ΣΧΟΛΗ Σ.Δ.Ο. ΑΤΕΙ ΠΑΤΡΩΝ
ΤΜΗΜΑ ΕΠΙΧΕΙΡΗΜΑΤΙΚΟΥ ΣΧΕΔΙΑΣΜΟΥ &
ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Πτυχιακή Εργασία: «Πυρότοιχοι (FIREWALLS) . Τα τείχη προστασίας κάθε σύγχρονου Η/Υ .»

Επιβλέπων : κ. Α. Μπακάλης
Φοιτητική Ομάδα: Αγγέλη Γεωργία
Υφαντή Μαρία

Firewalls

ΠΑΤΡΑ 2005

Περιεχόμενα

1. Γενικά

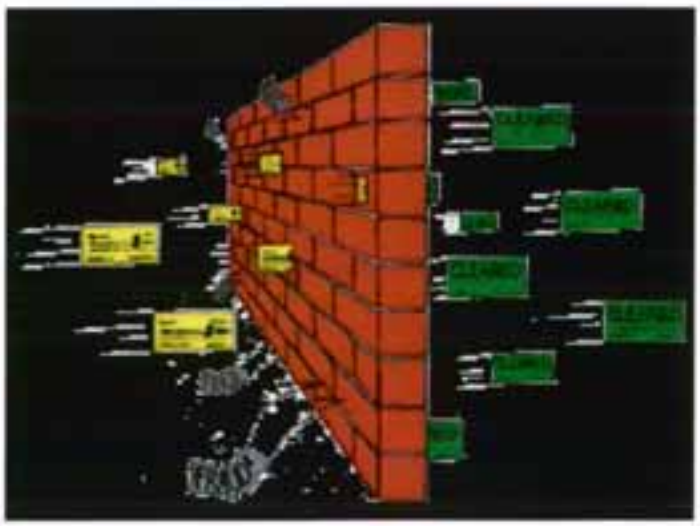
Το διαδίκτυο έχει καταστήσει μεγάλα ποσά πληροφοριών διαθέσιμα στο μέσο χρήστη υπολογιστών στο σπίτι, στην επιχείρηση και στην εκπαίδευση. Για πολλούς ανθρώπους, η απόκτηση πρόσβασης σε αυτές τις πληροφορίες δεν είναι πλέον μόνο ένα πλεονέκτημα, είναι θεμελιώδης ανάγκη. Όμως, η σύνδεση ενός ιδιωτικού δικτύου με το διαδίκτυο μπορεί να εκθέσει τα κρίσιμα ή εμπιστευτικά δεδομένα στην κακόβουλη επίθεση από οπουδήποτε στον κόσμο. Οι χρήστες που συνδέουν τους υπολογιστές τους με το διαδίκτυο πρέπει να γνωρίζουν αυτούς τους κινδύνους, τις επιπτώσεις τους και πώς να προστατεύσουν τα δεδομένα τους και τα κρίσιμα συστήματά τους. Τα Firewalls μπορούν να προστατεύσουν και τους μεμονωμένους υπολογιστές και τα εταιρικά δίκτυα από την εχθρική διείσδυση από το διαδίκτυο, αλλά πρέπει να γίνει κατανοητός ο τρόπος λειτουργίας τους ώστε να χρησιμοποιηθούν σωστά.

2. Εισαγωγή

Ο όρος firewall έχει επικρατήσει τα τελευταία χρόνια σαν ένας από τους πιο καλούς τρόπους για να διατηρήσει κάποιος ασφαλή τα δεδομένα του στον υπολογιστή του, όταν αυτός είναι συνδεδεμένος στο διαδίκτυο. Το firewall, ή αλλιώς ο τοίχος της φωτιάς, είναι ένα λογισμικό το οποίο αναλαμβάνει να ελέγχει όλες τις πληροφορίες που φθάνουν στον υπολογιστή μας από τον "έξω" κόσμο. Το firewall μπορεί να είναι εκτός από software και hardware, μια συσκευή δηλαδή που τοποθετείται στην σύνδεση του ηλεκτρονικού υπολογιστή με το διαδίκτυο.

Στην περίπτωση που έχουμε εγκαταστήσει ένα λογισμικό firewall στον προσωπικό μας υπολογιστή τότε με αυτό μπορούμε να καθορίσουμε από ποιούς υπολογιστές και με ποιούς τρόπους θα δεχόμαστε πληροφορίες. Αυτό επιτυγχάνεται με την χρήση διάφορων φίλτρων τα οποία αναλύουν τα εισερχόμενα πακέτα και ανάλογα με τις οδηγίες που υπάρχουν τα αφήνουν να περάσουν ή όχι. Η μεγάλη σημασία του firewall έγκειται στο ότι δεν μπορούμε να γνωρίζουμε απόλυτα τι λογισμικά υπάρχουν εγκατεστημένα στον υπολογιστή μας και ποιές "πόρτες" είναι ανοιχτές. Για παράδειγμα ο υπολογιστής μας μπορεί να είναι μολυσμένος από ένα worm το οποίο δίνει τη δυνατότητα σε κάποιον άλλο υπολογιστή να χρησιμοποιεί το CPU μας.

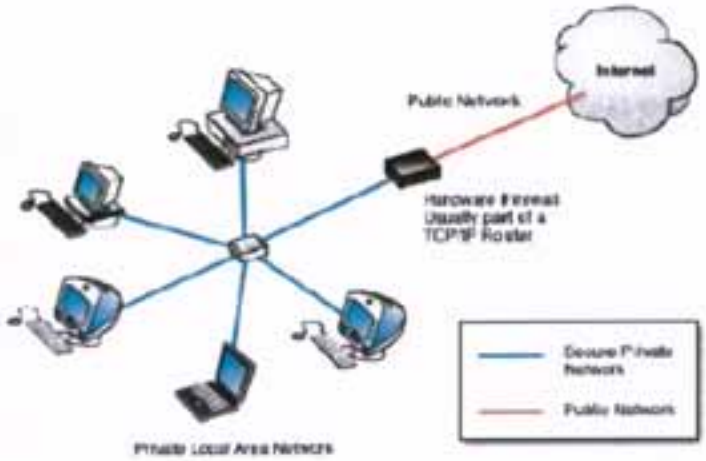
Το firewall δηλαδή είναι αυτό που συγκεντρώνει τον πλήρη έλεγχο των πακέτων που εισέρχονται στον υπολογιστή αποτελώντας ουσιαστικά έναν πύργο ελέγχου της πληροφορίας. Βέβαια η σημασία του firewall είναι πολύ πιο μεγάλη όταν πίσω από αυτό δεν υπάρχει μόνο ένας υπολογιστής αλλά μια μεγάλη ομάδα υπολογιστών π.χ. μια εταιρία, η οποία εμπιστεύεται το firewall για όλα τα πακέτα που καταφθάνουν σε αυτήν.



Ένα Firewall προστατεύει τους δικτυωμένους υπολογιστές από την σκόπιμη εχθρική διείσδυση που θα μπορούσε να οδηγήσει σε συμβιβασμούς στην εμπιστευτικότητα

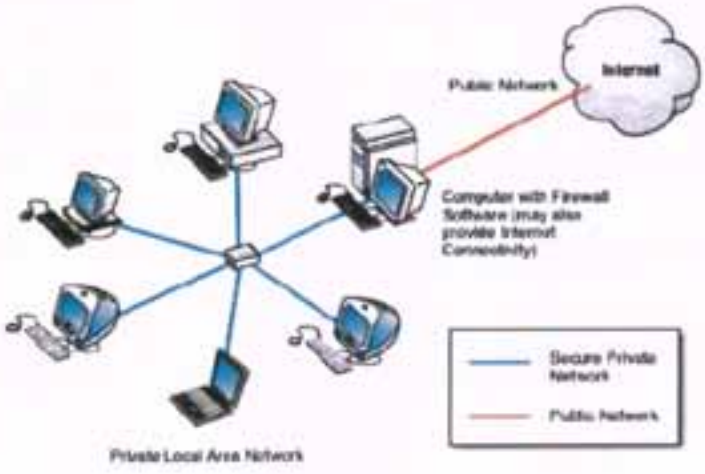
(confidentiality) ή σε καταστροφή δεδομένων ή και σε άρνηση της υπηρεσίας (Denial of Service-DoS). Μπορεί να είναι μια συσκευή υλικού (σχήμα 1) ή ένα πρόγραμμα λογισμικού (σχήμα 2) που τρέχει σε έναν ασφαλή host υπολογιστή. Σε καθεμία περίπτωση, πρέπει να έχει τουλάχιστον δύο διεπαφές (interfaces) δικτύων, μια για το δίκτυο το οποίο προορίζεται να προστατεύσει, και μια για το δίκτυο στο οποίο εκτίθεται. Το firewall τοποθετείται στο σημείο συνδέσεων ή στην πύλη (Gateway) μεταξύ των δύο δικτύων, συνήθως ενός ιδιωτικού δικτύου και ενός δημόσιου δικτύου όπως το διαδίκτυο. Τα πρώτα Firewalls ήταν απλά δρομολογητές. Ο όρος Firewall προέρχεται από το γεγονός ότι με την κατάτμηση ενός δικτύου στα διαφορετικά φυσικά υποδίκτυα, περιορίζεται η ζημιά που θα μπορούσε να διαδοθεί από ένα υποδίκτυο στο άλλο λειτουργώντας ακριβώς όπως οι αντιπυρικές πόρτες (firedoors) ή οι αντιπυρικές ζώνες (firewalls).

Στο παρακάτω σχήμα φαίνεται ένα firewall που δημιουργείται από υλικό (hardware firewall) και το οποίο προστατεύει ένα τοπικό δίκτυο.



Σχήμα 1

Στο παρακάτω σχήμα παρουσιάζεται η χρήση λογισμικού ως firewall για την προστασία του δικτύου.


Internet
Public Network
Computer with Firewall
Software (may also
provide Internet
Connectivity)
Secure Private
Network
Public Network
Private Local Area Network

Σχήμα 2

3. Λόγοι χρησιμοποίησης των Firewalls

Πριν εξετάσουμε την τεχνολογία των Firewalls είναι σκόπιμο να αναφερθούν οι λόγοι που επέβαλλαν τη χρησιμοποίηση τους.

α. Η "ανοικτή" αρχιτεκτονική του Internet μαζί με τις αυξανόμενες υπηρεσίες που προσφέρει στους χρήστες του. Δεν πρέπει να ξεχνάμε ότι το Internet δεν σχεδιάστηκε να είναι ασφαλές. Τα πρωτόκολλα TCP/IP σχεδιάστηκαν προκειμένου να είναι αξιόπιστα και όχι με κριτήριο την ασφάλεια..

β. Η ταυτόχρονη αύξηση του αριθμού των εισβολέων τυχαίων ή καλά οργανωμένων παράλληλα με την αύξηση των χρηστών του Internet.

γ. Η ολοένα και μεγαλύτερη ανάγκη δικτύωσης των Η/Υ ενός οργανισμού ή μιας επιχείρησης με την παράλληλη χρησιμοποίηση των υπηρεσιών που προσφέρονται από το Internet.

δ. Η ανάγκη ασφάλειας συγκεκριμένου τμήματος ενός τοπικού δικτύου (Intranet)από το υπόλοιπο δίκτυο του οργανισμού ή της εταιρείας.

ε. Η προστασία των χρηστών από τους ίδιους τους χρήστες. (αμελείς, δυσαρεστημένοι, ή από άλλη εταιρεία πληρωμένοι υπάλληλοι) είναι μερικοί από τους λόγους που επιβάλλουν την τοποθέτηση ενός ή και παραπάνω firewalls σε έναν οργανισμό ή επιχείρηση.

στ. Σύμφωνα με σοβαρή αναφορά από το US DoD (Department of Defense) το 1997 το 88% των υπολογιστών τους παρείχαν εύκολη πρόσβαση σε οποιαδήποτε μη εξουσιοδοτημένη προσπέλαση. Το χειρότερο όμως ήταν ότι στο 96% των περιπτώσεων των συστημάτων που είχαν παραβιασθεί, οι υπεύθυνοι ασφαλείας ήταν ανήμποροι να ανιχνεύσουν την εισβολή.

ζ. Στο 3° Ετήσιο Συνέδριο Information Week/Ernst & Young μία στις πέντε από τις εταιρείες που συμμετείχαν παραδέχθηκαν ότι οι εισβολείς είχαν παραβιάσει τα εταιρικά τους δίκτυα ή είχαν προσπαθήσει να τα παραβιάσουν. Αυτό όμως που επιπώθηκε ήταν ότι οι εισβολείς δεν ήταν "παιδιά" με αυξημένες ικανότητες και με σκοπό την προσωπική τους ικανοποίηση, αλλά οργανωμένοι πληρωμένοι hackers, μεσίτες πληροφοριών με σκοπό την βιομηχανική κατασκοπεία, ακόμη και ξένες κυβερνήσεις. Μεγάλοι οίκοι S/W & H/W που ειδικεύονται και προωθούν στην αγορά λύσεις ασφαλούς επικοινωνίας συζητούν ανοικτά μεταξύ τους προκειμένου να βρούν λύσεις αφού τα ενδεχόμενα οφέλη επιχειρήσεων που χρησιμοποιούν το Internet σε σύγκριση με dedicated ιδιωτικά δίκτυα είναι αναμφισβήτητα πολύ μεγαλύτερα.

Αυτό που πρέπει να γίνει κατανοητό και καθιστά επιβεβλημένη τη χρήση των Firewalls σαν ένα απαραίτητο στοιχείο της ασφάλειας του δικτύου και κατά συνέπεια των πολύτιμων δεδομένων τους από τις Δκσεις των οργανισμών και των εταιρειών που έχουν σύνδεση με το Internet αλλά και για αυτές που θέλουν να προστατεύσουν ένα

τμήμα του δικτύου τους (π.χ ενός WAN) είναι ότι το ερώτημα δεν εστιάζεται στο AN αλλά στο ΠΟΤΕ οι ανεπιθύμητες επιθέσεις θα συμβούν.

4. Ηλεκτρονικές Απειλές

4.1. Γενικά

Στα χρόνια πριν από την εξάπλωση της χρήσης των ηλεκτρονικών υπολογιστών ως εργαλεία επεξεργασίας της πληροφορίας, η διασφάλιση της μυστικότητας, ακεραιότητας και διαθεσιμότητας των σημαντικών πληροφοριών ενός οργανισμού γινόταν μέσω της φυσικής προστασίας των, καθώς και μέσω κάποιων διαδικασιών και κανονισμών ασφάλειας. Για παράδειγμα, τα ευαίσθητα έγγραφα κλείνονταν σε ντουλάπες ή χρηματοκιβώτια στιβαρής κατασκευής τα οποία προστατεύονταν από κλειδαριές, ενώ μόνον εξουσιοδοτημένο προσωπικό το οποίο επιλεγόταν αυστηρά, είχε πρόσβαση σε αυτά. Τις τελευταίες δεκαετίες, δύο γεγονότα έχουν αλλάξει δραστικά τις ανάγκες των οργανισμών σε σχέση με την ασφάλεια των πληροφοριών.

Το πρώτο γεγονός είναι η εισαγωγή των υπολογιστών ως εργαλεία αποθήκευσης και επεξεργασίας της πληροφορίας. Η προστασία της πληροφορίας ανάγεται πλέον στην προστασία των αρχείων των υπολογιστών στα οποία είναι αποθηκευμένη η πληροφορία, στον έλεγχο της πρόσβασης στα αρχεία αυτά, καθώς και στην προστασία των προγραμμάτων εκείνων που μπορούν να απειλήσουν την ασφάλεια των αρχείων αυτών. Ο όρος που χρησιμοποιείται για να περιγράψει το σύνολο των εργαλείων και διαδικασιών που έχουν σχεδιασθεί για την προστασία των ηλεκτρονικών δεδομένων είναι "ασφάλεια υπολογιστών" (computer security).

Το δεύτερο γεγονός το οποίο επηρέασε δραστικά τις ανάγκες σε ασφάλεια της πληροφορίας είναι η εισαγωγή των κατανεμημένων συστημάτων και η χρήση δικτύων και τηλεπικοινωνιακών συστημάτων για την μεταφορά δεδομένων μεταξύ υπολογιστών. Ο όρος "ασφάλεια δικτύων" (network security) αναφέρεται στα μέτρα προστασίας των δεδομένων κατά την μεταφορά τους μέσω του δικτύου διασύνδεσης.

4.2. Έρευνα για την άγνοια των χρηστών του Διαδικτύου

Μελέτη που διεξήχθη στις Ηνωμένες Πολιτείες υποδεικνύει ότι σε συντριπτική πλειοψηφία οι χρήστες οικιακών υπολογιστών δεν γνωρίζουν ότι το σύστημά τους έχει μολυνθεί από επιβλαβή προγράμματα.

Η μελέτη, η οποία έχει χρηματοδοτηθεί από την «America Online» (AOL) και την «Εθνική Ένωση Ασφάλειας στον Κυβερνοχώρο» (NCSA) διαπιστώνει ότι οι περισσότεροι άνθρωποι που έχουν πρόσβαση στο διαδίκτυο μέσω του υπολογιστή που έχουν στο σπίτι τους είναι σε πολύ μεγάλο ποσοστό απροστάτευτοι απέναντι σε κάθε είδους ηλεκτρονικών απειλών και σε μεγάλο βαθμό έχουν άγνοια των κινδύνων. Οι δύο εταιρείες που συνεργάστηκαν για την πραγματοποίηση της έρευνας, η AOL και η NCSA, έστειλαν τεχνικούς σε 329 σπίτια προκειμένου να εξετάσουν την κατάσταση των εκεί εγκατεστημένων υπολογιστών. «Κανένας καταναλωτής δεν πρόκειται να περπατήσει στο δρόμο κουνώντας στο χέρι ένα μάτσο χαρτονομίσματα, ούτε πρόκειται να αφήσει το πορτοφόλι του σε κοινή θέα σε δημόσιο χώρο, όμως είναι περισσότεροι από αρκετοί, εκείνοι που κάνουν την αντίστοιχη κίνηση όταν είναι συνδεδεμένοι στο διαδίκτυο», δήλωσε η Tatiana Gau, συνεργάτης της AOL, περιγράφοντας την κατάσταση με τα λόγια αυτά σε μια επίσημη αναφορά.

«Χωρίς τα βασικά μέτρα προστασίας, όπως τα προγράμματα προστασίας από ιούς (antivirus), τα προγράμματα εντοπισμού και καταστροφής των ηλεκτρονικών κατασκόπων (spyware) και το λογισμικό προστασίας (firewall), οι καταναλωτές αφήνουν τις προσωπικές και οικονομικές τους πληροφορίες σε κίνδυνο», συμπληρώνει η ίδια. Περίπου τρεις στους πέντε καταναλωτές δεν γνωρίζουν τη διαφορά ανάμεσα σε ένα πρόγραμμα εντοπισμού και «απενεργοποίησης» ηλεκτρονικών ιών (antivirus) και στο λογισμικό που ελέγχει ποια προγράμματα έχουν πρόσβαση στο διαδίκτυο (firewall). Επιπλέον, τα δύο τρίτα των χρηστών που συμμετείχαν στην έρευνα δεν είχαν στον υπολογιστή τους εγκατεστημένο κανένα λογισμικό τύπου firewall. Σα να μην έφτανε αυτό, ενώ το 85% είχε εγκαταστήσει αντιβιοτικά προγράμματα, τα δύο τρίτα εξ αυτών δεν είχαν «ενημερώσει» το λογισμικό επί μια ολόκληρη εβδομάδα. Το αποτέλεσμα; Σύμφωνα με τα στοιχεία που συνέλεξε η έρευνα, περίπου ένας στους πέντε υπολογιστές που εξετάστηκαν είχε μολυνθεί από κάποιον ιό, ο οποίος παρέμενε ενεργός στο σύστημα.

Επίσης, από τους 329 υπολογιστές που εξετάστηκαν κατά τη διάρκεια της μελέτης, η συντριπτική πλειοψηφία (περίπου 90%) ήταν προσβάσιμη από τρίτους, ενώ οι ιδιοκτήτες των υπολογιστών δεν είχαν καν την υπόνοια ότι μπορεί να συμβαίνει κάτι τέτοιο. Οι «ψηφιακοί εισβολείς» μπορούν να υποκλέψουν σημαντικές προσωπικές πληροφορίες ή οικονομικά στοιχεία και πολλοί από αυτούς καταφέρνουν να αποκτήσουν πλήρη έλεγχο του συστήματος.

Η έρευνα δημοσιεύτηκε στο πλαίσιο του «Εθνικού Μήνα Επαγρύπνησης για θέματα κυβερνο-ασφάλειας» που έχει κηρυχθεί από την «Εθνική Ένωση Ασφάλειας στον Κυβερνοχώρο». Να σημειώσουμε ότι η Ένωση αποτελεί μια κοινή προσπάθεια της βιομηχανίας, της ακαδημαϊκής κοινότητας και της Κυβέρνησης.

«Προστατεύοντας την ασφάλεια της τεχνολογίας μας σημαίνει να προστατεύσουμε τον υπολογιστή κάθε Αμερικανού ξεχωριστά», εξηγεί ο Dan Caprio, ειδικός σε θέματα τεχνολογικής πολιτικής του αμερικανικού υπουργείου Εμπορίου. «Αυτή η έρευνα τονίζει απλώς πόσο σημαντική είναι για κάθε Αμερικανό ως άτομο να εκλάβει την κυβερνο-

ασφάλεια ως ένα σημαντικό ζήτημα, όχι μόνο ως ένα θέμα ατομικής, αλλά και εθνικής ασφάλειας» Ένα από τα σημαντικότερα ζητήματα που θέτει η έρευνα είναι αυτό ακριβώς, ότι οι περισσότεροι χρήστες οικιακών υπολογιστών δεν αντιλαμβάνονται σε όλη τους την έκταση τους κινδύνους που περιλαμβάνονται στη σύνδεση του υπολογιστή τους με το διαδίκτυο, και κυριότερα δεν γνωρίζουν πώς μπορούν να εξασφαλίζουν τη σωστή προστασία του συστήματός τους.

4.3 Μορφές Απειλών

Οι διαφορετικές μορφές απειλών της ασφάλειας ενός υπολογιστή ή ενός δικτύου μπορούν να χαρακτηριστούν καλύτερα, αν ληφθεί υπ' όψη ότι ο σκοπός ενός υπολογιστή είναι η παροχή πληροφορίας. Γενικά υπάρχει μία ροή πληροφορίας από μία πηγή, όπως π.χ. ένα αρχείο ή μία περιοχή μνήμης, σε κάποιον προορισμό, όπως ένα άλλο αρχείο ή μία εφαρμογή κάποιου χρήστη. Με δεδομένη αυτή την θεώρηση, είναι δυνατές 4 κατηγορίες απειλών:

1. διακοπή (interruption): κάποιος πόρος του συστήματος καταστρέφεται ή καθίσταται μη χρησιμοποιήσιμος ή διαθέσιμος. Αυτού του τύπου η απειλή στρέφεται κατά της διαθεσιμότητας του συστήματος.

Παραδείγματα τέτοιων απειλών είναι η καταστροφή κάποιας συσκευής του δικτύου, όπως ο σκληρός δίσκος ενός server, το κόψιμο κάποιας γραμμής του δικτύου, ή η διακοπή τροφοδοσίας ενός δρομολογητή.

2. *υποκλοπή (interception):* πρόκειται για απειλή κατά της μυστικότητας της πληροφορίας, όπου κάποιος μη εξουσιοδοτημένος χρήστης, πρόγραμμα ή υπολογιστής αποκτά πρόσβαση στην πληροφορία με δυνατότητα καταγραφής της. Παραδείγματα αποτελούν η παρακολούθηση μίας γραμμής του δικτύου και η απαγορευμένη αντιγραφή αρχείων ή προγραμμάτων.

3. *τροποποίηση (modification):* πρόκειται για απειλή κατά της ακεραιότητας του συστήματος, όπου κάποιος μη εξουσιοδοτημένος χρήστης, πρόγραμμα ή υπολογιστής αποκτά πρόσβαση στο σύστημα με δυνατότητα τροποποίησης.

Παραδείγματα αποτελούν η αλλαγή των δεδομένων ενός αρχείου, η τροποποίηση ενός προγράμματος, η έναρξη κάποιας process και η τροποποίηση του περιεχομένου ενός μηνύματος που μεταδίδεται μέσω του δικτύου.

4. *πλαστογράφηση (fabrication):* πρόκειται για απειλή κατά της ακεραιότητας του συστήματος, κατά την οποία εισάγεται κάποιο πλαστό αντικείμενο στο σύστημα. Παραδείγματα τέτοιας απειλής είναι η αποστολή ενός μηνύματος από κάποιον υποτιθέμενο αποστολέα (fake e-mail) και η πρόσθεση εγγραφών σε κάποιο αρχείο.

Οι πόροι του δικτύου, όπως αυτό ορίσθηκε παραπάνω, αποτελούνται από ενεργά στοιχεία, παθητικά στοιχεία, λογισμικό και δεδομένα (static data, traffic data). Συνεπώς στα πλαίσια της ανάπτυξης μίας στρατηγικής για την ασφάλεια όλων των πόρων του δικτύου το ζητούμενο είναι και η ασφάλεια υπολογιστών και η ασφάλεια δικτύου. Στη συνέχεια θα παρουσιάσουμε τις απειλές κατά της ασφάλειας κάθε κατηγορίας πόρων του δικτύου.

4.3.1 Απειλές κατά των Ενεργών Στοιχείων

Η κύρια απειλή κατά των ενεργών στοιχείων του δικτύου (routers, hubs, servers, workstations, hosts, printers κλπ) αφορά στην διαθεσιμότητα των στοιχείων αυτών.

Ενέργειες όπως:

1. η σκόπιμη ή ακούσια καταστροφή ή φθορά

2. η κλοπή του στοιχείου ή τμήματος αυτού

3. η σκόπιμη ή ακούσια διακοπή τροφοδοσίας

αποτελούν τις πιο συνηθισμένες απειλές κατά του υλικού ενός δικτύου.

4.3.2 Απειλές κατά των Παθητικών Στοιχείων

Το παθητικό υλικό του δικτύου π.χ του Πανεπιστημίου αποτελείται από τις πρίζες του δικτύου, τα καλώδια χαλκού και οπτικών ινών και τους πίνακες μικτονόμησης (patch panels) και χρησιμοποιείται για την μεταφορά δεδομένων. Όπως και για τα ενεργά στοιχεία, η κύρια απειλή αφορά στην διαθεσιμότητα των στοιχείων και μπορεί να προκύψει από πράξεις όπως:

1. η σκόπιμη ή ακούσια καταστροφή ή φθορά

2. η κλοπή

4.3.3 Απειλές κατά των Κινούμενων Δεδομένων

Οι απειλές κατά της ασφάλειας των κινούμενων δεδομένων (traffic data) αφορούν στην ακεραιότητα, μυστικότητα και διαθεσιμότητα των δεδομένων και μπορούν να χωρισθούν σε δύο κατηγορίες:

Α. Απειλές Παθητικής Φύσης

Απειλούν την μυστικότητα των δεδομένων και υλοποιούνται με την παρακολούθηση των δεδομένων (π.χ. μέσω ειδικών προγραμμάτων packet sniffers) με σκοπό την απόκτηση πληροφοριών. Για παράδειγμα ο χρήστης ενός PC μπορεί να χρησιμοποιήσει ένα τέτοιο πρόγραμμα για να παρακολουθεί όλα τα πακέτα που εκπέμπονται στο τοπικό του δίκτυο (Ethernet subnet). Τέτοιου είδους ενέργειες είναι πολύ δύσκολο να αποκαλυφθούν διότι δεν προκαλούν αλλαγή στα δεδομένα και δεν επηρεάζουν την λειτουργία του δικτύου.
Η παρακολούθηση των δεδομένων είναι δυνατή και μέσω παρακολούθησης των καλωδιώσεων χαλκού του δικτύου (wire-tapping) ή των τηλεφωνικών συνδέσεων πρόσβασης στο δίκτυο.

Β. Απειλές Ενεργητικής Φύσης

Τέτοιου είδους απειλές έχουν σαν στόχο την τροποποίηση των κινούμενων δεδομένων ή την δημιουργία πλαστών δεδομένων και απειλούν τόσο την μυστικότητα, όσο την διαθεσιμότητα και την ακεραιότητα των δεδομένων. Είναι δυνατή μία περαιτέρω κατηγοριοποίηση τέτοιων απειλών ως εξής:

1. πρόκληση τροποποίησης της ροής των πακέτων δεδομένων (message-stream modification), όπου ένα τμήμα του κανονικού μηνύματος τροποποιείται, ή κάποια μηνύματα καθυστερούν, επαναλαμβάνονται, ή τροποποιείται η διαδοχή τους για να προκληθεί κάποιο αποτέλεσμα.

2. πρόκληση άρνησης παροχής υπηρεσιών (denial of service), κατά την οποία παρεμποδίζεται η κανονική χρήση των πόρων του δικτύου. Μία τέτοια μορφή επίθεσης είναι η υπερφόρτωση του δικτύου με πακέτα με αποτέλεσμα την επιβράδυνση ή και διακοπή της λειτουργίας του. Άλλο παράδειγμα είναι η εξάλειψη μηνυμάτων που απευθύνονται σε κάποιον συγκεκριμένο αποδέκτη, όπως για παράδειγμα σε ένα πρόγραμμα που εκτελεί την υπηρεσία ελέγχου ασφάλειας (security audit service).

3. μεταμφίεση (masquerade) κατά την οποία ο εισβολέας τροποποιεί τα δεδομένα με στόχο να ξεγελάσει τους μηχανισμούς ασφάλειας του δικτύου και να θεωρηθεί ως εξουσιοδοτημένος ή έμπιστος χρήστης. Τέτοια παραδείγματα είναι η αλλαγή της IP διεύθυνσης πακέτων του εξωτερικού εισβολέα, έτσι ώστε το σύστημα firewall να νομίσει ότι τα πακέτα έρχονται από το εσωτερικό δίκτυο, ή η ηχογράφηση κάποιας συνομιλίας ελέγχου αυθεντικότητας (authentication) μεταξύ ενός εξουσιοδοτημένου χρήστη και του συστήματος και κατόπιν η χρήση της από τον εισβολέα.

4.3.4 Απειλές κατά των Αποθηκευμένων Δεδομένων

Όπως και για τα κινούμενα δεδομένα, οι απειλές κατά της ασφάλειας των δεδομένων που είναι αποθηκευμένα σε αρχεία αφορούν στην ακεραιότητα, μυστικότητα και διαθεσιμότητα των δεδομένων. Αυτό που διαφέρει είναι οι μηχανισμοί πρόσβασης στα δεδομένα αυτά, μιας και βρίσκονται αποθηκευμένα στους χώρους μόνιμης αποθήκευσης κάποιων ενεργών στοιχείων.

Η απειλή κατά της μυστικότητας των δεδομένων έγκειται στην πρόσβαση στα αρχεία που τα περιέχουν από μη εξουσιοδοτημένους χρήστες, στους οποίους δίνεται η δυνατότητα να διαβάσουν τα αρχεία αυτά. Η διαθεσιμότητα των αρχείων απειλείται από την εσκεμμένη ή ακούσια διαγραφή των αρχείων. Τέλος, η ακεραιότητα των αρχείων απειλείται από την αλλαγή των χαρακτηριστικών τους (file attributes), την αλλαγή του περιεχομένου τους, καθώς και από την κακόβουλη δημιουργία νέων αρχείων.

4.4 Είδη και κίνητρα εισβολέων

Υπάρχουν δύο ειδών εισβολείς. Οι παθητικοί εισβολείς, οι οποίοι απλώς θέλουν να διαβάσουν αρχεία για τα οποία δεν έχουν αυτού του είδους την εξουσιοδότηση. Οι ενεργοί εισβολείς είναι πιο κακόβουλοι, και θέλουν να κάνουν μη εξουσιοδοτημένες αλλαγές σε δεδομένα. Κατά το σχεδιασμό της ασφάλειας ενός συστήματος από τους εισβολείς, πρέπει να γνωρίζουμε το είδος και τα κίνητρα του εισβολέα από τον οποίο θέλουμε να προστατευθούμε. Ορισμένες κοινές κατηγορίες είναι:

1.Περίεργοι χρήστες χωρίς τεχνικές γνώσεις. Πολλοί άνθρωποι έχουν στα γραφεία τους τερματικά σε συστήματα διαμερισμού χρόνου (timesharing systems), και εξαιτίας της ανθρώπινης φύσης, ορισμένοι από αυτούς θα διαβάσουν το ηλεκτρονικό ταχυδρομείο και τα αρχεία άλλων ανθρώπων, αν δεν υπάρχει κανένας φραγμός για αυτό.

2.Προσπάθεια προσπέλασης από εσωτερικούς εισβολείς. Οι φοιτητές, οι προγραμματιστές συστημάτων, οι χειριστές και το λοιπό τεχνικό προσωπικό, συχνά θεωρούν ως προσωπική πρόκληση την παράκαμψη της ασφάλειας του τοπικού υπολογιστικού συστήματος. Συχνά έχουν υψηλά προσόντα και είναι αποφασισμένοι να αφιερώσουν ένα σημαντικό μέρος του χρόνου τους στην προσπάθεια αυτή.

3.Ηθελημένες προσπάθειες για οικονομικά οφέλη. Ορισμένοι προγραμματιστές που εργάζονται σε τράπεζες έχουν προσπαθήσει να μπουν σε κάποιο σύστημα τράπεζας με σκοπό να κλέψουν από αυτή. Οι τρόποι ποικίλλουν, από την αλλαγή του λογισμικού ώστε να περικόπτει αντί να στρογγυλεύει τους τόκους, την κράτηση ενός κλάσματος της δραχμής για τους εαυτούς τους, την οικειοποίηση λογαριασμών που μένουν αχρησιμοποίητοι για χρόνια, μέχρι και τον εκβιασμό («Πληρώστε με αλλιώς θα καταστρέψω όλες τις εγγραφές της τράπεζας»).

4. Εμπορική ή στρατιωτική κατασκοπία. Η κατασκοπία συνίσταται σε μια σοβαρή και με καλή οργάνωση προσπάθεια ενός ανταγωνιστή ή μιας ξένης χώρας με στόχο να κλαπούν προγράμματα, εμπορικά μυστικά, ευρεσιτεχνίες, τεχνολογία, σχέδια κυκλωμάτων, σχέδια για μάρκετινγκ κ.ο.κ. Συχνά αυτή η προσπάθεια περιλαμβάνει παρακολούθηση τηλεπικοινωνιακών γραμμών ή ακόμα τοποθέτηση κεραιών κατευθυνόμενων προς τον υπολογιστή ώστε να λαμβάνουν τις ηλεκτρομαγνητικές του ακτινοβολίες.

4.5 Ο Δούρειος Ίππος

Δούρειος Ίππος είναι ένα κανονικό γενικά πρόγραμμα που εκτελεί σωστά τη λειτουργία του, αλλά εκτός από αυτήν εκτελεί και άλλες άσχημες για το χρήστη λειτουργίες. Για παράδειγμα, αν κάποιος εισβολέας θελήσει να κλέψει τα αρχεία κάποιου άλλου χρήστη μπορεί να δημιουργήσει ένα αντίγραφο του πρωτογενούς κώδικα του κειμενογράφου (editor), να τον μεταβάλλει έτσι ώστε να κλέβει αρχεία (αλλά να συνεχίσει να δουλεύει τέλεια ως κειμενογράφος) και να τον τοποθετήσει σε κάποιο κατάλληλο κατάλογο ώστε να τον εκτελέσει το θύμα αντί για τον πραγματικό κειμενογράφο. Την επόμενη φορά που το θύμα θα καλούσε ανυποψίαστο τον κειμενογράφο θα καλούσε ουσιαστικά την έκδοση του εισβολέα, η οποία θα έκανε τέλεια τη δουλειά της ως κειμενογράφος, αλλά εκτός από αυτό θα έκλεβε και τα αρχεία του θύματος.

4.6 Το «Σκουλήκι» του Internet

Η μεγαλύτερη παραβίαση ασφαλείας όλων των εποχών σε υπολογιστές ξεκίνησε το απόγευμα της 2ας Νοεμβρίου 1988, όταν ένας τελειόφοιτος του Πανεπιστημίου Cornell ελευθέρωσε το πρόγραμμα «σκουλήκι» (worm) μέσα στο δίκτυο Internet. Αυτή η πράξη είχε ως αποτέλεσμα να καταρρεύσουν χιλιάδες υπολογιστές σε πανεπιστήμια, εταιρίες και κυβερνητικά εργαστήρια σε ολόκληρο τον κόσμο, προτού αποκαλυφθεί και απομακρυνθεί το «σκουλήκι».

Το «σκουλήκι» εκμεταλλευόταν ένα σφάλμα που είχε τότε το λειτουργικό Berkeley UNIX, χάρη στο οποίο του επιτρεπόταν να έχει μη εξουσιοδοτημένη πρόσβαση σε υπολογιστές οι οποίοι ήταν συνδεδεμένοι στο Internet. Από τη στιγμή που αποκτούσε πρόσβαση σε ένα νέο υπολογιστή αναπαραγόταν σε αυτόν (αντέγραφε τον εαυτό του) και το αντίγραφο του έψαχνε με τη σειρά του να αποκτήσει πρόσβαση σε άλλους υπολογιστές κ.ο.κ. Τίποτα όμως στον κώδικα του «σκουληκιού» δεν υποδήλωνε προσπάθεια για να κλέψει ή να χαλάσει οτιδήποτε στους υπολογιστές που αποκτούσε πρόσβαση. Δεν είναι βέβαια γνωστό αν η μορφή που είχε το πρόγραμμα στις 2 Νοεμβρίου 1988 προοριζόταν απλώς για έλεγχο και ξέφυγε στο Internet κατά λάθος ή ήταν η τελική. Γεγονός πάντως είναι ότι οι «μολυσμένοι» υπολογιστές μετά από κάποιο διάστημα κατακλύζονταν από αντίγραφα του «σκουληκιού» και δεν μπορούσαν να λειτουργήσουν.

4.7 Ιοί

Μια ειδική κατηγορία επιθέσεων είναι οι ιοί (viruses) των υπολογιστών, οι οποίοι έχουν γίνει ένα μεγάλο πρόβλημα για πολλούς από τους χρήστες υπολογιστών. Ένας ιός είναι ένα κομμάτι προγράμματος το οποίο επισυνάπτεται σε ένα νομότυπο πρόγραμμα με σκοπό να «μολύνει» άλλα προγράμματα. Διαφέρει από το «σκουλήκι» μόνο στο ότι ένας ιός προσκολλάται σε ένα ήδη υπάρχον πρόγραμμα ενώ το «σκουλήκι» είναι από μόνο του ένα πλήρες πρόγραμμα. Τόσο οι ιοί, όσο και τα σκουλήκια προσπαθούν να διαδοθούν και μπορούν να προκαλέσουν σοβαρές ζημιές. Αυτός που γράφει έναν ιό συνήθως γράφει ένα χρήσιμο πρόγραμμα, όπως ένα παιχνίδι για MS-DOS και τοποθετεί μέσα του τον κώδικα του ιού. Στη συνέχεια το πρόγραμμα μεταφέρεται σε κάποιο Web site ή προσφέρεται δωρεάν ή σε κάποια χαμηλή τιμή σε δισκέτα. Στη συνέχεια το πρόγραμμα διαφημίζεται, οπότε οι άνθρωποι αρχίζουν να το μεταφέρουν στους υπολογιστές τους και να το χρησιμοποιούν.

Όταν το πρόγραμμα του ιού ξεκινάει, αρχίζει αμέσως να εξετάζει όλα τα εκτελέσιμα προγράμματα στο σκληρό δίσκο για να δει αν έχουν ήδη μολυνθεί. Όταν βρει ένα μη μολυσμένο πρόγραμμα, το μολύνει επισυνάπτοντας τον κώδικα του ιού στο τέλος του αρχείου. Με τον τρόπο αυτό, κάθε φορά που ένα μολυσμένο πρόγραμμα εκτελείται προσπαθεί να μολύνει και άλλα προγράμματα. Εκτός όμως από το να αντιγράψει τον εαυτό του ένας ιός μπορεί να κάνει και πολλά άλλα πράγματα, όπως να διαγράψει, να αλλάξει ή να κρυπτογραφήσει αρχεία. Υπήρξε ένας ιός που παρουσίαζε στην οθόνη ένα εκβιαστικό μήνυμα, το οποίο ζητούσε από το χρήστη να στείλει 500 δολάρια μετρητά σε μία ταχυδρομική θυρίδα στον Παναμά, διαφορετικά θα έχανε για πάντα όλα τα δεδομένα του.

4.8 Απειλές στο World Wide Web

Το World Wide Web είναι ίσως το γρηγορότερα αναπτυσσόμενο κομμάτι του Internet. Ολοένα όμως και περισσότερο γίνεται και το κομμάτι του Internet που είναι πιο ευάλωτο σε επιθέσεις. Οι υπολογιστές που φιλοξενούν ιστοσελίδες (web servers) αποτελούν ελκυστικούς στόχους για πολλούς λόγους:

1. *δημοσιότητα:* Οι ιστοσελίδες ενός οργανισμού ή μιας επιχείρησης αποτελούν την εικόνα του στον υπόλοιπο κόσμο του Internet. Μια επιτυχημένη επίθεση σε έναν web server μπορεί να αλλάξει πληροφορίες σε ιστοσελίδες που βλέπουν εκατοντάδες χιλιάδες ανθρώπων μέσα σε μερικές ώρες και είτε να προπαγανδίσει διαφορετικές φιλοσοφίες ή ιδεολογίες ή απλώς να χαλάσει τη δημόσια εικόνα του θύματος.

2. *Εμπόριο:* Πολλές ιστοσελίδες περιέχουν φόρμες για την αγορά αγαθών ή τη πραγματοποίηση άλλων εμπορικών συναλλαγών (π.χ. πληρωμή προστίμων στην τροχαία). Οι συναλλαγές αυτές γίνονται συνήθως μέσω της ανταλλαγής πληροφοριών που περιλαμβάνουν τα στοιχεία κάποιας πιστωτικής κάρτας του χρήστη, κάτι που κάνει αυτούς τους υπολογιστές στόχους επιθέσεων με σκοπό την υποκλοπή αυτών των πληροφοριών.

3. *«Εσωτερικές» Πληροφορίες:* Πολλές επιχειρήσεις χρησιμοποιούν το World Wide Web για να μεταδώσουν πληροφορίες στα μέλη τους ή σε άλλους συνεργάτες τους στο εξωτερικό. Οι πληροφορίες αυτές, όπως είναι φυσικό, αποτελούν στόχο των εμπορικών ανταγωνιστών ή εχθρών τους.

4. *Πρόσβαση σε δίκτυα:* Επειδή οι υπολογιστές που φιλοξενούν ιστοσελίδες κάποιας επιχείρησης χρησιμοποιούνται και από τους εργαζόμενους μέσα στην επιχείρηση αλλά και από τον υπόλοιπο κόσμο του Internet, αποτελούν μία γέφυρα επικοινωνίας ανάμεσα στο Internet και στα διάφορα τοπικά δίκτυα των επιχειρήσεων. Επομένως η θέση τους, τους κάνει ιδανικούς στόχους επίθεσης ώστε στη συνέχεια να αποτελέσουν «ορμητήρια» των εισβολέων στο εσωτερικό δίκτυο της επιχείρησης.

Οι *απειλές* στο World Wide Web χωρίζονται σε τρεις κατηγορίες:

1. *Απειλές κατά του web server* για τους λόγους που αναφέρθηκαν παραπάνω.

2. *Απειλές κατά τη μεταφορά των δεδομένων και κατά αποθηκευμένων δεδομένων* κυρίως όταν πρόκειται για αριθμούς πιστωτικών καρτών ή άλλες ευαίσθητες πληροφορίες εμπορικών επιχειρήσεων ή στρατιωτικών οργανώσεων.

3. *Απειλές κατά του υπολογιστή του χρήστη* μέσω προβλημάτων που πολλές φορές υπάρχουν στον κώδικα του προγράμματος που χρησιμοποιεί ο χρήστης για τη ανάγνωση των ιστοσελίδων (π.χ. Microsoft Internet Explorer, Netscape Navigator).

4.9 Οι 5 μεγαλύτερες ψηφιακές απειλές της τρέχουσας περιόδου

Σύμφωνα με το «Virus radar on-line», το πρότυπο παρατηρητήριο ιών, worms και trojans της εταιρείας ESET, οι 5 μεγαλύτερες -βάσει αριθμού υπολογιστών που έχουν πλήξει- ψηφιακές απειλές των ημερών μας, είναι οι ακόλουθες:

Απειλή νο 1:

HTML/Phishing.gen, trojan. Επίσης γνωστή ως HTML/Smithfraud.gen, HTML/Tcfbankfraud.gen, HTML/Bankfraud.gen, Phish-BankFraud.eml. Εντοπίστηκε για πρώτη φορά στις 14/4/2005 και έκτοτε έχει πλήξει περισσότερους από 12 εκ. υπολογιστές.

Τρόπος δράσης: Οι χρήστες λαμβάνουν ένα μήνυμα (e-mail), που τους καλεί επιτακτικά να ανοίξουν κάποιον σύνδεσμο (link), προκειμένου να επιβεβαιώσουν την ορθότητα ευαίσθητων προσωπικών τους δεδομένων (λ.χ. κωδικούς πιστωτικών καρτών). Αν οι χρήστες το πράξουν, μεταφέρονται σε ιστοσελίδα «πλαστού» site, όπου τους ζητείται να συμπληρώσουν κάποια φόρμα, με κρίσιμα στοιχεία.

Λεπτομέρειες: Τα sites στα οποία μεταφέρονται οι χρήστες, με μια πρώτη ματιά, θυμίζουν τα επίσημα γνωστών εταιρειών. Μια πιο προσεκτική εξέταση, όμως, φανερώνει ότι το url του site δεν είναι το αυθεντικό και ότι οι χρήστες βρίσκονται σε ένα site που «υποδύεται» κάποιο άλλο, προκειμένου να τους υποκλέψει πολύτιμα στοιχεία. Με τον ίδιο τρόπο, το e-mail φαίνεται ότι προέρχεται από τράπεζες, εταιρείες παροχής πρόσβασης στο Internet (ISP), ινστιτούτα ερευνών, εταιρείες κ.λπ., χωρίς, βέβαια, να ισχύει κάτι τέτοιο. Τα μηνύματα αποστέλλονται μαζικά από επιτήδειους, που στη συνέχεια κερδίζουν χρήματα, εκμεταλλευόμενοι ή εμπορευόμενοι τα στοιχεία που συγκέντρωσαν. Το μήνυμα, όπως επίσης και η ιστοσελίδα δεν εγκαθιστούν κάτι στον υπολογιστή του χρήστη και κατά συνέπεια το άνοιγμα του e-mail και του υπερσυνδέσμου δεν είναι επιβλαβή. Ωστόσο, σε περίπτωση που ο αποδέκτης πειστεί να παραχωρήσει προσωπικά του δεδομένα, τότε οι συνέπειες μπορεί να είναι πολύπλευρα καταστροφικές.

Προφυλάξεις: Οι χρήστες δεν πρέπει για κανένα λόγο να παραχωρούν κρίσιμα δεδομένα τους, μέσω e-mail. Καμιά σοβαρή (μεγάλη) εταιρεία, δεν ζητάει προσωπικά δεδομένα με αυτόν τον τρόπο και σε περίπτωση που λάβουν κάτι σχετικό η διαγραφή του μηνύματος θεωρείται επιβεβλημένη.

Απειλή νο 2:

Win32/NetSky.Q, worm. Εντοπίστηκε για πρώτη φορά στις 24/3/2004 και έκτοτε έχει πλήξει περισσότερους από 19 εκ. υπολογιστές.

Τρόπος δράσης: Το συγκεκριμένο worm εξαπλώνεται μέσω ηλεκτρονικού ταχυδρομείου, ομότιμων δικτύων (P2P) ή άλλων δικτύων. Το worm καταφθάνει στον υπολογιστή μέσω ενός επισυναπτόμενου αρχείου, που μπορεί να είναι είτε συμπιεσμένο είτε εκτελέσιμο και μπορεί να φέρει τις καταλήξεις .zip, .doc, .txt, .exe, .scr, .pif.

Λεπτομέρειες: Μερικές από τις φράσεις που μπορεί να φέρει το συνημμένο που περιέχει το worm, είναι και οι, approved, archive, attach, bill, confirm, info02, information, judge, letter, readme κ.ά. Το worm είναι ένα εκτελέσιμο 29 KB περίπου, το οποίο μετά το άνοιγμά του, αντιγράφει τον εαυτό του σε φάκελο των Windows, χρησιμοποιώντας το όνομα «FVProtect.exe». Ταυτόχρονα, δημιουργεί ένα αρχείο .dll («userconfig9x.dll»), που εκτελείται αυτόματα. Προκειμένου να μπορεί να «τρέχει» κάθε φορά που τα Windows ξεκινούν, δημιουργεί στο μητρώο (registry) την εγγραφή «Norton Antivirus AV» και την τοποθετεί στο κλειδί HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion \Run. Η νέα εγγραφή περιέχει τη σύνδεση με το FVProtect.exe. Στη συνέχεια το worm απομακρύνει περί τις 30 καταχωρήσεις από τη registry και δημιουργεί στο σύστημα τα αρχεία, base64.tmp, zip1.tmp, zip2.tmp, zip3.tmp, zipped.tmp, τα οποία και τρέχουν κάθε φορά που ο χρήστης δημιουργεί κάποιο e-mail. Παράλληλα, ψάχνει τους δίσκους του υπολογιστή για κάθε είδους αρχεία που μπορεί να περιέχουν ηλεκτρονικές διευθύνσεις, τις οποίες και συγκεντρώνει σε άλλα αρχεία, προκειμένου να τις χρησιμοποιήσει για την εξάπλωσή του.

Προφυλάξεις: Οι χρήστες θα πρέπει να επιδεικνύουν ιδιαίτερη προσοχή σε e-mails με συνημμένα, που προέρχονται από άγνωστες πηγές. Το NOD32 ανιχνεύει και καταστρέφει αυτόματα το συγκεκριμένο worm.

Απειλή νο 3:

Win32/NetSky.D, worm. Εντοπίστηκε για πρώτη φορά στις 16/3/2004 και έκτοτε έχει πλήξει περισσότερους από 5 εκ. υπολογιστές.
Τρόπος δράσης: Οι χρήστες λαμβάνουν e-mail με ένα συνημμένο αρχείο 17 KB, που περιέχει το worm. Το αρχείο είναι εκτελέσιμο της μορφής .pif. Αν ανοιχτεί, το worm συγκεντρώνει τις ηλεκτρονικές διευθύνσεις του υπολογιστή και αποστέλλει τον εαυτό του, μαζικά.

Λεπτομέρειες: Το θέμα του e-mail είναι πάντοτε απαντητικό, περιέχει, δηλαδή την ένδειξη «RE:», η οποία συνοδεύεται από φράσεις όπως, your details, your document, your letter, your music, your picture. Στο σώμα του μηνύματος υπάρχει μία φράση που παροτρύνει το χρήστη ν' ανοίξει το επισυναπτόμενο. Η ονομασία του επισυναπτόμενου, μπορεί να είναι μία από τις παρακάτω: all_document.pif, application.pif, document.pif, document_4351.pif, document_excel.pif, document_full.pif, document_word.pif, message_details.pif, message_part2.pif, mp3music.pif, my_details.pif, your_archive.pif, your_bill.pif, your_details.pif, your_document.pif, your_file.pif, your_letter.pif, your_picture.pif, your_product.pif, your_text.pif, your_website.pif, yours.pif. Όταν

εκτελεστεί το αρχείο αυτό, τότε το worm αντιγράφεται σε φάκελο των windows και κατόπιν προστίθεται μία καινούρια εγγραφή στο μητρώο, με σκοπό να εκτελείται αυτόματα. Αφού αφαιρέσει 20 εγγραφές από τη registry, ψάχνει τους δίσκους του υπολογιστή για κάθε είδους αρχεία που μπορεί να περιέχουν ηλεκτρονικές διευθύνσεις.
Προφυλάξεις: Οι χρήστες θα πρέπει να επιδεικνύουν ιδιαίτερη προσοχή σε e-mails με συνημμένα, που προέρχονται από άγνωστες πηγές. Το NOD32 ανιχνεύει και καταστρέφει αυτόματα το συγκεκριμένο worm, από την πρώτη κιόλας στιγμή της εμφάνισής του, χάρις στα advanced heuristics.

Απειλή νο 4:

Win32/Zafi.B, worm. Επίσης γνωστό ως W32.Erkez.B. Εντοπίστηκε για πρώτη φορά στις 10/6/2004 και έκτοτε έχει πλήξει περισσότερους από 10 εκ. υπολογιστές.
Τρόπος δράσης: Έρχεται μέσω συνημμένου, συμπιεσμένου αρχείου, μεγέθους 13 KB (49 μετά την αποσυμπίεση). Προσβάλλει υπολογιστές με λειτουργικό σύστημα Windows 95 ή μεταγενέστερο και εξαπλώνεται μέσω ηλεκτρονικού ταχυδρομείου και δίκτυα ομοτίμων (P2P).

Λεπτομέρειες: Μετά την εκτέλεση του αρχείου, το worm ενεργοποιείται και αντιγράφει τον εαυτό του σε φάκελο του συστήματος, με τυχαία ονομασία και κατάληξη .exe. Στον ίδιο φάκελο δημιουργεί και ένα αρχείο .dll, το οποίο χρησιμοποιείται για την καταχώριση των ηλεκτρονικών διευθύνσεων. Συγχρόνως, επεμβαίνει στη registry, «πειράζοντας» και δημιουργώντας καινούρια κλειδιά, για να μπορεί να φορτώνεται αυτόματα κατά την εκκίνηση του συστήματος, και τερματίζει οποιαδήποτε διαδικασία περιέχει τον όρο «virus» και «firewall». Κατόπιν, ψάχνει τους δίσκους για αρχεία που περιέχουν ηλεκτρονικές διευθύνσεις, τις οποίες και χρησιμοποιεί για να αποστείλει τον εαυτό του. Οι προσβεβλημένοι υπολογιστές, εκτός των άλλων, επιχειρούν να φορτώσουν ορισμένα συγγρικά sites.

Προφυλάξεις: Οι χρήστες θα πρέπει να επιδεικνύουν ιδιαίτερη προσοχή σε e-mails με συνημμένα, που προέρχονται από άγνωστες πηγές. Το NOD32 ανιχνεύει και καταστρέφει αυτόματα το συγκεκριμένο worm, από την πρώτη κιόλας στιγμή της εμφάνισής του, χάρις στα advanced heuristics.

Απειλή νο 5:

Win32/NetSky.Z, worm. Εντοπίστηκε αρχικά στις 21/4/2004 και έκτοτε έχει πλήξει περισσότερους από 2 εκ. υπολογιστές.
Τρόπος δράσης: Οι χρήστες λαμβάνουν e-mail με ένα συνημμένο αρχείο .zip 22 KB, που περιέχει την απειλή. Αν ανοιχτεί, το worm βρίσκει τις ηλεκτρονικές διευθύνσεις του υπολογιστή και αποστέλλει τον εαυτό του, μαζικά.

Λεπτομέρειες: Το θέμα του e-mail είναι μία από τις λέξεις Important, Information, Hello, Hi, Document, ενώ στο σώμα του e-mail υπάρχει μία από τις φράσεις, Important

informations!, Important textfile!, Important data! , Important bill!, Important document!, Important notice!, Important details! ή μόνο η λέξη Important. Το συνημμένο μπορεί να ονομάζεται ή Informations.zip, ή Textfile.zip ή Part-2.zip ή Data.zip ή Bill.zip ή Important.zip ή Notice.zip ή τέλος, Details.zip. Το αρχείο zip περιέχει ένα εκτελέσιμο που είναι της μορφής .exe, αν και το εικονίδιο που το συνοδεύει, υποδηλώνει (παραπλανητικά) ότι πρόκειται για αρχείο κειμένου. Με το άνοιγμά του, το worm δημιουργεί καινούριες εγγραφές στη registry προκειμένου να τρέχει αυτόματα και αντιγράφει τον εαυτό του σε φάκελο των Windows. Ύστερα, ψάχνει τους δίσκους για αρχεία που περιέχουν ηλεκτρονικές διευθύνσεις, τις οποίες και χρησιμοποιεί για να αποστείλει τον εαυτό του. Επιπλέον, το worm περιέχει μία εφαρμογή backdoor που επιτρέπει στο συγγραφέα του ιού να πάρει τον έλεγχο του συστήματος, μέσω της πύλης 665 της σύνδεσης TCP του υπολογιστή. Τέλος, σε συγκεκριμένες ημερομηνίες ο μολυσμένος υπολογιστής πραγματοποιεί επιθέσεις denial of service, εναντίον ορισμένων κόμβων.

Προφυλάξεις: Οι χρήστες θα πρέπει να επιδεικνύουν ιδιαίτερη προσοχή σε e-mails με συνημμένα, που προέρχονται από άγνωστες πηγές. Το NOD32 ανιχνεύει και καταστρέφει αυτόματα το συγκεκριμένο worm, από την πρώτη κιόλας στιγμή της εμφάνισής του, χάρις στα advanced heuristics που χρησιμοποιεί.

5. Λειτουργία των Firewalls

Ένα firewall εξετάζει όλη την κυκλοφορία που δρομολογείται μεταξύ των δύο δικτύων για να διαπιστώσει εάν ικανοποιούνται ορισμένα κριτήρια. Εάν ναι, τότε η κυκλοφορία (traffic) δρομολογείται μεταξύ των δικτύων, διαφορετικά διακόπτεται. Ένα firewall φιλτράρει και την εισερχόμενη και την εξερχόμενη κυκλοφορία. Μπορεί επίσης να διαχειριστεί την δημόσια πρόσβαση (public access) στους ιδιωτικούς δικτυωμένους πόρους, όπως κάνουν οι host εφαρμογές.

Μπορεί να χρησιμοποιηθεί για να καταγράψει (log) όλες τις προσπάθειες για πρόσβαση στο ιδιωτικό δίκτυο και να ενεργοποιήσει συναγερμούς (alerts) όταν επιχειρείται εχθρική (hostile) ή αναρμόδια (unauthorized) πρόσβαση. Τα firewalls μπορούν να φιλτράρουν τα πακέτα στις διευθύνσεις της πηγής και του προορισμού καθώς και στα port number τους. Αυτό είναι γνωστό ως φιλτράρισμα διευθύνσεων. Τα firewalls μπορούν επίσης να φιλτράρουν συγκεκριμένους τύπους κυκλοφορίας δικτύων. Αυτό είναι επίσης γνωστό ως φιλτράρισμα πρωτοκόλλου (protocol filtering) επειδή η απόφαση να διαβιβαστεί ή να απορριφθεί η κυκλοφορία εξαρτάται από το χρησιμοποιούμενο πρωτόκολλο, παραδείγματος χάριν HTTP, FTP ή Telnet. Τα firewalls μπορούν επίσης να φιλτράρουν την κυκλοφορία από τις ιδιότητες ή την κατάσταση των πακέτων.

Όταν μία εταιρία συνδέει το εσωτερικό επιχειρηματικό της δίκτυο στο Internet αντιμετωπίζει ορισμένους σημαντικούς κινδύνους. Εξαιτίας της ανοικτής δομής του Internet, κάθε επιχειρησιακό δίκτυο που είναι συνδεδεμένο σ' αυτό είναι εκτεθειμένο σε επιθέσεις. Οι hackers του Internet μπορούν θεωρητικά να εισέλθουν στο επιχειρησιακό δίκτυο και να προκαλέσουν ζημιά με διάφορους τρόπους: μπορούν να κλέψουν ή να καταστρέψουν σημαντικά δεδομένα, να προκαλέσουν ζημιά σε ανεξάρτητους υπολογιστές ή σε ολόκληρο το δίκτυο, να χρησιμοποιήσουν τους πόρους των επιχειρησιακών υπολογιστών ή να χρησιμοποιήσουν το επιχειρηματικό δίκτυο και τους πόρους του και να φαίνεται ότι το κάνει κάποιος υπάλληλος της επιχείρησης. Η λύση δεν είναι η αποκοπή του δικτύου από το Internet. Αντιθέτως, η εταιρία μπορεί να δημιουργήσει firewalls για να προστατεύσει το δίκτυό της.

Τα εν λόγω firewalls αφ' ενός επιτρέπουν στους υπαλλήλους της επιχείρησης να έχουν πρόσβαση στο Internet και αφ' ετέρου εμποδίζουν τους επίδοξους hackers και crackers να αποκτήσουν πρόσβαση στο επιχειρηματικό δίκτυο και να προκαλέσουν ζημιές. Τα firewalls αποτελούν συνδυασμούς hardware και software και δημιουργούνται χρησιμοποιώντας routers, servers και μία ποικιλία λογισμικού. Τα firewalls τοποθετούνται στο σημείο μεταξύ του επιχειρησιακού δικτύου και του Internet και μπορεί να είναι από απλά ως εξαιρετικά πολύπλοκα συστήματα.

Υπάρχουν πολλά είδη firewalls αλλά τα περισσότερα από αυτά διαθέτουν ορισμένα κοινά χαρακτηριστικά. Ένα από τα απλούστερα είδη των firewalls χρησιμοποιεί την τεχνική του φιλτραρίσματος των πακέτων. Στην περίπτωση αυτή ένας router εξετάζει την επικεφαλίδα κάθε πακέτου δεδομένων που ταξιδεύει μεταξύ του Internet και του

επιχειρησιακού δικτύου. Οι επικεφαλίδες αυτές διαθέτουν διάφορες πληροφορίες όπως την IP διεύθυνση του αποστολέα και του παραλήπτη, το πρωτόκολλο που χρησιμοποιείται για την αποστολή και άλλες παρόμοιες πληροφορίες. Βασιζόμενος σε αυτές τις πληροφορίες ο router γνωρίζει το είδος της Internet υπηρεσίας που χρησιμοποιείται για την αποστολή των δεδομένων καθώς και την ταυτότητα του αποστολέα και του παραλήπτη των δεδομένων. Αφού διευκρινιστούν αυτές οι πληροφορίες, ο router μπορεί να εμποδίσει την αποστολή ορισμένων πακέτων μεταξύ του Internet και του επιχειρησιακού δικτύου.

Για παράδειγμα ο router θα μπορούσε να μπλοκάρει όλη την κίνηση εκτός του ηλεκτρονικού ταχυδρομείου. Επιπροσθέτως θα μπορούσε να μπλοκάρει την κίνηση από και προς κάποιες ύποπτες τοποθεσίες ή από ορισμένους χρήστες. Οι proxy servers χρησιμοποιούνται αρκετά συχνά στα firewalls. Ένας proxy server είναι λογισμικό σε επίπεδο server το οποίο τρέχει σ' έναν host σ' ένα firewall και παίζει το ρόλο του οχυρού. Στην περίπτωση αυτή μόνο ο proxy server αλληλεπιδρά με το Internet (και όχι μεμονωμένα οι ανεξάρτητοι υπολογιστές του δικτύου) και ως εκ τούτου μπορούν να παρακολουθηθούν καλύτερα τα θέματα ασφάλειας. Είναι σαφώς ευκολότερο να κρατήσεις ασφαλή τον εν λόγω server παρά τους εκατοντάδες, σε ορισμένες περιπτώσεις, ανεξάρτητους υπολογιστές του δικτύου.

Όταν κάποιος χρήστης του επιχειρησιακού δικτύου θέλει να έχει πρόσβαση σε κάποιον server στο Internet, στέλνει μία αίτηση από τον υπολογιστή του στον proxy server, εν συνεχεία ο proxy server έρχεται σε επαφή με τον server του Internet και, τέλος, ο proxy server στέλνει τις πληροφορίες από τον Internet server στον υπολογιστή του επιχειρησιακού δικτύου. Ως εκ τούτου ο proxy server δρα σαν ενδιάμεσος προσφέροντας μεγαλύτερη ασφάλεια και καταγράφοντας όλη την κίνηση μεταξύ του Internet και του επιχειρηματικού δικτύου.

6. Δυνατότητες των Firewalls

Πριν δούμε τις δυνατότητες των firewalls είναι σκόπιμο να θυμηθούμε σε ποιο layer σύμφωνα με το μοντέλο αναφοράς OSI δρούν οι συσκευές ενός τυπικού LAN. Έτσι λοιπόν οι repeaters και τα hubs ενεργουν στο 1° layer (physical layer) τα switches και bridges στο 2° layer(data link layer) και οι routers στο 3° layer (network layer). Ένας Firewall περνά από όλα αυτά τα layers και δρα κυρίως στο 6° και 7° layer (presentation, application layer) τα οποία είναι και τα επίπεδα που είναι υπεύθυνα για την εγκατάσταση των ελέγχων (user authentication, privacy, identifying constraints of data syntax) και των εφαρμογών.

Έτσι ένας Firewall μπορεί να ελέγξει τη ροή των πληροφοριών από την αρχή μέχρι το τέλος της εγκατάστασης των συνόδων (sessions) είτε ακόμα να καθορίσει ποιες λειτουργίες θα επιτραπούν η θα απαγορευθούν. Επίσης μπορεί να βοηθήσει τον Administrator να καθορίσει ένα κεντρικό "choke point" κρατώντας τους μη εξουσιοδοτημένους χρήστες έξω από το τοπικό του δίκτυο, αφήνοντας τον απερίσπαστο να επικεντρωθεί στην εργασία του.

Ένας Firewall βελτιώνει σε μεγάλο βαθμό την ασφάλεια ενός δικτύου, μειώνοντας τους κινδύνους που την απειλούν, φιλτράροντας συνυπάρχουσες μη ασφαλείς υπηρεσίες. Το αποτέλεσμα είναι ότι το δίκτυο εκτίθεται σε λιγότερους κινδύνους διότι μόνο επιλεγμένα πρωτόκολλα είναι δυνατό να περάσουν από ένα Firewall.

Ιδιαίτερα δημοφιλείς εφαρμογές σε LAN's αλλά τρωτές όπως το NFS (Network File System) και το NIS (Network Information System), στα συστήματα που έχουν ως πλατφόρμα το UNIX, μπορούν να αποκλεισθούν από το Firewall κατά τη είσοδο τους έτσι ώστε να μην υλοποιηθούν μέσα σ΄ ένα τοπικό δίκτυο ενώ παράλληλα να χρησιμοποιούνται εντός του δικτύου μειώνοντας το φόρτο διαχείρισης του server.

Μπορούν να παρέχουν προστασία από routing – based επιθέσεις όπως είναι το source routing και προσπάθειες να ανακατευθύνουν τα routing paths σε έκθετα sites διαμέσου του ICMP (Internet Control Message Protocol). Οι Firewalls προσφέρουν τη δυνατότητα όπου η ασφάλεια του δικτύου μας μπορεί εύκολα να παρακολουθείται και να προειδοποιεί τον network administrator.

Αποτελεί το καλύτερο σημείο για έλεγχο και τήρηση αρχείων καταγραφής χρήσης του Internet από τους χρήστες του δικτύου. Επίσης προσφέρει την ιδανική τοποθεσία για εγκατάσταση Web και Ftp Servers διότι είναι δυνατή η διαμόρφωση τους ώστε να παρέχουν αυτές τις συγκεκριμένες υπηρεσίες απαγορεύοντας ταυτόχρονα την πρόσβαση από εξωτερικούς παράγοντες στο τοπικό του δίκτυο.

7. Υπηρεσίες των Firewalls

Όπως αναφέρθηκε, με τον όρο Firewall, περιγράφονται σήμερα τα ολοκληρωμένα συστήματα ασφαλείας ενός πληροφοριακού συστήματος. Ένα σύστημα Firewall περιλαμβάνει τόσο το κατάλληλο υλικό (routers, servers, firewall cards), όσο και λογισμικό. Παρεμβάλλεται δε, μεταξύ του τοπικού Intranet και του Internet , και προστατεύει το σύστημα από εξωτερικές επιθέσεις ασφαλείας. Ανάλογα με την πολιτική ασφάλειας του οργανισμού, ο Firewall μπορεί να παίζει ρόλο ελεγκτή, τόσο για την πρόσβαση από το Διαδίκτυο στο Τοπικό Σύστημα, όσο και αντίστροφα, ενεργώντας επιλεκτικά, σε άλλους επιτρέποντας την πρόσβαση και σε άλλους όχι.

Μερικές κύριες υπηρεσίες που παρέχει ένα σύστημα Firewall είναι:

Πρόληψη μη εξουσιοδοτημένης πρόσβασης: Αποτρέπει τους επίδοξους εισβολείς από το να αποκτήσουν πρόσβαση στο σύστημα.

Καταγραφή των ενεργειών που λαμβάνουν χώρα στο δίκτυο: Φιλτράρει όλες τις εφαρμογές, υπηρεσίες συστήματος, και πρωτόκολλα.

Διαφυλάσσει το σύστημα: Ενημερώνει για το ποιες εφαρμογές προσπαθούν να συνδεθούν στο Internet. Η πρόσβαση επιτρέπεται μόνο με την άδεια του οργανισμού.

Ασφαλίζει τις συνδέσεις Internet: Το σύστημα παραμένει ασφαλές ανεξάρτητα από το είδος της σύνδεσης. (π.χ. dial-up, direct connection όπως cable ή DSL κτλ)

Παρέχει παραμετροποίηση των επιλογών ασφαλείας: Προσφέρει interface για τον καθορισμό των επιλογών (set-up).

Παρακολουθεί και καταγράφει τις συνδέσεις στο Internet: Διαθέτει logging και tracking options για την ικανοποίηση των προδιαγραφών ασφαλείας και auditing.

Αξίζει να σημειωθεί ότι, σήμερα υπάρχουν συστήματα Firewall, τα οποία βρίσκουν εφαρμογή ακόμη και σε ένα απλό PC. Εκεί, το λογισμικό Firewall καλείται να προστατέψει το προσωπικό σύστημα Ηλεκτρονικού Υπολογιστή, από επιθέσεις που μπορεί να προέρχονται , όχι μόνο από το Internet, αλλά και από αυτό ακόμη το τοπικό δίκτυο του οργανισμού.

8. Περιορισμοί των Firewalls

Είναι προφανές ότι η χρησιμοποίηση firewall δεν επαυξάνει την φυσική ασφάλεια του δικτύου μας. Υπάρχουν όμως και περιορισμοί όπως οι παρακάτω:

α. Ο Firewall δεν μπορεί να μας προστατεύσει από επιθέσεις που δεν υφίστανται τον έλεγχο ενός firewall (π.χ Ο χρήστης που εκνευρίζεται από την επιπρόσθετη αυθεντικοποίηση που επιβάλλει ένας proxy server εγκαθιστά απ ευθείας σύνδεση με ένα παροχέα Internet υπηρεσιών).

β. Οι Firewalls δεν μπορούν να μας προστατεύσουν από τους ασυνείδητους χρήστες που μεταφέρουν πολύτιμα δεδομένα εκτός του κτιρίου που εργάζονται σε floppy dises η PCMCIA cards. Επίσης δεν μπορούν να ελέγξουν τον χρήστη που από άγνοια η έλλειψη εκπαίδευσης δίνει τηλεφωνικά στον εισβολέα (υποτιθέμενο system administrator) το password του Η/Υ τους.

γ. Επίσης είναι δύσκολη η προστασία από ιούς κατά την μεταφορά αρχείων. Η πολυπλοκότητα των λειτουργικών συστημάτων οι διάφοροι τύποι κωδικοποίησης και συμπίεσης των δυαδικών αρχείων και οι χιλιάδες ιοί που κυκλοφορούν καθιστούν δυσχερή την ακριβή ανίχνευση των ιών από τον firewall.

9. Πολιτικές των Firewalls

9.1. Πολιτική σχεδιασμού

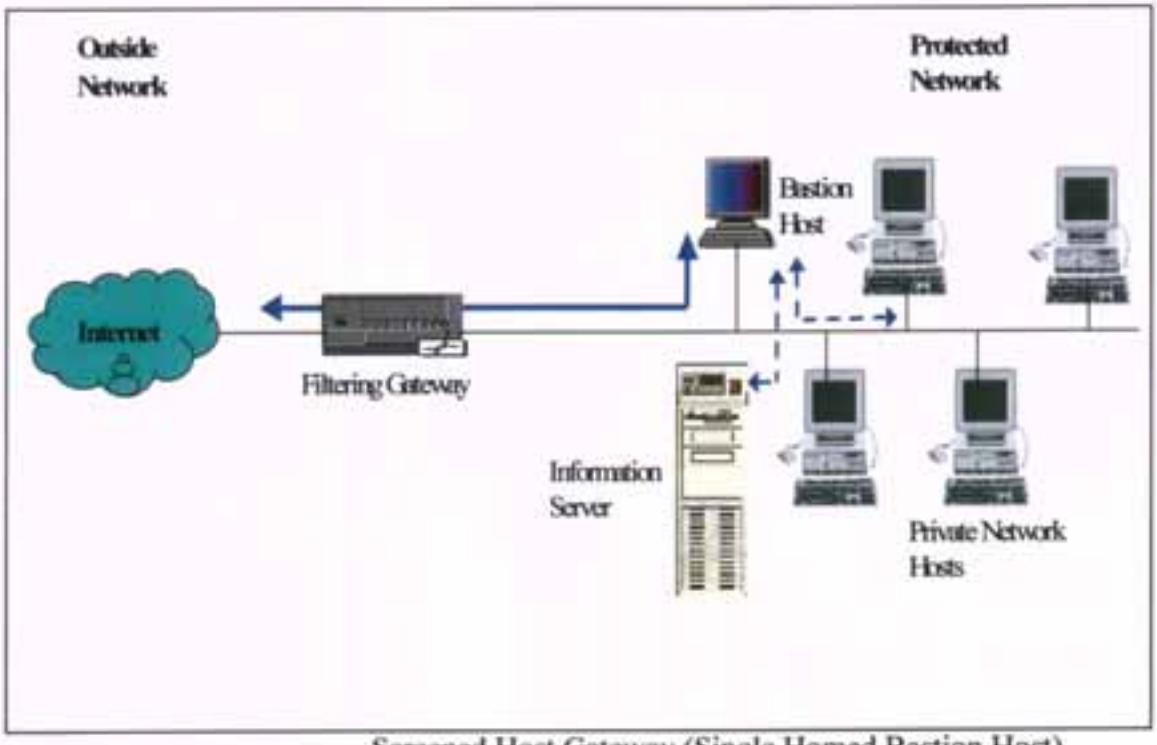
Η πολιτική σχεδιασμού των firewalls είναι ακριβής και σαφής στο firewall και καθορίζει τους κανόνες που χρησιμοποιούνται για να υλοποιηθεί η πολιτική ασφάλειας του δικτύου του οργανισμού η της εταιρείας. Η πολιτική ασφάλειας θα πρέπει να είναι τέτοια που με επίγνωση των κινδύνων και των ευπαθειών που απορρέουν από τη χρησιμοποίηση του TCP/IP θα πρέπει να καθορισθούν επακριβώς τα πλεονεκτήματα και τα μειονεκτήματα των Firewalls. Όπως αναφέρθηκε παραπάνω κατά τον σχεδιασμό των firewalls ακολουθείται μία εκ των δύο φιλοσοφιών:

1. **Ότι δεν επιτρέπεται ρητά, ΑΠΑΓΟΡΕΥΕΤΑΙ.**

2. **Ότι δεν απαγορεύεται ρητά, ΕΠΙΤΡΕΠΕΤΑΙ.**

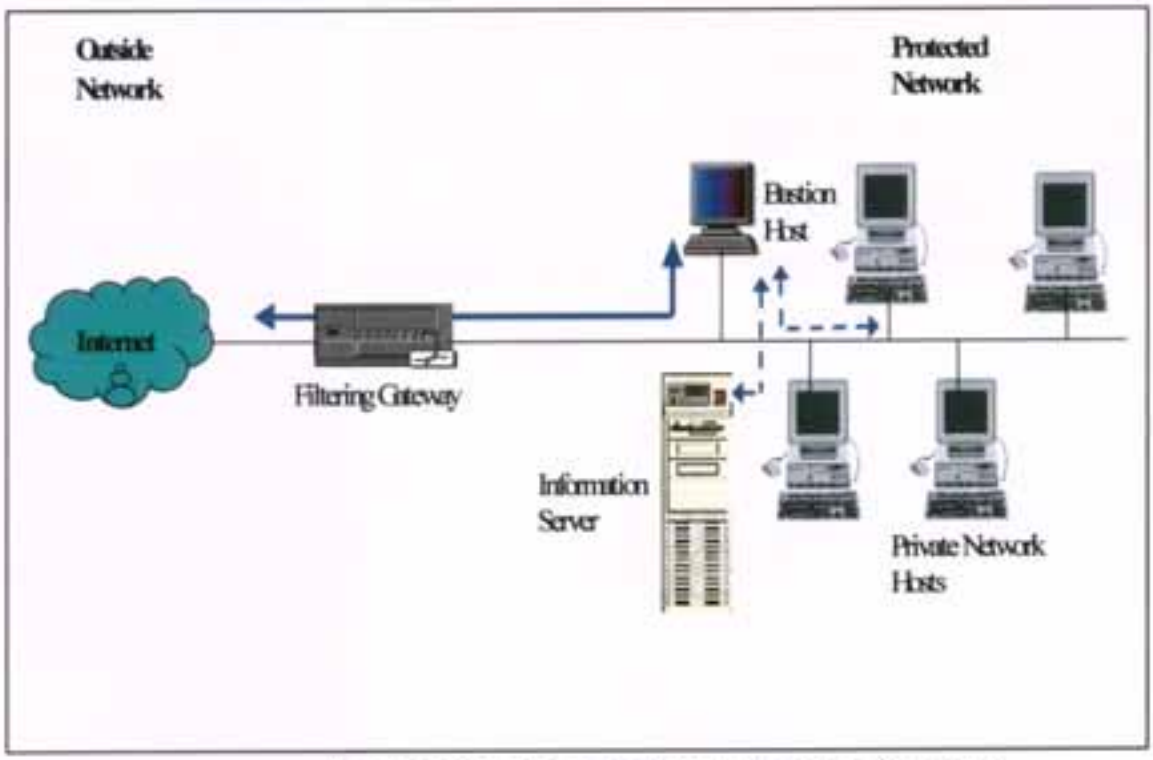
Από τις παραπάνω πολιτικές η συχνότερα απαντώμενη σε χώρους που χρειάζεται όσο το δυνατό μεγαλύτερη ασφάλεια με χρησιμοποίηση των υπηρεσιών του Internet είναι η δεύτερη, η "περιοριστική" πολιτική. Η δυσαρέσκεια των χρηστών θα τους οδηγήσει σε καταστρατήγηση όλων των κανόνων ασφαλείας. Εδώ λοιπόν υπεισέρχεται ο σχεδιασμός των firewalls. Συγκεκριμένοι firewalls θα υλοποιήσουν και θα παρέχουν περιοριστική η επιτρεπτική πολιτική ανάλογα με τις ανάγκες της επιχείρησης η του οργανισμού. Εκείνη θα καθορίσει εάν θα υπάρχουν και ποια θα είναι τα συστήματα που απαιτούν υπηρεσίες Internet αλλά που δεν θα διέρχονται διαμέσω ενός firewalls σε προστατευμένα υποδίκτυα.

Στα παρακάτω σχήματα φαίνονται διαφορετικές υλοποιήσεις σχεδιασμού firewalls.



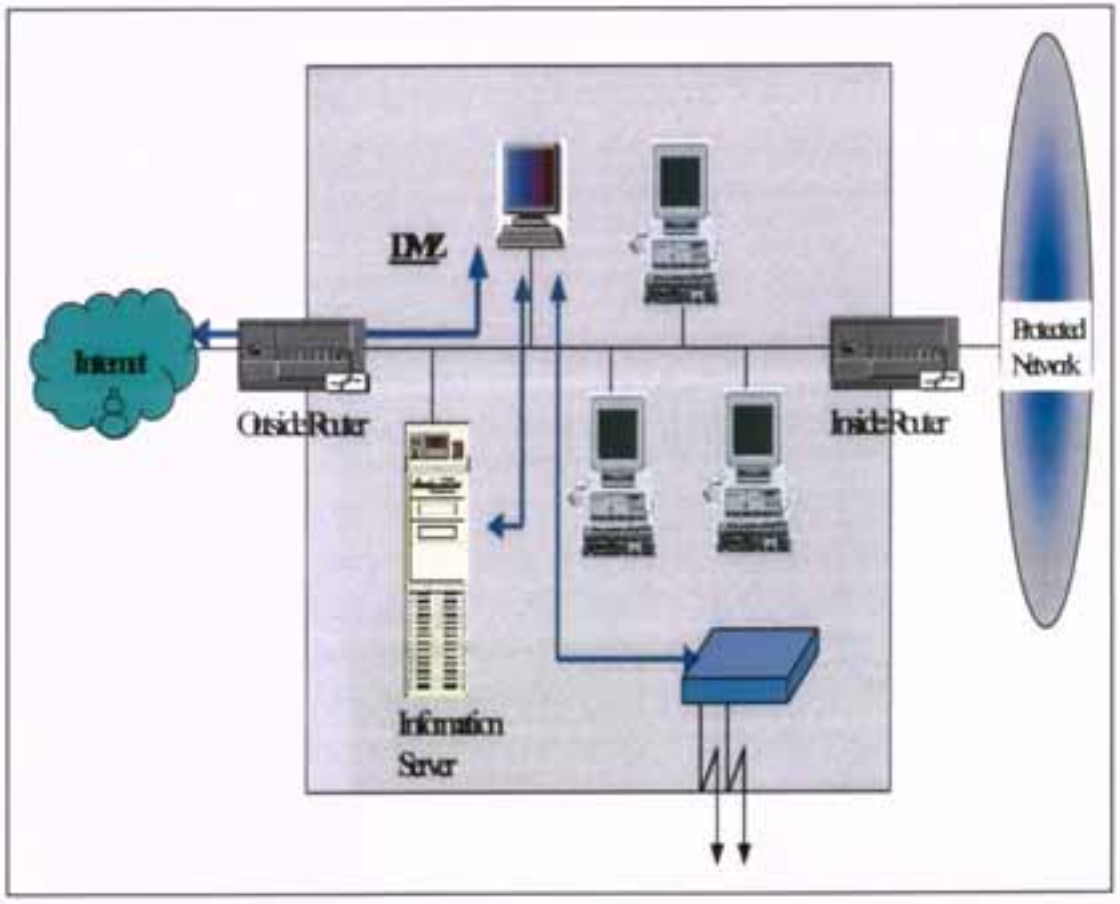
Screened Host Gateway (Single Homed Bastion Host)

Στο σχήμα φαίνεται ένα παράδειγμα σχεδιασμού το οποίο παρέχει υψηλοτέρου επιπέδου ασφάλεια από ένα packet filtering router επειδή υλοποιεί και την ασφάλεια του επιπέδου δικτύου (network layer security) και την ασφάλεια στο επίπεδο εφαρμογής (application layer security). Επίσης ο πιθανός εισβολέας πρέπει να διαπεράσει δύο διαφορετικά συστήματα πριν η ασφάλεια του προστατευμένου δικτύου μπορεί να μην είναι αποδεκτή. Σε αυτό το σύστημα ο Bastion host διαμορφώνεται με την τοποθέτηση ενός packet filtering router μεταξύ του Internet και του Bastion host. Το ruleset του firewall έχει διαμορφωθεί έτσι ώστε τα εξωτερικά συστήματα να προσπελαύνουν μόνο τον Bastion host. Η επικοινωνία με τα υπόλοιπα συστήματα του δικτύου δεν είναι επιτρεπτή. Ένα από τα πλεονεκτήματα αυτού του σχεδιασμού είναι ότι ένας κοινός information server παρέχει Web και Ftp υπηρεσίες τοποθετημένος μεταξύ του packet filtering router και του Bastion host. Στην περίπτωση της μέγιστης ασφάλειας οι εσωτερικοί και εξωτερικοί χρήστες προσπελαύνουν πρώτα τον bastion host ο οποίος τρέχει τις απαιτούμενες proxy services πριν επικοινωνήσουν με τον information server. Εάν χαμηλότερου επιπέδου ασφάλεια είναι επαρκής ο router μπορεί να διαμορφωθεί να επιτρέπει στους εξωτερικούς χρήστες την απ' ευθείας πρόσβαση στον κοινό information server.



Screened Host Gateway (Dual Homed Bastion Host)

Ένα πιο ασφαλές σύστημα firewall μπορεί να δημιουργηθεί με την κατασκευή ενός Dual Homed Bastion Host, ο οποίος έχει δύο δικτυακά interfaces αλλά η δυνατότητα του host να μεταδίδει την επικοινωνία μεταξύ των interfaces παρακάμπτοντας τις proxy services είναι απενεργοποιημένη. Η τοπολογία του δικτύου ενισχύει όλη την επικοινωνία που προορίζεται για το προστατευμένο δίκτυο διαμέσου του bastion host και παρέχει επιπρόσθετη ασφάλεια εάν στους εξωτερικούς χρήστες έχει παραχωρηθεί το δικαίωμα της απ' ευθείας πρόσβαση στον information server. Από τη στιγμή που ο Bastion Host είναι το μόνο τμήμα του προστατευμένου δικτύου που έχει άμεση πρόσβαση στο Internet και οι δυνατές εξωτερικές απειλές περιορίζονται σε αυτόν. Ωστόσο, επειδή οι χρήστες συνδέονται στο Bastion Host οι υποθετικές απειλές εξαπλώνονται και στο υπόλοιπο δίκτυο. Είναι απαραίτητο λοιπόν ότι ο bastion host πρέπει να ισχυροποιηθεί και να προστατευθεί από την διείσδυση και οι χρήστες του δικτύου δεν πρέπει για κανένα λόγο να συνδέονται στον Bastion Host.



Screened Subnet Firewall System (Demilitarized Zone)

Το τελευταίο σχήμα υλοποιεί δύο packet filtering routers και έναν bastion host. Σ΄ αυτή την περίπτωση έχουμε το ασφαλέστερο (από πλευράς σχεδιασμού) σύστημα firewalls διότι υποστηρίζει ταυτόχρονα την ασφάλεια στα επίπεδα δικτύου και εφαρμογής καθορίζοντας μια αποστρατικοποιημένη ζώνη ,Demilitarized Zone (DMZ), στο δίκτυο μας. Ο Διαχειριστής του δικτύου τοποθετεί τον bastion host τον information server τα modems και άλλους servers στο DMZ δίκτυο. Το DMZ δίκτυο λειτουργεί σαν μικρό απομονωμένο δίκτυο που τοποθετείται ανάμεσα στο Internet και στο προστατευμένο μας δίκτυο. Τυπικά το DMZ δίκτυο διαμορφώνεται έτσι ώστε οι εξωτερικοί Η/Υ και οι Η/Υ του δικτύου προσπελαύνουν ένα περιορισμένο αριθμό συστημάτων στο DMZ δίκτυο, αλλά η απευθείας διαβίβαση διαμέσου αυτού απαγορεύεται. Στην εσωτερική επικοινωνία ο εξωτερικός router προστατεύει από τις συνήθεις εξωτερικές επιθέσεις (source IP address spoofing, source routing attacks, κλπ) και διαχειρίζεται την πρόσβαση στο Internet μέσω του DMZ δικτύου. Επιτρέπει στα εξωτερικά συστήματα να προσπελάσουν

μόνο τον bastion host, πιθανόν και τον information server. Ο εσωτερικός router παρέχει μια δεύτερη γραμμή άμυνας πετυχαίνοντας την πρόσβαση στο προστατευμένο δίκτυο, μέσω του DMZ δικτύου, επιτρέποντας την επικοινωνία που προέρχεται από τον bastion host.

Υπάρχουν ορισμένα βασικά πλεονεκτήματα με την υλοποίηση ενός screened subnet firewall system:

α. Ο εισβολέας πρέπει να διασπάσει τρεις ξεχωριστές συσκευές διεισδύοντας στο προστατευμένο δίκτυο. Τον εξωτερικό router, τον bastion host και τον εσωτερικό router.

β. Το μόνο που φαίνεται στα συστήματα από το Internet είναι ορισμένα από τα συστήματα που βρίσκονται στο DMZ δίκτυο. Αυτό δίνει το πλεονέκτημα στον διαχειριστή του συστήματος να εξασφαλίσει ότι το προστατευμένο δίκτυο είναι αόρατο και μόνο αυστηρά επιλεγμένα συστήματα του DMZ δικτύου είναι γνωστά στο Internet μέσω routing tables και DNS.

γ. Αντίστροφα τα συστήματα του προστατευμένου δικτύου προσπελαύνουν ορισμένα συστήματα του DMZ δικτύου μέσω του εσωτερικού router χωρίς την απευθείας πρόσβαση στο Internet. Έτσι εξασφαλίζεται ότι οι χρήστες του προστατευμένου δικτύου χρησιμοποιούν proxy υπηρεσίες που βρίσκονται στον bastion host.

δ. Ο εσωτερικός router υποστηρίζει τη διακίνηση περισσότερων πακέτων από ένα dual – homed bastion host όταν λειτουργεί σαν τελικός firewall μεταξύ Internet και του προστατευμένου δικτύου μας.

ε. Επειδή το DMZ δίκτυο είναι διαφορετικό από το προστατευμένο δίκτυο, μπορεί να χρησιμοποιηθεί ένας "Network Address Translator" εγκατεστημένος στον bastion host για να αποφευχθεί η επαναρίθμηση του προστατευμένου δικτύου.

στ. Οι packet filtering routers κατευθύνουν την επικοινωνία απευθείας σε ορισμένα συστήματα στο DMZ δίκτυο, περιορίζοντας την ανάγκη χρησιμοποίησης dual – homed bastion host.

9.2. Πολιτική διαχείρισης

Ο υπεύθυνος ασφάλειας θα πρέπει να ορίσει τους αρμόδιους για τη διαχείριση του firewall(οι οποίοι θα πρέπει να αναφέρονται στην πολιτική ασφάλειας).

Κάθε υπεύθυνος διαχείρισης του firewall θα πρέπει να παρέχει επαρκή στοιχεία για να είναι εύκολη η επικοινωνία μαζί του σε περίπτωση ανάγκης, για παράδειγμα τον αριθμό τηλεφώνου του σπιτιού του, τον αριθμό του κινητού, την home e-mail address κτλ.

Ο υπεύθυνος διαχείρισης θα πρέπει να έχει τεχνικές γνώσεις σε δίκτυα υπολογιστών. Για παράδειγμα, δεδομένου του ότι οι περισσότεροι firewall βασίζονται στο πρωτόκολλο TCP/IP, ο διαχειριστής του firewall θα πρέπει να γνωρίζει τη λειτουργία και τις ιδιαιτερότητες του πρωτοκόλλου αυτού.

Οι υπεύθυνοι διαχείρισης του firewall θα πρέπει περιοδικά να εκπαιδεύονται σε τεχνικά θέματα firewalls και ασφάλειας δικτύων. Τα firewalls είναι ορατό τμήμα του δικτύου της επιχείρησης από το internet και επομένως αποτελούν κύριο στόχο επιθέσεων από επιτήδειους. Μόνο οι διαχειριστές τους θα πρέπει να έχουν λογαριασμούς στην κονσόλα του firewall. Απαιτείται αυστηρή προστασία των usernames/passwords των διαχειριστών του firewall.

Για οποιαδήποτε τροποποίηση στη διαμόρφωση του firewall απαιτείται η έγκριση του υπεύθυνου δικτύου και θα πρέπει να πραγματοποιείται μόνο από τον υπεύθυνο διαχείρισης του firewall. Επίσης απαιτείται ισχυρή φυσική προστασία γύρω από τον firewall host και είναι προτιμητέο η διαχείριση του firewall να γίνεται μόνο από άμεσο συνδεδεμένο τερματικό. Το firewall θα πρέπει να τοποθετείται σε ένα ελεγχόμενο περιβάλλον με επιτρεπόμενη πρόσβαση μόνο στον υπεύθυνο δικτύου και στους διαχειριστές του firewall.

Σε περίπτωση που το firewall λειτουργεί και ως DNS server(κάνει αντιστοίχηση των domain names σε IP address) θα πρέπει να διαμορφωθεί έτσι ώστε να μην αποκαλύπτει πληροφορίες σχετικά με την τοπολογία του δικτύου της επιχείρησης. Επίσης τα host names και οι διευθύνσεις των υπολογιστικών συστημάτων του δικτύου δεν θα πρέπει να αποκαλύπτονται στο εξωτερικό δίκτυο.

9.2.1. Πολιτική διαχείρισης από μακριά

Για λειτουργικούς λόγους συχνά απαιτείται η διαχείριση του firewall να γίνεται από μακριά. Προφανώς απαιτείται να ληφθούν ισχυρά μέτρα ασφάλειας έτσι ώστε η διαχείριση των firewalls να μην εκτίθεται σε κινδύνους.

Χαμηλό Επίπεδο Επικινδυνότητας :

Για την διαχείριση του firewall από μακριά μέσω αναξιόπιστων δικτύων θα πρέπει να χρησιμοποιούνται τεχνικές ισχυρής αυθεντικοποίησης όπως one-time passwords σε συνδυασμό με hardware tokens.

Μεσαίο Επίπεδο Επικινδυνότητας :

Είναι προτιμητέο η διαχείριση του firewall να γίνεται μόνο από άμεσα συνδεδεμένο τερματικό και όχι μέσω αναξιόπιστου δικτύου. Φυσική πρόσβαση στο τερματικό διαχείρισης του firewall θα πρέπει να έχουν μόνο οι υπεύθυνοι διαχείρισής του.

Η διαχείριση του firewall από μακριά θα πρέπει να περιορίζεται μόνο στα πλαίσια του εσωτερικού και αξιόπιστου δικτύου της επιχείρησης. Για λόγους ασφάλειας θα πρέπει να χρησιμοποιούνται τεχνικές ισχυρής αυθεντικοποίησης όπως one-time passwords και hardware tokens.

Εάν επιτραπεί η διαχείριση του firewall να γίνεται μέσω αναξιόπιστου δικτύου τότε θα πρέπει να χρησιμοποιηθεί απαραίτητα κρυπτογράφηση απ' άκρη σ' άκρη και τεχνικές ισχυρής αυθεντικοποίησης.

Υψηλό Επίπεδο Επικινδυνότητας

Απαγορεύεται η διαχείριση του firewall να γίνεται από μακριά αλλά μόνο από άμεσα συνδεδεμένο τερματικό. Φυσική πρόσβαση στο τερματικό διαχείρισης του firewall θα πρέπει να έχουν μόνο οι υπεύθυνοι διαχειριστές του firewall.

9.3. Πολιτική Recovery Plan

Προκειμένου να υποστηρικτεί επαναφορά του firewall σε περίπτωση αποτυχίας ή φυσικής καταστροφής απαιτείται να πραγματοποιείται back-up του firewall (λογισμικό του firewall, configuration data, αρχεία βάσεων δεδομένων κ.λ.π) σε ημερήσια βάση.

Το back-up του firewall θα πρέπει να αποθηκεύεται σε read-only συσκευές αποθήκευσης. Στα περιβάλλοντα μεσαίου και υψηλού επιπέδου επικινδυνότητας απαιτείται να υπάρχει διαθέσιμο και ένα δεύτερο firewall έτσι ώστε σε περίπτωση βλάβης ή δυσλειτουργίας η αντικατάσταση να είναι άμεση.

9.4. Πολιτική για τον Έλεγχο της Ακεραιότητας του Firewall

Προκειμένου να ελεχθούν μη εξουσιοδοτημένες τροποποιήσεις στη διαμόρφωση του firewall απαιτείται επιστάμενος έλεγχος ακεραιότητας.

Θα πρέπει να χρησιμοποιούνται διάφορες τεχνικές για τον έλεγχο της ακεραιότητας του firewall όπως αθροίσματα ελέγχου, αλγόριθμοι κατακερματισμού κ.λ.π.

Στην περίπτωση τροποποίησης της διαμόρφωσης του firewall θα πρέπει να ενημερώνεται η βάση δεδομένων για τον έλεγχο της ακεραιότητας και θα πρέπει να κρατείται αντίγραφο σε read-only συσκεύη αποθήκευσης.

Τουλάχιστον σε εβδομαδιαία βάση θα πρέπει να ελέγχεται η ακεραιότητα του firewall προκειμένου να εντοπιστούν τυχόν αρχεία που έχουν τροποποιηθεί, αντικατασταθεί ή διαγραφεί. Προκειμένου να ανιχθευθούν τυχόν εισβολές θα πρέπει να γίνεται καταγραφή της κίνησης.

Τα αρχεία καταγραφής του firewall θα πρέπει να επιθεωρούνται σε εβδομαδιαία βάση προκειμένου να εντοπιστούν τυχόν επιθέσεις στο δίκτυο της επιχείρησης.

9.5. Πολιτική Αναβάθμισης

Προκειμένου να βελτιωθεί η επίδοση του firewall θα πρέπει να ακολουθηθούν οι οδηγίες του προμηθευτή για το είδος του επεξεργαστή και τη μνήμη που απαιτείται.

Ο διαχειριστής του firewall θα πρέπει να ενημερώνεται και να αξιολογεί τα νέα προιόντα που κυκλοφορούν στην αγορά προκειμένου να εκτιμήσει εάν απαιτείται αναβάθμιση του firewall που χρησιμοποιεί η επιχείρηση.

Απαιτείται συνεχής συνεργασία με τον προμηθευτή του firewall έτσι ώστε η επιχείρηση να είναι ενήμερη εάν απαιτείται αναβάθμιση του firewall που χρησιμοποιεί.

Εάν η προμηθεύτρια εταιρεία προτείνει αναβάθμιση, ο διαχειριστής του firewall και ο υπέυθυνος διαχείρισης του συστήματος θα πρέπει να πιστοποιήσει την ανάγκη αναβάθμισης.

Αρχικά η νέα έκδοση του firewall θα πρέπει να χρησιμοποιηθεί σε πιλοτική βάση προκειμένου να ελεγχθεί η ποιότητα του προιόντος και σε μεταγενέστερη φάση θα πρέπει να τεθεί σε κανονική λειτουργία.

9.6. Πολιτική Χρήσης

Προφανώς και η πολιτική χρήσης των firewalls θα πρέπει να διαφοροποιείται ανάλογα με το επίπεδο επικινδυνότητας που χαρακτηρίζει την επιχείρηση.

Χαμηλό Επίπεδο Επικινδυνότητας :

Οι χρήστες για να έχουν πρόσβαση στις Internet υπηρεσίες θα πρέπει να χρησιμοποιούν company-approved λογισμικό και Internet gateways.

Το firewall τοποθετείται μεταξύ του ιδιωτικού δικτύου της επιχείρησης και του Internet προκειμένου να προστατευτούν τα υπολογιστικά συστήματα της επιχείρησης. Οι χρήστες θα πρέπει να συνδέονται στο Internet χρησιμοποιώντας υποχρεωτικά το firewall και όχι μέσω modem.

Θα πρέπει να απαγορεύεται η δρομολόγηση πηγής από όλους τους firewall και routers.

Το firewall δεν θα πρέπει να δέχεται αιτήσεις στις εξωτερικές διεπαφές του, όπου ως διεύθυνση πηγής εμφανίζεται κάποια διεύθυνση του εσωτερικού δικτύου της επιχείρησης.

Το firewall θα πρέπει να παρέχει λεπτομερή καταγραφή της κίνησης όλων των συνόδων και σε μεταγενέστερη φάση θα πρέπει να γίνεται επιθεώρηση των στοιχείων αυτών.

Ο διαχειριστής του firewall θα πρέπει να πιστοποιήσει την αξιοπιστία και την ποιότητα των firewalls προτού τεθούν σε κανονική λειτουργία.

Τα δεδομένα τεκμηρίωσης της λειτουργίας του firewall θα πρέπει να τηρούνται και off-line. Μεταξύ άλλων θα πρέπει να είναι διαθέσιμες πληροφορίες όπως : οι IP διευθύνσεις όλων των συσκευών του δικτύου, οι IP διευθύνσεις του Internet Service Provider, του DNS server καθώς και οι κανόνες φιλτραρίσματος των πακέτων. Τα στοιχεία αυτά θα πρέπει συνεχώς να ενημερώνονται προκειμένου να είναι ακριβή.

Μεσαίο Επίπεδο Επικινδυνότητας :

Συμπεριλαμβάνονται και οι οδηγίες του χαμηλού επιπέδου επικινδυνότητας .

Η πρόσβαση στα εσωτερικά συστήματα της επιχείρησης μέσω του firewall απαιτεί ισχυρή αυθεντικοποίηση χρησιμοποιώντας one-time passwords και hardware tokens.

Ο διαχειριστής του firewall και οι υπεύθυνοι ασφαλείας θα πρέπει να αναθεωρούν περιοδικά την πολιτική ασφάλειας του firewall (περίπου κάθε εξάμηνο).

Οι λεπτομέρειες για την τοπολογία και διαμόρφωση του εσωτερικού και αξιόπιστου δικτύου της επιχείρησης θα πρέπει να διατηρούνται μυστικές.
Το firewall θα πρέπει να διαμορφωθεί έτσι ώστε να απαγορεύει τις υπηρεσίες που δεν επιτρέπονται.

Το firewall θα πρέπει να ειδοποιεί τον διαχειριστή του συστήματος, σχεδόν σε πραγματικό χρόνο, για τυχόν εισβολή που έχει ανιχνευθεί έτσι ώστε η αντίδραση να είναι άμεση.

Το υπολογιστικό σύστημα του firewall θα πρέπει να έχει μόνο το λογισμικό που είναι απαραίτητο για να υλοποιηθούν οι λειτουργίες του firewall. Editors, Compilers και λογισμικό επικοινωνιών θα πρέπει να απενεργοποιηθεί ή διαγραφεί από το υπολογιστικό σύστημα του firewall.

Υψηλό Επίπεδο Επικινδυνότητας :

Συμπεριλαμβάνονται και οι οδηγίες του χαμηλού και μεσαίου επιπέδου επικινδυνότητας.

Η προσωπική χρήση του Internet από τα υπολογιστικά συστήματα της επιχείρησης απαγορεύεται.

Ο browser που χρησιμοποιούν οι εργαζόμενοι θα πρέπει να διαμορφωθεί έτσι ώστε να απαγορεύει την πρόσβαση σε sites που δεν εγκρίνονται από την διεύθυνση ασφαλείας της επιχείρησης.

Οι πληροφορίες πρόσβασης στις Internet υπηρεσίες θα πρέπει να καταγράφονται έτσι ώστε να εντοπίζεται τυχόν παραβίαση της πολιτικής ασφαλείας.

10. Προϋποθέσεις Τεχνολογίας Firewalls

Εκτός όμως από τις ανάγκες των χρηστών που καλύπτει ένα firewall πρέπει να συνεξετασθούν και οι προϋποθέσεις που πρέπει να ισχύουν προκειμένου να χρησιμοποιηθεί η τεχνολογία των firewalls.

α. Ο System Administrator ο οποίος θα προτείνει την αγορά και τοποθέτηση ενός Firewall στην εταιρεία ή τον οργανισμό τον οποίο αντιπροσωπεύει θα πρέπει σε συνεργασία με τη Δκση της εταιρείας ή του οργανισμού να αποφασίσουν αν και γιατί θα πρέπει να τοποθετήσουν Firewall στο δίκτυο τους. Στην περίπτωση που το είδος των δεδομένων που επεξεργάζονται είναι τέτοια που από τη φύση τους απαιτούν υψηλό επίπεδο ασφάλειας ,π.χ. διαβαθμισμένα, επιβάλλεται η μη χρησιμοποίηση των υπηρεσιών του Internet. Σε τέτοια περίπτωση κρίνεται σκόπιμη η χρησιμοποίηση Firewall σε τμήμα του δικτύου όπου απαιτείται υψηλό επίπεδο ασφάλειας και απομόνωσης του από το υπόλοιπο δίκτυο.

β. Η τοποθέτηση firewall στο δίκτυο μας, είτε σε τοπικό επίπεδο είτε για τη σύνδεση μας με Internet, πρέπει να εξετασθεί ως μέρος της συνολικής πολιτικής ασφάλειας και όχι η ασφάλεια του δικτύου να στηριχθεί στην χρησιμοποίηση του. Δηλαδή να μη θεωρηθεί η χρησιμοποίηση firewalls ως πανάκεια στον τομέα της ασφάλειας.

γ. Ο System Administrator σε συνεργασία με τη Δκση θα πρέπει να σταθμίσει το κόστος αγοράς και συντήρησης ενός firewall σε συνάρτηση με το κόστος οποιασδήποτε δολιοφθοράς εισβολέα στο δίκτυο που προίσταται. Σε περίπτωση που το κόστος της δολιοφθοράς είναι κατά πολύ μεγαλύτερο του κόστους αγοράς η κάθε Δκση θα πρέπει να πεισθεί στην αγορά και τοποθέτηση τεχνολογίας Firewall.

δ. Δεν θα πρέπει να ξεχνιέται το μελλοντικό κόστος συντήρησης ενός Firewall που πολλές φορές είναι πολλαπλάσιο του κόστους αγοράς του.

ε. Η πολιτική ασφάλειας είναι κάτι που ενδιαφέρει περισσότερους από τον System Administrator (Business administrators, network managers, information managers,webmasters e.t.c).

στ. Ο σχεδιασμός για τη διαμόρφωση ενός firewall υπάγεται στο γενικότερο σχεδιασμό πολιτικής ασφάλειας της Δκσης του οργανισμού ή της επιχείρησης. Η Δκση σε συνεργασία με τον System - Network Administrator, πιθανόν τον DBA θα πρέπει να αποφασίσουν από κοινού εάν και κατά πόσο η ασφάλεια του δικτύου είναι σημαντικότερη από την ευκολία χρήσης των υπολογιστικών πόρων και των ευκολιών του Internet κατά συνέπεια την ευκολία των εργαζομένων. Σ' αυτή την περίπτωση ισχύουν τα εξής αλληλοσυγκρουόμενα:

1. Ότι δεν επιτρέπεται ρητά, ΑΠΑΓΟΡΕΥΕΤΑΙ.
2. Ότι δεν απαγορεύεται ρητά, ΕΠΙΤΡΕΠΕΤΑΙ.

Η σπουδαιότητα του παραπάνω διαχωρισμού είναι κάτι στο οποίο δεν πρέπει να δοθεί παραπάνω έμφαση από όση απαιτείται. Στην 1η περίπτωση ο σχεδιασμός του firewall είναι τέτοιος όπου "μπλοκάρει" τα πάντα. Κάθε μία υπηρεσία παρέχεται μετά από προσεκτικό προσδιορισμό ανάγκης και κινδύνου και σε κάθε περίπτωση ξεχωριστά. Αυτό όμως μπορεί να προκαλέσει τη δυσφορία των χρηστών που θ' αντιμετωπίσουν τον firewall σαν εμπόδιο. Στη 2η περίπτωση ο System Administrator βρίσκεται σε δύσκολη θέση διότι θα πρέπει να έχει μαντικές ικανότητες προκειμένου να προσδιορίσει όλες τις πιθανές απειλές και επιθέσεις που θα δεχθεί μέσα και έξω από το δίκτυο του ώστε να λάβει τα μέτρα που απαιτούνται για ν' αντιμετωπίσει τους κινδύνους.

11. Στρατηγικές για την οργάνωση ενός Firewall

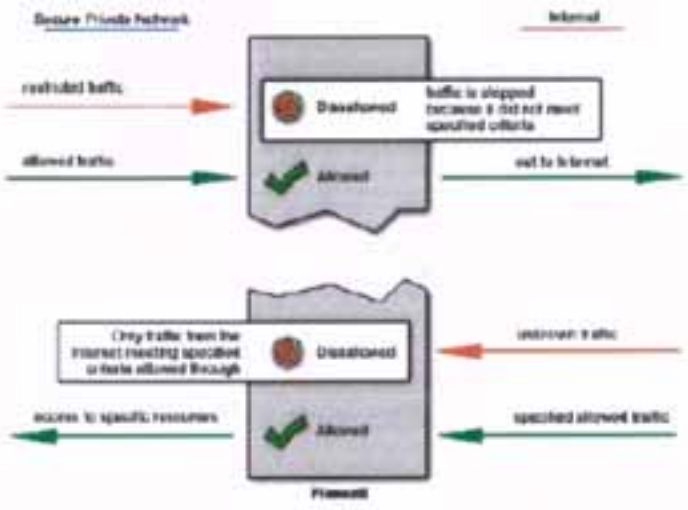
Υπάρχουν δύο μεθοδολογίες απαγόρευσης πρόσβασης από τα firewalls.

-**Default Permit**: Στην περίπτωση αυτή, δίνεται στο firewall το σύνολο των συνθηκών που απαιτούνται για να εμποδιστεί η διέλευση των δεδομένων. Κάθε υπολογιστής ή πρωτόκολλο που δεν αναφέρεται ρητά μπορεί να έχει πρόσβαση.

-**Default Deny**: Είναι το άλλο άκρο της πολιτικής που μπορεί να ακολουθείται και, στην περίπτωση αυτή, δίνεται στο firewall το σύνολο των συνθηκών που απαιτούνται, για να επιτραπεί η διέλευση των δεδομένων. Αν κάποιο πρωτόκολλο ή υπολογιστής δεν αναφέρεται ρητά τότε απαγορεύεται η διέλευση δεδομένων του .

Η υιοθέτηση της πρώτης τακτικής είναι επικίνδυνη, επειδή ο διαχειριστής μπορεί να μην αντιληφθεί εγκαίρως κάποιο λάθος που δίνει πρόσβαση σε εισβολείς.

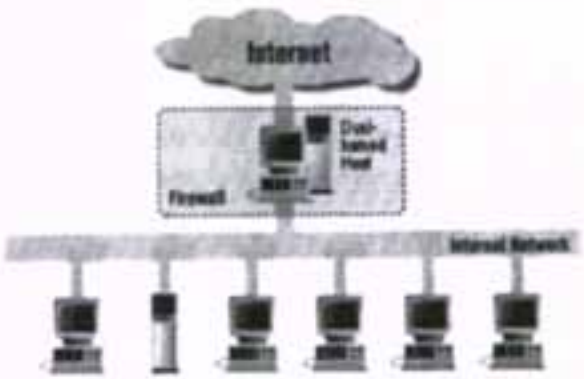
Οι δυο προαναφερθείσες στρατηγικές και ο τρόπος λειτουργίας τους φαίνεται στο παρακάτω σχήμα.



12. Αρχιτεκτονικές Διάρθρωσης

Τα Firewalls μπορούν να διαρθρωθούν ποικιλοτρόπως, σχηματίζοντας διαφορετικές αρχιτεκτονικές και παρέχοντας διαφορετικά επίπεδα ασφάλειας, με διαφορετικό κόστος εγκατάστασης και λειτουργίας. Η αρχιτεκτονική πρέπει να επιλεχτεί ανάλογα με τους κινδύνους που πρέπει να αντιμετωπιστούν.

Μια αρχιτεκτονική multi-homed είναι ένας υπολογιστής (στην δική μας περίπτωση ένα firewall) με περισσότερες από μια διεπαφές δικτύου, όπου κάθε επαφή αντιστοιχεί λογικά και φυσικά σε διαφορετικά τμήματα ενός δικτύου. Η αρχιτεκτονική dual-homed είναι ένας κεντρικός υπολογιστής με δυο διεπαφές: μια προς το εσωτερικό δίκτυο και μια προς το διαδίκτυο, που δεν επικοινωνούν μεταξύ τους παρά μόνο μέσω αυτού του υπολογιστή. Στο παρακάτω σχήμα φαίνεται η αρχιτεκτονική αυτή.



Αρχιτεκτονική Dual Homed

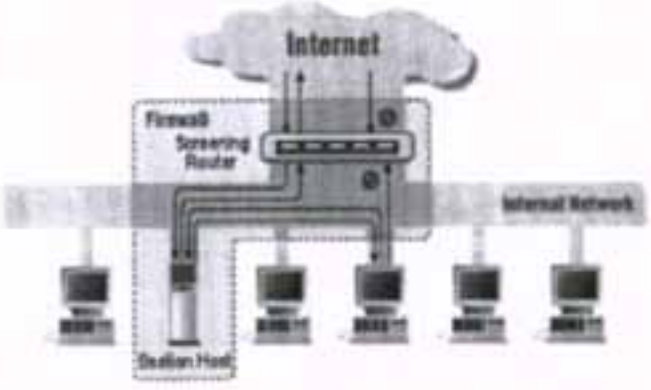
Στην αρχιτεκτονική screened-host προσφέρονται υπηρεσίες μέσω ενός κεντρικού υπολογιστή, ο οποίος συνδέεται μόνο με το εσωτερικό δίκτυο. Χρησιμοποιείται ένας ξεχωριστός δρομολογητής και η ασφάλεια πρώτου επιπέδου παρέχεται με φιλτράρισμα πακέτων. Το φιλτράρισμα πακέτων στον εξωτερικό δρομολογητή (screening router) είναι ρυθμισμένο έτσι, ώστε να επιτρέπονται συνδέσεις αφενός από το εξωτερικό δίκτυο μόνο προς τον κεντρικό υπολογιστή-ο οποίος πρέπει να έχει υψηλό επίπεδο ασφάλειας- αφετέρου συνδέσεις από τον κεντρικό υπολογιστή με το internet, οι οποίες θα καθορίζονται από την πολιτική ασφάλειας. Μπορούμε να ρυθμίσουμε το φιλτράρισμα πακέτων έτσι, ώστε να επιτρέπεται σε ορισμένους εσωτερικούς υπολογιστές να

συνδέονται απευθείας με το internet για ορισμένες υπηρεσίες, ή να τους εξαναγκάζει να χρησιμοποιούν τις υπηρεσίες proxy που παρέχει ο κεντρικός υπολογιστής. Επιπλέον είναι ευκολότερο να προστατευτεί ένας δρομολογητής που παρέχει περιορισμένες υπηρεσίες, παρά ο κεντρικός υπολογιστής. Η αρχιτεκτονική screened host παρέχει περισσότερη ασφάλεια και ευχρηστία.

Συγκρινόμενη με άλλες αρχιτεκτονικές ,όπως με την screened-subnet, παρουσιάζει ορισμένα μειονεκτήματα, διότι εάν κάποιος «καταλάβει» το δρομολογητή, τότε όλο το εσωτερικό δίκτυο είναι εκτεθειμένο. Αν καταλάβει και τον κεντρικό υπολογιστή τότε δεν υπάρχει τίποτα να τον σταματήσει, καθώς δεν υπάρχουν περαιτέρω επίπεδα ασφάλειας.

Η αρχιτεκτονική screened-subnet προσθέτει ένα επιπλέον επίπεδο ασφάλειας στη screenhost, δημιουργώντας ένα περιμετρικό δίκτυο που απομονώνει το εσωτερικό δίκτυο. Όταν απομονώσουμε τον κεντρικό υπολογιστή σε ένα περιμετρικό δίκτυο, ακόμη και αν κάποιος πετύχει πρόσβαση σε αυτόν, δεν θα έχει ολική πρόσβαση.

Υπάρχουν δυο δρομολογητές στο περιμετρικό δίκτυο: ένας συνδεμένος με το εσωτερικό δίκτυο και ένας με το internet. Μπορούμε να δημιουργήσουμε πολλά επίπεδα ασφάλειας, όσα και τα περιμετρικά δίκτυα, όπου οι περισσότερο ευπαθείς και λιγότερο ασφαλείς υπηρεσίες τοποθετούνται στα εξωτερικά επίπεδα. Έτσι εάν «σπάσει» κάποιο επίπεδο, δεν θα μείνει το υπόλοιπο δίκτυο απροστάτευτο. Αυτό προϋποθέτει διαφορετικό φιλτράρισμα σε κάθε επίπεδο. Η αρχιτεκτονική αυτή είναι ευρύτερα γνωστή ως αποστρατικοποιημένη ζώνη (Demilitarized Zone) και υποστηρίζεται από πολλά προϊόντα της αγοράς.



Αρχιτεκτονική Demilitarized zone

Συνήθως σε αυτό το ενδιάμεσο δίκτυο τοποθετούμε server δημόσια προσβάσιμους, ώστε να απομονώσουμε τον πιθανό εισβολέα έξω από το εσωτερικό μας δίκτυο. Με τον τρόπο αυτό παρεμβάλλονται τρεις συσκευές ασφαλείας στο δρόμο προς το εσωτερικό δίκτυο:ο εξωτερικός δρομολογητής που προστατεύει το δίκτυο από το internet, ο εσωτερικός δρομολογητής που προστατεύει το εσωτερικό δίκτυο από τον κεντρικό υπολογιστή και ο

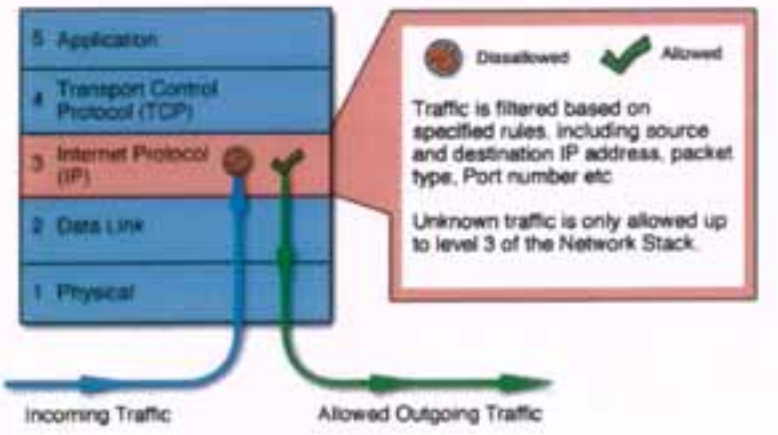
κεντρικός υπολογιστής (bastion host) που κατευθύνει όλη την κίνηση του εσωτερικού δικτύου.

13. Διάφοροι τύποι Firewalls

Τα διάφορα firewalls λειτουργούν σε διαφορετικά επίπεδα του OSI μοντέλου χρησιμοποιώντας διαφορετικά κριτήρια για τον έλεγχο της κυκλοφορίας. Το χαμηλότερο επίπεδο στο οποίο ένα firewall μπορεί να λειτουργήσει είναι το 3ο επίπεδο δηλ. το επίπεδο δικτύου στο μοντέλο OSI ή το επίπεδο του Internet Protocol για το TCP-IP μοντέλο. Στο επίπεδο αυτό ένα firewall μπορεί να καθορίσει εάν ένα πακέτο προέρχεται από έμπιστη πηγή, αλλά δεν μπορεί να γνωρίζει τι περιέχει ή με ποια άλλα πακέτα συνδέεται. Τα firewalls τα οποία λειτουργούν στο επίπεδο μεταφοράς γνωρίζουν παραπάνω πληροφορίες για τα πακέτα και μπορούν να επιτρέψουν ή να αρνηθούν πρόσβαση βασιζόμενα σε ποιο πολύπλοκα κριτήρια. Στο επίπεδο εφαρμογής, τα firewalls γνωρίζουν πολλές πληροφορίες και μπορεί να γίνουν πολύ εκλεκτικά στη χορήγηση της πρόσβασης.

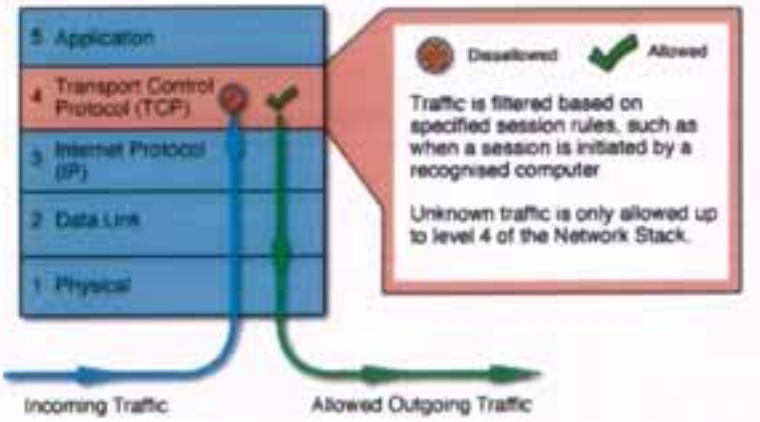
Σύμφωνα με τα προαναφερόμενα, τα firewalls που λειτουργούν σε υψηλότερα επίπεδα, όπως το επίπεδο εφαρμογής θα πρέπει να υπερέχουν των υπολοίπων. Αυτό όμως δεν είναι πάντα αλήθεια. Όσο πιο πολύ το πακέτο παρεμποδίζεται σε χαμηλότερο επίπεδο, τόσο πιο ασφαλές είναι το firewall. Εάν ο εισβολέας δεν μπορεί να περάσει το τρίτο επίπεδο είναι αδύνατο να αποκτηθεί έλεγχος του λειτουργικού συστήματος. Για το λόγο αυτό και τα επαγγελματικά firewalls λαμβάνουν κάθε πακέτο πριν από το λειτουργικό σύστημα.

Τα Firewalls εμπίπτουν σε τέσσερις ευρείες κατηγορίες: φίλτρα πακέτων (packet filters), πύλες επιπέδου κυκλώματος (circuit level gateways), πύλες επιπέδου εφαρμογής (application level gateways) και Stateful Multilayer Inspection Firewalls. Τα Packet filtering firewalls λειτουργούν στο επίπεδο δικτύου του μοντέλου OSI ή στο IP επίπεδο του μοντέλου TCP/IP. Είναι συνήθως μέρος ενός δρομολογητή. Σε ένα τέτοιο firewall κάθε πακέτο συγκρίνεται με ένα σύνολο κριτηρίων προτού να διαβιβαστεί. Ανάλογα με το πακέτο και τα κριτήρια, το Firewall μπορεί να απορρίψει το πακέτο, να το διαβιβάσει ή να στείλει ένα μήνυμα στο δημιουργό του. Οι κανόνες μπορούν να συμπεριλάβουν την διεύθυνση της πηγής (source address) και διεύθυνση προορισμού IP (destination IP address), το port πηγής και προορισμού και το χρησιμοποιούμενο πρωτόκολλο. Το πλεονέκτημα αυτών των firewalls είναι το χαμηλότερο κόστος και το χαμηλότερο αντίκτυπό τους στην απόδοση του δικτύου. Οι περισσότεροι δρομολογητές υποστηρίζουν το φιλτράρισμα πακέτων. Ακόμα κι αν χρησιμοποιούνται και άλλα firewalls, η εφαρμογή του φιλτραρίσματος πακέτων στο επίπεδο δρομολογητών προσδίδει έναν αρχικό βαθμό ασφάλειας στο επίπεδο δικτύου (Network layer). Αυτός ο τύπος Firewall λειτουργεί μόνο στο επίπεδο δικτύου και δεν υποστηρίζει ειδικούς περίπλοκους κανόνες ελέγχου. Οι Network Address Translation (NAT) routers προσφέρουν τα πλεονεκτήματα των packet filtering firewalls αλλά μπορούν επίσης να κρύψουν τις διευθύνσεις IP των υπολογιστών πίσω από το Firewall, και να προσφέρουν ένα επίπεδο circuit-based φιλτραρίσματος



Σχήμα: Packet filtering firewalls

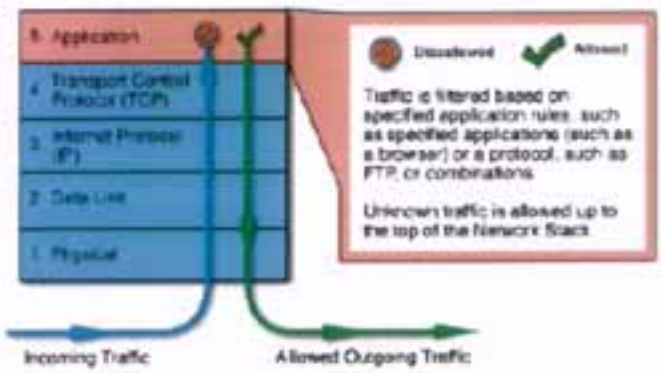
Οι πύλες επιπέδου κυκλώματος (circuit level gateways) λειτουργούν στο επίπεδο συνόδου (session layer) του προτύπου OSI, ή το επίπεδο TCP του TCP/ IP. Ελέγχουν το TCP handshaking μεταξύ των πακέτων για να καθορίσουν εάν μια ζητούμενη σύνοδος είναι νόμιμη. Οι πληροφορίες που περνούν στον απομακρυσμένο υπολογιστή (remote computer) μέσω μιας πύλης επιπέδου κυκλώματος (circuit level gateway) εμφανίζονται να προέρχονται από την πύλη. Αυτό είναι χρήσιμο για την απόκρυψη πληροφοριών που αφορούν προστατευμένα δίκτυα. Οι πύλες επιπέδου κυκλώματος (circuit level gateways) είναι σχετικά ανέξοδες και έχουν το πλεονέκτημα της απόκρυψης πληροφοριών για το ιδιωτικό δίκτυο που προστατεύουν. Στο παρακάτω σχήμα φαίνεται ο τρόπος λειτουργίας τους.



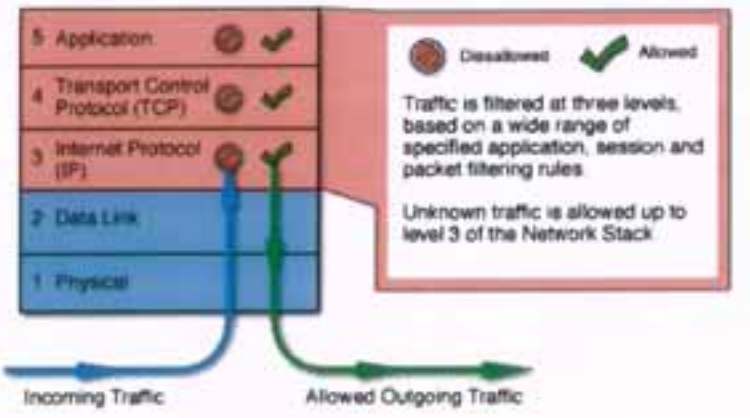
Σχήμα: Circuit Level Gateway

Οι πύλες επιπέδου εφαρμογής (Application level Gateway), αποκαλούμενες επίσης proxies, είναι παρόμοιες με τις circuit-level gateways εκτός από το ότι είναι για κάποια συγκεκριμένη εφαρμογή. Μπορούν να φιλτράρουν τα πακέτα στο επίπεδο εφαρμογής του προτύπου OSI. Τα εισερχόμενα ή εξερχόμενα πακέτα δεν μπορούν να έχουν πρόσβαση στις υπηρεσίες για τις οποίες δεν υπάρχει κανένα proxy. Με απλά λόγια, μια πύλη επιπέδου εφαρμογής που διαμορφώνεται να είναι ένα Web proxy δεν θα επιτρέψει οποιαδήποτε ftp, gopher, Telnet ή άλλη κυκλοφορία να περάσει. Επειδή εξετάζουν τα πακέτα στο επίπεδο εφαρμογής, μπορούν να φιλτράρουν τις συγκεκριμένες εντολές της εφαρμογής όπως http: post και get κ.λ.π. Αυτό δεν μπορεί να επιτευχθεί ούτε με firewalls τύπου packet filtering ούτε circuit level διότι κανένα από αυτά δεν έχει πληροφορίες στο επίπεδο εφαρμογής. Οι πύλες επιπέδων εφαρμογής μπορούν επίσης να χρησιμοποιηθούν για να καταγράψουν τη δραστηριότητα χρηστών και τα logins τους. Προσφέρουν ένα υψηλό επίπεδο ασφάλειας, αλλά ασκούν σημαντική επίδραση στην απόδοση των δικτύων.

Αυτό είναι λόγω των διακοπτών πλαισίου (context switches) που επιβραδύνουν την πρόσβαση στο δίκτυο. Οι πύλες αυτές δεν είναι διαφανείς στους τελικούς χρήστες και απαιτούν την manual διαμόρφωση κάθε client υπολογιστή. Στο παρακάτω σχήμα φαίνεται ο τρόπος λειτουργίας τους.



Τα Stateful multilayer Inspection Firewalls συνδυάζουν τις πτυχές των άλλων τριών τύπων firewalls. Φιλτράρουν τα πακέτα στο επίπεδο δικτύου, καθορίζουν εάν τα πακέτα συνόδου είναι νόμιμα και αξιολογούν το περιεχόμενο των πακέτων στο επίπεδο εφαρμογής. Επιτρέπουν τη άμεση σύνδεση μεταξύ του πελάτη (client) και του host, που μειώνει το πρόβλημα που προκαλείται από την έλλειψη διαφάνειας των πυλών επιπέδου εφαρμογής. Στηρίζονται σε αλγορίθμους για να αναγνωρίσουν και να επεξεργαστούν τα δεδομένα επιπέδου εφαρμογής αντί να τρέχουν εφαρμογές συγκεκριμένων proxies. Τα Stateful multiplayer Inspection firewalls προσφέρουν ένα υψηλό επίπεδο ασφάλειας, καλή απόδοση και διαφάνεια στους τελικούς χρήστες. Παρόλα αυτά είναι ακριβά, και λόγω της πολυπλοκότητάς τους, εάν δεν διαχειρίζονται από ικανό προσωπικό, είναι ενδεχομένως λιγότερο ασφαλή από τους απλούστερους τύπους Firewalls.



Σχήμα: Stateful Multilayer Inspection Firewall

14. Είδη Firewalls

Υπάρχουν πολλά και διάφορα είδη αρχιτεκτονικών firewalls που κυκλοφορούν στο εμπόριο. Δεν είναι δυνατό να προτείνει κάποιος κάποιο συγκεκριμένο προϊόν επειδή οι ανάγκες και τα χαρακτηριστικά καθ' ενός διαφοροποιούνται σημαντικά. Όλες οι πληροφορίες που τίθενται παρακάτω είναι ότι παρέχεται από τους πωλητές κάθε firewall. Όποιος θέλει να εγκαταστήσει ένα firewall πρέπει να καθορίσει επακριβώς τις ανάγκες του, να εγκαταστήσει ένα demo του προϊόντος και να έλθει σε επαφή με τον πωλητή του προϊόντος αφού αυτά αναβαθμίζονται σε πολύ σύντομα χρονικά διαστήματα και καινούργια χαρακτηριστικά προστίθενται έτσι ώστε η απόφαση του καθενός μπορεί να διαφοροποιηθεί κατά πολύ. Παρακάτω εξετάζονται και δίνονται περιληπτικά τα κυριότερα χαρακτηριστικά των περισσοτέρων γνωστών firewall της αγοράς. Αυτά δεν αντικατοπτρίζουν τις απόψεις του γράφοντος αλλά αυτά που ισχυρίζονται οι εταιρείες που αντιπροσωπεύουν τα προϊόντα καθώς και lab tests που διενήργησαν γνωστά εργαστήρια στον τομέα της ασφάλειας των προστατευμένων δικτύων.

Labyrinth 1.4 και 2.0

- Εγκατάσταση με χρήση command line (χρειάζονται γνώσεις Unix)
- Εγκατάσταση ήδη ρυθμισμένου πακέτου (δεν χρειάζονται γνώσεις Unix αλλά κοστίζει ακριβότερα)
- Υποστηρίζει TCP, IP, UDP, ICMP, telnet, archie, WWW, SSL-WWW, DNS, DNS Zone transfers, POP, SMTP, Finger και gopher υπηρεσίες σε επίπεδο πακέτων
- Διατίθεται VPN και κρυπτογράφηση (encryption) στην έκδοση 2.0 με χρήση του DES και του RC/5
- Το authentication περιορίζεται στη χρήση απλού user ID και password
- Υποστηρίζει logging μέσω SNMP ή απλού κειμένου
- Προσφέρει proxying των μη καταχωρημένων IP διευθύνσεων (unregistered IP addresses) (NAT)
- Δυναμική ρύθμιση κανόνων (Dynamic rule configuration)

- Παρέχεται Web-based κονσόλα διαχείρισης όπως επίσης και command line διασύνδεση με τον διαχειριστή
- Υποστηρίζει drop, deny και redirect τύπους απόκρισης, συνυπάρχει με άλλους service daemons
- Βασίζεται στις IP διευθύνσεις να υποδηλώνουν προέλευση και προορισμό, χρησιμοποιεί FIFO προσέγγιση
- V 1,4 δυσκολία στο να διατηρεί την περίμετρό του, κακό log file

Secure Network Gateway

- Βασικά είναι ένα φίλτρο πακέτων (packet filter), παρέχει telnet, SMTP και FTP
- Η εγκατάσταση δεν είναι πλήρως αυτοματοποιημένη
- Η GUI διασύνδεση με τον χρήστη είναι λειτουργική αλλά «επίπεδη»
- Οι Secure ID, SecureNET και Message Direct5 είναι οι διαθέσιμες μέθοδοι για authentication
- Παρέχεται DES-based VPN λειτουργικότητα και κρυπτογράφηση
- Παρέχει το SOCKS (λειτουργία proxy για έναν αριθμό από TCP/IP υπηρεσίες), το οποίο είναι μεν παλιό αλλά αποτελεσματικό
- Υποστηρίζει Real Audio και λειτουργεί σαν ένας SMPT mail και DNS server
- Επιτρέπει στους διαχειριστές να καθορίζουν χρόνους λήξης του authentication key (authentication key expiration times)
- Τυπικά σύνολα κανόνων (rule sets), εφαρμοσμένα σε FIFO
- Περισσότερο αποτελεσματικό σε ένα περιβάλλον IBM SystemView
- Τοπική διαχείριση με ένα GUI περιβάλλον (περιορισμένη όταν χρησιμοποιείται μέσω telnet, πιθανό πρόβλημα ασφάλειας) ή με ένα command-lin

Blackhole 3.0

- Ένας proxy εφαρμογών και circuit gateway.
- Κρυπτογραφημένο VPN (μέσω του DES) και δυνατότητες certification τρίτων κατασκευαστών μέσω του Kerberos.
- Αδυναμίες στην διαχείριση.
- Χαμηλή απόδοση.
- Παρέχει telnet, SMTP, FTP, NetACL, και gopher, ενώ για άλλες TCP/IP εφαρμογές χρησιμοποιεί γενικές TCP proxy και UDP relay επιλογές.
- MD2 και MD5 based ψηφιακές υπογραφές (digital signatures).
- Ισχυρές υπηρεσίες για authentication (S/Key. SecurID, Enigma Logic και μπορεί να ρυθμιστεί και για άλλες).
- Τυπικά ακολουθιακά σύνολα χαρακτήρων (sequential rule sets).
- Χαμηλή λειτουργικότητα.
- Δεν επιτρέπει την τυπική πρόσβαση ασφαλείας (standard security access denied) και έτσι βελτιώνει την ασφάλεια.
- Η διαχείριση του συστήματος μπορεί να γίνει με άμεση, authenticated πρόσβαση στην κονσόλα ή με απομακρυσμένη authenticated πρόσβαση μέσω του NetACL (μια όχι και τόσο φιλική προς τον χρήστη επιλογή).

Gauntlet 3.2

- Δεν έχει σαφή και καλογραμμένη τεκμηρίωση
- Περιορισμένη GUI διασύνδεση με τον χρήστη

- Παρέχει HTTP, SMTP/POP3, FTP, NNTP, SHTTP/SSL, gopher, X Window συστήματα, LP υπηρεσίες εκτύπωσης, telnet, Rlogin και Rsh
- Το VPN υποστηρίζεται μόνο σαν επιπρόσθετο (add-on)
- Λεπτομερής λειτουργία logging (μπορεί όμως να καταναλώσει χώρο στο δίσκο πολύ γρήγορα)
- Είναι φτηνό
- Δύσκολη εγκατάσταση λόγω της περιορισμένης GUI διασύνδεση με τον χρήστη

Cyberguard 2.2 και 3.0

- Διαθέσιμο σε προεγκατεστημένη (2.2) ή sofware(3.0) έκδοση
- Η έκδοση 2.2 είναι εύκολη στην εγκατάσταση, αλλά και η 3.0 απαιτεί μια ελάχιστη ρύθμιση
- Παρέχει Rlogin, telnet, FTP, HTTP, RealAudio, NNTP, X11, SMTP, SOCKS εφαρμογές και ένα εύκολα διαχειριζόμενο γενικό proxy
- Βελτιωμένη GUI διασύνδεση για διαχείριση
- Υποστήριξη για πολλαπλούς DNS servers, NAT-based illegal address proxying και SNMP traps.
- Authentication με χρήση του SecureID στην έκδοση 3.0
- Δύο τύποι VPN, tightly και loosely coupled.
- Εύχρηστο menu για τις ρυθμίσεις του VPN
- Άριστο logging utility
- Multiprocessor αρχιτεκτονική.

- Οι κανόνες του φίλτρου πακέτων (packet filter rules) εφαρμόζονται είτε λειτουργούν οι υπηρεσίες proxy services είτε όχι.
- Ξεκάθαροι και σαφείς Clear κανόνες του φίλτρου πακέτων.
- Deny, permit και proxy επιλογές.
- Τα σύνολα κανόνων εφαρμόζονται βάσει FIFO.
- Πολύ καλές logging και alarm notifications.

Eagle 3.1

- Το πλήρες GUI είναι δύσκολο να εγκατασταθεί
- Τα διαθέσιμα proxies στην έκδοση 3.1 είναι τα HTTP, telnet, SMTP, FTP, gopher, WWW και δύο ρυθμιζόμενα από τον χρήστη proxies
- Υποστηρίζει Web URL blocking
- Στην έκδοση 4.0 παρέχονται και RealAudio, Java protection και SQL *NET
- Υποστηρίζει τα Advanced Computing Environment (ACE) Server authentication, SecureID κάρτες, Cryptocards, S/Key, RADIUS και μια βασική gateway password υπηρεσία
- Το logging γίνεται μέσω ειδοποιήσεων στην κονσόλα, pager, fax, e-mail ή SNMP traps
- Υποστηρίζει τις καλύτερες VPN υπηρεσίες κάνοντας χρήση των DES, Triple DES, RC/2, IPSec και IPSwipe αλγορίθμων
- Υπάρχει (στην έκδοση 4.0) επιλογή για packet filtering για VPN
- Το σύνολο κανόνων αντιμετωπίζεται σαν να είναι «επίπεδο» έτσι ώστε να μπορούν να εφαρμοστούν οι πιο σημαντικοί κανόνες

- Η εγκατάσταση προσφέρεται σε 4mm και 8mm ταινίες, και εκτελείται μέσω UNIX command line, ενώ ρυθμίζεται μέσω ενός Motif-compliant GUI interface
- Η διαχείριση γίνεται είτε τοπικά είτε απομακρυσμένα. Και στις δύο περιπτώσεις χρησιμοποιείται το GUI interface (Hawk)
- Κάθε απομακρυσμένο σύστημα πρέπει να ρυθμίζεται ξεχωριστά (τα σύνολα κανόνων δεν μπορούν να αντιγραφούν από το ένα σύστημα σε ένα άλλο)

Firewall-1 2.1 και 3.0

- Πλήρες X-Windows GUI interface
- Υποστηρίζει HTTP, telnet, archie, SNMP, gopher, WWW, X11, DNS και POP2/3
- Ενσωματωμένη scripting γλώσσα που δίνει την δυνατότητα στον χρήστη να καθορίσουν νέες υπηρεσίες /λειτουργίες πέρα από τις παραπάνω
- Προσφέρει proxying των μη καταχωρημένων IP διευθύνσεων (unregistered IP addresses) (NAT)
- Ενισχυμένη ασφάλεια περιεχομένου μέσω virus checking, specified resource protection (ανά URL, file name) και SMTP command protection
- Πλήρης υποστήριξη για διάφορα news services όπως Netscape CoolTalk και Microsoft Meeting
- Γρήγορη και εύχρηστη VPN λειτουργία και η κρυπτογράφηση μπορεί να εφαρμοστεί σε οποιαδήποτε μορφή traffic που μπορεί να περάσει από το firewall
- Πολύ απλό και κατανοητό σύστημα κανόνων το οποίο ρυθμίζεται εξ' ολοκλήρου από το GUI

Borderware 3.1 και 4.0

- Υποστηρίζει telnet, gopher, Finger, POP, SMTP, FTP, WWW, NNTP
- Δεν υποστηρίζει proxying των μη καταχωρημένων IP διευθύνσεων (unregistered IP addresses) (NAT)
- Οι επιλογές για authentication είναι οι SecureID, CRYPTOcard, και ειδικοί ασφαλείς FTP και telnet daemons με password protection
- Λειτουργεί βασικά σαν ένα packet filtering firewall, αλλά υποστηρίζει και application services μέσω του Secure Server Network (SSN)
- Τα σύνολα κανόνων είναι FIFO και το φιλτράρισμα είναι ιεραρχικό
- Η απομακρυσμένη διαχείριση γίνεται μέσω ενός Web-based front-end με Java-enhanced security και end-to-end κρυπτογράφηση.

Alta Vista Software Firewall 97

- Υποστηρίζει Gopher, Http, Http/SSL, FTP.
- Υποστηρίζει alert με e – mail η pager η audio alarm.
- Συνδυάζει application gateways, real time alarms, ισχυρή αυθεντικοποίηση GUI.
- Επίσης είναι με μεγάλη διαφορά ο γρηγορότερος firewall χωρίς να "θυσιάζει" την ασφάλεια.
- Υποστηρίζει τα πιο κοινά services περιλαμβάνοντας FTP, remote sessions (Telnet), WWW, Mail, News, SQL*Net, RealAudio,και Finger.
- Χρησιμοποιεί SSL και έξυπνες κάρτες όπως SecureID από την Security Dynamics αλλά πρέπει να αγορασθούν ξεχωριστά.. Επίσης CryptoCards passwords.

- Επιτρέπει την απομακρυσμένη πρόσβαση από οποιοδήποτε μηχάνημα που τρέχει WinNT – 95 μέσω ενός HTML interface με την χρησιμοποίηση της Java προκειμένου να επιτευχθεί μεταφερσιμότητα. Επίσης επιτυγχάνει ασφαλή απομακρυσμένη διαχείριση μέσω του Altavista Tunnel που χρησιμοποιεί πιστοποίηση RSA 512 bit,MD5 ακεραιότητα και κρυπτογράφηση με SA 128 bit.

Gnat Box Firewall

- Ο απλούστερος firewall της αγοράς με τις λιγότερες απαιτήσεις σε υπολογιστικούς πόρους.
- "Μπουτάρει" και "τρέχει" από δισκέτα.
- Γρήγορη και απλή διευθέτηση (5 βήματα).
- Ασφαλής προστασία με τη χρησιμοποίηση δοκιμασμένης τεχνικής για firewalls.
- Διαφανής πρόσβαση για TCP, UDP εφαρμογές και μη συνήθεις εφαρμογές όπως RealAudio/Video, StreamWorks, VDOLive, Vextreme.
- Δεν υπάρχει περιορισμός στον αριθμό των χρηστών.
- Δεν υπάρχει δυνατότητα για loggin, Telnet ούτε μπορεί να χρησιμοποιηθεί σε έναν Mail η Web Server.
- Δεν τρέχει σε UNIX μολονότι χρησιμοποιεί την τεχνολογία του πυρήνα του UNIX.
- Η GTA εταιρεία κατασκευής του προιόντος πιστεύει τόσο πολύ σε αυτό ώστε το χρησιμοποιεί για την προστασία του site της με ταυτόχρονη δήλώση της.

15. Έρευνα αγοράς

15.1 Κριτήρια σύγκρισης Firewalls

Τα κριτήρια που μπορούν να χρησιμοποιηθούν για σύγκριση των firewalls είναι τα ακόλουθα:

1. Αποτελεσματικότητα της παρεχόμενης προστασίας (Effectiveness of security protection) σε: Διείσδυση (Penetretion), Δούρειοι Ίπποι (Trojans), Έλεγχο διαρροών (controlling leaks), Άρνηση της υπηρεσίας.(DoS-Denial of Service)

2. Αποτελεσματικότητα στην ανίχνευση παρείσφρησης (Effectiveness of intrusion detection): Μικρός αριθμός λανθασμένων προειδοποιήσεων, Ειδοποίηση σε περίπτωση επικίνδυνων επιθέσεων.

3. Αποτελεσματικότητα αντίδρασης (Effectiveness of reaction): Δυνατότητα ανακάλυψης της ταυτότητας του επιτιθεμένου, Μπλοκάρισμα επιθέσεων, Ευκολία στη χρήση (ease of use).

4. Διεπαφή με τον χρήστη (User interface): Ευκολία στη χρήση, Απλότητα, Ποιότητα της online βοήθειας. Ακόμα παροχή δυνατότητας πρόσθεσης, αφαίρεσης και ελέγχου κανόνων πρόσβασης. Επίσης εύκολη κατανόηση των ερωτήσεων του λογισμικού καθώς και των ενεργειών που αυτό εκτελεί.

5. Κόστος: Ύπαρξη δοκιμαστικής περιόδου, Δυνατότητα και κόστος υποστήριξης/έτος

15.2 Τρόποι ελέγχου των Firewalls

Α) Χρησιμοποίηση της εντολής ping και πρόσβαση σε δικαιώματα προς και από τον υπό έλεγχο host.

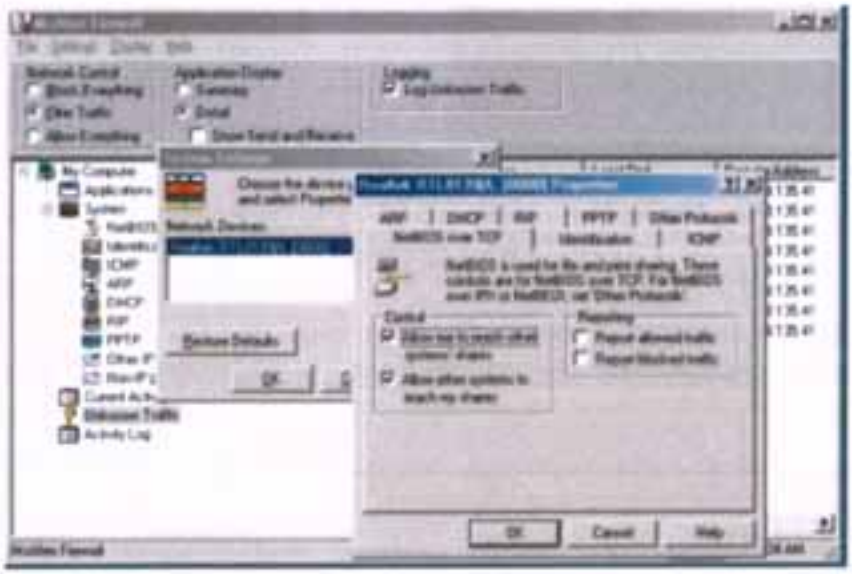
Β) Εγκατάσταση ενός ισχυρού "remote-control" Trojan (Netbus Pro v2.1) στο σύστημα σε ένα nonstandard port (για να γίνει η ανίχνευση πιο δύσκολη) και προσπάθεια του Netbus server να συνδεθεί από ενα remote system.

Γ) Ενεργοποίηση telnet server στον υπό έλεγχο υπολογιστή. Προσπάθεια σύνδεσης στον υπολογιστή αυτό από άλλη τοποθεσία.

Δ) Σκανάρισμα κάθε firewall χρησιμοποιώντας το εργαλείο nmap για να ελεγχθούν ποια ports μπλοκαρίστηκαν από τα firewalls αποτελεσματικά.

15.3 Αναλυτική παρουσίαση και σύγκριση των Firewalls

15.3.1 McAfee Firewall 2.1.3



Το McAfee Firewall βασίζεται στο Conseal Signal-9 Private Desktop. Σύμφωνα με το README αρχείο που το συνοδεύει η διαχείριση της ιδιωτικότητας του δικτύου γίνεται μέσω δυο περιοχών. Η μια είναι η κίνηση εφαρμογής και η άλλη η κίνηση συστήματος (APPLICATION traffic και SYSTEM traffic). Η APPLICATION traffic βασίζεται σε εφαρμογές που εμπιστευόμαστε και σε αυτές που δεν εμπιστευόμαστε αλλά γνωρίζουμε και χρησιμοποιούμε.

Η SYSTEM traffic είναι πιο στατική και θα επιτρέψει ή δεν θα επιτρέψει πράγματα όπως κοινή χρήση αρχείων (fileshare) και ICMP (control) traffic. Ακόμα το McAfee firewall θα διαχειριστεί μια λίστα από «έμπιστες εφαρμογές» και μια από «μη έμπιστες» εφαρμογές. Υπάρχει πάντα η δυνατότητα να γίνει κλικ πάνω στην εφαρμογή για να φανεί αυτή η λίστα και να μετακινηθούν εφαρμογές από την μια περιοχή στην άλλη.

Η συμπεριφορά του συστήματος καθορίζεται κάτω από το κουμπί System για κάθε υσκευή. Κάθε συσκευή μπορεί να έχει τη συμπεριφορά της. Π.χ μια κάρτα δικτύου μπορεί να επιτρέψει κοινή χρήση αρχείων-fileshares (με διαμοιρασμό των πόρων μεταξύ των έμπιστων υπολογιστών που χρησιμοποιούν το πρωτόκολλο NetBIOS). Το ίδιο πράγμα ισχύει και για άλλες βασικές υπηρεσίες.

Τα log files τοποθετούνται σε ένα ιδιωτικό folder, πχ. C:\PROGRAMFILES\McAfee\McAfeeFirewall. Τα αρχεία αυτά έχουν format YYYYMM.log. Κάθε log αρχείο μπορεί να είναι μέχρι 2 MB στο μέγεθος προτού να παραχθούν οι προειδοποιήσεις (warnings) από το σύστημα και μόνο τα ουσιαστικά μηνύματα γράφονται. Εάν δεν υπάρχει κανένα αρχείο log, δημιουργείται νέο για τον τρέχοντα μήνα. Αυτό σημαίνει ότι ένα πλήρες αρχείο log μπορεί να διαγραφεί ή να μετονομαστεί, και ένα νέο θα το αντικαταστήσει αμέσως.

Κόστος: $19.95

Κανένα πρόσθετο χαρακτηριστικό γνώρισμα όπως η προστασία από ActiveX/Java/cookies ή η antivirus προστασία. Γνωστά Trojans ή backdoors δεν ανιχνεύονται.

Κάθε εφαρμογή που προσπαθεί να επικοινωνήσει προκαλεί την εμφάνιση μηνύματος που ρωτάει τον χρήστη αν θέλει να προχωρήσει ή όχι.

Αποτελεσματικότητα προστασίας

Υπάρχουν προβλήματα με την αποτελεσματικότητα ασφάλειας:

1.Το GUI για τη διαμόρφωση του φίλτρου των πακέτων δεν είναι τόσο εύχρηστο. Υπάρχει κίνδυνος, παρά τα χρήσιμα χαρακτηριστικά γνωρίσματά του, ο χρήστης να μη μπορέσει να το χρησιμοποιήσει αποτελεσματικά.

2.Ο χρήστης μπορεί να ξεχάσει/παραμελήσει να εγκαταστήσει το φίλτρο πρωτοκόλλου, αφήνοντας μόνο την επιπέδου-εφαρμογής προστασία.

3.Η προεπιλογή (default) στη διεπαφή Ethernet, pings/shares, κ.λπ. ήταν disabled. Το σύστημα ήταν αρκετά αυστηρό.

4. Δεν είναι δυνατό κάποιος να διαμορφώσει κανόνες για συγκεκριμένα TCP/UDP ports.

Άμυνα ενάντια Netbus: Ο χρήστης ερωτάται όταν ο Netbus Server ξεκινάει: "επιτρέπετε σε NBSVR να επικοινωνήσει;". Κατόπιν το Netbus μπορεί να ελεγχθεί remotely, ανεμπόδιστο.

Το nmap ανιχνεύει την ίδια λίστα υπηρεσιών όπως χωρίς το firewall, αλλά το TCP fingerprint είναι ελαφρώς διαφορετικό. Το σκανάρισμα παρουσιάζεται ως "άγνωστη κυκλοφορία. στο GUI. Κατά την διάρκεια της κοινής χρήσης αρχείων (file sharing), αναγνώριση ταυτότητας (identification) και ICMP δεν επιτρέπονται, τα NetBIOS ports (135-139) δεν είναι πλέον ορατά στο nmap, και τα pings δεν λειτουργούν. Όλα τα άλλα ports είναι ορατά.

Αυτό το προϊόν έχει την ικανότητα να προστατεύει το PC αρκετά καλά και να καταστήσει τη διείσδυση δύσκολη, αλλά απαιτείται η προσεκτική διαμόρφωση (configuration).

Παρόλα αυτά οι λειτουργίες ανίχνευσης παρείσφρησης είναι οι βασικές.

Πλεονεκτήματα

1. Logging: Το GUI επιτρέπει στους χρήστες να δουν ποιες υπηρεσίες τρέχουν, σε ποια ports, και ποια επικοινωνία είναι κάθε στιγμή ανοικτή. Είναι εύκολο να φανεί ποια υπηρεσία δικτύων (network service) χρησιμοποιεί μια συγκεκριμένη εφαρμογή

2. Log αρχεία: Το log αρχείο είναι ένα απλό αρχείο κειμένου που μπορεί να ανοιχτεί εύκολα με το notepad. Περιλαμβάνει όχι μόνο ένα αντίγραφο της δραστηριότητας του δικτύου, αλλά και τα startup messages του firewall και ένα αρχείο με όλες τις αλλαγές των ρυθμίσεων (settings).

3. Το πρότυπο ασφάλειας είναι απλό: Ερώτηση του χρήστη εάν μια εφαρμογή επιτρέπεται να επικοινωνήσει, και μετά της επιτρέπει την ανεμπόδιστη πρόσβαση. Ο έμπειρος χρήστης μπορεί έπειτα να θέσει τους κανόνες για το επίπεδο πρωτοκόλλου και προσαρμογέα (adaptor). Υπάρχουν χαρακτηριστικά γνωρίσματα, όπως ο περιορισμός των pings σε τρία ανά sec, και η ενεργοποίηση/απενεργοποίηση της κοινής χρήσης αρχείων (file sharing) και/ή υποστήριξη remote χρήσης αρχείων.

4. Η πρόσβαση στο GUI μπορεί να προστατευθεί με password.

5. Ύπαρξη wizard κατά το configuration που καθοδηγεί το χρήστη.

6. Διαθέσιμη δοκιμαστική έκδοση 30 ημερών

Μειονεκτήματα

1.Installation:

-Ο χρήστης πρέπει να κοιτάξει το σύστημα αρχείων και να επιλέξει εκτελέσιμα (executables) των εφαρμογών που επιτρέπονται. Θα ήταν πιο φιλικό να μπορεί το firewall να ψάχνει τα drives και να παρουσιάζει στο χρήστη μια λίστα εφαρμογών για να επιλέξει από αυτές.

-Σε NT, ο χρήστης πρέπει χειροκίνητα να εγκαταστήσει τον driver του πρωτοκόλλου δικτύου. Εάν αυτό δεν γίνει, τότε κανένα φιλτράρισμα πρωτοκόλλου δεν είναι διαθέσιμο - μόνο επιτρέπει/απαγορεύει εφαρμογές. Επιπλέον, το Firewall δεν προειδοποιεί ότι το φίλτρο πρωτοκόλλου δεν είναι εγκατεστημένο.

2.Απεγκατάσταση: ο Network Driver δεν διαγράφεται αλλά πρέπει να αφαιρεθεί με το χέρι.

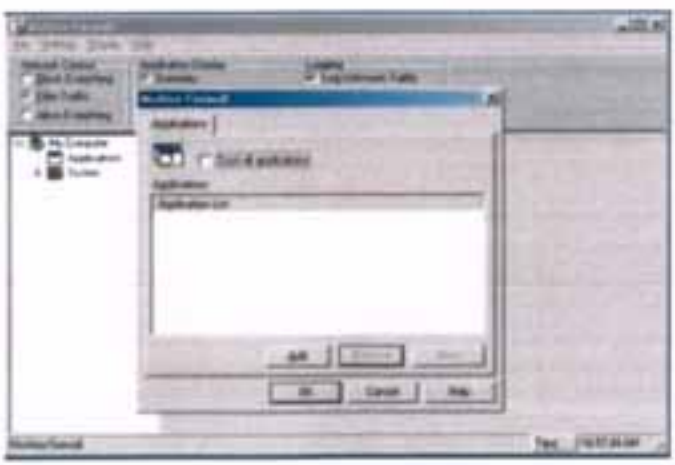
3.Το GUI είναι ιδιόμορφο:

-Όταν επιδεικνύει δραστηριότητα, έπρεπε να παρουσιάζει ποια κυκλοφορία διεπαφής (interface traffic) είναι ανοικτή.

-Ασυνέπεια: Κάνοντας δεξί κλίκ στο tray icon, το log αρχείο εμφανίζεται στο μέγιστο μέγεθος και στη σωστή θέση. Αυτές οι ρυθμίσεις δεν είναι διαθέσιμες από τη βασική διαμόρφωση του GUI.

-Το "system. GUI για τον καθορισμό των κανόνων ανάλογα με τη διεπαφή και το πρωτόκολλο πρέπει να βελτιωθεί. Τα ονόματα των διεπαφών δεν είναι πάντα κατανοητά.

-Υπάρχει μια επιλογή "trust all applications." Αυτό φαίνεται επικίνδυνο, δεδομένου ότι θα απενεργοποιούσε εντελώς το firewall.



4. Όταν μια κυκλοφορία μπλοκάρεται ακούγεται beep από το PC και μια προειδοποίηση καταγράφεται. Δεν υπάρχει κανένας τρόπος να σταματήσει αυτός ο ήχος κάτι που είναι ενοχλητικό εάν οι προειδοποιήσεις είναι εικονικές.

5. Τα port του NetBIOS δεν προστατεύονται by default.

6. Το πρότυπο ασφάλειας: Το McAfee ζητά από το χρήστη να εγκρίνει τις εφαρμογές που θέλει να μπορούν να επικοινωνούν. Αυτό είναι χρήσιμο, αλλά μερικές εφαρμογές έχουν ονόματα που δεν είναι κατανοητά στο χρήστη. Π.χ. mstask, tcpsvcs, svchost, tlntsvr

7. Δεν υποστηρίζει πλήρως Windows 2000

8. Μεγάλο μέγεθος (6.5 MB)

Προτεινόμενες βελτιώσεις:

-Επίδειξη ενός πιο κατανοητού ονόματος για την εφαρμογή και ερώτηση στο χρήστη ποιο port οι εφαρμογές θέλουν να χρησιμοποιήσουν, σε ποια διεπαφή και με ποιους επιθυμεί να επικοινωνήσει.

-Δημιουργία μιας επιλογής που θέτει σαφώς εκτός λειτουργίας την κοινή χρήση αρχείων σε όλες τις διεπαφές ή ανά διεπαφή

-Να ερωτάται ο χρήστης να επιτρέψει την εφαρμογή "μία φορά, μόνο αυτή τη φορά., " μέχρι το επόμενο reboot. ή "πάντα.."

7. Δεν είναι δυνατό να διαμορφωθούν οι κανόνες για συγκεκριμένα TCP/UDP ports

8. Καλύτερο documentation.

9.Τα power-saving modes των laptop δεν λειτουργούν με το firewall ενεργό.

10.Win2K: Η μηχανή φιλτραρίσματος πρωτοκόλλου δεν λειτουργεί - μόνο προστασία επιπέδου εφαρμογής είναι διαθέσιμη. Ακόμα τα "Systems settings" δεν λειτουργούν και όλα τα System elements στο GUI είναι κενά.

11. Εάν γίνουν αλλαγές στους κανόνες ή στις εφαρμογές, πρέπει να γίνει "Save Settings." διαφορετικά οι αλλαγές θα χαθούν στο επόμενο reboot.

12.Πιο εύκολη απεγκατάσταση

McAfee 2.1.3	
Κριτήριο	Βαθμολογία
Effectiveness of security protection (Αποτελεσματικότητα της παρεχόμενης προστασίας)	6
Αποτελεσματικότητα στην ανίχνευση παρείσφρυσης (Effectiveness of intrusion detection)	6
Αποτελεσματικότητα αντίδρασης (Effectiveness of reaction)	7
Διεπαφή με τον χρήστη (User interface)	6
Κόστος	5
Μέσος Όρος:	6

Σύνοψη

Το McAfee είναι ένα ενδιαφέρον firewall για τον συνηθισμένο και προηγμένο χρήστη εφόσον συνηθίσει τις ιδιορρυθμίες του GUI. Αυτό το προϊόν έχει την ικανότητα να προστατεύει αρκετά καλά (όχι όμως ικανοποιητικά), και να καταστήσει τη διείσδυση δύσκολη με προσεκτική διαμόρφωση. Οι ικανότητες ανίχνευσης παρείσφρησης είναι βασικές.Οι χρήστες Laptop δεν θα είναι ευχαριστημένοι γιατί δεν θα λειτουργούν τα power-saving modes.

15.3.2 TermiNET 1.76.13

Το Terminet, από την εταιρία DANU Industries , είναι ένα σχετικά απλό firewall. Από το website της εταιρίας που αναφέρεται στις ικανότητες του προϊόντος τονίζονται οι ακόλουθες ιδιότητες:

- Έλεγχος πρόσβασης - καμία αναρμόδια πρόσβαση από έξω.

- Stealth Mode - καθιστά το PC αόρατο στον εξωτερικό κόσμο.

- Web Blocking - εμποδίζει την πρόσβαση στα ανεπιθύμητα websites

- Υποστηρίζει πολλαπλά προφίλ χρηστών

- Ανακοίνωση κατά την ανίχνευση παρείσφρησης (Blocking notification on Intrusion detection)

- Ευέλικτος έλεγχος κατά την πλοήγηση στο Web (Flexible control for Web Browsing)

- Περιορίζει την πρόσβαση με κριτήρια τις διευθύνσεις IP, URLs, Ports και τα χρησιμοποιούμενα πρωτόκολλα.

- Εύκολο στην χρήση interface ανάλογο των "Windows Explorer"

- Κόστος $49.99

Μοντέλο Ασφαλείας

-Υπάρχουν 3 επίπεδα ασφάλειας: Stealth (προεπιλογή: επιτρέπει εξερχόμενες αλλά εμποδίζει τις εισερχόμενες επικοινωνίες), ανοικτό και κλειστό mode.

-Οι κανόνες μπορούν να δημιουργηθούν ανά χρήστη συστήματος. Ο χρήστης πρέπει να συνδεθεί στο TermiNet με χρησιμοποίηση username και password.

-Μετά την εγκατάσταση ένα password απαιτείται για τον TermiNET administrator, ο οποίος μπορεί να οργανώνει groups, χρήστες και να διαμορφώνει τους κανόνες.

-Τυπικοί κανόνες firewalls μπορούν να προστεθούν βασιζόμενοι στα ακόλουθα: web/IP address, κατεύθυνση (client/server), την εφαρμογή, το πρωτόκολλο, local/remote port/range, και το χρόνο (ημέρα της εβδομάδας).

Αποτεσματικότητα ασφάλειας

Το σύστημα εξετάστηκε στην προεπιλεγμένη "stealth mode"

Α. Ping & shares tests.
Τα εισερχόμενα pings και η πρόσβαση στα τοπικά shares μπλοκάρεται. Τα εξερχόμενα pings και η πρόσβαση σε απομακρυσμένα αρχεία λειτουργούν.

Β. The Netbus server
-Το firewall δεν παραπονέθηκε όταν ο Netbus server ξεκίνησε
-Η εισερχόμενη Netbus σύνδεση μπλοκαρίστηκε, αλλά καμιά συγκεκριμένη προειδοποίηση δεν ανακοινώθηκε

Γ. Σκανάρισμα με το Nmap
Όλα τα ports φιλτράρονται. Η έκδοση του λειτουργικού συστήματος δεν ανιχνεύθηκε. Τα logs γέμισαν με προειδοποιήσεις, μια για κάθε port που υπέστη σκαναρίσμα.

Δ. Άλλα Tests
-Η κυκλοφορία του NetBEUI δεν ανιχνεύθηκε ούτε μπλοκαρίστηκε.
-Δεδομένου ότι οι εξερχόμενες συνδέσεις επιτρέπονται, πληροφορίες θα μπορούσαν εύκολα να διαρρεύσουν από το PC χωρίς τη γνώση του χρήστη. Έτσι εάν μια επίθεση μπορούσε να τοποθετήσει ένα δούρειο ίππο (Trojan) στο PC, ένα reverse tunnel θα μπορούσε ενδεχομένως να χρησιμοποιηθεί για να αναλάβει τον έλεγχο του συστήματος

Πλεονεκτήματα

1. Απλό αλλά αρκετά ισχυρό

2. Εύκολη εγκατάσταση και απεγκατάσταση

3. Έκδοση αξιολόγησης 20 ημερών μπορεί να «κατεβαστεί» για εγκατάσταση και σύγκριση

4. Λειτουργεί στις πιο πολλές εκδόσεις των Windows

5. Είναι σταθερό και αξιόπιστο

6. Κανόνες Firewalls
-Οι κανόνες μπορούν να απενεργοποιηθούν χωρίς να διαγραφούν

-Οι τυπικοί κανόνες είναι πολύ ευέλικτοι π.χ βασισμένοι στον χρόνο πρόσβασης (ημέρα της εβδομάδας) και με επιλογή και των remote και των τοπικών ports.

7. Το log file έχει μεταβλητό μέγεθος που το καθορίζει ο χρήστης ανάλογα με τις ανάγκες του.

8. Σχετικά μικρό μέγεθος (3.4 MB)

Μειονεκτήματα

1.Τεκμηρίωση: η online βοήθεια είναι περιορισμένη

2.Διεπαφή χρήστη (User Interface): Το GUI είναι καλό, αλλά θα μπορούσε να βελτιωθεί.

3.Προστασία

- Οι τυπικοί κανόνες των firewalls δεν επιτρέπουν την εισαγωγή συνολικού κανόνα άρνησης για όλες τις διευθύνσεις IP.

- Η διεύθυνση IP δεν μπορεί να διευκρινιστεί ως πεδίο διευθύνσεων (πχ. 155.107.xxx)

4. Ανίχνευση Διείσδυσης (Intrusion Detection)

-Οι αλλαγές στη διαμόρφωση δεν καταγράφονται στο log, ούτε η ενεργοποίηση/απενεργοποίηση του firewall.

- Κάθε προειδοποίηση προκαλεί την εμφάνιση ενός μεγάλου παράθυρου, αλλά αυτό παρεμποδίζει, είναι κουραστικό και θα απενεργοποιηθεί από τους περισσότερους χρήστες.

-Οι πληροφορίες του παραθύρου προειδοποίησης (alert window) είναι ελάχιστες και δεν εξηγούν σε έναν αρχάριο πόσο σοβαρή είναι η επίθεση, ή ποια αντίμετρα πρέπει να ληφθούν.

-Λεπτομέρειες για τα πακέτα δεδομένων δεν προσφέρονται, μόνο οι διευθύνσεις IP και οι αριθμοί των ports.

- Τα logs δεν μπορούν να εξαχθούν σε HTML ή σε text format.

-Τα σκαναρίσματα δεν ανιχνεύονται, απλά κάθε απαγορευμένη σύνδεση σε port καταγράφεται. Αυτό κάνει πιο δύσκολο να γίνουν κατανοητές οι επιθέσεις που εξελίσσονται. Αναλύσεις επίθεσης υψηλού επιπέδου δεν παρέχονται.

-Τα διερχόμενα καθώς επίσης και τα μπλοκαρισμένα πακέτα καταγράφονται.

5. Ικανότητες αντίδρασης

-Δεν υπάρχει κανένας απλός τρόπος να εμποδιστεί όλη η κυκλοφορία (χωρίς logging) από μια διεύθυνση που ανιχνεύει την ίδια στιγμή το σύστημα

TermiNET 1.76.13	
Κριτήριο	Βαθμολογία
Effectiveness of security protection (Αποτελεσματικότητα της παρεχόμενης προστασίας)	8
Αποτελεσματικότητα στην ανίχνευση παρείσφρυσης (Effectiveness of intrusion detection)	7
Αποτελεσματικότητα αντίδρασης (Effectiveness of reaction)	7
Διεπαφή με τον χρήστη (User interface)	7
Κόστος	4
Μέσος Όρος:	6,6

Σύνοψη

-Διεπαφή χρήστη: για μερικούς Home users, η προεπιλεγμένη διαμόρφωση (default configuration) είναι χρήσιμη και θα λειτουργήσει ικανοποιητικά. Εάν οι κανόνες φίλτρων χρειαστούν αλλαγή, ο χρήστης θα χρειαστεί χρόνο για να καταλάβει το εργαλείο και να το διαμορφώσει σωστά.

-Αποτελεσματικότητα προστασίας: τα εισερχόμενα ports προστατεύονται καλά αλλά τα εξερχόμενα ports επιτρέπονται. Ακόμα είναι δυνατό να είναι το firewall ανοικτό, χωρίς να το αντιληφθεί ο χρήστης.

-Αποτελεσματικότητα της ανίχνευσης παρείσφρησης: οι προειδοποιήσεις και η καταγραφή στο log χρειάζεται βελτίωση

-Αποτελεσματικότητα της αντίδρασης: η ανακάλυψη της ταυτότητας των επιτιθεμένων και το μπλοκάρισμα των επιθέσεων δεν είναι εύκολα. Το TermiNET έχει μερικά ενδιαφέροντα χαρακτηριστικά όπως τα προφίλ πολλών χρηστών.

Εντούτοις, χρειάζονται μερικές βελτιώσεις ενώ και η τιμή του είναι υψηλή σε σχέση με τον ανταγωνισμό.

15.3.3 Tiny Personal Firewall 2.0.13

Απόσπασμα από το website Tiny Personal Firewall:

«Το Tiny Personal Firewall αντιπροσωπεύει τη έξυπνη, εύχρηστη προσωπική τεχνολογία ασφάλειας που προστατεύει πλήρως τους προσωπικούς υπολογιστές από τους hackers. Στηρίζεται στο αποδεδειγμένο WinRoute Pro, ICSA certified security technology. Το Tiny Personal Firewall είναι επίσης ένα αναπόσπαστο τμήμα από το Tiny Software.s new Centrally Managed DesktopSecurity (CMDS) System στο οποίο ανατέθηκε μια σύμβαση από την Πολεμική Αεροπορία των Η.Π.Α. για να καλυφθούν περίπου 500.000 υπολογιστές»

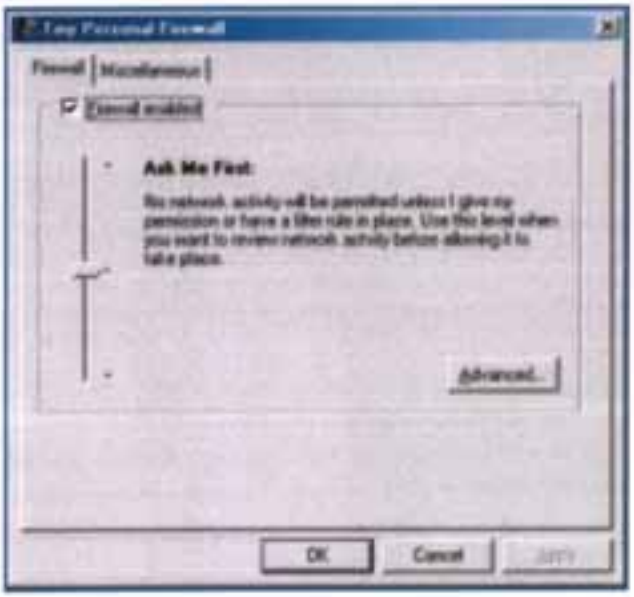
Ανίχνευση παρείσφρησης: Περιλαμβάνει έναν εύχρηστο wizard που ανιχνεύει κάθε άγνωστη δραστηριότητα και προτρέπει το χρήστη να χρησιμοποιήσει τις πληροφορίες εγκατάστασης .

Αφότου ολοκληρωθεί η εγκατάσταση, ένας νέος κανόνας προστίθεται στη λίστα με τους κανόνες των φίλτρων. Αυτή η επιλογή μπορεί να τεθεί εκτός λειτουργίας.

Φίλτρο εφαρμογής: Για την παροχή προστασίας από Trojan horses και άλλες αναρμόδιες εφαρμογές, το firewall περιλαμβάνει ένα φίλτρο εφαρμογών (application filter). Ο wizard θα ανιχνεύσει πότε μια εφαρμογή προσπαθεί να δεσμεύσει ένα port για επικοινωνία και θα δημιουργήσει έναν κανόνα φιλτραρίσματος βασισμένο στο input των χρηστών. Οι χρήστες μπορούν να επιτρέψουν την ενεργοποίηση εφαρμογών με το χέρι ενεργώντας πάνω στους κανόνες φίλτρων. Το firewall παρέχει επίσης μια βάση δεδομένων με τις κοινές εφαρμογές που χρησιμοποιούν τα γνωστά ports.

Τιμή: Δωρεάν για προσωπική χρήση, 39$ για εμπορική

Μέγεθος: 1.3 MB



Χαρακτηριστικά γνωρίσματα:

-Υπάρχουν τρία security modes:

1) Cut me off : απενεργοποίηση της σύνδεσης στο δίκτυο

2) Ask me first : η άγνωστη κυκλοφορία θα προτρέψει το χρήστη να δεχτεί να αρνηθεί η να προσθέσει έναν κατάλληλο κανόνα.

3) Don't bother me: η άγνωστη κυκλοφορία επιτρέπεται

-Η διαμόρφωση και η ανάγνωση του log μπορεί να προστατεύεται με password. Εάν η προστασία με password είναι ενεργοποιημένη, η απομακρυσμένη πρόσβαση (remote access) στην διαμόρφωση (configuration) και/ή στα logs μπορεί να ενεργοποιηθεί.

-Η απομακρυσμένη πρόσβαση στα logs και η διοίκηση από απόσταση (remote administration) μπορεί να ενεργοποιηθεί.

- Λειτουργία εκμάθησης-Learning mode (που μπορεί να απενεργοποιηθεί): ο χρήστης προτρέπεται να δεχτεί/αρνηθεί την νέα κυκλοφορία, ή δημιουργεί έναν κανόνα για να δέχεται/αρνείται την κυκλοφορία.

-Οι διευθύνσεις που εμπιστεύεται ο χρήστης μπορούν να διαμορφωθούν με τρεις τρόπους – single IPs, networks/subnet masks ή πεδία διευθύνσεων (ranges of addresses).

-Οι κανόνες μπορούν να είναι χρονικά ελεγχόμενες . ανά ημέρες της εβδομάδας, με χρονική σειρά ανά ημέρα.

-Οι κανόνες μπορούν προαιρετικά να δημιουργούν καταχωρήσεις σε logs

Αποτελεσματικότητα ασφάλειας

Οι ακόλουθες δοκιμές διενεργήθηκαν σε λειτουργία «high security mode»

-Η εντολή ping από ένα απομακρυσμένο Η/Υ προκάλεσε την ερώτηση στο χρήστη αν το εισερχόμενο ping πρέπει να επιτραπεί ή όχι.

-Ο Netbus server μπορούσε να ξεκινήσει χωρίς να το καταλάβει το firewall, αλλά όταν προσπαθούσε να συνδεθεί στον Netbus, προκαλούσε την εμφάνιση ενός πλαισίου διαλόγου που ζητούσε από το χρήστη να δεχτεί ή να απορρίψει τη σύνδεση.

-Ανίχνευση Nmap: όλες οι συνδέσεις εμποδίστηκαν, το nmap δεν μπορούσε να προσδιορίσει το λειτουργικό σύστημα ή οποιαδήποτε ανοικτά ports. Δεν υπήρχε καμία αναγραφή στο log της προσπάθειας σκαναρίσματος και με τον τρόπο που παρουσιάστηκαν οι προειδοποιήσεις μάλλον ήταν δύσκολο να γίνουν κατανοητές από ένα τυπικό χρήστη.

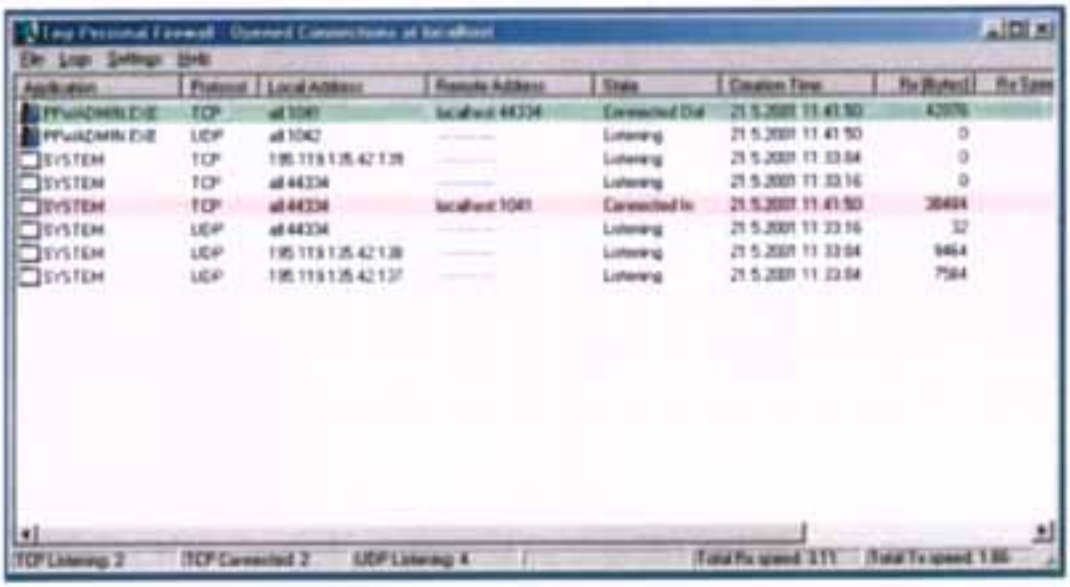
Πλεονεκτήματα

1. Σχετικά μικρό ίχνος (footprint)- (500KB στο σκληρό δίσκο).

2. Καλή σχεδίαση, αρκετά εύκολο να γίνει κατανοητή

3. Δυνατότητα να οργανωθεί με το χέρι ή ως υπηρεσία.

4. Ο Status/Log viewer είναι αρκετά πληροφοριακός, περιλαμβάνει στατιστικές όσον αφορά τα εκπεμπόμενα/λαμβανόμενα bytes ανά εφαρμογή/port και την ταχύτητα.



5. Στο mode εκμάθησης, ο χρήστης εφοδιάζεται με ένα μεγάλο αριθμό πληροφοριών σχετικά με τα νέα αιτήματα σύνδεσης (π.χ., εφαρμογή, ports και διευθύνσεις IP).

6. Ένα εγχειρίδιο χρηστών είναι διαθέσιμο σε μορφή pdf. Εξηγεί τα κύρια χαρακτηριστικά γνωρίσματα και τον τρόπο λειτουργίας του firewall.

Μειονεκτήματα

1. Το πρωτόκολλο FTP δεν γίνεται κατανοητό (αυτόματη διαχείριση των δυναμικών ports).

2. Οι ανιχνεύσεις (scans) παράγουν μεγάλο πλήθος προειδοποιήσεων.

3. Ο χρήστης πρέπει να έχει αρκετή γνώση σε θέματα ασφαλείας και δικτύων.

4. Οι προειδοποιήσεις μπορούν να είναι ενοχλητικές αρχικά, μέχρι να καθοριστούν οι πρώτοι κανόνες.

5. Οι προσαρμογείς δικτύων (network adapters) δεν μπορούν να επιλεχτούν/ αποκλειστούν από το firewall.

6. Εγχειρίδιο χρηστών: Θα μπορούσε να είναι πιο λεπτομερές

Προτεινόμενες βελτιώσεις:
-On-line βοήθεια

Tiny Personal Firewall 2.0.13	
Κριτήριο	Βαθμολογία
Effectiveness of security protection (Αποτελεσματικότητα της παρεχόμενης προστασίας)	8
Αποτελεσματικότητα στην ανίχνευση παρείσφρυσης (Effectiveness of intrusion detection)	8
Αποτελεσματικότητα αντίδρασης (Effectiveness of reaction)	7
Διεπαφή με τον χρήστη (User interface)	8
Κόστος	10
Μέσος Όρος:	8,2

Σύνοψη
Το Tiny Personal Firewall έχει μερικές ιδιορρυθμίες, αλλά είναι ένα χρήσιμο, σταθερό, ισχυρό προσωπικό firewall με μηδενικό κόστος για τους οικιακούς χρήστες. Χρήστες χωρίς εμπειρία θα πρέπει να κατεβάσουν το εγχειρίδιο χρηστών (σε μορφή pdf) για να μπορέσουν να εκμεταλλευτούν πλήρως τις ικανότητες του συγκεκριμένου firewall.

15.3.4 BlackIce Defender 2.1

Χαρακτηριστικά γνωρίσματα

- Το firewall αυτό τοποθετείται στην γραμμή εργασιών και ενημερώνει τον χρήστη για τις εισερχόμενες συνδέσεις δικτύων (πιθανές επιθέσεις).

- Έχει τέσσερα απλά επίπεδα προστασίας από παρανοϊκό-paranoid (δεν επιτρέπει κανένα εισερχόμενο TCP ή UDP port), νευρικό-nervous (επιτρέπει non-standard UDP), προσεκτικό-cautious (επιτρέπει non-standard TCP/UDP), έμπιστο-trusting (χωρίς να μπλοκάρει τίποτα, αλλά προειδοποιώντας όταν νομίζει ότι συμβαίνει κάτι κακό).

- Η κοινή χρήση αρχείων (file sharing) μπορεί να επιτραπεί ή να απενεργοποιηθεί, όπως επίσης και το NetBIOS neighborhood (ο υπολογιστής παραμένει ορατός σε άλλους hosts, από το ίδιο domain, μέσω του Network neighborhood).

- Όταν συμβαίνει μια επίθεση, το εικονίδιο στην γραμμή εργασιών αλλάζει χρώμα (γίνεται κίτρινο, πορτοκαλί ή κόκκινο, ανάλογα με την σοβαρότητα της επίθεσης). Κάνοντας κλικ πάνω στο εικονίδιο, παρουσιάζεται στον χρήστη ένας κατάλογος επιθέσεων. Με δεξί κλικ πάνω σε κάθε γεγονός μπορεί ο χρήστης να επιλέξει τα ακόλουθα:

α)να εμπιστευθεί αυτήν την διεύθυνση
β) να μπλοκάρει αυτή τη διεύθυνση (για κάποια ώρα, ημέρα, μήνα, ή για πάντα)
γ)να αγνοήσει αυτήν την επίθεση
δ)να αγνοήσει το ίδιο είδος επίθεσης από έναν άλλο εισβολέα

- Δεν δίνεται η ικανότητα να καθοριστούν λεπτομερείς κανόνες φίλτρων, αλλά η απλή διαμόρφωση του firewall το καθιστά ιδανικό για να προστατεύσει μη ειδικευμένους χρήστες

- Υπάρχει η δυνατότητα για αυτόματο μπλοκάρισμα όλης της κυκλοφορίας (και όλων των ports) που προέρχεται από μια διεύθυνση IP.

- Μέγεθος: 3MB

- Κόστος: 39$

Αποτελεσματικότητα ασφάλειας

- Netbus server
Το firewall BlackIce δεν παρατήρησε την εκκίνηση του server, αλλά αυτός δεν μπορούσε να συνδεθεί (υπήρξε μια αναφορά ελέγχου TCP port)

-Σκανάρισμα nmap
Το BlackIce ανίχνευσε την λειτουργία του προγράμματος nmap και άναψε ένα κόκκινο εικονίδιο ενώ τα παράθυρα επιθέσεων ανέφεραν: "TCP Port scan", "TCP port probe", "NMAP OS Fingerprint", "TCP Ace ping", "TCP OS Fingerprint" και "UDP Port Probe", μεταξύ πολλών άλλων. Το Nmap επέστρεψε έναν ογκώδη κατάλογο "unfiltered .ports όπως το port 113 και πολλά ports μεταξύ 1024 και 65031. Το Nmap δεν μπόρεσε να προσδιορίσει το OS.

Πλεονεκτήματα

- Μια καλά εφαρμοσμένη ιδέα με GUI που είναι αρκετά απλό και εύχρηστο.

- Σταθερότητα

- Καλή ανίχνευση παρείσφρησης.

- Δεν απαιτεί reboot στην διάρκεια της εγκατάστασης

- Επιτρέπει τη κοινή χρήση αρχείων (file sharing) και τη πρόσβαση στο Network Neighborhood.

- Και τα δυο αυτά χαρακτηριστικά μπορούν να απενεργοποιηθούν εύκολα.

- Το ιστορικό της επίθεσης που παρέχεται είναι χρήσιμο. Το firewall ενημερώνει αμέσως για μια επίθεση, και σημειώνει το host name του επιτιθεμένου και τη διεύθυνση IP.

- Είναι διαθέσιμη έκδοση για εταιρική χρήση όπου είναι δυνατή η κεντρική διαμόρφωση (centralised configuration) και ο καθορισμός διαφορετικών πολιτικών για το firewall και για το είδος των προειδοποιήσεων που παράγονται κάθε φορά.

- Νέες αναβαθμίσεις είναι διαθέσιμες και μπορεί ο καθένας να τις κατεβάσει από το internet. Το σύστημα ενημερώνει αυτόματα το χρήστη εάν η υπάρχουσα έκδοση χρειάζεται αναβάθμιση.

- Αρκετά καλή τεκμηρίωση .

Μειονεκτήματα

- Δεν διατίθεται καμία έκδοση δωρεάν (ούτε demo)

- Θα ήταν καλύτερο εάν δινόταν στους έμπειρους χρήστες η δυνατότητα να μπορούν να προσαρμόσουν περισσότερο τους κανόνες του firewall.

-Η προεπιλεγμένη διαμόρφωση (default configuration) δεν προστατεύει από Trojans

-Το firewall περιμένει έως ότου γίνει μια σύνδεση για να λάβει μέτρα, ενώ δεν αποτρέπει μια σύνδεση κλείνοντας τα ports του συστήματος

-Τα εξερχόμενα ports δεν μπορούν να μπλοκαριστούν

- Παράγει ψεύτικες προειδοποιήσεις όταν χρησιμοποιείται σε τοπικό LAN. Κάτι τέτοιο θα μπορούσε να προκαλέσει πρόβλημα σε ένα εταιρικό intranet.

-Κατά την απεγκατάσταση πολλά στοιχεία παραμένουν στο registry

-Οι αυτόματες αναβαθμίσεις δεν λειτουργούν πάντα

BlackIce Defender 2.1	
Κριτήριο	Βαθμολογία
Effectiveness of security protection (Αποτελεσματικότητα της παρεχόμενης προστασίας)	8
Αποτελεσματικότητα στην ανίχνευση παρείσφρυσης (Effectiveness of intrusion detection)	8
Αποτελεσματικότητα αντίδρασης (Effectiveness of reaction)	7
Διεπαφή με τον χρήστη (User interface)	8
Κόστος	4
Μέσος Όρος:	7

Σύνοψη
Χρήσιμο, εύκολο στην χρήση, διακριτικό. Για τους εταιρικούς χρήστες είναι πολύ χρήσιμη η κεντρική διαχείριση που διαθέτει. Παρόλα αυτά δεν παρέχει την καλύτερη δυνατή ασφάλεια (τα εξερχόμενα ports δεν μπλοκάρονται). Ακόμα οι έμπειροι χρήστες δεν θα μπορέσουν να διαμορφώσουν κανόνες φιλτραρίσματος πακέτων.

15.3.5 ZoneAlarm 2.6

Χαρακτηριστικά
-Τρία γενικά επίπεδα ασφάλειας "low", "medium" και "high" είναι διαθέσιμα, για το internet και τις τοπικές (δηλ έμπιστες) διεπαφές δικτύων.

-Η διεπαφή έμπιστου δικτύου (τοπικό) μπορεί επίσης να επιλεχτεί (χρήσιμο για να προστατεύσει μια dialup σύνδεση, αλλά όχι μια σύνδεση Ethernet). Εντούτοις, εάν χρησιμοποιείται dialup και για το διαδίκτυο και για την πρόσβαση σε intranet, τότε μπορεί να δημιουργήσει προβλήματα.

- Συγκεκριμένοι έμπιστοι hosts μπορούν να προστεθούν, αλλά δεν μπορούν να προστεθούν οι υπηρεσίες που επιθυμεί ο χρήστης.

-Το firewall ανιχνεύει τις δικτυακές εφαρμογές που τρέχουν και παρέχει μια λίστα με αυτές. Κάθε εφαρμογή μπορεί να επιτραπεί να λάβει τις εισερχόμενες συνδέσεις, είτε σε τοπική είτε σε διαδικτυακή σύνδεση (ή και στις δύο). Το ZoneAlarm εξετάζει τα application.s file header και την τοποθεσία του καταλόγου για να προσδιορίσει την εφαρμογή.

-Η διαμόρφωση του GUI επιτρέπει την γρήγορη απαγόρευση όλων των συνδέσεων

-Μετά την εγκατάσταση όταν γίνεται η πρώτη εκκίνηση εμφανίζεται ένα εύκολο σύντομο και κατατοπιστικό tutorial που εξηγεί τα βασικά χαρακτηριστικά του firewall.

- Μέγεθος: 1.5MB.

- Κόστος: Δωρεάν για τη προσωπική χρήση, $19.95 για επιχειρησιακή χρήση.

Αποτελεσματικότητα ασφάλειας

Το τρέξιμο nmap στο ZoneAlarm σε .high security. mode προκαλεί μια προειδοποίηση που δεν δίνει αρκετές πληροφορίες, και το σκανάρισμα είναι σε θέση να προσδιορίσει μερικές υπηρεσίες. Το λειτουργικό σύστημα δεν μπόρεσε να ανιχνευτεί.

Πλεονεκτήματα

1. Διακόπτει όλα τα αχρησιμοποίητα ports.

2. Κόστος: Δωρεάν για προσωπική χρήση.

3. Έχει διαφορετικούς κανόνες για τα τοπικά δίκτυα και για το διαδίκτυο.

4. Σταματά και ζητά την άδεια του χρήστη προτού μια εφαρμογή μπορέσει να χρησιμοποιήσει το δίκτυο, για πρώτη φορά, ή για κάθε φορά.

5. Είναι ευέλικτο.

6. Διαθέτει πλήκτρο για να μπλοκάρει το δίκτυο προσωρινά (που μπορεί να χρησιμοποιηθεί εάν υπάρχει υποψία ύπαρξης Trojan, ή άνοιγμα mail από μια untrusted πηγή. Τα προγράμματα που έχουν διαμορφωθεί ώστε «να περάσουν το κλείδωμα», επιτρέπεται ακόμα να επικοινωνήσουν.

7. Γρήγορο κατέβασμα λόγω του μικρού μεγέθους (1.5 MB).

8. Help icon στο πρόγραμμα με ενδιαφέρουσες πληροφορίες και οδηγίες. Ακόμα υπάρχει δυνατότητα βοήθειας on-line μέσω του site της εταιρίας

9. Υπάρχει δυνατότητα να ελέγχει το firewall για updates αυτόματα.

10. Υπάρχει επιλογή να ελέγχει τα e-mail scripts attachments

Μειονεκτήματα

-Εάν χρησιμοποιούνται πολλές εφαρμογές, οι συνεχείς ερωτήσεις στο χρήστη γίνονται ενοχλητικές, και ο χρήστης μπορεί να καταλήξει να εμπιστευθεί περισσότερες εφαρμογές από όσες πρέπει. Ακόμα δεν αναφέρει τι κάνει ακριβώς κάθε εφαρμογή (ούτε το όνομα της είναι χαρακτηριστικό), και έτσι μια εφαρμογή δεν αναγνωρίζεται αν είναι έμπιστη, ή όχι.

-Εάν χρησιμοποιηθεί μια dialup σύνδεση, μερικές φορές για το intranet και μερικές φορές για internet, το ZoneAlarm θα εφαρμόσει πάντα τους ίδιους κανόνες. Π.χ σε μια intranet dialup, το NetBIOS file sharing είναι επιθυμητό, αλλά δεν είναι στη σύνδεση με το διαδίκτυο.

-Δεν μπορεί να διαμορφωθεί να αγνοήσει τα pings από τις άγνωστες πηγές

-Θα ήταν καλύτερα οι έμπειροι χρήστες να μπορούν να προσαρμόσουν περισσότερο τους κανόνες

-Δεν υπάρχει κανένα φιλικό προς το χρήστη GUI για να παρατηρεί τις επιθέσεις.

-Τα αρχεία (logs) επίθεσης \winnt\Inernet Logs\ZALog.txt δεν είναι αρκετά λεπτομερή. Δίνουν τους αριθμούς ports, αλλά όχι τους λόγους για τους οποίους τα πακέτα εμποδίζονται ούτε κανένα packet header ή περιεχόμενο πακέτων, ούτε οποιεσδήποτε άλλες πληροφορίες.

ZoneAlarm 2.6	
Κριτήριο	Βαθμολογία
Effectiveness of security protection (Αποτελεσματικότητα της παρεχόμενης προστασίας)	8
Αποτελεσματικότητα στην ανίχνευση παρείσφρυσης (Effectiveness of intrusion detection)	8
Αποτελεσματικότητα αντίδρασης (Effectiveness of reaction)	7
Διεπαφή με τον χρήστη (User interface)	9
Κόστος	10
Μέσος Όρος:	8,4

Σύνοψη
Το ZoneAlarm είναι μια ενδιαφέρουσα και αξιόπιστη λύση που διανέμεται δωρεάν. Χρησιμοποιείται από πολλούς χρήστες. Τελευταία ανακοινώθηκε και μια επαγγελματική έκδοση (ή ZoneAlarm Pro)με επιπρόσθετα χαρακτηριστικά ασφάλειας και κόστος $39.95. Σε αυτά περιλαμβάνονται προστασία από την αποστολή e-mail, από Visual Basic Script worms,όπως ο ιός .I love you., χρησιμοποίηση κωδικού πρόσβασης κτλ.

15.3.6 Sygate Personal Firewall v4

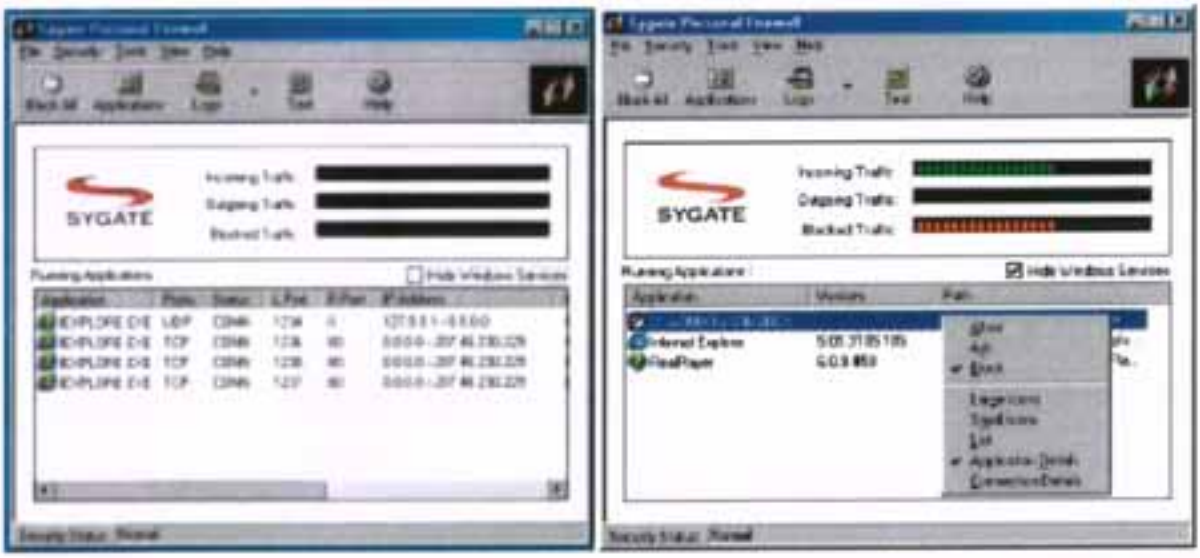
Σύμφωνα με το website του Sygate Personal Firewall:
«Το Firewall Sygate προστατεύει βασισμένους στα windows προσωπικούς υπολογιστές και servers με πέντε εξειδικευμένες ρυθμίσεις επιπέδου-προστασίας που παρέχουν πολλαπλά στρώματα ασφάλειας στον συνδεδεμένο υπολογιστή. Το firewall Sygate επιτρέπει ή αρνείται κάθε εισερχόμενο ή εξερχόμενο πακέτο διαδικτύου βασισμένο στις ρυθμίσεις ασφάλειας (ports, πρωτόκολλα, διεύθυνση IP, ώρα της μέρας, εφαρμογή).

Μπορεί επίσης να συνδέσει προνόμια πρόσβασης στο διαδίκτυο με ειδικές εφαρμογές και να επιτρέψει ή να εμποδίσει εφαρμογές από την πρόσβαση στο Διαδικτύο.»

Χαρακτηριστικά γνωρίσματα

Το firewall Sygate κοστίζει $39,95. Είναι ελεύθερο για τη προσωπική χρήση. Μέγεθος: 3.47MB

-Υποστηρίζει windows 95/98/ME και NT4 ή 2000.



-Έχει interactive τρόπο εκμάθησης: Ειδοποιεί το χρήστη εάν οποιεσδήποτε αναρμόδιες εφαρμογές προσπαθούν να αποκτήσουν πρόσβαση στο Διαδίκτυο.

-Η εγκατάσταση είναι εύκολη.

-Ανακοίνωση προειδοποιήσεων μέσω ηλεκτρονικού ταχυδρομείου.

-«Έμπιστες» διευθύνσεις μπορούν να προστεθούν ανά εφαρμογή.

-Εφαρμογές: οι εφαρμογές που προσπαθούν να αποκτήσουν πρόσβαση στο δίκτυο προστίθενται στον «έμπιστο» κατάλογο ή στον «μπλοκαρισμένο», ανάλογα με την απάντηση που δίνει ο χρήστης όταν ερωτάται.

-Σχέδιο ασφάλειας: όλη η κυκλοφορία από το διαδίκτο μπορεί να προκαθοριστεί σε προκαθορισμένους χρόνους (π.χ. τη νύχτα) ή όταν ο screen saver είναι ενεργοποιημένος

-Η διαμόρφωση (configuration) μπορεί να προστατευτεί με password.

-Κεντρική διαχείριση: Το επιχειρηματικό πακέτο του προγράμματος Sygate (Sygate Enterprise Network) επιτρέπει τη κεντρική (remote) διαχείριση. Από τον διαχειριστή μπορούν να καθοριστούν .οι παροχές. (ανάλογα με την πολιτική που ακολουθείται), για κάθε χρήστη firewall ή για ομάδες χρηστών. Αυτές οι πολιτικές μπορούν εύκολα να εφαρμοστούν στους πελάτες.

-Άλλες δοκιμές:

- Διαρρέουσα εξερχόμενη πληροφορία πάνω από standard ports: όλα τα πρωτόκολλα θα παραμείνουν μπλοκαρισμένα μέχρι ο χρήστης να εγκρίνει να χρησιμοποιήσουν οι εφαρμογές τα ports.

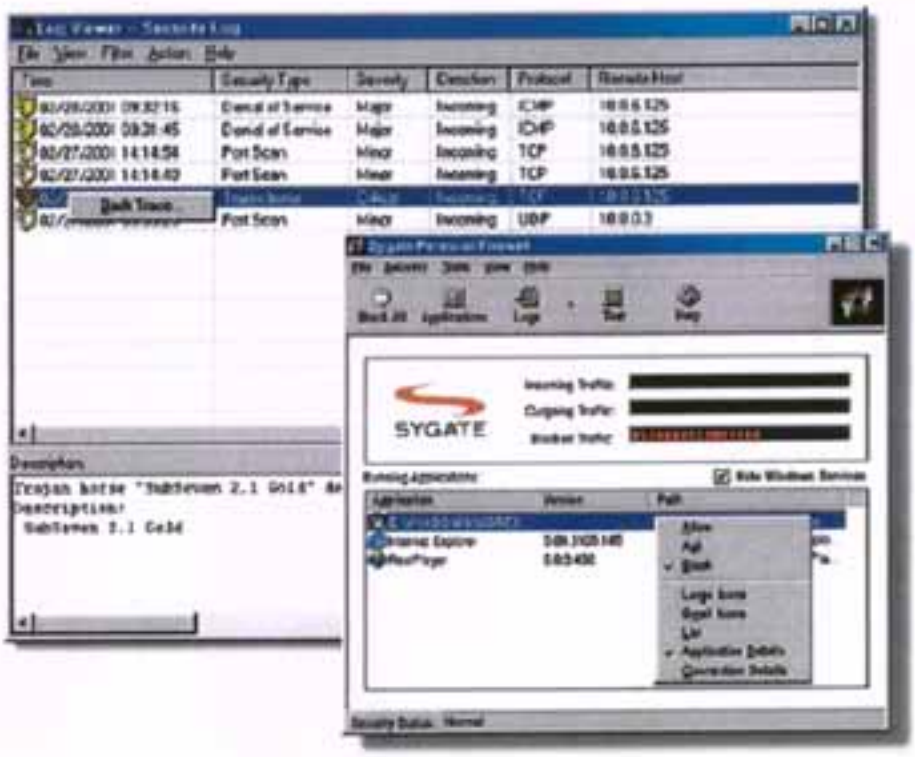
-Μεταμφίεση ως «έμπιστο» ή standard πρόγραμμα: η αντικατάσταση ενός εμπιστευτικού προγράμματος από Trojan ανιχνεύθηκε από το Sygate, ακόμη και με το ίδιο ακριβώς όνομα και path.

-Απόκτηση της πρόσβασης κατά τη διάρκεια της σύνδεσης: η κυκλοφορία της άγνωστης εφαρμογής εμποδίζεται κατά τη διάρκεια της σύνδεσης.

Αποτελεσματικότητα ασφάλειας

-Τα εξερχόμενα ping και η πρόσβαση σε αρχεία επιτράπηκαν, ενώ τα εισερχόμενα μπλοκαρίστηκαν.

-Ο Netbus Server δεν μπορούσε να ξεκινήσει χωρίς μια προειδοποίηση, εντούτοις όταν έγινε μια προσπάθεια να συνδεθεί με τον Netbus Server (για να εξομοιωθεί ένας επιτιθέμενος που παίρνει τον έλεγχο), το Sygate προέτρεψε το χρήστη να δεχτεί ή να αρνηθεί τη σύνδεση, αναφέροντας το path της εκτελέσιμης εφαρμογής, το port και τη IP διεύθυνση πηγής. Ένα παράθυρο .λεπτομερειών. επιτρέπει ακόμη και την εξέταση των λεπτομερειών των IP πακέτων. Ο χρήστης πρέπει να αποφασίσει εάν ο Netbus Server επιτρέπεται να συνδεθεί με το δίκτυο (ναι ή όχι) και μπορεί προαιρετικά "να θυμηθεί την απάντηση., οπότε σ'αυτή την περίπτωση ένας κατάλληλος μόνιμος firewall κανόνας δημιουργείται.



Η διαδικασία είναι αρκετά καλή, και θα ήταν πιο χρήσιμη εάν το Sygate αναγνώριζε τα πραγματικά trojans και τα προγράμματα τηλεχειρισμού τους, όπως το Netbus, και προειδοποιούσε το χρήστη για τους κινδύνους τέτοιων προγραμμάτων. Ο άπειρος χρήστης μπορεί να μπει στον πειρασμό να πει "ναι. εάν δεν καταλάβει το προειδοποιητικό μήνυμα. Οι επόμενες προσπάθειες σύνδεσης με Netbus μπλοκαρίστηκαν, παρόλο που δεν επιλέχθηκε το Sygate να θυμηθεί το "No..

Αυτό σημαίνει ότι Sygate αρνείται την πρόσβαση για την τρέχουσα login session, πράγμα που μπορεί να είναι χρήσιμο.

-Ένα σκανάρισμα με το nmap δεν προσδιόρισε κανένα ανοικτό port και δεν ήταν ικανό να ανιχνεύσει το λειτουργικό σύστημα. Όταν υπάρχει σκανάρισμα για ανοιχτά ports το firewall καταγράφει τις προσπάθειες σύνδεσης σε μη ενεργά ports και ταυτόχρονα ανάβει κόκκινο το εικονίδιο του. Όταν το nmap προσπαθεί να συνδεθεί σε ενεργά ports, αναδύεται το standard μήνυμα συναγερμού. Παρόλα αυτά δεν υπάρχει τρόπος ο χρήστης να μπλοκάρει όλα τα πακέτα από τον επιτιθέμενο, και μια προειδοποίηση θα ενεργοποιηθεί για κάθε ενεργό port.

Πλεονεκτήματα

-Πολύ ισχυρό

-Χρήσιμο και για τον αρχάριο και τον έμπειρο και τον εταιρικό χρήστη

-Περιεκτική αναγραφή στο log: ασφάλεια, σύστημα, κυκλοφορία, packet logs.

-Σχέδιο ασφάλειας: Όλη η κυκλοφορία διαδικτύου μπορεί να εμποδιστεί σε ορισμένους χρόνους (π.χ. τη νύχτα) ή όταν είναι ενεργοποιημένος ο screen saver.

-Το παράθυρο, των εφαρμογών που τρέχουν, παρουσιάζει ποιες εφαρμογές χρησιμοποιούν ποια ports για να επικοινωνήσουν με τα τοπικά ή μακρινά συστήματα.

-Σχετικά μικρό μέγεθος.

-Εύκολη εγκατάσταση.

-Από το παράθυρο των logs υπάρχει επιλογή για να ανιχνευτούν πηγές επιθέσεων.

Μειονεκτήματα

- Καταγραφή (logging): οι αλλαγές διαμόρφωσης δεν σημειώνονται στο system log.

- GUI: το μέγεθος του κύριου παράθυρου δεν μπορεί να μεταβληθεί.

- Προστασία
Οι «έμπιστες» διευθύνσεις δεν μπορούν να διαμορφωθούν για όλες τις εφαρμογές, πρέπει να γίνει ξεχωριστά για κάθε εφαρμογή.

- Μηνύματα προειδοποίησης:
Έπρεπε να προσφέρονται επιλογές είτε να μπλοκαριστεί όλη η κυκλοφορία από αυτήν ίδια διεύθυνση, είτε να «εμπιστευθεί» όλη η κυκλοφορία από την ίδια διεύθυνση. Κατά τη διάρκεια μιας επίθεσης, το εικονίδιο του firewall ανάβει κόκκινο. Θα ήταν χρήσιμο εάν το μήνυμα που επιδεικνύεται όταν το ποντίκι αιωρείται πάνω από το εικονίδιο να άλλαζε και αντί να δίνει πληροφορίες για το όνομα του firewall να έδινε πληροφορίες για την προειδοποίηση που σημειώθηκε .

Κατά τη διάρκεια μιας επίθεσης, εάν ο χρήστης πιέσει δύο φορές το εικονίδιο του firewall η οθόνη διαμόρφωσης του firewall παρουσιάζεται, αλλά χωρίς να δίνει τον τρόπο στο χρήστη για να εμποδίσει τον επιτιθέμενο ή να πάρει περισσότερες λεπτομέρειες. Πρέπει να πάει στο log για να μάθει τι συμβαίνει.

Το παράθυρο των log ασφάλειας είναι αρκετά καλό, επιτρέπει να εκτελεστεί ένα traceroute και ένα .who is. στις πηγές επίθεσης. Εντούτοις, θα ήταν επίσης χρήσιμο να υπάρχει επιλογή να μπλοκαριστούν όλα τα πακέτα από αυτή την πηγή. Τα ίδια και για τα log κυκλοφορίας Sygate v4

Sygate v4	
Κριτήριο	Βαθμολογία
Effectiveness of security protection (Αποτελεσματικότητα της παρεχόμενης προστασίας)	9
Αποτελεσματικότητα στην ανίχνευση παρείσφρυσης (Effectiveness of intrusion detection)	10
Αποτελεσματικότητα αντίδρασης (Effectiveness of reaction)	9
Διεπαφή με τον χρήστη (User interface)	9
Κόστος	10
Μέσος Όρος:	9,4

Σύνοψη

Η έκδοση 4 του Sygate Firewall αποτελεί μια πολύ καλή λύση. Από πάρα πολλούς χρήστες θεωρείται κορυφαία επιλογή.

15.3.7 Συμπερασματικός Πίνακας

Κριτήριο	McAfee 2.1.3	TerminNET	Tiny 2.0.13	Blacklce	ZoneAlarm	Sygate v4
	Βαθμολογία					
Effectiveness of security protection (Αποτελεσματικότητα της παρεχόμενης προστασίας)	6	8	8	8	8	9
Αποτελεσματικότητα στην ανίχνευση παρείσφρυσης (Effectiveness of intrusion detection)	6	7	8	8	8	10
Αποτελεσματικότητα αντίδρασης (Effectiveness of reaction)	7	7	7	7	7	9
Διεπαφή με τον χρήστη (User interface)	6	7	8	8	9	9
Κόστος	5	4	10	4	10	10
Μέσος Όρος:	6	6,6	8,2	7	8,4	9,4

16. Παράδειγμα - Zone Alarm Security Suite

16.1 Οδηγίες εγκατάστασης

Το Zone Alarm Security Suite έρχεται πρώτο σε προτιμήσεις από τα κλασικά firewalls που συνοδεύονται από τα γνωστά προγράμματα antivirus. Το Zone Alarm Security Suite παρέχει ασφάλεια και προστασία από hackers, spammers, dialers, gators και πολλά άλλα, για όση ώρα βρίσκεστε συνδεδεμένοι στο Internet. Επίσης σταματά την εμφάνιση των pop-ups και δίνει πολλές επιλογές και ρυθμίσεις για την καλύτερη απόδοσή του.

Ας δούμε με μια πρώτη ματιά πως μπορείτε να εκμεταλλευτείτε όλες τις λειτουργίες του Zone Alarm Security Suite. Είναι πολύ εύκολο στην εγκατάστασή του. Χρειάζεται μόνο να του δώσουμε κάποιες πληροφορίες σχετικά με τον υπολογιστή μας, και μόνο του κάνει τις υπόλοιπες ρυθμίσεις. Προσοχή μόνο σε περίπτωση που έχετε δίκτυο υπολογιστών θα πρέπει να το δηλώσετε στην αρχική εγκατάσταση του ZA για να αναγνωρίσει και τους άλλους Η/Υ , αλλιώς δεν θα επιτρέπει τη λειτουργία δικτύου.

ToZA αναλαμβάνει να ελέγχει για ενδεχόμενες αναβαθμίσεις στο Internet, και μας ενημερώνει γι΄ αυτό.

Χωρίζεται σε κατηγορίες και φακέλους όπου μπορείτε να κάνετε διαφορετικές ειδικές ρυθμίσεις. Στην βασική toolbar της επιφάνειας εργασίας του προγράμματος, κάτω δεξιά, θα βρείτε ένα εικονίδιο που θα σας ενημερώνει για κάθε "ύποπτη" κίνηση που συμβαίνει στον υπολογιστή σας.

Αφού κάνετε την εγκατάσταση, επιλέξτε να φορτώνει το πρόγραμμα κατά το Start Up των Windows ούτως ώστε να το έχετε έτοιμο όταν μπείτε στο Internet, γιατί συχνά θα ξεχνάτε να το ανοίγετε μόνοι σας.

Αφού συνδεθείτε στο Internet, κάτω δεξιά (στην Task Bar) το σύμβολο του Zone Alarm Security Suite θα μετατραπεί σε δύο μπάρες. Η κόκκινη δείχνει τις πληροφορίες που φεύγουν από τον υπολογιστή σας, ενώ η πράσινη δείχνει τις πληροφορίες που δέχεται ο υπολογιστής. Το φυσιολογικό είναι η πράσινη μπάρα να είναι πιο ενεργή, εκτός και αν στέλνετε E-Mail ή κάποιο αρχείο. Στην (ανησυχητική) περίπτωση που δείτε την κόκκινη μπάρα να είναι γεμάτη (δηλαδή σε πλήρη λειτουργία) ενώ δεν στέλνετε αρχεία, τότε κάτι δεν πάει καλά! Τότε θα πρέπει είτε να βγείτε από το Internet (Disconnect), είτε να κάνετε double click στο σύμβολο του Zone Alarm Security Suite στην Task Bar και να πατήσετε το μεγάλο κουμπί που δείχνει την κλειδαριά (και έτσι δεν θα δέχεται καμία πληροφορία ο υπολογιστής σας).

Την πρώτη φορά που θα χρησιμοποιήσετε το Zone Alarm Security Suite και θα αρχίσετε

να φορτώνετε προγράμματα σχετικά με το Internet (Internet Explorer, Outlook, ICQ, Getright κ.τ.λ.) θα εμφανίζετε ένα μήνυμα στην οθόνη το οποίο θα σας ενημερώνει ότι «το αντίστοιχο πρόγραμμα προσπαθεί να συνδεθεί στο Internet, να του δώσω την άδεια ή όχι;», ενώ επίσης υπάρχει ένα κουτάκι το οποίο, αν το επιλέξετε, το Zone Alarm Security Suite θα θυμάται την επιλογή, και δεν θα σας ζητήσει ξανά επιβεβαίωση για την λειτουργία του συγκεκριμένου προγράμματος, (για παράδειγμα αν το επιλέξετε και πατήσετε (Allow), τότε θα μπορείτε να μπαίνετε σε αυτό ανενόχλητα, ενώ αν πατήσετε (Deny) τότε κάθε φορά που φορτώνετε το πρόγραμμα το Zone Alarm Security Suite θα του "κόβει" την πρόσβαση στο Internet).

Με αυτό τον τρόπο εσείς επιλέγετε ποια προγράμματα μπορούν να συνδέονται στο Internet, ποια προγράμματα να λειτουργήσουν ως Servers και τα λοιπά. Για παράδειγμα, εάν ανοίξετε ένα File Sharing Utility, μετά την εγκατάσταση του Zone Alarm Security Suite θα εμφανιστούν δυο παραθυράκια το ένα από τα οποία θα σας ρωτάει εάν του επιτρέπετε να συνδεθεί με το Internet και το επόμενο εάν το αφήνετε να κάνει Server τον υπολογιστή σας (δηλαδή να μπορεί να στέλνει αρχεία). Τον πίνακα με τα προγράμματα στα οποία έχετε δώσει πρόσβαση στο Internet ή την δυνατότητα να λειτουργούν ως Servers, μπορείτε να τα δείτε στο μενού Programs του Zone Alarm Security Suite. Δίπλα στο όνομα του κάθε προγράμματος υπάρχουν τρεις στήλες.

Η πρώτη λέγεται Allow Connect και αναφέρεται στο αν επιτρέπεται στο πρόγραμμα να συνδέεται στο δίκτυο (είτε Local είτε Internet) για downloading, η δεύτερη στήλη ονομάζεται Allow Server, δηλαδή αναφέρεται στο uploading, και έχει πάλι δύο επιλογές, είτε Local είτε Internet.

Η τρίτη και τελευταία στήλη λέγεται Pass Lock και αναφέρεται στην περίπτωση που "κλειδωθεί» το μηχάνημα σας από το Zone Alarm Security Suite οπότε επιλέγετε ποια προγράμματα θα συνεχίζουν να δουλεύουν ανενόχλητα. Μέσω αυτού του μενού μπορείτε να ρυθμίσετε τις προσβάσεις των προγραμμάτων σας. Για παράδειγμα στα γνωστά προγράμματα θα επιτρέπετε «Allow Connect» στο Internet, αλλά όχι «Allow Server» εκτός και αν είναι κανένα πρόγραμμα ανταλλαγής αρχείων, όπως το Napster, οπότε πρέπει ο υπολογιστής σας να γίνει Server.

Σημαντική είναι και η επιλογή Security του προγράμματος από όπου μπορείτε να επιλέξετε το επίπεδο προστασίας που θα σας παρέχει το Zone Alarm Security Suite. Το συνιστώμενο είναι το High Security, οπότε από την στιγμή που θα μπείτε στο Internet τα πάντα λογοδοτούν στο Zone Alarm Security Suite και συν τοις άλλοις κρύβει και όλα τα Ports σας που δεν χρησιμοποιούνται (τα Ports είναι σημαντική παράμετρος για την ασφάλεια, απλά να γνωρίζετε ότι από τα "ανοιχτά" Ports θα προσπαθήσει κάποιος hacker να μπει στο μηχάνημά σας). Όσοι τώρα είστε πιο σίγουροι μπορείτε να βάλετε Medium επίπεδο στην Security, αλλά ο υπολογιστής μένει ορατός σε Port Scans του Internet και γενικά το πρόγραμμα συμπεριφέρεται πιο χαλαρά σε θέματα ασφαλείας. Φυσικά υπάρχει και το Low επίπεδο, αλλά δεν συνιστάτε.

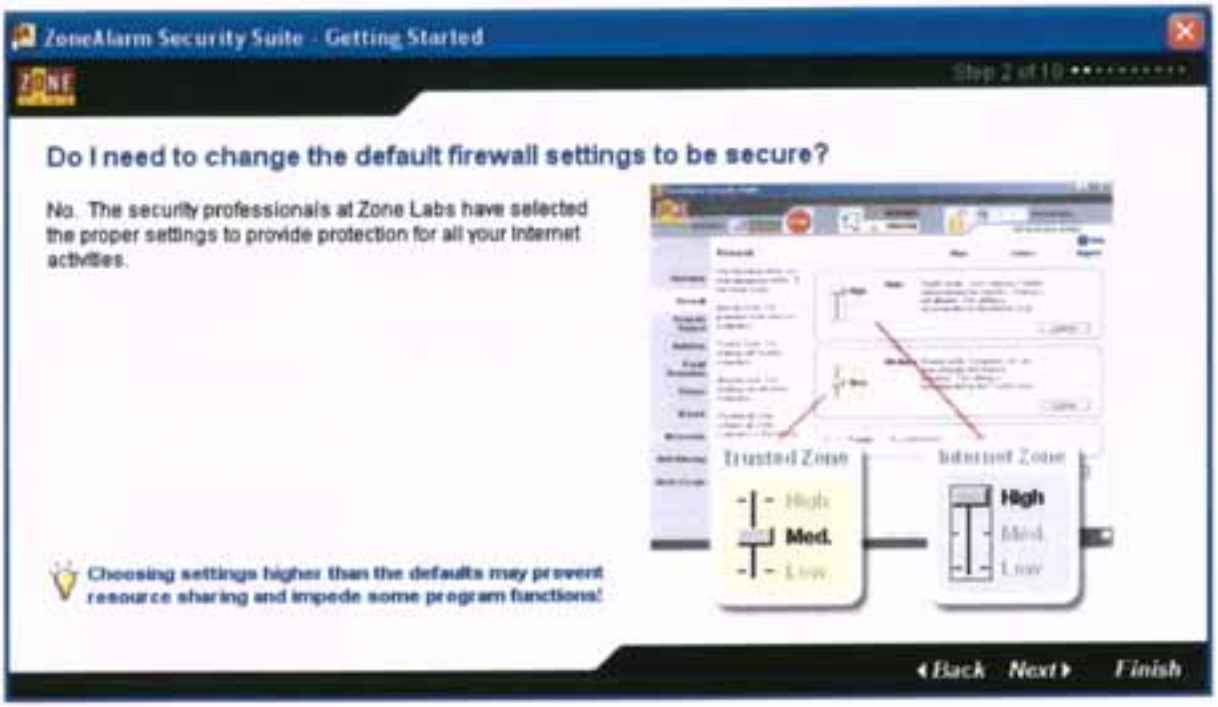
Τελευταία σημαντική επιλογή που πρέπει να γνωρίζετε είναι τα Alerts, από όπου βλέπετε τις προσπάθειες που έγιναν από άγνωστους χρήστες ή Sites, να πάρουν ή να

στείλουν δεδομένα από και προς τον υπολογιστή σας και τις οποίες το Zone Alarm Security Suite τις μπλόκαρε. Επιλέγοντας το Show the alert popup window, κάθε φορά που γίνεται μια τέτοια προσπάθεια θα ανοίγει και ένα παράθυρο για να σας ενημερώνει. Τα Alerts καταγράφονται σε ένα Log, σε Text μορφή, και μπορείτε να δείτε όλα μαζί όποτε θέλετε με αναλυτικές πληροφορίες από το κάθε Hit (IP, ώρα που έγινε η προσπάθεια κ.λ.π). Δεν μπορείτε να διανοηθείτε πόσες Alerts θα έχετε, ιδίως εάν είναι η πρώτη φορά που βάλατε Firewall

Από το μενού του προγράμματος, μπορείτε να ορίσετε την εμπλοκή των pop-ups που ανοίγουν σε διάφορα sites που επισκέπτεστε και την άμεση διαγραφή των cookies. Από τον κατάλογο privacy και τον φάκελο main μπορείτε να κάνετε τις προσωπικές ρυθμίσεις που θέλετε και από τον φάκελο site list μπορείτε να ορίσετε τα sites που θεωρείτε ασφαλή, ή να διαγράψετε κάποιο που είχατε ορίσει ελεύθερη είσοδο.
Πέρα από τις αρκετές ρυθμίσεις που θα βρείτε στο πρόγραμμα, υπάρχει και ο κατάλογος του e-mail protection. Ο συγκεκριμένος κατάλογος παρέχει προστασία στο mail account σας και στον κατάλογο alerts and logs που αναφέρονται όλα τα τελευταία συμβάντα και οι επιθέσεις που γίνονται στο σύστημά σας.

16.2 Συμπεριφορά

Μια ματιά τώρα στα βήματα ενημέρωσης του Zone Alarm Security Suite, για να γνωρίσουμε πως συμπεριφέρεται και τι ακριβώς κάνει για εμάς



Δεν είναι απαραίτητο να αλλάξετε τις προτεινόμενες ρυθμίσεις. Το Zone Alarm επιλέγει τις καλύτερες ρυθμίσεις προστασίας αυτόματα, ώστε να λειτουργούν χωρίς πρόβλημα όλες οι εργασίες που θέλετε στο Internet, με την καλύτερη δυνατή προστασία.

Το Zone Alarm Security Suite προστατεύει σε 5 διαφορετικά επίπεδα.

1) **Antivirus Protection**: Ανακαλύπτει και αποκλείει την επίθεση Virus στον υπολογιστή σας και στα e-mail σας, πριν προκαλέσουν ζημιά.

2) **Fire wall Protection**: Επιτηρεί τις πόρτες του υπολογιστή σας και κρατά έξω τους επίδοξους Hackers. Με την επιλογή απόκρυψης, κάνει τον υπολογιστή σας αόρατο στο Internet.

3) **Program Control**: Ελέγχει ποιο πρόγραμμα θα έχει πρόσβαση στο Internet και σταματά τα προγράμματα Spyware, Trojians και Malware να επικοινωνήσουν με τους κατασκευαστές τους.

4) **Identity Protection**: Προστατεύει τις προσωπικές πληροφορίες που είναι αποθηκευμένες στον Υπολογιστή σας, να μεταφερθούν χωρίς την άδειά σας, σε μη έμπιστα Sites.

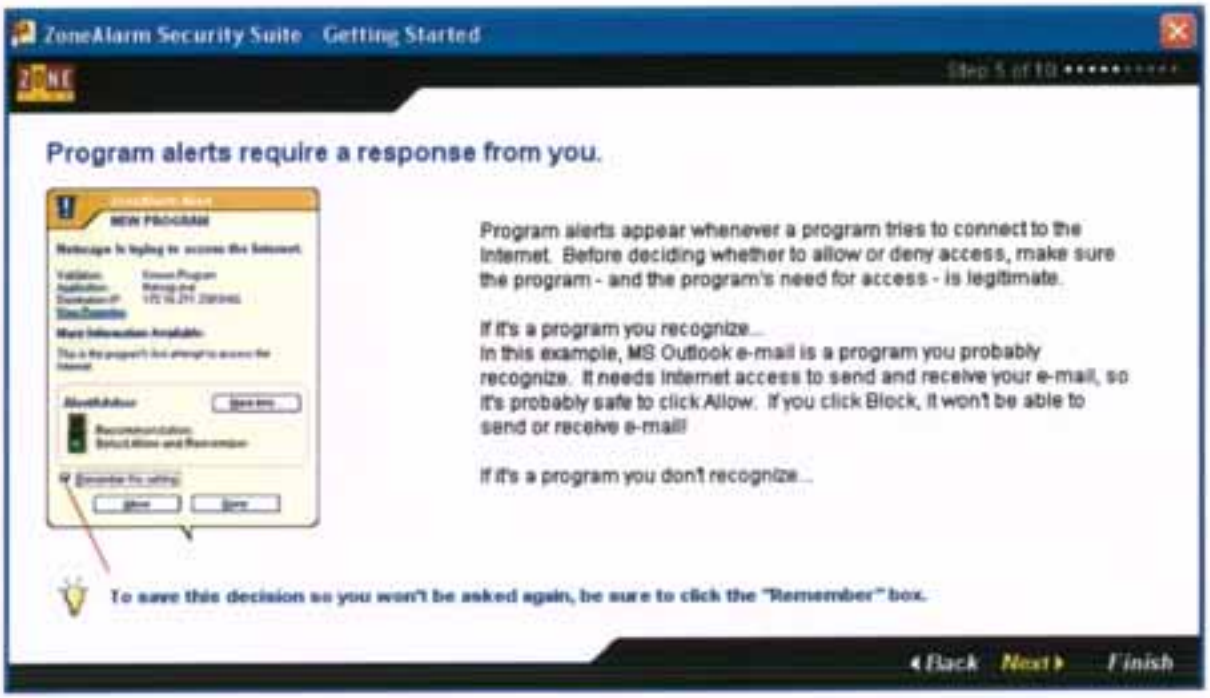
5) **IM Security**: Κρυπτογραφεί τα μηνύματα σας, ενώ εμποδίζει παράλληλα τους Hackers, τα Virus, και άλλες επικίνδυνες παραπομπές και συνδέσμους, που προσπαθούν να αποκτήσουν πρόσβαση μέσα από τις πόρτες επικοινωνίας του υπολογιστή σας.

Με το Zone Alarm Security Suite γνωρίζετε κάθε στιγμή ότι ο υπολογιστής σας είναι προστατευμένος. Ένα από τα πρώτα πράγματα που θα δείτε, όταν λειτουργεί το Zone Alarm Security Suite είναι κάποια αναδυόμενα μηνύματα προειδοποίησης. Όταν δεν εμφανίζονται σημαίνει ότι ο υπολογιστής είναι προστατευμένος. Υπάρχουν δυο βασικοί τύποι προειδοποίησης:

1) Προειδοποίηση Προγραμμάτων

2) Προειδοποίηση του Τοίχου Προστασίας

Στα επόμενα βήματα θα δούμε πως θα ανταποκριθούμε σε κάθε ένα τύπο προειδοποίησης.

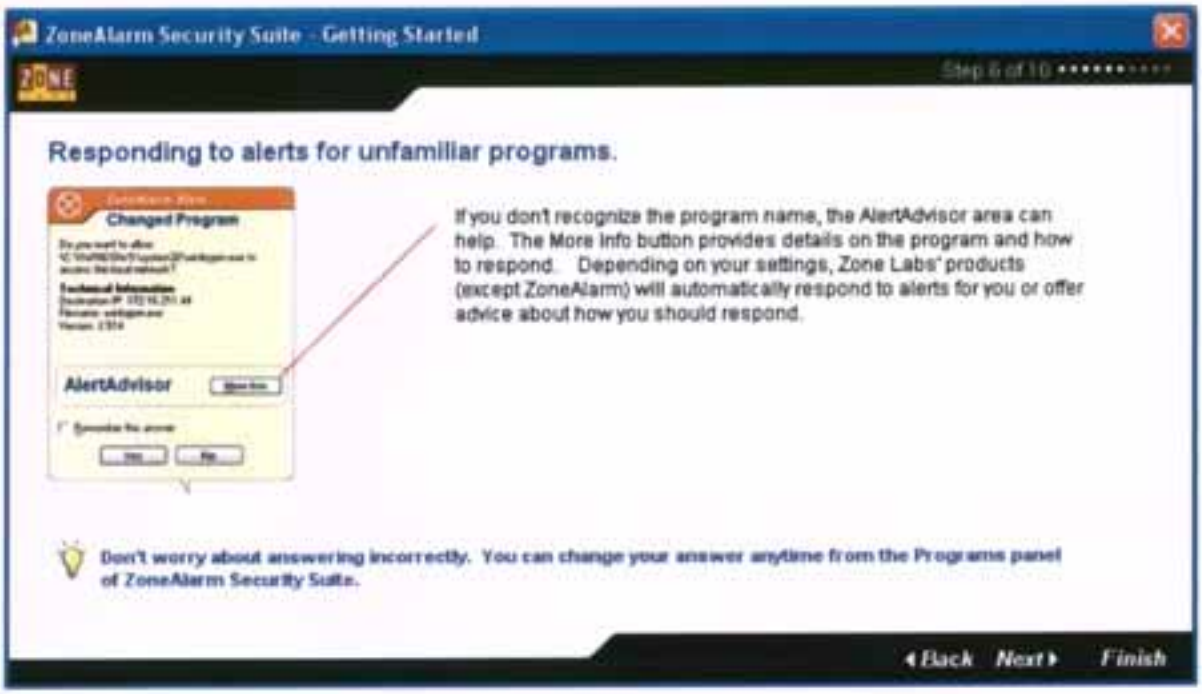


Η προειδοποίηση Προγράμματος εμφανίζεται, όταν ένα πρόγραμμα προσπαθεί να συνδεθεί στο Internet. Πριν αποφασίσετε εάν θα του επιτρέψετε (Allow) ή θα του απαγορεύσετε (Deny) να συνδεθεί, πρέπει να είστε σίγουροι ότι είναι απαραίτητο να συνδεθεί, για κάποιο σοβαρό λόγο.

Αν είναι πρόγραμμα που το γνωρίζετε, για παράδειγμα , Microsoft Outlook, πρέπει να του επιτρέψουμε την σύνδεση (Allow) αλλιώς δεν θα μπορείτε να στείλετε ή να λάβετε e-mail.

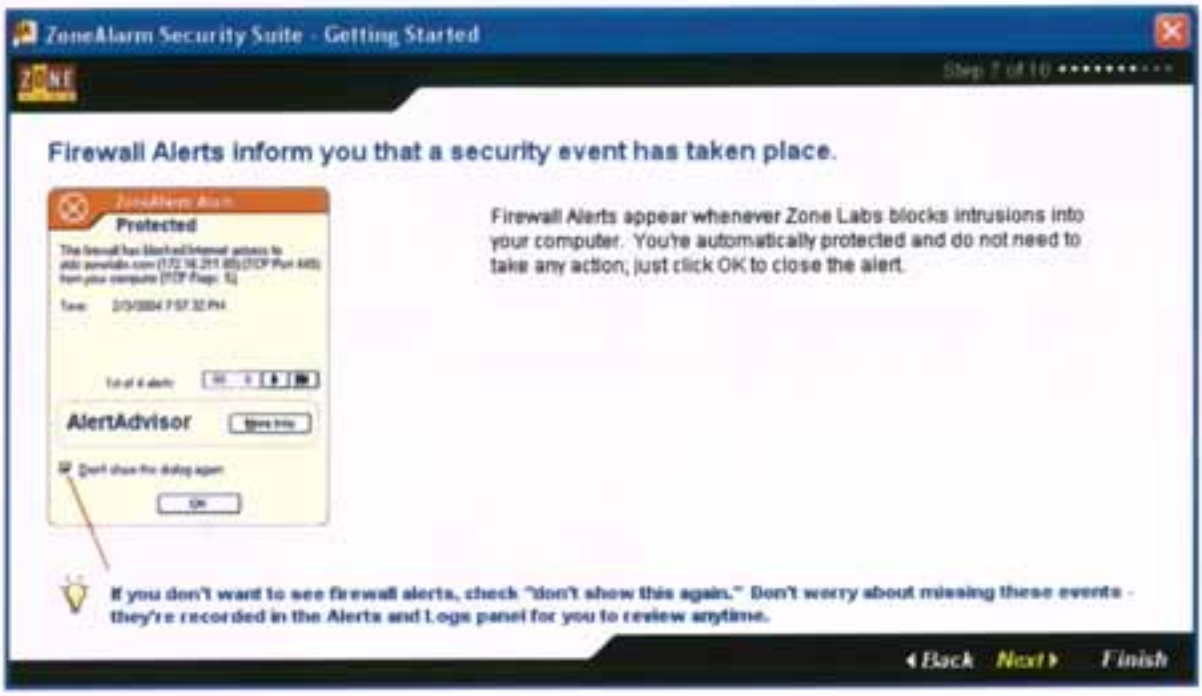
Σ΄ αυτήν την περίπτωση, στο λευκό τετραγωνάκι που είναι στο κάτω αριστερό μέρος, βάζουμε το βελάκι από το ποντίκι και πατάμε το αριστερό πλήκτρο μια φορά, ώστε να το τσεκάρουμε και να μη μας ρωτήσει άλλη φορά το Zone Alarm Security Suite, γ΄ αυτό το πρόγραμμα.

Το ίδιο θα κάνουμε και για άλλα προγράμματα που γνωρίζουμε, όπως ο Internet explorer, ή κάποιο από τα προγράμματα, που εμείς έχουμε εγκαταστήσει στον Υπολογιστή μας.



Επίσης υπάρχει και η δυνατότητα να ενημερωθούμε και μέσα από την σελίδα του Zone Alarm Security Suite, στο Internet, για προγράμματα που δεν αναγνωρίζουμε, και μας ζητούν σύνδεση.

Πάντως, εάν δώσουμε λάθος απάντηση, στην ερώτηση του Zone Alarm Security Suite, για Allow – Deny, δεν είναι και τίποτα τρομερό. Μπορούμε ανά πάσα στιγμή, μέσα από το μενού του Zone Alarm Security Suite, να αλλάξουμε την απάντηση.

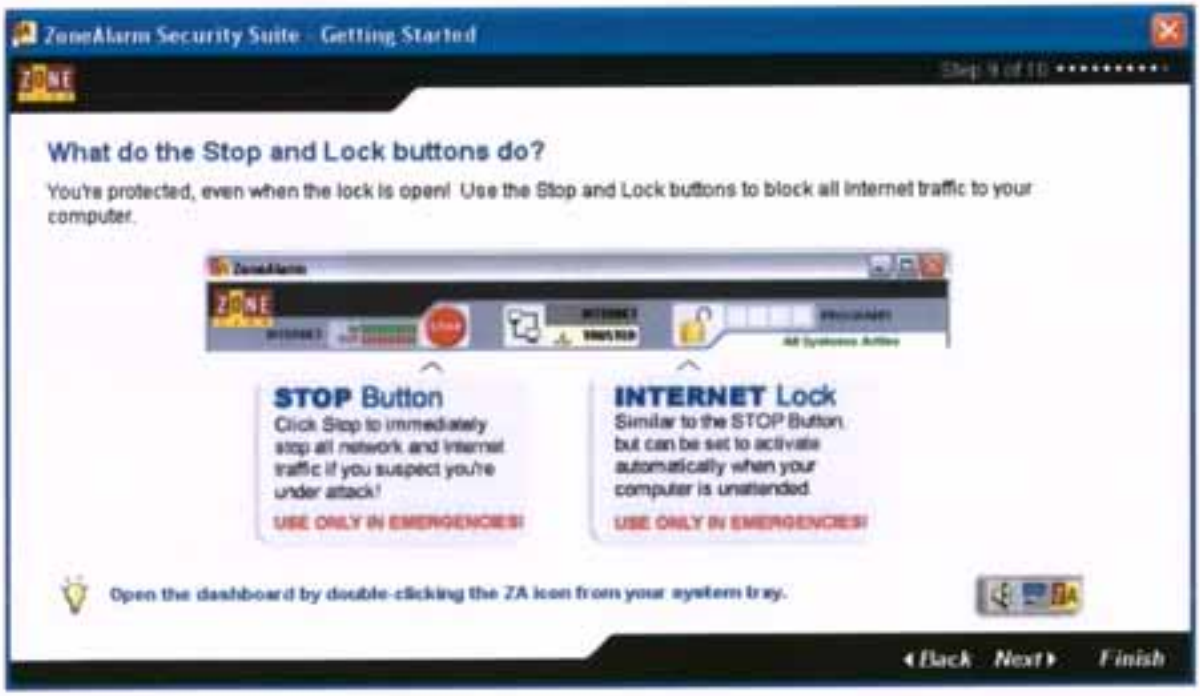


Η προειδοποίηση του Τοίχου προστασίας, εμφανίζετε όταν το Zone Alarm Security Suite μπλοκάρει και κόβει κάποια επίθεση στον υπολογιστή σας. Είστε αυτόματα προστατευμένοι από τέτοιου είδους επιθέσεις, και δεν είναι απαραίτητο να κάνετε καμία ενέργεια, απλά κάντε κλίκ στο OK για να κλείσει το μήνυμα του τοίχου προστασίας.

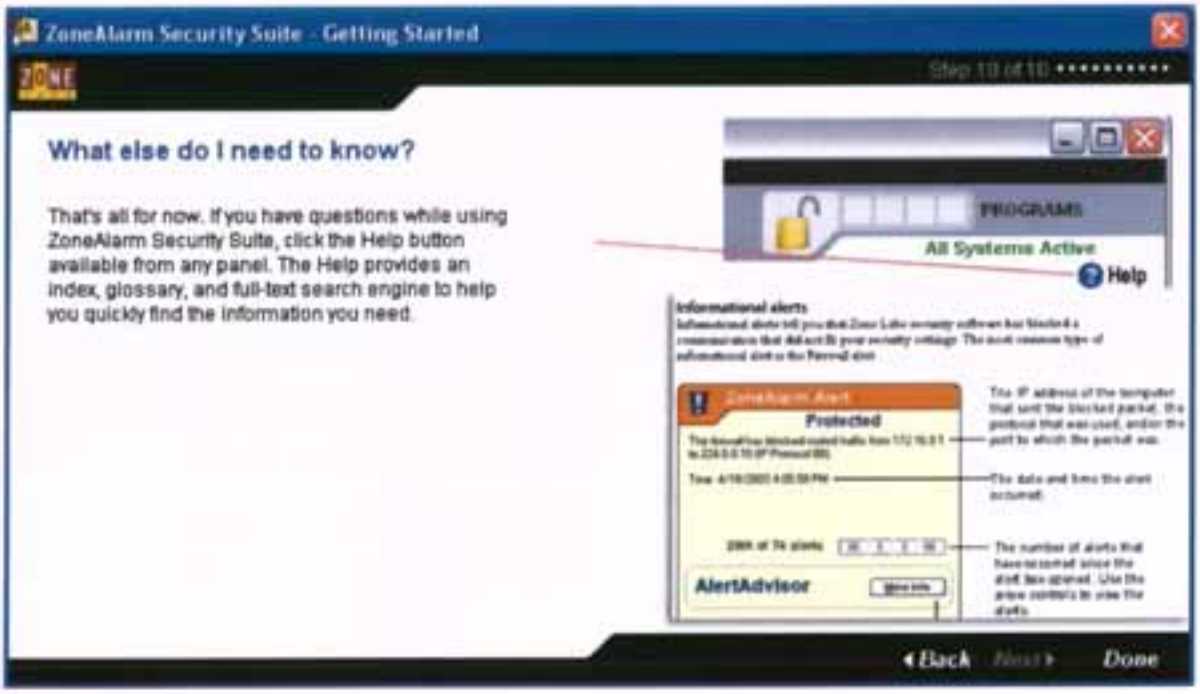
Το Zone Alarm Security Suite χρησιμοποιεί Ζώνες , για να ελέγχει τις καλές, τις κακές και τις άγνωστες σελίδες στο Internet.

Unknown Zone: Βασικά όλοι οι υπολογιστές στο Internet, από το Zone Alarm Security Suite, θεωρούνται άγνωστες, και κάθε προσπάθεια επικοινωνίας με τον υπολογιστή σας, είναι απαγορευμένη.

Trusted Zone: Εδώ τοποθετούμε τους υπολογιστές που εμπιστευόμαστε, όπως π.χ άλλοι υπολογιστές στο τοπικό δίκτυο του σπιτιού μας ή στο τοπικό δίκτυο του γραφείου.
Blocked Zone: Εδώ τοποθετούνται οι σελίδες του Internet που δεν θέλουμε να έχουμε επικοινωνία με αυτές.



Με την χρήση του κουμπιού Stop και του κουμπιού Internet Lock μπορούμε αμέσως να διακόψουμε κάθε επικοινωνία του υπολογιστή μας στο Internet, εάν αντιληφθούμε ότι ο υπολογιστής μας δέχεται επίθεση από κακόβουλους Hackers.



Αυτά είναι αρκετά, για να λειτουργήσει το Zone Alarm Security Suite, αποτελεσματικά.

Βιβλιογραφία

1. Firewalls Complete by Marcus Concalves
2. Hacker Proof by Lars Klander
3. Building Internet Firewalls by D. BrentChapman and Elizabeth Zwicky..
4. International Working Group on Data Protection in Telecommunications, "Data Protection on the Internet: Report and Guidance-Budapest Draft ", Revised on the basis of the discussion at the 19th meeting of the Group in Budapest. April 1996.
5. Bangermann H., "Eyrope and the Global Information Society", Report to the June 1994 meeting of the European Council, European Commission, Brussels.
6. Mayer-Schonberger V., "The Internet and Privacy Legistation", West Virginia Journal of Law and Technology. March 17 1997.
7. Chewick W., Bellovin S., "Firewalls and Internet Security", 2nd edition, Addison-Wesley, 1996

web-sites:

http://download.zonelabs.com/bin/promotions/zap/turbotax.html
http://www.howstuffworks.com/firewall.htm
http://www.interhack.net/pubs/fwfaq/
http://www.faqs.org/faqs/firewalls-faq/
http://www.firewallguide.com/software.htm
http://www.acm.org/crossroads/xrds2-1/security.html
http://www.wilders.org/firewalls.htm
http://www.dealtime.com/xPP-Firewalls
http://www.iopus.com/guides/free-firewall.htm
http://www.pcstats.com/articleview.cfm?articleID=1450
http://www.windowsecurity.com/software/Firewalls/
http://www.windowsecurity.com/software/Firewalls/
http://www.wilyhacker.com/1e/
http://www.wilyhacker.com/1e/
http://info.ccone.at/INFO/FreeBSD/firewalls.html
http://www.practicallynetworked.com/sharing/firewall.htm
http://www.practicallynetworked.com/sharing/firewall.htm
http://www.go-online.gr/ebusiness/specials/article.html?article_id=410
http://www.fotoart.gr/antivirus/firewalls.htm
http://www.pointer.gr/free_docs/greek_linux_howto/Firewall-and-Proxy-HOWTO-GR.html