Εργαστηριακή Άσκηση 10
Τείχη προστασίας (Firewalls) και NAT

Firewall (Τείχος Προστασίας)

Η ορολογία firewall προέκυψε από την επιστήμη των πολιτικών και μηχανολόγων μηχανικών, όπου κατασκευάζονται τοίχοι ή μεταλλικές κατασκευές για τον περιορισμό πυρκαγιάς σε κτήρια, σε αυτοκίνητα και σε διάφορες άλλες κατασκευές. Στους υπολογιστές αναφέρεται σε συστήματα σχεδιασμένα να αποτρέπουν τη μη εξουσιοδοτημένη πρόσβαση από και προς δίκτυα. Ειδικά στην εποχή του Internet κάτι τέτοιο είναι απολύτως απαραίτητο, καθώς στα Intranet (εσωτερικά δίκτυα) πρέπει τις περισσότερες φορές να υπάρχει περιορισμένη πρόσβαση από εξωτερικά μη εξουσιοδοτημένα δίκτυα. Τα τείχη προστασίας τοποθετούνται ανάμεσα σε δίκτυα (in-line) ώστε να περνάει όλη η κίνηση μέσα από αυτά και να ελέγχεται. Το τείχος προστασίας ενός δικτύου χτίζει μια «ελεγχόμενη γέφυρα» μεταξύ του εσωτερικού δικτύου ή υπολογιστή που προστατεύει και ενός εξωτερικού δικτύου, όπως το Internet, που θεωρείται ότι είναι ανασφαλές και αναξιόπιστο.

Η πρώτη γενιά τειχών ονομάστηκε “packet-filters” και η δομή ελέγχου σε πρώιμη μορφή ονομάστηκε (Access Control List – ACL). Τα φίλτρα πακέτων ελέγχουν με βάση προ-ρυθμισμένους κανόνες τα πακέτα που διέρχονται από μέσα τους και εάν κάποιο πακέτο δεν είναι σύμφωνο με τους κανόνες αυτούς απορρίπτεται (silent discard) ή αποβάλλεται (reject) στέλνοντας στον αποστολέα μήνυμα λάθους ICMP. Ο μηχανισμός ελέγχου ACL παρέχει κάποια βασική προστασία πρόσβασης, αλλά δεν μπορεί να κατανοήσει την έννοια της ροής δεδομένων και δεν ξέρει εάν κάποιο πακέτο συμμετέχει σε ήδη υπάρχουσα σύνδεση (stateless). Ελέγχει αυτόνομα κάθε πακέτο, με ορίσματα είτε τα πεδία της επικεφαλίδας IP είτε της επικεφαλίδας των πρωτοκόλλων ελέγχου (ICMP) είτε τα πεδία του πρωτοκόλλου μεταφοράς (TCP, UDP κλπ), λειτουργεί δηλαδή μέχρι τα πρώτα 3 επίπεδα του μοντέλου OSI.

Με την εξάπλωση του Internet και τη χρήση των πρωτοκόλλων TCP/IP έγινε απαραίτητη η κατασκευή δεύτερης γενιάς τειχών προστασίας με δυνατότητα λειτουργίας στο επίπεδο 4 του μοντέλου OSI. Αυτά ονομάζονται stateful και λειτουργούν ελέγχοντας πολλαπλά πακέτα ώστε να μπορούν να πάρουν αποφάσεις με βάση τις συνδέσεις, δηλαδή, το κατά πόσο κάποιο πακέτο είναι μέρος νέας ή κάποιας υπάρχουσας σύνδεσης. Ελέγχονται για παράδειγμα τα πεδία της επικεφαλίδας TCP (TCP flags SYN/ACK/RST/FIN) και παρακολουθείται η κατάσταση των ανοικτών συνδέσεων.

Σήμερα, σχεδόν όλα τα τείχη προστασίας που χρησιμοποιούνται είναι πλέον stateful. Χρησιμοποιούνται εκτενώς ως πρώτη γραμμή άμυνας για την αύξηση της ασφάλειας υπολογιστών και δικτύων προστατεύοντας την ιδιωτικότητα και ευαίσθητα δεδομένα και υποδομές. Αποτελούν εξέλιξη της τεχνικής φιλτραρίσματος πακέτων. Εκτός από τον έλεγχο πακέτων στο στρώμα μεταφοράς (transport) μπλοκάρουν και όλα τα πακέτα τα οποία δεν μπορούν να περάσουν επιτυχώς ένα έλεγχο κατάστασης (Stateful Packet Inspection – SPI). Σε αυτό τον έλεγχο το τείχος προστασίας, αντί να καταγράφει απλά τα πακέτα, προσπαθεί να αποτυπώσει τις επιχειρούμενες συνδέσεις. Με αυτό τον τρόπο καταγράφει όλες τις συνδέσεις που διέρχονται από αυτό και καθορίζει αν ένα πακέτο είναι η αρχή μιας νέας σύνδεσης, ένα μέρος από υπάρχουσα σύνδεση, ή αν δεν ανήκει σε καμία σύνδεση. Οι νέοι κανόνες μπορούν να περιέχουν πλέον την κατάσταση της σύνδεσης ως ένα από τα κριτήρια των ελέγχων τους.

Με αυτό τον τρόπο τα τείχη προστασίας μπορούν να ανταπεξέλθουν σε επιθέσεις DoS (Denial-of-Service) οι οποίες συνήθως βομβαρδίζουν τις πύλες εισόδου σε δίκτυα με χιλιάδες πλαστά πακέτα σύνδεσης, σε μια προσπάθεια να συντρίψουν το υποψήφιο θύμα καταναλώνοντας την μνήμη και

τους υπολογιστικούς πόρους που απαιτούνται ώστε ο εκάστοτε δικτυακός κόμβος (τερματικός σταθμός ή πύλη) να διατηρεί τις συνδέσεις του ανοικτές.

DMZ (demilitarized zone)[1]

Σε ένα δίκτυο υπολογιστών, οι σταθμοί που είναι πιο ευάλωτοι σε επιθέσεις είναι εκείνοι που για να παρέχουν υπηρεσίες σε χρήστες, όπως e-mail, web και Domain Name System (DNS), πρέπει να είναι προσβάσιμοι από το διαδίκτυο. Εξ αιτίας αυτού του αυξημένου κινδύνου τοποθετούνται συνήθως σε ξεχωριστό υπο-δίκτυο. Το τείχος προστασίας ελέγχει την κίνηση μεταξύ των εξυπηρετητών της περιοχής DMZ και των εσωτερικών σταθμών του δικτύου. Σε περίπτωση που ένας εισβολέας κατόρθωνε να αποκτήσει πρόσβαση σε κάποιον από αυτούς, το υπόλοιπο δίκτυο δεν θα εκτεθεί. Οι εξυπηρετητές σε ένα DMZ έχουν περιορισμένη συνδεσιμότητα με το εσωτερικό δίκτυο, παρόλο που η επικοινωνία με άλλους εξυπηρετητές στο DMZ και το εξωτερικό δίκτυο επιτρέπεται. Αυτό επιτρέπει την παροχή υπηρεσιών τόσο για το εσωτερικό δίκτυο όσο και έξω από αυτό.

NAT – Network Address Translation

Ένας από τους μηχανισμούς για την αντιμετώπιση της εξάντλησης διευθύνσεων IPv4 είναι η χρήση ιδιωτικών δικτύων. Υπάρχουν πολλές περιπτώσεις όπου οι υπολογιστές αρκεί να επικοινωνούν με τους ομόλογούς τους εντός ενός δικτύου και σπανίως απαιτείται πρόσβαση στο «δημόσιο» διαδίκτυο. Για τον σκοπό αυτό στο εσωτερικό του δικτύου μπορούν χρησιμοποιούνται ιδιωτικές διευθύνσεις (private addresses), όπως καθορίζονται στο RFC 1918. Προβλέπονται 3 κατηγορίες ιδιωτικών διευθύνσεων (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16). Οι ιδιωτικές διευθύνσεις **δεν** εμφανίζονται στο δημόσιο διαδίκτυο. Σε περίπτωση που κάποιος από το ιδιωτικό του δίκτυο χρειάζεται να συνδεθεί με το διαδίκτυο απαιτείται ένας μηχανισμός αντιστοίχησης μεταξύ ιδιωτικών και δημόσιων διευθύνσεων. Η τεχνική της μετάφρασης δικτυακών διευθύνσεων (Network Address Translation – NAT) δίνει τη λύση. Σε ορισμένες περιπτώσεις ο μηχανισμός NAT μπορεί να θεωρηθεί και ως μηχανισμός ασφαλείας επειδή λειτουργεί σαν μεταμφίεση (masquerade) όπως θα δούμε παρακάτω.

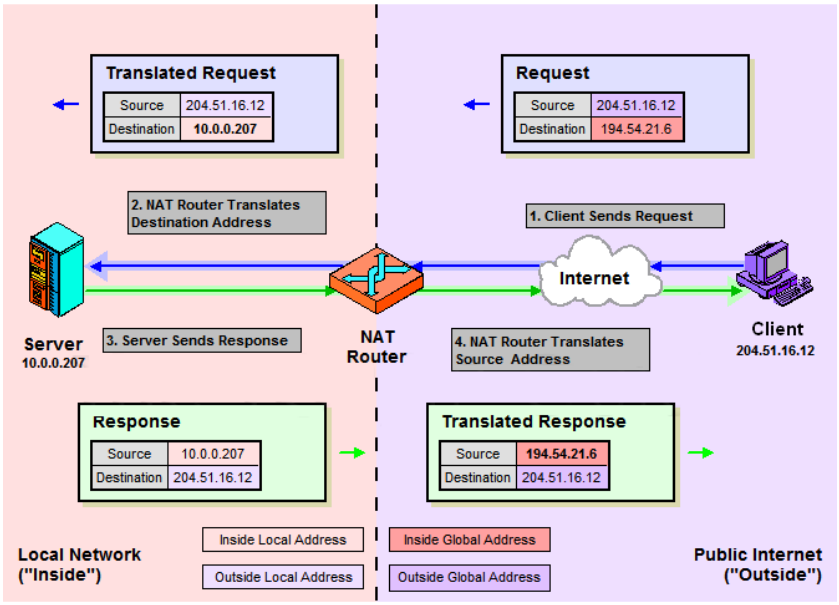
Η βασική ιδέα της μετάφρασης διευθύνσεων δικτύου (RFC 2663) είναι απλή[2]. Μια δικτυακή συσκευή, ο δρομολογητής NAT, δρα ως πύλη μεταξύ του διαδικτύου και του εσωτερικού δικτύου μεταφράζοντας τις εσωτερικές διευθύνσεις IP σε δημόσιες διευθύνσεις IP. Ουσιαστικά κρύβει όλο το εσωτερικό δίκτυο και το κάνει να εμφανίζεται στον υπόλοιπο κόσμο ως μία συσκευή. Το NAT είναι διαφανές όσον αφορά τις εσωτερικές συσκευές. Δεν απαιτούνται ιδιαίτερες ρυθμίσεις για αυτές, πλην του ορισμού του δρομολογητή NAT ως προκαθορισμένης πύλης.

Στην πιο απλή εκδοχή (Basic NAT), ο δρομολογητής NAT αντικαθιστά την IP διεύθυνση αποστολέα (source) κάθε εξερχόμενου πακέτου με τη διεύθυνση IP του NAT. Διατηρεί δε ένα πίνακα μετατροπής με τις αντιστοιχίες για κάθε μετατρεπόμενο ζεύγος διευθύνσεων. Οι μακρινοί host απαντούν χρησιμοποιώντας τη δημόσια διεύθυνση IP του NAT ως διεύθυνση προορισμού. Στα εισερχόμενα πακέτα αντικαθιστάται η διεύθυνση IP NAT στο πεδίο προορισμού κάθε πακέτου με την ιδιωτική IP διεύθυνση πηγής που διατηρείται στον πίνακα του δρομολογητή NAT.

Η λειτουργία αυτή είτε στη στατική είτε στη δυναμική εκδοχή της δεν είναι συνήθης για τα μικρά οικιακά δίκτυα. Στο Inbound NAT, η κεντρική ιδέα είναι να επιτρέπεται η πρόσβαση σε συγκεκριμένους υπολογιστές του εσωτερικού δικτύου από το διαδίκτυο χρησιμοποιώντας δημόσιες διευθύνσεις IP, όπως φαίνεται στο ακόλουθο σχήμα.

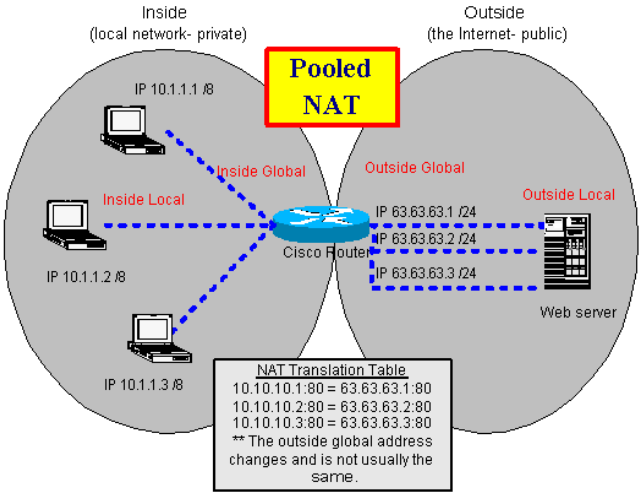
[1] Το όνομα DMZ προέρχεται από την στρατιωτική ορολογία. Είναι ο χώρος μεταξύ δύο αντιμαχομένων στον οποίο δεν επιτρέπεται οποιαδήποτε στρατιωτική επιχείρηση.

[2] Για μια πιο αναλυτική περιγραφή δείτε http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_7-3/anatomy.html).



Inbound NAT

Στο δυναμικό NAT (dynamic NAT) πολλαπλοί ιδιωτικοί σταθμοί[3] μοιράζονται μια σαφώς μικρότερη λίστα διευθύνσεων (address pool). Σε αυτό τον τρόπο λειτουργίας δημιουργούνται δυναμικά αντιστοιχήσεις (mapping) οι οποίες διατηρούνται από το NAT για περιορισμένο χρονικό διάστημα. Εάν δεν υπάρχουν πακέτα που χρησιμοποιούν την αντιστοίχηση μέσα σε ένα ορισμένο χρονικό παράθυρο, τότε η αντιστοίχηση αφαιρείται από το NAT και η δημόσια διεύθυνση επιστρέφεται στη λίστα των διαθέσιμων δημόσιων διευθύνσεων NAT.

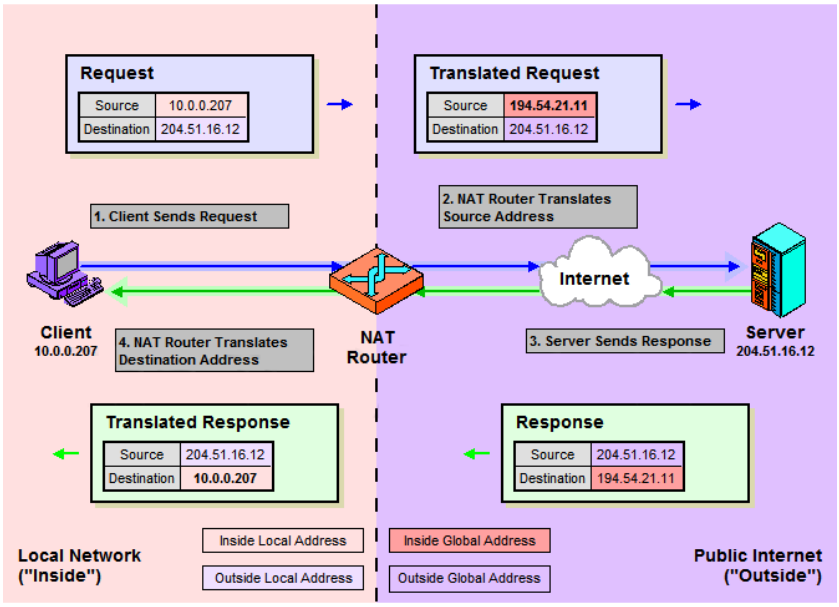


Pooled NAT

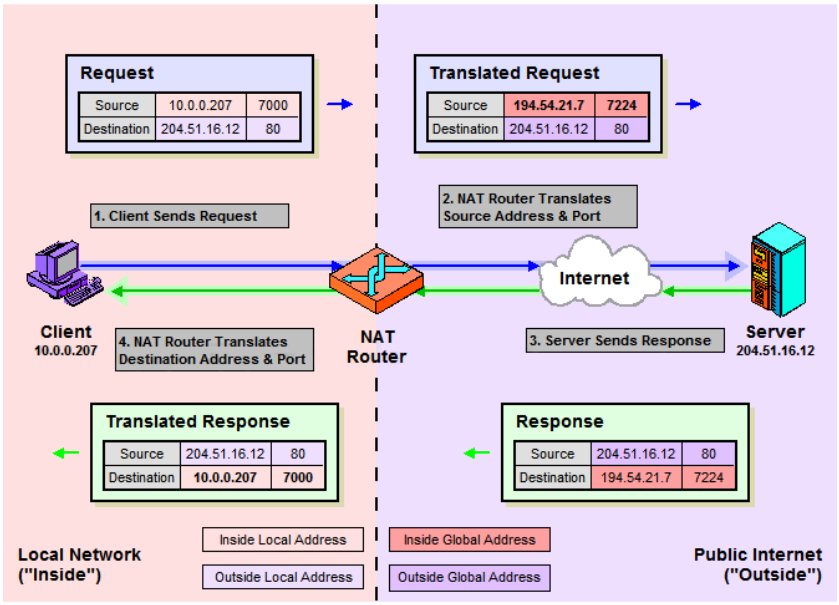
Στην πιο δημοφιλή περίπτωση χρήσης του NAT (Traditional NAT ή Outbound NAT) πολλαπλοί ιδιωτικοί σταθμοί επιτρέπεται να έχουν πρόσβαση στο διαδίκτυο. Για τον σκοπό αυτό μοιράζονται μία ή περισσότερες δημόσιες διευθύνσεις σε αυτό που συνήθως ονομάζεται NAPT (Network Address Port Translation) διότι χρησιμοποιούνται και οι θύρες των μηνυμάτων TCP ή/και UDP. Στα απερχόμενα μηνύματα TCP/UDP η τοπική IP διεύθυνση πηγής και η θύρα (source port number) μεταφράζεται σε ένα ζεύγος δημόσιας IP διεύθυνσης πηγής και θύρας. Στα εισερχόμενα μηνύματα που απευθύνονται σε αυτό το ζευγάρι δημόσιας IP διεύθυνσης και θύρας γίνεται

[3] Σταθμοί με ιδιωτικές διευθύνσεις (RFC 1917)

μετάφραση των πεδίων αυτών στο αντίστοιχο ζευγάρι τοπικής IP διεύθυνσης και θύρας. Και πάλι, η αντιστοίχηση διατηρείται για ένα χρονικό διάστημα μετά τη λήξη του οποίου επιστρέφεται ο συνδυασμός.



Traditional ή Outbound NAT



NAPT

Port Forwarding

Σε ένα τυπικό οικιακό δίκτυο, οι κόμβοι έχουν πρόσβαση στο διαδίκτυο μέσω DSL δρομολογητή που υλοποιεί και μετάφραση διευθύνσεων δικτύου (NAT/NAPT). Η εξωτερική διασύνδεση της συσκευής NAT έχει ρυθμιστεί με μια δημόσια διεύθυνση IP. Οι υπολογιστές πίσω από τον δρομολογητή, είναι «αόρατοι» στους σταθμούς του διαδικτύου, δηλαδή μη προσβάσιμοι από αυτούς, δεδομένου ότι διαθέτουν μόνο ιδιωτικές διευθύνσεις IP. Με την προώθηση θυρών (Port forwarding) επιτρέπεται σε απομακρυσμένους υπολογιστές (στο διαδίκτυο) να συνδεθούν σε έναν συγκεκριμένο υπολογιστή ή υπηρεσία μέσα στο ιδιωτικό δίκτυο. Στην προώθηση θυρών, ο διαχειριστής του ιδιωτικού δικτύου ρυθμίζει ένα αριθμό θύρας στην πύλη NAT για **αποκλειστική**

χρήση επικοινωνίας με μια υπηρεσία στο ιδιωτικό δίκτυο, που βρίσκεται σε ένα συγκεκριμένο host, στον οποίο προωθείται η εισερχόμενη κίνηση της θύρας. Οι εξωτερικοί σταθμοί πρέπει να γνωρίζουν τον αριθμό της θύρας και τη διεύθυνση της πύλης NAT προκειμένου να επικοινωνήσουν με τη συγκεκριμένη υπηρεσία. Συχνά χρησιμοποιούνται οι πασίγνωστοι αριθμοί θυρών υπηρεσιών Internet, π.χ. θύρα 80 για τις υπηρεσίες Web (HTTP), έτσι ώστε να μπορούν να δοθούν οι αντίστοιχες υπηρεσίες από υπολογιστές εντός ιδιωτικών δικτύων.

Το πρωτόκολλο Universal Plug and Play (UPnP) παρέχει μια δυνατότητα για αυτόματη εγκατάσταση προώθησης θυρών μεταξύ πυλών NAT και Host εντός των ιδιωτικών δικτύων. Το UPnP χρησιμοποιεί το πρωτόκολλο SSDP (Simple Service Discovery Protocol) για να εντοπίσει συσκευές που χρησιμοποιούν μηχανισμούς προώθησης θυρών. Επιπλέον ορίζει το πρωτόκολλο Internet Gateway Device (IGD) για την απομακρυσμένη προσθήκη/διαγραφή κανόνων προώθησης σε μια συσκευή NAT μέσω του SSDP. Μια εφαρμογή που παρέχει κάποια διαδικτυακή υπηρεσία μπορεί να ανακαλύψει τοπικά τέτοιες πύλες και στη συνέχεια να χρησιμοποιήσει το UPnP πρωτόκολλο IGD για να δεσμεύει έναν αριθμό θύρας στην πύλη NAT και να προκαλέσει την πύλη να προωθήσει πακέτα προς αυτή.

VPN (Virtual Private Network)

Όταν το ιδιωτικό δίκτυο (intranet) ενός οργανισμού επεκτείνεται σε πολλές γεωγραφικά διαφορετικές περιοχές, ανακύπτει η ανάγκη διασύνδεσης σε ένα εικονικό ιδιωτικό δίκτυο VPN μέσω του δημόσιου διαδικτύου (ως η οικονομικότερη λύση σε σχέση με την ενοικίαση ή την κατασκευή ιδιόκτητων τηλεπικοινωνιακών ζεύξεων). Τα PPTP, L2TP και IPsec είναι κάποιες από τις λύσεις που χρησιμοποιούνται για τον σκοπό αυτό.

IPsec

Το IPsec (Internet Protocol Security) είναι ένα σύνολο επεκτάσεων του πρωτοκόλλου IP που ορίζεται στο RFC 4301. Λειτουργεί περίπου το ίδιο σε αμφότερα τα IPv4 και IPv6 παρέχοντας δύο βασικές υπηρεσίες: Πιστοποίηση Αυθεντικότητας και Επαλήθευση (Authentication and Verification) και Εμπιστευτικότητα (Confidentiality). Με την πιστοποίηση αυθεντικότητας μπορεί κανείς να είναι σίγουρος ότι τα δεδομένα προέρχονται από αυτόν που ισχυρίζεται ότι τα στέλνει, με την επαλήθευση να βεβαιωθεί ότι δεν έχουν αλλαχθεί κατά τη μετάδοση και με την εμπιστευτικότητα ότι δεν μπορεί να τα δει ένας τρίτος ακόμη και εάν έχει πρόσβαση σε αυτά κατά τη διάρκεια μετάδοσής τους.

Οι δύο υπηρεσίες είναι διαφορετικές, αλλά το IPsec τις παρέχει ενοποιημένα. Η πιστοποίηση αυθεντικότητας επιτυγχάνεται με την προσθήκη της επικεφαλίδας Authentication Header (AH) που ακολουθεί την επικεφαλίδα IP και περιέχει κρυπτογραφημένες συνόψεις (Hashes) των δεδομένων και της ταυτότητας του αποστολέα. Η εμπιστευτικότητα επιτυγχάνεται με την προσθήκη της επικεφαλίδας Encapsulating Security Payload (ESP) και προαιρετικά την κρυπτογράφηση του πεδίου δεδομένων. Η επικεφαλίδα ESP δεν εξετάζει τα πεδία του πακέτου IP που προηγούνται αυτής. Επομένως δεν εγγυάται τίποτε εκτός του πεδίου δεδομένων (payload).

Το IPsec έχει δύο τρόπους λειτουργίας ανάλογα με το εάν η ενθυλάκωση γίνεται στον αρχικό κόμβο πηγής των δεδομένων ή σε κάποια πύλη. Η λειτουργία μεταφοράς (Transport**)** χρησιμοποιείται από τον host που παράγει τα πακέτα. Οι επικεφαλίδες IPsec προηγούνται αυτών του στρώματος μεταφοράς (π.χ. TCP, UDP) και κατόπιν προστίθεται η επικεφαλίδα IP. Με άλλα λόγια, η επικεφαλίδα AH που προστίθεται στο πακέτο καλύπτει την επικεφαλίδα TCP και κάποια σταθερά πεδία της επικεφαλίδας IP, ενώ η ESP θα καλύψει την κρυπτογράφηση της επικεφαλίδας TCP και των δεδομένων, αλλά όχι της επικεφαλίδας IP. Η λειτουργία σήραγγας (Tunnel)

χρησιμοποιείται όταν η επικεφαλίδα IP ήδη υφίσταται και το ένα άκρο της επικοινωνία είναι μια πύλη (gateway). Σε αυτή τη λειτουργία οι επικεφαλίδες AH και ESP καλύπτουν όλο το πακέτο και κατόπιν προτάσσεται μία νέα επικεφαλίδα IP για τη μετάβαση στο άλλο άκρο της ασφαλούς ζεύξης (που μπορεί να απέχει πολλά βήματα).

Οι ασφαλείς ζεύξεις IPsec ορίζονται ως σχέσεις ασφάλειας – Security Associations (SAs). Η SA ορίζεται για κάθε μονόδρομη ροή δεδομένων από ένα σημείο προς ένα άλλο. Όλη η κίνηση μιας SA λαμβάνει την ίδια μεταχείριση. Κάθε SA μπορεί να ορίσει μία επικεφαλίδα ESP και μία AH, ώστε η σύνοδος IPsec να έχει τουλάχιστον την μία εκ των δύο. Τα πακέτα αντιστοιχίζονται σε μία SA με βάση τα πεδία IP διεύθυνση προορισμού, Security Parameter Index – SPI και πρωτόκολλο ασφαλείας. Ορίζονται δύο διαχειριστικές οντότητες που ελέγχουν το τι συμβαίνει σε ένα πακέτο. Η μία είναι η Security Association Database (SAD) και η άλλη η Security Policy Database (SPD). Η SPD χρησιμοποιείται για να αποφασιστεί ποια εγγραφή SAD θα χρησιμοποιηθεί. Η SAD περιγράφει την πραγματική διαδικασία και τις παραμέτρους της. Οι εγγραφές SPD καθορίζουν ποιες από τις υπάρχουσες εγγραφές SAD θα χρησιμοποιηθούν. Εάν δεν υπάρχει εγγραφή SAD, δημιουργείται μια νέα από τα πεδία της SPD ή από τα πεδία του πακέτου.

FreeBSD firewalls

Στο FreeBSD υποστηρίζονται τρία διαφορετικά τείχη προστασίας τα ipfw, ipfilter και το pf. Συνήθως δεν ενσωματώνονται στον πυρήνα του FreeBSD, αλλά φορτώνονται ως λειτουργική μονάδα (βλ. παρακάτω) από όσους χρήστες επιθυμούν να χρησιμοποιήσουν κάποιο από αυτά. Εξ αυτών θα ασχοληθείτε με το ipfw (ip firewall) και το ipfilter. Η υλοποίηση του ipfw περιλαμβάνει πολλά προηγμένα χαρακτηριστικά που το καθιστούν ένα από τα πιο ευρέως χρησιμοποιούμενα τείχη προστασίας ανοικτού κώδικα. Λόγω της επιτυχίας του αυτής, έχει τροποποιηθεί για να χρησιμοποιείται και από άλλους πυρήνες UNIX, όπως είναι αυτός του Mac OS X της Apple.

Το m0n0wall είναι μια διανομή του FreeBSD για ενσωματωμένα συστήματα που κυρίως επιτελούν τη λειτουργία ενός τείχους προστασίας. Το m0n0wall χρησιμοποιεί το ipfilter, αλλά το πιο ενδιαφέρον χαρακτηριστικό του είναι το γραφικό περιβάλλον διαχείρισης μέσω ιστοσελίδων (webGUI) που περιλαμβάνεται στη διανομή. Επειδή η παραμετροποίηση των τειχών προστασίας με τον παραδοσιακό τρόπο μέσω γραμμής εντολών είναι μια διαδικασία που απαιτεί χρόνο και γνώση της σύνταξης της κάθε εντολής, το γραφικό περιβάλλον διευκολύνει σε μεγάλο βαθμό την πραγματοποίηση των απαιτούμενων ρυθμίσεων στο σύστημα, αλλά και τη διάγνωση προβλημάτων. Όμως, οι δικτυακές συσκευές τυπικά δεν περιλαμβάνουν οθόνη για την εμφάνιση του γραφικού περιβάλλοντος χρήστη. Η λειτουργικότητα αυτή λοιπόν υλοποιείται μέσω ενός εξυπηρετητή HTTP και μίας κατάλληλης ιστοσελίδας που αυτός προβάλλει, στην οποία ο διαχειριστής μπορεί να αποκτήσει πρόσβαση μέσω ενός φυλλομετρητή (browser) όπου κι αν βρίσκεται. Η ιστοσελίδα του m0n0wall δίνει τη δυνατότητα για επισκόπηση της κατάστασης και των ρυθμίσεων του τείχους προστασίας και άλλων παραμέτρων της συσκευής καθώς και την πραγματοποίηση οποιασδήποτε αλλαγής σε αυτές.

FreeBSD kernel modules

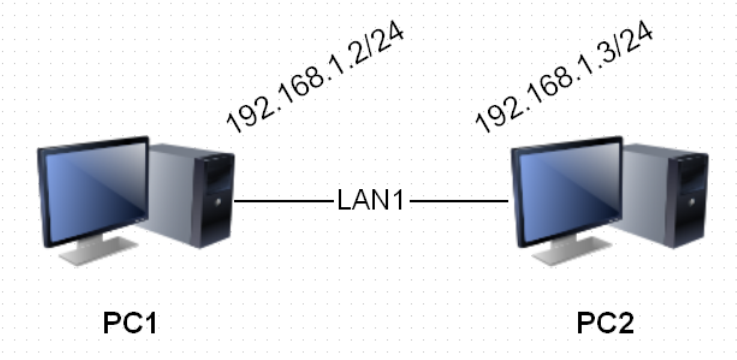
Στο FreeBSD και γενικά στο UNIX, η υποστήριξη κάποιων χαρακτηριστικών από το λειτουργικό σύστημα, όπως για παράδειγμα οδηγοί για περιφερειακές συσκευές, μπορεί είτε να ενσωματωθεί στον πυρήνα κατά τον χρόνο μεταγλώττισής (compile) του, είτε να φορτωθεί ως λειτουργική μονάδα (module) κατά τον χρόνο εκτέλεσης. Το κυριότερο πλεονέκτημα που προσφέρει η αρχιτεκτονική αυτή είναι η δυνατότητα χρήσης του ίδιου πυρήνα από πολλούς χρήστες με διαφορετικές ανάγκες, χωρίς να απαιτείται ο καθένας να μεταγλωττίσει τον πυρήνα συμπεριλαμβάνοντας τα χαρακτηριστικά που εκείνος χρειάζεται. Έτσι λοιπόν ο πυρήνας που χρησιμοποιούν όλοι οι χρήστες είναι ο ίδιος και ο κάθε χρήστης ανάλογα με τις ανάγκες του φορτώνει στον πυρήνα διάφορα modules κατά τον χρόνο εκτέλεσης, ώστε να υποστηριχθεί η

απαιτούμενη λειτουργικότητα. Οι εντολές με τις οποίες γίνεται η διαχείριση των modules στον πυρήνα του FreeBSD είναι οι kldload (φόρτωση), kldunload (αποφόρτωση) και kldstat (εμφάνιση κατάστασης).

Άσκηση 1: Ένα απλό firewall

Κατασκευάστε στο VirtualBox την παρακάτω τοπολογία, όπου τα PC είναι απλά FreeBSD images, με τη διαφορά ότι στο PC2 θα ενεργοποιήσουμε το τείχος προστασίας (firewall), το οποίο είναι απενεργοποιημένο από προεπιλογή. Στο PC2 εκτελέστε την εντολή kldload ipfw και αν θέλετε η ρύθμιση να παραμείνει και μετά από reboot θα πρέπει να προσθέσετε στο αρχείο /etc/rc.conf το εξής:

```
firewall_enable="YES"
```



Απαντήστε τις παρακάτω ερωτήσεις καταγράφοντας παράλληλα, όπου απαιτείται, την ακριβή σύνταξη των εντολών που χρησιμοποιήσατε.

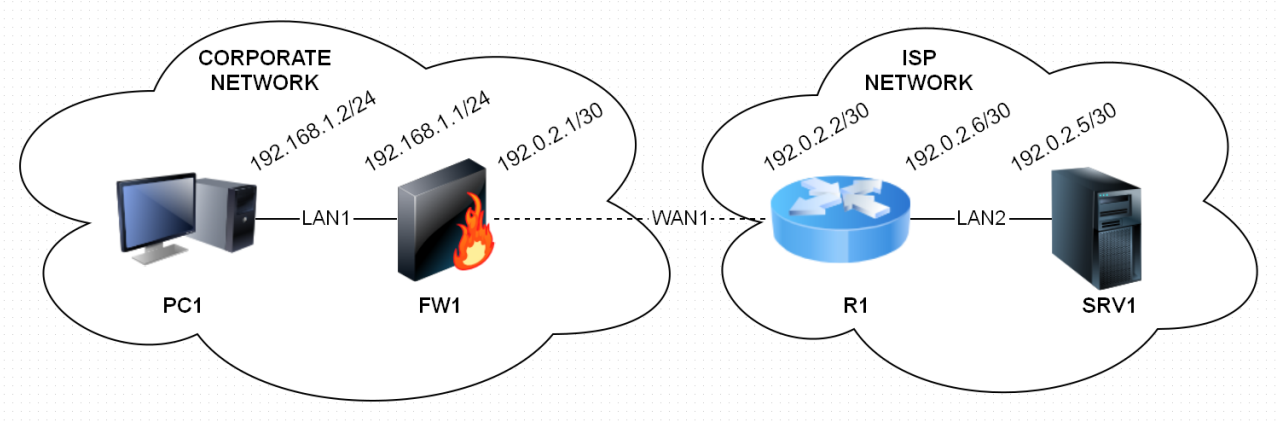
1.1 Στο PC2 επιβεβαιώστε αν είναι ενεργό το firewall module μέσω της εντολής "kldstat".
1.2 Μπορείτε να κάνετε ping από το PC1 στο PC2;
1.3 Μέσω της εντολής "ipfw list" βρείτε πόσοι κανόνες υπάρχουν στο PC2.
1.4 Εκτελέστε την εντολή "ipfw show". Βλέπετε κάποια διαφορά σε σχέση με την προηγούμενη ερώτηση;
1.5 Εκτελέστε την εντολή "ipfw zero && ipfw show". Τι διαφορά βλέπετε σε σχέση με την προηγούμενη ερώτηση;
1.6 Προσθέστε κανόνα firewall στο PC2 με την εντολή "ipfw add allow icmp from any to me". Μπορείτε να κάνετε ping από το PC1 στο PC2;
1.7 Τεκμηριώστε την απάντησή σας με τη βοήθεια της εντολής "ipfw show".
1.8 Προσθέστε κανόνα firewall στο PC2 ώστε να επιτρέπεται η κίνηση ICMP προς οποιαδήποτε διεύθυνση IP. *[Υποδ. Συμβουλευθείτε σελίδα βοήθειας για ipfw, κεφάλαιο RULE BODY]*.
1.9 Μηδενίστε τα packet counts.
1.10 Μπορείτε να κάνετε ping από το PC1 στο PC2;
1.11 Βλέπετε κάποια σχέση στα packet counts στους δύο ICMP κανόνες;
1.12 Διαγράψτε όλους τους κανόνες από το PC2. *[Υποδ. Συμβουλευθείτε σελίδα βοήθειας για ipfw]*.
1.13 Πόσοι κανόνες υπάρχουν τώρα στο PC2;

1.14 Προσθέστε κανόνα firewall στο PC2 με την εντολή “ipfw add allow icmp from any to me keep-state”. Μπορείτε να κάνετε ping από το PC1 στο PC2;
1.15 Αφήστε το προηγούμενο ping να τρέχει και εκτελέστε στο PC2 την εντολή “ipfw –d show”. Τι βλέπετε;
1.16 Σταματήστε το ping από το PC1, περιμένετε λίγα δευτερόλεπτα και ξαναεκτελέστε στο PC2 την προηγούμενη εντολή. Τι βλέπετε;
1.17 Μηδενίστε τα packet counts για τον κανόνα 100.
1.18 Διαγράψτε τον κανόνα 100.
1.19 Απενεργοποιήστε το ipfw με τη βοήθεια της εντολής “kldunload” και επιβεβαιώστε ότι απενεργοποιήθηκε.

Άσκηση 2: Firewall και απλό Network Address Translation

Κατασκευάστε στο VirtualBox την παρακάτω τοπολογία. Για εξυπηρετητή SRV1 χρησιμοποιήστε το PC2 από την προηγούμενη άσκηση και για δρομολογητή R1 ένα νέο BSDRP image. Για το τείχος προστασίας θα χρειαστείτε ένα νέο FreeBSD image με δύο κάρτες δικτύου και με τα ακόλουθα στο /etc/rc.conf:

```
ifconfig_em0=”192.168.1.1/24”
ifconfig_em1=”192.0.2.1/30”
defaultrouter=”192.0.2.2”
gateway_enable=”YES”
firewall_enable=”YES”
firewall_type=”OPEN”
firewall_nat_enable=”YES”
firewall_nat_interface=”em1”
```



Απαντήστε τις παρακάτω ερωτήσεις καταγράφοντας παράλληλα, όπου απαιτείται, την ακριβή σύνταξη των εντολών που χρησιμοποιήσατε.

2.1 Ορίστε τη σωστή διεύθυνση στο PC1.

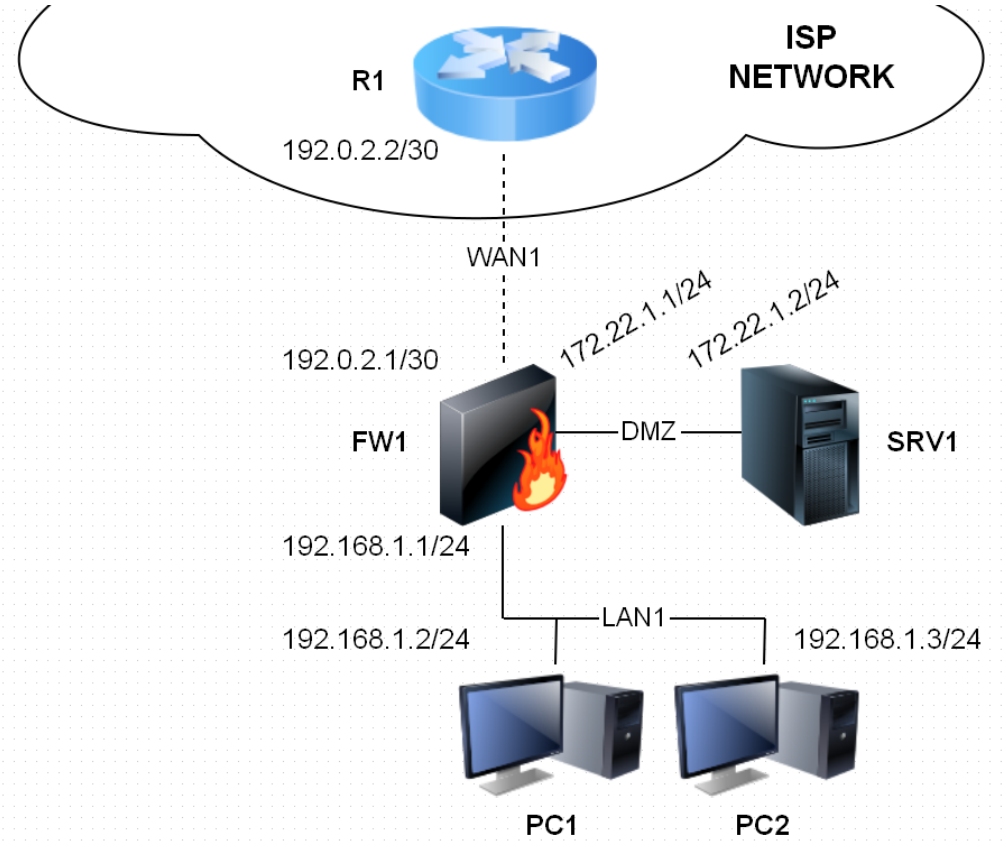
2.2 Ορίστε τη σωστή προεπιλεγμένη πύλη στο PC1.
2.3 Ορίστε στο quagga του R1 τη σωστή διεύθυνση για τη διεπαφή στο WAN1.
2.4 Ορίστε στο quagga του R1 τη σωστή διεύθυνση για τη διεπαφή στο LAN2.
2.5 Ορίστε τη σωστή διεύθυνση στον SRV1.
2.6 Ορίστε τη σωστή προεπιλεγμένη πύλη στο SRV1.
2.7 Μηδενίστε τα packet counts στο ipfw του FW1.
2.8 Πόσους κανόνες βλέπετε στο FW1;
2.9 Μπορείτε από το PC1 να κάνετε ping τη διεπαφή του FW1 στο LAN1; Γιατί η προεπιλεγμένη ρύθμιση είναι διαφορετική σε σχέση με την προηγούμενη άσκηση;
2.10 Μπορείτε από το PC1 να κάνετε ping τη διεπαφή του FW1 στο WAN1;
2.11 Μπορείτε από το PC1 να κάνετε ping τη διεπαφή του R1 στο WAN1;
2.12 Μπορείτε από το PC1 να κάνετε ping τη διεπαφή του R1 στο WAN2;
2.13 Ξεκινήστε καταγραφή πακέτων με το tcpdump στη διεπαφή του FW1 στο WAN1.
2.14 Κάντε ping από το PC1 το SRV1. Ποια η διεύθυνση πηγής των πακέτων που βλέπετε;
2.15 Ξεκινήστε νέα καταγραφή πακέτων με το tcpdump στη διεπαφή του FW1 στο LAN1.
2.16 Κάντε ping από το PC1 το SRV1. Τι διαφορετικό βλέπετε σε σχέση με πριν;
2.17 Εμφανίστε στο FW1 τα packet counts. Ποιοι κανόνες υπάρχουν και πόσα packet counts;
2.18 Μπορείτε από το SRV1 να κάνετε ping το PC1; Τεκμηριώστε την απάντησή σας.

Άσκηση 3: Ένα πιο πολύπλοκο δίκτυο και firewall με γραφικό περιβάλλον διαχείρισης

Κατασκευάστε στο VirtualBox την παρακάτω τοπολογία. Μπορείτε να χρησιμοποιήσετε τα μηχανήματα από την προηγούμενη άσκηση, εκτός από το FW1 όπου πρέπει να το αντικαταστήσετε με νέο από το αρχείο firewall.ova[4]. Θυμηθείτε να αλλάξετε τα τοπικά δίκτυα από το VirtualBox όπως στο σχήμα προτού ξεκινήσετε. Στο firewall.ova έχει προστεθεί μια ξεχωριστή κάρτα δικτύου για διαχείριση. Κάτι τέτοιο είναι παρόμοιο με τις τεχνικές "Out of band management", όπου η διαχείριση γίνεται από διαφορετικό δίκτυο από αυτό που εξυπηρετεί την κίνηση. Συνηθίζεται σε μεγάλες εγκαταστάσεις, σε συσκευές δικτύου και εξυπηρετητές. Εδώ όμως εξυπηρετεί μόνο ένα σκοπό, στο να μη χρειαστεί να εγκατασταθεί γραφικό περιβάλλον στα εικονικά μηχάνημα και η διαχείριση να γίνει από τον φυλλομετρητή του φιλοξενούντος συστήματος. Στο firewall.ova η 3^{η} κάρτα δικτύου είναι ήδη ρυθμισμένη σε δικτύωση host-only και μπορείτε να αποκτήσετε πρόσβαση στο γραφικό περιβάλλον του τείχους προστασίας με όνομα χρήστη "admin" και συνθηματικό "ntua", ακολουθώντας παρακάτω σύνδεσμο http://192.168.56.2.

Απαντήστε τις παρακάτω ερωτήσεις καταγράφοντας παράλληλα, όπου απαιτείται, την ακριβή σύνταξη των εντολών που χρησιμοποιήσατε. Στην περίπτωση που πρόκειται για χειρισμούς από το γραφικό περιβάλλον, απαντήστε σε ποιο μενού κάνατε ποια ρύθμιση και πώς την ενεργοποιήσατε.

[4] Θα το βρείτε με anonymous ftp στο edu-dy.cn.ntua.gr.



3.1 Ποια είναι η διεύθυνση που έχει ρυθμιστεί στη διεπαφή του FW1 στο LAN1;
3.2 Ποια είναι η διεύθυνση που έχει ρυθμιστεί στη διεπαφή του FW1 στο WAN1;
3.3 Ποιο είναι το ποσοστό της ελεύθερης μνήμης που βλέπετε στο FW1;
3.4 Πόσες διεπαφές δικτύου βλέπετε συνολικά στο FW1;
3.5 Ποια είναι η διεύθυνση που έχει ρυθμιστεί στη διεπαφή DMZ του FW1;
3.6 Ποιο είναι το όνομα (hostname) του FW1;
3.7 Αλλάξτε το hostname του FW1 σε “fw1”.
3.8 Στο μενού Firewall → Rules του FW1 υπάρχουν κανόνες για τη διεπαφή WAN;
3.9 Ορίστε τη σωστή διεύθυνση και προεπιλεγμένη πύλη του FW1 στο WAN1 και επιλέξτε το “Block private networks”.
3.10 Στο μενού Firewall → Rules του FW1 υπάρχουν τώρα κανόνες για τη διεπαφή WAN;
3.11 Βλέπετε να είναι ενεργοποιημένη κάποια υπηρεσία από αυτές των κατηγοριών “Services” και “VPN”;
3.12 Ενεργοποιήστε την υπηρεσία DNS forwarder χωρίς κάποια άλλη ρύθμιση (είναι προαπαιτούμενο για το παρακάτω).
3.13 Ενεργοποιήστε την υπηρεσία DHCP server ορίζοντας ως περιοχή διευθύνσεων την 192.168.1.2 έως 192.168.1.3.
3.14 Στο PC1 ξεκινήστε τον πελάτη DHCP. Ποια είναι η διεύθυνση IP, η προεπιλεγμένη πύλη και η διεύθυνση εξυπηρετητή DNS που αποδόθηκε;
3.15 Μπορείτε από το PC1 να κάνετε ping τη διεπαφή του FW1 στο LAN1;
3.16 Στο μενού Diagnostics → Logs → Firewall τι βλέπετε; Καθαρίστε το αρχείο καταγραφών.
3.17 Πόσες εγγραφές ARP βλέπετε από το αντίστοιχο μενού στο Diagnostics;
3.18 Πόσα firewall states βλέπετε από το αντίστοιχο μενού;

3.19 Πόσους κανόνες για το LAN1 βλέπετε από το μενού Firewall → Rules;
3.20 Προσθέστε στο FW1 κανόνα ώστε να επιτρέψετε <u>όλη</u> την κίνηση από το LAN1. *[Υποδ. Ο κανόνας ενεργοποιείται όταν κάνετε κλικ στο Apply Changes.]*
3.21 Μπορείτε τώρα από το PC1 να κάνετε ping τη διεπαφή του FW1 στο LAN1;
3.22 Από τον R1 μπορείτε να κάνετε ping τη διεπαφή του FW1 στο WAN1;
3.23 Εμφανίστε τον πίνακα ARP στον R1. Βλέπετε κάποια εγγραφή για τη διεύθυνση MAC της διεπαφής του FW1 στο WAN1;
3.24 Προσθέστε στο FW1 κανόνα ώστε να επιτρέψετε την ICMP κίνηση από το WAN1 προς "WAN Address".
3.25 Μπορείτε τώρα από τον R1 να κάνετε ping τη διεπαφή του FW1 στο WAN1;
3.26 Μπορείτε από τον R1 να κάνετε ping το PC1; Τεκμηριώστε την απάντησή σας.
3.27 Μπορείτε από το PC1 να κάνετε ping τον SRV1;
3.28 Ορίστε τη σωστή προεπιλεγμένη πύλη στον SRV1.
3.29 Μπορείτε από το PC1 να κάνετε ping τον SRV1;
3.30 Μπορείτε από τον SRV1 να κάνετε ping το PC1;
3.31 Στο PC2 ξεκινήστε τον πελάτη DHCP. Ποια είναι η διεύθυνση IP, η προεπιλεγμένη πύλη και η διεύθυνση εξυπηρετητή DNS που αποδόθηκε;
3.32 Προσθέστε στο FW1 κανόνα "Block", ώστε να αποτρέψετε στο LAN1 όλη την κίνηση από το PC2 προς το DMZ.
3.33 Πρέπει ο κανόνας να τοποθετηθεί πριν ή μετά από αυτόν που υπάρχει;
3.34 Μπορείτε από το PC1 να κάνετε ping τον SRV1;
3.35 Μπορείτε από το PC2 να κάνετε ping τον SRV1;
3.36 Μπορείτε από το PC2 να κάνετε ping τη διεπαφή του FW1 στο DMZ;

Άσκηση 4: Προχωρημένο Network Address Translation

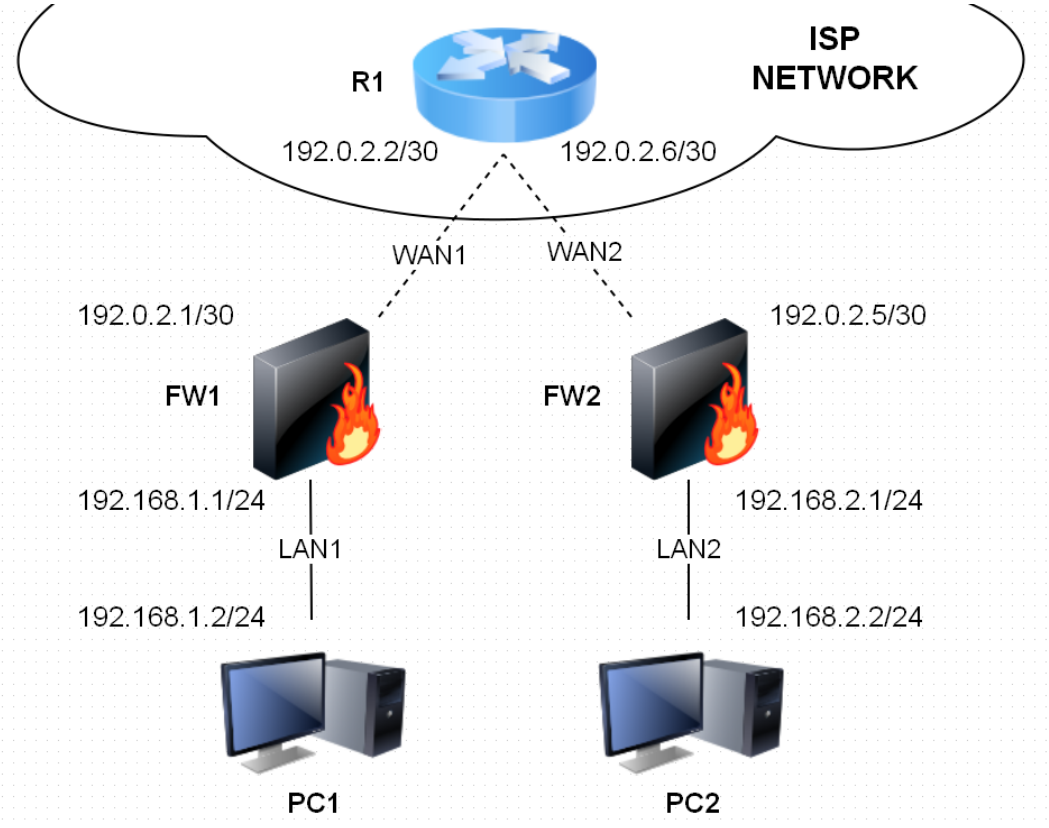
Θα χρησιμοποιήσετε την ίδια τοπολογία της προηγούμενης άσκησης προκειμένου να εμβαθύνετε στη χρήση του inbound και outbound NAT σε ένα firewall. Στην άσκηση αυτή υποτίθεται ότι ο πάροχος ISP σας έχει εκχωρήσει το υποδίκτυο 203.0.113.0/24. Θέλετε ο εξυπηρετητής SRV1 να είναι προσβάσιμος από το δημόσιο δίκτυο και να εμφανίζετε τα PC1 και PC2 στο διαδίκτυο με συγκεκριμένες δημόσιες διευθύνσεις IP από αυτές που σας εκχωρήθηκαν.

4.1 Προσθέστε στον R1 στατική εγγραφή για το 203.0.113.0/24 προς το FW1 ώστε η κίνηση προς το υποδίκτυό σας να διέρχεται μέσω του τείχους προστασίας.
4.2 Στο FW1 ενεργοποιήστε το "advanced outbound NAT". Με αυτό τον τρόπο απενεργοποιείτε το αυτόματο outbound NAT στη WAN IP.
4.3 Προσθέστε outbound NAT για το PC1 ώστε να εμφανίζεται με τη διεύθυνση 203.0.113.114. *[Υποδ. Χρησιμοποιείστε /32 μάσκα.]*
4.4 Προσθέστε outbound NAT για το PC2 ώστε να εμφανίζεται με τη διεύθυνση 203.0.113.115.
4.5 Ξεκινήστε καταγραφή πακέτων με το tcpdump στη διεπαφή του R1.
4.6 Μπορείτε να κάνετε ping από το PC1 τον R1; Αν ναι με ποια διεύθυνση IP φτάνουν τα πακέτα;

4.7 Μπορείτε να κάνετε ping από το PC2 τον R1; Αν ναι με διεύθυνση IP φτάνουν τα πακέτα;
4.8 Στο FW1 προσθέστε εγγραφή "Server NAT" με IP διεύθυνση 203.0.113.113.
4.9 Στο FW1 προσθέστε εγγραφή "Inbound NAT", ορίζοντας external address την 203.0.113.113, τη διεύθυνση του SRV1 για NAT IP, τη θύρα SSH ή τον αριθμό 22 ως external port και επιλέξτε το "Auto-add a firewall rule".
4.10 Μπορείτε από τον R1 να κάνετε ping το 203.0.113.113;
4.11 Μπορείτε από τον R1 να κάνετε SSH στο 203.0.113.113; Σε ποιο σύστημα συνδέεστε;
4.12 Μπορεί ο SRV1 να επικοινωνήσει με κάποια από τις διευθύνσεις IP της τοπολογίας του σχήματος; Τεκμηριώστε την απάντησή σας.

Άσκηση 5: IPSec site-to-site VPN

Κατασκευάστε στο VirtualBox την παρακάτω τοπολογία. Θα χρησιμοποιήσετε τα μηχανήματα από την προηγούμενη άσκηση εκτός του SRV1. Θα χρειαστείτε άλλο ένα firewall FW2 που θα κατασκευάσετε σύμφωνα με τις οδηγίες που ακολουθούν. Θυμηθείτε να αλλάξετε τα τοπικά δίκτυα από το VirtualBox.



Απαντήστε τις παρακάτω ερωτήσεις καταγράφοντας παράλληλα, όπου απαιτείται, την ακριβή σύνταξη των εντολών που χρησιμοποιήσατε.

5.1 Επαναφέρετε στο FW1 τις ρυθμίσεις από την προηγούμενη άσκηση για το NAT στις αρχικές. Θυμηθείτε να απενεργοποιήσετε το "advanced outbound NAT".
5.2 Διαγράψτε στον R1 τη στατική εγγραφή προς το FW1.
5.3 Αποσυνδέστε από το Virtualbox το καλώδιο της κάρτας δικτύου #3 του FW1.
5.4 Αλλάξτε τη διεύθυνση IP στη διεπαφή MNG του FW2 από 192.168.56.2 σε 192.168.56.3.
5.5 Ξανασυνδέστε από το Virtualbox το καλώδιο της κάρτας δικτύου #3 του FW1.
5.6 Αποσυνδέστε μέσω του VirtualBox και από τα δύο τείχη προστασίας το καλώδιο των διεπαφών DMZ.
5.7 Μπορείτε να συνδεθείτε ταυτόχρονα από τον φυλλομετρητή του φιλοξενούντος μηχανήματος στα τείχη προστασίας;
5.8 Αλλάξτε το hostname του FW2 σε "fw2".
5.9 Ορίστε τη σωστή τη διεύθυνση και προεπιλεγμένη πύλη του FW2 στο WAN2, επιλέγοντας το "Block private networks".
5.10 Ορίστε τη σωστή τη διεύθυνση και προεπιλεγμένη πύλη του FW2 στο LAN2.
5.11 Επανεκκινήστε το FW2.
5.12 Προσθέστε στο FW2 κανόνα ώστε να επιτρέψετε <u>όλη</u> την κίνηση από το LAN2.
5.13 Προσθέστε στο FW2 κανόνα ώστε να επιτρέψετε την ICMP κίνηση από το WAN2 προς "WAN Address".
5.14 Ορίστε τη σωστή διεύθυνση στο PC2.
5.15 Ορίστε τη σωστή προεπιλεγμένη πύλη στο PC2.
5.16 Μπορείτε από το PC1 να κάνετε ping τη WAN του FW2;
5.17 Μπορείτε από το PC2 να κάνετε ping τη WAN του FW1;
5.18 Μπορείτε από το PC1 να κάνετε ping το PC2;
5.19 Μπορείτε από το PC2 να κάνετε ping το PC1; Τεκμηριώστε την απάντησή σας.
5.20 Προσθέστε στο FW1 δυο κανόνες για να επιτραπεί κίνηση από το WAN2 του FW2 προς το WAN1 του FW1, επιλέγοντας ως πρωτόκολλα τα ESP και UDP/500, αντίστοιχα..
5.21 Επαναλάβατε και στο FW2.
5.22 Στο μενού VPN του FW1 δημιουργήστε ένα IPSec tunnel ορίζοντας μόνο: Local Subnet, Remote Subnet, Remote Gateway και Pre-Shared Key (κάποια λέξη, π.χ. το όνομά σας) και ενεργοποιήστε το.
5.23 Αντίστοιχα και στο FW2, βάζοντας το ίδιο Pre-Shared Key όπως και παραπάνω.
5.24 Στο FW1 → Diagnostics → IPSec → Security Association Database (SAD) βλέπετε να έχουν ορισθεί σχέσεις μεταξύ των δύο υποδικτύων;
5.25 Στο FW1 → Diagnostics → IPSec → Security Policy Database (SPD) βλέπετε να έχουν ορισθεί πολιτικές προώθησης κίνησης μεταξύ των δύο υποδικτύων;
5.26 Μπορείτε από το PC1 να κάνετε ping το PC2;
5.27 Μπορείτε από το PC2 να κάνετε ping το PC1;
5.28 Άλλαξε κάτι στο FW1 → Diagnostics → IPSec → SAD;
5.29 Άλλαξε κάτι στο FW1 → Diagnostics → IPSec → SPD;
5.30 Τι βλέπετε στο FW1 → Firewall → Rules →IPsec VPN;

Ονοματεπώνυμο:	**Όνομα PC:**
Ομάδα:	**Ημερομηνία:**
Διεύθυνση IP: . . .	**Διεύθυνση MAC: - - - - -**

Εργαστηριακή Άσκηση 10
Τείχη προστασίας (Firewalls) και NAT

Απαντήστε στα ερωτήματα στον χώρο που σας δίνεται παρακάτω και στην πίσω σελίδα εάν δεν επαρκεί. Το φυλλάδιο αυτό θα παραδοθεί στον επιβλέποντα.

1

1.1 .....

1.2 .....

1.3 .....

1.4 .....

.....

1.5 .....

.....

1.6 .....

.....

1.7 .....

.....

1.8 .....

1.9 .....

1.10 .....

1.11 .....

.....

1.12 .....

1.13 .....

1.14 .....

1.15 .....

.....

1.16 .....

.....

1.17 .....

1.18 .....

1.19 .....