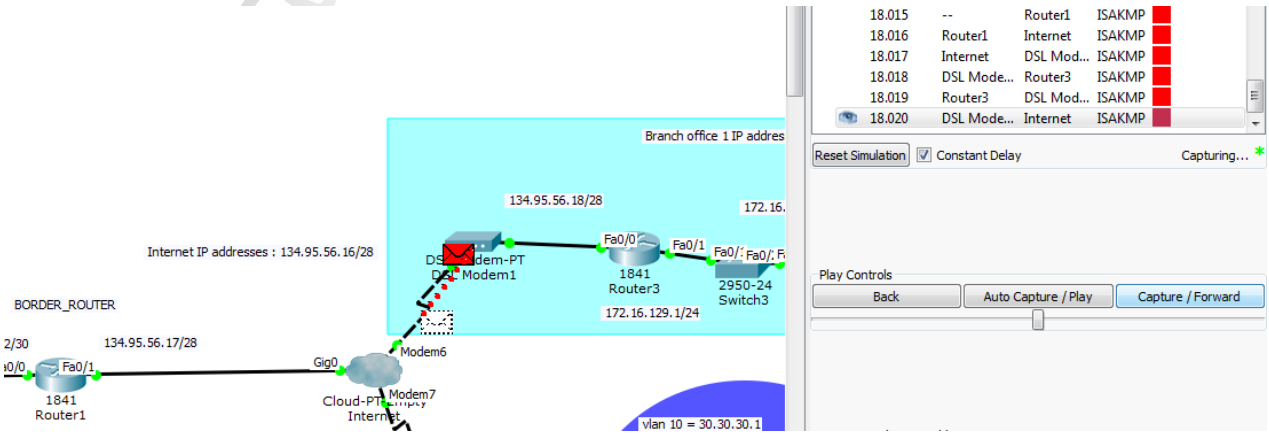
```
access-list 101 permit ip 192.168.0.0 0.0.0.63 172.16.129.0 0.0.0.255
access-list 101 permit ip 172.16.129.0 0.0.0.255 192.168.0.0 0.0.0.63
```

Ομοίως για τον Router3 έχουμε:

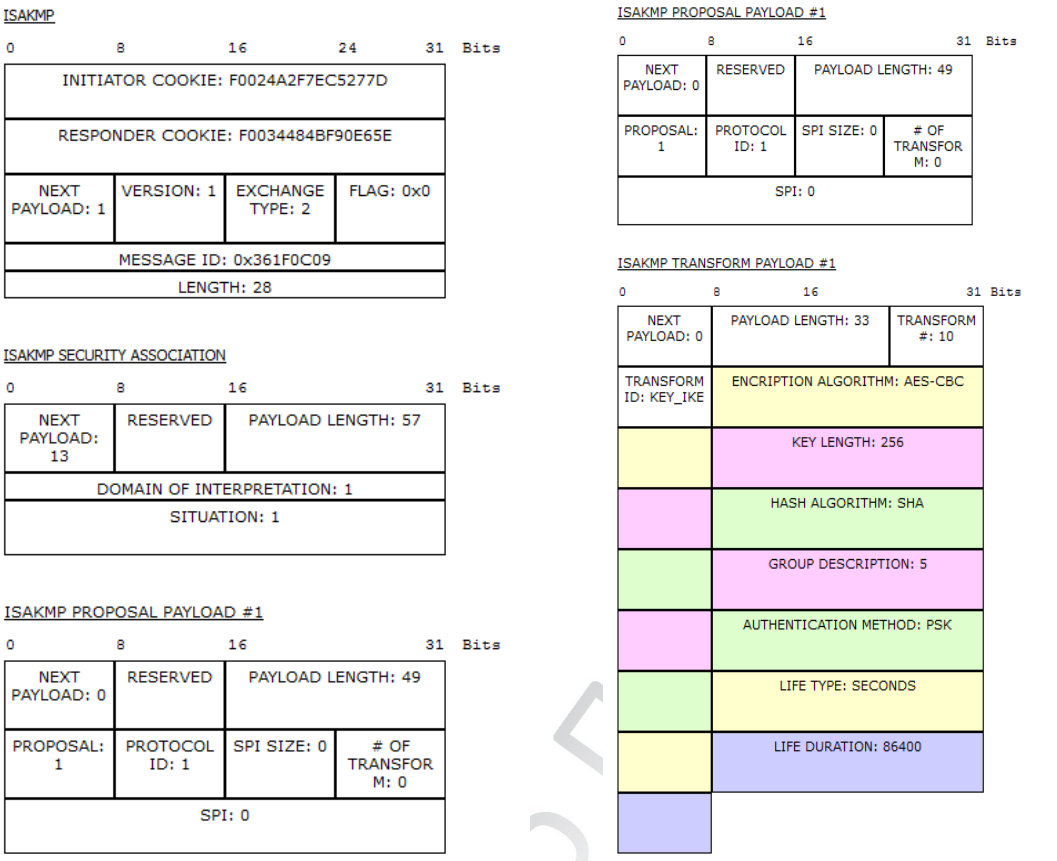
```
crypto isakmp policy 10
encr aes 256
authentication pre-share
group 5
!
crypto isakmp key ISAKMP_KEY address 134.95.56.17
!
!
!
crypto ipsec transform-set firstset esp-aes 256 esp-sha-hmac
!
crypto map vpn 10 ipsec-isakmp
set peer 134.95.56.17
set pfs group5
set transform-set firstset
match address 101
access-list 101 permit ip 192.168.0.0 0.0.0.63 172.16.129.0 0.0.0.255
access-list 101 permit ip 172.16.129.0 0.0.0.255 192.168.0.0 0.0.0.63
!
```

Προσομοίωση της διαδικασίας ενεργοποίησης της VPN σύνδεσης μεταξύ των 2 δρομολογητών

- **Πρώτη Φάση**
  Σε πρώτη φάση οι 2 δρομολογητές ανταλλάσουν ISAKMP μηνύματα, για την ανταλλαγή κλειδιών και για την εγκαθίδρυση της σύνδεσης μεταξύ τους.

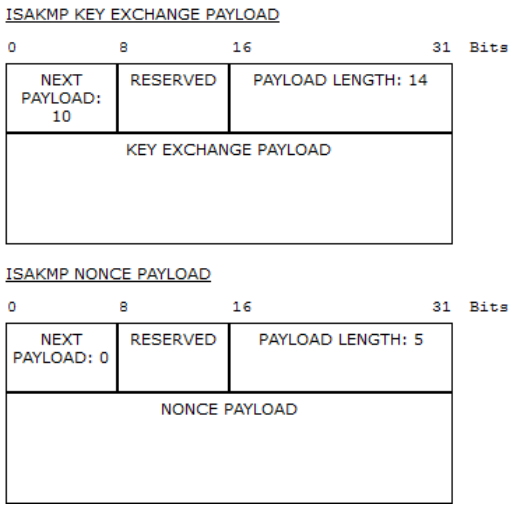


Εικόνα 4.27 Έναρξη εγκατάστασης σύνδεσης μέσω ISAKMP μηνυμάτων



Εικόνα 4.28 Βασικά χαρακτηριστικά του ISAKMP μηνύματος

Ο Δρομολογητής (BORDER ROUTER), παραλαμβάνει το isakmp μήνυμα και ξεκινάει την ανταλλαγή των κλειδιού ISAKMP_KEY.



Εικόνα 4.29 ανταλλαγή κλειδιών ISAKMP

Αφού ο δρομολογητής (BORDER ROUTER), παραλάβει ξανά ISAKMP μήνυμα, τότε ξεκινά την αποστολή κρυπτογραφημένης μορφής μηνυμάτων.

ISAKMP

0	8	16	24	31 Bits
INITIATOR COOKIE: F0024A2F7EC5277D				
RESPONDER COOKIE: F0034484BF90E65E				
NEXT PAYLOAD: 5	VERSION: 1	EXCHANGE TYPE: 2	FLAG: 0x1	
MESSAGE ID: 0x361F0C09				
LENGTH: 28				

ISAKMP ENCRYPTED PAYLOAD

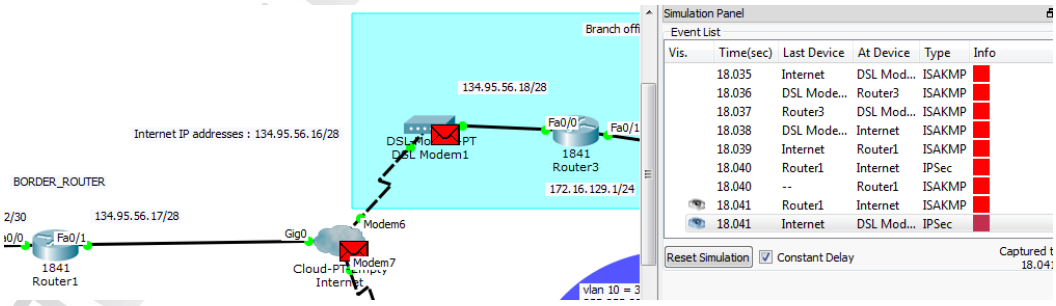
ENCRYPTED DATA

Εικόνα 4.30 κρυπτογραφημένο ISAKMP μήνυμα

Μετά από ανταλλαγές ISAKMP μηνυμάτων μεταξύ των δρομολογητών και την εγκαθίδρυση της VPN σύνδεσης ξεκινά σε δεύτερη φάση και η αποστολή των IPsec μηνυμάτων.

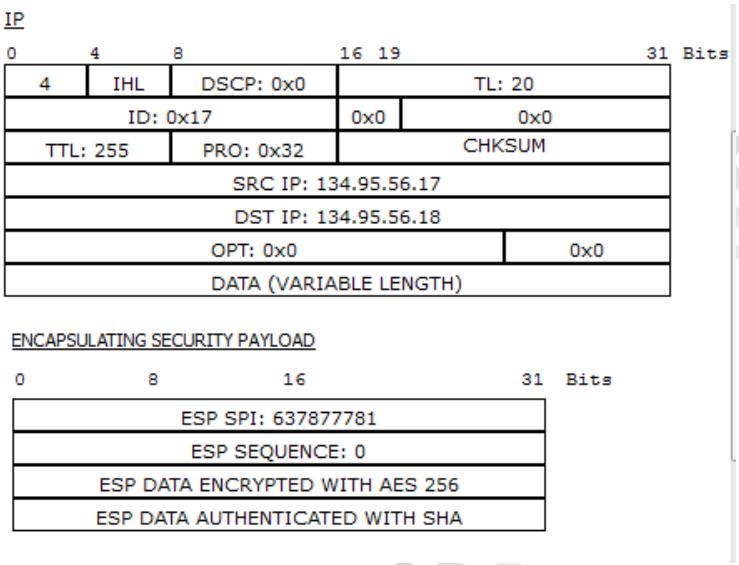
- **Δεύτερη Φάση**

Στην δεύτερη φάση τα δεδομένα που αποστέλλονται σε IPsec μορφή χρησιμοποιούνται για την προστασία των δεδομένων.



Εικόνα 4.31 ανταλλαγή IPSEC μηνυμάτων

Μετά την εγκαθίδρυση της VPN σύνδεσης των δρομολογητών, τα δεδομένα που μεταφέρονται από τον ένα δρομολογητή στον άλλον κρυπτογραφούνται σε IPsec μορφή και αποκρυπτογραφούνται πριν φτάσουν στον παραλήπτη.

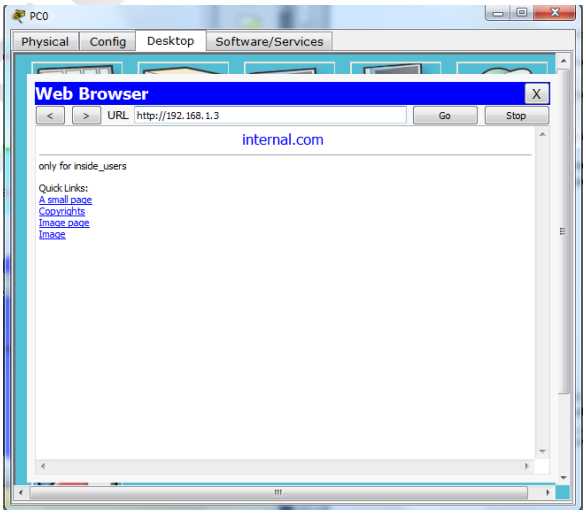


Εικόνα 4.32 κρυπτογράφηση PING μηνύματος σε IPsec μορφή

Στην συνέχεια ο άλλος δρομολογητής αφού παραλάβει το κρυπτογραφημένο μήνυμα και πιστοποιήσει ότι προέρχεται από τον προηγούμενο παραλήπτη και δεν υπέστη τροποποιήσεις κατά την μεταφορά του, το αποκρυπτογραφεί και το στέλνει στον παραλήπτη του.

Η ίδια διαδικασία πραγματοποιείται και σε αντίθετη φορά.

- **Επιβεβαίωση της επικοινωνίας του υποδικτύου 192.168.0.0/29 με το υποδίκτυο 172.16.129.0/24 με την χρήση ping μηνυμάτων.**



Εικόνα 4.33 επικοινωνία με tcp μηνύματα μεταξύ του χρήστη 172.16.129.2/24 και του web-dns_server 192.168.1.3/29

- **Επιβεβαίωση κρυπτογράφησης μηνυμάτων**

Για να μπορέσουμε να επιβεβαιώσουμε ότι η VPN σύνδεση έχει επιτευχθεί, πληκτρολογούμε στον δρομολογητή την εξής εντολή.

```
Router#show crypto ipsec sa

interface: FastEthernet0/1
Crypto map tag: vpn, local addr 134.95.56.17

protected vrf: (none)
local ident (addr/mask/prot/port): (192.168.1.0/255.255.255.192/0/0)
remote ident (addr/mask/prot/port): (172.16.129.0/255.255.255.0/0/0)
current_peer 134.95.56.18 port 500

PERMIT, flags={origin_is_acl,}

#pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 0

#pkts decaps: 3, #pkts decrypt: 3, #pkts verify: 0

#pkts compressed: 0, #pkts decompressed: 0

#pkts not compressed: 0, #pkts compr. failed: 0

#pkts not decompressed: 0, #pkts decompress failed: 0

#send errors 1, #recv errors 0

local crypto endpt.: 134.95.56.17, remote crypto endpt.:134.95.56.18

path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/1

current outbound spi: 0x26053E15(637877781)

inbound esp sas:

spi: 0x7D254A37(2099595831)

transform: esp-aes 256 esp-sha-hmac ,

in use settings ={Tunnel, }
conn id: 2001, flow_id: FPGA:1, crypto map: vpn
sa timing: remaining key lifetime (k/sec): (4525504/3425)
IV size: 16 bytes
replay detection support: N
Status: ACTIVE

inbound ah sas:
```

inbound pcp sas:

outbound esp sas:
spi: 0x26053E15(637877781)
transform: esp-aes 256 esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 2002, flow_id: FPGA:1, crypto map: vpn
sa timing: remaining key lifetime (k/sec): (4525504/3425)
IV size: 16 bytes
replay detection support: N
Status: ACTIVE

outbound ah sas:

outbound pcp sas:

4.5.6 Εξωτερικός δρομολογητής BRANCH OFFICE 1 (Router3)

- **Configuration file του εξωτερικού δρομολογητή (Router3)**

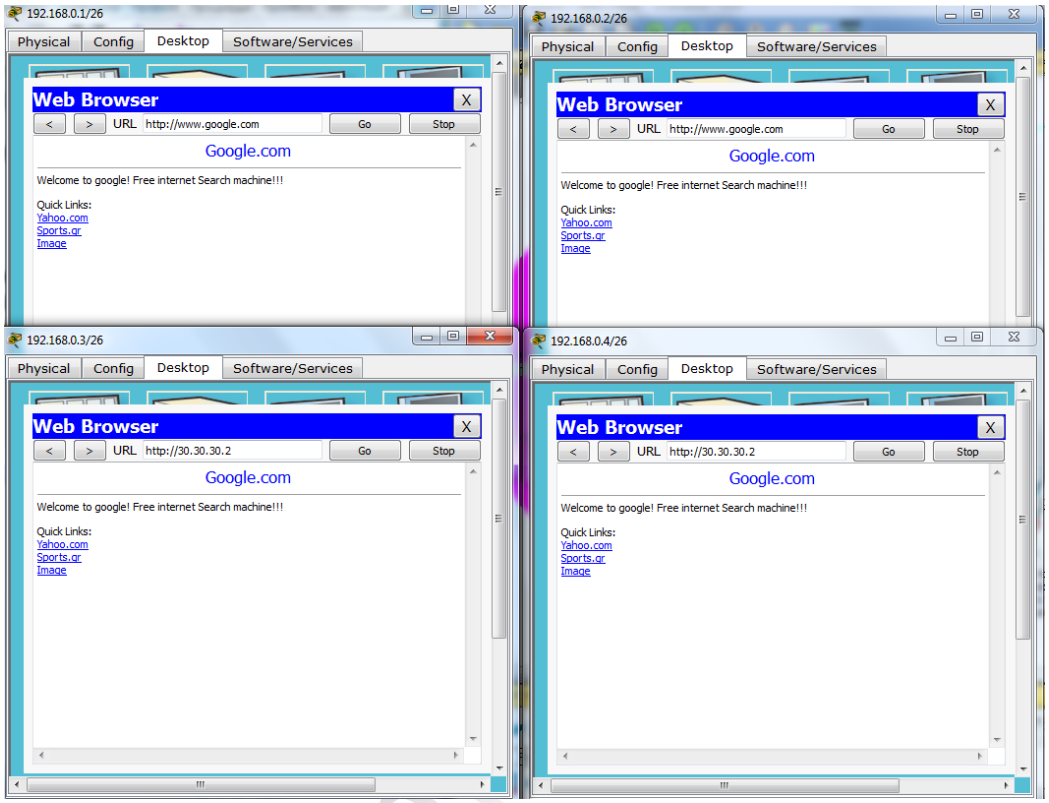
```
Router#show run
Building configuration...

Current configuration : 1213 bytes
!
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Router
!
!
!
!
!
!
ip cef
no ipv6 cef
!
!
!
!
```

```
crypto isakmp policy 10
encr aes 256
authentication pre-share
group 5
!
crypto isakmp key ISAKMP_KEY address 134.95.56.17
!
!
!
crypto ipsec transform-set firstset esp-aes 256 esp-sha-hmac
!
crypto map vpn 10 ipsec-isakmp
set peer 134.95.56.17
set pfs group5
set transform-set firstset
match address 101
!
!
!
!
!
!
spanning-tree mode pvst
!
!
!
!
!
!
interface FastEthernet0/0
ip address 134.95.56.18 255.255.255.240
duplex auto
speed auto
ipv6 ospf cost 1
crypto map vpn
!
interface FastEthernet0/1
ip address 172.16.129.1 255.255.255.0
duplex auto
speed auto
!
interface Vlan1
no ip address
shutdown
!
ip classless
ip route 192.168.0.0 255.255.255.192 134.95.56.17
ip route 192.168.1.0 255.255.255.252 134.95.56.17
ip route 192.168.3.0 255.255.255.252 134.95.56.17
```

```
!
ip flow-export version 9
!
!
access-list 101 permit ip 192.168.0.0 0.0.0.63 172.16.129.0 0.0.0.255
access-list 101 permit ip 172.16.129.0 0.0.0.255 192.168.0.0 0.0.0.63
!
!
!
!
!
line con 0
!
line aux 0
!
line vty 0 4
login
!
!
!
End
```

4.5.7 Πρόσβαση όλων των χρηστών στην ιστοσελίδα εξωτερικού δικτύου με διεύθυνση 30.30.30.2/24 (www.google.com)



Εικόνα 4.34 Πρόσβαση όλων των χρηστών στην ιστοσελίδα εξωτερικού δικτύου με διεύθυνση 30.30.30.2/24 (www.google.com)

4.5.8 Πρόσβαση του χρήστη 172.16.129.2/28 στην ιστοσελίδα εσωτερικού δικτύου με διεύθυνση 192.168.1.3/29 (www.internal.com)

Για να μπορεί ο συγκεκριμένος χρήστης να έχει πρόσβαση στην εσωτερική ιστοσελίδα του δικτύου, θα πρέπει να εφαρμοστούν κάποιες ρυθμίσεις τόσο από την πλευρά του δρομολογητή του, όσο και από τις συσκευές (FW-1, INSIDE ROUTER) που ανήκουν στο εσωτερικό δίκτυο και είναι οι εξής.

Router3:

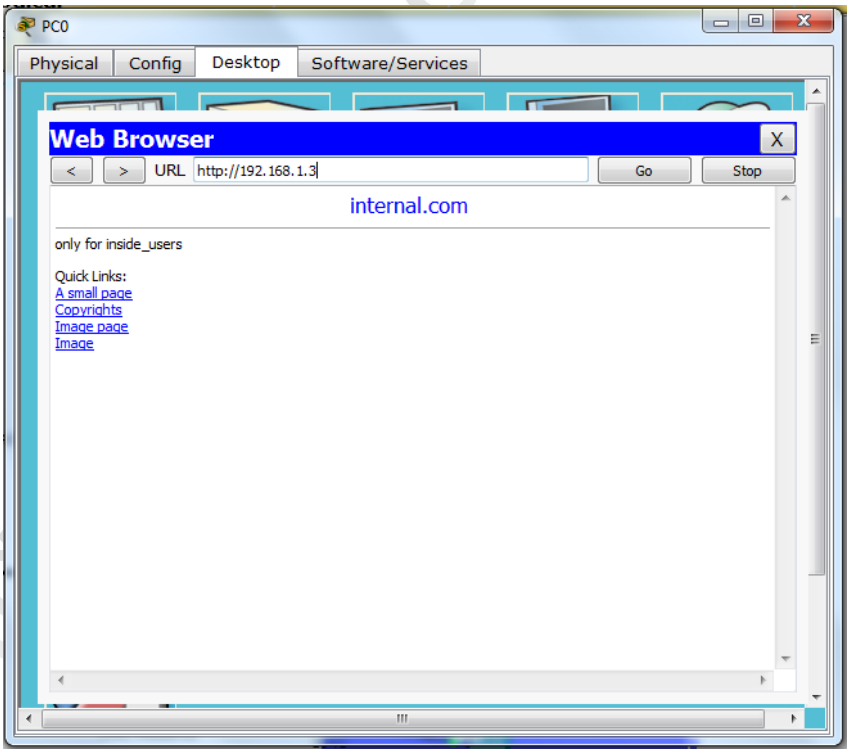
ip route 192.168.1.0 255.255.255.252 134.95.56.17

BORDER ROUTER:

ip route 30.30.30.0 255.255.255.0 134.95.56.19

FW-1

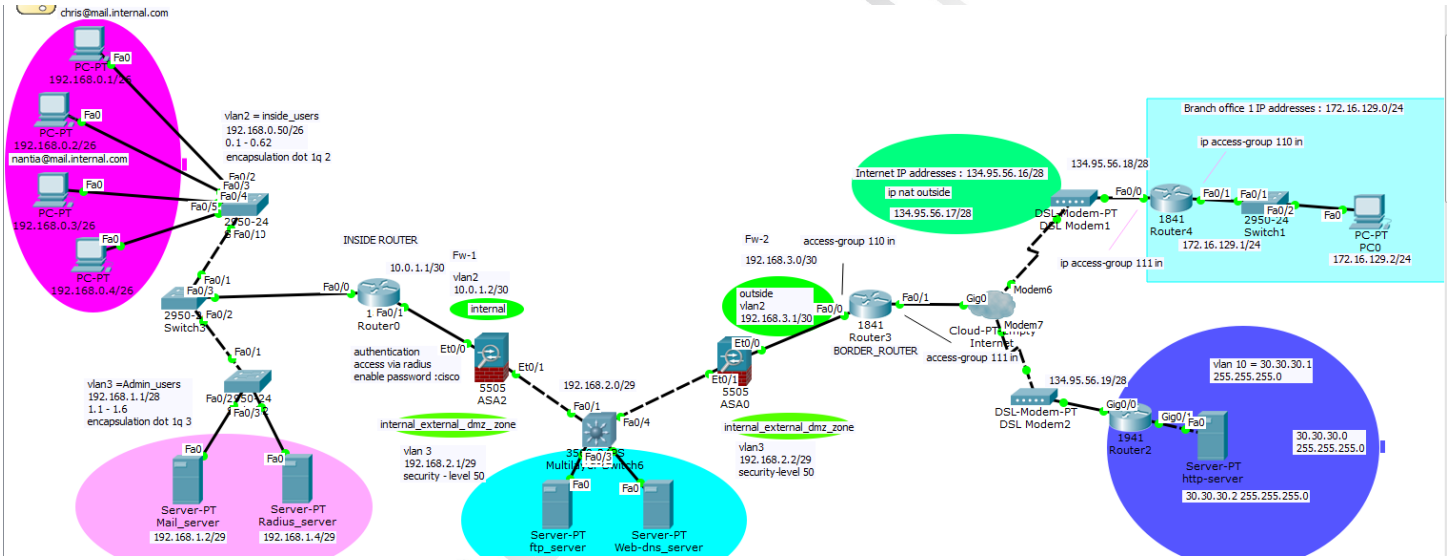
route outside 30.30.30.0 255.255.255.0 192.168.3.2 1
access-list outsidetoinside extended permit tcp host 172.16.129.2 host 192.168.1.3 eq www
access-list insidetooutside extended permit tcp host 192.168.1.3 host 172.16.129.2



Εικόνα 4.35 Πρόσβαση του χρήστη 172.16.129.2/28 στην ιστοσελίδα εσωτερικού δικτύου με διεύθυνση 192.168.1.3/29 (www.internal.com)

4.6 Εφαρμογή της αρχιτεκτονικής DMZ σε δίκτυο εταιρείας με την χρησιμοποίηση δύο Firewall (Dual firewall).

Στο παρακάτω σχήμα παρουσιάζετε ένα δίκτυο εταιρείας, το οποίο χρησιμοποιεί την αρχιτεκτονική DMZ και προστατεύετε με την χρησιμοποίηση δύο firewall. Το πρώτο firewall (FW-1) είναι υπεύθυνο για την προστασία των εσωτερικών χρηστών του δικτύου και για τους server's που ανήκουν στο εσωτερικό του δίκτυο (interface inside) και η άλλη διασύνδεση του firewall (interface internal_external_dmz_zone) προστατεύει την DMZ ζώνη που περιέχει τους server's που είναι διαθέσιμοι για παροχή υπηρεσιών προς το εξωτερικό δίκτυο και ελέγχει την κίνηση των δεδομένων που κατευθύνονται τόσο από το εσωτερικό δίκτυο προς τους server's που ανήκουν στην DMZ ζώνη όσο και την κίνηση των δεδομένων που προέρχεται τόσο από τους server's που ανήκουν στην DMZ ζώνη όσο και από τα δεδομένα που προέρχονται από την εξωτερική πλευρά του δικτύου.



Εικόνα 4.36 Εφαρμογή της αρχιτεκτονικής DMZ με την χρησιμοποίηση δύο Firewall (Dual Firewall)

Περιγραφή δεδομένων

Το συγκεκριμένο δίκτυο, αποτελείται από τα εξής στοιχεία:

- 4 Υπολογιστές, οι οποίοι ανήκουν στο εσωτερικό του δικτύου και έχουν διευθύνσεις IP, από 192.168.0.1 / 26 - 192.168.0.4/26

- 2 Server's, οι οποίοι ανήκουν στο εσωτερικό του δικτύου και επίσης ανήκουν και σε διαφορετικό υποδίκτυο, από αυτόν τον υπολογιστών που ανήκουν στους χρήστες του δικτύου και με διευθύνσεις IP συγκεκριμένα:

  - ✓ Για τον Mail_server με διεύθυνση 192.168.1.2/29
  - ✓ Για τον Radius_server με διεύθυνση 192.168.1.4/29

- Ένα τείχος προστασίας (Fw-1), ο οποίος βρίσκετε μπροστά από τον εσωτερικό δρομολογητή (INSIDE ROUTER) και ελέγχει τόσο την κίνηση των δεδομένων που έρχονται από την πλευρά της DMZ ζώνης και του εξωτερικού δικτύου προς το εσωτερικό, όσο και από το εσωτερικό δίκτυο προς την DMZ ζώνη του δικτύου και το εξωτερικό δίκτυο. Θα πραγματοποιηθεί εκτενέστερη ανάλυση του τείχους προστασίας, παρακάτω.

- 2 Server's, οι οποίοι ανήκουν στην DMZ ζώνη του δικτύου με διεύθυνση υποδικτύου 192.168.2.0/29 και συγκεκριμένα:

  - ✓ Για τον ftp_server με διεύθυνση 192.168.2.3/29
  - ✓ Για τον web-dns_server με διεύθυνση 192.168.2.4/29,

- Ένα δεύτερο τείχος προστασίας (Fw-2), το οποίο βρίσκετε μπροστά από την DMZ ζώνη του δικτύου και ελέγχει τόσο την κίνηση των δεδομένων που έρχονται από την πλευρά της DMZ ζώνης προς το εξωτερικό δίκτυο, όσο και από το εξωτερικό δίκτυο προς την DMZ ζώνη του δικτύου. Θα πραγματοποιηθεί εκτενέστερη ανάλυση και του δεύτερου τείχους προστασίας, παρακάτω.

- Ένας εσωτερικός δρομολογητής (BORDER ROUTER), ο οποίος αποτελεί το τελευταίο στοιχείο του δικτύου και αποτελεί το πρώτο φιλτράρισμα των δεδομένων που εισέρχονται στο δίκτυο. Εκτός από το φιλτράρισμα των δεδομένων πραγματοποιεί και την VPN σύνδεση με ένα δρομολογητή (Router3), ο οποίος βρίσκετε στην εξωτερική πλευρά του δικτύου (INTERNET) και επικοινωνεί μαζί του μέσω IPsec.

Από την μεριά του εξωτερικού δικτύου έχουμε τα εξής στοιχεία:

- Τον δρομολογητή (Router3), ο οποίος όπως αναφέραμε προηγουμένως χρησιμοποιείται για την VPN σύνδεση με τον δρομολογητή (BORDER ROUTER).
- Τον δρομολογητή (Router2), ο οποίος χρησιμοποιείται σαν δρομολογητής ενός απομακρυσμένου δικτύου για την εμφάνιση μίας ιστοσελίδας, την οποία έχουμε ονομάσει ως (google.com) με διεύθυνση 30.30.30.2.

Για να μπορούν να επικοινωνούν το εσωτερικό δίκτυο με τον εξωτερικά δίκτυα, τα οποία θεωρούμε, ότι υπάρχουν κάπου στο διαδίκτυο, χρησιμοποιούμε dsl-modem δίνοντας την εικόνα σύνδεσης των 3 αυτών δικτύων στο διαδίκτυο.
Και οι 3 Δρομολογητές, χρησιμοποιούν στατικές διευθύνσεις για την σύνδεση τους.

Αναλυτικά έχουμε:

- BORDER_ROUTER με διεύθυνση 134.95.56.17/28
- Router3 με διεύθυνση 134.95.56.18/28
- Router2 με διεύθυνση 134.95.56.19/28

Οι συγκεκριμένες εργασίες που πρέπει να εφαρμοστούν στο δίκτυο της εικόνας 4.17, είναι οι εξής:

- ✓ Επικοινωνία των 2 χρηστών 192.168.0.1/26 – 192.1168.0.2/26 μέσω ηλεκτρονικού ταχυδρομείου.
- ✓ Πρόσβαση στην εσωτερική ιστοσελίδα του δικτύου, μόνο των χρηστών 192.168.0.1/26 και 192.168.0.2/26.
- ✓ Επικοινωνία των 2 χρηστών 192.168.0.1/26 – 192.1168.0.2/26 με τον ftp server του δικτύου για την μεταφορά και ανταλλαγή αρχείων.
- ✓ Πραγματοποίηση VPN σύνδεσης μεταξύ των 2 δρομολογητών με διευθύνσεις IP 192.168.0.0/29 και 172.16.129.2/24.
- ✓ Όλοι οι χρήστες του δικτύου να έχουν πρόσβαση στην ιστοσελίδα εξωτερικού δικτύου με διεύθυνση 30.30.30.2/24.
- ✓ Ο χρήστης με διεύθυνση 172.16.129.2 να έχει πρόσβαση στην εσωτερική ιστοσελίδα του δικτύου με διεύθυνση 192.168.1.3.

4.6.1 Υπηρεσίες εσωτερικού δικτύου

Όπως και στην προηγούμενη εργαστηριακή άσκηση, έτσι και σε αυτήν υπάρχουν υπηρεσίες οι οποίες χρησιμοποιούνται μόνο για τους χρήστες που ανήκουν στο εσωτερικό Δίκτυο.

Ενδεικτικά, θα αναφέρουμε τις υπηρεσίες αυτές, οι οποίες είναι ίδιες με τις υπηρεσίες που υπάρχουν και στην προηγούμενη εργαστηριακή άσκηση και ο τρόπος λειτουργίας τους, είναι ίδιος με τον τρόπο λειτουργίας επίσης.

Οι υπηρεσίες που υπάρχουν είναι οι εξής:

- **Υπηρεσία Ηλεκτρονικού Ταχυδρομείου (e-mail)**

Η Υπηρεσία αυτή, χρησιμοποιείται μόνο από τους χρήστες του εσωτερικού δικτύου 192.168.0.1, με λογαριασμό (chris@mail.internal.com) και από τον χρήστη με διεύθυνση 192.168.0.2 και με λογαριασμό (nantia@mail.internal.com). Οι άλλοι 2 χρήστες του δικτύου δεν μπορούν να επικοινωνήσουν με τον mail_server του δικτύου, λόγω λίστας πρόσβασης (access-list 110) και με κανόνες:

```
access-list 110 permit tcp host 192.168.0.1 host 192.168.1.2 eq smtp
access-list 110 permit tcp host 192.168.0.2 host 192.168.1.2 eq smtp

access-list 110 permit tcp host 192.168.0.1 host 192.168.1.2 eq pop3
access-list 110 permit tcp host 192.168.0.2 host 192.168.1.2 eq pop3
```

- **Υπηρεσία Απομακρυσμένης μεταφοράς αρχείων, File Transfer Protocol (Ftp)**

Η Υπηρεσία αυτή, χρησιμοποιείται μόνο από τους χρήστες του εσωτερικού δικτύου 192.168.0.1 και 192.168.0.2 παρέχοντας την δυνατότητα μεταφοράς αρχείων με τον ftp_server του δικτύου, ο οποίος βρίσκετε στην DMZ ζώνη, δίνοντας την δυνατότητα παροχής υπηρεσιών του και σε χρήστες που μπορεί να ανήκουν και στην εξωτερική πλευρά του δικτύου. Οι άλλοι 2 χρήστες του εσωτερικού δικτύου, δεν μπορούν να επικοινωνήσουν με τον ftp_server, λόγω λίστας πρόσβασης (access-list 110) και με κανόνες:

```
access-list 110 permit ip host 192.168.0.1 host 192.168.2.3
access-list 110 permit ip host 192.168.0.2 host 192.168.2.3
```

Παρατηρούμε ότι στην συγκεκριμένη υπηρεσία, χρησιμοποιήσαμε πλήρης πρόσβαση στον ftp server από τους 2 χρήστες του δικτύου για τον λόγο ότι οι 2 χρήστες θα πρέπει να διαθέτουν πλήρης πρόσβαση στον server.

αποτρέποντας τους άλλους 2 χρήστες:

```
access-list 110 deny ip any any
```

- **Υπηρεσία αυθεντικοποίησης χρηστών για χρήση δικτυακών συσκευών (Radius server)**

Επίσης το δίκτυο, μας παρέχει την δυνατότητα χρησιμοποίησης υπηρεσίας, η οποία έχει την δυνατότητα αυθεντικοποίησης για χρησιμοποίηση δικτυακών συσκευών, (στην εργαστηριακή άσκηση έχουμε ρυθμίσει τον εσωτερικό δρομολογητή INSIDE ROUTER), από τον εσωτερικό χρήστη του δικτύου 192.168.0.1. Οι υπόλοιποι χρήστες του εσωτερικού δικτύου, δεν μπορούν έχουν πρόσβαση στις ρυθμίσεις του δρομολογητή μέσω telnet.

```
access-list 110 permit tcp host 192.168.0.1 host 192.168.1.4 eq 1645
access-list 110 permit udp host 192.168.0.1 host 192.168.1.4 eq 1645
access-list 110 permit tcp host 192.168.0.1 host 192.168.1.1 eq telnet
```

- **Υπηρεσία πρόσβασης των χρηστών στην εσωτερική ιστοσελίδα του δικτύου (internal.com) καθώς και χρησιμοποίηση της υπηρεσίας domain name**

Η Υπηρεσία αυτή, χρησιμοποιείται μόνο από τους χρήστες του εσωτερικού δικτύου 192.168.0.1 και 192.168.0.2 παρέχοντας την δυνατότητα πρόσβασης στην εσωτερική ιστοσελίδα του δικτύου που ανήκει στον web-dns_server του δικτύου, ο οποίος βρίσκετε στην εσωτερική πλευρά, δίνοντας την δυνατότητα παροχής υπηρεσιών του στον χρήστη με διεύθυνση 172.16.129.2 που ανήκει στην εξωτερική πλευρά του δικτύου. Οι άλλοι 2 χρήστες του εσωτερικού δικτύου, δεν μπορούν να έχουν πρόσβαση στον web-dns_server, λόγω λίστας πρόσβασης (access-list 110) και με κανόνες:

```
access-list 110 permit tcp host 192.168.0.1 host 192.168.2.4 eq www
access-list 110 permit tcp host 192.168.0.2 host 192.168.2.4 eq www
```

4.6.2 Εσωτερικός δρομολογητής (INSIDE ROUTER)

Είναι ο δρομολογητής, ο οποίος βρίσκετε από την πλευρά του εσωτερικού δικτύου, και είναι υπεύθυνος για τον έλεγχο της κίνησης των δεδομένων, τόσο από την πλευρά των χρηστών, όσο και από την πλευρά των server's που ανήκουν στην μεριά του εσωτερικού δικτύου.

Για να μπορέσουμε να χρησιμοποιήσουμε τον συγκεκριμένο δρομολογητή όπως έχουμε αναφέρει και προηγουμένως, θα πρέπει οι χρήστες να αυθεντικοποιήσουν την πρόσβαση τους μέσα από τον radius_server και χρησιμοποιώντας ως όνομα χρήστη το όνομα <chris> και ως κωδικό πρόσβασης τον κωδικό <secret>.

- **Configuration file του δρομολογητή (INSIDE ROUTER)**

```
User Access Verification

Username: chris
Password:
Router0>en
Router0#show run
Building configuration...
Current configuration : 3183 bytes
!
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Router0
!
!Ρυθμίσεις που χρησιμοποιούνται για την υποστήριξη της υπηρεσίας ftp ως προς
!τους χρήστες του υποδικτύου που θα την χρησιμοποιούν
ip dhcp pool ftppool
network 192.168.0.0 255.255.255.192
default-router 192.168.0.50
dns-server 192.168.2.4
!Η υποστήριξη της υπηρεσίας ftp θα πραγματοποιείται από server ο οποίος
!βρίσκετε στο υποδίκτυο 192.168.2.0
ip dhcp pool ftpserver
network 192.168.2.0 255.255.255.248
default-router 192.168.2.1
dns-server 192.168.2.4
!
```

```
!δημιουργία πολιτικής προστασίας του δρομολογητή στηριζόμενο στο μοντέλο
!AAA (Authentication Authorization Accounting)
aaa new-model
!
!Αυθεντικοποίηση των χρηστών μέσω του radius_server
aaa authentication login default group radius none
!Η πραγματοποίηση αυθεντικοποίησης των χρηστών για πρόσβαση στον
!δρομολογητή γίνετε μέσω telnet
aaa authentication login teknet-lines group radius
!
ip cef
no ipv6 cef
!
ip ftp username chris
ip ftp password ntikos
ip ssh version 1
!
!
spanning-tree mode pvst
!
interface FastEthernet0/0
no ip address
duplex auto
speed auto
!
!Είναι η διασύνδεση που χρησιμοποιείται τους εσωτερικούς χρήστες του δικτύου
interface FastEthernet0/0.2
!Σύνδεση του VLAN 2 των εσωτερικών χρηστών με την διασύνδεση που ανήκει
!στην fa0/0
encapsulation dot1Q 2
ip address 192.168.0.50 255.255.255.192
!ενεργοποίηση της λίστας πρόσβασης 110 που ανήκει στην διασύνδεση 0/0.2
ip access-group 110 in
!
!Σύνδεση του VLAN 3 των Server's που ανήκουν στο εσωτερικό δίκτυο με την
!διασύνδεση που ανήκει στην fa0/0
interface FastEthernet0/0.3
encapsulation dot1Q 3
ip address 192.168.1.1 255.255.255.248
!ενεργοποίηση της λίστας πρόσβασης 110 που ανήκει στην διασύνδεση 0/0.3
ip access-group 110 in
!
interface FastEthernet0/1
ip address 10.0.1.1 255.255.255.252
ip access-group 105 out
duplex auto
speed auto
ipv6 ospf cost 1
```

```
!
interface Vlan1
no ip address
shutdown
!
ip classless
!ενεργοποίηση στατικών δρομολογήσεων τόσο από την μεριά του εσωτερικού
!δικτύου, όσο και από την μεριά του εξωτερικού δικτύου και από την ζώνη DMZ
ip route 134.95.56.16 255.255.255.240 10.0.1.2
ip route 192.168.0.0 255.255.255.192 10.0.1.2
ip route 192.168.1.0 255.255.255.248 10.0.1.2
ip route 172.16.129.0 255.255.255.0 10.0.1.2
ip route 30.30.30.0 255.255.255.0 10.0.1.2
ip route 192.168.2.0 255.255.255.248 10.0.1.2
ip route 192.168.3.0 255.255.255.252 10.0.1.2
!
ip flow-export version 9
!
!
!Λίστα πρόσβασης 110
! είναι το σύνολο των κανόνων που ασχολούνται με το εσωτερικό δίκτυο
access-list 110 permit ip host 192.168.0.1 host 192.168.2.3
access-list 110 permit ip host 192.168.0.2 host 192.168.2.3
access-list 110 permit tcp host 192.168.0.1 host 192.168.2.4 eq www
access-list 110 permit tcp host 192.168.0.2 host 192.168.2.4 eq www
access-list 110 permit tcp host 192.168.0.1 host 192.168.1.2 eq smtp
access-list 110 permit tcp host 192.168.0.2 host 192.168.1.2 eq smtp
access-list 110 permit tcp host 192.168.0.1 host 192.168.2.4 eq 22
access-list 110 permit tcp host 192.168.0.2 host 192.168.2.4 eq 22
access-list 110 permit udp host 192.168.0.1 host 192.168.2.4 eq 22
access-list 110 permit udp host 192.168.0.2 host 192.168.2.4 eq 22
access-list 110 permit tcp host 192.168.0.1 host 192.168.1.2 eq pop3
access-list 110 permit tcp host 192.168.0.2 host 192.168.1.2 eq pop3
access-list 110 permit tcp 192.168.0.0 0.0.0.63 host 30.30.30.2 eq www
access-list 110 permit tcp host 192.168.0.1 host 192.168.1.4 eq 1645
access-list 110 permit udp host 192.168.0.1 host 192.168.1.4 eq 1645
access-list 110 permit tcp host 192.168.0.1 host 192.168.1.1 eq telnet
access-list 110 permit udp 192.168.0.0 0.0.0.63 host 192.168.2.4 eq domain
access-list 110 deny ip any any
!Λίστα πρόσβασης 111
!είναι το σύνολο των κανόνων που ασχολούνται με το δίκτυο των εσωτερικών
!δρομολογητών
access-list 111 permit tcp host 192.168.0.1 host 192.168.1.2 eq smtp
access-list 111 permit tcp host 192.168.0.2 host 192.168.1.2 eq smtp
access-list 111 permit tcp host 192.168.0.1 host 192.168.1.2 eq pop3
access-list 111 permit tcp host 192.168.0.2 host 192.168.1.2 eq pop3
access-list 111 permit tcp host 192.168.1.1 host 192.168.1.4 eq 1645
access-list 111 permit tcp host 192.168.0.1 host 192.168.1.4 eq 1645
```

```
access-list 111 permit tcp host 192.168.1.4 host 192.168.1.1 eq 1645
access-list 111 permit tcp host 192.168.1.2 host 192.168.0.1
access-list 111 permit tcp host 192.168.1.2 host 192.168.0.2
access-list 111 deny ip any any

! προσδιορισμός της διεύθυνσης του radius_server, της πόρτας στην οποία θα
!πραγματοποιηθεί η σύνδεση, αλλά και του κωδικού πρόσβασης (radius)
radius-server host 192.168.1.4 auth-port 1645 key radius
!
!
!
line con 0
!
line aux 0
!
line vty 0 4
!αυθεντικοποίηση των χρηστών μέσω telnet σύνδεσης
login authentication teknet-lines
!
!
!

end
```

4.6.3 Τείχος προστασίας – Firewall (FW-1)

Το πρώτο τείχος προστασίας, ελέγχει της κινήσεις των δεδομένων τόσο από το εσωτερικό δίκτυο προς την ζώνη DMZ του δικτύου, όσο και από την ζώνη DMZ προς το εσωτερικό.

Για την διευκόλυνση μας ορίσαμε την διασύνδεση η οποία βρίσκετε από την μεριά του εσωτερικού δικτύου ως inside και την διασύνδεση η οποία βρίσκετε από την μεριά της ζώνης DMZ του δικτύου ως internal_external_dmz_zone .

```
interface Ethernet0/0
switchport access vlan 2

!
interface Vlan2
nameif inside
security-level 100
ip address 10.0.1.2 255.255.255.252
!
interface Ethernet0/1
switchport access vlan 3

!
interface Vlan3
nameif internal_external_dmz_zone
security-level 50
ip address 192.168.2.1 255.255.255.248
!
```

Για να μπορούμε να ξεχωρίζουμε εύκολα τις 2 λίστες πρόσβασης που θα χρησιμοποιήσουμε, ονομάσαμε την μία λίστα πρόσβασης insidetooutside και απευθύνετε στα δεδομένα με κατεύθυνση από το εσωτερικό δίκτυο προς το εξωτερικό και την άλλη outsidetoinside με κατεύθυνση από το εξωτερικό δίκτυο προς το εσωτερικό.

```
access-list outsidetoinside extended permit icmp 192.168.2.0 255.255.255.248
192.168.0.0 255.255.255.192
access-list outsidetoinside extended permit icmp 192.168.2.0 255.255.255.248
192.168.1.0 255.255.255.248
access-list outsidetoinside extended permit udp 192.168.2.0 255.255.255.248
192.168.0.0 255.255.255.192
access-list outsidetoinside extended permit tcp 192.168.2.0 255.255.255.248
192.168.0.0 255.255.255.192
access-list outsidetoinside extended permit tcp host 30.30.30.2 192.168.0.0
255.255.255.192
access-list insidetooutside extended permit icmp 192.168.0.0 255.255.255.192
30.30.30.0 255.255.255.0
```

access-list insidetooutside extended permit udp 192.168.0.0 255.255.255.192 192.168.2.0 255.255.255.248
access-list insidetooutside extended permit tcp host 192.168.0.1 host 192.168.2.4 eq www
access-list insidetooutside extended permit tcp host 192.168.0.2 host 192.168.2.4 eq www
access-list insidetooutside extended permit tcp host 192.168.0.1 host 192.168.2.3
access-list insidetooutside extended permit udp host 192.168.0.1 host 192.168.2.3
access-list insidetooutside extended permit udp host 192.168.0.2 host 192.168.2.3
access-list insidetooutside extended permit tcp host 192.168.0.2 host 192.168.2.3
access-list insidetooutside extended permit tcp 192.168.0.0 255.255.255.192 host 30.30.30.2 eq www

Στην συνέχεια, για να μπορούν αυτές οι λίστες να εφαρμοστούν, επάνω στις διασυνδέσεις, χρησιμοποιούμε τις παρακάτω εντολές

access-group outsidetoinside out interface inside
access-group insidetooutside in interface inside

- **Configuration file του τείχους προστασίας (FW-1)**

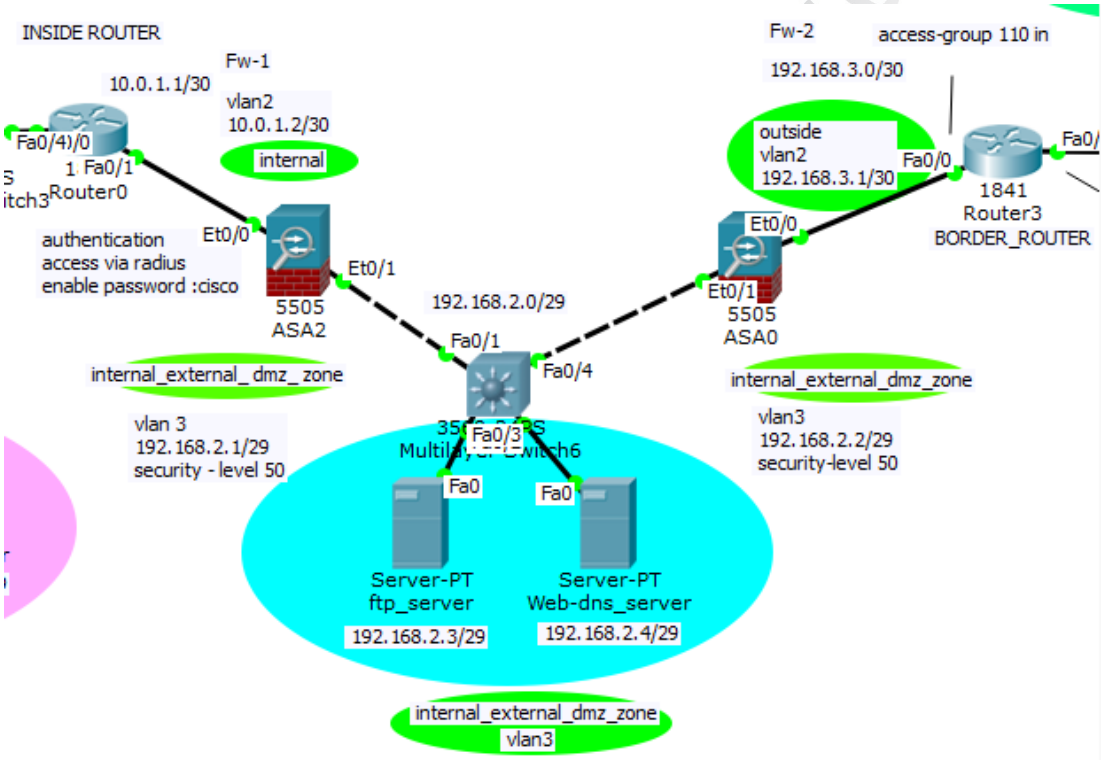
ciscoasa>
ciscoasa>en
Password:
ciscoasa#show run
: Saved
:
ASA Version 8.4(2)
!
hostname ciscoasa
names
!
interface Ethernet0/0
switchport access vlan 2
!
interface Ethernet0/1
switchport access vlan 3
!
interface Ethernet0/2
!
interface Ethernet0/3
!
interface Ethernet0/4
!
interface Ethernet0/5
!
interface Ethernet0/6
!

```
interface Ethernet0/7
!
interface Vlan1
no nameif
no security-level
no ip address
!
interface Vlan2
nameif inside
security-level 100
ip address 10.0.1.2 255.255.255.252
!
interface Vlan3
nameif internal_external_dmz_zone
security-level 50
ip address 192.168.2.1 255.255.255.248
!
!
route inside 192.168.0.0 255.255.255.192 10.0.1.1 1
route inside 192.168.1.0 255.255.255.248 10.0.1.1 1
route internal_external_dmz_zone 192.168.3.0 255.255.255.252 192.168.2.2 1
route internal_external_dmz_zone 172.16.129.0 255.255.255.0 192.168.2.2 1
route internal_external_dmz_zone 30.30.30.0 255.255.255.0 192.168.2.2 1
!
access-list outsidetoinside extended permit icmp 192.168.2.0 255.255.255.248
192.168.0.0 255.255.255.192
access-list outsidetoinside extended permit icmp 192.168.2.0 255.255.255.248
192.168.1.0 255.255.255.248
access-list outsidetoinside extended permit udp 192.168.2.0 255.255.255.248
192.168.0.0 255.255.255.192
access-list outsidetoinside extended permit tcp 192.168.2.0 255.255.255.248
192.168.0.0 255.255.255.192
access-list outsidetoinside extended permit tcp host 30.30.30.2 192.168.0.0
255.255.255.192
access-list insidetooutside extended permit icmp 192.168.0.0 255.255.255.192
30.30.30.0 255.255.255.0
access-list insidetooutside extended permit udp 192.168.0.0 255.255.255.192
192.168.2.0 255.255.255.248
access-list insidetooutside extended permit tcp host 192.168.0.1 host 192.168.2.4 eq
www
access-list insidetooutside extended permit tcp host 192.168.0.2 host 192.168.2.4 eq
www
access-list insidetooutside extended permit tcp host 192.168.0.1 host 192.168.2.3
access-list insidetooutside extended permit udp host 192.168.0.1 host 192.168.2.3
access-list insidetooutside extended permit udp host 192.168.0.2 host 192.168.2.3
access-list insidetooutside extended permit tcp host 192.168.0.2 host 192.168.2.3
access-list insidetooutside extended permit tcp 192.168.0.0 255.255.255.192 host
30.30.30.2 eq www
```

```
!
access-group outsidetoinside out interface inside
access-group insidetooutside in interface inside
!
!
!
!
!
!
!
telnet timeout 5
ssh timeout 5
!
dhcpd enable
!
dhcpd auto_config outside
!
!
!
!
!
```

4.6.4 DMZ ζώνη (internal_external_dmz_zone)

Πρόκειται για την ζώνη, η οποία περιβάλετε και προστατεύετε από τα 2 firewall του δικτύου (FW-1) και (FW-2). Η ζώνη αυτή περιλαμβάνει τους 2 server's, οι οποίοι παρέχουν υπηρεσίες εκτός από τους εσωτερικούς χρήστες του δικτύου και στους εξωτερικούς χρήστες του δικτύου με ελεγχόμενη κίνηση από τον FW-2. Για την επικοινωνία των 2 firewall μεταξύ τους, παρεμβάλετε ένα switch στο οποίο τα interface του, καθώς και τα interface E0/1 του FW-1 και του FW-2 ανήκουν όλα στο VLAN 3. Αυτό γίνετε για να υπάρχει η επικοινωνία με όλες τις δικτυακές συσκευές που υπάρχουν στο ίδιο εικονικό τοπικό δίκτυο.



Εικόνα 4.37 Απεικόνιση της ζώνης DMZ internal_external_dmz_zone

4.6.5 Τείχος προστασίας – Firewall (FW-2)

Το δεύτερο τείχος προστασίας, ελέγχει της κινήσεις των δεδομένων τόσο από την ζώνη DMZ του δικτύου προς το εξωτερικό δίκτυο, όσο και από το εξωτερικό δίκτυο προς την ζώνη DMZ.

Για την διευκόλυνση μας ορίσαμε την διασύνδεση η οποία βρίσκετε από την μεριά του εξωτερικού δικτύου ως outside και την διασύνδεση η οποία βρίσκετε από την μεριά της ζώνης DMZ του δικτύου ως internal_external_dmz_zone .

```
interface Ethernet0/0
switchport access vlan 2

!
interface Vlan2
nameif outside
security-level 0
ip address 192.168.3.1 255.255.255.252!
interface Ethernet0/1
switchport access vlan 3

!
interface Vlan3
nameif internal_external_dmz_zone
security-level 50
ip address 192.168.2.2 255.255.255.248
!
```

Για να μπορούμε να ξεχωρίζουμε εύκολα τις 2 λίστες πρόσβασης που θα χρησιμοποιήσουμε, ονομάσαμε την μία λίστα πρόσβασης insidetooutside και απευθύνετε στα δεδομένα με κατεύθυνση από το εσωτερικό δίκτυο προς το εξωτερικό και την άλλη outsidetoinside με κατεύθυνση από το εξωτερικό δίκτυο προς το εσωτερικό.

```
access-list insidetooutside extended permit udp 192.168.2.0 255.255.255.248 192.168.0.0 255.255.255.192
access-list insidetooutside extended permit tcp host 192.168.2.4 host 172.16.129.2
access-list insidetooutside extended permit tcp host 192.168.2.4 host 192.168.0.1
access-list insidetooutside extended permit tcp host 192.168.2.4 host 192.168.0.2
access-list insidetooutside extended permit icmp 192.168.0.0 255.255.255.192 host 30.30.30.2
access-list insidetooutside extended permit tcp 192.168.0.0 255.255.255.192 host 30.30.30.2 eq www
access-list insidetooutside extended permit tcp 192.168.2.0 255.255.255.248 192.168.0.0 255.255.255.192
```

access-list outsidetoinside extended permit icmp 192.168.3.0 255.255.255.252 192.168.0.0 255.255.255.192
access-list outsidetoinside extended permit icmp host 30.30.30.2 192.168.0.0 255.255.255.192
access-list outsidetoinside extended permit tcp host 30.30.30.2 192.168.0.0 255.255.255.192
access-list outsidetoinside extended permit tcp host 172.16.129.2 host 192.168.2.4 eq www

Στην συνέχεια, για να μπορούν αυτές οι λίστες να εφαρμοστούν, επάνω στις διασυνδέσεις, χρησιμοποιούμε τις παρακάτω εντολές

access-group insidetooutside out interface outside
access-group insidetooutside in interface internal_external_dmz_zone
access-group outsidetoinside in interface outside
access-group outsidetoinside out interface internal_external_dmz_zone

- **Configuration file του τείχους προστασίας (FW-2)**

ciscoasa>
ciscoasa>
ciscoasa>en
Password:
ciscoasa#show run
: Saved
:
ASA Version 8.4(2)
!
hostname ciscoasa
names
!
interface Ethernet0/0
switchport access vlan 2
!
interface Ethernet0/1
switchport access vlan 3
!
interface Ethernet0/2
!
interface Ethernet0/3
!
interface Ethernet0/4
!
interface Ethernet0/5
!
interface Ethernet0/6

```
!
interface Ethernet0/7
!
interface Vlan1
no nameif
no security-level
no ip address
!
interface Vlan2
nameif outside
security-level 0
ip address 192.168.3.1 255.255.255.252
!
interface Vlan3
nameif internal_external_dmz_zone
security-level 50
ip address 192.168.2.2 255.255.255.248
!
interface Vlan4
no nameif
no security-level
no ip address
!
!
route internal_external_dmz_zone 192.168.0.0 255.255.255.192 192.168.2.1 1
route internal_external_dmz_zone 192.168.0.0 255.255.255.192 172.16.129.2 1
route outside 172.16.129.0 255.255.255.0 192.168.0.0 1
route internal_external_dmz_zone 192.168.0.0 255.255.255.192 30.30.30.2 1
route outside 30.30.30.0 255.255.255.0 192.168.0.0 1
!
access-list insidetooutside extended permit udp 192.168.2.0 255.255.255.248
192.168.0.0 255.255.255.192
access-list insidetooutside extended permit tcp host 192.168.2.4 host 172.16.129.2
access-list insidetooutside extended permit tcp host 192.168.2.4 host 192.168.0.1
access-list insidetooutside extended permit tcp host 192.168.2.4 host 192.168.0.2
access-list insidetooutside extended permit icmp 192.168.0.0 255.255.255.192 host
30.30.30.2
access-list insidetooutside extended permit tcp 192.168.0.0 255.255.255.192 host
30.30.30.2 eq www
access-list insidetooutside extended permit tcp 192.168.2.0 255.255.255.248
192.168.0.0 255.255.255.192
access-list outsidetoinside extended permit icmp 192.168.3.0 255.255.255.252
192.168.0.0 255.255.255.192
access-list outsidetoinside extended permit icmp host 30.30.30.2 192.168.0.0
255.255.255.192
access-list outsidetoinside extended permit tcp host 30.30.30.2 192.168.0.0
255.255.255.192
```

```
access-list outsidetoinside extended permit tcp host 172.16.129.2 host 192.168.2.4 eq
www
!
access-group insidetooutside out interface outside
access-group insidetooutside in interface internal_external_dmz_zone
access-group outsidetoinside in interface outside
access-group outsidetoinside out interface internal_external_dmz_zone
!
!
!
!
!
!
!
telnet timeout 5
ssh timeout 5
!
dhcpd enable
!
dhcpd auto_config outside
!
!
!
!
!
```

4.6.6 Εσωτερικός δρομολογητής (BORDER ROUTER)

Ο δρομολογητής αυτός, αποτελεί τον <<ακρογωνιαίο λίθο>> του δικτύου, συνδεοντάς μας με τα υπόλοιπα δίκτυα του διαδικτύου. Εκτός από την σύνδεση μας με το διαδίκτυο, αποτελεί το ένα μέλους του ζεύγους (το άλλο είναι το router3), για την VPN σύνδεση που θα εφαρμόσουμε στην συγκεκριμένη εργαστηριακή άσκηση.

- **Configuration file του εσωτερικού δρομολογητή (BORDER ROUTER)**

```
Router#show run
Building configuration...

Current configuration : 1885 bytes
!
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Router
!
ip cef
no ipv6 cef
!
!
crypto isakmp policy 10
encr aes 256
authentication pre-share
group 5
!
crypto isakmp key ISAKMP_KEY address 134.95.56.18
!
!
!
crypto ipsec transform-set firstset esp-aes 256 esp-sha-hmac
!
crypto map vpn 10 ipsec-isakmp
set peer 134.95.56.18
set pfs group5
set transform-set firstset
match address 101
!
!
spanning-tree mode pvst
!
interface FastEthernet0/0
ip address 192.168.3.2 255.255.255.252
ip access-group 110 in
```

```
duplex auto
speed auto
ipv6 ospf cost 1
!
interface FastEthernet0/1
ip address 134.95.56.17 255.255.255.240
ip access-group 111 in
duplex auto
speed auto
crypto map vpn
!
interface Vlan1
no ip address
shutdown
!
ip classless
ip route 192.168.2.0 255.255.255.248 192.168.3.1
ip route 192.168.0.0 255.255.255.192 192.168.3.1
ip route 172.16.129.0 255.255.255.0 134.95.56.18
ip route 30.30.30.0 255.255.255.0 134.95.56.19
!
ip flow-export version 9
!
access-list 101 permit tcp 172.16.129.0 0.0.0.255 192.168.2.0 0.0.0.7
access-list 101 permit tcp 192.168.2.0 0.0.0.7 172.16.129.0 0.0.0.255
access-list 111 permit tcp host 172.16.129.2 host 192.168.2.4
access-list 111 permit udp host 134.95.56.18 host 134.95.56.17
access-list 111 permit ip host 30.30.30.2 192.168.0.0 0.0.0.63
access-list 111 permit esp host 134.95.56.18 host 134.95.56.17
!
line con 0
!
line aux 0
!
line vty 0 4
login
!
End
```

4.6.7 VPN σύνδεση site to site μεταξύ των 2 δρομολογητών BORDER ROUTER και Router3

Όπως και στην προηγουμένη εργαστηριακή άσκηση και εδώ θα εφαρμόσουμε μία VPN σύνδεση μεταξύ του BORDER ROUTER του εσωτερικού μας δικτύου και ενός Router που ανήκει στα εξωτερικά δίκτυα (Router4).

Σκοπός της VPN σύνδεσης μεταξύ 2 σημείων, όπως έχουμε αναφέρει και σε προηγούμενα κεφάλαια, είναι η κρυπτογράφηση και η αυθεντικοποίηση των δεδομένων που διέρχονται από αυτές τις 2 μεριές του δικτύου (μέσω ESP Tunnel), παρέχοντας παράλληλα την ασφάλεια ενός ιδιωτικού δικτύου και σε αυτή την περίπτωση η σύνδεση, αποτελεί την βασική αρχιτεκτονική μίας IPsec λειτουργίας.

Για να μπορέσουμε να εφαρμόσουμε αυτή την τεχνική στους 2 δρομολογητές θα κάνουμε τις εξής ρυθμίσεις:

Για τον BORDER ROUTER έχουμε :

```
! Προσδιορισμός της IKE πολιτικής για την συγκεκριμένη VPN σύνδεση.
! Χρησιμοποιήθηκε η AES κρυπτογραφία 256 bit, κλειδιά pre-share και αλγόριθμος
! diffie-hellman group 5. Επίσης χρησιμοποιήθηκε και η κρυπτογραφική function SHA-1
! η οποία επειδή είναι default δεν εμφανίζετε στο configuration file του δρομολογητή.
crypto isakmp policy 10
encr aes 256
authentication pre-share
group 5

! Προσδιορισμός των pre-share κλειδιών, τα οποία είναι μοναδικά για κάθε ζευγάρι.
! Ας σημειωθεί ότι τα κλειδιά όπως και κάθε κλειδί καλό είναι να αποτελούνται από
! διαφόρων είδη χαρακτήρων (πεζά, κεφαλαία, αριθμούς, σύμβολα)
! δυσκολεύοντας με αυτόν τον τρόπο την αποκωδικοποίηση τους.
crypto isakmp key ISAKMP_KEY address 134.95.56.18


! το  ipsec transform-set είναι ένα πρωτόκολλο επικοινωνίας μεταξύ των 2 συσκεύων το
! οποίο στην συγκεκριμένη περίπτωση μας κρυπτογραφεί τα δεδομένα μέσω aes μήκους
! 256 bit και χρησιμοποιεί την sha-1 για την ακεραιότητα των δεδομένων.
crypto ipsec transform-set firstset esp-aes 256 esp-sha-hmac


! το κάθε ζεύγος που χρησιμοποιείται για την vpn σύνδεση έχει το δικό του crypto map το
! οποίο εφαρμόζετε επάνω στην διασύνδεση του κάθε δρομολογητή και σε αυτόν
! καθορίζετε η συσκευή η οποία αποτελεί το άλλο μέλος του ζεύγους, το <<pfs>> το οποίο
! μας σιγουρεύει ότι τα κλειδιά τα οποία έχουν παραχθεί για αυτή την σύνδεση μετά το
! τέλος της διάρκειας τους, δεν θα είναι σε θέση να ξανά παραχθούν και ότι η κυκλοφορία
! των δεδομένων θα είναι σε συμφωνία με την λίστα πρόσβασης 101
crypto map vpn 10 ipsec-isakmp
set peer 134.95.56.18
```

```
set pfs group5
set transform-set firstset
match address 101
! λίστα πρόσβασης 101
access-list 101 permit ip 192.168.0.0 0.0.0.63 172.16.129.0 0.0.0.255
access-list 101 permit ip 172.16.129.0 0.0.0.255 192.168.0.0 0.0.0.63

! λίστα πρόσβασης 111
access-list 111 permit tcp host 172.16.129.2 host 192.168.2.4
access-list 111 permit udp host 134.95.56.18 host 134.95.56.17
access-list 111 permit ip host 30.30.30.2 192.168.0.0 0.0.0.63
access-list 111 permit esp host 134.95.56.18 host 134.95.56.17
```

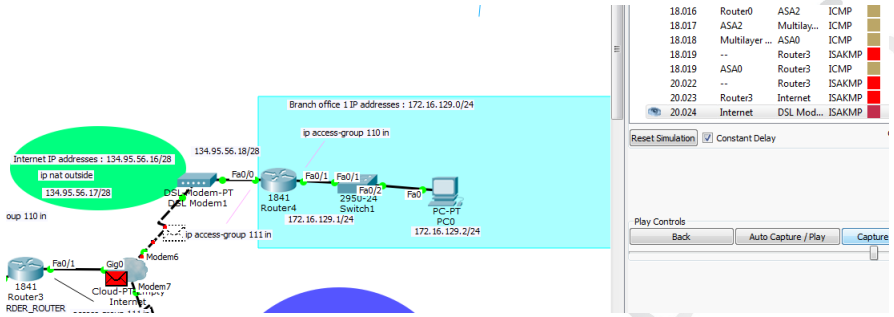
Ομοίως για τον Router4 έχουμε:

```
crypto isakmp policy 10
encr aes 256
authentication pre-share
group 5
!
crypto isakmp key ISAKMP_KEY address 134.95.56.17
!
!
!
crypto ipsec transform-set firstset esp-aes 256 esp-sha-hmac
!
crypto map vpn 10 ipsec-isakmp
set peer 134.95.56.17
set pfs group5
set transform-set firstset
match address 101
access-list 101 permit ip 192.168.0.0 0.0.0.63 172.16.129.0 0.0.0.255
access-list 101 permit ip 172.16.129.0 0.0.0.255 192.168.0.0 0.0.0.63
!
```

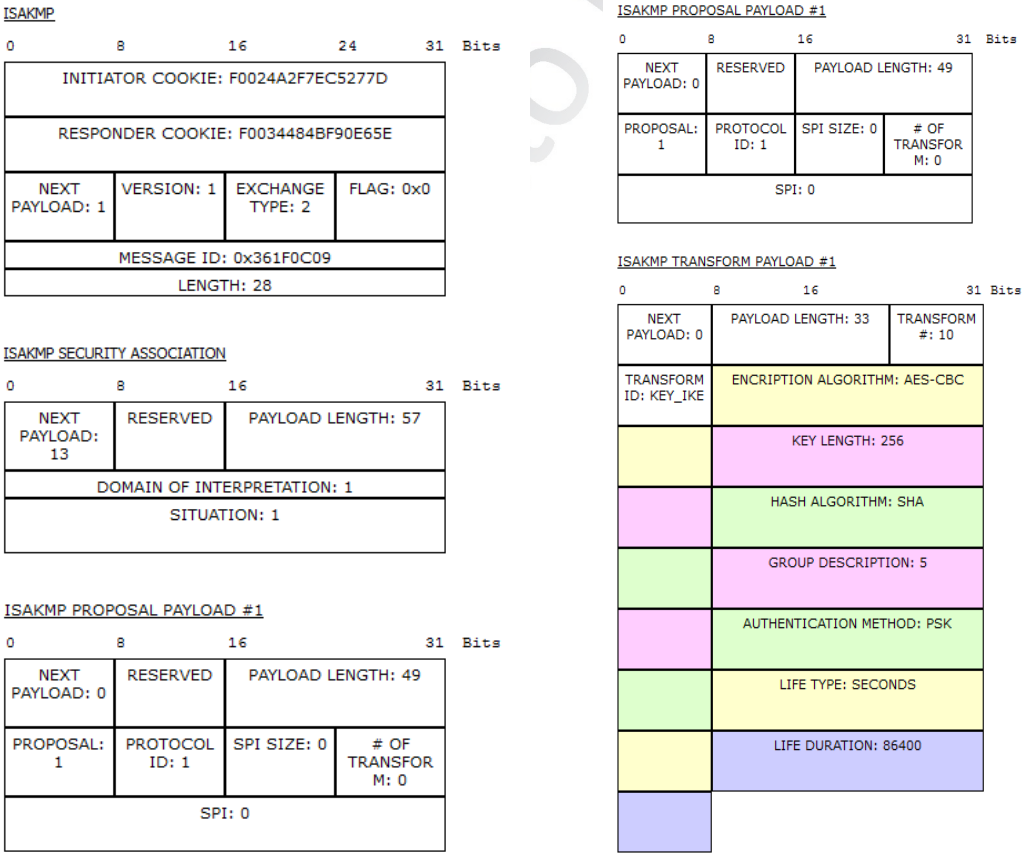
Προσομοίωση της διαδικασίας ενεργοποίησης της VPN σύνδεσης μεταξύ των 2 δρομολογητών

- **Πρώτη Φάση**

  Σε πρώτη φάση οι 2 δρομολογητές ανταλλάσουν ISAKMP μηνύματα, για την ανταλλαγή κλειδιών και για την εγκαθίδρυση της VPN σύνδεσης μεταξύ τους.

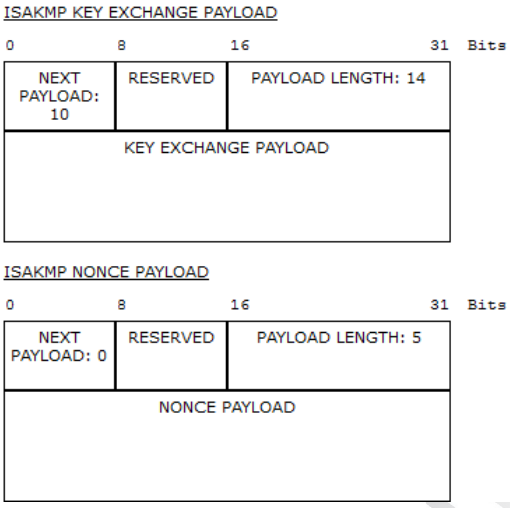


Εικόνα 4.38 Έναρξη εγκατάστασης σύνδεσης μέσω ISAKMP μηνυμάτων



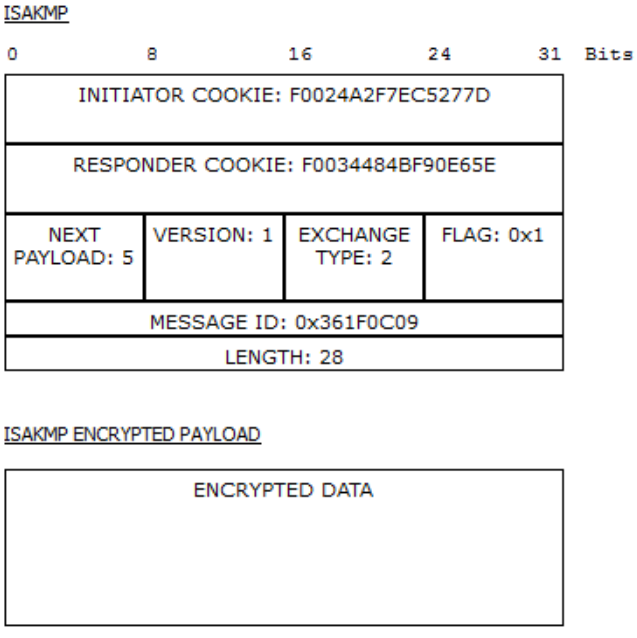
Εικόνα 4.39 Βασικά χαρακτηριστικά του ISAKMP μηνύματος

Ο Δρομολογητής (BORDER ROUTER), παραλαμβάνει το isakmp μήνυμα και ξεκινάει την ανταλλαγή των κλειδιού ISAKMP_KEY.



Εικόνα 4.40 ανταλλαγή κλειδιών ISAKMP

Αφού ο δρομολογητής (BORDER ROUTER), παραλάβει ξανά ISAKMP μήνυμα, τότε ξεκινά την αποστολή κρυπτογραφημένης μορφής μηνυμάτων.

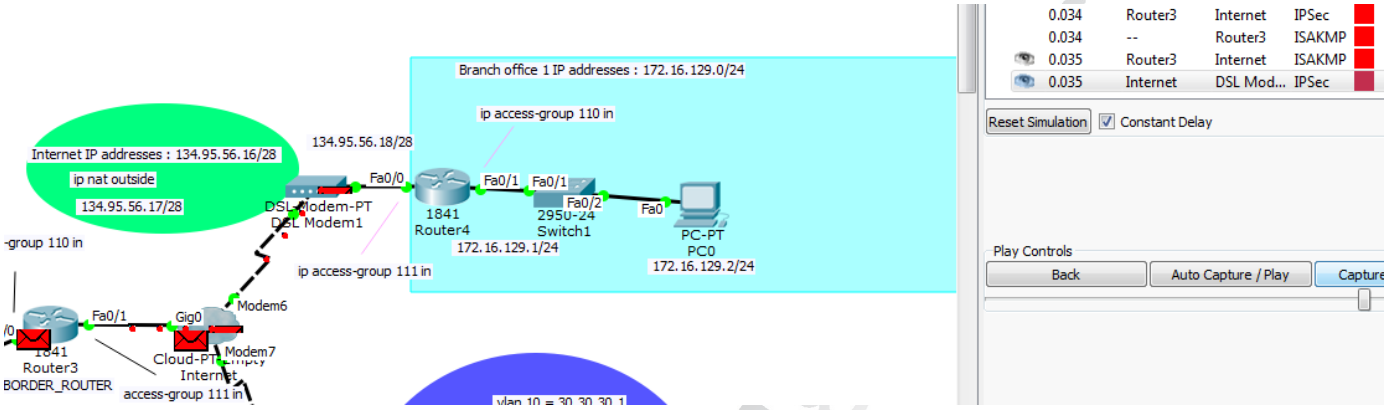


Εικόνα 4.41 κρυπτογραφημένο ISAKMP μήνυμα

Μετά από ανταλλαγές ISAKMP μηνυμάτων μεταξύ των δρομολογητών και την εγκαθίδρυση της VPN σύνδεσης ξεκινά σε δεύτερη φάση και η αποστολή των IPsec μηνυμάτων.

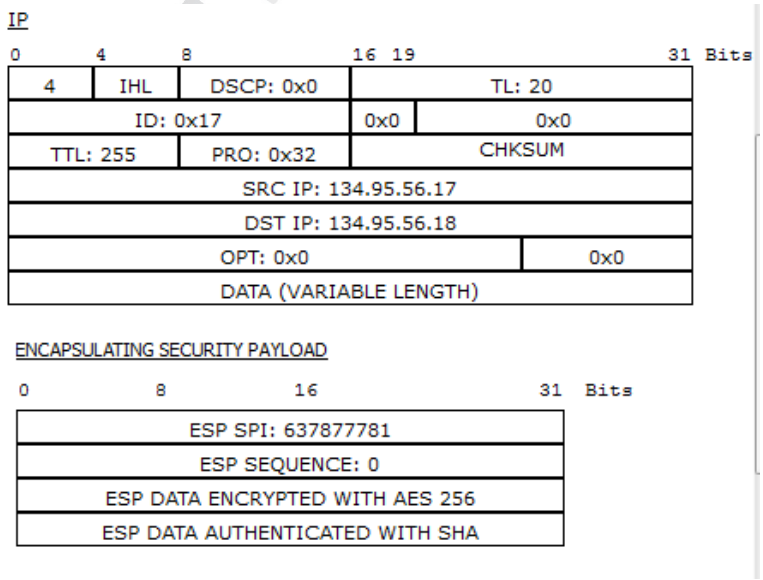
- **Δεύτερη Φάση**

Στην δεύτερη φάση τα δεδομένα που αποστέλλονται σε ipsec μορφή χρησιμοποιούνται για την προστασία των δεδομένων.



Εικόνα 4.42 ανταλλαγή IPSEC μηνυμάτων

Μετά την εγκαθίδρυση της VPN σύνδεσης των δρομολογητών, τα δεδομένα που μεταφέρονται από τον ένα δρομολογητή στον άλλον κρυπτογραφούνται σε IPsec μορφή και αποκρυπτογραφούνται πριν φτάσουν στον παραλήπτη.

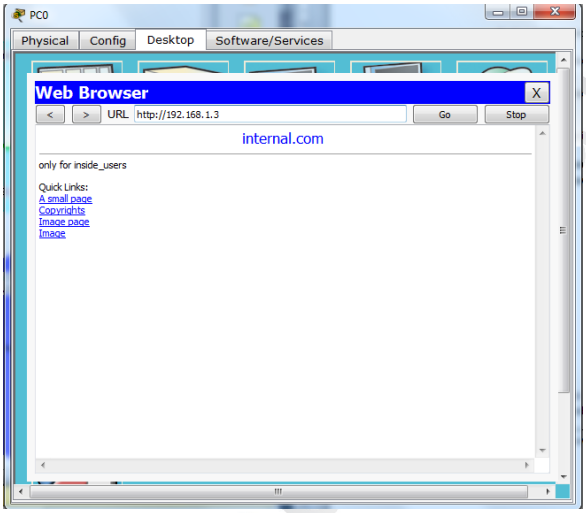


Εικόνα 4.43 κρυπτογράφηση PING μηνύματος σε IPsec μορφή

Στην συνέχεια ο άλλος δρομολογητής αφού παραλάβει το κρυπτογραφημένο μήνυμα και πιστοποιήσει ότι προέρχεται από τον προηγούμενο παραλήπτη και δεν υπέστη τροποποιήσεις κατά την μεταφορά του, το αποκρυπτογραφεί και το στέλνει στον παραλήπτη του.

Η ίδια διαδικασία πραγματοποιείται και σε αντίθετη φορά.

- **Επιβεβαίωση της επικοινωνίας του υποδικτύου 192.168.0.0/29 με το υποδίκτυο 172.16.129.0/24 με την χρήση ping μηνυμάτων.**



Εικόνα 4.44 επικοινωνία με tcp μυνήματατα μεταξύ του χρήστη 172.16.129.2/24 και του web-dns_server 192.168.1.3/29

- **Επιβεβαίωση κρυπτογράφησης μηνυμάτων**

Για να μπορέσουμε να επιβεβαιώσουμε ότι η VPN σύνδεση έχει επιτευχθεί, πληκτρολογούμε στον δρομολογητή την εξής εντολή.

```
Router#show crypto ipsec sa

interface: FastEthernet0/1
Crypto map tag: vpn, local addr 134.95.56.17

protected vrf: (none)
local ident (addr/mask/prot/port): (192.168.2.0/255.255.255.248/0/0)
remote ident (addr/mask/prot/port): (172.16.129.0/255.255.255.0/0/0)
current_peer 134.95.56.18 port 500

PERMIT, flags={origin_is_acl,}

#pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 0

#pkts decaps: 3, #pkts decrypt: 3, #pkts verify: 0
```

#pkts compressed: 0, #pkts decompressed: 0

#pkts not compressed: 0, #pkts compr. failed: 0

#pkts not decompressed: 0, #pkts decompress failed: 0

#send errors 1, #recv errors 0

local crypto endpt.: 134.95.56.17, remote crypto endpt.:134.95.56.18

path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/1

current outbound spi: 0x26053E15(637877781)

inbound esp sas:

spi: 0x7D254A37(2099595831)

transform: esp-aes 256 esp-sha-hmac ,

in use settings ={Tunnel, }
conn id: 2001, flow_id: FPGA:1, crypto map: vpn
sa timing: remaining key lifetime (k/sec): (4525504/3425)
IV size: 16 bytes
replay detection support: N
Status: ACTIVE

inbound ah sas:

inbound pcp sas:

outbound esp sas:
spi: 0x26053E15(637877781)
transform: esp-aes 256 esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 2002, flow_id: FPGA:1, crypto map: vpn
sa timing: remaining key lifetime (k/sec): (4525504/3425)
IV size: 16 bytes
replay detection support: N
Status: ACTIVE

outbound ah sas:

outbound pcp sas:

4.6.8 Εξωτερικός δρομολογητής BRANCH OFFICE 1 (Router4)

Ο δρομολογητής αυτός, εκτός από την access-list 101 η οποία χρησιμοποιεί τους κανόνες της για την ανταλλαγή δεδομένων μέσω της VPN σύνδεσης, χρησιμοποιεί και την λίστα πρόσβασης 111, η οποία εφαρμόζετε στην εξωτερική διασύνδεση του δρομολογητή.

- επιτρέπει στο υποδίκτυο 192.168.0.0 να έχει πλήρη πρόσβαση στο εσωτερικό του δρομολογητή
  access-list 111 permit ip 192.168.0.0 0.0.0.63 172.16.129.0 0.0.0.255
- επιτρέπει στην μετάδοση tcp μηνυμάτων που προέρχονται αποκλειστικά από την διεύθυνση 192.168.2.4 με κατεύθυνση την διεύθυνση 172.16.129.2
  access-list 111 permit tcp host 192.168.2.4 host 172.16.129.2
- επίσης για την αποδοχή των isakmp και των ipsec μηνυμάτων, από την στιγμή που εφαρμόσαμε λίστα πρόσβασης στην διασύνδεση θα πρέπει να εφαρμόσουμε τους εξής κανόνες
  access-list 111 permit udp host 134.95.56.17 host 134.95.56.18
  access-list 111 permit esp host 134.95.56.17 host 134.95.56.18

Από την άλλη πλευρά έχουμε και στην λίστα πρόσβασης 110 η οποία εφαρμόζετε στην εσωτερική διασύνδεση και εκτός του ότι επιτρέπει την επικοινωνία με το υποδίκτυο 192.168.0.0 επιτρέπει και την αποστολή tcp πακέτων με προορισμό την διεύθυνση 192.168.2.4 και την θύρα 80.

```
access-list 110 permit tcp host 172.16.129.2 host 192.168.2.4 eq www
access-list 110 permit ip 172.16.129.0 0.0.0.255 192.168.0.0 0.0.0.63
```

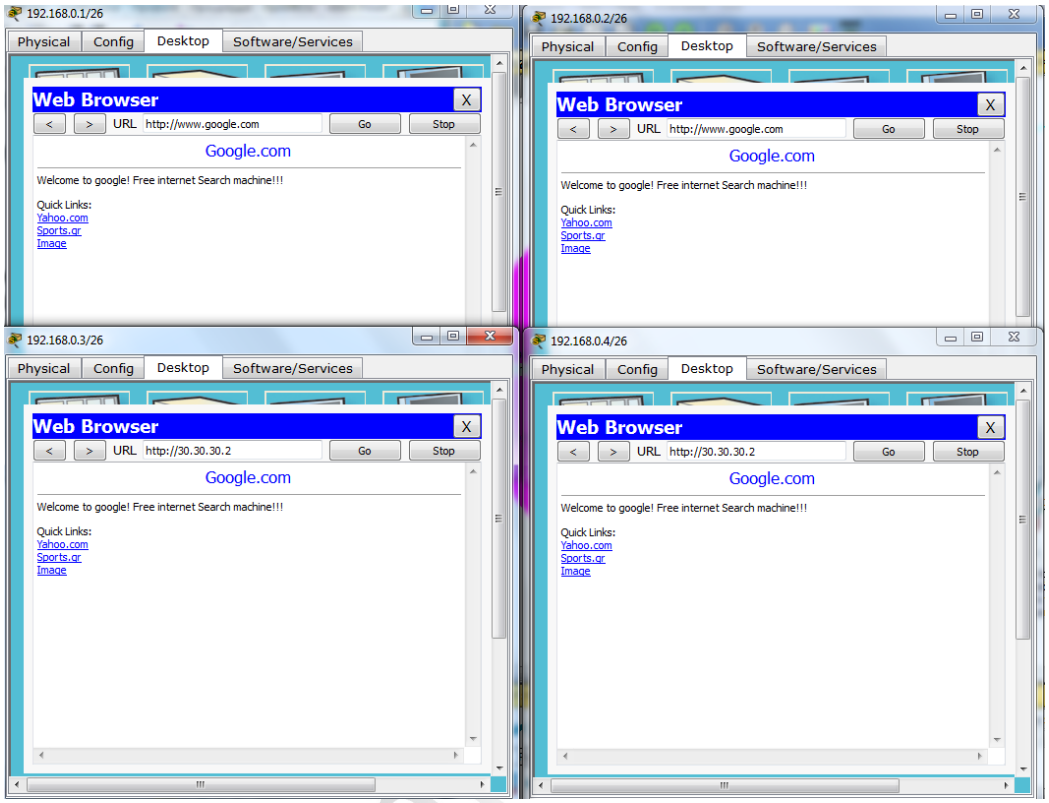
- **Configuration file του εξωτερικού δρομολογητή (Router4)**

```
Router#show run
Building configuration...

Current configuration : 1658 bytes
!
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Router
!
ip cef
no ipv6 cef
!
!
!
!
crypto isakmp policy 10
encr aes 256
authentication pre-share
group 5
!
crypto isakmp key ISAKMP_KEY address 134.95.56.17
!
crypto ipsec transform-set firstset esp-aes 256 esp-sha-hmac
!
crypto map vpn 10 ipsec-isakmp
set peer 134.95.56.17
set pfs group5
set transform-set firstset
match address 101
!
spanning-tree mode pvst
!
interface FastEthernet0/0
ip address 134.95.56.18 255.255.255.240
ip access-group 111 in
duplex auto
speed auto
ipv6 ospf cost 1
crypto map vpn
!
interface FastEthernet0/1
ip address 172.16.129.1 255.255.255.0
ip access-group 110 in
```

```
duplex auto
speed auto
!
interface Vlan1
no ip address
shutdown
!
ip classless
ip route 192.168.0.0 255.255.255.192 134.95.56.17
ip route 192.168.3.0 255.255.255.252 134.95.56.17
ip route 192.168.2.0 255.255.255.248 134.95.56.17
!
ip flow-export version 9
!
!
access-list 101 permit ip 192.168.0.0 0.0.0.63 172.16.129.0 0.0.0.255
access-list 101 permit ip 172.16.129.0 0.0.0.255 192.168.0.0 0.0.0.63
access-list 110 permit tcp host 172.16.129.2 host 192.168.2.4 eq www
access-list 110 permit ip 172.16.129.0 0.0.0.255 192.168.0.0 0.0.0.63
access-list 111 permit ip 192.168.0.0 0.0.0.63 172.16.129.0 0.0.0.255
access-list 111 permit tcp host 192.168.2.4 host 172.16.129.2
access-list 111 permit udp host 134.95.56.17 host 134.95.56.18
access-list 111 permit esp host 134.95.56.17 host 134.95.56.18
!
!
!
!
!
line con 0
!
line aux 0
!
line vty 0 4
login
!
!
!
end
```

4.6.9 Πρόσβαση όλων των χρηστών στην ιστοσελίδα εξωτερικού δικτύου με διεύθυνση 30.30.30.2/24 (www.google.com)



Εικόνα 4.45 Πρόσβαση όλων των χρηστών στην ιστοσελίδα εξωτερικού δικτύου με διεύθυνση 30.30.30.2/24 (www.google.com)

4.6.10 Πρόσβαση του χρήστη 172.16.129.2/28 στην ιστοσελίδα εσωτερικού δικτύου με διεύθυνση 192.168.1.3/29 (www.internal.com)

Για να μπορεί ο συγκεκριμένος χρήστης να έχει πρόσβαση στην εσωτερική ιστοσελίδα του δικτύου, θα πρέπει να εφαρμοσθούν κάποιες ρυθμίσεις τόσο από την πλευρά του δρομολογητή του, όσο και από τις συσκευές (FW-1, INSIDE ROUTER) που ανήκουν στο εσωτερικό δίκτυο και είναι οι εξής.

Router3:

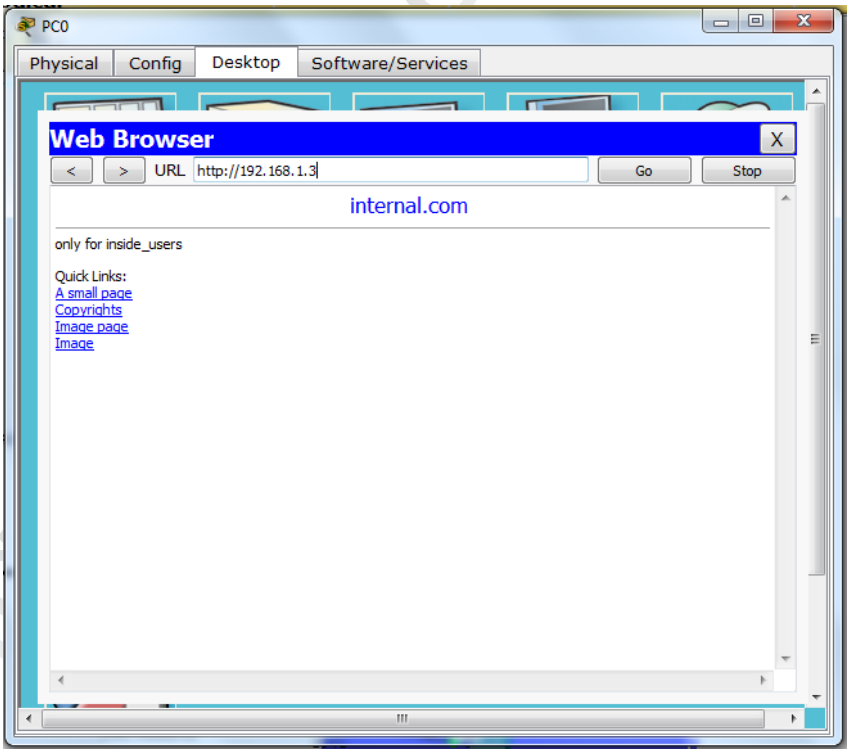
ip route 192.168.1.0 255.255.255.252 134.95.56.17

BORDER ROUTER:

ip route 30.30.30.0 255.255.255.0 134.95.56.19

FW-1

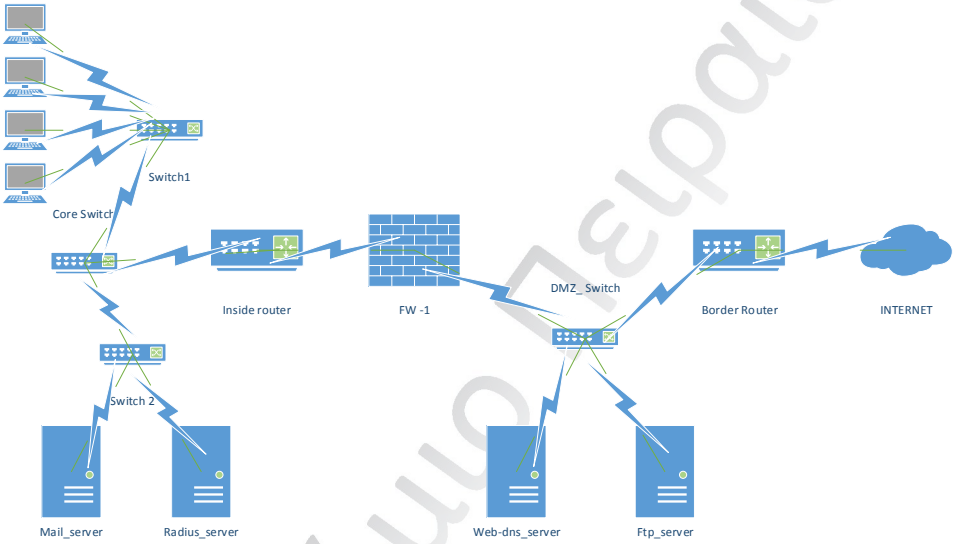
route outside 30.30.30.0 255.255.255.0 192.168.3.2 1
access-list outsidetoinside extended permit tcp host 172.16.129.2 host 192.168.1.3 eq www
access-list insidetooutside extended permit tcp host 192.168.1.3 host 172.16.129.2



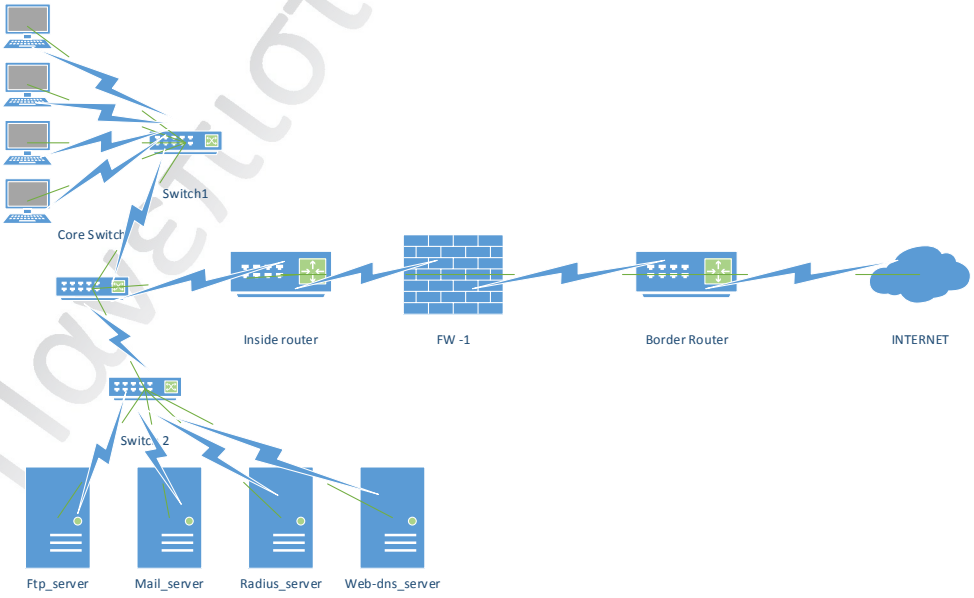
Εικόνα 4.46 Πρόσβαση του χρήστη 172.16.129.2/28 στην ιστοσελίδα εσωτερικού δικτύου με διεύθυνση 192.168.1.3/29 (www.internal.com)

4.7 Συμπεράσματα από τις 2 προηγούμενες εργαστηριακές ασκήσεις.

Στην πρώτη εργαστηριακή άσκηση αναφέραμε την τεχνική προστασίας δικτύου με την χρήση ενός τείχους προστασίας. Η συγκεκριμένη τεχνική αποτελεί την πιο σύγχρονη τεχνική με ένα Firewall, για τον λόγο ότι όλη η κίνηση των δεδομένων που κατευθύνετε προς το εσωτερικό δίκτυο της εταιρείας και κατά συνέπεια και προς τους Server's του δικτύου, θα ελέγχετε και θα φιλτράρετε από τον Firewall. Αυτό αποτελεί ένα πλεονέκτημα σε σχέση με μία προγενέστερη τεχνική που χρησιμοποιούταν, όπου στην ουσία βρισκόταν εκτεθειμένη η DMZ ζώνη του δικτύου που περιείχε τους Public Server's, η οποίοι προστατευόταν μόνο με ένα δρομολογητή με λίστες πρόσβασης.



Εικόνα 4.47 Προγενέστερη τεχνική με την χρησιμοποίηση ενός Firewall



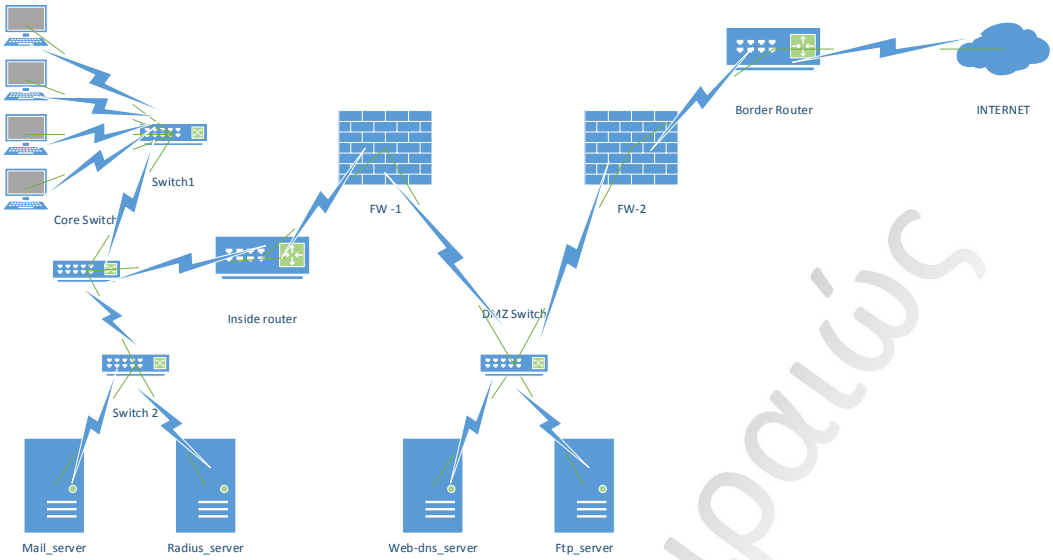
Εικόνα 4.48 Μεταγενέστερη τεχνική με την χρησιμοποίηση ενός Firewall

Παρόλα αυτά όμως ορισμένοι από τους server's του εσωτερικού δικτύου, που θα πρέπει να είναι προσβάσιμη από χρήστες που ανήκουν στο εξωτερικό δίκτυο θα δημιουργήσουν κενά ασφαλείας στις λίστες πρόσβασης που θα εφαρμοστούν στις διασυνδέσεις του τείχους προστασίας, με αποτέλεσμα να δημιουργηθεί ο κίνδυνος παραβίασης του από επιτιθεμένους οι οποίοι μέσω των κοινόχρηστών server θα μπορούν να έχουν πρόσβαση σε ολόκληρο το δίκτυο. Ο κίνδυνος αυτός μπορεί να αποτραπεί περιορίζοντας την κίνηση των δεδομένων που προέρχονται από τους server's αλλά δεν αρκεί για την πλήρη προστασία του Δικτύου.

Στην δεύτερη εργαστηριακή άσκηση, παρατηρούμε ότι η τεχνική που εφαρμόστηκε με 2 τείχη προστασίας, αποτελεί μία πιο ασφαλή μέθοδος στη ασφάλεια του δικτύου για τους εξής λόγους:

- Έχουμε διαχωρισμό τον server's η οποίοι θεωρούνται εμπιστοσύνης για το εσωτερικό δίκτυο (Trusted Server's) και δεν είναι προσβάσιμη σε καμία περίπτωση από χρήστες που ανήκουν στο εξωτερικό δίκτυο που θεωρούνται αγνώστου ταυτότητας.
- Οι server's οι οποίοι είναι κοινόχρηστοι (Untrusted Server's) θα μπορούν να έχουν πρόσβαση με τους εξωτερικούς χρήστες, αλλά η κυκλοφορία των δεδομένων τους θα ελέγχετε από έναν Firewall που θα είναι υπεύθυνος για την κίνηση των δεδομένων από την ζώνη DMZ προς τους εξωτερικούς χρήστες και το αντίθετο.
- Συγκεκριμένα παρατηρούμε ότι ο εσωτερικός Firewall (FW-1), παρουσιάζει πιο περιορισμένες λίστες πρόσβασης σε σχέση με τον εξωτερικό Firewall (FW-2), όπου οι λίστες πρόσβασης του θεωρούνται πιο ελαστικές λόγω των κοινόχρηστών server.
- Μία λύση που προτείνετε σχετικά με την χρήση 2 Firewall, είναι η δυνατότητα να μπορούμε να χρησιμοποιούμε τείχη προστασίας που προέρχονται από διαφορετικούς κατασκευαστές. Με αυτό τον τρόπο η μία συσκευή θα μπορεί να καλύπτει τα μειονεκτήματα ως προς τα χαρακτηριστικά ασφάλειας της άλλης. Αυτή τεχνική στην στρατηγική ασφάλειας είναι γνωστή ως «defense in depth». Στην εργαστηριακή άσκηση που έχουμε εφαρμόσει αυτή η τεχνική δεν μπορεί να αξιοποιηθεί λόγω περιορισμένων συσκευών τύπου Firewall.

Ένα ακόμα πλεονέκτημα που μπορούμε να αναφέρουμε είναι ότι με την χρήση 2 Firewall έχουμε μία πιο ομαλή κατανομή της συνολικής κυκλοφορίας των δεδομένων με αποτέλεσμα ο εξωτερικός firewall να ασχολείται αποκλειστικά και μόνο με τον έλεγχο των δεδομένων που αφορούν τους κοινόχρηστους server's ενώ ο εσωτερικός Firewall να ασχολείται μόνο με τον έλεγχο του εσωτερικού δικτύου.



Εικόνα 4.49 Δίκτυο με τεχνική προστασίας δύο Firewall

Ένα παράδειγμα απειλής κατά της ασφάλειας που μπορεί να παρουσιαστεί είναι η περίπτωση ενός επιτιθέμενου που μπορεί να αποκτήσει πρόσβαση στον web-server του δικτύου και μέσω αυτού, να προσπαθήσει να εισχωρήσει στο εσωτερικό του δικτύου.

Μία από τις λύσεις που έχει προταθεί για αυτή την περίπτωση είναι να περιορίσουμε της δυνατότητες πρόσβασης που μπορεί να έχει ο web-server ή ο οποιοσδήποτε public server προς το εσωτερικό δίκτυο.

5 Βιβλιογραφία

1. Andrew S. Tanenbaum,“Computer Networks (5th Edition)”, Prentice Hall 2011.
2. Sean Convery,”Network Security Architectures”,Cisco Press 2004.
3. Cisco Systems Inc,”CCNA 1 and 2 Companion Guide, Revised (Cisco Networking Academy Program)”,Cisco Press 2004.
4. SANS Institute,”Internal Lab Security Policy”, SANS Institute 2006.
5. Νικόλαος Ι. Στριλίγκας, “Practice Labs For the CCNA Book1”, Hellenic American Union 2008.
6. Steve McQuery CCNA Αυτοδιδασκαλία: Διασύνδεση Συσκεύων Δικτύου Cisco (ICDN) Δεύτερη Αμερικάνικη έκδοση, ciscopress.com – Κλειδάριθμος 2005.
7. www.ciscolearning.org,“CCNA Security Chapter Four Implementing Firewall Technologies”,cisco Learning Institute 2008.
8. Understanding IPsec, Yusuf Bhaiji
9. Cisco Systems Inc., “IPsec Dead Peer Detection Periodic Message Option”, May 1, 2004.
10. ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΛΑΜΙΑΣ - ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΚΩΝ ΕΦΑΡΜΟΓΩΝ - ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΕΧΝΟΛΟΓΙΑΣ ΥΠΟΛΟΓΙΣΤΩΝ, “ΣΧΕΔΙΑΣΗ ΕΙΚΟΝΙΚΩΝ ΔΙΚΤΥΩΝ”,Κώστας Λιμνιώτης, Ακαδημαϊκό έτος 2005-2006.
11. Cisco Systems, Inc.,”IP Tunneling and VPNs”, Cisco Systems, Inc. 2001.