University of Macedonia
Management in Information Systems

Lesson: "**Information Systems For Marketing & Polls**"
Teacher: **Anastasios Economides**

Comparison of Personal Firewalls

Christos Venetis
MIS-M5/01
May 2002

Πανεπιστήμιο Μακεδονίας
ΠΜΣ Πληροφοριακά Συστήματα

Μάθημα: "Πληροφοριακά Συστήματα για Μάρκετινγκ και Δημοσκοπήσεις"
Υπεύθυνος Καθηγητής: Αναστάσιος Οικονομίδης

Comparison of Personal Firewalls

Βενέτης Χρήστος
MIS-M5/01
Μάιος 2002

Abstract

In the present work, in the frames of course '**Informatics Systems for Marketing and Polls**', are presented the most known Personal Firewalls. The technologies of safety in the space of Information technology, become always more vital importance for the dissuasion of attacks and the obliteration of liabilities of systems safety. For most users of domestic computers and small enterprises, **Personal firewalls** constitute a tool that if it is used rightly it can increase considerably the safety of a system.

In the first chapter is examined generally the subject of safety of Informative Systems and the repercussions in the Society of Information and the Economy. The second chapter is concerning about the safety specifically in the Internet. In the next chapter are reported elements of Firewalls technologies. In the fourth chapter are reported general informations and the characteristics of the most popular software of firewalls. Then are mentioned comparatively elements of firewalls that were analyzed in the precedent chapter.

Περίληψη

Στην παρούσα εργασία, στα πλαίσια του μαθήματος "**Πληροφοριακά Συστήματα για Μάρκετινγκ και Δημοσκοπήσεις**", παρουσιάζονται τα πλέον γνωστά Personal Firewalls. Οι τεχνολογίες ασφάλειας στον χώρο της Πληροφορικής, γίνονται όλο και περισσότερο ζωτικής σημασίας για την αποτροπή επιθέσεων και την εξάλειψη των ευπαθειών στην ασφάλεια των συστημάτων. Για τους περισσότερους χρήστες οικιακών υπολογιστών και μικρών επιχειρήσεων τα φράγματα ή ευρύτερα γνωστά ως **Personal Firewalls**, αποτελούν ένα εργαλείο που αν χρησιμοποιηθεί σωστά μπορεί να αυξήσει σημαντικά την ασφάλεια ενός συστήματος.

Στο πρώτο κεφάλαιο εξετάζεται γενικά το θέμα της ασφάλειας Πληροφοριακών Συστημάτων και οι επιπτώσεις στην Κοινωνία της Πληροφορίας και στην Οικονομία. Στο δεύτερο κεφάλαιο αναπτύσσεται το θέμα της ασφάλειας ειδικά στο Διαδίκτυο. Στο επόμενο κεφάλαιο αναφέρονται στοιχεία της τεχνολογίας ασφαλείας των Firewalls. Στο τέταρτο κεφάλαιο αναφέρονται γενικές πληροφορίες και τα χαρακτηριστικά των πλέον δημοφιλών πακέτων λογισμικού firewalls. Στο τελευταίο κεφάλαιο παρατίθενται συγκριτικά στοιχεία-πίνακες των τύπων firewalls που αναλύθηκαν στο προηγούμενο κεφάλαιο.

CONTENTS

Περιεχόμενα

1. ΕΙΣΑΓΩΓΗ

1.1 Γενικά

«*Υπάρχουν πολλοί τρόποι για να ληστεύεις ανθρώπους. Οι υπολογιστές απλώς κάνουν τη δουλειά ευκολότερη*», είχε πει σε μια διάλεξή του ο κοινωνιολόγος-εγκληματολόγος Jim Thomas. Σε όλα λοιπόν τα προηγμένα τεχνολογικά κράτη το φάντασμα του ηλεκτρονικού εγκλήματος πλανάται απειλητικά, κινητοποιώντας δυνάμεις, δημιουργώντας νέες υπηρεσίες, απελευθερώνοντας ταλέντα με ροπή προς το έγκλημα.

Τα Πληροφοριακά Συστήματα συγκεντρώνουν σήμερα όλο και περισσότερες πληροφορίες. Η αύξηση του όγκου των πληροφοριών, σε συνδυασμό με τη δυνατότητα χειρισμού τους από μακριά λόγω των δικτύων ή την αποκεντρωμένη φύση των συστημάτων, τα καθιστά ευάλωτα. Βέβαια, απαιτείται ευρεία γνώση και επιδεξιότητα, για να μπορέσει κάποιος -που δεν είναι εξουσιοδοτημένος χρήστης- να επιτύχει πρόσβαση σε συστήματα. Όμως, ο όγκος και η μεγάλη αξία που έχουν οι πληροφορίες, ιδιαίτερα στο χώρο των ανταγωνιστικών εταιριών και των εθνικών συμφερόντων, ενθαρρύνει τις απόπειρες για προσβάσεις χωρίς την άδεια χρήσης και την τέλεση ηλεκτρονικού εγκλήματος. **(6)**

Ασφάλεια Πληροφοριακού Συστήματος, σημαίνει προστασία της εμπιστευτικότητας (confidentiality), της ακεραιότητας (integrity) και της διαθεσιμότητας (availability) των πληροφοριών. Οι επιπτώσεις είναι αναλόγου κάθε φορά βαθμού και τις διακρίνουμε σε: διαρροή πληροφοριών (disclosure), τροποποίηση δεδομένων (modification), καταστροφή δεδομένων ή εξοπλισμού (destruction) και μη διαθεσιμότητα (denial) των πληροφοριών και της λειτουργικότητας συστημάτων. Από τις τρεις κύριες λειτουργίες που εκτελούν τα πληροφοριακά συστήματα δηλαδή την απόκτηση, αποθήκευση και μετάδοση πληροφοριών αναμφίβολα η μετάδοση περιλαμβάνει τους περισσότερους κινδύνους ασφάλειας.

Για να περιοριστούν οι κίνδυνοι αθέμιτης πρόσβασης των Πληροφοριακών Συστημάτων και απώλειας ή καταστροφής πληροφοριακών δεδομένων έχει αναπτυχθεί η τεχνολογία και ο επιστημονικός κλάδος ασφάλειας των πληροφοριών. Κύριο μέλημα στα συστήματα αυτά είναι η προστασία των πληροφοριών από αθέμιτη χρήση. Για το λόγο αυτό οι πληροφορίες διαβαθμίζονται, ανάλογα με την εμπιστευτικότητά τους, και προστατεύονται με φυσικούς και λογικούς κανόνες. Λαμβάνονται τα απαραίτητα τεχνικά μέτρα και παράλληλα, προβλέπεται η τήρηση αυστηρών κανονισμών λειτουργίας και διαχείρισης των Υπολογιστικών Κέντρων.

1.2 Επιπτώσεις στην Κοινωνία της Πληροφορίας και στην Οικονομία

«*Ουδέν κακόν αμιγές καλού*» έλεγαν οι αρχαίοι μας πρόγονοι, αλλά σήμερα πια και κάτω από το πρίσμα των συνεχών κοσμογονικών τεχνολογικών εξελίξεων, ίσως η αντιστροφή του ρητού αυτού θα προσέγγιζε καλύτερα την πραγματικότητα.

Η περίοδος την οποία διανύουμε χαρακτηρίζεται από μία αυξανόμενη διαθεσιμότητα και χρήση των τεχνολογιών της Κοινωνίας της Πληροφορικής. Η περαιτέρω τεχνολογική ανάπτυξη και η αυξημένη χρήση των ανοικτών δικτύων, όπως το Internet, κατά τα επόμενα έτη θα δημιουργήσουν νέες σημαντικές δυνατότητες και θα θέσουν νέες προκλήσεις.

Οι υποδομές πληροφόρησης και επικοινωνίας έχουν καταστεί ουσιαστικό τμήμα των οικονομιών μας. Δυστυχώς, όμως, αυτές οι υποδομές έχουν τα δικά τους αδύνατα σημεία και προσφέρουν νέες ευκαιρίες για εγκληματικές συμπεριφορές. Αυτές οι εγκληματικές δραστηριότητες μπορούν να λάβουν διάφορες μορφές και να διασχίσουν πολλά σύνορα. Παρά το γεγονός ότι, για μια σειρά από διάφορους λόγους, δεν υπάρχουν αξιόπιστες στατιστικές, είναι αναμφίβολο ότι αυτά τα αδικήματα αποτελούν απειλή για τις βιομηχανικές επενδύσεις και κεφάλαια, καθώς και για την ασφάλεια και εμπιστοσύνη στην κοινωνία της πληροφορίας. Ορισμένα πρόσφατα παραδείγματα επιθέσεων ιών και άρνησης παροχής υπηρεσίας έχουν προξενήσει σημαντικές οικονομικές ζημιές.

Οι χρήστες πρέπει να μπορούν να υπολογίζουν στη διαθεσιμότητα υπηρεσιών πληροφόρησης και να έχουν εμπιστοσύνη στο γεγονός ότι οι επικοινωνίες τους και τα δεδομένα τους θα προστατεύονται κατά οιασδήποτε μη εξουσιοδοτημένης πρόσβασης ή τροποποίησης. **Η ανάπτυξη του ηλεκτρονικού εμπορίου και η πλήρης υλοποίηση της Κοινωνίας της Πληροφορίας εξαρτώνται άμεσα από αυτό**. Οι νέες ψηφιακές και ασύρματες τεχνολογίες υπάρχουν ήδη παντού. Μας παρέχουν επίσης τη δυνατότητα συμμετοχής, διδασκαλίας και εκμάθησης, από κοινού εργασίας και συμμετοχής στην πολιτική διαδικασία. Στο μέτρο εντούτοις που οι κοινωνίες θα εξαρτηθούν περισσότερο από τις νέες τεχνολογίες, θα πρέπει να χρησιμοποιηθούν τεχνολογικά και νομικά μέσα για να αντιμετωπιστούν οι κίνδυνοι που συνδέονται με αυτή την εξέλιξη. **(3)**

Τα προβλήματα ασφάλειας δεδομένων εξαρτώνται από τις σύγχρονες προόδους στις τεχνολογίες πληροφορικής όπως είναι οι τεράστιοι αποθηκευτικοί χώροι δεδομένων, και επεξεργαστές με μεγάλη υπολογιστική ισχύ και δυνατότητες στην διαχείριση δεδομένων. Οι απαιτήσεις λοιπόν στα θέματα ασφάλειας αλλάζουν συνεχώς καθόσον αλλάζουν και τα χαρακτηριστικά των νέων τεχνολογιών. Οι εισαγωγή της τηλε-επεξεργασίας σε όλες τις δραστηριότητες των επιχειρήσεων, εμπορίου και βιομηχανίας φέρνουν νέα προβλήματα στη ασφάλεια δεδομένων.

2. ΑΣΦΑΛΕΙΑ ΣΤΟ ΔΙΑΔΙΚΤΥΟ 

Πρόσφατα στοιχεία αναφέρουν ότι καθημερινά διακινούνται περισσότερα από τρία δισεκατομμύρια e-mail από 200 εκατομμύρια χρήστες, ο δε συνολικός αριθμός των χρηστών του Διαδικτύου ξεπερνά τα 400 εκατομμύρια σε όλο τον κόσμο. Στην Ελλάδα, στις αρχές του 2001, οι χρήστες του Διαδικτύου ξεπέρασαν τις 600.000 και υπολογίζεται ότι μέχρι το τέλος του ιδίου έτους έχουν ξεπεράσει τις 900.000. Αν και υπάρχει η γενική παραδοχή ότι το ηλεκτρονικό έγκλημα δεν είναι ευρέως διαδεδομένο, πολλοί είναι αυτοί που ανησυχούν για το άμεσο μέλλον και ιδίως εν όψει της Ολυμπιάδας, όπου η χρήση της τεχνολογίας θα είναι το Α και το Ω σε πάρα πολλούς τομείς. **(2)**

Οι συνήθεις απειλές στον κυβερνοχώρο είναι η διατάραξη επικοινωνιών, η εκμετάλλευση ευαίσθητων και διαβαθμισμένων πληροφοριών, η χειραγώγηση για πολιτικούς, οικονομικούς σκοπούς και τέλος η καταστροφή πληροφοριών και υποδομών. Λόγοι για τους οποίους το Διαδίκτυο είναι ευάλωτο σε επιθέσεις:

- Πολλά από τα αρχικά δικτυακά πρωτόκολλα που σήμερα αποτελούν μέρος της υποδομής του Διαδικτύου σχεδιάστηκαν χωρίς να ληφθεί υπόψη η ασφάλεια.
- Λόγω της ανοικτής φύσης του Διαδικτύου και του αρχικού σχεδιασμού των πρωτοκόλλων, οι επιθέσεις στο Διαδίκτυο είναι γενικά γρήγορες, εύκολες, χωρίς κόστος και μπορεί να είναι πολύ δύσκολο να ανιχνευθούν ή να βρεθεί η πηγή προέλευσής τους.
- Πολλές δικτυακές τοποθεσίες παρουσιάζουν αδικαιολόγητη εμπιστοσύνη στο Διαδίκτυο.
- Μια και ένα μεγάλο μέρος της κυκλοφορίας στο Διαδίκτυο δεν είναι κρυπτογραφημένη, η εμπιστευτικότητα και η ακεραιότητα της πληροφορίας είναι δύσκολα να επιτευχθούν.
- Προβλήματα ασφάλειας σε επίπεδο λειτουργικών συστημάτων
- Τέλος, ο εκρηκτικός ρυθμός ανάπτυξης του Διαδικτύου έχει αυξήσει την ανάγκη για καλά εκπαιδευμένο και έμπειρο προσωπικό. **(7)**

Ένα από τα πλέον, τα πιο κύρια ιδιοχαρακτηριστικά του συστήματος απειλής στον κυβερνοχώρο είναι αυτό που λέγεται "**Αόρατη Απειλή**". Δεν γνωρίζει κανείς ποια χρονική στιγμή θα εκδηλωθεί, δεν γνωρίζει κανείς από ποια αφετηρία θα εκδηλωθεί, δεν γνωρίζει πολύ καλά τον τρόπο με τον οποίο θα εκδηλωθεί το πρόβλημα. Μια άλλη επισήμανση είναι ότι κανένα σύστημα δεν είναι απόλυτα ασφαλές, ή με κάπως διαφορετικούς όρους για να καταστεί ένα σύστημα απόλυτα ασφαλές στον ύψιστο βαθμό, απαιτείται εξαιρετικά υψηλό κόστος και επομένως θα πρέπει να λάβει κανείς υπόψη του τις οικονομικές συνιστώσες. Και το ερώτημα που εγείρεται είναι, πως προκύπτει το πρόβλημα.

Το πρόβλημα προκύπτει κατά βάση επειδή τα συστήματα που οικοδομούμε είναι ανοιχτά στον έξω κόσμο, θέλουμε να είναι προσβάσιμα από πολλούς. Αυτό επιβάλλει τις δικτυακές διασυνδέσεις. Επομένως αρχίζει η εγγενής στο σύστημα διαδικασία προσβολής του και επιπλέον στο πρόβλημα συμβάλλουν οι αδυναμίες του λογισμικού λειτουργικών συστημάτων ή του λογισμικού εφαρμογών και όχι τόσο οι αδυναμίες του υλικού. Σε αυτές τις αδυναμίες πρέπει κανείς να ενσκήψει την προσοχή του. Ποιες βασικές, χωρίς να δώσει κανείς συνταγές ή απόλυτες λύσεις, θεραπείες επιδέχεται το πρόβλημα; Είναι λίγο προφανές ότι κάτι που πρέπει πρώτα απ' όλα να μεριμνήσουμε είναι η πρόληψη και η αποτροπή. Αυτό θα ήταν μια καλή αφετηρία για να αποφύγουμε τους κινδύνους. **(7)**

Τα προϊόντα ασφάλειας και μυστικότητας παρέχουν επαρκή προστασία επειδή οι περισσότερες "επιθέσεις" είναι απρόσωπες. Δηλαδή οι επιτιθέμενοι δεν στοχεύουν σε συγκεκριμένο χρήστη ή υπολογιστή αλλά ψάχνουν οποιοδήποτε εύκολο στόχο συνδεδεμένο στο Διαδίκτυο. Εάν ο χρήστης καταστήσει δύσκολο να εντοπισθεί το μηχάνημα και δύσκολη την είσοδο στον υπολογιστή, θα τον αφήσουν πιθανότατα ανενόχλητο. Εάν ένας πραγματικός χάκερ αποφασίσει να επιτεθεί στον υπολογιστή σας, μπορείτε να τον καταστήσετε δύσκολο για προσβολή αλλά εάν είναι καλός, θα βρεί πιθανώς έναν τρόπο. Γι' αυτό οι μεγάλες οργανώσεις έχουν το προσωπικό και τους συμβούλους ασφάλειας υπολογιστών να απασχολούνται 24/7/365 ώρες/ημέρες για να προστατεύσουν τα δίκτυα υπολογιστών τους.

Είναι δυνατόν οι επιθέσεις στο διαδίκτυο να αντιμετωπισθούν; Σύμφωνα με το CERT **ναι** στο 99% των περιπτώσεων. Οι διάφορες μορφές επίθεσης χρήζουν αντιμετώπισης που εξαρτάται από τη φύση τους, από τον άμεσο δηλαδή στόχο τους. Έχει αναπτυχθεί ειδικό λογισμικό για τον εντοπισμό και εξουδετέρωση ιών, worms και toolkits καθώς επίσης για τον έλεγχο (monitoring) και την καταγραφή (logging) της δράσης προγραμμάτων αποκάλυψης κωδικών (password crackers) ή απλών εντολών χρηστών. Τα συστήματα μπορούν να υφίστανται "φιλτράρισμα" απέναντι σε συγκεκριμένες μορφές επίθεσης όπως IP spoofing packets, mail spam κτλ. Επιπλέον, ατέλειες που εντοπίζονται σε λογισμικό μπορούν να διορθώνονται (patch), αρχεία να προστατεύονται με κωδικοποίηση ή με περιορισμό στα δικαιώματα πρόσβασης των χρηστών σε αυτά. Μια τελευταία λύση ενάντια στις ανεξέλεγκτες επιθέσεις είναι η διατήρηση αντιγράφων, αν όχι για όλα τουλάχιστο για τα "σημαντικά" τμήματα των πόρων ενός συστήματος που είναι και πιο ευάλωτα σε επιθέσεις. **(4)**

Τα φράγματα ή ευρύτερα γνωστά ως **firewalls**, αποτελούν επίσης ένα εργαλείο που αν χρησιμοποιηθεί σωστά μπορεί να αυξήσει σημαντικά την ασφάλεια ενός συστήματος. Πλέον των προαναφερθέντων η πιο αποτελεσματική ασπίδα προστασίας απέναντι στις επιθέσεις είναι η αναγνώριση του κινδύνου, η ύπαρξη πολιτικής ασφαλείας και η αυστηρή εφαρμογή της.

3. Firewalls (Φράγματα)

3.1 Γενικά

«Το τέλειο firewall θα πρέπει να είναι φθηνό, εύκολο στην εγκατάσταση και στη χρησιμοποίηση, με σαφείς επεξηγήσεις στις επιλογές διαμόρφωσης, να έχει την δυνατότητα να κρύβει όλες τις θύρες του PC ώστε να είναι αόρατο στις ανιχνεύσεις, να προστατεύει το σύστημά από όλες τις επιθέσεις, να προειδοποιεί τον χρήστη αμέσως από σοβαρές επιθέσεις, και να εξασφαλίζει ότι τίποτα αναρμόδιο δεν εισέρχεται ή φεύγει από το PC», [1]

Firewall (Φράγμα), είναι μια συσκευή υλικού ή λογισμικού, ένα σύστημα που επιβάλλει πολιτική ελέγχου πρόσβασης μεταξύ δύο δικτύων -- όπως μεταξύ ενός ιδιωτικού τοπικού LAN και του επισφαλούς δημόσιου Διαδικτύου. Επίσης καθορίζει ποιες εσωτερικές υπηρεσίες μπορούν να προσεγγιστούν από το εξωτερικό περιβάλλον, και αντίστροφα. Τα μέσα με τα οποία αυτό ολοκληρώνεται ποικίλλουν ευρέως, αλλά σε γενικές γραμμές, το firewall μπορεί να θεωρηθεί ως ένα ζεύγος μηχανισμών: ένας για να εμποδίσει και ένας για να επιτρέψει την κυκλοφορία. Ένα firewall είναι κάτι περισσότερο από την κλειδωμένη μπροστινή πόρτα σε ένα σύστημα ή δίκτυο -- είναι επίσης η φρουρά ασφάλειάς του συστήματος.

Η έννοια του firewall είναι να παρέχει ένα ελεγχόμενα διαπερατό εμπόδιο μεταξύ του χρήστη PC και του Διαδικτύου κατά την διάρκεια της σύνδεσης. Το διαπερατό μέρος της υπόθεσης είναι σημαντικό, δεδομένου ότι ένα εμπόδιο που δεν θα επέτρεπε τίποτα να περάσει θα έκανε το σέρφινγκ στον Παγκόσμιο Ιστό αδύνατο. Εντούτοις, το εμπόδιο πρέπει να εφαρμόσει πολύ ακριβείς κανόνες για αυτό που επιτρέπεται και τι δεν είναι επιτρεπτό. Οι σελίδες από έναν επισκεπτόμενο κεντρικό υπολογιστή δικτύου είναι κάτι επιθυμητό να διαπεράσουν μέσω του firewall. Ένας κώδικας δούρειου ίππου όμως όχι!

Το firewall μπορεί να παρέχει σε έναν διαχειριστή δικτύων τα στοιχεία για τα είδη data και ποσό κυκλοφορίας που πέρασε μέσω αυτού, πόσες προσπάθειες έγιναν να σπάσουν το σύστημα ασφάλειας, και άλλες υπηρεσίες επίσης. Όπως ένα κλειστό σύστημα TV ασφάλειας κυκλωμάτων, το firewall όχι μόνο αποτρέπει την πρόσβαση, αλλά αποθαρρύνει και τους κακόβουλους ανιχνευτές του δικτύου που ανιχνεύουν τριγύρω για ανοικτές θύρες, και βοηθά επίσης στον προσδιορισμό εκείνων που προσπαθούν να παραβιάσουν την ασφάλειά ενός συστήματος. Το firewall αρχικά καθορίζει εάν η εισερχόμενη μετάδοση είναι κάτι που ζητείται από έναν χρήστη στο δίκτυο, και απορρίπτει όλα τα άλλα. Οτιδήποτε εισέρχεται εξετάζεται περισσότερο. Ελέγχεται η διεύθυνση υπολογιστών του πομπού για να εξασφαλιστεί ότι είναι εμπιστευμένη περιοχή ή όχι. Ελέγχεται επίσης το περιεχόμενο της μετάδοσης. **(5)**

---

[1] *Make Your PC Hacker Proof, Jeff Sengstack, PC World, July 21, 2000.*

Εξ' αιτίας της θέσης τους στη τομή δύο δικτύων, μπορούν να εξυπηρετήσουν και άλλους σκοπούς, όπως να εμποδίσουν την πρόσβαση σε συγκεκριμένες τοποθεσίες του Διαδικτύου ή τη χρήση κάποιων εξυπηρετών ή υπηρεσιών. Ανάλογα με την μέθοδο διαλογής και αποτροπής πρόσβασης, είναι γνωστοί τρεις τύποι προϊόντων υλικού ή λογισμικού firewall,:

- Απαγόρευση εισερχομένων δεδομένων τα οποία δεν έχουν ζητηθεί από τον χρήστη στο δίκτυο.
- Διαλογή από τη διεύθυνση του πομπού.
- Διαλογή από το περιεχόμενο της επικοινωνίας. **(4)**

Ο οργανισμός **ICSA**[2] τα ταξινομεί σε τρεις κατηγορίες: φίλτρων πακέτων, application-level proxy servers, και επιθεώρησης πακέτων.

3.2 Μηχανισμός Λειτουργίας

Θα πρέπει να θεωρήσουμε ότι το καλώδιο που συνδέει έναν υπολογιστή με το Διαδίκτυο είναι ίσως η πιο βασική μορφή firewall. Χωρίς το καλώδιο ή άλλη συσκευή μετάδοσης που συνδέει μια μηχανή με το Διαδίκτυο, οι κακόβουλοι hackers θα τα είχαν εντελώς χαμένα στην προσπάθειά τους να πετύχουν πρόσβαση στον υπολογιστή από απόσταση. Μερικοί ιδιαίτεροι υπολογιστές που περιέχουν ευαίσθητες πληροφορίες προστατεύονται, στην πραγματικότητα, με αυτόν ακριβώς τον τρόπο. Μια ομάδα μηχανών σε μια επιχείρηση μπορεί να διαχωριστεί από το μεγαλύτερο εταιρικό δίκτυο, επομένως και από το Διαδίκτυο, για να εξασφαλιστεί η πλήρης ασφάλεια της.

Η λύση βέβαια της απομόνωσης από το Διαδίκτυο ακούγεται μάλλον ακραία και μη πρακτική. Στην πραγματικότητα χρειαζόμαστε μια λύση που θα φιλτράρει το Διαδίκτυο, επιτρέποντας τη δίοδο δεδομένων που χρειαζόμαστε και απαγορεύοντάς την σε αυτά που δεν θέλουμε.

Το Διαδίκτυο δεν δημιουργεί πραγματικά άμεσες συνδέσεις μεταξύ μηχανών που μπορούν εύκολα να αποτελέσουν στόχο εισβολής ή πειρατείας. Αν για παράδειγμα κάποιος χρήστης Α καλέσει κάποιον άλλο Β μέσω τηλεφώνου, τότε σε ένα εκπληκτικά σύντομο χρονικό διάστημα, δημιουργείται ένα άμεσο κύκλωμα, συνδέοντας τα δύο τηλέφωνα σε καθένα από τα δύο άκρα της συνομιλίας. Η φωνή του Α μετατρέπεται τότε σε ένα ηλεκτρικό σήμα που ρέει κατά μήκος του κυκλώματος σαν αυτοκίνητα που τρέχουν σε ένα αυτοκινητόδρομο και ενώ οι υπόλοιπες έξοδοι του δρόμου παραμένουν κλειστές.

Αν άντ' αυτού ο χρήστης Α χρησιμοποιούσε έναν άλλο υπολογιστή προκειμένου να δει κάποιες πληροφορίες στο site της εταιρείας στην οποία εργάζεται, ο φυλλομετρητής του δεν δημιουργεί κάποια άμεση σύνδεση ανάμεσα στο σπίτι του χρήστη και στους διακομιστές (servers) της εταιρείας. Μια πιθανή αίτηση του χρήστη να δει συγκεκριμένες ιστοσελίδες ρέει από τον υπολογιστή του με τη μορφή ανεξάρτητων πακέτων πληροφορίας.

[2] Διεθνής Ένωση Ασφάλειας Υπολογιστών

Κάθε ένα από αυτά τα πακέτα περιλαμβάνει ένα τμήμα δεδομένων επικοινωνίας, μαζί με την IP διεύθυνση του υπολογιστή προέλευσης στο σπίτι του χρήστη Α, και τον υπολογιστή προορισμού, στην εταιρεία στην οποία εργάζεται. Κάθε πακέτο περιλαμβάνει επίσης μια σημαία, γνωστή ως δυαδικό ψηφίο **ack**, το οποίο δείχνει εάν η μηχανή προορισμού ζήτησε ένα ιδιαίτερο πακέτο. Έτσι για παράδειγμα όταν αρχίζουν τα πακέτα που περιέχουν τα στοιχεία της ιστοσελίδας που ζητήθηκε, να ρέουν πίσω προς τον υπολογιστή του Α, το δυαδικό ψηφίο ack τίθεται ναι. Σημειώνεται ότι το αρχικό αίτημα του χρήστη Α προς τον κεντρικό υπολογιστή του δικτύου θα έθετε ένα δυαδικό ψηφίο [ack όχι], δεδομένου ότι αρχίζει η επικοινωνία. Αυτό γίνεται πολύ σημαντικό αργότερα.

Με κάθε πακέτο πληροφοριών να περιέχει τις διευθύνσεις πομπού και δέκτη, μια συγκεκριμένη, άμεση σύνδεση μεταξύ δύο μηχανών δεν είναι απαραίτητη. Άντ' αυτού, το πακέτο κατευθύνεται από έναν υπολογιστή δρομολογητή Διαδικτύου σε έναν άλλο. Κάθε δρομολογητής (router) κοιτάζει τη διεύθυνση προορισμού και στέλνει το πακέτο λίγο πιο κοντά προς το στόχο του. Κατά μήκος της διαδρομής αναμιγνύεται με άλλα πακέτα -- στην αναλαμπή ενός ματιού, κυριολεκτικά -- βρίσκει τον δρόμο του προς το σωστό υπολογιστή, όπου επανασυνδέεται με άλλα πακέτα από τον ίδιο πομπό και ανασυγκροτείται σε ένα αναγνώσιμο από τη μηχανή μήνυμα.

Πώς όμως όλα αυτά μας βοηθούν να χτίσουμε ένα firewall-φίλτρο. Κατ' αρχάς, οι πληροφορίες διευθύνσεων είναι σημαντικές. Εάν κάθε πακέτο περιλαμβάνει τη διεύθυνση του πομπού του, ένα firewall μπορεί εύκολα να τεθεί ως το τείχος που θα εμποδίσει όλα τα πακέτα από έναν συγκεκριμένο πομπό, ή να επιτρέψει μόνο τα πακέτα από έναν κατάλογο συγκεκριμένων πομπών. Ενώ αυτό είναι ένα βήμα προς τα εμπρός, σημαίνει επίσης ότι είτε πρέπει να περιοριστεί μέρος της πρόσβασης είτε να προβλεφθούν οι διευθύνσεις των hackers εκ των προτέρων. Αυτό είναι και το σημείο στο οποίο μπαίνει το δυαδικό ψηφίο ack. Εάν έχουν ζητηθεί ιστοσελίδες από τον κεντρικό υπολογιστή της εταιρείας, τα πακέτα θα κατευθυνθούν πίσω στον υπολογιστή του χρήστη Α, με μια διεύθυνση επιστροφής της εταιρείας, και το δυαδικό ψηφίο ack τίθεται ναι.

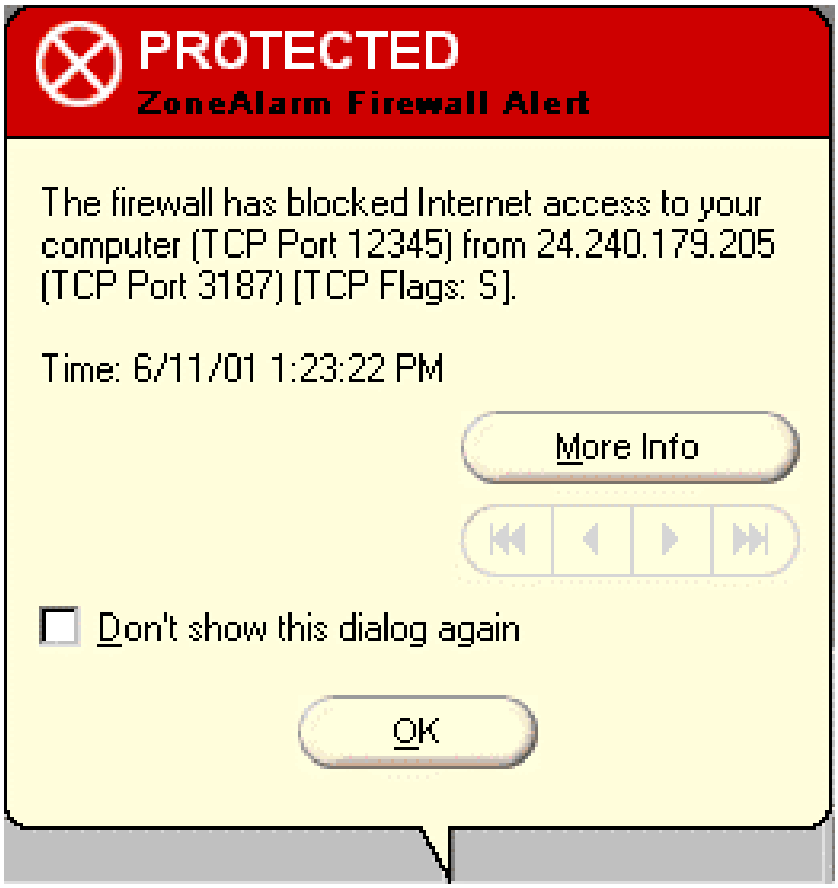
Σε μια τυπική επίθεση υπολογιστών, επειδή στο άκρο της σύνδεσης δεν έχουν ζητηθεί πακέτα, το ψηφίο ack έχει τεθεί στην ένδειξη όχι. Η διεύθυνση επιστροφής είναι άγνωστη, γεγονός που υποδεικνύει ότι ο αποστολέας είναι κάποιος άγνωστος. Παρατηρώντας αυτά τα χαρακτηριστικά, ένα firewall θα μπορούσε να αρνηθεί τη διέλευση τέτοιων πακέτων, αποβάλλοντας οποιαδήποτε κρυφή απειλή που τα δεδομένα μπορεί να περιέχουν. Η κατάσταση είναι πιο περίπλοκη για τους χρήστες που θέλουν να έχουν πρόσβαση σε κάποιο συγκεκριμένο site από τον υπολογιστή τους. Κατά τη λειτουργία ενός Web Server παρατηρείται μια συνεχής ροή πακέτων που ποτέ δεν έχουν ζητηθεί. Ολόκληρες στρατιές πακέτων παρουσιάζονται με αρνητικά δυαδικά ψηφία ack, και με άγνωστες συνημμένες διευθύνσεις επιστροφής. Ένα αποτελεσματικό firewall για έναν κεντρικό υπολογιστή πρέπει να είναι σε θέση να αναλύσει τη συμπεριφορά των πακέτων με περισσότερη λεπτομέρεια και να εμποδίζει την διέλευση ύποπτων προγραμμάτων και δραστηριότητας.

4. Δημοφιλή Πακέτα Λογισμικού Personal Firewall

Για τους περισσότερους χρήστες οικιακών υπολογιστών και μικρών επιχειρήσεων, είναι διαθέσιμο ένα αρκετά υψηλό επίπεδο αποτελεσματικής προστασίας μέσω ποικίλων προσωπικών firewalls. Κατωτέρω παρουσιάζονται μερικά από τα δημοφιλέστερα πακέτα λογισμικού firewall. Όλα τους παρέχουν περισσότερη προστασία από αυτή που απαιτεί ένας μέσος υπολογιστής γραφείου, και μερικά είναι ακόμα και ελευθέρα για προσωπική χρήση. [19]

4.1 ZoneAlarm™ & ZoneAlarm Pro

Τα Zone Labs παρέχουν δωρεάν τη έκδοση ZoneAlarm (download από το επίσημο Web Site). Το ZoneAlarm λειτουργεί σε Stealth Mode, που καθιστά το PC κυριολεκτικά "αόρατο" στο διαδίκτυο. Το πρόγραμμα είναι κάτι παραπάνω από αρκετό για την προστασία ενός απλού χρήστη. Διαθέτει εξαιρετικά απλό interface και δίνει τη δυνατότητα στους χρήστες να αποφασίσουν ποια προγράμματα θα έχουν πρόσβαση στο Ίντερνετ αλλά και να ορίσουν αν θα υπάρχει πρόσβαση κατά την απουσία τους. Τηρείται ημερολόγιο με τους συναγερμούς και συνεργάζεται και με προγράμματα ηλεκτρονικού ταχυδρομείου. Υπάρχει ακόμη πλήκτρο άμεσης διακοπής της σύνδεσης με το Ίντερνετ.



Πλεονεκτήματα: Δωρεάν, προστασία από εξωτερικές επιθέσεις, εύκολο στην εγκατάσταση και στη χρησιμοποίηση.
Μειονεκτήματα: Ενοχλητική οθόνη στο ξεκίνημα.
Συμπέρασμα: Παρέχει- δωρεάν- εξαιρετική προστασία σε κάθε χρήστη που σερφάρει στο Ίντερνετ. (8)

ZoneAlarm Pro Edition

Η έκδοση **ZoneAlarm Pro 3.0** προσθέτει την προστασία σύνδεσης ηλεκτρονικού ταχυδρομείου παρόμοια με αυτήν που προσφέρεται από το λογισμικό αντιιών και επίσης την προστασία κωδικού πρόσβασης. Τα προηγμένα χαρακτηριστικά ασφάλειας και προστασίας του προγράμματος Zone Alarm Pro 3.0 είναι:

- Το πρόγραμμα Mail Safe έχει επιπρόσθετα ανιχνευτή ιών για την απομόνωση των συνημμένων αρχείων που πιθανώς είναι μολυσμένα.
- Με ένα βελτιωμένο πρόγραμμα παρακολουθούνται οι προσπάθειες των χάκερς για εισβολή στο σύστημα και εντοπίζονται οι IP διευθύνσεις τους σε όλο τον κόσμο.
- Με τον έλεγχο των Cookies εμποδίζονται τα διάφορα Web sites να κατασκοπεύουν το σύστημα. Με ειδικό εργαλείο (ιδιωτικός σύμβουλος) ενημερώνεται ο χρήστης πότε οι ρυθμίσεις συγκρούονται με την επίσκεψη σε συγκεκριμένο Web site.
- Με την χρήση κωδικού εμποδίζονται άλλοι χρήστες να τροποποιήσουν τις ρυθμίσεις ασφαλείας που έχουν ορισθεί.
- Τοποθετεί Web sites ή IP addresses στη Ζώνη απομόνωσης και τα απομονώνει προσωρινά από την επαφή με το σύστημα του χρήστη. Εντοπίζει και αναγνωρίζει υπολογιστή που επανειλημμένα επιχειρεί "pings" στο μηχάνημα του χρήστη ή απαγορεύει την πρόσβαση σε επιλεγμένα Web sites.
- Προσαρμόζει τις προσωπικές ρυθμίσεις ασφάλειας σε περιβάλλον δικτύου και σε ασύρματα δίκτυα.

Επιπλέον Χαρακτηριστικά του ZoneAlarm Pro 3.0

Features	ZoneAlarm Pro 3.0	ZoneAlarm (βασική έκδοση)
Email virus protection with enhanced MailSafe	√	
"WHOIS" service included	√	
Block specific IP addresses or Web sites	√	
Cookie control for online privacy	√	
Online ad blocking for faster surfing	√	
Auto-config for mobile users	√	
Password protection for security settings	√	
Award-winning security	√	√
Advanced firewall configurations	√	
Backup Disc from Zone Labs	√	

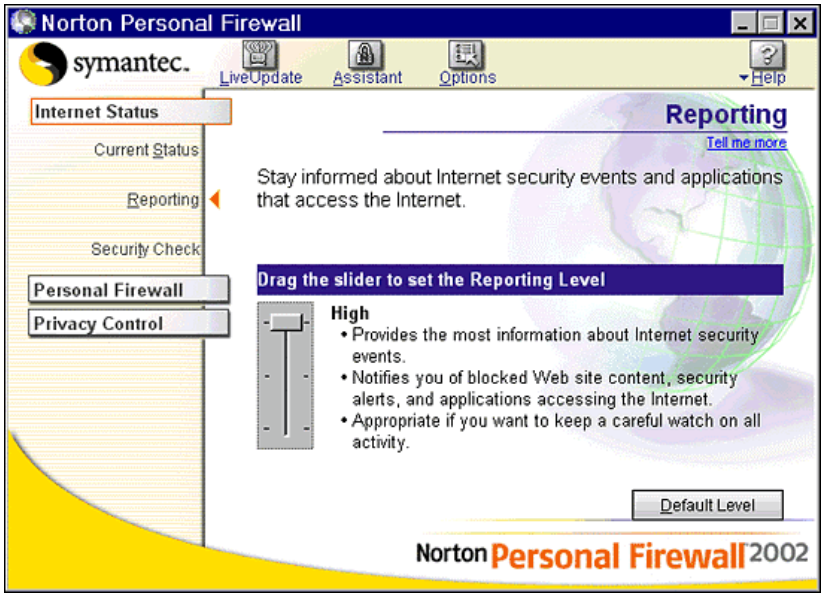
4.2 Norton Personal Firewall 2002

Το Norton Personal Firewall αποτελεί την πιο πρόσφατη έκδοση του προσωπικού πακέτου προστασίας της Symantec και περιλαμβάνει διάφορα καινοτόμα χαρακτηριστικά γνωρίσματα. Απαγορεύει προσωπικές και εμπιστευτικές πληροφορίες να στέλνονται σε μη ασφαλή Web sites χωρίς την γνώση του χρήστη. Με την λειτουργία-δυνατότητα προστασίας εισβολών ειδοποιεί τον χρήστη όταν κάποιος χάκερ προσπαθεί να ανιχνεύσει τον υπολογιστή για ευπάθειες (τρωτότητα).

Για τους προηγμένους χρήστες, το προσωπικό firewall Norton προσφέρει έναν μακρύ κατάλογο προσαρμόσιμων κανόνων που ελέγχουν την πρόσβαση προς και από τον υπολογιστή με λεπτομέρειες ασφάλειας. Η εισερχόμενη ή εξερχόμενη επικοινωνία εμποδίζεται, εξ ορισμού, εκτός αν συγκεκριμένος κανόνας (rule) την επιτρέπει. Οι κανόνες ενεργοποιούνται αυτόματα όποτε συμβαίνει κάποιο “alert” και ο χρήστης αποφασίζει αν η πρόσβαση πρέπει να αμφισβητηθεί ή να επιτραπεί σε ένα συγκεκριμένο πρόγραμμα. Οι χρήστες μπορούν επίσης να διαμορφώσουν τους κανόνες από την αρχή, ενώ το πρόγραμμα παρέχεται με ένα σύνολο προκαθορισμένων κανόνων για τα πιο κοινά προγράμματα Δούρειων Ίππων (Trojan Horses). Για τους περισσότερους χρήστες - μη ενδιαφερόμενους -για τις λεπτομέρειες ασφάλειας, παρέχεται η δυνατότητα επιλογής ενός επιθυμητού (υψηλό, μέσο, χαμηλό) επίπεδου.

Το πρόγραμμα ελέγχει τα εισερχόμενα cookies και περιλαμβάνει μέθοδο ελέγχου εφαρμογών HTTP, όπως οι φυλλομετρητές, για μη διαβίβαση ορισμένων λέξεων μέσω του Διαδικτύου, χωρίς τη δικαιοδοσία του χρήστη. Για παράδειγμα μπορεί κάποιος να εισάγει το όνομα, τη διεύθυνση, και τον τηλεφωνικό του αριθμό για να εμποδίζει αυτές τις πληροφορίες από την υποβολή σε φόρμες του Διαδικτύου και άλλα απευθείας σύνδεσης εργαλεία. Αυτή η προστασία δεν εξετάζει προγράμματα μη- HTTP, όπως το ηλεκτρονικό ταχυδρομείο. **[22]**

Μερικοί υποστηρίζουν ότι το interface δεν είναι τόσο εύχρηστο όσο σε μερικά άλλα προϊόντα αυτής της κατηγορίας. Το κόστος ανέρχεται σε($29.95). Η Symantec δεν προσφέρει έκδοση ελεύθερης δοκιμής. **(8)**



Πλεονεκτήματα:
σταθερή προστασία και διπλή ζώνη άμυνας ενάντια σε μη εξουσιοδοτημένες συνδέσεις μέσω διαδικτύου.
Μειονεκτήματα: δεν απομώνει ή επιτρέπει πρόσβαση σε συγκεκριμένα sites.

Συμπέρασμα:

Ακριβό ώστε να ανταγωνισθεί το δωρεάν ZoneAlarm.

Με την υποστήριξη για τα Windows XP, το Norton Personal Firewall 2002 προσθέτει περισσότερο διαμορφώσιμο έλεγχο της σύνδεσης με το Διαδίκτυο και στους τρόπους άμυνας ενάντια στις απειλές των χάκερ. Η γενική εικόνα της διεπαφής είναι συγκρίσιμη με τον εξερευνητή Windows, με την πλευρά πλοήγησης στα αριστερά και το παράθυρο πληροφοριών στα δεξιά. Υπάρχουν τρία προκαθορισμένα επίπεδα ελέγχου πρόσβασης: Υψηλό, μέσο και χαμηλό τα οποία επιλέγονται με μια απλή ράβδο κύλισης. Για τους πιο πεπειραμένους χρήστες, μπορεί να επιλεχτεί ένα προσαρμοσμένο επίπεδο. Από εδώ, μπορεί να ρυθμιστεί το επίπεδο ασφάλειας των συστατικών Java και ActiveX.

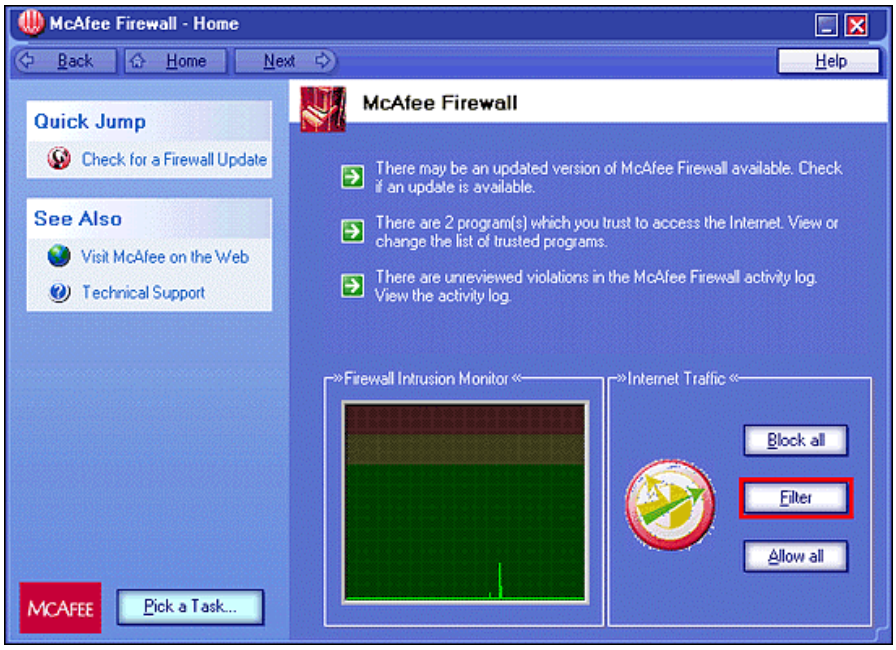
Ένα πρακτικό χαρακτηριστικό γνώρισμα που έχει περιληφθεί είναι η προαιρετική δυνατότητα εξωτερικής ανίχνευσης κινδύνου ασφάλειας (Security Risk Scan option). Με την επιλογή αυτή συνδέεται ο υπολογιστής του χρήστη με τον ιστοχώρο της Symantec, ο οποίος τρέχει έπειτα μια ανίχνευση στο σύστημα. Ελέγχεται το σύστημα ενάντια στις πιο κοινές απειλές των χάκερς και δίνεται αναφορά για τα αποτελέσματα. Με το LiveUpdate program, το λογισμικό του firewall ενημερώνεται με τα πιο πρόσφατα στοιχεία για τις απειλές στον ιστοχώρο της Symantec. Για το πρώτο έτος μετά την αγορά η δυνατότητα αυτή παρέχεται δωρεάν ενώ στη συνέχεια η συνδρομή ενός έτους κοστίζει $9.95. **(20)**

4.3 McAfee.com Personal Firewall.

Το προσωπικό firewall McAfee.com είναι μια υπηρεσία απευθείας σύνδεσης που προσφέρει προστασία, μέσω ενός όχι και τόσο ισχυρού είναι αλήθεια interface, με χαρακτηριστικά γνωρίσματα διάφορους ήχους προειδοποίησης. Εν τούτοις, εκτελεί τα βασικά καθήκοντα. Εκτός από τη παρεχόμενη προστασία ενάντια στις εξωτερικές απειλές, το πρόγραμμα παρεμποδίζει άλλες εφαρμογές που προσπαθούν να πετύχουν πρόσβαση στο Διαδίκτυο.

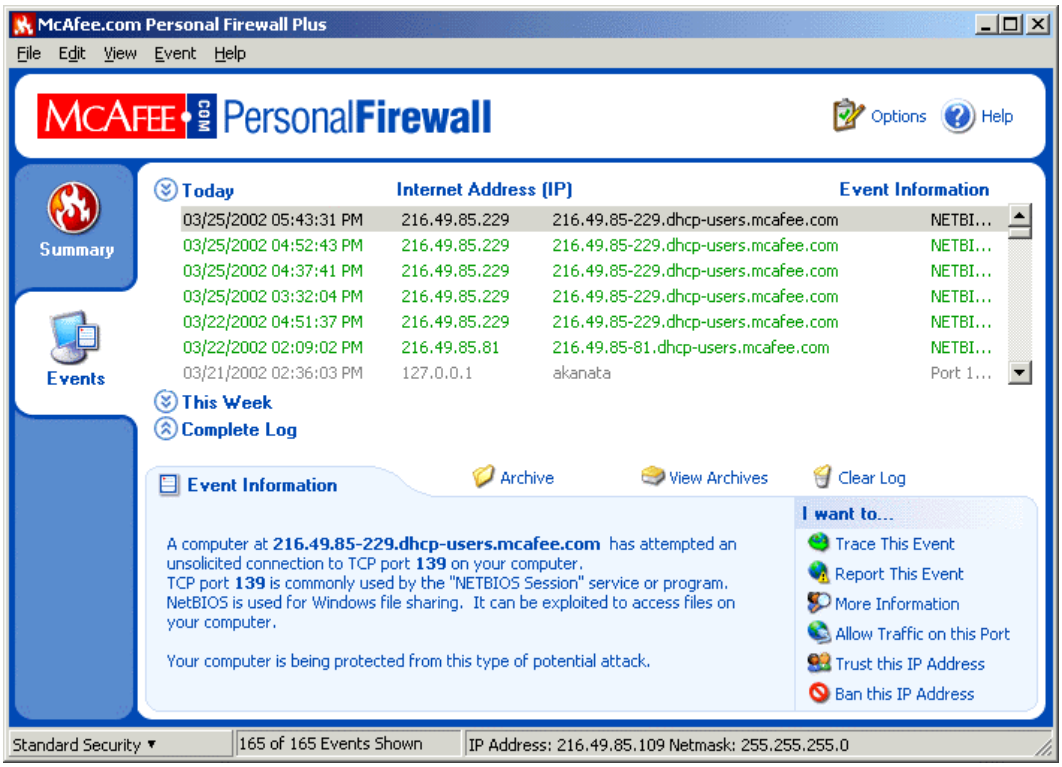
Ενημερώνει τι συμβαίνει στον υπολογιστή σε καθημερινή ή εβδομαδιαία βάση. Καταγράφει την ενδεχομένως εχθρική κυκλοφορία στο Διαδίκτυο και προειδοποιεί με σαφείς δυνατότητες-επιλογές απάντησης για κάθε μια από τις σημειωθείσες προσπάθειες παρείσφρησης.

Το λογισμικό της εταιρίας McAfee πωλείται σε ετήσια βάση συνδρομής, ένα χαρακτηριστικό γνώρισμα που μπορεί να απευθυνθεί σε μερικούς, αλλά δεν υπάρχει έκδοση ελεύθερης δοκιμής. Η ετήσια τιμή συνδρομής εξουσιοδοτεί τους χρήστες στις αυτόματες αναπροσαρμογές και βελτιώσεις. Οι αναπροσαρμογές προϊόντων εμφανίζονται "on-line" μέσω του Διαδικτύου. Επίσης το προσωπικό firewall McAfee.com μπορεί να χρησιμοποιηθεί από κοινού με άλλα προϊόντα McAfee. Παρέχει πλήρη, πολυεπίπεδη ασφάλεια σε PC όταν συνδυάζεται με πρόγραμμα VirusScan Online. Το κόστος του ανέρχεται περίπου στα 29.95$. [10]

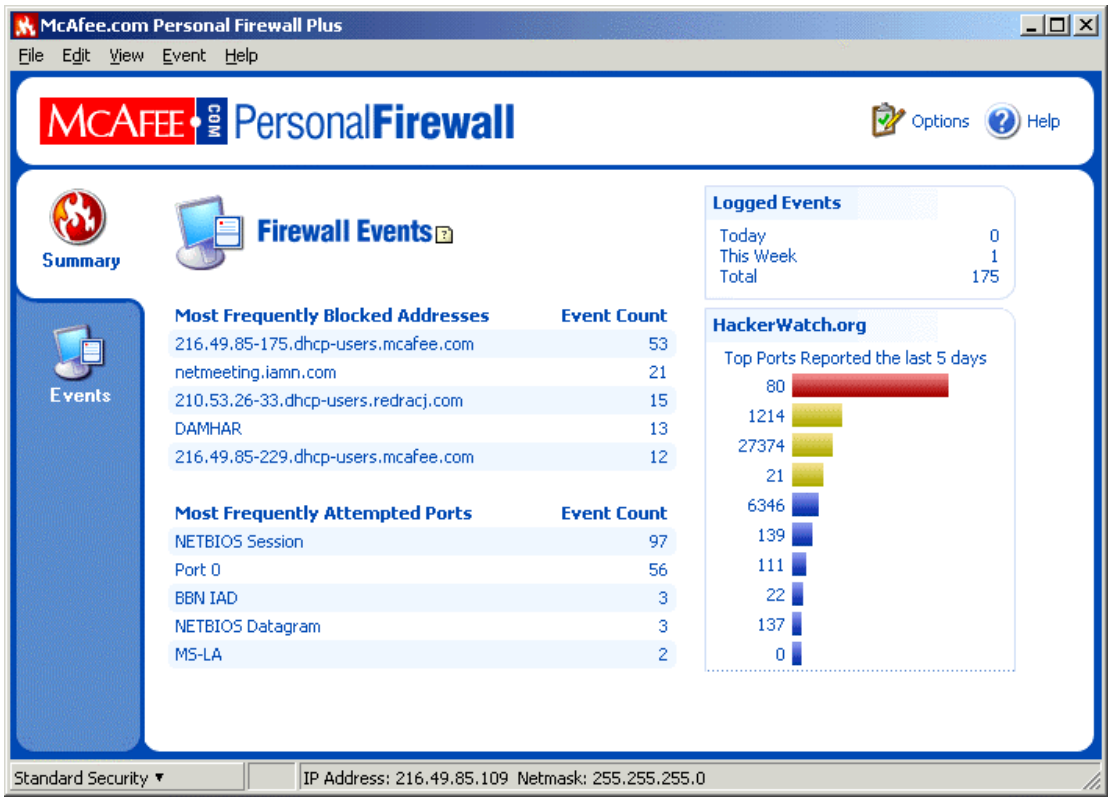


Πλεονεκτήματα:
Εύκολο στην εκμάθηση, παρουσιάζει την δραστηριότητα και υπάρχει στην κεντρική οθόνη ρύθμιση φίλτρων.
Μειονεκτήματα:
Προσανατολισμένο σε XP Windows
Συμπέρασμα: Χαμηλό κόστος με ικανοποιητική προστασία

McAfee Firewall-Events



McAfee Firewall Results Summary



4.4 Tiny Personal Firewall (TPF) 2.0

Μια συγκριτικά νέα συσκευασία (διατίθεται δωρεάν για προσωπική χρήση και $39 για επαγγελματική), με ιδιαίτερο χαρακτηριστικό τη χαμηλή χρήση μνήμης στα εγκατεστημένα συστήματα. Είναι έξυπνη τεχνολογία προσωπικής ασφάλειας, εύκολη στη χρησιμοποίηση που προστατεύει πλήρως τα PC από τους χάκερς. Περιέχει επίσης ένα ενδιαφέρον χαρακτηριστικό γνώρισμα βασισμένο στον χρόνο-, όπου τα φίλτρα πακέτων μπορούν να τεθούν να λειτουργήσουν μόνο σε ορισμένους χρόνους της ημέρας. Η Πολεμική Αεροπορία των Η.Π.Α. επέλεξε αυτό το προϊόν ως πρότυπο Firewall για τους υπολογιστές της.

Το πρόγραμμα προστατεύει το PC από μη εξουσιοδοτημένες προσβάσεις ελέγχοντας συνεχώς τις θύρες TCP/IP τις οποίες οι επίδοξοι χάκερς χρησιμοποιούν για να εισέλθουν στο σύστημα. Στη συνέχεια παρέχεται η δυνατότητα στον χρήστη του συστήματος να επιτρέψει ή απαγορεύσει την δημιουργία σύνδεσης είτε την ίδια χρονική στιγμή είτε σε μελλοντική επανεμφάνιση.

Περιλαμβάνεται μια εφαρμογή φίλτρου (application filter) για την προστασία από Trojan horse και άλλες μη εξουσιοδοτημένες εφαρμογές. Το πρόγραμμα “wizard” ανιχνεύει πότε ένα πρόγραμμα προσπαθεί να εισβάλει από μία θύρα επικοινωνίας και δημιουργεί ένα φίλτρο με κανόνες βασισμένο σε επιλογές του χρήστη. Για την εξασφάλιση ότι προγράμματα Trojan horse δεν θα θεωρηθούν -κατόπιν μπλόφας- ως εγγυημένες εφαρμογές, το Tiny Personal Firewall προσφέρει την επιλογή ελέγχου για **MD5** -Signature Support- ψηφιακής υπογραφής. Παρέχεται επίσης βάση δεδομένων με γνωστές εφαρμογές που χρησιμοποιούν τις θύρες επικοινωνίας.

Πλεονεκτήματα: Δωρεάν, σταθερή προστασία από εξωτερικές επιθέσεις, εύκολο στην εγκατάσταση και στη χρησιμοποίηση.

Μειονεκτήματα: Δεν υπάρχει online help.

Συμπέρασμα: παρέχει εξαιρετική δωρεάν προστασία σε κάθε χρήστη που σερφάρει στο Ίντερνετ και ευκολία στο «download”. **(8)**

4.5 BlackICE™ PC Protection

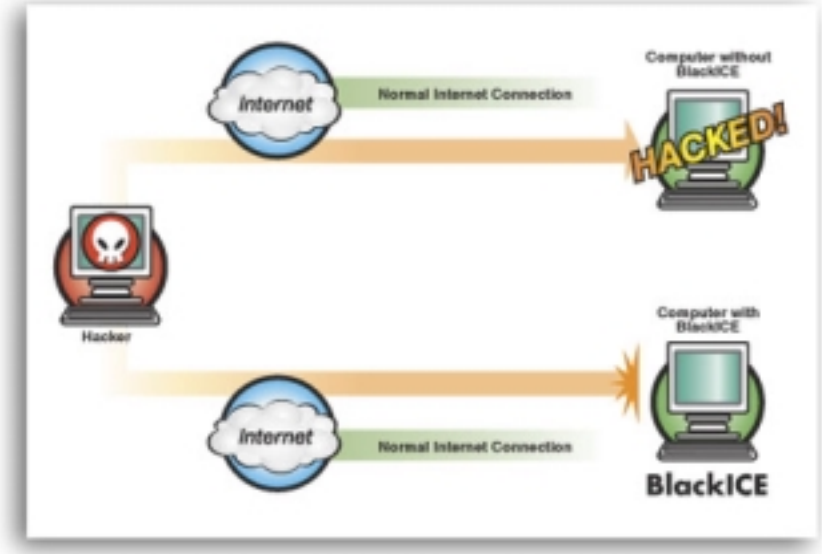
Το γνωστό **BlackICE™ Defender** στην νέα του έκδοση ονομάζεται **BlackICE™ PC Protection**!

Ο υπερασπιστής BlackICE είναι ένα καθιερωμένο προϊόν, με καλό όνομα στην τεχνολογία των firewalls. Το κόστος του (περίπου $40 για τον πρώτο χρόνο και $20 για ετήσια ανανέωση) κρίνεται μάλλον ικανοποιητικό. Δυνατότητα δωρεάν δοκιμής για 30 ημέρες με φόρτωση αντιγράφου από το Web Site.

Ιδιαίτερα αποτελεσματικό για την εισερχόμενη κυκλοφορία, εύκολο στην εγκατάσταση και χρήση, με υψηλής ποιότητας διεπαφή, πολύ καλή ανίχνευση προσπαθειών εισβολής, και ικανοποιητικές αναφορές αποτελεσμάτων, με αναδρόμηση ιχνών για ανακάλυψη των χάκερς. Προσπαθεί από μόνο του να εντοπίσει τις προσπάθειες των hackers, χωρίς να υποβάλλει συχνές ερωτήσεις, που έτσι κι αλλιώς αρκετοί από τους χρήστες του δεν είναι σε θέση να απαντήσουν επιτυχώς. Αντ' αυτού, ο χρήστης θέτει επακριβώς ένα επιθυμητό επίπεδο ασφάλειας, και αφήνει την υπόλοιπη εργασία στο firewall.

Ένα ιδιαίτερο χαρακτηριστικό του υπερασπιστή BlackICE είναι η έμφαση που δίνει όχι μόνο στην αποτροπή των επιθέσεων, αλλά και στην ανίχνευση και καταγραφή πληροφοριών για αυτές. Ενώ μερικά προγράμματα στηρίζονται στην ανάλυση αρχείων ημερολογίου μετά από το γεγονός, για να δημιουργήσουν ένα προφίλ με πληροφορίες της προσβολής, το BlackICE προσπαθεί να ανακαλύψει πληροφορίες ακόμη και για τους επίδοξους hackers, όπως π.χ την IP διεύθυνση τους. **[20]**

Το BlackICE ήταν το πρώτο ευρέως-διαθέσιμο προσωπικό προϊόν firewall και παραμένει μια από τις κορυφαίες επιλογές. Η υψηλής ποιότητας διεπαφή, η ικανότητα καταγραφής, και η υποστήριξή για αυτόματο-φράξιμο κυκλοφορίας από συγκεκριμένες διευθύνσεις δικτύων είναι μεγάλα χαρακτηριστικά γνωρίσματα για τους αρχαρίους και για πιο προχωρημένους networkers επίσης. Οι πελάτες BlackICE λαμβάνουν περιοδικά ελεύθερα τις αναπροσαρμογές στο λογισμικό για (1) έτος μετά από την αγορά. Επίσης αναβαθμίζεται εύκολα μέσω του Internet. **(8)**



Πλεονεκτήματα: Συλλέγει περιεκτικά data των επίδοξων εισβολέων.
Μειονεκτήματα:
Δεν ελέγχει εξερχόμενα δεδομένα ή ύποπτα εισερχόμενα μηνύματα.
Συμπέρασμα: Προϊόν για πιο εξειδικευμένες χρήσεις, όχι το ιδανικότερο για απλούς χρήστες, όπως το ZoneAlarm.

4.6 Sygate® Personal Firewall™ PRO

Το Sygate Personal Firewall, προσφέρει σταθερή προστασία, καταγραφή δραστηριότητας, και αυτόματες ανακοινώσεις ηλεκτρονικού ταχυδρομείου. Παρέχεται δωρεάν για προσωπική χρήση. Προστατεύει ενάντια σε Trojans και άλλες απειλές περιλαμβανομένων και αυτών που χρησιμοποιούν δικούς τους οδηγούς πρωτοκόλλων. Εμποδίζει μη εξουσιοδοτημένες εφαρμογές να περάσουν μέσω αυτού. Παρέχεται η δυνατότητα και σε μη έμπειρους χρήστες να διαμορφώνουν εύκολα και να προσαρμόζουν τις απαιτήσεις ασφάλειας υποστηρίζοντας σχετικά προηγμένες δυνατότητες διαμόρφωσης.

Περιλαμβάνει επίσης ένα χαρακτηριστικό γνώρισμα που επιτρέπει στο χρήστη να οργανώσει διαφορετικούς κανόνες για ορισμένα χρονικά διαστήματα της ημέρας που είτε ισχύουν για όλη την κυκλοφορία είτε για ορισμένα μόνο προγράμματα. Για παράδειγμα οι βασικοί χρήστες που αφήνουν τους υπολογιστές τους ανοικτούς ενώ απουσιάζουν από την εργασία τους, μπορούν μ' αυτόν τον τρόπο να τους εξασφαλίσουν.

Επίσης ενσωματώνει μερικά στοιχειώδη εργαλεία για τον εντοπισμό κακόβουλων hackers, ή στοιχεία της συμπεριφοράς τους κατά την προσπάθεια τους να διεισδύσουν στην υπόψη μηχανή. Έτσι ο χρήστης μπορεί να καθορίζει ποιο από τα εργαλεία μπορεί να τους αποτρέψει πραγματικά. **[18]**

Η **PRO έκδοση** περιλαμβάνει εγγυημένη VPN υποστήριξη, απεριόριστο αριθμό κανόνων ασφάλειας, δυνατότητα να εισαγάγει/εξάγει τις τιμές των παραμέτρων σε πολλαπλάσιους υπολογιστές, και δωρεάν βελτιώσεις για επιπλέον ένα έτος. Παρέχει πολυεπίπεδη προστασία γύρω από το σύστημα που εξασφαλίζει ακεραιότητα δεδομένων και αξιόπιστη ασφάλεια. Το κόστος αγγίζει τα $30. Περιλαμβάνει ανίχνευση θυρών για να ελέγξει τους "σε-αναζήτηση" hackers, καθώς και δυναμικό "φράξιμο" θυρών, για να μπλοκάρει αυτές που είναι ανοικτές όταν οι εφαρμογές που τις χρησιμοποιούν είναι ανενεργές. Οι πολιτικές ασφάλειας μπορούν επίσης να προσαρμοστούν από τη θύρα (port).

Το Sygate Personal Firewall PRO τερματίζει αυτόματα επιθέσεις γνωστών κακόβουλων προγραμμάτων όπως Trojans, Denial of Service (DoS) Zombies. Επίσης διαθέτει μηχανισμούς άμυνας που εμποδίζουν βλαβερούς κώδικες/ και ή χρήστες που προσπαθούν να ακυρώσουν την λειτουργία ή να παραμερίσουν το personal firewall.

Χαρακτηριστικά Sygate Personal Firewall and Pro Edition

Sygate Personal Firewall	Sygate Personal Firewall PRO	Benefits
Basic Security Features (SPF and SPF PRO)		
Multi-Layered Firewall Engine	Multi-Layered Firewall Engine	Provides easy to use application control protection and the power of a flexible rule-based firewall engine
Backtrace/WHOIS Feature	Backtrace/WHOIS Feature	Feature allows you to lookup and identify suspicious traffic and unauthorized attempts to communicate to your computer.
Customizable Packet Level Log	Customizable Packet Level Log	Reports incoming and outgoing packet level traffic.
Configurable Email Security Alerts	Configurable Email Security Alerts	Feature allows you to remotely monitor security events based on time intervals you specify.
Advanced Security Features (SPF PRO only)		
N/A	Intrusion Prevention System & Online Updates	Provides updated protection against known Trojans, Worms, and malicious code.
	Full ICS Support	Supports Internet Connection Sharing for Windows 98/ME/2000/XP operating systems.
	VPN Support	For business and remote users, SPF PRO supports compatibility with numerous VPN vendors.
	Protocol Driver Level Protection	Prevents malicious applications from using their own protocol adapter to bypass outbound application firewalling.
	Stealth Browsing	Stealths & prevents your browser from revealing OS and browser information.
	Multi-User Pack	Simplifies the deployment and installation of SPF PRO on multiple computers.
	Advanced Trojan Protection	Automatically terminates all known Trojan horse programs before the Trojan attempts to communicate.
	Protocol Driver Level Protection	Prevents malicious applications from using their own protocol adapter to bypass outbound application firewalling.
	ICSA Certification	Security certification that distinguishes this product from other personal firewall products.

5. Συγκρίσεις Χαρακτηριστικών Personal Firewalls

(http://www.cnet.com/software/)

Η δοκιμή προϊόντων ξεκινά με το IP Agent, ένα δωρεάν πρόγραμμα της ***ShieldsUp,*** το οποίο προσδιορίζει την τρέχουσα IP address του προς εξέταση υπολογιστή και στη συνέχεια γίνεται σύνδεση με το ***ShieldsUp Web site*** για την έναρξη του διαγνωστικού. Στη συνέχεια το Port Probe utility εξετάζει την άμυνα του συστήματος ενάντια σε ανιχνευτές Internet port. Οι διάφορες θύρες που εξετάζονται είναι:

Port 21-FTP
Port 23-Telnet
Port 25-SMTP
Port 79-Finger
Port 80-HTTP
Port 110-POP3
Port 113-IDENT
Port 130-NetBIOS
Port 143-IMAP
Port 443-HTTPS

Κάθε θύρα δίνει ένα από τα παρακάτω αποτελέσματα.
Stealth (Μυστικότητα): Το αποτέλεσμα δείχνει ότι το διαγνωστικό πρόγραμμα «probe» δεν μπόρεσε να εντοπίσει την συγκεκριμένη θύρα στον υπολογιστή. Αυτό το αποτέλεσμα πιστοποιεί ότι η ασφάλεια σε αυτή την θύρα είναι εξασφαλισμένη.

Closed (Κλειστό σύστημα): Το αποτέλεσμα δείχνει ότι το διαγνωστικό πρόγραμμα probe ήταν σε θέση να προσδιορίσει την συγκεκριμένη θύρα αλλά δεν επιτεύχθηκε σύνδεση.

Open (Ανοικτό σύστημα: Η θύρα δηλώνει ανοικτά την παρουσία της στο Ίντερνετ. Οι ανιχνευτές θυρών δεν θα αντιμετωπίσουν πρόβλημα στον εντοπισμό της θύρας.

1ος Συγκριτικός Πίνακας

Product	Incoming protection	Outgoing protection	E-mail protection	Blocks specific IP addresses	Security logs
ZoneAlarm 2.6	Yes	Yes	Yes	No	Yes
Norton Personal Firewall 2002	Yes	Yes	No	No	Yes
McAfee Firewall 3.0	Yes	Yes	No	Yes	Yes
Tiny Personal Firewall 2.0.14	Yes	Yes	No	No	Yes
BlackIce Protection 2.5	Yes	No	No	Yes	Yes

2ος Συγκριτικός Πίνακας

Manufacturer	Zone Labs	Symantec	McAfee	Tiny Software	Network Ice	Sybergen Networks
Product:	**Zone Alarm**	**Norton Personal Firewall**	**Firewall 3.0**	**Tiny Personal Firewall**	**Black Ice Protection**	**Sygate Personal Firewall**
FEATURES						
MD5 Signature Support	**YES**	**NO**	**NO**	**YES**	**NO**	**NO**
Trusted Applications	**YES**	**YES**	**YES**	**YES**	**NO**	**YES**
Trusted Address Groups	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**
Intrusion Detection	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**
Remote Administration	**NO**	**NO**	**NO**	**YES**	**NO****	**NO**
Time Intervals	**NO**	**NO**	**NO**	**YES**	**NO**	**NO**
Login Authentication	**YES**	**NO**	**YES**	**YES**	**NO**	**YES**
Runs as Service	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**
File Size (Before Installation)	**1,920 KB**	**43,377 KB**	**7,650 KB**	**1324 KB**	**2,910 KB**	**2,690 KB**
Supported Operating Systems	95, 98, NT, 2k, ME	95, 98, NT, 2K	95, 98, NT	95, 98, NT, 2k, ME	95, 98, NT, 2K	95, 98, NT, 2k, ME
Prices	Free*	$ 29.95	$ 39.95	Free*	$ 39.95	Free*

ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] Network Security-Internet security and the evolution of apps-
by Margaret Grayson

[2] Το Δίκτυο των παρανόμων
http://www.enet.gr/online/online_p1_obj.jsp?pid=25&tp=T&id=68725

[3] Για μια ασφαλέστερη Κοινωνία της Πληροφορίας
http://www.enet.gr/online/online_p1_obj.jsp?pid=25&tp=T&id=68727

[4] Εισαγωγή Στις Υπηρεσίες Δικτύου Δεδομένων-
Επιτροπή Δικτύου Δεδομένων ΑΠΘ- Θεσσαλονίκη 2000

[5] 3com: Network Security: A Simple Guide toFirewalls
http://www.3com.com/

[6] Παιδαγωγικό Ινστιτούτο
http://www.pi-schools.gr/greek/epps/but3-informatics.htm

[7] Ασφάλεια στον Κυβερνοχώρο: Πρακτικά Διημερίδας Γενικού Επιτελείου Στρατού -Δεκ. 2001
http://www.army.gr/

[8] Στοιχεία για Personal Firewalls
http://compnetworking.about.com/library/reviews/aatp-firewalls_personal.htm

[9] White papers: Telecommunications, Wireless Communications, Network management, Network technologies, Internet, Security, Hardware, Software, IT management.
http://www.itpapers.com/

[10] Πληροφορίες για PERSONAL FIREWALLS
http://www.monitor.ca/monitor/issues/vol8iss3/feature4.html

[11] Technology guides. Αναλύονται θέματα σχετικά με το Internet, Enterprise solutions, Network management, Networking technology, Security, Software applications, Telecommunications. Επίσης περιέχονται πρόσφατα άρθρα επάνω στις σύγχρονες τεχνολογίες επικοινωνιών και δικτύων και μηχανή αναζήτησης.
http://www.techguide.com/

[12] Networkmagazine.com. Τα πάντα για τα δίκτυα, λογισμικό, εξοπλισμό, πρωτόκολλα. TechEncyclopedia, Techlibrary, ενημέρωση για προϊόντα, για ασφάλεια δικτύων.
http://www.networkmagazine.com/static/tutorial/index.html

[13] Webopedia: Links on Data Transfer Rates, Directory Services, Electronic Mail, Ethernet, File Transfer, Groupware, Internet Access, Network Interface Cards (NICs), Network Management, Network Protocols, Network Topologies, Networking Companies, Networking Hardware, Networking Standards, Security.
http://webopedia.internet.com/Networks/

[14] Personal Firewalls
http://seattletimes.nwsource.com/html/businesstechnology/

[15] Ασφάλεια Υπολογιστών: Περιέχει links σε ιστοσελίδες με θέματα σχετικά με Firewalls, Security Policy, Monitoring Tools, Anti-Virus κλπ.
http://www.securitypointer.com

[16] McAfee Co.
http://www.mcafee.com

[17] Symantec Co.
http://www.symantec.com

[18] Sygate Co.
http://www.sygate.com

[20] Άρθρο για Symantec Norton Personal Firewall 2002
http://networknews.vnunet.com/Products/Software/1131081

[21] BlackICE PC Protection 3.5
http://www.iss.net