Εργαστηριακή Άσκηση 10
Τείχη προστασίας (Firewalls) και NAT

Firewall (Τείχος Προστασίας)

Η ορολογία firewall προέκυψε από την περιοχή 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 φίλτρα πακέτων (packet-filters) και η δομή ελέγχου σε πρώιμη μορφή ήταν λίστα ελέγχου πρόσβασης (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 αγνοείται (silent discard) ή απορρίπτεται (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 του πρωτοκόλλου ελέγχου ICMP είτε οι θύρες των πρωτοκόλλου μεταφοράς (TCP, UDP), λειτουργεί δηλαδή στα στρώματα δικτύου και μεταφοράς του μοντέλου OSI.

Με την εξάπλωση του Internet έγινε απαραίτητη η κατασκευή δεύτερης γενιάς τειχών προστασίας με δυνατότητα λειτουργίας στα ανώτατα στρώματα του μοντέλου OSI. Αυτά λειτουργούν βάσει της κατάστασης (stateful), ελέγχουν 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 τα πεδία της επικεφαλίδας TCP (TCP flags SYN/ACK/RST/FIN), παρακολουθείται η κατάσταση των ανοικτών συνδέσεων, αποκωδικοποιείται πληροφορία στρώματος εφαρμογής (π.χ εντολές ελέγχου FTP) κλπ.

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, 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 απλώς τα πακέτα, προσπαθεί να αποτυπώσει τις επιχειρούμενες συνδέσεις. Έτσι 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 τη 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 εξυπηρετητές ηλεκτρονικού ταχυδρομείου, ιστού και DNS (Domain Name System), 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 να χρησιμοποιούνται ιδιωτικές διευθύνσεις (private addresses), όπως καθορίζονται στο RFC 1918. Προβλέπονται 3 ομάδες 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 αντιστοίχισης μεταξύ ιδιωτικών και δημόσιων διευθύνσεων. Ο μηχανισμός 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. Μια δικτυακή συσκευή, ο δρομολογητής NAT, δρα ως πύλη μεταξύ του διαδικτύου και του εσωτερικού δικτύου μεταφράζοντας τις εσωτερικές διευθύνσεις IPv4 σε δημόσιες διευθύνσεις IPv4. 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 ορολογία NAT το ιδιωτικό δίκτυο αναφέρεται ως **εσωτερικό (inside)** και το δημόσιο ως **“εξωτερικό” (outside)**. Μια διεύθυνση IPv4 όπως τη βλέπουν οι host στο “εσωτερικό” αποκαλείται **τοπική διεύθυνση (local address)**. Μια διεύθυνση IPv4 που τη βλέπουν host στο “εξωτερικό” αποκαλείται **παγκόσμια διεύθυνση (global address)**. Υπάρχουν τέσσερεις διαφορετικοί τύποι διευθύνσεων:

εσωτερική τοπική διεύθυνση (**inside local address**) είναι μια διεύθυνση στο ιδιωτικό δίκτυο που δεν είναι ορατή στο δημόσιο δίκτυο, συνήθως μια ιδιωτική διεύθυνση RFC 1918 που έχει αποδοθεί στη διεπαφή ενός υπολογιστή εντός του ιδιωτικού δικτύου,

εσωτερική παγκόσμια διεύθυνση (**inside global address**) είναι μια διεύθυνση που μπορεί να χρησιμοποιηθεί στο δημόσιο (εξωτερικό) δίκτυο για την αναπαράσταση μίας ή περισσότερων εσωτερικών τοπικών διευθύνσεων συσκευών, δηλαδή, η διεύθυνση μιας εσωτερικής συσκευής όπως τη βλέπει το εξωτερικό δίκτυο,

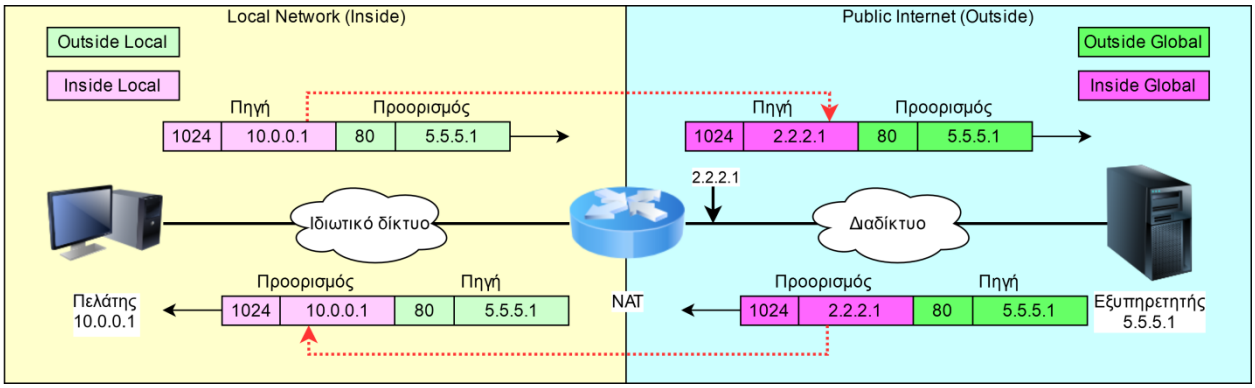
[1] Το όνομα DMZ προέρχεται από την στρατιωτική ορολογία. Είναι ο χώρος μεταξύ δύο αντιμαχόμενων στον οποίο δεν επιτρέπεται οποιαδήποτε στρατιωτική επιχείρηση.

εξωτερική τοπική διεύθυνση (**outside local address**) είναι η διεύθυνση με την οποία αναπαρίσταται στο ιδιωτικό δίκτυο ένας υπολογιστής που βρίσκονται στο δημόσιο δίκτυο, μπορεί να είναι η πραγματική διεύθυνση του εξωτερικού υπολογιστή ή μια ιδιωτική διεύθυνση που χρησιμοποιείται εντός του ιδιωτικού δικτύου.

εξωτερική παγκόσμια διεύθυνση (**outside global address**) είναι η διεύθυνση μιας συσκευής στο δημόσιο δίκτυο.

Basic NAT

Στην πιο απλή εκδοχή (βασικό NAT), ο δρομολογητής NAT αντικαθιστά την IPv4 διεύθυνση αποστολέα (source) κάθε εξερχόμενου πακέτου με μια δημόσια διεύθυνση IPv4 του NAT. Διατηρεί δε ένα πίνακα μετατροπής με τις αντιστοιχίες για κάθε μετατρεπόμενο ζεύγος διευθύνσεων. Οι μακρινοί host απαντούν χρησιμοποιώντας τη δημόσια διεύθυνση IPv4 του NAT ως διεύθυνση προορισμού. Στα εισερχόμενα πακέτα αντικαθίσταται η διεύθυνση IPv4 NAT στο πεδίο προορισμού κάθε πακέτου με την ιδιωτική IPv4 διεύθυνση πηγής που διατηρείται στον πίνακα του δρομολογητή NAT.



Σχήμα 1: Basic NAT

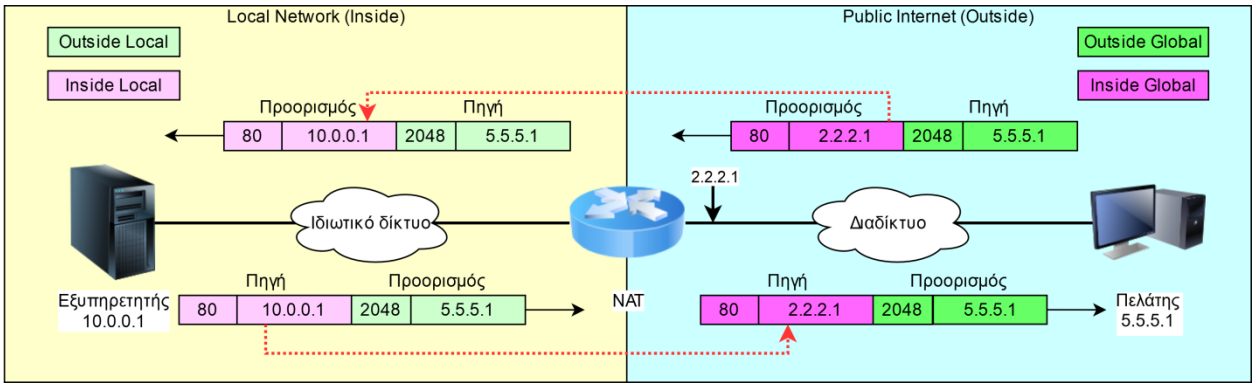
Επειδή η αντιστοιχία διευθύνσεων είναι 1:1 (μία ιδιωτική, μία δημόσια) απαιτείται πλήθος δημόσιων διευθύνσεων ίσο με τις ιδιωτικές που πρέπει να έχουν πρόσβαση στο διαδίκτυο. Ως εκ τούτου, η λειτουργία αυτή είτε στη στατική είτε στη δυναμική εκδοχή της χρησιμοποιείται μόνο σε εταιρικά δίκτυα για λόγους ασφαλείας (π.χ. στο τείχος προστασίας) και δεν είναι συνήθης για τα μικρά οικιακά δίκτυα.

Dynamic NAT

Στο δυναμικό NAT πολλαπλοί ιδιωτικοί σταθμοί με ιδιωτικές διευθύνσεις RFC 1918 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 αντιστοίχιση μέσα σε ένα ορισμένο χρονικό παράθυρο, τότε η αντιστοίχιση αφαιρείται από το NAT και η δημόσια διεύθυνση επιστρέφεται στη λίστα των διαθέσιμων δημόσιων διευθύνσεων NAT.

Inbound NAT

Στο δυναμικό NAT οι υπολογιστές πίσω από τον δρομολογητή, είναι «αόρατοι» στους σταθμούς του διαδικτύου, δηλαδή μη προσβάσιμοι από αυτούς, δεδομένου ότι διαθέτουν μόνο ιδιωτικές διευθύνσεις IPv4. Στο εισερχόμενο NAT, η κεντρική ιδέα είναι να επιτρέπεται η πρόσβαση σε συγκεκριμένους υπολογιστές του εσωτερικού δικτύου από το διαδίκτυο χρησιμοποιώντας δημόσιες διευθύνσεις IPv4, όπως φαίνεται στο ακόλουθο σχήμα. Αυτό τυπικά επιτυγχάνεται με την προώθηση θυρών (Port forwarding), όπου ο διαχειριστής του ιδιωτικού δικτύου ρυθμίζει έναν 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.

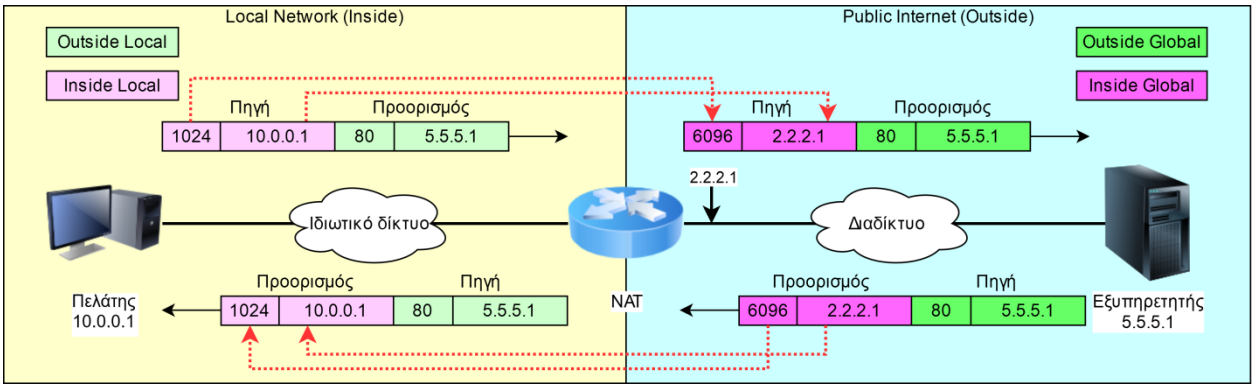


Σχήμα 2: Inbound NAT

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.

Traditional NAT

Η πιο δημοφιλής περίπτωση χρήσης NAT είναι το παραδοσιακό NAT ή απερχόμενο NAT (Outbound NAT) που ορίζεται στο RFC 3022. Στο παραδοσιακό NAT πολλαπλοί ιδιωτικοί σταθμοί επιτρέπεται να έχουν πρόσβαση στο διαδίκτυο. Για τον σκοπό αυτό μία ή περισσότερες δημόσιες διευθύνσεις IPv4 χρησιμοποιούνται μαζί με τις θύρες TCP ή/και UDP σε αυτό που συνήθως ονομάζεται NAPT (Network Address Port Translation). Στα απερχόμενα μηνύματα TCP/UDP η τοπική διεύθυνση IPv4 και η θύρα πηγής μεταφράζονται σε ένα ζεύγος δημόσιας IPv4 διεύθυνσης και θύρας πηγής. Στα εισερχόμενα μηνύματα που απευθύνονται σε αυτό το ζευγάρι δημόσιας IPv4 διεύθυνσης και θύρας γίνεται μετάφραση των πεδίων αυτών στο αντίστοιχο ζευγάρι τοπικής IPv4 διεύθυνσης και θύρας. Όπως στο δυναμικό NAT, η αντιστοίχιση διατηρείται για ένα χρονικό διάστημα μετά τη λήξη του οποίου επιστρέφεται ο συνδυασμός.



Σχήμα 3: Traditional ή Outbound NAT

Port Forwarding

Σε ένα τυπικό οικιακό δίκτυο, οι κόμβοι έχουν πρόσβαση στο διαδίκτυο μέσω xDSL δρομολογητή που υλοποιεί και μετάφραση διευθύνσεων δικτύου (NAT/NAPT). 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.

NAT μεγάλης κλίμακας

Η χρήση NAT δεν αφορά πλέον μόνο την περίπτωση οικιακών χρηστών. Οι τηλεπικοινωνιακοί πάροχοι χρησιμοποιούν NAT μεγάλης κλίμακας (Large Scale NAT – LSN) ή Carrier Grade NAT (CGN) σε δίκτυα κινητής τηλεφωνίας 3G/4G/5G, ασύρματης πρόσβασης WiFi ή ενσύρματης πρόσβασης xDSL. Στην περίπτωση LSN/CGN όλοι οι χρήστες έχουν ιδιωτικές διευθύνσεις IPv4 από το μπλοκ 100.64.0.0/10 και η πρόσβαση στο διαδίκτυο γίνεται μέσω NAT. Ο κύριος λόγος είναι η εξοικονόμηση δημόσιων διευθύνσεων IPv4 και η προστασία των κινητών συσκευών και των δικτύων των παρόχων από εξωτερικές επιθέσεις (όπως με τα τείχη προστασίας).

Συμπεριφορά NAT

Παρότι η κεντρική ιδέα είναι απλή, ο τρόπος λειτουργίας των συσκευών NAT δεν προδιαγράφεται στα σχετικά πρότυπα, με αποτέλεσμα οι διάφορες υλοποιήσεις να μην συμπεριφέρονται ταυτόσημα. Αυτό δεν θα ήταν ιδιαίτερο πρόβλημα εάν μόνο το ένα άκρο βρίσκονταν πίσω από NAT ή εάν δεν υπήρχαν εφαρμογές που χρησιμοποιούν πρωτόκολλα (π.χ. FTP, SIP, RSTP) τα οποία μεταφέρουν πληροφορία για διευθύνσεις και θύρες στο πεδίο δεδομένων τους. Εξ αιτίας αυτών και προκειμένου να επιτευχθεί η επικοινωνία μεταξύ δύο ακραίων κόμβων, για διάφορες συνήθως πολυμεσικές υπηρεσίες, απαιτείται η εξακρίβωση του κατά πόσο το ακραίο σημείο βρίσκεται πίσω από NAT και, εάν αληθεύει, του τρόπου λειτουργίας του NAT. Οι διάφοροι τρόποι συμπεριφοράς των NAT ταξινομούνται στο RFC 4787. Αυτοί αφορούν τους κανόνες αντιστοίχισης διευθύνσεων-θυρών (Address and Port Mapping), τον διαμοιρασμό διευθύνσεων IP (IP Address Pooling) και την εκχώρηση θυρών (Port Assignment).

Όσον αφορά την αντιστοίχιση διευθύνσεων-θυρών υπάρχουν τρεις τρόποι: η ανεξάρτητη του ακραίου σημείου αντιστοίχιση (endpoint-independent mapping), η εξαρτώμενη από τη διεύθυνση αντιστοίχιση (address-dependent mapping) και η εξαρτώμενη από τη διεύθυνση και τη θύρα αντιστοίχιση (address and port-dependent mapping). Στην ανεξάρτητη του ακραίου σημείου αντιστοίχιση, το NAT αποδίδει στα απερχόμενα πακέτα την ίδια εξωτερική θύρα πηγής (π.χ. 6000) για κάθε πακέτο με την ίδια εσωτερική θύρα πηγής (π.χ. 5000) και ίδια διεύθυνση πηγής (π.χ. 10.0.0.1) ανεξαρτήτως διεύθυνσης και θύρας προορισμού. Στην εξαρτώμενη από τη διεύθυνση αντιστοίχιση, το NAT αποδίδει στα απερχόμενα πακέτα την ίδια εξωτερική θύρα πηγής (π.χ. 6000) για κάθε πακέτο με την ίδια εσωτερική θύρα πηγής (π.χ. 5000), ίδια διεύθυνση πηγής (π.χ. 10.0.0.1) και ίδια διεύθυνση προορισμού (π.χ. 5.5.5.1) ανεξαρτήτως θύρας προορισμού. Τέλος, στην εξαρτώμενη από τη διεύθυνση και τη θύρα αντιστοίχιση, το NAT αποδίδει στα απερχόμενα πακέτα την ίδια εξωτερική θύρα πηγής (π.χ. 6000) για κάθε πακέτο με την ίδια εσωτερική θύρα πηγής (π.χ. 5000), ίδια διεύθυνση πηγής (π.χ. 10.0.0.1), ίδια διεύθυνση προορισμού (π.χ. 5.5.5.1) και ίδια θύρα προορισμού (π.χ. 80).

Ο διαμοιρασμός διευθύνσεων IPv4, στην περίπτωση που είναι περισσότερες της μίας διαθέσιμες, μπορεί να είναι αυθαίρετος ή σε ζεύγη. Στον αυθαίρετο διαμοιρασμό, αποδίδεται η ίδια εξωτερική διεύθυνση IPv4 πηγής για όλα τα πακέτα που ανήκουν σε μια συγκεκριμένη σύνοδο (έχουν στο εσωτερικό δίκτυο την ίδια τετράδα διευθύνσεων και θυρών IPv4, πηγής και προορισμού). Στο διαμοιρασμό σε ζεύγη, αποδίδεται η ίδια εξωτερική διεύθυνση IPv4 πηγής για την ίδια εσωτερική διεύθυνση IPv4.

Στην εκχώρηση θυρών, το NAT μπορεί κατά τη μετάφραση να διατηρεί (port preservation) ή να μην διατηρεί (no port preservation) την εσωτερική θύρα πηγής. Στη διατήρηση εσωτερικών θυρών, δεν μπορεί να αποκλεισθεί η περίπτωση συγκρούσεων. Τότε η εξωτερική θύρα πηγής αναγκαστικά επιλέγεται διαφορετική της εσωτερικής. Στην περίπτωση μη διατήρησης, το NAT χρησιμοποιεί ως εξωτερικές θύρες την περιοχή των ιδιωτικών/δυναμικών θυρών (49192 ~ 65535). Τότε για κάθε

δημόσια διεύθυνση που διαθέτει μπορεί να υποστηρίξει έως 16.000 συνόδους. Εναλλακτικά, το NAT μπορεί να χρησιμοποιήσει και την περιοχή των καταχωρημένων (registered) θυρών (1024 ~ 65535), αφού προηγουμένως εξαντλήσει τις ιδιωτικές.

Παρόμοια με την αντιστοίχιση θυρών και διευθύνσεων που αφορά τα εξερχόμενα πακέτα διακρίνονται τρεις τρόποι φιλτραρίσματος των εισερχόμενων πακέτων. Το ανεξάρτητο του ακραίου σημείου φιλτράρισμα (endpoint-independent filtering), το εξαρτώμενο από τη διεύθυνση φιλτράρισμα (address-dependent filtering) και το εξαρτώμενο από τη διεύθυνση και τη θύρα φιλτράρισμα (address and port-dependent filtering). Στο ανεξάρτητο του ακραίου σημείου φιλτράρισμα, το NAT δέχεται τα εισερχόμενα πακέτα βάσει της διεύθυνσης προορισμού και της θύρας προορισμού, ανεξάρτητα της διεύθυνσης πηγής και θύρας πηγής. Στο εξαρτώμενο από τη διεύθυνση φιλτράρισμα, το NAT δέχεται τα εισερχόμενα πακέτα βάσει της διεύθυνσης προορισμού, της θύρας προορισμού και της διεύθυνσης πηγής, ανεξάρτητα της θύρας πηγής. Στο εξαρτώμενο από τη διεύθυνση και τη θύρα φιλτράρισμα, το NAT δέχεται τα εισερχόμενα πακέτα βάσει της διεύθυνσης προορισμού, της θύρας προορισμού, της διεύθυνσης πηγής και της θύρας πηγής.

Με βάση την παραπάνω κατηγοριοποίηση της συμπεριφοράς οι τέσσερεις παραδοσιακές υλοποιήσεις NAT (Full cone, Restricted Cone, Port Restricted Cone, Symmetric) που περιγράφονται στη συνέχεια μπορούν απλά να ορισθούν ως συνδυασμός κανόνων αντιστοίχισης και φιλτραρίσματος. Στο NAT πλήρους κώνου, η κίνηση από την ίδια εσωτερική θύρα και διεύθυνση αντιστοιχεί στην ίδια εξωτερική θύρα και διεύθυνση [ανεξάρτητη του ακραίου σημείου αντιστοίχιση]. Οποιοσδήποτε εξωτερικός υπολογιστής μπορεί να στείλει πακέτα σε ένα εσωτερικό υπολογιστή χρησιμοποιώντας τη μεταφρασμένη εξωτερική θύρα και διεύθυνση [ανεξάρτητο του ακραίου σημείου φιλτράρισμα]. Στο NAT περιορισμένου κώνου και πάλι η κίνηση από την ίδια εσωτερική θύρα και διεύθυνση αντιστοιχεί στην ίδια εξωτερική θύρα και διεύθυνση [ανεξάρτητη του ακραίου σημείου αντιστοίχιση]. Σε αντίθεση με το NAT πλήρους κώνου, ένας εξωτερικός υπολογιστής μπορεί να στείλει πακέτα σε εσωτερικό υπολογιστή μόνο με διεύθυνση πηγής στην οποία προηγουμένως έχει λάβει ένα πακέτο από τον εσωτερικό υπολογιστή [εξαρτώμενο από τη διεύθυνση φιλτράρισμα]. Το NAT περιορισμένου ανά θύρα κώνου είναι ένα NAT περιορισμένου κώνου [ανεξάρτητη του ακραίου σημείου αντιστοίχιση], όπου ένας εξωτερικός υπολογιστής μπορεί να στείλει πακέτα με διεύθυνση και θύρα πηγής στις οποίες έχει προηγουμένως έχει λάβει ένα πακέτο από τον εσωτερικό υπολογιστή [εξαρτώμενο από τη διεύθυνση και τη θύρα φιλτράρισμα]. Στο συμμετρικό NAT όλα τα πακέτα με την ίδια εσωτερική θύρα και διεύθυνση αντιστοιχούν στην ίδια εξωτερική θύρα και διεύθυνση. Πακέτα με την ίδια εσωτερική θύρα και διεύθυνση, αλλά διαφορετικό προορισμό αντιστοιχούν σε διαφορετικό ζεύγος εξωτερικής θύρας και διεύθυνσης [εξαρτώμενη από τη διεύθυνση και τη θύρα αντιστοίχιση]. Επιπλέον μόνο ο εξωτερικός υπολογιστής που έχει λάβει πακέτο μπορεί να στείλει σε εσωτερικό μηχάνημα [εξαρτώμενο από τη διεύθυνση και τη θύρα φιλτράρισμα].

FreeBSD firewalls

Στο FreeBSD υποστηρίζονται τρία διαφορετικά τείχη προστασίας τα ipfw, ipfilter και 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). 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.

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:

kldload *module* φορτώνει στον πυρήνα το αρχείο *module.ko*

kldunload *module* αφαιρεί από τον πυρήνα τη μονάδα με όνομα *module*

kldstat εμφανίζει την κατάσταση όλων των φορτωμένων λειτουργικών μονάδων.

Το τείχος προστασίας ipfw

Λειτουργεί βάσει λίστας κανόνων (ruleset) που αριθμούνται από 1 μέχρι 65535. Για κάθε πακέτο που διέρχεται από το τείχος προστασίας ελέγχονται οι κανόνες της λίστας κατ' αύξουσα σειρά. Εάν υπάρχουν πολλοί κανόνες με τον ίδιο αύξοντα αριθμό, τότε ο έλεγχος γίνεται με τη σειρά εισαγωγής τους. Εάν βρεθεί ταίριασμα σε κάποιο κανόνα, εκτελείται η ενέργεια που αντιστοιχεί σε αυτόν και τερματίζει η αναζήτηση (first match wins). Όμως, ανάλογα με την ενέργεια που ορίζεται, το πακέτο μπορεί να εισέλθει ξανά στο τείχος για περαιτέρω επεξεργασία. Η λίστα κανόνων περιέχει πάντα τον προκαθορισμένο κανόνα με α/α 65535 που δεν μπορεί να αλλάξει ή διαγραφεί. Η ενέργεια σε περίπτωση ταιριάσματος με τον προκαθορισμένο κανόνα είναι να απορρίψει σιωπηλά όλα τα πακέτα.

Η εντολή φλοιού ipfw είναι η διεπαφή χρήστη για την παραμετροποίηση του αντίστοιχου τείχους προστασίας στο FreeBSD και διαθέτει μια μεγάλη σειρά υπο-εντολών ως εξής:

ipfw add *rule* για την εισαγωγή του κανόνα *rule* στο τείχος προστασίας,

ipfw delete *number* για τη διαγραφή του υπ' αριθμόν *number* κανόνα,

ipfw flush για τη διαγραφή όλων των κανόνων,

ipfw list για εμφάνιση λίστας με όλους τους κανόνες,

ipfw show για εμφάνιση των κανόνων σε συνδυασμό με τους αντίστοιχους μετρητές χρήσης τους,

ipfw zero για μηδενισμό των μετρητών χρήσης,

ipfw nat για εντολές σχετικά με τη λειτουργία NAT (δείτε λεπτομέρειες πιο κάτω).

Όταν δημιουργείτε ένα κανόνα με την εντολή "ipfw add" οι λέξεις κλειδιά πρέπει να γραφτούν με τη σωστή σειρά (κάποιες είναι υποχρεωτικές, οι άλλες προαιρετικές) ως εξής:

ipfw add *rule_number action proto* **from** *src src_port* **to** *dst dst_port options*, όπου

rule_number είναι ο αύξων αριθμός του κανόνα. Εάν δεν τεθεί ρητά, ο πυρήνας ορίζει αυτόματα αριθμό μεγαλύτερο κατά 100 του αύξοντα αριθμού του τελευταίου πριν τον προκαθορισμένο κανόνα,

action είναι η ενέργεια που σχετίζεται με τον κανόνα, όπως *allow* για να γίνει αποδεκτό το πακέτο, *deny* για να απορριφθεί το πακέτο, *check-state* για να ελεγχθούν τυχόντες κανόνες που έχουν δημιουργηθεί δυναμικά (δείτε *keep-state* πιο κάτω) και εάν βρεθεί ταίριασμα να εκτελείται η ενέργεια που αντιστοιχεί στη δημιουργία του δυναμικού κανόνα, *nat nat_nr* για να σταλεί το πακέτο για μετάφραση διευθύνσεων σύμφωνα με τον υπ' αριθμό *nat_nr* πίνακα NAT (δείτε μηχανισμό NAT πιο κάτω), *skipto number* για να συνεχισθεί ο έλεγχος με τον κανόνα υπ' αριθμό *number*, κλπ,

proto είναι το <u>όνομα</u> του πρωτοκόλλου (ή ο <u>αριθμός</u> πρωτοκόλλου όπως εμφανίζεται στο αρχείο /etc/protocols), είτε η λέξη <u>*ip4*</u> ή <u>*ipv4*</u> για το πρωτόκολλο IPv4, είτε η λέξη <u>*ip6*</u> ή <u>*ipv6*</u> για το πρωτόκολλο IPv6 είτε η λέξη <u>*ip*</u> ή <u>*all*</u> που δηλώνει οποιοδήποτε πρωτόκολλο,

το *src* ακολουθεί το **from** και αντιστοιχεί στη <u>διεύθυνση πηγής</u> των πακέτων, όπου η λέξη <u>*any*</u> δηλώνει οποιαδήποτε διεύθυνση και η λέξη <u>*me*</u> δηλώνει οποιαδήποτε διεύθυνση έχει ορισθεί σε κάποια διεπαφή του συστήματος,

το προαιρετικό *src_port* δηλώνει το <u>όνομα</u> της θύρας (ή τον <u>αριθμό</u> θύρας όπως εμφανίζεται στο αρχείο /etc/services),

το *dst* ακολουθεί το **to** και αντιστοιχεί στη <u>διεύθυνση προορισμού</u> των πακέτων,

το προαιρετικό *dst_port* δηλώνει το <u>όνομα</u> ή τον <u>αριθμό</u> θύρας, και τέλος

στο *options* μπορεί μεταξύ πολλών άλλων να δηλωθεί, <u>*in*</u> ή <u>*out*</u> για να προσδιοριστεί η φορά της ροής των πακέτων, <u>*recv*</u>, <u>*xmit*</u>, <u>*via*</u> για να προσδιοριστεί η διεπαφή από όπου λαμβάνεται, μεταδίδεται ή διέρχεται το πακέτο, <u>*icmptypes*</u> ακολουθούμενο από τους τύπους πακέτων ICMP για συγκεκριμένα μηνύματα ICMP, <u>*setup*</u> για πακέτα εγκατάστασης σύνδεσης TCP (με σημαία SYN, χωρίς ACK), <u>*established*</u> για πακέτα TCP που ανήκουν σε κάποια σύνδεση (περιέχουν σημαία ACK ή RST) και το <u>*keep-state*</u>, για τη δημιουργία δυναμικού κανόνα.

Όταν υπάρξει ταίριασμα σε κανόνα που λήγει με το *keep-state*, τότε το τείχος προστασίας λειτουργεί βάσει της κατάστασης (stateful behavior). Δημιουργείται δηλαδή ένας δυναμικός κανόνας που ταιριάζει για το συγκεκριμένο πρωτόκολλο την αμφίδρομη κίνηση μεταξύ των διευθύνσεων πηγής και προορισμού και των αντίστοιχων θυρών πηγής και προορισμού. Οι δυναμικοί κανόνες έχουν περιορισμένο χρόνο ζωής που ανανεώνεται όσο υπάρχει κίνηση που ταιριάζει. Οι δυναμικοί κανόνες ελέγχονται με κανόνα που έχει ως ενέργεια το *check-state* και εάν δεν υπάρχει τέτοιος στην πρώτη εμφάνιση κανόνα με *keep-state*. Για τον λόγο αυτό ο κανόνας *check-state* πρέπει να τίθεται στην αρχή ώστε να αποφεύγεται ο άσκοπος έλεγχος αυτών που έπονται μέχρι την εμφάνιση του *keep-state* και ίσως απαγορεύουν την εν λόγω κίνηση.

Εάν χρειάζεται καταγραφή των πακέτων που ταιριάζουν σε κάποιο κανόνα, τότε πρέπει να προστεθεί η λέξη *log* αμέσως μετά το εκάστοτε *action*. Για παράδειγμα η εντολή "*ipfw add 100 deny log ip from 10.0.0.0/8 to me*" εισάγει κανόνα με αριθμό 100 που απορρίπτει όλη την κίνηση από το δίκτυο 10.0.0.0/8 και καταγράφει τα πακέτα που απορρίφθηκαν. Η καταγραφή μπορεί να γίνει είτε σε αρχείο είτε με tcpdump στη ψευδο-διεπαφή ipfw0, η οποία όμως θα πρέπει να έχει δημιουργηθεί προηγουμένως με την εντολή *ifconfig ipfw0 create*.

Πολλές φορές για να επιτραπεί κάποιου είδους κίνηση απαιτείται η συνδυασμένη χρήση κανόνων. Για παράδειγμα, οι εντολές "*ipfw add 200 allow tcp from any to any established*" και "*ipfw add 210 allow tcp from me to any setup*" εισάγουν στατικούς κανόνες που επιτρέπουν την εγκατάσταση συνδέσεων TCP προς οποιαδήποτε διεύθυνση IP (ο δεύτερος) και την ανταλλαγή τεμαχίων TCP σε συνδέσεις που έχουν ήδη εγκατασταθεί (ο πρώτος). Εναλλακτικά, οι εντολές "*ipfw add 10 check-state* ", "*ipfw add 200 deny tcp from any to any established*" και "*ipfw add 210 allow tcp from me to any setup keep-state*" εισάγουν (stateful) κανόνα που επιτρέπει την εγκατάσταση συνδέσεων TCP προς οποιαδήποτε διεύθυνση IP (ο τελευταίος) και στατικό κανόνα που απορρίπτει τεμάχια TCP για τα οποία δεν έχει εγκατασταθεί σύνδεση (ο δεύτερος). Αντίστοιχα, οι εντολές "*ipfw add 300 allow udp from me to any 53 keep-state*" και "*ipfw add 310 allow tcp from me to any 53 setup keep-state*" εισάγουν (stateful) κανόνες που επιτρέπουν τις ερωτήσεις σε εξυπηρετητή DNS και λήψη απαντήσεων από αυτόν. Ο κανόνας με την εντολή *check-state* πρέπει να προηγηθεί όλων ώστε να επιτραπεί η διέλευση πακέτων τα οποία ταιριάζουν στους κανόνες που δημιουργήθηκαν δυναμικά. Στο παράδειγμα, χωρίς αυτόν, ο δεύτερος κανόνας θα τα απέρριπτε.

Για περισσότερες λεπτομέρειες για το ipfw δείτε το εγχειρίδιο του FreeBSD στην ιστοθέση https://docs.freebsd.org/en/books/handbook/firewalls/#firewalls-ipfw. Η πλήρης τεκμηρίωση βρίσκεται στη σχετική σελίδα man https://www.freebsd.org/cgi/man.cgi?query=ipfw. Τέλος στην ιστοσελίδα https://www.adminbyaccident.com/freebsd/how-to-freebsd/how-to-configure-the-ipfw-firewall-on-freebsd/ θα βρείτε ένα πλήρες παράδειγμα χρήσης του ipfw.

Ο ενσωματωμένος στον πυρήνα μηχανισμός NAT

Το FreeBSD περιλαμβάνει έναν ενσωματωμένο στον πυρήνα μηχανισμό NAT (in-kernel NAT) που λειτουργεί σε συνδυασμό με το ipfw χρησιμοποιώντας τη βιβλιοθήκη libalias. Για τη λειτουργία μετάφρασης διευθύνσεων (NAT) πρέπει πρώτα να δημιουργηθεί στο τείχος προστασίας ένας πίνακας NAT (δείτε πιο κάτω) και μετά να προστεθεί στο τείχος προστασίας κανόνας (δείτε ενέργεια *nat* *nat_nr* της εντολής "ipfw add" προηγουμένως) ώστε η κίνηση που ταιριάζει σε αυτόν να ωθείται στον πίνακα NAT προκειμένου να υποστεί την οριζόμενη εκεί μετάφραση διευθύνσεων (και θυρών). Οι σχετικές με τον ενσωματωμένο στον πυρήνα μηχανισμό NAT εντολές είναι:

ipfw nat *nat_number* **config** *nat-configuration* για τη δημιουργία πίνακα NAT όπου *nat_number* είναι ο αριθμός παρουσίας (instance) του πίνακα NAT στο τείχος προστασίας, και *nat-configuration* ορίζει τη μετάφραση (aliasing) διευθύνσεων IP (και θυρών) που υφίσταται η κίνηση που ωθείται στη συγκεκριμένη παρουσία πίνακα NAT.

ipfw nat *nat_number* **show config** για να δείτε την τρέχουσα διάρθρωση του πίνακα NAT με αριθμό *nat_number*.

ipfw nat show config για να δείτε την τρέχουσα διάρθρωση όλων των πινάκων NAT.

Όσον αφορά τη διάρθρωση ενός πίνακα NAT μερικές συνήθεις εντολές ρύθμισης είναι:

ip *ip_address*: ορίζει τη διεύθυνση IPv4 που θα χρησιμοποιηθεί στη μετάφραση (aliasing)

if *nic*: ορίζει ότι στη μετάφραση θα χρησιμοποιηθεί η διεύθυνση IPv4 της κάρτας *nic* (ακόμη και εάν αυτή αλλάζει δυναμικά)

same_ports: προσπάθεια να μην αλλάξουν οι αριθμοί θυρών κατά τη μετάφραση

reset: αρχικοποιεί τον πίνακα εάν αλλάζει η διεύθυνση για τη μετάφραση

deny_in: απορρίπτει εισερχόμενη κίνηση για την οποία δεν υπάρχει εγγραφή στον πίνακα

unreg_only: μόνο πακέτα με ιδιωτικές διευθύνσεις RFC 1918 υφίστανται μετάφραση

Για την απερχόμενη κίνηση, η διεύθυνση πηγής των πακέτων μεταφράζεται στη διεύθυνση που ορίζει η εντολή **ip** ή **if**. Για εισερχόμενη κίνηση γίνεται πρώτα έλεγχος για το κατά πόσο υπάρχει ήδη αντιστοιχία στον πίνακα NAT λόγω απερχόμενης κίνησης. Εάν δεν υπάρχει, θα γίνει έλεγχος για εντολές ανακατεύθυνσης. Η ανακατεύθυνση (redirection) της εισερχόμενης κίνησης μπορεί να γίνει με τις εντολές:

redirect_addr *localIP publicIP*: στατικό NAT που μεταφράζει εισερχόμενη κίνηση με προορισμό τη δημόσια διεύθυνση *publicIP* στην εσωτερική διεύθυνση *localIP*, και αντιστρόφως.

redirect_proto *proto localIP [publicIP [remoteIP]]*: εισερχόμενη κίνηση πρωτοκόλλου *proto* με προορισμό τη δημόσια διεύθυνση *publicIP* μεταφράζεται στην εσωτερική διεύθυνση *localIP*, και αντιστρόφως. Εάν δεν ορίζεται *publicIP*, χρησιμοποιείται η προκαθορισμένη για τη μετάφραση NAT διεύθυνση. Εάν προσδιορίζεται *remoteIP*, τότε μόνο πακέτα από ή προς αυτή τη διεύθυνση υφίστανται μετάφραση.

redirect_port *proto targetIP:targetPort [aliasIP:]aliasPort [remoteIP[:remotePort]]*: εισερχόμενη κίνηση με προορισμό τη θύρα *aliasPort* του πρωτοκόλλου *proto* (μόνο tcp ή udp) μεταφράζεται στη διεύθυνση *targetIP* και θύρα *targetPort*. Εάν ορίζεται, *aliasIP* είναι η εξωτερική διεύθυνση. Εάν

προσδιορίζεται *remoteIP* (και *remotePort*) τότε μόνο πακέτα από ή προς αυτή τη διεύθυνση (και θύρα) υφίστανται μετάφραση.

Οι εντολές διάρθρωσης μπορούν να συγκεντρωθούν σε μία σύνθετη εντολή. Π.χ, για να μεταφράζει το NAT με αριθμό 123 όλη την εξερχόμενη κίνηση στη διεύθυνση IPv4 192.0.2.1, να μπλοκάρει τις εισερχόμενες συνδέσεις, να προσπαθεί να διατηρήσει τους ίδιους αριθμούς θυρών και να αρχικοποιεί τον πίνακα σε περίπτωση αλλαγής της διεύθυνσης IPv4, πρέπει να δοθεί η εντολή διάρθρωσης "*ipfw nat 123 config ip 192.0.2.1 deny_in reset same_ports*". Για να επιτελείται η λειτουργία NAT που ορίζει η προηγούμενη εντολή διάρθρωσης πρέπει στη συνέχεια να εισαχθεί στο τείχος προστασίας κανόνας ώστε η κίνηση να ωθείται προς μετάφραση. Π.χ. με την εντολή "*ipfw add 100 nat 123 all from any to any*" όλη η κίνηση γίνεται δεκτή και ωθείται στον πίνακα NAT με αριθμό 123 για μετάφραση.

Για περισσότερες λεπτομέρειες δείτε τις εντολές διάρθρωσης του NAT στην παράγραφο "NETWORK ADDRESS TRANSLATION (NAT)" της σελίδας man του ipfw στην ιστοσελίδα https://www.freebsd.org/cgi/man.cgi?query=ipfw καθώς και τα παραδείγματα χρήσης στην παράγραφο "NAT, REDIRECT AND LSNAT" της ως άνω ιστοσελίδας. Τέλος θα βρείτε ένα πλήρες παράδειγμα χρήσης NAT στην ιστοθέση https://sirtoffski.github.io/docs/freebsd-ipfw.

Το τείχος προστασίας m0n0wall

Το m0n0wall είναι μια διανομή του FreeBSD για ενσωματωμένα συστήματα που κυρίως επιτελούν τη λειτουργία ενός τείχους προστασίας σε συνδυασμό με NAT. Το m0n0wall χρησιμοποιεί το ipfilter, αλλά το πιο ενδιαφέρον χαρακτηριστικό του είναι το γραφικό περιβάλλον διαχείρισης μέσω ιστοσελίδων (webGUI) που περιλαμβάνεται στη διανομή. Όπως θα διαπιστώσετε, 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. Για περισσότερες λεπτομέρειες δείτε το σχετικό εγχειρίδιο https://doc.m0n0.ch/handbook/.

Προετοιμασία στο σπίτι

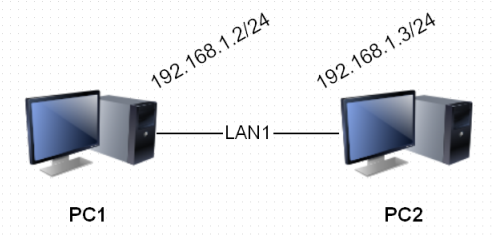
Ετοιμάστε ένα τείχος προστασίας ξεκινώντας από ένα νέο FreeBSD 12.4 με δύο κάρτες δικτύου. Χρησιμοποιώντας την εντολή sysrc (δείτε https://www.freebsd.org/cgi/man.cgi?query=sysrc) προσθέστε τις ακόλουθες μεταβλητές στο /etc/rc.conf:

```
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_nat_enable="YES"
firewall_logif="YES"
```

Ονοματίστε το εικονικό μηχάνημα ως FW1, ορίστε τις δύο κάρτες δικτύου σε εσωτερική δικτύωση και στη συνέχεια κλείστε το. Ακολουθώντας την διαδρομή *File→Export Appliance* στο Virtual Box αποθηκεύεστε την εικόνα του τείχους προστασίας ως FW1.ova, που θα χρησιμοποιήσετε στη συνέχεια της άσκησης.

Άσκηση 1: Ένα απλό τείχος προστασίας

Κατασκευάστε στο VirtualBox το παρακάτω δίκτυο, όπου τα PC είναι απλά εικονικά μηχανήματα FreeBSD 12.4. Το PC1 είναι ένας απλός πελάτης και το PC2 είναι ένας απλός εξυπηρετητής. Στο PC1 θα ενεργοποιήσετε το τείχος προστασίας και θα εισάγετε κανόνες ώστε να μπορεί να επικοινωνεί με μηχανήματα στο LAN1, το PC2 στην άσκηση αυτή.



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

1.1 Στο PC1 φορτώστε στον πυρήνα το τείχος προστασίας ipfw.

1.2 Με ποια εντολή στο PC1 μπορείτε να επιβεβαιώσετε ότι είναι ενεργό το τείχος προστασίας ipfw;

1.3 Μπορείτε να κάνετε ping στη διεύθυνση IP του βρόχου επιστροφής lo0 ή της διεπαφής em0; Ποιο λάθος βλέπετε;

1.4 Βρείτε τους κανόνες που υπάρχουν στο τείχος προστασίας του PC1.

1.5 Βρείτε στοιχεία για τη χρήση των προηγούμενων κανόνων.

1.6 Πώς μπορείτε να μηδενίσετε τους σχετικούς με τη χρήση των κανόνων μετρητές;

1.7 Προσθέστε στο τείχος προστασίας του PC1 κανόνα με αύξοντα αριθμό 100 που να επιτρέπει μέσω της διεπαφής lo0 όλη την κίνηση (οποιοδήποτε πρωτόκολλο, από και προς οποιαδήποτε διεύθυνση). *[Υποδ. Δείτε παράδειγμα στην παράγραφο Example Ruleset για το IPFW στο FreeBSD Handbook https://docs.freebsd.org/en/books/handbook/firewalls/#firewalls-ipfw.]*

1.8 Είναι τώρα τα ping της 1.3 επιτυχή;

1.9 Μπορείτε να κάνετε ping από το PC1 στο PC2; Ποιο λάθος βλέπετε;

1.10 Προσθέστε κανόνα στο τείχος προστασίας του PC1 ώστε να επιτρέπεται η κίνηση ICMP από και προς οποιαδήποτε διεύθυνση IP.

1.11 Τι αύξοντα αριθμό έλαβε ο κανόνας;

1.12 Μπορείτε τώρα να κάνετε ping από το PC1 στο PC2; Μπορείτε από το PC2 στο PC1;

1.13 Γιατί δεν μπορείτε από το PC1 να κάνετε traceroute στο PC2; Με ποια απλή αλλαγή στη σύνταξη της εντολής traceroute θα λάβετε απάντηση από το PC2;

1.14 Προσθέστε κανόνα στο τείχος προστασίας του PC1 ώστε το traceroute από το PC1 προς οποιοδήποτε προορισμό να λειτουργεί. *[Υποδ. Δείτε σελίδες man για τη λειτουργία του traceroute και τη χρήση θυρών από αυτό.]*

1.15 Μπορείτε από το PC1 να συνδεθείτε με ssh στο PC2;

1.16 Προσθέστε δύο στατικούς κανόνες που να επιτρέπουν τη σύνδεση του PC1 σε απομακρυσμένους εξυπηρετητές με tcp.

1.17 Στο PC1 μηδενίστε τους μετρητές χρήσης των κανόνων και συνδεθείτε με ssh στο PC2, εκτελέστε την εντολή ls και αποσυνδεθείτε.

1.18 Πόσες φορές εφαρμόσθηκε ο κάθε κανόνας που προσθέσατε; Γιατί;

1.19 Μπορείτε από το PC2 να συνδεθείτε με ssh στο PC1; Γιατί;

1.20 Στο PC2 ξεκινήστε τον δαίμονα ftpd ώστε αυτό να λειτουργεί ως εξυπηρετητής FTP. *[Υποδ. σελίδες man για την εντολή service.]*

1.21 Μπορείτε από το PC1 να συνδεθείτε με ftp στο PC2 ως χρήστης lab και να κατεβάσετε ένα αρχείο από το /usr/bin του PC2 στο PC1;

Άσκηση 2: Ένα πιο σύνθετο τείχος προστασίας

Στο δίκτυο της προηγούμενης άσκησης θα ενεργοποιήσετε το τείχος προστασίας (firewall) και στο PC2. Απαντήστε τις παρακάτω ερωτήσεις καταγράφοντας παράλληλα, όπου απαιτείται, την ακριβή σύνταξη των εντολών που χρησιμοποιήσατε.

2.1 Στο PC2 φορτώστε στον πυρήνα το τείχος προστασίας ipfw.

2.2 Μπορείτε να κάνετε ping από το PC2 στο PC1;

2.3 Προσθέστε στο τείχος προστασίας του PC2 κανόνα που να επιτρέπει μέσω της διεπαφής lo0 όλη την κίνηση.

2.4 Προσθέστε κανόνα στο τείχος προστασίας του PC2 που να επιτρέπει κίνηση ICMP τύπου echo request από το PC2 προς οποιαδήποτε διεύθυνση IP. *[Υποδ. Συμβουλευθείτε σελίδα βοήθειας man για ipfw, κεφάλαιο RULE OPTIONS για τους τύπους ICMP.]*

2.5 Μπορείτε να κάνετε ping από το PC2 στο PC1;

2.6 Περνούν τα πακέτα ICMP το τείχος προστασίας του PC2; Τεκμηριώστε την απάντησή σας παρατηρώντας του σχετικούς με τον προηγούμενο κανόνα μετρητές πακέτων.

2.7 Διαγράψτε τον κανόνα για το ICMP και επανεισάγετέ τον προσθέτοντας στο τέλος το "*keep-state*". Μπορείτε να κάνετε ping από το PC2 στο PC1;

2.8 Ξεκινήστε πάλι το ping από το PC2 στο PC1 και αφήστε το να τρέχει. Μπορείτε να κάνετε ping από το PC1 στο PC2;

2.9 Σταματήστε τα ping στο PC2 και περιμένετε λίγο. Επιτυγχάνει τώρα το ping από το PC1 στο PC2; Γιατί;

2.10 Προσθέστε (stateful) κανόνα ώστε το PC2 να απαντά σε ICMP echo request ανεξάρτητα από πού προέρχονται.

2.11 Ξεκινήστε ένα ping από το PC1 στο PC2 και αφήστε το να τρέχει. Εκτελέστε στο PC2 την εντολή "*ipfw –d show*". Τι βλέπετε;

2.12 Σταματήστε το ping από το PC1, περιμένετε λίγα δευτερόλεπτα και ξαναεκτελέστε στο PC2 την προηγούμενη εντολή. Τι βλέπετε;

2.13 Προσθέστε <u>δύο</u> κανόνες στο τείχος προστασίας του PC2 ώστε το traceroute προς το PC2 να λειτουργεί. Ο πρώτος να επιτρέπει τη λήψη από οποιαδήποτε διεύθυνση IP των πακέτων UPD που παράγει η traceroute. Ο δεύτερος να επιτρέπει την αποστολή μηνυμάτων ICMP destination unreachable προς οποιονδήποτε προορισμό.

2.14 Προσθέστε <u>δύο</u> κανόνες στο τείχος προστασίας του PC2 ώστε να λειτουργεί το traceroute από το PC2 προς οποιαδήποτε διεύθυνση IP

2.15 Ποιον κανόνα πρέπει να προσθέσετε στο PC1 ώστε να απαντά σε traceroute από οποιαδήποτε διεύθυνση IP;

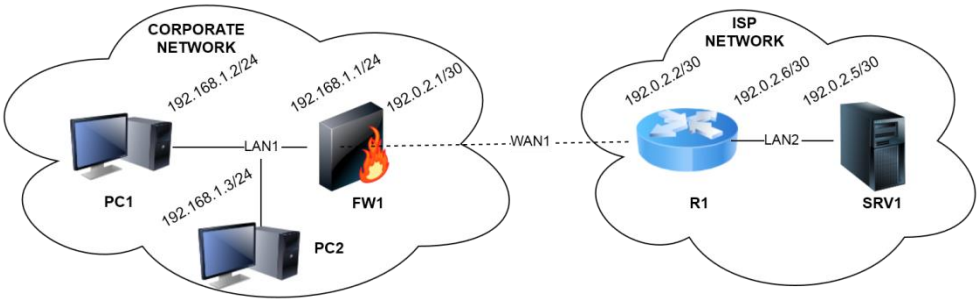
2.16 Προσθέστε <u>ένα</u> (stateful) κανόνα στο τείχος προστασίας του PC2 ώστε να μπορείτε να συνδεθείτε σε αυτό με ssh από οποιονδήποτε υπολογιστή του υποδικτύου 192.168.1.0/24.

2.17 Με ποια εντολή επιβεβαιώσατε στο PC1 την ορθότητα του προηγούμενου κανόνα;

2.18 Προσθέστε ένα (stateful) κανόνα στο τείχος προστασίας του PC2 ώστε να μπορείτε να συνδεθείτε με ssh σε οποιοδήποτε άλλο μηχάνημα.
2.19 Ποιον έναν επιπλέον κανόνα πρέπει να προσθέσετε στο PC1 ώστε να δέχεται συνδέσεις ssh μόνο από το PC2;
2.20 Μπορείτε από το PC1 να συνδεθείτε με sftp στο PC2 ως χρήστης lab και να κατεβάσετε το αρχείο /etc/rc.conf;
2.21 Μπορείτε από το PC1 να συνδεθείτε με ftp στο PC2; Εάν όχι, προσθέστε κανόνα στο τείχος προστασίας του PC2 ώστε να επιτρέπει τη σύνδεση ftp.
2.22 Συνδεθείτε με ftp ως χρήστης lab και εκτελέστε τις εντολές "*cd /usr*" και "*ls*". Γιατί η πρώτη εκτελείται επιτυχώς ενώ η δεύτερη αποτυγχάνει;
2.23 Ποιον κανόνα πρέπει να προσθέσετε στο τείχος προστασίας του PC2 ώστε το ftp σε passive mode να λειτουργεί σωστά; *[Δείτε http://www.slacksite.com/other/ftp.html.]*
2.24 Μπορείτε τώρα να κατεβάσετε ένα αρχείο από το /usr/bin του PC2 στο PC1;
2.25 Εάν θέλετε να λειτουργεί και το active mode του ftp, ποιον κανόνα πρέπει να προσθέσετε στο τείχος προστασίας του PC2 και ποιον στο τείχος προστασίας του PC1; *[Υπόδειξη: Επειδή το ftp ξεκινά σε passive mode και εάν αποτύχει μεταπίπτει σε active mode, δώστε την εντολή passive πριν την ls ώστε να ακυρωθεί το passive mode.]*
2.26 Σχολιάστε το θέμα χρήσης πρωτοκόλλων όπως το FTP και τειχών προστασίας.
2.27 Απενεργοποιήστε το ipfw στα PC1, PC2 και επιβεβαιώστε ότι απενεργοποιήθηκε.

Άσκηση 3: Απλό Network Address Translation

Κατασκευάστε στο VirtualBox το δίκτυο του παρακάτω σχήματος που αναπαριστά την περίπτωση ενός εταιρικού δικτύου συνδεδεμένου στο διαδίκτυο μέσω κάποιου ISP. Για PC χρησιμοποιήστε αυτά της προηγούμενης άσκησης και για το τείχος προστασίας FW1 το εικονικό μηχάνημα FW1.ova που κατασκευάσατε. Για δρομολογητή R1 χρησιμοποιήστε ένα εικονικό μηχάνημα BSDRP (router.ova) και για εξυπηρετητή SRV1 ένα νέο FreeBSD 12.4.



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

3.1 Ορίστε το όνομα, τη διεύθυνση IP και προεπιλεγμένη πύλη στα PC1 και PC2.
3.2 Ορίστε μέσω cli του R1 το όνομα, τη διεύθυνση IP για τη διεπαφή στο WAN1 και τη διεπαφή στο LAN2.
3.3 Ορίστε το όνομα, τη διεύθυνση IP και προεπιλεγμένη πύλη στο SRV1.
3.4 Στα PC2 και SRV1 ξεκινήστε τον δαίμονα ftpd ώστε αυτά να λειτουργούν ως εξυπηρετητές FTP.
3.5 Ποια modules έχουν φορτωθεί στον πυρήνα του FreeBSD στο FW1;

3.6 Ποιο τείχος προστασίας ενεργοποιήθηκε με την εντολή firewall_enable="YES" που θέσατε στο /etc/rc.conf; *[Υποδ. Δείτε https://www.freebsd.org/doc/handbook/firewalls.html]*.
3.7 Τι είδους λειτουργία του τείχους προστασίας έχει εγκατασταθεί; *[Υποδ. Με τη βοήθεια της sysrc δείτε τιμή της μεταβλητής firewall_type.]*
3.8 Πόσους κανόνες βλέπετε στο FW1; Ποιος είναι ο τελευταίος;
3.9 Έχουν ορισθεί πίνακες in-kernel NAT στο FW1; Εάν ναι, ποιοι;
3.10 Μπορείτε από το PC1 να κάνετε ping τη διεπαφή του FW1 στο LAN1 ή στο WAN1;
3.11 Μπορείτε από το SRV1 να κάνετε ping τη διεπαφή του FW1 στο WAN1;
3.12 Δημιουργήστε στο τείχος προστασίας του FW1 πίνακα in-kernel NAT με αριθμό παρουσίας 123 ώστε τα πακέτα με ιδιωτικές διευθύνσεις που ωθούνται σε αυτόν να υφίστανται μετάφραση στη διεύθυνση της διεπαφής του στο WAN1 και επιπλέον να αρχικοποιείται (reset) σε περίπτωση αλλαγής της διεύθυνσης IP της διεπαφής.
3.13 Προσθέστε κανόνα στο τείχος προστασίας του FW1 ώστε όλη η κίνηση IPv4 (από οποιαδήποτε πηγή προς οποιοδήποτε προορισμό) να ωθείται προς μετάφραση στον πίνακα NAT με αριθμό παρουσίας 123.
3.14 Μπορείτε από το PC1 να κάνετε ping τη διεπαφή του FW1 στο LAN1 (ή στο WAN1);
3.15 Ξεκινήστε καταγραφή πακέτων με το tcpdump στη διεπαφή του R1 στο WAN1.
3.16 Δείτε και μηδενίστε τους μετρητές πακέτων στο τείχος προστασίας του FW1.
3.17 Κάντε ping από το PC1 στο R1 και στείλτε τρία ICMP Echo request. Ποια η IP διεύθυνση πηγής των πακέτων ICMP echo request που βλέπετε στην καταγραφή;
3.18 Ποια η IP διεύθυνση προορισμού των ICMP Echo reply της καταγραφής στον R1;
3.19 Ποιος κανόνας του τείχους προστασίας είναι υπεύθυνος για την επιτυχία του ping;
3.20 Πόσες φορές εφαρμόσθηκε και γιατί;
3.21 Μπορείτε από το SRV1 να κάνετε ping τη διεπαφή του FW1 στο WAN1;
3.22 Ποιος κανόνας είναι υπεύθυνος για την αποδοχή της προηγούμενης κίνησης;
3.23 Ωθείται αυτή στο NAT προς μετάφραση διευθύνσεων; Γιατί;
3.24 Μπορείτε από το PC2 να συνδεθείτε με ssh ως χρήστης lab στο SRV1;
3.25 Γιατί δεν μπορείτε να κάνετε το αντίστροφο; Είναι θέμα δρομολόγησης ή NAT; Πώς το διαπιστώσατε;
3.26 Δημιουργήστε πίνακα NAT με αριθμό παρουσίας 123 (θα αντικαταστήσει τον υπάρχοντα) επαναλαμβάνοντας τις εντολές διάρθρωσης της ερώτησης 3.12 και προσθέτοντας νέα εντολή ώστε η κίνηση προς τη διεύθυνση IPv4 του FW1 στο WAN1 να ανακατευθύνεται στο PC2.
3.27 Από το SRV1 συνδεθείτε με ssh ως χρήστης lab στη διεύθυνση 192.0.2.1. Είναι η προσπάθεια επιτυχής; Εάν ναι, σε ποιο μηχάνημα συνδεθήκατε; Πως το εξακριβώσατε;
3.28 Δημιουργήστε πίνακα NAT με αριθμό παρουσίας 123 επαναλαμβάνοντας τις εντολές διάρθρωσης της ερώτησης 3.26 και προσθέτοντας νέα εντολή ώστε η κίνηση tcp για τη θύρα 22 να ανακατευθύνεται στο PC1 στην αντίστοιχη θύρα.
3.29 Συνδεθείτε και πάλι από το SRV1 με ssh ως χρήστης lab στη διεύθυνση 192.0.2.1. Σε ποιο μηχάνημα συνδέεστε τώρα και πώς το εξακριβώνετε;
3.30 Συνδεθείτε από το SRV1 με ftp ως χρήστης lab στη διεύθυνση 192.0.2.1. Σε ποιο μηχάνημα συνδέεστε και πώς το εξακριβώνετε;
3.31 Μπορείτε να δείτε τα περιεχόμενα το φακέλου /etc και να κατεβάσετε το αρχείο rc.conf;
3.32 Ποιο μηχάνημα απαντά εάν από το PC1 κάνετε ftp στη διεύθυνση 192.0.2.1;
3.33 Σε ποιο μηχάνημα θα συνδεθείτε εάν από το PC2 κάνετε ssh στη διεύθυνση 192.0.2.1;

Άσκηση 4: Τείχος προστασίας και NAT

Στην προηγούμενη άσκηση, με τον ορισμό του πίνακα NAT και τον αντίστοιχο κανόνα στο τείχος προστασίας, οι υπολογιστές του εταιρικού δικτύου, παρότι διαθέτουν ιδιωτικές διευθύνσεις, μπορούν να συνδέονται σε εξωτερικά μηχανήματα. Πέραν της μετάφρασης των διευθύνσεων, κρίσιμο για την εν λόγω λειτουργία είναι το γεγονός ότι η προκαθορισμένη λειτουργία one-pass του NAT στο ipfw επιτρέπει ταυτόχρονα την αποδοχή της κίνησης και τη μετάφραση διευθύνσεων. Όπως παρατηρήσατε, ο κανόνας ώθησης στο NAT της ερώτησης 3.13 αποδέχεται όλη την κίνηση IPv4. Έτσι τα μηχανήματα του LAN1 είχαν πρόσβαση τόσο στο FW1 όσο και σε εξωτερικά μηχανήματα (το διαδίκτυο). Για τα εξωτερικά μηχανήματα ο κανόνας επιτρέπει πρόσβαση μόνο στη δημόσια διεύθυνση του τείχους προστασίας στο WAN1, αλλά με τις εντολές ανακατεύθυνσης του πίνακα NAT επιτυγχάνεται πρόσβαση σε συγκεκριμένο ή συγκεκριμένα ανά υπηρεσία εσωτερικά μηχανήματα. Επιπλέον επειδή ο κανόνας δεν κάνει διάκριση σε διαπαφές και/ή φορά της κίνησης, οι εντολές ανακατεύθυνσης του NAT λειτουργούν και για κίνηση από το LAN1 προς τη δημόσια διεύθυνση του FW1.

Πολλές φορές στην πράξη απαιτείται πιο λεπτομερής έλεγχος της εισερχόμενης και εξερχόμενης κίνησης από το εταιρικό δίκτυο. Σε αυτές τις περιπτώσεις μπορεί να απενεργοποιηθεί η λειτουργία one-pass. Τότε μετά τη μετάφραση διευθύνσεων IP, η επεξεργασία των πακέτων συνεχίζει με τον επόμενο κανόνα του τείχους προστασίας. Προφανώς, η μετάφραση διευθύνσεων για τα εξερχόμενα από το τείχος προστασίας πακέτα γίνεται μετά τον έλεγχο αποδοχής τους. Όμως στην αντίστροφη κατεύθυνση, η μετάφραση διευθύνσεων για τα εισερχόμενα (σε απάντηση των εξερχόμενων) πακέτα πρέπει να προηγηθεί του ελέγχου αποδοχής τους. Για τον λόγο αυτό πρέπει να διαχωρίζεται η εισερχόμενη από την εξερχόμενη κίνηση, ώστε η λειτουργία της μετάφρασης NAT και της εφαρμογής των κανόνων τείχους προστασίας να πραγματοποιείται ακολουθιακά.

Στη συνέχεια θα εφαρμόσετε την τακτική αυτή στην τοπολογία της προηγούμενης άσκησης για ένα πιο λεπτομερή έλεγχο της κίνησης από και προς το εταιρικό δίκτυο. Πρώτα θα εγκαταστήσετε τους κανόνες που επιτρέπουν τον διαχωρισμό της μετάφρασης NAT από τον έλεγχο αποδοχής κίνησης. Στη συνέχεια θα εγκαταστήσετε (stateful) κανόνες που θα επιτρέπουν συγκεκριμένη εισερχόμενη ή εξερχόμενη κίνηση. Έτσι η κίνηση θα ελέγχεται ρητά κατά την φορά αυτού που εκκινεί την επικοινωνία (initiator) προς αυτόν που απαντά (responder). Ο χειρισμός κατά την αντίστροφη κατεύθυνση θα είναι έμμεσος λόγω του δυναμικού κανόνα που δημιουργεί το keep-state.

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

4.1 Με την εντολή "*ipfw disable one_pass*" απενεργοποιήστε τη λειτουργία one-pass, διατηρήστε όμως τον ορισμό του πίνακα NAT της ερώτησης 3.28. Μπορείτε τώρα να κάνετε ping από το PC1 στη διεπαφή του FW1 στο LAN1 ή από το SRV1 στη διεπαφή του FW1 στο WAN1;

4.2 Γίνονται δεκτά τα πακέτα από τον κανόνα ώθησης στο NAT της ερώτησης 3.13; Εάν ναι, γιατί αποτυγχάνει το ping;

4.3 Ως πρώτο βήμα πρέπει να επιτρέψετε την εντός του εταιρικού δικτύου κίνηση. Διαγράψτε τον προηγούμενο κανόνα και προσθέστε νέο με αύξοντα αριθμό 1100 που να επιτρέπει όλη την κίνηση μέσω (via) της διεπαφής του FW1 στο LAN1.

4.4 Είναι τώρα το ping από το PC1 προς οποιαδήποτε διεπαφή του FW1 επιτυχές;

4.5 Σε ποιο μηχάνημα θα συνδεθείτε εάν από το PC2 κάνετε ssh στη διεύθυνση 192.0.2.1;

4.6 Ποιοι κανόνες είναι υπεύθυνοι για ό,τι παρατηρήσατε προηγουμένως;

4.7 Για να επικοινωνούν τα μηχανήματα του LAN1 (εταιρικό δίκτυο) με το εξωτερικό δίκτυο (διαδίκτυο), πρέπει τα εξερχόμενα στο WAN1 πακέτα να υφίστανται μετάφραση από το NAT. Προς τούτο προσθέστε κανόνα στο τείχος προστασίας του FW1 με αύξοντα αριθμό 3000 ώστε

να ωθείται προς μετάφραση στον πίνακα NAT με αριθμό παρουσίας 123, η μεταδιδόμενη (xmit) κίνηση από τη διεπαφή του στο WAN1, ανεξάρτητα διεύθυνσης IP πηγής και προορισμού.

4.8 Επειδή έχει ακυρωθεί η λειτουργία one-pass, τα πακέτα που ταιριάζουν στον προηγούμενο κανόνα, θα απορριφθούν στη συνέχεια από τον τελικό κανόνα 65535 του ipfw. Προσθέστε αμέσως επόμενο κανόνα με αύξοντα αριθμό 3001 που να αποδέχεται οποιαδήποτε κίνηση μετά τη μετάφραση.

4.9 Τα πακέτα που φτάνουν σε απάντηση αυτών που εξήλθαν από το τείχος προστασίας, πρέπει και αυτά να υποστούν μετάφραση από το NAT. Προς τούτο προσθέστε κανόνα στο FW1 με αύξοντα αριθμό 2000 ώστε να ωθείται προς μετάφραση στον πίνακα NAT με αριθμό παρουσίας 123 η οποιαδήποτε εισερχόμενη κίνηση λαμβάνεται (recv) στη διεπαφή του στο WAN1, ανεξάρτητα διεύθυνσης IP πηγής και προορισμού.

4.10 Στη συνέχεια θα εγκαταστήσετε (stateful) κανόνες. Προσθέστε κανόνα με αύξοντα αριθμό 2001 που να ελέγχει εάν η κίνηση έχει γίνει αποδεκτή από δυναμικό κανόνα.

4.11 Ποιο μηχάνημα απαντά εάν κάνετε ping από το PC1 στη διεύθυνση 192.0.2.1;

4.12 Ποιο μηχάνημα απαντά εάν κάνετε ping από το SRV1 στη διεύθυνση 192.0.2.1;

4.13 Σε ποιο μηχάνημα συνδέεστε εάν κάνετε ssh από το PC1 στη διεύθυνση 192.0.2.1;

4.14 Σε ποιο μηχάνημα συνδέεστε εάν κάνετε ssh από το SRV1 στη διεύθυνση 192.0.2.1;

4.15 Σε ποιο μηχάνημα συνδέεστε εάν κάνετε ftp από το SRV1 στη διεύθυνση 192.0.2.1;

4.16 Μπορείτε να κάνετε ping από το PC1 στο SRV1;

4.17 Μπορείτε να συνδεθείτε με ssh από το PC1 στο SRV1;

4.18 Μπορείτε από το PC1 να συνδεθείτε με ftp ως χρήστης lab στο SRV1, να δείτε τα περιεχόμενα κάποιου φακέλου και να κατεβάσετε ένα αρχείο;

4.19 Οι προηγούμενοι κανόνες ώθησης στο NAT επιτυγχάνουν τη μετάφραση διευθύνσεων αλλά επιτρέπουν οποιαδήποτε κίνηση ανεξάρτητα από το κατά πόσον αυτή είναι επιθυμητή. Προσθέστε στο τείχος προστασίας FW1 κανόνα με αύξοντα αριθμό 2999 που να απαγορεύει οποιαδήποτε κίνηση μέσω (via) της διεπαφής του στο WAN1, ανεξάρτητα διεύθυνσης IP πηγής και προορισμού.

4.20 Ποια από τα ping, ssh ftp των προηγούμενων ερωτήσεων επιτυγχάνουν;

4.21 Προσθέστε (stateful) κανόνα στο τείχος προστασίας του FW1 με αύξοντα αριθμό 2500 ώστε η μεταδιδόμενη (xmit) από τη διεπαφή του στο WAN1 κίνηση ICMP, ανεξάρτητα διεύθυνσης IP πηγής και προορισμού, να στέλνεται (skipto) στη μετάφραση NAT του κανόνα 3000.

4.22 Μπορείτε να κάνετε ping από το PC1 στο SRV1;

4.23 Προσθέστε (stateful) κανόνα στο τείχος προστασίας του FW1 με αύξοντα αριθμό 2600 ώστε η εξερχόμενη μέσω (out via) της διεπαφής του στο WAN1 κίνηση tcp για σύνδεση με προορισμό τη θύρα 22, ανεξάρτητα διεύθυνσης IP πηγής και προορισμού, να στέλνεται στη μετάφραση NAT του κανόνα 3000.

4.24 Μπορείτε να συνδεθείτε με ssh από το PC1 στο SRV1;

4.25 Τα εισερχόμενα από το WAN1 πακέτα στο FW1, εάν πρόκειται να γίνουν δεκτά, όσο και εάν φαίνεται λάθος, θα πρέπει να στέλνονται στον κανόνα 3000. Η μετάφραση όμως δεν θα εφαρμοσθεί στα εισερχόμενα, αλλά στα πακέτα που θα παραχθούν ως απάντηση σε αυτά. Προσθέστε (stateful) κανόνα στο τείχος προστασίας του FW1 με αύξοντα αριθμό 2100 ώστε η εισερχόμενη μέσω (in via) της διεπαφής του στο WAN1 κίνηση ICMP, ανεξάρτητα διεύθυνσης IP πηγής και προορισμού, να στέλνεται (skipto) στη μετάφραση NAT του κανόνα 3000.

4.26 Ποιο μηχάνημα απαντά εάν κάνετε ping από το SRV1 στη διεύθυνση 192.0.2.1;

4.27 Προσθέστε (stateful) κανόνα στο τείχος προστασίας του FW1 με αύξοντα αριθμό 2200 ώστε η λαμβανόμενη (recv) στη διεπαφή του στο WAN1 κίνηση tcp για σύνδεση με προορισμό τη θύρα 22, ανεξάρτητα διεύθυνσης IP πηγής και προορισμού, να στέλνεται (skipto) στη μετάφραση NAT του κανόνα 3000.

4.28 Σε ποιο μηχάνημα συνδέεστε εάν από το SRV1 κάνετε ssh ως χρήστης lab στη διεύθυνση 192.0.2.1;

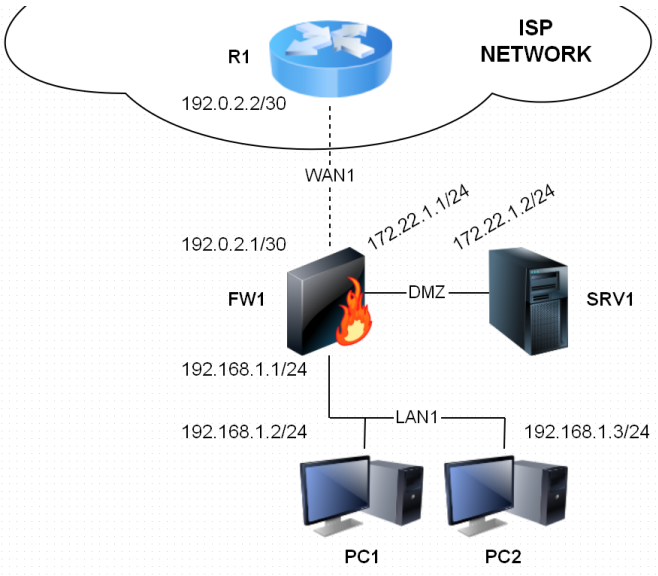
4.29 Επιτυγχάνει τώρα το ftp από το SRV1 στη διεύθυνση 192.0.2.1;

4.30 Ποιους δύο νέους κανόνες πρέπει να προσθέσετε ώστε να λειτουργεί το προηγούμενο ftp σε active mode;

Άσκηση 5: Τείχος προστασίας με γραφικό περιβάλλον διαχείρισης

Κατασκευάστε στο VirtualBox το δίκτυο του επόμενου σχήματος. Μπορείτε να χρησιμοποιήσετε τα εικονικά μηχανήματα από τις προηγούμενες ασκήσεις, εκτός από το FW1 που θα το αντικαταστήσετε με το m0n0wall από το αρχείο firewall.ova, φάκελος VMs, δικτυακός δίσκος Y των μηχανημάτων του PC Lab ή θα κατεβάσετε με ανώνυμο ftp από το ftp://edu-dy.cn.ntua.gr/ επιλέγοντας δυαδικό (bin) τρόπο μεταφοράς. Ορίσετε τα τοπικά δίκτυα στο FW1 και SRV1 από το VirtualBox όπως στο σχήμα. Μην απενεργοποιήσετε τη δεύτερη διεπαφή του R1, θα τη χρησιμοποιήσετε στην άσκηση 7.

Στο firewall.ova έχουν ορισθεί 4 κάρτες δικτύου. Η 1η , 2η και 4η είναι για τα LAN, WAN και DMZ, αντίστοιχα. Η 3η κάρτα δικτύου είναι ρυθμισμένη σε δικτύωση host-only. Μέσω αυτής μπορείτε να αποκτήσετε πρόσβαση στο γραφικό περιβάλλον του τείχους προστασίας με όνομα χρήστη "admin" και συνθηματικό "ntua", ακολουθώντας τον παρακάτω σύνδεσμο http://192.168.56.2[2]. 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.



[2] Η διεπαφή Host only του φιλοξενούντος μηχανήματος πρέπει να βρίσκεται στο υποδίκτυο 192.168.56.0/24.

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.

5.1 Ποια είναι η διεύθυνση που έχει ρυθμιστεί στη διεπαφή του FW1 στο LAN1;
5.2 Ποια είναι η διεύθυνση που έχει ρυθμιστεί στη διεπαφή του FW1 στο WAN1;
5.3 Ποιο είναι το ποσοστό της ελεύθερης μνήμης που βλέπετε στο FW1;
5.4 Πόσες διεπαφές δικτύου βλέπετε συνολικά στο FW1; Επιβεβαιώστε ότι στο VirtualBox οι κάρτες δικτύου έχουν το σωστό τρόπο δικτύωσης και βρίσκονται στα σωστά υποδίκτυα. Εάν όχι διορθώστε.
5.5 Ποια είναι η διεύθυνση που έχει ρυθμιστεί στη διεπαφή DMZ του FW1;
5.6 Ποιο είναι το όνομα (hostname) του FW1;
5.7 Αλλάξτε το hostname του FW1 σε "fw1". *[Υποδ. Η ενεργοποίηση των αλλαγών γίνεται όταν αποθηκεύετε.]*
5.8 Στο μενού *Firewall → Rules* του FW1 υπάρχουν κανόνες για το WAN;
5.9 Ορίστε τη σωστή διεύθυνση και προεπιλεγμένη πύλη του FW1 στο WAN1 και επιλέξτε το "Block private networks".
5.10 Στο μενού *Firewall → Rules* του FW1 υπάρχουν τώρα κανόνες για το WAN;
5.11 Βλέπετε να είναι ενεργοποιημένη κάποια υπηρεσία από αυτές των κατηγοριών "Services" και "VPN";
5.12 Ενεργοποιήστε την υπηρεσία DNS forwarder χωρίς κάποια άλλη ρύθμιση (είναι προαπαιτούμενο για το παρακάτω).
5.13 Ενεργοποιήστε την υπηρεσία DHCP server στο LAN1 ορίζοντας ως περιοχή διευθύνσεων την 192.168.1.2 έως 192.168.1.3.
5.14 Στο PC1 ξεκινήστε τον πελάτη DHCP. Ποια είναι η διεύθυνση IP, η προεπιλεγμένη πύλη και η διεύθυνση εξυπηρετητή DNS που αποδόθηκε;
5.15 Γιατί χρειάστηκε η ενεργοποίηση της υπηρεσίας DNS forwarder; *[Υποδ. Δείτε σημείωση στη σελίδα ενεργοποίησής του.]*
5.16 Σε πιο μέρος του μενού *Diagnostics* μπορείτε να δείτε ότι έχει αποδοθεί η συγκεκριμένη διεύθυνση στο PC1;
5.17 Πόσες εγγραφές ARP βλέπετε στο μενού *Diagnostics → ARP Table*;
5.18 Μπορείτε από το PC1 να κάνετε ping τη διεπαφή του FW1 στο LAN1;
5.19 Στο μενού *Diagnostics → Logs* καρτέλα *Firewall* τι βλέπετε; Καθαρίστε το αρχείο καταγραφών.
5.20 Πόσα firewall states βλέπετε από το αντίστοιχο μενού στο *Diagnostics*;
5.21 Πόσους κανόνες για το LAN βλέπετε από το μενού *Firewall → Rules*;
5.22 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.]*
5.23 Μπορείτε τώρα από το PC1 να κάνετε ping τις διεπαφές του FW1 στα LAN1, WAN1, DMZ;
5.24 Από τον R1 μπορείτε να κάνετε ping τη διεπαφή του FW1 στο WAN1;
5.25 Εμφανίστε τον πίνακα ARP στον R1. Βλέπετε κάποια εγγραφή για τη διεύθυνση MAC της διεπαφής του FW1 στο WAN1;
5.26 Προσθέστε στο FW1 κανόνα ώστε να επιτρέψετε όλη την εισερχόμενη ICMP κίνηση με προορισμό την "WAN Address".

5.27 Μπορείτε τώρα από τον R1 να κάνετε ping τη διεπαφή του FW1 στο WAN1;
5.28 Μπορείτε από τον R1 να κάνετε ping το PC1; Γιατί;
5.29 Μπορείτε από το PC1 να κάνετε ping τον R1; Τι συμπεραίνετε όσον αφορά τη λειτουργία NAT;
5.30 Εάν δεν το έχετε ήδη κάνει, τοποθετήστε το SRV1 στο DMZ και ορίστε τη διεύθυνση IPv4 όπως στο σχήμα. Μπορείτε από το PC1 να κάνετε ping τον SRV1; Γιατί;
5.31 Ορίστε τη σωστή προεπιλεγμένη πύλη στον SRV1.
5.32 Μπορείτε τώρα από το PC1 να κάνετε ping τον SRV1;
5.33 Μπορείτε από τον SRV1 να κάνετε ping τη διεπαφή του FW1 στο DMZ; Γιατί;
5.34 Μπορείτε από τον SRV1 να κάνετε ping το PC1 ή το R1; Γιατί;
5.35 Προσθέστε στο FW1 κανόνα ώστε να επιτρέψετε εξερχόμενη κίνηση από το DMZ προς οποιονδήποτε προορισμό πλην του LAN1.
5.36 Μπορείτε τώρα από τον SRV1 να κάνετε ping τη διεπαφή του FW1 στο DMZ;
5.37 Μπορείτε τώρα από τον SRV1 να κάνετε ping τη διεπαφή του FW1 στο WAN1;
5.38 Μπορείτε από τον R1 να κάνετε ping τον SRV1; Γιατί;
5.39 Μπορείτε από τον SRV1 να κάνετε ping τον R1; Αιτιολογήστε.
5.40 Στο PC2 ξεκινήστε τον πελάτη DHCP. Ποια είναι η διεύθυνση IP, η προεπιλεγμένη πύλη και η διεύθυνση εξυπηρετητή DNS που αποδόθηκε;
5.41 Προσθέστε στο FW1 κανόνα “Block”, ώστε να απαγορεύσετε στο LAN1 όλη την κίνηση από το PC2 προς το SRV1.
5.42 Πρέπει ο κανόνας να τοποθετηθεί πριν ή μετά από αυτόν που υπάρχει; Γιατί;
5.43 Μπορείτε από το PC2 να κάνετε ping τον SRV1;
5.44 Μπορείτε από το PC2 να κάνετε ping τη διεπαφή του FW1 στο DMZ; Γιατί;

Άσκηση 6: Τείχος προστασίας και προχωρημένο NAT

Θα χρησιμοποιήσετε το δίκτυο της προηγούμενης άσκησης προκειμένου να εμβαθύνετε στη χρήση του inbound και outbound NAT σε ένα firewall. Στην άσκηση αυτή υποτίθεται ότι ο πάροχος ISP σάς έχει εκχωρήσει το υποδίκτυο 203.0.118.0/24. Θέλετε ο εξυπηρετητής SRV1 να είναι προσβάσιμος από το δημόσιο δίκτυο και τα PC1 και PC2 να εμφανίζονται στο διαδίκτυο με συγκεκριμένες δημόσιες διευθύνσεις IP από αυτές που σας εκχωρήθηκαν.

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.

6.1 Προσθέστε στον R1 στατική εγγραφή για το 203.0.118.0/24 προς το FW1 ώστε η κίνηση προς το υποδίκτυό σας να διέρχεται μέσω του τείχους προστασίας.
6.2 Στο μενού *Firewall → NAT* του FW1 σελίδα Outbound ενεργοποιήστε το “advanced outbound NAT”. Με αυτό τον τρόπο απενεργοποιείτε (δείτε και σχετική σημείωση) την αυτόματη δημιουργία κανόνων για απερχόμενη κίνηση (outbound NAT).
6.3 Προσθέστε αντιστοίχιση outbound NAT ώστε το PC1 να εμφανίζεται στον έξω κόσμο με τη διεύθυνση 203.0.118.14 και ενεργοποιήστε την. *[Υποδ. Χρησιμοποιήστε /32 μάσκα.]*
6.4 Προσθέστε αντιστοίχιση outbound NAT ώστε το PC2 να εμφανίζεται στον έξω κόσμο με τη διεύθυνση 203.0.118.15 και ενεργοποιήστε την.
6.5 Ξεκινήστε καταγραφή πακέτων με το tcpdump στη διεπαφή του R1 και αφήστε τη να τρέχει.
6.6 Μπορείτε να κάνετε ping από τα PC1, PC2 στον R1; Αν ναι, με ποια διεύθυνση IP φτάνουν τα πακέτα από τα PC1, PC2;

6.7 Από νέο παράθυρο εντολών στον R1 κάντε ping στο PC1 χρησιμοποιώντας τη διεύθυνση 203.0.118.14; Για ποιο λόγο αποτυγχάνει;

6.8 Από το μενού *Firewall → NAT* του FW1 σελίδα "Server NAT" προσθέστε αντιστοίχιση για την IP διεύθυνση 203.0.118.18 και ενεργοποιήστε την.

6.9 Από το μενού *Firewall → NAT* του FW1 σελίδα "Inbound" προσθέστε αντιστοίχιση ορίζοντας ως εξωτερική διεύθυνση IP τη 203.0.118.18, ως NAT IP τη διεύθυνση του SRV1, ως πρωτόκολλο το TCP, ως εξωτερική θύρα την SSH ή τον αριθμό 22 και ως τοπική θύρα την ίδια με την εξωτερική. Αφού επιλέξετε το "Auto-add a firewall rule to permit traffic through this NAT rule", ενεργοποιήστε την.

6.10 Ποιος κανόνας τοποθετείται αυτόματα στο Firewall για τη διεπαφή WAN και γιατί;

6.11 Μπορείτε από τον R1 να συνδεθείτε με ssh στο 203.0.118.18; Σε ποιο σύστημα συνδέεστε; *[Υποδ. Εάν εμφανισθεί μήνυμα λάθους σχετικό με το κλειδί κρυπτογράφησης, διαγράψτε το υπάρχον στο αρχείο /root/.ssh/know_hosts]*

6.12 Μπορείτε από τον R1 να κάνετε ping το 203.0.118.18; Ποιος είναι ο λόγος της αποτυχίας;

6.13 Μπορείτε να συνδεθείτε με ssh από το PC2 στο SRV1 χρησιμοποιώντας τη διεύθυνση 203.0.118.118; Εάν ναι, ποια διαδρομή ακολουθούν τα πακέτα IP από το PC2 προς το SRV1 και αντιστρόφως; Πώς το επιβεβαιώνετε;

6.14 Καταργήστε την outbound NAT αντιστοίχιση για το PC1. Μπορείτε να κάνετε ping στον R1 από το PC1; Γιατί; *[Υποδ. Συμβουλευθείτε καταγραφή.]*

6.15 Καταργήστε το advanced outbound NAT. Είναι το ping προς τον R1 επιτυχές;

6.16 Εξακολουθείτε να μπορείτε να συνδέεστε από τον R1 στο SRV1 χρησιμοποιώντας τη διεύθυνση 203.0.118.18; Ισχύει το ίδιο για τα PC1, PC2;

6.17 Ξεκινήστε μια καταγραφή πακέτων στο SRV1 και άλλη στο R1 εμφανίζοντας επικεφαλίδες Ethernet. Επιχειρήστε πάλι να συνδεθείτε με SSH από το PC2 στο SRV1. Εξηγήστε γιατί αποτυγχάνει η σύνδεση tcp.

6.18 Για τη συμπεριφορά που παρατηρήσατε προηγουμένως είναι υπεύθυνος ο κανόνας Block που θέσατε στην ερώτηση 5.41 ή ο κανόνας για το DMZ στην ερώτηση 5.35; Εάν όχι, ποιος είναι ο λόγος; *[Υποδ. Δείτε και σημείωση στην καρτέλα για Inbound.]*

Άσκηση 7: IPSec site-to-site VPN

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.

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.

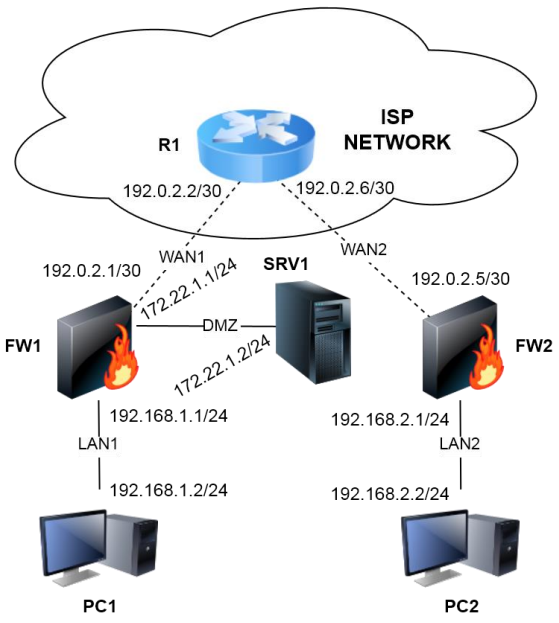
Οι δύο υπηρεσίες είναι διαφορετικές, αλλά το IPsec τις παρέχει ενοποιημένα. Η πιστοποίηση αυθεντικότητας επιτυγχάνεται με την προσθήκη της επικεφαλίδας Authentication Header (AH) που

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 επικοινωνίας 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.

Στη συνέχεια θα δείτε πώς μπορείτε να φτιάξετε ένα εκτεταμένο VPN με τη βοήθεια του m0n0wall. Κατασκευάστε στο VirtualBox το δίκτυο του σχήματος. Θα χρησιμοποιήσετε τα μηχανήματα από την προηγούμενη άσκηση και θα προσθέσετε ένα νέο firewall FW2 σύμφωνα με τις οδηγίες που ακολουθούν. Θυμηθείτε να αλλάξετε από το VirtualBox τα τοπικά δίκτυα για τα R1, PC2 και FW2.



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.

7.1 Αποσυνδέστε από το Virtualbox το καλώδιο της κάρτας δικτύου #3 του FW1.
7.2 Συνδεθείτε από τον φυλλομετρητή στο FW2 και αλλάξτε τη διεύθυνση IP στη διεπαφή MNG από 192.168.56.2 σε 192.168.56.3.
7.3 Ξανασυνδέστε από το Virtualbox το καλώδιο της κάρτας δικτύου #3 του FW1.
7.4 Μπορείτε να συνδεθείτε ταυτόχρονα από τον φυλλομετρητή του φιλοξενούντος μηχανήματος στα δύο τείχη προστασίας;
7.5 Αλλάξτε το hostname του FW2 σε “fw2”.
7.6 Ορίστε τη σωστή διεύθυνση και προεπιλεγμένη πύλη του FW2 στο WAN2, επιλέγοντας το “Block private networks”.
7.7 Ορίστε τη σωστή διεύθυνση του FW2 στο LAN2.
7.8 Επανεκκινήστε το FW2.
7.9 Προσθέστε στο FW2 κανόνα ώστε να επιτρέψετε <u>όλη</u> την κίνηση από το LAN2.
7.10 Προσθέστε στο FW2 κανόνα ώστε να επιτρέψετε όλη την εισερχόμενη ICMP κίνηση με προορισμό την “WAN Address”.
7.11 Εάν δεν το έχετε ήδη κάνει, μετακινήστε το PC2 στο LAN2. Ορίστε τη σωστή διεύθυνση και προεπιλεγμένη πύλη στο PC2.
7.12 Μπορείτε από το PC1 να κάνετε ping τη διεπαφή του FW2 στο WAN2;
7.13 Μπορείτε από το PC2 να κάνετε ping τη διεπαφή του FW1 στον WAN1;
7.14 Μπορείτε από το PC1 να κάνετε ping το PC2 ή το αντίστροφο. Τεκμηριώστε την απάντησή σας.
7.15 Στο μενού VPN του FW1 ενεργοποιήστε το IPSec. Μετά δημιουργήστε ένα IPSec tunnel ορίζοντας τα ακόλουθα: ως Local Subnet το τοπικό LAN, ως Remote Subnet τη διεύθυνση του LAN2, ως Remote Gateway τη διεύθυνση του FW2 στο WAN2, ως Pre-Shared Key κάποια λέξη (π.χ. το όνομά σας) και ενεργοποιήστε το.
7.16 Ποιο κανόνα βλέπετε στο *FW1 → Firewall → Rules → IPsec VPN*;
7.17 Στο *FW1 → Diagnostics → IPSec → Security Association Database (SAD)* βλέπετε να έχουν ορισθεί σχέσεις μεταξύ των δύο υποδικτύων;
7.18 Στο *FW1 → Diagnostics → IPSec → Security Policy Database (SPD)* βλέπετε να έχουν ορισθεί πολιτικές προώθησης κίνησης μεταξύ των δύο υποδικτύων;
7.19 Στο μενού VPN του FW2 ενεργοποιήστε το IPSec. Μετά δημιουργήστε ένα IPSec tunnel ορίζοντας τα ακόλουθα: ως Local Subnet το τοπικό LAN, ως Remote Subnet τη διεύθυνση του LAN1, ως Remote Gateway τη διεύθυνση IP του FW1 στο WAN1, ως Pre-Shared Key τη λέξη που δηλώσατε προηγουμένως στην ερώτηση 7.15 και ενεργοποιήστε το.
7.20 Στο *FW2 → Diagnostics → IPSec → Security Association Database (SAD)* βλέπετε να έχουν ορισθεί σχέσεις μεταξύ των δύο υποδικτύων;
7.21 Στο *FW2 → Diagnostics → IPSec → Security Policy Database (SPD)* βλέπετε να έχουν ορισθεί πολιτικές προώθησης κίνησης μεταξύ των δύο υποδικτύων;
7.22 Μπορείτε από το PC1 να κάνετε ping το PC2;
7.23 Μπορείτε από το PC2 να κάνετε ping το PC1;
7.24 Άλλαξε κάτι στο *FW1 → Diagnostics → IPSec → SAD*;
7.25 Άλλαξε κάτι στο *FW2 → Diagnostics → IPSec → SAD*;

7.26 Ξεκινήστε μια καταγραφή στον R1 στο WAN1 εμφανίζοντας λεπτομέρειες και το περιεχόμενο των πακέτων και αφήστε την να τρέχει.
7.27 Παρατηρείτε πακέτα ICMP όταν κάνετε ping από ένα PC στο άλλο;
7.28 Τι είδους πακέτα εμφανίζονται, ποια είναι η πηγή και ποιος ο προορισμός τους;
7.29 Υπάρχει κάπου η πληροφορία για τις διευθύνσεις IP των PC1, PC2;
7.30 Μπορείτε από το PC2 να συνδεθείτε με SSH στο SRV1 στη διεύθυνση 203.0.118.18; Εάν ναι, τι άλλαξε σε σχέση με την προηγούμενη άσκηση;
7.31 Τι είδους πακέτα παρατηρείτε στην καταγραφή, ποιες είναι οι διευθύνσεις IP και θύρες πηγής και προορισμού τους;
7.32 Είναι κρυπτογραφημένα; Με το IPsec;