Ελληνικό Firewalling και Proxy Server HOWTO

Mark Grennan, markg@netplus.net

v0.4, 8 November 1996

Αυτή η τεκμηρίωση είναι σχεδιασμένη να διδάξει τα βασικά των firewall συστημάτων και να δώσει μερικές λεπτομέρειες για την εγκατάσταση firewall, εξουσιοδότησης (proxy) και φίλτρων (filtering), σε PC βασισμένα σε Linux. Μία HTML έκδοση (αγγλική) αυτής της τεκμηρίωσης είναι διαθέσιμη στο *http://okcforum.org/~markg/Firewall-HOWTO.html*

Contents

1 Εισαγωγή

Η αυθεντική έκδοση του Firewall-HOWTO γράφτηκε από τον David Rudder, **drig@execpc.com**. και θέλω να τον ευχαριστήσω που με άφησε να ανανεώσω τη δουλειά του.

Τα firewalls έχουν κερδίσει πρόσφατα μεγάλη φήμη σαν ύστατη ασφάλεια μέσα στο Internet. Όπως στα περισσότερα πράγματα που κερδίζουν φήμη έρχονται και παρερμηνεύσεις. Αυτό το HOWTO θα καλύψει τα βασικά του τί είναι ένα firewall, πώς να στήσετε ένα, τί είναι διακομιστές εξουσιοδότησης (proxy servers), πώς να στήσετε έναν διακομιστή εξουσιοδότησης, καθώς και οι εφαρμογές αυτής της τεχνολογίας εκτός του ασφαλούς βασιλείου.

1.1 Ανάδραση

Οποιαδήποτε ανάδραση είναι καλοδεχούμενη. **ΠΑΡΑΚΑΛΩ ΝΑ ΑΝΑΦΕΡΕΤΕ ΤΥΧΟΝ ΑΝΑΚΡΙΒΙΕΣ ΣΕ ΑΥΤΗ ΤΗ ΤΕΚΜΙΡΙΩΣΗ !!!** Είμαι άνθρωπος και επιρρεπής στο να κάνω λάθη. Εάν βρείτε κανένα η διόρθωσή τους είναι ο απώτερος σκοπός μου. Θα προσπαθήσω να βρω απαντήσεις σε όλα τα e-mail, αλλά είμαι απασχολημένος, γι' αυτό μην προσβληθείτε αν δεν απαντήσω.

Η email διέυθυνσή μου είναι ***markg@netplus.net***

1.2 Αποκύρηξη

ΔΕΝ ΕΙΜΑΙ ΥΠΕΥΘΥΝΟΣ ΓΙΑ ΟΠΟΙΑΔΗΠΟΤΕ ΖΗΜΙΑ ΣΥΜΒΕΙ ΚΑΤΑ ΤΩΝ ΕΝΕΡΓΕΙΩΝ ΠΟΥ ΘΑ ΠΑΡΘΟΥΝ ΒΑΣΙΣΜΕΝΕΣ ΣΕ ΑΥΤΗ ΤΗ ΤΕΚΜΙΡΙΩΣΗ.. Η τεκμηρίωση αυτή προορίζεται σαν μία εισαγωγή στο πως τα firewalls και οι διακομιστές εξουσιοδότησης δουλεύουν. Δεν είμαι, ούτε προσποιούμαι ότι είμαι, ένας ειδικός ασφαλείας. Είμαι ένας απλός τύπος που διάβασε αρκετά και αγαπά περισσότερο του Η/Υ από τη πλειοψηφία των ανθρώπων. Παρακαλώ, γράφω αυτό το βοήθημα κάνοντας γνωστό στο κόσμο αυτό το αντικείμενο, και δεν είμαι έτοιμος να κολλήσω τη ζωή μου σε ό,τι είναι εδώ.

1.3 Δικαιώματα

Αν δεν έχει δηλωθεί διαφορετικά, οι Linux HOWTO τεκμηριώσεις ανήκουν δικαιωματικά στους αντίστοιχους συγγραφείς. Οι Linux HOWTO τεκμηριώσεις μπορούν να αναπαραχθούν, να αναδιανεμειθούν ολόκληρές ή σε τμήματα μέσω κάθε φυσικού ή ηλεκτρονικού μέσου, όσο αυτή η ειδοποίηση δικαιωμάτων είναι προσαρτημένη μαζί με τα αντίγραφα. Η εμπορική αναδιανομή επιτρέπεται και υποστηρίζεται παρ' όλα αυτά, ο συγγραφέας επιθυμεί να ενημερωθεί για οποιεσδήποτε τέτοιες διανομές.

Όλες οι μεταφράσεις, παράγωγα ή αθροιστικές εργασίες που ενσωματώνουν κάθε Linux HOWTO τεκμηρίωση, πρέπει να καλύπτονται κάτω από αυτή την ειδοποίηση δικαιωμάτων. Αυτό σημαίνει, ότι δεν μπορείτε να παράξετε παράγωγη εργασία από ένα HOWTO και σελιδοποιήσετε επιπλέον περιορισμούς στη διανομή. Εξαιρέσεις των κανόνων αυτών μπορούν να γίνουν παραδεκτές κάτω από συγκεκριμένες καταστάσεις, παρακαλούμε να έρθετε σε επαφή με το συντονιστή των Linux HOWTO.

Αν έχετε πιθανές ερωτήσεις, παρακαλούμε επικοινωνήστε με τον Mark Grennan <markg@netplus.net>.

1.4 Οι λόγοι που έγραψα αυτό

Αν και μολονότι υπάρχουν πολλές συζητήσεις κατά το περασμένο έτος στο comp.os.linux.* για το firewalling το βρήκα δύσκολο να βρω τις πληροφορίες που χρειαζόμουν για να στήσω ένα firewall. Η αυθεντική έκδοση αυτού του HOWTO, βοηθούσε αλλά ήταν ελλιπής. Ελπίζω αυτή η ενισχυμένη έκδοση του David Rudder's Firewall HOWTO θα δώσει στον καθένα τις πληροφορίες που χρειάζεται για να δημιουργήσει ένα λειτουργικό firewall μέσα σε ώρες και όχι εβδομάδες.

Επίσης αισθάνομαι ότι θέλω να επιστρέψω κάτι στη κοινότητα του Linux.

1.5 TODO

- Να δώσω κάποια εκπαίδευση πως να εγκατασταθεί ένας πελάτης (client)
- Να βρω ένα ωραίο UDP διακομιστή εξουσιοδότησης να δουλεύει στο Linux.

1.6 Επιπλέον Αναγνώσματα

- Το NET-2 HOWTO
- Το Ethernet HOWTO
- Το Multiple Ethernet Mini HOWTO
- Networking with Linux
- Το PPP HOWTO
- TCP/IP Network Administrator's Guide by O'Reilly and Associates
- Το Documentation για το TIS Firewall Toolkit

Στην ιστοσελίδα της Trusted Information System's (TIS)**http://www.tis.com/** Θα βρείτε μία μεγάλη συλλογή από τεκμηριώσεις πάνω στα firewalls και συναφή υλικά.

Επίσης δουλεύω πάνω σε ένα σχέδιο ασφαλείας, καλείται, που εγώ αποκαλώ *Secure Linux*. Στη *Secure Linux* ιστοσελίδα συγκεντρώνω όλες τις πληροφορίες, τεκμηριώσεις και προγράμματα που χρειάζονται για να δημιουργηθεί ένα ασφαλές σύστημα Linux. Στείλτε μου e-mail εάν θέλετε πληροφορίες.

2 Κατανοώντας το Firewall

Ένας firewall είναι κάτι που χρησιμοποιείται ως κομμάτι ενός αυτοκινήτου. Στα αυτοκίνητα firewalls είναι τα φυσικά αντικείμενα που χωρίζουν το κινητήρα από τους επιβάτες. Αυτά προστατεύουν τους επιβάτες στη περίπτωση που ο κινητήρας πιάσει φωτιά ενώ παρέχουν ακόμη στον οδηγό, πρόσβαση στο χειρισμό του κινητήρα. Ένας firewall στους υπολογιστές είναι μία συσκευή (Η/Υ) που προστατεύει ένα προσωπικό δίκτυο από το δημόσιο κομμάτι. (Το Internet σαν σύνολο.)

Ο firewall υπολογιστής, από εδώ και πέρα θα ονομάζεται "firewall", μπορεί να "ακουμπά" αμφότερα, το προστατευόμενο δίκτυο και το Internet. Το προστατευόμενο δίκτυο δεν μπορεί να προσεγγίσει το Internet, ούτε το Internet μπορεί να προσεγγίσει το προστατευόμενο δίκτυο.

Για κάποιον που θέλει να επικοινωνήσει με το Internet μέσα από το προστατευόμενο δίκτυο, πρέπει να κάνει σύνδεση telnet στο firewall, και να χρησιμοποιήσει το Internet από εκεί.

Η απλούστερη μορφή ενός firewall είναι ένα διπλό σπιτικό σύστημα (ένα σύστημα με δύο συνδέσεις δικτύου). ΕΑΝ ΜΠΟΡΕΙΤΕ ΝΑ ΕΜΠΙΣΤΕΥΤΗΤΕ ΟΛΟΥΣ ΤΟΥΣ ΧΡΗΣΤΕΣ ΣΑΣ μπορείτε απλά να στήσετε ένα Linux (μεταγλωττίστε το πυρήνα με IP Forwarding απενεργοποιημένο) και δώστε όλους τους λογαριασμούς πάνω του. Θα μπορούν να κάνουν σύνδεση στο σύστημα (login), telnet, FTP, να διαβάζουν e-mail, και να χρησιμοποιούν ό,τι έχετε εφοδιάσει. Με αυτό το στήσιμο, ο μόνος υπολογιστής στο προσωπικό σας δίκτυο που θα γνωρίζει τα πάντα σχετικά με τον έξω κόσμο είναι ο firewall. Το άλλο σύστημα στο προστατευόμενο δίκτυο σας, δεν χρειάζονται καν να ορίσετε το συνήθες δρομολόγιο (default route).

Αυτό χρειάζεται μία διευκρίνηση. Για να δουλέψει ο παραπάνω firewall **ΠΡΕΠΕΙ ΝΑ ΕΜΠΙΣΤΕΥΕΣΤΕ ΟΛΟΥΣ ΤΟΥΣ ΧΡΗΣΤΕΣ ΣΑΣ!** Δεν το προτείνω αυτό.

2.1 Μειονεκτήματα με τους firewalls

Το πρόβλημα με τους firewalls φίλτραρίσματος είναι ότι παρεμποδίζουν τη πρόσβαση στο δίκτυο από το Internet. Μόνο υπηρεσίες στα συστήματα που έχουν περάσει το φιλτράρισμα μπορεί να παρεχθεί πρόσβαση. Με τους διακομιστές εξουσιοδότησης οι χρήστες μπορούν να συνδεθούν (login) στο firewall, έχοντας πρόσβαση σε κάθε σύστημα μέσα στο προσωπικό σας δίκτυο, όπου έχουν πρόσβαση.

Επίσης, νέοι τύποι από πελάτες δικτύων (network clients) και διακομιστών έρχονται σχεδόν κάθε μέρα. Όταν αυτό συμβεί θα πρέπει να βρείτε νέους τρόπους για να επιτρέψετε την ελεγχόμενη πρόσβαση πριν αυτές οι υπηρεσίες μπορούν να χρημοποιηθούν.

2.2 Τύποι των Firewalls

Υπάρχουν δύο τύποι firewalls

1. IP Firewalls Φιλτραρίσματος (filtering firewalls) - μπλοκάρουν τα πάντα αλλά σε επιλεγμένα κυκλοφοριακά δίκτυα.
2. Διακομιστές Εξουσιοδότησης (Proxy Servers) - αυτοί κάνουν τη δικτυακή σύνδεση για εσάς.

2.2.1 IP Firewalls Φιλτραρίσματος

Ο IP firewall φιλτραρίσματος δουλεύει σαν ισοσταθμιστής πακέτων. Έχει σχεδιαστεί για να ελέγχει τη ροή από πακέτα βασισμένα στη πηγαία (προορισμένη) πύλη και στις πληροφοριές που περιέχει κάθε πακέτο.

Αυτός ο firewall είναι πολύ ασφαλής αλλά στερήται οποιασδήποτε είδους χρήσιμη εγγραφή συμβάντων. Μπορεί να μπλοκάρει το κόσμο από τη πρόσβαση στο προσωπικό σας δίκτυο αλλά δεν θα αναφέρει ποιός προσπέλασε το δημόσιο σύστημα ή ποιος το Internet από μέσα.

Τα Firewalls φιλτραρίσματος είναι απόλυτα φίλτρα. Ακόμη και αν θέλετε να δώσετε πρόσβαση απ' έξω από τους προσωπικούς σας διακομιστές δεν μπορείτε να το κάνετε χωρίς να δώσετε στους πάντες πρόσβαση στους διακομιστές.

Το Linux περιλαμβάνει το πακέτο φιλτραρίσματος στο πυρήνα από την έκδοση 1.3.χ

2.2.2 Διακομιστές Εξουσιοδότησης

Οι διακομιστές εξουσιοδότησης επιτρέπουν την έμμεση πρόσβαση στο Internet μέσω του firewall. Καλλίτερο παράδειγμα πως δουλεύει είναι, ένα άτομο κάνει telnet σε ένα σύστημα και μετά άλλο telnet από εκεί προς κάπου αλλού. Μόνο με τους διακομιστές εξουσιοδότησης η λειτουργία είναι αυτόματη. Όταν συνδεθείτε σε ένα διακομιστή εξουσιοδότησης με το δικό σας πελατειακό λογισμικό (client software) ο διακομιστής ξεκινά το δικό του πελατειακό (εξουσιοδοτούμενο) λογισμικό και μεταβιβάζει τα δεδομένα σας.

Επειδή οι διακομιστές εξουσιοδότησης αναπαράγουν όλες τις επικοινωνίες μπορούν να καταγράφουν ό,τι κάνουν.

Το καλό με τους διακομιστές εξουσιοδότησης είναι ότι, είναι εντελώς ασφαλείς, όταν ρυθμιστούν σωστά. Δεν θα επιτρέψουν σε κάποιον να περάσει από μέσα τους. Δεν υπάρχουν άμεσα IP δρομολόγια.

3 Στήνοντας ένα Firewall

3.1 Απαιτήσεις Συσκευών (Hardware)

Για το παράδειγμά μας, ο υπολογιστής είναι ένας 486-DX66 με 16MB RAM και 500MB κατάτμηση Linux. Αυτό το σύστημα έχει δύο κάρτες δικτύου, η μία συνδεδεμένη στο τοπικό προσωπικό σας δίκτυο (LAN) και η άλλη με το δίκτυο που καλούμε Αποστρατικοποιημένη Ζώνη (DMZ De-Militarize Zone). Η Α.Ζ. (DMZ) έχει ένα δρομολογητή με σύνδεση στο Internet.

Αυτό είναι ένα ωραίο τοπικό στήσιμο για επιχειρήσεις. Μπορείτε να χρησιμοποιήσετε μία κάρτα δικτύου και ένα modem με PPP στο Internet. Το θέμα είναι ο firewall να έχει δύο IP αριθμούς δικτύου.

Γνωρίζω ότι αρκετά άτομα έχουν μικρά τοπικά δίκτυα (LANs) στο σπίτι με δύο ή τρεις Η/Υ επάνω. Κάτι που πρέπει να σκεφτήτε είναι να βάλετε όλα τα modem σας σε ένα κουτί Linux (ίσως σε ένα παλιό 386) και να συνδέσετε όλα στο Internet με φορτωμένη ισοστάθμιση. Με αυτό το στήσιμο όταν ένα μόνο πρόσωπο τραβάει δεδομένα θα μπορεί να χρησιμοποιεί αμφότερα τα modems διπλασιάζοντας τη ταχύτητα σύνδεσης :-)

4 Λογισμικό για Firewalls.

4.1 Διαθέσιμα πακέτα

Εάν αυτό που ζητάτε είναι ένας firewall φιλτραρίσματος θα χρειαστήτε μόνο το Linux και το βασικό πακέτο για δίκτυα. Ένα πακέτο που μπορεί να μην περιέχεται στη διανομή σας είναι το IP Firewalling Administration Tool.

Το (IPFWADM) υπάρχει στο **http://www.xos.nl/linux/ipfwadm/**

Εάν θέλετε να στήσετε ένα διακομιστή εξουσιοδότησης θα χρειαστήτε ένα από τα παρακάτω πακέτα.

1. SOCKS
2. TIS Firewall Toolkit (FWTK)

4.2 Το TIS Firewall Toolkit εναντίον SOCKS

Το Trusted Information System (http://www.tis.com) έχει εκδόσει μία συλλόγη από προγράμματα σχεδιασμένα για τη διευκόλυνση του firewalling (firewalling). Τα προγράμματα αυτά κάνουν τα ίδια με το SOCS πακέτο, αλλά με διαφορετική σχεδιασμένη στρατηγική. Εκεί που το SOCS έχει ένα πρόγραμμα που καλύπτει όλες τις συναλλαγές του Internet, το TIS παρέχει ένα πρόγραμμα για κάθε τι που επιθυμεί να χρησιμοποιήσει το firewall.

Σε αντιπαραβολή και των δύο, ας πάρουμε το παράδειγμα του World Wide Web και της πρόσβασης telnet. Με το SOCS παίρνετε ένα αρχείο ρυθμίσεων και ένα δαίμονα. Μέσα από το αρχείο αυτό και το δαίμονα, έχετε αμφότερα WWW και telnet ενεργοποιημένα, καθώς και άλλες υπηρεσίες που δεν έχετε απενεργοποιήσει.

Με τη TIS εργαλειοθήκη, στήνετε από ένα δαίμονα στα WWW και telnet, αλλά και από ένα αρχείο ρυθμίσεων επίσης, στο καθένα. Αφού έχετε κάνει τα παραπάνω, οι άλλες προσβάσεις (υπηρεσίες) στο Internet είναι ακόμα απενεργοποιημένες μέχρι να τις στήσετε. Εάν δεν έχετε στήσει ένα δαίμονα για μία συγκεκριμένη υπηρεσία, υπάρχει ένας "plug-in" δαίμονας , αλλά δεν είναι ούτε εύκαμπτος ούτε τόσο εύκολος στην εγκατάσταση, σαν τα άλλα εργαλεία.

Αυτό μπορεί να μην φαίνεται τόσο σοβαρό, αλλά κάνει μεγάλη διαφορά. Το SOCS επιτρέπει να είστε ακατάστατοι. Με ένα φτωχό στήσιμο διακομιστή SOCS, κάποιος από μέσα μπορεί να κερδίσει περισσότερη πρόσβαση από αυτή που κανονικά του έχετε προορίσει. Με τη TIS εργαλειοθήκη, τα άτομα που είναι μέσα έχουν πρόσβαση μόνο εκεί που ο διαχειριστής του συστήματος θέλει να έχουν.

Το SOCS είναι εύκολο στο στήσιμο, ευκολότερο στη μεταγλώττιση (compile) και επιτρέπει μεγάλη ευκαμψία. Η TIS εργαλειοθήκη είναι πιο ασφαλής αν θέλετε να τακτοποιήσετε τους χρήστες σας μέσα στο προσωπικό σας δίκτυο. Και οι δύο παρέχουν απόλυτη προστασία απ' έξω.

Θα καλύψω την εγκατάσταση και το στήσιμο και των δύο.

5 Προετοιμάζοντας το σύστημα Linux

5.1 Μεταγλωττίζοντας το πυρήνα

Ξεκινάμε με μία καθαρή εγκατάσταση της Linux διανομής σας. (Χρησιμοποίησα το RH 3.0.3 και τα παραδείγματα είναι βασισμένα σε αυτή τη διανομή). Όσο πιο λίγο λογισμικό έχετε φορτώσει, τόσο πιο λίγες τρύπες, πίσω πόρτες και (ή) bugs θα υπάρχουν για να παρουσιάσουν προβλήματα ασφαλείας στο σύστημά σας, έτσι φορτώνετε μόνο την έλαχιστη συλλογή από εφαρμογές (minimum installation).

Πάρτε ένα σταθερό πυρήνα. Χρησιμοποίησα τον 2.0.14 πυρήνα του Linux για το σύστημά μου. Έτσι αυτή η τεκμηρίωση είναι βασισμένη στη δική μου σύνθεση.

Θα χρειαστεί να μεταγλωττίσετε ξανά το πυρήνα του Linux με τις ανάλογες ρυθμίσεις. Γι' αυτό κοιτάξτε στα Kernel-HOWTO, Ethernet-HOWTO και NET-2 HOWTO, εάν δεν το έχετε ξανακάνει.

Παρακάτω ακολουθούν οι ρυθμίσεις που γνωρίζω ότι δουλεύουν με το make config.

1. Κάτω από το General setup
   (a) Βάλτε Networking Support ON
2. Κάτω από το Networking Options
   (a) Βάλτε Network firewalls ON
   (b) Βάλτε TCP/IP Networking ON
   (c) Βάλτε IP forwarding/gatewaying OFF (UNLESS you wish to use IP filtering)
   (d) Βάλτε IP Firewalling ON
   (e) Βάλτε IP firewall packet loggin ON (this is not required but it is a good idea)
   (f) Βάλτε IP: masquerading OFF (I am not covering this subject here.)
   (g) Βάλτε IP: accounting ON
   (h) Βάλτε IP: tunneling OFF
   (i) Βάλτε IP: aliasing OFF
   (j) Βάλτε IP: PC/TCP compatibility mode OFF
   (k) Βάλτε IP: Reverse ARP OFF
   (l) Βάλτε Drop source routed frames ON
3. Κάτω από το Network device support
   (a) Βάλτε Network device support ON
   (b) Βάλτε Dummy net driver support ON
   (c) Βάλτε Ethernet (10 or 100Mbit) ON
   (d) Επιλέξτε τη κάρτα δικτύου σας (network card)

Τώρα μπορείτε να μεταγλωττίσετε και να επανεγκαταστήσετε το πυρήνα και επανεκκίνηση (reboot). Η κάρτα (-ες) δικτύου θα εμφανιστούν κατά τη διάρκεια της εκκίνησης. Εάν όχι, πηγαίνετε στα άλλα HOWTO ξανά μέχρι να δουλέψουν

5.2 Ρυθμίζοντας δύο κάρτες δικτύου

Εάν έχετε δύο κάρτες δικτύου στον υπολογιστή σας, πιθανώς θα χρειαστεί να προσθέσετε μία δήλωση στο αρχείο /etc/lilo.conf για τη περιγραφή των IRQ και των διευθύνσεων των δύο καρτών. Η δήλωση στο δικό μου lilo.conf είναι κάπως έτσι:

```
append="ether=12,0x300,eth0 ether=15,0x340,eth1"
```

5.3 Ρυθμίζοντας τις Διευθύνσεις του Δικτύου

Αυτό είναι πραγματικά ένα ενδιαφέρον κομμάτι. Τώρα θα έχετε μερικές αποφάσεις να πάρετε. Επειδή δεν θέλουμε το Internet να έχει πρόσβαση σε κανένα τμήμα του προσωπικού μας δικτύου, δεν χρειάζεται να χρησιμοποιήσουμε πραγματικές διευθύνσεις. Υπάρχει ένας αριθμός διευθύνσεων Internet που βρίσκονται στην άκρη για τα προσωπικά δίκτυα. Επειδή ο καθένας χρειάζεται περισσότερες διευθύνσεις και επειδή αυτές οι διευθύνσεις δεν μπορούν να διασταυρωθούν μέσα στο Internet, είναι καλή επιλογή.

Αυτές, 192.168.2.χχχ, είναι τοποθετημένες στην άκρη και θα τις χρησιμοποιήσουμε στο παράδειγμά μας.

Ο firewall σας, θα είναι μέλος και στα δύο δίκτυα και έτσι θα μπορεί να μεταβιβάζει δεδομένα από και προς το προσωπικό σας δίκτυο.

```
           199.1.2.10   __________    192.168.2.1
   _  __  _          \ |          | /           _______________
  | \/  \/ |          \| Firewall |/           |               |
 / Internet \--------|  System  |------------| Workstation/s |
 \_/\_/\_/\_/        |__________|            |_______________|
```

Εάν επιθυμείτε να χρησιμοποιήσετε firewalls φιλτραρίσματος μπορείτε να χρησιμοποιήσετε ακόμη και τους παραπάνω αριθμούς. Θα χρειαστεί όμως να χρησιμοποιήσετε IP masqurading για να συμβεί αυτό. Με αυτή τη διαδικασία ο firewall θα προωθεί πακέτα και θα τα μεταβιβάζει σε "REAL (πραγματικές)" διευθύνσεις για το ταξίδι τους στο Internet.

Θα πρέπει να ορίσετε τις πραγματικές IP διευθύνσεις στη κάρτα δικτύου πάνω στη (έξω) πλευρά του Internet. Και να ορίσετε 192.168.2.1 στην Ethernet κάρτα στο εσωτερικό. Αυτή θα είναι η IP διεύθυνση του εξουσιοδοτή/πύλη. Μπορείτε να ορίσετε σε όλους τους άλλου Η/Υ μέσα στο προστατευόμενο δίκτυο μερικούς αριθμούς από το 192.168.2.χχχ πεδίο (192.168.2.2 έως 192.168.2.254)

Επειδή χρησιμοποιώ RH Linux (Ε! Παιδιά, μου κάνετε ένα αντίγραφο για τα plugs? ;-) για να ρυθμίσω το δίκτυο κατά το χρόνο εκκίνησης πρόσθεσα ένα ifcfg-eth1 αρχείο στο κατάλογο /etc/sysconfig/network-scripts. Αυτό το αρχείο διαβάζεται κατά τη διάρκεια της εκκίνησης για την εγκατάσταση του δικτύου και των πινάκων.

Παρακάτω παρουσιάζω με τί το ifcfg-eth1 μοιάζει.

```
#!/bin/sh
#>>>Device type: ethernet
#>>>Variable declarations:
DEVICE=eth1
IPADDR=192.168.2.1
NETMASK=255.255.255.0
NETWORK=192.168.2.0
BROADCAST=192.168.2.255
GATEWAY=199.1.2.10
ONBOOT=yes
#>>>End variable declarations
```

Μπορείτε να χρησιμοποιήσετε αυτά τα scripts για να συνδεθήτε αυτόματα μέσω modem στο παροχέα σας Internet. Κοιτάξτε στο ipup-ppp script.

Εάν προορίζετε να χρησιμοποιήσετε modem για τη σύνδεσή σας με το Internet, η εξωτερική IP διεύθυνση θα πρέπει να οριστεί από τον ISP για εσάς κατά τη διάρκεια της σύνδεσης.

5.4 Ελέγχοντας το δίκτυό σας.

Ξεκινήστε ελέγχοντας τα ifconfig και route. Εάν έχετε δύο κάρτες δικτύου το ifconfig θα είναι κάπως έτσι:

```
#ifconfig
lo        Link encap:Local Loopback
          inet addr:127.0.0.0  Bcast:127.255.255.255  Mask:255.0.0.0
          UP BROADCAST LOOPBACK RUNNING  MTU:3584  Metric:1
          RX packets:1620 errors:0 dropped:0 overruns:0
          TX packets:1620 errors:0 dropped:0 overruns:0

eth0      Link encap:10Mbps Ethernet  HWaddr 00:00:09:85:AC:55
          inet addr:199.1.2.10 Bcast:199.1.2.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0
          TX packets:0 errors:0 dropped:0 overruns:0
          Interrupt:12 Base address:0x310

eth1      Link encap:10Mbps Ethernet  HWaddr 00:00:09:80:1E:D7
          inet addr:192.168.2.1  Bcast:192.168.2.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0
          TX packets:0 errors:0 dropped:0 overruns:0
          Interrupt:15 Base address:0x350
```

και ο πίνακας route κάπως έτσι:

```
#route -n
Kernel routing table
Destination     Gateway         Genmask         Flags MSS    Window Use Iface
199.1.2.0       *               255.255.255.0   U     1500   0        15 eth0
192.168.2.0     *               255.255.255.0   U     1500   0         0 eth1
127.0.0.0       *               255.0.0.0       U     3584   0         2 lo
default         199.1.2.10      *               UG    1500   0        72 eth0
```

Σημείωση: 199.1.2.0 είναι η Internet πλευρά αυτού του firewall και 192.168.2.0 η προσωπική πλευρά.

Τώρα προσπαθήστε να κάνετε ping το Internet από το firewall. Συνήθιζα να χρησιμοποιώ το nic.ddn.mil σαν δοκιμαστικό σημείο. Είναι καλό σημείο δοκιμής, αλλά έχει αποδειχθεί ότι είναι λιγότερο αξιόπιστο απ' ότι είχα ελπίσει. Αν δεν δουλέψει με τη πρώτη, προσπαθήστε να κάνετε ping σε μερικά άλλα σημεία που δεν είναι συνδεδεμένα με το τοπικό σας δίκτυο (LAN). Εάν δεν δουλέψει ούτε τώρα, τότε το PPP δεν είναι στημένο σωστά. Ξαναδιαβάστε το NET-2 HOWTO και προσπαθήστε ξανά.

Μετά, προσπαθήστε να κάνετε ping ένα host μέσα στο προστατευόμενο δίκτυο από το firewall. Όλοι οι υπολογιστές μπορούν να κάνουν ping μεταξύ τους. Εάν όχι, πηγαίνετε στο NET-2 HOWTO ξανά και δουλέψετε λίγο πάνω στο δίκτυό σας ακόμη.

Ύστερα, προσπαθήστε να κάνετε ping την εξωτερική διεύθυνση του firewall από το εσωτερικό του προστατευόμενου δικτύου. (Σημείωση: Η διεύθυνση της εξωτερικής πλευράς του firewall δεν είναι κανένας 192.168.2.χχχ IP αριθμός). Εάν μπορείτε, τότε δεν έχετε απενεργοποιήσει το IP Forwarding. Σιγουρευτήτε ότι το θέλετε αυτό. Εάν το αφήσετε ενεργοποιημένο μπορείτε να πάτε κατευθείαν στο κεφάλαιο "**IP εγκατάσταση φιλτραρίσματος (κεφάλαιο 6)**" αυτής της τεκμηρίωσης.

Τώρα, προσπαθήστε να κάνετε ping στο Internet πίσω από το firewall χρησιμοποιώντας τις ίδιες διευθύνσεις που δούλεψαν προηγουμένος. (πχ nic.ddn.mil). Ξανά, εάν έχετε απενεργοποιημένο το IP Forwarding, αυτό δεν πρόκειται να δουλέψει. Αν όμως το έχετε ενεργοποιημένο αυτό θα δουλέψει.

Αν έχετε το IP Forwarding επιλεγμένο να χρησιμοποιήτε "Πραγματικές (REAL)" (και όχι 192.168.2.χχχ) IP διευθύνσεις για το προσωπικό σας δίκτυο. Αν δεν μπορείτε να κάνετε ping το Internet αλλά μπορείτε την Internet πλευρά του firewall ελέξτε αν ο επόμενος δρομολογητής της γραμμής (προς το Internet) δρομολογεί πακέτα στη διεύθυνση του προσωπικού σας δικτύου. (Ο ISP το κάνει αυτό για εσάς)

Εάν έχετε καθορίσει το προστατευόμενο δίκτυο στο 192.168.2.χχχ, τότε κανένα πακέτο δεν μπορεί να δρομολογηθεί σε αυτό με τίποτα. Εάν έχετε προχωρίσει και έχετε ήδη το IP masqurading ενεργοποιημένο, αυτό το τεστ θα δουλέψει.

Τώρα έχετε το βασικό σας σύστημα έτοιμο.

5.5 Ασφαλίζοντας το Firewall.

Ο firewall δεν κάνει καλό αν τον έχουμε διάπλατα ανοικτό σε επιθέσεις μέσω μη χρησιμοποιούμενων υπηρεσιών. Ένας "κακός τύπος (bad guy)" μπορεί να αποκτήσει πρόσβαση στο firewall και να τον τροποποιήσει ανάλογα με τις ανάγκες του.

Ξεκινάμε απενεργοποιώντας όλες τις άχρηστες υπηρεσίες. Κοιτάξτε το αρχείο /etc/inetd.conf. Αυτό το αρχείο ελέγχει το τι κάλεσε τον "υπέρ διακομιστή (super server)". Ελέγχει μία ομάδα από δαίμονες υπηρέτες και τους ξεκινά όταν αυτοί ζητηθούν.

Οπωσδήποτε απενεργοποιούμε τα netstat, systat, tftp, bootp, και finger. Για να απενεργοποιήσουμε μία υπηρεσία, βάλτε # στο πρώτο χαρακτήρα της γραμμής της κάθε υπηρεσίας που δεν θέλουμε. Όταν το κάνετε αυτό, στείλτε ένα SIG-HUP στη διεργασία γράφοντας "**kill -HUP <pid>**", όπου <pid> είναι ο αριθμός εργασίας του inetd. Αυτό μπορεί να κάνει το inedt να ξαναδιαβάσει το αρχείο ρυθμίσεών του (inedt.conf) και επανεκκίνηση (restart).

6 IP εγκατάσταση φιλτραρίσματος (IPFWADM)

Για ξεκίνημα, θα πρέπει να έχετε το IP Forwarding ενεργοποιημένο στο πυρήνα και το σύστημα θα πρέπει να είναι φορτωμένο και να προωθεί ό,τι του στέλνετε. Οι πίνακες δρομολογίων (routing tables) θα πρέπει να είναι στη θέση τους και θα πρέπει να έχετε πρόσβαση παντού, από μέσα έξω και από έξω μέσα.

Άλλα εμείς χτίζουμε ένα firewall, έτσι χρειάζεται να ξεκινήσουμε να βουλώνουμε σε τί υπάρχει πρόσβαση, από όλους.

Στο σύστημά μου δημιούργησα μερικά scripts γα να τοποθετώ στο firewall πολιτική προώθησης και πολιτική θεώρησης. Καλώ αυτά τα scripts από τα /etc/rc.d scripts έτσι το σύστημά μου είναι ρυθμισμένο από τη στιγμή της εκκίνησης.

Εξ ορισμού το IP Forwarding σύστημα στο πυρήνα του Linux προωθεί τα πάντα. Γι' αυτό το script του firewall θα πρέπει να ξεκινά από το να αρνείται πρόσβαση στα πάντα και να καθαρίζει όποιους ipfw κανόνες είναι τοποθετημένοι από τη τελευταία φορά που έτρεξε. Την εργασία αυτή τη κάνει το παρακάτω script :

```
#
```

```
# setup IP packet Accounting and Forwarding
#
#   Forwarding
#
# By default DENY all services
ipfwadm -F -p deny
# Flush all commands
ipfwadm -F -f
ipfwadm -I -f
ipfwadm -O -f
```

Τώρα έχουμε τον τελικό firewall. Τίποτα δεν μπορεί να περάσει από μέσα. Χωρίς αμφιβολία έχετε κάποιες υπηρεσίες που χρειάζεται να προωθήσετε (ενεργοποιήσετε) έτσι εδώ υπάρχουν μερικά παραδείγματα που θα βρείτε χρήσιμα.

- # Προώθηση email στο διακομιστή

  ipfwadm -F -a accept -b -P tcp -S 0.0.0.0/0 1024:65535 -D 192.1.2.10 25
- # Προώθηση σύνδεσης email στον εξωτερικό διακομιστή email

  ipfwadm -F -a accept -b -P tcp -S 196.1.2.10 25 -D 0.0.0.0/0 1024:65535
- # Προώθηση σύνδεσης Web στον Web διακομιστή

  /sbin/ipfwadm -F -a accept -b -P tcp -S 0.0.0.0/0 1024:65535 -D 196.1.2.11 80
- # Προώθηση σύνδεσης Web για τον εξωτερικό Web διακομιστή

  /sbin/ipfwadm -F -a accept -b -P tcp -S 196.1.2.* 80 -D 0.0.0.0/0 1024:65535
- # Προώθηση DNS συναλλαγής

  /sbin/ipfwadm -F -a accept -b -P udp -S 0.0.0.0/0 53 -D 196.1.2.0/24

Μπορείτε να ενδιαφερθήτε επίσης για την καταγραφή των συνδιαλλαγών που περνούν το firewall. Αυτό το script θα καταγράφει κάθε πακέτο. Μπορείτε να προσθέσετε μία γραμμή ή δύο για να καταγράφετε για πακέτα μεταβαίνοντας σε ένα μονό σύστημα.

```
# \textgreek{Kajar'iste} \textgreek{tou} \textgreek{up'arqontec} \textgreek{kan'onec} \textgreek{katagraf'hc}
ipfwadm -A -f
# \textgreek{Katagr'afwntac}
/sbin/ipfwadm -A -f
/sbin/ipfwadm -A out -i -S 196.1.2.0/24 -D 0.0.0.0/0
/sbin/ipfwadm -A out -i -S 0.0.0.0/0 -D 196.1.2.0/24
/sbin/ipfwadm -A in -i -S 196.1.2.0/24 -D 0.0.0.0/0
/sbin/ipfwadm -A in -i -S 0.0.0.0/0 -D 196.1.2.0/24
```

Εάν τα όσα ζητάτε ήταν ένας firewall φιλτραρίσματος μπορείτε να σταματήσετε εδώ. Απολάυστε το :-)

7 Εγκαθιστώντας τον διακομιστή εξουσιοδότησης TIS

7.1 Αποκτώντας το λογισμικό

Η TIS fwtk είναι διαθέσιμη στο **ftp://ftp.tis.com/**.

Μην κάνετε το λάθος που έκανα εγώ. Όταν κατεβάζετε αρχεία από το TIS ΔΙΑΒΑΣΤΕ ΤΑ README. Η TIS fwtk είναι κλειδωμένη μέσα σε ένα κρυφό κατάλογο στο διακομιστή τους.Το TIS ζητά να στείλετε ένα email στο **fwtk-request@tis.com** με μόνο τη λέξη **SEND** στο σώμα του μυνήματος για να μάθετε το όνομα αυτού του κρυμμένου καταλόγου. Δεν χρειάζεται θέμα (subject) στο μήνυμα. Το σύστημά τους θα σας στείλει το όνομα αυτού του κρυφού καταλόγου (καλό για 12 ώρες) για να κατεβάσετε το πηγαίο αρχείο.

Τη στιγμή που γράφω αυτό (το HOWTO) το TIS εκδίδει την έκδοση 2.0 (beta) της FWTK. Αυτή η έκδοση φαίνεται ότι μεταγλωττίζεται καλά (με μερικές εξαιρέσεις) και τα πάντα δουλεύουν. Αυτή είναι η έκδοση που θα καλύψω εδώ. Όταν διαθέσουν το τελικό κώδικα θα ανανεώσω το HOWTO.

Για την εγκατάσταση τη FWTK, δημιουργήστε το κατάλογο fwtk-2.0 στο /usr/src. Μετακινήστε το αντίγραφο της FWTK fwtk-2.0.tar.gz) από το κατάλογό σας σε αυτόν το κατάλογο (/usr/src/fwtk-2.0) και αποσυμπιέστε το. (tar zxf fwtk-2.0.tar.gz)

Η FWTK δεν εξουσιοδοτεί (υποστηρίζει) SSL web κείμενα αλλά υπάρχει ένα πρόσθετο (add on) γι' αυτή γραμμένο από τον Jean-Christophe Touvet. Είναι διαθέσιμο στο **ftp://ftp.edelweb.fr/pub/contrib/fwtk/ssl-gw.tar.Z**. Ο Touvet δεν υποστηρίζει αυτό το κώδικα

Χρησιμοποιώ μία τροποποιημένη έκδοση που περιλαμβάνει πρόσβαση για Netscape ασφαλείς διακομιστές νέων γραμμένο από τον Eric Wedel. Είναι διαθέσιμη στο **ftp://mdi.meridian-data.com/pub/tis.fwtk/ssl-gw/ssl-gw2.tar.Z**.

Στο παράδειγμά μας θα χρησιμοποιήσω την έκδοση του Eric Wedel.

Για να το εγκαταστήσετε, απλά δημιουργήστε το ssl-gw κατάλογο στο /usr/src/fwtk-2.0 και βάλτε τα αρχεία εκεί μέσα.

Όταν εγκατέστησα αυτή τη πύλη απαίτησε μερικές αλλαγές πριν μεταγλωττιστεί μαζί με την υπόλοιπη εργαλειοθήκη.

Η πρώτη αλλαγή ήταν στο ssl-gw.c αρχείο. Βρήκα ότι δεν περιελάμβανε ένα χρήσιμο περιελαμβανόμενο (included) αρχείο.

```
#if defined(__linux)
#include        <sys/ioctl.h>
#endif
```

Δεύτερον δεν έρχεται με Makefile. Αντέγραψα ένα έξω από τους άλλους καταλόγους πυλών και αντικατέστησα το όνομα της πύλης με το ssl-gw.

7.2 Μεταγλωττίζοντας την TIS FWTK

Η έκδοση 2.0 της FWTK μεταγλωττίζεται πολύ πιο εύκολα από οποιαδήποτε παλαιότερη έκδοση. Βρίσκω ακόμα μερικά πράγματα που χρειάζεται να αλλαχθούν πριν η BETA έκδοση μπορεί να μεταγλωττιστεί καθαρά. Ελπίζω αυτές οι αλλαγές να γίνουν στη τελική έκδοση.

Για τη διόρθωσή τους, ξεκινήστε αλλάζοντας το /usr/src/fwtk/fwtk κατάλογο και αντιγράψτε το Makefile.config.linux πάνω από το Makefile.config

ΜΗΝ ΕΚΤΕΛΕΣΕΤΕ ΤΟ FIXMAKE. Οι οδηγίες λένε να το εκτελέσετε. Εάν το κάνετε θα σπάσει τα Makefiles στο κάθε κατάλογο

Δεν έχω καμία διόρθωση για το fixmake. Το πρόβλημα είναι το sed script προσθέστε ένα '.' και " στη κάθε γραμμή που περιλαμβάνει τα Makefiles.

```
sed 's/^include[        ]*\([^  ].*\)/include \1/' $name .proto > $name
```

Μετά χρειάζεται να επεξεργαστούμε το αρχείο Makefile.config. Υπάρχουν δύο αλλαγές που χρειάζεται να κάνετε.

Ο συγγραφέας έθεσε ως πηγαίο κατάλογο το δικό του σπιτικό κατάλογο. Θα μεταγλωττίσουμε το κώδικά μας στο /usr/src έτσι πρέπει να αλλάξουμε τη μεταβλητή FWTKSRCDIR για να αντικατροπτίζει αυτό.

```
FWTKSRCDIR=/usr/src/fwtk/fwtk
```

Δεύτερον, σε ορισμένα λίγα συστήματα Linux χρησιμοποιήται η βάση δεδομένων gdbm. Το Makefile.conf χρησιμοποιεί dbm. Θα χρειαστεί να αλλάξετε αυτό. Είχα για το RH 3.0.3

```
DBMLIB=-lgdbm
```

Η τελευταία διόρθωση είναι στο x-gw. Το bug στη BETA έκδοση είναι μέσα στο socket.c κώδικα. Για να το φτιάξετε σβήστε τις παρακάτω γραμμές κώδικα

```
#ifdef SCM_RIGHTS  /* 4.3BSD Reno and later */
                     + sizeof(un_name->sun_len) + 1
#endif
```

Εάν προσθέσετε το ssl-gw στο FWTK πηγαίο κατάλογο σας. Θα χρειαστήτε να προσθέσετε αυτό στη λίστα καταλόγων στο Makefile.

```
DIRS=   smap smapd netacl plug-gw ftp-gw tn-gw rlogin-gw http-gw x-gw ssl-gw
```

Τώρα εκτελέστε το **make**.

7.3 Εγκαθιστώντας την TIS FWTK

Εκτελέστε **make install**.

Ο εξ ορισμού κατάλογος εγκατάστασης είναι ο /usr/local/etc. Μπορείτε να τον αλλάξετε (εγώ όχι) σε ένα πιο ασφαλές κατάλογο. Διάλεξα να αλλάξω τη πρόσβαση στο κατάλογο αυτό με chmod 700.

Όλα αυτά που έμειναν τώρα είναι η τελική ρύθμιση του firewall

7.4 Ρυθμίζοντας την TIS FWTK

Τώρα αρχίζει η πραγματική διασκέδαση. Πρέπει να μάθουμε :-) το σύστημα να καλεί αυτές τις νέες υπηρεσίες και να δημιουργεί τους πίνακες για τον έλεγχό τους.

Δεν πρόκειται να δοκιμάσω να ξαναγράψω το εγχειρίδιο της TIS FWTK, εδώ. Θα σας δείξω τις ρυθμίσεις που ανακάλυψα δουλεύοντας και θα εξηγήσω τα προβλήματα που βρήκα και πώς τα ξεπέρασα.

Υπάρχουν τρία αρχεία που ρυθμίζουν αυτά τα χειριστήρια

- /etc/services
  - Λέει στο σύστημα τί πόρτες υπηρεσιών είναι ανοικτές
- /etc/inetd.conf
  - Λέει στο inetd τί πρόγραμμα να καλεί όταν κάποιος χτυπά πόρτα υπηρεσίας

- /usr/local/etc/netperm-table
  - Λέει στις FWTK υπηρεσίες σε ποιόν να επιτρέπουν και σε ποιόν να απαγορεύουν της υπηρεσίες τους.

Για να πάρετε τη FWTK λειτουργική, θα πρέπει να επεξεργαστήτε αυτά τα αρχεία από το τελευταίο προς τα πάνω. Επεξεργάζοντας τα αρχεία των υπηρεσιών χωρίς το inedt.conf ή το netperm-table ρυθμισμένα σωστά μπορεί να κάνετε το σύστημά σας απροσπέλαστο.

7.4.1 Το αρχείο netperm-table

Αυτό το αρχείο ελέγχει ποιός μπορεί να έχει πρόσβαση στις υπηρεσίες από τη TIS FWTK. Οφείλετε να σκεφτήτε σχετικά με το κυκλοφοριακό χρησιμοποιώντας το firewall και από τις δύο πλευρές. Ο κόσμος έξω από το δίκτυό σας, οφείλει να αναγνωρίσει τους εαυτούς των πριν κερδίσουν πρόσβαση, αλλά ο κόσμος μέσα στο δίκτυό σας μπορεί να αφεθεί να περνά απλά από μέσα.

Έτσι ο κόσμος μπορεί να αναγνωρίσει τους εαυτούς τους, ο firewall χρησιμοποιεί ένα πρόγραμμα που καλείται **authsrv** για να κρατά μία βάση δεδομένων τα user ID και τους κωδικούς. Το τμήμα επικύρωσης από το netperm-table ελέγχει που η βάση δεδομένων βρίσκεται και ποιός μπορεί να έχει πρόσβαση σε αυτή.

Είχα κάποια προβλήματα κλείνοντας τη πρόσβαση σε αυτή την υπηρεσία. Σημειώστε ότι η γραμμή permit-hosts που παρουσιάζω χρησιμοποιεί '*' για να δίνει σε όλους πρόσβαση. Οι σωστές ρυθμίσεις για τη γραμμή αυτή είναι " `authsrv: premit-hosts localhost` εάν μπορέσετε να το παρέτε αυτό δουλεύοντας

```
#
# Proxy configuration table
#
# Authentication server and client rules
authsrv:      database /usr/local/etc/fw-authdb
authsrv:      permit-hosts *
authsrv:      badsleep 1200
authsrv:      nobogus true
# Client Applications using the Authentication server
*:            authserver 127.0.0.1 114
```

Για να ορίσετε τη βάση δεδομένων, γίνετε root, και εκτελέστε **./authsrv** μέσα στο /var/local/etc κατάλογο για να δημιουργηθεί η εγγραφή του χρήστη που εκτελεί χρέη διαχειριστή. Εδώ είναι ένα απλό παράδειγμα.

Διαβάστε τη τεκμηρίωση της FWTK για να μάθετε πώς να προσθέτετε χρήστες και ομάδες.

```
#
# authsrv
authsrv# list
authsrv# adduser admin "Auth DB admin"
ok - user added initially disabled
authsrv# ena admin
enabled
authsrv# proto admin pass
changed
authsrv# pass admin "plugh"
Password changed.
authsrv# superwiz admin
```

```
set wizard
authsrv# list
Report for users in database
user   group  longname           ok?    proto   last
------ ------ ------------------ -----  ------  -----
admin         Auth DB admin      ena    passw   never
authsrv# display admin
Report for user admin (Auth DB admin)
Authentication protocol: password
Flags: WIZARD
authsrv# ^D
EOT
#
```

Το χειριστήριο της telnet πύλης (tn-gw) είναι κατευθείαν μπροστά και το πρώτο που οφείλετε να στήσετε.

Στο παράδειγμά μου, επιτρέπω σε host από το εσωτερικό του προσωπικού δικτύου να περνάει από μέσα χωρίς να επικυρώνουν τους εαυτούς τους. (permit-hosts 19961.2.* -passok) Αλλά, κάθε άλλος χρήστης πρέπει να εισάγει τα user ID και το κωδικό του για να χρησιμοποιεί τον εξουσιοδοτητή. (permit-hosts * -auth)

Επίσης επιτρέπω σε ένα άλλο σύστημα (196.1.2.202) να έχει πρόσβαση στο firewall χωρίς να περνά μέσα από το firewall στη πραγματικότητα. Οι δύο γραμμές inetacl-in.telnetd το κάνουν αυτό. Θα εξηγήσω πώς αυτές οι γραμμές καλούνται αργότερα.

Το Telnet time out οφείλεται να κρατηθεί μικρό.

```
# telnet gateway rules:
tn-gw:              denial-msg      /usr/local/etc/tn-deny.txt
tn-gw:              welcome-msg     /usr/local/etc/tn-welcome.txt
tn-gw:              help-msg        /usr/local/etc/tn-help.txt
tn-gw:              timeout 90
tn-gw:              permit-hosts 196.1.2.* -passok -xok
tn-gw:              permit-hosts * -auth
# Only the Administrator can telnet directly to the Firewall via Port 24
netacl-in.telnetd: permit-hosts 196.1.2.202 -exec /usr/sbin/in.telnetd
```

Οι r-commands δουλεύουν με τον ίδιο τρόπο όπως το telnet.

```
# rlogin gateway rules:
rlogin-gw:    denial-msg      /usr/local/etc/rlogin-deny.txt
rlogin-gw:    welcome-msg     /usr/local/etc/rlogin-welcome.txt
rlogin-gw:    help-msg        /usr/local/etc/rlogin-help.txt
rlogin-gw:    timeout 90
rlogin-gw:    permit-hosts 196.1.2.* -passok -xok
rlogin-gw:    permit-hosts * -auth -xok
# Only the Administrator can telnet directly to the Firewall via Port
netacl-rlogind: permit-hosts 196.1.2.202 -exec /usr/libexec/rlogind -a
```

Δεν οφείλετε να έχετε σε κανέναν άμεση πρόσβαση στο firewall και αυτό περιλαμβάνει το FTP έτσι δεν βάζουμε το FTP, διακομιστή πάνω στο firewall.

Ξανά, οι γραμμές permit-hosts επιτρέπουν μέσα στο προστατευόμενο δίκτυο ελεύθερη πρόσβαση στο Intenet και όλοι οι άλλοι πρέπει να επικυρώσουν τους εαυτούς τους. Συμπεριέλαβα τη καταγραφή συμβάντων για κάθε αρχείο που αποστέλεται και παραλαμβάνεται για τον ελέγχό μου. (-log { retr stor })

Το ftp timeout ελέγχει πόσο θα πάρει για να ρίξει μία κακή σύνδεση τόσο όσο πόσο θα κρατήσει μία σύνδεση που έχει μείνει ανοικτή χωρίς δραστηριότητα.

```
# ftp gateway rules:
ftp-gw:             denial-msg      /usr/local/etc/ftp-deny.txt
ftp-gw:             welcome-msg     /usr/local/etc/ftp-welcome.txt
ftp-gw:             help-msg        /usr/local/etc/ftp-help.txt
ftp-gw:             timeout 300
ftp-gw:             permit-hosts 196.1.2.* -log { retr stor }
ftp-gw:             permit-hosts * -authall -log { retr stor }
```

Web, gopher και σε browser βασισμένο ftp είναι παραμορφωμένα από τη http-gw. Οι δύο πρώτες γραμμές δημιουργούν ένα κατάλογο για αποθήκευση των ftp και web κειμένων καθώς αυτά περνούν μέσα από το firewall. Έκανα αυτά τα αρχεία να ανοίκουν στον root και τα τοποθέτησα σε ένα κατάλογο προσβάσιμο μόνο από τον root.

Η σύνδεση Web οφείλεται να κρατηθεί μικρή. Ελέγχει πόσο ο χρήστης θα περιμένει σε μία κακή σύνδεση.

```
# www and gopher gateway rules:
http-gw:      userid          root
http-gw:      directory       /jail
http-gw:      timeout 90
http-gw:      default-httpd   www.afs.net
http-gw:      hosts           196.1.2.* -log { read write ftp }
http-gw:      deny-hosts      *
```

Το ssl-gw είναι πράγματι απλά μία διάβαση οποιασδήποτε πύλης. Προσέξτε με αυτό. Σε αυτό το παράδειγμα επιτρέπω στον καθένα από μέσα του προστατευόμενου δικτύου να συνδέεται σε κάθε διακομιστή έξω από το δίκτυο εκτός των διευθύνσεων 127.0.0.χχχ και 192.1.1.χχχ και μόνο στις πόρτες 443 έως 563. Οι πόρτες 443 έως 563 είναι γνωστές SSL πόρτες.

```
# ssl gateway rules:
ssl-gw:        timeout 300
ssl-gw:        hosts           196.1.2.* -dest { !127.0.0.* !192.1.1.* *:443:563 }
ssl-gw:        deny-hosts      *
```

Εδώ είναι ένα παράδειγμα στο πώς να χρησιμοποιήσετε το plug-gw για να επιτρέψετε συνδέσεις σε διακομιστές νέων. Σε αυτό το παράδειγμα επιτρέπω στο καθένα μέσα στο προστατεύομενο δίκτυο να συνδεθεί σε ένα μόνο σύστημα και μόνο στη πόρτα νέων του.

Η δεύτερη γραμμή επιτρέπει το διακομιστή νέων να περνά τα δεδομένα του πίσω στο προστατευόμενο δίκτυο.

Επειδή πολλοί πελάτες περιμένουν να στέκονται συνδεδεμένοι όσο ο χρήστης διαβάζει τα νέα, το timeout για διακομιστές νέων οφείλεται να είναι μεγάλο.

```
# NetNews Pluged gateway
plug-gw:       timeout 3600
plug-gw: port nntp 196.1.2.* -plug-to 199.5.175.22 -port nntp
plug-gw: port nntp 199.5.175.22 -plug-to 196.1.2.* -port nntp
```

Η πύλη finger είναι απλή. Ο καθένας μέσα στο προστατευόμενο δίκτυο πρέπει να κάνει login πρώτα και μετά επιτρέπουμε να χρησιμοποιήσουν το πρόγραμμα finger πάνω στο firewall. Όλοι οι άλλοι απλά πέρνουν ένα μήνυμα.

```
# Enable finger service
netacl-fingerd: permit-hosts 196.1.2.* -exec /usr/libexec/fingerd
netacl-fingerd: permit-hosts * -exec /bin/cat /usr/local/etc/finger.txt
```

Δεν έχω στήσει τις Mail και X-windows υπηρεσίες έτσι δεν περιλαμβάνω παραδείγματα. Εάν κάποιος έχει δουλέψει ένα παράδειγμα, παρακαλώ στείλτε μου email.

7.4.2 Το αρχείο inetd.conf

Εδώ είναι πλήρες ένα αρχείο /etc/inetd.conf. Όλες οι άχρηστες υπηρεσίες έχουν αφαιρεθεί ως σχόλια. Έχω συμπεριλάβει το πλήρες αρχείο για να δείξω τί να απενεργοποιήσετε, τόσο όσο το πώς να στήνετε τις νέες υπηρεσίες του firewall.

```
#echo stream  tcp  nowait  root       internal
#echo dgram   udp  wait    root       internal
#discard      stream  tcp  nowait  root       internal
#discard      dgram   udp  wait    root       internal
#daytime      stream  tcp  nowait  root       internal
#daytime      dgram   udp  wait    root       internal
#chargen      stream  tcp  nowait  root       internal
#chargen      dgram   udp  wait    root       internal
# FTP firewall gateway
ftp-gw      stream  tcp  nowait.400  root  /usr/local/etc/ftp-gw  ftp-gw
# Telnet firewall gateway
telnet        stream  tcp  nowait      root  /usr/local/etc/tn-gw /usr/local/etc/tn-gw
# local telnet services
telnet-a    stream  tcp  nowait      root  /usr/local/etc/netacl in.telnetd
# Gopher firewall gateway
gopher        stream  tcp  nowait.400  root  /usr/local/etc/http-gw /usr/local/etc/http-gw
# WWW firewall gateway
http  stream  tcp  nowait.400  root  /usr/local/etc/http-gw /usr/local/etc/http-gw
# SSL firewall gateway
ssl-gw  stream  tcp     nowait  root /usr/local/etc/ssl-gw   ssl-gw
# NetNews firewall proxy (using plug-gw)
nntp    stream  tcp     nowait  root    /usr/local/etc/plug-gw plug-gw nntp
#nntp stream  tcp     nowait  root    /usr/sbin/tcpd  in.nntpd
# SMTP (email) firewall gateway
#smtp stream  tcp     nowait  root    /usr/local/etc/smap smap
#
# Shell, login, exec and talk are BSD protocols.
#
#shell        stream  tcp     nowait  root    /usr/sbin/tcpd  in.rshd
#login        stream  tcp     nowait  root    /usr/sbin/tcpd  in.rlogind
#exec stream  tcp     nowait  root    /usr/sbin/tcpd  in.rexecd
#talk dgram   udp     wait    root    /usr/sbin/tcpd  in.talkd
#ntalk        dgram  udp     wait    root    /usr/sbin/tcpd  in.ntalkd
#dtalk        stream  tcp     waut    nobody  /usr/sbin/tcpd  in.dtalkd
#
# Pop and imap mail services et al
```

```
#
#pop-2   stream  tcp  nowait  root  /usr/sbin/tcpd    ipop2d
#pop-3   stream  tcp  nowait  root  /usr/sbin/tcpd    ipop3d
#imap    stream  tcp  nowait  root  /usr/sbin/tcpd    imapd
#
# The Internet UUCP service.
#
#uucp    stream  tcp  nowait  uucp  /usr/sbin/tcpd  /usr/lib/uucp/uucico -l
#
# Tftp service is provided primarily for booting.  Most sites
# run this only on machines acting as "boot servers." Do not uncomment
# this unless you *need* it.
#
#tftp dgram   udp     wait    root    /usr/sbin/tcpd  in.tftpd
#bootps       dgram   udp     wait    root    /usr/sbin/tcpd  bootpd
#
# Finger, systat and netstat give out user information which may be
# valuable to potential "system crackers."  Many sites choose to disable
# some or all of these services to improve security.
#
# cfinger is for GNU finger, which is currently not in use in RHS Linux
#
finger       stream  tcp  nowait  root   /usr/sbin/tcpd  in.fingerd
#cfinger     stream  tcp  nowait  root   /usr/sbin/tcpd  in.cfingerd
#systat      stream  tcp  nowait  guest  /usr/sbin/tcpd  /bin/ps -auwwx
#netstat     stream  tcp  nowait  guest  /usr/sbin/tcpd  /bin/netstat -f inet
#
# Time service is used for clock syncronization.
#
#time stream  tcp  nowait  root  /usr/sbin/tcpd  in.timed
#time dgram   udp  wait    root  /usr/sbin/tcpd  in.timed
#
# Authentication
#
auth         stream  tcp  wait    root  /usr/sbin/tcpd  in.identd -w -t120
authsrv      stream  tcp  nowait  root  /usr/local/etc/authsrv authsrv
#
# End of inetd.conf
```

7.4.3 Το αρχείο /etc/services

Εδώ είναι που ξεκινούν όλα. Όταν ένας πελάτης συνδεθεί στο firewall αυτό συνδέεται σε μία γνωστή πόρτα. (μικρότερη από 1024). π.χ. Το telnet συνδέεται στη πόρτα 23. Ο inetd δαίμονας ακούει αυτή τη σύνδεση και κοιτά το όνομα αυτής της υπηρεσίας στο αρχείο /etc/services. Αυτό τότε καλεί το πρόγραμμα ορισμένο για το όνομα στο μέσα στο αρχείο /etc/inetd.conf.

Κάποιες υπηρεσίες που δημιουργούμε δεν είναι κανονικά στο αρχείο /etc/sevices. Μπορείτε να ορίσετε μερικές από αυτές σε όποια πόρτα θέλετε. π.χ. Έχω ορίσει τη telnet πόρτα του διαχειριστή (telnet-a) στη πόρτα 24. Μπορείτε να το ορίσετε στη πόρτα 2323 εάν επιθυμήτε. Για το διαχειριστή (ΕΣΕΙΣ), για να συνδέεστε άμεσα στο firewall θα χρειάζεστε να κάνετε telnet στη πόρτα 24 και όχι 23 εάν στήσετε το αρχείο netperm-table, όπως εγώ έκανα, θα είστε ικανοί να το κάνετε αυτό μόνο από το εσωτερικό του προστατευόμενου δικτύου.

```
telnet-a        24/tcp
ftp-gw          21/tcp          # this named changed
auth            113/tcp   ident    # User Verification
ssl-gw          443/tcp
```

8 O SOCKS Διακομιστής Εξουσιοδότησης

8.1 Στήνοντας το Διακομιστή Εξουσιοδότησης

O SOCKS διακομιστής εξουσιοδότησης είναι διαθέσιμος από το **ftp://sunsite.unc.edu/pub/Linux/system/Network/misc/socks-linux- src.tgz**. Εκεί είναι και ένα παράδειγμα του αρχείου ρυθμίσεων (config file) που καλείται "socks-conf". Αποσυμπιέστε τα αρχεία μέσα σε κατάλογο του συστήματός σας, και ακολουθήστε τις οδηγίες πάνω στο πώς θα το φτιάξετε. Είχα μερικά προβλήματα όταν το έφτιαξα αυτό. Σιγουρευτήτε ότι τα Makefile αρχεία σας είναι εντάξει.

Ένα συμαντικό πράγμα για να σημειώσουμε είναι ότι ο διακομιστής εξουσιοδότησης χρειάζεται να προστεθεί στο αρχείο /etc/inetd.conf. Πρέπει να προσθέσετε τη γραμμή :

```
socks  stream  tcp  nowait  nobody  /usr/local/etc/sockd  sockd
```

για να πείτε στο διακομιστή να τρέξει όταν του ζητηθεί. to tell the server to run when requested.

8.2 Ρυθμίζοντας το Διακομιστή Εξουσιοδότησης.

Το πρόγραμμα SOCKS χρειάζεται δύο χωριστά αρχεία ρυθμίσεων. Ένα να λέει την επιτρεπόμενη πρόσβαση, και ένα για να δρομολογεί τις αιτήσεις στο κατάλληλο διακομιστή εξουσιοδότησης. Το αρχείο πρόσβασης πρέπει να βρίσκεται στο διακομιστή. Το αρχείο δρομολόγησης οφείλεται να βρίσκεται σε κάθε Un*x μηχάνημα. Οι DOS και, υποτιθέμενοι, Macintosh Υ/Η θα κάνουν δικές τους δρομολογήσεις.

8.2.1 Το Αρχείο Πρόσβασης

Με το socks4.2 Beta, το αρχείο πρόσβασης καλείται "sockd.conf". Αυτό οφείλει να περιέχει 2 γραμμές, μία γραμμή αδεία και μία αρνήσεως. Κάθε γραμμή θα έχει τρία πεδία:

- Τον Εξακριβωτή (Identifier) (permit/deny)
- Την IP διεύθυνση
- Το Τροποποιητή Διευθύνσεων

Ο εξακριβωτής είναι ή αδείας ή αρνήσεως. Οφείλετε να έχετε αμφότερα μία γραμμή αδείας και μία αρνήσεως.

Η IP διεύθυνση κρατά μία τεσσάρων byte διεύθυνση σε τυπική IP σημείωση κουκίδας. π.χ. 192.168.2.0.

Ο τροποποιητής διευθύνσεων είναι επίσης μία τυπική IP διεύθυνση τεσσάρων byte. Αυτό δουλεύει σαν μάσκα δικτύου (netmask). Οραματιστήτε αυτό τον αριθμό να είναι 32 bit (1 ή 0). Εάν το bit είναι 1, το αντίστοιχο bit από τη διεύθυνση που ελέγχετε πρέπει να είναι ίδιο με το αντίστοιχο bit μέσα στο πεδίο των IP διευθύνσεων. π.χ. εάν η γραμμή είναι:

```
permit 192.168.2.23 255.255.255.255
```

αυτό θα δίνει άδεια μόνο σε IP διευθύνσεις που ταιριάζουν σε κάθε bit μέσα 192.168.2.23, π.χ. μόνο 192.168.2.3. Η γραμμή:

```
permit 192.168.2.0 255.255.255.0
```

θα δώσει άδεια σε κάθε αριθμό μέσα στην ομάδα 192.168.2.0 έως 192.168.2.255, όλη η C κλάση περιοχή. Δεν πρέπει να έχετε τη γραμμή:

```
permit 192.168.2.0 0.0.0.0
```

επειδή αυτή δίνει άδεια σε κάθε διεύθυνση, αδιάφορο.

Έτσι, πρώτα δίνουμε άδεια σε όλες τις διευθύνσεις που θέλουμε να δώσουμε άδεια, και τότε απορρίπτουμε τις υπόλοιπες. Για να αφήσετε τους πάντες μέσα στη περιοχή 192.168.2.χχχ, οι γραμμές:

```
permit 192.168.2.0 255.255.255.0
deny 0.0.0.0 0.0.0.0
```

θα δουλέψουν καλά. Σημειώστε ότι το πρώτο "0.0.0.0" είναι η γραμμή αρνήσεως. Με έναν ένα τροποποιητή από 0.0.0.0, το πεδίο IP διεύθυνσης δεν πειράζει. Όλα τα 0 είναι κανόνας επειδή είναι εύκολα στη πληκτρολόγηση.

Περισσότερες από μία καταγραφές από το καθένα επιτρέπονται.

Συγκεκριμένοι χρήστες μπορούν επίσης να κερδίσουν ή να τους απαγορευτούν προσβάσεις. Αυτό γίνεται μέσω διαμόρφωσης της διαδικασίας επικύρωσης. Δεν το υποστηρίζουν όλα τα συστήματα τη διαμόρφωση, περιλαμβανόμενου του Trumpet Winsock, έτσι δεν θα αναφερθώ σε αυτό εδώ. Η τεκμηρίωση που περιέχει το socks είναι εντελώς επαρκής γι' αυτό το αντικείμενο.

8.2.2 Το αρχείο Δρομολόγησης.

Το αρχείο δρομολόγησης είναι φτωχά ονομασμένο στο SOCKS "socks.conf". Είπα "φτωχά ονομασμένο" επειδή είναι τόσο κοντά στο όνομα του αρχείο πρόσβασης που είναι εύκολο να τα μπερδέψετε.

Το αρχείο δρομολόγησης είναι εκεί για να λέει στους SOCKS πελάτες πότε να χρησιμοποιούν το socks και πότε όχι. π.χ. Στο δίκτυό μας, το 192.168.2.3 δεν θα χρειαστεί μα χρησιμοποιήσει το socks για να επικοινωνήσει με το 192.168.2.1, το firewall. Έχει άμεση σύνδεση μέσω του Ethernet. Αυτό καθορίζει το 127.0.0.1, τον επιστρεφόμενο βρόγχο (loopback), αυτόματα. Βεβαίως δεν χρειάζεστε το SOCKS για να επικοινωνήσετε με τον εαυτό σας. Υπάρχουν τρεις εισαγωγές:

- deny
- direct
- sockd

Η άρνηση (deny) λέει στο SOCKS πότε να απορρίπτει μία αίτηση. Αυτή η εισαγωγή έχει τα ίδια τρία πεδία όπως το sockd.conf, τον εξακριβωτή (identifier), διεύθυνση και τροποποιητή (modifier). Γενικά, επειδή αυτό χειρίζεται επίσης από το sockd.conf, το αρχείο πρόσβασης, το πεδίο του τροποποιητή είναι ορισμένο στο 0.0.0.0. Εάν θέλετε να προλογήσετε τον εαυτό σας στο να καλείτε από παντού, μπορείτε να το κάνετε εδώ.

Η direct εισαγωγή λέει για ποιές διευθύνσεις να μην χρησιμοποιήται το socks. Αυτές είναι όλες οι διευθύνσεις που μπορούν να προσεγγισθούν χωρίς το διακομιστή εξουσιοδότησης. Ξανά έχουμε τρία πεδία, εξακριβωτή, διεύθυνση και τροποποιητή. Το παράδειγμά μας θα έχει

```
direct 192.168.2.0 255.255.255.0
```

Έτσι μεταβαίνει άμεσα ο καθένας πάνω στο προστατευόμενο δίκτυο.

Η sockd εισαγωγή λέει στον Η/Υ ποιος host έχει τον socks διακομιστή δαίμονα πάνω του. Η σύνταξη είναι:

```
sockd @=<serverlist> <IP address> <modifier>
```

Σημειώστε τη @= εισαγωγή. Αυτή επιτρέπει να στήσετε τις IP διευθύνσεις από μια λίστα από διακομιστές εξουσιοδότησης. Στο παράδειγμά μας, χρησιμοποιούμε μόνο ένα διακομιστή εξουσιοδότησης. Αλλά, μπορείτε να έχετε αρκετούς για να επιτρέπετε μεγαλύτερα φορτία και για πλεόνασμα σε περίπτωση έλλειψης.

Τα πεδία IP διεύθυνση και τροποποιητής δουλεύουν σαν όλα τα άλλα παραδείγματα. Να καθορίζετε ποιές διευθύνσεις πηγαίνουν που μέσω από αυτά. The IP address and modifier fields work just like in the other examples. You specify which addresses go where through these.

8.2.3 DNS πίσω από το firewall. Στήνοντας την Όνομα Περιοχής Υπηρεσία (Domain Name Service) πίσω από firewall είναι ομολογουμένος εύκολο θέμα. Χρειάζεστε απλά και μόνο να στήσετε το DNS πάνω στο μηχάνημα που είναι ο firewall. Μετά, ορίστε σε κάθε μηχάνημα πίσω από το firewall να χρησιμοποιούν αυτή τ ο DNS.

8.3 Δουλεύοντας με Διακομιστή Εξουσιοδότησης.

8.3.1 Uniχ

Για να έχετε τις εφαρμογές σας να δουλεύουν με το διακομιστή εξουσιοδότησης, χρειάζονται να γίνουν "sockified". Θα χρειαστήτε δύο διαφορετικά telnet, ένα για άμεση επικοινωνία και ένα για επικοινωνία μέσω του διακομιστή εξουσιοδότησης. Το SOCS έρχεται με οδηγίες πάνω στο πώς να κάνετε SOCKify ένα πρόγραμμα, τόσο όσο και μερικά pre-SOCKified προγράμματα. Εάν χρησιμοποιήτε μία SOCKified έκδοση για να πάτε κάπου άμεσα, το SOCS αυτόματα θα αλλάξει στην άμεση έκδοση για εσάς. Επειδή γίνεται αυτό, θέλουμε να μετονομάσουμε όλα τα προγράμματα στο προσωπικό μας δίκτυο και να τα αντικαταστήσουμε με SOCKified προγράμματα. π.χ το "Finger" γίνεται "finger.orig", το "telnet" γίνεται "telnet.orig", κ.ο. Πρέπει να πείτε στο SOCKS σχετικά με αυτά μέσω του include/socks.h αρχείου.

Συγκεκριμένα προγράμματα θα χειρίζονται ρουτίνες και θα κάνουν sockify τον εαυτό τους. Το Netscape είναι ένα από αυτά. Μπορείτε να χρησιμοποιήτε διακομιστή εξουσιοδότησης κάτω από το Netscape εισάγοντας τη διεύθυνση του διακομιστή (192.168.2.1 στη περίπτωσή μας) μέσα στο πεδίο SOKCs κάτω από τα Proxies. Η κάθε εφαρμογή θα χρειαστεί λίγη τροφοδότηση, άσχετα από το πώς της χειρίζεται ο διακομιστή εξουσιοδότησης.

8.3.2 MS Windows με Trumpet Winsock

Το Trumpet Winsock έρχεται με ενσωματωμένες διακομιστή εξουσιοδότησης δυνατότητες. Μέσα στο μενού "εγκατάστασης (setup)", εισάγετε την IP διεύθυνση από το διακομιστή, και τις διευθύνσεις από όλους του Η/Υ που είναι συνδεδεμένοι άμεσα. Το Trumpet τότε θα χειριστεί όλα τα εξερχόμενα πακέτα.

8.3.3 Κάνοντας το Διακομιστή Εξουσιοδότησης να δουλεύει με UDP Πακέτα

Το πακέτο SOCKS δουλεύει μόνο με πακέτα TCP, και όχι UDP. Αυτό το κάνει λιγότερο χρήσιμο. Πολλά χρήσιμα προγράμματα, όπως το talk και το Archie, χρησιμοποιούν UDP. Υπάρχει ένα πακέτο σχεδιασμένο για να χρησιμοποιηθεί σαν διακομιστής εξουσιοδότησης για πακέτα UDP και καλείται UDPrelay, από τον Tom Fitzgerald <fitz@wang.com>. Δυστυχώς, τη στιγμή που γράφετε αυτό το HOWTO, δεν είναι συμβατό με το Linux.

8.4 Μειονεκτήματα με τους Διακομιστές Εξουσιοδότησης

Ο διακομιστής εξουσιοδότησης είναι, πάνω απ' όλα, μία **ασφαλής συσκευή**. Χρησιμοποιώντας τον για να αυξήσετε την πρόσβαση στο Internet με περιορισμένες IP διευθύνσεις θα έχετε πολλά μειονεκτήματα. Ένας διακομιστής εξουσιοδότησης θα επιτρέπει καλλίτερη πρόσβαση από το εσωτερικό του προστατευόμενου δικτύου προς τα έξω, αλλά θα κρατά το εσωτερικό απολύτως απρόσβαστο απ' έξω. Αυτό σημαίνει όχι διακομιστές, talk ή archie συνδέσεις, ή άμεσο ταχυδρομείο στους εσωτερικούς υπολογιστές. Αυτά τα μειονεκτήματα μπορεί να φαίνονται ασήμαντα, αλλά σκεφτήτε με αυτό το τρόπο:

- Έχετε αφήσει μία αναφορά που φτιάχνετε στο υπολογιστή σας μέσα σε ένα δίκτυο προστατευμένο με firewall. Είστε στο σπίτι, και αποφασίζετε ότι θέλετε να μεταβήτε σε αυτόν. Δεν μπορείτε. Δεν μπορείτε να προσεγγίσετε τον υπολογιστή σας επειδή είναι πίσω από το firewall. Προσπαθήτε να κάνετε log στο `firewall` πρώτα, αλλά από τότε που ο καθένας έχει διακομιστή εξουσιοδότησης πρόσβαση, κανένας δεν έχει εγκαταστήσει ένα λογαριασμό πάνω σε αυτόν για εσάς.
- Η κόρη σας πηγαίνει στο κολέγιο. Θέλετε να τις στέλνετε email. Έχετε κάποια προσωπικά πράγματα να συζητήσετε, και αναμφιβόλως έχετε το ταχυδρομείο σας να αποστέλεται κατευθείαν στο μηχάνημά σας. Εμπιστεύεστε το διαχειριστή του συστήματος απόλυτα, αλλά ακόμα, αυτό είναι προσωπικό mail.
- Η ανικανότητα να χρησιμοποιεί UDP πακέτα αντιπροσωπεύει ένα μεγάλο μειονέκτημα με τους διακομιστές εξουσιοδότησης. Οραματίζομαι τις δυνατότητες του UDP που έρχονται σύντομα.

Το FTP δημιουργεί άλλο ένα πρόβλημα με το διακομιστή εξουσιοδότησης. Όταν κατεβάζετε ή κάνετε `ls`, ο διακομιστής FTP ανοίγει μία υποδοχή στη μηχανή πελάτη και στέλνει τις πληροφορίες μέσω αυτής. Ο διακομιστής εξουσιοδότησης δεν θα το επιτρέψει αυτό, έτσι το FTP συγκεκριμένα δεν θα δουλέψει.

Και, οι διακομιστές εξουσιοδότησης είναι αργοί. Λόγω της καλλίτερης μεγάλης κάλυψης-ελέγχου (overhead), σχεδόν κάθε άλλο μέσο από το οποίο παίρνουμε αυτή τη πρόσβαση θα είναι ταχύτερο.

Βασικά, εάν έχετε τις IP διευθύνσεις, και δεν ανησυχήτε σχετικά με την ασφάλεια, μην χρησιμοποιείτε firewall και/ή διακομιστές εξουσιοδότησης. Εάν δεν έχετε τις IP διευθύνσεις, και επίσης δεν έχετε να ανησυχήτε για την ασφάλεια, μπορείτε επίσης να ρίξετε μία ματιά για να χρησιμοποιήσετε ένα εξομοιωτή IP, σαν τα Term, Slirp ή TIA. Το Term είναι διαθέσιμο από το `ftp://sunsite.unc.edu`, το Slirp είναι διαθέσιμο από το `ftp://blitzen.canberra.edu.au/pub/slirp`, και το TIA είναι διαθέσιμο από το marketplace.com. Αυτά τα πακέτα θα τρέχουν ταχύτερα, επιτρέπουν καλλίτερες συνδέσεις, και παρέχουν μεγάλου επιπέδου από πρόσβαση για το εσωτερικό του δικτύου από το Internet. Οι διακομιστές εξουσιοδότησης είναι καλοί για τα δίκτυα αυτά που έχουν πολλούς host που θα θέλουν να συνδέονται στο Internet "on the fly", με μία εγκατάσταση και λίγη δουλειά μετά.

9 Προηγμένες Μορφές

Υπάρχει μία μορφή που θα ήθελα να ασχοληθώ πριν κλείσω αυτή τη τεκμηρίωση. Αυτή μόλις τη σκιαγράφησα και πιθανώς θα ικανοποιήσει αρκετούς. Πάντως, σκέφτομαι ότι το επόμενο σκιαγράφημα θα δείξει περισσότερο προηγμένης μορφής από το να ξεκαθαρίσει κάποιες ερωτήσεις. Εάν έχετε ερωτήσεις πέρα από αυτές που μόλις κάλυψα, ή απλά ενδιαφέρεστε για την ευκαμψία των διακομιστών εξουσιοδότησης και των firewalls, συνεχίστε το διάβασμα.

9.1 Ένα μεγάλο δίκτυο με έμφαση στην ασφάλεια

Πείτε, για παράδειγμα, ότι είστε ο επικεφαλής παραστρατιωτικής οργάνωσης και θέλετε να δικτυώσετε τη θέση σας. Έχετε 50 Η/Υ και ένα υποδίκτυο από 32 IP αριθμούς των 5 στοιχείων (bits). Χρειάζεστε διαφορετικά επίπεδα πρόσβασης μέσα στο δίκτυό σας επειδή λέτε στους ακολούθους σας διαφορετικά πράγματα. Έτσι, θα χρειαστήτε να προστατεύσετε συγκεκριμένα τμήματα του δικτύου από το υπόλοιπο.

Τα επίπεδα είναι:

1. Το εξωτερικό επίπεδο. Αυτό το επίπεδο που δείχνετε στους πάντες. Εδώ είναι που φωνάζετε και παραλληλήτε για να πάρετε νέους εθελοντές.
2. **Στρατιωτικό** Εδώ είναι το επίπεδο από άτομα που έχουν περάσει πέρα από το εξωτερικό επίπεδο. Εδώ είναι που τους διδάσκετε σχετικά με την evail κυβέρνηση και στο πώς να φτιάχνουν βόμβες.
3. **Μισθοφόροι** Εδώ είναι που τα *πραγματικά* πλάνα κρατούνται. Σε αυτό το επίπεδο είναι αποθηκευμένες όλες οι πληροφοριές πάνω στο πώς η τριτοκοσμική κυβέρνηση πηγαίνει να κατακτήσει το κόσμο, τα πλάνα σας εμπλέκουν τις Newt Gingrish, Oklahoma City, lown ενδιαφέροντος προϊόντα και τί πραγματικά είναι αποθηκευμένο μέσα στα υπόστεγα τις περιοχής 51.

9.1.1 Η εγκατάσταση του δικτύου

Οι IP αριθμοί είναι κατανεμημένοι ως εξής:

- 1 αριθμός είναι 192.168.2.2555, που είναι η διεύθυνση εκπομπής και δεν χρησιμοποιείται
- 23 από τις 32 IP διευθύνσεις είναι τοποθετημένες στα 23 μηχανήματα που θα είναι προσβάσημα στο Internet.
- 1 επιπλέον IP πηγαίνει σε ένα κουτί linux σε αυτό το δίκτυο
- 1 επιπλέον πηγαίνει σε ένα διαφορετικό κουτί linux σε αυτό το δίκτυο.
- 2 IP αριθμοί πάνε στο δρομολογητή
- 4 αφέθηκαν στη πάντα, αλλά τους δόθηκαν τα τοπικά ονόματα paul, ringo, john, και george, απλά για να μπερδεύουν τα πράγματα λιγάκι.
- Τα προστατευόμενα δίκτυα αμφότερα έχουν διευθύνσεις 192.168.2.χχχ

Μετά, δύο χωριστά δίκτυα δημιουργήθηκαν, το καθένα σε διαφορετικά δωμάτια. Αυτά δρομολογήθηκαν μέσω υπέρυθρου Ethernet έτσι είναι απολύτως αόρατα στα εξωτερικά δωμάτια. Ευτυχώς, τα υπέρυθρα ethernet δουλεύουν σαν τα κανονικά ethernet.

Αυτά τα δίκτυα είναι το καθένα συνδεδεμένο με από ένα κουτί linux με μία επιπλέον IP διεύθυνση.

Υπάρχει ένας διακομιστής αρχείων (file server) που συνδέει τα δύο προστατευόμενα δίκτυα. Αυτό γίνεται επειδή για την κατάκτηση του κόσμου εμπλέκονται και υψηλότεροι στρατιώτες. Ο διακομιστής αρχείων κρατά την διεύθυνση 192.168.2.17 για το Στρατιωτικό δίκτυο και την 192.168.2.23 για το Μισθοφορικό δίκτυο. Αυτός έχει διαφορετικές IP διευθύνσεις επειδή έχει διαφορετικές κάρτες Ethernet. Το IP Forwarding πάνω σε αυτόν είναι κλειστό.

Το IP Forwarding είναι και στα δύο κουτιά linux επίσης κλειστό. Ο δρομολογητής δεν θα προωθεί πακέτα προορισμένα για 192.168.2.χχχ εκτός εάν δεν του δηλωθεί κατηγορηματικά να το κάνει, έτσι το Internet δεν θα είναι ικανό να μπεί μέσα. Ο λόγος που απενεργοποιήθηκε το IP Forwarding εδώ έγινε γιατί έτσι τα πακέτα από το δίκτυο των Στρατιωτών δεν θα είναι ικανά να προσεγγίσουν το Μισθοφορικό δίκτυο, και το ανάποδο.

Ο διακομιστής NFS μπορεί επίσης να οριστεί για να προσφέρει διαφορετικά αρχεία σε διαφορετικά δίκτυα. Αυτό γίνεται χειροκίνητα, και με λίγα τρυκ με τις συμβολικές συνδέσεις (symbolic links) μπορεί να γίνει έτσι ώστε τα κοινά αρχεία να μοιράζονται σε όλους. Χρησιμοποιώντας αυτό το στήσιμο και άλλη μία ethernet κάρτα μπορούμε να προσφέρουμε αυτό τον ένα διακομιστή αρχείων και για τα τρία δίκτυα.

9.1.2 Η εγκατάσταση των εξουσιοδότησεων

Τώρα, αφού και τα τρία επίπεδα θέλουν να είναι ικανά να συμβουλεύονται το δίκτυο για τους δικούς τους σκοτεινούς σκοπούς, και οι τρεις χρειάζονται να έχουν πρόσβαση στο Internet, έτσι δεν έχουμε να τα τροφοδοτήσουμε εδώ με διακομιστές εξουσιοδότησης. Τα Μισθοφορικό και Στρατιωτικό δίκτυα είναι πίσω από firewalls, έτσι είναι αναγκαίο να στήσουμε διακομιστές εξουσιοδότησης εκεί.

Αμφότερα τα δίκτυα θα έχουν εγκατασταθεί παρόμοια. Και τα δύο έχουν τις ίδιες IP διευθύνσεις τοποθετημένες επάνω τους. Θα πετάξω μερικές παραμέτρους, απλά για να κάνω τα πράγματα πιο ενδιαφέροντα.

1. Κανένας δεν μπορεί να χρησιμοποιεί το διακομιστή αρχείων για πρόσβαση στο Internet. Αυτή εκθέτει το διακομιστή αρχείων σε ιούς και άλλα δυσάρεστα πράγματα, και αυτό είναι κάπως σοβαρό, έτσι είναι εκτός των ορίων.

2. Δεν θα επιτρέπουμε πρόσβαση των στρατιωτών στο World Wide Web. Αυτοί είναι σε εκπαίδευση, και αυτής της φύσης οι πληροφορίες, ανάκτησης δύναμης, μπορεί να αποδειχθούν καταστροφικές.

Έτσι, το αρχείο sockd.conf στο κουτί linux των Στρατιωτών θα έχει αυτή τη γραμμή:

```
deny 192.168.2.17 255.255.255.255
```

και στον Μισθοφόρων το μηχάνημα:

```
deny 192.168.2.23 255.255.255.255
```

Και, το κουτί linux των Στρατιωτών θα έχει την εξής γραμμή:

```
deny 0.0.0.0 0.0.0.0 eq 80
```

Αυτή λέει να αρνηθεί πρόσβαση σε όλες τις μηχανές που προσπαθούν να αποκτήσουν πρόσβαση σε πόρτα ίση (equal) με 80, την http πόρτα. Αυτό ακόμα επιτρέπει όλες τις άλλες υπηρεσίες, απλά απαγορεύει Web πρόσβαση.

Μετά, αμφότερα τα αρχεία θα έχουν:

```
permit 192.168.2.0 255.255.255.0
```

για να επιτρέψετε σε όλους τους υπολογιστές πάνω στο 192.168.2.χχχ δίκτυο να χρησιμοποιούν αυτό το διακομιστή εξουσιοδότησης εκτός για αυτούς που τους έχει ήδη απαγορευτή. (π.χ ο διακομιστής αρχείων και η Web πρόσβαση από το δίκτυο των στρατιωτών.)

Το αρχείο sockd.conf των Στρατιωτών θα είναι κάπως έτσι:

```
deny 192.168.2.17 255.255.255.255
deny 0.0.0.0 0.0.0.0 eq 80
permit 192.168.2.0 255.255.255.0
```

και των Μισθοφόρων κάπως έτσι:

```
deny 192.168.2.23 255.255.255.255
permit 192.168.2.0 255.255.255.0
```

Αυτό οφείλει να έχει τα πάντα ρυθμισμένα σωστά. Κάθε δίκτυο είναι απομονωμένο ανάλογα, με τη σωστή ποσότητα αλληλεπίδρασης. Όλοι οφείλουν να είναι χαρούμενοι.

Τώρα, κατακτήστε το κόσμο!

Σημείωση του Μεταφραστή

Για οποιοδήποτε λάθος στη μετάφραση ζητώ να με συγχωρήσετε μιάς και παρόλο που έδωσα το καλλίτερο εαυτό μου σε μερικά σημεία δεν μπόρεσα να κάνω ακριβή μετάφραση. Σε μερικά σημεία υπάρχουν αγγλικές λέξεις που ήταν αδύνατο να τις μεταφράσω ούτε με τη βοήθεια λεξικών. Ελπίζω να δείξετε τη κατανόηση σας όπως επίσης και στα ορθογραφικά λάθη :-> Παρακαλώ όσους έχουν επισημάνει λάθη ή ανακρίβειες να τις σημειώσουν και να τις στείλουν είτε στη συντηρήτρια των ελληνικών HOWTO, Βούλα Σανιδά voulariba@hellug.gr, είτε σε εμένα προσωπικά. Οποιαδήποτε επιπλέον πληροφορία για τους firewalls που πιθανώς θα βοηθήσει στην εγκατάστασή τους, επικοινωνήστε με τη συντηρήτρια.

Παναγιώτης Τσακίρης mazestix@ath.forthnet.gr 26 Ιουνίου 1999