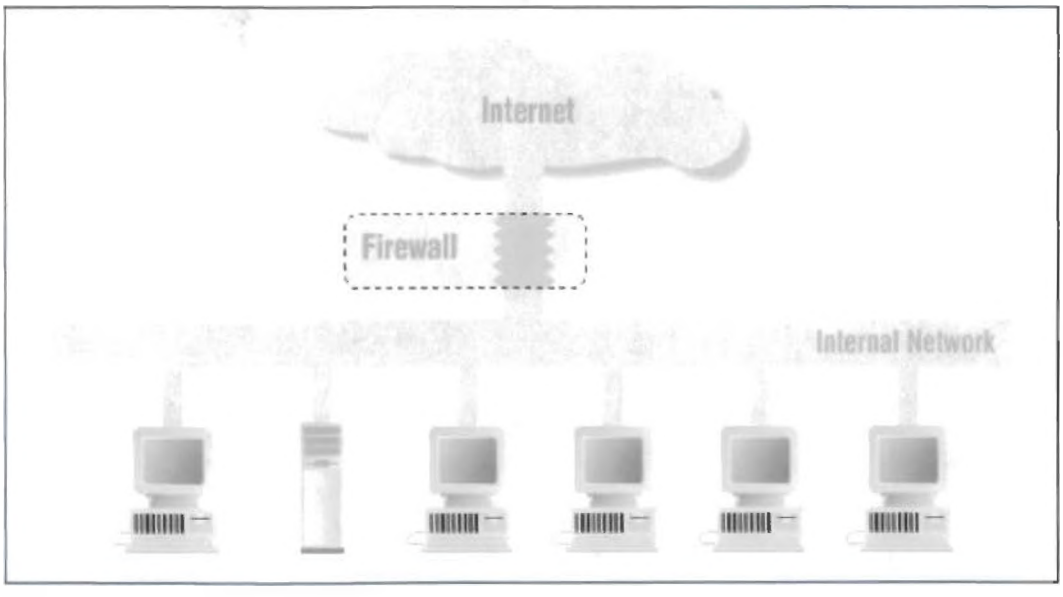
Α.Τ.Ε.Ι. ΜΕΣΟΛΟΓΓΙΟΥ
ΣΧΟΛΗ ΔΙΟΙΚΗΣΗΣ & ΟΙΚΟΝΟΜΙΑΣ
ΤΜΗΜΑ ΕΦΑΡΜΟΓΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΣΤΗ ΔΙΟΙΚΗΣΗ & ΣΤΗΝ ΟΙΚΟΝΟΜΙΑ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΘΕΜΑ:

*"ΣΥΣΤΗΜΑΤΑ ΠΡΟΣΔΙΟΡΙΣΜΟΥ ΕΙΣΒΟΛΕΩΝ ΜΕ ΤΗ ΧΡΗΣΗ **FIREWALL**"*



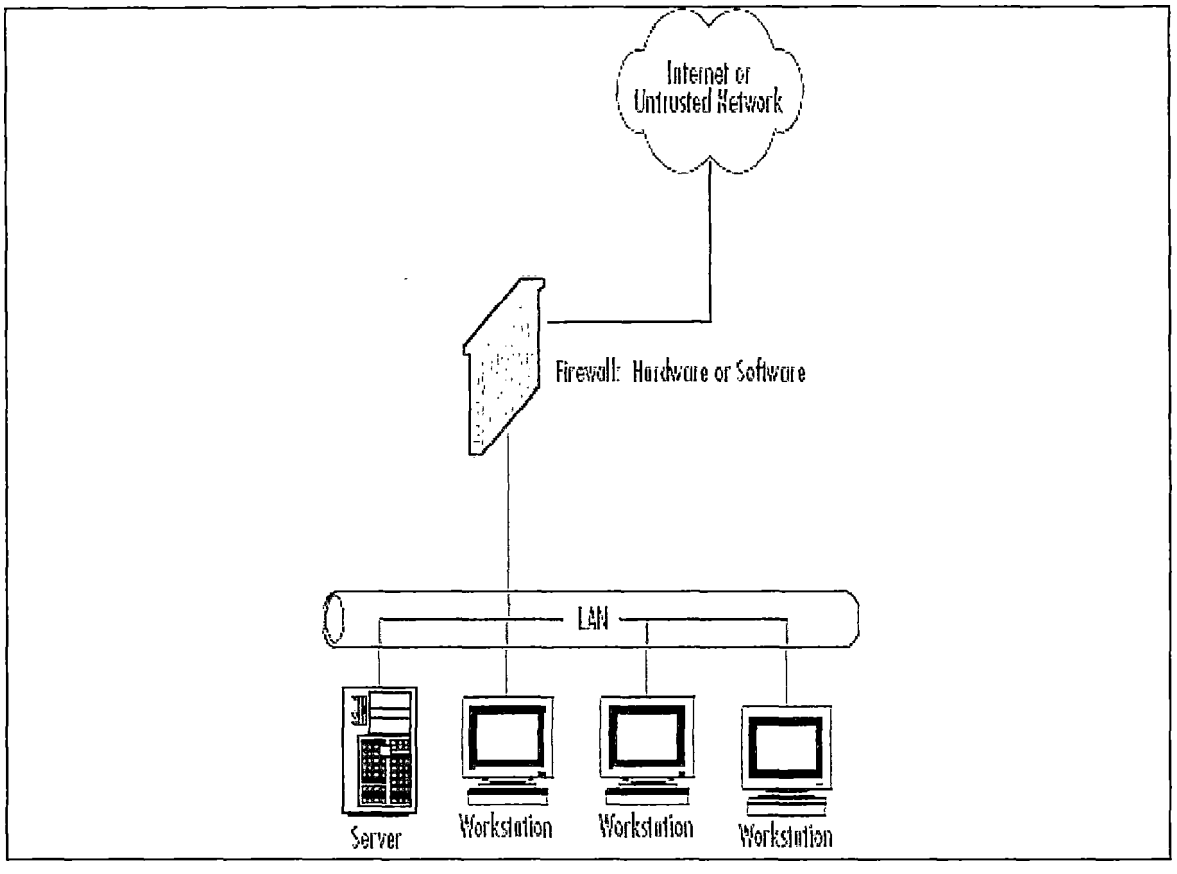
ΚΙΚΙΛΗΣ ΜΙΧΑΛΗΣ - Α.Μ. 7103

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ: *ΠΑΠΑΘΑΝΑΣΙΟΥ ΛΕΩΝΙΔΑΣ*

"Υπάρχουν πολλοί τρόποι για να ληστεύεις ανθρώπους. Οι υπολογιστές απλώς κάνουν τη δουλειά ευκολότερη."
-Jim Thomas κοινωνιολόγος-εγκληματολόγος

"Είναι εύκολο να έχεις ένα ασφαλές υπολογιστικό σύστημα. Το μόνο που χρειάζεται είναι να αποσυνδέσεις όλες τις τηλεφωνικές του συνδέσεις, να τοποθετήσεις το σύστημα σε ένα θωρακισμένο δωμάτιο, και να στήσεις έναν φύλακα έξω από την πόρτα."
- F.T. Gramp & R.H. Morris

"Η μόνη ασφαλής άμυνα είναι όταν κρατάς θέσεις που δε γίνεται να υποστούν επίθεση."
-«η Τέχνη του πολέμου» , *Sun Tzu / κινέζος στρατηγός*



Firewall.
[Σύνθετη λέξη αποτελούμενη από τις λέξεις Fire και Wall.Ελεύθερη μετάφραση, Τοίχος Φωτιάς ή Πύρινος Τοίχος].

ΚΕΦΑΛΑΙΟ 1^{Ο}: ΕΙΣΑΓΩΓΗ ΣΤΗΝ ΑΣΦΑΛΕΙΑ ΣΥΣΤΗΜΑΤΩΝ 6

1.1 ΕΙΣΑΓΩΓΗ 6
1.2 ΠΟΣΟ ΣΗΜΑΝΤΙΚΟ ΕΙΝΑΙ ΤΟ ΖΗΤΗΜΑ ΤΗΣ ΑΣΦΑΛΕΙΑΣ; 7
1.3 ΓΙΑΤΙ ΧΡΕΙΑΖΟΜΑΣΤΕ ΑΣΦΑΛΕΙΑ - ΤΙ ΠΡΟΣΠΑΘΟΥΜΕ ΝΑ ΠΡΟΣΤΑΤΕΨΟΥΜΕ 8

ΚΕΦΑΛΑΙΟ 2^{Ο} : ΑΠΕΙΛΕΣ ΚΑΙ ΑΝΤΙΜΕΤΩΠΙΣΗ 12

2.1 ΑΝΑΓΚΗ ΓΙΑ ΓΝΩΣΗ ΤΩΝ ΚΙΝΔΥΝΩΝ 12
2.2 ΠΟΙΕΣ ΑΠΕΙΛΕΣ ΔΕΧΟΜΑΣΤΕ 12
2.3 ΑΠΟ ΠΟΙΟΥΣ ΑΠΕΙΛΟΥΜΑΣΤΕ ΚΑΙ ΜΕ ΠΟΙΟ ΤΡΟΠΟ ΕΚΔΗΛΩΝΟΝΤΑΙ ΟΙ ΑΠΕΙΛΕΣ. 14
2.4 ΤΡΟΠΟΙ ΑΝΤΙΜΕΤΩΠΙΣΗΣ 20
2.5 ΓΙΑΤΙ ΕΙΝΑΙ ΑΝΑΓΚΑΙΑ Η ΧΡΗΣΗ FIREWALL 23

ΚΕΦΑΛΑΙΟ 3^{Ο} :ΕΝΝΟΙΑ ΚΑΙ ΧΡΗΣΗ ΤΩΝ FIREWALL 24

3.1 ΤΙ ΕΙΝΑΙ FIREWALL 24
3.2 ΣΚΟΠΟΣ ΤΗΣ ΧΡΗΣΗΣ FIREWALL 26
3.3 ΧΡΗΣΕΙΣ ΚΑΙ ΠΕΡΙΟΡΙΣΜΟΙ 27
3.3.1 ΧΡΗΣΕΙΣ 27
3.3.2 ΠΕΡΙΟΡΙΣΜΟΙ 28

ΚΕΦΑΛΑΙΟ 4^{Ο} : ΤΕΧΝΟΛΟΓΙΕΣ FIREWALL 30

4.1 SECURITY POLICY 30
4.2 SCREENING ROUTERS 32
4.3 PACKET FILTERING 34
4.3.1 ΕΙΣΑΓΩΓΗ 34
4.3.2 STATEFUL & DYNAMIC PACKET FILTERING 36
4.3.3 PROTOCOL CHECKING 38
4.3.4 ΠΑΡΑΜΕΤΡΟΙ ΕΓΚΑΤΑΣΤΑΣΗΣ ΕΝΟΣ PACKET FILTERING ΔΡΟΜΟΛΟΓΗΤΗ 39
4.3.5 ΕΝΕΡΓΕΙΕΣ ΤΟΥ ROUTER ΣΧΕΤΙΚΑ ΜΕ ΤΗΝ ΤΥΧΗ ΤΩΝ ΠΑΚΕΤΩΝ 40
4.3.6 ΑΛΛΑΖΟΝΤΑΣ ΤΟ ΠΑΚΕΤΟ 42
4.3.7 ΠΛΕΟΝΕΚΤΗΜΑΤΑ ΚΑΙ ΜΕΙΟΝΕΚΤΗΜΑΤΑ ΤΟΥ PACKET FILTERING 43
4.4 PROXY SERVICES 45
4.4.1 ΕΙΣΑΓΩΓΗ 45
4.4.2 ΟΙ ΛΟΓΟΙ ΓΙΑ ΤΟΥΣ ΟΠΟΙΟΥΣ ΕΠΙΛΕΓΟΥΜΕ PROXIES 47
4.4.3 Η ΛΕΙΤΟΥΡΓΙΑ ΤΩΝ PROXIES 48
4.4.3.1 ΧΡΗΣΙΜΟΠΟΙΩΝΤΑΣ PROXY-AWARE APPLICATION SOFTWARE 49
4.4.3.2 ΧΡΗΣΙΜΟΠΟΙΩΝΤΑΣ PROXY-AWARE OPERATING SYSTEM SOFTWARE 50
4.4.3.3 ΧΡΗΣΙΜΟΠΟΙΩΝΤΑΣ PROXY-AWARE ΔΙΑΔΙΚΑΣΙΕΣ ΧΡΗΣΤΗ 51
4.4.3.4 ΧΡΗΣΙΜΟΠΟΙΩΝΤΑΣ PROXY-AWARE ROUTER 52
4.4.4 PROXYING ΧΩΡΙΣ ΤΟΝ PROXY SERVER 53
4.4.5 ΠΛΕΟΝΕΚΤΗΜΑ ΚΑΙ ΜΕΙΟΝΕΚΤΗΜΑΤΑ ΤΩΝ PROXY SERVICES 54
4.5 NETWORK ADDRESS TRANSLATION (NAT) 56
4.5.1 ΕΙΣΑΓΩΓΗ 56
4.5.2 Η ΛΕΙΤΟΥΡΓΙΑ ΤΗΣ NETWORK ADDRESS TRANSLATION 56
4.5.3 ΠΛΕΟΝΕΚΤΗΜΑΤΑ ΚΑΙ ΜΕΙΟΝΕΚΤΗΜΑΤΑ ΤΗΣ NETWORK ADDRESS TRANSLATION 60
4.6 VIRTUAL PRIVATE NETWORKS 62
4.6.1 ΤΕΧΝΟΛΟΓΙΑ ΤΩΝ VPN 62
4.6.2 ΚΟΙΝΕΣ ΧΡΗΣΕΙΣ ΤΩΝ VPN 63
4.6.3 ΒΑΣΙΚΕΣ ΠΡΟΫΠΟΘΕΣΕΙΣ ΓΙΑ ΤΑ VPN 66
4.6.4 ΠΛΕΟΝΕΚΤΗΜΑΤΑ ΚΑΙ ΜΕΙΟΝΕΚΤΗΜΑΤΑ ΤΟΥ VIRTUAL PRIVATE NETWORKING 67

ΚΕΦΑΛΑΙΟ 5^{Ο} : ΑΡΧΙΤΕΚΤΟΝΙΚΕΣ FIREWALL 68

5.1 DUAL-HOMED HOST ΑΡΧΙΤΕΚΤΟΝΙΚΕΣ 68
5.2 SCREENED HOST ΑΡΧΙΤΕΚΤΟΝΙΚΕΣ 73
5.3 SCREENED SUBNET ΑΡΧΙΤΕΚΤΟΝΙΚΕΣ 75
5.4 APPLICATION LEVEL GATEWAYS 77
5.5 INTERNAL FIREWALL 81

ΚΕΦΑΛΑΙΟ 6^{Ο} : Η ΚΑΤΑΣΤΑΣΗ ΣΗΜΕΡΑ **82**

6.1 ΕΡΕΥΝΑ ΑΓΟΡΑΣ 82
6.2 ΕΠΙΛΟΓΟΣ 91

ΒΙΒΛΙΟΓΡΑΦΙΑ **94**

ΚΕΦΑΛΑΙΟ 1ο: ΕΙΣΑΓΩΓΗ ΣΤΗΝ ΑΣΦΑΛΕΙΑ ΣΥΣΤΗΜΑΤΩΝ

1.1 ΕΙΣΑΓΩΓΗ

Στα μέσα της δεκαετίας του 1960 , εν μέσω ψυχρού πολέμου ,το Υπουργείο Άμυνας των Η.Π.Α. ήθελε ένα δίκτυο εντολών και ελέγχου που θα μπορούσε να επιβιώσει ενός πυρηνικού πολέμου. Η δημιουργία του δικτύου αυτού ανατέθηκε στο ερευνητικό τμήμα του Υπουργείου, το Advanced Research Project Agency (ARPA).Το ARPA δεν διέθετε επιστήμονες ή εργαστήρια , έκανε τη δουλειά του προσφέροντας επιδοτήσεις και συμβόλαια σε πανεπιστήμια και εταιρείες . Έτσι λοιπόν, στα τέλη της ίδιας δεκαετίας δημιουργείται το ARPANET ο πρόγονος ουσιαστικά του INTERNET όπως το ξέρουμε σήμερα.

Το INTERNET στην αρχική του μορφή, αποτελείτο από μια σχετικά μικρή κοινότητα χρηστών στη δεκαετία του 1980 , κυρίως στον τομέα της έρευνας και στις ακαδημαϊκές κοινότητες. Λόγω της δυσκολίας στην πρόσβαση στα συστήματα αυτών των τομέων , αλλά και του γεγονότος ότι οι κοινότητες αυτές είναι αρκετά στενά συνδεδεμένες, το ζήτημα της ασφάλειας, μάλλον λογικά, δεν προκαλούσε ανησυχία σε αυτό το περιβάλλον. Άλλωστε , ο αντικειμενικός στόχος της διασύνδεσης των δικτύων αυτών ήταν η κοινή χρήση των πληροφοριών, όχι η απόκρυψή τους. Τεχνολογίες όπως το λειτουργικό σύστημα UNIX και τα Transmission Control Protocol / Internet Protocol (TCP/IP) πρωτόκολλα που σχεδιάστηκαν για αυτό το περιβάλλον είναι ενδεικτικές της έλλειψης ανησυχίας για την ασφάλεια. Η ασφάλεια απλώς δε θεωρείτο απαραίτητη.

Ωστόσο , στις αρχές της δεκαετίας του 1990 , το εμπορικό ενδιαφέρον για το INTERNET μεγάλωσε . Και οι φορείς του ενδιαφέροντος αυτού είχαν εντελώς διαφορετικές απόψεις πάνω στο θέμα της ασφάλειας , από ότι η ακαδημαϊκή κοινότητα .Η εμπορική πληροφορία είχε αξία, και η πρόσβαση σε αυτή έπρεπε να περιοριστεί σε συγκεκριμένους εξουσιοδοτημένους χρήστες. Το UNIX , το TCP/IP , οι συνδέσεις στο INTERNET έγιναν λεωφόροι (πιθανών) επιθέσεων χωρίς να έχουν την δυνατότητα να θέσουν σε εφαρμογή ισχυρές άμυνες.

Πρόσφατα στοιχεία αναφέρουν ότι καθημερινά διακινούνται περισσότερα από τρία δισεκατομμύρια e-mail από 200 εκατομμύρια χρήστες .Ο δε συνολικός αριθμός των χρηστών του διαδικτύου ξεπερνά τα 400 εκατομμύρια παγκοσμίως. Ο αριθμός αυτός είναι ενδεικτικός της ραγδαίας εξάπλωσης της χρήσης του INTERNET. Πρέπει πάντως να σημειωθεί πως σήμερα , η ασφάλεια των υπολογιστικών συστημάτων δεν έχει γίνει βεβαίως αυτοσκοπός. Είναι (ή τουλάχιστον θα έπρεπε να είναι) ωστόσο , το μέσο για έναν καθολικό σκοπό , την ασφάλεια της πληροφορίας.

1.2 ΠΟΣΟ ΣΗΜΑΝΤΙΚΟ ΕΙΝΑΙ ΤΟ ΖΗΤΗΜΑ ΤΗΣ ΑΣΦΑΛΕΙΑΣ;

Πριν δούμε οτιδήποτε άλλο αξίζει να εστιάσουμε στην αξία που έχει η ασφάλεια ενός δικτύου. Βέβαια ο καλύτερος τρόπος για να καταλάβει κάποιος την αξία ενός πράγματος είναι να αναλογιστεί τις συνέπειες πιθανής απώλειας. Αυτές τις συνέπειες θα εξετάσουμε . Πρέπει να σημειωθεί βέβαια ότι γίνεται περισσότερο αναφορά σε δίκτυα επιχειρήσεων, και όχι σε μεμονωμένους οικιακούς χρήστες, γιατί τα μεγέθη είναι μεγαλύτερα και καθίστανται ευκολότερα κατανοητές οι συνέπειες της έλλειψης ασφάλειας .Πάντως οι επιπτώσεις και για οικιακούς χρήστες είναι ,τηρουμένων των αναλογιών, ανάλογες.

Ακολουθεί αναφορά σε απώλειες που μπορεί να υπάρξουν και στα αποτελέσματα τους.

Α. Απώλεια δεδομένων. Για να κατανοήσουμε τις συνέπειες πρέπει να αναλογιστούμε τι θα γινόταν αν χάνονταν το σύνολο των δεδομένων μιας επιχείρησης. Οικονομικά στοιχεία, στοιχεία πελατών , υπαλλήλων κ.λ.π. Μια τέτοια απώλεια θα έθετε σε κίνδυνο ακόμα και την ύπαρξη της επιχείρησης .

Β. Πρόσβαση σε εμπιστευτικά δεδομένα. Αν κάποιος μπορούσε να αποκτήσει πρόσβαση σε τέτοιου είδους δεδομένα αυτό θα ήταν πλήγμα για την επιχείρηση. Οι λόγοι είναι προφανείς .Σημαντικά οικονομικά στοιχεία που δεν πρέπει να γίνονται γνωστά ή πλάνα της επιχείρησης που θα ήθελε να ξέρει ο ανταγωνισμός, στα χέρια κάποιου μη εξουσιοδοτημένου χρήστη θα ήταν καταστροφή.

Γ. «Νεκρός χρόνος» .Μετά από κάθε επιτυχημένη επίθεση στο δίκτυο μιας επιχείρησης χρειάζεται κάποιος χρόνος για να επανέλθει σε φυσιολογική λειτουργία. Στη διάρκεια του «νεκρού χρόνου» καμία λειτουργία της

επιχείρησης δεν μπορεί να εκτελεστεί. Αυτό συνεπάγεται χάσιμο χρόνου και χρήματος αλλά και δυσαρέσκεια από τους πελάτες ή όποιους άλλους συνεργάζονται με την επιχείρηση , με ότι αυτό συνεπάγεται.

Δ. Χαμένες εργατοώρες. Λέγεται ότι «ο χρόνος είναι χρήμα».Για να διορθωθεί η ζημία μετά από μια επίθεση χρειάζονται και τα δύο. Πολύς χρόνος και αρκετά χρήματα .Αλλά και πολλές χαμένες ώρες για τους υπαλλήλους της επιχείρησης αφού όλα πρέπει να γίνουν από την αρχή. Όπως για παράδειγμα σε περίπτωση επίθεσης με ιό.

Ε. Προβλήματα για την φήμη της επιχείρησης . Κάθε επίθεση που γίνεται δεν αποτελεί πλήγμα μόνο για τα πληροφοριακά συστήματα αλλά και για την φήμη της επιχείρησης. Δημιουργούνται ερωτηματικά για την αξιοπιστία της εταιρίας. Επίσης, και αυτό είναι πιο σημαντικό , φτάνει να φανταστούμε τι θα γινόταν αν κάποιος εισβολέας χρησιμοποιούσε έναν υπολογιστή της εταιρίας για να κάνει παράνομες πράξεις. Η ευθύνη θα βάρυνε την επιχείρηση.

1.3 ΓΙΑΤΙ ΧΡΕΙΑΖΟΜΑΣΤΕ ΑΣΦΑΛΕΙΑ - ΤΙ ΠΡΟΣΠΑΘΟΥΜΕ ΝΑ ΠΡΟΣΤΑΤΕΨΟΥΜΕ

Τις τελευταίες δύο δεκαετίες αρκετές εταιρίες άρχισαν να συνειδητοποιούν πως τα πολυτιμότερα περιουσιακά στοιχεία δεν ήταν απλά οι κτιριακές εγκαταστάσεις και η πνευματική περιουσία, αλλά και οι πληροφορίες που έρεαν εσωτερικά αλλά και προς τα έξω σε προμηθευτές και πελάτες. Σταδιακά οι διευθυντές των εταιρειών άρχισαν να σκέφτονται τι θα γινόταν εάν οι ζωτικής σημασίας πληροφορίες της επιχείρησης έφταναν σε λάθος χέρια. Για κάποιο διάστημα ο κίνδυνος δεν ήταν μεγάλος , λόγω του τρόπου αποθήκευσης των πληροφοριών. Η φράση κλειδί εδώ είναι «κλειστά συστήματα». Πιο συγκεκριμένα, οι σημαντικές πληροφορίες της επιχείρησης αποθηκεύονταν σε servers η πρόσβαση στους οποίους γινόταν μέσω τερματικών και οι οποίοι είχαν ελάχιστες διασυνδέσεις με άλλα συστήματα. Όλες οι διασυνδέσεις δε ήταν μέσω ιδιωτικών μισθωμένων γραμμών σε επιλεγμένα περιορισμένες τοποθεσίες , είτε μέσα στην επιχείρηση είτε σε έμπιστους επαγγελματικούς συνεργάτες.

Ωστόσο , την τελευταία πενταετία το INTERNET άλλαξε τον τρόπο λειτουργίας των επιχειρήσεων. Σημειώθηκε μεγάλη επιτάχυνση στην διασυνδεσιμότητα οργανισμών συστημάτων και δικτύων. Ολόκληρα

επιχειρηματικά δίκτυα έχουν αποκτήσει πρόσβαση στο INTERNET και μάλιστα σε πολλαπλά σημεία .Η εξάπλωση αυτή δημιούργησε κινδύνους για ευαίσθητες πληροφορίες και κρίσιμα επιχειρησιακά συστήματα , κίνδυνοι που σχεδόν δεν υπήρχαν παλιότερα. Η σημασία της ασφάλειας πληροφοριών στο επιχειρηματικό περιβάλλον έχει πλέον υπογραμμιστεί , όπως και η ανάγκη για ικανούς και έμπιστους συνεργάτες αυτής της ειδικότητας.

Παραδοσιακά , έχουμε συνδέσει την ασφάλεια με ανθρώπους κάποιες φορές ένοπλους , οι οποίοι φυλάσσουν απτά περιουσιακά στοιχεία , όπως χρήματα . Καθισμένοι άλλοτε πίσω από γραφεία ελέγχοντας το χώρο μέσω κλειστού κυκλώματος τηλεόρασης. Οι άνθρωποι αυτοί συνήθως είχαν ελάχιστη εκπαίδευση και δεν είχαν επίγνωση τι ακριβώς προστάτευαν και πόσο πολύτιμο ήταν. Έκαναν ωστόσο τη δουλειά τους το ίδιο καλά και σύμφωνα με δεδομένες διαδικασίες όπως για παράδειγμα η περιφρούρηση ανά τακτά χρονικά διαστήματα και ο έλεγχος για ύποπτες κινήσεις. Η ασφάλεια της πληροφορίας εισήγαγε το μοντέλο αυτό στον ,απροσδιόριστο, κόσμο της πληροφορικής. Στην ουσία η ασφάλεια της πληροφορίας ασχολείται με την διασφάλιση της πρόσβασης στην πληροφορία μόνο από εξουσιοδοτημένους χρήστες και συστήματα.

Οι ειδικοί του χώρου έχουν συχνά διαφορετικές απόψεις πάνω στο ρόλο και τον ορισμό της ασφάλειας της πληροφορίας .Υπάρχουν ωστόσο τρεις θεμελιώδεις περιοχές ανησυχίας , κοινής παραδοχής. Αυτά για τα οποία μεριμνούμε για προστασία. Όταν λοιπόν υπάρχει σύνδεση στο INTERNET τίθενται σε κίνδυνο τα εξής :

Τα δεδομένα

Οι πόροι

Η φήμη

Τα δεδομένα έχουν τρία ξεχωριστά χαρακτηριστικά που χρειάζονται προστασία .Αυτά είναι:

Α. ΕΜΠΙΣΤΕΥΤΙΚΟΤΗΤΑ .Εξασφάλιση πρόσβασης μόνο από εξουσιοδοτημένου χρήστες. Προστασία δηλαδή από προσπάθεια παραβίασης.

Β. ΑΚΕΡΑΙΟΤΗΤΑ .Εξασφάλιση ότι οι πληροφορίες δεν τροποποιούνται από μη εξουσιοδοτημένους χρήστες , αλλά και αποφυγή λανθασμένης τροποποίηση από εξουσιοδοτημένους . Λάθος χειρισμό δηλαδή, ακούσιο η εκούσιο.

Γ. ΔΙΑΘΕΣΙΜΟΤΗΤΑ. Εξασφάλιση ότι οι πληροφορίες είναι διαθέσιμες όποτε χρειάζεται. Η διαθεσιμότητα περιλαμβάνει εγγύηση ότι τα συστήματα παραμένουν διαθέσιμα σε περίπτωση επίθεσης DoS (denial of service) . Σημαίνει επίσης προστασία κρίσιμων δεδομένων από διαγραφή.

Συνήθως η μεγαλύτερη ανησυχία για τις πληροφορίες αφορούν την εμπιστευτικότητα. Και είναι αλήθεια ότι σε αυτόν τον τομέα υπάρχει μεγάλη επικινδυνότητα. Πολλές μεγάλες εταιρείες φυλάσσουν κρίσιμες πληροφορίες στους υπολογιστές της εταιρείας .Βεβαίως , μπορούν να αποθηκευτούν οι σημαντικές πληροφορίες σε υπολογιστές από τους οποίους δεν υπάρχει πρόσβαση στο INTERNET . Η λύση αυτή , αν και δεν είναι πάντα πρακτικά εφαρμόσιμη, μπορεί να καλύψει το θέμα της εμπιστευτικότητας. Σε καμία περίπτωση όμως την ακεραιότητα και την διαθεσιμότητα.

Οι πόροι περιλαμβάνουν τον εξοπλισμό της επιχείρησης που δέχεται επίθεση. Στην ουσία οι πληροφορίες που περιέχουν είναι ο στόχος όμως πλήττονται και τα συστήματα. Χρειάζεται χρόνος και χρήμα για να διορθωθεί η ζημιά , ενώ κάποιες φορές η καταστροφή είναι ολική. Ακόμα και αν δεν υπάρχει ζημία υπάρχει και η περίπτωση εισβολής και χρήσης των πόρων από μη εξουσιοδοτημένους χρήστες κάτι που προφανώς κανείς δεν επιθυμεί.

Σε κίνδυνο βρίσκεται και η φήμη μιας επιχείρησης σε περίπτωση εισβολής. Για δύο κυρίως λόγους. Πρώτον ,σε περίπτωση εισβολής και χρήσης των συστημάτων της εταιρείας για παράνομες πράξεις χρησιμοποιώντας την ταυτότητά της , τίθεται η εταιρεία αντιμέτωπη με τον νόμο. Ένας εισβολέας μπορεί να αλλάξει το web site μιας εταιρίας , να στείλει e-mail η δελτία τύπου εμφανιζόμενος ως μέλος της εταιρείας. Συνήθως, οι εισβολείς δίνουν σημασία κυρίως αυτό που κάνουν να προκαλέσει μεγαλύτερη έκπληξη , πάρα να γίνει πιστευτό. Ακόμα και έτσι όμως κάποιοι θα ξεγελαστούν και η αποκατάσταση της αλήθειας θα είναι χρονοβόρα και ταπεινωτική. Οτιδήποτε έστω και ελάχιστα πιστευτό είναι πιθανόν να προκαλέσει ανεπανόρθωτη ζημιά στη φήμη της εταιρείας. Πρέπει να γίνει κατανοητό πως οτιδήποτε πράξει ο εισβολέας μέσω των συστημάτων της εταιρείας , θα μοιάζει με πράξη της γιατί ακριβώς θα προέρχεται από την εταιρεία! Δεύτερον , ακόμα και αν δεν χρησιμοποιηθούν τα συστήματα της εταιρείας για παράνομες πράξεις χρησιμοποιώντας την ταυτότητα της εταιρείας , είναι επόμενο μια εισβολή να κλονίσει την εμπιστοσύνη του κοινού

προς την εταιρεία. Αν δηλαδή η εισβολή έχει σκοπό να αποκτηθεί πρόσβαση σε πειρατικό λογισμικό, πορνογραφία η σε συστήματα άλλης εταιρείας με σκοπό την κλοπή, τα αποτελέσματα θα είναι τα ίδια για την φήμη της εταιρείας.

Όπως προείπαμε ανάλογη είναι η περίπτωση και για μεμονωμένους οικιακούς χρήστες. Αν εξαιρέσει κανείς την φήμη , στα υπόλοιπα η κατάσταση είναι η ίδια. Σε μικρότερη κλίμακα βέβαια .Κυρίως στο θέμα της ποσότητας, αφού για τον καθένα τα δεδομένα του και ο εξοπλισμός του είναι εξίσου σημαντικά όπως και για μια επιχείρηση. Απλά έχει μικρότερο (ίσως και λιγότερης σημασίας) αριθμό κρίσιμων δεδομένων, και μικρότερης αξίας εξοπλισμό. Ακόμα και για την φήμη , σε αντίστοιχη περίπτωση (όπως αυτές που αναφέρθηκαν πιο πάνω) θα έχει ,ομοίως, προβλήματα με το νόμο.

ΚΕΦΑΛΑΙΟ 2ο: ΑΠΕΙΛΕΣ ΚΑΙ ΑΝΤΙΜΕΤΩΠΙΣΗ

2.1 ΑΝΑΓΚΗ ΓΙΑ ΓΝΩΣΗ ΤΩΝ ΚΙΝΔΥΝΩΝ

Είναι γεγονός ότι η απώλεια κρίσιμων πληροφοριών είναι μια πολύ μεγάλη απειλή για μια επιχείρηση το δίκτυο της οποίας είναι συνδεδεμένο με τον έξω κόσμο. Βεβαίως η απομακρυσμένη πρόσβαση για τους εργαζομένους και η σύνδεση στο INTERNET βελτιώνουν τη λειτουργία της επιχείρησης σε μεγάλο βαθμό .Προσφέρει δε άμεση πρόσβαση σε πηγές πληροφοριών και επικοινωνία με πελάτες και προμηθευτές. Οι δυνατότητες αυτές όμως καθιστούν ένα τοπικό δίκτυο ευάλωτο σε επιθέσεις εισβολέων και καταχρήσεις των υπαλλήλων της ίδιας της επιχείρησης .

Το πρώτο βήμα για την αντιμετώπιση ενός προβλήματος είναι η κατανόησή του. Για την προστασία λοιπόν των πόρων ενός δικτύου από απώλεια, καταστροφή, ή ανεπιθύμητη πρόσβαση πρέπει να γίνει κατανοητό ποιος επιχειρεί τις επιθέσεις αυτές, για πιο λόγο και με ποιόν τρόπο. Η γνώση αυτή θα βοηθήσει στην αντιμετώπιση των επιθέσεων με τον προσδιορισμό της κατάλληλης πολιτικής ασφάλειας.

2.2 ΠΟΙΕΣ ΑΠΕΙΛΕΣ ΔΕΧΟΜΑΣΤΕ

Όταν το επιχειρησιακό υπολογιστικό περιβάλλον ήταν ένα κλειστό περιορισμένης πρόσβασης σύστημα, οι απειλές προέρχονταν κυρίως από το εσωτερικό της επιχείρησης . Οι εσωτερικές αυτές απειλές προέρχονταν από δυσαρεστημένους υπαλλήλους με προνομιακή πρόσβαση που μπορούσαν να προκαλέσουν μεγάλη ζημιά. Επιθέσεις από έξω ήταν σχεδόν ανύπαρκτες μιας και υπήρχαν τυπικά ελάχιστες ,αν όχι καθόλου, ιδιωτικές συνδέσεις σε έμπιστες οντότητες. Οι πιθανοί εισβολείς ήταν λίγοι σε αριθμό καθώς ο συνδυασμός της απαραίτητης δεξιότητας και κακόβουλων προθέσεων δεν ήταν καθόλου αναπτυγμένος.

Ωστόσο με την ανάπτυξη του INTERNET αναπτύχθηκαν επίσης και εξωτερικές απειλές. Υπάρχουν πλέον εκατομμύρια hosts στο INTERNET ως πιθανοί στόχοι επιθέσεων , που δελεάζουν , τον μεγάλο αριθμό πλέον των επίδοξων εισβολέων. Η δεξιότητα των οποίων έχει βελτιωθεί , ενώ υπάρχει και συνεννόηση ανταλλάσσοντας πληροφορίες για τους τρόπους εισβολής στα συστήματα , για όφελος ή για διασκέδαση. Η γεωγραφία δεν αποτελεί εμπόδιο πλέον. Η επίθεση μπορεί να γίνει από ανθρώπους σε άλλη ήπειρο έως στο απέναντι σπίτι .

Ένας αρχικός διαχωρισμός των απειλών μπορεί να γίνει ανάμεσα σε δομημένες και μη. Οι μη δομημένες επιθέσεις προέρχονται από άτομα με ελάχιστη δεξιότητα και επιμονή. Συνήθως πρόκειται για άτομα που ονομάζονται script kiddies –εισβολείς με ελάχιστη έως μηδαμινή γνώση προγραμματισμού , και πολύ λίγη γνώση των συστημάτων. Επιχειρούν εισβολές απλά για να καυχηθούν στους όμοιους τους. Αποκτούν εργαλεία επίθεσης που έχουν δημιουργηθεί από πιο έμπειρους και τα χρησιμοποιούν συχνά αδιακρίτως για να εντοπίσουν κάποια αδυναμία στο στόχο τους. Αν δεν τα καταφέρουν προχωρούν σε επόμενο στόχο. Πρόσθετος κίνδυνος προκύπτει από το γεγονός ότι συχνά χρησιμοποιούν αυτά τα εργαλεία χωρίς να γνωρίζουν το περιβάλλον του στόχο με αποτέλεσμα να προξενούνται απροσδιόριστες συνέπειες. Οι επιθέσεις αυτές μπορούν να προκαλέσουν σημαντική ζημιά ή δυσλειτουργία παρά τις προθέσεις και τις γνώσεις των επιτιθέμενων. Πάντως , οι επιθέσεις αυτές είναι συνήθως ανιχνεύσιμες από τα τρέχοντα εργαλεία ασφάλειας.

Οι δομημένες επιθέσεις είναι πιο ενοχλητικές καθώς προέρχονται από άτομα με αξιοσημείωτες δεξιότητες. Αν τα υπάρχοντα εργαλεία δεν τους εξυπηρετούν έχουν την δυνατότητα και την θέληση να τα τροποποιήσουν ή να φτιάξουν δικά τους. Είναι ικανοί να ανακαλύψουν νέες αδυναμίες στα συστήματα μέσω περίπλοκων ενεργειών έναντι των οποίων δεν πήραν μέτρα προστασίας οι σχεδιαστές των συστημάτων. Τα κίνητρα των επιθέσεων αυτών είναι συνήθως πολύ ισχυρότερα από τη απλή πρόκληση ζημιάς. Μια δομημένη επίθεση ενδέχεται να μην μπορεί να μπλοκαριστεί από τις παραδοσιακές μεθόδους ασφάλειας. Ενδεικτικό είναι το γεγονός ότι σε αυτού του είδους των επιθέσεων μπορούν να χρησιμοποιηθούν και μη ηλεκτρονικές μέθοδοι , όπως το social engineering . Το social engineering είναι ένας τρόπος απόκτησης κρίσιμων πληροφοριών ασφάλειας εξαπατώντας κάποιους ανθρώπους .

Οι απειλές με βάση τη φύση τους χωρίζονται σε φυσικές και ηλεκτρονικές. Φυσική απειλή έχουμε όταν ο εισβολέας έχει φυσική πρόσβαση στο σύστημα . Όταν μπορεί δηλαδή να έχει πρόσβαση στις εγκαταστάσεις και

τον εξοπλισμό της επιχείρησης. Οι ηλεκτρονικές απειλές , αυτές τις οποίες εξετάζουμε , υφίστανται μέσω του δικτύου της επιχείρησης και φυσικά του INTERNET , και αφορούν επιθέσεις από απόσταση. Αν θελήσουμε τώρα να κατηγοριοποιήσουμε τις απειλές με βάση τα αποτελέσματά τους , θα προκύψουν οι εξής κατηγορίες :

ΑΠΩΛΕΙΑ ΔΕΔΟΜΕΝΩΝ .Περιλαμβάνει την κλοπή εμπιστευτικών πληροφοριών της εταιρείας , όπως οικονομικά στοιχεία, φακέλους των υπαλλήλων πνευματική ιδιοκτησία κλπ.

ΠΑΡΑΠΟΙΗΣΗ / ΚΑΤΑΣΤΡΟΦΗ ΔΕΔΟΜΕΝΩΝ. Αφορά , ανεξαρτήτως κινήτρων , την τροποποίηση κάποιων κρίσιμων δεδομένων της επιχείρησης ή την διαγραφή τους.

Denial Of Service (DoS) . Αφορά το "κατέβασμα" του δικτύου ή του server μιας εταιρείας με αντικειμενικό στόχο να μην μπορούν οι νόμιμοι χρήστες τους να έχουν πρόσβαση σε αυτά. Επιτυγχάνεται με την υπερφόρτωση του συστήματος ώστε να μην είναι διαθέσιμο και να μην μπορεί να παράσχει τις υπηρεσίες του. Πιο συγκεκριμένα , στέλνονται τεράστιες ποσότητες πακέτων δεδομένων ή προγραμμάτων που απαιτούν το σύστημα να ανταποκρίνεται συνεχώς σε εικονικές εντολές.

ΠΑΡΑΝΟΜΗ ΧΡΗΣΗ ΤΩΝ ΠΟΡΩΝ ΤΗΣ ΕΠΙΧΕΙΡΗΣΗΣ . Αφορά εισβολές στο σύστημα από μη εξουσιοδοτημένους χρήστες με σκοπό την χρήση των πόρων του .Είναι ίσως η πιο κοινή επίθεση που μπορεί να εκδηλωθεί σε ένα σύστημα . Μπορεί δε να επιτευχθεί με πολλούς τρόπους .

2.3 ΑΠΟ ΠΟΙΟΥΣ ΑΠΕΙΛΟΥΜΑΣΤΕ ΚΑΙ ΜΕ ΠΟΙΟ ΤΡΟΠΟ ΕΚΔΗΛΩΝΟΝΤΑΙ ΟΙ ΑΠΕΙΛΕΣ.

Πριν δούμε ποιοι είναι αυτοί που εκδηλώνουν τις επιθέσεις , είναι χρήσιμο να εξετάσουμε τις αιτίες της εκδήλωσης επιθέσεων .Για ποιο λόγο δηλαδή προσπαθούν να παραβιάσουν ένα σύστημα. Αν και πιθανώς τα κίνητρα είναι τόσο πολλά όσο και οι επίδοξοι εισβολείς , μπορούν εντούτοις να χωριστούν, τουλάχιστον τα πιο συνηθισμένα από αυτά ,στις εξής κατηγορίες :

ΔΙΑΣΚΕΔΑΣΗ. Επιχειρούν εισβολή σε ένα σύστημα απλά για διασκέδαση ή για επιβεβαίωση. Για να αποδείξουν τις ικανότητες τους. Πρόκειται κυρίως για άτομα νεαρής ηλικίας η για τους αποκαλούμενους

αντιεξουσιαστές. Είναι ένα ανόητο και εγωιστικό παιχνίδι, που μπορεί πάντως να έχει σημαντικές επιπτώσεις για την επιχείρηση.

ΚΕΡΔΟΣ. Ίσως το κυριότερο κίνητρο. Κάποια άτομα που για προσωπικό όφελος επιχειρούν επίθεση. Είτε αυτοβούλως για κλοπή χρημάτων , διαγραφή χρεών τους κλπ , είτε έμμισθοι για λογαριασμό άλλων που δεν μπορούν η δεν θέλουν να εισβάλουν οι ίδιοι.

ΕΚΔΙΚΗΣΗ .Πολλές φορές το κίνητρο είναι η εκδίκηση. Τις περισσότερες φορές πρόκειται είτε για δυσαρεστημένους πελάτες είτε για αδικημένους , νυν ή πρώην υπαλλήλους .

Πάντως, πολλές (αν όχι τις περισσότερες) φορές πρόκειται για συνδυασμό κάποιων από τα παραπάνω κίνητρα. Προφανώς το αποτέλεσμα είναι το ίδιο.

Μια τέταρτη κατηγορία που δεν αποτελεί κίνητρο , αποτελεί όμως αιτία εκδήλωσης απειλής είναι η : ΑΦΕΛΕΙΑ Ή ΑΤΥΧΗΜΑ .Αφορά περιπτώσεις όπου από απροσεξία, ή από άγνοια δημιουργείται απειλή για το σύστημα. Είναι προφανές ότι πρόκειται για ακούσιες ενέργειες , εξακολουθούν ωστόσο να είναι αιτία για εκδήλωση απειλής.

Οποιοσδήποτε έχει ασχοληθεί έστω και ελάχιστα με το INTERNET έχει σίγουρα ακούσει τον όρο hacker ή cracker . Το άκουσμά τους βέβαια προκαλεί ποικίλα συναισθήματα, σε άλλους φόβο, σε άλλους (που έχουν δεχθεί επίθεση) θυμό ή απέχθεια. Αναμφίβολα πάντως πρόκειται για άτομα που, στη συντριπτική τους πλειονότητα, έχουν πλούσιες γνώσεις γύρω από τους υπολογιστές. Ο αρχικός ορισμός που αποδόθηκε στους hackers ήταν περίπου ως εξής :hacker είναι εκείνος ο χρήστης υπολογιστή που χαρακτηρίζεται από μεγάλη δίψα για μάθηση τω εσωτερικών μηχανισμών του και από την ικανότητα να ωθεί τον υπολογιστή του στο μέγιστο των δυνατοτήτων του με υγιή προγραμματισμό. Αυτό βέβαια ίσχυε μέχρι τα μέσα της δεκαετίας του 1980. Από εκεί και μετά , για λόγους που εξηγήσαμε πιο πάνω άλλαξε η κατάσταση. Ο όρος χρησιμοποιείται πλέον για να χαρακτηρίσει και αυτούς τους χρήστες που αποκτούν μη εγκεκριμένη πρόσβαση σε ξένα υπολογιστικά συστήματα στην προσπάθεια τους να αποκτήσουν γνώσεις. Αργότερα βέβαια παραχώρησαν την θέση τους σε νέες γενιές χρηστών πληροφορικής που καταστρέφουν , τροποποιούν η μετακινούν τα δεδομένα των υπολογιστικών συστημάτων που αποκτούν πρόσβαση με τέτοιο τρόπο που προκαλούν ζημιά ή επιβάρυνση του κόστους λειτουργίας τους. Με βάση αυτόν τον τελευταίο ορισμό , οι σημερινοί hackers μπορούν εύστοχα να χαρακτηριστούν crackers , αφού επιδιώκουν την μη

εγκεκριμένη πρόσβαση με σκοπό τη ζημία (=crack) . Οι δύο έννοιες λοιπόν θεωρούνται σήμερα ταυτόσημες ,ο hacker θεωρείται cracker .Άλλωστε και στο μυαλό του κοινού, ο ορισμός "hacker" έχει πια μόνιμα ορισθεί σαν ένα άτομο ιδιαίτερα ταλαντούχο με τους υπολογιστές που όμως συχνά χρησιμοποιεί αυτό το ταλέντο του για μη ευγενικούς σκοπούς.

Σε κάθε περίπτωση πάντως οι hackers δεν αποτελούν ολοκληρωμένη απάντηση στο ερώτημα: από ποιους απειλούμαστε; Αυτή είναι μια γενική απάντηση που δεν καλύπτει όλο το φάσμα των επίδοξων εισβολέων. Υπάρχουν αρκετές κατηγορίες ανάλογα με τα κίνητρα και κυρίως, την ιδιότητα τους.

Συγκεκριμένα , μη εγκεκριμένη πρόσβαση επιχειρούν :

Εργαζόμενοι.

Μια από τις μεγαλύτερες κατηγορίες ατόμων που προκαλούν προβλήματα ασφαλείας περιλαμβάνει τους δυσαρεστημένους υπαλλήλους ή πρώην υπαλλήλους που νιώθουν ότι αδικήθηκαν ή φέρουν μια βαθιά αντιπάθεια για τους εργοδότες τους. Οι εργαζόμενοι ή πρώην εργαζόμενοι αποτελούν συνήθως τους πιο επικίνδυνους πληροφορικούς εγκληματίες αφού γνωρίζουν πολλούς από τους κωδικούς ασφαλείας και μέτρα προστασίας που είναι ήδη εγκατεστημένα. Ξέρουν σε ποιους υπολογιστές να επιτεθούν, ποια αρχεία θα δημιουργήσουν την μεγαλύτερη ζημιά αν σβηστούν και που βρίσκονται αποθηκευμένα τα αντίγραφα ασφαλείας.

Κλέφτες.

Μια δεύτερη κατηγορία περιλαμβάνει τους κλέφτες και τους παραχαράκτες. Αυτά τα άτομα θα μπορούσαν να εμποδίσουν την ομαλή λειτουργία ενός υπολογιστικού συστήματος για να εκμεταλλευθούν την κατάσταση που θα προκύψει ή να καλύψουν αποδείξεις της εγκληματικής τους δραστηριότητας.

Κατάσκοποι.

Βιομηχανική και πολιτική κατασκοπία ή σαμποτάζ είναι ένας άλλος λόγος συγγραφής κακόβουλου κώδικα. Οι προγραμματιζόμενες απειλές είναι ένα πολύ ισχυρό και δύσκολο στον εντοπισμό , μέσο απόκτησης απόρρητων ή ευαίσθητων πληροφοριών, ή καθυστέρησης του ανταγωνισμού (σαμποτάζ).

Εκβιαστές .

Ο εκβιασμός μπορεί επίσης να αποτελέσει κίνητρο για την συγγραφή τέτοιου είδους λογισμικού. Σε αυτήν την περίπτωση οι εκβιαστές απειλούν να ενεργοποιήσουν καταστροφικό λογισμικό αν δεν πληρωθεί κάποιο ποσό ή αν δεν ικανοποιηθεί κάποια άλλη τους επιθυμία. Πολλές εταιρίες έχουν πέσει θύματα κάποιας μορφής εκβιασμού στην οποία έχουν συμφωνήσει να μην κινηθούν δικαστικά εναντίον των ατόμων που παραβίασαν την ασφάλεια των υπολογιστικών τους συστημάτων. Δεν είναι λίγες οι περιπτώσεις μάλιστα όπου οι εταιρίες έχουν προσλάβει στο προσωπικό τους τέτοιου είδους άτομα. Σε αντάλλαγμα οι εκβιαστές συμφωνούν να μην φανερώσουν δημόσια τις ατέλειες των δικτύων των εταιριών που τους επέτρεψαν την παράνομη πρόσβαση Φυσικά ο σημαντικότερος λόγος για τον οποίο οι εταιρίες διστάζουν να οδηγήσουν σε δίκη κάποιο εκβιαστή είναι η δυσφήμιση που θα υποστούν σχετικά με την ασφάλεια τους και επίσης η απειλή περαιτέρω ζημιάς αν δεν ανακαλυφθούν και διορθωθούν οι αδυναμίες στην ασφάλεια .

Πειραματιστές

Αναμφίβολα κάποιες προγραμματιζόμενες απειλές θα γραφτούν από πειραματιστές και περίεργους. Μερικές φορές τα άτομα αυτής της κατηγορίας μπορεί να δημιουργήσουν κάποιο πρόγραμμα που να αποβεί επικίνδυνο λόγω κάποιων προγραμματιστικών λαθών στον κώδικα του ή λόγω αφέλειας ή κακής κρίσης από μέρους τους.

Λαγωνικά δημοσιότητας.

Άλλο μεγάλο κίνητρο μπορεί να είναι το κέρδος, η φήμη ή απλά η ικανοποίηση του εγώ από το κυνηγητό. Σε αυτό το συχνό σενάριο, κάποιος θα συγγράψει έναν ιό, θα τον εξαπολύσει στο διαδίκτυο και μετά θα προσπαθήσει να κερδίσει δημοσιότητα σαν αυτός που τον ανακάλυψε, ή σαν ο πρώτος που θα δημιουργήσει κώδικα που τον απενεργοποιεί, ή απλά να καυχηθεί για το δημιούργημα του σε κάποιο δημόσιο χώρο συνομιλιών στο διαδίκτυο. Αυτού του είδους το σενάριο εμφανίζεται με αυξημένη συχνότητα τελευταία αφού τώρα πια δίνεται μεγάλη έμφαση από τον δημοσιογραφικό τύπο και την τηλεόραση σε τέτοιου είδους γεγονότα.

Πολιτικοί ακτιβιστές.

Ένα στοιχείο με αυξανόμενη συχνότητα στον χώρο της συγγραφής ιών φαίνεται να είναι υποθάλπουσα πολιτική σκοπιμότητα. Οι ιοί σε αυτήν την κατηγορία μεταφέρουν κάποιο είδος πολιτικού μηνύματος είτε σαν κύριο λόγο ύπαρξης τους είτε για αντιπερισπασμό. Αυτό το στοιχείο αναγάγει την συγγραφή ιών σε ένα εργαλείο στα χέρια πολιτικών εξτρεμιστών που ζητάνε

κάποιο κοινό ή ακόμη χειρότερα όταν επιθυμούν την παρενόχληση κυβερνητικών, κοινωνικών ή επιχειρησιακών ιδρυμάτων. Προφανώς η επίθεση στα υπολογιστικά δίκτυα τέτοιων ιδρυμάτων και οργανισμών εξυπηρετεί τους σκοπούς κάποιου μεγαλύτερου πολιτικού σκοπού.

Αφού είδαμε ποιες απειλές αντιμετωπίζει ένα πληροφοριακό σύστημα , ποιοι και με ποια κίνητρα τις επιχειρούν, μένει να δούμε με ποιο τρόπο πραγματοποιούνται αυτές οι απειλές, με άλλα λόγια, τα είδη των επιθέσεων.

Τα είδη των επιθέσεων αφορούν τον τρόπο με τον οποίο οι εισβολείς αποκτούν πρόσβαση και τι γίνεται μόλις την αποκτήσουν. Ακολουθούν οι πιο διαδεδομένοι τρόποι επίθεσης. Παραθέτονται με χρήση αγγλικής γλώσσας, ούτως ώστε να είναι όσο το δυνατόν σωστότερη η απόδοση τους.

1. *Social engineering attacks*

Σε αντίθεση με τις υπόλοιπες μεθόδους επίθεσης , το *Social engineering* δεν αναφέρεται σε τεχνολογικούς χειρισμούς κάποιων αδυναμιών υλικού ή λογισμικού ενός συστήματος και δεν απαιτεί ιδιαίτερες τεχνικές δεξιότητες Απλά εκμεταλλεύεται ανθρώπινες αδυναμίες όπως την απροσεξία και την αφέλεια ή ακόμα και τη διάθεση για συνεργασία. Ορίζεται ως : απόκτηση εμπιστευτικών πληροφοριών με μέσα ανθρώπινης αλληλεπίδρασης. Στη ουσία , κάποιο άτομο με ανεπτυγμένη την ικανότητα της πειθούς καταφέρνει με δόλιο τρόπο κάποιον που βρίσκεται σε καίρια θέση να του αποκαλύψει σημαντικές πληροφορίες για την πρόσβαση στο σύστημα .Όπως για παράδειγμα τους κωδικούς ασφαλείας .Πρόκειται για ιδιαίτερα αποτελεσματική μέθοδο.

2. *DoS attacks*

Οι επιθέσεις DoS είναι μια από τις πιο δημοφιλείς επιλογές για να διακοπεί η λειτουργία ενός δικτύου. Είναι δε αρκετά εύκολο να εκδηλωθούν .Το κατάλληλο λογισμικό είναι διαθέσιμο σε web sites αρκετών hackers και εύκολο να εφαρμοστεί με ελάχιστες τεχνικές γνώσεις.

3. *Scanning and spoofing*

Ο όρος scanning στα πλαίσια της ηλεκτρονικής ασφάλειας αναφέρεται σε λογισμικό πρόγραμμα που χρησιμοποιούν οι hackers για να αναγνωρίσουν ποιες θύρες είναι ανοιχτές σε ένα σύστημα και έτσι ευάλωτες σε επίθεση.(Υπάρχουν 65535 TCP θύρες, και άλλες τόσες UDP που χρησιμοποιούνται από διάφορες εφαρμογές. Αν μια θύρα είναι ανοιχτή αποκρίνεται όταν ένας άλλος υπολογιστής προσπαθεί να επικοινωνήσει μέσω του δικτύου.) Χρησιμοποιούνται επίσης από διαχειριστές δικτύων για να εντοπίσουν τις αδυναμίες και να τις διορθώσουν. Ένα καλό πρόγραμμα scanning μπορεί να εντοπίσει έναν

υπολογιστή στόχο στο INTERNET , να καθορίσει τις εφαρμογές TCP/IP που τρέχουν στον υπολογιστή και να τις ερευνήσουν για αδυναμίες ασφάλειας.

4. *Source routing*

Το TCP/IP υποστηρίζει το source routing το οποίο είναι μια επιλογή που επιτρέπει στο αποστολέα κάποιων δεδομένων να δρομολογήσει τα πακέτα σε ένα συγκεκριμένο σημείο στο δίκτυο. Είναι μια επιλογή στη IP κεφαλίδα που επιτρέπει στον αποστολέα να παραβλέψει τις αποφάσεις δρομολόγησης που φυσιολογικά παίρνονται από τους δρομολογητές πηγής και προορισμού. Είναι ένα εργαλείο των διαχειριστών δικτύων που βοηθά σε περιπτώσεις προβληματικής δρομολόγησης ή όταν χρειάζεται να δρομολογηθεί η κίνηση από κάποια κατεύθυνση πιο αποτελεσματική. Βέβαια χρησιμοποιείται και από hackers καθώς , εάν το σύστημα επιτρέπει αυτήν την λειτουργία, μπορεί να χρησιμοποιηθεί για την πρόσβαση σε ιδιωτικές εσωτερικές διευθύνσεις του LAN κάτι που φυσιολογικά δεν επιτρέπεται.

5. *Software and system exploits*

Επιτρέπουν στους hacker να εκμεταλλευτούν κάποιες αδυναμίες (bugs) συγκεκριμένων λειτουργικών συστημάτων και προγραμμάτων. Χρησιμοποιούνται με σκοπό την απόκτηση μη εξουσιοδοτημένης πρόσβασης σε υπολογιστές και δίκτυα ,ή την κατάρρευση , ή το μπλοκάρισμα συστημάτων ώστε να αρνούνται να παράσχουν υπηρεσίες σε άλλα.

6. *Malware (Trojans, viruses, and worms)* .

Ο συνηθέστερος τύπος malicious software (αλλιώς malware) , είναι ένας ιός, κώδικας που εισβάλει είτε μέσω e-mail attachment είτε μέσω κατεβασμένου αρχείου. Υπάρχουν γενικά τρία είδη ιομορφικού λογισμικού:προγράμματα ιοί, Trojan horses και worms :

Viruses: περιλαμβάνουν κάθε πρόγραμμα που εγκαθίσταται χωρίς την συγκατάθεση του χρήστη και εκτελεί ανεπιθύμητες ενέργειες (συνήθως ζημιογόνες, αν και κάποιες φορές απλά ενοχλητικές.)Μπορούν να αντιγράψουν τον εαυτό τους και να μεταδοθούν μέσω floppy discs ή μέσω δικτύου. Εγκαθίστανται είτε μέσω e-mail attachment είτε ως μακροεντολές σε αρχεία επεξεργαστών κειμένου. Κάποιοι ιοί ενεργοποιούνται με την εγκατάσταση ενώ άλλοι όχι . Υπάρχει πάντως μεγάλη ποικιλία ιών , μπορεί να εμφανίζουν από ένα απλό μήνυμα έως να σβήσουν τα περιεχόμενα του σκληρού δίσκου!

Trojans: Τα Trojans ή αλλιώς Trojan horses (Δούρειοι Ίπποι) εμφανίζονται σαν χρήσιμα προγράμματα όμως στην ουσία πρόκειται για κακόβουλο λογισμικό, είναι «μεταμφιεσμένα» με σκοπό να εξαπατήσουν τον χρήστη. Με την εγκατάσταση τους , ο hacker μπορεί να εκμεταλλευτεί τα κενά ασφάλειας που δημιουργούνται και να αποκτήσει πρόσβαση. Οι δούρειοι ίπποι (προφανής ο λόγος που ονομάστηκαν έτσι) μπορούν επίσης να συντελέσουν στην διαγραφή ή την μετατροπή αρχείων, τη μετάδοση αρχείων και την εγκατάσταση άλλων προγραμμάτων και ιών. Δεν μπορούν να πολλαπλασιαστούν , ωστόσο είναι πολύ επικίνδυνα λόγω του ότι δεν προκαλούν υποψίες.

Worms: Πρόκειται για προγράμματα που ταξιδεύον μέσω του διαδικτύου από πρόγραμμα σε πρόγραμμα. Κάποιες φορές διαφορετικά μέρη ενός worm ("σκουληκιού") τρέχουν σε διαφορετικούς υπολογιστές. Δημιουργούν πολλαπλά αντίγραφα του εαυτού τους και μεταδίδονται μέσω διαδικτύου. Η διαφορά μεταξύ σκουληκιού και ιού είναι πλέον δυσδιάκριτη. Αρχικά ο όρος worm χρησιμοποιήθηκε για να περιγράψει επιθέσεις που γίνονταν σε δίκτυα ενώ ο ιός σε μεμονωμένες επιθέσεις. Πάντως ο πρωταρχικός στόχος των σκουληκιών είναι να πολλαπλασιάζονται και να μεταδίδονται .

2.4 ΤΡΟΠΟΙ ΑΝΤΙΜΕΤΩΠΙΣΗΣ

Η ύπαρξη τόσων πολλών απειλών για κάθε πληροφοριακό σύστημα κάνουν την ανάγκη για λήψη μέτρων προστασίας επιτακτική .Βεβαίως δεν υπάρχει το μαγικό φίλτρο που θα δώσει τη λύση σε όλα και πολύ περισσότερο δεν υπάρχει κοινή λύση για όλους .Για τον οικιακό χρήστη, την μικρή επιχείρηση ή τον κρατικό οργανισμό. Για τον οικιακό χρήστη ένα antivirus και ένα καλό software firewall είναι μάλλον αρκετά. Για τους υπόλοιπους όμως ; Η κάθε επιχείρηση έχει ξεχωριστές ανάγκες για ασφάλεια οι οποίες απαιτούν διαφορετική αντιμετώπιση. Επιβάλλεται λοιπόν πριν γίνει οτιδήποτε να ληφθούν υπόψη τα εξής: ο τύπος και το μέγεθος της επιχείρησης ,ο τύπος των δεδομένων που φυλάσσονται. Ο τύπος των συνδέσεων του δικτύου και τέλος η φιλοσοφία της εταιρείας. Καθένας από αυτούς τους παράγοντες θα καθορίσουν το επίπεδο της επιθυμητής αλλά και απαραίτητης ασφάλειας κατά περίπτωση .Αυτά θα αποτελέσουν τη βάση για τον σχεδιασμό του πλάνου ασφάλειας και τελικά της πολιτικής ασφάλειας που θα ακολουθηθεί. Στην ουσία , Το πλάνο ασφάλειας περιλαμβάνει το σχεδιασμό των διαδικασιών *πρόληψης*, *ανίχνευσης* και *αντίδρασης* .Η

πολιτική ασφάλειας θέτει τους κανόνες βάσει των οποίων εκτελούνται αυτές οι διαδικασίες.

Κάθε πολύ-στρωματικό πλάνο ασφάλειας περιλαμβάνει πολλαπλές μεθόδους ασφάλειας .Πρέπει πάντως να σημειωθεί ότι κάθε μέθοδος είναι απαραίτητη καθώς παίζει σημαντικό ρόλο στην διεκπεραίωση των διαδικασιών πρόληψης , ανίχνευσης και αντίδρασης, στα πλαίσια πάντα της πολιτικής ασφάλειας που έχει εφαρμοστεί. Έχουμε λοιπόν:

ΠΙΣΤΟΠΟΙΗΣΗ . Δεν είναι τίποτα άλλο από τη χρήση κωδικών ασφαλείας ως μέσο επιβεβαίωσης της ταυτότητας για να επιτραπεί η χρήση του συστήματος. Γενικά, όσο πιο αξιόπιστη είναι η μορφή της πιστοποίησης, τόσο πιο περίπλοκη και άβολη είναι για τον χρήστη, και τόσο πιο "επιθετικός" και ριψοκίνδυνος πρέπει να είναι ο εισβολέας για να την παραβιάσει.

ΚΡΥΠΤΟΓΡΑΦΗΣΗ .Είναι μια διαδικασία με την οποία ένα μήνυμα (plain text) μετατρέπεται σε ένα άλλο μήνυμα (cipher text) χρησιμοποιώντας μια μαθηματική συνάρτηση και ένα ειδικό κωδικό κρυπτογράφησης που λέγεται κλειδί (key).Η κρυπτογράφηση μπορεί να παίξει πολύ σημαντικό ρόλο στην καθημερινή χρήση υπολογιστών και πληροφοριακών δικτύων: Μπορεί να προστατεύσει πληροφορίες που βρίσκονται αποθηκευμένες σε υπολογιστικά συστήματα από μη εξουσιοδοτημένη πρόσβαση .Μπορεί να προστατέψει πληροφορίες καθώς αυτές μεταφέρονται. Μπορεί να χρησιμοποιηθεί για να πιστοποιήσει ότι ο δημιουργός ενός αρχείου είναι αυτός που διατείνεται ότι είναι. Η κρυπτογράφηση θεωρείται από πολλούς το υπέρτατο όπλο στον πόλεμο της ασφάλειας. Δεν είναι όμως .Είναι χρήσιμο αλλά έχει και μειονεκτήματα .Δεν μπορεί να αποτρέψει για παράδειγμα την διαγραφή του εγγράφου σε περίπτωση εισβολής.

ΑΝΤΙ-ΙΙΚΟ ΛΟΓΙΣΜΙΚΟ (ANTIVIRUS SOFTWARE) . Την πιο διαδεδομένη άμυνα ενάντια σε σχεδόν όλους τους τύπους κακόβουλου λογισμικού αποτελούν αναμφίβολα τα αντί-ιικά προγράμματα. Ένα τυπικό πρόγραμμα αυτής της κατηγορίας (αφού εγκατασταθεί) δίνει αρκετές επιλογές στον χρήστη του όπως τον έλεγχο των τοπικών μέσων αποθήκευσης για ιούς, δούρειους ίππους κλπ. καθώς επίσης και τον έλεγχο στο δίκτυο με το οποίο είναι συνδεδεμένος ο υπολογιστής . Η βασική φιλοσοφία πίσω από τα αντί-ιικά προγράμματα είναι η εξής: κάθε ιός σαν πρόγραμμα που είναι έχει διαφορετικό κώδικα από όλους τους υπόλοιπους. Το αντί-ιικό πρόγραμμα διαθέτει καταχωρημένα στην βάση δεδομένων του μοναδικά κομμάτια κώδικα που το κάθε ένα αντιστοιχεί σε κάποιον ιό. Αυτά τα κομμάτια λέγονται υπογραφές (signatures) και αποτελούν πλεονέκτημα αλλά και μειονέκτημα για την άμυνα του συστήματος. Πλεονέκτημα γιατί το αντί-ιικό πρόγραμμα μπορεί

να αναγνωρίσει και να "σκοτώσει" με μεγάλη ακρίβεια οποιαδήποτε ιό που είναι καταχωρημένος στην βάση του οπουδήποτε και αν βρίσκεται στο σύστημα. Μειονέκτημα γιατί απλά οποιοσδήποτε ιός δεν είναι καταχωρημένος στην βάση δεν θα ανιχνευθεί με αποτέλεσμα να δώσει λανθασμένο αίσθημα ασφάλειας. Αυτό το πρόβλημα λύνεται με την συνεχόμενη παραγωγή πρόσθετων συμπληρωμάτων (updates) .

FIREWALL: Τα Firewalls είναι ειδικά προγράμματα προστασίας από τα περισσότερα είδη επιθέσεων. Τοποθετούμενα μεταξύ του εσωτερικού και του εξωτερικού δικτύου μιας εταιρίας, παρέχουν ένα απλό τρόπο να ελεγχθεί το μέγεθος και το είδος των μεταφερόμενων πληροφοριών μεταξύ των δύο δικτύων.

ANTI-SPAM: Εργαλεία για να αποτρέψουν τα spam από το να εισβάλουν στο σύστημα ή να αποτρέψουν να χρησιμοποιηθεί το σύστημα για την αναμετάδοσή τους.

VPN: Το VPN είναι ένας τρόπος χρήσης του διαδικτύου για παροχή ασφαλούς πρόσβασης σε ένα κλειστό σύστημα (LAN) , σε χρήστες των οποίων η φυσική θέση είναι μακριά από τις εγκαταστάσεις της εταιρείας όπου βρίσκεται το δίκτυο. Ειδικότερα , πρόκειται για ιδιωτικό δίκτυο δεδομένων που χρησιμοποιεί την διάρθρωση του διαδικτύου . Η βασική ιδέα είναι να δώσει στην εταιρεία που το χρησιμοποιεί τις ίδιες δυνατότητες με μια ιδιωτική μισθωμένη γραμμή , με μικρότερο κόστος .Παρέχει ασφαλές μοίρασμα των δημόσιων πόρων για δεδομένα με τη χρήση τεχνικών κρυπτογράφησης για την εξασφάλιση της πρόσβασης μόνο από εξουσιοδοτημένους χρήστες.

SCANNERS: Προγράμματα ανίχνευσης του δικτύου για αδυναμίες (ανοιχτά ports) που μπορούν να εκμεταλλευτούν επίδοξοι εισβολείς. Διαγνωστικά προγράμματα δικτύου όπως το περίφημο Security Administrator's Tool for Analyzing Networks (SATAN), ή μια UNIX εφαρμογή , περιλαμβάνουν port-scanning δυνατότητες.

INTRUSION DETECTION SYSTEMS: Πρόκειται για εξειδικευμένο εργαλείο ανίχνευσης μη εξουσιοδοτημένης χρήσης ή επίθεσης σε ένα σύστημα ή ένα δίκτυο. Είναι σχεδιασμένο να ανιχνεύει και έπειτα να εκτρέπει ή να αποτρέπει αυτές τις επιθέσεις. Είναι εφαρμογές που μπορεί να διαβάζει και να διερμηνεύει τα περιεχόμενα των αρχείων καταγραφής των firewall ,routers,serves και άλλων συσκευών δικτύου. Επιπλέον ένα IDS δημιουργεί βάση δεδομένων με υπογραφές γνωστών επιθέσεων και τα συγκρίνει με τα στοιχεία από τα αρχεία καταγραφής και να εμφανίζει προειδοποιήσεις όταν χρειάζεται. Διενεργεί για το δίκτυο , κατά αναλογία , ότι για τα αρχεία ένα

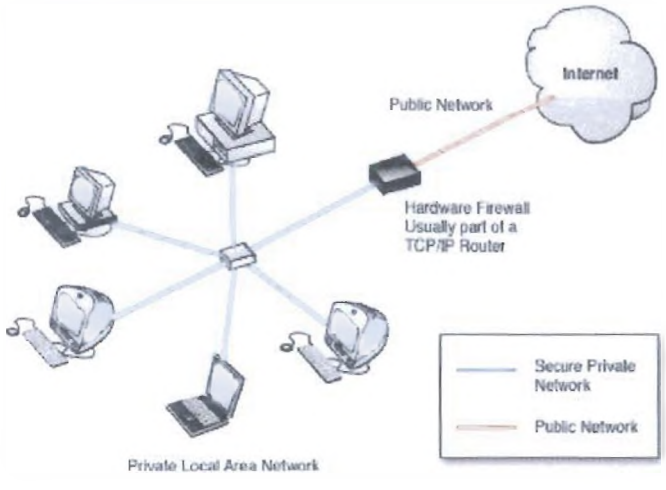
πρόγραμμα antivirus.Τέλος μπορεί να είναι απλά λογισμικό ή να συνδυάζει υλικό με λογισμικό.

2.5 ΓΙΑΤΙ ΕΙΝΑΙ ΑΝΑΓΚΑΙΑ Η ΧΡΗΣΗ FIREWALL .

Μόλις περάσει η αρχική ικανοποίηση για την σύνδεση ενός υπολογιστή ή ενός δικτύου στο διαδίκτυο , γίνεται εύκολα κατανοητό πως , το να έχουμε μια λεωφόρο στην αυλή μας εκτός του ότι μας επιτρέπει να ταξιδέψουμε , επιτρέπει σε μεγάλο αριθμό αγνώστων να έρθει στην αυλή μας. Και όχι πάντα με καλές προθέσεις. Οπωσδήποτε το INTERNET είναι μια θαυμάσια τεχνολογική εξέλιξη που άλλαξε τον τρόπο επικοινωνίας με επαναστατικό τρόπο. Με τον ίδιο επαναστατικό τρόπο όμως επιτρέπει και ανεπιθύμητες επιθέσεις. Το firewall λοιπόν είναι ένας τρόπος προστασίας που επιτρέπει να συνδεθεί ένα δίκτυο στο INTERNET διατηρώντας παράλληλα ένα βαθμό ασφάλειας .Η συχνή παρομοίωση ενός υπολογιστή συνδεδεμένου στο INTERNET με ένα αυτοκίνητο με ανοιχτές τις πόρτες και αναμμένη μηχανή μπορεί να ηχεί ως υπερβολή στα αυτιά ενός μέσου ή έμπειρου χρήστη , δεν απέχει ωστόσο πολύ από την πραγματικότητα. Συχνά τίθεται το ερώτημα : γιατί είναι απαραίτητη η χρήση firewall ; Γιατί είναι η πιο αποτελεσματική μέθοδος σύνδεσης στο διαδίκτυο και παράλληλα διατήρησης ενός επιπέδου ασφάλειας. Σε κάποιες περιπτώσεις, ίσως και η μοναδική. "*Αν είσαι συνδεδεμένος με το INTERNET χρειάζεσαι firewall !* " λένε κατηγορηματικά κάποιοι ειδικοί του χώρου. Η απάντηση είναι αφοπλιστική.

ΚΕΦΑΛΑΙΟ 3^{ο} :ΕΝΝΟΙΑ ΚΑΙ ΧΡΗΣΗ ΤΩΝ FIREWALL

3.1 ΤΙ ΕΙΝΑΙ FIREWALL



Ο όρος firewall ετυμολογικά σημαίνει τείχος φωτιάς, από τις λέξεις fire και wall . Προέρχεται από τον χώρο της κατασκευαστικής βιομηχανίας. Πολλά εργαστήρια, γραφεία και εργοστάσια όταν κατασκευάζονται εξοπλίζονται με firewalls , δηλαδή ειδικά κατασκευασμένους πυρίμαχους τοίχους. Σε περίπτωση που ξεσπάσει μια πυρκαγιά στο κτίριο, είναι πολύ πιθανόν ότι θα είναι εκτός ελέγχου μόνο στο συγκεκριμένο κομμάτι του κτιρίου που ξεκίνησε καθότι τα firewalls θα σταματήσουν ή θα συγκρατήσουν την εξέλιξη της φωτιάς μέχρι να έρθει βοήθεια. Η ίδια ακριβώς φιλοσοφία μπορεί να εφαρμοσθεί και για την προστασία τοπικών δικτύων από εξωτερικές επιθέσεις. Ένα firewall μπορεί να περιορίσει το μέγεθος της ζημιάς: ένας εισβολέας μπορεί να καταφέρει να διεισδύσει σε μια ομάδα μηχανημάτων ενός οργανισμού αλλά το firewall θα προστατεύσει τις υπόλοιπες ομάδες. Τα firewalls είναι πολύ διαδεδομένα σήμερα αφού τώρα πια φαίνεται ότι όλο και κάποια φωτιά θα καίει στο διαδίκτυο...

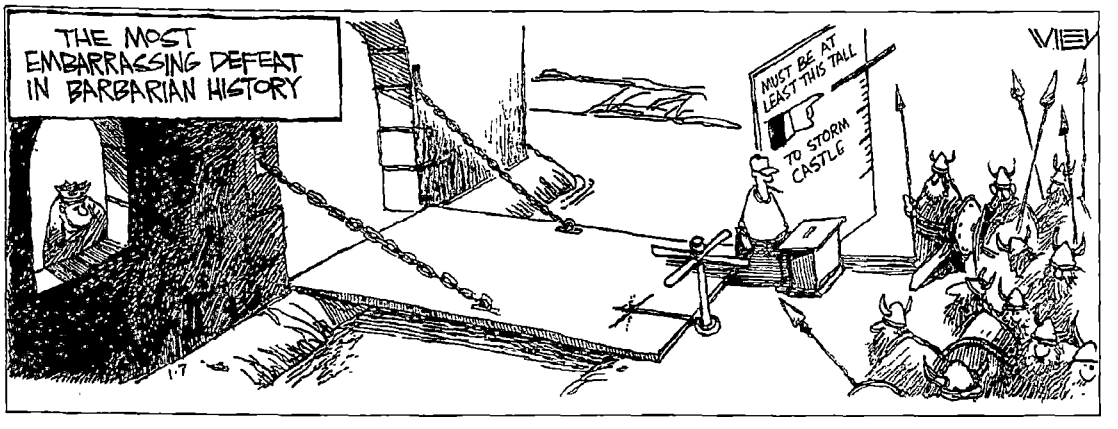
Το firewall είναι ένα σύστημα που επιβάλει πολιτική ελέγχου πρόσβασης μεταξύ δύο δικτύων –όπως μεταξύ ενός ιδιωτικού LAN και του επισφαλούς δημόσιου διαδικτύου. Καθορίζει ποιες εσωτερικές υπηρεσίες μπορούν να προσεγγιστούν από έξω και το αντίστροφο. Τα μέσα με τα οποία αυτό επιτυγχάνεται ποικίλλουν ευρέως , σε γενικές γραμμές πάντως , το

firewall μπορεί να θεωρηθεί ως ένα ζεύγος μηχανισμών : ένας για να εμποδίζει και ένας για να επιτρέπει την κυκλοφορία. Είναι πάντως κάτι παραπάνω από την κλειδωμένη μπροστινή πόρτα σε ένα σύστημα ή δίκτυο – είναι και η φρουρά ασφαλείας του συστήματος.

Ένα firewall για να είναι αποτελεσματικό, όλη η κυκλοφορία δεδομένων θα πρέπει να περνά δια μέσω αυτού ώστε να μπορεί να ελεγχθεί. Για αυτό ακριβώς το λόγο συνήθως εγκαθίσταται στο σημείο όπου το εσωτερικό προστατευμένο δίκτυο συνδέεται με το διαδίκτυο .Το firewall θα πρέπει να επιτρέπει μόνο την εξουσιοδοτημένη πληροφορία να περάσει ενώ το ίδιο θα πρέπει να είναι απρόσβλητο στις επιθέσεις . Είναι φανερό ότι το firewall δεν μπορεί να προσφέρει καμία προστασία αν ο επίδοξος εισβολέας μπορεί να το παρακάμψει χρησιμοποιώντας άλλα συστήματα για την είσοδο του. Παρόλα αυτά το firewall είναι μέρος της γενικής πολιτικής ασφάλειας δεδομένων και δημιουργεί περιμετρική προστασία για τους πόρους ενός οργανισμού.

Λογικά , ένα firewall είναι ένα σύστημα διαχωρισμού, περιορισμού και ανάλυσης. Η φυσική εγκατάσταση του όμως ποικίλλει . Μπορεί να είναι software ή hardware . Συνήθως , πρόκειται για εξοπλισμό που αποτελείται από μια ομάδα συσκευών hardware –ένα router ,έναν υπολογιστή host ή συνδυασμός από routers , υπολογιστές και δίκτυο με το κατάλληλο software.Εξαρτάται πάλι από την πολιτική ασφάλειας που έχει εφαρμοστεί, αλλά και από τα χρήματα που διαθέτει η εταιρεία και από τη φιλοσοφία της στο θέμα της ασφάλειας .Υπάρχει μια θεωρία που υποστηρίζει ότι υπάρχουν δυο αντιπροσωπευτικές φιλοσοφίες στο θέμα της ασφάλειας. Η πρώτη χαρακτηρίζεται από το εξής :*Ότι δεν επιτρέπεται απαγορεύεται.* Η δεύτερη από το :*Ότι δεν απαγορεύεται επιτρέπεται.* Πέρα πάντως από τις υποκειμενικές απόψεις κάθε εταιρείας , υπάρχουν κάποιες δεσμευτικές απαγορεύσεις που πρέπει να περιλαμβάνονται υποχρεωτικά στην πολιτική ασφάλειας αλλιώς δεν έχει νόημα η χρήση του firewall .

3.2 ΣΚΟΠΟΣ ΤΗΣ ΧΡΗΣΗΣ FIREWALL



Στην κατασκευαστική βιομηχανία , το firewall είναι σχεδιασμένο να αποτρέπει την εξάπλωση της φωτιάς από το ένα μέρος του κτιρίου στο άλλο. Θεωρητικά , και το internet firewall εξυπηρετεί παρόμοιο σκοπό : αποτρέπει την εξάπλωση των κινδύνων του INTERNET στο εσωτερικό δίκτυο. Στην πράξη το internet firewall μοιάζει περισσότερο με την τάφρο που υπήρχε γύρω από τα μεσαιωνικά κάστρα παρά με τον πύρινο τοίχο σε ένα μοντέρνο κτίριο . Εξυπηρετεί δε πολλαπλούς σκοπούς .Μπορούν γενικά να κατηγοριοποιηθούν ως εξής.

ΑΠΑΓΟΡΕΥΕΙ ΤΗΝ ΕΙΣΟΔΟ ΣΕ ΠΡΟΣΕΚΤΙΚΑ ΕΛΕΓΧΟΜΕΝΑ ΣΗΜΕΙΑ ΤΟΥ ΣΥΣΤΗΜΑΤΟΣ

ΑΠΟΤΡΕΠΕΙ ΤΟΥΣ ΕΠΙΔΟΞΟΥΣ ΕΙΣΒΟΛΕΙΣ ΝΑ ΠΛΗΣΙΑΣΟΥΝ ΣΤΙΣ ΥΠΟΛΟΙΠΕΣ ΑΜΥΝΕΣ ΤΟΥ ΣΥΣΤΗΜΑΤΟΣ

ΑΠΑΓΟΡΕΥΕΙ ΣΕ ΧΡΗΣΤΕΣ ΝΑ ΑΠΟΜΑΚΡΥΝΘΟΥΝ ΑΠΟ ΠΡΟΣΕΚΤΙΚΑ ΕΛΕΓΧΟΜΕΝΑ ΣΗΜΕΙΑ ΤΟΥ ΣΥΣΤΗΜΑΤΟΣ

Ο σκοπός της χρήσης του firewall είναι , σε γενικές γραμμές ,η προστασία ενός συνδεδεμένου στο INTERNET δικτύου η υπολογιστή. Η διατύπωση πάντως αυτή αναφέρεται στο γενικευμένο θεωρητικό σκοπό. Πιο συγκεκριμένα , ο σκοπός περικλείεται σε αυτά που επιγραμματικά αναφέρονται πιο πάνω. Απαγόρευση εισόδου εξόδου σε / από ελεγχόμενα

σημεία και αποτροπή εισβολής. Οι μέθοδοι με τις οποίες επιτυγχάνεται αναλύονται στην επόμενη ενότητα.

3.3 ΧΡΗΣΕΙΣ ΚΑΙ ΠΕΡΙΟΡΙΣΜΟΙ

3.3.1 ΧΡΗΣΕΙΣ

Οι χρήσεις των firewalls είναι πολυάριθμες και καλύπτουν πολλούς τομείς, τόσους ώστε να ξεφεύγουν από τον πρωταρχικό τους στόχο, την ασφάλεια. Λαμβάνοντας υπόψη ότι το κάθε είδους firewall έχει διαφορετικά χαρακτηριστικά , και ότι δρουν πάντα στα πλαίσια της πολιτικής ασφάλειας που έχει εφαρμοστεί , έχουμε :

Α. Είναι το κέντρο τω αποφάσεων ασφάλειας. Αρκεί να σκεφτούμε το firewall σαν σημείο φραγής. Ολόκληρη η κίνηση εισερχόμενη και εξερχόμενη περνά από αυτό το σημείο .Επομένως , δίνεται η δυνατότητα όλα τα μέτρα ασφάλειας να επικεντρωθούν σε αυτό το σημείο. Το σημείο σύνδεσης με το διαδίκτυο.

Β. Έχει τη δυνατότητα να επιβάλει κάποια πολιτική ασφάλειας. Για παράδειγμα για κάποιες υπηρεσίες του internet μπορεί να μην επιτρέπεται η πρόσβαση σε αυτές από την εφαρμοσμένη πολιτική ασφάλειας. Το firewall έχει τη δυνατότητα να επιτρέπει την κίνηση μόνο σε επιτρεπόμενες υπηρεσίες και να μπλοκάρει τις υπόλοιπες.

Γ. Κάποιες φορές χρησιμοποιείται για να κρατήσει ένα μέρος του συστήματος μακρά από ένα άλλο που ενδεχομένως έχει πληροφορίες μεγαλύτερης αξίας . Με αυτόν τον τρόπο αν κάποιος τομέας δεχθεί επίθεση, η ζημιά να περιοριστεί σε αυτόν και να μην επεκταθεί .

Δ. Κρύβει τις πληροφορίες σχετικά με το δίκτυο κάνοντας να φαίνεται ότι όλη η εξερχόμενη κίνηση προέρχεται από το firewall και όχι από το δίκτυο. Αυτό επιτυγχάνεται με τη χρήση Network Address Translation (NAT) , το οποίο μεταφράζει μια IP διεύθυνση σε μια άλλη.

Ε. Μπλοκάρει εισερχόμενα δεδομένα που μπορεί να περιέχουν μια επίθεση hackers .

Στ. Το firewall είναι το βασικό εργαλείο δημιουργίας συνόρου μεταξύ του δικτύου μας και ενός άλλου δικτύου. Ακριβώς επειδή δημιουργεί μια ξεκάθαρη ανάμεσα στα δυο δίκτυα βοηθά στη διαχείριση της κυκλοφορίας. Βέβαια , το άλλο δεν δίκτυο δεν πρέπει απαραίτητα να είναι το INTERNET . Πολλές φορές βοηθά να χωριστεί κάποιο τμήμα μιας εταιρείας (όπως το λογιστήριο) από το υπόλοιπο δίκτυο της εταιρείας.

Ζ. Παρέχει προστασία απέναντι σε Dos και scanning επιθέσεις. Ένα firewall δρα σαν ένα σημείου που παρακολουθεί όλη την εισερχόμενη και την εξερχόμενη κίνηση. Περιορίζει λοιπόν οτιδήποτε κρίνει απαραίτητο με βάση τις ρυθμίσεις που έχει.

Η. IP και port φιλτράρισμα. Έχει τη δυνατότητα να επιτρέπει ή να απορρίπτει μια σύνδεση με βάση την IP address και το port .

Θ. Φιλτράρισμα περιεχομένου. Μόνο οι proxy servers έχουν την δυνατότητα να διαχειριστούν και να ελέγξουν την κίνηση , με βάση την ανίχνευση URL και του περιεχομένου των σελίδων .Η σωστή χρήση μπορεί να βοηθήσει στον εντοπισμό και στο μπλοκάρισμα ύποπτου περιεχομένου.

Ι. Ενίσχυση της κρυπτογράφησης και της πιστοποίησης . Το firewall έχει τη δυνατότητα να πιστοποιήσει την ταυτότητα χρηστών και να κρυπτογραφήσει μετάδοση μεταξύ αυτού κα firewall άλλου δικτύου.

3.3.2 ΠΕΡΙΟΡΙΣΜΟΙ

Τα firewalls , δεν παρέχουν όλες τις απαραίτητες λειτουργίες ασφάλειας και μάλλον δεν θα έπρεπε. Εξορισμού δεν αποτελούν ολοκληρωμένες λύσεις ασφάλειας , και αυτό πρέπει να γίνει σαφές .Αποτελούν μέρος της ολοκληρωμένης ασφάλειας, δεν την παρέχουν.

Έχουν λοιπόν κάποιες αδυναμίες , κάποια σημεία στα οποία δεν μπορούν να βοηθήσουν.

1.Δεν παρέχουν προστασία από εσωτερικές απειλές. Προστατεύουν από τις απειλές που προέρχονται από εξωτερικούς παράγοντες. Που βρίσκονται εκτός του ιδιωτικού δικτύου. Δεν μπορούν , φυσιολογικά , να αποτρέψουν επιθέσεις που γίνονται από μέσα .Για παράδειγμα από εργαζόμενους , ή από εισβολείς που η είσοδος τους έχει προηγηθεί της εγκατάστασης του firewall .

2. Δεν μπορούν να προστατέψουν διασυνδέσεις που δεν περνούν μέσα από αυτά. Για παράδειγμα , μια σύνδεση εκτός της κανονικής που περνά από το firewall όπως μια dial-up σύνδεση μέσω modem . Σε αυτήν την περίπτωση δεν μπορούν να κάνουν τίποτα. Βεβαίως το πρόβλημα είναι διαχειριστικό και όχι τεχνικό, αφού ευθύνεται αυτός που επέτρεψε αυτήν την σύνδεση και όχι φυσικά το firewall .

3. Δεν προστατεύουν από εντελώς νέες απειλές. Ένα firewall είναι σχεδιασμένο να προστατεύει ενάντια σε γνωστές απειλές. Ενδεχομένως κάποια να προστατεύουν από ορισμένες νέες. Ωστόσο , κανένα δεν μπορεί να προστατεύει αυτόματα από κάθε νέα απειλή που προκύπτει. Συνεχώς αναπτύσσονται νέοι τρόποι επίθεσης , χρησιμοποιώντας πολλές φορές αξιόπιστες μέχρι τότε υπηρεσίες. Δεν είναι δυνατόν να στήσουμε ένα firewall και να περιμένουμε να μας προστατεύει για πάντα.

4. Δεν προστατεύουν πλήρως απέναντι σε ιούς. Ένα firewall δεν μπορεί να κρατήσει έναν ιό μακριά από ένα δίκτυο. Πράγματι , όλα τα firewalls ελέγχουν την εισερχόμενη κυκλοφορία έως ένα βαθμό , και κάποια ίσως να παρέχουν υποτυπώδη προστασία από ιούς .Τα περισσότερα όμως παρέχουν από ελάχιστη έως καθόλου . Ο εντοπισμός ενός ιού σε ένα τυχαίο πακέτο δεδομένων που περνά από το firewall είναι τρομερά δύσκολος γιατί στην ουσία απαιτεί : αναγνώριση ότι το πακέτο είναι μέρος προγράμματος. Προσδιορισμός για το πώς θα έπρεπε να είναι το πρόγραμμα αυτό. Αναγνώριση ότι μια πιθανή αλλαγή στο πρόγραμμα είναι αποτέλεσμα ιού. Ακόμα και το πρώτο από αυτά τα τρία είναι πρόκληση για τα σημερινά firewall! Άλλωστε υπάρχει πιο ενδεδειγμένος τρόπος αντιμετώπισης των ιών, τα antivirus.

5. Κανένα firewall δεν μπορεί να στηθεί μόνο του. Κάθε firewall χρειάζεται οπωσδήποτε ρύθμιση πριν χρησιμοποιηθεί αλλά και στη διάρκεια. Απ' την άλλη , ένα firewall που δεν έχει ρυθμιστεί καλά παρέχει την ψευδαίσθηση ασφάλειας και όχι πραγματική. Πρέπει να γίνει κατανοητό ότι δεν πρόκειται για μαγικές συσκευές που θα δουλεύουν ανεξαρτήτως ρυθμίσεων. Αν τα αντιμετωπίσουμε έτσι όχι μόνο δεν προστατευόμαστε αλλά επιπλέον αυξάνουμε τους κινδύνους .

ΚΕΦΑΛΑΙΟ 4ο : ΤΕΧΝΟΛΟΓΙΕΣ FIREWALL

4.1 SECURITY POLICY

Προτού εξετάσουμε αναλυτικά τις τεχνολογίες και τις αρχιτεκτονικές των firewalls, θα πρέπει πρώτα να αναφερθούμε στον ορισμό της πολιτικής ασφάλειας (security policy) ενός δικτύου. Η ορισμός της πολιτικής αυτής είναι πολύ σημαντικός καθώς καθορίζει τις διαδικασίες και τον σχεδιασμό της προστασίας ενός δικτύου απέναντι σε απώλειες και πιθανές ζημιές.

Μια πολύ καλή προσέγγιση για τη δημιουργία μιας πολιτικής ασφάλειας είναι η προσπάθεια να δοθούν απαντήσεις στις ακόλουθες ερωτήσεις:

- Τι δεδομένα προσπαθούμε να προστατεύσουμε;
- Ποιοι άνθρωποι αποτελούν απειλή για τα δεδομένα μας;
- Πόσο πιθανές είναι οι απειλές;
- Πόσο σημαντικά είναι τα δεδομένα μας;
- Τι μέτρα πρέπει να πάρουμε έτσι ώστε οι τρόποι προστασίας που θα εφαρμόσουμε να μην είναι οικονομικά και χρονικά ασύμφορα;

Ο ορισμός πολιτικής ασφάλειας μπορεί σε απλούς χρήστες-ιδιώτες να μην είναι και τόσο αναγκαίος, αλλά σε επίπεδο οργανισμών και επιχειρήσεων είναι πάγια τακτική, εξαιτίας των ευαίσθητων δεδομένων και των ανταγωνιστικών "μυστικών" που μπορεί να κρύβουν στα δίκτυα τους. Αυτά πρέπει να προστατεύονται από επιθέσεις και "βανδαλισμούς" με την ίδια βαρύτητα που προστατεύεται και η φυσική περιουσία μιας εταιρείας, όπως είναι για παράδειγμα τα κτίρια και ο εξοπλισμός της.

Γενικά, το κόστος της προστασίας των δικτύων θα πρέπει να είναι μικρότερο από το κόστος της ανάκτησης πληροφοριών και δεδομένων από μια ενδεχόμενη απειλή. Αρκετές φορές εταιρείες έχουν παραλύσει για μεγάλο χρονικό διάστημα από επίθεση στο δίκτυο της που προξένησε είτε απώλεια δεδομένων είτε άρνηση του συστήματος σε πρόσβαση στους νόμιμους χρήστες του δικτύου (denial of service). Είναι αναγκαίο να υπάρχει γνώση τι

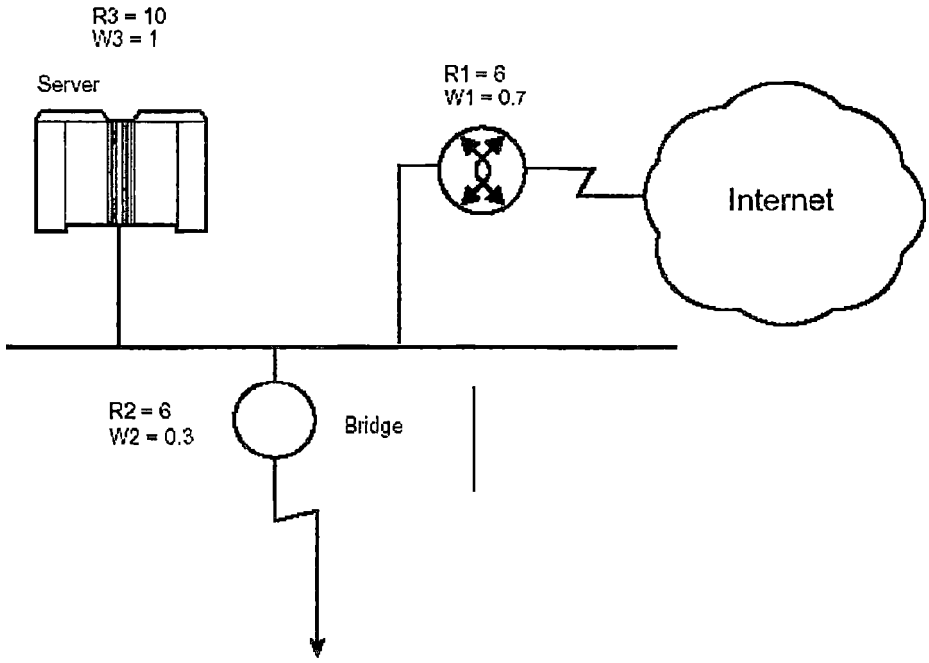
πρέπει να προστατεύεται έτσι ώστε τελικά το επίπεδο ασφαλείας να φθάσει σε ένα πολύ καλό επίπεδο.

Για να σχεδιασθεί σωστά η πολιτική ασφάλειας, θα πρέπει να προηγηθεί πρώτα η ανάλυση των κινδύνων (risk analysis) που διατρέχει ένα δίκτυο. Αυτό προϋποθέτει τον σωστό προσδιορισμό των τμημάτων του δικτύου που απαιτούν ενισχυμένη προστασία σε σύγκριση με κάποια άλλα. Οι κίνδυνοι μπορούν να προσδιοριστούν ποσοτικά με τον ακόλουθο απλό μα συνάμα αποτελεσματικό αλγόριθμο:

$$WR_{source} = W \cdot R$$

όπου:
- R (risk) το ρίσκο ενός συγκεκριμένου τμήματος του δικτύου, με τιμές από 0 έως 10 (το 0 αντιπροσωπεύει μηδενικό κίνδυνο και το 10 μέγιστο κίνδυνο)
- W (weight) το ειδικό βάρος του τμήματος αυτού, με τιμές από 0 έως 1.

Ας εξετάσουμε ένα παράδειγμα, το οποίο απεικονίζεται στο σχήμα 1. Έχουμε ένα απλοποιημένο δίκτυο που αποτελείται από έναν σταθμό εξυπηρέτησης (server), έναν δρομολογητή (router) και μια γέφυρα (bridge). Υποθέτοντας ότι ο server είναι το πιο σημαντικό μέρος του δικτύου, έχει ρίσκο 10 με ειδικό βάρος 1 και το weighted risk ισούται με $10 \cdot 1 = 10$. Ομοίως, για τον δρομολογητή 4,2 και για την γέφυρα 1,8. Έτσι, μπορούμε να έχουμε ένα "πλάνο" του δικτύου μας με weighted risks, αντιστοιχώντας τα σε χαμηλό, μέσο, υψηλό και πολύ υψηλό.



Σχήμα 1

Τέλος, αφού έχει οριστεί κατάλληλα η πολιτική ασφαλείας, επιλέγεται η κατάλληλη τεχνολογία firewall που θα εφαρμοστεί. Αφού ο τομέας του Internet και των δικτύων γενικότερα αλλάζουν δυναμικά μορφή σε σχέση με τον χρόνο, η πολιτική πρέπει να αναθεωρείται διαρκώς, σύμφωνα με τις νέες απαιτήσεις και υπάρχουσες τεχνολογίες, έτσι ώστε τα firewall που θα επιλέγονται να έχουν τα μέγιστα αποτελέσματα.

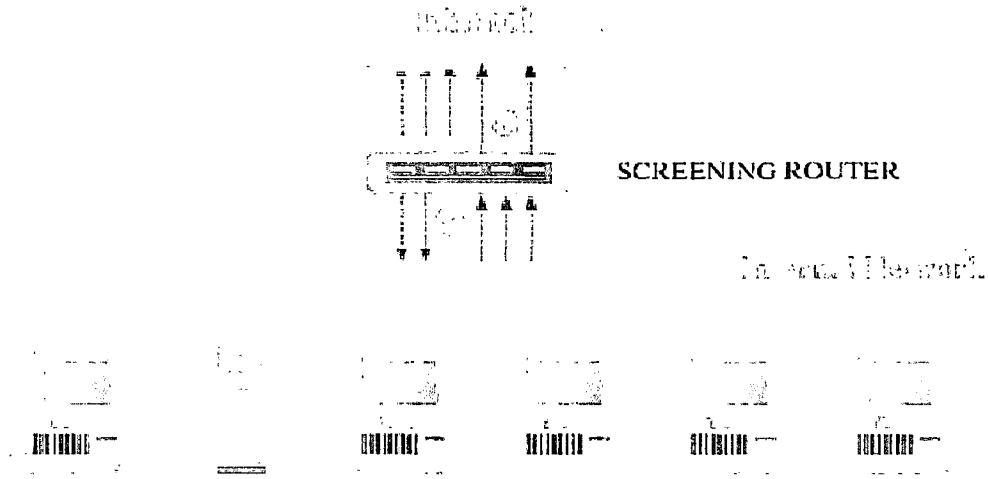
4.2 SCREENING ROUTERS

Αν και οι screening routers ανήκουν θεωρητικά στο κομμάτι των αρχιτεκτονικών firewall, αναφέρονται σε αυτό το σημείο προκειμένου να γίνει πιο εύκολη η περιγραφή της τεχνολογίας packet filtering που αναφέρεται στην συνέχεια.

Οι δρομολογητές (routers) είναι σύνθετες διατάξεις οι οποίες αναπτύχθηκαν από την δεκαετία του 1970 για την υποστήριξη της διασύνδεσης των τοπικών δικτύων. Πολλοί routers που κυκλοφορούν πλέον στο εμπόριο έχουν την δυνατότητα να ελέγχουν τα εισερχόμενα πακέτα ενός δικτύου με βάση κάποια κριτήρια, όπως:

- Τον τύπο πρωτοκόλλου
- Τα πεδία διεύθυνσης πηγής (source address)
- Την διεύθυνση προορισμού (destination address field)

Η ικανότητα αυτή να επιτρέπουν ή να απορρίπτουν εισερχόμενα πακέτα σε ένα δίκτυο από το Internet ή από κάποιο άλλο δίκτυο ονομάζεται packet filtering και οι routers αυτοί ονομάζονται screening routers ή αλλιώς και packet filter routers και αποτελούν ένα δυνατό μηχανισμό ελέγχου της κυκλοφορίας σε ένα δίκτυο, με σχετικά χαμηλό κόστος. Μια απλοποιημένη διάταξη παριστάνεται στο Σχήμα 2



Σχήμα 2

Για την καλύτερη κατανόηση του μηχανισμού του packet filtering, ας εξετάζουμε πρώτα τις διαφορές μεταξύ ενός απλού router και ενός screening router. Ο απλός router απλώς ελέγχει την διεύθυνση προορισμού κάθε πακέτου και επιλέγει τον καλύτερο δρόμο προς την παράδοση του. Οι αποφάσεις σχετικά με την διαχείριση του πακέτου βασίζονται αποκλειστικά από τον προορισμό του. Υπάρχουν δύο πιθανότητες: α) ο router γνωρίζει πώς να στείλει το πακέτο στον προορισμό του και β) ο router δεν γνωρίζει πώς να στείλει το πακέτο στον προορισμό του και επιστρέφει ένα μήνυμα λάθους στην πηγή του πακέτου.

Από την άλλη μεριά, ο screening router εξετάζει το πακέτο πιο προσεκτικά. Πέρα από τις αποφάσεις που παίρνει σχετικά με την προώθηση του πακέτου στον τελικό προορισμό του, ο screening router παίρνει

πρωτοβουλίες σχετικά με το αν "πρέπει" το πακέτο να παραδοθεί, βασιζόμενος βέβαια στην πολιτική ασφαλείας που έχει επιλεγεί για το δίκτυο.

Το packet filtering μπορεί επίσης να εκτελεστεί και από συσκευές οι οποίες δεν έχουν δυνατότητες δρομολόγησης παρά μόνο ελέγχου των πακέτων. Οι συσκευές αυτές ονομάζονται packet filtering bridges και η χρήση τους συναντάται λιγότερο συχνά από τους screening routers εξαιτίας της εξειδικευμένης λειτουργία τους. Οι περισσότεροι κατασκευαστές δικτύων προτιμούν να έχουν routers που παρέχουν προστασία στο δίκτυο παρά να έχουν μια εξειδικευμένη συσκευή που ασχολείται αποκλειστικά με αυτό. Από την άλλη όμως, οι packet filtering bridges παρέχουν περισσότερα πλεονεκτήματα από τους screening routers, καθώς είναι πιο δύσκολο να εντοπιστούν και να δεχτούν επίθεση από κάποιον εισβολέα.

4.3 PACKET FILTERING

4.3.1 ΕΙΣΑΓΩΓΗ

Τα πακέτα μου μεταδίδονται σε ένα δίκτυο αποτελούν τις πρωταρχικές μονάδες επικοινωνίας μεταξύ των κόμβων του δικτύου. Κάθε πακέτο απαρτίζεται από ένα σύνολο επικεφαλίδων (headers), τα οποία εσωκλείουν συγκεκριμένες πληροφορίες. Οι κυριότερες από αυτές είναι:

- Διεύθυνση πηγής IP (IP source address)
- Διεύθυνση προορισμού (IP destination address)
- Πρωτόκολλο (εάν το πακέτο είναι TCP, UDP ή ICMP)
- TCP or UDP source port
- TCP or UDP destination port
- Τύπος μηνύματος ICMP
- Μέγεθος πακέτου

Πέρα από τις επικεφαλίδες των πακέτων, ένας screening router που εκτελεί packet filtering μπορεί να εξετάσει περαιτέρω ένα πακέτο. Αυτό του επιτρέπει να φιλτράρει πακέτα βασισμένα σε πιο λεπτομερής πληροφορίες (όπως είναι για παράδειγμα το όνομα μιας ιστοσελίδας που κάποιος αναζητεί) και να πιστοποιεί ότι τα πακέτα εμφανίζονται να έχουν μορφοποίηση κατάλληλη για την θύρα προορισμού (destination port). Επίσης, ο screening router μπορεί να επιβεβαιώσει αν τα πακέτα είναι έγκυρα (δηλαδή αν το μέγεθος τους αντιστοιχεί στο μέγεθος που αναγράφει η επικεφαλίδα), κάτι που βοηθάει στον εντοπισμό των επιθέσεων βασισμένων σε παραμορφωμένων

πακέτων. Επιπρόσθετα, ο router γνωρίζει πληροφορίες για το πακέτο οι οποίες δεν αντικατοπτρίζονται από αυτό, όπως:

- Το είδος της διεπιφάνειας (interface) στην οποία καταφθάνει το πακέτο
- Το είδος της διεπιφάνειας στην οποία θα αποσταλεί το πακέτο

Τέλος, ο screening router, καταγράφοντας συνεχώς τα πακέτα που έχει "δει", μπορεί να γνωρίζει κάποιες χρήσιμες πληροφορίες, όπως:

- Αν ένα πακέτο αποτελεί απάντηση για ένα άλλο πακέτο
- Πόσα πακέτα έχουν αναγνωριστεί από ή προς τον ίδιο host
- Αν ένα πακέτο είναι ίδιο με κάποιο που έχει κάποιο άλλο που πέρασε στο παρελθόν
- Αν ένα πακέτο είναι μέρος από ένα μεγαλύτερο πακέτο που έχει χωριστεί σε κομμάτια (fragmented packet)

Μόλις λάβει όλες τις πληροφορίες για τα πακέτο, ο screening router μπορεί να κάνει τις ακόλουθες ενέργειες:

- Να στείλει το πακέτο στον αρχικό προορισμό του
- Να εγκαταλείψει το πακέτο, χωρίς να ειδοποιήσει τον αποστολέα
- Να απορρίψει το πακέτο και να στείλει μήνυμα λάθους στον αποστολέα του
- Να καταγράψει πληροφορίες σχετικά με το πακέτο
- Να "θέσει τον συναγερμό" και να ειδοποιήσει άμεσα κάποιον για το πακέτο

Οι πιο εξελιγμένοι routers μπορούν να εκτελέσουν τις ακόλουθες διαδικασίες:

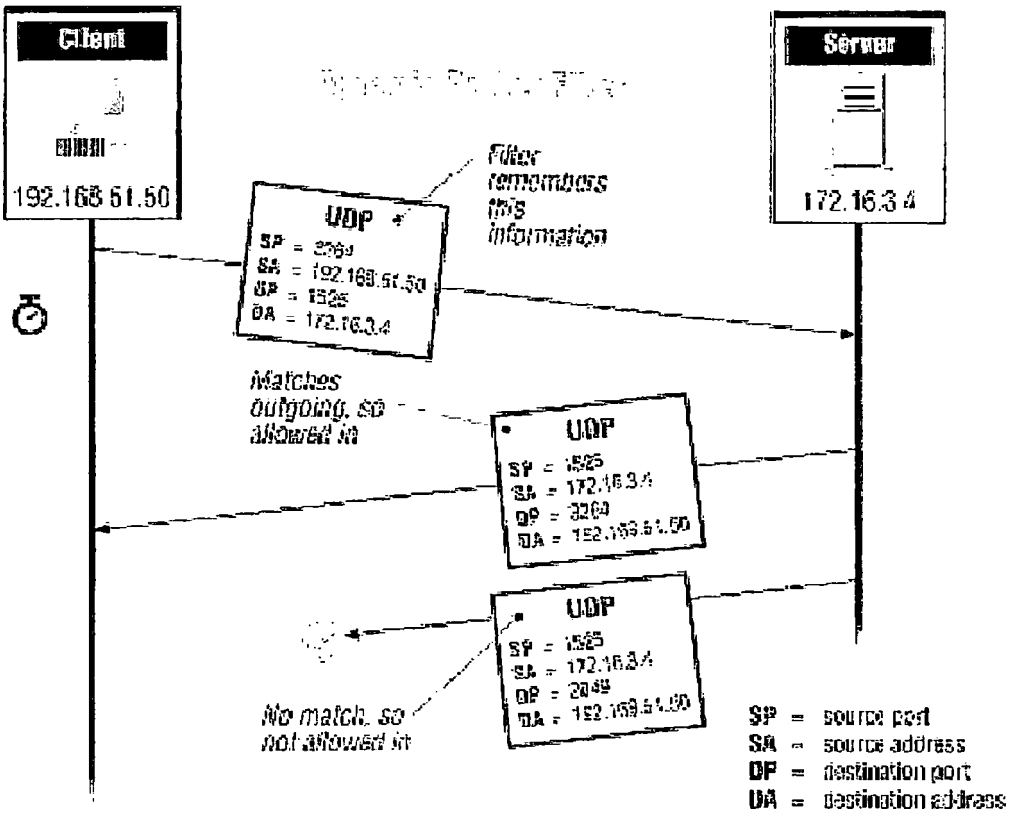
- Να αλλάξει το ίδιο το πακέτο (για παράδειγμα, να εκτελέσει network address translation)
- Να στείλει το πακέτο σε διαφορετικό προορισμό απ' ότι ήταν καθορισμένο να μεταβεί
- Να αλλάξει τους κανόνες φιλτραρίσματος (για παράδειγμα, να αρνηθεί οποιαδήποτε πακέτα που προέρχονται από ένα site που έστειλε επικίνδυνα πακέτα

Παρακάτω αναφέρονται κάποια παραδείγματα σε τρόπους με τους οποίους μπορούμε να προγραμματίσουμε έναν screening router για τη μορφή δρομολόγησης ή όχι πακέτων από και προς ένα δίκτυο.

- Να αποκλείει όλες τις συνδέσεις από συστήματα πέρα του εσωτερικού δικτύου, εκτός από εισερχόμενες SMPT συνδέσεις (έτσι ώστε να μπορεί το δίκτυο να δέχεται μηνύματα ηλεκτρονικού ταχυδρομείου
- Να αποκλείει όλες τις συνδέσεις από συστήματα που δεν εμπιστευόμαστε
- Να επιτρέπει υπηρεσίες FTP και ηλεκτρονικού δικτύου αλλά να αποκλείει επικίνδυνες υπηρεσίες όπως TFTP, RPC και τις "r" υπηρεσίες (rlogin, rsh, rcp κλπ)

4.3.2 STATEFUL & DYNAMIC PACKET FILTERING

Τα πιο εξελιγμένα packet filtering συστήματα προσφέρουν τη δυνατότητα να γίνεται έλεγχος της κατάστασης (state tracking) ή έλεγχος του πρωτοκόλλου (protocol checking). Στον έλεγχος της κατάστασης υπάρχει η δυνατότητα να επιτρέπονται UDP πακέτα τα οποία αποτελούν απάντηση στα εξερχόμενα UDP πακέτα τα οποία έχει "δει" ο packet filter. Αυτή η διαδικασία ονομάζεται stateful packet filtering γιατί ο packet filter αναγκαστικά θα πρέπει να καταγράφει τις καταστάσεις (states) των εισερχόμενων και εξερχόμενων πακέτων. Επίσης η διαδικασία αυτή μπορεί να χαρακτηριστεί και ως dynamic packet filtering εξαιτίας της προσαρμοζόμενης συμπεριφοράς του συστήματος, εξαρτώμενο από την κυκλοφορία που εντοπίζει.



Σχήμα 3. Dynamic Packet Filtering στο UDP layer

Ο έλεγχος της κατάστασης προσφέρει δυνατότητες που άλλα συστήματα δεν παρέχουν αλλά ταυτόχρονα προσθέτει πολυπλοκότητα στο όλο σύστημα. Αφού ο router πρέπει να ελέγχει την κατάσταση κάθε πακέτου, σε περίπτωση μεγάλου φόρτου υπάρχει το ενδεχόμενο υπερφόρτωσης. Αν αυτό συνδυαστεί με ενδεχόμενη επανεκκίνηση του router, τα πακέτα που μπορεί να περνούσαν από τη διαδικασία του φιλτραρίσματος θα απορριφθούν. Επίσης, στην περίπτωση που τα πακέτα διέρχονται διαμέσου πολλών routers, τότε όλοι θα πρέπει να γνωρίζουν πληροφορίες για την κατάσταση. Υπάρχουν βέβαια πρωτόκολλα που μεταδίδουν τέτοιου είδους πληροφορίες, αλλά πάλι η όλη διαδικασία εξακολουθεί να είναι περίπλοκη. Αν ένα δίκτυο έχει πολλούς εφεδρικούς routers για την περίπτωση βλάβης και όλη η κυκλοφορία ελέγχεται από έναν router, τότε η διαδικασία είναι απλή. Όταν όμως χρησιμοποιούνται πολλοί routers ταυτόχρονα, θα πρέπει οι πληροφορίες που αφορούν την κατάσταση να αποστέλλεται σχεδόν ταυτόχρονα γιατί διαφορετικά τα πακέτα θα περνάνε χωρίς ο router να είναι ενημερωμένος για την κατάσταση τους.

Επιπρόσθετα, ο δρομολογητής θα πρέπει να πραγματοποιεί τον έλεγχο της κατάστασης του πακέτου χωρίς να είναι βέβαιος ότι θα

ακολουθήσει ένα αντίστοιχο πακέτο απάντησης. Λαμβάνοντας υπ' όψη ότι ορισμένος αριθμός UDP πακέτων δεν έχουν απάντηση, ο δρομολογητής μπορεί να περιμένει αρκετή ώρα για την απάντηση, προκαλώντας έτσι κυκλοφοριακό φόρτο. Τέτοια φαινόμενα μπορεί να προκληθούν και από το γεγονός ότι αρκετές φορές στο Internet τα απαντητικά πακέτα καθυστερούν σημαντικά να φτάσουν στον προορισμό τους (ο μέσος χρόνος απαντήσεων UDP πακέτων κυμαίνεται στα 5 δευτερόλεπτα, ενώ στο Διαδίκτυο ο αριθμός αυτός μπορεί να φτάσει και τα 15).

Τέτοιου είδους συστήματα packet filtering είναι επίσης ευάλωτα και σε επιθέσεις βασισμένες στην πλαστογράφηση της διεύθυνσης. Σε μια τέτοια περίπτωση, υποκλέπτονται τα εξερχόμενα πακέτα, και συνεπώς η πηγαία διεύθυνση τους, και πλαστογραφούνται έτσι επιτρεπόμενα απαντητικά πακέτα. Παρ' όλα αυτά, η μέθοδος αυτή προσφέρει ασφάλεια για κάποια πρωτόκολλα βασισμένα στο UDP που διαφορετικά θα ήταν δύσκολο να προστατευτούν.

4.3.3 PROTOCOL CHECKING

Ο έλεγχος του πρωτοκόλλου επιτρέπει σε έναν screening router να εκτελεί αποφάσεις που μπορεί να έχουν τη μορφή:

"Να επιτραπούν τα πακέτα που προορίζονται για την DNS θύρα, μόνο αν έχουν τη διαμόρφωση DNS πακέτων".

Ο έλεγχος αυτός βοηθάει στις περιπτώσεις όπου κάποιοι έχουν εγκαταστήσει μια μη ασφαλή υπηρεσία σε μια θύρα, η οποία είναι επιτρεπόμενη από τον δρομολογητή γιατί φαινομενικά ανήκει στην κατηγορία των ασφαλών υπηρεσιών. Ο έλεγχος αυτός μπορεί επίσης να αποτρέψει κάποιες επιθέσεις που αφορούν αποστολή παραμορφωμένων πακέτων σε έναν γνήσιο, αληθή server. Συνήθως, ο έλεγχος πρωτοκόλλου είναι θεμελιώδης και συγκριτικά απλός και μπορεί άνετα να απατηθεί από κάποιον αποφασισμένο χρήστη του εσωτερικού δικτύου, όπως επίσης δεν παρέχει καμία εγγύηση ότι τα πακέτα είναι ασφαλή και συνεπώς θα εντοπίσει ένα σημαντικά μικρό αριθμό επιθέσεων από το εσωτερικό του δικτύου προς άλλους servers. Από την άλλη όμως, ελέγχοντας το πρωτόκολλο, παρέχεται η δυνατότητα ελέγχου λογικής σε ικανοποιητικό επίπεδο.

Τα πιο ανεπτυγμένα συστήματα packet filtering επιτρέπουν κάποιους συγκεκριμένους κανόνες για δημοφιλή πρωτόκολλα, όπως για παράδειγμα η διακοπή κάθε FTP σύνδεσης όπου το username είναι "anonymous" ή η αποτροπή HTTP συναλλαγών σε συγκεκριμένα sites. Προκειμένου να γίνει αυτό, οι packet filters αυτοί θα πρέπει να "κατανοούν" απόλυτα το πρωτόκολλο εφαρμογής. Ορισμένα πρωτόκολλα εμπεριέχουν πληροφορίες που αφορούν το ποιες θύρες θα χρησιμοποιηθούν κατά τις συναλλαγές πληροφοριών. Παράδειγμα αποτελεί το γεγονός ότι το FTP συχνά χρησιμοποιεί μια σύνδεση που η εκκίνηση της έγινε από τον server προς τον client, κατά την οποία και οι δύο διαπραγματεύονται για το πια θύρα θα χρησιμοποιήσουν για την συγκεκριμένη σύνδεση. Ένας stateful packet filter που κατανοεί το FTP πρωτόκολλο μπορεί να παρακολουθήσει την παραπάνω διαπραγμάτευση και να επιτρέψει την εγκαθίδρυση της σύνδεσης, αποτρέποντας όμως κάθε άλλη με την ίδια θύρα.

4.3.4 ΠΑΡΑΜΕΤΡΟΙ ΕΓΚΑΤΑΣΤΑΣΗΣ ΕΝΟΣ PACKET FILTERING ΔΡΟΜΟΛΟΓΗΤΗ

Προκειμένου να εγκατασταθεί επιτυχώς ένας packet filtering δρομολογητής, θα πρέπει να ληφθούν αποφάσεις που σχετίζονται με τις επιθυμητές ή μη υπηρεσίες που θα εκτελούνται και έπειτα να μεταφραστούν οι αποφάσεις αυτές σε κανόνες για τα πακέτα που θα εφαρμοστούν στον δρομολογητή. Τον απλό χρήστη δεν τον απασχολούν οι λεπτομέρειες για τους κανόνες των πακέτων, παρά μόνο η φυσιολογική και ασφαλή εκτέλεση όλων των διαδικασιών δρομολόγησης. Από την άλλη όμως, τον δρομολογητή τον απασχολούν αποκλειστικά και μόνο τα πακέτα, και μάλιστα μόνο συγκεκριμένα κομμάτια από αυτά. Για παράδειγμα, η γενική και καθημερινή εργασία "λήψη και αποστολή e-mail" θα πρέπει να μεταφραστεί στον δρομολογητή σε μια ακριβή περιγραφή συγκεκριμένων πακέτων που θα επιτρέπονται να περάσουν.

Τα πρωτόκολλα είναι συνήθως αμφίδρομα, που σημαίνει ότι όταν κάποιος αποστέλλει μια εντολή ή ένα ερώτημα, η άλλη πλευρά ανταποκρίνεται με κάποιου είδους απάντηση, γεγονός που πρέπει να λαμβάνεται υπ' όψη στην εγκατάσταση κανόνων σε έναν packet filter. Για παράδειγμα, δεν ωφελεί σε τίποτα να επιτρέπονται τα πακέτα που περιλαμβάνουν τους χαρακτήρες που πληκτρολογούμε σε μια Telnet σύνδεση και να απαγορεύονται τα απαντητικά πακέτα που είναι υπεύθυνα για την απεικόνιση στην οθόνη του χρήστη των χαρακτήρων αυτών.

Ένας λόγος ακόμη που αποτρέπει τον αποκλεισμό της μισό μέρος μιας αμφίδρομης σύνδεσης είναι το γεγονός ότι πολλές επιθέσεις μπορούν να πραγματοποιηθούν μόνο με την αποστολή πακέτων στο εσωτερικό του δικτύου, χωρίς να είναι απαραίτητη μια απάντηση. Για παράδειγμα, οι εισβολείς ενδιαφέρονται στο να εκδώσουν μόνο μια συγκεκριμένη εντολή, όπως ο τερματισμός του network interface, για να πετύχουν ένα denial of service χρησιμοποιώντας ένα SNMP πακέτο εντολών, η οποία είτε δεν απαιτεί απαντητικά πακέτα για να πραγματοποιηθεί είτε η απάντηση είναι τόσο προβλεπόμενη ώστε να μη απασχολεί τους εισβολείς. Στην τελευταία περίπτωση, αν και δεν θα υπάρχει το ενδεχόμενο να αποσπαστούν άμεσα πληροφορίες, οι εισβολείς θα μπορούν εκτελέσουν πράξεις οι οποίες προσδίδουν πληροφορίες με έμμεσο τρόπο. Για παράδειγμα, αν και κάποιος δεν μπορεί να δει το αρχείο /etc/passwd άμεσα, θα μπορέσει να εκδώσει άνετα μια εντολή που θα αντιγράφει ένα μήνυμα ηλεκτρονικού ταχυδρομείου.

4.3.5 ΕΝΕΡΓΕΙΕΣ ΤΟΥ ROUTER ΣΧΕΤΙΚΑ ΜΕ ΤΗΝ ΤΥΧΗ ΤΩΝ ΠΑΚΕΤΩΝ

Από την στιγμή που ο packet filtering router έχει τελειώσει με την εξέταση του πακέτου, υπάρχουν δύο βασικοί άξονες που καθορίζουν την τύχη των πακέτων. Ο ένας είναι να επιτρέψει το πακέτο να φτάσει στον τελικό προορισμό του, αφού πληρεί τα κριτήρια, και συνεπώς να εκτελέσει χρέη απλού δρομολογητή και ο άλλος είναι να αποτρέψει το πακέτο να περάσει λόγω κινδύνου στην ασφάλεια του δικτύου.

Ανεξάρτητα με το αν το πακέτο προωθηθεί στον τελικό του προορισμό ή όχι, υπάρχει η δυνατότητα καταγραφής των πράξεων του δρομολογητή (logging). Αυτή η τακτική είναι πολύ χρήσιμη όταν θέλει κάποιος να εξετάσει τον λόγο για τον οποίο κάποια πακέτα απορρίφθηκαν και να "προβλέψει" ενδεχόμενες μελλοντικές επιθέσεις.

Μπορεί κάποιος να συναντήσει πολλούς τρόπους καταγραφής των πακέτων, οι οποίοι εφαρμόζονται ανάλογα με τις δυνατότητες των δρομολογητών. Κάποιοι μπορεί να καταγράψουν μόνο πληροφορίες σχετικά με το πακέτο ενώ μερικοί έχουν τη δυνατότητα να καταγράψουν ολόκληρο το πακέτο που απορρίφθηκε, αποθηκεύοντας το έπειτα σε έναν host μέσω της υπηρεσίας syslog. Ο λόγος που γίνεται η μεταφορά του πακέτου σε κάποιον host είναι ο λιγοστός χώρος που μπορεί να έχει ένας δρομολογητής και, το σημαντικότερο, η μη εναπόθεση επικίνδυνων πακέτων μέσα στον router,

γεγονός που μπορεί να αποβεί μοιραίο σε περίπτωση που το δίκτυο καταληφθεί από εισβολείς.

Όταν ένα πακέτο απορριφθεί, ο router έχει τη δυνατότητα να στείλει στον αποστολέα του πακέτου έναν ICMP κώδικα λάθους, υποδεικνύοντας το σφάλμα που πραγματοποιήθηκε. Αυτός το μήνυμα λάθους προειδοποιεί το αποστολέα να μην ξαναστείλει το ίδιο πακέτο έτσι ώστε να γλιτώσει χρόνο ο απομακρυσμένος χρήστης και να μην επιβαρυνθεί περαιτέρω η κυκλοφορία του δικτύου.

Ένα δεύτερο σετ από ICMP κωδικούς λάθους που μπορεί να επιστρέψει ο δρομολογητής, όπως τα "host administratively unreachable" και "network administratively unreachable" προστέθηκαν αργότερα στην επίσημη ICMP λίστα μηνυμάτων λάθους. Αν και αποτελούν πλέον στάνταρτ, δεν εφαρμόζονται παντού. Θεωρητικά αυτό δεν αποτελεί πρόβλημα όταν ένας host λαμβάνει ένα πακέτο που δεν καταλαβαίνει, αφού έπειτα απλά το αγνοεί. Πρακτικά όμως, υπάρχει το ενδεχόμενο ένα σύστημα να παρουσιάσει σφάλμα εξαιτίας αυτού του πακέτου.

Υπάρχουν πολλοί παράμετροι οι οποίοι πρέπει να ληφθούν υπ' όψη σχετικά με τον αν θα πρέπει ή όχι ένας δρομολογητής να αποστέλλει μηνύματα λάθους. Θα πρέπει να αποφασιστεί τι είδους μήνυμα θα αποστέλλεται, αν υπάρχει η δυνατότητα από τον δρομολογητή να "αντέξει" τον φόρτο της παραγωγής και αποστολής των μηνυμάτων και αν τελικά, τα μηνύματα αυτά προσδίδουν πληροφορίες ζωτικής σημασίας για το packet filter σύστημα μας.

Είναι τεχνικά εσφαλμένο να επιστρέφονται τα "host unreachable" και "network unreachable" μηνύματα, γιατί αφενός ο host μπορεί ή όχι να είναι προσπελάσιμος, ανάλογα με ποια τα υπηρεσία προσπαθεί κάποιος να τον προσεγγίσει. Επίσης, σε πολλά συστήματα τα μηνύματα αυτά μπορεί να προκαλέσουν την απώλεια της σύνδεσης στον απομακρυσμένο host ή δίκτυο. Επιστρέφοντας τους νέους "host administratively unreachable" ή "network administratively unreachable" κώδικες "διαφημίζεται" ότι το σύστημα απαρτίζεται από ένα packet filtering σύστημα, γεγονός που κάποιες φορές είναι επιθυμητό και άλλοτε όχι.

Η παραγωγή και η αποστολή ICMP κωδικών λάθους επιβαρύνει τον packet filtering δρομολογητή. Ένας εισβολέας θα μπορούσε να πραγματοποιήσει μια denial of service επίθεση με το να "πλημμυρίσει" τον δρομολογητή με πακέτα που απορρίπτονται και συνεπώς να τον αναγκάσει να παράγει μηνύματα λάθους, απασχολώντας τον έτσι από τις πρωταρχικές

του packet filtering διαδικασίες του. Πρέπει να αναφερθεί ότι σε αυτό δεν οφείλεται το εύρος ζώνης του δικτύου αλλά μόνο η δύναμη του επεξεργαστή του δρομολογητή. Από την άλλη όμως, αν δεν αποστέλλονται μηνύματα λάθους θα προκαλέσει σημαντική αύξηση στον φόρτο του δικτύου, καθώς το σύστημα που στέλνει το εσφαλμένο πακέτο επαναλαμβάνει συνεχώς την αποστολή του.

Αν ο δρομολογητής επιστρέφει ένα ICMP κώδικα λάθους για κάθε πακέτο που παραβιάζει την πολιτική ασφαλείας ενός δικτύου, ταυτόχρονα προσδίδει σε έναν ενδεχόμενο εισβολέα πληροφορίες για το σύστημα φιλτραρίσματος. Αυτές οι πληροφορίες αφορούν το ποια πακέτα επιτρέπονται από τον packet filter και ποια όχι και έτσι ο εισβολέας μπορεί να καθορίσει σε ποια πρωτόκολλα έχει αδυναμίες ασφαλείας ο σύστημα. Επίσης, η επιστροφή μηνυμάτων λάθους επιταχύνει τα προγράμματα που χρησιμοποιεί ένας εισβολέας, αφού λαμβάνοντας κωδικούς λάθους δοκιμάζει άλλες ρουτίνες και δεν περιμένει για την λήξη χρόνου (timeout).

Λαμβάνοντας υπ' όψη τα παραπάνω δεδομένα μπορεί κάποιος να φτάσει στο συμπέρασμα ότι η ασφαλέστερη τακτική είναι η μη αποστολή ICMP πακέτων λάθους. Εάν ο δρομολογητής σε ένα δίκτυο είναι ευέλικτος, μπορεί να ρυθμιστεί έτσι ώστε να αποστέλλει μηνύματα λάθους στα εσωτερικά συστήματα του δικτύου, για να μπορούν να αναγνωρίσουν ότι κάτι πήγε λάθος και να μην περιμένουν τη λήξη χρόνου, και όχι σε συστήματα εκτός της περιμέτρου, θέτοντας αυτόματα το δίκτυο σε κίνδυνο. Επιπρόσθετα, κάποια packet filtering συστήματα επιτρέπουν τη διακοπή TCP συνδέσεων χωρίς τη χρήση ICMP, απαντώντας με μια επανεκκίνηση TCP και λήγοντας έτσι τη σύνδεση. Αυτή είναι η απάντηση που θα πραγματοποιούσε φυσιολογικά ένα μηχάνημα εάν λάμβανε ένα TCP πακέτο που προοριζόταν για μια θύρα στην οποία κανένας δεν θα το αντιλαμβανόταν. Αν και οι TCP επανεκκινήσεις προσδίδουν λιγότερες πληροφορίες απ' ότι τα ICMP μηνύματα λάθους, επιταχύνουν και αυτές προγράμματα κατασκευασμένα από εισβολείς για τις επιθέσεις τους.

4.3.6 ΑΛΛΑΖΟΝΤΑΣ ΤΟ ΠΑΚΕΤΟ

Πιο εξελιγμένα packet filtering συστήματα μπορούν να εκτελέσουν πιο πολύπλοκες διαδικασίες. Σε αντίθεση με τη διεργασία της δρομολόγησης ή όχι του πακέτου στον τελικό προορισμό του, τα συστήματα αυτά έχουν τη

δυνατότητα να επιλέξουν αν θα δρομολογήσουν το πακέτο σε διαφορετική από την αρχική διεύθυνση, να αλλάξουν την κατάσταση (state change) ή να μεταλλάξουν τα περιεχόμενα του ίδιου του πακέτου.

Ένας packet filter μπορεί να αλλάξει τον προορισμό του πακέτου είτε μεταβάλλοντας τις πληροφορίες δρομολόγησης είτε ενθυλακώνοντας το σε ένα άλλο πακέτο, γεγονός που επιτρέπει στον δρομολογητή να συνεργαστεί με κάποιο άλλο μηχάνημα για να παρέχει τελικά διαφανή proxying.

Όταν ένας stateful packet filter λαμβάνει ένα πακέτο, δεν αποφασίζει μόνο αν θα το εγκαταλείψει ή θα το επιτρέψει, αλλά παίρνει και αποφάσεις που σχετίζονται με την δυναμική αλλαγή της κατάστασης του. Για παράδειγμα, αν ένα πακέτο είναι εξερχόμενο UDP πακέτο, ο δρομολογητής μπορεί να αλλάξει την κατάσταση του ώστε να επιτρέπει απαντητικά πακέτα σε αυτό. Αν ένα πακέτο είναι το πρώτο σε μια TCP σύνδεση (έχει το SYN bit σετ και όχι το ACK), ο packet filter μπορεί να αλλάξει την κατάσταση έτσι ώστε να περιμένει πακέτα με SYN και ACK bit sets. Όταν θα παραλάβει το δεύτερο πακέτο, θα αλλάξει πάλι την κατάσταση ώστε να αναμένει πακέτα με το ACK σετ αλλά όχι το SYN bit σετ. Αυτή η διαδικασία ενδυναμώνει μια TCP σύνδεση και την προστατεύει από επιθέσεις που σχετίζονται με αλλαγές στις επικεφαλίδες των πακέτων.

Μερικά packet filter συστήματα θα μεταβάλλουν, πέρα από την διεύθυνση προορισμού, και μέρος του πακέτου. Η διαδικασία αυτή αποτελεί τη βάση των packet filtering συστημάτων που παρέχουν network address translation.

4.3.7 ΠΛΕΟΝΕΚΤΗΜΑΤΑ ΚΑΙ ΜΕΙΟΝΕΚΤΗΜΑΤΑ ΤΟΥ PACKET FILTERING

Ένα από τα βασικά πλεονεκτήματα του packet filtering είναι ότι ένας στρατηγικά τοποθετημένος packet filtering router μπορεί να βοηθήσει στην προστασία ολόκληρου του δικτύου. Με το να προσθέτουμε σε έναν και μόνο router, ο οποίος είναι υπεύθυνος για τη διασύνδεση του δικτύου μας με το διαδίκτυο, την αρμοδιότητα του packet filter, έχουμε σημαντικό πλεονέκτημα ασφάλειας, ανεξάρτητα από το μέγεθος του δικτύου.

Πέρα από το γεγονός ότι η μέθοδος του packet filtering είναι πολύ αποτελεσματική, είναι και ευρέως διαθέσιμη. Δυνατότητες packet filtering είναι διαθέσιμες σε πολλά hardware ή software προϊόντα δρομολόγησης, τα οποία μπορούν να βρεθούν και δωρεάν από το διαδίκτυο. Επίσης, πολλοί routers που κυκλοφορούν στο εμπόριο έχουν δυνατότητες packet filtering.

Σχήμα 4. Screening router της εταιρείας Netgear

Πέρα όμως από τα πλεονεκτήματα, η τεχνολογία του packet filtering παρουσιάζει και ορισμένα μειονεκτήματα. Αν και, όπως αναφέρθηκε, η τεχνολογία αυτή περιλαμβάνεται σε πολλά hardware και software πακέτα, το packet filtering δεν αποτελεί το "τέλειο" εργαλείο. Παρουσιάζονται κάποιοι περιορισμοί, όπως:

- Οι κανόνες του φιλτραρίσματος που θα εφαρμοστούν είναι δύσκολο να ρυθμιστούν και όταν τελικά συμβεί, είναι δύσκολο να ελεγχθούν
- Οι packet filter δυνατότητες πολλών εμπορικών πακέτων είναι ημιτελής, καθιστώντας την υλοποίηση ορισμένων επιθυμητών τύπων φίλτρων δύσκολη ή και αδύνατη

Όπως είναι λογικό, όταν ένας δρομολογητής είναι υπεύθυνος με την ευθύνη του packet filtering, ο φόρτος εργασίας του αυξάνεται κατακόρυφα, μειώνοντας την απόδοση του σε αισθητά επίπεδα. Αυτό συμβαίνει κυρίως εξαιτίας της έλλειψης στρατηγικής caching του router, που χρησιμοποιείται συνήθως για θέματα βελτίωσης της απόδοσης. Για παράδειγμα, η εταιρεία Cisco ανέπτυξε την τεχνική "fastpatch", στην οποία οι βασικές λειτουργίες που έχουν σχέση με το packet filtering βασίζονται στην interface κάρτα. Όταν όμως υπάρχει απαίτηση για εξελιγμένες λειτουργίες φιλτραρίσματος, καταναλώνεται και αρκετή υπολογιστική ισχύς, μειώνοντας έτσι την συνολική απόδοση.

Οι πληροφορίες που έχει στην διάθεση του ένας packet filter router δεν μας επιτρέπει να εφαρμόσουμε κάποιους συγκεκριμένους κανόνες ασφαλείας που επιθυμούμε. Για παράδειγμα, τα πακέτα μας πληροφορούν από ποιον host έχουν προέλθει, όχι όμως και από ποιον χρήστη. Συνεπώς, είναι αδύνατη η εφαρμογή περιορισμών για συγκεκριμένους χρήστες. Το πρόβλημα αυτό μπορεί να περιοριστεί με κάποιους πιο εξελιγμένους packet filters, με κόστος όμως κάποιων πλεονεκτημάτων του "απλού" packet filtering. Για

παράδειγμα, ένας packet filter μπορεί να απαιτεί την αυθεντικοποίηση των χρηστών πριν στείλουν κάποιο πακέτο και έπειτα να φιλτράρει πακέτα βάση του ονόματος χρήστη, αφαιρώντας όμως έτσι τα πλεονεκτήματα της διαφάνειας των μεθόδων packet filtering.

4.4 PROXY SERVICES

4.4.1 ΕΙΣΑΓΩΓΗ

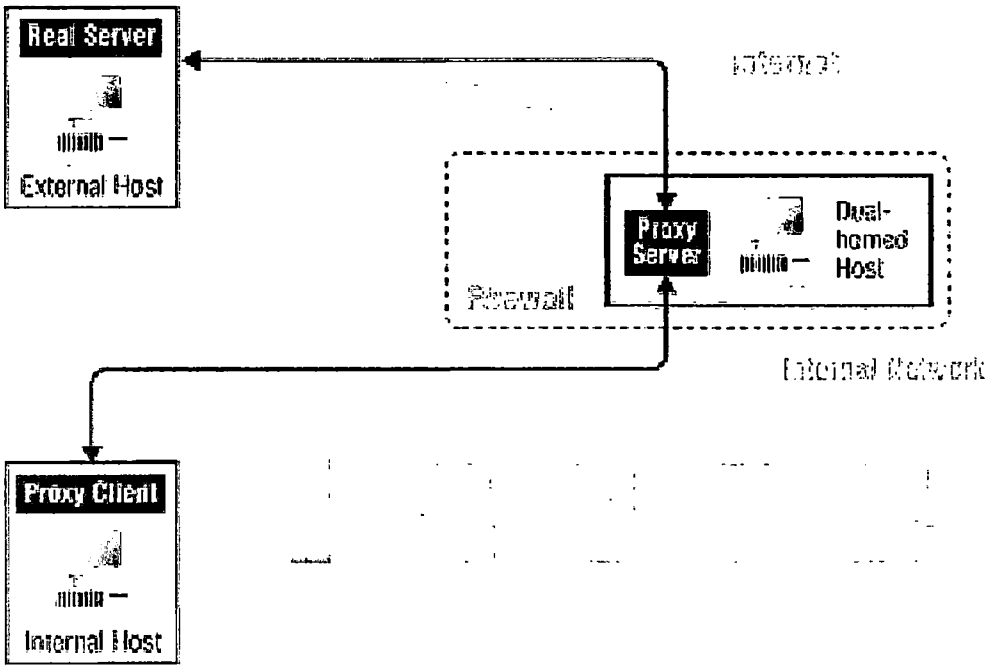
Γενικά, proxy είναι κάτι ή κάποιος που εκτελεί κάποια διαδικασία για τον λογαριασμό κάποιου άλλου. Οι proxy υπηρεσίες είναι εξειδικευμένες εφαρμογές ή προγράμματα σταθμών εξυπηρέτησης τα οποία λαμβάνουν αιτήματα χρηστών για υπηρεσίες Internet (όπως FTP και Telnet) και τα προωθούν στις πραγματικές τους υπηρεσίες. Οι proxies παρέχουν αντικατάσταση των συνδέσεων και λειτουργούν ως gateways για τις υπηρεσίες. Για αυτόν τον λόγο, πολλές φορές οι proxies ονομάζονται και application-level gateways. Όταν στη συνέχεια θα αναφέρεται ο όρος proxies, θα εννοούνται οι proxies που εκτελούνται για λόγους ασφάλειας, και δρουν σε έναν firewall host (είτε σε έναν dual-homed host με ένα interface στο εσωτερικό δίκτυο και ένα στο εξωτερικό δίκτυο, είτε σε έναν bastion host ο οποίος έχει πρόσβαση στο διαδίκτυο και είναι προσβάσιμος εσωτερικά από το δίκτυο).

Οι proxy services τοποθετούνται μεταξύ ενός "εσωτερικού" χρήστη (εσωτερικού δικτύου) και μιας "εξωτερικής" υπηρεσίας (Internet). Αντί να υπάρχει απευθείας επικοινωνία, και οι δύο απευθύνονται στον proxy. Οι proxies διαχειρίζονται επικοινωνιακά ζητήματα μεταξύ χρηστών και υπηρεσιών Internet, σε "παρασκηνιακό" επίπεδο.

Η διαφάνεια (transparency) είναι ουσιαστικά το βασικό κλειδί επιτυχίας των proxy services. Για έναν χρήστη, ένας proxy server του παρέχει την ψευδαίσθηση ότι συναλλάσσεται απευθείας με τον πραγματικό server. Για τον πραγματικό server υπάρχει η ψευδαίσθηση ότι συναλλάσσεται απευθείας με τον χρήστη.

Για την καλύτερη κατανόηση της λειτουργίας των proxy services εξετάζουμε την ακόλουθη απλή περίπτωση (Σχήμα 3), όπου προσθέσαμε proxy υπηρεσίες σε έναν dual-homed host. Όπως δείχνει και το σχήμα, οι

proxy services απαιτούν έναν proxy server και έναν proxy client. Ο proxy client είναι μια ειδική, τροποποιημένη έκδοση του κανονικού client προγράμματος (όπως ένας Telnet ή FTP client) ο οποίος "συνομιλεί" με τον proxy server και όχι με τον κανονικό. Έπειτα, ο proxy server κρίνει τα αιτήματα του proxy client και αποφασίζει ποια να επιτρέψει και ποια να απορρίψει. Αν ένα αίτημα επιτραπεί, ο proxy server επικοινωνεί με τον πραγματικό server (εξού και ο όρος proxy),όπου και προωθεί τελικά το αίτημα και αντίστροφα.



Σχήμα 5

Ο σκοπός του proxy server δεν είναι απλώς να προωθεί αιτήματα χρηστών στις πραγματικές διαδικτυακές υπηρεσίες. Μπορεί να ελέγχει τις πράξεις των χρηστών γιατί παίρνει δυναμικές αποφάσεις σχετικά με τα αιτήματα που επεξεργάζεται. Ανάλογα με την πολιτική ασφάλειας που έχει επιβληθεί, τα αιτήματα μπορεί να επιτρέπονται ή να απορρίπτονται. Για παράδειγμα, το FTP proxy μπορεί να μην επιτρέπει σε χρήστες να εξάγουν αρχεία ή να μην τους επιτρέπει να εισάγουν αρχεία από συγκεκριμένα sites. Πιο εξελιγμένα proxy services έχουν την δυνατότητα να επιτρέπουν διαφορετικές δυνατότητες σε διαφορετικούς hosts, παρά να εφαρμόζουν τους ίδιους περιορισμούς σε όλους.

Οι περισσότεροι proxy servers χρησιμοποιούνται για να ελέγχουν και να βελτιστοποιούν εξωτερικές συνδέσεις. Επίσης, είναι δυνατό να χρησιμοποιηθούν proxy συστήματα και για τον έλεγχο εσωτερικών συνδέσεων

στους servers (όπως για παράδειγμα να εξισορροπεί συνδέσεις μεταξύ πολλαπλών server). Η διαδικασία αυτή ονομάζεται πολλές φορές και reverse proxying.

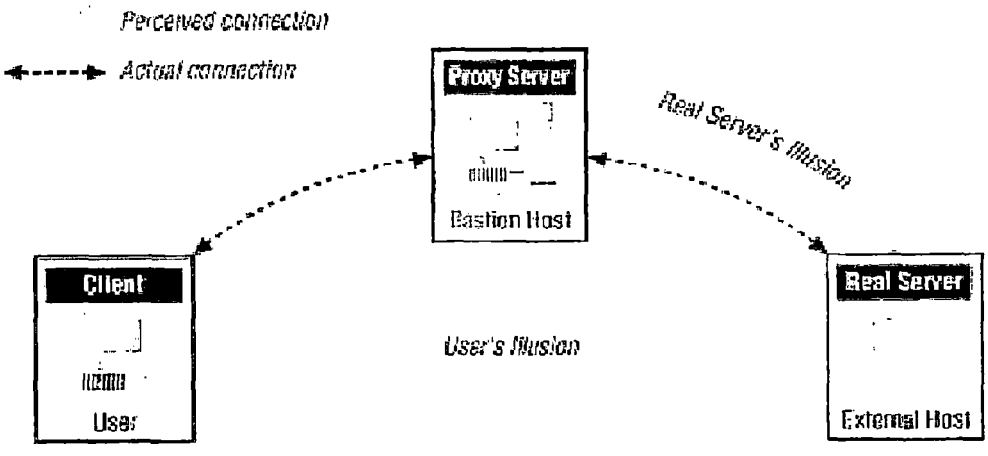
4.4.2 ΟΙ ΛΟΓΟΙ ΓΙΑ ΤΟΥΣ ΟΠΟΙΟΥΣ ΕΠΙΛΕΓΟΥΜΕ PROXIES

Δεν υπάρχει κανένας λόγος να διασυνδεθεί ένα δίκτυο με το Internet αν οι χρήστες του δεν έχουν πρόσβαση σ' αυτό. Από την άλλη, δεν νοείται ασφάλεια στο διαδίκτυο αν μεταξύ του Internet και κάθε host σε ένα δίκτυο υπάρχει ελεύθερη πρόσβαση. Συνεπώς είναι αναγκαίο να βρεθεί μια συμβιβαστική λύση.

Ο πιο προφανής συμβιβασμός που μπορεί να πραγματοποιηθεί είναι η παροχή ενός και μοναδικού host με πρόσβαση στο Internet για όλους τους χρήστες. Αυτή όμως δεν είναι ικανοποιητική λύση εξαιτίας του γεγονότος ότι αυτοί οι hosts δεν είναι διαφανείς στους χρήστες, οι οποίοι δεν μπορούν να έχουν άμεση πρόσβαση σε υπηρεσίες δικτύου. Θα πρέπει να εκτελούν login και να εκτελούν όλες τις εργασίες τους στον dual-homed host και έπειτα με κάποιο τρόπο να μεταφέρονται τα αποτελέσματα στους υπολογιστές τους. Στην καλύτερη των περιπτώσεων, οι πολλαπλές αυτές μεταφορές των πληροφοριών είναι τουλάχιστον ενοχλητικές για τους χρήστες, που έχουν συνηθίσει να εργάζονται με διαφορετικό τρόπο. Το πρόβλημα αυτό είναι χειρότερο σε δίκτυα με πολλαπλά λειτουργικά συστήματα. Εάν φερειπήν ένας χρήστης εργάζεται σε Macintosh και ο dual-homed host τρέχει σε Unix, θα δυσκολευτεί πάρα πολύ να εκτελέσει εργασίες μέσω του host, αφού τα εργαλεία είναι εντελώς διαφορετικά.

Οι dual-homed hosts χωρίς proxies τείνουν να ενοχλούν τους χρήστες και να μειώνουν την αποτελεσματικότητα των χρηστών, όσο αφορά τις εργασίες τους στο διαδίκτυο. Ακόμη χειρότερα, δεν προσφέρουν συνήθως και ικανοποιητική ασφάλεια. Είναι σχεδόν αδύνατο να ασφαλιστεί ένα μηχάνημα με πολλούς χρήστες, και ειδικά αυτούς που αποκλειστικά επιθυμούν να έχουν πρόσβαση στον εξωτερικό κόσμο. Επίσης, δεν έχει νόημα να αποκλειστούν εργαλεία συναλλαγής με το Internet γιατί οι χρήστες πάντα θα έχουν τη δυνατότητα να μεταφέρουν τα δικά τους όμοια εργαλεία από τους υπολογιστές τους. Για παράδειγμα, δεν μπορεί να εγγυηθεί κανένας ότι σε έναν dual-homed host θα καταγράφονται οι μεταφορές αρχείων γιατί οι χρήστες μπορούν να μεταφέρουν τους δικούς τους agents οι οποίοι δεν απαιτούν logging.

Τα proxy συστήματα δεν μπερδεύουν τους χρήστες, αφού αυτοματοποιούν τις συναλλαγές με τον host, και αποφεύγουν την ανασφάλεια που παρέχει ενός dual-homed host. Αντί να απαιτούν από τους χρήστες να συναλλάσσονται απ' ευθείας με τον host, το proxy συστήματα επιτρέπουν οι συναλλαγές να εκτελούνται "παρασκηνιακά". Έτσι, ο χρήστης έχει την ψευδαίσθηση ότι συναλλάσσεται με άμεσο ή σχεδόν άμεσο τρόπο με τον διακομιστή στο Internet. Το σχήμα απεικονίζει τη διαφορά μεταξύ πραγματικότητας και ψευδαίσθησης με τα proxy συστήματα.



Σχήμα 6

Τα proxy συστήματα αντιμετωπίζουν προβλήματα ασφάλειας με το να αποτρέπουν τους χρήστες να πραγματοποιούν logins στον dual-homed host και να οδηγούν τις συνδέσεις μέσα από ελεγχόμενο λογισμικό. Επίσης, είναι αδύνατο για κάποιον χρήστη να εγκαταστήσει ανεξέλεγκτα λογισμικό, αφού ο proxy δρα σαν σημείο ελέγχου.

4.4.3 Η ΛΕΙΤΟΥΡΓΙΑ ΤΩΝ PROXIES

Οι λεπτομέρειες των ρυθμίσεων λειτουργίας των proxies διαφέρουν από υπηρεσία σε υπηρεσία. Κάποιες υπηρεσίες παρέχουν proxying εύκολα ή αυτόματα. Για τις περισσότερες όμως, απαιτείται το κατάλληλο proxy server λογισμικό στον διακομιστή. Όσο αφορά την πλευρά του client, απαιτούνται τα εξής:

- Proxy-aware application software

Με αυτή την προσέγγιση, το λογισμικό θα πρέπει να γνωρίζει πως να επικοινωνεί με τον proxy server αντί του πραγματικού όταν ένας χρήστης πραγματοποιεί ένα request, όπως FTP ή Telnet, και πως να προστάξει τον proxy server με ποιόν πραγματικό διακομιστή να συνδεθεί.

- Proxy-aware operating system software

  Στην περίπτωση αυτή, το λειτουργικό σύστημα που είναι εγκατεστημένο στον client είναι τροποποιημένο με τέτοιο τρόπο έτσι ώστε οι IP συνδέσεις ελέγχονται για το αν θα πρέπει να αποσταλούν στον proxy server. Ο μηχανισμός αυτός συνήθως εξαρτάται από dynamic runtime linking (την ικανότητα δηλαδή να παρέχονται βιβλιοθήκες όταν εκτελείται μια εφαρμογή). Ο μηχανισμός αυτός δεν λειτουργεί πάντα και μπορεί να αποτυγχάνει με τρόπους μη προφανείς στους χρήστες.

- Proxy-aware user procedures

  Με την προσέγγιση αυτή, ο χρήστης χρησιμοποιεί client λογισμικό το οποίο δεν κατανοεί λειτουργίες proxying προκειμένου να επικοινωνήσει με τον proxy server και δίνει εντολή στον proxy να συνδεθεί αυτός με τον πραγματικό διακομιστή και όχι του λογισμικό του client.

- Proxy-aware router

  Εδώ, καμία αλλαγή δεν πραγματοποιείται από την πλευρά του client. Ένας δρομολογητής συλλαμβάνει την σύνδεση και την κατευθύνει στον proxy server, γεγονός που απαιτεί βέβαια έναν "έξυπνο" router.

4.4.3.1 ΧΡΗΣΙΜΟΠΟΙΩΝΤΑΣ PROXY-AWARE APPLICATION SOFTWARE

Οι κατάλληλες proxy-aware εφαρμογές είναι αρκετά συχνά διαθέσιμες μόνο για συγκεκριμένες πλατφόρμες. Για παράδειγμα, το Igateway πακέτο που δημιουργήθηκε από την Sun είναι ένα proxy πακέτο για FTP και Telnet, το οποίο όμως χρησιμοποιείται μόνο σε μηχανήματα Sun, όπως το Solaris, και παρέχει μόνο precompiled binaries της Sun. Συνεπώς, αν κάποιος επιθυμεί να χρησιμοποιήσει proxy εφαρμογές, θα πρέπει να κάνει πρώτα έναν έλεγχο συμβατότητας με τις διαθέσιμες πλατφόρμες της αγοράς.

Ακόμα και στην περίπτωση που το λογισμικό υποστηρίζεται από την πλατφόρμα, δεν σημαίνει ότι και είναι επιθυμητό και από τους χρήστες. Για παράδειγμα, πολλά FTP προγράμματα υπάρχουν διαθέσιμα για τον Macintosh. Κάποια από αυτά διαθέτουν εντυπωσιακό γραφικό περιβάλλον ενώ κάποια άλλα διαθέτουν πολύ χρήσιμες επιλογές, όπως το να επιτρέπουν στον χρήστη να αυτοματοποιεί τις συναλλαγές. Όπως είναι φυσικό, όταν ένας χρήστης χρησιμοποιεί έναν client που δεν υποστηρίζει τον εγκατεστημένο proxy server μηχανισμό παρουσιάζονται πολλά προβλήματα. Σε τέτοιες περιπτώσεις, μια λύση είναι η μετατροπή του ίδιου του client έτσι ώστε να υπάρχει συμβατότητα, γεγονός όμως που απαιτεί ότι είναι διαθέσιμος ο πηγαίος κώδικας του client καθώς και τα κατάλληλα εργαλεία για να ξαναγίνει compilation. Δυστυχώς όμως, πολύ λίγα προγράμματα συνοδεύονται από τον κώδικα τους, που συνήθως τοποθετούνται στην κατηγορία των open source εφαρμογών. Εξαίρεση στον κανόνα αυτόν είναι οι φυλλομετρητές Netscape Navigator, Internet Explorer και Lynx. Τα προγράμματα αυτά υποστηρίζουν διαφόρων ειδών proxies (όπως SOCKS και HTTP) και είναι κατασκευασμένα μετά από την εγκαθίδρυση των firewalls και proxy συστημάτων στο διαδίκτυο.

Διαπράττοντας αλλαγές στις proxying εφαρμογές δεν σημαίνει και ότι η όλη διαδικασία είναι κατανοητή και διαφανής στους χρήστες. Μετά την πραγμάτωση της αλλαγής, το πρόγραμμα πρέπει πάλι να ρυθμιστεί ώστε να χρησιμοποιεί τον κατάλληλο proxy διακομιστή και γενικά να χρησιμοποιείται μόνο στις περιπτώσεις που απαιτείται πραγματικά proxying. Αν και μερικές εφαρμογές παρέχουν κάποιους είδους βοήθεια στον χρήστη αυτοματοποιώντας κάπως την διαδικασία, η κακή ρύθμιση και αλλαγή των proxy εφαρμογών αποτελεί μέχρι και σήμερα από τα πιο κοινά χρηστικά προβλήματα που συναντώνται σε δίκτυα που χρησιμοποιούν proxies.

4.4.3.2 ΧΡΗΣΙΜΟΠΟΙΩΝΤΑΣ PROXY-AWARE OPERATING SYSTEM SOFTWARE

Αντί για αλλαγή της εφαρμογής, μπορεί να κάποιος να μεταβάλλει το περιβάλλον γύρω από την εφαρμογή έτσι ώστε όταν η εφαρμογή προσπαθεί να εγκαθιδρύσει μια σύνδεση, πραγματοποιούνται αλλαγές για να συμπεριληφθεί αυτόματα, στην περίπτωση που χρειαστεί, και ο proxy server. Αυτό επιτρέπει στις εφαρμογές που δεν έχουν υποστεί καμία αλλαγή να χρησιμοποιηθούν σε proxy περιβάλλοντα. Η εφαρμογή των κανόνων αυτών διαφέρει από πλατφόρμα σε πλατφόρμα. Όταν υπάρχουν ήδη δυναμικές, συνδεδεμένες μεταξύ τους, βιβλιοθήκες, απλώς προσθέτεται μια ακόμη, ενώ

όταν δεν είναι διαθέσιμες, απαιτείται η επανεγκατάσταση των οδηγών του δικτύου.

Και στις δύο περιπτώσεις όμως, υπάρχει το ενδεχόμενο να παρουσιαστούν προβλήματα και επιπλοκές. Εάν οι εφαρμογές συμπεριφέρονται απρόσμενα, μπορεί να προσπεράσουν την proxying διαδικασία ή να σταματήσουν εξαιτίας της. Μερικοί παράγοντες που προκαλούν προβλήματα είναι λογισμικό ποτ είναι στατικά συνδεδεμένο με άλλα προγράμματα, λογισμικό που παρέχει τις δικές του δυναμικές βιβλιοθήκες για λειτουργίες του δικτύου, πρωτόκολλα που χρησιμοποιούν προκαθορισμένες και αμετάβλητες IP διευθύνσεις και αριθμούς θυρών και τέλος, λογισμικό που προσπαθεί να διαχειριστεί σε χαμηλό επίπεδο τις συνδέσεις.

4.4.3.3 ΧΡΗΣΙΜΟΠΟΙΩΝΤΑΣ PROXY-AWARE ΔΙΑΔΙΚΑΣΙΕΣ ΧΡΗΣΤΗ

Με την προσέγγιση αυτή, οι proxy servers σχεδιάζονται έτσι ώστε να συνεργάζονται με προκαθορισμένο λογισμικό client και απαιτούν συνεπώς από τους χρήστες να εκτελούν αυστηρά καθορισμένες διαδικασίες. Ο χρήστης δίνει εντολή στον client να συνδεθεί με τον proxy server ο οποίος έπειτα παίρνει εντολή να συνδεθεί με έναν συγκεκριμένο host. Επειδή λίγα πρωτόκολλα είναι σχεδιασμένα να μεταβιβάζουν τέτοιου είδους πληροφορίες, ο χρήστης όχι μόνο είναι αναγκασμένος να θυμάται το όνομα του proxy server αλλά και τα μέσα τα οποία χρησιμοποιούνται για να διαβιβαστεί και το όνομα του άλλου host.

Προκειμένου να εξεταστεί ο συγκεκριμένος τρόπος λειτουργίας, ας εξετάσουμε ένα παράδειγμα. Έστω ότι κάποιος χρήστης θέλει να παραλάβει ένα αρχείο από ένας ανώνυμο FTP διακομιστή (έστω τον ftp.downloads.com). Οι διαδικασίες τις οποίες ακολουθεί ο χρήστης είναι οι εξής:

1. Χρησιμοποιώντας έναν FTP client, συνδέεται με τον proxy server (που πιθανώς τρέχει στον bastion host – την πύλη για το Internet) αντί να συνδεθεί απ΄ ευθείας με τον ανώνυμο FTP server.

2. Όταν του ζητηθεί το όνομα χρήστη, θα πρέπει να το προσδιορίσει και γράψει και το όνομα του πραγματικού server που θέλει να συνδεθεί. Εάν θέλει να έχει πρόσβαση στον ανώνυμο FTP διακομιστή, αντί να γράψει στο prompt του proxy server το "anonymous", θα πρέπει να δώσει το "anonymous@ftp.download.com".

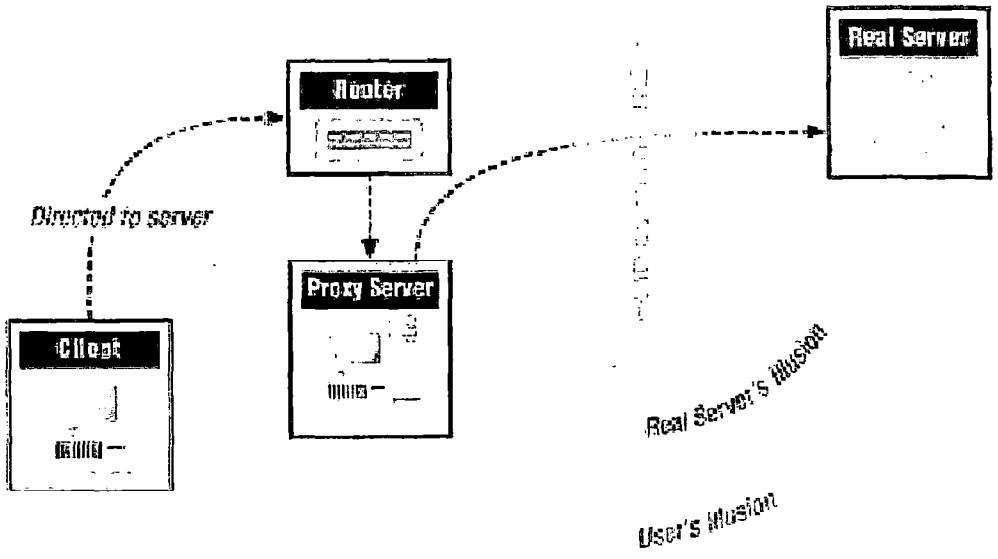
Όπως η χρήση των proxy-aware εφαρμογών απαιτεί κάποια τροποποίηση των διαδικασιών του χρήστη, έτσι και η χρήση proxy-aware ενεργειών θέτουν κάποια όρια για το ποιοι client μπορούν να χρησιμοποιηθούν. Κάποιοι από αυτούς προσπαθούν αυτόματα να πραγματοποιήσουν ανώνυμο FTP και δεν γνωρίζουν πως να "περάσουν" μέσα από τον proxy server.

Το κύριο πρόβλημα με προσαρμοζόμενες διαδικασίες είναι η εκμάθηση τους στους χρήστες. Για παράδειγμα, θα υπάρχει τρομερό πρόβλημα εάν μια επιχείρηση έχει 10.000 χρήστες και είναι διασπαρμένοι και στις πέντε ηπείρους γιατί από τη μία θα υπάρχουν χιλιάδες βιβλία και άρθρα για το πως να εκπαιδεύονται σε στάνταρτ βασικές υπηρεσίες όπως το FTP και από την άλλη, θα υπάρχει ο διαχειριστής του συστήματος που θα προσπαθεί να πείσει όλους αυτούς ότι οι διαδικασίες που μάθανε δεν εφαρμόζονται στο σύστημα που δουλεύουν. Πέρα από αυτό, οι χρήστες θα πρέπει να θυμούνται και το όνομα του gateway και τις λεπτομέρειες για το πως να το χρησιμοποιούν. Όπως είναι φυσικό, τέτοιου είδους προσεγγίσεις δεν μπορούν να εφαρμοστούν σε πολύ μεγάλους οργανισμούς με πολυάριθμους χρήστες.

4.4.3.4 ΧΡΗΣΙΜΟΠΟΙΩΝΤΑΣ PROXY-AWARE ROUTER

Με έναν proxy-aware δρομολογητή, οι clients προσπαθούν να συνδεθούν με τον παραδοσιακό τρόπο αλλά τα πακέτα τα συλλαμβάνονται και καθοδηγούνται στον proxy server. Αυτό πολλές φορές εκτελείται από τον proxy server, που αναλαμβάνει ρόλους δρομολογητή. Σε άλλες όμως, ένας ξεχωριστός router εξετάζει τα πακέτα και αποφασίζει αν θα τα επιτρέψει να φτάσουν τελικά στον προορισμό τους, αν θα τα εγκαταλείψει ή αν θα τα δρομολογήσει στον proxy server. Αυτό πολλές ονομάζεται υβριδικό proxying, γιατί τα πακέτα επεξεργάζονται όπως στην περίπτωση του packet filtering, ή διαφανές proxying, γιατί δεν είναι ορατό στους χρήστες.

Ένας proxy-aware δρομολογητής, όπως φαίνεται και στο σχήμα, αποτελεί την πιο εύκολη λύση για τους χρήστες οι οποίοι δεν χρειάζονται να πραγματοποιήσουν αλλαγές ή να εκπαιδευτούν περισσότερο. Όλη η διαδικασία εκτελείται από συσκευές που συλλαμβάνουν τα πακέτα και από τους διαχειριστές του συστήματος που τις ρυθμίζουν.



Σχήμα 7

Υπάρχουν κάποιοι proxy διακομιστές, οι λεγόμενοι intelligent proxy servers, που εκτελούν πολλά περισσότερα από το να υπηρετούν και να ικανοποιούν requests. Για παράδειγμα, σχεδόν όλοι οι HTTP proxy servers εκτελούν caching των δεδομένων, ώστε πολλαπλά requests που αφορούν τις ίδιες πληροφορίες δεν ξεφεύγουν προς το Internet. Οι proxy servers, και ειδικά οι servers στο επίπεδο εφαρμογής, μπορούν να παρέχουν καλύτερο logging και έλεγχο από αυτούς που χρησιμοποιούν παραδοσιακές μεθόδους και καθώς οι τεχνολογίες εξελίσσονται, οι ικανότητες τους όλο και αυξάνονται.

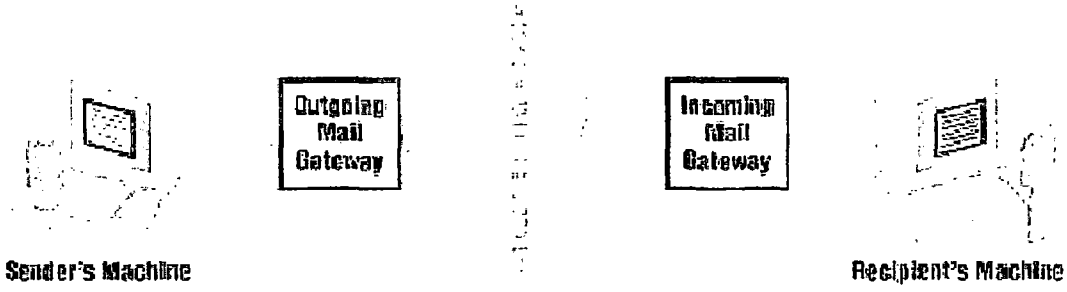
4.4.4 PROXYING ΧΩΡΙΣ ΤΟΝ PROXY SERVER

Κάποιες υπηρεσίες, όπως οι SMPT, NNTP και NTP, υποστηρίζουν proxying. Όλες αυτές οι υπηρεσίες είναι σχεδιασμένες με τέτοιο τρόπο ώστε οι ηλεκτρονικές συναλλαγές (όπως μηνύματα ηλεκτρονικού ταχυδρομείου για τις SMPT) μετακινούνται μεταξύ των διακομιστών αντί να καθοδηγούνται απ' ευθείας από έναν client στον τελικό διακομιστή. Έτσι, κάθε ενδιάμεσος server ενεργεί σαν proxy για τον αρχικό αποστολέα ή διακομιστή.

Αν εξετάσει κάποιος τις επικεφαλίδες από τα εισερχόμενα μηνύματα ηλεκτρονικού ταχυδρομείου (οι οποίες εσωκλείουν πληροφορίες για την διαδρομή του μηνύματος από τον αποστολέα ως τον παραλήπτη) θα διαπιστώσει ότι πολύ λίγα από αυτά "ταξιδεύουν" χωρίς ενδιάμεσους σταθμούς. Στις μέρες μας, είναι πιο συνήθες τα μηνύματα να περνούν τουλάχιστον από τέσσερα μηχανήματα:

- Το μηχάνημα του αποστολέα
- Τον παροχέα υπηρεσιών διαδικτύου του αποστολέα
- Το gateway υπεύθυνο για τα εισερχόμενα e-mails στην πλευρά του παραλήπτη
- Το μηχάνημα του παραλήπτη

Κάθε ένας από τους ενδιάμεσους servers (οι mail gateways) συμπεριφέρεται σαν proxy server για τον αποστολέα, άσχετα αυτός αν δεν συναλλάσσεται μαζί τους άμεσα (σχήμα).



Σχήμα 8

4.4.5 ΠΛΕΟΝΕΚΤΗΜΑ ΚΑΙ ΜΕΙΟΝΕΚΤΗΜΑΤΑ ΤΩΝ PROXY SERVICES

Επειδή οι proxy servers μπορούν να ανιχνεύσουν το application protocol, μπορούν να επιτρέψουν τη διαδικασία του logging (καταγραφής) να εκτελείται με έναν συγκεκριμένο και αποτελεσματικό τρόπο. Για παράδειγμα, αντί να καταγράφονται όλα τα δεδομένα που έχουν μεταβιβαστεί, ένας FTP proxy καταγράφει μόνο τις εντολές που έχουν δοθεί και τις αντίστοιχες

ληφθείσες απαντήσεις από τον server. Αυτό έχει σαν αποτέλεσμα σε ένα μικρότερο και αποτελεσματικότερο αρχείο καταγραφής.

Από την στιγμή που όλα τα requests διαβιβάζονται μέσα από το proxy service, ο proxy κρατάει αντίγραφα από τα δεδομένα που ζητήθηκαν. Αν ο αριθμός των ίδιων αιτημάτων είναι σημαντικός, το caching μπορεί να αυξήσει σημαντικά την απόδοση και να μειώσει τον φόρτο στις συνδέσεις του δικτύου.

Από την στιγμή μια proxy υπηρεσία εξετάζει συγκεκριμένες συνδέσεις, είναι πολλές φορές πιο ικανή να φιλτράρει πακέτα δεδομένων πιο "έξυπνα" από έναν packet filter. Για παράδειγμα, οι proxy services είναι πολύ πιο αποτελεσματικές στο να φιλτράρει το πρωτόκολλο HTTP με βάση τον τύπο των περιεχομένων (όπως Java και JavaScript) και καλύτερες στον εντοπισμό ιών από τα συστήματα packet filtering.

Επειδή ένα proxy σύστημα παίζει σημαντικό ρόλο σε μια σύνδεση, είναι εύκολο για αυτό να πιστοποιήσει την αυθεντικότητα ενός χρήστη και να πράττει ανάλογα με την περίσταση. Αν και αυτό είναι εφικτό από τα packet filter συστήματα, είναι πιο δύσκολο να πραγματοποιηθεί.

Τέλος, λαμβάνοντας υπ΄ όψη ότι ένα proxy σύστημα εγκαθίσταται μεταξύ ενός client και ενός server, δημιουργεί καινούργια IP πακέτα για τον client. Με αυτόν τον τρόπο μπορεί να προστατεύσει τους clients από παραμορφωμένα IP πακέτα, κατασκευασμένα με σκοπό να τους απειλήσουν.

Από την άλλη πλευρά όμως, υπάρχουν και κάποιοι περιορισμοί και μειονεκτήματα της χρήσης των proxies. Αν και proxy προγράμματα και εργαλεία είναι ευρέως διαθέσιμα για τις απλές και παλιές υπηρεσίες όπως το FTP και το Telnet, υπάρχει δυσκολία σε ότι αφορά καινούργιες ή τις λιγότερο διαδεδομένες. Έτσι πολλές φορές οι διαχειριστές ενός site, προκειμένου να προσφέρουν μια πρόσφατη υπηρεσία, είναι αναγκασμένοι να την τοποθετούν εξωτερικά από την περίμετρο του firewall, αφήνοντας έτσι "τρύπες" στην ασφάλεια.

Άλλο ένα σημαντικό μειονέκτημα είναι ότι πιθανώς να απαιτείται διαφορετικός proxy server για κάθε πρωτόκολλο. Προκειμένου ο proxy server να "μεταμφιεστεί" ως client για τον πραγματικό sever και ως πραγματικός server για τον proxy πελάτη, είναι επιτακτική ανάγκη να "κατανοεί" εξολοκλήρου το πρωτόκολλο που διαχειρίζεται και να αποφασίζει ποια πακέτα θα επιτρέψει και ποια όχι. Η συλλογή, η εγκατάσταση και η ρύθμιση πολλών server μπορεί να είναι δύσκολη και χρονοβόρα διεργασία. Μπορούμε μεν να χρησιμοποιήσουμε έναν γενικευμένο proxy, αλλά έτσι βρισκόμαστε στα

μειωμένα, σε σχέση με τους proxies, επίπεδα ασφάλειας και λειτουργικότητας που παρέχουν οι packet filters.

4.5 NETWORK ADDRESS TRANSLATION (NAT)

4.5.1 ΕΙΣΑΓΩΓΗ

Η ανάπτυξη του διαδικτύου είναι αδιαμφισβήτητα μεγάλη και για πολλούς απρόβλεπτη. Αν και το ακριβές μέγεθος του δεν μπορεί να προσδιοριστεί, εκτιμάται ότι υπάρχουν περίπου 100 εκατομμύρια hosts και πάνω από 350 εκατομμύρια ενεργοί χρήστες. Επιπρόσθετα, κάθε χρόνο, ο ετήσιος ρυθμός αύξησης των χρηστών αγγίζει το 100%.

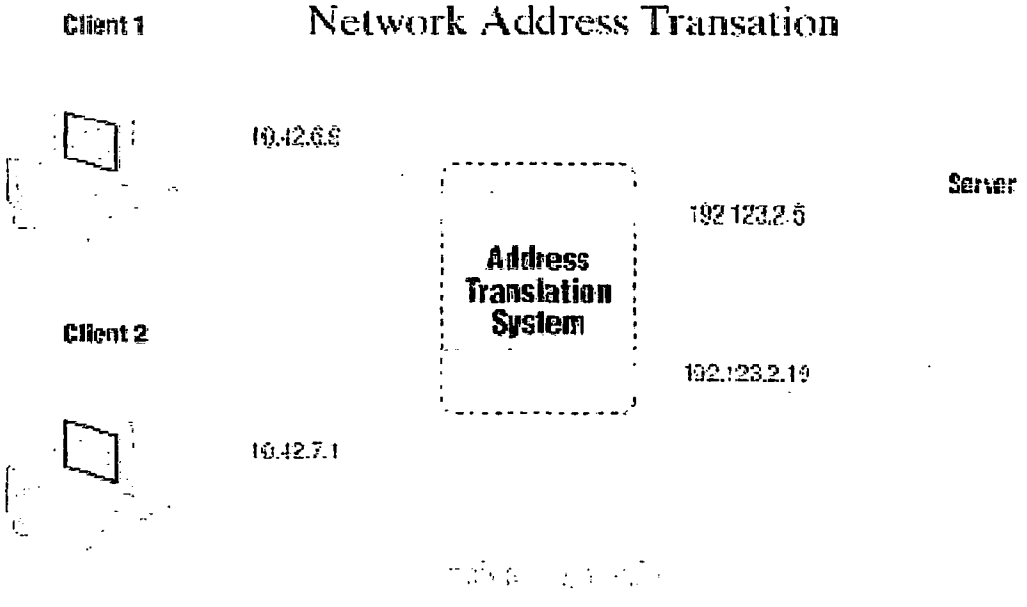
Το Internet Protocol (IP) χρησιμοποιεί διευθύνσεις που απαρτίζονται η κάθε μία από 32 δυαδικά ψηφία. Ο συνδυασμός των ψηφίων αυτών δίνει τη δυνατότητα να υπάρχουν θεωρητικά 4.294.967.296 (2^{32}) διαφορετικές IP διευθύνσεις. Ο πραγματικός αριθμός τους όμως κυμαίνεται μεταξύ 3,2 και 3,3 δισεκατομμύρια εξαιτίας των διαχωρισμών τους σε κλάσεις και της ανάγκης παρακράτησης μερικών διευθύνσεων για multicasting και δοκιμαστικούς λόγους.

Με την έκρηξη του Internet και την αύξηση των προσωπικών και εταιρικών δικτύων, ο αριθμός των διαθέσιμων IP διευθύνσεων δεν επαρκεί. Η προφανής λύση είναι ο επανασχεδιασμός του IP, έτσι ώστε να παρέχει πολύ περισσότερες διευθύνσεις, γεγονός που βρίσκεται ήδη "στα σκαριά" (IPv6), αν και θα χρειαστούν αρκετά χρόνια για την τελική εφαρμογή του, αφού θα απαιτήσει αλλαγές στις υποδομές όλου του διαδικτύου.

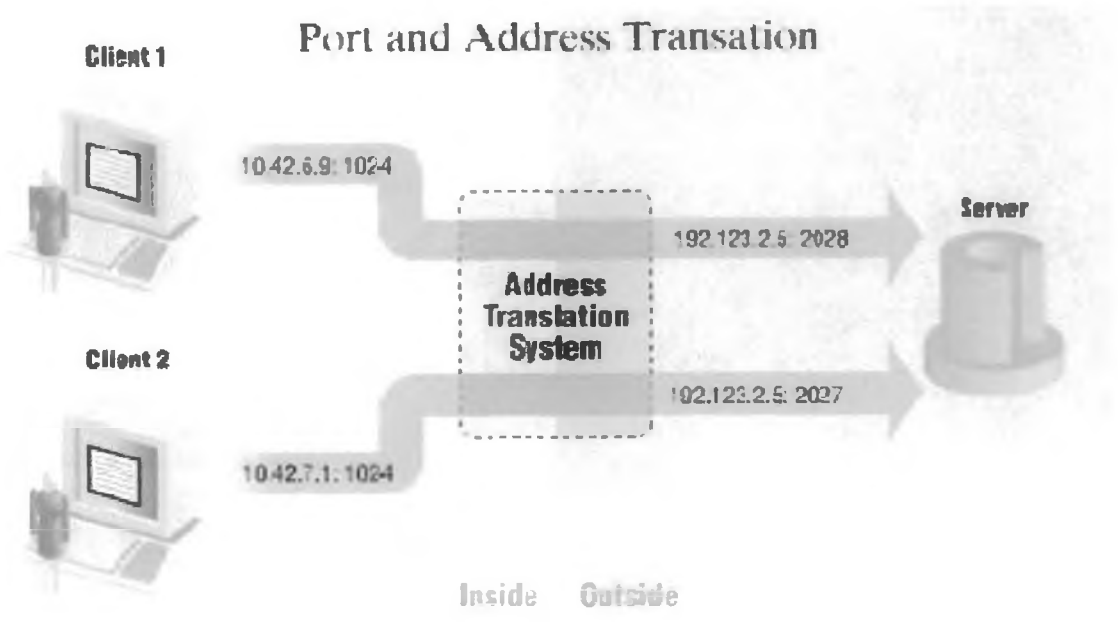
Το παραπάνω πρόβλημα αντιμετωπίστηκε επιτυχώς με τη network address translation τεχνολογία, με τη βοήθεια της οποίας μοναδικές IP διευθύνσεις αντιπροσωπεύουν στο διαδίκτυο ένα σύνολο από πολλούς υπολογιστές του εσωτερικού δικτύου.

4.5.2 Η ΛΕΙΤΟΥΡΓΙΑ ΤΗΣ NETWORK ADDRESS TRANSLATION

Η network address translation τεχνολογία, που αναπτύχθηκε από την Cisco, επιτρέπει σε ένα δίκτυο να χρησιμοποιεί τοπικά μία ομάδα διευθύνσεων δικτύου και μία άλλη, διαφορετική ομάδα όταν υπάρχει επικοινωνία με ένα εξωτερικό δίκτυο. Η NAT δεν προσφέρει από μόνη της κάποια ασφάλεια, αλλά βοηθάει στην απόκρυψη της δομής και του πλάνου ενός εσωτερικού δικτύου. Όπως και το packet filtering, έτσι και η NAT απαιτεί έναν δρομολογητή όχι μόνο για δρομολογεί τα πακέτα, αλλά και να τα τροποποιεί. Όταν ένας κόμβος του εσωτερικού δικτύου αποστέλλει πακέτα σε εξωτερικές διευθύνσεις, η NAT τροποποιεί με τέτοιο τρόπο τη διεύθυνση πηγής του πακέτου έτσι ώστε να φαίνεται ότι τι πακέτο προέρχεται από μια έγκυρη διεύθυνση. Όταν το εσωτερικό δίκτυο δέχεται πακέτα από εξωτερικές πηγές, η NAT μεταλλάσσει την διεύθυνση προορισμού για να αλλάξει την ορατή εξωτερικά διεύθυνση στην σωστή εσωτερική διεύθυνση. Επίσης, η NAT μπορεί να μεταβάλλει τους source και destination αριθμούς των ports (αυτή η διαδικασία ονομάζεται μερικές φορές και Port and Address Translation ή PAT). Το σχήμα 4 απεικονίζει ένα σύστημα NAT που μεταβάλλει μόνο διευθύνσεις, ενώ το σχήμα 5 απεικονίζει μετάφραση διεύθυνσης και PAT.



Σχήμα 9



Σχήμα 10

Αναλυτικότερα, τα network address translation συστήματα μπορούν να χρησιμοποιήσουν διαφορετικούς τρόπους μετάφρασης εσωτερικών και εξωτερικών διευθύνσεων:

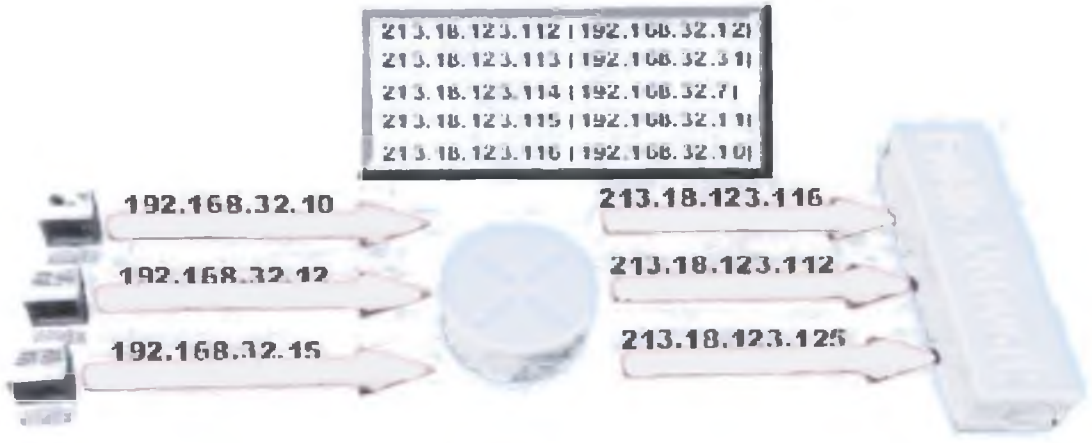
- **Static NAT**

  Με τη στατική αυτή μέθοδο, υπάρχει η δυνατότητα να γίνει η "χαρτογράφηση" (mapping) μιας μη εγγεγραμμένης (non-registered) IP διεύθυνσης με σε μια εγγεγραμμένη σε βάση μία-προς-μία. Η μέθοδος αυτή είναι πολύ χρήσιμη στην περίπτωση που μια συσκευή πρέπει να προσπελαστεί από το εξωτερικό του δικτύου

Σχήμα 11. Στην στατική NAT, η διεύθυνση του υπολογιστή 192.168.32.10 θα μεταφράζεται πάντα ως 213.18.123.110.

- **Dynamic NAT**

Στην περίπτωση αυτή, μια μη εγγεγραμμένη διεύθυνση χαρτογραφείται σε ένα ευρύτερο σύνολο διευθύνσεων



Σχήμα 12. Στην Dynamic NAT, η διεύθυνση του υπολογιστή 192.168.32.10 θα μεταφράζεται στην πρώτη διαθέσιμη διεύθυνση από 213.18.123.100 έως 213.18.123.150.

- **Overloading**

Η μέθοδος του overloading είναι μια παραλλαγή της dynamic NAT, κατά την οποία πολλές IP διευθύνσεις μεταφράζονται σε μία και μοναδική διεύθυνση, χρησιμοποιώντας πολλές διαφορετικές θύρες, και ονομάζεται αλλιώς, όπως αναφέρθηκε και παραπάνω, και ως PAT, single address NAT ή και port-level multiplexed NAT.

Σχήμα 13. Στο overloading, κάθε υπολογιστής ενός ιδιωτικού δικτύου μεταφράζεται στην ίδια IP διεύθυνση (213.18.123.100) αλλά με διαφορετικό αριθμό θυρών.

- **Overlapping**

  Όταν οι διευθύνσεις που βρίσκονται σε χρήση στο εσωτερικό δίκτυο είναι εγγεγραμμένες διευθύνσεις σε χρήση σε ένα άλλο δίκτυο, ο δρομολογητής θα πρέπει να τις καταγράφει σε ένα πίνακα (lookup table) με απώτερο σκοπό να δημιουργεί νέες μοναδικές εγγεγραμμένες διευθύνσεις. Είναι σημαντικό να σημειωθεί ότι ο δρομολογητής πρέπει να μεταφράζει τις εσωτερικές διευθύνσεις σε μοναδικές, εγγεγραμμένες διευθύνσεις καθώς και τις εξωτερικές σε διευθύνσεις που είναι μοναδικές στο ιδιωτικό δίκτυο. Αυτό μπορεί να πραγματοποιηθεί είτε με static NAT είτε με τη χρήση DNS και ταυτόχρονη εφαρμογή dynamic NAT.

Σχήμα 14. Οι εσωτερικές IP διευθύνσεις (237.16.32.xx) χρησιμοποιούνται επίσης από κάποιο άλλο δίκτυο. Συνεπώς ο δρομολογητής μεταφράζει τις διευθύνσεις προς αποφυγή συγκρούσεων με το άλλο δίκτυο.

4.5.3 ΠΛΕΟΝΕΚΤΗΜΑΤΑ ΚΑΙ ΜΕΙΟΝΕΚΤΗΜΑΤΑ ΤΗΣ NETWORK ADDRESS TRANSLATION

Αν και το κύριο μέλημα του NAT είναι να εξοικονομούν χώρο για διευθύνσεις, μπορούν όμως και να παρέχουν και κάποια πλεονεκτήματα σε ζητήματα ασφάλειας. Μπορεί, για παράδειγμα, να ενδυναμώσει τον έλεγχο του firewall σε εξωτερικές συνδέσεις. Αφού κάποιοι συγκεκριμένοι hosts έχουν διευθύνσεις τέτοιες που δεν αρμόζουν για το εξωτερικό δίκτυο, χρειάζονται τη βοήθεια του συστήματος NAT, το οποίο θα τους εξασφαλίσει την σύνδεση. Αν ένας host βρει τρόπο να συνδεθεί χωρίς το σύστημα NAT, τότε αυτή η σύνδεση θα αποτύχει.

Ανάλογα με τον τρόπο με τον οποίο "στήσουμε" ένα network address translation σύστημα, υπάρχει η δυνατότητα καλύτερου ελέγχου της

εισερχόμενης κίνησης από τους packets filters. Τα συστήματα αυτά που πραγματοποιούν δυναμικές μεταφράσεις θα επιτρέψουν πακέτα που ανήκουν μόνο στην τρέχουσα σύνδεση, η οποία ξεκίνησε από το εσωτερικό του δικτύου. Αυτή η τακτική μπορεί να μοιάζει με αυτήν των packet filters, αλλά οι μεταβαλλόμενες IP διευθύνσεις περιορίζουν χρονικά τους ενδεχόμενους εισβολείς, οι οποίοι αναγκάζονται να επιτεθούν σε συγκεκριμένες ports, έχοντας πολύ λίγο χρόνο στην διάθεση τους, αφού η διεύθυνση θα έχει εξαφανιστεί ή δοθεί σε κάποιον άλλο host.

Ένα NAT σύστημα κάνει πολύ δύσκολο σε κάποιον εισβολέα να προσδιορίσει από ποιους και από πόσους υπολογιστές απαρτίζεται ένα δίκτυο, καθώς και την διάταξη τους μέσα σε αυτό. Πολλές φορές όμως μερικά πρωτόκολλα "διαρρέουν" χρήσιμες πληροφορίες σε κάποιον τρίτο, όπως η IP διεύθυνση ή το όνομα του host, σε σημεία βέβαια που το NAT σύστημα δεν χρειάζεται να τις μεταβάλλει.

Αν και η network address translation είναι ένας πολύ αποτελεσματικός τρόπος διατήρησης χώρου για διευθύνσεις, μπορεί να προκαλέσει κάποια προβλήματα. Τα συστήματα NAT συνήθως μεταφράζουν τις διευθύνσεις στην επικεφαλίδα του πακέτου. Πολλά πρωτόκολλα όμως κρύβουν διευθύνσεις και σε άλλες τοποθεσίες, και προκειμένου να γίνει η αναγνώριση και η τροποποίηση του πακέτου, χωρίς απώλειες στην ακεραιότητα του, ο network address μεταφραστής πρέπει να "γνωρίζει" καλά το πρωτόκολλο. Πολλά NAT συστήματα έχουν αυτή την δυνατότητα για κάποια πρωτόκολλα (για παράδειγμα το FTP), αλλά όχι για όλα.

Συστήματα κρυπτογράφησης δεδομένων συχνά επιχειρούν να εξασφαλίζουν την ακεραιότητα των δεδομένων, έτσι ώστε τα συστήματα που επικοινωνούν να γνωρίζουν ότι τα πακέτα δεν έχουν αλλοιωθεί κατά τη μεταφορά. Η NAT όμως, είναι μια μορφή "μετάλλαξης" των πακέτων. Αν το πρωτόκολλο το οποίο μεταφράζεται δεν προστατεύει τα δεδομένα που μεταβάλλονται από ένα σύστημα NAT τότε δεν θα υπάρχει πρόβλημα στην σύνδεση. Αν, από την άλλη, υπάρχει προστασία των δεδομένων, η σύνδεση θα αποτύχει. Στις περισσότερες περιπτώσεις, τα πρωτόκολλα που δεν έχουν embedded IP διευθύνσεις (δηλαδή οι επικεφαλίδες των πακέτων δεν αποτελούν μέρος της προστασίας) είναι συμβατά με NAT συστήματα. Μεγάλη εξαίρεση αποτελεί το IPsec, το οποίο προστατεύει ολόκληρο το πακέτο, συμπεριλαμβάνοντας και την επικεφαλίδα.

Στην περίπτωση που καταγράφονται πληροφορίες (logging) αφού έχει πραγματοποιηθεί η network address μετάφραση, το ημερολόγιο, όπως φαίνεται και στο σχήμα, θα παρουσιάζει μεταφρασμένες διευθύνσεις, οι

οποίες θα πρέπει να συσχετιστούν με πληροφορίες από το NAT σύστημα προκειμένου να κατανοηθεί ποιο εσωτερικό σύστημα στην πραγματικότητα πήρε μέρος στην όλη διαδικασία. Αν και αυτός ο συσχετισμός είναι θεωρητικά εφικτός, αποτελεί δύσκολη διαδικασία.

Source Computer	Source Computer's IP Address	Source Computer's Port	NAT Router's IP Address	NAT Router's Assigned Port Number
A	192.168.32.10	400	215.37.32.203	1
B	192.168.32.13	50	215.37.32.203	2
C	192.168.32.15	3750	215.37.32.203	3
D	192.168.32.18	206	215.37.32.203	4

Σχήμα 15

Τα packet filtering συστήματα εστιάζονται στους αριθμούς θυρών πηγής και προορισμού (source και destination port numbers) προκειμένου να αναγνωρίσουν ποιο πρωτόκολλο ένα πακέτο πρέπει να χρησιμοποιεί. Αλλάζοντας την θύρα πηγής μπορεί να αλλάξει και η δυνατότητα αποδοχής του πακέτου. Στις περισσότερες των περιπτώσεων, αυτό δεν αποτελεί πρόβλημα γιατί τα NAT συστήματα μεταφράζουν για λογαριασμό των client, όπου επιτρέπεται να χρησιμοποιούν οποιουσδήποτε αριθμούς θυρών πάνω από 1023. Αν όμως οι θύρες πάνω από 1023 μεταφραστούν σε θύρες κάτω από αυτό το νούμερο, η κυκλοφορία πακέτων μπορεί να διακοπεί.

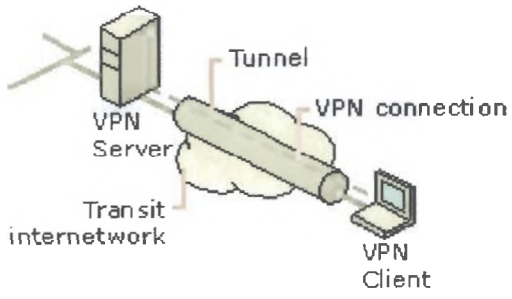
4.6 VIRTUAL PRIVATE NETWORKS

4.6.1 ΤΕΧΝΟΛΟΓΙΑ ΤΩΝ VPN

Ένα virtual private network (VPN) είναι η προέκταση ενός ιδιωτικού δικτύου το οποίο προσανατολίζει υπερσυνδέσεις ανάμεσα κοινόχρηστα ή δημόσια δίκτυα όπως το Internet. Ένα VPN επιτρέπει στους χρήστες να μεταδίδουν πληροφορίες μεταξύ δύο υπολογιστών σε ένα δημόσιο δίκτυο ενσωματώνοντας τις ιδιότητες των ιδιωτικών σημείο-προς-σημείο (point-to-point) συνδέσεων. Η διαδικασία της δημιουργίας και ρύθμισης ενός τέτοιου εικονικού ιδιωτικού δικτύου ονομάζεται virtual private networking.

Για να λάβει χώρα μια point-to-point σύνδεση, τα δεδομένα ενθυλακώνονται (encapsulation) με μια επικεφαλίδα που παρέχει πληροφορίες δρομολόγησης, επιτρέποντας τα έτσι να διασχίσουν το

κοινόχρηστο ή δημόσιο δίκτυο για να φτάσουν στον προορισμό τους. Για να εξομοιωθεί μια ιδιωτική υπερσύνδεση (private link), τα δεδομένα που αποστέλλονται κρυπτογραφούνται για μεγαλύτερη ασφάλεια, κάνοντας τα έτσι αδύνατο να "διαβαστούν" χωρίς την χρήση του αρχικού κλειδιού κρυπτογράφησης. Το μέρος της σύνδεσης που πραγματοποιείται η ενθυλάκωση ονομάζεται tunnel, ενώ το μέρος της σύνδεσης κατά το οποίο τα δεδομένα κρυπτογραφούνται είναι γνωστό ως virtual private network connection.



Σχήμα 16

Οι συνδέσεις VPN επιτρέπουν στους χρήστες να συνδέονται στον απομακρυσμένο εταιρικό server με ασφάλεια από το σπίτι τους ή και γενικά από χώρους εκτός του εργασιακού δικτύου τους με το να χρησιμοποιούν την υποδομή δρομολόγησης που παρέχει ένα δημόσιο δίκτυο, όπως το Internet. Από την πλευρά και την αντίληψη του χρήστη, η VPN σύνδεση είναι μια σύνδεση σημείο προς σημείο μεταξύ του υπολογιστή του και του εταιρικού διακομιστή. Η φύση των ενδιάμεσων δικτυακών διεργασιών είναι άσχετη με τον χρήστη γιατί φαίνεται ότι τα δεδομένα αποστέλλονται διαμέσου μιας ιδιωτικής υπερσύνδεσης.

Η VPN τεχνολογία επιτρέπει επίσης σε μια εταιρεία, λόγου χάρη, να συνδέεται με τα απομακρυσμένα γραφεία της ή με άλλες εταιρείες με τη βοήθεια ενός δημοσίου δικτύου, με ιδιαίτερα ασφαλή τρόπο. Η VPN σύνδεση διαμέσου του Internet λειτουργεί σαν ένα σύνδεσμο δικτύου ευρείας περιοχής μεταξύ των sites.

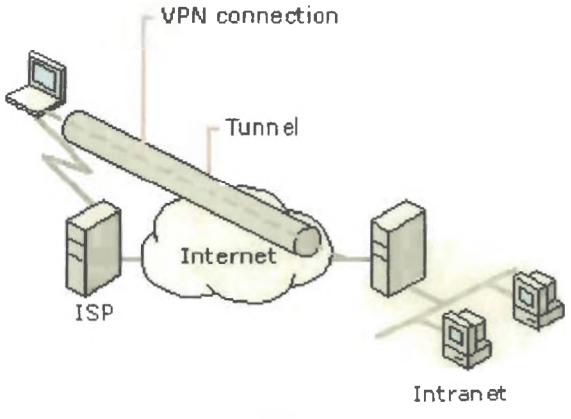
Η VPN τεχνολογία είναι σχεδιασμένη έτσι ώστε να ανταποκρίνεται στις σύγχρονες τηλεπικοινωνιακές απαιτήσεις και στις παγκόσμια κατανεμημένες υπολογιστικές εφαρμογές, όπου οι χρήστες θα πρέπει να συνδέονται σε κεντρικές πηγές πληροφοριών και να έχουν τη δυνατότητα να επικοινωνούν μεταξύ τους.

4.6.2 ΚΟΙΝΕΣ ΧΡΗΣΕΙΣ ΤΩΝ VPN

Στη συνέχεια αναφέρονται οι συνήθεις χρήσεις και τακτικές εγκατάστασης ιδιωτικών εικονικών δικτύων που συναντώνται σήμερα.

- Απομακρυσμένη σύνδεση μέσω του διαδικτύου

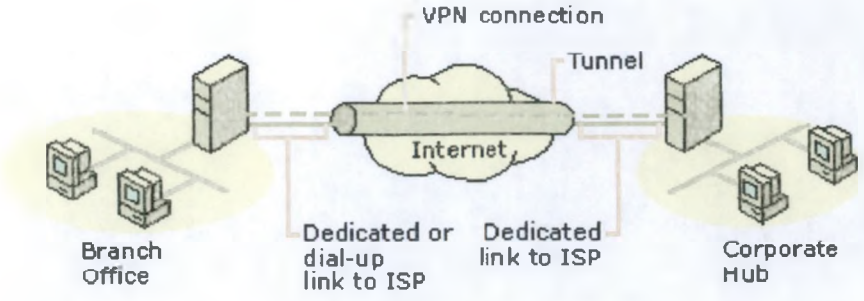
  Τα VPN παρέχουν απομακρυσμένες συνδέσεις διαμέσου δημοσίων δικτύων, διατηρώντας ταυτόχρονα την ασφάλεια των πληροφοριών που διακινούνται (σχήμα). Ο χρήστης συνδέεται μέσω dial up με τη βοήθεια του τοπικού παροχέα Internet και στη συνέχεια, το VPN λογισμικό δημιουργεί ένα εικονικό ιδιωτικό δίκτυο ανάμεσα στο δίκτυο και στον VPN διακομιστή.



Σχήμα 17

- Διασύνδεση τοπικών δικτύων διαμέσου του διαδικτύου

  Υπάρχουν δύο μέθοδοι που χρησιμοποιούνται έτσι ώστε τα VPN να συνδέουν τοπικά δίκτυα μεταξύ τους. Η πρώτη αφορά τη χρήση αποκλειστικών γραμμών και η δεύτερη τη χρήση dial up συνδέσεων, όπου και στις δύο περιπτώσεις, δημιουργείται ένα VPN που είναι υπεύθυνο για τη μεταφορά των πληροφοριών (σχήμα)

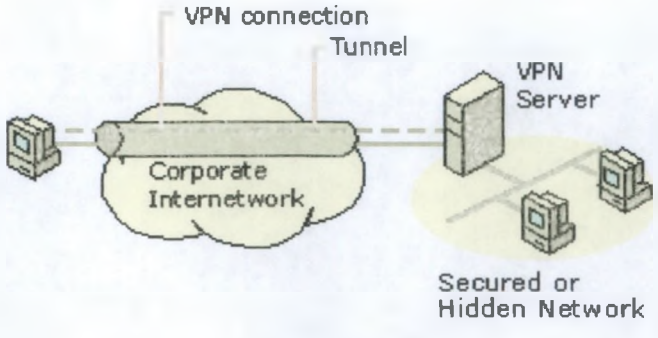


Σχήμα 18

- Διασύνδεση υπολογιστών μέσα σε τοπικό δίκτυο

Σε κάποιες εταιρείες και οργανισμούς, υπάρχουν ορισμένα τμήματα τους τα οποία περιέχουν ευαίσθητες πληροφορίες, που δεν πρέπει να είναι ορατά από όλα τα υπόλοιπα τμήματα. Μια συνήθης τακτική είναι η φυσική αποσύνδεση τους από το υπόλοιπο δίκτυο. Αυτό όμως, αν και είναι απολύτως ασφαλής μέθοδος, δημιουργεί προβλήματα πρόσβασης στις συγκεκριμένες πληροφορίες για απομακρυσμένους χρήστες, που έχουν δικαιώματα στα δεδομένα αυτά.

Τα VPN επιτρέπουν σε ένα εταιρικό τοπικό δίκτυο να συνδεθεί φυσικά με ένα ευαίσθητο τμήμα του χρησιμοποιώντας έναν VPN διακομιστή, ο οποίος δεν εκτελεί χρέη δρομολογητή αλλά δίνει τη δυνατότητα σε όλους τους χρήστες του δικτύου να μπορούν να συνδεθούν, εφόσον πληρούν τις κατάλληλες προϋποθέσεις που ορίζονται από την προκαθορισμένη πολιτική ασφαλείας.



Σχήμα 19

4.6.3 ΒΑΣΙΚΕΣ ΠΡΟΫΠΟΘΕΣΕΙΣ ΓΙΑ ΤΑ VPN

Τυπικά, όταν μια εταιρεία ή ένας οργανισμός δημιουργεί ένα δίκτυο προκειμένου να ικανοποιεί τις ανάγκες, θα πρέπει φυσικά να μπορεί να ελέγχει ποιοι χρήστες ή μηχανήματα θα έχουν πρόσβαση σε αυτό. Όπως προαναφέρθηκε, μια πολύ καλή λύση είναι αυτή των virtual private networks. Αυτή θα πρέπει οπωσδήποτε να παρέχει τουλάχιστον τις εξής υπηρεσίες:

- **User Authentication**

  Η λύση που θα εφαρμοστεί σε ένα δίκτυο θα πρέπει να επαληθεύει την ταυτότητα του client και επιτρέπει την πρόσβαση σε συγκεκριμένους μόνο χρήστες. Επίσης, θα πρέπει να καταγράφει συνεχώς το όνομα του χρήστη καθώς και την ημερομηνία και ώρα που αυτός είχε πρόσβαση στα δεδομένα του συστήματος.

- **Διαχείριση Διευθύνσεων**

  Είναι βασικό στοιχείο το να υπάρχει η δυνατότητα καθορισμού της διεύθυνσης ενός VPN client στο διαδίκτυο και η διασφάλιση ότι η διεύθυνση αυτή θα παραμείνει ιδιωτική.

- **Κρυπτογράφηση δεδομένων**

  Τα δεδομένα που θα μεταφέρονται από και προς ένα δημόσιο δίκτυο θα πρέπει να κρυπτογραφούνται έτσι ώστε να μην μπορεί κάποιος που δεν έχει δικαιώματα πρόσβασης να τα "διαβάσει".

- **Διαχείριση κλειδιών**

  Για να είναι επιτυχημένη η μέθοδος της κρυπτογράφησης, είναι αναγκαίο τα κλειδιά που χρησιμοποιούνται να αλλάζουν συνεχώς, προς αποφυγή υποκλοπής τους.

- **Υποστήριξη πρωτοκόλλων**

  Η λύση που θα εφαρμοστεί θα πρέπει να μπορεί να υποστηρίξει τα συνήθη πρωτόκολλα που χρησιμοποιούνται σε δημόσια δίκτυα όπως το IP, το IPX κλπ.

4.6.4 ΠΛΕΟΝΕΚΤΗΜΑΤΑ ΚΑΙ ΜΕΙΟΝΕΚΤΗΜΑΤΑ ΤΟΥ VIRTUAL PRIVATE NETWORKING

Τα περισσότερα οφέλη από την χρήση virtual private networks είναι οικονομικά. Είναι βέβαια ποιο συμφέρον να χρησιμοποιηθούν κοινόχρηστα δημόσια δίκτυα από το να εγκατασταθούν αποκλειστικές (**dedicated)** συνδέσεις, μισθωμένες ή μη. Επίσης, η χρήση των virtual private networks προσφέρουν και πλεονεκτήματα σε θέματα ασφαλείας.

Ένα virtual private network αποκρύπτει όλη την κίνηση σε ένα δίκτυο. Όχι μόνο εγγυάται ότι όλες οι πληροφορίες κρυπτογραφούνται, αλλά επίσης αποτρέπει από τρίτους να γνωρίζουν ποια μηχανήματα και πρωτόκολλα χρησιμοποιούνται. Εάν προσπαθούμε να προστατέψουμε πληροφορίες χρησιμοποιώντας μόνο πρωτόκολλα κρυπτογράφησης, οι εισβολείς θα γνωρίζουν τα μηχανήματα και υπολογιστές που αλληλεπιδρούν, καθώς και το πρωτόκολλο επικοινωνίας, όπως για παράδειγμα στην περίπτωση της αποστολής κρυπτογραφημένου e-mail, όπου μπορεί μεν κάποιος να μην μπορεί υποκλέψει το περιεχόμενου του αλλά γνωρίζει ότι "κυκλοφορούν" δεδομένα σε αυτή τη μορφή. Ένα virtual private network μπορεί να υποκρύψει τέτοιου είδους πληροφορίες.

Σε κάποια πρωτόκολλα είναι δύσκολα να εφαρμοστούν τεχνικές ασφάλειας με τη βοήθεια κάποιου firewall. Για παράδειγμα, ένας μεγάλος αριθμός πρωτοκόλλων που χρησιμοποιούνται σε συστήματα της Microsoft βασίζονται στο SMB, το οποίο παρέχει πληθώρα υπηρεσιών με διαφορετικές εφαρμογές πάνω στις ίδιες θύρες και συνδέσεις. Ενώ οι proxying και packet filtering αποδεικνύονται κακές λύσεις στην προκειμένη περίπτωση, τα virtual private networks κρίνονται αρκετά ικανοποιητικά στον τρόπο που παρέχουν απομακρυσμένες συνδέσεις από το διαδίκτυο.

Από την άλλη, τα virtual private networks παρουσιάζουν και κάποια προβλήματα. Όταν γίνονται προσθήκες κόμβων σε ένα virtual private network, τότε αυτομάτως ανήκουν και στο εσωτερικό. Αν κάποιος εισβολέας πάρει τον έλεγχο ενός υπολογιστή του virtual private network, θα έχει την δυνατότητα να επιτεθεί και στο υπόλοιπο μέρος του δικτύου. Συνήθως, η μέθοδος του virtual private networking εφαρμόζεται στο να παρέχεται πρόσβαση σε συστήματα που είναι πιο ευάλωτα απ' ότι από αυτά που έχουν "φυσική" πρόσβαση στο δίκτυο. Όπως για παράδειγμα φορητοί υπολογιστές που μετακινούνται συχνά και μηχανήματα που ανήκουν σε άλλα sites, όπου τα συμφέροντα και οι πολιτικές ασφαλείας διαφέρουν από την δική μας. Τα virtual private networks εξουδετερώνουν άλλες χρήσεις του πρωτοκόλλου επικοινωνίας το οποίο

χρησιμοποιεί ένα σύστημα, χωρίς όμως να αποκλείεται ότι αυτό το σύστημα μπορεί να έχει την δυνατότητα να έχει και άλλα πρωτόκολλα επικοινωνίας. Έτσι, το σύστημα αυτό μπορεί να μετατραπεί ως πύλη μεταξύ του δικτύου μας και κάποιων τρίτων, μέσα στην περίμετρο ασφαλείας μας. Εξαιτίας αυτού, πρέπει να επιλέγεται με προσοχή ο τρόπος που σχετίζεται το virtual private network με το πραγματικό δίκτυο.

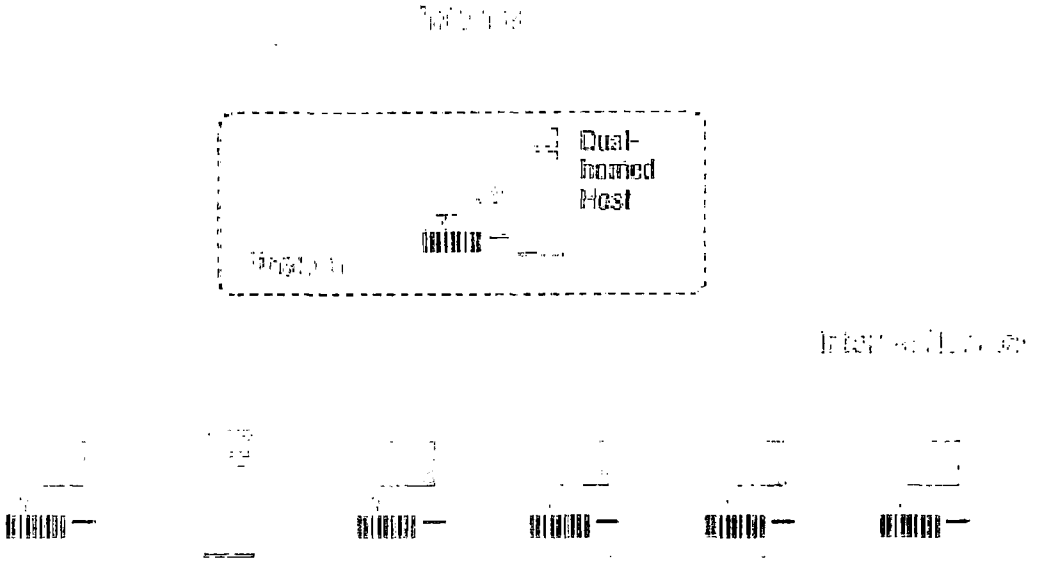
ΚΕΦΑΛΑΙΟ 5ο : ΑΡΧΙΤΕΚΤΟΝΙΚΕΣ FIREWALL

5.1 DUAL-HOMED HOST ΑΡΧΙΤΕΚΤΟΝΙΚΕΣ

Η dual-homed αρχιτεκτονική είναι βασισμένη σε έναν dual-homed host υπολογιστή, δηλαδή έναν υπολογιστή ο οποίος έχει δύο τουλάχιστον διεπιφάνειες (interfaces) δικτύου. Ένας τέτοιος host μπορεί να εκτελέσει καθήκοντα δρομολογητή μεταξύ των δύο δικτύων που έχουν εφαρμοστεί αυτές οι διεπιφάνειες, όπου δρομολογεί IP πακέτα από το ένα δίκτυο στο άλλο. Αν όμως χρησιμοποιηθεί ο host αυτός ως firewall, εξουδετερώνονται οι δυνατότητες δρομολόγησης. Συστήματα έξω και μέσα στην περίμετρο του firewall, ενώ μπορούν να επικοινωνήσουν με τον dual-homed host, δεν μπορούν να επικοινωνήσουν απευθείας μεταξύ τους, αφού η TCP/IP κυκλοφορία μεταξύ τους έχει διακοπεί.

Η αρχιτεκτονική δικτύου για έναν dual-homed host firewall είναι αρκετά απλή: ο host εγκαθίσταται ανάμεσα στο διαδίκτυο και στο εσωτερικό δίκτυο, όπως φαίνεται και στο σχήμα 6, και προσφέρει υψηλό βαθμό ελέγχου. Αφού δεν επιτρέπονται να "κυκλοφορούν" πακέτα μεταξύ του εσωτερικού και εξωτερικού δικτύου, κάθε πακέτο μέσα στο εσωτερικό δίκτυο που έχει εξωτερική πηγή αποτελεί ένδειξη προβλήματος στην ασφάλεια. Από την άλλη, οι dual-homed host δεν είναι συσκευές υψηλής απόδοσης, αφού έχουν περισσότερο φόρτο εργασίας για κάθε σύνδεση και απαιτούν περισσότερους πόρους συγκριτικά με έναν packet filter.

Η αρχιτεκτονική αυτή απαιτεί ότι ο dual-homed host είναι στο μέγιστο βαθμό ασφαλής. Ένας εισβολέας που μπορεί να αποκτήσει τον έλεγχο του host, έχει ταυτόχρονα και πλήρη έλεγχο του εσωτερικού δικτύου, ανεξάρτητα από τα πρωτόκολλα που χρησιμοποιούνται. Επίσης, αν ο host καταρρεύσει από έναν εισβολέα, τότε διακόπτεται και η επικοινωνία με το Internet. Αυτό το γεγονός καθιστά τους dual-homed hosts κακή λύση εάν η επικοινωνία με το διαδίκτυο είναι σημαντική για μια εταιρεία ή ένα οργανισμό.

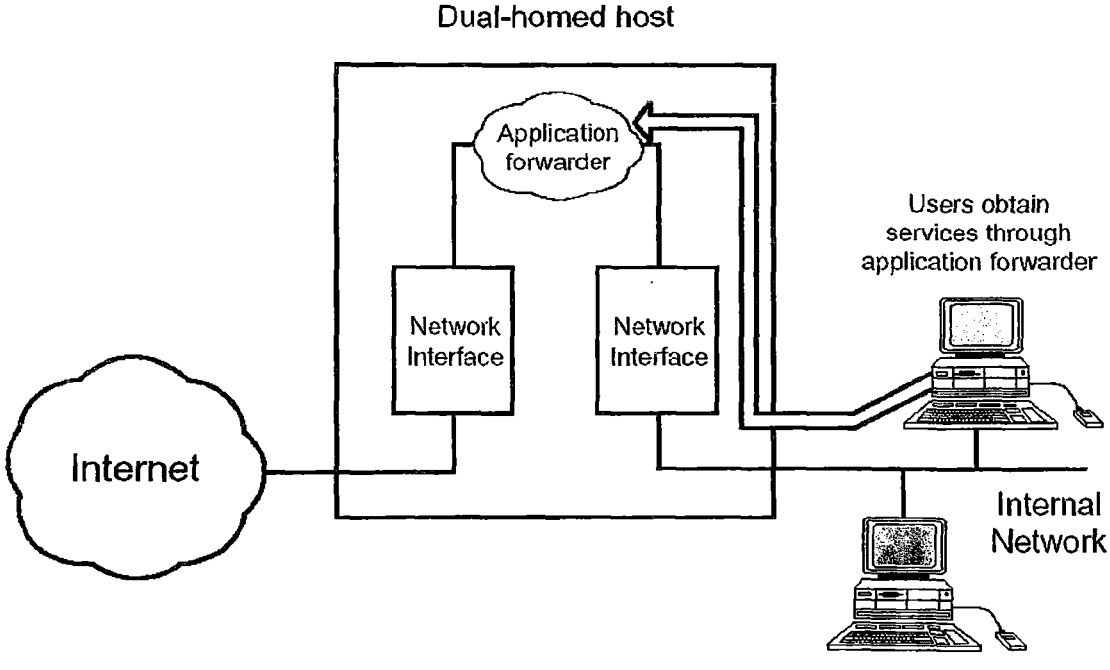


Σχήμα 20

Ένας dual-homed host μπορεί να παρέχει υπηρεσίες μόνο αν εφαρμόζει μεθόδους proxying ή αν συνδέονται οι χρήστες απευθείας με τον host, γεγονός που δεν αποτελεί καλή λύση αφού οι λογαριασμοί χρηστών εξ' ορισμού παρουσιάζουν αρκετά προβλήματα σε θέματα ασφαλείας. Επίσης, επιτρέποντας κάποιον χρήστη να κάνει login σε έναν host, υπάρχει η πιθανότητα να ενεργοποιήσει κάποιες υπηρεσίες οι οποίες θεωρούνται επικίνδυνες. Οι μέθοδοι proxying είναι λιγότερο προβληματικές και μπορεί να μην είναι διαθέσιμες για κάποιες επιθυμητές υπηρεσίες. Επίσης, οι μέθοδοι αυτοί προτιμούνται για outbound υπηρεσίες (εσωτερικοί χρήστες να χρησιμοποιούν πηγές από το Internet) παρά για inbound υπηρεσίες (χρήστες του Internet εκμεταλλεύονται πηγές του εσωτερικού δικτύου.

Σε μία dual-homed διάταξη, υπάρχει η απαίτηση να παρέχονται υπηρεσίες διαδικτύου, οι οποίες θα τρέχουν στον dual-homed host. Αυτό όμως προσδίδει υψηλό ποσοστό επικινδυνότητας και γενικά συνιστάται η εγκατάσταση ενός περιορισμένου λειτουργικά web server ο οποίος θα είναι ικανός να παρέχει HTML αρχεία χωρίς επιπλέον πρωτόκολλα και επεξεργασίες φορμών.

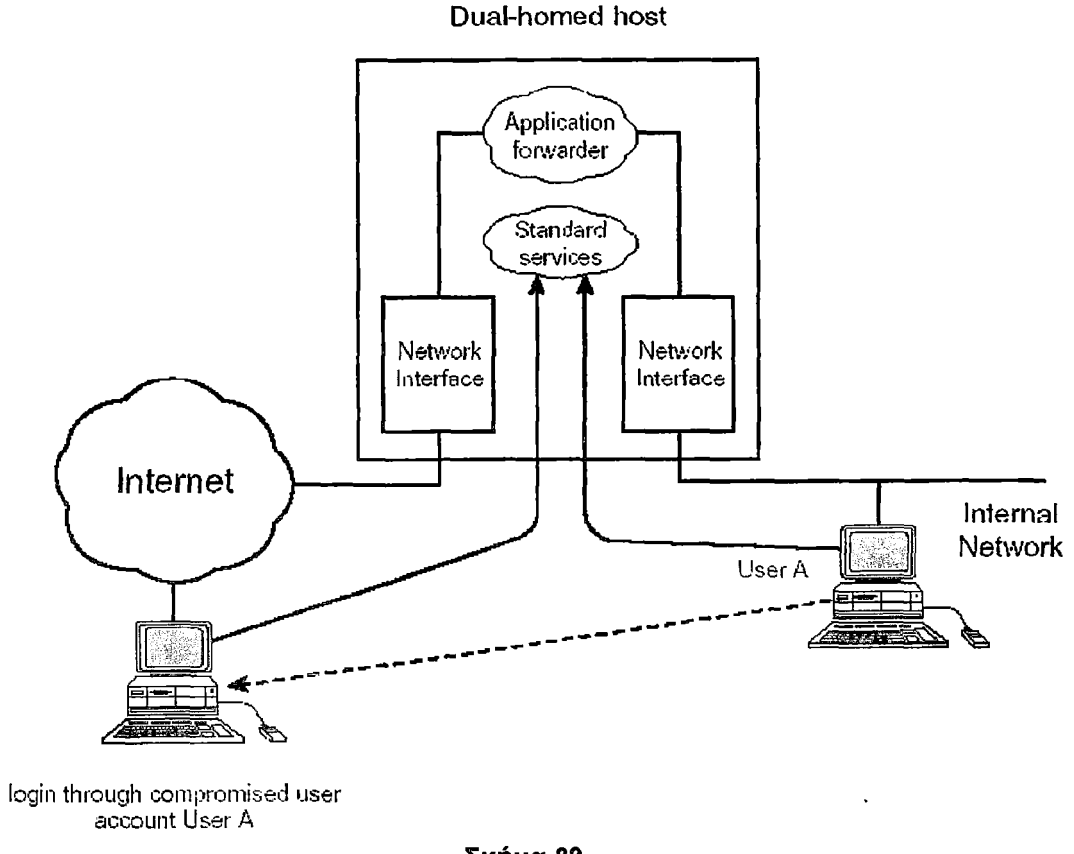
Υπηρεσίες διαδικτύου όπως το ηλεκτρονικό ταχυδρομείο και τα newsgroups αποκαλούνται και ως store-and-forward (αποθήκευση και προώθηση) υπηρεσίες. Επίσης, και ο παγκόσμιος ιστός μπορεί να θεωρηθεί γενικότερα ότι λειτουργεί με διαδικασίες αποθήκευσης και προώθησης αλλά συνήθως χαρακτηρίζεται από τους όρους "caching" και "proxy". Αν αυτές οι υπηρεσίες εκτελούνται πάνω σε έναν dual-homed host, τότε μπορούν να ρυθμιστούν με τέτοιο τρόπο που να μεταδίδονται υπηρεσίες από ένα δίκτυο σε ένα άλλο. Αν τα δεδομένα των εφαρμογών διασχίζουν ένα firewall, τότε οι agents των εφαρμογών προώθησης (ειδικό πακέτα λογισμικού που χρησιμοποιούνται στην προώθηση αιτημάτων μεταξύ δύο διασυνδεδεμένων δικτύων) μπορούν να τρέξουν στον dual-homed host (σχήμα). Μια άλλη τακτική είναι το να επιτρέπονται οι χρήστες να συνδέονται πρώτα οι χρήστες στον dual-homed host και έπειτα να έχουν προσπέλαση σε εξωτερικές υπηρεσίες με τη βοήθεια του εξωτερικού δικτυακού interface του host (σχήμα).



Σχήμα 21

Αν οι εφαρμογές προώθησης βρίσκονται σε χρήση, τα δεδομένα των εφαρμογών δεν μπορούν να διαπεράσουν τον dual-homed firewall εκτός και

αν αυτές εκτελούνται πάνω στο firewall μηχάνημα. Αν οι χρήστες έχουν το δικαίωμα να συνδεθούν απ' ευθείας με το firewall (σχήμα), τότε η ασφάλεια του μπορεί να τεθεί υπό κίνδυνο. Αυτό συμβαίνει γιατί ο dual-homed firewall είναι κεντρικό σημείο διασύνδεσης μεταξύ του εξωτερικού και εσωτερικού δικτύου. Εξ' ορισμού, ο dual-homed firewall βρίσκεται μέσα στη ζώνη υψηλού κινδύνου. Αν ο χρήστης επιλέξει ένα αδύναμο password ή να επιτρέψει να τεθεί σε κίνδυνο ο λογαριασμός του (με το να δώσει για παράδειγμα ηθελημένα το password του) η ζώνη κινδύνου μπορεί να επεκταθεί και στο εσωτερικό δίκτυο, μηδενίζοντας έτσι την χρησιμότητα του firewall.

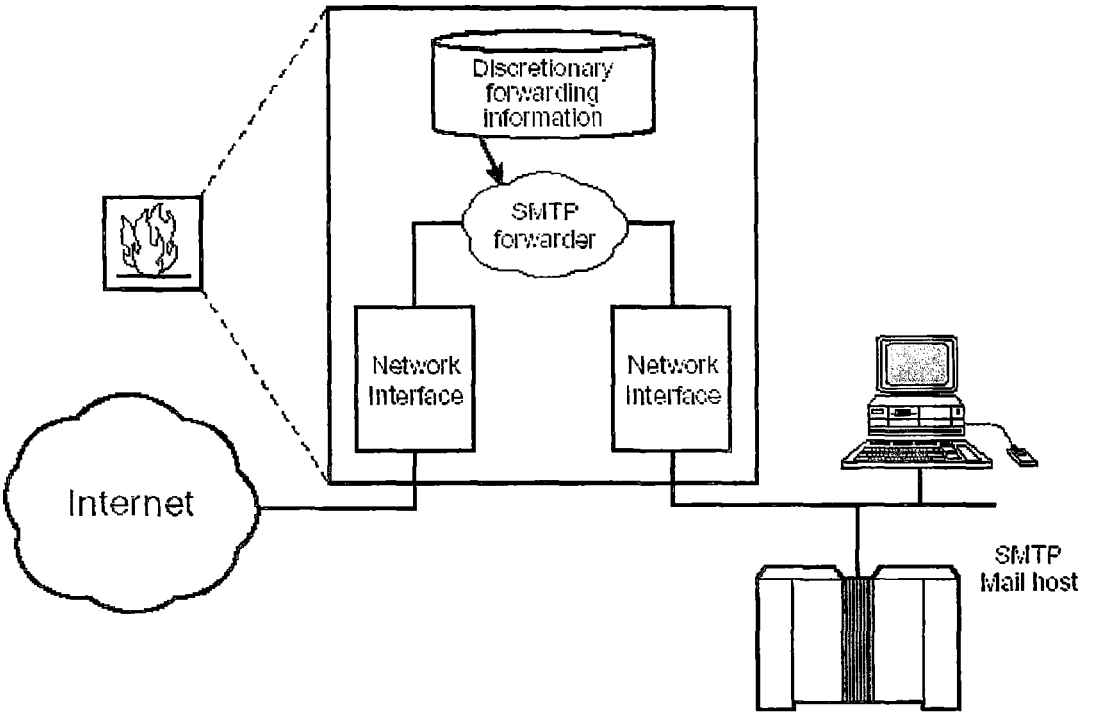


Σχήμα 22

Χαρακτηριστικό παράδειγμα υπηρεσιών διαδικτύου αποτελούν τα SMTP (ηλεκτρονικό ταχυδρομείο) και NNTP (newsgroups). Το σχήμα 23 απεικονίζει μια κατάσταση στην οποία ο dual-homed host είναι ρυθμισμένος με τέτοιο τρόπο ώστε να παρέχει προαιρετικά προώθηση των μηνυμάτων ηλεκτρονικού ταχυδρομείου μεταξύ ενός αναξιόπιστου εξωτερικού δικτύου και του εσωτερικού δικτύου.

Υπάρχουν και πολλές αρχιτεκτονικές που έχουν την δυνατότητα να συνδυάσουν proxying και packet filtering τεχνικές και αποτελούν καλή λύση όταν το προστατευόμενο δίκτυο είναι μικρό και δεν παρέχονται υπηρεσίες

προς το διαδίκτυο. Βέβαια, έτσι μπορεί από τη μία να υπάρχει ο συνδυασμός των πλεονεκτημάτων των δύο αυτών τεχνικών (όπως το να επιτρέπονται κάποια πρωτόκολλα σε υψηλές ταχύτητες, κρατώντας ταυτόχρονα λεπτομερή έλεγχο), αλλά από την άλλη "κληρονομούνται" και τα μειονεκτήματα τους. Επιπρόσθετα, υπάρχει και το ρίσκο της ύπαρξης μόνο μίας "οντότητας" ανάμεσα στο δίκτυο και στον εξωτερικό κόσμο.



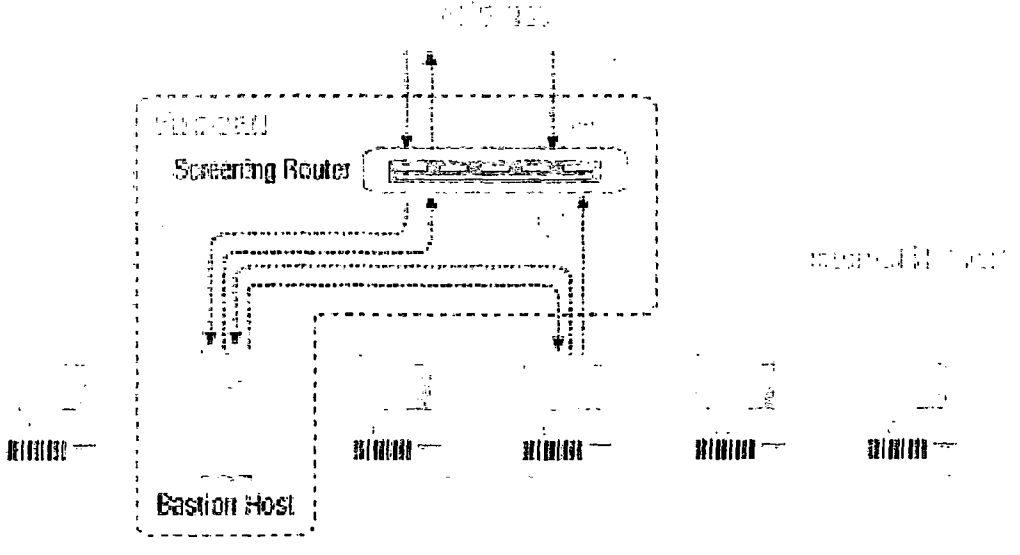
Σχήμα 23

5.2 SCREENED HOST ΑΡΧΙΤΕΚΤΟΝΙΚΕΣ

Προκειμένου να αναλυθούν οι αρχιτεκτονικές αυτές, απαιτείται ο ορισμός της έννοιας του bastion host. Ένας bastion host είναι η παρουσία, το "πρόσωπο" ενός δικτύου προς το διαδίκτυο. Μπορεί να παρομοιαστεί με το προθάλαμο ενός κτιρίου, όπου ο οποιοσδήποτε μπορεί να εισέλθει και να ρωτάει κάποιες πληροφορίες. Το αν τελικά αποκτά ο επισκέπτης αυτό που ζητά ή όχι εξαρτάται από την πολιτική ασφαλείας του κτιρίου. Όπως και ο προθάλαμος, έτσι και ο bastion host είναι εκτεθειμένος σε πιθανές επιθέσεις από εισβολείς. Αποτελεί το σύστημα το οποίο οι εξωτερικοί παράγοντες,

φιλικοί ή όχι, πρέπει να συνδεθούν προκειμένου με επικοινωνήσουν με το εσωτερικό δίκτυο και όπως είναι λογικό, η βαθμός προστασίας που εφαρμόζεται πάνω του είναι πολύ μεγάλος.

Ενώ η αρχιτεκτονική dual-homed host προσφέρει υπηρεσίες από έναν host που είναι εγκατεστημένος σε πολλαπλά δίκτυα, η screened host αρχιτεκτονική παρέχει υπηρεσίες από έναν host εγκατεστημένο μόνο στο εσωτερικό δίκτυο, χρησιμοποιώντας έναν ξεχωριστό δρομολογητή. Το σχήμα 7 δείχνει μια απλή εκδοχή μιας screened host αρχιτεκτονικής. Ο bastion host εγκαθίσταται "πάνω" από το εσωτερικό δίκτυο, ενώ η διαδικασία του packet filtering την εκτελεί ο screening router, που είναι τοποθετημένος με τέτοιο τρόπο ώστε ο bastion host να είναι είναι το μοναδικό σύστημα του δικτύου που εκκινήσει συνδέσεις με το διαδίκτυο (όπως για παράδειγμα να παραδώσει εισερχόμενη ηλεκτρονική αλληλογραφία). Αυτό όμως δεν σημαίνει ότι ο host αυτός αποδέχεται όλων των ειδών τις συνδέσεις. Κάθε εξωτερικό σύστημα που προσπαθεί να έχει πρόσβαση στο εσωτερικό δίκτυο θα πρέπει να συνδεθεί με αυτόν, οπότε και πρέπει τα επίπεδα ασφαλείας του να διατηρούνται σε υψηλά επίπεδα.



Σχήμα 24

Αυτή η αρχιτεκτονική, εξαιτίας του γεγονότος ότι επιτρέπει πακέτα να εισέρχονται από το διαδίκτυο, φαίνεται λιγότερη ασφαλής συγκριτικά με την dual-homed αρχιτεκτονική, η οποία είναι σχεδιασμένη να μην επιτρέπει τέτοια πακέτα. Στην πράξη όμως, και η dual-homed αρχιτεκτονική είναι επιρρεπής στον να αφήνει πακέτα να εισέρχονται. Επίσης, είναι γενικά αποδεκτό ότι είναι

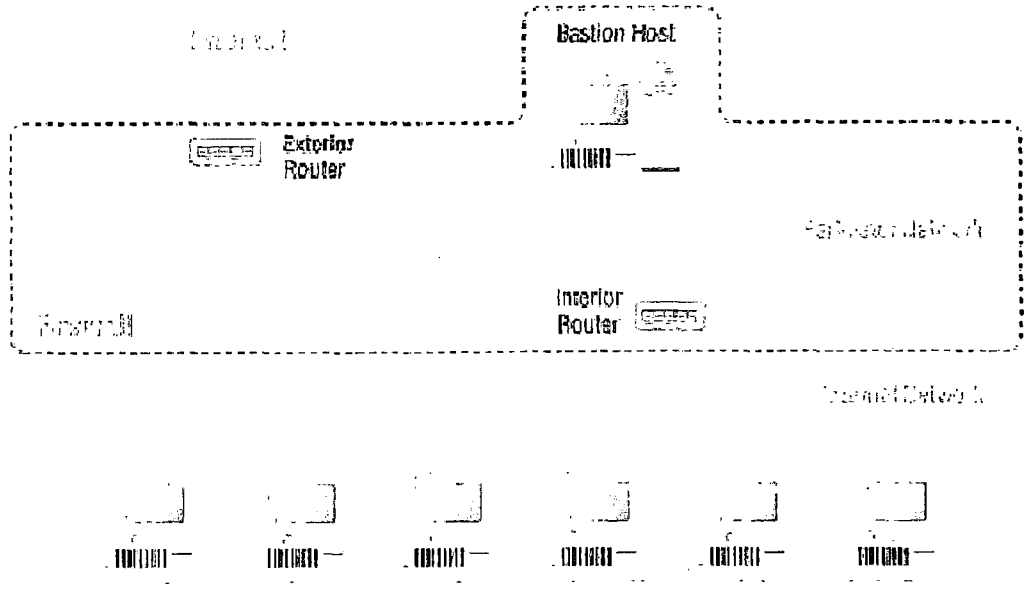
πιο εύκολο το να προστατεύσει κάποιος έναν δρομολογητή παρά έναν host. Στις περισσότερες των περιπτώσεων, η αρχιτεκτονική screened host αποδεικνύεται πιο χρηστική από αυτήν του dual-homed host.

Συγκριτικά όμως με τις υπόλοιπες αρχιτεκτονικές, όπως για παράδειγμα αυτή της screened subnet που θα εξετάσουμε παρακάτω, αυτή της screened host παρουσιάζει και κάποια μειονεκτήματα. Το μεγαλύτερο από αυτά είναι ότι αν καταφέρει κάποιος να εισβάλει στον bastion host, αυτομάτως έχει και τον έλεγχο του εσωτερικού δικτύου, αφού τίποτα δεν υπάρχει στο ενδιάμεσο να τον σταματήσει. Επίσης, εάν ο δρομολογητής αδρανοποιηθεί, τότε πάλι το δίκτυο είναι εύκολος στόχος για μια ενδεχόμενη επίθεση.

Συνοψίζοντας, η screened host αρχιτεκτονική αποτελεί καλή λύση όταν λίγες συνδέσεις προέρχονται από το διαδίκτυο (και πιο συγκεκριμένα, όταν ο host δεν εκτελεί χρέη web server) και όταν το επίπεδο ασφαλείας που έχει εφαρμοστεί στον bastion host είναι πολύ υψηλό.

5.3 SCREENED SUBNET ΑΡΧΙΤΕΚΤΟΝΙΚΕΣ

Η screened subnet αρχιτεκτονική είναι μια εξέλιξη της screened host αρχιτεκτονικής. Όπως και προηγούμενα αναφέρθηκε, αν στην screened host αρχιτεκτονική κάποιος εισβολέας αποκτήσει τον έλεγχο του bastion host τότε τίποτα δεν τον χωρίζει από το εσωτερικό δίκτυο. Προσθέτοντας όμως ένα επιπρόσθετο περιμετρικό δίκτυο το οποίο απομονώνει το εσωτερικό δίκτυο από το internet, αυξάνουμε σε σημαντικό βαθμό τον συνολικό βαθμό ασφάλειας.



Σχήμα 25

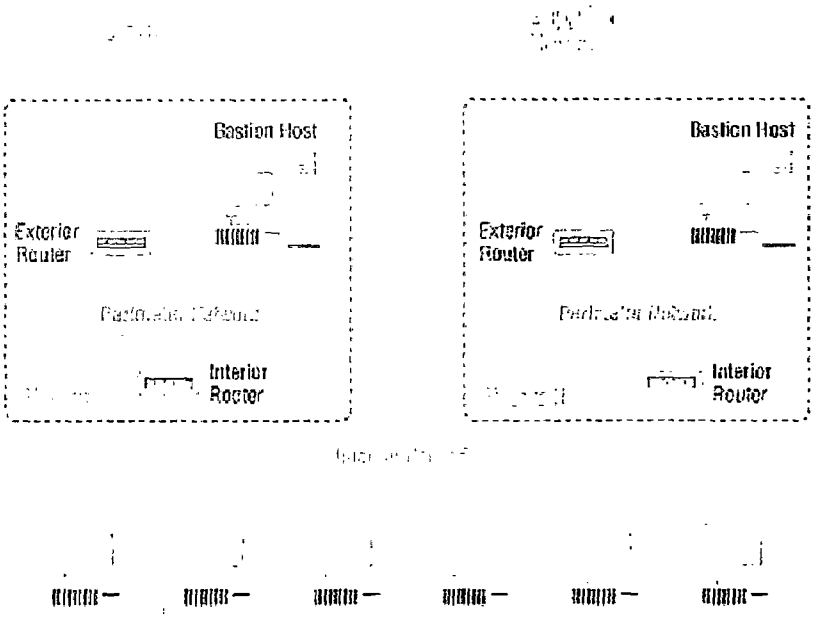
Όπως φαίνεται και στο σχήμα 8, μπορούμε να υλοποιήσουμε την screened subnet αρχιτεκτονική με την βοήθεια δύο δρομολογητών, οι οποίοι εκτελούν την packet filtering διαδικασία. Ο ένας συνδέει το εσωτερικό δίκτυο με το περιμετρικό, ενώ ο άλλος είναι υπεύθυνος για την δρομολόγηση πακέτων από το διαδίκτυο προς το περιμετρικό δίκτυο. Έτσι, για να εισχωρήσει κάποιος στο εσωτερικό δίκτυο, θα πρέπει να βρει τρόπο να υπερνικήσει και τους δύο δρομολογητές.

Ο φόρτος εργασίας σε θέματα packet filtering του εξωτερικού δρομολογητή είναι συγκριτικά λιγότερος σε σχέση με τον εσωτερικό. Το κύριο μέλημα του είναι να προστατεύει την περίμετρο (δηλαδή τον bastion host και τον εσωτερικό δρομολογητή από εξωτερικές επιθέσεις. Αυτές, πολλές φορές έχουν την μορφή των "πλαστογραφημένων" πακέτων, όπου τα πακέτα φαινομενικά δείχνουν να προέρχονται από το εσωτερικό δίκτυο, ενώ στην πραγματικότητα η προέλευση τους είναι εξωτερική. Επίσης, ο εξωτερικός router έχει την δυνατότητα να σταματά εξερχόμενα προς το διαδίκτυο πακέτα τα οποία θεωρεί ότι οι πηγαίες διευθύνσεις τους είναι ύποπτες, αφού γνωρίζει εκ των πραγμάτων ποιες είναι έγκυρες και ανήκουν πραγματικά στο εσωτερικό δίκτυο.

Από την άλλη πλευρά, ο εσωτερικός δρομολογητής προστατεύει το εσωτερικό δίκτυο από το περιμετρικό και το διαδίκτυο. Διαφέρει με τον εξωτερικό ως προς τις υπηρεσίες που παρέχει. Συνήθως, αυτές περιορίζονται στις απολύτως απαραίτητες, όπως για παράδειγμα υπηρεσίες

ηλεκτρονικού ταχυδρομείου SMPT και DNS, και έτσι σε περίπτωση που ο bastion host δεχθεί επίθεση, να προστατευθεί το ενδοδίκτυο όσο το πιθανό περισσότερο.

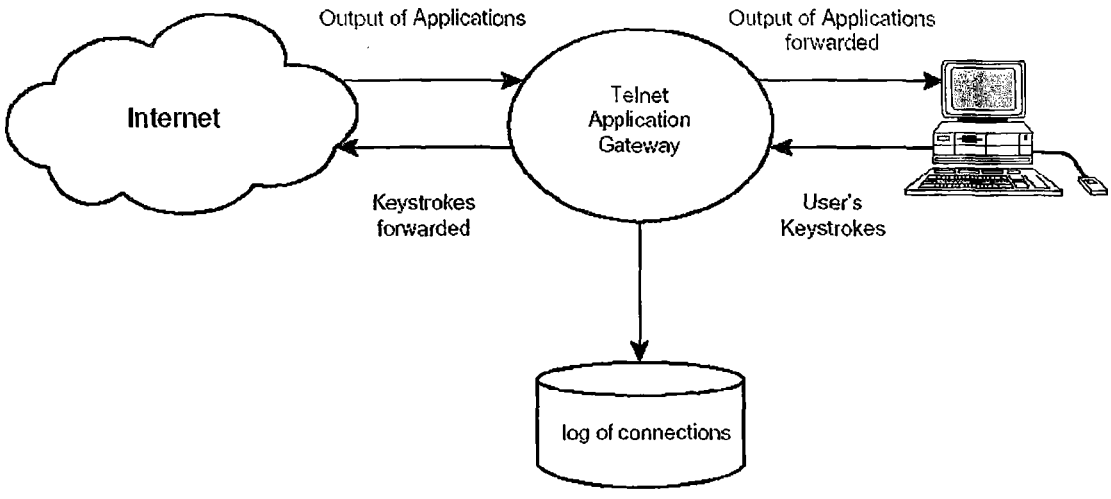
Σε πολλές περιπτώσεις χρησιμοποιούνται και οι πιο πολύπλοκες μορφές της αρχιτεκτονικής αυτής, όπως αυτή των ανεξάρτητων screened subnets με πολλαπλούς δρομολογητές, όπως φαίνονται στο σχήμα 9. Με αυτόν τον τρόπο, αν υποθέσουμε ότι υπάρχουν δύο περιμετρικά δίκτυα, οι σημαντικές και ευαίσθητες πληροφορίες να τις χειρίζεται το ένα μέρος ενώ το άλλο θα είναι υπεύθυνο για τις υπηρεσίες διαδικτύου. Αν και αυτή η τεχνική είναι πιο δύσκολη στην εγκατάσταση και στην συντήρηση, παρέχει πολύ καλά επίπεδα ασφάλειας και αξιοπιστίας



Σχήμα 26

5.4 APPLICATION LEVEL GATEWAYS

Οι application level gateways (πύλες επιπέδου εφαρμογών) είναι προγραμματισμένες να "καταλαβαίνουν" την κίνηση (traffic) των πακέτων στο επίπεδο εφαρμογών (επίπεδο 7 στο μοντέλο αναφοράς του OSI). Συνεπώς μπορούν να παρέχουν έλεγχο στην πρόσβαση σε επίπεδο χρήστη και σε επίπεδο πρωτοκόλλου εφαρμογών. Επιπρόσθετα, μπορούν να χρησιμοποιηθούν στην διατήρηση "έξυπνων" ημερολογίων καταγραφής της χρήσης όλης των εφαρμογών. Η ικανότητα της καταγραφής και ελέγχου όλης της εισερχόμενης και εξερχόμενης κίνησης είναι ένα από τα κυριότερα πλεονεκτήματα της χρήσης των application level gateways.



Σχήμα 27

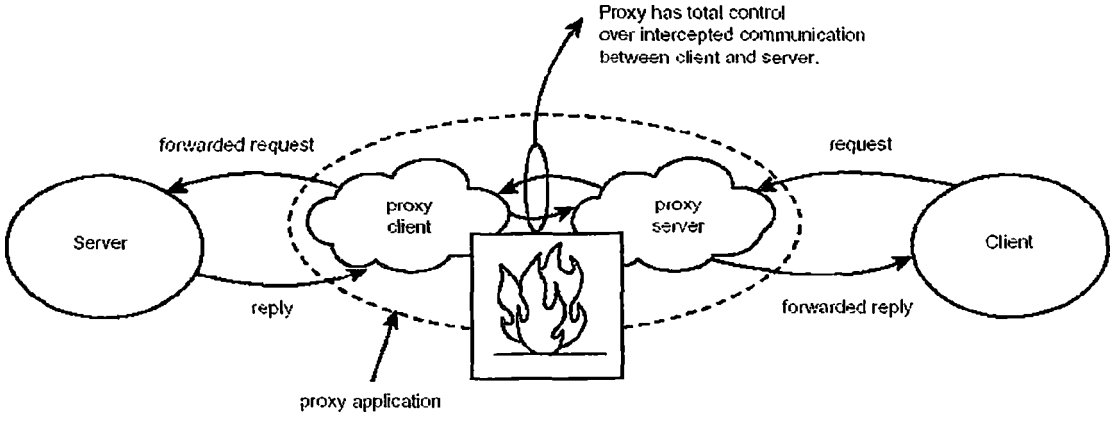
Για κάθε δικτυακή εφαρμογή, οι application-level gateways χρησιμοποιούν έναν ειδικό κώδικα, και εξαιτίας αυτού, οι πύλες παρέχουν σημαντικό βαθμό ασφάλειας. Για κάθε νέο είδος εφαρμογών που προστίθεται στο δίκτυο και απαιτούν προστασία, απαιτείται εγγραφή νέου, εξειδικευμένου κώδικα. Συνεπώς, οι περισσότερες πύλες παρέχουν ένα περιορισμένο υποσύνολο βασικών εφαρμογών και υπηρεσιών.

Προκειμένου να χρησιμοποιήσουν οι χρήστες application level gateways, θα πρέπει να συνδεθούν στο application gateway μηχάνημα ή να εκτελέσουν μία συγκεκριμένη client υπηρεσία εφαρμογής σε κάθε host που θα υλοποιήσει την συγκεκριμένη υπηρεσία. Κάθε application-specific gateway υπομονάδα μπορεί να έχει το δικό της σύνολο από διαχειριστικά εργαλεία και γλώσσα εντολών.

Ένα μειονέκτημα των application level gateways είναι ότι για κάθε δικτυακή εφαρμογή πρέπει να γραφτεί εξειδικευμένο πρόγραμμα. Το γεγονός αυτό όμως αποτελεί πλεονέκτημα από πλευρά ασφάλειας, γιατί δεν υπάρχει η δυνατότητα εισχώρησης μέσα από έναν firewall εκτός και αν παρέχεται μια συγκεκριμένη application level πύλη.

Τα εξειδικευμένα αυτά προγράμματα λειτουργούν σαν έναν "proxy" που δέχονται εισερχόμενες κλήσεις και πραγματοποιούν έλεγχο με βάση μια λίστα στην οποία είναι καταγραμμένες ποιες είναι επιτρεπτές και ποιες όχι. Ο proxy (αντιπρόσωπος) δρα στην προκειμένη περίπτωση σαν application server proxy. Με το που δέχεται την κλήση, και αφού βεβαιωθεί ότι ανήκει σε μία από τις επιτρεπόμενες, ο proxy προωθεί το αίτημα στον διακομιστή, λειτουργώντας ταυτόχρονα σαν client, λαμβάνοντας τα εισερχόμενα αιτήματα και server,

προωθώντας το αίτημα αυτό (σχήμα 28). Αφότου έχει εγκατασταθεί η σύνδεση-συνεδρία, ο application proxy εκτελεί χρέη αναμεταδότη και αντιγράφει δεδομένα μεταξύ του client που ξεκίνησε την εφαρμογή και του server. Επειδή όλα τα δεδομένα μεταξύ τους αναχαιτίζονται από τον application proxy, αυτός έχει τον πλήρη έλεγχο της συνεδρίας και μπορεί να εκτελέσει λεπτομερέστατα την απαιτούμενη καταγραφή στο ημερολόγιο.

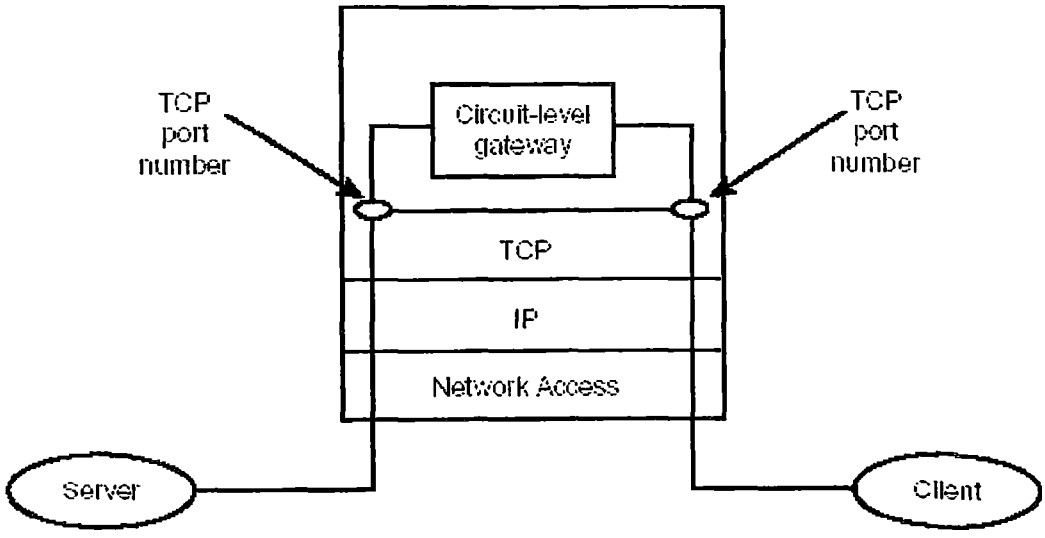


Σχήμα 28

Προκειμένου κάποιος χρήστης να συνδεθεί με μια εφαρμογή proxy, πολλές application level gateways απαιτούν την εκτέλεση κάποιου εξειδικευμένου client προγράμματος στο μηχάνημα του. Εναλλακτικά, υπάρχει η δυνατότητα της χρήσης της εντολής telnet για να καθοριστεί σε ποια θύρα είναι διαθέσιμη η proxy υπηρεσία. Αν για παράδειγμα η εφαρμογή βρίσκεται στον gatekeeper.kinetics.com host, θύρα 63, ο χρήστης θα πρέπει να χρησιμοποιήσει την εντολή "telnet gatekeeper.kinetics.com 63".

Μετά που θα επιτευχθεί η σύνδεση στην συγκεκριμένη θύρα, ο χρήστης βλέπει ένα ειδικό prompt που προσδιορίζει την proxy εφαρμογή και θα πρέπει να εκτελέσει ειδικές εντολές προκειμένου να προσδιορίσει τον προοριζόμενο server. Ανεξαρτήτου με το ποια μέθοδος χρησιμοποιείται, ο client συνήθως τροποποιείται ώστε να συνδέεται στο proxy μηχάνημα και να το καθοδηγεί στο που θα συνδεθεί. Έπειτα, το proxy μηχάνημα συνδέεται με τον τελικό προορισμό και αποστέλλει τα δεδομένα.

Ένας διαφορετικός τύπος application level gateway είναι τα αποκαλούμενα circuit-gateway. Στην περίπτωση αυτή, τα πακέτα αποστέλλονται σε επίπεδο εφαρμογής του χρήστη. Γενικά, μια circuit-gateway χρησιμοποιείται για αναμετάδοση πακέτων μεταξύ των δύο τηλεπικοινωνιακών άκρων, όπου απλά αντιγράφονται δεδομένα από και προς τις δύο άκρες (σχήμα 29).



Σχήμα 29

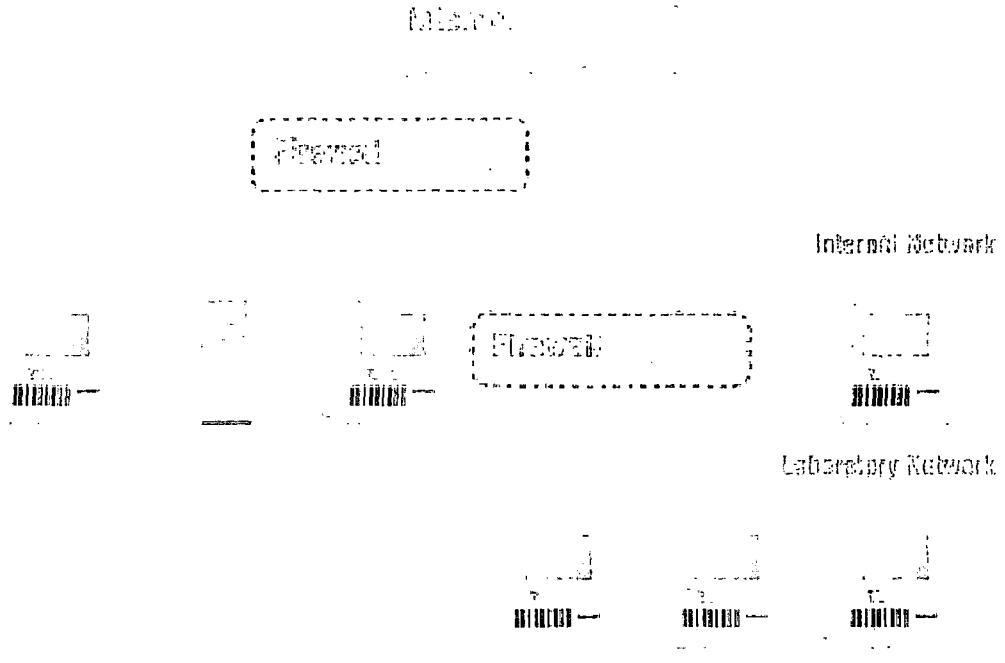
Οι circuit-gateway gateways αποτελούν μια πιο ευέλικτη και γενικευμένη προσέγγιση για την δημιουργία application gateways. Αν και μπορεί να συμπεριλαμβάνουν κώδικα προκειμένου να υποστηρίξουν μια συγκεκριμένη TCP/IP εφαρμογή, αυτό συμβαίνει σε περιορισμένη κλίμακα. Εάν γενικότερα υποστηρίζουν μια εφαρμογή, το πιο πιθανό είναι να είναι TCP/IP εφαρμογή.

Σε αυτού του είδους gateways, υπάρχει η πιθανότητα να χρειαστεί εγκατάσταση ειδικού client λογισμικού και οι χρήστες ενδέχεται να αναγκαστούν να αλληλεπιδράσουν με ένα τροποποιημένο interface ή, σε τελική ανάλυση, να αλλάξουν τον συνήθη τρόπο εργασίας τους. Η εγκατάσταση και η ρύθμιση τέτοιων εφαρμογών σε κάθε εσωτερικό host μπορεί να αποβεί χρονοβόρα και επιρρεπής σε λάθη διαδικασία για μεγάλα ετερογενή δίκτυα εξαιτίας των διαφορών που συναντώνται σε πλατφόρμες και λειτουργικά συστήματα.

Επειδή κάθε πακέτο τίθεται υπό επεξεργασία από πακέτα λογισμικών που τρέχουν στο επίπεδο εφαρμογών, παρουσιάζεται μείωση στην απόδοση του host. Κάθε πακέτο τίθεται δύο φορές υπό επεξεργασία από όλα τα επικοινωνιακά layers και απαιτεί επεξεργασία και από το επίπεδο του χρήστη. Η application level πύλη (είτε είναι bastion-host είτε dual-homed host) παραμένει εκτεθειμένη σε όλο το δίκτυο, όπου σε αυτή την περίπτωση μπορούμε να εφαρμόσουμε άλλες τεχνικές για την προστασία της, όπως ένα packet filtering σύστημα.

5.5 INTERNAL FIREWALL

Η λογική ενός εσωτερικού firewall είναι αρκετά απλή, όσο αφορά την κατανόηση της. Εάν κάποιος επιθυμεί, μπορεί να τοποθετήσει έναν μηχανισμό προστασίας μέσα στο εσωτερικό δίκτυο, όπως φαίνεται και στο σχήμα. Υπάρχουν πολλοί λόγοι για την τακτική αυτή. Ξεφεύγοντας από την νοοτροπία του απλού χρήστη και των αναγκών του, μια μεγάλη εταιρεία είναι πιθανό να διαχωρίζεται σε πολλά τμήματα. Αυτό κατ' ανάγκη δεν σημαίνει ότι θα πρέπει και τα δίκτυα της να είναι διαφορετικά. Μια άλλη περίπτωση μπορεί να είναι και ένα κοινό δίκτυο το οποίο μοιράζονται δύο διαφορετικοί οργανισμοί.



Σχήμα 30

Είναι λογικό ότι κάποια μέρη του δικτύου μιας εταιρείας να χρειάζονται περισσότερη προστασία από κάποια άλλα, όπως είναι για παράδειγμα ένα λογιστήριο. Άλλο παράδειγμα μπορεί να αποτελέσει και ένα δίκτυο ενός σχολείου ή πανεπιστημίου, όπου σε κάποιο χώρο υπάρχουν κοινόχρηστοι υπολογιστές. Σε τέτοιες καταστάσεις απαιτείται αυξημένη ασφάλεια προκειμένου να διασφαλιστούν σημαντικά και πολύτιμα μέρη ενός δικτύου.

ΚΕΦΑΛΑΙΟ 6ο : Η ΚΑΤΑΣΤΑΣΗ ΣΗΜΕΡΑ

6.1 ΕΡΕΥΝΑ ΑΓΟΡΑΣ

Αναμφίβολα, η χρήση των υπολογιστών και κατ' επέκταση των δικτύων τη σημερινή εποχή είναι τεράστια. Όλο και περισσότερες ανθρώπινες λειτουργίες που αφορούν την εργασία και την καθημερινότητα περνούν στα χέρια και στις δυνατότητες αυτών των "θαυματουργών" μηχανημάτων. Το μέγεθος των πληροφοριών που διακινούνται καθημερινά σε οποιασδήποτε μορφής δίκτυα είναι ασύλληπτα μεγάλος. Φυσικά, η ανάγκη προστασία τους είναι επιτακτική και όχι πάντα εύκολη και αποτελεσματική.

Τα firewall συστήματα εξελίχθηκαν και αυτά με εντυπωσιακό ρυθμό κατά τη διάρκεια των τελευταίων ετών. Αρχικά, τα firewalls ήταν χειροποίητα συστήματα με δύο δικτυακά interfaces τα οποία προωθούσαν τα πακέτα μεταξύ δύο διαφορετικών δικτύων και μόνο εξειδικευμένο προσωπικό με ειδική τεχνική κατάρτιση και διαχειριστικό ταλέντο μπορούσε να τα λειτουργήσει και να τα διαχειριστεί. Κατανοώντας την ανάγκη και το κενό που υπήρχε στην τεχνολογία αυτή, ο Marcus Ranum, εργαζόμενος στην εταιρεία TIS, ανέπτυξε στις αρχές του 1990 τον πρώτο εμπορικό firewall, με την ονομασία "Firewall Toolkit". Ο στόχος του ήταν η απλοποίηση της ανάπτυξης και εφαρμογής των firewalls, ελαχιστοποιώντας τον χρόνο και προσπάθεια που απαιτούσε μέχρι τότε η κατασκευή ενός firewall. Το γνωστό στις ημέρες μας firewall προϊόν Gauntlet εξελίχθηκε από το αρχικό "Firewall Toolkit" και η TIS εξαγοράσθηκε από την Network Associates, Inc. Και άλλοι κατασκευαστές μπήκαν στην αγορά των firewall, όπως για παράδειγμα οι Check Point, Secure Computing, Symantec και φυσικά, η Cisco. Η εταιρεία RBC Capital Markets πραγματοποίησε το 2002 μια έρευνα η οποία έδειξε ότι στο έτος 2000, η αξία της αγοράς των firewall έφτανε το ποσό των 736 εκατομμυρίων δολαρίων, με πρόβλεψη για ετήσιο ρυθμό ανάπτυξης της τάξης του 16% για τα επόμενα πέντε χρόνια.

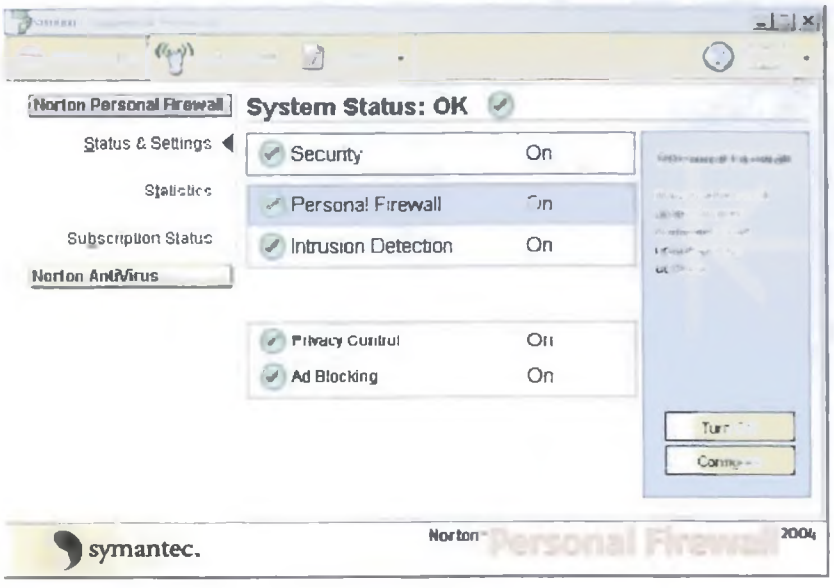
Οι firewalls έχουν διττή "φυσική" υπόσταση. Μπορούμε να τους συναντήσουμε είτε με τη μορφή software, δηλαδή προγραμμάτων που εγκαθίστανται πάνω σε ένα κοινό λειτουργικό ή λειτουργικών συστημάτων που εκτελούν χρέη firewall (όπως το NetBSD και το Solaris της Sun), είτε με τη μορφή hardware, όπως είναι για παράδειγμα ένας screening router. Στον ακόλουθο πίνακα απεικονίζονται οι πρωτοπόροι κατασκευαστές τεχνολογιών firewall.

Firewall Vendor	Form	OS
3Com Corporation & SonicWALL	Hardware	Custom
Check Point Software Technologies	Both	Windows, Solaris, IPSO
Cisco Systems, Inc.	Hardware	Custom
CyberGuard	Hardware	Custom
Microsoft	Software	Windows 2000 Server
NetScreen	Hardware	Custom
Novell	Software	Netware
Secure Computing	Hardware	Custom
Stonesoft, Inc.	Software	Linux
Symantec Corporation	Software	Windows, Solaris
WatchGuard Technologies, Inc.	Hardware	Custom

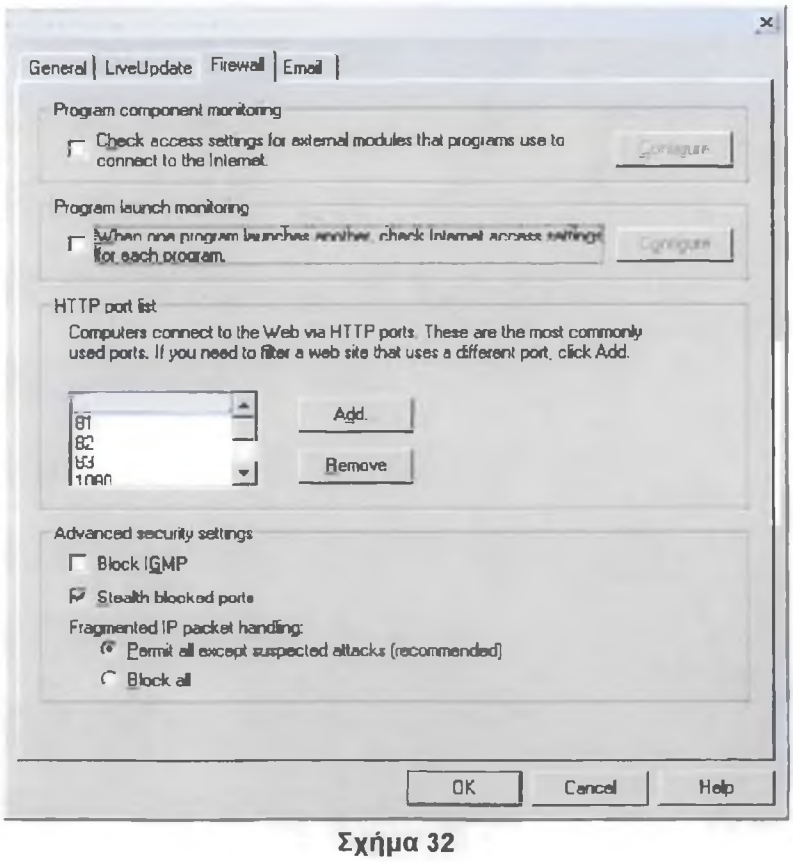
Οι κατασκευαστές που παρέχουν αποκλειστικά software λύσεις βασισμένο σε κοινά λειτουργικά ευρείας χρήσης γενικά εστιάζονται στο να αποτρέψουν επιθέσεις στο λειτουργικό πάνω στο οποίο τοποθετείται ο firewall και όχι στον firewall τον ίδιο, αφού η πλειοψηφία των hackers εστιάζουν τις προσπάθειες τους στις αδυναμίες των λειτουργικών συστημάτων, σε μια απόπειρα να δρομολογηθούν πακέτα προτού τα "δει" ο firewall.

Τα προϊόντα της εταιρείας Symantec αποτελούν την πιο δημοφιλή χρήση για οικιακή χρήση, χωρίς βέβαια να αποκλείονται και οι μικρές επιχειρήσεις. Πιο συγκεκριμένα, το πακέτο "Norton Personal Firewall" είναι η πιο ενδεδειγμένη λύση για απλούς χρήστες και για μικρά εταιρικά δίκτυα και το κόστος απόκτησης του είναι πολύ χαμηλό.

Στο σχήμα 31 απεικονίζεται το κύριο μενού του Norton Personal Firewall. Στις επόμενες εικόνες παρουσιάζονται κάποια από το βασικά υπομενού της εφαρμογής, όπου μπορεί ο χρήστης να ρυθμίσει διάφορες επιλογές, όπως τα επιτρεπόμενα HTTP ports στα οποία ο υπολογιστής θα συνδέεται στο διαδίκτυο και η διαχείριση fragmented πακέτων (σχήμα 32).



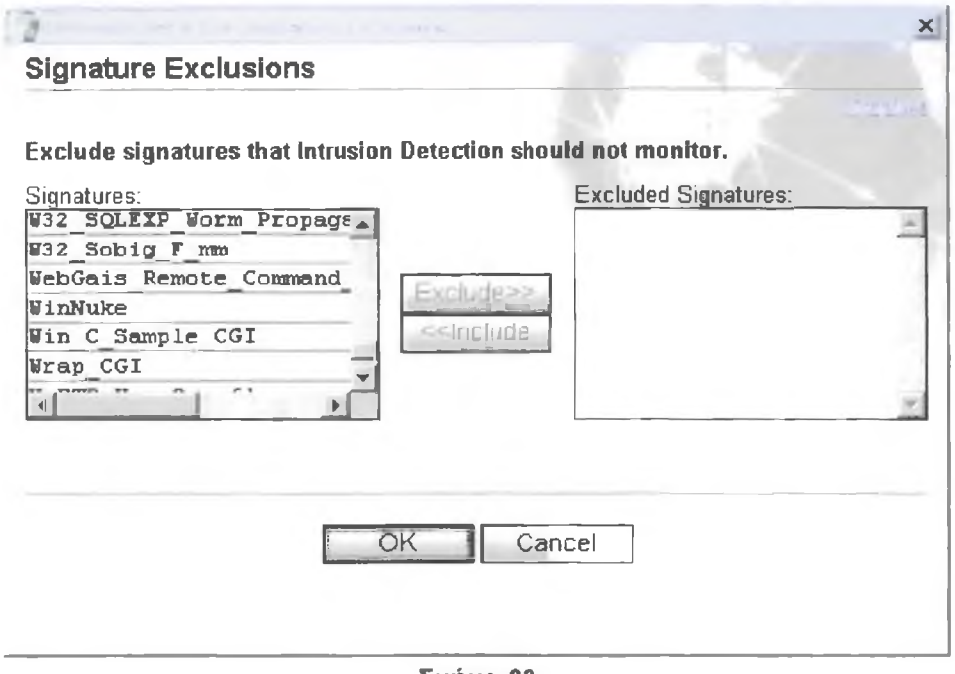
Σχήμα 31
Βασικό μενού του Norton Personal Firewall



Σχήμα 32

Για κάθε ενδεχόμενη απειλή που αναγνωρίζεται, η εφαρμογή αυτή δημιουργεί την δικιά της υπογραφή. Στο σχήμα 33 απεικονίζεται το μενού στο οποίο μπορεί κάποιος να τροποποιήσει την αντιμετώπιση του προγράμματος απέναντι στις απειλές αυτές. Για παράδειγμα, αν ο χρήστης δέχεται συνεχώς

προειδοποιητικά μηνύματα τα οποία όμως θεωρεί ασφαλή, μπορεί με τις κατάλληλες ρυθμίσεις, να αποτρέψει την εμφάνιση τους. Επίσης, στο σχήμα φαίνεται και η προεπιλογή για κάποιες υπογραφές που έχουν γίνει από την Symantec. Για παράδειγμα, το WinNuke είναι ένα πρόγραμμα γραμμένο σε ελάχιστες γραμμές κώδικα της γλώσσας C, το οποίο μπορεί να φέρει έναν υπολογιστή με λειτουργικό Windows 98 στην γνωστή "μπλε οθόνη" (το σημείο όπου το λειτουργικό έχει καταρρεύσει και χρειάζεται επανεκκίνηση), εκμεταλλεύοντας κάποιες αδυναμίες του συγκεκριμένου λειτουργικού.

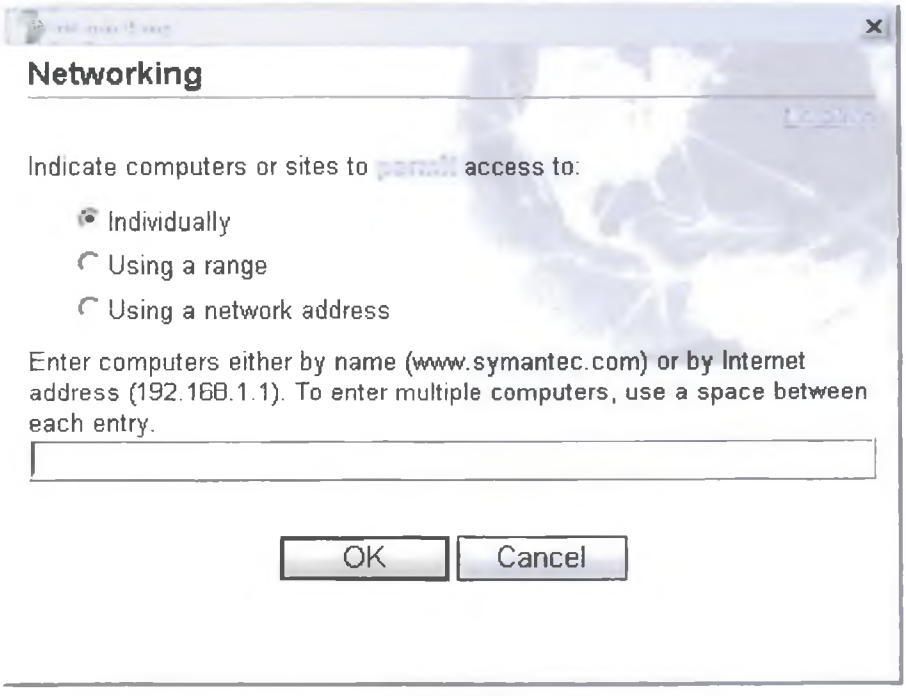


Σχήμα 33

Πολλές φορές, εγκαθιστώντας software firewalls, παρουσιάζονται προβλήματα όσο αφορά την επικοινωνία υπολογιστών σε ένα δίκτυο. Το γεγονός αυτό παρουσιάζεται αρκετά συχνά, ειδικά σε χρήστες με λιγότερη εμπειρία. Όπως φαίνεται και στο σχήμα 34, υπάρχει η δυνατότητα να καθοριστεί μέσα από τον Norton Personal Firewall ποιοι υπολογιστές επιτρέπονται, είτε με τον καθορισμό της IP διεύθυνσης είτε με την μορφή URL, να έχουν πρόσβαση σε έναν υπολογιστή.

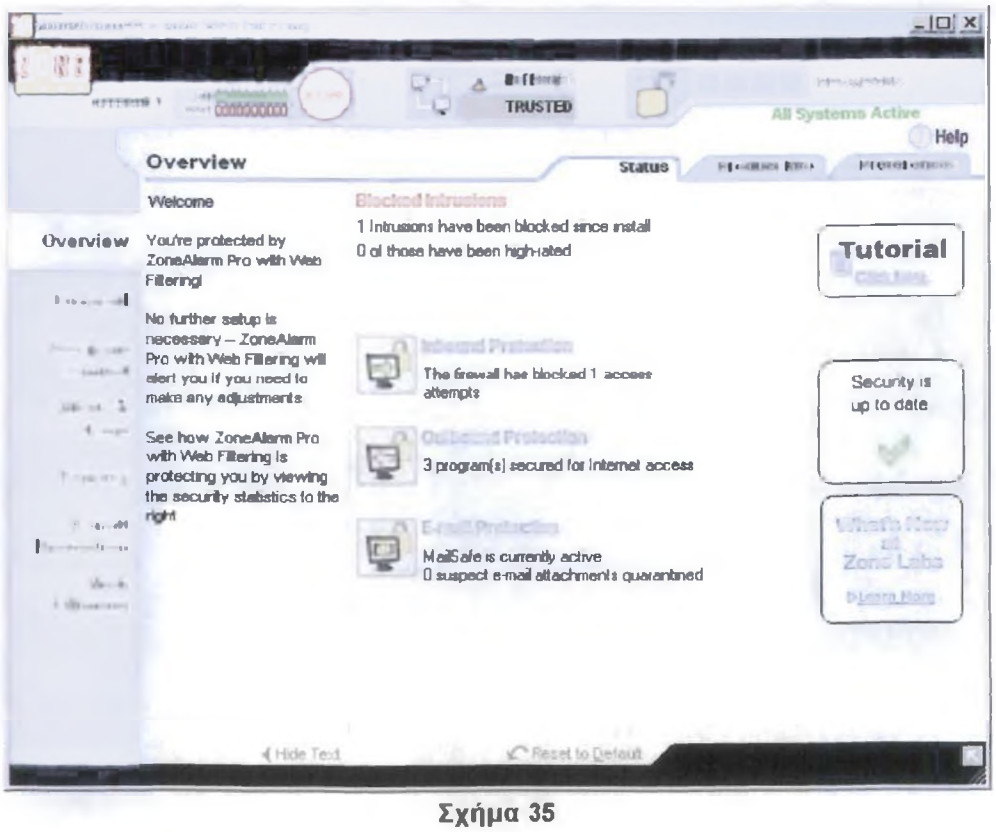
Πέρα όμως από καθαρά firewall παροχές, εφαρμογές τέτοιου τύπου πλέον έχουν εφοδιαστεί και με εργαλεία του τύπου Web Filtering και Ad-Blocking, με τα οποία προστατεύεται ο χρήστης από επικίνδυνες και ενοχλητικές διαφημίσεις σε ιστοσελίδες, οι οποίες πολλές φορές μπορούν να θέσουν σε πολλούς μπελάδες τους χρήστες. Πρόσφατο παράδειγμα αποτελούν οι λεγόμενοι dialers, προγράμματα τα οποία εγκαθίστανται στον

υπολογιστή και καλούν μέσω των modems σε νούμερα εξωτερικών χωρών και ακριβών τηλεφωνικών υπηρεσιών.



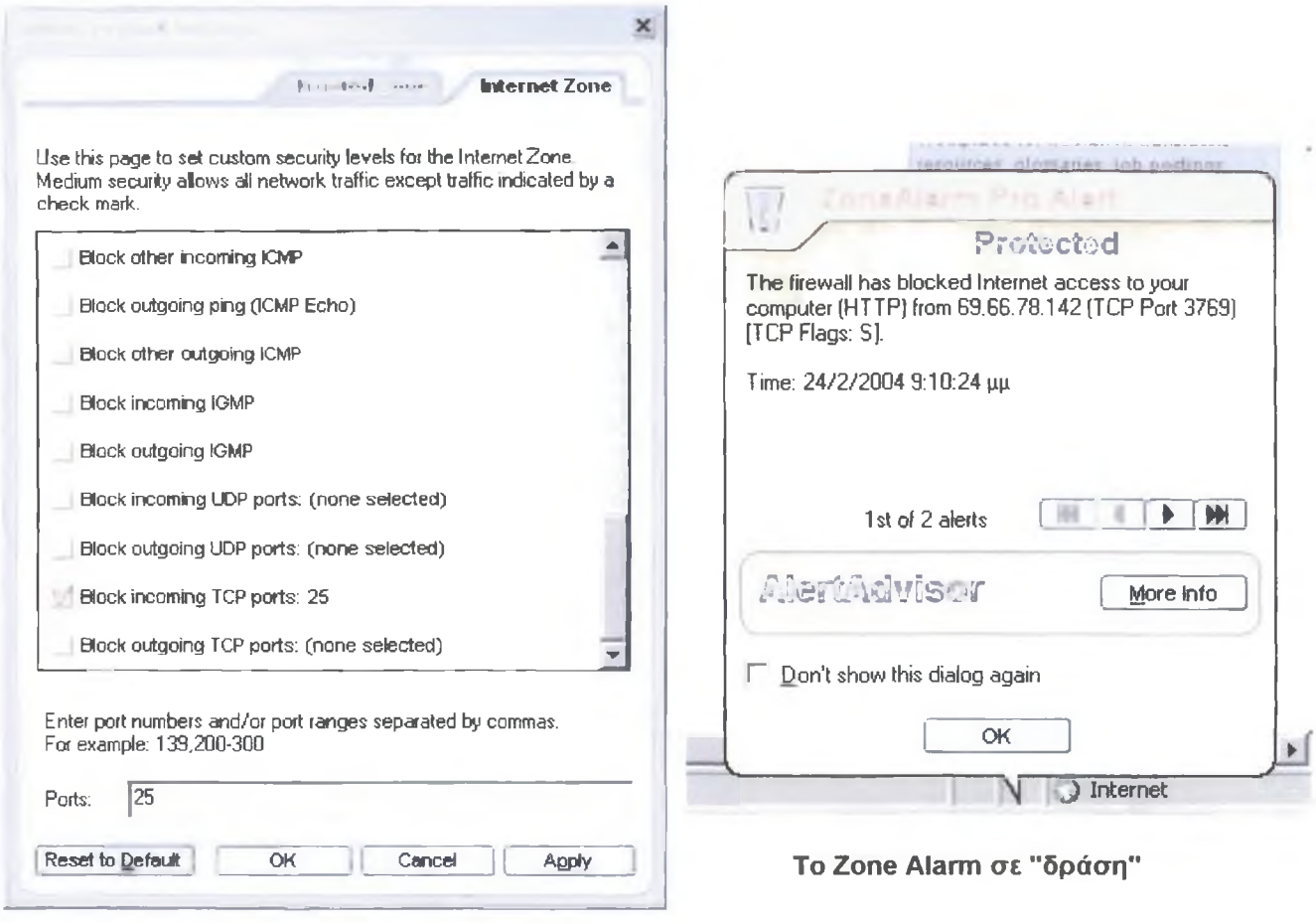
Σχήμα 34

Άλλο μία δημοφιλής εφαρμογή η οποία διακρίνεται για την αποτελεσματικότητα της είναι το ZoneAlarm της εταιρείας ZoneLabs (Σχήμα 35).



Σχήμα 35

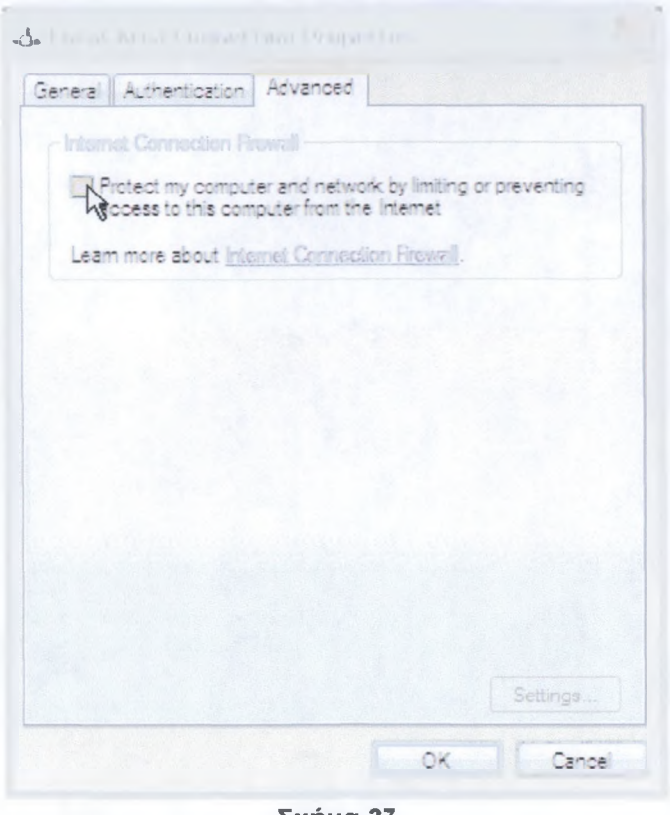
Η εφαρμογή αυτή απαιτεί για την σωστή και αποτελεσματική χρήση του ελάχιστα καλύτερες γνώσεις από αυτή της Symantec. Στο σχήμα 36 απεικονίζεται ένα υπομενού της εφαρμογής αυτής, στο οποίο επιλέχτηκε η απόρριψη εισερχόμενων μηνυμάτων ηλεκτρονικού ταχυδρομείου (port 25), και μια προειδοποίηση στον χρήστη που αφορά την απόρριψη ανεπιθύμητης εισόδου στον υπολογιστή μας.



Το Zone Alarm σε "δράση"

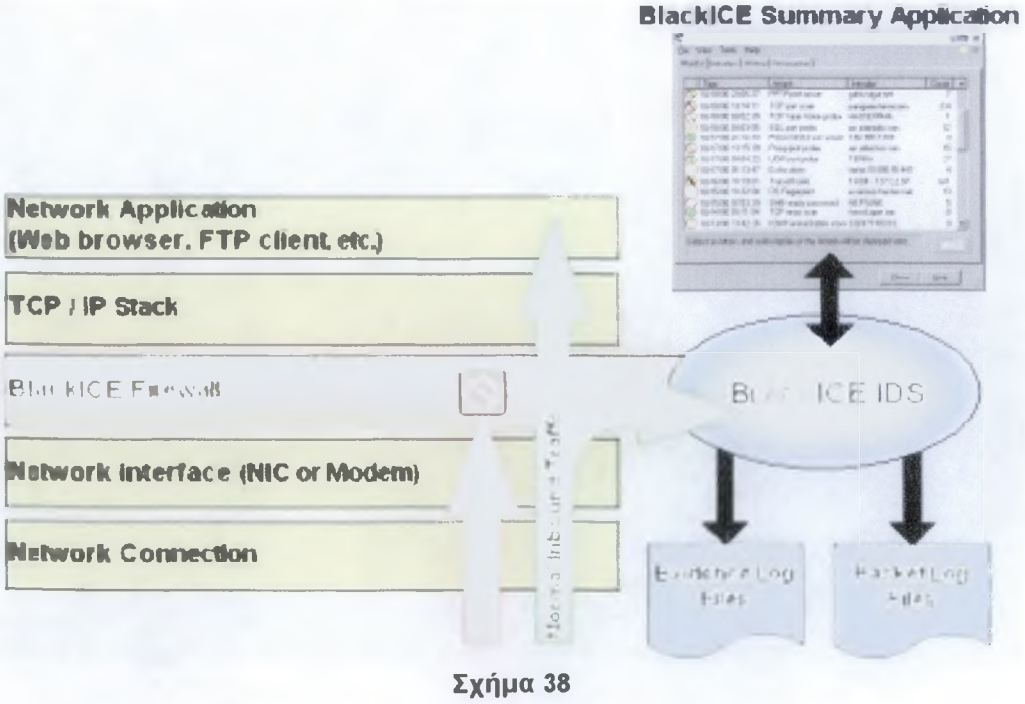
Σχήμα 36

Το τελευταίο λειτουργικό σύστημα της Microsoft, τα Windows XP έχουν ενσωματώσει μια ψευδο-firewall δυνατότητα (σχήμα 37), η οποία βέβαια δεν συγκρίνεται με τα πολύ πιο εξελιγμένα προγράμματα. Έχει αποδειχθεί ότι μπορεί μεν αυτή η δυνατότητα να παρέχει μια αυξημένη προστασία σε έναν χρήστη, αλλά κάποιος "μελετημένος" καλά hacker μπορεί να τον προσπεράσει χωρίς ιδιαίτερες δυσκολίες, εκμεταλλεύοντας άλλα κενά και σχεδιαστικά λάθη στο λειτουργικό.

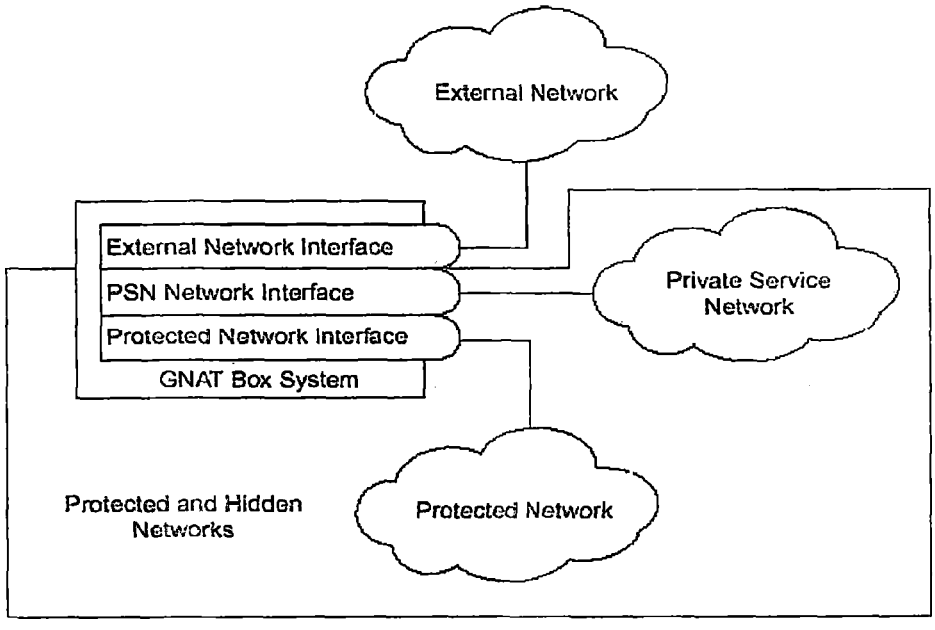


Σχήμα 37

Αξίζει να αναφερθούμε και σε δύο ακόμα λύσεις firewall, η οποίες κατέχουν ικανοποιητικό μερίδιο της αγοράς. Πρόκειται για το BlackICE της Internet Security Systems, Inc (σχήμα 38) και το GNAT Box της Global Technologies Associates, Inc (σχήμα 39).



Σχήμα 38

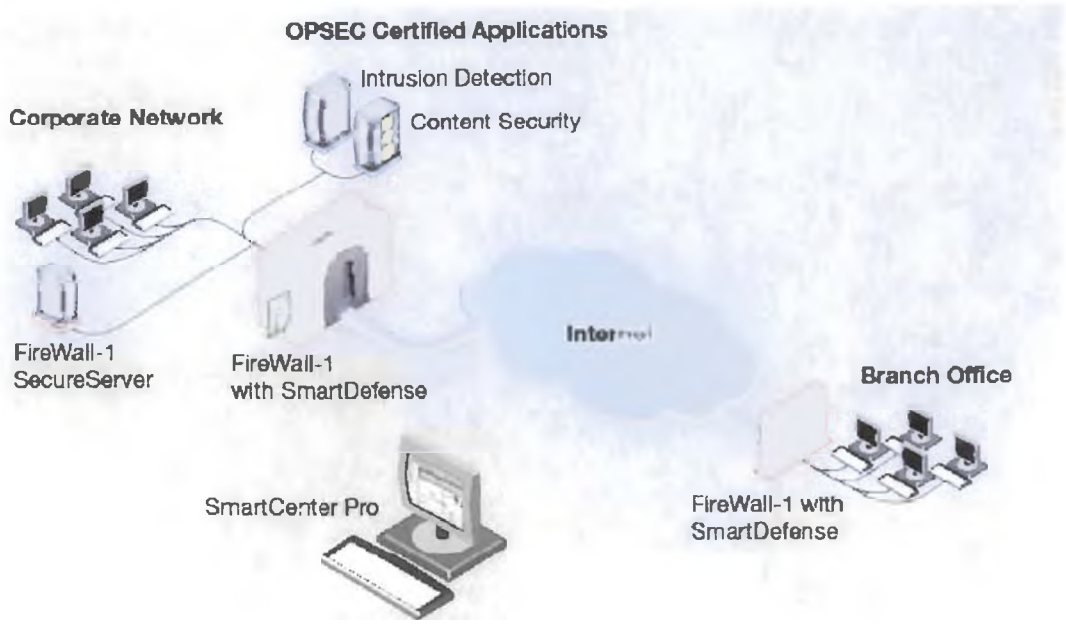


The Standard GNAT Box System Diagram

Σχήμα 39

Το BlackICE είναι ένα firewall που εργάζεται στο επίπεδο εφαρμογών και ασφαλίζει όλες τις θύρες και υπηρεσίες που είναι "ανοικτές" σε έναν διακομιστή και παρέχει, πέρα από ασφάλεια στην περίπτωση εισβολής, έλεγχο για ιούς και worms. Από την άλλη, το GNAT box παρέχει και αυτό όλα τα πλεονεκτήματα και υπηρεσίες που περιμένει ένας χρήστης από τέτοιου είδους πακέτα, όπως για παράδειγμα IP Tunneling, κρυπτογράφηση, ειδικά φίλτρα πακέτων κ.ά.

Πέρα από την οικιακή χρήση, υπάρχουν διαθέσιμα στην αγορά επαγγελματικά και υπερ-εξειδικευμένα προγράμματα προστασίας, που αφορούν κυρίως μεγάλα εταιρικά δίκτυα. Κυρίαρχος στο κομμάτι αυτό της αγοράς αποτελεί η CheckPoint, με το προϊόν FireWall-1. Εκτιμάται ότι μία στις τέσσερις εταιρείες ή οργανισμοί χρησιμοποιούν το προϊόν αυτό της CheckPoint. Αξίζει να τονιστεί ότι το FireWall-1 παρέχει πληθώρα επιλογών όπως επίσης και μεγάλη πολυπλοκότητα, γεγονός που το έκανε τόσο δημοφιλές. Χρησιμοποιεί stateful packet filtering, έχει τη δυνατότητα να εργάζεται με πολλαπλά interfaces και μπορεί να εκτελέσει υπηρεσίες Network Address Translation.



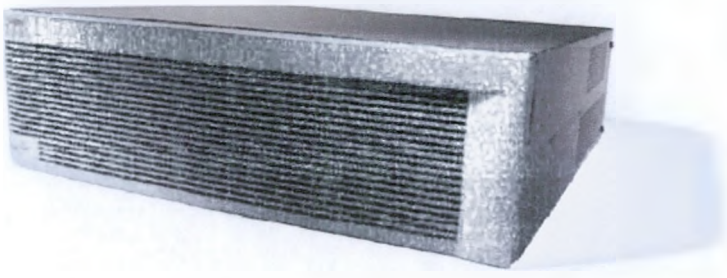
Υλοποίηση firewall με τη χρήση του FireWall-1

Μία ακόμη εφαρμογή που ξεφεύγει από την οικιακή χρήση είναι αυτή του IPFilter, που δημιουργήθηκε από τον Darren Reed. Πρόκειται για μια προσωπική εργασία που εξελίχθηκε σε μια δυναμική και αξιόπιστη εφαρμογή firewall που ανταγωνίζεται ισάξια τα υπόλοιπα εμπορικά πακέτα της κατηγορίας του. Το σημαντικότερο ατού του IPFilter είναι ότι διατίθεται δωρεάν. Έχει τη δυνατότητα να παρέχει stateful επιτήρηση της δικτυακής κίνησης, υποστήριξη πολλαπλών δικτυακών interfaces και υπηρεσίες NAT.

Η Microsoft, μία από τις μεγαλύτερες εταιρείες κατασκευής λογισμικού στον κόσμο, είναι λογικό ότι θα ήθελε να κατακτήσει ένα μερίδιο στην αγορά των firewalls και στην ασφάλεια των υπολογιστών γενικότερα. Έτσι, δημιούργησε το Microsoft ISA Server, που σκοπός του είναι να παρέχει ένα ολοκληρωμένο πακέτο ασφαλείας. Το πακέτο αυτό προσφέρει δυνατότητες firewall, ανίχνευση εισβολέων, Active Directory, κρυπτογράφηση και ικανότητα στην εύρεση της σωστής πολιτικής ασφαλείας. Εξαιτίας του γεγονότος ότι το ISA Server είναι κατασκευασμένο να λειτουργεί σαν το κεντρικό σημείο διασύνδεσης ενός δικτύου με το Internet ή με κάποιο άλλο αναξιόπιστο δίκτυο, οι υπόλοιπες υπηρεσίες που προσφέρει το πακέτο αυτό θα πρέπει να εκτελούνται σε διαφορετικούς διακομιστές, γεγονός που αποτελεί ένα μελανό σημείο στη λύση στο λογισμικό αυτό.

Όσο αφορά hardware λύσεις σε firewalls, όπου η πλειοψηφία των λύσεων που βρίσκεται στην αγορά σήμερα βασίζεται στο packet filtering. Οι πιο δημοφιλείς λύσεις είναι αυτές των Cisco PIX Firewall, SonicWall, το Webramp 1700, το FireBox από την WatchGuard και οι OfficeConect firewall

της 3Com. Τέτοιου είδους firewalls μπορούν να εφαρμοστούν σε δίκτυα οποιουδήποτε μεγέθους. Για παράδειγμα, η 3Com εστιάζεται σε λύσεις για μικρές επιχειρήσεις, ενώ το Cisco PIX μπορεί να υποστηρίξει μέχρι και 250.000 συνδέσεις.



Cisco PIX 535 firewall

Μπορεί κανείς με ασφάλεια να ισχυριστεί ότι για οικιακή χρήση και μικρές εταιρείες οι πιο ενδεδειγμένες λύσεις είναι αυτές των software, λόγω του περιορισμένου κόστους, ενώ οι hardware λύσεις, που τους κόστος τους φαίνεται απαγορευτικό στο περισσότερο καταναλωτικό κοινό, προτείνονται για μεγάλες εταιρείες και οργανισμούς. Αυτό όμως δεν αποκλείει τους απλούς χρήστες που μπορεί να θέλουν να διαφυλάξουν πολύτιμες πληροφορίες στο να προτιμήσουν ακριβές λύσεις, για να διασφαλίσουν το μέγιστο δυνατό αποτέλεσμα.

6.2 ΕΠΙΛΟΓΟΣ

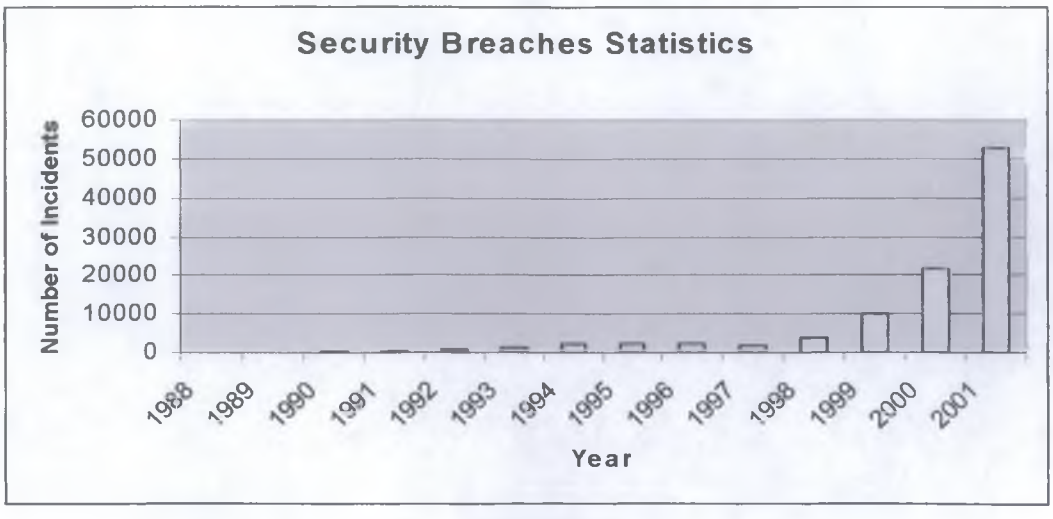
Διανύοντας πλέον τον 21^{ο} αιώνα, η ανθρωπότητα βασίζεται όλο και περισσότερο στην χρήση των υπολογιστικών συστημάτων και των δικτύων. Ο παγκόσμιος ιστός μετατρέπει τον πλανήτη μας σε ένα μεγάλο παγκόσμιο χωριό, όπου οι πολίτες – χρήστες του διαδικτύου ανταλλάσσουν πληροφορίες, επικοινωνούν μεταξύ τους και πραγματοποιούν κάθε είδους οικονομικές συναλλαγές. Αν και οι τεχνολογικές καινοτομίες στον χώρο των επικοινωνιών είναι καταιγιστικές, κάποια δεδομένα δυστυχώς δύσκολα αλλάζουν: μέσα στον μεγάλο αριθμό των ανθρώπων που "κυκλοφορούν" στο διαδίκτυο, πάντα υπάρχουν και κάποιοι που οι προθέσεις τους αποτελούν απειλή για κάποιους άλλους. Το έγκλημα παίρνει πλέον τη μορφή του

ηλεκτρονικού εγκλήματος, που μπορεί να είναι από την ανεπιθύμητη πρόσβαση στην ηλεκτρονική αλληλογραφία μας μέχρι την κλοπή κρατικών μυστικών και οικονομικών εγκλημάτων, όπως η εισβολή στο δίκτυο κάποιας τράπεζας και παράνομη μεταφορά χρημάτων από λογαριασμούς τρίτων.

Η ασφάλεια στα δίκτυα θυμίζει λίγο την περίπτωση "κλέφτες και αστυνόμοι". Όσο και αν εξελίσσονται οι τεχνολογίες firewall, τις περισσότερες φορές θα υπάρχει τρόπος ώστε κάποιος καλά οργανωμένος και "διαβασμένος" hacker, δρώντας ατομικά ή ομαδικά, να διαπεράσει την περίμετρο ενός εσωτερικού δικτύου. Δηλαδή, επικρατεί η "μηδενιστική" άποψη ότι κανένα σύστημα δεν είναι απόλυτα ασφαλές.

Στο σημείο αυτό μπορούμε να παραθέσουμε ένα γράφημα (σχήμα 40), το οποίο δείχνει την αύξηση που παρατηρήθηκε στις επιτυχημένες απόπειρες εισβολής σε ένα δίκτυο, σύμφωνα με τον οργανισμό CERT. Αξίζει να τονισθεί ότι το έτος 2001, ο αριθμός των επιθέσεων αυτών ξεπέρασε τις 50.000. Υπολογίζεται επίσης ότι το ποσοστό των επιτυχημένων αποπειρών εισβολής αγγίζει το 65%. Τα νούμερα αυτά αναμφισβήτητα μπορούν να βάλουν τουλάχιστον σε σοβαρές σκέψεις όλους τους ανθρώπους που χρησιμοποιούν καθημερινά κάθε είδους δίκτυα.

Εν κατακλείδι, μπορούμε να ισχυριστούμε ότι με τις κατάλληλες επιλογές σε αρχιτεκτονικές και τεχνολογίες firewall, μπορούμε να ασφαλίσουμε σε πολύ μεγάλο βαθμό ένα δίκτυο και να καταφέρουμε να μην αποτελέσουμε και εμείς μέρος των παραπάνω στατιστικών. Αν αυτό συνδυαστεί με την έξυπνη και αποτελεσματική χρήση καινούργιων τεχνολογιών που προκύπτουν σχεδόν σε καθημερινή βάση, μειώνουμε πολύ τις πιθανότητες επιτυχημένης επίθεσης στο δίκτυο μας.



Σχήμα 40

ΒΙΒΛΙΟΓΡΑΦΙΑ

- ELIZABETH D. ZWICKY, SIMON COOPER, D. BRENT CHAPMAN, *Building Internet Firewalls*, *Second Edition,* O' Reilly & Associates, Inc., 2000
- CHRIS HARE, KARANJIT SIYAN, *Internet Firewalls And Network Security, Second Edition*, New Riders Publishing, 1996
- ROBERT J. SHIMONSKI, DEBRA LITTLEJOHN SHINDER, DR. THOMAS W. SINDER, *Best Damn Firewall Book Period*, Syngress Publishing, 2003
- http://www.firewallguide.com/
- http://www.cisco.com
- http://www.howstuffworks.com
- http://www.netgear.com
- http://www.microsoft.com
- www.checkpoint.com
- www.cert.org