«Ασφάλεια Δικτύων»

Αζακά Στυλιανή

Ιτζάρης Θεόδωρος

Άρτα, 15 Ιουνίου 2002

Πτυχιακή Εργασία, μέρος των απαιτήσεων
του τμήματος Τηλεπληροφορικής και Διοίκησης

Πίνακας περιεχομένων

Ακρωνύμια

API: Application Programming Interface

BOOTP: Πρωτόκολλο εκκίνησης (bootstrap)

CARP: Cache Array Routing Protocol

CERT: Computer Emergency Response Team

DHCP: Dynamic Host Configuration Protocol

DMZ: Demilitarized Zone Firewall

DNS: Domain Name System

FTP: File Transfer Protocol

GUI: Graphic User Interface

HTML: HyperText Markup Language

ICMP: Internet Control Message Protocol

IP: Internet Protocol

IIS: Internet Information Service

IPX/SPX: Internet Packet Exchange/Sequenced Packet Exchange

IRC: Internet Relay Chat

ISAPI: Internet Service Application Programming Interface

ISDN: Integrated Services Digital Network

ISP: Internet Service Provider

LAN: Local Area Network

LAT: Local Address Table

LDAP: Lightweight Directory Access Protocol

MAC: Media Access Control

NAT: Network Address Translation

NETBEUI: NetBIOS Extended User Interface

NFS: Network File System

NIC: Network Interface Card

NNTP: Network News Transfer Protocol

NOC: Network Operating Center

NTP: Network Time Protocol

POP3: Post Office Protocol V.3

PPP: Point to Point Protocol

PPTP: Point to Point Tunneling Protocol

RAS: Remote Access Service

RAM: Random Access Memory

RLOGIN: Remote Login

SHTTP: Secure HyperText Transport Protocol

SMTP: Simple Mail Transfer Protocol

SQL: Structured Query Language

SSL: Secure Sockets Layer

TCP/IP: Transmission Control Protocol/Internet Protocol

TTL: Time To Live

UDP: User Datagram Protocol

URL: Uniform Resource Locator

VPN: Virtual Private Network

WAN: Wide Area Network

WWW: World Wide Web

ΔΗΛΩΣΗ ΠΕΡΙ ΛΟΓΟΚΛΟΠΗΣ

Όλες οι προτάσεις οι οποίες παρουσιάζονται σ' αυτό το κείμενο και οι οποίες ανήκουν σε άλλους αναγνωρίζονται από τα εισαγωγικά και υπάρχει η σαφής δήλωση του συγγραφέα. Τα υπόλοιπα γραφόμενα είναι επινόηση του γράφοντος ο οποίος φέρει και την καθολική ευθύνη γι' αυτό το κείμενο και δηλώνουμε υπεύθυνα ότι δεν υπάρχει λογοκλοπή γι' αυτό το κείμενο.

Ονοματεπώνυμο: Αζακά Στυλιανή

Υπογραφή……

Ονοματεπώνυμο: Ιτζάρης Θεόδωρος

Υπογραφή……

Ημερομηνία:……

Εισαγωγή

Στα χρόνια πριν από την εξάπλωση της χρήσης των ηλεκτρονικών υπολογιστών ως εργαλεία επεξεργασίας της πληροφορίας, η διασφάλιση της μυστικότητας, ακεραιότητας και διαθεσιμότητας των σημαντικών πληροφοριών ενός οργανισμού γινόταν μέσω της φυσικής προστασίας των, καθώς και μέσω κάποιων διαδικασιών και κανονισμών ασφάλειας. Τα ευαίσθητα έγγραφα κλείνονταν μέσα σε ντουλάπες ή χρηματοκιβώτια στιβαρής κατασκευής τα οποία προστατεύονταν από κλειδαριές, ενώ μόνον εξουσιοδοτημένο προσωπικό είχε πρόσβαση σε αυτά. Τις τελευταίες δεκαετίες, δύο γεγονότα έχουν αλλάξει δραστικά τις ανάγκες των οργανισμών σε σχέση με την ασφάλεια των πληροφοριών.

Το πρώτο γεγονός είναι η εισαγωγή των υπολογιστών ως εργαλεία αποθήκευσης και επεξεργασίας της πληροφορίας. Η προστασία της πληροφορίας ανάγεται πλέον στην προστασία των αρχείων των υπολογιστών στα οποία είναι αποθηκευμένη η πληροφορία, στον έλεγχο της πρόσβασης στα αρχεία αυτά, καθώς και στην προστασία των προγραμμάτων εκείνων που μπορούν να απειλήσουν την ασφάλεια των αρχείων αυτών. Ο όρος που χρησιμοποιείται για να περιγράψει το σύνολο εργαλείων και διαδικασιών που έχουν σχεδιαστεί για την προστασία των ηλεκτρονικών δεδομένων είναι “ασφάλεια υπολογιστών”.

Το δεύτερο γεγονός το οποίο επηρέασε δραστικά τις ανάγκες σε ασφάλεια της πληροφορίας είναι η εισαγωγή των κατανεμημένων συστημάτων και η χρήση των δικτύων και τηλεπικοινωνιακών συστημάτων για την μεταφορά δεδομένων μεταξύ υπολογιστών. Ο όρος “ασφάλεια δικτύων” αναφέρεται στα μέτρα προστασίας των δεδομένων κατά την μεταφορά τους μέσω του δικτύου διασύνδεσης. Στα πλαίσια της διαχείρισης ενός δικτύου, η διαχείριση ασφάλειας αναφέρεται στην παροχή ασφάλειας σε όλα τα στοιχεία του δικτύου, δηλαδή σε ασφάλεια υπολογιστών και ασφάλεια δικτύου.

Μέρος Πρώτο

Ασφάλεια

1 Απειλές κατά της Ασφάλειας

Η ασφάλεια των υπολογιστών και δικτύων καλύπτει τις παρακάτω απαιτήσεις:

- μυστικότητα: απαιτείται η πληροφορία να είναι προσπελάσιμη για ανάγνωση μόνον από εξουσιοδοτημένους χρήστες. Αυτού του είδους η πρόσβαση περιλαμβάνει την εκτύπωση, την προβολή και άλλες φορές ακόμα και την αποκάλυψη ύπαρξης κάποιου είδους πληροφορίας.
- ακεραιότητα: απαιτείται οι πόροι του συστήματος (data, processes κλπ) να μπορούν να τροποποιηθούν μόνον από εξουσιοδοτημένους χρήστες. Η τροποποίηση περιλαμβάνει την εγγραφή, τροποποίηση, αλλαγή κατάστασης, διαγραφή και δημιουργία.
- Διαθεσιμότητα: απαιτείται οι πόροι του συστήματος να είναι διαθέσιμοι στους εξουσιοδοτημένους χρήστες.

1.1 Μορφές απειλών

Οι απειλές κατά των κινούμενων δεδομένων αφορούν στην ακεραιότητα, μυστικότητα και διαθεσιμότητα των δεδομένων και μπορούν να χωρισθούν σε δύο κατηγορίες:

A. **Απειλές παθητικής φύσης.** Απειλούν την μυστικότητα των δεδομένων (π.χ. μέσω ειδικών προγραμμάτων packet sniffers) με σκοπό την απόκτηση των πληροφοριών. Για παράδειγμα ο χρήστης ενός Η/Υ μπορεί να χρησιμοποιήσει ένα τέτοιο πρόγραμμα για να παρακολουθεί όλα τα πακέτα που εκπέμπονται στο τοπικό δίκτυο. Τέτοιου είδους ενέργειες είναι πολύ δύσκολο να αποκαλυφθούν διότι δεν προκαλούν αλλαγή στα δεδομένα και δεν επηρεάζουν την λειτουργία του δικτύου. Η παρακολούθηση των δεδομένων είναι δυνατή και μέσω παρακολούθησης των καλωδιώσεων χαλκού του δικτύου ή των τηλεφωνικών συνδέσεων πρόσβασης στο δίκτυο.

B. **Απειλές ενεργητικής φύσης.** Τέτοιου είδους απειλές έχουν σαν στόχο την τροποποίηση των κινούμενων δεδομένων. Είναι δυνατή μια περαιτέρω κατηγοριοποίηση τέτοιων απειλών ως εξής:

1. πρόκληση τροποποίησης της ροής των πακέτων δεδομένων (message-stream modification), όπου ένα τμήμα του μηνύματος τροποποιείται ή κάποια καθυστερούν, επαναλαμβάνονται ή τροποποιείται η διαδοχή τους για να προκληθεί κάποιο αποτέλεσμα
2. πρόκληση άρνησης παροχής υπηρεσιών (denial of service), κατά την οποία παρεμποδίζεται η κανονική χρήση των πόρων του δικτύου. Μία τέτοια μορφή επίθεσης είναι η υπερφόρτωση του δικτύου με πακέτα με αποτέλεσμα την επιβράδυνση ή και διακοπή της λειτουργίας του. Άλλο παράδειγμα είναι η εξάλειψη μηνυμάτων που απευθύνονται σε κάποιο συγκεκριμένο αποδέκτη, όπως για παράδειγμα σε ένα πρόγραμμα που εκτελεί την υπηρεσία ελέγχου ασφάλειας (security audit service).
3. μεταμφίεση (masquerade) κατά την οποία ο εισβολέας τροποποιεί τα δεδομένα με στόχο να ξεγελάσει τους μηχανισμούς ασφάλειας του δικτύου και να θεωρηθεί ως εξουσιοδοτημένος ή έμπιστος χρήστης. Τέτοια παραδείγματα είναι η αλλαγή της IP διεύθυνσης πακέτων του εξωτερικού εισβολέα έτσι ώστε το σύστημα firewall να νομίσει ότι τα πακέτα έρχονται από το εσωτερικό δίκτυο (IP Spoofing), ή η ηχογράφηση κάποιας συνομιλίας ελέγχου αυθεντικότητας (authentication) μεταξύ ενός εξουσιοδοτημένου χρήστη και του συστήματος και κατόπιν η χρήση της από τον εισβολέα.

1.2 Τρόποι προστασίας της δικτυακής μας τοποθεσίας

Οι άνθρωποι επιλέγουν ποικίλα πρότυπα ασφάλειας, ή προσεγγίσεις, που κυμαίνονται από καθόλου ασφάλεια , μέσω αυτού που καλείται «ασφάλεια

μέσω της ασημότητας- αφάνειας» και την ασφάλεια των host, στην ασφάλεια δικτύων.

❖ *Καμία Ασφάλεια*

Η απλούστερη πιθανή προσέγγιση είναι να μην τεθεί καμία προσπάθεια στην ασφάλεια, και να τρέξει με ο,τιδήποτε ελάχιστη ασφάλεια ο προμηθευτής σας σας παρέχει εξ ορισμού.

❖ *Ασφάλεια μέσω της ασημότητας- αφάνειας*

Ένα άλλο πιθανό πρότυπο ασφάλειας είναι αυτό καλούμενο συνήθως «η ασφάλεια μέσω της ασημότητας- αφάνειας.» Με αυτό το πρότυπο, ένα σύστημα θεωρείται ασφαλές απλά επειδή (υποθετικά) κανένας δεν ξέρει για την ύπαρξή του, το περιεχόμενο, τα μέτρα ασφάλειας, ή τίποτ' άλλο. Αυτή η προσέγγιση λειτουργεί σπάνια για πολύ γιατί υπάρχουν πάρα πολλοί τρόποι να βρεθεί ένας ελκυστικός στόχος.

Πολλοί άνθρωποι υποθέτουν ότι ακόμα κι αν οι επιτιθέμενοι μπορούν να τους βρουν, δεν θα ενοχλήσουν. Λογαριάζουν ότι μια μικρή επιχείρηση ή ένας ιδιωτικός υπολογιστής δεν πρόκειται να είναι ελκυστικός στόχος στους εισβολείς. Στην πραγματικότητα, πολλοί εισβολείς δεν στοχεύουν στους ιδιαίτερους στόχους, θέλουν ακριβώς να σπάσουν σε όσο το δυνατόν περισσότερους Η/Υ. Σε αυτούς, οι μικρές επιχειρήσεις και οι ιδιωτικοί υπολογιστές μοιάζουν απλά με εύκολους στόχους. Πιθανώς δεν θα μείνουν για πολύ, αλλά θα προσπαθήσουν να μπουν μέσα, και μπορούν να κάνουν ιδιαίτερη ζημιά προσπαθώντας να καλύψουν τα ίχνη τους.

Για να λειτουργήσει σε οποιοδήποτε δίκτυο, συμπεριλαμβανομένου το Διαδίκτυο, ένα site πρέπει να κάνει τουλάχιστον μια ελάχιστη εγγραφή και ένα μεγάλο μέρος αυτών των πληροφοριών εγγραφής είναι διαθέσιμο στον καθέναν. Κάθε φορά που ένα site χρησιμοποιεί τις υπηρεσίες του δικτύου, κάποιος – τουλάχιστον όποιος παρέχει την υπηρεσία – ξέρει ότι είναι εκεί. Οι εισβολείς

προσέχουν για τις νέες συνδέσεις, με την ελπίδα ότι στα site αυτά δεν θα έχουν ακόμα τα μέτρα ασφάλειας σε ισχύ.

Είναι εκπληκτικό το πόσοι τρόποι υπάρχουν για να ανακαλύψει κανείς τις ευαίσθητες από άποψη ασφάλειας πληροφορίες του site μας. Παραδείγματος χάριν, η γνώση του ποιου υλικού και λογισμικού έχετε και ποια έκδοση του λειτουργικού συστήματος χρησιμοποιείτε δίνει στους εισβολείς σημαντικές ενδείξεις για ποιες τρύπες ασφάλειας να προσπαθήσουν. Μπορούν συχνά να πάρουν αυτές τις πληροφορίες από την εγγραφή(registration) των host, ή με την προσπάθεια να συνδεθούν με τον υπολογιστή σας. Πολλοί υπολογιστές αποκαλύπτουν τον τύπο λειτουργικού συστήματός τους στο χαιρετισμό που παίρνετε κατά την διαδικασία του login, έτσι ένας εισβολέας δεν χρειάζεται την πρόσβαση για να αποκτήσει τέτοιου είδους πληροφορίες.

Οι εισβολείς έχουν πολύ χρόνο στη διάθεση τους και μπορούν συχνά να αποφύγουν να πρέπει να υπολογίσουν τα σκοτεινά γεγονότα με απλά να δοκιμάσουν όλες τις δυνατότητες. Μακροπρόθεσμα, δεν είναι μια έξυπνη επιλογή μεθόδου ασφάλειας η ασφάλεια μέσω της ασημότητας- αφάνειας.

❖ *Ασφάλεια των host*

Πιθανώς το πιο κοινό πρότυπο για την ασφάλεια υπολογιστών είναι η ασφάλεια των host. Με αυτό το πρότυπο, επιβάλλετε την ασφάλεια σε κάθε host χωριστά, και καταβάλλετε κάθε προσπάθεια να αποφύγετε όλα τα γνωστά προβλήματα ασφάλειας που έχουν επιπτώσεις σε εκείνο τον ιδιαίτερο host. Πού είναι το πρόβλημα με την ασφάλεια των host; Δεν είναι ότι δεν λειτουργεί στις μεμονωμένες μηχανές, αλλά ότι δεν βολεύει για μεγάλους αριθμούς μηχανών.

Το σημαντικότερο εμπόδιο στην αποτελεσματική ασφάλεια των host στα σύγχρονα υπολογιστικά περιβάλλοντα είναι η πολυπλοκότητα και η ποικιλομορφία εκείνων των περιβαλλόντων. Τα περισσότερα σύγχρονα περιβάλλοντα περιλαμβάνουν μηχανές από τους πολλούς και διάφορους προμηθευτές, κάθε ένας με το λειτουργικό σύστημά του, και κάθε ένας με το σύνολό του προβλημάτων ασφάλειας. Ακόμα κι αν το site έχει μηχανές από μόνο έναν προμηθευτή, οι διαφορετικές εκδόσεις του ίδιου λειτουργικού συστήματος έχουν συχνά σημαντικά διαφορετικά προβλήματα ασφάλειας. Ακόμα κι αν όλες αυτές οι μηχανές είναι από

έναν ενιαίο προμηθευτή και τρέχουν μια την ίδια έκδοση του λειτουργικού συστήματος, οι διαφορετικές διαμορφώσεις (διαφορετικές υπηρεσίες που χρησιμοποιεί ή τρέχει το καθένα, και τα λοιπά) μπορούν να φέρουν τα διαφορετικά υποσυστήματα στο παιχνίδι (και στη σύγκρουση) και οδηγούν στα διαφορετικά σύνολα προβλημάτων ασφάλειας. Και, ακόμα κι αν οι μηχανές είναι όλες απολύτως ίδιες, ο μεγάλος αριθμός τους επί μερικών site μπορεί να κάνει την ασφάλισή τους κάτι αρκετά δύσκολο. Απαιτείται ένα σημαντικό ποσό δύσκολης και συνεχούς εργασίας για να εφαρμοστεί αποτελεσματικά και να διατηρηθεί η ασφάλεια των host. Ακόμη και με όλη αυτήν την εργασία να γίνεται σωστά, η ασφάλεια των host συχνά αποτυγχάνει λόγω των bugs στο λογισμικό, ή λόγω έλλειψης αρκετά ασφαλούς λογισμικού για ορισμένες απαιτούμενες λειτουργίες.

Η ασφάλεια των host στηρίζεται επίσης στις καλές προθέσεις και την ικανότητα του καθενός που έχει προνόμια στην πρόσβαση σε οποιαδήποτε μηχανή. Δεδομένου ότι ο αριθμός μηχανών αυξάνεται, ο αριθμός προνομιούχων χρηστών αυξάνεται γενικά επίσης. Η ασφάλιση μιας μηχανής είναι δυσκολότερη από ότι να την συνδέσεις σε ένα δίκτυο. Η σύνδεση μιας μηχανής χωρίς τις κατάλληλες ασφαλίσεις μπορεί να επιφέρει απρόσμενες εκπλήξεις στο δίκτυο.

Ένα πρότυπο ασφάλειας των host μπορεί να είναι ιδιαίτερα κατάλληλο για μικρά site ή για site με ακραίες απαιτήσεις ασφάλειας. Πράγματι, όλες τα site πρέπει να συμπεριλάβουν κάποιο επίπεδο ασφάλειας host στα γενικά σχέδια ασφάλειάς τους. Ακόμα κι αν υιοθετείτε ένα πρότυπο ασφάλειας δικτύων, όπως περιγράφουμε στο επόμενο τμήμα, ορισμένα συστήματα στη διαμόρφωσή σας θα ωφεληθούν από την δυναμική της ασφάλειας των host. Παραδείγματος χάριν, ακόμα κι αν έχετε ένα firewall γύρω από το εσωτερικό δίκτυο και τα συστήματά σας, θα υπάρξουν ορισμένα συστήματα που θα είναι εκτεθειμένα στον εξωτερικό κόσμο τα οποία και απαιτούν ασφάλεια των host. Το πρόβλημα είναι ότι το πρότυπο ασφάλειας των host δεν είναι ακριβώς μια φτηνή λύση παρά μόνο για μικρά ή πολύ απλά site. Το να δουλέψει απαιτεί υπερβολικά πολλούς περιορισμούς και ανθρώπους .

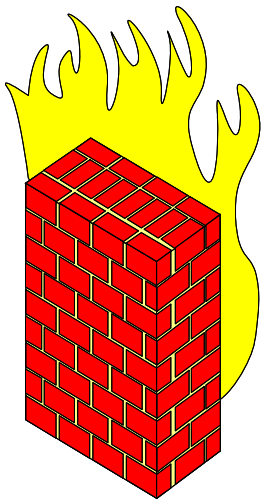
❖ *Ασφάλεια Δικτύων*

Καθώς τα υπολογιστικά περιβάλλοντα μεγαλώνουν και αλλάζουν και καθώς η δυσκολία της ασφάλειας σε μια host-προς-host βάση μεγαλώνει όλο και πιο πολλά

site στρέφονται σ' ένα μοντέλο ασφάλειας δικτύων. Με ένα πρότυπο ασφάλειας δικτύων, επικεντρώνεστε στο να ελέγχετε τη δικτυακή πρόσβαση στους διάφορους host σας και τις υπηρεσίες που αυτοί προσφέρουν, παρά στο να ασφαλιστούν ένας-ένας. Οι προσεγγίσεις ασφάλειας δικτύων περιλαμβάνουν το χτίσιμο αντιπυρικών ζωνών για να προστατεύσουν τα εσωτερικά συστήματα και δίκτυά σας, χρησιμοποιώντας προσεγγίσεις πιστοποίησης (όπως οι κωδικοί πρόσβασης "μιας χρήσεως"), και κρυπτογράφηση για την προστασία των ιδιαίτερα ευαίσθητων δεδομένων καθώς διέρχονται το δίκτυο.

Ένα site μπορεί να αποκτήσει τεράστια δύναμη και ευελιξία από τις προσπάθειες ασφάλειάς της με τη χρησιμοποίηση ενός προτύπου ασφάλειας δικτύων. Παραδείγματος χάριν, ένα firewall δικτύου μπορεί να προστατεύσει εκατοντάδες, χιλιάδες, ή ακόμα και δεκάδες χιλιάδες μηχανές από την επίθεση από τα δίκτυα πέρα από το firewall, ανεξάρτητα από το επίπεδο ασφάλειας των host των μεμονωμένων μηχανών.

Μέρος Δεύτερο



FIREWALLS

2 Firewalls

2.1 Τι είναι το firewall;

Το firewall είναι μια διάταξη εξειδικευμένων μηχανισμών ασφαλείας που ελέγχει την πρόσβαση και την μετακίνηση πληροφορίας μεταξύ ενός αξιόπιστου και ενός μη αξιόπιστου δικτύου. Δεν είναι απλώς ένα συστατικό λογισμικού ή υλικού αλλά μια ενιαία στρατηγική προφύλαξης πόρων.

Το firewall υλοποιεί και ενδυναμώνει μια πολιτική ασφαλείας. Χωρίς την ανάλογη πολιτική καθίσταται άσκοπο. Αφορά στο σύνολο του λογισμικού και των διαδικασιών που χρησιμοποιούνται για την υλοποίηση της πολιτικής ασφαλείας μέσω της διαχείρισης της εισερχόμενης και εξερχόμενης κίνησης από το εσωτερικό δίκτυο. Αποτελεί την πρώτη γραμμή άμυνας, αλλά οπωσδήποτε ποτέ την μόνη, έναντι οποιασδήποτε παράνομης κίνησης.

Η κύρια λειτουργία του είναι ο κεντρικός έλεγχος των σημείων πρόσβασης στο εσωτερικό μας δίκτυο. Το κρίσιμο θέμα είναι εάν μπορούν βέβαια να προσδιοριστούν όλα τα σημεία εισόδου και να προστατευθούν ανάλογα. Ακόμα και εάν έχει ληφθεί μέριμνα για τα παραπάνω, εφόσον εξωτερικοί χρήστες αποκτήσουν πρόσβαση στο εσωτερικό δίκτυο, χωρίς να περάσουν μέσω του firewall, η αποτελεσματικότητά του εκμηδενίζεται. Αυτό θα μπορούσε να συμβεί, για παράδειγμα, εάν ο υπάλληλος ενός οργανισμού επέλεγε να συνδεθεί με το internet μέσω ενός modem που βρίσκεται στο γραφείο του. Σε μια τέτοια περίπτωση δημιουργεί μια ανασφαλή σύνδεση, παρακάμπτοντας το firewall και εκθέτοντας το εσωτερικό δίκτυο στους επίδοξους εισβολείς.

Όπως και με κάθε μέτρο ασφαλείας, υπάρχουν συμβιβασμοί που πρέπει να γίνουν μεταξύ επιπέδων ασφάλειας και άνεσης. Το firewall θα πρέπει

να είναι διαφανές προς τους χρήστες, ενώ αντίθετα θα είναι ένα ορατό εμπόδιο για τους εξωτερικούς χρήστες.

2.2 Τα οφέλη και οι περιορισμοί των firewall

Τα firewall παρέχουν ορισμένους τύπους προστασίας:

- Μπορούν να μπλοκάρουν μη επιθυμητή κίνηση.
- Μπορούν να κατευθύνουν εσωτερική κίνηση σε πιο αξιόπιστα εσωτερικά συστήματα.
- Μπορούν να αποκρύψουν ευαίσθητα ή ευπρόσβλητα συστήματα, τα οποία δεν είναι εύκολο να αποκοπούν και να προστατευθούν από το Διαδίκτυο .
- Μπορούν να παρακολουθούν και να καταγράφουν την κίνηση από και προς το εσωτερικό δίκτυο.
- Μπορούν να αποκρύψουν ονόματα συστημάτων, τοπολογίες δικτύων, τύπους συσκευών δικτύων, τοπολογίες δικτύων, τύπους συσκευών δικτύων και ταυτότητες εσωτερικών χρηστών.
- Μπορούν να προσφέρουν καλύτερο και πιο αξιόπιστο έλεγχο ταυτότητας από ότι άλλες εφαρμογές.
- Δεν παρέχουν επαρκή προστασία όσον αφορά τους ιούς.

Το firewall είναι μια προσέγγιση στην ασφάλεια του εσωτερικού δικτύου. Συνεισφέρει στην υλοποίηση μιας πολιτικής ασφάλειας που ορίζει υπηρεσίες και επιτρεπόμενη πρόσβαση. Γενικά υλοποιούνται δύο κύριες σχεδιαστικές πολιτικές: η στάση ”default deny” και η στάση “default permit”. Η πρώτη απαγορεύει κάθε υπηρεσία εκτός και αν έχει επιτραπεί ρητά, ενώ η δεύτερη επιτρέπει κάθε υπηρεσία εκτός και αν έχει απαγορευτεί ρητά.

Η δεύτερη πολιτική διευκολύνει περισσότερο τους επίδοξους εισβολείς. Ο οργανισμός μπορεί να τοποθετήσει τον κεντρικό υπολογιστή που θα τρέχει έναν Web server έξω από το firewall , ενώ όταν ο web server θα πρέπει να επικοινωνήσει με βάσεις δεδομένων εντός του εσωτερικού δικτύου, η σύνδεση θα προστατεύεται από ένα firewall, υλοποιώντας έτσι μια αρχιτεκτονική ελεγχόμενων υποδικτύων (screened subnets).

Τα firewall που βασίζονται σε δρομολογητές δεν προσφέρουν έλεγχο ταυτότητας του χρήστη, ενώ αυτά που βασίζονται σε κεντρικό υπολογιστή υποστηρίζουν τα συνήθη password, password μιας χρήσης τα οποία αλλάζουν σε κάθε σύνδεση και ψηφιακά πιστοποιητικά. Η πολιτική θα πρέπει να ορίζει σαφώς εάν επιτρέπεται να κάνει και δρομολόγηση πακέτων ή απλώς θα τα προωθεί. Οι δρομολογητές που φιλτράρουν τα πακέτα (ενεργώντας ως firewall) κάνουν δρομολόγηση πακέτων. Αντίθετα οι *proxy server* δεν συνίσταται να κάνουν δρομολόγηση πακέτων, γιατί υπάρχει ο κίνδυνος να παρακαμφθούν οι έλεγχοι ασφάλειας. Επίσης, η δρομολόγηση πηγής (source routing) δεν πρέπει να επιτρέπεται και τα πακέτα να απορρίπτονται από το δρομολογητή. Εάν λειτουργεί και ως DNS Server, τότε οι εξωτερικοί υπολογιστές δεν γνωρίζουν τίποτα για το εσωτερικό δίκτυο. Μπορεί να χρησιμοποιηθεί για την προστασία υποτμημάτων ενός εσωτερικού δικτύου αλλά και για τη σύνδεση με ένα άλλο firewall, δημιουργώντας ένα ιδεατό δίκτυο (VPN). Τα περισσότερα προϊόντα πλέον υποστηρίζουν και αυτήν την δυνατότητα.

Προκειμένου ένας οργανισμός να υλοποιήσει ένα σύστημα firewall, συνίσταται η ασφαλής οδός: άρνηση κάθε υπηρεσίας εκτός αυτών που έχουν σαφώς οριστεί (default deny stance). Ο σχεδιαστής θα πρέπει να προσδιορίσει τα εξής:

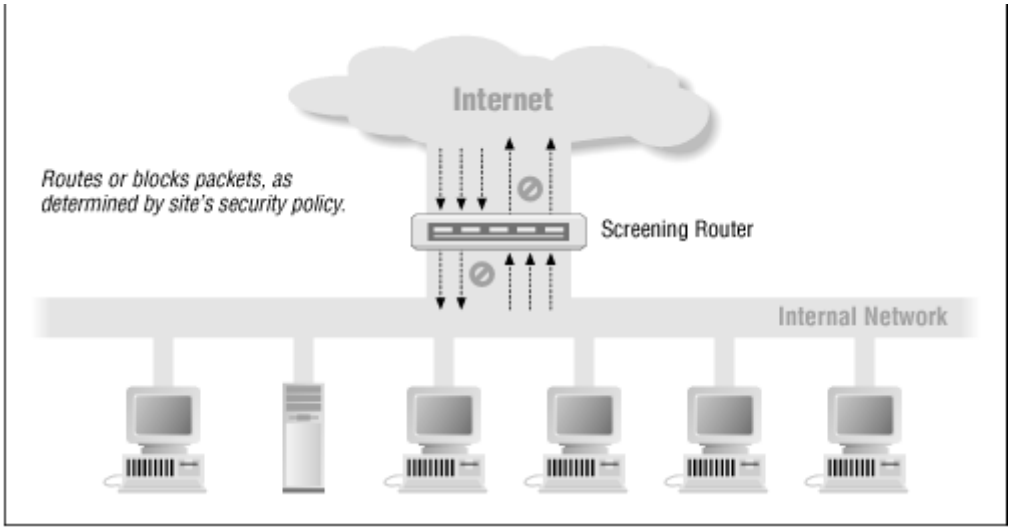
- Διαδικτυακές υπηρεσίες που χρειάζεται ο οργανισμός (telnet, http, smtp e-mail κλπ.)
- Τρόπους χρήσης των υπηρεσιών (τοπικά, από το σπίτι, από οποιοδήποτε σημείο του Internet κλπ.)
- Υποστήριξη πρόσθετων αναγκών όπως κρυπτογράφηση και dial-in.
- Κίνδυνοι που μπορούν να προέλθουν από την παροχή των συγκεκριμένων υπηρεσιών και επιπέδων πρόσβασης.
- Κόστος παροχής προστασίας σε επίπεδο ελέγχου και επίδρασης στους πόρους του δικτύου.
- Προτεραιότητα της ασφάλειας έναντι της χρήσης των πόρων και υπηρεσιών του δικτύου.

2.3 Σχεδιασμός των Firewall

Θα δώσουμε ορισμένους ορισμούς που αφορούν τα firewalls και την ασφάλεια δικτύων:

- *Firewall* – Μια συνιστώσα ή ένα σύνολο συνιστωσών που περιορίζει την πρόσβαση μεταξύ ενός προστατευμένου δικτύου και του Διαδικτύου ή μεταξύ κάποιων άλλων δικτύων.
- *Host* - Ένα υπολογιστικό σύστημα συνδεδεμένο σ' ένα δίκτυο.
- *Bastion host* - Ένα υπολογιστικό σύστημα που πρέπει να ασφαλιστεί ιδιαίτερα επειδή είναι τρωτό στις επιθέσεις, συνήθως επειδή εκτίθεται στο Internet και είναι ένα κύριο σημείο της επαφής για τους χρήστες των εσωτερικών δικτύων.
- *Dual homed host* – Ένα γενικής- χρήσεως υπολογιστικό σύστημα που έχει τουλάχιστον δύο κάρτες δικτύου.
- *Packet* – Η θεμελιώδης μονάδα επικοινωνίας στο Internet.
- *Packet Filtering* - Φιλτράρισμα πακέτων. Η δράση που αναλαμβάνει μια συσκευή για να ελέγξει επιλεκτικά τη ροή των δεδομένων από και προς ένα δίκτυο. Τα φίλτρα πακέτων επιτρέπουν ή αποτρέπουν τα πακέτα, συνήθως δρομολογώντας τα από το ένα δίκτυο στο άλλο (συχνότερα από το Διαδίκτυο σε ένα εσωτερικό δίκτυο, και αντίστροφα). Για να πραγματοποιήσετε το φιλτράρισμα πακέτων, οργανώνετε ένα σύνολο κανόνων που διευκρινίζουν ποιους τύπους πακέτων (π.χ., αυτά που προέρχονται από ή κατευθύνονται προς μια συγκεκριμένη διεύθυνση IP ή port) θα επιτρέψουμε και ποιους θα απορρίψουμε. Το φιλτράρισμα πακέτων μπορεί να εμφανιστεί σε έναν δρομολογητή, σε μια γέφυρα, ή σε έναν μεμονωμένο host. Είναι μερικές φορές γνωστό και ως *screening*.
- *Perimeter Network* – Περιμετρικό Δίκτυο. Ένα δίκτυο που προστίθεται μεταξύ ενός προστατευμένου δικτύου και ενός εξωτερικού δικτύου, ώστε να προστεθεί ένα επιπλέον στρώμα ασφάλειας. Πολλές φορές αναφέρεται και ως DMZ (από το "***D***e-***M***ilitarized ***Z***one)
- *Proxy Server* – Διακομιστής Διαμεσολάβησης. Ένα πρόγραμμα που διαπραγματεύεται με εξωτερικούς διακομιστές εκ μέρους εσωτερικών πελατών. Οι πελάτες-proxy μιλούν στον proxy server, ο οποίος αναμεταδίδει τις αιτήσεις των πελατών στους πραγματικούς διακομιστές, οι οποίοι με τη σειρά τους απαντούν στον proxy server. Τέλος, αυτός αναμεταδίδει τις απαντήσεις στον πελάτη του δικτύου.

2.4 Φιλτράρισμα πακέτων



Φιλτράρισμα Πακέτων 2.4.1

Τα συστήματα φιλτραρίσματος πακέτων δρομολογούν πακέτα μεταξύ εσωτερικών και εξωτερικών host, αλλά το κάνουν επιλεκτικά. Επιτρέπουν ή αποτρέπουν την προσπέλαση ορισμένων ειδών πακέτα με τρόπο που αντανακλά την πολιτική ασφάλειας του site μας (Εικόνα 2.4.1). Ο δρομολογητής ο οποίος χρησιμοποιείται από τα firewall φιλτραρίσματος πακέτων ονομάζεται *screening router.*

Κάθε πακέτο έχει ένα σύνολο από "κεφαλίδες" (headers), που περιέχουν συγκεκριμένες σημαντικές πληροφορίες, κάποιες από τις οποίες είναι: IP διεύθυνσης πηγής, IP διεύθυνσης προορισμού, το πρωτόκολλο (TCP,UDP ή ICMP), το TCP ή UDP port πηγής και προορισμού καθώς και τον τύπο του ICMP μηνύματος. Επιπρόσθετα ο δρομολογητής γνωρίζει κάποια πράγματα για τα πακέτα που εισέρχονται ή εξέρχονται από αυτόν τα οποία δεν αναφέρονται στις πληροφορίες των κεφαλίδων όπως για παράδειγμα το interface(η διεπαφή) απ' το οποίο μπήκε το πακέτο ή αυτό απ' το οποίο θα βγει.

Το γεγονός ότι χρησιμοποιούνται συγκεκριμένοι αριθμοί port στους server των υπηρεσιών Internet δίνει στον δρομολογητή τη δυνατότητα να επιτρέπει ή να αποτρέπει συγκεκριμένα είδη συνδέσεων απλά προσδιορίζοντας το κατάλληλο port (π.χ. TCP port 23 για συνδέσεις Telnet) στους κανόνες προσδιορισμού του φίλτρου πακέτων.

Εδώ παρουσιάζονται κάποια παραδείγματα με τον οποίο θα μπορούσαμε να προγραμματίσουμε έναν screening router ώστε να δρομολογεί τα πακέτα επιλεκτικά από ή προς το site μας:

- Μπλοκάρισμα όλων των εισερχόμενων συνδέσεων από συστήματα έξω από το δίκτυο μας, εκτός από τις εισερχόμενες SMTP συνδέσεις ώστε να λαμβάνουμε αλληλογραφία.
- Μπλοκάρισμα των συνδέσεων σε ή από μη-έμπιστα συστήματα.
- Αποδοχή υπηρεσιών αλληλογραφίας και FTP, αλλά μπλοκάρισμα επικίνδυνων υπηρεσιών όπως TFTP, του συστήματος X Window, των υπηρεσιών "*r"* (rlogin, rsh, rcp κτλ)

Για να γίνει πιο σαφής και κατανοητή η διαδικασία του φιλτραρίσματος πακέτων θα εξηγήσουμε τη διαφορά μεταξύ ενός συνηθισμένου router και ενός screening router.

Ένας συνηθισμένος δρομολογητής απλά ελέγχει τη διεύθυνση προορισμού του πακέτου και επιλέγει τον καλύτερο τρόπο που γνωρίζει ώστε να κατευθύνει το πακέτο προς τον προορισμό του. Η απόφαση που εκλαμβάνεται για τη μοίρα του πακέτου βασίζεται αποκλειστικά από τον προορισμό του. Υπάρχουν δύο εκδοχές που αφορούν τη μοίρα του πακέτου: είτε γνωρίζει ο δρομολογητής πώς να το στείλει προς τον προορισμό του και το πράττει, είτε δε γνωρίζει και το επιστρέφει από όπου ήρθε στέλνοντας και ένα ICMP μήνυμα "destination unreachable".

Από την άλλη ο screening router ρίχνει μια πιο προσεκτική ματιά στα πακέτα. Επιπρόσθετα, προσδιορίζοντας αν μπορεί ή όχι να δρομολογήσει το πακέτο προς τον προορισμό του, ένας screening router αποφαίνεται στο αν πρέπει ή όχι να το δρομολογήσει. Το αν πρέπει ή όχι προσδιορίζεται από την πολιτική ασφάλειας του site μας η οποία του έχει επιβληθεί.

Παρόλο που είναι δυνατό να βρίσκεται ένας screening router μεταξύ του Internet και του εσωτερικού μας δικτύου (Εικόνα 2.4.1) αυτό εναποθέτει τεράστια

ευθύνη σ' αυτόν. Όχι μόνο πρέπει να εκπληρώσει όλες τις διαδικασίες δρομολόγησης και λήψης αποφάσεων για τις δρομολογήσεις, αλλά είναι και το μόνο σύστημα ασφάλειας. Εάν η ασφάλειά του αποτύχει ή καταρρεύσει από μια επίθεση το εσωτερικό δίκτυο μένει εκτεθειμένο. Επιπρόσθετα, ένας γνήσιος screening router δεν μπορεί να τροποποιεί υπηρεσίες. Μπορεί να επιτρέψει ή όχι μια υπηρεσία , αλλά δεν μπορεί να προστατεύσει μεμονωμένες λειτουργίες μιας υπηρεσίας. Αν μια επιθυμητή υπηρεσία έχει κάποιες μη ασφαλής λειτουργίες ή αν η υπηρεσία συνήθως παρέχεται με έναν ανασφαλή server, το φιλτράρισμα πακέτων από μόνο του δε μπορεί να παρέχει την επιθυμητή ασφάλεια.

2.5 Υπηρεσίες Proxy

Οι υπηρεσίες *proxy* είναι εξειδικευμένες εφαρμογές ή προγράμματα διακομιστή τα οποία "τρέχουν" στο firewall το οποίο είναι είτε ένας *dual-homed host* με τη μία διεπαφή στο εσωτερικό δίκτυο και την άλλη στο εξωτερικό είτε ένας *bastion host* ο οποίος είναι προσπελάσιμος από τις εσωτερικές μηχανές του δικτύου και έχει πρόσβαση στο Διαδίκτυο. Αυτά τα προγράμματα υποκλέπτουν τις αιτήσεις των χρηστών για υπηρεσίες του Διαδίκτυου και τις προωθούν, καθώς αρμόζει σύμφωνα με την πολιτική ασφάλειας, προς τις πραγματικές υπηρεσίες. Τα proxy παρέχουν συνδέσεις αντικατάστασης και ενεργούν ως πύλες προς τις υπηρεσίες. Γι' αυτό το λόγο τα proxy είναι και γνωστά ως *πύλες επιπέδου εφαρμογής* (*application-level gateways).*

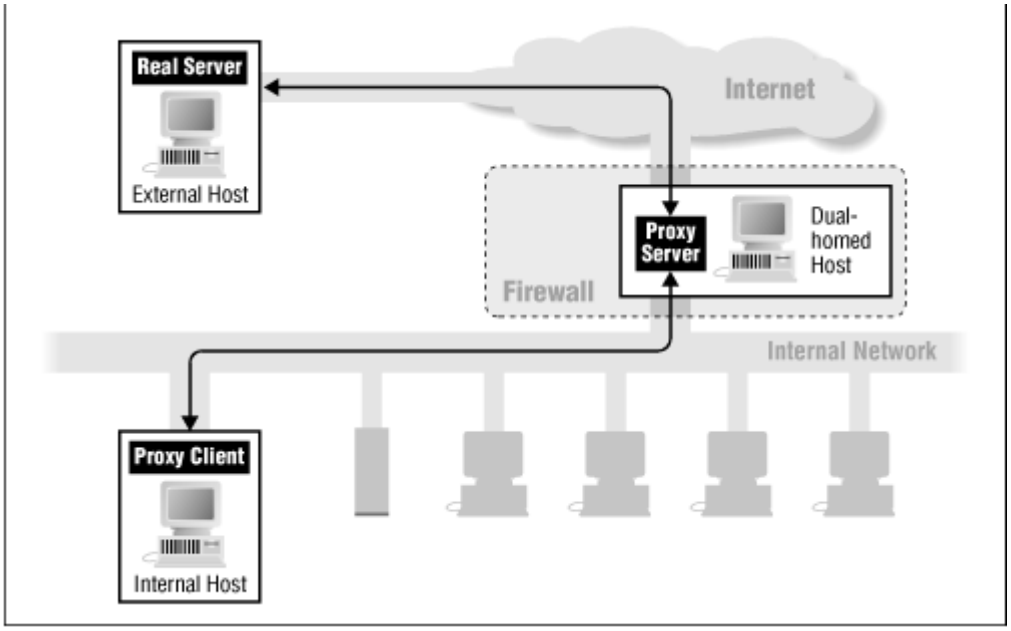
Οι υπηρεσίες proxy, άλλοτε αντιληπτές και άλλοτε όχι (transparent), βρίσκονται ανάμεσα στο χρήστη του εσωτερικού δικτύου και μιας υπηρεσίας έξω από αυτό (Διαδίκτυο). Αντί να μιλάνε κατ' ευθείαν ο ένας στον άλλον, μιλά ο καθένας σ 'έναν proxy. Οι proxy χειρίζονται όλες τις επικοινωνίες μεταξύ των εσωτερικών χρηστών και των υπηρεσιών του Διαδικτύου στο παρασκήνιο.

Η *διαφάνεια (transparency)* είναι το βασικό πλεονέκτημα των υπηρεσιών proxy. Στον πραγματικό server, ο proxy δίνει την ψευδαίσθηση ότι έχει να κάνει μ' έναν χρήστη απ' ευθείας στον proxy host. Στον πραγματικό χρήστη, ο proxy δίνει την ψευδαίσθηση ότι μιλά απ 'ευθείας με τον πραγματικό server.

Οι υπηρεσίες proxy μπορούμε να πούμε ότι είναι αποτελεσματικές όταν χρησιμοποιούνται σε συνάφεια με κάποιο μηχανισμό ο οποίος αποτρέπει την άμεση επικοινωνία μεταξύ των εσωτερικών και εξωτερικών host. Οι dual-homed hosts και τα φίλτρα πακέτων είναι τέτοιοι μηχανισμοί. Εάν υπάρχει επικοινωνία άμεση του εσωτερικού με το εξωτερικό περιβάλλον, εξουδετερώνεται η ανάγκη χρήσης του proxy, οπότε και δε θα χρησιμοποιούν. Μία τέτοια παρακαμπτήρια οδός πιθανώς δεν είναι σύμφωνη με την πολιτική ασφάλειας του site μας.

2.5.1 Υπηρεσίες Proxy σε ένα *Dual-homed Host.*

Δύο είναι οι συνιστώσες μιας υπηρεσίας proxy: ο proxy server και ο proxy client. Στην περίπτωσή μας ο server βρίσκεται στον Dual-homed host. Ο πελάτης είναι μια ειδική έκδοση ενός συνηθισμένου προγράμματος πελάτη (όπως είναι τα FTP,telnet κλπ.) που μιλά στον proxy server αντί για τον πραγματικό server. Επιπρόσθετα, αν στους χρήστες έχουν δοθεί συγκεκριμένες οδηγίες, τα συνηθισμένα προγράμματα πελάτη μπορούν να χρησιμοποιηθούν ως proxy πελάτες. Ο proxy server εκτιμά τις αιτήσεις των πελατών και αποφαίνεται στο αν θα τις δεχτεί ή αν θα τις απορρίψει. Αν αποδεχτεί κάποια αίτηση, τότε επικοινωνεί με τον πραγματικό server εκ μέρους του πελάτη και προχωρεί στην αναμετάδοση της αίτησης προς τον πραγματικό server από τον πελάτη και τις απαντήσεις από τον πραγματικό server προς τον πελάτη.



Υπηρεσίες proxy σε Dual-homed host 2.5.1

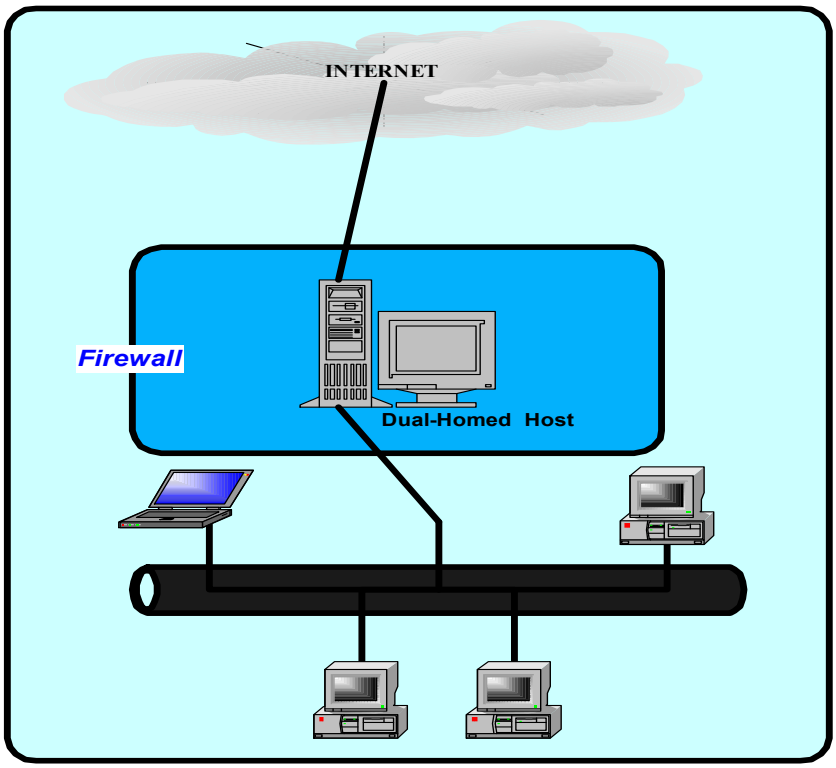
3 Αρχιτεκτονικές σχεδίασης των Firewalls

Σε αυτό το μέρος θα δούμε διάφορους τρόπους που μπορούμε να συνδυάσουμε στοιχεία των firewalls.

3.1 Η Αρχιτεκτονική Dual-Homed Host

Όπως καταλαβαίνουμε από τον τίτλο αυτή η αρχιτεκτονική είναι οικοδομημένη γύρω απ' το dual-homed host υπολογιστή, ένας υπολογιστής ο οποίος έχει τουλάχιστον δύο διεπαφές δικτύου. Ένας τέτοιος υπολογιστής θα μπορούσε να δουλεύει και σαν δρομολογητής μεταξύ των δικτύων που συνδέονται στις διεπαφές, έχει δηλαδή την ικανότητα να δρομολογεί πακέτα IP από το ένα δίκτυο στο άλλο. Όμως για να λειτουργήσει ένα firewall με αυτή την αρχιτεκτονική απενεργοποιούμε αυτή τη λειτουργία της δρομολόγησης. Έτσι, πακέτα από το ένα δίκτυο δεν δρομολογούνται απ' ευθείας στο άλλο. Συστήματα μέσα από το firewall μπορούν να επικοινωνήσουν με τον dual-homed host, εξωτερικά συστήματα μπορούν να επικοινωνήσουν με τον dual-homed host, αλλά δεν μπορούν να επικοινωνήσουν μεταξύ τους. Η IP κίνηση μεταξύ τους είναι εντελώς μπλοκαρισμένη.

Η αρχιτεκτονική του δικτύου με ένα dual-homed host firewall host είναι σχετικά απλή: ο dual-homed host κάθεται μεταξύ των δικτύων και είναι συνδεδεμένος σε αυτά (Εικόνα 3.1.1).



Αρχιτεκτονική του Dual-homed host 3.1.1

Οι Dual-homed hosts μπορούν να προσφέρουν υψηλό επίπεδο ελέγχου. Εάν δεν επιτρέπουμε την κίνηση μεταξύ εσωτερικού και εξωτερικού δικτύου και εντοπίσουμε πακέτο στο εσωτερικό δίκτυο το οποίο έχει εξωτερική πηγή σημαίνει ότι κάπου υπάρχει πρόβλημα ασφάλειας. Σε κάποιες περιπτώσεις ο Dual-homed host μπορεί να αποτρέψει συνδέσεις που ισχυρίζονται ότι είναι από μια συγκεκριμένη υπηρεσία αλλά δεν περιέχουν τη σωστή, για την υπηρεσία αυτή, δεδομένα, κάτι στο οποίο δεν τα καταφέρνει ένα φίλτρο πακέτων σε αυτό το επίπεδο ελέγχου.

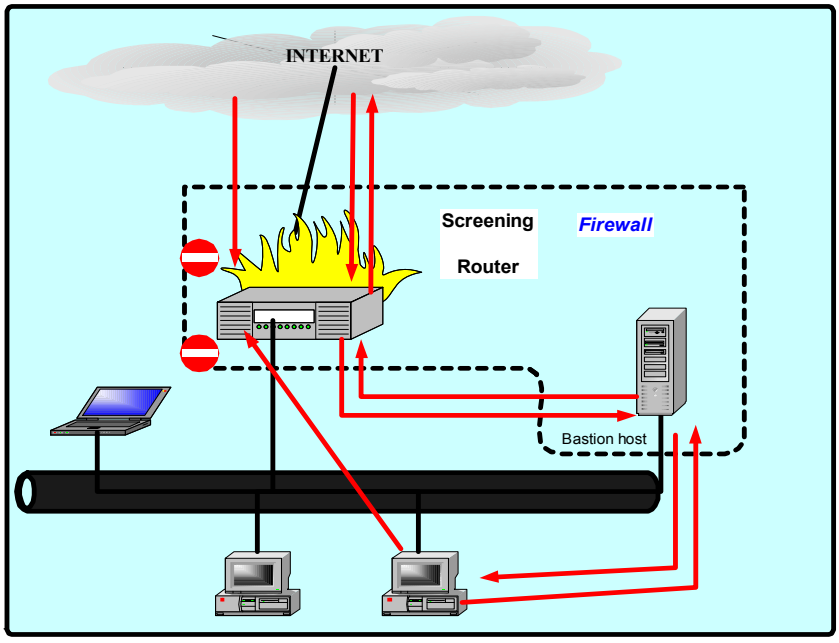
Ένας Dual-homed host μπορεί να προσφέρει υπηρεσίες μόνο μέσω της τεχνικής proxy ή βάζοντας τους χρήστες να συνδέονται απ' ευθείας με τον Dual-homed host. Όμως, λόγω προβλημάτων στην ασφάλεια που κρύβουν οι λογαριασμοί χρηστών και ιδιαίτερα σ' έναν Dual-homed host και λόγω του ότι

οι χρήστες δεν το βλέπουν σαν κάτι το εύκολο να συνδέονται σ ‘αυτόν, αυτή η μέθοδος δε χρησιμοποιείται ιδιαίτερα.

Η τεχνική του proxy παρουσιάζει πολύ λιγότερα προβλήματα αλλά μπορεί να μην προσφέρεται για όλες τις υπηρεσίες τις οποίες θέλουμε.

3.2 Αρχιτεκτονική του Screened Host

Η αρχιτεκτονική του screened host προσφέρει υπηρεσίες από ένα host ο οποίος είναι συνδεδεμένος μόνο στο εσωτερικό δίκτυο, χρησιμοποιώντας έναν ξεχωριστό router. Σε αυτή την αρχιτεκτονική, η βασική ασφάλεια παρέχεται από κάποιο φίλτρο πακέτων.(π.χ. τα φίλτρα πακέτων είναι αυτά που αποτρέπουν κάποιον από το να βγει έξω από το δίκτυο παρακάμπτοντας έναν proxy). Στην εικόνα 3.2.1 βλέπουμε μια απλή εκδοχή της αρχιτεκτονικής του screened host.



Αρχιτεκτονική του Screened Host 3.2.1

Ο bastion host βρίσκεται στο εσωτερικό δίκτυο. Το φίλτρο πακέτων στο screening router είναι έτσι ρυθμισμένος ώστε ο bastion host να είναι ο μόνος host του δικτύου που μπορεί να ανοίξει συνδέσεις προς το Διαδίκτυο (π.χ. για να παραδώσει την εισερχόμενη αλληλογραφία). Ακόμα και τότε δεν επιτρέπονται όλων των ειδών οι συνδέσεις. Οποιοδήποτε εξωτερικό σύστημα

αποπειραθεί να προσπελάσει εσωτερικά συστήματα ή υπηρεσίες θα συνδεθεί σε αυτόν τον host. Συνεπώς θα πρέπει να διατηρεί ένα υψηλό επίπεδο ασφάλειας host.

Τα φιλτράρισμα των πακέτων επιτρέπει επίσης στο bastion host να ανοίξει επιτρεπτές συνδέσεις προς τον έξω κόσμο.

3.3 Αρχιτεκτονική του Screened Subnet

Η αρχιτεκτονική του *screened subnet* προσθέτει ένα επιπλέον επίπεδο ασφάλειας στην αρχιτεκτονική του screened host προσθέτοντας ένα περιμετρικό δίκτυο που απομονώνει ακόμα παραπάνω το εσωτερικό δίκτυο από το Διαδίκτυο.

Λόγω της φύσης τους οι bastion hosts είναι τα πιο ευάλωτα μηχανήματα στο δίκτυο. Παρόλο τις προσπάθειες που γίνονται για την ασφάλισή του, είναι τα μηχανήματα που έχουν τις μεγαλύτερες πιθανότητες να δεχτούν επίθεση και αυτό επειδή αυτά είναι τα μηχανήματα *που μπορούν* να δεχτούν επίθεση.

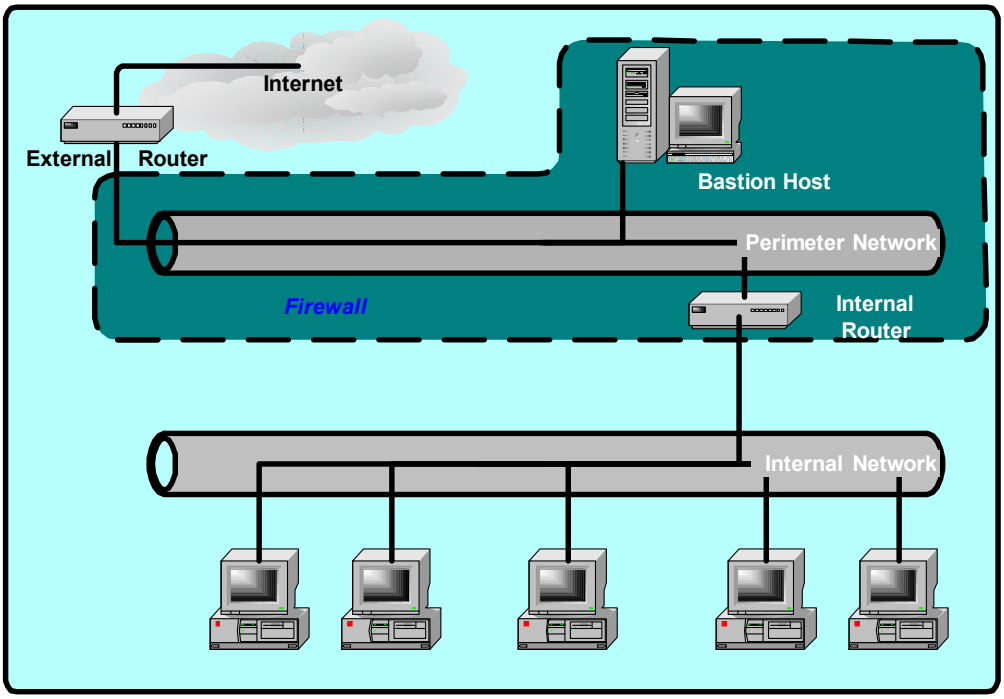
Απομονώνοντας τον bastion host σε ένα περιμετρικό δίκτυο μπορείς να μειώσεις την επίδραση μιας εισβολής σε αυτόν. Δίνει στον εισβολέα κάποια πρόσβαση αλλά όχι ολοκληρωτική.

Με την απλούστερη μορφή της αρχιτεκτονικής του screened subnet υπάρχουν δύο screening routers οι οποίοι συνδέονται και οι δύο στο περιμετρικό δίκτυο. Ο ένας βρίσκεται ανάμεσα στο περιμετρικό δίκτυο και στο εσωτερικό δίκτυο και ο άλλος βρίσκεται ανάμεσα στο περιμετρικό δίκτυο και στο εξωτερικό δίκτυο, συνήθως το Διαδίκτυο. Με αυτή την αρχιτεκτονική ένας εισβολέας θα πρέπει να περάσει και από τους δύο δρομολογητές για να φτάσει στο εσωτερικό δίκτυο. Ακόμα και αν ο επιτιθέμενος καταφέρει να εισβάλει στον bastion host θα πρέπει ακόμα να περάσει και τον εσωτερικό δρομολογητή. Έτσι εξαλείφεται η εκδοχή του ενός τρωτού σημείου που θα θέσει σε άμεσο κίνδυνο το εσωτερικό μας δίκτυο.

Ορισμένα site φτιάχνουν μια σειρά από επίπεδα περιμετρικών δικτύων μεταξύ του εξωτερικού και του εσωτερικού τους δικτύου. Οι λιγότερο έμπιστες υπηρεσίες και πιο ευάλωτες τοποθετούνται στα εξωτερικά περιμετρικά δίκτυα, όσο πιο μακριά από τ εσωτερικό δίκτυο. Η βασική ιδέα αυτής της δομής είναι να προσθέσουμε επίπεδα ασφάλειας στην πορεία προς τα περιμετρικά δίκτυα

ώστε να δυσκολέψουμε το έργο του εισβολέα, που έχει καταφέρει να παρακάμψει τα ανώτερα, και ασθενέστερα, περιμετρικά δίκτυα και θα προσπαθήσει να εισβάλει στο εσωτερικό μας δίκτυο. Αυτή η δομή βέβαια δεν έχει κανένα νόημα αν τα φίλτρα πακέτων επιτρέπουν στα ίδια πράγματα να περάσουν, δηλαδή να έχουν τους ίδιους κανόνες. Έτσι δεν έχουμε καμία αύξηση ασφάλειας.

Μια απεικόνιση της αρχιτεκτονικής των screened subnets φαίνεται στην εικόνα 3.3.1



Αρχιτεκτονική του Screened Subnet 3.3.1

3.3.1 Ορισμένες διαφοροποιήσεις των αρχιτεκτονικών

Ασφαλείς διαφοροποιήσεις:

- **Πολλαπλούς Bastion Host σε περιμετρικό δίκτυο**
- **Συγχώνευση εξωτερικού και εσωτερικού screening router ενός περιμετρικού δικτύου**
- **Συγχώνευση του bastion host με τον εξωτερικό screening router**
- **Χρήση πολλών εξωτερικών screening router**
- **Χρήση πολλών περιμετρικών δικτύων**
- **Χρήση dual-homed host και screened subnet**

Μη ασφαλείς διαφοροποιήσεις:

- **Συγχώνευση του εσωτερικού screening router με τον bastion host**
- **Χρήση πολλών εσωτερικών screening router**

3.4 Φιλτράρισμα Πακέτων (Packet Filtering)

Το φιλτράρισμα πακέτων είναι ένας μηχανισμός ασφάλειας δικτύων ο οποίος ελέγχει τα δεδομένα που ρέουν προς και από ένα δίκτυο. Επιτρέπει (allow, accept) ή αποτρέπει (deny, reject) τη μεταφορά δεδομένων βασιζόμενο:

- Στη διεύθυνση από όπου έρχονται τα δεδομένα
- Στη διεύθυνση στην οποία πηγαίνουν τα δεδομένα
- Τα πρωτόκολλα εφαρμογής και μεταφοράς που χρησιμοποιούνται για την μεταφορά των δεδομένων.

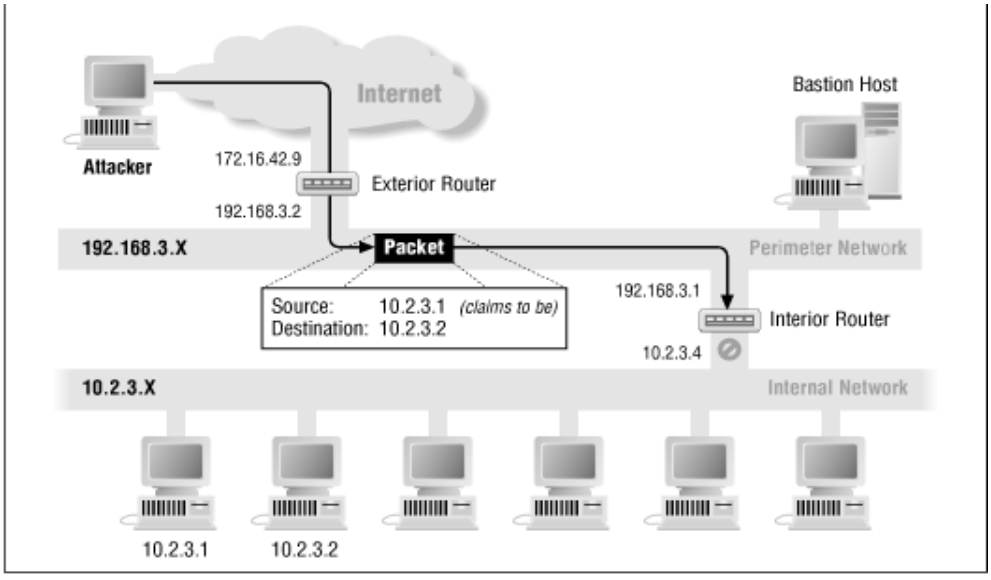
Τα περισσότερα φίλτρα πακέτων δεν παίρνουν αποφάσεις για την μοίρα των δεδομένων βασιζόμενα στα δεδομένα. Αποφάσεις που μπορεί να πάρει είναι του τύπου: Να μην επιτραπεί σε κανέναν από έξω να συνδεθεί προς τα μέσα με telnet, να επιτραπεί σε όλους να στείλουν αλληλογραφία με smtp, αυτός ο υπολογιστής μπορεί να στείλει ειδήσεις με nntp αλλά κανένας άλλος δεν μπορεί.

Δεν επιτρέπει εκφράσεις του τύπου: αυτός ο χρήστης μπορεί να χρησιμοποιήσει telnet για να συνδεθεί από έξω αλλά κανένας άλλος δεν μπορεί επειδή το "χρήστης" δεν είναι κάτι που μπορεί να αναγνωρίσει ένα φίλτρο πακέτων. Όπως επίσης η έκφραση "μετέφερε αυτό το αρχείο αλλά κανένα άλλο" δεν είναι αναγνωρίσιμη.

Το βασικό πλεονέκτημα των φίλτρων πακέτων είναι η ισχύς. Σου επιτρέπει την παροχή ασφάλειας σε ένα μοναδικό σημείο, για συγκεκριμένους τρόπους προστασίας που αφορούν όλο το δίκτυο. Αν, για λόγους ασφάλειας, έχουμε απενεργοποιήσει όλους τους telnet server στους υπολογιστές του δικτύου τότε τι γίνεται σε περίπτωση που κάποιος απ' τον οργανισμό φέρει μαζί του ένα νέο υπολογιστή ή εγκαταστήσει μόνος του έναν; Έχοντας ένα φίλτρο πακέτων όμως το οποίο αποτρέπει το telnet από έξω μας καθησυχάζει γιατί δεν έχει πια σημασία αν υπάρχει telnet server μέσα το δίκτυο.

Ορισμένα είδη προστασίας μπορούν να προσφερθούν *μόνο* από δρομολογητές φιλτραρίσματος και μπορούν να αναπτυχθούν σε συγκεκριμένες τοποθεσίες του

δικτύου μας. Για παράδειγμα μια καλή ιδέα είναι να απορρίπτουμε όλα τα πακέτα τα οποία έχουν εσωτερική διεύθυνση πηγής, δηλαδή πακέτα τα οποία ισχυρίζονται ότι έρχονται από το εσωτερικό δίκτυο αλλά στην πραγματικότητα έρχονται από το εξωτερικό δίκτυο γιατί τέτοια πακέτα είναι συνήθως μέρος μιας επίθεσης που ονομάζεται *address-spoofing*. Σε τέτοιες επιθέσεις ο επιτιθέμενος προσποιείται ότι έρχεται από το εσωτερικό μας δίκτυο. Αποφάσεις τέτοιου είδους μπορούν να παρθούν μόνο από ένα δρομολογητή φιλτραρίσματος ο οποίος βρίσκεται στην περίμετρο του δικτύου μας. Μόνο σε έναν δρομολογητή αυτού του είδους ,ο οποίος είναι η διαχωριστική γραμμή μεταξύ εσωτερικού και εξωτερικού δικτύου, έχουμε την δυνατότητα να αναγνωρίσουμε ένα τέτοιο πακέτο ελέγχοντας την διεύθυνση πηγής και το σύνδεση του δικτύου από την οποία προήλθε, από την εσωτερική ή την εξωτερική. Στην εικόνα 2.4.1 βλέπουμε ένα παράδειγμα της πλαστογράφησης της διεύθυνσης πηγής (source address forgery ή και IP spoofing).



IP Spoofing ή πλαστογράφηση διεύθυνσης πηγής 3.3.1

3.4.1 Πλεονεκτήματα του Φιλτραρίσματος Πακέτων

❖ Ένα από τα βασικότερα πλεονεκτήματα ενός φίλτρου πακέτων είναι ότι ένας μόνο, στρατηγικά τοποθετημένος δρομολογητής πακέτων μπορεί να προστατέψει ένα ολόκληρο δίκτυο.

❖ Το φιλτράρισμα πακέτων δεν απαιτεί γνώσεις ή συμμετοχή των χρηστών, όπως για έναν proxy. Δεν απαιτεί συγκεκριμένο λογισμικό ή ρυθμίσεις λογισμικού όπως για έναν proxy. Όταν περάσει ένα πακέτο το φίλτρο δεν υπάρχει καμία διαφοροποίηση από έναν απλό δρομολογητή. Οι χρήστες δεν θα καταλάβουν καν ότι υπάρχει εκτός και αν προσπαθήσουν κάτι το οποίο απαγορεύεται από την πολιτική ασφάλειάς μας. Αυτή η "διαφάνεια" σημαίνει ότι μπορούμε να κάνουμε φιλτράρισμα χωρίς την επίγνωση ή την συμμετοχή των χρηστών, κάτι το οποίο πολλές φορές διευκολύνει πολύ το έργο της ασφάλισης.

❖ Δυνατότητες φιλτραρίσματος πακέτων υπάρχουν στα περισσότερα προγράμματα δρομολόγησης (λογισμικό) και στους περισσότερους δρομολογητές (υλικό) που κυκλοφορούν στο Διαδίκτυο και στο εμπόριο.

3.4.2 Μειονεκτήματα του Φιλτραρίσματος Πακέτων

❖ Παρόλο την πληθώρα υλικών και λογισμικών φίλτρων πακέτων, τα φίλτρα δεν είναι ακόμα ένα τέλειο εργαλείο και συνεπώς έχουν και κάποια μειονεκτήματα. Ένα από αυτά είναι ότι οι κανόνες των φίλτρων είναι αρκετά δύσκολο να οριστούν. Όταν οριστούν, είναι δύσκολο να δοκιμαστούν. Οι δυνατότητες των φίλτρων πακέτων, σε ορισμένα προϊόντα, είναι ατελής με κάνοντας την εφαρμογή επιθυμητών δυνατοτήτων πολύ δύσκολη ή και απίθανη. Όπως κάθε είδος λογισμικού στους υπολογιστές, , μπορεί να υπάρχουν bugs. Στους δρομολογητές φιλτραρίσματος είναι πιο επικίνδυνα από άποψη ασφάλειας από ότι για έναν proxy, γιατί το φίλτρο πακέτων θα αφήσει απλά το πακέτο να περάσει, ενώ ο proxy απλά δεν θα το προωθήσει.

❖ Ορισμένα πρωτόκολλα δεν είναι κατάλληλα για φιλτράρισμα ακόμα και αν έχουμε κάνει μια πάρα πολύ καλή δουλειά στον ορισμό των κανόνων του φίλτρου. Τέτοια είναι τα NFS, NIS/YP (πρωτόκολλα που βασίζονται από το RPC) και οι εντολές "r" (rlogin, rdist, rcp κτλ.).

❖ Ορισμένες πολιτικές δεν μπορούν να εφαρμοσθούν σε ένα φίλτρο πακέτων. Για παράδειγμα, μπορείς να ορίσεις κανόνες με βάση τον host απ΄ τον οποίο έρχονται ή πηγαίνουν κάποια πακέτα αλλά δεν μπορείς να του ορίσεις κανόνες με βάση τον χρήστη. Ακόμα, στα φίλτρα μπορείς να ορίσεις κανόνες με

βάση το πρωτόκολλο μεταφοράς και το port ελπίζοντας ότι σε αυτό είναι ορισμένη η εφαρμογή για την οποία προορίζεται.

3.5 Τι κάνει ένας δρομολογητής τα πακέτα;

Όταν ένας δρομολογητής πακέτων τελειώσει με τον έλεγχο ενός πακέτου υπάρχουν δύο ενέργειες που μπορεί να κάνει: Να προωθήσει το πακέτο, να το δρομολογήσει σαν να ήταν ένας απλός δρομολογητής ή να το απορρίψει αν δεν συμφωνεί με τα κατάλληλα κριτήρια.

3.5.1 Ενέργειες Logging

Πέρα απ' το αν ένα πακέτο προωθείται ή απορρίπτεται, ίσως να θέλουμε να καταγράψουμε τις ενέργειες έκανε ο δρομολογητής μας για τα πακέτα (να κρατήσει δηλαδή ένα *log)*. Αυτό συνήθως συμβαίνει με τα πακέτα που απορρίπτονται για να γνωρίζουμε ποιες ενέργειες έγιναν οι ποίες δεν επιτρέπονταν.

Μπορεί επίσης να θέλουμε να καταγράψουμε τα TCP πακέτα τα οποία επιτρέπονται και ανοίγουν μια σύνδεση για να γνωρίζουμε το πλήθος των εισερχόμενων και εξερχόμενων συνδέσεων.

Διαφορετικές εφαρμογές φιλτραρίσματος πακέτων υποστηρίζουν διάφορες μορφές καταγραφής (logging). Κάποιες μπορεί να καταγράψουν συγκεκριμένες πληροφορίες ενός απορριφθέντος πακέτου και άλλες ολόκληρο το πακέτο. Κάποιες άλλες μπορεί να μην έχουν επιλογές για την καταγραφή πακέτων που επιτρέπονται. Καλό είναι πάντως να κρατάμε ένα αντίγραφο των logs και κάπου αλλού (π.χ. σύνδεση σε κάποιο host μέσω syslog).

3.5.2 Επιστρέφοντας Κωδικούς Σφαλμάτων ICMP

Εάν ένα πακέτο απορριφθεί, ο δρομολογητής μπορεί (ή και όχι) να επιστρέψει ένα μήνυμα κωδικού σφάλματος icmp που να ενημερώνει για το τι απέγινε το πακέτο. Αν αποφασίσουμε να επιστρέφουμε ένα icmp, η απόπειρα σύνδεσης θα αποτύχει αυτομάτως. Σε αντίθετη περίπτωση μπορεί να περάσουν κάποια λεπτά μέχρι το time out.

Υπάρχουν δύο ομάδες από μηνύματα icmp απ' τα οποία μπορούμε να διαλέξουμε :

- Τα γενικά “destination unreachable” (προορισμός απροσπέλαστος)- πιο συγκεκριμένα τα “host unreachable” και “network unreachable”.
- Οι κωδικοί "destination administratively unreachable" – συγκεκριμένα τα "host administratively unreachable" και "network administratively unreachable" codes.

Τα πρώτα φτιάχτηκαν για να δείχνουν ότι κάποια σύνδεση δεν υπάρχει ή δεν δουλεύει. Τα δεύτερα, φτιάχτηκαν συγκεκριμένα για να έχουν τα φίλτρα πακέτων κάτι να επιστρέφουν όταν ένα πακέτο απορρίπτεται.

3.6 Φιλτράροντας τη Διεύθυνση

Ο πιο απλός τρόπος για να φιλτράρουμε ένα πακέτο είναι το φιλτράρισμα της διεύθυνσης. Φιλτράροντας κατ’ αυτόν τον τρόπο περιορίζουμε τη ροή των πακέτων βασιζόμενοι στη διεύθυνση πηγής ή/ και προορισμού, δίχως να λάβουμε υπ’ όψιν το πρωτόκολλο που χρησιμοποιείται. Με τέτοιου είδους φιλτράρισμα μπορούμε να επιτρέψουμε σε ορισμένους εξωτερικούς host να επικοινωνούν με συγκεκριμένους εσωτερικούς ή να αποτρέψουμε μια επίθεση IP Spoofing. Ας πούμε για παράδειγμα ότι θέλουμε να αποτρέψουμε πακέτα με πλαστή διεύθυνση πηγής, θα δίναμε αυτόν τον κανόνα:

Κανόνας	**Κατεύθυνση**	**Διεύθυνση πηγής**	**Διεύθυνση προορισμού**	**Ενέργεια**
Α	Μέσα	Εσωτερική	Οποιαδήποτε	Απόρριψη

Πίνακας 3.5.21.1

Δηλαδή, ένα πακέτο, με κατεύθυνση προς τα μέσα (προς το εσωτερικό δίκτυο) και διεύθυνση πηγής κάποια διεύθυνση από το δίκτυό μας και με κατεύθυνση προς οπουδήποτε, απορρίπτεται.

3.6.1 Κίνδυνοι που απορρέουν

Δεν είναι, σε γενικές γραμμές, ασφαλές να εμπιστευόμαστε διευθύνσεις πηγής, γιατί είναι δυνατόν να πλαστογραφηθούν. Εκτός και αν χρησιμοποιείται κάποια μέθοδος κρυπτογραφικής πιστοποίησης μεταξύ μας και του host με τον

οποίο μιλάμε ώστε να είμαστε σίγουροι ότι μιλάμε με τον συγκεκριμένο host. Υπάρχουν δύο είδη επιθέσεων οι οποίες βασίζονται σε πλαστογράφηση (forgery) της διεύθυνσης πηγής:

- ***Source address forgery.*** Σε αυτό το είδος επίθεσης, ο επιτιθέμενος στέλνει πακέτα τα οποία ισχυρίζονται ότι είναι από κάποιον τον οποίο εμπιστευόμαστε κατά κάποιον τρόπο, ελπίζοντας να υπάρξει κάποια αντίδραση από αυτήν την εμπιστοσύνη, χωρίς όμως απαραίτητα να περιμένει να του σταλθούν κάποια πακέτα (Εικόνα 3.3.1).
- ***Man in the Middle forgery.*** Αυτό το είδος επίθεσης βασίζεται στο να υπάρχει κανονική σύνδεση και επικοινωνία, ισχυριζόμενος ότι αυτός είναι ο έμπιστός μας host.

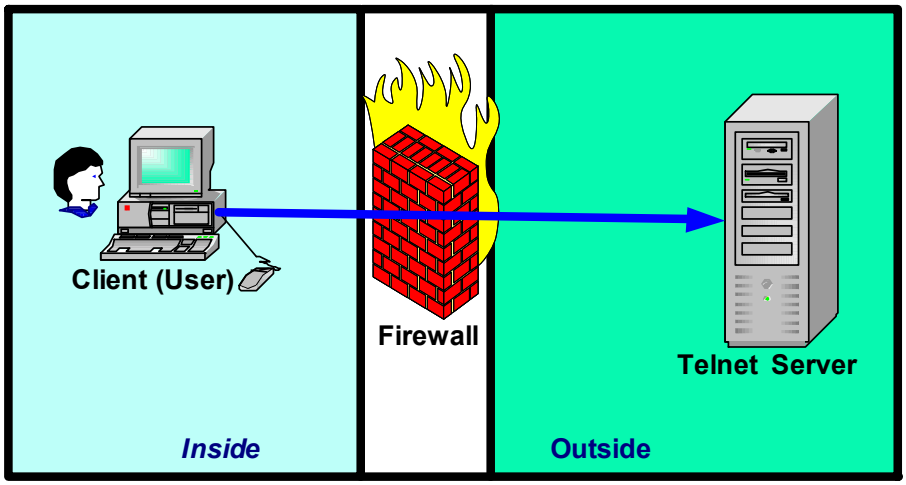
3.7 Φιλτράροντας την Υπηρεσία

Το μπλοκάρισμα των εισερχόμενων πακέτων με πλαστή διεύθυνση πηγής είναι η πιο κοινή χρήση του φιλτραρίσματος με τη διεύθυνση αποκλειστικά. Οι περισσότερες εφαρμογές του φιλτραρίσματος πακέτων αφορούν το φιλτράρισμα της υπηρεσίας.

Θα χρησιμοποιήσουμε ένα παράδειγμα με την υπηρεσία telnet. Θα δούμε την εξερχόμενη κίνηση telnet και την εισερχόμενη κίνηση telnet.

3.7.1 Εξερχόμενο Telnet.

Στην εξερχόμενη υπηρεσία telnet, κατά την οποία ένας τοπικός πελάτης (χρήστης) μιλά με έναν απομακρυσμένο διακομιστή, πρέπει να χειριστούμε και τα εισερχόμενα και τα εξερχόμενα πακέτα.



Εξερχόμενο Telnet 3.7.1.1

Τα εξερχόμενα πακέτα της εξερχόμενης υπηρεσίας περιέχουν την πληκτρολόγηση του χρήστη και αποτελούνται από τα εξής χαρακτηριστικά:

- Η IP διεύθυνση πηγής του εξερχόμενου πακέτου είναι η τοπική IP διεύθυνση της μηχανής του χρήστη.
- Η IP διεύθυνση προορισμού είναι η IP διεύθυνση του απομακρυσμένου διακομιστή.
- Το TCP port προορισμού είναι το 23, το γνωστό για telnet διακομιστές.
- Το TCP port πηγής είναι κάποιος τυχαίος αριθμός άνω του 1023. Θα το αποκαλούμε Y.
- Στο πρώτο εξερχόμενο πακέτο, το οποίο και εγκαθιστά τη σύνδεση, το ACK bit δεν θα είναι ανατεθειμένο. Σε όλα τα υπόλοιπα εξερχόμενα πακέτα θα είναι.

Τα εισερχόμενα πακέτα αυτής της εξερχόμενης υπηρεσίας περιέχουν τα δεδομένα που θα εμφανιστούν στην οθόνη του χρήστη και έχουν τα εξής χαρακτηριστικά:

- Η IP διεύθυνση πηγής του εισερχόμενου πακέτου είναι η IP διεύθυνση του απομακρυσμένου διακομιστή.
- Η IP διεύθυνση προορισμού του εισερχόμενου πακέτου είναι η IP διεύθυνση της μηχανής του τοπικού μας χρήστη.
- Ο τύπος του πακέτου IP είναι TCP.
- Το TCP port πηγής είναι 23, το port που χρησιμοποιεί ο διακομιστής δηλαδή.

- Το TCP port προορισμού είναι το ίδιο “Y” που χρησιμοποιήσαμε ως το port πηγής για τα εξερχόμενα πακέτα.
- Όλα τα πακέτα θα έχουν το ACK bit ανατεθειμένο γιατί έχει γίνει η σύνδεση από το πρώτο εξερχόμενο πακέτο.

3.7.2 Εισερχόμενο Telnet

Στην εισερχόμενη υπηρεσία telnet, ένας απομακρυσμένος πελάτης-χρήστης επικοινωνεί με έναν τοπικό διακομιστή telnet. Ας δούμε και εδώ τι γίνεται με τα εισερχόμενα και εξερχόμενα πακέτα.

Τα εισερχόμενα πακέτα για την εισερχόμενη υπηρεσία telnet περιλαμβάνουν την πληκτρολόγηση του χρήστη και περιέχουν τα ακόλουθα χαρακτηριστικά:

- Η IP διεύθυνση πηγής αυτών των πακέτων είναι η διεύθυνση της μηχανής του απομακρυσμένου χρήστη.
- Η IP διεύθυνση προορισμού είναι η διεύθυνση του τοπικού διακομιστή telnet.
- Ο τύπος του πρωτοκόλλου IP είναι TCP.
- Το TCP port πηγής είναι κάποιος τυχαίος αριθμός μεγαλύτερος του 1023 (Το βαφτίζουμε “Z”).
- Το TCP port προορισμού είναι το 23
- Το TCP ACK bit δεν θα ανατεθεί στο πρώτο εισερχόμενο πακέτο, που εγκαθιστά τη σύνδεση, αλλά θα ανατεθεί σε όλα τα υπόλοιπα εισερχόμενα πακέτα.

Τα εξερχόμενα πακέτα αυτής της εισερχόμενης telnet υπηρεσίας περιέχουν τις αποκρίσεις του διακομιστή μας, δηλαδή αυτά που θα εμφανιστούν στην οθόνη του απομακρυσμένου χρήστη και περιέχουν τα εξής χαρακτηριστικά:

- Η IP διεύθυνση πηγής είναι η διεύθυνση του τοπικού μας διακομιστή
- Η IP διεύθυνση προορισμού είναι αυτή του απομακρυσμένου χρήστη.
- Ο τύπος του πρωτοκόλλου IP είναι TCP.
- Το TCP port πηγής είναι το 23
- Το TCP port προορισμού είναι ο ίδιος τυχαίος αριθμός μεγαλύτερος του 1023 (“Z”).
- Το TCP ACK bit θα ανατεθεί σε όλα τα εξερχόμενα πακέτα.

3.7.3 Σύνοψη

Στον παρακάτω πίνακα βλέπουμε μια σύνοψη των εισερχόμενων και εξερχόμενων υπηρεσιών Telnet. (Πίνακας 3.7.3)

Κατεύθυνση υπηρεσίας	Κατεύθυνση πακέτου	Διεύθυνση πηγής	Διεύθυνση προορισμού	Τύπος πακέτου	PORT πηγής	PORT προορ.	ACK set
Εξερχόμενη	**Εξερχόμενη**	**Εσωτερική**	**Εξωτερική**	**TCP**	**Y**	**23**	**No**
Εξερχόμενη	**Εισερχόμενη**	**Εξωτερική**	**Εσωτερική**	**TCP**	**23**	**Y**	**Yes**
Εισερχόμενη	**Εισερχόμενη**	**Εξωτερική**	**Εσωτερική**	**TCP**	**Z**	**23**	**No**
Εισερχόμενη	**Εξερχόμενη**	**Εσωτερική**	**Εξωτερική**	**TCP**	**23**	**Z**	**Yes**

Συνοπτικός πίνακας για υπηρεσία TELNET 3.7.3.1

Αν θέλαμε να επιτρέψουμε εξερχόμενο telnet, αλλά τίποτα άλλο θα δίναμε τους κανόνες:

Rule	Direc-tion	Source Address	Dest. Address	Pro-tocol	Source Port	Dest. Port	ACK Set	Action
A	Out	Internal	Any	TCP	>1023	23	Either	Permit
B	In	Any	Internal	TCP	23	>1023	Yes	Permit
C	Either	Any	Any	Any	Any	Any	Either	Deny

Εξερχόμενο Telnet 3.7.3.2

- Ο κανόνας A επιτρέπει εξερχόμενα προς τους απομακρυσμένους διακομιστές telnet.
- Ο κανόνας B επιτρέπει τα πακέτα που επιστρέφουν από αυτήν τη σύνδεση να εισέλθουν. Ελέγχει αν το ACK bit είναι ανατεθειμένο έτσι ώστε να μην είναι δυνατόν να ανοιχτεί μια εισερχόμενη TCP σύνδεση από το port 23 της άλλης πλευράς σε ένα port μεγαλύτερο του 1023 στη δική μας πλευρά από κάποιον που μας επιτίθεται.
- Ο κανόνας C είναι ο προεπιλεγμένος κανόνας. Αν κανένας από τους προηγούμενους κανόνες δεν ταιριάξει, το πακέτο απορρίπτεται.

3.7.4 Κίνδυνοι που απορρέουν από το φιλτράρισμα της Υπηρεσίας

Υπάρχει ένα θεμελιώδες πρόβλημα με αυτόν τον τρόπο φιλτραρίσματος: μπορούμε να εμπιστευτούμε το port πηγής μόνο τόσο όσο εμπιστευόμαστε τον host τον οποίο χαρακτηρίζει.

Αν κατά λάθος μείνει ανοιχτό ένα port το οποίο δεν εξυπηρετείται από κάποια υπηρεσία, ένας απομακρυσμένος χρήστης θα μπορούσε να τρέξει έναν διακομιστή ή ένα πρόγραμμα πελάτη σε αυτό το port.

Όπως είπαμε και νωρίτερα, δεν μπορούμε να εμπιστευόμαστε μια διεύθυνση πηγής ποτέ. Αυτό που μπορούμε να κάνουμε είναι να περιορίσουμε τα ανοιχτά port όσο πιο πολύ μπορούμε. Πρέπει να μένουν ανοιχτά μόνο τα port στα οποία αντιστοιχούν κάποιες έμπιστες υπηρεσίες-διακομιστές, τους οποίους πρέπει να ασφαλίζουμε και αυτούς όσο μπορούμε περισσότερο.

Επειδή πολλές υπηρεσίες χρησιμοποιούν τυχαίους αριθμούς port άνω του 1023 για τους πελάτες και επειδή ορισμένες υπηρεσίες κάνουν το ίδιο για κάποιους διακομιστές πρέπει συχνά να αποδεχόμαστε εισερχόμενα πακέτα για port τα οποία μπορεί να έχουν μη-έμπιστους διακομιστές. Με το TCP μπορούμε να αποδεχόμαστε εισερχόμενα πακέτα χωρίς να αποδεχόμαστε εισερχόμενες συνδέσεις με το να απαιτούμε το ACK bit να είναι ορισμένο. Με το UDP δεν έχουμε αυτή την επιλογή γιατί δεν υπάρχει αντίστοιχο ACK bit.

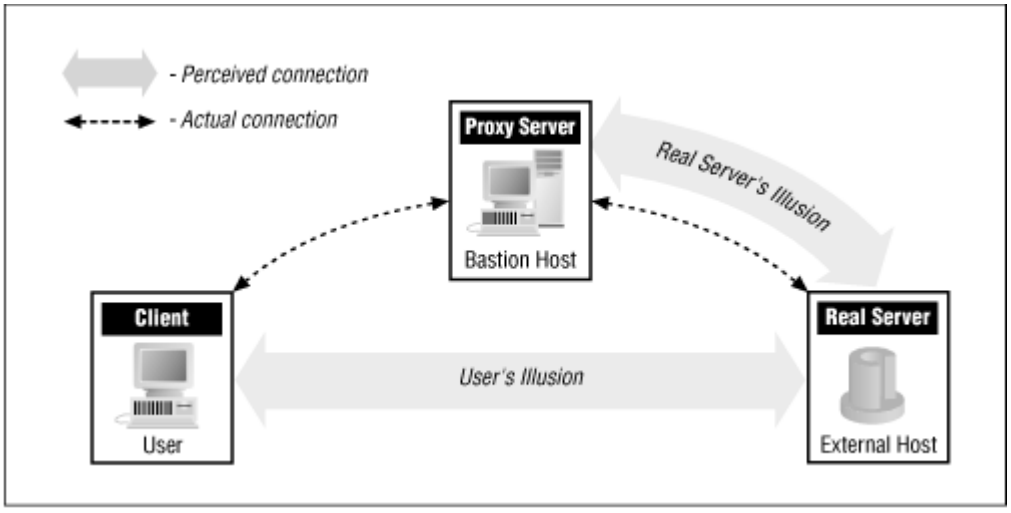
Μέρος Τρίτο

Proxy Servers

4 Διακομιστές διαμεσολάβησης- Proxy Servers

Ένας proxy είναι ένας μεσάζων σε μια διαδικτυακή συναλλαγή. Είναι μια εφαρμογή βρίσκεται μεταξύ ένα πελάτη και έναν πραγματικό διακομιστή. Χρησιμοποιούνται πάρα πολύ συχνά και για firewalls για την παροχή ασφάλειας. Επιτρέπουν και μπορούν και να καταγράψουν αιτήσεις από το εσωτερικό μας δίκτυο προς το εξωτερικό δίκτυο.

Ένας proxy συμπεριφέρεται και σαν πελάτης, για τους εξωτερικούς διακομιστές, και σαν διακομιστής για τους εσωτερικούς πελάτες. Ο proxy δέχεται και επεξεργάζεται αιτήσεις από τους εσωτερικούς πελάτες και μετά τις προωθεί, σαν δικές του αιτήσεις προς τους εξωτερικούς διακομιστές. Όταν απαντήσει ένας εξωτερικός διακομιστής στον proxy, αυτός προωθεί τις απαντήσεις στον κατάλληλο πελάτη του δικτύου. Πολλές φορές οι proxy αναφέρονται και σαν “application layer gateways” (πύλες επιπέδου εφαρμογής). Αυτό το όνομα αντικατοπτρίζει το γεγονός ότι ο proxy βρίσκεται στο επίπεδο εφαρμογής του μοντέλου OSI , όπως και οι πελάτες –διακομιστές.



Διακομιστές Διαμεσολάβησης-Proxy Servers 4.1

Οι proxy βρίσκουν πολλές εφαρμογές στον κόσμο των δικτύων. Μερικές από αυτές είναι:

- logging. Η καταγραφή συμβάντων
- Access controls.

- Φιλτράρισμα.
- Μετάφραση-μεταγλώττιση
- Έλεγχος για ιούς.
- Caching.
- Reverse proxy
- Reverse hosting
- Server proxying

Τα βασικότερα πλεονεκτήματα ενός proxy server είναι

- ***Η ασφάλεια:*** η δυνατότητα να επιτρέπεις ή να αποτρέπεις την πρόσβαση σε εξωτερικούς διακομιστές με την χρήση κάποιων "access list".
- ***Καταγραφή συμβάντων:*** Η καταγραφή των κινήσεων των πελατών με πρόσβαση στο εξωτερικό δίκτυο. Αναφορές και στατιστικά μπορούν να γεννηθούν από τα *logs*.
- ***Caching:*** ιστοσελίδες που ζητούνται πολύ συχνά από πελάτες του δικτύου, αποθηκεύονται τοπικά σε κάποιο κοινόχρηστο πόρο και είναι προσβάσιμες για όλους τους τοπικούς πελάτες.. Αυτό εξυπηρετεί διότι κάνουμε εξοικονόμηση του bandwidth (εύρους ζώνης) της σύνδεσης του Internet.

Υπάρχουν δύο τύποι proxy. Ο πρώτος είναι ο application-level proxy (επιπέδου εφαρμογής), ο οποίος καταλαβαίνει την υπηρεσία του επιπέδου εφαρμογής για την οποία κάνει την διαμεσολάβηση. Καταλαβαίνει και μπορεί και διερμηνεύει τις εντολές του πρωτοκόλλου του επιπέδου εφαρμογής που χρησιμοποιείται.

4.1 Πώς λειτουργούν οι Proxy Servers και οι Transparent Proxy Servers

Ας υποθέσουμε ότι έχουμε την εταιρία comp.com. Έχουμε ένα εσωτερικό δίκτυο και μια σύνδεση για το Internet, την ppp στον proxy (proxy.comp.com με εξωτερική διεύθυνση την 1.2.3.4 και εσωτερική την 192.168.0.1). έχουμε και έναν host που θα τον λέμε "εγώ" και έχει διεύθυνση 192.168.0.100.

4.1.1 Παραδοσιακό proxy

Σε αυτό το σενάριο, τα πακέτα από το ιδιωτικό δίκτυο προς το Internet ποτέ δεν θα το διασχίσουν και το αντίθετο. Οι διευθύνσεις του δικτύου πρέπει να είναι εσωτερικές (οι 192.168.*.*, 10.*.*.*, 172.16.*.* - 172.31.*.* δεν είναι πραγματικές διευθύνσεις του Internet). Ο μόνος τρόπος που βγαίνει κάποιο πακέτο προς το Internet είναι από τον proxy-firewall. Έχουμε εγκαταστήσει τον proxy μας στο port 8080. Ο "εγώ" έχει ρυθμίσει τον φυλλομετρητή του να χρησιμοποιεί τον proxy στο port 8080. Στο ιδιωτικό δίκτυο δεν χρειάζεται να ορίσουμε gateway.

Δίνουμε στο φυλλομετρητή του host την διεύθυνση http://www.teiep.gr. Ο φυλλομετρητής μας πηγαίνει στον proxy port 8080 χρησιμοποιώντας για εαυτό του το port 1100. Του ζητά την σελίδα. Εάν την έχει στην cache του την επιστρέφει. Αν όχι, τότε ψάχνει το www.teiep.gr και βρίσκει την διεύθυνση Α.Β.Γ.Δ Ανοίγει τότε μια σύνδεση προς αυτόν από το port 1123 στο port 80 του διακομιστή και ζητά την ιστοσελίδα. Καθώς την παραλαμβάνει, την κρατά στην cache και την προωθεί στη σύνδεση προς το φυλλομετρητή του "εγώ".

Από την πλευρά του teiep.gr, η σύνδεση γίνεται από το 1.2.3.4 της ppp σύνδεσης του proxy με port 1123 προς το Α.Β.Γ.Δ στο port 80 του διακομιστή του. Από την πλευρά του "εγώ", η σύνδεση γίνεται από το 192.168.0.100 με port 1100 προς το 192.168.0.1, την εσωτερική διασύνδεση του proxy, στο port 8080.

4.1.2 Διαφανής Proxy (Transparent proxy)

Και σε αυτό το σενάριο, τα πακέτα από το ιδιωτικό δίκτυο προς το Internet ποτέ δεν θα το διασχίσουν και το αντίθετο. Οι διευθύνσεις του δικτύου μας είναι και εδώ ιδιωτικές. Ο μόνος τρόπος που βγαίνει κάποιο πακέτο προς το Internet είναι από τον proxy-firewall ο οποίος συνδέεται και στα δύο δίκτυα. Τρέχουμε ένα πρόγραμμα για transparent proxying (διαφανής διαμεσολάβηση) και τα πακέτα που εξέρχονται από αυτό το μηχάνημα, αλλάζουν προορισμό και πηγαίνουν προς τον transparent proxy. Διαφανής διαμεσολάβηση (transparent proxy) σημαίνει ότι οι πελάτες δεν χρειάζεται ότι ανακατεύεται ένας proxy.

Θα χρησιμοποιήσουμε ένα παρόμοιο παράδειγμα με το προηγούμενο. Οι διευθύνσεις του δικτύου είναι ίδιες με το παραπάνω παράδειγμα, καθώς και του "εγώ", του transparent proxy-firewall και του www.teiep.gr. Ο proxy είναι

εγκατεστημένος στο port 8080. Ο πυρήνας κάνει ανακατεύθυνση του port πηγής 80 προς το port 8080 του proxy. Ο φυλλομετρητής μας είναι ρυθμισμένος να συνδέεται απ' ευθείας. Το gateway στο ιδιωτικό μας δίκτυο πρέπει να δείχνει στον proxy – firewall (gw:192.168.0.1).

Δίνουμε στο φυλλομετρητή μας την διεύθυνση www.teiep.gr. Τότε ανοίγει μια σύνδεση προς αυτή τη διεύθυνση από το τοπικό port 1050 και ζητά από το διακομιστή την ιστοσελίδα (port 80). Καθώς τα πακέτα από το Εγώ(1050) παιρνούν στο μηχάνημα με τον proxy (80), ανακατευθύνονται στον αναμένοντα proxy στο port 8080. Ο proxy ανοίγει μια σύνδεση από το port 1100 προς το Α.Β.Γ.Δ port 80 όπου πήγαιναν τα πρωτότυπα πακέτα. Καθώς ο proxy παίρνει τα δεδομένα από αυτή τη σύνδεση τα ανακατευθύνει προς τη σύνδεση με τον φυλλομετρητή ο οποίος και ανακατασκευάζει και προβάλλει την ιστοσελίδα.

Από την πλευρά του teiep.gr η σύνδεση γίνεται από το 1.2.3.4 (port 1100) προς το Α.Β.Γ.Δ στο port 80. Από την πλευρά του εγώ, η σύνδεση γίνεται από το 192.168.0.100 port 1050 προς το Α.Β.Γ.Δ στο port 80, αλλά στην πραγματικότητα μιλά με τον transparent proxy μας.

4.2 Χαρακτηριστικά ενός Caching Proxy Server

Το βασικότερο χαρακτηριστικό ενός caching proxy είναι η δυνατότητα να αποθηκεύει απαντήσεις άλλων διακομιστών για μετέπειτα χρήση, κάτι το οποίο μας γλιτώνει χρόνο και εύρος ζώνης. Συνήθως έχουν και πολλά άλλα πολύ χρήσιμα χαρακτηριστικά που μπορούν να φανούν πολύτιμα. Τα περισσότερα από αυτά είναι λίγο άσχετα με το caching αλλά μπορείς να τα κάνεις μόνο με έναν caching proxy. Για παράδειγμα αν θέλεις να αυθεντικοποιείς τους χρήστες σου αλλά δεν ενδιαφέρεσαι να κάνεις caching, είναι πολύ πιθανό να χρησιμοποιήσεις έναν caching proxy για αυτό το σκοπό.

4.2.1 Authentication (Αυθεντικοποίηση)

Ο proxy μπορεί να ζητά από τους χρήστες του να αυθεντικοποιούνται πριν εξυπηρετήσει οποιεσδήποτε αιτήσεις τους. Αυτό είναι πολύ χρήσιμο για proxy-firewall. Όταν ο κάθε χρήστης έχει το δικό του όνομα χρήστη και κωδικό πρόσβασης, μόνο εξουσιοδοτημένοι χρήστες μπορούν, π.χ. να δουν ιστοσελίδες από το WWW από το δίκτυό μας. Ακόμα, προσφέρει έναν ποιοτικότερο τρόπο παρακολούθησης πιθανών προβλημάτων.

4.2.2 Φιλτράρισμα αιτήσεων

Οι caching proxy συχνά χρησιμοποιούνται για να φιλτράρουν αιτήσεις (Request Filtering) των χρηστών. Οι οργανισμοί συνήθως έχουν κάποιες πολιτικές οι οποίες απαγορεύουν στο προσωπικό την πρόσβαση πορνογραφικού υλικού τις ώρες εργασίας. Για την ενίσχυση της εφαρμογής αυτής της πολιτικής μπορεί να ρυθμιστεί ο proxy να απορρίπτει αιτήσεις προς γνωστές πορνογραφικές ιστοσελίδες. Αυτού του είδους το φιλτράρισμα είναι πολλές φορές αμφισβητήσιμο. Πολλοί το εξισώνουν με λογοκρισία και διευκρινίζουν, σωστά συχνά, ότι το φιλτράρισμα αιτήσεων δεν είναι και τέλειο.

4.2.3 Φιλτράρισμα απαντήσεων

Οι proxy μπορούν να φιλτράρουν απαντήσεις (response filtering). Αυτό συνήθως αναφέρεται στον έλεγχο των περιεχομένων ενός αντικειμένου που κατεβάζουμε. Ένα φίλτρο που ελέγχει για ιούς σε λογισμικό είναι ένα καλό παράδειγμα.

4.2.4 Prefetching

Prefetching είναι η διαδικασία ορισμένων δεδομένων προτού ζητηθεί. Συστήματα δίσκων και μνημών συνήθως χρησιμοποιούν τη μέθοδο “Prefetching” επίσης γνωστό και ως “read ahead” (προ διάβασμα). Για τον ιστό συνήθως χρησιμοποιείται για να ανακτήσει υπέρ-συνδέσμους και εικόνες από ένα αρχείο HTML.

Είναι μια ανταλλαγή μεταξύ του χρόνου απόκρισης (latency) και του εύρους ζώνης. Ένας proxy επιλέγει αντικείμενα για το prefetch υποθέτοντας ότι κάποιος πελάτης θα τα ζητήσει. Σωστές προβλέψεις έχουν ως αποτέλεσμα μείωση του χρόνου απόκρισης. Λανθασμένες προβλέψεις ωστόσο χρησιμοποιούν άδικα το εύρος ζώνης.

4.2.5 Μετάφραση και Μετατροπή κώδικα

Η μετάφραση και η μετατροπή του κώδικα αναφέρονται στην επεξεργασία του περιεχομένου χωρίς τη σημαντική μετατροπή του νοήματος ή της εμφάνισης. Σαν παράδειγμα μπορούμε να φανταστούμε μια εφαρμογή η οποία μεταφράζει μια ιστοσελίδα από αγγλικά σε ελληνικά καθώς την κατεβάζει.

Η μετατροπή του κώδικα συνήθως αναφέρεται σε χαμηλού επιπέδου αλλαγές σε ψηφιακά δεδομένα παρά σε υψηλού επιπέδου ανθρώπινη γλώσσα. Η αλλαγή του format μιας εικόνας από giff σε jpeg είναι ένα καλό παράδειγμα. Το νόημα αυτής της διαδικασίας είναι ότι μια εικόνα σε jpeg είναι μικρότερη σε μέγεθος, άρα και μπορούμε να μειώσουμε το χρόνο μεταφοράς. Ένα ζεύγος proxy που συνεργάζονται, μπορούν να συμπιέσουν όλες τις μεταφορές μεταξύ τους και να τις αποσυμπιέσουν πριν φτάσουν στον πελάτη.

4.2.6 Σχηματισμός Κίνησης (Traffic Shaping)

Ένας σημαντικός αριθμός οργανισμών χρησιμοποιούν proxy επιπέδου εφαρμογής για να ελέγχουν τη χρησιμοποίηση του εύρους ζώνης. Κατά μιαν έννοια, αυτή η διαδικασία γίνεται στο επίπεδο δικτύου όπου είναι δυνατόν ο έλεγχος της ροής των πακέτων ωστόσο, το επίπεδο εφαρμογής παρέχει πολύ χρήσιμες, επιπλέον, πληροφορίες που οι διαχειριστές.

Πριν συνεχίσουμε, πρέπει να εξηγήσουμε τι είναι cache hits και cache misses. Τα “cache-hits” είναι οι αιτήσεις σελίδων ή αντικειμένων που βρέθηκαν στην cache και δεν χρειάσθηκε να γίνει καν σύνδεση με τον πραγματικό διακομιστή. Αυτό συνήθως γίνεται επειδή κάποιος χρήστης έχει νωρίτερα ζητήσει την σελίδα και αυτή έχει κρατηθεί στην cache. Αυτή είναι η πλέον επιθυμητή κατάσταση μιας cache-proxy. Τα “cache-misses” είναι οι αιτήσεις οι οποίες δεν ικανοποιήθηκαν από την cache μας και χρειάστηκε η επικοινωνία της cache με τον πραγματικό διακομιστή ώστε να πάρει απάντηση ο πελάτης. Τα ποσοστά αυτών των επιτυχιών και αποτυχιών, καθώς και άλλα στατιστικά στοιχεία μπορούμε να τα καταγράφουμε (logging).

4.3 Transparent Caching

Το transparent caching ή διαφανής caching, λέγεται έτσι γιατί αναχαιτίζει την δικτυακή κίνηση στον φυλλομετρητή. Σε αυτή την κατάσταση, η cache “βραχυκυκλώνει” την διαδικασία ανάκτησης εάν το επιθυμητό αρχείο βρίσκεται στην cache. Τα transparent caches είναι εξαιρετικά χρήσιμα για τις εταιρίες παροχής υπηρεσιών Internet οι φυλλομετρητές δεν χρειάζονται ρύθμιση. Αλλά είναι και ο πιο απλός τρόπος να χρησιμοποιούμε μία cache σ’

ένα ιδιωτικό δίκτυο και αυτό επειδή δεν απαιτούν κάποιο σαφή συντονισμό με άλλες cache.

Ο όρος διαφανής- transparent είναι υπερφορτωμένος, έχοντας διαφορετικές έννοιες κατά περίσταση. Κάποιες φορές εννοείται μια ρύθμιση η οποία παρεμβάλλεται στην κίνηση του port 80 προς εξωτερικούς διακομιστές από κάποιο χρήστη και την παρακάμπτει και κάποιες άλλες εννοείται ένας σημασιολογικά διαφανής proxy που δεν αλλάζει την σημασία ή το περιεχόμενο των αιτήσεων και απαντήσεων του πελάτη. Στην πραγματικότητα δεν υπάρχει πραγματική διαφάνεια, μόνο ημιδιαφάνεια και σίγουρα δεν υφίσταται διαφανής cache.

4.3.1 Πλεονεκτήματα της διαφανούς Caching

Τα πλεονεκτήματα της διαφανούς caching είναι περίπου τα αντίθετα από αυτά του proxy caching. Τα βασικότερα είναι:

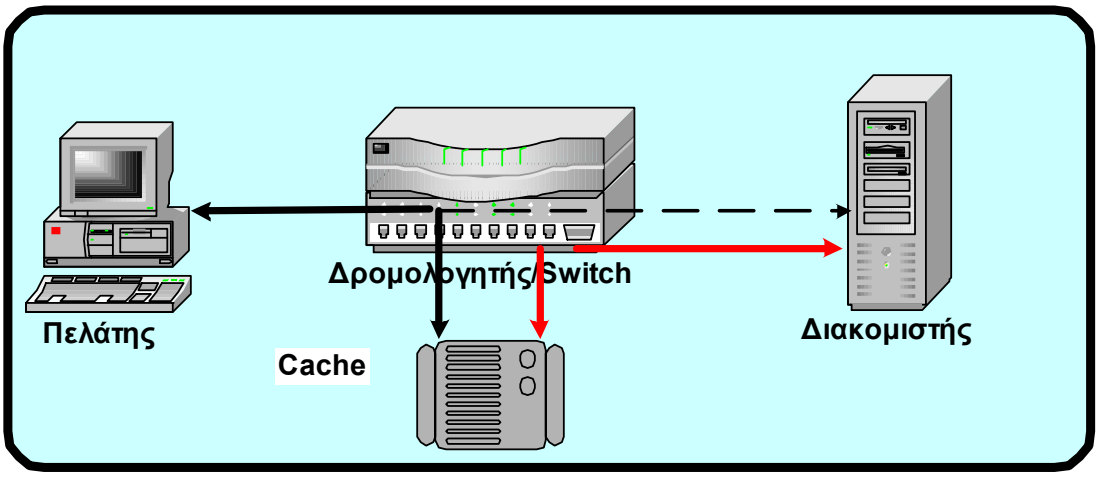
- Εύκολη Διαχείριση- Ο φυλλομετρητής μας δεν χρειάζεται να είναι κατάλληλα ρυθμισμένος για να επικοινωνεί με την cache.
- Κεντρικός Έλεγχος- Ο χρήστης δεν μπορεί να αλλάξει τις ρυθμίσεις του φυλλομετρητή του ώστε να παρακάμψει τον proxy.

4.3.2 Μειονεκτήματα της διαφανούς caching

Κάποια από τα μειονεκτήματα που έχει η διαφανής caching είναι :

- Έλλειψη σταθερότητας- Λόγω του ότι βασίζεται στη σταθερή διαδρομή δρομολόγησης μεταξύ του πελάτη και του πραγματικού διακομιστή, η οποία τυγχάνει να περνά μέσα από μια cached διαδρομή, είναι ευάλωτη σε αλλαγές δρομολόγησης στο Διαδίκτυο. Δηλαδή, αν μια γίνει σύνδεση ενός πελάτη με μια cache και συμβεί μια αλλαγή δρομολόγησης η οποία αναγκάζει τον πελάτη να πάρει μια διαδρομή η οποία δεν περνά από την συσκευή που έκανε την εκτροπή, η συνεδρία θα διακοπεί και ο χρήστης θα πρέπει να ξαναζητήσει την σελίδα. Αν, διαδρομές στο Διαδίκτυο αλλάζουν συνεχώς τότε τα αποτελέσματα θα είναι ακόμα πιο απρόβλεπτα.

- Έλεγχος χρηστών- Η διαφανής caching παίρνει τον έλεγχο από το χρήστη. Πολλοί χρήστες έχουν σοβαρές προκαταλήψεις σε ότι αφορά το caching και θα άλλαζαν παροχέα για να την αποφύγουν ή να την αποκτήσουν.
- Προαπαίτηση φυλλομετρητών- Πολλές διαφανής cache έχουν συγκεκριμένες απαιτήσεις από τους φυλλομετρητές των πελατών, δηλαδή στην κεφαλίδα του πακέτου να αναγράφεται το όνομα του host για τον οποίο προορίζεται και αυτό διότι οι cache αυτές δεν μπορούν να προσπελάσουν την IP διεύθυνση προορισμού από την IP διεύθυνση του πακέτου. Δηλαδή, σε περίπτωση που δεν υπάρχει η ζητούμενη στην cache, δεν μπορούν να καταλάβουν ποιος είναι ο πραγματικός διακομιστής για να ζητήσουν από αυτόν τη σελίδα. Αν και σήμερα, πάνω του 90% των φυλλομετρητών παρέχουν αυτό το χαρακτηριστικό.



Διαφανής (Transparent) Caching 4.3.1

4.3.3 Η Δρομολόγηση

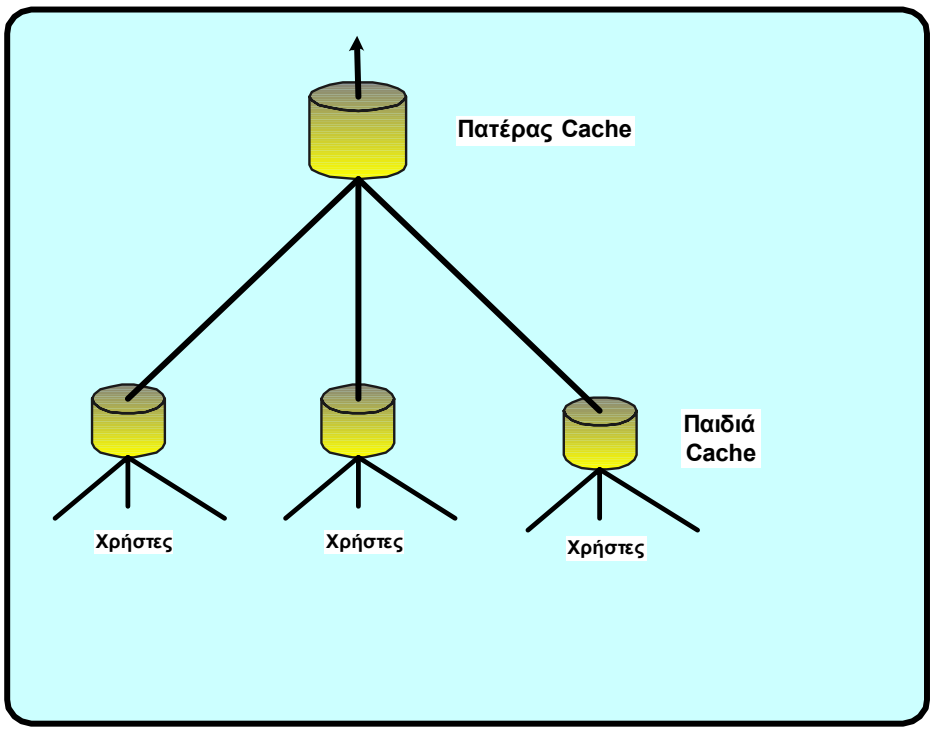
Η διαδικασία της "απαγωγής" των πακέτων ξεκινά στο επίπεδο δικτύου (IP), όπου όλα τα IP πακέτα δρομολογούνται μεταξύ κόμβων. Σε αυτό το επίπεδο ένας δρομολογητής ή ένα switch αναγνωρίζει πακέτα HTTP και τα εκτρέπει προς μια cache αντί να τα προωθήσει στον αρχικό προορισμό. Υπάρχουν αρκετοί τρόποι για να πετύχουμε την απαγωγή:

- ***Inline*** **–** Ένα Inline cache είναι μια συσκευή η οποία συνδυάζει δρομολόγηση (ή και γεφύρωμα δικτύων-bridge) και caching ιστού σε ένα κομμάτι υλικού. Ένα παράδειγμα μπορεί να είναι ένας υπολογιστής με δύο ή περισσότερες κάρτες δικτύου το οποίο έχει για λειτουργικό σύστημα Linux ή Unix και σε αυτό τρέχει ο Squid cache-proxy.
- ***Επιπέδου 4 Switch*** **–** Το switch δουλεύει συνήθως στο επίπεδο 2 (επίπεδο σύνδεσης δεδομένων). Ένα switch επιπέδου 4 μπορεί να παίρνει και αποφάσεις προώθησης βασιζόμενο στα χαρακτηριστικά του επιπέδου 4 (επίπεδο μεταφοράς), όπως είναι οι διευθύνσεις IP και αριθμοί port του TCP. Χρησιμοποιούνται επίσης και για εξισορρόπηση του φόρτου του διακομιστή.
- ***Web Cache Coordination Protocol*** **–** Το **WCCP** είναι ένα πρωτόκολλο της Cisco Systems που απαιτεί την υλοποίησή του σ' ένα δρομολογητή (ή ακόμα και ένα switch) και στην cache. Αποτελείται από δύο συστατικά μέρη. Το πρώτο είναι το πρωτόκολλο ελέγχου και το δεύτερο είναι ο μηχανισμός ανακατεύθυνσης της κίνησης.
- ***Cisco Policy Routing*** **–** Η πολιτική δρομολόγησης (policy routing) αναφέρεται στην ικανότητα ενός δρομολογητή να παίρνει αποφάσεις για την προώθηση βασιζόμενο όχι μόνο στην διεύθυνση προορισμού του πακέτου. Μπορούμε να το χρησιμοποιήσουμε αυτό για να ανακατευθύνουμε πακέτα βασιζόμενοι στους αριθμούς port προορισμού.

4.4 Ιεραρχίες Cache

Μια ιεραρχία από cache είναι μια διευθέτηση από cache που συνεργάζονται μεταξύ τους. Σε μια τέτοια ιεραρχία, οι cache των κατώτερων επιπέδων προωθούν αποτυχίες (cache misses) της cache προς τα ανώτερα επίπεδα ώσπου να αποδεχτεί την αίτηση κάποια άλλη cache ή να προωθηθεί στον πραγματικό διακομιστή. Οι ιεραρχίες είναι ελκυστικές γιατί μπορούν να προσφέρουν βελτιώσεις της αποδοτικότητας. Κάποιες αποτυχίες της cache μας θα είναι επιτυχίες σε κάποιες από τις ανώτερες cache με αποτέλεσμα την μείωση του

εύρους ζώνης του δικτύου και βελτιώνει την ταχύτητα του κατεβάσματος (downloads).



Ιεραρχία Cache 4.4.1

Το παιδί-cache προωθεί τις αποτυχίες του (cache misses) σ' έναν πατέρα-cache. Τότε ο πατέρας του παρέχει μια απάντηση από τη δική του cache, τον πραγματικό διακομιστή ή μια άλλη cache. Ένας πατέρας μπορεί να χρησιμοποιεί bandwidth προς τους πραγματικούς διακομιστές ώστε να ικανοποιήσει την αίτηση της cache του παιδιού.

Οι σχέσεις των αδερφών-cache είναι σχεδιασμένες ώστε να αποτρέπουν μια cache να επιβαρύνει με κάποιο τίμημα μια άλλη cache. Όλες οι αιτήσεις που στέλνονται προς έναν αδερφό-cache θα πρέπει να είναι επιτυχίες (cache hits). Ένας αδερφός δε θα πρέπει ποτέ να δώσει ένα αντικείμενο που έχει ζητηθεί από έναν πατέρα-cache και δεν υπάρχει στην cache του. Αν δεν υπάρχει επιστρέφει ένα μήνυμα ότι αρνείται να προωθήσει την αίτηση. Μια cache επικοινωνεί με τα παιδιά-cache χρησιμοποιώντας ένα από τα πρωτόκολλα *"Intercache"* . Αυτά τα πρωτόκολλα επιτρέπουν στις cache να μαθαίνουν εάν μια γειτονική cache έχει κάποιο συγκεκριμένο αντικείμενο στην cache τους. Μια αίτηση πρέπει να σταλθεί μόνο σ' έναν αδερφό εάν το πρωτόκολλο intercache προβλέπει ότι θα είναι επιτυχία cache.

Αυτές οι σχέσεις δεν είναι δεδομένες. Μια cache μπορεί να είναι πατέρας για κάποιες cache και αδερφός για άλλες. Αυτή είναι η πιο χρησιμοποιημένη μορφή ιεραρχίας από τους παροχείς Internet. Μια απεικόνιση αυτής της ιεραρχίας φαίνεται στην εικόνα 4.4.1.

4.4.1 Πλεονεκτήματα της ένταξης σε ιεραρχία

- Αποδοτικότητα. Κλειδιά στο αν η ένταξη σε μια ιεραρχία cache θα είναι αποδοτική, είναι η επιτυχία σε μια γειτονική cache σε περίπτωση που είναι αποτυχία στη δική μας cache, η γειτονική επιτυχία cache να φτάνει σε εμάς πιο γρήγορα από ότι θα έφτανε αν ήταν αποτυχία και ερχόταν από τον πραγματικό διακομιστή. Ακόμα, οι αποτυχίες των ανωτέρων cache δεν θα πρέπει να είναι αισθητά πιο αργές από ότι θα ήταν η απάντηση από τον πραγματικό διακομιστή.
- Μη προεπιλεγμένη δρομολόγηση. Οι πατέρες-cache είναι χρήσιμοι όταν πρέπει να επιβάλλεις την ροή της κίνησης μέσω μιας συγκεκριμένης διαδρομής στο δίκτυο. Ένα διάσημο παράδειγμα είναι όταν έχεις ένα firewall. Θέλεις να περνά όλη η κίνηση του δικτύου μέσω αυτού. Είναι πολύ συνηθισμένο πλέον πολλοί οργανισμοί και πολλές εταιρίες να χρησιμοποιούν ένα διαφανή (transparent) proxy. Οι HTTP συνδέσεις των πελατών ανακατευθύνονται προς έναν caching proxy σε αυτές τις περιπτώσεις και δεν απορρίπτονται. Αν σε μια τέτοια περίπτωση πελάτης είναι ο caching proxy, το firewall proxy είναι ένας πατέρας-cache και ας μην το καταλαβαίνει το παιδί. Ακόμα, μπορούν να χρησιμοποιηθούν πολλαπλοί πατέρες-cache για πολλαπλές συνδέσεις προς τα εξωτερικά δίκτυα όπου το φόρτο μοιράζεται αναλόγως με τις απαιτήσεις.

4.4.2 Μειονεκτήματα της ένταξης σε ιεραρχία

Πριν αποφασίσουμε την ένταξη σε μια ιεραρχία θα πρέπει να γνωρίζουμε και κάποια από τα μειονεκτήματά της.

- Εμπιστοσύνη. Όταν ενταχθούμε σε μια ιεραρχία είναι σαν να λέμε ότι εμπιστευόμαστε όλα τα μέλη της ιεραρχίας απόλυτα. Πιστεύουμε ότι

τα δεδομένα που μας δίνει είναι έγκυρα, δεν έχουν τροποποιηθεί με κάποιο τρόπο. Εμπιστευόμαστε σε όλα τα μέλη την ιδιωτικότητα των αιτήσεών μας.

- Χαμηλά ποσοστά επιτυχίας (Low hit Ratio). Τα ποσοστά επιτυχιών από πατέρες και αδερφούς-cache είναι συνήθως πολύ χαμηλά σε σύγκριση με μια cache η οποία εξυπηρετεί απ' ευθείας τελικούς χρήστες.
- Επιπτώσεις στις δρομολογήσεις. Όσο η απόσταση μεταξύ των δρομολογητών αυξάνεται (hops), αυξάνονται και οι επιπτώσεις στις διαφοροποιήσεις της δρομολόγησης. Αν για παράδειγμα ένας πατέρας έχει πολλές συνδέσεις για το Internet και κάποια από αυτές διακοπεί, ενώ το παιδί-cache έχει και αυτό μια σύνδεση Internet, αν μια απ' τις συνδέσεις του πατέρα κοπεί δεν θα μπορεί να επικοινωνήσει με κάποιους πραγματικούς διακομιστές και θα στέλνει στα παιδιά-cache μηνύματα σφαλμάτων. Όμως, εφόσον υπάρχει και η άλλη σύνδεση του παιδιού, ίσως αυτό να θελήσει να χρησιμοποιήσει αυτήν.
- Η διατήρηση της συνέπειας και της εγκυρότητας, από χρονικής άποψης, μιας σελίδας μεταξύ των μελών της ιεραρχίας είναι δύσκολη διαδικασία. Σε μια περίπτωση όπου ένα παιδί έχει δύο πατέρες-cache και έχουν και οι δύο μια απάντηση πως θα μπορούμε να ξέρουμε ποια απάντηση είναι πιο έγκυρη; Το καλύτερο που μπορούμε να κάνουμε είναι να χρησιμοποιήσουμε μια διαδικασία ακύρωσης αντικειμένων (object invalidation process). Ορισμένα από τα πρωτόκολλα cache έχουν τέτοια χαρακτηριστικά.
- Μεγάλες οικογένειες. Τα πολλά επίπεδα στην ιεραρχία πολλές φορές προκαλούν προβλήματα, ειδικά στα ανώτερα επίπεδά της και αυτό λόγω των πολλών αιτήσεων που δέχονται από τους εκατοντάδες ή και χιλιάδες πελάτες που βρίσκονται από κάτω.
- Όποτε ένας proxy προωθεί μια αίτηση προς έναν πραγματικό διακομιστή καταγράφει τη σύνδεση από την IP του proxy. Όταν ένας παροχέας υπηρεσιών ή ο ιδιοκτήτης της σελίδας πιστεύει ότι γίνεται κάποια κατάχρηση ή κακομεταχείριση επικοινωνεί με τον υπεύθυνο της IP από όπου έρχονται οι αιτήσεις (proxy) για τα παράπονα.

- Πολλές φορές δεν επιστρέφουν σωστά ή έγκυρα μηνύματα σφαλμάτων. Ένα παράδειγμα είναι ότι ένας proxy δεν μπορεί να καταλάβει τη διαφορά μεταξύ ενός ονόματος DNS που πραγματικά δεν υπάρχει ή απλά δεν δουλεύει η υπηρεσία προσωρινά.
- Μεταξύ μιας σχέσης αδερφών-cache υπάρχει ένας μηχανισμός πρόβλεψης επιτυχίας (cache hit) η οποία γίνεται από τα πρωτόκολλα cache. Στην περίπτωση που η πρόβλεψη δεν είναι σωστή, δηλαδή όταν μια αίτηση προβλέπεται να είναι επιτυχία στην cache του αδερφού αλλά τελικά δεν είναι, το αποκαλούμε *λανθασμένη επιτυχία (false hit).*
- Βρόχος προώθησης. Ένας βρόχος προώθησης παρουσιάζεται όταν μια αίτηση στέλνεται πάνω – κάτω μεταξύ δύο ή παραπάνω κόμβων της ιεραρχίας. Αυτό μπορεί να συμβεί μεταξύ δυο cache όταν στον καθένα είναι δηλωμένος ο άλλος ως πατέρας-cache.
- Βλάβες και άρνηση υπηρεσίας (Service Denial). Υπάρχουν κάποια προβλήματα, που είναι πιο δύσκολα να εντοπιστούν, από ότι μια ολοκληρωτική, μηχανική βλάβη σε έναν πατέρα-cache όπως είναι η υπερφόρτωση με κίνηση του πατέρα , το οποίο έχει σαν αποτέλεσμα την αύξηση του χρόνου των αποκρίσεων. Μια πιθανή αιτία άρνησης υπηρεσίας είναι κάποιο πρόβλημα με τον διακομιστή DNS του πατέρα-cache. Αυτές οι ενδείξεις βέβαια δεν είναι σίγουρο ότι οφείλονται σε κάποιο σφάλμα.

4.5 InterCache Protocols

Αυτά τα πρωτόκολλα χρησιμοποιούνται μεταξύ συνεργαζόμενους cache-proxy για πολλούς λόγους, ο βασικότερος εκ των οποίων είναι να βοηθούν σε αποφάσεις προώθησης, δηλαδή δεδομένου κάποιων στοιχείων, προς ποια κατεύθυνση να στείλει την αίτηση;

4.5.1 ICP

Είναι το αυθεντικό πρωτόκολλο intercache. Πρωταρχικός του σκοπός είναι να μαθαίνει εάν κάποια γειτονική cache έχει πιο φρέσκο αντίγραφο ενός συγκεκριμένου αντικειμένου. Οι γείτονες-cache απαντούν είτε με ένα ναι (HIT),

είτε με ένα όχι (MISS). Η cache συλλέγει ένα συγκεκριμένο αριθμό από απαντήσεις ICP και παίρνει μια απόφαση προώθησης. Ακόμα και αν όλοι οι γείτονες απαντήσουν με MISS, το ICP μπορεί να παρέχει πρόσθετες υποδείξεις που βοηθούν στο να διαλέξει τον καλύτερο πατέρα-cache.

Το ICP είναι πέραν του τέλειου, όμως χρησιμοποιείται ακόμα ευρέως.

4.5.2 CARP (Cache Array Routing Protocol)

Το CARP δεν είναι ένα πρωτόκολλο αυτό καθεαυτό. Σχεδιάστηκε για να επιλύσει ένα πού συγκεκριμένο πρόβλημα. Το πώς να επιτύχουμε αποδοτικά και κλιμακωτά την εξισορρόπηση του φόρτου ενώ αυξάνουμε τα ποσοστά επιτυχιών (hit ratios) και μειώνουμε το χρόνο αδράνειας. Είναι πολύ χρήσιμο σε περιπτώσεις που η cache μας αποτελείται από πολλά μηχανήματα (cache *Cluster*).

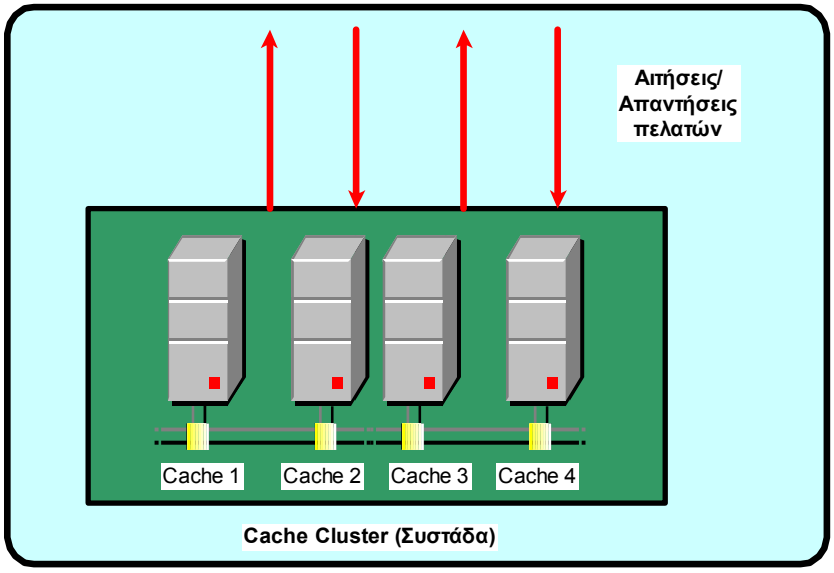
Για κάθε αίτηση, το CARP υπολογίζει ένα βαθμό για κάθε proxy cache. Η αίτηση προωθείται στον proxy με το μεγαλύτερο βαθμό. Εάν αυτό αποτύχει, τότε δοκιμάζεται η cache με το δεύτερο μεγαλύτερο βαθμό. Ο βαθμός είναι ένας υπολογισμός βασιζόμενος σ' ένα hash του URL, ένα hash του ονόματος της cache, και τα ειδικό βάρος που έχει ανατεθεί στην κάθε cache. Το σημαντικότερο χαρακτηριστικό αυτής της διαδικασίας είναι ότι εάν προστεθεί άλλη μια μηχανή για την cache δεν αλλάζει την ιεραρχία των βαθμών των υπολοίπων cache, αλλά δημιουργεί νέες βαθμολογίες. Στατιστικά, οι νέοι βαθμοί θα είναι μεγαλύτεροι από τους προηγούμενους για το μέρος των URL που είναι ανάλογο στο βάρος της cache στο cluster.

Το CARP καθορίζει και έναν τύπο αρχείων για ένα *Proxy Array Membership Table.* Έναν πίνακα δηλαδή, ο οποίος επιτρέπει σε πελάτες να διαπιστώσουν ποιες cache ανήκουν σε μια ομάδα, σε ένα *group.* Ο αλγόριθμος του CARP μπορεί να χρησιμοποιηθεί σε οποιοδήποτε πελάτη ιστού, όπως είναι ένας φυλλομετρητής ή έναν proxy cache. Το CARP δουλεύει μόνο για σχέσεις γονέων- παιδιών γιατί προβλέπει cache hits.

4.6 Cache Cluster (Συστάδα Cache)

Ένα *Cache cluster* είναι μια ομάδα από ξεχωριστούς proxy cache που είναι ρυθμισμένοι να ενεργούν σαν να ήταν ένας διακομιστής. Δηλαδή, οι χρήστες και οι πελάτες τους αντιλαμβάνονται ως μια μονάδα.

Μια συστάδα διαφέρει από την ιεραρχία σε κάποιες λεπτομέρειες. Αρχικά, τα μέλη της συστάδας βρίσκονται το ένα κοντά στο άλλο, φυσικά και τοπολογικά, δηλαδή βρίσκονται στο ίδιο δωμάτιο και ανήκουν στο ίδιο υποδίκτυο. Πολλοί οργανισμοί χρησιμοποιούν cache clusters για να εξυπηρετούν ή να παρέχουν περισσότερες σελίδες και περίσσιες υπηρεσίες. Αν σε έναν οργανισμό υπάρχει ένας proxy, αλλά η κίνηση αυξάνεται και επιβαρύνονται, με αποτέλεσμα να γίνονται αργές, οι υπηρεσίες τότε μια καλή λύση, χωρίς να χαθεί το υπάρχον προϊόν cache και τα περιεχόμενα της, είναι να πάρει άλλη μια μηχανή και να φτιάξει ένα μικρό cluster.



Cache Cluster 4.6.1

Βέβαια, υπάρχουν και άλλοι λόγοι για να χρησιμοποιήσει ένας οργανισμός συστάδες. Αναφέρω τρεις:

4.6.1 Η "Ρεζέρβα"

Ένας τρόπος να παρέχουμε πλεονάζουσες υπηρεσίες είναι να έχουμε σε αναμονή μια δεύτερη cache. Σε κανονική λειτουργία, όλες οι αιτήσεις πηγαίνουν στην πρωταρχική cache. Αν αυτή αποτύχει αναλαμβάνει η δεύτερη.

Αυτή η διαρρύθμιση δεν είναι ακριβώς μια συστάδα, μιας και μόνο μία εκ των δύο cache λειτουργεί σε μια χρονική στιγμή. Οι τεχνικές όμως είναι παρόμοιες.

Κάποια γνωστά προϊόντα (Switch Επιπέδου 4 και 7) μπορούν να ρυθμιστούν να δουλεύουν ως transparent proxy ή με μια εικονική διεύθυνση διακομιστή (virtual server). Μπορούμε να πούμε στο switch τις πραγματικές IP διευθύνσεις για την πρωταρχική cache και την cache – ρεζέρβα. Κανονικά προωθεί όλες τις συνδέσεις στην πρωταρχική. Αν το switch διαπιστώσει ότι η πρωταρχική έχει πέσει, τότε χρησιμοποιεί τη ρεζέρβα. Εφόσον οι χρήστες μιλούν στον εικονικό διακομιστή, δεν υπάρχουν προβλήματα με DNS και ARP timeouts.

4.6.2 Ταχύτητα διεκπεραίωσης και Κατανομή Φόρτου

Ένα cache cluster με κατανομή φόρτου (load sharing) μπορεί να βελτιώσει την ταχύτητα διεκπεραίωσης και την αξιοπιστία. Η ταχύτητα διεκπεραίωσης αυξάνεται διότι πολλές cache μπορούν να χειριστούν περισσότερη κίνηση από ότι μία. Η αξιοπιστία αυξάνεται γιατί όταν παρουσιαστεί κάποιο πρόβλημα σε μία cache, οι άλλες απορροφούν τον αυξημένο φόρτο.

Ο πιο φτηνός τρόπος για να πετύχουμε κατανομή του φόρτου είναι με το DNS Server, να δηλώσουμε το ίδιο όνομα host σε όλα τα μέλη της συστάδας, δηλαδή η μέθοδος *round-robin,* κατά την οποία ο DNS server θα ανακυκλώνει τις IP των μελών και θα δίνει άλλη IP σε κάθε lookup.

Μια πιο ρωμαλέα προσέγγιση, αν και πιο ακριβή, είναι η χρήση ενός switch επιπέδου 4 ή κάποια γνωστά προϊόντα για εξισορρόπηση φόρτου. Με αυτή την προσέγγιση η κατανομή του φόρτου γίνεται αρκετά πιο ισορροπημένα από ότι στην προσέγγιση round-robin και δεν έχουμε μεγάλες καθυστερήσεις.

Σε πολλές περιπτώσεις όπου υπάρχει cache cluster και στον πραγματικό διακομιστή (ιστού) με ένα switch επιπέδου 4 μπροστά από αυτό, το οποίο διανέμει τις αιτήσεις με βάση τη διεύθυνση IP. Όταν η επικοινωνία όμως περιέχει πληροφορίες συνεδρίας (session information, π.χ. χρήση “cookies”), και κάποια ακόλουθα πακέτα πάνε σε κάποιον άλλον διακομιστή του cluster, απορρίπτονται. Αυτό λύνεται με τη χρήση των switch επιπέδου 7 τα οποία καταλαβαίνουν πληροφορίες όπως τα cookies.

4.6.3 Εύρος Ζώνης (Bandwidth)

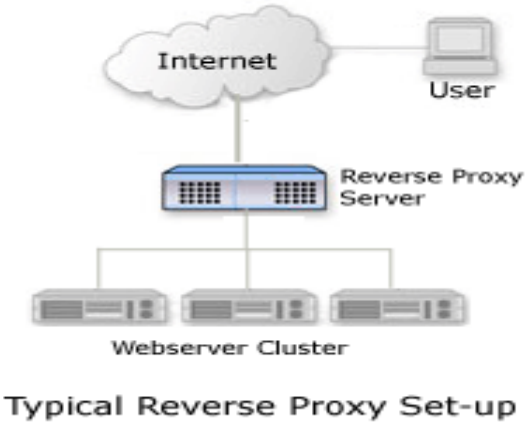
Μια απλή διαμόρφωση για κατανομή φόρτου αποτελεί χαμένο χώρο στο αποθηκευτικό μέσο και σπατάλη του εύρους ζώνης. Λέμε χαμένος χώρος γιατί η ίδια απάντηση μπορεί να αποθηκευτεί σε πολλές cache και λέμε σπατάλη του εύρους ζώνης γιατί δεν χρειάζεται πάντα να προωθούμε ένα "cache miss" προς τον πραγματικό διακομιστή εάν γνωρίζουμε ότι ένα άλλο μέλος της συστάδας έχει ήδη την απάντηση αποθηκευμένη.

Υπάρχουν δύο τρόποι να βελτιώσουμε την χρήση των δίσκων και του εύρους ζώνης. Ο ένας είναι να διανεμηθούν οι αιτήσεις πριν μπουν στη συστάδα, δηλαδή κάποια συσκευή ή κάποιος αλγόριθμος φροντίζει ώστε η ίδια αίτηση να πηγαίνει προς το ίδιο μέλος της συστάδας. Ο δεύτερος τρόπος είναι να δημιουργήσουμε "αδερφικές σχέσεις" μεταξύ των cache-μελών της συστάδας και να χρησιμοποιήσουμε ένα πρωτόκολλο intercache να εντοπίζουμε απαντήσεις που βρίσκονται ήδη στην cache μας. Σε αυτή την περίπτωση δεν μας ενδιαφέρει ποια cache παρέλαβε την αρχική αίτηση.

Υπάρχουν αρκετές τεχνικές και προϊόντα που διανέμουν αιτήσεις και τις αναθέτουν σε συγκεκριμένα μέλη της συστάδας. Κάποια από αυτά είναι το WCCP, τα switch επιπέδου 4 και επιπέδου 7 και το πρωτόκολλο CARP.

4.7 Reverse Proxy

Το *reverse proxy cache*, γνωστό και ως *Web Server Acceleration* (επιτάχυνση διακομιστή ιστού), είναι ένας τρόπος να μειώνουμε το φόρτο ενός αρκετά φορτωμένου web server, βάζοντας ανάμεσα σε αυτόν και το Διαδίκτυο έναν proxy cache, το οποίο προσθέτει και επιπλέον ασφάλεια. Με σωστή χρήση του reverse proxy διευκολύνεται πολύ η δουλειά ενός web server ο οποίος παράγει στατικά και δυναμικά αντικείμενα. Τα στατικά μπορούν να αποθηκευτούν στην cache του reverse proxy, ενώ ο web server θα είναι πιο ελεύθερος να παράγει το δυναμικό περιεχόμενο.



Reverse proxying ή web acceleration 4.7.1

Εφαρμόζοντας έναν reverse proxy παράλληλα με κάποιους web servers, το site μας μπορεί:

- Να αποφύγει περιττά έξοδα για την αγορά πρόσθετων web server, αυξάνοντας τις ικανότητες του υπάρχοντος.
- Θα εξυπηρετούν περισσότερες αιτήσεις για στατικό υλικό από τον web server.
- Θα εξυπηρετούν περισσότερες αιτήσεις για δυναμικό υλικό από τον web server
- Να αυξήσει το κέρδος της επιχείρησης, μειώνοντας τα λειτουργικά έξοδα συμπεριλαμβανομένου και τα έξοδα που απαιτούνται για το εύρος ζώνης που χρειάζεται.
- Επιτάχυνση του χρόνου απόκρισης των σελίδων και επιτάχυνση των download για τους εξωτερικούς χρήστες, μεταφέροντάς τους μια γρηγορότερη και καλύτερη εμπειρία της σελίδας και των υπηρεσιών μας.

Εάν η ιστοσελίδα μας δεν έχει γραφτεί με τρόπο να δουλεύει με κάποιο proxy, δε θα μπορεί να εκμεταλλευτεί όλες τις δυνατότητες ενός reverse proxy.

5 Η Αρχιτεκτονική του Proxy Server

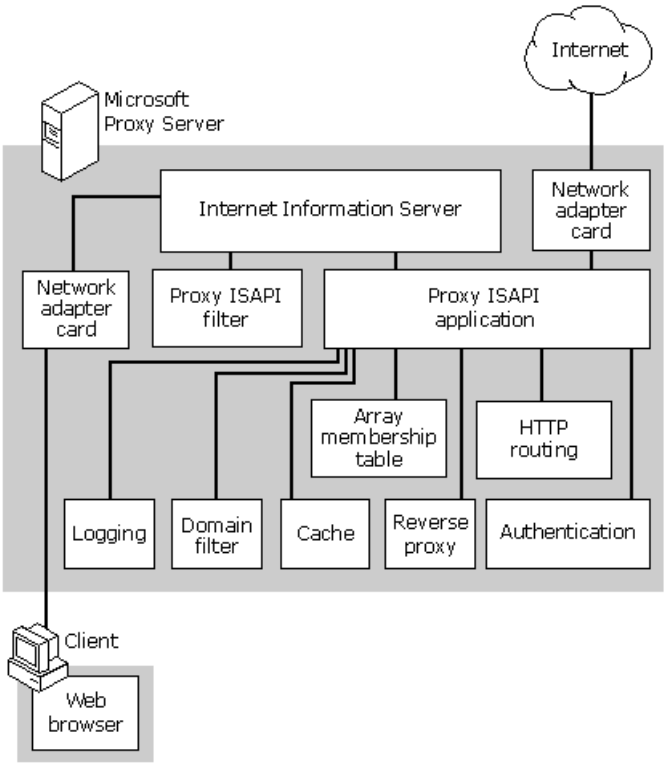
Ο Proxy Server αποτελείται από τις ακόλουθες τρεις υπηρεσίες :

- **Υπηρεσία Web Proxy**: παρέχει δυνατότητα caching, δρομολόγηση της cache (CARP), υποστήριξη για αλυσίδες και Reverse Proxying. Η υπηρεσία Web Proxy υποστηρίζει κάθε πελάτη που χρησιμοποιεί το HTTP πρωτόκολλο.
- **Υπηρεσία WinSock Proxy**: παρέχει υποστήριξη Winsock για κάθε windows socket API συναρτήσεις, εκτελεί μετατροπή IPX σε IP, και παρέχει Server Proxying. Η υπηρεσία WinSock Proxy υποστηρίζει κάθε πελάτη που χρησιμοποιεί Winsock 1.1, ή μεγαλύτερη έκδοση.
- **Υπηρεσία Socks Proxy**: παρέχει υποστήριξη SOCKS και λειτουργικότητα για διαδικασίες βασισμένες σε Socket.

5.1 Υπηρεσία Web Proxy

Ο Proxy Server υποστηρίζει πλήρως το πρωτόκολλο CERN-Proxy, με επιπρόσθετη υποστήριξη για υπηρεσίες Proxy επιπέδου εφαρμογής. Ο Web Proxy εκτελεί λειτουργίες συσχετιζόμενες και με τους πελάτες και με τους Servers. Σαν Server, δέχεται WWW αιτήσεις από πελάτες του εσωτερικού δικτύου. Σαν πελάτης, απαντά στις αιτήσεις των πελατών του εσωτερικού δικτύου, εκδίδοντας τις κατάλληλες αιτήσεις σε έναν WWW Server στο Internet. Αυξάνοντας την ασφάλεια και την λειτουργικότητα για τις συνδέσεις των χρηστών, η υπηρεσία Web Proxy κάνει πολύ περισσότερα από το να μεταβιβάζει απλώς τα δεδομένα ανάμεσα στους Servers και τους πελάτες.

Λειτουργικά, η υπηρεσία Web Proxy αποτελείται από δύο συστατικά: το Proxy ISAPI φίλτρο και την Proxy ISAPI εφαρμογή, όπως φαίνεται στην Εικόνα 6.



Εικόνα 6
Η αρχιτεκτονική της υπηρεσίας Web Proxy

Η υπηρεσία Web Proxy παρέχει τα ακόλουθα χαρακτηριστικά:

- **Συμβατότητα με CERN-Proxy.** Η υπηρεσία Web Proxy υποστηρίζει όλους τους δημοφιλείς φυλλομετρητές του Internet και το πρωτόκολλο μεταφοράς υπερκειμένου (HTTP), το Gopher και το πρωτόκολλο μεταφοράς αρχείων (FTP). Επίσης, η υπηρεσία Web Proxy υποστηρίζει το πρωτόκολλο HTTP-S για ασφαλείς συνεδριάσεις με τη χρήση Secure Socket Layer (SSL) συνδέσεων.
- **Internet Server Application Programming Interface(ISAPI)** Το ISAPI αποτελείται από δύο εφαρμογές : το ISAPI φίλτρο και την ISAPI εφαρμογή, τα οποία στην πραγματικότητα είναι DLLs και παρέχουν συγκεκριμένες λειτουργίες μέσα στον Proxy Server.
  - Το ISAPI φίλτρο παρέχει μία επέκταση στον IIS Web Server, και χρησιμοποιείται όταν ο Server δέχεται μία HTTP αίτηση. Ένα ISAPI φίλτρο παρεμβάλλεται μεταξύ γεγονότων και του Server. Μπορεί να ανακόψει συγκεκριμένα γεγονότα του Server πριν αυτός τα διαχειριστεί. Όταν φορτώνεται ένα φίλτρο, ανακοινώνει στον Server τι είδους γεγονότα θα χειριστεί. Αν προκύψουν αυτά τα γεγονότα, το φίλτρο τα

επεξεργάζεται, τα προωθεί σε άλλο φίλτρο, ή τα στέλνει στον Server. Το ISAPI φίλτρο κοιτάει το είδος της αίτησης που δέχεται. Αν είναι αίτηση CERN Proxy, το ISAPI φίλτρο προσθέτει πληροφορίες για να στείλει την αίτηση στην ISAPI εφαρμογή. Αν δεχτεί μία HTTP αίτηση, την προωθεί απλά στον IIS Server για επεξεργασία.

- Η ISAPI εφαρμογή παίρνει την αίτηση από το φίλτρο για περαιτέρω επεξεργασία. Ελέγχει την αίτηση με ποικίλους τρόπους όπως: αναζητά την αυθεντικότητα του πελάτη ελέγχοντας άλλα φίλτρα για να δει αν η αίτηση επιτρέπεται, ή ελέγχοντας την cache για να δει αν η αίτηση είναι τρέχουσα. Αν η αίτηση είναι τρέχουσα, η εφαρμογή την επιστρέφει στον πελάτη. Αν όχι, η εφαρμογή συνδέεται στο Internet site και ανακτά την αίτηση από τον πελάτη. Η ISAPI εφαρμογή έχει την δυνατότητα να κρατάει μια σύνδεση ενεργή, καθώς ο Proxy Server στέλνει τα δεδομένα στον πελάτη. Αυτό είναι γνωστό σαν keep-alive. Η keep-alive λειτουργία επιταχύνει την ανάκτηση επιπρόσθετων πληροφοριών από την σύνδεση εάν αυτό είναι επιθυμητό. Επειδή οι φυλλομετρητές πρέπει να συνδεθούν στο Internet για να ανακτήσουν πληροφορίες, η λειτουργία keep-alive κρατάει τη γραμμή ανοιχτή για μια περίοδο του χρόνου, σε περίπτωση που ζητηθούν επιπρόσθετες πληροφορίες.

➢ **Caching HTTP και FTP αντικειμένων.** Η υπηρεσία Web Proxy αποθηκεύει αντίγραφα των πηγών του Internet που έχουν ζητηθεί σε μια αφιερωμένη cache. Μεταγενέστερες αιτήσεις για αυτά τα αντικείμενα μπορούν να εξυπηρετηθούν από τον δίσκο του Server, αντί να προωθηθούν στο Internet. Αυτό βελτιώνει την εκτέλεση του φυλλομετρητή του χρήστη, μειώνει τον χρόνο απόκρισης του χρήστη, και ελαχιστοποιεί την κατανάλωση του bandwidth στην σύνδεση του Internet. Επίσης, ο Proxy Server χρησιμοποιεί ενεργό caching. Η υπηρεσία Web Proxy υποστηρίζει δύο είδη caching: το παθητικό caching και το ενεργητικό caching.

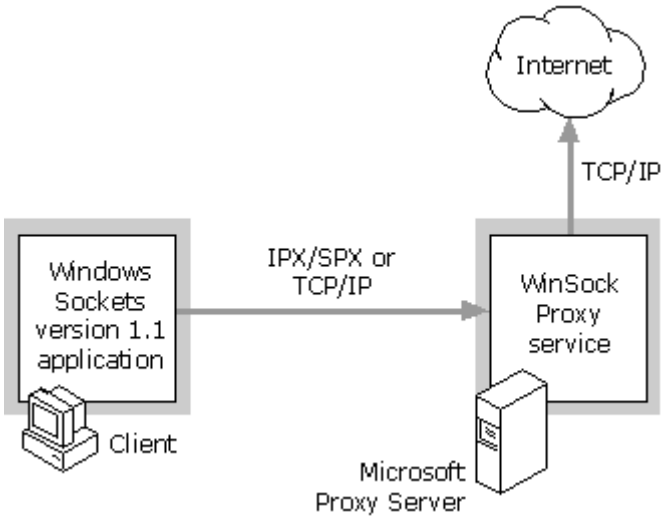
- Το παθητικό caching είναι η βασική μορφή του caching για τον Proxy Server και αυτή που χρησιμοποιούμε πιο συχνά. Ο Proxy Server παρεμβάλλεται ανάμεσα στον χρήστη και το τοπικό, ή απομακρυσμένο Web. Πριν προωθήσει την αίτηση στο Web, ο Proxy Server καλεί πρώτα την cache του για να αποφασίσει αν η cache μπορεί να ικανοποιήσει την

αίτηση, χρησιμοποιώντας το RetrieveUrlFile API. Αν τα δεδομένα είναι στην cache και δεν έχει λήξει το TTL τους, επιστρέφεται αμέσως στον πελάτη το Windows Sockets TransmitFile. Αν δεν υπάρχουν στην cache, ή το αντίγραφο τους στην cache έχει λήξει, ο Proxy Server ανακτά το αντικείμενο από το Web, το επιστρέφει στον χρήστη και το εισάγει στην cache. Αν ο χώρος που κρατείται για την cache στον τοπικό δίσκο είναι γεμάτος και δεν χωράει καινούργια δεδομένα, τα παλιά αντικείμενα απομακρύνονται από την cache με τη χρήση μιας φόρμουλας η οποία αξιολογεί την ηλικία, την δημοτικότητα και το μέγεθος.

- Το ενεργητικό caching προσθέτει λειτουργικότητα στο παθητικό caching. Τυπικά, κατά τη διάρκεια του παθητικού caching, ένα αντικείμενο τοποθετείται στην cache και του δίνεται μία Time-To-Live (TTL) τιμή. Κατά την διάρκεια αυτού του χρόνου, όλες οι αιτήσεις για τα αντικείμενα εξυπηρετούνται από την cache χωρίς να δημιουργούν κίνηση στον Web Server. Μετά την λήξη του TTL, μεταγενέστερες αιτήσεις πελατών για το αντικείμενο δημιουργούν κίνηση από και προς τον Web Server. Η απάντηση από το Server αποθηκεύεται στην cache και υπολογίζεται ένα νέο TTL.

5.2 Υπηρεσία WinSock Proxy

Η υπηρεσία WinSock Proxy κάνει μια εφαρμογή πελάτη η οποία είναι συμβατή με Windows Sockets όπως Telnet, mail, NetShow, RealAudio, ή IRC να εκτελείται σαν να ήταν απευθείας συνδεδεμένη στο Internet. Η εφαρμογή πελάτη κάνει τις Windows Socket API κλήσεις να επικοινωνούν με μια εφαρμογή, η οποία τρέχει σε έναν υπολογιστή βασιζόμενο στο Internet. Τα components του WinSock Proxy ανακατευθύνουν τα απαραίτητα APIs στον Proxy Server υπολογιστή και μ' αυτόν τον τρόπο εγκαθιδρύει ένα μονοπάτι επικοινωνίας από την εσωτερική εφαρμογή στην εφαρμογή Internet μέσω του Proxy Server. Στην Εικόνα 7 φαίνεται το μονοπάτι επικοινωνίας για την υπηρεσία WinSock Proxy.



Εικόνα 7

Το μονοπάτι επικοινωνίας της υπηρεσίας WinSock Proxy

Η υπηρεσία WinSock Proxy παρέχει τα ακόλουθα χαρακτηριστικά:

- Υποστήριξη για TCP/IP και IPX/SPX για το εσωτερικό δίκτυο**.** Η υπηρεσία WinSock Proxy υποστηρίζει την επικοινωνία πάνω από το TCP/IP και IPX/SPX στο εσωτερικό δίκτυο, επιτρέποντας πρόσβαση στα Internet sites από τις Internet εφαρμογές του δικτύου. Ωστόσο, μόνο εφαρμογές οι οποίες έχουν γραφτεί για να χρησιμοποιούν Windows Sockets πάνω από TCP/IP (εφαρμογές του Internet) μπορούν να ανακατευθυνθούν.
- Έλεγχος πρόσβασης εισερχομένων και εξερχόμενων. Ελέγχουμε την πρόσβαση μέσω του port, του πρωτοκόλλου, όπως επίσης και μέσω των χρηστών, ή των ομάδων χρηστών. Κάθε port μπορεί να ενεργοποιηθεί ή να απενεργοποιηθεί για επικοινωνίες μέσω μιας συγκεκριμένης λίστας χρηστών, ή ομάδων χρηστών. Η λίστα των χρηστών η οποία αρχικοποιεί τις εξερχόμενες συνδέσεις σε ένα port, μπορεί να είναι μία λίστα διαφορετική από αυτή των χρηστών οι οποίοι «ακούν» για εισερχόμενες συνδέσεις στο ίδιο port.
- Περιορισμένη (φιλτραρισμένη) πρόσβαση στα Internet Sites. Μπορούμε να περιορίσουμε την πρόσβαση σε απομακρυσμένα Web Sites με το Domain Name, την IP διεύθυνση, και την subnet mask. Μπορούμε να επιτρέψουμε ή να απαγορεύσουμε την πρόσβαση σε όλα τα Web Sites, εκτός από αυτά που

περιέχονται στη λίστα. Οι ρυθμίσεις είναι γενικές και επηρεάζουν όλους τους χρήστες που έχουν πρόσβαση στο Internet μέσω του Proxy Server.

- Εμποδίζεται η πρόσβαση στους υπολογιστές του εσωτερικού δικτύου από εξωτερικούς χρήστες. Η υπηρεσία WinSock Proxy αποτρέπει την δρομολόγηση από το Internet στο εσωτερικό δίκτυο.
- Χρήση μιας IP διεύθυνσης. Όλες οι αιτήσεις στο Internet, γίνονται με την εξωτερική IP διεύθυνση του Proxy Server σαν διεύθυνση πηγή. Αυτό κρύβει τις εσωτερικές διευθύνσεις και επιτρέπει τη χρήση ιδιωτικών διευθύνσεων.
- Ασφάλεια. Η υπηρεσία WinSock Proxy υποστηρίζει SSL και NT πρόκληση/απάντηση, καθώς και ακεραιότητα του δικτύου κρατώντας τους χρήστες του Internet έξω από το LAN.

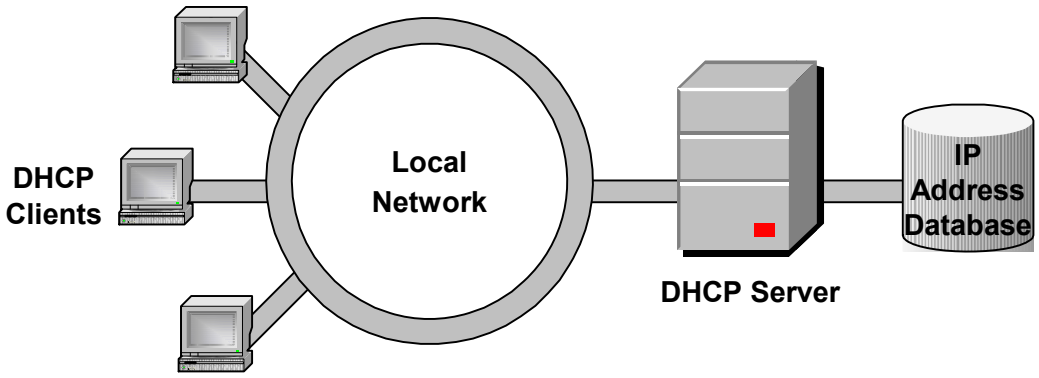
5.3 Υπηρεσία Socks Proxy

Τα SOCKS είναι ένας μηχανισμός πλατφόρμας, ο οποίος εγκαθιδρύει ασφαλείς επικοινωνίες ανάμεσα στους πελάτες και τους Server υπολογιστές. Η υπηρεσία Socks Proxy επιτρέπει στους χρήστες αόρατη πρόσβαση στο Internet μέσω του Proxy Server. Η υπηρεσία Socks Proxy επεκτείνει την ανακατεύθυνση που παρέχεται από την υπηρεσία WinSock Proxy σε μη παραθυρικές πλατφόρμες. Χρησιμοποιεί TCP/IP και μπορεί να χρησιμοποιηθεί για Telnet, FTP, Gopher, και HTTP. Η υπηρεσία Socks Proxy δεν υποστηρίζει εφαρμογές που βασίζονται στο πρωτόκολλο UDP.

Οι πελάτες του Socks Proxy εγκαθιδρύουν μια σύνδεση με τον Proxy Server υπολογιστή και η υπηρεσία Socks Proxy συσχετίζει τις πληροφορίες ανάμεσα στον πελάτη και τον Internet Server.

6 Το πρωτόκολλο DHCP

Το Dynamic Host Configuration Protocol (DHCP) είναι ένα Internet πρωτόκολλο, σχεδιασμένο να αναθέτει και να κατανέμει IP διευθύνσεις δυναμικά, όπως επίσης και TCP/IP πληροφορίες διαχείρισης. Το DHCP χρησιμοποιεί ένα μοντέλο λειτουργίας client/Server (Εικόνα 8), όπου ένας DHCP πελάτης κάνει μια αίτηση σε έναν DHCP Server για μία IP διεύθυνση και άλλες παραμέτρους διαχείρισης. Όταν ο DHCP πελάτης κάνει την αίτηση, ο DHCP Server του αναθέτει μία IP διεύθυνση και ενημερώνει την βάση του, σημειώνοντας ποιος πελάτης έχει την διεύθυνση και τον χρόνο που χρησιμοποιείται η διεύθυνση. Το ποσό αυτό του χρόνου είναι γνωστό ως μίσθωση (lease). Όταν ο χρόνος λήξει, ο DHCP πελάτης πρέπει να ανανεώσει την μίσθωση, ή να διαπραγματευτεί μια καινούργια μίσθωση για διαφορετική IP διεύθυνση. Μέσω της χρήσης της μίσθωσης , ο DHCP Server μπορεί να αξιοποιήσει μη χρησιμοποιούμενες IP διευθύνσεις.



Εικόνα 8
Το μοντέλο client/Server του DHCP

Η χρήση του DHCP επιτρέπει σε έναν διαχειριστή να κάνει αλλαγές στις ρυθμίσεις της IP διεύθυνσης ενός χρήστη, χωρίς να χρειάζεται να επισκέπτεται κάθε πελάτη ξεχωριστά. Ο χρήστης του σταθμού εργασίας χρειάζεται μόνο να απελευθερώνει και να ανανεώνει την DHCP μίσθωση του. Αυτή είναι η δύναμη και το όφελος του DHCP.

6.1 Τι επιτυγχάνουμε με το DHCP

- Το DHCP επιτρέπει στους διαχειριστές να ελέγχουν τις παραμέτρους ρυθμίσεων του δικτύου τους.

- Μπορούμε να διαχειριστούμε τους πελάτες που χρησιμοποιούν το DHCP δυναμικά. Αυτό επιτρέπει προσθήκες και αλλαγές στο δίκτυο, χωρίς να είναι απαραίτητο ο διαχειριστής να αλλάζει τις ρυθμίσεις στον κάθε πελάτη ξεχωριστά.
- Για να έχουμε ανοχή στα λάθη χρησιμοποιούνται πολλαπλοί DHCP Servers σε ένα, ή περισσότερα υποδίκτυα.
- Οι DHCP Servers μέσω των BOOTP πρακτόρων διαβίβασης, μπορούν να εξυπηρετήσουν περισσότερα από ένα υποδίκτυα.
- Το DHCP παρέχει μία δυναμική βάση για την κατανομή IP διευθύνσεων. Αυτές οι IP διευθύνσεις, όταν δεν χρησιμοποιούνται μπορούν να αξιοποιηθούν, μέσω της διάρκειας μίσθωσης.
- Οι πελάτες μπορούν να συνεχίσουν να χρησιμοποιούν μία DHCP κατανεμημένη IP διεύθυνση, ακόμα και μετά την επανεκκίνηση του υπολογιστή.

6.2 Χρησιμοποιώντας το DHCP για την ρύθμιση των IP διευθύνσεων

Με την χρήση του DHCP για την κατανομή και διαχείριση των ρυθμίσεων των IP διευθύνσεων λύνονται τα περισσότερα από τα προβλήματα που σχετίζονται με ένα στατικά διατηρούμενο περιβάλλον. Απλά προβλήματα όπως λάθος IP διεύθυνση, subnet mask, ή default gateway έχουν εξαλειφθεί πλήρως. Αν οι IP διευθύνσεις των DNS ή WINS Servers αλλάξουν, ο διαχειριστής απλά ενημερώνει την DHCP βάση οπότε οι αλλαγές στέλνονται στους DHCP πελάτες με την επόμενη επανεκκίνηση, ή όταν η μίσθωση τους λήξει.

Οι χρήστες με laptops μπορούν να μετακινούνται από μία περιοχή της επιχείρησης σε μία άλλη, ή σε διάφορα μέρη της χώρας. Όταν ο χρήστης συνδέσει το laptop στο δίκτυο, το laptop επικοινωνεί με τον DHCP Server ο οποίος του λέει την σωστή ρύθμιση που πρέπει να χρησιμοποιήσει γι' αυτή την περιοχή. Τη στιγμή που το laptop πάρει την πληροφορία, ο χρήστης μπορεί να ξεκινήσει να χρησιμοποιεί τις πηγές του δικτύου. Το DHCP πραγματοποιεί πολλές από αυτές τις εργασίες με τη χρήση του scope και των μισθώσεων (lease).

Το scope είναι μια συλλογή από παραμέτρους ρυθμίσεων των IP διευθύνσεων που θα χρησιμοποιηθούν από όλους τους DHCP πελάτες σε ένα δοσμένο υποδίκτυο.

Η μίσθωση (lease) είναι μία περίοδος του χρόνου κατά την οποία ο DHCP Server επιτρέπει στον DHCP πελάτη να χρησιμοποιήσει μια IP διεύθυνση.

Η όλη DHCP διαδικασία γίνεται χωρίς να το ξέρει ο χρήστης. Επίσης δεν απαιτεί από έναν διαχειριστή δικτύου να κάνει τις ρυθμίσεις στο μηχάνημα του χρήστη όταν προστίθεται αρχικά στο δίκτυο. Ούτε απαιτεί από τον διαχειριστή να επισκέπτεται και να επαναρυθμίζει τα laptops, όταν οι χρήστες μετακινούνται μέσα στην επιχείρηση. Όλα αυτά μεταφράζονται ως όφελος για την επιχείρηση και τον διαχειριστή του δικτύου.

6.3 Τα μέρη της DHCP επικοινωνίας

Υπάρχουν τρία βασικά μέρη σε μία DHCP επικοινωνία. Το πρώτο μέρος, ο DHCP πελάτης, είναι ένα κομμάτι λογισμικού ενός λειτουργικού συστήματος, το οποίο είναι σχεδιασμένο να ζητάει IP διευθύνσεις και άλλες σχετικές πληροφορίες διαχείρισης. Από τη στιγμή που ανακτά την αιτούμενη πληροφορία, το λογισμικό επαναρυθμίζει το λειτουργικό σύστημα.

Το δεύτερο μέρος, ο DHCP Server, είναι ένα πρόγραμμα που «ακούει» για αιτήσεις από DHCP πελάτες του δικτύου και τους εφοδιάζει με τις πληροφορίες που ζητούν. Ο DHCP Server συντηρείται από έναν διαχειριστή δικτύου, ρυθμίζεται με μία βάση στην οποία είναι αποθηκευμένες οι πληροφορίες διαχείρισης , συμπεριλαμβανομένων των IP διευθύνσεων, subnet masks, default gateways, και οι διευθύνσεις των DNS και WINS Servers. Επίσης, στη βάση σημειώνονται ποιες IP διευθύνσεις χρησιμοποιούνται τη τρέχουσα στιγμή και ποιες MAC διευθύνσεις τις χρησιμοποιούν.

Το τρίτο μέρος είναι ο DHCP relay agent, ο οποίος «ακούει» για DHCP αναμεταδόσεις στα τοπικά του υποδίκτυα. Ο DHCP relay agent είναι ρυθμισμένος με τις IP διευθύνσεις των DHCP Servers. Αν δεχτεί μία DHCP αναμετάδοση από έναν ο DHCP πελάτη, τότε ο DHCP relay agent θα στείλει την αίτηση σαν unicast μήνυμα απευθείας σε έναν DHCP Server.

7 Case Studies

Ο Proxy Server μπορεί να χρησιμοποιηθεί σε διάφορες μορφές δικτύων. Κάποιες από αυτές είναι οι εξής:

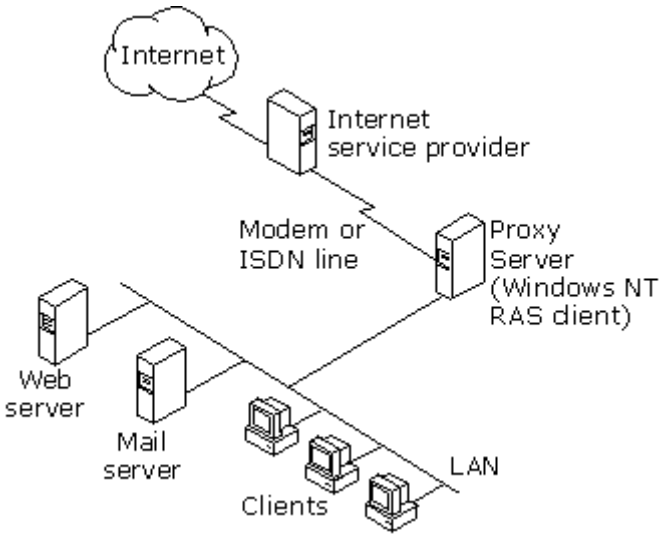
- Δίκτυο μικρού γραφείου
- Δίκτυο μεσαίου μεγέθους γραφείου με ένα υποκατάστημα
- Δίκτυο μεγάλης επιχείρησης

7.1 Δίκτυο μικρού γραφείου

Ένα δίκτυο μικρού γραφείου μπορεί να αποτελείται από τα εξής:

- Ένα τμήμα LAN
- Χρήση του NetBEUI ή του IPX πρωτοκόλλου δικτύου
- Σύνδεση demand-dial σε έναν ISP
- Λιγότερους από 250 πελάτες

Ο Proxy Server χρησιμοποιείται για την παροχή σύνδεσης στο Internet και ασφάλειας του δικτύου, όπως φαίνεται στην Εικόνα 9.



Εικόνα 9
Δίκτυο μικρού γραφείου

Το Auto Dial χρησιμοποιεί μια καταχώρηση τηλεφωνικού καταλόγου RAS για να παρέχει demand-dialing στο Internet, οπότε ο Proxy Server υπολογιστής πρέπει να ρυθμιστεί σαν Windows NT RAS πελάτης.

Ο Proxy Server υπολογιστής αποτελείται από δυο interfaces δικτύου: έναν προσαρμογέα δικτύου για να συνδεθεί στο εσωτερικό δίκτυο, και ένα modem ή προσαρμογέα ISDN για να συνδεθεί στο εξωτερικό δίκτυο (Internet). Ο πίνακας τοπικών διευθύνσεων (LAT) είναι φτιαγμένος για να έχει έναν κατάλογο του χώρου των IP διευθύνσεων του εσωτερικού δικτύου.

Σ' αυτό το σενάριο, ενεργοποιείται και ρυθμίζεται το cashing έτσι ώστε να ελαχιστοποιηθεί η ύπαρξη demand-dialing στο Internet. Χρησιμοποιούμε το cashing για την αποθήκευση ενός τοπικού αντιγράφου των πιο συχνά αιτούμενων URLs σε αφιερωμένους δίσκους. Μπορούμε να χρησιμοποιήσουμε ενεργό cashing για να ανακτήσουμε αυτόματα τα πιο δημοφιλή URLs, χωρίς την πρωτοβουλία του πελάτη.

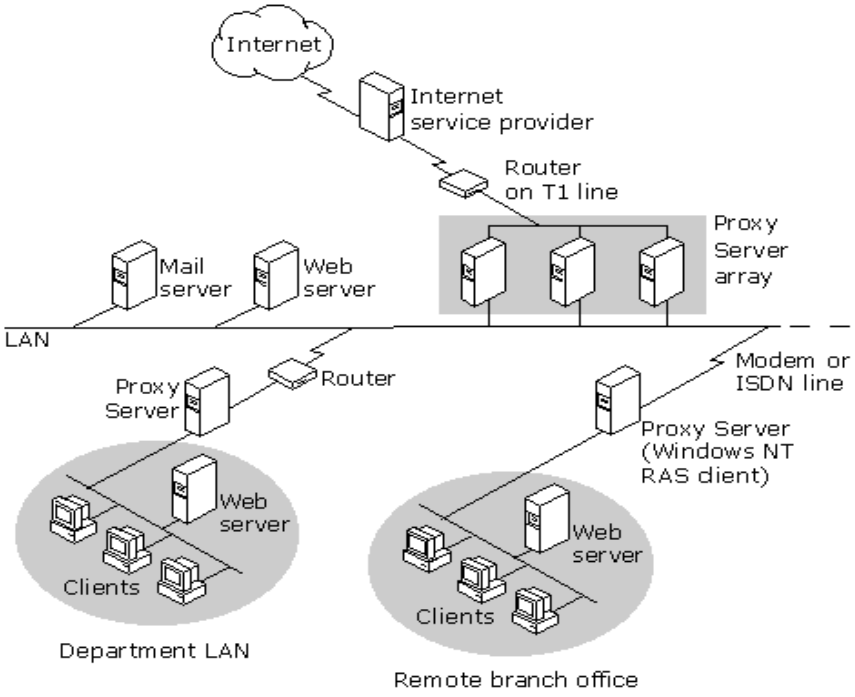
Η πιστοποίηση του password, ο ορισμός των πρωτοκόλλων, το φιλτράρισμα περιοχών, το φιλτράρισμα της cache και το δυναμικό φιλτράρισμα πακέτου χρησιμοποιούνται για να παρέχουν ασφάλεια στο δίκτυο κατά τη διάρκεια της πρόσβασης στο Internet.

7.2 Δίκτυο γραφείου μεσαίου μεγέθους

Το δίκτυο ενός γραφείου μεσαίου μεγέθους μπορεί να χαρακτηριστεί με τα ακόλουθα:

- Ένα κεντρικό γραφείο με πολλά τμήματα LAN
- Ένα γραφείο-παράρτημα με ένα τμήμα LAN
- Χρήση των πρωτοκόλλων δικτύου IP ή IPX
- Σύνδεση demand-dial από το γραφείο-παράρτημα στο κεντρικό γραφείο
- Σύνδεση demand-dial ή σύνδεση αφιερωμένης γραμμής από το κεντρικό γραφείο στον ISP
- Λιγότερους από 2000 πελάτες

Γι' αυτό το σενάριο, χρησιμοποιείται ένας Proxy Server υπολογιστής στο παράρτημα-γραφείο για να παρέχει τοπικό caching, τοπική διαχείριση του ελέγχου πρόσβασης και σύνδεση με το κεντρικό γραφείο. Στο κεντρικό γραφείο, πολλοί Proxy Server υπολογιστές συνδέονται σε έναν πίνακα για να παρέχουν μια καθολική πολιτική ασφάλειας για όλους τους πελάτες, όπως επίσης και κατανεμημένο caching και αφιερωμένη σύνδεση στο Internet, όπως φαίνεται στην Εικόνα 10.



Εικόνα 10
Σενάριο δικτύου γραφείου μεσαίου μεγέθους

- **Το δίκτυο του γραφείου-παραρτήματος**

Η επιλογή Auto Dial του Proxy Server χρησιμοποιείται για να παρέχει demand-dialing στο κεντρικό γραφείο, μέσω του πίνακα του Proxy Server και μετά έξω στο Internet. Το Auto Dial χρησιμοποιεί μια καταχώρηση τηλεφωνικού καταλόγου RAS για να παρέχει demand-dialing, οπότε ο Proxy Server υπολογιστής στο γραφείο-παράρτημα πρέπει να ρυθμιστεί σαν Windows NT RAS πελάτης. Ένας ξεχωριστός RAS Server χρησιμοποιείται στο κεντρικό γραφείο για να χειρίζεται τις εισερχόμενες αιτήσεις από το γραφείο-παράρτημα.

Ο Proxy Server υπολογιστής αποτελείται από δυο εσωτερικά interfaces δικτύου: έναν προσαρμογέα δικτύου για να συνδέεται στο τοπικό δίκτυο του γραφείου-παραρτήματος και ένα modem ή προσαρμογέα ISDN για να συνδέεται στο απομακρυσμένο δίκτυο του κεντρικού γραφείου. Ο πίνακας τοπικών διευθύνσεων (LAT) είναι φτιαγμένος για να έχει έναν κατάλογο του χώρου των IP διευθύνσεων ολόκληρου του δικτύου. Κάθε εξωτερική (Internet) IP διεύθυνση πρέπει να εξαιρεθεί. Servers ονομάτων, όπως DNS, WINS, ή DHCP, πρέπει να εγκατασταθούν στο γραφείο-παράρτημα για να ενεργοποιηθεί η τοπική ανάλυση ονομάτων. Ο Server

ονόματος του γραφείου-παρακλαδιού πρέπει τότε να ανταποκρίνεται με τους Servers ονομάτων του κεντρικού γραφείου.

Σ' αυτό το σενάριο, ενεργοποιείται και ρυθμίζεται το cashing έτσι ώστε να ελαχιστοποιηθεί η ύπαρξη demand-dialing στο κεντρικό γραφείο, επομένως μειώνονται οι τηλεφωνικές χρεώσεις μεγάλων αποστάσεων. Χρησιμοποιούμε το cashing για την αποθήκευση ενός τοπικού αντιγράφου των πιο συχνά αιτούμενων URLs σε αφιερωμένους δίσκους. Δεν πρέπει να χρησιμοποιούμε το ενεργό cashing, διότι υπάρχει στον πίνακα του Proxy Server στο κεντρικό γραφείο.

Η πιστοποίηση του password, ο ορισμός των πρωτοκόλλων, το φιλτράρισμα περιοχών, το φιλτράρισμα της cache και το δυναμικό φιλτράρισμα πακέτου χρησιμοποιούνται για να παρέχουν ασφάλεια στο δίκτυο κατά τη διάρκεια της πρόσβασης στο Internet.

Επειδή ο Proxy Server υπολογιστής του γραφείου-παραρτήματος δεν έχει εξωτερικό interface, είναι απενεργοποιημένο το φιλτράρισμα πακέτου. Η διαχείριση του Server είναι απλή—μια καθολική πολιτική ασφάλειας μπορεί να ρυθμιστεί στο κεντρικό γραφείο, με την τοπική διαχείριση του ελέγχου πρόσβασης στο γραφείο παράρτημα. Ο Proxy Server του γραφείου-παραρτήματος δε συνδέεται στο Internet. Όλες οι αιτήσεις των πελατών δρομολογούνται στον πίνακα του Proxy Server στο κεντρικό γραφείο.

- **Το δίκτυο του κεντρικού γραφείου**

Το κεντρικό γραφείο χρησιμοποιεί έναν πίνακα από Proxy Servers για να παρέχει κατανεμημένο caching, ισορρόπηση του φόρτου εργασίας και ανοχή λαθών. Κάθε μέλος του πίνακα είναι ρυθμισμένο με δυο interfaces δικτύου: έναν προσαρμογέα δικτύου για να συνδεθεί στο εσωτερικό δίκτυο, και ένα προσαρμογέα δικτύου για να συνδεθεί στο εξωτερικό δίκτυο (Internet).

Γι' αυτό το σενάριο, μπορούμε να θεωρήσουμε ότι η άμεση σύνδεση στον ISP γίνεται μέσω ενός router και μιας γραμμής T1/E1, και σε περίπτωση αποτυχίας θα υπάρχει μια backup dial-up γραμμή. Κάθε πίνακας τοπικών διευθύνσεων (LAT) είναι φτιαγμένος πανομοιότυπα για να έχει έναν κατάλογο του χώρου των IP διευθύνσεων ολόκληρου του δικτύου—και για το δίκτυο του γραφείου παραρτήματος και για του κεντρικού γραφείου. Η IP διεύθυνση του εξωτερικού interface πρέπει να εξαιρεθεί από κάθε υπολογιστή.

Σ' αυτό το σενάριο, ο RAS Server χρησιμοποιείται για να χειρίζεται τις εισερχόμενες αιτήσεις από τον Proxy Server υπολογιστή του γραφείου-παραρτήματος (RAS πελάτης). Ο RAS Server εγκαθίσταται σε έναν ξεχωριστό υπολογιστή από αυτούς που χρησιμοποιούνται για να τρέχουν τον Proxy Server.

Σ' αυτό το σημείο, όλες οι Internet αιτήσεις, ανεξάρτητα από το αν προέρχονται από το τοπικό ή από το γραφείο-παράρτημα, διαχειρίζονται από τον πίνακα του Proxy Server. Για Web Proxy πελάτες, οι αιτήσεις δρομολογούνται εσωτερικά μέσα στον πίνακα και εξυπηρετούνται από το κατάλληλο μέλος του πίνακα ο οποίος κρατάει ένα cached αντίγραφο του URL στο δικό του cache οδηγό. Αν η αίτηση δεν μπορεί να εξυπηρετηθεί από τον πίνακα, τότε προωθείται στο Internet. Μ' αυτό τον τρόπο, οι πίνακες σχηματίζουν μια μεγάλη κατανεμημένη cache, η οποία μπορεί να βελτιώσει την επίδοση του πελάτη. Μπορούμε να χρησιμοποιήσουμε ενεργό caching για να ανακτήσουμε αυτόματα τα πιο δημοφιλή URLs, χωρίς την πρωτοβουλία του χρήστη. Επιπρόσθετα, κρίσιμο εύρος ζώνης διαφυλάσσεται για τη WAN σύνδεση.

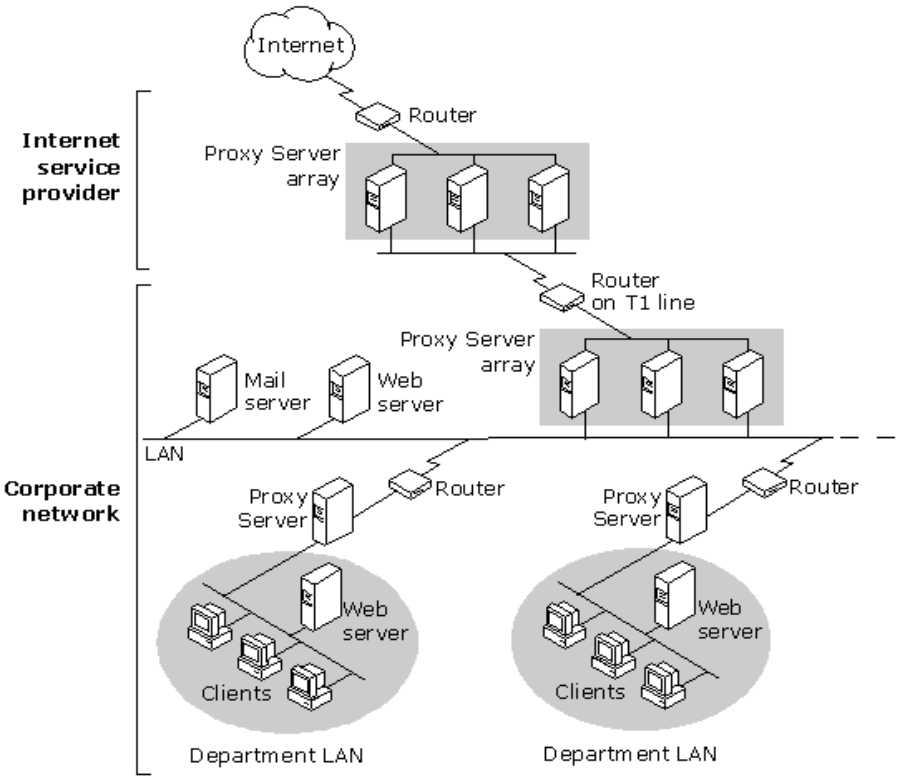
Μια καθολική πολιτική ασφάλειας ρυθμίζεται στο κεντρικό γραφείο για ολόκληρο τον οργανισμό. Μπορούμε να χρησιμοποιήσουμε πιστοποίηση του password, ορισμό των πρωτοκόλλων, φιλτράρισμα περιοχών, φιλτράρισμα της cache και στατικό (χειρωνακτικό) φιλτράρισμα πακέτου για να παρέχουμε maximum ασφάλεια στο δίκτυο. Η διαχείριση του Server είναι απλή—μπορούμε να ρυθμίζουμε ένα μέλος πίνακα και αυτόματα να μεταδίδονται οι αλλαγές σε όλους τους άλλους Proxy Server υπολογιστές του πίνακα.

7.3 Δίκτυο μεγάλης επιχείρησης

Το δίκτυο μιας μεγάλης επιχείρησης μπορεί να χαρακτηριστεί με τα ακόλουθα:

- Ένα κεντρικό γραφείο με πολλά LAN τμήματα και ένα backbone LAN
- Πολλά γραφεία-παραρτήματα, καθένα με ένα μοναδικό LAN τμήμα
- Χρήση των πρωτοκόλλων IP και IPX
- Σύνδεση demand-dial από τα γραφεία-παραρτήματα με το κεντρικό γραφείο
- Σύνδεση με αφιερωμένη γραμμή σε έναν ISP
- Πάνω από 2000 πελάτες

Γι' αυτό το σενάριο, χρησιμοποιείται ένας Proxy Server υπολογιστής για να εξυπηρετεί το LAN κάθε τμήματος, και ένας πίνακας από Proxy Servers στο κεντρικό LAN, όπως φαίνεται στην Εικόνα 11.



Εικόνα 11
Σενάριο δικτύου μεγάλης επιχείρησης

Για τα δίκτυα των γραφείων-παραρτημάτων, μπορούμε να χρησιμοποιήσουμε τις ίδιες ρυθμίσεις με αυτές του δικτύου του γραφείου μεσαίου μεγέθους. Συνοπτικά, οι Proxy Server υπολογιστές του γραφείου-παραρτήματος εξυπηρετούν τους τοπικούς πελάτες και χρησιμοποιούν το Auto Dial για demand-dialing σε ένα RAS Server στα συνεταιρικά κεντρικά γραφεία. Όλες οι αιτήσεις Internet που δε μπορούν να εξυπηρετηθούν από την τοπική cache, προωθούνται στον συνεταιρικό πίνακα από Proxy Servers. Η διαχείριση του Server είναι απλή—καθολικές πολιτικές μπορούν να ρυθμιστούν στο κεντρικό γραφείο.

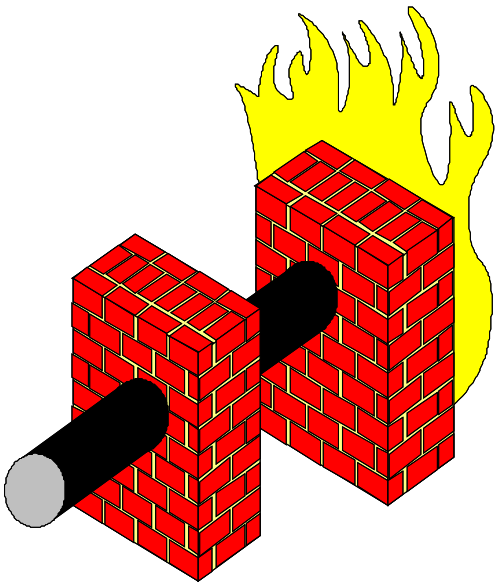
Οι τμηματικοί Proxy Servers στα κεντρικά γραφεία έχουν εγκατασταθεί όμοια με αυτούς του Proxy Server του γραφείου-παραρτήματος, με μια σημαντική διάκριση—σύνδεση στο δίκτυο. Οι τμηματικοί Proxy Server υπολογιστές έχουν ο καθένας από δυο εσωτερικούς προσαρμογείς δικτύου: ένα για να συνδέεται στο τμηματικό τους LAN, και έναν για να συνδέεται στο backbone LAN. Κάθε τμήμα έχει το δικό του Proxy Server για να παρέχει caching. Οι αιτήσεις των Web Proxy

πελατών που δε μπορούν να εξυπηρετηθούν, δρομολογούνται upstream στον πίνακα από Proxy Servers.

Ο πίνακας από Proxy Servers στο backbone LAN, είναι *dual-homed*: κάθε μέλος του πίνακα έχει έναν εσωτερικό και έναν εξωτερικό προσαρμογέα δικτύου για τη σύνδεση του στο Internet.

Ο ISP μπορεί να χρησιμοποιήσει μεγάλους πίνακες από Proxy Servers για να εξυπηρετεί τις ανάγκες της κοινωνίας των επιχειρήσεων. Χρησιμοποιώντας τον Proxy Server μ' αυτό τον τρόπο επιτυγχάνουμε μεγάλη κλιμάκωση, ισορρόπηση του φόρτου εργασίας και ανοχή λαθών. Οι αιτήσεις των πελατών οι οποίες δε μπορούν να εξυπηρετηθούν από τον συνεταιρικό Proxy Server πίνακα, δρομολογούνται στον Proxy Server πίνακα του ISP. Ο ISP μπορεί να αποθηκεύει στην cache μεγάλα ποσά πληροφοριών, με αποτέλεσμα να αυξάνει την επίδοση του πελάτη και να διατηρεί το εύρος ζώνης του ISP στο Internet backbone.

Μέρος Τρίτο



Firewalls

1 Firewalls

7.4 Τι είναι τα Firewalls

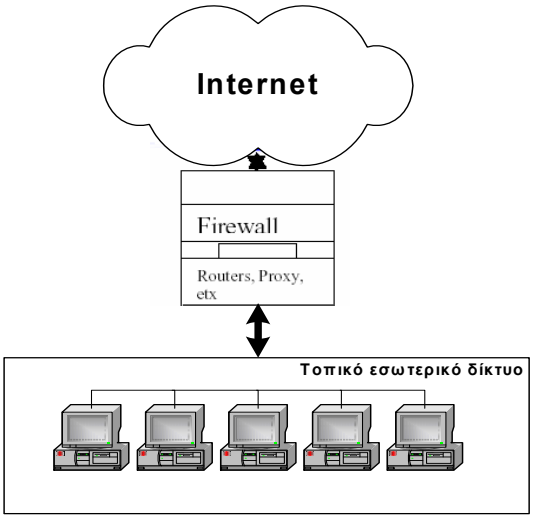
Ο όρος firewall δεν αναφέρεται σε κάποιο συγκεκριμένο κομμάτι υλικού ή λογισμικού. Το firewall είναι απλά η γενική ονομασία για υλικό, λογισμικό, ή συχνά για συνδυασμό αυτών των δύο, που χρησιμεύει για την προστασία του εσωτερικού δικτύου από εισβολείς.

Τα firewalls είναι συσκευές και συστήματα προσεκτικά ολοκληρωμένα για να ελέγχουν τη ροή της πληροφορίας ανάμεσα σε δύο δίκτυα. Τα firewalls μπορεί να είναι τόσο απλά όσο ένας router ρυθμισμένος για φιλτράρισμα των IP σε ένα τοπικό υπολογιστή, ή ακόμη πιο πολύπλοκες συσκευές από συνδυασμούς πολλών συστημάτων για την ανάλυση όλων των πακέτων που περνούν μέσα και έξω από ένα τοπικό δίκτυο και εκτέλεση στατιστικών και συνδυαστικών αναλύσεων σ' αυτά.

Ένα τυπικό firewall μπορεί να περιέχει ένα, ή περισσότερα από τα παρακάτω συστατικά:

- Ένα router φιλτραρίσματος πακέτων
- Μία πύλη εξόδου επιπέδου εφαρμογής (ή Proxy Server)
- Μία πύλη εξόδου επιπέδου κυκλώματος

Η Εικόνα 12 δείχνει πως μπορούν να δουλέψουν μαζί αυτές οι συσκευές για να επιτύχουν ένα κοινό στόχο προστασίας του δικτύου από εισβολή μη εξουσιοδοτημένου χρήστη.



Εικόνα 12
Παράδειγμα χρήσης Firewall

Το Firewall βελτιώνει αισθητά την ασφάλεια του δικτύου και μειώνει τον κίνδυνο που διατρέχουν οι Servers του δικτύου, φιλτράροντας υπηρεσίες που δεν είναι ασφαλείς. Σαν αποτέλεσμα, το δίκτυο εκτίθεται σε λιγότερους κινδύνους, επειδή μόνο επιλεγμένα πρωτόκολλα περνούν μέσα από αυτό. Για παράδειγμα, ένα firewall μπορεί ν' απαγορεύσει συγκεκριμένες ευαίσθητες περιοχές όπως το NFS να μπαίνουν και να βγαίνουν από ένα προστατευμένο δίκτυο. Μ' αυτόν τον τρόπο, αποφεύγεται η εκμετάλλευση κάποιων υπηρεσιών από εξωτερικούς εισβολείς.

Τα firewalls επίσης, παρέχουν προστασία από routing-based επιθέσεις, όπως η δρομολόγηση πηγής και προσπάθειες ανακατεύθυνσης μονοπατιών δρομολόγησης σε άλλα sites μέσω του ICMP. Μπορούν ν' απορρίψουν όλα τα source-routed πακέτα και τις ICMP ανακατευθύνσεις και έπειτα να πληροφορήσουν το διαχειριστή.

7.5 Χαρακτηριστικά των Firewalls

Τα Firewalls πρέπει να χαρακτηρίζονται από τα εξής :

- Εγγύηση ασφάλειας: Βεβαίωση ότι η τεχνολογία του firewall πλήρη τις προδιαγραφές και ότι είναι εγκατεστημένη σωστά. Να είναι πιστοποιημένο από την διεθνή οργάνωση ασφάλειας υπολογιστών.
- Έλεγχος προνομίων: Ο βαθμός που επιβάλλει το firewall περιορισμό πρόσβασης στον χρήστη.
- Πιστοποίηση: Τι είδους έλεγχο πρόσβασης παρέχει. Υποστηρίζει πιστοποιήσεις; Τεχνικές πιστοποιήσεις; Αυτές οι τεχνικές περιλαμβάνουν χαρακτηριστικά ασφαλείας όπως πιστοποίηση της διεύθυνσης πηγής / προορισμού του υπολογιστή του δικτύου, πιστοποίηση κωδικού, καρτών ελέγχου πρόσβασης, και συσκευών αναγνώρισης αποτυπωμάτων.
- Ικανότητες ελέγχου: Η ικανότητα να παρακολουθεί την κίνηση του δικτύου, συμπεριλαμβανομένων των προσπαθειών πρόσβασης, δημιουργίας log files, και παροχής αναφορών με στατιστικά και alarms.
- Ευελιξία: Το firewall πρέπει να είναι αρκετά ανοιχτό για να διευκολύνει την πολιτική ασφάλειας της εταιρίας, καθώς θα πρέπει να γίνονται αλλαγές στα χαρακτηριστικά της. Η πολιτική ασφάλειας πρέπει να αλλάζει πολύ σπάνια, αλλά η διαδικασίες ασφάλειας πρέπει να επαληθεύονται πάντα.

- Απόδοση: Το firewall πρέπει να είναι αρκετά γρήγορο έτσι ώστε να μην καταλαβαίνουν οι χρήστες τον έλεγχο των πακέτων.
- Κλιμάκωση: Το προϊόν πρέπει να είναι ικανό να προσαρμόζεται σε multi-platforms και σε διάφορα περιστατικά μέσα στο προστατευμένο δίκτυο. Αυτό περιλαμβάνει λειτουργικά συστήματα, μηχανήματα, και ρυθμίσεις ασφάλειας.
- Ευκολία στη χρήση: Το firewall πρέπει να έχει γραφικό περιβάλλον (GUI) το οποίο διευκολύνει την δουλεία του διαχειριστή όταν το εγκαθιστά, το ρυθμίζει ή το διαχειρίζεται.
- Διαφάνεια: Αν υιοθετηθεί ένα πολύπλοκο σύστημα, οι χρήστες θ' αντισταθούν σ' αυτό και τελικά δεν θα το χρησιμοποιήσουν. Αντιθέτως, όσο περισσότερο διαφανές είναι το firewall στους χρήστες, τόσο πιο πιθανό είναι να υποστηρίζουν τον διαχειριστή και να το χρησιμοποιούν κατάλληλα.
- Ένα firewall θα πρέπει να έχει τεχνικές φιλτραρίσματος που θα επιτρέπουν ή όχι υπηρεσίες σε συγκεκριμένα συστήματα Server.
- Ένα firewall θα πρέπει να χρησιμοποιεί Proxy για υπηρεσίες όπως FTP και TELNET έτσι ώστε να μπορούν να απασχολούνται και να συγκεντρώνονται τα αυξημένα μέτρα πιστοποίησης στο firewall. Αν απαιτούνται υπηρεσίες όπως το NNTP, HTTP, ή GOPHER, το firewall θα πρέπει να περιέχει τις αντίστοιχες υπηρεσίες Proxy.
- Ένα firewall θα πρέπει να διευθετεί τη δημόσια πρόσβαση στο site, έτσι ώστε οι δημόσιοι Servers πληροφοριών να είναι προστατευμένοι από το firewall, αλλά να μπορεί να διαχωριστεί από συστήματα των site που δεν απαιτούν δημόσια πρόσβαση.
- Ένα firewall θα πρέπει να έχει την ικανότητα να συγκεντρώνει και να φιλτράρει την dial-in πρόσβαση.

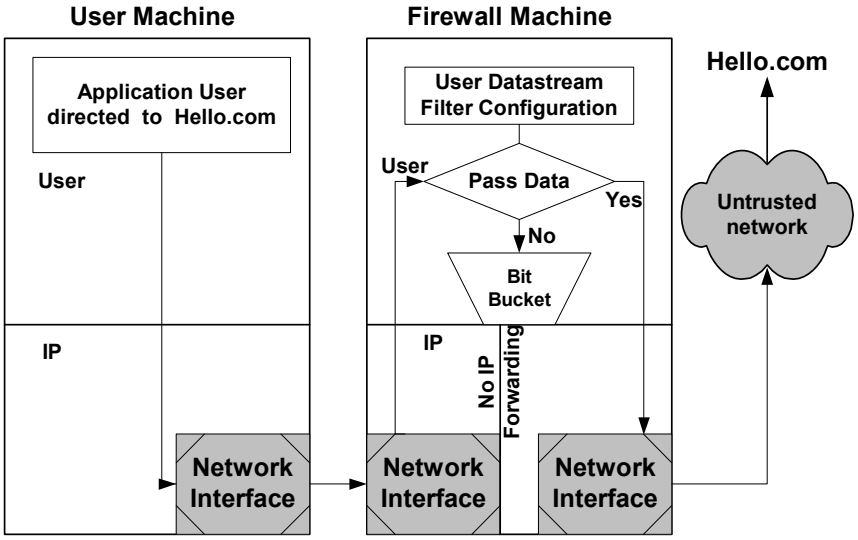
7.6 Κατηγορίες των Firewall

Τα firewalls ανάλογα με την τεχνολογία τους κατατάσσονται σε τέσσερις κατηγορίες :

- **Firewalls φιλτραρίσματος πακέτων.**

  Αυτός ο τύπος firewall όπως φαίνεται στην Εικόνα 13, παρέχει έλεγχο πρόσβασης στο στρώμα IP και είτε δέχεται, απορρίπτει, ή «ρίχνει» πακέτα που είναι βασισμένα κυρίως στην πηγή, τη διεύθυνση του δικτύου

προορισμού και στον τύπο των εφαρμογών. Τα firewalls φιλτραρίσματος πακέτου παρέχουν ένα απλό επίπεδο ασφάλειας σε σχετικά χαμηλή τιμή. Αυτός ο τύπος των firewall επίσης παρέχει υψηλό επίπεδο απόδοσης και είναι διαφανής στους χρήστες .



Εικόνα 13
Firewall φιλτραρίσματος πακέτων

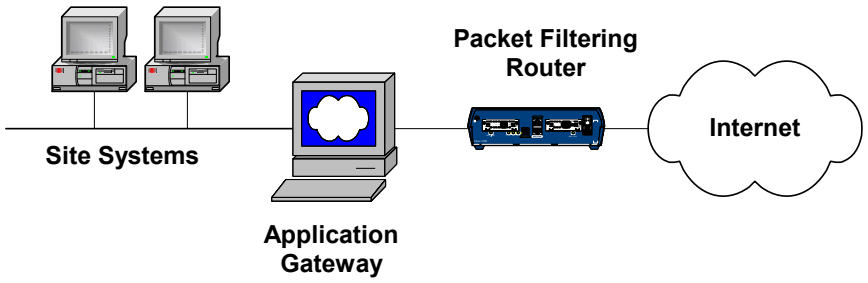
Αδυναμίες των firewalls φιλτραρίσματος πακέτων :

- Είναι ευαίσθητα σε επιθέσεις που στοχεύουν σε πρωτόκολλα υψηλότερα από το πρωτόκολλο επιπέδου δικτύου, το οποίο είναι το μοναδικό επίπεδο που καταλαβαίνουνε.
- Επειδή το πρωτόκολλο επιπέδου δικτύου απαιτεί συγκεκριμένες γνώσεις στις τεχνικές λεπτομέρειες τις οποίες δεν έχει κάθε διαχειριστής δικτύου, τα firewalls αυτά είναι συνήθως πιο δύσκολο να ρυθμιστούν και να επαληθευθούν, πράγμα το οποίο αυξάνει τον κίνδυνο για security holes και αποτυχίες.
- Δεν μπορούν να κρύψουν την τοπολογία του ιδιωτικού δικτύου, επομένως εκθέτουν το δίκτυο στον εξωτερικό κόσμο.
- Έχουν πολύ περιορισμένες δυνατότητες ελέγχου και όπως είναι γνωστό ο έλεγχος παίζει πολύ σημαντικό ρόλο στην πολιτική ασφάλειας της επιχείρησης.
- Δεν υποστηρίζονται όλες οι Internet εφαρμογές.

- Δεν υποστηρίζουν πάντα κάποιους από τους όρους της πολιτικής ασφάλειας, όπως πιστοποίηση σε επίπεδο χρήστη και έλεγχο πρόσβασης σε συγκεκριμένο ωράριο.

➢ **Firewalls επιπέδου εφαρμογής**

Τα firewalls αυτά παρέχουν έλεγχο πρόσβασης στο στρώμα εφαρμογής επιπέδου. Έτσι, συμπεριφέρονται ως gateway επιπέδου εφαρμογής ανάμεσα σε δύο δίκτυα. Επειδή τα firewalls αυτά λειτουργούν στο στρώμα εφαρμογής, έχουν την δυνατότητα να εξετάζουν λεπτομερώς την κίνηση. Αυτό τα κάνει πιο ασφαλή από τα firewalls φιλτραρίσματος πακέτων. Επίσης, αυτό το είδος των firewall είναι πιο αργό από τα firewalls φιλτραρίσματος πακέτων λόγω του λεπτομερούς ελέγχου της κίνησης. Γι' αυτό το λόγο είναι σε κάποιο βαθμό επιρρεπή στις εισβολές, περιοριστικά και συνήθως απαιτούν από τους χρήστες είτε να αλλάζουν την συμπεριφορά τους, ή να χρησιμοποιούν εξειδικευμένο λογισμικό έτσι ώστε να επιτυγχάνουν τους στόχους της πολιτικής. Επομένως, τα firewalls επιπέδου εφαρμογής δεν είναι διαφανή στους χρήστες. Η Εικόνα 14, δείχνει το διάγραμμα ενός τυπικού firewall επιπέδου εφαρμογής.



Εικόνα 14
Firewall επιπέδου εφαρμογής

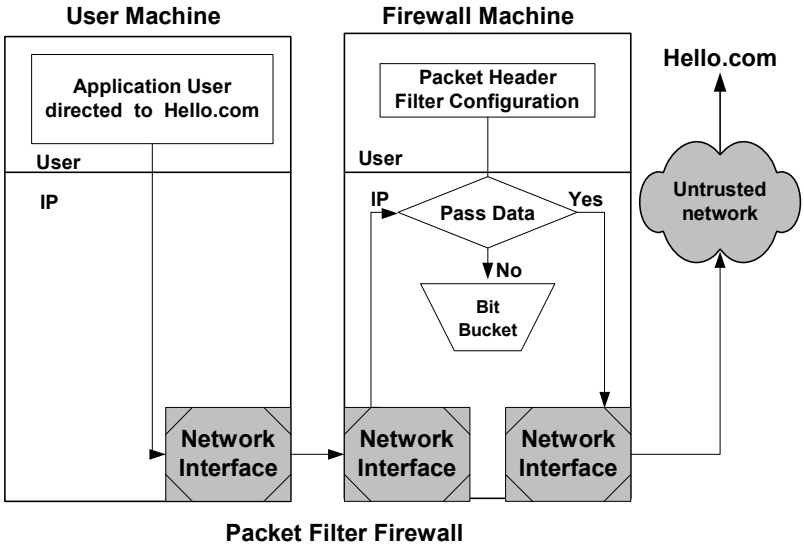
Πλεονεκτήματα χρήσης των firewalls επιπέδου εφαρμογής :

- Επειδή καταλαβαίνουν το πρωτόκολλο επιπέδου εφαρμογής, μπορούν να αντιταθούν σ' όλες τις επιθέσεις.
- Είναι πιο εύκολα στη ρύθμιση από τα firewalls φιλτραρίσματος πακέτων, αφού δεν απαιτείται να γνωρίζουμε όλες τις λεπτομέρειες των πρωτοκόλλων των κατώτερων επιπέδων.

- Μπορούν να κρύψουν την τοπολογία του ιδιωτικού δικτύου.
- Έχουν πλήρη εργαλεία ελέγχου για παρακολούθηση της κίνησης των πακέτων και διαχείριση των log files τα οποία περιέχουν πληροφορίες όπως πηγή, διεύθυνση δικτύου προορισμού, τύπο εφαρμογής, κωδικό χρήστη, χρόνο αρχής και τέλους πρόσβασης και το μέγεθος των bytes που μεταφέρθηκαν.
- Μπορούν να υποστηρίξουν περισσότερες πολιτικές ασφάλειας συμπεριλαμβανομένης της πιστοποίησης σε επίπεδο χρήστη και έλεγχο πρόσβασης σε συγκεκριμένο ωράριο.

- **Υβριδικά firewalls**

Για την αντιμετώπιση των αδυναμιών που παρουσιάζουν τα firewalls φιλτραρίσματος πακέτου και επιπέδου εφαρμογής, δημιουργήθηκαν τα υβριδικά firewalls, τα οποία συνδυάζουν τις τεχνικές των δυο προηγούμενων firewalls όπως φαίνεται στην Εικόνα 15.



Εικόνα 15
Υβριδικό firewall

Αδυναμία των υβριδικών firewalls :

- Επειδή βασίζονται στους μηχανισμούς φιλτραρίσματος πακέτων για την υποστήριξη συγκεκριμένων εφαρμογών έχουν τις ίδιες αδυναμίες στην ασφάλεια.

- **Firewalls επιπέδου εφαρμογής δεύτερης γενιάς**

  Αυτό το firewall λύνει το πρόβλημα της διαφάνειας της προηγούμενης έκδοσης χωρίς να διακινδυνεύεται η απόδοση.

Πλεονεκτήματα των firewalls επιπέδου εφαρμογής δεύτερης γενιάς:

- Μπορούν να χρησιμοποιηθούν σαν intranet firewalls λόγω της διαφάνειας τους και της υψηλότερης απόδοσης τους.
- Παρέχουν πλήρη μετάφραση διεύθυνσης δικτύου εκτός από την απόκρυψη της τοπολογίας του δικτύου.
- Υποστηρίζουν πιο εξελιγμένους μηχανισμούς πιστοποίησης σε επίπεδο χρήστη.

7.7 Σκοποί των firewalls

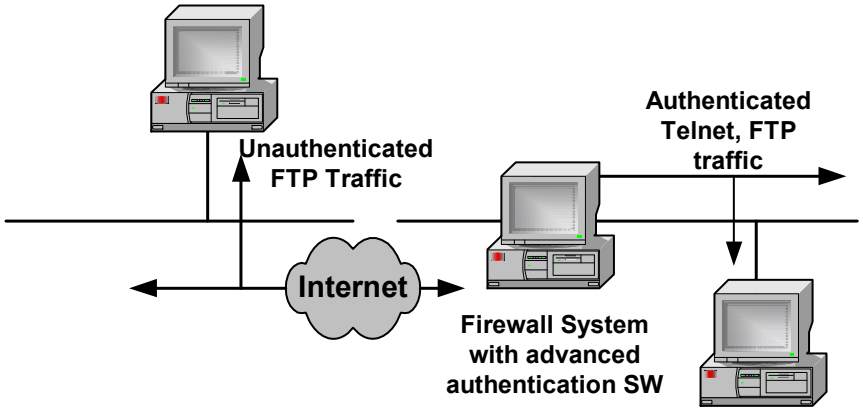
Τα firewalls έχουν σχεδιαστεί έτσι ώστε να κρατούν μακριά την ανεπιθύμητη και μη εξουσιοδοτημένη κίνηση που υπάρχει σε ένα απροστάτευτο δίκτυο όπως το Internet, από ένα ιδιωτικό δίκτυο LAN ή WAN, παρόλο που κάποιοι χρήστες του εσωτερικού δικτύου έχουν πρόσβαση στο Internet. Η Εικόνα 16 δείχνει τον σκοπό του firewall.

Εικόνα 16
Σκοπός του Firewall

Τα περισσότερα firewalls είναι routers οι οποίοι φιλτράρουν εισερχόμενα datagrams βασισμένοι στην διεύθυνση πηγής του datagram, τη διεύθυνση προορισμού, πρωτόκολλα υψηλότερου επιπέδου, ή σε άλλα κριτήρια που καθορίζονται από τον διαχειριστή ασφάλειας του ιδιωτικού δικτύου ή την πολιτική ασφάλειας του δικτύου.

Τα πιο σοφιστικέ firewalls χρησιμοποιούν ένα Proxy Server ο οποίος ονομάζεται και bastion host, όπως φαίνεται στην Εικόνα 17. Ο bastion host

απαγορεύει στους εσωτερικούς χρήστες την άμεση πρόσβαση στο Internet, σαν να είναι ο Proxy τους, ενώ φιλτράρει μη εξουσιοδοτημένη εισερχόμενη Internet κίνηση.



Εικόνα 17
Firewall με χρήση bastion host

Ο σκοπός του firewall ως πύλη ασφαλείας, είναι να παρέχει ασφάλεια σε όλα τα συστατικά που βρίσκονται πίσω από την πύλη, όπως και να ελέγχει ποιος ή τι επιτρέπεται να εισέλθει στο προστατευόμενο περιβάλλον και ποιος ή τι επιτρέπεται να βγει έξω. Είναι σαν ένας φύλακας ασφάλειας που ελέγχει και πιστοποιεί ποιος μπορεί ή δεν μπορεί να έχει πρόσβαση σ' αυτό το site.

Είναι εγκατεστημένο να παρέχει ελεγχόμενο φιλτράρισμα στην κίνηση του δικτύου, επιτρέποντας περιορισμένη πρόσβαση σε συγκεκριμένα Internet ports μπλοκάροντας σχεδόν όλα τα άλλα. Για να γίνει αυτό, πρέπει να λειτουργούν σαν μοναδικό σημείο εισόδου. Αυτός είναι ο λόγος που πολλές φορές τα firewalls ολοκληρώνονται με τους routers.

Με τα firewalls μπορούμε να προστατεύσουμε το site μας από αυθαίρετες συνδέσεις και να εγκαταστήσουμε εργαλεία ανίχνευσης, τα οποία μπορούν να μας ενημερώσουν σχετικά με την προέλευση των συνδέσεων, το μέγεθος της κίνησης που εξυπηρετεί ο χρήστης και αν δέχτηκε επίθεση παραβίασης από κάποιον εισβολέα.

Ένας βασικός σκοπός του firewall είναι να προστατεύει το site από hackers. Δεν μπορεί όμως να το προστατεύσει από συνδέσεις που το διαπερνάνε. Επομένως πρέπει να προσέχουμε τις πίσω πόρτες όπως τη σύνδεση των modems στο LAN, ειδικά αν ο Remote Access Server(RAS) είναι μέσα στο LAN.

Το φιλτράρισμα των πακέτων ήταν πάντα ένας εύκολος και αποδοτικός τρόπος για να φιλτράρονται τα εισερχόμενα ανεπιθύμητα πακέτα πληροφοριών. Αυτό

γίνεται διασπώντας τα πακέτα δεδομένων, διαβάζοντας τα, και απορρίπτοντας αυτά που δεν συμφωνούν με τα κριτήρια που προγραμματίστηκαν στον router. Δυστυχώς, το φιλτράρισμα πακέτων δεν είναι αρκετό για να εγγυηθεί την ασφάλεια ενός site. Υπάρχουν πολλές απειλές και πολλά νέα πρωτόκολλα που μπορούν να διαπεράσουν τα φίλτρα με μικρή προσπάθεια.

Για παράδειγμα, το φιλτράρισμα πακέτων δεν είναι αποδοτικό στο FTP πρωτόκολλο, επειδή το FTP επιτρέπει στον εξωτερικό Server με τον οποίο είναι συνδεδεμένος να κάνει συνδέσεις πίσω στο port 20 για να ολοκληρώσει την μεταφορά των δεδομένων. Ακόμη και αν προσθέταμε έναν επιπλέον κανόνα στον router, το port 20 στα μηχανήματα του εσωτερικού δικτύου θα ήταν προσιτό από έξω. Παρόλα αυτά, οι hackers μπορούν εύκολα να κάνουν ‘spoofing’ στους routers. Τα firewalls κάνουν αυτές ενέργειες δυσκολότερες, αν όχι σχεδόν ακατόρθωτες.

8 Η υλοποίηση των Firewalls

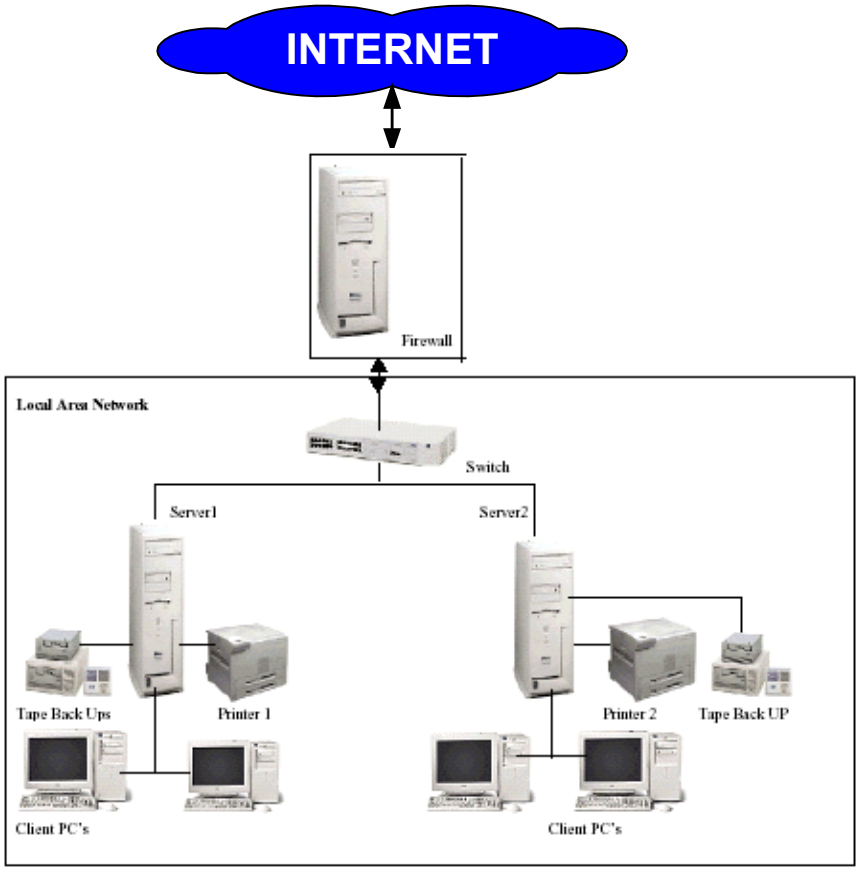
Μιας επαρκής και αποτελεσματική τεχνολογία υλοποίησης firewall σε οποιοδήποτε λειτουργικό σύστημα χωρίζεται στα εξής τέσσερα κομμάτια : Προετοιμασία, ρύθμιση, έλεγχος και υλοποίηση.

8.1 Προετοιμασία

Ένα καλά σχεδιασμένο σύστημα δικτύου είτε στις πλατφόρμες των windows NT, είτε του UNIX ή το συνδυασμό τους, απαιτεί το λογικό διαχωρισμό των υπολογιστών σε groups βασιζόμενα στις λειτουργίες τους. Αυτά τα groups γνωστά ως Domains είναι η βάση των τοπικών δικτύων μεγάλης κλίμακας και αφορά την κατηγοριοποίηση υπολογιστών που λειτουργούν κάτω από μία κοινή πολιτική ασφάλειας, για εύκολη διαχείριση. Όταν τα Domains αλληλεπιδρούν, είναι πιθανόν να υπάρξουν προβλήματα ασφάλειας στο δίκτυο και εδώ μπαίνει η υλοποίηση του firewall.

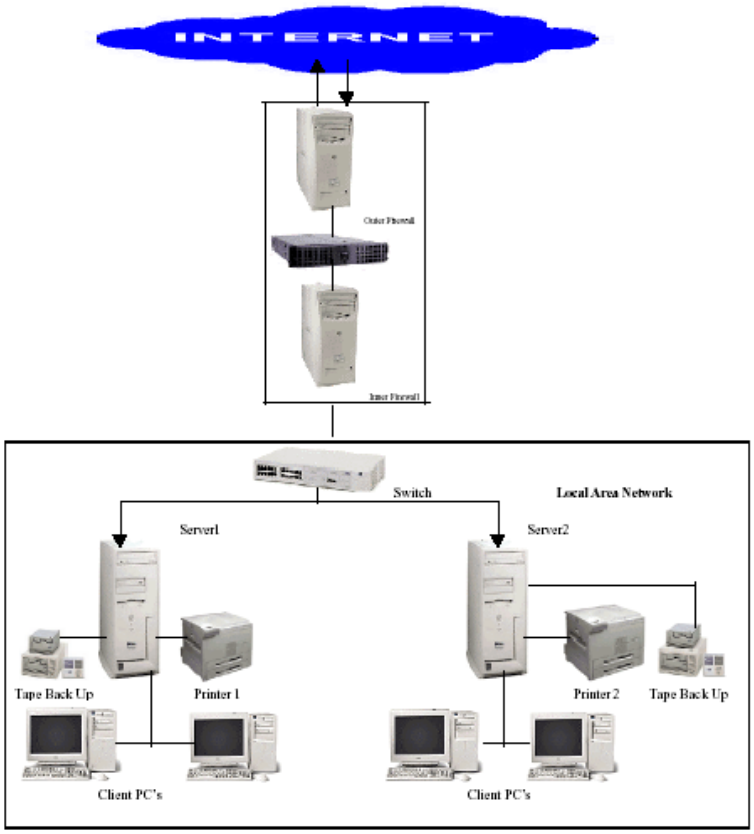
Η προετοιμασία του firewall αφορά την χρησιμοποίηση των υλικών και του εξοπλισμού. Περιλαμβάνει την γνώση του επιπέδου ασφάλειας που θα βάλουμε στα δεδομένα, έτσι ώστε να βρεθεί ο πιο κατάλληλος σχεδιασμός firewall για την αρχιτεκτονική του δικτύου. Η πιο κοινή υλοποίηση firewall, είναι συνήθως να ασφαλίσουμε ένα τοπικό δίκτυο από το Internet. Υπάρχουν δύο κύριοι σχεδιασμοί: ο σχεδιασμός firewall μονού επιπέδου και ο σχεδιασμός firewall πολλαπλών επιπέδων.

- **Σχεδιασμός firewall μονού επιπέδου**: Αφορά μια κατάσταση όπου ένας μοναδικός host είναι επιφορτισμένος με όλες τις ευθύνες υλοποίησης του firewall και ελέγχει την πρόσβαση σε ολόκληρο το τοπικό δίκτυο. Αυτός ο σχεδιασμός είναι συνήθως βολικός για μικρού έως μεσαίου μεγέθους δίκτυα, όπου το κόστος είναι περιοριστικός παράγοντας και είναι ευκολότερος στην υλοποίηση. Ωστόσο η παγίδα αυτού του στιλ σχεδιασμού, είναι ότι είναι ευάλωτο σε λάθη υλοποίησης και η απλότητα του κάνει ολόκληρο το δίκτυο ανασφαλή, καθώς υπάρχει μόνο ένα εστιακό σημείο για υλοποίηση ασφάλειας. Η Εικόνα 18, απεικονίζει ένα απλό σχεδιασμό υλοποίησης firewall μονού επιπέδου.



Εικόνα 18
Παράδειγμα σχεδιασμού υλοποίησης firewall μονού επιπέδου

- **Σχεδιασμός firewall πολλαπλών επιπέδων:** αφορά το μοίρασμα της ευθύνης της ασφάλισης του δικτύου σε περισσότερους του ενός host, οι οποίοι στις περισσότερες περιπτώσεις είναι συνδεδεμένοι σε σειρά. Αυτός ο σχεδιασμός είναι δύσκολος και πολύπλοκος, αλλά όχι μόνο γλιτώνει ένα host από πολύ bandwidth και αποτελέσματα επεξεργασίας από την ασφάλιση ολόκληρου του δικτύου, αλλά επίσης παρέχει μία οδό για την υλοποίηση πολλών μηχανισμών ασφάλειας πάνω από πολλούς hosts. Η πιθανότητα αποτυχίας της ασφάλειας μειώνεται σημαντικά. Ωστόσο, αυτός ο τύπος firewall κοστίζει περισσότερο από τον προηγούμενο. Η Εικόνα 19, είναι μια αναπαράσταση ενός σχεδιασμού υλοποίησης firewall πολλαπλών επιπέδων.



Εικόνα 19

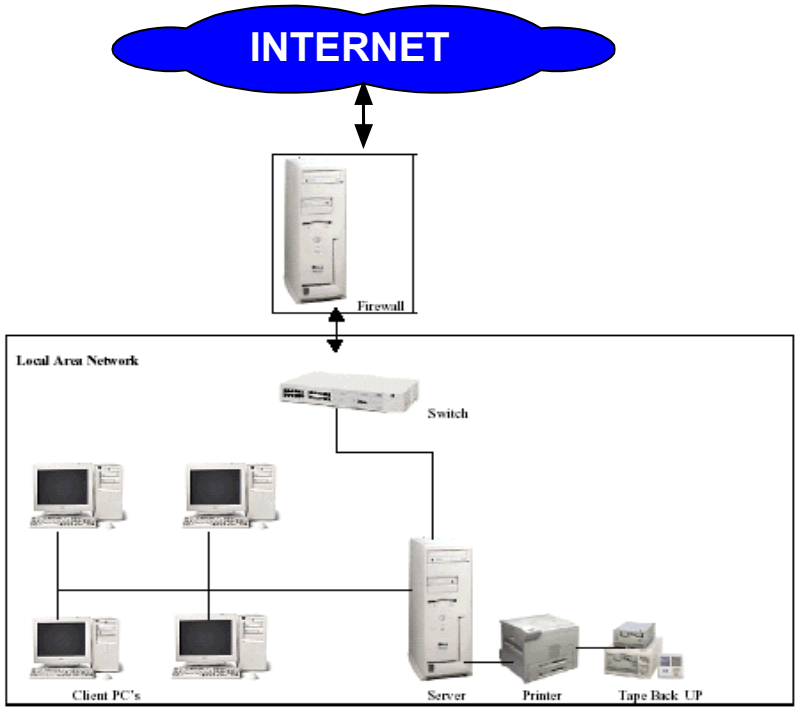
Παράδειγμα σχεδιασμού firewall πολλαπλών επιπέδων.

Μία άλλη απόφαση που πρέπει να παρθεί οποιοσδήποτε από τους δύο σχεδιασμούς κι αν υιοθετηθεί, είναι αν το firewall θα υλοποιηθεί σαν φιλτράρισμα πακέτων ή σαν Proxy εφαρμογών. Είναι σημαντικό να τονίσουμε ότι ενώ οι υπηρεσίες όπως SMTP, HTTP, ή NTP παρακολουθούνται και ελέγχονται καλύτερα μέσω του φιλτραρίσματος πακέτων, υπηρεσίες όπως το DNS και το FTP μπορεί να απαιτήσουν κάποια πολύπλοκα χαρακτηριστικά που είναι διαθέσιμα μόνο στους proxies, για να επιτύχουν την επιθυμητή ασφάλεια στο δίκτυο.

Έχοντας εξηγήσει τους σχεδιασμούς των firewalls αξιολογούμε στη συνέχεια τρεις διαφορετικές τοπολογίες των firewalls, κάθε μία από τις οποίες μπορεί να υλοποιηθεί σε κάθε έναν από τους δύο σχεδιασμούς που αναφέρθηκαν προηγουμένως.

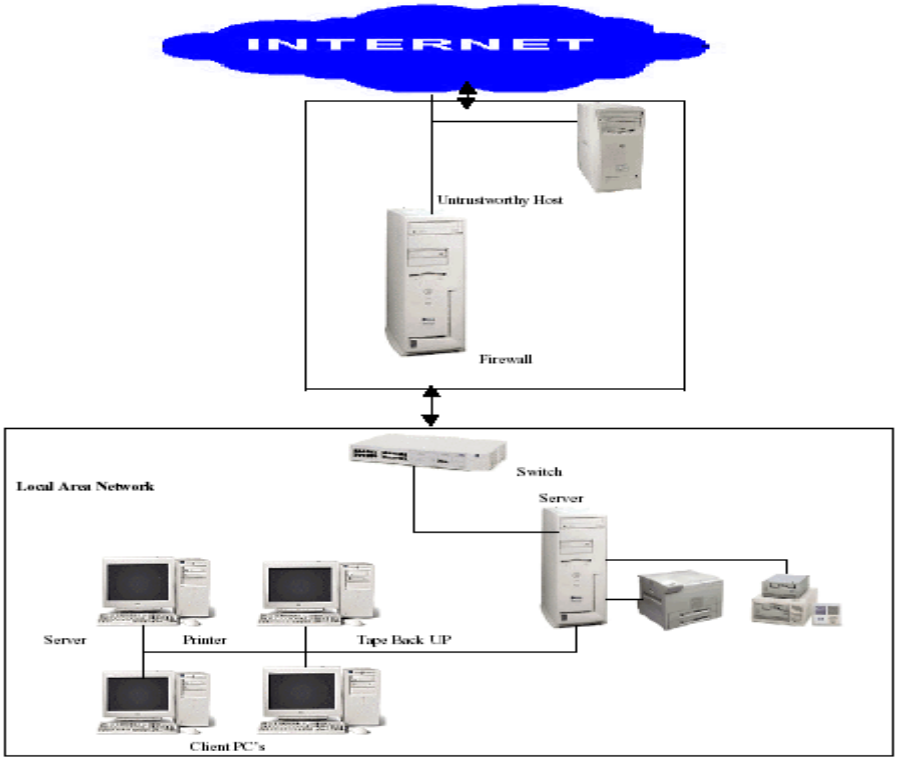
- **Τοπολογία Basic border firewall:** αυτή είναι η απλούστερη φόρμα σχεδιασμού firewall. Αφορά τη σύνδεση του δικτύου με το εξωτερικό δίκτυο όπως το Internet και την τοποθέτηση ενός αφιερωμένου host ανάμεσα στα δύο δίκτυα, ο οποίος θα παρέχει όλες τις λειτουργίες του firewall. Ο host στις

περισσότερες περιπτώσεις είναι ένας router φιλτραρίσματος πακέτων, ο οποίος παρακολουθεί την ροή της κίνησης ανάμεσα στα δίκτυα και επιτρέπει ή απορρίπτει πακέτα με βάση το πώς είναι ρυθμισμένος. Στην Εικόνα 20, φαίνεται η διαγραμματική αναπαράσταση της υλοποίησης του. Αυτός ο σχεδιασμός είναι εύκολος να υλοποιηθεί και απαιτεί ελάχιστη τεχνική εξειδικεύσει σε αντίθεση με τους άλλους δύο.



Εικόνα 20
Τοπολογία Basic border firewall

- **Τοπολογία μη έμπιστου host:** ένας άλλος δημοφιλής σχεδιασμός είναι ο σχεδιασμός του μη έμπιστου host ο οποίος επεκτείνετε πιο πολύ σε θέματα ασφάλειας και σχεδιασμού από τον basic border firewall σχεδιασμό. Οι σχεδιασμοί αυτοί είναι παρόμοιοι με την διαφορά της προσθήκης ενός host ανάμεσα στο εξωτερικό δίκτυο και στο firewall που προστατεύει το εσωτερικό δίκτυο. Μ' αυτή την υλοποίηση η ασφάλεια των επιπέδων δικτύου και εφαρμογής αναβαθμίζεται. Ο host ρυθμίζεται να παρέχει κάποιο βαθμό ασφάλειας στο firewall που προστατεύει το τοπικό δίκτυο. Η Εικόνα 21, δείχνει την τοπολογία μη έμπιστου host.



Εικόνα 21
Τοπολογία μη έμπιστου host

- **Τοπολογία DMZ firewall:** αυτός ο σχεδιασμός γνωστός σαν Demilitarized Zone firewall σχεδιασμός, είναι μία αρχιτεκτονική πολλαπλών στρωμάτων και είναι αναμφισβήτητα ο πιο ασφαλής από όλους. Αφορά τη χρήση περισσοτέρων του ενός φιλτραρίσματος πακέτων και ακόμη έναν host που συμπεριφέρεται σαν ένα firewall ανάμεσα στο εσωτερικό και στο εξωτερικό δίκτυο, ενώ οι routers που είναι απευθείας συνδεδεμένοι στο Internet, προστατεύουν το τοπικό δίκτυο από άμεσες εξωτερικές επιθέσεις, όπως spoofing της IP διεύθυνσης πηγής και επιθέσεις στην δρομολόγηση πηγής. Ο εσωτερικός router διασφαλίζει ότι μόνο οι αιτήσεις που έρχονται από τον firewall host που τρέχει σαν Proxy Server, επιτρέπεται να περάσουν στο εσωτερικό δίκτυο. Μ' αυτή τη διάταξη, δεν υπάρχει άμεση ροή κίνησης ανάμεσα στο εσωτερικό και στο εξωτερικό δίκτυο.

8.2 Ρύθμιση

Όταν επιλεχθεί ο κατάλληλος τρόπος σχεδιασμού αποκτάτε το απαιτούμενο υλικό και λογισμικό. Το υλικό που χρειάζεται περιλαμβάνει επεξεργαστές, μνήμη RAM, routers, switches, hubs, backup συσκευές, κάρτες δικτύου κ.τ.λ. Από την άλλη

πλευρά, το λογισμικό περιλαμβάνει λειτουργικά συστήματα, λογισμικό για τους drivers και λογισμικά για παρακολούθηση του δικτύου και ανάλυση της κίνησης.

8.3 Έλεγχος

Είναι σημαντικό να ελέγξουμε το firewall για να δούμε αν έχει τα απαιτούμενα προσόντα. Αυτό γίνεται σε εφεδρικό σύστημα, ή σε ένα δοκιμαστικό περιβάλλον. Αυτά που πρέπει να προσέξουμε κατά την διάρκεια του ελέγχου, είναι τα εξαρτήματα του υλικού όπως οι επεξεργαστές, οι δίσκοι, η μνήμη και τα interfaces δικτύου. Επίσης, πρέπει να ελεγχθεί το λειτουργικό σύστημα και η διεργασίες όπως το booting και η πρόσβαση στην κονσόλα για να δούμε πως λειτουργεί. Συσκευές όπως ο εξοπλισμός διασύνδεσης δικτύων και το λογισμικό του firewall, πρέπει επίσης να ελεγχθούν για να διασφαλίσουμε ότι έχουν τα επιθυμητά στάνταρτ.

8.4 Υλοποίηση

Το ελεγμένο σύστημα firewall πρέπει τώρα να υλοποιηθεί στο περιβάλλον παραγωγής το οποίο τις περισσότερες φορές είναι ένα υπάρχον δίκτυο. Αυτό πρέπει να σχεδιαστεί και να εκτελεστεί προσεκτικά για να ελαχιστοποιηθεί η πιθανότητα διάρρηξης. Ενώ θα υλοποιείται το νέο σύστημα firewall, τα μη φιλτραρισμένα πακέτα δεν πρέπει να περνάνε σ' αυτό και πρέπει να γίνει ένα κατάλληλο documentation για όλες τις ενέργειες.

9 Απειλές

9.1 Σπάσιμο κωδικών πρόσβασης

Οι κωδικοί στο Internet μπορούν να «σπάσουν» με πολλούς τρόπους. Ακόμη και ο καλύτερος μηχανισμός για κωδικούς θα είναι άχρηστος αν υπάρχουν χρήστες που πιστεύουν ότι το όνομα τους είναι καλός κωδικός!

Το πρόβλημα με τους κωδικούς είναι ότι από τη στιγμή που θα φτιαχτεί ο αλγόριθμος δημιουργίας τους, είναι θέμα ανάλυσης του αλγορίθμου για να βρεθούν όλοι οι κωδικοί του συστήματος. Ο cracker μπορεί να αναλύσει το αποτέλεσμα του προγράμματος δημιουργίας κωδικών και να καταλάβει τον αλγόριθμο που χρησιμοποιείται. Έπειτα θα εκτελέσει τον αλγόριθμο στους άλλους χρήστες για να βρει τους δικούς τους κωδικούς.

Υπάρχουν πολλά δωρεάν προγράμματα στο Internet για το «σπάσιμο» κωδικών. Το crack για παράδειγμα, είναι ένα πρόγραμμα με σκοπό το σπάσιμο ανασφαλών κωδικών.

9.2 IP Spoofing

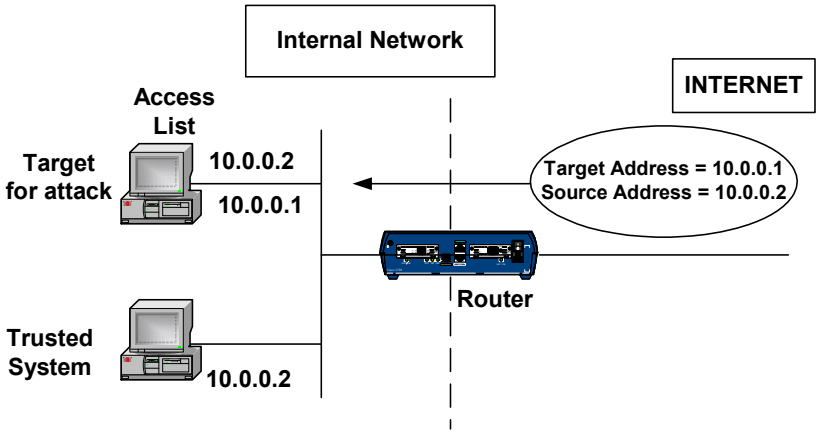
Το IP spoofing είναι μία νέα (σχετικά) τεχνική επίθεσης σε δικτυωμένους υπολογιστές. Αν και η πιθανότητα τέτοιας επίθεσης είχε προβλεφθεί από το 1989 σε ένα paper του Steve Bellovin, μόνο από τις αρχές του 1995 άρχισε να χρησιμοποιείται από τους hackers.

Περιλαμβάνει την μίμηση της IP διεύθυνσης κάποιου έμπιστου host ή router, για να κερδίσει πρόσβαση στις προστατευμένες πηγές πληροφοριών. Μια οδός για την spoofing επίθεση είναι να εκμεταλλευτεί ένα χαρακτηριστικό του IPv4 γνωστό ως ‘source routing’, κατά το οποίο ένας hacker κατασκευάζει ένα μονοπάτι πηγή στο Server, καθορίζοντας το απευθείας μονοπάτι όπου τα IP πακέτα φεύγουν από τον δικό μας web Server και πάνε στον Server του hacker, όλα αυτά χρησιμοποιώντας τον έμπιστο πελάτη σαν τελευταίο hop στην διαδρομή για τον web Server. Ο hacker στέλνει μια αίτηση πελάτη στον web Server χρησιμοποιώντας την διαδρομή πηγής. Ο Server δέχεται την αίτηση σαν να ήταν από τον έμπιστο πελάτη και του επιστρέφει την απάντηση. Ο έμπιστος πελάτης χρησιμοποιώντας την διαδρομή πηγής, προωθεί τα πακέτα στον Server του hacker.

Αλλά τι είναι πραγματικά το spoofing; Είναι μια τεχνική που χρησιμοποιείται για να μειώσει το overhead του δικτύου, ειδικά σε δίκτυα ευρείας περιοχής (WANs).

Με το spoofing μπορούμε να μειώσουμε το απαιτούμενο μέγεθος του bandwidth έχοντας συσκευές όπως bridges και routers για τις απομακρυσμένες συσκευές. Αυτή η τεχνική ξεγελάει τη συσκευή του LAN κάνοντας την να νομίζει ότι το απομακρυσμένο LAN είναι ακόμα συνδεδεμένο, παρόλο που δεν είναι.

Το spoofing, μπορεί να είναι επιτυχημένο ακόμη και αν εφαρμοστεί μέσω firewall, αν δεν είναι ρυθμισμένο να φιλτράρει εισερχόμενα πακέτα των οποίων η διεύθυνση πηγής είναι από τοπικό Domain. Μπορούμε να εντοπίσουμε το IP spoofing ελέγχοντας τα πακέτα. Ένα πρόγραμμα που μας βοηθάει σ' αυτό είναι το NetLog το οποίο κοιτάει στο εξωτερικό interface για πακέτα που έχουν και τις δύο διευθύνσεις πηγής και προορισμού στο τοπικό Domain.



Εικόνα 22

Παράδειγμα IP spoofing.

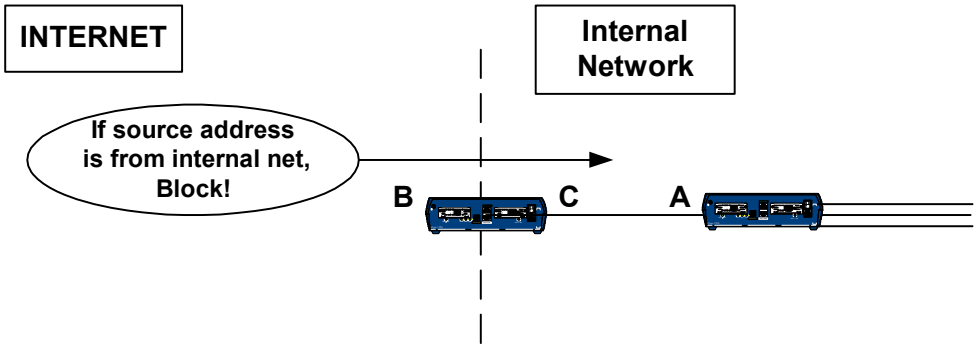
Παρακάτω υπάρχουν παραδείγματα από ρυθμίσεις που είναι ευαίσθητες σε τέτοιες επιθέσεις :

- Routers στα εξωτερικά δίκτυα που υποστηρίζουν πολλαπλά εσωτερικά interfaces.
- Routers με δύο interfaces που υποστηρίζουν υποδίκτυο στο εσωτερικό δίκτυο.
- Proxy firewalls όπου οι Proxy εφαρμογές χρησιμοποιούν την IP διεύθυνση πηγής για πιστοποίηση.

Δυο βήματα που μπορούμε να κάνουμε για να αποτρέψουμε αυτού του είδους τις επιθέσεις είναι τα εξής :

- εγκαθιστούμε έναν router φιλτραρίσματος, ο οποίος θα περιορίσει την εισαγωγή πακέτων σε εξωτερικό interface αν αναγνωρίσει την πηγή του πακέτου καθώς θα έρχεται μέσα από το δίκτυο. Ακόμη και αν είναι πιστοποιημένο πακέτο δε θα περάσει.
- θα φιλτράρονται τα εξερχόμενα πακέτα, για να αποφασίζεται αν η διεύθυνση είναι διαφορετική από το εσωτερικό δίκτυο, έτσι οι επιθέσεις από μέσα θα αποτρέπονται.

Στην Εικόνα 23, βλέπουμε μια περίπτωση αποτροπής IP spoofing. Σ' αυτή τη περίπτωση, κάθε εισερχόμενο πακέτο από το εξωτερικό δίκτυο πρέπει να περάσει μέσα από έναν router που είναι εγκατεστημένος ανάμεσα στο εξωτερικό interface (A) και την εξωτερική σύνδεση (B). Αυτός ο καινούργιος ενδιάμεσος router πρέπει να ρυθμιστεί έτσι, ώστε να μπλοκάρει τα πακέτα που έχουν εσωτερική διεύθυνση (C) στο interface που βγαίνει προς τα έξω και είναι συνδεδεμένο στον αρχικό router.



Εικόνα 23
Περίπτωση αποτροπής IP spoofing

9.3 IP smurfing

Πρόκειται για ένα νέο είδος επίθεσης που πρωτοεμφανίστηκε στις αρχές του 1998. Βασίζεται στο IP spoofing, ενώ εκμεταλλεύεται και αδυναμίες της υλοποίησης των IP και ICMP (Internet Control Message Protocol) πρωτοκόλλων σε δικτυακές συσκευές.

Το smurf είναι ένα πρόγραμμα, το οποίο προσποιείται ότι στέλνει πακέτα από άσχετο αποστολέα (εδώ χρησιμοποιούνται οι τεχνικές του IP spoofing). Τα πακέτα αυτά είναι του πρωτοκόλλου ICMP, το οποίο και χρησιμοποιείται από βασικές

λειτουργίες του δικτύου (π.χ. τις υπηρεσίες ping και traceroute). Στέλνοντας ένα ping πακέτο στην διεύθυνση εκπομπής (broadcast address) ενός δικτύου, ο αποστολέας δέχεται απάντηση από κάθε έναν από τους κόμβους που δέχθηκαν το ICMP ping πακέτο (δηλ. όλους του κόμβους του δικτύου).

Σε ένα μεγάλο B-class δίκτυο όπου λ.χ. χρησιμοποιείται το ένα τέταρτο του πεδίου διευθύνσεων, η απάντηση είναι ίση με περίπου 16.000 πακέτα. Είναι προφανές ότι με μερικές εκατοντάδες πακέτα ping μπορούν να κάνουν άχρηστο το δίκτυο, φέρνοντάς το σε μία κατάσταση Denial-of-Service.

9.4 Απειλές ασφάλειας στα e-mail

Το e-mail είναι ένα καλό εργαλείο του Internet, αλλά κρύβει πολλές απειλές για την ιδιωτική μας ασφάλεια. Κάποιες από αυτές τις απειλές είναι το e-mail bombing & spamming. Μια από τις κυριότερες αδυναμίες των e-mail μηνυμάτων είναι ότι δεν ανιχνεύονται πάντα. Στις απειλές των e-mail περιλαμβάνονται άνθρωποι που ανιχνεύουν τα μηνύματα ψάχνοντας πολύτιμες πληροφορίες, όπως κωδικούς από πιστωτικές κάρτες ή δημόσια passwords.

Το e-mail bombing είναι παράνομο, αλλά δύσκολο να εντοπιστεί επειδή υπάρχουν πολλοί ανώνυμοι τρόποι για να σταλεί. Συνήθως στέλνονται πάρα πολλά μηνύματα σε μια e-mail διεύθυνση από εκατοντάδες, μέχρι μερικές χιλιάδες και αυτό τις περισσότερες φορές προκαλεί denial of service στον mail Server.

Το e-mail bombing, δεν είναι το ίδιο με το spamming. Το e-mail bombing χαρακτηρίζετε από άτομα που επανειλημμένα στέλνουν πολλά αντίγραφα του ίδιου μηνύματος σε μια συγκεκριμένη διεύθυνση, ενώ το e-mail spamming είναι μια διαφορετική μορφή του bombing. Αναφέρεται στην αποστολή του ίδιου e-mail σε χιλιάδες χρήστες. Το e-mail spamming γίνεται χειρότερο αν οι παραλήπτες απαντήσουν στο μήνυμα, προκαλώντας όλες τις άλλες αρχικές διευθύνσεις να πάρουν την απάντηση. Αν η ταυτότητα του λογαριασμού που στέλνει το μήνυμα τροποποιηθεί, τότε τα e-mail spamming ή bombing συνδυάζονται με το spoofing, πράγμα που κάνει σχεδόν αδύνατο να εντοπιστεί ο συντάκτης και ο προορισμός του μηνύματος.

Είναι πολύ σημαντικό ν' ανιχνευτούν τα bombing & spamming των e-mail όσο το δυνατόν πιο γρήγορα. Ένα από τα σημάδια που παρουσιάζει το σύστημα όταν βρίσκεται υπό επίθεση είναι η βραδύτητα. Αν το e-mail είναι αργό, ή δεν

αποστέλλεται/παραλαμβάνεται μπορεί να σημαίνει ότι ο mail Server μας είτε προσπαθεί να επεξεργαστεί ένα μεγάλο αριθμό μηνυμάτων, ή έχει ήδη υποστεί μια ζημιά.

Όταν συμβαίνει αυτό, συνιστάται να κάνουμε τα εξής:

- Αναγνώριση της πηγής του e-mail, ελέγχοντας τις επικεφαλίδες και άμεση επαναρύθμιση του firewall (ή του router) για να μπλοκάρουμε τα εισερχόμενα πακέτα από αυτή τη διεύθυνση. Πρέπει να προσέχουμε πριν υποθέσουμε ότι υπαίτιος αυτής της επίθεσης είναι το άτομο που φαίνεται στην επικεφαλίδα του μηνύματος, επειδή πολλές φορές το όνομα που εμφανίζεται εκεί είναι απλώς ένα ψευδώνυμο στην προσπάθεια του να κρύψει την αληθινή του ταυτότητα.
- Αν η e-mail υπηρεσία μας είναι μέσω ενός ISP, πρέπει να τους κάνουμε γνωστό το περιστατικό έτσι ώστε να επαναρυθμίσουν τους routers ή το firewall τους. Έτσι θ' αποτρέψουν την εισαγωγή τέτοιων μηνυμάτων από αυτή τη διεύθυνση προορισμού.
- Να επικοινωνήσουμε με τον οργανισμό επειγόντων περιστατικών (CERT), για την επίθεση έτσι ώστε να εντοπίσουν τα περιστατικά.

Δεν υπάρχει τρόπος να σταματήσουμε το e-mail bombing. Ωστόσο, υπάρχουν μερικά πράγματα που μπορούμε να κάνουμε, έτσι ώστε να προστατεύσουμε τον εαυτό μας και να μειώσουμε την πιθανότητα επίθεσης. Πρώτον, πρέπει να κρατάμε πάντα ενημερωμένο το λογισμικό του e-mail. Δεύτερον, πρέπει να κρατάμε τις ενημερώσεις, τα patches και τις διορθώσεις των bugs που εκδίδονται από τον e-mail developer. Το τρίτο πράγμα είναι λίγο πιο τεχνικό. Θα μπορούσαμε ν' αναπτύξουμε ένα εργαλείο που θα ελέγχει και θα μας προειδοποιεί σε πολύ μικρό χρονικό διάστημα για εισερχόμενα μηνύματα που προέρχονται από τον ίδιο χρήστη ή το ίδιο site. Τότε θα μπορούμε να μπλοκάρουμε αυτές τις συνδέσεις σε επίπεδο router.

10 Τρόποι αντιμετώπισης των απειλών

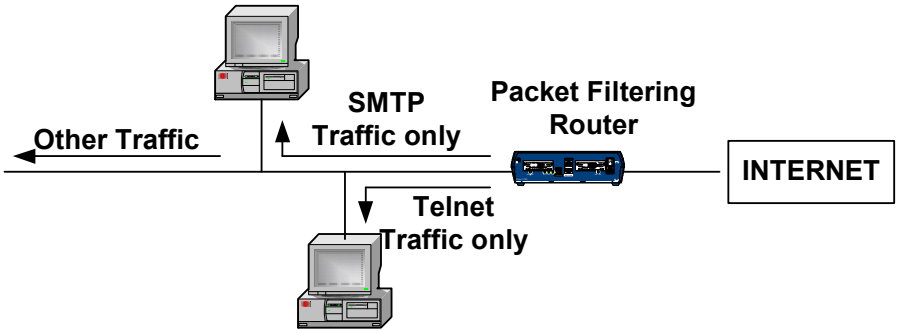
10.1 Φιλτράρισμα πακέτων

Συνήθως το φιλτράρισμα πακέτων γίνεται χρησιμοποιώντας έναν router, ο οποίος φιλτράρει τα πακέτα καθώς περνούν ανάμεσα στα interfaces του router. Αυτοί οι routers, μπορούν να φιλτράρουν IP πακέτα βασισμένα στα ακόλουθα πεδία:

- Την IP διεύθυνση πηγής.
- Την IP διεύθυνση προορισμού.
- Το TCP/UDP port πηγής.
- ΤοTCP/UDP port προορισμού.

Για να μπλοκάρουν συνδέσεις από ή σε συγκεκριμένους Web Servers ή δίκτυα, το φιλτράρισμα μπορεί να γίνει με πολλούς τρόπους, περιλαμβανομένου του μπλοκαρίσματος στις συνδέσεις συγκεκριμένων ports. Servers όπως ο telnet deamon συνήθως βρίσκονται σε συγκεκριμένα ports. Αν ενεργοποιηθεί το firewall να μπλοκάρει τις TCP ή τις UDP συνδέσεις προς ή από συγκεκριμένα ports, θα μπορέσουν να πραγματοποιηθούν πολιτικές για κάποιους τύπους συνδέσεων που γίνονται σε συγκεκριμένους Servers. Μπορούμε, για παράδειγμα να μπλοκάρουμε όλες τις εισερχόμενες συνδέσεις στους Web Servers του δικτύου μας, εκτός από αυτούς που είναι συνδεδεμένοι στο firewall. Σ’ αυτά τα συστήματα μπορεί να θέλουμε να επιτρέψουμε μόνο κάποιες συγκεκριμένες υπηρεσίες. όπως το SMTP στο ένα σύστημα και τις telnet ή FTP συνδέσεις στο άλλο. Φιλτράροντας τα TCP ή UDP ports, μας βοηθά να πραγματοποιήσουμε μια πολιτική μέσω κάποιου router φιλτραρίσματος πακέτων, ή ακόμη κάποιου Server με δυνατότητες φιλτραρίσματος πακέτων.

Η Εικόνα 24, δείχνει ένα router που φιλτράρει πακέτα.



Εικόνα 24
Παράδειγμα router φιλτραρίσματος πακέτων

Ο Πίνακας 1, δείχνει ένα set από access list που βοηθούν στην κατανόηση της παραπάνω εικόνας.

Class A	*Src ADDR*	*Dest ADDR*	*Src port*	*Dest port*	*Action*
Tcp	*	123,4,5,6	>1023	23	permit
Tcp	*	123,4,5,7	>1023	25	Permit
Tcp	*	123,4,5,8	>1023	25	Permit
Tcp	129,6,48,254	123,4,5,9	>1023	119	Permit
Upd	*	123,4,*,*	>1023	123	Permit
*	*	*	*	*	Deny

Πίνακας 1
Set από access list

Ο πρώτος κανόνας επιτρέπει τα TCP πακέτα που έρχονται από οποιαδήποτε διεύθυνση και με port number μεγαλύτερο του 1023 να περάσουν στην διεύθυνση 123,4,5,6 και στο port 23 μέσα στο site. Ο δεύτερος και τρίτος κανόνας λειτουργεί σαν τον πρώτο μόνο που τώρα επιτρέπεται η πρόσβαση του port number 25 για SMTP μόνο μέσω των διευθύνσεων 123.4.5.7 και 123.4.5.8. Ο τέταρτος κανόνας επιτρέπει πακέτα στον NNTP Server, αλλά μόνο από την διεύθυνση πηγής 129.6.48.254 στη διεύθυνση προορισμού 123.4.5.9 και στο port number 119. Ο πέμπτος κανόνας επιτρέπει την NTP κίνηση που χρησιμοποιεί UDP από οποιαδήποτε πηγή, σε οποιαδήποτε διεύθυνση προορισμού στο site. Και τέλος, ο έκτος κανόνας απαγορεύει την πρόσβαση σε όλα τα άλλα πακέτα.

Παρόλο που το φιλτράρισμα των πακέτων μπλοκάρει αποτελεσματικά τις συνδέσεις από ή προς συγκεκριμένους hosts, το οποίο αυξάνει το επίπεδο της ασφάλειας, οι routers έχουν πολλές αδυναμίες. Οι κανόνες είναι πολύπλοκοι να καθορισθούν και δύσκολο να επιβεβαιωθούν.

10.2 Τι πρέπει να κάνουμε σε περίπτωση επίθεσης

Πολλές φορές μετά την επίθεση του hacker δεν υπάρχουν πολλά που μπορεί να κάνει ένας διαχειριστής. Άλλες φορές, είναι σε θέση να σταματήσει τον hacker στο σημείο που έφτασε, οπότε τα βήματα σε περίπτωση επίθεσης είναι τα ακόλουθα :

1. Εκτίμηση της κατάστασης.
2. Αποσύνδεση του Server
3. Ανάλυση του προβλήματος
4. Ανάληψη δράσης.

Εκτίμηση της κατάστασης.

Το πρώτο πράγμα που πρέπει να γίνει όταν επιβεβαιωθεί η επίθεση, είναι η εκτίμηση των ζημιών και η σοβαρότητα της επίθεσης, όσο το δυνατόν πιο γρήγορα. Κάποιες ερωτήσεις που πρέπει να γίνουν, έτσι ώστε να εκτιμηθεί η κατάσταση είναι οι εξής :

- Κατάφερε τελικά ο hacker να μπει στο site; Αν ναι, ο διαχειριστής πρέπει να δράσει γρήγορα γιατί ο hacker μπορεί να είναι ακόμα μέσα.
- Πειράζει ακόμα ο hacker το σύστημα; Αν ναι, πρέπει να τον σταματήσουμε. Πρέπει να αποφασίσουμε με ποιον τρόπο, όσο το δυνατόν πιο γρήγορα. Αν όχι, υπάρχει λίγος χρόνος να βελτιωθεί η ασφάλεια, πριν ο hacker ξαναχτυπήσει.
- Ποιος είναι ο καλύτερος τρόπος να σταματήσουμε το σύστημα μέχρι να έχουμε καλύτερο έλεγχο της κατάστασης; Μπορεί να χρειαστεί να σταματήσουμε το σύστημα, ή τουλάχιστον την υπηρεσία που δέχτηκε επίθεση (όπως FTP, GOPHER, TELNET κτλ) Ίσως ακόμη χρειαστεί να κοπεί η σύνδεση στο Internet.
- Υπάρχει περίπτωση η επίθεση να είναι από μέσα; Αν ναι, πρέπει να είμαστε πιο προσεχτικοί και να μην αφήσουμε να διαρρεύσει η επίλυση του προβλήματος.

Αποσύνδεση του Server

Μετά την εκτίμηση της κατάστασης, πρέπει να πάρουμε κάποιες αποφάσεις και να προβούμε σε κάποιες ενέργειες. Η πρώτη απόφαση, είναι το κόψιμο της σύνδεσης. Ποια σύνδεση θα κοπεί, εξαρτάται από το δίκτυο. Οι παρακάτω ερωτήσεις θα μας βοηθήσουν να πάρουμε τις σωστές αποφάσεις.

- Μπορούμε να «κατεβάσουμε» τον Server; Αν ναι, το κάνουμε. Αν όχι, τότε κατεβάζουμε κάποιες υπηρεσίες, ή τουλάχιστον βγάζουμε όλους τους χρήστες από το σύστημα.
- Μας ενδιαφέρει να εντοπίσουμε τον hacker; Αν ναι, τότε δεν κόβουμε την σύνδεση με το Internet γιατί θα χάσουμε τα ίχνη του.
- Μπορεί να έχουν επηρεαστεί άλλοι πελάτες; Αν ναι, τότε «κατεβάζουμε» τον Server και ελέγχουμε όσους είναι απευθείας συνδεδεμένοι σ' αυτόν.
- Μπορούμε να ανεχτούμε χάσιμο πληροφοριών αν «κατεβάσουμε» τον Server;

Ανάλυση του προβλήματος

Μαζεύουμε όλες τις πληροφορίες που έχουμε και βγάζουμε τα αποτελέσματα. Πρέπει να σκεφτούμε σοβαρά τις επόμενες κινήσεις μας. Έχουμε βρει την «τρύπα» και θα την διορθώσουμε. Απλά πρέπει να σιγουρευτούμε ότι δεν θα δημιουργήσουμε άλλη «τρύπα», ή ότι δεν θα επηρεάσουμε άλλες υπηρεσίες ή επεξεργασίες.

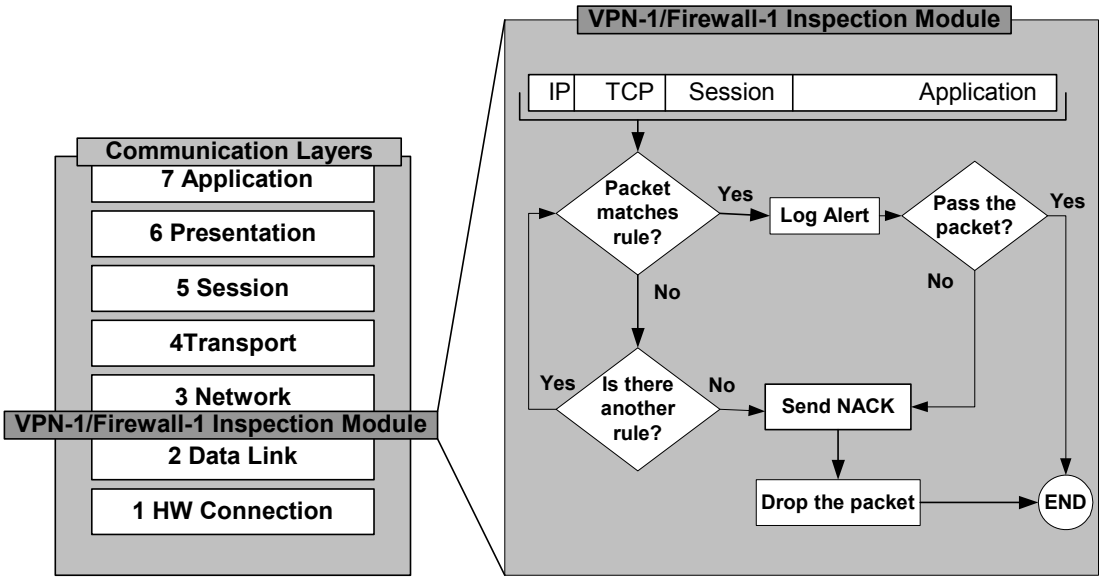
Ανάληψη δράσης

Σ' αυτό το στάδιο, γίνεται η υλοποίηση του σχεδίου που έχουμε καταστρώσει. Πρέπει να ειδοποιήσουμε το CERT και να ανταλλάξουμε πληροφορίες μ' αυτούς. Όχι μόνο θα τους βοηθήσουμε να ενημερώσουν κι άλλους γι' αυτό το περιστατικό, αλλά μπορούν ακόμα και να μας βοηθήσουν. Τελικά επισκευάζουμε την «τρύπα» στην ασφάλεια και αποκαθιστούμε το σύστημα.

11 Check Point

11.1 VPN-1/Firewall-1 inspection module

Το VPN-1/Firewall-1 inspection module βρίσκεται μέσα στον πυρήνα του λειτουργικού συστήματος, ανάμεσα στο επίπεδο σύνδεσης δεδομένων (data link layer) και στο επίπεδο του δικτύου (network layer). Εφόσον το data link είναι το πραγματικό interface δικτύου (NIC) και το network link είναι το πρώτο στρώμα του stack πρωτοκόλλου (π.χ. IP), τότε το VPN-1/Firewall-1 βρίσκεται στο χαμηλότερο στρώμα λογισμικού, όπως φαίνεται στην Εικόνα 25.



Εικόνα 25
Η θέση του VPN-1/Firewall-1 inspection module μέσα στον πυρήνα του λειτουργικού συστήματος

Με την επιθεώρηση σ' αυτό το επίπεδο, διασφαλίζεται ότι το VPN-1/Firewall-1 inspection module παρεμβαίνει και επιθεωρεί όλα τα εισερχόμενα και εξερχόμενα πακέτα στην πύλη. Τα πακέτα δεν επεξεργάζονται από τα υψηλότερα στρώματα των stack πρωτοκόλλων, εκτός και αν το inspection module επιβεβαιώσει ότι συμμορφώνονται με την πολιτική ασφάλειας. Το VPN-1/Firewall-1 εξετάζει τις IP διευθύνσεις, τα ports και κάθε άλλη πληροφορία που απαιτείται, έτσι ώστε να καθοριστεί αν πρέπει να δεχτούμε τα πακέτα σύμφωνα με την πολιτική ασφάλειας.
Το VPN-1/Firewall-1 προσπελαύνει και αναλύει τα δεδομένα που φτάνουν από όλα τα επίπεδα επικοινωνίας.

11.2 Log viewer: visual tracking and accounting

Το γραφικό περιβάλλον του log viewer παρέχει εικονική ανίχνευση, παρακολούθηση και πληροφορίες λογαριασμών, για όλες τις καταγραμμένες συνδέσεις από τις firewall πύλες. Ακόμη, είναι εφικτή και η παρακολούθηση του δικτύου σε πραγματικό χρόνο.

11.3 Διαχείριση ασφάλειας και δικτύου

Πέρα από τον υψηλό έλεγχο πρόσβασης, το VPN-1/Firewall-1 περιλαμβάνει χαρακτηριστικά διαχείρισης ασφάλειας και δικτύου, ανεπτυγμένα μέσα στην πολιτική ασφάλειας της επιχείρησης, τα οποία διαχειρίζονται μέσα από το γραφικό περιβάλλον του χρήστη.

Το πακέτο ασφάλειας του VPN-1/Firewall-1 έχει τις εξής δυνατότητες:

- Πιστοποίηση (Authentication)
- Μετάφραση διευθύνσεων δικτύου (Network Address Translation)
- VPNs
- Ασφάλεια περιεχομένου (Content Security)
- Έλεγχο σύνδεσης
- LDAP Account Management
- Open Security Extension
- Υψηλή διαθεσιμότητα (High Availability)

Πιστοποίηση

Το VPN-1/Firewall-1, παρέχει στους τοπικούς και απομακρυσμένους χρήστες ασφαλή, πιστοποιημένη πρόσβαση στις πηγές του δικτύου. Ευέλικτες μέθοδοι πιστοποίησης παρέχουν πρόσβαση στους χρήστες οποιασδήποτε IP εφαρμογής ή υπηρεσίας. Οι διαχειριστές αποφασίζουν πως πιστοποιείται ο κάθε χρήστης, σε ποιους Servers και σε ποιες εφαρμογές επιτρέπεται η πρόσβαση, και ποιες ώρες την ημέρα παρέχεται πρόσβαση στους χρήστες, όπως φαίνεται στον Πίνακα 2.

No.	Source	Destination	Service	Action	Track	Install On	Time
1	All Users@Any	pub_servers	smtp	User Auth	Short	Gateways	work_hours

Πίνακας 2
Παράδειγμα πιστοποίησης χρήστη

Μέθοδοι πιστοποίησης

Το VPN-1/Firewall-1παρέχει τις ακόλουθες μεθόδους πιστοποίησης:

- ***Πιστοποίηση Χρήστη***

  Η πιστοποίηση χρήστη παρέχει δικαιώματα πρόσβασης για κάθε χρήστη για FTP, TELNET, HTTP και RLOGIN, ανεξάρτητα από την IP διεύθυνση του χρήστη. Αν ένας τοπικός χρήστης είναι προσωρινά μακριά από το γραφείο και συνδέεται σε διαφορετικό host, ο διαχειριστής μπορεί να καθορίσει ένα κανόνα που θα επιτρέπει σ' αυτόν τον χρήστη να δουλεύει στο τοπικό δίκτυο, χωρίς να επεκτείνει την πρόσβαση σε όλους τους χρήστες του ίδιου host. Η πιστοποίηση του χρήστη είναι διαφανής— ο χρήστης δεν είναι υποχρεωμένος να συνδεθεί αποκλειστικά στην firewalled πύλη αλλά μπορεί να συνδεθεί απευθείας στον Server στόχο.

- ***Πιστοποίηση Πελάτη***

  Η πιστοποίηση πελάτη επιτρέπει πρόσβαση από κάποια συγκεκριμένη IP διεύθυνση. Ο χρήστης που δουλεύει σ' ένα client εκτελεί την πιστοποίηση συναντώντας επιτυχημένα μια πρόκληση πιστοποίησης, αλλά είναι το client μηχάνημα αυτό που παρέχει την πρόσβαση. Η πιστοποίηση του χρήστη είναι διαθέσιμη για κάθε υπηρεσία. Ευέλικτοι μέθοδοι επιτρέπουν στους χρήστες διαφανή ή μη διαφανή πρόσβαση, βασισμένη στις ιδιότητες του κανόνα πιστοποίησης του χρήστη.

- ***Πιστοποίηση Session***

  Η πιστοποίηση του session μπορεί να χρησιμοποιηθεί για τη διαφανή πιστοποίηση κάθε υπηρεσίας για κάθε session. Μετά την αρχικοποίηση της σύνδεσης του χρήστη σε ένα Server πίσω από τη firewalled πύλη, το VPN-1/Firewall-1 ανοίγει μια σύνδεση μ' έναν πράκτορα πιστοποίησης session. Ο πράκτορας προκαλεί το χρήστη για μια απάντηση κατάλληλης πιστοποίησης, πριν το VPN-1/Firewall-1 επιτρέψει στη σύνδεση να συνεχιστεί στον αιτούμενη Server.

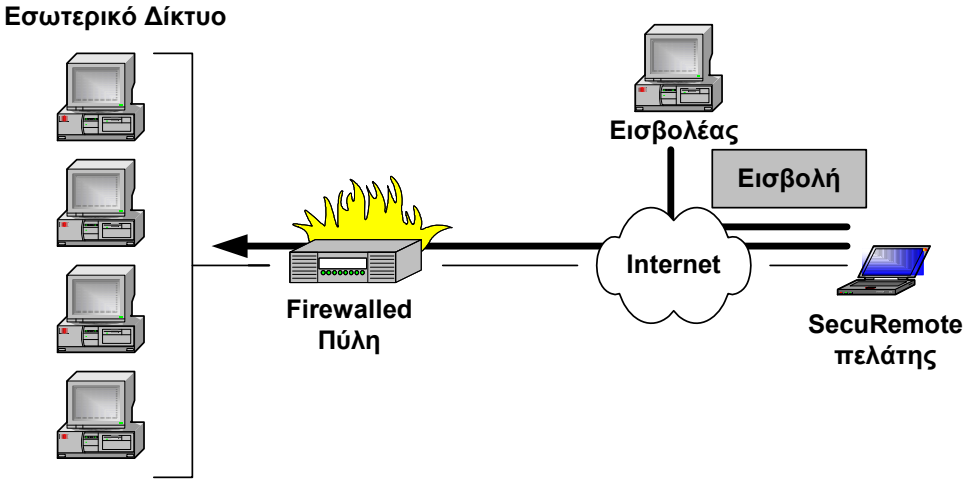
Virtual Private Networks (VPNs)

Η αποτροπή των παραβιάσεων των ιδιωτικών δικτύων, είναι μόνο ένας από τους στόχους που έχει η πολιτική ασφάλειας του δικτύου μιας επιχείρησης. Μια επιχείρηση η οποία επιθυμεί να προστατέψει την ακεραιότητα και τη μυστικότητα

των δεδομένων της, πρέπει να προσθέσει ακόμα ένα επίπεδο προστασίας στην πολιτική ασφάλειας: κρυπτογραφία και πιστοποίηση.

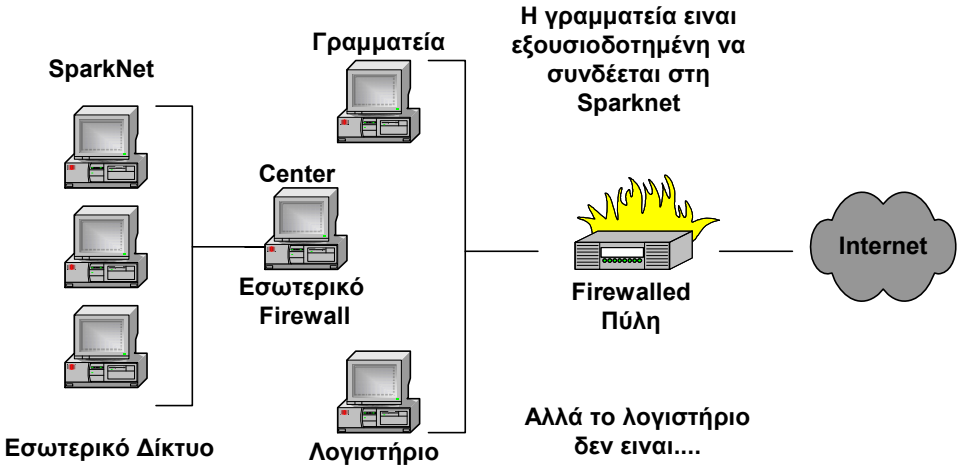
11.4 Παραδείγματα διαμόρφωσης δικτύου.

Η Εικόνα 26, δείχνει πως ένας εισβολέας μπορεί να εκμεταλλευτεί μία SecuRemote σύνδεση για να διεισδύσει στο εσωτερικό δίκτυο της επιχείρησης. Αυτού του είδους η επίθεση, μπορεί να αποτραπεί επιβάλλοντας στον VPN-1 SecuRemote πελάτη, μία desktop πολιτική που δε θα επιτρέπει τις εισερχόμενες συνδέσεις στον VPN SecuRemote πελάτη.



Εικόνα 26
Παράδειγμα επίθεσης μέσω SecuRemote σύνδεσης

Στην Εικόνα 27, οι Servers της Sparknet προστατεύονται από ένα εσωτερικό VPN/Firewall module στον H/Y center. Η πολιτική ασφάλειας, επιτρέπει σε κάποιον χρήστη από την γραμματεία να συνδεθεί στην Sparknet, αλλά χρήστες από το τμήμα λογιστηρίου δεν επιτρέπεται να συνδεθούν.

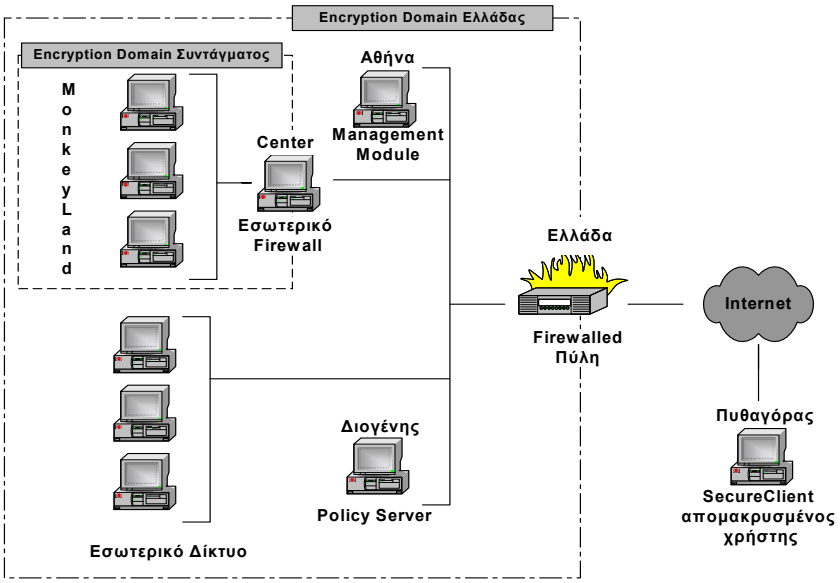


Εικόνα 27
Παράδειγμα πολιτικής ασφάλειας σε VPN/Firewall module

Εγκαθιστώντας το SecureClient στη γραμματεία, το επίπεδο της ασφάλειας μπορεί να βελτιωθεί έτσι ώστε να :

- Αποτρέπουμε τους χρήστες του λογιστηρίου (και οποιονδήποτε άλλων) από το να πάρουν τον έλεγχο της σύνδεσης της γραμματείας με τη Sparknet.
- Κρυπτογραφούμε τις συνδέσεις της γραμματείας με την Sparknet
- Επιβεβαιώνουμε ότι η γραμματεία είναι σωστά ρυθμισμένη.

Η Εικόνα 28, παρουσιάζει μια διαμόρφωση στην οποία το secureClient παρέχει ασφάλεια μέσα και έξω από το LAN.



Εικόνα 28
Παράδειγμα ασφαλισμένου δικτύου

Η διαμόρφωση αυτή αποτελείται από :

- Ένα management module (Τράπεζα), από όπου καθορίζεται η πολιτική ασφάλειας.
- Μία firewalled gateway (Θεσσαλονίκη), η οποία εφαρμόζει την πολιτική ασφάλειας.
- Ένα policy Server (Διογένης), από τον οποίο η desktop πολιτική «κατεβαίνει» στους secureClients.
- Ένα εσωτερικό VPN/firewall module (Σύνταγμα), το οποίο προστατεύει το υποδίκτυο MonkeyLand από τις κρυπτογραφημένες συνδέσεις. Το εσωτερικό VPN/firewall module απαιτείται για να προστατέψει το δίκτυο, αλλά μόνο όταν ο host πρέπει να προστατευτεί, τότε το VPN-1 secureServer module είναι επαρκές.
- Κάποια εσωτερικά SecureClient desktops.
- Έναν απομακρυσμένο SecureClient (Πυθαγόρας).

Για να γίνει η ρύθμιση του SecureClient πρέπει να γίνουν τα ακόλουθα :

1. Να εγκαταστήσουμε το κατάλληλο VPN-1/Firewall-1 λογισμικό και τις άδειες σε κάθε μηχάνημα, όπως φαίνεται στον Πίνακα 3:

Μηχάνημα	**Λογισμικό**
Πυθαγόρας	SecureClient (SecuRemote με ενεργοποιημένη την desktop ασφάλεια)
Ελλάδα	VPN/Firewall module
Αθήνα	Management module
Σύνταγμα	VPN/Firewall module
Διογένης	VPN/Firewall module με άδεια για SecureClients
Desktops	SecureClient (SecuRemote με ενεργοποιημένη την desktop ασφάλεια)

Πίνακας 3
Αντιστοίχιση VPN-1/Firewall-1 λογισμικού σε κάθε μηχάνημα

2. Φτιάχνουμε τα αντικείμενα του δικτύου (Ελλάδα, Πυθαγόρας, Διογένης) και τα διαμορφώνουμε κατάλληλα.

3. Διαμορφώνουμε το SecuRemote και την Desktop ασφάλεια.
4. Καθορίζουμε τους χρήστες και τα group χρηστών που θα έχουν πρόσβαση στο προστατευόμενο δίκτυο.
5. Καθορίζουμε τον policy Server και αναθέτουμε ένα group χρηστών.
6. Καθορίζουμε τους κατάλληλους κανόνες, για να επιτρέψουμε στους εξουσιοδοτημένους χρήστες να μπουν στο προστατευμένο δίκτυο. Ο Πίνακας 4, δείχνει ένα παράδειγμα κανόνα:

Source	Destination	Services	Action	Track	Install on
monkeylandUser@Any	monkeyland	Any	Client encrypt	None	Gateways

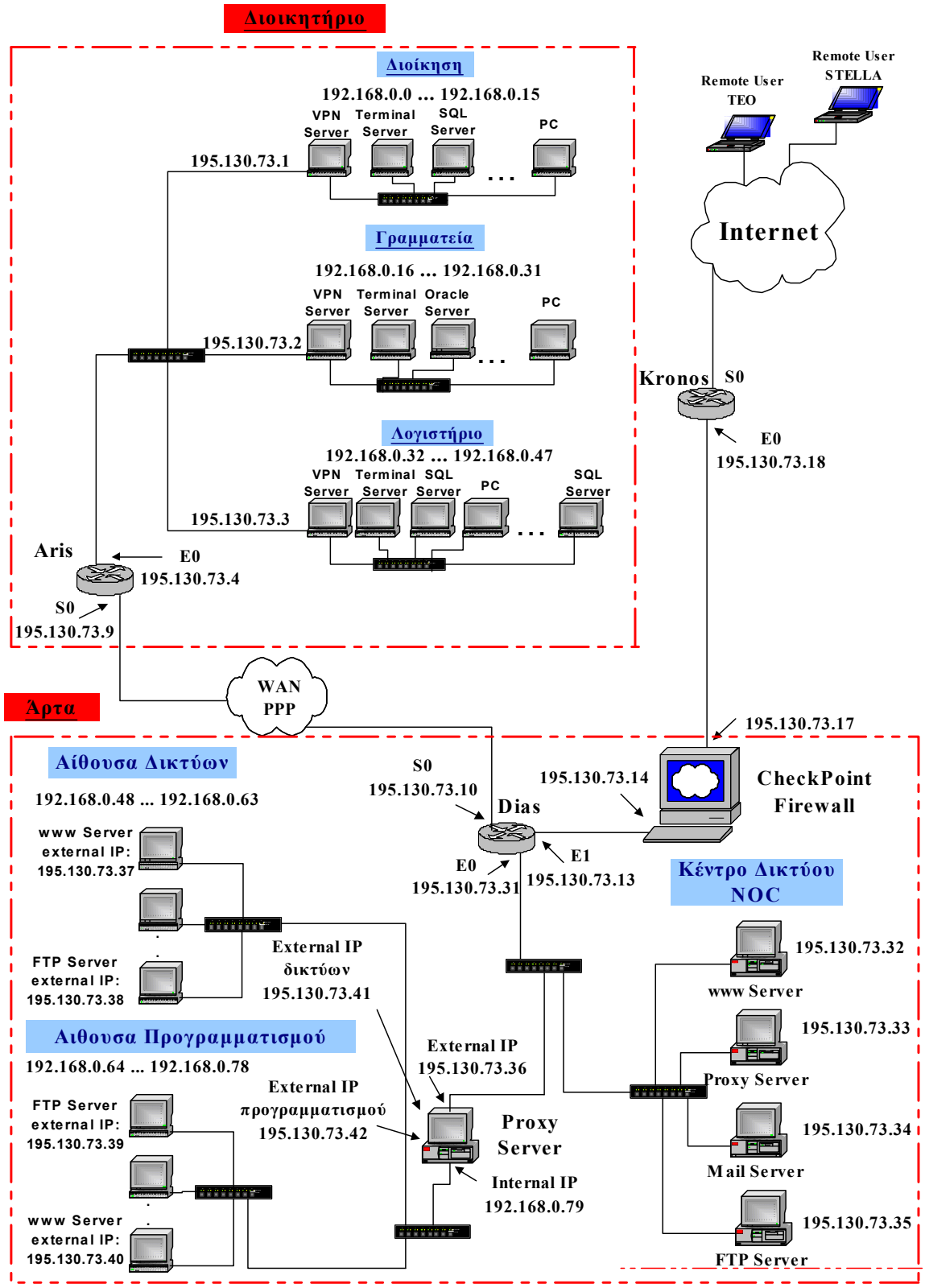
Πίνακας 4
Παράδειγμα κανόνα

7. Αν η διαμόρφωση περιλαμβάνει επικαλυμμένα, κρυπτογραφημένα domains, τότε καθορίζουμε έναν κανόνα που επιτρέπει πρόσβαση μέσω του εξωτερικού VPN/Firewall module.
8. Εγκαθιστούμε την πολιτική ασφάλειας. Επίσης θα εγκαταστήσουμε την Desktop πολιτική στον policy Server.
9. Οι SecureClient χρήστες «κατεβάζουν» την desktop πολιτική.

12 Case study

Το case study όπως φαίνεται στην Εικόνα 29, περιλαμβάνει τα εξής:

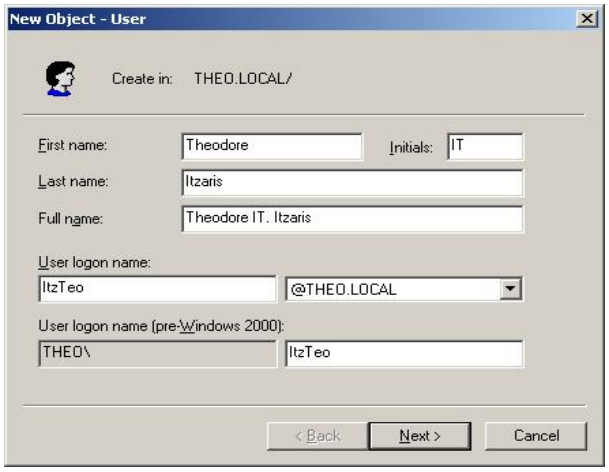
- Ένα LAN (Διοικητήριο) το οποίο αποτελείται από τρία υποδίκτυα (Διοίκηση, Γραμματεία, Λογιστήριο) με εσωτερικές διευθύνσεις Class C, τα οποία αποτελούνται από 16 hosts. Σε κάθε γραφείο υπάρχει ένας VPN Server, ο οποίος χρησιμοποιείται για να πιστοποιεί τους remote χρήστες που θέλουν να έχουν πρόσβαση σε κάποιες εφαρμογές του VPN δικτύου (χρησιμοποιώντας το πρωτόκολλο PPTP), όπως στους SQL ή Oracle Servers. Επίσης, υπάρχει ένας Terminal Server ο οποίος τρέχει την εφαρμογή και επιστρέφει τα αποτελέσματα στους remote χρήστες. Ακόμη, έχουμε δημιουργήσει ένα group από εξωτερικούς χρήστες και τους έχουμε δώσει δικαιώματα πρόσβασης στα VPN δίκτυα.
- Ένα LAN (Άρτα) το οποίο αποτελείται από δύο υποδίκτυα (αίθουσα δικτύων, αίθουσα προγραμματισμού) με εσωτερικές διευθύνσεις Class C τα οποία προστατεύονται από έναν Proxy Server και από ένα υποδίκτυο (κέντρο δικτύου) που περιλαμβάνει έναν WWW, έναν Proxy, έναν FTP και έναν Mail Server με εξωτερικές διευθύνσεις, στους οποίους μπορούν να έχουν πρόσβαση όλοι οι χρήστες.
- Ένα Checkpoint Firewall, στο οποίο έχουμε αναπτύξει μια πολιτική ασφάλειας η οποία προστατεύει τα δύο LANs από μη εξουσιοδοτημένη πρόσβαση και αποτρέπει την εσωτερική επίθεση σε κάποιες υπηρεσίες ή εφαρμογές.
- Τρεις routers: Ένας router (Kronos), ο οποίος δρομολογεί τα εξερχόμενα πακέτα στο Internet και στέλνει τα εισερχόμενα στον επόμενο router με στατική δρομολόγηση. Ένας router (Dias), ο οποίος δρομολογεί τα εισερχόμενα πακέτα στα κατάλληλα υποδίκτυα του δικτύου της Άρτας και επιτυγχάνει μια WAN σύνδεση χρησιμοποιώντας το πρωτόκολλο PPP με το δίκτυο του διοικητηρίου. Ένας router (Aris), ο οποίος δρομολογεί τα εισερχόμενα και εξερχόμενα πακέτα στα κατάλληλα υποδίκτυα του διοικητηρίου.



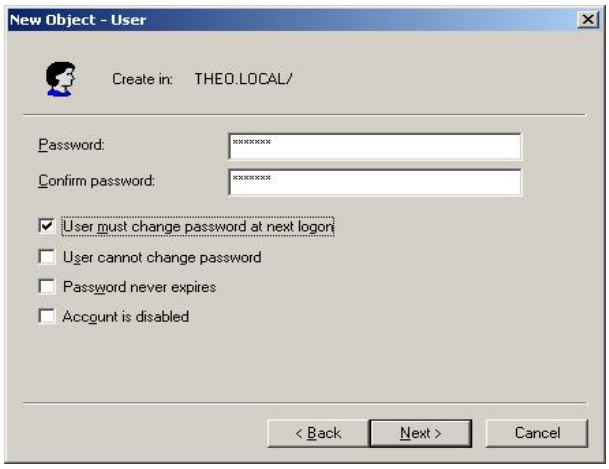
Εικόνα 29
Σχέδιο του case study

Για να μπορέσει κάποιος χρήστης να μπει απομακρυσμένα στο υποδίκτυο της Γραμματείας, κάνουμε τα εξής βήματα:

- Δημιουργούμε χρήστες τους οποίους θα βάλουμε σε group, όπως φαίνεται στις Εικόνες 30-31.

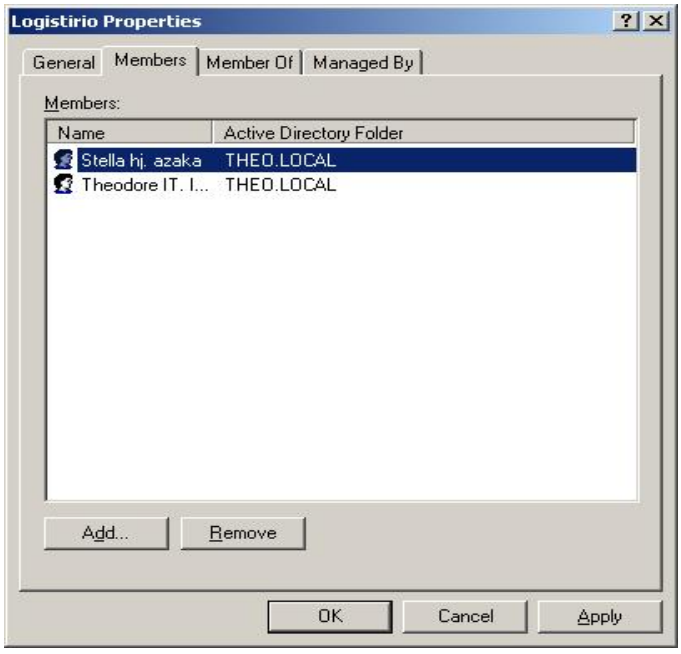


Εικόνα 30
Δημιουργία χρήστη



Εικόνα 31
Εισαγωγή password

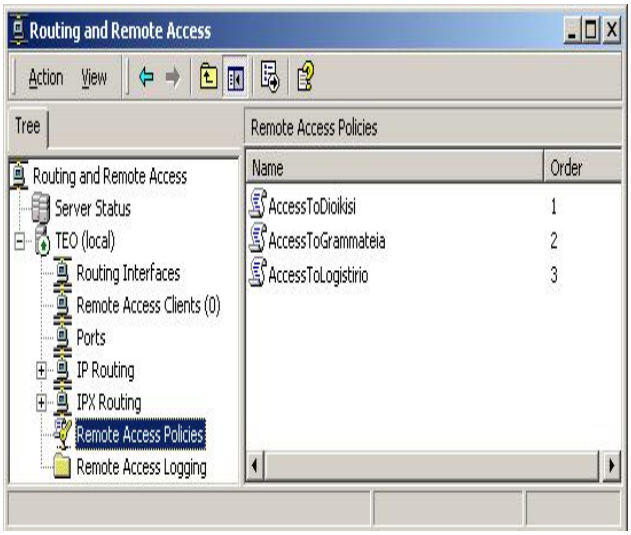
- Δημιουργούμε ένα group, στο οποίο βάζουμε τους χρήστες που δημιουργήσαμε, όπως φαίνεται στην Εικόνα 32.



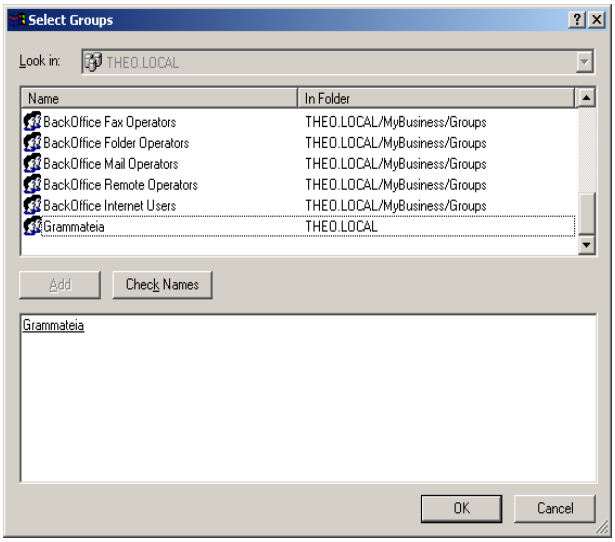
Εικόνα 32
Τοποθέτηση χρηστών σε group

- Αναπτύσσουμε πολιτικές στη διοίκηση, στη γραμματεία και στο λογιστήριο, όπως δείχνει η Εικόνα 33, στις οποίες προσθέτουμε τα groups που έχουμε

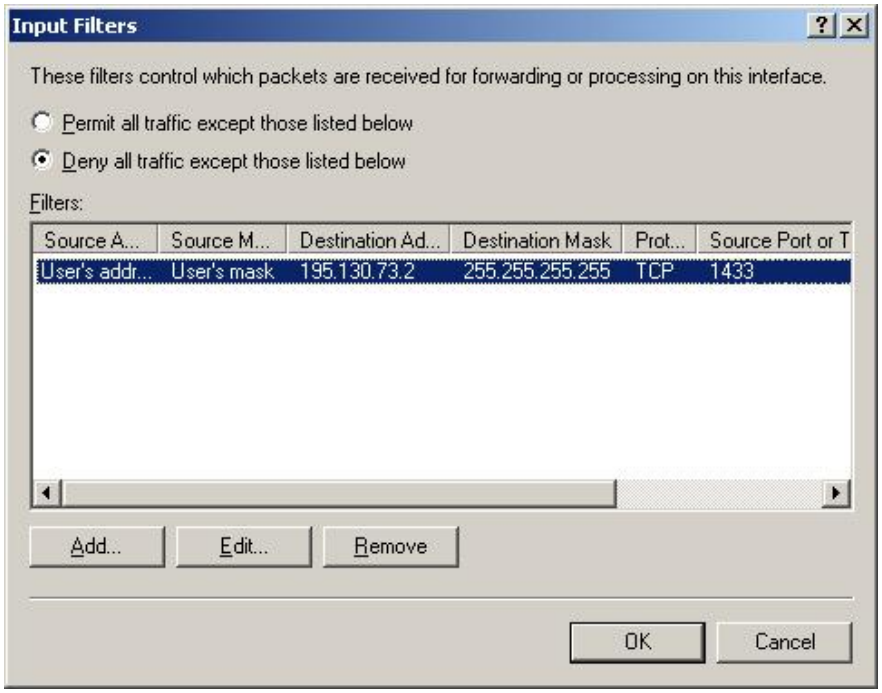
δημιουργήσει (Εικόνα 34). Στις πολιτικές αυτές, προκειμένου να τρέχουν οι απομακρυσμένοι χρήστες sql εφαρμογές έχουμε αφήσει ανοιχτό σε κάθε υποδίκτυο το port number 1433 και για oracle εφαρμογές το port number 1521, όπως φαίνεται στην Εικόνα 35.



Εικόνα 33
Δημιουργία πολιτικών πρόσβασης



Εικόνα 34
Επιλογή group



Εικόνα 35
Δημιουργία Φίλτρου

Κάθε VPN Server έχει δύο κάρτες δικτύου, δηλαδή μία εσωτερική και μία εξωτερική διεύθυνση, έτσι ώστε αν κάποιος απομακρυσμένος χρήστης θέλει να

τρέξει μια εφαρμογή του εσωτερικού δικτύου, συνδέεται στην εξωτερική διεύθυνση του VPN Server και βλέπει το εσωτερικό δίκτυο σαν να είναι συνδεδεμένος τοπικά. Επίσης ένας άλλος λόγος που χρησιμοποιούμε εσωτερικές διευθύνσεις, είναι για να μην μπορούν χρήστες από το Internet να βλέπουν άμεσα και να έχουν πρόσβαση σ' αυτά τα δίκτυα.

Για να προστατεύσουμε το κέντρο δικτύου από πιθανή εσωτερική επίθεση από τους χρήστες του διοικητηρίου, δημιουργούμε τα παρακάτω access lists στον router Dias:

```
access-list 101 permit tcp host 195.130.73.32 195.130.73.0 0.0.0.7 established
access-list 101 permit tcp host 195.130.73.34 195.130.73.0 0.0.0.7 established
access-list 101 permit tcp host 195.130.73.35 195.130.73.0 0.0.0.7 established
access-list 101 permit 195.130.73.0  0.0.0.7  host 195.130.73.32 eq 80
access-list 101 permit 195.130.73.0  0.0.0.7  host 195.130.73.34 eq 25
access-list 101 permit 195.130.73.0  0.0.0.7  host 195.130.73.35 eq 21
access-list 101 permit 195.130.73.0  0.0.0.7  host 195.130.73.37 eq 80
access-list 101 permit 195.130.73.0  0.0.0.7  host 195.130.73.38 eq 21
access-list 101 permit 195.130.73.0  0.0.0.7  host 195.130.73.39 eq 21
access-list 101 permit 195.130.73.0  0.0.0.7  host 195.130.73.40 eq 80
access-list 101 deny any any
```

Γραμμή 1: επιτρέπουμε τα TCP πακέτα από τον WWW Server στο δίκτυο του διοικητηρίου αν η σύνδεση έχει εγκαθιδρυθεί από το δίκτυο αυτό

Γραμμή 2: επιτρέπουμε τα TCP πακέτα από τον Mail Server στο δίκτυο του διοικητηρίου αν η σύνδεση έχει εγκαθιδρυθεί από το δίκτυο αυτό

Γραμμή 3: επιτρέπουμε τα TCP πακέτα από τον FTP Server στο δίκτυο του διοικητηρίου αν η σύνδεση έχει εγκαθιδρυθεί από το δίκτυο αυτό

Γραμμή 4: επιτρέπουμε στο δίκτυο 195.130.73.0 την πρόσβαση στον web Server του NOC μέσω του port 80

Γραμμή 5: επιτρέπουμε στο δίκτυο 195.130.73.0 την πρόσβαση στον mail Server του NOC μέσω του port 25

Γραμμή 6: επιτρέπουμε στο δίκτυο 195.130.73.0 την πρόσβαση στον ftp Server του NOC μέσω του port 21

Γραμμή 7: επιτρέπουμε στο δίκτυο 195.130.73.0 την πρόσβαση στον web Server της αίθουσας Δικτύων μέσω του port 80
Γραμμή 8: επιτρέπουμε στο δίκτυο 195.130.73.0 την πρόσβαση στον ftp Server της αίθουσας Δικτύων μέσω του port 21
Γραμμή 9: επιτρέπουμε στο δίκτυο 195.130.73.0 την πρόσβαση στον web Server της αίθουσας Προγραμματισμού μέσω του port 80
Γραμμή 10: επιτρέπουμε στο δίκτυο 195.130.73.0 την πρόσβαση στον ftp Server της αίθουσας Προγραμματισμού μέσω του port 21
Γραμμή 11: απορρίπτουμε όλα τα υπόλοιπα πακέτα

Για να ενεργοποιηθούν τα access-lists στο Interface E0 του router Dias για τα εισερχόμενα πακέτα, δίνουμε τις εξής εντολές:

Interface E0
Ip access-group 101 in

Τα φίλτρα πακέτων που έγιναν στον Proxy Server του υποδικτύου της Άρτας όπως φαίνεται στην Εικόνα 36, είναι τα εξής :

- ***AccessToFtp :*** σ' αυτό το φίλτρο επιτρέπουμε όλα τα εισερχόμενα πακέτα από το δίκτυο 195.130.73.0/29 (Διοικητήριο) στον Ftp Server της αίθουσας δικτύων.
- ***AccessToWWW :*** σ' αυτό το φίλτρο επιτρέπουμε όλα τα εισερχόμενα πακέτα από το δίκτυο 195.130.73.0/29 (Διοικητήριο) στον Web Server της αίθουσας δικτύων.
- ***FTPSvr:*** σ' αυτό το φίλτρο επιτρέπουμε την αμφίδρομη επικοινωνία των TCP πακέτων στο port number 21 , μεταξύ του Ftp server της αίθουσας δικτύων και του FTP server του NOC.
- ***MailSrv:*** σ' αυτό το φίλτρο επιτρέπουμε τα εισερχόμενα TCP πακέτα στο port number 25 , από τον υπολογιστή 195.130.73.34(Mail server) στο υποδίκτυο της αίθουσας προγραμματισμού με την εξωτερική διεύθυνση του proxy server 195.130.73.42 .
- ***NoChat:*** σ' αυτό το φίλτρο απαγορεύουμε την χρήση του chat στο

υποδίκτυο της αίθουσας προγραμματισμού με την εξωτερική διεύθυνση του proxy server 195.130.73.42 από οποιονδήποτε βρίσκεται εκτός του δικτύου αυτού

- ***NoPing:*** σ' αυτό το φίλτρο απαγορεύουμε την χρήση της εντολής ping στο υποδίκτυο της αίθουσας προγραμματισμού με την εξωτερική διεύθυνση του proxy server 195.130.73.42 από οποιονδήποτε βρίσκεται εκτός του δικτύου αυτού

Name	Mode	Filter type	Local computer	Remote computer	Protocol	Direction	Local Port	Remote Port
AccessToFTP	Allow	Custom filter	Internal machine - 195.130.73.38	195.130.73.0 255.255.255.248	TCP	Both	21	21
AccessToWWW	Allow	HTTP server (port 80)	Internal machine - 195.130.73.37	195.130.73.0 255.255.255.248	TCP	Inbound	80	All ports
FTPSrv	Allow	Custom filter	Internal machine - 195.130.73.38	195.130.73.35	TCP	Both	21	21
MailSrv	Allow	Custom filter	Internal machine - 195.130.73.42	195.130.73.34	TCP	Inbound	25	All ports
NoChat	Block	Custom filter	Internal machine - 195.130.73.42	Any	UDP	Both	194	194
NoPing	Block	ICMP ping query	Internal machine - 195.130.73.42	Any	ICMP	Inbound		

Εικόνα 36
Δημιουργία φίλτρων πακέτων

Δημιουργούμε τα εξής αντικείμενα :

- ***LocalDioikitirio:*** περιλαμβάνει τις IP διευθύνσεις των VPN Server του λογιστηρίου, της γραμματείας και της διοίκησης.
- ***NOC:*** περιλαμβάνει τις IP διευθύνσεις των www, Proxy, mail και ftp Server.
- ***FWall:*** είναι ο υπολογιστής στον οποίο έχει εγκατασταθεί το Check point firewall.

Στον Πίνακα 5, φαίνεται η πολιτική ασφάλειας που ακολουθούμε γι' αυτό το case.

No	Source	Destination	Service	Action	Track	Install on
1	Any	FWall	Any	Reject	alert	Firewall Gateway
2	LocalDioikitirio	Any	ICMP Irc	reject	long	Firewall Gateway
3	LocalDioikitirio	Any	Any	accept	long	Firewall Gateway
4	AllUsers@any	LocalDioikitirio	Any	userauth	long	Firewall Gateway
5	AllUsers@any	Any	telnet	UserAuth	Long	Firewall Gateway
6	Any	NOC	Smtp, WWW, Ftp	accept	short	Firewall Gateway
7	Any	NOC	Any	drop	short	Firewall Gateway
8	NOC	Any	Any	accept	long	Firewall Gateway
9	Any	Any	Any	drop	long	Firewall Gateway

Πίνακας 5
Πολιτική ασφάλειας

Στον πρώτο κανόνα απορρίπτουμε οποιαδήποτε άμεση σύνδεση γίνεται στον υπολογιστή που είναι εγκατεστημένο το firewall.

Στον δεύτερο κανόνα απορρίπτουμε τα ICMP μηνύματα και το chat από τους χρήστες του διοικητηρίου προς οποιονδήποτε άλλο.

Στον τρίτο κανόνα δεχόμαστε όλες τις υπόλοιπες συνδέσεις που γίνονται από τους χρήστες του διοικητηρίου προς οποιονδήποτε.

Στον τέταρτο κανόνα γίνεται πρώτα πιστοποίηση των εξωτερικών χρηστών και μετά τους επιτρέπεται η πρόσβαση στο διοικητήριο.

Στον πέμπτο κανόνα γίνεται πρώτα πιστοποίηση των εξωτερικών χρηστών και μετά τους επιτρέπεται να κάνουν Telnet.

Στον έκτο κανόνα επιτρέπουμε σε οποιονδήποτε το Ftp, το www και να στέλνει email στο NOC.

Στον έβδομο κανόνα απαγορεύουμε όλες τις υπόλοιπες υπηρεσίες μπαίνουν στο NOC.

Στον όγδοο κανόνα επιτρέπουμε όλες τις υπηρεσίες από το NOC προς οποιαδήποτε κατεύθυνση.

Στον ένατο κανόνα απορρίπτουμε όλες τις υπηρεσίες από οποιαδήποτε κατεύθυνση προς οποιαδήποτε κατεύθυνση χωρίς να ενημερώνεται αυτός που επιχειρεί να κάνει τη σύνδεση.

Επίλογος

Στην παρούσα εργασία παρουσιάσαμε την έννοια της ασφάλειας δικτύων, τους βασικούς της όρους καθώς και τους σημαντικότερους και επικρατέστερους τρόπους ασφάλισης των δικτύων. Περιγράψαμε διάφορους τρόπους με τους οποίους μπορεί να απειληθεί ένα δίκτυο και τις μεθόδους αντιμετώπισης τους, με τη χρήση του Proxy Server, των VPNs και των firewalls. Τέλος έγινε ανάλυση ενός case study στο οποίο φαίνεται ένας τρόπος ασφάλισης δικτύου με παράλληλη χρήση Proxy Server, VPNs και firewall.

Πάνω από όλα όμως δείξαμε την αναγκαιότητα της ασφάλειας σε ατομικό και συλλογικό επίπεδο, στην υπεράσπιση δικαιωμάτων του απλού πολίτη και την απόκρυψη υπερπολύτιμων δεδομένων επιχειρήσεων και οργανισμών. Εκεί έγκειται η δύναμη της ασφάλειας, στις ανάγκες που εξυπηρετεί και τις λειτουργίες που πραγματώνει και όχι στους αλγορίθμους που διαρκώς βελτιώνονται για να την ισχυροποιήσουν.

Το μέλλον στον τομέα απόκρυψης δεδομένων είναι ευοίωνο και οι τεχνολογικές εξελίξεις του πρόσφατου παρελθόντος αποτελούν τα εχέγγυα για ισχυρότερη ασφάλεια, για ισχυρότερη προστασία της ελευθερίας.

ΒΙΒΛΙΟΓΡΑΦΙΑ

1. “Check Point Getting Started Guide”
CheckPoint Software Technologies Ltd.
Internet Security Systems, Inc - 2000

2. “Check Point™ Virtual Private Networks”
CheckPoint Software Technologies Ltd.
Internet Security Systems, Inc - 2000

3. “Check Point™ VPN-1/Firewall-1® Administration Guide”
CheckPoint Software Technologies Ltd.
Internet Security Systems, Inc - 2000

4. “DHCP for Windows 2000”
Alcott Neall
O’ Reilly & Associates, Inc – 2001

5. “Firewall and Proxy Server HOWTO, http://www.grennan.com/Firewall-HOWTO.html

6. “Microsoft® Proxy Server 2.0 MCSE Study System”
Simmons Curt
IDG Books Worldwide, Inc - 1999

7. “Security in computing”
Pfleeger Charles P.
1996

8. “Web Proxy Servers”