Τ.Ε.Ι. ΗΠΕΙΡΟΥ
ΣΧΟΛΗ ΔΙΟΙΚΗΣΗΣ ΚΑΙ ΟΙΚΟΝΟΜΙΑΣ (Σ.Δ.Ο.)
ΤΜΗΜΑ ΤΗΛΕΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΔΙΟΙΚΗΣΗΣ

ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ – ΑΝΤΙΠΥΡΙΚΗ ΖΩΝΗ ΠΡΟΣΤΑΣΙΑΣ (FIREWALL)

ΓΚΙΩΡΓΚΑΣ ΙΩΑΝΝΗΣ

ΙΑΝΟΥΑΡΙΟΣ 2005
ΑΡΤΑ

ΠΕΡΙΕΧΟΜΕΝΑ

ΚΕΦΑΛΑΙΟ 1^{Ο} : ΕΙΣΑΓΩΓΗ ΣΤΑ ΣΥΣΤΗΜΑΤΑ FIREWALL

1.1 Ορισμός ενός firewall

Ένα firewall είναι ένα σύστημα ή μια ομάδα συστημάτων τα οποία επιβάλλουν μία πολιτική ελέγχου πρόσβασης στην κυκλοφορία του δικτύου καθώς διέρχεται από συγκεκριμένα σημεία πρόσβασης. Αφού καθορίσετε τα επίπεδα διασύνδεσης που θέλετε να παρέχετε, είναι ευθύνη του firewall να διασφαλίσει ότι επιτρέπεται πρόσβαση μόνο μέσα στο εύρος που έχετε καθορίσει. Είναι επίσης ευθύνη του firewall να διασφαλίζει ότι η πολιτική ελέγχου πρόσβασης που καθορίσατε τηρείται απ' όλους τους χρήστες του δικτύου.[1]

Με άλλα λόγια ένα firewall είναι ουσιαστικά ένα πρόγραμμα το οποίο "φιλτράρει" τις πληροφορίες που δέχεται και στέλνει ο υπολογιστής σας μέσω του Internet. Αν κάποιο πακέτο δεδομένων έχει οριστεί ως απαγορευμένο από τα "φίλτρα" του προγράμματος, τότε το συγκεκριμένο πακέτο δεν περνάει. Αυτό σημαίνει αυτόματα πως δεν μπορεί να περάσει στον υπολογιστή σας κανένα επικίνδυνο πακέτο δεδομένων, που μπορεί να βλάψει τον υπολογιστή σας ή το τοπικό σας δίκτυο.[2]

Τα firewalls μοιάζουν με άλλες συσκευές του δικτύου στο ότι ο σκοπός τους είναι να ελέγχουν την ροή της κυκλοφορίας. Ωστόσο, ανόμοια με άλλες συσκευές του δικτύου, ένα firewall πρέπει να ελέγχει την κυκλοφορία λαμβάνοντας ταυτόχρονα υπόψη ότι τα πακέτα δεδομένων που βλέπει μπορεί να μην είναι αυτό που δείχνουν με την πρώτη ματιά.[3]

Ωστόσο, ένα firewall πρέπει να υποθέτει ότι μπορεί να υπάρχουν συστήματα τα οποία θα προσπαθήσουν να το ξεγελάσουν για να υποκλέψουν τις πληροφορίες που περνούν από αυτό. Ένα firewall δεν μπορεί να στηρίζεται πάντα στους κανόνες επικοινωνίας του δικτύου· αντίθετα, θα πρέπει να υποψιάζεται πάντα ότι οι κανόνες αυτοί μπορεί να μην ακολουθούνται. Το σκεπτικό αυτό δημιουργεί πολλές δυσκολίες στην σχεδίαση των συστημάτων firewall, τα οποία πρέπει να είναι προετοιμασμένα για κάθε ενδεχόμενο.[3]

1.2 Πότε χρειάζεται ένα firewall

Τις περισσότερες φορές τα firewalls χρησιμοποιούνται για τον έλεγχο της πρόσβασης μεταξύ του εσωτερικού δικτύου ενός οργανισμού και του Internet, αλλά καθώς τα όρια των εσωτερικών δικτύων γίνονται ολοένα και πιο δυσδιάκριτα (λόγω της προσθήκης των ασύρματων δικτύων, των συνδέσεων VPN με απομακρυσμένους υπολογιστές και των extranet) και ο όγκος του κακόβουλου κώδικα που κυκλοφορεί στο

Internet ολοένα και αυξάνεται, τα firewalls έχουν αρχίσει πλέον να θεωρούνται σαν μία βασική λειτουργία η οποία προστίθεται σε κάθε υπολογιστή που συνδέεται σε δίκτυα. Ωστόσο, υπάρχουν περιπτώσεις στις οποίες τα firewalls είναι απολύτως απαραίτητα.[3]

1.2.1 Εισερχόμενες συνδέσεις μέσω μόντεμ και VPN

Ένα firewall μπορεί να χρησιμοποιηθεί για τον έλεγχο της πρόσβασης εισερχόμενων συνδέσεων μέσω μιας ομάδας μόντεμ ή VPN (virtual private network). Για παράδειγμα, ένας οργανισμός μπορεί να έχει μια πολιτική ελέγχου πρόσβασης η οποία συμβουλεύει ότι οι χρήστες που συνδέονται μέσω μόντεμ θα μπορούν να προσπελάζουν μόνο ένα σύστημα ηλεκτρονικού ταχυδρομείου. Επειδή ο οργανισμός δεν θέλει να επιτρέπει την πρόσβαση αυτών των χρηστών στους άλλους servers του δικτύου του ή στο Internet μπορεί να χρησιμοποιήσει για την υλοποίηση αυτής της πολιτικής ένα firewall.[3]

1.2.2 Εξωτερικές συνδέσεις με επαγγελματικούς συνεργάτες

Στην πλειονότητα τους οι οργανισμοί διατηρούν μόνιμες συνδέσεις προς τις απομακρυσμένες εγκαταστάσεις των επαγγελματικών τους συνεργατών. Αυτή είναι μία δύσκολη περίπτωση ως προς την ασφάλεια. Η σύνδεση είναι απαραίτητη στις δύο επιχειρήσεις, αλλά τώρα πια υπάρχουν κάποιοι οι οποίοι έχουν πρόσβαση στο δίκτυο τους από μία περιοχή στην οποία η ασφάλεια δεν ελέγχεται από το δικό τους οργανισμό. Σ' αυτή την περίπτωση μπορεί να χρησιμοποιηθεί ένα firewall για να κάνει τον έλεγχο της πρόσβασης των εξωτερικών χρηστών μέσω αυτών των συνδέσεων και την καταγραφή των ενεργειών τους.[4]

1.2.3 Μεταξύ τμημάτων του ίδιου οργανισμού

Ορισμένοι οργανισμοί (π.χ. χρηματιστηριακές εταιρείες) χρειάζονται επίσης firewalls μεταξύ των διαφόρων τομέων του εσωτερικού δικτύου. Αυτά τα firewalls χρησιμοποιούνται για να εξασφαλίσουν ότι οι εσωτερικοί χρήστες του οργανισμού έχουν πρόσβαση μόνο στις πληροφορίες που χρειάζονται πραγματικά.[4]

1.2.4 Συγκεκριμένα συστήματα

Επειδή σωστή άμυνα που θα πρέπει να ακολουθεί μία προσέγγιση πολλαπλών επιπέδων, υπάρχει η δυνατότητα να προστεθεί λειτουργικότητα firewall σε επίπεδο λογισμικού σε καθορισμένα συστήματα – servers ή σταθμούς εργασίας – ακόμη κι αν αυτά τα συστήματα συνδέονται σε δίκτυα ήδη προστατευμένα από το Internet μέσω ενός

firewall. Εξαιτίας των φθηνών, βασιζόμενων σε λογισμικό προϊόντων firewall όπως το ZoneAlarm, ακόμη και τα συστήματα τα οποία δεν τρέχουν πρωταρχικής σημασίας εφαρμογές ή δεν αποθηκεύουν σημαντικά δεδομένα μπορούν να προστατεύονται από μία πρόσθετη γραμμή άμυνας.[4]

1.3 Λειτουργίες των συστημάτων firewall

Στην εποχή μας τα περισσότερα firewall χρησιμοποιούν έναν συνδυασμό λειτουργιών για την προστασία των δικτύων από την εχθρική κυκλοφορία. Οι δημοφιλέστερες από αυτές είναι[5]:

1) Στατικό φιλτράρισμα πακέτων (static packet filtering)
2) Δυναμικό φιλτράρισμα πακέτων (dynamic packet filtering)
3) Φιλτράρισμα βάση κατάστασης (stateful filtering)
4) Διακομιστές μεσολάβησης (proxy)

1.3.1 Στατικό φιλτράρισμα πακέτων

Το στατικό φιλτράρισμα πακέτων ελέγχει την κυκλοφορία του δικτύου χρησιμοποιώντας τις πληροφορίες που είναι αποθηκευμένες στις κεφαλίδες των πακέτων. Καθώς τα πακέτα λαμβάνονται από την συσκευή που εκτελεί το φιλτράρισμα, οι παράμετροι που περιέχονται στις κεφαλίδες των πακέτων συγκρίνονται έναντι της πολιτικής ελέγχου πρόσβασης – η οποία αναφέρεται σαν λίστα ελέγχου πρόσβασης (access control list ή ACL). Ανάλογα με το αποτέλεσμα αυτή της σύγκρισης, η συσκευή φιλτραρίσματος επιτρέπει ή απαγορεύει την διέλευση της κυκλοφορίας.

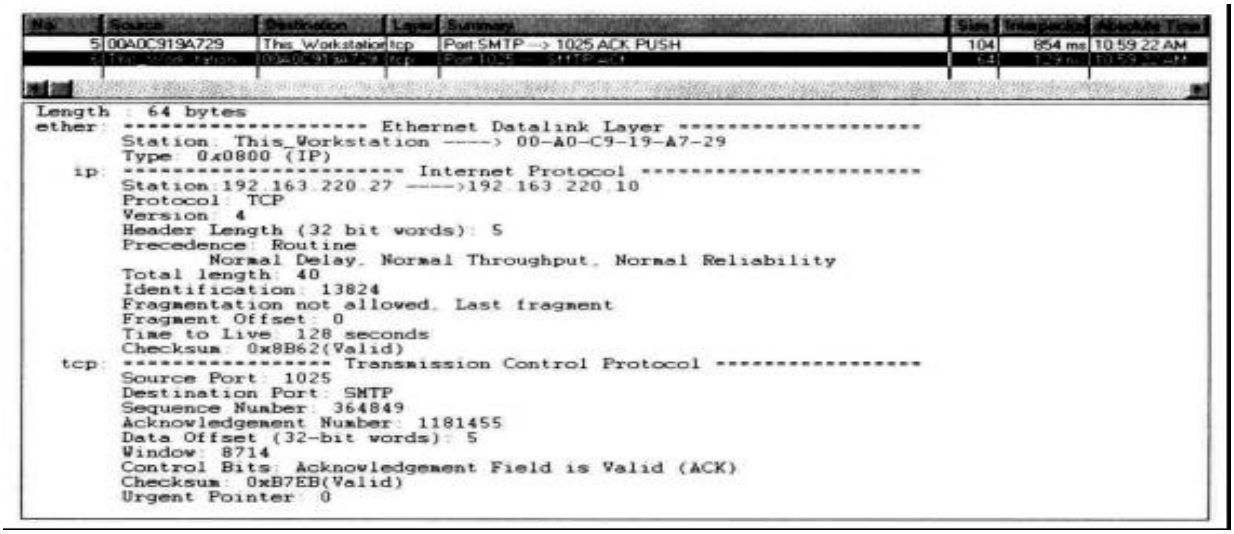
Ένα στατικό φίλτρο πακέτων μπορεί να χρησιμοποιεί τις ακόλουθες πληροφορίες όταν ελέγχει την ροή της κυκλοφορίας στο δίκτυο[6]:

1) Διεύθυνση IP ή υπο-δίκτυο προορισμού
2) Διεύθυνση IP ή υπο-δίκτυο προέλευσης
3) Θύρα υπηρεσίας στον προορισμό
4) Θύρα υπηρεσίας στην προέλευση
5) Σήμανση (μόνο στο TCP)

1.3.2 Το πεδίο σημάνσεων του TCP

Όταν χρησιμοποιείται το TCP σαν πρωτόκολλο μεταφοράς, οι συσκευές που χρησιμοποιούν στατικό φιλτράρισμα πακέτων μπορούν να εξετάζουν το πεδίο σημάνσεων (flag) της κεφαλίδας του TCP για να λαμβάνουν αποφάσεις σχετικά με τον

έλεγχο της κυκλοφορίας του δικτύου. Η εικόνα 1.1 παρουσιάζει την αποκωδικοποίηση ενός πακέτου TCP/IP. Το πεδίο Control Bits καθορίζει ποιες σημάνσεις έχουν οριστεί. Για τον ορισμό των σημάνσεων χρησιμοποιείται το δυαδικό σύστημα· μία ενεργοποιημένη σήμανση έχει τιμή 1, ενώ μία απενεργοποιημένη έχει τιμή 0.[6]



ΕΙΚΟΝΑ 1.1: Αποκωδικοποίηση ενός πακέτου του TCP/IP. [6]

Οι διάφορες τιμές σημάνσεων χρησιμοποιούνται για τον προσδιορισμό διαφορετικών απόψεων μιας συνόδου επικοινωνίας. Το πεδίο σημάνσεων δίνει στους υπολογιστές που λαμβάνουν λίγες επιπλέον πληροφορίες για τα δεδομένα που μεταφέρουν τα πακέτα. Ο πίνακας 1.1 παρουσιάζει τις έγκυρες σημάνσεις και τις χρήσεις τους.[7]

ΠΙΝΑΚΑΣ 1.1: Έγκυρες σημάνσεις του TCP/IP [7]

Σήμανση του TCP	Περιγραφή
ACK (Acknowledgement)	Υποδεικνύει ότι τα εν λόγω δεδομένα είναι μία απάντηση σε μία αίτηση δεδομένων και ότι υπάρχουν χρήσιμες πληροφορίες στο πεδίο Acknowledgement Number.
FIN (Final)	Υποδεικνύει ότι το σύστημα αποστολής επιθυμεί να τερματίσει την τρέχουσα σύνοδο επικοινωνίας. Τυπικά, σε μία σύνοδο επικοινωνίας κάθε εμπλεκόμενο σύστημα στέλνει μία σήμανση FIN πριν κλείσει πραγματικά την σύνδεση.
PSH (Push)	Εμποδίζει το σύστημα αποστολής να τοποθετήσει τα δεδομένα σε ουρά πριν από την μετάδοση. Σε πολλές περιπτώσεις είναι πιο αποτελεσματικό να επιτρέπετε στο σύστημα αποστολής να τοποθετεί σε ουρά μικρές ποσότητες δεδομένων πριν από την μετάδοση, έτσι ώστε να δημιουργούνται λιγότερα πακέτα. Στην πλευρά του παραλήπτη, η σήμανση Push λέει στο απομακρυσμένο σύστημα να μην τοποθετήσει σε ουρά τα δεδομένα, αλλά να στείλει απευθείας τις πληροφορίες στα πρωτόκολλα των ανώτερων επιπέδων.
RST (Reset)	Αρχικοποιεί την κατάσταση της τρέχουσας συνόδου επικοινωνίας. Η σήμανση Reset χρησιμοποιείται όταν λαμβάνει χώρα ένα μη-αναστρέψιμο πρόβλημα κατά την μετάδοση. Είναι ο τρόπος με τον οποίο το σύστημα αποστολής ρωτά τον παραλήπτη "Με άκουγες τόση ώρα; Να τα επαναλάβω;". Τέτοια προβλήματα προκαλούνται συνήθως από ένα σύστημα το οποίο είναι εκτός λειτουργίας.

SYN (Synchronize)	Χρησιμοποιείται κατά την αρχικοποίηση μιας συνόδου επικοινωνίας. Η σήμανση αυτή δεν θα πρέπει να ενεργοποιείται σε καμία άλλη φάση της διαδικασίας επικοινωνίας.
URG (Urgent)	Υποδεικνύει ότι το σύστημα αποστολής θέλει να στείλει πληροφορίες υψηλής προτεραιότητας και ότι υπάρχουν χρήσιμες πληροφορίες στο πεδίο Urgent Pointer. Όταν ένα σύστημα λαμβάνει ένα πακέτο με ενεργοποιημένη την σήμανση Urgent, επεξεργάζεται τις πληροφορίες του πριν από οποιαδήποτε άλλα δεδομένα μπορεί να περιμένουν στην ουρά. Η διαδικασία αυτή αναφέρεται σαν επεξεργασία δεδομένων "εκτός σειράς" (out-of-band).

Το πεδίο των σημάνσεων παίζει πολύ σημαντικό ρόλο όταν χρησιμοποιείται μία συσκευή στατικού φιλτραρίσματος πακέτων, επειδή την βοηθάει να ελέγξει καλύτερα την κυκλοφορία του δικτύου. Αυτό οφείλεται στο γεγονός ότι τα συστήματα firewall σπανίως παίρνουν οδηγίες να μπλοκάρουν όλη την κυκλοφορία που προέρχεται από μία συγκεκριμένη θύρα ή προορίζεται για ένα συγκεκριμένο σύστημα. Για παράδειγμα, ένας οργανισμός μπορεί να έχει μία πολιτική ελέγχου πρόσβασης η οποία υπαγορεύει ότι "Οι εσωτερικοί χρήστες του οργανισμού μπορούν να προσπελάζουν οποιαδήποτε υπηρεσία προς το Internet, αλλά όλη η προερχόμενη από το Internet κυκλοφορία που κατευθύνεται στο εσωτερικό δίκτυο πρέπει να μπλοκάρεται". Αν και με την πρώτη ματιά κάποιος θα πίστευε ότι αυτή η λίστα ACL (Access Control List) μπλοκάρει όλη την κυκλοφορία που προέρχεται από το Internet, αυτό δεν ισχύει.[8]

Όλες οι μορφές επικοινωνίας αναλύονται σε μία διαδικασία. Όταν προσπελάζετε μία ιστοσελίδα Web site, κάνετε μία αίτηση για δεδομένα (βήμα 1) στην οποία το Web site απαντά επιστρέφοντας σας τα δεδομένα που ζητήσατε (βήμα 2). Αυτό σημαίνει ότι κατά την διάρκεια του βήματος 2 αναμένετε δεδομένα τα οποία θα αποσταλούν από το σύστημα του Internet σε ένα σύστημα του εσωτερικού σας δικτύου. Εάν παίρναμε κατά γράμμα το δεύτερο μισό της πολιτικής ελέγχου πρόσβασης ("…όλη η προερχόμενη από το Internet κυκλοφορία που κατευθύνεται στο εσωτερικό δίκτυο πρέπει να μπλοκάρεται"), οι απαντήσεις στις αιτήσεις μας δεν θα κατάφερναν να φθάσουν ποτέ στον υπολογιστή μας. Το firewall του δικτύου μας δεν θα επέτρεπε μία πλήρη σύνοδο επικοινωνίας με το Web site.[9]

1.3.3 Σαρωτές FIN

Αφού ένα απλό φίλτρο πακέτων έχει τη δυνατότητα να εμποδίζει την σάρωση θυρών, ορισμένοι άνθρωποι αποφάσισαν να γίνουν πιο δημιουργικοί. Γι' αυτό οι απλοί σαρωτές θυρών εξελίχθηκαν σε σαρωτές FIN. Η λειτουργία ενός σαρωτή FIN βασίζεται στις ίδιες αρχές όπως οι σαρωτές θυρών (Οι σαρωτές θυρών μπορούν να εξετάζουν έναν υπολογιστή για να εξακριβώσουν εάν οποιεσδήποτε θύρες είναι ανοικτές. Ένας σαρωτής θυρών στέλνει μία αίτηση σύνδεσης (SYN=1) σε όλες τις θύρες υπηρεσιών

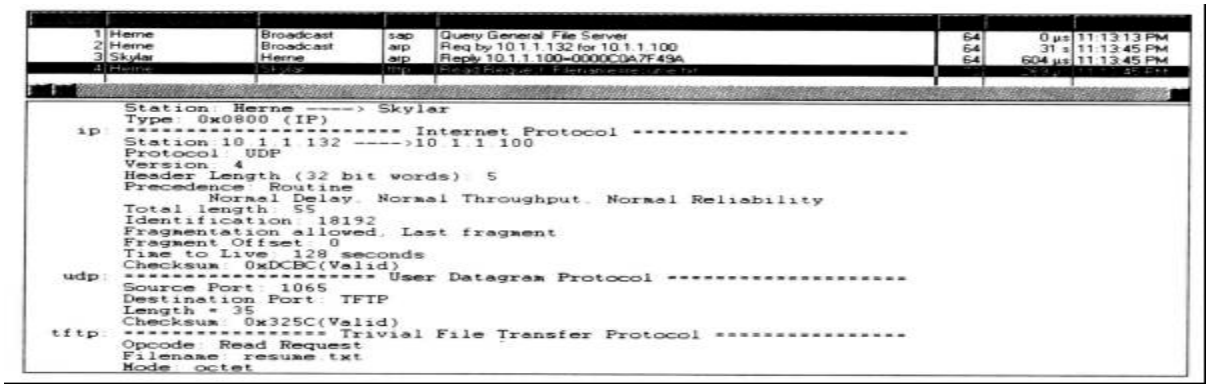
μέσα σε μία περιοχή τιμών.), εκτός από το γεγονός ότι τα μεταδιδόμενα πακέτα έχουν τις σημάνσεις FIN και ACK ορισμένες σε τιμή 1 και όλες τις υπόλοιπες σημάνσεις σε τιμή 0.[9]

Σε αυτή την περίπτωση, επειδή το φίλτρο πακέτων που χρησιμοποιούμε επιδιώκει να μπλοκάρει μόνο τα πακέτα που έχουν την σήμανση SYN=1 και όλες τις άλλες σημάνσεις σε τιμή 0, όλα τα προαναφερθέντα πακέτα περνούν από το φίλτρο. Το αποτέλεσμα που προκύπτει είναι ότι ένας εισβολέας μπορεί να αναλύσει την ροή των δεδομένων που επιστρέφει σ' αυτόν και να εξακριβώσει ποιοι υπολογιστές του δικτύου παρέχουν ποιες υπηρεσίες. Εάν ο υπολογιστής προορισμού επιστρέψει ACK=1, RST=1 (μία γενικευμένη απάντηση συστημάτων για ανύπαρκτες υπηρεσίες), το λογισμικό αντιλαμβάνεται ότι αυτή είναι μία μη-χρησιμοποιούμενη θύρα. Πάντως, εάν ο υπολογιστής προορισμού επιστρέψει ACK=1, FIN=1 (η υπηρεσία συμφωνεί να κλείσει την σύνδεση), ο σαρωτής FIN ξέρει ότι υπάρχει μία υπηρεσία που ακροάζεται σ' αυτή την θύρα. Αυτό σημαίνει ότι το φίλτρο πακέτων που χρησιμοποιούμε δεν μπορεί να αποκρούσει αυτούς τους σαρωτές.[9]

Επιπλέον, οι σαρωτές FIN μπορούν να χρησιμοποιηθούν για την αναγνώριση του λειτουργικού συστήματος του απομακρυσμένου υπολογιστή. Αυτό είναι δυνατό επειδή κάθε κατασκευαστής υλοποιεί το TCP/IP ελαφρώς διαφορετικά, πράγμα το οποίο έχει σαν αποτέλεσμα ένα μοναδικό "αποτύπωμα".[9]

1.3.4 Φιλτράρισμα πακέτων του πρωτοκόλλου UDP

Μπορεί να ήταν αρκετά δύσκολος ο έλεγχος της κυκλοφορίας στο επίπεδο του πρωτοκόλλου TCP, η κυκλοφορία στο επίπεδο του πρωτοκόλλου UDP είναι ακόμη χειρότερη. Αυτό οφείλεται στο γεγονός ότι το UDP παρέχει ακόμη λιγότερες πληροφορίες σχετικά με την κατάσταση μιας σύνδεσης από το TCP. Η εικόνα 1.2 παρουσιάζει την αποκωδικοποίηση της κεφαλίδας ενός πακέτου UDP.[10]



ΕΙΚΟΝΑ 1.2 : Η κωδικοποίηση της κεφαλίδας ενός πακέτου UDP.[11]

Παρατηρήστε ότι η κεφαλίδα του πακέτου UDP δεν χρησιμοποιεί σημάνσεις για να υποδείξει την κατάσταση μιας συνόδου επικοινωνίας. Αυτό σημαίνει ότι δεν υπάρχει τρόπος για να καθορίσουμε εάν ένα πακέτο αντιπροσωπεύει μία αίτηση για δεδομένα, ή μία απάντηση σε μία προηγούμενη αίτηση. Οι μόνες πληροφορίες που μπορούν να χρησιμοποιηθούν για τον έλεγχο της κυκλοφορίας είναι ο αριθμός θύρας προέλευσης και προορισμού. Αλλά ακόμη και αυτές οι πληροφορίες έχουν ελάχιστη χρησιμότητα σε πολλές περιπτώσεις, επειδή ορισμένες υπηρεσίες χρησιμοποιούν τον ίδιο αριθμό θύρας προέλευσης και προορισμού.[10]

Για παράδειγμα, όταν δύο Domain Name Servers (DNS) ανταλλάσσουν πληροφορίες μεταξύ τους, χρησιμοποιούν την θύρα με αριθμό 53 σαν θύρα προέλευσης και προορισμού. Διαφορετικά με πολλές άλλες υπηρεσίες, δεν χρησιμοποιούν σαν θύρα απάντησης μία θύρα με αριθμό μεγαλύτερο από 1023. Αυτό σημαίνει ότι ένα στατικό φίλτρο πακέτων δεν έχει κάποιο αποτελεσματικό μέσο για να περιορίσει την κυκλοφορία DNS μόνο προς μία κατεύθυνση. Δεν μπορείτε να μπλοκάρουμε την εισερχόμενη κυκλοφορία στην θύρα 53, επειδή η ενέργεια αυτή θα παρεμπόδιζε την αποστολή τόσο των απαντητικών μηνυμάτων, όσο και των αιτήσεων για δεδομένα.[11]

Για αυτό τον λόγο, σε πολλές περιπτώσεις, το μόνο αποτελεσματικό μέσο για τον έλεγχο της κυκλοφορίας του UDP με ένα στατικό φίλτρο πακέτων είναι είτε το μπλοκάρισμα της θύρας, είτε η ελεύθερη διέλευση της κυκλοφορίας με την ελπίδα ότι δεν θα συμβεί το χειρότερο. Οι περισσότεροι άνθρωποι προτιμούν την πρώτη λύση, εκτός κι αν αντιμετωπίζουν μία εξαιρετικά πιεστική ανάγκη για να επιτρέψουν την διέλευση κυκλοφορίας UDP.[11]

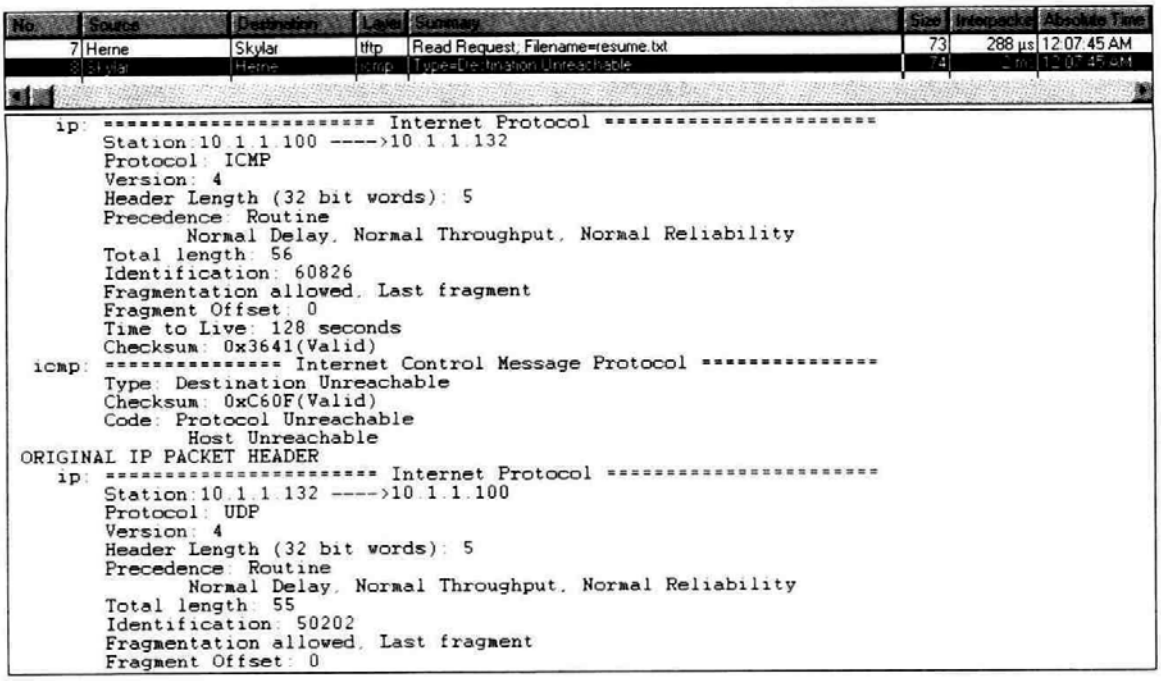
1.3.5 Φιλτράρισμα πακέτων του πρωτοκόλλου ICMP

Το ICMP (Internet Control Message Protocol, Πρωτόκολλο Ελέγχου Μηνυμάτων Διαδικτύου) παρέχει υποστήριξη για το πρωτόκολλο IP. Δεν χρησιμοποιείται για τηνμετάδοση δεδομένων από τους χρήστες, αλλά για εργασίες συντήρησης, οι οποίες διασφαλίζουν ότι τα πάντα λειτουργούν ομαλά. Η εικόνα 1.3 παρουσιάζει την αποκωδικοποίηση της κεφαλίδας ενός πακέτου ICMP.[11]

Το ICMP δεν χρησιμοποιεί θύρες υπηρεσιών. Υπάρχει ένα πεδίο Type το οποίο προσδιορίζει τον τύπο του πακέτου ICMP, καθώς και ένα πεδίο Code το οποίο παρέχει ακόμη πιο αναλυτικές πληροφορίες για την τρέχουσα σύνοδο. Για παράδειγμα, στην εικόνα 1.3 το πεδίο Code περιέχει την καταχώριση "Protocol Unreachable; Host Unreachable" (το πρωτόκολλο και το σύστημα host είναι απροσπέλαστα). Εάν συγκρίνετε την διεύθυνση IP προορισμού του πακέτου ICMP με την διεύθυνση IP

προορισμού στο τμήμα μετά το "Original IP Packet Header", θα παρατηρήσετε ότι είναι ίδιες (10.1.1.100). Επομένως, εάν ο προορισμός ήταν πραγματικά "απροσπέλαστος", πώς μπόρεσε να στείλει αυτή την απάντηση;[12]

Ο συνδυασμός αυτών των δύο τιμών στο πεδίο Code σημαίνει στην πραγματικότητα ότι η ζητούμενη υπηρεσία δεν ήταν διαθέσιμη. Ο πίνακας 1.2 περιγράφει τις τιμές των πεδίων των πακέτων ICMP.[13]



ΕΙΚΟΝΑ 1.3 : Η αποκωδικοποίηση της κεφαλίδας ενός πακέτου ICMP.[13]

ΠΙΝΑΚΑΣ 1.2 : Περιγραφή των τιμών του πεδίου Type στα πακέτα ICMP [14]

Type	Όνομα	Περιγραφή
0	Echo Reply	Απαντά σε αίτηση echo.
3	Destination	Υποδεικνύει ότι το υπο-δίκτυο, ο υπολογιστής, ή η υπηρεσία προορισμού δεν μπορούν να προσπελαστούν.
4	Source Quench	Υποδεικνύει ότι το σύστημα λήψης ή μία συσκευή δρομολόγησης μεταξύ προέλευσης και προορισμού δυσκολεύεται να συμβαδίσει με την ταχύτητα ροής των δεδομένων. Τα συστήματα που λαμβάνουν ένα πακέτο με τύπο Source Quench είναι υποχρεωμένοι να μειώσουν την ταχύτητα μετάδοσης τους. Αυτό γίνεται για να διασφαλιστεί ότι το σύστημα που λαμβάνει δεν θα αρχίσει να απορρίπτει τα δεδομένα λόγω υπερφόρτωσης της ουράς εισερχόμενων

		δεδομένων.
5	Redirect	Πληροφορεί ένα τοπικό σύστημα ότι υπάρχει ένας άλλος router ή μία πύλη επικοινωνίας η οποία είναι πιο ικανή να προωθήσει τα δεδομένα που μεταδίδει το σύστημα. Πακέτα με τύπο Redirect στέλνονται από τοπικούς routers.
8	Echo	Ζητά από το σύστημα προορισμού να επιστρέψει μία απάντηση echo (Echo Reply). Η απάντηση echo χρησιμοποιείται για τον έλεγχο της σύνδεσης μεταξύ των δύο συστημάτων, καθώς και για την μέτρηση του χρόνου απόκρισης.
9	Router Advertisement	Χρησιμοποιείται από routers για τον προσδιορισμό της ταυτότητας τους σε ένα υπο-δίκτυο. Δεν είναι ένα πραγματικό πρωτόκολλο δρομολόγησης, δεδομένου ότι δεν μεταφέρονται πληροφορίες δρομολόγησης. Χρησιμοποιείται απλώς για να γνωστοποιήσει στους υπολογιστές του υπο-δικτύου τις διευθύνσεις IP των τοπικών routers.
10	Router Selection	Επιτρέπει σε έναν υπολογιστή να ζητήσει πληροφορίες για routers χωρίς να είναι υποχρεωμένος να περιμένει την επόμενη περιοδική ενημέρωση.
11	Time Exceeded	Πληροφορεί τα συστήματα αποστολής ότι η τιμή TTL (Time To Live, χρόνος ζωής) που περιέχεται στην κεφαλίδα του πακέτου έχει "λήξει" και η πληροφορία δεν έφτασε ποτέ στον προορισμό της.
12	Parameter Problem	Μία γενικευμένη απάντηση η οποία επιστρέφεται στο σύστημα αποστολής όταν προκύπτει ένα πρόβλημα το οποίο δεν προσδιορίζεται με έναν από τους άλλους τύπους του ICMP.
13	Timestamp	Χρησιμοποιείται όταν θέλετε να μετρήσετε περισσότερο την ταχύτητα της σύνδεσης, παρά την ταχύτητα απόκρισης του συστήματος. Η αίτηση Timestamp είναι παρόμοια με μία αίτηση Echo, εκτός από το γεγονός ότι μία γρήγορη απάντηση

		σε μία αίτηση Timestamp θεωρείται πιο σημαντική.
14	Timestamp Reply	Η απάντηση σε μία αίτηση Timestamp.
15	Information Request	Έχει υποσκελιστεί από την χρήση των πρωτοκόλλων bootp και DHCP. Αρχικά αυτή η αίτηση χρησιμοποιούνταν από τα συστήματα που είχαν δυνατότητα αυτό-διαμόρφωσης για να πάρουν την δική τους διεύθυνση IP.
16	Information Reply	Απάντηση σε μία αίτηση για πληροφορίες.
17	Address Mask Request	Επιτρέπει σε ένα σύστημα να εξετάσει με δυναμικό τρόπο το τοπικό υπο-δίκτυο για να εξακριβώσει την σωστή μάσκα υπο-δικτύου. Εάν δεν λάβει απάντηση, το σύστημα θα υποθέσει ότι ισχύει μία μάσκα υπο-δικτύου κατάλληλη για την κλάση της διεύθυνσης του.
18	Address Mask Reply	Η απάντηση σε μία αίτηση Address Mask Request.
30	Traceroute	Παρέχει ένα αποτελεσματικότερο μέσο για την "ιχνηλάτηση" μιας διαδρομής από ένα σύστημα IP σ' ένα άλλο, σε σύγκριση με την απαρχαιωμένη εντολή Traceroute. Η επιλογή αυτή μπορεί να χρησιμοποιείται μόνο όταν όλοι οι ενδιάμεσοι routers έχουν προγραμματιστεί ώστε να αναγνωρίζουν αυτό τον τύπο πακέτου ICMP. Εφαρμόζεται με την χρήση μιας παραμέτρου στην εντολή ping.

Ο πίνακας 1.3 παρουσιάζει τις έγκυρες τιμές του πεδίου Code που μπορούν να χρησιμοποιούνται όταν ο τύπος του πακέτου ICMP είναι Destination Unreachable (Type=3).[15]

ΠΙΝΑΚΑΣ 1.3: Έγκυρες τιμές του πεδίου Code για πακέτα ICMP με Type=3 [15]

ode	Όνομα	Περιγραφή
	Net Unreachable	Το δίκτυο προορισμού δεν μπορεί να προσπελαστεί λόγω ενός σφάλματος δρομολόγησης (π.χ. ανυπαρξία πληροφοριών δρομολόγησης), ή ανεπαρκούς τιμής TTL.
	Host Unreachable	Ο υπολογιστής προορισμού δεν μπορεί να προσπελαστεί λόγω ενός σφάλματος δρομολόγησης (π.χ. ανυπαρξία πληροφοριών δρομολόγησης), ή ανεπαρκούς τιμής TTL.

	Protocol Unreachable	Ο υπολογιστής προορισμού με τον οποίο επικοινωνήσατε δεν έχει την υπηρεσία που ζητήσατε. Ο κωδικός αυτός επιστρέφεται συνήθως από έναν υπολογιστή· όλοι οι άλλοι επιστρέφονται από τους routers που βρίσκονται κατά μήκος της διαδρομής.
	Port Unreachable	Η υπηρεσία που αντιστοιχεί κανονικά σ' αυτή τη θύρα δεν είναι ενεργή.
	Fragmentation Needed and Don't Fragment Was Set	Τα δεδομένα που επιχειρείτε να στείλετε πρέπει να διασχίσουν ένα δίκτυο το οποίο χρησιμοποιεί μικρότερο μέγεθος πακέτου, αλλά είναι ενεργοποιημένο το bit "Don't Fragment" (να μην γίνεται κατακερματισμός).
	Source Route Failed	Το πακέτο που μεταδόθηκε καθόριζε την διαδρομή προς το σύστημα προορισμού, αλλά οι πληροφορίες δρομολόγησης ήταν λανθασμένες.

Ο πίνακας 1.4 παρουσιάζει έγκυρους κωδικούς που μπορούν να χρησιμοποιούνται όταν ο τύπος του πακέτου ICMP είναι Redirect (Type=5) [16]

ΠΙΝΑΚΑΣ 1.4 : Έγκυρες τιμές του πεδίου Code για πακέτα ICMP με Type=5 [16]

Code	Όνομα	Περιγραφή
0	Redirect Datagram for the Network (or Subnet)	Υποδεικνύει ότι ένας άλλος router του τοπικού υπο-δικτύου έχει καλύτερη οδό προς το υπο-δίκτυο προορισμού.
1	Redirect Datagram for the Host	Υποδεικνύει ότι ένας άλλος router του τοπικού υπο-δικτύου έχει καλύτερη οδό προς το υπο-δίκτυο προορισμού.

Εφαρμόζοντας φιλτράρισμα βάσει των τιμών των πεδίων Type και Code, έχουμε στην διάθεση μας πιο αναλυτικά στοιχεία από την απλή εξέταση των διευθύνσεων IP προέλευσης και προορισμού. Δεν έχουν όλα τα φίλτρα πακέτων την δυνατότητα να φιλτράρουν βάσει όλων των τιμών των πεδίων Type και Code. Αυτός ο περιορισμός μπορεί να προκαλέσει ορισμένα προβλήματα στην επικοινωνία.[16]

1.4 Στατικό φιλτράρισμα – Περίληψη

Οι συσκευές που χρησιμοποιούνται για στατικό φιλτράρισμα πακέτων δεν είναι έξυπνες. Παρέχουν ελάχιστη προστασία έναντι προχωρημένων μορφών επιθέσεων. Εξετάζουν το ελάχιστο δυνατό ποσό πληροφοριών για να εξακριβώσουν ποια είδη κυκλοφορίας θα επιτρέπουν και ποια θα μπλοκάρουν. Πολλοί routers έχουν την δυνατότητα να εκτελούν στατικό φιλτράρισμα πακέτων.[17]

1.5 Δυναμικό φιλτράρισμα πακέτων

Το δυναμικό φιλτράρισμα προάγει το στατικό φιλτράρισμα πακέτων σε ένα ανώτερο επίπεδο, διατηρώντας έναν πίνακα συνδέσεων για την παρακολούθηση της κατάστασης μιας συνόδου επικοινωνίας. Δεν βασίζεται μόνο στις τιμές των σημάνσεων.

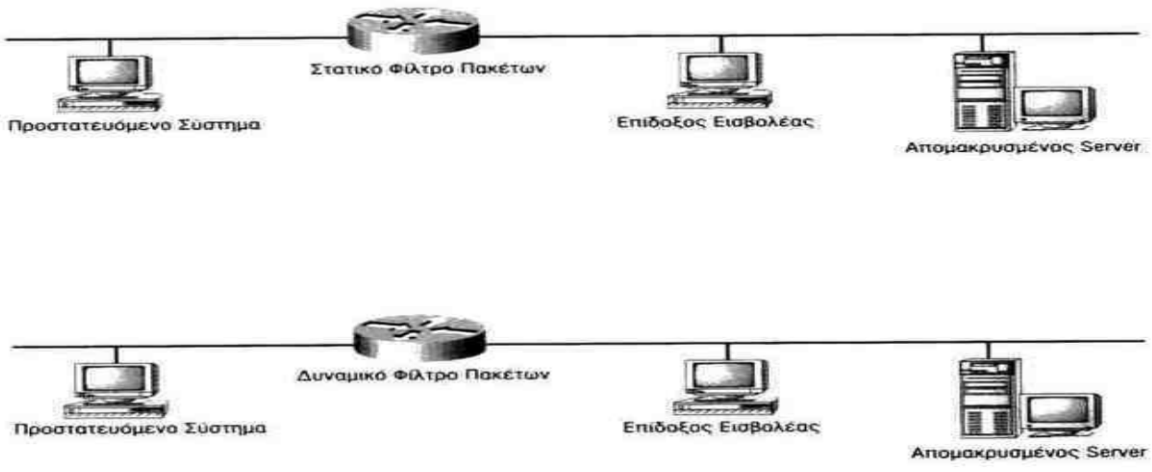
Αυτή είναι μία ισχυρή λειτουργία, η οποία μπορεί να χρησιμοποιηθεί για τον καλύτερο έλεγχο της ροής της κυκλοφορίας.[17]

Για παράδειγμα, ας υποθέσουμε ότι ένας εισβολέας στέλνει στο σύστημα σας ένα πακέτο δεδομένων με περιεχόμενο ειδικά σχεδιασμένο για να προκαλέσει την κατάρρευση του συστήματος σας. Ο εισβολέας μπορεί να χρησιμοποιήσει κάποια "κόλπα" για να κάνει αυτό το πακέτο να δείχνει σαν απάντηση σε μία προηγούμενη αίτηση για δεδομένα ενός εσωτερικού συστήματος του δικτύου. Ένα απλό φίλτρο πακέτων θα ανέλυε αυτό το πακέτο, θα έβλεπε ότι το bit ACK έχει τιμή 1 και θα πίστευε ότι είναι πράγματι μία απάντηση προς μία αίτηση για δεδομένα. Έτσι, θα περνούσε την πληροφορία στο εσωτερικό σύστημα χωρίς δισταγμό.[18]

Ένα δυναμικό φιλτράρισμα δεν ξεγελιέται τόσο εύκολα. Όταν λαμβάνει πληροφορίες, το δυναμικό φίλτρο πακέτων συμβουλεύεται τον πίνακα συνδέσεων του (ορισμένες φορές αναφέρεται και σαν πίνακας κατάστασης, state table). Εξετάζοντας τις καταχωρίσεις του πίνακα, το δυναμικό φίλτρο πακέτων αντιλαμβάνεται ότι το εσωτερικό σύστημα δεν συνδέθηκε ποτέ με το συγκεκριμένο εξωτερικό σύστημα και, προφανώς, δεν έκανε καμία αίτηση για δεδομένα. Επειδή η εισερχόμενη πληροφορία δεν ζητήθηκε ρητά, το δυναμικό φίλτρο πακέτων θα απορρίψει το πακέτο εν ριπή οφθαλμού.[18]

1.6 Δυναμικό φιλτράρισμα πακέτων στην πράξη

Για να κατανοηθεί καλύτερα η αυξημένη ασφάλεια που μπορεί να παρέχει το δυναμικό φιλτράρισμα πακέτων, θα το εξετάσουμε στην πράξη. Στην εικόνα 1.4 βλέπετε δύο διαφορετικές διαμορφώσεις δικτύων : ένα δίκτυο στο οποίο ένα από τα εσωτερικά συστήματα προστατεύεται με ένα στατικό φίλτρο πακέτων και ένα δεύτερο δίκτυο στο οποίο ένα από τα εσωτερικά του συστήματα προστατεύεται με δυναμικό φίλτρο πακέτων.[18]



ΕΙΚΟΝΑ 1.4 :Σύγκριση μεταξύ στατικού και δυναμικού φιλτραρίσματος πακέτου.[18]

Ας υποθέσουμε ότι η λίστα ACL και στις δύο συσκευές firewall υπαγορεύει τους ακόλουθους κανόνες[19]:

Το προστατευόμενο σύστημα μπορεί να υλοποιήσει οποιεσδήποτε συνόδους υπηρεσιών με τον απομακρυσμένο server.

Επιτρέπεται η διέλευση της κυκλοφορίας για οποιαδήποτε σύνοδο έχει υλοποιηθεί ήδη.Απορρίπτεται όλη η άλλη κυκλοφορία.

Ο πρώτος κανόνας επιτρέπει στο προστατευόμενο σύστημα να υλοποιεί συνδέσεις με τον απομακρυσμένο server. Αυτό σημαίνει ότι η μόνη φορά που επιτρέπεται η διέλευση ενός πακέτου με ενεργοποιημένο (1) το bit SYN (synchronize) είναι όταν η διεύθυνση προέλευσης αντιστοιχεί στο προστατευόμενο σύστημα και η διεύθυνση προορισμού αντιστοιχεί στον απομακρυσμένο server. Όταν ισχύουν αυτές οι συνθήκες, τότε μπορεί να προσπελάζεται οποιαδήποτε υπηρεσία στον απομακρυσμένο server.

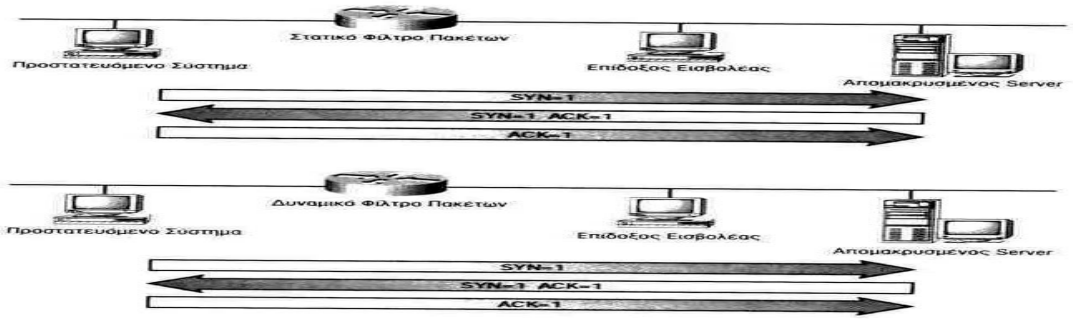
Ο δεύτερος κανόνας είναι πιο γενικός. Ουσιαστικά λέει ότι "Εάν η κυκλοφορία δείχνει να ανήκει σε μία ήδη υλοποιημένη σύνδεση, άφησε την να διέλθει". Με άλλα λόγια, όλη η κυκλοφορία είναι αποδεκτή, υπό το όρο ότι το bit SYN δεν έχει τιμή 1 και όλα τα άλλα bits είναι απενεργοποιημένα.

Ο τρίτος κανόνας δηλώνει ότι εάν υπάρχει κυκλοφορία η οποία δεν συμφωνεί με έναν από τους δύο κανόνες, αυτή θα απορρίπτεται, απλά και μόνο για να είμαστε ασφαλείς.

Και οι δύο συσκευές firewall που χρησιμοποιούμε έχουν την ίδια λίστα ACL. Η διαφορά επικεντρώνεται στην ποσότητα των πληροφοριών που έχει στην διάθεση της κάθε συσκευή για να ελέγξει την κυκλοφορία.[19]

Στην εικόνα 1.5[19], το εσωτερικό σύστημα προσπαθεί να υλοποιήσει μία σύνοδο επικοινωνίας με τον απομακρυσμένο server. Επειδή όλη η διερχόμενη κυκλοφορία ικανοποιεί τα κριτήρια που ορίζουν οι λίστες ελέγχου πρόσβασης, και τα δύο firewalls επιτρέπουν την διέλευση αυτής της κυκλοφορίας.

Αφού ολοκληρωθεί ο χαιρετισμός, το προστατευόμενο σύστημα μας στέλνει μία αίτηση για δεδομένα. Στο πακέτο της αίτησης, το bit ACK θα έχει τιμή 1 (πιθανώς και το bit PSH). Όταν ο απομακρυσμένος server λάβει αυτή την αίτηση, θα απαντήσει

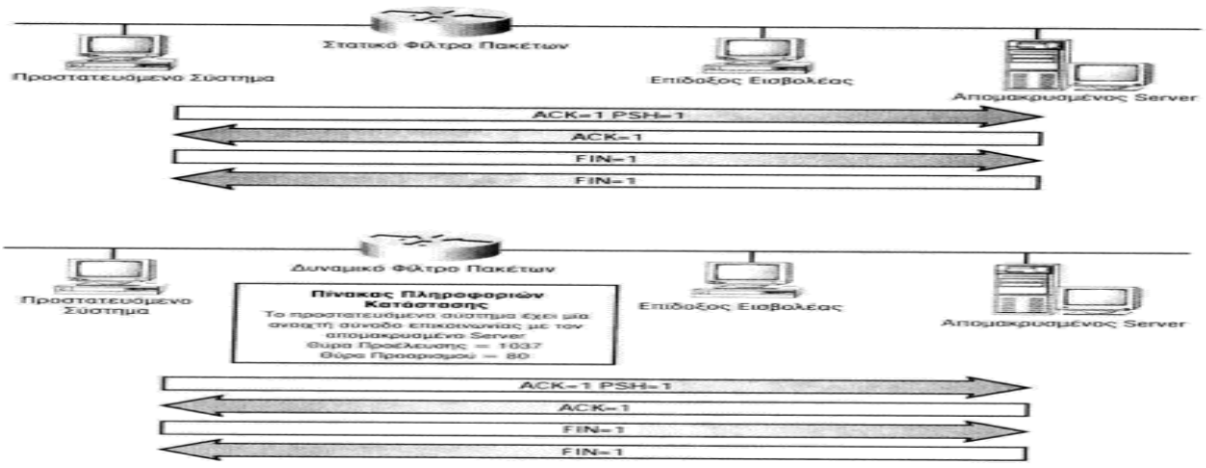


ΕΙΚΟΝΑ 1.5 : Υλοποίηση της σύνδεσης από το προστατευόμενο σύστημα προς τον απομακρυσμένο server.[20]

στέλνοντας ένα πακέτο στο οποίο το bit ACK θα έχει πάλι τιμή 1 (και πιθανώς και το bit PSH). Αφού ολοκληρωθεί η μεταφορά δεδομένων, η σύνοδος επικοινωνίας θα κλείσει, και τα δύο εμπλεκόμενα συστήματα θα μεταδώσουν αμφότερα ένα πακέτο με το bit FIN σε τιμή 1.

Στην εικόνα 1.6[20] βλέπετε μία σχηματική αναπαράσταση της διέλευσης δεδομένων μέσω αυτής της συνόδου επικοινωνίας. Όπως μπορείτε να παρατηρήσετε δεν αντιμετωπίσαμε κανένα πρόβλημα καθώς διερχόμασταν από τα firewalls, λόγω του δεύτερου κανόνα των λιστών ελέγχου πρόσβασης. Ωστόσο, κάθε firewall τηρεί αυτό τον κανόνα με ελαφρώς διαφορετικό τρόπο.

Το στατικό φίλτρο πακέτων εξετάζει απλώς το πεδίο σημάνσεων για να εξακριβώσει εάν το bit SYN είναι το μοναδικό bit με τιμή 1. Επειδή αυτό δεν ισχύει, το στατικό φίλτρο πακέτων υποθέτει ότι τα δεδομένα αυτά ανήκουν σε μία ήδη υλοποιημένη σύνοδο επικοινωνίας και επιτρέπει την διέλευση τους.



ΕΙΚΟΝΑ 1.6 : Η σύνοδος επικοινωνίας μεταξύ του προστατευόμενου συστήματος και του απομακρυσμένου server έχει υλοποιηθεί.[21]

Το δυναμικό φίλτρο πακέτων εκτελεί τον ίδιο έλεγχο, αλλά δημιούργησε επίσης μία καταχώριση στον πίνακα καταστάσεων όταν αρχικά υλοποιήθηκε η σύνδεση. Έτσι, κάθε φορά που ο απομακρυσμένος server επιχειρεί να απαντήσει σε μία αίτηση από το προστατευόμενο σύστημα, συμβουλεύεται τον πίνακα καταστάσεων για να διασφαλίσει τα ακόλουθα[21]:

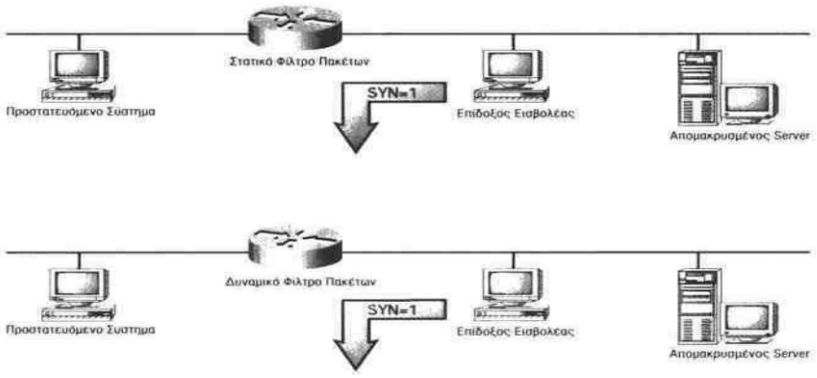
Το προστατευόμενο σύστημα έκανε πράγματι μία αίτηση για δεδομένα. Οι πληροφορίες της θύρας προέλευσης ταιριάζουν με τις πληροφορίες της αίτησης για δεδομένα.

Οι πληροφορίες της θύρας προορισμού ταιριάζουν με τις πληροφορίες της αίτησης για δεδομένα.

Επιπρόσθετα, το δυναμικό φίλτρο πακέτων μπορεί να επαληθεύσει ότι οι αριθμοί ακολουθίας και επιβεβαίωσης ταιριάζουν μεταξύ τους. Εάν όλα τα αυτά τα δεδομένα είναι σωστά, το δυναμικό φίλτρο πακέτων επιτρέπει την διέλευση των πακέτων. Αφού αποσταλούν τα πακέτα FIN από κάθε σύστημα, διαγράφεται η σχετική καταχώριση από τον πίνακα καταστάσεων. Επίσης, εάν δεν ληφθεί καμία απάντηση για ένα συγκεκριμένο χρονικό διάστημα (το οποίο μπορεί να κυμαίνεται από ένα λεπτό έως μία ώρα, ανάλογα με την διαμόρφωση), το firewall θα υποθέσει ότι ο απομακρυσμένος server δεν αποκρίνεται πλέον και θα διαγράψει την σχετική καταχώριση από τον πίνακα καταστάσεων. Η προσέγγιση αυτή διατηρεί διαρκώς ενημερωμένο τον πίνακα καταστάσεων.[22]

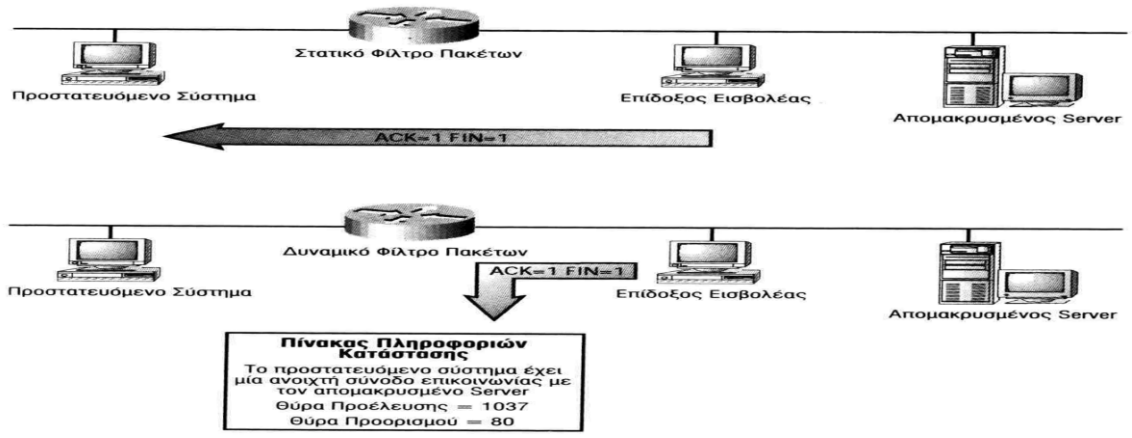
Ας υποθέσουμε τώρα ότι αυτή η ροή δεδομένων γίνεται αντιληπτή από τον κύριο εισβολέα, ο οποίος και αποφασίζει να επιτεθεί στο προστατευόμενο σύστημα. Το πρώτο πράγμα που δοκιμάζει είναι μία σάρωση θυρών (port scan) στο προστατευόμενο σύστημα, για να εξακριβώσει εάν υπάρχουν οποιεσδήποτε υπηρεσίες που ακροάζονται σ' αυτές τις θύρες. Όπως βλέπεται στην εικόνα 1.7[22], η σάρωση αυτή μπλοκάρεται και από τα δύο firewalls, επειδή τα αρχικά πακέτα σάρωσης έχουν το bit SYN ορισμένο σε τιμή 1 και όλα τα υπόλοιπα bits ορισμένα σε τιμή 0.

Χωρίς να απογοητευτεί, ο κύριος εισβολέας επιχειρεί να εκτελέσει σάρωση FIN μεταδίδοντας πακέτα με τα bit ACK και FIN ορισμένα σε τιμή 1. Σ' αυτή την περίπτωση τα αποτελέσματα είναι λίγο διαφορετικά. Επειδή το στατικό φίλτρο πακέτων εξετάζει απλώς την περίπτωση όπου μόνο το bit SYN έχει τιμή 1, επιτρέπει χωρίς τύψεις την διέλευση αυτής της κυκλοφορίας, δεδομένου ότι δεν ικανοποιούνται όλες οι συνθήκες για την απαγόρευση της.



ΕΙΚΟΝΑ 1.7 : Και οι δύο μέθοδοι φιλτραρίσματος μπορούν να μπλοκάρουν την σάρωση θυρών.[22]

Σε αντίθεση, το δυναμικό φίλτρο πακέτων είναι λίγο πιο "ιδιότροπο". Αναγνωρίζει ότι το bit SYN δεν έχει τιμή 1 και προχωρά συγκρίνοντας αυτή την κυκλοφορία με τις καταχωρίσεις στον πίνακα καταστάσεων. Σε αυτό το σημείο αντιλαμβάνεται ότι το προστατευόμενο σύστημα δεν υλοποίησε ποτέ κάποια σύνοδο επικοινωνίας με τον κύριο εισβολέα. Επομένως, είναι παράλογο ο εισβολέας να προσπαθεί να τερματίσει μία σύνοδο επικοινωνίας εάν αυτή δεν δημιουργήθηκε ποτέ. Για τον λόγο αυτό η συγκεκριμένη κυκλοφορία μπλοκάρεται από το δυναμικό φίλτρο πακέτων. Αυτό φαίνεται σχηματικά στην εικόνα 1.8.[23]



ΕΙΚΟΝΑ 1.8 : Το αποτέλεσμα που έχει η εκτέλεση μιας διαδικασίας με πακέτα FIN.[23]

Τι θα γίνει όμως εάν ο κύριος εισβολέας προσπαθήσει να ξεγελάσει το firewall προσποιούμενος ότι είναι ο απομακρυσμένος server; Για να ολοκληρώσει με επιτυχία αυτή την επίθεση, πρέπει να ικανοποιούνται αρκετές συνθήκες[24]:

- Ο εισβολέας θα πρέπει με κάποιο τρόπο να υποδυθεί τον απομακρυσμένο server (ή να λάβει την διεύθυνση IP αυτού του συστήματος).

- Εάν δεν καταφέρει να λάβει την διεύθυνση IP, ο εισβολέας μπορεί να προχωρήσει σε άλλα μέτρα για να διασφαλίσει ότι ο απομακρυσμένος server δεν θα μπορεί να απαντήσει στις αιτήσεις που του στέλνουν τα άλλα συστήματα.
- Εάν κατάφερε να αποκτήσει την διεύθυνση IP, ο εισβολέας χρειάζεται κάποια μέθοδο για να διαβάζει τις απαντήσεις που διακινούνται μέσω του καλωδίου.
- Ο εισβολέας θα πρέπει ακόμη να γνωρίζει τις θύρες που χρησιμοποιούνται από τις υπηρεσίες προέλευσης και προορισμού, έτσι ώστε η κυκλοφορία που παράγει να ταιριάζει με τις καταχωρίσεις του πίνακα καταστάσεων.
- Ανάλογα με την υλοποίηση, μπορεί να απαιτείται επίσης η απόλυτη σύμπτωση των αριθμών αναγνώρισης και ακολουθίας.
- Ο εισβολέας θα πρέπει να χειριστεί αρκετά γρήγορα την σύνοδο επικοινωνίας για να αποφύγει τυχόν προβλήματα λήξης χρόνου (timeout) τόσο στο firewall, όσο και στο προστατευόμενο σύστημα.

Για όλους τους παραπάνω λόγους, αν και μία τέτοια μορφή επίθεσης είναι εφικτή, δεν είναι εύκολο να επιτύχει. Προφανώς, ο εισβολέας θα πρέπει να έχει ουσιώδεις τεχνικές γνώσεις και να πιστεύει ότι μπορεί να κερδίσει πολλά οφέλη από μία τέτοια προσπάθεια.[25]

Πρέπει να έχετε υπόψη ότι τα παραπάνω που προαναφέρθηκαν είναι καθαρά θεωρητικά. Η δική σας περίπτωση πιθανότατα θα διαφέρει, ανάλογα με το συγκεκριμένο firewall που χρησιμοποιείται. Για παράδειγμα, το προϊόν Firewall-1 της Check Point (το οποίο είναι δυναμικό φίλτρο πακέτων) διαθέτει μία λειτουργία η οποία επιτρέπει την διατήρηση του πίνακα καταστάσεων ακόμη και μετά από μία αλλαγή της ομάδας κανόνων. Δυστυχώς, η λειτουργία αυτή σημαίνει επίσης ότι η κατάσταση δεν διατηρείται πάντα τόσο αποτελεσματικά όσο θα έπρεπε. Σε μία επίθεση με πακέτα FIN όπως αυτή που περιγράφτηκε λίγο παραπάνω, το Firewall-1 της Check Point θα επέτρεπε την διέλευση αυτών των πακέτων.[25]

1.7 Κυκλοφορία πρωτοκόλλου UDP και δυναμικό φιλτράρισμα πακέτων

Το στατικό φιλτράρισμα πακέτων αντιμετωπίζει σημαντικά προβλήματα όταν καλείται να χειριστεί κυκλοφορία του UDP. Αυτό οφείλεται στο γεγονός ότι η κεφαλίδα του UDP δεν περιλαμβάνει πληροφορίες για την κατάσταση της σύνδεσης. Σ' αυτή την περίπτωση, το δυναμικό φιλτράρισμα πακέτων μπορεί να αποδειχθεί εξαιρετικά χρήσιμο, δεδομένου ότι το ίδιο το firewall μπορεί να "θυμάται" πληροφορίες κατάστασης. Δεν βασίζεται σε πληροφορίες που περιέχονται στην κεφαλίδα των πακέτων, αλλά

διατηρεί τους δικούς του πίνακες με καταχωρίσεις για την κατάσταση όλων των συνόδων επικοινωνίας.[25]

1.8 Δυναμικά φίλτρα – Περίληψη

Τα δυναμικά φίλτρα πακέτων είναι ευφυείς συσκευές οι οποίες λαμβάνουν αποφάσεις για τον έλεγχο της κυκλοφορίας βασιζόμενες στα χαρακτηριστικά των πακέτων και στις καταχωρίσεις των πινάκων κατάστασης. Οι πίνακες κατάστασης δίνουν στην συσκευή firewall τη δυνατότητα να "θυμάται" προηγούμενες ενέργειες επικοινωνίας για την ανταλλαγή πακέτων και να λαμβάνουν αποφάσεις με βάση αυτές τις πρόσθετες πληροφορίες.[26]

Ο μεγαλύτερος περιορισμός ενός δυναμικού φίλτρου πακέτων είναι ότι δεν μπορεί να λάβει αποφάσεις για το φιλτράρισμα βασιζόμενο στα δεδομένα που περιέχονται στο πακέτο. Για την επίτευξη φιλτραρίσματος με βάση τα περιεχόμενα του πακέτου, θα πρέπει να χρησιμοποιήσετε ένα βασιζόμενο σε proxy (διακομιστή μεσολάβησης) σύστημα firewall.[26]

1.9 Φιλτράρισμα βασιζόμενο σε πληροφορίες κατάστασης

Το βασιζόμενο σε πληροφορίες κατάστασης φιλτράρισμα (stateful filtering) βελτιώνει την ισχύ και τις δυνατότητες του δυναμικού φιλτραρίσματος πακέτων. Υλοποιημένοι αρχικά από την εταιρεία Check Point με το όνομα "Stateful Multilevel Inspection", οι βασιζόμενοι στην κατάσταση της επικοινωνίας κανόνες είναι συγκεκριμένοι για το εκάστοτε πρωτόκολλο και παρακολουθούν το πλαίσιο στο οποίο διεξάγεται μία σύνοδος επικοινωνίας (όχι μόνο την κατάσταση της). Αυτό επιτρέπει στους κανόνες φιλτραρίσματος να κάνουν διάκριση μεταξύ των διαφόρων μη-βασιζόμενων σε σύνδεση πρωτοκόλλων (π.χ. UDP, NFS και RPC), τα οποία – λόγω της φύσης τους – δεν μπορούσαν να προσδιορίζονται με μονοσήμαντο τρόπο από τα δυναμικά φίλτρα πακέτων.[26]

Η μεγαλύτερη προσθήκη του βασιζόμενου σε πληροφορίες κατάστασης φιλτραρίσματος έναντι του απλού δυναμικού φιλτραρίσματος είναι η δυνατότητα του να διατηρεί πληροφορίες για την κατάσταση των εφαρμογών, και όχι μόνο για την κατάσταση της σύνδεσης. Οι πληροφορίες για την κατάσταση των εφαρμογών επιτρέπουν σε έναν ήδη πιστοποιημένο χρήστη να δημιουργεί νέες συνδέσεις χωρίς να απαιτείται η εκ νέου πιστοποίηση του, σε αντίθεση με τις πληροφορίες της κατάστασης σύνδεσης, οι οποίες διατηρούν την πιστοποίηση του χρήστη μόνο για την διάρκεια μιας συνόδου επικοινωνίας.[26]

1.10 Διακομιστές μεσολάβησης

Ένας διακομιστής μεσολάβησης (proxy server) – ορισμένες φορές αναφέρεται και σαν πύλη επικοινωνίας εφαρμογών (application gate) ή σύστημα προώθησης (forwarder) – είναι μία εφαρμογή η οποία ρυθμίζει την κυκλοφορία μεταξύ δύο τομέων του δικτύου. Οι διακομιστές μεσολάβησης χρησιμοποιούνται συχνά αντί των συσκευών φιλτραρίσματος για να εμποδίσουν την απευθείας διέλευση της κυκλοφορίας μεταξύ δικτύων. Με τον διακομιστή μεσολάβησης να λειτουργεί σαν ρυθμιστής της κυκλοφορίας, τα συστήματα προέλευσης και προορισμού δεν συνδέονται ποτέ πραγματικά το ένα με το άλλο. Ο διακομιστής μεσολάβησης παίζει το ρόλο που περιγράφει το όνομα του για όλες τις απόπειρες σύνδεσης που πέφτουν στην αντίληψη του.[27]

1.11 Πως διακινεί την κυκλοφορία ένας διακομιστής μεσολάβησης

Σε αντίθεση με τις συσκευές φιλτραρίσματος πακέτων, ένας διακομιστής μεσολάβησης δεν δρομολογεί κυκλοφορία στο δίκτυο. Στην πραγματικότητα ένας σωστά διαμορφωμένος διακομιστής μεσολάβησης έχει απενεργοποιημένες όλες τις δυνατότητες δρομολόγησης κυκλοφορίας. Όπως υπονοεί το όνομα του, ο διακομιστής μεσολάβησης αντιπροσωπεύει ή ομιλεί εκ μέρους των δύο συστημάτων που βρίσκονται εκατέρωθεν του firewall.[27]

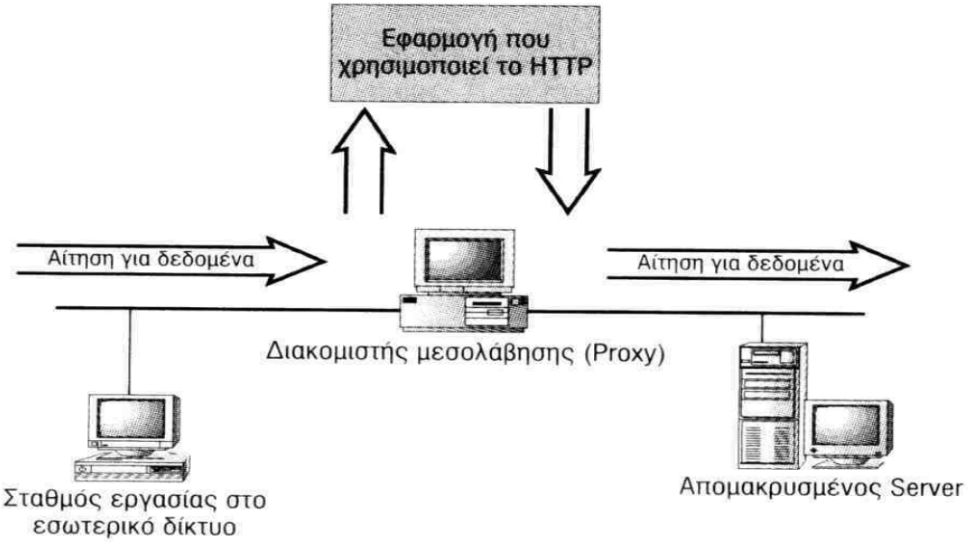
Για παράδειγμα, σκεφτείτε δύο ανθρώπους οι οποίοι συνομιλούν μέσω ενός διερμηνέα. Αν και αυτοί οι δύο άνθρωποι διεξάγουν μία συνομιλία, κανένας από τους δύο δεν μιλάει πραγματικά στον άλλον. Όλη η μεταξύ τους επικοινωνία διέρχεται από τον διερμηνέα πριν σταλεί στο άλλο μέρος. Ο διερμηνέας μπορεί να κάνει κάποιες διορθωτικές ενέργειες όσον αφορά στην γλώσσα που χρησιμοποιήθηκε, ή να φιλτράρει σχόλια ή δηλώσεις οι οποίες μπορεί να δείχνουν εχθρικές.[27]

Για να κατανοήσετε πόσο σχετικό είναι αυτό το παράδειγμα με τις επικοινωνίες δικτύων, μελετήστε την εικόνα 1.9. Το σύστημα στο εσωτερικό δίκτυο επιθυμεί να ζητήσει μία ιστοσελίδα από τον απομακρυσμένο server. Διατυπώνει την αίτηση του και την μεταδίδει στην πύλη επικοινωνίας (gate) που οδηγεί στο απομακρυσμένο δίκτυο, η οποία σ ‘αυτή την περίπτωση είναι ο διακομιστής μεσολάβησης.[27]

Αφού ο διακομιστής μεσολάβησης λάβει την αίτηση, προσδιορίζει του τύπο της υπηρεσίας που προσπαθεί να προσπελάσει το σύστημα από το εσωτερικό δίκτυο. Επειδή σ’ αυτή την περίπτωση το σύστημα έχει ζητήσει μία ιστοσελίδα, ο διακομιστής μεσολάβησης περνάει την αίτηση του σε μία ειδική εφαρμογή η οποία χρησιμοποιείται μόνο για την επεξεργασία και διεκπεραίωση συνόδων επικοινωνίας με το πρωτόκολλο

HTTP. Η εφαρμογή αυτή είναι απλώς ένα πρόγραμμα του οποίου η αποκλειστική λειτουργία είναι να ασχολείται με την επικοινωνία μέσω του πρωτοκόλλου HTTP.[27]

Όταν η συσχετιζόμενη με το HTTP εφαρμογή λάβει την αίτηση, πιστοποιεί κατ' αρχήν ότι η λίστα ελέγχου πρόσβασης (ACL) επιτρέπει αυτό το είδος κυκλοφορίας. Εάν η κυκλοφορία είναι αποδεκτή, ο διακομιστής μεσολάβησης διατυπώνει μία νέα αίτηση προς τον απομακρυσμένο server – αλλά αυτή τη φορά χρησιμοποιεί τον εαυτό του σαν σύστημα προέλευσης. Με άλλα λόγια, ο διακομιστής μεσολάβησης δεν περνά απλώς την αίτηση προς τον προορισμό της· παράγει μία νέα αίτηση.[27]



ΕΙΚΟΝΑ 1.9 : Ένας διακομιστής μεσολάβησης παίζει τον ρόλο του ρυθμιστή σε μία σύνοδο επικοινωνίας.[28]

Αυτή η νέα αίτηση στέλνεται κατόπιν στον απομακρυσμένο server. Εάν η αίτηση ελέγχονταν από μία συσκευή ανάλυσης δικτύου (network analyzer), θα έδειχνε σαν να την έκανε ο διακομιστής μεσολάβησης και όχι το σύστημα από το εσωτερικό δίκτυο. Γι' αυτό τον λόγο, όταν ο απομακρυσμένος server απαντά, απαντά στον διακομιστή μεσολάβησης.[28]

Αφού ο διακομιστής μεσολάβησης λάβει την απάντηση από τον απομακρυσμένο server, την στέλνει στην συσχετιζόμενη με το HTTP εφαρμογή. Η εφαρμογή αυτή εξετάζει κατόπιν τα πραγματικά δεδομένα που στάλθηκαν από τον απομακρυσμένο server για τυχόν ανωμαλίες. Εάν τα δεδομένα είναι αποδεκτά, η εφαρμογή δημιουργεί ένα νέο πακέτο και προωθεί τα δεδομένα στο εσωτερικό σύστημα.[28]

Όπως βλέπεται, τα δύο συστήματα που βρίσκονται στα δύο άκρα της επικοινωνίας δεν έρχονται ποτέ σε απευθείας επαφή. Ο διακομιστής μεσολάβησης παρεμβαίνει διαρκώς στην συνομιλία για να βεβαιωθεί ότι τα πάντα γίνονται με ασφάλεια.[28]

Επειδή οι διακομιστές μεσολάβησης πρέπει να "κατανοούν" το πρωτόκολλο που χρησιμοποιείται στο επίπεδο εφαρμογής, μπορούν επίσης να υλοποιήσουν συστήματα ασφαλείας συγκεκριμένα για το εκάστοτε πρωτόκολλο. Για παράδειγμα, ένας διακομιστής μεσολάβησης ο οποίος ελέγχει την εισερχόμενη κυκλοφορία FTP μπορεί να διαμορφωθεί έτσι ώστε να μπλοκάρει όλες τις αιτήσεις put και mput που λαμβάνονται από ένα εξωτερικό σύστημα. Ουσιαστικά σ' αυτή την περίπτωση θα δημιουργούνταν ένας FTP server μόνο για ανάγνωση: οι χρήστες που βρίσκονται στην εξωτερική πλευρά του συστήματος firewall δεν θα μπορούσαν να στείλουν στον FTP server εντολές για την έναρξη της διαδικασίας εγγραφής αρχείων. Θα μπορούσαν, ωστόσο, να εκτελέσουν εντολές get για την λήψη αρχείων από τον FTP server.[28]

Υπάρχουν επίσης μειωμένων δυνατοτήτων διακομιστές μεσολάβησης οι οποίοι αναφέρονται με τον όρο plug gateways. Τα συστήματα αυτά δεν είναι πραγματικοί διακομιστές μεσολάβησης, επειδή δεν κατανοούν την εφαρμογή που υποστηρίζουν. Παρέχουν απλώς τη δυνατότητα σύνδεσης για μία συγκεκριμένη θύρα υπηρεσίας και παρέχουν ελάχιστα πλεονεκτήματα πέρα από το δυναμικό φιλτράρισμα πακέτων.[29]

ΚΕΦΑΛΑΙΟ 2Ο : ΚΑΤΗΓΟΡΙΕΣ ΣΥΣΤΗΜΑΤΩΝ FIREWALL

Το κεφάλαιο αυτό αναφέρεται στους τύπους firewall. Πιο συγκεκριμένα αναλύονται δύο από τους τύπους οι οποίοι είναι συνηθισμένοι.

2.1 Τύποι firewall

Τα firewalls μπορούν να χωριστούν στις ακόλουθες κατηγορίες[30]:

1) Ενσωματωμένα σε συσκευές
2) Υλοποιημένα με λογισμικό
3) Υλοποιημένα με hardware
4) Επιπέδου εφαρμογής

2.1.1 Firewalls ενσωματωμένα σε συσκευές

Όταν οι λειτουργίες firewall περιέχονται σε έναν router ή σε ένα switch, το firewall ονομάζεται ενσωματωμένο (embedded). Τα ενσωματωμένα firewalls εκτελούν συνήθως έλεγχο των πακέτων στο επίπεδο του IP χωρίς να εξετάζουν την κατάσταση της σύνδεσης, πράγμα το οποίο έχει σαν αποτέλεσμα μεγαλύτερη απόδοση αλλά αυξημένη ευαισθησία σε εχθρικό κώδικα.[31]

2.1.2 Firewalls υλοποιημένα με λογισμικό

Τα υλοποιημένα με λογισμικό firewalls χωρίζονται σε δύο τύπους: α) για μεγάλες επιχειρήσεις και οργανισμούς, τα οποία απευθύνονται σε μεγάλα δίκτυα, και β) για μικρά γραφεία και οικιακές εφαρμογές (SOHO). Παρέχουν συνήθως όλη την γκάμα των λειτουργιών firewall και εγκαθίστανται σε συστήματα επιπέδου server με αντίστοιχο λειτουργικό σύστημα (π.χ. Linux, Unix, ή Windows 2000).[31]

2.1.3 Firewalls υλοποιημένα με hardware

Τα firewalls αυτής της κατηγορίας σχεδιάζονται σαν ολοκληρωμένα συστήματα "με το κλειδί στο χέρι". Αυτό σημαίνει ότι δεν απαιτούν εκτεταμένες και πολύπλοκες εργασίες εγκατάστασης ή διαμόρφωσης για να ξεκινήσουν να παρέχουν υπηρεσίες firewall. Τα firewalls που είναι υλοποιημένα με hardware, όμοια με τα υλοποιημένα με λογισμικό firewalls, μπορεί να στοχεύουν είτε σε μεγάλους οργανισμούς, είτε σε μικρές επιχειρήσεις.[31]

2.1.4 Firewalls επιπέδου εφαρμογής

Τα firewalls επιπέδου εφαρμογής αποτελούν συνήθως πρόσθετα στοιχεία υπαρχόντων firewalls υλοποιημένων με hardware ή λογισμικό. Ο βασικός τους στόχος είναι να παρέχουν προηγμένο φιλτράρισμα περιεχομένου για τα δεδομένα που διακινούνται στο επίπεδο εφαρμογής. Καθώς οι δυνατότητες των firewalls αυξάνονται και το φιλτράρισμα επικεντρώνεται όλο και περισσότερο στα δεδομένα του επιπέδου εφαρμογής, αυτά τα firewalls γίνονται όλο και πιο εξειδικευμένα.[31]

2.2 Τι είδους firewall πρέπει να χρησιμοποιούμε

Δεν υπάρχουν απόλυτες υποδείξεις όσον αφορά στην επιλογή ενός συγκεκριμένου τύπου firewall, αν και οι εξελίξεις στον τομέα των υβριδικών router μας δίνουν πλέον τη δυνατότητα να αποκτήσουμε όλες τις αναγκαίες λειτουργίες χωρίς να αγοράσουμε δύο ξεχωριστά προϊόντα – έναν router και ένα firewall. Συνήθως ο καθοριστικός παράγοντας διάκρισης είναι το επίπεδο ελέγχου που παρέχει ο router (ή το firewall), καθώς και οι λειτουργίες διαχείρισης και υποστήριξης VPN. Κατά την αναζήτηση της κατάλληλης λύσης θα πρέπει επίσης να λάβουμε υπόψη τις επιχειρησιακές ανάγκες και τις απαιτήσεις μας στον τομέα της ασφάλειας.[31]

Γνωρίζοντας ότι το στατικό φιλτράρισμα πακέτων θεωρείται "αδύναμο", είναι το χαμηλότερο επίπεδο περιμετρικής ασφάλειας που μπορούμε να υλοποιήσουμε στο δίκτυο μας. Ωστόσο, είναι επίσης το πιο ουσιώδες, δεδομένου ότι η δυνατότητα του στατικού φιλτραρίσματος πακέτων είναι ενσωματωμένη στους περισσότερους routers.

Εάν έχουμε μόνιμη σύνδεση με ένα δίκτυο WAN, κατά πάσα πιθανότητα χρησιμοποιούμε έναν router. Εάν έχουμε έναν router, θα πρέπει να χρησιμοποιήσουμε κατ’ ελάχιστον στατικό φιλτράρισμα πακέτων.[32]

Κάθε τύπος firewall έχει τα δυνατά και τα αδύνατα σημεία του. Το δυναμικό φιλτράρισμα πακέτων είναι συνήθως πιο εύκολο στην διαχείριση συγκριτικά με έναν διακομιστή μεσολάβησης, και έχει καλύτερες πιθανότητες να ικανοποιήσει την πλειονότητα των επιχειρησιακών αναγκών, αλλά δεν είναι τόσο ικανό στον έλεγχο της διερχόμενης κυκλοφορίας όσο θα μπορούσε να είναι ένας διακομιστής μεσολάβησης. Αν και αμφότερες οι λύσεις – δυναμικό φιλτράρισμα πακέτων και διακομιστής μεσολάβησης – θα μπλοκάρουν την γνωστή ως "κακή" κυκλοφορία, η κάθε λύση αντιδρά λίγο διαφορετικά όταν αντιμετωπίζει αμφιλεγόμενη κυκλοφορία.[33]

Για παράδειγμα, υποθέτουμε ότι έχουμε δύο firewalls: ένα δυναμικό φίλτρο πακέτων και έναν διακομιστή μεσολάβησης. Κάθε firewall λαμβάνει ένα πακέτο

δεδομένων το οποίο έχει ενεργοποιημένη την σήμανση υψηλής προτεραιότητας για μία συγκεκριμένη εφαρμογή και κανένα από τα δύο δεν είναι προγραμματισμένο ώστε να γνωρίζει πώς να χειρίζεται αυτό τον τύπο δεδομένων. Συνήθως (αλλά όχι πάντα) το δυναμικό φίλτρο πακέτων επιτρέπει την διέλευση της αμφισβητούμενης κυκλοφορίας, ενώ ο διακομιστής μεσολάβησης την απορρίπτει. Επιπρόσθετα, επειδή ο διακομιστής μεσολάβησης είναι ενήμερος για την εφαρμογή, θα μπορούσε να εκτελέσει περισσότερους ελέγχους στο πραγματικό περιεχόμενο των δεδομένων, ενώ το δυναμικό φίλτρο πακέτων δεν έχει αυτή την δυνατότητα. Ωστόσο, αυτή είναι μία θεωρητική σύγκριση μεταξύ δύο μορφών περιμετρικής προστασίας ενός δικτύου. Η δική σας περίπτωση μπορεί να διαφέρει, ανάλογα με το προϊόν που επιλέξατε.[33]

Οι διακομιστές μεσολάβησης τείνουν να είναι λίγο πιο ασφαλείς, αλλά μπορεί να είναι δυσκολότερη η προσαρμογή τους ώστε να ικανοποιούν συγκεκριμένες επιχειρησιακές ανάγκες.[33]

Επειδή κάποιο επίπεδο κινδύνου θα θεωρείτε πάντα αποδεκτό, η πρόκληση είναι να δημιουργήσετε ένα πολλαπλών επιπέδων σύστημα ασφάλειας με λογικό κόστος, το οποίο θα προστατεύει το δίκτυο σας χωρίς να μειώνει την ευχρηστία και την λειτουργικότητα του. Ένα σωστά επιλεγμένο firewall ικανοποιεί όλες τις ανάγκες του οργανισμού στον τομέα της σύνδεσης, παρέχοντας ταυτόχρονα το υψηλότερο δυνατό επίπεδο ασφάλειας. Επιπλέον, ένα καλό προϊόν firewall μπορεί να ενσωματώνει ταυτόχρονα δυναμικό φιλτράρισμα πακέτων και τεχνολογία διακομιστή μεσολάβησης για να παρέχει το υψηλότερο επίπεδο ασφάλειας και ευελιξίας.[33]

2.3 Ποιον τύπο πρέπει να διαλέξουμε

Δεν μπορούμε να δώσουμε μία ξεκάθαρη απάντηση στο ερώτημα του τίτλου, όμως θα επισημάνουμε απλώς ορισμένα από τα ισχυρά και αδύνατα σημεία κάθε πλατφόρμας, αφήνοντας την τελική απόφαση σε εσάς.[34]

Θα επικεντρωθούμε στους δύο συνηθέστερους τύπους firewall λόγω της ευρείας χρήσης τους: τα υλοποιημένα με hardware και τα υλοποιημένα με λογισμικό. Επειδή ακόμη και τα firewalls που είναι υλοποιημένα με hardware χρησιμοποιούν λογισμικό, θα αναφερόμαστε σ’ αυτά με τον όρο ολοκληρωμένες συσκευές. Τα firewalls απευθύνονται σε μεγάλες επιχειρήσεις και οργανισμούς τρέχουν συνήθως σε υπολογιστές με εξοπλισμό και λειτουργικό σύστημα επιπέδου server· θα αναφερόμαστε σ’ αυτά με τον όρο βασιζόμενα σε server firewalls. Ένα παράδειγμα βασιζόμενου σε server firewall είναι το firewall-1 της Check Point, οποίο τρέχει σε διάφορα λειτουργικά συστήματα (Windows, Solaris και Linux). Ένα βασιζόμενο σε hardware firewall είναι μία εφαρμογή

firewall η οποία τρέχει σε εξειδικευμένο εξοπλισμό και απαιτεί ειδικό λογισμικό. Για παράδειγμα, το PIX της Cisco είναι ένα παράδειγμα ολοκληρωμένης συσκευής η οποία δεν έχει δυνατότητα να κάνει οτιδήποτε άλλο πέρα από το να λειτουργεί σαν firewall και δεν περιλαμβάνει σκληρό δίσκο ή οποιαδήποτε άλλα συμβατικά συστατικά ενός server. Λόγω της ολοκληρωμένης και εξειδικευμένης φύσης τους, οι συσκευές αυτές είναι κατά παράδοση γρηγορότερες, πιο εύρωστες και θεωρούνται πιο ασφαλείς σε σύγκριση με τα βασιζόμενα σε server firewalls. Τα βασιζόμενα σε server firewalls, από την άλλη, παρέχουν συνήθως περισσότερες επιλογές διαμόρφωσης και υποστήριξης, ενώ μπορεί να είναι φθηνότερα από τις ολοκληρωμένες λύσεις.[34]

2.3.1 Βασιζόμενα σε server firewalls

Τα βασιζόμενα σε server firewalls είναι εφαρμογές οι οποίες τρέχουν σε "πάνω από" ένα λειτουργικό σύστημα. Υπάρχουν τέτοιες εφαρμογές firewall για τις ακόλουθες πλατφόρμες[34]:

- Apple Mac OS X
- Unix (Solaris, HP-UX, IBM AIX)
- Linux
- Microsoft Windows NT, 2000, XP και .NET

2.3.1.1 Το λειτουργικό σύστημα Mac OS

Το λειτουργικό σύστημα των Macintosh υπέστη μία ριζική αλλαγή το 2001, με την έκδοση OS X (10). Το OS X βασίζεται στο λειτουργικό σύστημα NeXTStep, το οποίο μετη σειρά του βασίζεται στον πυρήνα Mach και στο BSD (Berkeley Software Distribution) UNIX. Αν και η Apple κατέστησε ευρέως διαθέσιμο τον πηγαίο κώδικα του πυρήνα OS X (με όνομα Darwin), έκανε σημαντικές αλλαγές για να τον προσαρμόσει στην πλατφόρμα των Macintosh. Αν και δεν έχουν ανακαλυφθεί σημαντικές αδυναμίες του OS X στον τομέα της ασφάλειας, ο ανοικτός πηγαίος κώδικας του λειτουργικού συστήματος και η καταγωγή του από το Unix δίνουν τη δυνατότητα προσαρμογής πολλών υπαρχόντων προϊόντων ασφαλείας ώστε να τρέχουν στο σύστημα – επιπρόσθετα του firewall API που υπάρχει ενσωματωμένο στο σύστημα.[35]

Τα ισχυρά σημεία του Mac OS

Λόγω του ότι βασίζεται στο Unix και διαθέτει ελεύθερα τον πηγαίο κώδικα, το OS X παρέχει την ίδια πλούσια γκάμα λειτουργιών με τα άλλα βασιζόμενα στο Unix λειτουργικά συστήματα. Επίσης, επειδή ο πηγαίος κώδικας του πυρήνα του λειτουργικού

συστήματος (Darwin) είναι ανοικτός, υπάρχει η δυνατότητα υλοποίησης αλλαγών για την διόρθωση τυχόν σφαλμάτων, ή για την αύξηση της λειτουργικότητας του.[36]

Επιπρόσθετα, οι περισσότερες υλοποιήσεις server συστημάτων με το OS X χρησιμοποιούν τα ίδια γενικευμένα συστατικά όπως και τα άλλα βασιζόμενα στο Unix συστήματα (όπως ο Web Server Apache, η βάση δεδομένων MySQL και ο server ηλεκτρονικού ταχυδρομείου Sendmail). Πάντως, υπάρχει μία ευρέως διαδεδομένη άποψη ότι η χρήση ενός firewall σε Mac είναι ελαφρώς ασφαλέστερη, απλά και μόνο επειδή οι περισσότεροι χάκερ δεν είναι εξοικειωμένοι με την τεχνολογία των Mac. Αν και έχουν αναφερθεί ορισμένα τρωτά σημεία σε εφαρμογές που τρέχουν σε Mac, ελάχιστες είναι οι αναφορές που υπάρχουν για αδυναμίες του ίδιου του λειτουργικού συστήματος.[36]

Υπάρχει επίσης και το θέμα της εύκολης διαμόρφωσης των βασικών υπηρεσιών firewall.Το BrickHouse είναι ένα γραφικό σύστημα επικοινωνίας με τον χρήστη για την διαμόρφωση του firewall API που είναι ενσωματωμένο στο OS X. Αν και παρέχει μόνο στατικό φιλτράρισμα πακέτων, διαθέτει εκτενείς δυνατότητες καταγραφής. Για τους πιο προχωρημένους χρήστες, το API είναι επίσης διαθέσιμο μέσω της γραμμής εντολών.[36]

Συμπερασματικά, ένα firewall το οποίο τρέχει στο νέο λειτουργικό OS X είναι σίγουρο ότι θα δει πλεονεκτήματα στην απόδοση, στην διαμόρφωση και στα εργαλεία υποστήριξης (τα περισσότερα βασιζόμενα στο Unix βοηθήματα για την ασφάλεια τρέχουν στο OS X).[36]

Οι αδυναμίες του Mac OS

Υπάρχουν ωστόσο και ορισμένες σημαντικές αδυναμίες. Επειδή αυτό το σύστημα δεν είναι πολύ καλά γνωστό, είναι πιθανό να υπάρχουν πολλά τρωτά σημεία τα οποία περιμένουν απλώς να ανακαλυφθούν από οποιονδήποτε χάκερ θα προσπαθήσει σοβαρά να τα παραβιάσει.[36]

Επίσης, επειδή ένας Macintosh server έχει περιορισμένο αριθμό εφαρμογών και σταθερών επιλογών διαμόρφωσης του firewall API, οι επόπτες ίσως αισθανθούν ότι στερούνται ορισμένων απαραίτητων επιλογών – όπως για παράδειγμα η δυνατότητα της προσαρμογής του API για την προσθήκη επιπλέον λειτουργιών ασφάλειας και ανίχνευσης επιθέσεων. Αν και υπάρχουν ορισμένες λύσεις ανοικτού κώδικα οι οποίες παρέχουν αυτές τις δυνατότητες, κανένας κατασκευαστής δεν έχει παρουσιάσει ακόμη

ένα βασιζόμενο σε λογισμικό firewall για το OS X που να καλύπτει μεγάλους οργανισμούς.[37]

2.3.1.2 UNIX

Το Unix υπάρχει και χρησιμοποιείται για πολύ περισσότερο χρόνο από οποιοδήποτε άλλο λειτουργικό σύστημα, συμπεριλαμβανομένων των Windows NT της Microsoft (και των βασιζόμενων στα NT λειτουργικών συστημάτων όπως τα Windows 2000, XP και .NET). Δεν αποτελεί έκπληξη το γεγονός ότι τα πρώτα συστήματα firewall σχεδιάστηκαν για υπολογιστές Unix. Αυτό σημαίνει ότι οι ιδιοσυγκρασίες αυτής της πλατφόρμας έχουν γίνει απόλυτα κατανοητές και είναι καλά τεκμηριωμένες, καθώς και ότι τα προϊόντα firewall που τρέχουν σ' αυτό το λειτουργικό σύστημα είναι σταθερά. Όταν αποκαλύπτονται αδυναμίες του Unix στον τομέα της ασφάλειας, αυτές συνήθως δεν σχετίζονται με τον πυρήνα του λειτουργικού συστήματος, αλλά με υπηρεσίες και εφαρμογές που τρέχουν πάνω από αυτόν.[38]

Το Unix έχει επίσης το πλεονέκτημα της απόδοσης έναντι των άλλων λειτουργικών συστημάτων. Το γεγονός αυτό, σε συνδυασμό με την υποστήριξη του από πολλές πλατφόρμες και διαμορφώσεις υπολογιστών, καθιστά το Unix προτιμώμενο λειτουργικό σύστημα σε όλες τις περιπτώσεις που απαιτούν εκτενή επεξεργασία μεγάλου όγκου δεδομένων. Οι καλές πρακτικές χρήσης των firewall υπαγορεύουν την απενεργοποίηση όλων των εφαρμογών και συστατικών που δεν είναι ζωτικής σημασίας για την λειτουργία του firewall, και αυτό είναι ιδιαίτερα εύκολο να επιτευχθεί στο Unix.[38]

Τα ισχυρά σημεία του Unix

Τα ισχυρά σημεία του Unix είναι πολλά. Πρόκειται για ένα λειτουργικό σύστημα με εξαιρετικές δυνατότητες διαμόρφωσης και απόλυτα κατανοητό από πολλά στελέχη που εργάζονται στον τομέα της ασφάλειας, ενώ δεν πρέπει να ξεχνάμε ότι είναι ένα από τα σημαντικότερα λειτουργικά συστήματα που υπάρχουν σήμερα. Πολλοί πόροι πληροφοριών είναι αποκλειστικά αφιερωμένοι στην κατανόηση και διόρθωση οποιωνδήποτε προβλημάτων μπορεί να προκύψουν στον τομέα της ασφάλειας.[38]

Το Unix θεωρείται επίσης σαν ένα λειτουργικό σύστημα με εξαιρετική σταθερότητα και υψηλή απόδοση. Επιπρόσθετα, λόγω της δυνατότητας του να τρέχει σε πολλαπλές πλατφόρμες hardware, καθώς και σε εκδόσεις συστημάτων με πολλαπλούς επεξεργαστές, μπορεί να υποστηρίξει την διακίνηση μεγάλων όγκων δεδομένων, η οποία είναι απαραίτητη σε οποιοδήποτε firewall υποστηρίζει ένα μεγάλο δίκτυο. Επίσης,

σε πολλές περιπτώσεις δεν απαιτεί την επανεκκίνηση του υπολογιστή αφού γίνουν αλλαγές στην διαμόρφωση, κάτι από το οποίο υποφέρουν τα βασιζόμενα στα Windows NT συστήματα.[38]

Όσον αφορά στην ασφάλεια, υπάρχουν περισσότερα προϊόντα για το Unix παρά για οποιαδήποτε άλλη πλατφόρμα (με τα Windows NT να έρχονται δευτέρα με μικρή διαφορά). Το γεγονός αυτό, σε συνδυασμό με την 30-χρονη ιστορία του, καθιστά το Unix το προτιμώμενο λειτουργικό σύστημα για πολλούς μεγάλους οργανισμούς.[39]

Τα αδύνατα σημεία του Unix

Προβλήματα μπορεί να προκύψουν όταν άπειροι επόπτες συστημάτων Unix εγκαθιστούν firewalls χωρίς πρώτα να απενεργοποιήσουν τα πολλά τρωτά (αλλά ενδεχομένως πολύτιμα σε διαφορετικά, μη-firewallI συστήματα) προγράμματα και υπηρεσίες (δαίμονες) τα οποία είναι εξ ορισμού ενεργοποιημένα. Και επειδή πολλές από αυτές τις υπηρεσίες (δαίμονες) είναι διαμορφωμένες ώστε να τρέχουν με το καθεστώς ασφάλειας του root (ο ισχυρότατος λογαριασμός του superuser), παρέχουν σε έναν πιθανό εισβολέα πλήρη πρόσβαση στο σύστημα αφού καταφέρει να παραβιάσει τα τρωτά σημεία μιας υπηρεσίας.[39]

Η απενεργοποίηση των υπηρεσιών που τρέχουν σαν δαίμονες είναι σχετικά απλή υπόθεση. Το μόνο που χρειάζεται να κάνει ένας επόπτης είναι να διαγράψει ή να μετονομάσει τα scripts που ενεργοποιούν έναν δαίμονα κατά τον χρόνο εκκίνησης του συστήματος, ή να μετατρέψει σε σχόλιο την κατάλληλη γραμμή στο αρχείο παραμέτρων διαμόρφωσης inetd.conf, εάν ένας δαίμονας καλείται από τον inetd.[39]

Το Unix θεωρείται ότι είναι ένα από τα πλέον δύσκολα λειτουργικά συστήματα στην εκμάθηση και εποπτεία, και το κόστος ενός συστήματος Unix είναι κατά παράδοση πιο μεγάλο από το κόστος οποιουδήποτε άλλου λειτουργικού συστήματος. Επειδή δεν υπάρχουν τόσα πολλά τεκμηριωμένα αδύνατα σημεία στο Unix, ένας επόπτης πρέπει να επενδύσει περισσότερο χρόνο για να ασφαλίσει το σύστημα του· εάν δεν το κάνει, ένας εισβολέας που γνωρίζει τα τρωτά σημεία του Unix μπορεί να τα εκμεταλλευτεί.[40]

2.3.1.3 Linux

Όμοια με το Unix, το Linux έχει αυξημένες δυνατότητες διαμόρφωσης, είναι σταθερό, καλά κατανοητό και υπάρχουν γι' αυτό πολλά σχετιζόμενα με την ασφάλεια προϊόντα. Ωστόσο, το πιο ελκυστικό στοιχείο του Linux είναι η ανοικτή του φύση.[41]

Τα ισχυρά σημεία του Linux

Η καθιερωμένη αίσθηση συνεργασίας που επικρατεί στην κοινότητα του Linux σημαίνει ότι υπάρχει μία έτοιμη και πρόθυμη ομάδα υποστήριξης για τους ειδικούς της ασφάλειας, όταν προκύπτουν θέματα που πρέπει να επιλυθούν.[41]

Ένα άλλο πλεονέκτημα του Linux είναι οικονομικής φύσης: ο πηγαίος κώδικας διανέμεται ελεύθερα, κάτι το οποίο γίνεται ολοένα και πιο ελκυστικό στους οργανισμούς που προσπαθούν να περιορίσουν το κόστος των επενδύσεων στον τομέα της πληροφορικής. Αλλά δεν είναι μόνο το μηδενικό κόστος του πηγαίου κώδικα του Linux που το καθιστά ελκυστικό. Είναι η ελευθερία τροποποίησης του λειτουργικού συστήματος ακόμη και σε βασικά θέματα, έτσι ώστε να καλύπτει τις εξειδικευμένες ανάγκες ενός οργανισμού. Συγκρίνετε αυτή την προσέγγιση με τις ιδιαίτερα περιοριστικές (και ακριβές) άδειες χρήσης των προϊόντων της Microsoft.[41]

Λόγω της ελεύθερης και ανοικτής φύσης του Linux, οι λύσεις firewall που υπάρχουν γι' αυτό είναι πολύ περισσότερες απ' ότι για οποιοδήποτε άλλο λειτουργικό σύστημα.Αν και η πολύ μεγάλη ποικιλία επιλογών μπορεί να προκαλέσει σύγχυση, σημαίνει επίσης ότι το Linux μπορεί να αποτελέσει την ιδανική λύση για εξειδικευμένες διαμορφώσεις ασφάλειας.[41]

Αδύνατα σημεία του Linux

Αν και το Linux θεωρείται εξαιρετικά ισχυρό, είναι επίσης πολύπλοκο. Η χρήση της γραμμής εντολών μπορεί να αποδειχθεί εκφοβιστική για μία γενιά χρηστών οι οποίοι έμαθαν να στηρίζονται στην ευκολία ενός γραφικού περιβάλλοντος. Λόγω των πολλών διανομών του Linux, κάθε μία από τις οποίες χρησιμοποιεί διαφορετικές θέσεις αποθήκευσης των αρχείων διαμόρφωσης και εκδόσεις του πυρήνα, η διατήρηση της ομοιομορφίας στα πλαίσια ενός οργανισμού μπορεί να αποδειχτεί δύσκολη υπόθεση. Προσθέστε στα παραπάνω την συνεχή παραγωγή διορθώσεων σφαλμάτων, ενημερώσεων και βελτιωμένων εκδόσεων προϊόντων, και θα διαπιστώσετε ότι η υποστήριξη του Linux μπορεί να αυξήσει το συνολικό κόστος υποστήριξης του δικτύου, ειδικά εάν δεν υπάρχει ένα γενικό πλάνο συντήρησης των συστημάτων.[42]

2.3.1.4 Windows NT

Επειδή τα Windows NT είναι μία επέκταση των λειτουργικών συστημάτων Windows που προορίζονται για τελικούς χρήστες (εκ του μακρόθεν τα δημοφιλέστερα λειτουργικά συστήματα που υπήρξαν ποτέ), τα NT είναι ένα πολύ πιο οικείο περιβάλλον

για τον τυπικό τελικό χρήστη. Αυτό σημαίνει ότι ο χρήστης δεν είναι υποχρεωμένος να μάθει ένα εντελώς νέο περιβάλλον απλά και μόνο για να τρέξει λογισμικό firewall.[42]

Ισχυρά σημεία τωνWindows NT

Σημαντικό είναι το γεγονός ότι μία εταιρεία δεν είναι υποχρεωμένη να προσλάβει επιπλέον στελέχη απλά και μόνο για την διαχείριση του συστήματος firewall. Μάλιστα, τα βασιζόμενα σε NT συστήματα είναι κατά παράδοση λιγότερο ακριβά από τα αντίστοιχα συστήματα Unix, και το γεγονός ότι η επένδυση σε εξοπλισμό και λογισμικό (για να μην πούμε τίποτα για την τεχνογνωσία και την εμπειρία) είναι συνήθως μικρότερη για ένα βασιζόμενο στα NT σύστημα, πρέπει να συνυπολογίζεται πάντα.[42]

Λέγεται ότι η ευχρηστία και η εξοικείωση επαυξάνει την ασφάλεια. Επειδή οι χρήστες είναι εξοικειωμένοι με τα NT, υπάρχουν λιγότερες πιθανότητες να διαμορφώσουν λανθασμένα το λειτουργικό σύστημα και να προκαλέσουν προβλήματα στην ασφάλεια. Αν και ίσως ισχύει το γεγονός ότι το Unix μπορεί να διαμορφωθεί με τέτοιο τρόπο ώστε να είναι ένα πιο ασφαλές περιβάλλον, είναι σίγουρο ότι δεν μπορεί ποτέ να επιτευχθεί ένα ασφαλές περιβάλλον εάν οι χρήστες δεν κατανοούν τις σωστές διαδικασίες χειρισμού του.[42]

Τέλος, υπάρχει και το επιχείρημα της ομοιομορφίας. Επειδή πολλοί οργανισμοί χρησιμοποιούν τα Windows NT για την παροχή υπηρεσιών αρχείων, εκτυπώσεων και εφαρμογών, είναι λογικό να θέλουν να βασιστούν αποκλειστικά σ' αυτή την πλατφόρμα για όλες τις υπηρεσίες που χρειάζονται. Αυτό καθιστά πιο εύκολη και πιο αρμονική την διαχείριση. Επίσης βοηθά στο να μειωθούν (έως να εκμηδενιστούν) τα προβλήματα συμβατότητας.[42]

Τα αδύνατα σημεία των Windows NT

Η μεγαλύτερη αδυναμία που αποδίδεται στα NT σχετίζεται με μία αντίληψη - την αντίληψη ότι η Microsoft είναι απρόθυμη να παραδεχθεί και να διορθώσει οποιεσδήποτε αδυναμίες στον τομέα της ασφάλειας. Αν και είναι γεγονός ότι κάποιος ανακάλυψε μία αδυναμία, ειδοποίησε ιδιωτικά την Microsoft και αργότερα την ανακοίνωσε στο ευρύ κοινό επειδή περίμενε ανεπιτυχώς για περισσότερο από έναν μήνα μέχρι να αναγγείλει μία διόρθωση η Microsoft, δεν υπάρχουν βάσιμα στοιχεία τα οποία να συνηγορούν ότι αυτή είναι η επίσημη πρακτική της Microsoft. Και μολονότι έχουν αποκαλυφθεί σημαντικά τρωτά σημεία, κατά το μεγαλύτερο μέρος τους περιορίζονται σε υπηρεσίες οι οποίες δεν εγκαθίστανται εκ των προτέρων στα NT και δεν πρέπει να ενεργοποιούνται

σε ένα σύστημα το οποίο λειτουργεί σαν firewall (όπως το IIS - το λογισμικό Web server της Microsoft).[43]

Λόγω της εξειδικευμένης και κλειστής φύσης των NT, δεν είναι γνωστά πολλά πράγματα για τις εσωτερικές διεργασίες των υπηρεσιών τους, ενώ και οι ίδιες οι υπηρεσίες δεν επιδέχονται διαμόρφωση σε τόσο υψηλό βαθμό όσο οι δαίμονες του Unix. Αυτό είναι ένας παράγοντας αβεβαιότητας για τους ειδικούς που αναζητούν την ασφαλέστερη πλατφόρμα για να εγκαταστήσουν μία λύση firewall.[43]

Άλλα αρνητικά σημεία είναι η ανάγκη επανεκκίνησης των NT servers όταν γίνονται αλλαγές στην διαμόρφωση τους (ή ακόμη και μετά από μερικές ημέρες/εβδομάδες συνεχούς λειτουργίας λόγω της αστάθειας του συστήματος), καθώς και το κόστος αγοράς και απόκτησης αδειών χρήσης για έναν NT server.[43]

2.3.1.5 Microsoft Windows 2000

Τα Windows 2000 έχουν πολλές από τις αδυναμίες των Windows NT, συμπεριλαμβανομένης της κλειστής φύσης τους, της πιθανολογούμενης απροθυμίας της Microsoft να παραδεχθεί (και να διορθώσει) τυχόν τρωτά σημεία και του σημαντικά αυξημένου κόστους που απαιτείται για την χρήση ενός προϊόντος Windows. Όμοια με τα NT, στα ισχυρά σημεία των Windows 2000 περιλαμβάνονται η εξοικείωση των χρηστών και η καθιέρωση ενός ομοιόμορφου περιβάλλοντος σε όλη την έκταση του δικτύου.[43]

Ωστόσο, σε αντίθεση με τα NT, τα Windows 2000 διαθέτουν κάποια μοναδικά στο είδος τους ισχυρά σημεία. Πρώτο απ' όλα είναι η δυνατότητα υλοποίησης αλλαγών στην διαμόρφωση χωρίς ανάγκη για την επανεκκίνηση του server. Κατά δεύτερον, η αυξημένη σταθερότητα του server, η οποία επιμηκύνει τον χρόνο συνεχούς λειτουργίας του (και κατά συνέπεια αυξάνει την αξιοπιστία). Και, τέλος, η δυνατότητα κεντρικού καθορισμού και επιβολής λεπτομερών ρυθμίσεων ασφάλειας (ονομάζονται Group Policies, Πολιτικές Ομάδων) αυξάνει δραματικά την συνολική ασφάλεια.[43]

Μετά από αρκετά χρόνια εμπειρίας με τα Windows 2000, οι περισσότεροι ειδικοί στον τομέα της ασφάλειας συμφωνούν ότι τα τρωτά σημεία του συστήματος βρίσκονται κυρίως στις πρόσθετες υπηρεσίες (όπως π.χ. στον Web server IIS που τρέχουν πάνω από το λειτουργικό σύστημα. Ωστόσο, ο πυρήνας του λειτουργικού συστήματος θεωρείται σε γενικές γραμμές ισχυρός. Επιπρόσθετα, η Windows παρουσίασε ένα δικό της firewall για τα Windows 2000. Γνωστό με το όνομα ISA Server (Internet Security and

Accelaration), το λογισμικό αυτό υποστηρίζει όλες τις βασικές λειτουργίες firewall και περιλαμβάνει πρόσθετες δυνατότητες, όπως τοπική αποθήκευση δεδομένων του Web, ανίχνευση εισβολών και ενοποίηση με το Active Directory της Microsoft.[44]

2.4 Βασιζόμενα σε hardware firewalls

Ονομαζόμενα επίσης "ολοκληρωμένες λύσεις", τα βασιζόμενα σε hardware firewalls χρησιμοποιούν εξειδικευμένο εξοπλισμό και λογισμικό. Συνήθως διατίθενται με την μορφή μιας μικρής σε μέγεθος συσκευής η οποία διαθέτει συνδέσεις δικτύου και ρεύματος. Στα βασιζόμενα σε hardware firewalls περιλαμβάνονται τα ακόλουθα[45]:

1) PIX της Cisco
2) Firewall-1 της Check Point
3) InstaGate της eSoft
4) WALL PRO της Sonic
5) Firebox της Watchguard

Τα ολοκληρωμένα συστήματα firewall παρέχουν μία λύση "όλα σε ένα", με τον κατασκευαστή τους να παρέχει τόσο το hardware, όσο και το λογισμικό και το λειτουργικό σύστημα. Οι ολοκληρωμένες λύσεις firewall είναι πολύ δημοφιλείς, κυρίως για τις μικρές επιχειρήσεις οι οποίες δεν διαθέτουν προσωπικό πληροφορικής πλήρους απασχόλησης και χρειάζονται μόνο τις βασικές λειτουργίες ενός firewall, χωρίς εξειδικευμένη διαμόρφωση. Οι μεγαλύτερες επιχειρήσεις βασίζονται σε ακριβότερες, τεχνολογίας αιχμής ολοκληρωμένες λύσεις firewall για την διαχείριση της αυξημένης κυκλοφορίας που παράγουν, επειδή έχουν πολύ μεγαλύτερο αριθμό υπολογιστών που χρειάζονται προστατευόμενη πρόσβαση στο internet, ή διαθέτουν sites ηλεκτρονικού εμπορίου τα οποία δέχονται εκατομμύρια επισκέπτες καθημερινά.[46]

2.4.1 Τα ισχυρά σημεία των βασιζόμενων σε hardware firewalls

Το μεγαλύτερο πλεονέκτημα των ολοκληρωμένων λύσεων firewall είναι ότι απαιτούν πολύ λίγο χρόνο για την διαμόρφωση τους. Πολλά firewalls είναι εκ των προτέρων διαμορφωμένα ώστε να προστατεύουν το δίκτυο σας κυριολεκτικά από την πρώτη στιγμή που τα εγκαθιστάτε. Συνδέοντας απλώς το internet στην μία θύρα και το εσωτερικό σας δίκτυο σε μία άλλη θύρα, η συσκευή αρχίζει αμέσως να φιλτράρει την κυκλοφορία του δικτύου. Οι μικρές επιχειρήσεις έχουν πολλά να ωφεληθούν από αυτή την απλότητα, κυρίως όταν δεν διαθέτουν έμπειρα στελέχη στο τμήμα μηχανογράφησης.

Εάν απαιτείται διαμόρφωση, αυτή μπορεί να γίνει μέσω μιας απλής εφαρμογής Web browser, ή με την εγκατάσταση ενός ειδικού βοηθήματος διαμόρφωσης.[46]

Η απόδοση είναι το άλλο πλεονέκτημα που εκτιμούν συχνά οι μεγάλες επιχειρήσεις οι οποίες αγοράζουν ολοκληρωμένες λύσεις firewall. Επειδή αυτά τα firewalls χρησιμοποιούν προγραμματιζόμενο hardware (γνωστό σαν firmware), μπορούν να λειτουργούν με πολύ υψηλότερες ταχύτητες σε σύγκριση με τα firewalls που διαθέτουν ένα επιπλέον επίπεδο λειτουργικού συστήματος και εξοπλισμού (τα οποία είναι αμφότερα σχεδιασμένα για την εκτέλεση εργασιών γενικής φύσης και δεν έχουν βελτιστοποιηθεί για τις εργασίες που σχετίζονται με την λειτουργία ενός firewall).[46]

Αυτή η επικέντρωση στην σχεδίαση ενός ειδικευμένου συστήματος μπορεί να οδηγήσει στην μείωση του κόστους ενός firewall, επειδή δεν απαιτείται η αγορά ενός λειτουργικού συστήματος και αδειών χρήσης, επιπρόσθετα με την εφαρμογή firewall τα πάντα περιλαμβάνονται σε ένα απόλυτα ενοποιημένο πακέτο από τον κατασκευαστή.[46]

2.4.2 Οι αδυναμίες των βασιζόμενων σε hardware firewalls

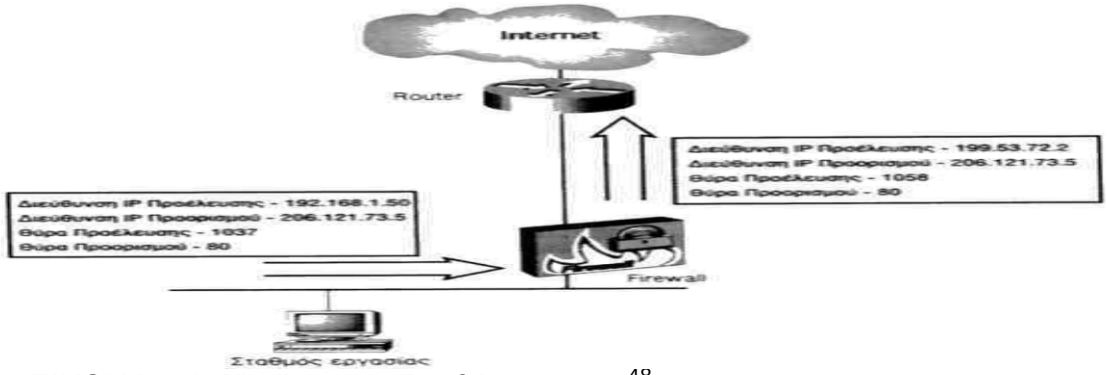
Από την άλλη, μία τέτοια μονολιθική προσέγγιση μπορεί να περιορίσει την ευελιξία ενός προϊόντος, ή την δυνατότητα αναβάθμισης του υποκείμενου hardware (π.χ. εγκατάσταση περισσότερης μνήμης RAM, όποτε απαιτηθεί). Τα βασιζόμενα σε hardware firewalls είναι επίσης περιοριστικά επειδή υποχρεώνουν έναν οργανισμό να βασίζεται σε έναν μόνο κατασκευαστή για ολόκληρο το σύστημα ασφάλειας του, σε αντίθεση με ένα πιο αρθρωτό σύστημα του οποίου τα επιμέρους συστατικά θα μπορούσαν να είναι "τα καλύτερα του είδους τους" - το καλύτερο λειτουργικό σύστημα με το καλύτερο firewall, το οποίο θα τροφοδοτεί με δεδομένα το καλύτερο σύστημα ανάλυσης, προερχόμενα όλα από διαφορετικούς κατασκευαστές.[47]

Τα βασιζόμενα σε hardware firewalls θεωρούνται επίσης πιο ακριβά από τις απλούστερες, βασιζόμενες μόνο σε λογισμικό λύσεις και, ανάλογα με το επίπεδο της πολυπλοκότητας που απαιτεί ο οργανισμός σας, ένα "παραδοσιακό", βασιζόμενο σε λογισμικό firewall μπορεί να σας εξυπηρετεί καλύτερα. Ωστόσο, η θεώρηση αυτή αλλάζει πολύ γρήγορα, δεδομένου ότι οι τιμές πέφτουν (ενώ οι δυνατότητες αυξάνονται). Σε συνδυασμό με την πληθώρα των βασιζόμενων σε hardware firewalls με τιμές που στοχεύουν στην αγορά των μικρών γραφείων και επιχειρήσεων, πολλές εταιρείες βρίσκουν αυτές τις συσκευές εξαιρετικά ελκυστικές.[47]

2.5 Μετάφραση διευθύνσεων IP

Η μετάφραση IP διευθύνσεων θεωρείται βασική λειτουργία σε ένα firewall. Μην εμπιστεύεστε προϊόντα firewall τα οποία δεν περιλαμβάνουν αυτή τη δυνατότητα. Όταν μία διεύθυνση IP μετατρέπεται από μία τιμή σε μία άλλη, η διαδικασία αυτή αποκαλείται μετάφραση διευθύνσεων (address translation). Η δυνατότητα αυτή υλοποιείται στα περισσότερα προϊόντα firewall και τυπικά χρησιμοποιείται όταν δεν θέλετε να επιτρέπετε στα απομακρυσμένα συστήματα να γνωρίζουν τις πραγματικές διευθύνσεις IP των συστημάτων του εσωτερικού σας δικτύου. Η εικόνα 2.1 παρουσιάζει ένα τυπικό δείγμα αυτής της διαμόρφωσης.[47]

Ένας σταθμός εργασίας στο εσωτερικό μας δίκτυο επιθυμεί να προσπελάσει ένα εξωτερικό Web site. Διατυπώνει μία αίτηση και παραδίδει αυτή την πληροφορία στην προεπιλεγμένη πύλη επικοινωνίας, η οποία στην περίπτωση μας είναι το firewall. Ωστόσο, ο σταθμός εργασίας έχει ένα μικρό πρόβλημα: το υπο-δίκτυο στο οποίο βρίσκεται χρησιμοποιεί ιδιωτική διευθυνσιοδότηση.



ΕΙΚΟΝΑ 2.1: Μετάφραση διευθύνσεων IP.[48]

Ο όρος ιδιωτική *διευθυνσιοδότηση (private addressing*) σημαίνει την χρήση περιοχών διευθύνσεων IP σε υπο-δίκτυα οι οποίες μπορούν να χρησιμοποιούνται από οποιονδήποτε οργανισμό για την διευθυνσιοδότηση των εσωτερικών του συστημάτων. Αυτό είναι δυνατό επειδή αυτές οι περιοχές διευθύνσεων δεν επιτρέπεται να δρομολογούνται στο Internet. Αν και αυτό σημαίνει ότι μπορούμε να χρησιμοποιούμε αυτές τις διευθύνσεις χωρίς φόβο συγκρούσεων, σημαίνει επίσης ότι για οποιαδήποτε αίτηση στέλνουμε σε ένα εξωτερικό σύστημα, δεν υπάρχει έγκυρη οδός για την αποστολή της απάντησης. Αυτές οι περιοχές διευθύνσεων είναι[48]:

10.0.0.0 έως 10.255.255.255
172.16.0.0 έως 172.32.255.255
192.168.0.0 έως 192.168.255.255

Συνεπώς, αν και ο σταθμός εργασίας μας μπορεί να στείλει μία αίτηση στον απομακρυσμένο server, ο απομακρυσμένος server δεν μπορεί να του στείλει την απάντηση. Σ' αυτό ακριβώς το σημείο είναι χρήσιμη η μετάφραση διευθύνσεων: μπορούμε να αντιστοιχίσουμε την διεύθυνση IP του σταθμού εργασίας σε κάποια άλλη, έγκυρη διεύθυνση IP. Στην περίπτωση της εικόνας 1.10, μεταφράσαμε την διεύθυνση IP του σταθμού εργασίας (192.168.1.50) στην έγκυρη διεύθυνση που χρησιμοποιείται από την θύρα επικοινωνίας του firewall με τον έξω κόσμο, 199.53.72.2. [48]

Υπάρχουν τρεις τρόποι χρήσης της δυνατότητας μετάφρασης διευθύνσεων[49]:

1. Απόκρυψη της Μετάφρασης Διευθύνσεων Δικτύου (Network Address Translation,NAT)
2. Στατική Μετάφραση Διευθύνσεων Δικτύου
3. Μετάφραση Διευθύνσεων θυρών (Port Address Translation, PAT)

2.5.1 Απόκρυψη της Μετάφρασης Διευθύνσεων Δικτύου

Η απόκρυψη μετάφρασης διευθύνσεων δικτύου λειτουργεί ακριβώς όπως περιγράφεται στην εικόνα 2.1. Όλα τα συστήματα του εσωτερικού δικτύου "κρύβονται" πίσω από μία μεμονωμένη διεύθυνση IP. Αυτή μπορεί να είναι η διεύθυνση IP του ίδιου του firewall, ή κάποια άλλη έγκυρη διεύθυνση IP. Αν και η απόκρυψη NAT μπορεί θεωρητικά να υποστηρίξει χιλιάδες ταυτόχρονες συνόδους επικοινωνίας, μπορούν να χρησιμοποιηθούν περισσότερες από μία διευθύνσεις απόκρυψης, εάν χρειάζεστε επιπλέον υποστήριξη.[50]

Ο μεγαλύτερος περιορισμός της απόκρυψης NAT είναι ότι δεν επιτρέπει την δημιουργία συνόδων εισερχόμενης επικοινωνίας. Επειδή όλα τα συστήματα του εσωτερικού δικτύου κρύβονται πίσω από μία μόνο διεύθυνση, το firewall δεν έχει τρόπο για να εξακριβώσει σε ποιο σύστημα του εσωτερικού δικτύου απευθύνεται μία αίτηση για επικοινωνία από ένα απομακρυσμένο σύστημα. Επειδή δεν υπάρχει αντιστοίχιση με συγκεκριμένα συστήματα του εσωτερικού δικτύου, όλες οι αιτήσεις για επικοινωνία που προέρχονται από εξωτερικά συστήματα απορρίπτονται.[51]

Ο περιορισμός αυτός μπορεί στην πραγματικότητα να θεωρηθεί λειτουργία, δεδομένου ότι βοηθά στην επαύξηση της ασφάλειας του δικτύου σας. Εάν η πολιτική ασφάλειας για το δίκτυο σας υπαγορεύει ότι οι χρήστες των εσωτερικών συστημάτων δεν επιτρέπεται να τρέχουν δικούς τους servers στους σταθμούς εργασίας τους (Web, FTP, κ.λ.π.), η χρήση απόκρυψης NAT για όλους τους σταθμούς εργασίας του

εσωτερικού δικτύου είναι ένας γρήγορος τρόπος για να διασφαλίζετε ότι οι υπηρεσίες αυτές δεν θα μπορούν να προσπελάζονται απευθείας από εξωτερικά συστήματα.[51]

2.5.2 Στατική Μετάφραση Διευθύνσεων Δικτύου

Η στατική μετάφραση διευθύνσεων δικτύου λειτουργεί παρόμοια με την απόκρυψη της Μετάφρασης Διευθύνσεων Δικτύου, εκτός από το ότι αντιστοιχίζεται μία μεμονωμένη ιδιωτική διεύθυνση IP σε κάθε χρησιμοποιούμενη δημόσια διεύθυνση IP. Αυτό είναι χρήσιμο εάν έχετε ένα εσωτερικό σύστημα το οποίο χρησιμοποιεί ιδιωτικές διευθύνσεις IP, αλλά θέλετε να κάνετε το σύστημα αυτό προσπελάσιμο από το Internet. Επειδή μόνο ένα σύστημα του εσωτερικού δικτύου σχετίζεται με κάθε έγκυρη διεύθυνση IP, το firewall δεν έχει κανένα πρόβλημα να εξακριβώσει πού πρέπει να προωθήσει την κυκλοφορία.[51]

Για παράδειγμα, ας υποθέσουμε ότι έχετε έναν Exchange server στο δίκτυο σας και θέλετε να ενεργοποιήσετε την υπηρεσία SMTP για να μπορείτε να διακινείτε ηλεκτρονικό ταχυδρομείο μέσω Internet. Ο Exchange server έχει διεύθυνση IP 172.25.23.13, η οποία ανήκει στον χώρο ιδιωτικών διευθύνσεων. Για τον λόγο αυτό, το συγκεκριμένο σύστημα δεν μπορεί να επικοινωνήσει με συστήματα από το Internet.[51]

Στο σημείο αυτό έχουμε δύο επιλογές:

Μπορούμε να αλλάξουμε την διεύθυνση από έναν αριθμό "ιδιωτικής" χρήσης σε έναν έγκυρο αριθμό για ολόκληρο το υπο-δίκτυο στο οποίο βρίσκεται ο Exchange server.

Μπορούμε να εκτελούμε στατική μετάφραση διευθύνσεων δικτύου στο firewall.Σαφώς, η δεύτερη επιλογή είναι πολύ πιο εύκολο να υλοποιηθεί, θα επέτρεπε στα συστήματα του εσωτερικού δικτύου να συνεχίσουν να επικοινωνούν με τον Exchange server· χρησιμοποιώντας την ιδιωτική διεύθυνση, ενώ θα μετάφραζε όλη την προοριζόμενη για το Internet επικοινωνία σε μία εικονική έγκυρη διεύθυνση IP.[51] Η στατική μετάφραση διευθύνσεων δικτύου είναι επίσης χρήσιμη για υπηρεσίες οι οποίες θα καταρρεύσουν εάν χρησιμοποιηθεί απόκρυψη NAT. Για παράδειγμα, ορισμένες μορφές επικοινωνίας μεταξύ DNS servers απαιτούν τον ορισμό τόσο της θύρας προέλευσης, όσο και της θύρας προορισμού στον αριθμό 53. Εάν χρησιμοποιείτε απόκρυψη NAT, το firewall θα είναι υποχρεωμένο να αλλάξει την θύρα προέλευσης σε κάποιον αυθαίρετα επιλεγμένο ανώτερο αριθμό θύρας, πράγμα το οποίο θα διέκοπτε αυτή την σύνοδο επικοινωνίας. Χρησιμοποιώντας στατική μετάφραση διευθύνσεων

δικτύου, ο αριθμός θύρας δεν χρειάζεται να αλλαχθεί και οι σύνοδοι επικοινωνίας μπορούν να διεξάγονται κανονικά.[52]

2.5.3 Μετάφραση Διευθύνσεων θυρών

Η μετάφραση διευθύνσεων θυρών *(*Port Address Translation, PAT*)* χρησιμοποιείται από τα περισσότερα προϊόντα firewall που λειτουργούν σαν διακομιστές μεσολάβησης (proxy). Όταν χρησιμοποιείται μετάφραση διευθύνσεων θυρών, όλη η εξερχόμενη κυκλοφορία μεταφράζεται στην εξωτερική διεύθυνση IP που χρησιμοποιεί το firewall, παρόμοια με την απόκρυψη NAT. Ωστόσο, ανόμοια με την απόκρυψη NAT, πρέπει να χρησιμοποιείται η εξωτερική διεύθυνση του firewall δεν μπορεί να οριστεί κάποια άλλη έγκυρη τιμή.[53]

Η μέθοδος με την οποία αντιμετωπίζεται η εισερχόμενη κυκλοφορία διαφέρει από προϊόν σε προϊόν. Σε ορισμένες υλοποιήσεις αντιστοιχίζονται θύρες σε συγκεκριμένα συστήματα. Για παράδειγμα, όλη η κυκλοφορία SMTP που φτάνει στο firewall από τον έξω κόσμο (με αριθμό θύρας προορισμού 25) προωθείται αυτόματα σε ένα συγκεκριμένο σύστημα του εσωτερικού δικτύου. Για ένα μικρό περιβάλλον, ο περιορισμός αυτός σπανίως αποτελεί πρόβλημα. Ωστόσο, για μεγαλύτερα περιβάλλοντα με πολλαπλά συστήματα τα οποία τρέχουν τον ίδιο τύπο server (π.χ. πολλαπλοί mail ή FTP servers), η διαδικασία αυτή μπορεί να αποτελέσει μεγάλο εμπόδιο.[53]

Για να παρακάμψουν αυτό το πρόβλημα, ορισμένοι διακομιστές μεσολάβησης μπορούν να αναλύουν το περιεχόμενο των δεδομένων με στόχο την υποστήριξη πολλαπλών υπηρεσιών στο εσωτερικό δίκτυο. Για παράδειγμα, ένας διακομιστής μεσολάβησης μπορεί να έχει τη δυνατότητα να προωθεί όλη την εισερχόμενη ηλεκτρονική αλληλογραφία (SMTP) που στέλνεται στην διεύθυνση user@eng.bofh.org σε ένα σύστημα του εσωτερικού δικτύου και όλη την εισερχόμενη ηλεκτρονική αλληλογραφία που στέλνεται στην διεύθυνση user@hr.bofh.org σε ένα άλλο σύστημα.[53]

Εάν έχετε πολλαπλούς servers στο εσωτερικό δίκτυο οι οποίοι τρέχουν την ίδια υπηρεσία, βεβαιωθείτε ότι το σύστημα firewall που επιλέγετε μπορεί να κάνει διάκριση μεταξύ τους.[53]

2.6 Καταγραφή και ανάλυση δραστηριοτήτων από το firewall

Αν και η βασική λειτουργία ενός firewall είναι ο έλεγχος της κυκλοφορίας που περνάει από την περίμετρο ενός δικτύου, η δεύτερη πιο σημαντική λειτουργία του είναι η δυνατότητα να καταγράφει και να αναλύει όλη την κυκλοφορία που συναντά. Η

καταγραφή είναι σημαντική, επειδή σας επιτρέπει να γνωρίζετε ποιοι διασχίζουν την περίμετρο του δικτύου σας - και ποιοι επιχείρησαν να την διασχίσουν αλλά απέτυχαν. Η ανάλυση είναι σημαντική επειδή μπορεί να μην είναι άμεσα εμφανές με μια πρόχειρη ματιά στα αρχεία καταγραφής ποια περιστατικά είναι πραγματικές απόπειρες παραβίασης της περιμέτρου του δικτύου και ποια αποτελούν απλώς έρευνες για ανοίγματα στον "φράχτη" κατά την προετοιμασία για μία μελλοντική εισβολή.[54]

Τι είναι αυτό που χαρακτηρίζει την λειτουργία καταγραφής ενός firewall σαν καλή;Προφανώς, η απάντηση σ' αυτό το ερώτημα είναι υποκειμενική. Ωστόσο, υπάρχουν ορισμένα χαρακτηριστικά τα οποία είναι απαραίτητα και θα πρέπει να τα εξετάσετε[54]:

Η λειτουργία καταγραφής θα πρέπει να παρουσιάζει όλες τις καταχωρίσεις με σαφή, ευανάγνωστη μορφή.

Θα πρέπει να έχετε τη δυνατότητα να εμφανίζετε όλες τις καταχωρίσεις που περιέχει ένα αρχείο καταγραφής για να μπορείτε να προσδιορίζετε ευκολότερα τα μοτίβα κυκλοφορίας, αν και η δυνατότητα εξαγωγής των δεδομένων του αρχείου καταγραφής σε ένα ειδικευμένο εργαλείο ανάλυσης έχει ακόμη μεγαλύτερη αξία.

Η λειτουργία καταγραφής θα πρέπει να προσδιορίζει με σαφήνεια ποια κυκλοφορία έχει μπλοκαριστεί και σε ποια κυκλοφορία επετράπη η διέλευση.

Στην ιδανική περίπτωση, θα πρέπει να έχετε δυνατότητα διαχείρισης του αρχείου καταγραφής με λειτουργίες όπως το φιλτράρισμα και η ταξινόμηση, έτσι ώστε να μπορείτε να επικεντρώνεστε σε συγκεκριμένα είδη κυκλοφορίας, αν και η λειτουργία αυτή ανήκει περισσότερο σε ένα εργαλείο ανάλυσης.

Το αρχείο καταγραφής δεν θα πρέπει να απορρίπτει τα προηγούμενα περιεχόμενα του (ολόκληρα ή μεμονωμένες καταχωρίσεις) όταν υπερβαίνει ένα συγκεκριμένο όριο μεγέθους.

Θα πρέπει να έχετε τη δυνατότητα να εξετάζετε με ασφάλεια τα αρχεία καταγραφής από μια απομακρυσμένη θέση.

Το λογισμικό που χρησιμοποιείται για την καταγραφή θα πρέπει να παρέχει κάποια μέθοδο για την εξαγωγή των δεδομένων σε μία τουλάχιστον κοινή μορφή αρχείου, όπως π.χ. στην μορφή απλού κειμένου ASCII (κατά προτίμηση με κάποιο είδος οριοθέτησης). Η δυνατότητα αυτή επιτρέπει την περαιτέρω διαχείριση των δεδομένων καταγραφής με ειδικά εργαλεία παραγωγής αναφορών, ή εφαρμογές φύλλων εργασίας ή βάσεων δεδομένων.

Αν και είναι αρκετές, όλες οι προαναφερθείσες δυνατότητες είναι σημαντικές. Σπανίως ένας εισβολέας θα καταφέρνει να αποκτήσει πρόσβαση με την πρώτη του προσπάθεια. Εάν προϋπολογίσετε χρόνο για την σχολαστική εξέταση των αρχείων καταγραφής σε τακτική βάση, θα μπορείτε να αποθαρρύνετε επίδοξους εισβολείς πριν καν κάνουν την πρώτη τους προσπάθεια. Για τον σκοπό αυτό, ένα καλό εργαλείο καταγραφής είναι σίγουρα πολύ χρήσιμο.[55]

2.7 Εικονικά δίκτυα (VPN)

Τα εικονικά ιδιωτικά δίκτυα (Virtual Private Networks, VPN) θεωρούνται σαν το χαρακτηριστικό εκείνο που ξεχωρίζει ένα υψηλών προδιαγραφών firewall από τα υπόλοιπα. Τα VPN επιτρέπουν πιστοποιημένη και κρυπτογραφημένη πρόσβαση από το "δημόσιο" Internet σε ένα εσωτερικό δίκτυο intranet. Αυτό σημαίνει ότι αντί για την ακριβή επικοινωνία από σημείο σε σημείο, τα τοπικά δίκτυα και οι χρήστες φορητών υπολογιστών μπορούν να χρησιμοποιούν τις φθηνές υπηρεσίες μιας εταιρείας παροχής Internet για να επικοινωνούν με τα εσωτερικά συστήματα του οργανισμού τους.

Ωστόσο, το να παρέχει κανείς απλές υπηρεσίες VPN δεν είναι αρκετό, θα πρέπει να εξακριβώσετε τις επιλογές διαμόρφωσης, διαχείρισης και κρυπτογράφησης που παρέχει το προϊόν firewall που επιλέξατε για εικονικά ιδιωτικά δίκτυα. Σε ορισμένες περιπτώσεις, μία αποκλειστικής λειτουργίας, εξειδικευμένη λύση VPN η οποία συνεργάζεται με το firewall παρέχει τα καλύτερα αποτελέσματα.[56]

2.8 Ανίχνευση εισβολέων και άμυνα

Η δυνατότητα ενός firewall να ειδοποιεί τον επόπτη του δικτύου όταν λαμβάνει χώρα μία επίθεση είναι επίσης ένας παράγοντας ο οποίος θα πρέπει να λαμβάνεται υπόψη κατά την αγορά. Στην περίπτωση των πολυδιαφημισμένων επιθέσεων DoS (άρνηση εξυπηρέτησης) που συνέβησαν τον Φεβρουάριο του 2000, η δυνατότητα των συστημάτων firewall να ειδοποιήσουν αμέσως το προσωπικό της μηχανογράφησης για ασυνήθιστη δραστηριότητα στο δίκτυο επέτρεψε σε πολλές εγκαταστάσεις να επανέλθουν σε κανονική λειτουργία μέσα σε μία μόλις ώρα.[56]

Τα μελλοντικά συστήματα firewall υπόσχονται έναν βαθμό συνεργασίας ο οποίος θα επιτρέπει σε ολόκληρα δίκτυα να αντιδρούν και να αναδιαμορφώνουν τους εαυτούς τους στην περίπτωση επιθέσεων. Αν και οι ειδικοί πιστεύουν ότι η τεχνολογία που απαιτείται γι' αυτό το επίπεδο προληπτικής παρακολούθησης και αντίδρασης είναι εφικτή, παραμένουν αρκετές προκλήσεις. Για να είναι αληθινά αποτελεσματικό ένα τέτοιο σύστημα, θα απαιτούσε την συνεργασία και επικοινωνία όλων των

επηρεαζόμενων μερών, ακόμη κι αν εμπλέκονται διαφορετικές (ή ακόμη και ανταγωνιστικές) επιχειρήσεις και οργανισμοί. Υποθέτοντας ότι υπάρχει ένα τέτοιο επίπεδο επικοινωνίας και ενοποίησης, οι εισβολείς θα ήταν πολύ πιο δύσκολο να διατηρήσουν την ανωνυμία τους και τα αποτελέσματα μιας επίθεσης θα εξουδετερώνονταν πολύ πιο γρήγορα.[56]

Υπάρχουν ήδη επίσημες και ανεπίσημες ομάδες οι οποίες παρακολουθούν και αναφέρουν τις περιπτώσεις επιθέσεων, καθώς και τα περιστατικά μόλυνσης από ιούς, worms και Δουρείους ίππους (θυμηθείτε το worm "I love You" τον Μάιο του 2000). Ωστόσο, οι μηχανισμοί αναφοράς είναι συνήθως "χειροκίνητοι" και απαιτούν την επίβλεψη κάποιου. Στην ιδανική περίπτωση, οι αναφορές θα πρέπει να παράγονται αυτόματα, να είναι τυποποιημένες και να προβλέπουν ευφυή συστήματα με επαρκείς πληροφορίες για την λήψη αυτόματων ή προληπτικών αμυντικών μέτρων.[57]

Σαν αποτέλεσμα της ανάγκης για αυτοματοποιημένη αντίδραση, πολλά firewalls παρέχουν λειτουργίες ανίχνευσης εισβολών (IDS, Intrusion Detection System), ενώ ειδικευμένα συστήματα IDS επιχειρούν, με ανάμεικτα αποτελέσματα, να ενημερώνουν αυτόματα τους κανόνες των firewalls όταν ανιχνεύονται επιθέσεις. Ένα πιθανό πρόβλημα αυτής της προσέγγισης είναι ότι ένας εισβολέας μπορεί να εκμεταλλευτεί αυτή την δυναμική αντίδραση για να προκαλέσει το κλείσιμο έγκυρων θυρών, προκαλώντας την υπερ-αντίδραση των συνεργαζόμενων συστημάτων IDS και firewall.[57]

2.9 Ενοποίηση και έλεγχος πρόσβασης

Τα firewalls ενοποιούνται ολοένα και περισσότερο με άλλα συστήματα και υπηρεσίες δικτύου. Η τάση αυτή υπόσχεται να απλοποιήσει τη διαχείριση και να μειώσει την πολυπλοκότητα και το συνολικό κόστος λειτουργίας, δεδομένου ότι τα firewalls δεν θα χρειάζεται πλέον να παρέχουν υπηρεσίες οι οποίες υπάρχουν ήδη στο δίκτυο που εγκαθίστανται.[57]

Παραδείγματα ενοποίησης είναι οι υπηρεσίες καταλόγου και πιστοποίησης (directory/ authentication services) που εξαλείφουν την ανάγκη ύπαρξης διπλότυπων πληροφοριών για τους λογαριασμούς χρηστών και επιτρέπουν την δημιουργία προσαρμόσιμων οχημάτων πιστοποίησης. Δυο πρότυπα τα οποία παρέχουν αυτές τις υπηρεσίες είναι το LDAP (Lightweight Directory Access Protocol) και το RADIUS (Remote Authentication Dial In User Service).[57]

2.9.1 Lightweight Directory Access Protocol (LDAP)

Το LDAP δημιουργεί ένα "τούνελ" μεταξύ δυο υπηρεσιών καταλόγου (directory services), ή μεταξύ μιας υπηρεσίας καταλόγου και ενός client συστήματος. Για τα firewalls, αυτό σημαίνει ότι αντι να δημιουργούν διπλότυπους λογαριασμούς χρηστών και ομάδων/ρόλων, το σύστημα μπορεί να χρησιμοποιεί τους λογαριασμούς και τις ιδιότητες που είναι αποθηκευμένες σε μία υπηρεσία καταλόγου τρίτου κατασκευαστή για τον καθορισμό των επιπέδων πρόσβασης. Αυτό έχει άμεση θετική επίδραση, επειδή μειώνει τον διαχειριστικό φόρτο (δημιουργία και διαχείριση διπλότυπων λογαριασμών χρηστών/ρόλων) και την πολυπλοκότητα - τον μεγαλύτερο εχθρό οποιουδήποτε συστήματος ασφάλειας. Παραδείγματα υπηρεσιών καταλόγου είναι το AD (Active Directory) της Microsoft, το NDS (Netware Directory Services) της Novell και το Directory Server της iPlanet.[57]

2.9.2 Remote Authentication Dial In User Service (RADIUS)

Το RADIUS αποτελεί μία ανεξάρτητη και επεκτάσιμη πλατφόρμα πιστοποίησης. Οι RADIUS servers όχι μόνο επιτρέπουν την υλοποίηση προσαρμοζόμενων σχημάτωνπιστοποίησης (όπως οι έξυπνες κάρτες [smart cards] ή οι συσκευές ελέγχου βιομετρικών χαρακτηριστικών), αλλά αφαιρούν επίσης από το firewall (ή τις συμβατές με LDAP υπηρεσίες καταλόγου) τον φόρτο της πιστοποίησης. Παρέχοντας μία υποδομή αποκλειστικά αφιερωμένη στην πιστοποίηση, το RADIUS απλοποιεί και ενδυναμώνει την διαδικασία πιστοποίησης.[58]

2.10 Εργαλεία τρίτων κατασκευαστών

Πολλά σύγχρονα δίκτυα βασίζονται σε πολλαπλές τεχνολογίες διάφορων κατασκευαστών αν και αυτό μπορεί να είναι η ιδανική επιλογή για τον οργανισμό σας, αποτελεί πραγματικό εφιάλτη για τους επόπτες δικτύων. Ευτυχώς αρχίζουν να παρουσιάζονται νέες τεχνολογίες, οι οποίες είναι ειδικά σχεδιασμένες ώστε να επιτρέπουν την κεντρική παρακολούθηση και διαχείριση όλων των συσκευών και εφαρμογών ενός δικτύου. Ένα θαυμάσιο τέτοιο παράδειγμα είναι το OpenView της HP, το οποίο παρέχει λειτουργίες διαχείρισης στους ακόλουθους τομείς[59]:

- Εφαρμογές
- Διαθεσιμότητα
- Δίκτυα
- Απόδοση

- Υπηρεσίες
- Συστήματα
- Αποθήκευση και Δεδομένα

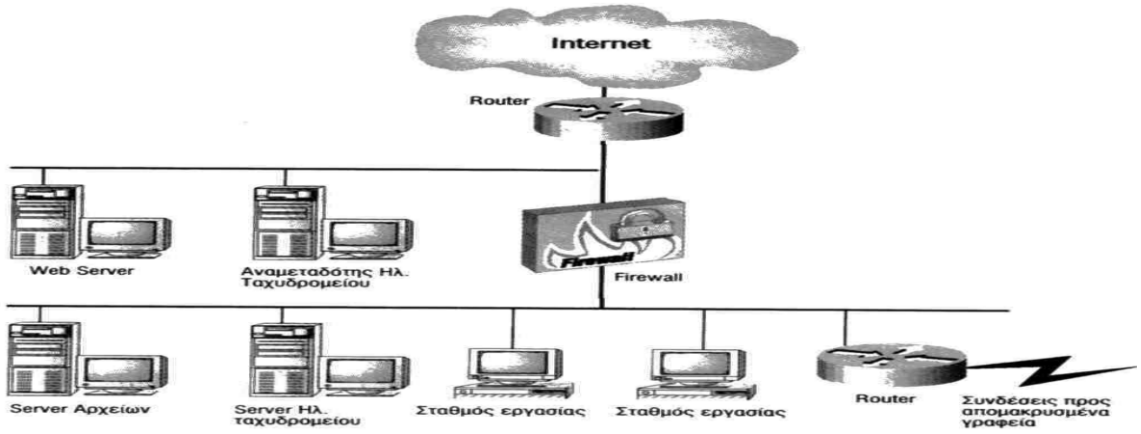
Η δυνατότητα ενός firewall να συνεργάζεται με εργαλεία διαχείρισης τρίτων κατασκευαστών θα μπορούσε να είναι αποφασιστικός παράγοντας κατά την επιλογή ενός συγκεκριμένου προϊόντος.[59]

Αλλά η διαχείριση δεν είναι ο μοναδικός τομέας για τον οποίο μπορείτε να βρείτε προϊόντα τρίτων. Πολλά προϊόντα, συμπεριλαμβανομένου του VPN-1 της Check Point, του PIX της Cisco και του ISA της Microsoft, επιτρέπουν σε άλλους κατασκευαστές να επεκτείνουν τις λειτουργίες τους ώστε να περιλαμβάνουν φιλτράρισμα διευθύνσεων URL, ανίχνευση/εξάλειψη ιών και προστασία από ανεπιθύμητα e-mail.

Αυτά τα επιπλέον πλεονεκτήματα θα μπορούσαν κάλλιστα να αιτιολογήσουν το αυξημένο κόστος ενός τέτοιου προϊόντος.[59]

2.11 Η εγκατάσταση ενός firewall

Αν και υπάρχουν πολλές απόψεις σχετικά με την εγκατάσταση ενός firewall, ο πιο κοινός τρόπος εγκατάστασης παρουσιάζεται στην εικόνα 2.2.



ΕΙΚΟΝΑ 2.2: Σχηματική αναπαράσταση της εγκατάστασης του firewall σε ένα δίκτυο.[60]

Μ' αυτή την προσέγγιση, το firewall προστατεύει όλα τα συστήματα του εσωτερικού δικτύου από τις προερχόμενες από το Internet επιθέσεις. Προστατεύονται ακόμη και τα απομακρυσμένα συστήματα που συνδέονται στο δίκτυο του οργανισμού μέσω μιας σύνδεσης WAN. Όλα τα συστήματα που είναι προσπελάσιμα από το Internet (π.χ. ο Web server και ο αναμεταδότης ηλεκτρονικού ταχυδρομείου) είναι απομονωμένα

σε ξεχωριστό υπο-δίκτυο. Αυτό το υπο-δίκτυο αναφέρεται με τον όρο DMZ (demilitarized zone, αποστρατικοποιημένη ζώνη), επειδή αν και μπορεί να είναι ασφαλές από τυχόν επιθέσεις, δεν μπορείτε να είστε 100% σίγουροι για την ασφάλεια του, δεδομένου ότι επιτρέπετε τις εισερχόμενες συνδέσεις στα συστήματα του.[60]

Η χρήση ενός υπο-δικτύου σαν αποστρατικοποιημένη ζώνη σας παρέχει πρόσθετη προστασία έναντι επιθέσεων. Επειδή ορισμένες εισερχόμενες υπηρεσίες είναι ανοικτές σ' αυτά τα συστήματα, ένας εισβολέας ίσως καταφέρει να αποκτήσει πρόσβαση υψηλού επιπέδου σ' αυτά. Ακόμη κι αν συμβεί αυτό, όμως, υπάρχουν λίγες πιθανότητες να παραβιαστούν άλλα συστήματα του εσωτερικού δικτύου, δεδομένου ότι οι μηχανές αυτές είναι απομονωμένες από το υπόλοιπο δίκτυο.[61]

Στο firewall μπορεί να προστεθούν επιπλέον κάρτες δικτύου για τον έλεγχο άλλων μορφών απομακρυσμένης πρόσβασης. Για παράδειγμα, εάν μία εταιρεία έχει συνδέσεις WAN με συνεργάτες που δεν ανήκουν επίσημα σ' αυτήν, θα μπορούσατε να δημιουργήσετε ένα νέο υπο-δίκτυο μέσω μιας επιπλέον κάρτας δικτύου στο firewall.

Όλοι οι routers που χρησιμοποιούνται για την επικοινωνία με τους απομακρυσμένους συνεργάτες θα έπρεπε να τοποθετηθούν σ' αυτό το υπο-δίκτυο. Το firewall θα μπορούσε να ελέγχει την κυκλοφορία μεταξύ των συστημάτων αυτών των συνεργατών και του εσωτερικού δικτύου του οργανισμού σας.[61]

Επίσης, μπορούμε να χρησιμοποιήσουμε την δυνατότητα στατικού φιλτραρίσματος πακέτων του router μας για να αυξήσουμε ακόμη περισσότερο την ασφάλεια. Αυτή η προσέγγιση μας επιτρέπει να υλοποιήσουμε ένα πολλαπλών επιπέδων τείχος προστασίας στην περίμετρο του δικτύου σας. Εάν παρουσιαστεί απόπειρα παραβίασης σε μία από τις συσκευές ασφάλειας, η δεύτερη συσκευή θα μπορέσει να "καλύψει" την διαρροή.[61]

ΚΕΦΑΛΑΙΟ 3^{Ο} : ΤΟ PIX FIREWALL ΤΗΣ CISCO

Σε αυτό το κεφάλαιο παρουσιάζεται το PIX firewall της Cisco όπου αναφέρονται οι λειτουργίες και τα χαρακτηριστικά του.

3.1 Περιληπτική παρουσίαση του PIX Firewall

Ο στόχος της σειράς προϊόντων Firewall PIX της Cisco είναι η επέκταση της ήδη μεγάλης παρουσίας αυτής της εταιρείας στην αναπτυσσόμενη αγορά των βασιζόμενων σε hardware συστημάτων firewall - κυρίως για μικρότερες επιχειρήσεις. Η Cisco προσπαθεί να παρέχει υπηρεσίες οι οποίες καλύπτουν ολόκληρη την επιχείρηση σε ένα μικρό "πακέτο", για δίκτυα τα οποία διαθέτουν μόνιμη σύνδεση στο Internet.[62]

Ειλικρινά, η *Cisco* έχει κάνει θαυμάσια δουλειά: κατάφερε να ενσωματώσει εξελιγμένες δυνατότητες σε ένα σχετικά φθηνό, εύκολο στην διαχείριση, μικρό πακέτο. Στις λειτουργίες firewall του PIX περιλαμβάνονται οι ακόλουθες[62]:

- **Adaptive Security Algorithm (ASA).** Η διαδικασία που εξετάζει την κατάσταση κάθε πακέτου.
- **Έλεγχος πρόσβασης (Access Control).** Το PIX προκαθορίζει περισσότερα από 85 πρωτόκολλα, υπηρεσίες και εφαρμογές, για γρήγορη και ευέλικτη διαχείριση.
- **Υποστήριξη για ιδιωτικά εικονικά δίκτυα (VPN).** Χρησιμοποιώντας το πρωτόκολλο IPsec, το PIX μπορεί να συνεργάζεται με άλλα προϊόντα VPN.
- **Σύστημα Ανίχνευσης Εισβολών σε Δίκτυα (Network Intrusion Detection System, NIDS).** Οι ενσωματωμένες λειτουργίες ανίχνευσης εισβολών μπορούν να εντοπίζουν πάνω από 55 τύπους βασιζόμενων στο Internet επιθέσεων.
- **Φιλτράρισμα διευθύνσεων URL** Όταν το PIX χρησιμοποιείται μαζί με τον Web-sense server της Cisco, η εξερχόμενη κυκλοφορία μπορεί να φιλτράρεται με βάση την διεύθυνση URL.
- **Μετάφραση Διευθύνσεων Δικτύου (Network Address Translation, NAT).** Πολλαπλοί υπολογιστές μπορούν να μοιράζονται την ίδια σύνδεση ευρείας ζώνης.

Στην πραγματικότητα, το PIX είναι ένας συνδυασμός hardware (η συσκευή) και λειτουργικού συστήματος (το λειτουργικό σύστημα της σειράς Firewall PIX). Το μέγεθος

της συσκευής εξαρτάται από το εκάστοτε μοντέλο· τα μικρότερα μοντέλα είναι ειδικά σχεδιασμένα ώστε να τοποθετούνται πάνω στο γραφείο, ενώ τα μεγαλύτερα μοντέλα είναι σχεδιασμένα ώστε να τοποθετούνται σε μια βάση στήριξης. Σ' αυτό το κεφάλαιο θα σας παρουσιάσουμε το μοντέλο 501, το οποίο απαιτεί ελάχιστα περισσότερο χώρο από την παλάμη του χεριού σας. Η συγκεκριμένη συσκευή έχει τα ακόλουθα χαρακτηριστικά[63]:

- Επεξεργαστή 133MHZ
- Μνήμη RAM 16 MB
- Σύνδεση WAN-Ethernet
- Τέσσερις θύρες για τοπικά δίκτυα (switched, 10/ 100 Mbps)
- Θύρα σειριακής επικοινωνίας (χρησιμοποιείται για την διαχείριση του firewall)
- Προαιρετικό φυσικό κλείδωμα ασφάλειας

Το λειτουργικό σύστημα που χρησιμοποιείται σ' αυτή την συσκευή (μέχρι την στιγμή που γράφονται αυτές οι γραμμές) βρίσκεται στην έκδοση 6.1 και είναι ειδικά σχεδιασμένο ώστε να υποστηρίζει της λειτουργίες firewall της συσκευής. Στις δυνατότητες αυτού του λειτουργικού συστήματος περιλαμβάνονται οι ακόλουθες[64]:

- Προκαθορισμένη διαμόρφωση για γρήγορη εγκατάσταση.
- Το εργαλείο *PDM* (PIX Device Manager) της Cisco, το οποίο παρέχει δυνατότητες διαχείρισης μέσω web.
- Πρόσβαση των χρηστών με βάση τις άδειες χρήσης (αρχικά παρέχονται άδειες για 10 χρήστες, αλλά προαιρετικά μπορείτε να αγοράσετε επιπλέον άδειες Χρήσης)
- Ενσωματωμένος DHCP (Dynamic Host Configuration Protocol) server
- Υποστήριξη για τα συστήματα κρυπτογράφησης DES (Data Encryption Standard και 3DES (Triple DES), με προαιρετική άδεια χρήσης.

Φυσικά, πριν μπορέσετε να εκμεταλλευτείτε όλες αυτές τις δυνατότητες θα πρέπει να εγκαταστήσετε το firewall. Αυτή η διαδικασία απαιτεί αρκετή προκαταρκτική μελέτη κα' μία συνολικότερη κατανόηση του δικτύου σας.[64]

3.2 Adaptive Security Algorithm

Τα περισσότερα σημερινά firewalls που καλύπτουν τις ανάγκες ενός ολόκληρου οργανισμού διαθέτουν κάποια μορφή φιλτραρίσματος με βάση την κατάσταση (stateful

filtering). Ο τρόπος με τον οποίο υλοποίησε η Cisco αυτή την δυνατότητα είναι γνωστός με το όνομα Adaptive Security Algorithm (ASA). Ο αλγόριθμος ASA παρακολουθεί όλα τα εξερχόμενα πακέτα και καταγράφει τις σχετικές πληροφορίες συνόδου. Καθώς φτάνουν εισερχόμενα πακέτα στο firewall, συγκρίνονται με τις ήδη αποθηκευμένες πληροφορίες κατάστασης για να επαληθευτεί το γεγονός ότι ανήκουν σε μία προϋπάρχουσα "συνομιλία" ή σύνοδο επικοινωνίας μεταξύ ενός υπολογιστή του εσωτερικού δικτύου και ενός υπολογιστή που βρίσκεται στον "έξω κόσμο".[65]

Ο αλγόριθμος ASA χρησιμοποιεί τους ακόλουθους κανόνες για την ανάλυση των πακέτων[65]:

- Εάν διαπιστωθεί ότι ένα πακέτο δεν ταιριάζει με τις ήδη αποθηκευμένες πληροφορίες κατάστασης, δεν επιτρέπεται να περάσει από το firewall.
- Οι εξερχόμενες συνδέσεις (συνδέσεις οι οποίες εκκινούν από το εσωτερικό δίκτυο) επιτρέπονται πάντα, εκτός από τις περιπτώσεις όπου έχει καθοριστεί μία συγκεκριμένη λίστα ελέγχου πρόσβασης (access control list).
- Όλες οι εισερχόμενες συνδέσεις (συνδέσεις οι οποίες εκκινούν από συστήματα του "έξω κόσμου") δεν επιτρέπονται, εκτός κι αν έχει δημιουργηθεί μία εξαίρεση. Πολλαπλές εξαιρέσεις μπορούν να διασυνδέονται με μία μετάφραση (xlate).

Εκτός από τις εξαιρέσεις, δεν επιτρέπεται η διέλευση πακέτων του ICMP (Internet Control Message Protocol) από το firewall.

Οποιαδήποτε απόπειρα παράκαμψης των κανόνων διακόπτεται άμεσα (δεν απορρίπτεται, επειδή αυτή η ενέργεια θα έστελνε στο σύστημα προέλευσης ένα μήνυμα κατάστασης μέσω του ICMP) επίσης, οι προσπάθειες παράκαμψης των κανόνων καταγράφονται.

Στο σημείο αυτό θα πρέπει να εξηγήσουμε τι είναι οι μεταφράσεις (xlates). Η Cisco χρησιμοποιεί τον όρο xlate για να αναφερθεί στην προώθηση πακέτων, επιτρέποντας σε εξωτερικά συστήματα να εκκινούν μία σύνδεση με ένα σύστημα τοποθετημένο σε μία αποστρατικοποιημένη ζώνη (DMZ) ή ακόμη και στο εσωτερικό δίκτυο (αν και είναι προτιμότερο όλοι οι προσπελάσιμοι από το Internet υπολογιστές να τοποθετούνται σε μία αποστρατικοποιημένη ζώνη του δικτύου). Ορίζετε μια μετάφραση xlate συσχετίζοντας μια "δημόσια" (κοινοποιημένη) διεύθυνση IP και θύρα με την διεύθυνση 1P και θύρα ενός υπολογιστή ο οποίος βρίσκεται στην αποστρατικοποιημένη

ζώνη του δικτύου σας (ή στο εσωτερικό σας δίκτυο). Αφού οριστεί μια μετάφραση xlate, οι εξαιρέσεις που αφορούν στην εισερχόμενη κυκλοφορία μπορούν να συσχετιστούν μ' αυτή την μετάφραση, πράγμα το οποίο επιτρέπει την αποστολή πολλαπλών μορφών κυκλοφορίας στους υπολογιστές που βρίσκονται στην αποστρατικοποιημένη ζώνη.[66]

Ο αλγόριθμος ASA είναι σχεδιασμένος ώστε να συνεργάζεται με το πρωτόκολλο TCP επειδή το TCP είναι το μοναδικό πρωτόκολλο που διατηρεί πληροφορίες κατάστασης, και η κατάσταση είναι η βάση της ανάλυσης που εκτελεί ο αλγόριθμος ASA. Τι γίνεται όμως με την κυκλοφορία του πρωτοκόλλου UDP ; Το *UDP* είναι ένα πρωτόκολλο το οποίο δεν διατηρεί πληροφορίες κατάστασης και χρησιμοποιείται ευρέως για την μετάδοση πολυμέσων με συνεχή ροή (streaming multimedia). Όταν ένα εξερχόμενο πακέτο του UDP διέρχεται από το PIX, αυτό αποθηκεύει πληροφορίες ψευδο-κατάστασης για το πακέτο (συμπεριλαμβανομένης της ώρας και της διεύθυνσης IP προορισμού). Όταν φτάνουν εισερχόμενα πακέτα του UDP στο PIX, αυτό επιχειρεί να ταιριάξει τις πληροφορίες "κατάστασης σύνδεσης" για να εξακριβώσει εάν τα πακέτα είναι έγκυρα. Ακόμη και μ' αυτή την δυνατότητα, το PIX υποστηρίζει μόνο το ON5 και έναν περιορισμένο αριθμό άλλων πρωτοκόλλων για την μετάδοση πολυμέσων.[67]

Πώς λειτουργεί ο αλγόριθμος A5A υπό το πρίσμα της συνολικής δραστηριότητας του firewall; Όταν το interface inside (ή οποιοδήποτε άλλο interface με επίπεδο ασφάλειας υψηλότερο από αυτό του outside) λαμβάνει ένα εξερχόμενο πακέτο, χρησιμοποιεί τον αλγόριθμο A5A για να επαληθεύσει την εγκυρότητα του. Κατόπιν το PIX ελέγχει εάν το πακέτο αυτό ανήκει σε μία προϋπάρχουσα σύνοδο επικοινωνίας. Εάν το πακέτο είναι έγκυρο αλλά δεν αποτελεί μέρος μιας υπάρχουσας συνόδου επικοινωνίας, το PIX δημιουργεί μία καταχώριση στον πίνακα καταστάσεων του (state table), στην οποία αποθηκεύει την εσωτερική διεύθυνση IP και την γενική (δημόσια) διεύθυνση IP που χρησιμοποιείτο NAT. Κατόπιν τροποποιείται η διεύθυνση IP προέλευσης του πακέτου έτσι ώστε να αντιστοιχεί στην γενική διεύθυνση IP, και το πακέτο στέλνεται στον προορισμό.[67]

Όταν ένα εισερχόμενο πακέτο φτάνει στο interface outside , ο αλγόριθμος ASA το συγκρίνει με τις πληροφορίες που έχουν αποθηκευτεί στον πίνακα καταστάσεων, καθώς και με οποιουσδήποτε άλλους περιορισμούς ισχύουν για την ασφάλεια. Εάν το πακέτο βρεθεί έγκυρο, το PIX διαγράφει την διεύθυνση IP προορισμού (την γενική διεύθυνση), τοποθετεί στην θέση της την πραγματική διεύθυνση IP του υπολογιστή στο εσωτερικό δίκτυο και κατόπιν στέλνει το πακέτο στο interface με το οποίο έγινε η αρχική σύνδεση.[67]

3.3 Μετάφραση Διευθύνσεων Δικτύου (Network Address Translation)

Η χρήση του NAT είναι ένας θαυμάσιος τρόπος για να προστατεύετε τις διευθύνσεις IP των υπολογιστών του εσωτερικού σας δικτύου από δημόσια κοινοποίηση. Συνήθως θα χρησιμοποιείτε το NAT για να καθορίσετε όχι μόνο μια σχέση "ένα-προς-ένα" μεταξύ των μεταφραζόμενων διευθύνσεων (πράγμα το οποίο σημαίνει ότι για κάθε διεύθυνση IP του εσωτερικού δικτύου υπάρχει μια εξίσου έγκυρη εξωτερική διεύθυνση IP), αλλά και την πιο κοινή μέθοδο μετάφρασης "ένα-προς-πολλά", στην οποία μία μεμονωμένη δημόσια διεύθυνση IP χρησιμοποιείται για όλες τις ιδιωτικές διευθύνσεις IP του εσωτερικού δικτύου. Αυτή η λειτουργικότητα "ένα-προς-πολλά" επιτυγχάνεται μέσω του PAT (Port Address Translation, μετάφραση διευθύνσεων θυρών), βάσει του οποίου χρησιμοποιούνται οι διάφορες θύρες της εξωτερικής διεύθυνσης IP για τον διαχωρισμό των διάφορων συνδέσεων που υλοποιούνται από υπολογιστές του εσωτερικού δικτύου. Εξ ορισμού, όλες αυτές οι μεταφράσεις έχουν δυναμική φύση· δηλαδή, εκτελούνται την στιγμή που δημιουργείται η σύνδεση.[68]

Μπορείτε επίσης να διαμορφώσετε το NAT για την δημιουργία στατικών μεταφράσεων. Οι στατικές μεταφράσεις δημιουργούν έναν μόνιμο συσχετισμό μεταξύ μιας εξωτερικής διεύθυνσης IP και μιας μεμονωμένης, εσωτερικής διεύθυνσης IP. Αυτός ο τύπος μετάφρασης αποτελεί την βάση για τις μεταφράσεις xlate και επιτρέπει στους servers που βρίσκονται στην αποστρατικοποιημένη ζώνη ή στο εσωτερικό δίκτυο να απαντούν στις συνδέσεις που προέρχονται από ένα εξωτερικό δίκτυο.[69]

3.4 Έλεγχος πρόσβασης (Access control)

Το PIX μπορεί να επιβάλλει βασιζόμενη στον εκάστοτε χρήστη πιστοποίηση και εξουσιοδότηση, με δύο τρόπους[69]:

- **Authentication, Acounting, Authorization (AAA).** Δίνει στο PIX την δυνατότητα να χρησιμοποιεί έναν TACACS+ server (Terminal Access Controller Access Control System) ή έναν RADIUS server (Remote Authentication Dial-In User Service) για την πιστοποίηση των λογαριασμών των χρηστών. Αφού ο server επαληθεύσει την ταυτότητα του χρήστη (και, προαιρετικά, οποιωνδήποτε ομάδων στις οποίες ανήκει ο λογαριασμός), το PIX συγκρίνει τον χρήστη (ή την ομάδα) έναντι μιας λίστας ελέγχου πρόσβασης (Access Control List, ACL).

- **Λίστες πρόσβασης.** Ελέγχουν συνδέσεις και τύπους συνδέσεων. Μία λίστα πρόσβασης περιορίζει τις συνδέσεις βασιζόμενη σε τρία χαρακτηριστικά: διεύθυνση IP προέλευσης, διεύθυνση IP προορισμού και/ή θύρα. Οι πιο περιοριστικές λίστες πρόσβασης βασίζονται και στα τρία προαναφερθέντα χαρακτηριστικά.

Σαν αποτέλεσμα του AAA και των λιστών πρόσβασης, το PIX μπορεί να υποστηρίζει έναν τύπο ενδιάμεσου server (proxy) ο οποίος αναφέρεται σαν cut-through proxy (διακομιστής με συντομευμένη διαδικασία μεσολάβησης). Ενώ οι περισσότεροι proxy servers αναλύουν ολόκληρο τον σωρό πρωτοκόλλων (protocol stack) κάθε πακέτου, ένας cut-though proxy server πιστοποιεί απλώς τον χρήστη που ζητά την σύνδεση και χρησιμοποιεί τις πληροφορίες κατάστασης αυτής της σύνδεσης για να διατηρήσει μία απευθείας σύνδεση μεταξύ των δύο επικοινωνούντων μερών.[69]

Οι cut-through proxy servers δίνουν επίσης στον επόπτη του δικτύου την δυνατότητα να εφαρμόζει συγκεκριμένες για τον εκάστοτε χρήστη λίστες ελέγχου πρόσβασης σε εξερχόμενες (και εισερχόμενες) συνόδους επικοινωνίας. Ο χρήστης εισάγει τον κωδικό πρόσβασης του σαν μέρος μιας συνόδου επικοινωνίας μέσω HTTP, FTP, ή ακόμη και Telnet. Κατόπιν το PIX επαληθεύει την ταυτότητα του χρήστη, συγκρίνει τις πληροφορίες πιστοποίησης του με την κατάλληλη λίστα ελέγχου πρόσβασης και υλοποιεί την συνοδό επικοινωνίας.[70]

3.5 Προστασία από επιθέσεις

Αν και μπορείτε να ενεργοποιήσετε πολλές γενικευμένες ρυθμίσεις σ' ένα firewall το PIX περιλαμβάνει τις ακόλουθες τεχνολογίες οι οποίες είναι ειδικά σχεδιασμένες ώστε να προστατεύουν το δίκτυο σας από συγκεκριμένους τύπους επιθέσεων[71]:

- **Unicast RPF (Reverse Path Forwarding).** Αυτή η απλή λειτουργία συγκρίνει τις διευθύνσεις IP των εισερχόμενων πακέτων για να διασφαλίσει ότι έχουν νόημα για το δίκτυο σας. Αναλύει επίσης τα εξερχόμενα πακέτα και τα συγκρίνει με τονπίνακα δρομολόγησης για να διασφαλίσει ότι υπάρχει μία διαδρομή προς το δίκτυο προορισμού. Αν και η λειτουργία αυτή είναι καλή, δεν είναι τέλεια. Εάν ένα εισερχόμενο πακέτο δεν ταιριάζει με καμία από τις γνωστές διαδρομές, είναι αδύνατο να καθοριστεί η εγκυρότητα του.

- **Flood Guard.** Ενεργοποιημένη εξαρχής, η λειτουργία Flood Guard θέτει όρια όσον αφορά στο πλήθος και στην συχνότητα των προσπαθειών σύνδεσης που παρουσιάζονται από το AAA. Εάν δεν υπήρχαν αυτά τα όρια, θα ήταν δυνατή η έναρξη μιας επίθεσης άρνησης εξυπηρέτησης (DoS) εναντίον του PIX, με την μορφή επαναλαμβανόμενων προσπαθειών υλοποίησης μιας πιστοποιημένης συνόδου επικοινωνίας οι οποίες αγνοούν τις επόμενες προτροπές σύνδεσης· αυτή η κατάσταση υποχρεώνει το AAA να καταναλώνει πόρους κατά την διάρκεια που περιμένει απαντήσεις γι' αυτές τις προτροπές σύνδεσης, οι οποίες όμως δεν έρχονται ποτέ.
- **Flood Defender.** Η λειτουργία αυτή προστατεύει τα συστήματα του εσωτερικούδικτύου που έχουν στατική καταχώριση στο NAT (ή μετάφραση xlate) από επιθέσεις κατακλυσμού σημάτων SYN (SYN Floods). Μία επίθεση SYN flood παράγει όσο το δυνατόν περισσότερες αιτήσεις σύνδεσης μέσω TCP στην προσπάθεια της να καταναλώσει όλους τους πόρους του υπολογιστή-στόχου, καθώς αυτός περιμένει να ολοκληρωθεί η διαδικασία "χαιρετισμού" (handshake) του TCP. Η λειτουργία Flood Defender εντοπίζει τις επιθέσεις SYN flood και ανταποκρίνεται στις αιτήσεις σύνδεσης TCP εκ μέρους του υπολογιστή-στόχου μέχρι να σταματήσει η επίθεση.
- **FragGuard.** Συγκεκριμένες επιθέσεις (όπως η teardrop.c) δημιουργούν κομμάτια (fragments) πακέτων τα οποία επικαλύπτονται και μετατίθενται σε διαφορετικές θέσεις. Αυτά τα προβληματικά κομμάτια πακέτων μπορούν να προκαλέσουν την κατάρρευση ενός συστήματος, ή απλώς να παρακάμψουν τις σχετιζόμενες με τα πακέτα διαδικασίες ασφάλειας. Η λειτουργία FragGuard συναρμολογεί στην ολότητα τους τα μήνυμα σφάλματος του ICMP πριν τα στείλει στα συστήματα του εσωτερικού δικτύου, εξαλείφοντας αυτή την αδυναμία.
- **DNS Control.** Ενεργοποιημένη εξαρχής, η λειτουργία DNS Control επιτρέπει την αποστολή μόνο μιας απάντησης από τον DNS server όταν στέλνεται μία αίτηση DNS από ένα client σύστημα, ανεξάρτητα από τον αριθμό των servers που έχουν απαντήσει πραγματικά.
- **ActiveX Blocking.** Όταν η *Microsoft* ενσωμάτωσε την τεχνολογία ActiveX στα λειτουργικά της interfaces, δεν έθεσε αυστηρά όρια στον ίδιο τον κώδικα (ανόμοια με την^3V3, η οποία διαθέτει ένα "sandbox" - ή, ακριβέστερα, εγγενείς περιορισμούς σχετικά με το τι μπορεί να γίνει στο client σύστημα). Το PIX "αδρανοποιεί" (μετατρέποντας σε σχόλια) όλα τα tags <object> που περιέχονται στον HTML κώδικα των ιστοσελίδων που φιλτράρει, πράγμα το οποίο ουσιαστικά

αδρανοποιεί τους μηχανισμούς ActiveX απ' όλες τις ιστοσελίδες που εξετάζει ο χρήστης.

- ***Java* Filtering.** Αν και η *Java* διαθέτει μηχανισμούς προστασίας έναντι συγκεκριμένων μεθόδων απευθείας τροποποίησης των αρχείων, συνεχίζει να είναι πιθανή η έναρξη επιθέσεων σε ένα εσωτερικό δίκτυο μέσω μικροεφαρμογών Java (Java applets). Το PIX απενεργοποιεί την δυνατότητα ανάκτησης και εκτέλεσης μικροεφαρμογών Java, μετατρέποντας σε σχόλια τις σχετικές αναφορές που συναντά σε μία ιστοσελίδα. Αν και οι μικροεφαρμογές Java δεν αποτελούν τόσο σημαντική απειλή για τους υπολογιστές όσο τα συστατικά ActiveX, μπορούν να χρησιμοποιηθούν σαν μία μέθοδος ανακάλυψης στοιχείων για έναν υπολογιστή ή ένα δίκτυο.
- **URL Filtering.** Όταν το PIX χρησιμοποιείται με το λογισμικό Websense της NetPartners, μπορεί να πιστοποιεί ότι οι διευθύνσεις URL που ζητούνται από έναν υπολογιστή του εσωτερικού δικτύου είναι επιτρεπτές σύμφωνα με την πολιτική που έχει καθοριστεί στον Websense server.

Αν και οι προαναφερθείσες λειτουργίες ασφάλειας παρέχουν προστασία έναντι συγκεκριμένων μορφών επιθέσεων, το PIX υποστηρίζει επιπλέον τις ακόλουθες δυνατότητες για το ασφαλές φιλτράρισμα συγκεκριμένων εφαρμογών και πρωτοκόλλων[73]:

- **RIPv2 :** Το PIX μπορεί να υποστηρίζει τις μεθόδους πιστοποίησης *MD5* του πρωτοκόλλου RIPv2 (συμπεριλαμβανομένου ενός κλειδιού ανά interface).
- **Configurable Proxy Pinging :** Μπορείτε να προστατέψετε το PIX από επιθέσεις μέσω του ping (οι οποίες χρησιμοποιούνται για την βολιδοσκόπηση υπολογιστών ή δικτύων) χρησιμοποιώντας αυτή την λειτουργία, η οποία ουσιαστικά ορίζει πώς θα ανταποκρίνεται το PIX στην κυκλοφορία του ICMP(το πρωτόκολλο που χρησιμοποιεί η εντολή ping). Ωστόσο, εάν θέλετε να επιτρέπεται η διέλευση κυκλοφορίας VPN (πρωτόκολλα IPsec ή PPTP από το PIX, θα πρέπει να ενεργοποιήσετε το ICMP type 3.
- **Mail *Guard* :** Η λειτουργία Mail Guard επιτρέπει μόνο έναν ελάχιστο αριθμό εντολών του SMTP και καταγράφει όλες τις συνδέσεις μέσω SMTP.

- **Πρωτόκολλα για πολυμέσα και τηλεφωνία.** Το PIX υποστηρίζει τα ακόλουθα πρωτόκολλα:
    1. RealAudio
    2. Streamworks
    3. CU-SeeMe
    4. Internet Phone
    5. IRC (Internet Relay Chat)
    6. Vxtreme
    7. VDO Live
    8. H.323
    9. SIP (Session Initiation Protocol)

- **NetBios πάνω από το IP.** Η δυνατότητα αυτή είναι απαραίτητη εάν έχουμε σταθμούς εργασίας με παλαιότερες εκδόσεις λειτουργικών συστημάτων Windows της Microsoft, οι οποίοι χρειάζονται πρόσβαση μέσω SMB (Server Message Block) σε servers ενός εξωτερικού δικτύου.

ΚΕΦΑΛΑΙΟ 4^{Ο} : Το FireWall-1 της Check Point

Στο κεφάλαιο αυτό γίνεται αναφορά στο Firewall –1 της Check Point όπου αναλύονται οι λειτουργίες του.

4.1 Εισαγωγή στο FireWall-1

Το FireWall-1 είναι ένα βασικό συστατικό της αρχιτεκτονικής SVN (Secure Virtual Network) και επιτρέπει την ασφάλεια δικτύων να ρυθμιστεί με μια ενιαία ευρεία επιχειρηματική πολιτική.[74]

Σαν πιο αποδεδειγμένη λύση ασφάλειας της βιομηχανίας, το FireWall-1 δίνει περισσότερο από έναν απλό έλεγχο πρόσβασης που ορίζει την κυκλοφορία διαχείρισης σε ένα προστατευμένο δίκτυο. Το FireWall-1 της Check Point είναι μια περιεκτική πλατφόρμα ασφάλειας που ενσωματώνει και διαχειρίζεται όλα τα στοιχεία επιχειρηματικής ασφάλειας, η οποία περιλαμβάνει[74]:

1) Έλεγχο πρόσβασης (Access Control)
2) Πιστοποίηση χρήστη (User Authentication)
3) Μετάφραση διευθύνσεων δικτύου (NAT)
4) Εικονική ιδιωτική δικτύωση (VPN)
5) Ικανοποιητική ασφάλεια (anti-virus, URL και Java/ActiveX screening)
6) LDAP - βασισμένη στη διαχείριση χρήστη
7) Ανίχνευση εισβολής
8) Ανίχνευση κακόβουλης δραστηριότητας

4.2 Έλεγχος πρόσβασης

Ο έλεγχος του FireWall-1 της Check Point υποστηρίζει περισσότερες από 150 προκαθορισμένες εφαρμογές, υπηρεσίες και πρωτόκολλα εκτός του πλαισίου. Η υποστήριξη παρέχεται για όλες τις δημοφιλείς υπηρεσίες διαδικτύου, περιλαμβάνοντας τις πιο κοινά χρησιμοποιούμενες εφαρμογές (HTTP, SMTP, Telnet, FTP, κ.λ.π.), ολόκληρης της οικογένειας TCP εφαρμογών και μη συνδεδεμένων πρωτοκόλλων όπως το UDP.

Επιπλέον, το FireWall-1 υποστηρίζει σημαντικές επιχειρησιακές εφαρμογές όπως η Oracle SQL, εφαρμογές πολυμέσων όπως το RealAudio και οι υπηρεσίες βασισμένες σε H.323 όπως η Voice over IP (VoIP).

Το FireWall-1 της Check Point βασίζεται πάνω σε επιθεώρηση βάση κατάστασης (Stateful Inspection), το ουσιαστικό πρότυπο για τα firewalls του διαδικτύου

κατασκευάστηκε από την Check Point. Η επιθεώρηση βάση κατάστασης παρέχει το υψηλότερο δυνατό επίπεδο ασφάλειας ενσωματώνοντας επικοινωνία - και την προερχόμενη δήλωση της εφαρμογής και το περιβάλλον της πληροφορίας η οποία είναι αποθηκευμένη και ενημερωμένη δυναμικά. Αυτό παρέχει τα συσσωρευτικά δεδομένα ενάντια στα οποία οι επόμενες προσπάθειες επικοινωνίας μπορούν να αποτιμηθούν. Η επιθεώρηση βάση κατάστασης παρέχει πλήρη ενημερότητα επιπέδου εφαρμογής χωρίς να απαιτείται ένας ξεχωριστός proxy για κάθε υπηρεσία. Αυτό οδηγεί σε βελτιωμένη απόδοση, προσαρμοστικότητα και τη δυνατότητα να υποστηρίξει νέες και συνηθισμένες εφαρμογές γρήγορα. Αυτοί είναι μόνο μερικοί από τους λόγους για του οποίους η επιθεώρηση βάση κατάστασης έχει υιοθετηθεί από τους πελάτες ως η επιλογή της τεχνολογίας firewall.

4.3 Πιστοποίηση χρήστη

Τα σημερινά επιχειρηματικά δίκτυα περιλαμβάνουν όχι μόνο τους τοπικούς εταιρικούς χρήστες, αλλά και τις απομακρυσμένες θέσεις, φορητοί εργαζόμενοι και εργαζόμενοι εξ αποστάσεως. Πριν να παραχωρήσει την πρόσβαση σε ένα δίκτυο ευαίσθητων πόρων, οι οργανισμοί χρειάζονται ένα τρόπο επιβεβαίωσης της αυθεντικότητας του χρήστη.

Το FireWall-1 της Check Point καλύπτει αυτή την απαίτηση με την ολοκληρωμένη υποστήριξη των τριών ισχυρών μεθόδων πιστοποίησης και των πολλαπλών σχεδίων πιστοποίησης, περισσότερο από οποιονδήποτε άλλο πωλητή ασφάλειας. Οι χρήστες μπορούν να είναι πιστοποιημένοι χωρίς οποιαδήποτε τροποποίηση στον διακομιστή ή σε εφαρμογές πελάτη. Και αντίθετα με πολλά προϊόντα ασφάλειας δικτύου, το FireWall-1 μπορεί να πιστοποιήσει χρήστες οποιασδήποτε εφαρμογής βασισμένη σε IP.

Η ανοικτή αρχιτεκτονική του FireWall-1 επιτρέπει πολυάριθμες λύσεις πιστοποίησης να ολοκληρωθούν μέσα σε μία ευρέως επιχειρηματική πολιτική ασφάλειας, περιλαμβάνοντας κωδικούς πρόσβασης του FireWall-1, έξυπνες κάρτες, προϊόντα βασισμένα σε σκυτάλη όπως το SecureID, L-DAP αποθηκευμένους κωδικούς πρόσβασης, RADIUS ή TACACS+ διακομιστές πιστοποίησης, X.509 ψηφιακά πιστοποιητικά και ακόμα και βιομετρικές τεχνικές. Επιπλέον, η Check Point παρέχει μία ανοικτή διασύνδεση προγραμματισμού εφαρμογών (application programming interface, API) ως τμήμα του OPSEC (Open Platform for Security) που επιτρέπει στους πωλητές ασφάλειας τρίτων να αναπτύξουν συμβατά προϊόντα πιστοποίησης.

4.4 Μετάφραση διευθύνσεων δικτύου (NAT)

Το χαρακτηριστικό γνώρισμα της μετάφρασης διευθύνσεων δικτύου του FireWall-1 είναι ότι κρύβει τις διευθύνσεις του εσωτερικού δικτύου από το διαδίκτυο, αποφεύγοντας την αποκάλυψη τους ως δημόσιες πληροφορίες. Εκτός από την ενίσχυση της επιχειρηματικής ασφάλειας, η μετάφραση διευθύνσεων δικτύου επιτρέπει στους οργανισμούς να διατηρήσουν τα μη καταχωρημένα IP σχέδια διευθυνσιοδότησης και να παρέχουν πρόσβαση στο διαδίκτυο σε όλους τους χρήστες που χρησιμοποιούν μια ενιαία εταιρική διεύθυνση IP. Η δυνατότητα της προηγμένης μετάφρασης διεύθυνσης του FireWall-1 υποστηρίζει όλες τις υπηρεσίες του διαδικτύου.

4.5 Εικονική ιδιωτική δικτύωση (VPN)

Παρέχοντας την πλήρη ολοκλήρωση της εικονικής ιδιωτικής δικτύωσης και την ασφάλεια του firewall, το VPN-1 της Check Point δίνει μία ασφαλή και ευέλικτη αρχιτεκτονική για μία πλήρη επέκταση του VPN ευρέως επιχειρησιακά.

- **Remote Access VPN** : Οι κινητοί και απομακρυσμένοι χρήστες μπορούν να έχουν πρόσβαση στις εταιρικές πληροφορίες του δικτύου μέσω του διαδικτύου χρησιμοποιώντας το VPN-1 SecureClient και το VPN-1 SecuRemote™ λογισμικό πελάτη.
- **Site-to-Site VPN :** Η VPN-1 πύλη μπορεί να προστατεύσει τις επιχειρησιακές επικοινωνίες που ταξιδεύουν μεταξύ εταιρικών θέσεων μέσω του διαδικτύου ή οποιουδήποτε μη εμπιστοσύνης IP δίκτυο.
- **Extranet VPN :** Οι επιχειρησιακοί συνεργάτες μπορούν ακίνδυνα να συνδεθούν με το δίκτυο επιχείρησης για να τρέξουν τις εφαρμογές ηλεκτρονικού εμπορίου.
- **Client/Server VPN :** Οι τοπικοί υπολογιστές γραφείου μπορούν να καθιερώσουν τις διόδους VPN με οποιαδήποτε εφαρμογή διακομιστή για να προστατευτούν εναντίον των απειλών εσωτερικού δικτύου.

Η ολοκλήρωση της ασφάλειας δικτύων και η δυνατότητα της VPN να εξαλείψει την ανάγκη να ανοιχτούν πολλαπλές θύρες, ή "τρύπες", στο firewall να περάσει τυφλά την VPN κυκλοφορία όπως είναι απαραίτητο με πολλές αυτόνομες VPN συσκευές. Αντ' αυτού, όλοι οι έλεγχοι που καθορίζονται από την πολιτική ασφάλειας του FireWall-1 εφαρμόζονται για την εγγύηση της κυκλοφορίας του VPN και για την πλήρη ακεραιότητα της ασφάλειας του δικτύου.

4.6 Ικανοποιητική ασφάλεια

Το FireWall-1 της Check Point προστατεύει τους χρήστες από επιθέσεις ιών, κακόβουλες Java και ActiveX μικροεφαρμογές και το ανεπιθύμητο περιεχόμενο του ιστού μέσω των ολοκληρωμένων δυνατοτήτων περιεχομένου ασφάλειας του.

4.6.1 Ολοκληρωμένοι διακομιστές ασφάλειας

Για κάθε σύνδεση που εγκαθιστάτε μέσω ενός FireWall-1 HTTP, ενός SMTP ή ενός FTP διακομιστή ασφάλειας, ο διαχειριστής δικτύου ελέγχει την πρόσβαση στους συγκεκριμένους πόρους με έναν υψηλό βαθμό κοκκοποίησης. Για παράδειγμα, η πρόσβαση μπορεί να ελεγχθεί σε συγκεκριμένες ιστοσελίδες και ενέργειες, σε FTP αρχεία και διαδικασίες (π.χ PUT/GET εντολές), σε συγκεκριμένα SMPT πεδία επικεφαλίδας και αλλού.

4.6.2 Υποστήριξη εφαρμογής τρίτων

Μέσω της υποστήριξης του για το OPSEC πλαίσιο, το FireWall-1 της Check Point μπορεί να ισχυροποιήσει διάφορα ανοικτά APIs να διασυνδεθούν με το περιεχόμενο ασφάλειας εφαρμογών τρίτων. Αυτό επιτρέπει στους διαχειριστές ασφάλειας να επεκτείνουν την ασφάλεια της δικής τους FireWall-1 εγκατάστασης για να παρέχουν προηγμένη λειτουργικότητα, όπως :

- **Anti-virus screening** για να προστατεύει τους πόρους του εσωτερικού δικτύου από ιούς που μπορεί να έχουν περιληφθεί μέσα στην εισερχόμενη κυκλοφορία. Η ανίχνευση ιών επιτρέπεται χρησιμοποιώντας το Content Vectoring Protocol (CVP).
- **Φιλτράρισμα URL** για να εμποδίσει τα εξερχόμενα αιτήματα ιστού για το ακατάλληλο ή μη παραγωγικό περιεχόμενο Ιστού χρησιμοποιώντας το πρωτόκολλο φιλτραρίσματος του URL (UFP).

4.7 LDAP - βασισμένη στη διαχείριση χρήστη

Η ενότητα διαχείρισης λογαριασμού επιτρέπει στο FireWall-1 να ρωτήσει το LDAP προσαρμόσιμο κατάλογο διακομιστών για ασφάλεια πληροφοριών σε επίπεδο χρήστη που χρησιμοποιούνται για να ενισχύσουν τα στοιχεία της επιχειρηματικής πολιτικής ασφάλειας, όπως η πιστοποίηση χρήστη, τα προνόμια κρυπτογράφησης δεδομένων και ελέγχου πρόσβασης.

4.8 Ανίχνευση εισβολής

Το RealSecure της Check Point είναι ένα σύστημα πραγματικού χρόνου αναγνώρισης και ανταπόκρισης, παρέχοντας μη αντιδραστική προστασία δικτύου από επιθέσεις ή κακή χρήση. Αναγνωρίζει περισσότερους από 300 τύπους επιθέσεων και ανταποκρίνεται αυτόματα αναδιευθετώντας το FireWall-1 να τερματίσει τις συνδέσεις και να προστατεύσει ενάντια σε μελλοντικές επιθέσεις.

4.9 Ανίχνευση κακόβουλης δραστηριότητας

Το FireWall-1 μπορεί να ανιχνεύσει την κακόβουλη δραστηριότητα στην πύλη του διαδικτύου και να προειδοποιήσει τον διαχειριστή ασφαλείας για τις αποπειραθείσες παραβιάσεις της πολιτικής ασφάλειας δικτύου. Η λειτουργικότητα της κακόβουλης ανίχνευσης δραστηριότητας του FireWall-1 αναλύει την καταγραφή εγγραφών του FireWall-1 για να ανιχνεύσει ένα ατίθασο γνωστό δίκτυο επιθέσεων και ενδείξεων ύποπτης δραστηριότητας.

ΚΕΦΑΛΑΙΟ 5^{Ο} : Το Armor2net firewall

Στο κεφάλαιο αυτό αναφέρεται στο Armor2net firewall όπου αναλύονται οι λειτουργίες του.

5.1 Εισαγωγή στο Armor2net firewall

Το Armor2net είναι μία εναλλακτική πρόταση firewall κύρια χαρακτηριστικά του οποίου είναι η ευκολία χρήσης, το πρακτικό interface και βέβαια οι πρόσθετες δυνατότητες αφαίρεσης των λεγόμενων “κατασκοπευτικών” στοιχείων, που συνοδεύουν τις επισκέψεις μας στο Internet. Η κυρίως λειτουργία του προγράμματος στοχεύει στο να επιτρέψει μόνο στις εφαρμογές που γνωρίζει ο χρήστης να χρησιμοποιούν τη σύνδεση στο Internet. Το πρόγραμμα με άλλα λόγια, εμφανίζει τη λίστα με τις παρούσες συνδέσεις μέσα από ένα κατανοητό περιβάλλον χρήσης, επιτρέποντας στο χρήση να αποσυνδέσει μία από αυτές (τις εφαρμογές). Ανάμεσα στα χαρακτηριστικά που ενσωματώνει το εν λόγω firewall, είναι και η επιλογή stealth, με την οποία μπλοκάρεται κάθε πρόσβαση στο σύστημα του χρήστη. Ωστόσο, η συγκεκριμένη δυνατότητα είναι ανενεργή σε συστήματα που ανήκουν σε δίκτυο. Μέσω επίσης του pop up killer, το πρόγραμμα σκανάρει το λειτουργικό για τυχόν ύπαρξη adware/spyware προγραμμάτων, και τα απομακρύνει. Στην ουσία πρόκειται για μία καλή εφαρμογή ασφαλείας, για όσους δεν αποζητούν υψηλές παραμέτρους προστασίας του συστήματος, με χαμηλό κόστος, που το καθιστά προσιτό οικονομικά για τους περισσότερους χρήστες. [75]

5.2 Έλεγχος της κατάστασης σύνδεσης

Το Armor2net στο section net state σάς δείχνει τις ενεργές συνδέσεις καθώς και τις παραμέτρους που τις συνοδεύουν (remote address/port, local application/port, protocol και status). Μπορείτε να τερματίσετε τις συνδέσεις αυτές (επιλέγοντας shut) στην περίπτωση που τις θεωρείτε επικίνδυνες για το σύστημα. Επιπλέον υπάρχει το traffic indicator, που δείχνει με κόκκινο το εξερχόμενο και με πράσινο το εισερχόμενο traffic. Στο ίδιο επίσης tab, μπορείτε να δείτε εκτενείς πληροφορίες των προγραμμάτων που τρέχουν. Κάνοντας δεξί κλικ στο local application port, βλέπετε στοιχεία όπως την έκδοση της εφαρμογής, το μέγεθος του αρχείου, ημερομηνία δημιουργίας κ.λπ. Θα σας συμβουλεύαμε επίσης, να αξιοποιήσετε και τα μηνύματα των tips που εμφανίζει το πρόγραμμα, κατά την ενεργοποίησή του.[75]

5.3 Σημασία των application alerts

Το πρόγραμμα εμφανίζει διαφορετικού είδους application alerts, κάθε φορά που εντοπίζει επικίνδυνη εισαγωγή δεδομένων στο σύστημά σας. Ένα νέο application alert, εμφανίζεται συγκεκριμένα στις περιπτώσεις που: ένα πρόγραμμα του υπολογιστή σας συνδέεται στο Internet (π.χ. filesharing tool, mailclient κ.λπ.) ή το αντίστροφο, ή όταν ένα πρόγραμμα επιτρέπει σε κάποιο ανοιχτό port (θύρα επικοινωνίας) να δεχθεί αίτημα σύνδεσης στο Internet, χωρίς όμως να έχει οριστεί σε αυτό το permission από το χρήστη. Το εν λόγω μήνυμα εμφανίζεται συχνά, ιδιαίτερα κατά την αρχική χρήση του προγράμματος, όταν δεν έχουν οριστεί οι παράμετροι μπλοκαρίσματος. Άλλοι τύπου μηνύματος, είναι το blocked banned site alert (το πρόγραμμα μπλοκάρει τη σύνδεση στο συγκεκριμένο site που είναι στη banned sites list), το stopped popup window alert (σταματάει την εμφάνιση των pop up windows κατά την επίσκεψη σε sites) κ.λπ.[75]

5.4 Καθορίστε τα permissions εφαρμογών

Ενα από τα σημαντικότερα χαρακτηριστικά του προγράμματος Armor2net, είναι το program filter. Μέσω αυτού, μπορείτε να ορίσετε ποια προγράμματα θα έχουν πρόσβαση στο Internet ή θα δέχονται μία σύνδεση από το Internet, που κανονικά δεν θα έπρεπε. Εμφανίζει λοιπόν το πρόγραμμα μία λίστα με τις εφαρμογές που “επιχείρησαν” να συνδεθούν στο Internet, συμπεριλαμβανομένων και αυτών στις οποίες επιτρέψατε ή απορρίψατε την πρόσβαση στο δίκτυο. Στη λίστα λοιπόν αυτή μπορείτε να επιτρέψετε ή να απαγορέψετε την πρόσβαση, αλλάζοντας τα permissions (άδειες). Επιλέγοντας pass, επιτρέπετε στο πρόγραμμα να συνδεθεί στο δίκτυο. Επιλέγοντας block εμποδίζετε το πρόγραμμα να συνδεθεί στο Web.[75]

5.5 Μπλοκάρετε τα επικίνδυνα sites

Ενα από τα αρνητικά στοιχεία (λιγότερο επικίνδυνα ίσως) του Internet, είναι ότι τα sites δεν συνοδεύονται πάντα από “κατάλληλο” περιεχόμενο. Μπορείτε λοιπόν μέσω του προγράμματος, να φιλτράρετε τις κατηγορίες των sites που θεωρείτε “κακές”, μπλοκάροντας την πρόσβασή τους σε αυτά. Υποστηρίζονται δύο τρόποι εισαγωγής κάποιου site στη λίστα μπλοκαρίσματος: 1. Κάντε κλικ στο “I want ...” bar και μέσα από το μενού, ενεργοποιήστε την επιλογή block some sites. Κάντε κλικ στο add και στο παράθυρο που θα εμφανιστεί πληκτρολογήστε το URL ή την IP του site που θέλετε να μπλοκάρετε. 2. Μεταβείτε στο tab net state. Εντοπίστε το site του οποίου την πρόσβαση θέλετε να μπλοκάρετε και κάντε κλικ στην πρώτη στήλη της σειράς που εντοπίζετε. Θα

εμφανιστεί ένα popup menu, από όπου θα επιλέξετε “add to banned sites list”. Το site θα μεταφερθεί στην banned sites list.[75]

5.6 Εντοπισμός των spyware

Το personal firewall Armor2net υποστηρίζει δύο τρόπους εντοπισμού των στοιχείων spyware στο λειτουργικό σας. Ο ένας είναι ότι εντοπίζει αυτόματα τα spyware σε ένα διάστημα 7 ημερών, το οποίο καθορίζεται από το χρήστη. Ο δεύτερος είναι ότι μπορείτε να το κάνετε χειροκίνητα (manually) οποιαδήποτε στιγμή το θελήσετε. Σημειώνεται ότι στην περίπτωση που επιλέξετε τον αυτόματο έλεγχο των spyware, όταν αυτά εντοπιστούν, εμφανίζεται το σχετικό παράθυρο διαλόγου (“remove spywares”) και επιλέγετε ποια από αυτά θα απομακρύνετε. Εάν θέλετε να το κάνετε χειροκίνητα, κάντε κλικ στο εικονίδιο “clean spywares” στην toolbar ή δεξί κλικ στο δεξί κάτω μέρος (στη γραμμή κατάστασης) και ενεργοποιήστε την επιλογή clean spywares”. Ενεργοποιείται το “scanning spywares” window και το πρόγραμμα σκανάρει το σύστημά σας για αυτού του είδους το υλικό.[75]

5.7 Εξαιρέσεις σε spyware/adware

Εάν δεν θέλετε να καταργήστε κάποια spyware, τα οποία ουσιαστικά δεν ανήκουν σε αυτήν την κατηγορία, αλλά τα firewalls τις περισσότερες φορές τα αναγνωρίζουν ως “κατασκοπευτικά” στοιχεία, μπορείτε να τα μεταφέρετε στο section “exceptions”, κάνοντας κλικ στην επιλογή “I want ...” bar και επιλέγοντας “Define the exceptions on cleaning spywares”. Το “define exceptions” υποστηρίζει δύο λίστες: στην αριστερή λίστα, το “all spywares” εμφανίζει όλα τα γνωστά spyware items. Στη δεξιά, το “exceptions” εμφανίζει αυτά που έχετε εξαιρέσει και που δεν θέλετε να μπλοκάρονται από το πρόγραμμα. Σημειώνεται, ότι κάνοντας κλικ στο add, μεταφέρετε τα spyware items από την αριστερή στήλη στη δεξιά.[75]

5.8 Ορίστε τα security options

Όπως ισχύει σε κάθε πρόγραμμα τύπου firewall, έτσι και το Armor2net, σας επιτρέπει να ορίσετε τις δικές σας παραμέτρους ως προς τον τρόπο ελέγχου των στοιχείων spyware. Από το κεντρικό παράθυρο, κάντε κλικ στο “I want ...” bar για να ανοίξει το dynamic menu με τις επιλογές. Ορίστε τον αριθμό των ημερών για να καθορίσετε την αυτόματη περίοδο εντοπισμού των spyware items στο σύστημά σας (η default ρύθμιση είναι 7 ημέρες). Ορίστε επίσης τον αριθμό των ημερών για τη διατήρηση

αρχείου backup των spyware, ώστε να μπορείτε εάν θέλετε να τα επαναφέρετε κάποια στιγμή. Το προκαθορισμένο όριο από το πρόγραμμα, είναι 20 μέρες.[75]

5.9 Ενεργοποίηση της επιλογής stealth

Άλλη μία χρήσιμη δυνατότητα που ενσωματώνει το πρόγραμμα Armor2net, είναι η επιλογή stealth. Μέσω αυτής, εμποδίζετε τους hackers να εντοπίσουν το σύστημά σας στο Internet και κατά συνέπεια να έχουν πρόσβαση σε αυτό. Πρόκειται γενικότερα για ένα αρκετά αποτελεσματικό στοιχείο προστασίας, το οποίο ενσωματώνουν στην πλειοψηφία τους τα περισσότερα firewalls - σε κάποια μάλιστα δίνεται η δυνατότητα περαιτέρω παραμετροποίησης αυτής της δυνατότητας. Κάντε λοιπόν κλικ στο ομώνυμο εικονίδιο στο πάνω μέρος του παραθύρου για να ενεργοποιήσετε τη σχετική δυνατότητα. Κάνοντας ξανά κλικ την απενεργοποιείτε. Τέλος, στην περίπτωση που θέλετε να δείτε τις ενέργειες που έχει σημειώσει το πρόγραμμα στο σύστημά σας, μπορείτε να επιλέξετε το logs tab.[75]

ΚΕΦΑΛΑΙΟ 6^{Ο} : Το ZoneAlarm Pro 4 firewall

Στο κεφάλαιο αυτό αναφέρονται οι λειτουργίες του ZoneAlarm Pro 4 firewall και τα χαρακτηριστικά του.

6.1 Εισαγωγή στο ZoneAlarm Pro 4 firewall

Η νέα έκδοση 4 της εφαρμογής προστασίας Zone Alarm Pro της εταιρείας Zonelabs, συγκεντρώνει αρκετές δυνατότητες ασφαλείας, στις οποίες έχουν προστεθεί καινούργιες ενώ έχουν γίνει και σημαντικές βελτιώσεις στις ήδη υπάρχουσες. Το πρόγραμμα σε γενικές γραμμές παρέχει προστασία στο σύστημα του χρήστη, κατά τη διάρκεια σύνδεσης στο Internet, κατά το άνοιγμα των e-mails, κατά τη χρήση εφαρμογών, κλπ. Εχει σχεδιαστεί με άλλα λόγια, ώστε να μπλοκάρει και να αναφέρει τις προσπάθειες πρόσβασης, να βάζει σε καραντίνα τους ιούς καθώς και να φιλτράρει την εμφάνιση των Internet cookies στο σύστημα. Δύο απο τα νέα χατακτηριστικά που έχουν προστεθεί στο πρόγραμμα ZoneAlarm Pro 4, είναι το myVAULT και το ID Lock. Το πρώτο, σας ειδοποιεί προτού ανταλλάξετε πολύτιμες πληροφορίες στο Internet και το δεύτερο διατηρεί τα πολύτιμα δεδομένα σας ασφαλή στο σύστημά σας. Ειδικότερα, το πρόγραμμα υποστηρίζει τα εξής χαρακτηριστικά[76]:

- **Αποτροπή προσβάσεων από hackers:** Κάνει αδιόρατο το σύστημα του χρήστη σε ενδεχόμενες επιθέσεις από hackers, ελέγχοντας συνεχώς την πορεία λειτουργίας του συστήματος, χωρίς να μειώνει την απόδοσή του.
- **Ελεγχος για την ύπαρξη ιών:** Το ZoneAlarm Pro 4 βάζει σε καραντίνα ύποπτα e-mail attachements, αποτρέποντας έτσι την εκτέλεση malicious codes στο σύστημα. Επιπρόσθετα, ελέγχει και σταματά την ενδεχόμενη καταστροφική δράσης απο Trojan horses, spyware, και worms, προτού δημιουργήσουν σοβαρότερα προβλήματα στον υπολογιστή.
- **Μπλοκάρισμα ενοχλητικών popups** κατά τη διάρκεια του surf, για την αποτροπή καθυστερήσεων των down loadings. Επίσης είναι σχεδιασμένο ώστε να υποστηρίζει όλους τους internet browsers.
- **Αναφορά ενδεχόμενων παράνομων προσβάσεων:** Το ZoneAlarm Pro εμφανίζει στο χρήστη ολοκληρωμένες και κατανοητές αναφορές, οι οποίες σχετίζονται είτε με απόπειρες παραβίασης του συστήματος, είτε με τον εντοπισμό ιών, κλπ. Επειδή όμως η ύπαρξη και μόνο του firewall στο σύστημα, δεν επαρκεί για την αποτροπή δυσάρεστων εκπλήξεων, θα πρέπει στο πρόγραμμα να έχουν γίνει και οι κατάλληλες ρυθμίσεις. Τις

παραμέτρους αυτές πρόκειται να σας δείξουμε στο παρακάτω workshop, ώστε να αντιμετωπίσετε σωστά την όποια παράνομη πρόσβαση.

6.2 Configuration wizard

Σε πρώτο στάδιο και αφού ολοκληρώσετε την εγκατάσταση του Zone Alarm Pro στο σύστημά σας, μπορείτε να ενεργοποιήσετε κάποιες προαιρετικές μεν, πλην χρήσιμες ρυθμίσεις που θα ισχυροποιήσουν τα επίπεδα προστασίας. Το πρόγραμμα εμφανίζει την πρώτη φορά που θα το τρέξετε ένα configuration wizard, όπου μπορείτε να ορίσετε settings όπως passwords, τύπο firewall alerts, κλπ. Αναφορικά με τα firewall alerts, θα σας προτείναμε να ενεργοποιήσετε τη μεσαία επιλογή, με την οποία το πρόγραμμα ειδοποιεί μόνο σε περίπτωση εντοπισμού παράνομης δραστηριότητας, και όχι σε κάθε εισερχόμενο traffic.[76]

6.3 Edit Network settings

Έχοντας ολοκληρώσει τον οδηγό ρυθμίσεων το πρόγραμμα είναι έτοιμο να δεχθεί τις λοιπές παραμέτρους. Κάντε διπλό κλικ στο tray icon του zone alarm και μεταβείτε Firewall / Zones. Επιλέξτε ένα απο τα δίκτυα που ανήκετε - εάν υπάρχουν - και κάντε κλικ στο Edit. Ουσιαστικά υποστηρίζονται τρεις ζώνες: internet, trusted και blocked. Κάντε κλικ στο Add για να εισάγετε στο blocked κάποια IP ή site που “χτυπάει” (ping) το σύστημά σας, ή για να εισάγετε στο trusted zone κάποιο IP address , με το οποίο επικοινωνείτε ή ανταλλάσετε αρχεία. Στην περίπτωση που έχετε κάποια εμπειρία με firewall software, μπορείτε να αξιοποιήσετε και το χαρακτηρισιτκό expert rules (Firewall / Expert) του Zone Alarm, ορίζοντας αυστηρότερους κανόνες με βάση τα ports και τα protocols που χρησιμοποιούνται, ή την IP του πακέτου δεδομένων προέλευσης/προορισμού.[76]

6.4 Ρύθμιση των security zones

Στην καρτέλα “main” του Firewall tab, έχετε τη δυνατότητα να ορίσετε τις ζώνες ασφαλείας που υποστηρίζει το πρόγραμμα. Περιλαμβάνονται 3: High (Stelath mode) Medium (sharing mode) και Low (όπου η προστασία firewall απενεργοποιείται τελείως). Στο Blocked security zone (όπου καμία επικοινωνία δεν είναι εφικτή), κάνοντας κλικ στο Advanced μπορείτε να ορίσετε παραμέτρους και για τη δυνατότητα “Internet Connection Sharing” των Windows, στην περίπτωση που τη χρησιμοποιείτε στο σπίτι (σε small home network). Σε κάθε περίπτωση να θυμάστε ότι η ρύθμιση High προτείνεται για το

internet, και η Medium μόνο για τα συστήματα (τις IP) που εμπιστεύεστε, με άλλα λόγια για το trusted zone. [76]

6.5 Ρύθμιση του Program control

Μεταβείτε στην επιλογή Program Controls και συγκεκριμένα στο Programs tab, για να εισάγετε την κατάλληλη παράμετρο αποδοχής, άρνησης ή ερώτησης (Allow, Block, Ask), των permissions με άλλα λόγια που έχει το πρόγραμμα για κάθε ζώνη ασφαλείας. Για να τα ορίσετε κάντε κλικ στις στήλες: Access, Server και Send Mail. Επιπρόσθετα κάνοντας κλικ στο Options ή δεξί κλικ σε κάθε στήλη εφαρμογής που επιλέξατε, μπορείτε να ορίσετε και άλλες παραμέτρους στο επίπεδο ασφαλείας της, όπως πχ. Authentication, filter options, κλπ. Εάν θέλετε να προσθέσετε και άλλα προγράμματα του συστήματος που δεν εμφανίζονται στη λίστα, κάντε κλικ στο Add.[76]

6.6 Ρύθμιση Alert & Logos

Μεταβείτε στην επιλογή Alerts and Logs για να ορίσετε τις παραμέτρους συναγερμών και της καταγραφής τους στο σύστημα. Το Zone Alarm με άλλα λόγια υποστηρίζει τη δυνατότητα ειδοποίησης όταν εντοπίζει κάποια ύποπτη δραστηριότητα, είτε μέσω popup messages, είτε ως logged files, που μπορεί να ελέγξει ανά πάσα στιγμή ο χρήστης. Σημειώνεται ότι τα program alerts, εμφανίζονται πάντα, καθώς απαιτούν το Yes ή No από τον χρήστη. Εάν θέλετε να βλέπετε τα action events που καταγράφονται από το πρόγραμμα, κάντε κλικ στο tab: Log Viewer, του προγράμματος.[76]

6.7 Ρύθμιση E-mail protection

Ένα άλλο στοιχείο του συστήματος που θα πρέπει επίσης να διασφαλίσετε, είναι αυτό της ηλεκτρονικής αλληλογραφίας, από το οποίο ας μην ξεχνάμε ότι περνούν και στο σύστημά μας τα λεγόμενα malicious codes (μέσω των συνημμένων αρχείων) ή κοινώς τους ιούς!. Ειδικότερα, στο tab Attachements, μπορείτε να επιλέξετε τους τύπους των extensions που δεν θα είναι σε καραντίνα (κάνοντας δεξί κλικ σε κάποιο από αυτά στη στήλη Quarantine. Εάν πάλι θέλετε να εισάγετε έναν τύπο συνημμένου αρχείου που δεν υπάρχει στη λίστα, απλά κάντε κλικ στο Add. Επίσης υποστηρίζεται “inbound” και “outbound” mail protection, για εκτενή έλεγχο εισερχόμενης και εξερχόμενης αλληλογραφίας.[76]

6.8 ID Lock: My Vault

Το χαρακτηριστικό ID Lock, υποστηρίζεται μόνο στην τελευταία έκδοση 4 του Zone Alarm Pro 4, και περιλαμβάνει δύο παραμέτρους προστασίας: My Vault και Trusted Sites. Αναφορικά με το My Vault, πρόκειται για την προστασία των προσωπικών σας δεδομένων, διασφαλίζοντάς τα από hackers και identity thieves. Όταν είναι ενεργό το εν λόγω χαρακτηριστικό, κάθε πληροφορία που έχετε αποθηκεύσει εκεί, είναι ασφαλής. Το status area του Zone Alarm, σας ενημερώνει με αναφορές, κάθε φορά που επιχειρήθηκε η κλοπή ταυτότητας ή των προσωπικών σας δεδομένων από το σύστημά σας. [76]

6.9 ID Lock: Trusted sites

Αναφορικά με τη δεύτερη παράμετρο ρύθμισης του χαρακτηριστικού ID Lock, το “Trusted Sites”, το πρόγραμμα υποστηρίζει δύο κατηγορίες διασφάλισης και ελέγχου των web pages: Security Alliance Partner (sites που έχουν πιστοποιηθεί απο το Zone Alarm) και Custom (sites για το περιεχόμενο και την ασφάλεια των οποίων ευθύνεται ο χρήστης και τα οποία έχει εισάγει στη λίστα, καθώς τα θεωρεί έμπιστα. Για να εισάγετε τα sites που θέλετε, κάντε κλικ στο Add. Αφού πληκτρολογήσετε την ηλεκτρονική διεύθυνση, το πρόγραμμα επιβεβαιώνει ότι όντως είναι υπαρκτή στο web και καταγράφει την IP της.[76]

ΚΕΦΑΛΑΙΟ 7^{Ο} : ΣΥΜΠΕΡΑΣΜΑΤΑ ΓΙΑ ΤΑ FIREWALLS

7.1 Συμπεράσματα για τα firewalls

Ένα firewall παρέχει τα μέσα για την υλοποίηση και εφαρμογή πολιτικής πρόσβασης στο δίκτυο. Άσχετα από την ύπαρξη ή όχι ενός firewall η ύπαρξη μιας τέτοιας πολιτικής εξαρτάται αποκλειστικά από τη συνεργασία των χρηστών. Εκτός από τα οφέλη από τη χρήση των firewalls υπάρχουν επίσης κάποια μειονεκτήματα, όπως επίσης υπάρχουν και κίνδυνοι από τους οποίους δεν μπορούν να προστατεύσουν το δίκτυο. Το firewall δεν είναι σε καμία περίπτωση πανάκεια για την επίλυση όλων των προβλημάτων ασφάλειας.[77]

Το πλέον φανερό μειονέκτημα ενός firewall είναι ότι μπορεί να μπλοκάρει κάποιες υπηρεσίες τις οποίες οι χρήστες θέλουν να χρησιμοποιήσουν όπως TELNET, FTP, X/Windows, NFS, κλπ. Εν τούτοις αυτά τα μειονεκτήματα δεν αφορούν μόνο στα firewalls, η πρόσβαση στο δίκτυο μπορεί να περιορίζεται επίσης και στο επίπεδο του host, ανάλογα με την πολιτική ασφάλειας της εγκατάστασης. Μία καλοσχεδιασμένη πολιτική η οποία εξισορροπεί τις ανάγκες ασφάλειας με τις απαιτήσεις των χρηστών μπορεί να βοηθήσει στο ξεπέρασμα των προβλημάτων.[77]

Μερικές εγκαταστάσεις έχουν τοπολογία η οποία δεν προσαρμόζεται σε ένα firewall, ή μπορεί να χρησιμοποιεί υπηρεσίες με τέτοιο τρόπο ώστε η χρήση ενός firewall να απαιτεί μεγάλες ανακατασκευές στη χρήση του δικτύου.[77]

Γενικά τα Firewalls δεν παρέχουν προστασία από εσωτερικές απειλές. Ενώ ένα firewall έχει σχεδιασθεί για να αποτρέπει εξωτερική πρόσβαση σε ευαίσθητα δεδομένα, δεν σταματά τους εσωτερικούς χρήστες από την αντιγραφή δεδομένων σε κάποιο μαγνητικό μέσο. Έτσι είναι λάθος να πιστέψει κανείς ότι η ύπαρξη ενός firewall παρέχει προστασία από κακόβουλες πράξεις εσωτερικά.[77]

Άλλα προβλήματα ή θέματα που ανακύπτουν σχετικά με τα firewalls είναι τα ακόλουθα:

- Ιοί - Τα firewalls δεν προστατεύουν τους χρήστες από τα προσβεβλημένα από ιούς προγράμματα που "κατεβάζουν" από το Διαδίκτυο ή μεταφέρουν σαν attachments με τα e-mail. Επειδή αυτά τα προγράμματα κωδικοποιούνται ή συμπιέζονται με πολλούς τρόπους δεν μπορεί ένα firewall να αναγνώσει τέτοια προγράμματα. Το πρόβλημα πρέπει να αντιμετωπισθεί με ειδικό λογισμικό.

- Throughput - Τα firewalls αντιπροσωπεύουν ένα δυνητικό bottleneck, αφού όλες οι συνδέσεις περνούν μέσα από αυτά και σε πολλές περιπτώσεις εξετάζονται και από αυτά. Εν τούτοις σήμερα αυτό δεν αποτελεί τόσο μεγάλο πρόβλημα αφού έχει αυξηθεί ιδιαίτερα το bandwidth των γραμμών που χρησιμοποιούνται για τη σύνδεση.
- Ένα σύστημα firewall συγκεντρώνει τα θέματα ασφάλειας σε ένα σημείο σε αντίθεση με την κατανομή τους στα διάφορα συστήματα.. Ένα πρόβλημα στο firewall μπορεί να αποβεί καταστροφικό για άλλα λιγότερο προστατευμένα συστήματα του δικτύου.

Παρόλα τα μειονεκτήματα συνίσταται η χρήση των firewalls όπως και άλλων τεχνικών και εργαλείων για την ασφάλεια.[77]

ΒΙΒΛΙΟΓΡΑΦΙΑ

1. Brenton C., Hunt C. (2003), “Ασφάλεια δικτύων – Ο απόλυτος οδηγός για την προστασία του δικτύου σας”, εκδόσεις Γκιούρδας, Αθήνα, σελ. 182-183
2. http//www.chip.gr/_magazine/viewthema.asp?=23901
3. Brenton C., Hunt C. (2003), “Ασφάλεια δικτύων – Ο απόλυτος οδηγός για την προστασία του δικτύου σας”, εκδόσεις Γκιούρδας, Αθήνα, σελ. 183
4. Brenton C., Hunt C. (2003), “Ασφάλεια δικτύων – Ο απόλυτος οδηγός για την προστασία του δικτύου σας”, εκδόσεις Γκιούρδας, Αθήνα, σελ. 184
5. Brenton C., Hunt C. (2003), “Ασφάλεια δικτύων – Ο απόλυτος οδηγός για την προστασία του δικτύου σας”, εκδόσεις Γκιούρδας, Αθήνα, σελ. 184-185
6. Brenton C., Hunt C. (2003), “Ασφάλεια δικτύων – Ο απόλυτος οδηγός για την προστασία του δικτύου σας”, εκδόσεις Γκιούρδας, Αθήνα, σελ. 185
7. Brenton C., Hunt C. (2003), “Ασφάλεια δικτύων – Ο απόλυτος οδηγός για την προστασία του δικτύου σας”, εκδόσεις Γκιούρδας, Αθήνα, σελ. 186
8. Brenton C., Hunt C. (2003), “Ασφάλεια δικτύων – Ο απόλυτος οδηγός για την προστασία του δικτύου σας”, εκδόσεις Γκιούρδας, Αθήνα, σελ. 186-187
9. Brenton C., Hunt C. (2003), “Ασφάλεια δικτύων – Ο απόλυτος οδηγός για την προστασία του δικτύου σας”, εκδόσεις Γκιούρδας, Αθήνα, σελ. 187
10. Brenton C., Hunt C. (2003), “Ασφάλεια δικτύων – Ο απόλυτος οδηγός για την προστασία του δικτύου σας”, εκδόσεις Γκιούρδας, Αθήνα, σελ. 188
11. Brenton C., Hunt C. (2003), “Ασφάλεια δικτύων – Ο απόλυτος οδηγός για την προστασία του δικτύου σας”, εκδόσεις Γκιούρδας, Αθήνα, σελ. 189
12. Brenton C., Hunt C. (2003), “Ασφάλεια δικτύων – Ο απόλυτος οδηγός για την προστασία του δικτύου σας”, εκδόσεις Γκιούρδας, Αθήνα, σελ. 189-190
13. Brenton C., Hunt C. (2003), “Ασφάλεια δικτύων – Ο απόλυτος οδηγός για την προστασία του δικτύου σας”, εκδόσεις Γκιούρδας, Αθήνα, σελ. 190
14. Brenton C., Hunt C. (2003), “Ασφάλεια δικτύων – Ο απόλυτος οδηγός για την προστασία του δικτύου σας”, εκδόσεις Γκιούρδας, Αθήνα, σελ. 191-192
15. Brenton C., Hunt C. (2003), “Ασφάλεια δικτύων – Ο απόλυτος οδηγός για την προστασία του δικτύου σας”, εκδόσεις Γκιούρδας, Αθήνα, σελ. 192
16. Brenton C., Hunt C. (2003), “Ασφάλεια δικτύων – Ο απόλυτος οδηγός για την προστασία του δικτύου σας”, εκδόσεις Γκιούρδας, Αθήνα, σελ. 193
17. Brenton C., Hunt C. (2003), “Ασφάλεια δικτύων – Ο απόλυτος οδηγός για την προστασία του δικτύου σας”, εκδόσεις Γκιούρδας, Αθήνα, σελ. 195

18. Brenton C., Hunt C. (2003), “Ασφάλεια δικτύων – Ο απόλυτος οδηγός για την προστασία του δικτύου σας”, εκδόσεις Γκιούρδας, Αθήνα, σελ. 196
19. Brenton C., Hunt C. (2003), “Ασφάλεια δικτύων – Ο απόλυτος οδηγός για την προστασία του δικτύου σας”, εκδόσεις Γκιούρδας, Αθήνα, σελ. 197
20. Brenton C., Hunt C. (2003), “Ασφάλεια δικτύων – Ο απόλυτος οδηγός για την προστασία του δικτύου σας”, εκδόσεις Γκιούρδας, Αθήνα, σελ. 198
21. Brenton C., Hunt C. (2003), “Ασφάλεια δικτύων – Ο απόλυτος οδηγός για την προστασία του δικτύου σας”, εκδόσεις Γκιούρδας, Αθήνα, σελ. 199
22. Brenton C., Hunt C. (2003), “Ασφάλεια δικτύων – Ο απόλυτος οδηγός για την προστασία του δικτύου σας”, εκδόσεις Γκιούρδας, Αθήνα, σελ. 200
23. Brenton C., Hunt C. (2003), “Ασφάλεια δικτύων – Ο απόλυτος οδηγός για την προστασία του δικτύου σας”, εκδόσεις Γκιούρδας, Αθήνα, σελ. 201
24. Brenton C., Hunt C. (2003), “Ασφάλεια δικτύων – Ο απόλυτος οδηγός για την προστασία του δικτύου σας”, εκδόσεις Γκιούρδας, Αθήνα, σελ. 201-202
25. Brenton C., Hunt C. (2003), “Ασφάλεια δικτύων – Ο απόλυτος οδηγός για την προστασία του δικτύου σας”, εκδόσεις Γκιούρδας, Αθήνα, σελ. 202
26. Brenton C., Hunt C. (2003), “Ασφάλεια δικτύων – Ο απόλυτος οδηγός για την προστασία του δικτύου σας”, εκδόσεις Γκιούρδας, Αθήνα, σελ. 203
27. Brenton C., Hunt C. (2003), “Ασφάλεια δικτύων – Ο απόλυτος οδηγός για την προστασία του δικτύου σας”, εκδόσεις Γκιούρδας, Αθήνα, σελ. 204
28. Brenton C., Hunt C. (2003), “Ασφάλεια δικτύων – Ο απόλυτος οδηγός για την προστασία του δικτύου σας”, εκδόσεις Γκιούρδας, Αθήνα, σελ. 205
29. Brenton C., Hunt C. (2003), “Ασφάλεια δικτύων – Ο απόλυτος οδηγός για την προστασία του δικτύου σας”, εκδόσεις Γκιούρδας, Αθήνα, σελ. 206
30. Brenton C., Hunt C. (2003), “Ασφάλεια δικτύων – Ο απόλυτος οδηγός για την προστασία του δικτύου σας”, εκδόσεις Γκιούρδας, Αθήνα, σελ. 209
31. Brenton C., Hunt C. (2003), “Ασφάλεια δικτύων – Ο απόλυτος οδηγός για την προστασία του δικτύου σας”, εκδόσεις Γκιούρδας, Αθήνα, σελ. 210
32. Brenton C., Hunt C. (2003), “Ασφάλεια δικτύων – Ο απόλυτος οδηγός για την προστασία του δικτύου σας”, εκδόσεις Γκιούρδας, Αθήνα, σελ. 210-211
33. Brenton C., Hunt C. (2003), “Ασφάλεια δικτύων – Ο απόλυτος οδηγός για την προστασία του δικτύου σας”, εκδόσεις Γκιούρδας, Αθήνα, σελ. 211
34. Brenton C., Hunt C. (2003), “Ασφάλεια δικτύων – Ο απόλυτος οδηγός για την προστασία του δικτύου σας”, εκδόσεις Γκιούρδας, Αθήνα, σελ. 212

35. Brenton C., Hunt C. (2003), “Ασφάλεια δικτύων – Ο απόλυτος οδηγός για την προστασία του δικτύου σας”, εκδόσεις Γκιούρδας, Αθήνα, σελ. 212-213
36. Brenton C., Hunt C. (2003), “Ασφάλεια δικτύων – Ο απόλυτος οδηγός για την προστασία του δικτύου σας”, εκδόσεις Γκιούρδας, Αθήνα, σελ. 213
37. Brenton C., Hunt C. (2003), “Ασφάλεια δικτύων – Ο απόλυτος οδηγός για την προστασία του δικτύου σας”, εκδόσεις Γκιούρδας, Αθήνα, σελ. 213-214
38. Brenton C., Hunt C. (2003), “Ασφάλεια δικτύων – Ο απόλυτος οδηγός για την προστασία του δικτύου σας”, εκδόσεις Γκιούρδας, Αθήνα, σελ. 214
39. Brenton C., Hunt C. (2003), “Ασφάλεια δικτύων – Ο απόλυτος οδηγός για την προστασία του δικτύου σας”, εκδόσεις Γκιούρδας, Αθήνα, σελ. 215
40. Brenton C., Hunt C. (2003), “Ασφάλεια δικτύων – Ο απόλυτος οδηγός για την προστασία του δικτύου σας”, εκδόσεις Γκιούρδας, Αθήνα, σελ. 216
41. Brenton C., Hunt C. (2003), “Ασφάλεια δικτύων – Ο απόλυτος οδηγός για την προστασία του δικτύου σας”, εκδόσεις Γκιούρδας, Αθήνα, σελ. 217
42. Brenton C., Hunt C. (2003), “Ασφάλεια δικτύων – Ο απόλυτος οδηγός για την προστασία του δικτύου σας”, εκδόσεις Γκιούρδας, Αθήνα, σελ. 218
43. Brenton C., Hunt C. (2003), “Ασφάλεια δικτύων – Ο απόλυτος οδηγός για την προστασία του δικτύου σας”, εκδόσεις Γκιούρδας, Αθήνα, σελ. 219
44. Brenton C., Hunt C. (2003), “Ασφάλεια δικτύων – Ο απόλυτος οδηγός για την προστασία του δικτύου σας”, εκδόσεις Γκιούρδας, Αθήνα, σελ. 219-220
45. Brenton C., Hunt C. (2003), “Ασφάλεια δικτύων – Ο απόλυτος οδηγός για την προστασία του δικτύου σας”, εκδόσεις Γκιούρδας, Αθήνα, σελ. 220-221
46. Brenton C., Hunt C. (2003), “Ασφάλεια δικτύων – Ο απόλυτος οδηγός για την προστασία του δικτύου σας”, εκδόσεις Γκιούρδας, Αθήνα, σελ. 221
47. Brenton C., Hunt C. (2003), “Ασφάλεια δικτύων – Ο απόλυτος οδηγός για την προστασία του δικτύου σας”, εκδόσεις Γκιούρδας, Αθήνα, σελ. 222
48. Brenton C., Hunt C. (2003), “Ασφάλεια δικτύων – Ο απόλυτος οδηγός για την προστασία του δικτύου σας”, εκδόσεις Γκιούρδας, Αθήνα, σελ. 223
49. Brenton C., Hunt C. (2003), “Ασφάλεια δικτύων – Ο απόλυτος οδηγός για την προστασία του δικτύου σας”, εκδόσεις Γκιούρδας, Αθήνα, σελ. 224
50. Brenton C., Hunt C. (2003), “Ασφάλεια δικτύων – Ο απόλυτος οδηγός για την προστασία του δικτύου σας”, εκδόσεις Γκιούρδας, Αθήνα, σελ.224-225
51. Brenton C., Hunt C. (2003), “Ασφάλεια δικτύων – Ο απόλυτος οδηγός για την προστασία του δικτύου σας”, εκδόσεις Γκιούρδας, Αθήνα, σελ. 225

52. Brenton C., Hunt C. (2003), “Ασφάλεια δικτύων – Ο απόλυτος οδηγός για την προστασία του δικτύου σας”, εκδόσεις Γκιούρδας, Αθήνα, σελ. 225-226
53. Brenton C., Hunt C. (2003), “Ασφάλεια δικτύων – Ο απόλυτος οδηγός για την προστασία του δικτύου σας”, εκδόσεις Γκιούρδας, Αθήνα, σελ. 226
54. Brenton C., Hunt C. (2003), “Ασφάλεια δικτύων – Ο απόλυτος οδηγός για την προστασία του δικτύου σας”, εκδόσεις Γκιούρδας, Αθήνα, σελ. 227
55. Brenton C., Hunt C. (2003), “Ασφάλεια δικτύων – Ο απόλυτος οδηγός για την προστασία του δικτύου σας”, εκδόσεις Γκιούρδας, Αθήνα, σελ. 227-228
56. Brenton C., Hunt C. (2003), “Ασφάλεια δικτύων – Ο απόλυτος οδηγός για την προστασία του δικτύου σας”, εκδόσεις Γκιούρδας, Αθήνα, σελ. 229
57. Brenton C., Hunt C. (2003), “Ασφάλεια δικτύων – Ο απόλυτος οδηγός για την προστασία του δικτύου σας”, εκδόσεις Γκιούρδας, Αθήνα, σελ. 230
58. Brenton C., Hunt C. (2003), “Ασφάλεια δικτύων – Ο απόλυτος οδηγός για την προστασία του δικτύου σας”, εκδόσεις Γκιούρδας, Αθήνα, σελ. 230-231
59. Brenton C., Hunt C. (2003), “Ασφάλεια δικτύων – Ο απόλυτος οδηγός για την προστασία του δικτύου σας”, εκδόσεις Γκιούρδας, Αθήνα, σελ. 231
60. Brenton C., Hunt C. (2003), “Ασφάλεια δικτύων – Ο απόλυτος οδηγός για την προστασία του δικτύου σας”, εκδόσεις Γκιούρδας, Αθήνα, σελ. 232
61. Brenton C., Hunt C. (2003), “Ασφάλεια δικτύων – Ο απόλυτος οδηγός για την προστασία του δικτύου σας”, εκδόσεις Γκιούρδας, Αθήνα, σελ. 234
62. Brenton C., Hunt C. (2003), “Ασφάλεια δικτύων – Ο απόλυτος οδηγός για την προστασία του δικτύου σας”, εκδόσεις Γκιούρδας, Αθήνα, σελ. 238
63. Brenton C., Hunt C. (2003), “Ασφάλεια δικτύων – Ο απόλυτος οδηγός για την προστασία του δικτύου σας”, εκδόσεις Γκιούρδας, Αθήνα, σελ. 238-239
64. Brenton C., Hunt C. (2003), “Ασφάλεια δικτύων – Ο απόλυτος οδηγός για την προστασία του δικτύου σας”, εκδόσεις Γκιούρδας, Αθήνα, σελ. 239
65. Brenton C., Hunt C. (2003), “Ασφάλεια δικτύων – Ο απόλυτος οδηγός για την προστασία του δικτύου σας”, εκδόσεις Γκιούρδας, Αθήνα, σελ. 248
66. Brenton C., Hunt C. (2003), “Ασφάλεια δικτύων – Ο απόλυτος οδηγός για την προστασία του δικτύου σας”, εκδόσεις Γκιούρδας, Αθήνα, σελ. 248-249
67. Brenton C., Hunt C. (2003), “Ασφάλεια δικτύων – Ο απόλυτος οδηγός για την προστασία του δικτύου σας”, εκδόσεις Γκιούρδας, Αθήνα, σελ. 249
68. Brenton C., Hunt C. (2003), “Ασφάλεια δικτύων – Ο απόλυτος οδηγός για την προστασία του δικτύου σας”, εκδόσεις Γκιούρδας, Αθήνα, σελ. 249-250

69. Brenton C., Hunt C. (2003), “Ασφάλεια δικτύων – Ο απόλυτος οδηγός για την προστασία του δικτύου σας”, εκδόσεις Γκιούρδας, Αθήνα, σελ. 250
70. Brenton C., Hunt C. (2003), “Ασφάλεια δικτύων – Ο απόλυτος οδηγός για την προστασία του δικτύου σας”, εκδόσεις Γκιούρδας, Αθήνα, σελ. 250-251
71. Brenton C., Hunt C. (2003), “Ασφάλεια δικτύων – Ο απόλυτος οδηγός για την προστασία του δικτύου σας”, εκδόσεις Γκιούρδας, Αθήνα, σελ. 251-252
72. Brenton C., Hunt C. (2003), “Ασφάλεια δικτύων – Ο απόλυτος οδηγός για την προστασία του δικτύου σας”, εκδόσεις Γκιούρδας, Αθήνα, σελ. 252
73. Brenton C., Hunt C. (2003), “Ασφάλεια δικτύων – Ο απόλυτος οδηγός για την προστασία του δικτύου σας”, εκδόσεις Γκιούρδας, Αθήνα, σελ. 252-253
74. Brenton C., Hunt C. (2003), “Ασφάλεια δικτύων – Ο απόλυτος οδηγός για την προστασία του δικτύου σας”, εκδόσεις Γκιούρδας, Αθήνα, συνοδευτικό cd αρχείο FW1-4.1_ Brochure.pdf
75. http//www.chip.gr/_magazine/viewthema.asp?=28622
76. http//www.chip.gr/_magazine/viewthema.asp?=28465
77. http//www.noc.tuc.gr