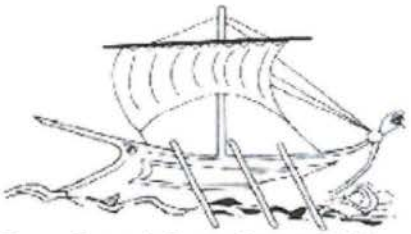


Τεχνολογικό Εκπαιδευτικό Ίδρυμα
Τ.Ε.Ι. ΠΕΙΡΑΙΑ

ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΚΩΝ ΕΦΑΡΜΟΓΩΝ
ΗΛΕΚΤΡΟΝΙΚΑ ΥΠΟΛΟΓΙΣΤΙΚΑ ΣΥΣΤΗΜΑΤΑ
ΕΡΓΑΣΤΗΡΙΟ ΛΕΙΤΟΥΡΓΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΠΤΥΧΙΑΚΉ ΕΡΓΑΣΙΑ ΤΟΥ ΦΟΙΤΗΤΗ
ΠΑΠΑΔΟΠΟΥΛΟΥ ΧΡΗΣΤΟΥ(ΑΜ:34525) ΜΕ ΘΕΜΑ:

Μελέτη σχεδιασμός και υλοποίηση firewall για ασύρματα δίκτυα

Επιβλέποντες Καθηγητές:
Διλιντάς Γεώργιος
Βουτσινάς Στυλίανος

Περιεχόμενα

ΕΥΡΕΤΗΡΙΟ ΕΙΚΟΝΩΝ

ΠΡΟΛΟΓΟΣ

Η συγκεκριμένη πτυχιακή εργασία έχει σαν στόχο να παρουσιάσει πως μπορεί να δημιουργήθει μιο πλατφόρμα προστασίας (firewall) του δικτύου υπολογιστών που διαθέτουμε από ανεπιθύμητες επισκέψεις από/προς το δίκτυο του από/σε επικίνδυνους ή ανεπιθύμητους ιστότοπους ,άλλα δίκτυα υπολογιστών κτλ .Επίσης την εγκατάσταση και διαχείρηση εξοπλισμού και προγραμμάτων εντοπίσμου απειλών στο δίκτυο μας. Τη διαχείριση των δικαιωμάτων, χρήσης και επεξεργασίας ,κάθε χρήστη στο δίκτυο του στις πληροφορίες, τα αρχεία, τις εφαρμογές που διαθέτει το δίκτυο.Το πειραματικό κομμάτι της εργασίας πραγματοποιήθηκε στο χώρο του εργαστηριακού μαθήματος Λειτουργηκών Συστημάτων (O.S.LAB) και συγκεκριμένα στη εγκατάσταση Firewallκαι IDSστο ασύρματο δίκτυο του O.S.LABπροκειμένου να προστατεύσουμε το δικτυο από ανεπιθύμητες ενέργειες ειτε για λογους δεοντολογικούς,προστασίας είτε για λόγους αποφυγής υπερφόρτωσης του δικτύου.

ΚΕΦΑΛΑΙΟ 1

1.1.Τι είναι Firewall

Η ονομασία firewall προήλθε από τους ειδικούς τοίχους, οι οποίοι σχεδιάστηκαν ώστε να περιορίσουν μια φωτιά σε περίπτωση εκδήλωσής της και να μην την αφήσουν να επεκταθεί και στο υπόλοιπο κτήριο. Αργότερα, firewall ονομάστηκαν μεταλλικές πλάκες σε αυτοκίνητα και αεροπλάνα, σκοπός των οποίων ήταν να διαχωρίσουν το χώρο των επιβατών από τη μηχανή.

Εισαγωγικά θα προσπαθήσουμε να εξηγήσουμε την έννοια του firewall, τη χρησιμότητά του και τα βασικά είδη που συναντώνται στους υπολογιστές μας. Με πολύ απλό τρόπο μπορούμε να παρομοιάσουμε τα καθήκοντα του firewall με ένα φύλακα κτιρίου που βρίσκεται στην είσοδο.Το καθήκον του φύλακα είναι το εξής:

- Ελέγχει ποιός μπαίνει και ποιός βγαίνει από το κτήριο βάσει συγκεκριμένων κανόνων που του έχει ορίσει ο υπεύθυνος ασφαλείας.
- Απαγορεύει την είσοδο ή την έξοδο σε συγκεκριμένα άτομα βάση των κανόνων .
- Αν δεν γνωρίζει για τα δικαιώματα εισόδου ή εξόδου για κάποιο συγκεκριμένο άτομο, συμβουλεύεται τους ανωτέρους του για το πώς να πράξει.

Το firewall λοιπόν μπορεί να είναι ένα πρόγραμμα(softwarefirewall), μία συσκευή ή ένα σύνολο συσκευών (hardwarefirewall) που κάνει αυτή ακριβώς τη δουλειά για τον υπολογιστή μας.Ελέγχει την επικοινωνία, τη λήψη ή την αποστολή δεδομένων συγκεκριμένων προγραμμάτων, μέσω δικτύου.Κάποια προγράμματα έχουν ελεύθερη πρόσβαση στο να στείλουν και να λάβουν δεδομένα στο δίκτυο (όπως ο browser, το πρόγραμμα του e-mail ή η υπηρεσία για τα updates του λειτουργικού συστήματος).Άλλα προγράμματα, όπως αναγνωρισμένα mallware, έχουν απαγορευμένη την πρόσβαση - για τα προγράμματα αυτά, ουσιαστικά είναι σαν να μην υπάρχει δίκτυο.Τέλος, επειδή κανένα firewall δεν έχει κανόνες για τα εκατομμύρια προγράμματα του κυκλοφορούν στην αγορά, τα περισσότερα "οικιακά" firewall ρωτούν το χρήστη όταν κάποιο νέο, άγνωστο πρόγραμμα προσπαθεί για πρώτη φορά να έχει πρόσβαση στο δίκτυο. Στην ερώτηση αυτή σχεδόν πάντα υπάρχει και η επιλογή το firewall να θυμάται τον κανόνα, και να μην ξαναρωτήσει.

1.1.1. Τρόποι αξιοποίησης κάθε είδους σήμερα

Στη συντριπτική πλειοψηφία των περιπτώσεων, τα software firewall απευθύνονται σε οικιακούς χρήστες και τα harware firewall απευθύνονται σε επιχειρήσεις ή μεγάλους οργανισμούς με δίκτυα υπολογιστών σχολεία, πανεπιστήμια, δημόσιες υπηρεσίες κλπ).

Χρειάζεται να ξέρουμε ποιά προγράμματα του υπολογιστή μας επικοινωνούν με το δίκτυο αν θέλουμε να νιώθουμε ασφαλείς.Υπάρχουν πολλά είδη προγράμματων που κανείς δεν θέλει να βρίσκονται στον υπολογιστή του αλλά αν υπάρχουν πρέπει να το ξέρεις . Π.χ. τα keyloggers τα οποία, αν έχουν προσβάλλει το σύστημά μας, καταγράφουν όλα όσα γράφουμε στο πληκτρολόγιο (οπως passwords και αριθμούς πιστωτικών

καρτών) και τα στέλνουν αυτόματα σε κάποιον server ή προγράμματα remote administration που επιτρέπουν σε κάποιον να βλέπει όλα όσα βλέπουμε στην οθόνη μας και επιπλέον να πάρει ολόκληρο τον έλεγχο του υπολογιστή μας, ακόμα και του πληκτρολογίου, του ποντικιού .

Έχει κάνει την εμφάνισή του τουλάχιστον ένας ιός ο οποίος προσβάλλει μηχανήματα που δεν έχουν firewall, μόνο και μόνο επειδή τα βρίσκει απροστάτευτα.Οπότε το να μην διαθέτει Firewall ο υπολογιστή μας μπορεί να παρομοιαστεί είναι σαν να κατοικούμε σε ισόγειο διαμέρισμα σε πόλη εκατομμυρίων κατοίκων με και να αφήνουμε πάντα τα παράθυρα ορθάνοιχτα. Μπορεί να μη συμβεί και τίποτα , αν και παραείναι αισιόδοξη σαν σκέψη. Βέβαια, όπως και στην περίπτωση των παραθύρων, πάντα υπάρχει η πιθανότητα κάποιο malware να απενεργοποιήσει ή να παρακάμψει το firewall μας.

Οπότε, έτσι και αλλιώςπρέπει να είμαστε προσεκτικοί στο τι είδους προγράμματα κατεβάζουμε και τρέχουμε στον υπολογιστή μας - ιδιαίτερα αν επισκεπτόμαστε ύποπτα sites. Αν θέλουμε ένα firewall που να είναι πιο ευέλικτο και να έχει περισσότερες δυνατότητες, θα πρέπει να επιλέξουμε κάποιο firewall τρίτου κατασκευαστή.

Επειδή δυστυχώς τα antivirus είναι χρήσιμα μόνο για τα malware που είναι αναγνωρισμένα ως απειλή. Αφού αν ένας ιός που υποκλέπτει λ.χ. τα στοιχεία πιστωτικών καρτών είναι πολύ καινούριος, και ο τρόπος που είναι κατασκευασμένος δεν θυμίζει κάποιον ήδη γνωστό ιό, το Antivirus δεν θα τον αναγνωρίσει σαν ιό. Μέχρι το Antivirus να κατεβάσει τις νεότερες ενημερώσεις ασφαλείας από την εταιρεία του, θα αφήσει τον ιό να δρα ανενόχλητος στο σύστημά μας , με ότι αυτό συνεπάγεται.

Το firewall, από την αλλή, είναι εξ' ορισμού καχύποπτο. Αν οποιοδήποτε νέο πρόγραμμα προσπαθεί να αποκτήσει πρόσβαση στο internet - στο παράδειγμά μας, αν ο ιός προσπαθήσει να στείλει τα στοιχεία της πιστωτικής μας κάρτας σε κάποιον εξωτερικό server - το firewall αμέσως θα ρωτήσει αν θέλουμε να αφήσουμε το συγκεκριμένο πρόγραμμα να επικοινωνήσει μέσω δικτύου. Απαντώντας "Όχι" στην ερώτηση αυτή, τα στοιχεία της κάρτας μας παραμένουν ασφαλή.Όμως αν το σύστημά μας προσβληθεί από έναν ιό που καταστρέφει τα αρχεία του word, το firewall δεν πρόκειται να τον εντοπίσει ή να τον σταματήσει, καθώς δεν κάνει κάποια απόπειρα να επικοινωνήσει με το δίκτυο.

Το antivirus λοιπόν και το firewall είναι δύο εντελώς διαφορετικά προϊόντα που εξυπηρετούν διαφορετικούς σκοπούς.Όσον αφορά το firewall, θα πρέπει να είστε πολύ προσεκτικοί όταν σας ρωτάει να δώσετε την άδεια για κάποιο πρόγραμμα ώστε να έχει πρόσβαση στο δίκτυο.

Αν πατήσουμε "Ναι" ενώ δεν πρέπει, θα επιτρέψουμε σε κάποιο κακόβουλο πρόγραμμα να επικοινωνήσει με το servertου οπότε αχρηστεύουμε το firewall.Αντίθετα, αν πατήσουμε "Όχι" σε μια ερώτηση για ένα νόμιμο πρόγραμμα, θα το μπλοκάρουμε από το δίκτυο και δεν θα μπορέσει να λειτουργήσει όπως πρέπει. Αν π.χ. είναι το πρόγραμμα update για τους drivers του εκτυπωτή μας, το πρόγραμμα δεν θα μπορεί να επικοινωνήσει με το διαδίκτυο και να κατεβάσει την τελευταία έκδοση.Ουσιαστικά, όλη η ευθύνη για τη λειτουργία του firewall, σε οικιακό περιβάλλον, πέφτει λίγο-πολύ στο χρήστη.Τα περισσότερα firewall, όταν ζητούν την άδεια για ένα πρόγραμμα, έχουν κάποια επιλογή details η οποία δείχνει και το path του αρχείου του προγράμματος.

Π.χ ρωταεί το firewall για το αρχείο C:\program files\Hewlett Packard\HPupdate.exe, και πρόσφατα εχουμε εγκαταστήσει τους drivers για μία συσκευή της Hewlett Packard στο σύστημά μας, τότε κατά 90% το αρχείο αυτό είναι ασφαλές να έχει πρόσβαση στο internet.

Αντίθετα, αν χωρίς να κάνουμε τίποτα, εμφανιστεί μια οθόνη που λέει πως το αρχείο C:\Windows\Temp\13sdfasdnbv.js θέλει να έχει πρόσβαση στο δίκτυο, λογικά πρόκειται για κάτι κακόβουλο, οπότε του απαγορεύουμε την πρόσβαση και να φροντίζουμε να το διαγράψουμε και από το σύστημά μας.

Τέλος μπορεί να ανοίξουμε ένα αρχείο που πιστεύουμε πως είναι αρχείο εικόνας ή τραγούδι mp3 και το firewall να εντοπίσει πως το πρόγραμμα ζητάει πρόσβαση στο διαδίκτυο. Σε αυτή την περίπτωση, το αρχείο εικόνας ή το τραγούδι που επιχειρήσαμε να τρέξουμε είναι καμουφλαρισμένο εκτελέσιμο αρχείο, με εμφανώς κακόβουλο κώδικα, οπότε πάλι απαγορέουμε την πρόσβαση και να το σβήνουμε το συντομότερο από το σύστημα.

Καλώς ή κακώς, στην περίπτωση των οικιακών firewall η ασφάλεια σε μεγάλο βαθμό εξαρτάται από την κρίση του χρήστη. Οι χρήστες που πατάνε άκριτα "ναι" ή "όχι" σε ό,τι τους εμφανίσει το firewall είναι σαν τα μικρά παιδιά, που μπορεί να ανοίξουν την πόρτα στον οποιονδήποτε ή, αντίθετα, να μην ανοίξουν την πόρτα στη μητέρα τους που ξέχασε τα κλειδιά της.

1.1.2 Είδη firewall τα υπέρ και τα κατά του κάθε είδους

Τα firewall χωρίζονται σε software και hardware.

1.1.2.1 Software firewall

Είναι προγράμματα που εγκαθίστανται στον υπολογιστή, με τον ίδιο τρόπο που εγκαθιστούμε ένα antivirus για την προστασία από ιούς.

Πλεονεκτήματα

- Είναι οικονομικότερα από τα harware firewall
- Ρυθμίζονται και χρησιμοποιούνται ευκολότερα
- Ενα software firewall μπορούμε να το εγκαταστήσομε σε laptop που χρησιμοποιείται οπουδήποτε.

Μειονεκτήματα

- Χρειάζεται να έχουμε άδεια χρήσης για κάθε τερματικό που χρησιμοποιούμε .
- Καταναλώνουν ισχύ από τον επεξεργαστή και μνήμη του υπολογιστή μας.
- Λιγότερες δυνατότητες ρυθμίσεων σε σχέσημε τα harware firewall.

1.1.2.2Harware firewall

Είναι συσκευές η σύνολο συσκευών ,που παρεμβάλλονται ανάμεσα στον υπολογιστή ή το δίκτυο και το internet. Κάποιοι καλύτερης ποιότητας δρομολογητής έχουν ενσωματωμένο ένα hardware firewall.

Πλεονεκτήματα

- Προστατεύει ένα ολόκληρο δίκτυο υπολογιστών και όχι ένα τερματικό.
- Διαθέτουν δικό τους επεξεργαστή και μνήμη, και δεν επιβαρύνουν καθόλου τον υπολογιστή
- Τα malware δεν μπορουν να το απενεργοποιήσουν, όπως με ενα software firewall

- Προστατεύουν το σύστημα σε όλες τις κατάστασειςτου λειτουργικού συστήματος - ακόμα κι αν μόλις εγκατασταθάθηκε.
- Ίπροηγμένα hardwarefirewall περιλαμβάνουν και προστασία antivirus-antispyware

Μειονεκτήματα

- Κοστίζουν σαφώς ακριβότερα απ' ότι μία άδεια για ένα software firewall.
- Η ρύθμιση τους απαιτεί πιο εξειδικευμένους χρήστες.
- Επειδή είναι συσκευή χρειάζεται να εγκατασταθεί σε συγκεκριμένο σημείο και να έχει πρόσβαση σε ρεύμα και στο δίκτυο.
- Αν μπλοκάρει καποιο πρόγραμμα, δεν εμφανίζεται κάποιο μήνυμα στον υπολογιστή του χρήστη αυτομάτως; αλλά χρειάζεταινα μπεί ο ίδιος στο διαχειριστικό σύστημα του firewall και να επιτρέψει τη λειτουργία του.
- Αν αποτύχει και προστατεύει ολόκληρο δίκτυο υπολογιστών, όλοι οι υπολογιστές μένουν απροστάτευτοι.
- Δεν μπορούμε να το εγκαταστήσουμε ανέξοδα όπως με κάποια δωρεάν έκδοση ενός software.

1.2.Τι είναι το IDS;

Όταν το δίκτυο μια εταιρείας ή ενός οργάνισμού συνδέεται στο διαδίκτυο εκτίθεται σε μεγάλο βαθμόσε κινδύνους. Οι οποίοι προέρχονται από σφάλματα (bugs) και «τρύπες» της ασφάλειάς του υλικού και του λογισμικού που χρησιμοποιείται στο δίκτυο τους, τα σφάλματα αυτά αυξάνονται αναλογικά με το μέγεθος του δικτύου. Οπότε οι μηχανισμοί ασφάλειας που εγκαθίστανται είναι επιτακτική ανάγκη να απαγορέυουν οποιαδήποτε μη εξουσιοδοτημένη πρόσβαση στους πόρους του συστήματος ή στα δεδομένα του. Βεβαια είναι αναμενόμενο ειναι ότι απόλυτη ασφάλεια δεν μπορεί να υπάρξει. Οπότε το βέλτιστο δυνατό είναι να διαγνωσθούν οι όποιες εισβολές ή απόπειρες για κάτι τέτοιο το συντομότερο δυνατόν, για να ελαχιστοποιηθούν οι συνέπειες τους .

Αυτή τη δουλεία αναλαμβάνουν τα Συστήματα Ανίχνευσης Εισβολής (IntrusionDetectionSystems). Τα IDS είναι συστήματα υλικού ή λογισμικού, που παρακολουθούν όσα γίνονται σε ένα δίκτυο ή σύστημα υπολογιστών και τα αναλύει ώστε να εντοπίσει παραβιάσεις ασφάλειας. Η ολο και αυξανόμενη εμφάνιση δικτυακών επιθέσων καθιστά πλέον τα συστήματα ανίχνευσης εισβολής απαραίτητα στις υποδομές ασφάλειας σε ολο και περισσότερους οργανισμούς. Τα IDS αναλαμβάνουν γνωστοποιούν την εισβολή κάποιου στο σύστημα ή ακόμη και για την απόπειρα ειβολής φροντίζοντας ταυτόχρονα για την κατάλληλη αντιμετώπισή του. Η ολο και πιο διευρυμένη χρήση διαδικτυακών συναλλαγών τα τελευταία χρόνια (ηλεκτρονικό εμπόριο κτλ) αυξάνει και την ανάγκη για πληρέστερη προστασία από εισβολές που πραγματοποιούνται σε δίκτυα οργανισμών και επειδή εμφανίζονται νέου τύπου επιθέσεις που τα υπόλοιπα συστήματα δεν ήταν δυνατό να αντιμετωπίσουν τα IDSγινονται ολο και πιο απαραίτητα μέρα με τη μέρα

1.2.1 Κατηγορίες Συστημάτων Ανίχνευσης Εισβολής (I.D.S)

Μπορούμε να ξεχωρίσουμε τα IDSπροιόντα σε τέσσερις κατηγορίες.

1.2.1.1 HostIDS

Τα HIDSδρουν σε κάθε τερματικό του δικτύου μας , εξετάζοντας συνεχώς τα αρχεία καταγραφής logfiles) που διατηρεί το κάθε ένα τερματικό.Τα κρίσιμα αρχεία του συστήματος, τις διεργασίες που κτελούνται ,τηχρηση CPU ,του σκληρού δίσκου κ.α για ύποπτη συμπεριφορά ,μη εξουσιοδοτημένες λλαγές κτλ. Αν παρατηρηθεί κατι απρόσμενο ή ανεπιθύμητο ενημερώνει τους αρμόδιους με προειδοποιήση η ιήνυμα.Κομμάτι των HIDS είναι τα συστήματα ελέγχου ακεραιότητας (FileIntegrityAssessment) που ροστατεύουν από Trojans, backdoors και ιούς. Τα συστήματα αυτά λειτουργούν κυρίως αφούγίνει κάποια πίθεση οπότε και την ανιχνέυουν και ειδοποιούν για αυτήν. Ορισμένα όμως λειτουργούν προληπτικά ποτρέπουν έτσι την εξέλιξή της επίθεσης με το που ανιχνεύθει κάποια ύποπτη συμπεριφορά.

.2.1.2NetworkIDS

Τα NIDSδρούν πάνω στο επικοινωνιακό μέσο για ένα κομμάτι του δικτύου . Εξετάζουν μεμεγάλη επτομέρεια τα πακέτα που μεταφέρονται από και προς το κομμάτι του δικτύου ώστε οι διενεργούμενες πιθέσεις να εντοπιστούν πριν φτάσουν στο στόχο τους.

Αυτό γίνεται πρώτον με τη ταυτοποίηση των πακέτων με γνωστές υπογραφέςεπιθέσεων. Οι υπογραφές υτές μπορεί να είναι βασισμένες στα περιεχόμενα των πακέτων, στις πόρτες που αυτά απευθύνονται (π.χ. σε ια υπηρεσία με γνωστή αδυναμία στην ασφάλειά της),στο πρωτόκολλο που χρησιμοποιείται (π.χ. παράνομες ή αράλογες επίκεφαλίδες στο TCP/IP πακέτο, χρησιμοποείτα κατά κόρον σεDoS επίθεσεις). Επειδή συνέχεια ίνονται γνωστές νέες επιθέσεις, οι κατασκευαστές ενημερώνουν διαρκώς τις υπογραφές .Τα NIDS έχουν τη υνατότητα όχι απλώς να ειδοποιήσουναν εντοπιστεί κάποια ύποπτη δραστηριότητααλλα να τερματίσουν και ην σύνδεση που χρησιμοποιείται για αυτή.

Η σύγκριση με τις «υπογραφές» των επιθέσεων δεν μπορεί να γίνεται με καθέ πακέτο ξεχωριστά γιατι ις περισσότερες φορές απαιτούνται περισσότερα πακέτα για αυτές. Οπότε κάθε πακέτο πρέπει να ελέγχεται αι σε σχέση με το τι έχει προηγηθεί και με έτσι να γίνεται η σύγκριση με τις καταχωρημένες πογραφέςΥλοποιείται λοιπόν μεγάλος φόρτος εργασίας από τα NIDS οπότε και είναι αναγκαίος ένας πολογιστής στον οποίο θα λειτουργούν αποκλειστικά .

Δευτερη μέθοδος ανίχνευσης επιθέσεων είναι ο εντοπισμός ανώμαλης δραστηριότητας inomalydetection). Σύμφωνα με αυτήν, το NIDS παρακολουθεί την κίνησηκαι την συμπεριφορά των υστημάτων, στο κομμάτι του δικτύου που βρίσκεται στην ευθύνη του και ειδοποιεί για οποιαδήποτε ανόμαλη ραστηριότητα. Το επιτυγχάνει βασισμένο στα δεδομένα που συλλέγει για την χρήση των συστημάτων ,το δος και την ποσότητα των πακέτων που διακινούνται. Φτιάχνει πρότυπα λειτουργίας για το υγκεκριμένοκομμάτι του δικτύου ,αν κάτι παρεκλίνει από τα πρότυπα θεωρεί ότι γίνεται επίθεση.

.2.1.3 Υβριδικά IDS (NNIDS)

Τα NNIDS ειναι υβρίδιο των Hostκαι των NetworkIDS. Λειτουργούν σχεδόν όπως τα NIDS. αρακολουθούν τα πακέτα και τα συγκρίνουν με τις καταχωρημένες υπογραφές επιθέσεων.Αυτό όμως γίνεται οκλειστικά για τα πακέτα από και προς τον συγκεκριμένο κόμβο του δικτύου στον οποίο τρέχει το NNIDS .

Οπότε τα NNIDSκαι απαιτούν πολύ μικρότερους πόρους και καταργούν πολλά προβλήματα των NIDS, όπως την σωστή λειτουργία κάτω από μεγάλη κίνηση πακέτων, σε συστήματα με κρυπτογραφημένες επικοινωνίες .

1.2.1.4 Honey-pots

Ταhoney-potsλειτουργούν βάση της τακτικής της παραπλάνησης. Είναι συστήματα που αφήνονται σκόπιμα εκτεθειμένα έτσι ώστε να προσπαθήσουν να εισβάλουν σε αυτά ,να γίνει γνωστή η πρόθεσή των εισβολέων και να παρθούν τα απαραίτητα μέτρα αντιμετώπισης. Ετσι χωρίς κόστος, αφού τα εν λόγω συστήματα έχουν μόνο άχρηστες πληροφορίες και δεδομένα, οι διαχειριστές του κανονικού δικτύου αποκτούν πολύτιμο χρόνο και γνώσεις για τους τρόπους επίθεσης. Οπότε γίνεται ευκολότερη και η προστασία των πόρων του δικτύου και το να αντιμετωπιστούν ενεργά οι εισβολείς.

1.2.2 ΤοIDS σαν μέρος του συστήματος της ασφάλειας

Το να εγκαταστήσουμε έναIDS και να λειτουργεί σωστά προφανώς είναι ένα κομμάτι της ασφάλειας που χρειάζεται ένα δίκτυο οργανισμού, που για να έχει αποτελέσματα αντάξια των προσδοκιών μας πρέπει να συνεργαστεί αρμονικά με όλα τα υπόλοιπα τμήματα του σύστημα ασφάλειας (Firewall,antiviruskτλ). Η πολιτική ασφάλειας του οργανισμού καθορίζει τα πλαίσια μέσα στα οποία όλα τα μέρη του συστήματος ασφαλείας λειτουργούν και τον τρόπο με τον οποίο θα χειρίζονται τα γεγονότα, συμπεριλαμβανομένων των εισβολών τις οποίες αποτρέπει το IDS.

Οι επιθέσεις έχουν διαφορετικό βαθμό σοβαρότητας και επικινδυνότητας. Οπότε τα IDS πρέπει αναλόγα με το βαθμό επικινδυνότητας των εισβολών να τις αντιμετωπίζουν. Μια εισβολή μπορεί δηλαδή να αντιμετωπιστεί με αποστολή e-mail ή SNMP μηνύματος ενώ μια πολύ επικίνδυνη μετερματισμό της ύποπτης συνόδου) και επαναρρύθμιση του firewall.

Το πόσο μπορεί να ενισχύσει το IDS την ασφάλεια του δικτύου στην ανίχνευση των εισβολών είναι άρικτα συνδεδεμένο με το πόσο άρτια εκπαιδευμένο είναι το προσωπικό που θα χειρίζεται τις προειδοποιήσεις και τους συναγερμούς που προκαλεί.Αν δεν μπορεί ο διαχειριστής ασφαλείας να ανταποκριθεί στις απαιτήσεις, τότε το IDSδυστυχώς αχρηστεύεται.

Επίσης επειδή οι επιθέσεις και οι εισβολές που δέχονται τα δίκτυα δεν σταματάνε μπροστά σε ενα καλά στημένο σύστημα ασφάλειας,ούτε παραμένουν ίδιοι οι τρόποι εισβολής που χρησιμοποιούνται. Η διατήρηση της ασφάλειας είναι επίσης συνδυασμένη με τη συνεχή επικαιροποίηση και εκσυγχρονισμό των μέσων που χρησιμοποιούμε για αυτή.

Ετσιόταν οι κατασκευαστές κάνουν διαθέσιμες καινούριες υπογραφές για τα IDS, διορθωτικά patches για τα λειτουργικά συστήματα και για το λογισμικό, αναβαθμίσεις για τα firewall κ.τ.λ. πρέπει αυτά να ενσωματώνονται άμεσα στις υποδομές. Πρέπει να υπάρχει συνεχής ενημέρωση για νέες τεχνικές επιθέσεων ή για προβλήματα που αφορούν το υπάρχον υλικό ή λογισμικό και να λαμβάνονται μέτρα προστασίας πριν ακόμη βγουν τα διορθωτικά προγράμματα και οι νέες υπογραφές. Επίσης χρειάζεταινα εξετάζεται διαρκώς το σύστημα μας για τρωτά σημεία που επίσης μεταβάλλονται συνέχειακαι έγκαιρα να γίνονται οι κατάλληλες ενέργειες.

1.2.3 Προβλήματα των IDS

Για να μπορέσουμε να έχουμε ένα όσο πιο ολοκληρωμένο σύστημα ασφαλείας είναι επιβεβλημένος ο συνδυασμός IDSαπό όλες τις προαναφερθήσες κατηγορίες που θα λειτουργεί φυσικά μαζί με το απαραίτητο firewall αφού όπως είδαμε κάθε είδοςIDS έχει διαφορετικά χαρακτηριστικά λειτουργίας, τύπους επιθέσεων που ανιχνεύει και συστήματα στα οποία εφαρμόζεται

Ακόμα και στο συνδυασμό τους δεν μπορούμε να πούμε ότι δενυπάρχουν προβλήματα στην λειτουργία ή την αποτελεσματικότητα των Συστημάτων Ανίχνευσης Εισβολής.

Είναι ξεκάθαρο ότι μόνο με την αγορά ή μια απλή εγκατάστασηIDSδεν λύνουμε τα προβλήμα της ασφάλειας του δικτύου. Τα IDS πρέπει να εγκατασταθούν σύμφωνα με τις ανάγκες του κάθε περιβάλλοντος, στο οποίο τοποθετούνται.Δημιουργούνται συχνά προβλήματα είτε γιατί οι ρυθμίσεις τους. δεν ανταποκρίνονται στα χαρακτηριστικά λειτουργίας του περιβάλλοντος εργασίας τους, είτε γιατί αφήνονται με τις εργοστασιακές ρυθμίσεις .Άλλο ένα συνηθισμένολάθος είναι η αμελής ή ελλειπής ενημέρωσή τους με νέες εκδόσεις υπογραφών και patches, που αναμενόμενα μειώνει την αποτελεσματικότητά τους σε βάθος χρόνου.

Υφίστης σημασίας είναι επίσης το θέμα των λανθασμένων συναγερμών Αρκετά IDS στην προσπάθειά τους να αποκλείσουν κάθε πιθανότητα να μην ανιχνεύθεί μια εισβολή, επισημαίνουν σαν εισβολή οποια διεργασία ξεφεύγει έστω και λίγο από τα πρότυπα λειτουργίας. Το αποτέλεσμα να παράγει μεγάλο αριθμό ειδοποιήσεων για απόλυτα νόμιμες ενέργειες που απλώς είναι κάπως διαφορετικές από τα συνηθισμένα. Πάντως το πρόβλημα σιγά-σιγά δείχνει να ξεπερνιέται με τα ποσοστά των λανθασμένων συναγερμών και των μη ανιχνευόμενων επιθέσεων να είναι αρκετά χαμηλά στα συγχρονα IDS.

Επίσης αναφέραμε ότι τα NIDS έχουν πρόβλημα κρυπτογραφημένα δίκτυα, όπως τα Εικονικά Ιδιωτικά Δίκτυα (VirtualPrivateNetworks), γιατι δεν μπορούν να «διαβάσουν» το περιεχόμενο τωνπακέτων αλλά και σε switched δίκτυα όπου το πρωτόκολλο επικοινωνίας είναι διαφορετικής φιλοσοφίας. Η χρήση HIDS ή NNIDS μπορεί να λύσει τετοιου είδους προβλήματαπου οφείλονται στη φιλοσοφία λειτουργίας των NIDS.

ΚΕΦΑΛΑΙΟ 2

2.1 Firewall

Σκοπός του Firewallείναι να προστατέψει το δίκτυο μας από επιθέσεις που προέρχονται από ένα άλλο δίκτυο. Το δικό μας είναι υπο την ευθύνη ενός η παραπάνω ανθρώπων, ενώ το άλλο από το οποίο μας προστατεύει είναι ένα αναξιόπιστο εξωτερικό δίκτυο. Οπότε σε απόρρητα ή ευαίσθητα δεδομένα δεν εχουν πρόσβαση χρήστες χωρίς εξουσιοδότηση.

Μπορούμε να κατηγοριοποιήσουμε τα firewall σε τρία είδη:

1) Δρομολογητέςφιλτραρίσματοςή Packet-Filtering

2) Application Gateways ή Proxy,

3) Circuit-level Gateways.

2.1.1 Σχεδιάζοντας μια πολιτική ασφαλείας

Την περίμετρος ασφαλείας που θα εγκαταστήσουμε ώστε να ασφαλίσουμε το δίκτυο μας την καθορίζει η **πολιτική ασφαλείας** μαζί με τους μηχανισμούς και τις μεθόδους που την προάγουν και την ενισχύουν. Το firewallανήκει σε αυτούς τους μηχανισμούς ασφάλειας οπου χρειάζεται μαζί με τους υπόλοιπουςνα εξετάζονται μετά τοσχεδιασμό της πολιτικής ασφαλείας που θα ακολουθηθεί, αφού ουσιαστιακά αποτελούν την υλοποίησή της. Οπότε πριν υλοποιηθεί χρειάζεται να κάνουμε **ανάλυση κινδύνων και απαιτήσεων**.

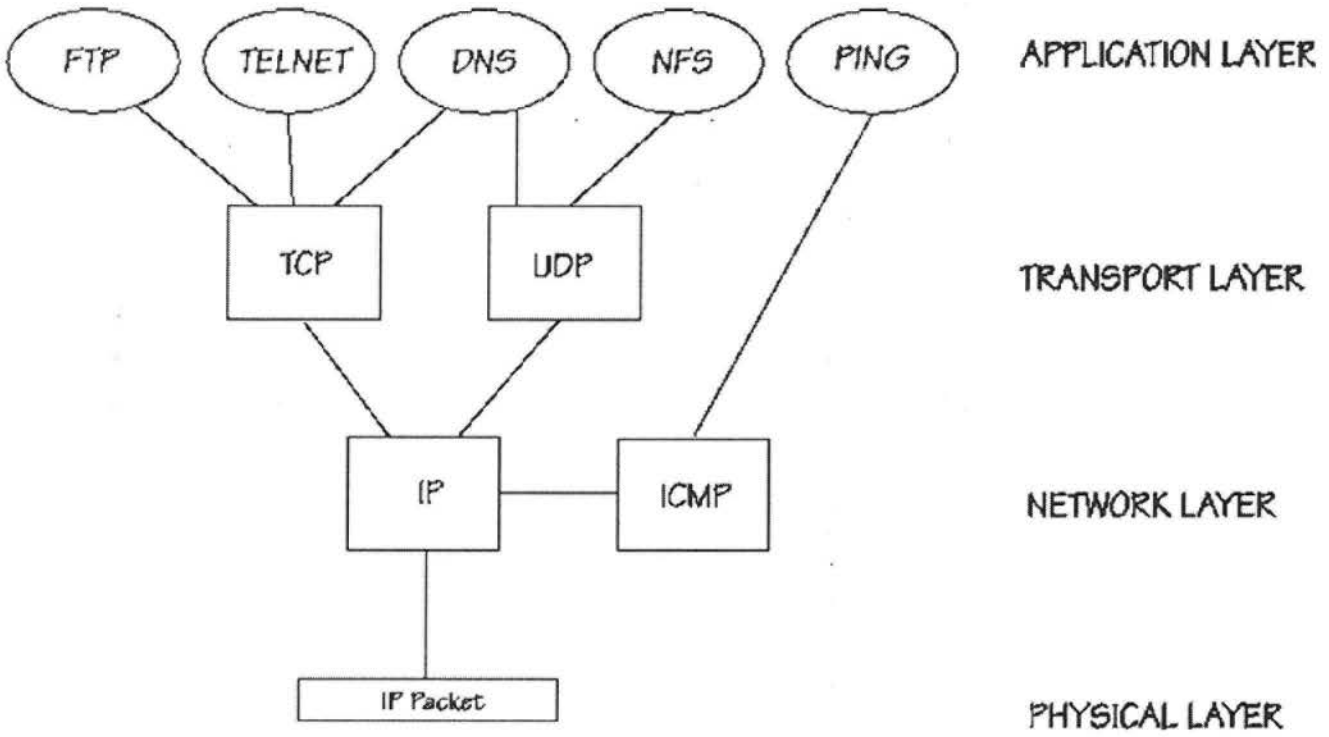
Πριν λοιπόν θέσουμε και ξεκινήσουμε να απαντάμε στην ερώτηση : *"Τί είδους firewallχρειαζόμαστε στο δίκτυό μας;"* Πρέπει να έχουμε απαντήσει αναλυτικά ερώτηση *"Τι είδους απειλές θα αντιμετωπίσει ;"* Με άλλα λόγια πρέπει να ξέρουμε τι θέλουμε να προστατεύσουμε από το δίκτυο μας και από τι θέλουμε να το προστατεύσουμε . Στην ανάλυση κινδύνων λοιπόν καθορίζουμε:

- Ποια είναι τα σημεία που είναι τρωτό το σύστημα μας,
- Ποιες είναι οι πιθανότητες να χρησιμοποιήσει κάποιος αυτά τα τρωτά σημεία ,
- Ποιατα μέτρα που χρειάζονται και τι κόστος έχουν.

Στη ανάλυση απαιτήσεων, καθορίζουμε την υπηρεσία που απαιτείται σγκεκριμένα καθώςκαι τι γίνεται σεπερίπτωση διακοπής της. Μόνο εφόσον έχει σχεδιαστεί η πολιτική ασφαλείας, επιλέγουμε το firewall που θα ενταχθείστους μηχανισμούς ασφαλείας του δικτύου. Εδω να τονισούμε ότι η πολιτική ασφαλείας δεν σχεδιάζεται μια φορά. Επειδήαλλάζουν συνεχώς οι συνθήκες, το Internet παίρνει καινούριες μορφές, οι αδυναμίες τωνσυστημάτων μεταβάλλονται, τα firewall αποκτούν καινούρια χαρακτηριστικά. Έτσι, και η πολιτική ασφαλείας πρέπει να επανασχεδιάζεται ή να ανανεώνεταιανά περιόδους, ανάλογα πάντα και με τις εξελίξεις και τις οικονομικές δυνατότητες.

2.1.2 Δρομολογητές φιλτραρίσματος(Packet-Filtering)

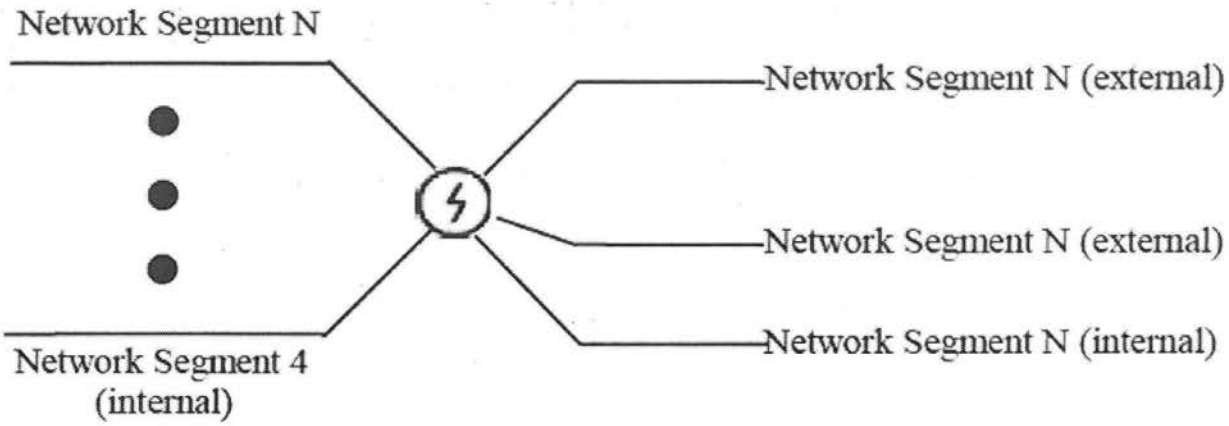
Αρκετοί δρομολογητέςτου εμπορίου μπορούν να ελέγχουν τα πακέτα με βασηορισμένα κριτήρια όπως:τύπος του πρωτοκόλλου, πεδία διεύθυνσης πηγής (source address),διεύθυνσης προορισμού (destination address) κ.α . Οι δρομολογητές φιλτραρίσματοςδιαθέτουν έναν ισχυρό μηχανισμό για τον έλεγχο κίνησης των πακέτων στο δίκτυο,επομένως και των υπηρεσιών που παρέχονται σε αυτό. Αυτή ακριβώς την ικανότητα ενόςδρομολογητήνα επιτρέπει ή να απορρίπτει τα πακέτα βάση κριτήριων αυστηρά για τις ιδιότητες πρωτοκόλλου ονομάζουμε*packet filtering* (φιλτράρισμα πακέτου).



Εικόνα 1TCPmodel

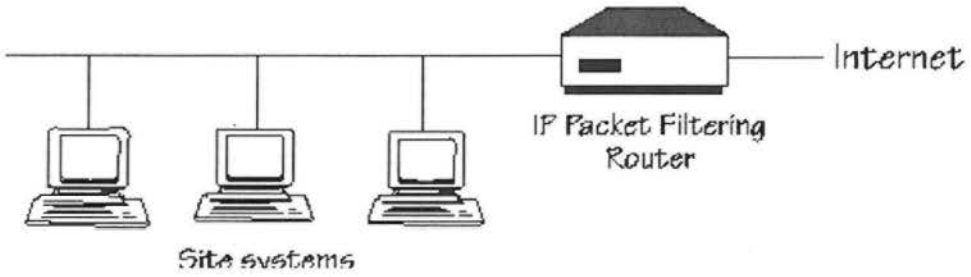
Η πολιτική ασφαλείας που υιοθετείται έχει κυρίως σαν στόχο την αποτροπή των εκτόςδικτύου τακέτων, και όχι τον έλεγχο των ύποπτων πακέτων εντός δικτύου. Με την αυτή τη λογική , αποφασίζουμεπου θα τοποθετηθεί ο δρομολογητής, και τι προγραμματισμό χρειάζεται για να εκτελεί φιλτράρισμα πακέτων. Επίσης η πολιτική ασφαλείας πρέπει να παρέχει ένα αόρατο μηχανισμό, για να μην τον αντιλαμβάνονται οι χρήστες. Το φιλτράρισμα των πακέτων, επειδήγίνεται στα **επίπεδα δικτύου** (Network layer) και **μεταφοράς** Transport layer) του μοντέλου TCP/IP, και όχι στο επίπεδο εφαρμογής , εξασφαλίζει σε μεγάλο βαθμό αυτή τη διακριτικότητα.

Ένα packet filter συνήθως το τοποθετούμε ανάμεσα σε ένα ή περισσότερα τμήματα δικτύου όπως βλέπυμε στηνεικόνα 2. Τα τμήματα του δικτύου χωρίζονται στα εξωτερικά (external) στα εσωτερικά (internal) και. Τα εξωτερικά τμήματα συνδέουν το δίκτυο μας με άλλα δίκτυα όπως το Internet. Τα εσωτερικά συνδέουν τους hosts του δικτύου μας και άλλους πόρους εντόςτου δικτύου.



Εικόνα 2Screening router ανάμεσα σε πολλά segments

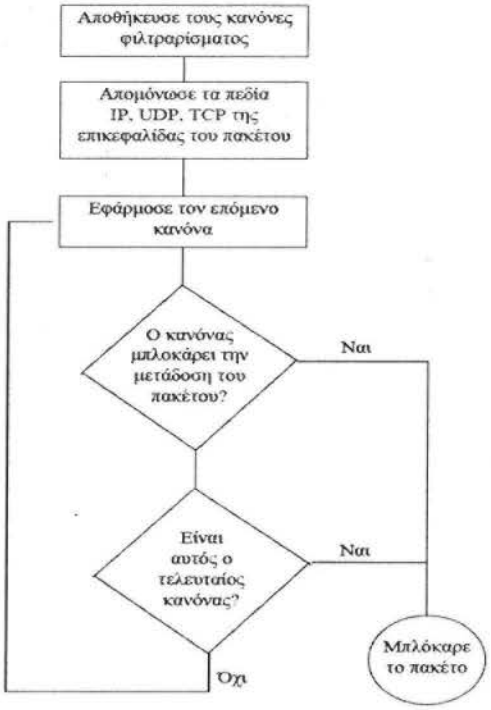
Για κάθε πόρτα του δρομολογητή μπορούμε να σχεδιάσουμε ξεχωριστή πολιτική ασφαλείας που θα καθορίζει τον τύπο πρόσβασης από/προς το δίκτυο για την κάθε μία.Όσο αυξάνεται ο αριθμός των τμημάτων του δικτύου που συνδεέται με το Routertόσο πιο πολύπλοκες γίνονται οι πολιτικές ασφαλείας. Επείδη η πολιτική ασφαλείας σχεδιάζεται έτσι ώστε να ευνοέι του hosts του δικτύου όταν επικοινωνούν με αλλους εκτός δικτύου πρέπει να προσαρμόζεται και το φίλτρο ανάλογα. Οπότε αναφερόμαστε σε μη συμμετρικά φίλτρα.



Εικόνα 3Packetfilteringrouter

Ο συνήθης τρόπος λειτουργίας ενός packet-filtering firewalleίναι ο εξής:

- Τα κριτήρια φιλτραρίσματος των πακέτωνείναι και οι κανόνες φιλτραρίσματος (packet filter rules) και έχουν τη δυνατότητα να εφαρμοστόυν και στις δύο πλευρές του δρομολογητή από και προς το δίκτυο.
- Όταν ένα πακέτο φθάνει σε μια πόρτα,οι επικεφαλίδες κάθε πακέτου απομονώνονται. Οι περισσότερες συσκευές φιλτραρίσματος εξετάζουν μόνο τα πεδία των IP, TCP, ή UDP πακέτων.
- Οι κανόνες φιλτραρίσματος αποθηκεύονται με αυστηρή σειρά προτεραιότητας και κάθε κανόνας εφαρμόζεταιστο πακέτομε τη σειρά της αποθήκευσης του.
- Αν ένας κανόνας μπλοκάρειτη λήψη ή μετάδοση ενός πακέτου, το πακέτο απορρίπτεται.
- Αν ένας κανόνας επιτρέπει τη λήψη ή μετάδοση ενός πακέτου, το πακέτο είναι αποδεκτό.
- Αν ένα πακέτο δεν ικανοποιεί κανέναν κανόνα, το πακέτο μπλοκάρεται



Εικόνα4packet-filteringfirewallalgorithm

Το πόσο σημαντική είναι οι προτεραιότητα των κανόνων φαίνεται από τον κανόνα 4 και 5.Αν τοποθετηθούν με λανθασμένη σειρά, μπορει να οδηγήσει στο να απαγορεύονται νόμιμες υπηρεσίες, ενώ τα παράνομα δεδομένανα επιτρέπονται .Οκανόνας 6ακολοθεί την εξής πολιτική ασφαλείας:

Οτιδήποτε δεν επιτρέπεται ρητά, απαγορεύεται.

Είναι μια ασφαλής θεωρία που ενδείκνυται για την ύπαρξη ασφαλών δικτύων. Μιαπιο 'χαλαρή' πολιτική ασφαλείας είναι η:*Οτιδήποτε δεν απαγορεύεται ρητά, επιτρέπεται.*Για να αξιοποιηθεί η δεύτερη λογική στην κατασκευή packet filters, οδιαχειριστήςπρέπει να σκεφτεί όλες τις πιθανές περιπτώσεις που δεν καλύπτονταιαπό τους κανόνες φιλτραρίσματος, ώστε να καταστήσει ασφαλέςτο δίκτυο. Και όσοπροστίθενται καινούριες υπηρεσίες με την πάροδο του χρονου,θα εμπλέκεται σε καταστάσεις όπου κανένας κανόνας δενταιριάζει με την υπηρεσία. Οπότε, για όποιες υπηρεσίες δεν υπάρχει κανόνας θα γίνονται επιτρεπτές.

2.1.2.1Σχεδιασμός ενός packet filter

Υποθέτοντας ότι η πολιτική ασφαλείας του δικτύου επιτρέπει τη λήψη Internetmail (SMTP, port 25) στην gateway μηχανή του δικτύου μας. Απαγορεύεται όμως ηλήψη mail από ένα συγκεκριμένο host, κάπου στο Internet. Η πολιτική ασφαλείας θα υλοποιηούνταν με τους εξής κανόνες:

1) *Μπλοκάρεται κάθε σύνδεση από τον SPIGOT απο οποιαδήποτε port του./σε οποιαδήποτε από τις port, οποιουδήποτε από τους hosts του δικτύου μας.*

2) *Επετρέπεται κάθε σύνδεση από οποιονδήποτε εξωτερικό host που προέρχεται απόοποιαδήποτε port του, στην port 25 της OUR-GW του δικτύου μας.*

Ενώ το φίλτρο, πουθα υλοποιούσε αυτούς τους δύο κανόνες, μοίαζει ως εξής:

Filter rule number	Action	Our Host	Port on Our Host	External Host	Port on Ex. Host
1	block	*	*	SPIGOT	*
2	allow	OUR_GW	25	*	*

Εικόνα 4παραδειγμα 1ο

Το πρόβλημα με το φίλτρο αυτό, είναι ότι ο περιορισμός που επιβάλλουμε, βασίζεταιστον αριθμό της port του εξωτερικού host. Παρότι η port 25 είναι όντως mailport, δεν μπορούμε να το ελέγξουμε σε έναν απομακρυσμένο υπολογιστή.Αν κάποιος λοιπόνέκανε μια κλήση για σύνδεση από την port 25, όχι ομως για αποστολή mail, θα αποκτούσε πρόσβαση σε όποιο hosttου δικτύου μας ήθελε. Για να αποφύγουμε τέτοια προβλήματα θα μπορούσαμε να επιτρέψουμε στους hosts του δικτύου μας να πραγματοποιούν εξερχόμενες κλήσεις στην port 25 οποιουδήποτε εξωτερικού host. Αν το εξωτερικό site δεν χρησιμοποιεί τηνγια το SMTP port 25 τότε η διαδικασία αποστολήςSMTP δεν στέλνει mail.Που ισοδυναμεί με αδυναμία υποστήριξης mail από τον εξωτερικό host.

Μία συνομιλίαTCPυλοποιείτια με πακετα που κινούνται και προς τις δύο κατευθύνσεις (full duplex σύνδεση). Ακόμα και όταν πρόκειται για πακέτα επιβεβαίωσης (aknowledgement packets) που κινούνται προς μια κατεύθυνση και πακέτα ελέγχου(control packets) πρέπει να έρχονται από την αντίθετη κατεύθυνση. Δηλαδή αν για παράδειγμα μια αίτηση δημιουργίας σύνδεσης (open request packet) έχει ψευδές ACK bit (flag)στην επικεφαλίδα του πακέτου, ενώ όλα τα άλλα πακέτα έχουν αληθές. Τα πακέτα με το αληθές ACK αποτελούν τμήμα προϋπάρχουσας σύνδεσης ενώ τα πακέτα μετο ψευδές ACK αντιπροσωπεύουν μηνύματα δημιουργίας σύνδεσης, τα οποία θέλουμενα επιτρέψουμε μόνο στους ενός δικτύου hosts. Το σκεπτικό είναι πωςένας εξωτερικός host μπορεί μονο να αποδεχθεί μια σύνδεση και όχι να τη δημιουργήσει. Έτσι, το σύνολο τον κανόνων, πρέπει τελικά να γραφτεί ως εξής για το δίκτυοπ.χ. 199.232.18.0:

Filter rule number	Action	Source Host	Port	Destination Host	Port	TCP flags	Comment
1	allow	199.232.18.0	*	*	25		our mail
2	allow	*	*	199.232.18.0	*	AC K	their replies

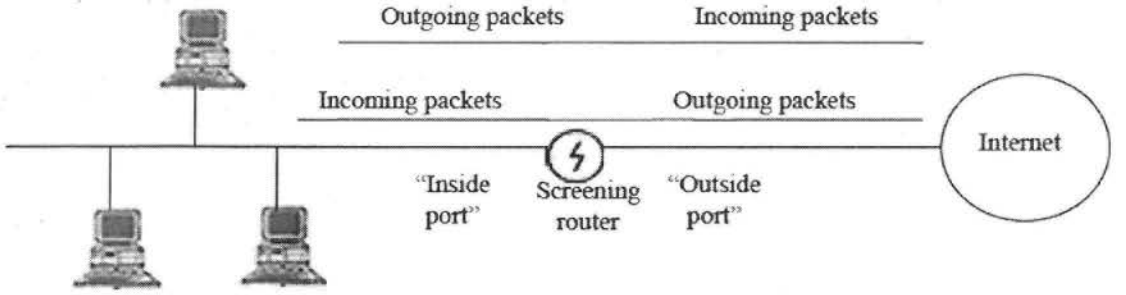
Εικόνα 5 παραδείγμα 2ο

Κανόνας 1 επιτρέπει μια σύνδεση και μεταφράζεται ως εξής:

Επέτρεπεται κάθε σύνδεση από το δίκτυο 199.232.18.0που προέρχεται από οποιαδήποτε απότις ports του, στην port 25 οποιουδήποτε host ή δικτύου.

Κανόνας 2 επιτρέπει μια σύνδεση και μεταφράζεται ως εξής:

Επέτρεπεται οποιαδήποτε σύνδεση από οποιοδήποτε δίκτυο προερχόμενη από την port 25 καιπου έχει το TCP ACK bit αληθές, σε οποιαδήποτε port οποιουδήποτε host του δικτύου199.232.18.0.

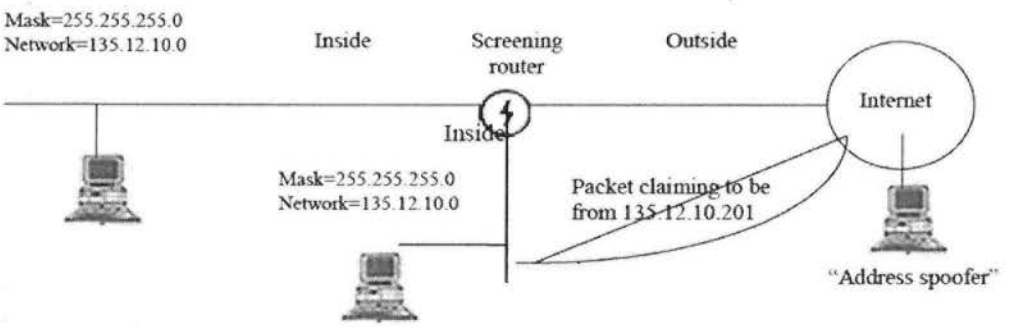


Εικόνα 6Τοποθέτηση packet filter

Αν έχουμε εναδρομολογητή φιλτραρίσματοςόπως στην εικόνας 7 . μπορεί να ελέγχει (screen) πακέτα και στα δυο του interfaces καιστην εσωτερική port, και στην εξωτερική port. Επίσης πρέπεινα τονίσουμε ότι τα πακέτα μπορεί να είναι είτε εισερχόμενα είτε εξερχόμενα και στα δύο interfaces του δρομολογητή. Γιαν μπορέσουμε να εφαρμοσουμε τους κανόνες φιλτραρίσματος σταεξερχόμενα πακέτα πρέπει να συμβουλεύεται οδρομολογητής τους τα routing tables που διαθέτει,για να καθοριστεί ο προορισμός που έχει το πακέτο. Ανδεν υπάρχει αντιστοιχία με τους κανόνες ή αν δεν είναι δρομολογήσιμο το πακέτο τότε απορρίπτεται,και αποστέλεταιτο μήνυμα "*ICMP απρόσιτος προορισμός*".

Αν οι δρομολογητές ελέγχουν τα εξερχόμενα πακέταόταν αυτά βγαίνουν έξωαπό την port του δρομολογητή,θα έχουμε απώλεια πληροφορίας.Αυτό συμβαίνει επειδή ο δρομολογητής δεν γνωρίζει το interface προέλευσης του πακέτου. Ετσι μπορεί να κατασταθεί τρωτό το δίκτυο μας σε επιθέσειςμεταμφιεσμένης διεύθυνσης γνωστές ως **address spoofing επιθέσεις**.

Εστω ένα δίκτυο Τάξης Β όπως στην εικόνα 8, το 135.12.0.0που είναι συνδεδεμένο στο Internet. Χρησιμοποιεί όπως βλέπουμε στην εικόνα ένα δρομολογητή φιλτραρίσματος. Το δίκτυο περιλαμβάνει δύο υποδίκτυα 10 και 11 με subnetmask για τα δύο υποδίκτυατην 255.255.255.0. Ένας εξωτερικός TCP/IP host στέλνει έναπακέτο υποστηρίζοντας ότι προέρχεται από τη 135.12.10.201 IPδιεύθυνση. Ο δρομολογητήςλαμβάνει το πακέτο στην εξωτερική του port . Αν οδρομολογητής φίλτραρε εισερχόμενα πακέτα, θα μπορούσε άμεσα να αποτρέψει το"κακόβουλο" πακέτο, αφού θα γνώριζεπως το δίκτυο 135.12.10.0 είναι συνδεέται σεδιαφορετική port (σε μια από τις εσωτερικές). Αν όμως, ο έλεγχος γίνεται σταεξερχόμενα πακέτα, το πακέτο θα δρομολογηθεί κανονικά, καθώς θα φαίνεται νόμιμο.



Εικόνα 8 Τοποθέτηση ενός packet filter - 2

Αν ο δρομολογητής διαθέτει μόνο δυο ports -μια που συνδέεται με το εξωτερικό δίκτυο και μια με το εσωτερικό τότε οι κανόνες φιλτραρίσματοςαποκτούν συμμετρία, είτε γράφονται για την εσωτερική είτε για την εξωτερική port. Αφού τα εισερχόμενα πακέταστη μία port,αν δεν απορρίπτονται από τον πίνακα δρομολόγησης του δρομολογητή, θα εμφανίζονται ως εξερχόμενα πακέταστην άλλη.

2.1.2.2.Πρωτόκολλα που πρέπει να φιλτράρονται

Η απόφαση να φιλτραριστούν ορισμένα πρωτόκολλα και πεδία εξαρτάται από τηνπολιτική ασφαλείας του δικτύου . Πάντως, υπάρχουν ορισμένες υπηρεσίες οι οποίεςείναι εκ φύσεως ευάλωτες σε παραβιάσεις, και συνήθως μπλοκάρονται στο firewall, είτεόταν προσπαθούν να μπουν στο δίκτυο, είτε όταν προσπαθούν να βγουν από αυτό:

- TFTP, port 69, trivial FTP
- X Windows, ports 6000+
- RPC, port 111
- rlogin, rsh, rexec, ports 513, 514 και 512
- TELNET, port 23
- FTP ports 20 και 21
- SMTP, port 25
- RIP, port 520
- DNS, port 53
- UUCP, port 540
- NNTP, port 119
- HTTP, port 80

2.1.2.3.Πλεονεκτήματατων packet filtering firewall

Σήμερα τα firewall που βασίζονται στο φιλτράρισμα IP πακέτων έχουν εξελιχθείσε αρκετά μεγάλο βαθμό, ώστε πλέον ο όρος δρομολογητή να αντικαθίσταται δικαιωματικά μετον όρο firewall. Υπάρχουν δύο είδη φιλτραρίσματος: το **στατικό φιλτράρισμα** καιτο **δυναμικό φιλτράρισμα**.

Τα **στατικά φίλτρα**, τα οποία υλοποιούνται στους δρομολογητές, εξετάζουν κάθεπακέτο που φθάνει στην port και παίρνουν απόφαση δρομολόγησης βασισμένα σεπληροφορίες που υπάρχουν στην επικεφαλίδα του πακέτου (packet header), όπως διεύθυνση πηγής (source) και προορισμού (destination), πρωτόκολλα και port αριθμούς.

Τα **δυναμικά φίλτρα**, εντούτοις είναι περισσότερο "έξυπνα" και μπορούν ναλάβουν αποφάσεις δρομολόγησης βασισμένα σε πρωτόκολλα υψηλότερου επιπέδου(όπως NFS, HTTP και RPC). Επίσης, και αυτό ίσως να είναι το περισσότερο σημαντικό,γνωρίζουν εάν το πακέτο είναι αναμενόμενο, με βάση την ύπαρξη προηγούμενηςεπικοινωνίας, δηλαδή **συγκρατούν την κατάσταση του πακέτου** που καταφθάνει. Έτσι,με αυτά τα φίλτρα δεν επιτρέπονται πακέτα τα οποία για παράδειγμα περιέχουν έναδιαφορετικό αριθμό SYN (Sequence Number, σε μια TCP σύνδεση) από αυτόν πουαναμενόταν.

Επίσης, επειδή τα φίλτρα λειτουργούν στα επίπεδα δικτύου και μεταφοράς(TCP/IP μοντέλο), εκτός του ότι είναι διάφανα στον χρήστη, είναι εκ φύσεως**περισσότερο προσαρμόσιμα σε καινούρια πρωτόκολλα**.

Τα φίλτρα **δεν απαιτούν μεγάλη επεξεργασία από την CPU**, και συνήθωςυλοποιούνται στο επίπεδο του λειτουργικού συστήματος. Έτσι, ιδιαίτερα σε δίκτυαυψηλής ταχύτητας (100 Megabit/second ή περισσότερο) υπάρχει μεγάλη απόδοση.

2.1.2.4. Μειονεκτήματατωνpacketfilteringfirewall

Οι packet filtering δρομολογητές έχουν κάποιες εγγενείς αδυναμίες, οι οποίεςδημιουργούν προβλήματα στους διαχειριστές των συστημάτων:

Πρώτον, ο καθορισμός των κανόνων φιλτραρίσματος είναι μια πολύπλοκη καισυχνά επίπονη διαδικασία, πόσο μάλλον όταν συνήθως δεν υπάρχουν έτοιμαπρογράμματα που να τεστάρουν την αποτελεσματικότητά τους. Ένα αξίωμα στηνβιομηχανία ασφάλειας υπολογιστών, είναι το "*Η πολυπλοκότητα είναι αντιστρόφως*

ανάλογη με την ασφάλεια". Λάθη στην υλοποίηση του filtering κώδικα, καθιστούν ταδίκτυα τρωτά από κάθε άποψη.

Δεύτερον, η αυθεντικοποίηση του χρήστη, όπως αυτή καθορίζεται από τηνπολιτική ασφαλείας, υλοποιείται σε άλλα συστήματα και όχι από το firewall. Ακριβώςεπειδή το firewall είναι **χαμηλού-επιπέδου** ως προς το TCP/IP μοντέλο), δεν μπορεί νακατανοήσει αφηρημένες έννοιες όπως "χρήστης".

Τρίτον, οι δρομολογητές φιλτραρίσματος δεν παρέχουν δυνατότητα καταγραφής (logging) λειτουργιών που βρίσκονται σε εξέλιξη, καθιστώντας δύσκολη την ανίχνευση μιαςπαραβίασης . Έτσι, εάν παρακαμφθεί κάποιος κανόνας φιλτραρίσματος από κάποιονhacker, υπάρχει ο κίνδυνος να εντοπιστεί η παραβίαση αφότου ο hacker έχει ήδηεπιτελέσει το έργο του.

Τέταρτον, ένας αριθμός RPC (Remote Procedure Call) υπηρεσιών είναι δύσκολονα φιλτραριστεί αποτελεσματικά, επειδή οι αντίστοιχοι servers "ακούνε" σε ports πουκαθορίζονται τυχαία κατά την εκκίνηση του συστήματος. Μία υπηρεσία που καλείται*portmapper* αντιστοιχεί τις αρχικές κλήσεις RPC υπηρεσιών στους προκαθορισμένουςαριθμούς υπηρεσιών (δηλαδή στις ports), αλλά στους δρομολογητές δεν υπάρχει τέτοιαυπηρεσία. Έτσι εφόσον ο δρομολογητή δεν μπορεί να ξέρει σε ποιες ports "κατοικούν" οιυπηρεσίες, δεν είναι δυνατόν να μπλοκάρει αποτελεσματικά τις υπηρεσίες αυτές, εκτόςκαι αν μπλοκάρει όλα τα UDP πακέτα (Οι RPC υπηρεσίες χρησιμοποιούν συνήθως τοUDP). Μπλοκάροντας όμως το UDP σημαίνει ότι μπλοκάρονται απαραίτητες υπηρεσίεςόπως το DNS (που χρησιμοποιεί το UDP).

Πέμπτον, αδυναμίες των δρομολογητών φιλτραρίσματος θεωρούνται και αυτές που οφείλονταιστην λανθασμένη τοποθέτησή τους, όπως είδαμε και στην προηγούμενη ενότητα.

2.1.3 Application Gateways

Τα gateways επιπέδου εφαρμογής ή application gateways προγραμματίζονταιώστε να καταλαβαίνουν την κίνηση στο **επίπεδο εφαρμογής** του TCP/IP . Έτσι,παρέχουν ελέγχους προσπέλασης σε επίπεδο χρήστη και σε επίπεδο πρωτοκόλλωνεφαρμογής.

Τα application gateways υιοθετήθηκαν προκειμένου να εξαλειφθούν κάποιες απότις αδυναμίες που εμφανίστηκαν στην υλοποίηση των φίλτρων στους δρομολογητές .Έτσι, χρησιμοποιούνται software εφαρμογές, οι οποίες προωθούν και φιλτράρουνσυνδέσεις για υπηρεσίες όπως HTTP, TELNET και FTP. Μια τέτοια εφαρμογή καλείται**proxy υπηρεσία**. Ένας χρήστης που επιθυμεί να συνδεθεί στο σύστημα, θα πρέπει

πρώτα να συνδεθεί στο gateway και ύστερα στο host προορισμού, όπως και στοπαράδειγμα που ακολουθεί (εικόνα 9):

1) Ο χρήστης κάνει telnet στο application gateway και πληκτρολογεί το όνομα ενός εσωτερικού host,

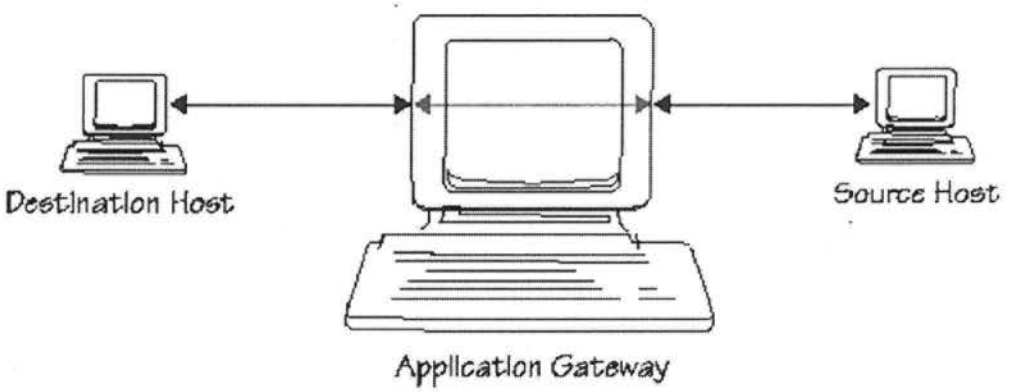
2) Το gateway ελέγχει την IP διεύθυνση του χρήστη (source) και την εγκρίνει ή τηναπορρίπτει, σύμφωνα με ορισμένα κριτήρια προσπέλασης,

3) Ο χρήστης ενδεχομένως να πρέπει να αυθεντικοποιήσει τον εαυτό του (π.χ.χρησιμοποιώντας μια one-time password συσκευή),

4) Η proxy υπηρεσία δημιουργεί μια TELNET σύνδεση μεταξύ του gateway και τουεσωτερικού host,

5) Η proxy υπηρεσία "μεταφέρει" bytes μεταξύ των δύο συνδέσεων, και

6) Το application gateway καταγράφει (log) τη σύνδεση.



Εικόνα 7Virtual σύνδεση που υλοποειται από το application gateway και τις proxy

2.1.3.1 Τρόπος λειτουργίας

Το Gateway έχει την ευθύνη να λαμβάνει πακέτα από το ένα δίκτυο και να παραδίδει σε ένα άλλο δίκτυο. Συνήθως αυτό σημαίνει ότι λαμβάνει πακέτα από τοInternet και τα παραδίδει στο τοπικό δίκτυο (και αντιστρόφως). Το Gateway "ανοίγει" ταπακέτα, εξετάζει το περιεχόμενό τους, και εξασφαλίζει ότι δεν μπορούν να βλάψουνδυνητικά το τοπικό δίκτυο. Αφού τα πακέτα ελέγχονται ως προς την ασφάλειά τους, το

Gateway "χτίζει" καινούρια, με το ίδιο περιεχόμενο. Έτσι, **μόνο οι τύποι πακέτων γιατους οποίους υπάρχει κώδικας κατασκευής μπορούν να εγκαταλείψουν το Gateway**.Είναι αδύνατον να σταλεί μη εξουσιοδοτημένος τύπος πακέτου, αφού δεν υπάρχεικώδικας για να το δημιουργήσει. Έτσι αποτρέπονται τα

"back doors". Τα καινούριαπακέτα στέλνονται μέσω ενός ξεχωριστού interface δικτύου.Για να χρησιμοποιήσουν το Gateway, οι χρήστες πρέπει να συνδεθούν (log in) μετην Gateway μηχανή, ή να υλοποιήσουν μια συγκεκριμένη client εφαρμογή σε κάθε hostαπό τον οποίο θα συνδεθούν . Έτσι, ένα custom πρόγραμμα πρέπει να γραφτεί γιακάθε εφαρμογή, και οι εφαρμογές που επιτρέπονται είναι μονάχα αυτές για τις οποίεςέχει γραφτεί πρόγραμμα. Αυτό ίσως να είναι ένα εγγενές μειονέκτημα, αλλά αποτελεί

πλεονέκτημα ως προς την ασφάλεια του συστήματος, καθώς εφαρμόζει πλήρως τηνφιλοσοφία "*Αυτό που δεν επιτρέπεται ρητά, απαγορεύεται*".Το custom πρόγραμμα εφαρμογής λειτουργεί ως proxy που δέχεται κλήσεις καιτις εξετάζει με βάση λίστες προσπέλασης που διαθέτει. Στην περίπτωση αυτή το proxy

λειτουργεί ως **proxy server**. Λαμβάνοντας την κλήση και αφότου πιστοποιηθεί ότι ηκλήση είναι επιτρεπόμενη, ο proxy προωθεί την αίτηση στον αντίστοιχο server. Τότε, oproxy λειτουργεί τόσο ως server, όσο και ως client. Ως server προκειμένου να λάβει τηναίτηση και ως client προκειμένου να την προωθήσει. Αφότου εγκατασταθεί η (session), ο proxy απλά αντιγράφει και μεταδίδει τα δεδομένα ανάμεσα στον client πουέκανε την αίτηση και στον server τον οποίο στόχευε η αίτηση.

Εφόσον είναι απαραίτητη μια custom client εφαρμογή για την επικοινωνία με τονproxy server, ορισμένες standard κλήσεις συστήματος, όπως η connect( ), πρέπει νααντικατασταθούν με μια proxy έκδοση αυτών των κλήσεων συστήματος. Έπειτα, η clientεφαρμογή πρέπει να μεταγλωττιστεί και να συνδεθεί με τις proxy αυτές εκδόσεις.

2.1.3.2 Πλεονεκτήματα των Application Gateways

Πλεονεκτήματα από τη χρήση των application gateways για την προστασία τουσυστήματος μπορούν να θεωρηθούν τα εξής :

- Τα gateways μπορούν να απορρίψουν ή να επιτρέψουν μια σύνδεση, βασιζόμενα όχιμόνο στο όνομα χρήστη, στις διευθύνσεις και τα πρωτόκολλα, αλλά προχωρούν πιο"βαθειά": μπορούν για παράδειγμα να φιλτράρουν μια FTP σύνδεση, επιτρέποντας τηχρήση της εντολής "get" και απαγορεύοντας τη χρήση της εντολής "put".
- Μπορούν να φιλτράρουν Java applets και ActiveX προγράμματα.
- Δεν επιτρέπουν την εκτέλεση εφαρμογών για τις οποίες δεν έχει γραφτεί proxy, όπως ήδη αναφέρθηκε, αυξάνοντας την ασφάλεια του συτήματος.
- Αποκρύπτουν πληροφορίες για το σύστημα, αφού τα ονόματα των εσωτερικών hostsδεν είναι απαραίτητο να είναι γνωστά μέσω DNS σε απομακρυσμένα συστήματα. Τασυστήματα αυτά χρειάζεται να γνωρίζουν μόνο το όνομα του host που "φιλοξενεί" toapplication gateway".
- Υποστηρίζουν τη δυνατότητα αυθεντικοποίησης (authentication) και καταγραφής(logging) .
- Είναι αποτελεσματικά ως προς το κόστος τους, καθώς το ανεξάρτητο software ήhardware που απαιτείται για την αυθεντικοποίηση ή την καταγραφή, εγκαθίσταται**μόνο** στο application gateway host και πουθενά αλλού.
- **Σε περίπτωση που συνδυάζονται με packet filtering δρομολογητές**, απαιτούνλιγότερο περίπλοκους κανόνες φιλτραρίσματος, από ότι εάν υφίστατο μονάχα οδρομολογητής. Αυτό

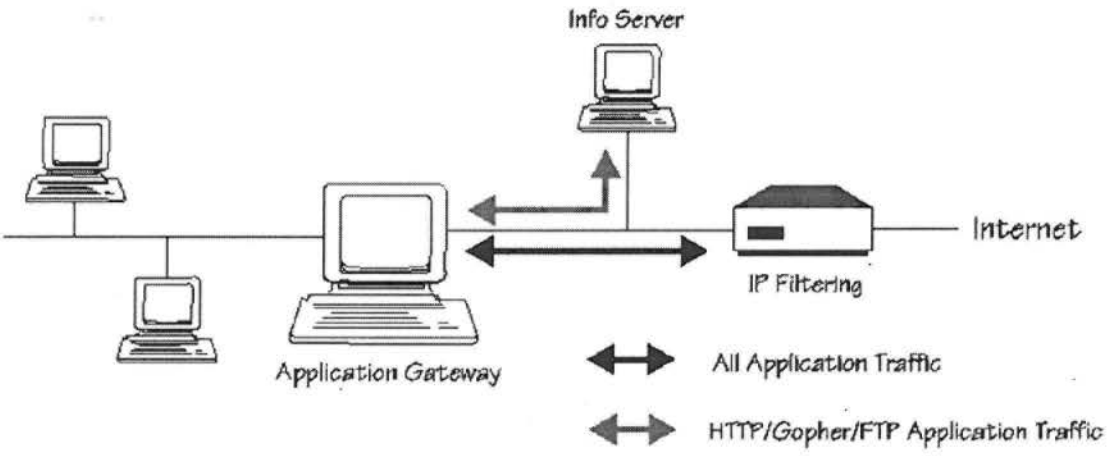
συμβαίνει διότι το μόνο που πρέπει να κάνει ο δρομολογητήςείναι να επιτρέπει πακέτα που προορίζονται για το application gateway.

2.1.4 Υλοποιήσεις των Firewall

Τα firewall μπορούν, με συνδυασμούς από application gateways και packetfiltering δρομολογητές, να υλοποιηθούν με τρείς σχηματισμούς: Dual-homed host,Screenedhost, και Screenedsubnetfirewall.

2.1.4.1. Dual-homed Gateway

Στηνεικόνα 10 αναπαρίσταται η διαμόρφωση ενός δικτύου υπό την προστασία ενός dual-homed host (δηλαδή ενός host που έχει δύο interfaces δικτύου). Ο host αυτός έχειαπενεργοποιημένες τις λειτουργίες IP δρομολόγησης (δηλαδή, δεν μπορεί να δρομολογείπακέτα μεταξύ των δύο δικτύων). Επιπρόσθετα, χρησιμοποιείται ένας packet filtering(screening) δρομολογητής, στο σημείο όπου συνδέεται το δίκτυο με το Internet, ώστε ναυπάρχει μεγαλύτερη ασφάλεια. Έτσι, δημιουργείται ένα εσωτερικό, ελεγχόμενο(screened) subnetστο οποίο μπορούν να τοποθετηθούν ειδικά συστήματα όπως Webservers.



Εικόνα10Dual-HornedGatewayFirewall

Αυτός ο τύπος firewall υλοποιεί την πολιτική ασφαλείας, σύμφωνα με την οποία"*απορρίπτεται ό,τι δεν επιτρέπεται ρητά*", εφόσον δεν υποστηρίζονται υπηρεσίες για τις οποίες δεν υπάρχουν proxy servers στο gateway. Ο host **δεν θα πρέπει να δέχεταιsource-routed πακέτα**. (πακέτα στα οποία ο αποστολέας αναγράφει τον δρόμο πουπρέπει να ακολουθήσουν, παρακάμπτοντας έτσι τους δρομολογητές). Με αυτόν τοσχηματισμό ασφαλίζεται σε μεγάλο βαθμό η ασφάλεια του δικτύου (ιδιαίτερα ηασφάλεια των hosts που βρίσκονται στο interface αριστερά του application gateway),καθώς οι "δρόμοι" προς το προστατευμένο subnet είναι γνωστοί μονάχα στο firewall καιόχι στο υπόλοιπο Internet, εφόσον τα Internet συστήματα μπορούν να αποστείλουνπακέτα μονάχα στο firewall (μόνο τότε θα τα κάνει αποδεκτά ο δρομολογητή). Τα ονόματα καιοι IP διευθύνσεις των "προστατευμένων" hosts του συστήματος είναι "κρυμμένα" από ταInternet συστήματα, αφόσον το firewall δεν χρειάζεται να μεταδίδει DNS πληροφορίες.

Εφόσον το firewall χρησιμοποιεί ένα host σύστημα, μπορεί (και πρέπει) ναδιαθέτει ειδικό software που θα αναγκάζει τους χρήστες να αποδείξουν την ταυτότητάτους. Οι μηχανισμοί ασφαλείας που υλοποιούνται

στον host πρέπει να είναι πολύαυστηροί και αποτελεσματικοί (π.χ έλεγχοι ορθότητας-audit, καταγραφής (log) κ.λ.π),καθώς το gateway είναι και το τελευταίο οχυρό ασφαλείας του συστήματος. Εάν παρακαμφθεί η ασφάλειά του, τότε ο εισβολέας μπορεί να κάνει σοβαρές παραβιάσεις(π.χ να επανενεργοποιήσει τη δρομολόγηση IP πακέτων στο firewall).

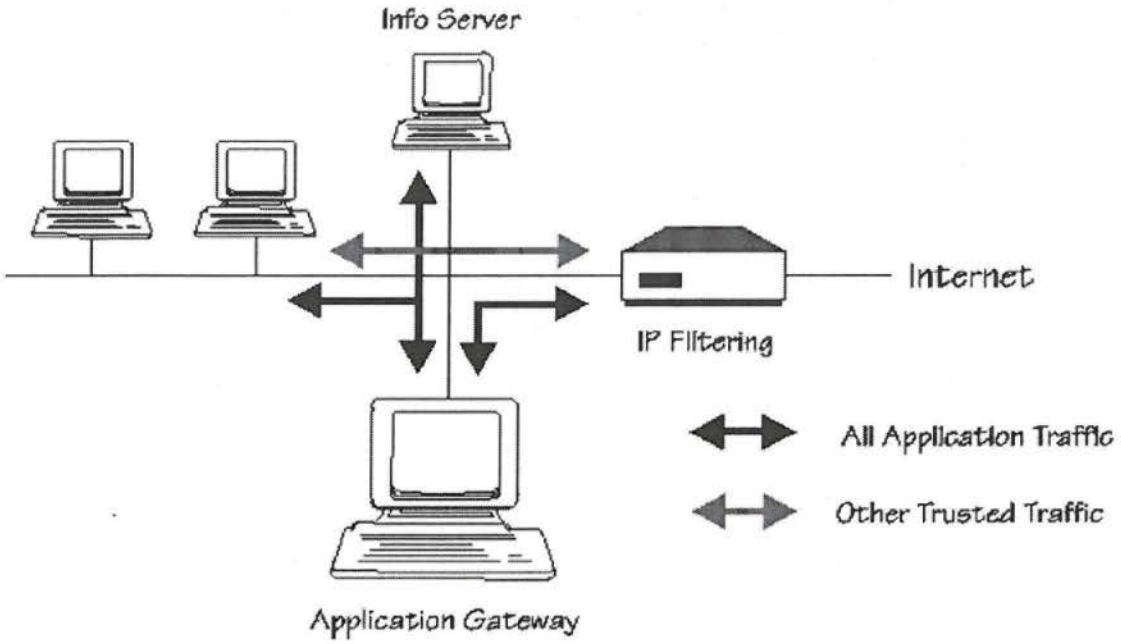
Το dual-homedgatewayfirewall, όπως και το screenedsubnetfirewall για τοοποίο θα δούμε στη συνέχεια, παρέχει τη δυνατότητα διαχωρισμού των πακέτων πουσχετίζονται με έναν information server, από άλλα πακέτα που προορίζονται ήπροέρχονται από το site. Έτσι, ο information server τοποθετείται στο subnet μεταξύ τουgateway και του δρομολογητή, όπως φαίνεται στο σχήμα. Υποθέτοντας ότι το gateway παρέχειτις κατάλληλες proxy υπηρεσίες για τον information server (π.χ http, ftp ή gopher), οδρομολογητή μπορεί να αποτρέψει την απευθείας πρόσβαση στον server και να υποχρεώσει ταπακέτα να πηγαίνουν στο firewall. Εαν επιτρέπεται η απευθείας πρόσβαση στον server,τότε το όνομα και η IP διεύθυνση του server μπορούν να "διαφημιστούν" μέσω DNS(κάτι που δεν είναι πολύ ασφαλές).

Με την τοποθέτηση του information server στο subnet μεταξύ του gateway καιτου δρομολογητή, εξασφαλίζεται ότι: Εαν ένας εισβολέας καταφέρει να παρακάμψει τον δρομολογητήκαι αποκτήσει μη εξουσιοδοτημένη πρόσβαση στον server, για να αποκτήσει πρόσβασηστους host αριστερά από το gateway (που λογικά έχουν και τις περισσότερο πολύτιμεςπληροφορίες) πρέπει να παρακάμψει **και** το μηχανισμό ασφαλείας του dual-homedgateway, κάτι που είναι εξαιρετικά δύσκολο.

Η εγγενής ακαμψία του dual-homed gateway μπορεί να αποτελεί σοβαρόμειονέκτημα για ορισμένα sites: εφόσον οι υπηρεσίες επιτρέπονται μόνο εαν υπάρχουνproxies για αυτές, δεν μπορεί να υπάρχει πρόσβαση σε άλλες υπηρεσίες, εκτός και αναυτές τοποθετηθούν στην Internet πλευρά του gateway (δεξιά απο το gateway στοσχήμα). Εαν δεν υπάρχει packet filtering δρομολογητή που να προστατεύει τις υπηρεσίες αυτές,τότε υπάρχει πρόβλημα ασφαλείας.

2.1.4.2 Screened Host Firewall

Το screened host (ελεγχόμενος host) firewall, που αναπαρίσταται στην εικόνα 11,παρέχει έναν πιο εύκαμπτο μηχανισμό από το dual-homed gateway firewall, αν και τοτίμημα της ευκαμψίας αυτής είναι συνήθως η ασφάλεια. Ο σχηματισμός αυτός θεωρείταιιδανικός για sites που αναζητούν προστασία, αλλά όχι σε τέτοιο βαθμό ώστε ναπροτιμήσουν ένα dual-homed gateway.



Εικόνα 8Screened Host Firewall

Το firewall αποτελείται από έναν packet filtering δρομολογητή και έναapplication gateway, το οποίο οποθετείται στο "προστατευμένο" subnet αριστερα απότον δρομολογητή. Το application gateway χρειάζεται ιόνο ένα interface δικτύου. Οιproxy υπηρεσίες του application gateway μεταβιβάζουν FTP, TELNET, HTTP :αι άλλες υπηρεσίες για τις οποίες υπάρχουν proxies, στα συτήματα του site. Ο δρομολογητήςφιλτράρει και λέγχει "επικίνδυνα" πρωτόκολλα προτού αυτά φτάσουν (αν φτάσουν) στοapplicationgateway και στους :λλους hosts. Απορρίπτει (ή δέχεται) πακέτα εφαρμογήςσύμφωνα με τους εξής κανόνες:

- Πακέτα εφαρμογής από τα Internet sites προς το application gateway, δρομολογούνταικανονικά,
- Όλα τα άλλα πακέτα απορρίπτονται,
- Ο δρομολογητής απορρίπτει κάθε πακέτο εφαρμογής που προέρχεται από τοεσωτερικό του δικτύου, εκτός και αν έρχεται από το application gateway.

Το ότι το application gateway διαθέτει μόνο ένα interface δικτύου, καθιστά τοσχηματισμό περισσότερο ύκαμπτο, αλλά και λιγότερο ασφαλή, καθώς ο δρομολογητήςμπορεί να παρακάμψει το gateway στην ερίπτωση κάποιων "έμπιστων" υπηρεσιών. Οιέμπιστες υπηρεσίες μπορεί να είναι αυτές για τις οποίες δεν πάρχουν proxy υπηρεσίες,και προφανώς θα είναι έμπιστες υπό την έννοια ότι η πολιτική ασφαλείας του ικτύου θατις έχει καταστήσει έμπιστες. Για παράδειγμα, υπηρεσίες όπως το NNTP ή το DNSμπορεί να εωρούνται έμπιστες.

.1.4.3 Screened Subnet Firewall

Το screened subnet firewall είναι ένας συνδυασμόςμεταξύ του dual-homedgateway και του :reenedhostfirewall. Στην εικόνα 12,χρησιμοποιούνται δύο δρομολογητές για τη δημιουργία ενός εσωτερικού, *λεγχόμενου*(screened) υποδικτύου (subnet). Αυτό το subnet (που συχνά καλείταιΑποστρατικοποιημένη Ζώνη -

DMZ), "φιλοξενεί" το application gateway, όπως επίσης (χωρίς να είναι απαραίτητο) και άλλα συστήματα που απαιτούν προσεκτικά ελεγχόμενηπροσπέλαση, π.χ.Informationservers.

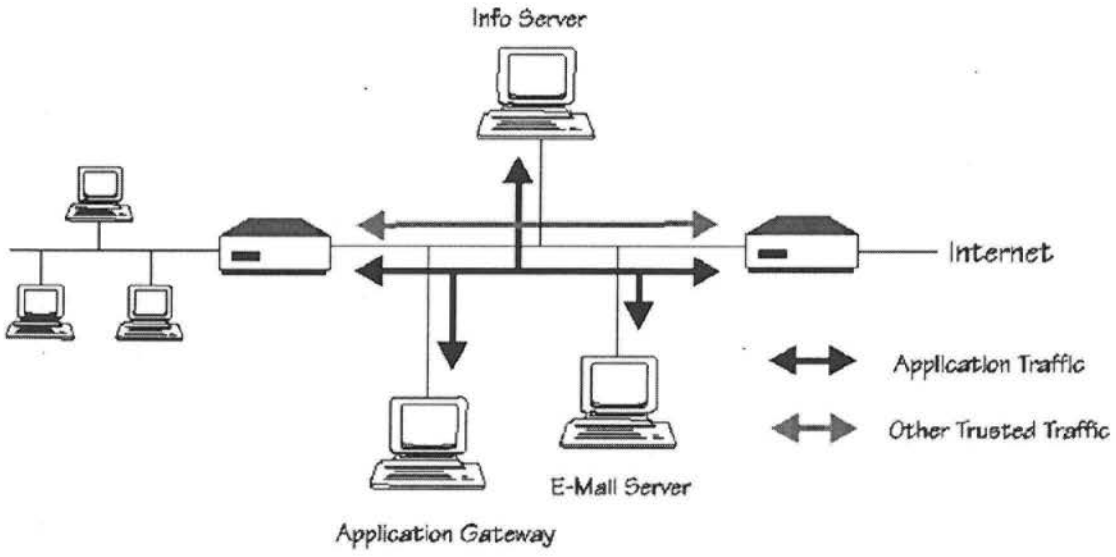
Ο δρομολογητής που βρίσκεται στο σημείοσύνδεσης του δικτύου με το Internet εφαρμόζει τους ακόλουθους κανόνες:

- πακέτα εφαρμογής από το application gateway στα Internet συστήματα,δρομολογούνται κανονικά,
- e-mail κίνηση από τον e-mail server προς τα Internet sites, δρομολογείται κανονικά,
- πακέτα εφαρμογής από τα Internet sites προς το application gateway, δρομολογούνταικανονικά,
- e-mail κίνηση από τα Internet sites προς τον e-mail server, δρομολογείται κανονικά,
- όλα τα άλλα πακέτα απορρίπτονται.

Ο εξωτερικός δρομολογητής επίσης, θα μπορούσε να χρησιμοποιηθεί για να"μπλοκάρει" πακέτα πρωτοκόλλων όπως NFS και NIS, ή άλλων επισφαλώνπρωτοκόλλων που δεν θα έπρεπε να μεταβιβάζονται προς ή από τους hosts στο screenedsubnet.

Ο δεύτερος δρομολογητής (εσωτερικός) δρομολογεί τα πακέτα με βάση τουςακόλουθους κανόνες:

- πακέτα εφαρμογής από το application gateway στα site συστήματα, δρομολογούνταικανονικά,
- e-mail κίνηση από τον e-mail server προς τα site συστήματα, δρομολογείται κανονικά,
- πακέτα εφαρμογής από τα site συστήματα προς το application gateway,δρομολογούνται κανονικά,
- e-mail κίνηση από τα site συστήματα προς τον e-mail server, δρομολογείται κανονικά,
- όλα τα άλλα πακέτα απορρίπτονται.



Εικόνα 9Screened Subnet Firewall

Με το σχηματισμό αυτόν, κανένας host του δικτύου δεν είναι άμεσαπροσπελάσιμος από το Internet και αντίστροφα, όπως και στο dual-homed gateway. Μιαμεγάλη διαφορά όμως που υπάρχει μεταξύ των δύο μηχανισμών, είναι ότι εδώ πέραχρησιμοποιούνται δρομολογητές προκειμένου να μεταβιβάσουν πακέτα σε ειδικάπροστατευμένα συστήματα, εξαλείφοντας έτσι την ανάγκη το application gateway να έχειδύο interfaces.

Το γεγονός αυτό αποτελεί και ένα μεγάλο πλεονέκτημα του σχηματισμούαυτού, καθώς είναι πιο εύκαμπτος και ενδείκνυται για δίκτυα που χρειάζονται μεγάληταχύτητα.

Οι δύο δρομολογητές αποτελούν τα δύο βασικά "οχυρά" που πρέπει ναπαρακάμψει ένας hacker προκειμένου να αποκτήσει πρόσβαση στα προστατευμένασυστήματα του δικτύου (πρέπει λοιπόν να δοθεί μεγάλη έμφαση στους κανόνεςφιλτραρίσματος που διαθέτουν). Το application gateway, ο e-mail server και ο information server μπορούν να διαμορφωθούν κατάλληλα ώστε να είναι και τα μόνα"γνωστά" συστήματα στο Internet. Κανένα άλλο σύστημα δεν πρέπει να αναφέρεται σεμια DNS βάση δεδομένων. Επίσης, ο application gateway μπορεί να διαθέτει softwareαυθεντικοποίησης ώστε να ταυτοποιεί όλες τις εισερχόμενες συνδέσεις. Προφανώς, ηδιατήρηση ξεχωριστών συστημάτων για τα application gateways και τα packet filters,συνεισφέρει στην διαμόρφωση ενός δικτύου το οποίο ελέγχεται απλά και εύκολα.

2.1.5 Firewall: Ολοένα και περισσότερο ασφαλή

Σε πολύ σύντομο χρονικό διάστημα, τα firewall έχουν κερδίσει την εκτίμησησχεδόν όλων των οργανισμών στο Internet .Χωρίς αυτά, οι διαχειριστές ενός δικτύου θα έπρεπε να διατηρούν την ασφάλεια όλων των συστημάτωντους σε υψηλό επίπεδο, κάτι που είναι εξαιρετικά δύσκολο αν λάβει κανείς υπ'όψιν τουτο το γεγονός ότι ο αριθμός των συστημάτων ανά δίκτυο αυξάνει ραγδαία στις μέρες μας.

2.1.5.1 Αυξημένες απειλές

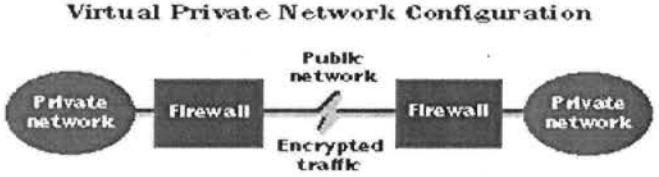
Η σημερινή κατάσταση στο Internet εξακολουθεί να είναι πηγή ανησυχιών γιατους διαχειριστές δικτύων. Ενώ πρέπει να φροντίζουν ώστε οι χρήστες να είναι"ευτυχισμένοι", με την υιοθέτηση νέων υπηρεσιών, ταυτόχρονα πρέπει να μεριμνούν γιατην ασφάλειά τους. Όμως, καθώς ο αριθμός των χρηστών και των υπηρεσιών αυξάνεταικάθε μέρα, έτσι αυξάνονται και οι διαγραφόμενες απειλές.Σήμερα υπάρχουν ειδικές ομάδες σύνταξης αναφορών περί παραβιάσεων στοInternet (π.χ. η CERT*), οι οποίες δέχονται καθημερινά χιλιάδες κλήσεις από χρήστεςπου έχουν να αναφέρουν κάποια παραβίαση στο σύστημά τους. Επίσης, τα θέματα περίασφαλείας έχουν γίνει πλέον αντικείμενο "ανοικτής" συζήτησης σε mailing lists και σενewsgroups στο USENET, όπου συζητούνται και καυτηριάζονται οι αδυναμίες τωνσυστημάτων και οι τρόποι εκμετάλλευσής των. Έτσι, αποτρέπονται αλλά καιδημιουργούνται καινούριες παραβιάσεις.Οι source-route επιθέσεις που στοχεύουν τα συστήματα πίσω από τα firewall,έχουν γίνει ευκολότερες χάρη στην ύπαρξη εργαλείων που αυτοματοποιούν τηδιαδικασία. Επίσης, έχουν αυξηθεί οι επιθέσεις άρνησης υπηρεσίας (denial of service) οιοποίες δημιουργούν σύγχυση και ελαττώνουν την παραγωγικότητα. Συνήθεις επιθέσειςάρνησης υπηρεσίας περιλαμβάνουν το "πλημμύρισμα" (flooding) των e-mail συνδέσεωνώστε να αποτρέψουν τη χρήση τους, καθώς και την αποστολή ICMP echo πακέτων πουκορέζουν τα δίκτυα μπλοκάροντας τις επικοινωνίες. Ορισμένα firewall παραμένουνευάλωτα σε αυτού του είδους τις επιθέσεις.

2.1.5.2 Καινούρια χαρακτηριστικά

Αποκρινόμενοι στις αυξανόμενες απειλές, οι εταιρίες firewall έχουν εισάγει αρκετάκαινούρια χαρακτηριστικά στα προϊόντα τους. Αυτά τα χαρακτηριστικά ποικίλουν απότην αύξηση των τύπων των proxies και των υπηρεσιών που υποστηρίζουν, εως τηναύξηση των μηχανισμών ασφαλείας και της ευκολίας διαχείρισης:

Εργαλεία Διαχείρισης και Διαμόρφωσης των firewallεμφανίζονται καθημερινάστην αγορά του Internet. Ορισμένα firewall χρησιμοποιούν GUIs (Graphical UserInterfaces) ώστε να διευκολύνονται οι διαχειριστές στην διαμόρφωσή τους. Άλλασυστήματα firewall επιτρέπουν την **απομακρυσμένη** άσκηση διαχείρισης καιελέγχου ορθότητας (auditing) μέσω διαφόρων πρωτοκόλλων, όπως το SMTP (SimplemailTransferProtocol), το SNMP (SimpleNetworkManagementProtocol) και toHTTP μέσω του WorldWideWeb. Εξυπακούεται ότι αυτοί οι μηχανισμοίπροϋποθέτουν ισχυρή αυθεντικοποίηση και ελέγχους προσπέλασης.

Virtual Private Networks (Εικονικά Ιδιωτικά Δίκτυα)**:** Σε πολλές επιχειρήσεις υπάρχειη ανάγκη ασφαλούς επικοινωνίας μεταξύ των ιδιωτικών δικτύων που διαθέτουν σεδιαφορετικά σημεία στο Internet. Προκειμένου να εξασφαλίσουν την ασφάλειατέτοιου είδους επικοινωνιών, οι εταιρίες firewall εφαρμόζουν κρυπτογραφικούςμηχανισμούς στα προϊόντα τους με σκοπό τη δημιουργία ενός virtual ιδιωτικούδικτύου μεταξύ δύο sites, όπου η πληροφορία μεταδίδεται κρυπτογραφημένη. ΤαVPNs επιτυγχάνονται με κρυπτογράφιση στο επίπεδο του Internet Protocol, μεταξύδύο "συνεργαζόμενων" firewall. Εφόσον το VPN εγκατασταθεί, οι hosts σε έναση μείο μπορούν να επικοινωνούν με τους hosts στο απομακρυσμένο σημείο χωρίς τοφόβο της παραβίασης της εμπιστευτικότητας των πληροφοριών που ανταλλάσσονται.Φυσικά, όπως και σε κάθε κρυπτογραφικό σχήμα, το VPN είναι ασφαλές εφόσον είναιασφαλή και τα κρυπτογραφικά κλειδιά που χρησιμοποιούνται.



Εικόνα 10VPNconfiguration

Network Address Translation: Σε μια διαδικασία NAT (Μετάφραση ΔιεύθυνσηςΔικτύου), το firewall αντικαθιστά τις IP διευθύνσεις των πακέτων με διαφορετικέςδιευθύνσεις. Αυτό μπορεί να γίνει για διάφορους λόγους, οι περισσότεροι από τους οποίους σχετίζονται με την ασφάλεια. Καταρχήν, το NAT επιτρέπει σε ένανοργανισμό να αποκρύψει τόσο την ύπαρξη συγκεκριμένων συστημάτων στοεσωτερικό του δίκτυο, όπως και την δομή καθ'αυτή του εσωτερικού του δικτύου. Έναχαρακτηριστικό που καθιστά το NAT πολύ ελκυστικό αλλά δεν σχετίζεται με τηνασφάλεια, είναι η ικανότητά του να μετατρέπει hosts δικτύου με μη μοναδικέςδιευθύνσεις, σε hosts με μοναδικές διευθύνσεις, επιτρέποντας έτσι στον οργανισμό νασυνδεθεί με το Internet.

Αυτή η τεχνική είναι χρήσιμη στο να "κρύβει" διευθύνσεις που περιέχονται σεεπικεφαλίδες πακέτων. Εντούτοις, προκειμένου να αποκρύπτονται αποτελεσματικά οιεσωτερικές διευθύνσεις, είναι προτιμότερη η

'παρέμβαση" μέσα στο πακέτοκαθ'αυτό. Έτσι, ορισμένα προϊόντα firewall ξαναγράφουν π.χ. τις e-mail επικεφαλίδεςώστε να κρύψουν το όνομα του εσωτερικού συστήματος από το οποίο προήλθε τομήνυμα.

Proxies και υπηρεσίες:

Με στόχο την επέκταση της λειτουργικότητας τωνfirewall, ολοένα και περισσότερα proxies τροστίθενται στα συστήματα. Αυτό είναικαι ένα από τα χαρακτηριστικά στο οποίο "ποντάρουν" οι τρομηθευτέςfirewall. Ούτως ήάλλως, εαν δεν υπάρχουν διαθέσιμα τα κατάλληλα proxies, οι υπηρεσίες προς τους πελάτες και τους χρήστες ελαττώνονται αισθητά, ενώ αυξάνεται και ο φόρτος τωνδιαχειριστές που πρέπει να παρακάμπτουν τα firewall διατηρώντας παράλληλα τοσύστημα ασφαλές. Κάποια από τα proxies που έχουν ανακοινωθεί είναι:

- POP3 - Αυτό το proxy επιτρέπει απομακρυσμένη σύνδεση σε e-mail χωρίς να είναιαπαραίτητη η παρουσία ενός SMTP server στον απομακρυσμένο host. Το POP3πρωτόκολλο υποστηρίζει τη χρήση της εντολής APOP, που επιτρέπει στοναπομακρυσμένο client να αυθεντικοποιηθεί στον εσωτερικό POP3 server.
- LP (Printer) - Αυτό το proxy επιτρέπει τη διέλευση εργασιών εκτύπωσης (print jobs)μέσω του firewall.
- SecureSocketslayer (SSL) και Secure-HTTP (SHTTP) - Αυτά τα δύο proxies"επεκτείνουν" τα υπάρχοντα HTTP proxies στο να υποστηρίζουν επιπλέονμηχανισμούς ασφαλείας για Web πρόσβαση.
- Domain Name System (DNS) - Όταν χρησιμοποιείται το NAT, είτε για ναντιστοιχίσει μη μοναδικές διευθύνσεις σε μοναδικές, είτε για να αποκρύψειεσωτερικές διευθύνσεις, πρέπει να υπάρχει έγκυρη DNS πληροφόρηση τόσο στους εσωτερικούς όσο και στους εξωτερικούς χρήστες. Οι πωλητές firewallενσωματώνουν πλέον dual-DNS servers στα προϊόντα τους, ένα για περιορισμένηπληροφόρηση προς το κοινό (το Internet) και ένα για πλήρη πληροφόρηση προς ταεσωτερικά συστήματα του δικτύου.

Transparent Proxies (Διάφανα Proxies):

Εκτός από τα proxies που αναφέρθηκανπροηγουμένως, οι πωλητές firewall υλοποιούν επίσης τα εγόμενα *διάφανα proxies.Διάφανο proxy* υφίσταται όταν οι χρήστες δεν ξέρουν ότι όντως χρησιμοποιείται τοproxy. Οι χρήστες, μπορούν να είναι ενήμεροι για την ύπαρξη ενός proxy, με δύοτρόπους: πρώτον, μερικά proxies απαιτούν αλληλεπίδραση του χρήστη με το firewall,όπως π.χ η πληκτρολόγηση ενός ID και ενός συνθηματικού. Δεύτερον, ένα μη-διάφανο proxy μπορεί να απαιτεί την εγκατάσταση custom client software από τονχρήστη, όπως π.χ οι clients που βασίζονται στο Socks. Πολλοί οργανισμοί θαπροτιμούσαν να μην επιφορτώνουν τους χρήστες τους με τέτοιες διαδικασίες, κάτιπου εξασφαλίζεται με τα *διάφανα proxies*. Αντούτοις, τα *διάφανα proxies* απαιτούνμερικές ρυθμίσεις σε ορισμένα client sotware. Για παράδειγμα, ένας Web browserπρέπει να υποστεί κάποιες ρυθμίσεις για proxies πρωτοκόλλων όπως το ftp ή togopher.

Καταγραφή (log) και έλεγχος ορθότητας:

Τα περισσότερα firewall παρέχουνμηχανισμούς καταγραφής (logging) λειτουργιών. Εντούτοις, ορισμένα firewallπαρέχουν τη δυνατότητα υποστήριξης μηχανισμών ελέγχου ορθότητας (audit)

καιπροειδοποιητικών (alert) μηχανισμών. Τα auditing εργαλεία επεξεργάζονται την ήδηκαταγραφόμενη (από τα logs) πληροφορία και την παρουσιάζουν με έναν περισσότεροευανάγνωστο τρόπο. Οι alert μηχανισμοί πληροφορούν σε πραγματικό χρόνο τους διαχειριστές για "επικίνδυνες" λειτουργίες που επιχειρούνται στο firewall.Επιπρόσθετα, το SNMP μπορεί να χρησιμοποιηθεί για την προειδοποίηση (alert)απομακρυσμένων hosts.

2.1.6 Κριτήρια επιλογής ενός firewall

Ίσως η σημαντικότερη απόφαση που πρέπει να πάρει ένας οργανισμός πουεπιδιώκει να εγκαταστήσει ένα ασφαλές δίκτυο στο Internet, είναι η επιλογή τουκατάλληλου firewall που θα πλαισιώσει τους μηχανισμούς ασφαλείας του δικτύου**[naim]**. Τα κριτήρια επιλογής ενός firewall, εξαρτώνται άμεσα από τα ακόλουθα θέματα:

2.1.6.1 Λειτουργικό σύστημα (OS)

Η επιλογή της πλατφόρμας, πάνω στην οποία θα "τρέχει" το firewall, εξαρτάταιαπό τη φύση του δικτύου και από το κατά πόσο οι διαχειριστές αισθάνονται"άνετα" με το ένα ή το άλλο λειτουργικό.

2.1.6.2 Αρχιτεκτονική

Η αρχιτεκτονική ενός firewall περιλαμβάνει τις εγγενείς δυνατότητές του καθώςκαι διάφορους ειδικούς μηχανισμούς που ενσωματώνει προκειμένου να ενισχύσει τηνασφάλεια που παρέχει **[naim]**. Ένα firewall πρέπει καταρχήν να είναι "χτισμένο" επάνωσε ασφαλές OS, και να επιτρέπει την έλευση μόνο σε συγκεκριμένους τύπους πακέτων.Η ειρωνία είναι, ότι όσο περισσότερα πρωτόκολλα και υπηρεσίες υποστηρίζει έναfirewall, τόσο μεγαλύτερη είναι η πιθανότητα παράκαμψής του από κάποιον επιτήδειο.

Τα περισσότερα firewall υποστηρίζουν τις δημοφιλείς IP υπηρεσίες,συμπεριλαμβανομένων των FTP, TELNET, HTTP, και SMTP, αλλά διαφέρουν στοντρόπο με τον οποίο υλοποιούν αυτήν την υποστήριξη. Οι περισσότερες ασφαλείςπροσεγγίσεις είναι αυτές των application gateways σε συνδυασμό με packet filteringδρομολογητές.Όταν πιστοποιούν την ακεραιότητα των συστημάτων τους, ορισμένα firewallελέγχουν ψηφιακές υπογραφές ή checksums, είτε στον κώδικα των προγραμμάτων πουλειτουργούν, είτε σε αρχεία συστήματος. Ο τρόπος με τον οποίο αντιδρούν τα firewallσε μια διαπιστωμένη παραβίαση, διαφέρει δραματικά από firewall σε firewall. Γιαπαράδειγμα, το firewall Eagle της Raptor "ρίχνει" (shut down) το σύστημα με το πουδιαπιστώσει μια παράβαση, ενώ το InterLock της ANS Inc. απλά καταγράφει τιςλειτουργίες που βρίσκονται σε εξέλιξη, επιτρέποντας την κανονική λειτουργία τουσυστήματος.

2.1.6.3 Διαχείριση (Configuration)

Λέγοντας διαχείριση εννοούμε το περιβάλλον κάτω από το οποίο ο χρήστης τουfirewall (ο administrator) ενεργοποιεί ή απενεργοποιεί πρωτόκολλα, περιορίζει τις παρεχόμενες υπηρεσίες με κριτήριο

ονόματα χρηστών ή/και διευθύνσεις, πιστοποιεί καιελέγχει τις παραμέτρους του συστήματος. Ιδανικά, ένα firewall πρέπει να παρέχει στους διαχειριστές των δικτύων ένα ξεκάθαρο σύνολο επιλογών και ρυθμίσεων για κάθεπρωτόκολλο, και μια ευέλικτη μέθοδο ελέγχου των τρεχουσών ρυθμίσεων. Εάν οιδιαχειριστές δεν μπορούν εύκολα να καθορίζουν τα πρωτόκολλα που "ελέγχονται" και νααλλάζουν τις ρυθμίσεις, τότε το firewall μάλλον δυσχεραίνει παρά διευκολύνει τις προσπάθειές τους. Έτσι, τα firewall που διαθέτουν GUIs (Graphical User Interfaces)έχουν το προβάδισμα σε αυτόν τον τομέα.

2.1.6.4 Σύστημα προειδοποίησης

Ένα "ισχυρό" σύστημα προειδοποίησης σε ένα firewall θα πρέπει ναπεριλαμβάνει ενημέρωση σχετικά με το τρέχων status λειτουργίας, λάθη που έχουν γίνει,πιθανές ενέργειες παραβιάσεων, και "συναγερμούς3υ" προειδοποίησης. Το ιδανικό firewallθα πρέπει έγκαιρα και σε πραγματικό χρόνο να ενημερώνει το διαχειριστή γιαοποιοδήποτε πρόβλημα.

2.1.6.5 Αυθεντικοποίηση

Ένα αξιόπιστο firewall θα πρέπει να διαθέτει ισχυρούς μηχανισμούςαυθεντικοποίησης, για όσους συνδέονται σε αυτό ή διαμέσου αυτού. Σήμερα, ταfirewall χρησιμοποιούν one-time passwords, ψηφιακές υπογραφές πακέτων, καιεπαναχρησιμοποιήσιμα passwords.Τα one-time passwords είναι έγκυρα για μία και μόνο σύνδεση. Ανσυνδυάζονται και με ψηφιακές υπογραφές, αποτελούν ισχυρό όπλο στα χέρια τουδιαχειριστή.Οι υπογραφές πακέτων είναι προσδιοριστές αυθεντικοποίησης (authenticationindicators) που περιλαμβάνονται σε ένα πακέτο δεδομένων (συνήθως σε όλα τα πακέταμιας σύνδεσης) και που χρησιμοποιούν κρυπτογράφηση δημοσίου-/ιδιωτικού κλειδιούγια τη ψηφιακή υπογραφή κάθε πακέτου.

Τα επαναχρησιμοποιήσιμα passwords παραμένουν απαράλλαχτα για πολλαπλέςlogin συνδέσεις. Δεν είναι ασφαλή και αποτελούν την έσχατη λύση.Η πιο ασφαλής λύση αυθεντικοποίησης συνδυάζει τα one-time passwords με τις ψηφιακές υπογραφές πακέτων.

2.1.7 Firewall και Multicasting

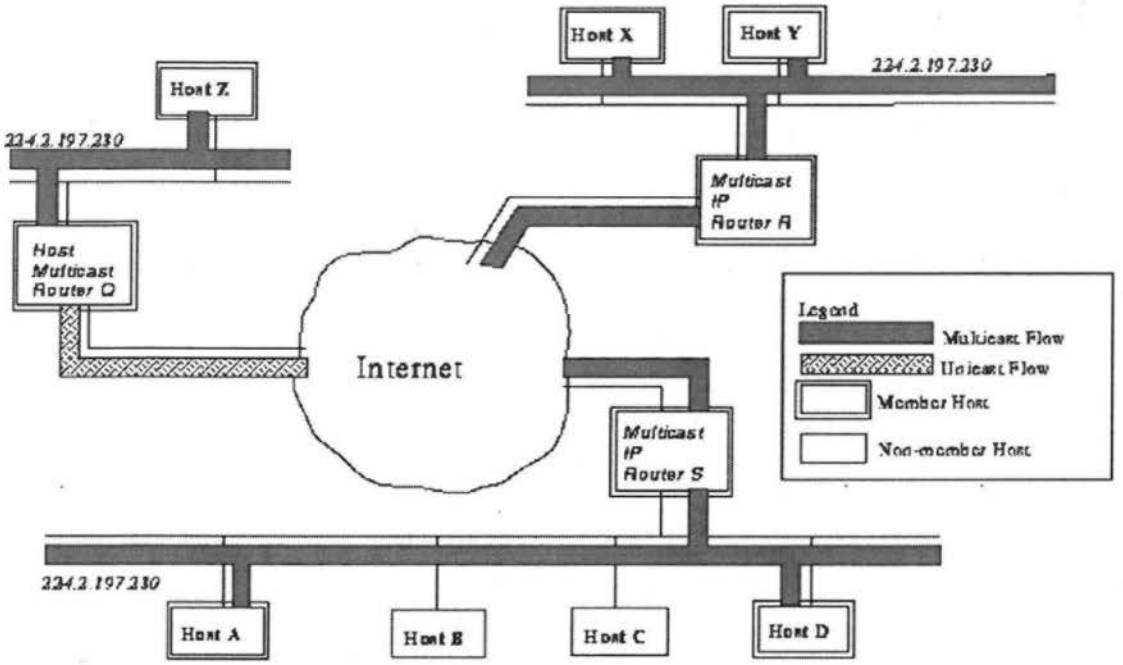
Η δραματική εξάπλωση του Internet έχει στιγματιστεί από την υιοθέτησηκαινούριων τεχνολογιών, όπως το audio και video conferencing (συνεδρίαση)**[karanaim]**. Το conferencing επιτρέπει σε ανθρώπους που βρίσκονται μακριά ο ένας απότον άλλον, να ακούσουν και να δουν ο ένας τον άλλον, να μοιραστούν και ναεπεξεργαστούν γραφικές εικόνες. Μια από τις γνωστότερες τεχνολογίες για toconferencing μέσω του Internet είναι το MulticastBackbone ή απλά "MBone". Η χρήσητου MBone εξαπλώνεται γρήγορα, καθώς υπάρχει δωρεάν MBone software για πολλές υπολογιστικές πλατφόρμες.

Η ευρεία χρήση του MBone, εντούτοις, εμποδίζεται από προβλήματα πουσχετίζονται με την ασφάλεια στο Internet. Τα πρωτόκολλα στα οποία το MBoneβασίζεται, γίνονται εκμεταλλεύσιμα από "κακόβουλους" hackers. Γι'αυτόν το λόγο, ταπερισσότερα application gateways firewall μπλοκάρουν τα MBone πακέτα. Έτσι, οιοργανισμοί που τα χρησιμοποιούν δεν μπορούν να έχουν πρόσβαση στο MBone.Προκειμένου να διευθετηθεί αυτό το πρόβλημα, η Trusted Information Systems, Inc. (TIS) ανέπτυξε και υλοποίησε μια προσέγγιση που επιτρέπει στα Internet firewall να"περάσουν" MBone πακέτα από και προς το τοπικό δίκτυο, ενώ ταυτόχρονα ασκούνταιοι απαραίτητοι έλεγχοι ασφαλείας.**Σημείωση:** Το TIS Internet Firewall Toolkit (FTWK) παρέχει όλους τους απαραίτητουςcomponents με τους οποίους μπορεί να "χτιστεί" ένα application gateway. Το FTWKείναι δωρεάν για τους χρήστες του Internet.

2.1.7.1 MBone και Multicast

Το MBone είναι μια συλλογή Internet κόμβων που καταλαβαίνουν έννοιες όπως "ομάδες IP multicast", "διευθυνσιοδότηση", "δρομολόγηση". Τα MBone δεδομένα(audio, video, εικόνα, κείμενο) μεταδίδονται σε UDP datagrams (πακέτα) τα οποία έχουνmulticast διευθύνσεις ως διευθύνσεις προορισμού. Οι multicast διευθύνσεις είναι IPδιευθύνσεις τάξης D (224.0.0.0 εως 239.255.255.255) που δεν αντιπροσωπεύουν απλάέναν host αλλά ομάδες hosts. Όταν ένας host εισέρχεται σε μια multicast ομάδα,λαμβάνει όλα τα datagrams που προορίζονται για την multicast διεύθυνση της ομάδας.Ένας host μπορεί να είναι ταυτόχρονα μέλος σε πολλές ομάδες. Η IANA (InternetAssignedNumbersAuthority) έχει καθορίσει το 224.2. ως το εύρος των διευθύνσεωνστο MBone conferencing. Το μοναδικό πρωτόκολλο μεταφοράς που επιτρέπει tomulticasting, είναι το UDP.

Τα multicast datagrams διανείμονται στο Internet από multicast δρομολογητές, ήαλλοιώς mrouters. Αλλά και απλοί hosts μπορούν να χρησιμοποιηθούν για δρομολόγησημulticast πακέτων (από εδώ και πέρα θα τους λέμε host-based mrouters). Οι (τελικοί)MBone end hosts (που δεν είναι δρομολογητής) χρησιμοποιούν το πρωτόκολλο IGMP (InternetGroup Management Protocol) στα τοπικά τους δίκτυα για να αποστείλουν "αιτήσειςσυμμετοχής σε μία ομάδα" (group-join request) στους τοπικούς mrouters. Οιmrouters,προκειμένου να επικοινωνήσουν μεταξύ τους χρησιμοποιούν το πρωτόκολλο DVMRP(DistanceVectorMulticastRoutingProtocol). Υπάρχουν και άλλα multicast πρωτόκολλαδρομολόγησης, όπως το MOSPF (MulticastOSPF) και το PIM (ProtocolIndependentMulticasting).



Εικόνα 11Τοπολογία Δικτύου για Multicast Δρομολογητές και Hosts

ΕπειδήπολλοίIPδρομολογητέςδενυποστηρίζουνακόμαIPMulticasting, othost-basedmrouters μεταδίδουν" ενθυλακωμένα (encapsulated) IPmulticastπακέτασεάλλουςmrouters. "Ενθυλακώνω" ένα πακέτο ημαίνει "μεταβάλλω το πακέτο ώστε οιενδιάμεσοι IP δρομολογητές να το αντιλαμβάνονται σαν ένα υνηθισμένο unicastπακέτο". Όταν ένας mrouter λαμβάνει ένα ενθυλακωμένο multicast πακέτο, αφαιρεί ηνencapsulating IP επικεφαλίδα και, ανάλογα με τους multicast πίνακες δρομολόγησης πουδιαθέτει, το ροωθεί σε έναν άλλο mrouter ή/και το κάνει multicast στο τοπικό τουδίκτυο (το μεταδίδει σε όλους τους hosts ου ανήκουν στην ομάδα της multicastδιεύθυνσης που αναγράφεται στο πακέτο).

Στην εικόνα 14 απεικονίζεται η διαμόρφωση ενός δικτύου για χρήση του MBone μεhost-basedmrouters αι IPδρομολογητής. Στο σχήμα, τα multicast μονοπάτια αναπαρίστανταιμε "σκοτεινό" γκρίζο χρώμα, ενώ τα nicast μονοπάτια με "φωτεινό" γκρίζο χρώμα. Οι(τελικοί) end hosts A, B, C, και D είναι στο ίδιο τοπικό ίκτυο. Οι A και D γίνονται μέλητης multicast ομάδας 224.2.197.230 στέλνοντας IGMP datagrams που αμβάνονται απότον mrouter S. Ο mrouter S είναι ένας IP mrouter και προωθεί το group-join datagram εγειτονικούς mrouters στο Internet, προσδιορίζοντας ότι "χρειάζεται" να λάβει όλα tadatagrams που πευθύνονται στο 224.2.197.230. Οι hosts X, Y και Z είναι (τελικοί) endhosts σε άλλα δίκτυα τα οποία υνδέονται με το MBone μέσω των mrouters R και Q, καιέχουν (οι hosts) επίσης γίνει μέλη της multicast μάδας 224.2.197.230.

.1.7.2 Θέματα ασφαλείας που αφορούν το MBone

Η multicast διευθυνσιοδότηση δημιουργεί προβλήματα ασφαλείας επειδήδημιουργεί "*ψευδώνυμα ιευθύνσεων*" (*address aliases*) τα οποία μπορούν ναχρησιμοποιηθούν για κακό σκοπό. Όταν ένας host που πορεί να λάβει multicast πακέτααπό το Internet, γίνεται μέλος μιας multicast ομάδας, δίνει στους "έξω"

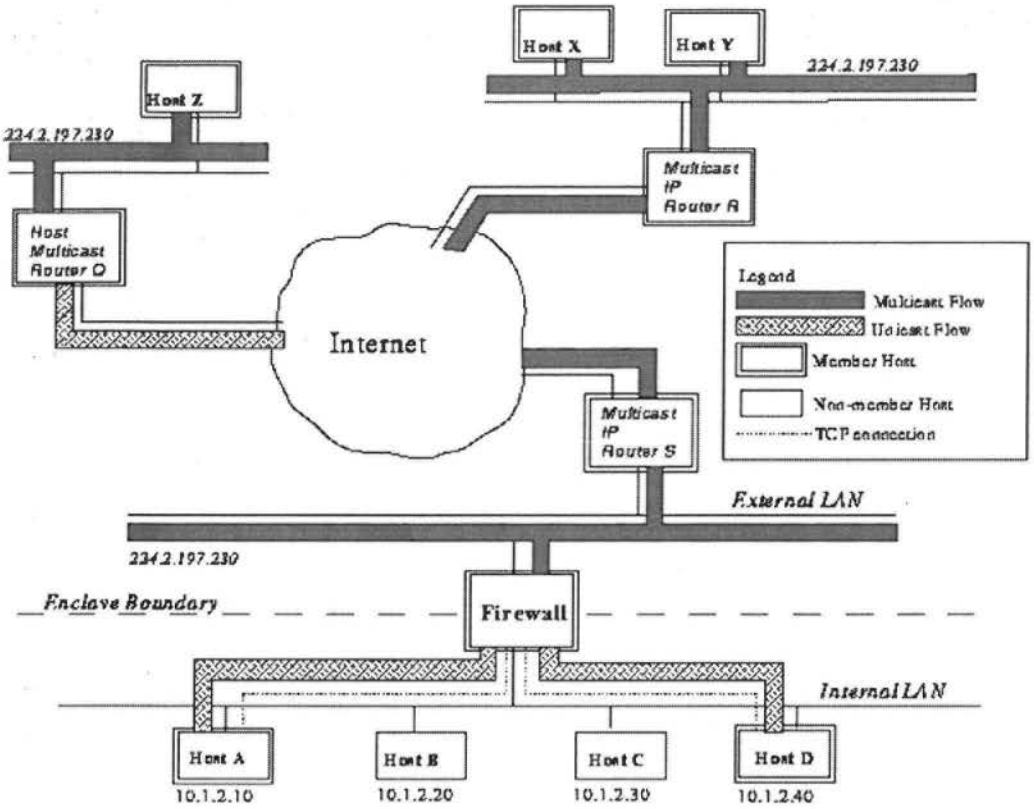
(outsiders) τηνικανότητα απευθείας πρόσβασης σε **οποιαδήποτε** από τις UDP ports του,συμπεριλαμβανομένων και ports που θα έπρεπε να είναι προσβάσιμες μόνο από τους "μέσα" (insiders). Για παράδειγμα, α θεωρήσουμε έναν host που η κανονική unicast IPδιεύθυνσή του είναι η 10.1.2.10. Αυτός ο host γίνεται μέλο της multicast ομάδας224.2.197.230 ώστε να λάβει μια MBone συνεδρίαση στις UDP ports 5001, 5002 και5003 Επιπλέον, ας υποθέσουμε ότι ο host παρέχει NFS υπηρεσίες (για τους "μέσα") στηport 2049. Εαν ένα συμμετέχων στο MBone ή κάποιος άλλος outsider στείλει ένα"κακόβουλο" πακέτο στο 224.2.197.230 στη por 2049, το kernel του host θα παραδώσειτο πακέτο στην NFS υπηρεσία του host, όπως ακριβώς και εαν το πακέτ προορίζοντανγια τη διεύθυνση 10.1.2.10, δηλαδή την κανονική IP διεύθυνση του host. Εαν υπήρχανκαι άλλο εσωτερικοί hosts που είχαν γίνει μέλη της ίδιας multicast ομάδας, **όλα** θαλάμβαναν αντίγραφα κάθ "κακόβουλου" εισερχόμενου πακέτου. Καταλαβαίνουμελοιπόν πόσο μεγάλος είναι ο κίνδυνος με τα multicas πακέτα.Τα προβλήματα αυτά θα μπορούσαν να λυθούν εάνπιστοποιήσουμε όλη τηνMBone κίνηση (traffic) κα απορρίπταμε όλα τα πακέτα εκτός από αυτά που προέρχονταναπό "έμπιστους" χρήστες. Αυτή η λύση δεν είνα βιώσιμη, καθώς δεν είναι δυνατόν ναυποχρεώσει κάποιος τους χρήστες που στέλνουν multicast πακέτα νο πιστοποιηθούν.Αλλά και αν οι αποστολείς των πακέτων αυτών ήταν πρόθυμοι να πιστοποιηθούν,δεν υπάρχε έως σήμερα διαθέσιμη τεχνολογία για κάτι τέτοιο.

2.1.7.3.Διαμόρφωση του firewall

Για τους λόγους που περιγράψαμε παραπάνω, πρέπει να αντιμετωπίσουμε τηνMBone κίνηση ω δυνητικά επικίνδυνη. Εντούτοις, δεν μπορούμε να τη μπλοκάρουμεεξ'ολοκλήρου καθώς ο σκοπός μας είναι νο παρέχουμε πρόσβαση στο MBone. Συνεπώς,η στρατηγική μας πρέπει επικεντρωθεί στην ελάττωση τω κινδύνων που παρουσιάζει οχειρισμός MBone πακέτων, και όχι στην εξάλειψή τους (των κινδύνων). Η στρατηγικήεκφράζεται μέσα από τις ακόλουθες τρεις απαιτήσεις:

- Ελαχιστοποίηση της "άσκοπης" έκθεσης των hosts στην MBone κίνηση.
- Επιτρέπουμε την αποστολή Mbone πακέτων μόνο σε ασφαλείς ports.
- Ασκούμε έλεγχο ορθότητας σε όλες τις απόπειρες εισόδου MBone πακέτων στοδίκτυο, έτσ ώστε εάν υπάρξει παραβίαση, να λογοδοτήσουν οι υπεύθυνοι.

Προκειμένου να ελαχιστοποιηθεί η "άσκοπη" έκθεση, το firewall προωθεί έναεισερχόμενο MBone feed στο εσωτερικό δίκτυο, μόνο εάν αυτό έχει ζητηθεί **ρητά** απόέναν χρήστη. Το firewall τότε προωθεί τα πακέτ στον host που έκανε την αίτηση, **καιμόνον στον host αυτόν**, μέσω unicasting πλέον και όχι multicasting, κα μόνο για τηδιάρκεια της MBone εφαρμογής.



Εικόνα 12Το firewall προωθεί την εισερχόμενη MBone κίνηση χρησιμοποιώντας unicast addressing

Όπως φαίνεται και στην εικόνα 15, το firewall δέχεται datagrams από ένα MBone feed,διανεμημένου έσω της multicast διεύθυνσης 224.2.197.230, και τα προωθεί στους hostsA και D χρησιμοποιώντας τις unicast ους διευθύνσεις, 10.1.2.10 και 10.1.2.40αντίστοιχα. Επιπλέον, το firewall δέχεται αιτήσεις προώθησης MBone **όνο από hostsπου έχει καθορίσει ο firewall administrator**.

Για να εξασφαλιστεί η κατεύθυνση των MBone datagrams μόνο προς ασφαλείςports, το firewall τα ροωθεί μόνο σε ports που έχουν καθοριστεί εκ των προτέρων ως"μη χρησιμοποιούμενες", τόσο από τον ιτούντα host όσο και από το firewall kernel. Tofirewall θα προωθήσει το ίδιο εισερχόμενο multicast datagram ε διαφορετικές portsπροορισμού σε διαφορετικούς hosts.Πριν αρχίσει η προώθηση των πακέτων, το firewall έχεται ένα UserID από τοναιτούντα host, με στόχο την υπευθυνότητα των χρηστών. Το firewall μπορεί ιαπαιτήσει και επιπλέον αυθεντικοποίηση του χρήστη. Επίσης, καταγράφει τηνημερομηνία, το χρόνο, το νομα του χρήστη, και τέλος τους αριθμούς των ports και τις διευθύνσεις τόσο του feed όσο και του αιτούντα ost.

2.2Συστήματα Ανίχνευσης Επιθέσεων (I.D.S.)

Το Internet έχει γνωρίσει αλματώδη ανάπτυξη τα τελευταία χρόνια. Η ανάπτυξη αυτή αφορά τα διαφόρων ειδών σχετιζόμενα με αυτό συστήματα, τις ολένα και περισσότερες εφαρμογές που εμφανίζονται, τις διαθέσιμες δικτυακές υπηρεσίες κ.ο.κ. Όμως, αυτή η ανάπτυξη έχει και τα παρεπόμενά της. Έτσι, θα μπορούσαμε να πούμε ότι αντίστοιχα έχει αυξηθεί και το πλήθος των κακόβουλων χρηστών και των δικτυακών επιθέσεων, οι οποίες καθίστανται ολοένα και πιο σύνθετες και επιβλαβείς, . Ως επακόλουθο, τα ως σήμερα διαδεδομένα μέτρα ασφάλειας δεν μπορούν να παράσχουν επαρκή προστασία στα συστήματα και τις πληροφορίες του μέσου χρήστη. Απαιτείται, λοιπόν, αναβαθμισμένο επίπεδο ασφάλειας και προστασίας έναντι των δικτυακών επιθέσεων. Στην κατεύθυνση ανάπτυξης νέων μηχανισμών ασφαλείας, στρέφεται μεγάλο μέρος της προσπάθειας που καταβάλονται. Η αυτοματοποιημένη μέθοδος προστασίας αποτελεί μια σχετικά νέα τέτοια προσπάθεια, η οποία εξελίσσεται.

Ο όρος ***IntrusionDetection(Ανίχνευση Εισβολής)χρησιμοποιείται για να περιγράψει την παρακολούθηση και ανάλυση των τεκταινομένων σε ένα σύστημα ή δίκτυο για την ανίσχευση σημαδιών που υποδεικνύουν επιθέσεις.***.Ο όρος ***Εισβολή χρησιμοποιείται για να περιγραφούν οι απόπειρες παραβίασης*** της *εμπιστευτικότητας, ακεραιότητας, διαθεσιμότητας* ή *των μηχανισμών ασφάλειας* ενός συστήματος ή ενός δικτύου.Οι Εισβολής πραγματοποιούνται από άτομα που μπορούν να αποκτήσουν πρόσβαση στους στόχους μέσω διαδικτύου, εξουσιοδοτημένοους χρήστες που αποπειρώνται να αποκτήσουν περισσότερα από τα ως τότε δικαιώματα, καθώς και από κακόβουλη εκμετάλλευση δικαιωμάτων από εξουσιοδοτημένους χρήστες.

Ο όρος **IntrusionDetectionSystems(IDSs)** ***(Συστήματα Ανίχνευσης Εισβολής) χρησιμοποιείται για να περιγράψει προϊόντα***software ή hardware, τα οποία αυτοματοποιούν την διαδικασία που περιγράφηκε προηγμουμένως..Τα προϊόντα αυτά γνωρίζουν αλματώδη ανάπτυξη τα τελευταία χρόνια και καταβάλλονται διαρκώς προσπάθειες για να βελτιστοποιηθεί η απόδοσή τους, με επίκεντρο τα *FalsePositives*και *FalseNegatives*που δίνουν ως αποτελέσματα.Στην παρούσα φάση, τα προϊόντα αυτά δύνανται να υποστηρίξουν σημαντικά τα μέτρα προστασίας ενός δικτύου και σε συνέργεια με διάφορους μηχανισμούς ασφαλείας καθίστανται αποτελεσματικά εργαλεία εντοπισμού και αντιμετώπισης δικτυακών επιθέσεων.

FalsePositives:Εσφαλμένες επισημάνσεις που προκύπτουν από την ανίχνευση ενός συμβάντος και επισήμανσή του ως περίπτωση πιθανής επίθεσης, χωρίς κάτι τέτοιο να ισχύει . Μπορεί να είναι αποτέλεσμα εσφαλμένης ρύθμισης του IDS ή μη σαφώς διακρινόμενα από πραγματική επίθεση.

FalseNegatives: Μη επισημασμένες επιθέσεις. Μπορεί να είναι αποτέλεσμα εσφαλμένης ρύθμισης του IDS ή πρωτοεμφανιζόμενης επίθεσης, περί της οποίας στερούμαστε πρότερηςγνώσης.

Χρησιμότητα των IDSs: Με δεδομένη τη μεγέθυνση της κλίμακας (τόσο ως προς τον αριθμό όσο και ως προς την επικινδυνότητα) των δικτυακών επιθέσεων, τα IDSs έχουν πλέον καταστεί ουσιώδες μέρος της πολιτικής ασφάλειας οποιουδήποτε οργανισμού.

Με την *Ανίχνευση Εισβολής καθίσταται εφικτή η προστασία των συστημάτων και των πληροφοριών ενός οργανισμού, από τις αρνητικές και ενδεχομένως επιβλαβείς συνέπειες που επιφέρει η* επιτρέπει στους οργανισμούς να προστατέψουν τα συστήματά τους και τις πληροφορίες που βρίσκονται σε αυτά, από κινδύνους

:ου προκύπτουν από την αυξημένη δικτυακή διασύνδεση μεταξύ των συστημάτων τους. Πιο συγκεκριμένα, η :ρήση IDSs έχει σήμερα καταστεί σχεδόν αναγκαία, μεταξύ άλλων, για τα εξής:

1.Δύνανται να ανιχνέυσουν εισβολές και άλλου είδους παραβιάσεις ασφάλειας, οι οποίες είναι μη ντοπίσιμες από άλλα προϊόντα.. Πολλές φορές, ο εισβολέας έχει τη δυνατότητα πρόσβασης σε ένα ή :ερισσότερα συστήματα, καθώς δεν έχουν επιλυθεί και αντιμετωπιστεί διάφορα, δημοσίως γνωστά, υπρόσβλητα σημεία στην ασφάλεια τους. Μολονότι δεν είναι ιδιαίτερα δύσκολή η επίλυση αντίστοιχων :ροβλημάτων από τον εκάστοτε διαχειριστή, συχνά κάτι τέτοιο δε γίνεται, για πολλούς λόγους, όπως οι κάτωθι: :ίναι σύνηθες κάποιος που διαχειρίζεται πολλά συστήματα σε ένα περιβάλλον να μην μπορεί (είτε λόγω υνατοτήτων είτε λόγω φόρτου εργασίας) να ενημερώνει και να διορθώνει τις ρυθμίσεις των μηχανισμών σφαλείας.

Συχνά χρησιμοποιούνται λογισμικά που δυνητικά καθιστούν τρωτή την ασφάλεια ενός συστήματος

Ένας ακόμα παράγοντας είναι λάθη στα οποία υποπίπτουν είτε οι διαχειριστές είτε οι χρήστες σε ότι φορά τη χρήση και τις ρυθμίσεις συστημάτων και υπηρεσιών.

Μηχανισμοί πρόσβασης στα συστήματα (π.χ. passwords) με χαμηλό δείκτη ασφάλειας .

Η ελαχιστοποίηση των δομικών αδυναμιών στην ασφάλεια των προϊόντων και η ταχύτατη και ξιόπιστη διόρθωση και ενημέρωση των συστημάτων είναι η ευκταία εικόνα, που όμως σπάνια απαντάται σε υνήθεις συνθήκες, πολλώ δε μάλλον εφόσον αναφύονται ολοένα και περισσότερα καινοφανείς αδυναμίες και λαττώματα στην ασφάλεια συστημάτων.

Η απόπειρα (επιτυχης ή όχι) κάποιου να εισβάλει σε ένα σύστημα αξιοποιώντας κάποιο εκ των ροτέρων εντοπισμένο ελάττωμα στην ασφάλειά του ανιχνεύεται με την χρήση ενός IDS. Ακόμα, αυτό υντελεί στην επισήμανση του σφάλματος στο μηχανισμό ασφάλειας που κατέστησε δυνατή την παραβίαση ου συστήματος, κάτι που συμβάλλει στην αποκατάσταση και επιδιόρθωσή του.

2. Ανιχνεύονται αναγνωριστικές ενέργειες που αποτελούν προπομπούς μίας επίθεσης. Προτού συμβεί ια επίθεση, ο πιθανός στόχος γίνεται αντικείμενο διερεύνησης, ώστε να εντοπιστούν πιθανά σημεία εισόδου scanning). Εάν δεν χρησιμοποιείται κάποιο IDS, τέτοιες διαδικασίες που αποτελούν προπομπούς μιας πόπειρας εισβολής ίσως να μην εντοπιστούν έγκαιρα. Αυτό κάνει ένα IDS, καθορίζοντας έτσι και μια σειρά λλων βημάτων: καταγράφει το συμβάν, ενημερώνει τον εκάστοτε αρμόδιο, παρακωλύει την εισβολή κ.ο.κ.

3. Η επιτυχής αποκατάσταση ενός προσβεβλημένου συστήματος και οι επιδιορθώσεις στην ασφάλειά ου άπαιτούν την σωστή πληροφόρηση του διαχειριστή. Μολονότι είναι πιθανό ένα IDS να μην κατορθώσει να αρακωλύσει μια απόπειρα εισβολής, δύναται να συγκεντρώσει αξιοποιήσιμα προς τους παραπάνω σκοπούς τοιχεία, καθώς και άλλα που μπορεί να οδηγήσουν τον αποπειρώμενο την εισβολή ενώπιον της δικαιοσύνης.**4.** εξακρίβωση των στοιχείων ενός εισβολέα επισύρει ποινικές ευθύνες. Αντιλαμβανόμενος ο επίδοξος σβολέας την παρουσία ενός IDS, συνειδητοποιεί ότι ο κίνδυνος για τον ίδιο αυξάνεται κι έτσι μπορεί να μην ροχωρήσει στην ολοκλήρωση της επίθεσης.

5. Η χρησιμοποίηση ενός IDS συμβάλει στην απόκτηση πληροφόρησης και εντοπισμό προτύπων patterns) σε επαναλαμβανόμενες διεργασίες έναντι ενός δικτύου και των συστημάτων του. Με αυτό τον τρόπο ι IDS συμβάλλουν στο σχεδιασμό μέτρων ασφαλείας μεγαλύτερης αξιοπιστίας, με καλύτερη προσαρμογή στις παιτήσεις που απορρέουν από τον τρόπο λειτουργίας και χρήσης του εκάστοτε συγκεκριμένου δικτύου, ελτιώνοντας έτσι την προστασία του.

Με τον όρο **patterns**, εννοούμε τα προκύπτοντα δείγματα από ένα σύνολο δραστηριοτήτων οι οποίε γίνονται αντικείμενο μελέτης και καταγραφής και παρουσιάζονται ως πρότυπα εκφράζοντα τη συνολική δραστηριότητα..

2.2.1 Είδη IDSs

Η ποικιλότητα των σημερινών IDS χαρακτηρίζεται από πλήθος διαφορετικών τρόπων με τους οποίου πραγματοποιείται η διαδικασία παρακολούθησης και ανάλυσης γεγονότων, ώστε να ανιχνεύονται πιθανέ εισβολές. Τα διάφορα IDS μπορούν να κατηγοριοποιηθούν στη βάση διαφόρων παραγόντων, οι οποίο προκύπτουν από ένα γενικό μοντέλο περιγραφής του τρόπου λειτουργίας τους. Τρεις λειτουργίες είνα θεμελιώδεις για την πλειονότητά τους και με βάση το πώς αυτές πραγματοποιούνται, διαχωρίζονται τα διάφορ IDS.

ΠηγέςΠληροφορίας (*InformationSources*)

Είναι οι πηγές που χρησιμοποιεί το IDS για τη συλλογή των κατάλληλων πληροφοριών, οι οποίες στη συνέχεια γίνονται αντικείμενο ανάλυσης, ώστε να καθοριστεί αν έχει συμβεί κάποια επίθεση. Συχνότερα, αυτέ είναι σε επίπεδο παρακολούθησης *συστήματος(Host)* και *δικτύου (Network)*.

Ανάλυση (*Analysis*)

Ο τρόπος με τον οποίο το IDS οργανώνει και επεξεργάζεται τα ληφθέντα από τις *Πηγές Πληροφορίας* στοιχεία, ώστε να αποφανθεί για το αν κάποια αποτελούν επίθεση και ποια είναι αυτά.Συνήθεις μέθοδοι η *MisuseDetection*, η *AnomalyDetection*και η*ProtocolAnomalyDetection*.

Απόκριση (*Response*)

Είναι το σύνολο των ενεργειών που εκτελούνται από το IDS, μετά την ανίχνευση κάποιαςεπίθεσης.Διακρίνονται σε*Παθητικές (Passive)* και *Ενεργητικές (Active)*.Οι πρώτες, συνήθως περιορίζονται στην καταγραφή του συμβάντος και την ενημέρωση των αρμοδίων για τη λήψη των απαραίτητων μέτρων.Οι δεύτερες αφορούν την αυτοματοποιημένη διαδικασία αντιμετώπισης μιας επίθεσης από το IDS.

Στα επόμενα μέρη της εργασίας αναλύουμε διεξοδικότερα τις λειτουργίες αυτές και παρουσιάζουμε τα διάφορα είδη των IDSs, διαχωρίζοντάς τα βάσει αυτών.

2.2.1.1. InformationSources(ΠηγέςΠληροφορίας)

Συχνότερα τα IDS διαχωρίζονται βάσει των χρησιμοποιούμενων πηγών πληροφορίας, εκ των οποίων απορρέουν όσα αναλύονται στη συνέχεια, για να ανιχθευθεί τελικά κάποια επίθεση.

Υπάρχουν IDSs τα οποίαπαρακολουθούν και αναλύουν πακέτα πουανήκουν στο traffic ενός δικτύου, το οποίο μπορεί να είναι ένα δίκτυο κορμού (Backbone) ή ένα τμήμα (segment) ενός τοπικού δικτύου (LAN), ώστε να εντοπίσουν επιθέσεις. Άλλα, παρακολουθούν και αναλύουν πληροφορία που εξάγεται από το Λειτουργικό Σύστημα ή από τις εφαρμογές ενός συστήματος. Ανάλογα με την πηγή της πληροφορίας, τα IDS διακρίνονται σε δύο κατηγορίες, καθεμία εκ των οποίων έχει τα δικά της προτερήματα:

2.2.1.2. NetworkIDSs (NIDS)

Είναι τα πιο συχνά IDS που συναντάμε.Τα NIDSs παρακολουθούν και αναλύουν κάθε πακέτο που ανήκει στο traffic ενός δικτύου.Ένα NIDS εγκατεστημένο σε ένα segment ή ένα switch ενός δικτύου, επεξεργάζεται κάθε πακέτο που περνάει από εκεί, προστατεύοντας κάθε σύστημα που είναι συνδεδεμένο στο δίκτυο. Τα NIDS συνήθως απαρτίζονται από συστήματα (*Sensors*),τοποθετημένα σε διάφορα σημεία ενός δικτύου. Ο *Sensor*εκτελεί όλες τις λειτουργίες του NIDS και είναι ένα σύστημα επικεντρωμένο αποκλειστικά σε αυτές. Οι *Sensors*παρακολουθούν το traffic του δικτύου, αναλύουν τοπικά τα πακέτα σε πραγματικό χρόνο και καταγράφουν τα αποτελέσματά τους τοπικά ή/και απομακρυσμένα σε ένα κεντρικό σύστημα. Επίσης,*έ*χουν κανότητα απόκρυψης της παρουσίαςτους (StealthMode),γεγονός που εμποδίζει τον εντοπισμός τους από τον επιτιθέμενο.

Πλεονεκτήματα των NIDS

Αρκεί ένας μικρός αριθμός*Sensors*για την προστασία ενόςπολύ μεγάλου δικτύου.

Η υλοποίηση και η εφαρμογή ενός NIDS δεν επηρεάζει σχεδόν καθόλου τη λειτουργία του δικτύου. Οι *Sensors*στους οποίους εκτελούνται οι λειτουργίες του NIDS, είναι συνήθως

παθητικές συσκευές που περιορίζονται στην παρακολούθηση και επεξεργασία του traffic του δικτύου, έχως παρέμβαση στηνκανονική λειτουργία του. Μπορεί, λοιπόν, κάποιος εύκολα να προσθέσει ένα *Sensor*σε να δίκτυο.

Έχουν αρκετά μεγάλο βαθμό ασφάλειας απέναντι σε επιθέσεις εναντίον τους, λόγω της δυνατότητας πόκρυψης της παρουσίας τους.

Μειονεκτήματα των NIDS

Σε δίκτυα με όπου υπάρχει πολύ μεγάλο traffic, τα NIDS συχνά εμφανίζουν προβλήματα, καθώς δεν χουν επαρκείς πόρους για την ανάλυση όλων των πακέτων. Ως αποτέλεσμα, παραλείπουν κάποια εξ αυτών ατά την επεξεργασία, με δυνητική συνέπεια τηναποτυχία αναγνώρισης μίας επίθεσης.Καταβάλλονται ροσπάθειες για την παραγωγήNIDSs με τη μορφή Hardware. Κατ' αυτό τον τρόπο θα γίνουν ταχύτερα και θα χουν μεγαλύτερη αντοχή, όμως θα έχουν υψηλότερο κόστος και μικρότερη ευελιξία.

Τα NIDS αδυνατούν να επεξεργαστούνπληροφορία σε κρυπτογραφημένη μορφή, όπως στα 'irtualPrivateNetworks(VPNs) .Τα περισσότερα NIDS δεν μπορούν να καθορίσουν αν μία επίθεση ήταν

επιτυχής. Περιορίζονται στην επισήμανση του συμβάντος και των στόχων. Για την επιτυχία ή αποτυχία της επίθεσης πρέπει να αποφανθεί ο εκάστοτε υπεύθυνος για το σύστημα.

2.2.1.3. HostIDSs (HIDS)

Η συλλογή της πληροφορίας γίνεται μόνο από ένα, προστατευόμενο από αυτά, σύστημα. Έτσι μπορούν να δώσουν αναλυτικές πληροφορίες για τις διαδικασίες (processes) και τουςχρήστες που έλαβαν μέρος στην συγκεκριμένη επίθεση στο σύστημα που προστατεύουν.Κατά μείζονα λόγο ελέγχουν τα αρχεία καταγραφής του συστήματος. Λόγω του ότι μπορούν άμεσα να παρακολουθήσουν τα αρχεία και τις διαδικασίες του συστήματος που συχνά αποτελούν στόχο επίθεσης, μπορούν να ελέγξουν το αποτέλεσμα αυτής. ΥπάρχουνHIDSs που επιτρέπουν τη χρήση κοινής κονσόλας διαχείρισης και ελέγχου πολλών συστημάτων. απλοποιώντας κατ' αυτό τον τρόπο την χρήση τους.

Πλεονεκτήματα των HIDSs

Λόγω τοπικότητας στη λειτουργία τους εντός του προστατευόμενου συστήματος, μπορούν να ανιχνεύουν μη ανιχνεύσιμες από τα NIDS επιθέσεις.

Λόγω του ότι εξετάζουν την πληροφορία προτού κρυπτογραφηθεί από το σύστημα αποστολέα και αφού αποκρυπτογραφηθεί από το σύστημα παραλήπτη, είναι αξιοποιήσιμα σε περιβάλλοντα με κρυπτογραφημένη επικοινωνία μεταξύ συστημάτων (VPNs).

Μειονεκτήματα των HIDS

Δεν είναι εύκολα διαχειρίσιμα, λόγω του ότι απαιτείτια ιδιαίτερη ρυθμιση του κάθε παρακολουθούμενου συστήματος

Λόγω της τοπικής υλοποίησής τους στο προστατευόμενο σύστημα, είναι επιρρεπή σε επιθέσεις, καθώς σε ενδεχόμενη παραβίαση αυτού, ο επιτιθέμενος μπορεί να τα απενεργοποιήσει

Δεν δύνανται να ανιχνεύσουν ενέργειες αναγνωριστικού χαρακτήρα που προηγούνται μιας επιθεσης, λ.χ. scans που πραγματοποιεί σε ολόκληρο το δίκτυο.

Είναι επιρρεπή σε κάποιες DenialOfService (DoS) επιθέσεις, λόγω των οποίων μπορεί να διακοπεί η λειτουργία τους.

Έχουν αρνητική επίδραση στην απόδοση του προστατευόμενου συστήματος , λόγω του ότι εκτελούν τις λειτουργίες τους αξιοποιώντας δικούς του πόρους.

2.2.2. Τεχνικές Ανάλυσης (Analysis)

Οι συνηθέστερες μέθοδοι που χρησιμοποιούνται για να αναλύσουμε τα δεδομένα που θα μας βοηθήσουν να ανιχνεύσουμε απόπειρες εισβολής είναι τρεις:.

Α) *MisuseDetection: πρόκειται για τη συνηθέστερη μέθοδο, η οποία συνίσταται στον εντοπισμό «ύποπτων» συμβάντων, τα οποία έχουν παρατηρηθεί σε προηγούμενες απόπειρες επίθεσης .*

Β)*AnomalyDetection: συνίσταται στον εντοπισμό* patternsδραστηριότητας, τα οποία δεν θα έπρεπε υπό φυσιολογικές συνθήκες να εντοπίζονται. Πρόκειται για αναπτυσσόμενη ερευνητικά τεχνική. που δεν θεωρούνται φυσιολογικά και η οποία βρίσκεται σε ερευνητικό στάδιο μέχρι σήμερα.

Γ)*ProtocolAnomalyDetection: συνιστά διαφοροποιημένη εκδοχήτης AnomalyDetection,στην οποία* λέγχεται *η* λανθασμένη, μη φυσιολογική χρήση των πρωτοκόλλων επικοινωνίας.Δεν είναι πολλές οι τεριπτώσεις IDSs που αρκούνται στην εφαρμογή αποκλειστικά της μεθόδου*AnomalyDetection*.

Για κάθε μια εξ αυτών των μεθόδων μπορούμε να εντοπίσουμε ιδιαίτερα προτερήματα και αδυναμίες. Η βέλτιστη αποτελεσματικότητα προκύπτει στη βάση της μεθόδου *MisuseDetection, σε συνδυασμό με* ιποτελέσματα του *ProtocolAnomalyDetection*και κάποια «έξυπνα» στοιχεία του *AnomalyDetection*.

2.2.2.1. MisuseDetection

Αφορά την απόπειρα εντοπισμού συμβάντων που ανταποκρίνονται σε προκαθορισμένα πρότυπα εγονότων, τα οποία έχουν επανεμφανιστεί σε προηγούμενες επιθέσεις, μέσα από την παρακολούθηση της ραστηριότητας του δικτύου. Τα πρότυπα αυτά είναι γνωστά ως*Signatures*(υπογραφές), εξ ου και η νομασία*Signature-baseddetection*.

Σε κάποιο *signature*μπορεί να αποτυπώνονται κάποια χαρακτηριστικά ενός πακέτου, π.χ η εμφάνιση tadata του κάποιου συγκεκριμένου λεκτικού που χρησιμοποιείται σε επίθεση. Συχνά, κάθε επίθεση φέρει και ιαφορετικό*signature*, όμως σε εναλλακτικές παραλλαγέςένα signature αφορά σε ένα σύνολο επιθέσεων *Statebaseddetection)*.

Πλεονεκτήματα

Εντοπισμός επιθέσεων με περιορισμό του πλήθους των FalsePositivesΗ τεχνική του *AisuseDetection*έχει την ικανότητα να ανιχνεύει επιθέσεις χωρίς να παράγει πολύ μεγάλο αριθμό από alsePositives.

Μεγάλη ταχύτητα και ικανοποιητική ακρίβεια στην εξακρίβωση των εργαλείων που αξιοποιήθηκαν ατά την επίθεση.

Μειονεκτήματα

Η εμβέλειά της περιορίζεται μόνο σε εκ των προτέρων γνωστές επιθέσεις, με αποτέλεσμα να απαιτείται υχνή επικαιροποίηση των *signatures*.

Λόγω του ότι η αποτελεσματικότητά της δεσμεύεται από τα αξιοποιούμενα signatures, όσα IDS ρησιμοποιούν signatures που αντιστοιχούν αποκλειστικά σε μια επίθεση δεν μπορούν να εντοπίσουν ροποποιημένες εκδοχές τους. Εν πολλοίς, η *state-based*μέθοδος υπερβαίνει αυτό το μειονέκτημα.

2.2.2.2. AnomalyDetection

Αφορά την προσπάθεια ανίχνευσης μη συνήθους και ομαλής συμπεριφοράς σε κάποιο σύστημα ή ίκτυο.Βασίζεται στη θεώρηση ότι η δραστηριότητα που προκαλείται από την εκδήλωση μιας επίθεσης οκλίνει από τη συνήθη, ως εκ τούτου η ανίχνευση τέτοιων αποκλίσεων σηματοδοτεί την επίθεση.

Σε πρώτη φάση, διαμορφώνονται πρότυπα (patterns) τα οποία αντιστοιχούν στη συνήθη συμπεριφορά ων χρηστών ή των συστημάτων ή του traffic ενός δικτύου, τα οποία προκύτουν απόδεδομένα που ερισυλλέγονται σε φάση ομαλής λειτουργίας και αποτελούν δείγμα στάθμισης της ομαλήςδραστηριότητας. Ιρόκειται για το πιο δύσκολο μέρος αυτής της μεθόδου, καθώς οι μεγάλες διακυμάνσεις κατά τη ειτουργίαενός δικτύου ή ενός συστήματος είναι δύσκολο να προτυποποιηθει. Σε δεύτερη φάση, τα διάφορα

συμβάντα προσφέρουν δεδομένα, τα οποία αναλύονται με ποικίλους τρόπους για να εντοπιστούν παρεκκλίσει από τα πρότυπα.. Υπάρχουν διάφορες τεχνικές που εφαρμόζονται για την διαμόρφωση των προτύπων και την αντιπαραβολή τους με τα διάφορα συμβάντα, όπως:

2.2.2.2.1. ThresholdDetection

Απαριθμώνται στοιχεία ενδεικτικάτης συμπεριφοράς του χρήστη και του συστήματος, το οποίων τ πλήθος αντιπαραβάλλεται με το καθοριζόμενο ως μέγιστο αποδεκτό όριο. Για παράδειγμα, τέτοια είναι αριθμός των προσβάσιμων σε ένα χρήστη αρχείων, εντός κάποιου διαστήματος, ή ο αριθμός των μη επιτυχών απόπειρων login σε ένα σύστημα, το ποσοστό της CPU που κάνει χρήση ένα process κ.α.Το μέγιστο αποδεκτ όριο μπορεί να ορίζεται είτε σε κάποια σταθερή τιμή, είτε να είναι δυναμικά τροποποιούμενο, προσαρμοζόμεν στις παρατηρούμενες στη διάρκεια του χρόνου τιμές, οι οποίες εκλαμβάνονται ως μη αποκλίνουσες από την ομαλή συμπεριφορά.

2.2.2.2.2. Στατιστικές Μέθοδοι

Στις *παραμετρικές μεθόδους*, η ομαλή και συνήθη δραστηριότητα δίνεται ποσοστιαία, στη βάσ δεδομένων προτύπων. Στις *μη-παραμετρικές, από την άλλη, τα αντίστοιχα ποσοστά διαμορφώνονται δυναμικά βάση της χρονικής εξέλιξης των παρατηρησιακών δεδομένων.*

2.2.2.2.3. RuleBased

Προσομοιάζει στην*Μη-Παραμετρική Στατιστική* μέθοδο, καθότι τα πρότυπα δραστηριότητα διαμορφώνονται στη βάση της χρονικής εξέλιξης των παρατηρησιακών δεδομένων, αλλά διαφοροποιείται απ αυτή λόγω του ότι τα πρότυπα αποδίδονται με κανόνες (rules) κι όχι νουμερικά. με την έννοια ότι τα pattern της φυσιολογικής δραστηριότητας, δημιουργούνται από δεδομένα που παρατηρούνται με το πέρασμα το χρόνου, αλλά διαφέρει στο ότι αυτά τα patterns δεν εκφράζονται με αριθμητικές ποσότητες αλλά με κάποιου κανόνες (rules).

2.2.2.2.4. Άλλες Μέθοδοι

Αποτελούν εφαρμογές*νευρωνικών δικτύων* και *γενετικών αλγορίθμων*.Στα συστήματα όπο εφαρμόζονται τέτοιες μέθοδοι, τα patterns κανονικής συμπεριφοράς διαμορφώνονται στη βάση ενό ευμεγέθους πλήθους δεδομένων, κανόνων και σχέσεων μεταξύ πληροφοριών.

Σοβαρό μειονέκτημα της εφορμογής του *AnomalyDetection αποτελεί ο σημαντικός αριθμό* FalsePositives και FalseNegatives που δίνουν. Αυτό οφείλεται στο ότι τα patterns κανονικής συμπεριφορά μπορεί να εμφανίζονται διάφορες τροποποιήσεις.Από την άλλη, η μέθοδος αυτή επιτυγχάνει στον αντοπισμό καινοφανών επιθέσεως, ενώ και οι εκροές της εφαρμογής τους τροφοδοτούν με δεδομένα IDSs στα οποί εφαρμόζεται η*MisuseDetection*.Δεν είναι πολλά τα IDSs τα οποία εφαρμόζουν αποκλειστικά*AnomalyDetection,* ενώ και αυτήπροορίζεται κατά μείζοντα λόγο για Network και Portscans.Τ *AnomalyDetection είναι ένα πολλά υποσχόμενο εργαλείο, το οποίο σήμερα* αποτελεί ερευνητικό αντικείμενο.

Πλεονεκτήματα

Λόγω του ότι βασίζεται στον εντοπισμό αποκκλίσουσας από την κανονική δραστηριότητας, έχει την ικανότητανα ανιχνεύει μια επίθεση ακόμα κι αν δεν υπάρχει γνώση των χαρακτηριστικών της.

Έχει την ικανότητανα ανίχνευσης επιθεσων, ακόμα και σε περιπτώσεις που δεν αν δεν υπάρχει πρότερη ;μπειρία από αυτές.

Τα εξαγόμενά της μπορούν να αξιοποιηθούν σαν είσοδοι σε IDSs όπου εφαρμόζεται*MisuseDetection*.

Μειονεκτήματα

Σημαντικός αριθμόςFalsePositives και FalseNegatives,λόγω του ότι η μη προβλέψιμη συμπεριφορά ;ρηστών και δικτύων δυσχαιρένει τη διαμόρφωση σωστών προτύπων.

Η διαμόρφωση προτύπων συνήθους και ομαλής συμπεριφοράς, απαιτεί

εκτεταμένα εκπαιδευτικά σύνολα τα οποία θα αξιοποιηθούνως παράδειγμα.

2.2.2.2.5. ProtocolAnomalyDetection

Πρόκειται για πρόσφατα εισηγμένη μέθοδο, η οποία αποτελεί τροποποίηση της *AnomalyDetection*, που ιαφοροποιείται κατά το ότι εστιάζει στον έλεγχο ορθής χρήσης πρωτοκόλλων επικοινωνίας (ιδίως όσων υγκαταλέγονται στην οικογένεια του TCP/IP). Τα πρωτόκολλα επικοινωνίας είναι σύνολα κανόνων και ;ρχών, εκ των οποίων καθορίζεται ο τρόπος επικοινωνίας μεταξύ δύο διασυνδεδεμένων συστημάτων. ;ημαντικό μέρος των διαδικτυακών επιθέσεων πραγματοποιείται με μη φυσιολογική χρήση των πρωτοκόλλών πικοινωνίας. Ο προβλεπόμενος τρόπος χρήσης τους ορίζεται σε επίσημα, ευρέως αποδεκτά έγγραφα τα RFCs RequestForComments). Σε αυτά προσδιορίζονται τα standards, που κάθε πρωτόκολλο πρέπει να ακολουθεί ;ατά την υλοποίησή του.

Οι επιθέσεις που στηρίζονται στην μη φυσιολογική χρήση των πρωτοκόλλων, αξιοποιούν παραλείψεις την πρόβλεψη τέτοιων δράσεων από τα RFCs ή στη λανθασμένη εφαρμογή των περιγραφόμενων σε αυτά ανόνων και αρχών από τους δημιουργούς λειτουργικών συστημάτων και λογισμικών.

Σε αυτή τη μέθοδο έχουμε εποπτεία και επεξεργασία της σχετικής με την εφαρμογή των πρωτοκόλλων ραστηριότητας, καθώς και έλεγχο για τυχόν ασυμφωνία με τα patterns που προσδιορίζουν την ορθή εφαρμογή υτών. Πλεονεκτεί έναντι της *AnomalyDetection,* σε ότι αφορά τη διαμόρφωσηpatterns, καθότι εδώ αφορούν ους προκαθορισμένους κανόνες που περιγράφονται από τα RFCs και όχι από κανόνες που περιγράφουν τις υνήθεις, ομαλές διεργασίες που λαμβάνουν χώρα σε ένα δίκτυο ή σύστημα, οι οποίες χαρακτηρίζονται από λλειψη σταθερότητας και ευμεταβλητότητα.

Πλεονεκτήματα

- Είναι εφικτή η ανίχνευση αποκλίνουσας από τα συνήθη δραστηριότητας που σχετίζεται με τη χρήση κάποιου πρωτοκόλλου και ως εκ τούτου εντοπίζει επιθέσεις χωρίς να προϋποτίθεται η γνώσηλεπτομερειών για αυτή.
- Είναι εφικτός ο εντοπισμός καινοφανών επιθέσεων.
- Οι εξ αυτής προκύπτουσες πληροφορίες μπορούν δυνητικά να αξιοποιηθούν σε σε IDSs που εφαρμόζουν *MisuseDetection*.

Μειονεκτήματα

- Δεν είναι πάντα εφικτό να ακολουθούνται οι κανόνες που προσδιορίζονται από τα RFC από τα patterns που διαμορφώνονται, καθώς και από τα λειτουργικά συστήματα καιτα άλλα λογισμικά

που κάνουν χρήση των πρωτοκόλλων. Έτσι, χρειάζεται να υπάρχει σχετική πρόβλεψη κατά τη διαμόρφωση τωνpatterns.

- Είναι αδύνατη η ανίχνευση επίθεσης που δε σχετίζεται μεμη φυσιολογική χρήση των πρωτοκόλλων.

Συνήθως, ο εντοπισμός μιας επίθεσης δε συνοδεύεται από στοιχεία που περιγράφουν με πληρότητα το είδος της. Ως εκ τούτου απαιτείται εξειδικευμένο προσωπικό για να συνάγει τα απαιτούμενα συμπεράσματα.

2.2.3. Responses

Η επεξεργασία των ληφθέντων δεδομένων ακολουθείται από την κοινοποίηση των εξ αυτής πορισμάτων και την αναφορά συμβάντων που σηματοδοτούν ενδεχόμενες απόπειρες εισβολής ή και ενέργειες απόκρουσής τους. Η τέτοια δράση των IDSs έχει μεγάλη αξία, καθότι σε αυτή εδράζει η ταχεία και αποδοτική οργάνωση των μέτρων προσταστίας.Τα διάφορα είδηResponses, διακρίνονται σε *ActiveResponses*, *PassiveResponses και MixedResponses*. (αποτελούν συγκερασμό στοιχείων των άλλων δυο και ως εκ τούτου δε θα επεκταθούμε σχετικά) .

2.2.3.1. ActiveResponses

Προκειται για αυτοματοποιημένες ενέργειες που εκτελούνται από το IDS, μετά τον εντοπισμό επιθέσεων συγκεκριμένου είδους. Διακρίνονται σε:

2.2.3.1.1. Συλλογή επιπρόσθετων πληροφοριών

Πρόκειται για τη μικρότερου βαθμού ενεργητικότητας αντίδραση, που όμως ενίοτε είναι η πιο παραγωγική. Συλλέγονται δεδομένα για ενδεχόμενα εντοπισμένη επίθεση, τα οποία θα συναξιολογηθούν για να κριθεί αν χρειάζεται ή όχι ενίσχυση των μέτρων προστασίας. Όταν ενά IDS ανιχνεύση ενδεχόμενη εισβολή δύναται να αναβαθμίση το το επίπεδο ευαισθησίας των χρησιμοποιούμενων *InformationSources*(πχ. να ρυθμίσει κάποιον*Sensor*να καταγράφει όλα τα πακέτα ενός δικτύου και όχι αυτά που αφορούν συγκεκριμένασυστήματα ή πόρτες). Μετά από αυτό, καθίσταται εφικτό να ολοκληρωθεί η καταγραφή στοιχείων για μία πιθανή επίθεση, τα οποία αξιοποιούνται για να μην εξάγονται εσφαλμένα συμπεράσματα, όσο και στην αναγνώριση του επιτιθέμενου και την επιβολή των σχετικών ποινικών κυρώσεων.

2.2.3.1.2. Παρεμπόδιση του επιτιθέμενου.

Μια πιο ενεργητική διεργασία αφορά την παρεμπόδιση της επίθεσης όταν αυτή βρίσκεται σε εξέλιξη ή την αποτροπή της πρόσβασης του επιτιθέμενου και σε άλλα σημεία του προστατευόμενου συστήματος ή δικτύου. Αυτό που συμβαίνει είναι ότι το IDS εμποδίζει πακέτα που έχουν IP διεύθυνση, απ᾽όπου φαίνεται να προέρχεται ο επιτιθέμενος και όχι αυτόν. Συχνά δεν έχει τα προσδωκόμενα αποτελέσματα, λόγω του ότι οι πιο πεπειραμένοι επιτιθέμενοι αξιοποιούνψεύτικες IPδιευθύνσεις. Παρόλο που, τέτοιες δράσεις μπορεί να παρακωλύουν λιγότερο πεπειραμένους ή και να προβληματίσουν τους εμπειρότερους. Τέτοιες ενέργειες περιλαμβάνουν :

Να σταλούν πακέτα (με ενεργοποιημένο το RSTflag στον TCPheader) τα οποία θατερματίσουν οποιαδήποτε σύνδεση του επιτιθέμενου με το σύστημα – στόχο.

Να ρυθμιστούν οι δρομολογητής και τα firewall του δικτύου, ώστε να μην επιτρέπουν την διέλευση οποιουδήποτε πακέτου, το οποίο έχει διεύθυνση αποστολέα ή παραλήπτη, την IP διεύθυνση την οποία χρησιμοποιεί ο επιτιθέμενος στα πακέτα που στέλνει.

Να ρυθμιστούν οι δρομολογητής και τα firewall του δικτύου, ώστε να μην είναι δυνατή πρόσβασησε τόρτες υπηρεσίες και πρωτόκολλα που κάνει χρήση ο επιτιθέμενος.

2.2.3.1.3. Δράση εναντίον του επιτιθέμενου.

Υπάρχουν πολλές σκέψεις για το αν είναι σωστό κατά την ανίχνευση μίας επίθεσης να παρθούν μέτρα του συμπεριλαμβάνουν την δράση εναντίον του επιτιθέμενου. Στην πιο ακραία μορφή της αυτή η δράση θα μπορούσε να είναι η υλοποίηση επίθεσης με στόχο τον επιτιθέμενο ή η συλλογή πληροφοριών για το δίκτυό του.Παρόλο που αυτή η αντιμετώπιση μοιάζει αρκετά αποτελεσματική και δίκαιη, κρύβει πολλούς κινδύνους. Κατά πρώτο λόγο αυτού του είδους η δράση μπορεί να είναι παράνομη. Επιπρόσθετα καθώς πολλοί επιτιθέμενοι χρησιμοποιούν ψεύτικες IP διευθύνσεις όταν εξαπολύουν μία επίθεση, τέτοιου είδους δράση θα μπορούσε να προκαλέσει ζημιές σε λάθος χρήστες ή και δίκτυα.

Τέλος κάτι τέτοιο θα μπορούσε να προκαλέσει περισσότερο τον επιτιθέμενο και αυτός να αντιδράσει εξαπολύοντας μία επίθεση που θα μπορούσε να έχει καταστροφικά αποτελέσματα.Τέτοιου είδους δράση εναντίον του επιτιθέμενου πρέπει να γίνεται με πολύ προσοχή και πρινκάποιος αποφασίσει να υιοθετήσει αυτήν την τεχνική, καλό είναι να έχει συμβουλευτεί κάποιον ειδικό για τα νομικά θέματα που προκύπτουν.

2.2.3.2. PassiveResponses

Τα *PassiveResponses*είναι η μέθοδος με την οποία το IDS απλά προμηθεύουν τους αρμόδιους χρήστες, με τις πληροφορίες που αφορούν την ανίχνευση μίας επίθεσης. Στη συνέχεια είναι στην ευθύνη των αρμοδίων να δράσουν κατάλληλα, εκμεταλλευόμενοι τις πληροφορίες αυτές. Αυτού του είδους η αντίδραση είναι και η πιο συνήθης από τα περισσότερα IDSs. Υπάρχουν διάφοροι τρόποι με τους οποίους μπορεί ένα IDS να γνωστοποιήσει τα αποτελέσματά του στους αρμόδιους χρήστες.

2.2.3.2.1 Ανακοίνωση των Alerts

Αυτή η τεχνική έχει να κάνει με τον τρόπο που ένα IDS ανακοινώνει και παρουσιάζει στουςαρμόδιους χρήστες, τις επισημάνσεις του για μία επίθεση. Μία επισήμανση για την ανίχνευσηκάποιας επίθεσης, συνήθως ονομάζεται *alert*.Τα περισσότερα IDSs δίνουν την δυνατότητα στον χρήστη να καθορίσει με σχετική ευχέρεια,την στιγμή και την μορφή που θα παράγονται τα *alerts*και σε ποιους χρήστες θαπαρουσιάζονται.

Ένα IDS είναι δυνατόν να ρυθμιστεί ώστε τα *alerts*να εμφανίζονται σε πραγματικό χρόνο, την ώρα που εντοπίζεται μία επίθεση, όπως για παράδειγμα με αναδυόμενα παράθυρα στην οθόνη ή μπορεί να ρυθμιστεί ώστε να καταγράφει τα *alerts*σε κάποιο αρχείο για μετέπειτα εξέταση.Η μορφή που θα παράγεται ένα *alert*από το IDS, μπορεί να είναι από μία απλή αναφορά στοείδος της επίθεσης με έναν τίτλο, στον επιτιθέμενο και στο θύμα αυτής, μέχρι και αναλυτικήαναφορά που θα περιέχει και πληροφορίες για το πακέτο που οδήγησε στον εντοπισμό τηςεπίθεσης, κάνοντας λεπτομερή περιγραφή του ή αναφορά στο εργαλείο που χρησιμοποιήθηκεγια την υλοποίησή της.Επίσης κάποια IDSs έχουν την δυνατότητα να πληροφορούν με *alerts*απομακρυσμένα

τουςεξουσιοδοτημένους χρήστες, είτε με αποστολή e-mail σε αυτούς, είτε ακόμα μέσω κλήσεων ήαποστολή γραπτών μηνυμάτων σε κινητά τηλέφωνα που ανήκουν σε αυτούς.

2.2.3.3.. SNMPTraps

Κάποια IDSs έχουν την δυνατότητα να αναφέρουν τα *alerts*που παράγουν, σε ένα κεντρικόσύστημα διαχείρισης του δικτύου με την χρήση SNMPTraps. Έτσι με την αποστολή σε ένα κεντρικό σύστημα, των *alerts*που παράγονται από διάφορα IDSs ενός δικτύου, καθώς και άλλων πληροφοριών που εξάγονται από άλλους μηχανισμούς ασφάλειας, όπως Firewall, είναι δυνατό να γίνει ευκολότερα συσχετισμός μεταξύ των αποτελεσμάτων που έχουν προκύψει από διαφορετικές πηγές και να σχηματιστεί μία πιο σαφής και λεπτομερής εικόνα των γεγονότων.

2.2.4 Ισχυρά και Αδύναμα Σημεία των IDSs

Παρόλο που τα IDSs θεωρούνται μία πολύτιμη προσθήκη στην πολιτική ασφάλειας ενόςδικτύου υπάρχουν κάποιες λειτουργίες τις οποίες εκτελούν ικανοποιητικά και άλλες για τιςοποίες δεν θεωρούνται επαρκή. Σε καμία περίπτωση δεν πρέπει να ανατίθεται σε ένα IDS ναεκτελέσει λειτουργίες, τις οποίες εκτελούν άλλοι τύποι μηχανισμών ασφάλειας, πιο ολοκληρωμένα και πιο αποδοτικά. Μερικές από τις λειτουργίες που επιτελούνται με επιτυχία από τα IDSs είναι :

Η παρακολούθηση και η ανάλυση των δραστηριοτήτων σε ένα σύστημα και τηςσυμπεριφοράς των χρηστών.

Μοντελοποίηση της φυσιολογικής, συνήθους δραστηριότητας ενός συστήματος ή ενόςδικτύου και στην συνέχεια παρακολούθηση για διακυμάνσεις και αλλαγές που μπορεί ναπροκύψουν στη δραστηριότητα αυτή.

Αναγνώριση των συμβάντων που αντιστοιχούν σε μία γνωστή επίθεση.

Ειδοποίηση των αρμόδιων υπευθύνων, με το κατάλληλο τρόπο, όταν εντοπιστεί μίαεπίθεση.

Επιτρέπουν σε άτομα που δεν θεωρούνται ειδικοί σε θέματα ασφάλειας δικτύων, ναεκτελούν σημαντικές λειτουργίες παρακολούθησης του δικτύου για πιθανές επιθέσεις.Μερικές από τις λειτουργίες που τα IDSs δεν μπορούν να εκτελέσουν ικανοποιητικά είναι :

Να αναπληρώσουν άλλους, ανύπαρκτους ή κακώς ρυθμισμένους μηχανισμούςασφάλειας. Τέτοιοι μπορεί να είναι firewall, μηχανισμοί αυθεντικοποίησης καιταυτοποίησης, μηχανισμοί ελέγχου πρόσβασης, ανίχνευση και αντιμετώπιση ιών,κρυπτογραφημένη διασύνδεση μεταξύ συστημάτων.

Άμεσα να ανιχνεύσουν, να ειδοποιήσουν και να αντιδράσουν σε μία επίθεση, σε μεγάλαδίκτυα με πολύ αυξημένο traffic ή σε συστήματα με λίγους ελεύθερους πόρους.

Να ανιχνεύσουν νέα είδη επιθέσεων ή παραλλαγές παλαιοτέρων.

Να δράσουν αποτελεσματικά σε επιθέσεις που υλοποιούνται από εξειδικευμένους καιέμπειρους επιτιθέμενους και ειδικά στην περίπτωση που αυτοί έχουν αντιληφθεί τηνύπαρξή τους και γνωρίζουν τρόπους να τα παρακάμψουν.

Αυτοματοποιημένα να ερευνήσουν και να αναλύσουν μία επίθεση, χωρίς την ανθρώπινησυμμετοχή.

Παρουσιάζουν πρόβλημα σε δίκτυα που διασυνδέονται με switches, καθώς αυτά δεντους επιτρέπουν να έχουν παθητικά πρόσβαση σε όλο το traffic του δικτύου.

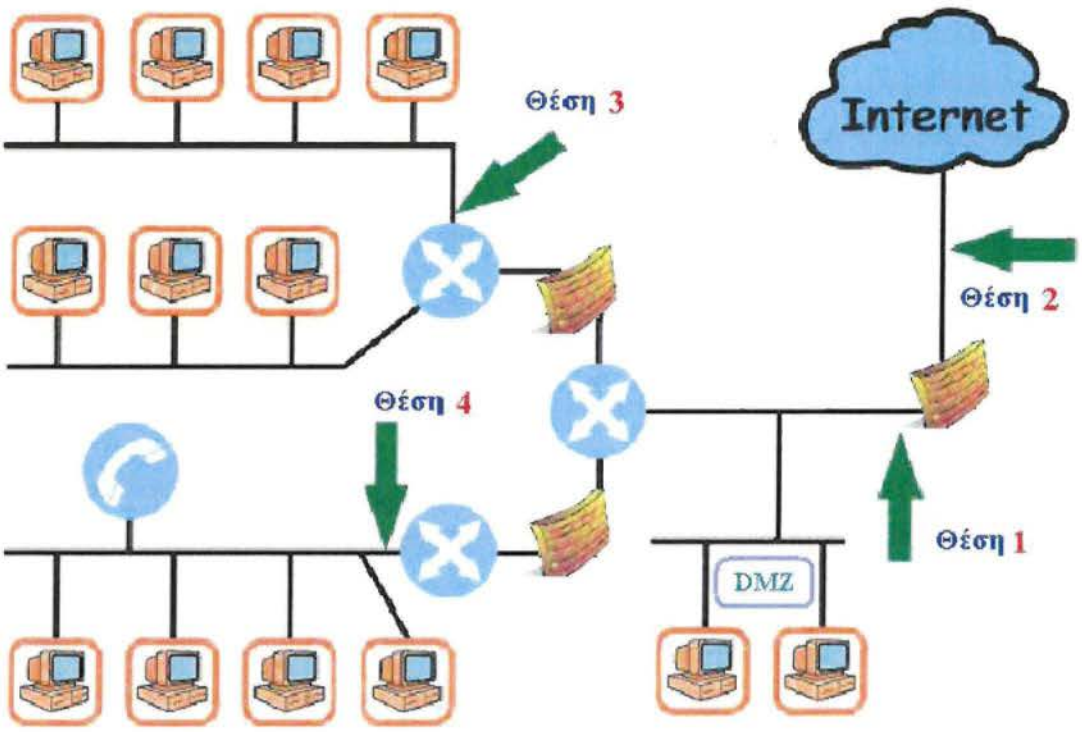
Παρουσιάζουν συμπτώματα από *FalsePositives*και *FalseNegatives*, ιδιαίτερα στηνπερίπτωση που δεν έχουν ρυθμιστεί σωστά, και αυτό είναι κάτι που μειώνει τηναξιοπιστία τους.

2.2.5 Πρακτική Χρήσης των IDSs

Ο τρόπος με τον οποίο ένας οργανισμός θα σχεδιάσει την στρατηγική χρήσης και υλοποίησηςIDSs, ώστε να προστατέψει αποτελεσματικά το δίκτυό του και κατ' επέκταση τα συστήματα που συνδέονται σε αυτό και τις πληροφορίες που περιέχουν, έχει άμεση σχέση με την τοπολογία του δικτύου και το είδος της πληροφορίας που πρέπει να διαφυλαχτεί.Σε κάθε περίπτωση η εφαρμογή IDSs, για να καλύψει με επιτυχία τις ανάγκες για προστασίαενός δικτύου, απαιτεί μελέτη και σχεδιασμό, καθώς και εξειδικευμένο προσωπικό, ώστε ναδιαχειρίζεται και να επιβλέπει συνεχώς την λειτουργία τους και να δρα αποτελεσματικά καιυπεύθυνα στην περίπτωση εμφάνισης μίας επίθεσης. Στις περισσότερες περιπτώσεις η πιο αποδοτική και προτεινόμενη πρακτική για την πληρέστερη προστασία ενός μεγάλου δικτύου, είναι η χρήση NIDSs και HIDSs σε συνδυασμό μεταξύ τους.

2.2.6 Πρακτική Χρήσης των NIDSs

Η πιο συνήθης δυσκολία στην εφαρμογή των NIDSs, είναι η επιλογή των σημείων του δικτύουστα οποία θα τοποθετηθούν οι *Sensors*. Όπως φαίνεται και στην εικόνα 16, υπάρχουνδιάφορες πιθανές λύσεις, από τις οποίες η κάθε μία έχει τα δικά της πλεονεκτήματα :



Εικόνα 13Πιθανές θέσεις τοποθέτησης ενός Sensor

Θέση 1: Πίσω από κάθε συνοριακό firewall, στην DMZ

Πλεονεκτήματα

Το IDS εντοπίζει όλες τις επιθέσεις που προέρχονται εκτός του δικτύου και καταφέρνουννα ιαπεράσουν το firewall.

Με την τοποθέτηση του IDS σε αυτήν την θέση είναι δυνατόν να επισημανθούν πιθανάλάθη στις υθμίσεις του firewall.

Είναι δυνατόν να ανιχνευτούν επιθέσεις που στοχεύουν τον webserver ή τον ftpserverκαι άλλ συστήματα που πέφτουν συχνά στόχοι μίας επίθεσης και συνήθως βρίσκονταιστην DMZ ενός δικτύου.

Ακόμα και αν δεν ανιχνευτεί η επίθεση, όπως αυτή κατευθύνεται προς το εσωτερικό τουδικτύου, είν δυνατό με το IDS σε αυτή τη θέση, να εντοπιστεί το εξερχόμενο trafficπου δημιουργείται από τα συστήματ που ήταν στόχοι και μέσω αυτού να γίνειαντιληπτή η επίθεση.

Θέση 2: Μπροστά από κάθε συνοριακό firewall.

Πλεονεκτήματα

Σε αυτό το σημείο το IDS είναι δυνατό να εντοπίσει όλες τις επιθέσεις πουστοχεύουν το δίκτυο, ακόμ και αυτές που θα αποτραπούν από το firewall. Μεαυτόν τον τρόπο υπάρχει η δυνατότητα να καταγραφεί, τ πλήθος και το είδος τωνεπιθέσεων που στοχεύουν το δίκτυο καθημερινά.

Θέση 3: Στο δίκτυο κορμού (backbone) του δικτύου.

Πλεονεκτήματα

Σε αυτή την θέση το IDS παρακολουθεί ένα μεγάλο μέρος του traffic του δικτύου,που έχει σχέση με τ υποδίκτυα που συνδέονται πάνω στο backbone και έχει τηνδυνατότητα να εντοπίσει επιθέσεις που σχετίζοντ με αυτά.

Είναι δυνατό να ανιχνευτούν επιθέσεις που προέρχονται από συστήματα, που ανήκουν μέσα στην ζών ασφαλείας του δικτύου.

Θέση 4: Σε σημαντικά υποδίκτυα του δικτύου.

Πλεονεκτήματα

Το IDS μπορεί να εντοπίσει επιθέσεις που στοχεύουν σημαντικά συστήματα του δικτύου,που περιέχου κρίσιμες πληροφορίες.

Επιτρέπει την εστίαση της προσοχής σε πόρους του δικτύου που έχουν μεγάλη αξία.

2.2.7 Πρακτική Χρήσης των HIDSs

Η πιο αποτελεσματική χρήση των HIDSs θα ήταν η εφαρμογή τους σε κάθε σύστημα τουδικτύου. Κά τέτοιο όμως και ιδιαίτερα σε μεγάλα δίκτυα, θα αποτελούσε μία αρκετά ακριβή, χρονοβόρα και επίπονη λύσ καθώς για κάθε σύστημα που παρακολουθείται θα απαιτούνταν και ξεχωριστές ρυθμίσεις που να τ αντιπροσωπεύουν.Για αυτό το λόγο, το πιο λογικό θα ήταν σε πρώτη φάση να τοποθετηθούν HIDSs στ πιοσημαντικά συστήματα του δικτύου, τα οποία περιέχουν κρίσιμες πληροφορίες ή των οποίων η σωστ λειτουργία είναι απαραίτητη. Στη συνέχεια θα μπορούσαν τα τοποθετηθούν HIDSs και στην πλειοψηφία τω υπόλοιπων συστημάτων, για τα οποία η εγκατάσταση ενός HIDS απαιτεί περίπου τις ίδιες ρυθμίσεις.Με αυτό τον τρόπο είναι δυνατόν τα σημαντικά συστήματα του δικτύου να επιβλέπονταιξεχωριστά, αφού μπορούν τ HIDSs που λειτουργούν σε αυτά, να παρουσιάζουν τα *alerts*που παράγουν σε ένα κεντρικό σύστημ παρακολούθησης αφιερωμένο μόνο για αυτό το σκοπό

ΚΕΦΑΛΑΙΟ 3

3.1IPFIRE

3.1.1 Τι είναι και γιατι το διαλεξαμε ;

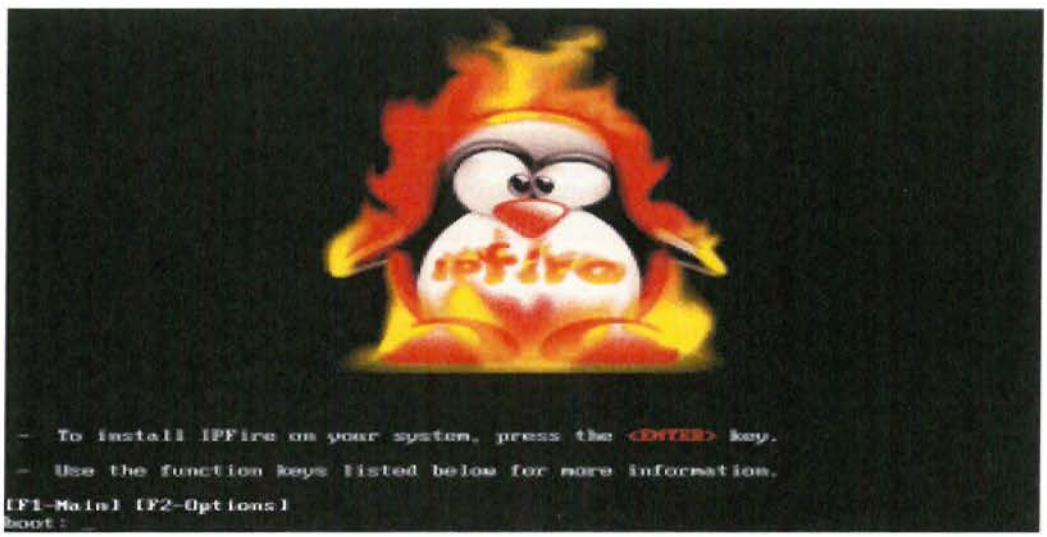
Το IpFire είναι μια διανομή Firewall ανοιχτού κώδικα χρησιμοποιείται σαν το λειτουργικο και διαχειρηστικό σύστημα σε firewall τυπου hardware. Το IPFire βασίζεται σε μια πρόσφατη έκδοση του πυρήνα του Linux,και μπορεί να υποστηρίζει τα περισσότερα από τα πιο πρόσφατα hardware, όπως 10Gbit κάρτες δικτύου και μια ποικιλία από ασύρματο υλικό έξω από το κουτί. Έχει τη δύναμη στα δίκτυα τομέα, με βάση τα αντίστοιχα επίπεδα ασφαλείας τους που του καθιστά εύκολο να δημιουργήσουμε προσαρμοσμένες πολιτικές που διαχειρίζονται κάθε τμήμα.

Οι προγραμματιστέςτουIPFireπροσέχουν αρκετά ώστε να έχει την ικανότητα να τρέχει όσο το δυνατόν πιο πολλές παραλλαγές του συστήματος. Αυτό βοηθά το IPFire να τρέξει σε παλαιότερο ή φθηνό υλικό, καθώς και συστήματα υψηλής απόδοσης. Αυτός είναι και ο βασικός λόγος που το επιλέξαμε αφού εχει πραγματικά πολύ μικρές απαιτήσεις ώστε να λειτουργεί άρτια.

Ελάχιστες απαιτήσεις συστήματος είναι ένας IntelPentiumI (i586), 128MBRAM και 2GB χώρο στο σκληρό δίσκο. Ορισμένα πρόσθετα έχουν επιπλέον απαιτήσεις για να εκτελέσει ομαλά αν και στη δική μας περίπτωση δεν χρειαστήκαμε καποια από τις προσθετε υπηρεσίες της διανομής. Σε ένα σύστημα που να ταιριάζει με τις απαιτήσεις υλικού,το IPFire είναι σε θέση να εξυπηρετεί εκατοντάδες clients ταυτόχρονα. Την υλοποιήση μας την κάναμε σε ένα μηχάνημα με IntelCeleronTualeron στα 1,7GHz 512MB RAM2GB σκληρό δίσκο και 2 κάρτες δικτύου.

3.1.2 Εγκατασταση IPFire

3.1.2.1Boot από CD



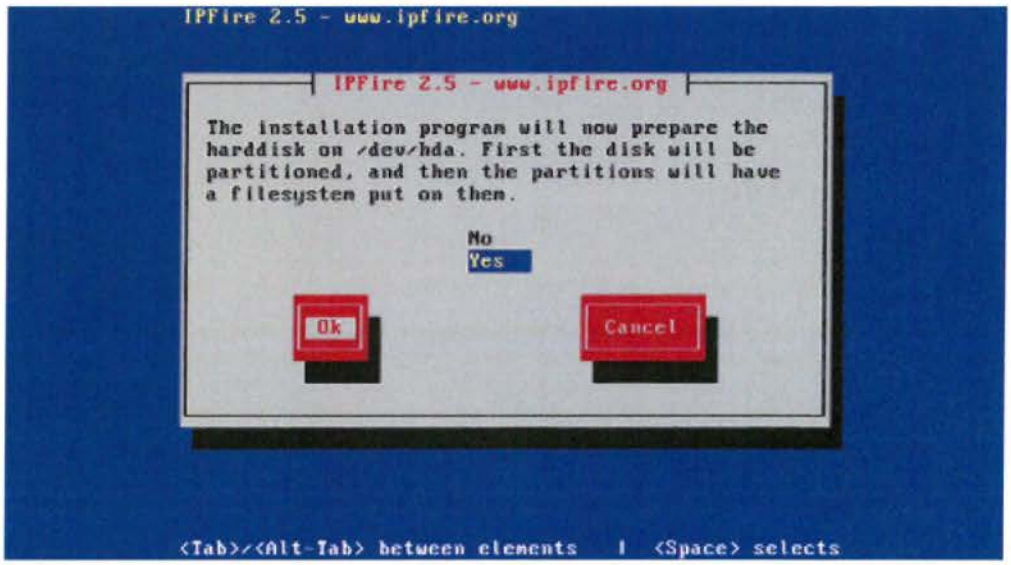
Εικόνα 14 έναρξη εκκίνησης από το CDτου IPFire

Για να εγκαταστησου με το ipfire πρωτα γραψαμε το iso σε ενα cd ωστε το μηχανημα να κανει boot απο το cdrom.Όταν ξεκινησε η εγκατασταση στην πρωτη οθονη ζητασε τις ρυθμισεις οθονης οπου επιλεξαμε τις προκαθορισμενες.

Εικόνα 15εναρξή εγκατάστασης

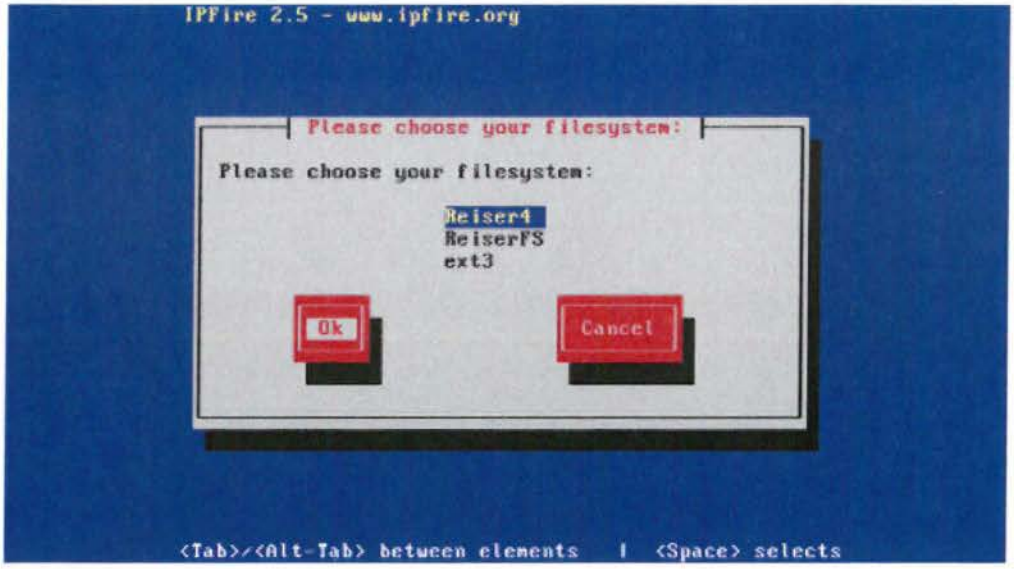
Μετά επιλέξαμε τη γλώσσα για την εγκατασταση και το webinterface. Λόγο έλλειψης της Ελληνικής επιλέχθηκαν τα Αγγλικά.

3.1.2.2 Format & Copy



Εικόνα 16 προετοιμασία Format

Μετά γίνεται το Format του σκληρού Δίσκου ώστε να επτοιμαστεί για την εγκατάσταση του IpFire.



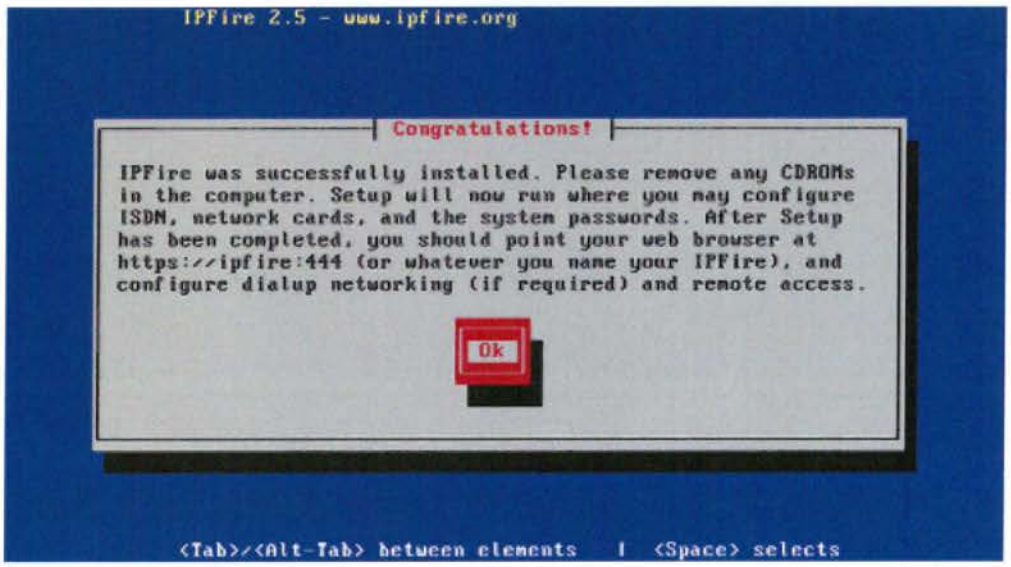
Εικόνα 17επιλογή filesystem

Εδώ επιλέξαμε το Filesystem του λειτουργικού, επιλέξαμε το ext3 .

Εικόνα 18 Προειδοποίηση για τη μικρή χωριτηκότητα του σκληρού δίσκου.

Εικόνα 19εγκατάσταση

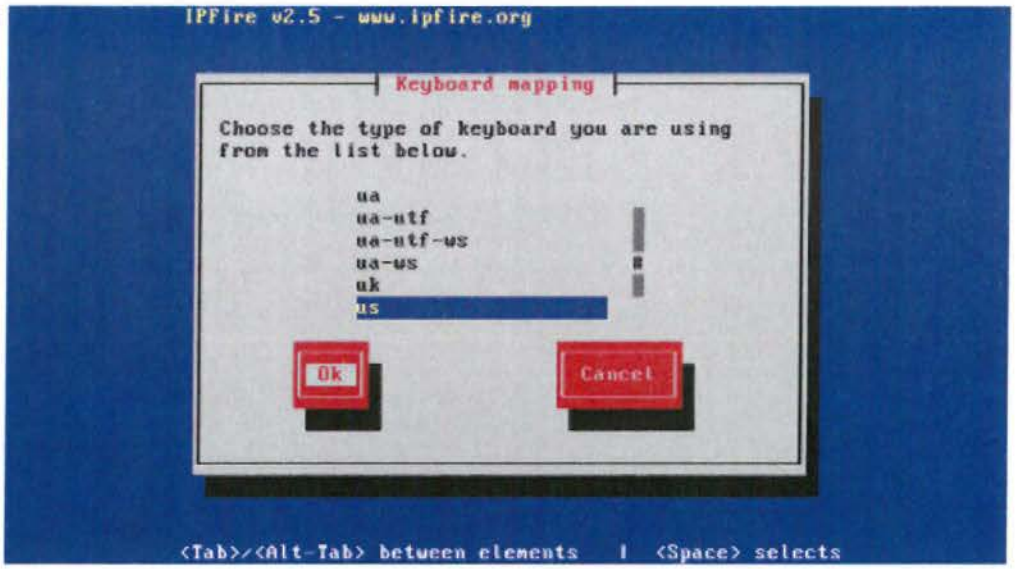
Εδώ έγινε το partition και toformat του σκληρού δίσκου και μετά τα αρχεία συστήματα φορτώθηκαν στο σκληρό μας δίσκο.



Εικόνα 20 τερματισμός εγκατάστασης

Με την ολοκλήρωση αφαιρουμε το cd ώστε να γινει το boot πλέον από το σκληρό με το λογισμικό που μόλις εγκαταστήσαμε.

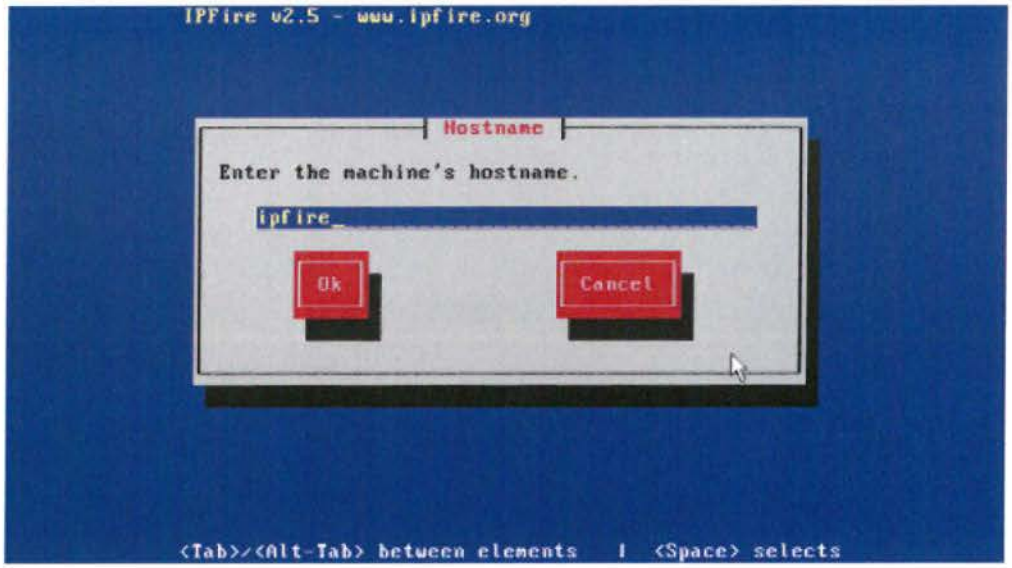
3.1.2.3 Local Settings



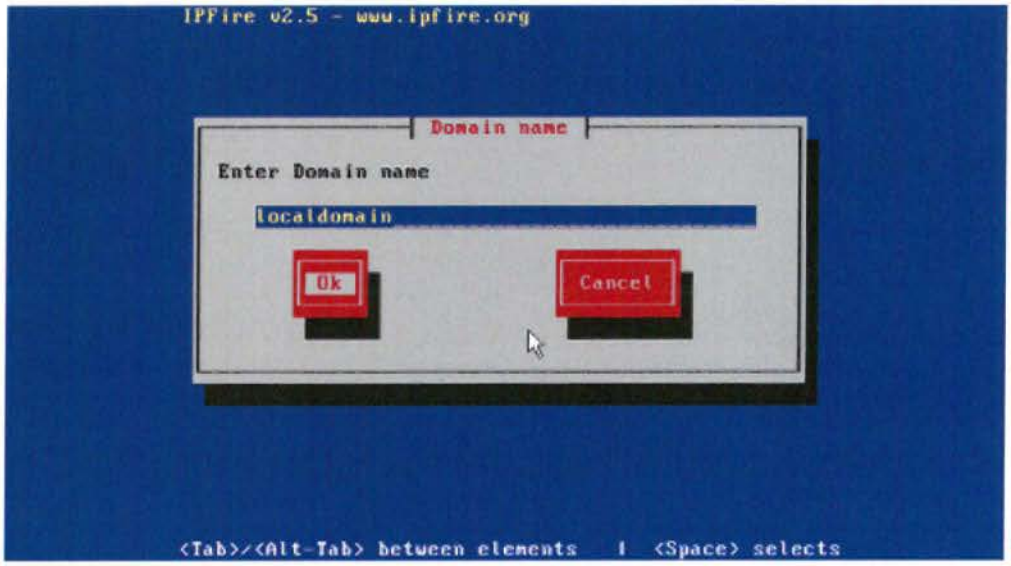
Εικόνα 21Επιλογή της γλωσσας/τύπου πληκτρολογίου.

Εικόνα 22Επιλογή ζώνης ώρας .

3.1.2.4 Hostname & Domain



Εικόνα 23hostname



Εικόνα 24domain

Αφου επιλέξαμε γλώσσα εισαγώγης και ρυθμίσαμε την ώρα, ορισαμε το Hostname του μηχανήματος στην σε firewall και το DomainNametουδικτύουμαςσεοslab.

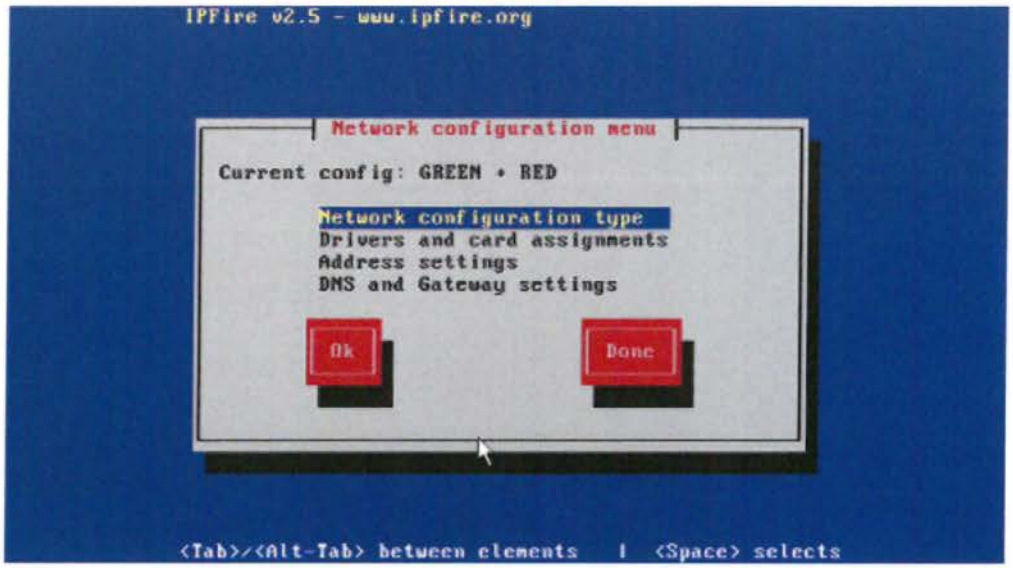
3.1.2.5 Passwords

Εικόνα 25rootuser

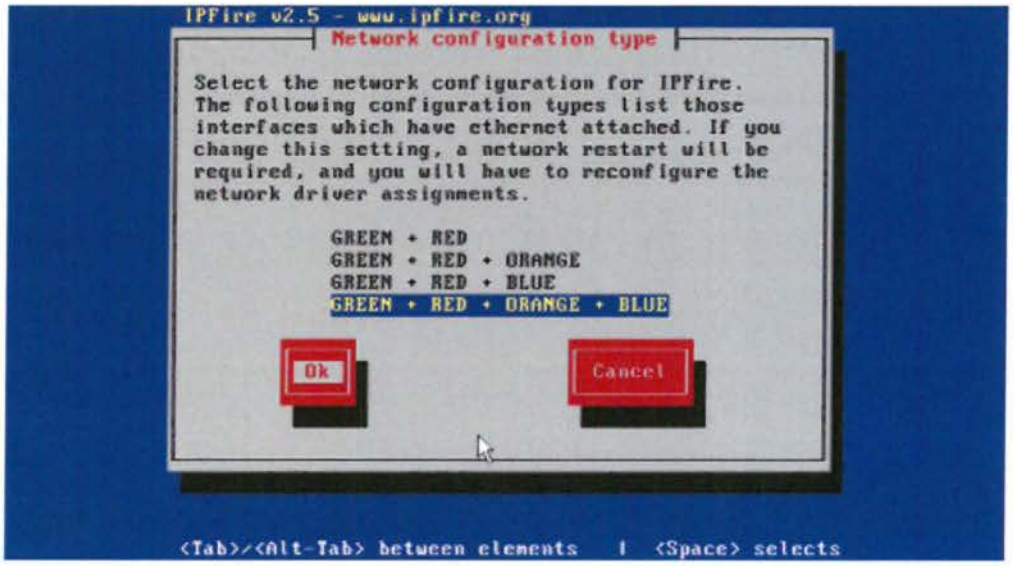
Προκειμένου να έχουμε πρόσβαση τοπικά στο μηχάνιμα έπρεπε να φτιάξουμε τον χρήστη Rootuser: root, rootpassword: e8PySb.Αν χρειαστουμε να επαναλάβουμε κάποια ρύθμηση από την αρχή τότε μπορούμε να τρέξουμε το setup ξανα κάνοντας login στο rootaccount τοπικά. Για την ρύθμηση του ipfireμέσω της webεφαρμογής που έχει έπρεπε να δημιουργήσουμε άλλον έναν χρήστη τον admin.Adminuser: admin, adminpassword: 1234e8PySb

3.1.3Δίκτυο

3.1.3.1 Αριθμός Δικτύων.



Εικόνα 26διαχειριστικό μενου δικτύων

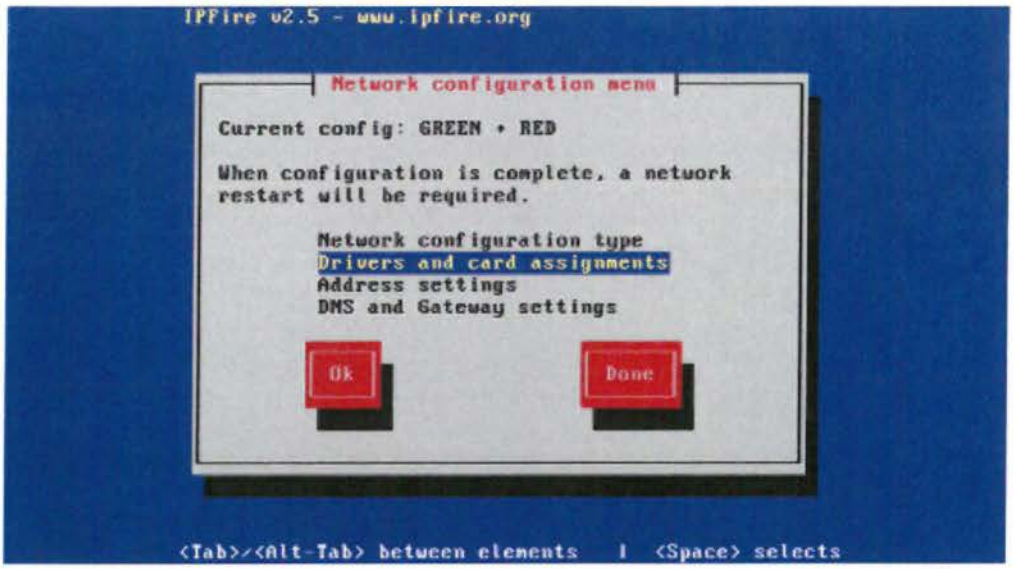


Εικόνα 27 επιλογή NICs

Μπήκαμε στις ρυθμίσεις δικτύου για να ορίσουμε των αριθμό των δικτύων.Μπορούσαμε να επιλέξουμε μέχρι 4 δικτυα και να χωριστούν σε**Πράσινο**,**Μπλε**, **Πορτοκαλί**, **Κόκκινο**υποδίκτυο. Επειδή εμείς κάνουμε μι πιο απλή εγκατάσταση του IPFire επιλέξαμε **Green** + **Red**, που σημαίνει 2 Δικτυα.Που τυπικά έχεις ένα δίκτυ για τους υπολογιστές του τοπικού δικτύου το **Green** δίκτυο και ένα για σύνδεση στο Internet το **Red**δίκτυο.

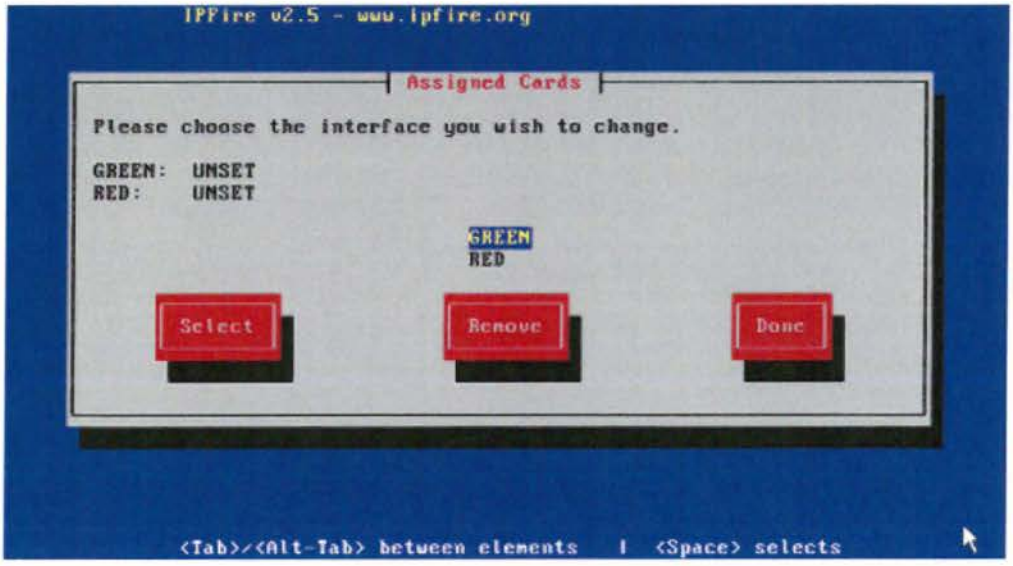
Red	WAN	Εξωτερικό Δίκτυο ,Συνδεδεμένο στο Internet (τυπικά μία σύνδεση στο ISP)
Green	LAN	Εσωτερικο,Ιδιωτικό δίκτυο . Συνδεδεμλενο Τοπικά.
Orange	DMZ	Η 'αποστρατικοποιημένη' ζώνη. Ένα απροστάτευτο/Server δίκτυο προσβάσιμο από το internet.
Blue	WLAN	Ασύρματο Δικτυο,Ένα ξεχωριστό δίκτυο για ασύρματη πρόσβαση.

3.1.3.2Αναθεση καρτών δικτύου NICs



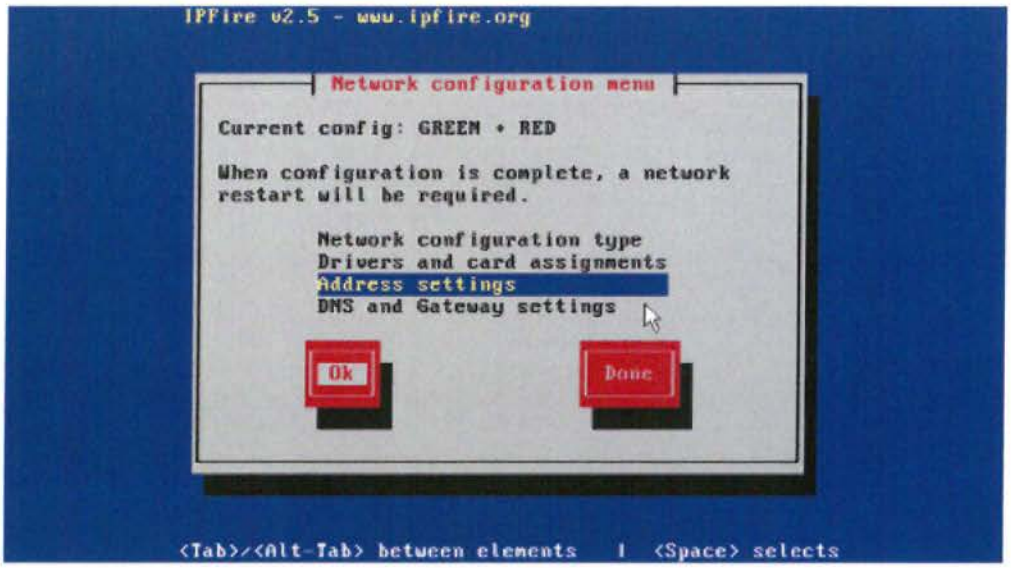
Εικόνα 28διαχειριστικό μενου δικτύων συν.

Επειδή όλα τα προηγούμενα επιλεγμένα δίκτυα πρέπει να έχουν μια NIC (networkinterfacecard) χρειάζεται να ορίσουμε ποια Κάρτα Δικτύου ανήκει στο Green και ποια στο Red δικτυο από το Μενού Ανάθεσης Οδηγών και ΚαρτώνΕδώ ορίσαμε της κάρτες δικτύου για το red και greeninterface. Πιοαναλυτικάγιατογreeninterfaceεπιλέχτηκε ηRTL8139, ενώ για toredinterface ηRTL8029AS.



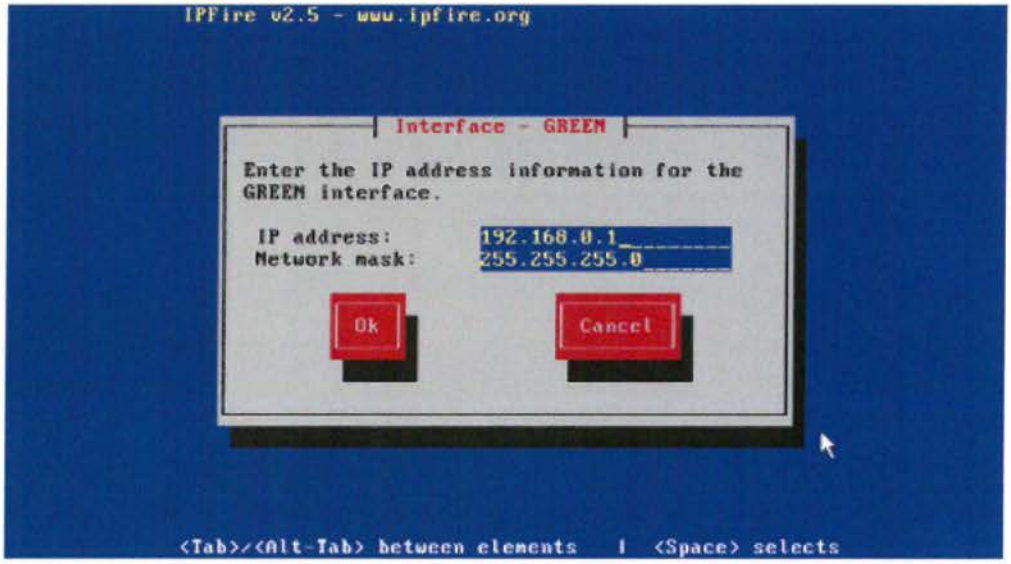
Εικόνα 29 επιλογή NICγια τα δυο δίκτυα

3.1.3.3Network Addresses

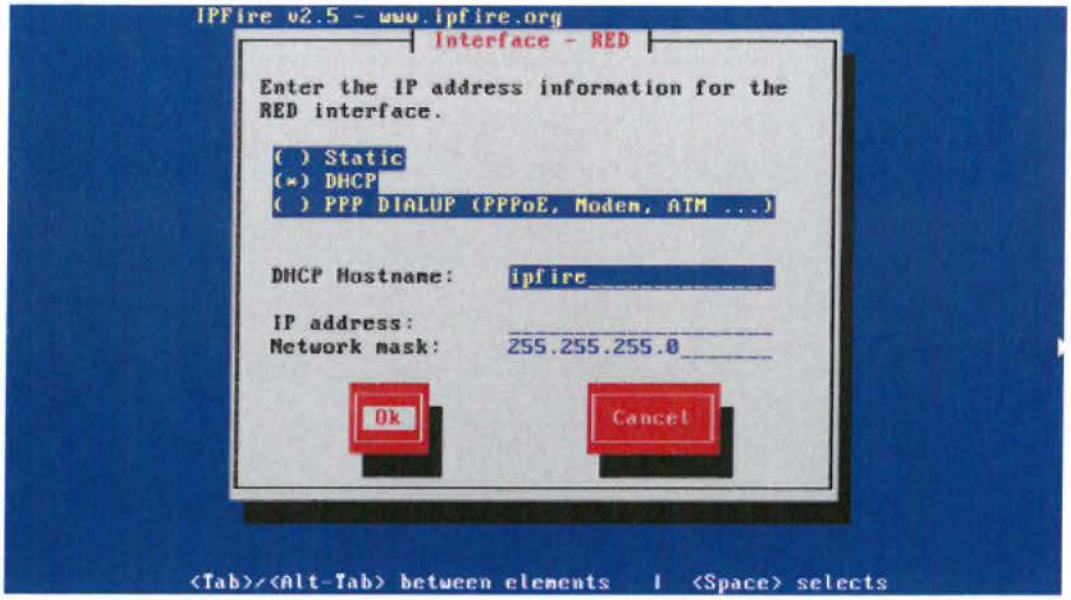


Εικόνα 30διαχειριστικό μενου δικτύων συν.

Στις Ρυθμίσεις Διευθύνσεων κάνουμε την ανάθεση της διευθύνσης του Green δικτύου, σε 10.0.0.10/24



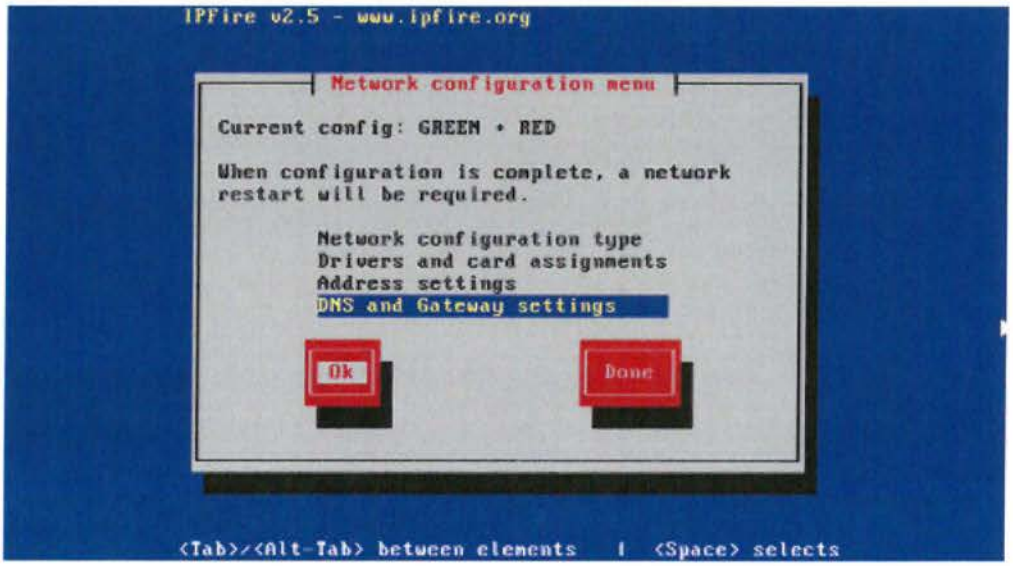
Εικόνα 31configuration



Εικόνα 32redintrerfaceconfiguration

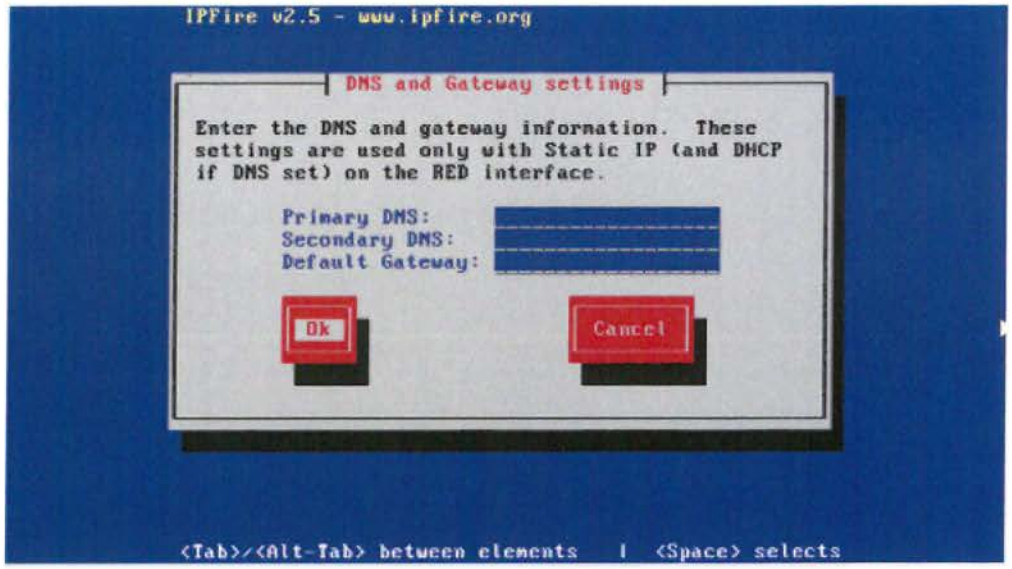
Για τοRed δικτυο δεν κάναμε κάποια τροποποίηση και το αφήσαμε στην προεπιλεγμενη επιλογή του DHCP, μιας και παιρνει διεύθυνση κατευθείαν από τον κεντρικό δρομολογιτή του εργαστήριου.

3.1.3.4DNS and Gateway Installation



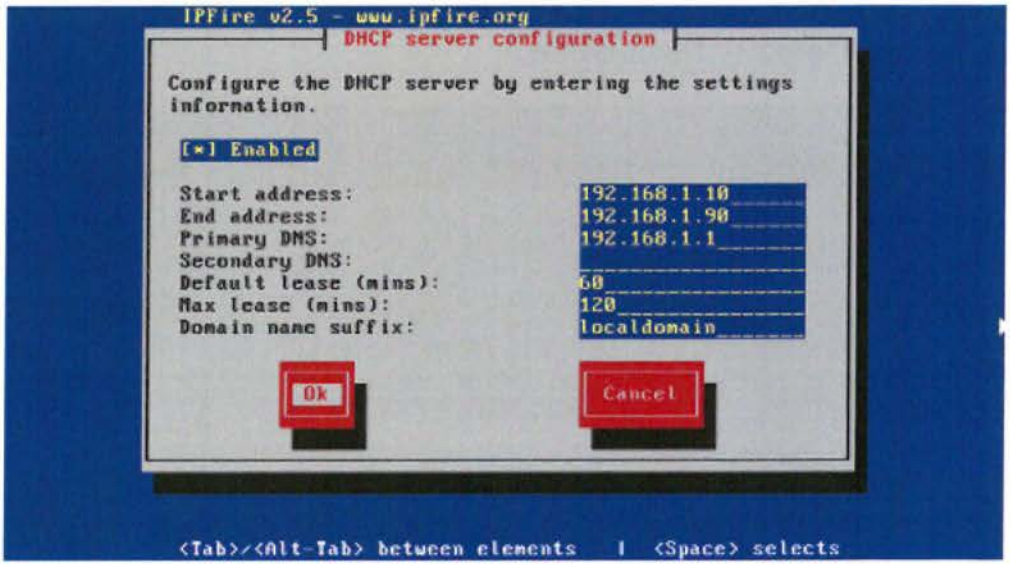
Εικόνα 33διαχειριστικό μενου δικτύων συν.

Επίσης δεν χρειάστηκε να κάνουμε κάποια ρύθμηση για DNSκαι Gateway



Εικόνα 34 DNS

3.1.3.5 DHCP Server

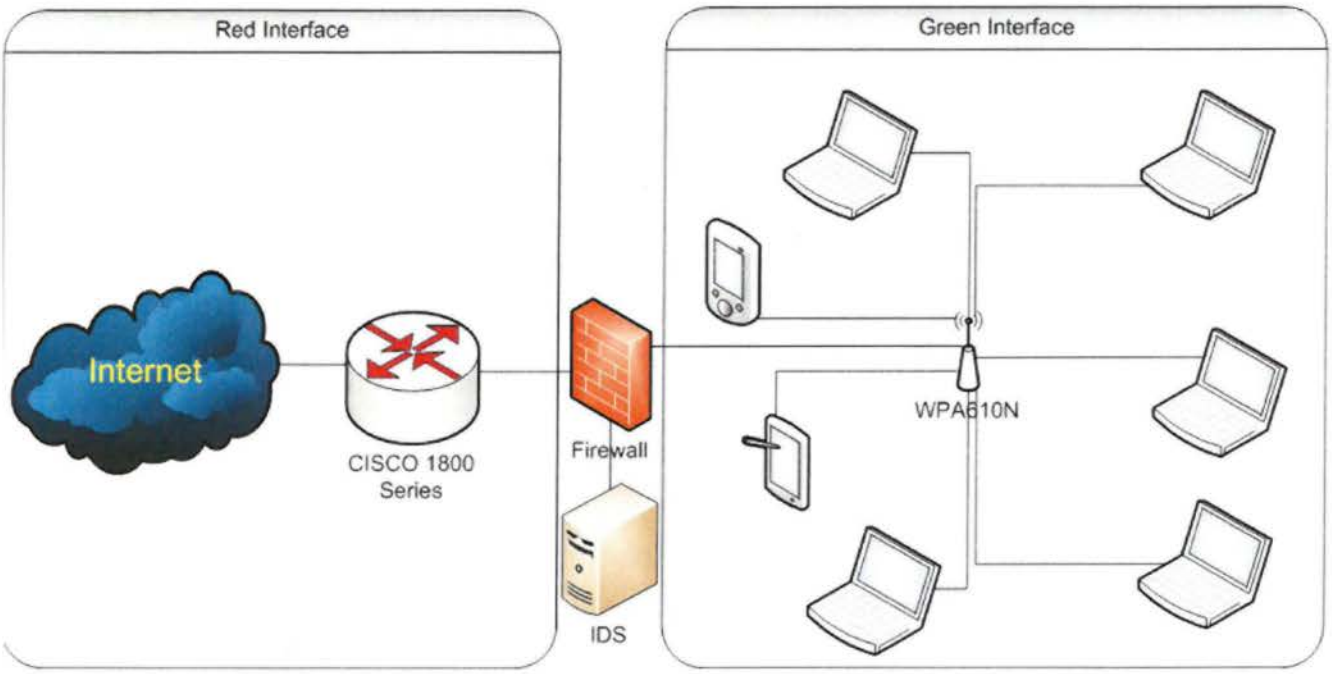


Εικόνα 35DHCP

Το τελευταιο που επερεπε να κάνουμε είναι το κανουμε το configure του DHCP (DynamicHostConfigurationProtocol) Server για το green δίκτυο. Θεσαμε ως έυρος του δικτύου 10.0.0.10-10.0.0.200.

3.1.4 BlockΔιάγραμμα

Στο παρακάτω block διαγραμμα απεικονίζεται η δομή του δκτυου μας . Όπως βλεπουμε οτιδήποτε εχει να κάνει με την ενδοεπικοινωνία των τερματικών του δικτύου μας ανήκει στο GreenInterface και ελέγχεται από το IDS ώστε να ανιχνευθεί οποιαδήποτε προσπαθεια απειλής μέσα από το GreenInterface .Στη συνέχεια οποιοδήποτε τερματικό του δικτύου μας συνδέεται στο internet μέσο του cisco δρομολογητή (RedInterface) αφού πρώτα εγκριθεί από το Firewall ο προορισμός του.



Εικόνα 36Η υλοποίηση που ακολουθήθηκε

3.1.5ConfigurationIpFire

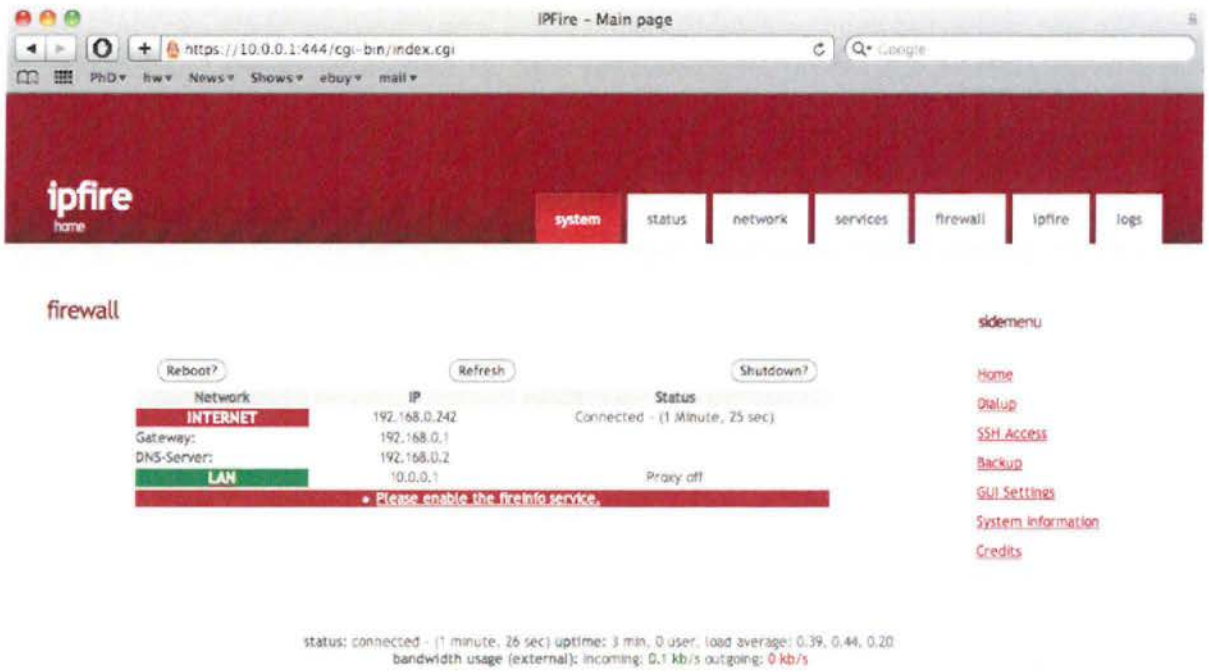
Αφου έχουμε ολοκληρώσει την εγκατασταση και το setup του hardware που διαθέτουμε με την διανομή του IpFire . Φθάσμε στο τελευταιο κομμάτι που είναι να ορίσουμε την πολιτική διαχείρησης που θα ακολουθήσουμε για το Firewall που εχουμε στήσει και αντιστοίχος να το παραμετροποιήσουμε.

Εμείς λοιπόν αυτό που θέλουμε να αποτρέψουμε από το δικτυο μας είναι οι clients που συνδεόνται ευρίως ασύρματα στο δίκτυο να μην εχουν πρόσβαση σε ιστοτοπους με :

- Μεγάλη επικινδυνότητα για το δίκτυο μας(Πορνογραφία Τσόγος Κτλ) .
- Μεγάλες απιτήσεις σε bandwidth (Youtube , P2P torrent κτλ)
- Προορισμούς που αποσπούν την προσοχή των σπουδαστών εν ωρα μαθήματος (FacebookTwitter ,αθλητικη δημοσιογραφια κτλ)

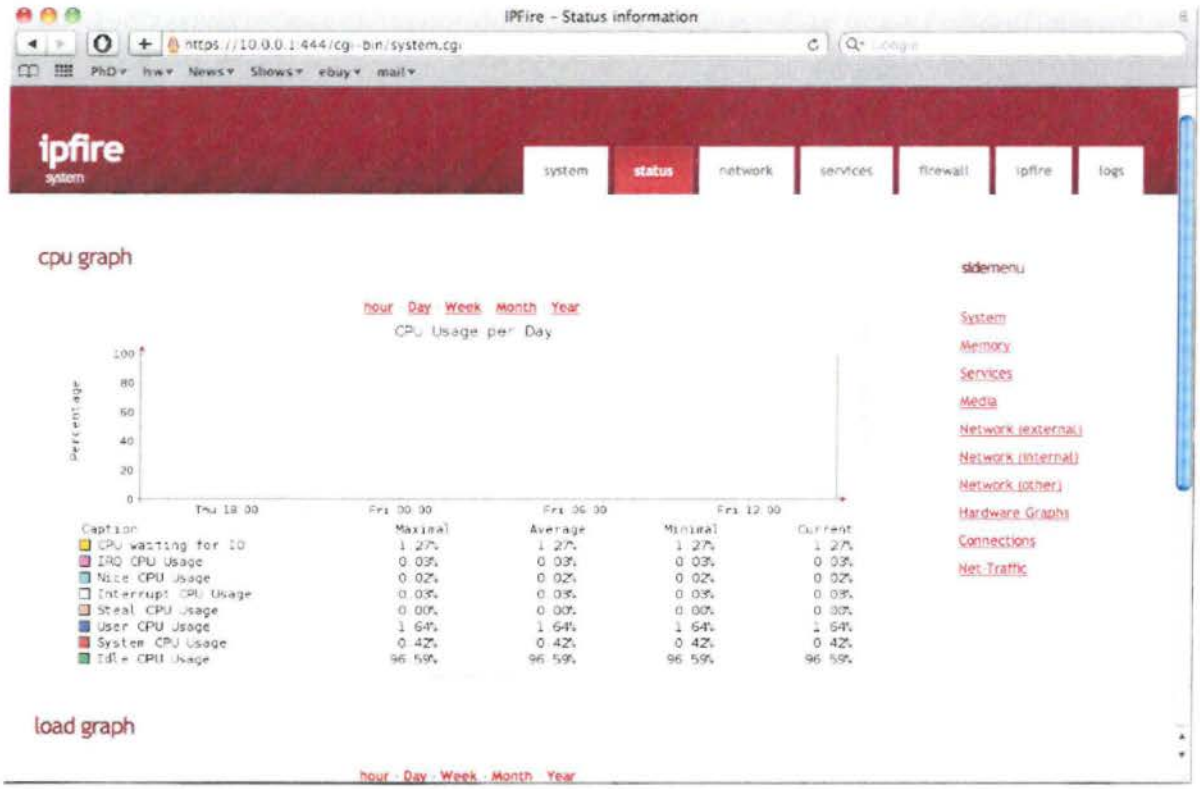
Προκειμένου λοιπόν να μπούμε στην διαχειριστική σελίδα της εφαρμογής, συνδεόμαστε σε κάποια συσκευή που είναι συνδέδεμένη πάνω στο greeninterface, και μέσω κάποιας εφάρμογής περιήγησης

μπαίνουμε στην σελίδα https://firewall.oslab:444 ή στην https://10.0.0.1:444. Αφού βάλουμε σωστά τα στοιχεί του διαχειρηστή μπορούμε να πλοηγηθούμε στην εφαρμογή.



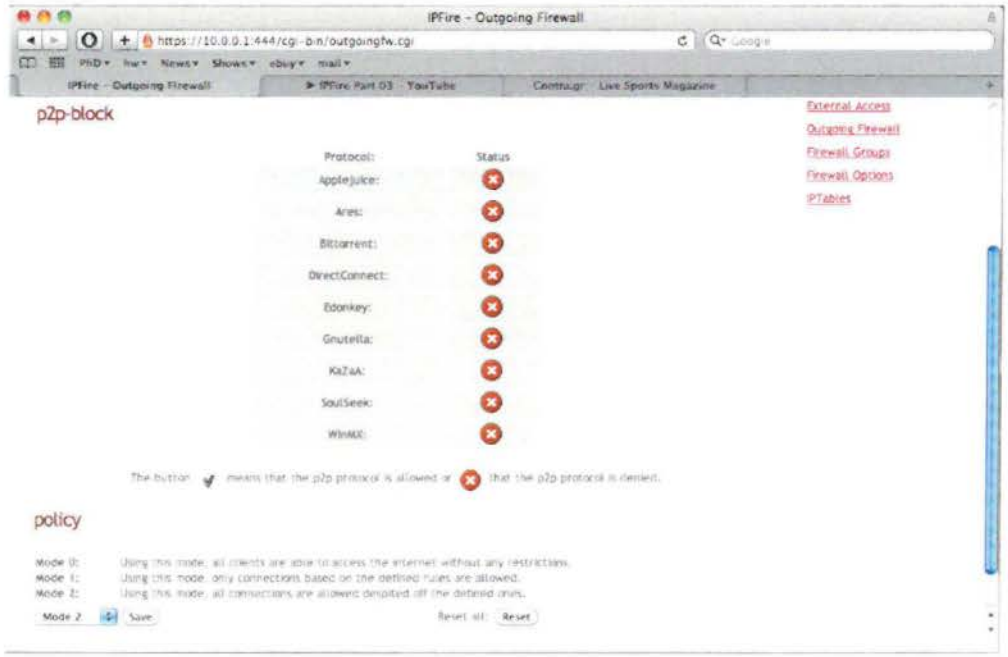
Εικόνα 37 κεντρική σελίδα

Εδώ εχουμε μπεί στη Κεντρική σελίδα του συστήματος μας, οπου φένεται ο χρόνος λειτουργίας της υπηρεσίας, καθώς και πληροφορίες για το πόσοι χρήστες είναι συνδεδεμένοι αλλα και πληροφορίες για τον φόρτο του δικτύου.



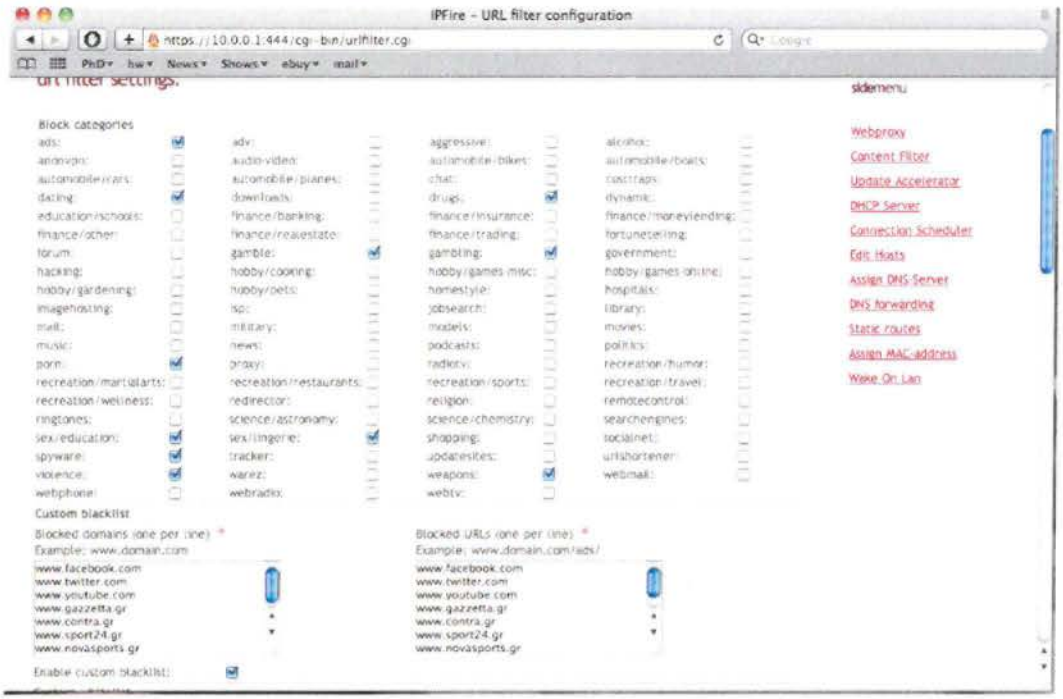
Εικόνα 38 φόρτος επεξεργαστή

Προκειμένου να είναι αδύνατη η πρόσβαση στους χρήστες του ασύρματου σε υπηρεσίες P2P απαγορεύτηκε η λειτουργία τους.

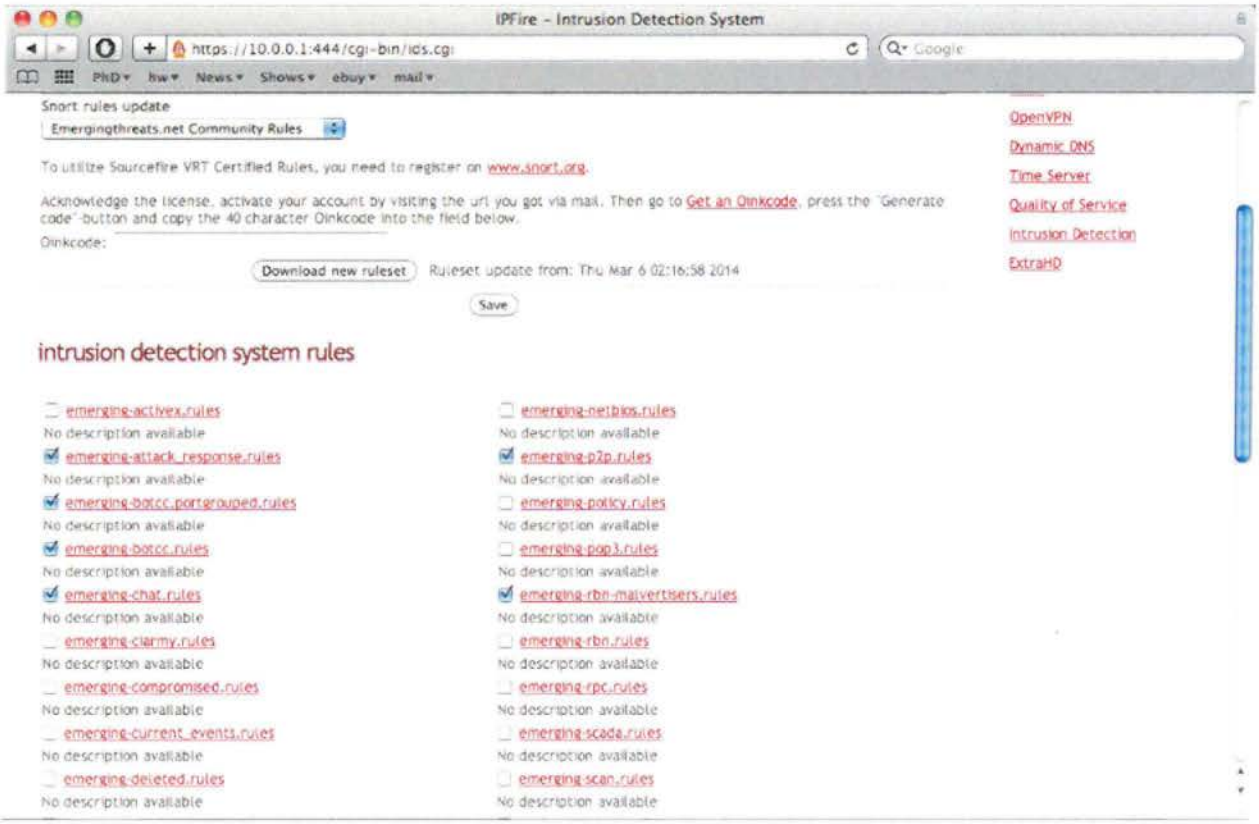


Εικόνα 39p2p-block

Για την ασκοπη χρήση πόρων καθώς και ύποπτων ιστοσελίδων απαγορεύτηκε η είσοδος σε αντιστοιχε
ιστοσελιδες (ναρκωτικά, όπλα, πορνεία)



Εικόνα 40url filtering



Εικόνα 41IDS

3.2IDSSnort

Το Snort είναι ένα ακόμη NIDS του οποίου καταρχήν η ειδοποιός διαφορά σε σχέση με τα υπόλοιπα που έχουν αναφερθεί παραπάνω είναι ότι διατίθεται δωρεάν. Το γεγονός αυτό όμως δεν δείχνει το παραμικρό για την ποιότητα των υπηρεσιών που μπορεί να προσφέρει. Παρακάτω ακολουθεί μια λίστα που συνοψίζει μερικά από τα κύρια χαρακτηριστικά του.

- Μη απαιτητικό σε πόρους για την λειτουργία του
- Ανάλυση της διακινούμενης κίνησης και καταγραφή (logging) πακέτων σε πραγματικό χρόνο
- Ικανότητα ανίχνευσης μεγάλου εύρους επιθέσεων όπως : bufferoverflows, portscans, επιθέσεις που εκμεταλλεύονται αδυναμίες του CGI, σφάλματα των λειτουργικών συστημάτων κ.α.
- Απλός, εύχρηστος και ευέλικτος τρόπος καθορισμού των κανόνων με βάση τους οποίους συμπεριφέρεται το σύστημα στα πακέτα που κυκλοφορούν στο δίκτυο.
- Άμεση ειδοποίηση σε περίπτωση ύποπτης δραστηριότητας η οποία υπάρχει η δυνατότητα να πραγματοποιηθεί με πολλούς τρόπους (π.χ. e-mail, UNIXsocket κτλ)

Στον τομέα των συστημάτων ανίχνευσης εισβολών δικτύου, το Snort αποτελεί ένα από τα πλέον διαδεδομένα, αποτελεσματικά και αξιόπιστα συστήματα. Πρόκειται για μία εφαρμογή ανοιχτού κώδικα που έχει αναπτυχθεί ώστε να λειτουργεί σε μία μεγάλη ποικιλία λειτουργικών συστημάτων (Windows, Solaris, συστήματα τύπου Unix και άλλα) η οποία διατίθεται δωρεάν μέσω της ιστοσελίδας www.snort.org. Το γεγονός της ελεύθερης διάθεσης του πηγαίου κώδικα αποτέλεσε κίνητρο και πρόκληση για αρκετούς ανθρώπους, με αποτέλεσμα τη σταδιακή δημιουργία μίας μεγάλης κοινότητας από άτομα που ασχολούνται, τακτικά ή περιστασιακά, με το Snort και αναζητούν τρόπους ώστε να γίνει ακόμα πιο αποτελεσματικό και γρήγορο.

Στη συνέχεια του κεφαλαίου παρουσιάζεται οι ο τρόπος λειτουργίας του Snort καθώς και ορισμένα από τα κυριότερα χαρακτηριστικά και υποσυστήματά του.

3.2.1 Οι κανόνες του Snort.

Οι κανόνες του Snort είναι αυτοί που υποδηλώνουν όχι μόνο τι θέλουμε να ψάξει το σύστημα στα εισερχόμενα πακέτα, αλλά επίσης και τι ενέργεια θέλουμε να εκτελέσει σε περίπτωση που βρεθεί πακέτο που θα ικανοποιεί όλες τις συνθήκες του κανόνα.

Σχεδόν όλοι οι κανόνες έχουν γραφτεί με στόχο την ανίχνευση και απαγόρευση διέλευσης σε πακέτα που περιέχουν «υπογραφές εισβολής» (intrusionsignatures), δηλαδή ορισμένα χαρακτηριστικά στοιχεία ενός συγκεκριμένου τύπου επίθεσης, τα οποία μπορεί να είναι καθορισμένες παράμετροι στην επικεφαλίδα του πακέτου (packetheader) ή/και στα δεδομένα του πακέτου (payload). Τέτοιου είδους πακέτα συνήθως ποτελούν έρος προσπάθειας που γίνεται με στόχο να πληγεί η ακεραιότητα του υπολογιστή του χρήστη και δεν θέλουμε α επιτραπεί η διέλευσή τους. Δίνεται, όμως, και η δυνατότητα συγγραφής κανόνων οι οποίοι έχουν ως στόχο α *επιτρέπουν* τη διέλευση πακέτων που πληρούν συγκεκριμένες προϋποθέσεις.

Οι κανόνες του Snort βρίσκονται κατηγοριοποιημένοι σε διάφορα αρχεία με κατάληξη ".rules", με τ
κάθε αρχείο να περιέχει, συνήθως, κανόνες που συμπεριλαμβάνονται σε ένα συγκεκριμένο τύπο επίθεση
απέναντι στο σύστημα. Για παράδειγμα, το αρχείο "ftp.rules" περιέχει κανόνες που είναι γραμμένοι με στόχ
πακέτα που σχετίζονται με εφαρμογές ftp.

Σε κάθε έκδοση του Snort που είναι διαθέσιμη στο δίκτυο συμπεριλαμβάνονται και συγκεκριμέν
αρχεία κανόνων, ενώ ανά περιόδους γίνονται διαθέσιμα νέα αρχεία κανόνων ώστε να είναι εύκολος
εκσυγχρονισμός του Snort απέναντι σε νέες μορφές επίθεσης. Επιπλέον, ο χρήστης μπορεί να επιλέγει ποι
αρχεία κανόνων θέλει να χρησιμοποιούνται στο σύστημα του κάνοντας απλές τροποποιήσεις σε ένα αρχεί
ρύθμισης (configuration) του Snort. Το σημαντικότερο, όμως, είναι πως ο χρήστης έχει τη δυνατότητα ν
γράφει νέους κανόνες, επιτρέποντας έτσι την προσαρμογή του Snort στις απαιτήσεις του κάθε χρήστη και στ
είδος κίνησης που αναμένεται να υπάρχει στο συγκεκριμένο δίκτυο.

Το Snort χρησιμοποιεί μια απλή γλώσσα περιγραφής κανόνων η οποία όμως προσφέρει πληθώρ
επιλογών που την κάνουν αρκετά ισχυρή και ευέλικτη. Υπάρχουν ορισμένες απλές αρχές που χρειάζεται ν
θυμάται κάποιος που ενδιαφέρεται να γράψει δικούς του κανόνες για το Snort.

Οι περισσότεροι κανόνες γράφονται σε μια μόνο γραμμή. Σε εκδώσεις του Snort πριν από την 1.8 κά
τέτοιο ήταν απαραίτητο, όμως στις νεότερες εκδόσεις είναι εφικτό να έχουμε κανόνες που καταλαμβάνου
περισσότερο από μία γραμμή, αρκεί στο τέλος κάθε ενδιάμεσης γραμμής να βρίσκεται ο χαρακτήρας '\'.

Όλοι οι κανόνες αποτελούνται από δύο λογικές ενότητες, την επικεφαλίδα του κανόνα (ruleheader) κα
τις ρυθμίσεις του κανόνα (ruleoption). Στην επικεφαλίδα του κανόνα περιέχονται οι πληροφορίες για τη
ενέργεια που θα εκτελέσει το Snort σε περίπτωση που επαληθευτεί ο κανόνας, το πρωτόκολλο, οι διευθύνσει
IP του αποστολέα και του παραλήπτη μαζί με τις κατάλληλες μάσκες δικτύου (netmasks) καθώς και οι θύρε
(ports) αποστολέα και παραλήπτη. Το τμήμα των ρυθμίσεων του κανόνα περιλαμβάνει τα μηνύματ
προειδοποίησης (alerts) που θα παράγει το Snort σε περίπτωση επαλήθευσης καθώς και πληροφορίες για τ
ποια τμήματα του εισερχόμενου πακέτου πρέπει να εξεταστούν ώστε να αποφασίσουμε αν το πακέτο είνα
ύποπτο, οπότε το Snort θα δράσει κατάλληλα, ή όχι.

Ένας τυπικός κανόνας του Snort φαίνεται παρακάτω.

```
alert tcp any any -> 192.168.1.0/24 111 (content:"|00 01 86 a5|"; msg:"mountd access";)
```

Οτιδήποτε πριν την πρώτη παρένθεση αποτελεί την επικεφαλίδα του κανόνα, ενώ το τμήμα μέσα στι
παρενθέσεις αποτελεί τις ρυθμίσεις του κανόνα. Στο κομμάτι των ρυθμίσεων του κανόνα, οι λέξεις πο
βρίσκονται αμέσως πριν από ':' είναι οι εντολές ή λέξεις κλειδιά των ρυθμίσεων. Αξίζει να σημειωθεί οτι τ
τμήμα των ρυθμίσεων δεν είναι αναγκαίο για τη δήλωση ενός κανόνα, όμως χρησιμοποιείται για να δίνετα
ένας πιο ακριβής προσδιορισμός των πακέτων για τα οποία θέλουμε να δημιουργηθεί κάποια προειδοποίηση
των πακέτων που θέλουμε να καταγράψουμε ή να απορρίψουμε. Όλα τα προσδιοριστικά στοιχεία ενός κανόν
πρέπει να ισχύουν για ένα πακέτο ώστε να εκτελεστεί η ενέργεια του κανόνα. Αν εξετάσουμε όλα μαζί τ
προσδιοριστικά στοιχεία ενός κανόνα μπορούμε να θεωρήσουμε ότι δημιουργούν μια μεγάλη πρόταση λογικο

ΚΑΙ. Αντίστοιχα, οι διάφοροι κανόνες μέσα σε μία βιβλιοθήκη κανόνων του Snort μπορούν να θεωρηθούν σαν μια μεγάλη πρόταση λογικού Ή.

3.2.2 Ο Βελτιστοποιητής Κανόνων.

Ο Βελτιστοποιητής Κανόνων (RuleOptimizer) αποτελεί σημαντικό κομμάτι του Snort από την έκδοση 2.0 και μετά. Σκοπός της λειτουργίας του Βελτιστοποιητή είναι να επιταχύνει τη λειτουργία του Snort και αυτό το επιτυγχάνει διαχωρίζοντας τους κανόνες σε ξεχωριστές ομάδες με κατάλληλο τρόπο ώστε κάθε εισερχόμενο πακέτο να συγκρίνεται μονάχα με μία ομάδα από κανόνες και η σύγκριση αυτή να μπορεί να γίνεται με τρόπο παράλληλο.

Το Snort χρησιμοποιεί τις παραμέτρους των πρωτοκόλλων για να διαχωρίζει τους κανόνες σε ξεχωριστές ομάδες. Στις παλιότερες εκδόσεις του Snort, χρησιμοποιούταν μια καθαρά παραμετρική αναζήτηση για να εξετάζεται κατά πόσο ένα πακέτο ικανοποιεί τις παραμέτρους μίας ομάδας κανόνων.

Οι κανόνες κατατάσσονταν σε διαφορετικές ομάδες με βάση τέσσερα γενικά χαρακτηριστικά, τέσσερις βασικές παραμέτρους:

1. Η διεύθυνση IP του αποστολέα.
2. Η διεύθυνση IP του παραλήπτη.
3. Οι πιθανές τιμές για τη θύρα του αποστολέα.
4. Οι πιθανές τιμές για τη θύρα του παραλήπτη.

Προκειμένου να βελτιωθεί η ταχύτητα επεξεργασίας των κανόνων, ήταν απαραίτητη η υλοποίηση μεθόδων ομαδικής επεξεργασίας. Το πρόβλημα ήταν οτι η παραδοσιακή επεξεργασία κανόνων στο Snort δεν προσφερόταν για εφαρμογή ομαδικής επεξεργασίας επειδή σε κάθε εισερχόμενο πακέτο αντιστοιχούσαν περισσότερες από μία ομάδες κανόνων. Για να είναι δυνατή η αποδοτική εφαρμογή μεθόδων ομαδικής επεξεργασίας πρέπει για κάθε εισερχόμενο πακέτο να χρειάζεται να εξετάσουμε τους κανόνες που περιέχονται σε μία μόνο ομάδα. Η δημιουργία και επιλογή των ομάδων από κανόνες είναι η αποκλειστική λειτουργία του Βελτιστοποιητή Κανόνων.

Ο Βελτιστοποιητής Κανόνων δημιουργεί ομάδες από κανόνες με μορφή κατάλληλη ώστε να είναι εφικτή η αποδοτική χρήση μεθόδων ομαδικής επεξεργασίας.Για να επιτευχθεί ο σκοπός αυτός, χρειάζεται ο Βελτιστοποιητής να πληρεί δύο προϋποθέσεις:

1. Να δημιουργεί όσο το δυνατόν πιο μικρές και αποδοτικές ομάδες κανόνων.
2. Να δημιουργεί διακριτές ομάδες με τέτοιο τρόπο ώστε για κάθε εισερχόμενο πακέτο να απαιτείται η εξέταση μίας και μόνο ομάδας κανόνων.

3.2.3 Η μηχανή πολλαπλής αναζήτησης.

Στην καρδιά του Snort 2.0 βρίσκεται η Μηχανή Επιθεώρησης Πολλαπλών Κανόνων (HighPerformanceMulti-RuleInspectionEngine), η οποία επωμίζεται το φορτίο της αναζήτησης ύποπτου περιεχόμενου που μπορεί να βρίσκεται μέσα στα εισερχόμενα πακέτα. Η διαδικασία της επιθεώρησης της κίνησης δικτύου για τυχόν επαληθεύσεις των κανόνων εκτελείται σε τρία βήματα:

1. Βελτιστοποίηση των κανόνων για την παραγωγή αποδοτικών ομάδων.

2. Χρήση αλγορίθμων πολλαπλής αναζήτησης για γρήγορη αναζήτηση των ζητούμενων περιεχομένων.

3. Παραμετρικές τεχνικές αναζήτησης που επιτρέπουν πολύπλοκες επιθεωρήσεις παραμέτρων.

Στην πράξη τα εισερχόμενα πακέτα εξετάζονται πρώτα από τον Βελτιστοποιητή κανόνων ώστε ν επιλεγεί η κατάλληλη ομάδα κανόνων με την οποία θα εξεταστεί κάθε πακέτο. Στη συνέχεια η μηχαν πολλαπλής αναζήτησης ανιχνεύει το πακέτο για περιεχόμενα που ταιριάζουν με τους κανόνες που επιλέχθηκαν κατασκευάζει μία λίστα από τους κανόνες που επαληθεύτηκαν και επιλέγει τον καλύτερο κανόνα γι καταγραφή χρησιμοποιώντας ένα απλό σύνολο προτεραιοτήτων.

Η βελτιστοποίηση κανόνων και η πολλαπλή αναζήτηση παρέχουν την υψηλή απόδοση που απαιτείτα στα σύγχρονα δίκτυα υψηλών ταχυτήτων. Η χρήση της παραδοσιακής μεθόδου του Snort για παραμετρικ αναζήτηση επιτρέπει την επέκταση της γλώσσας κανόνων χωρίς να επηρεάζεται η υψηλή απόδοση της μηχανή επιθεώρησης. Ο κατάλληλος συνδυασμός των μεθόδων αυτών επιτρέπει την εφαρμογή της κάθε μεθόδου στο τομέα που αποδίδει καλύτερα, ενώ επιτρέπει στη γλώσσα του Snort να παραμείνει ευέλικτη για μελλοντικέ εξελίξεις.

Η μηχανή πολλαπλής αναζήτησης του Snort μπορεί να επιθεωρεί δίκτυα με ταχύτητες Gigabi ανιχνεύοντας και καταγράφοντας γεγονότα από πολύ μεγάλες ομάδες κανόνων χωρίς να υπάρχουν απώλειε πακέτων.

3.2.4 Προεπεξεργαστές.

Το Snort υποστηρίζει τη λειτουργία διαφόρων προεπεξεργαστών με τους οποίους επεκτείνεται λειτουργικότητα του Snort, ενώ ο χρήστης μπορεί να υλοποιήσει τους δικούς του προεπεξεργαστές και να του συμπεριλάβει με ευκολία στο Snort. Ο κώδικας των προεπεξεργαστών εκτελείται μετά από τη αποκωδικοποίηση του πακέτου και πριν από την εφαρμογή της μηχανής αναζήτησης.

Υπάρχουν διάφοροι προεπεξεργαστές για το Snort, οι οποίοι μπορούν να εκτελούν λειτουργίε διαμόρφωσης των εισερχόμενων πακέτων (για παράδειγμα ο προεπεξεργαστής 'Frag2' συναρμολογε κατακερματισμένα πακέτα IP), να μετράνε την απόδοση του συστήματος ('perfmonitor'), να προστατεύουν απ ορισμένα είδη επιθέσεων (για παράδειγμα ο 'stream4' παρακολουθεί την κατάσταση κάθε ροής TCP κα απορρίπτει πακέτα από ροές που δεν έχουν δημιουργηθεί μέσω 3-wayhandshake) και άλλα.

Επειδή οι προεπεξεργαστές αποτελούν προέκταση της βασικής λειτουργικότητας και όχι απαραίτητ στοιχείο, δε θα αναφερθούμε με περισσότερες λεπτομέρειες σε αυτούς.

3.2.5 Οι τρόποι λειτουργίας του Snort.

Το Snort διαθέτει τους ακόλουθους τρεις διαφορετικούς τρόπους λειτουργίας:

- *Παρατήρησης* (sniffermode): όταν επιλέγεται αυτός ο τρόπος λειτουργίας, το Snort απλά διαβάζει τα εισερχόμενα πακέτα και εμφανίζει στην οθόνη τις επικεφαλίδες των πακέτων ή/και τα δεδομένα τους.
- *Καταγραφής* (packetloggermode): με τη λειτουργία καταγραφής, το Snort απλά καταγράφει όλα τα εισερχόμενα πακέτα. Η καταγραφή των πακέτων μπορεί να γίνει με δύο τρόπους. Ο πρώτος τρόπος είναι λεπτομερής καταγραφή, οπότε τα πακέτα αποθηκεύονται σε διαφορετικούς φακέλους ανάλογα με τη διεύθυνση IP και η καταγραφή των πακέτων γίνεται σε μορφή εύκολα αναγνώσιμη από τον χρήστη. Ο δεύτερος τρόπος καταγραφής των πακέτων είναι σε ένα ενιαίο αρχείο σε μορφή tcpdump, δηλαδή με λίγες πληροφορίες για το πότε και που ήρθε το πακέτο αλλά χωρίς καμία αποκωδικοποίηση. Προφανώς ο δεύτερος τρόπος καταγραφής είναι ο γρηγορότερος.
- *Ανίχνευσης εισβολών δικτύου* (NetworkIntrusionDetection): η πιο ενδιαφέρουσα μέθοδος λειτουργίας του Snort. Αρχικά διαβάζεται το κατάλληλο αρχείο ρυθμίσεων, στο οποίο περιέχονται οι πληροφορίες για τα αρχεία κανόνων που θα χρησιμοποιηθούν, τους προεπεξεργαστές και άλλα.

Αφού ολοκληρωθεί η αρχικοποίηση και γίνει ο διαχωρισμός των κανόνων στις κατάλληλες ομάδες, το σύστημα είναι έτοιμο να δεχτεί τα πακέτα. Κάθε πακέτο που έρχεται αρχικά αποκωδικοποιείται και περνάει από τους προεπεξεργαστές (εάν υπάρχουν). Εφόσον το πακέτο δεν απορριφθεί τότε εξετάζεται για πιθανή επαλήθευση κανόνων. Αν το πακέτο είναι καθαρό και δεν ενεργοποιηθεί ούτε ένας κανόνας τότε το Snort δεν εκτελεί καμία ενέργεια. Σε περίπτωση που επαληθευτούν κανόνες τότε καταγράφεται (συνήθως) το πακέτο ενώ αποθηκεύονται και πληροφορίες σχετικά με τους κανόνες που ενεργοποιήθηκαν. Η μορφή με την οποία καταγράφονται τα πακέτα αλλά και η λεπτομέρεια των πληροφοριών για τους κανόνες που ενεργοποιήθηκαν επιλέγονται ανάλογα με τις απαιτήσεις του χρήστη.

ΚΕΦΑΛΑΙΟ 4

Επίλογος

Τα τελευταία χρόνια με την ραγδαία ανάπτυξη του Internet, παρατηρείται και το φαινόμενο τη αύξησης των επιθέσεων, που έχουν στόχο τα δικτυωμένα συστήματα που το αποτελούν.Το γεγονός αυτ οδήγησε στην ανάγκη παρακολούθησης και ανάλυσης των επιθέσεων αυτών, με σκοπό την έγκαιρη ανίχνευσ και αποτελεσματική αντιμετώπιση τους.Καθώς οι ήδη υπάρχον μηχανισμοί ασφάλειας δεν φαίνεται ν επαρκούν για τον σκοπό αυτό,προέκυψε η εμφάνιση των *Intrusion Detection Systems*, τα οποία πλέο θεωρούνται μίααπαραίτητη προσθήκη στην πολιτική ασφάλειας κάθε δικτύου και κατέχουν έν πρωταγωνιστικό ρόλο στην προστασία από δικτυακές επιθέσεις

Παρόλο που τα IDSs δεν αποτελούν μία ολοκληρωμένη λύση για την πλήρη προστασία ενός δικτύου, συνδυασμός των αποτελεσμάτων τους με τα αποτελέσματα των κλασσικώνμηχανισμών ασφάλειας, όπως τ Firewall, μπορεί να οδηγήσει στον σχηματισμό μιας πιοολοκληρωμένης εικόνας των κινδύνων που προκύπτου από διάφορες δικτυακές απειλές και να συντελέσει στον σχεδιασμό πιο αποτελεσματικών μέτρων ασφάλεια ενός δικτύου.

Τα IDSs βρίσκονται υπό συνεχή εξέλιξη που κυρίως έχει να κάνει με την βελτίωση τηςαποδοτικότητά τους και την εξάλειψη των συμπτωμάτων από *False Positives* και *FalseNegatives* που παρουσιάζουν.Κάθε ID υλοποιεί τρεις θεμελιώδεις λειτουργίες, που έχουν να κάνουν με τις *Πηγές τηςΠληροφορίας* από τις οποίε συλλέγει τα γεγονότα που θα εξετάσει για την ανίχνευση μίαςεπίθεσης, τις *Τεχνικές Ανάλυσης* που χρησιμοποιε για να εξετάσει τα γεγονότα αυτά και τοντρόπο που αντιδρά όταν ανιχνεύσει μία πιθανή επίθεση.

Η κατηγοριοποίηση των IDS προκύπτει από τον διαχωρισμό τους, σύμφωνα με τον τρόπο που το κάθ ένα προσεγγίζει τις παραπάνω λειτουργίες. Τα IDS που κυρίως χρησιμοποιούνται σήμερα, είναι αυτά πο λειτουργούν σε επίπεδο δικτύου (NIDS) και χρησιμοποιούν για την ανάλυση των γεγονότων που εξετάζουν τη τεχνική του *Misuse Detection*, η οποία συνήθως συνδυάζεται κατά κύριο λόγο με την τεχνική το *ProtocolAnomaly Detection* και ίσως με κάποια αποτελέσματα της *Anomaly Detection*.

Η προτεινόμενη πρακτική χρήσης IDS σε ένα δίκτυο, περιλαμβάνει την εφαρμογή NIDS σε ζωτικ σημεία του δικτύου και την εφαρμογή HIDS στα σημαντικότερα συστήματα του. Σε κάθε περίπτωση αποτελεσματική εφαρμογή των IDS, απαιτεί προσεκτική μελέτη και σχεδιασμό, καθώς και την ύπαρξ εξειδικευμένου προσωπικού που θα τα διαχειρίζεται και θα εξετάζει τα αποτελέσματά τους με την απαιτούμεν προσοχή.

Ένα IDS από μόνο του δεν επαρκεί για την ολοκληρωμένη προστασία ενός δικτύου, ενώ η σωστ εφαρμογή των κλασσικών μηχανισμών ασφάλειας πρέπει να θεωρείται δεδομένη. Σήμερα διατίθενται αρκετ και διάφορα IDSs, υλοποιημένα τόσο σε Hardware ή Software, όσο και με την μορφή εμπορικών ή Ope Source εφαρμογών, ενώ η σωστή επιλογή ενός τέτοιου εργαλείου, εξαρτάται από τους στόχους και τις ανάγκε προστασίας κάθε δικτύου.

Στο Κεφάλαιο 3 παρουσιάστηκε το πειραματικό κομμάτι της εργασίας, Η επιλογή της διανομής firewal (IpFire), η εγκατασταση του λογισμικου , tosetup του δικτυου , το configuration καθώς κα το Open Sourc NIDS Snort, το οποίο θεωρείται ένα από τα πιο πετυχημένα και αποτελεσματικά εργαλεία για την Ανίχνευσ Δικτυακών Επιθέσεων.

ΒΙΒΛΙΟΓΡΑΦΙΑ

[1]http://www.pcsteps.gr/1295-technologi-explained-firewall/

[2] http://www.sans.org/reading-room/whitepapers/detection/

[3]http://www.securityfocus.com/

[4] S. Garfinkel, G. Spafford - *"Practical Unix& Internet Security"*, 2nd edition – O' Reilly

[5] Dr. KAREN A. FORCHT, "*Privacy, Confidentiality, Security*" http://lattanze.loyola.edu/lattanze/research/wp0996_031.html#chap5

[6] FREDERICK M. AVOLIO, "*Firewall Are Not Enouth*", Gauntlet FirewallPapers, www.tiw.com/docs/products/gauntlet/FirewallNotEnough.html

[7] KARANJIT SIYAN, "*Internet Firewall and Network Security*", New Riders Publishing, 1995, σελ.174-178, 192-194, 299

[8]"*Network Security White Paper*", 1995, http://www.zeuros.co.uk/cgibin/ whtpap2.html

[9] JOHN P. WACK, "*Keeping your Site Confortably secure: An Introduction to Internet Firewall*", NIST Special Publication 800-10, U.S.Department of Commerce, http://csrc.nist.gov/nistpubs/800-10/main.html

[10] DALVA DAVID, "*Filtering Gateways vs. Application Gateways*", Gauntlet Firewall papers, http://www.tis.com/docs/prodycts/gauntlet/FWComp.html

[11] BASHAM LARRY, "*New Sparks in Firewall Technology*", Infosecurity Magazine, February, ıttp://www.infosecnews.com/articles/9702/article3.htm

[12] TOLLY KEVIN, "*Firewall: Defending the front line*", LAN TIMES Online ıttp://www.lantimes.com/96jun/606s049.html

[13] BRUNO LEE, "*Internet Security: How much is enough?*" ıttp://www.data.com/Roundups/How_Much_is_Enough.html

[14]] DJAHANDARI KELLY, "*An MBone Proxy for an Application Gateway*", TrustedInformation Systems ıttp://www.tis.com/docs/research/network/mbone/mboneabs.html

[15] *Δίκτυα Δημόσιας Χρήσης και Διασύνδεση Δικτύων*.Χρηστος Ι. Μπουρας

[16] *Δικτυα Υπολογιστών*AndrewS. Tanenbaum

[17] www.bbc.co.uk/greek/neww/030821sobig.shtml

[18] cynet.ac.cy/stayalert

ΠΑΡΑΡΤΗΜΑΤΑ

Παράρτημα ΑΚατάλογος IDS

Στον παρακάτω πίνακα αναφέρονται μερικά από τα πιο γνωστά IDS, διαχωρισμένα σύμφωνα με τις πηγέ πληροφορίας που χρησιμοποιούν. Δηλαδήσε NIDSs και HIDSs.

NIDS:

BlackIce Guard (ISS)	http://www.iss.net/products_services/enterprise_protection/rsnetwork/guard.php
BlackIceSentry (ISS)	http://www.iss.net/products_services/enterprise_protection/rsnetwork/sensor.php
BorderGuard	http://www2.stillsecure.com/products/bg/bg1.html
CaptIO	http://www.captusnetworks.com/captio.htm
Cisco Secure IDS (Netranger)	http://www.wheelgroup.com/warp/public/cc/pd/sqsw/sqidsz/index.shtml
CyberTrace	http://www.cybertrace.com/ctids.html
Defense Worx IDS	http://www.defenseworx.com
Dragon	http://www.enterasys.com/products/ids/
E-Trust IDS (Sessionwall3)	http://www3.ca.com/Solutions/Product.asp?ID=163
Hogwash	http://hogwash.sourceforge.net
IntruShield	http://www.intruvert.com/products/sensors.htm
Manhunt	http://www.recourse.com/product/ManHunt
Netprowler	http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=50&PID=10298687&EID=0
Network Flight Recorder	http://www.nfr.com/products/NID/
NID/JID	http://ciac.llnl.gov/cstc/nid/nid.html
nPatrol	http://www.nsecure.net
OneSecure IDP	http://www.onesecure.com/products.html
Sourcefire	http://www.sourcefire.com
RealSecure Network Sensor (BlackICE Sentry)	http://www.iss.net/products_services/enterprise_protection/rsnetwork/sensor.php
RealSecure Guard	http://www.iss.net/products_services/enterprise_protection/rsnetwork/guard.php
SecureNet Pro	http://www.intrusion.com/products/productcategory.asp?lngCatId=4
SHADOW	http://www.nswc.navy.mil/ISSEC/CID/
Shoki	http://shoki.sourceforge.net
Sentrus	http://www.silicondefense.com
Snort	http://www.snort.org/
StealthWatch	http://www.lancope.com
Tamandua	http://www.lancope.com

HIDS:

Abacus Project	http://www.psionic.com/abacus/
Appshield	http://www.sanctuminc.com/solutions/appshield/index.html
auditGUARD	http://www.sanctuminc.com/solutions/appshield/index.html
Dragon Squire	http://www.enterasys.com/ids/squire/
eXpert-BSM	http://www.sdl.sri.com/emerald/releases/eXpert-BSM/
Entercept	http://www.clicknet.com/products/entercept
Entercept WebSE	http://www.clicknet.com/products/WSE/
Enterprise Guard	http://www.rsodata.com/products/eguard/overview.html
E-Trust Audit	http://www.cai.com/solutions/enterprise/etrust/audit/
praesidium (HP)	http://www.hp.com/products1/unix/operating/security/
Intruder Alert	http://enterprisesecurity.symantec.com/products/ p roducts.cfm?ProductID=48&PID=12 812915&EID=0
LANguard	http://www.gfisoftware.com/stats/adentry.asp?adv=158&loc=1
LIDS	http://www.lids.org/about.html
Logsurfer	http://www.cert.dfn.de/eng/logsurf/
NFR HID (Centrax)	http://www.nfr.com/products/HID/
Precis	http://www.bellevue.prc.com/precis
RealSecure OS Sensor	http://www.iss.net/products_services/enterpriseprotection/rsserver/protector_server.p hp
Secure Host Series	http://www.cert.dfn.de/eng/logsurf/
SNARE	http://www.intersectalliance.com/projects/Snare/index.html
SNIPS	http://www.navya.com/software/snips/
Stormwatch	http://www.okena.com/areas/products/products_stormwatch.html
Swatch	ftp://ftp.stanford.edu/general/security-tools/swatch

Παράρτημα ΒΣυνοδευτικό CD-ROM

Περιεχόμενα:

Πτυχιακή Εργασία – Κείμενο

Πτυχιακή Εργασία – Παρουσίαση

Διανόμη IPFire