ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Μελέτη Προσομοιωτών Δικτύου και Υλοποίηση Περιβάλλοντος για την Αποφυγή Δικτυακών Επιθέσεων

Διονύσιος Αποστολόπουλος

Επιβλέπων Καθηγητής:

Χρήστος Ξενάκης, Καθηγητής

ΠΕΙΡΑΙΑΣ

ΦΕΒΡΟΥΑΡΙΟΣ 2023

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Μελέτη Προσομοιωτών Δικτύου και Υλοποίηση Περιβάλλοντος για την Αποφυγή Δικτυακών Επιθέσεων

Διονύσιος Αποστολόπουλος

Α.Μ.: MTE2001

ΠΕΡΙΛΗΨΗ

Η παρούσα διπλωματική εργασία εντάσσεται στο ερευνητικό πεδίο της Ασφάλειας Δικτύων και πιο συγκεκριμένα στη χρήση Προσομοιωτή Δικτύου για την υλοποίηση περιβάλλοντος με σκοπό την διαχείριση της δικτυακής κίνησης, την προφύλαξη της υποδομής καθώς και την αποτροπή δικτυακών επιθέσεων. Η ασφάλεια των δικτύων ηλεκτρονικών υπολογιστών αποτελεί κρίσιμο ζήτημα στη σημερινή κοινωνία. Οι προσομοιωτές δικτύων αποτελούν ένα πολύτιμο εργαλείο για τη δοκιμή μέτρων ασφαλείας δικτύων χωρίς να διακινδυνεύεται η πρόκληση ζημιών σε πραγματικά δίκτυα. Η παρούσα εργασία ξεκινά στο πρώτο μέρος με τη βιβλιογραφική μελέτη της ασφάλειας δικτύων, την χρησιμότητα της καθώς και το πεδίο εφαρμογής της. Εν συνεχεία, αναλύεται εκτενώς η λειτουργία και η χρησιμότητα των προσομοιωτών δικτύου καθώς και οι διαφορές τους από τους εξομοιωτές. Τέλος, παρουσιάζονται διάφοροι τύποι προσομοιωτών δικτύου που είναι διαθέσιμοι για ερευνητικούς σκοπούς με στόχο την έρευνα διαφόρων υλοποιήσεων ασφαλείας. Στο δεύτερο μέρος μελετώνται εκτενώς διάφορα σενάρια σχετικά με την ασφάλεια των σύγχρονων υπολογιστικών δικτύων όπως εναλλακτικοί τρόποι διασύνδεσης και προστασίας δικτύων, όπως επίσης και λύσεις ασφαλείας. Τέλος, πραγματοποιείται και παρουσιάζεται αναλυτικά η υλοποίησή των σεναρίων αυτών με τη χρήση του προσομοιωτή Cisco Packet Tracer, ενός προσομοιωτή ελεύθερου στην αγορά για μηχανικούς και ερευνητές.

ΘΕΜΑΤΙΚΗ ΠΕΡΙΟΧΗ: Ασφάλεια Δικτύων

ΛΕΞΕΙΣ ΚΛΕΙΔΙΑ: ασφάλεια δικτύου, προσομοιωτής δικτύου, IPsec, zone-based πολιτικές, λίστες ελέγχου πρόσβασης, συστήματα αποτροπής διείσδυσης

ABSTRACT

This thesis is part of the research field of Network Security and more specifically the use of a Network Simulator for the implementation of an environment for the management of network traffic, the protection of the infrastructure and the prevention of network attacks. The security of computer networks is a critical issue in today's society. Network simulators are a valuable tool for testing network security measures without risking damage to real networks. This paper starts in the first part with a literature study of network security, its usefulness and its scope. Subsequently, the function and utility of network simulators and their differences from simulators are extensively discussed. Finally, various types of network simulators available for research purposes are presented with the aim of investigating various security implementations. In the second part, various scenarios related to the security of modern computer networks such as alternative ways of interconnecting and protecting networks as well as security solutions are extensively studied. Finally, the implementation of these scenarios is carried out and presented in detail using the Cisco Packet Tracer simulator, a simulator free on the market for engineers and researchers.

SUBJECT AREA: Network Security

KEYWORDS: network security, network simulator, IPsec, zone-based policy firewall, access-control-list, intrusion prevention systems.

…αφιερωμένη σε όλους τους φίλους μου,

που είναι πάντα δίπλα μου και με στηρίζουν σε κάθε μου βήμα..

ΕΥΧΑΡΙΣΤΙΕΣ

Για την εκπόνηση της παρούσας διπλωματικής εργασίας, θα ήθελα να ευχαριστήσω τον επιβλέποντα Καθηγητή μου, κύριο Χρήστο Ξενάκη που μου έδωσε την δυνατότητα να πραγματοποιήσω την εργασία αυτή, για το χρόνο που αφιέρωσε, την πολύτιμη συμβολή του καθώς και για την κάθε εποικοδομητική συζήτηση που είχαμε.

ΠΕΡΙΕΧΟΜΕΝΑ

ΚΑΤΑΛΟΓΟΣ ΣΧΗΜΑΤΩΝ

ΚΑΤΑΛΟΓΟΣ ΕΙΚΟΝΩΝ

ΑΚΡΩΝΥΜΙΑ

IoT	Internet of Things
DoS	Denial of Service
DDoS	Distributed Denial of Service
NGFW	Next Generation Firewall
IAM	Identity Access Management
VPN	Virtual Private Network
MFA	Multi Factor Authentication
ZTN	Zero Trust Network
ZTNA	Zero Trust Network Access
DLP	Data Loss Prevention
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
PII	Personal Identifying Information
SDN	Software Defined Network
SD-WAN	Software Defined - Wide Area Network
FWaaS	Firewall as a Service
MitM	Man in the Middle
CPT	Cisco Packet Tracer
UI	User Interface
CLI	Command Line Interface
GUI	Graphical User Interface
VM	Virtual Machine
LAN	Local Area Network
P2P	Peer to Peer
IP	Internet Protocol
IPsec	Internet Protocol Security
TLS	Transport Layer Security

TCP	Transmission Control Protocol
UDP	User Datagram Protocol
NAT	Network Address Translation
CBAC	Context-Based Access Control
ACL	Access Control List
DMZ	Demilitarized Zone
ISP	Internet Service Provider

1 Εισαγωγή

Στον σημερινή εποχή, η οποία θα μπορούσε να χαρακτηριστεί και ως «η εποχή του διασυνδεδεμένου κόσμου», η ασφάλεια του δικτύου αποτελεί βασική πτυχή των λειτουργιών κάθε οργανισμού, καθώς διαδραματίζει κρίσιμο ρόλο λόγω της ευρείας χρήσης των δικτύων υπολογιστών για επικοινωνία και ανταλλαγή δεδομένων. Στον σημερινό κόσμο, οι άνθρωποι και οι οργανισμοί βασίζονται σε μεγάλο βαθμό στα δίκτυα για τη διεξαγωγή των καθημερινών τους δραστηριοτήτων. Η ραγδαία άνοδος του IoT (Internet of Things) έχει επεκτείνει περαιτέρω τη χρήση των δικτύων, συνδέοντας έναν αυξανόμενο αριθμό συσκευών στο διαδίκτυο. Ωστόσο, με την αυξημένη εξάρτηση από τα δίκτυα αυξάνεται και ο κίνδυνος απειλών ασφαλείας, όπως κυβερνοεπιθέσεις, παραβιάσεις δεδομένων και μη εξουσιοδοτημένη πρόσβαση.

Ο ρόλος της ασφάλειας δικτύων είναι η προστασία των δικτύων υπολογιστών από αυτές τις απειλές με την εφαρμογή διαφόρων μέτρων ασφαλείας. Η ασφάλεια δικτύου περιλαμβάνει τη χρήση τεχνολογιών υλικού και λογισμικού, καθώς και πολιτικών και διαδικασιών, για την ασφάλεια της υποδομής, των δεδομένων και των σημείων πρόσβασης ενός δικτύου. Στόχος της ασφάλειας δικτύου είναι η αποτροπή μη εξουσιοδοτημένης πρόσβασης, η προστασία ευαίσθητων πληροφοριών και η διασφάλιση της διαθεσιμότητας και της αξιοπιστίας του δικτύου.

Ένα από τα κρίσιμα στοιχεία της ασφάλειας δικτύου είναι η χρήση προσομοιωτών δικτύου. Οι προσομοιωτές δικτύων είναι εφαρμογές λογισμικού που προσομοιώνουν δίκτυα υπολογιστών, επιτρέποντας στους διαχειριστές δικτύων και στους ειδικούς ασφαλείας να δοκιμάζουν την αποτελεσματικότητα των μέτρων ασφαλείας τους σε ένα ελεγχόμενο περιβάλλον. Αυτοί οι προσομοιωτές είναι ζωτικής σημασίας για να διασφαλιστεί ότι ένα δίκτυο είναι ασφαλές και μπορεί να αντέξει διαφορετικούς τύπους απειλών ασφαλείας.

Οι προσομοιωτές δικτύων επιτρέπουν σε ερευνητές, μηχανικούς και επαγγελματίες της ασφαλείας να προσομοιώνουν διάφορους τύπους επιθέσεων, όπως οι επιθέσεις κατανεμημένης άρνησης παροχής υπηρεσιών (Distributed Denial of Service - DDoS), για να αξιολογούν την ανθεκτικότητα του δικτύου. Μπορούν επίσης να χρησιμοποιηθούν για τη δοκιμή της αποτελεσματικότητας των τειχών προστασίας, των συστημάτων ανίχνευσης εισβολών και άλλων μέτρων ασφαλείας. Με την προσομοίωση διαφορετικών σεναρίων επίθεσης, οι ειδικοί ασφαλείας μπορούν να εντοπίσουν τα τρωτά σημεία του δικτύου και να αναπτύξουν στρατηγικές για τον μετριασμό των κινδύνων. Χρησιμοποιούνται επίσης για τη δοκιμή των διαμορφώσεων του δικτύου πριν από την υλοποίηση. Επιτρέπουν στους διαχειριστές δικτύου να προσομοιώνουν διαφορετικές τοπολογίες δικτύου και να δοκιμάζουν τον αντίκτυπο των αλλαγών στο δίκτυο. Η διαδικασία αυτή βοηθά στον εντοπισμό πιθανών προβλημάτων πριν από την υλοποίηση και μειώνει τον κίνδυνο διακοπής λειτουργίας λόγω λανθασμένων ρυθμίσεων ή άλλων σφαλμάτων.

Επιπλέον, οι προσομοιωτές δικτύου αποτελούν εξαιρετικό εργαλείο για σκοπούς κατάρτισης και εκπαίδευσης. Επιτρέπουν στους επαγγελματίες της ασφάλειας δικτύου να αποκτήσουν πρακτική εμπειρία με διάφορες έννοιες και τεχνολογίες ασφάλειας δικτύου. Επιπρόσθετα, δίνουν τη δυνατότητα στους ειδικούς ασφαλείας να προσομοιώνουν διαφορετικούς τύπους σεναρίων, τα οποία μπορούν να χρησιμοποιηθούν για την εκπαίδευση του προσωπικού στον αποτελεσματικό χειρισμό περιστατικών ασφαλείας.

Η παρούσα Διπλωματική εργασία εντάσσεται στο ερευνητικό πεδίο της ασφάλειας δικτύων και πιο συγκεκριμένα μελετάει την χρήση των προσομοιωτών δικτύου. Στόχος είναι η δημιουργία περιβάλλοντος όπου θα δίνεται η δυνατότητα να ελεγχθεί η κίνηση, εισερχόμενη και εξερχόμενη, και να διαφυλαχθεί η ακεραιότητα των περιουσιακών στοιχείων της υποδομής, όπως και η ακεραιότητα των πληροφοριών. Στην παρούσα μελέτη αρχικά

παρουσιάζεται εκτενώς το πεδίο της ασφάλειας δικτύων και των εφαρμογών της και εν συνεχεία αναλύεται η χρήση των προσομοιωτών ασφαλείας καθώς και το ρόλο που διαδραματίζουν στην επίτευξη των στόχων της. Γίνεται επίσης μελέτη και αναφορά σε διάφορους προσομοιωτές δικτύου που είναι διαθέσιμοι στο διαδίκτυο και είναι ελεύθερα και χωρίς κόστος προσβάσιμοι στον ερευνητικό κόσμο καθώς και στους επαγγελματίες στο χώρο της ασφάλειας. Από τους διαθέσιμους προσομοιωτές, αφού επιλεχθεί ο προσομοιωτής Cisco Packet Tracer, αναπτύσσονται διάφορα σενάρια που βρίσκουν εφαρμογή στο χώρο της ασφάλειας, παρουσιάζεται εκτενώς το θεωρητικό τους υπόβαθρο και εν συνεχεία παρουσιάζεται και η υλοποίησή τους με τη χρήση του συγκεκριμένου προσομοιωτή.

2 Ασφάλεια Δικτύου

2.1 Εισαγωγή

Η ασφάλεια δικτύου αναφέρεται στα μέτρα που λαμβάνει κάθε επιχείρηση, οργανισμός ή οποιοδήποτε πληροφοριακό σύστημα για την ασφάλεια του δικτύου υπολογιστών και των δεδομένων του, χρησιμοποιώντας συστήματα υλικού και λογισμικού. Αυτό αποσκοπεί στην εξασφάλιση της εμπιστευτικότητας και της προσβασιμότητας των δεδομένων και του δικτύου. Κάθε επιχείρηση ή οργανισμός που διαχειρίζεται μεγάλο όγκο δεδομένων, έχει ένα βαθμό λύσεων έναντι πολλών απειλών στον κυβερνοχώρο [1].

Το πιο βασικό παράδειγμα ασφάλειας δικτύου είναι η προστασία με κωδικό πρόσβασης που επιλέγει ο ίδιος ο χρήστης του δικτύου. Τον τελευταίο καιρό, η Ασφάλεια Δικτύων έχει γίνει το κεντρικό θέμα της ασφάλειας στον κυβερνοχώρο με πολλούς οργανισμούς να προσκαλούν αιτήσεις από άτομα που έχουν δεξιότητες σε αυτόν τον τομέα. Οι λύσεις ασφάλειας δικτύου προστατεύουν διάφορα τρωτά σημεία των υπολογιστικών συστημάτων, όπως:

- Χρήστες
- Τοποθεσίες
- Δεδομένα
- Συσκευές
- Εφαρμογές

2.2 Η Σημασία της Ασφάλειας Δικτύου

Η ασφάλεια του δικτύου είναι ζωτικής σημασίας για τη διατήρηση της ακεραιότητας των δεδομένων και της ιδιωτικής ζωής του οργανισμού και των υπαλλήλων σας. Περιλαμβάνει τα πάντα, από τις πιο βασικές πρακτικές, όπως η δημιουργία ισχυρών κωδικών πρόσβασης και η πλήρης αποσύνδεση από τους υπολογιστές της κοινότητας, μέχρι τις πιο σύνθετες, υψηλού επιπέδου διαδικασίες που διατηρούν τα δίκτυα, τις συσκευές και τους χρήστες τους ασφαλείς. Όλο και περισσότερες ευαίσθητες πληροφορίες αποθηκεύονται στο διαδίκτυο και σε αυτές τις διάφορες συσκευές, και αν ένας μη εξουσιοδοτημένος χρήστης αποκτήσει πρόσβαση σε αυτά τα δεδομένα, αυτό θα μπορούσε να οδηγήσει σε καταστροφικά αποτελέσματα.

Η ασφάλεια του δικτύου είναι το κλειδί για την ασφάλεια αυτών των ευαίσθητων πληροφοριών και, καθώς όλο και περισσότερα ιδιωτικά δεδομένα αποθηκεύονται και μοιράζονται σε ευάλωτες συσκευές, συνεπώς θα αυξάνεται σε σημασία και αναγκαιότητα. Οι ειδικοί αναμένουν ότι θα υπάρχουν περισσότερα από 2.314 exabytes (ή πάνω από 2 τρισεκατομμύρια gigabytes) δεδομένων- η διαχείριση αυτού του όγκου δεδομένων είναι αρκετά δύσκολη και η προστασία τους θα είναι ένα εντελώς διαφορετικό ζήτημα [2].

Ενώ κάθε μέλος ενός οργανισμού μπορεί να κάνει βήματα για να συμβάλει στην ασφάλεια των πραγμάτων, η ασφάλεια του δικτύου έχει γίνει πιο σύνθετη τα τελευταία χρόνια. Η επαρκής προστασία των δικτύων και των συνδεδεμένων με αυτά συσκευών απαιτεί ολοκληρωμένη εκπαίδευση σε θέματα δικτύων, ενδελεχή κατανόηση του τρόπου με τον οποίο λειτουργούν στην πραγματικότητα τα δίκτυα και τις δεξιότητες για την εφαρμογή αυτών των γνώσεων στην πράξη. Είναι ζωτικής σημασίας για τα δίκτυα να είναι διεξοδικά και σωστά ρυθμισμένα, ασφαλισμένα και παρακολουθούμενα για την πλήρη διαφύλαξη της ιδιωτικής ζωής [3].

2.3 Πού Εφαρμόζεται η Ασφάλεια Δικτύων

Η βασική αρχή της ασφάλειας δικτύων είναι η προστασία των τεράστιων αποθηκευμένων δεδομένων και των δικτύων σε επίπεδα που εξασφαλίζουν την τήρηση κανόνων και κανονισμών που πρέπει να αναγνωρίζονται πριν από την εκτέλεση οποιασδήποτε δραστηριότητας στα δεδομένα [4].

Τα επίπεδα αυτά είναι τα εξής:

- Φυσικό Επίπεδο
- Τεχνικό Επίπεδο
- Διοικητικό Επίπεδο

Πιο αναλυτικά:

- Φυσική ασφάλεια δικτύου: Αυτό είναι το πιο βασικό επίπεδο που περιλαμβάνει την προστασία των δεδομένων και του δικτύου μέσω μη εξουσιοδοτημένου προσωπικού από την απόκτηση ελέγχου της εμπιστευτικότητας του δικτύου. Σε αυτά περιλαμβάνονται εξωτερικά περιφερειακά και δρομολογητές που ενδέχεται να χρησιμοποιούνται για καλωδιακές συνδέσεις. Το ίδιο μπορεί να επιτευχθεί με τη χρήση συσκευών όπως τα βιομετρικά συστήματα.
- Τεχνική ασφάλεια δικτύου: Επικεντρώνεται κυρίως στην προστασία των δεδομένων που είναι αποθηκευμένα στο δίκτυο ή των δεδομένων που εμπλέκονται σε μεταβάσεις μέσω του δικτύου. Αυτός ο τύπος εξυπηρετεί δύο σκοπούς. Ο ένας είναι η προστασία από μη εξουσιοδοτημένους χρήστες και ο άλλος είναι η προστασία από κακόβουλες δραστηριότητες.
- Διοικητική ασφάλεια δικτύου: Αυτό το επίπεδο ασφάλειας δικτύου προστατεύει τη συμπεριφορά των χρηστών, όπως τον τρόπο με τον οποίο έχει χορηγηθεί η άδεια και τον τρόπο με τον οποίο πραγματοποιείται η διαδικασία εξουσιοδότησης. Αυτό εξασφαλίζει επίσης το επίπεδο πολυπλοκότητας που μπορεί να χρειάζεται το δίκτυο για την προστασία του από όλες τις επιθέσεις. Αυτό το επίπεδο υποδεικνύει επίσης τις απαραίτητες τροποποιήσεις που πρέπει να γίνουν στην υποδομή.

2.4 Οφέλη της Ασφάλειας Δικτύου

Η ασφάλεια του δικτύου είναι ζωτικής σημασίας για την προστασία των δεδομένων και των πληροφοριών των πελατών, τη διατήρηση των κοινών δεδομένων σε ασφάλεια και τη διασφάλιση αξιόπιστης πρόσβασης και απόδοσης του δικτύου, καθώς και την προστασία από απειλές στον κυβερνοχώρο. Μια καλά σχεδιασμένη λύση ασφάλειας δικτύου μειώνει τα γενικά έξοδα και προστατεύει τους οργανισμούς από δαπανηρές απώλειες που προκύπτουν από παραβίαση δεδομένων ή άλλο περιστατικό ασφάλειας. Η διασφάλιση της νόμιμης πρόσβασης σε συστήματα, εφαρμογές και δεδομένα επιτρέπει την επιχειρηματική λειτουργία και την παροχή υπηρεσιών και προϊόντων στους πελάτες [5].

2.5 Τύποι Προστασίας της Ασφάλειας Δικτύου

Οι πιο διαδεδομένοι τύποι ασφάλειας δικτύου είναι [5]:

Firewalls: Τα τείχη προστασίας (Firewalls) ελέγχουν την εισερχόμενη και εξερχόμενη κυκλοφορία στα δίκτυα, με προκαθορισμένους κανόνες ασφαλείας. Τα τείχη προστασίας εμποδίζουν την μη φιλική κυκλοφορία και αποτελούν απαραίτητο μέρος της καθημερινής πληροφορικής. Η ασφάλεια δικτύου βασίζεται σε μεγάλο βαθμό στα Firewalls, και ιδίως στα Firewalls επόμενης γενιάς (Next Generation Firewalls), τα οποία επικεντρώνονται στον αποκλεισμό κακόβουλου λογισμικού και επιθέσεων επιπέδου εφαρμογών.

Network Segmentation: Η τμηματοποίηση δικτύου (Network Segmentation) ορίζει τα όρια μεταξύ τμημάτων δικτύου όπου τα περιουσιακά στοιχεία εντός της ομάδας έχουν κοινή λειτουργία, κίνδυνο ή ρόλο σε έναν οργανισμό. Για παράδειγμα, η περιμετρική πύλη τμηματοποιεί ένα εταιρικό δίκτυο από το Διαδίκτυο. Οι πιθανές απειλές εκτός του δικτύου αποτρέπονται, διασφαλίζοντας ότι τα ευαίσθητα δεδομένα ενός οργανισμού παραμένουν εντός. Οι οργανισμοί μπορούν να προχωρήσουν περαιτέρω, ορίζοντας πρόσθετα εσωτερικά όρια εντός του δικτύου τους, τα οποία μπορούν να παρέχουν βελτιωμένη ασφάλεια και έλεγχο πρόσβασης.

Access Control: Ο έλεγχος πρόσβασης (Access Control) ορίζει τα άτομα ή τις ομάδες και τις συσκευές που έχουν πρόσβαση σε εφαρμογές και συστήματα του δικτύου, αρνούμενοι έτσι τη μη εγκεκριμένη πρόσβαση και τις απειλές. Οι ενοποιήσεις με προϊόντα διαχείρισης ταυτότητας και πρόσβασης (Identity Access Management - IAM) μπορούν να προσδιορίσουν σε μεγάλο βαθμό τον χρήστη και οι πολιτικές ελέγχου πρόσβασης βάσει ρόλων (RBAC) διασφαλίζουν ότι το άτομο και η συσκευή έχουν εξουσιοδοτημένη πρόσβαση στο περιουσιακό στοιχείο.

Απομακρυσμένη Πρόσβαση VPN: Το (Virtual Private Network – VPN) απομακρυσμένης πρόσβασης παρέχει απομακρυσμένη και ασφαλή πρόσβαση σε ένα εταιρικό δίκτυο σε μεμονωμένους κεντρικούς υπολογιστές ή πελάτες, όπως εργαζόμενους εξ αποστάσεως και κινητούς χρήστες. Κάθε κεντρικός υπολογιστής έχει συνήθως εγκατεστημένο λογισμικό VPN ή χρησιμοποιεί έναν πράκτορα (agent) που βασίζεται στο διαδίκτυο. Το απόρρητο και η ακεραιότητα των ευαίσθητων πληροφοριών διασφαλίζεται μέσω ελέγχου ταυτότητας πολλαπλών παραγόντων MFA (Multi Factor Authentication - MFA), σάρωσης συμμόρφωσης τελικών σημείων και κρυπτογράφησης όλων των μεταδιδόμενων δεδομένων.

Zero Trust Network: Το μοντέλο Ασφάλειας Μηδενικής Εμπιστοσύνης (Zero Trust Network - ZTN) δηλώνει ότι ένας χρήστης θα πρέπει να έχει μόνο την πρόσβαση και τα δικαιώματα που απαιτούνται για την εκπλήρωση του ρόλου του. Πρόκειται για μια πολύ διαφορετική προσέγγιση από αυτή που παρέχουν οι παραδοσιακές λύσεις ασφαλείας, όπως τα VPN, οι οποίες παρέχουν στον χρήστη πλήρη πρόσβαση στο δίκτυο-στόχο. Η πρόσβαση στο δίκτυο μηδενικής εμπιστοσύνης (Zero Trust Network Access - ZTNA), γνωστή και ως λύση περιμέτρου καθορισμένης από λογισμικό (SDP), επιτρέπει την αναλυτική πρόσβαση στις εφαρμογές ενός οργανισμού από χρήστες που χρειάζονται αυτή την πρόσβαση για την εκτέλεση των καθηκόντων τους.

Email Security: Η ασφάλεια ηλεκτρονικού ταχυδρομείου (Email Security) αναφέρεται σε οποιεσδήποτε διαδικασίες, προϊόντα και υπηρεσίες που έχουν σχεδιαστεί για να

προστατεύουν τους λογαριασμούς ηλεκτρονικού ταχυδρομείου και το περιεχόμενο ηλεκτρονικού ταχυδρομείου με ασφάλεια από εξωτερικές απειλές. Οι περισσότεροι πάροχοι υπηρεσιών ηλεκτρονικού ταχυδρομείου διαθέτουν ενσωματωμένες λειτουργίες ασφαλείας ηλεκτρονικού ταχυδρομείου που έχουν σχεδιαστεί για να σας κρατούν ασφαλείς, αλλά αυτές μπορεί να μην είναι αρκετές για να εμποδίσουν τους εγκληματίες του κυβερνοχώρου να αποκτήσουν πρόσβαση στις πληροφορίες.

Data Loss Prevention (DLP): Η πρόληψη απώλειας δεδομένων (DLP) είναι μια μεθοδολογία κυβερνοασφάλειας που συνδυάζει τεχνολογία και βέλτιστες πρακτικές για την αποτροπή της έκθεσης ευαίσθητων πληροφοριών εκτός ενός οργανισμού, ιδίως ρυθμιζόμενων δεδομένων, όπως προσωπικά αναγνωρίσιμες πληροφορίες (Personal Identifying Information - PII) και δεδομένα που σχετίζονται με τη συμμόρφωση: HIPAA, SOX, PCI DSS κ.λπ.

Intrusion Prevention System (IPS): Οι τεχνολογίες IPS μπορούν να ανιχνεύσουν ή να αποτρέψουν επιθέσεις ασφάλειας δικτύου, όπως επιθέσεις ωμής βίας, επιθέσεις άρνησης παροχής υπηρεσιών (Denial of Service - DoS) και εκμεταλλεύσεις γνωστών ευπαθειών. Μια ευπάθεια είναι μια αδυναμία π.χ. σε ένα σύστημα λογισμικού και μια εκμετάλλευση είναι μια επίθεση που εκμεταλλεύεται αυτή την ευπάθεια για να αποκτήσει τον έλεγχο του εν λόγω συστήματος. Όταν ανακοινώνεται ένα exploit (πρόγραμμα εκμετάλλευσης ευπάθειας), υπάρχει συχνά ένα παράθυρο ευκαιρίας για τους επιτιθέμενους να εκμεταλλευτούν την εν λόγω ευπάθεια πριν εφαρμοστεί η επιδιόρθωση ασφαλείας. Ένα σύστημα πρόληψης εισβολών μπορεί να χρησιμοποιηθεί σε αυτές τις περιπτώσεις για τον γρήγορο αποκλεισμό αυτών των επιθέσεων.

Sandboxing: Το Sandboxing είναι μια πρακτική κυβερνοασφάλειας κατά την οποία ένα πρόγραμμα εκτελείται ή ανοίγεται σε ένα ασφαλές, απομονωμένο περιβάλλον σε ένα μηχάνημα υποδοχής που μιμείται τα λειτουργικά περιβάλλοντα του τελικού χρήστη. Το Sandboxing παρατηρεί τα αρχεία ή τον κώδικα καθώς ανοίγουν και αναζητά κακόβουλη συμπεριφορά για να αποτρέψει την είσοδο απειλών στο δίκτυο. Για παράδειγμα, το κακόβουλο λογισμικό σε αρχεία όπως PDF, Microsoft Word, Excel και PowerPoint μπορεί να ανιχνευθεί με ασφάλεια και να αποκλειστεί πριν τα αρχεία φτάσουν σε έναν ανυποψίαστο τελικό χρήστη.

Hyperscale Security: Η υπερκλίμακα (Hyperscale) είναι η ικανότητα μιας αρχιτεκτονικής να κλιμακώνεται κατάλληλα, καθώς προστίθεται αυξημένη ζήτηση στο σύστημα. Αυτή η λύση περιλαμβάνει ταχεία ανάπτυξη και κλιμάκωση προς τα πάνω ή προς τα κάτω για να ανταποκρίνεται στις αλλαγές των απαιτήσεων ασφάλειας δικτύου. Με τη στενή ενσωμάτωση των πόρων δικτύωσης και υπολογισμού σε ένα σύστημα καθορισμένο από λογισμικό, είναι δυνατή η πλήρης αξιοποίηση όλων των διαθέσιμων πόρων υλικού σε μια λύση ομαδοποίησης.

Cloud Security: Οι εφαρμογές και οι φόρτοι εργασίας δεν φιλοξενούνται πλέον αποκλειστικά σε ένα τοπικό κέντρο δεδομένων. Η προστασία του σύγχρονου κέντρου δεδομένων απαιτεί μεγαλύτερη ευελιξία και καινοτομία για να συμβαδίζει με τη μετάβαση των φόρτων εργασίας εφαρμογών στο cloud. Οι λύσεις Software-defined Networking (SDN) και Software-defined Wide Area Network (SD-WAN) επιτρέπουν λύσεις ασφάλειας δικτύου σε ιδιωτικές, δημόσιες, υβριδικές και cloud-hosted εφαρμογές Firewall-as-a-Service (FWaaS).

2.6 Κοινά Τρωτά Σημεία Ασφάλειας Δικτύου

Προκειμένου να υλοποιηθούν και να διατηρηθούν αποτελεσματικά ασφαλή δίκτυα, είναι σημαντικό να κατανοήσουμε τα κοινά τρωτά σημεία, τις απειλές και τα ζητήματα που αντιμετωπίζουν σήμερα οι επαγγελματίες της πληροφορικής. Ενώ ορισμένα μπορούν να διορθωθούν σχετικά εύκολα, άλλα απαιτούν πιο περίπλοκες λύσεις.

Σχεδόν όλα τα δίκτυα υπολογιστών έχουν τρωτά σημεία που τα αφήνουν ανοιχτά σε εξωτερικές επιθέσεις. Επιπλέον, οι συσκευές και τα δίκτυα εξακολουθούν να είναι ευάλωτα ακόμη και αν κανείς δεν τα απειλεί ενεργά ή δεν τα στοχεύει. Μια ευπάθεια είναι μια κατάσταση του δικτύου ή του υλικού του και όχι το αποτέλεσμα εξωτερικής δράσης [5].

Αυτά είναι μερικά από τα πιο συνηθισμένα τρωτά σημεία δικτύων:

- Ακατάλληλο εγκατεστημένο υλικό ή λογισμικό
- Λειτουργικά συστήματα ή υλικολογισμικό που δεν έχουν ενημερωθεί
- Κακή χρήση υλικού ή λογισμικού
- Κακή ή πλήρης έλλειψη φυσικής ασφάλειας
- Ανασφαλείς κωδικοί πρόσβασης
- Ατέλειες σχεδιασμού στο λειτουργικό σύστημα μιας συσκευής ή στο δίκτυο

Παρόλο που μια ευπάθεια δεν εγγυάται ότι ένας επιτιθέμενος ή ένας μη εξουσιοδοτημένος χρήστης θα στοχεύσει ένα δίκτυό, καθιστά πολύ πιο εύκολο - και πιθανό - για αυτούς να αποκτήσουν πρόσβαση σε αυτό.

2.7 Πεδία Πρόληψης Ασφάλειας Δικτύου

Η ισχυρή ασφάλεια δικτύου θα προστατεύσει από [6]:

- Ιούς (Viruses): Ο ιός είναι ένα κακόβουλο αρχείο που μπορεί να μεταφορτωθεί και να παραμείνει σε λανθάνουσα κατάσταση, το οποίο αναπαράγεται αλλάζοντας άλλα προγράμματα υπολογιστή με τον δικό του κώδικα. Μόλις εξαπλωθεί, τα αρχεία αυτά μολύνονται και μπορούν να εξαπλωθούν από τον έναν υπολογιστή στον άλλο ή/και να καταστρέψουν ή να καταστρέψουν δεδομένα του δικτύου.
- Worms: Μπορούν να επιβραδύνουν τα δίκτυα υπολογιστών καταναλώνοντας εύρος ζώνης καθώς και να επιβραδύνουν την αποδοτικότητα του υπολογιστή σας στην επεξεργασία δεδομένων. Ένα σκουλήκι είναι ένα αυτόνομο κακόβουλο λογισμικό που μπορεί να διαδοθεί και να λειτουργήσει ανεξάρτητα από άλλα αρχεία, ενώ ένας ιός χρειάζεται ένα πρόγραμμα-ξενιστή για να εξαπλωθεί.
- Trojan: Ένα trojan είναι ένα πρόγραμμα κερκόπορτας (backdoor) που δημιουργεί μια είσοδο για κακόβουλους χρήστες για πρόσβαση στο σύστημα του υπολογιστή χρησιμοποιώντας κάτι που μοιάζει με πραγματικό πρόγραμμα, αλλά γρήγορα αποδεικνύεται επιβλαβές. Ένας ιός trojan μπορεί να διαγράψει αρχεία, να ενεργοποιήσει άλλα κακόβουλα προγράμματα που είναι κρυμμένα στο δίκτυο του υπολογιστή σας, όπως έναν ιό και να κλέψει πολύτιμα δεδομένα.
- Spyware: Όπως και το όνομά του, το spyware είναι ένας ιός υπολογιστή που συλλέγει πληροφορίες για ένα άτομο ή έναν οργανισμό χωρίς τη ρητή γνώση του και μπορεί να στείλει τις πληροφορίες που συλλέγονται σε τρίτους χωρίς τη συγκατάθεση του καταναλωτή.

- Adware: Μπορεί να ανακατευθύνει τα αιτήματα αναζήτησής σας σε διαφημιστικούς ιστότοπους και να συλλέγει δεδομένα μάρκετινγκ για εσάς κατά τη διαδικασία, ώστε να εμφανίζονται προσαρμοσμένες διαφημίσεις με βάση το ιστορικό αναζήτησης και αγορών σας.
- Ransomware: Πρόκειται για έναν τύπο trojan κυβερνολογισμικού που έχει σχεδιαστεί για να κερδίζει χρήματα από τον υπολογιστή ενός ατόμου ή ενός οργανισμού στον οποίο έχει εγκατασταθεί, κρυπτογραφώντας τα δεδομένα ώστε να είναι άχρηστα, μπλοκάροντας την πρόσβαση στο σύστημα του χρήστη.

3 Προσομοιωτές Δικτύου

3.1 Εισαγωγή

Σήμερα, η πρόοδος της τεχνολογίας αυξάνεται με ταχείς ρυθμούς. Στα δίκτυα υπολογιστών, τα μη αποδεδειγμένα πρωτόκολλα δεν μπορούν να υλοποιηθούν σε μεγάλη κλίμακα λόγω της αβεβαιότητας του επιτυχούς αποτελέσματός τους. Έτσι, τα πιο πρόσφατα πρωτόκολλα δοκιμάζονται μέσω αναλυτικής μοντελοποίησης ή αλλιώς μέσω εργαλείων προσομοίωσης. Εάν τα τελευταία πρωτόκολλα παρουσιάζουν καλά αποτελέσματα μετά την προσομοίωση, τότε τα πρωτόκολλα θα εκτελεστούν στον πραγματικό κόσμο. Η προσομοίωση δικτύου είναι η κοινή και πιο χρήσιμη μέθοδος, που χρησιμοποιείται για τον υπολογισμό διαφόρων τοπολογιών δικτύου αποκλειστικά για την εφαρμογή στον πραγματικό κόσμο [7]. Αυτές χρησιμοποιούνται εκτενώς από την ερευνητική κοινότητα για την εκτίμηση νέων θεωριών & υποθέσεων. Υπάρχουν διάφορα είδη προσομοιωτών, αλλά η επιλογή τους στην ερευνητική εργασία είναι κρίσιμη για τους ερευνητές.

3.2 Προσομοίωση Δικτύου

Η προσομοίωση δικτύου (Network Simulation) είναι ένα είδος μεθόδου στην έρευνα ενός δικτύου υπολογιστών όπου ένα πρόγραμμα λογισμικού διαμορφώνει την απόδοση ενός δικτύου αναλύοντας τις σχέσεις μεταξύ των διαφόρων οντοτήτων του δικτύου, όπως συνδέσεις, Nswitched, δρομολογητές, κόμβοι, σημεία πρόσβασης. Η απόδοση του δικτύου, οι διάφορες εφαρμογές, οι υπηρεσίες και οι υποστηρίξεις μπορούν να παρακολουθούνται σε ένα εργαστήριο ανάλυσης. Διαφορετικά χαρακτηριστικά του περιβάλλοντος μπορούν επίσης να μεταβληθούν με ελεγχόμενο τρόπο για να αξιολογηθεί ο τρόπος με τον οποίο το δίκτυο ή τα πρωτόκολλα θα αποδίδουν κάτω από διαφορετικές συνθήκες.

3.3 Προσομοιωτής δικτύου

Το λογισμικό που χρησιμοποιείται για την πρόβλεψη της απόδοσης ενός δικτύου υπολογιστών είναι γνωστό ως προσομοιωτής δικτύου. Αυτά χρησιμοποιούνται όταν τα δίκτυα επικοινωνίας έχουν καταστεί πολύ δύσκολα για τις σταθερές αναλυτικές τεχνικές που προσφέρουν ακριβή κατανόηση της απόδοσης του συστήματος. Σε έναν προσομοιωτή, το δίκτυο υπολογιστών μπορεί να διαμορφωθεί με τη βοήθεια συνδέσεων, συσκευών και εφαρμογών και να αναφερθεί η απόδοση ενός δικτύου. Αυτά είναι διαθέσιμα με τη χρήση νέων δικτύων και τεχνολογιών που χρησιμοποιούνται σήμερα, όπως IoT, 5G, WLANs, ad hoc δίκτυα κινητής τηλεφωνίας, WSNs, LTE, ad hoc δίκτυα οχημάτων κ.λπ.

3.4 Εξομοίωση δικτύου

Πρόκειται για ένα είδος μεθόδου που χρησιμοποιείται για τη δοκιμή της δράσης πραγματικών εφαρμογών σε ένα εικονικό δίκτυο. Αυτό είναι ανόμοιο με την προσομοίωση δικτύου, όπου εφαρμόζονται μόνο μαθηματικές μορφές κυκλοφορίας, κανάλια, πρωτόκολλα και μοντέλα δικτύου. Η κύρια λειτουργία της είναι η αξιολόγηση της απόδοσης, η εκτίμηση του αντίκτυπου της αλλαγής και η βελτιστοποίηση της λήψης αποφάσεων στην τεχνολογία.

3.5 Διαφορές μεταξύ Προσομοιωτών και Εξομοιωτών Δικτύου

Ο προσομοιωτής δικτύου και ο εξομοιωτής δικτύου είναι δύο τύποι εργαλείων που χρησιμοποιούνται για τη δοκιμή και την αξιολόγηση της απόδοσης των δικτύων υπολογιστών. Και τα δύο εργαλεία έχουν σχεδιαστεί για να προσομοιώνουν τη συμπεριφορά ενός πραγματικού δικτύου, αλλά το κάνουν με διαφορετικούς τρόπους.

Ένας προσομοιωτής δικτύου είναι ένα εργαλείο λογισμικού που χρησιμοποιείται για τη μοντελοποίηση και την προσομοίωση της συμπεριφοράς ενός δικτύου. Επιτρέπει στους χρήστες να δημιουργούν εικονικά δίκτυα και να δοκιμάζουν διαφορετικές διαμορφώσεις και πρωτόκολλα δικτύου χωρίς την ανάγκη φυσικού υλικού. Οι προσομοιωτές δικτύων

χρησιμοποιούν μαθηματικά μοντέλα για την προσομοίωση της συμπεριφοράς των στοιχείων του δικτύου, όπως δρομολογητές και μεταγωγείς, και μπορούν να χρησιμοποιηθούν για τη δοκιμή της απόδοσης διαφόρων πρωτοκόλλων δικτύωσης. Παραδείγματα προσομοιωτών δικτύου είναι το NS-3 και το OPNET.

Ο εξομοιωτής δικτύου, από την άλλη πλευρά, είναι ένα εργαλείο υλικού ή λογισμικού που χρησιμοποιείται για τη μίμηση της συμπεριφοράς ενός πραγματικού δικτύου. Επιτρέπει στους χρήστες να δοκιμάζουν την απόδοση συσκευών και εφαρμογών δικτύου σε ένα ελεγχόμενο περιβάλλον που μιμείται στενά ένα πραγματικό δίκτυο. Οι εξομοιωτές δικτύων λειτουργούν αναπαράγοντας τα φυσικά και λογικά χαρακτηριστικά ενός πραγματικού δικτύου, όπως το εύρος ζώνης, η καθυστέρηση και η απώλεια πακέτων. Παραδείγματα εξομοιωτών δικτύου είναι το GNS3 και το EVE-NG.

Μία από τις κύριες διαφορές μεταξύ ενός προσομοιωτή δικτύου και ενός εξομοιωτή δικτύου είναι το επίπεδο αφαίρεσης. Οι προσομοιωτές δικτύων χρησιμοποιούν συνήθως μαθηματικά μοντέλα για την προσομοίωση της συμπεριφοράς των στοιχείων του δικτύου, ενώ οι εξομοιωτές δικτύων αναπαράγουν τα φυσικά και λογικά χαρακτηριστικά ενός πραγματικού δικτύου. Αυτό σημαίνει ότι οι προσομοιωτές δικτύων είναι γενικά πιο αφηρημένοι, ενώ οι εξομοιωτές δικτύων είναι πιο ρεαλιστικοί.

Μια άλλη διαφορά είναι ότι οι προσομοιωτές δικτύου χρησιμοποιούνται συνήθως για τη δοκιμή της απόδοσης πρωτοκόλλων και διαμορφώσεων δικτύου, ενώ οι εξομοιωτές δικτύου χρησιμοποιούνται για τη δοκιμή της απόδοσης συσκευών και εφαρμογών δικτύου. Οι προσομοιωτές δικτύων είναι χρήσιμοι για τη δοκιμή της συμπεριφοράς νέων πρωτοκόλλων και διαμορφώσεων, ενώ οι εξομοιωτές δικτύων είναι χρήσιμοι για τη δοκιμή της συμβατότητας και της απόδοσης υφιστάμενων συσκευών και εφαρμογών δικτύου.

Όσον αφορά το κόστος, οι προσομοιωτές δικτύων είναι γενικά λιγότερο ακριβοί από τους εξομοιωτές δικτύων, καθώς δεν απαιτούν φυσικό υλικό. Οι εξομοιωτές δικτύου, από την άλλη πλευρά, μπορεί να είναι ακριβοί, καθώς απαιτούν εξειδικευμένο υλικό και λογισμικό.

Συμπερασματικά, ο προσομοιωτής δικτύου και ο εξομοιωτής δικτύου είναι δύο τύποι εργαλείων που χρησιμοποιούνται για τη δοκιμή και την αξιολόγηση της απόδοσης των δικτύων υπολογιστών. Και τα δύο εργαλεία έχουν σχεδιαστεί για να προσομοιώνουν τη συμπεριφορά ενός πραγματικού δικτύου, αλλά το κάνουν με διαφορετικούς τρόπους. Οι προσομοιωτές δικτύων χρησιμοποιούνται συνήθως για τη δοκιμή της απόδοσης πρωτοκόλλων και διαμορφώσεων δικτύου, ενώ οι εξομοιωτές δικτύων χρησιμοποιούνται για τη δοκιμή της απόδοσης συσκευών και εφαρμογών δικτύου. Οι προσομοιωτές δικτύων είναι λιγότερο ακριβοί από τους εξομοιωτές δικτύων.

3.6 Προσομοιωτές Δικτύου στην Ασφάλεια στον Κυβερνοχώρο

Οι προσομοιωτές δικτύου χρησιμοποιούνται στην ασφάλεια στον κυβερνοχώρο για την προσομοίωση και τη δοκιμή διαφόρων σεναρίων και διαμορφώσεων δικτύου σε ελεγχόμενο περιβάλλον. Αυτό επιτρέπει στους επαγγελματίες ασφαλείας να δοκιμάζουν και να αξιολογούν διάφορα μέτρα ασφαλείας, όπως διαμορφώσεις τείχους προστασίας, συστήματα ανίχνευσης εισβολών και άλλα εργαλεία ασφαλείας, χωρίς να διακινδυνεύουν ζημιές σε ένα ζωντανό δίκτυο.

Μία από τις κύριες χρήσεις των προσομοιωτών δικτύου στην ασφάλεια στον κυβερνοχώρο είναι η δοκιμή της αποτελεσματικότητας διαφόρων μέτρων ασφαλείας. Για παράδειγμα, ένας επαγγελματίας ασφαλείας μπορεί να χρησιμοποιήσει έναν προσομοιωτή δικτύου για να δημιουργήσει ένα δίκτυο με μια συγκεκριμένη διαμόρφωση και στη συνέχεια να δοκιμάσει πώς αποδίδουν διαφορετικές διαμορφώσεις τείχους προστασίας ή συστήματα ανίχνευσης εισβολών σε αυτό το περιβάλλον. Αυτό επιτρέπει στον επαγγελματία να εντοπίσει τυχόν

αδυναμίες ή τρωτά σημεία στα μέτρα ασφαλείας και να προβεί στις απαραίτητες προσαρμογές.

Μια άλλη χρήση των προσομοιωτών δικτύου στην ασφάλεια στον κυβερνοχώρο είναι η προσομοίωση διαφόρων τύπων επιθέσεων, όπως επιθέσεις άρνησης παροχής υπηρεσιών (DoS) ή επιθέσεις man-in-the-middle (MitM), και η αξιολόγηση της αποτελεσματικότητας των διαφόρων μέτρων ασφαλείας για την πρόληψη ή τον μετριασμό αυτών των επιθέσεων. Αυτό μπορεί να βοηθήσει τους επαγγελματίες της ασφάλειας να προσδιορίσουν τα πιο αποτελεσματικά μέτρα ασφαλείας για διαφορετικούς τύπους επιθέσεων και να αναπτύξουν στρατηγικές για την καλύτερη προστασία των δικτύων από αυτές τις απειλές [7].

Οι προσομοιωτές δικτύων μπορούν επίσης να χρησιμοποιηθούν για την εκπαίδευση των επαγγελματιών ασφαλείας στον εντοπισμό και την αντιμετώπιση διαφόρων τύπων επιθέσεων στον κυβερνοχώρο. Για παράδειγμα, ένας προσομοιωτής δικτύου μπορεί να χρησιμοποιηθεί για την προσομοίωση ενός συγκεκριμένου σεναρίου επίθεσης και στη συνέχεια να ζητηθεί από τους επαγγελματίες ασφαλείας να εντοπίσουν και να αντιδράσουν στην επίθεση σαν να συνέβαινε σε ένα ζωντανό δίκτυο. Αυτό επιτρέπει στους επαγγελματίες να αποκτήσουν πρακτική εμπειρία στον εντοπισμό και την αντιμετώπιση διαφόρων τύπων απειλών στον κυβερνοχώρο και να αναπτύξουν τις δεξιότητές τους στην αντιμετώπιση και τη διαχείριση περιστατικών.

Επιπλέον, οι προσομοιωτές δικτύου μπορούν επίσης να χρησιμοποιηθούν για την προσομοίωση των επιπτώσεων διαφορετικών διαμορφώσεων και τοπολογιών δικτύου στη συνολική ασφάλεια ενός δικτύου. Αυτό μπορεί να βοηθήσει τους επαγγελματίες της ασφάλειας να εντοπίσουν πιθανές αδυναμίες στο σχεδιασμό ενός δικτύου και να κάνουν προσαρμογές για να βελτιώσουν τη συνολική κατάσταση ασφαλείας του.

Συνολικά, οι προσομοιωτές δικτύων διαδραματίζουν σημαντικό ρόλο στην ασφάλεια στον κυβερνοχώρο, επιτρέποντας στους επαγγελματίες της ασφάλειας να δοκιμάζουν και να αξιολογούν διάφορα μέτρα ασφαλείας, να προσομοιώνουν διάφορους τύπους κυβερνοεπιθέσεων, να εκπαιδεύουν επαγγελματίες στην αντιμετώπιση και τη διαχείριση περιστατικών και να προσομοιώνουν τον αντίκτυπο διαφορετικών διαμορφώσεων και τοπολογιών δικτύου στη συνολική ασφάλεια ενός δικτύου [8]. Αυτό επιτρέπει στους οργανισμούς να προστατεύουν καλύτερα τα δίκτυά τους από απειλές στον κυβερνοχώρο και να ελαχιστοποιούν τις πιθανές ζημιές από επιθέσεις στον κυβερνοχώρο.

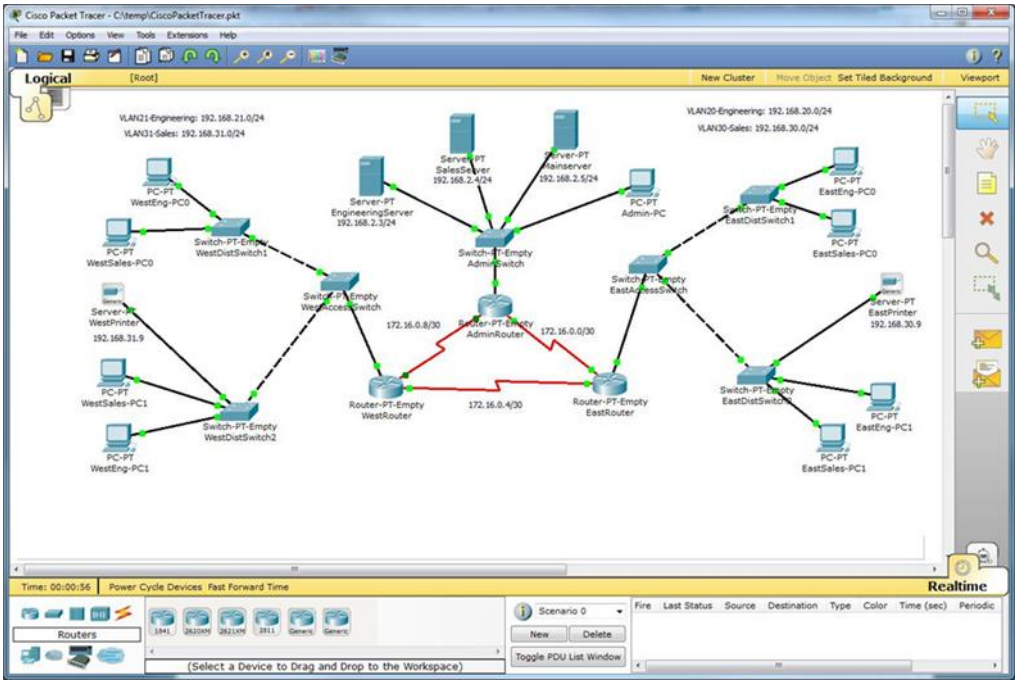
4 Συνοπτική Μελέτη και Παρουσίαση Open-Source Network Simulators

4.1 Cisco Packet Tracer

Το Cisco Packet Tracer αναπτύχθηκε από την εταιρεία Cisco. Πρόκειται για έναν προσομοιωτή δικτύου για απλά και σύνθετα δίκτυα. Ο κύριος σκοπός του Cisco Packet Tracer (CPT) είναι να βοηθήσει τον μηχανικό ή τον ερευνητή στην εκμάθηση και απόκτηση εμπειρίας από κοντά σε ζητήματα δικτύων υπολογιστών. Παρέχει επίσης συγκεκριμένες δεξιότητες για την τεχνολογία Cisco. Αυτό το εργαλείο δεν μπορεί να αντικαταστήσει ένα router ή ένα switch, καθώς επίσης υποστηρίζει μόνο λύσεις και προϊόντα της Cisco.

Το Cisco Packet Tracer βοηθά επίσης τον σπουδαστή να υλοποιήσει μία εργασία του δουλεύοντας μόνος του ή συνεργαζόμενος με μια ομάδα. Βοηθά επίσης τον μηχανικό να δοκιμάσει την εφαρμογή μίας προσομοίωσης του πριν την υλοποίησή της. Επίσης, οι μηχανικοί που εργάζονται στην υποστήριξη δικτύων μπορούν επίσης να αναπτύξουν τυχόν αλλαγές χρησιμοποιώντας επίσης το Cisco Packet Tracer. Αρχικά, οι μηχανικοί δοκιμάζουν τις αλλαγές που θέλουν να κάνουν. Στη συνέχεια, εάν όλες οι αλλαγές λειτούργησαν ορθά, το η υλοποίηση προχωρά προς την ανάπτυξη της δοκιμής [9].

Με τη βοήθεια του Cisco Packet Tracer, είναι πολύ πιο εύκολο για όλους τους μηχανικούς να προσθέσουν ή να αφαιρέσουν οποιεσδήποτε προσομοιωμένες συσκευές δικτύου. Οι λειτουργίες αυτές μπορούν να εκτελεστούν με δύο τρόπους. Ο πρώτος είναι με drag and drop στο User Interface και ο άλλος είναι το command line interface (cli).



Εικόνα 1: Cisco Packet Tracer GUI

4.1.1 Χώροι Εργασίας

Το Cisco Packet Tracer παρέχει 2 χώρους εργασίας:

- Το Λογικό χώρο εργασίας: Ο λογικός χώρος εργασίας εμφανίζει τη λογική τοπολογία δικτύου που έχει κατασκευάσει ο χρήστης. Εμφανίζει τη σύνδεση, την τοποθέτηση και την ομαδοποίηση των εικονικών συσκευών δικτύου.

- Το Φυσικό χώρο εργασίας: Στο φυσικό χώρο εργασίας αναπαρίσταται η φυσική υλοποίηση του λογικού δικτύου. Δείχνει επίσης πώς συνδέονται οι συσκευές δικτύου, όπως τα switches, τα routers και οι κεντρικοί υπολογιστές, σε μια πραγματική τοπολογία δικτύου.

4.1.2 Βασικά Χαρακτηριστικά

Cisco Packet Tracer Modes: Το Cisco Packet Tracer παρέχει δύο τρόπους λειτουργίας για την απεικόνιση της συμπεριφοράς ενός δικτύου, τη λειτουργία πραγματικού χρόνου (Real Time Mode) και τη λειτουργία προσομοίωσης (Simulation Mode). Στη λειτουργία πραγματικού χρόνου το δίκτυο συμπεριφέρεται όπως οι πραγματικές συσκευές, με άμεση απόκριση σε πραγματικό χρόνο για όλες τις δραστηριότητες του δικτύου. Η λειτουργία πραγματικού χρόνου παρέχει στους ερευνητές μια βιώσιμη εναλλακτική λύση σε σχέση με τον πραγματικό εξοπλισμό και τους επιτρέπει να αποκτήσουν πρακτική εξάσκηση στη διαμόρφωση πριν εργαστούν με πραγματικό εξοπλισμό. Στη λειτουργία προσομοίωσης ο χρήστης μπορεί να δει και να ελέγξει τα χρονικά διαστήματα, τις εσωτερικές λειτουργίες της μεταφοράς δεδομένων και τη διάδοση των δεδομένων σε ένα δίκτυο. Αυτό βοηθά τους ερευνητές να κατανοήσουν τις θεμελιώδεις έννοιες πίσω από τις λειτουργίες του δικτύου. Η καλή κατανόηση των βασικών αρχών του δικτύου μπορεί να βοηθήσει στην επιτάχυνση της εκμάθησης σχετικών εννοιών.

Πρωτόκολλά: Το Cisco Packet Tracer υποστηρίζει τα πολλαπλά πρωτόκολλα που καλύπτουν διάφορα επίπεδα του OSI Model. Τα πρωτόκολλα αυτά παρουσιάζονται αναλυτικά στην παρακάτω εικόνα:

Layer	Cisco Packet Tracer Supported Protocols
Application	• FTP , SMTP, POP3, HTTP, TFTP, Telnet, SSH, DNS, DHCP, NTP, SNMP, AAA, ISR VOIP, SCCP config and calls ISR command support, Call Manager Express
Transport	• TCP and UDP, TCP Nagle Algorithm & IP Fragmentation, RTP
Network	• BGP, IPv4, ICMP, ARP, IPv6, ICMPv6, IPSec, RIPv1/ v2/ng, Multi-Area OSPF, EIGRP, Static Routing, Route Redistribution, Multilayer Switching, L3 QoS, NAT, CBAL , Zone-based policy firewall and Intrusion Protection System on the ISR, GRE VPN, IPSec VPN
Network Access/ Interface	• Ethernet (802.3), 802.11, HDLC, Frame Relay, PPP, PPPoE, STP, RSTP, VTP, DTP, CDP, 802.1q, PAgP, L2 QoS, SLARP, Simple WEP, WPA, EAP

Εικόνα 2: Πρωτόκολλα Cisco Packet Tracer

Modular Devices: Οι γραφικές αναπαραστάσεις προσομοιώνουν οπτικά το hardware και προσφέρουν τη δυνατότητα εισαγωγής καρτών διασύνδεσης σε routers και switches, οι οποίοι στη συνέχεια γίνονται μέρος της προσομοίωσης.

Multiuser Functionality: Το Cisco Packet Tracer μια εφαρμογή που μπορεί να χρησιμοποιηθεί σε δίκτυο, με λειτουργία ομότιμων πολλαπλών χρηστών και επιτρέπει τη συνεργατική κατασκευή εικονικών δικτύων πάνω σε ένα πραγματικό δίκτυο. Η λειτουργία πολλαπλών χρηστών επιτρέπει συνεργατικές και διαδραστικές αλληλεπιδράσεις, παρέχοντας τη δυνατότητα εξέλιξης από την ατομική στην κοινωνική μάθηση και διαθέτει δυνατότητες για συνεργασία, ανταγωνισμό, αλληλεπιδράσεις μεταξύ ερευνητών από απόσταση, κοινωνική δικτύωση και εξατομίκευση.

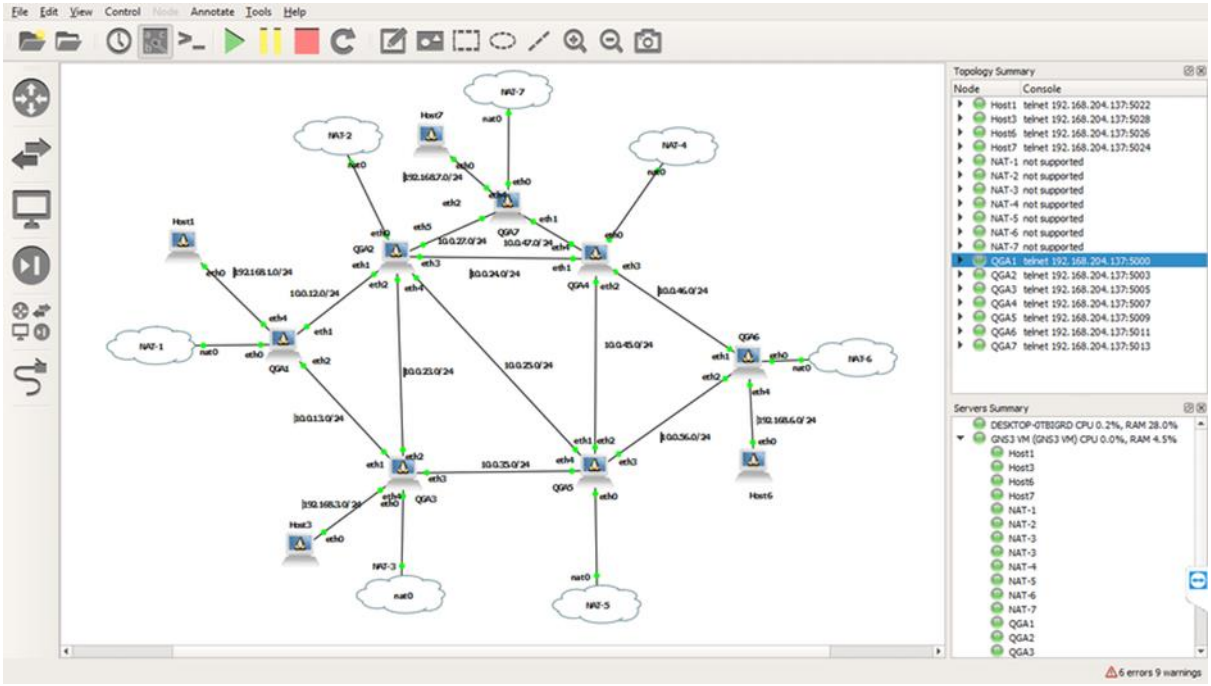
Tutorials: Το Cisco Packet Tracer περιλαμβάνει αρκετά βασικά σεμινάρια βήμα προς βήμα που εξοικειώνουν τους χρήστες με τις λειτουργίες του προϊόντος και εξηγούν πώς να συμμετέχουν σε προσομοιώσεις. Πρόσθετα εκπαιδευτικά σεμινάρια για προχωρημένους είναι διαθέσιμα για λήψη από το Cisco NetAcademy.

Help: Είναι διαθέσιμη μια λειτουργία βοήθειας για την εξοικείωση των χρηστών με το περιβάλλον εργασίας, τις λειτουργίες και τα χαρακτηριστικά του Cisco Packet Tracer. Η περιοχή βοήθειας περιλαμβάνει σημαντικές σημειώσεις και συμβουλές και παρέχει σχολιασμένα στιγμιότυπα οθόνης για την καλύτερη κατανόηση.

Activity Wizard: Ο οδηγός δραστηριοτήτων επιτρέπει στους χρήστες να συντάσσουν τις δικές τους μαθησιακές δραστηριότητες, δημιουργώντας σενάρια με τη χρήση διδακτικού κειμένου και δημιουργώντας αρχικές και τελικές τοπολογίες δικτύου και προκαθορισμένα πακέτα. Ο Οδηγός δραστηριοτήτων περιλαμβάνει επίσης δυνατότητες βαθμολόγησης και ανατροφοδότησης.

4.2 GNS3

Το GNS3 χρησιμοποιείται από εκατοντάδες χιλιάδες μηχανικούς δικτύων παγκοσμίως για την εξομοίωση, διαμόρφωση, δοκιμή και αντιμετώπιση προβλημάτων εικονικών και πραγματικών δικτύων. Το GNS3 επιτρέπει να τρέξουμε μια μικρή τοπολογία που αποτελείται από λίγες μόνο συσκευές σε έναν φορητό υπολογιστή, μέχρι και αυτές που έχουν πολλές συσκευές που φιλοξενούνται σε πολλούς διακομιστές ή ακόμη και φιλοξενούνται στο cloud. Αποτελεί μία open-source λύση και είναι διαθέσιμο στο https://gns3.com.



Εικόνα 3: GNS3 GUI

Το GNS3 επιτρέπει στους μηχανικούς δικτύων να εικονικοποιούν πραγματικές συσκευές υλικού για πάνω από 10 χρόνια. Ενώ αρχικά προσομοίωνε μόνο συσκευές της Cisco χρησιμοποιώντας λογισμικό που ονομάζεται Dynamips, το GNS3 έχει πλέον εξελιχθεί και υποστηρίζει πολλές συσκευές από πολλούς προμηθευτές δικτύων, συμπεριλαμβανομένων των Cisco virtual switches, των Cisco ASA, των Brocade vRouters, των μεταγωγέων Cumulus Linux, των Docker instances, των HPE VSR, των πολλαπλών συσκευών Linux και πολλών άλλων [10].

4.2.1 Αρχιτεκτονική

Το GNS3 αποτελείται από δύο software components:

- Το GNS3-all-in-one software (GUI): Όπου αφορά την πλευρά του χρήστη και αποτελεί τη γραφική διεπαφή (Graphical User Interface - GUI) και εγκαθίσταται στο host μηχάνημα του χρήστη.
- Το GNS3 virtual machine (VM): Όπου αφορά την πλευρά του server και πιο συγκεκριμένα το που φιλοξενούνται οι τοπολογίες που δημιουργεί ο χρήστης. Στην περίπτωση αυτή προσφέρονται τρεις επιλογές:
    1. Τοπικός GNS3 server, προσφέρεται δηλαδή να στηθεί η υλοποίηση τοπικά.

2. Τοπικό GNS3 VM, όπου στην περίπτωση αυτή η τοπολογία φιλοξενείται σε τοπικό εικονικό μηχάνημα (Virtual Machine - VM) και είναι η προτεινόμενη λύση.
3. Απομακρυσμένο GNS3 VM, όπου προσφέρεται η δυνατότητα στον χρήστη να αποθηκεύσει την τοπολογία στο υπολογιστικό νέφος και να έχει πρόσβαση από οποιοδήποτε μηχάνημα.

Το GNS3 προσφέρει την επιλογή και για εξομοίωση (emulation) όσο και για προσομοίωση (simulation) δικτύου.

- Εξομοίωση: Το GNS3 μιμείται ή εξομοιώνει το υλικό (hardware) μιας συσκευής και δίνει την δυνατότητα να εκτελεστούν πραγματικά images στην εικονική συσκευή. Για παράδειγμα, ένας ερευνητής μπορεί να αντιγράψει το Cisco IOS από έναν πραγματικό, φυσικό router Cisco και να το εκτελέσει σε έναν εικονικό, εξομοιωμένο δρομολογητή Cisco στο GNS3.
- Προσομοίωση: Το GNS3 προσομοιώνει τα χαρακτηριστικά και τη λειτουργικότητα μιας συσκευής, όπως ένα switch. Δεν δύναται η δυνατότητα να εκτελεστούν πραγματικά λειτουργικά συστήματα (όπως το Cisco IOS), αλλά μάλλον μια προσομοιωμένη συσκευή που έχει αναπτυχθεί από το GNS3, όπως το ενσωματωμένο switch επιπέδου 2 (built-in Layer 2 switch).

4.2.2 Πλεονεκτήματα και Μειονεκτήματα Χρήσης του GNS3:

Η χρήση του συγκεκριμένου προϊόντος, παρέχει τα εξής πλεονεκτήματα:

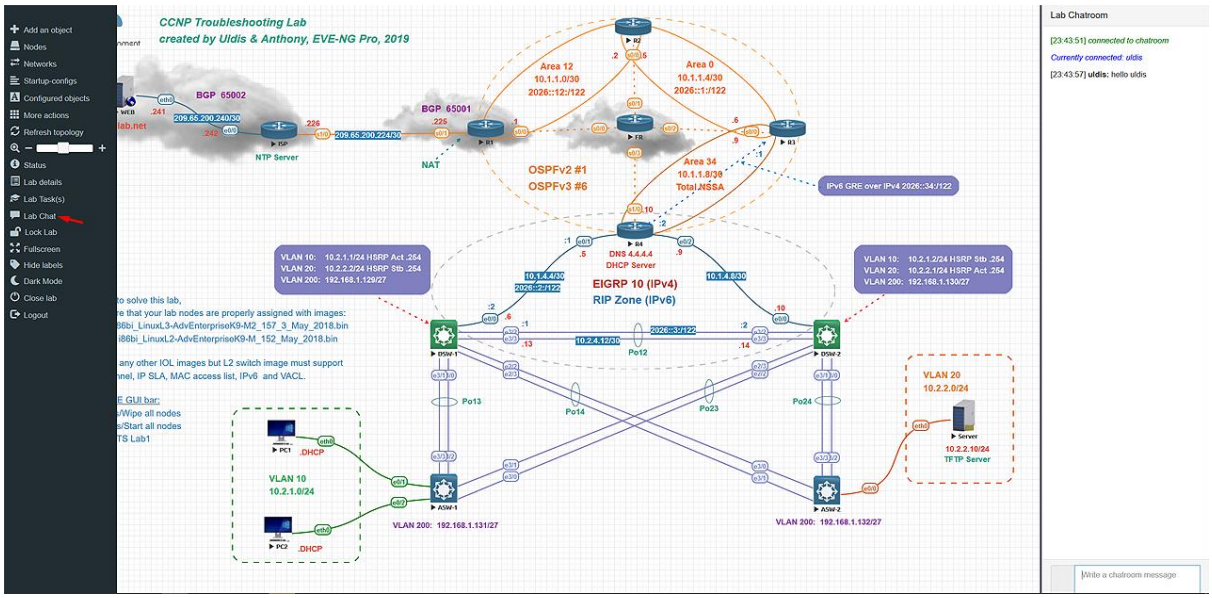
- Το λογισμικό είναι ελεύθερο και δωρεάν προς εγκατάσταση χωρίς να απαιτείται κάποια επιπλέον συνδρομή.
- Δεν υπάρχει κάποιος περιορισμός στη χρήση υποστηριζόμενων συσκευών.
- Υποστηρίζει πολλαπλές λύσεις δικτύου και ασφάλειας από πολλαπλούς κατασκευαστές.
- Δεν απαιτείται οπωσδήποτε η χρήση κάποιου hypervisor, καθώς επίσης υποστηρίζεται και από όλους τους δωρεάν hypervisors (VirtualBox, VMware Workstation).
- Παρέχεται μεγάλη υποστήριξη όντας μέλος στην κοινότητα του προϊόντος.

Στην αντίπερα όχθη, ο χρήστης αντιμετωπίζει τα εξής μειονεκτήματα:

- Τα images των συσκευών πρέπει να κατέβουν και να εγκατασταθούν από το χρήστη, γεγονός που προϋποθέτει την αγορά της άδειας χρήσης της συσκευής.
- Δεν υπάρχει αυτοματοποιημένη διαδικασία προσθήκης κάποιας συσκευής (firewall, router, switch) όταν κατέβει από τον χρήστη.
- Η χρήση του GNS3 επιβαρύνει τις επιδόσεις του υπολογιστή σε όρους μνήμης και επεξεργαστή.

4.3 EVE-NG

Το Emulated Virtual Environment Next Generation (EVE-NG) είναι ένας προσομοιωτής δικτύου πολλαπλών προμηθευτών που παρέχει παρόμοια χαρακτηριστικά με το GNS3.



Εικόνα 4: EVE-NG GUI

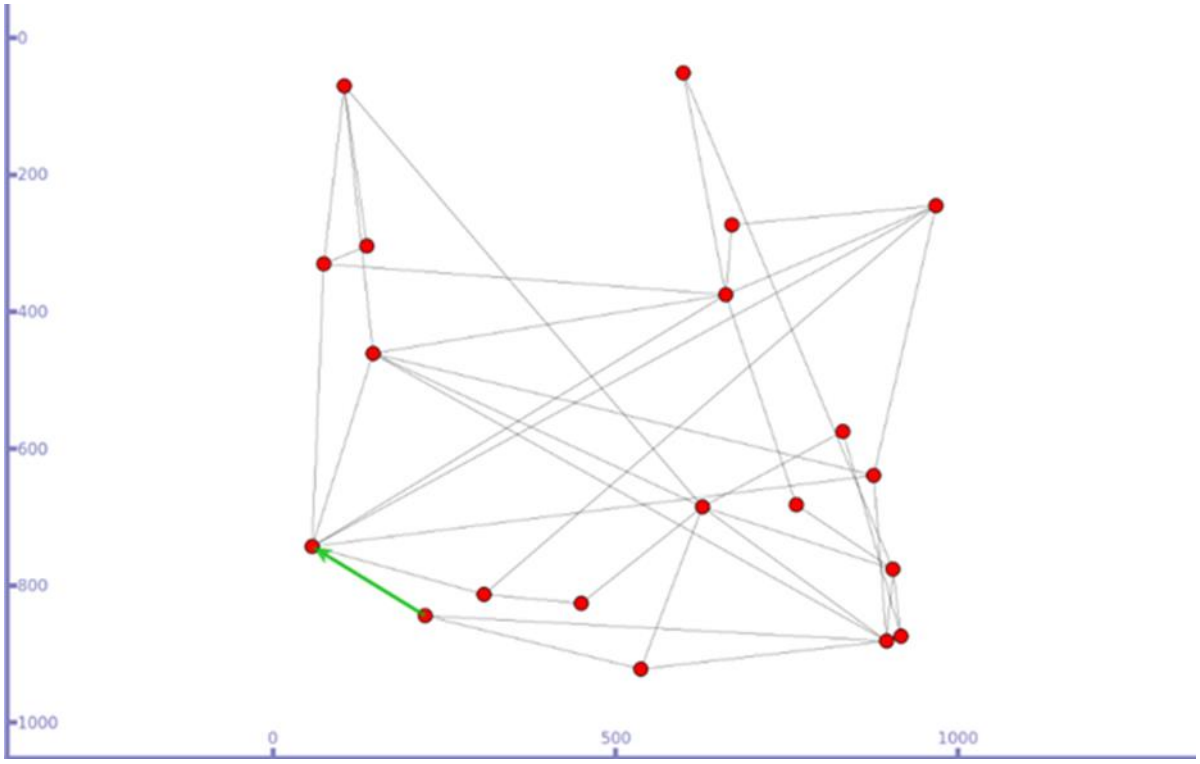
Η κύρια διαφορά σε σχέση με το GNS3 είναι ότι το EVE-NG δεν χρειάζεται κάποιο client για να λειτουργήσει. Αυτό ουσιαστικά σημαίνει ότι λειτουργεί ως αυτόνομη εικονική μηχανή και δεν απαιτεί την εγκατάσταση πρόσθετων στοιχείων λογισμικού στην τοπική συσκευή για να λειτουργήσει [11].

Όπως και το GNS3, το EVE-NG απαιτεί τη χρήση εικόνων Cisco IOS ή εικόνων Cisco VIRL για να λειτουργήσει. Ωστόσο, σε αντίθεση με το GNS3, το EVE-NG διαθέτει μια δωρεάν έκδοση που υποστηρίζεται από την κοινότητα και μια επαγγελματική έκδοση που μπορεί να αγοραστεί με την αντίστοιχη τιμή. Τα πρόσθετα οφέλη της pro έκδοσης περιλαμβάνουν χρονομετρητές εργαστηρίου, ενσωμάτωση του Wireshark και άλλα πολύτιμα εργαλεία.

4.4 NS-3

Το NS-3 είναι ένας προσομοιωτής δικτύων διακριτών συμβάντων, που απευθύνεται κυρίως για ερευνητική και εκπαιδευτική χρήση. Το ns-3 είναι ελεύθερο λογισμικό, με άδεια χρήσης GNU GPLv2, και είναι διαθέσιμο στο κοινό για έρευνα, ανάπτυξη και χρήση.

Ο στόχος του έργου ns-3 είναι να αναπτύξει ένα ελεύθερο και ανοικτού κώδικα περιβάλλον προσομοίωσης κατάλληλο για την έρευνα δικτύων: θα πρέπει να είναι ευθυγραμμισμένο με τις ανάγκες προσομοίωσης της σύγχρονης έρευνας δικτύων και να ενθαρρύνει τη συνεισφορά της κοινότητας, την αξιολόγηση από ομότιμους και την επικύρωση του λογισμικού. Επίσης, βασίζεται στη χρήση scripts σε γλώσσα είτε C++ είτε Python [12].



Εικόνα 5: NS-3 GUI

4.4.1 Μοντέλα Προσομοίωσης

Το project του NS-3 έχει δεσμευτεί να δημιουργήσει έναν σταθερό πυρήνα προσομοίωσης, ο οποίος είναι καλά τεκμηριωμένος, εύκολος στη χρήση και το debug, και ο οποίος καλύπτει τις ανάγκες ολόκληρης της ροής εργασίας προσομοίωσης, από τη διαμόρφωση της προσομοίωσης έως τη συλλογή και την ανάλυση ιχνών (trace collection and analysis) [13].

Επιπλέον, η υποδομή λογισμικού του NS-3 ενθαρρύνει την ανάπτυξη μοντέλων προσομοίωσης που είναι επαρκώς ρεαλιστικά ώστε να επιτρέπουν στο NS-3 να χρησιμοποιείται ως εξομοιωτής δικτύου σε πραγματικό χρόνο, διασυνδεδεμένο με τον πραγματικό κόσμο, και που επιτρέπει την επαναχρησιμοποίηση πολλών υφιστάμενων υλοποιήσεων πρωτοκόλλων του πραγματικού κόσμου στο πλαίσιο του NS-3.

Ο πυρήνας προσομοίωσης ns-3 υποστηρίζει την έρευνα τόσο σε δίκτυα IP όσο και σε δίκτυα που δεν βασίζονται στο πρωτόκολλο IP. Ωστόσο, η μεγάλη πλειονότητα των χρηστών του επικεντρώνεται σε προσομοιώσεις ασύρματων/IP που περιλαμβάνουν μοντέλα για Wi-Fi, LTE ή άλλα ασύρματα συστήματα για τα Layers 1 και 2. Άλλα δημοφιλή ερευνητικά θέματα

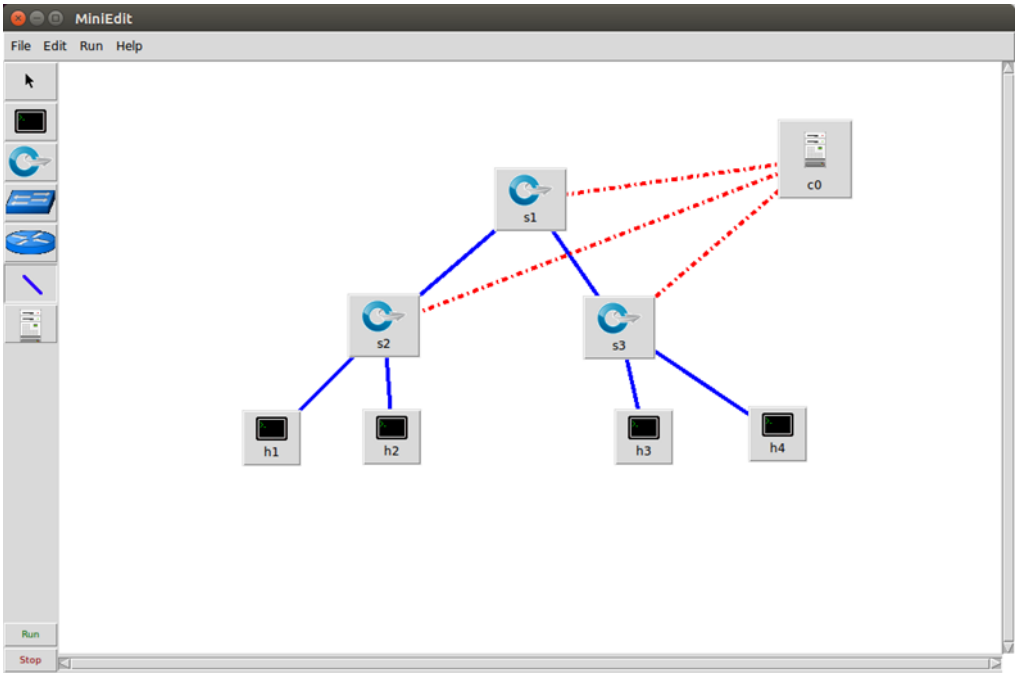
περιλαμβάνουν την απόδοση του TCP και την απόδοση των κινητών ad hoc πρωτοκόλλων δρομολόγησης.

Το NS-3 υποστηρίζει επίσης έναν χρονοπρογραμματιστή πραγματικού χρόνου που διευκολύνει ορισμένες περιπτώσεις χρήσης "προσομοίωσης στο βρόχο" για την αλληλεπίδραση με πραγματικά συστήματα. Για παράδειγμα, οι χρήστες μπορούν να εκπέμπουν και να λαμβάνουν πακέτα που παράγονται από τον ns-3 σε πραγματικές συσκευές δικτύου και ο ns-3 μπορεί να χρησιμεύσει ως πλαίσιο διασύνδεσης για την προσθήκη αποτελεσμάτων σύνδεσης μεταξύ εικονικών μηχανών.

Μια άλλη έμφαση του προσομοιωτή είναι η επαναχρησιμοποίηση πραγματικού κώδικα εφαρμογών και πυρήνα. Το πλαίσιο άμεσης εκτέλεσης κώδικα επιτρέπει στους χρήστες να εκτελούν εφαρμογές βασισμένες σε C ή C++ ή τη στοίβα δικτύωσης του πυρήνα Linux (Linux kernel networking stack) μέσα στον ns-3.

4.5 Mininet

Το Mininet είναι ένας εξομοιωτής δικτύου που δημιουργεί ένα δίκτυο με εικονικούς χρήστες (hosts), ελεγκτές (controllers), switches και συνδέσεων (links). Το Mininet βασίζεται σε ένα τυπικό λογισμικό Linux και οι μεταγωγείς του υποστηρίζουν OpenFlow για εξαιρετικά ευέλικτη προσαρμοσμένη δρομολόγηση και Software-Defined Networking [14].



Εικόνα 6: Mininet GUI

Το Mininet υποστηρίζει την έρευνα, την ανάπτυξη, την εκμάθηση, την κατασκευή πρωτοτύπων, το testing, το debugging και κάθε άλλη εργασία που θα μπορούσε να επωφεληθεί από την ύπαρξη ενός πλήρους πειραματικού δικτύου σε έναν οποιοδήποτε υπολογιστή.

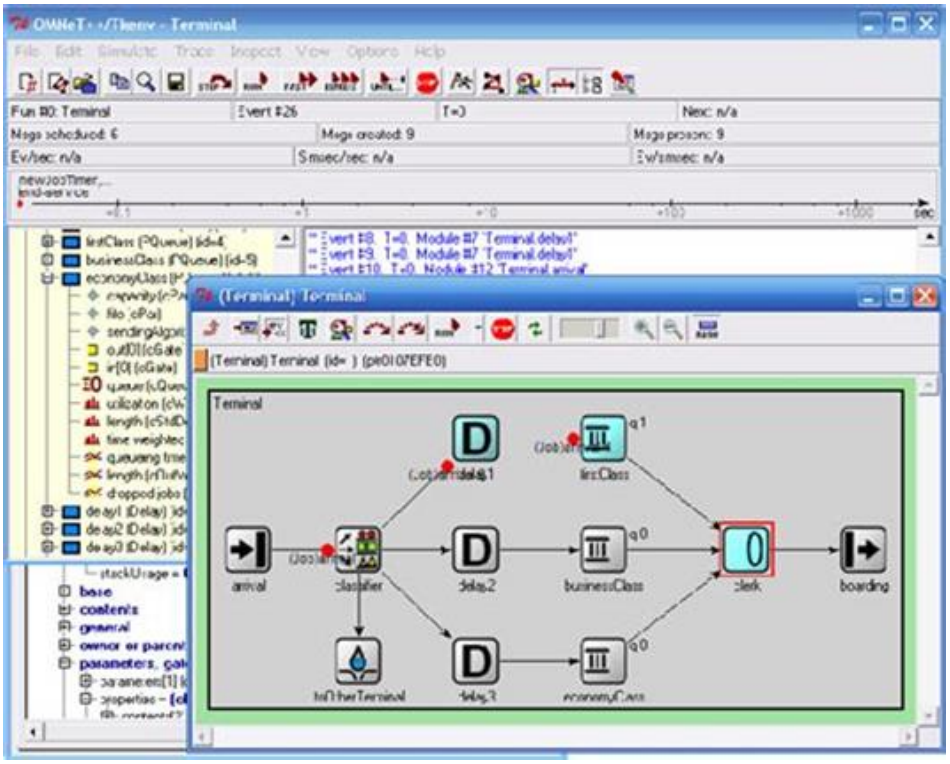
Επιπρόσθετα, το Mininet:

- Παρέχει ένα απλό και φθηνό περιβάλλον δοκιμών δικτύου για την ανάπτυξη εφαρμογών OpenFlow.
- Δίνει τη δυνατότητα σε πολλούς προγραμματιστές να εργάζονται ανεξάρτητα στην ίδια τοπολογία.
- Επιτρέπει τη δοκιμή σύνθετης τοπολογίας, χωρίς να χρειάζεται να συνδεθεί ένα φυσικό δίκτυο.
- Υποστηρίζει αυθαίρετες προσαρμοσμένες τοπολογίες και περιλαμβάνει ένα βασικό σύνολο παραμετροποιημένων τοπολογιών.
- Παρέχει στον ερευνητή έναν εύκολο τρόπο να αποκτήσει σωστή συμπεριφορά του συστήματος (και, στο βαθμό που υποστηρίζεται από το υλικό, απόδοση) και να πειραματιστεί με τοπολογίες.
- Υποστηρίζει και τρέχει πραγματικό κώδικα, συμπεριλαμβανομένων των στάνταρ εφαρμογών δικτύου των Unix/Linux περιβαλλόντων.

Συνεπώς, βάσει όλων αυτών, ο κώδικας που αναπτύσσεται και τεστάρεται σε ένα περιβάλλον Mininet για έναν ελεγκτή OpenFlow ή ένα παραμετροποιημένο switch, δύναται να μετακινηθεί σε ένα πραγματικό περιβάλλον με ελάχιστες αλλαγές, για δοκιμές σε πραγματικά δίκτυα, αποτίμηση απόδοσης, και testing. Αυτό σημαίνει ότι ένας σχεδιασμός που λειτουργεί στο Mininet μπορεί συνήθως να μεταβεί απευθείας σε hardware switches για προώθηση πακέτων με ρυθμό γραμμής.

4.6 OMneT++

Το OMNeT++ είναι μια επεκτάσιμη, αρθρωτή, βασισμένη σε συστατικά βιβλιοθήκη και πλαίσιο προσομοίωσης C++, κυρίως για τη δημιουργία προσομοιωτών δικτύων. Ο όρος "δίκτυο" εννοείται με μια ευρύτερη έννοια που περιλαμβάνει ενσύρματα και ασύρματα δίκτυα επικοινωνίας, δίκτυα εντός του chip, δίκτυα ουρών αναμονής και ούτω καθεξής [15]. Η λειτουργικότητα συγκεκριμένων τομέων, όπως η υποστήριξη δικτύων αισθητήρων, ασύρματων ad-hoc δικτύων, πρωτοκόλλων διαδικτύου, μοντελοποίησης επιδόσεων, φωτονικών δικτύων κ.λπ., παρέχεται από πλαίσια μοντέλων, που αναπτύσσονται ως ανεξάρτητα έργα. Το OMNeT++ προσφέρει ένα IDE βασισμένο στο Eclipse, ένα γραφικό περιβάλλον εκτέλεσης και ένα πλήθος άλλων εργαλείων. Υπάρχουν επεκτάσεις για προσομοίωση σε πραγματικό χρόνο, εξομοίωση δικτύου, ενσωμάτωση βάσεων δεδομένων και πολλές άλλες λειτουργίες.



Εικόνα 7: OMneT++ GUI

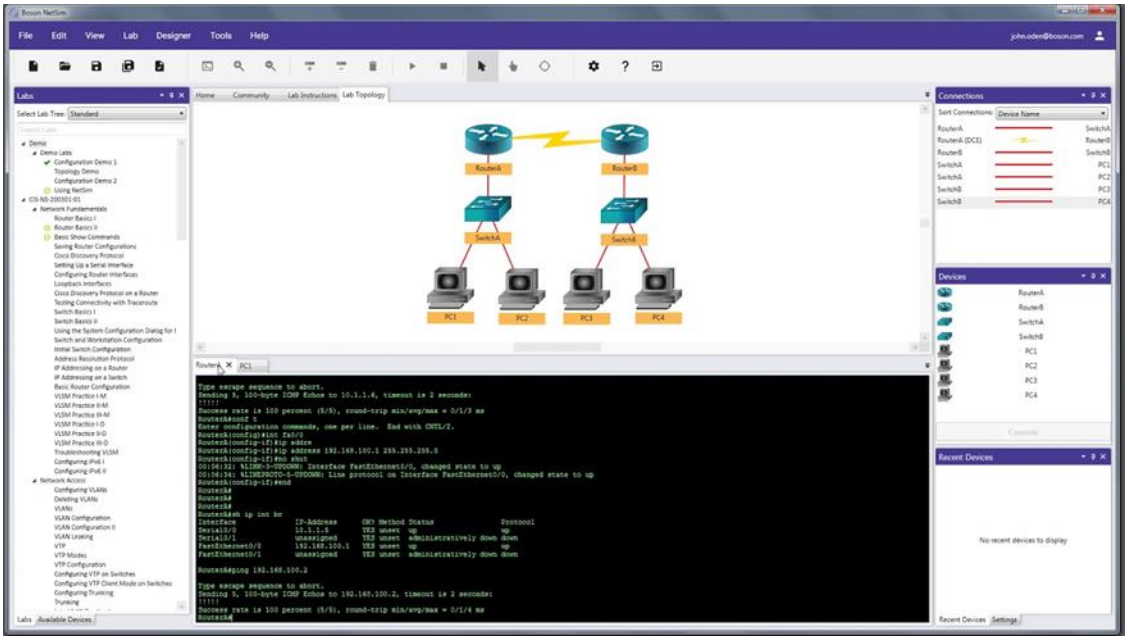
Παρόλο που το OMNeT++ δεν είναι από μόνος του ένας προσομοιωτής δικτύου, έχει αποκτήσει ευρεία δημοτικότητα ως πλατφόρμα προσομοίωσης δικτύων στην επιστημονική κοινότητα καθώς και σε βιομηχανικά περιβάλλοντα και έχει δημιουργήσει μια μεγάλη κοινότητα χρηστών.

Το OMNeT++ παρέχει μια αρχιτεκτονική στοιχείων (components) για μοντέλα. Τα components (modules) προγραμματίζονται σε C++ και στη συνέχεια συναρμολογούνται σε μεγαλύτερα στοιχεία και μοντέλα χρησιμοποιώντας μια γλώσσα υψηλού επιπέδου (NED). Η δυνατότητα επαναχρησιμοποίησης των μοντέλων παρέχεται δωρεάν. Το OMNeT++ διαθέτει εκτεταμένη υποστήριξη GUI, και λόγω της αρθρωτής αρχιτεκτονικής του, ο πυρήνας προσομοίωσης (και τα μοντέλα) μπορούν να ενσωματωθούν εύκολα στις εφαρμογές σας.

Κατά τη διάρκεια των ετών που το OMNeT++ είναι διαθέσιμο, αμέτρητα μοντέλα προσομοίωσης και πλαίσια μοντέλων έχουν γραφτεί για αυτό από ερευνητές σε διάφορους τομείς: ουρές αναμονής, μοντελοποίηση πόρων, πρωτόκολλα διαδικτύου, ασύρματα δίκτυα, switched LANs, peer-to-peer (P2P) δίκτυα, media streaming, κινητά ad-hoc δίκτυα, δίκτυα πλέγματος, ασύρματα δίκτυα αισθητήρων, δίκτυα οχημάτων, οπτικά δίκτυα, συστήματα HPC, υπολογιστικό νέφος και άλλα. Τα περισσότερα από αυτά τα πλαίσια μοντέλων είναι ανοικτού κώδικα, αναπτύσσονται ως ανεξάρτητα έργα και ακολουθούν τους δικούς τους κύκλους έκδοσης.

4.7 Boson NetSim

Το NetSim αποτελεί μία ιδιαίτερη λύση για την προετοιμασία των σπουδαστών για πιστοποιήσεις όπως το CCNA, ENCOR και ENARSI.



Εικόνα 8: Boson NetSim GUI

Ο πυρήνας του NetSim είναι ο σχεδιαστής δικτύου - ένα εργαλείο που επιτρέπει τη δημιουργία διαισθητικών τοπολογιών με ευκολία. Μεταξύ των πραγμάτων που επιτρέπει ο σχεδιαστής δικτύου είναι η ευθυγράμμιση στοιχείων, ο σχολιασμός τοπολογιών και ο εύκολος εντοπισμός ενεργών ή ανενεργών συνδέσεων [16].

Το NetSim επιτρέπει σε έναν σπουδαστή να μοιράζεται τα δικά του εργαστήρια, τα πακέτα εργαστηρίων και τις τοπολογίες δικτύου με άλλους σπουδαστές. Ομοίως, μπορεί να δει τα εργαστήρια και τις τοπολογίες άλλων χρηστών του NetSim, γεγονός που μπορεί να σας δώσει ένα πλεονέκτημα στην εκπαίδευση.

5 Παρουσίαση Σεναρίων Ασφάλειας

5.1 IPsec VPN Tunneling

5.1.1 Εισαγωγή

Το IPsec (Internet Protocol Security) είναι μια ομάδα πρωτοκόλλων που χρησιμοποιούνται μαζί για τη δημιουργία κρυπτογραφημένων συνδέσεων μεταξύ συσκευών και έχει κερδίσει τεράστια δημοτικότητα μεταξύ των υπηρεσιών VPN. Το IPsec είναι αλληλένδετο με τις απαρχές του Διαδικτύου και είναι το αποτέλεσμα των προσπαθειών για την ανάπτυξη μεθόδων κρυπτογράφησης στο επίπεδο IP στις αρχές της δεκαετίας του '90. Ως ανοιχτό πρωτόκολλο που υποστηρίζεται από συνεχή ανάπτυξη, έχει αποδείξει τις ιδιότητές του με την πάροδο των ετών και παρόλο που έχουν εμφανιστεί ανταγωνιστικά πρωτόκολλα, το IPsec διατηρεί τη θέση του ως το πιο ευρέως χρησιμοποιούμενο πρωτόκολλο VPN μαζί με το OpenVPN.

5.1.2 Τι είναι το IPsec

Το IPsec είναι μια σουίτα πρωτοκόλλων δικτύου που επιτρέπει την ασφαλή επικοινωνία μεταξύ δύο συσκευών μέσω δικτύων IP, τα οποία χρησιμοποιούνται σήμερα κυρίως στο δημόσιο διαδίκτυο. Είναι επίσης μια σουίτα πρωτοκόλλων δικτύου που εξασφαλίζει τόσο την κρυπτογράφηση πακέτων όσο και την αυθεντικοποίηση της πηγής [17].

Το IPsec είναι απόλυτα κατάλληλο για τη διασφάλιση του απορρήτου των επικοινωνιών δικτύου IP, γι' αυτό και χρησιμοποιείται συχνά για τη δημιουργία μιας σύνδεσης VPN από εργαλεία VPN IPsec. Σήμερα, το IPsec θεωρείται πρότυπο ασφάλειας λόγω της χρήσης ισχυρών (αδιάσπαστων) κρυπτογραφήσεων και αλγορίθμων, της πιστοποίησης ταυτότητας TLS, της προστασίας από επιθέσεις Man-in-the-Middle (MitM), του Perfect Forward Secrecy για ποικίλες εφαρμογές όπως:

- Εξασφάλιση ιδιωτικών επικοινωνιών δικτύου.
- Προστασία της διαδικτυακής κίνησης από κατασκοπεία ή υποκλοπές.
- Διασφάλιση της ακεραιότητας των πακέτων IP.

Πολλά routers διαθέτουν τουλάχιστον κάποια υλοποίηση των πρωτοκόλλων IPsec, όπως και τα περισσότερα λειτουργικά συστήματα.

5.1.3 Λειτουργία IPsec

Οι συνδέσεις IPsec περιλαμβάνουν τα ακόλουθα βήματα [18]:

- Key Exchange: Το κλειδί (key) είναι μια συμβολοσειρά τυχαίων χαρακτήρων που μπορεί να χρησιμοποιηθεί για το "κλείδωμα" (κρυπτογράφηση) και το "ξεκλείδωμα" (αποκρυπτογράφηση) των μηνυμάτων. Το IPsec δημιουργεί κλειδιά με ανταλλαγή κλειδιών μεταξύ των συνδεδεμένων συσκευών, έτσι ώστε κάθε συσκευή να μπορεί να αποκρυπτογραφήσει τα μηνύματα της άλλης συσκευής.
- Packet headers and trailers: Όλα τα δεδομένα που αποστέλλονται μέσω ενός δικτύου αναλύονται σε μικρότερα κομμάτια που ονομάζονται πακέτα. Τα πακέτα περιέχουν τόσο ωφέλιμο φορτίο (payload), δηλαδή τα πραγματικά δεδομένα που αποστέλλονται, όσο και επικεφαλίδες (headers), δηλαδή πληροφορίες σχετικά με τα δεδομένα αυτά, ώστε οι υπολογιστές που λαμβάνουν τα πακέτα να γνωρίζουν τι να κάνουν με αυτά. Το IPsec προσθέτει διάφορες επικεφαλίδες στα πακέτα δεδομένων που περιέχουν πληροφορίες ελέγχου ταυτότητας και κρυπτογράφησης. Προσθέτει επίσης trailers, τα οποία ακολουθούν το ωφέλιμο φορτίο κάθε πακέτου αντί να προηγούνται.

- Authentication: Το IPsec παρέχει αυθεντικοποίηση για κάθε πακέτο, όπως μια σφραγίδα γνησιότητας σε ένα συλλεκτικό αντικείμενο. Αυτό διασφαλίζει ότι τα πακέτα προέρχονται από αξιόπιστη πηγή και όχι από μη εξουσιοδοτημένο χρήστη.
- Encryption: Το IPsec κρυπτογραφεί τα ωφέλιμα φορτία μέσα σε κάθε πακέτο και την επικεφαλίδα IP κάθε πακέτου (εκτός εάν χρησιμοποιείται λειτουργία μεταφοράς αντί για λειτουργία tunneling). Αυτό διατηρεί τα δεδομένα που αποστέλλονται μέσω IPsec ασφαλή και ιδιωτικά.
- Transmission: Τα κρυπτογραφημένα πακέτα IPsec ταξιδεύουν σε ένα ή περισσότερα δίκτυα προς τον προορισμό τους χρησιμοποιώντας ένα πρωτόκολλο μεταφοράς. Σε αυτό το στάδιο, η κυκλοφορία IPsec διαφέρει από την κανονική κυκλοφορία IP στο ότι χρησιμοποιεί συχνότερα το UDP ως πρωτόκολλο μεταφοράς και όχι το TCP. Το TCP (Transmission Control Protocol) δημιουργεί αποκλειστικές συνδέσεις μεταξύ συσκευών και διασφαλίζει ότι όλα τα πακέτα φτάνουν. Το UDP (User Datagram Protocol) δεν δημιουργεί αυτές τις αποκλειστικές συνδέσεις. Το IPsec χρησιμοποιεί το UDP επειδή αυτό επιτρέπει στα πακέτα IPsec να περνούν μέσα από firewalls.
- Decryption: Στο άλλο άκρο της επικοινωνίας, τα πακέτα αποκρυπτογραφούνται και οι εφαρμογές (π.χ. ένα πρόγραμμα περιήγησης) μπορούν πλέον να χρησιμοποιήσουν τα παραδοθέντα δεδομένα.

5.1.4 Πρωτόκολλα που χρησιμοποιεί το IPSec

Είναι σημαντικό να κατανοήσουμε ότι το IPsec δεν είναι ένα ενιαίο πρωτόκολλο. Χρησιμοποιεί μια ομάδα πρωτοκόλλων ελέγχου ταυτότητας και κρυπτογράφησης για την εκτέλεση συγκεκριμένων εργασιών. Τα πιο σημαντικά από αυτά είναι

- Security Authentication Header (AH): Χρησιμεύει μόνο για τον έλεγχο ταυτότητας πακέτων (προέλευση, ακεραιότητα) και όχι για κρυπτογράφηση. Η επικεφαλίδα αυθεντικοποίησης (Authentication Header) ενθυλακώνει το πακέτο, διασφαλίζοντας την ακεραιότητα του πακέτου μέσω MD5/SHAxxx, και μετά από αυτό τα δεδομένα αποστέλλονται στο router του προορισμού. Μόλις παραληφθεί από router, το πακέτο αποκαψιλώνεται και ελέγχεται για πιθανές παραβιάσεις της ακεραιότητας. Δεν υπάρχει κρυπτογράφηση του payload κατά τη διαδικασία, γεγονός που περιορίζει τη χρήση αυτού του πρωτοκόλλου. Το AH χρησιμοποιείται συνήθως στη λειτουργία μεταφοράς IPsec.
- Encapsulating Security Payload (ESP): Ομοίως με το Security Authentication Header, το ESP είναι ένα μέρος της σουίτας πρωτοκόλλων του IPsec που είναι υπεύθυνο για την ακεραιότητα των δεδομένων, μόνο για το payload και επιπλέον για την κρυπτογράφηση του. Η επικεφαλίδα IP του πακέτου ESP δεν κρυπτογραφείται και η ακεραιότητά της δεν προστατεύεται, ώστε να μπορεί να αλλάξει κατά τη διάρκεια της μεταφοράς, γεγονός που επιτρέπει την επιτυχή διάσχιση του NAT (Network Address Translation). Το ESP χρησιμοποιείται συνήθως σε λειτουργία tunneling.
- Internet Security Association and Key Management Protocol (ISAKMP): Το ISAKMP είναι ένα πρωτόκολλο που χρησιμοποιείται για τη δημιουργία σύνδεσης ασφαλείας (SA). Η διαδικασία αυτή περιλαμβάνει δύο βήματα:
    - Στο πρώτο βήμα εγκαθιστά το tunnel IKE SA, ένα αμφίδρομη tunnel διαχείρισης για την ανταλλαγή κλειδιών. Μόλις εγκαθιδρυθεί η επικοινωνία, στο δεύτερο βήμα εγκαθιδρύονται κανάλια IPSEC SA για ασφαλή μεταφορά δεδομένων. Τα χαρακτηριστικά αυτού του μονόδρομου tunnel IPsec VPN, όπως η κρυπτογράφηση, η μέθοδος ή το κλειδί που θα χρησιμοποιηθεί, είχαν συμφωνηθεί εκ των προτέρων και από τους δύο κεντρικούς υπολογιστές (στην περίπτωση του IPsec VPN, πρόκειται για μια σύνδεση μεταξύ μιας πύλης και ενός υπολογιστή).

- Για κάθε tunnel IPsec VPN στη φάση 2, πρέπει να δημιουργηθούν δύο ξεχωριστές IPSEC SA, μία για την εισερχόμενη (IN) και μία για την εξερχόμενη (OUT) κίνηση. Η πιο συχνά χρησιμοποιούμενη διαμόρφωση ISAKMP είναι η χειροκίνητη (προ-διαμοιραζόμενα κλειδιά, PSK) και η δυναμική (IKEv1, IKEv2).

5.1.5 Διαφορές μεταξύ λειτουργιών Tunneling και Transport του IPsec

Υπάρχουν δύο λειτουργίες στις οποίες μπορεί να ρυθμιστεί η λειτουργία του IPsec [19]:

- Η λειτουργία IPsec tunneling κρυπτογραφεί και πιστοποιεί ολόκληρο το πακέτο δεδομένων. Το πακέτο ενθυλακώνεται σε ένα άλλο, ώστε να είναι επιλέξιμο για την αλλαγή μιας επικεφαλίδας IP. Μια τέτοια διαδικασία συνεπάγεται τη δυνατότητα αλλαγών στη δρομολόγηση, την υπέρβαση του NAT και την επιτυχή διέλευση δεδομένων από έναν υπολογιστή πίσω από το δρομολογητή μέσω του δημόσιου διαδικτύου στον προορισμό τους (για παράδειγμα έναν άλλο υπολογιστή πίσω από έναν διαφορετικό δρομολογητή). Ένα IPsec VPN tunnel επιτρέπει τη δημιουργία VPN (τόσο site-to-site VPN όσο και VPN απομακρυσμένης πρόσβασης) και χρησιμοποιείται πολύ συχνότερα από τη λειτουργία διαμετακόμισης (transit mode).
- Η λειτουργία IPsec Transport κρυπτογραφεί μόνο το payload του πακέτου δεδομένων. Η επικεφαλίδα IP δεν υπόκειται σε αλλαγές, οπότε δεν είναι δυνατές αλλαγές στη δρομολόγηση. Αυτός ο περιορισμός καθορίζει ότι η λειτουργία μεταφοράς IPsec πρέπει να χρησιμοποιείται μόνο για επικοινωνία από άκρο σε άκρο. Και τα δύο άκρα πρέπει να βλέπουν το ένα το άλλο, οπότε μπορεί να χρησιμοποιηθεί για κρυπτογράφηση εντός ενός ήδη εγκατεστημένου GRE tunnel.

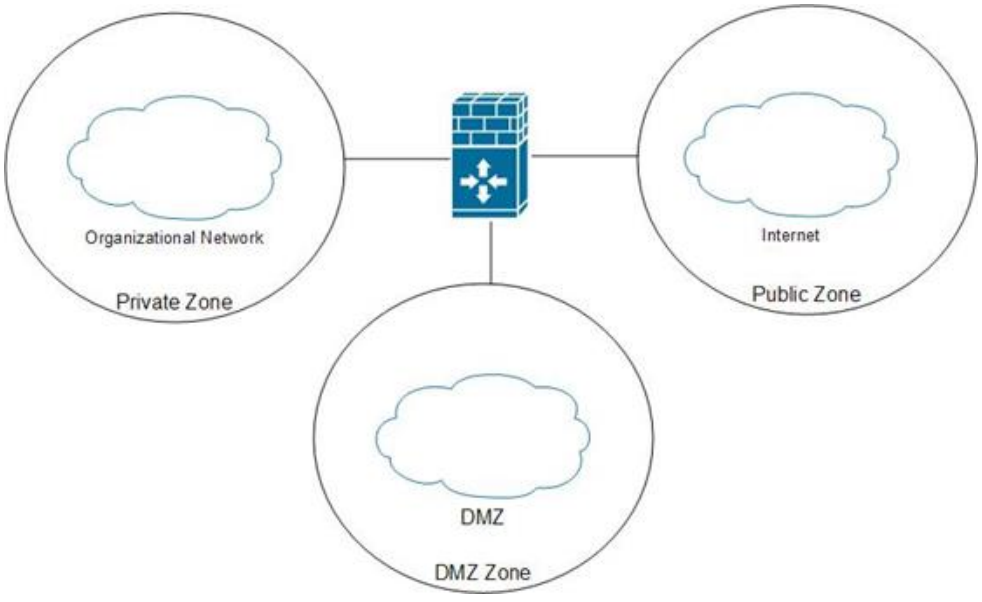
5.2 Zone-Based Policy Firewall

Η υλοποίηση ενός τείχους προστασίας (firewall) με υλοποίηση Zone-Based Policy (ZBF) είναι ότι η διαμόρφωσή του διαφέρει από τις παραδοσιακές διαμορφώσεις firewall (Context-Based Access Control - CBAC) που χρησιμοποιούνταν στο παρελθόν. Στις προηγούμενες διαμορφώσεις firewall, κάθε διασύνδεση διαμορφωνόταν ξεχωριστά με μια συγκεκριμένη πολιτική που λειτουργούσε σε συνδυασμό με μια λίστα πρόσβασης. Η κυκλοφορία επιθεωρούνταν για ειδικά διαμορφωμένα πρωτόκολλα και επιτρεπόταν με βάση τη διαμόρφωση. Ένα από τα κύρια προβλήματα που αντιμετώπιζαν οι μηχανικοί με το CBAC ήταν ότι απαιτούσε την εισαγωγή μεγάλου αριθμού εντολών διαμόρφωσης σε κάθε σχετική διασύνδεση, πράγμα που έκανε τη διαμόρφωση χρονοβόρα και τις μικρές τροποποιήσεις εξίσου χρονοβόρες [20].

Με μια λύση τείχους προστασίας που βασίζεται σε ζώνες, δημιουργούνται ζώνες για κάθε τμήμα του δικτύου που απαιτεί διαφορετικές πολιτικές ελέγχου πρόσβασης/κυκλοφορίας. Η πιο συνηθισμένη διαμόρφωση αυτών είναι να υπάρχουν ιδιωτικές (internal), δημόσιες (external) και DMZ ("αποστρατιωτικοποιημένες" ή ουδέτερες) ζώνες. Η ιδιωτική ζώνη είναι για τις διεπαφές που δρομολογούν την κυκλοφορία προς το εσωτερικό του οργανωτικού δικτύου, η δημόσια ζώνη είναι για τις διεπαφές με κυκλοφορία που κατευθύνεται προς ένα δημόσιο δίκτυο (παραδείγματος χάρει το Διαδίκτυο) και η ζώνη DMZ (εάν χρειάζεται) είναι για τις διεπαφές με κυκλοφορία που κατευθύνεται προς μια DMZ (public web και mail servers). Κατά τη υλοποίηση αυτής της διαμόρφωσης, οι διασυνδέσεις στο router μπορούν να είναι μέρος μόνο μιας ζώνης κάθε φορά. Φυσικά, ο αριθμός των ζωνών δεν περιορίζεται σε αυτό το παράδειγμα διαμόρφωσης [21].

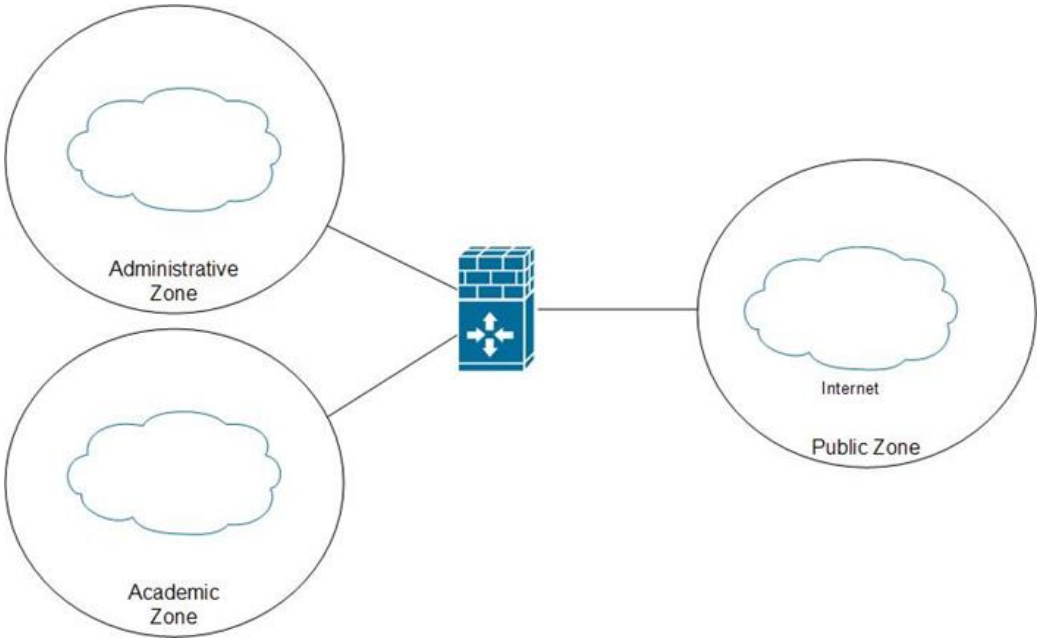
Για την καλύτερη κατανόηση των εννοιών αυτών, παρακάτω παρουσιάζονται αναλυτικά κάποια παραδείγματα.

Όπως αναφέρθηκε παραπάνω, οι περισσότερες διαμορφώσεις ζωνών χρησιμοποιούν δημόσιες, ιδιωτικές και DMZ ζώνες. Στην παρακάτω εικόνα παρουσιάζεται ένα παράδειγμα αυτής της διαμόρφωσης:



Σχήμα 1: Παράδειγμα διαμόρφωσης ζωνών με DMZ

Ένα άλλο κοινό παράδειγμα χρησιμοποιείται όταν υπάρχουν πολλαπλές διοικητικές περιοχές μέσα σε έναν οργανισμό. Για παράδειγμα, σε ένα πανεπιστημιακό περιβάλλον, υπάρχουν συσκευές που χρησιμοποιούνται κυρίως για τη διοίκηση και συσκευές που χρησιμοποιούνται κυρίως για ακαδημαϊκούς σκοπούς. Προκειμένου να προστατευθούν οι συσκευές διαχείρισης από τις ακαδημαϊκές συσκευές, μπορούν να δημιουργηθούν ξεχωριστές ζώνες. Ένα παράδειγμα αυτής της διαμόρφωσης ζώνης παρουσιάζεται στην επόμενη εικόνα:



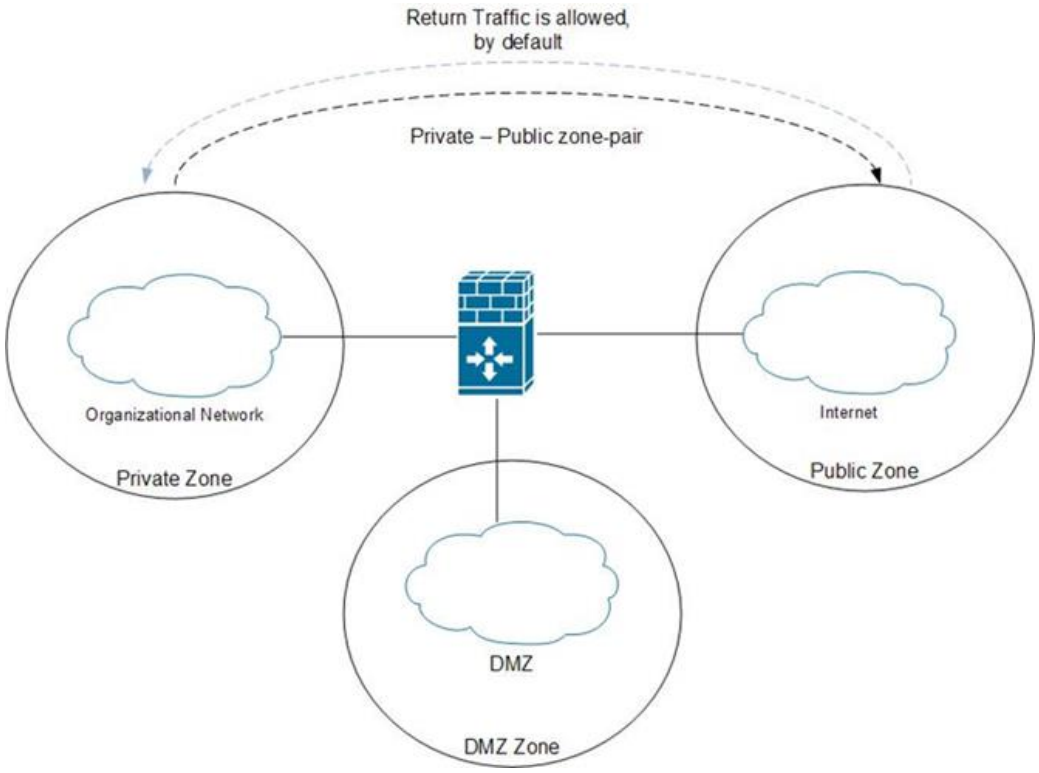
Σχήμα 2: Παράδειγμα διαμόρφωσης ζωνών με δύο εσωτερικές ζώνες

Κατά τη διαμόρφωση της πρόσβασης και της πολιτικής μεταξύ των ζωνών, δημιουργούνται ζεύγη ζωνών για τη σύνδεση μιας ζώνης με μια άλλη. Αυτά τα ζεύγη ζωνών είναι μονής κατεύθυνσης και ρυθμίζονται με μια συγκεκριμένη πολιτική κυκλοφορίας που χρησιμοποιείται όταν η κυκλοφορία περνάει από τη ζώνη προέλευσης στη ζώνη προορισμού. Εάν η κυκλοφορία πρέπει να διέρχεται μεταξύ δύο ζωνών και προς τις δύο κατευθύνσεις, τότε πρέπει να διαμορφωθούν δύο ξεχωριστά ζεύγη ζωνών.

Από προεπιλογή, όλη η κυκλοφορία που διακινείται μέσω του router, από οποιαδήποτε ζώνη πηγής ή προορισμού, απορρίπτεται. Υπάρχουν δύο εξαιρέσεις σε αυτόν τον προεπιλεγμένο κανόνα:

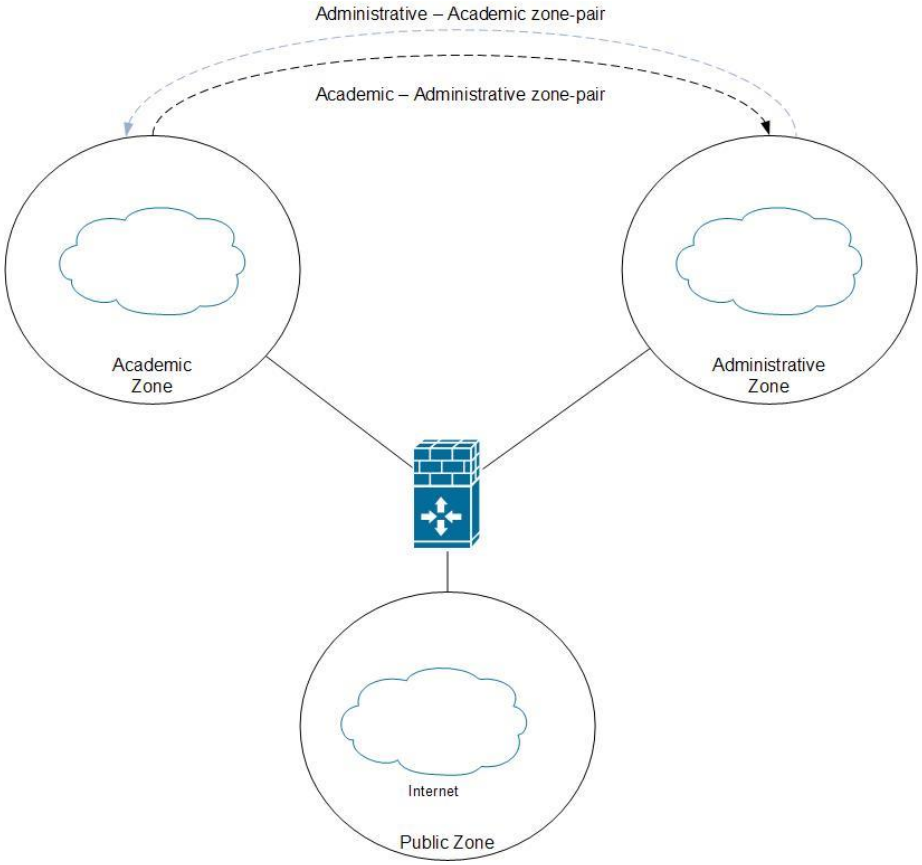
- Όταν η κυκλοφορία έχει πηγή και προορισμό σε διασυνδέσεις στην ίδια ζώνη.
- Όταν η κυκλοφορία έχει πηγή ή προορισμό τον ίδιο το δρομολογητή.

Χρησιμοποιώντας το πρώτο παραπάνω παράδειγμα, μπορεί να δημιουργηθεί ένα ζεύγος ζωνών μεταξύ της ιδιωτικής και της δημόσιας ζώνης. Σε μια κατάσταση όπως αυτή, όπου υπό κανονικές συνθήκες η δημόσια ζώνη δεν θα πρέπει ποτέ να μπορεί να έρθει σε άμεση επαφή με μια συσκευή στην ιδιωτική ζώνη, μπορεί να χρησιμοποιηθεί ένα άλλο χαρακτηριστικό της διαμόρφωσης firewall με βάση τη ζώνη. Σε αυτή την περίπτωση, η ιδιωτική ζώνη πρέπει να έχει πρόσβαση στη δημόσια ζώνη, αλλά όχι το αντίστροφο. Τα ζεύγη ζωνών, από προεπιλογή, θα επιτρέπουν όλη την κυκλοφορία επιστροφής. Σε αυτή την περίπτωση, απαιτείται μόνο η διαμόρφωση ενός ζεύγους ζωνών, όπως φαίνεται στην παρακάτω εικόνα:



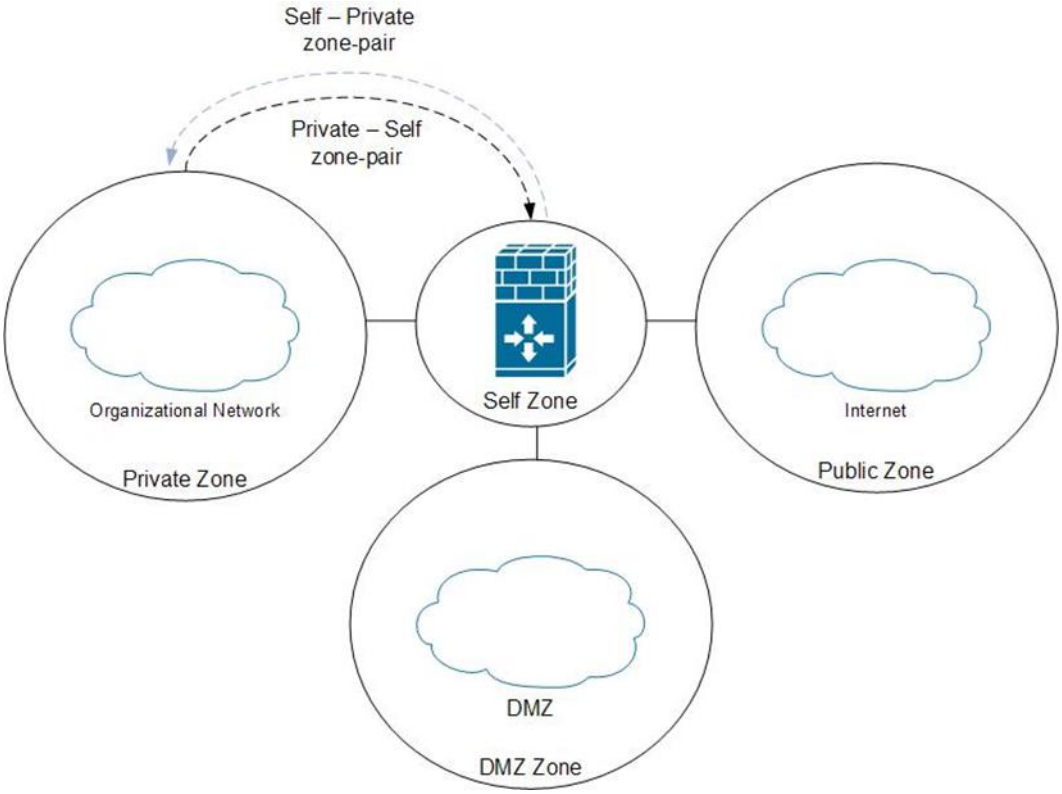
Σχήμα 3: Παράδειγμα διαμόρφωσης ζεύγους ζωνών

Σε μια κατάσταση όπως φαίνεται στο δεύτερο σχήμα, μπορεί να απαιτείται η διαμόρφωση δύο ζευγών ζωνών μεταξύ της διοικητικής και της ακαδημαϊκής ζώνης, εάν η κυκλοφορία προέρχεται και προορίζεται ανεξάρτητα και από τις δύο πλευρές, όπως παρουσιάζεται στο παρακάτω σχήμα:



Σχήμα 4: Παράδειγμα διαμόρφωσης 2 εσωτερικών ζωνών

Η άλλη εξαίρεση στον προεπιλεγμένο κανόνα απόρριψης είναι όταν η κυκλοφορία προορίζεται για τον ίδιο το δρομολογητή, γεγονός που συνήθως πρόκειται για κυκλοφορία στο επίπεδο ελέγχου και διαχείρισης. Από προεπιλογή, όλη η κυκλοφορία από και προς τον ίδιο το δρομολογητή περνάει. Για να ελέγξετε την κυκλοφορία που επιτρέπεται να εισέρχεται ή να εξέρχεται απευθείας από το δρομολογητή, μπορεί να χρησιμοποιηθεί η αυτό-ζώνη (self-zone) που ορίζεται από το σύστημα. Στην παρακάτω εικόνα παρουσιάζεται ένα παράδειγμα ζεύγους ζωνών μεταξύ της ιδιωτικής και της αυτό-ζώνης:



Σχήμα 5: Παράδειγμα ζεύγους ζωνών μεταξύ ιδιωτικής και αυτο-ζώνης

Το τελευταίο από τα βασικά θεμελιώδη στοιχεία που πρέπει να γίνει κατανοητό είναι ο τρόπος με τον οποίο ένα τείχος προστασίας με βάση τη ζώνη αλληλεπιδρά με την υπάρχουσα λίστα ελέγχου πρόσβασης (Access Contol List - ACL). Καθώς οι ACL δεν χρησιμοποιούνται στη διαμόρφωση ενός firewall με βάση τη ζώνη, είναι σημαντικό να σημειωθεί ότι όταν συνυπάρχουν σε μια διασύνδεση που έχει επίσης ρυθμιστεί ως μέρος μιας ζώνης, η ACL θα λαμβάνεται πάντα υπόψη πριν από οποιαδήποτε από τις πολιτικές τείχους προστασίας με βάση τη ζώνη. Οι υπάρχουσες ACL πρέπει να ρυθμιστούν ώστε να επιτρέπουν τη διέλευση κάποιας κυκλοφορίας προκειμένου να ληφθεί υπόψη η πολιτική που βασίζεται στη ζώνη.

5.3 IP Access-Control-Lists

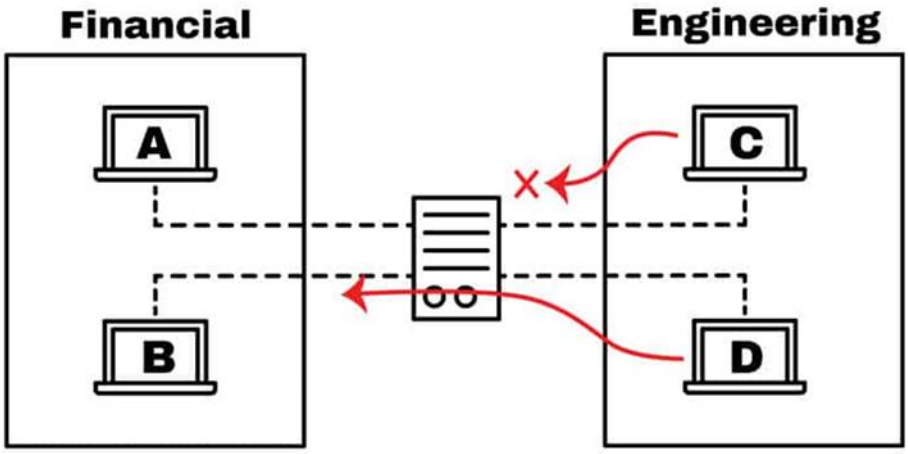
5.3.1 Εισαγωγή

Στον κόσμο των δικτύων υπολογιστών, η λίστα ελέγχου πρόσβασης (Access-Control-List – ACL) είναι ένα από τα πιο θεμελιώδη στοιχεία της ασφάλειας. Μια λίστα ελέγχου πρόσβασης "ACL" είναι μια λειτουργία που παρακολουθεί την εισερχόμενη και εξερχόμενη κυκλοφορία και τη συγκρίνει με ένα σύνολο καθορισμένων δηλώσεων. Είναι φίλτρα κυκλοφορίας δικτύου που μπορούν να ελέγχουν την εισερχόμενη ή εξερχόμενη κυκλοφορία. Οι ACLs λειτουργούν με βάση ένα σύνολο κανόνων που καθορίζουν τον τρόπο προώθησης ή αποκλεισμού ενός πακέτου στη διασύνδεση του δρομολογητή. Επίσης, είναι το ίδιο με ένα Stateless Firewall, το οποίο περιορίζει, μπλοκάρει ή επιτρέπει μόνο τα πακέτα που ρέουν από την πηγή στον προορισμό.

Όταν ορίζετε μία ACL σε μια συσκευή δρομολόγησης για μια συγκεκριμένη διασύνδεση, όλη η κυκλοφορία που ρέει μέσω αυτής θα συγκρίνεται με τη δήλωση ACL, η οποία είτε θα την εμποδίζει είτε θα την επιτρέπει. Τα κριτήρια για τον ορισμό των κανόνων ACL θα μπορούσαν να είναι η πηγή, ο προορισμός, ένα συγκεκριμένο πρωτόκολλο ή περισσότερες πληροφορίες. Τα ACL είναι κοινά στα routers ή στα firewalls, αλλά μπορούν επίσης να τα ρυθμίσουν σε οποιαδήποτε συσκευή που εκτελείται στο δίκτυο, όπως hosts, συσκευές δικτύου και διακομιστές.

5.3.2 Χρησιμότητα Λιστών Ελέγχου Πρόσβασης (ACL)

Η κύρια ιδέα της χρήσης μίας ACL είναι να παρέχει ασφάλεια στο δίκτυο. Χωρίς αυτήν, οποιαδήποτε κίνηση επιτρέπεται είτε να εισέλθει είτε να εξέλθει, καθιστώντας το πιο ευάλωτο σε ανεπιθύμητη και επικίνδυνη κίνηση [22]. Για να βελτιωθεί το επίπεδο ασφάλειας με μία ACL ένας μηχανικός μπορεί, για παράδειγμα, να αρνηθεί συγκεκριμένες ενημερώσεις δρομολόγησης ή να παρέχει έλεγχο ροής κίνησης. Όπως φαίνεται στην παρακάτω εικόνα, η συσκευή δρομολόγησης διαθέτει μία ACL που αρνείται την πρόσβαση του host C στο οικονομικό δίκτυο και ταυτόχρονα επιτρέπει την πρόσβαση στον host D.



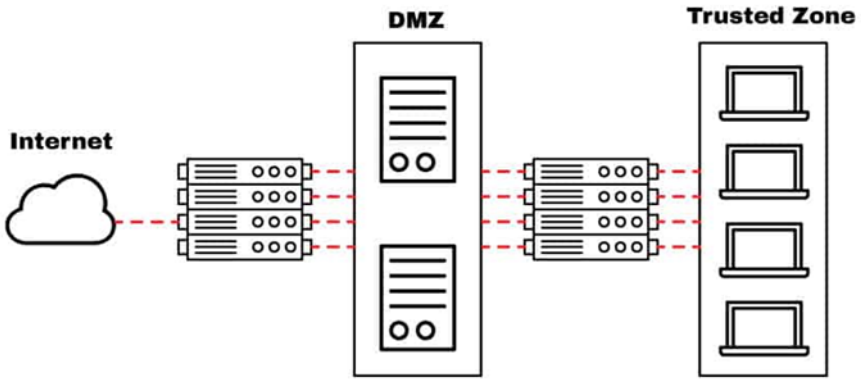
Σχήμα 6: Παράδειγμα δρομολόγησης με χρήση ACL

Με μία ACL μπορούμε να φιλτράρουμε πακέτα για μία ή περισσότερες διευθύνσεις IP ή διαφορετικά πρωτόκολλα, όπως TCP ή UDP. Έτσι, για παράδειγμα, αντί να μπλοκάρεται μόνο ένας κεντρικός υπολογιστής της ομάδας μηχανικών, μπορούμε να αρνηθούμε την πρόσβαση σε ολόκληρο το δίκτυο και να επιτρέψουμε μόνο σε ένα. Ή μπορείτε επίσης να περιορίσετε την πρόσβαση στον κεντρικό υπολογιστή C. Εάν ο μηχανικός από τον κεντρικό υπολογιστή C, πρέπει να έχει πρόσβαση σε έναν διακομιστή ιστού που βρίσκεται στο οικονομικό δίκτυο, μπορείτε να επιτρέψετε μόνο τη θύρα 80 και να αποκλείσετε όλα τα υπόλοιπα.

5.3.3 Που εφαρμόζονται οι ACLs

Οι συσκευές που αντιμετωπίζουν άγνωστα εξωτερικά δίκτυα, όπως το Διαδίκτυο, πρέπει να έχουν έναν τρόπο να φιλτράρουν την κυκλοφορία. Έτσι, ένα από τα καλύτερα μέρη για να ρυθμιστεί μία ACL είναι στα δρομολογητές άκρων (edge routers) [23]. Μια συσκευή δρομολόγησης με μια ACL μπορεί να τοποθετηθεί απέναντι από το Διαδίκτυο και να συνδέει το DMZ, η οποία είναι μια ζώνη απομόνωσης που χωρίζει το δημόσιο Διαδίκτυο και το ιδιωτικό δίκτυο. Η DMZ προορίζεται για servers που χρειάζονται πρόσβαση από το εξωτερικό δίκτυο, όπως Web servers, application servers, DNS servers και VPN.

Όπως φαίνεται στο παρακάτω σχήμα, ο σχεδιασμός δείχνει μια DMZ που χωρίζεται από δύο συσκευές, μία που χωρίζει την αξιόπιστη ζώνη από την DMZ και μία άλλη που τη χωρίζει με το διαδίκτυο.



Σχήμα 7: Παράδειγμα σχεδιασμού με DMZ

Τα routers που βλέπουν στο διαδίκτυο λειτουργούν ως πύλη για όλα τα εξωτερικά δίκτυα. Παρέχουν γενική ασφάλεια εμποδίζοντας μεγαλύτερα υποδίκτυα να βγουν ή να μπουν. Μια ACL μπορεί επίσης να ρυθμιστεί σε αυτό το router για να προστατεύσει από συγκεκριμένες γνωστές θύρες (TCP ή UDP). Ο εσωτερικός router, που βρίσκεται μεταξύ της DMZ και της αξιόπιστης ζώνης, μπορεί να ρυθμιστεί με πιο περιοριστικούς κανόνες για την προστασία του εσωτερικού δικτύου. Ωστόσο, αυτό είναι ένα εξαιρετικό μέρος για να επιλεγεί ένα τείχος Stateful Firewall αντί για μια ACL.

Οι ACL ρυθμίζονται απευθείας στο υλικό προώθησης μιας συσκευής, οπότε δεν θέτουν σε κίνδυνο την τελική απόδοση. Η τοποθέτηση ενός stateful firewall για την προστασία μιας DMZ μπορεί να θέσει σε κίνδυνο την απόδοση του δικτύου σας. Η επιλογή ενός router ACL για την προστασία περιουσιακών στοιχείων υψηλής απόδοσης, όπως applications ή servers, μπορεί να είναι μια καλύτερη επιλογή. Παρόλο που οι ACL μπορεί να μην παρέχουν

το επίπεδο ασφάλειας που προσφέρει ένα stateful firewall, είναι βέλτιστες για τα τελικά σημεία του δικτύου που χρειάζονται υψηλή ταχύτητα και απαραίτητη προστασία.

5.3.4 Συστατικά Μέρη μίας ACL

Η υλοποίηση των ACLs είναι αρκετά παρόμοια στις περισσότερες πλατφόρμες δρομολόγησης, οι οποίες έχουν γενικές οδηγίες για τη διαμόρφωσή τους. Υπενθυμίζεται ότι μία ACL είναι ένα σύνολο κανόνων ή καταχωρίσεων. Μπορούμε να έχουμε μία ACL με μία ή πολλές καταχωρήσεις, όπου η κάθε μία έχει ένα ρόλο, μπορεί να είναι να επιτρέπει τα πάντα ή να μην εμποδίζει τίποτα [24].

Για να οριστεί μια καταχώρηση ACL, χρειάζονται οι απαραίτητες πληροφορίες.

- Sequence Number: Προσδιορίζει μια καταχώρηση ACL χρησιμοποιώντας έναν αριθμό.
- ACL Name: Ορίζει μια καταχώρηση ACL χρησιμοποιώντας ένα όνομα. Αντί να χρησιμοποιηθεί μια ακολουθία αριθμών, ορισμένοι δρομολογητές επιτρέπουν συνδυασμό γραμμάτων και αριθμών.
- Remark: Ορισμένοι δρομολογητές επιτρέπουν την προσθήκη σχολίων σε μια ACL, τα οποία μπορούν να βοηθήσουν στην προσθήκη λεπτομερών περιγραφών.
- Statement: Απαγόρευση ή έγκριση μιας συγκεκριμένης πηγής με βάση τη διεύθυνση και τη wildcard mask. Ορισμένες συσκευές δρομολόγησης, όπως η Cisco, ρυθμίζουν από προεπιλογή μια έμμεση δήλωση άρνησης στο τέλος κάθε ACL.
- Network Protocol: Καθορίζει την άρνηση/απδοχή IP, IPX, ICMP, TCP, UDP, NetBIOS και άλλα.
- Source or Destination: Καθορίζει την πηγή ή τον προορισμό ως μια μεμονωμένη IP, μια περιοχή διευθύνσεων (CIDR) ή όλες τις διευθύνσεις.
- Log: Ορισμένες συσκευές έχουν τη δυνατότητα να τηρούν αρχεία καταγραφής όταν εντοπίζονται αντιστοιχίες ACL.
- Άλλα κριτήρια: Οι προηγμένες ACL επιτρέπουν τη χρησιμοποίηση ελέγχου της κυκλοφορίας μέσω του Τύπου υπηρεσίας (ToS), της προτεραιότητας IP και της προτεραιότητας κωδικοποιημένων υπηρεσιών διαφοροποίησης (DSCP).

5.3.5 Διαφορετικοί Τύποι ACL

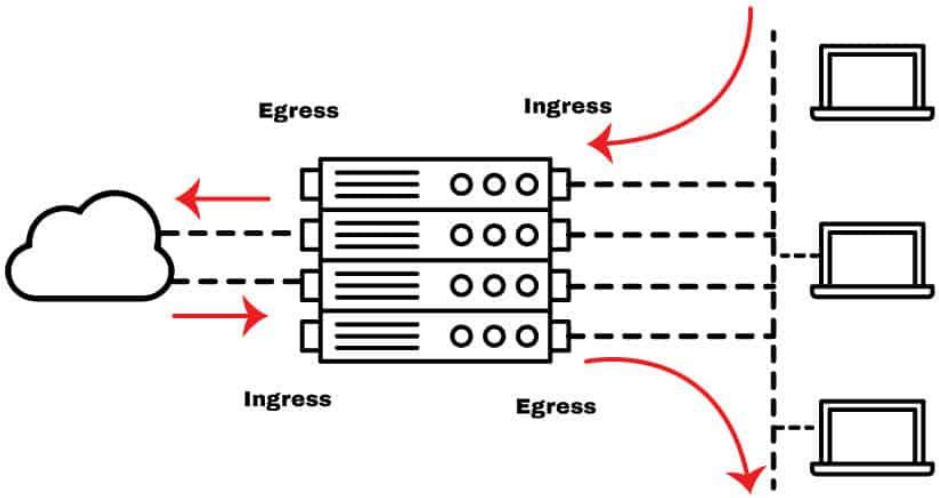
Υπάρχουν τέσσερις διαφορετικοί τύποι ACL, οι οποίοι χρησιμοποιούνται για διαφορετικούς σκοπούς:

- Standard ACL: Οι τυπικές (Standard) ACL στοχεύουν στην προστασία ενός δικτύου χρησιμοποιώντας μόνο τη διεύθυνση προέλευσης. Είναι ο πιο βασικός τύπος και μπορεί να χρησιμοποιηθεί για απλές εγκαταστάσεις, αλλά δυστυχώς δεν παρέχει ισχυρή ασφάλεια.
- Extended ACL: Με τις διευρυμένες (Extended) ACL, μπορεί επίσης να αποκλειστεί η πηγή και ο προορισμό για μεμονωμένους υπολογιστές ή ολόκληρα δίκτυα. Δίνεται η ευκαιρία επίσης να χρησιμοποιηθεί μία εκτεταμένη ACL για να φιλτραριστεί η κυκλοφορία με βάση πληροφορίες πρωτοκόλλου (IP, ICMP, TCP, UDP).
- Dynamic ACL: Οι δυναμικές (Dynamic) ACL, βασίζονται σε εκτεταμένες ACL, στο πρωτόκολλο Telnet και στην αυθεντικοποίηση. Αυτός ο τύπος ACL αναφέρεται συχνά ως "Lock and Key" και μπορεί να χρησιμοποιηθεί για συγκεκριμένα χρονικά πλαίσια. Επίσης επιτρέπουν την πρόσβαση ενός χρήστη σε μια πηγή ή έναν προορισμό μόνο εάν ο χρήστης αυθεντικοποιηθεί στη συσκευή μέσω Telnet.
- Reflexive ACL: Οι αντανακλαστικές (Reflexive) ACL αναφέρονται επίσης ως ACL IP session. Αυτού του τύπου οι ACLs, φιλτράρουν την κυκλοφορία με βάση τις πληροφορίες συνόδου ανώτερου επιπέδου. Αντιδρούν στις συνόδους που

προέρχονται μέσα στο router για να επιτρέψουν την εξερχόμενη κυκλοφορία ή να περιορίσουν την εισερχόμενη κυκλοφορία. Το router αναγνωρίζει την εξερχόμενη ACL και δημιουργεί μια νέα καταχώρηση ACL για την εισερχόμενη. Όταν το session ολοκληρώνεται, η καταχώρηση αφαιρείται.

5.3.6 Εφαρμογή μίας ACL

Η κατανόηση της εισερχόμενης και εξερχόμενης κυκλοφορίας (ή εισερχόμενης και εξερχόμενης) σε ένα router είναι ζωτικής σημασίας για τη σωστή εφαρμογή μίας ACL. Κατά τον καθορισμό κανόνων για μία ACL, όλες οι ροές κυκλοφορίας βασίζονται στην οπτική γωνία της διασύνδεσης του router (όχι των άλλων δικτύων). Όπως παρουσιάζεται στο παρακάτω σχήμα, η εισερχόμενη κυκλοφορία είναι η ροή που έρχεται από ένα δίκτυο, είτε είναι εξωτερικό είτε εσωτερικό, στη διασύνδεση του δρομολογητή. Η κίνηση εξόδου, από την άλλη πλευρά, είναι η ροή από τη διασύνδεση που βγαίνει προς ένα δίκτυο.



Σχήμα 8: Παράδειγμα εισερχόμενης και εξερχόμενης κίνησης

Για να δημιουργηθεί μια ACL, αρκεί να εφαρμοστεί στη διασύνδεση ενός router. Δεδομένου ότι όλες οι αποφάσεις δρομολόγησης και προώθησης λαμβάνονται από το υλικό του router, οι δηλώσεις ACL μπορούν να εκτελεστούν πολύ πιο γρήγορα. Όταν δημιουργηθεί μια καταχώρηση ACL, η διεύθυνση προέλευσης πηγαίνει πρώτη και ο προορισμός ακολουθεί. Στο παράδειγμα της διευρυμένης διαμόρφωσης ACL για IP σε έναν δρομολογητή Cisco, όταν δημιουργηθεί ένας κανόνας Deny/Permit, πρέπει πρώτα να οριστεί η πηγή και μετά η IP προορισμού. Η εισερχόμενη ροή είναι η πηγή όλων των κεντρικών υπολογιστών ή του δικτύου, και η εξερχόμενη είναι ο προορισμός όλων των κεντρικών υπολογιστών και των δικτύων.

5.4 Intrusion Prevention Systems (IPS)

5.4.1 Εισαγωγή

Οι διαχειριστές δικτύων πρέπει να χρησιμοποιούν εργαλεία για να προστατεύουν το δίκτυό τους και να αποτρέπουν την πρόσβαση κακόβουλων παραγόντων. Τα συστήματα ανίχνευσης εισβολών (Intrusion Detection Systems - IDS) και τα συστήματα πρόληψης εισβολών (Pntrusion Prevention Systems - IPS) είναι κατηγορίες εργαλείων που χρησιμοποιούνται συνήθως για το σκοπό αυτό [25].

5.4.2 Διαφορές μεταξύ IDS και IPS

Το IDS είναι κατά βάση ένα σύστημα ειδοποίησης που ενημερώνει έναν οργανισμό εάν εντοπιστεί ανώμαλη ή κακόβουλη δραστηριότητα. Το IPS προχωράει ένα βήμα μπροστά και κλείνει το δίκτυο πριν από την απόκτηση πρόσβασης ή για να αποτρέψει την περαιτέρω κίνηση σε αυτό.

5.4.3 Τύποι IDS και Τύπου Ανιχνεύσεων τους

Υπάρχουν δύο τύποι ανιχνεύσεων του IDS [26]:

- Signature-based detection: Οι λύσεις IDS που βασίζονται στα signatures (υπογραφές) ειδοποιούν τους διαχειριστές με βάση τα προϋπάρχοντα signatures που αναφέρονται σε έναν τύπο επίθεσης ή κακόβουλης συμπεριφοράς. Αυτό επιτρέπει την ακριβή και αυτοματοποιημένη ειδοποίηση, επειδή το σύστημα παραπέμπει σε μια υπάρχουσα βάση δεδομένων υπογραφών. Αυτό το είδος συστήματος συχνά αναζητά δείκτες συμβιβασμού (indicators of compromise), όπως η σάρωση κατακερματισμών αρχείων, η κυκλοφορία που πηγαίνει σε γνωστούς κακόβουλους τομείς, κακόβουλες ακολουθίες byte, ακόμη και γραμμές θέματος ηλεκτρονικού ταχυδρομείου που αποτελούν γνωστές επιθέσεις phishing.
- Anomaly-based detection: Οι λύσεις IDS που βασίζονται σε ανωμαλίες θεωρούνται πιο αποτελεσματικές από τις λύσεις που βασίζονται σε υπογραφές, επειδή παρακολουθούν κακόβουλα ή ύποπτα μοτίβα συμπεριφοράς. Αυτό τους επιτρέπει να ανιχνεύουν νέα είδη απειλών, κάτι που είναι σχεδόν αδύνατο για τα συστήματα που βασίζονται σε υπογραφές. Η ανίχνευση με βάση τις ανωμαλίες συχνά αναζητά συμπεριφορά που διαφέρει από μια καθιερωμένη βασική γραμμή. Για παράδειγμα, αν έχουν οριστεί κανονικές ώρες εργασίας για τους υπαλλήλους, ένα IDS που βασίζεται σε ανωμαλίες μπορεί να επισημάνει μια σύνδεση που πραγματοποιείται το Σαββατοκύριακο. Το σύστημα μπορεί επίσης να ειδοποιήσει με βάση τον όγκο της κυκλοφορίας που συνδέεται στο δίκτυό ή την προσθήκη νέων συσκευών χωρίς τη σωστή εξουσιοδότηση.

Οι πέντε τύποι IDS είναι:

- Network Intrusion Detection Systems (NIDS): Ένα σύστημα ανίχνευσης εισβολής στο δίκτυο θα παρακολουθεί την κυκλοφορία μέσω διαφόρων αισθητήρων, που τοποθετούνται είτε μέσω υλικού είτε μέσω λογισμικού, στο ίδιο το δίκτυο. Στη συνέχεια, το σύστημα θα παρακολουθεί όλη την κυκλοφορία που περνάει μέσα από τις συσκευές στα πολλαπλά σημεία των αισθητήρων.
- Host Intrusion Detection Systems (HIDS): Ένα HIDS τοποθετείται απευθείας στις συσκευές για την παρακολούθηση της κυκλοφορίας, δίνοντας στους διαχειριστές του δικτύου λίγο περισσότερο έλεγχο και ευελιξία. Ωστόσο, αυτό μπορεί να γίνει επαχθές ανάλογα με το μέγεθος του οργανισμού. Εάν ένας οργανισμός αξιοποιεί μόνο τα HIDS, η εταιρεία θα πρέπει να λογοδοτεί για κάθε νέα συσκευή που προστίθεται στον οργανισμό, αφήνοντας περιθώρια για λάθη, ενώ παράλληλα απαιτεί πολύ χρόνο.

- Protocol-based Intrusion Detection Systems (PIDS): Ένα IDS με βάση το πρωτόκολλο τοποθετείται συχνά στο μπροστινό μέρος ενός διακομιστή και παρακολουθεί την κυκλοφορία που ρέει από και προς τις συσκευές. Αυτό αξιοποιείται για την ασφάλεια των χρηστών που περιηγούνται στο διαδίκτυο.
- Application protocol-based Intrusion Detection Systems (APIDS): Ένα APIDS είναι παρόμοιο με ένα σύστημα βασισμένο σε πρωτόκολλο, αλλά παρακολουθεί την κυκλοφορία σε μια ομάδα διακομιστών. Αυτό αξιοποιείται συχνά σε συγκεκριμένα πρωτόκολλα εφαρμογών για την ειδική παρακολούθηση της δραστηριότητας, βοηθώντας τους διαχειριστές δικτύου να τμηματοποιήσουν και να ταξινομήσουν καλύτερα τις δραστηριότητες παρακολούθησης του δικτύου τους.
- Hybrid Intrusion Setection Systems: Οι υβριδικές λύσεις IDS παρέχουν έναν συνδυασμό των παραπάνω τύπων ανίχνευσης εισβολής. Οι προσφορές ορισμένων πωλητών διασταυρώνουν πολλαπλές κατηγορίες IDS για να καλύψουν πολλαπλά συστήματα σε ένα περιβάλλον εργασίας.

5.4.4 Λειτουργία και Τύποι IPS

Ένα IPS έχει την ίδια λειτουργικότητα με τα συστήματα IDS όσον αφορά την ανίχνευση, αλλά περιέχει επίσης δυνατότητες απόκρισης [25]. Μια λύση αναλαμβάνει δράση όταν ανιχνεύεται μια πιθανή επίθεση, κακόβουλη συμπεριφορά ή ένας μη εξουσιοδοτημένος χρήστης.

Οι συγκεκριμένες λειτουργίες ενός IPS εξαρτώνται από τον τύπο της λύσης, αλλά γενικά, η ύπαρξη ενός IPS είναι χρήσιμη για την αυτοματοποίηση των ενεργειών και τον περιορισμό των απειλών χωρίς την ανάγκη ενός διαχειριστή.

- Network-based Intrusion Prevention System (NIPS): Ένα NIPS παρακολουθεί και προστατεύει ολόκληρο το δίκτυο από ανώμαλη ή ύποπτη συμπεριφορά. Πρόκειται για ένα σύστημα ευρείας βάσης, το οποίο μπορεί να ενσωματωθεί με πρόσθετα εργαλεία παρακολούθησης για να βοηθήσει στην παροχή μιας ολοκληρωμένης εικόνας του δικτύου ενός οργανισμού.
- Wireless Intrusion Prevention System (WIPS): Τα WIPS είναι επίσης αρκετά διαδεδομένα και συχνά παρακολουθούν όλα τα ασύρματα δίκτυα που ανήκουν σε έναν οργανισμό. Αυτός ο τύπος είναι παρόμοιος με ένα NIPS, αλλά εντοπίζεται σε ασύρματα δίκτυα για πιο στοχευμένη ανίχνευση και αντίδραση.
- Host-based Intrusion Prevention System (HIPS): Τα HIPS αναπτύσσονται συχνά σε βασικές συσκευές ή κεντρικούς υπολογιστές που ένας οργανισμός πρέπει να διασφαλίσει. Το σύστημα παρακολουθεί στη συνέχεια όλη την κυκλοφορία που ρέει μέσω και από τον κεντρικό υπολογιστή για να ανιχνεύσει κακόβουλη συμπεριφορά.
- Network Behavioral Analysis (NBA): Σε αντίθεση με το NIPS, μια λύση NBA θα αναζητήσει την ανώμαλη συμπεριφορά μέσα στα μοτίβα του ίδιου του δικτύου, καθιστώντας το βασικό στοιχείο για την ανίχνευση περιστατικών όπως επιθέσεις DDoS, συμπεριφορές ενάντια στην πολιτική και άλλους τύπους κακόβουλου λογισμικού.

5.4.5 Ομοιότητες και Διαφορές Μεταξύ IDS και IPS

Μεταξύ αυτών των δύο λύσεων, όμοια συμπεριφορά εντοπίζεται σε:

- Monitoring: Διαφέρουν μόνο στο πόσο στοχευμένες ή ευρείες είναι οι δυνατότητές τους.
- Alerting: Μετά την ανακάλυψη μιας πιθανής απειλής, μόνο ένα IPS θα κάνει το επόμενο απαιτούμενο βήμα, αλλά και οι δύο λύσεις σας ειδοποιούν πρώτα για την ανακάλυψη και τη σχετική ενέργεια.

- Learning: Ανάλογα με το σύστημα ανίχνευσης που χρησιμοποιείται είτε από ένα σύστημα IPS είτε από ένα σύστημα IDS, πιθανότατα και τα δύο θα μάθουν να εντοπίζουν ύποπτες συμπεριφορές και να ελαχιστοποιούν τα ψευδώς θετικά αποτελέσματα.
- Logging: Και τα δύο συστήματα θα τηρούν λογαριασμό σχετικά με το τι παρακολουθείται και ποια ενέργεια έχει αναληφθεί, ώστε να μπορείτε να επανεξετάζετε ανάλογα την απόδοση.

Οι βασικές διαφορές εντοπίζονται σε:

- Response: Αυτή είναι η σημαντικότερη διαφορά μεταξύ των δύο συστημάτων. Ένα IDS θα σταματήσει στη φάση της ανίχνευσης, αφήνοντας τον χρήστη και την υπηρεσία σας ελεύθερους να αποφασίσετε ποια ενέργεια θα λάβετε. Ένα IPS, ανάλογα με τις ρυθμίσεις και την πολιτική, θα αναλάβει δράση για να προσπαθήσει να περιορίσει την απειλή ή να αποτρέψει τους μη εξουσιοδοτημένους χρήστες από το να ενσωματωθούν περαιτέρω στο δίκτυό σας.
- Protection: Λόγω των διαφορών που αναφέρονται παραπάνω, ένα IPS προσφέρει μεγαλύτερη προστασία επειδή ενεργεί αυτόματα, αφήνοντας ελάχιστο χρόνο σε έναν μη εξουσιοδοτημένο χρήστη να συνεχίσει να θέτει σε κίνδυνο έναν οργανισμό.
- Impact: Ως παρενέργεια αυτής της αυτοματοποίησης, τα ψευδώς θετικά αποτελέσματα ενδέχεται να έχουν αρνητικό αντίκτυπο σε έναν οργανισμό. Ένα IPS μπορεί να κλείσει το δίκτυό ή να σταματήσει την κυκλοφορία από και προς μια συγκεκριμένη συσκευή στο όνομα της προφύλαξης και της ασφάλειας, ακόμη και αν η απειλή δεν απαιτούσε τόσο δραστική δράση (ή η ειδοποίηση ήταν ψευδώς θετική).

6 Υλοποίηση Σεναρίων με Χρήση του Cisco Packet Tracer

6.1 IPsec VPN Security

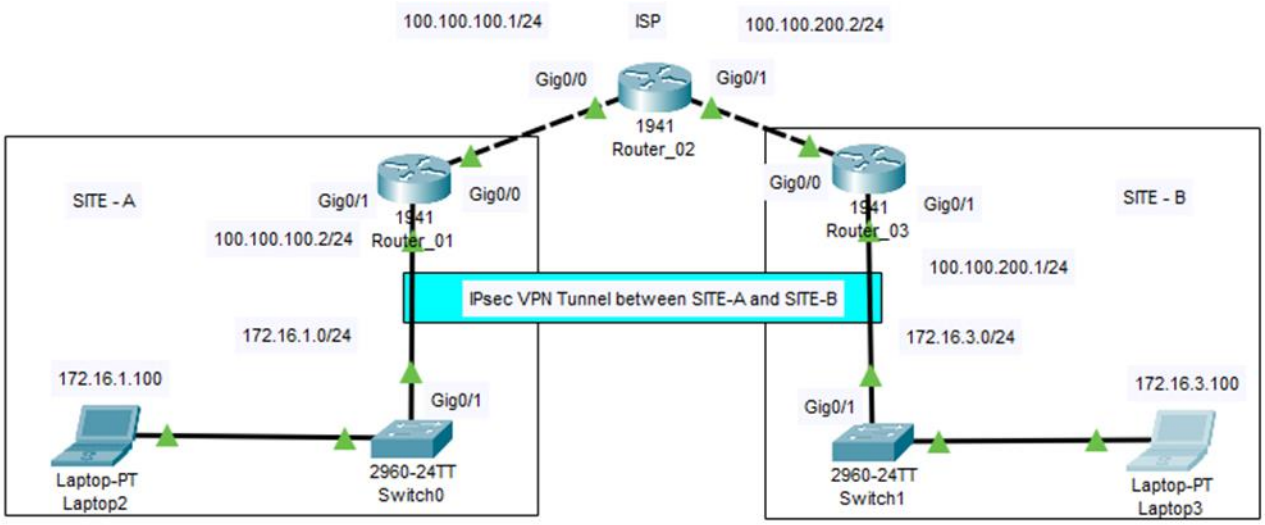
Σκοπός της παρούσας υλοποίησης είναι η δημιουργία ασφαλούς κρυπτογραφημένου καναλιού επικοινωνίας μεταξύ των Site-A και Site-B.

Για την υλοποίηση του περιβάλλοντος αυτού χρησιμοποιήθηκε ο παρακάτω εξοπλισμός:

- 3 x Cisco 1941 Routers
- 2 x Cisco 2960 Switches
- 2 x Laptops

Επίσης, ο εξοπλισμός συνδέθηκε με την κατάλληλη συνδεσμολογία, δηλαδή crossover cable για την σύνδεση των routers μεταξύ τους και straight through cable για τις συνδέσεις των υπόλοιπων συσκευών του δικτύου.

Τα δίκτυα της τοπολογίας παρουσιάζονται στο παρακάτω σχήμα:



Σχήμα 9: Τοπολογία υλοποίησης IPsec VPN Tunneling

Το εσωτερικό υποδίκτυο του Site-A είναι το 172.16.0.0/24 ενώ του Site-B είναι το 172.16.3.0/24 αντίστοιχα.

6.1.1 Initial Configuration

Για το αρχικό configuration των routers, ρυθμίστηκαν τα routers Router_01 και Router_03 να στοχεύουν το Router_02 που διαδραματίζει το ρόλο του ISP (Internet Service Provider) και το οποίο δεν έχει γνώση για τα άλλα δίκτυα πέραν των απευθείας συνδέσεων στις διεπαφές των routers. Το initial configuration είναι το εξής:

```
# Configuration on Router_01:
      hostname Router_01
      interface g0/1
      ip address 172.16.1.1 255.255.255.0
      no shut
      interface g0/0
      ip address 100.100.100.1 255.255.255.0
      no shut
      exit
      ip route 0.0.0.0 0.0.0.0 100.100.100.2

# Configuration on Router_02:
      hostname Router_02
      interface g0/1
      ip address 100.100.200.2 255.255.255.0
      no shut
      interface g0/0
      ip address 100.100.100.2 255.255.255.0
      no shut
      exit

# Configuration on Router_03:
      hostname Router_03
      interface g0/1
      ip address 172.16.3.1 255.255.255.0
      no shut
      interface g0/0
      ip address 100.100.200.1 255.255.255.0
      no shut
      exit
      ip route 0.0.0.0 0.0.0.0 100.100.200.2
```

Στα laptops της υποδομής, έχουμε δώσει στατικές IPs:

- Laptop2: 172.16.1.100
- Laptop3: 172.16.3.100

Όπως φαίνεται στις παρακάτω εικόνες, μετά το initial configuration οι δύο hosts δεν επικοινωνούν μεταξύ τους:

```
C:\>ipconfig

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: FE80::2D0:BCFF:FEC8:D1E5
   IPv6 Address.....: ::
   IPv4 Address.....: 172.16.3.100
   Subnet Mask.....: 255.255.0.0
   Default Gateway.....: ::
                                 172.16.3.1

Bluetooth Connection:

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: ::
   IPv6 Address.....: ::
   IPv4 Address.....: 0.0.0.0
   Subnet Mask.....: 0.0.0.0
   Default Gateway.....: ::
                                 0.0.0.0

C:\>ping 172.16.1.100

Pinging 172.16.1.100 with 32 bytes of data:

Request timed out.
Request timed out.

Ping statistics for 172.16.1.100:
    Packets: Sent = 2, Received = 0, Lost = 2 (100% loss),
```

Εικόνα 9: Το Laptop2 δεν επικοινωνεί με το Laptop3

```
C:\>ipconfig

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: FE80::20C:CFFF:FE11:4821
   IPv6 Address.....: ::
   IPv4 Address.....: 172.16.1.100
   Subnet Mask.....: 255.255.0.0
   Default Gateway.....: ::
                                 172.16.1.1

Bluetooth Connection:

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: ::
   IPv6 Address.....: ::
   IPv4 Address.....: 0.0.0.0
   Subnet Mask.....: 0.0.0.0
   Default Gateway.....: ::
                                 0.0.0.0

C:\>ping 172.16.3.100

Pinging 172.16.3.100 with 32 bytes of data:

Request timed out.

Ping statistics for 172.16.3.100:
    Packets: Sent = 2, Received = 0, Lost = 2 (100% loss),
```

Εικόνα 10: Το Laptop3 δεν επικοινωνεί με το Laptop2

Αρχικά το Security License στα edge routers (Router_01 και Router_03), δεν ήταν ενεργοποιημένο. Όπως φαίνεται χρησιμοποιώντας την εντολή show version:

```
Technology Package License Information for Module:'c1900'

-----------------------------------------------------------------
Technology    Technology-package          Technology-package
              Current       Type          Next reboot
-----------------------------------------------------------------
ipbase        ipbasek9      Permanent     ipbasek9
security      None          None          None
data          None          None          None

Configuration register is 0x2102
```

Εικόνα 11: Ανενεργό Security License

Για την ενεργοποίηση του Security License χρησιμοποιήθηκαν οι παρακάτω εντολές:

```
license boot module c1900 technology-package securityk9
copy run start
reload
show version
```

```
Technology Package License Information for Module:'c1900'

-----------------------------------------------------------------
Technology    Technology-package          Technology-package
              Current       Type          Next reboot
-----------------------------------------------------------------
ipbase        ipbasek9      Permanent     ipbasek9
security      securityk9    Evaluation    securityk9
data          disable       None          None

Configuration register is 0x2102
```

Εικόνα 12: Ενεργό Security License

6.1.2 IPsec VPN Configuration

Για τη ρύθμιση και εγκατάσταση του IPsec Tunnel, η διαμόρφωση και στα δύο άκρα πρέπει να ταιριάζει για να είναι επιτυχής τόσο η Φάση 1 όσο και η Φάση 2. Το Tunnel θα εγκατασταθεί μεταξύ των Router_01 και Router_03.

Αρχικά ρυθμίστηκε μια ACL που καθορίζει την κίνηση που μας ενδιαφέρει να περάσει μέσω του Tunnel:

```
#Configuration on Router_01
      access-list 100 permit ip 172.16.1.0 0.0.0.255 172.16.3.0 0.0.0.255
#Configuration on Router_03
      access-list 100 permit ip 172.16.3.0 0.0.0.255 172.16.1.0 0.0.0.255
```

Εν συνεχεία, εγκαταστάθηκε η πρώτη φάση του IPsec. Σε αυτό το σημείο, ορίστηκε η ISAKAMP πολιτική και καθορίστηκε ότι θα χρησιμοποιείται ένα προσυμφωνημένο κλειδί. Αυτό ορίζεται και σε αυτή την περίπτωση χρησιμοποιώντας τις εντολές:

```
#Configuration on Router_01
      crypto isakmp policy 10
          encryption aes 256
          authentication pre-share
          group 5
      #
      crypto isakmp key Secret-2020 address 100.100.200.1
#Configuration on Router_03
      crypto isakmp policy 10
          encryption aes 256
          authentication pre-share
          group 5
      #
      crypto isakmp key Secret-2020 address 100.100.100.1
```

Επόμενο βήμα είναι η εγκατάσταση της δεύτερης φάσης του IPsec Tunnel (IPsec Transform-set). Στην φάση αυτή λαμβάνει χώρα η διαπραγμάτευση IKE. Θα χρησιμοποιηθεί AES 256bit με hash message authentication code, παρέχοντας έτσι εμπιστευτικότητα, ακεραιότητα και αυθεντικοποίηση:

```
#Configuration on Router_01
      crypto ipsec transform-set Router_01-Router_03 esp-aes 256 esp-sha-
      hmac
#Configuration on Router_03
      crypto ipsec transform-set Router_03-Router_01 esp-aes 256 esp-sha-
      hmac
```

Επόμενο βήμα είναι η σύνδεση της πρώτης με τη δεύτερη φάση μαζί, ορίζοντας τον λεγόμενο χάρτη κρυπτογράφησης (crypto map):

```
#Configuration on Router_01
      crypto map IPSEC-CRYPTOMAP 100 ipsec-isakmp
      set peer 100.100.200.1
      set pfs group5
      set security-association lifetime seconds 86400
      set transform-set Router_01-Router_03
      match address 100

#Configuration on Router_03
      crypto map IPSEC-CRYPTOMAP 100 ipsec-isakmp
      set peer 100.100.100.1
      set pfs group5
      set security-association lifetime seconds 86400
      set transform-set Router_03-Router_01
      match address 100
```

Στο σημείο αυτό, ενεργοποιούμε το IPsec στην εξωτερική διεπαφή εφαρμόζοντας το χάρτη κρυπτογράφησης που δημιουργήθηκε:

```
#Configuration on Router_03
      interface GigabitEthernet0/0
      crypto map IPSEC-CRYPTOMAP
#Configuration on Router_03
      interface GigabitEthernet0/0
      crypto map IPSEC-CRYPTOMAP
```

6.1.3 Επαλήθευση Λειτουργικότητας Υλοποίησης

Η υλοποίηση IPsec VPN Tunneling έχει ολοκληρωθεί επιτυχώς, γεγονός που καταδεικνύεται και από το ότι τα δύο laptops μπορούν να επικοινωνήσουν μεταξύ τους πλέον, όπως φαίνεται και στις παρακάτω εικόνες:

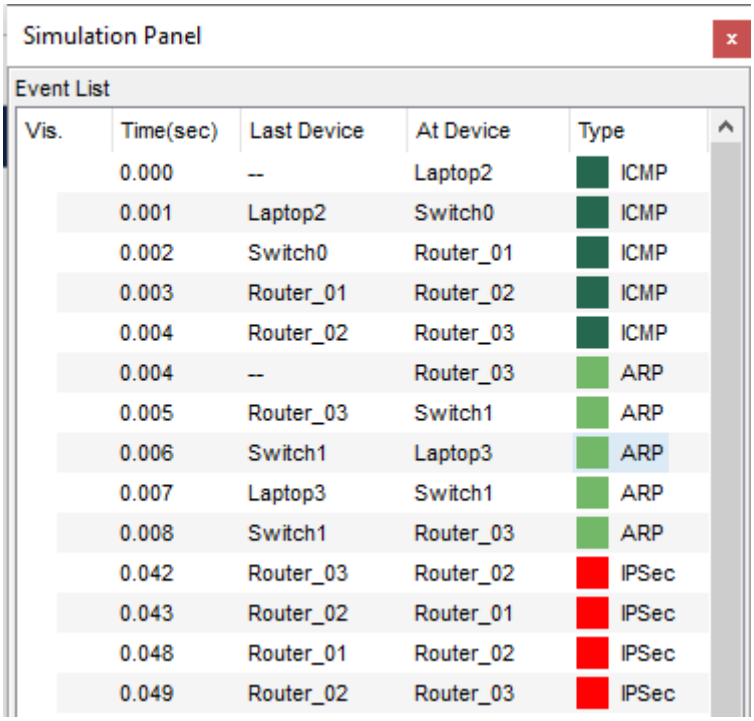
```
C:\>ipconfig

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: FE80::20C:CFFF:FE11:4821
   IPv6 Address.....: ::
   IPv4 Address.....: 172.16.1.100
   Subnet Mask.....: 255.255.0.0
   Default Gateway.....: ::
                                 172.16.1.1

Bluetooth Connection:

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: ::
   IPv6 Address.....: ::
   IPv4 Address.....: 0.0.0.0
   Subnet Mask.....: 0.0.0.0
   Default Gateway.....: ::
                                 0.0.0.0

C:\>ping 172.16.3.100

Pinging 172.16.3.100 with 32 bytes of data:

Reply from 172.16.3.100: bytes=32 time<1ms TTL=126
Reply from 172.16.3.100: bytes=32 time=12ms TTL=126
Reply from 172.16.3.100: bytes=32 time=1ms TTL=126
Reply from 172.16.3.100: bytes=32 time=1ms TTL=126

Ping statistics for 172.16.3.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 12ms, Average = 3ms

C:\>
```

Εικόνα 13: Το Laptop2 επικοινωνεί επιτυχώς με το Laptop3

```
C:\>ipconfig

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: FE80::2D0:BCFF:FEC8:D1E5
   IPv6 Address.....: ::
   IPv4 Address.....: 172.16.3.100
   Subnet Mask.....: 255.255.0.0
   Default Gateway.....: ::
                                 172.16.3.1

Bluetooth Connection:

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: ::
   IPv6 Address.....: ::
   IPv4 Address.....: 0.0.0.0
   Subnet Mask.....: 0.0.0.0
   Default Gateway.....: ::
                                 0.0.0.0

C:\>ping 172.16.1.100

Pinging 172.16.1.100 with 32 bytes of data:

Reply from 172.16.1.100: bytes=32 time<1ms TTL=126
Reply from 172.16.1.100: bytes=32 time<1ms TTL=126
Reply from 172.16.1.100: bytes=32 time=12ms TTL=126
Reply from 172.16.1.100: bytes=32 time=11ms TTL=126

Ping statistics for 172.16.1.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 12ms, Average = 5ms

C:\>
```

Εικόνα 14: Το Laptop3 επικοινωνεί επιτυχώς με το Laptop2

Επίσης, χρησιμοποιώντας το Simulation Panel του CPT και στέλνοντας ένα πακέτο από το Laptop2 στο Laptop3, επαληθεύεται η επιτυχής εγκαθίδρυση του IPsec VPN Tunnel:



Εικόνα 15: Επιτυχής εγκαθίδρυση IPsec VPN Tunnel

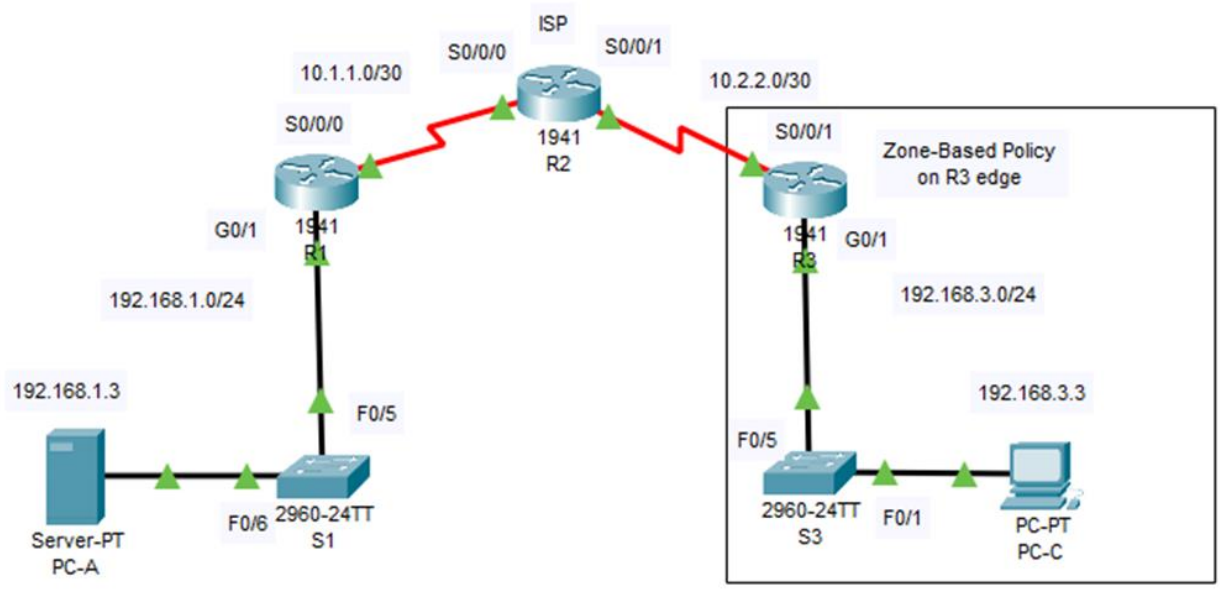
6.2 Zone-Based Policy Firewall

Σκοπός αυτής της υλοποίησης είναι ο σχεδιασμός και η υλοποίηση Zone-Based Policy Firewall στο router R3 με στόχο να επιτρέπεται η εξερχόμενη κίνηση και να αποτρέπεται η εισερχόμενη.

Για την υλοποίηση του περιβάλλοντος αυτού χρησιμοποιήθηκε ο παρακάτω εξοπλισμός:

- 3 x Cisco 1941 Routers
- 2 x Cisco 2960 Switches
- 1 x PC
- 1 x Server

Τα δίκτυα της τοπολογίας παρουσιάζονται στο παρακάτω σχήμα:



Σχήμα 10: Τοπολογία υλοποίησης Zone-Based Policy Firewall

Ο Server ανήκει στο υποδίκτυο 192.168.1.0/24 και έχει στατική IP 192.168.1.3, ενώ το PC ανήκει στο υποδίκτυο 192.168.3.0/24 και έχει στατική IP 192.168.3.3. Επίσης, οι συσκευές είναι συνδεδεμένες με την κατάλληλη συνδεσμολογία.

6.2.1 Initial Configuration

Στην υλοποίηση αυτή, όπως και στην προηγούμενη, τα routers R1 και R3 στοχεύουν στο router R2 που διαδραματίζει το ρόλο του ISP, δηλαδή το διαδίκτυο.

Το initial configuration των routers είναι αντίστοιχο της υλοποίησης της παραγράφου 6.1.1, όπως επίσης και η διαδικασία ενεργοποίησης του Security License (ή αλλιώς Security Technology Package).

Όπως παρουσιάζεται στις παρακάτω εικόνες, το PC-A μπορεί να επικοινωνήσει αρχικά με το PC-C:

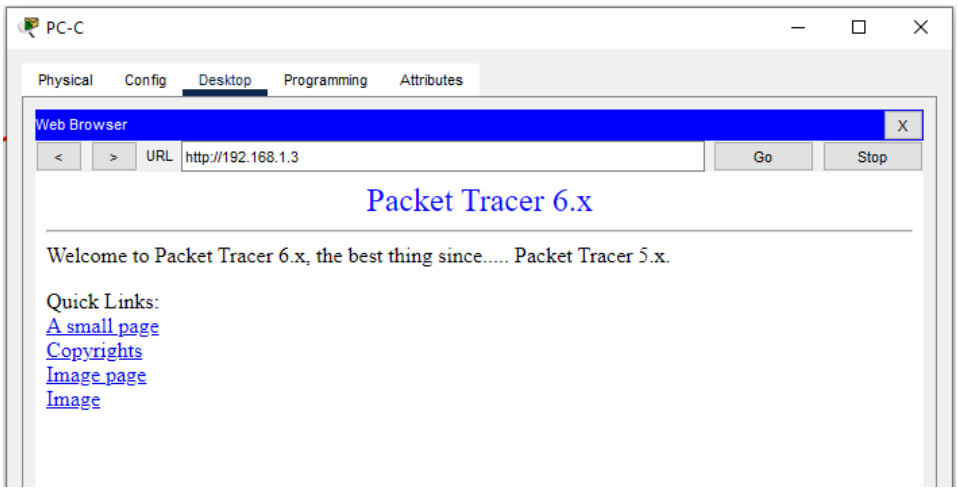
```
C:\>ipconfig

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: ::
   IPv6 Address.....: ::
   IPv4 Address.....: 192.168.1.3
   Subnet Mask.....: 255.255.255.0
   Default Gateway.....: ::
                                 192.168.1.1

C:\>ping 192.168.3.3

Pinging 192.168.3.3 with 32 bytes of data:

Reply from 192.168.3.3: bytes=32 time=17ms TTL=125
Reply from 192.168.3.3: bytes=32 time=3ms TTL=125
Reply from 192.168.3.3: bytes=32 time=20ms TTL=125
Reply from 192.168.3.3: bytes=32 time=11ms TTL=125

Ping statistics for 192.168.3.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 20ms, Average = 12ms

C:\>
```

Εικόνα 16: Επικοινωνία PC-A με PC-C

Επίσης, από τον host PC-C έχουμε πρόσβαση στο Router R2 μέσω ssh, καθώς επίσης και στο http service που τρέχει στον Server PC-A:

```
C:\>ssh -l Admin 10.2.2.2

Password:



R2#
R2#
```

Εικόνα 17: Επικοινωνία PC-C με R2 μέσω ssh



Εικόνα 18: Επικοινωνία PC-C με Server μέσω http

6.2.2 Zone-Based Policy Firewall Configuration

Αρχικά δημιουργήθηκαν οι Ζώνες Firewall στο R3. Με τη χρήση της εντολής zone security αρχικά δημιουργείται η ζώνη IN-ZONE καθώς και η ζώνη OUT-ZONE.

```
#Configuration on R3
      zone security IN-ZONE
      zone security OUT-ZONE
```

Στο επόμενο βήμα, αναγνωρίστηκε η κίνηση χρησιμοποιώντας την επιλογή Class-Map. Πρώτα δημιουργήθηκε μία εκτεταμένη ACL 101 για να επιτρέπει όλα τα πρωτόκολλα IP από το υποδίκτυο 192.168.3.0/24 προς οποιοδήποτε προορισμό.

```
#Configuration on R3
      access-list 101 permit ip 192.168.3.0 0.0.0.255 any
```

Στη συνέχεια δημιουργήθηκε το class map IN-NET-CLASS-MAP που να αντιστοιχεί στην ACL 101.

```
#Configuration on R3
      class-map type inspect match-all IN-NET-CLASS-MAP
      match access-group 101
```

Επόμενο βήμα ήταν ο καθορισμός των πολιτικών του Firewall. Αρχικά δημιουργήθηκε το policy map IN-2-OUT-PMAP:

```
#Configuration on R3
      policy-map type inspect IN-2-OUT-PMAP
```

Εν συνεχεία ο καθορισμός μίας κλάσης τύπου inspect και αναφοράς στο class map N-NET-CLASS-MAP:

```
#Configuration on R3
      class type inspect IN-NET-CLASS-MAP
```

Με τη χρήση της εντολής inspect ορίσαμε το context-based access control:

```
#Configuration on R3
      inspect
```

Τελευταίο βήμα ήταν η εφαρμογή των πολιτικών του Firewall. Αρχικά δημιουργήθηκε το ζεύγος ζωνών IN-2-OUT-ZPAIR και ορίστηκαν οι ζώνες πηγής και προορισμού που δημιουργήθηκαν νωρίτερα:

```
#Configuration on R3
      zone-pair security IN-2-OUT-ZPAIR source IN-ZONE destination OUT-ZONE
```

Εν συνεχεία, καθορίστηκε το policy map για τη διαχείριση της κίνησης μεταξύ των δύο ζωνών και εφαρμόστηκε μαζί με τις πολιτικές του:

```
#Configuration on R3
      service-policy type inspect IN-2-OUT-PMAP
```

Τέλος, τα interfaces ανατέθηκαν στις κατάλληλες ζώνες ασφάλειας:

```
#Configuration on R3
      interface g0/1
      zone-member security IN-ZONE
      interface s0/0/1
      zone-member security OUT-ZONE
```

Η υλοποίηση έχει πλέον ολοκληρωθεί.

6.2.3 Επαλήθευση Λειτουργικότητας Υλοποίησης

Αρχικά επαληθεύτηκε η εξερχόμενη κίνηση από το router R3. Παρατηρήθηκε πως ο host PC-C συνεχίζει να επικοινωνεί κανονικά με τον host PC-A:

```
C:\>ipconfig

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: FE80::201:64FF:FEB1:8D85
   IPv6 Address.....: ::
   IPv4 Address.....: 192.168.3.3
   Subnet Mask.....: 255.255.255.0
   Default Gateway.....: ::
                                 192.168.3.1

Bluetooth Connection:

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: ::
   IPv6 Address.....: ::
   IPv4 Address.....: 0.0.0.0
   Subnet Mask.....: 0.0.0.0
   Default Gateway.....: ::
                                 0.0.0.0

C:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Reply from 192.168.1.3: bytes=32 time=22ms TTL=125
Reply from 192.168.1.3: bytes=32 time=2ms TTL=125
Reply from 192.168.1.3: bytes=32 time=20ms TTL=125
Reply from 192.168.1.3: bytes=32 time=14ms TTL=125

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 22ms, Average = 14ms
```

Εικόνα 19: Επαλήθευση επικοινωνίας PC-C με PC-A

Επίσης, ο host PC-C συνεχίζει να έχει πρόσβαση τόσο στο Router R2 μέσω ssh όσο και στον http Server. Τα sessions γίνονται κανονικά inspect στο Router R3 όπως φαίνεται στις παρακάτω εικόνες:

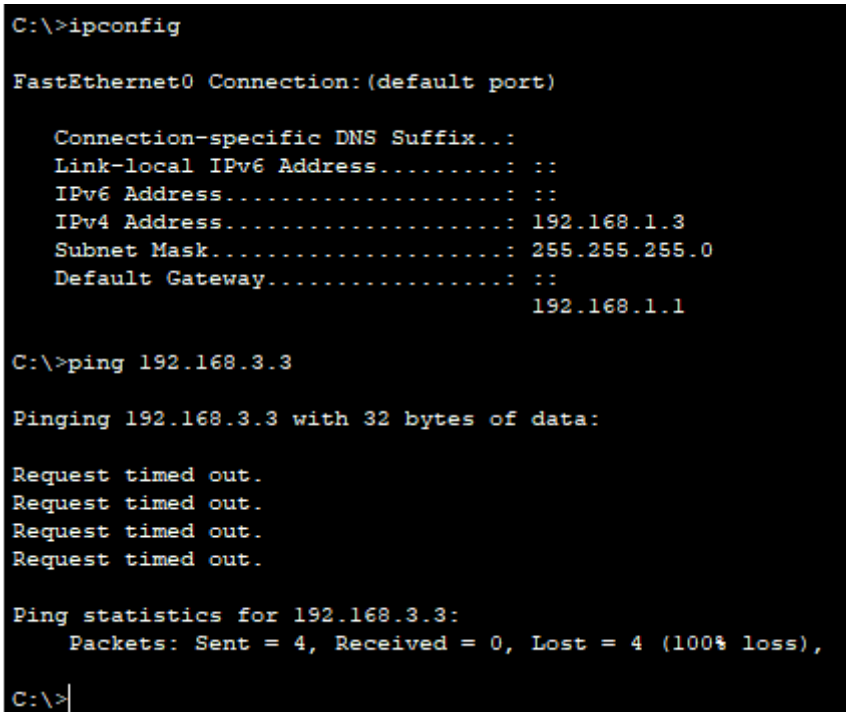
```
R3#show policy-map type inspect zone-pair sessions

policy exists on zp IN-2-OUT-ZPAIR
 Zone-pair: IN-2-OUT-ZPAIR

  Service-policy inspect : IN-2-OUT-PMAP

    Class-map: IN-NET-CLASS-MAP (match-all)
      Match: access-group 101
      Inspect

        Number of Established Sessions = 1
        Established Sessions
         Session 3291136608 (192.168.3.3:1025)=>(10.2.2.2:22) tcp SIS_OPEN/TCP_ESTAB
          Created 00:01:26, Last heard  00:01:07
          Bytes sent (initiator:responder) [1064:895]
    Class-map: class-default (match-any)
      Match: any
      Drop (default action)
        0 packets, 0 bytes
R3#
```

Εικόνα 20: Ανοιχτό ssh session PC-C με R2

```
R3#show policy-map type inspect zone-pair sessions

policy exists on zp IN-2-OUT-ZPAIR
 Zone-pair: IN-2-OUT-ZPAIR

  Service-policy inspect : IN-2-OUT-PMAP

    Class-map: IN-NET-CLASS-MAP (match-all)
      Match: access-group 101
      Inspect

        Number of Established Sessions = 1
        Established Sessions
         Session 3646565792 (192.168.3.3:1026)=>(192.168.1.3:80) tcp SIS_OPEN/TCP_ESTAB
          Created 00:00:03, Last heard  00:00:02
          Bytes sent (initiator:responder) [284:552]
    Class-map: class-default (match-any)
      Match: any
      Drop (default action)
        0 packets, 0 bytes
R3#
```

Εικόνα 21: Ανοιχτό http session PC-C με Server

Τέλος, παρατηρείται ότι ο host PC-A δεν μπορεί να επικοινωνήσει με τον host PC-C καθώς η εισερχόμενη κίνηση στο υποδίκτυο 192.168.3.0/24 απορρίπτεται στο R3:



Εικόνα 22: Αδυναμία επικοινωνίας PC-A με PC-C λόγω εφαρμογής Zone-Based Policies στο R3

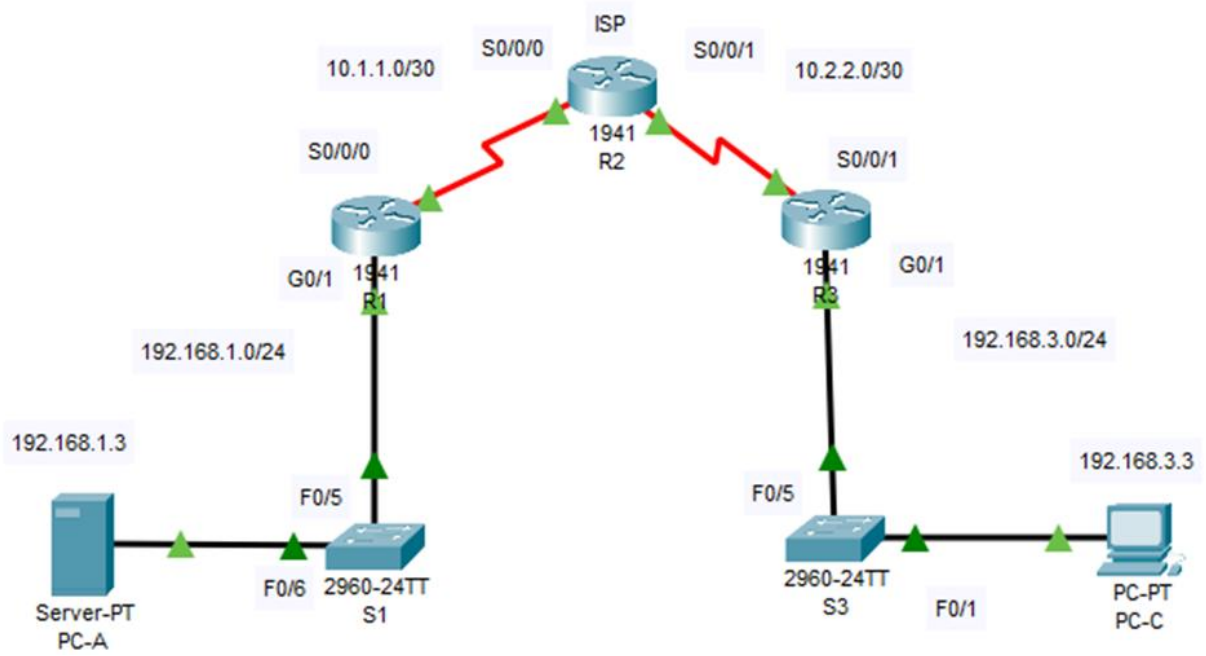
6.3 IP Access Control Lists

Σκοπός της υλοποίησης αυτής είναι η δημιουργία ACLs, βασισμένων στις source και destination IPs, οι οποίες θα εφαρμοστούν στα edge routers R1 και R3, με στόχο τον έλεγχο της κίνησης και την αποφυγή κοινών απειλών και επιθέσεων.

Η τοπολογία που χρησιμοποιείται είναι αντίστοιχη με αυτή της προηγούμενης προσομοίωσης. Συνεπώς χρησιμοποιήθηκε ο παρακάτω εξοπλισμός:

- 3 x Cisco 1941Routers
- 2 x Cisco 2960 Switches
- 1 x PC
- 1 x Server

Τα δίκτυα της τοπολογίας παρουσιάζονται στο παρακάτω σχήμα:



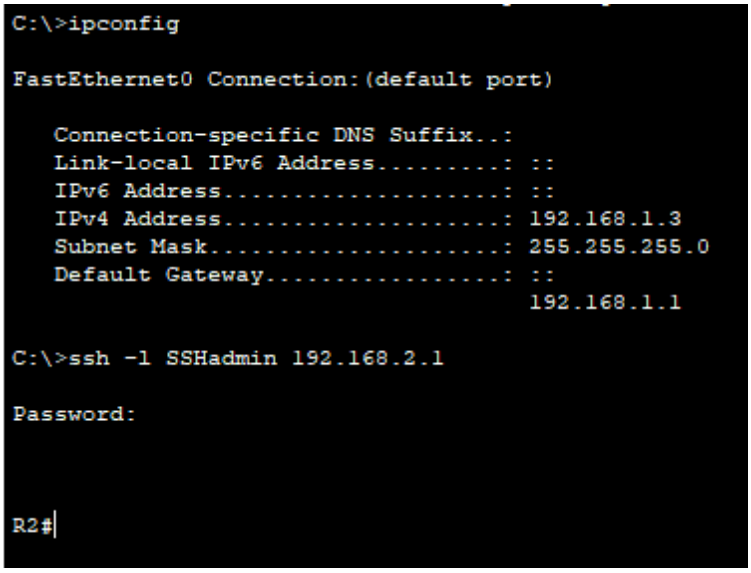
Σχήμα 11: Τοπολογία υλοποίησης IP ACLs

Υπενθυμίζεται πως ο Server ανήκει στο υποδίκτυο 192.168.1.0/24 και έχει στατική IP 192.168.1.3, ενώ το PC ανήκει στο υποδίκτυο 192.168.3.0/24 και έχει στατική IP 192.168.3.3. Επίσης, οι συσκευές είναι συνδεδεμένες με την κατάλληλη συνδεσμολογία.

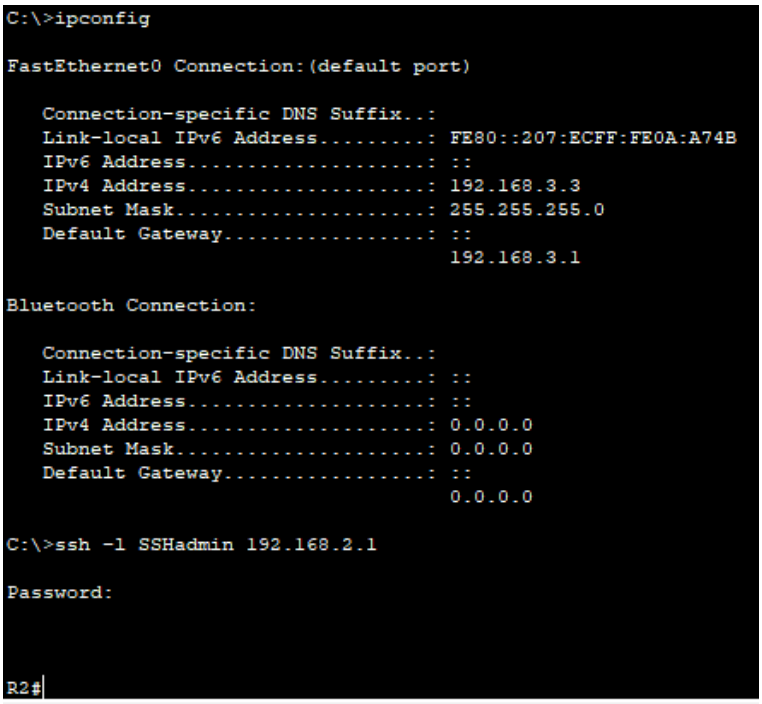
6.3.1 Initial Configuration

Όπως περιεγράφηκε και στην παράγραφο 6.2.1, τα routers R1 και R3 στοχεύουν στο router R2 που διαδραματίζει το ρόλο του ISP, δηλαδή το διαδίκτυο και η διαδικασία της ενεργοποίησης του Security Technology Package έχει περιγραφεί στην ενότητα 6.1.1.

Καθώς πρόκειται για την ίδια τοπολογία με αυτήν της παραγράφου 6.2, θεωρούμε δεδομένο πως οι δύο hosts PC-A και PC-C επικοινωνούν μεταξύ τους. Επίσης, και οι δύο hosts έχουν πρόσβαση στην κονσόλα του router R2 μέσω ssh.



Εικόνα 23: Επιτυχής επικοινωνία PC-A με R2 μέσω SSH



Εικόνα 24: Επιτυχής επικοινωνία PC-C με R2 μέσω SSH

6.3.2 Configuration IP ACL

Αρχικά διαμορφώθηκαν ACL 10 ώστε να μπλοκαριστεί η απομακρυσμένη πρόσβαση εκτός του PC-C σε όλα τα routers και στη συνέχεια εφαρμόστηκαν οι access lists VTY lines με τις εντολες:

```
# Configuration on R1
      access-list 10 permit host 192.168.3.3
      line vty 0 4
      access-class 10 in
# Configuration on R2
      access-list 10 permit host 192.168.3.3
      line vty 0 4
      access-class 10 in
# Configuration on R3
      access-list 10 permit host 192.168.3.3
      line vty 0 4
      access-class 10 in
```

Στο σημείο αυτό παρατηρείται πως το PC-A έχει χάσει τη σύνδεση στο R2 μέσω ssh, σε αντίθεση με το PC-C που συνεχίζει να επικοινωνεί κανονικά:

```
C:\>ipconfig

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: ::
   IPv6 Address.....: ::
   IPv4 Address.....: 192.168.1.3
   Subnet Mask.....: 255.255.255.0
   Default Gateway.....: ::
                                 192.168.1.1

C:\>ssh -l SSHadmin 192.168.2.1

% Connection refused by remote host
C:\>
```

Εικόνα 25: Αδυναμία σύνδεσης PC-A με R2 μέσω ssh

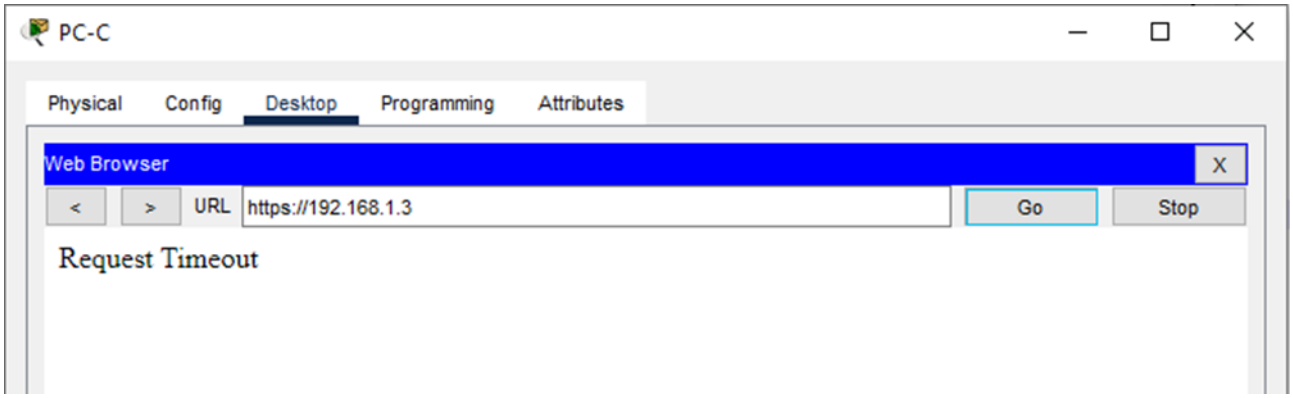
Επόμενο βήμα είναι η δημιουργία μίας αριθμημένης IP ACL στο R1 και η εφαρμογή της στο interface S0/0/0, με στόχο:

- Να επιτρέπεται από οποιοδήποτε εξωτερικό host η πρόσβαση στα services (DNS, SMTP και FTP) του Server.
- Το μπλοκάρισμα του service HTTPS από οποιοδήποτε εξωτερικό host.
- Το PC-C να μπορεί να συνδεθεί στο R1 μέσω ssh

Για το σκοπό αυτό χρησιμοποιήθηκαν οι εντολές:

```
#Configuration on R1
      access-list 120 permit udp any host 192.168.1.3 eq domain
      access-list 120 permit tcp any host 192.168.1.3 eq smtp
      access-list 120 permit tcp any host 192.168.1.3 eq ftp
      access-list 120 deny tcp any host 192.168.1.3 eq 443
      access-list 120 permit tcp host 192.168.3.3 host 10.1.1.1 eq 22
      interface s0/0/0
      ip access-group 120 in
```

Όπως παρουσιάζεται στην παρακάτω εικόνα, ο PC-C δεν έχει https πρόσβαση στον Server:

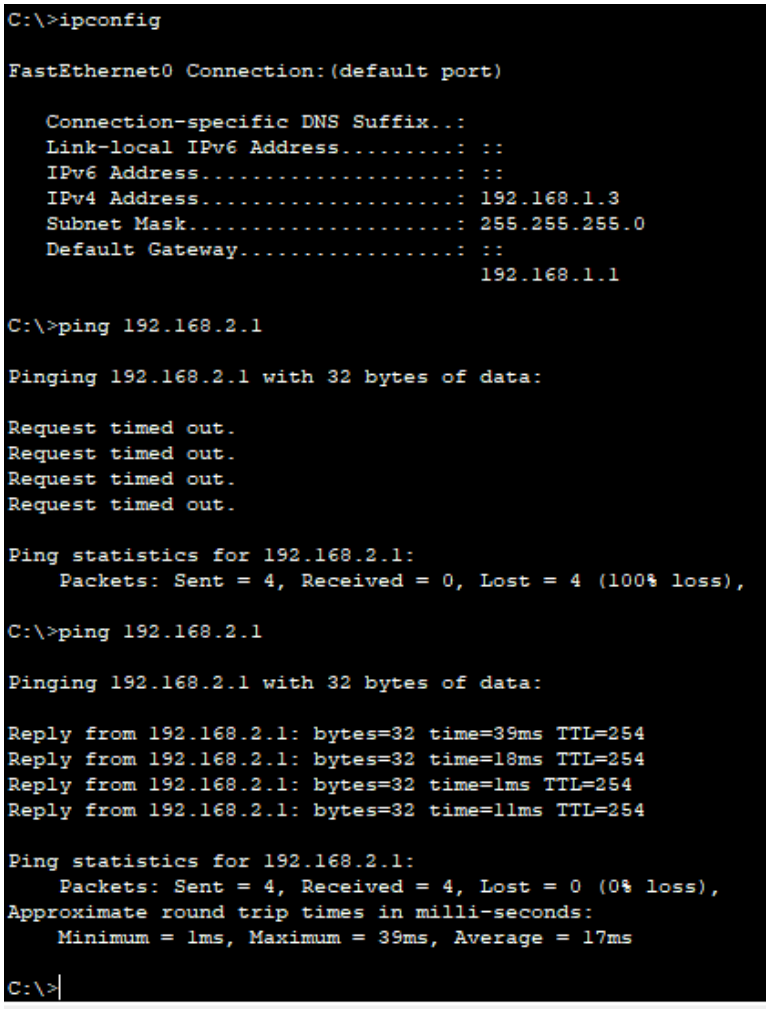


Εικόνα 26: Αδυναμία σύνδεσης PC-C με Server μέσω https

Στο σημείο αυτό θα παραμετροποιηθεί η υπάρχουσα ACL στο R1 έτσι ώστε να μπορεί να λαμβάνει ICMP πακέτα:

```
#Configuration on R1
      access-list 120 permit icmp any any echo-reply
      access-list 120 permit icmp any any unreachable
      access-list 120 deny icmp any any
      access-list 120 permit ip any any
```

Όπως παρουσιάζεται και στην παρακάτω εικόνα, ενώ το PC-A αρχικά δεν μπορούσε να επικοινωνήσει με το loopback interface του R2, μετά τις κατάλληλες αλλαγές στη ACL, επικοινωνεί επιτυχώς:



Εικόνα 27: Επιτυχής επικοινωνία PC-A με R2

Επόμενο βήμα στην υλοποίησή, είναι η δημιουργία μίας αριθμημένης ACL στο R3 που να απορρίπτει οποιαδήποτε κίνηση έρχεται από δίκτυα εξωτερικά του R3, δηλαδή υποδίκτυα πέραν του 192.168.3.0/24:

```
#Configuration on R3
      access-list 110 permit ip 192.168.3.0 0.0.0.255 any
      interface g0/1
      ip access-group 110 in
```

Τέλος, δημιουργήθηκε μία νέα αριθμημένη ACL 100 στο R3, η οποία απορρίπτει την εισερχόμενη κίνηση από οποιοδήποτε ιδιωτικό υποδίκτυο (δηλαδή τα δίκτυα 10.0.0.0/8, 172.16.0.0/16 και 192.168.0.0/24), το υποδίκτυο 127.0.0.0/8 και οποιαδήποτε multicast IP διεύθυνση. Δεδομένου όμως ότι το PC-C χρησιμοποιείται και για απομακρυσμένη διαχείριση του R2 (μέσω ssh), θα επιτραπεί η εισερχόμενη κίνηση ssh από το δίκτυο 10.0.0.0/24. Επομένως, ακολούθησαν οι παρακάτω εντολές:

```
#Configuration on R3
      access-list 100 permit tcp 10.0.0.0 0.255.255.255 eq 22 host
      192.168.3.3
      access-list 100 deny ip 10.0.0.0 0.255.255.255 any
      access-list 100 deny ip 172.16.0.0 0.15.255.255 any
      access-list 100 deny ip 192.168.0.0 0.0.255.255 any
      access-list 100 deny ip 127.0.0.0 0.255.255.255 any
      access-list 100 deny ip 224.0.0.0 15.255.255.255 any
      access-list 100 permit ip any any
      interface s0/0/1
      ip access-group 100 in
```

6.3.3 Επαλήθευση Λειτουργικότητας Υλοποίησης

Όπως δείχνει και η παρακάτω εικόνα, το PC-C δεν μπορεί πλέον να επικοινωνήσει με το PC-A καθώς η επικοινωνία μπλοκαρίστηκε μετά την εφαρμογή της τελευταίας ACL:

```
C:\>ipconfig

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: FE80::207:ECFF:FE0A:A74B
   IPv6 Address.....: ::
   IPv4 Address.....: 192.168.3.3
   Subnet Mask.....: 255.255.255.0
   Default Gateway.....: ::
                                 192.168.3.1

Bluetooth Connection:

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: ::
   IPv6 Address.....: ::
   IPv4 Address.....: 0.0.0.0
   Subnet Mask.....: 0.0.0.0
   Default Gateway.....: ::
                                 0.0.0.0

C:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

Εικόνα 28: Τελική αδυναμία PC-C να επικοινωνήσει με PC-A

Στον αντίποδα, το PC-C συνεχίζει να επικοινωνεί κανονικά με το loopback interface του R2:

```
C:\>ipconfig

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: FE80::207:ECFF:FE0A:A74B
   IPv6 Address.....: ::
   IPv4 Address.....: 192.168.3.3
   Subnet Mask.....: 255.255.255.0
   Default Gateway.....: ::
                                 192.168.3.1

Bluetooth Connection:

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: ::
   IPv6 Address.....: ::
   IPv4 Address.....: 0.0.0.0
   Subnet Mask.....: 0.0.0.0
   Default Gateway.....: ::
                                 0.0.0.0

C:\>ssh -l SSHadmin 192.168.2.1

Password:



R2#
```

Εικόνα 29: Επιτυχής επικοινωνία PC-C με R2 μέσω ssh

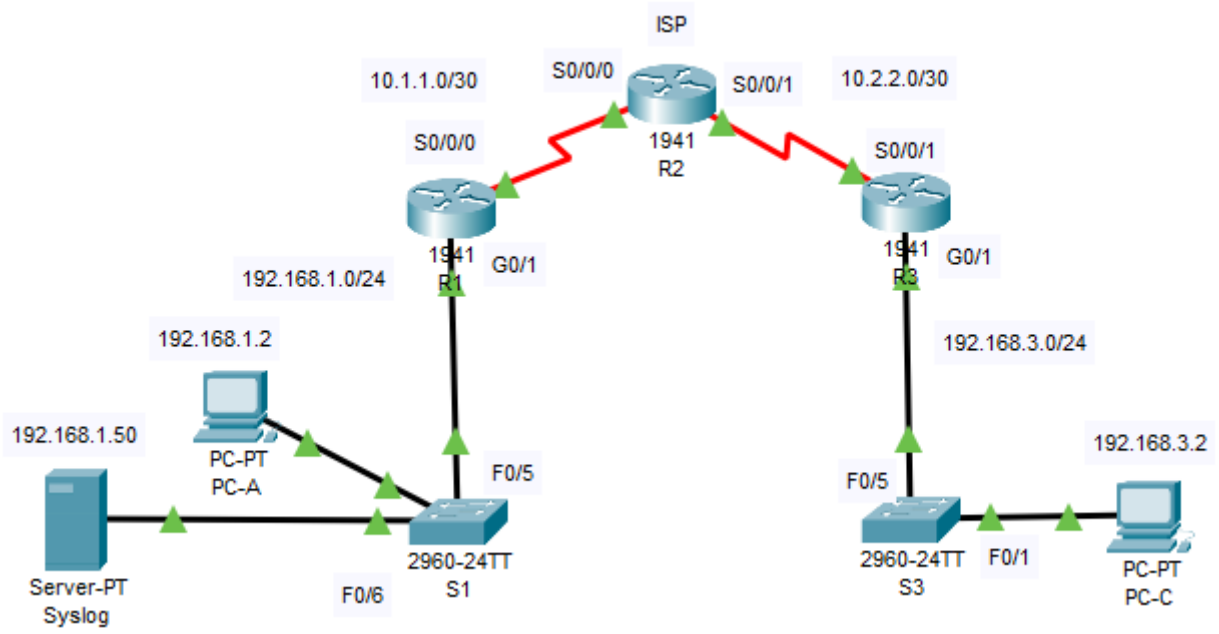
6.4 Intrusion Prevention System

Σκοπός της υλοποίησης αυτής είναι διαμόρφωση ενός IPS με στόχο να σαρώνει το εσωτερικό υποδίκτυο 192.168.1.0/24 και να αποτρέπει την εισερχόμενη κίνηση σε αυτό, καθώς επίσης και η επιτυχή καταγραφή της κίνησης αυτής στο Server, που στο σενάριο αυτό λειτουργεί ως Syslog Server

Η τοπολογία που χρησιμοποιείται είναι αντίστοιχη με αυτή της προηγούμενης προσομοίωσης. Συνεπώς χρησιμοποιήθηκε ο παρακάτω εξοπλισμός:

- 3 x Cisco 1941 Routers
- 2 x Cisco 2960 Switches
- 2 x PC
- 1 x Server

Τα δίκτυα της τοπολογίας παρουσιάζονται στο παρακάτω σχήμα:



Σχήμα 12: Τοπολογία υλοποίησης IPS

Υπενθυμίζεται πως ο Syslog Server ανήκει στο υποδίκτυο 192.168.1.0/24 και έχει στατική IP 192.168.1.50, ενώ το PC-C ανήκει στο υποδίκτυο 192.168.3.0/24 και έχει στατική IP 192.168.3.2. Στην συγκεκριμένη υλοποίηση, το PC-A έχει επίσης στατική IP, την 192.168.1.2. Επίσης, οι συσκευές είναι συνδεδεμένες με την κατάλληλη συνδεσμολογία.

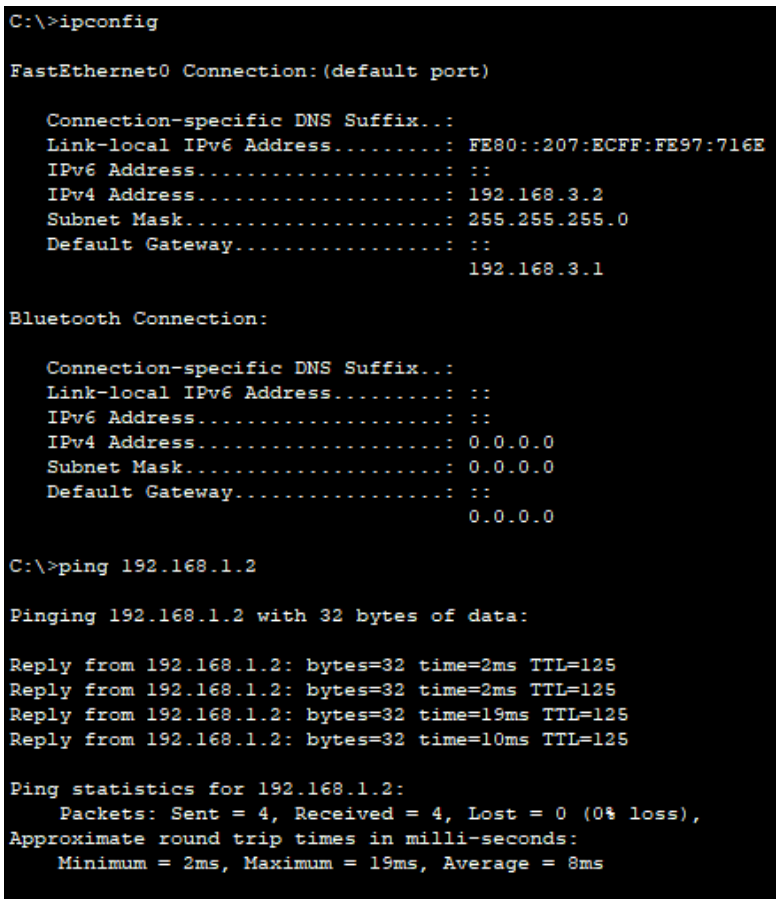
6.4.1 Initial Configuration

Όπως περιεγράφηκε και στην παράγραφο 6.2.1, τα routers R1 και R3 στοχεύουν στο router R2 που διαδραματίζει το ρόλο του ISP, δηλαδή το διαδίκτυο και η διαδικασία της ενεργοποίησης του Security Technology Package έχει περιγραφεί στην ενότητα 6.1.1.

Δεδομένου ότι πρόκειται για την ίδια τοπολογία, με την μόνη διαφορά ότι έχουν οριστεί διαφορετικές στατικές IP για τα μηχανήματα, υπενθυμίζουμε πως ο host PC-A επικοινωνεί κανονικά με τον PC-C, και το αντίστροφο:

```
C:\>ipconfig

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: FE80::290:21FF:FEC1:A069
   IPv6 Address.....: ::
   IPv4 Address.....: 192.168.1.2
   Subnet Mask.....: 255.255.255.0
   Default Gateway.....: ::
                                 192.168.1.1

Bluetooth Connection:

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: ::
   IPv6 Address.....: ::
   IPv4 Address.....: 0.0.0.0
   Subnet Mask.....: 0.0.0.0
   Default Gateway.....: ::
                                 0.0.0.0

C:\>ping 192.168.3.2

Pinging 192.168.3.2 with 32 bytes of data:

Reply from 192.168.3.2: bytes=32 time=21ms TTL=125
Reply from 192.168.3.2: bytes=32 time=21ms TTL=125
Reply from 192.168.3.2: bytes=32 time=13ms TTL=125
Reply from 192.168.3.2: bytes=32 time=12ms TTL=125

Ping statistics for 192.168.3.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 12ms, Maximum = 21ms, Average = 16ms

C:\>
```

Εικόνα 30: Επιτυχής επικοινωνία PC-A με PC-C



Εικόνα 31: Επιτυχής επικοινωνία PC-C με PC-A

6.4.2 IPS Configuration

Η υλοποίηση ξεκινάει ενεργοποιώντας το IOS του IPS στο R1, καθώς το εσωτερικό δίκτυο του router R1 θα προστατευτεί από το IPS. Η ενεργοποίηση αφορά τη δημιουργία χώρου αποθήκευσης για τα signatures του IPS, τη δημιουργία κανόνων καθώς και την ενεργοποίηση της καταγραφής των συμβάντων:

```
# Configuration on R1
      mkdir ipsdir
      ip ips config location flash:ipsdir
      ip ips name iosips
      ip ips notify log
      clock set 10:20:00 10 january 2023
      service timestamps log datetime msec
      logging host 192.168.1.50
```

Εν συνεχεία διαμορφώνεται το IPS ώστε να χρησιμοποιήσει τις κατηγορίες των signatures:

```
# Configuration on R1
      ip ips signature-category
      category all
      retired true
      category ios_ips basic
      retired false
      interface g0/1
      ip ips iosips out
```

Επόμενο βήμα είναι η παραμετροποίηση των signatures:

```
# Configuration on R1
      ip ips signature-definition
      signature 2004 0
      status
      retired false
      enabled true
      engine
      event-action produce-alert
      event-action deny-packet-inline
```

Στη παρακάτω εικόνα παρουσιάζεται η τελική διαμόρφωση και παραμετροποίηση του IPS:

```
R1#show ip ips all
IPS Signature File Configuration Status
    Configured Config Locations: flash:ipsdir
    Last signature default load time:
    Last signature delta load time:
    Last event action (SEAP) load time: -none-

    General SEAP Config:
    Global Deny Timeout: 3600 seconds
    Global Overrides Status: Enabled
    Global Filters Status: Enabled

IPS Auto Update is not currently configured

IPS Syslog and SDEE Notification Status
    Event notification through syslog is enabled
    Event notification through SDEE is enabled

IPS Signature Status
    Total Active Signatures: 1
    Total Inactive Signatures: 0

IPS Packet Scanning and Interface Status
    IPS Rule Configuration
      IPS name iosips
    IPS fail closed is disabled
    IPS deny-action ips-interface is false
    Fastpath ips is enabled
    Quick run mode is enabled
    Interface Configuration
      Interface GigabitEthernet0/1
        Inbound IPS rule is not set
        Outgoing IPS rule is iosips

IPS Category CLI Configuration:
    Category all
            Retire: True
    Category ios_ips basic
            Retire: False
R1#
```

Εικόνα 32: IPS Configuration – CLI view

Στο σημείο αυτό η υλοποίηση έχει ολοκληρωθεί επιτυχώς.

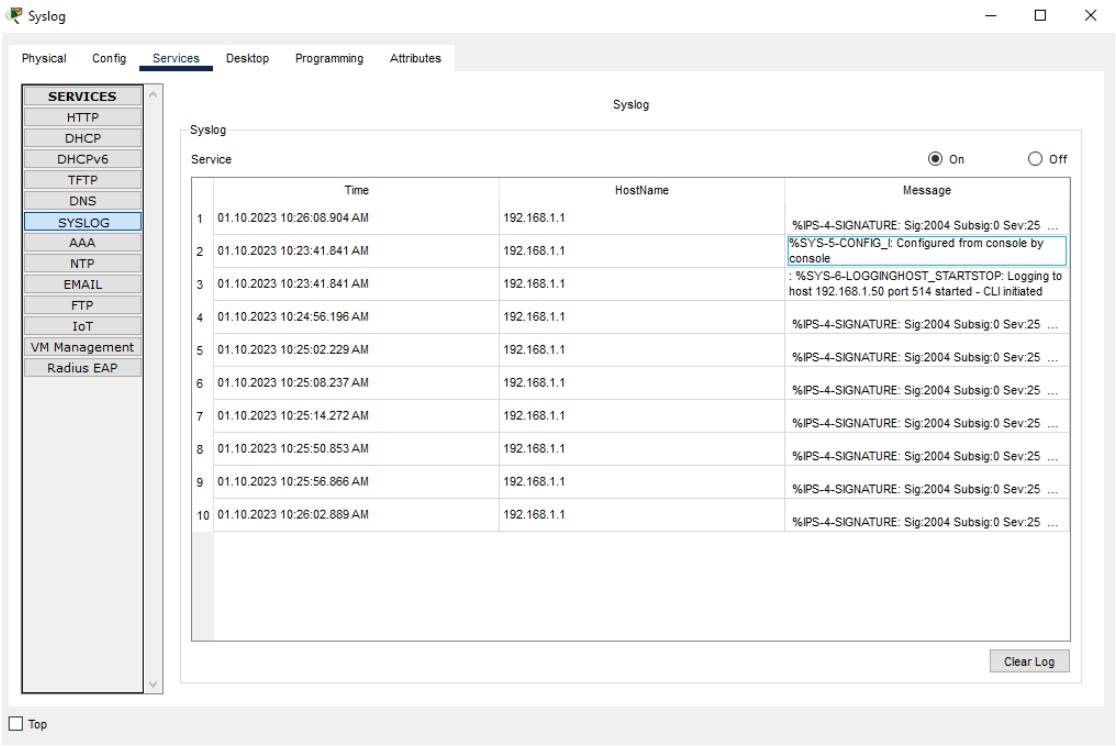
6.4.3 Επαλήθευση Λειτουργικότητας Υλοποίησης

Όπως παρουσιάζεται στις παρακάτω εικόνες, ενώ ο host PC-A συνεχίζει να βλέπει και να επικοινωνεί με τον PC-C, ο PC-C δεν μπορεί να επικοινωνήσει με τον PC-A, καθώς η εισερχόμενη κίνηση στο υποδίκτυο 192.168.1.0/24 μπλοκάρεται από το IPS στο R1:

```
C:\>ipconfig

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: FE80::207:ECFF:FE97:716E
   IPv6 Address.....: ::
   IPv4 Address.....: 192.168.3.2
   Subnet Mask.....: 255.255.255.0
   Default Gateway.....: ::
                                 192.168.3.1

Bluetooth Connection:

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: ::
   IPv6 Address.....: ::
   IPv4 Address.....: 0.0.0.0
   Subnet Mask.....: 0.0.0.0
   Default Gateway.....: ::
                                 0.0.0.0

C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Εικόνα 33: Το IPS μπλοκάρει την κίνηση στο εσωτερικό υποδίκτυο

Επίσης, τα συμβάντα αυτά καταγράφονται επιτυχώς και παρουσιάζονται στο Syslog Server:



Εικόνα 34: Syslog Events

7 Συμπεράσματα

Στην παρούσα διπλωματική εργασία μελετήθηκε ο ρόλος των Προσομοιωτών Δικτύων στην Ασφάλεια στον Κυβερνοχώρο και πιο συγκεκριμένα στην Ασφάλεια των Δικτύων καθώς και τη σημασία τους στη δοκιμή και την αξιολόγηση των μέτρων ασφαλείας. Η έρευνα έδειξε ότι οι προσομοιωτές δικτύου παρέχουν μια αποτελεσματική και οικονομικά αποδοτική μέθοδο για την προσομοίωση της συμπεριφοράς του δικτύου και ότι αποτελούν πολύτιμα εργαλεία για τους ερευνητές και τους επαγγελματίες της ασφάλειας για την αξιολόγηση των τρωτών σημείων, τον εντοπισμό πιθανών απειλών και τη δοκιμή των ελέγχων ασφαλείας. Με τη χρήση προσομοιωτών δικτύου, οι οργανισμοί μπορούν να ενισχύσουν τα επίπεδα ασφαλείας τους, να μειώσουν την έκθεση ή τον κίνδυνο κυβερνοεπιθέσεων και να αυξήσουν την αποτελεσματικότητα των μέτρων που έχουν ήδη παρθεί. Προσδιορίστηκαν επίσης διάφοροι τύποι προσομοιωτών δικτύου που είναι διαθέσιμοι και τα συγκεκριμένα χαρακτηριστικά και τις δυνατότητές τους.

Πέραν της βιβλιογραφικής προσέγγισης στα ζητήματα της ασφάλειας και των προσομοιωτών δικτύου, παρουσιάστηκαν και διάφορα σενάρια σχετικά της ασφάλειας δικτύων. Στο πρώτο μέρος παρουσιάστηκε η θεωρητική τους προσέγγιση και εν συνεχεία η μελέτη προχώρησε στην υλοποίησή τους με τη χρήση του προσομοιωτή δικτύων Cisco Packet Tracer, έναν προσομοιωτή ελεύθερα διαθέσιμο στους επαγγελματίες του χώρου της ασφάλειας. Στόχος των υλοποιήσεων αυτών ήταν η εφαρμογή των σεναρίων με στόχο την δημιουργία περιβάλλοντος για την αποφυγή δικτυακών επιθέσεων. Κατά την πραγματοποίηση των προσομοιώσεων αυτών εξήχθησαν χρήσιμα συμπεράσματα.

Αρχικά, μέσω της επιτυχούς υλοποίησης του IPsec VPN Tunneling παρουσιάστηκε πως, παραμετροποιώντας κατάλληλα τον εξοπλισμό μας, μπορούμε να συνδέσουμε απομακρυσμένα δύο διαφορετικές περιοχές με ασφάλεια, κρυπτογραφημένα, διασφαλίζοντας έτσι την εμπιστευτικότητα και την ακεραιότητα της πληροφορίας κατά την μετάδοσή της.

Εν συνεχεία, μέσω της υλοποίησης του Zone-Based Policy Firewall, μελετήθηκε πως μία υποδομή ενός μεγάλου οργανισμού, μπορεί να χωριστεί σε ζώνες αναλόγως τα πρόσωπα ενδιαφέροντος. Με τον τρόπο αυτό δύναται να ελεγχθεί η ροή της κίνησης σε συγκεκριμένες ζώνες, συνεισφέροντας έτσι στην αυθεντικοποίηση, καθώς συγκεκριμένοι χρήστες, από συγκεκριμένες ζώνες έχουν πρόσβαση σε συγκεκριμένες ζώνες ενδιαφέροντος.

Το ίδιο αποτέλεσμα επετεύχθη και μέσω της υλοποίησης των IP Access Control Lists, καθώς και σε αυτή την περίπτωση οι IP λίστες ελέγχου πρόσβασης ήλεγξαν την κίνηση και παρείχαν εξουσιοδοτημένη πρόσβαση σε υπηρεσίες, μόνο σε συγκεκριμένους και εξουσιοδοτημένους χρήστες.

Τέλος, μέσω της προσομοίωσης της λύσης ασφάλειας Intrusion Prevention System, μελετήσαμε όχι μόνο πως μπορεί να αποκλειστεί η πρόσβαση σε συγκεκριμένα δίκτυα από μη εγκεκριμένους ή εξουσιοδοτημένους χρήστες, αλλά και το πως οποιαδήποτε παραβίαση κάποιας πολιτικής ασφάλειας μπορεί να καταγραφεί ακαριαία και είτε να σταλθεί κάποια ειδοποίηση με σκοπό την αντιμετώπιση του περιστατικού (incidence response) είτε να μείνει αποθηκευμένη και διαθέσιμη για κάποια μελλοντική μελέτη περιστατικού παραβίασης (digital forensics).

Εν κατακλείδι, η εργασία αυτή κατέδειξε την σημασία της ασφάλειας δικτύων στην σύγχρονη εποχή καθώς και την αναγκαιότητα της. Κατέδειξε όμως και τη χρησιμότητα των προσομοιωτών δικτύου καθώς προσφέρουν την δυνατότητα πραγματοποίησης δοκιμών σε μη παραγωγικά περιβάλλοντα όπου θα υπάρχει κίνδυνος διακοπής υπηρεσίας, καθώς και

την δυνατότητα που δίνεται σε ερευνητές να μελετήσουν διάφορα σενάρια υλοποίησης νέων τεχνολογιών και λύσεων, με στόχο πάντα την αποφυγή των δικτυακών επιθέσεων.

8 Βιβλιογραφικές Αναφορές

[1] M. Ciampa, Security + Guide to Network Security Fundamentals, Boston, MA 02210, USA: Course Technology, 2011.

[2] M. Howard and J. Whittaker , "Network Security Basics," *IEEE Security & Privacy,* pp. 68-72, November - December 2005.

[3] M. Bishop, Computer Security Art and Science, Pearson Education, 2003.

[4] J. E. Canavan, Fundamentals od Network Security, Artech House, 2001.

[5] B. Daya, Network Security: History, Importane and Future, Florida: University of Florida Department of Electrical and Computer Engineering , 2013.

[6] M. Pawar and A. Anuradha, "Network Security and Types of Attacks in Network," in *International Conference on Intelligent Computing, Communication & Convergence*, Bhubaneswar, Odisha, India, 2015.

[7] E. Breslau, D. Estrin, K. Fall, S. Floyd, A. Helmy and Xa Xu, "Advances in network simulation," *Compter,* pp. 59-67, May 2000.

[8] E. Weingartner, H. vom Lehn and K. Wehrle, "A Performance Comparison of Recent Network Simulators," in *IEEE International Conference on Communications*, Dresden, Germany, 2009.

[9] Cisco, «Cisco Packet Tracer Data Sheet,» [Ηλεκτρονικό]. Available: https://www.cisco.com/c/dam/en_us/training-events/netacad/course_catalog/docs/Cisco_PacketTracer_DS.

[10] "GNS3," [Online]. Available: https://docs.gns3.com/.

[11] "EVE-NG," [Online]. Available: https://www.eve-ng.net/index.php/documentation/.

[12] "ns-3," [Online]. Available: https://www.nsnam.org/documentation/.

[13] T. Henderson, M. Lacage and G. Riley, "Network Simulations with the ns-3 Simulator," in *SIGCOMM'08*, Seattle, Washington, USA, 2008.

[14] "Mininet Walkthrough," [Online]. Available: http://mininet.org/walkthrough/.

[15] "OMNeT++," [Online]. Available: https://omnetpp.org/documentation/.

[16] "Boson," [Online]. Available: http://www.boson.com/files/support/netsim-8-user-manual.pdf.

[17] B. Chawla, O P Gupta and B.K. Sawhney, "A Review on IPsec and SSL VPN," *International Journal of Scientific and Engineering Research,* November 2014.

[18] Weimin Gan και Xiaogui Yin, «Research on high security of IP tunnel in virtual,» 2021.

[19] Valerianus Hashiyana, Titus Haiduwa, Aubrey Bratha and Nalina Suresh, "Design and Implementation of an IPSec Virtual Private Network," in *Conference: 2020 IST-Africa COnferenceAt: Uganda*, Namibia, 2020.

[20] "Cisco.com," 28 Septenber 2022. [Online]. Available: https://www.cisco.com/c/en/us/support/docs/security/ios-firewall/98628-zone-design-guide.html.

[21] Alnuman Mohammed Abubaker Altamezwi, Abdulwahed Omran E Alalwani and Ashour Alsllami, "Comparing Context Based Access Control to Zonebased Policy Firewalls," *International Journal for Research in Applied Science & Engineering Technology (IJRASET),* pp. 1215-1222, June 2022.

[22] S. Pozo, A.J. Varela-Vaca and R.M. Gasca, "A quadratic, complete, and minimal consistency diagnosis process for firewall acls," in *24th IEEE International Conference*, 2010.

[23] Sharat Kaushik, Anita Tomar and Poonam, "Access Control List Implementation in a Private Network," *International Journal of Information & Computation Technology,* pp. 1361-1366, 14 November 2014.

[24] Shipra Suman and Er. Aditi Agrawal, "IP Traffic Management With Access Control List Using Cisco Packet Tracer," *International Journal of Science, Engineering and Technology Research (IJSETR,* May 2016.

[25] Karen Scarfone και Peter Mell, Guide to Intrusion Detection and Prevention Systems (IDPS), NIST, 2007.

[26] S. Axelsson, "Research in Intrusion-Detection Systems: A Survey," Chalmers University of Technology, G• oteborg, Sweden, 1999.