ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΠΑΤΡΑΣ

ΣΧΟΛΗ ΔΙΟΙΚΗΣΗΣ ΚΑΙ ΟΙΚΟΝΟΜΙΑΣ

ΤΜΗΜΑ ΕΦΑΡΜΟΓΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΣΤΗΝ ΔΙΟΙΚΗΣΗ ΚΑΙ ΟΙΚΟΝΟΜΙΑ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Συγκριτική μελέτη τειχών προστασίας όσο αφορά την απόδοση, ασφάλεια και παραμετροποίηση τους

Comparative study firewalls regarding performance, safety and parameterization

Σπουδαστής: Τσίκας Φώτιος

Κουμουλίδης Γεώργιος

Εισηγητής: Χόχολης Διονυσιός

ΑΜΑΛΙΑΔΑ 2013

Περιεχόμενα

Περίληψη

Ο τομέας των δικτύων αποτελεί πλέον τον πυρήνα των τεχνολογικών υποδομών ενός οργανισμού. Οι κάθε είδους οργανισμοί όλο και περισσότερο βασίζονται στην δικτυακή τους υποδομή, για χρήση είτε από τους ίδιους τους εργαζομένους είτε από εξωτερικούς χρήστες ή συνεργάτες. Επιπλέον οι σύγχρονες τάσεις και εξελίξεις της τεχνολογίας λογισμικού οδηγούν προς την ανάπτυξη και χρήση διαδικτυακών εφαρμογών και την σταδιακή απομάκρυνση των παραδοσιακών κλειστών επιτραπέζιων εφαρμογών. Οι εφαρμογές παρέχουν πρόσβαση στα δεδομένα του οργανισμού και το δίκτυο είναι το μέσο που δίνει την δυνατότητα στους χρήστες να αλληλεπιδρούν με την εφαρμογή και επομένως και με τα δεδομένα. Κατά συνέπεια εάν δεν ενισχυθεί η ασφάλεια του δικτύου κρίσιμα και ευαίσθητα δεδομένα του οργανισμού είναι ευάλωτα σε κάθε είδους κακόβουλες επιθέσεις.

Τα τελευταία χρόνια λόγω του πρωτεύοντα ρόλου των δικτύων στην παγκόσμια πραγματικότητα, η ασφάλεια που παρέχουν αποτελούν πλέον πρωταρχική προτεραιότητα για την τεχνολογική έρευνα και εξέλιξη. Μία από τις βασικότερες τεχνολογίες για την ενίσχυση της ασφάλειας των δικτύων είναι τα Τείχη Προστασίας. Τα Τείχη Προστασίας επιβάλλουν μια πολιτική ελέγχου πρόσβασης στην κυκλοφορία του δικτύου διασφαλίζοντας ότι η ροή των πακέτων υπόκειται σε συγκεκριμένους κανόνες. Τα Τείχη Προστασίας υλοποιούνται είτε σαν λογισμικό, είτε σαν μια αυτόνομη συσκευή, είτε σαν μέρος του δρομολογητή. Κάθε μία από τις προηγούμενες λύσεις παρέχει διαφορετικές προδιαγραφές όσον αφορά την απόδοση την ασφάλεια και την παραμετροποίηση.

Σκοπός της συγκεκριμένης πτυχιακής είναι η συγκριτική μελέτη των παραπάνω τύπων Τειχών Προστασίας, μέσα από ένα σύνολο πειραμάτων, με στόχο την εξαγωγή σαφών συμπερασμάτων και αποτελεσμάτων για τις δυνατότητες κάθε ενός από τους παραπάνω τύπους όσον αφορά την απόδοση, την ασφάλεια και την παραμετροποίηση. Για την διεξαγωγή των πειραμάτων θα χρησιμοποιηθούν εργαλεία προσομοίωσης δικτύων (Network Simulator) και εργαλεία ελέγχου και αποτίμησης της ασφάλειας του δικτύου.

Abstract

The area networks has become the core of the technological infrastructure of an organization. All kinds of organizations increasingly rely on network infrastructure, for use either by the workers themselves or by external users or partners. Moreover, the modern trends and developments of software engineering lead to the development and use of web applications and the gradual removal of traditional closed desktop applications. These applications provide access to the organization's data and the network is the medium that enables users to interact with the application and therefore with the data. Consequently without strengthening network security critical and sensitive data of the organization is vulnerable to all kinds of malicious attacks.

In recent years because of the primary role of networks in the global reality, the protection offered are now a top priority for technological research and development. One of the key technologies to enhance network security is the firewall. Firewalls enforce an access control policy in network traffic by ensuring that the flow of packets subject to specific rules. Firewalls are implemented either as software or as a standalone device or as part of the router. Each of the previous solutions provide different standards of performance security and customization.

The purpose of this thesis is a comparative study of these types of firewall, through a set of experiments with the aim to draw clear conclusions and results for the possibilities of each of the above types in terms of performance, security, and configuration. To conduct the experiments will be used simulation tools network (Network Simulator) and tools of monitoring and assessment of network security.

Εισαγωγή

Η παρούσα πτυχιακή έχει ως στόχο την συγκριτική μελέτη τειχών προστασίας όσο αφορά την απόδοση, ασφάλεια και παραμετροποίηση τους. Συγκεκριμένα σε θεωρητικο και ερευνητικό επίπεδο θα μελετηθεί θέματα δικτύων, ασφαλείας, κατηγορίες πυρότειχων καθώς και τρόποι εισβολής σε ένα Η/Υ. Αναλυτικά:

Το 1^{ο} κεφάλαιο μελετάει την αρχιτεκτονική του διαδικτύου, ποια η χρηση του διαδικτύου σε Ελλάδα και Ευρωπαϊκή Ένωση καθώς και τι ορίεται ως αρχιτεκτονική. Επίσης θα μελετηθεί το μοντέλο OSI και τέλος τα επίπεδα πρόσβασης του διαδικτύου.

Στο κεφάλαιο 2 θα δούμε πως προστατευόμαστε από τις απειλές στο διαδίκτυο με την βοήθεια των firewall. Θα μελετηθεί η λειτουργία τους, η ιστορία τους, το πώς σχεδιάζονται και αναλύονται, τις αδυναμίες που παρουσιάζονται καθώς και το πώς εγκαθιστόνται σε ένα σύστημα.

Στο 3^{ο} κεφάλαιο θα αναγραφφεί τα συστήματα firewall και το πώς ταξινομούνται. Επίσης γίνεται αναφορά στην διαχείρηση συστημάτων firewall, στον σχεδιασμό και στις βασικές μέθοδοι ελέγχου ασφάλειας των εφαρμογών ιστού.

Το 4^{ο} και τελευταίο κεφάλαιο είναι η μελέτη περίπτωσης όπου με την χρήση εργαλείων και προγραμμάτων θα δοκιμαστούν διάφορα γνωστά firewall και θα δεικτεί η αποτελεσματικότητα αυτών. Τέλος θα καταλήξει η μελέτη σε κάποια συμπεράσματα και θα αναφέρε μελλοντικές πράξεις που μπορεί να γίνουν.

1 ΚΕΦΑΛΑΙΟ ΤΟ ΔΙΑΔΙΚΤΥΟ ΚΑΙ Η ΑΡΧΙΤΕΚΤΟΝΙΚΗ ΤΟΥ ΔΙΑΔΙΚΤΥΟΥ

Το καθημερινό όμως δίκτυο το οποίο μοιάζει περισσότερο με το Internet είναι... ο δρόμος. Έχετε μια διεύθυνση σ' αυτόν τον δρόμο. Και αυτός, και οι άλλοι δρόμοι στη γειτονιά σας ή στην πόλη σας, συνδέονται και τελικά οδηγούν σ' ένα μεγαλύτερο δρόμο ή σε λεωφόρο. Αυτή η λεωφόρος διατρέχει άλλες γειτονιές. Και αυτές οι λεωφόροι τελικά οδηγούν σε μεγαλύτερες λεωφόρους οι οποίες με τη σειρά τους οδηγούν σε πύλες: αεροδρόμια και λιμάνια τα οποία συνδέουν μεταξύ τους. Σκεφτείτε την κάθε γειτονιά ή πόλη σαν ένα δίκτυο από δρόμους. Εάν γνωρίζετε την διεύθυνση που θέλετε, μπορείτε να βρείτε έναν δρόμο που οδηγεί σε ένα άλλο κτίριο στον κόσμο. Σκεφτείτε, έπειτα, το σύνολο των δικτύων σαν ένα "δίκτυο των δικτύων". Αυτό είναι το Internet. Το Web, ο παγκόσμιος ιστός, είναι λοιπόν ένα τεράστιο δίκτυο μεταφοράς ενός απίστευτου όγκου αρχείων, κειμένων, δεδομένων, φωτογραφιών κτλ. Απλά φανταστείτε την εποχή όπου ο μοναδικός τρόπος αποστολής δεδομένων ήταν το ταχυδρομείο και ύστερα το φαξ. Όπως και σε ότι αφορά τη σύλληψη του Internet, η ιδιωτική επιχείρηση δεν έπαιξε μεγάλο ρόλο στη φάση της δημιουργίας του παγκόσμιου ιστού. Η ανάπτυξη του Web προήλθε μετά από έρευνα και ξεκίνησε το 1980 στο CERN (European Particle Physics Laboratory) από τον Tim Berners-Lee. (Κάτσικας)

1.1 Η χρήση του διαδικτύου στην Ελλάδα

Σχετικά με τη χρήση του Διαδικτύου στην Ελλάδα, παρατηρείται σημαντική αύξηση του αριθμού των χρηστών (από 13% το 2001 σε 31% το 2007) ηλικίας 15 έως 65 ετών που κατέχουν προσωπικό Η/Υ. Αντίστοιχα, παρατηρείται αύξηση των ωρών χρήσης του Διαδικτύου που φτάνουν κατά μέσω όρο τις 8,6 ανά εβδομάδα. Η υπηρεσία που χρησιμοποιείται περισσότερο είναι το ηλεκτρονικό ταχυδρομείο (e-mail) αλλά και η ενημέρωση (νέα, καιρός, αθλητικά) αποτελεί από τους κυριότερους λόγους χρήσης του Διαδικτύου. (Κάτσικας)

Αντίθετα, η αναζήτηση για προϊόντα και υπηρεσίες ακολουθεί πτωτική πορεία από το 2002. Ιδιαίτερα χαμηλή παραμένει η χρήση του Διαδικτύου για αγορά προϊόντων και υπηρεσιών. Περίπου 18% των χρηστών προχώρησε σε κάποια αγορά κατά το 2006 ωστόσο το ποσοστό αυτό ανέρχεται μόλις στο 4,5% του γενικού πληθυσμού. Παρόλα

αυτά, οι αγορές πραγματοποιήθηκαν κυρίως από ελληνικούς ιστοχώρους (sites) (41%) έναντι των ξένων (35%).

Οι χρήστες που αγοράζουν μέσω του Διαδικτύου συνήθως δεν επισκέπτονται τα αντίστοιχα καταστήματα, ενώ οι κυριότεροι λόγοι αγοράς είναι η προσιτή τιμή και η καλή εξυπηρέτηση.

Τέλος, αξιοσημείωτο είναι το γεγονός ότι σε ποσοστό πάνω από 60% οι χρήστες θεωρούν ότι ο κίνδυνος διαρροής προσωπικών δεδομένων κατά τη χρήση πιστωτικής κάρτας στις ηλεκτρονικές αγορές είναι μεγάλος ή πολύ μεγάλος. (Κάτσικας)

1.2 Το διαδίκτυο και η Ευρωπαική Ένωση

Το δικαίωμα των Ευρωπαίων πολιτών για ελεύθερη πρόσβαση στο Διαδίκτυο κατοχυρώνεται στο άρθρο 11 του Χάρτη των Θεμελίων Δικαιωμάτων της Ευρωπαϊκής Ένωσης περί ελευθερίας της έκφρασης και της ενημέρωσης. Πρόσφατα στο Ευρωπαϊκό Κοινοβούλιο ψηφίστηκε τροπολογία σύμφωνα με την οποία «δεν μπορεί να επιβάλλεται περιορισμός επί των θεμελιωδών δικαιωμάτων και ελευθεριών των τελικών χρηστών, χωρίς να προηγηθεί δικαστική απόφαση... εκτός από περιπτώσεις όπου απειλείται η ασφάλεια των πολιτών και στις οποίες η απόφαση δύναται να είναι αντίστοιχη». Ακόμη όμως και με την εν λόγω τροπολογία η πρόσβαση στο Διαδίκτυο θα μπορεί να απαγορευτεί με σχετικές δικαστικές αποφάσεις που θα επιβάλλει η εκάστοτε εθνική νομοθεσία στο όνομα της απειλής της ασφάλειας. (Κάτσικας)

Συγκεκριμένα, η τροπολογία αναφέρει επίσης «…η πρόσβαση στο Διαδίκτυο δεν μπορεί να περιοριστεί χωρίς να προηγηθεί δικαστική απόφαση. Εξαιρούνται οι περιπτώσεις όπου απειλείται η ασφάλεια των πολιτών.» Χαρακτηριστικό παράδειγμα αποτελεί η Βρετανία, στην οποία οι πάροχοι απαγόρευσαν την πρόσβαση σε μια λίστα ιστοσελίδων στην οποία μέχρι τώρα βρίσκονταν σελίδες παιδικής πορνογραφίας, όμως πρόσφατα προστέθηκαν και άλλες, όπως αυτή που αφορά το χάκινγκ (hacking). Στους χρήστες που θα επιχειρούν να εισέλθουν σε κάποια από αυτές τις σελίδες θα απαγορεύεται η είσοδος, ενώ τα ηλεκτρονικά τους ίχνη θα καταγράφονται. (Κάτσικας)

Έτσι, παρά την εν λόγω τροπολογία, εξακολουθεί να μην λαμβάνεται υπ’ όψη ότι το αδιάσειστο δικαίωμα της πρόσβασης των πολιτών στο Διαδίκτυο αποτελεί

προαπαιτούμενο για την προάσπιση και άλλων θεμελιωδών δικαιωμάτων όπως η γνώση, η παιδεία η ελευθερία έκφρασης και πολιτικής δράσης. (Κάτσικας)

Είναι σημαντικό, επίσης, να κατανοηθεί πως οι χρήστες του Διαδικτύου δεν είναι πελάτες αλλά πολίτες και ως τέτοιοι θα πρέπει να λογίζονται σε θέματα που αφορούν αφενός την υποδομή του διαδικτύου και αφετέρου το δικαίωμα πρόσβασης σε αυτό.

Σχετικά με την υποδομή οφείλει η εκάστοτε εθνική αρχή να μεριμνά για την επέκταση του δικτύου, ακόμα και σε περιοχές που η ιδιωτική πρωτοβουλία αρνείται να προβεί στην απαιτούμενη επένδυση, όταν τη θεωρεί οικονομικά ασύμφορη. Έτσι θα διασφαλιστεί το δικαίωμα των πολιτών για ενημέρωση και ελευθερία έκφρασης. Όσον αφορά την πρόσβαση πρέπει να κατοχυρώνεται το δικαίωμα των πολιτών για ελεύθερη και ισότιμη πρόσβαση όπως αναφέρθηκε και με τα παραπάνω. (Κάτσικας)

1.3 Η αρχιτεκτονική του διαδικτύου

Το Internet υιοθετεί το μοντέλο client/server (πελάτη/διακομιστή) όσον αφορά στην παράδοση των πληροφοριών. Βάσει του μοντέλου αυτού ένας client υπολογιστής συνδέεται σε έναν server υπολογιστή στον οποίο υπάρχουν οι πληροφορίες και φυσικά ο client εξαρτάται από τον server για να παραλάβει τις πληροφορίες. (Κάτσικας)

Πρακτικά ο client ζητά τις υπηρεσίες του μεγαλύτερου υπολογιστή. Οι υπηρεσίες αυτές μπορούν να αφορούν στην εύρεση πληροφοριών και την αποστολή τους στον client, όπως γίνεται στην περίπτωση ερωτήσεων σε μία βάση δεδομένων του Web.

Αλλα παραδείγματα τέτοιων υπηρεσιών είναι η παράδοση Web σελίδων και η διαχείριση του εισερχόμενου και εξερχόμενου ταχυδρομείου. Οποτε χρησιμοποιείτε το Internet, είστε συνδεδεμένος σε έναν server και ζητάτε τη χρήση των υπολογιστικών του πόρων. (Κάτσικας)

Στη συνηθισμένη περίπτωση ο client είναι ο τοπικός προσωπικός υπολογιστής και ο server (γνωστός επίσης και ως host) είναι ένας πολύ ισχυρότερος υπολογιστής που φιλοξενεί τα δεδομένα. Οι υπολογιστές αυτοί μπορεί να είναι διαφόρων ειδών: πανίσχυρα PCs με Windows, Macintoshes καθώς και ένα ευρύ φάσμα συστημάτων με λειτουργικό σύστημα Unix. (Κάτσικας)

Η σύνδεση στον server πραγματοποιείται μέσω ενός LAN, μίας τηλεφωνικής γραμμής ή ενός δικτύου ευρείας περιοχής (WAN) το οποίο βασίζεται στο TCP/IP.

Ενας βασικός λόγος υιοθέτησης ενός δικτύου client/server είναι η δυνατότητα που παρέχει σε πολλούς χρήστες να χρησιμοποιούν ταυτόχρονα την ίδια εφαρμογή και τα αρχεία που βρίσκονται αποθηκευμένα στον server.

Στην περίπτωση του World Wide Web, client είναι ουσιαστικά ο browser του προσωπικού υπολογιστή σας και server είναι ο host υπολογιστής που βρίσκεται κάπου στο Internet. Τυπικά, ο browser στέλνει στον server μία αίτηση για μια καθορισμένη Web σελίδα. (Κάτσικας)

Ο server επεξεργάζεται την αίτηση και στέλνει μία απάντηση στον browser (επίσης, πιο συχνά με τη μορφή μιας Web σελίδας). Η σύνδεση μεταξύ του client και του server διατηρείται μόνο κατά τη διάρκεια της πραγματικής ανταλλαγής πληροφοριών.

Συνεπώς, αφού ολοκληρωθεί η μεταφορά της Web σελίδας από τον host υπολογιστή, διακόπτεται η HTTP σύνδεση μεταξύ του συστήματος και του client (HTTP αντιστοιχεί στο Hypertext Transfer Protocol, δηλαδή στο πρωτόκολλο που χρησιμοποιείται στον World Wide Web). (Blaze)

Ακόμη και όταν κλείσει η HTTP σύνδεση, ο ISP διατηρεί την TCP/IP σύνδεση στο Internet. Το μοντέλο client/server επιτρέπει στο επιτραπέζιο PC να τρέχει τον browser και να αναζητά πληροφορίες στο Internet αλλά και να έχει πρόσβαση στους host servers του Internet για την εκτέλεση λειτουργιών αναζήτησης και ανάκλησης πληροφοριών. Ουσιαστικά αυτή η αρχιτεκτονική επιτρέπει στον Web να θεωρείται ως ένα αποθηκευτικό μέσο και βάση δεδομένων απεριόριστης χωρητικότητας κατανεμημένα μεταξύ χιλιάδων υπολογιστών, οι οποίοι είναι προσβάσιμοι από οποιοδήποτε ανεξάρτητο PC. (Blaze)

Στο επίπεδο της φυσικής πρόσβασης (network access) ανήκουν τα πρωτόκολλα LAN όπως Ethernet, Token Ring, FDDI και πρωτόκολλα WAN όπως X.25, Frame Relay, SLIP, PPP που επιτρέπουν την φυσική διασύνδεση, την πρόσβαση στο μέσο και τον έλεγχο της ζεύξης.

- Στο επίπεδο δικτύου (network) χρησιμοποιείται το πρωτόκολλο IP, του οποίου τα πακέτα δρομολογούνται με ειδικές συσκευές, τους δρομολογητές (routers).

- Στο επίπεδο μεταφορά (transport) χρησιμοποιείται το πρωτόκολλο TCP και δευτερευόντως το UDP.

- Στο επίπεδο εφαρμογών (application) ανήκουν μεταξύ άλλων και τα πρωτόκολλα FTP, Telnet, SMTP, HTTP για την παροχή διάφορων υπηρεσιών όπως την μεταφορά αρχείων, την πρόσβαση σε υπολογιστές, ηλεκτρονικό ταχυδρομείο και το Web. (Blaze)

1.4 Το μοντέλο OSI

Το μοντέλο OSI υποδιαιρεί τις λειτουργίες ενός τηλεπικοινωνιακού δικτύου σε μια «κατακόρυφη» στοίβα από επίπεδα, για το καθένα από τα οποία μπορεί να οριστεί κάποιο πρωτόκολλο σε μία συγκεκριμένη υλοποίηση. Κάθε επίπεδο αξιοποιεί τις λειτουργίες του κατώτερού του στη στοίβα επιπέδου, ενω στόχος του είναι να παρέχει λειτουργικότητα στο αμέσως ανώτερο επίπεδό του. Μία συγκεκριμένη υλοποίηση του μοντέλου, με καθορισμένα πρωτόκολλα για κάθε επίπεδο, ονομάζεται στοίβα πρωτοκόλλων ή απλά στοίβα. Το κάθε πρωτόκολλο υλοποιείται είτε σε υλικό είτε σε λογισμικό. Συνήθως τα κατώτερα επίπεδα υλοποιούνται στο υλικό ενώ τα ανώτερα σε λογισμικό. (Blaze)

Το μοντέλο OSI είναι στενά συσχετισμένο με τον κλάδο της επιστήμης υπολογιστών και τη δικτύωση υπολογιστών. Το βασικό χαρακτηριστικό του είναι η διασύνδεση μεταξύ των επιπέδων, η οποία υπαγορεύει τις προδιαγραφές της αλληλεπίδρασής τους. Αυτό σημαίνει ότι ένα επίπεδο υλοποιημένο με κάποιο συγκεκριμένο πρωτόκολλο μπορεί να συνεργαστεί με το γειτονικό του στη στοίβα επίπεδο, το οποίο υλοποιείται με κάποιο άλλο πρωτόκολλο, υπό την προϋπόθεση ότι οι προδιαγραφές του καθενός έχουν δημοσιευθεί και έχουν γίνει αντιληπτές σωστά. Αυτές οι προδιαγραφές είναι τυπικά γνωστές ως RFC (Requests for Comments) και αποτελούν πρότυπα του Διεθνούς Οργανισμού Τυποποίησης ISO. (Blaze)

Συνήθως τα επίπεδα είναι αυστηρά διαχωρισμένα μεταξύ τους: αξιοποιούν τις υπηρεσίες του κατώτερου επιπέδου τους και προσφέρουν υπηρεσίες στο ανώτερό

τους, αλλά το καθένα δεν παρεμβαίνει στις λειτουργίες του άλλου· πιθανόν να μη γνωρίζει καν γι' αυτές. (Blaze)

Αυτός ο λογικός διαχωρισμός των επιπέδων διευκολύνει πολύ τη μελέτη της συμπεριφοράς των πρωτοκόλλων και επιτρέπει τη σχεδίαση πολύπλοκων και αξιόπιστων στοιβών πρωτοκόλλων. (Blaze)

Ορισμένες φορές όμως αυτή η αρχή ανεξαρτησίας των επιπέδων παραβιάζεται, για λόγους βελτιστοποίησης της απόδοσης ή αύξησης της λειτουργικότητας, με πρωτόκολλα διαφορετικών επιπέδων να συγχωνεύονται ή να παρεμβαίνουν το ένα στη λειτουργία του άλλου.

1.5 Το φυσικό επίπεδο πρόσβασής

Το φυσικό επίπεδο ορίζει όλες τις ηλεκτρικές και φυσικές προδιαγραφές της επικοινωνίας. Σ’ αυτές περιλαμβάνονται οι σχηματισμοί των ακίδων, οι επιτρεπτές τάσεις, οι προδιαγραφές των καλωδίων κλπ. (Blaze)

Συσκευές φυσικού επιπέδου είναι οι διανεμητές (αγγλ. hub), οι επαναλήπτες (αγγλ. repeater), οι κάρτες δικτύου (αγγλ. card), οι προσαρμοστές (αγγλ. adaptor) διαύλου (αγγλ. bus). Οι κυριότερες λειτουργίες και υπηρεσίες του φυσικού επιπέδου είναι: (Blaze)

- Έναρξη και τερματισμός της ηλεκτρικής σύνδεσης μιας επικοινωνιακής συσκευής.
- Συμμετοχή σε διαδικασίες όπου οι επικοινωνιακές συσκευές εξυπηρετούν αποτελεσματικά πολλούς χρήστες (πολυπλεξία). Επιλύονται προβλήματα προτεραιότητας πρόσβασης και ελέγχου ροής δεδομένων.
- Διαμόρφωση και αποδιαμόρφωση των ψηφιακών δεδομένων κατά τη μετάδοση από συσκευή σε συσκευή. Για παράδειγμα, τα ψηφιακά ηλεκτρικά σήματα μπορεί να ταξιδέψουν ως αναλογικά σε χάλκινο καλώδιο, μετά σε οπτική ίνα, μετά να μεταδοθούν από ραδιοζεύξη ή δορυφορικά, να φθάσουν πάλι αναλογικά σε χάλκινο καλώδιο και να γίνουν ψηφιακά στον παραλήπτη.

Οι παράλληλοι δίαυλοι SCSI λειτουργούν στο επίπεδο αυτό. Επίσης τα επίπεδα 1 και 2 αφορούν οι προδιαγραφές των πρωτοκόλλων Ethernet, Token Ring, FDDI (αγγλ.

Fiber Distributed Data Interface, Διασύνδεση Κατανεμημένων Δεδομένων με Οπτικές Ίνες) και IEEE 802.11. (Blaze)

1.6 Τα επίπεδα του διαδικτύου

1.6.1 Το επίπεδο φυσικής πρόσβασης.

Σε αυτό το επίπεδο ανήκουν οι εκάστοτε δικτυακές τεχνολογίες όπως Ethernet, FDDI και Token Ring. Το επίπεδο ασχολείται με την μετάδοση των bit μέσω διάφορων μέσων και αναλυτικότερα με τα ηλεκτρικά, μηχανικά και λειτουργικά χαρακτηριστικά των διασυνδέσεων. Επίσης ασχολείται με τον τρόπο που γίνεται η πρόσβαση στο φυσικό μέσον και καθορίζει τους κανόνες επικοινωνίας στο τοπικό δίκτυο. (Γκρίτζαλης)

1.6.2 Το επίπεδο δικτύου (IP PROTOCOL)

Η μετάδοση στο IP (Internet Protocol) γίνεται με την τεχνική των datagrams. Το κάθε datagram (πακέτο) φθάνει στον παραλήπτη διασχίζοντας ένα η περισσότερα διασυνδεόμενα IP δίκτυα, χωρίς να εξαρτάται από άλλα προηγούμενα ή επόμενα πακέτα. (Γκρίτζαλης)

Το IP, σαν πρωτόκολλο του τρίτου επιπέδου, δεν ασχολείται με τις φυσικές συνδέσεις ή τον έλεγχο των ενδιάμεσων ζεύξεων μεταξύ των κόμβων του δικτύου. Αυτά είναι αρμοδιότητα των χαμηλότερων επιπέδων. Στην ουσία ασχολείται με την διευθυνσιοδότητη, τον τεμαχισμό και την επανασυγκόληση των πακέτων. Το πρωτόκολλο IP δεν είναι αξιόπιστης μεταφοράς (reliable transfer) καθώς δεν εξασφαλίζει την σίγουρη παράδοση των πακέτων με τεχνικές επανεκπομπής και έλεγχο ροής. Επιπλέον είναι connectionless γιατί δεν απαιτεί την αποκατάσταση σύνδεσης μεταξύ των δύο σημείων πριν την ανταλλαγή δεδομένων. Τα IP πακέτα μπορεί να ακολουθήσουν διαφορετικές διαδρομές και να φθάσουν με λανθασμένη σειρά στον αποδέκτη. Προβλήματα σαν αυτό αναλαμβάνουν να διορθώσουν το πρωτόκολλο TCP του ανωτέρου επιπέδου. (Γκρίτζαλης)

1.6.3 Δρομολόγηση

Τα IP πακέτα διασχίζουν το Διαδίκτυο από δρομολογητή σε δρομολογητή με κατεύθυνση τον τελικό αποδέκτη. Κάθε δρομολογητής διατηρεί πίνακες δρομολόγησης βάσει των οποίων το κάθε πακέτο αποστέλλεται στον επόμενο δρομολογητή που θα αναλάβει να το προωθήσει προς τον αποδέκτη του. Ο

καθορισμός του επόμενου δρομολογητή γίνεται με την ανάγνωση της IP διευθύνσεως του παραλήπτη. Ανάλογα με το δίκτυο στο οποίο βρίσκεται ο παραλήπτης, επιλέγεται από τον πίνακα δρομολόγησης διαδεχόμενος router. (Γκρίτζαλης)

Όταν ένα πακέτο φθάσει σε ένα δρομολογητή αποθηκεύεται προσωρινά σε μία ουρά (queue). Τα IP πακέτα επεξεργάζονται με την σειρά άφιξης τους. Κατά την επεξεργασίας τους, διαβάζεται η διεύθυνση του τελικού παραλήπτη. Εάν υπάρχει μποτιλιάρισμα στο δίκτυο, τότε η ουρά των πακέτων μέσα στον δρομολογητή μπορεί να γίνει μεγάλη, αυξάνοντας έτσι τις καθυστερήσεις μετάδοσης. Σε περίπτωση που η ουρά γίνει τόσο μεγάλη που να ξεπερνά τις χωρητικές δυνατότητες του δρομολογητή, τα πακέτα απορρίπτονται και χάνονται. (Γκρίτζαλης)

1.6.4 Διευθυνσιοδότηση

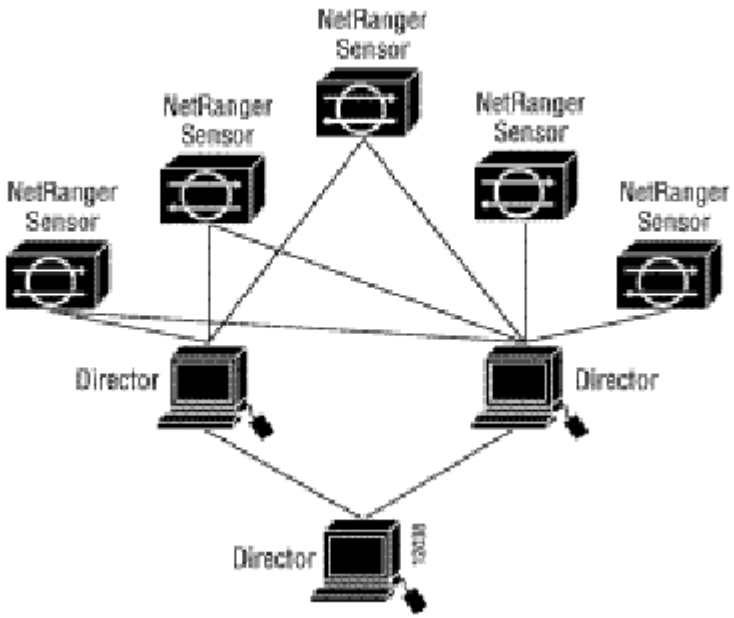
Καθ' ότι το Διαδίκτυο είναι μια εικονική κατασκευή που εφαρμόζεται λογισμικά, οι σχεδιαστές του είναι ελεύθεροι να διαλέξουν σχήμα διευθυνσιοδότησης που να μην σχετίζεται με κανένα υπάρχον δικτυακό υλικό. Το IP λειτουργεί με βάσει ένα νέο σετ διευθύνσεων που είναι ανεξάρτητο από τις υποκείμενες δικτυακές διευθύνσεις των υπολογιστών. Οι νέες αυτές διευθύνσεις καλούνται Internet Addresses ή IP διευθύνσεις. (Γκρίτζαλης)

Οι IP διευθύνσεις είναι φτιαγμένες έτσι ώστε να διευκολύνουν την δρομολόγηση. Κάθε IP πακέτο περιέχει την διεύθυνση του αποστολέα και του παραλήπτη, κάθε μια από τις οποίες έχει μήκος 32 bits. Μια IP διεύθυνση αποτελείται από δύο μέρη: το netid και το hostid. Το netid προσδιορίζει το δίκτυο στο οποίο βρίσκεται ο υπολογιστής, ενώ το hostid προσδιορίζει τον υπολογιστή. Ανάλογα με το μήκος της διευθύνσεως που αφιερώνεται σε κάθε τμήμα αυτής, οι διευθύνσεις διακρίνονται σε τρεις κλάσεις δικτύων: (Γκρίτζαλης)

- Κλάση Α: 8 bit διεύθυνση δικτύου / 24 bit διεύθυνση υπολογιστή
- Κλάση Β: 16 bit διεύθυνση δικτύου / 16 bit διεύθυνση υπολογιστή
- Κλάση Γ: 24 bit διεύθυνση δικτύου / 8 bit διεύθυνση υπολογιστή

Επειδή οι IP διευθύνσεις κωδικοποιούν ένα δίκτυο αλλά και έναν υπολογιστή σε αυτό το δίκτυο, δεν καθορίζουν έναν συγκεκριμένο υπολογιστή, αλλά μία σύνδεση σε ένα δίκτυο.

Στην πράξη η απομνημόνευση των 32 bits είναι εξαιρετικά δύσκολη. Γι' αυτό έχει επινοηθεί η αναπαράσταση της διεύθυνσης με την χρήση δεκαδικών αριθμών. Η διεύθυνση διαχωρίζεται με τελείες σε τέσσερα πεδία των οκτώ bit. Κάθε πεδίο μετατρέπεται στο ισοδύναμο δεκαδικό αριθμό, όπως φαίνεται στο παρακάτω σχήμα. (Γκρίτζαλης)



Εικόνα 1 Internet Control Message Protocol (ICMP)

Ένα άλλο πρωτόκολλο αυτού του επιπέδου είναι το Internet Control Message Protocol (ICMP). Το ICMP δρα βοηθητικά, παράγοντας και διαχειρίζοντας μηνύματα λάθους για το πακέτο πρωτοκόλλων TCP/IP. Επιτρέπει στους δρομολογητές να επιστρέφουν μηνύματα λάθους σε άλλους δρομολογητές ή υπολογιστές. Για παράδειγμα, εάν ζητηθεί η σύνδεση με υπολογιστή που δεν υπάρχει ή δεν είναι διαθέσιμος προς το παρών, το ICMP σε κάποιον router θα επιστρέψει στον αποστολέα του αρχικού μηνύματος ένα μήνυμα με περιεχόμενο "host unreachable". Επιπλέον, το ICMP μπορεί να χρησιμοποιηθεί για την συλλογή πληροφοριών για ένα δίκτυο και για σκοπούς debugging. Περαιτέρω και πιο αναλυτικές λεπτομέρειες για το ICMP υπάρχουν στο RFC 792. (Γκρίτζαλης)

1.6.5 Το επίπεδο μεταφοράς

Το επίπεδο μεταφοράς διεκπεραιώνει τη μεταφορά των δεδομένων από χρήστη σε χρήστη, απαλλάσσοντας έτσι τα ανώτερα επίπεδα από κάθε φροντίδα να προσφέρουν

αξιόπιστη και μεταφορά ο ένα άκρο της επικοινωνίας στο άλλο. Το επίπεδο μεταφοράς ελέγχει την αξιοπιστία ενός χρησιμοποιούμενου καναλιού με έλεγχο ροής (αγγλ. flow control), κατάτμηση και τμηματοποίηση (αγγλ. segmentation / desegmentation), καθώς και έλεγχο σφαλμάτων (αγγλ. error control). Ορισμένα πρωτόκολλα καταγράφουν καταστάσεις και συνδέσεις, οπότε κρατούν λογαριασμό των πακέτων και επανεκπέμπουν αυτά που δεν παρελήφθησαν σωστά. Τα διάφορα πρωτόκολλα μορφοποιούν διαφορετικά τα εκπεμπόμενα πακέτα πληροφοριών, αλλά τα προς αποστολή δεδομένα παραλαμβάνονται αρχικά από τα ανώτερα επίπεδα. (Γκρίτζαλης)

Το συνηθέστερο παράδειγμα πρωτοκόλλου μεταφοράς είναι το TCP (αγγλ. Transmission Control Protocol, πρωτόκολλο ελέγχου μετάδοσης). Άλλα πρωτόκολλα μεταφοράς είναι τα UDP (αγγλ. User Datagram Protocol, πρωτόκολλο για ασυνδεσμική αποστολή δεδομένων, SCTP (αγγλ. Stream Control Transmission Protocol, πρωτόκολλο ελέγχου της ροής μετάδοσης), κλπ. (Γκρίτζαλης)

Το TCP (Transmission Control Protocol - Πρωτόκολλο Ελέγχου Μεταφοράς) είναι ένα από τα κυριότερα πρωτόκολλα της Σουίτας Πρωτοκόλλων Διαδικτύου. Βρίσκεται πάνω από το IP protocol (πρωτόκολλο IP). Οι κύριοι στόχοι του πρωτοκόλλου TCP είναι να επιβεβαιώνεται η αξιόπιστη αποστολή και λήψη δεδομένων, επίσης να μεταφέρονται τα δεδομένα χωρίς λάθη μεταξύ του στρώματος δικτύου (network layer) και του στρώματος εφαρμογής (application layer) και, φτάνοντας στο πρόγραμμα του στρώματος εφαρμογής, να έχουν σωστή σειρά. Οι περισσότερες σύγχρονες υπηρεσίες στο Διαδίκτυο βασίζονται στο TCP. Για παράδειγμα το SMTP (port 25), το παλαιότερο (και μη-ασφαλές) Telnet (port 23), το FTP και πιο σημαντικό το HTTP (port 80), γνωστό ως υπηρεσίες World Wide Web (WWW - Παγκόσμιος Ιστός). Το TCP χρησιμοποιείται σχεδόν παντού, για αμφίδρομη επικοινωνία μέσω δικτύου. (Γκρίτζαλης)

Το πρωτόκολλο User Datagram Protocol (UDP) είναι ένα από τα βασικά πρωτόκολλα που χρησιμοποιούνται στο Διαδίκτυο. Μία εναλλακτική ονομασία του πρωτοκόλλου είναι Universal Datagram Protocol. Διάφορα προγράμματα χρησιμοποιούν το πρωτόκολλο UDP για την αποστολή σύντομων μηνυμάτων (γνωστών και ως datagrams) από τον έναν υπολογιστή στον άλλον μέσα σε ένα δίκτυο υπολογιστών.

Ένα από τα κύρια χαρακτηριστικά του UDP είναι ότι δεν εγγυάται αξιόπιστη επικοινωνία. Τα πακέτα UDP που αποστέλλονται από έναν υπολογιστή μπορεί να φτάσουν στον παραλήπτη με λάθος σειρά, διπλά ή να μην φτάσουν καθόλου εάν το δίκτυο έχει μεγάλο φόρτο. Αντιθέτως, το πρωτόκολλο TCP διαθέτει όλους τους απαραίτητους μηχανισμούς ελέγχου και επιβολής της αξιοπιστίας και συνεπώς μπορεί να εγγυηθεί την αξιόπιστη επικοινωνία μεταξύ των υπολογιστών. Η έλλειψη των μηχανισμών αυτών από το πρωτόκολλο UDP το καθιστά αρκετά πιο γρήγορο και αποτελεσματικό, τουλάχιστον για τις εφαρμογές εκείνες που δεν απαιτούν αξιόπιστη επικοινωνία. (Γκρίτζαλης)

Οι εφαρμογές audio και video streaming χρησιμοποιούν κατά κόρον πακέτα UDP. Για τις εφαρμογές αυτές είναι πολύ σημαντικό τα πακέτα να παραδοθούν στον παραλήπτη σε σύντομο χρονικό διάστημα ούτως ώστε να μην υπάρχει διακοπή στην ροή του ήχου ή της εικόνας. Κατά συνέπεια προτιμάται το πρωτόκολλο UDP διότι είναι αρκετά γρήγορο, παρόλο που υπάρχει η πιθανότητα μερικά πακέτα UDP να χαθούν. Στην περίπτωση που χαθεί κάποιο πακέτο, οι εφαρμογές αυτές διαθέτουν ειδικούς μηχανισμούς διόρθωσης και παρεμβολής ούτως ώστε ο τελικός χρήστης να μην παρατηρεί καμία αλλοίωση ή διακοπή στην ροή του ήχου και της εικόνας λόγω του χαμένου πακέτου. Σε αντίθεση με το πρωτόκολλο TCP, το UDP υποστηρίζει broadcasting, δηλαδή την αποστολή ενός πακέτου σε όλους τους υπολογιστές ενός δικτύου, και multicasting, δηλαδή την αποστολή ενός πακέτου σε κάποιους συγκεκριμένους υπολογιστές ενός δικτύου. Η τελευταία δυνατότητα χρησιμοποιείται πολύ συχνά στις εφαρμογές audio και video streaming ούτως ώστε μία ροή ήχου ή εικόνας να μεταδίδεται ταυτόχρονα σε πολλούς συνδρομητές. Μερικές σημαντικές εφαρμογές που χρησιμοποιούν πακέτα UDP είναι οι εξής: Domain Name System (DNS), IPTV, Voice over IP (VoIP), Trivial File Transfer Protocol (TFTP) και τα παιχνίδια που παίζονται ζωντανά μέσω του Διαδικτύου. (Γκρίτζαλης)

1.6.6 Το επίπεδο εφαρμογών

Το επίπεδο εφαρμογών παρέχει στον χρήστη έναν τρόπο να προσπελάσει μέσω μιας εφαρμογής τις πληροφορίες ενός δικτύου. Αυτό το επίπεδο είναι η κύρια διασύνδεση του χρήστη με την εφαρμογή και, συνεπώς, με το δίκτυο. Στο επίπεδο αυτό γίνεται η διαχείριση των κατανεμημένων εφαρμογών, η αποστολή του ηλεκτρονικού ταχυδρομείου κλπ. Παραδείγματα πρωτοκόλλων επιπέδου εφαρμογών αποτελούν τα Telnet, FTP, SMTP και http. (Γκρίτζαλης)

Το ηλεκτρονικό ταχυδρομείο (αγγλικά e-mail, email ή mail προφέρεται "ιμέιλ" ή "μέιλ" αντίστοιχα) είναι μια μέθοδος συγγραφής, αποστολής, λήψης και αποθήκευσης μηνυμάτων με χρήση ηλεκτρονικών συστημάτων τηλεπικοινωνιών. Γενικά ο όρος "ηλεκτρονικό ταχυδρομείο" αναφέρεται στο σύστημα ηλεκτρονικού ταχυδρομείου του Διαδικτύου που χρησιμοποιεί το Simple Mail Transfer Protocol πρωτόκολλο, σε δικτυακά συστήματα που βασίζονται σε άλλα πρωτόκολλα μεταφοράς μηνυμάτων, αλλά και σε διάφορα συστήματα μηνυμάτων σε μικρά δίκτυα, υπερυπολογιστές, κλπ που επιτρέπουν στους χρήστες τους να στέλνουν μηνύματα μεταξύ τους για την υποστήριξη ομαδικής συνεργασίας. Τα συστήματα σε τοπικά δίκτυα ή σε δίκτυα intranet είναι πιθανόν να βασίζονται σε ιδιωτικά πρωτόκολλα, που υποστηρίζονται από το συγκεκριμένο σύστημα, ή να είναι τα ίδια πρωτόκολλα που χρησιμοποιούνται στα δημόσια δίκτυα. Το ηλεκτρονικό ταχυδρομείο χρησιμοποιείται συχνά για τη μεταφορά ανεπιθύμητων μηνυμάτων σε μεγάλο όγκο (σπάμ (spam)), αλλά υπάρχουν προγράμματα που μπορούν να "φιλτράρουν" και να σταματήσουν ή να σβήσουν αυτόματα τα περισσότερα από αυτά. (Γκρίτζαλης)

Ο User Agent (UA) είναι το πρόγραμμα client στον υπολογιστή του χρήστη που αναλαμβάνει την διαχείριση και ανάκτηση του ταχυδρομείου. Με την βοήθεια αυτού του προγράμματος ο χρήστης γράφει τα μηνύματα του, τα στέλνει, παραλαμβάνει άλλα μηνύματα και τα διαβάζει. Ο Mail Transfer Agent (MTA) παραλαμβάνει τα μηνύματα από τον UA και τα προωθεί στον επόμενο MTA μέχρι να βρεθεί ο MTA που έχει άμεση σύνδεση με τον υπολογιστή του χρήστη. Ο τελευταίος MTA επικοινωνεί με τον UA του παραλήπτη για την παράδοση των μηνυμάτων. Το σύνολο των MTA καλείται Message Transfer System (MTS). (Γκρίτζαλης)

Η επικοινωνία από MTA σε MTA γίνεται με χρήση του πρωτοκόλλου SMTP (Simple Mail Transfer Protocol, ενώ η επικοινωνία του UA με τον MTA γίνεται με χρήση των πρωτοκόλλων POP (Post Office Protocol) και IMAP (Internet Message Access Protocol). Τα ίδια τα μηνύματα συντάσσονται με βάσει το πρωτόκολλο MIME (Multipurpose Internet Mail Extensions) ή με το RFC822.Το παραπάνω σύστημα παράδοσης του ηλεκτρονικού ταχυδρομείου επιτρέπει το ηλεκτρονικό ταχυδρομικό του χρήστη να βρίσκεται σε κάποιον server και έτσι δεν είναι απαραίτητο να είναι εν λειτουργία ο υπολογιστή του αποδέκτη κατά την αποστολή του μηνύματος. Ο αποδέκτης θα παραλάβει τα μηνύματα του όταν ανοίξει τον υπολογιστή του και συνδεθεί με τον server (MTA). (Γκρίτζαλης)

Το File Transfer Protocol (FTP), (ελληνικά: Πρωτόκολλο Μεταφοράς Αρχείων) είναι ένα ευρέως χρησιμοποιούμενο πρωτόκολλο σε δίκτυα τα οποία υποστηρίζουν το πρωτόκολλο TCP/IP (δίκτυα όπως internet ή intranet). Ο υπολογιστής που τρέχει εφαρμογή FTP client μόλις συνδεθεί με τον server μπορεί να εκτελέσει ένα πλήθος διεργασιών όπως ανέβασμα αρχείων στον server, κατέβασμα αρχείων από τον server, μετονομασία ή διαγραφή αρχείων από τον server κ.ο.κ. Το πρωτόκολλο είναι ένα ανοιχτό πρότυπο. Είναι δυνατό κάθε υπολογιστής που είναι συνδεδεμένος σε ένα δίκτυο, να διαχειρίζεται αρχεία σε ένα άλλο υπολογιστή του δικτύου, ακόμη και εάν ο δεύτερος διαθέτει διαφορετικό λειτουργικό σύστημα. (Γκρίτζαλης)

Το Simple Mail Transfer Protocol (SMTP) έχει καθιερωθεί για την μετάδοση μηνυμάτων ηλεκτρονικού ταχυδρομείου στο Διαδίκτυο. Επίσημα περιγράφεται στα έγγραφα RFC821 και RFC1123. Το πρωτόκολλο που χρησιμοποιείται σήμερα αποτελεί επέκταση του αρχικού προτύπου και περιγράφεται στο έγγραφο RFC 2821.

Το Πρωτόκολλο Μεταφοράς Υπερκειμένου (HyperText Transfer Protocol, HTTP) είναι η κύρια μέθοδος που χρησιμοποιούν τα πρωτόκολλα του Παγκοσμίου Ιστού για να μεταφέρουν δεδομένα ανάμεσα σε έναν διακομιστή (server) και ένα πελάτη (client).Η ανάπτυξη του HTTP έγινε υπό την εποπτεία του World Wide Web Consortium και του Internet Engineering Task Force (IETF).Το HTTP είναι ο συνήθης για τη διεκπαιρέωση αιτήσεων/απαντήσεων μεταξύ ενός υπολογιστή πελάτη (client) και ενός εξυπηρέτη (server). Πελάτης ονομάζεται ο τελικός χρήστης, και ο εξυπηρέτης είναι η εκάστοτε ιστοσελίδα. (Γκρίτζαλης)

2 ΚΕΦΑΛΑΙΟ Η ΠΡΟΣΤΑΣΙΑ ΑΠΟ ΤΙΣ ΑΠΕΙΛΕΣ ΣΤΟ ΔΙΑΔΙΚΤΥΟ ΜΕ ΤΗΝ ΧΡΗΣΗ ΜΕΣΩΝ ΑΣΦΑΛΕΙΑΣ FIREWALL

2.1 Η λειτουργία των firewall

Η κύρια λειτουργία ενός firewall είναι η ρύθμιση της κυκλοφορίας δεδομένων ανάμεσα σε δύο δίκτυα υπολογιστών. Συνήθως τα δύο αυτά δίκτυα είναι το Διαδίκτυο και το τοπικό/εταιρικό δίκτυο. Ένα firewall παρεμβάλλεται ανάμεσα σε δύο δίκτυα που έχουν διαφορετικό επίπεδο εμπιστοσύνης. Το διαδίκτυο έχει μικρό βαθμό εμπιστοσύνης (low level of trust), ενώ το εταιρικό δίκτυο ή το δίκτυο ενός σπιτιού διαθέτει τον μέγιστο βαθμό εμπιστοσύνης. Ένα περιμετρικό δίκτυο (perimeter network) ή μία Demilitarized Zone (DMZ) διαθέτουν μεσαίο επίπεδο εμπιστοσύνης. (Cisco Press)

Ο σκοπός της τοποθέτησης ενός firewall είναι η πρόληψη επιθέσεων στο τοπικό δίκτυο και η αντιμετώπισή τους. Παρόλα αυτά όμως, ένα firewall μπορεί να αποδειχθεί άχρηστο εάν δεν ρυθμιστεί σωστά. Η σωστή πρακτική είναι το firewall να ρυθμίζεται ούτως ώστε να απορρίπτει όλες τις συνδέσεις εκτός αυτών που επιτρέπει ο διαχειριστής του δικτύου (default-deny). Για να ρυθμιστεί σωστά ένα firewall θα πρέπει ο διαχειριστής του δικτύου να έχει μία ολοκληρωμένη εικόνα για τις ανάγκες του δικτύου και επίσης να διαθέτει πολύ καλές γνώσεις πάνω στα δίκτυα υπολογιστών. Πολλοί διαχειριστές δεν έχουν αυτά τα προσόντα και ρυθμίσουν το firewall ούτως ώστε να δέχεται όλες τις συνδέσεις εκτός από εκείνες που ο διαχειριστής απαγορεύει (default-allow). Η ρύθμιση αυτή καθιστά το δίκτυο ευάλωτο σε επιθέσεις από εξωτερικούς χρήστες. (Cisco Press)

2.2 Ιστορικά στοιχεία

Ο όρος firewall είναι αρκετά παλιός. Πρωτοεμφανίστηκε στις αρχές του 20ού αιώνα, όταν οι άνθρωποι χρησιμοποιούσαν στα σπίτια τους τούβλα για τους εσωτερικούς τοίχους ούτως ώστε να τα κάνουν πιο ανθεκτικά στην διάδοση της φωτιάς. Σήμερα ο όρος αυτός έφτασε να σημαίνει το λογισμικό ή υλικό που παρεμβάλλεται μεταξύ δικτύων υπολογιστών ούτως ώστε να αποτρέψει την διάδοση ιών, δούρειων ίππων και τις επιθέσεις από κακόβουλους χρήστες. (Cisco Press)

Η τεχνολογία του firewall εμφανίστηκε στα τέλη της δεκαετίας του 1980, όταν ακόμη το Διαδίκτυο ήταν σε πρώιμα στάδια. Εκείνη την εποχή είχαν παρατηρηθεί αρκετές "τρύπες" ασφαλείας στο Διαδίκτυο οπότε έπρεπε να βρεθεί μία λύση. Η λύση αυτή ήταν η δημιουργία της τεχνολογίας firewall. (Cisco Press)

2.2.1 1η γενιά - Φίλτρα πακέτων

Το πρώτο ερευνητικό δημοσίευμα πάνω στην τεχνολογία firewall προέκυψε το 1988 όταν οι μηχανικοί της DEC (Digital Equipment Corporation) ανέπτυξαν φίλτρα πακέτων δεδομένων (data packet filters). Τα φίλτρα αυτά θεωρούνται ως η πρώτη γενιά firewall.Τα φίλτρα πακέτων δρουν ως εξής: (Cisco Press)

Διαβάζουν τα πακέτα δεδομένων που διακινούνται από το ένα δίκτυο στο άλλο και, εάν κάποιο πακέτο ταιριάζει με κάποιο συγκεκριμένο κανόνα, τότε το απορρίπτουν. (Cisco Press)

Ο διαχειριστής του δικτύου είναι σε θέση να ορίσει τους κανόνες βάσει των οποίων θα απορρίπτονται τα πακέτα. Αυτός ο τύπος firewall δεν ενδιαφέρεται για το εάν κάποιο πακέτο ανήκει σε μία σύνδεση, δηλαδή δεν αποθηκεύει πληροφορίες σχετικά με την κατάσταση των διαφόρων συνδέσεων από το ένα δίκτυο στο άλλο (stateless packet filtering). Αντιθέτως, φιλτράρει κάθε πακέτο με βάση την πληροφορία που περιέχεται στο ίδιο το πακέτο (π.χ. διεύθυνση IP προέλευσης, διεύθυνση IP προορισμού, πρωτόκολλο, αριθμός θύρας κοκ). Επειδή τα πρωτόκολλα TCP και UDP χρησιμοποιούν τις ευρέως διαδεδομένες θύρες (Well known ports), ένα firewall πρώτης γενιάς μπορεί να ξεχωρίσει τα πακέτα που αφορούν διάφορες λειτουργίες, όπως για παράδειγμα το email, την μεταφορά αρχείων, την περιήγηση στο Διαδίκτυο κοκ. (Cisco Press)

2.2.2 2η γενιά - Φίλτρα κατάστασης

Η δεύτερη γενιά firewall αναπτύχθηκε από τρεις ερευνητές στα εργαστήρια της AT&T Bell: Dave Presetto, Howard Trickey και Kshitij Nigam. Τα firewall της δεύτερης γενιάς δρουν όπως τα firewall πρώτης γενιάς με κάποιες επιπρόσθετες λειτουργίες. (Cisco Press)

Μία από αυτές είναι το γεγονός ότι πλέον εξετάζουν και την κατάσταση (state) του κάθε πακέτου, δηλαδή την σύνδεση από την οποία προήλθε. Για τον λόγο αυτό και αναφέρονται ως φίλτρα κατάστασης (stateful firewalls). Τα φίλτρα αυτά κρατούν ανά

πάσα στιγμή πληροφορίες για τον αριθμό και το είδος των συνδέσεων μεταξύ των δύο δικτύων και επιπλέον μπορούν να ξεχωρίσουν εάν ένα πακέτο αποτελεί την αρχή ή το τέλος μία νέας σύνδεσης ή μέρος μίας ήδη υπάρχουσας.Οι διαχειριστές τέτοιων firewalls μπορούν να ορίσουν τους κανόνες βάσει των οποίων θα επιτρέπεται η δημιουργία συνδέσεων από το εξωτερικό δίκτυο (Διαδίκτυο) προς το τοπικό/εταιρικό δίκτυο. Με τον τρόπο αυτό γίνεται πιο εύκολη η πρόληψη διαφόρων ειδών επιθέσεων, όπως για παράδειγμα ή επίθεση SYN flood. (Cisco Press)

2.2.3 3η γενιά - Επίπεδο εφαρμογών

Η τρίτη γενιά firewall βασίζεται πλέον στο επίπεδο εφαρμογών σύμφωνα με το μοντέλο αναφοράς OSI (Open Systems Interconnection). Το κύριο χαρακτηριστικό αυτής της γενιάς firewall είναι ότι μπορεί να αντιλαμβάνεται ποια προγράμματα και πρωτόκολλα προσπαθούν να δημιουργήσουν μία νέα σύνδεση (πχ FTP - File Transfer Protocon, DNS - Domain Name System, περιήγηση στο Διαδίκτυο κοκ). Με τον τρόπο αυτό μπορούν να εντοπιστούν εφαρμογές που προσπαθούν να δημιουργήσουν ανεπιθύμητες συνδέσεις ή καταχρήσεις ενός πρωτοκόλλου ή μίας υπηρεσίας. (Cisco Press)

2.3 Ορισμός του firewall

Είναι ένας συνδυασμός υλικού και λογισμικού που απομονώνει το εσωτερικό δίκτυο ενός υπολογιστή από το υπόλοιπο διαδίκτυο, επιτρέποντας σε ορισμένα πακέτα να περνούν και μπλοκάροντας άλλα πακέτα. Ένα firewall επιτρέπει σε ένα διαχειριστή δικτύου να ελέγχει την προσπέλαση ανάμεσα στον έξω κόσμο και στους πόρους μέσα στο διαχειριζόμενο δίκτυο, διαχειριζόμενο την κίνηση προς και από αυτούς τους πόρους ω

Υπάρχουν δύο τύποι firewalls: firewalls φιλτραρίσματος πακέτων (τα οποία λειτουργούν στο επίπεδο δικτύου) και firewalls επιπέδου εφαρμογής (τα οποία λειτουργούν στο επίπεδο εφαρμογής). Τα firewalls ελέγχουν τα εισερχόμενα και εξερχόμενα πακέτα δεδομένων και σύμφωνα με τους κανόνες που έχουν οριστεί από τον διαχειριστή του δικτύου επιτρέπουν να συνεχίσουν την πορεία τους ή διαφορετικά την φράζουν. (Cisco Press)

Τα firewalls επιτρέπουν την πρόσβαση σε εξουσιοδοτημένους χρήστες ενώαποκλείουν εκείνους οι οποίοι δεν έχουν δικαιώματα πρόσβασης. Γενικά αποτελεί

ένα σύστημα το οποίο προστατεύει από την μη εξουσιοδοτημένη πρόσβαση προς ή από σε ένα ιδιωτικό δίκτυο.Firewalls μπορούν να υλοποιηθούν είτε με hardware είτε με software ή μεμσυνδυασμό αυτών των δύο. Σήμερα firewalls χρησιμοποιούνται συχνά για να εμποδίζουν χρήστες του Internet να προσπελάσουν ιδιωτικά δίκτυα που συνδέονται με το Internet και ειδικότερα τα intranets. Όλα τα μηνύματα τα οποία εισέρχονται ήφεύγουν από το intranet περνούν διαμέσου του firewall, το οποίο εξετάζει κάθε μήνυμα και εμποδίζει να συνεχίσουν εκείνα τα οποία δεν ικανοποιούν δοθέντα κριτήρια. Μπορούμε να φανταστούμε ως firewall την πρώτη γραμμή της άμυνας στηνπροστασία ιδιωτικής πληροφορίας. Στην συνέχεια για μεγαλή ασφάλεια η πληροφορία θα πρέπει να κρυπρογραφηθεί. (Cisco Press)

2.4 Σχεδίαση και υλοποίηση ενός firewall

Κατά την σχεδίαση ενός firewall υπάρχουν ορισμένα στοιχεία τα οποία θα πρέπει να ληφθούν υπόψη. Τα στοιχεία αυτά αφορούν περισσότερο την πολιτική που θέλει να ακολουθήσει ένας οργανισμός για την πρόσβαση του στο Internet και όχι τόση στο καθαρά τεχνικό κομμάτι. Έτσι θα πρέπει να οριστούν αρχικά οι υπηρεσίες οι οποίες θέλουμε να περνούμε διαμέσου του firewall και ποιοί θα έχουν πρόσβαση σε αυτές. Θα πρέπει να διευκρινιστεί αν το επιδιωκόμενο είναι μία λεπτομερής και αναλυτική πρόσβαση ή το απλό φιλτράρισμα. (Dahlin)

Αφού οριστεί η πολιτική που θα ακολουθηθεί στο firewall στο επόμενο στάδιο δημιουργείται μια λίστα από το τι θα πρέπει να παρακολουθείται και να ελέγχεται και από το τι θα επιτρέπεται ή θα απορρίπτεται. Στο τρίτο μέρος θα πρέπει να ληφθούν υπόψη τα οικονομικά στοιχεία της υλοποίησης ενός firewall. Στο σημείο αυτό υπάρχει αρκετή ασάφεια σχετικά με το κόστος της αγοράς ή το κόστος της κατασκευής. Έτσι υπάρχουν λύσεις οι οποίες περιλαμβάνουν την αγορά ενός router ή τον προγραμματισμό ενός Unix συστήματος. Η κατασκευή ενός firewall εξειδικευμένου στις ανάγκες ενός Οργανισμού μπορεί να απασχολήσει προσωπικό για αρκετούς μήνες και πάλι να μην υπάρχει η δυνατότητα να ελεγχθεί σε όλα του τα σημεία. Είναι φανερό όμως ότι θα λάβει υπόψη της η λύση αυτή καλύτερα όλες τις ειδικές ανάγκες Οργανισμού και το αποτέλεσμα αναμένεται καλύτερα προσαρμοσμένο σε αυτόν. (Dahlin)

2.5 **Αδυναμίες ενός** firewall

Ένα firewall δεν αποτελεί ολοκληρωμένη λύση ασφαλείας. Για την κάλυψη κάποιων απειλών απαιτούνται άλλες συμπληρωματικές ενέργειες, όπως: (Dahlin)

1. Μηχανισμοί φυσικής προστασίας

2. Ενσωμάτωση ασφάλειας σε επίπεδο εξυπηρετητή

3. Εκπαίδευση των χρηστών στο πλαίσιο του συνολικού πλάνου ασφάλειας.

Οι αδυναμίες των firewall είναι οι εξής:

1. Δεν μπορεί να προστατέψει από συνδέσεις που δεν διέρχονται από αυτό: παρέχει πλήρη προστασία μόνο αν ελέγχει όλη την περίμετρο του περιβάλλοντος. Για παράδειγμα να επιτρέπεται σε εσωτερικούς χρήστες συνδέονται με απευθείας PPP συνδέσεις με το Internet. Άλλο παράδειγμα αποτελεί ένα site που επιτρέπει ελεύθερα την πρόσβαση στους εσωτερικούς υπολογιστές και ελέγχει μόνο τα εξωτερικά αιτήματα. (Dahlin)

2. Δεν μπορεί να προστατεύσει από προγράμματα-ιούς: τα firewalls δεν ασκούν σε βάθος έλεγχο των δεδομένων που εισέρχονται στο δίκτυο. Ο έλεγχος αφορά στις διευθύνσεις και στις θύρες πηγής και προορισμού και όχι στις λεπτομέρειες των δεδομένων. Έτσι απαιτείται σε κάθε υπολογιστή και ιδιαίτερα στους servers η χρήση antivirus λογισμικού. (Dahlin)

3. Δεν μπορεί να προστατεύσει από επιθέσεις κακόβουλων χρηστών από το εσωτερικό του οργανισμού: Οι εσωτερικές απειλές απαιτούν εσωτερικά μέτρα ασφάλειας, όπως ασφάλεια σε επίπεδο ξενιστή (host)και εκπαίδευση των χρηστών. Οι χρήστες πρέπει να ενημερωθούν σχετικά με τις διάφορες απειλές, τη σημασία της μυστικότητας του συνθηματικού τους και περιοδικής αλλαγής του. (Dahlin)

4. Δεν μπορεί να προστατέψει τον οργανισμό από επιθέσεις σχετιζόμενες με δεδομένα: συμβαίνουν όταν φαινομενικώς ακίνδυνα δεδομένα εισάγονται σε κάποιον από τους εξυπηρετητές του οργανισμού, είτε μέσω e-mail,είτε διαμέσου της αντιγραφής από δισκέτα και εκτελούνται με σκοπό να εξαπολύσουν επίθεση εναντίον του συστήματος. Π.χ. μια επίθεση θα μπορούσε να οδηγήσει σε μεταβολή των αρχείων προνομίων. (Dahlin)

5. Δεν μπορεί να προστατεύσει από απειλές άγνωστου τύπου: δεν μπορεί να αμυνθεί αυτομάτως σε νέες απειλές που προκύπτουν κατά καιρούς. (Dahlin)

6. Η αυστηρή ρύθμιση ασφάλειας διαμέσου του firewall: είναι δυνατό ένα firewall να ρυθμιστεί με πολύ αυστηρό τρόπο με αποτέλεσμα να μην επιτρέπει τη δικτύωσης ή να προκαλεί δυσαρέσκεια στους χρήστες εξαιτίας των πολλών ελέγχων, των πολλαπλών επιπέδων ασφαλείας και κατά συνέπεια της συνολικής ελαττωμένης φιλικότητας και μειωμένης ευχρηστίας . (Dahlin)

2.6 Ζητήματα σχεσίασης των firewall

Η υλοποίηση ενός firewall δεν αποτελεί τετριμμένο θέμα και δεν παρέχεται ενσωματωμένη σε κανένα λειτουργικό σύστημα. Ο λόγος είναι ότι ένα firewall αποτελεί περισσότερο φιλοσοφία προστασίας και λιγότερο υλικό και λογισμικό που παρέχει πλήρη προστασία από κάθε εξωτερική απειλή. Υπάρχει μια αντίληψη ότι το firewall εξασφαλίζει την πλήρη προστασία ενός δικτύου απέναντι σε κάθε είδους απειλή η οποία είναι τελείως λανθασμένη και μπορεί να οδηγήσει το διαχειριστή ασφάλειας ενός οργανισμού στην καταστροφική άποψη ότι με την εγκατάσταση ενός firewall είναι εγγυημένη η ασφάλεια του εσωτερικού δικτύου του οργανισμού την οποία διαχειρίζεται. (CERT)

Η εγκατάσταση ενός firewall αποτελεί σημαντική σχεδιαστική απόφαση για τους παρακάτω λόγους:

1) Η εγκατάσταση ενός firewall επιφέρει καθυστέρηση στο χρόνο απόκρισης των προγραμμάτων που υλοποιούν τις υπηρεσίες που παρέχει η ιστοθέση.

2.7 Εγκατάσταση ενός firewall

Η εγκατάσταση ενός firewall περιλαμβάνει μια σειρά διαδοχικά εκτελούμενων φάσεων. Αυτές είναι: (CERT)

2.7.1 Σχεδιασμός Πολιτικής.

Ο σχεδιασμός ενός firewall προϋποθέτει τον ακριβή προσδιορισμό των ορίων των διακριτών περιοχών ασφάλειας του δικτύου, καθεμιά από τις οποίες λειτουργεί με βάση συγκεκριμένη πολιτική ασφάλειας. Στη συνέχεια επιλέγονται:

- Η βασική αρχιτεκτονική (αριθμός υπολογιστών, μέθοδοι συνδέσεων, λειτουργίες που εκτελούνται).
- Οι λειτουργίες που θα υλοποιηθούν (επίπεδο δικτύου, επίπεδο εφαρμογής, υβριδικός συνδυασμός).
- Το αρχιτεκτονικό σχέδιο του firewall (διπλοσυνδεδεμένο, με υπολογιστή διαλογής, με υποδίκτυο διαλογής). (CERT)

Στη φάση αυτή εξασφαλίζεται η ύπαρξη του κατάλληλου εξοπλισμού (υλικό και λογισμικό), για να είναι δυνατή η εγκατάσταση, ο δοκιμαστικός έλεγχος, η λειτουργία και η επίβλεψη του firewall. Συγκεκριμένα εκτελείται: (CERT)

- Προσδιορισμός των απαραίτητων τμημάτων υλικού (υπολογιστές, δρομολογητές, επεξεργαστές, μνήμη, δίσκος, κάρτες, καλώδια κλπ).
- Προσδιορισμός των απαραίτητων τμημάτων λογισμικού (λειτουργικά συστήματα, patches, device drivers, λογισμικό firewall, λογισμικό παρακολούθησης δικτύου). (CERT)

2.7.2 Απόκτηση τεκμηρίωσης, εκπαίδευσης και υποστήριξης.

Ανάλογα με τον επιλεγέντα αρχιτεκτονικό σχεδιασμό, πιθανότατα απαιτείται επιπρόσθετη εκπαίδευση και υποστήριξη από την προμηθεύτρια εταιρεία. Εάν ο οργανισμός δε διαθέτει εμπειρία στις τεχνολογίες που πρόκειται να υλοποιήσει, υπάρχει σοβαρό ενδεχόμενο να οδηγηθεί σε σφάλματα που θα μπορούσαν να προκαλέσουν καθυστέρηση στην εγκατάσταση, στη ρύθμιση και στη λειτουργία του firewall. Επιπλέον η συντήρηση του υλικού και του λογισμικού μπορεί να είναι τόσο περίπλοκη ώστε να απαιτείται εκπαίδευση και συνεχής υποστήριξη. Όλα αυτά πρέπει να μελετηθούν λεπτομερώς στη φάση αυτή. (CERT)

2.7.3 Εγκατάσταση υλικού και λογισμικού.

Στη φάση αυτή εγκαθίσταται και ρυθμίζεται το λειτουργικό σύστημα που θα υποστηρίξει το λογισμικό του firewall. Το λειτουργικό σύστημα περιλαμβάνει μόνο τις υπηρεσίες που είναι απαραίτητες για τη λειτουργία του firewall, ενώ όλες οι υπόλοιπες υπηρεσίες πρέπει να είναι απενεργοποιημένες. (CERT)

Στη συνέχεια το λογισμικό του firewall εγκαθίσταται στο επιλεγμένο υλικό για δοκιμαστικό έλεγχο.

3 ΚΕΦΑΛΑΙΟ ΣΥΣΤΗΜΑΤΑ FIREWALL

3.1 Ταξινόμηση συστημάτων firewall

3.1.1 Προσωπικό Firewall

Ο όρος προσωπικό firewall αναφέρεται γενικά στο λογισμικό που τρέχει σε ένα μεμονωμένο σταθμό εργασίας και ενεργεί ως φίλτρο πακέτων Το πλεονέκτημα του προσωπικού firewall είναι ότι μπορεί να συνδέσει τους κανόνες με τα προγράμματα. Έτσι, παραδείγματος χάριν, ο φυλλομετρητής Ιστού (web browser) μπορεί να συνδεθεί με εξυπηρετητές διαδικτύου (web servers) σε όλο το Διαδίκτυο μέσω της θύρας HTTP (port 80), αλλά όχι και η εφαρμογή επεξεργασίας κειμένου. (Stalings)

Αυτό συμβαίνει επειδή το τοίχος προστασίας βρίσκεται στην ίδια μηχανή με τους κανόνες αποστολής των πακέτων. Το προσωπικό firewall εγκαθιστά λογισμικό σε επίπεδο πυρήνα λειτουργικού συστήματος το οποίο ελέγχει και παρεμποδίζει τις σχετικές με το δίκτυο κλήσεις. Κατ' αυτό τον τρόπο το firewall μπορεί να καθορίσει ποια διαδικασία στέλνει τα πακέτα. (Stalings)

Εντούτοις, η έννοια του προσωπικού firewall έχει διάφορες αδυναμίες. Κατ αρχήν, το προσωπικό firewall λειτουργεί στο πλαίσιο ενός γενικού σκοπού (general- purpose) λειτουργικού συστήματος και πρέπει να συνυπάρχει με υπηρεσίες που τρέχουν με αυξημένα προνόμια (μερικές φορές χωρίς ακόμη και να το γνωρίζει ο χρήστης). Εάν μια διαδικασία με αυξημένα προνόμια παραβιαστεί, τότε η το λειτουργικού συστήματος μπορεί εύκολα να παρακαμφθεί. (Stalings)

Συνήθως, μια από τις πρώτες ενέργειες των ιών που μολύνουν έναν υπολογιστή είναι η απενεργοποίηση του λογισμικό ελέγχου ιών (antivirus). Συνεπώς, είναι θέμα χρόνου να απενεργοποιήσουν το προσωπικό firewall σε εκείνη την μηχανή. (Stalings)

Ένας άλλος σημαντικός περιορισμός των προσωπικών τοίχων προστασίας είναι ότι η εμπιστοσύνη που αποδίδεται σε μία διαδικασία, συνήθως κληρονομείται και στις ελεγχόμενες από αυτήν διαδικασίες. Έτσι, ενώ ένας ιός δεν μπορεί να κάνει μια διαδικασία να εκτελέσει τις ενέργειες που δεν είναι μέρος του εξουσιοδοτημένου σχεδιαγράμματος εκτέλεσής της, μπορεί να εκμεταλλευθεί όλα τα προνόμια που αποδίδονται σε εκείνη τη διαδικασία. Κατά συνέπεια, υποθέτοντας ότι οι διαδικασίες

που σχετίζονται εμ δικτυακές υπηρεσίες μπορούν επίσης να μολυνθούν, ο εισβολέας θα έχει όλα τα προνόμια της μολυσμένης διαδικασίας, η οποία μπορεί να είναι επαρκής για να πραγματοποιήσει ο εισβολέας το στόχο του. Μία τέτοια αδυναμία που υφίσταται στο λειτουργικό σύστημα windows περιγράφεται με μεγάλη λεπτομέρεια σε ένα πρόσφατο άρθρο. (Stalings)

3.1.2 **Κατανεμημένα** firewall

Τα συμβατικά firewall στηρίζονται στους περιορισμούς τοπολογίας και σε ελεγχόμενα σημεία εισόδου δικτύων, ώστε να επιβάλουν το φιλτράρισμα της κυκλοφορίας. Επιπλέον, εφόσον ένα τοίχος προστασίας δεν μπορεί να φιλτράρει την κυκλοφορία που δεν βλέπει, όσοι βρίσκονται στην πλευρά που είναι προστατευμένη θεωρούνται εξ ορισμού έμπιστοι. Παρόλο που αυτό το μοντέλο λειτουργεί αποδοτικά για δίκτυα μικρά και μεσαίου μεγέθους δίκτυα, οι τάσεις για αυξανόμενη συνδεσιμότητα, οι υψηλότερες ταχύτητες, τα εξωτερικά δίκτυα και η τηλεργασία, καθιστούν αυτό το μοντέλο ανεπαρκές. (Stalings)

Προκειμένου να ξεπεραστούν οι ανεπάρκειες των firewall έχουν προταθεί τα κατανεμημένα συστήματα firewall. Στα κατανεμημένα firewall, ενώ η πολιτική ασφάλειας καθορίζεται κεντρικά, επιβάλλεται σε κάθε μεμονωμένο σημείο το δικτύου (κόμβους, δρομολογητές, κ.λπ.). Το σύστημα μεταδίδει την κεντρική πολιτική σε όλα τα σημεία επιβολής της. Η διανομή της πολιτικής μπορεί να λάβει διάφορες μορφές. (Stalings)

Παραδείγματος χάριν, μπορεί να ωθηθεί (push) άμεσα στα ακραία συστήματα που πρέπει να την εφαρμόσουν, ή μπορεί να οριστεί στους χρήστες υπό μορφή δικαιωμάτων χρηστών (credentials) τα οποία χρησιμοποιούν για να επικοινωνήσουν με τους διάφορους κόμβους, ή μπορεί να είναι ένας συνδυασμός και των δύο. Η έκταση της αμοιβαίας εμπιστοσύνης μεταξύ των ακραίων σημείων καθορίζεται από την πολιτική. (Stalings)

Για την υλοποίηση ενός κατανεμημένου firewall, απαιτούνται τα ακόλουθα τρία στοιχεία:

- Μια γλώσσα για την έκφραση των πολιτικών (policy language) και την επίλυση των αιτημάτων. Στην απλούστερη μορφή τους, οι πολιτικές σε ένα κατανεμημένο σύστημα firewall είναι λειτουργικά ισοδύναμες με τους

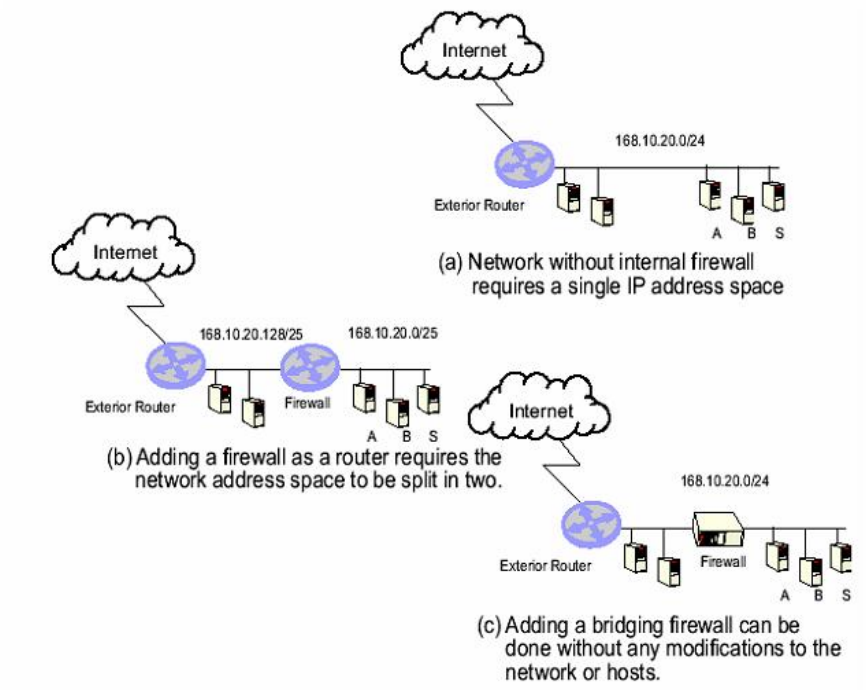
κανόνες φιλτραρίσματος πακέτων. Εντούτοις, είναι επιθυμητό να χρησιμοποιηθεί ένα εκτεταμένο σύστημα, ώστε να μπορούν να οριστούν και να εφαρμοστούν και άλλοι τύποι ελέγχων ασφάλειας εφαρμογών να μπορούν να οριστούν και να επιβληθούν στο μέλλον. Η γλώσσα και ο μηχανισμός λήψης αποφάσεων μπορούν επίσης να υποστηρίζουν προνόμια, για την μεταβίβαση δικαιωμάτων.

- Ένα μηχανισμό για την ασφαλή διανομή πολιτικών ασφάλειας (policy distribution). Η ακεραιότητα των πολιτικών που μεταφέρονται πρέπει να είναι εγγυημένη, είτε μέσω του πρωτοκόλλου επικοινωνίας είτε ως τμήμα της περιγραφής της πολιτικής αντικειμένου (π.χ., μπορούν να υπογραφούν ψηφιακά).

- Ένας μηχανισμός εφαρμογής της πολιτικής ασφάλειας (policy enforcement mechanism) στα εισερχόμενα πακέτα ή τις συνδέσεις. (Stalings)

3.1.3 Firewall 2ου επιπέδου

Όπως έχει αναφερθεί προηγουμένως, ένα τυπικό firewall λειτουργεί κυρίως στο επίπεδο δικτύου και στο πρωτόκολλο IP (3ο επίπεδο). Αυτό οφείλεται κυρίως στην τοποθεσία των περισσότερων firewall: αντικαθιστούν συνήθως τον δρομολογητή που συνδέει το εσωτερικό δίκτυο με το εξωτερικό δίκτυο. Συνεπώς, σχεδιάστηκαν με σκοπό να λειτουργήσουν στο ίδιο επίπεδο με τη συσκευή που αντικατέστησαν (τους δρομολογητές). Εντούτοις υπάρχουν περιπτώσεις που είναι επιθυμητή η τοποθέτηση του firewall «πάνω στο καλώδιο», δηλαδή με τέτοιο τρόπο ώστε είναι διαφανές στα υπόλοιπα δικτυακά στοιχεία. Η επίτευξη αυτού στο επίπεδο IP είναι δύσκολη δεδομένου ότι θα απαιτούσε τη δημιουργία ενός νέου δικτύου μεταξύ του firewall και του εξωτερικού δρομολογητή (δείτε την εικόνα 2). (Stalings)



Εικόνα 2 Αντιπυρική ζώνη δύο στρωμάτων

Η διαφάνεια του firewall 2ου επιπέδου στους κόμβους IP επιτρέπει την εισαγωγή του firewall χωρίς να παρεμποδίσει τη λειτουργία του δικτύου. Στην πραγματικότητα, οι διάφοροι οικοδεσπότες και τα σχετικά δικτυακά στοιχεία δεν χρειάζεται να έχουν γνώση της εγκατάστασης του τοίχους προστασίας. Αυτό το χαρακτηριστικό γνώρισμα του firewall 2ου επιπέδου, επιτρέπει στην εύκολη επέκταση (ουσιαστικά κατόπιν απαιτήσεως), προκειμένου να παρασχεθεί αυξημένη ασφάλεια σε ένα συγκεκριμένο τμήμα του εσωτερικού δικτύου, για την ανίχνευση λαθών, ή για το μετριασμό μίας επίθεσης. Για παράδειγμα, εάν κάποιοι κόμβοι έχουν μολυνθεί από έναν νέο ιό, τα firewall2ου επιπέδου μπορούν να επεκταθούν σε διάφορα σημεία του δικτύου για να αποτρέψουν τη διάδοση της μόλυνσης. (Stalings)

3.1.4 Παράδειγμα χρήσης firewall 2ου επιπέδου

Ας υποτεθεί ότι έχουμε ορισμένους κόμβους στο ίδιο δίκτυο και ότι επιθυμούμε να επιτρέψουμε σε μερικές υπηρεσίες από τον οικοδεσπότη S να είναι διαθέσιμες στους οικοδεσπότες A και B εικόνα 2 (α)), αλλά όχι στους άλλους οικοδεσπότες στο δίκτυο. Μία λύση είναι να δημιουργήσουμε ένα μικρό δίκτυο που περιλαμβάνει τους οικοδεσπότες S, A και B και να το συνδέσουμε με το κύριο δίκτυο με ένα firewall F. Εντούτοις, σε αυτήν την περίπτωση θα πρέπει να βρούμε τις νέες διευθύνσεις για τους οικοδεσπότες S, A και B, οι οποίες θα ήταν εξωτερικές από το κύριο δίκτυο. Θα έπρεπε έπειτα να σιγουρευτούμε ότι οι αλλαγές δρομολόγησης υλοποιήθηκαν σε όλο

το κύριο τοπικό LAN για να εξασφαλισθεί οτι τα πακέτα που κατευθύνονται προς τους S, A, και B στέλνονται πλέον στο F. Εάν οι διευθύνσεις για το νέο δίκτυο δεν ήταν διαθέσιμες, τότε το F θα έπρεπε να εκτελέσει μερικές πρόσθετες τροποποιήσεις στα πακέτα (π.χ. μετάφραση διευθύνσεων δικτύου – Network Address Translation / NAT) περιπλέκοντας περαιτέρω τη διαμόρφωση των συστημάτων firewall. Με τη χρήση ενός firewall επιπέδου 2, οι τρεις κόμβοι S, A, και B τοποθετούνται σε χωριστό Ethernet LAN με την αντιπυρική ζώνη (F) να ενεργεί ως γέφυρα μεταξύ του νέου LAN και του κυρίου LAN (σχήμα 2 (γ)). Εφόσον το γεφύρωμα γίνεται στο επίπεδο Ethernet είναι διαφανές στο στρώμα IP και επιτρέπει έτσι στους κόμβους να διατηρήσουν τις αρχικές διευθύνσεις IP για το κύριο δίκτυο. Κατά συνέπεια το firewall μπορεί να εγκατασταθεί χωρίς οποιοδήποτε είδος τροποποίησης στους κόμβους (ακόμα και οι υπηρεσίες όπως το DHCP θα είναι αμετάβλητες). Το τοίχος προστασίας μπορεί στη συνέχεια να εμποδίσει την πρόσβαση στις υπό περιορισμό υπηρεσίες σε όλους τους οικοδεσπότες στο κύριο δίκτυο. (Stalings)

3.1.5 **Χρησιμοποίηση** firewall **2ου επιπέδου για αποτροπή επιθέσεων** ARP spoofing

Ένας κόμβος A που επιθυμεί να στείλει ένα πακέτο σε έναν άλλο κόμβο στο ίδιο δίκτυο πρέπει να εντοπίσει τη διεύθυνση Ethernet (ή MAC) του κόμβου προορισμού. Πρέπει, επομένως, να ανακαλύψει ποια διεύθυνση MAC αντιστοιχεί στη διεύθυνση IP του παραλήπτη. Στην έκδοση 4 του πρωτοκόλλου IP, οι κόμβοι χρησιμοποιούν το πρωτόκολλο επίλυσης διευθύνσεων (Address Resolution Protocol – ARP) για να εκτελέσουν αυτήν την μετατροπή. (Stalings)

Με βάση το πρωτόκολλο αυτό ο κόμβος αποστολέας μεταδίδει σε όλους (broadcast) ένα πακέτο Ethernet που περιέχει τη διεύθυνση IP του παραλήπτη ρωτώντας ουσιαστικά ποιος έχει τη διεύθυνση IP. Ο κάτοχος της διεύθυνσης IP θα απαντήσει στη συνέχεια απευθείας (unicast) στον κόμβο που προκάλεσε την αναζήτηση. Σε μερικές περιπτώσεις οι δρομολογητές μπορούν να στείλουν τα πακέτα ARP με τις IP και MAC διευθύνσεις τους, ώστε να αποτρέψουν τους κόμβους από τον καθαρισμό αυτών των διευθύνσεων. Τέτοιες μεταδόσεις καλούνται δωρεάν ARPs (gratuitous ARPs). Οι επιθέσεις παραποίησης ARP (ARP spoofing) περιλαμβάνουν χαρακτηριστικά έναν (εχθρικό) κόμβο (H) που εκδίδει πλαστά δωρεάν πακέτα ARP τα οποία μεταδίδουν τη διεύθυνση MAC του H ως τη διεύθυνση MAC ενός κόμβου (R) που πρόκειται να παραποιηθει. Εάν ο λαμβάνων (S) του δωρεάν πακέτου ARP

έχει τη διεύθυνση IP του κόμβου (R), θα την αντικαταστήσει με την πλαστή διεύθυνση MAC που απέστειλε ο κόμβος (H). Σε ένα δίκτυο Ethernet με μεταγωγέα, ο πραγματικός ιδιοκτήτης της διεύθυνσης IP δεν θα ανιχνεύσει την πλαστή δραστηριότητα επειδή η μετάδοση γίνεται απευθείας (unicast). Ένας κόμβος-θύμα της επίθεσης θα στείλει τώρα όλα τα πακέτα που προορίζονται για τον R στο H αφού η ARP cache που διατηρεί έχει μολυνθεί. Ο κόμβος H μπορεί τώρα είτε παθητικά να ελέγξει τις μεταδόσεις του κόμβου S είτε να συμμετέχει σε μια ενεργό επίθεση με την τροποποίηση των πακέτων που τον περνούν μέσω αυτού. (Stalings)

Οι επιθέσεις ARP spoofing είναι ιδιαίτερα αποτελεσματικές όταν χρησιμοποιούνται για την παραπλάνηση ενός τοπικού δρομολογητή ή εξυπηρετητή DNS, και είναι αρκετά δύσκολες να ανιχνευθούν. Ας δούμε τη διαμόρφωση που χρησιμοποιείται στο προηγούμενο παράδειγμά μας. Το firewall F θα επιτρέψει στα πακέτα ARP να περάσουν εφόσον ελέγξουν ότι οι πληροφορίες σε αυτά είναι σύμφωνες με τις προηγούμενες αντιστοιχίσεις διευθύνσεων MAC και IP. (Stalings)

Παρά τα οφέλη τους, η χρήση των firewall 2ου επιπέδου,είναι μάλλον περιορισμένη λόγω των προβλημάτων με την αποδοτικότητα και το κόστος διαχείρισής τους. Το φιλτράρισμα των πλαισίων Ethernet θεωρείται περισσότερο απαιτητικό σε πόρους, που δημιουργεί τους φόβους οτι τα firewall αυτά μπορεί να μην είναι σε θέση να εξυπηρετήσουν την κυκλοφορία που παράγεται από τα σύγχρονα LAN μεγάλης ταχύτητας. Επίσης, η προστιθέμενη πολυπλοκότητα που επιβάλλεται από την ανάγκη να δημιουργηθούν οι κανόνες που λειτουργούν στο επίπεδο Ethernet, έχει δημιουργήσει την εντύπωση ότι τα firewall 2ου επιπέδου, είναι δυσκολότερο να διαμορφωθούν. Δικαιολογημένοι ή όχι, αυτοί οι προβληματισμοί έχουν εμποδίσει τη διάδοση των firewall αυτού του τύπου. (Stalings)

3.1.6 Firewall **υλοποιημένο σε ανεξάρτητη συσκευή**

Τα κατανεμημένα και τα προσωπικά τείχη προστασίας έχουν το μειονέκτημα ότι τρέχουν στο ίδιο υλικό (και στο ίδιο λειτουργικό συστήματος γενικού σκοπού) όπως οι εφαρμογές. επιπέδου χρήστη. Κατά συνέπεια, οποιαδήποτε παραβίαση της ασφάλειας από μια από τις άλλες εφαρμογές (π.χ. μια μόλυνση ιών), μπορεί να παρεμποδίσει τη λειτουργία του firewall. (Stalings)

Λόγω των περιορισμών στο σχεδιασμό των περισσοτέρων από τα τρέχοντα δημοφιλή λειτουργικά συστήματα, τα προσωπικά firewall είναι πιθανό να παρέχουν

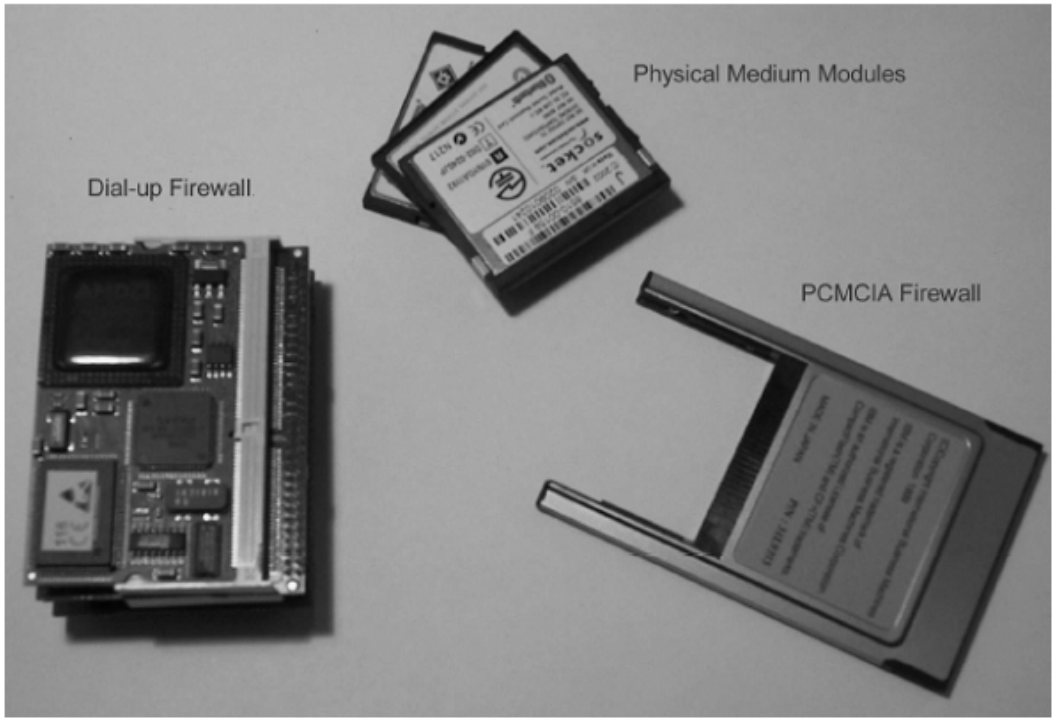
μια ψεύτικη αίσθηση ασφάλειας, παρά πραγματική προστασία. Στην περίπτωση των κατανεμημένων firewall, οι μηχανισμοί πολιτικής επιβολής που λειτουργούν στο επίπεδο κλήσεων συστήματος, παρέχουν επιπρόσθετη προστασία. Εντούτοις, η λειτουργία του firewall μπορεί να επηρεαστεί από ενέργειες χρηστών (είτε σκόπιμες, είτε τυχαίες). (Stalings)

Τέτοιες ανησυχίες αντιμετωπίζονται εν μέρει από τα firewall που είναι υλοποιημένα σε ανεξάρτητη συσκευή (hardware) και λειτουργεί αποκλειστικά για την προστασία του δικτύου. Η συσκευή firewall ενεργεί γενικά ως παραδοσιακό τοίχος προστασίας, αλλά προστατεύει μόνο ένα μόνο κόμβο. Έχει δύο διεπαφές, μια για να συνδεθεί με τον υπολογιστή που προστατεύει, και άλλη που συνδέει με το υπόλοιπο του δικτύου. Ο κόμβος επικοινωνεί πάντα με τον εξωτερικό κόσμο μέσω της συσκευής firewall. Δεδομένου ότι η συσκευή πρέπει να εφαρμόζει την πολιτική ασφάλειας, υπάρχει ανάγκη διανομής αυτής της πολιτικής, σε όλες τις συσκευές firewall του δικτύου με ένα ασφαλή τρόπο. Αυτό επιτυγχάνεται με δύο τρόπους: (Stalings)

(α) παραμετροποιώντας τις συσκευές να κατεβάζουν τις ανανεώσεις των πολιτικών ασφάλειας σε τακτά χρονικά διαστήματα (αυτό είναι παρόμοιο με την αυτόματη μεταφόρτωση των αρχείων υπογραφών ιών), ή (Stalings)

(β) ο χρήστης του προστατευμένου κόμβου εκκινεί την ανανέωση της πολιτικής (παραδείγματος χάριν, έτσι ώστε να μπορεί να εκτελέσει έναν νέο έλεγχο που δεν καλύπτεται από την υπάρχουσα πολιτική). (Stalings)

Οι συσκευές firewall είναι ιδιαίτερα αποτελεσματικές στη προστασία των φορητών υπολογιστών. Σε μια τέτοια περίπτωση, μπορεί να χρησιμοποιηθούν ως πύλη VPN για να επιτρέψουν στον κινητό χρήστη την πρόσβαση στο τοπικό δίκτυο. Για να είναι αποτελεσματικές οι συσκευές firewall σε τόσους διαφορετικούς ρόλους, πρέπει να είναι εύχρηστες και εύκολα διαχειρίσιμες. Όπως μπορεί να φανεί στην εικόνα 3, η πιό πρόσφατη γενιά των συσκευών αντιπυρικών ζωνών έχει μικρύνει σε τέτοιο σημείο ώστε να αποτελούν μικρό φορτίο για τον κινητό χρήστη. (Stalings)



Εικόνα 3 Δύο τύποι συσκευών firewall. Η συσκευή στα αριστερά σχεδιάζεται για τη χρήση με σύνδεση dial-up. Η συσκευή στα δεξιά περιλαμβάνει τη λειτουργικότητα του firewall στον προσαρμογέα δικτύου και χρησιμοποιεί κατάλληλες θυγατρικές κάρτες για συμβατότητα με διάφορα φυσικά μέσα, όπως ενσύρματο και ασύρματο Ethernet, Bluetooth, κ.λπ.

3.2 Διαχείρηση συστημάτων firewall

3.2.1 Τοποθέτηση

Όπως έχει ήδη αναφερθεί, τα παραδοσιακά συστήματα firewall εκμεταλλεύονται τους περιορισμούς στην τοπολογία δικτύων για να επιβάλουν μια πολιτική ασφάλειας. Όμως, αυτό που ίσχυε παλαιότερα όπου οι περισσότεροι οργανισμοί είχαν σχετικά μικρά δίκτυα με μία ή δύο συνδέσεις προς ένα δημόσιο δίκτυο, δεν συμβαίνει απαραιτήτως στα σημερινά περιβάλλοντα. Κατά συνέπεια, ιδιαίτερη φροντίδα απαιτείται στον καθορισμό της τοποθέτησης των firewall. Οι οργανισμοί προσπαθούν ακόμα, όσο το δυνατόν περισσότερο, να ακολουθήσουν το μοντέλο του περιμετρικού firewall, όπου ένα firewall βλέπει όλα την κυκλοφορία από και πρός το δίκτυο και επιβάλλει την πολιτική ασφάλειάς. Ο κύριος λόγος είναι η ευκολία διαχείρισης – αρκεί μόνο να μετατραπεί ένας μικρός αριθμό κόμβων για να πραγματοποιηθεί μια αλλαγή στην πολιτική ασφάλειας. Η εξασφάλιση της φυσικής ακεραιότητας του τοίχους προστασίας είναι επίσης ευκολότερη όταν αποτελείται από λίγα μόνο συστήματα (Bartal)

Άλλα οφέλη που προκύπτουν από μία τέτοια συγκεντρωτική τοποθέτηση οφείλονται στη συνάθροιση της κίνησης. Διάφορες μεγάλης κλίμακας επιθέσεις, όπως καταιγίδες worms, επιθέσεις άρνησης υπηρεσιών (DoS), ή δακτυλοσκόπησης (fingerprinting) σε όλο το δικτυακό εύρος του οργανισμού είναι ευκολότερο να ανιχνευθούν εάν όλη η κυκλοφορία παρακολουθείται από το ίδιο IDS. Επιπλέον, η αντιμετώπιση μερικών από αυτά τα γεγονότα μπορεί να γίνει μόνο στον πυρήνα δικτύων: το φιλτράρισμα μιας επίθεσης DoS στο υπό στόχευση κόμβο είναι σχεδόν άνευ αξίας, δεδομένου ότι η συνέπεια της επίθεσης (η μη διαθεσιμότητα του κόμβου από άλλους) έχει ήδη πραγματοποιηθεί. (Bartal)

Στην πράξη, διάφορα firewall περιμέτρου χρησιμοποιούνται συχνά, όπως φαίνεται στην εικόνα 4: (Bartal)

- Για λόγους πλεονασμού (failover), μια μικρή ομάδα από firewall μοιράζεται το φορτίο της διαχείρισης μιας σύνδεσης δικτύων. Διάφορα εμπορικά προϊόντα επιτρέπουν τη διαμοίραση μεταξύ των μελών αυτής της ομάδας ώστε να εξασφαλίσουν διαφανή λειτουργία σε περίπτωση αποτυχίας οποιουδήποτε μέλους.

- Η προσέγγιση συστάδας ή συμπλέγματος firewall (firewall cluster) χρησιμεύει επίσης στο να μετριάσει τον αντίκτυπο στην απόδοση των firewall, εξισορροπώντας την κυκλοφορία του φορτίου στα μέλη της. Η διαμοίραση φορτίου γίνεται συνήθως με βάση κάθε ξεχωριστή σύνοδο (session), δηλαδή όλα τα πακέτα που ανήκουν στην ίδια σύνδεση TCP ή όλα τα πακέτα που προέρχονται από ή προορίζονται στον ίδιο κόμβο κ.λπ εξετάζονται αποτελούν την ομάδα εξέτασης των πακέτων. Η εξισορρόπηση φορτίου γίνεται επιτακτική όταν το σύστημα firewall χρησιμοποιείται για απαιτητική λειτουργία, όπως ο έλεγχος και το φιλτράρισμα σε επίπεδο εφαρμογών, η λειτουργία VPN, η ανίχνευση ιών και ενοχλητικής αλληλογραφίας, κ.λ.π. Ο συντονισμός της απόδοσης των firewall παραμένει μια δύσκολη εργασία που συχνά εκτελείται από το διαχειριστή κατά τη διάρκεια της λειτουργίας των συστημάτων.

- Οι περισσότεροι οργανισμοί σήμερα έχουν πολλές συνδέσεις στο δημόσιο δίκτυο (Διαδίκτυο), συχνά για λόγους αντιμετώπισης πτώσεων δικτύου. Επιπλέον, διαφορετικά τμήματα μιας επιχείρησης είναι πιθανό να έχουν

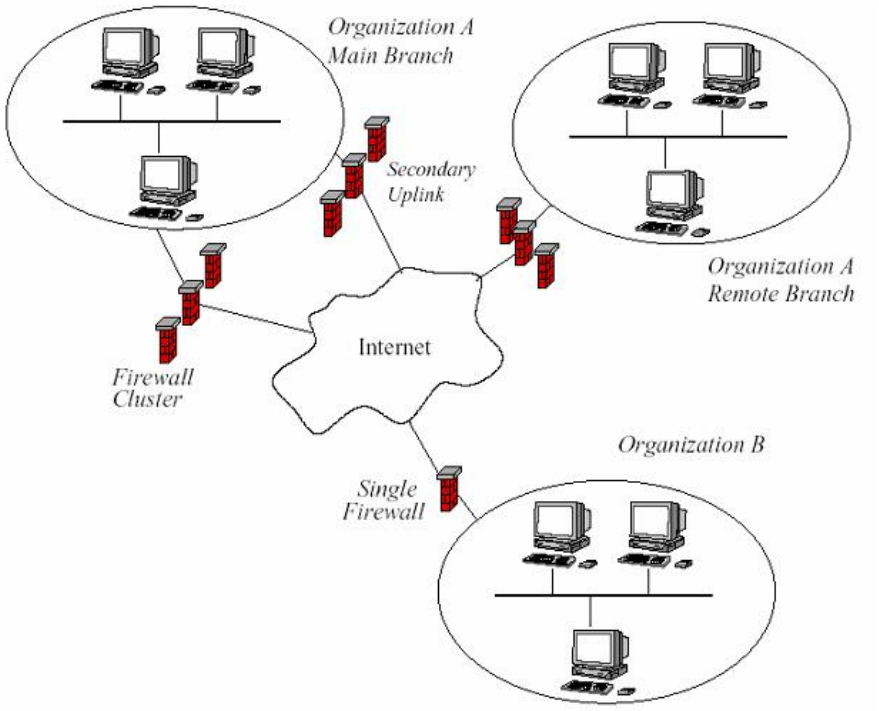
τοπικές συνδέσεις των δικτύων τους, που απαιτούν το δικό τους τείχος προστασίας (ή συστάδα firewall).

Οι σύγχρονοι οργανισμοί, επαυξάνουν περαιτέρω την ασφάλεια των περιμετρικών firewall με βοηθητικές εσωτερικά firewall που προστατεύουν συγκεκριμένα δίκτυα και πόρους. Αυτός ο διαχωρισμός του εσωτερικού δικτύου γίνεται συχνά με βάση τα υπηρεσιακά όρια (π.χ. διαχωρισμός κάθε υποδικτύου κάθε τμήματος του οργανισμού), και αντανακλά τη προσέγγιση της ασφάλεια που είναι γνωστή ως «ανάγκη γνώσης» (need-to-know ή need-to-access). Παραδείγματος χάριν, το νομικό και οικονομικό τμήμα είναι πιθανό να έχουν τα δικά τους firewall, δεδομένου ότι διαχειρίζονται ευαίσθητες πληροφορίες που πρέπει να προστατευθούν από άλλους υπαλλήλους της επιχείρησης όσο και από εξωτερικούς χρήστες. Τέτοια βοηθητικά τείχη προστασίας χρησιμεύουν επίσης ως ένα δευτεροβάθμιο εμπόδιο ενάντια σε εξωτερικούς επιτιθεμένους που κατορθώνουν με κάποιο τρόπο να διαπεράσουν στο εσωτερικό δίκτυο του οργανισμού. (Bartal)

Τα εσωτερικά συστήματα firewall χρησιμοποιούνται επίσης για να καθορίσουν τα όρια των αποκαλούμενων εξω-δικτύων (Extranets). Αυτά είναι ιδεατά δίκτυα που κατασκευάζονται πάνω από τους φυσικούς πόρους (συνδέσεις δικτύων, δρομολογητές, εξυπηρετητές) για τα οποία συνεισφέρουν δύο ή περισσότεροι συνεργαζόμενοι οργανισμοί. Κατασκευάζονται συνήθως για να διευκολύνουν την ανταλλαγή πληροφοριών και τη συνεργασία στα συγκεκριμένα προγράμματα. Ο ρόλος των αντιπυρικών ζωνών που τοποθετούνται "γύρω από" τους φυσικούς πόρους που συμβάλλουν εξωτερικό δίκτυο είναι να αποτραπούν οι εξωτερικοί χρήστες, που είναι νόμιμοι συμμετέχοντες στο εξωτερικό δίκτυο, από να αποκτήσουν πρόσβαση σε άλλους πόρους που συμβαίνουν να είναι τοπολογικά κοντά από διοικητικά ευδιάκριτο εξωτερικό δίκτυο. (Bartal)

Τέλος, οι αντιπυρικές ζώνες χρησιμοποιούνται συχνά για να μεσολαβήσουν την πρόσβαση μεταξύ των όλο και περισσότερο κοινών τοπικών ασύρματων δικτύων, όπως το 802.11WiFi, και το υπόλοιπο δίκτυο της επιχείρησης. Πολλοί οργανισμοί μεταχειρίζονται την ασύρματη υποδομή τους ως τμήμα του δημόσιου δικτύου, απαιτώντας από τους χρήστες να συνδεθούν στην αντιπυρική ζώνη προτού τους επιτραπεί είσοδος στο εσωτερικό δίκτυο ακόμα και όταν τα χαρακτηριστικά

γνωρίσματα ασφάλειας του ασύρματου δικτύου, (όπως η κρυπτογράφηση και η επικύρωση).είναι ενεργοποιημένα. (Bartal)



Εικόνα 4 Ο οργανισμός Α έχει δύο γεωγραφικά (και τοπολογικά) ευδιάκριτους κλάδους δικτύου, όπου ο κάθε κλάδος έχει μία σύνδεση στο Διαδίκτυο. Ο κύριος κλάδος έχει επίσης μία δευτεροβάθμια σύνδεση, και χρησιμοποιεί συστάδες firewall για λόγους πλεονασμού και απόδοσης. Η οργάνωση Β, έχει μόνο μια σύνδεση και χρησιμοποιεί ένα μόνο firewall.

Από τεχνική σκοπιά, δέν υπάρχει διαφορά μεταξύ των εσωτερικών και των περιμετρικών συστημάτων firewall. Συνήθως τα περιμετρικά συστήματα είναι γρηγορότερα και ακριβότερα, αφού πρέπει να χειριστούν σημαντικά περισσότερη κυκλοφορία. Η λειτουργία πρόληψης παρείσφρυσης (Intrusion Prevention), που αναλύεται στην ενότητα 3.2.3, χρησιμοποιείται συχνότερα από τα εσωτερικά συστήματα. Σε περιπτώσεις μόλυνσης από ιομορφικό λογισμικό τύπου «σκουληκιών» (worm), τα εσωτερικά firewall επιτρέπουν τη γρήγορη απολύμανση των συστημάτων προτού να μπορέσει το ιομορφικό λογισμικό να διαδοθεί στα υπόλοιπα συστήματα ενός υποδικτύου. (Bartal)

3.2.2 Εικονικά ιδιωτικά δίκτυα (VPNs)

Τα συστήματα firewall αποτελούν τα φυσικά άκρα για τη δημιουργία ασφαλών συνδέσεων και συχνά αποτελούν μέρος εικονικών ιδιωτικών δικτύων (Virtual Private Networks – VPNs). Ο λόγος που δεν επιτρέπεται στα VPN να τοποθετηθούν σε

εσωτερικότερο σημείο από το firewall είναι εφόσον οι πληροφορίες που μεταφέρονται μέσω του VPN είναι κρυπτογραφημένες, το firewall δεν θα είναι πλέον σε θέση να εφαρμόσει την πολιτική ασφάλειας δικτύου σε αυτά. Επιπλέον, μερικές υλοποιήσεις VPN (π.χ. εκείνες που χρησιμοποιούν το πρωτόκολλο IPSEC) είναι μη συμβατές με το πρωτόκολλο NAT (δείτε την παράγραφο 3.2) και συνεπώς το VPN δεν μπορεί να επεκταθεί στους εσωτερικούς κόμβους που διαθέτουν ιδιωτικές διευθύνσεις IP. (Cheswick)

Σε κάθε περίπτωση, οι διάφορες υλοποιήσεις VPN θα πρέπει να περιλαμβάνουν ένα firewall φιλτραρίσματος πακέτων για να καθορίσουν ποια πακέτα θα σταλούν μέσω του VPN. Προκειμένου να αποτραπούν οι επιθέσεις παραποίησης (spoofing) ή παρείσφρησης (injection), το VPN firewall θα πρέπει επίσης να εξετάζει τα εισερχόμενα πακέτα: εάν τα πακέτα προέρχονται από το εξωτερικό του VPN δίκτυο, αλλά εμφανίζονται να ανήκουν σε κόμβους που ανήκουν στο VPN δίκτυο, τότε το firewall θα τα απορρίψει. Γενικά, υπάρχουν τρεις πιθανές περιπτώσεις για τα εξεταζόμενα πακέτα: (Cheswick)

- Πρέπει να σταλούν μέσω του VPN.
- Πρέπει να σταλούν εκτός VPN (δηλαδή χωρίς κρυπτογράφηση).
- Δεν πρέπει να σταλούν καθόλου.

Τέτοιες αποφάσεις είναι κρίσιμες για την ασφάλεια του VPN επειδή καθορίζουν την επιβολή ή μη του διαχωρισμού μεταξύ του VPN και του ενδεχομένως μη έμπιστου δικτύου. Παραδείγματος χάριν, έστω ότι η Alice, μία διευθύντρια πωλήσεων μιας μεγάλης εταιρίας, επισκέπτεται μερικούς πελάτες. Δεδομένου ότι θα πρέπει να συνδεθεί με το εσωτερικό δίκτυο της εταιρείας, εγκαθιστά το λογισμικό πελάτη VPN (VPN client) στο φορητό υπολογιστή της. Η διαμόρφωση του VPN πρέπει να καθορίσει τι συμβαίνει εάν η Alice πρέπει να συνδεθεί σε ένα ιστότοπο στο Διαδίκτυο. Η εταιρική πολιτική μπορεί να απαιτεί η Alice να περάσει πάντα μέσα από το εταιρικό δίκτυο, οπότε σε αυτή την περίπτωση το λογισμικό VPN στον φορητό υπολογιστή της θα κατευθύνει όλα τα εξερχόμενα πακέτα στο VPN. Μόλις φθάσουν αυτά τα πακέτα στο εσωτερικό δίκτυο της Alice, θα σταλούν εν συνεχεία στο Διαδίκτυο (αυτή τη φορά μη κρυπτογραφημένα) και η απάντηση θα σταλεί μέσω του VPN στην Alice. Κατά συνέπεια, τα πακέτα θα διασχίσουν το Διαδίκτυο δύο φορές,

μιά φορά μέσω του VPN, και μια άλλη φορά καθαρά. Φυσικά, εάν το VPN τεθεί για κάποιο λόγο εκτός λειτουργίας, η Alice δεν θα είναι σε θέση να συνδεθεί με οποιοδήποτε κόμβο στο διαδίκτυο. (Cheswick)

Μια άλλη διαμόρφωση μπορεί να επιτρέψει στα πακέτα που προορίζονται για τους κόμβους εκτός του VPN, να παρακάμψουν το VPN και να σταλούν άμεσα στον τελικό προορισμό τους. Αυτή η διαμόρφωση θα επιτρέψει στην Alice να επικοινωνήσει με τους κόμβους που δεν είναι μέρος του VPN χωρίς την ανάγκη για περιττή πορεία διαμέσου της έδρας της επιχείρησης. Εντούτοις, αυτή η προσέγγιση μπορεί να επιτρέψει σε κακόβουλο περιεχόμενο να εγκατασταθεί στο φορητό υπολογιστή της Alice. (Cheswick)

Κατά συνέπεια, η σημαντικότερη ανησυχία ασφάλειας για τους πελάτες VPN είναι η αδυναμία ελέγχου του τι συμβαίνει σε αυτούς ενώ είναι μακρυά από το εταιρικό δίκτυο. Εάν αυτοί συνδέονται με άλλα δίκτυα μπορούν να μολυνθούν από τους ιούς ή ακόμα και να χρησιμοποιηθούν ώς ενδιάμεσοι σταθμοί σε μια επίθεση εναντίον του εσωτερικού δικτύου. Ακόμη και με το προηγούμενο σενάριο όπου ο φορητός υπολογιστής της Alice πηγαίνει πάντα μέσω του VPN, το κακόβουλο περιεχόμενο μπορεί ακόμα να περάσει, μέσω συσκευών που δεν είναι δικτυακές (π.χ. συσκευή μνήμης USB, CD-ROM, DVD δεδομένων, και τα λοιπά). Για αυτούς τους λόγους, οι συνδέσεις VPN από το εξωτερικό δεν θεωρούνται πλήρως έμπιστες και οι εξωτερικοί χρήστες αναγκάζονται να χρησιμοποιήσουν τα δίκτυα μορφής DMZ που παρέχουν περιορισμένες υπηρεσίες. (Cheswick)

3.2.3 Τεχνικές μετριασμού συνεπειών

Από τη μέχρι στιγμής ανάλυση, είναι προφανές ότι τα συστήματα firewall λειτουργούν πρωτίστως ως μηχανισμοί πρόληψης ζημίας. Ο αρχικός ρόλος τους είναι να κρατήσουν τις μη εξουσιοδοτημένες οντότητες έξω από το προστατευμένο δίκτυο, με την επιβολή της πολιτικής ασφάλειας του οργανισμού. Συχνά εντούτοις, η πολιτική ή οι μηχανισμοί που επιβάλλουν αυτό αποδεικνύεται αναποτελεσματικά σε μια επίθεση. Σε αυτή την περίπτωση, οι διαχειριστές του δικτύου αναμένεται να επέμβουν, συχνά μετά από την προειδοποίηση από ένα σύστημα ανίχνευσης παρείσφρυσης (IDS) το οποίο έχει ανιχνεύσει μια συγκεκριμένη επίθεση ή γενικά κάποια αντικανονική λειτουργία (π.χ. άφιξη πάρα πολλών μικρών πακέτων UDP). Δεδομένου ότι οι διαχειριστές δεν είναι πάντα διαθέσιμοι, και δεδομένου ότι ο

ρυθμός μερικών επιθέσεων καθιστά την αντίδραση μη πραγματοποιήσιμη σε χρονική κλίμακα ανθρώπων, τα σύγχρονα firewall υιοθετούν όλο και περισσότερο αυτοματοποιημένα αντίμετρα. Μερικά από αυτά, περιλαμβάνουν τα συστήματα πρόληψης παρείσφρησης (Intrusion Prevention Systems – IPS) και την απομόνωση. (Cheswick)

3.2.3.1 Συστήματα πρόληψης παρείσφρυσης (IPS)

Δεδομένου ότι οι διαχειριστές δικτύων αντιδρούν συχνά στις επιθέσεις εφόσον προειδοποιηθούν από ένα σύστημα ανίχνευσης παρείσφρυσης (IDS), είναι σημαντικό να υπάρχει συσχετισμός μεταξύ της λειτουργίας ελέγχου πρόσβασης και ανίχνευσης παρείσφρυσης. Σε γενικές γραμμές, αυτό μπορεί να επιτρέψει στα συστήματα firewall να αντιδρούν γρήγορα αντικανονική συμπεριφορά από φαινομενικά νόμιμους χρήστες (π.χ., μια επίθεση από ένα κακόβουλο εσωτερικό χρήστη, ή από ένα μολυσμένο σύστημα). (Cheswick)

Τα IPS μπορούν επίσης να επιτρέψουν μία περισσότερο ανεκτική πολιτική για τους εξωτερικούς ή άγνωστους χρήστες, επιτρέποντας την αλληλεπίδρασή τους με τα προστατευμένα συστήματα με περιορισμένους τρόπους: εάν μία επίθεση ή έστω ύποπτη συμπεριφορά ανιχνευθεί, τα προνόμια αυτών των χρηστών μπορούν να ανακληθούν αυτόματα. (Cheswick)

Στην πράξη, τα συστήματα IPS είναι τόσο καλά όσο τα συστήματα ανίχνευσης παρείσφρυσης που τα ελέγχουν. Ένα κοινό πρόβλημα στα IDS είναι το ποσό λανθασμένων θετικών σημάτων που παράγουν, (αναγνώριση νόμιμης συμπεριφοράς ως κακόβουλης). Οι συχνές αναδιαμορφώσεις μπορούν να προκαλέσουν σημαντική υποβάθμιση της απόδοσης και ακόμη και την απώλεια λειτουργίας π.χ., με την εξάντληση των πολιτικών πινάκων του firewall με ψευδείς κανόνες. (Cheswick)

Επιπλέον, ένας αντίπαλος που γνωρίζει το IPS μπορεί να παραπλανήσει το σύστημα ώστε να εξαπολύσει το IPS μία επίθεση άρνησης υπηρεσιών ενάντια σε έναν νόμιμο χρήστη ή ολόκληρο τον οργανισμό. Παραδείγματος χάριν, με την αποστολή παραποιημένων πακέτων που φαίνονται ότι προέρχονται από έναν νόμιμο χρήστη από απόσταση, είναι συχνά δυνατό να εμποδιστεί εκείνος ο χρήστης από την είσοδο στο εσωτερικό δίκτυο. Μια τέτοια επίθεση μπορεί ειδάλλως να ήταν αδύνατη για τον επιτιθέμενο χωρίς την κατάχρηση του IPS. (Cheswick)

Από την άποψη των οργανισμών, τα περισσότερα IDS παρουσιάζουν έναν μη αποδεκτό αριθμό ψευδών αρνήσεων, δηλ., αναγνωρίζουν λανθασμένα τις επιθέσεις ως νόμιμη κίνηση χωρίς να προκαλούν κάποιο συναγερμό. Ανάλογα με κάθε σύστημα, τα ποσοστά ψευδούς άρνησης μπορεί είναι σημαντικά χαμηλότερα από 1%. (Cheswick)

Όμως οι επιθέσεις μπορούν να εξαπολυθούν επανειλημμένως από διαφορετικές θέσεις. Εφόσον το κόστος μιας επιτυχούς επίθεσης στον οργανισμό μπορεί να είναι απαγορευτικά υψηλό (π.χ., απώλεια οικονομικών ή επιχειρηματικών δεδομένων), δεν είναι λογικό να εξαρτάται ένας οργανισμός από ένα IDS ως τη μόνη γραμμή άμυνας.

Κατά συνέπεια, τα συστήματα IPS χρησιμοποιούνται συχνά για να ανιχνεύσουν την πιθανή αντικανονική συμπεριφορά των νόμιμων χρηστών, ενώ οι εξωτερικοί χρήστες ελέγχονται αποκλειστικά από κανόνες ελέγχου πρόσβασης. (Cheswick)

3.2.3.2Απομόνωση κόμβου ή υποδικτύου

Με τη δραστική αύξηση του κακόβουλου λογισμικού τα τελευταία χρόνια (σκουληκιών, δικτυακών ιών κτλ), οι οργανισμοί έχουν στραφεί στα συστήματα firewall ως μέσο περιορισμού τέτοιων επιθέσεων. Το πρώτο προφανές βήμα για την αντιμετώπιση τέτοιων επιθέσεων, είναι η συνεχής ανανέωση της πολιτικής περιμέτρου ώστε να λαμβάνει υπόψη το συντομότερο δυνατό, τις νεοεμφανιζόμενες κάθε φορά επιθέσεις. Βέβαια, μία τέτοια αντιμετώπιση είναι από μόνη της ανεπαρκής να αντιμετωπίσει την απειλή των σκουληκιών (worms). Αυτά συχνά εμφανίζονται χωρίς προγενέστερη προειδοποίηση (σκουλήκια "μηδενικών ημερών" “zero-day” worms), ή μπορεί να εμφανιστούν στο εσωτερικό του δικτύου χωρίς να γίνουν αντιληπτά από το firewall. Αυτό είναι δυνατό να πραγματοποιηθεί για διάφορους λόγους, όπως είναι η χρήση κρυπτογράφησης (π.χ., ένας χρήστης που λαμβάνει ένα κρυπτογραφημένο ηλεκτρονικό ταχυδρομείο, ή που έχει πρόσβαση σε έναν μολυσμένο εξυπηρετητή διαδικτύου μέσα από μια σύνδεση SSL), ή επίσης λόγω της κινητικότητας των χρηστών (π.χ., ένας χρήστης που εισάγει ένα ήδη μολυσμένο φορητό υπολογιστή στο εσωτερικό δίκτυο). (Cheswick)

Κατά συνέπεια , για την απομόνωση εσωτερικών κόμβων ή υποδικτύων που επιδεικνύουν ύποπτη συμπεριφορά (π.χ. επιθέσεις γνωστών σκουληκιών), χρησιμοποιούνται όλο και περισσότερο εσωτερικά συστήματα firewall.

Παραδείγματος χάριν, τα σκουλήκια όπως το Slammer ή το CodeRed στέλνουν έναν μεγάλο αριθμό πακέτων σε διαφορετικούς κόμβους εντός μίας μικρής χρονικής περιόδου. Επιπλέον, τα περισσότερα σκουλήκια ηλεκτρονικού ταχυδρομείου χρησιμοποιούν δικό τους εξυπηρετητή SMTP ώστε να έρχονται άμεσα σε επαφή με απομακρυσμένους εξυπηρετητές (σε αντιδιαστολή με την αποστολή των μηνυμάτων ηλεκτρονικού ταχυδρομείου μέσω των κεντρικών εξυπηρετητών ταχυδρομείου του οργανισμού). Άλλοι τύποι επιθέσεων, όπως η άρνηση υπηρεσίας, παράγουν επίσης μεγάλους όγκους κυκλοφορίας, συχνά χρησιμοποιώντας πλαστές IP διευθύνσεις πηγής. (Cheswick)

Τα εσωτερικά συστήματα firewall, που λειτουργούν συνήθως στο επίπεδο του τοπικού δικτύου, μπορούν να απομονώσουν τα συστήματα που εμφανίζονται να είναι μολυνσμένα ή να συμμετέχουν σε μία εξελισσόμενη επίθεση. Ο απλούστερος τρόπος για να υλοποιηθεί κάτι τέτοιο είναι να φιλτραριστεί όλη η κυκλοφορία από εκείνον τον κόμβο ή το υποδίκτυο, να απενεργοποιηθεί η θύρα (port) στον μεταγωγέα Ethernet από όπου προέρχεται κυκλοφορία, ή να αποσυνδεθεί ο κόμβος από το σημείο ασύρματης πρόσβασης και να το αποτραπεί η επανασύδεσή του. Σε πιο προηγμένες προσεγγίσεις, ο μολυσμένος κόμβος τοποθετείται στο εικονικό τοπικό δίκτυο (Virtual LAN) που του επιτρέπει να έχει πρόσβαση σε έναν κεντρικό υπολογιστή που περιέχει τις πιο πρόσφατες ενημερώσεις/επιδιορθώσεις λογισμικού για διάφορα λειτουργικά συστήματα. Ο χρήστης μπορεί έπειτα να εγκαταστήσει αυτές οι επιδιορθώσεις και να επανεκινήσει το σύστημα χωρίς τον κίνδυνο επαναμόλυνσης από το ίδιο κακόβουλο λογισμικό λόγω των προηγούμενων αδυναμιών του λογισμικού του. (Cheswick)

Αυτή η προσέγγιση χρησιμοποιείται επίσης προληπτικά: όταν ένας νέος κόμβος εμφανίζεται στο δίκτυο, το firewall το ανιχνεύει για γνωστές ευπάθειες, χρησιμοποιώντας τις ίδιες τεχνικές (και συχνά το ίδιο λογισμικό) που οι επιτιθέμενοι χρησιμοποιούν για να αναγνωρίσουν γνωστές αδυναμίες. Εάν το firewall αναγνωρίσει γνωστές ευπάθειες, τότε ο κόμβος οικοδεσπότης τοποθετείται στο ίδιο VLAN και ο χρήστης κατευθύνεται σε μια ιστοσελίδα με οδηγίες για το πώς να ενημερώσει το σύστημα. Όλοι οι κόμβοι που συνδέονται με το δίκτυο ελέγχονται με τον ίδιο τρόπο.

Συχνά, το firewall ζώνη περιοδικά σαρώνει όλους τους κόμβους για να ανιχνεύσει τις τρωτές υπηρεσίες που εκκινήθηκαν μετά από την αρχική (ή την προηγούμενη)

σάρωση. Σε μερικά περιβάλλοντα, οι γνωστοί χρήστες που αυθεντικοποιούνται στο δίκτυο, σε αντιδιαστολή με τους «φιλοξενουμένους χρήστες» (guest users) απαλλάσσονται από αυτήν την ανίχνευση, αλλά υπόκεινται σε καραντίνα εάν το σύστημα πρόληψης εισβολών (IPS) ανιχνεύσει μια πιθανή προσβολή. (Cheswick)

3.3 **Σχεδιασμός** firewall

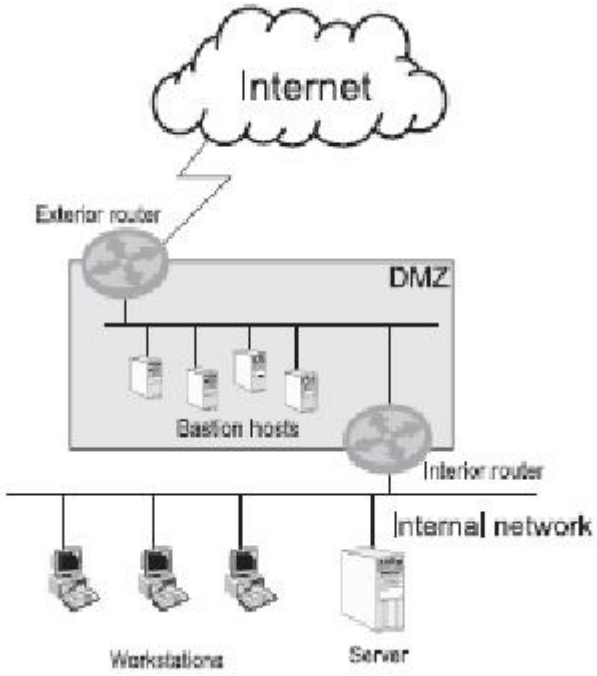
Ως αντιπυρική ζώνη (firewall), ορίζεται μία συλλογή στοιχείων τα οποία παρεμβάλλονται μεταξύ δύο δικτύων και φιλτράρουν την κυκλοφορία μεταξύ τους σύμφωνα με κάποια πολιτική ασφάλειας. Συνήθως, οι αντιπυρικές ζώνες στηρίζονται σε περιορισμούς της τοπολογίας των δικτύων ώστε να εκτελέσουν αυτό το φιλτράρισμα. Μια βασική υπόθεση σε αυτό το πρότυπο είναι ότι ο κάθε κόμβος στο προστατευμένο δίκτυο θεωρείται έμπιστος, δεδομένου ότι η εσωτερική κυκλοφορία δεν περνά μέσα από την αντιπυρική ζώνη και έτσι δεν μπορεί να φιλτραριστεί. Σε διαφορετική περίπτωση, πρόσθετες εσωτερικές αντιπυρικές ζώνες πρέπει να αναπτυχθούν στο εσωτερικό δίκτυο. Η μεγαλύτερη δυσκολία στη χρήση αντιπυρικών ζωνών σήμερα, βρίσκεται στη διαχείριση (management) ενός μεγάλου αριθμού αντιπυρικών ζωνών και την εξασφάλιση οτι αυτοί επιβάλλουν μια σταθερή πολιτική μέσα στο δίκτυο μιας οργάνωσης. Η χαρακτηριστική διαμόρφωση αντιπυρικών ζωνών, που παρουσιάζεται στην εικόνα 5, περιλαμβάνει συνήθως δύο δρομολογητές φιλτραρίσματος πακέτων (packet filtering routers) που δημιουργούν ένα δίκτυο περιορισμένης πρόσβασης αποκαλούμενο αποστρατικοποιημένη ζώνη (Demiliterized Zone – DMZ). Η DMZ ενεργεί ως απομονωτής μεταξύ των εσωτερικών (έμπιστων) και εξωτερικών (μη έμπιστων) δικτύων. Μία τέτοια διαμόρφωση προσπαθεί να ικανοποιήσει διάφορους στόχους όπως: (Prevelakis)

- Προστασία στους οικοδεσπότες (hosts) στο εσωτερικό δίκτυο από τις επιθέσεις στο εξωτερικό περιβάλλον
- Να επιτρέπει στους κόμβους που βρίσκονται στο DMZ να είναι προσβάσιμοι από το εξωτερικό δίκτυο και έτσι, να είναι σε θέση να παρέχουν υπηρεσίες στον εξωτερικό κόσμο, ή να χρησιμεύσει ως να ενδιάμεσο βήμα που συνδέει τους κόμβους από το εσωτερικό δίκτυο με τους κόμβους στον εξωτερικό κόσμο.

- Να επιβληθεί μια πολιτική ασφάλειας σε όλο τον οργανισμό, η οποία μπορεί να περιλαμβάνει περιορισμούς ανεξάρτητους από την ασφάλεια, π.χ., πρόσβαση σε ορισμένους ιστοχώρους κατά τη διάρκεια των ωρών εργασίας.

Για να είναι αποτελεσματικό ένα firewall, θα πρέπει να τοποθετηθεί σε κατάλληλο σημείο, έτσι ώστε όλη η κυκλοφορία μεταξύ του εσωτερικού και του εξωτερικού δικτύου να περνά μέσα από αυτό. Αυτό υπονοεί ότι το(τα) firewall παραδοσιακά βρίσκονται στα σημεία όπου το εσωτερικό δίκτυο διασυνδέεται με το εξωτερικό δίκτυο (π.χ., το φορέα παροχής υπηρεσιών Διαδικτύου).

Αυτοί καλούνται σημεία διασύνδεσης. Με την τοποθέτηση των firewall στα σημεία διασύνδεσης ελέγχεται όλη η κυκλοφορία που εισέρχεται ή εξέρχεται από το εσωτερικό δίκτυο. Εντούτοις, καθώς η ταχύτητα των δικτυακών συνδέσεων αυξάνεται διαρκώς και οι πολιτικές πρόσβασης που πρέπει να εφαρμοστούν από τα firewall γίνονται ολοένα και πιο σύνθετες, τα firewall μπορεί να αποτελέσουν σημεία συμφόρησης του δικτύου (bottlenecks) οι και να περιορίζουν το ποσό των δεδομένων που μπορούν να εξυπηρετήσουν τους. (Prevelakis)



Εικόνα 5 Μια τυπική διαμόρφωση αντιπυρικής ζώνης

3.3.1 Η αποστρατικοποιημένη ζώνη (DMZ)

Η αποστρατικοποιημένη ζώνη (Demiliterized Zone – DMZ) είναι ένα ειδικό μέρος του δικτύου που απολαμβάνει μερική μόνο προστασία από το firewall. Αυτό επιτρέπει στο διαχειριστή του δικτύου να καθιερώσει ένα ειδικό σύνολο πολιτικών

για τους δικτυακούς κόμβους που βρίσκονται στη ζώνη DMZ. Για παράδειγμα, ενώ η κύρια πολιτική ασφάλειας μπορεί να απαγορεύει στους εσωτερικούς εξυπηρετητές (servers) να επικοινωνούν με το εξωτερικό δίκτυο, μια ειδική πολιτική DMZ μπορεί να επιτρέψει εξαιρέσεις έτσι ώστε: (Prevelakis)

- ένας Web server που βρίσκεται μπορεί στη ζώνη DMZ να είναι προσπελάσιμος από το εξωτερικό δίκτυο στη θύρα 80 μέσω του πρωτοκόλλου TCP ή
- ένας εξυπηρετητής ηλεκτρονικού ταχυδρομείου που βρίσκεται μπορεί στη ζώνη DMZ να είναι προσπελάσιμος από το εξωτερικό δίκτυο στη θύρα 25 η οποία αντιστοιχεί στο πρωτόκολλο απλού ταχυδρομείου (Simple Mail Transfer Protocol – SMTP)

Η τοποθέτηση των δικτυακών κόμβων στη ζώνη DMZ τους καθιστά πιο ευάλωτους σε επιθέσεις ασφάλειας. Για αυτό το λόγο ρυθμίζονται συνήθως με κατάλληλη διαμόρφωση ενίσχυσης της ασφάλειάς τους. Οι εξυπηρετητές οι οποίοι βρίσκονται στην ζώνη DMZ αναφέρονται επίσης και ως εξυπηρετητές έπαλξης (bastion hosts). Οι bastion hosts, είναι κατάλληλα διαμορφωμένοι υπολογιστές οι οποίοι έχουν ρυθμιστεί να εκτελούν μόνο τις οριζόμενες υπηρεσίες και τίποτα περισσότερο. Μερικές φορές, αυτές οι μηχανές τρέχουν με στατικά ορισμένες παραμέτρους λειτουργίας (π.χ. χρησιμοποίηση του αρχείου “/etc/hosts” για την επίλυση ονόματος (name resolution) αντί για την υπηρεσία Domain Name System – DNS). Αυτό γίνεται ώστε να ελαχιστοποιηθεί ο κίνδυνος ένας επιτιθέμενος ο οποίος καταφέρνει να διεισδύσει στον εξυπηρετητή έπαλξης να χρησιμοποιήσει ταυτόχρονα και μία υπηρεσία ανεξάρτητη από τη λειτουργία του εξυπηρετητή. (Prevelakis)

Επιπλέον, το λειτουργικό σύστημα που εγκαθίσταται στους εξυπηρετητές έπαλξης είναι συνήθως ένα υποσύνολο της τυποποιημένης διανομής (π.χ., μπορεί να μην έχει μεταγλωττιστές, εργαλεία ελέγχου δικτύων, κτλ) έτσι ώστε ένας πιθανός εισβολέας να μην είναι σε θέση να χρησιμοποιήσει τον εξυπηρετητή έπαλξης για να εκτελέσει νέες επιθέσεις σε άλλους κόμβους του δικτύου. (Prevelakis)

Μία καλή τακτική είναι οι διαχειριστές δικτύου να μεταχειρίζονται τους κόμβους που βρίσκονται στη ζώνη DMZ ως δυνητικά μη έμπιστους κόμβους και να έχουν προετοιμάσει κατάλληλες στρατηγικές και τεχνικές αποκατάστασης. Τέτοιες

στρατηγικές μπορούν να περιλάβουν βήματα για τη συγκέντρωση αποδείξεων πιθανών εισβολών ή πληροφοριών για τον επιτιθέμενο, περιορισμού των συνεπειών της επίθεσης κτλ.. (Prevelakis)

Ανεξάρτητα από την υιοθετούμενη στρατηγική αποκατάστασης, ο διαχειριστής των συστημάτων πρέπει να είναι σε θέση να αποκαταστήσει την υπηρεσία σε κάθε δικτυακό κόμβο το συντομότερο δυνατόν. Αυτό υπονοεί ότι ολόκληρη η διαμόρφωση των συστημάτων (λειτουργικού συστήματος, υπηρεσίας κτλ) έχει διατηρηθεί σε εφεδρικό αρχείο ασφαλείας και υπάρχουν διαδικασίες για την επαναφορά του μολυσμένου κόμβου και την αποκατάσταση της διαμόρφωσης και των σχετικών δεδομένων. Εάν η μέθοδος επίθεσης δεν είναι δυνατό να προσδιοριστεί επακριβώς, η επαναφορά του κόμβου με μία καθαρή διαμόρφωση δεν είναι αρκετή. Ο επιτιθέμενος θα επαναλάβει απλώς το ίδιο μοτίβο επίθεσης για να επιτύχει και πάλι το ίδιο αποτέλεσμα. Η ανίχνευση και η κατανόηση της επίθεσης είναι την ευπάθεια που επέτρεψε στην επίθεση να πραγματοποιηθεί και να την αντιμετωπίσουμε, προτού να μπορέσει η μηχανή να συνδεθεί στο δίκτυο. Ο προσδιορισμός της αδυναμίας ή των αδυναμιών που χρησιμοποίησε ο επιτιθέμενος και η ανίχνευση και κατανόηση της επίθεσης ενάντια στους κόμβους που βρίσκονται στη ζώνη DMZ ή το εσωτερικό δίκτυο, είναι μια σημαντική πτυχή της διαμόρφωσης του firewall. Ο έλεγχος της κίνησης (traffic monitoring) και η καταγραφή των γεγονότων (event logging) είναι βασικά εργαλεία του διαχειριστή του δικτύου. Επιπλέον είναι δυνατό να εγκατασταθούν στη ζώνη DMZ συστήματα ανίχνευσης παρείσφρησης (IDSs) ώστε να ελέχγουν (και μερικές φορές να αντιδρούν) στις επιθέσεις. (Prevelakis)

3.3.2 Firewall **φίλτρου πακέτων** (packet filtering) **εναντίον** firewall **πυλών επιπέδου εφαρμογής** (application-level gateways)

Οι δύο δρομολογητές του προηγούμενου παραδείγματος, υιοθετούν μερικούς κανόνες, για παράδειγμα μέσω μίας Λίστας Ελέγχου Πρόσβασης (Access Control List – ACL), για να καθοριστεί ποιοι τύποι πακέτων επιτρέπονται να περνούν. Το φιλτράρισμα επιπέδων πακέτων είναι αρκετά απλοϊκό αφού τοποθετείται στα επίπεδα δικτύου και μεταφοράς, και ως εκ τούτου έχει ελάχιστη ή καμία πληροφορία για ότι συμβαίνει στο επίπεδο εφαρμογής. Κατά συνέπεια, πολιτικές του τύπου: «μόνο ο χρήστης X μπορεί να έχει πρόσβαση στο www.xyz.com μέσω του HTTP κατά τη διάρκεια των ωρών απασχόλησης», δεν μπορούν να εκφραστούν. (Prevelakis)

Οι υψηλοτέρου επιπέδου πολιτικές οι οποίες απαιτούν συγκεκριμένη γνώση της εφαρμογής (π.χ., ανιχνευτές ιών ηλεκτρονικού ταχυδρομείου), ή την αυθεντικοποίηση των χρηστών, αντιμετωπίζονται καλύτερα μέσα από υπηρεσίες πληρεξουσίων (proxy services) οι οποίες εκτελούνται σε εξυπηρετητές έπαλξης (bastion hosts) και είναι επίσης γνωστοί ως πύλες επιπέδου εφαρμογής (application-level gateways). Τέτοιες μηχανές βρίσκονται συνήθως στη ζώνη DMZ επεξεργάζονται την κίνηση για συγκεκριμένες εφαρμογές. (Prevelakis)

Ένα τέτοιο παράδειγμα είναι η πύλη ηλεκτρονικού ταχυδρομείου (e-mail gateway). Συνήθως, ο κεντρικός υπολογιστής ηλεκτρονικού ταχυδρομείου (e-mail server) βρίσκεται στο προστατευμένο δίκτυο δεδομένου ότι πρέπει να χειρίζεται και το εσωτερικό ηλεκτρονικό ταχυδρομείο. Προκειμένου να αποτραπεί μία επίθεση του κεντρικού υπολογιστή ηλεκτρονικού ταχυδρομείου δεν επιτρέπεται σε αυτόν να δεχθεί άμεσες συνδέσεις από το εξωτερικό δίκτυο (Διαδίκτυο). Επομένως, τοποθετείται μία υπηρεσία πληρεξουσίου ηλεκτρονικού ταχυδρομείου στο DMZ (e-mail proxy server) που απλά συλλέγει το εισερχόμενο ηλεκτρονικό ταχυδρομείο. Ο κεντρικός υπολογιστής ηλεκτρονικού ταχυδρομείου, έρχεται σε επαφή με το πληρεξούσιο σε τακτά χρονικά διαστήματα για να λάβει οποιοδήποτε ηλεκτρονικό ταχυδρομείο που μπορεί να είχε φθάσει στο μεταξύ. (Prevelakis)

Παρατηρήστε ότι ο email proxy έχει παθητική λειτουργικότητα. Απλώς αναμένει να έρθει σε επαφή μαζί του ο εσωτερικός εξυπηρετητής ηλεκτρονικού ταχυδρομείου ή από τους εξωτερικούς οικοδεσπότες. Αυτό εξασφαλίζει ότι ακόμα σε περίπτωση επιτυχημένης επίθεσης στον e-mail proxy, ο εισβολέας δεν θα ήταν σε θέση να εξετάσει ή να επιτεθεί στον εσωτερικό κεντρικό υπολογιστή. (Prevelakis)

Φυσικά, αυτή η ρύθμιση μπορεί μόνο να προστατεύσει από τις επιθέσεις στο επίπεδο δικτύου και δεν μπορεί να προστατεύσει από επιθέσεις στο τμήμα των δεδομένων όπως είναι οι ιοί. Θα πρέπει να πραγματοποιηθεί πρόσθετη ανάλυση του περιεχομένου των μηνυμάτων ηλεκτρονικού ταχυδρομείου, προκειμένου να καθοριστεί εάν περιέχουν ύποπτο περιεχόμενο. Για να γίνει αυτό, η πύλη θα πρέπει να γνωρίζει τον τρόπο που κατασκευάζονται τα μηνύματα ηλεκτρονικού ταχυδρομείου (δηλ., τα πρότυπα κωδικοποίησης όπως το MIME (Multipurpose Internet Mail Extension), το uuencode, το zip, κ.λ.π.). Δεδομένου ότι οι επιτιθέμενοι βρίσκουν συνεχώς διαφορετικές στρατηγικές, οι διαχειριστές δικτύου θα πρέπει να

είναι πολύ αυστηροί ώστε να εφαρμόζουν τις συμβουλές ασφάλειας και τις καινούριες υπογραφές ιών (virus signatures). Αυτό μοιάζει όλο και περισσότερο με έναν πλήρους απασχόλησης στόχο, και συχνά οι επιχειρήσεις εκτελούν με υπεργολαβία την ανάλυση του εισερχόμενου ηλεκτρονικού ταχυδρομείου σε εξωτερικές εταιρίες ασφάλειας. Σε τέτοιες περιπτώσεις, το ηλεκτρονικό ταχυδρομείο μπορεί να εκτραπεί μέσω του Διαδικτύου στην περιοχή μιας εταιρίας ασφάλειας όπου αναλύεται και αξιολογείται. Το ηλεκτρονικό ταχυδρομείο που θεωρείται ασφαλές, επιστρέφεται έπειτα στο πληρεξούσιο ηλεκτρονικού ταχυδρομείου όπου μπορεί να παρθεί από τον εσωτερικό κεντρικό υπολογιστή. (Prevelakis)

3.3.3 Τα firewall ελέγχου καταστάσεων (stateful inspection)

Αρχικά, τα firewall σχεδιάστηκαν για να εξετάσουν κάθε πακέτο χωριστά, και αποφάσιζαν εάν θα επιτρέπει τη διέλευση σε ένα πακέτο κατευθείαν, μόνο βάσει των πληροφοριών που περιλήφθηκαν μέσα σε εκείνο το πακέτο. Αυτό δημιούργησε δυσκολίες με τα πρωτόκολλα που στηρίζονταν σε δευτερεύουσες συνδέσεις για την ανταλλαγή πρόσθετων πληροφοριών (π.χ., FTP). Δεδομένου ότι το firewall δεν μπορεί να ξέρει εάν το (δευτεροβάθμιο) αίτημα σύνδεσης προήλθε από μια υπάρχουσα σύνδεση ή εάν δημιουργήθηκε ανεξάρτητα, το firewall αναγκαζόταν να το απορρίψει. (Prevelakis)

Τα firewall ελέγχου καταστάσεων, χρησιμοποιούν μηχανές καταστάσεων για να διατηρήσουν πληροφορίες της κατάστασης των ήδη εγκατεστημένων συνδέσεων πρωτοκόλλου. Οι αποφάσεις λαμβάνονται βάσει των πληροφοριών στο πακέτο συν την κατάσταση της σύνδεσης που διατηρείται από την αντιπυρική ζώνη. Κατά συνέπεια, ένα πακέτο TCP με καθαρή σημαία SYN, θα απορριφθεί εκτός αν ανήκει σε μια ήδη υπάρχουσα σύνδεση. Ακόμη και σε περιπτώσεις όπου οι πληροφορίες ανταλλάσσονται χωρίς πραγματοποίηση σύνδεσης (επικοινωνίες χωρίς σύνδεση όπως εκείνες που χρησιμοποιούν το πρωτόκολλο UDP), το firewall μπορεί να κάνει μια σημείωση ότι ένα πακέτο αιτήματος έχει περάσει την έξοδο του προστατευμένου δικτύου και επιτρέπει έτσι την απάντηση κατευθείαν (π.χ., μια ερώτηση SNMP από έναν εσωτερικό σταθμό διαχείρισης δικτύου σε έναν πράκτορα (agent) που βρίσκεται στο DMZ). (Prevelakis)

3.3.4 Πρόσθετες υπηρεσίες

Σε πολλές περιπτώσεις, τα firewall παρέχουν επίσης διάφορες πρόσθετες υπηρεσίες που ενώ δεν αποτελούν αυστηρά μέρος της εργασίας τους, έχουν χρησιμοποιηθεί τόσο ευρέως ώστε να θεωρούνται πλέον αναπόσπαστο τμήμα τους. (Prevelakis)

3.3.4.1 Η υπηρεσία Μετάφρασης Διεύθυνσης Δικτύου (NAT)

Η αυξανόμενη έλλειψη των διευθύνσεων IP έχει αναγκάσει τους διαχειριστές δικτύων να χρησιμοποιούν ειδικές διευθύνσεις IP που θεωρούνται ιδιωτικές. Τέτοιες διευθύνσεις μπορούν να χρησιμοποιηθούν μόνο μέσα στα όρια ενός δεδομένου δικτύου, αλλά δεν έχουν υπόσταση στο διαδίκτυο. Αυτό οφείλεται στο ότι οι διευθύνσεις αυτές δεν είναι μοναδικές, έτσι οι δρομολογητές στους κεντρικούς άξονες δεν φέρνουν καμία πληροφορία δρομολόγησης για αυτές. Εάν οι οικοδεσπότες με τις ιδιωτικές διευθύνσεις IP απαιτούν πρόσβαση στο Διαδίκτυο, πρέπει να χρησιμοποιήσουν έναν ενδιάμεσο οικοδεσπότη που έχει μία πραγματική διεύθυνση. Ένας τέτοιος οικοδεσπότης μπορεί να ενεργήσει ως πληρεξούσιος, αναμεταδίδοντας το αίτημα στον τελικό προορισμό. (Prevelakis)

Εντούτοις, οι πληρεξούσιοι δεν είναι πάντα χρησιμοποιήσιμοι λόγω των περιορισμών του πρωτοκόλλου, της χρήσης κρυπτογράφησης από-άκρο-σε-άκρο, αλλά επιπλέον, και των εξόδων διαχείρισης για τη συντήρηση χωριστών πληρεξουσίων για κάθε μια από τις επιθυμητές υπηρεσίες. Σε τέτοιες περιπτώσεις συστήνεται η χρήση της Μετάφρασης Διευθύνσεων Δικτύων (Network Address Translation – NAT), ή μεταμφίεσης IP. Με τη χρήση της υπηρεσίας NAT, ο ενδιάμεσος οικοδεσπότης τροποποιεί το εξερχόμενο πακέτο αλλάζοντας τη διεύθυνση προέλευσης με τη δική του διεύθυνσή. Κατ' αυτό τον τρόπο, η απάντηση θα παραληφθεί από τον ενδιάμεσο οικοδεσπότη που θα τροποποιήσει πάλι τη διεύθυνση προορισμού του πακέτου σε αυτή του εσωτερικού οικοδεσπότη. (Prevelakis)

Λαμβάνοντας υπόψη τη θέση του firewall, είναι αρκετά φυσικό να οριστεί η υπηρεσία NAT στο firewall. Αυτό συμβαίνει επειδή το firewall πρέπει ήδη να εξετάσει (για λόγους φιλτραρίσματος πακέτων) τα πακέτα που διασχίζουν τα όρια δικτύων και επίσης επειδή τα firewall διατηρούν ήδη την κατάσταση για τις συνδέσεις που υπάρχουν μεταξύ των εσωτερικών και εξωτερικών οικοδεσποτών.

3.3.4.2 *Οριζόντια διάσπαση DNS*

Το Σύστημα Ονοματοδοσίας Περιοχών (Domain Name System – DNS) παρέχει τις πληροφορίες σχετικά με την αντιστοίχηση μεταξύ των διευθύνσεων IP και των ονομάτων των κόμβων/εξυπηρετητών. Αυτές οι πληροφορίες μπορούν να χρησιμοποιηθούν από έναν επιτιθέμενο για τον προσδιορισμό των πιθανών στόχων (π.χ. ένας κόμβος που ονομάζεται mailhost είναι πιθανό να είναι ο κεντρικός υπολογιστής ταχυδρομείου ενός οργανισμού και ως εκ τούτου να έχει ενεργοποιημένες τις σχετικές με το ταχυδρομείο υπηρεσίες). Για αυτό το λόγο, υιοθετούνται συχνά δύο εξυπηρετητές DNS, ένας για το εσωτερικό δίκτυο και ένας για τη ζώνη DMZ ο οποίος παρέχει πληροφορίες στους εξωτερικούς κόμβους. Ο εσωτερικός DNS διατηρεί τις πληροφορίες για όλους τους κόμβους στο εσωτερικό δίκτυο , ενώ ο εξυπηρετητής DNS που βρίσκεται στη ζώνη DMZ αποθηκεύει μόνο τις πληροφορίες που πρέπει να κοινοποιηθούν σε εξωτερικά συμβαλλόμενα μέρη, έναν εσωτερικό σταθμό διαχείρισης δικτύου σε έναν πράκτορα (agent) που βρίσκεται στο DMZ). (Prevelakis)

3.3.4.3 *Αντιμετώπιση ταυτοποίησης κόμβων (host fingerprinting)*

Τα συστήματα ηλεκτρονικών υπολογιστών είναι σε μεγάλο βαθμό ντετερμινιστικά Για αυτό το λόγο είναι δυνατό να χρησιμοποιηθούν τεχνικές ταυτοποίησης ή δακτυλοσκόπησης (fingerprinting). Η δακτυλοσκόπηση είναι μια τεχνική η οποία επιτρέπει σε επιτιθεμένους να συγκεντρώσουν αρκετές πληροφορίες για ένα απομακρυσμένο σύστημα, ώστε να καθορίσουν τον τύπο και τη διαμόρφωση λογισμικού του (για παράδειγμα , την έκδοση του λειτουργικού συστήματος, των εφαρμογών του κ.λπ.). Αυτές οι πληροφορίες μπορούν έπειτα να χρησιμοποιηθούν για να καθοριστούν οι αδυναμίες που υπάρχουν στη συγκεκριμένη διαμόρφωση και συνεπώς να σχεδιαστεί ένα πιο αποτελεσματικό σχέδιο επίθεσης. (Prevelakis)

Πολλά firewall φιλτραρίσματος πακέτων, περιλαμβάνουν μια λειτουργία “scrub” που κανονικοποιεί και επανασυνδέει τα εισερχόμενα πακέτα. Αυτό παρέχει μερική προστασία στις εφαρμογές και στους κόμβους του εσωτερικού δικτύου, έναντι σε κατάλληλα τροποποιημένα πακέτα που έχουν σκοπό να εκμεταλλευτούν ευπάθειες. Μια άλλη προσέγγιση είναι να εφαρμοστεί μία παρόμοια τεχνική στα εξερχόμενα πακέτα, προκειμένου να μην αποκαλύπτονται στοιχεία που προσδιορίζουν τα χαρακτηριστικά γνωρίσματα της υλοποίησης της στοίβας IP. Ένα βασικό μέρος της διαδικασίας «συσκότισης» είναι η προστασία ενάντια στους χρονικά εξαρτημένους

ελέγχους. Οι διαφορετικές υλοποιήσεις του πρωτοκόλλου TCP, έχουν παραλλαγές στην υλοποίηση των μετρητών λήξης, των αλγορίθμων αποφυγής συμφόρησης, κ.λ.π.

Ελέγχοντας την απάντηση του υπό έλεγχο κόμβου σε εξομοιωμένη απώλεια πακέτων, ο έλεγχος συγχρονισμού μπορεί να καθορίσει την έκδοση της εφαρμογής TCP και κατ' επέκταση την έκδοση του λειτουργικού συστήματος. Επίσης η χρήση διάφορων τεχνικών περιορισμού του επιτρεπτού ποσοστού μηνυμάτων ICMP στο υπό επίθεση σύστημα, μπορεί να παρέχει χρήσιμη πληροφορία στον επιτιθέμενο. Η αποτελεσματικότητα τέτοιων ελέγχων μπορεί να μειωθεί, με την ομογενοποίηση του ποσοστού κυκλοφορίας ICMP που περνά από το σύστημα firewall, ή με την εισαγωγή τυχαίων καθυστερήσεων στις απαντήσεις των ICMP μηνυμάτων. (Prevelakis)

3.3.4.4Συστήματα ανίχνευσης παρείσφρυσης

Μία συνέπεια του γενικού κανόνα ότι "δεν υπάρχει απόλυτη ασφάλεια" είναι ότι και το ίδιο το firewall ενδέχεται κάποια στιγμή να παραβιαστεί. Συνεπώς, είναι αναγκαία η εφαρμογή μίας στρατηγικής για τον εντοπισμό παραβιάσεων ασφάλειας.

Τα συστήματα ανίχνευσης παρείσφρυσης (Intrusion Detection Systems – IDS) τοποθετούνται μέσα στη ζώνη DMZ και μπορούν να είναι ελεγκτές κυκλοφορίας ή συστήματα-παγίδες. Συστήματα ελέγχου κυκλοφορίας, παρεμβάλονται στε ολόκληρη την κυκλοφορία που διασχίζει το DMZ και προσπαθούν να προσδιορίσουν δομές ή μοτίβα που να προσδιορίζουν μία πιθανή επίθεση. Τα συστήματα «δοχεία μελιού» (honeypots) είναι συστήματα που διαμορφώνονται έτσι ώστε να μοιάσουν με πιθανούς στόχους επίθεσης (π.χ. λειτουργούν πολλές υπηρεσίες, τρέχουν τις παλαιές εκδόσεις του λογισμικού που είναι γνωστές για να περιέχουν τις ευπάθειες, κ.λπ.). (Prevelakis)

Δεδομένου ότι οι εξουσιοδοτημένοι χρήστες του δικτύου ξέρουν ότι δεν πρέπει να χρησιμοποιούν τον οικοδεσπότη αυτό, οποιοσδήποτε προσπαθεί να έχει πρόσβαση σε αυτόν είναι, εξ ορισμού ένδειξη ενός εισβολέα.

3.3.5 **Περιορισμοί των συστημάτων** firewall

Τα συστήματα firewall θεωρούνται γενικά απαραίτητα για την προστασία των υπολογιστικών συστημάτων. Εντούτοις, ένα ιδεατό και "γενικής χρήσης» firewall θα ήταν ουσιαστικά μικρής χρησιμότητας. Προκειμένου να είναι αποτελεσματικό ένα

firewall θα πρέπει να προσαρμόζεται στις ανάγκες του περιβάλλοντός του. (Prevelakis)

Παραδείγματος χάριν, σε ένα οικιακό δίκτυο το firewall εμποδίζει γενικά τις εισερχόμενες συνδέσεις, αλλά εάν ο τοπικός ιδιοκτήτης επιθυμεί να λειτουργήσει έναν ιστοχώρο, τότε το firewall θα πρέπει να προσαρμοσθεί. (Prevelakis)

Παρά τις προόδους που έγιναν στα τελευταία χρόνια, η διαμόρφωση των firewall είναι ακόμα μια διαδικασία δύσκολη και επιρρεπής σε λάθη, που απαιτεί προσεκτική επαλήθευση και δοκιμές για να εξασφαλίσει η ορθή και αποτελεσματική λειτουργία τους. Προκειμένου να γίνει αυτό, ο διαχειριστής πρέπει να καταλάβει τις απαιτήσεις του δικτύου που θα προστατευθεί, τις απαιτήσεις και τα πρωτόκολλα που χρησιμοποιούνται από τις διάφορες εφαρμογές που πρέπει να επιτρέπονται μέσω του firewall, και, τελικά, τον τρόπο που το ίδιο το firewall επιβάλλει τη διαμόρφωση που καθορίζεται από το διαχειριστή. (Prevelakis)

Οι λεπτές διαφορές μεταξύ αυτού που αναμένουμε να κάνει το firewall και αυτού που τελικά ισχύει, μπορεί να προκαλέσει δυσκολίες στη λειτουργία των εξουσιοδοτημένων εφαρμογών, ή ακόμα και να επιτρέπει την κυκλοφορία μη εξουσιοδοτημένης κίνησης μέσω του firewall.

Η επίθεση "μικρών πακέτων" (short-packet attack) είναι ένα καλό παράδειγμα μιας κατάστασης όπου ο επιτιθέμενος προσπαθεί να αναγκάσει το σύστημα firewall να λάβει μια απόφαση με ανεπαρκή δεδομένα. Αυτή η επίθεση στηρίζεται στην παρατήρηση ότι πολλά firewall δεν συγκεντρώνουν εκ νέου τα τεμαχισμένα πακέτα και ουσιαστικά λαμβάνουν την απόφασή τους με βάση το πρώτο τμήμα του πακέτου.

Στη συνέχεια επιτρέπουν το υπόλοιπο τμήμα να περάσει κατευθείαν, ουσιαστικά ανεξέλεγκτο. Η επίθεση "μικρών πακέτων" τεμαχίζει τα πακέτα έτσι ώστε το πρώτο τεμάχιο δεν περιέχει την ολόκληρη επικεφαλίδα TCP (και στερείται έτσι τις πληροφορίες όπως η θύρα προορισμού). Τα σύγχρονα συστήματα firewall απορρίπτουν τέτοια πακέτα. (Prevelakis)

Άλλοι περιορισμοί των παραδοσιακών firewall περιλαμβάνουν τα εξής:

- Λόγω των αυξανόμενων ταχυτήτων των γραμμών και των περισσότερο υπολογιστικά απαιτητικών πρωτοκόλλων που πρέπει να υποστηρίξει, πολλές

φορές το firewall τείνει να γίνει σημείο συμφόρησης. Το χάσμα μεταξύ των ταχυτήτων επεξεργασίας και δικτύωσης είναι πιθανό να αυξηθεί, τουλάχιστον στο εγγύς μέλλον: ενώ οι υπολογιστές (και ως εκ τούτου τα συστήματα firewall) γίνονται γρηγορότεροι (ακολουθώντας το νόμο του Moore), τα πρωτόκολλα και η τεράστια αύξηση στο ποσό δεδομένων που πρέπει να υποβληθεί σε επεξεργασία από το firewall ξεπερνούσαν και θα συνεχίσουν πιθανώς να ξεπερνούν το νόμο του Moore. (Ioannidis)

- Η διαρκής διεύρυνση των σύγχρονων δικτύων υπονοεί έναν μεγάλο αριθμό συνδέσεων στο Διαδίκτυο για καλύτερη απόδοση, αντιμετώπιση σφαλμάτων, και άλλους λόγους. Τα firewall πρέπει να επεκταθούν σε όλες αυτές τις συνδέσεις, αυξάνοντας πολύ το πρόβλημα διαχείρισης.

- Η διαρκής διεύρυνση των δικτύων σημαίνει επίσης ότι συχνά υπάρχουν επιτιθέμενοι ήδη στο εσωτερικό δίκτυο, π.χ., ένας δυσαρεστημένος υπάλληλος. Τα παραδοσιακά συστήματα firewall μπορούν να κάνουν πολύ λίγα, ενάντια σε μια τέτοια απειλή.

- Επιπλέον, η χρήση των ασυρμάτων (802.11 ή παρομοίων) δικτύων, είτε εξουσιοδοτημένων είτε όχι, σημαίνει ότι οι διαχειριστές δεν έχουν απαραιτήτως τον αυστηρό έλεγχο στα σημεία εισόδου των δικτύων: οι επιτιθέμενοι μπορούν να εμφανιστούν μέσα από το δίκτυο. Παρόμοιες ανησυχίες προκύπτουν λόγω της (Ioannidis)

- Αυξανόμενης χρήσης των εγκαταστάσεων τηλεργασίας, οι οποίες επεκτείνουν de facto το όριο του προστατευμένου δικτύου για να περιλάβουν την υποδομή που υπάρχει στις εγκαταστάσεις των υπαλλήλων κ.λπ. Ενώ τα συστήματα firewall δεν σκοπεύουν γενικά στην προστασία ενάντια στη λανθασμένη συμπεριφορά από τα μέλη, υπάρχει μια αντίθεση μεταξύ των εσωτερικών αναγκών για περισσότερη συνδεσιμότητα και της δυσκολίας ικανοποίησης τέτοιων αναγκών με ένα συγκεντρωτικό σύστημα firewall. (Ioannidis)

- Η κρυπτογράφηση από άκρο σε άκρο μπορεί επίσης να είναι μια απειλή, δεδομένου ότι εμποδίζει την εξέταση των πεδίων των πακέτων που είναι απαραίτητα για το φιλτράρισμα. Η κρυπτογράφηση από άκρο σε άκρο μέσω

ενός firewall υπονοεί αυξημένη εμπιστοσύνη στους χρήστες από μέρους των διαχειριστών των δικτύων. (Ioannidis)

- Υπάρχουν πρωτόκολλα που τα firewall δύσκολα μπορούν να χειριστούν, επειδή περιλαμβάνουν πολλαπλάσιες, φαινομενικά ανεξάρτητες ροές πακέτων. Ένα παράδειγμα είναι το πρωτόκολλο FTP, όπου μια σύνδεση ελέγχου αρχίζει από τον πελάτη στον εξυπηρετητή αλλά (τουλάχιστον σε μερικές διαμορφώσεις) οι συνδέσεις δεδομένων αρχίζουν από τον εξυπηρετητή στον πελάτη. Αν και τα σύγχρονα firewall μπορούν και χειρίζονται αυτά τα πρωτόκολλα, τέτοιες λύσεις αντιμετωπίζονται ως αρχιτεκτονικά "μη καθαρές" και σε μερικές περιπτώσεις αρκετά επιθετικές.

- Τέλος, υπάρχει μια αυξανόμενη ανάγκη για λεπτομερή έλεγχο πρόσβασης (και ακόμα για έλεγχο οριζόμενο από την εφαρμογή) που τα τυποποιημένα firewall δεν μπορούν εύκολα να επιτρέψουν χωρίς να αυξήσουν πολύ την πολυπλοκότητά τους και την επεξεργασία των απαιτήσεων τους. (Ioannidis)

Παρά τις όποιες ανεπάρκειές τους, τα firewall είναι ακόμα χρήσιμα στην παροχή κάποιου βαθμού ασφάλειας. Ο βασικός λόγος για τη χρησιμότητα των συστημάτων firewall είναι ότι παρέχουν έναν προφανή, μηχανισμό για επιβολή πολιτικής ασφάλειας δικτύων. Για τις μη τυποποιημένες εφαρμογές και δίκτυα, είναι πιθανώς ο μόνος μηχανισμός για την παροχή υπηρεσιών ασφάλειας. Ενώ τα νεώτερα πρωτόκολλα σε αρκετές περιπτώσεις παρέχουν υπηρεσίες ασφάλειας, δεν ισχύει το ίδιο για τα παλαιότερα πρωτόκολλα και τις εφαρμογές τους. Επιπλέον, τα firewall αποτελούν ένα πρώτου επιπέδου εμπόδιο που επιτρέπει άμεσες αποκρίσεις σε καινούρια προβλήματα και αδυναμίες. (Ioannidis)

3.4 Βασικές Μέθοδοι Ελέγχου Ασφάλειας των Εφαρμογών Ιστού

Ο συνεχής έλεγχος και η μέτρηση της ασφάλειας των εφαρμογών ιστού είναι απαραίτητη προϋπόθεση για τη διατήρηση της ασφάλειας ενός συστήματος, το οποίο συνδέεται στο Web. Όμως σε έναν ιστότοπο είναι δυνατό να φιλοξενείται ένα μεγάλο πλήθος εφαρμογών ιστού διαφορετικού τύπου με διαφορετικό λογισμικό. Οι εφαρμογές ιστού κατασκευάζονται σε επίπεδα, από προγράμματα και δεδομένα τα οποία φιλοξενούνται σε πολλαπλούς servers(web servers, application servers, database servers). Για το λόγο αυτό υπάρχουν διάφορες μέθοδοι ελέγχου ασφάλειας

των εφαρμογών ιστού. Οι σημαντικότερες και ευρέως χρησιμοποιούμενες μέθοδοι είναι οι ακόλουθες: (Μακρής)

- Επιθεώρηση Ασφάλειας (security audit):
    - Ένα σύστημα ελέγχεται με βάση ένα σύνολο από λίστες ελέγχου (checklists), οι οποίες διαμορφώνονται με βάση διεθνή πρότυπα σχετικά με την ασφάλεια, καθώς και κατάλληλες πολιτικές ασφάλειας του οργανισμού, που χρησιμοποιεί την εφαρμογή ιστού.
    - Οι ελεγκτές εκτελούν την εργασία τους μέσα από προσωπικές συνεντεύξεις, ανιχνεύσεις αδυναμιών, εξετάσεις των ρυθμίσεων, αναλύσεις των διαμοιρασμένων πόρων δικτύου και μελέτες των ιστορικών στοιχείων (log files). (Μακρής)
- Αυτο - αξιολόγηση Ασφάλειας (security self-assessment):
    - Εδώ δεν υπάρχουν συγκεκριμένα standards ως προς τα οποία θα μετρηθεί το σύστημα, αλλά ο στόχος προσδιορίζεται από την περιοχή, που χρειάζεται διερεύνηση και βελτίωση στη θωράκισή της.
    - Ξεπερνά τους πίνακες ελέγχου (checklists) και επεκτείνεται σε ένα πιο λεπτομερή έλεγχο για εντοπισμό αδυναμιών, αλλά και σε συστάσεις για επιδιορθώσεις και βελτιώσεις.
    - Πλεονέκτημά της είναι η δυνατότητα να οριστούν επίπεδα προτεραιότητας σε κάθε συστατικό που αξιολογείται, έτσι ώστε με την ολοκλήρωσή της να δοθεί μια κατάταξη προτεραιοτήτων στην επιδιόρθωση των ευπαθειών που ανιχνεύθηκαν. (Μακρής)
- Δοκιμή Διείσδυσης (penetration testing ή "ethical hacking"):
    - Είναι η ελεγχόμενη προσομοίωση μιας επίθεσης προκειμένου να επιτευχθεί ένας προκαθορισμένος στόχος. Επίσης είναι γνωστή και ως εσωτερική επιθεώρηση ασφάλειας (internal security auditing).
    - Σκοπός της είναι να εντοπιστούν συγκεκριμένες πληροφορίες σχετικές με την ύπαρξη γνωστών ευπαθειών και να διερευνηθεί κατά πόσο είναι δυνατόν ένας ξένος, κάνοντας χρήση αυτών των πληροφοριών, να

είναι σε θέση να δημιουργήσει προβλήματα στην εφαρμογή ιστού. Δεν έχει σκοπό να εντοπίσει όλες τις ευπάθειες, αλλά να αποδείξει ότι η ασφάλεια του συστήματος μπορεί να διακυβευτεί.

- Η δοκιμή μπορεί να πραγματοποιηθεί στη βάση μηδενικής γνώσης (zero knowledge) ή με πλήρη γνώση (full knowledge) του συστήματος, που δοκιμάζεται. Χρησιμοποιείται για να καθορίσει την αξιοπιστία και τη δύναμη των μέτρων ασφάλειας, που παίρνουμε.
- Οι "ethical hackers" προσπαθούν να υιοθετήσουν τις τεχνικές επιθέσεων των hackers, ώστε να μπορέσουν να μετρήσουν το επίπεδο ασφάλειας της εφαρμογής. (Μακρής)

3.4.1 Σύγκριση των Μεθόδων Μέτρησης Ασφάλειας

Κάνοντας μια σύγκριση των μεθόδων μέτρησης ασφάλειας των εφαρμογών ιστού μπορούμε να πούμε ότι: (Μακρής)

- Για τον έλεγχο της ασφάλειας μιας εφαρμογής ιστού με τις μεθόδους της επιθεώρησης ασφάλειας και της αυτο-αξιολόγησης απαιτείται η μετακίνηση μιας μεγάλης ομάδας ειδικών ασφαλείας στον τόπο που λειτουργεί ο οργανισμός, του οποίου η ασφάλεια της εφαρμογής ελέγχεται.
- Η ομάδα αυτή πρέπει να έχει στη διάθεσή της τα κατάλληλα checklists, να έχει υψηλή τεχνογνωσία και να είναι άρτια συντονισμένη.
- Για την ενέργεια των ελέγχων απαιτείται πολύς χρόνος, ώστε να ολοκληρωθούν οι συνεντεύξεις, οι επιθεωρήσεις, οι αξιολογήσεις και οι έρευνες στη διάρκεια των οποίων αποκαλύπτεται και διαταράσσεται η λειτουργία του οργανισμού. (Μακρής)

Όλα τα παραπάνω σε συνάρτηση με την ανάγκη για συνεχείς και επαναλαμβανόμενους ελέγχους καθιστούν τη δοκιμή διείσδυσης μονόδρομο. Επιπλέον, η δοκιμή διείσδυσης έχει τα ακόλουθα πλεονεκτήματα: (Μακρής)

- απαιτείται ελάχιστο προσωπικό και δεν είναι αναγκαία η μετακίνησή του
- παρέχει τη δυνατότητα πλήρους αυτοματοποίησης

- διαρκεί ελάχιστο χρόνο και είναι εύκολα επαναλαμβανόμενη
- δεν απαιτεί τη σε βάθος γνώση της ελεγχόμενης εφαρμογής
- δεν διαταράσσει τη λειτουργία της
- είναι πολύ οικονομικότερη από τις δύο άλλες μεθόδους.

3.4.2 Τεχνικές Δοκιμής Διείσδυσης

Υπάρχουν δύο κύριες προσεγγίσεις τεχνικών ελέγχου ασφάλειας των εφαρμογών ιστού με τη μέθοδο της δοκιμής διείσδυσης: (Μακρής)

- Χειροκίνητη (manual), στην οποία όλη η διαδικασία ελέγχου γίνεται βήμα-βήμα χωρίς την ύπαρξη αυτοματισμών επανάληψης παρόμοιων βημάτων.
- Αυτοματοποιημένη (automated), στην οποία με τη χρήση εργαλείων αυτοματοποιούνται μερικοί ή όλοι οι έλεγχοι και οι διαδικασίες ελέγχου. Η αυτοματοποιημένη διακρίνεται σε δύο τεχνικές:
    - Black Box : ονομάζεται η εφαρμογή δοκιμαστικών δεδομένων που έχουν προέλθει από καθορισμένες λειτουργικές απαιτήσεις χωρίς να λαμβάνουν υπόψη τη δομή της εφαρμογής, στην οποία εφαρμόζονται. Η εφαρμογή εξετάζεται χρησιμοποιώντας την εξωτερική της διεπαφή, αυτή, που χρησιμοποιούν οι απλοί χρήστες. Μιμούνται την ακολουθία αλληλεπιδράσεων χρήστη-εφαρμογής και κάθε αποτυχία δείχνει ότι ο χρήστης έλαβε ανεπαρκή υπηρεσία.
    - White Box : ονομάζεται η τεχνική στην οποία εξετάζεται η δομή της εφαρμογής και στη βάση αυτής καθορίζονται τα δεδομένα της δοκιμής. Εξετάζεται η εσωτερική δομή της εφαρμογής χρησιμοποιώντας τη διεπαφή προγραμματισμού εφαρμογών (Application Programming Interface), η οποία αποτελεί το μέσο επικοινωνίας των εφαρμογών με τον πυρήνα του λειτουργικού συστήματος ή με βιβλιοθήκες τρίτων κατασκευαστών. (Μακρής)

4 ΚΕΦΑΛΑΙΟ ΜΕΛΕΤΗ ΠΕΡΙΠΤΩΣΗΣ

Για την σύγκριση των firewalls χρησιμοποιήθηκαν τα κριτήρια που καθορίζονται στην διεύθυνση www.giac.org. Έτσι συγκρίνονται τα πιο γνωστά προσωπικά firewalls και στην συνέχεια παρουσιάζονται τα χαρακτηριστικά τους σε ένα συγκεντρωτικό πίνακα. Τα κριτήρια είναι τα ακόλουθα: (Epstein)

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): Δυ νατότητα 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 (Epstein)

4.1 Τρόποι ελέγχου των firewalls

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

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

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

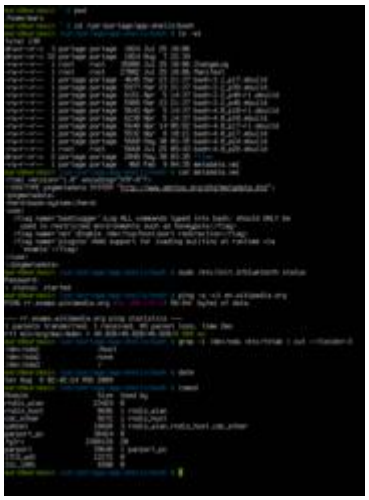
Δ) Σκανάρισα κάθε firewall χρησιμοποιώντας το εργαλείο nmap για να ελεγχθούν ποια ports μπλοκαρίστηκαν από τα firewalls αποτελεσματικά.

Η συγκριση έγινε με επίθεση από Η/Υ σε Η/Υ ίδιας τεχνολογιας, ήτοι Intel Pentium 4 με επεξεργαστή 3,2Ghz, 160 Gb σκληρό δίσκο και 4 gb RAM. (Epstein)

4.2 Εργαλεία που χρησιμοποιήσαμε

4.2.1 Διερμηνέας γραμμής εντολών

Ένας διερμηνέας γραμμής εντολών (Command line Interpreter) ή κέλυφος γραμμής εντολών είναι ένα πρόγραμμα υπολογιστή το οποίο διαβάζει γραμμές κειμένου από τον χρήστη και τα διερμηνεύει προς τον αντίστοιχο λειτουργικό σύστημα ή γλώσσα προγραμματισμού. (Epstein)



Εικόνα 6 Windows Command promnt

Ο διερμηνέας γραμμής εντολών δίνει στον χρήστη την δυνατότητα να χρησιμοποιήσει διάφορες εντολές με πολύ αποτελεσματικό (και συχνά λιτό) τρόπο. Απαιτείται από τον χρήστη να γνωρίζει τα ονόματα των εντολών και τους (αν παίρνει) παραμέτρους της κάθε εντολής, και την σύνταξη της γλώσσας την οποία ο χρήστης χρησιμοποιεί. Από το 1960 και μετά, η αλληλεπίδραση του χρήστη με τους υπολογιστές γινόταν κατά κύριο λόγο μέσω της διεπαφής γραμμής εντολών. Στην δεκαετία του 1970 άρχισε η έρευνα για την ανάπτυξη γραφικού περιβάλλοντος χρήστη (GUI) οπού όλες οι λειτουργίες θα γινόταν μέσω γραφικού περιβάλλοντος σε αντίθεση με την διεπαφή γραμμής εντολών που χρησιμοποιείται κείμενο. Μετά από

αυτό το GUI είναι ο πιο συνηθισμένος τρόπος επικοινωνίας με τον υπολογιστή. Παρόλα αυτά η γραμμή εντολών χρησιμοποιείται ακόμα σε ορισμένες περιπτώσεις οπού παρέχει ευελιξία έναντι του γραφικού περιβάλλοντος. (http://osarena.net)

Εμείς χρησιμοποιήσαμε την γραμμη εντολών των Windows για να κανουμε επιθεσή με την εντολή: (Epstein)

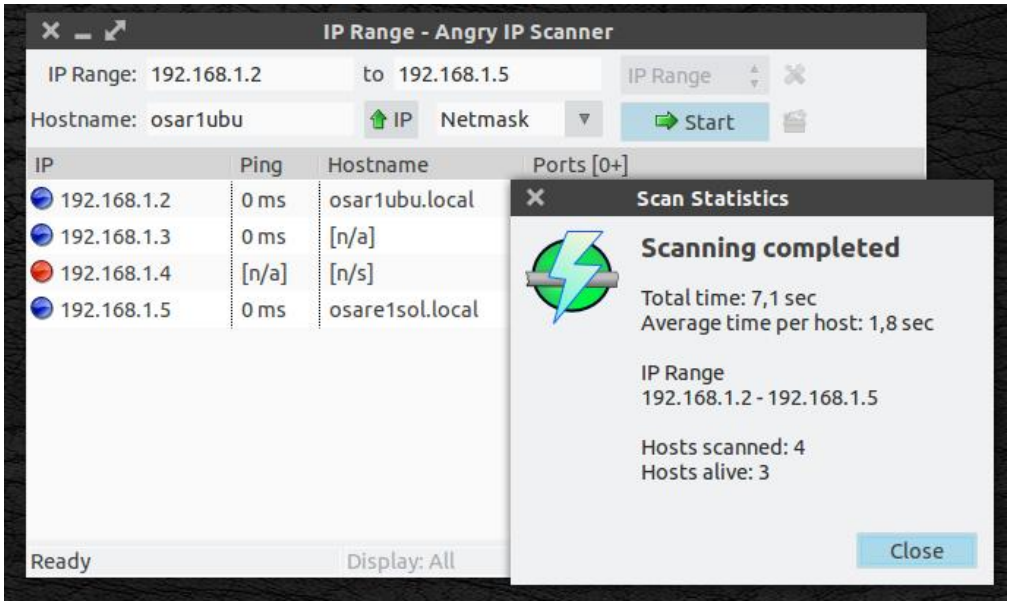
ping -a -t 192.168.2.1

4.2.2 Angry IP Scanner

Το **Angry IP Scanner**, είναι ένα πολύ καλό εργαλείο που επιτρέπει εύκολη και γρήγορη σάρωση ενός τοπικού δικτύου, τόσο από τον διαχείριση του δικτύου, όσο και από τον οποιοδήποτε χρήστη. Με εύκολο περιβάλλον και ρυθμίσεις, είναι γραμμένο σε Java και διαθέσιμο για Linux, Windows, OSX. (http://osarena.net)

Μόλις το Angry IP Scanner ανιχνεύσει μια ενεργή διεύθυνση IP, θα δώσει πληροφορίες για MAC, ports και hostname. Τα δεδομένα που συγκεντρώθηκαν στη συνέχεια μπορούν να αποθηκευτούν ως TXT, CSV, XML ή IP-Port list files. Ακόμα, το ποσό των δεδομένων που συγκεντρώθηκαν για κάθε host, μπορεί να επεκταθεί με plugins.

Έχει, επίσης, πρόσθετα χαρακτηριστικά, όπως πληροφορίες NetBIOS (το όνομα του υπολογιστή, workgroup όνομα, κλπ). Επίσης έχει την δυνατότητα υποβολής αιτήσεων στην ip που επιθυμούμε. Αρα μέσω αυτού μπορούμε να στειλουμε πολλαπλες αιτήσεις –εισβολές στην ip του αλλου Η/Υ. (http://osarena.net)



Εικόνα 7 Angry ip scanner

Εικόνα 8 Angry ip scanner

4.2.3 Nessus 5.0

Το Nessus 5.0 Vulnerability scanner είναι ιδιοκτησία της Tenable Network Security®. (www.tenable.com)

Το εργαλείο Nessus παρέχει υποστήριξη για πληθώρα λειτουργικα συστήματα στα οποία μπορεί να εγκατασταθεί και λειτουργήσει, οπως λειτουργικά τύπου *NIX, Windows και Mac OS/ Βασίζεται στην αρχιτεκτονική πελάτη – εξυπηρετητή, η οποία έχει ως προτερήματα τη διαχείριση καθώς και τη λειτουργία του λογισμικού να πραγματοποιείται μέσω της web διεπαφής που παρέχεται και η οποία είναι κοινή για όλα τα λειτουργικα συστήματα αφού η χρήση της υποστηρίζεται σχεδόν απο κάθε

γνωστή φυλλομετρητή ιστού με ενεργοποιημένη την τεχνολογία flash. (www.tenable.com)

Το Nessus είναι ένα ισχυρό και εύκολο στη χρήση εργαλεκο σάρωσης, για την ασφάλεια δικτύων. Περιέχει μια ευρεία βάση δεδομένων απο plugins που ενημερώνεται καθημερινα. Σήμερα καταλέγεται μεταξύ των κορυφαίων προίοντων αυτού του τύπου σε όλη τη βιομηχανία της ασφάλειας και έχει εγκριθεί απο επαγγελματικές οργανώσεις της ασφάλειας πληροφοριών, όπως το Ινστιτούτο SANS. Επιτρέπει τον έλεγχο εξ' αποστάσεως ενός δεδομένου δικτύου και μπορεί να διαπιστώσει κατα πόσο το συγκεκριμένο δίκτυο έχει παραβιαστεί με κάποιο τρόπο. Το Nessus επίσης παρέχει τη δυνατότητα τοπικού ελέγχου σε συγκεκριμένα μηχανήματα-στόχους, είτε για τρωτά σημεία που ίσως διαθέτουν, είτε για την διαπίστωση τήρησης προδιαγραφών, είτε για παραγιάσεις της πολιτικής περιεχομένου, και πολλά αλλα.

4.2.4 Διαδικασία που ακολουθήθηκε

Εμείς από ένα κεντρικό Η/Υ με την χρήση των παραπάνων εργαλείων κάναμε μια σειρά από διαφόρων εδώ εισβολές σε Η/Υ που ηταν εγκατεστημένα τα διαφορα firewalls. Με το πρόγραμμα Nessus είδαμε τις τρύπες του κάθε firewall σε όλα τα επίπεδα. Στο κείμενο που ακολουθεί θα αναλύσουμε το κάθε firewall και τι συμπέρασμα προέκυψε από την ερευνα μας.

4.3 Αναλυτική παρουσίαση των firewalls

4.3.1 McAfee Firewall 2.1 .3

Το McAfee Firewall βασίζεται στο Conseal Signal-9 Private Desktop. 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. (Rattle)

Η SYSTEM traffic είναι πιο στατική και θα επιτρέψει ή δεν θα επιτρέψει πράγμ ατα 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. (Rattle)

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 αρχείω ν-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. (Rattle)

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 : (Rattle)

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 αποτελεσμ ατικά.

2. Ο χρήστης μπορεί να ξεχάσει/παραμελήσει να εγκαταστήσει το φίλτρο πρωτοκόλλου , αφήνοντας όνο 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 δια ορφώσει κανόνες για συγκεκριμένα TCP/UDP ports. (Rattle)

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) χρησιοποιεί μια συγκεκριμένη εφαρμογή

2. Log αρχεία: Το log αρχείο είναι ένα απλό αρχείο κει ένου που μπορεί να ανοιχτεί εύκολα με το notepad. Περιλα βάνει 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 (Rattle)

Μειονεκτήματα :

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

2. 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.

3. Απενγκατάσταση: ο Network Driver δεν διαγράφεται αλλά πρέπει να αφαιρεθεί με το χέρι.

4. The GUI είναι ιδιόορφο: - Όταν επιδεικνύει δραστηριότητα, έπρεπε να παρουσιάζει ποια κυκλοφορία διεπαφής (interface traffic) είναι ανοικτή.

5. 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.

6. 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.

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

8. 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 .

9. Τα port του NetBIOS δεν προστατεύονται by default.

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

11. Δεν υποστηρίζει πλήρως Windows 2000, XP, 7

12. Μεγάλο μέγεθος (6.5 MB) (Rattle)

Προτεινόμενες βελτιώσεις :

- Επίδειξη ενός πιο κατανοητού ονόματος για την εφαρμογή και ερώτηση στο χρήστη ποιο port οι εφαρμογές θέλουν να χρησι οποιήσουν, 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.
- Δεν είναι δυνατό να διαμορφωθούν οι κανόνες για συγκεκριμένα TCP/UDP ports
- Καλύτερο documentation.
- Τα power-saving modes των laptop δεν λειτουργούν με το firewall ενεργό .
- 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.
- Εάν γίνουν αλλαγές στους κανόνες ή στις εφαρμογές, πρέπει να γίνει "Save Settings." διαφορετικά οι αλλαγές θα χαθούν στο επόμενο reboot.
- Πιο εύκολη απεγκατάσταση (Rattle)

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

Εικόνα 9 McAfee 2.1 .3

Σύνοψη

Το McAfee είναι ένα 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 laptop δεν θα είναι ευχαριστημένοι γιατί δεν θα λειτουργούν τα power-saving modes.

Αποτέλεσματα γραμής εντολών

Από το Angry Ip scanner στελναμε 2000 αιτήσεις ανα 1s με καθυστερηση 10ms. Ταυτοχρονα από την γραμμη εντολών στελναμε πακετα των 32 bytes περιμένωντας ποτε θα «πέσει» το τείχος προστασίας:

C:\Documents and Settings\admin>ping -t -a 192.168.2.1

Γίνεται Ping στο 192.168.2.1 με 32 bytes δεδομένων:

Απάντηση από: 192.168.2.1: bytes=32 χρόνος<1ms TTL=64

Απάντηση από: 192.168.2.1: bytes=32 χρόνος<1ms TTL=64

....

Απάντηση από: 192.168.2.1: bytes=32 χρόνος<1ms TTL=64

Απάντηση από: 192.168.2.1: bytes=32 χρόνος<1ms TTL=64

Στατιστικά στοιχεία Ping για 192.168.2.1:

Πακέτα: Απεσταλμένα = 3218, Ληφθέντα = 3200, Απολεσθέντα = 18 (απώλεια 0%),

Πλήθος διαδρομών αποστολής και επιστροφής κατά προσέγγιση σε χιλιοστά του δευτερ ολέπτου:

Ελάχιστο = 0ms, Μέγιστο = 15s, Μέσος όρος = 7s

Report firewall

Χρόνος κατάρευσης firewall: 45s

4.3.2 TermiNET 1 .76.1 3

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

- Έλεγχος πρόσβασης - καμία αναρμόδια πρόσβαση από έξω. - Stealth Mode - καθιστά το PC αόρατο στον εξωτερικό κόσμο . - Web Blocking - εμποδίζει την πρόσβαση στα ανεπιθύμητα websites - Υποστηρίζει πολλαπλά προφίλ χρηστών - Ανακοίνωση κατά την ανίχνευση παρείσφρησης (Blocking notification on Intrusion detection) - Ευέλικτος έλεγχος κατά την πλοήγηση στο Web (Flexible control for Web Browsing) - Περιορίζει την πρόσβαση με κριτήρια τις διευθύνσεις IP, URLs, Ports και τα χρησιοποιού ενα 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 (η έρα της εβδομάδας).

Αποτελεσματικότητα ασφάλειας

Το σύστημα εξετάστηκε στην προεπιλεγμένη "stealth mode"

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

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

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

Δ. Άλλα Tests -Η κυκλοφορία του NetBEUI δεν ανιχνεύθηκε ούτε μπλοκαρίστηκε. -Δεδομένου ότι οι εξερχόμενες συνδέσεις επιτρέπο νται , πληροφορίες θα μπορού σαν εύκολα να διαρρεύσουν από το PC χωρίς τη γνώση του χρήστη. Έτσι εάν ια 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 (η μέρα 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 . 1 55.1 07.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 καταγράφετα.

5. Αυτό κάνει πιο δύσκολο να γίνουν κατανοητές οι επιθέσεις που εξελίσσονται . Αναλύσεις επίθεσης υψηλού επιπέδου δεν παρέχονται . Τα διερχόμενα καθώς επίσης και τα πλοκαρισμένα πακέτα καταγράφονται.

6. 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

Εικόνα 10 TermiNET 1 .76.1 3

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 -Αποτελεσατικότητα της αντίδρασης: η ανακάλυψη της ταυτότητας των επιτιθεμένων και το μπλοκάρισμα των επιθέσεων δεν είναι εύκολα.

Το TermiNET έχει κι αλλά χαρακτηριστικά όπως τα προφίλ πολλών χρηστών. Εντούτοις, χρειάζονται μερικές βελτιώσεις ενώ και η τιμή του είναι υψηλή σε σχέση με τον ανταγωνισμό.

Αποτέλεσματα γραμής εντολών

Από το Angry Ip scanner στελναμε 2000 αιτήσεις ανα 1s με καθυστερηση 10ms. Ταυτοχρονα από την γραμμη εντολών στελναμε πακετα των 32 bytes περιμένωντας ποτε θα «πέσει» το τείχος προστασίας:

C:\Documents and Settings\admin>ping -t -a 192.168.2.1

Γίνεται Ping στο 192.168.2.1 με 32 bytes δεδομένων:

Απάντηση από: 192.168.2.1: bytes=32 χρόνος<1ms TTL=64

Απάντηση από: 192.168.2.1: bytes=32 χρόνος<1ms TTL=64

....

Απάντηση από: 192.168.2.1: bytes=32 χρόνος<1ms TTL=64

Απάντηση από: 192.168.2.1: bytes=32 χρόνος<1ms TTL=64

Στατιστικά στοιχεία Ping για 192.168.2.1:

Πακέτα: Απεσταλμένα = 2700, Ληφθέντα = 2682, Απολεσθέντα = 18 (απώλεια 0%),

Πλήθος διαδρομών αποστολής και επιστροφής κατά προσέγγιση σε χιλιοστά του δευτερ ολέπτου:

Ελάχιστο = 0ms, Μέγιστο = 13s, Μέσος όρος = 6s

Report firewall

Χρόνος κατάρευσης firewall: 115s

4.3.3 Tiny Personal Firewall 2.0.1 3

Σημειώνω ένα απόσπασμα από το website Tiny Personal Firewall: «Το Tiny Personal Firewall αντιπροσωπεύει τη έξυπνη, εύχρηστη προσωπική τεχνολογία ασφάλειας που προστατεύει πλήρως τους προσωπικούς υπολογιστές από τους hackers. Στηρίζεται στο αποδεδειγ ένο 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 περιλα βάνει 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

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 αιτή ατα 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

7. 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

Εικόνα 11 Tiny Personal Firewall 2.0.1 3

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 ορφή pdf) για να μπορέσονν να εκμεταλλευτούν πλήρως τις ικανότητες του συγκεκριμένου firewall.

Αποτέλεσματα γραμής εντολών

Από το Angry Ip scanner στελναμε 2000 αιτήσεις ανα 1s με καθυστερηση 10ms. Ταυτοχρονα από την γραμμη εντολών στελναμε πακετα των 32 bytes περιμένωντας ποτε θα «πέσει» το τείχος προστασίας:

C:\Documents and Settings\admin>ping -t -a 192.168.2.1

Γίνεται Ping στο 192.168.2.1 με 32 bytes δεδομένων:

Απάντηση από: 192.168.2.1: bytes=32 χρόνος<1ms TTL=64

Απάντηση από: 192.168.2.1: bytes=32 χρόνος<1ms TTL=64

....

Απάντηση από: 192.168.2.1: bytes=32 χρόνος<1ms TTL=64

Απάντηση από: 192.168.2.1: bytes=32 χρόνος<1ms TTL=64

Στατιστικά στοιχεία Ping για 192.168.2.1:

Πακέτα: Απεσταλμένα = 6432, Ληφθέντα = 6418, Απολεσθέντα = 18 (απώλεια 0%),

Πλήθος διαδρομών αποστολής και επιστροφής κατά προσέγγιση σε χιλιοστά του δευτερ ολέπτου:

Ελάχιστο = 0ms, Μέγιστο = 45s, Μέσος όρος = 22s

Report firewall

Χρόνος κατάρευσης firewall: 85s

4.3.4 ZoneAlarm 2.6

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

-Η διεπαφή εμπιστού 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 μ ια 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 applications 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 πρόγραμα με ενδιαφέρουσες πληροφορίες και οδηγίες . Ακόμα υπάρχει δυνατότητα βοήθειας on-line έσω 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

1. Εάν χρησιμοποιούνται πολλές εφαρμογές, οι συνεχείς ερωτήσεις στο χρήστη γίνονται ενοχλητικές, και ο χρήστης μπορεί να καταλήξει να εμπιστευθεί περισσότερες εφαρμογές από όσες πρέπει.

2. 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 .

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

4. Δεν μπορεί να διαμορφωθεί να αγνοήσει τα pings από τις άγνωστες πηγές

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

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

7. 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

Εικόνα 12 ZoneAlarm 2.6

Σύνοψη

Το ZoneAlarm είναι μια λύση που διανέμεται δωρεάν. Χρησιμοποιείται από πολλούς χρήστες. Τελευταία ανακοινώθηκε και μια επαγγελματική έκδοση (ή ZoneAlarm Pro) με επιπρόσθετα χαρακτηριστικά ασφαλειας 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

Αποτέλεσματα γραμής εντολών

Από το Angry Ip scanner στελναμε 2000 αιτήσεις ανα 1s με καθυστερηση 10ms. Ταυτοχρονα από την γραμμη εντολών στελναμε πακετα των 32 bytes περιμένωντας ποτε θα «πέσει» το τείχος προστασίας:

C:\Documents and Settings\admin>ping -t -a 192.168.2.1

Γίνεται Ping στο 192.168.2.1 με 32 bytes δεδομένων:

Απάντηση από: 192.168.2.1: bytes=32 χρόνος<1ms TTL=64

Απάντηση από: 192.168.2.1: bytes=32 χρόνος<1ms TTL=64

....

Απάντηση από: 192.168.2.1: bytes=32 χρόνος<1ms TTL=64

Απάντηση από: 192.168.2.1: bytes=32 χρόνος<1ms TTL=64

Στατιστικά στοιχεία Ping για 192.168.2.1:

Πακέτα: Απεσταλμένα = 3264, Ληφθέντα = 3232, Απολεσθέντα = 18 (απώλεια 0%),

Πλήθος διαδρομών αποστολής και επιστροφής κατά προσέγγιση σε χιλιοστά του δευτερ ολέπτου:

Ελάχιστο = 0ms, Μέγιστο = 38s, Μέσος όρος = 19s

Report firewall

Χρόνος κατάρευσης firewall: 225s

4.3.5 Sygate Personal Firewall v4

Σύμφωνα με το website του Sygate Personal Firewall: «Το Firewall Sygate προστατευει 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 διαδίκτυο 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.

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 δια ορφωθούν 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, 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 ασφ άλειας 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

Εικόνα 13 Sygate v4

Σύνοψη

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

Αποτέλεσματα γραμής εντολών

Από το Angry Ip scanner στελναμε 2000 αιτήσεις ανα 1s με καθυστερηση 10ms. Ταυτοχρονα από την γραμμη εντολών στελναμε πακετα των 32 bytes περιμένωντας ποτε θα «πέσει» το τείχος προστασίας:

C:\Documents and Settings\admin>ping -t -a 192.168.2.1

Γίνεται Ping στο 192.168.2.1 με 32 bytes δεδομένων:

Απάντηση από: 192.168.2.1: bytes=32 χρόνος<1ms TTL=64

Απάντηση από: 192.168.2.1: bytes=32 χρόνος<1ms TTL=64

....

Απάντηση από: 192.168.2.1: bytes=32 χρόνος<1ms TTL=64

Απάντηση από: 192.168.2.1: bytes=32 χρόνος<1ms TTL=64

Στατιστικά στοιχεία Ping για 192.168.2.1:

Πακέτα: Απεσταλμένα = 12800, Ληφθέντα = 12768, Απολεσθέντα = 18 (απώλεια 0%),

Πλήθος διαδρομών αποστολής και επιστροφής κατά προσέγγιση σε χιλιοστά του δευτερ ολέπτου:

Ελάχιστο = 0ms, Μέγιστο = 138s, Μέσος όρος = 69s

Report firewall

Χρόνος κατάρευσης firewall: 625s

4.3.6 Συμπερασματικός πίνακας

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

Οι επιθέσεις γίναν μεταξύ 2 υπολογιστών (ίδιων επιδόσεων, ίδιων λειτουργικών) συνδεμένοι μεταξύ τους χωρις να παρεμβαλετε κατι άλλο μεταξυ τους. Τα firewalls κατεβάστηκαν οι free εκδόσεις τους.

FIREWALL	Χρόνος Κατάρευσης
McAfee	45
TermiNET	115
Tiny Personal Firewall	85
ZoneAlarm	225
Sygate Firewall	625

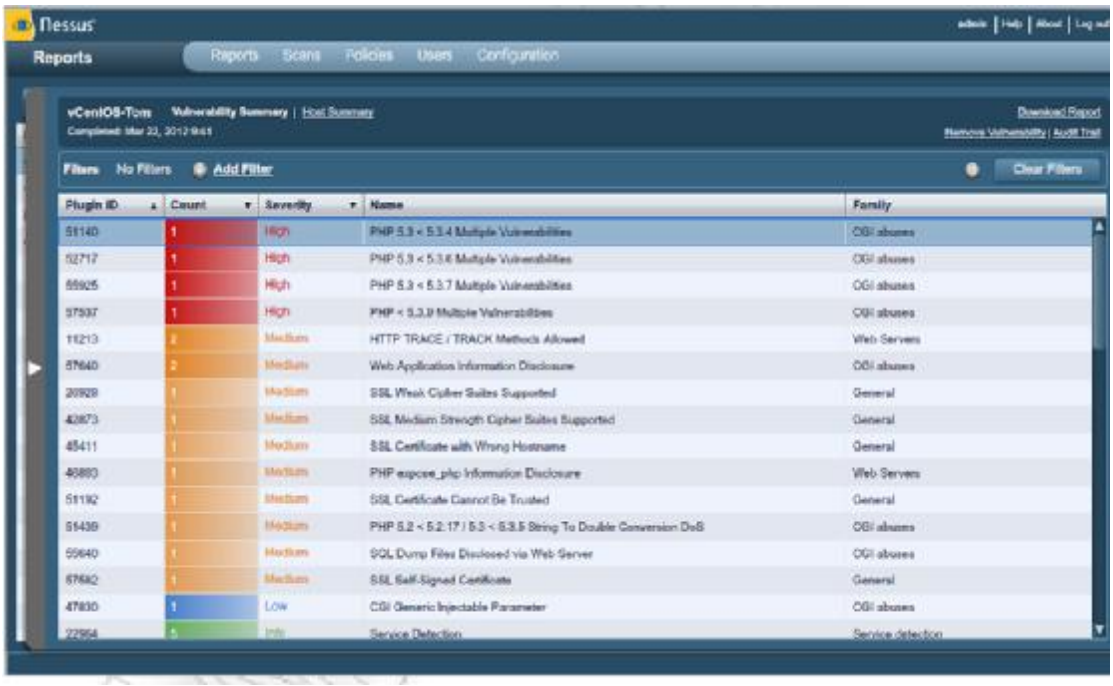
Εικόνα 14 Πίνακας αποτελεσμάτων ερευνας

4.3.7 Άλλα Firewall-like Προϊόντα

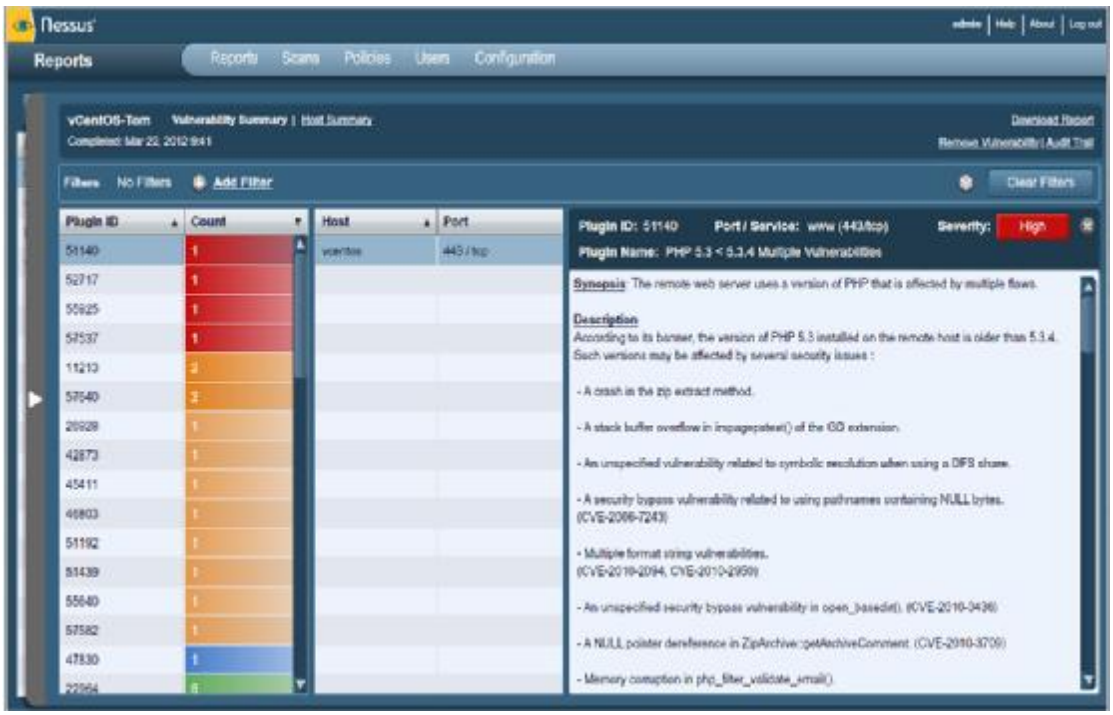
- MailControl 1 .0

- WinRoute Pro 4.1 Build 24
- SOCKS2HTTP 0.73 Beta

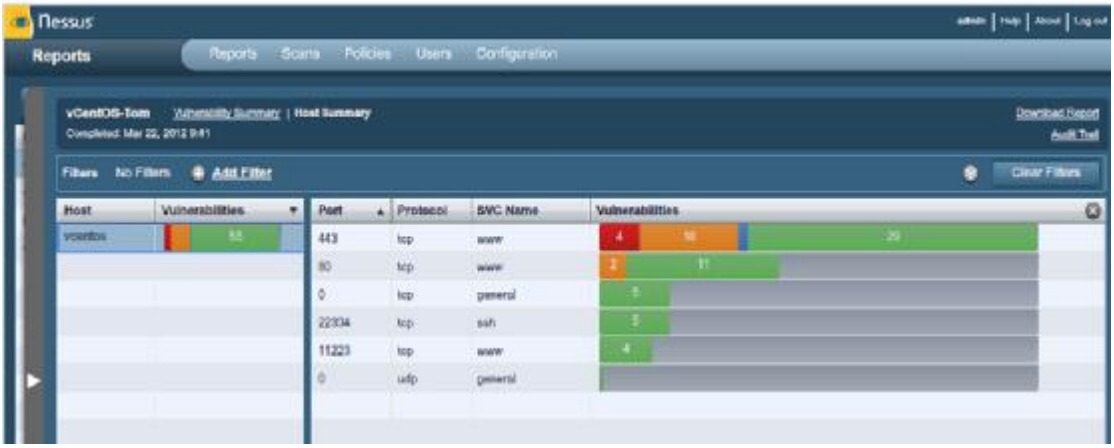
4.4 Αποτελέσματα από το πρόγραμμα Nessus



Εικόνα 15 Εμφάνιση αποτελεσμάτων σάρωσης

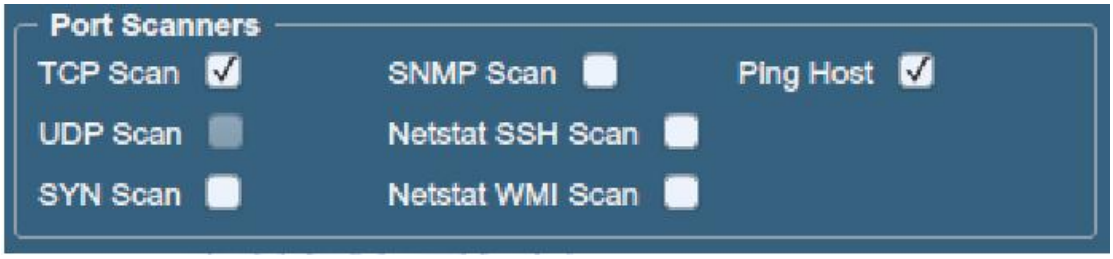


Εικόνα 16 Επισκόπηση αποτελέσματος αππ Plugin

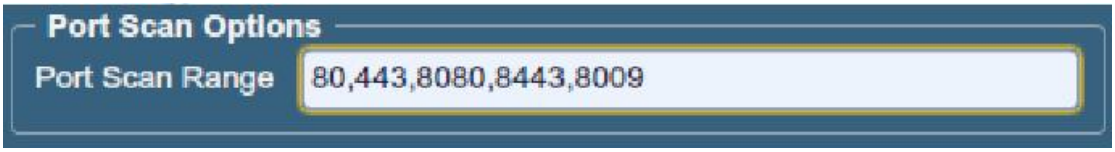


Εικόνα 17 Αποτελέσματα που αφορούν το συγκεκριμένο Host name

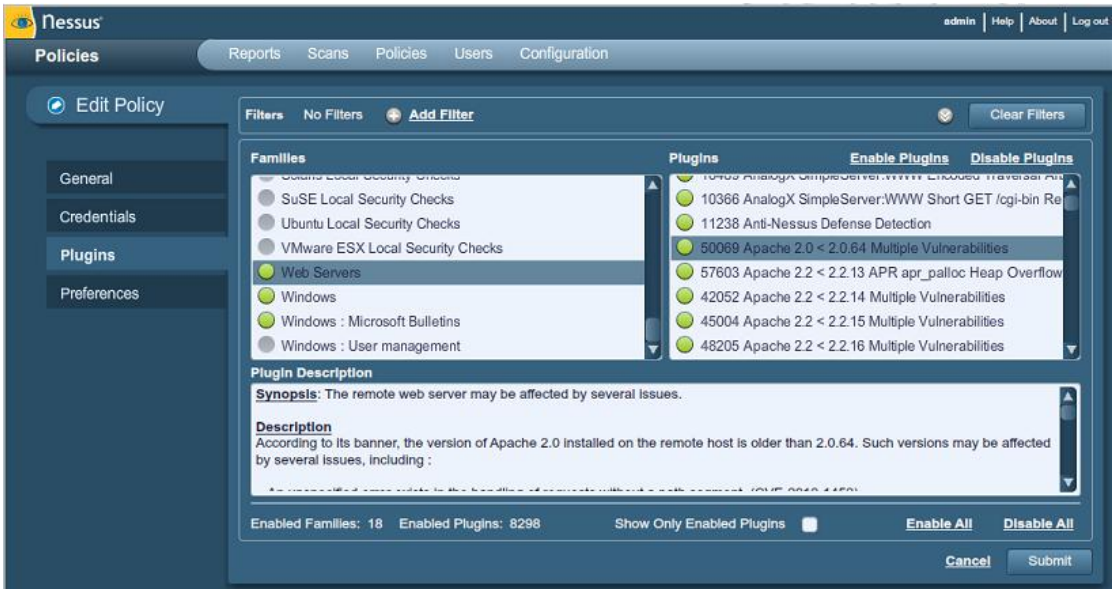
Εικόνα 18 Policy



Εικόνα 19 policy/Port Scanners



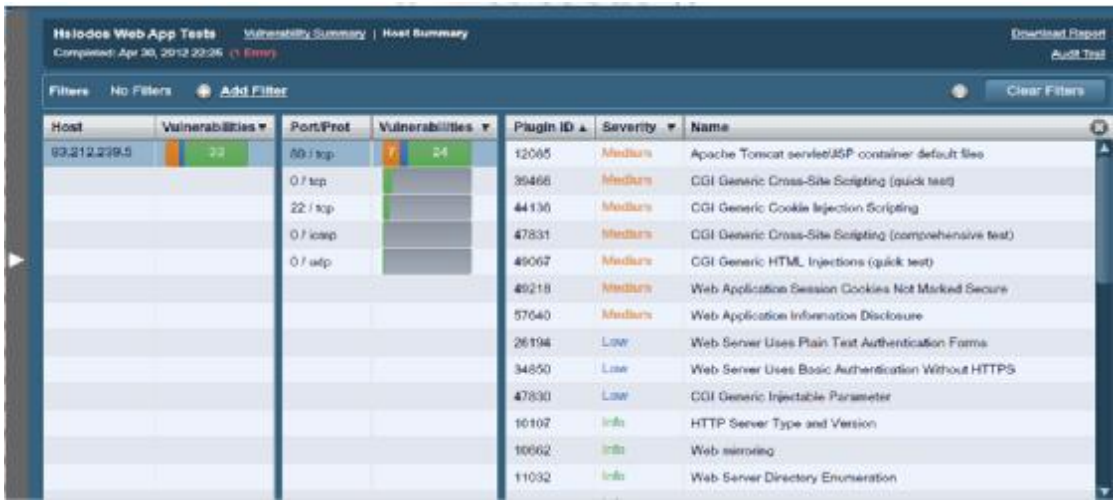
Εικόνα 20 policy/Port Scan Options



Εικόνα 21 Policy/Plugins

Εικόνα 22 Παρουσίαση αποτελεσμάτων

Εικόνα 23 Ανοικτών Ports



Εικόνα 24 Παρουσίαση ευπαθειών που αφορούν το port 80

Εικόνα 25 Παρουσίση ελεγχού σε τοπικό επίπεδο

Κατηγορία	**Περιγραφή**
A1 - Injections	SQL Injection (CGI abuses) • 11139, 42424, 42426, 42427, 42479, 43160, 51973 XML Injection (CGI abuses) • 46196 HTTP Header Injection (CGI abuses: XSS)

	• 39468, 49067 Cookie Injection (CGI abuses) • 44135
A2 – Cross-Site Scripting (XSS)	Cross-Site Scripting (CGI abuses: XSS) • 10815, 39466, 42425, 47831, 46193, 49067, 51972
A3 – Broken Authentication and Session Management	Μη πραγματοποίηση αυθεντικοποίησης μέσω SSL πρωτοκόλλου • 26194, 34850 Δέουσα εφαρμογή του πρωτοκόλλου SSL • 15901, 20007, 26928, 35291, 42053, 42873 , 42880, 53491, 53360, 56043, 56284, 56984, 57041
A4 – Insecure Direct Object References	Δυνατότητα περιήγησης σε καταλόγους ιστού (web catalogs) • 40984 Path Transversal (CGI abuses) • 50494 Παράμετροι που προσδιορίζονται για χειροκίνητες δοκιμές • 40773, 44134, 47830
A5 – Cross-Site Request Forgery (CSRF)	On Site Request Forgery (CGI Generic) • 47832

Εικόνα 26 Plugin και έλεγχος

4.5 Συμπεράσματα

Από την παραπάνω εργασία καταλήξαμε σε συμπεράσματα, τόσο θεωρητικού όσο και πρακτικού ενδιαφέροντος, σχετικά με τον σχεδιασμό και την διαμόρφωση των αντιπυρικών ζωνών στα σημερινά δίκτυα.

Όσο αφορά το θεωρητικό κομμάτι, έγινε αντιληπτό ότι οι αντιπυρικές ζώνες, ανεξάρτητα από την πολυπλοκότητα του σχεδιασμού και της υλοποίησης, έχουν την ευθύνη να ενεργήσουν ως σημεία επιβολής της πολιτικής ασφάλειας. Αυτό επιτυγχάνεται με την επιθεώρηση των δεδομένων που λαμβάνονται και την παρακολούθηση των συνδέσεων, ώστε να καθοριστούν τα δεδομένα που πρέπει να επιτραπούν η όχι. Επιπλέον, οι αντιπυρικές ζώνες μπορούν να ενεργήσουν ως ενδιάμεσοι και πληρεξούσιοι στα αιτήματα ενός προστατευμένου συστήματος, παρέχοντας συγχρόνως επικύρωση πρόσβασης για να εξασφαλίσουν ότι χορηγείται μόνο εγκεκριμένη πρόσβαση. Τέλος, οι αντιπυρικές ζώνες μπορούν να υποβάλουν εκθέσεις και προειδοποιήσεις σχετικά με τα γεγονότα και τις διαδικασίες, επιτρέποντας στον διαχειριστή να γνωρίζει την κατάσταση της αντιπυρικής ζώνης και των συστημάτων που προστατεύει.

Η σημαντικότερη εργασία που μπορεί να γίνει για να εξασφαλιστεί ότι μια αντιπυρική ζώνη μπορεί να προστατεύσει αποτελεσματικά τους πόρους, γίνεται με τη λήψη της καλύτερης απόφασης σχετικά με το τι πρέπει να προστατεύσει και πού θα τοποθετηθεί. Είναι σημαντικό να γίνει κατανοητός ο σχεδιασμός αντιπυρικών ζωνών που θα προστατεύσει καλύτερα τους πόρους που χρειάζονται προστασία. Αν και μια αντιπυρική ζώνη θα δίνει μια επαρκή προστασία των περισσότερων πόρων, ορισμένα περιβάλλοντα υψηλής ασφάλειας μπορούν να χρησιμοποιήσουν μια αρχιτεκτονική διπλών-αντιπυρικών ζωνών ώστε να ελαχιστοποιήσουν την έκθεση σε κίνδυνο.

Ένας μεγάλος αριθμός κινήτρων οδηγεί τους ανθρώπους σε απειλές και επιθέσεις προς στα συστήματά μας. Με την εξέταση των απειλών και των κατάλληλων απαντήσεων, μπορούμε να αναπτύξουμε μια πολιτική ασφάλειας που θα ελαχιστοποιεί τον κίνδυνο που παρουσιάζεται από μια απειλή, μέσω του κατάλληλου σχεδιασμού και διαμόρφωσης της αντιπυρικής ζώνης. Αν και μια αντιπυρική ζώνη δεν μπορεί να αποτρέψει όλες τις επιθέσεις, είναι μια από τις καλύτερες μεθόδους για να προστατεύουμε τους πόρους.. Ένα άλλο σημαντικό στοιχειό που πρέπει να θυμόμαστε, είναι ότι μια αντιπυρική ζώνη δεν είναι απλά μια συσκευή. Είναι ένα

σύστημα συσκευών που, εάν εφαρμόζεται κατάλληλα, παρέχει σε πολλαπλά επίπεδα μια άμυνα μεταξύ των πόρων που θέλετε να προστατεύσετε και τους κακόβουλους χρήστες που θέλουν να αποκτήσουν πρόσβαση σε αυτά.

4.6 Μελλοντικές έρευνες

Μελλοντικά μπορούν να γίνουν έρευνες σε προπτυχιακό ή και σε μεταπτυχιακό επίπεδο. Οι έρευνες αυτές μπορεί να έχουν ως αντικείμενο άλλα firewall της αγοράς ή και κρατικών οργανισμών, μη εμπορεύσιμα. Επίσης θα μπορούν να επεκταθούν σε άλλα κριτήρια συγκρισημότητας όπως αυτά που εμφανίζονται στην ελληνική και παγκόσμια βιβλιογραφία.

Επίσης οι μελέτες αυτές θα μπορούσαν να βοηθήσουν στην ανάπτυξη καλύτερων τειχών προστασίας και να βελτιωθεί η ασφάλεια σε όλους τους τομείς. Παράλληλα να μελετηθούν νέα δεδομένα πρόσβασης και να αναπτυχθούν προγράμματα αποτροπής πρόσβασης.

Καλό θα ήταν και η αρτιότερη και ορθότερη εκπαίδευση και ενημέρωση των χρηστών των προγραμμάτων αυτών, όπως και η αναπττυξή νέων λογισμικών στο τομέα αυτό. Επίσης πρέπει να εξετάστει η νομική και ηθική πλευρά των προγράμματων και των συστημάτων αυτών.

5 Βιβλιογραφία

Έντυπη ελληνόγλωσση βιβλιογραφία

- "Ασφάλεια Πληροφοριακών και Επικοινωνιακών Συστημάτων (Εννοιολογική θεμελίωση)", Κάτσικας Σωκράτης, Σημειώσεις Ασφάλειας, Τμήμα Μηχανικών Πληροφοριακών & Επικοινωνιακών Συστημάτων Πανεπιστήμιο Αιγαίου.
- "Ασφάλεια Πληροφοριακών Συστημάτων σε περιβάλλοντα υψηλής ευπάθειας", Γκρίτζαλης Δημήτρης, Διδακτορική Διατριβή, Πανεπιστήμιο Αιγαίου, Μάιος 1994.
- "Ασφάλεια στις τεχνολογίες πληροφοριών και επικοινωνιών: Εννοιολογική θεμελίωση", Γκρίτζαλης Δημήτρης, Εκδόσεις Νέων Τεχνολογιών, 1996.
- Μακρής Χαράλαμπος, Αξιολόγηση ευπαθειών και τρόποι αντιμετώπισης τους σε διαδικτυακές εφαρμογές και εξυπηρετητές, 2011, Πανεπιστήμιο Πειραιώς
- Βασικές Αρχές Ασφάλειας Δικτύων by Stalings Williams,Κλειδάριθμος.
- Παπαδόπουλός Αν. Σχολικό βιβλίο για ΤΕΕ/ΕΠΑΛ στο μάθημα «ΔΙΚΤΥΑ Η/Υ ΙΙ», ΟΕΣΒ

Έντυπη ξενόγλωσση βιβλιογραφία

- J. Epstein, Architecture and concepts of the ARGuE guard, In Proceedings of the Fifteenth Annual Computer Security Applications Conference (ACSAC), Scotsdale, Dec. 1999.
- *Building Internet Firewalls, Second Edition* by Elizabeth D. Zwicky, Simon Cooper; D. Brent Chapman, O'Reilly Media, Inc.
- CERT, Advisory CA-2001-19: "Code red" worm exploiting buffer overfl ow in IIS Indexing Service DLL, http://www.cert.org/advisories/CA-2001-19.html, July 2001.
- CERT, Advisory CA-2003-04: MS-SQL server worm, http://www.cert.org/advisories/CA-2003-04.html, Jan. 2003.

- Designing Network Security Second Edition by Merike Kaeo, Cisco Press.
- *Firewall Fundamentals* by Wes Noonan, Ido Dubrawsky, Cisco Press.
- M. Blaze, J. Feigenbaum, J. Ioannidis, and A. Ker-omytis, The role of trust management in distributed systems security, in Secure Internet Programming, LNCS 1603, Springer-Verlag, New York, 1999, pp. 185–210.
- M. Dahlin, Serverless Network File Systems, PhD thesis, University of California, Berkeley, Dec. 1995.
- Network Security Architectures by Sean Convery, Cisco Press.
- Rattle, Using process infection to bypass windows software fi rewalls. Phrack, 13(62), July 2004.
- S. Ioannidis, A. D. Keromytis, S. M. Bellovin, and J. M. Smith, Implementing a distributed fi rewall, in Proceedings of Computer and Communications Secu-rity (CCS) 2000, Nov. 2000, Athens, pp. 190–199.
- S. M. Bellovin, Distributed fi rewalls, login: magazine, special issue on security, Nov. 1999, pp. 37–39.
- T. A. Limoncelli, Tricks you can do if your fi rewall is a bridge, in Proceedings of the fi rst USENIX Conference on Network Administration, Santa Clara, CA, Apr. 1999.
- V. Prevelakis and A. D. Keromytis, Drop-in security for distributed and portable computing elements. Inter-net Research: Electronic Networking, Applications and Policy, 13(2), 2003, pp. 107–115.
- W. R. Cheswick and S. M. Bellovin, Firewalls and Internet Security: Repelling the Wily Hacker, Addison-Wesley, Reading, MA, 1994.
- Y. Bartal, A. Mayer, K. Nissim, and A. Wool, Firmato: A novel firewall management toolkit, in Pro-ceedings of the 1999 IEEE Symposium on Security and Privacy, May 1999, pp. 17–31.

Διαδικτυακές πηγές

- msdn.microsoft.com

- unipi.gr
- www.cisco.com
- http://www.giac.org/paper/gsec/566/connecting-home-lan-internet-securely/101343
- http://osarena.net/logismiko/applications/angry-ip-scanner-grigori-ke-efkoli-sarosi-tou-diktiou-sas.html