ΔΙΕΘΝΕΣ
ΠΑΝΕΠΙΣΤΗΜΙΟ
ΤΗΣ ΕΛΛΑΔΟΣ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ,
ΥΠΟΛΟΓΙΣΤΩΝ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

ΜΕΤΑΠΤΥΧΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΣΤΙΣ
ΤΗΛΕΠΙΚΟΙΝΩΝΙΕΣ ΚΑΙ ΔΙΚΤΥΑ Η/Υ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

«ΣΚΛΗΡΥΝΣΗ ΔΙΚΤΥΑΚΩΝ ΣΥΣΚΕΥΩΝ»

Του φοιτητή
Διαμαντή Αριστοτέλη
Αρ. Μητρώου: 19

Επιβλέπων
Πολίτης Αναστάσιος
Επίκουρος καθηγητής

Φεβρουάριος 2024

Σκλήρυνση Δικτυακών Συσκευών
Κωδικός Δ.Ε. …
Αριστοτέλης Διαμαντής
Αναστάσιος Πολίτης
Ημερομηνία ανάληψης Δ.Ε. …
Ημερομηνία περάτωσης Δ.Ε. …

Βεβαιώνω ότι είμαι ο συγγραφέας αυτής της εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της είναι πλήρως αναγνωρισμένη και αναφέρεται στην εργασία. Επίσης, έχω καταγράψει τις όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών, εικόνων και κειμένου, είτε αυτές αναφέρονται ακριβώς είτε παραφρασμένες. Επιπλέον, βεβαιώνω ότι αυτή η εργασία προετοιμάστηκε από εμένα προσωπικά, ειδικά ως διπλωματική εργασία, στο Τμήμα Μηχανικών Πληροφορικής και Ηλεκτρονικών Συστημάτων του ΔΙ.ΠΑ.Ε.

Η παρούσα εργασία αποτελεί πνευματική ιδιοκτησία του φοιτητή Αριστοτέλη Διαμαντή που την εκπόνησε. Στο πλαίσιο της πολιτικής ανοικτής πρόσβασης, ο συγγραφέας/δημιουργός εκχωρεί στο Διεθνές Πανεπιστήμιο της Ελλάδος άδεια χρήσης του δικαιώματος αναπαραγωγής, δανεισμού, παρουσίασης στο κοινό και ψηφιακής διάχυσης της εργασίας διεθνώς, σε ηλεκτρονική μορφή και σε οποιοδήποτε μέσο, για διδακτικούς και ερευνητικούς σκοπούς, άνευ ανταλλάγματος. Η ανοικτή πρόσβαση στο πλήρες κείμενο της εργασίας, δεν σημαίνει καθ' οιονδήποτε τρόπο παραχώρηση δικαιωμάτων διανοητικής ιδιοκτησίας του συγγραφέα/δημιουργού, ούτε επιτρέπει την αναπαραγωγή, αναδημοσίευση, αντιγραφή, πώληση, εμπορική χρήση, διανομή, έκδοση, μεταφόρτωση (downloading), ανάρτηση (uploading), μετάφραση, τροποποίηση με οποιονδήποτε τρόπο, τμηματικά ή περιληπτικά της εργασίας, χωρίς τη ρητή προηγούμενη έγγραφη συναίνεση του συγγραφέα/δημιουργού.

Η έγκριση της διπλωματικής εργασίας από το Τμήμα Μηχανικών Πληροφορικής και Ηλεκτρονικών Συστημάτων του Διεθνούς Πανεπιστημίου της Ελλάδος, δεν υποδηλώνει απαραιτήτως και αποδοχή των απόψεων του συγγραφέα, εκ μέρους του Τμήματος.

Πρόλογος

Επέλεξα να ερευνήσω το θέμα της σκλήρυνσης δικτυακών συσκευών λόγω της σημασίας της για την ασφάλεια και τη λειτουργικότητα των δικτύων. Καθώς η τεχνολογία εξελίσσεται, οι απειλές στην κυβερνοασφάλεια αυξάνονται, και είναι αναγκαίο να αναβαθμίσουμε την προστασία των δικτύων. Μέσω αυτής της διπλωματικής, είχα την ευκαιρία να εξερευνήσω τις τεχνικές και τις διαδικασίες για την ενίσχυση της ασφάλειας στις δικτυακές συσκευές, συμβάλλοντας έτσι στην καλύτερη κατανόηση και προστασία των δικτύων επικοινωνιών. Η εμβάθυνση σε αυτό το θέμα με βοήθησε να αναδείξω τη σημασία της προληπτικής αντίδρασης έναντι των κυβερνοεπιθέσεων και των απειλών, ενώ παράλληλα είχα την ευκαιρία να επεκτείνω τις τεχνικές μου γνώσεις στον τομέα της δικτυακής ασφάλειας. Αυτή η εμπειρία μου προσέφερε επίσης τη δυνατότητα να αναπτύξω δεξιότητες που με βοήθησαν όχι μόνο στις σπουδές μου αλλά και στην επαγγελματική μου πορεία.

Περίληψη

Η εργασία εστιάζει στη μελέτη και στην πρόταση ενεργειών σχετικά με την σκλήρυνση των δικτυακών συσκευών με σκοπό τη μεγαλύτερη ασφάλεια των συσκευών από τυχόν κυβερνοεπιθέσεις από κακόβουλους χρήστες. Η εργασία είναι χωρισμένη σε τρείς ενότητες. Η πρώτη ενότητα αναφέρεται στους ενδεχόμενους κινδύνους και στις αδυναμίες που μπορεί να έχει μια δικτυακή συσκευή. Επίσης σε κάθε πιθανό κίνδυνο παρουσιάζεται και μια προτεινόμενη ενέργεια προκειμένου να μετριαστεί ο κίνδυνος. Η δεύτερη ενότητα λειτουργεί ως εγχειρίδιο παραμετροποίησης μιας δικτυακής συσκευής. Οι συσκεύες που αναλύονται είναι ο δρομολογητής (router) και ο μεταγωγέας (switch) οι οποίες είναι της εταιρείας Cisco. Τέλος , στην τρίτη ενότητα αναπτύσσεται και ελέγχεται ένας κώδικας σε γλώσσα προγραμματισμού Python ο οποίος αυτοματοποιεί κάποιες παραμετροποιήσεις που αναλύονται στην δεύτερη ενότητα.

«NETWORK DEVICE HARDENING»

«Aristotelis Diamantis»

Abstract

The thesis focuses on studying and proposing actions regarding the hardening of network devices to enhance their security against potential cyberattacks by malicious users. The thesis is divided into three sections. The first section deals with the possible risks and vulnerabilities that a network device may have. Also, for each potential risk, a suggested action is presented to mitigate it. The second section serves as a configuration manual for a network device. The devices analyzed are the router and the switch, both from Cisco. Finally, the third section develops and tests a Python programming language code that automates some of the configurations discussed in the second section.

Ευχαριστίες

Θα ήθελα θερμά να ευχαριστήσω όλους όσους συνέβαλαν στην ολοκλήρωση αυτής της διπλωματικής εργασίας. Καταρχάς, θέλω να εκφράσω την ευγνωμοσύνη μου προς τον κ. Αναστάσιο Πολίτη για την υποστήριξή του κατά τη διάρκεια αυτής της διαδικασίας. Τέλος, ευχαριστώ την οικογένειά μου και τους φίλους μου για τη στήριξη και την κατανόησή τους κατά τη διάρκεια αυτής της πορείας. Η συνεισφορά και η υποστήριξή σας ήταν ανεκτίμητη και με βοήθησε να φτάσω στο τέλος αυτού του σημαντικού ταξιδιού. Ευχαριστώ θερμά.

Περιεχόμενα

Συντομογραφίες

I.S.P.	Internet Service Provider
D.M.Z.	Demilitarized Zone
V.L.A.N.	Virtual Local Area Network
A.C.L.	Access Control List
V.P.N.	Virtual Private Network
I.P.S.	Intrusion Prevention System
D.o.S.	Denial of Service
A.A.A.	Authentication, Authorization, and Accounting
S.SH.	Secure Shell
H.T.T.P.	Hypertext Transfer Protocol
F.T.P.	File Transfer Protocol
S.N.M.P.	Simple Network Management Protocol
A.E.S.	Advanced Encryption Standard
E.C.D.S.A.	Elliptic Curve Digital Signature Algorithm
S.H.A.	Secure Hash Algorithm
T.C.P.	Transmission Control Protocol
U.D.P.	User Datagram Protocol
C.D.P.	Cisco Discovery Protocol
L.L.D.P.	Link Layer Discovery Protocol
I.P.	Internet Protocol
u.R.P.F.	Unicast Reverse Path Forwarding
C.L.I.	Command Line Interface
N.T.P.	Network Time Protocol

Κεφάλαιο 1ο: Ανάλυση κινδύνων κυβερνοασφάλειας και προτεινόμενες λύσεις μετριασμού.

1.1 Εισαγωγή

Λόγω της αυξημένης χρήσης συσκευών που συνδέονται στο διαδίκτυο, επιβάλλεται η ενίσχυση της διαδικτυακής ασφάλειας ενάντια σε απειλές από κακόβουλους χρήστες, οι οποίοι επιδιώκουν να εκμεταλλευτούν ευπάθειες του συστήματος. Ένας κλάδος που αναμφίβολα πρέπει να ενισχυθεί και να ασφαλιστεί είναι οι δικτυακές συσκευές (δρομολογητές, μεταγωγείς, τείχη προστασίας (firewalls) κλπ.), οι οποίες αποτελούν την ραχοκοκαλιά του διαδικτύου. Η διαδικασία ασφάλειας των συσκευών, γνωστή ως "σκλήρυνση δικτυακών συσκευών", αποσκοπεί στην ελαχιστοποίηση του κινδύνου μη εξουσιοδοτημένης πρόσβασης στην υποδομή του δικτύου. Τα ευάλωτα σημεία στη διαχείριση και τις παραμετροποιήσεις των συσκευών παρουσιάζουν αδυναμίες που μπορούν να εκμεταλλευτούν από κακόβουλους διαδικτυακούς επιτιθέμενους, με σκοπό να εισέλθουν και να διατηρήσουν παρουσία σε ένα δίκτυο.

1.2 Zero Trust Model

Τα παραδοσιακά μοντέλα διαχείρισης δικτύων χαρακτηρίζονται από απόλυτη εμπιστοσύνη προς τους εσωτερικούς χρήστες του δικτύου, ενώ παράλληλα είναι αυστηρά ως προς την πρόσβαση για τους εξωτερικούς (εκτός δικτύου). Βασίζονται στην έννοια ενός "κάστρου με τάφρο", καθιστώντας δύσκολη την πρόσβαση εξωτερικών χρηστών, ειδικά εκείνων που μπορεί να είναι κακόβουλοι. Στο αντίθετο άκρο, το μοντέλο μηδενικής εμπιστοσύνης αποτελεί μια προσέγγιση κυβερνοασφάλειας που τονίζει την ανάγκη συνεχούς αξιολόγησης της εμπιστοσύνης. Η αρχιτεκτονική αυτή αποτελεί ολοκληρωμένη προσέγγιση για την ασφάλεια των πόρων και των δεδομένων της επιχείρησης, περιλαμβάνοντας ταυτοποίηση, διαχείριση διαπιστευτηρίων, διαχείριση πρόσβασης και άλλες λειτουργίες ασφαλείας. Η πρωταρχική εστίαση συνίσταται στον περιορισμό των προνομίων πρόσβασης μόνο στους απαραίτητους πόρους για την εκτέλεση των καθηκόντων.

1.2.1 Αρχιτεκτονική μηδενικής εμπιστοσύνης

Μια αρχιτεκτονική μηδενικής εμπιστοσύνης θα πρέπει να σχεδιάζεται και να εφαρμόζεται με βάση τις ακόλουθες βασικές αρχές:

- Όλες οι πηγές δεδομένων και οι υπηρεσίες υπολογιστών θεωρούνται πόροι.
- Η ασφάλεια της επικοινωνίας πρέπει να διασφαλίζεται ανεξάρτητα από την τοποθεσία στο δίκτυο.
- Η πρόσβαση σε πόρους πρέπει να παρέχεται ανά συνεδρία.
- Η πρόσβαση στους πόρους πρέπει να καθορίζεται από μια δυναμική πολιτική, λαμβάνοντας υπόψη την ταυτότητα του χρήστη, την εφαρμογή/υπηρεσία που ζητεί και άλλες παραμέτρους συμπεριφοράς.

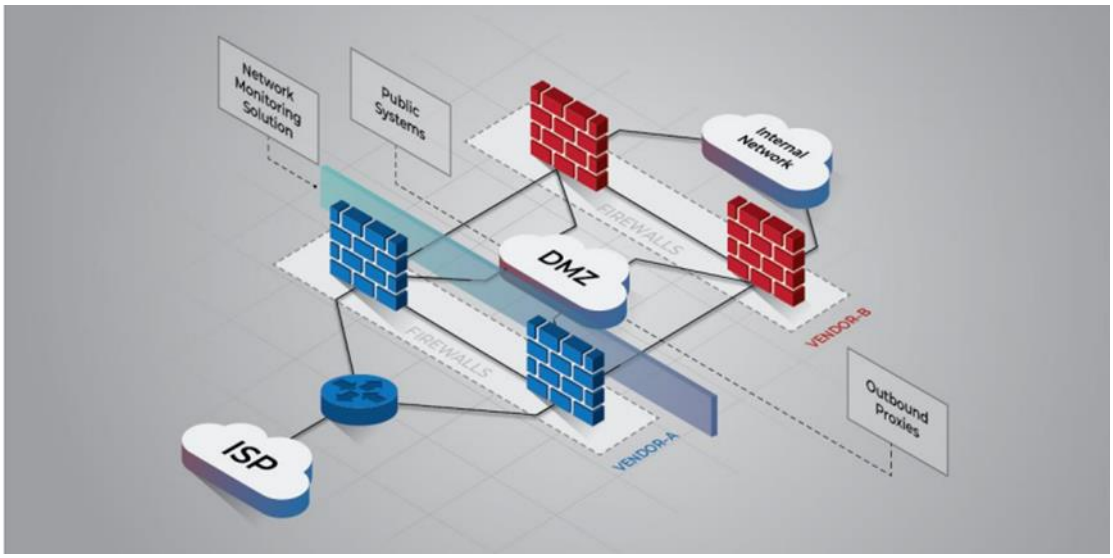
- Η ακεραιότητα και η ασφάλεια των δεδομένων πρέπει να παρακολουθείται και να μετράται.
- Όλοι οι έλεγχοι ταυτότητας και η εξουσιοδότηση πρέπει να είναι δυναμικοί και αυστηροί προτού επιτραπεί η πρόσβαση.
- Πρέπει να συλλέγονται όσο το δυνατόν περισσότερες πληροφορίες σχετικά με την τρέχουσα κατάσταση της υποδομής του δικτύου.

Ένα δίκτυο που αναπτύσσεται βάσει των παραπάνω αρχών της μηδενικής εμπιστοσύνης θα πρέπει να λαμβάνει υπόψη του και τις παρακάτω παραδοχές:

- Δεν θεωρείται ολόκληρο το ιδιωτικό δίκτυο ενός οργανισμού ως "σιωπηρή ζώνη εμπιστοσύνης".
- Οι συσκευές του δικτύου μπορεί να μην ανήκουν όλες στον ίδιο οργανισμό.
- Κανένας πόρος δεν είναι εγγενώς αξιόπιστος.
- Δεν υπάρχουν όλοι οι πόροι του οργανισμού σε υποδομές που ανήκουν στον ίδιο οργανισμό.
- Τα στοιχεία του οργανισμού που βρίσκονται απομακρυσμένα δεν μπορούν να εμπιστευτούν πλήρως το τοπικό δίκτυο στο οποίο συνδέονται.
- Στα στοιχεία και στις ροές εργασίας που κινούνται μεταξύ υποδομών που ανήκουν και δεν ανήκουν στον οργανισμό, πρέπει να εφαρμόζεται μια σταθερή πολιτική ασφαλείας.

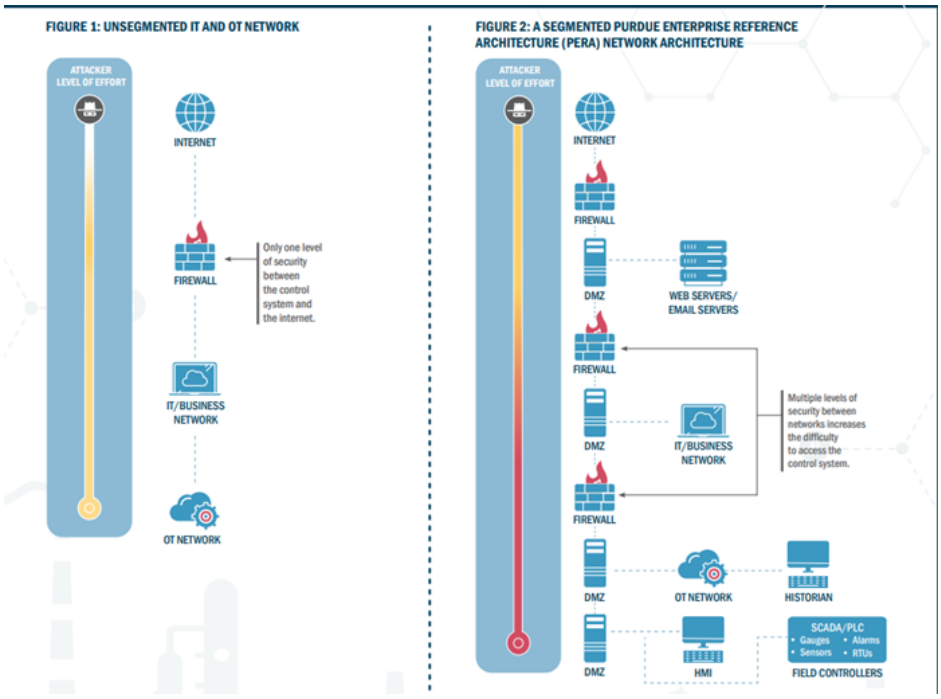
1.3 Αρχιτεκτονική Δικτύου και Σχεδιασμός

Για να υπάρχει ένα ασφαλές δίκτυο και να είναι ανθεκτικό απέναντι σε διάφορες απειλές, είναι απαραίτητο ο σχεδιασμός να ακολουθεί τις απαιτούμενες πρακτικές ασφάλειας τόσο στις περιμετρικές συσκευές του δικτύου όσο και στις εσωτερικές. Είναι αναγκαίο να εφαρμοστούν πολλαπλά επίπεδα άμυνας με σκοπό την προστασία ενάντια στις εξωτερικές απειλές, την παρακολούθηση και την απόρριψη της εσωτερικής ή εξωτερικής κίνησης. Ειδικότερα, προτείνεται η εγκατάσταση ενός συνοριακού router με σκοπό τη σύνδεση σε ένα εξωτερικό δίκτυο (π.χ. ISP). Επίσης, η εγκατάσταση πολλαπλών επιπέδων με firewalls, ώστε να περιοριστεί η εισερχόμενη ή εξερχόμενη κίνηση και να εξετάζεται η δραστηριότητα μεταξύ των διάφορων περιοχών μέσα στο δίκτυο. Μια πρακτική ενίσχυσης της ασφάλειας του δικτύου είναι η τοποθέτηση συστημάτων που έχουν δημόσια πρόσβαση και η χρήση των proxies για την εξυπηρέτηση της εξερχόμενης κίνησης, ανάμεσα στα επίπεδα των firewalls. Έτσι δημιουργείται μια αποστρατικοποιημένη ζώνη (DMZ) όπου η πρόσβαση μεταξύ των εξωτερικών συσκευών, των DMZ συσκευών και του εσωτερικού συστήματος ελέγχεται κατάλληλα. Επιπλέον σημαντική είναι και η ανάπτυξη εξυπηρετητών ώστε να γίνεται καταγραφή των αιτημάτων τόσο της εξερχόμενης όσο και της εισερχόμενης κίνησης. Είναι θεμιτό τα firewalls που τοποθετούνται να είναι διαφορετικών κατασκευαστών. Στην παρακάτω εικόνα φαίνεται ένα σχεδιάγραμμα της παραπάνω αρχιτεκτονικής.



Εικόνα 1 Αρχιτεκτονική δικτύου με DMZ

Ένας κακόβουλος χρήστης θα αναζητήσει και θα επιτεθεί σε ένα σύστημα που είναι γενικά ευπρόσβλητο για εκείνον, όπως για παράδειγμα ένας εκτυπωτής που βρίσκεται στο δίκτυο. Χρησιμοποιώντας αυτήν την αρχική πρόσβαση, θα εισβάλει στο υπόλοιπο δίκτυο. Για να αντιμετωπιστεί αυτή η απειλή, το δίκτυο θα πρέπει να διακριθεί σε τμήματα. Για παράδειγμα, ένα σύστημα ελέγχου μιας βιομηχανίας θα πρέπει να είναι απομονωμένο από συστήματα που αποτελούν πιθανούς κινδύνους, όπως το παγκόσμιο διαδίκτυο. Αυτή η διάκριση μπορεί να επιτευχθεί είτε με τη δημιουργία υποδικτύων ή εικονικών τοπικών δικτύων (VLANs), είτε με τη χρήση firewalls για τον διαχωρισμό τους. Όπως φαίνεται και στο παρακάτω παράδειγμα, ένας κακόβουλος χρήστης θα πρέπει να καταβάλει πολύ μεγαλύτερη προσπάθεια σε ένα δίκτυο που είναι διακριτικά διαχωρισμένο σε τμήματα, σε σύγκριση με ένα δίκτυο που δεν έχει υποστεί τέτοιο διαχωρισμό.



Εικόνα 2 Παρουσίαση της προσπάθειας που πρέπει να καταβάλει ένας χρήστης για την εισβολή σε ένα μη τμηματοποιημένο και σε ενα τμηματοποιημένο δίκτυο

Κάποιες φορές, ένας επιβλαβής χρήστης ενδέχεται να προσπαθήσει να αξιοποιήσει μια σύνδεση που λειτουργεί ως κρυφή πύλη (backdoor). Μια τέτοια σύνδεση παρουσιάζεται, για παράδειγμα, όταν ένας συνοριακός δρομολογητής συνδέεται απευθείας με τον πάροχο υπηρεσιών Internet (ISP) και με ένα εσωτερικό υποδίκτυο. Αν επιτευχθεί πρόσβαση στον συνοριακό δρομολογητή, τότε ο κακόβουλος χρήστης αποκτά και πρόσβαση στο εσωτερικό δίκτυο, ανακατευθύνοντας την κυκλοφορία των δεδομένων παρά τους προστατευτικούς φραγμούς των firewalls. Επομένως, είναι απαραίτητο να αποκλειστούν τέτοιου είδους συνδέσεις προκειμένου να διασφαλιστεί η υψηλότερη δυνατή επίπεδο ασφάλειας.

Για την επίτευξη ακόμη μεγαλύτερης ασφάλειας και ενίσχυσης της ανθεκτικότητας του δικτύου, είναι απαραίτητο να εφαρμοστούν αυστηρές λίστες πρόσβασης (ACLs) στις περιμετρικές συσκευές. Αυτές οι ACLs πρέπει να επιτρέπουν μόνο την κίνηση και τις υπηρεσίες που είναι αναγκαίες για την υποστήριξη του σκοπού του εκάστοτε δικτύου. Μια αποτελεσματική προσέγγιση στην υλοποίηση των ACLs είναι η αρχή της προκαθορισμένης απόρριψης με την εξαίρεση. Αυτό σημαίνει ότι οι ACLs πρέπει να σχεδιάζονται έτσι ώστε να απορρίπτουν από προεπιλογή οποιαδήποτε κίνηση ή υπηρεσίες ζητούν πρόσβαση, εκτός από εκείνες που καθορίζονται με αυστηρότητα. Επιπλέον, είναι χρήσιμο να διατηρείται αρχείο καταγραφής για τις εγκεκριμένες και απορριφθείσες επικοινωνίες, προκειμένου να επιτυγχάνεται πλήρης επίγνωση της δικτυακής κυκλοφορίας και παρακολούθησης των δραστηριοτήτων του δικτύου.

Το Virtual Private Network (VPN) αναπαριστά ένα κρυπτογραφημένο δίαυλο επικοινωνίας μεταξύ δύο απομακρυσμένων σημείων, εγγυώντας την εμπιστευτικότητα και την ακεραιότητα των δεδομένων. Ωστόσο, η χρήση του πρέπει να προβλέπεται μόνο όταν έχουν διασφαλιστεί αυτά τα χαρακτηριστικά. Δεδομένου ότι τα VPN είναι προσβάσιμα μέσω του Διαδικτύου, εκτίθενται σε πολλούς κινδύνους, επομένως η χρήση τους πρέπει να περιορίζεται στις περιπτώσεις που είναι πραγματικά αναγκαία. Εκεί

όπου είναι δυνατό, πρέπει να επιτρέπεται μόνο η κίνηση που προέρχεται από γνωστές VPN συνδέσεις, ενώ σε περιπτώσεις που αυτό δεν είναι εφικτό, η εφαρμογή ενός Intrusion Prevention System (IPS) πριν από την πύλη του VPN επιτρέπει τον έλεγχο της κίνησης.

1.4 Ενδυνάμωση της Ασφάλειας Δικτύου

Για τη διασφάλιση της ασφάλειας ενός δικτύου, είναι απαραίτητο τόσο το υλικό όσο και το λογισμικό που χρησιμοποιούνται να διατηρούνται ενημερωμένα. Σε πολλές περιπτώσεις, το λογισμικό και το υλικό που έχουν απαρχαιωθεί ενδέχεται να παρουσιάζουν γνωστές ευπάθειες, κάτι που καθιστά ευκολότερη την εκμετάλλευσή τους από ανεπιθύμητους χρήστες. Η εντοπισμένη αδυναμία στο λογισμικό μπορεί να επιτρέψει σε κακόβουλους χρήστες να διεισδύσουν στο σύστημα, ενώ το κακόβουλο λογισμικό μπορεί να παρεμποδίσει την ακεραιότητα των δεδομένων, να διαρρεύσει ευαίσθητες πληροφορίες και να προκαλέσει διακοπή υπηρεσιών (DoS). Για την αποτροπή αυτών των καταστάσεων, είναι ουσιώδες να υιοθετηθεί πρακτική που να περιλαμβάνει τη σύγκριση του κρυπτογραφημένου hash των αρχείων συστήματος με αυτό που δημοσιεύει ο κατασκευαστής, προκειμένου να εξασφαλιστεί η ακεραιότητα του λογισμικού. Επιπλέον, είναι κρίσιμο να διατηρείται το λογισμικό ενημερωμένο, καθώς οι κατασκευαστές επιλύουν γνωστές αδυναμίες σε κάθε νέα έκδοση. Ως εκ τούτου, είναι σημαντικό να εγκαθίσταται η τελευταία σταθερή έκδοση του λογισμικού και να πραγματοποιούνται αυτόματες ενημερώσεις, όταν αυτό είναι εφικτό. Επιπλέον, η χρήση συσκευών που εξακολουθούν να υποστηρίζονται από τον κατασκευαστή είναι απαραίτητη, καθώς οι συσκευές που παραμένουν αναβαθμίσιμες διασφαλίζουν την παροχή υποστήριξης για τυχόν ζητήματα ασφάλειας και διατηρούν τη διαθεσιμότητα των υπηρεσιών του δικτύου. Όταν η υποστήριξη διακοπεί, η αντικατάσταση των συσκευών με νεότερες εκδόσεις αποτελεί αναπόφευκτη πρακτική για τη διατήρηση της ασφάλειας και της διαθεσιμότητας των υπηρεσιών δικτύου.

1.5 Αυθεντικοποίηση , Εξουσιοδότηση και Καταγραφή δικτυακών συσκευών

Η χρήση κεντρικών διακοσμητών για την αυθεντικοποίηση και την εξουσιοδότηση των χρηστών, καθώς και για την καταγραφή των αιτημάτων τους, αποτελεί κρίσιμη πρακτική στη διαχείριση πρόσβασης σε συστήματα πληροφορικής. Αυτή η προσέγγιση ενισχύει την ασφάλεια του συστήματος, καθώς δυσχεραίνει σημαντικά τη διείσδυση από επιτιθέμενους. Η παραμετροποίηση των κεντρικών διακοσμητών είναι ουσιαστική προκειμένου να επιτευχθεί βέλτιστη συνοχή και συνέπεια στον έλεγχο πρόσβασης, μείωση του κόστους συντήρησης και διαχείρισης, καθώς και ενίσχυση της αντοχής του συστήματος. Κατά συνέπεια, η χρήση ενιαίων διακοσμητών αυθεντικοποίησης, εξουσιοδότησης και καταγραφής (AAA servers) αποτελεί προτιμώμενη πρακτική.

Επιπλέον, η ύπαρξη τουλάχιστον δύο κεντρικών διακομιστών ενισχύει τη διαθεσιμότητα του συστήματος και βελτιώνει την ανίχνευση και πρόληψη επιθέσεων. Αυτός ο διπλός διακομιστής αρκεί για να αντιμετωπίσει απρόβλεπτες διακοπές λειτουργίας ενός εκ των δύο διακομιστών, εξασφαλίζοντας τη συνεχή λειτουργία του συστήματος. Συνεπώς, η εφαρμογή τουλάχιστον δύο κεντρικών διακομιστών αποτελεί πρακτική που συμβάλλει στην επίτευξη υψηλού επιπέδου ασφάλειας και αξιοπιστίας στη διαχείριση των προσβάσεων.

Η αυθεντικοποίηση αποτελεί τη διαδικασία επαλήθευσης της ταυτότητας ενός ατόμου ή μιας οντότητας σε ένα σύστημα πληροφορικής. Συνήθως, η αυθεντικοποίηση πραγματοποιείται μέσω κεντρικών διακομιστών, γνωστών ως AAA servers, οι οποίοι αναλαμβάνουν την πρωταρχική διαχείριση των

αιτημάτων αυθεντικοποίησης. Στην περίπτωση μη διαθεσιμότητας των κεντρικών διακομιστών, επιτρέπεται η τοπική αυθεντικοποίηση με βάση τις τοπικές ρυθμίσεις ασφαλείας.

Από την άλλη, η εξουσιοδότηση αφορά την επιβεβαίωση του δικαιώματος πρόσβασης ενός χρήστη ή μιας οντότητας σε συγκεκριμένους πόρους του συστήματος. Προκειμένου να διασφαλιστεί η ασφάλεια, συνιστάται η εφαρμογή της εξουσιοδότησης στην έναρξη κάθε συνεδρίας. Επιπλέον, προτείνεται η περιορισμένη εκχώρηση δικαιωμάτων σε εξουσιοδοτημένους διαχειριστές, με σκοπό την αποτροπή ανεπιθύμητων ενεργειών από λογαριασμούς που ενδέχεται να έχουν παραβιαστεί ή καταχρηστικά χρησιμοποιηθεί.

Η διαδικασία της καταγραφής δημιουργεί αρχεία καταγραφής που περιλαμβάνουν τις ενέργειες και τις προσπελάσεις που έχουν λάβει χώρα σε ένα σύστημα πληροφορικής. Εν προκειμένω, είναι αναγκαίο η κάθε αλλαγή στις παραμέτρους μιας συσκευής να καταγράφεται στους κεντρικούς διακομιστές ΑΑΑ. Με αυτόν τον τρόπο, επιτυγχάνεται η δυνατότητα εντοπισμού ενδεχόμενων ύποπτων δραστηριοτήτων. Συνιστάται η καταγραφή των ενεργειών σε επίπεδο συνεδρίας, δηλαδή κατά την έναρξη και το τέλος μιας συνεδρίας, καθώς και κατά την έναρξη και το τέλος μιας εντολής κελύφους. Με αυτόν τον τρόπο, διασφαλίζεται η πληρέστερη και συστηματική καταγραφή των ενεργειών, προσφέροντας ταυτόχρονα μία πληρέστερη εικόνα της διαχείρισης και της ασφάλειας του συστήματος.

Ένα σημαντικό μέτρο ασφαλείας που αξίζει να εξεταστεί είναι η εφαρμογή του ελάχιστου προνομίου, το οποίο αναφέρεται στο ελάχιστο επίπεδο προνομίων που απαιτούνται για την εκτέλεση συγκεκριμένων ενεργειών. Πολλές καθημερινές ενέργειες, όπως η παρακολούθηση της κατάστασης των δικτυακών διεπαφών, δεν απαιτούν προνομιούχα πρόσβαση. Για την ενίσχυση της ασφάλειας, είναι σημαντικό να εφαρμόζεται το πρότυπο του ελάχιστου προνομίου και να επιβάλλεται η απαίτηση αυτού για την πρόσβαση των διαχειριστών στις συσκευές.

Επιπλέον, για την ενίσχυση της ασφάλειας, προτείνεται η θέσπιση ενός ορίου στον αριθμό των προσπαθειών σύνδεσης που επιτρέπονται από έναν χρήστη. Αυτό το μέτρο προστατεύει τη συσκευή από επιθέσεις "brute force", καταπολεμώντας την προσπάθεια ανεπιτυχούς σύνδεσης προκειμένου να αποκτηθεί πρόσβαση στο σύστημα.

1.6 Υιοθέτηση Τοπικής Διαχείρισης Λογαριασμών και Κωδικών Πρόσβασης

Σε περιπτώσεις αποτυχίας της κεντρικής αυθεντικοποίησης μέσω των ΑΑΑ servers, προτείνεται η εφαρμογή της τοπικής διαχείρισης λογαριασμών για την πρόσβαση στις συσκευές δικτύου. Αυτοί οι τοπικοί λογαριασμοί πρέπει να διαθέτουν μοναδικές και περίπλοκες κωδικούς πρόσβασης. Επιπλέον, είναι σημαντικό να καθοριστεί μια πολιτική για τους κωδικούς πρόσβασης, στην οποία θα ορίζονται οι κανόνες και οι διαδικασίες. Για παράδειγμα, οι προκαθορισμένοι κωδικοί πρόσβασης που παρέχονται από τον κατασκευαστή της συσκευής, τα οποία συνήθως είναι ευρέως γνωστοί και παρέχουν πλήρη πρόσβαση διαχείρισης, πρέπει να αναθεωρούνται. Επίσης, πρέπει να εφαρμόζονται αλγόριθμοι κρυπτογράφησης για την αποθήκευση των κωδικών πρόσβασης, ενώ είναι αναγκαίο να μην χρησιμοποιούνται οι ίδιοι κωδικοί για πολλές συσκευές. Τέλος, οι κωδικοί πρόσβασης πρέπει να πληρούν συγκεκριμένα κριτήρια για να θεωρηθούν ισχυροί, όπως:

- Χρήση συνδυασμού πεζών και κεφαλαίων γραμμάτων, αριθμών και ειδικών χαρακτήρων.
- Επιλογή κωδικού με τουλάχιστον 15 χαρακτήρες.
- Αποφυγή βάσης του κωδικού σε κοινές λέξεις ή φράσεις.
- Αποκλεισμός της ταυτότητας του χρήστη από τον κωδικό πρόσβασης.

- Αποφυγή συσχέτισης με προηγούμενους κωδικούς πρόσβασης.
- Αποφυγή κενών ή κοινών κωδικών που είναι ευρέως γνωστοί

Επιπλέον, προτείνεται η απενεργοποίηση των διαμοιραζόμενων λογαριασμών διαχείρισης που χρησιμοποιούνται από ομάδες διαχειριστών δικτύου, με κάθε διαχειριστή να διαθέτει έναν μοναδικό λογαριασμό. Αυτή η πρακτική διευκολύνει την καταγραφή και τον έλεγχο ύποπτων ενεργειών που ενδέχεται να θέλουν να διαταράξουν το σύστημα. Πέραν αυτού, η απομάκρυνση των λογαριασμών που δεν είναι απαραίτητοι αποτελεί επιπλέον μέτρο πρόληψης κατά των πιθανών απειλών για την ασφάλεια του συστήματος.

1.7 Απομακρυσμένη Καταγραφή και Παρακολούθηση Δικτυακών Συσκευών

Η καταγραφή των γεγονότων σε ένα δίκτυο αποτελεί έναν ουσιώδη μηχανισμό, επιτρέποντας στους διαχειριστές να πραγματοποιούν ανασκόπηση των καταγεγραμμένων αρχείων και να εξετάζουν ενδεχόμενες ύποπτες δραστηριότητες εντός του δικτύου. Η ορθή καταγραφή προϋποθέτει την αποστολή των αρχείων καταγραφής σε απομακρυσμένους διακομιστές, τα οποία πρέπει να συμμορφώνονται με τις θεσπισμένες πολιτικές και προδιαγραφές. Για τον σκοπό αυτό, οι συσκευές θα πρέπει να είναι ρυθμισμένες ώστε να καταγράφουν τα γεγονότα τοπικά, ενώ παράλληλα να τα μεταφέρουν και σε κεντρικούς AAA servers. Η αποστολή σε κεντρικούς servers είναι προτιμότερη, δεδομένου ότι αυτοί είναι λιγότερο ευάλωτοι σε επιθέσεις, εξάντληση μνήμης ή επανεκκινήσεις. Επιπλέον, είναι προτιμότερο τα μηνύματα που αποστέλλονται από τις συσκευές να είναι κρυπτογραφημένα για περαιτέρω ενίσχυση της ασφάλειας. Επίσης, είναι ουσιώδες να διατηρείται συγχρονισμός των ρολογιών των συσκευών και των απομακρυσμένων servers, ενώ παράλληλα να διασφαλίζεται ότι η χρονική σήμανση των καταγεγραμμένων συμβάντων είναι ακριβής. Συνιστάται η χρήση τουλάχιστον δύο αξιόπιστων πηγών χρόνου για τον συγχρονισμό των ρολογιών.

1.8 Απομακρυσμένη Διαχείριση και Υπηρεσίες Δικτύου

Η ασφαλής απομακρυσμένη διαχείριση των δικτυακών συσκευών αποτελεί κρίσιμο μέλημα για τους διαχειριστές, καθώς παρέχει τη δυνατότητα ελέγχου και διαχείρισης του δικτύου από απόσταση. Παρότι οι διάφορες υπηρεσίες, όπως τα SSH, HTTP, FTP και SNMP, προσφέρουν αποτελεσματικούς τρόπους απομακρυσμένης πρόσβασης, αποτελούν επίσης στόχο για κακόβουλους επιτιθέμενους που επιδιώκουν παραβίαση του δικτύου. Είναι απαραίτητο να χρησιμοποιούνται πρωτόκολλα που υποστηρίζουν κρυπτογράφηση κατά τη μετάδοση των δεδομένων, αποφεύγοντας πρωτόκολλα όπως τα Telnet, HTTP, FTP και SNMP που μεταδίδουν την κίνηση σε μορφή καθαρού κειμένου. Με τη χρήση κρυπτογραφημένων πρωτοκόλλων, εξασφαλίζεται ότι οι ευαίσθητες πληροφορίες δεν διαρρέουν εύκολα σε εχθρικά μέρη. Επιπλέον, οι αλγόριθμοι κρυπτογράφησης πρέπει να είναι ισχυροί και να χρησιμοποιούν έναν επαρκώς μεγάλο αριθμό bits για να αντισταθούν σε επιθέσεις. Προτείνεται η χρήση αξιόπιστων αλγορίθμων κρυπτογράφησης, όπως το AES (Advanced Encryption Standard), για τη διασφάλιση της ασφάλειας των δεδομένων κατά τη μετάδοση. Συνεπώς, η ρύθμιση του συστήματος να επιτρέπει αποκλειστικά τη χρήση κρυπτογραφημένων πρωτοκόλλων για την απομακρυσμένη διαχείριση συμβάλλει στην ενίσχυση της ασφάλειας του δικτύου. Κάποιοι από τους αξιόπιστους αλγόριθμους είναι:

- AES – Advanced Encryption Standard
- ECDSA – Elliptic Curve Digital Signature Algorithm

- SHA – Secure Hash Algorithm

Επιπλέον, είναι απαραίτητο το πρωτόκολλο που χρησιμοποιείται για την απομακρυσμένη διαχείριση να είναι ενημερωμένο στην τελευταία του έκδοση και να έχει προσαρμοστεί με τις κατάλληλες ρυθμίσεις ασφαλείας. Για παράδειγμα, στην περίπτωση των κρυπτογραφημένων HTTP servers, είναι απαραίτητο να εφαρμόζονται τεχνικές κρυπτογράφησης και υπογραφής για την προστασία των επικοινωνιών. Επιπλέον, συνιστάται η περιορισμένη πρόσβαση από πολλές συσκευές σε υπηρεσίες διαχείρισης, με τη χρήση λιστών ελέγχου πρόσβασης (ACLs) που επιτρέπουν μόνο συστήματα που διαθέτουν αποκλειστική δικαιοδοσία. Είναι επίσης σημαντικό να διαγράφονται οι ACL που δεν χρησιμοποιούνται πλέον, προκειμένου να αποφευχθεί η σύγχυση με τυχόν νέες λίστες ελέγχου πρόσβασης. Για τη διασφάλιση της ασφάλειας, οι συνεδρίες πρέπει να τερματίζονται μετά από μια προκαθορισμένη χρονική περίοδο, αλλά αυτή η περίοδος πρέπει να είναι λογική, καθώς μια υπερβολικά μεγάλη περίοδος ενδέχεται να προκαλέσει αρνητικά αποτελέσματα, όπως απόρριψη υπηρεσιών (DoS) ή να προσφέρει στον επιτιθέμενο αρκετό χρόνο για να εκμεταλλευτεί μια ενεργή συνεδρία. Για τις απομακρυσμένες συνδέσεις συσκευών, συνιστάται η διατήρηση της συνεδρίας ανοικτής για μια χρονική διάρκεια που δεν υπερβαίνει τα πέντε λεπτά.

Είναι ουσιώδους σημασίας να ενεργοποιηθούν τα μηνύματα TCP keep-alive σε μια συσκευή δικτύου. Τα εν λόγω μηνύματα αποστέλλονται και λαμβάνονται από τη συσκευή προκειμένου να ελέγχουν την κατάσταση μιας σύνδεσης όταν δεν παρατηρείται κίνηση δεδομένων. Η αποτυχία εκτέλεσης αυτής της διαδικασίας ενδέχεται να διατηρήσει ενεργές συνδέσεις TCP με κίνδυνο, καθώς η απόσυνδεση μπορεί να είναι ακούσια. Σε τέτοιες περιπτώσεις, κακόβουλοι χρήστες ενδέχεται να επαναλάβουν τη συνεδρία, ιδίως σε μη κρυπτογραφημένες συνδέσεις, με σκοπό να αποκτήσουν προνομιούχα δικαιώματα πρόσβασης. Επομένως, είναι αναγκαίο να ρυθμιστεί η συσκευή έτσι ώστε να είναι ικανή να αποστέλλει και να λαμβάνει αυτά τα μηνύματα TCP keep-alive.

Τα SNMP read-write community strings αντιστοιχούν σε αλφαριθμητικά που επιτρέπουν την ανάγνωση και την εγγραφή σε συσκευές δικτύου μέσω του πρωτοκόλλου SNMP. Παρόλο που αυτά τα strings επιτρέπουν στους χρήστες να αποκτήσουν πρόσβαση σε μια συσκευή ή να τροποποιήσουν τις ρυθμίσεις της, η αποστολή τους ως "καθαρό κείμενο" διατηρεί τον κίνδυνο ασφαλείας. Συνεπώς, προτείνεται η αντικατάστασή τους με την ενημέρωση στην έκδοση SNMP 3, η οποία υποστηρίζει κρυπτογράφηση και αυθεντικοποίηση, παρέχοντας έτσι περισσότερη ασφάλεια και προστασία από ανεπιθύμητες παρεμβάσεις.

Ορισμένες υπηρεσίες δικτύου UDP και TCP ενεργοποιούνται προεπιλεγμένα σε πολλές συσκευές, παρά το γεγονός ότι για πολλές χρήσεις δεν είναι απαραίτητες. Ωστόσο, η διατήρησή τους σε λειτουργία μπορεί να επιφέρει ρίσκα ασφαλείας στο δίκτυο. Επομένως, είναι προτιμότερο να απενεργοποιηθούν όλες οι προαναφερθείσες υπηρεσίες σε κάθε συσκευή, προκειμένου να ενισχυθεί το επίπεδο ασφαλείας του δικτύου.

Τα πρωτόκολλα ανακάλυψης, όπως το Cisco Discovery Protocol (CDP) και το Link Layer Discovery Protocol (LLDP), μεταδίδουν τακτικά πληροφορίες σχετικά με την τοπολογία του δικτύου και τα χαρακτηριστικά των συσκευών σε γειτονικές συσκευές. Ένας διεισδυτικός χρήστης μπορεί να αξιοποιήσει αυτήν τη διαδικασία εγκαθίδρυσης πληροφοριών με τη χρήση ενός sniffer, ένα εργαλείο παρακολούθησης που αναλύει τη διακίνηση πακέτων στο δίκτυο, προκειμένου να αποκτήσει πρόσβαση σε ευαίσθητες πληροφορίες που ενδέχεται να εκμεταλλευτεί. Για να αποτραπεί αυτή η δυνατότητα, είναι σημαντικό να απενεργοποιούνται αυτά τα πρωτόκολλα, και σε περιπτώσεις όπου η λειτουργία

τους είναι αναγκαία, να περιορίζεται η ενεργοποίησή τους μόνο σε συγκεκριμένες ζεύξεις μεταξύ σημείων του δικτύου.

1.9 Δρομολογητές και Δρομολόγηση

Η βασική λειτουργία ενός δρομολογητή είναι η διακίνηση πακέτων δεδομένων μεταξύ δικτύων. Κατά τη λήψη ενός πακέτου, ο δρομολογητής χρησιμοποιεί τον πίνακα δρομολόγησης για να αποφασίσει την επόμενη κατεύθυνση προς τον επόμενο κόμβο, προκειμένου το πακέτο να φτάσει στον τελικό προορισμό του. Ωστόσο, μια ακατάλληλη ρύθμιση του δρομολογητή ή των πρωτοκόλλων δρομολόγησης μπορεί να δημιουργήσει ευκαιρίες για ανεπιθύμητη ανακατεύθυνση των πακέτων προς διαφορετικούς προορισμούς. Αυτό μπορεί να αποτελέσει παραβίαση της εμπιστευτικότητας, της ακεραιότητας ή της διαθεσιμότητας του δικτύου.

Ένα παράδειγμα αυτού του φαινομένου αποτελεί το IP source routing, ένα χαρακτηριστικό που επιτρέπει στον αποστολέα να καθορίσει τη διαδρομή που θα ακολουθήσουν τα πακέτα μέσω μιας προκαθορισμένης λίστας κόμβων, αντί να βασίζονται στον εσωτερικό πίνακα δρομολόγησης. Αυτό επιτρέπει σε κακόβουλους χρήστες να μεταδώσουν πακέτα μέσω εναλλακτικών διαδρομών, παρακάμπτοντας ίσως κάποιους περιορισμούς όπως ACLs. Για την αποτροπή αυτής της δυνατότητας, προτείνεται η απενεργοποίηση του συγκεκριμένου χαρακτηριστικού σε όλες τις συσκευές (δρομολογητές, μεταγωγείς κ.λπ.).

Μια σημαντική ενέργεια που απαιτείται είναι η ενεργοποίηση του uRPF (unicast Reverse Path Forwarding). Το uRPF αντιπροσωπεύει μια αποτελεσματική μέθοδο προστασίας κατά της πλαστογράφησης της IP διεύθυνσης. Κατά τη λήψη ενός πακέτου, το uRPF εξετάζει τη διεύθυνση αποστολέα σε σύγκριση με τον πίνακα δρομολόγησης. Εάν η διαδρομή επιστροφής του πακέτου ταιριάζει με το σημείο λήψης, τότε το πακέτο προωθείται. Αντίθετα, απορρίπτεται εάν δεν υπάρχει ταιριάσμα. Η ενεργοποίηση της υπηρεσίας uRPF πρέπει να εφαρμόζεται σε εξωτερικές διεπαφές περιμετρικών δρομολογητών, προκειμένου να αποφευχθεί η απόρριψη νόμιμων πακέτων. Επιπλέον, ο έλεγχος ταυτότητας δρομολόγησης πρέπει να ενεργοποιηθεί για να διασφαλιστεί ότι οι πληροφορίες που διανέμονται από τα πρωτόκολλα δρομολόγησης δεν έχουν υποστεί παραποίηση από μη εξουσιοδοτημένες πηγές.

1.10 Θύρες Διεπαφών

Οι θύρες διεπαφών των διακομιστών συνδέουν φυσικά σταθμούς εργασίας, διακομιστές και άλλες συσκευές δικτύου στο επίπεδο του φυσικού δικτύου. Οι συνδέσεις μεταξύ δρομολογητών και μεταγωγέων καθορίζουν τον τρόπο με τον οποίο τα διάφορα συστήματα επικοινωνούν μέσω του δικτύου. Η κατάλληλη ρύθμιση των θυρών αποτελεί κρίσιμη διαδικασία που εμποδίζει τους μη εξουσιοδοτημένους χρήστες από το να εκμεταλλευτούν το δίκτυο είτε συνδέοντας μη εξουσιοδοτημένες συσκευές είτε εκμεταλλευόμενοι υπάρχοντα συστήματα.

Για την πρόληψη τέτοιων καταστάσεων, προτείνονται διάφορες ενέργειες. Μια από αυτές είναι η απενεργοποίηση του δυναμικού trunking. Το trunking επιτρέπει σε μια σύνδεση να λειτουργεί ως σύνδεση δύο συσκευών από σημείο σε σημείο (point-to-point), ανταλλάσσοντας δεδομένα μέσω των VLAN. Μια διεπαφή μπορεί να διαμορφωθεί δυναμικά ώστε να λειτουργεί ως trunk ή ως θύρα πρόσβασης ανάλογα με την κίνηση που ανιχνεύεται. Εάν ένας χρήστης είναι συνδεδεμένος σε μια δυναμική θύρα, μπορεί να εκμεταλλευτεί το γεγονός αυτό και να ενεργοποιήσει τη λειτουργία trunk, παρακάμπτοντας έτσι τις διαχωριστικές λειτουργίες που προσφέρουν τα VLAN. Συνεπώς, κατά την

προσθήκη νέας συσκευής στο δίκτυο, είναι αναγκαίο να εξασφαλιστεί ότι οι θύρες έχουν ρυθμιστεί αυστηρά είτε ως θύρες trunk είτε ως θύρες πρόσβασης.

Η ενεργοποίηση της ασφάλειας θύρας αποτελεί σημαντική προφυλάξη που περιορίζει τον αριθμό των εγκεκριμένων MAC διευθύνσεων που μπορούν να συνδεθούν σε μια θύρα μεταγωγής, επιτρέποντας την πρόσβαση μόνο σε εξουσιοδοτημένα συστήματα. Η μη ενεργοποίηση αυτής της λειτουργίας μπορεί να δημιουργήσει την δυνατότητα παραβίασης των περιορισμών από κακόβουλους χρήστες, οι οποίοι μπορούν να αποκτήσουν φυσική πρόσβαση και να αποκτήσουν πρόσβαση σε ευαίσθητες πληροφορίες του δικτύου. Επιπλέον, η παράμετρος που ορίζει τον μέγιστο επιτρεπόμενο αριθμό των MAC διευθύνσεων πρέπει να εξεταστεί προσεκτικά, ειδικά όταν χρησιμοποιούνται υπηρεσίες Voice over IP (VoIP). Συνήθως, η επιτρεπόμενη ποσότητα πρέπει να περιορίζεται στη μία ή το πολύ δύο MAC διευθύνσεις, προκειμένου να διασφαλιστεί η ομαλή λειτουργία των υπηρεσιών VoIP.

Είναι γνωστό ότι τα περισσότερα switches χρησιμοποιούν το VLAN 1 ως προεπιλεγμένο VLAN, συμπεριλαμβανομένων των θυρών διαχείρισης που παρέχουν πρόσβαση στο switch για διαχείριση. Ωστόσο, αυτό έχει ως αποτέλεσμα το VLAN να καλύπτει όλο το δίκτυο, προκαλώντας την έκθεση εξουσιοδοτημένων συστημάτων σε πιθανούς κινδύνους από μη εξουσιοδοτημένα συστήματα. Για να αντιμετωπιστεί αυτό το πρόβλημα, η κίνηση διαχείρισης (management traffic) θα πρέπει να μεταφερθεί σε ένα διαφορετικό VLAN από αυτό της λειτουργικής κίνησης (operational traffic). Το προεπιλεγμένο VLAN πρέπει να αποκλειστεί λογικά σε όλες τις θύρες, είτε αυτές λειτουργούν ως trunk είτε ως θύρες πρόσβασης (εκτός αν απαιτείται), προκειμένου να διασφαλιστεί η αποφυγή της μετάδοσης περιττής κίνησης.

Μια πρόσθετη προτεινόμενη ενέργεια είναι η απενεργοποίηση των θυρών που δεν χρησιμοποιούνται στο δίκτυο. Οι ανενεργές θύρες μπορούν να αποτελέσουν πηγή ασφαλειακού κινδύνου, καθώς ενδέχεται να επιτρέψουν σε μη εξουσιοδοτημένα άτομα να συνδέσουν συσκευές με σκοπό την απόκτηση πληροφοριών για το δίκτυο. Για τον λόγο αυτό, είναι σημαντικό να απενεργοποιούνται όλες οι θύρες που δεν χρησιμοποιούνται και να τοποθετούνται σε ένα VLAN το οποίο δεν χρησιμοποιείται στο δίκτυο, αποφεύγοντας ωστόσο το προεπιλεγμένο VLAN για να αποτραπεί η πιθανή πρόσβαση σε ευαίσθητες πληροφορίες.

Επιπλέον, η παρακολούθηση (monitoring) των θυρών αποτελεί αναπόσπαστο μέρος της διαδικασίας διαχείρισης του δικτύου. Πρόκειται για ένα εργαλείο που επιτρέπει την ανίχνευση και την ανάλυση της κίνησης δεδομένων που διαμένει σε μια συγκεκριμένη θύρα μεταγωγής. Ωστόσο, η παρακολούθηση θύρας μπορεί να αποτελέσει ευκαιρία για επιθέσεις, καθώς ένας επιτιθέμενος που έχει πρόσβαση στην θύρα προορισμού μπορεί να ανακτήσει αντίγραφα της κίνησης δεδομένων του δικτύου. Για τον λόγο αυτό, είναι αναγκαίο να απενεργοποιούνται όλες οι ανενεργές συνεδρίες παρακολούθησης σε μια συσκευή και να διατηρούνται ενεργές μόνο οι συνεδρίες που είναι απαραίτητες για την ομαλή λειτουργία του δικτύου.

Η τεχνική του ενδιάμεσου ARP (proxy Address Resolution Protocol) αποτελεί έναν μηχανισμό που επιτρέπει σε έναν ενδιάμεσο διακομιστή (proxy server) να αναλαμβάνει την απάντηση σε ARP αιτήματα που αποστέλλονται για την εύρεση μιας IP διεύθυνσης που δεν ανήκει στο τοπικό δίκτυο. Η εφαρμογή αυτής της τεχνικής επιτρέπει σε συσκευές να αποκτήσουν πρόσβαση σε απομακρυσμένα δίκτυα χωρίς την ανάγκη ρύθμισης διαδρομών (routing) προς την προεπιλεγμένη πύλη δρομολόγησης. Παρόλα αυτά, αξίζει να σημειωθεί ότι αυτή η λειτουργία μπορεί να διευκολύνει κακόβουλες ενέργειες, καθώς κακόβουλοι χρήστες μπορούν να εκμεταλλευτούν την προσβασιμότητα στο σύστημα για την εκτέλεση διαφόρων επιθέσεων, συμπεριλαμβανομένου του σκαναρίσματος δικτύου και της διακοπής της ροής των πακέτων.

Συνιστάται, επομένως, η απενεργοποίηση της λειτουργίας ενδιάμεσου ARP σε όλες τις διεπαφές, εκτός εάν η συσκευή χρησιμοποιείται ως γέφυρα LAN για την εκτέλεση μεταφράσεων διευθύνσεων δικτύου (Network Address Translations – NAT) για την εισερχόμενη κίνηση.

1.11 Χρήση Ειδοποιήσεων Χρήστη (Banners)

Τα banners των δικτυακών συσκευών αποτελούν σημαντικά στοιχεία της διαχείρισης ασφαλείας σε ένα δίκτυο. Αυτά τα μηνύματα, τα οποία εμφανίζονται κατά τη σύνδεση σε μια συσκευή μέσω του πρωτοκόλλου Telnet ή SSH, παρέχουν πληροφορίες σχετικά με τη συσκευή και τη διαμόρφωσή της. Η χρήση των banners αποσκοπεί στην ενημέρωση του χρήστη για τους όρους χρήσης, τους περιορισμούς πρόσβασης και άλλες πολιτικές ασφαλείας που διέπουν τη χρήση της συσκευής. Συγκεκριμένα, τα banners μπορεί να περιλαμβάνουν πληροφορίες όπως οι όροι χρήσης του συστήματος, οι κανόνες ασφαλείας, οι προειδοποιήσεις σχετικά με την παράνομη χρήση, οι ευθύνες του χρήστη και άλλες σχετικές πληροφορίες. Αυτές οι προειδοποιητικές και ενημερωτικές ανακοινώσεις βοηθούν στην αύξηση της επίγνωσης των χρηστών σχετικά με τους κανόνες και τις πολιτικές ασφαλείας του δικτύου. Επιπλέον, τα banners συμβάλλουν στην ενίσχυση της ασφάλειας της συσκευής με διάφορους τρόπους. Κατ' αρχάς, παρέχουν προειδοποιήσεις σε πιθανούς κακόβουλους χρήστες σχετικά με την πολιτική ασφαλείας του συστήματος και τις συνέπειες της παράβασής της. Επιπλέον, μπορούν να αποθαρρύνουν ανεπιθύμητες προσπάθειες παραβίασης του συστήματος από μη εξουσιοδοτημένους χρήστες. Τέλος, η προβολή ενός banner κατά τη σύνδεση με μια συσκευή μπορεί να δώσει στον διαχειριστή την επιβεβαίωση ότι συνδέθηκε στην σωστή συσκευή, αυξάνοντας έτσι την εμπιστοσύνη στην αυθεντικότητα της σύνδεσης. Συνολικά, η χρήση των banners αποτελεί ένα σημαντικό μέσο για την αύξηση της επίγνωσης και της ασφάλειας στο πλαίσιο της διαχείρισης δικτύου.

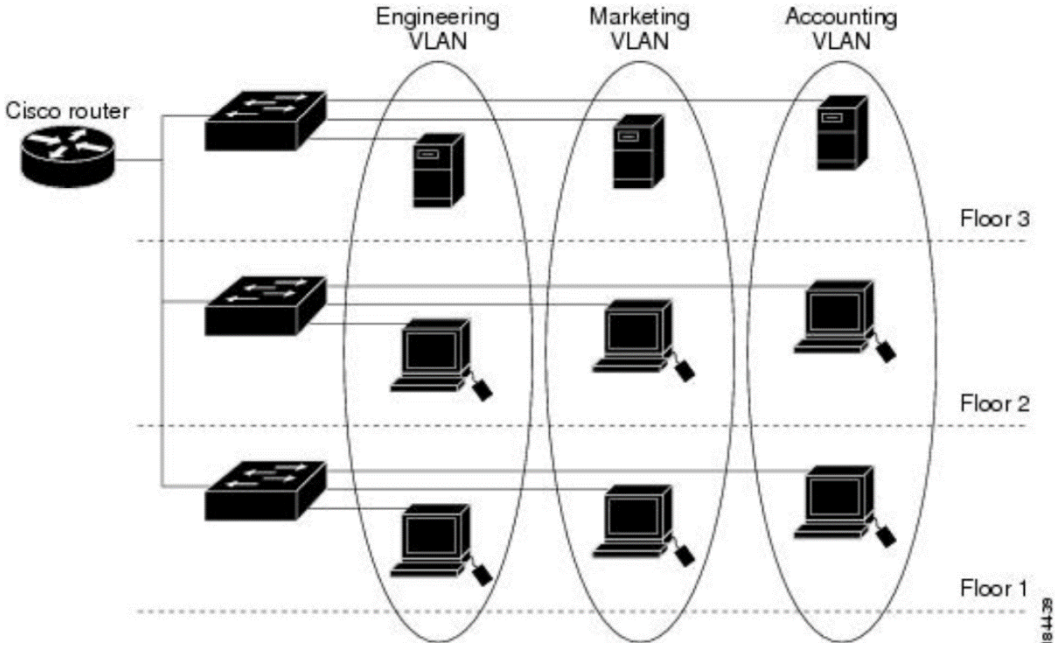
Κεφάλαιο 2ο: Προσομοίωση Σκλήρυνσης Συσκευών και Εντολές Παραμετροποίησης

2.1 Εισαγωγή

Στο πλαίσιο του επόμενου κεφαλαίου, επικεντρωνόμαστε στην προσομοίωση παραμετροποίησης δικτυακών συσκευών, με σκοπό την ενίσχυση της κυβερνοασφάλειας. Οι συσκευές που διερευνούνται είναι της Cisco, μιας από τις κορυφαίες εταιρείες στον τομέα της δικτυακής τεχνολογίας και της κυβερνοασφάλειας. Η παραμετροποίηση γίνεται μέσω του Command Line Interface (CLI). Μέσω αυτής της διαδικασίας, εξετάζουμε διάφορες πτυχές της παραμετροποίησης, συμπεριλαμβανομένων των προηγμένων ρυθμίσεων ασφαλείας, δικτυακής πολιτικής και διαχείρισης πρόσβασης, με στόχο την ενίσχυση της ασφάλειας του δικτύου. Μέσα από αυτήν την ανάλυση, αναδεικνύονται οι βέλτιστες πρακτικές και οι πιθανές αδυναμίες, επιτρέποντας την υλοποίηση αποτελεσματικών μέτρων προστασίας και την ενίσχυση της γενικής ασφάλειας του δικτύου. Η προσομοίωση των εντολών γίνεται στο περιβάλλον του Packet Tracer.

2.2 Τμηματοποίηση Δικτύων και VLANs

Η τμηματοποίηση δικτύου αντιπροσωπεύει μια κρίσιμη πρακτική στον τομέα των δικτύων, καθώς επιτρέπει τη διαχείριση και την ασφάλεια των δικτύων με αποτελεσματικότητα και αποτελεσματικό τρόπο. Στη βάση αυτής της πρακτικής, το δίκτυο διαιρείται σε διάφορα υποδίκτυα, γνωστά ως VLANs, όπου συσκευές με κοινές απαιτήσεις ασφαλείας ομαδοποιούνται μαζί. Η τμηματοποίηση αυτή επιτρέπει μια πιο αποτελεσματική παρακολούθηση του δικτύου, δίνοντας τη δυνατότητα για γρήγορη ανίχνευση πιθανών απειλών ή προβλημάτων. Σημαντική διάκριση στην τμηματοποίηση δικτύου είναι μεταξύ φυσικής και εικονικής τμηματοποίησης. Η πρώτη, φυσική τμηματοποίηση, επιτυγχάνεται μέσω της τοποθέτησης φυσικών συσκευών, όπως δρομολογητές και μεταγωγείς. Αυτή η προσέγγιση προσφέρει υψηλό επίπεδο ασφάλειας, αν και συνήθως είναι πιο κοστοβόρα λόγω της ανάγκης για επιπλέον εξοπλισμό. Η εικονική τμηματοποίηση, από την άλλη, γίνεται μέσω λογισμικού και χρησιμοποιεί VLANs για τον διαχωρισμό του δικτύου. Κάθε VLAN αποτελεί ένα λογικό δίκτυο, ανεξάρτητα από τη φυσική του θέση. Οι συσκευές μπορεί να ανήκουν σε διαφορετικά VLANs, και κάθε θύρα μεταγωγέα μπορεί να ανήκει σε διαφορετικό VLAN. Με αυτόν τον τρόπο, τα πακέτα δεδομένων μπορούν να δρομολογούνται αποτελεσματικά μέσα στο δίκτυο, με αυστηρό έλεγχο πρόσβασης. Η προσέγγιση αυτή επιτρέπει μεγαλύτερη ευελιξία και διαχείριση του δικτύου, ενώ ταυτόχρονα διασφαλίζει την ασφάλεια και την αποτελεσματικότητά του.



Εικόνα 3 Εικονική Τμηματοποίηση με VLAN

2.2.1 VLAN στις συσκευές Cisco και εντολές παραμετροποίησης

Στη συσκευή της CISCO που μελετάμε μπορούμε να έχουμε 4094 διαφορετικά VLANs, στο παρακάτω πίνακα φαίνονται μερικές πληροφορίες σχετικά με αυτά.

Πίνακας 2-1 Χρήση των VLANs

VLAN ID	Εύρος	Χρήση
1	Τυπικό	Το προκαθορισμένο VLAN της CISCO. Μπορεί να χρησιμοποιηθεί αλλά όχι να τροποποιηθεί και να διαγραφεί.
2-1005	Τυπικό	Τα VLAN αυτά μπορούν να δημιουργηθούν, να τροποποιηθούν και να διαγραφούν.
1006-3967 και 4048-4093	Εκτεταμένο	Τα VLAN αυτά μπορούν να δημιουργηθούν, να τροποποιηθούν και να διαγραφούν, αλλά δε μπορούν να αλλάξουν τα παρακάτω:

		• Η κατάσταση του VLAN είναι πάντα ενεργή Το VLAN είναι πάντα ενεργοποιημένο
3968-4047 και 4094	Εσωτερικά	Τα VLAN αυτά διατίθενται για εσωτερική χρήση της συσκευής. Δε μπορούν να δημιουργηθούν, να τροποποιηθούν και να διαγραφούν.

Στη συνέχεια αναλύονται οι εντολές CLI που χρειάζονται ώστε να δημιουργηθεί , τροποποιηθεί και να διαγραφεί ένα VLAN

Πίνακας 2-2 Εντολές Παραμετροποίησης VLAN

Εντολή	Περιγραφή
enable	Εισάγει το χρήστη σε privileged mode
configure terminal	Εισάγει το χρήστη σε global mode
vlan {vlan-id | vlan-range}	Δημιουργεί το vlan με το id που δίνεται ή τα vlan στο εύρος που ορίζεται
exit	Επιστρέφει στο προηγούμενο mode
do show vlan	Εμφανίζει της πληροφορίες σχετικά με τα vlans της συσκευής
copy running-config startup-config	Αντιγράφει το αρχείο των προσωρινών ρυθμίσεων στο αρχείο των ρυθμίσεων εκκίνησης , ώστε σε περίπτωση επανεκκίνησης αυτές να μη χαθούν.

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan 10
Switch(config-vlan)#exit
Switch(config)#do show vlan

VLAN Name                                Status    Ports
---- ----------------------------------- --------- -------------------------------
1    default                             active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                   Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                   Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                   Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                   Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                   Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                   Gig0/1, Gig0/2
10   VLAN0010                            active
1002 fddi-default                        active
1003 token-ring-default                  active
1004 fddinet-default                     active
1005 trnet-default                       active

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
10   enet  100010     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    -        0      0
1004 fdnet 101004     1500  -      -      -        ieee -        0      0
1005 trnet 101005     1500  -      -      -        ibm  -        0      0

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------

Remote SPAN VLANs
------------------------------------------------------------------------------

Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------
```

Εικόνα 4 Εμφάνιση πληροφοριών των vlan της συσκευής

Προκειμένου ρυθμίσουμε τις παραμέτρους ενός VLAN πρέπει να εκτελέσουμε τις εντολές που ακολουθούν.

Πίνακας 2-3 Εντολές παραμετροποίησης VLAN

Εντολή	Περιγραφή
enable	Εισάγει το χρήστη σε privileged mode.
configure terminal	Εισάγει το χρήστη σε global mode
vlan {*vlan-id* | *vlan-range*}	Εισάγει το χρήστη στο vlan που επιλέγει.
name *vlan-name*	Η εντολή αυτή δίνει όνομα στο vlan.
state {active | suspend}	Ορίζει την κατάσταση του VLAN. Όταν το vlan είναι suspend, οι θύρες που σχετίζονται με αυτό το VLAN απενεργοποιούνται και δε περνάει κίνηση απ' αυτές. Στα VLANs 1006-4094 δε μπορεί να αλλάξει η κατάσταση του VLAN.

no shutdown	Ενεργοποιεί το VLAN. (Στις προκαθορισμένες ρυθμίσεις το VLAN είναι ενεργοποιημένο.

2.3 Αναβάθμιση Λογισμικού

Η συνεχής αναβάθμιση του λογισμικού αναδεικνύεται ως κρίσιμη διαδικασία, δεδομένου ότι κάθε νέα έκδοση παρέχει διορθώσεις για προβλήματα που εντοπίζονται σε προηγούμενες εκδόσεις. Αυτή η πρακτική αποτρέπει την εκμετάλλευση ενδεχόμενων αδυναμιών του συστήματος από επιθετικούς χρήστες. Συνεπώς, είναι αναγκαίο να εξετάζουμε τους τρόπους αναβάθμισης του λογισμικού, ιδίως σε συσκευές δικτύου όπως οι δρομολογητές.

Για να επιτευχθεί η ενημέρωση του λογισμικού ενός δρομολογητή, απαιτείται η εγκατάσταση ενός TFTP (Trivial File Transfer Protocol) server. Το TFTP αποτελεί πρωτόκολλο μεταφοράς αρχείων που χρησιμοποιεί το UDP για την αποστολή δεδομένων. Ένας TFTP server συχνά χρησιμοποιείται για τη μεταφορά αρχείων εκκίνησης στο σύστημα εκκίνησης του υπολογιστή.

Μετά την επιλογή και λήψη της επιθυμητής έκδοσης λογισμικού από την ιστοσελίδα υποστήριξης και λήψεων της Cisco, το αρχείο μεταφέρεται στον εξυπηρετητή TFTP. Στη συνέχεια, μέσω του υπολογιστή στον οποίο είμαστε συνδεδεμένοι, εκτελούμε τις απαραίτητες ενέργειες στον δρομολογητή για την ενημέρωση του λογισμικού.

Πίνακας 2-4 Εμφανιση αρχείων flash

dir *flash:*	Εμφανίζει τα αρχεία στον φακελο flash

```
Router#dir flash:
Directory of flash0:/

    3  -rw-    33591768          <no date>  c2900-universalk9-mz.SPA.151-4.M4.bin
    2  -rw-       28282          <no date>  sigdef-category.xml
    1  -rw-      227537          <no date>  sigdef-default.xml

255744000 bytes total (221896413 bytes free)
```

Εικόνα 5 Εμφάνιση αρχείων φακέλου flash

Επιστρέφει το αρχείο με την έκδοση που έχει ο δρομολογητής *c2900-universalk9-mz.SPA.151-4.M4.bin.* Επίσης εμφανίζεται και ο ελεύθερος χώρος που υπάρχει. Εάν είναι αναγκαίο θα πρέπει να διαγραφούν κάποια αρχεία με την εξής εντολή:

Πίνακας 2-5 Διαγραφή αρχείου απο φακελο flash

delete flash0:{*ονομα αρχείου}*	Διαγραφή αρχείου

Στη συνέχεια ελέγχεται εάν υπάρχει επικοινωνία μεταξύ server και δρομολογητή με την εντολή **ping.** Αφού επιβεβαιωθεί η επικοινωνία θα πρέπει να γίνει η αντιγραφή του αρχείου από τον TFTP server στο δρομολογητή. Αυτό γίνεται με τον εξής τρόπο:

Πίνακας 2-6 Αντιγραφή επιθυμητού αρχείου απο TFTP server

copy tftp: flash:	Ατιγραφή του αρχείου απο τον TFTP server

Στη συνέχεια δίνουμε την ip διεύθυνση του server και μετά το όνομα του αρχείου που θέλουμε να μεταφέρουμε στον δρομολογητή. Σαν όνομα αρχείου στο προορισμό μπορεί να οριστεί και το ίδιο όνομα με αυτό στην πηγή.

```
Router#copy tftp: flash:
Address or name of remote host []? 192.168.1.2
Source filename []? c2900-universalk9-mz.SPA.155-3.M4a.bin
Destination filename [c2900-universalk9-mz.SPA.155-3.M4a.bin]?
%Warning:There is a file already existing with this name
Do you want to over write? [confirm]y

Accessing tftp://192.168.1.2/c2900-universalk9-mz.SPA.155-3.M4a.bin...
Loading c2900-universalk9-mz.SPA.155-3.M4a.bin from 192.168.1.2:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 33591768 bytes]

33591768 bytes copied in 0.722 secs (4885037 bytes/sec)
```

Εικόνα 6 Αντιγραφή αρχείου απο TFTP server στη συσκευή

Αφού έχουμε το αρχείο στη μνήμη του δρομολογητή, ρυθμίζουμε να γίνεται εκκίνηση με την έκδοση που επιθυμούμε.

configure terminal	Εισάγει το χρήστη σε global mode
boot system flash {*όνομα-αρχείου}*	Εκκίνηση συστήματος με το αρχείο που επιθυμεί ο χρήστης
Ctrl+Z	
write mem	Αποθήκευση αλλαγών
reload	Επανεκίνηση συσκευής

```
Router#show version | inc Version
Cisco IOS Software, C2900 Software (C2900-UNIVERSALK9-M), Version 15.1(4)M4, RELEASE SOFTWARE (fc2)
```

```
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#boot system flash c2900-universalk9-mz.SPA.155-3.M4a.bin
Router(config)#^Z
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#write mem
Building configuration...
[OK]
Router#reload
```

Εικόνα 7 Διαδικασία εγκατάστασης έκδοσης

Τέλος με την εντολή *show version* ελέγχουμε εάν έχει αναβαθμιστεί το λογισμικό.

```
Router>en
Router#show version | include Version
Cisco IOS Software, C2900 Software (C2900-UNIVERSALK9-M), Version 15.5(3)M4a, RELEASE SOFTWARE (fc1)
```

Εικόνα 8 Έλεγχος έκδοσης

2.4 Αυθεντικοποίηση , Εξουσιοδότηση και Καταγραφή δικτυακών συσκευών

Η διαδικασία της αυθεντικοποίησης αποτελεί κρίσιμο στάδιο για τη διαχείριση πρόσβασης σε δίκτυα, με δύο κύριους τύπους servers που χρησιμοποιούνται γι' αυτόν τον σκοπό: ο RADIUS και ο TACACS. Οι διαφορές μεταξύ τους είναι σημαντικές και περιλαμβάνουν τα ακόλουθα:

- Ο TACACS+ προσφέρει πλήρη κρυπτογράφηση των πακέτων κατά την επικοινωνία, ενώ ο RADIUS κρυπτογραφεί μόνο τα συνθηματικά.
- Ο TACACS+ χρησιμοποιεί το πρωτόκολλο TCP, ενώ ο RADIUS χρησιμοποιεί το UDP.
- Ο TACACS+ είναι συμβατός μόνο με συσκευές της Cisco, ενώ ο RADIUS λειτουργεί με ποικίλες συσκευές.

Στη συνέχεια παρουσιάζεται η βασική διαμόρφωση των συσκευών για την τοπική αυθεντικοποίηση, την αυθεντικοποίηση μέσω TACACS+ και την αυθεντικοποίηση μέσω RADIUS.

2.4.1 Τοπική Αυθεντικοποίηση

Παρακάτω παρουσιάζονται οι εντολές με τις οποίες ενεργοποιείται η αυθεντικοποίηση ενός χρήστη τοπικά στη συσκευή.

Πίνακας 2-7 Εντολές ενεργοποίησης τοπικής αυθεντικοποίησης

configure terminal	Εισάγει το χρήστη σε global mode
username {*username*} secret {*password*}	Ορίζει ένα όνομα χρήστη και ένα κρυπτογραφημένο συνθηματικό.
aaa new-model	Ενεργοποιεί τις εντολές για το AAA.
aaa authentication login default local	Ορίζει ότι για την είσοδο η σειρά προτεραιότητας για την αυθεντικοποίηση είναι οι local ρυθμίσεις και είναι οι default ρυθμίσεις.
line console 0	Εισάγει το χρήστη στις ρυθμίσεις της γραμμής κονσόλας.
login authentication default	Για την είσοδο απο κοσνόλα, για την αυθεντικοποίηση χρησιμοποιούνται οι default ρυθμίσεις.

```
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#username Adminl secret adminlpa
R1(config)#aaa new-model
R1(config)#aaa authentication login default local
R1(config)#line console 0
R1(config-line)#login authentication default
R1(config-line)#exit
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console
```

Εικόνα 9 Τοπική αυθεντικοποίηση

2.4.2 Αυθεντικοποίηση μέσω TACACS+ server

Παρακάτω παρουσιάζονται οι εντολές με τις οποίες ενεργοποιείται η αυθεντικοποίηση ενός χρήστη μέσω ενός tacacs+ server.

Πίνακας 2-8 Εντολές ενεργοποίησης αυθεντικοποίησης μέσω tacacs

configure terminal	Εισάγει το χρήστη σε global mode
username {*username*} secret {*password*}	Ορίζει ένα όνομα χρήστη και ένα κρυπτογραφυμένο συνθηματικό. (Για περιπτώσεις όπου η επικοινωνία με το server δεν είναι δυνατή , η αυθεντικοποίηση γίνεται τοπικά).
tacacs-server host {*ip-address*}	Ορίζει ποια είναι η ip διεύθυνση του server όπου θα γίνει η αυθεντικοποίηση.
tacacs-server key {*key*}	Το συνθηματικό για την αναγνώριση της συσκευής από τον server.
aaa new-model	Ενεργοποιεί τις εντόλες για το AAA.
aaa authentication login default group tacacs+ local	Ορίζει ότι για την είσοδο η σειρα προτεραιότητας για την αυθεντικοποίηση. Πρώτα είναι οι tacacs ρυθμίσεις και μετά οι local ρυθμίσεις και είναι οι default ρυθμίσεις.
line console 0	Μπαίνει στις ρυθμίσεις της γραμμής κονσόλας.
login authentication default	Για την είσοδο απο κοσνόλα, για την αυθεντικοποίηση χρησιμοποιούνται οι default ρυθμίσεις.

```
R2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#username Admin2 secret admin2pa55
R2(config)#tacacs-server host 192.168.2.2
R2(config)#tacacs-server key tacacspa55
R2(config)#aaa new-model
R2(config)#aaa authentication login default group tacacs+ local
R2(config)#line console 0
R2(config-line)#login authentication default
R2(config-line)#exit
```

Εικόνα 10 Αυθεντικοποίηση μέσω tacacs

2.4.3 Αυθεντικοποίηση μέσω RADIUS server

Παρακάτω παρουσιάζονται οι εντολές με τις οποίες ενεργοποιείται η αυθεντικοποίηση ενός χρήστη μέσω ενός RADIUS server.

Πίνακας 2-9 Ενεργοποίηση αυθεντικοποίησης μέσω RADIUS

configure terminal	Εισάγει το χρήστη σε global mode
username {*username*} secret {*password*}	Ορίζει ένα όνομα χρήστη και ένα κρυπτογραφημένο συνθηματικό. (Για περιπτώσεις όπου η επικοινωνία με το server δεν είναι δυνατή , η αυθεντικοποίηση γίνεται τοπικά).
radius-server host {*ip-address*}	Ορίζει ποια είναι η ip διεύθυνση του server όπου θα γίνει η αυθεντικοποίηση.
radius-server key {*key*}	Το συνθηματικό για την αναγνώριση της συσκευής από τον server.
aaa new-model	Ενεργοποιεί τις εντολές για το AAA.
aaa authentication login default group radius local	Ορίζει ότι για την είσοδο η σειρά προτεραιότητας για την αυθεντικοποίηση. Πρώτα είναι οι radius ρυθμίσεις και μετά οι local ρυθμίσεις και είναι οι default ρυθμίσεις.
line console 0	Μπαίνει στις ρυθμίσεις της γραμμής κονσόλας.
login authentication default	Για την είσοδο απο κοσνόλα, για την αυθεντικοποίηση χρησιμοποιούνται οι default ρυθμίσεις.

```
R3#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#username Admin3 secret admin3pa55
R3(config)#radius-server host 192.168.3.2
R3(config)#radius-server key radiuspa55
R3(config)#aaa new-model
R3(config)#aaa authentication login default group radius local
R3(config)#line console 0
R3(config-line)#login authentication default
R3(config-line)#exit
```

Εικόνα 11 Ενεργοποίηση αυθεντικοποίσησης μέσω RADIUS

Με παρόμοιο τρόπο εκτελούνται και οι εντολές για την ενεργοποίηση της εξουσιοδότησης και της καταγραφής.

2.5 Απομακρυσμένη καταγραφή

Με τις παρακάτω εντολές μπορούμε να ρυθμίσουμε την καταγραφή (logging) των γεγονότων που συμβαίνουν στο δρομολογητή και αυτά να αποθηκεύονται σε έναν απομακρυσμένο server.

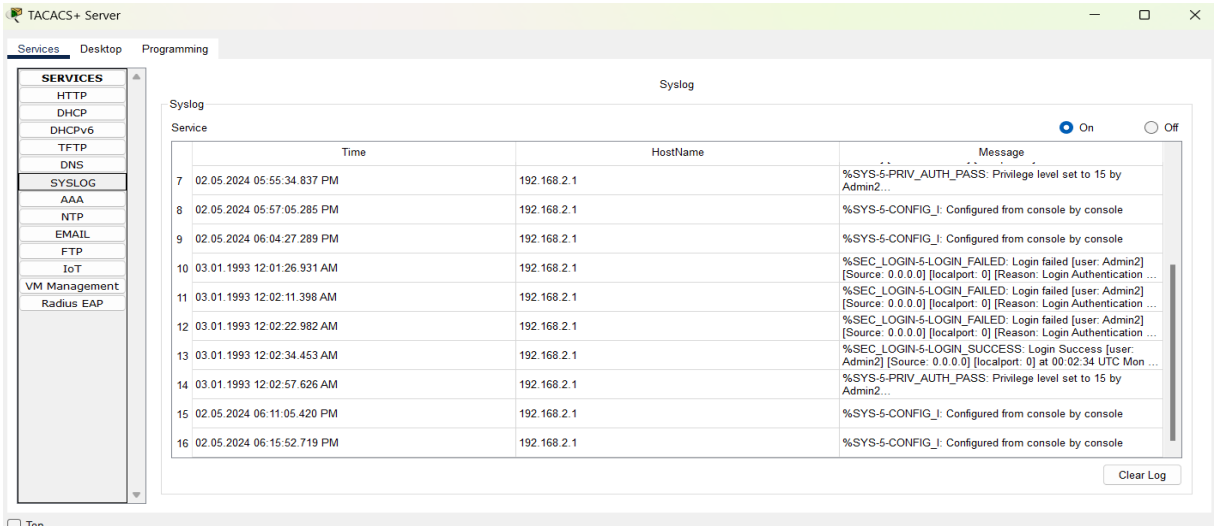
Πίνακας 2-10 Εντολές ενεργοποίησης απομακρυσμένης καταγραφής

configure terminal	Εισάγει το χρήστη σε global mode
logging on	Ενεργοποιεί την καταγραφή
logging host {*host-address*}	Ορίζει την ip του server που θα γίνεται η καταγραφή των γεγονότων
login on-failure log	Καταγραφή αποτυχημένων προσπαθειών
login on-success log	Καταγραφή επιτυχημένων προσπαθειών

```
Username: Admin2
Password:
R2>
*Feb 05, 17:55:08.5555: SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user:
Admin2] [Source: 0.0.0.0] [localport: 0] at 17:55:08 UTC Mon Feb 5 2024

R2>
R2>enable
Password:
R2#
*Feb 05, 17:55:34.5555: SYS-5-PRIV_AUTH_PASS: Privilege level set to 15 by
Admin2

R2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#logging on
R2(config)#logging host 192.168.2.2
R2(config)#login on-failure log
R2(config)#login on-success log
R2(config)#exit
R2#
*Feb 05, 17:57:05.5757: SYS-5-CONFIG_I: Configured from console by console
R2#
```

Εικόνα 12 Ενεργοποίηση απομακρυσμένης καταγραφής

Στην εικόνα που ακολουθεί φαίνεται το αρχείο καταγραφής στον απομακρυσμένο server.



Εικόνα 13 Αρχείο καταγραφής στον απομακρυσμένο server

2.6 Ενεργοποίηση συγχρονισμού ρολογιού

Για τον συγχρονισμό του ρολογιού σε μια συσκευή, είναι ζωτικής σημασίας να χρησιμοποιείται το πρωτόκολλο Network Time Protocol (NTP). Αυτό επιτυγχάνεται με τη ρύθμιση και τον συγχρονισμό της συσκευής με έναν εξωτερικό NTP server. Η ενεργοποίηση του NTP και η καθορισμένη σύνδεση με έναν αξιόπιστο NTP server εξασφαλίζει όχι μόνο την ευστάθεια του ρολογιού της συσκευής, αλλά και την εύρυθμη λειτουργία των διάφορων υπηρεσιών και διαδικασιών που εξαρτώνται από ακριβή χρονική σήμανση. Με τη συμμόρφωση προς το NTP πρωτόκολλο, εξασφαλίζεται η συνοχή και η ακρίβεια των χρονικών σφραγίδων που χρησιμοποιούνται στην καταγραφή δεδομένων και στις διάφορες λειτουργίες του συστήματος.

Πίνακας 2-11 Εντολές ενεργοποίησης NTP

ntp authentication-key {*#1*} md5 {*key*}	Προσθέτει ένα κλειδί αυθεντικοποίησης MD5 για το NTP, όπου "{#1}" είναι ο αριθμός του κλειδιού και "{key}" το ίδιο το κλειδί
ntp trusted-key {*key*}	Ορίζει ένα κλειδί ως αξιόπιστο για την επικύρωση των μηνυμάτων NTP.
ntp authentication	Ενεργοποιεί την αυθεντικοποίηση για το NTP, δίνοντας τη δυνατότητα στο δίκτυο να ελέγχει την ταυτότητα των συσκευών που συμμετέχουν στο πρωτόκολλο.
ntp server {*ip-address*} key {*#1*}	Ορίζει έναν NTP server με την διεύθυνση IP "{ip-address}" και τον αριθμό κλειδιού "{#1}"

exit	Επιστροφή
show ntp status	Εμφάνιση πληροφοριών σχετικά με τον NTP.

```
R2(config)#ntp authentication-key 1 md5 cisco
R2(config)#ntp trusted-key 1
R2(config)#ntp authenticate
R2(config)#ntp server 192.168.2.2 key 1
R2(config)#exit
R2#
*Feb 05, 18:15:52.1515: SYS-5-CONFIG_I: Configured from console by console
R2#show ntp status
Clock is synchronized, stratum 2, reference is 192.168.2.2
nominal freq is 250.0000 Hz, actual freq is 249.9990 Hz, precision is 2**24
reference time is E942C5D3.0000029C (18:15:47.668 UTC Mon Feb 5 2024)
clock offset is 3.00 msec, root delay is 6.00  msec
root dispersion is 61.27 msec, peer dispersion is 0.00 msec.
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is - 0.000001193
s/s system poll interval is 4, last update was 15 sec ago.
```

Εικόνα 14 Ενεργοποίηση συγροχνισμού με NTP

2.7 Καθορισμός των Access Lists (ACL)

Για τον έλεγχο και τον περιορισμό της διέλευσης κίνησης μέσω ενός δρομολογητή, χρησιμοποιούνται οι λίστες πρόσβασης (Access Control Lists - ACLs). Ορίζονται με σκοπό να επιτρέπουν ή να αποκλείουν τη μετάδοση πακέτων δεδομένων, βασιζόμενες σε διάφορα κριτήρια όπως η προέλευση, ο προορισμός, ο τύπος του πρωτοκόλλου, και άλλες παράμετροι. Η καθορισμένη με ακρίβεια εφαρμογή των ACLs στον δρομολογητή επιτρέπει τη διαχείριση της κίνησης με βάση τις ανάγκες και τις απαιτήσεις του δικτύου. Μέσω της ανάλυσης και του ορισμού συγκεκριμένων κανόνων στις ACLs, επιτυγχάνεται η αποτελεσματική διαχείριση της κίνησης, η προστασία του δικτύου από ανεπιθύμητες εισβολές και η εξασφάλιση της ασφάλειας των εφαρμογών και των δεδομένων που μεταδίδονται. Στη συνέχεια παρατίθενται οι εντολές ενεργοποίησης των λιστών.

Πίνακας 2-12 Εντολές καθορισμού μιας λίστας ελέγχου πρόσβασης

ip access-list standard {*list-number*}	Ορίζει μια λίστα ελέγχου πρόσβασης
permit {*network_id*} {*wildcard*}	Ορίζει από ποιες ip τα μηνύματα θα επιτρέπονται
deny {*ip* | *any*}	Ορίζει απο ποιες ip τα μηνλθματα θα απορρίπτονται
no access-list {*list-number*}	Σβήνει μια λίστα
show access-list	Εμφανίζει τις πληροφορίες για τις λίστες

```
R2(config)#ip access-list standard 1
R2(config-std-nacl)#permit 192.168.1.0 0.0.0.255
R2(config-std-nacl)#deny any
R2(config-std-nacl)#exit
R2(config)#exit
R2#
*Feb 05, 18:50:07.5050: SYS-5-CONFIG_I: Configured from console by console
R2#show access-list
Standard IP access list 2
    10 permit 190.168.2.0 0.0.0.255
Standard IP access list 1
    10 permit 192.168.1.0 0.0.0.255
    20 deny any

R2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#no access-list 2
R2(config)#exit
R2#
*Feb 05, 18:50:54.5050: SYS-5-CONFIG_I: Configured from console by console
R2#show access-list
Standard IP access list 1
    10 permit 192.168.1.0 0.0.0.255
    20 deny any

R2#
```

Εικόνα 15 Καθορισμός λίστας ελέγχου πρόσβασης

2.8 Απενεργοποίηση θυρών διεπαφής

Προκειμένου να απενεργοποιηθούν οι διεπαφές οι οποίες δε χρησιμοποιούνται πρέπει να ακολουθηθούν οι παρακάτω ενέργειες.

Πίνακας 2-13 Εντολές απενεργοποίησης διεπαφών

configure terminal	Εισάγει το χρήστη σε global mode
interface range {*interface*} – {*interface*}	Επιλέγει τις θύρες στις οποίες θα εφαρμοστούν οι ρυθμίσεις
shutdown	Απενεργοποιεί τις θύρες
switchport access vlan {*vlan_id*}	Τοποθετεί τις θύρες σε ένα vlan που είναι ανενεργό

```
Switch>en
Switch#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface range f0/4 - f0/10
Switch(config-if-range)#shutdown

%LINK-5-CHANGED: Interface FastEthernet0/4, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/5, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/6, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/7, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/8, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/9, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/10, changed state to administratively down
Switch(config-if-range)#switchport access vlan 999
% Access VLAN does not exist. Creating vlan 999
Switch(config-if-range)#exit
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#show vlan

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/11
                                                 Fa0/12, Fa0/13, Fa0/14, Fa0/15
                                                 Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                                 Fa0/20, Fa0/21, Fa0/22, Fa0/23
                                                 Fa0/24, Gig0/1, Gig0/2
999  VLAN0999                          active    Fa0/4, Fa0/5, Fa0/6, Fa0/7
                                                 Fa0/8, Fa0/9, Fa0/10
```

Εικόνα 16 Απενεργοποίηση θυρών που δε χρησιμοποιούνται

2.9 Εισαγωγή μηνυμάτων banner

Τα banners αποτελούν μηνύματα που παρουσιάζονται πριν από την είσοδο του χρήστη σε ένα σύστημα, με σκοπό την παροχή συγκεκριμένων πληροφοριών. Διακρίνονται σε δύο βασικές κατηγορίες: τα μηνύματα της ημέρας (message of the day - motd), τα οποία παρέχουν προσωρινές ενημερώσεις, όπως αναγγελία προγραμματισμένων συντηρήσεων του συστήματος, και τα μηνύματα σύνδεσης (login banners), τα οποία εκφράζουν ένα μήνυμα που εμφανίζεται πριν την είσοδο του χρήστη. Συνήθως, αυτά τα μηνύματα επισημαίνουν ότι η μη εξουσιοδοτημένη πρόσβαση απαγορεύεται, ενισχύοντας έτσι την ασφάλεια του συστήματος και την ενημέρωση των χρηστών σχετικά με τους κανόνες και τις πρακτικές που διέπουν τη χρήση αυτού του συστήματος.

Πίνακας 2-14 Ενεργοποίηση banners

configure terminal	Εισάγει το χρήστη σε global mode
banner login	Καθορίζει το login μήνυμα
banner motd	Καθορίζει το message of the day μήνυμα

```
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/
Router(config)#banner motd #
Enter TEXT message.  End with the character '#'.
Maintenance at midnight#

Router(config)#banner login #
Enter TEXT message.  End with the character '#'.
Unauthorized Access is forbidden #

Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#exit



Router con0 is now available



Press RETURN to get started.



Maintenance at midnight

Unauthorized Access is forbidden
```

Εικόνα 17 Καθορισμός login και motd banner

Κεφάλαιο 3ο: Ανάπτυξη λογισμικού για αυτοματοποίηση ενεργειών με σκοπό τη σκλήρυνση δικτυακών συσκευών

3.1 Εισαγωγή

Το παρόν κεφάλαιο περιγράφει ένα λογισμικό που αναπτύχθηκε σε Python για την αυτοματοποίηση συγκεκριμένων λειτουργιών σε έναν δρομολογητή, εστιάζοντας στην ασφάλεια και την ενίσχυση της ακεραιότητας της συσκευής. Το πρόγραμμα περιλαμβάνει τη διαμόρφωση ποικίλων παραμέτρων, μεταξύ των οποίων αναφέρονται η αυθεντικοποίηση του χρήστη μέσω απομακρυσμένου server (AAA), η συγχρονισμός του ρολογιού του δρομολογητή μέσω ενός NTP server, η ενεργοποίηση του κλειδιού ενεργοποίησης (Enable mode), καθώς και η διαμόρφωση συνοδευτικών παραμέτρων, όπως οι timestamps και η καταγραφή σε έναν syslog server.

Μέσω του προγράμματος, ο χρήστης έχει τη δυνατότητα να περιηγηθεί σε ένα μενού επιλογών και να επιλέξει τις ενέργειες που επιθυμεί να εκτελέσει, προσφέροντας προηγουμένως τα αναγκαία διαπιστευτήρια για την απομακρυσμένη σύνδεση με τον δρομολογητή. Σημαντικότερες λειτουργίες που προσφέρονται είναι η διαμόρφωση των μηνυμάτων (banners), ο έλεγχος για ενημερώσεις λογισμικού, η διαμόρφωση access-lists και η αποθήκευση των αλλαγών.

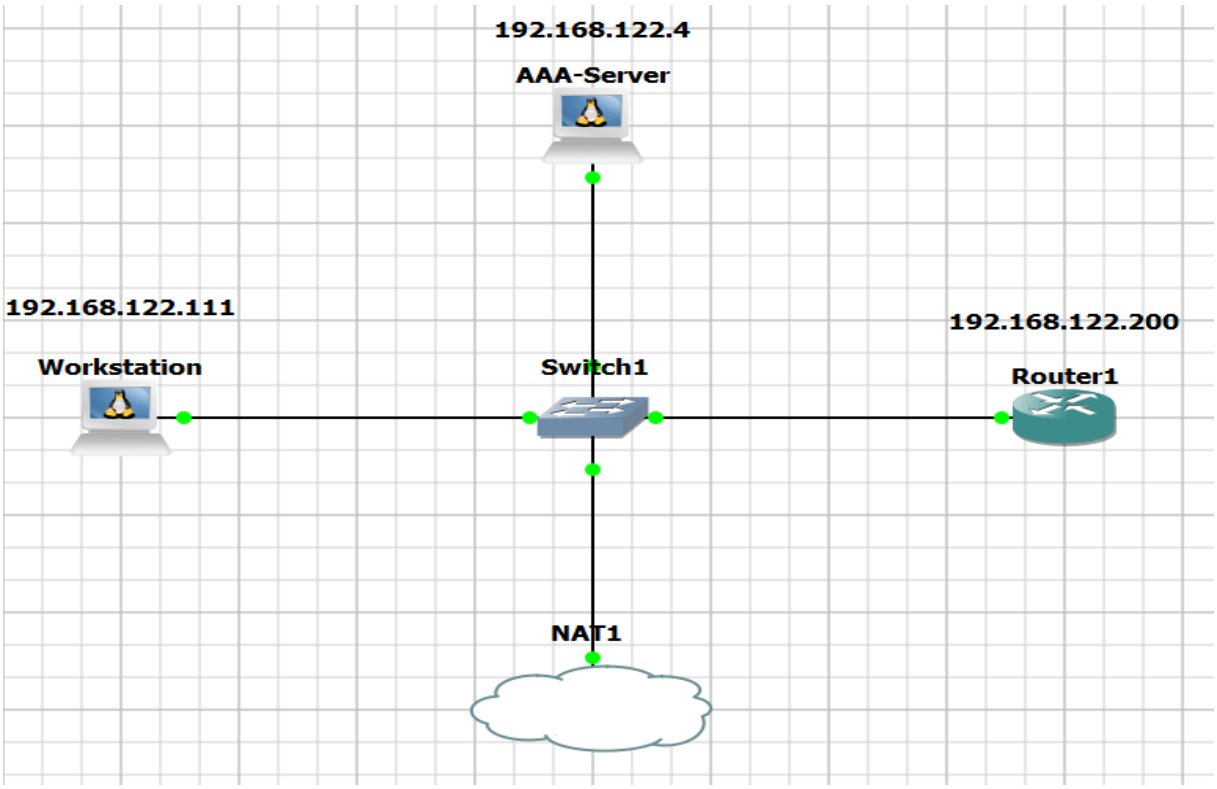
Η ορθή λειτουργία του προγράμματος επαληθεύτηκε μέσω προσομοίωσης στο περιβάλλον GNS3. Στη συνέχεια παρουσιάζεται η εκτέλεση της προσομοίωσης, καταδεικνύοντας την αποτελεσματικότητα και τη συμβατότητα του προγράμματος με τις αναμενόμενες λειτουργίες του δρομολογητή.

3.2 Προετοιμασία και τοπολογία δικτύου

Αρχικά, γίνεται η εισαγωγή των στοιχείων του δικτύου, το οποίο περιλαμβάνει:

- Έναν σταθμό εργασίας, ο οποίος λειτουργεί ως χώρος εκτέλεσης του κώδικα.
- Έναν δρομολογητή (Router), ο οποίος ρυθμίζεται αυτόματα.
- Έναν διακομιστή AAA (AAA server), ο οποίος χρησιμοποιείται για την απομακρυσμένη αυθεντικοποίηση.
- Ένα μεταγωγέα Ethernet (Ethernet Switch).
- Έναν NAT Cloud, ο οποίος συνδέει το δίκτυο με το διαδίκτυο.

Στη συνέχεια, γίνεται η παραμετροποίηση των συσκευών του δικτύου. Συγκεκριμένα, στον δρομολογητή εισάγεται η στατική διεύθυνση 192.168.122.200 στη διεπαφή gi0/0 και ενεργοποιείται. Επιπλέον, ρυθμίζεται ώστε να δέχεται απομακρυσμένο έλεγχο, χρησιμοποιώντας στοιχεία εισόδου που ελέγχονται τοπικά, με το όνομα χρήστη "cisco" και τον κωδικό πρόσβασης "cisco". Ο σταθμός εργασίας και ο διακομιστής AAA ρυθμίζονται ώστε να λαμβάνουν δυναμική διεύθυνση IP μέσω του NAT. Στην τρέχουσα διαμόρφωση, ο σταθμός εργασίας λαμβάνει τη διεύθυνση IP 192.168.122.111, ενώ ο διακομιστής AAA λαμβάνει τη διεύθυνση 192.168.122.4. Στη συνέχεια, πραγματοποιείται έλεγχος για την επικοινωνία μεταξύ όλων των συσκευών.

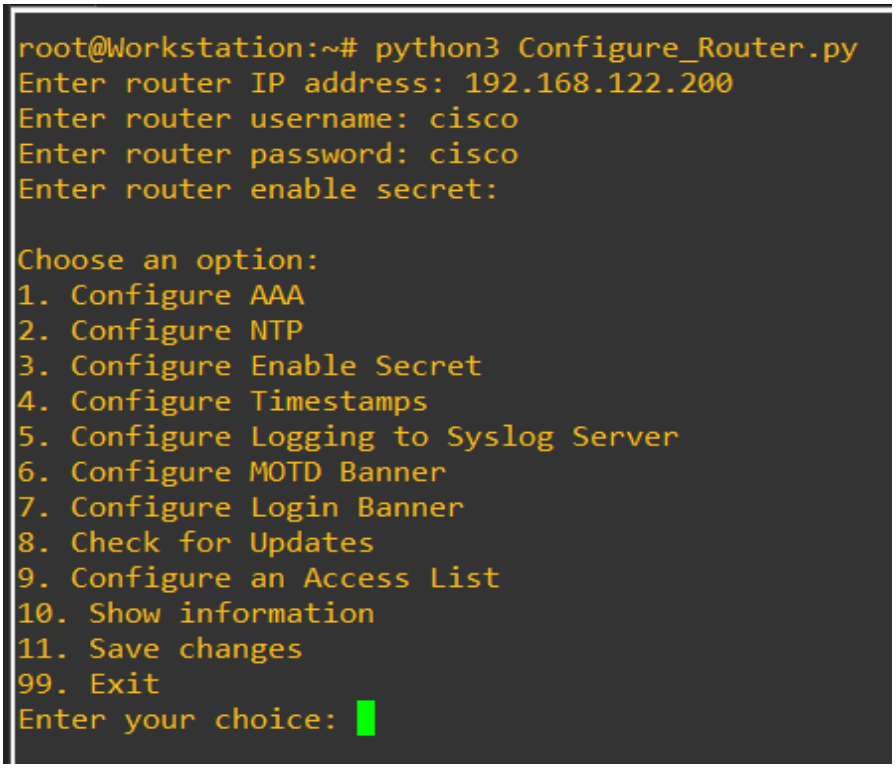


Εικόνα 18 Τοπολογία δικτύου

3.3 Εκτέλεση κώδικα

Μετά την εκτέλεση του αρχείου Configure_Router.py μέσω του Python 3, ο χρήστης καλείται να εισάγει τη διεύθυνση IP του δρομολογητή που επιθυμεί να παραμετροποιήσει, καθώς και τα διαπιστευτήριά του για την απομακρυσμένη είσοδο στον δρομολογητή. Αφού αυτά τα στοιχεία εισαχθούν με επιτυχία, παρουσιάζεται το μενού επιλογών. Σε αυτό το σημείο, ο χρήστης έχει τη δυνατότητα να επιλέξει την επιθυμητή λειτουργία που επιθυμεί να εκτελέσει στον δρομολογητή.

Το μενού επιλογών προσφέρει μια σειρά από επιλογές, οι οποίες σχετίζονται με διάφορες λειτουργίες ασφαλείας και παραμετροποίησης του δρομολογητή. Κατά την επιλογή μιας ενέργειας, το πρόγραμμα εκτελεί τις απαραίτητες ενέργειες για την ρύθμιση και την εφαρμογή των σχετικών ρυθμίσεων στον δρομολογητή. Με αυτόν τον τρόπο, παρέχεται στον χρήστη η δυνατότητα να επιλέξει και να εκτελέσει διάφορες λειτουργίες, ενώ ταυτόχρονα διευκολύνεται η διαχείριση και η παραμετροποίηση του δρομολογητή.



Εικόνα 19 Εκτέλεση του κώδικα και σύνδεση με το δρομολογητή

3.4 Διαμόρφωση AAA

Όταν ο χρήστης επιλέγει την επιλογή '1', πραγματοποιείται η διαμόρφωση της αυθεντικοποίησης μέσω ενός διακομιστή AAA (Authentication, Authorization, and Accounting). Σε αυτό το παράδειγμα, ο διακομιστής έχει τη διεύθυνση IP 192.168.122.4. Τα διαπιστευτήρια που έχουν καταχωρηθεί στον διακομιστή AAA είναι το όνομα χρήστη "gns3" και ο κωδικός πρόσβασης "gns3". Με την παροχή αυτών των πληροφοριών, εκτελούνται οι απαραίτητες εντολές προκειμένου να ρυθμιστεί η αυθεντικοποίηση του δρομολογητή. Έτσι, η είσοδος στο command-line interface (CLI) του δρομολογητή γίνεται με τον έλεγχο των διαπιστευτηρίων από έναν απομακρυσμένο διακομιστή.

Σε πιο λεπτομερές επίπεδο, η διαμόρφωση της αυθεντικοποίησης περιλαμβάνει τη διαμόρφωση του δρομολογητή ώστε να αναγνωρίζει τον διακομιστή AAA ως μέσο ελέγχου ταυτότητας και εξουσιοδότησης. Επίσης, η παραμετροποίηση των διαπιστευτηρίων είναι ουσιώδης για τη σωστή αυθεντικοποίηση των χρηστών. Τα δεδομένα αυτά αποτελούν την πρόσβαση σε ευαίσθητες πληροφορίες και, συνεπώς, η σωστή διαχείρισή τους είναι ζωτικής σημασίας για την ασφάλεια και την ομαλή λειτουργία του δικτύου.

```
Choose an option:
1. Configure AAA
2. Configure NTP
3. Configure Enable Secret
4. Configure Timestamps
5. Configure Logging to Syslog Server
6. Configure MOTD Banner
7. Configure Login Banner
8. Check for Updates
9. Configure an Access List
10. Show information
11. Save changes
99. Exit
Enter your choice: 1
Enter TACACS+ server IP: 192.168.122.4
Enter TACACS+ server username: gns3
Enter TACACS+ server password: gns3
configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#aaa new-model
R1(config)#tacacs server MyTacServ
R1(config-server-tacacs)#address ipv4 192.168.122.4
R1(config-server-tacacs)#key  gns3
 WARNING: Command has been added to the configuration using a type 0 password. Ho
recated. Migrate to a supported password type
 WARNING: Command has been added to the configuration using a type 0 password. Ho
recated. Migrate to a supported password type
R1(config-server-tacacs)#exit
R1(config)#aaa group server tacacs+ gns3group1
R1(config-sg-tacacs+)#server name MyTacServ
R1(config-sg-tacacs+)#exit
R1(config)#aaa authentication login default group gns3group1 local
R1(config)#end
R1#
Successful Configuration
```

Εικόνα 20 Εκτέλεση της επιλογής 1

Εν προκειμένω, όπως παρατηρείται στην εικόνα που ακολουθεί, η διαδικασία αυθεντικοποίησης των χρηστών επαναπροσδιορίζεται, επιτρέποντας την εκτέλεση της διαδικασίας από απομακρυσμένο εξυπηρετητή (server). Τα στοιχεία εισόδου που προσδιορίζονται όχι πλέον τοπικά στη συσκευή, αλλά αντίθετα, διατίθενται από τον εξυπηρετητή AAA (Authentication, Authorization, and Accounting), με τη χρήση των διαπιστευτηρίων χρήστη "gns3" και κωδικού πρόσβασης "gns3". Επομένως, η διαδικασία επικύρωσης ταυτότητας των χρηστών διεκπεραιώνεται από τον εξυπηρετητή, υποβαθμίζοντας την εξουσία ελέγχου από τη συσκευή στον εξυπηρετητή. Συνεπώς, κάθε φορά που εκτελείται ο κώδικας, οι παρεχόμενες πληροφορίες εισόδου πρέπει να αντιστοιχούν στα στοιχεία που καθορίζονται από τον εξυπηρετητή.

Εικόνα 21 Είσοδος με αυθεντικοποίηση μέσω του AAA server

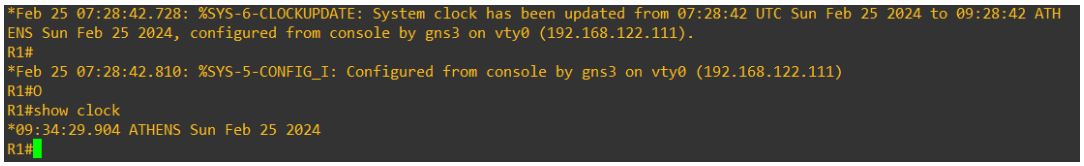
3.5 Διαμόρφωση NTP

Η διαδικασία της επιλογής 2 αφορά τον συγχρονισμό του χρονισμού του δρομολογητή με την κανονική χρονική παροχή, η οποία επιτυγχάνεται μέσω του πρωτοκόλλου NTP. Συγκεκριμένα, κατά την επιλογή αυτή, ο δρομολογητής επικοινωνεί με έναν εξυπηρετητή NTP με διεύθυνση IP 64.209.210.20, ο οποίος παρέχει την τρέχουσα χρονική πληροφορία. Έπειτα, με βάση την ανάκτηση αυτής της πληροφορίας, το ρολόι του δρομολογητή ρυθμίζεται αντίστοιχα, προσαρμόζοντας την τρέχουσα ώρα στην τοπική ζώνη χρόνου UTC +2.

Ο ρόλος του NTP στη διαδικασία αυτή είναι κρίσιμος, καθώς εξασφαλίζει την ακρίβεια και τον συγχρονισμό του χρονισμού σε δίκτυα όπου είναι απαραίτητη η συνέπεια του χρόνου για λειτουργικούς λόγους, όπως οι αρχειοθετήσεις, οι χρονοσφραγίδες, και ο συγχρονισμός συστημάτων καταγραφής γεγονότων. Με τη χρήση του NTP, η ακρίβεια του χρονισμού βελτιώνεται και ο δρομολογητής είναι σε θέση να διατηρεί ακριβή χρονική συγχρονισμένη προβολή, προσφέροντας έτσι αξιόπιστη λειτουργία στο δίκτυο.

```
Enter your choice: 2
configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ntp server 64.209.210.20
R1(config)#clock timezone ATHENS 2
R1(config)#end
R1#
Successful Configuration
```

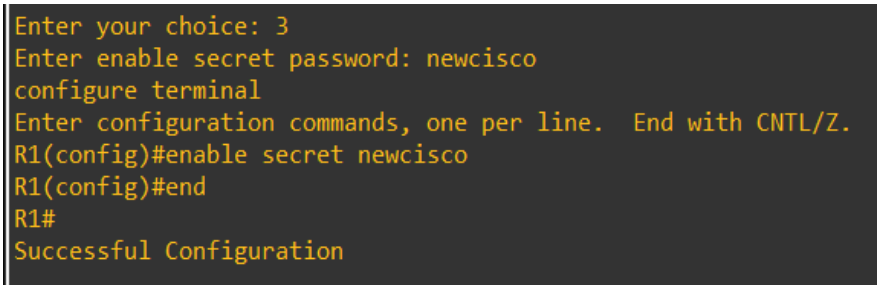
Εικόνα 22 Εκτέλεση της διαμόρφωσης NTP



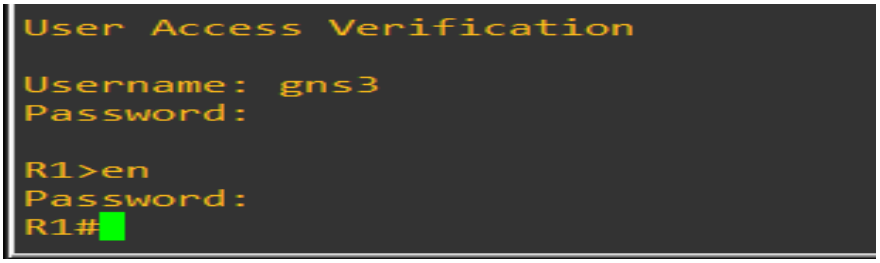
Εικόνα 23 Έλεγχος ρολογιού του δρομολογητή

3.6 Ενεργοποίηση secret password

Η τρίτη επιλογή του μενού αφορά την ενεργοποίηση του κωδικού πρόσβασης που απαιτείται για την είσοδο στη λειτουργία ενεργοποίησης (enable mode) του δρομολογητή. Συγκεκριμένα, χρησιμοποιείται ο κωδικός enable secret, ο οποίος αποτελεί έναν κρυπτογραφημένο κωδικό πρόσβασης που προστατεύει την πρόσβαση σε προνομιούχες λειτουργίες του δρομολογητή. Η χρήση του enable secret είναι κρίσιμη για την ασφάλεια του δικτύου, καθώς προσφέρει υψηλό επίπεδο προστασίας από μη εξουσιοδοτημένη πρόσβαση. Αυτός ο κωδικός αποθηκεύεται με ασφαλή τρόπο στη μνήμη του δρομολογητή, κρυπτογραφημένος έτσι ώστε να εξασφαλίζεται η μέγιστη προστασία των διαπιστευτηρίων. Η χρήση του enable secret αντιπροσωπεύει ένα σημαντικό βήμα για τη διασφάλιση της ασφάλειας του δικτύου, καθώς εξασφαλίζει ότι μόνο εξουσιοδοτημένοι χρήστες θα έχουν πρόσβαση σε ευαίσθητες λειτουργίες του δρομολογητή.



Εικόνα 24 Καθορισμος του secret password



Εικόνα 25 Επιβεβαίωση ενεργοποίησης του secret password

3.7 Ενεργοποίηση των Timestamps

Με την επιλογή αυτή, ενεργοποιείται η λειτουργία των χρονικών σφραγίδων (timestamps) στα μηνύματα που εκδίδει ο δρομολογητής. Κάθε φορά που συμβαίνει ένα γεγονός ή μια ενέργεια στον δρομολογητή, όπως μια αλλαγή στις ρυθμίσεις ή ένα συμβάν δικτύου, η ημερομηνία και η ώρα του γεγονότος καταγράφονται αυτόματα στα αντίστοιχα μηνύματα που καταγράφονται στο σύστημα καταγραφής (logging system) του δρομολογητή. Αυτό δίνει τη δυνατότητα στον διαχειριστή να αναγνωρίζει με ακρίβεια τον χρόνο και τη σειρά που συνέβησαν τα γεγονότα, επιτρέποντας έτσι μια ευκολότερη παρακολούθηση της δραστηριότητας του δικτύου και μια πιο αποτελεσματική διαχείριση των αλλαγών και των προβλημάτων. Με τη χρήση των χρονικών σφραγίδων, ο διαχειριστής μπορεί να αναλύει τα μηνύματα καταγραφής και να εξετάζει την ακριβή χρονική σειρά των εκδηλώσεων, βοηθώντας τον να προσδιορίζει την προέλευση πιθανών προβλημάτων και να λαμβάνει τα απαραίτητα μέτρα αντιμετώπισής τους.

```
Enter your choice: 4
configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#service timestamps debug datetime localtime show-timezone msec year
R1(config)#service timestamps log datetime localtime show-timezone msec year
R1(config)#end
R1#
Successful Configuration
```

Εικόνα 26 Εκτέλεση επιλογής 4

```
*Feb 25 2024 09:47:13.134 ATHENS: %SYS-5-CONFIG_I: Configured from console by gns3 on vty0 (192.168.122.111)
R1#
```

Εικόνα 27 Επιβεβαίωση ενεργοποίησης των timestamps

3.8 Ενεργοποίηση καταγραφής

Το logging αναφέρεται στη διαδικασία καταγραφής των διαφόρων γεγονότων, ενεργειών και εκδηλώσεων που συμβαίνουν σε ένα δίκτυο ή σε μια δικτυακή συσκευή, όπως ένας δρομολογητής ή ένας διακομιστής. Τα γεγονότα αυτά καταγράφονται σε ένα αρχείο καταγραφής (log file) με σκοπό την αρχειοθέτηση και την ανάλυσή τους από τους διαχειριστές του δικτύου. Η καταγραφή των γεγονότων μέσω του logging είναι απαραίτητη για την παρακολούθηση της λειτουργίας του δικτύου, τον εντοπισμό προβλημάτων, την ανίχνευση ασφαλείας και τη διερεύνηση περιστατικών. Καταγράφονται διάφορα συμβάντα όπως αποτυχίες σύνδεσης, επιθέσεις ασφαλείας, αλλαγές στις ρυθμίσεις, ενημερώσεις λογισμικού και πολλά άλλα. Η παρακολούθηση των καταγεγραμμένων γεγονότων μπορεί να βοηθήσει τους διαχειριστές να προλάβουν προβλήματα, να αποκαταστήσουν πιθανά προβλήματα και να βελτιώσουν την ασφάλεια και την απόδοση του δικτύου. Με την επιλογή 5, ο χρήστης ενεργοποιεί την λειτουργία απομακρυσμένης καταγραφής συμβάντων στο δίκτυο. Μέσω της επιλογής αυτής, ο χρήστης καθορίζει τη διεύθυνση IP του καταγραφικού (logging server) και τη διεπαφή του δρομολογητή από την οποία επιθυμεί να καταγράφονται τα γεγονότα. Αυτό επιτρέπει στο δίκτυο να αποθηκεύει τα λογισμικά και τα γεγονότα δικτύου σε ένα κεντρικό σημείο, προσφέροντας έτσι εύκολη πρόσβαση, ανάκτηση και ανάλυση των δεδομένων.

```
Enter your choice: 5
Enter syslog server IP address: 192.168.122.192
Enter interface for syslog: g0/0
configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#logging host 192.168.122.192
R1(config)#logging trap notifications
R1(config)#logging source-interface g0/0
R1(config)#end
R1#
Successful Configuration
```

Εικόνα 28 Εκτέλεση της επιλογής 5

```
R1#
*Feb 25 2024 09:52:58.298 ATHENS: %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 192.168.122.192 port 514 started - CLI initiated
```

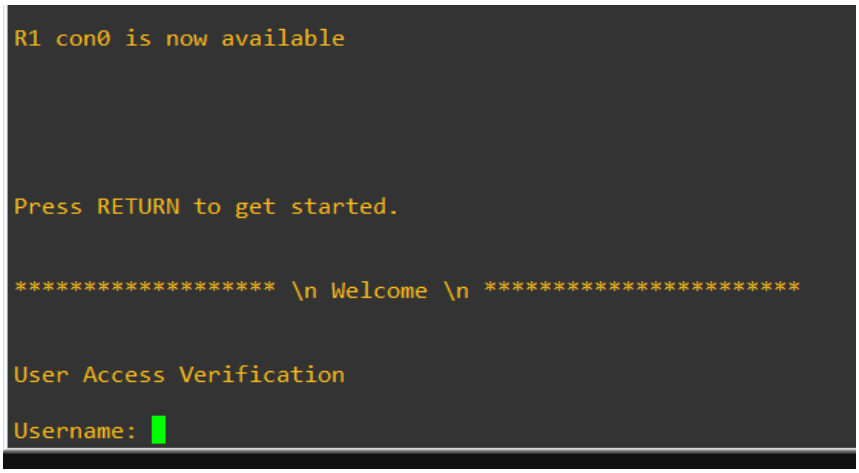
Εικόνα 29 Επιβεβαίωση έναρξης καταγραφής

3.9 Ενεργοποίηση του MOTD Banner

Με την επιλογή 6, ο χρήστης μπορεί να καθορίσει ένα μήνυμα που θα εμφανίζεται κατά την είσοδό του στον δρομολογητή, γνωστό ως Message of the Day (motd). Το μήνυμα αυτό είναι ένα κείμενο που παρέχει πληροφορίες, ειδοποιήσεις ή οδηγίες που απευθύνονται στους χρήστες κατά την είσοδό τους στο σύστημα. Η λειτουργία αυτή επιτρέπει στους διαχειριστές του δικτύου να επικοινωνούν σημαντικές πληροφορίες με τους χρήστες κατά την είσοδό τους, όπως προγραμματισμένες συντηρήσεις, πολιτικές χρήσης του συστήματος, πληροφορίες ασφαλείας ή οποιεσδήποτε άλλες σημαντικές ειδοποιήσεις. Μέσω αυτής της λειτουργίας, οι διαχειριστές μπορούν να διασφαλίσουν ότι οι χρήστες είναι ενήμεροι για τυχόν σημαντικές αλλαγές ή πληροφορίες που αφορούν το δίκτυο ή τη χρήση του συστήματος.

```
Enter your choice: 6
Enter delimiter character: #
Enter Message of the Day (MOTD):
 ********** \n Welcome \n **********
```

Εικόνα 30 Ενεργοποίηση του motd

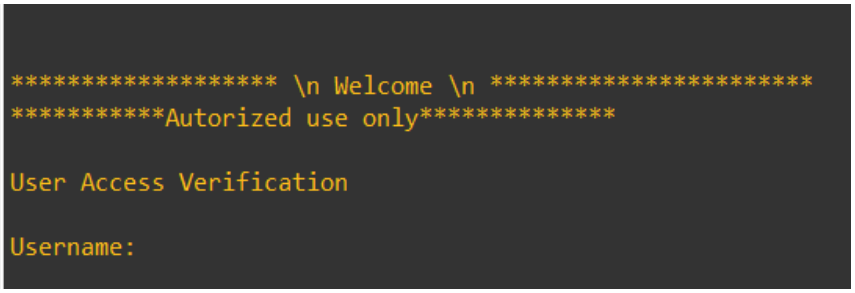


Εικόνα 31 Επιβεβαίωση ενεργοποίησης motd

3.10 Ενεργοποίηση του Login Banner

Με την επιλογή 7, ο χρήστης μπορεί να ορίσει ένα μήνυμα που θα εμφανίζεται κατά την είσοδο του στον δρομολογητή, γνωστό ως Login Banner. Το μήνυμα αυτό είναι ένα κείμενο που εμφανίζεται πριν ακόμη ο χρήστης εισέλθει στο σύστημα, προσφέροντας πληροφορίες, ειδοποιήσεις ή οδηγίες. Η λειτουργία του Login Banner επιτρέπει στους διαχειριστές του δικτύου να επικοινωνούν σημαντικές πληροφορίες με τους χρήστες πριν ακόμη αυτοί αποκτήσουν πρόσβαση στο σύστημα. Αυτό μπορεί να περιλαμβάνει πληροφορίες σχετικά με την πολιτική χρήσης του συστήματος, προειδοποιήσεις ασφαλείας, αιτήματα για την προστασία του απορρήτου ή άλλες σχετικές ειδοποιήσεις. Μέσω αυτής της λειτουργίας, οι διαχειριστές μπορούν να διασφαλίσουν ότι οι χρήστες είναι ενημερωμένοι για τυχόν πολιτικές ή ασφαλείας πριν από την πρόσβασή τους στο σύστημα.

Εικόνα 32 Ενεργοποίση του login banner



Εικόνα 33 Επιβεβαίωση του login banner

3.11 Διαμόρφωση Λιστών Ελέγχου Πρόσβασης

Με την επιλογή 9, ο χρήστης έχει τη δυνατότητα να δημιουργήσει μια access-list και να την εφαρμόσει σε μια συγκεκριμένη διεπαφή του δρομολογητή. Η διαδικασία αυτή χαρακτηρίζεται από ένα οδηγούμενο μενού, στο οποίο ο χρήστης καθορίζει πρώτα εάν η εντολή θα είναι permit ή deny, και στη συνέχεια επιλέγει τον στόχο της εντολής. Αυτό μπορεί να είναι ένας συγκεκριμένος χρήστης (any), μια διεύθυνση IP (ip) ή ένα δίκτυο (net). Μετά την καθορισμένη εντολή, ο χρήστης έχει τη δυνατότητα να προσθέσει επιπλέον κανόνες στη λίστα, ανάλογα με τις ανάγκες του δικτύου. Στο τέλος, ο χρήστης καθορίζει σε ποια διεπαφή του δρομολογητή θα εφαρμοστεί η access-list και εάν αυτή θα ισχύει για εισερχόμενη ή εξερχόμενη κίνηση. Με τη χρήση της access-list, ο χρήστης μπορεί να ελέγξει και να περιορίσει την κίνηση που περνάει μέσα από μια συγκεκριμένη διεπαφή του δρομολογητή, βασιζόμενος σε διάφορα κριτήρια όπως η προέλευση ή ο προορισμός της κίνησης, ο τύπος του πρωτοκόλλου κ.λπ. Με αυτόν τον τρόπο, επιτυγχάνεται προστασία και ασφάλεια του δικτύου, ελέγχοντας την πρόσβαση και τη ροή των δεδομένων.

```
Enter your choice: 9
Enter the number of the access list to configure (e.g., 10): 10
Configure Access List:
1. Permit
2. Deny
Enter your choice (1/2): 1
Enter IP type ('any' for any IP, 'host' for single host, 'net' for network/subnet): any
Do you want to add another rule? (yes/no): yes
Configure Access List:
1. Permit
2. Deny
Enter your choice (1/2): 2
Enter IP type ('any' for any IP, 'host' for single host, 'net' for network/subnet): host
Enter source IP address: 192.168.1.1
Do you want to add another rule? (yes/no): yes
Configure Access List:
1. Permit
2. Deny
Enter your choice (1/2): 2
Enter IP type ('any' for any IP, 'host' for single host, 'net' for network/subnet): net
Enter source IP address: 192.168.2.0
Enter mask type ('subnet' for subnet mask or 'wildcard' for wildcard mask): wildcard
Enter wildcard mask (in the format 0.0.0.255): 0.0.0.255
Do you want to add another rule? (yes/no): no
Enter interface (e.g., GigabitEthernet0/0): g0/0
Enter traffic direction (in or out): in
configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#access-list 10 permit any
R1(config)#access-list 10 deny 192.168.1.1
% Access rule can't be configured at higher sequence num as it is part of the existing rule at sequence num 10
R1(config)#access-list 10 deny 192.168.2.0 0.0.0.255
R1(config)#interface g0/0
R1(config-if)#ip access-group 10 in
R1(config-if)#end
R1#
```

Εικόνα 34 Διαμόρφωση μιας access list

```
*Feb 25 2024 11:05:47.924 ATHENS: %SYS-5-CONFIG_I: Configured from console by gns3 on vty0 (192.168.122.192)
R1#show access-lists
Standard IP access list 10
    10 permit any (8 matches)
    20 deny   192.168.2.0, wildcard bits 0.0.0.255
```

Εικόνα 35 Επιβεβαίωσης δημιουργίας της λίστας

3.12 Εμφάνιση ρυθμίσεων

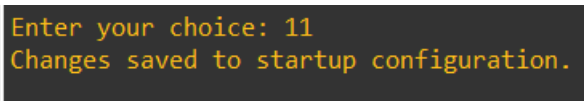
Με την επιλογή 10 προβάλλονται λεπτομερείς πληροφορίες σχετικά με τις τρέχουσες ρυθμίσεις που έχουν εφαρμοστεί στον δρομολογητή (router). Αυτές οι πληροφορίες μπορεί να περιλαμβάνουν τις διαμορφωμένες λίστες ελέγχου πρόσβασης (access-lists), τις ρυθμίσεις αυθεντικοποίησης, τα μηνύματα των banners που εμφανίζονται κατά τη σύνδεση, καθώς και άλλες καίριες παραμέτρους διαμόρφωσης του δικτύου. Αυτή η λειτουργία παρέχει στον χρήστη μια ολοκληρωμένη εικόνα των τρεχουσών ρυθμίσεων, επιτρέποντας την εύκολη παρακολούθηση και διαχείριση των δικτυακών παραμέτρων. Αυτό είναι ιδιαίτερα χρήσιμο για τους διαχειριστές δικτύων, καθώς τους επιτρέπει να επαληθεύουν τις ρυθμίσεις και να εντοπίζουν πιθανά προβλήματα ή κενά ασφαλείας.

```
AAA Configuration:
aaa new-model
aaa group server tacacs+ gns3group1
aaa authentication login default group gns3group1 local
aaa session-id common

NTP Configuration:

ntp server 64.209.210.20

Enable Secret Configuration:

enable secret 9 $9$9uGXhVRmUXi2rM$A8CD1nggUK97p9RNYbpmvI5mNAH5IsFcCi9XM11rZ.2

Timestamps Configuration:

service timestamps debug datetime msec localtime show-timezone year
service timestamps log datetime msec localtime show-timezone year

Logging Configuration:
logging host 192.168.122.111
logging host 192.168.122.192

MOTD Configuration:

banner motd ^C

Login Banner Configuration:

banner login ^C**********Autorized use only**************^C

IP Access-Group Configuration:
 ip access-group 10 in
 ip access-group 15 out

Interface Configuration:
interface GigabitEthernet0/0
interface GigabitEthernet0/1
interface GigabitEthernet0/2
interface GigabitEthernet0/3
logging source-interface GigabitEthernet0/0
Software Version:

Cisco IOS Software, IOSv Software (VIOS-ADVENTERPRISEK9-M), Version 15.9(3)M6, RELEASE SOFTWARE (fc1)
ROM: Bootstrap program is IOSv
Cisco IOSv (revision 1.0) with  with 460009K/62464K bytes of memory.
```

Εικόνα 36 Εμφανιση τρέχουσων ρυθμίσεων

3.13 Αποθήκευση αλλαγών

Με την επιλογή 11, οι αλλαγές που έχουν γίνει στις ρυθμίσεις του δρομολογητή αποθηκεύονται μόνιμα. Αυτή η ενέργεια εξασφαλίζει ότι οι τροποποιήσεις που έχουν γίνει θα διατηρηθούν ακόμα και μετά από επανεκκίνηση της συσκευής ή απώλεια ενέργειας. Αυτή η διαδικασία αποθήκευσης είναι κρίσιμη για τη σταθερότητα και την αξιοπιστία του δικτύου, καθώς διασφαλίζει ότι οι ρυθμίσεις παραμένουν σύμφωνες με τις επιθυμίες του διαχειριστή. Επιπλέον, η δυνατότητα αυτή εξασφαλίζει ότι οι αλλαγές που έχουν γίνει δεν θα χαθούν λόγω τυχόν αναποδιών στο δίκτυο ή απρόσμενων προβλημάτων στη συσκευή.



Εικόνα 37 Εκτέλεση επιλογής 11

Εικόνα 38 Επιβαιβέωση αποθήκευσης αλλαγών

Κεφάλαιο 4ο: Συμπεράσματα και προτάσεις βελτίωσης

Συμπερασματικά, η ανάλυση της σκληρυνσης δικτυακών συσκευών αναδεικνύει την ουσιώδη σημασία της για την ενίσχυση της ασφάλειας του δικτύου. Τα μέτρα αυτά περιλαμβάνουν την εφαρμογή πολυεπίπεδων προστατευτικών μέτρων, όπως η αυθεντικοποίηση, η κρυπτογράφηση και ο έλεγχος πρόσβασης. Η ανάλυση αποκαλύπτει την ανάγκη για την τακτική αναθεώρηση και ενημέρωση των προκαθορισμένων ρυθμίσεων, καθώς και την ανάγκη για την υιοθέτηση των πιο σύγχρονων προτύπων ασφάλειας.

Όσον αφορά τη βελτίωση του λογισμικού αυτοματοποίησης, προτείνεται η ενσωμάτωση πρόσθετων λειτουργιών που θα επιτρέπουν την πιο εκτεταμένη παραμετροποίηση και διαχείριση του δικτύου. Η προσθήκη επιλογών για τη διαμόρφωση προηγμένων ασφαλειακών πολιτικών, όπως η ευέλικτη διαχείριση access control lists (ACLs) και η ενίσχυση των λειτουργιών logging, θα επιτρέψει στους διαχειριστές να προσαρμόζουν το δίκτυο στις συγκεκριμένες απαιτήσεις ασφάλειας και διαθεσιμότητας. Επιπλέον, η ενσωμάτωση μηχανισμών παρακολούθησης και ειδοποίησης για την άμεση ανίχνευση και αντίδραση σε πιθανές απειλές θα ενισχύσει την ασφάλεια του δικτύου.

ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] National Security Agency. (June 2022). Cybersecurity Technical Report: Network Infrastructure Security Guide (Version 1.1). U/OO/118623-22, PP-22-0293.

[2] Cisco Systems. (Release 5.x). Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide. Chapter: Configuring VLANs. [Online]. Available: https://www.cisco.com

[3] Department for Works and Pensions. (March 2020). Security Standard Network Security Design (SS-018). Version 1.4. Chief Security Office.

[4] Michalski, J. T., & Wyant, F. J. (2012). Secure Network Design. Manuscript Completed: January 2012. Albuquerque, New Mexico: Sandia National Laboratories.

[5] Διεύθυνση Στρατηγικού Σχεδιασμού Κυβερνοασφάλειας, Τμήμα Απαιτήσεων και Αρχιτεκτονικής Ασφάλειας. (Ημερομηνία έκδοσης μη διαθέσιμη). Εγχειρίδιο Κυβερνοασφάλειας: Cybersecurity Handbook - Βέλτιστες πρακτικές για την προστασία και την ανθεκτικότητα των πληροφοριακών συστημάτων.

[6] Elwing-Malmfelt, L., & Keresztes, O. (2021). Semi-automated hardening of networks based on security classifications. Master's thesis, Master of Science in Engineering: Computer Security, June 2021.

[7] Strassberg, K. E. (n.d.). Network Device Security. In Strassberg, K. E. (Ed.), Network Device Security (pp. XX-XX). Chapter 10.

[8] Odom, W. (2020). CCNA 200-301 Official Cert Guide, Volume 1. Cisco Press.

[9] Odom, W. (2020). CCNA 200-301 Official Cert Guide, Volume 2. Cisco Press.

[10] Πολίτης, Α., & Χειλάς, Κ. (2023). *Προγραμματισμός Δικτυακών Συσκευών* [Εργαστηριακός Οδηγός]. Κάλλιπος, Ανοικτές Ακαδημαϊκές Εκδόσεις. https://dx.doi.org/10.57713/kallipos-343

[11] Cisco. (2020, September 4). Cisco Guide to Harden Cisco IOS Devices (Document ID: 13608). [Online]. Available: https://www.cisco.com

ΠΑΡΑΡΤΗΜΑ Α : ΚΩΔΙΚΑΣ ΛΟΓΙΣΜΙΚΟΥ

```
from netmiko import ConnectHandler
import logging
import logging.handlers
import requests
from bs4 import BeautifulSoup

def connect_to_router():
    # Prompt the user for router details
    host = input("Enter router IP address: ")
    username = input("Enter router username: ")
    password = input("Enter router password: ")
    secret = input("Enter router enable secret: ")

    router = {
        'device_type': 'cisco_ios',
        'host': host,
        'username': username,
        'password': password,
        'secret': secret,
    }

    try:
        net_connect = ConnectHandler(**router)
        net_connect.enable()
        return net_connect
    except Exception as e:
        print(f"Failed to connect to router: {e}")
        return None

def configure_aaa(net_connect, tacacs_host, tacacs_username, tacacs_password):
    # Implement AAA configuration with TACACS+
```

```
    aaa_config_commands = [
        'aaa new-model',
        'tacacs server MyTacServ',
        f'address ipv4 {tacacs_host}',
        f'key  {tacacs_password}',
        'exit',
        'aaa group server tacacs+ gns3group1',
        'server name MyTacServ',
        'exit' ,
        'aaa authentication login default group gns3group1 local',
            ]


 output = net_connect.send_config_set(aaa_config_commands)
    print(output)
    print('Successful Configuration')

def configure_ntp(net_connect, ntp_server):
    # Implement NTP configuration
    ntp_config_commands = [
        'ntp server 64.209.210.20',
        'clock timezone ATHENS 2' ,
        # Add more NTP server configurations as needed
    ]
    output = net_connect.send_config_set(ntp_config_commands)
    print(output)
    print('Successful Configuration')

def configure_enable_secret(net_connect, secret_password):
    # Configure enable secret password
    enable_secret_command = f'enable secret {secret_password}'
    output = net_connect.send_config_set([enable_secret_command])
    print(output)
```

```
    print('Successful Configuration')

def configure_timestamps(net_connect):
    # Implement Timestamps configuration
    timestamps_config_commands = [
        'service timestamps debug datetime localtime show-timezone msec year',
        'service timestamps log datetime localtime show-timezone msec year',
    ]
    output = net_connect.send_config_set(timestamps_config_commands)
    print(output)
    print('Successful Configuration')

def configure_logging(net_connect, syslog_server, interface):
    # Implement Logging configuration
    logging_config_commands = [
        f'logging host {syslog_server}',
        'logging trap notifications',  # Adjust logging level as needed
        f'logging source-interface {interface}',  # Specify the source interface
    ]
    output = net_connect.send_config_set(logging_config_commands)
    print(output)
    print('Successful Configuration')

def configure_syslog_logging(syslog_server):
    # Create a logger
    logger = logging.getLogger('my_logger')
    logger.setLevel(logging.DEBUG)

    # Create a SysLogHandler to send logs to the syslog server
    syslog_handler = logging.handlers.SysLogHandler(address=(syslog_server, 514))
    syslog_handler.setLevel(logging.DEBUG)

    # Set the formatter
```

```
    formatter = logging.Formatter('%(asctime)s - %(name)s - %(levelname)s - %(message)s')
    syslog_handler.setFormatter(formatter)

    # Add the SysLogHandler to the logger
    logger.addHandler(syslog_handler)

    return logger

def configure_motd(net_connect, motd):
    # Configure Message of the Day (MOTD)
    try:
        motd_config_commands = [
            f'banner motd ^{motd}^',
        ]
        output = net_connect.send_config_set(motd_config_commands)
        print(output)
        print('Successful Configuration')
    except Exception as e:
        print(f"Failed to configure MOTD: {e}")

def configure_login_banner(net_connect, banner):
    # Configure Login Banner
    try:
        login_banner_config_commands = [
            f'banner login ^{banner}^',
        ]
        output = net_connect.send_config_set(login_banner_config_commands)
        print(output)
        print('Successful Configuration')
    except Exception as e:
        print(f"Failed to configure login banner: {e}")

def check_for_updates():
```

```
    try:
        # Send a GET request to the Cisco software download page
        url = "https://software.cisco.com/download/home"
        response = requests.get(url)
        response.raise_for_status()

        # Parse the HTML content of the page
        soup = BeautifulSoup(response.text, "html.parser")

        # Extract relevant information (e.g., latest software version)
        latest_version = soup.select_one(".latest-release-row .release-version").get_text(strip=True)
        release_notes_link = soup.select_one(".latest-release-row .release-notes a")["href"]

        print("Latest software version:", latest_version)
        print("Release notes:", release_notes_link)

    except Exception as e:
        print("Failed to check for updates:", e)

def display_router_info(net_connect):
    try:
        print("\nCurrent Router Configuration:")
        print("-------------------------------")

        # Retrieve and print AAA configuration
        aaa_config = net_connect.send_command("show running-config | include aaa")
        print("AAA Configuration:")
        print(aaa_config)

        # Retrieve and print NTP configuration
        ntp_config = net_connect.send_command("show running-config | include ntp")
        print("\nNTP Configuration:")
```

```
print(ntp_config)

# Retrieve and print enable secret configuration
enable_secret_config = net_connect.send_command("show running-config | include enable secret")
print("\nEnable Secret Configuration:")
print(enable_secret_config)

# Retrieve and print timestamps configuration
timestamps_config = net_connect.send_command("show running-config | include service timestamps")
print("\nTimestamps Configuration:")
print(timestamps_config)

# Retrieve and print logging configuration
logging_config = net_connect.send_command("show running-config | include logging host")
print("\nLogging Configuration:")
print(logging_config)

# Retrieve and print MOTD configuration
motd_config = net_connect.send_command("show running-config | include banner motd")
print("\nMOTD Configuration:")
print(motd_config)

# Retrieve and print login banner configuration
login_banner_config = net_connect.send_command("show running-config | include banner login")
print("\nLogin Banner Configuration:")
print(login_banner_config)

    # Retrieve and print IP access-group configuration
ip_access_group_config = net_connect.send_command("show running-config | include ip access-group")
print("\nIP Access-Group Configuration:")
print(ip_access_group_config)
```

```
            # Retrieve and print interface configuration
        interface_config = net_connect.send_command("show running-config | include interface")
        print("\nInterface Configuration:")
        print(interface_config)

       # Retrieve and print software version
        software_version = net_connect.send_command("show version | include IOS")
        print("Software Version:")
        print(software_version)



    except Exception as e:
        print(f"Failed to display router info: {e}")

def configure_access_lists(net_connect):
    try:
        acl_number = input("Enter the number of the access list to configure (e.g., 10): ")

        # Check if the ACL number already exists
        existing_acl = check_existing_access_lists(net_connect, acl_number)

        if existing_acl:
            print(f"Access list {acl_number} already exists.")
            modification_option = input("Do you want to modify it? (yes/no): ")
            if modification_option.lower() != 'yes':
                print("Exiting.")
                return

        access_list_config_commands = []

        while True:
            print("Configure Access List:")
```

```
        print("1. Permit")
        print("2. Deny")
        choice = input("Enter your choice (1/2): ")

        if choice not in ['1', '2']:
            print("Invalid choice.")
            continue

        action = 'permit' if choice == '1' else 'deny'

        ip_type = input("Enter IP type ('any' for any IP, 'host' for single host, 'net' for network/subnet):
")
        if ip_type.lower() == 'any':
            source_ip = 'any'
        elif ip_type.lower() == 'host':
            source_ip = input("Enter source IP address: ")
        elif ip_type.lower() == 'net':
            source_ip = input("Enter source IP address: ")
            mask_type = input("Enter mask type ('subnet' for subnet mask or 'wildcard' for wildcard
mask): ")
            if mask_type.lower() == 'subnet':
                subnet_mask = input("Enter subnet mask (in the format /nn): ")
                source_ip += subnet_mask
            elif mask_type.lower() == 'wildcard':
                wildcard_mask = input("Enter wildcard mask (in the format 0.0.0.255): ")
                source_ip += f" {wildcard_mask}"
            else:
                print("Invalid mask type.")
                continue
        else:
            print("Invalid IP type.")
            continue

        access_list_config_commands.append(f'access-list {acl_number} {action} {source_ip}')
```

```
            add_another = input("Do you want to add another rule? (yes/no): ")
            if add_another.lower() != 'yes':
                break

        interface = input("Enter interface (e.g., GigabitEthernet0/0): ")
        direction = input("Enter traffic direction (in or out): ")

        if direction.lower() not in ['in', 'out']:
            print("Invalid direction.")
            return

        access_list_config_commands.append(f'interface {interface}')
        access_list_config_commands.append(f'ip access-group {acl_number} {direction.lower()}')

        # If the access list already exists, remove it first before applying the modified configuration
        if existing_acl:
            remove_acl_command = f'no access-list {acl_number}'
            net_connect.send_config_set([remove_acl_command])

        # Send the access list configuration commands
        output = net_connect.send_config_set(access_list_config_commands)
        print(output)
    except Exception as e:
        print(f"Failed to configure access lists: {e}")


def save_to_startup_config(net_connect):
    try:
        save_command = "write memory"
        output = net_connect.send_command(save_command)
        print("Changes saved to startup configuration.")
    except Exception as e:
```

```
        print(f"Failed to save changes to startup configuration: {e}")


def main():
    net_connect = connect_to_router()
    if net_connect:
        while True:
            print("\nChoose an option:")
            print("1. Configure AAA")
            print("2. Configure NTP")
            print("3. Configure Enable Secret")
            print("4. Configure Timestamps")
            print("5. Configure Logging to Syslog Server")
            print("6. Configure MOTD Banner")
            print("7. Configure Login Banner")
            print("8. Check for Updates")
            print("9. Configure an Access List")
            print("10. Show information")
            print("11. Save changes")

            # Add more options for other configurations
            print("99. Exit")
            choice = input("Enter your choice: ")

            if choice == '1':
                tacacs_host = input("Enter TACACS+ server IP: ")
                tacacs_username = input("Enter TACACS+ server username: ")
                tacacs_password = input("Enter TACACS+ server password: ")
                configure_aaa(net_connect, tacacs_host, tacacs_username, tacacs_password)
            elif choice == '2':
                 configure_ntp(net_connect, ntp_server)
            elif choice == '3':
                secret_password = input("Enter enable secret password: ")
                configure_enable_secret(net_connect, secret_password)
```

```
        elif choice == '4':
            configure_timestamps(net_connect)
        elif choice == '5':
            syslog_server = input("Enter syslog server IP address: ")
            interface = input("Enter interface for syslog: ")
            configure_logging(net_connect, syslog_server, interface)
        elif choice == '6':
            motd = input("Enter Message of the Day (MOTD): ")
            configure_motd(net_connect, motd)
        elif choice == '7':
            banner = input("Enter login banner: ")
                    configure_login_banner(net_connect, banner)
        elif choice == '8':
            check_for_updates()
        elif choice == '9' :
            configure_access_lists(net_connect)
        elif choice == '10':
            display_router_info(net_connect)
        elif choice == '11' :
           save_to_startup_config(net_connect)
        elif choice == '99':
            print("Exiting program.")
            break
        else:
            print("Invalid choice. Please try again.")

if __name__ == "__main__":
    main()
```