Εργασία

Πληροφοριακά Συστήματα για Μάρκετινγκ & Δημοσκοπήσεις

Personal Firewalls Comparison

-McAfee Firewall 2.1.3

-TermiNET 1.76.13

-Tiny Personal Firewall 2.0.13

-BlackIce Defender 2.1

-ZoneAlarm 2.6

-Sygate Personal Firewall v4

Firewall-like Products Comparison

-WinRoute Pro 4.1Build 24

-MailControl 1.0

-Socks2HTTP 0.74

Μουρατίδης Ευστράτιος

Αρ.Μητρ.: M11/00

Θεσσαλονίκη 17 Μαΐου 2001

Περιεχόμενα

Περίληψη

Η εργασία αυτή αποτελεί μια προσπάθεια να αξιολογηθούν τα κυριότερα και ευρέως χρησιμοποιούμενα προσωπικά firewalls. Στην αρχή δίδονται κάποια εισαγωγικά στοιχεία για τα firewalls, όπως οι λειτουργίες που εκτελούν, οι διαφορετικές στρατηγικές που μπορούν να ακολουθηθούν για την οργάνωσή τους, οι διαφορετικοί τύποι που υπάρχουν, καθώς και οι αρχιτεκτονικές διάρθρωσής τους. Αμέσως μετά αναφέρονται τα κριτήρια με τα οποία έγινε η σύγκριση (Security Effectiveness, Scanning Effectiveness, Effectiveness of reaction, User Interface, Price) και ο τρόπος που έγινε η αξιολόγηση. Ακολουθεί αναλυτική παρουσίαση κάθε προϊόντος, η οποία περιέχει και τα πλεονεκτήματα και μειονεκτήματα καθενός από αυτά. Τα συμπεράσματα της αξιολόγησης τοποθετήθηκαν σε συγκριτικό πίνακα. Τα firewalls που εξετάστηκαν είναι: McAfee Firewall 2.1.3, TermiNET, Tiny Personal Firewall, BlackIce Defender, ZoneAlarm και Sygate. Στο τελευταίο μέρος αναλύονται οι δυνατότητες προϊόντων που δεν αποτελούν firewalls, αλλά έχουν κάποιες firewall ικανότητες όπως το MailControl 1.0, toWinRoute Pro 4.1 Build 24 και το SOCKS2HTTP 0.73 Beta.

Abstract

This paper is an effort to evaluate the main and most commonly used personal firewalls. In the beginning some introductive elements about firewalls are given, like the functions they execute, the different strategies that can be used for their organization, the different types of firewalls that exist, and their architectional structures. Afterwards, the comparison criteria are reported (Security Effectiveness, Scanning Effectiveness, Effectiveness of Reaction, User Interface, Price), together with the way the evaluation was conducted. After that follows an analytical presentation of every product, which contains the advantages and disadvantages of each one. The conclusions of the evaluation were placed in a comparative table. The examined firewalls are : McAfee Firewall 2.1.3, TermiNET, Tiny Personal Firewall, BlackIce Defender, ZoneAlarm and Sygate. The last part analyses the abilities of products that are not firewalls, but have firewall capabilities. Those products are MailControl 1.0, WinRoute Pro 4.1 Build 24 and SOCKS2HTTP 0.73 Beta.

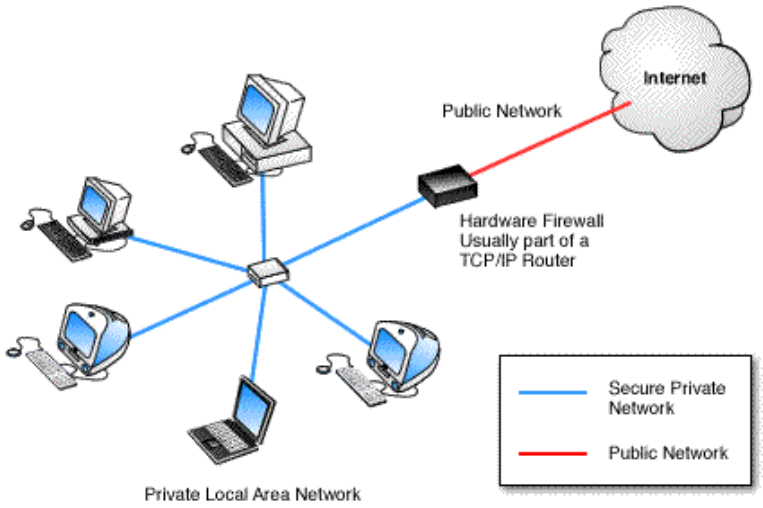
1. ΓΕΝΙΚΑ [1]

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. ΕΙΣΑΓΩΓΙΚΑ

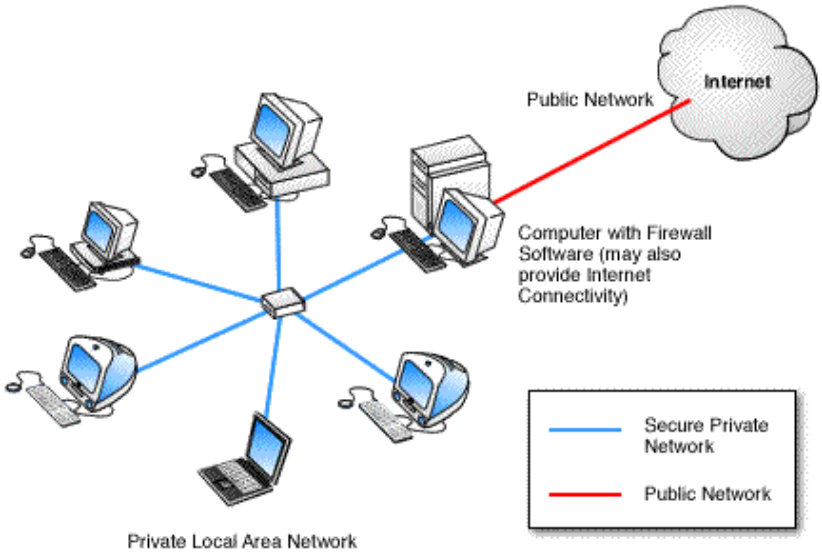
Ένα Firewall προστατεύει τους δικτυωμένους υπολογιστές από την σκόπιμη εχθρική διείσδυση που θα μπορούσε να οδηγήσει σε συμβιβασμούς στην εμπιστευτικότητα (confidentiality) ή σε καταστροφή δεδομένων ή και σε άρνηση της υπηρεσίας (Denial of Service-DoS). Μπορεί να είναι μια συσκευή υλικού (σχήμα 1) ή 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.



Σχήμα 2

2.1 Λειτουργίες ενός Firewall

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 βασιζόμενα

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.

Ένα Firewall δεν μπορεί να αποτρέψει τους μεμονωμένους χρήστες με modem να καλέσουν μέσα ή έξω από το δίκτυο (κάνοντας dial-up), παρακάμπτοντας το firewall. Η κακή μεταχείριση ή η απροσεξία υπαλλήλων δεν μπορεί να ελεγχθεί από τα firewalls. Οι πολιτικές (policies) που περιλαμβάνουν τη χρησιμοποίηση και την κακή χρήση των passwords και των λογαριασμών χρηστών πρέπει να είναι αυστηρές. Αυτά είναι διοικητικά ζητήματα που πρέπει να προκύψουν κατά τη διάρκεια του προγραμματισμού οποιασδήποτε πολιτικής ασφαλείας αλλά που δεν μπορούν να λυθούν με τα firewalls.

2.2 Στρατηγικές για την οργάνωση ενός Firewall [ΠΟ]

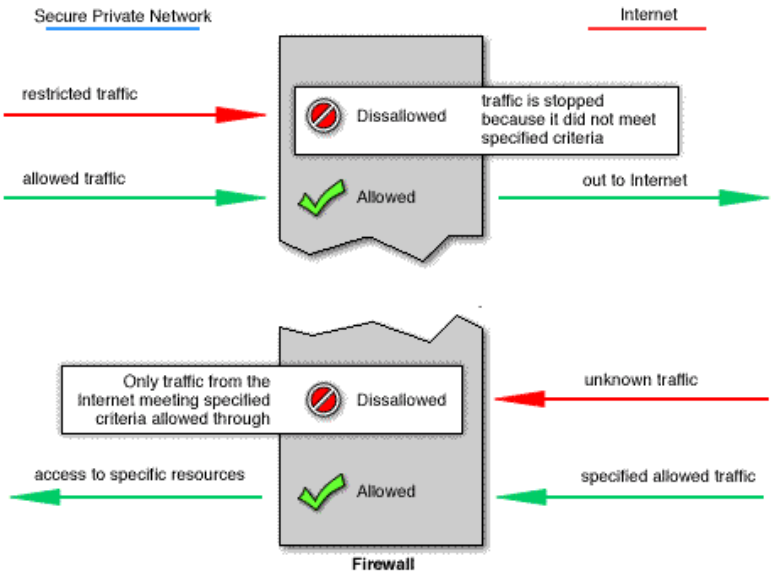
Υπάρχουν δύο μεθοδολογίες απαγόρευσης πρόσβασης από τα firewalls.

-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.



2.3 Διάφοροι τύποι Firewalls [1]

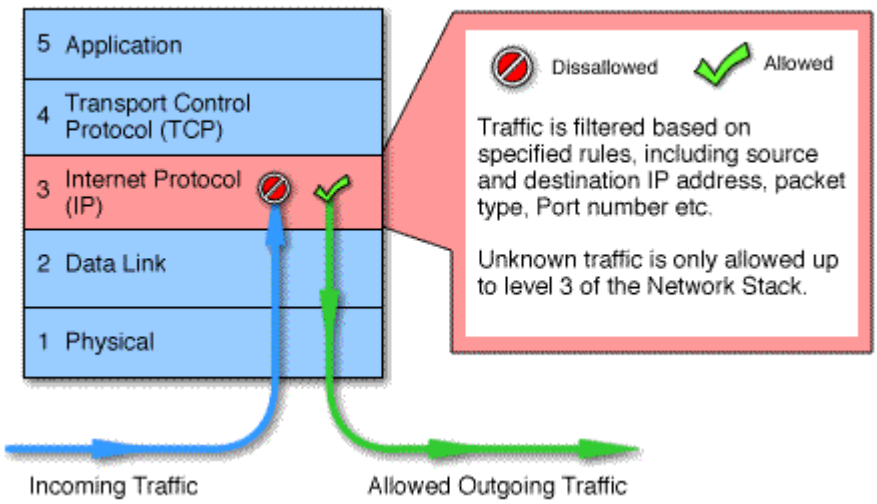
Τα διάφορα firewalls λειτουργούν σε διαφορετικά επίπεδα του OSI μοντέλου χρησιμοποιώντας διαφορετικά κριτήρια για τον έλεγχο της κυκλοφορίας. Το χαμηλότερο επίπεδο στο οποίο ένα firewall μπορεί να λειτουργήσει είναι το 3ο επίπεδο δηλ. το επίπεδο δικτύου στο μοντέλο OSI ή το επίπεδο του Internet Protocol 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

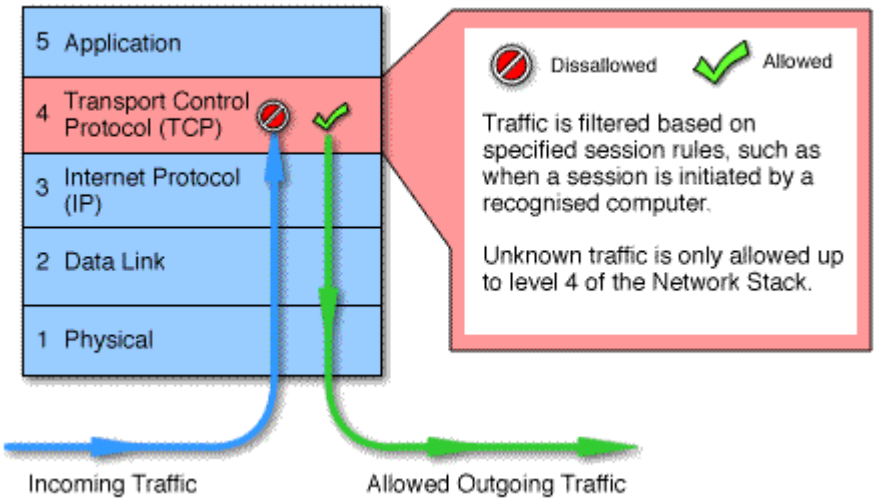
κριτήρια, το Firewall μπορεί να απορρίψει το πακέτο, να το διαβιβάσει ή να στείλει ένα μήνυμα στο δημιουργό του. Οι κανόνες μπορούν να συμπεριλάβουν την διεύθυνση της πηγής (source address) και διεύθυνση προορισμού IP (destination IP address), το port πηγής και προορισμού και το χρησιμοποιούμενο πρωτόκολλο. 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

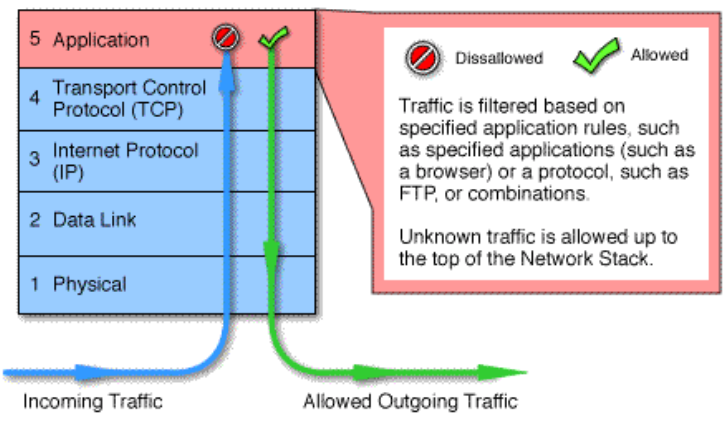
Οι πύλες επιπέδου κυκλώματος (circuit level gateways) λειτουργούν στο επίπεδο συνόδου (session layer) του προτύπου OSI, ή το επίπεδο TCP του TCP/ IP. Ελέγχουν το TCP handshaking[1] μεταξύ των πακέτων για να καθορίσουν εάν μια ζητούμενη σύνοδος είναι νόμιμη. Οι πληροφορίες που περνούν στον απομακρυσμένο 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.

[1] Αρχική ανταλλαγή δεδομένων του TCP πρωτοκόλλου για την επίτευξη της σύνδεσης

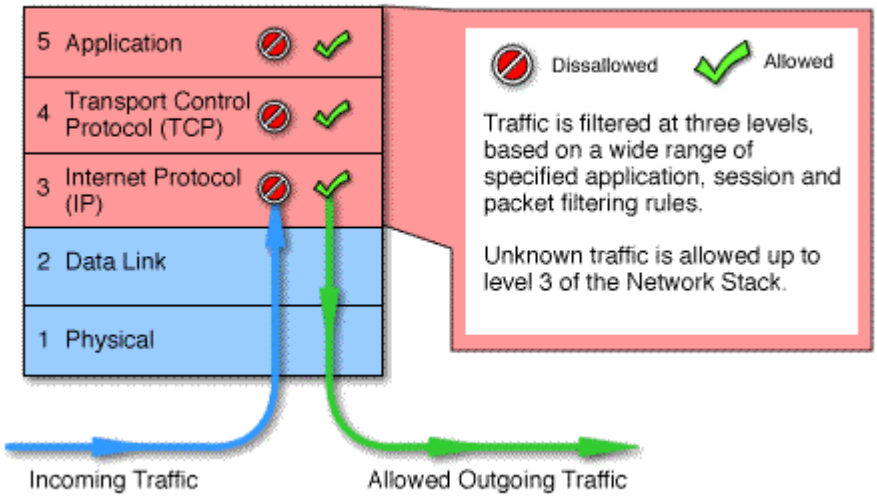


Σχήμα: Circuit Level Gateway

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.

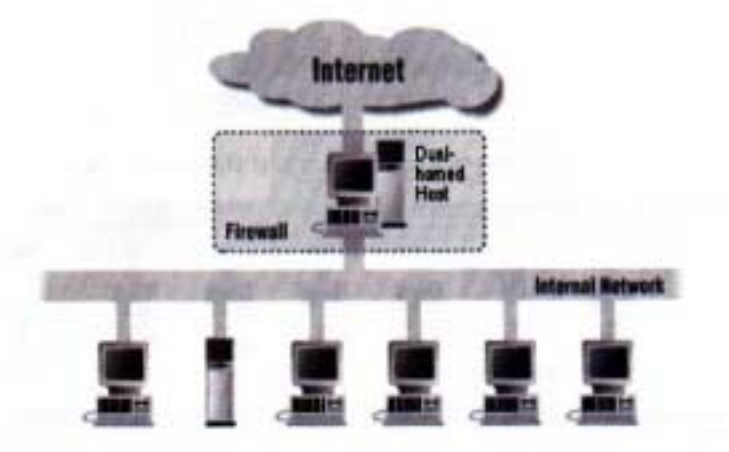


Σχήμα: Stateful Multilayer Inspection Firewall

2.4 Αρχιτεκτονικές Διάρθρωσης [RAM]

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.



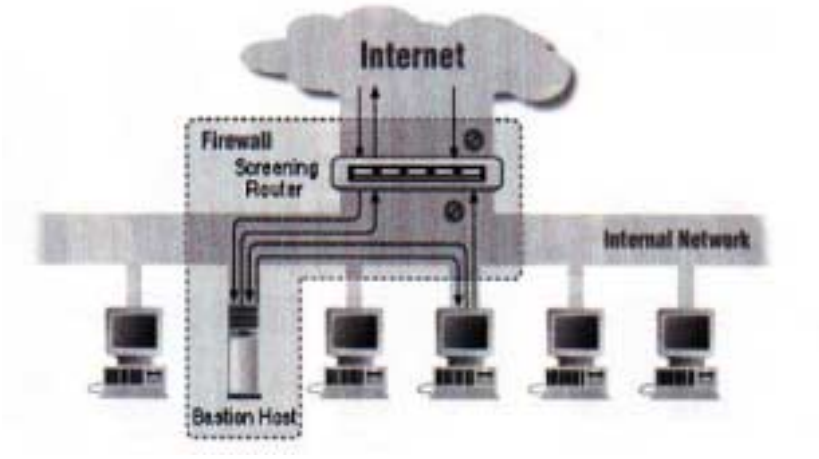
Αρχιτεκτονική Dual Homed

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 τον κεντρικό υπολογιστή. 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 screen-host, 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.

3. ΚΡΙΤΗΡΙΑ ΣΥΓΚΡΙΣΗΣ FIREWALLS

Για την σύγκριση των firewalls χρησιμοποιήθηκαν τα κριτήρια που καθορίζονται στην διεύθυνση http://www.securityportal.com/articles/pf_main20001023.html. Έτσι συγκρίνονται τα ποιο γνωστά προσωπικά firewalls και στην συνέχεια παρουσιάζονται τα χαρακτηριστικά τους σε ένα συγκεντρωτικό πίνακα. Τα κριτήρια 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

3.1 ΤΡΟΠΟΙ ΕΛΕΓΧΟΥ ΤΩΝ FIREWALLS

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

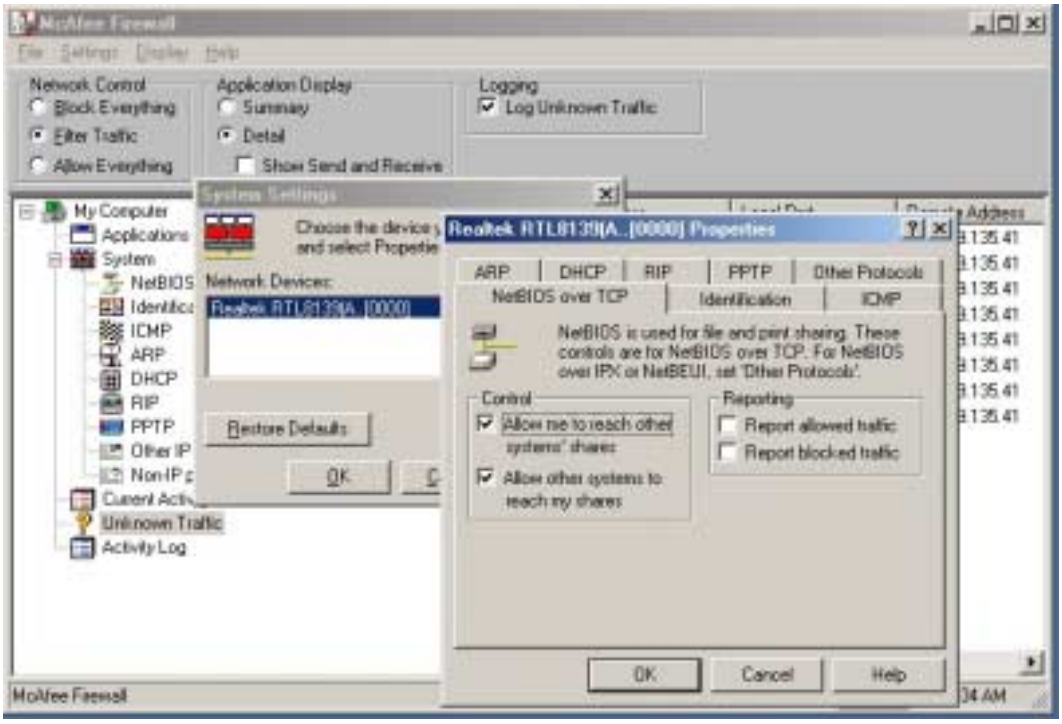
Β)Εγκατάσταση ενός ισχυρού "remote-control" Trojan (Netbus Pro v2.1) [2] στο σύστημα σε ένα nonstandard port (για να γίνει η ανίχνευση πιο δύσκολη) και προσπάθεια του Netbus server να συνδεθεί από ενα remote system.

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

Δ) Σκανάρισμα κάθε firewall χρησιμοποιώντας το εργαλείο nmap [3] για να ελεγχθούν ποια ports μπλοκαρίστηκαν από τα firewalls αποτελεσματικά.

4. ΑΝΑΛΥΤΙΚΗ ΠΑΡΟΥΣΙΑΣΗ FIREWALLS

4.1.1 McAfee Firewall 2.1.3



Το McAfee Firewall βασίζεται στο Conseal Signal-9 Private Desktop [4]. Σύμφωνα με το REAME 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 συσκευή. 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:\PROGRAM FILES\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.Απενγκατάσταση: ο Network Driver δεν διαγράφεται αλλά πρέπει να αφαιρεθεί με το χέρι.

3.The 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 μόλις αυτός συνηθίσει τις ιδιορρυθμίες του GUI. Αυτό το προϊόν έχει την ικανότητα να προστατεύει το PC αρκετά καλά (όχι όμως ικανοποιητικά), και να καταστήσει τη διείσδυση δύσκολη, αλλά απαιτείται προσεκτική διαμόρφωση. Οι ικανότητες ανίχνευσης παρείσφρησης είναι βασικές. Οι χρήστες lap-top δεν θα είναι ευχαριστημένοι γιατί δεν θα λειτουργούν τα power-saving modes.

4.1.2 TermiNET 1.76.13

Το Terminet, από την εταιρία DANU Industries [5], 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

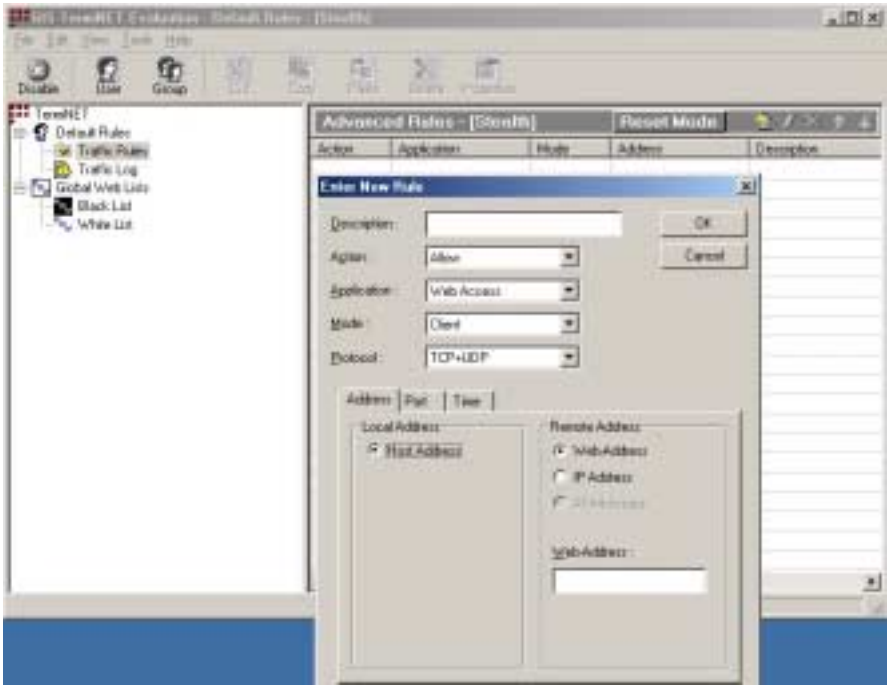
Μοντέλο Ασφαλείας

-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 (βλ. επόμενη εικόνα) 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"

A. Ping & shares tests.

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

B. 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.

4.1.3 Tiny Personal Firewall 2.0.13

Σημειώνω ένα απόσπασμα από το website Tiny Personal Firewall [6]:

«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 Desktop

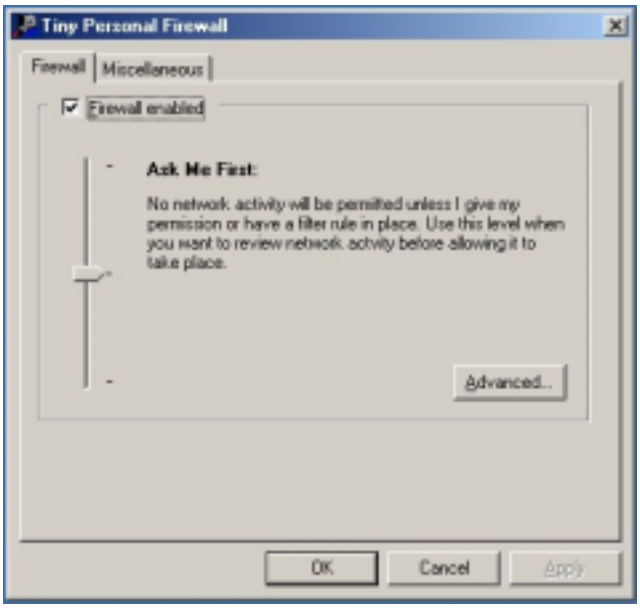
Security (CMDS) System στο οποίο ανατέθηκε μια σύμβαση από την Πολεμική Αεροπορία των Η.Π.Α. για να καλυφθούν περίπου 500.000 υπολογιστές»

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

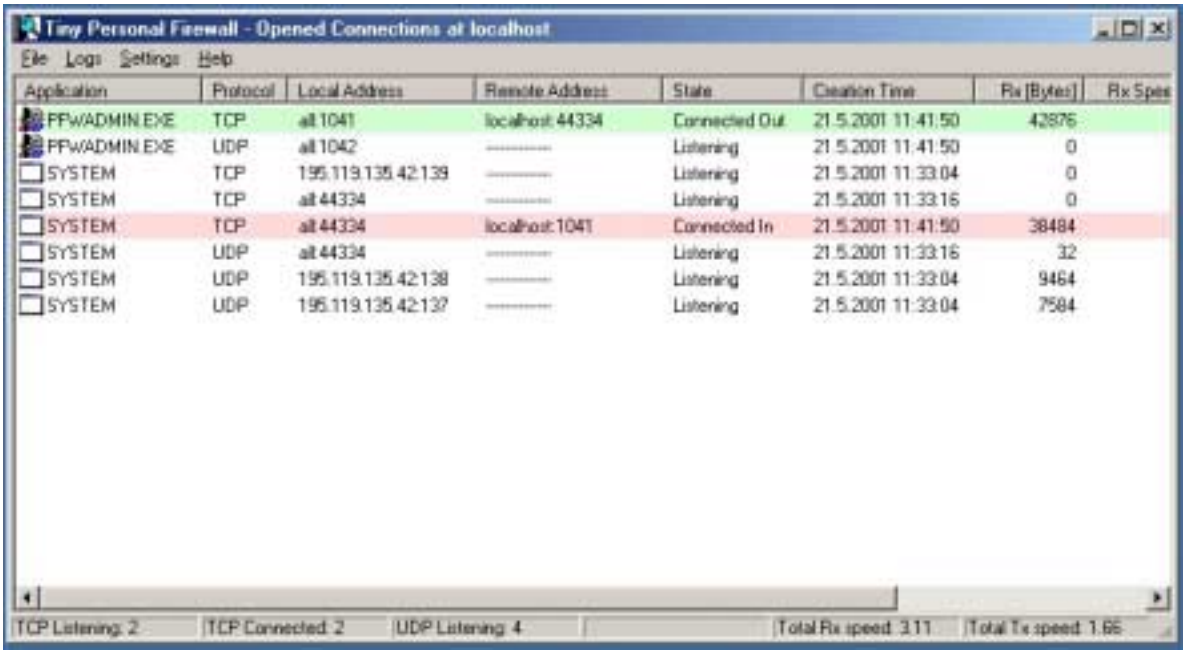
-Η διαμόρφωση και η ανάγνωση του log μπορεί να προστατεύεται με password. Εάν η προστασία με password είναι ενεργοποιημένη, η απομακρυσμένη πρόσβαση (remote access) στην διαμόρφωση (configuration) και/ή στα logs μπορεί να ενεργοποιηθεί.
-Η απομακρυσμένη πρόσβαση στα logs και η διοίκηση από απόσταση (remote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



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.

4.1.4 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

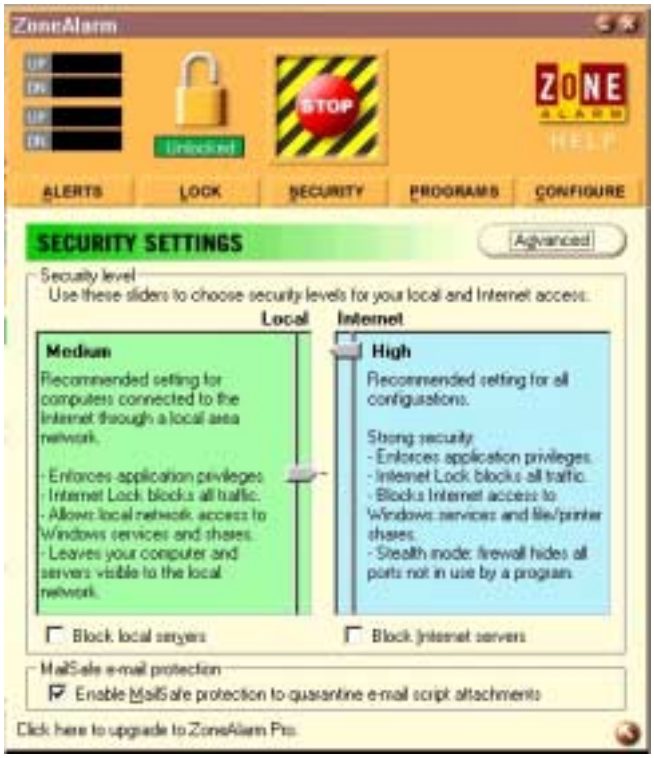
Σύνοψη

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.

4.1.5 ZoneAlarm 2.6 [7]

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

4.1.6 Sygate Personal Firewall v4 [8]

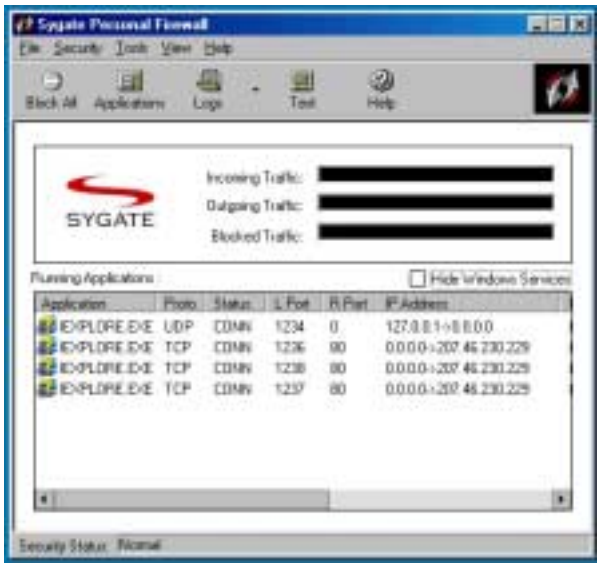
Σύμφωνα με το website του Sygate Personal Firewall:

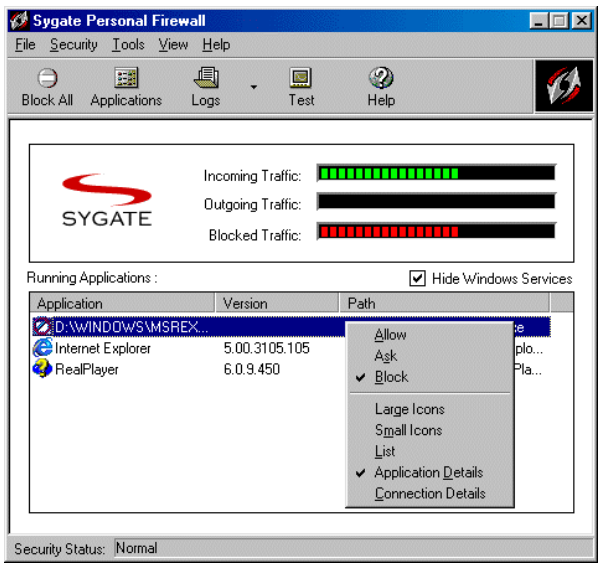
«Το Firewall Sygate προστατεύει βασισμένους στα windows προσωπικούς υπολογιστές και servers με πέντε εξειδικευμένες ρυθμίσεις επιπέδου-προστασίας που παρέχουν πολλαπλά στρώματα ασφάλειας στον συνδεδεμένο υπολογιστή. Το firewall Sygate επιτρέπει ή αρνείται κάθε εισερχόμενο ή εξερχόμενο πακέτο διαδικτύου 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:

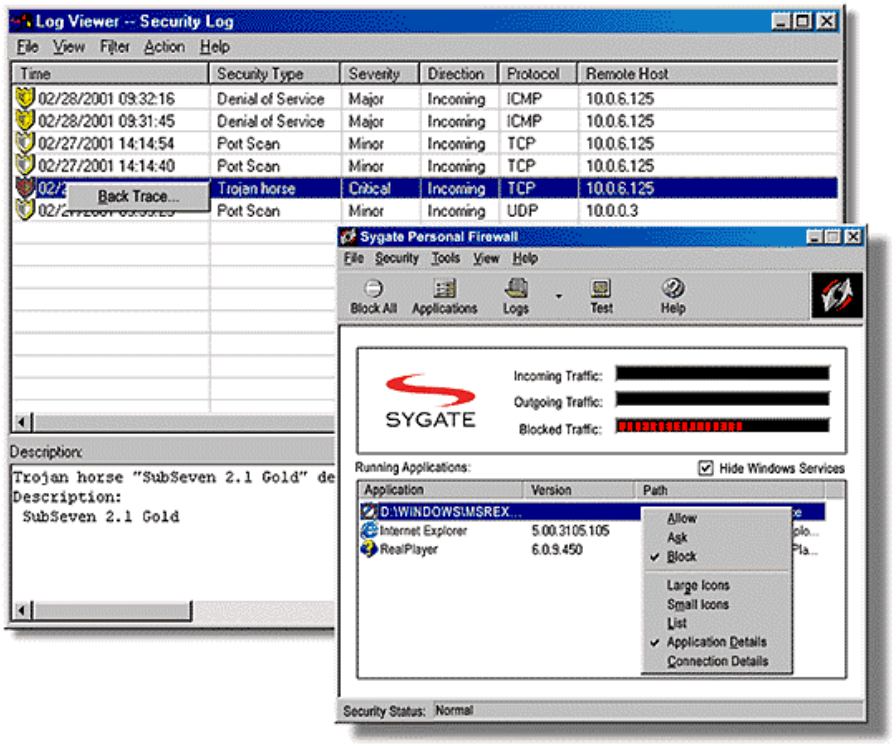
- Διαρρέουσα εξερχόμενη πληροφορία πάνω από standard ports: όλα τα πρωτόκολλα θα παραμείνουν μπλοκαρισμένα μέχρι ο χρήστης να εγκρίνει να χρησιμοποιήσουν οι εφαρμογές τα ports.
- Μεταμφίεση ως «έμπιστο» ή standard πρόγραμμα: η αντικατάσταση ενός εμπιστευμένου προγράμματος από Trojan ανιχνεύθηκε από το 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	
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

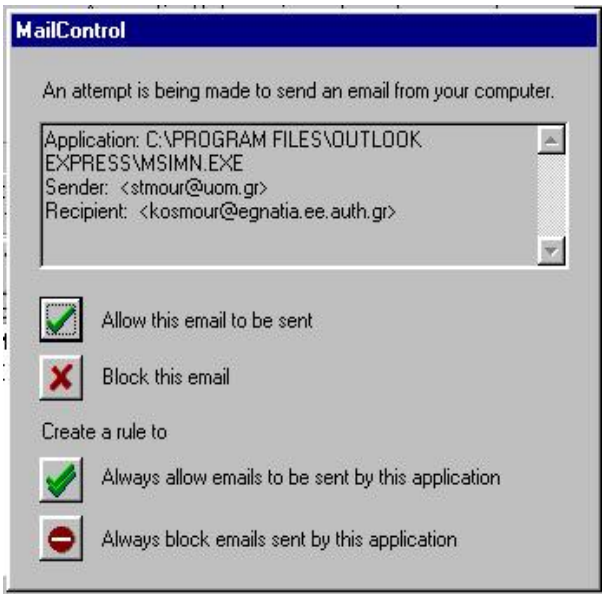
Η έκδοση 4 του Sygate Firewall αποτελεί μια πολύ καλή λύση. Από πάρα πολλούς χρήστες θεωρείται κορυφαία επιλογή.

4.2 Συμπερασματικός πίνακας

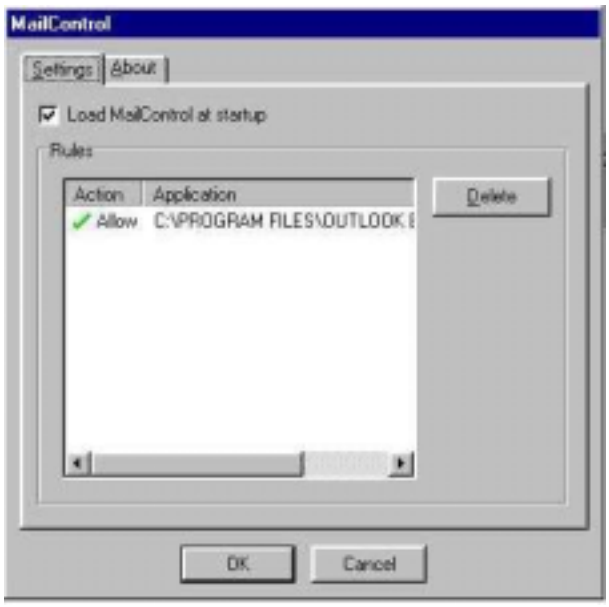
Κριτήριο	McAfee 2.1.3	TermiNET	Tiny 2.0.13	BlackIce	ZoneAlarm	Sygate v4
	Βαθμολογία					
Effectiveness of security protection (Αποτελεσματικότητα της παρεχόμενης προστασίας)	6	8	8	8	8	9
Αποτελεσματικότητα στην ανίχνευση παρείσφρυσης (Effectiveness of intrusion detection)	6	7	8	8	8	10
Αποτελεσματικότητα 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

5. Firewall-like Προιόντα

5.1 MailControl 1.0[9]



Σχήμα1



Σχήμα 2

Σύμφωνα με την διεύθυνση http://www.wincomplete.com/download/?id=755 στην οποία διατίθεται για download, το MailControl είναι ένα προσωπικό firewall ηλεκτρονικού ταχυδρομείου. Ελέγχει συνεχώς τι στέλνεται από τον υπολογιστή στο δίκτυο, αποτρέποντας αναρμόδιες εφαρμογές από την αποστολή e-mail εξ ονόματός του χρήστη. Όποτε μια εφαρμογή προσπαθεί να στείλει ένα e-mail, το MailControl ενεργοποιεί ένα μήνυμα προειδοποίησης (σχήμα 1), ρωτώντας πώς να προχωρήσει. Ο χρήστης μπορεί έπειτα να εμποδίσει το e-mail, να το επιτρέψει, ή να δημιουργήσει έναν κανόνα που να αφορά την συγκεκριμένη εφαρμογή, για να εξασφαλίσει ότι οι μελλοντικές προσπάθειες θα υποβάλλονται σε ανάλογη επεξεργασία αυτόματα. Πατώντας το εικονίδιο της γραμμής εργασιών εμφανίζεται το 2^{ο} σχήμα στο οποίο μπορούν να τροποποιηθούν οι κανόνες που εφαρμόζονται σε κάθε εφαρμογή που έχει πρόσβαση στο δίκτυο. Ο τρόπος λειτουργίας του μάλλον βασίζεται στον έλεγχο του port 25 που χρησιμοποιείται από διακομιστές αλληλογραφίας.

Στην πράξη το MailControl δεν είναι τόσο αποτελεσματικό. Μπορεί να μπλοκάρει μόνο ένα mail κάθε φορά. Αν ο χρήστης έχει αποθηκευμένα στα εξερχόμενα 2 και παραπάνω μηνύματα τότε στην προσπάθεια για αποστολή θα εμφανιστεί το σχήμα 1. Στο σημείο αυτό αν ο χρήστης επιλέξει allow ή block για το mail, αυτό θα ισχύσει μόνο για το πρώτο mail για το οποίο θα του επιτραπεί ή αποτραπεί ή έξοδος αντίστοιχα. Όμως τα υπόλοιπα mail που βρίσκονται στα εξερχόμενα θα αποσταλούν όποια και να είναι η παραπάνω επιλογή. Το πρόγραμμα αυτό χρησιμοποιήθηκε για να αντιμετωπίσει τον ιό “Happy New year’99” (ο οποίος σε κάθε mail που στέλνει ο χρήστης του μολυσμένου υπολογιστή, στέλνει ταυτόχρονα και 2^{ο} mail με τον εαυτό του στην ίδια διεύθυνση) και τελικά δεν μπόρεσε να παράσχει καμία προστασία. Το ίδιο βέβαια ισχύει και για τον πιο εξελιγμένο ιό “I love you”.

Επίσης σε δοκιμές που έγιναν το πρόγραμμα δεν μπόρεσε να καταλάβει την αποστολή mail μέσω telnet, με χρήση pine, ούτε και την αποστολή μέσω webmail (πράγμα που ενισχύει την άποψη για έλεγχο μόνο του port 25).

Καταλήγοντας, το πρόγραμμα MailControl 1.0 δεν μπορεί να θεωρηθεί firewall ηλεκτρονικού ταχυδρομείου(όπως σημειώνεται στην διεύθυνση http://www.wincomplete.com/download/?id=755) αφού έχει πολύ σοβαρές ελλείψεις και η προστασία που παρέχει είναι ελάχιστη. Ακόμα κατά την απεγκατάσταση το πρόγραμμα προκάλεσε αλλαγές στο registry και προβλήματα στην λειτουργία των windows (ειδικότερα στην πρόσβαση στο δίκτυο).

Σημείωση: Αυτό το πρόγραμμα είναι ελεύθερο για τη προσωπική χρήση, αλλά οι επιχειρήσεις, οι εκπαιδευτικοί οργανισμοί και οι κυβερνητικοί χρήστες πρέπει να κατέχουν άδειες χρήσης $19.95 ανά χρήστη. Το MailControl είναι Freeware και συμβατό σύστημα με τα WINDOWS Windows 95 / 98 / Me / NT / 2000.

5.2 WinRoute Pro 4.1 Build 24 [10] [14][15][16][17]

Το WinRoute Pro 4.1 είναι ένα πακέτο λογισμικού που εκτελεί διαδικασίες δρομολόγησης και firewalling. Έχει αναπτυχθεί από την Tiny Software για Windows 95, 98, 2000 and NT 4.0. Θεωρείται ως ιδανική λύση [11] για δίκτυα μικρού εώς μεσαίου μεγέθους.

Το προϊόν αυτό έχει πολλά προηγμένα χαρακτηριστικά όπως: προηγμένο NAT, τρόπο κρυφής λειτουργίας (stealth mode operation), απομακρυσμένη διαχείριση (remote administration), καταγραφή (logging), ενσωματωμένο DHCP (Dynamic Host Configuration Protocol) server (built in DHCP server), URL filtering, VPN support, port mapping, DNS forwarding, και HTTP cache και proxy server. Όλα αυτά τα χαρακτηριστικά το καθιστούν πολύ καλή λύση για μικρού-μεσαίου μεγέθους δίκτυα. Επιπλέον περιέχει και ένα πλήρη SMTP/POP3 e-mail server με απεριόριστο αριθμό ψευδωνύμων (aliases) και έτσι είναι λύση για δίκτυα που δεν θέλουν διαχείριση βασισμένη σε Unix ή Linux.

Απαιτήσεις συστήματος:

- Pentium class PC (single or dual processor)
- Windows 95/98/NT4/2000 OS
- 32MB memory
- 1MB of free disk space
- Τουλάχιστον δυο interfaces. Μπορούν να είναι Ethernet, TokenRing, DirectPC, ή RAS.

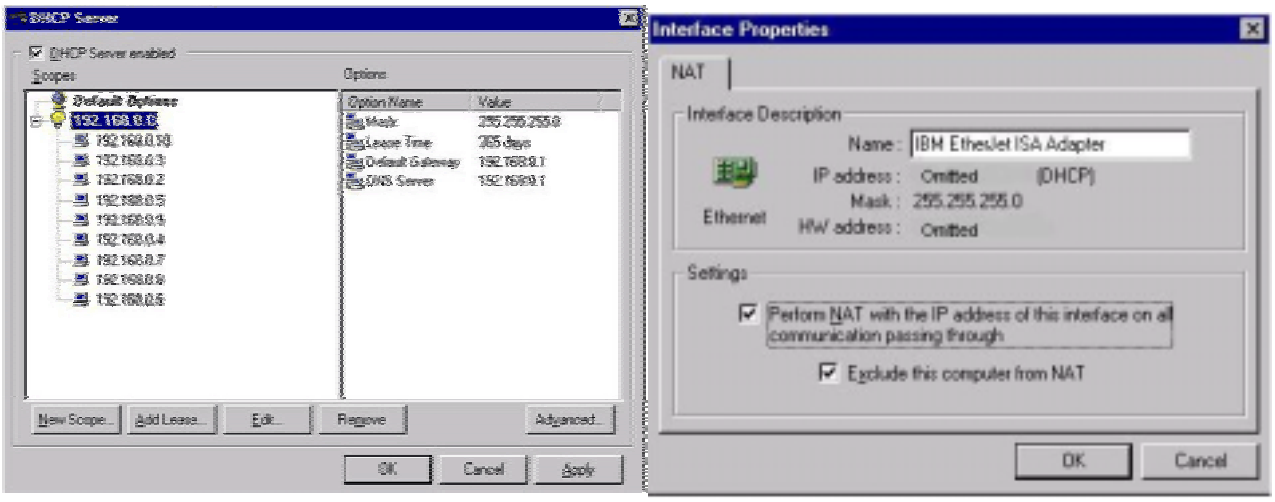
Εγκατάσταση

Το WinRoute Pro είναι διαθέσιμο σε μια δοκιμαστική έκδοση 30 ημερών. Μετά από 30 ημέρες απαιτείται ένα κλειδί για να μπορέσει να συνεχιστεί η λειτουργία του. Η τιμή του εξαρτάται από τον αριθμό των αδειών χρήσης (5, 10, 25, unlimited) και ποικίλει από 199$ μέχρι 699$, με ειδικές εκπτώσεις για εκπαιδευτικούς σκοπούς. Κάθε μηχάνημα συμπεριλαμβανομένου και του host (που δρομολογεί μέσω του WinRoute Pro) μετρά σαν χρήστης ενώ ο αριθμός των mail boxes περιορίζεται στον αριθμό των χρηστών αλλά μπορούν να υπάρξουν απεριόριστα aliases.

Το αρχείο εγκατάστασης του προγράμματος είναι μόλις 1,5 MB ενώ περιλαμβάνει και ένα πολύ χρήσιμο αρχείο help. Η εγκατάσταση είναι εύκολη και απαιτεί επανεκκίνηση για να ολοκληρωθεί. Ο κεντρικός υπολογιστής χρειάζεται να είναι συνδεμένος στο διαδίκτυο και να έχει μια κάρτα δικτύου συνδεμένη σε ένα port switch στο οποίο θα συνδεθούν οι υπόλοιποι υπολογιστές.

Διαμόρφωση (Configuration)

Ο πιο εύκολος τρόπος είναι να χρησιμοποιηθεί ένας DHCP (Dynamic Host Configuration Protocol) server στο Winroute Pro για να αποδοθούν IP στους client υπολογιστές. Η εγκατάσταση είναι απλή και απαιτεί το εύρος των τιμών IP που θα αποδοθούν, την gateway, DNS και τον χρόνο λήξης των IPs που αποδίδονται σε κάθε client. Όλοι οι clients ρυθμίζονται ώστε να δέχονται τις ρυθμίσεις που τους καθορίζει ο DHCP server. Μετά την επανεκκίνηση όλων των clients όλοι έχουν πλέον την IP διεύθυνση που τους απέδωσε το Winroute Pro.



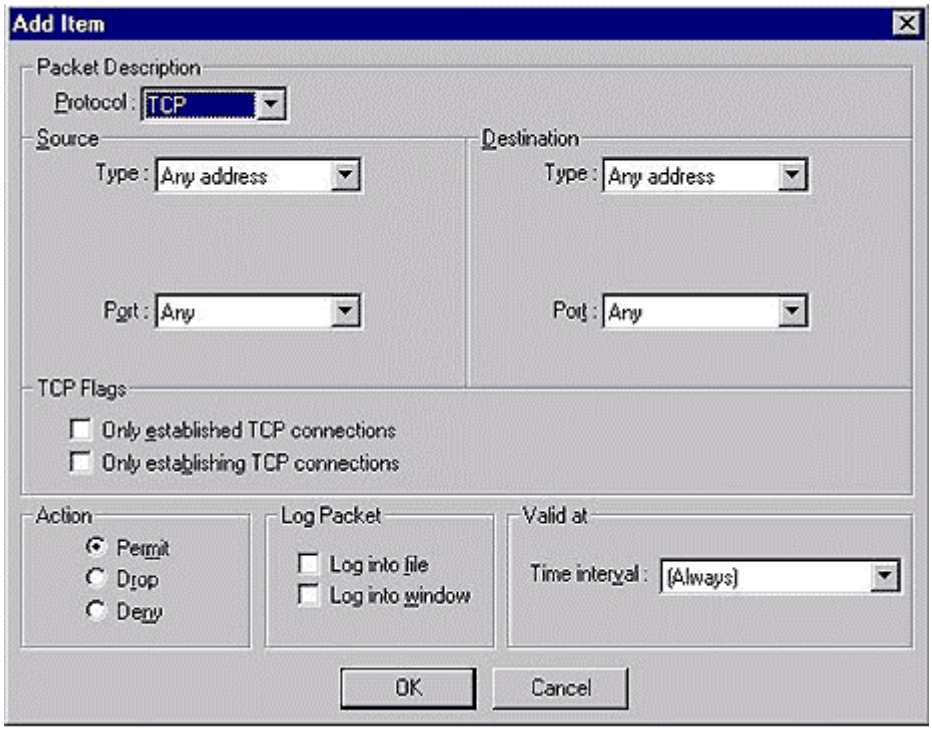
Το επόμενο βήμα είναι η ενεργοποίηση του NAT (Network Address Translation) στην εξωτερική διεπαφή του δικτύου. Αυτό απλά απαιτεί την επιλογή στο παράθυρο των ιδιοτήτων της διεπαφής (Interface Properties window) που φαίνεται παραπάνω. Με την επιλογή αυτή όλα τα client PCs έχουν πλήρως λειτουργικές δικτυακές συνδέσεις. Web, FTP, Telnet, και e- mail λειτουργούν άψογα στα client PCs. Όλη η κυκλοφορία από το διαδίκτυο για κάθε client PC

φαίνεται ότι προέρχεται από τον host. Αυτό έχει σαν αποτέλεσμα την απόκρυψη των IPs των client PCs από το υπόλοιπο δίκτυο.

Ασφάλεια

Το Winroute Pro σχεδίαστηκε με σκοπό να προσφέρει υψηλή ασφάλεια. Είναι πιστοποιημένο από την ICSA (International Computer Security Association) και χρησιμοποιείται από πολλές κρατικές υπηρεσίες στις ΗΠΑ όπως την U.S. Naval Aviation Systems Team. Η ενοποίηση με το λειτουργικό σύστημα είναι μεγάλη και παρέχει πλήρη προστασία κάθε χρονική στιγμή. Το ενδιαφέρον για την ασφάλεια είναι τόσο μεγάλο που το πρόγραμμα «φορτώνεται» πριν τα modules του δικτύου ώστε να παρέχει ασφάλεια ακόμα από τα πρώτα δευτερόλεπτα μετά την εκκίνηση του υπολογιστή.

Το WinRoute υιοθετεί την stealth mode λειτουργία πράγμα που κάνει το δίκτυο να φαίνεται «αόρατο». Αυτό γίνεται κόβοντας (drop) αντί να αρνείται(deny) τα ανεπιθύμητα πακέτα. Έτσι στον αποστολέα δεν επιστρέφονται error messages αλλά δεν πηγαίνει καμία απάντηση. Με τον τρόπο αυτό το δίκτυο είναι αόρατο σε οποιοδήποτε σκανάρει τα ports. Επίσης το πρόγραμμα έχει πλήρεις δυνατότητες logging ώστε να μπορεί να παρακολουθείται η κίνηση του δικτύου.



Ακόμα, πολλά προηγμένα χαρακτηριστικά ασφαλείας μπορούν να τροποποιηθούν ανάλογα με τις ανάγκες. Για παράδειγμα κανόνες μπορούν να καθοριστούν για κάθε port, όπως και η χρονική περίοδος για την εφαρμογή τους. Οι κανόνες αυτοί πιο πολύ θα ενδιαφέρουν τον έμπειρο χρήστη.

Επίσης είναι δυνατόν να εφαρμοστεί φιλτράρισμα πακέτων με anti-spoofing χαρακτηριστικά. Με τον τρόπο αυτό μπορεί να υπάρξει πλήρης έλεγχος των εισερχόμενων και εξερχόμενων

πακέτων με την δυνατότητα να εμποδιστεί η κυκλοφορία σε συγκεκριμένα ports ή και διευθύνσεις IP.

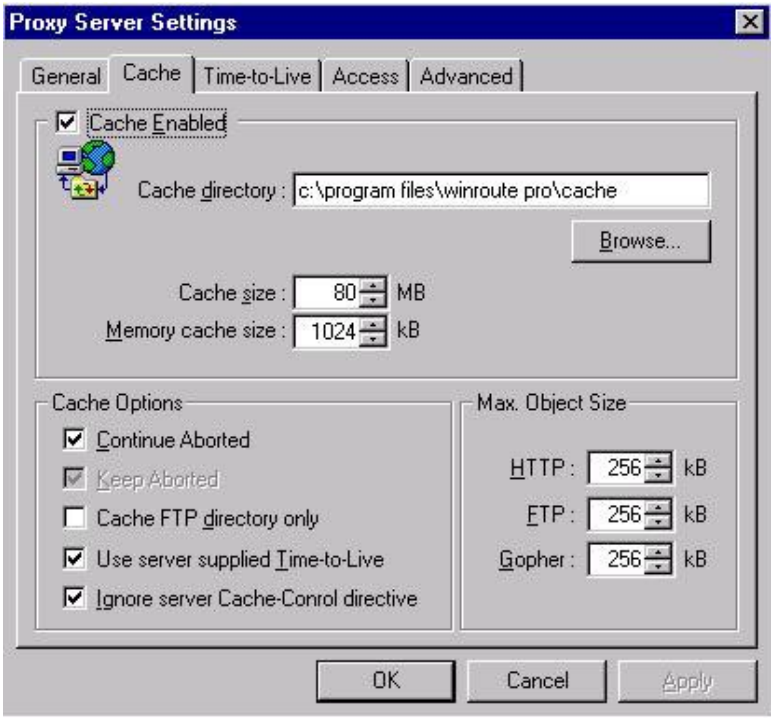
Το πρόγραμμα επίσης παρέχει προηγμένα NAT χαρακτηριστικά που μπορούν να επιτρέψουν τον έλεγχο της κυκλοφορίας μεταξύ των υπολογιστών του δικτύου και να απαγορέψουν ή να επιτρέψουν επιλεκτικά την κυκλοφορία μεταξύ κάποιου εσωτερικού μηχανήματος και του εξωτερικού δικτύου.

Επιπρόσθετα Χαρακτηριστικά

Τα επιπρόσθετα χαρακτηριστικά που έχει το Winroute Pro μπορούν πολύ εύκολα να απλοποιήσουν την διοίκηση του δικτύου.

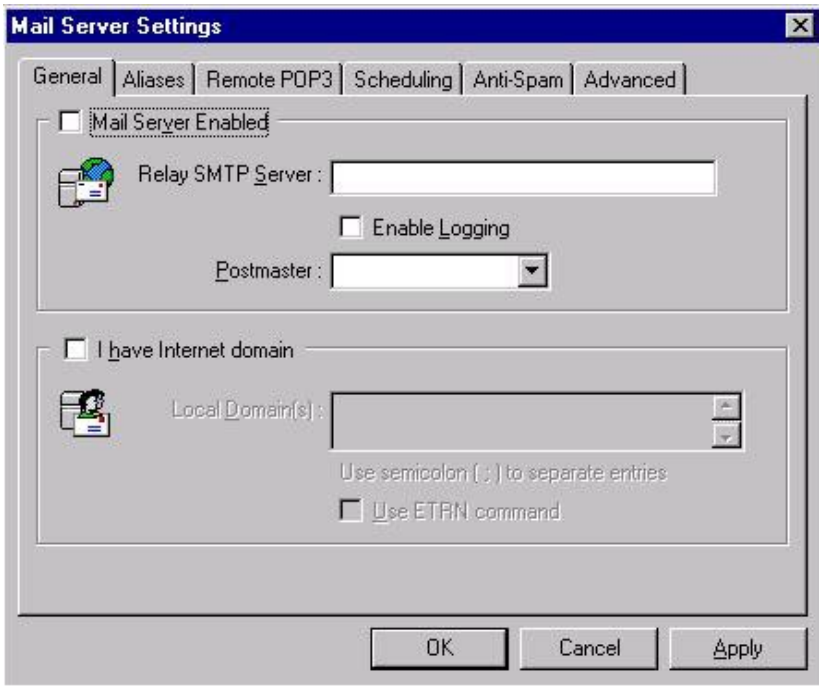
Ένα εύκολο στη χρήση port mapping δίνει την δυνατότητα παράδοσης εισερχόμενων πακέτων σε συγκεκριμένα μηχανήματα στο δίκτυο, βασιζόμενο στο port προορισμού. Αυτό επιτρέπει την εύκολη εγκατάσταση WWW, FTP, Mail, ή Telnet server πίσω από το firewall και την καθοδήγηση της σωστής κυκλοφορίας σε καθέναν από αυτούς.

Το Winroute Pro περιλαμβάνει ένα προηγμένο HTTP cache και proxy server (βλέπε επόμενο σχήμα) έτσι ώστε να βελτιστοποιηθεί η χρήση του bandwidth. Αυτό γίνεται αποθηκεύοντας στην cache ιστοσελίδες που έχουν πρόσφατα επισκεφθεί οι χρήστες. Ακόμα το πρόγραμμα μπορεί να επιτρέψει τον έλεγχο της πρόσβασης σε URLs με βάση συγκεκριμένη λέξη κλειδί.Π.χ να απαγορευτεί πρόσβαση σε URLs που περιέχουν την φράση “xxx”.



Στο ίδιο πακέτο περιλαμβάνεται και ένας SMTP/POP3 mail server (βλ παρακάτω σχήμα) που τον χαρακτηρίζει η δυνατότητα για απεριόριστο αριθμό ψευδωνύμων (aliases). Όμως το

πρόγραμμα απαιτεί ένα εξωτερικό SMTP server από ένα provider που θα μεταδίδει τα e-mail από τους χρήστες σε υπολογιστές εκτός δικτύου.



Η διαχείριση των εισερχόμενων e-mail μπορεί να γίνει με 3 διαφορετικούς τρόπους ανάλογα με την ύπαρξη ή όχι domain name.

- Εάν δεν υπάρχει domain name κάθε χρήστης πρέπει να έχει ξεχωριστό λογαριασμό POP3 στον provider. Το WinRoute θα συλλέγει τα mail από κάθε λογαριασμό και θα τα αποδίδει στον σωστό παραλήπτη
- Εάν υπάρχει domain name τότε υπάρχουν 2 λύσεις:

Α) η δημιουργία ενός POP3 account στον provider βασισμένο στο domain name. Το WinRoute θα συλλέγει τα mail από τον λογαριασμό και θα τα αποδίδει στον σωστό παραλήπτη

Β)Χωρίς δημιουργία του παραπάνω λογαριασμού αλλά λήψη mail χρησιμοποιώντας το πρωτόκολλο SMTP.

Ένα επιπλέον παρεχόμενο χαρακτηριστικό είναι και η απομακρυσμένη διοίκηση (Remote administration). Μια ξεχωριστή εφαρμογή η οποία μπορεί να τρέξει σε οποιοδήποτε υπολογιστή μπορεί να συνδεθεί στον υπολογιστή που «τρέχει» το WinRoute και να αλλάξει την διαμόρφωση και τις ρυθμίσεις. Για να γίνει αυτό με ασφάλεια χρησιμοποιείται ένα 128-bit Blowfish based πρωτόκολλο κρυπτογράφησης.

Μειονεκτήματα

Το πρόγραμμα δεν διαθέτει κάποια χαρακτηριστικά που θα ήταν πολύ χρήσιμα. Ένα από αυτά είναι η παρουσίαση του διαθέσιμου bandwidth λόγω των πολλών χρηστών που το μοιράζονται. Ακόμα είναι αναγκαία και η ύπαρξη μιας εύχρηστης λίστας επιθέσεων που να

περιέχει τις ιδιότητες των επιτιθέμενων. Με τον τρόπο αυτό δεν θα χρειάζεται συνεχής επίσκεψη στα logs. Τέλος κατά καιρούς έχουν αναφερθεί προσπάθειες για cracking του προγράμματος καθώς και κάποια bugs που περιέχει.[12]

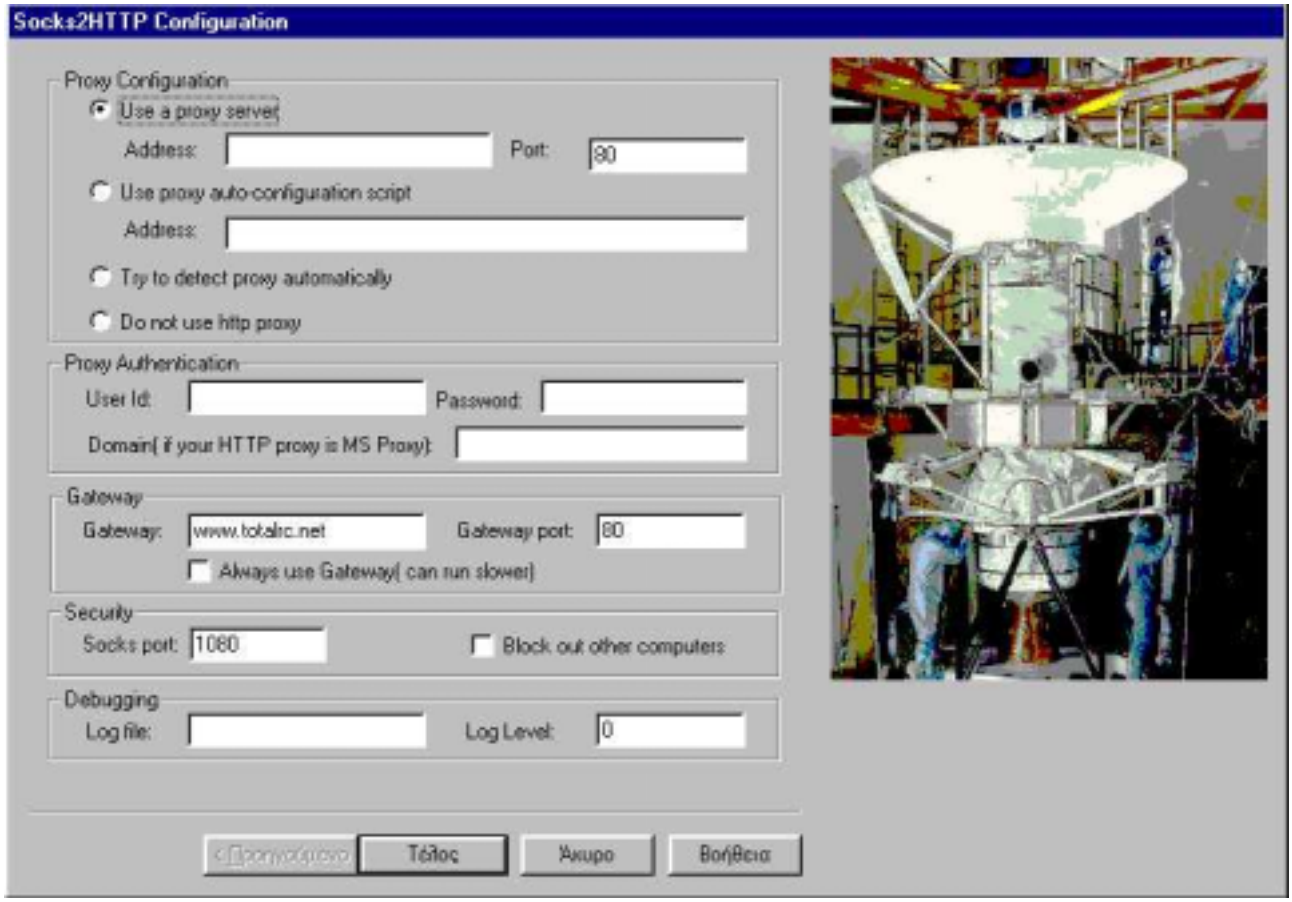
Σύνοψη

Το WinRoute Pro είναι ένα προϊόν που καλύπτει τις ανάγκες πολλών δικτύων μικρού ως και μεσαίου μεγέθους. Προσφέρει μεγάλες δυνατότητες ασφάλειας, πολλές δυνατότητες ρυθμίσεων ανάλογα με τις απαιτήσεις και δεν έχει απαιτήσεις σε υπολογιστική ισχύ και σε χωρητικότητα Ακόμα η τιμή στην οποία διατίθεται είναι πολύ καλή και υπάρχουν διάφορα πακέτα ανάλογα με των αριθμό των χρηστών ενώ και παρέχεται on-line υποστήριξη. Τέλος θα πρέπει να σημειωθεί ότι δεν απαιτεί πολλές γνώσεις για δίκτυα υπολογιστών ενώ υπάρχει και δοκιμαστική έκδοση 30 ημερών. Η βαθμολογία του σε πολλές συγκρίσεις που έχουν γίνει είναι αρκετά υψηλή[13]

5.3 SOCKS2HTTP 0.73 Beta [18]

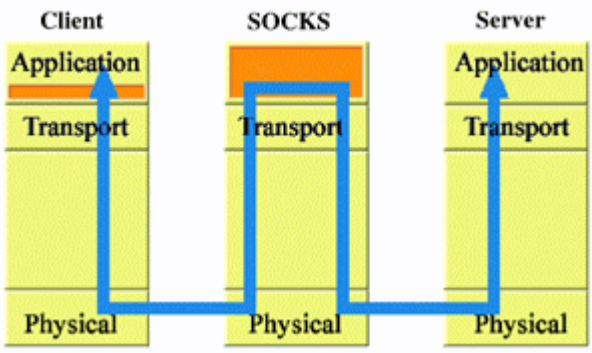
Το πρόγραμμα Socks2HTTP είναι ένας πράκτορας (agent) που μετατρέπει αιτήσεις (requests) του πρωτοκόλλου SOCKS v.5 σε HTTP αιτήσεις και τις κατευθύνει, χρησιμοποιώντας την τεχνική του tunneling, διαμέσω HTTP proxy server. Το πρωτόκολλο Socks επιτρέπει σε προγράμματα να διαπερνούν firewalls σε οποιοδήποτε port και χρησιμοποιείται από πολλά δημοφιλή προγράμματα όπως Napster, Gnutella, MSN Messanger. Πολλές εταιρίες περιορίζουν την διέλευση από το firewall μόνο σε HTTP αιτήσεις, απενεργοποιώντας τους SOCKS proxy servers. Το πρόγραμμα Socks2HTTP παρέχει ένα μικρό socks server για τον socks client, που εκτελεί την σύνδεση διαμέσω του HTTP proxy server.Το κύριο μειονέκτημά του είναι ότι μειώνει την ταχύτητα μεταφοράς δεδομένων.

Εάν ένα πρόγραμμα πελάτη δεν υποστηρίζει το socks πρωτόκολλο το socks2HTTP μπορεί πάλι να λειτουργήσει χρησιμοποιώντας το "socksificator": ένα SocksCap32 πρόγραμμα από την διεύθυνση www.socks.nec.com



Τι είναι το socks πρωτόκολλο;[19]

Το socks είναι ένα proxy πρωτόκολλο για εφαρμογές βασισμένες στο TCP/IP. Το SOCKS επιτρέπει σε hosts από την μια πλευρά του SOCKS server να αποκτήσουν πλήρη πρόσβαση σε hosts στην άλλη πλευρά του SOCKS server χωρίς να απαιτείται απευθείας πρόσβαση IP (without direct IP reachability). Περιλαμβάνει δυο κομμάτια, τον SOCKS server και τον SOCKS client. Ο SOCKS server λειτουργεί στο επίπεδο εφαρμογής ενώ ο SOCKS client λειτουργεί μεταξύ των εφαρμογών και του επιπέδου μεταφοράς.



Όταν ένας client χρειάζεται να συνδεθεί στον application Server, συνδέεται πρώτα σε ένα socks proxy server.Ο socks proxy server συνδέεται στον application Server αντί για τον client και μεταβιβάζει δεδομένα μεταξύ client και application server. Για τον application server ο proxy server είναι ο client .

Υπάρχουν δυο εκδόσεις του SOCKs η V4 και V5. Η έκδοση 4 εκτελεί την σύνδεση, δημιουργεί το κύκλωμα και μεταβιβάζει τα δεδομένα, ενώ η έκδοση 5 παρέχει επιπλέον πιστοποίηση και UDP proxy[20]
Τα πρωτόκολλα αυτά περιγράφονται στα ακόλουθα RFCs: RFC1928, RFC1929, RFC1961

Γιατί το Socks;
Το Socks αρχικά σχεδιάστηκε ως ένα firewall δικτύου. Ακόμα και σήμερα αποτελεί μια εναλλακτική λύση αντί για firewall. Λόγω της απλότητας και ευελιξίας του, χρησιμοποιήθηκε ως γενικός proxy εφαρμογών σε εικονικά ιδιωτικά δίκτυα (VPN) και σε extranet εφαρμογές. Οι proxies που βασίζονται στο socks έχουν τα ακόλουθα πλεονεκτήματα:
-Παρέχουν διαφανή πρόσβαση διαμέσου πολλών proxy servers
-Εύκολη εφαρμογή πιστοποίησης και μεθόδων κρυπτογράφησης
-Έχουν απλή πολιτική ασφαλείας δικτύου

[21]Για την ανώνυμη πλοήγηση στο δίκτυο απλά μπορεί να επιλεχτεί ότι η σύνδεση στο δίκτυο είναι απευθείας (no proxy), δηλ να επιλεχθεί “do not use http proxy”.
Επίσης είναι δυνατό να αποφευχθεί η λογοκρισία (censorship)[22]
Οι ενέργειες του προγράμματος SOCKS2HTTP μπορούν να συνοψισθούν στις εξής δυο ενέργειες:
1.δημιουργεί ένα socks server στον υπολογιστή
2. δημιουργεί μια σύνδεση μέσω HTTP με ένα remote server ο οποίος μπορεί να μετατρέψει SOCKS2HTTP protocol σε Socks protocol.

Χρησιμοποιείται διαμορφώνοντας socks-capable programs ώστε να χρησιμοποιούν τον τοπικό socks server. Έτσι εάν χρειάζεται να τρέξει κάτι που δεν είναι socks-capable, μπορούμε εύκολα να το καταστήσουμε ικανό με την εφαρμογή sockscap από την εταιρία NEC (www.socks.nec.com).
Έτσι ο τρόπος λειτουργίας του είναι ο ακόλουθος (εδώ διακρίνονται τα πρωτόκολλα σε κάθε φάση)
program --> sockscap --> socks2http socks server --> ETC/ISU (or corp) proxy --> remote server --> socks server --> destination

whatever socks http http socks whatever

6. Βιβλιογραφία

[1]http://www.vicomsoft.com/index.html?page=http://www.vicomsoft.com/knowledge/reference/firewalls1.html*track=internal

[ΠΟ][Firewalls, Εισαγωγή στις υπηρεσίες δικτύου δεδομένων-Πομπόρτσης, 4η έκδοση-2000,σελ324-328,ISBN 960-243-575-5]

[RAM] Ένθετο Τεύχος Μάιος 2001 σελ.52-56

[2]Netbus Pro: Remote-control program often used as an attack tool to control remote PCs. http://netbus.nu/)

[3] Nmap http://www.insecure.org/nmap

[4] www.signal9.com

[5] http://www.danu.ie/terminet.htm

[6] http://www.tinysoftware.com/pwall.php

[7] www.zonealarm.com

[8] http://www.sygate.com/products/shield_ov.htm

[9] http://www.wincomplete.com/Security_&_Privacy/Firewalls/

[10] http://hardware.earthweb.com/moth/article/0,,12102_620721_1,00.html

[11] http://securityportal.com/pr/pr.20000727140145.html)

[12] http://securityportal.com/list-archive/bugtraq/2001/Jan/0014.html)

[13] http://www.speedguide.net/reviews/tinisoft/tiny_firewall_p4.shtml

[14] http://www.dsi-web.com/reviews/WinRoutePro/WinRoute.html

[15]http://www.icsalabs.com/html/communities/firewalls/certification/vendors/tinysoftware/winroute/nt/30a_report.shtml

[16] http://securityportal.com/pr/pr.20000727140145.html

[17] http://securityportal.com/pr/pr.20000906093239.html

[18] http://www.ProgramFiles.com/index.asp?ID=9707 και manual του προγράμματος

[19] http://www.socks.nec.com/aboutsocks.html

[20] http://www.socks.nec.com/socksfaq.html

[21] http://www.totalrc.net/s2h/faq.html

[22] http://plaguesplace.dyndns.org/proxy-elites-faq/x84.html)