Ασφάλεια Δικτύων και Επικοινωνιών

(Network and Communication Security)

7. Συστήματα firewall

8. Βασική διαμόρφωση iptables

9. Παράδειγμα υλοποίησης Πολιτικής Ασφάλειας Δικτύου

Αν.Καθ. Παναγιώτης Κοτζανικολάου

ΠΜΣ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ ΚΑΙ ΕΠΙΣΤΗΜΗ ΔΕΔΟΜΕΝΩΝ

7. Έλεγχος δικτυακής πρόσβασης
Συστήματα firewall

Περιεχόμενα

- Εισαγωγικές έννοιες
  - Ορισμοί, Καλυπτόμενες Υπηρεσίες Ασφάλειας
- Δυνατότητες συστημάτων Firewall
- Περιορισμοί συστημάτων Firewall
- Κατηγορίες συστημάτων Firewall
  - Επιπέδου 3: packet filtering firewalls
  - Επιπέδου 4: circuit
  - Επιπέδου 3,4,5: hybrid –dynamic statefull inspection
- Τοπολογία συστημάτων Firewall
- Συμπεράσματα και ερωτήσεις

Τοίχος προστασίας (Firewall)

- Σύστημα (ή σύνολο συστημάτων), το οποίο σκοπό έχει την επιβολή μίας προκαθορισμένης πολιτικής πρόσβασης (access policy enforcement)
- Επιβάλει διαφορετική πολιτική (δικαιώματα) σε σε επιμέρους δίκτυα
- Ορίζει τα σημεία διασύνδεσης με άλλα δίκτυα
- Παρέχει προστασία στην περίμετρο του δικτύου (network perimeter security)

Τοίχος προστασίας (Firewall)

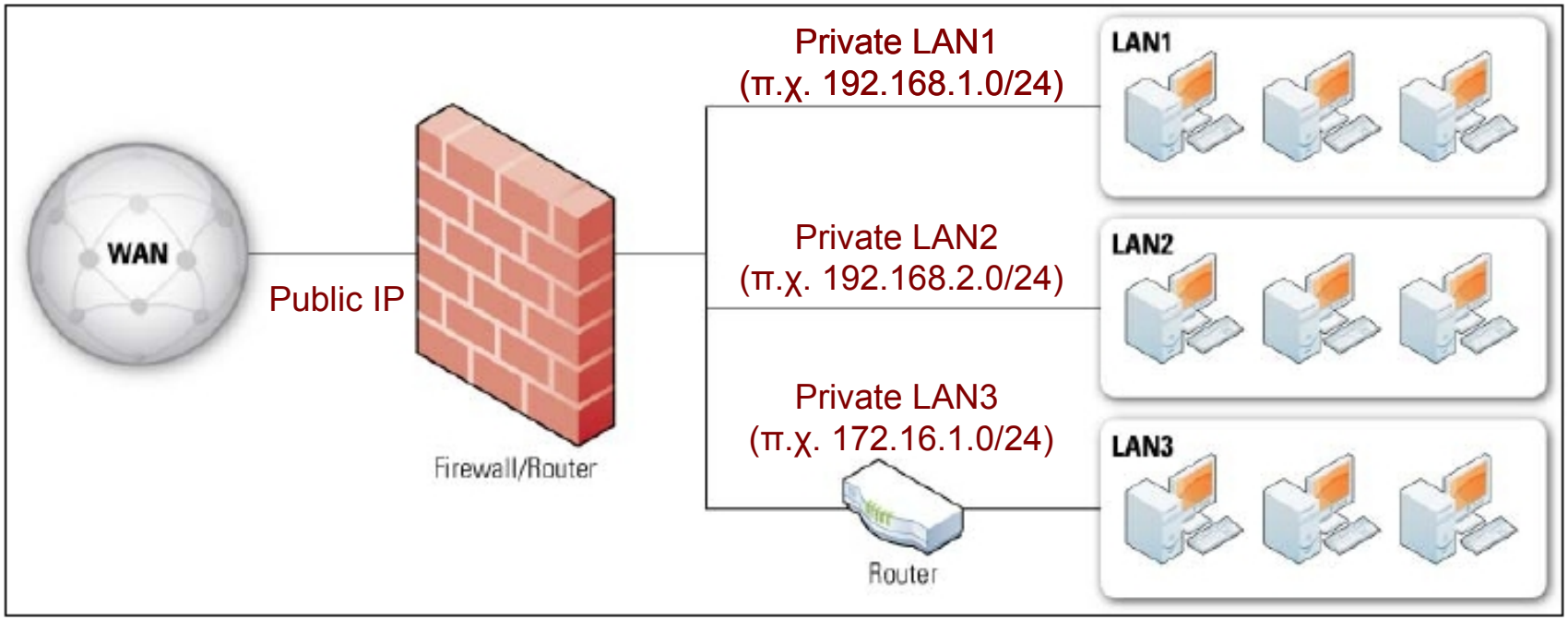


Figure 3-1. Simple Routed Network with Firewall Device (Πηγή: NIST SP 800-41)

RFC 1918 private IP address ranges
10.0.0.0 - 10.255.255.255
172.16.0.0 - 172.31.255.255
192.168.0.0 - 192.168.255.255

Δυνατότητες συστημάτων firewall

- Διευκολύνει την επιβολή σύνθετων πολιτικών πρόσβασης μέσα από ένα κεντρικό σημείο
- Επιτρέπει την καταγραφή γεγονότων (event logs) σχετικά με τη δικτυακή κίνηση (network activity logging)
  - Παρέχει δυνατότητες ανάλυσης και εντοπισμού ύποπτης κίνησης ή συνδέσεων
- Απόκρυψη των πραγματικών IP διευθύνσεων και των πραγματικών θυρών επικοινωνίας (μέσω της υπηρεσίας NAT)
  - Συνεπώς παρέχει (εν μέρει) και μηχανισμούς προστασίας κίνησης (traffic padding)

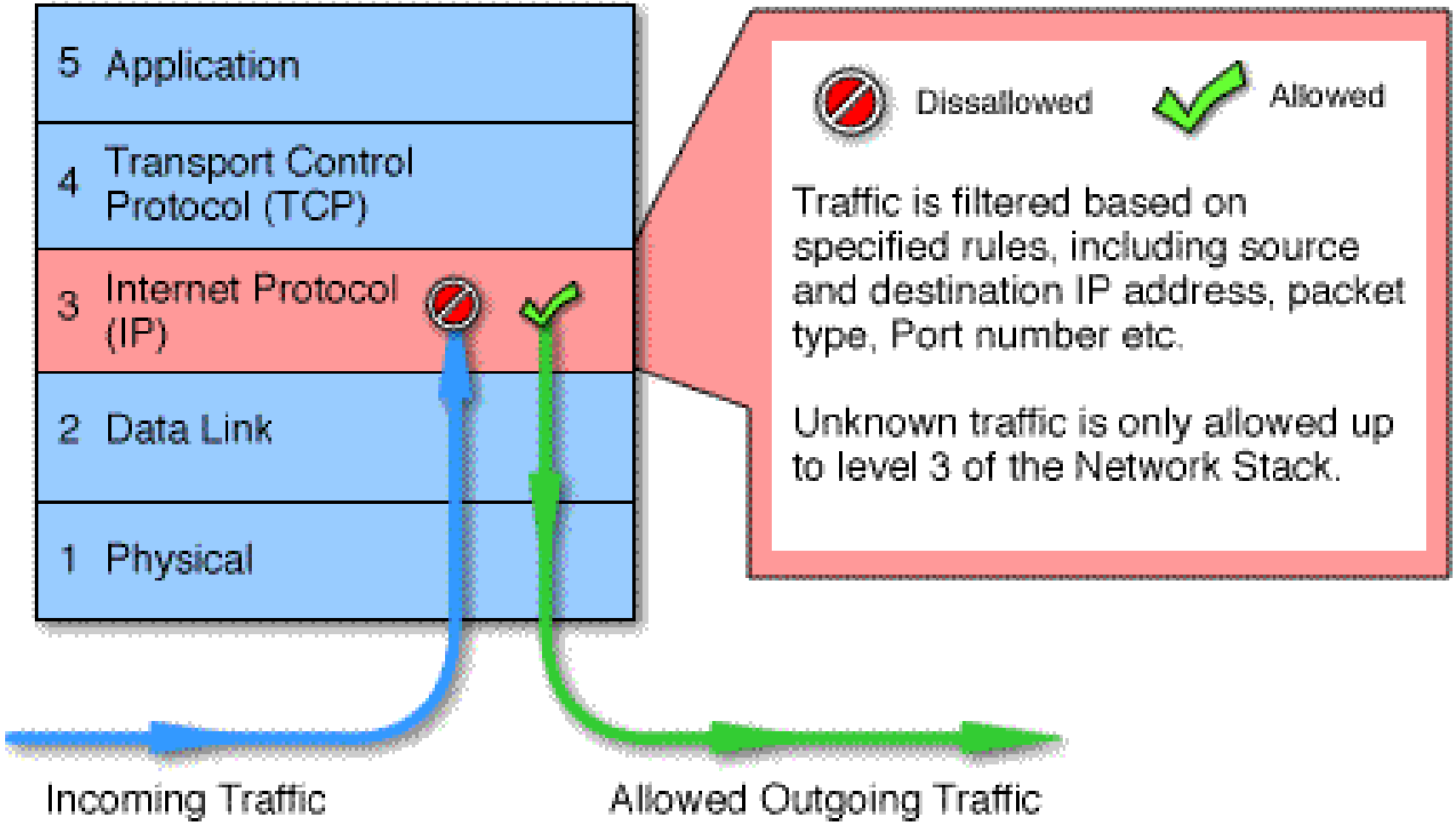
Περιορισμοί συστημάτων firewall

- Ένα firewall **δεν προστατεύει από:**
  - Δεδομένα τα οποία δεν μπορεί να “διαβάσει”
    - π.χ. Κρυπτογραφημένα δεδομένα μέσω IPSec ή SSL/TLS
  - Ορισμένες επιθέσεις από το “εσωτερικό” του δικτύου
    - Κακόβουλοι χρήστες
    - Μολυσμένα συστήματα
    - Κακόβουλο λογισμικό (Virus, Trojans κτλ)
  - Κάθε είδος επικοινωνίας που τα παρακάμπτει: Π.χ.
    - Συσκευές που συνδέονται μέσω τρίτων wireless access point
    - Πρωτοκόκολλα που παρέχονται μέσω https συνδέσεων
    - Modems και συνδέσεις dial-up
  - Άγνωστες απειλές (υπάρχει μερική προστασία στα πιο εξελιγμένα συστήματα)

Κατηγορίες firewall ανά επίπεδο δικτύου (network layer)

- Firewalls επιπέδου δικτύου (layer-3 firewalls)
  - **Packet filtering**
- Firewalls επιπέδου μεταφοράς (layer 3-4 firewalls)
  - **Packet filtering with stateful inspection**
- Firewalls επιπέδου εφαρμογής (application-layer firewalls)
  - **Proxy Gateway**
- Υβριδικά (hybrid firewalls) επιπέδου 3-4-5.

Firewall επιπέδου δικτύου (Packet filtering) (1)



http://www.ing-steen.se/share/text/school/security/document/firewalls.ppt

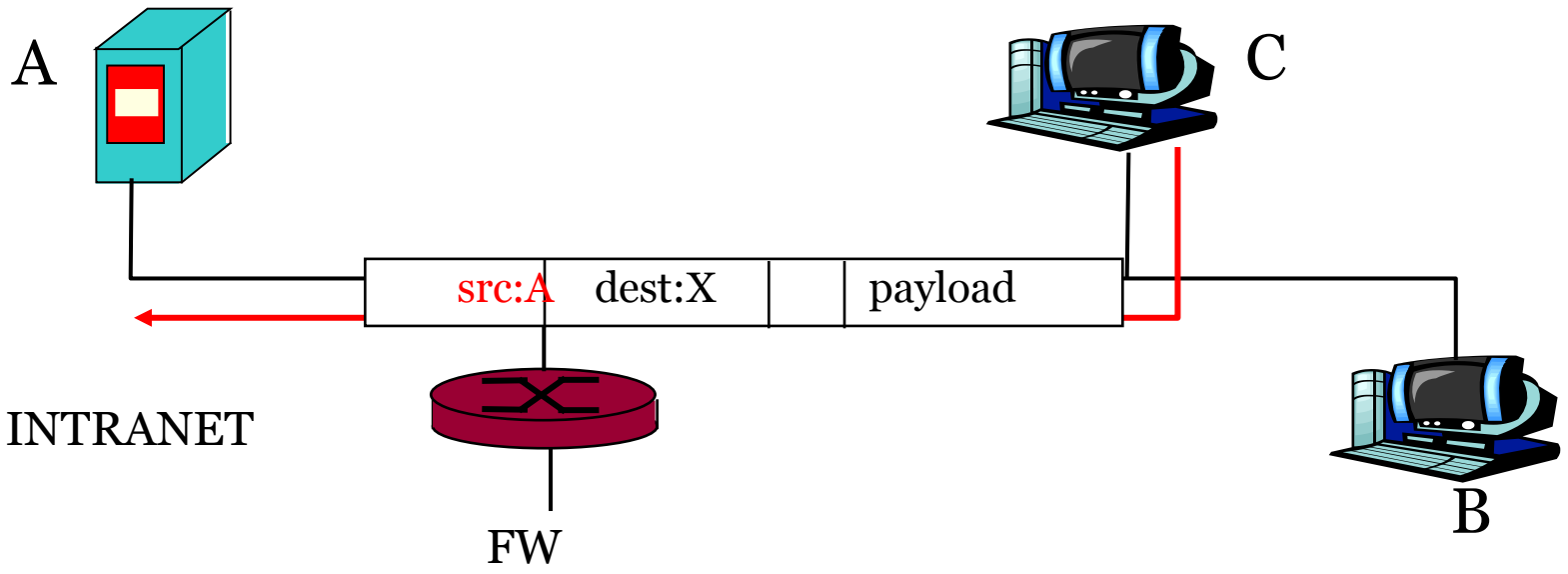
Firewall επιπέδου δικτύου (Packet filtering) (2)

- Δρομολογητές (routers) με αυξημένες δυνατότητες
- Για κάθε πακέτο που λαμβάνεται εξετάζεται:
  - Η IP διεύθυνση και η θύρα πηγής (source IP/port)
  - Η IP διεύθυνση και η θύρα προορισμού (destination IP/port)
  - Το είδος πρωτοκόλλου επιπέδου μεταφοράς (TCP, UDP, ICMP, κτλ)
- Με βάση την πολιτική πρόσβασης αποφασίζεται:
  - Εάν είναι δυνατή η δρομολόγηση **(reachable address)**
  - Εάν επιτρέπεται η δρομολόγηση **(accept/deny)**
- Η πολιτική πρόσβασης υλοποιείται με Λίστες Ελέγχου Πρόσβασης (Access Control Lists – ACLs)

Firewall επιπέδου δικτύου (Packet filtering) (3)
Ανοικτές και Κλειστές Πολιτικές

- Πολιτική προκαθορισμένης άδειας (default accept): Ανοιχτή προσέγγιση
  - Ότι δεν απαγορεύεται ρητά, επιτρέπεται
- Πολιτική προκαθορισμένης απαγόρευσης (default deny): Κλειστή προσέγγιση
  - Ότι δεν επιτρέπεται ρητά, απαγορεύεται
- Συνηθίζεται η πολιτική default deny

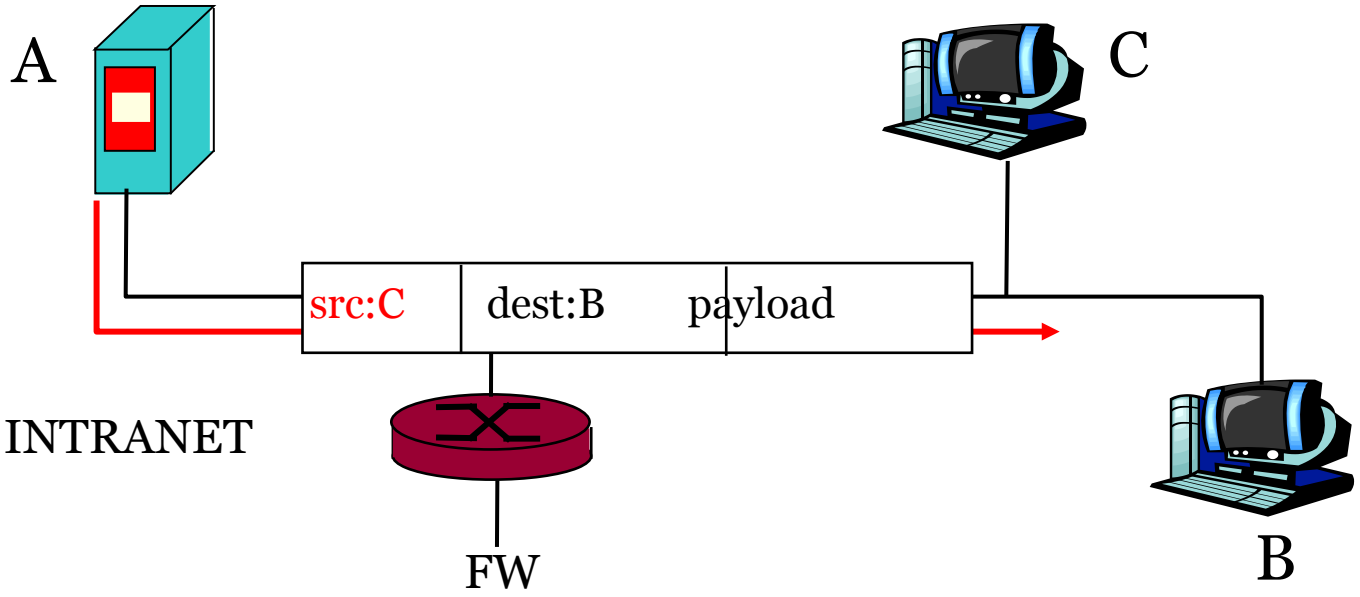
Firewall επιπέδου δικτύου (Packet filtering) (4)
Τυπικοί Κανόνες: Ingress Filtering



- Ingress filtering: Απόρριψη **εισερχόμενων** πακέτων που έχουν IP διεύθυνση προέλευσης **οποιουδήποτε εσωτερικού κόμβου**

In	TCP/UDP	10.10.10.0	*	*	*	Deny	Ingress filetring

Firewall επιπέδου δικτύου (Packet filtering) (5)
Τυπικοί Κανόνες: Egress Filtering



- Egress filtering: Απόρριψη **εξερχόμενων** πακέτων που **δεν έχουν εσωτερικές** IP διευθύνσεις προέλευσης

Out	TCP/UDP	NOT IN 10.10.10.0	*	*	*	Deny	Egress filetring

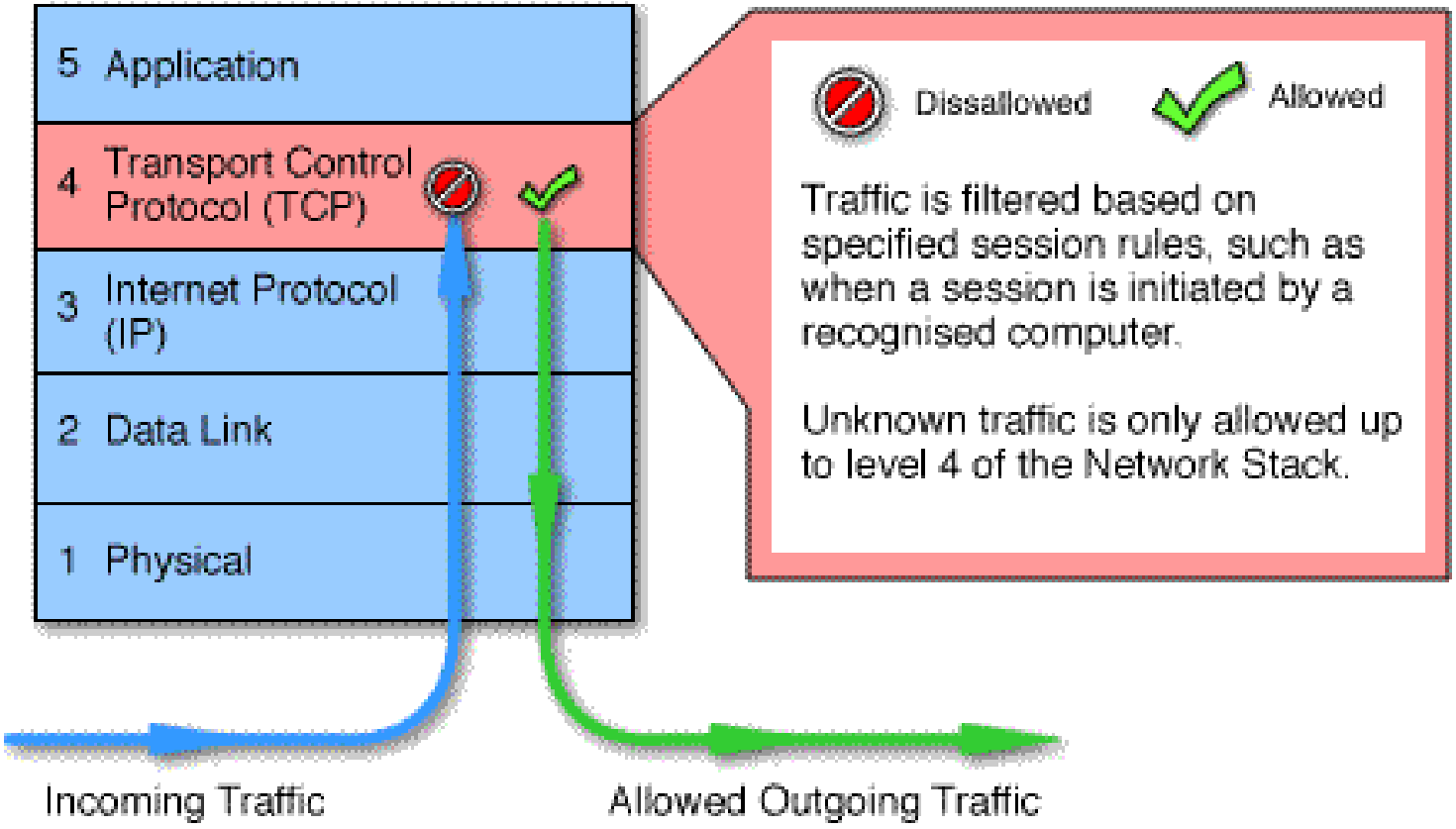
Το πρόβλημα του Stateless Filtering (1)

- Στις συνδέσεις TCP, σε κάθε υπηρεσία **εξυπηρετητών (servers)** αντιστοιχίζονται οι **θύρες (ports) [1 – 1023]**
  - 20,21 για FTP
  - 23 για Telnet
  - 25 for SMTP
  - 80 για HTTP…
- Οι **πελάτες (clients)** χρησιμοποιούν τις θύρες **[1024 -16383]** για να συνδεθούν με εξυπηρετητές
  - Στην περίπτωση του packet filtering, οι θύρες αυτές θα πρέπει να είναι ανοικτές για να λάβει ο πελάτης την απάντηση

Το πρόβλημα του Stateless Filtering (2)

- Τι κάνει ένα packet-filtering firewall όταν δει εισερχόμενη αίτηση από (επιτρεπόμενη) εξωτερική IP διεύθυνση προς ένα client σε θύρα >1023;
  - Θα την αποδεχθεί: πιθανώς να είναι η απάντηση του server σε προηγούμενο αίτημα του client
- Όμως μπορεί να είναι κακόβουλη αίτηση σύνδεσης
- Αδύνατη η διάκριση χωρίς τη διατήρηση ελέγχου στο επίπεδο μεταφοράς!

Firewall επιπέδου μεταφοράς (stateful inspection) (1)



http://www.ing-steen.se/share/text/school/security/document/firewalls.ppt

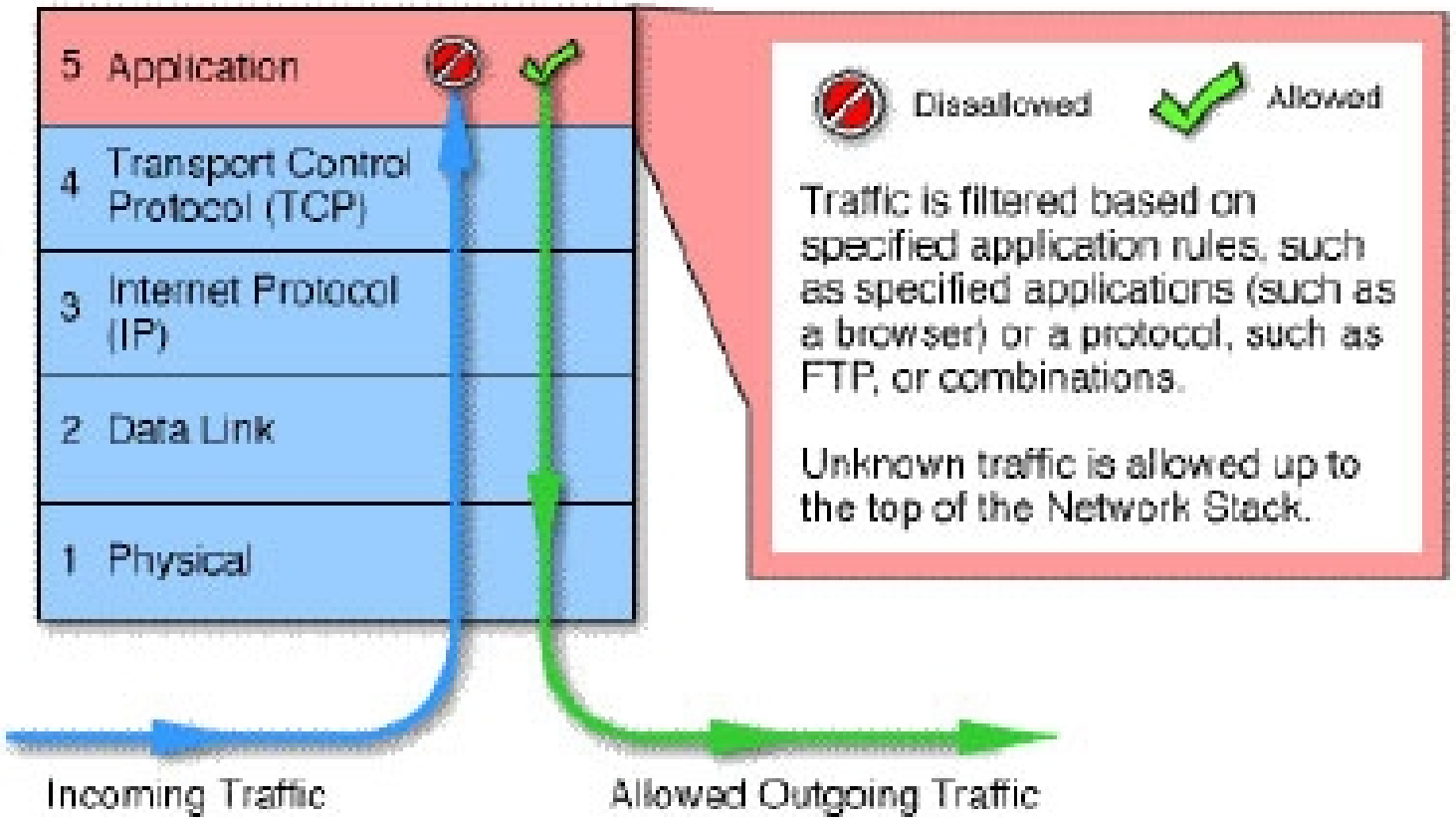
Firewall επιπέδου μεταφοράς (stateful inspection) (2)

- Ελέγχουν το πρωτόκολλο «χειραψίας» (TCP handshake)
  - Πακέτα που στέλνονται κατά την αρχικοποίηση της TCP σύνδεσης (TCP ACK bit =? 1)
- Δεν επιτρέπει συνδέσεις TCP από άκρο-σε-άκρο (end-to-end)
- Δημιουργεί για κάθε επικοινωνία δύο TCP συνδέσεις,
  - Μία TCP σύνδεση μεταξύ του firewall και ενός εσωτερικού client, και
  - Μία TCP σύνδεση μεταξύ του firewall και του εξωτερικού κόμβου
- Μεταφέρει τα TCP segments από τη μία σύνδεση στην άλλη
- Κλείσιμο θυρών εκτός από αυτές που χρησιμοποιούνται

Firewall επιπέδου μεταφοράς (stateful inspection) (3)

- Ο έλεγχος γίνεται και πάλι ανά πακέτο, αλλά στο πλαίσιο της σύνδεσης. Για κάθε πακέτο εξετάζεται:
  - Είναι νέα αίτηση; Έλεγχος με βάση την πολιτική πρόσβασης (ACL)
  - Συνέχεια υπάρχουσας σύνδεσης; Έλεγχος με βάση τους κανόνες που αφορούν την τρέχουσα σύνδεση
  - Η εισερχόμενη κίνηση σε ένα port >1023 επιτρέπεται μόνο εφόσον έχει ήδη εγκατασταθεί μία σύνδεση
  - Τυπικό φίλτρο: default deny για οτιδήποτε δεν επιτρέπεται

Firewall επιπέδου εφαρμογής (Proxy Gateway) (1)



http://ivs.cs.uni-magdeburg.de/EuK/lehre/lehrveranstaltungen/Sommersemester_2005/kun/Transport_layer.pdf

Firewall επιπέδου εφαρμογής (Proxy Gateway) (2)

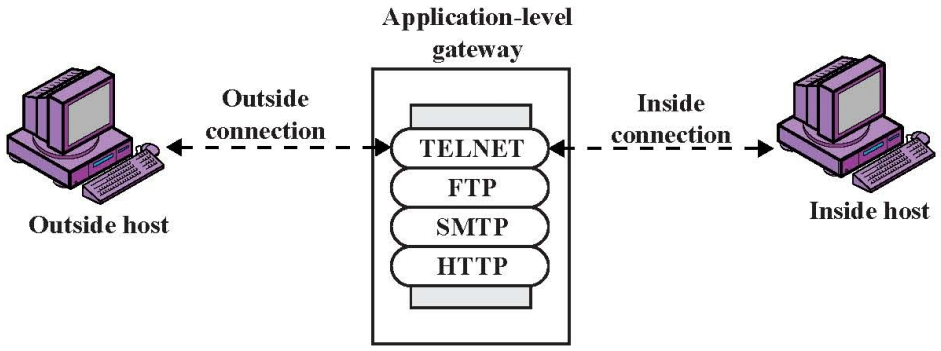
- Τα Proxy Gateways (ή Application Gateways ή Bastion Hosts) αποτελούν εξειδικευμένους server με δυνατότητες εξέτασης των δεδομένων για κάθε υπηρεσία
- Λαμβάνουν αποφάσεις με βάση τα δεδομένα της εφαρμογής.
  - Ταυτότητα χρήστη
  - Περιεχόμενο επικοινωνίας
- Ένα firewall μπορεί να περιλαμβάνει πολλά Proxy Gateways (ένα για κάθε εφαρμογή) .
- Κάθε ένα όμως λειτουργεί ως αυτόνομη διεργασία.

Firewall επιπέδου εφαρμογής (Proxy Gateway)(3)
Παράδειγμα υπηρεσίας Telnet

- Έστω ότι θέλουμε να επιτρέψουμε την υπηρεσία Telnet μόνο σε συγκεκριμένους χρήστες.
  - Δεν είναι δυνατό με packet filtering ή/και stateful inspection firewalls
- Λύση: Συνδυασμός packet filter (επίπεδο-3) και Telnet Proxy (επίπεδο-5).
  - Το packet filter διαμορφώνεται ώστε να απαγορεύει όλες της συνδέσεις Telnet, εκτός από εκείνες που ξεκινούν από την IP διεύθυνση του Telnet Proxy.
  - Αναγκάζει όλες τις εξερχόμενες συνδέσεις Telnet να περάσουν από τον Proxy.
  - Ένας εσωτερικός χρήστης, για να χρησιμοποιήσει την υπηρεσία Telnet προς το εξωτερικό δίκτυο, πρέπει πρώτα να ξεκινήσει ένα Telnet session με τον Telnet Proxy.
  - Ο Telnet Proxy ζητά αυθεντικοποίηση του χρήστη (π.χ. Password) και ελέγχει τα δικαιώματα του χρήστη.
  - Αν ο χρήστης έχει δικαίωμα, τότε ο Proxy:
    - (1) ζητά από τον χρήστη το όνομα του εξωτερικού κόμβου
    - (2) εγκαθιστά ένα Telnet session μεταξύ του Proxy και του εξωτερικού κόμβου
    - (3) μεταδίδει τα δεδομένα από τον εξωτερικό κόμβο προς τον χρήστη και αντίστροφα.
  - Συνεπώς ο Proxy λειτουργεί ταυτόχρονα σαν Telnet Server και Client.

Firewall επιπέδου εφαρμογής (Proxy Gateway)(4)
Πολλαπλά Proxy firewalls

- HTTP Application Level Gateway
  - … Μπλοκάρισμα συγκεκριμένων URL, web caching
- E-Mail Application Level Gateway
  - … Φιλτράρισμα μηνύματος βάσει αποστολέα, παραλήπτη, περιεχομένου, μεγέθους μηνύματος, κ.λ.π



(b) Application-level gateway

Firewall επιπέδου εφαρμογής (Proxy Gateway)(5)
Πολλαπλά Proxy firewalls

- Ο Proxy δεν βλέπει απλώς IP πακέτα, αλλά εξετάζει τα δεδομένα της επικοινωνίας και το είδος της εφαρμογής.
- Ένας mail gateway, μπορεί να εξετάζει για κάθε μήνυμα που ανταλλάσσεται:
  - Τις επικεφαλίδες του μηνύματος (αποστολέας, παραλήπτης κτλ)
  - Το μέγεθος
  - Το είδος των συνημμένων αρχείων
  - Το περιεχόμενο του μηνύματος, …
- HTTP Proxy:
  - Μπορεί να επιτρέπει πρόσβαση μόνο σε συγκεκριμένες σε σελίδες
  - Να απαγορεύει πρόσβαση σε συγκεκριμένου τύπου σελίδες

Διαμόρφωση Application Proxy

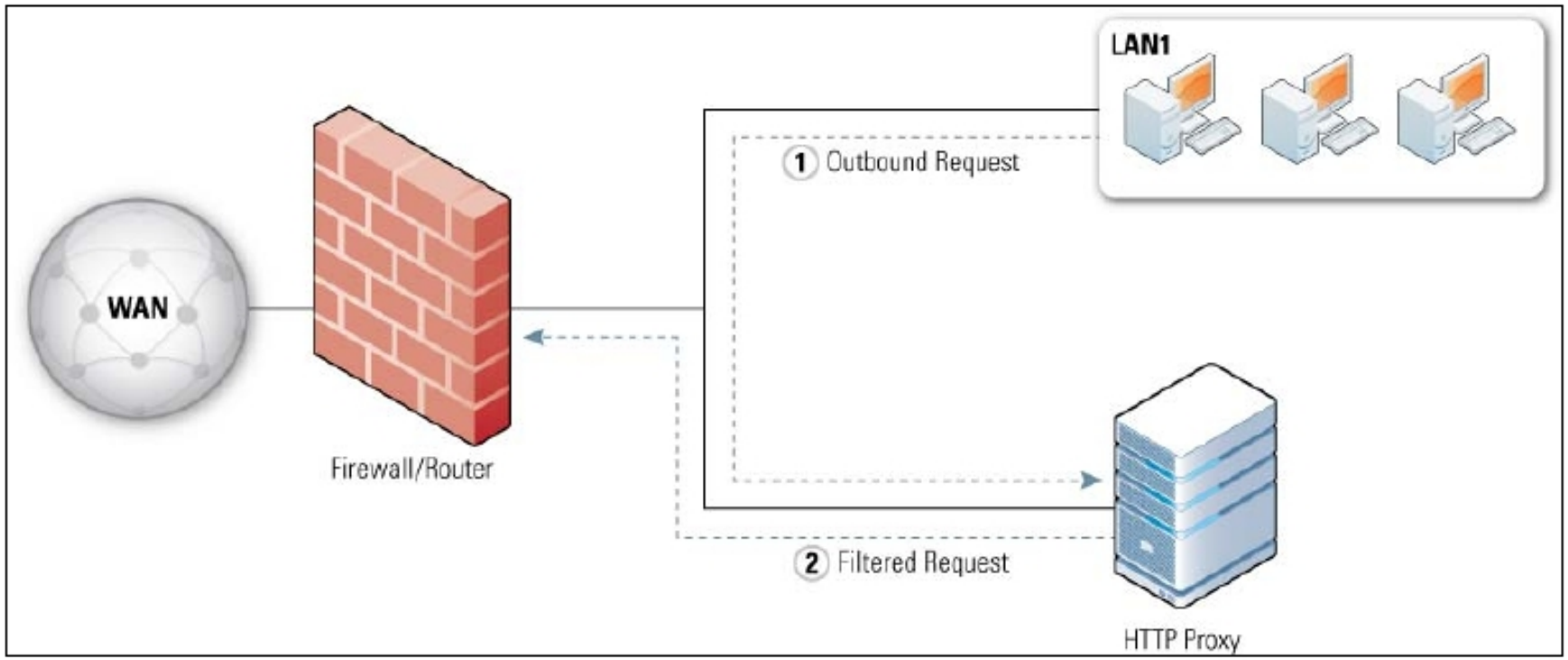
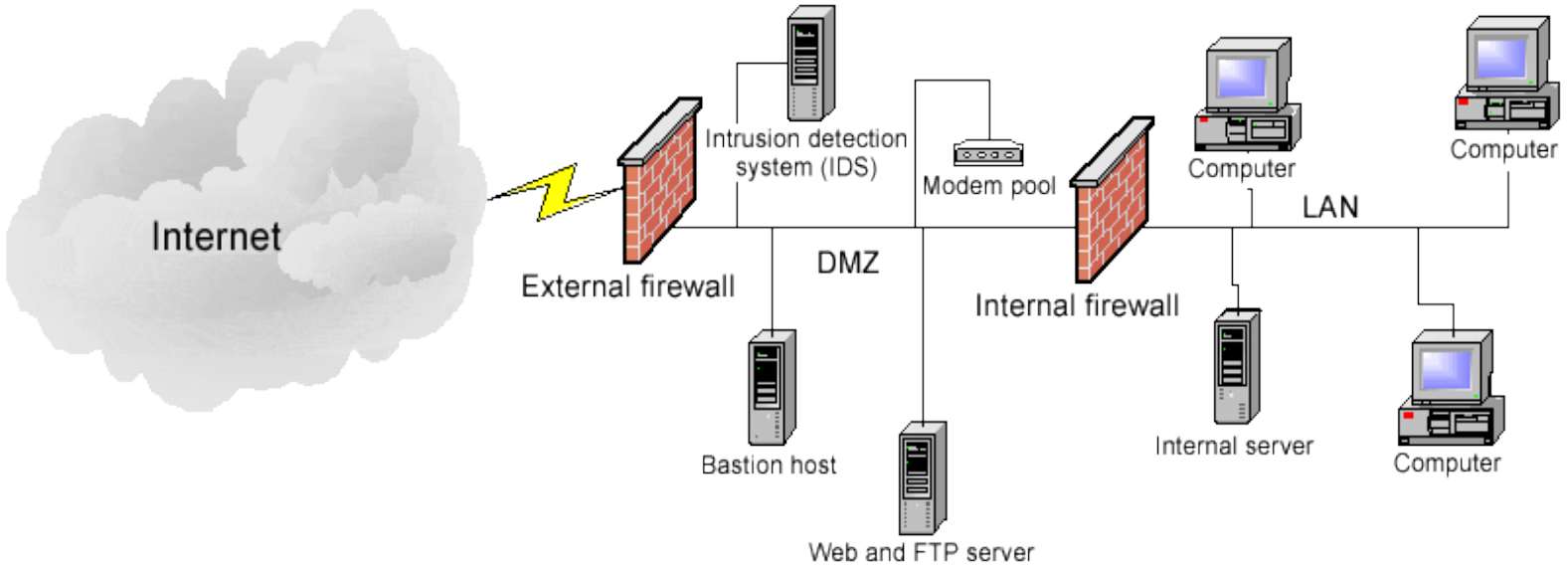


Figure 2-2. Application Proxy Configuration (Πηγή: NIST SP 800-41)

Firewalls και Τοπολογίες: DMZ

DMZ (Demilitarized Zone structure)

«*Αποστρατικοποιημένη Ζώνη*»



http://www.cmpe.boun.edu.tr/courses/cmpe526/spring2005/Cmpe526-20050505-GokhanAydin-Firewalls.ppt

Firewalls και Τοπολογίες: παραλλαγή DMZ

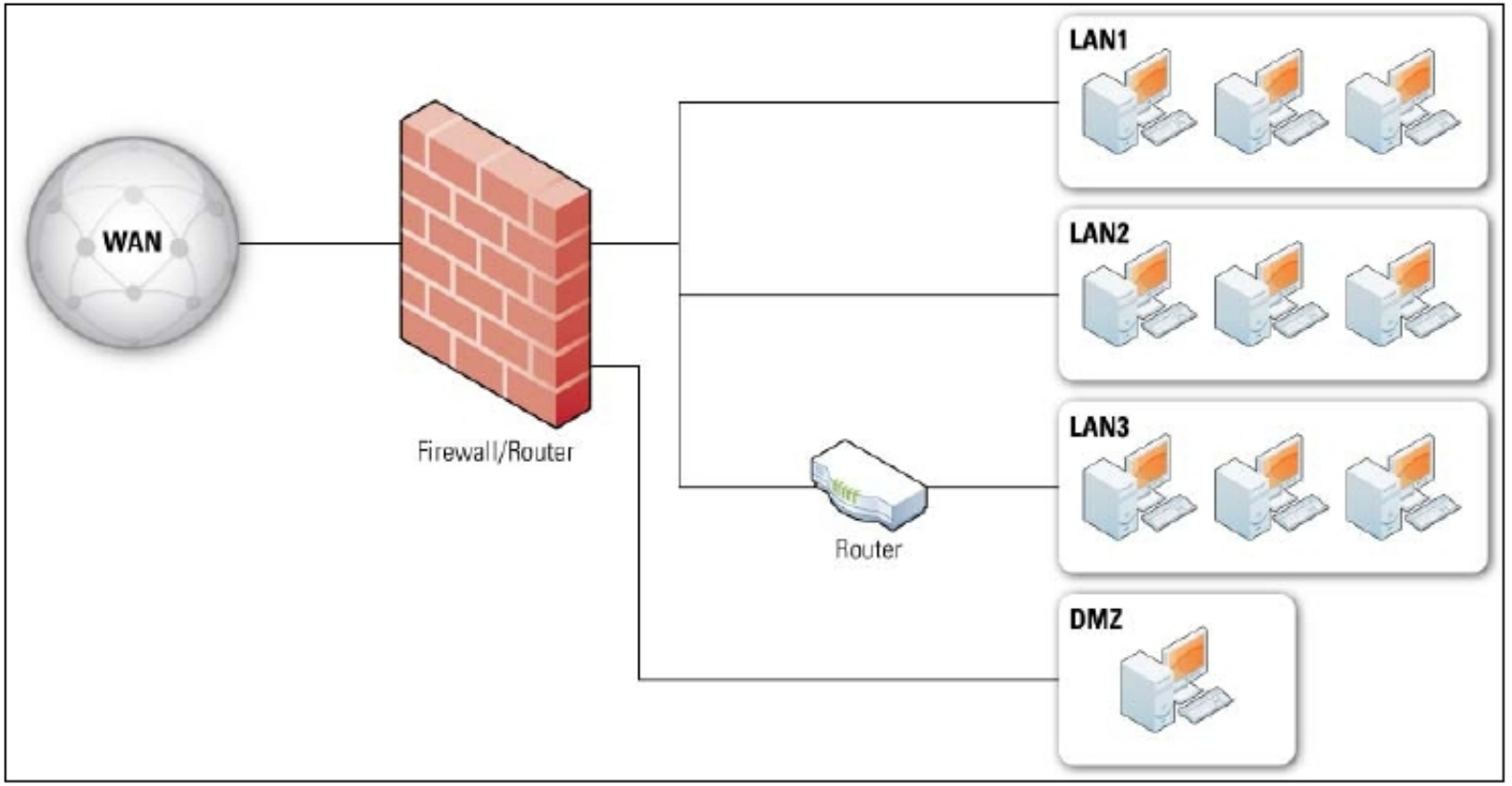
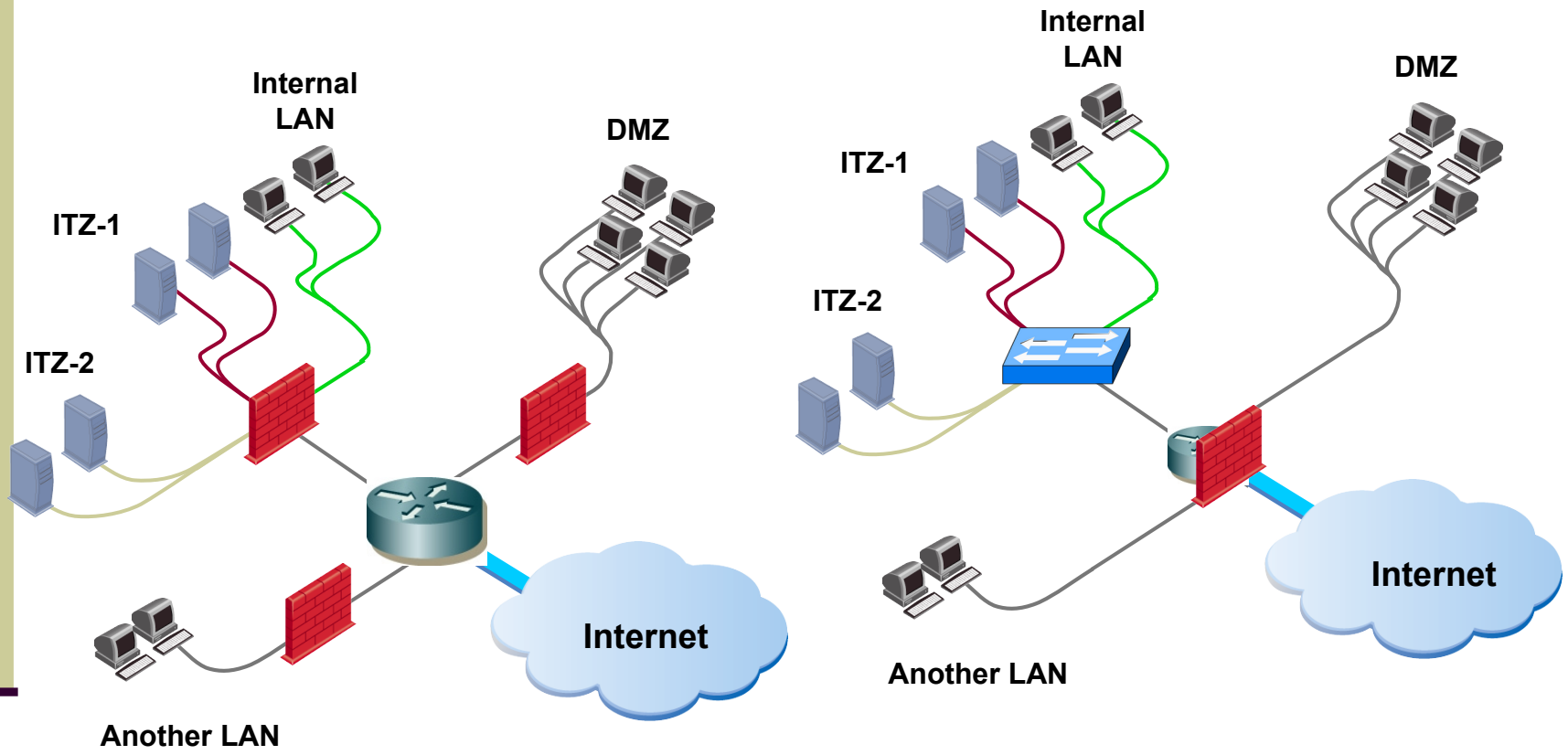


Figure 3-2. Firewall with a DMZ (Πηγή: NIST SP 800-41)

Firewalls και Τοπολογίες...



Συμπεράσματα

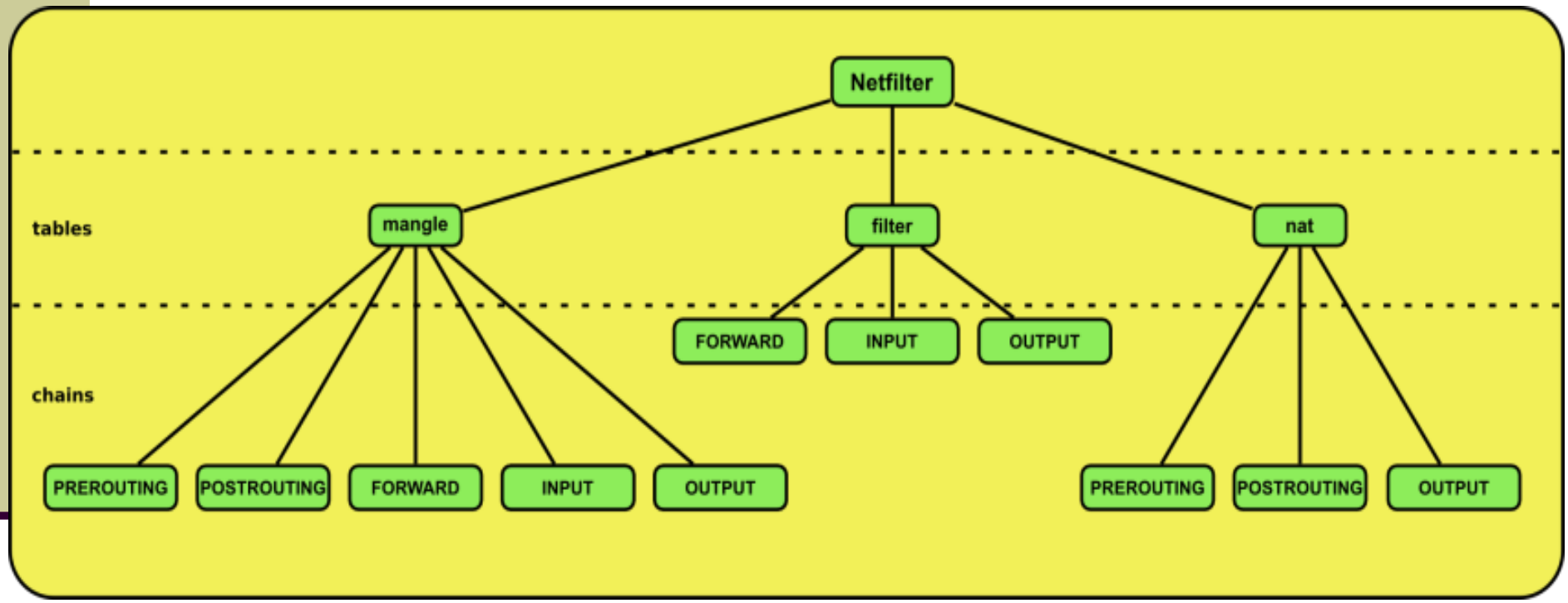
- Τα firewalls παρέχουν υπηρεσίες ελέγχου πρόσβασης σε διάφορα επίπεδα
- Με κατάλληλο συνδυασμό υπηρεσιών ασφάλειας διαφορετικών επιπέδων, κανόνων πρόσβασης και τοπολογίας μπορεί να επιτευχθεί σημαντικό επίπεδο ασφάλειας
- Τα συστήματα firewalls δεν είναι πανάκεια. Ευάλωτα σε:
  - Μη ελεγχόμενες συνδέσεις
  - Λανθασμένη διαμόρφωση κανόνων πρόσβασης
  - Spoofing
  - Ευπάθειες Εφαρμογών
  - Εσωτερικές επιθέσεις
  - ...

8. Βασική διαμόρφωση firewall με τη χρήση iptables

Δομή Netfilter (1/2)

- Χρησιμοποιεί τρεις βασικές δομές (πίνακες):
  - Filtering
    - Χρησιμοποιείται για το φιλτράρισμα των πακέτων
  - NAT
    - Χρησιμοποιείται για την υλοποίηση της υπηρεσίας NAT
  - Mangling
    - Χρησιμοποιείται για την τροποποίηση χαρακτηριστικών των πακέτων
- Ο κάθε πίνακας χρησιμοποιεί τις δικές του «αλυσίδες» (chains) από κανόνες

Δομή Netfilter (2/2)



Ο πίνακας filter

- Χρησιμοποιείται κυρίως για το φιλτράρισμα των πακέτων.
- Με βάση τους κανόνες του filter αποφασίζεται εάν θα γίνει αποδοχή ή απόρριψη του κάθε πακέτου
- Ο κάθε κανόνας εξετάζει το πακέτο.
  - Εάν τα χαρακτηριστικά του συμφωνούν με αυτά που περιγράφονται στον κανόνα, τότε το πακέτο στέλνεται στον προορισμό που περιγράφει ο κανόνας.
- Υπάρχει η δυνατότητα φιλτραρίσματος σε κάποια από τα προηγούμενα στάδια.
  - Ο πίνακας αυτός είναι σχεδιασμένος ειδικά για αυτό το σκοπό.

Πίνακας filter: αλυσίδες και προορισμοί

Πίνακας Filter		
Build-in αλυσίδες	INPUT	Εισερχόμενα πακέτα που προορίζονται για το μηχάνημα μας
	OUTPUT	Εξερχόμενα πακέτα που προέρχονται από το μηχάνημα μας
	FORWARD	Πακέτα που διέρχονται από το μηχάνημα μας (περιπτώσεις routing)
Συνήθεις	ACCEPT	Αποδοχή του πακέτου
	DROP	Σιωπηλή απόρριψη του πακέτου
	REJECT	Απόρριψη του πακέτου με

Ο πίνακας **NAT** (Network Address Translation)

- Χρησιμοποιείται για τη μετάφραση εσωτερικών IP διευθύνσεων σε δημόσιες IP διευθύνσεις.
  - Αντικαθιστά τη διεύθυνση του αποστολέα ή/και παραλήπτη ενός πακέτου με κάποια άλλη ώστε να είναι δυνατή η δρομολόγησή του στο Internet.
  - Μόνο το πρώτο πακέτο μίας ροής θα περάσει από τον πίνακα NAT.
    - Αφού αποφασισθεί ο προορισμός του τα υπόλοιπα πακέτα της ροής αυτής θα ακολουθήσουν αυτόματα την ίδια διαδρομή με το πρώτο πακέτο

Πίνακας NAT: αλυσίδες και προορισμοί

Πίνακας NAT		
Build-in αλυσίδες	PREROUTING	Η μετάφραση της διεύθυνσης γίνεται πριν τη δρομολόγηση. Εφαρμόζει NAT στην IP προορισμού.
	POSTROUTING	Η μετάφραση της διεύθυνσης γίνεται μετά τη δρομολόγηση. Εφαρμόζει NAT στην IP διεύθυνση πηγής.
	OUTPUT	Πακέτα που προέρχονται από το μηχάνημα μας
Συνήθεις Προορισμοί	DNAT	Αλλαγή της διεύθυνσης προορισμού ενός πακέτου
	SNAT	Αλλαγή της διεύθυνσης αποστολέα ενός πακέτου
	MASQUERADE	Αλλαγή της διεύθυνσης αποστολέα ενός πακέτου με την διεύθυνση του interface εξόδου

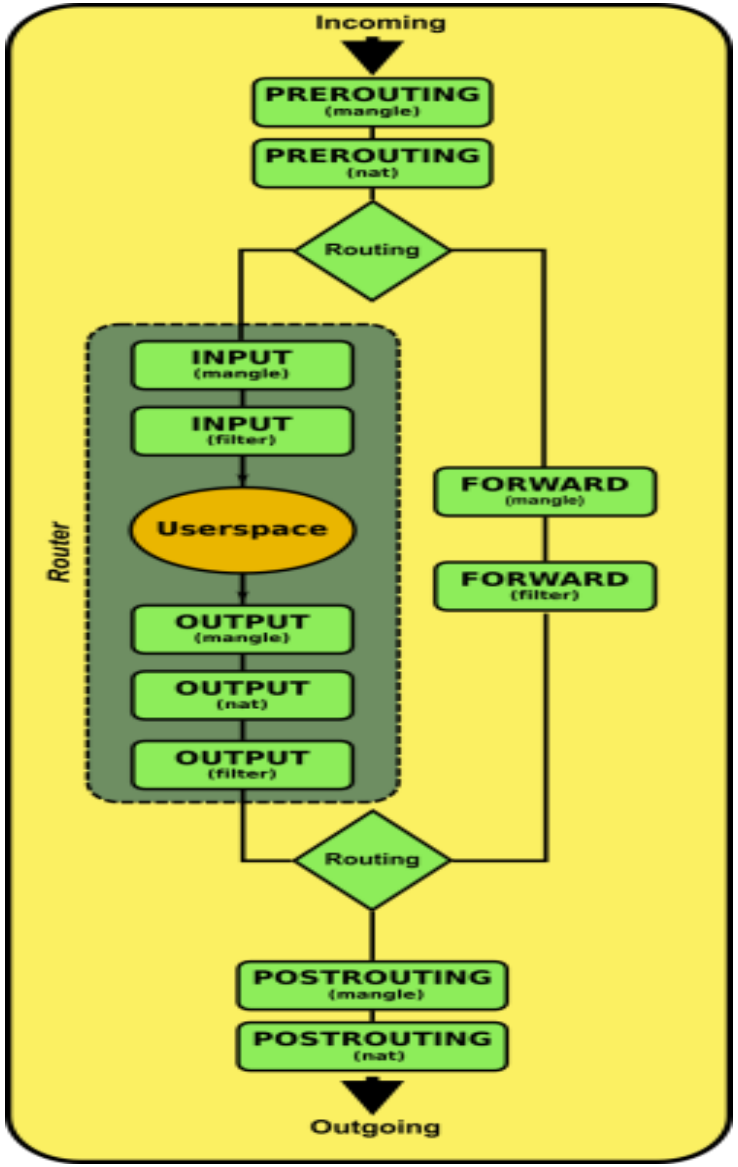
Ο πίνακας Mangle

- Χρησιμοποιείται για την αλλοίωση των χαρακτηριστικών των πακέτων για υπηρεσίες QoS.
- Μπορεί να τροποποιήσει πεδία όπως
  - TOS (Type of Service)
  - TTL (Time to Live)
- Μπορεί να «μαρκάρει» πακέτα με κάποια ειδική τιμή με σκοπό την ευκολότερη εύρεσή του.

Πίνακας Mangle: αλυσίδες και προορισμοί

Πίνακας Mangle		
Build-in αλυσίδες	INPUT	Εισερχόμενα πακέτα που προορίζονται για το μηχάνημα μας
	OUTPUT	Εξερχόμενα πακέτα που προέρχονται από το μηχάνημα μας
	FORWARD	Πακέτα που διέρχονται από το μηχάνημα μας (περιπτώσεις routing)
	PREROUTING	Εισερχόμενα πακέτα (ανεξαρτήτως αν προέρχονται από το μηχάνημα μας)
	POSTROUTING	Εξερχόμενα πακέτα (ανεξαρτήτως αν προέρχονται από το μηχάνημα μας)
Συνήθεις Προορισμοί	MARK	Μαρκάρισμα ενός πακέτου με ένα συγκεκριμένο mark
	CONNMARK	Μαρκάρισμα ολόκληρης της σύνδεσης στην οποία ανήκει το πακέτο
	TCPMSS	Αλλαγή διάφορων χαρακτηριστικών των πακέτων
	DSCP	
	TTL	
	TOS	
	ECN	

Σειρά διέλευσης πακέτων από αλυσίδες



Βασικές λειτουργίες

Κόμβοι	Ενέργεια
Linux (Kali)	**iptables –L**
	Προβάλει τις λίστες (αλυσίδες) κανόνων
	iptables –L –v
	Προβάλει τις λίστες με περισσότερες λεπτομέρειες
	iptables –A <CHAIN_NAME> : Προσθήκη κανόνα στο τέλος
	iptables -I <CHAIN_NAME> <rule_number> : Προσθήκη κανόνα στη θέση rule_number
	iptables -D <CHAIN_NAME> <rule_number> : Διαγραφή κανόνα στη θέση rule_number
	iptables -R <CHAIN_NAME> <rule_number> «νέος κανόνας» : Αντικατάσταση του κανόνα στη θέση rule_number με το νέο κανόνα
	iptables -F <CHAIN_NAME> : Διαγραφή όλων των κανόνων
	iptables -N <CHAIN_NAME> : Δημιουργία νέας λίστας
	iptables -X <CHAIN_NAME> : Διαγραφή κενής λίστας

Έγκριση κίνησης σε συγκεκριμένη πόρτα

Κόμβοι	**Ενέργεια**
Linux (Kali)	**iptables -A INPUT -p tcp --dport 80 -j ACCEPT**
	Επιτρέπει εισερχόμενη tcp κίνηση στο port 80 (default web port)
	iptables -A INPUT -p tcp --dport ssh -j ACCEPT
	Επιτρέπει εισερχόμενη tcp κίνηση στο default ssh port (δηλαδή στο 22)
	-A INPUT : προσθήκη του κανόνα στην αλυσίδα INPUT
	-p tcp: ο κανόνας ισχύει μόνο για TCP συνδέσεις
	-dport ssh: ο κανόνας ισχύει μόνο για την πόρτα του SSH (22)
	-j ACCEPT: εφόσον ισχύουν όλα τα παραπάνω, επιτρέπεται η πρόσβαση

Απαγόρευση κίνησης

Κόμβοι	**Ενέργεια**
Linux (Kali)	
	iptables -A INPUT -j DROP
	iptables -L
	Πρόβλημα διαμόρφωσης: απαγορεύει την κίνηση και για το loopback port.
	Πιθανή λύση: **iptables -A INPUT -i eth0 -j DROP**
	Ισχύει μόνο για το interface eth0

Εισαγωγή κανόνα σε συγκεκριμένη θέση

Κόμβοι	**Ενέργεια**
Linux (Kali)	
	iptables -I INPUT 1 -i lo -j ACCEPT
	-i lo: Επιτρέπει εισερχόμενη κίνηση εφόσον το interface είναι το loopback
	-I INPUT 1: γίνεται ο πρώτος κανόνας της αλυσίδας
	Πολύ χρήσιμος κανόνας για προγράμματα που χρησιμοποιούν το loopback interface
	iptables -L
	iptables -L -v

Διαγραφή κανόνα

Κόμβοι	Ενέργεια
Linux (Kali)	
	iptables -D INPUT 4
	Διαγραφή του 4ου κανόνα
	iptables -L
	iptables -L -v

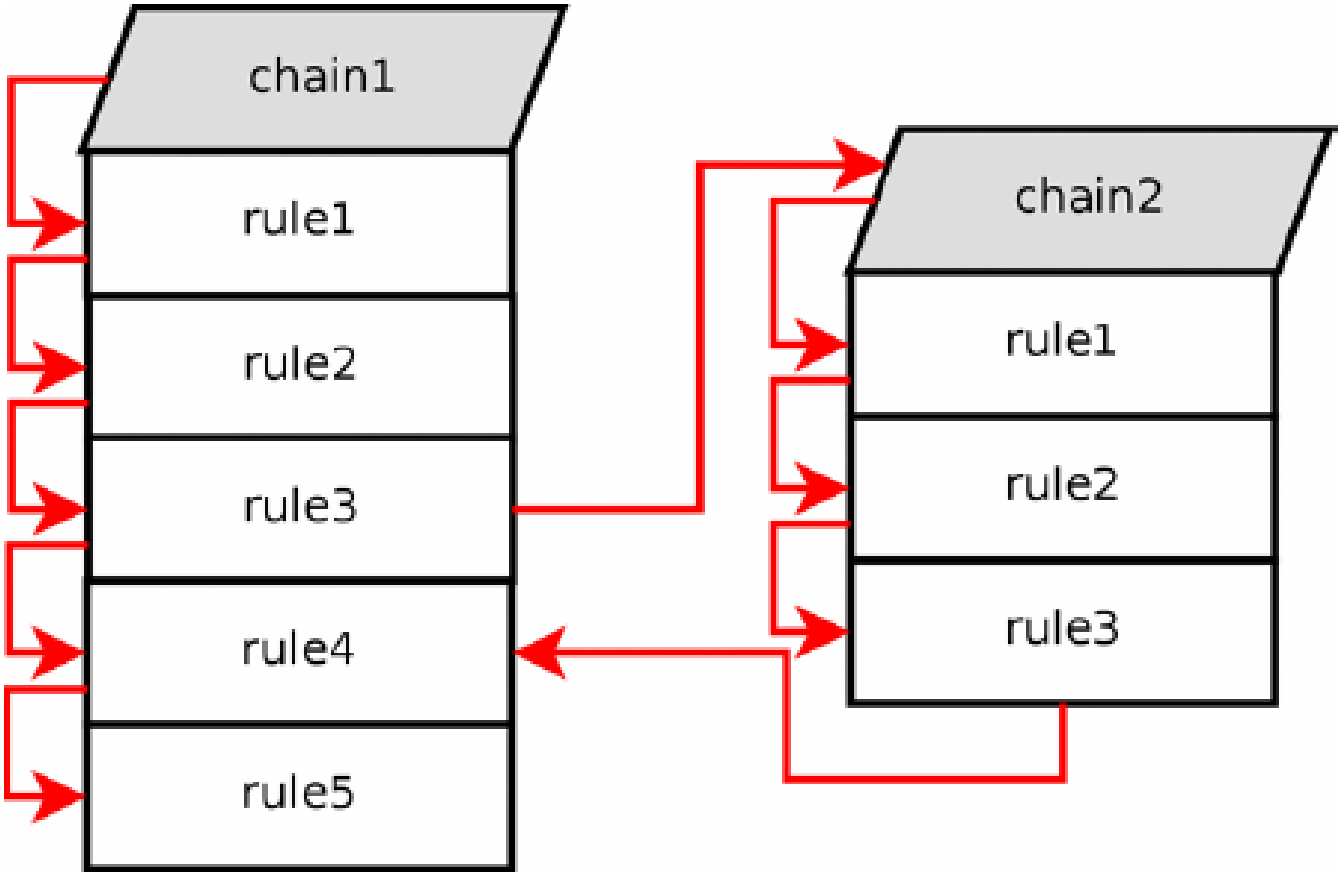
Καταγραφή κίνησης (logging)

Κόμβοι	**Ενέργεια**
Linux (Kali)	
	iptables -I INPUT 4 -m limit --limit 5/min -j LOG --log-prefix "iptables denied: " --log-level 7
	-m limit --limit 5/min: Ο κανόνας εφαρμόζεται με συχνότητα 5 φορές/λεπτό
	--log-level 7: επίπεδο καταγραφής syslog
	iptables -L
	iptables -L -v

Λεπτομερής καταγραφή κίνησης

Κόμβοι	Ενέργεια
Linux (Kali)	**iptables –N LOGNDROP**
	iptables -A INPUT -j LOGNDROP
	iptables -A LOGNDROP -p tcp -m limit --limit 5/min -j LOG --log-prefix "Denied TCP: " --log-level 7
	iptables -A LOGNDROP -p udp -m limit --limit 5/min -j LOG --log-prefix "Denied UDP: " --log-level 7
	iptables -A LOGNDROP -p icmp -m limit --limit 5/min -j LOG --log-prefix "Denied ICMP: " --log-level 7
	iptables -A LOGNDROP -j DROP
	Η αλυσίδα LOGNDROP είναι καινούρια. Αντί για DROP στο τέλος της αλυσίδα INPUT, υπάρχει η LOGNDROP.
	Η αλυσίδα LOGNDROP προσθέτει λεπτομέρειες στην καταγραφή και στο τέλος της αλυσίδας, εφόσον έχει πραγματοποιηθεί η καταγραφή, η κίνηση γίνεται DROP.

Σύνδεση αλυσίδων



Έγκριση εγκαταστημένων συνδέσεων (sessions) – Statefull inspection

Κόμβοι	Ενέργεια
Linux (Kali)	
	iptables –L
	iptables -I INPUT 2 -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
	iptables -I INPUT 2 -m state --state ESTABLISHED,RELATED -j ACCEPT Επιτρέπει στα ήδη εγκατεστημένα sessions να λαμβάνουν κίνηση

Αποθήκευση iptables

Κόμβοι	**Ενέργεια**
Linux (Kali)	**iptables-save > /etc/iptables.rules :** Αποθήκευση κανόνων
	Για την ενεργοποίηση των κανόνων υπάρχουν δύο εναλλακτικές:
	Α) Πραγματοποίηση αλλαγών στο /etc/network/interfaces
	Β) Προσθήκη scripts στα /etc/network/if-pre-up.d/ και /etc/network/if-post-down.d/

1η λύση: /etc/network/interfaces

Κόμβοι	Ενέργεια
Linux (Kali)	**iwconfig :** Προβολή των interfaces (συνήθως eth0)
	Επεξεργασία του αρχείου **/etc/network/interfaces**
	Προσθήκη στο τέλος των εντολών για το interface: **pre-up iptables-restore < /etc/iptables.rules**
	Μπορούν να ετοιμαστούν κανόνες και για τερματισμό (down rules) στο αρχείο **/etc/iptables.downrules**
	post-down iptables-restore </etc/iptables.downrules

2η λύση: /etc/network/if-pre-up.d και /etc/network/ifpost-down

Κόμβοι	Ενέργεια
Linux (Kali)	Το script /etc/network/if-pre-up.d/iptablesload θα περιλαμβάνει: **!bin/sh** **ip-table-restore < /etc/iptables.rules** **exit 0**
	Το script /etc/network/if-pre-up.d/iptablesload θα περιλαμβάνει: **!/bin/sh** **if [-f /etc/iptables.downrules]; then** **iptables-restore < /etc/iptables.downrules** **fi** **iptables-save -c > /etc/iptables.rules** **exit 0**
	chmod +x /etc/network/if-post-down.d/iptablessave **chmod +x /etc/network/if-pre-up.d/iptablesload** Δίνουν δικαιώματα εκτέλεσης στα scripts

Απόρριψη κίνησης με βάση την IP διεύθυνση

Κόμβοι	**Ενέργεια**
Επιτιθέμενος:	**nmap -iflist**
	nmap –e eth0 –PN "victim_IP"
Στόχος	**iptables -I INPUT 5 –s "attacker_IP" -j LOGNDROP**
	-s IP_X: όπου η source IP είναι η IP_X

Αποθήκευση iptables logs σε αρχείο

Κόμβοι	**Ενέργεια**
Linux (Kali)	**ls /etc/syslog.conf**
	Προβολή αρχείου **/etc/syslog.conf**
	Για αποθήκευση σε ξεχωριστό αρχείο, προσθήκη στο syslog.conf της εντολής: **kern.warning /var/log/iptables.log**
	Επανεκκίνηση syslogd: **/etc/init.d/sysklogd restart**

9. Παράδειγμα υλοποίησης Πολιτικής Ασφάλειας Δικτύου

Περιγραφή υπηρεσιών δικτύου (1)

- Καθορισμός παρεχόμενων **εξωτερικών** υπηρεσιών:
  - Υπηρεσίες web, email και VPN.
    - Ο web server υποστηρίζει τα πρωτόκολλα **http (80)** και **https (443)** .
    - Ο mail server υποστηρίζει πρωτόκολλα **smtp (25)** και **imap**.
    - Ο web server και ο mail server είναι προσβάσιμοι και από τους εσωτερικούς κόμβους του δικτύου.

Περιγραφή υπηρεσιών δικτύου (2)

- Καθορισμός παρεχόμενων **εσωτερικών** υπηρεσιών:
  - Υπηρεσίες application server, database server και print server.
    - Ο application server είναι προσβάσιμος μέσω του πρωτοκόλλου **http** στη θύρα **8080**.
    - Ο database server είναι PostgereSQL και είναι προσβάσιμος στην θύρα **5432**.
    - Ο print server είναι προσβάσιμος μέσω του πρωτοκόλλου **lpd**.

Οριοθέτηση περιοχών δικτύου (1)

Το δίκτυο χωρίζεται σε 3 ζώνες:

1. Demilitarized Zone (DMZ) (192.168.0.0/24)

- Στο DMZ τοποθετούνται οι web, mail και vpn servers, καθώς και ένας HTTP proxy. Αναλυτικά:
  - 192.168.0.1 Firewall 1 (default gateway)
  - 192.186.0.2 Firewall 2
  - 192.168.0.25 Mail Server
  - 192.186.0.80 HTTP Server
  - 192.168.0.81 HTTP Proxy

Οριοθέτηση περιοχών δικτύου (2)

2. Internal Trusted Zone (10.1.1.0/24)

- Στην εσωτερική ζώνη του δικτύου τοποθετούνται οι application, database και print servers. Αναλυτικά:
  - 10.1.1.1 Firewall 3 (default gateway)
  - 10.1.1.10 Print Server
  - 10.1.1.11 Application Server
  - 10.1.1.12 Database Server

Οριοθέτηση περιοχών δικτύου (3)

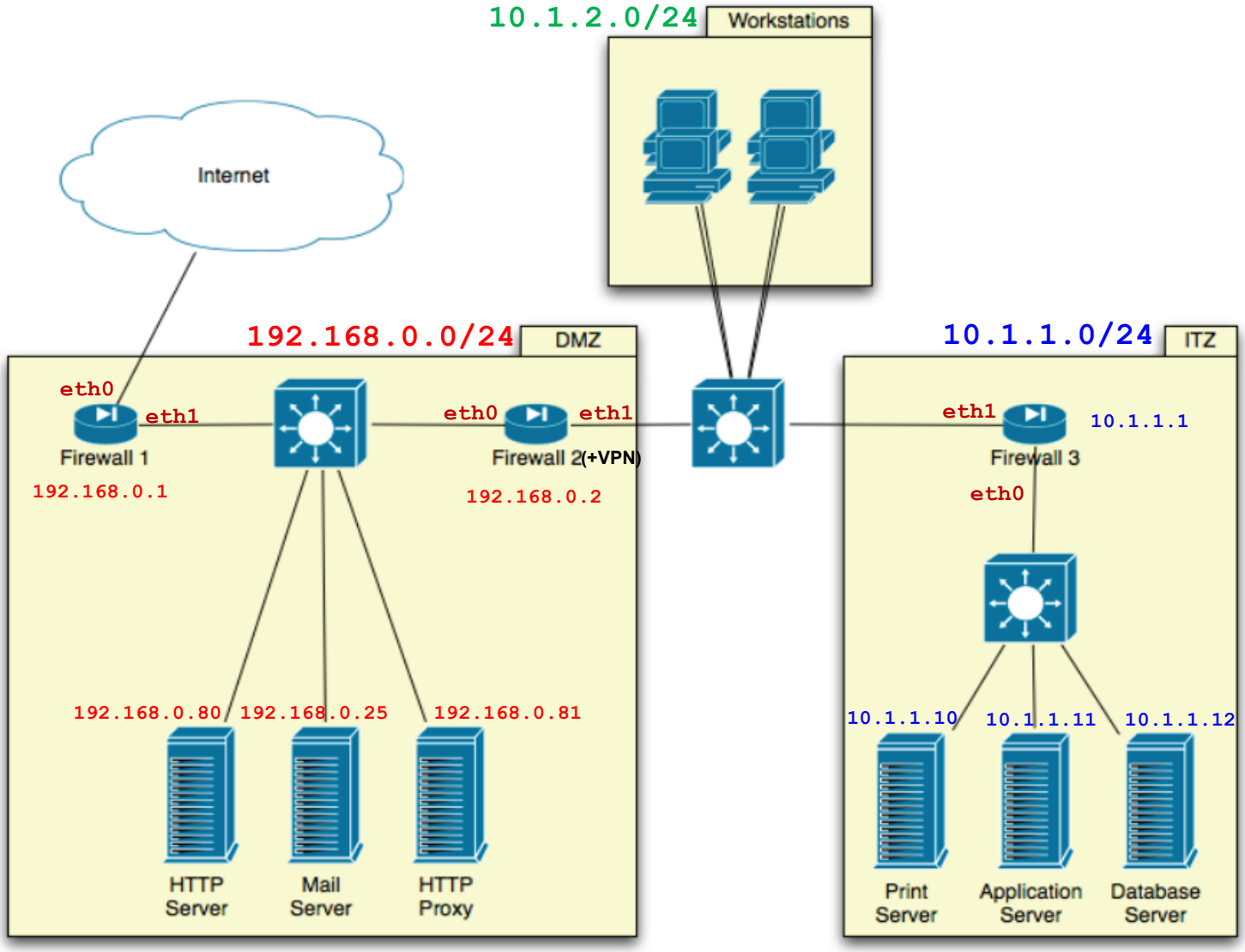
3. Εσωτερικό υποδίκτυο workstations (10.1.2.0/24)

- Στην εσωτερική ζώνη του δικτύου τοποθετούνται οι application, database και print servers. Αναλυτικά:
  - 10.1.0.1 Firewall 2 (default gateway)
  - 10.1.1.1 Firewall 3
  - 10.1.2.1-255 Workstations

(4. Εξωτερικό δίκτυο)

Το firewall 1 ελέγχει την κίνηση προς και από αυτό

Διάγραμμα δικτύου



Καθορισμός Πολιτικής Πρόσβασης για κάθε περιοχή (1)

1. Demilitarized Zone (DMZ)

1) Επιτρέπεται εισερχόμενη κίνηση στις θύρες 80 και 443 του web server.
2) Επιτρέπεται εισερχόμενη κίνηση στις θύρες 25 και 443 του mail server.
3) Επιτρέπεται εισερχόμενη κίνηση πρωτοκόλλου esp στην θύρα 500, προς το firewall 2.
4) Επιτρέπεται εισερχόμενη κίνηση προς το firewall 2 η οποία έχει γίνει established, ώστε να καταλήξει στα workstations.
5) Επιτρέπεται εξερχόμενη κίνηση από τον HTTP Proxy από τις θύρες 80 και 443.
6) Επιτρέπεται εξερχόμενη κίνηση από τον mail server από τη θύρα 25.
7) Επιτρέπεται εξερχόμενη κίνηση από τους mail και web server αν είναι established (ως απαντήσεις σε http, https και smtp requests).
8) Όλη η υπόλοιπη κίνηση απορρίπτεται.

Καθορισμός Πολιτικής Πρόσβασης για κάθε περιοχή (2)

2. Internal Trusted Zone

1) Εισερχόμενη κίνηση επιτρέπεται μόνο από το εσωτερικό τοπικό υποδίκτυο (Workstations) προς τους print και application servers.
2) Εξερχόμενη κίνηση επιτρέπεται μόνο από τον application server προς το τοπικό υποδίκτυο (Workstations), αν και μόνο αν πρόκειται για απάντηση ήδη established σύνδεσης.
3) Ο database server μπορεί να προσπελασθεί (και να απαντήσει) μόνο από τον application server.
4) Κάθε άλλη κίνηση απορρίπτεται.

Καθορισμός Πολιτικής Πρόσβασης για κάθε περιοχή (3)

3. Εσωτερικό δίκτυο Workstations

1) Επιτρέπονται οι εισερχόμενες συνδέσεις πρωτοκόλλου esp και οι συνδέσεις στην θύρα 500 από το Firewall 2 για το ipsec και το vpn.
2) Επιτρέπονται οι ήδη established συνδέσεις από και προς το Internal Trusted Zone.
3) Επιτρέπονται οι ήδη established συνδέσεις με τους web και mail servers του DMZ
4) Επιτρέπονται οι ήδη estabilished συνδέσεις με εξωτερικούς web servers.
5) Επιτρέπονται εξερχόμενη κίνηση από το δίκτυο Workstations προς τον Print server και τον application server (που βρίσκονται στο Internal Trusted Zone). Οι εξερχόμενες συνδέσεις στις θύρες 515 και 8080 επιτρέπονται και δρομολογούνται προς το firewall 3 ώστε να καταλήξουν στους print και application servers αντίστοιχα.
6) Επιτρέπονται εξερχόμενες συνδέσεις προς τις θύρες 80 και 443 του HTTP Proxy (στο DMZ) ώστε να ελέγχεται η περιήγηση των χρηστών του δικτύου.
7) Οι εξερχόμενες συνδέσεις στις θύρες 25 και 143 δρομολογούνται στον mail server (στο DMZ).
8) Οι εξερχόμενες συνδέσεις στις θύρες 20 και 21 δρομολογούνται στο firewall 1 ώστε να καταλήξουν στο εξωτερικό δίκτυο.
9) Οποιαδήποτες άλλη κίνηση απορρίπτεται.

Διαμόρφωση Firewall 1

#eth0: internet, eth1: DMZ

#nat eth1

iptables -t nat -A POSTROUTING -s 192.168.0.0/24 -i eth1 -j MASQUERADE

#allow incoming connections from the internet to ports 80, 443 (http, https) and forward them to the HTTP Server

iptables -A FORWARD -s 0/0 -i eth0 -d 192.168.0.80 -o eth1 -p TCP --dport 80 -j ACCEPT

iptables -A FORWARD -s 0/0 -i eth0 -d 192.168.0.80 -o eth1 -p TCP --dport 443 -j ACCEPT

#allow incoming connections from the internet to ports 25, 143 (smtp, imap) and forward them to the Mail Server

iptables -A FORWARD -s 0/0 -i eth0 -d 192.168.0.25 -o eth1 -p TCP --dport 25 -j ACCEPT

iptables -A FORWARD -s 0/0 -i eth0 -d 192.168.0.25 -o eth1 -p TCP --dport 443 -j ACCEPT

#allow incoming esp connections from the internet (for ipsec)

iptables -A FORWARD -s 0/0 -i eth0 -d 192.168.0.2 -o eth1 -p esp -j ACCEPT

#allow incoming connections from the internet to port 500 (isakmp; for vpn)

iptables -A FORWARD -s 0/0 -i eth0 -d 192.168.0.2 -o eth1 --sport 500 --dport 500 -j ACCEPT

#allow all incoming connections if established

iptables -A FORWARD -s 0/0 -i eth0 -d 192.168.0.2 -o eth1 -m state --state ESTABLISHED,RELATED -j ACCEPT

#allow outgoing connections from the internal network to ports 20, 21 (ftp data, ftp cmd) and forward them to the internet

iptables -A FORWARD -s 192.168.0.2 -i eth1 -d 0/0 -o eth0 -p tcp --dport 20 -j ACCEPT

iptables -A FORWARD -s 192.168.0.2 -i eth1 -d 0/0 -o eth0 -p tcp --dport 21 -j ACCEPT

#allow outgoing connections from the HTTP proxy to ports 80, 443 (http, https) and forward them to the internet

iptables -A FORWARD -s 192.168.0.81 -i eth1 -d 0/0 -o eth0 -p tcp --dport 80 -j ACCEPT

iptables -A FORWARD -s 192.168.0.81 -i eth1 -d 0/0 -o eth0 -p tcp --dport 443 -j ACCEPT

#allow outgoing connections from the Mail Server to port 25

iptables -A FORWARD -s 192.168.0.25 -i eth1 -d 0/0 -o eth0 -p tcp --dport 25

#allow outgoing connections from the Http Server if established (for HTTP responses)

iptables -A FORWARD -s 192.168.0.80 -i eth1 -d 0/0 -o eth0 -p tcp -m state --state ESTABLISHED,RELATED -j ACCEPT

#allow outgoing connections from the Mail Server if established (for IMAP responses)

iptables -A FORWARD -s 192.168.0.25 -i eth1 -d 0/0 -o eth0 -p tcp -m state --state ESTABLISHED,RELATED -j ACCEPT

#drop everything else

iptables -A FORWARD -drop

Διαμόρφωση Firewall 2

#eth0: DMZ, eth1: LAN

#nat eth1

iptables -t nat -A POSTROUTING -s 10.1.2.0/24 -i eth1 -j MASQUERADE

#allow and handle incoming esp connections from the internet (for ipsec)

iptables -A INPUT -s 192.168.0.1 -i eth0 -p esp -j ACCEPT

#allow and handle incoming connections from the internet to port 500 (isakmp; for vpn)

iptables -A INPUT -s 192.168.0.1 -i eth0 --sport 500 --dport 500 -j ACCEPT

#allow all incoming connections if established

iptables -A FORWARD -s 0/0 -i eth0 -d 10.1.2.0/24 -o eth1 -p tcp -m state --state ESTABLISHED,RELATED -j ACCEPT

#allow outgoing connections from the workstation LAN to ports 20, 21 (ftp data, ftp cmd) and forward them to firewall 1

iptables -A FORWARD -s 10.1.2.0/24 -i eth1 -d 192.168.0.1 -o eth0 -p tcp --dport 20 -j ACCEPT

iptables -A FORWARD -s 10.1.2.0/24 -i eth1 -d 192.168.0.1 -o eth0 -p tcp --dport 21 -j ACCEPT

#allow outgoing connections from the workstation LAN to ports 80, 443 (http, https) and forward them to the HTTP Proxy

iptables -A FORWARD -s 10.1.2.0/24 -i eth1 -d 192.168.0.81 -o eth0 -p tcp --dport 80 -j ACCEPT

iptables -A FORWARD -s 10.1.2.0/24 -i eth1 -d 192.168.0.81 -o eth0 -p tcp --dport 443 -j ACCEPT

#allow outgoing connections from the workstation LAN to ports 25, 143 (smtp, imap) and forward them to the Mail Server

iptables -A FORWARD -s 10.1.2.0/24 -i eth1 -d 192.168.0.25 -p tcp --dport 25 -j ACCEPT

iptables -A FORWARD -s 10.1.2.0/24 -i eth1 -d 192.168.0.25 -p tcp --dport 143 -j ACCEPT

#allow outgoing connections from the workstation LAN to ports 515, 8080 (LPD, HTTP) and forward them to the firewall 3

iptables -A FORWARD -s 10.1.2.0/24 -i eth1 -d 10.1.1.1 -p tcp --dport 515 -j ACCEPT

iptables -A FORWARD -s 10.1.2.0/24 -i eth1 -d 10.1.1.1 -p tcp --dport 8080 -j ACCEPT

#drop everything else

iptables -A FORWARD -drop

Διαμόρφωση Firewall 3

#nat eth0

iptables -t nat -A POSTROUTING -s 10.1.1.0/24 -i eth0 -j MASQUERADE

#allow incoming connections from the workstation LAN to port 515 (LPD) and forward them to the print server

iptables -A FORWARD -s 10.1.2.0/24 -i eth0 -d 10.1.1.10 -o eth1 -p tcp --dport 515 -j ACCEPT

#allow incoming connections from the workstation LAN to port 8080 (HTTP) and forward them to the application server

iptables -A FORWARD -s 10.1.2.0/24 -i eth0 -d 10.1.1.11 -o eth1 -p tcp --dport 8080 -j ACCEPT

#allow incoming concoctions from the application server to port 5432 (PostgreSQL) and forward them to the database server

iptables -A FORWARD -s 10.1.1.11 -i eth1 -d 10.1.1.12 -o eth1 -p tcp --dport 5432 -j ACCEPT

#allow incoming concoctions from the database server to port 5432 (PostgreSQL) and forward them to the application server

iptables -A FORWARD -s 10.1.1.12 -i eth1 -d 10.1.1.11 -o eth1 -p tcp --dport 5432 -j ACCEPT

#allow established outgoing connections from the application server and forward them to the workstation LAN

iptables -A FORWARD -s 10.1.1.11 -i eth1 -d 10.1.2.0/24 -o eth0 -p tcp -m state --state ESTABLISHED,RELATED -j ACCEPT

#drop everything else

iptables -A FORWARD -drop

Πηγές

1. Stallins William. (2011). Cryptography and Network Security: Principles and Practice. USA: Pearson Education, Inc.
2. NIST Special Publication 800-41, "Guidelines on Firewalls and Firewall Policy", http://csrc.nist.gov/publications/nistpubs/800-41-Rev1/sp800-41-rev1.pdf
3. The netfilter iptables project, http://www.netfilter.org/projects/iptables/index.html
4. Iptables manpage, http://ipset.netfilter.org/iptables.man.html
5. Οδηγός για την χρήση των Iptables: http://www.yolinux.com/TUTORIALS/LinuxTutorialIptablesNetworkGateway.html