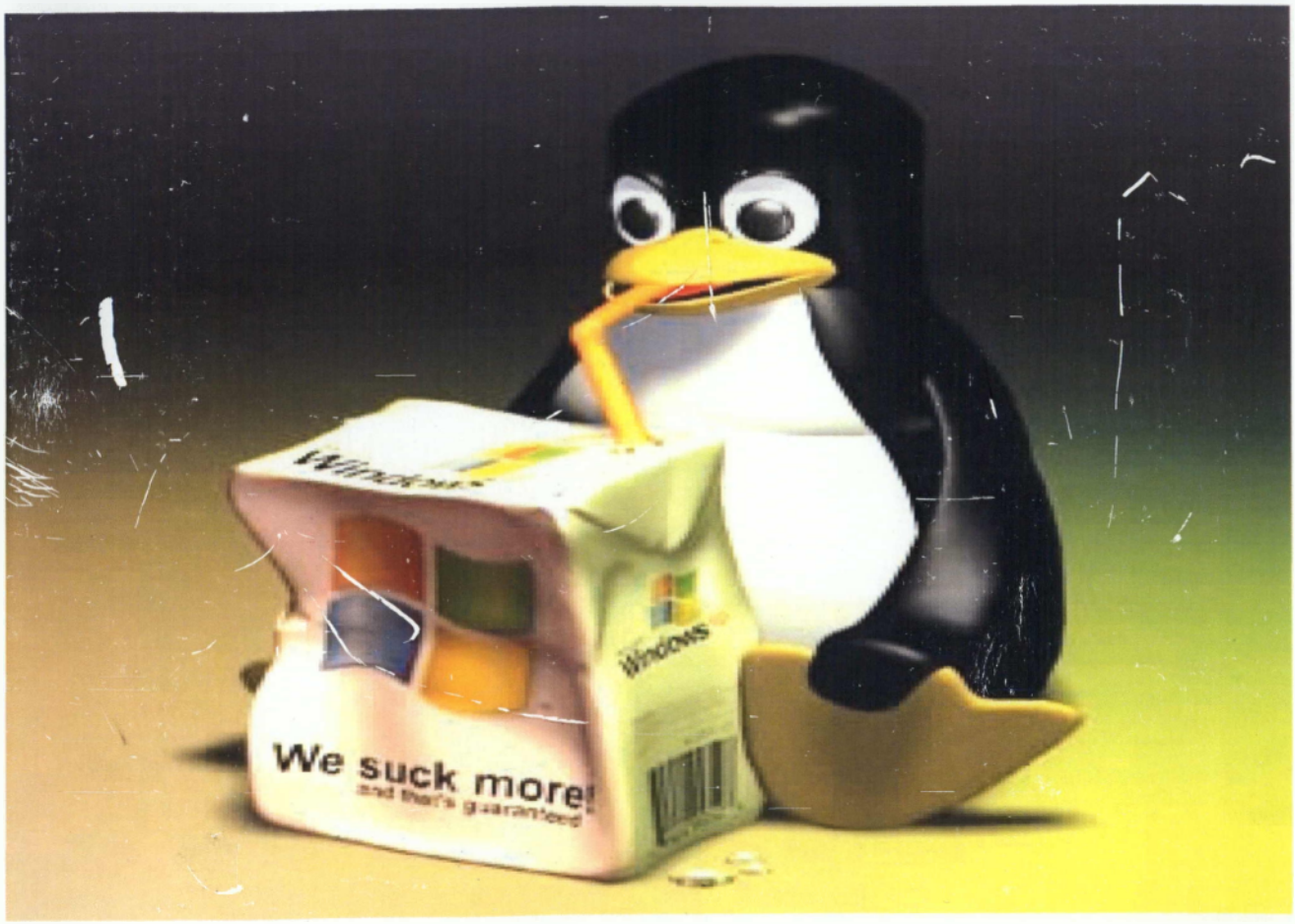
Α.Τ.Ε.Ι. ΚΑΛΑΜΑΤΑΣ

ΤΜΗΜΑ ΤΕΧΝΟΛΟΓΙΑΣ ΠΛΗΡΟΦΟΡΙΚΗΣ & ΤΗΛΕΠΙΚΟΙΚΩΝΙΩΝ



ΑΣΦΑΛΕΙΑ ΣΤΟ ΛΕΙΤΟΥΡΓΙΚΟ ΣΥΣΤΗΜΑ LINUX

ΦΟΙΤΗΤΗΣ: ΚΙΚΙΜΕΝΗΣ ΣΙΜΩΝ

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ: ΜΑΚΡΟΔΗΜΗΤΡΗΣ ΓΕΩΡΓΙΟΣ

- 2011 -

Α.Τ.Ε.Ι. ΚΑΛΑΜΑΤΑΣ

ΤΜΗΜΑ ΤΕΧΝΟΛΟΓΙΑΣ ΠΛΗΡΟΦΟΡΙΚΗΣ & ΤΗΛΕΠΙΚΟΙΚΩΝΙΩΝ

ΑΣΦΑΛΕΙΑ ΣΤΟ ΛΕΙΤΟΥΡΓΙΚΟ ΣΥΣΤΗΜΑ LINUX

ΦΟΙΤΗΤΗΣ: ΚΙΚΙΜΕΝΗΣ ΣΙΜΩΝ /200063

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ: ΜΑΚΡΟΔΗΜΗΤΡΗΣ ΓΕΩΡΓΙΟΣ

Περιεχόμενα

ΚΕΦ.0 ΕΙΣΑΓΩΓΗ

ΚΕΦ.1 Περί Firewall και Proxy διακομιστών

ΚΕΦ.2 Σχεδιασμός του Firewall

ΚΕΦ.3 Απειλές και Αρχές της Άμυνας Δικτύων

ΚΕΦ.4 Windows VS Linux

Εισαγωγή

Η διπλωματική αυτή εργασία πραγματεύεται θέματα δικτυακής ασφάλειας υπολογιστών και το πώς κάτι τέτοιο μπορεί να επιτευχθεί με τη χρήση ενός κατεξοχήν δικτυακού λειτουργικού συστήματος, του Linux. Μιλώντας τόσο σε θεωρητικό επίπεδο, αναλύοντας τις δυνατότητες και τις εφαρμογές του, αλλά και σε πρακτικό με οδηγίες και συμβουλές για την κατασκευή ενός Firewall και Proxy Server για την βελτίωση της ασφάλειας της ασφάλειας δικτύων.

Ένας firewall server αποτελείται από δυο ή περισσότερους προσαρμογείς δικτύου (κάρτες Ethernet) οι οποίοι συνδέουν διαφορετικά δίκτυα μεταξύ τους. Μπορεί να φιλτράρει IP πακέτα με βάση τις τιμές του περιεχομένου της επικεφαλίδας του πακέτου, όπως η διεύθυνση αφετηρίας και προορισμού. Επίσης μπορεί να παραμετροποιηθεί ώστε να επιτρέπει πρόσβαση μόνο σε συγκεκριμένα πακέτα, να επιτρέπει την πραγματοποίηση συνδέσεων μόνο από συγκεκριμένους υπολογιστές και να μπλοκάρει την πρόσβαση μη εξουσιοδοτημένων υπολογιστών.

Ένας Proxy server είναι μια εφαρμογή η οποία τρέχει στο firewall και αναμεταδίδει την κίνηση μεταξύ αυτού και του προορισμού. Έτσι αντί να επιτρέψουμε σε δύο υπολογιστές να επικοινωνήσουν μεταξύ τους κατευθείαν, τους αναγκάζουμε να επικοινωνήσουν μέσω ενός άλλου υπολογιστή ο οποίος λέγεται εξυπηρετητής (Proxy). Πιο εξειδικευμένα εξυπηρετητές μπορούν να χειριστούν πιο πολύπλοκες διαδικασίες οι οποίες είναι πέρα από τις δυνατότητες των firewalls. Μπορούν να καταλάβουν την εφαρμογή και το περιεχόμενό της ώστε να εκτελέσουν διεργασίες όπως το φιλτράρισμα mail ανάλογα με την προέλευσή του ή μπορεί να έχουν ακόμα υψηλότερου επιπέδου φιλτράρισμα ώστε να ψάχνουν για πορνογραφικό υλικό ή ακόμα και για συντακτικά και ορθογραφικά λάθη. Το κλειδί για αυτό είναι ο server να μπορεί να καταλάβει το περιεχόμενο που μεταφέρεται ακόμα και αν χρειαστεί να το αναγνωρίσει αναλύοντας το πρωτόκολλο.

Μερικά οφέλη από τα οποία μπορεί να προσφέρει η πραγματοποίηση ενός τέτοιου συστήματος, πέρα από την προστασία των host του εσωτερικού δικτύου, είναι η χρησιμοποίηση λιγότερου bandwidth σύνδεσης internet, η μείωση του χρόνου φόρτωσης των σελίδων, η συλλογή στατιστικών για την κίνηση του δικτύου, η παρεμπόδιση χρηστών

από το να επισκέπτονται συγκεκριμένα site (π.χ. πορνογραφικού υλικού κτλ), η βεβαίωση ότι μόνο εξουσιοδοτημένοι χρήστες μπορούν να σερφάρουν στο internet, και η βελτίωση της ασφάλειας των χρηστών φιλτράροντας ευαίσθητες πληροφορίες.

ΚΕΦΑΛΑΙΟ 1°

Περί Firewall και Proxy Διακομιστών

1.1Γιατί χρειαζόμαστε τα firewall;

Ο ρόλος των firewall είναι η προστασία των δικτύων. Πιο συγκεκριμένα επειδή ο όρος δίκτυο δεν είναι απόλυτα σαφής μπορεί να μην είναι και κατανοητό και για ποιο λόγο το δίκτυο χρειάζεται προστασία.

Από πλευράς επιχειρήσεων τα πολύτιμα στοιχεία ενός δικτύου είναι:

- Η εμπιστευτικότητα των δεδομένων που μεταφέρονται
- Η αξιοπιστία μεταφοράς δεδομένων
- Η διαθεσιμότητα του δικτύου

Εμπιστευτικότητα δεδομένων

Μερικά δεδομένα είναι πολύτιμα γιατί δεν είναι ευρέως γνωστά. Για παράδειγμα θα ήταν πολύτιμο αν γνωρίζαμε τις αυριανές τιμές του χρηματιστηρίου. Αν όμως είχαν όλοι πρόσβαση σε αυτές τις πληροφορίες τότε πιθανόν να ήταν άνευ αξίας. Πολλές εταιρίες κατέχουν εμπιστευτικά δεδομένα αποθηκευμένα σε αρχεία υπολογιστών. Αυτοί οι υπολογιστές πρέπει να προστατευτούν από επιθέσεις, μη εξουσιοδοτημένη χρήση και από άλλα γεγονότα τα οποία μπορούν να οδηγήσουν σε διαρροές δεδομένων.

Αξιοπιστία δεδομένων

Η αξιοπιστία των δεδομένων είναι ο βαθμός στον οποίο κάποιος μπορεί να είναι σίγουρος ότι τα δεδομένα θα είναι πλήρη και ακριβή. Η αξιοπιστία των δεδομένων είναι σημαντική γιατί η αξία τους μειώνεται η χάνεται αν τα περιεχόμενά τους μεταβληθούν ή είναι ανακριβή.

Διαθεσιμότητα του δικτύου

Μερικά δίκτυα υποστηρίζουν επιχειρήσεις ή παρέχουν υπηρεσίες, έτσι μία δυσλειτουργία τους μπορεί να είναι πολλές φορές καταστροφική. Για παράδειγμα το

«Ebay» έχει γίνει πολλές φορές θύμα επιθέσεων λόγω του ότι παρέχει On-Line συναλλαγές. Η αναστολή της λειτουργίας του για κάποιο διάστημα μπορεί να αποφέρει σημαντικές απώλειες κερδών.

1.2 Πως απειλούνται τα δίκτυα

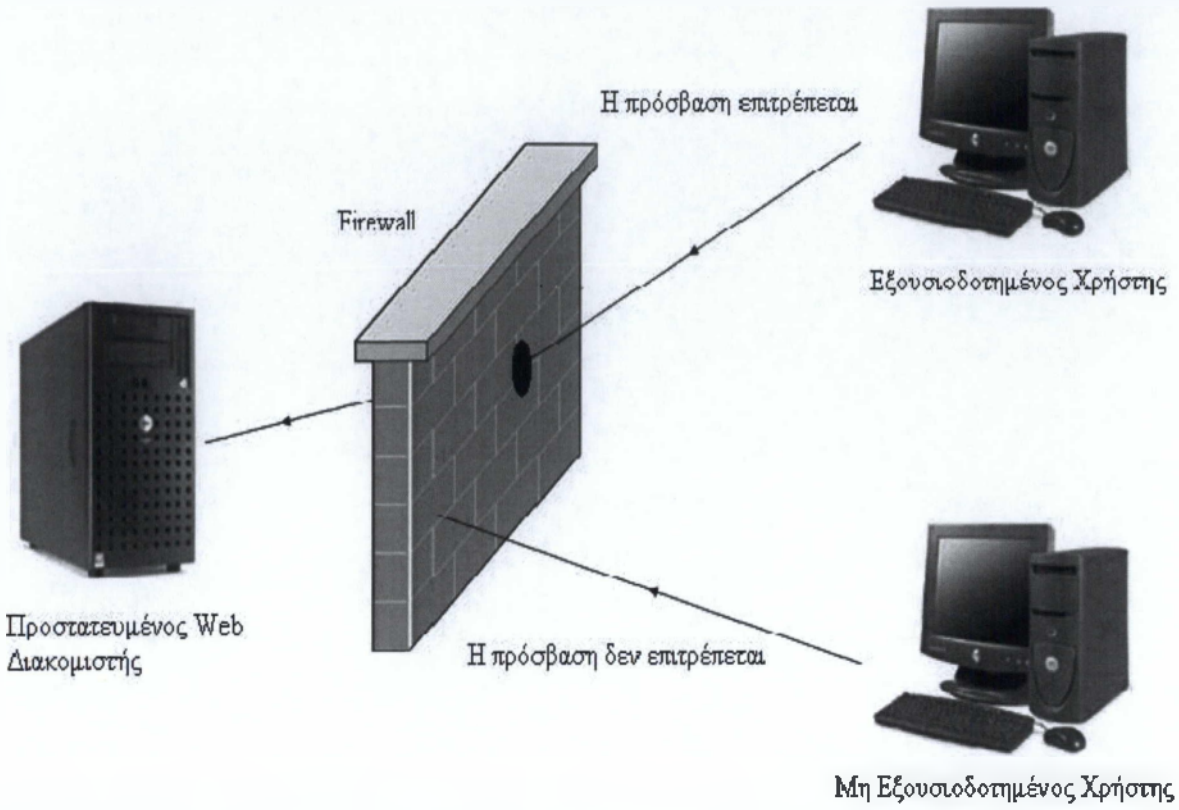
Πριν την εξάπλωση του internet οι οργανισμοί και οι επιχειρήσεις διατηρούσαν ιδιωτικά δίκτυα υπολογιστών τα οποία δεν παρείχαν απομακρυσμένη πρόσβαση. Έτσι η επίθεση σε έναν υπολογιστή ή γενικότερα σε ένα δίκτυο απαιτούσε φυσική επαφή με το στόχο. Ο επιτιθέμενος έπρεπε να είχε εξουσιοδοτημένη πρόσβαση ή με κάποιον τρόπο να εισβάλει παράνομα στην εταιρία με σκοπό την πρόσβαση σε κάποιο τερματικό. Έτσι οι περισσότερες επιθέσεις γίνονταν από υπαλλήλους. Με τη χρήση των modem ανοίχτηκε μία νέα οδός επιθέσεων και αρκούσε μία τηλεφωνική κλήση από απομακρυσμένη περιοχή αντί για την παραβίαση φυσικών μέτρων ασφαλείας.

Στις μέρες μας όλες οι επιχειρήσεις έχουν δημόσια δίκτυα τα οποία περιέχουν και δεδομένα τα οποία χρειάζονται προστασία. Ένας επιτιθέμενος ο οποίος μπορεί να αποκτήσει παραπάνω προνόμια πρόσβασης μπορεί να προκαλέσει από απώλεια δεδομένων μέχρι κατάρρευση του δικτύου.

1.3 Τι κάνει το firewall

Το firewall ενός αυτοκινήτου είναι σχεδιασμένο για να εμποδίζει την εξάπλωση της φωτιάς από το χώρο της μηχανής στην καμπίνα των επιβατών. Σκοπός του είναι ο περιορισμός. Ένα firewall δικτύου είναι επίσης μία συσκευή περιορισμού. Ένα firewall λειτουργεί με το να διαιρεί ένα δίκτυο σε πολλαπλές ζώνες και να περιορίζει τη λειτουργία σε αυτές. Αυτό γίνεται με το να εμποδίζει τη μη εξουσιοδοτημένη κίνηση να εισέρχεται ή να εξέρχεται. Αν ρυθμιστεί σωστά μπορεί να εμποδίσει μια επίθεση να φτάσει στον προορισμό της.

Το παρακάτω σχήμα δείχνει ένα απλό τυπικό firewall το οποίο επιτρέπει μόνο σε συγκεκριμένους χρήστες να προσπελάσουν τον Web Server. Ένας επιτιθέμενος για να αποκτήσει πρόσβαση στον Web Server πρέπει πρώτα να νικήσει το firewall.



Ένα firewall κάνει περισσότερα από το να μπλοκάρει απλά τη μη εξουσιοδοτημένη τρόσβαση. Το firewall έχει δύο πρωταρχικούς ρόλους: παρεμπόδιση και ανίχνευση. Η τολιτική ασφαλείας καθορίζει τις λειτουργίες που ένας χρήστης είναι εξουσιοδοτημένος να :κτελεί. Το firewall εμποδίζει τις επιθέσεις με το να φιλτράρει την κίνηση, βασιζόμενο στην τολιτική ασφαλείας και επίσης ανιχνεύει επιθέσεις. Η ανίχνευση αυτή γίνεται με το να :ρατάει αρχείο (log) για τις προσπάθειες και της πραγματοποιήσεις συνδέσεων με ιηχανήματα του δικτύου και να ενημερώνει τους διαχειριστές για ύποπτες ενέργειες.

Προφανώς το firewall δεν μπορεί να εμποδίσει μια επίθεση την οποία απέτυχε να ντοπίσει. Άρα η ανίχνευση προηγείται της παρεμπόδισης.

Ένα firewall μπορεί να φιλτράρει την κίνηση με διάφορους τρόπους. Οι πιο κοινοί είναι μέσω των:

- IP διευθύνσεων
- Υπηρεσιών

Η κίνηση του δικτύου σηματοδοτείται από τις διευθύνσεις IP, οι οποίες δείχνουν την αφετηρία και τον προορισμό του host. Η κίνηση η οποία απαιτεί πρόσβαση σε μια

υπηρεσία καθορίζεται από τον αριθμό του port το οποίο συνδυαζόμενο με την διεύθυνση IP καθορίζει την υπηρεσία.

Επίσης ένα firewall πρέπει να μπορεί να προστατεύσει τον κεντρικό υπολογιστή του δικτύου από επιθέσεις οι οποίες προέρχονται και από τους υπολογιστές του τοπικού δικτύου. Κάτι τέτοιο μπορεί να μοιάζει ασήμαντο αλλά φανταστείτε αν ο επιτιθέμενος αποκτώντας πρόσβαση, χρησιμοποιήσει αυτόν σαν μεσάζοντα της επιθέσεώς του. Αυτό σημαίνει ότι ένα firewall πρέπει να ελέγχει την εισερχόμενη και την εξερχόμενη κίνηση.

1.4 Τύποι firewall

Οι μεγάλες οργανώσεις χρησιμοποιούν χαρακτηριστικά τα firewalls για να χωρίσουν τι πηγαίνει μέσα («πίσω από» το firewall) από τον έξω κόσμο. Τα firewalls μπορούν να αντιμετωπίσουν τους hackers και να φιλτράρουν ένα μεγάλο μέρος της εκούσιας διαφήμισης, ή spam, που μπορεί να πλημμυρίζει τους χρήστες ηλεκτρονικού ταχυδρομείου πίσω από το firewall, καθώς επίσης και εντοπίζοντας και αποτρέποντας τους ιούς, τα worms, και τα Trojan horses από το να περάσουν.

Τα firewalls και άλλα λογισμικά μπορούν επίσης να σταματήσουν τους χρήστες μέσα στο firewall από την πρόσβαση σε ακατάλληλους ιστοχώρους και ομάδων πληροφόρησης έξω από το firewall. Ένα firewall, που συνδυάζεται με ένα VPN, μπορεί να παρέχει στις ασφαλείς, κρυπτογραφημένες επικοινωνίες με τον έξω κόσμο του firewall.

Σε γενικές γραμμές υπάρχουν τρεις τύποι firewall:

Προσωπικά firewall

Προστατεύουν τον υπολογιστή ενός μικρού δικτύου, δηλαδή ενός δικτύου με σύνδεση DSL ή καλωδιακών modem. Σε αυτήν την περίπτωση δεν χρησιμοποιούνται διακομιστές firewall αλλά κάποιο απλό λογισμικό του εμπορίου με εύκολη χρήση και συντήρηση γιατί η χρήση ενός διακομιστή firewall απαιτεί προχωρημένες γνώσεις θεμάτων ασφαλείας.

Τμηματικά firewall

Σε γενικές γραμμές προστατεύουν περισσότερους υπολογιστές από ότι έναπροσωπικό firewall. Οι υπολογιστές οι οποίοι προστατεύονται είναι πιθανό να παρέχουν περισσότερες και πιο εξελιγμένες υπηρεσίες και επιπλέον να μπορούν να χειριστούν μεγαλύτερο όγκο

πληροφοριών. Τα τμηματικά firewall είναι συνδυασμοί πολλών firewall με σκοπό να παρέχουν αυξημένες υπηρεσίες ασφαλείας.

Επιχειρησιακά firewall

Αποτελούνται από πολλά τμηματικά firewall τα οποία φιλτράρουν και κρατάνε αρχείο της εισερχόμενης και εξερχόμενης κίνησης (log). Η διαφορά τους είναι ότι χρειάζονται περισσότερη γνώση και συντήρηση για τη σωστή λειτουργία τους. Επειδή διαχειρίζονται μεγάλο όγκο πληροφοριών απαιτούν αυτοματοποιημένες διαδικασίες για την παρακολούθηση και την ανάλυση των αρχείων καταγραφής κίνησης.

1.5 Πλεονεκτήματα-Μειονεκτήματα των firewall

Τα πλεονεκτήματα των firewall είναι τα έξης:

- Ένα συναίσθημα αυξημένης ασφάλειας ότι ο υπολογιστής και το περιεχόμενό σας προστατεύεται.
- Σχετικά φθηνό ή δωρεάν για προσωπική χρήση.
- Νέες κυκλοφορίες γίνονται όλο και πιο φιλικές προς το χρήστη.
- Μπορείτε να παρακολουθείτε τις εισερχόμενες και εξερχόμενες ειδοποιήσεις ασφαλείας και η εταιρεία firewall θα τις καταγράψει και έτσι να εντοπίσουμε μια απόπειρα εισβολής ανάλογα με τη βαρύτητα.
- Ορισμένα τείχη προστασίας, αλλά όχι όλα μπορεί να ανιχνεύσουν ιούς, worms, δούρειους ίππους, ή συλλέκτες δεδομένων.

Τα firewall παρουσιάζουν διάφορα μειονεκτήματα. Στις περισσότερες περιπτώσεις τα οφέλη υπερέχουν των μειονεκτημάτων, παρόλα αυτά πρέπει να γνωρίζουμε τα μειονεκτήματα με σκοπό να τα ελαχιστοποιήσουμε ή να τα υπερπηδήσουμε.

Τα μειονεκτήματα πηγάζουν από το γεγονός ότι το firewall μετατρέπεται σε ένα στενό πέρασμα επηρεάζοντας το δίκτυο με τους τρεις παρακάτω τρόπους:

- Αξιοπιστία
- Απόδοση
- Ευκαμψία

Η αποτυχία λειτουργίας ενός firewall μειώνει την αξιοπιστία του δικτύου. Αυτό αποφεύγεται με τη χρήση πολλαπλών firewall ρυθμιζόμενα έτσι ώστε η αποτυχία λειτουργίας του ενός να ενεργοποιήσει το άλλο διαπερνόντας το οποίο τελικά η κίνηση να φτάσει στον προορισμό της. Με παρόμοιο τρόπο μπορεί να μειωθεί και η απόδοση του δικτύου.

Επειδή όλη η κίνηση πρέπει να περάσει μέσα από το firewall η απόδοση του δικτύου επηρεάζεται από την ικανότητα χειρισμού του όγκου πληροφοριών από το firewall και επιπλέον για να χειριστεί ένα νέο τύπο δεδομένων το firewall πρέπει να ρυθμιστεί ξανά.

1.6 Τεχνολογίες firewall

Οι τεχνολογίες οι οποίες χρησιμοποιούνται κατά την δόμηση των firewall περιλαμβάνουν την προώθηση πακέτων και το φιλτράρισμά τους, τους εξυπηρετητές εφαρμογών και τέλος πιο σύγχρονες τεχνολογίες όπως τα λεπτομερούς επιθεώρησης και τα υβριδικά firewall. Επιπλέον υπάρχουν κάποιες άλλες σημαντικές τεχνολογίες οι οποίες χρησιμοποιούνται σε συνδυασμό με τα firewall, όπως η μετάφραση διευθύνσεων δικτύου (NAT) και η χρήση εικονικών ιδιωτικών δικτύων (VPNs).

Προώθηση Πακέτων

Ο όρος προώθηση (δρομολόγηση) αναφέρεται σε διαδικασίες μετακίνησης πακέτων από ένα δίκτυο σε ένα άλλο. Αυτό συχνά γίνεται από μονάδες που ονομάζονται δρομολογητές. Στον κόσμο του Linux είναι πολύ πιθανό να δούμε έναν υπολογιστή να εκτελεί χρέη δρομολογητή. Ένα firewall μπορεί να πραγματοποιηθεί με το συνδυασμό τεχνολογιών δρομολόγησης και άλλων λειτουργιών.

Ένας δρομολογητής αποτελείται από δυο ή περισσότερους προσαρμογείς δικτύου οι οποίοι συνδέουν διαφορετικά δίκτυα μεταξύ τους. Κάθε δρομολογητής περιλαμβάνει ένα πακέτο δρομολόγησης με ένα σύνολο κανόνων το οποίο καθορίζει ποια πακέτα θα προωθηθούν και που.

Το πότε και που θα προωθηθούν τα πακέτα καθορίζεται από:

- Τον προσαρμογέα δικτύου στον οποίο φτάνει το πακέτο
- Τη διεύθυνση αφετηρίας του πακέτου

- Τη διεύθυνση προορισμού του πακέτου

Φιλτράρισμα πακέτων

Θεωρήστε το firewall σαν μία συσκευή διέλευσης η οποία διαχειρίζεται την κυκλοφορία. Τα firewall υλικού αποτελούνται από δρομολογητές ή από υπολογιστές οι οποίοι φέρουν το κατάλληλο λογισμικό. Οι δρομολογητές λειτουργούν σε επίπεδο δικτύου και μπορούν να φιλτράρουν IP πακέτα βασιζόμενα στις τιμές του περιεχομένου της επικεφαλίδας του πακέτου όπως η διεύθυνση αφετηρίας και προορισμού.

Οι δρομολογητές μπορούν να παραμετροποιηθούν ώστε να επιτρέπουν πρόσβαση μόνο σε συγκεκριμένα πακέτα, να επιτρέπουν την πραγματοποίηση συνδέσεων μόνο από συγκεκριμένους υπολογιστές και να μπλοκάρουν την πρόσβαση των μη εξουσιοδοτημένων μηχανημάτων. Αυτή η διαδικασία συχνά αναφέρεται σαν φιλτράρισμα πακέτων (Packet Filtering).

Εξυπηρετητές εφαρμογών

Ένα firewall στρώματος εφαρμογών είναι ένας proxy διακομιστής ο οποίος παρέχει ένα άλλο στρώμα ασφαλείας το οποίο δεν παρέχουν τα firewall φιλτραρίσματος πακέτων. Βασικά ένας εξυπηρετητής εφαρμογών είναι μια εφαρμογή η οποία τρέχει στο firewall και αναμεταδίδει την κίνηση μεταξύ αυτού και του προορισμού. Το πλεονέκτημα εδώ είναι ότι η κίνηση ανάμεσα στις δύο πλευρές μπορεί να ελεγχθεί μέσω τρίτων εφαρμογών.

Λεπτομερούς επιθεώρησης

Αυτά είναι τα τρίτης γενιάς firewall τα οποία σχετίζονται με τη μέθοδο του φιλτραρίσματος πακέτων αλλά επεκτείνουν τις λειτουργίες του firewall με το να συνεχίζουν να επιθεωρούν τα πακέτα τη στιγμή που περνάνε μέσα από το firewall.

Υβριδικά

Είναι τα τέταρτης γενιάς firewall τα οποία είναι συνδυασμός όλων των προηγουμένων και δίνουν σε όλους τους χρήστες περισσότερο έλεγχο.

1.7 Άλλες σημαντικές τεχνολογίες

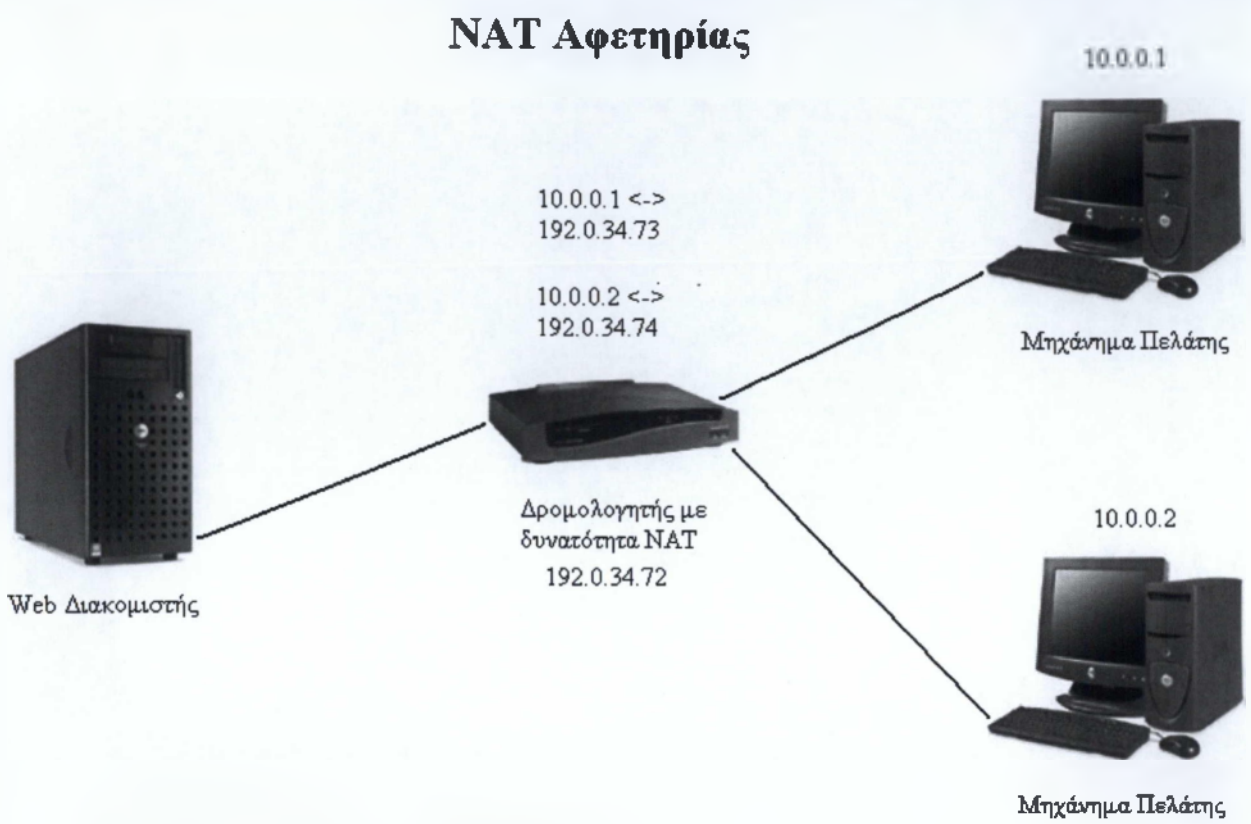
Μετάφραση διευθύνσεων δικτύου (NAT)

Η μετάφραση διευθύνσεων δικτύου σχεδιάστηκε για να επιτρέπει σε πολλαπλούς host να μοιράζονται μια IP διεύθυνση. Το NAT είναι μία απλή λειτουργία φιλτραρίσματος πακέτων η οποία πραγματοποιείται από δρομολογητές ή firewall κατά την οποία η διεύθυνση προορισμού ή αφετηρίας μεταβάλλεται.

Με χρήση DNAT (destination) μεταβάλλεται η διεύθυνση προορισμού ενώ με χρήση SNAT (source) μεταβάλλεται η διεύθυνση αφετηρίας. Με τη χρήση NAT επιτυγχάνεται η οικονομία διευθύνσεων IP. Για παράδειγμα, ο πελάτης καλώντας την ίδια IP διεύθυνση μπορεί να συνδεθεί μέσο του δρομολογητή με πολλούς διακομιστές ανάλογα με την υπηρεσία για την οποία έχει κάνει αίτηση.

Στο παρακάτω σχήμα παρατηρούμε ένα παράδειγμα NAT προορισμού. Το μηχάνημα πελάτης (client) δρομολογείται μέσω του δρομολογητή είτε στον mail διακομιστή, είτε στον web διακομιστή, ανάλογα με την αίτηση.

Στο παρακάτω σχήμα παρατηρούμε ένα παράδειγμα NAT αφετηρίας.



Ιδιωτικά εικονικά δίκτυα (VPNs)

Συχνά είναι σημαντική η υποστήριξη απομακρυσμένων συνδέσεων έτσι ώστε ένας υπάλληλος να μπορεί να προσπελάσει το δίκτυο μιας εταιρίας ακόμα και από το σπίτι. Χωρίς κάποια συγκεκριμένη λειτουργία που να το επιτρέπει, το firewall θα εμπόδιζε την πρόσβαση.

Ένας δημοφιλής τρόπος υποστήριξης αυτών των χρηστών είναι μέσω VPNs. Το VPN πραγματοποιεί τη σύνδεση, τη λεγόμενη tunnel, μεταξύ δυο δικτύων ή ανάμεσα σε ένα host και ένα δίκτυο. Το tunnel παρέχει εξειδικευμένη δρομολόγηση των δεδομένων. Τα VPN γενικά κρυπτογραφούν τα δεδομένα έτσι ώστε να ταξιδεύσουν ασφαλή μέσω ενδιάμεσων δικτύων.

Τύποι VPNs

Τα VPN χωρίζονται σε 3 κατηγορίες:

- Hardware VPN
- Firewall VPN
- Stand Alone εφαρμογές VPN

Το κάθε ένα από αυτά τα συστήματα έχει προτερήματα αλλά και μειονεκτήματα τα οποία θα αναλύσουμε παρακάτω με μεγαλύτερη λεπτομέρεια.

Hardware VPN Συστήματα

Ο μεγαλύτερος όγκος των Hardware VPN συστημάτων είναι στην πραγματικότητα δρομολογητές κρυπτογράφησης. Όλη η κρυπτογράφηση γίνεται μέσω υλικού, το οποίο είναι πιο γρήγορο από αυτή του λογισμικού. Αυτοί οι δρομολογητές είναι πολύ εύκολοι στη χρήση, στην εγκατάσταση, και παρέχουν αυξημένη ασφάλεια. Μερικά hardware VPN περιλαμβάνουν και λογισμικό πελάτη για απομακρυσμένη εγκατάσταση και έχουν ενσωματωμένα μερικά από τα χαρακτηριστικά ελέγχου πρόσβασης τα οποία περιλαμβάνονται σε firewall και άλλους εξοπλισμούς ασφαλείας.

Τα συστήματα αυτά παρουσιάζουν δύο κύρια προβλήματα. Πρώτον δεν παρουσιάζουν εύκολη παραμετροποίηση όπως αυτά του λογισμικού, και δεύτερον είναι εξαιρετικά ακριβά, πράγμα το οποίο τα κάνει απροσπέλαστα για ένα μέσο χρήστη και αναφέρονται κυρίως για μεγάλα εταιρικά δίκτυα.

Firewall VPN

Τα firewall VPN συστήματα αναφέρονται και σε εταιρική αλλά και σε προσωπική χρήση. Εκμεταλλεύονται τα προτερήματα ασφαλείας που προσφέρουν τα firewall περιλαμβάνοντας ελεγχόμενη πρόσβαση σε εσωτερικό δίκτυο, NAT και άλλα. Επιπλέον παρέχουν αυξημένο έλεγχο πρόσβασης καθώς και λειτουργίες εγγραφών (logging).

Σε αυτήν την εγκατάσταση υπάρχουν πολλά μειονεκτήματα. Ένα από αυτά είναι ότι το λειτουργικό που τρέχει το VPN σύστημα πρέπει να είναι όσο πιο ασφαλές γίνεται. Αν το λειτουργικό είναι μη ασφαλές το δίκτυο ή το VPN μπορούν να παραβιαστούν.

VPN λογισμικού

Τα VPN λογισμικού παρέχουν περισσότερες λειτουργίες, αλλά είναι πιο δύσκολο να εγκατασταθούν και να διαχειριστούν σε σύγκριση με τα VPN του υλικού. Τα περισσότερα VPN λογισμικού μπορούν να δρομολογούν την κίνηση βασιζόμενα στην διεύθυνση ή στο πρωτόκολλο. Η δρομολόγηση μόνο συγκεκριμένου τύπου κίνησης μας δίνει τη δυνατότητα να διαχειριστούμε τον όγκο της.

Τα VPN προσφέρουν πολλά πλεονεκτήματα σε σχέση με τα παλιά παραδοσιακά δίκτυα μισθωμένων γραμμών. Μερικά από αυτά είναι :

- Μικρότερο κόστος από αυτό των ιδιωτικών δικτύων : το ολικό κόστος ιδιοκτησίας μειώνεται μέσο του μικρότερου κόστους του εύρους ζώνης, backbone εξοπλισμού και των λειτουργικών αναγκών σύμφωνα με μελέτη της Infonetics (εταιρία διαχείρισης δικτύων και παροχής συμβουλευτικών υπηρεσιών)το κόστος LAN-to-LAN σύνδεσης μειώνεται κατά 20% με 40% σε σχέση με αυτό των δικτύων μισθωμένων γραμμών.
- Ενίσχυση της Οικονομίας του Internet : Τα VPN είναι αρχιτεκτονικές δικτύωσης περισσότερο ευέλικτες και διαβαθμισμένες από τα κλασικά WAN δίνοντας έτσι την ευχέρεια στις επιχειρήσεις να επεκτείνουν τη διασύνδεσή τους εύκολα και γρήγορα επιτυγχάνοντας σύνδεση και αποσύνδεση απομακρυσμένων γραφείων, σημείων σε όλη την υδρόγειο,
  τηλεργαζομένους, περιπλανώμενους κινούμενους χρήστες και εξωτερικούς συνεργάτες κατά τις επιταγές και τις ανάγκες της επιχείρησης.
- Μειωμένα έξοδα διαχείρισης συγκρινόμενα με αυτά της ιδιοκτησίας και λειτουργίας ιδιωτικού δικτύου.
- Απλοποίηση των δικτυακών τοπολογιών μειώνοντας έτσι το φόρτο διαχείρισης.

Τα μειονέκτημα των VPN λογισμικού είναι το ότι είναι δύσκολα στη διαχείριση τους, αλλά και το ότι απαιτούν αλλαγές στους πίνακες δρομολόγησης και στα προσχέδια διευθύνσεων δικτύου.

1.8 Αρχιτεκτονικές Firewall

Η αρχιτεκτονική ενός firewall περιλαμβάνει τις εγγενείς δυνατότητές του καθώς και διάφορους ειδικούς μηχανισμούς που ενσωματώνει προκειμένου να ενισχύσει την ασφάλεια που παρέχει . Ένα firewall πρέπει καταρχήν να είναι "χτισμένο" επάνω σε ασφαλές OS, και να επιτρέπει την έλευση μόνο σε συγκεκριμένους τύπους πακέτων. Η ειρωνεία είναι, ότι όσο περισσότερα πρωτόκολλα και υπηρεσίες υποστηρίζει ένα

firewall, τόσο μεγαλύτερη είναι η πιθανότητα παράκαμψής του από κάποιον επιτήδειο.

Τα περισσότερα firewalls υποστηρίζουν τις δημοφιλείς IP υπηρεσίες, συμπεριλαμβανομένων των FTP, TELNET, HTTP, και SMTP, αλλά διαφέρουν στον τρόπο με τον οποίο υλοποιούν αυτήν την υποστήριξη. Οι περισσότερες ασφαλείς προσεγγίσεις είναι αυτές των application gateways σε συνδυασμό με packet filtering δρομολογητές.

Όταν πιστοποιούν την ακεραιότητα των συστημάτων τους, ορισμένα firewalls ελέγχουν ψηφιακές υπογραφές ή checksums, είτε στον κώδικα των προγραμμάτων που λειτουργούν, είτε σε αρχεία συστήματος. Ο τρόπος με τον οποίο αντιδρούν τα firewalls σε μια διαπιστωμένη παραβίαση, διαφέρει δραματικά από firewall σε firewall. Για παράδειγμα, το firewall Eagle της Raptor "ρίχνει" (shut down) το σύστημα με το που διαπιστώσει μια παράβαση, ενώ το InterLock της ANS Inc. απλά καταγράφει τις λειτουργίες που βρίσκονται σε εξέλιξη, επιτρέποντας την κανονική λειτουργία του συστήματος.

Ο σχεδιασμός ενός firewall περιλαμβάνει δύο βασικές διεργασίες.

- Σχεδιασμός των κανόνων
- Καθορισμός της τοποθέτησης του firewall ή των firewalls

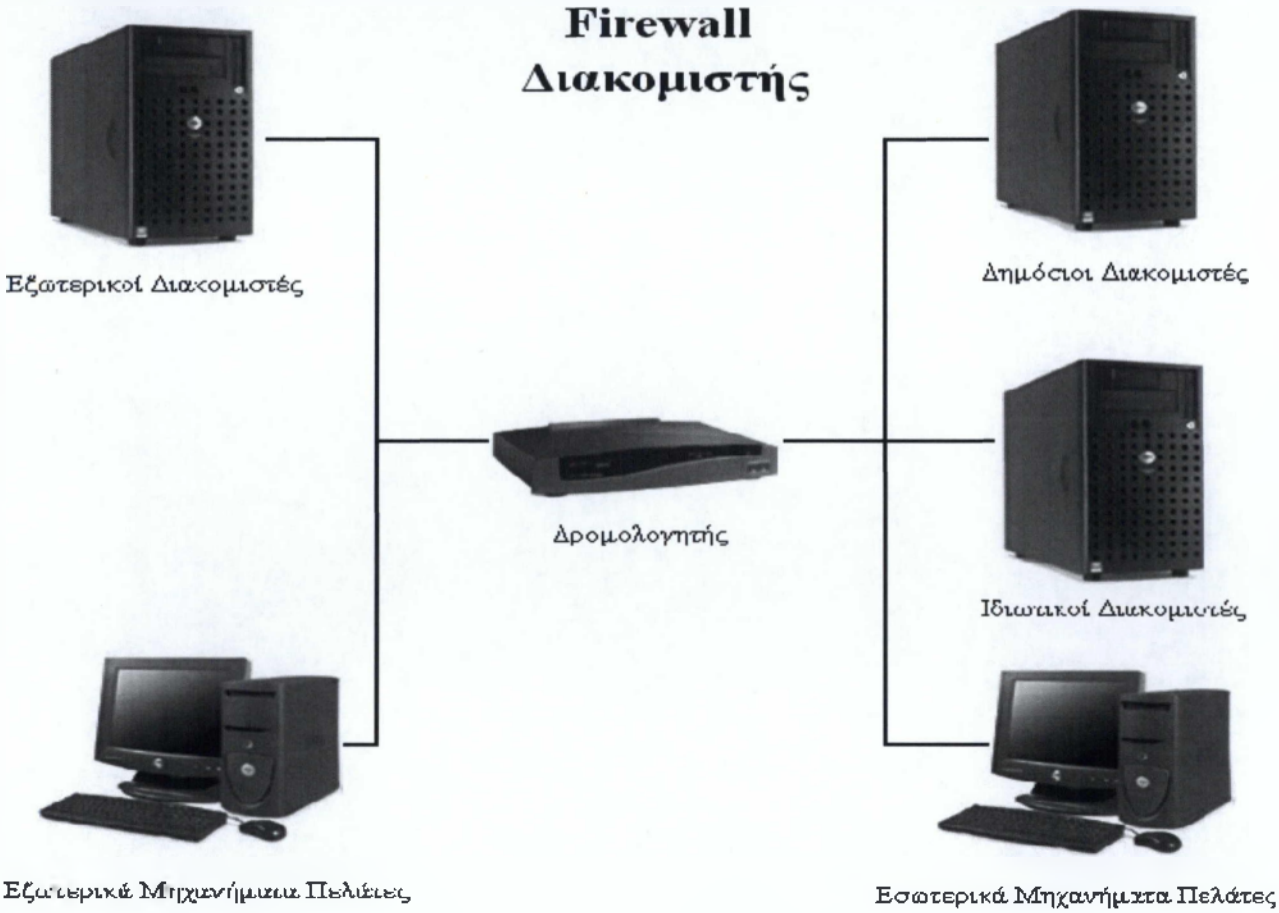
Η τοποθέτηση του firewall σε ένα δίκτυο ονομάζεται αρχιτεκτονική. Η αρχιτεκτονική του firewall είναι πολύ στενά συνδεδεμένη με την αρχιτεκτονική του δικτύου. Για αυτό και ο σχεδιασμός του firewall συνδέεται με το σχεδιασμό του δικτύου. Ο σχεδιασμός του firewall είναι μια διεργασία του σχεδιασμού δικτύων. Αυτός ο τομέας περιγράφει μερικές κοινές αρχιτεκτονικές firewall.

Router Firewall

Το παρακάτω σχήμα μας δείχνει την αρχιτεκτονική η οποία ονομάζεται router firewall. Στην πραγματικότητα αυτή η αρχιτεκτονική δεν περιλαμβάνει firewall. Αντί για αυτό ένας δρομολογητής αναλαμβάνει την επικοινωνία του εξωτερικού δικτύου με το εσωτερικό. Το ότι ο δρομολογητής παρέχει λειτουργίες προώθησης πακέτων είναι μια απλή μορφή φιλτραρίσματος πακέτων, η οποία μπορεί να χρησιμοποιηθεί για να προστατεύσει ένα δίκτυο. Το μέγεθος προστασίας είναι μικρό διότι η προώθηση πακέτων επιθεωρεί μόνο την διεύθυνση IP του πακέτου. Η άμυνα που παρέχει αυτή η αρχιτεκτονική δεν είναι επαρκής

επειδή έχει μόνο ένα επίπεδο ασφαλείας. Ο δρομολογητής δεν μπορεί να προγραμματιστεί για να μπλοκάρει ή να δέχεται πακέτα βασιζόμενος στο port.

Έτσι κάθε υπηρεσία που παρέχεται από το εσωτερικό δίκτυο είναι διαθέσιμη και ως προς τρίτους. Για αυτό δεν είναι δυνατό να παρέχουμε ιδιωτικές υπηρεσίες. Παρά τις αδυναμίες της αρχιτεκτονικής αυτής μπορούμε να την επιλέξουμε λόγο του ελάχιστου κόστους και της μέγιστης απόδοσης. Η προώθηση πακέτων αν και παρέχει χαμηλή ασφάλεια είναι η πιο γρήγορη από τις άλλες τεχνολογίες firewall.

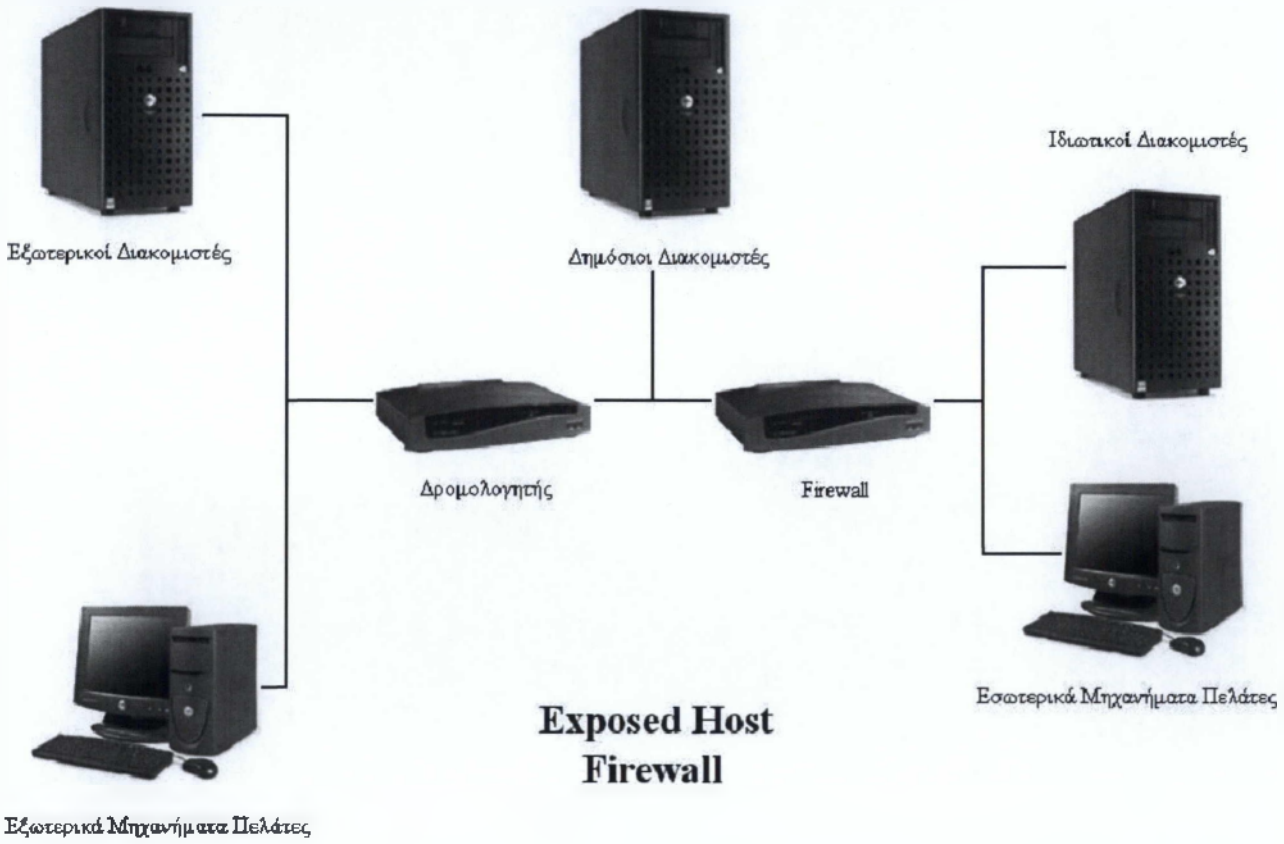


Single Host firewall

Αυτός ο τομέας εξηγεί τις αρχιτεκτονικές firewall οι οποίες πραγματοποιούνται μόνο με ένα firewall φιλτραρίσματος πακέτων ή proxy. Τα firewall φιλτραρίσματος πακέτων είναι πιο δημοφιλή από τα proxy γιατί μπορούν να στεγάσουν μεγαλύτερη ποικιλία πρωτοκόλλων. Εντούτοις, τα proxy firewall είναι ικανά να πραγματοποιήσουν πιο εξειδικευμένο φιλτράρισμα από αυτά των φιλτραρίσματος πακέτων. Έχοντας ένα φιλτραρίσμα πακέτων ή proxy firewall διαιρούμε το δίκτυο σε δυο υποδίκτυα:

- Το εσωτερικό ιδιωτικό δίκτυο
- Το περιμετρικό δίκτυο, γνωστό σαν DMZ (DeMilitarized Zone)

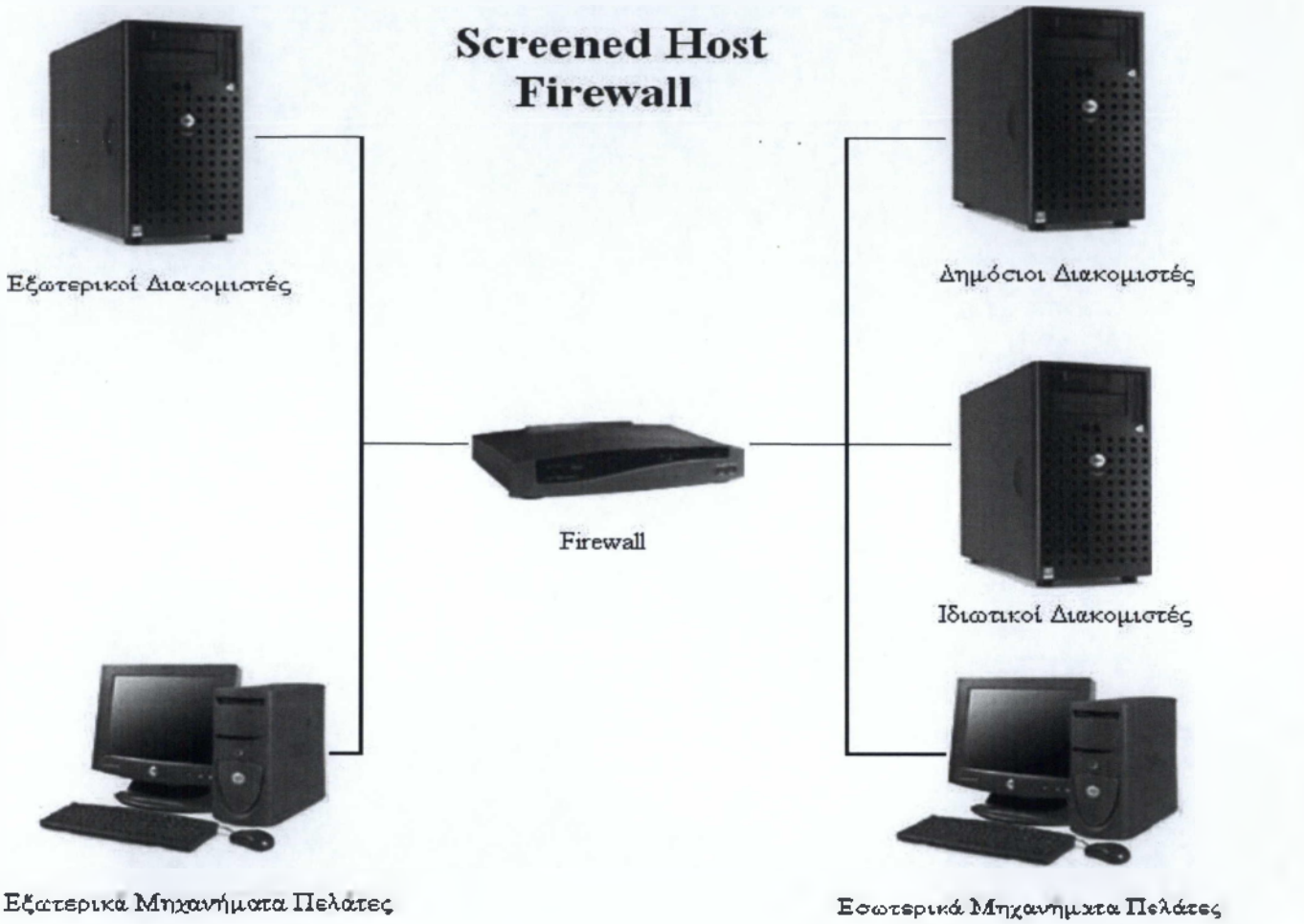
Το παρακάτω σχήμα απεικονίζει μια απλή αρχιτεκτονική single host firewall γνωστή σαν exposed host firewall.



Το firewall μπορεί όχι μόνο να προωθήσει πακέτα αλλά και να φιλτράρει από και προς το εσωτερικό δίκτυο. Οι κανόνες του firewall μπορεί να είναι πιο εξειδικευμένοι από ότι στα firewall δρομολόγησης. Αν συνδυαστούν με αυξημένη host-based ασφάλεια ένα exposed firewall παρέχει ικανοποιητική προστασία στο εσωτερικό δίκτυο. Το αδύνατο σημείο αυτής της αρχιτεκτονικής είναι οι εκτεθειμένοι hosts.

Αυτή η αρχιτεκτονική τοποθετεί τους δημόσιους διακομιστές σε μια ευαίσθητη θέση και έτσι είναι εκτεθειμένοι σε επιθέσεις από το εξωτερικό δημόσιο δίκτυο. Ένα single host firewall παρέχει μόνο δύο δίκτυα και έτσι οι δημόσιοι διακομιστές μπορεί να είναι μόνο σε μια από τις δύο πλευρές: στο περιμετρικό δίκτυο ή στο εσωτερικό ιδιωτικό δίκτυο. Η αρχιτεκτονική exposed host firewall τοποθετεί τους δημόσιους διακομιστές στο

περιμετρικό δίκτυο. Μια άλλη single host αρχιτεκτονική η οποία ονομάζεται screened host firewall τοποθετεί τους δημόσιους διακομιστές στο εσωτερικό ιδιωτικό δίκτυο.



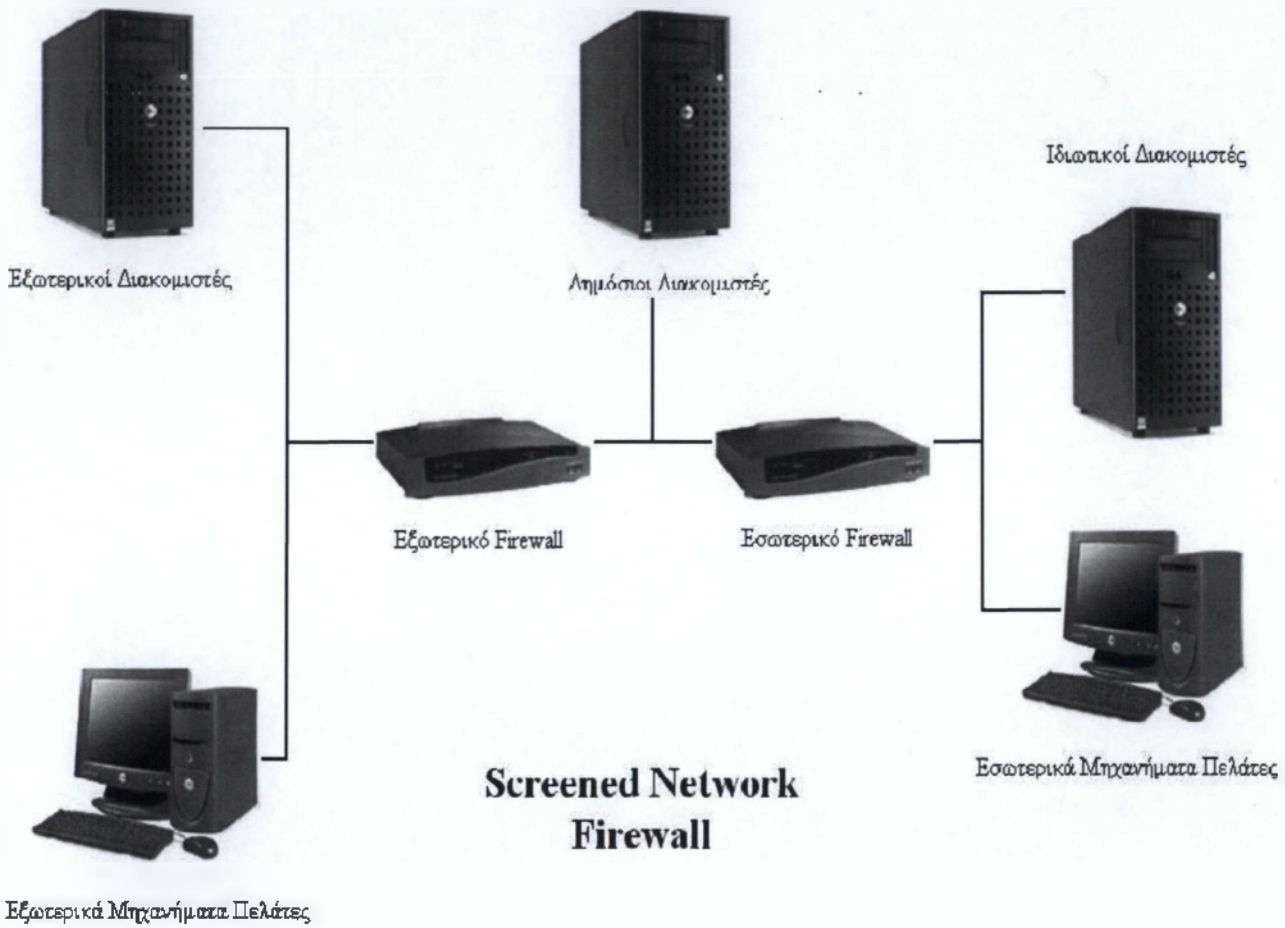
Η screened host αρχιτεκτονική μοιάζει με αυτή του δρομολογητή firewall. Η μόνη διαφορά είναι η αντικατάσταση του δρομολογητή προώθησης πακέτων με έναν φιλτραρίσματος πακέτων ή proxy firewall. Μεταφέροντας τους δημόσιους διακομιστές πίσω από το firewall έχουμε τη δυνατότητα να φιλτράρουμε την κίνηση που κατευθύνεται από και προς τους διακομιστές και έτσι μειώνουμε την ευαισθησία τους σε επιθέσεις. Αυτή η αρχιτεκτονική είναι γενικά πιο ασφαλείς γιατί αφήνουμε εκτεθειμένο μόνο το firewall το οποίο είναι λιγότερο ευπαθή σε επιθέσεις από ότι ο host.

Multi-Host firewall

Με τα multi-host firewall μπορούμε να υπερνικήσουμε τους περιορισμούς ασφαλείας των single-host firewall. Το επόμενο σχήμα μας δείχνει μια multi-host firewall αρχιτεκτονική γνωστή σαν screened network firewall.

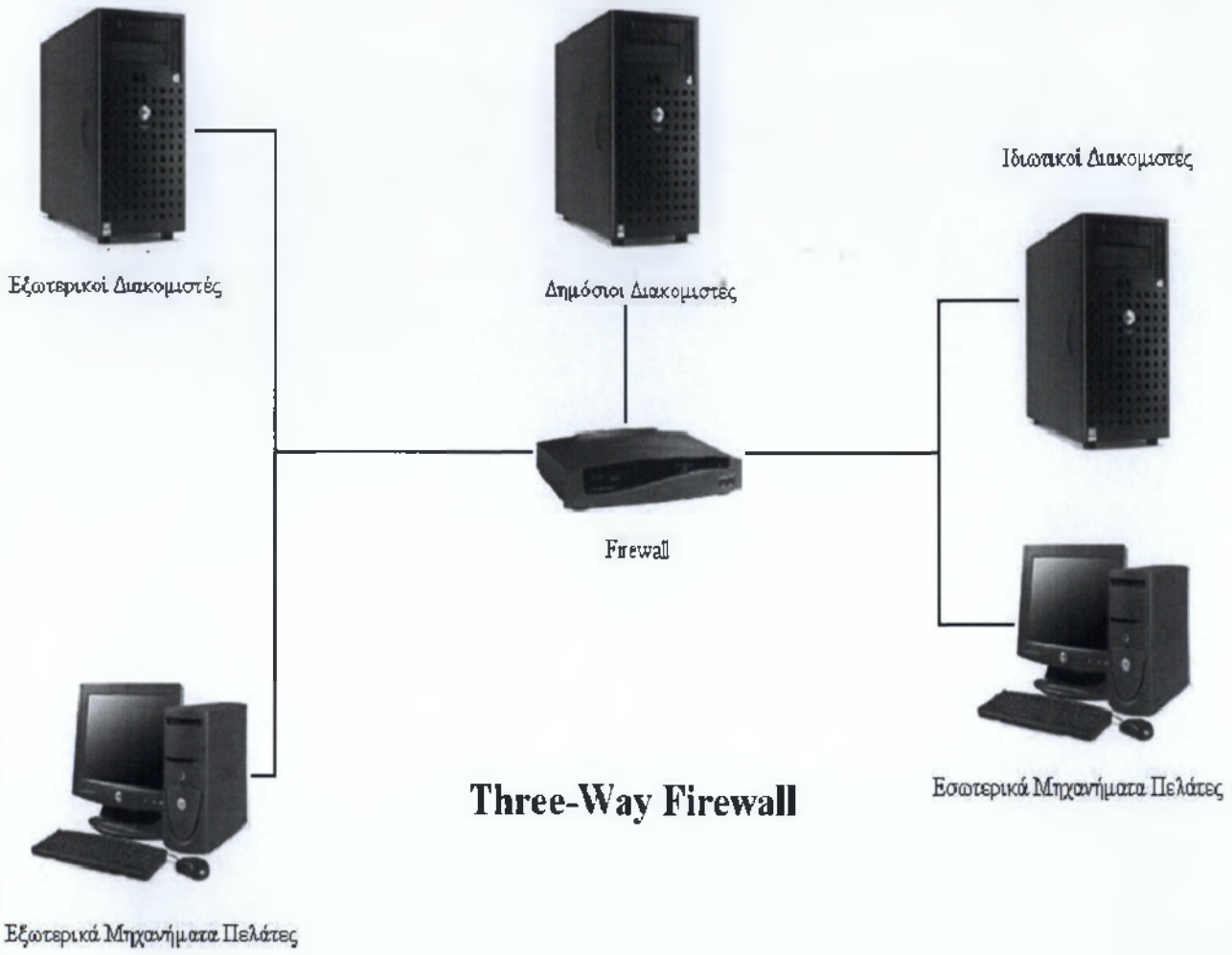
Αυτή η αρχιτεκτονική περιλαμβάνει δύο firewall:

- Ένα εξωτερικό firewall, γνωστό σαν gateway firewall
- Εσωτερικό firewall, γνωστό σαν choke firewall



Η διαφορά με τα exposed host-firewall είναι ότι αντικαθιστάμε τον δρομολογητή με ένα δεύτερο firewall. Το δεύτερο firewall μπορεί να προστατεύσει τους δημόσιους διακομιστές από επιθέσεις. Κάθε Host προστατεύεται από ένα firewall. Έτσι αυτή η αρχιτεκτονική παρέχει υψηλό βαθμό ασφαλείας. Μπορούμε να προσομοιώσουμε αυτήν την αρχιτεκτονική χρησιμοποιώντας ένα single, multi-homed host.

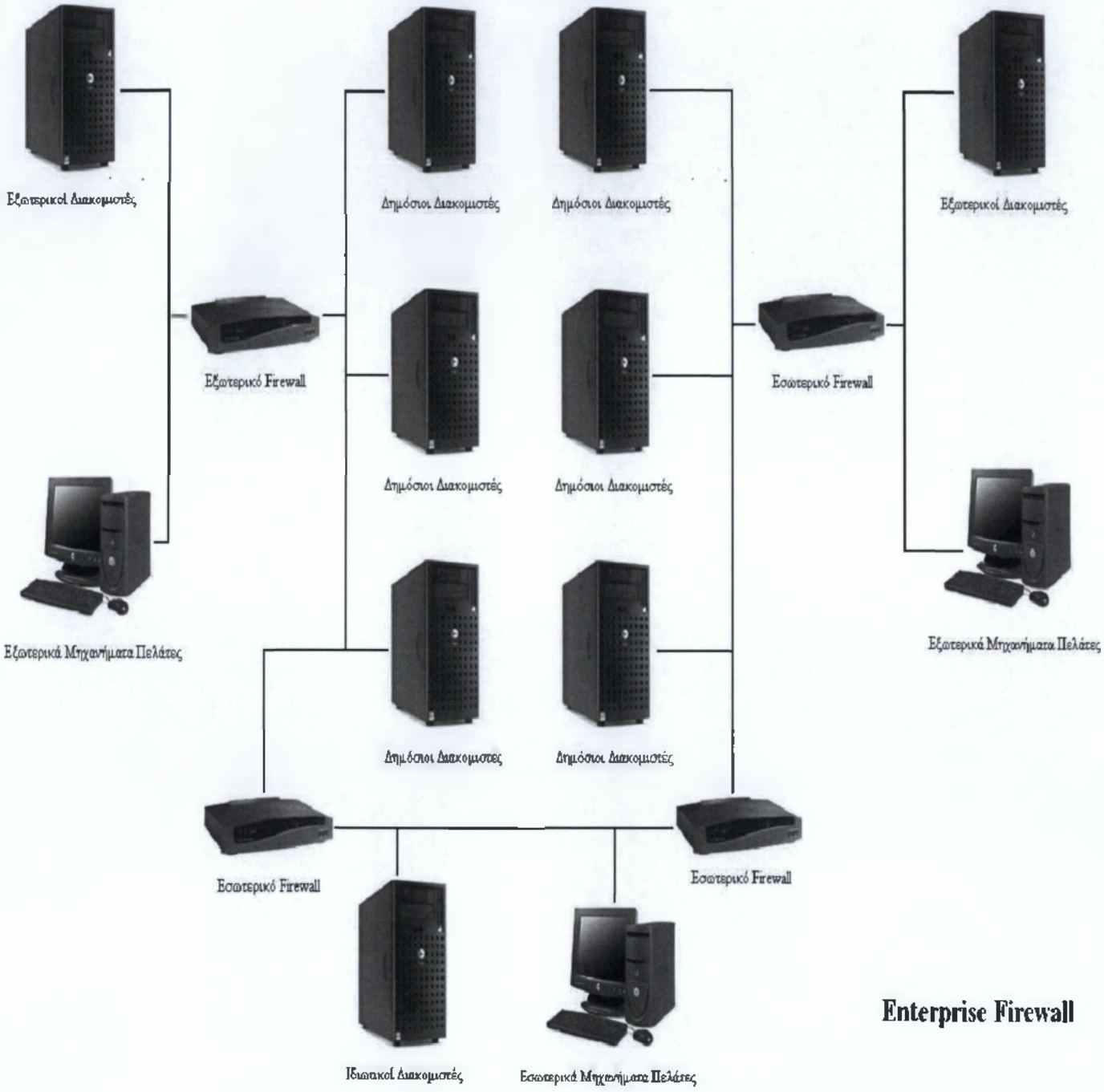
Το αποτέλεσμα απεικονίζεται παρακάτω και είναι γνωστό σαν three-way firewall, γιατί έχει τρεις προσαρμογείς δικτύου.



Three-Way Firewall

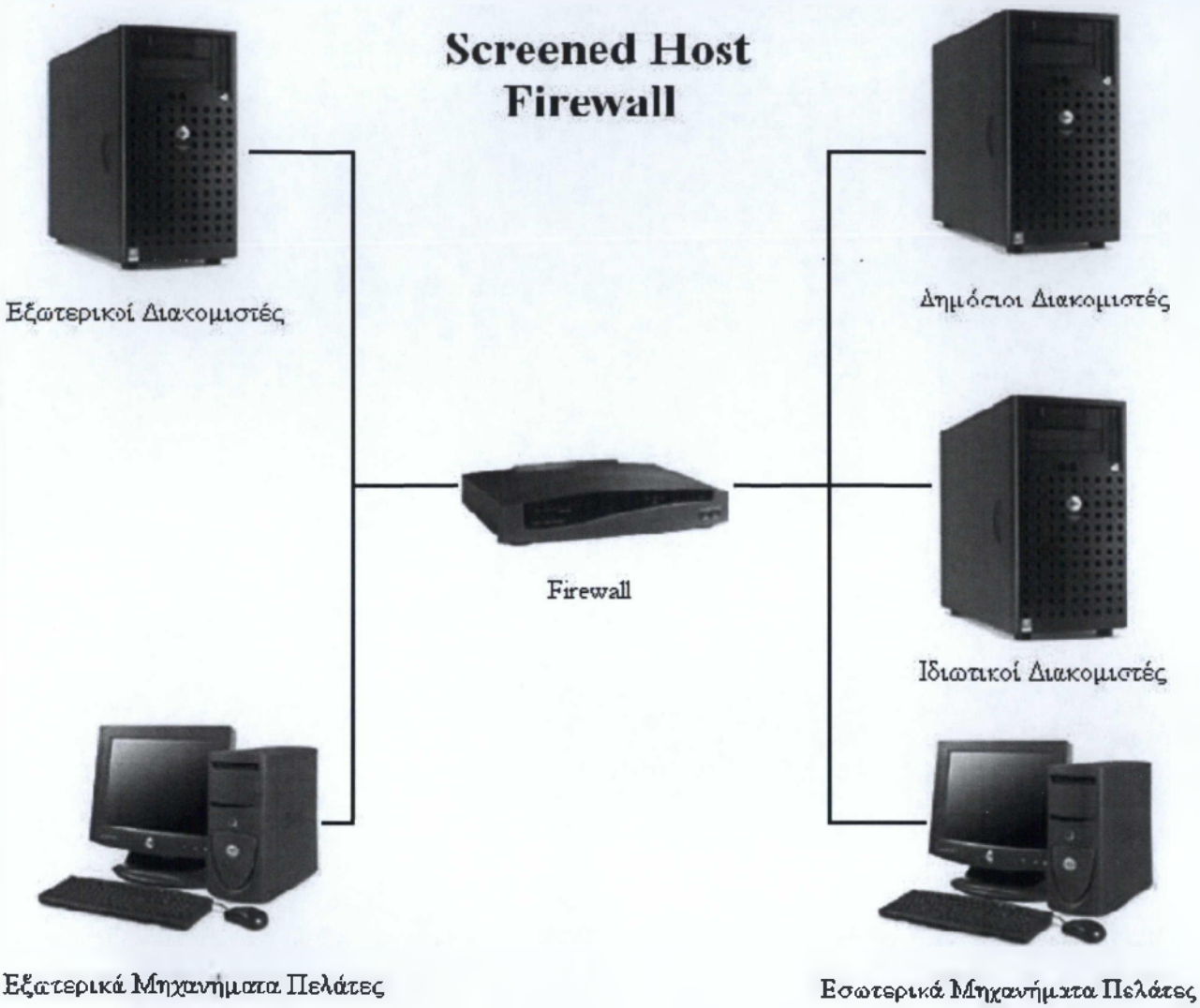
Όπως στην screened network firewall αρχιτεκτονική έτσι και στην three-way firewall αρχιτεκτονική τοποθετούμε τους δημόσιους διακομιστές και τους ιδιωτικούς host πίσω από το firewall παρέχοντας ικανοποιητικό βαθμό ασφαλείας. Ακόμα πιο εξειδικευμένες αρχιτεκτονικές είναι πιθανές.

Μεγάλες επιχειρήσεις χρειάζονται πιο εξειδικευμένες αρχιτεκτονικές. Για παράδειγμα μια επιχείρηση που επικοινωνεί με πολλαπλά εξωτερικά δίκτυα μπορεί να χρησιμοποιήσει μια αρχιτεκτονική όπως η παρακάτω. Η αρχιτεκτονική αυτή προσφέρει υπεράριθμη δρομολόγηση από το εσωτερικό ιδιωτικό δίκτυο, στο εξωτερικό δημόσιο δίκτυο. Συνεπώς, η πρόσβαση του δικτύου είναι αξιόπιστη. Επίσης, επειδή η αρχιτεκτονική αυτή βασίζεται στην screened network, το επίπεδο ασφαλείας είναι αυξημένο. Ένα παράδειγμα της αρχιτεκτονικής αυτής διακρίνεται στο παρακάτω σχήμα.



Enterprise Firewall

Η αρχιτεκτονική αυτή παρέχει πλήρης δρομολόγηση από το εσωτερικό ιδιωτικό δίκτυο στο εξωτερικό δίκτυο και έτσι η πρόσβαση είναι αξιόπιστη. Επιπλέον επειδή η μορφοποίηση βασίζεται σε screened network αρχιτεκτονική το επίπεδο ασφαλείας είναι υψηλό.



Η αρχιτεκτονική αυτή παρέχει πλήρη δρομολόγηση από το εσωτερικό ιδιωτικό δίκτυο στο εξωτερικό δίκτυο και έτσι η πρόσβαση είναι αξιόπιστη. Επιπλέον, επειδή η μορφοποίηση βασίζεται σε screened network αρχιτεκτονική, το επίπεδο ασφαλείας είναι υψηλό.

1.9 Τύποι εξυπηρετητών

Γενικοί Proxy διακομιστές

Οι γενικοί proxy διακομιστές είναι ο πιο κοινός τύπος των εξυπηρετητών. Χειρίζονται την κίνηση web περιλαμβάνοντας τα πρωτόκολλα HTTP, FTP κτλ. Τα χαρακτηριστικά

http://forum.ubuntu-gr.org/viewforum.php?f=43&http

τους είναι πλούσια. Παρέχουν πολλούς τρόπους πρόσβασης, ελέγχου, φιλτραρίσματος, logging και caching.

Οι firewall proxy διακομιστές δέχονται αιτήσεις μέσα από το firewall, το οποίο τις προωθεί στο internet και επιστρέφει τα αποτελέσματα στον πελάτη. Η χρήση cache γίνεται συχνά από αυτούς τους proxy έτσι ώστε οι αιτήσεις να μην προωθούνται από το διακομιστή προέλευσης, αλλά από την cache.

Τμηματικοί Proxy διακομιστές

Οι τμηματικοί proxy διακομιστές είναι όμοιοι με τους firewall proxy διακομιστές. Το λογισμικό το οποίο χρησιμοποιείται είναι ίδιο με διαφορετικές παραμέτρους. Για παράδειγμα κάποια τμήματα μπορεί να έχουν πιο αυστηρές μεθόδους ελέγχου και ο τρόπος πρόσβασης να ποικίλει από το ένα τμήμα στο άλλο.

Αλυσωτοί Proxy διακομιστές

Οι πελάτες μπορούν να κάνουν αίτηση για δεδομένα μέσω ενός τμηματικού έξυπηρετητή, ο οποίος είναι συνδεδεμένος αλυσωτά με τον firewall proxy διακομιστή. Αλυσωτά σημαίνει ότι ο τμηματικός proxy διακομιστής αναλαμβάνει τις αιτήσεις μέσω ενός άλλου proxy διακομιστή, σε αυτήν την περίπτωση του firewall proxy. Ο ένας proxy ωφελείται από τον άλλο γιατί αν γίνει μια αίτηση για ένα αντικείμενο, αυτό χρησιμοποιείται από την cache του κοντινότερου εξυπηρετητή στην οποία υπάρχει.

Η χρήση αλυσωτών εξυπηρετητών μειώνει το φόρτο εργασίας του κεντρικού firewall εξυπηρετητή. Μόνο οι αιτήσεις, τα περιεχόμενα των οποίων δεν βρίσκονται στην cache των τμηματικών εξυπηρετητών, προωθούνται στον κεντρικό firewall εξυπηρετητή.

Προσωπικοί proxy διακομιστές

Οι προσωπικοί proxy διακομιστές τρέχουν στον ίδιο host με το λογισμικό του πελάτη. Ο διαχωρισμός των χαρακτηριστικών του λογισμικού πελάτη και του προσωπικού διακομιστή είναι ασαφής. Στην πραγματικότητα κάποιος μπορεί να ισχυριστεί ότι οι προσωπικοί διακομιστές θα έπρεπε να ήταν ενσωματωμένοι με το λογισμικό του πελάτη.

Εξειδικευμένοι διακομιστές

Οι εξειδικευμένοι proxy διακομιστές λειτουργούν σαν ομάδα και εκτελούν ειδικές λειτουργίες. Ένα καλό παράδειγμα είναι ο proxy διακομιστής ενσωματωμένος σε ένα

λογισμικό ενός υπολογιστή παλάμης. Αυτός ο τύπος του proxy θα μπορούσε να μειώσει την ποιότητα εικόνας και τον αριθμό των χρωμάτων ώστε μετατρέποντας το format της, να γίνεται αντιληπτή από τον υπολογιστή παλάμης. Με αυτόν τον τρόπο μειώνει το bandwidth το οποίο απαιτείται, και είναι περιορισμένο για έναν υπολογιστή παλάμης καθώς επίσης την ίδια στιγμή διαμορφώνει τα δεδομένα, ώστε να είναι κατάλληλα για το λογισμικό και υλικό που απευθύνονται.

Αντίστροφοι Proxy διακομιστές

Ο όρος αντίστροφος proxy αναφέρεται στις ρυθμίσεις κατά τις οποίες ο proxy εκτελείται με τέτοιο τρόπο ώστε να εμφανίζεται στον πελάτη σαν ένας κανονικός web διακομιστής. Έτσι οι πελάτες συνδέονται με αυτόν θεωρώντας τον σαν έναν κανονικό διακομιστή προέλευσης χωρίς να ξέρουν αν οι αιτήσεις τους θα καθυστερηθούν περισσότερο μέσο ενός άλλου διακομιστή ή ακόμα και ενός άλλου proxy.

Ο ορισμός αυτός αναφέρεται στον αντίστροφο ρόλο του proxy διακομιστή. Σε κανονική μορφή ο proxy λειτουργεί για τον πελάτη και η αίτηση γίνεται εκ μέρους του. Σε αντίστροφη μορφή ο αντίστροφος proxy λειτουργεί για τον διακομιστή και οι proxy υπηρεσίες κάνουνε αιτήσεις εκ μέρους του διακομιστή.

1.10 Τί είναι το Squid

Το Squid είναι ένα δωρεάν, υψηλών ταχυτήτων, internet proxying – caching λογισμικό. Αλλά τι σημαίνει ο όρος proxy cache; Οι όροι μεταφράζονται ως εξής:

Proxy: Ένας μεσάζοντας με την εξουσιοδότηση να λειτουργεί για κάποιον άλλον.

Cache: Ένα μέρος αποθήκευσης για τη διαφύλαξη και τη διατήρηση δεδομένων τα οποία χρησιμοποιούνται συχνά από εξουσιοδοτημένους χρήστες.

Το Squid δρα σαν ένας μεσάζοντας, δέχεται αιτήσεις από πελάτες όπως browsers, τις περνάει στον αρμόδιο internet διακομιστή, και αποθηκεύει ένα αντίγραφο των προς επιστροφή δεδομένων σε ένα δίσκο cache. Το μεγάλο προτέρημα είναι ότι το Squid ξαναπαρουσιάζεται στο προσκήνιο όταν τα ίδια δεδομένα ζητηθούν πολλές φορές. Εφόσον ένα αντίγραφο δεδομένων υπάρχει στο δίσκο τα δεδομένα επιστρέφονται στον πελάτη και έτσι γίνεται πιο γρήγορη η πρόσβαση εφόσον σώζονται bandwidth.

Πολλά internet firewall συχνά περιλαμβάνουν έναν proxy. Η διαφορά του Squid proxy με έναν firewall proxy είναι ότι οι firewall proxies δεν αποθηκεύουν αντίγραφα προς επιστροφή δεδομένων, αλλά αντί για αυτό αναεξάγουν τις αιτήσεις από τον απομακρυσμένο internet διακομιστή.

Χαρακτηριστικά του Squid:

- Χρησιμοποίηση λιγότερου bandwidth της σύνδεσης του internet όταν σερφάρουμε στο web
- Μείωση του χρόνου φόρτωσης των σελίδων web
- Προστασία των host του εσωτερικού δικτύου χρησιμοποιώντας proxy για την κίνηση web
- Συλλογή στατιστικών για την κίνηση του δικτύου
- Παρεμπόδιση χρηστών από το να επισκέπτονται συγκεκριμένα site (π.χ. πορνογραφικού υλικού κτλ)
- Επιβεβαίωση ότι μόνο εξουσιοδοτημένοι χρήστες μπορούν να σερφάρουν στο internet
- Βελτίωση της ασφάλειας των χρηστών φιλτράροντας ευαίσθητες πληροφορίες
- Μείωση του φόρτου στους web διακομιστές
- Μετατροπή κωδικοποιημένων αιτήσεων σε αποκωδικοποιημένες (HTTPS σε HTTP)
- Υποστήριξη πολλών πρωτοκόλλων (Τα firewalls συχνά έχουν συγκεκριμένους proxy για κάθε πρωτόκολλο, πράγμα το οποίο καθιστά δύσκολο την επιβεβαίωση της ασφάλειας κώδικα σε ένα μεγάλο πρόγραμμα)

1.12 Γιατί οι εξυπηρετητές δεν είναι μέρος των διακομιστών web

Ο λόγος δεν είναι τόσο τεχνικός όσο το ότι υπάρχουν διαφορές στις απαιτήσεις χρηστών. Ο εξυπηρετητής και ο διακομιστής web συχνά έχουν διαφορετική βάση χρηστών. Οι διακομιστές web μπορεί να είναι εστιασμένοι σε ολόκληρο το Internet ή σε μια εταιρία ενώ οι proxy διακομιστές για εξειδικευμένη χρήση από μια εταιρία ή από ένα τμήμα της. Σε γενικές γραμμές χρησιμοποιούνται από διαφορετικά είδη ανθρώπων.

Πρακτικά είναι δυνατόν να φτιάξουμε ένα διακομιστή web που να λειτουργεί και σαν proxy. Εντούτοις υπάρχουν διάφοροι λόγοι για τους οποίους πρέπει να υπάρχει διαχωρισμός.

Βελτιωμένη ασφάλεια

Οι web διακομιστές δεν χρειάζεται να πραγματοποιούν συνδέσεις στο εσωτερικό δίκτυο. Έτσι το firewall μπορεί να ρυθμιστεί ώστε να κόβει συνδέσεις οι οποίες ξεκινούν από τον web διακομιστή. Αυτό προστατεύει το εσωτερικό δίκτυο αν ο web διακομιστής δεσμευτεί από επίθεση. Ακόμα και αν ένας εισβολέας αποκτήσει πρόσβαση στον web διακομιστή δεν θα μπορεί να συνδεθεί με τους host μέσα στο firewall.

Οι proxy διακομιστές από την άλλη δεν χρειάζεται να είναι ικανοί να δεχτούν νέες συνδέσεις προερχόμενες από το εξωτερικό δίκτυο. Αυτό σημαίνει ότι ο proxy μπορεί να είναι προστατευμένος από εισβολείς. Οι ρυθμίσεις του firewall δρομολογητή μπορούν να κόβουν κάθε προσπάθεια σύνδεσης από την proxy διακομιστή.

Ευκολία διαχείρισης

Διαχωρίζοντας τον web διακομιστή και τον proxy διακομιστή γίνεται πιο εύκολη η διαχείρισή τους. Αυτό μειώνει τις πιθανότητες εσφαλμένης λειτουργίας. Για παράδειγμα αν ο έλεγχος πρόσβασης είναι λανθασμένα ρυθμισμένος στον διακομιστή web αυτό δεν επηρεάζει τον proxy διακομιστή και το αντίστροφο.

Δόμηση μέσω υπομονάδων

Από πλευράς ανάπτυξης λογισμικού ο διαχωρισμός των λειτουργιών κάνει την κατασκευή λειτουργικού πιο εύκολη. Διαχωρίζοντας τις λειτουργίες η σταθεροποίηση, η ανάπτυξη, η δοκιμή γίνονται πιο εύκολα και το μέγεθος του λειτουργικού γίνεται μικρότερο.

Marketing

Από πλευράς πωλήσεων λογισμικού είναι φυσικά προτιμότερο να υπάρχουν περισσότερα πακέτα. Από πλευράς αγοραστικού κοινού η δυνατότητα να αγοράσεις μόνο το λογισμικό το οποίο χρειάζεσαι είναι καλό γιατί αποφεύγεις το επιπλέον κόστος υπηρεσιών.

ΚΕΦΑΛΑΙΟ 2°

Σχεδιασμός του Firewall

[2] 2.1 Κύκλος ζωής του firewall

Στην ανάπτυξη λογισμικού έχει καθιερωθεί ένα μοντέλο λεγόμενο «ο κύκλος ζωής του λογισμικού». Αν και το firewall δεν είναι ακριβός λογισμικό η διαδικασία δημιουργίας του είναι παρόμοια. Και οι δυο διαδικασίες παρουσιάζουν ίδια βήματα σε ίδια σειρά. Όπως ο κύκλος ζωής λογισμικού είναι ένας χρήσιμος οδηγός στην ανάπτυξή του, έτσι και ο κύκλος ζωής του firewall είναι ένας χρήσιμος οδηγός στην ανάπτυξη του. Ο κύκλος ζωής του firewall αποτελείται από τα εξής βήματα:

- Καθορισμός απαιτήσεων
- Δικαιολόγηση
- Αρχιτεκτονικός σχεδιασμός
- Καθορισμός πολιτικής
- Υλοποίηση
- Δοκιμή
- Διαχείριση & συντήρηση

Καθορισμός απαιτήσεων

Ο καθορισμός απαιτήσεων καθορίζει τη λειτουργία του firewall. Αναλύει τις απειλές και τους κίνδυνους τους οποίους το firewall πρόκειται να μετριάσει. Ο καθορισμός απαιτήσεων δίνει έμφαση περισσότερο στο τι κάνει το firewall παρά στο πώς. Σκεφτείτε τον καθορισμό απαιτήσεων σαν ερμηνεία των στόχων του firewall.

Δικαιολόγηση

Η κατασκευή ενός firewall περιλαμβάνει την δαπάνη οργανωτικών και οικονομικών τόρων. Τα άτομα της διοίκησης τα οποία έχουν αναλάβει την εξουσιοδότηση για την κατασκευή του firewall πρέπει να πειστούν ότι οι απώλειές τους θα αντισταθμιστούν με τα κέρδη από την κατασκευή του firewall. Συχνά οι απειλές και τα ρίσκα τα οποία σχετίζονται

[2] http://www.linuxtopia.org/LinuxSecurity/LinuxSecurity_Firewall_Intro.html

με επιθέσεις υπολογιστών δεν μοιάζουν σημαντικά σε διοικητικά μέλη τα οποία μπορεί να μην είναι πρόθυμα να χρηματοδοτήσουν το project. Αντίστοιχα οι διαχειριστές δικτύου μπορεί να έχουν έλλειψη ικανοτήτων στο να πείσουν τα μέλη της διοίκησης για τη σπουδαιότητα της ασφάλειας δικτύου.

Αρχιτεκτονικός σχεδιασμός

Ο αρχιτεκτονικός σχεδιασμός του firewall αποτελείται από την απόφαση του ποιες βασικές αρχιτεκτονικές είναι κατάλληλες, οι οποίες έπειτα αν τροποποιηθούν να πληρούν τις απαιτήσεις.

Ο αρχιτεκτονικός σχεδιασμός περιλαμβάνει τέσσερα βήματα:

1) Αναγνωρίζει την υποψήφια αρχιτεκτονική και τεχνολογία

2) Κατανόηση του πώς οι υποψήφιες αρχιτεκτονικές και τεχνολογίες θα λειτουργήσουν στην συγκεκριμένη περίσταση

3) Επιλογή της υποψήφιας αρχιτεκτονικής και τεχνολογίας η οποία είναι η πιο κατάλληλη

4) Βελτίωση της επιλεγμένης αρχιτεκτονικής για καλύτερη απόδοση

Καθορισμός πολιτικής

Ο καθορισμός πολιτικής περιλαμβάνει τις πολιτικές και τους κανόνες, οι οποίοι θα κατευθύνουν την λειτουργία του firewall. Οι διεργασίες οι οποίες περιλαμβάνει είναι οι εξής:

- Αναγνώριση των host, οι οποίοι θα έχουν εξουσιοδότησε σε συγκεκριμένες υπηρεσίες
- Αναγνώριση των χαρακτηριστικών της κάθε υπηρεσίας
- Προετοιμασία εγγράφων για το πώς το firewall χειρίζεται τα δεδομένα
- Στο σχεδιασμό ενός μικρού firewall ο σχεδιαστής συνήθως συνδυάζει τον σχεδιασμό πολιτικής με την πραγματοποίηση.

Έτσι, όταν αυτό το μέρος πραγματοποιηθεί το firewall παίρνει την τελική του μορφή. Εντούτοις είναι γενικά χρήσιμο να δημιουργούμε έγγραφα σχεδιασμού ακόμα και για μικρά firewall. Αυτά τα έγγραφα είναι λιγότερο ογκώδη και πιο εύκολο να διαβαστούν.

Υλοποίηση firewall

Η υλοποίηση του firewall περιλαμβάνει τη μετατροπή των πολιτικών του σε μορφή τελικού firewall. Συχνά αυτή η διαδικασία περιλαμβάνει την μετάφραση του σχεδιασμού του firewall σε εντολές και συντακτικές παραμέτρους οι οποίες είναι κατανοητές από την εκάστοτε χρησιμοποιούμενη τεχνολογία.

Εντούτοις κάποια σύγχρονα firewall περιλαμβάνουν γραφικά περιβάλλοντα αντί για χρήση γλώσσας εντολών. Σε αυτές τις περιπτώσεις η υλοποίηση του firewall αποτελείται από την παραμετροποίηση του προϊόντος ώστε να εκτελεί τις καθορισμένες λειτουργίες από τον σχεδιασμό πολιτικής του firewall.

Δοκιμή

Αφού το firewall έχει υλοποιηθεί ο έλεγχος της σωστής λειτουργίας του είναι απαραίτητος. Η δοκιμή του firewall περιλαμβάνει την δημιουργία δεδομένων εγγράφων για το πώς ανταποκρίνεται το firewall σε συγκεκριμένες λειτουργίες. Με την εκτέλεση προγραμμάτων ελέγχου firewall και συγκρίνοντας έπειτα τα αποτελέσματα με αυτά των εγγράφων προσδιορίζεται η σωστή λειτουργία του firewall. Ακόμα και οι πιο προσεκτικοί άνθρωποι είναι πιθανόν να κάνουν λάθη. Ένα μικρό λάθος μπορεί να εξασφαλίσει στον επιτιθέμενο την ευκαιρία να παραβιάσει ακόμα και το πιο εξεζητημένο firewall. Έτσι δεν πρέπει να βασιζόμαστε σε firewall μέχρις ότου η λειτουργία τους δοκιμαστεί και επαληθευτεί.

Διαχείριση και συντήρηση

Τα firewall χρειάζονται συνεχή διαχείριση και συντήρηση. Πιο συγκεκριμένα η χρήση των firewall logs μπορεί να μας ενημερώσει για επιθέσεις δίνοντάς μας την ευκαιρία να βελτιώσουμε την άμυνα του δικτύου απέναντι σε καθορισμένους τύπους επιθέσεων.

2.2 Κόστος και οφέλη

Οι αποφάσεις διαχείρισης συχνά βασίζονται σε οικονομικές παραμέτρους. Στην υπόδειξη ενός προσχεδίου firewall πρέπει να καθοριστούν το κόστος και τα οφέλη με οικονομικές ορολογίες. Ένα συχνό λάθος στην αναφορά του κόστους είναι η θεώρηση μόνο των αρχικών δαπανών, δηλαδή του σχεδιασμού και της υλοποίησης του firewall.

Ακόμα και το πιο απλό firewall απαιτεί κάποια διαρκή διαχείριση και συντήρηση. Για αυτόν το λόγο η εκτίμηση πρέπει να περιλαμβάνει μια πρόβλεψη και των μελλοντικών δαπανών.

[3] 2.3 Επιλογή Λογισμικού και υλικού

Ο δεύτερος στόχος του σχεδιασμού του firewall είναι η επιλογή της τεχνολογίας. Πρέπει να έχουμε στο μυαλό μας ότι η επιλογή τεχνολογιών μπορεί να είναι συμπληρωματική. Ένα μικρό δίκτυο μπορεί να πραγματοποιηθεί με τη χρήση μιας μόνο τεχνολογίας αλλά ένα μεγάλο δίκτυο μπορεί να ωφεληθεί από ένα σχεδιασμό, ο οποίος μπορεί να ενσωματώνει πολλαπλές τεχνολογίες. Γενικά, οι σχεδιαστές δεν επιλέγουν μια τεχνολογία, αλλά ένα προϊόν που ενσωματώνει περισσότερες από μια τεχνολογίες. Σαν χαρακτηριστικά επιλογής τεχνολογιών έχουμε τα εξής:

- Κόστος
- Χαρακτηριστικά όπως NAT, VPN, Logs κτλ.
- Τεχνική υποστήριξη και τεκμηρίωση με έγγραφα
- Ευκολία χρήσης
- Σταθερότητα
- Απόδοση

Σε αυτό το κεφάλαιο αναφέρουμε τα δημοφιλέστερα προϊόντα firewall δίνοντας έμφαση στις τεχνολογίες που ενσωματώνουν. Τα προϊόντα αυτά που θα μας απασχολήσουν είναι τα παρακάτω:

- IPTables
- IPChains
- TIS Firewall Toolkit
- Firewall-1
- Firewall Υλικού

[3] http://www.yolinux.com/TUTORIALS/LinuxTutorialIptablesNetworkGateway.html

IPChains

Το RedHat Linux 6.2 και οι προηγούμενες εκδόσεις του υποστήριζαν το IPChains. Το IPChains παρέχει stateless packet filtering. Συνεπώς το IPChains firewall πρέπει να δέχεται τις εισερχόμενες συνδέσεις άσχετα με την προέλευσή τους. Έτσι τα IPChains firewall είναι σχετικά ευπαθή σε σαρώσεις που έχουν το TCP flag δηλωμένο σαν ACK. Τα firewall αυτά δεν μπορούν να εμποδίσουν χρήστες ή ύποπτο λογισμικό, όπως Trojans, από το να παρακολουθούνε εισερχόμενες συνδέσεις. Το IPChains υποστηρίζει μασκάρισμα και προώθηση πόρτων. Η προώθηση πόρτων είναι μια ειδική περίπτωση του NAT προορισμού στην οποία ο αριθμός του Port και όχι η διεύθυνση IP είναι το αντικείμενο προς τροποποίηση. Το IPChains περιλαμβάνει καταγραφή πακέτων (logs) με τη λειτουργία syslog.

Χαρακτηριστικά του IPChains

Χαρακτηριστικά	Περιγραφή
Τεχνολογία	Stateless Packet Filtering
Μασκάρισμα	NAI
NAT	Περιορισμένο
Logging	Syslog
Περιβάλλον Χρήστη	Γραμμή Εντολών

IPTables

Το RedHat Linux 9 και οι επόμενες εκδόσεις περιλαμβάνουν το IPTables το οποίο είναι ο διάδοχος του IPChains. Η ασφάλεια που παρέχει το IPTables είναι ανώτερη του IPChains γιατί το IPTables χρησιμοποιεί Statefull Packet Filtering. Έτσι μπορεί να μπλοκάρει εισερχόμενα πακέτα τα οποία δεν είναι μέρη ή δεν σχετίζονται με Established συνδέσεις. Συνεπώς το IPTables αντίθετα με το IPChains μπορεί να μπλοκάρει ανεπιθύμητη κίνηση σε συγκεκριμένα port. Επιπλέον, υποστηρίζει μασκάρισμα IP και NAT διεύθυνσης και προορισμού. Ένα δίκτυο προστατευμένο από το IPTables μπορεί να αντισταθεί σε ACK

σαρώσεις και να περιορίσει την ικανότητα χρηστών ή ύποπτου λογισμικού να παρακολουθεί ή να δέχεται εισερχόμενες συνδέσεις.

Χαρακτηριστικά του IPTables

Χαρακτηριστικά	Περιγραφή
Τεχνολογία	Statefull Packet Filtering
Μασκάρισμα	NAI
NAT	NAI
Logging	Syslog
Περιβάλλον Χρήστη	Γραμμή Εντολών

TIS Firewall Toolkit

Το TIS Firewall Toolkit αναπτύχθηκε στα τέλη της δεκαετίας του 90 υπό την εποπτεία του DARPA (US Defence Advanced Research Projects Agency). Το πακέτο συνεχίζει να χρησιμοποιείται και να παραμένει δημοφιλές μέχρι σήμερα. Όπως μας παραπέμπει και το όνομα, είναι μια συλλογή εργαλείων για την δημιουργία firewalls. Επειδή είναι μια συλλογή εργαλείων και όχι ένα έτοιμο προς χρήση firewall η κατασκευή ενός firewall με τη χρήση του απαιτεί παραμετροποίηση και προγραμματισμό.

Αντίθετα με το IPChains και το IPTables το TIS Firewall Toolkit παρέχει Proxy-Based firewalling δίνοντας μας αυξημένο επίπεδο ασφαλείας και ευκαμψίας. Το TIS Firewall Toolkit περιλαμβάνει SMPT, HTTP, FTP και πολλούς άλλους proxy και ακόμα παρέχει την δυνατότητα κατασκευής proxy για ακόμα περισσότερα πρωτόκολλα.

Χαρακτηριστικά του TIS Firewall Toolkit

Χαρακτηριστικά	Περιγραφή
Τεχνολογία	Proxy
Μασκάρισμα	NAI
NAT	NAI
Logging	Syslog
Περιβάλλον Χρήστη	Γραμμή Εντολών

CheckPoint Firewall-1

Το Firewall-1 από την εταιρία CheckPoint είναι ένα δημοφιλές εμπορικό firewall που τρέχει κάτω από πολλές πλατφόρμες περιλαμβάνοντας και το RedHat Linux. Μερικοί ειδικοί θεωρούν το Firewall-1, το κυρίαρχο εμπορικό προϊόν firewall. Το Firewall-1 παρέχει statefull packet filtering και NAT. Επιπλέον έχει πολλές αξιοσημείωτες δυνατότητες:

- Υψηλή διαθεσιμότητα
- Γραφικό περιβάλλον
- Φιλτράρισμα περιεχομένου σε επίπεδο εφαρμογών
- Υποστήριξη proxy για πολλά πρωτόκολλα
- Υποστήριξη multimedia πρωτοκόλλων

Η υψηλή διαθεσιμότητα του firewall σημαίνει ότι είναι σχεδιασμένο να λειτουργεί συνεχώς. Για να παρέχει υψηλή διαθεσιμότητα το firewall-1 μπορεί να πραγματοποιηθεί με multi-host αρχιτεκτονική στην οποία ένα δευτερεύον firewall αυτόματα αναλαμβάνει τον έλεγχο όταν το πρωτεύον βρεθεί εκτός λειτουργίας. Το φιλτράρισμα περιεχομένου σε επίπεδο εφαρμογών μπορεί να πραγματοποιήσει λειτουργίες όπως μπλοκάρισμα επικίνδυνων e-mail.

Επιπλέον το Firewall-1 παρέχει χρήση Proxy για πρωτόκολλα όπως RealVideo, Windows Media και H323 τα οποία χρησιμοποιούνται για VoIP, Netmeeting κτλ. Το Firewall-1 δεν χρησιμοποιεί την Syslog λειτουργία, αλλά αντί για αυτό έχει μια ιδιωτική μέθοδο καταγραφών.

Χαρακτηριστικά του Firewall-1

Χαρακτηριστικά	Περιγραφή
Τεχνολογία	Statefull Packet Filtering
Μασκάρισμα	NAI
NAT	NAI
Logging	Ιδιωτική Μέθοδος
Περιβάλλον Χρήστη	Γραφικό

Firewall Υλικού

Ένας εναλλακτικός τύπος firewall είναι αυτά που στεγάζονται σε μονάδες υλικού όπως για παράδειγμα τα Cisco PIX firewalls. Η αξιοπιστία τους MTBF (Mean Time Between Failure) είναι υψηλότερη από αυτή των υπόλοιπων firewall. Τα PIX περιλαμβάνουν Statefull Packet Filtering με περιορισμένη υποστήριξη για proxy όπως H323. Είναι διαθέσιμα σε πολλά μοντέλα έχοντας υποστήριξη για bandwidth από 10MBps έως 1GBps. Επειδή οι μονάδες PIX δεν έχουν εσωτερικούς δίσκους πρέπει να κάνουν τις καταγραφές τους σε ένα ξεχωριστό διακομιστή καταγραφών. Αυτός μπορεί να είναι ένας Syslog server ή μια μονάδα υλικού σχεδιαζόμενη από τη Cisco σαν συμπλήρωμα στο PIX.

Χαρακτηριστικά των PIX Firewalls

Χαρακτηριστικά	Περιγραφή
Τεχνολογία	Statefull Packet Filtering
Μασκάρισμα	NAI
NAT	NAI
Logging	Εξωτερικό
Περιβάλλον Χρήστη	Γραφικό και Γραμμής Εντολών

ΚΕΦΑΛΑΙΟ 3°

Απειλές και Αρχές της Άμυνας Δικτύων

[4] 3.1 Απειλές στην ασφάλεια του δικτύου

Μία αποτελεσματική στρατηγική για την άμυνα του δικτύου θα πρέπει να μπορεί να αντιμετωπίσει καινούρια είδη επιθέσεων. Ωστόσο η πλειονότητα των επιθέσεων είναι σχετικά προβλέψιμες. Έτσι πρέπει κανείς να εξασφαλίσει υψηλή ασφάλεια στο δίκτυο του για να μπορεί να επικεντρωθεί σε λιγότερο γνώριμες μορφές απειλών.

3.2 Κατηγορίες επιτιθέμενων

Σε αντίθεση με το κυρίαρχο στερεότυπο των νεαρών εισβολέων η ειδικοί της ασφάλειας αναγνωρίζουν δυο κατηγορίες εισβολέων. Τους blackhats και script kiddies.

Οι blackhats εξαιτίας της μεγάλης εξειδίκευσης τους είναι ικανοί να εξαπολύσουν μία μεγάλη γκάμα επιθέσεων εναντίων μιας μεγάλης γκάμας συστημάτων. Ωστόσο οι περισσότερες επιθέσεις εξαπολύονται από τους script kiddies που επιτίθενται με προγράμματα που κατεβάζουν από το internet. Τέτοια προγράμματα μπορεί να είναι τα scanners τα οποία εξετάζουν host και δίκτυα για ευάλωτα σημεία. Όταν βρεθεί ένα ευάλωτο σημείο οι script kiddies εκτελούν ένα πρόγραμμα με την ονομασία exploit το οποίο παραβιάζει την ασφάλεια του host. Όταν η ασφάλεια παραβιαστεί εγκαθιστούν ένα rootkit το οποίο καλύπτει την εισβολή και δίνει στον εισβολέα τον έλεγχο του host.

Οι blackhats επίσης μπορεί να χρησιμοποιήσουν αυτά τα εργαλεία, αλλά τα χρησιμοποιούν με ένα πιο εξελιγμένο τρόπο σε αντίθεση με τους script kiddies που επιτίθενται λιγότερο διακριτικά.

Παράλληλα ένας αυξανόμενος αριθμός επιθέσεων εξαπολύονται αυτόματα από προγράμματα γνωστά ως worms. Ένα τέτοιο worm εκμεταλλεύεται την ευαισθησία ενός Microsoft SQL διακομιστή για να πάρει τον έλεγχο του host θύματος. Έτσι σε σύντομο χρόνο το worm προσβάλει χιλιάδες συστήματα και δημιουργεί μια «πίσω πόρτα» από όπου

[4] http://www.islab.demokritos.gr/gr/html/index.htm

ένας εισβολέας μπορεί να ελέγξει ένα μολυσμένο σύστημα. Έτσι οι script kiddies βρίσκουν ήδη μολυσμένα συστήματα και τα χρησιμοποιούν για δικούς τους σκοπούς.

3.3 Κίνητρα των εισβολέων

Οικονομικό ή προσωπικό όφελος

Οι εισβολείς υπολογιστών συχνά στοχεύουν βάσεις δεδομένων που περιέχουν πληροφορίες πιστωτικών καρτών. Ένας εισβολέας που μπαίνει σε μια τέτοια βάση δεδομένων μπορεί να έχει πρόσβαση σε χιλιάδες πιστωτικές κάρτες. Ωστόσο η επίθεση μπορεί να είναι και για προσωπικό όφελος και ένα παράδειγμα είναι οι φοιτητές που εισβάλουν σε βάσεις για την αλλαγή βαθμών.

Πρόσβαση σε υπολογιστικούς πόρους

Ορισμένες φορές οι εισβολείς θέλουν απλά να έχουν πρόσβαση στους υπολογιστικούς πόρους των συστημάτων που στοχεύουν . Για παράδειγμα ένας blackhat που θέλει να μολύνει ένα σύστημα μπορεί πρώτα να επιτεθεί σε διάφορα άλλα μη σχετιζόμενα συστήματα και να τα χρησιμοποιήσει για να καλύψει την ταυτότητα του.

Αναδημιουργία και εξαπάτηση

Μερικοί εισβολείς και πιο συγκεκριμένα οι script kiddies αντιμετωπίζουν τις εισβολές τους σαν σπορ και συχνά ο μοναδικός τους σκοπός δεν είναι άλλος από το να εισβάλουν στον σύστημα. Απολαμβάνουν την εκτίμηση των άλλων ανάλογα με τον αριθμό των συστημάτων που έχουν εισβάλει και συχνά ανακοινώνουν στο δίκτυο τα επιτεύγματα τους.

Πολιτικές σκοπιμότητες

Σε ορισμένες περιπτώσεις ο στόχος των εισβολέων είναι να ενοχλήσουν ολικά πρόσωπα του έχουν διαφορετικές απόψεις από τις δικές τους, αλλά και δημόσιους οργανισμούς ή εταιρίες που αντιπαθούν. Για παράδειγμα πολλοί blackhats μπορεί να αντιτίθενται στην βιομηχανία εμπορικής ασφάλειας και για αυτό επιχειρούν να παραβιάσουν αυτές τις εταιρίες και ειδικότερα όσες υποστηρίζουν ότι είναι ιδιαίτερα αξιόπιστες.

3.4 Τύποι επιθέσεων

Αυτή η ενότητα εξετάζει μερικούς από τους τρόπους με τους οποίους διαπράττονται παράνομες δραστηριότητες στο Internet. Αυτές κυμαίνονται από ενέργειες οι οποίες απλά

εκμεταλλεύονται την απλή ανθρώπινη αδυναμία έως αυτές που απαιτούν εξειδικευμένες τεχνολογικές γνώσεις και βαθιά κατανόηση της δομής του Internet. Ωστόσο, πριν εξετάσουμε αυτούς τους τρόπους με τους οποίους μπορεί να απειληθεί ένα σύστημα, αξίζει να δούμε τους τύπους απειλών που μπορεί να αντιμετωπίσει ένα Web Site.

- *Απειλές ακεραιότητας δεδομένων.* Αυτές οι απειλές αφορούν την παραποίηση αποθηκευμένων δεδομένων από έναν εισβολέα όπως την αλλαγή στοιχείων πιστωτικών καρτών σε μια βάση δεδομένων ή την παραποίηση στοιχείων κατά την μεταφορά τους όπως την μεταβολή ενός μηνύματος κατά τη μεταφορά του.
- *Απειλές εμπιστευτικών δεδομένων.* Αυτές οι απειλές αφορούν την ανάγνωση σημαντικών αποθηκευμένων δεδομένων από μη εξουσιοδοτημένα άτομα όπως π.χ. διοικητικά μυστικά εταιρειών κ.λπ.
- *Απειλές άρνησης υπηρεσιών (Denial of Service - DoS).* Αυτές οι απειλές αφορούν το πλημμύρισμα ενός Web server με μεγάλο αριθμο αιτημάτων ώστε να μην μπορεί πλέον αυτός να λειτουργήσει λόγω έλλειψης πόρων.
- *Απειλές πιστοποίησης χρηστών.* Σε τέτοιου είδους απειλές ο εισβολέας προσποιείται πως είναι ένας χρήστης ενώ δεν είναι.

Μη-τεχνολογικές επιθέσεις

Αυτές είναι επιθέσεις οι οποίες είτε βασίζονται σε κάποια αδυναμία μιας επιχείρησης ή οργανισμού είτε απαιτούν ελάχιστες γνώσεις υπολογιστών για να γίνουν. Μερικά παραδείγματα είναι:

- Να μαντέψει κανείς το password κάποιου άλλου και να αποκτήσει έτσι πρόσβαση στα αρχεία του. Συχνά τα passwords επιλέγονται ώστε να είναι ευκολομνημόνευτα, για παράδειγμα το όνομα της συζύγου του κατόχου του λογαριασμού, των παιδιών του κ.λπ. Όταν τα password είναι ευκολομνημόνευτα, μπορεί να μην είναι τελικά τόσο δύσκολο για κάποιον να το μαντέψει.
- Να κλέψει κανείς password το οποίο είναι εύκολο να βρεθεί με φυσικό τρόπο, π.χ. θα μπορούσε να είναι γραμμένο σε ένα πίνακα, σε ένα ημερολόγιο ή σε ένα κομμάτι χαρτί στο συρτάρι σας.
- Να εκμεταλλευτεί κανείς ελλιπείς φυσικούς η λειτουργικούς ελέγχους. Υπάρχουν για

παράδειγμα αρκετές ιστορίες υπαλλήλων τραπεζών οι οποίοι εκδίδανε πιστωτικές κάρτες σε μη υπάρχοντες πελάτες, κρατούσαν την κάρτα οι ίδιοι και την χρησιμοποιούσαν. Αυτός ο τύπος απειλής είναι βέβαια πολύ μακριά από μια τεχνολογική απειλή και απλά βασίζεται σε εσωτερικές αδυναμίες ενός οργανισμού.

- Να γράψει ένα μικρό πρόγραμμα το οποίο παρουσιάζει ένα παράθυρο το οποίο ζητά από τον χρήστη κάποιες σημαντικές πληροφορίες όπως στοιχεία πιστωτικών καρτών, password κ.λπ. Ένα συνηθισμένο παράθυρο ήταν κάποιο το οποίο έλεγε πως έχει πέσει η σύνδεση τους και ότι πρέπει να συνδεθούν ξανά δίνοντας ένα password. Οι γλώσσες Java και JavaScript μπορούν να κάνουν τη συγγραφή ενός τέτοιου προγράμματος αρκετά εύκολη.

Καταστροφικές επιθέσεις

Αυτά είναι τα ηλεκτρονικά αντίστοιχα των βομβών: απαιτούν πολύ λίγες γνώσεις αλλά τα αποτελέσματα τους μπορεί να είναι αρκετά σημαντικά.

Είδη επιθέσεων DoS (Denial of Service)

Τον τελευταίο καιρό έχουν γίνει πολλές συζητήσεις για το θέμα των επιθέσεων DoS χάρη στις οποίες είναι δυνατή η σχετικά εύκολη απενεργοποίηση ενός κόμβου Internet, ακόμη και από άτομα με μικρές τεχνικές γνώσεις. Παρακάτω περιγράφουμε τα κυριότερα είδη αυτών των επιθέσεων οι οποίες έχουν ως κοινό χαρακτηριστικό την αποστολή στο θύμα (τον server που αποτελεί τον στόχο της επίθεσης) ενός τόσο μεγάλου αριθμού πλαστών αιτημάτων σύνδεσης ώστε δεν μπορεί πλέον να διαχειριστεί το παραμικρό και διακόπτει τη λειτουργία του.

Οι κυριότερες μορφές επιθέσεων αυτής της μορφής είναι:

Ping of Denial (γνωστή και ως Ping of Death)

Πρόκειται για την παλαιότερη και πιο διαδεδομένη μορφή επίθεσης. Για καθαρά τεχνικούς λόγους κάθε server συνδεδεμένος με το Internet πρέπει να μπορεί να δεχθεί μηνύματα ping στα οποία απαντά αποστέλλοντας μια σειρά από μηνύματα pong χάρη στα οποία μετράται η ταχύτητα ανταπόκρισής του.

Για την επίθεση αυτή ο επιτιθέμενος απλώς αποστέλλει πάρα πολλά μηνύματα ping τα οποία ο server είναι υποχρεωμένος να απαντήσει, δαπανώντας φυσικά υπολογιστική ισχύ

και bandwidth. Αν τα μηνύματα ping είναι πάρα πολλά τότε ο αποδέκτης τους καθυστερεί σημαντικά στην εκτέλεση άλλων εργασιών (π.χ. αποστολή web σελίδων) διότι είναι πολύ απασχολημένος στέλνοντας pong, ενώ αν ο φόρτος γίνει πολύ μεγάλος είναι πιθανό να διακόψει τελείως τη λειτουργία του.

Δυστυχώς, η άμυνα από το Ping of Death είναι εξαιρετικά δυσχερής, καθώς το Ping αποτελεί τη μέθοδο με την οποία ένας Η/Υ δηλώνει ότι είναι ενεργός μέσα στο δίκτυο. Δεν είναι λοιπόν δυνατόν να αρνηθεί να απαντήσει σε όποιο Ping δέχεται. Τελευταία, μερικά συστήματα έχουν αποκτήσει μεγάλους Ping buffers και έτσι μπορούν είτε να απαντούν σε πολλά Ping χωρίς να επηρεάζεται η λειτουργία τους, είτε να επεξεργάζονται όσα Ping δέχονται, αναγνωρίζοντας και αγνοώντας αυτόματα όποια από αυτά αποτελούν προϊόν επιθέσεως.

ICMP

Το πρωτόκολλο ICMP χρησιμοποιείται για την επικοινωνία μεταξύ υπολογιστών, χωρίς να χρειάζεται η υλοποίηση ενός ισχυρότερου και πιο περίπλοκου (συνεπώς και πιο αργού) πρωτοκόλλου όπως το TCP. Το ICMP μεταφέρει πολύ λίγες πληροφορίες οι οποίες ενημερώνουν κάθε υπολογιστή για την κατάσταση της σύνδεσής του με άλλα μηχανήματα. Για να "κλείσει" τη σύνδεση ενός Η/Υ ο επιτιθέμενος δεν έχει παρά να του στείλει μέσω του ICMP ένα από τα ακόλουθα μηνύματα:

- Destination Unreachable
- Time to Live Exceeded
- Parameter Problem
- Packet Too Big
- Source Quench

Ουσιαστικά δηλαδή, ο επιτιθέμενος δηλώνει απλώς στο θύμα πως υπάρχει πρόβλημα και ο αποδέκτης διακόπτει τη σύνδεσή του! Θεωρητικά, αυτό το πρόβλημα μπορεί να αντιμετωπιστεί αν απενεργοποιηθεί (κλείσει) η ICMP port (στα Windows αυτή είναι η default επιλογή). Δυστυχώς, με τον τρόπο αυτό μειώνεται η ταχύτητα σύνδεσης ενός Η/Υ με το δίκτυο. Έτσι, πολλοί administrators προτιμούν να διατηρούν αυτή τη δυνατότητα εν λειτουργία, παρ' όλους τους κινδύνους που συνεπάγεται κάτι τέτοιο.

Fragmentation

Αποτελεί τον πιο μοντέρνο, και γι' αυτό πιο δύσκολο στην αντιμετώπιση, τρόπο επιθέσεως. Όταν δύο Η/Υ επικοινωνούν με το πρωτόκολλο TCP/IP ουσιαστικά ανταλλάσσουν αρχεία τα οποία ο αποστολέας "τεμαχίζει" σε μικρότερα κομμάτια τα οποία και αποστέλλει στον παραλήπτη ο οποίος τα συναρμολογεί, ανασυνθέτοντας το αρχικό αρχείο.

Τα πακέτα αυτά περιέχουν μια σειρά από στοιχεία ελέγχου μέσω των οποίων ο παραλήπτης ελέγχει αν τα δεδομένα έφτασαν σε καλή κατάσταση. Σε περίπτωση που διαπιστωθεί κάποιο πρόβλημα, τότε ο παραλήπτης επικοινωνεί με τον αποστολέα και του ζητάει να ξαναστείλει τα πακέτα που αλλοιώθηκαν κατά τη μεταφορά.

Εκμεταλλευόμενος αυτό το χαρακτηριστικό, ο επιτιθέμενος στέλνει συνεχώς πακέτα με λανθασμένα στοιχεία ελέγχου. Έτσι, υποχρεώνει τον παραλήπτη να σπαταλά υπολογιστική ισχύ και bandwidth, ζητώντας συνεχώς την επανάληψη της αποστολής τους.

Αν και έχουν βρεθεί κάποια αντίμετρα για τις επιθέσεις Fragmentation, κανένα από αυτά δεν είναι αρκετά αποτελεσματικό. Αν η επίθεση συνεχιστεί για μεγάλο χρονικό διάστημα ή αν γίνεται από μια γρήγορη γραμμή, τελικά το θύμα θα υποχρεωθεί να αποσυνδεθεί από το δίκτυο.

E-mail bombing

Αν και από πολλούς δεν θεωρείται ως Denial of Service Attack, το E-mail bombing είναι πολύ αποτελεσματικό όταν χρησιμοποιείται εναντίον υπολογιστών οι οποίοι διαχειρίζονται mail. Το μόνο που έχει να κάνει κανείς είναι να τους στείλει τόσα πολλά (σε μέγεθος και αριθμό) e-mail μηνύματα, ώστε ο φόρτος των εργασιών διαχείρισής τους να οδηγήσει το σύστημα σε κατάρρευση.

Port Flooding

Όλοι οι υπολογιστές διαθέτουν μια σειρά από λογικές πόρτες μέσω των οποίων μπορεί ένα άλλο μηχάνημα συνδέεται μαζί τους για να εκτελέσει μια σειρά από εργασίες. Για παράδειγμα, στο UNIX η πόρτα 25 χρησιμοποιείται από την υπηρεσία Sendmail.

Ο επιτιθέμενος μπορεί να γράψει ένα πρόγραμμα για οποιαδήποτε πόρτα, το οποίο θα ζητάει να ανοιχθούν μέσω αυτής όσο γίνεται περισσότερες (πλαστές φυσικά) συνδέσεις.

Όσο αυξάνει ο αριθμός των συνδέσεων, τόσο μεγαλύτερος γίνεται και ο φόρτος για το μηχάνημα το οποίο επιβαρύνεται όλο και περισσότερο μέχρι που τελικά "κολλάει" και διακόπτει τη λειτουργία του.

Σπάσιμο κωδικών (Password crackers)

Ένα password cracker είναι ένα πρόγραμμα το οποίο προσπαθεί να βρει το password κάποιου χρήστη ή το όνομα του χρήστη που αντιστοιχεί σε κάποια passwords που υπάρχουν αποθηκευμένα σε ένα αρχείο με passwords σε κάποιο υπολογιστή. Τα εργαλεία αυτά χρησιμοποιήθηκαν αρχικά από διαχειριστές συστημάτων ώστε να σιγουρευτούν ότι τα passwords που επέλεξαν οι χρήστες τους δεν μπορούσαν να εντοπιστούν εύκολα. Ωστόσο, χρησιμοποιήθηκαν επίσης κακόβουλα, για παράδειγμα για να αποκτήσουν πρόσβαση σε συστήματα όπου οι χρήστες είχαν εύκολα passwords όπως 'system' ή 'admin'.

Τα περισσότερα password crackers είτε προσπαθούν να ανακαλύψουν ένα password χρησιμοποιώντας μια μεγάλη λίστα λέξεων που επιλέγουν συχνά οι χρήστες ως passwords και δοκιμάζουν πολλά από αυτά είτε επιχειρούν να αποκτήσουν απευθείας πρόσβαση στο αρχείο των password.

Προγράμματα Υποκλοπής (Sniffers)

Αυτά είναι εργαλεία τα οποία υποκλέπτουν πακέτα δεδομένων τα οποία ταξιδεύουν στο δίκτυο. Υπάρχει μια νόμιμη χρήση τους από τους διαχειριστές συστημάτων καθώς μπορούν να χρησιμοποιηθούν για να εντοπίσουν αδυναμίες ενός δικτύου, για παράδειγμα μπορούν να χρησιμοποιηθούν για να εντοπίσουν σημεία πολύ έντονης κυκλοφορίας όπου μπορεί να υπάρχει πρόβλημα. Χρησιμοποιούνται επίσης από προγραμματιστές κατανεμημένων συστημάτων για να πάρουν μια ιδέα της αναμενόμενης κυκλοφορίας στο δίκτυο και να προσαρμόσουν την εφαρμογή τους σε αυτή.

Ωστόσο, έχουν συχνά επίσης χρησιμοποιηθεί για την υποκλοπή σημαντικών δεδομένων. Ενας εισβολέας μπορεί να εγκαταστήσει ένα sniffer σε ένα σημαντικό σημείο ενός δικτύου, για παράδειγμα σε μια πύλη και να διαβάσει τα μηνύματα καθώς αυτά περνάνε από αυτή. Ενας πετυχημένος sniffer μπορεί να εντοπίσει εκατοντάδες, αν όχι χιλιάδες passwords μέσα σε λίγες ώρες και να τα στείλει σε ένα απομακρυσμένο υπολογιστή από όπου κάποιος μη εξουσιοδοτημένος χρήστης θα μπορεί να τα χρησιμοποιήσει για να εισβάλει στο σύστημα.

Οι επιθέσεις με sniffer είναι παραδόξως όχι πολύ συνηθισμένες, ωστόσο όταν συμβαίνουν μπορεί να θέσουν σε κίνδυνο την ασφάλεια πολλών υπολογιστών και χρηστών. Για παράδειγμα, μια πρόσφατη επίθεση με sniffer είχε ως αποτέλεσμα 268 sites (όχι υπολογιστές αλλά sites!) να έχουν σοβαρά προβλήματα ασφάλειας.

l0phtCrack

Αυτό είναι ένα password cracker για Windows. Λειτουργεί με δυο τρόπους. Ο ένας είναι να ελέγχει τα passwords σε ένα δίκτυο χρησιμοποιώντας ένα αρχείο με passwords που έδωσε ο χρήστης. Ο δεύτερος τρόπος είναι να δοκιμάζει όλα τα δυνατά passwords χρησιμοποιώντας ένα περιορισμένο σύνολο χαρακτήρων: όλα τα γράμματα , κεφαλαία και πεζά καθώς και τα ψηφία από το 0 έως το 9.

Δούρειοι ίπποι (Trojan horses)

Ένας δούρειος ίππος είναι ένα κακόβουλο κομμάτι κώδικα το οποίο υπάρχει μέσα σε ένα κατά τα άλλα αθώο πρόγραμμα και το οποίο επιχειρεί να κάνει κάτι το οποίο ο χρήστης δεν περιμένει να κάνει. Για παράδειγμα, ένα ελεύθερης πρόσβασης πρόγραμμα το οποίο παρέχει σε ένα διαχειριστή συστημάτων πληροφορίες σχετικά με τη χρήση των αρχείων σε ένα δικτυακό σύστημα, αλλά το οποίο μετά από κάποια στιγμή υποκλέπτει πληροφορίες ή αλλάζει αρχεία είναι ένας δούρειος ίππος.

Οι δούρειοι ίπποι μπορούν να χρησιμοποιηθούν για διάφορους λόγους όπως την υποκλοπή passwords και άλλων πληροφοριών ή για να καταστρέψουν πόρους (π.χ. αρχεία) και να προκαλέσουν κατάρρευση ενός συστήματος.

Το κύριο πρόβλημα με τους δούρειους ίππους είναι ότι είναι πολύ δύσκολο να εντοπιστούν. Οι λόγοι είναι δυο: ο πρώτος είναι ότι συχνά παίρνουν τη μορφή ιδιαίτερα συνηθισμένων εργαλείων ή εργαλείων που απαιτούν την χειροκίνητη εγκατάσταση τους από το χρήστη. Ο δεύτερος λόγος για τον οποίο είναι δύσκολο να εντοπιστούν είναι ότι υπάρχουν σε κάποιο υπολογιστή με τη μορφή ενός μεταφρασμένου προγράμματος το οποίο είναι δύσκολο να ελεγχθεί τι ακριβώς κάνει.

Spoofing

Αυτός είναι ένας όρος ο οποίος χρησιμοποιείται για να περιγράψει την κατάσταση κατά την οποία ένας εισβολέας χρησιμοποιεί κάποιο υπολογιστή προσποιούμενος στο σύστημα

στο οποίο επιτίθεται ότι ο υπολογιστής που χρησιμοποιεί είναι κάποιος άλλος τον οποίο το σύστημα εμπιστεύεται και συνεπώς μπορεί να εκτελέσει λειτουργίες που κανονικά δεν θα επιτρεπόταν. Το spoofing δεν απαιτεί πολλές γνώσεις σχετικά με passwords και μεθόδους πιστοποίησης χρηστών όπως οι προηγούμενες μέθοδοι. Έχει σχέση μόνο με το να νομίζει το δίκτυο ότι ο υπολογιστής που χρησιμοποιεί ο εισβολέας είναι κάποιος άλλος υπολογιστής που το δίκτυο εμπιστεύεται.

Για να καταλάβουμε πως λειτουργεί το spoofing μπορούμε να δούμε μια συγκεκριμένη μορφή της τεχνικής αυτής που λέγεται **IP spoofing**. Αυτή η επίθεση χρησιμοποιεί το πρωτόκολλο TCP-IP για να παρακάμψει τις κανονικές λειτουργίες πιστοποίησης σε ένα σύστημα και γίνεται χρησιμοποιώντας έναν υπολογιστή που ισχυρίζεται πως έχει μια έμπιστη IP διεύθυνση.

Cookies

Ένα cookie είναι ένα αρχείο που τοποθετείται στον υπολογιστή ενός χρήστη από έναν browser και που συνήθως περιέχει στοιχεία συναλλαγών του χρήστη με συγκεκριμένους δικτυακούς τόπους. Για παράδειγμα, ένα cookie μπορεί να περιέχει στοιχεία για τα προϊόντα που επέλεξε και θα χρησιμοποιείται στο τέλος της συναλλαγής για να υπολογίσει το τελικό κόστος. Τέτοια cookies είναι παροδικά, ωστόσο υπάρχουν άλλα που είναι περισσότερο μόνιμα και μένουν στον δίσκο του χρήστη για πολύ καιρό. Μια συνηθισμένη χρήση τέτοιων cookies είναι να κρατάνε στοιχεία πιστωτικών καρτών για παράδειγμα ώστε να μην απαιτείται ο χρήστης να επανεισάγει τα στοιχεία του κάθε φορά που θέλει να κάνει μια συναλλαγή.

Τα cookies είναι όμως απειλή για προσωπικά σας στοιχεία τα οποία πιθανόν δεν θέλετε να είναι γνωστά σε άλλους: είναι σχετικά εύκολο να μαζέψει κανείς στοιχεία σχετικά με τις συνήθειες σας, τις προτιμήσεις σας κ.λπ. Αν αισθάνεστε άβολα με μια τέτοια κατάσταση υπάρχει απλή λύση: να απενεργοποιήσετε την επιλογή του browser σχετικά με την χρήση των cookies. Ωστόσο, αυτό μπορεί μερικές φορές να μην είναι βολικό καθώς πολλά sites θα απαιτούν τη χρήση των cookies.

Όταν ένας υπολογιστής ανοίγει μια σύνδεση με έναν άλλο χρησιμοποιώντας TCP-IP, ο πελάτης στέλνει ένα TCP πακέτο με έναν αρχικό ακέραιο αριθμό. Ο λαμβάνων

υπολογιστής (ο διακομιστής) επιστρέφει ένα πακέτο το οποίο περιλαμβάνει έναν άλλο ακέραιο, οι αριθμοί αυτοί είναι γνωστοί ως αριθμοί ακολουθίας. Επίσης στέλνει μια επιβεβαίωση η οποία είναι ο αριθμός ακολουθίας του πελάτη συν ένα. Ο πελάτης στη συνέχεια πρέπει να επιστρέψει μια επιβεβαίωση η οποία περιλαμβάνει τον αριθμό του ακολουθίας του διακομιστή συν ένα. Από τη στιγμή αυτή, ο πελάτης και ο διακομιστής μπαίνουν σε μια διαδικασία διαλόγου στην οποία ο πελάτης και ο διακομιστής στέλνουν πακέτα τα οποία περιέχουν αριθμούς ακολουθίας τους οποίους η άλλη πλευρά πρέπει να επιστρέψει για να πιστοποιήσει ότι είναι αυτή που ισχυρίζεται.

Οι αριθμοί ακολουθίας προσδιορίζονται από έναν αλγόριθμο του TCP-IP. Το κύριο πρόβλημα για να επιτευχθεί το IP spoofing είναι ότι ο εισβολέας θα πρέπει να γνωρίζει τους αριθμούς ακολουθιών που δημιούργησε και έστειλε ο διακομιστής κατά την αρχική εγκατάσταση της επικοινωνίας: ο διακομιστής θα λαμβάνει πακέτα από έναν υπολογιστή που ισχυρίζεται ότι έχει μια IP διεύθυνση αλλά τα πακέτα που στέλνει θα μεταφέρονται από το δίκτυο στον υπολογιστή που πραγματικά έχει την διεύθυνση αυτή και συνεπώς ο εισβολέας δεν θα παίρνει τις απαντήσεις για να δει τον αριθμό ακολουθίας που πρέπει να στείλει. Επειδή ο εισβολέας πρέπει να απαντήσει με πακέτα τα οποία περιέχουν τον κατάλληλο αριθμό ακολουθίας, κάθε πακέτο το οποίο θα λαμβάνεται στον διακομιστή και δεν περιέχει τον κατάλληλο αριθμό ακολουθίας θα θεωρείται ύποπτο και θα παρουσιάζεται το κατάλληλο μήνυμα.

Για να κάνει μια επίθεση IP spoofing, ο εισβολέας πρέπει να πετύχει τα εξής:

- Ο πραγματικός υπολογιστής που θα προσποιηθείτε ότι είστε πρέπει να είναι εκτός λειτουργίας. Αυτό συνήθως επιτυγχάνεται με μια επίθεση άρνησης υπηρεσίας.
- Ο υπολογιστής που θα χρησιμοποιηθεί για την επίθεση πρέπει να πάρει την IP διεύθυνση του υπολογιστή που θα προσποιηθεί ότι είναι.
- Ο υπολογιστής του εισβολέα, τότε, θα πρέπει να συνδεθεί με τον διακομιστή και να ξεκινήσει έναν διάλογο προσποιούμενος ότι είναι κάποιος άλλος υπολογιστής.
- Ο υπολογιστής του εισβολέα πρέπει με κάποιο τρόπο να ανακαλύψει τον αριθμό ακολουθίας που δημιούργησε ο διακομιστής. Αυτό είναι αρκετά δύσκολο αλλά όχι ακατόρθωτο. Σε μερικά τοπικά δίκτυα μπορεί επίσης να γίνει αρκετά εύκολα.

Μερικές φορές πάντως, οι αριθμοί ακολουθίας που φτιάχνει κάποιος ευάλωτος διακομιστής μπορούν να βρεθούν απλά με δοκιμή πολλών διαφορετικών αριθμών σε μια σειρά πολλών διαφορετικών προσπαθειών για σύνδεση. Συνήθως αφού κάποιος εισβολέας καταφέρει να μπει στο σύστημα, βρίσκει ένα πιο απλό και βολικό τρόπο για να συνεχίσει τη δραστηριότητα του, αλλάζοντας κάποιο password ή κάποια ρύθμιση στον διακομιστή κ.λπ. Αυτή είναι μια μόνο μορφή spoofing, υπάρχουν και άλλες.

Το **ARP spoofing** για παράδειγμα. Τα αρχικά ARP σημαίνουν Address Resolution Protocol, το πρωτόκολλο ARP είναι το κομμάτι του TCP-IP, που συνδέει φυσικές διευθύνσεις υπολογιστών (κάρτας δικτύου π.χ.) με IP διευθύνσεις. Το τμήμα του λειτουργικού συστήματος το οποίο αποθηκεύει τα απαραίτητα στοιχεία για να γίνεται η απαραίτητη μετατροπή διευθύνσεων είναι γνωστό ως **ARP cache**. Μια επίθεση ARP spoofing πραγματοποιείται μεταβάλλοντας την cache, ώστε η IP διεύθυνση ενός υπολογιστή που ο διακομιστής εμπιστεύεται στην πραγματικότητα θα ισοδυναμεί με τη φυσική διεύθυνση του υπολογιστή του εισβολέα.

Άλλη μια μορφή spoofing είναι το **DNS spoofing**. Αυτό είναι μια λιγότερο σημαντική απειλή από τα δυο προηγούμενα καθώς μπορεί σχετικά εύκολα να εντοπιστεί.. Ωστόσο, κάποιες επιθέσεις αυτού του είδους εξακολουθούν να συμβαίνουν ενίοτε. Σε μια επίθεση DNS spoofing μεταβάλλονται τα στοιχεία ενός DNS server ώστε να αντιστοιχεί το συμβολικό όνομα κάποιου υπολογιστή που εμπιστεύονται οι χρήστες στην IP διεύθυνση ενός υπολογιστή που χρησιμοποιείται από το άτομο που στήνει το κόλπο. Αυτό σημαίνει ότι οι υπολογιστές που θα προσπαθούν να συνδεθούν με τον υπολογιστή που εμπιστεύονται θα συνδέονται στην πραγματικότητα με κάποιον άλλο υπολογιστή, κατά τη διάρκεια της επικοινωνίας με τον οποίο θα μπορούσαν να αντληθούν σημαντικά δεδομένα. Για παράδειγμα θα μπορούσε ο χρήστης να δώσει τον αριθμό της πιστωτικής του κάρτας νομίζοντας πως πραγματικά η άλλη πλευρά θα το χρησιμοποιήσει απλά για να φέρει εις πέρας μια επιθυμητή συναλλαγή.

SYNFlooding

Το πρωτόκολλο SYN-ACK αποτελεί τη βάση κάθε έναρξης σύνδεσης μέσα στο Internet. Όταν ένας Η/Υ θέλει να συνδεθεί με έναν άλλο του αποστέλλει ένα πακέτο SYN στο οποίο

ο server απαντάει με ένα πακέτο ACK (acknowledge). Όταν ο Η/Υ που ζήτησε τη σύνδεση λάβει το ACK θεωρεί ότι η σύνδεση έχει ολοκληρωθεί και αρχίζει τη μετάδοση των δεδομένων. Σε μια επίθεση SYN Flooding ο επιτιθέμενος στέλνει συνεχώς πακέτα SYN αλλά όχι ACK.

Οι επιθέσεις Denial of Service ως μέσο εισβολής σε ένα σύστημα

Για τους περισσότερους ειδικούς, οι επιθέσεις DoS θεωρούνται πολύ ενοχλητικές, αλλά όχι θανάσιμα επικίνδυνες για ένα σύστημα. Ο επιτιθέμενος μπορεί ίσως να διακόψει τη λειτουργία ενός μηχανήματος για μερικές ώρες, αλλά δεν έχει τη δυνατότητα να αποκτήσει πρόσβαση σε αυτό και να τροποποιήσει δεδομένα σε κάποιο από τα άλλα μηχανήματα τα οποία μοιράζονται το ίδιο δίκτυο.

Δυστυχώς, αυτό δεν είναι αλήθεια. Μια καλή και δοκιμασμένη τεχνική (χρησιμοποιήθηκε από τον Kevin Mitnick για να εισβάλει στο σύστημα του διώκτη του κ. Tsutomu Shinomura) είναι η εισβολή σε ένα δίκτυο μέσω επίθεσης DoS σε έναν από τους servers του. Όταν το μηχάνημα αυτό πάψει να λειτουργεί, τότε ο επιτιθέμενος επικοινωνεί με άλλα μηχανήματα του ίδιου δικτύου "υποκρινόμενος" ότι τα πακέτα που στέλνει προέρχονται από το αχρηστεμένο και εκτός λειτουργίας πλέον μηχάνημα. Με τον τρόπο αυτό αυξάνονται σημαντικά οι πιθανότητες να επιτευχθεί πρόσβαση στα άλλα μηχανήματα του δικτύου, καθώς η εντολή πρόσβασης δεν δίνεται από έναν τρίτο, αλλά από μια έμπιστη πηγή (ένα μηχάνημα εντός του δικτύου).

Ανιχνευτές (Scanners)

Ένα scanner είναι ένα πρόγραμμα το οποίο ανιχνεύει αδυναμίες ασφάλεια σε υπολογιστικά συστήματα. Είναι λίγο αμφιλεγόμενο αν θα έπρεπε να μπει αυτό το θέμα σε μια ενότητα σχετική με επιθέσεις αφού τα προγράμματα αυτά αναπτύχθηκαν για να βοηθήσουν τους διαχειριστές συστημάτων να εντοπίσουν αδυναμίες. Ωστόσο κάποια από αυτά μπορούν να χρησιμοποιηθούν για να διερευνήσουν τρόπους εισβολής σε ένα δίκτυο.

SATAN

Πιθανότατα το πιο γνωστό scanner είναι το SATAN. Όταν κυκλοφόρησε το 1995 δημιούργησε σάλο καθώς ήταν το πρώτο πρόγραμμα το οποίο μπορούσε να εντοπίσει προβλήματα ενός δικτύου λειτουργώντας έξω από το δίκτυο. Υπήρχαν άλλοι δυο λόγοι για

τους οποίους δημιουργήθηκε τόσος θόρυβος για το πρόγραμμα αυτό: ο πρώτος είναι ότι όταν εντόπιζε κάποια αδυναμία εμφάνιζε και ένα ακατάλληλο και αρκετά αυστηρό μήνυμα σχετικά με τους κινδύνους της αδυναμίας αυτής και το δεύτερο ήταν το ίδιο το όνομα του προγράμματος, ήταν μια ένδειξη κακόβουλων προθέσεων εκ μέρους του εκάστοτε χρήστη του. Το SATAN δημιουργήθηκε από δυο σύμβουλους ασφαλείας, τον Dan Farmer και τον Weitse Venema, στο UNIX. Τα αρχικά SATAN σημαίνουν Security Administrator's Tool for Analyzing Networks.

Ένα **scanner** είναι ένα πρόγραμμα το οποίο ερευνά τα διάφορα στοιχεία ενός λειτουργικού συστήματος και ελέγχει αν είναι ασφαλή, για παράδειγμα μερικοί scanners για το UNIX μπορούν να ελέγχουν αν η δημοφιλής εφαρμογή *sendmail* είναι αρκετά ασφαλής για να αποτρέψει την εισβολή, άλλοι scanners μπορούν να ελέγξουν την ανθεκτικότητα ενός ftp server, για παράδειγμα βρίσκοντας αν ένα πολύ μεγάλο password θα μπλοκάρει τον ftp server. Τα scanners συνήθως είναι γραμμένα στο UNIX, αλλά τα τελευταία χρόνια έχουν δημιουργηθεί αντίστοιχα και για άλλα λειτουργικά συστήματα όπως τα Windows NT.

Επιθέσεις βασισμένες σε κενά ασφαλείας νέων τεχνολογιών

Υπάρχουν είδη επιθέσεων που εκμεταλλεύονται κενά ασφαλείας σε νέες τεχνολογίες. Συνήθως τεχνολογίες που έχουν σχέση με εφαρμογές απομακρυσμένων εφαρμογών είναι αρκετά ευάλωτες σε κενά ασφαλείας.

Υπάρχει ένας τόσο μεγάλος αριθμός σφαλμάτων ασφαλείας σε νέες τεχνολογίες που χρησιμοποιούνται στο Internet που αν αυτή η ενότητα ασχολούνταν με όλες αυτές θα είχε μέγεθος δυσανάλογο από τη σημασία της καθώς πολλά από τα λάθη αυτά έχουν ανακαλυφθεί και πολλά από αυτά διορθώθηκαν γρήγορα μετά την ανακάλυψη τους. Στην ενότητα αυτή θα επικεντρωθούμε στα προβλήματα ασφαλείας δυο συγκεκριμένων τεχνολογιών της Java και του Active X και θα δούμε παραδείγματα επιθέσεων βάσει αυτών.

Java

Όταν παρουσιάστηκε η Java η προσοχή του κόσμου εστιάστηκε στα applets. Αυτά είναι μικρά προγράμματα Java που εισάγονται σε HTML σελίδες και τα οποία εκτελούνται στον πελάτη.

Τα applets παρείχαν σημαντικές βελτιώσεις στην εμφάνιση των Web σελίδων: επέτρεπαν animations, image maps και επεξεργασία φορμών στον πελάτη. Ωστόσο, το μειονέκτημα ήταν ότι αποτελούσαν ένα μέσο με το οποίο έξυπνοι προγραμματιστές της Java θα μπορούσαν να θέσουν σε κίνδυνο την ασφάλεια ενός υπολογιστή που τρέχει applets. Πριν αναφερθούμε σε λεπτομέρειες για αυτό, πρέπει να αναφέρουμε ότι πολλά από τα αρχικά προβλήματα ασφαλείας της Java αντιμετωπίστηκαν γρήγορα με αλλαγές στον κώδικα της Java από την Sun Microsystems.

Υπήρχαν κάποια αρχικά προβλήματα με την Java τα οποία εντοπίστηκαν νωρίς από τους ερευνητές:

- Τα applets μπορούσαν να χρησιμοποιηθούν για επιθέσεις άρνησης υπηρεσιών σε συνδυασμό με συγκεκριμένους browsers.
- Κάποιος browser ήταν ευάλωτος σε επιθέσεις με applets τα οποία μπορούσαν να γράψουν αρχεία σε συστήματα που χρησιμοποιούσαν Windows 95.
- Υπήρχε κάποιο applet που προκαλούσε επανεκκίνηση των Windows 95.
- Σε κάποια έκδοση του Netscape Navigator ένα applet παγίδευε μια σελίδα που περιείχε κάποια φόρμα, να διαβάσει κάποια δεδομένα και να τα στείλει σε κάποιο απομακρυσμένο υπολογιστή.
- Μερικές εκδόσεις του Netscape Navigator και του Internet Explorer μπορούν να επιτρέψουν τον εντοπισμό IP διευθύνσεων σε ένα κλειστό δίκτυο από applets.

Πολλά από τα αρχικά προβλήματα της Java εξαλείφθηκαν, ωστόσο το δίδαγμα από τις αρχικές της ατέλειες ήταν πως κάθε νέα τεχνολογία θα έχει λάθη τα οποία μπορούν να θέσουν σοβαρά σε κίνδυνο την ασφάλεια.

Active X

Αυτή είναι μια τεχνολογία από την Microsoft που είναι παρόμοια με τα applets. Επειδή το Active X, όπως και τα applets της Java, είναι μια τεχνολογία η οποία αφορά εκτελέσιμο κώδικα ενσωματωμένο σε μια ιστοσελίδα έχει και αυτό πολλά από τα προβλήματα ασφαλείας που έχουν και τα applets. Για παράδειγμα, τον Ιανουάριο του 1996 δυο Γερμανοί έφτιαξαν ένα Active X αντικείμενο το οποίο μπορούσε να μεταφέρει χρήματα μεταξύ τραπεζικών λογαριασμών.

3.5 Ιοί

Οι ιοί είναι ένα είδος κακόβουλα γραμμένου κώδικα που θέτει σε κίνδυνο την ασφαλή λειτουργία του συστήματος και μπορούν να χρησιμοποιηθούν για μια ποικιλία διαφορετικών επιθέσεων. Περιγράφονται ξεχωριστά εδώ καθώς απαιτούν αρκετά υψηλό επίπεδο τεχνικών γνώσεων. Οι συνηθισμένες επιθέσεις άρνησης υπηρεσιών είναι απλές και όχι ιδιαίτερα εξεζητημένες ενώ η επίθεση με ιό απαιτεί μεγαλύτερο βαθμό τεχνικών γνώσεων.

Ένας **ιός** είναι ένα πρόγραμμα, το οποίο επισυνάπτει τον εαυτό του σε αρχεία τα οποία υπάρχουν στον υπολογιστή - μια διαδικασία που είναι γνωστή ως **μόλυνση.** Αφού ένας ιός εγκατασταθεί σε έναν υπολογιστή, μπορεί να αντιγράψει τον εαυτό του και σε άλλα αρχεία στον υπολογιστή.

Κατηγορίες ιών

Υπάρχουν τρεις κύριες κατηγορίες ιών: εκτελέσιμοι ιοί, ιοί δεδομένων και ιοί οδηγών συσκευών. Ένας **εκτελέσιμος ιός** είναι ένας ιός ο οποίος προστίθεται σε ένα εκτελέσιμο αρχείο, το οποίο όταν εκτελεστεί θα έχει ως αποτέλεσμα να εκτελεστεί και ο κώδικας του ιού. Αυτός ο κώδικας στη συνέχεια θα κάνει κάποια κακόβουλη ενέργεια όπως να διαγράψει κάποια σημαντικά αρχεία. Ένας **ιός δεδομένων** είναι ένας ιός ο οποίος μολύνει ένα αρχείο που περιέχει δεδομένα αντί για εκτελέσιμο κώδικα. Συχνά τα δεδομένα αυτά είναι συνδεδεμένα με κάποιο πρόγραμμα, το οποίο χρειάζεται τα δεδομένα για να εκτελέσει τη λειτουργία του.

Για παράδειγμα, πολλά προγράμματα χρειάζονται ένα **startup αρχείο** το οποίο αρχικοποιεί το πρόγραμμα και ορίζει βασικές παραμέτρους της λειτουργίας του. Ένας ιός δεδομένων θα μπορούσε να μολύνει ένα τέτοιο αρχείο και να αλλάξει τα δεδομένα του, ώστε το πρόγραμμα δεν θα μπορεί να λειτουργήσει ή η λειτουργία του θα τεθεί σε κίνδυνο. Ένας άλλος τύπος ιού δεδομένων θα μπορούσε να προσθέσει μια καταχώρηση σε ένα αρχείο με password κι έτσι θα επέτρεπε πρόσβαση σε ένα εισβολέα.

Άλλο ένα παράδειγμα, είναι αυτό ενός ιού δεδομένων για έναν επεξεργαστή κειμένου, που θα μπορούσε επίσης να γραφτεί και εύκολα και που θα μπορούσε να αλλάζει τα περιεχόμενα κάθε αρχείου που ανοίγει από τον επεξεργαστή κειμένου ή ακόμη χειρότερα να το σβήνει. Μια τρίτη κατηγορία είναι οι **ιοί οδηγών συσκευών**. Αυτοί επηρεάζουν τους οδηγούς συσκευών ενός λειτουργικού συστήματος που χρησιμοποιούνται για τον χειρισμό διαφόρων στοιχείων του υπολογιστή, όπως ο δίσκος. Ευτυχώς αυτός ο τύπος ιού εμφανιζόταν κυρίως σε παλιότερα λειτουργικά συστήματα όπως το MS-DOS.

Υπάρχει επίσης ένας τρόπος κατηγοριοποίησης των ιών βάσει του τρόπου που χρησιμοποιούν για να κρύψουν την παρουσία τους στον υπολογιστή. Βάσει του κριτηρίου αυτού υπάρχουν δυο ειδών ιοί, οι **stealth ιοί** και οι **πολυμορφικοί ιοί**. Πριν περιγράψουμε αυτούς τους δυο τύπους ιών είναι χρήσιμο να μιλήσουμε για το πώς τα προγράμματα εντοπισμού ιών λειτουργούν. Τα προγράμματα αυτά λειτουργούν ελέγχοντας τα αρχεία που υπάρχουν αποθηκευμένα ψάχνοντας σε αυτά είτε γνωστούς ιούς είτε αλλαγές σε σημαντικά αρχεία, π.χ. αλλαγές σε αρχεία κώδικα του λειτουργικού συστήματος παρότι δεν υπήρξε άμεση αναβάθμιση του.

Οι ιοί Stealth κρύβουν την παρουσία τους χρησιμοποιώντας διάφορες τεχνικές, για παράδειγμα αλλάζοντας τις ημερομηνίες αλλαγής ή το πραγματικό μέγεθος των αρχείων ώστε το πρόγραμμα εντοπισμού ιών να μην μπορεί να εντοπίσει κάποια αλλαγή και να μην θεωρεί αυτά τα αρχεία ύποπτα, ενώ στην πραγματικότητα είναι μολυσμένα.

Οι πολυμορφικοί ιοί μπορούν να αλλάζουν συχνά τα χαρακτηριστικά τους – για παράδειγμα το μέγεθος τους - μια διαδικασία που είναι γνωστή ως **μετάλλαξη**. Αυτό σημαίνει ότι είναι πολύ πιο δύσκολο για τα προγράμματα εντοπισμού ιών να τους εντοπίσουν βασιζόμενοι μόνο στα γνωστά χαρακτηριστικά τους.

Δημιουργία ιών

Υπάρχουν διάφοροι τρόποι δημιουργίας ιών. Μπορούν να δημιουργηθούν από την αρχή χρησιμοποιώντας μια γλώσσα όπως η C ή assembly. Χρησιμοποιούνται τέτοιες γλώσσες γιατί πρέπει ο κώδικας του ιού να είναι όσο το δυνατόν μικρότερος για να μπορεί να αποφεύγει τον εντοπισμό από προγράμματα anti-virus.Οι γλώσσες αυτές επίσης παρέχουν αρκετές δυνατότητες σχετικά χαμηλού επιπέδου που δεν προσφέρονται από άλλες γλώσσες όπως κάποιες λειτουργίες εισόδου / εξόδου. Υπάρχουν επίσης κάποια εργαλεία κατασκευής ιών τα οποία μπορούν να βρεθούν σε διάφορα μέρη στο internet.

Ένας τυπικός ιός

Θα συμπληρώσουμε την ενότητα των ιών εξετάζοντας τη λειτουργία ενός συγκεκριμένου ιού βλέποντας έτσι πόσο πονηροί μπορεί να είναι οι κατασκευαστές ιών. Ο ιός αυτός είναι γνωστός σας ιός οικογένειας και φίλων. Χρησιμοποιεί επισυναπτόμενα αρχεία σε e-mails για να διαδοθεί ωστόσο το κάνει με ένα ιδιαίτερα πονηρό τρόπο.

Υπάρχει ένας ιδιαίτερα μεγάλος αριθμός ιών (εκτελέσιμων ιών ή ιών δεδομένων) που διαδόθηκαν μέσω e-mail. Το μόνο που πρέπει να κάνει ο παραλήπτης ενός μολυσμένου e-mail είναι να ανοίξει ένα επισυναπτόμενο αρχείο. Το αποτέλεσμα θα είναι να εκτελεστεί ένα πρόγραμμα που θα μολύνει τον υπολογιστή του παραλήπτη. Συχνά τέτοια e-mail έχουν μια απλή επικεφαλίδα όπως 'Γεια' ή 'Πως πάει;' που ίσως αποτελεί ένδειξη ότι ο αποστολέας είναι γνωστός του παραλήπτη και το αρχείο πιθανότατα μπορεί με ασφάλεια να ανοιχθεί. Μια άλλη ανάλογη μέθοδος είναι μέσω ηλεκτρονικών ευχετήριων καρτών, όπου τα ύποπτα επισυναπτόμενα αρχεία μπορεί να φαίνονται σαν ευχετήριες κάρτες.

Υπήρξε έντονη δημοσιότητα σχετικά με τη διάδοση ιών μέσω e-mail και σαν συνέπεια πολλοί χρήστες του Internet είναι διστακτικοί να ανοίξουν επισυναπτόμενα αρχεία από χρήστες που δεν γνωρίζουν. Αυτό είναι το ιδιαίτερο σημείο στο οποίο οι ιοί του τύπου "φίλοι και οικογένεια" αποδεικνύονται τόσο ύπουλοι. Ο ιός μπορεί να μολύνει κάποιον υπολογιστή χρησιμοποιώντας κάποιο άλλο μέσο και όχι e-mail, για παράδειγμα μπορεί να μολύνει κάποιο υπολογιστή όταν ο χρήστης του κατεβάζει κάποιο δωρεάν πρόγραμμα από ένα ftp site. Ανεξάρτητα από τον τρόπο με τον οποίο έγινε η μόλυνση, ο ιός στη συνέχεια θα δει τη λίστα διευθύνσεων του χρήστη και θα στείλει e-mails σε όλα τα άτομα που είναι

καταχωρημένα στη λίστα διευθύνσεων του χρήστη προσποιούμενος πως είναι ο χρήστης του υπολογιστή. Το e-mail που στέλνεται θα περιέχει και ένα επισυναπτόμενο αρχείο.

Οι χρήστες οι οποίοι δεν θα άνοιγαν κάποιο επισυναπτόμενο αρχείο από άγνωστο αποστολέα κατά πάσα πιθανότητα θα ανοίξουν το αρχείο που προέρχεται κατά τα φαινόμενα από κάποιον που γνωρίζουν. Συνεπώς ο ιός θα μολύνει όλους τους υπολογιστές των ατόμων που θα ανοίξουν το αρχείο και θα στείλει ακόμα περισσότερα e-mails χρησιμοποιώντας το νέο κατάλογο διευθύνσεων κ.ο.κ.

3.6 Τρόποι με τους οποίους μπορεί ένας ιός να μεταφερθεί στον υπολογιστή σας

Οι ιοί εξαπλώνονται με πολλούς τρόπους:

- Με μεταφορτώσεις (downloads) από το διαδίκτυο.
- Με πειρατικό λογισμικό.
- Με ανταλλαγή δισκετών.
- Με επισυνάψεις του ηλεκτρονικού ταχυδρομείου και σε μηνύματα ηλεκτρονικού ταχυδρομείου.
- Με έγγραφα. Οι Macro-viruses που περιγράφονται παραπάνω, μπορεί να κρύβονται σε καθημερινά έγγραφα κειμένου, υπολογιστικά φύλλα και παρουσιάσεις.

Οι ιοί μπορεί να εμπεριέχονται σε τέτοιες εφαρμογές. Μόλις μεταφορτωθούν και εκτελεστούν οι εφαρμογές, ο ιός φορτώνεται στη μνήμη του υπολογιστή και μολύνει άλλα προγράμματα στον υπολογιστή σας. Αυτοί οι ιοί μπορούν να κάνουν πολύ ανεπιθύμητες λειτουργίες όπως η αποστολή μολυσμένων μηνυμάτων ηλεκτρονικού ταχυδρομείου σε διευθύνσεις που βρίσκονται στο βιβλίο διευθύνσεών σας. Μερικοί ιοί μπορούν ακόμα και να κλείσουν τον υπολογιστή σας και να εμποδίζουν την επανεκκίνηση του λειτουργικού σας συστήματος.

Γι' αυτό είναι πολύ σημαντικό να εγκαθιστάτε λογισμικό και ανοικτά αρχεία από αξιόπιστες πηγές. Αν δεν είστε σίγουρος για κάτι που κατεβάσατε από το διαδίκτυο ή λάβατε μέσω ηλεκτρονικού ταχυδρομείου, θα είναι καλύτερο να μην το ανοίξετε ή να μην το εκτελέσετε.

3.7 Τρόποι με τους οποίους μπορούμε να αντιμετωπίσουμε έναν ιό

Αντι-ιικό λογισμικό

Το λογισμικό αυτό σαρώνει τα αρχεία για να εντοπίσει τμήματα κώδικα, που ονομάζονται υπογραφές (signatures), τα οποία τα αναγνωρίζει ως μέρη ενός ιού. Μία υπογραφή είναι μια διακριτική σειρά εντολών, οι οποίες βρίσκονται μόνο στο σχετικό ιό. Γι' αυτό το σάρωμα εμπλέκει και την ανάλυση του κώδικα των προγραμμάτων στην έρευνα για υπογραφές που εμπεριέχονται σε νόμιμα προγράμματα.

Η ενημέρωση του αντι-ιικού λογισμικού περιλαμβάνει κυρίως την ενημέρωση των αρχείων των υπογραφών. Αυτό θα πρέπει να γίνεται τακτικά, όσο το δυνατόν. Πολύ περισσότερο μάλιστα, όταν λαμβάνετε συχνά αρχεία από εξωτερικές πηγές. Αυτό καθεαυτό το αντι-ιικό πρόγραμμα θα ενημερώνεται κατά καιρούς. Αυτές οι ενημερώσεις θα περιλαμβάνουν πρόσθετα χαρακτηριστικά και βελτιωμένες μεθόδους σάρωσης.

Η ενημέρωση του αντι-ιικού και η σάρωση των περιεχομένων ενός υπολογιστή σε τακτά διαστήματα, θα σας παρέχουν ένα καλό μέτρο προστασίας, σε περίπτωση που ο υπολογιστής σας μολυνθεί. Καλό αντι-ιικό λογισμικό μπορεί επίσης να μπλοκάρει την είσοδο ιών στο σύστημά σας.

Άλλα μέτρα προστασίας

Υπάρχει πλήθος προστατευτικών μέτρων που μπορείτε να λάβετε προκειμένου να προστατευτείτε από ιούς:

- Να εγκαταστήσετε ένα καλό αντι-ιικό λογισμικό και να το ενημερώνετε τακτικά, για παράδειγμα τουλάχιστον μια φορά το μήνα ή καλύτερα μία φορά την εβδομάδα. Πάντα όμως να θυμάστε, ότι ένα αντι-ιικό λογισμικό δεν είναι τέλειο. Δεν μπορεί να είναι το μοναδικό μέτρο προστασίας.
- Να ελέγχετε όλες τις δισκέτες προτού τις διαβάσετε.
- Ενεργοποιήστε τη λειτουργία αυτόματης προστασίας του αντι-ιικού λογισμικού, για να ελέγχονται όλα τα μηνύματα ηλεκτρονικού ταχυδρομείου.
- Να είστε επιφυλακτικοί με μηνύματα ηλεκτρονικού ταχυδρομείου από άγνωστους αποστολείς, ιδίως αν περιέχουν επισυναπτόμενα. Ορισμένοι,

πολύ προσεκτικοί χρήστες διαγράφουν μηνύματα ηλεκτρονικού ταχυδρομείου για τα οποία δεν είναι σίγουροι, χωρίς να τα ανοίξουν.

- Χρησιμοποιήστε έναν ISP που ελέγχει μηνύματα ηλεκτρονικού ταχυδρομείου πριν αυτά φτάσουν στον παραλήπτη.
- Μη μεταφορτώνετε λογισμικό από άγνωστους ιστότοπους.
- Προσέχετε όταν χρησιμοποιείτε δισκέτες από άγνωστες πηγές.
- Μην εγκαθιστάτε πειρατικό λογισμικό.

Η σημασία της «απολύμανσης» αρχείων

Όταν εντοπιστεί ένας ιός, το λογισμικό θα επιχειρήσει να τον απομακρύνει. Αυτό ονομάζεται **καθαρισμός** ή **απολύμανση**. Η απολύμανση περιλαμβάνει απομάκρυνση του κώδικα του ιού από το αρχείο στο οποίο είναι επισύναψη.

Μερικές φορές συμβαίνει το σύστημα να εντοπίζει ιούς αλλά να μην μπορεί να τους αποβάλει. Σε αυτή την περίπτωση, συχνά θα δίνεται η επιλογή της **διαγραφής** ή της **απομόνωσης** του μολυσμένου αρχείου. Μία μελλοντική ενημέρωση του λογισμικού μπορεί να είναι ικανή να απομακρύνει τον ιό. Αν μπορεί να γίνει αυτό, παύει η απομόνωση.

ΚΕΦΑΛΑΙΟ 4°

Windows VS Linux

Αναμφίβολα η πλέον φανατική αντιπαράθεση στο χώρο της πληροφορικής έχει να κάνει με τον πόλεμο των λειτουργικών συστημάτων. Η κόντρα Windows-Linux που κλιμακώνεται τα τελευταία χρόνια, έχει αγγίξει τα όρια του «οπαδισμού» με συχνά ακραίες αντιπαραθέσεις, οι οποίες κάνουν τις αντίστοιχες παλαιότερες κόντρες Amiga-Atari και PC-Mac να μοιάζουν με αθώες διαλέξεις φιλολογικού ενδιαφέροντος.

[5] 4.1 Από το 0 έως τα... Windows

Σύμφωνα με την ιστορία, το Σεπτέμβριο του 1982 τα PCs μπαίνουν σε παραθυρικό περιβάλλον με το VisiOn της VisiCorp, το οποίο όμως «εξαφανίζεται» κάτω από το βάρος των Windows 1.0 δύο χρόνια μετά. Το τελευταίο δεν είναι παρά ένα στοιχειώδες γραφικό περιβάλλον στο παλιό καλό MS-DOS (και αρκετά παρωχημένο τόσο προς την εμφάνιση όσο και ως προς τη λειτουργία σε σχέση με το παραθυρικό OS του Macintosh). Έως το 1990, έτος κυκλοφορίας των Windows 3.0, οι χρήστες των PCs παραμένουν λίγο πολύ στην «πρωτόγονη» εποχή της command line του MS-DOS.

Πλέον όμως τα πράγματα έχουν ωριμάσει, το ίδιο και το γραφικό λειτουργικό της Microsoft. Η ευρεία υποστήριξη καταρχάς της ίδιας της Microsoft κυρίως με το Office καθιστά τα Windows (3.0 και αργότερα τα 3.11 for Workgroups) στάνταρ στις οθόνες των PCs τόσο στο γραφείο όσο και στο σπίτι. Η σημερινή κατάσταση διαμορφώνεται με τα Windows XP, οπότε ουσιαστικά παύουν να αποτελούν ένα πρόγραμμα με γραφικό περιβάλλον που τρέχει πάνω στο MS-DOS. Σημαίνουν επίσης την είσοδο στο multitasking. Τα Windows από το 1995 έως σήμερα προέρχονται από δύο γραμμές: τη Win9x (Win95/98/Me) και τη WinNT (Win NT/2000/XP). Έως τα Windows NT το λειτουργικό της Microsoft λειτουργούσε ουσιαστικά ως κέλυφος (shell) στο MS-DOS, διατηρώντας τους τεχνικούς περιορισμούς του 30χρονου συστήματος (διαχείριση μνήμης κ.α.). Τα

[5] http://forum.ubuntu-gr.org/viewforum.php?f=60&http

Windows NT, με τον εντελώς νέο πυρήνα τους αρχίζουν να ξεφεύγουν από τα δεσμά του MS-DOS, κάτι που ολοκληρώνεται στη συνέχεια με τα Windows 2000 και τα Windows XP. Με την πρόσφατη εμφάνιση των Windows XP Media Center η Microsoft μπαίνει και στο χώρο της οικιακής ψυχαγωγίας έχοντας ως βάση τα Windows XP, ενώ πλέον έχουμε περάσει στην επόμενη γενιά με ονομασία Vista.

4.2 Από το 0 έως το... Linux

Πίσω από το Linux κρύβεται το παλιό, καλό Unix. Ο δημιουργός του, Linus Torvalds, προέρχεται από τη χώρα των «χιλίων λιμνών». Εργαζόμενος ως τεχνικός υπολογιστών, ο Torvalds επιχειρεί το 1991 να δημιουργήσει έναν Unix-Κλώνο στο PC του. Όχι μόνο κατάφερε να φτιάξει το εναλλακτικό OS, αλλά έσπασε τον πάγο για το ελεύθερο λογισμικό, δημιουργώντας μια νέα σχολή που αγγίζει τα όρια του... φιλοσοφικού ρεύματος. Καθώς ο πυρήνας έχει τις ρίζες του στο 1960 και σχεδιάζεται πάνω σε ένα 386 PC, το Linux γίνεται διάσημο για την λειτουργικότητά του ακόμα και σε πολύ «αδύναμα» συστήματα. Πέρα όμως από αυτά, είναι συμβατό με μία τεράστια γκάμα συστημάτων, από Z series mainframes της IBM έως και μίνι υπολογιστές με επεξεργαστές ARM.

Η τελική μορφή του λειτουργικού παρουσιάζει διαφοροποιήσεις ανάλογα με τις διανομές του, σε σημεία όπως το περιβάλλον χρήσης, το ενσωματωμένο software και η διαδικασία εγκατάστασης. Ο πυρήνας παραμένει ο ίδιος, ενώ υπάρχουν εκδοχές για desktops και servers. Τα KDE και GNOME περιβάλλοντα παραπέμπουν στα Windows. Μάλιστα σε δύο περιπτώσεις (Lindows και XPde) η εμφάνιση είναι σχεδόν όμοια με αυτή των Windows.

4.3 Το «One-on-One» των λειτουργικών συστημάτων

Εγκατάσταση

Τα Windows XP απαιτούν «καθαρή» εγκατάσταση, κάτι που σημαίνει format στο σκληρό δίσκο και εγκατάσταση σε αυτόν (ή σε partition αυτού) μόνο του λειτουργικού. Η είναι εξαιρετικά απλή και εύκολη (απλά κάποια κλικ του ποντικιού).

Η εγκατάσταση του Linux εξαρτάται από τη διανομή και συνήθως απαιτεί (όπως και στα Windows) μισή με μία ώρα. Παρόλο που στις περισσότερες διανομές η διαδικασία έχει

αυτοματοποιηθεί σημαντικά, χρειάζεται κάποια εξοικείωση, καθώς δεν λείπουν οι χειροκίνητες ρυθμίσεις τη στιγμή μάλιστα που η ορολογία είναι πιο στρυφνή και απευθύνεται σε γνώστες. Η εγκατάσταση σε «καθαρό» σύστημα (χωρίς άλλο λειτουργικό) είναι σαφώς πιο εύκολη. Άλλη μια διαφοροποίηση σε σχέση με τα Windows είναι το ότι σε κάποιες εκδοχές του, το Linux τρέχει μέσα από το CD (π.χ. Knoppix). Σε αυτή την περίπτωση δεν χρειάζεται εγκατάσταση στο σκληρό δίσκο.

Σταθερότητα

Εδώ τα Windows έχουν κακή ιστορία. Σαφώς και τα Windows XP είναι θεαματικά πιο σταθερά σε σχέση με τα Windows 98, όμως η πολιτική της Microsoft και το παιχνίδι του marketing έχουν αφήσει ουκ ολίγα προβλήματα ακάλυπτα (δεν ξεχνάμε τις μπλε οθόνες οι οποίες δεν μας έχουν εγκαταλείψει τελείως). Αφενός η βιασύνη να κυκλοφορήσει γρήγορα το προϊόν και αφετέρου οι εταιρικές διαδικασίες δημιουργίας patches συχνά οδηγούν στην παρουσίαση δυσλειτουργιών, αλλά και στην καθυστέρηση της επίλυσης τους.

Αποτελεί γενικότερη πεποίθηση ότι το Linux παρουσιάζει λιγότερες δυσλειτουργίες σε σχέση με τα Windows, κάτι που σε γενικές γραμμές είναι σωστό. Το σίγουρο είναι ότι επειδή το Linux υποστηρίζεται από μια τεράστια κοινότητα (έξω από το παιχνίδι του marketing), τα όποια προβλήματα παρουσιάζουν οι διανομές του επιλύονται ταχύτερα. Το γεγονός και μόνο ότι ο κώδικας είναι ανοιχτός δίνει τη δυνατότητα σε πολλούς χρήστες να εντοπίζουν και να διορθώνουν τις δυσλειτουργίες του.

Interface

Το interface των Windows XP αποτελεί σημαντική βελτίωση σε σχέση με τα Windows 98. Δημιουργημένο για τους πιο αρχάριους είναι περισσότερο εργονομικό και «φαντεζί». Στον τομέα της εργονομίας παραμένουν κάποιες ελλείψεις (κυρίως εξαιτίας των διάσπαρτων μενού και των κρυφών δυνατοτήτων), αλλά γενικότερα η φιλικότητα είναι επαρκείς. Για τους πιο παλιούς η command line παραμένει και συχνά απαιτείται στις πιο ειδικές διαδικασίες.

Το interface είναι ένα ισχυρό όπλο του Linux. Όπως αναφέραμε έχουμε να κάνουμε με ένα σταθερό πυρήνα Unix και με πολλαπλά περιβάλλοντα. Τα δύο πιο καθιερωμένα GUI είναι το KDE και το GNOME, που λίγο-πολύ θυμίζουν τα Windows (π.χ. το κουμπί Start,

ο κάδος ανακύκλωσης κ.α.). Από την άλλη μεριά το GUI μπορεί κάλλιστα να απουσιάζει, ενώ ανάλογα με την ισχύ του μηχανήματος όπου εγκαθίσταται το Linux μπορούν να χρησιμοποιηθούν πιο «light» GUI. Φυσικά η command line διατηρεί τον πρωταρχικό ρόλο της στον έλεγχο του λειτουργικού.

Πολλαπλοί χρήστες

Έπρεπε να φτάσουν τα Windows 2000/XP για να αποκαλέσουμε τα Windows «πολυχρηστικά», καθώς μέχρι τότε ο όρος user ήταν περισσότερο σχήμα λόγου (στα Windows 98 ήταν εξαιρετικά εύκολη η παράκαμψη του παραθύρου εισόδου στο λειτουργικό σύστημα με πληκτρολόγηση password). Το σύστημα του administrator και των επιμέρους χρηστών με συγκεκριμένους κανόνες χρήσης είναι αρκετά εκλεπτυσμένο, αν και απαιτεί κάποιο χρόνο εξοικείωσης, δεν παρέχει ωστόσο απόλυτη ασφάλεια.

Κάθε διανομή Linux διαθέτει στάνταρ δυνατότητα «πολυχρησίας». Μπορεί η μέθοδος να φαίνεται «πρωτόγονη» σε σχέση με τα Windows XP, καθώς ο καθορισμός των χρηστών γίνεται ουσιαστικά βάση των περιοχών του directory στις οποίες έχουν πρόσβαση, όμως το πιο σοβαρό σύστημα διαχείρισης προστατεύει τον υπολογιστή από πιθανές βλάβες ή ιούς. Μια επιπλέον διαφοροποίηση έναντι των Windows έχει να κάνει με τον καθορισμό ομάδων χρηστών στο Linux.

Ασφάλεια

Ομολογουμένως τα Windows υστερούν έναντι του Linux στο θέμα της ασφάλειας για διάφορους λόγους. Ο κυριότερος είναι ότι αφενός ο σχεδιασμός τους αφήνει ανοιχτές πολλές «πόρτες» για την εισβολή ιών, worms κ.λπ. και αφετέρου η διείσδυσή τους είναι ακόμα μεγαλύτερη, άρα οι χρήστες τους γίνονται πιο εύκολα στόχοι hackers, crackers και συναφών… επιδρομέων. Ειδικά η έκδοση server έχει αποδειχθεί πολύ πιο ευπαθής από τις αντίστοιχες πλατφόρμες του Linux (π.χ. RedHat, Slackware, Suse).

Τέλος όταν παρουσιάζονται κενά, η Microsoft δεν αντιδρά το ίδιο γρήγορα με την ενεργή παγκόσμια κοινότητα του Linux. Στον τομέα ασφάλεια το Linux βασιλεύει, καθώς συγκρινόμενο με τα Windows μπορεί να θεωρηθεί virus free. Ο κώδικας και γενικότερα ο σχεδιασμός του είναι συμπαγείς και δύσκολα αφήνουν ανοίγματα στους κάθε λογής εισβολείς. Ας σκεφτούμε μονάχα ότι οι Apache Servers που βασίζονται στο Linux είναι

περισσότεροι, ακόμη και μέσα από αυτούς προσβάλλονται πολύ περισσότερα συστήματα Windows. Υπάρχει μάλιστα η πεποίθηση ότι ακριβώς επειδή ο κώδικας του Linux είναι ανοιχτός, δεν είναι πρόκληση για τους hackers, οι οποίοι προτιμούν τα «δύσκολα» του «κλειδωμένου» κώδικα των Windows.

Software

Ένα από τα μεγαλύτερα πλεονεκτήματα των Windows, καθώς το λειτουργικό της Microsoft τυγχάνει τεράστιας υποστήριξης. Οι διαδικασίες εγκατάστασης είναι παντού λίγο πολύ ίδιες και σε μεγάλο βαθμό πλήρως αυτοματοποιημένες, απλούστερες ακόμα και για τον πλέον αρχάριο χρήστη. Εδώ βέβαια τίθεται ακόμα ένα ζήτημα μονοπωλίου, καθώς η Microsoft έχει κατορθώσει σχεδόν σε όλους τους τομείς του software που παράγει (σουίτες Office, web browsers κ.α.) να επιβληθεί (ας μην ξεχνάμε άλλωστε, ότι ο περίφημος δικαστικός αγώνας ξεκίνησε με αφορμή της πολιτική προώθησης του Internet Explorer). Παραμένει βέβαια το μειονέκτημα του αυξημένου κόστους αγοράς, αν και η open source κοινότητα παρέχει αρκετές δελεαστικές προτάσεις και για το λειτουργικό της Microsoft.

Παρά τη ραγδαία ανάπτυξη της open source κοινότητας και την αυξανόμενη υποστήριξη του Linux από το εμπορικό λογισμικό, στον τομέα του software το Linux παραμένει υποδεέστερο έναντι των Windows. Βέβαια για μια τυπική έως και απαιτητική χρήση γραφείου, όχι μόνο δεν λείπει τίποτα από το Linux, αλλά και δεν είναι λίγες οι διανομές που παρέχει ένα υπερεπαρκές πακέτο εφαρμογών. Το δε open source λογισμικό διατηρεί τα πλεονεκτήματα του πολύ χαμηλού έως μηδενικού κόστους απόκτησης και χρήσης, αν και στις περισσότερες περιπτώσεις τα ίδια προγράμματα παρέχονται και για Windows. Εκεί όπου χρειάζεται ακόμα δουλειά είναι η φιλικότητα κατά την εγκατάσταση, αφού εδώ σημειώνονται σημαντικές διαφοροποιήσεις ανάλογα με τη διανομή, ενώ παράλληλα η διαδικασία δεν είναι το ίδιο αυτόματη όπως στα Windows.

Hardware

Χωρίς αμφιβολία τα Windows εγγυώνται την πλέων ομαλή συνύπαρξη με τη μεγαλύτερη γκάμα περιφερειακών, απλούστατα λόγο της μακροχρόνιας επικράτησής τους που αναγκάζει τους κατασκευαστές να σχεδιάζουν drivers πρωτίστως για το συγκεκριμένο λειτουργικό σύστημα. Το σύστημα plug'n'play το οποίο καθιερώθηκε από τα Windows 95

και παραμένει μέχρι σήμερα εξυπηρετεί τον αρχάριο χρήστη, καθώς η εγκατάσταση των περισσότερων συσκευών γίνεται αυτόματα χωρίς σχεδόν την παραμικρή παρέμβαση εκ μέρους τους. Βέβαια πρέπει να σημειωθεί ότι με το πέρασμα από τη μία έκδοση Windows στην άλλη, αλλάζουν και οι drivers, κάτι που δεν ισχύει για το Linux.

Αν και έχουν αλλάξει πολλά σε σχέση με τα προηγούμενα χρόνια, η συνεργασία του Linux με τα διάφορα περιφερειακά απέχει πολύ από το να χαρακτηριστεί απρόσκοπτη. Ειδικά σε ότι αναφορά τους μικρότερους κατασκευαστές η ενδεχόμενη απουσία υποστήριξης μόνο αμελητέα δεν μπορεί να θεωρηθεί (ευτυχώς η κοινότητα του Linux καλύπτει σε μεγάλο βαθμό τα κενά). Ακόμα όμως και με τα chipsets καρτών γραφικών παρατηρούνται προβλήματα.

Τεχνολογίες όπως το WiFi και το Bluetooth, αλλά και όλη η κατηγορία των laptops, τυγχάνουν περισσότερο θεωρητικής παρά πρακτικής υποστήριξης. Το Linux παίρνει το αίμα του πίσω χάρη στην εγγενή υποστήριξη που παρέχει σε μία τεράστια γκάμα αρχιτεκτονικών (επίσης χάρη στον πυρήνα Unix).

Δικτύωση

Τα Windows έχουν κάνει άλματα σε αυτόν τον τομέα. Αρκετά φιλικά και αυτοματοποιημένα ως προς τη χρήση τους, με λειτουργικούς wizards και εκτενείς διαδικασίες ορισμού πολλαπλών χρηστών στο δίκτυο καλύπτουν κάθε ανάγκη δικτύωσης. Ειδική μνεία πρέπει να γίνει στην υποστήριξη των νεότερων προτύπων ασύρματης δικτύωσης (WiFi, Bluetooth). Σημειώνεται ότι τα Windows «βλέπουν» συστήματα Linux μέσω δικτύου.

Το Linux είναι εγγενώς... δικτυακό. Με πυρήνα το κατεξοχήν δικτυακό Unix, διαδικασίες όπως ο διαμοιρασμός αρχείων και η σχέση client-server αποτελούν αναπόσπαστο τμήμα του κώδικά του, το ίδιο και η εξ αποστάσεως διαχείριση. Όμως υπάρχει ακόμα δρόμος μέχρι την πλήρη συνεργασία με τα ασύρματα πρότυπα, η οποία παραμένει στα χαρτιά εν πολλοίς. Τέλος, μέσω του Samba, η δικτύωση με συστήματα Windows είναι αρκετά εύκολη.

Κόστος

Εδώ παρατηρείται η μεγάλη διαφοροποίηση μεταξύ των δύο αντιπάλων, καθώς τα Windows ήταν, είναι και θα είναι ένα σχετικά ακριβό λειτουργικό σύστημα (ειδικά στις εκδόσεις server). Με τη μείωση των τιμών στο hardware, το κλάσμα της τιμής του συστήματος είναι πλέον σημαντικό. Ιδιαίτερα στο εξωτερικό ολοένα αυξάνονται οι κατασκευαστές που προκειμένου να μειώσουν την τιμή του υπολογιστή επιλέγουν Linux αντί για Windows ως προεγκατεστημένο λειτουργικό.

Όσο αναφορά το Linux τα πράγματα ακολουθούν άλλη πολιτική. Στις περισσότερες περιπτώσεις μπορούμε να κατεβάσουμε ολόκληρη τη διανομή από το internet χωρίς το παραμικρό κόστος. Οι διανομές προσφέρονται εμπορικά και σε CD, με το κόστος να διατηρείται σε χαμηλά επίπεδα. Όσο αναφορά στο κατά πόσο, σε βάθος χρόνου, το κόστος χρήσης των δύο λειτουργικών διαφέρει πραγματικά, έχει δημιουργηθεί ένα πολύ σοβαρό debate, όμως τουλάχιστον όσο αναφορά στην οικιακή χρήση το πλεονέκτημα του Linux παραμένει πέρα από κάθε αμφισβήτηση. Άλλωστε έχουμε να κάνουμε με ουκ ολίγες εναλλακτικές και όχι με μία, όπως στα Windows.

4.4 Η θεωρία του «τζάμπα»

Η άποψη ότι το Linux έρχεται δωρεάν δεν είναι απόλυτα ακριβής, τουλάχιστον σε επαγγελματικό επίπεδο. Τα τελευταία χρόνια είναι σε εξέλιξη ένα σημαντικό debate αναφορικά με το κατά πόσο τελικά το Linux είναι φθηνότερο από τα Windows. Ένα debate στο πλαίσιο του οποίου δεν έχουν λείψει οι διεθνείς στατιστικές μελέτες, τα μεγάλα λόγια από δημιουργούς και κατασκευαστές και βέβαια το πανταχού παρόν παιχνίδι του marketing.

Η πιο περίφημη μελέτη προέρχεται από την IDC κατόπιν αίτησης της Microsoft και αφορά στο λειτουργικό κόστος των Windows 2000 σε 104 εταιρίες. Σύμφωνα με τα πορίσματα της μελέτης, υπό συνθήκες και σε βάθος πενταετίας, το κόστος χρήσης του λειτουργικού της Microsoft είναι μικρότερο από του μεγάλου ανταγωνιστή της. Βέβαια δεδομένου του κόστους των επαγγελματικών λύσεων της Microsoft, το γεγονός αυτό προκύπτει ξεκάθαρα από τα λειτουργικά έξοδα των τεχνικών ομάδων IT των εταιριών.

Πράγματι λόγω της διάδοσης των Windows και τουλάχιστον σε εταιρικό επίπεδο, η υποστήριξη ενός φθηνού εναλλακτικού OS όπως το Linux, ενδέχεται να αποδειχθεί αρκετά δαπανηρή εξαιτίας των αναγκών περαιτέρω εκπαίδευσης και εξειδίκευσης του τεχνικού προσωπικού.

Αναμφίβολα η διείσδυση του επαγγελματικού λογισμικού επηρεάζει ευθέως ανάλογα το κόστος χρήσης του, κάτι άλλωστε που αποδεικνύεται και από το χώρο του Web, όπου η επικράτηση των λύσεων του Linux (για διάφορους λόγους, ξεκινώντας από το αρχικό κόστος και φτάνοντας στην παρεχόμενη ασφάλεια), έχουν αντιστρέψει την κατάσταση, αφήνοντας τη Microsoft δεύτερη.

Συμπεράσματα

Το συμπέρασμα που προκύπτει από τη συμβίωση με το Linux είναι οι αστείρευτες δυνατότητες σε συνδυασμό με την πλήρη παραμετροποιησιμότητα του. Κάθε τι όμως έχει και αρνητικά και θετικά στοιχεία. Η πλήρης αυτή παραμετροποιησιμότητα δίνει στο χρήστη τη δυνατότητα να πετύχει αυτό ακριβώς που θέλει, εδώ όμως συνίσταται και το αρνητικό στοιχείο, ο χρήστης πρέπει να γνωρίζει ακριβώς τι θέλει να κάνει καθώς και τον τρόπο με τον οποίο θα πετύχει αυτό το αποτέλεσμα. Αυτό σημαίνει βαθιά γνώση του πρωτοκόλλου επικοινωνίας καθώς και τον διαδικασιών η οποίες είναι αλληλένδετες με τη λειτουργία που θέλει να επιτευχθεί. Όπως αναφέρθηκε η κατασκευή ενός firewall ξεκινάει με την απαγόρευση όλων των κινήσεων εντός και εκτός του δικτύου, αυτό σημαίνει μέγιστη δυνατή ασφάλεια αλλά ταυτόχρονα καθιστά το δίκτυο πλήρως άχρηστο να χειριστεί οποιαδήποτε πληροφορία, το επόμενο βήμα είναι ο καθορισμός της πολιτικής ασφάλειας και στη συνέχεια η πλήρης κατανόηση των αλληλένδετων διαδικασιών του κάθε πρωτοκόλλου που απαιτούνται για την επίτευξη αυτής της πολιτικής.

Από την αντίπερα όχθη, στα windows υπάρχουν έτοιμα πακέτα λογισμικού τα οποία αν παραμετροποιηθούν καταλλήλως μπορούν να μετατρέψουν τον υπολογιστή σε έναν firewall server πολύ πιο εύκολα και με λιγότερες γνώσεις. Το πρόβλημα σε αυτή τη περίπτωση είναι τα κατασκευάστηκα bugs τα οποία πιθανόν να έχει το ίδιο το software καθώς και τα κενά ασφαλείας τα οποία θα δημιουργεί το ίδιο το λειτουργικό το οποίο δεν μπορούμε να παραμετροποιήσουμε ανάλογα με τη χρήση του υπολογιστή όπως στην περίπτωση του Linux.

[6] Βιβλιογραφία

- **Red Hat® Linux Firewalls**
  Bill McCarty | 2004, Wiley Publishing, Inc.

- **Linux Firewalls**
  Robert L. Ziegler | 2007, New Riders

- **Firewalls and Internet Security, Repelling the Wily Hacker**
  William R. Cheswick, Steven M. Bellovin, Aviel D. Rubin | 2007, Addition Wesley

- **TroubleShooting Linux® Firewalls**
  Michael Shinn, Scott Shinn | 2005, Addition Wesley

- **Red Hat® Certified Engineer Linux, RHCE**
  Michael Jang | 2004, McGraw Hill

Μελέτες

- **Ασφάλεια Λειτουργικού Συστήματος Linux**
  Μακροδημήτρης Γεώργιος,Όσσας Λεωνίδας|2009

- **Μελέτη των επιθέσεων που στηρίζονται σε πακέτα με ψευδή IP Διεύθυνση αποστολέα**
  Ιωάννης Παπαπάνου|2003

SITES

- http://forum.ubuntu-gr.org/
- http://www.linuxsecurity.com/
- http://www.yolinux.com/tutorials/linuxsecuritytools.html
- http://www.linuxtopia.org/LinuxSecurity/
- http://www.islab.demokritos.gr

[6] Όλες οι εικόνες που χρησιμοποιήθηκαν για τις ανάγκες της εργασίας είναι κατεβασμένες από την πηγή αναζήτησης Google.