Κεφάλαιο 13. Έλεγχος πρόσβασης με Firewall

Σύνοψη
Στο τελευταίο αυτό κεφάλαιο, θα εξεταστούν ορισμένες τεχνολογίες ελέγχου πρόσβασης και οι δυνατότητες που παρέχουν για τη θωράκιση της περιμέτρου του συστήματος με τη χρήση ενός Τείχους Προστασίας (Firewall). Η εργαστηριακή δραστηριότητα θα επικεντρωθεί σε προσωπικά firewalls, τα οποία χρησιμοποιούνται για την προστασία ενός προσωπικού υπολογιστής από εξωτερικούς εισβολείς. Σε αυτό το πλαίσιο, θα εξεταστούν τα προϊόντα λογισμικού Windows Firewall σε περιβάλλον Windows Server, καθώς και το Netfilter/Iptables σε περιβάλλον Linux.

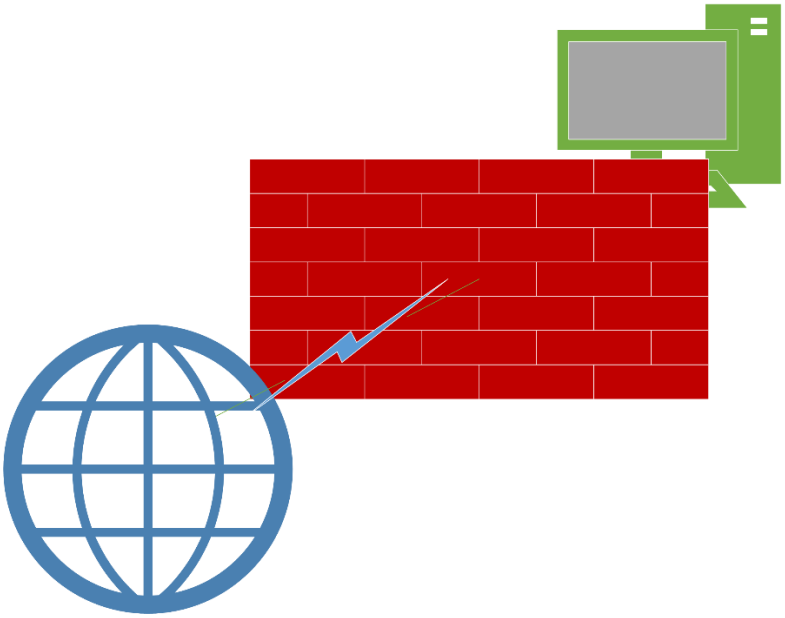
Προαπαιτούμενη γνώση
Για την ολοκλήρωση της Δραστηριότητας απαιτείται βασική γνώση δικτύων TCP/IP και δυνατότητα χρήσης των συστημάτων Windows και Linux που χρησιμοποιήθηκαν στα προηγούμενα κεφάλαια.

13.1 Εισαγωγή

Το τείχος προστασίας (firewall) χρησιμοποιείται για να διαχωρίσει δύο δίκτυα με διαφορετικό βαθμό εμπιστοσύνης, ελέγχοντας την κίνηση δεδομένων από το ένα δίκτυο στο άλλο. Τα firewalls μπορούν να διακριθούν σε δύο βασικές κατηγορίες:

- Τα δικτυακά (network firewalls), τα οποία συνήθως υλοποιούνται ως εξειδικευμένης χρήσης υπολογιστικά συστήματα (hardware και software) για να ελέγχουν το σύνολο της κίνησης μεταξύ δύο ή περισσότερων δικτύων.

- Τα προσωπικά (personal firewalls), τα οποία υλοποιούνται από ένα πρόγραμμα λογισμικού εγκατεστημένο σε έναν υπολογιστή γενικής χρήσης, το οποίο ελέγχει την κίνηση από και προς τον υπολογιστή, όπως αφαιρετικά παρουσιάζεται στο Σχήμα 13.1.



Εικόνα 13.1 *Διάταξη σύνδεσης στο διαδίκτυο με χρήση τείχους προστασίας*

Η αποτελεσματική λειτουργία ενός firewall βασίζεται στην πιστή τήρηση των τριών (3) βασικών αρχών που ακολουθούν:

- Όλη η κίνηση μεταξύ των δικτύων πρέπει να διέρχεται από το firewall.
- Μόνο η κίνηση που καθορίζεται από την πολιτική που εφαρμόζει το firewall επιτρέπεται να προωθείται.
- Η ασφάλεια του συστήματος firewall να είναι απαραβίαστη.

Τα firewalls, ανάλογα με την τεχνολογία την οποία υλοποιούν για τη λειτουργία τους, διακρίνονται στις ακόλουθες κατηγορίες:

- **Φιλτράρισμα πακέτων (Packet Filters)**
  Είναι το είδος του firewall που συναντάται πιο συχνά. Ένα packet filter συγκρίνει τη διερχόμενη κίνηση δεδομένων, ελέγχοντας τις κεφαλίδες του επιπέδου δικτύου και του επιπέδου μεταφοράς. Οι επικεφαλίδες αυτές εξετάζονται σε σχέση με ένα προκαθορισμένο σύνολο κανόνων, προκειμένου να ληφθεί μια απόφαση σχετικά με την αποδοχή (permit) ή την απαγόρευση (deny) της αιτούμενης κίνησης. Το σύνολο αυτό των κανόνων δημιουργεί μια λίστα, η οποία ονομάζεται λίστα ελέγχου πρόσβασης. Με βάση τον τρόπο λειτουργίας του packet filter, αυτό μπορεί να χαρακτηριστεί ως stateless ή stateful.

  - **Stateless Packet Filter**
    Σε ένα stateless packet filter ελέγχεται κάθε ένα πακέτο που εισέρχεται ή εξέρχεται από το σύστημα. Αυτό σημαίνει πως πρέπει να καθορίζονται κανόνες για το σύνολο της κίνησης, κάτι που δημιουργεί διαχειριστικό φόρτο. Ακόμη, δημιουργείται επιβάρυνση και στη λειτουργία του firewall, το οποίο πρέπει να ελέγχει ξεχωριστά κάθε ένα από τα πολλά πακέτα που διακινούνται.

  - **Stateful Packet Filter**
    Το stateful packet filter έχει την ικανότητα να τηρεί πίνακα με την κατάσταση (state) κάθε σύνδεσης. Όταν ξεκινά μια σύνδεση προς έναν άλλο κόμβο, το firewall καταχωρεί τη σύνδεση αυτή σε έναν πίνακα καταστάσεων (state table). Έτσι, για κάθε νέο εισερχόμενο ή εξερχόμενο από το δίκτυο πακέτο που φτάνει στο firewall, εφαρμόζονται τα ακόλουθα:
    - Αν το πακέτο αυτό ανήκει σε μια εδραιωμένη (established) επικοινωνία, η διέλευσή του επιτρέπεται.
    - Αν το πακέτο ξεκινά μια νέα σύνδεση (πακέτο τύπου SYN), δημιουργείται νέα εγγραφή στον πίνακα καταστάσεων.
    - Αν το πακέτο δεν ανήκει σε μια εδραιωμένη σύνδεση και δεν ξεκινά μια νέα σύνδεση (δεν είναι τύπου SYN), τότε απορρίπτεται.

- **Πύλες κυκλώματος (Circuit-level Gateways)**
  Οι πύλες κυκλώματος δεν ελέγχουν απλά τη ροή δεδομένων μεταξύ δύο ή περισσότερων συστημάτων, αλλά υλοποιούν συνδέσεις με κάθε ένα από αυτά, ενώ μέσω των συνδέσεων αυτών προωθείται η επιτρεπόμενη κίνηση από το ένα σύστημα στο άλλο.

- **Πύλες εφαρμογών (Application-level Gateways)**
  Οι πύλες εφαρμογών υλοποιούνται από πακέτα λογισμικού τα οποία αναλαμβάνουν να λειτουργήσουν ως πληρεξούσιοι (proxies) για κάθε υπηρεσία στην οποία αιτείται πρόσβαση ο χρήστης.

Στη συνέχεια, θα μελετηθεί η υλοποίηση ενός προσωπικού τείχους προστασίας, φιλτραρίσματος πακέτων, σε λειτουργικά συστήματα Windows και Linux. Πριν την εκκίνηση της εργαστηριακής

δραστηριότητας και για την αποφυγή απώλειας πρόσβασης στα συστήματα από λάθος χειρισμό, βεβαιωθείτε πως έχετε δυνατότητα σύνδεσης μέσω της κονσόλας του συστήματος (είτε τοπικά είτε μέσω της διεπαφής της υπηρεσίας Okeanos).

13.2 Προεργασία

Σε αυτή την εργαστηριακή δραστηριότητα, θα μελετηθούν οι δύο πιο διαδεδομένες λύσεις για την υλοποίηση προσωπικού firewall: το Windows Firewall και το Netfilter/Iptables, για λειτουργικά συστήματα Windows και Linux, αντίστοιχα. Για την επιτυχή ολοκλήρωση της δραστηριότητας, θα πρέπει οι μηχανές Windows και Linux που θα χρησιμοποιηθούν, να διασυνδεθούν με τέτοιο τρόπο ώστε να είναι εφικτός ο έλεγχος λειτουργίας του τείχους προστασίας.

Στις ακόλουθες παραγράφους, αναλύεται η διαδικασία σύνδεσης των μηχανών σε ένα νέο δίκτυο, με τη χρήση της υπηρεσίας Okeanos, αλλά και με τη χρήση του Oracle VirtualBox για τοπική εκτέλεση της εργαστηριακής δραστηριότητας.

13.2.1 Χρήση Υπηρεσίας Okeanos

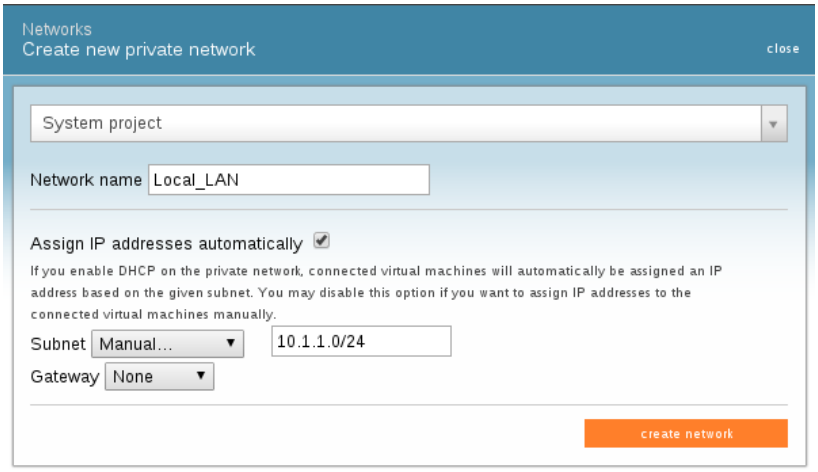
Η δημιουργία δικτύου στο περιβάλλον της υπηρεσίας Okeanos, γίνεται ως εξής:

- Από την κεντρική κονσόλα της εφαρμογής Cyclades, επιλέξτε το εικονίδιο των δικτύων (όπως φαίνεται στην Εικόνα 13.2) και επιλέξτε New Network.

Εικόνα 13.2 *Διαχείριση δικτύων*

- Στο παράθυρο διαλόγου που εμφανίζεται (Εικόνα 13.3), επιλέξτε αρχικά το project από το οποίο θα αντλήσετε πόρους (κατά κανόνα θα είναι ίδιο με αυτό που χρησιμοποιήσατε κατά τη δημιουργία των εικονικών μηχανών) και δώστε ένα όνομα στο δίκτυο (Network name).

- Επιλέξτε το checkbox «Assign IP Address Automatically», έτσι ώστε να αποδοθούν διευθύνσεις IP αυτόματα στις εικονικές μηχανές που θα συνδεθούν στο δίκτυο αυτό. Καθορίστε το Subnet που θα χρησιμοποιηθεί επιλέγοντας Manual και καταχωρώντας ως διεύθυνση υποδικτύου: 10.1.1.0/24. **Στην επιλογή Gateway επιλέξτε None.**



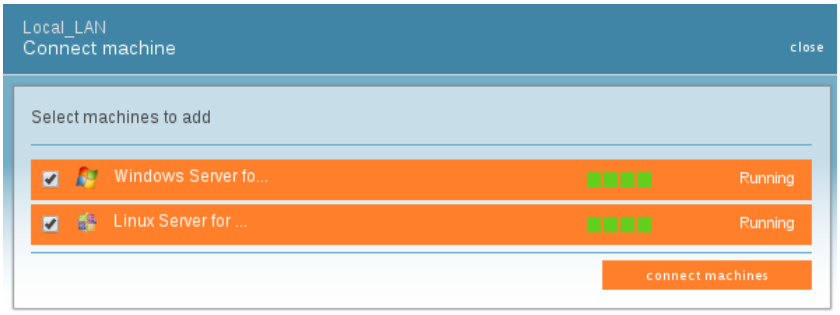
Εικόνα 13.3 *Δημιουργία δικτύου*

- Επιλέξτε «create network».

- Περνώντας τον κέρσορα του ποντικιού πάνω από το δίκτυο που έχει δημιουργηθεί (και προστεθεί στη σχετική λίστα), εμφανίζεται, μεταξύ άλλων, η επιλογή Connect machine (Εικόνα 13.4), την οποία και επιλέγετε.

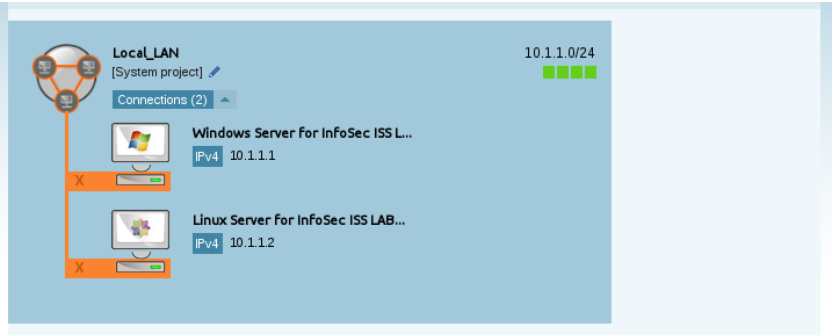
Εικόνα 13.4 *Επιλογή σύνδεσης μηχανών*

- Στο παράθυρο που θα εμφανιστεί, επιλέξτε και τις δύο εικονικές μηχανές που δημιουργήσατε για τις ανάγκες των εργαστηριακών δραστηριοτήτων του παρόντος βιβλίου και πατήστε connect machines, όπως φαίνεται στην Εικόνα 13.5.



Εικόνα 13.5 *Σύνδεση των 2 εικονικών μηχανών*

- Τέλος, μπορείτε να δείτε τις διευθύνσεις IPv4 που έχουν εκχωρηθεί σε κάθε μηχανή, αν επιλέξετε Connections. Στην Εικόνα 13.6, φαίνεται ότι στη μηχανή Windows έχει εκχωρηθεί η διεύθυνση 10.1.1.1 και στη μηχανή Linux η διεύθυνση 10.1.1.2.

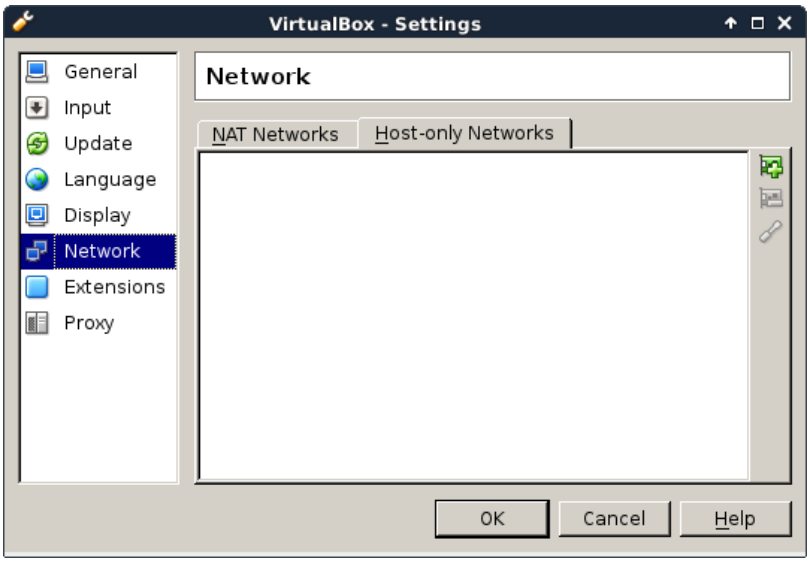


Εικόνα 13.6 *Εκχωρημένες διευθύνσεις IPv4 ανά μηχανή*

13.2.2 Χρήση Τοπικού Hypervisor

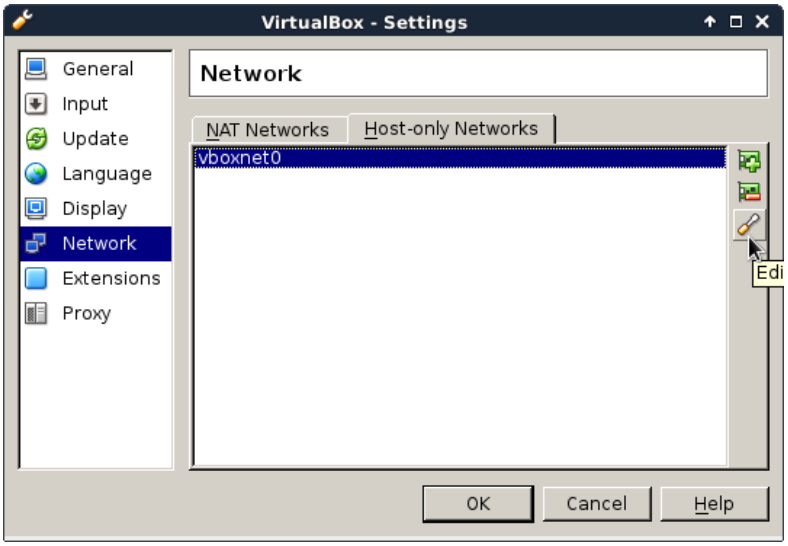
Στον τοπικό hypervisor VirtualBox, θα δημιουργήσουμε ένα Host-only network. Αυτό το είδος του εικονικού δικτύου, επιτρέπει την επικοινωνία μεταξύ των μηχανών τις οποίες διασυνδέει, καθώς και την επικοινωνία τους με τον host.

Για να δημιουργηθεί το δίκτυο, ανοίγουμε το VirtualBox και πατάμε Ctrl + G ή από το μενού File επιλέγουμε Preferences. Με τον τρόπο αυτό, ανοίγει το παράθυρο ρυθμίσεων, στο οποίο επιλέγουμε την επιλογή Network (από το αριστερό πλαίσιο) και στη συνέχεια την καρτέλα Host-only Networks, όπως φαίνεται στην Εικόνα 13.7.



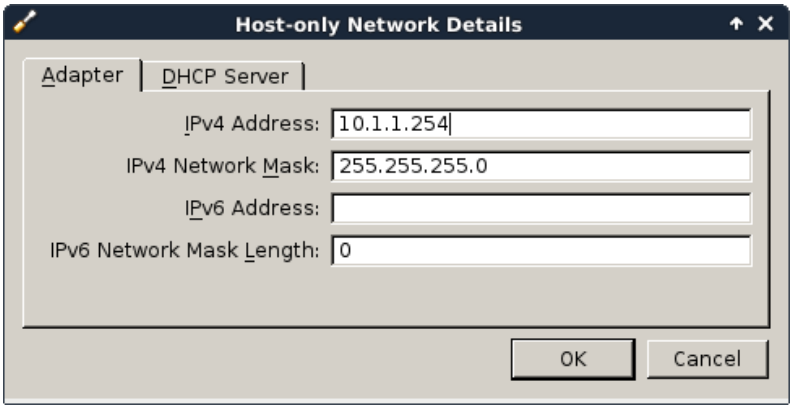
Εικόνα 13.7 *Ρυθμίσεις δικτύων*

Στη συνέχεια επιλέγουμε το κουμπί προσθήκης δικτύου ώστε να προστεθεί ένα νέο δίκτυο (vboxnet0, αν δεν υπάρχει κάποιο προηγούμενο). Επιλέγουμε το νέο δίκτυο και πατάμε το κουμπί διαμόρφωσης ρυθμίσεων που έχει εμφανιστεί δεξιά με το σχήμα κατσαβιδιού.



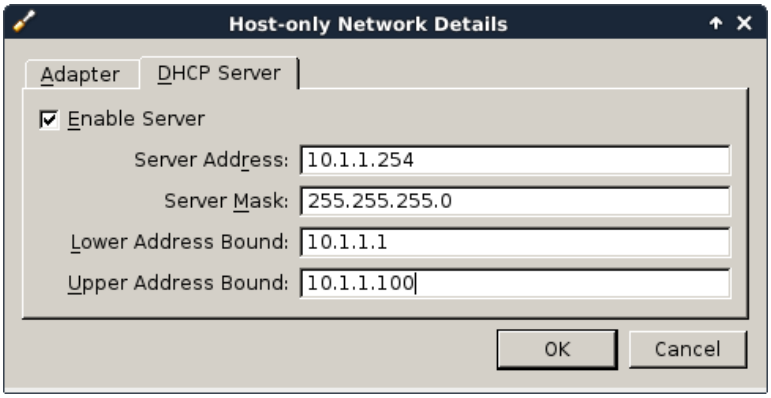
Εικόνα 13.8 *Επιλογή ρυθμίσεων νέου δικτύου*

Εμφανίζεται ένα νέο παράθυρο με δύο καρτέλες. Στην πρώτη καρτέλα ορίζεται η διεύθυνση IPv4 του εικονικού προσαρμογέα της host μηχανής, στην οποία εκτελείται ο hypervisor. Καταχωρείστε τη διεύθυνση 10.1.1.254 με μάσκα υποδικτύου (IPv4 Network Mask) 255.255.255.0.



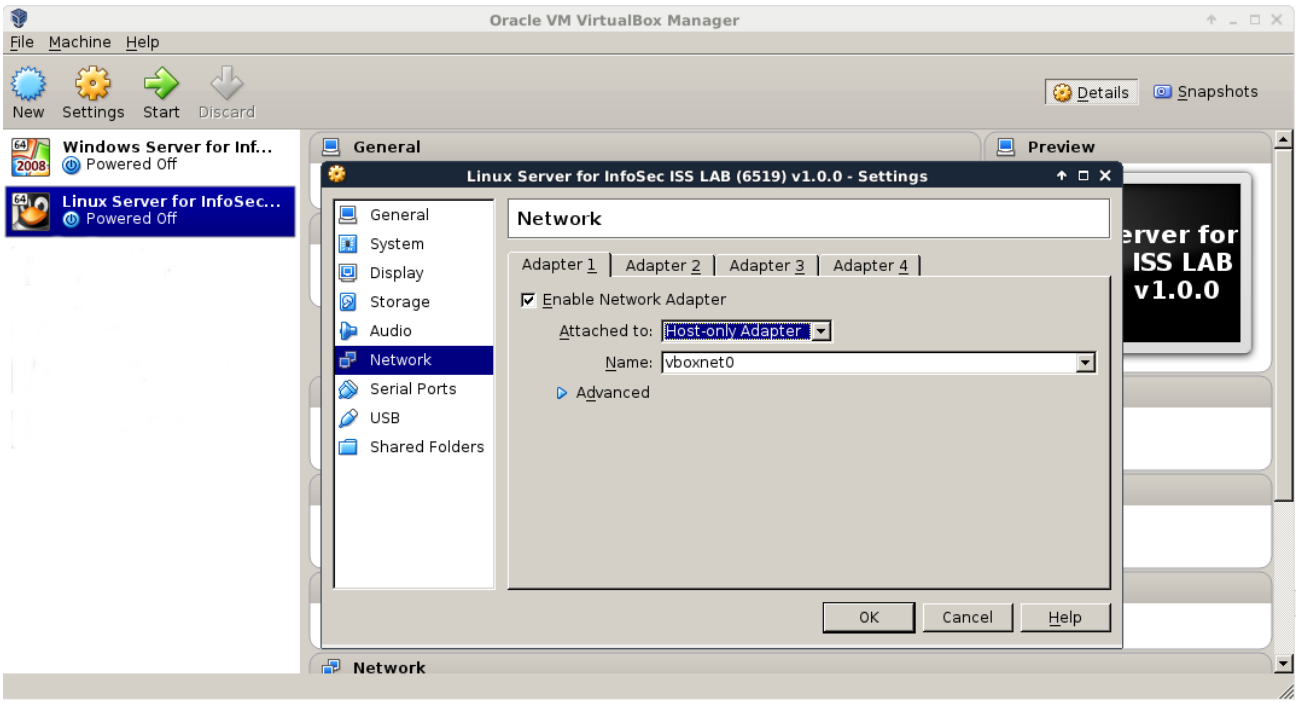
Εικόνα 13.9 *Ορισμός διεύθυνσης host adapter*

Στη δεύτερη καρτέλα, ορίζονται οι ιδιότητες του διακομιστή διευθυνσιοδότησης (DHCP Server). Καταχωρείστε τη διεύθυνση διακομιστή (Server Address) 10.1.1.254, με μάσκα (Server Mask) 255.255.255.0 και ένα διάστημα διευθύνσεων που ορίζεται από το κάτω όριο (Lower Address Bound) 10.1.1.1 και το άνω όριο (Upper Address Bound) 10.1.1.100, όπως φαίνεται στην Εικόνα 13.10.



Εικόνα 13.10 *Ορισμός ιδιοτήτων DHCP Server*

Τέλος, για να συνδεθούν οι εικονικές μηχανές με το δίκτυο, επιλέγουμε την κάθε μηχανή ξεχωριστά (στο αριστερό πλαίσιο) και στη συνέχεια το εικονίδιο Settings από τη γραμμή εργαλείων ή από το μενού Machine ή κάνοντας δεξί κλικ πάνω στο όνομά της. Στο παράθυρο ρυθμίσεων που εμφανίζεται, επιλέγουμε από αριστερά Network και συνδέουμε (attach) τον εικονικό προσαρμογέα δικτύου (Network Adapter) με το Host-only Adapter που δημιουργήσαμε προηγουμένως, όπως φαίνεται στην Εικόνα 13.11.



Εικόνα 13.11 *Σύνδεση μηχανών με το Host-only Adapter.*

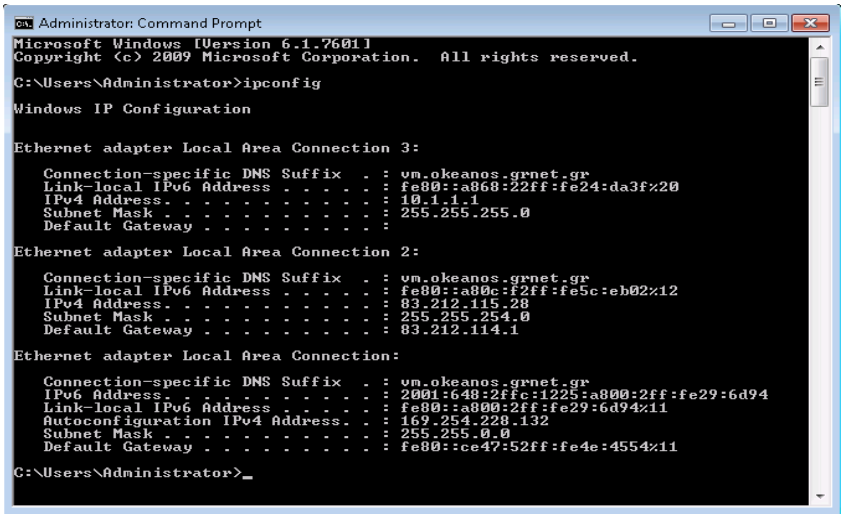
13.3 Τείχος Προστασίας σε Λ.Σ. Windows

Στο λειτουργικό σύστημα Windows, υλοποιείται ένα προσωπικό stateful packet filter για το οποίο υπάρχουν δύο διαφορετικοί τρόποι παραμετροποίησης:

- Το Windows Firewall που βρίσκεται στον Πίνακα Ελέγχου (Control Panel) και το οποίο ο κατασκευαστής προτείνει να χρησιμοποιείται σε οικιακά περιβάλλοντα.

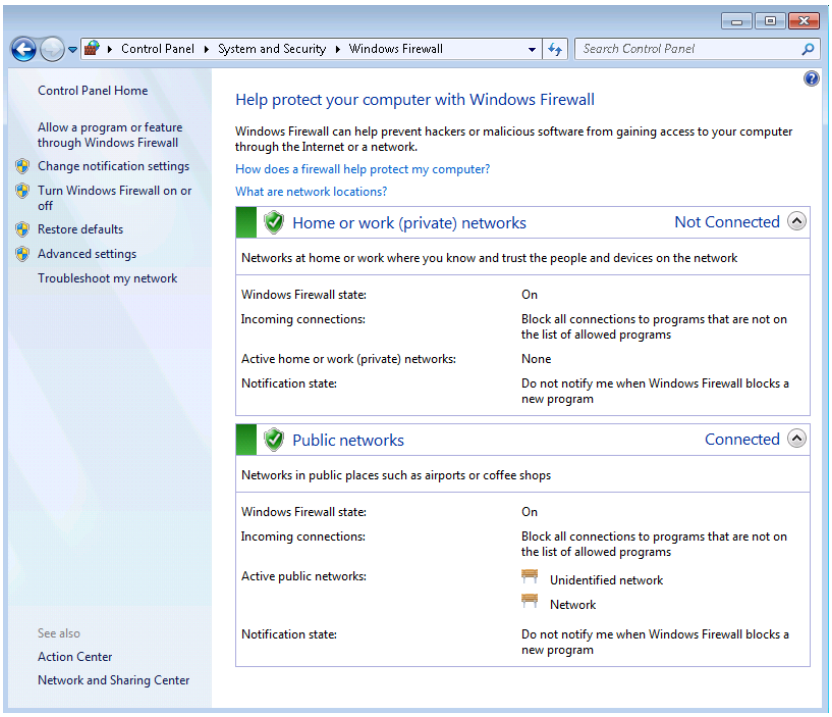
- Το Windows Firewall with Advanced Security, το οποίο προτείνεται να χρησιμοποιείται από χρήστες σε επιχειρησιακά περιβάλλοντα.

Συνδεόμαστε με το σύστημα Windows και εντοπίζουμε τη νέα δικτυακή διεπαφή που δημιουργήθηκε στο προηγούμενο βήμα, εκτελώντας την εντολή ipconfig. Καταγράφουμε τη σύνδεση δικτύου με IPv4 διεύθυνση που ανήκει στο υποδίκτυο 10.1.1.0/24. Σύμφωνα με τα περιεχόμενα της Εικόνας 13.12, η σύνδεση αυτή είναι η «Local Area Connection 3» με διεύθυνση IPv4: 10.1.1.1.



Εικόνα 13.12 *Εντοπισμός σύνδεσης*

Από τον πίνακα ελέγχου (Start → Control Panel) επιλέξτε System and Security και, στη συνέχεια, Windows Firewall, ώστε να ανοίξει το παράθυρο με την αρχική οθόνη του Windows Firewall, όπως φαίνεται στην Εικόνα 13.13.

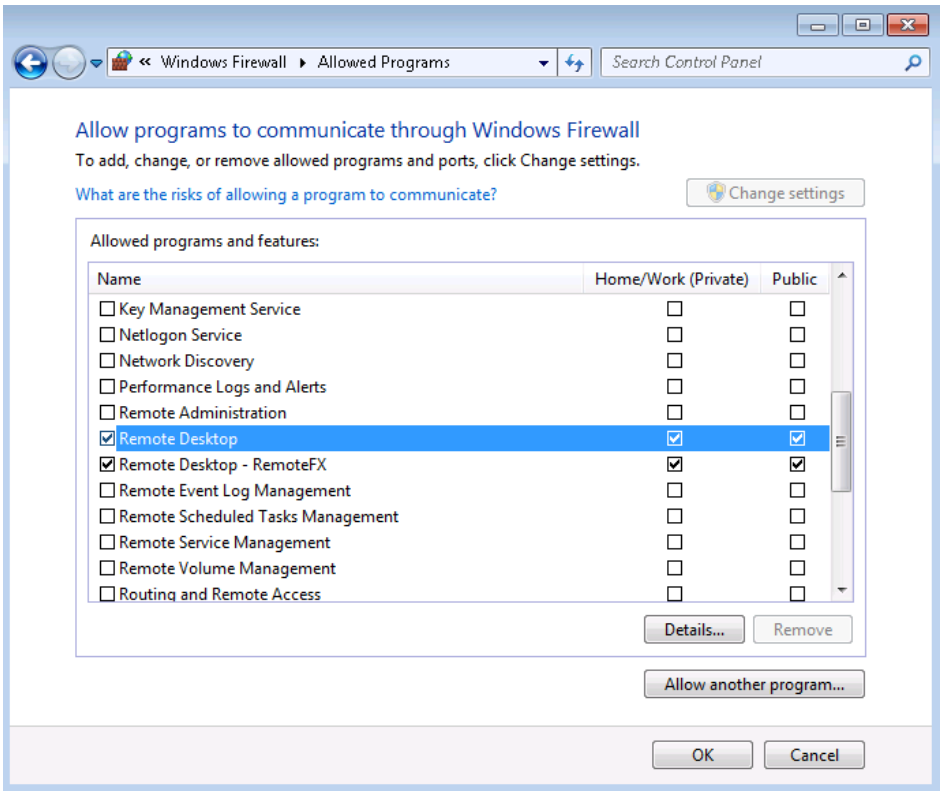


Εικόνα 13.13 *Windows Firewall*

Παρατηρήστε πως υπάρχει ένας διαχωρισμός των δικτύων σε private (ιδιωτικά) και public (δημόσια). Με τον τρόπο αυτό, το Windows firewall μπορεί να καθορίσει τη συμπεριφορά του, ανάλογα με τη σύνδεση από την οποία μεταφέρονται τα δεδομένα πάνω στα οποία εφαρμόζει τους κανόνες που θέτει ο χρήστης.

Θεωρείτε πως ο διαχωρισμός αυτός προσφέρει κάτι χρήσιμο στο χρήστη; Αν δεν υπήρχε ένας τέτοιος διαχωρισμός, τι πρόβλημα θα υπήρχε; Τελικά, ποια δίκτυα είναι ιδιωτικά και ποια είναι δημόσια;

Παρατηρήστε τις επιλογές στο αριστερό μέρος και επιλέξτε «Allow a program or feature through Windows Firewall». Στο παράθυρο που θα ανοίξει (Εικόνα 13.14), μπορείτε να παρατηρήσετε πως υπάρχει η δυνατότητα επιλογής εφαρμογών ή υπηρεσιών του συστήματος που είναι προσβάσιμες δικτυακά, όπως για παράδειγμα το Remote Desktop Connection που χρησιμοποιούμε για την απομακρυσμένη μας σύνδεση. Επίσης, υπάρχει η δυνατότητα προσθήκης νέας εφαρμογής.

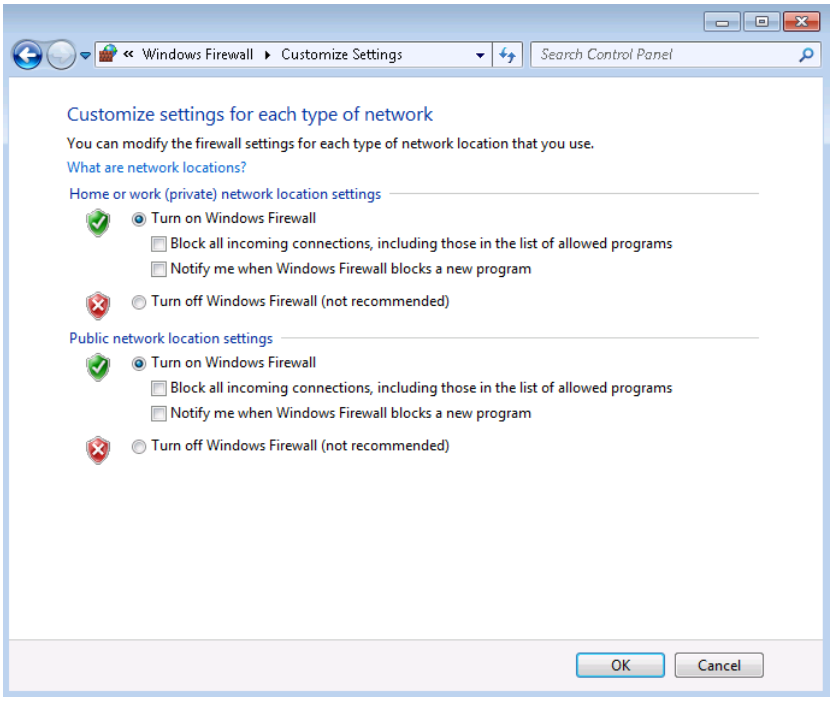


Εικόνα 13.14 *Εφαρμογές που επικοινωνούν μέσω του windows firewall*

Χωρίς να κάνετε κάποια αλλαγή, πατήστε Cancel και στη συνέχεια (από την προηγούμενη οθόνη) επιλέξτε «Turn Windows Firewall on or off».

Παρατηρήστε πως έχετε τη δυνατότητα να ενεργοποιήσετε ή απενεργοποιήσετε το τείχος προστασίας ή μεμονωμένες υπηρεσίες για τα ιδιωτικά (private) ή δημόσια (public) δίκτυα, καθώς και να επιλέξετε να λαμβάνετε ειδοποιήσεις όταν το τείχος προστασίας απαγορεύει μια σύνδεση και να απαγορεύσετε κάθε εισερχόμενη σύνδεση, ακόμη και από τις εφαρμογές που βρίσκονται στη λίστα των επιτρεπόμενων εφαρμογών.

Ποια η χρησιμότητα αυτών των επιλογών; Από τις επιλογές αυτές και μόνο, μπορείτε να εικάσετε αν το Windows Firewall είναι stateful ή stateless packet filter;

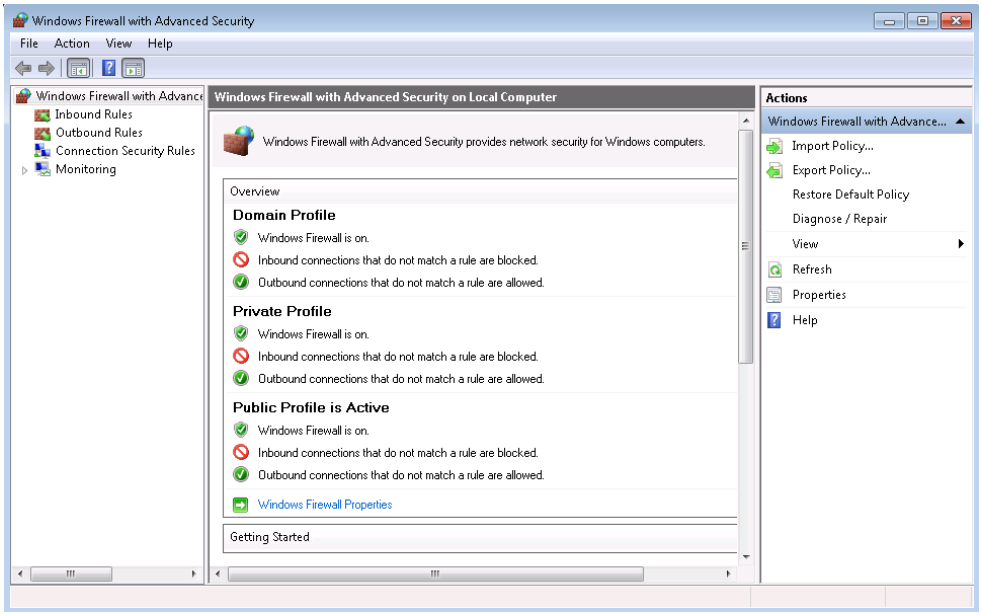


Εικόνα 13.15 *Παραμετροποίηση του Windows Firewall*

Το Windows Firewall, όπως φαίνεται στην Εικόνα 13.15, έχει περιορισμένες δυνατότητες παραμετροποίησης. Σε κανένα σημείο δεν υπάρχει τρόπος για να καθορίσετε ρυθμίσεις που έχουν επιμέρους σχέση με πρωτόκολλο επιπέδου μεταφοράς ή διευθύνσεις δικτύου.

Για να έχετε τη δυνατότητα να καθορίσετε τέτοιους κανόνες φιλτραρίσματος, επιλέγετε από την αρχική οθόνη του Windows Firewall, την επιλογή Advanced Settings, η οποία θα εκκινήσει το Windows Firewall with Advanced Security (μπορείτε να το εκκινήσετε κατευθείαν από το Λ.Σ. Windows εκτελώντας διαδοχικά: Start → Run → fw.msc).

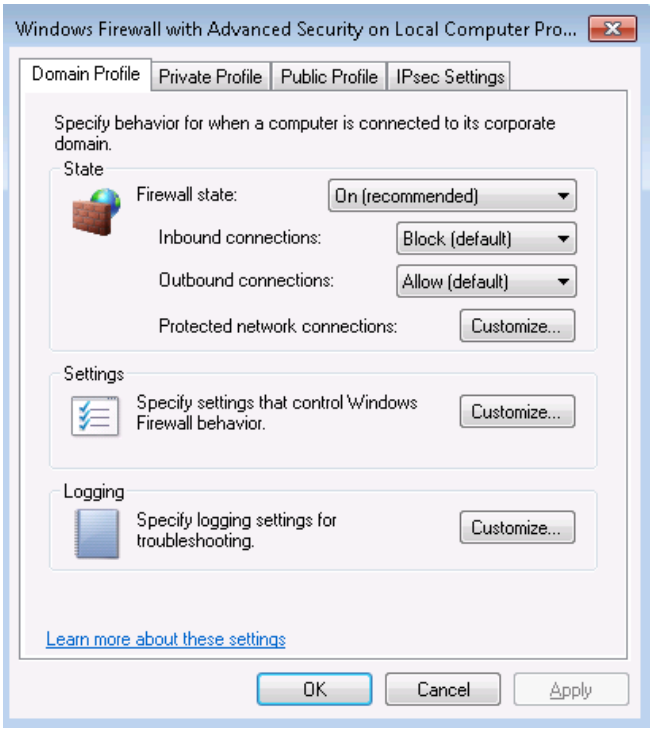
Η αρχική κονσόλα διαχείρισης του Windows Firewall with Advanced Security, όπως φαίνεται στην Εικόνα 13.16, δείχνει πως το τείχος προστασίας διέπεται από τρία (3) προφίλ: τα private και public, όπως είδαμε και στο απλό Windows Firewall, καθώς και το domain, το οποίο αφορά τη σύνδεση δικτύου μέσω της οποίας ο server συμμετέχει σε έναν τομέα Windows (Windows Domain). Η λεπτομέρεια αυτή δεν είναι σημαντική για την κατανόηση της λειτουργίας του firewall (μπορείτε να αναζητήσετε περισσότερες πληροφορίες για το Windows Domain στο Διαδίκτυο).



Εικόνα 13.16 *Windows Firewall with Advanced Security*

Επιλέγοντας Windows Firewall Properties στο τέλος του πλαισίου Overview, μπορείτε επιλέγοντας το κουμπί Customize (που αφορά την επιλογή «Protected network Connections») να καθορίσετε:

- τη λειτουργία του firewall για κάθε προφίλ,
- τη συμπεριφορά του για εισερχόμενες και εξερχόμενες συνδέσεις,
- ποιες συνδέσεις δικτύου ανήκουν σε κάθε προφίλ.



Εικόνα 13.17 *Ιδιότητες προφίλ Windows Firewall with Advanced Security*

Μια ιδιαίτερα χρήσιμη δυνατότητα του Windows Firewall with Advanced Security είναι ο καθορισμός κανόνων για την εισερχόμενη και εξερχόμενη κίνηση. Ο κατασκευαστής έχει ήδη εγκαταστήσει ένα σύνολο προκαθορισμένων κανόνων, στους οποίους έχουμε πρόσβαση επιλέγοντας από το αριστερό μέρος της αρχικής οθόνης Inbound και Outbound rules (Εικόνα 13.16).

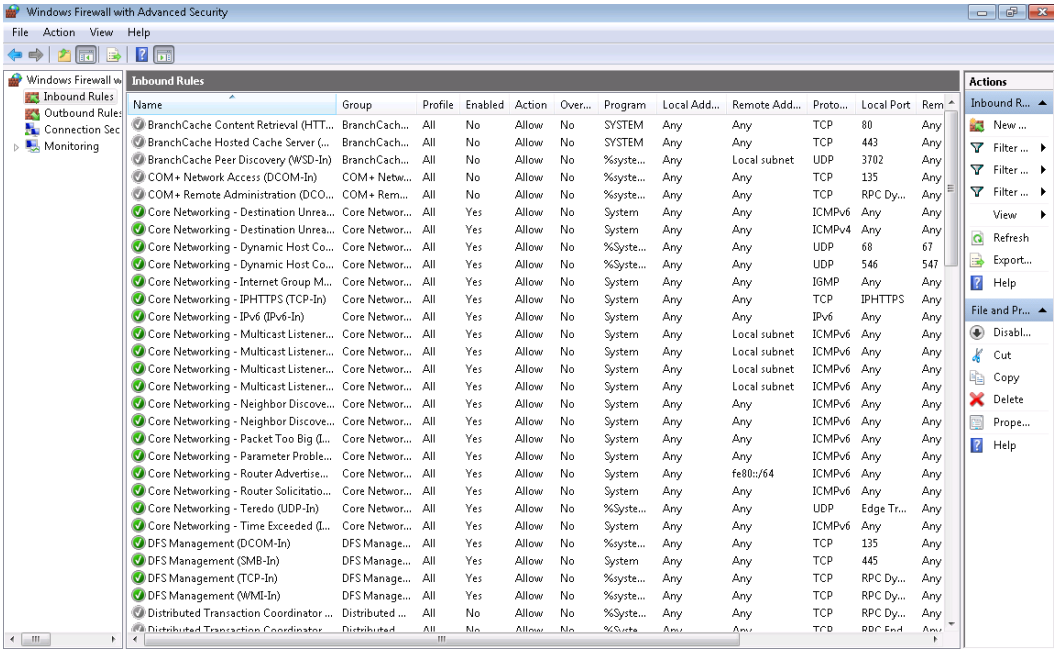
Στη συνέχεια, θα ελέγξουμε τους προκαθορισμένους αυτούς κανόνες και θα ενεργοποιήσουμε έναν Web server για τον οποίο θα καθορίσουμε τους απαραίτητους κανόνες πρόσβασης, έτσι ώστε να είναι προσβάσιμος μέσω του τείχους προστασίας από συγκεκριμένους μόνο χρήστες.

13.3.1 Έλεγχος Προεπιλεγμένων Κανόνων

Στην αρχική οθόνη του Windows Firewall with Advanced Security, επιλέξτε από το αριστερό πλαίσιο Inbound Rules. Στο κεντρικό πλαίσιο θα εμφανιστεί το σύνολο των κανόνων του packet filter που αφορούν τις συνδέσεις οι οποίες εκκινούν από τον έξω κόσμο με προορισμό το συγκεκριμένο μηχάνημα.

Παρατηρούμε ότι κάθε κανόνας αποτελείται από:

- Ένα χαρακτηριστικό όνομα (Name).
- Μια ομάδα στην οποία ανήκει (Group).
- Το προφίλ για το οποίο ισχύει (Profile).
- Το κατά πόσον είναι ενεργός ή όχι (Enabled).
- Την ενέργεια που εκτελεί το packet filter σε περίπτωση ικανοποίησης του κανόνα (Action)
- Εάν υπερισχύει (Override) ενός αντίστοιχου block κανόνα. Στο Windows Firewall, οι block κανόνες έχουν πάντα προτεραιότητα, εκτός αν υπάρχει αντίστοιχος override κανόνας.
- Την εφαρμογή για την οποία ισχύει ο κανόνας (Program).
- Την τοπική (Local) και την απομακρυσμένη (Remote) διεύθυνση (Address).
- Το δικτυακό πρωτόκολλο (Protocol).
- Την τοπική (Local) και την απομακρυσμένη (Remote) θύρα (Port).
- Τους χρήστες και υπολογιστές για τους οποίους ισχύει ο κανόνας (Allowed Users και Allowed Computers).

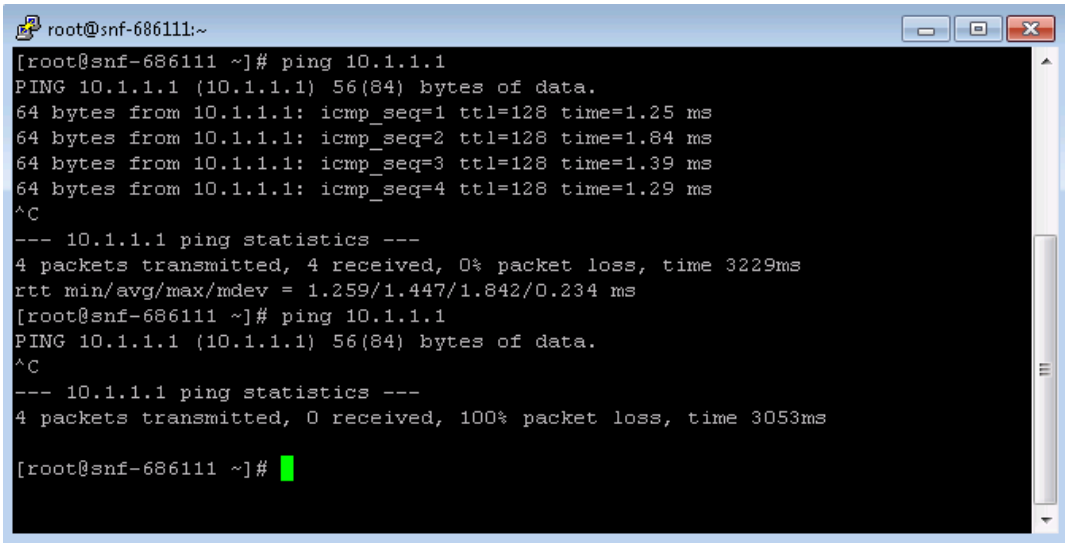


Εικόνα 13.18 *Προεπιλεγμένοι κανόνες εισερχόμενης κίνησης*

Συνδεθείτε με τη Linux μηχανή και χρησιμοποιήστε το τοπικό δίκτυο που δημιουργήσατε για να αποστείλετε ICMP πακέτα τύπου echo request στη Windows μηχανή με τη χρήση της εντολής ping, όπως φαίνεται στην Εικόνα 13.19. Λαμβάνετε απαντήσεις (echo reply);

Στη συνέχεια, εντοπίστε στο Windows Firewall τον inbound rule με όνομα «File and Printer Sharing (Echo Request - ICMPv4-In)» και απενεργοποιήστε τον κάνοντας δεξί κλικ επάνω του και επιλέγοντας Disable Rule.

Δοκιμάστε εκ νέου να στείλετε echo requests. Λαμβάνετε απάντηση; Αφού κατανοήσετε τι και γιατί συμβαίνει, ενεργοποιήστε (enable) εκ νέου τον κανόνα.



Εικόνα 13.19 *Έλεγχος λειτουργίας firewall με χρήση ICMP echo requests*

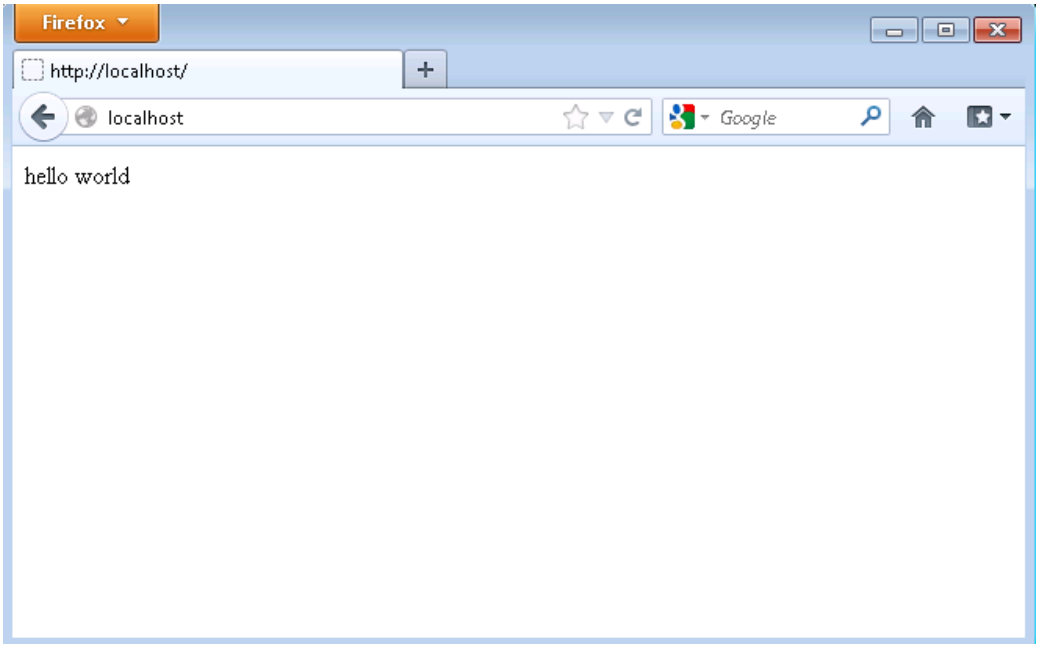
Στην περίπτωση που επιθυμούσατε να επιτρέψετε τα εισερχόμενα echo requests και επίσης ο server σας να απαντούσε κανονικά (echo reply), αλλά κανείς χρήστης από το server σας να μη μπορούσε να αποστείλει echo request προς οπουδήποτε, τι θα μπορούσατε να κάνετε, πέρα από το να τους το απαγορεύσετε με μια ρητή προφορική ή γραπτή οδηγία;

13.3.2 Ενεργοποίηση Web Server

Στη συνέχεια, θα ενεργοποιήσουμε ένα Web server, δηλαδή μια υπηρεσία που θα έχει τη δυνατότητα να παρουσιάζει ιστοσελίδες στους πελάτες. Εκτελέστε τις παρακάτω ενέργειες:

- Δημιουργήστε μέσα στο ριζικό κατάλογο του δίσκου C: ένα κατάλογο (directory) με όνομα tiny.
- Δημιουργήστε ένα αρχείο με όνομα index.html και περιεχόμενο τη φράση hello world.
- Κατεβάστε το αρχείο:
  - http://infosec.uom.gr/Study/LAB/ISS/6519/tiny.zip
- Αποσυμπιέστε το και αποθηκεύστε το στον κατάλογο C:\tiny.
- Εκτελέστε το αρχείο αυτό:
  - C:\tiny\tiny c:\tiny

Ανοίξτε ένα browser και δώστε τη διεύθυνση http://localhost για να σας επιστραφεί μια κατάσταση όπως αυτή που φαίνεται στην Εικόνα 13.20.



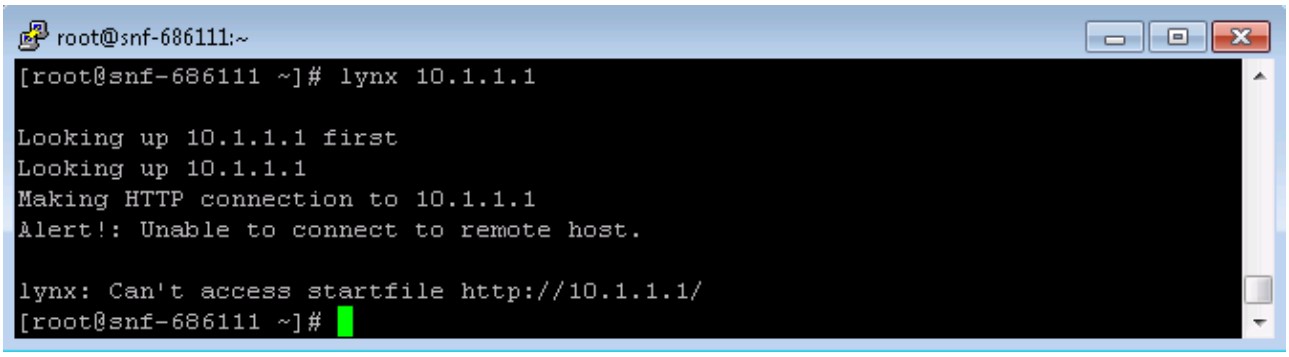
Εικόνα 13.20 *Ο Web server λειτουργεί*

13.3.3 Σύνδεση από τη Μηχανή Linux

Συνδεθείτε στη μηχανή Linux και εκτελέστε την ακόλουθη εντολή (για τον command line browser Lynx):

```
lynx http://10.1.1.1
```

Σε αυτή την εντολή αντικαταστήστε, αν χρειαστεί, τη διεύθυνση IP 10.1.1.1 με τη διεύθυνση IP της Windows μηχανής. Μπορέσατε να δείτε το Hello world; Αν όχι, τότε βλέπετε την κατάσταση που φαίνεται στην Εικόνα 13.21.



Εικόνα 13.21 *Προσπάθεια πρόσβασης στην ιστοσελίδα*

Θυμίζουμε πως ο Web server εκτελείται στη θύρα 80, χρησιμοποιώντας το πρωτόκολλο TCP. Έστω ότι επιθυμούμε η πρόσβαση να είναι δυνατή μόνο από το δίκτυο 10.1.1.0/24.

- Στη μηχανή Windows και συγκεκριμένα στο παράθυρο του Windows Firewall with Advanced Security, κάντε δεξί κλικ στο Inbound Rules και επιλέξτε New Rule. Αρχικά, θα σας ζητηθεί το είδος του κανόνα. Αν, δηλαδή, αφορά ένα συγκεκριμένο πρόγραμμα (Program), μια συγκεκριμένη θύρα (Port), αν ακολουθεί κάποιες προεπιλογές (Predefined), ή αν είναι ένας προσαρμοσμένος κανόνας (Custom).

- Επιλέγετε Custom και, στη συνέχεια, πατάτε Next.

- Επειδή ο κανόνας που θέλουμε να θέσουμε δεν αφορά κάποιο πρόγραμμα, επιλέγετε All Programs και πατάτε Next.

- Επιλέγετε το πρωτόκολλο TCP.

- Το επιθυμητό port number είναι το 80. Άρα, στο Local Port επιλέγετε Specific Port και εισάγετε τον αριθμό 80. Στο Remote Port επιλέγετε All Ports.

    - Γιατί; Δεν θα μπορούσατε να επιλέξετε κάποιο συγκεκριμένο port; Μήπως θα μπορούσατε να επιλέξετε ένα εύρος θυρών;

- Αφού πατήσετε Next, ο οδηγός σας ζητά να καθορίσετε το τοπικό δίκτυο (προορισμού) και το απομακρυσμένο δίκτυο (προέλευσης). Επειδή επιθυμούμε να επιτρέπεται η σύνδεση για την τοπική διεύθυνση (Local Address) IP 10.1.1.1, επιλέγετε «These IP Addresses», πατάτε Add και εισάγετε 10.1.1.1/32 ή σκέτο 10.1.1.1 (τι σημαίνει το /32;). Ομοίως, για την απομακρυσμένη διεύθυνση (Remote Address) εισάγετε το υποδίκτυο 10.1.1.0/24 και πατάτε Next.

- Στη συνέχεια, θα καθορίσετε την ενέργεια η οποία θα εκτελείται όταν ένα εισερχόμενο πακέτο πληροί τα παραπάνω κριτήρια. Επειδή σε μια τέτοια περίπτωση, η επιθυμητή ενέργεια είναι η αποδοχή της διέλευσης του πακέτου, επιλέγετε Allow the connection και πατάμε Next.

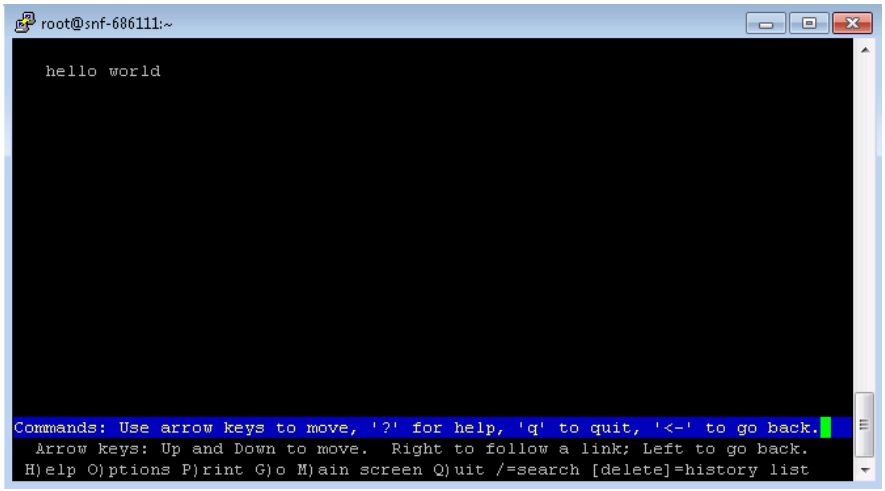
- Καθορίζετε τα προφίλ (domain, private ή public) για τα οποία θα ισχύει ο κανόνας. Μπορείτε να τα αφήσετε όλα επιλεγμένα οπότε ο κανόνας θα ισχύει παντού.

- Πατάτε Next και καθορίζετε ένα όνομα (π.χ. Web Server – LAB test), ώστε να ξεχωρίζετε εύκολα τον κανόνα. Επίσης, αν επιθυμείτε, ως περαιτέρω τεκμηρίωση μπορείτε να προσθέσετε και μια περιγραφή. Πατάτε Finish και ο κανόνας έχει δημιουργηθεί.

- Στο Linux εκτελείτε εκ νέου την εντολή:

```
lynx http://10.1.1.1
```

Τι παρατηρείτε; Ήταν πλέον δυνατή η προβολή της σελίδας;



Εικόνα 13.22 *Προβολή μετά την εισαγωγή του κανόνα*

13.4 Τείχος Προστασίας σε Λ.Σ. Linux

Στον πυρήνα του Λ.Σ. Linux περιλαμβάνεται ένα ισχυρό σύστημα χειρισμού και φιλτραρίσματος πακέτων, το Netfilter. Το τελευταίο παρέχει τη βάση πάνω στην οποία με τη χρήση των Iptables υλοποιείται ένα αποδοτικό σύστημα τείχους προστασίας.

Η δομή του Netfilter/Iptables περιλαμβάνει πέντε πίνακες (tables), οι οποίοι περιέχουν έναν αριθμό αλυσίδων (chains), οι οποίες με τη σειρά τους αποτελούνται από ένα σύνολο κανόνων (rules). Πιο αναλυτικά, έχουμε τους πίνακες:

- **FILTER**
  Είναι ο default πίνακας που συνδέεται με τη βασική λειτουργικότητα του firewall και αυτός με τον οποίο θα ασχοληθούμε στη συνέχεια. Περιέχει τις **αλυσίδες:**
  - **INPUT**, που περιέχει κανόνες για τα εισερχόμενα πακέτα.
  - **FORWARD**, που περιέχει κανόνες για τα πακέτα που διέρχονται από τη μηχανή.
  - **OUTPUT**, που περιέχει κανόνες για τα πακέτα που δημιουργούνται στη μηχανή με εξωτερικό προορισμό.

- **NAT**
  Ο πίνακας αυτός διαχειρίζεται τα πακέτα που υπόκεινται σε μετάφραση διεύθυνσης δικτύου NAT (Network Address Translation).
  Περιέχει τις **αλυσίδες**:
  - **PREROUTING**
  - **OUTPUT**
  - **POSTROUTING**

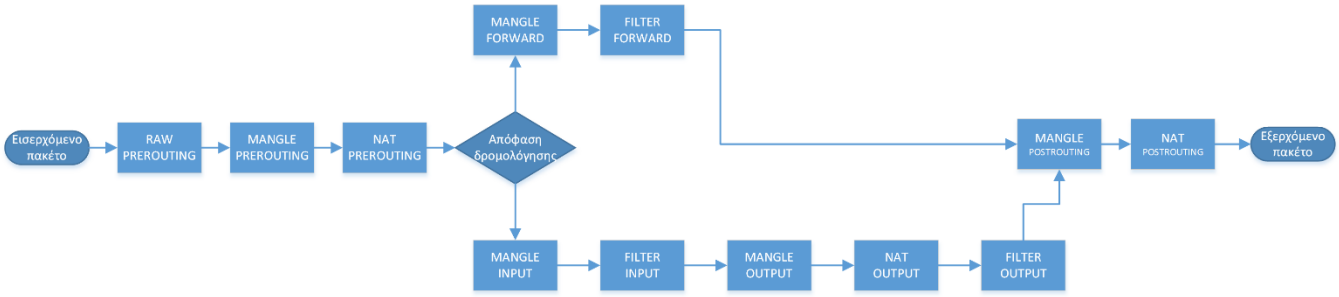
- **MANGLE**
  Χρησιμοποιείται για ειδικές μετατροπές πακέτων και αποτελείται από τις αλυσίδες:
  - **PREROUTING**
  - **OUTPUT**
  - **INPUT**
  - **FORWARD**
  - **POSTROUTING**

- **RAW**
  Χρησιμοποιείται για εξαιρέσεις πακέτων από παρακολούθηση της σύνδεσης και αποτελείται από τις αλυσίδες:
  - **PREROUTING**
  - **OUTPUT**

- **SECURITY**
  Χρησιμοποιείται για την υλοποίηση ελέγχου πρόσβασης κατά-απαίτηση (Mandatory Access Control). **Αποτελείται από** τις αλυσίδες:
  - **INPUT**
  - **FORWARD**
  - **OUTPUT**

Ακόμη, υπάρχει η δυνατότητα προσθήκης επιπρόσθετων αλυσίδων χρήστη (User chains), στις οποίες μπορεί να προωθηθεί ένα πακέτο από μια προκαθορισμένη αλυσίδα.

Πιο συγκεκριμένα, ένα πακέτο εισέρχεται στο σύστημα και ακολουθεί μια πορεία, σύμφωνα με το διάγραμμα που φαίνεται στην Εικόνα 13.23.



Εικόνα 13.23 *Πορεία εισερχόμενου στο netfilter πακέτου*

Οι κανόνες που συνθέτουν τις αλυσίδες, μπορούν να διακριθούν σε δύο μέρη:

- τα OPTIONS, που αποτελούνται από εντολές (commands) και παραμέτρους (parameters) και καθορίζουν τη θέση του κανόνα στην αλυσίδα, καθώς και τα πακέτα για τα οποία εφαρμόζεται,
- το TARGET, που ορίζει την ενέργεια που θα εκτελεστεί από το firewall.

Για να θέσουμε τους κανόνες, χρησιμοποιούμε την εντολή Iptables η οποία δέχεται options με εντολές, παραμέτρους και ενέργεια.

Ενδεικτικές επιλογές είναι:

- -A για append
- -D για delete
- -L για list
- -F για flush
- -I για insert σε καθορισμένη θέση

Ενδεικτικές παράμετροι είναι:

- -p για πρωτόκολλο
- -m για ταίριασμα (-m tcp --dport και –m tcp --sport για destination και source tcp port, αντίστοιχα)
- -s για διεύθυνση πηγής
- -d για διεύθυνση προορισμού
- -i για input interface
- -o για output interface

Οι βασικές ενέργειες είναι:

- -j ACCEPT για αποδοχή του πακέτου
- -j DROP για απόρριψη του πακέτου

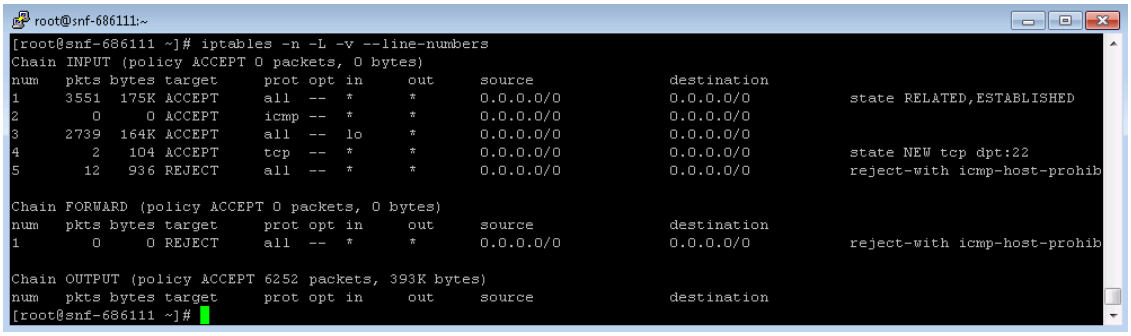
Στη συνέχεια, θα χρησιμοποιήσουμε την εντολή Ipfilter για την παραμετροποίηση του firewall.

13.4.1 Έλεγχος και Καθαρισμός tables

Συνδεθείτε στη μηχανή Linux και εκτελέστε την εντολή:

```
iptables -n -L -v --line-numbers
```

για να δείτε τις τρέχουσες ρυθμίσεις, δηλαδή τους κανόνες των αλυσίδων του πίνακα filter με αριθμητική σειρά. Η σειρά είναι ιδιαίτερα σημαντική, καθώς το κάθε πακέτο εξετάζεται από τους κανόνες με τη σειρά που θα δηλωθεί, ενώ ισχύει η ενέργεια του πρώτου ταιριάσματος (πρώτου κανόνα που ικανοποιείται). Αν δεν βρεθεί κανόνας που να ταιριάζει, εκτελείται η προεπιλεγμένη ενέργεια.



Εικόνα 13.24 *Κανόνες αλυσίδων του πίνακα filter*

Στην εικόνα 13.24 παρατηρούμε ότι:

- Στην αλυσίδα INPUT με προεπιλεγμένη ενέργεια ACCEPT:

1. Επιτρέπεται η είσοδος σε όλα τα πακέτα που ανήκουν σε εδραιωμένες (established) συνδέσεις.
2. Επιτρέπεται η είσοδος πακέτων ICMP.
3. Επιτρέπεται η είσοδος πακέτων από το interface loopback.
4. Επιτρέπεται η είσοδος πακέτων που δημιουργούν νέα σύνδεση στην πόρτα 22/tcp (SSH).
5. Απορρίπτονται όλα τα υπόλοιπα πακέτα.

- Στην αλυσίδα FORWARD με προεπιλεγμένη ενέργεια ACCEPT:

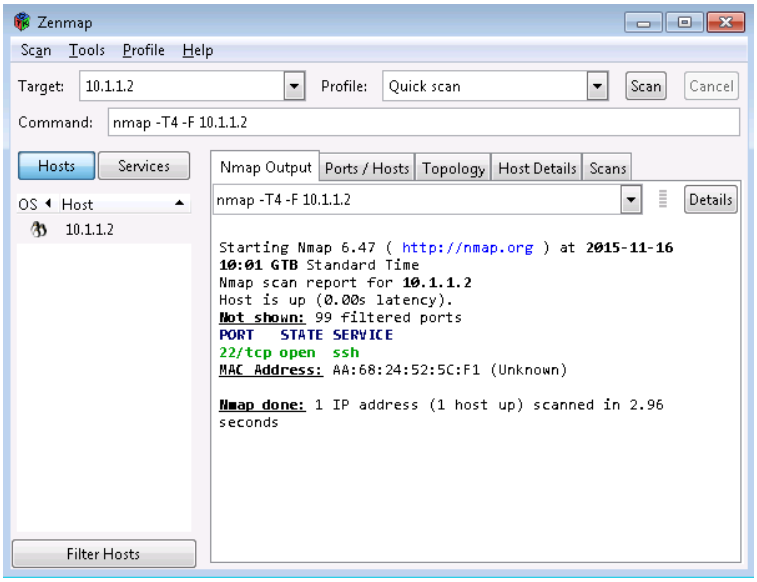
6. Απορρίπτονται όλα τα πακέτα

- Στην αλυσίδα OUTPUT με προεπιλεγμένη ενέργεια ACCEPT δεν υπάρχει κανόνας.

Στη μηχανή με Λ.Σ. Windows, εγκαταστήστε το λογισμικό Zenmap, που θα βρείτε στη διεύθυνση: http://infosec.uom.gr/Study/LAB/ISS/6519/nmap-6.47-setup.exe αποδεχόμενοι τις προεπιλεγμένες ρυθμίσεις.

Στη συνέχεια, εκτελέστε το Zenmap.exe και ορίστε ως Target τη διεύθυνση της Linux μηχανής (10.1.1.2) με Profile Quick Scan και πατήστε Scan.

Ελέγξτε το αποτέλεσμα της εκτέλεσης (για πιο ευανάγνωστη απεικόνιση μπορείτε να επιλέξετε την καρτέλα Ports/Hosts). Συμφωνεί το αποτέλεσμα ελέγχου με το Zenmap με ότι είχατε προηγουμένως παρατηρήσει στους κανόνες του Iptables;

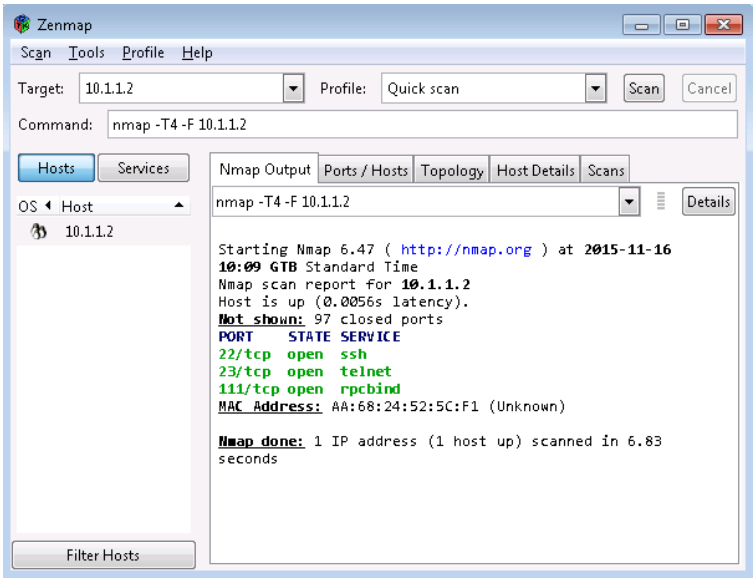


Εικόνα 13.25 *Αποτέλεσμα ελέγχου με Zenmap*

Στη συνέχεια, διαγράψτε όλους τους κανόνες του πίνακα filter, εκτελώντας την εντολή:

```
iptables -F
```

Ελέγξτε αν έχουν διαγραφεί οι κανόνες και εκτελέστε εκ νέου τον έλεγχο με Zenmap. Τι παρατηρείτε;



Εικόνα 13.26 *Αποτέλεσμα ελέγχου με Zenmap μετά την εκκαθάριση των κανόνων*

Αφαιρώντας όλους τους κανόνες, τι παρατηρείτε ότι ισχύει;

13.4.2 Ρύθμιση Τείχους Προστασίας

Το Netfilter μπορεί να λειτουργήσει ως stateless και ως stateful firewall. Έστω ότι σε ένα σύστημα όπου η προεπιλεγμένη ενέργεια ήταν DROP, επιθυμούμε να ρυθμίσουμε το τείχος προστασίας, έτσι ώστε να επιτρέπονται μόνο συνδέσεις από τον έξω κόσμο προς τον SSH server.

Θέτουμε έναν απλό κανόνα με την εντολή:

```
iptables -A INPUT -p tcp –dport 22 -j ACCEPT
```

για να επιτρέψουμε τις εισερχόμενες συνδέσεις προς την πόρτα 22 (για τον ssh server που εκτελείται στον υπολογιστή). Τότε κάθε πελάτης θα μπορεί να έχει πρόσβαση στην πόρτα αυτή. Θα μπορεί όμως να εδραιωθεί η επικοινωνία; Για να συμβεί αυτό θα πρέπει αντιστοίχως να ορίσουμε εξερχόμενες συνδέσεις ως εξής:

```
iptables -A OUTPUT -p tcp –sport 22 -j ACCEPT
```

Για να αποφύγουμε αυτή την απαίτηση του stateless filter, που αν και είναι απλή για τις εισερχόμενες συνδέσεις, γίνεται ιδιαίτερα απαιτητική στις εξερχόμενες οι οποίες εκκινούν από τυχαίες πόρτες, τα iptables παρέχουν τη δυνατότητα δημιουργίας και χρήσης της κατάστασης (state) έτσι ώστε το packet filter να μετατραπεί σε stateful. Έτσι, αρχικά καθορίζουμε στο input chain πως επιτρέπουμε (accept) τη διέλευση πακέτων που ακολουθούν μια εδραιωμένη σύνδεση (match established state) αφού πρώτα αφαιρέσουμε όλους τους προηγούμενους κανόνες:

```
iptables -F
iptables -A INPUT -m state --state RELATED,ESTABLISHED -j
ACCEPT
```

Στη συνέχεια επιτρέπουμε τη διέλευση πακέτων από το interface loopback

```
iptables -A INPUT -i lo -j ACCEPT
```

Τέλος επιτρέπουμε τη σύνδεση με τον ssh server από το δίκτυο 10.1.1.0/24

```
 -A INPUT -p tcp -m state --state NEW -s 10.1.1.0/24 -m tcp --
dport 22 -j ACCEPT
```

Μπορούμε να ελέγξουμε την παραμετροποίηση εκτελώντας:

```
iptables -n -L -v --line-numbers
```

Δοκιμάστε με χρήση του nmap ή εκτελώντας telnet στην πόρτα 23/tcp του Linux server αν επιτρέπεται η σύνδεση. Είναι το αποτέλεσμα κάτι που αναμένατε; Τι παρατηρείτε; Πώς μπορείτε να απαγορεύσετε κάθε σύνδεση εκτός ssh; Δοκιμάστε τις ιδέες σας στη μηχανή.

13.4.3 Απόρριψη Πακέτων.

Στη συνέχεια θα χρησιμοποιήσουμε το πρωτόκολλο icmp έτσι ώστε να γίνει κατανοητή η διαφορά μεταξύ της ενέργειας REJECT και της ενέργειας DROP. Εκτελούμε

```
iptables –F
iptables -A INPUT -p icmp -j REJECT
```

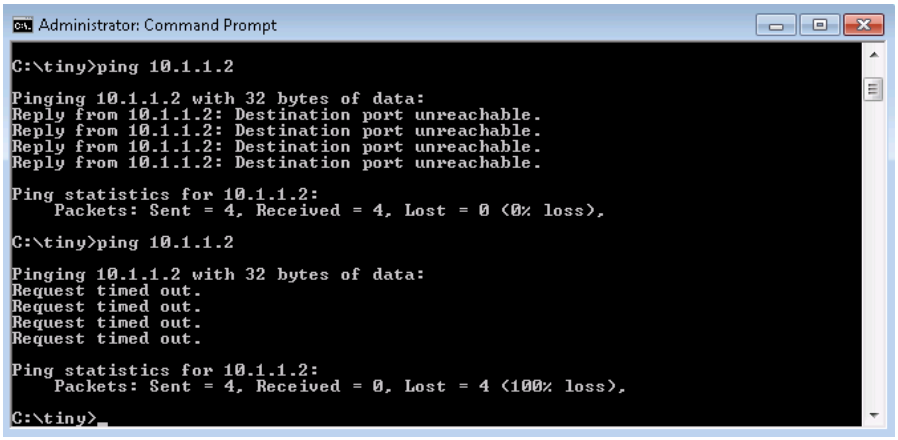
Και από τη μηχανή Windows, εκτελούμε σε ένα command prompt

```
ping 10.1.1.2
```

Στη συνέχεια αλλάζουμε το target:

```
iptables –F
iptables -A INPUT -p icmp -j DROP
```

και εκτελούμε εκ νέου το ping από τη windows μηχανή. Τι διαφορά παρατηρείτε;



Εικόνα 13.27 *Διαφορά drop και reject*

Σε ποια περίπτωση θα επιλέγατε να χρησιμοποιήσετε REJECT και σε ποια DROP;

Επανεκκινήστε τον Linux server εκτελώντας:

```
shutdown -r now
```

ή χρησιμοποιώντας την κονσόλα του Cyclades ή του VirtualBox (ανάλογα με το περιβάλλον στο οποίο εργαστήκατε), ώστε να επανέλθουν οι αρχικές ρυθμίσεις.

Βιβλιογραφία

Bautts, T., Dawson, T., & Purdy, G. (2005). Linux Network Administrator's Guide. O'Reilly Media, Inc.

Cheswick, W. R., Bellovin, S. M., & Rubin, A. D. (2003). Firewalls and Internet Security: Repelling the Wily Hacker. Addison-Wesley Professional.

Noonan, W., & Dubrawsky, I. (2006). Firewall Fundamentals. Pearson Education.

Northcutt, S., Zeltser, L., Winters, S., Kent, K., & Ritchey, R. W. (2005). Inside Network Perimeter Security (Inside). Sams.

Purdy, G. N. (2004). Linux iptables Pocket Reference. O'Reilly Media, Inc.

Rash, M. (2007). Linux Firewalls: Attack Detection and Response with iptables, psad, and fwsnort. No Starch Press.

Shapiro, J. R. (2008). Windows Server 2008 Bible. John Wiley & Sons.

Stewart, J. M. (2013). Network Security, Firewalls and VPNs. Jones & Bartlett Publishers.

Whitman, M., Mattord, H., & Green, A. (2011). Guide to Firewalls and VPNs. Cengage Learning.

Ziegler, R. L., & Constantine, C. B. (2002). Linux Firewalls. Sams Publishing.

Κριτήρια αξιολόγησης

Ερωτήσεις κατανόησης

Απαντήστε στις ακόλουθες ερωτήσεις. Κάθε ερώτηση μπορεί να έχει μοναδική ή περισσότερες απαντήσεις.

1. Ποιες από τις παρακάτω είναι κατηγορίες τείχους προστασίας;
α) State
β) No State
γ) Packet Filter
δ) Application Gateway

2. Το τείχος προστασίας μπορεί να εποπτεύει
α) μόνο τα εισερχόμενα πακέτα δεδομένων
β) μόνο τα εξερχόμενα πακέτα δεδομένων
γ) τα εισερχόμενα και τα εξερχόμενα πακέτα δεδομένων
δ) κανένα από τα παραπάνω

3. Σε περιβάλλον Windows, το τείχους προστασίας αποτελεί ένα:
α) Packet filter
β) Circuit-Level Gateweay
γ) Application-Level Gateweay
δ) Unified Threat Management Gateway

4. Το τείχος προστασίας προστατεύει:
α) Από κάθε κακόβουλο λογισμικό (malware)
β) Από trojan horses
γ) Από επιθέσεις τύπου phising
δ) Από επιθέσεις τύπου pharming
ε) Από ιούς υπολογιστών (viruses)
στ) Κανένα από τα παραπάνω

5. Το windows firewall
α) Είναι stateless
β) Είναι stateful
γ) Απαιτεί την ύπαρξη domain controller για τη λειτουργία του
δ) Εξετάζει τους κανόνες με τη σειρά δημιουργίας τους

6. Για να αποτρέψουμε τη σύνδεση στην υπηρεσία web, πρέπει να δηλώσουμε το ζεύγος θύρας/πρωτοκόλλου
α) 80/UDP
β) 80/TCP
γ) 80/HTTP
δ) 80/WEB

7. Στο netfilter ισχύει:
α) Ένας πίνακας περιέχει κανόνες που σχηματίζονται από αλυσίδες
β) Η αλυσίδα περιέχει ένα σύνολο κανόνων που σχηματίζουν σε πίνακες
γ) Ένας πίνακας περιέχει αλυσίδες που αποτελούνται από κανόνες
δ) Οι κανόνες αποτελούνται από αλυσίδες

8. Στα iptables:
α) Οι κανόνες εξετάζονται με τη σειρά και η εξέταση σταματά στο πρώτο ταίριασμα
β) Οι κανόνες εξετάζονται με τη σειρά και υλοποιείται ο κανόνας στο τελευταίο ταίριασμα
γ) Οι κανόνες εξετάζονται τυχαία και η εξέταση σταματά στο πρώτο ταίριασμα
δ) Πρώτα εφαρμόζεται η προεπιλεγμένη ενέργεια

9. Στην εντολή iptables όταν δε δηλώνεται πίνακας, υπονοείται ο:
α) raw
β) filter
γ) mangle
δ) nat
ε) security

10. Για τις αλυσίδες ισχύει:
α) Είναι 3 σε κάθε πίνακα
β) Ο χρήστης μπορεί να επιλέξει να προωθήσει πακέτα από τη μία στην άλλη
γ) Εκτός από τις προεπιλεγμένες μπορούν να δημιουργηθούν επιπρόσθετες και από το χρήστη
δ) Δε χρησιμοποιούνται πια