

ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ
ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ
ΚΑΙ ΗΛΕΚΤΡΟΝΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

«Σχεδιασμός και ανάπτυξη εργαλείου για την μαζική
και αυτοματοποιημένη παραμετροποίηση δικτυακών
συσκευών»



Του φοιτητή
Βασίλειου Μπιμπίλα
Αρ. Μητρώου: 113758

Επιβλέπων
Δρ. Σαρηγιαννίδης Αντώνης

Ημερομηνία 24/05/2024

Σχεδιασμός και ανάπτυξη εργαλείου για την μαζική και αυτοματοποιημένη παραμετροποίηση
δικτυακών συσκευών
24108

Βασίλειος Μπιμπίλας
Δρ. Σαρηγιαννίδης Αντώνης
Ημερομηνία ανάληψης Δ.Ε. 18-01-2024
Ημερομηνία περάτωσης Δ.Ε. 24-05-2024

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 Βασίλειου Μπιμπίλα 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 απαραίτητως και αποδοχή των απόψεων του συγγραφέα, εκ μέρους του Τμήματος.

Πρόλογος

Στην εποχή της ψηφιακής επανάστασης, η αποτελεσματική διαχείριση δικτύων αποτελεί βασικό παράγοντα για την επιτυχία και τη βιωσιμότητα των επιχειρήσεων. Η παρούσα διατριβή επικεντρώνεται στην ανάλυση και αξιολόγηση της πλατφόρμας “nimble”, ενός καινοτόμου εργαλείου αυτοματοποίησης και διαχείρισης δικτύων. Σκοπός της διατριβής είναι να παρουσιάσει τα οφέλη και τις δυνατότητες της πλατφόρμας “nimble” στην καθημερινή λειτουργία ενός εκτεταμένου εταιρικού δικτύου με κεντρικά γραφεία και πολλαπλά υποκαταστήματα. Η εταιρία που μελετάται διαθέτει Κέντρο Διαχείρισης Δικτύων (NOC) και αντιμετωπίζει αυξημένες ανάγκες για αποτελεσματική διαχείριση και ασφάλεια του δικτύου. Η ανάλυση περιλαμβάνει τη σύγκριση των παραδοσιακών χειροκίνητων διαδικασιών με τις αυτοματοποιημένες λύσεις που προσφέρει η πλατφόρμα “nimble”. Μέσω συγκεκριμένων σεναρίων χρήσης, αναδεικνύεται η συμβολή της πλατφόρμας στη μείωση των λειτουργικών δαπανών, την αύξηση της αποδοτικότητας και τη βελτίωση της ασφάλειας. Ελπίζω η παρούσα διατριβή να προσφέρει πολύτιμες γνώσεις και να συμβάλει στην κατανόηση των σύγχρονων εργαλείων διαχείρισης δικτύων, ενισχύοντας την καινοτομία και την αποτελεσματικότητα στις επιχειρησιακές πρακτικές.

Περίληψη

Στην ψηφιακή εποχή, η αποτελεσματική διαχείριση δικτύων είναι ζωτικής σημασίας για την επιτυχία των επιχειρήσεων. Η παρούσα διατριβή εστιάζει στην ανάλυση και αξιολόγηση της πλατφόρμας “nimble”, ενός σύγχρονου εργαλείου αυτοματοποίησης και διαχείρισης δικτύων, και εξετάζει την εφαρμογή της σε ένα εκτεταμένο εταιρικό περιβάλλον. Η μελέτη περίπτωσης αφορά μια υποθετική εταιρία με κεντρικά γραφεία και πολυάριθμα υποκαταστήματα σε όλη την Ελλάδα. Η εταιρία διαθέτει NOC, το οποίο αντιμετωπίζει αυξημένο φόρτο εργασίας και δυσκολίες στην εκπαίδευση νέων μηχανικών. Αναλύονται συγκεκριμένα σενάρια χρήσης της πλατφόρμας “nimble”, όπως η εγκατάσταση συστημάτων ασφαλείας σε υποκαταστήματα, περιγράφοντας λεπτομερώς τις διαδικασίες διευθυνσιοδότησης, ονοματοδοσίας, σύνδεσης νέου εξοπλισμού, διαχείρισης πρόσβασης και των απαιτούμενων εντολών και ενεργειών. Συγκρίνονται οι παραδοσιακές χειροκίνητες διαδικασίες με τις αυτοματοποιημένες λύσεις που προσφέρει η πλατφόρμα “nimble”. Τα αποτελέσματα δείχνουν ότι η χρήση της πλατφόρμας “nimble” μειώνει σημαντικά τον χρόνο και τον κόπο που απαιτούνται για τη διαχείριση του δικτύου. Η αυτοματοποίηση των διαδικασιών διευκολύνει την ενσωμάτωση νέου εξοπλισμού, βελτιώνει την ασφάλεια και εξασφαλίζει τη συμμόρφωση με τους κανονισμούς. Επιπλέον, η πλατφόρμα συμβάλλει στη μείωση των λειτουργικών δαπανών και στην αύξηση της αποδοτικότητας του NOC. Συμπερασματικά, η πλατφόρμα “nimble” αποδεικνύεται ως ένα ισχυρό εργαλείο για την αντιμετώπιση των προκλήσεων της σύγχρονης διαχείρισης δικτύων, προσφέροντας λύσεις που ενισχύουν την καινοτομία και την αποτελεσματικότητα στις επιχειρησιακές πρακτικές.

«Design and development of a tool for the mass and automated configuration of network devices»

Vasileios Bimpilas

Abstract

In the digital age, effective network management is vital for business success. This thesis focuses on the analysis and evaluation of the “nimble” platform, a modern tool for network automation and management, and examines its application in an extensive corporate environment. The case study involves a hypothetical company with headquarters and numerous branches throughout Greece. The company has a specialized Network Operations Center (NOC) that faces increased workload and challenges in training new engineers. Specific use cases of the “nimble” platform are analysed, such as the installation of security systems in branches, detailing the processes of addressing, naming, connecting new equipment, access management, and the required commands and actions. Traditional manual procedures are compared with the automated solutions offered by the “nimble” platform. The results show that using the “nimble” platform significantly reduces the time and effort required for network management. Automating processes facilitates the integration of new equipment, improves security, and ensures regulatory compliance. Additionally, the platform helps reduce operational costs and increases the efficiency of the NOC. In conclusion, the “nimble” platform proves to be a powerful tool for addressing the challenges of modern network management, offering solutions that enhance innovation and efficiency in business practices.

Ευχαριστίες

Θέλω να εκφράσω τις ειλικρινείς μου ευχαριστίες στην αγαπημένη μου οικογένεια για τη συνεχή υποστήριξη κατά τη διάρκεια των σπουδών μου. Η στήριξη και η αγάπη της μου έδωσαν τη δύναμη και τα εφόδια για να ολοκληρώσω αυτό το σπουδαίο ταξίδι.

Θέλω να ευχαριστήσω θερμά τους καθηγητές και συμφοιτητές μου για όλες τις γνώσεις και τις εμπειρίες που μοιραστήκαμε κατά τη διάρκεια των σπουδών μου. Η συνεργασία μας μου έδωσε την ευκαιρία να αναπτύξω τις δεξιότητές μου. Ειδικά θέλω να ευχαριστήσω τον καθηγητή κύριο Βασίλη Βίτσα διότι η πολύτιμη βοήθειά του ήταν κρίσιμη για την επίτευξη των στόχων μου.

Τέλος, δεν μπορώ παρά να ευχαριστήσω τον επιβλέποντα καθηγητή κύριο Αντώνη Σαρηγιαννίδη διότι πίστεψε στις δυνατότητες μου, αλλά και για την αμέριστη καθοδήγησή του κατά τη διάρκεια της συγγραφής της πτυχιακής μου διατριβής. Η υποστήριξή του ήταν καθοριστική για την ολοκλήρωση των σπουδών μου.

Περιεχόμενα

Πρόλογος.....	5
Περίληψη.....	6
Abstract.....	7
Ευχαριστίες.....	8
Περιεχόμενα.....	9
Κατάλογος Σχημάτων.....	11
Κατάλογος Πινάκων.....	12
Συνομογραφίες.....	13
Κεφάλαιο 1ο: Εισαγωγή	14
1.1 Εισαγωγή.....	14
1.2 Στόχοι και Σκοποί της Πτυχιακής Εργασίας	15
1.3 Δομή της Πτυχιακής Διατριβής	15
1.4 Επίλογος.....	16
Κεφάλαιο 2ο: Αυτοματοποιημένη Παραμετροποίηση Δικτυακών Συσκευών	17
2.1 Εισαγωγή.....	17
2.2 Παραδοσιακός τρόπος παραμετροποίησης δικτυακών συσκευών.....	17
2.2.1 Παραδοσιακός τρόπος παραμετροποίησης firewall.....	17
2.2.2 Παραδοσιακός τρόπος παραμετροποίησης routers και switches.....	18
2.2.3 Προβλήματα παραδοσιακής προσέγγισης	18
2.3 Εργαλεία αυτοματοποιημένης παραμετροποίησης	19
2.3.1 Cisco Catalyst Center.....	19
2.3.2 Terraform.....	19
2.3.3 IP Fabric.....	20
2.3.4 Itential.....	20
2.3.5 Junos Space Network Management Platform.....	21
2.4 Συνεισφορά της πλατφόρμας “nimble”.....	22
2.5 Επίλογος.....	23
Κεφάλαιο 3ο: Η Πλατφόρμα “nimble”	24
3.1 Εισαγωγή.....	24
3.2 Λειτουργία της Πλατφόρμας.....	24
3.2.1 Εργαλεία “Objects” και “Groups” για το Cisco FMC.....	24
3.2.2 Εργαλείο “Bulk Configurator” για τη Μαζική Παραμετροποίηση Δικτυακών Συσκευών	

3.3	Οφέλη για τους Network Administrators.....	24
3.4	Εργαλεία.....	25
3.4.1	Django για το Front και το Back-end.....	25
3.4.2	Python για την Υλοποίηση όλων των Λειτουργιών.....	25
3.4.3	Python API της Cisco για το FMC.....	25
3.4.4	Paramiko.....	26
3.4.5	Βιβλιοθήκη Python concurrent.....	26
3.4.6	Βιβλιοθήκη Bootstrap.....	26
3.4.7	Javascript.....	26
3.4.8	JSON και CSV.....	27
3.4.9	EVE-NG και VMware.....	27
3.5	Αρχιτεκτονική και λειτουργικότητα.....	28
3.5.1	Είσοδος στην πλατφόρμα.....	28
3.5.2	Βασικό Μενού.....	29
3.6	Δημιουργία νέου target.....	29
3.7	Εργαλεία για το FMC.....	31
3.7.1	Εργαλείο “Objects” για τη διαχείριση αντικειμένων.....	31
3.7.2	Εργαλείο “Groups” για διαχείρισης ομάδων object.....	36
3.8	Εργαλείο “Bulk Configurator” για μαζική και ταυτόχρονη παραμετροποίηση.....	42
3.9	Βάση δεδομένων.....	44
3.10	Επίλογος.....	45
Κεφάλαιο 4ο: Μελέτη Περίπτωσης Λειτουργίας της “nimble”		46
4.1	Εισαγωγή.....	46
4.2	Προφίλ Εικονικής Εταιρίας.....	46
4.3	Εξοπλισμός και Τοπολογία.....	47
4.4	Σενάριο Χρήσης της “nimble”.....	49
4.4.1	Σενάριο Α – Εγκατάσταση Συστημάτων Ασφαλείας.....	52
4.5	Επίλογος.....	79
Κεφάλαιο 5ο: Συμπεράσματα και Μελλοντικές Επεκτάσεις		81
5.1	Συμπεράσματα.....	81
5.2	Μελλοντικές επεκτάσεις.....	81
ΒΙΒΛΙΟΓΡΑΦΙΑ.....		82

Κατάλογος Σχημάτων

Σχήμα 3.1 Είσοδος στην πλατφόρμα.....	28
Σχήμα 3.2 Βασικό Μενού.....	29
Σχήμα 3.3 Προσθήκη νέου target Cisco FMC.....	30
Σχήμα 3.4 Προσθήκη νέου target group Cisco IOS.....	31
Σχήμα 3.5 Δυνατότητες εργαλείου Objects.....	32
Σχήμα 3.6 Δυνατότητα GET του εργαλείου Objects.....	33
Σχήμα 3.7 Δυνατότητα INSERT του εργαλείου Objects.....	34
Σχήμα 3.8 Δυνατότητα INSERT του εργαλείου Objects.....	35
Σχήμα 3.9 Δυνατότητα DELETE του εργαλείου Objects.....	36
Σχήμα 3.10 Δυνατότητες εργαλείου Groups.....	37
Σχήμα 3.11 Δυνατότητα GET του εργαλείου Groups.....	38
Σχήμα 3.12 Δυνατότητα INSERT του εργαλείου Groups.....	39
Σχήμα 3.13 Δυνατότητα MODIFY του εργαλείου Groups.....	40
Σχήμα 3.14 Δυνατότητα MODIFY MEMBERS του εργαλείου Groups.....	41
Σχήμα 3.15 Δυνατότητα DELETE του εργαλείου Groups.....	42
Σχήμα 3.16 Εργαλείο Bulk Configurator.....	44
Σχήμα 3.17 Βάση δεδομένων εφαρμογής.....	45
Σχήμα 4.1 Συσκευές τοπολογίας υποκαταστημάτων.....	48
Σχήμα 4.2 Τοπολογία υποκαταστημάτων.....	49
Σχήμα 4.3 VM που φιλοξενεί την πλατφόρμα.....	49
Σχήμα 4.4 Είσοδος στην πλατφόρμα.....	50
Σχήμα 4.5 Υποδοχή χρήστη από την πλατφόρμα.....	50
Σχήμα 4.6 Τοπολογία EVE-NG.....	51
Σχήμα 4.7 Cisco FMC.....	55
Σχήμα 4.8 Εντολές για Cisco router καταστημάτων.....	55
Σχήμα 4.9 Εντολές για Aruba switchr καταστημάτων.....	56
Σχήμα 4.10 Επιλογή προσθήκης νέου object στο FMC.....	57
Σχήμα 4.11 Προσθήκη νέου object στο FMC.....	57
Σχήμα 4.12 Επιλογή προσθήκης νέου group στο FMC.....	58
Σχήμα 4.13 Προσθήκη object group στο FMC.....	58
Σχήμα 4.14 Έλεγχος πλήθους object.....	60
Σχήμα 4.15 Έλεγχος απουσίας object.....	60
Σχήμα 4.16 Έλεγχος απουσίας subinterface.....	61
Σχήμα 4.17 Έλεγχος απουσίας subinterface.....	61
Σχήμα 4.18 Έλεγχος απουσίας switch configuration.....	62
Σχήμα 4.19 Έλεγχος απουσίας switch configuration.....	62
Σχήμα 4.20 Υποδοχή χρήστη από την πλατφόρμα.....	63
Σχήμα 4.21 Προσθήκη target FMC.....	63
Σχήμα 4.22 Υποδοχή χρήστη από την πλατφόρμα.....	64
Σχήμα 4.23 Εργαλεία για FMC.....	64
Σχήμα 4.24 Εργαλείο objects.....	64
Σχήμα 4.25 Προσθήκη FMC objects.....	65
Σχήμα 4.26 Προσθήκη FMC objects.....	66
Σχήμα 4.27 Αρχείο JSON για FMC objects.....	66

Σχήμα 4.28 Επιβεβαίωση πλήθους object.....	67
Σχήμα 4.29 Επιβεβαίωση object.....	67
Σχήμα 4.30 Εργαλείο groups.....	68
Σχήμα 4.31 Δημιουργία νέου object group.....	69
Σχήμα 4.32 Αρχείο JSON για FMC groups.....	69
Σχήμα 4.33 Επιβεβαίωση object group.....	69
Σχήμα 4.34 Επιβεβαίωση object group.....	69
Σχήμα 4.35 FMC ACP.....	70
Σχήμα 4.36 Κανόνες ACP.....	70
Σχήμα 4.37 Δημιουργία target group IOS.....	71
Σχήμα 4.38 Εργαλείο για Cisco IOS.....	71
Σχήμα 4.39 Εργαλείο Bulk Configurator.....	72
Σχήμα 4.40 Παραμετροποίηση Cisco routers.....	73
Σχήμα 4.41 Αρχείο JSON για Cisco routers.....	73
Σχήμα 4.42 Επιβεβαίωση παραμετροποίησης subinterface Cisco router.....	73
Σχήμα 4.43 Επιβεβαίωση παραμετροποίησης subinterface Cisco router.....	74
Σχήμα 4.44 Επιβεβαίωση παραμετροποίησης ACL Cisco router.....	74
Σχήμα 4.45 Επιβεβαίωση παραμετροποίησης ACL Cisco router.....	75
Σχήμα 4.46 Προσθήκη νέου target group AOS-CX.....	75
Σχήμα 4.47 Εργαλείο για AOS-CX.....	76
Σχήμα 4.48 Εργαλείο Bulk Configurator.....	76
Σχήμα 4.49 Παραμετροποίηση Aruba switches.....	77
Σχήμα 4.50 Αρχείο JSON για Aruba switches.....	78
Σχήμα 4.51 Επιβεβαίωση παραμετροποίησης VLAN Aruba switch.....	78
Σχήμα 4.52 Επιβεβαίωση παραμετροποίησης θυρών Aruba switch.....	78
Σχήμα 4.53 Επιβεβαίωση παραμετροποίησης θυρών Aruba switch.....	79

Κατάλογος Πινάκων

Πίνακας 4.1 Υποδίκτυα καταστημάτων.....	52
Πίνακας 4.2 IP διευθύνσεις συσκευών.....	52
Πίνακας 4.3 IP διευθύνσεις νέων συστ, ασφαλείας.....	53

Συντομογραφίες

ACP	Access Control Policy
CLI	Command Line Interface
CSV	Comma Separated Values
DNA	Digital Network Architecture
DVR	Digital Video Recorder
FMC	Firepower Management Center
FMCv	Firepower Management Center virtual
ID	Identification
IP	Internet Protocol
IaC	Infrastructure as Code
JS	Javascript
JSON	JavaScript Object Notation
MAC	Media Access Control
NOC	Network Operations Center
OSI	Open Systems Interconnection
TCP	Transport Control Protocol
UI	User Interface
URL	Uniform Resource Locator
VLAN	Virtual Local Area Network
VM	Virtual Machine
VPN	Virtual Private Network
NGFW	Next-Generation Firewall
VENV	Virtual Environment

Κεφάλαιο 1ο: Εισαγωγή

1.1 Εισαγωγή

Στη σύγχρονη εποχή, η δικτύωση αποτελεί ένα ζωτικό στοιχείο για τη λειτουργία και την επιτυχία των επιχειρήσεων [1]. Η ανάπτυξη και η διαχείριση αποτελεσματικών δικτύων επιτρέπει στις επιχειρήσεις να επικοινωνούν, να μοιράζονται πόρους και πληροφορίες, να βελτιστοποιούν τις διαδικασίες εργασίας και να ενισχύουν την ασφάλεια των δεδομένων τους [2]. Η δικτύωση επιτρέπει σε μια εταιρία να δημιουργήσει ένα ενιαίο περιβάλλον εργασίας, επιτρέποντας τη συνεργασία μεταξύ των εργαζομένων, την αποτελεσματική διαχείριση των διαδικασιών και την ανταλλαγή δεδομένων μεταξύ των διαφόρων τμημάτων της επιχείρησης.

Ένα δίκτυο μίας εταιρίας αποτελείται από μια ποικιλία δικτυακών συσκευών που συνεργάζονται για τη μεταφορά δεδομένων [3]. Αυτές οι συσκευές περιλαμβάνουν τα εξής:

- Δρομολογητές (Routers): Οι routers είναι υπεύθυνοι για τη μεταφορά των πακέτων δεδομένων μεταξύ διαφορετικών δικτύων. Αυτές οι συσκευές λειτουργούν στο επίπεδο 3 (επίπεδο δικτύου) του μοντέλου OSI και λαμβάνουν αποφάσεις για τη διαδρομή των πακέτων με βάση τις διευθύνσεις IP.
- Μεταγωγείς (Switches): Τα switches είναι υπεύθυνα για τη μετάδοση δεδομένων μεταξύ συσκευών εντός του ίδιου δικτύου. Λειτουργούν στο επίπεδο 2 (επίπεδο διασύνδεσης δεδομένων) του μοντέλου OSI και λαμβάνουν αποφάσεις για την παράδοση των πακέτων με βάση τη φυσική διεύθυνση MAC.
- Ασύρματα σημεία πρόσβασης (Wireless Access Points): Τα ασύρματα σημεία πρόσβασης επιτρέπουν στις συσκευές να συνδεθούν στο τοπικό δίκτυο χρησιμοποιώντας ασύρματη σύνδεση. Παρέχουν πρόσβαση στο δίκτυο για φορητές συσκευές, όπως φορητούς υπολογιστές, ταμπλέτες και smartphones.
- Διακομιστές (Servers): Οι servers είναι υπεύθυνοι για την παροχή υπηρεσιών στο δίκτυο. Αυτές οι υπηρεσίες μπορεί να περιλαμβάνουν αποθήκευση δεδομένων, κοινή χρήση αρχείων, εκτέλεση εφαρμογών, διαχείριση email και πολλά άλλα.
- Τοίχοι Προστασίας (Firewalls): Τα firewalls αποτελούν κρίσιμο κομμάτι της ασφάλειας του δικτύου, προστατεύοντας το από ανεπιθύμητη και κακόβουλη κίνηση. Επιτρέπουν ή αποκλείουν την πρόσβαση σε συγκεκριμένες υπηρεσίες ή πόρους βάσει των κανόνων πολιτικής ασφαλείας που έχουν οριστεί.

Αυτές οι δικτυακές συσκευές συνθέτουν το δίκτυο μιας εταιρίας και επιτρέπουν την αποτελεσματική επικοινωνία, διαχείριση και ασφάλεια των δεδομένων στο εργασιακό περιβάλλον.

Η διαχείριση μεγάλων εταιρικών δικτύων απαιτεί προσεκτικό σχεδιασμό, υλοποίηση και συντήρηση. Οι προκλήσεις περιλαμβάνουν [4]:

- Κλιμάκωση: Η διαχείριση ενός μεγάλου δικτύου απαιτεί την αντιμετώπιση προβλημάτων κλιμάκωσης, καθώς ο αριθμός των συνδεδεμένων συσκευών και χρηστών αυξάνεται.
- Ασφάλεια: Η προστασία των δεδομένων από απειλές όπως οι εξωτερικές επιθέσεις, οι κακόβουλες εφαρμογές και οι εσωτερικές απειλές απαιτεί προηγμένες λύσεις ασφαλείας.

- **Διαχείριση απόδοσης:** Η εξασφάλιση της ομαλής λειτουργίας και της υψηλής απόδοσης του δικτύου απαιτεί την παρακολούθηση της κίνησης δεδομένων, την αντιμετώπιση της συμφόρησης και τη βελτιστοποίηση των ρυθμίσεων.
- **Διαχείριση πόρων:** Η αποτελεσματική διαχείριση των δικτυακών πόρων, οι διαμοιρασμένες υπηρεσίες και η διαχείριση των δικαιωμάτων πρόσβασης είναι ζωτικής σημασίας.

Συνολικά, η επιτυχημένη διαχείριση ενός μεγάλου εταιρικού δικτύου απαιτεί τη χρήση προηγμένων τεχνολογιών και βέλτιστων πρακτικών, καθώς και τη συνεχή εκπαίδευση και ενημέρωση του προσωπικού [5].

Η πλατφόρμα “nimble” προσφέρει λύσεις αυτοματοποίησης [6], καθώς και μαζικής και ταυτόχρονης παραμετροποίησης πολλαπλών δικτυακών συσκευών, καθιστώντας το έργο της διαχείρισης μεγάλης κλίμακας δικτύων μία απλή και αποδοτική διαδικασία, μειώνοντας το χρόνο και το κόστος που απαιτείται για χειροκίνητες παρεμβάσεις. Επιπλέον, εξασφαλίζει υψηλά επίπεδα ασφάλειας και συμμόρφωσης με κανονισμούς, βελτιώνοντας την αξιοπιστία και την απόδοση των δικτύων.

1.2 Στόχοι και Σκοποί της Πτυχιακής Εργασίας

Οι στόχοι και σκοποί της πτυχιακής διατριβής είναι στενά συνδεδεμένοι με την ανάγκη για αποτελεσματική διαχείριση των δικτύων στον σύγχρονο επαγγελματικό χώρο. Με την έμφαση στην αυτοματοποίηση και την εξοικονόμηση χρόνου, η πλατφόρμα “nimble” έχει στόχο να παρέχει λύσεις που ανταποκρίνονται στις ανάγκες των διαχειριστών δικτύων [7] (*network administrators*), επιτρέποντάς τους να εστιάσουν τον χρόνο και τους πόρους τους σε πιο προχωρημένες και στρατηγικές εργασίες. Αντί να αφιερώνουν χρόνο σε διαδικασίες ρουτίνας και επαναλαμβανόμενες εργασίες, όπως η χειροκίνητη ρύθμιση συσκευών ή η επαναλαμβανόμενη εφαρμογή παραμέτρων, μπορούν να επικεντρωθούν σε άλλες δραστηριότητες που απαιτούν περισσότερη προσοχή και ανάλυση, όπως η ανάπτυξη στρατηγικών ασφαλείας, η επιλογή και η εφαρμογή νέων τεχνολογιών, ή η βελτίωση της απόδοσης του δικτύου. Κατ’ αυτόν τον τρόπο, η πλατφόρμα “nimble” επιτρέπει στους διαχειριστές να γίνουν πιο αποτελεσματικοί και προοδευτικοί στη διαχείριση των εταιρικών δικτύων.

Κεντρικός σκοπός της πλατφόρμας είναι η επιτάχυνση και η απλοποίηση των διαδικασιών διαχείρισης μεγάλης κλίμακας εταιρικών δικτύων [8]. Μέσω της αυτοματοποίησης, οι *network administrators* μπορούν να δημιουργούν και να εφαρμόζουν μαζικές ρυθμίσεις σε δικτυακές συσκευές, εξοικονομώντας σημαντικό χρόνο και αποφεύγοντας ανθρώπινα λάθη.

Οι *network administrators* θα επωφεληθούν από τη χρήση της πλατφόρμας “nimble” με την εξοικονόμηση χρόνου, την ελαχιστοποίηση λαθών, τη βελτίωση και την προβλεψιμότητα των χρόνων παράδοσης των εργασιών. Με αυτόν τον τρόπο, η πλατφόρμα “nimble” συμβάλλει στην επίτευξη υψηλού επιπέδου αποτελεσματικότητας και ασφάλειας στη διαχείριση των εταιρικών δικτύων.

1.3 Δομή της Πτυχιακής Διατριβής

Στο κεφάλαιο 2, με τίτλο “Αυτοματοποιημένη Παραμετροποίηση Δικτυακών Συσκευών”, περιγράφεται η παραδοσιακή διαδικασία παραμετροποίησης των δικτυακών συσκευών, εστιάζοντας στα προβλήματα που αντιμετωπίζονται σε αυτήν τη διαδικασία. Επιπλέον, περιγράφονται οι λύσεις που προσφέρει η πλατφόρμα “nimble”, συμπεριλαμβανομένων των οφελών της σε σχέση με άλλα εργαλεία αυτοματοποιημένης και μαζικής παραμετροποίησης [9]. Τέλος, αναδεικνύεται η προστιθέμενη αξία (*added value*) που προσφέρει η πλατφόρμα “nimble” σε σύγκριση με άλλες λύσεις.

Το κεφάλαιο 3, με τον τίτλο “Η Πλατφόρμα nimble”, παρουσιάζει λεπτομερώς τη λειτουργία και τα οφέλη της πλατφόρμας για τους network administrators. Περιγράφεται η πρακτική χρήση της πλατφόρμας από έναν network administrator, ενώ εξετάζονται επίσης η αρχιτεκτονική, η λειτουργικότητα και τα εργαλεία που περιλαμβάνει. Τέλος, παρουσιάζονται τα εργαλεία που χρησιμοποιήθηκαν για την ανάπτυξη της πλατφόρμας, καθώς και η δομή της βάσης δεδομένων που χρησιμοποιείται.

Στο κεφάλαιο 4, με τον τίτλο “Μελέτη Περίπτωσης Λειτουργίας της nimble”, πραγματοποιείται μια ανάλυση ενός υποθετικού σεναρίου χρήσης της πλατφόρμας. Αξιοποιώντας όλες τις δυνατότητες, τα εργαλεία και τις λειτουργίες της, παρουσιάζονται όλα τα οφέλη και ο τρόπος χρήσης της πλατφόρμας.

Τέλος, στο κεφάλαιο 5, με τον τίτλο “Συμπεράσματα και Μελλοντικές Επεκτάσεις”, περιγράφονται τα συμπεράσματα μετά την ανάπτυξη και τη χρήση της πλατφόρμας “nimble” στα πλαίσια της πτυχιακής διατριβής. Επίσης, αναφέρονται οι μελλοντικές επεκτάσεις που μπορούν να πραγματοποιηθούν για τη βελτίωση της πλατφόρμας και την εξέλιξή της.

1.4 Επίλογος

Τα δίκτυα υπολογιστών αποτελούν κρίσιμο συστατικό για τη λειτουργία και την ανάπτυξη των επιχειρήσεων στη σημερινή ψηφιακή εποχή. Με την αύξηση του αριθμού των συσκευών και των υπηρεσιών η διαχείριση των δικτύων απαιτεί μία νέα προσέγγιση, διότι οι παραδοσιακοί τρόποι δεν είναι πλέον επαρκώς αποτελεσματικοί. Η παραδοσιακή προσέγγιση οδηγεί σε αυξημένους χρόνους απασχόλησης, αυξημένο κόστος λειτουργίας και μειωμένη αποτελεσματικότητα της διαχείρισης δικτύων.

Επομένως, η ανάγκη για λύσεις που προσφέρουν αυτοματοποίηση και ευελιξία στη διαχείριση των δικτύων γίνεται ολοένα και πιο επιτακτική. Η πλατφόρμα “nimble” ανταποκρίνεται σε αυτήν την ανάγκη προσφέροντας λύσεις που επιτρέπουν την αυτοματοποίηση των διαδικασιών παραμετροποίησης δικτυακών συσκευών, καθώς και την εκτέλεση πολλαπλών ενεργειών ταυτόχρονα, βοηθώντας τις επιχειρήσεις να διαχειρίζονται αποτελεσματικά την ανάπτυξη και τη συντήρηση των δικτύων τους.

Μέσω της “nimble”, οι εταιρίες μπορούν να αξιοποιήσουν πλήρως το δυναμικό της τεχνολογίας για να αντιμετωπίσουν τις προκλήσεις της σύγχρονης διαχείρισης δικτύου και να επιτύχουν τους στόχους τους με αποτελεσματικότητα και ασφάλεια.

Κεφάλαιο 2ο: Αυτοματοποιημένη Παραμετροποίηση Δικτυακών Συσκευών

2.1 Εισαγωγή

Το κεφάλαιο αυτό επικεντρώνεται στην ανάλυση της αυτοματοποιημένης παραμετροποίησης δικτυακών συσκευών και τη σύγκριση της με τους παραδοσιακούς τρόπους παραμετροποίησης [10]. Αρχικά, εξετάζονται οι προκλήσεις και οι περιορισμοί των παραδοσιακών μεθόδων παραμετροποίησης, εστιάζοντας στα προβλήματα που προκύπτουν και στην ανάγκη για αυτοματοποιημένες λύσεις. Στη συνέχεια, παρουσιάζονται και συγκρίνονται άλλα εργαλεία αυτοματοποιημένης παραμετροποίησης, ενώ τέλος, δίνεται έμφαση στην προστιθέμενη αξία της πλατφόρμας “nimble” σε σχέση με αυτά τα εργαλεία.

2.2 Παραδοσιακός τρόπος παραμετροποίησης δικτυακών συσκευών

Ο παραδοσιακός τρόπος παραμετροποίησης των δικτυακών συσκευών συνήθως απαιτεί την σύνδεση του network administrator στις δικτυακές συσκευές και την προετοιμασία του περιβάλλοντος για την παραμετροποίησή της. Έπειτα ο network administrator εισάγει τις επιθυμητές και προσαρμοσμένες στην εκάστοτε συσκευή ρυθμίσεις, όπως κανόνες ασφαλείας, δρομολόγησης, VLANs, διαμόρφωση διεπαφών, κλπ. Μετά την παραμετροποίηση, ο διαχειριστής επικυρώνει τις ρυθμίσεις για τη σωστή λειτουργία της συσκευής και τη συμβατότητά της με το υπάρχον δίκτυο. Ακολουθούν δοκιμές για να επιβεβαιωθεί η ορθή λειτουργία των ρυθμίσεων. Οι ρυθμίσεις που έχουν εφαρμοστεί στη συσκευή αποθηκεύονται, συνήθως, στη μνήμη της συσκευής, προκειμένου να ανακτηθούν σε περίπτωση επανεκκίνησής της. Αυτή η διαδικασία βασίζεται στη χειροκίνητη επέμβαση του ανθρώπου σε κάθε στάδιο.

2.2.1 Παραδοσιακός τρόπος παραμετροποίησης firewall

Στην προσέγγιση αυτή για την παραμετροποίηση του firewall, ο διαχειριστής λαμβάνει υπόψη τις απαιτήσεις και τον σχεδιασμό που έχουν προηγουμένως ολοκληρωθεί για το δίκτυο. Η προτεραιότητα του είναι η διασφάλιση της ορθής λειτουργίας του δικτύου, με έμφαση στην ασφάλεια. Όταν πρέπει να προσθέσει ή να τροποποιήσει μία πολιτική ασφαλείας, ο διαχειριστής πρέπει να ερευνήσει και να βρει τον καταλληλότερο τρόπο να επιτύχει τον στόχο του χωρίς να θέσει σε κίνδυνο την ασφάλεια του δικτύου.

Καθώς μια επιχείρηση μεγαλώνει, οι απαιτήσεις και οι ανάγκες για το firewall αυξάνονται. Αυτό οδηγεί σε πολύπλοκες και δυσκίνητες πολιτικές ασφαλείας, με αρνητικές επιπτώσεις στην διαχείρισή τους. Για τον λόγο αυτό, ο σωστός αρχικός σχεδιασμός των πολιτικών ασφαλείας και η χρήση αντικειμένων (*objects*) και ομάδων αντικειμένων (*object groups*) είναι ουσιώδους σημασίας. Οργανωμένες και καλά δομημένες πολιτικές ασφαλείας με χρήση object μπορούν να διευκολύνουν τη διαχείριση και τη συντήρηση του firewall.

Παρόλα αυτά, η δημιουργία και η συντήρηση των object και των object-group με τον παραδοσιακό χειροκίνητο τρόπο μπορεί να είναι χρονοβόρα και επιρρεπής σε ανθρώπινα λάθη. Καθώς η επιχείρηση αναπτύσσεται, οι ανάγκες αλλάζουν, και η διαδικασία αυτή γίνεται ακόμα πιο περίπλοκη. Επομένως, η αυτοματοποίηση της διαδικασίας αυτής μέσω εργαλείων που παρέχουν έξυπνη διαχείριση των object μπορεί να αποδειχθεί ως ένα αναγκαίο επόμενο βήμα για τη βελτίωση της αποδοτικότητας και τη μείωση των πιθανών σφαλμάτων.

2.2.2 Παραδοσιακός τρόπος παραμετροποίησης routers και switches

Στην προσέγγιση αυτή για την παραμετροποίηση των δικτυακών συσκευών τύπου router ή/και switch, ο διαχειριστής έχοντας αναλύσει προσεκτικά τις απαιτήσεις και έχοντας ολοκληρώσει τον απαραίτητο σχεδιασμό, καταλήγει σε μία σειρά από εντολές που θα πρέπει να εφαρμοστούν στις δικτυακές συσκευές.

Κάθε συσκευή απαιτεί ξεχωριστή προσέγγιση και προσαρμογή των εντολών σύμφωνα με τις δικές της ανάγκες και ρυθμίσεις. Έτσι, ο διαχειριστής πρέπει να συνδεθεί σε κάθε μία συσκευή ξεχωριστά και να εφαρμόσει τις προσαρμοσμένες εντολές για τη συγκεκριμένη συσκευή.

Η διαδικασία αυτή απαιτεί χρόνο και προσοχή, καθώς ο διαχειριστής θα πρέπει να είναι προσεκτικός στην εφαρμογή κάθε εντολής για να αποφύγει τυχόν σφάλματα ή προβλήματα στη λειτουργία της συσκευής, και κατ' επέκταση του δικτύου. Επιπλέον, η επαναλαμβανόμενη φύση της διαδικασίας την καθιστά επιρρεπή σε ανθρώπινα λάθη, καθώς είναι και χρονοβόρα. Η χρήση λοιπόν εργαλείων αυτοματοποίησης μπορεί να βοηθήσει στη μείωση του χρόνου και των πιθανών λαθών που συνδέονται με τη διαδικασία αυτή.

2.2.3 Προβλήματα παραδοσιακής προσέγγισης

Η παραδοσιακή χειροκίνητη παραμετροποίηση των δικτυακών συσκευών αποτελεί μία διαδικασία που συνοδεύεται από πολλά προβλήματα και περιορισμούς. Ας εξετάσουμε εκτενώς αυτά τα προβλήματα:

1. Χρονοβόρα διαδικασία: Η χειροκίνητη παραμετροποίηση απαιτεί σημαντικό χρόνο και επίβλεψη από τον network administrator. Κάθε συσκευή πρέπει να παραμετροποιηθεί μεμονωμένα, μία διαδικασία που είναι χρονοβόρα.
2. Επιρρεπής σε ανθρώπινα σφάλματα: Η επαναλαμβανόμενη φύση της διαδικασίας την καθιστά επιρρεπή σε ανθρώπινα σφάλματα. Οι διαχειριστές που εκτελούν αυτές τις εργασίες μπορεί να κάνουν λάθη λόγω κόπωσης ή έλλειψης προσοχής.
3. Απασχόληση προσωπικού: Η παραδοσιακή παραμετροποίηση απαιτεί την πολύωρη απασχόληση υψηλά καταρτισμένου προσωπικού που γνωρίζει τις λεπτομέρειες και τις διαδικασίες για κάθε συσκευή και της τοπολογίας του δικτύου.
4. Ασυνέπειες: Η χειροκίνητη διαδικασία μπορεί να οδηγήσει σε ασυνέπειες και διαφορές στην εφαρμογή των ρυθμίσεων.
5. Δυσκολία βελτιστοποίησης: Η διαδικασία αυτή δυσχεραίνει τη βελτιστοποίηση των παραμέτρων και των ρυθμίσεων των συσκευών, καθώς οι αλλαγές πρέπει να εφαρμόζονται μεμονωμένα σε κάθε μία συσκευή.
6. Δυσκολία κλιμάκωσης: Καθώς το δίκτυο αναπτύσσεται και αλλάζει, η διαχείριση του με τον παραδοσιακό τρόπο γίνεται ακόμα πιο δύσκολη και χρονοβόρα.
7. Ασαφείς χρόνοι παράδοσης: Οι χρόνοι παράδοσης των ρυθμίσεων είναι ασαφείς, μη προβλέψιμοι και μεγάλοι λόγω της χειροκίνητης διαδικασίας και της πιθανής ανάγκης για επαναληπτικές ενέργειες.

Συνολικά, η παραδοσιακή χειροκίνητη παραμετροποίηση των δικτυακών συσκευών αντιμετωπίζει πολλά προβλήματα που μπορούν να επιλυθούν με τη χρήση αυτοματοποιημένων διαδικασιών και εργαλείων διαχείρισης δικτύου.

2.3 Εργαλεία αυτοματοποιημένης παραμετροποίησης

2.3.1 Cisco Catalyst Center

Το Cisco Catalyst Center [11] (πρώην *DNA Center*) είναι μια ολοκληρωμένη πλατφόρμα διαχείρισης δικτύου που παρέχεται από την Cisco. Σχεδιασμένο για να παρέχει ένα ολοκληρωμένο σετ λειτουργιών για τη διαχείριση, την αυτοματοποίηση και την επίλυση προβλημάτων σε δίκτυα επιχειρήσεων, το Cisco Catalyst Center αποτελεί ένα κεντρικό σημείο για τη διαχείριση του δικτύου.

Μερικά από τα κύρια χαρακτηριστικά και λειτουργίες του Cisco Catalyst Center περιλαμβάνουν:

- **Διαχείριση Συσκευών:** Το Cisco Catalyst Center παρέχει ένα κεντρικό σημείο για τη διαχείριση και τον έλεγχο των δικτυακών συσκευών, όπως routers, switches και wireless access points.
- **Εφαρμογή Πολιτικών και Ασφαλείας:** Η πλατφόρμα επιτρέπει την εφαρμογή και τη διαχείριση πολιτικών ασφαλείας σε επίπεδο δικτύου, ενώ παρέχει επίσης λειτουργίες εντοπισμού και απόκρισης σε απειλές (*threat detection and response*).
- **Αυτοματοποίηση Δικτύου:** Μέσω του Cisco Catalyst Center, οι διαχειριστές μπορούν να εφαρμόσουν αυτοματοποιημένες διαδικασίες για τη διαμόρφωση, την ενημέρωση και τη συντήρηση του δικτύου.
- **Επίλυση Προβλημάτων:** Το Cisco Catalyst Center παρέχει εργαλεία για τον εντοπισμό και την επίλυση προβλημάτων στο δίκτυο, επιτρέποντας στους διαχειριστές να ανιχνεύουν και να διορθώνουν προβλήματα με ευκολία.

Συνολικά, το Cisco Catalyst Center προσφέρει μια ολοκληρωμένη και ευέλικτη πλατφόρμα για τη διαχείριση και την αυτοματοποίηση δικτύων επιχειρήσεων, επιτρέποντας την επίτευξη υψηλής απόδοσης και ασφαλείας σε όλο το δίκτυο.

2.3.2 Terraform

Το Terraform [12] είναι ένα εργαλείο υποδομής ως κώδικα (*IaC*) που αναπτύσσεται από την HashiCorp. Χρησιμοποιείται για την αυτοματοποίηση της διαχείρισης υποδομής και των υπηρεσιών σε διάφορα περιβάλλοντα όπως δημόσια νέφη (*public clouds*), ιδιωτικά νέφη (*private clouds*) και υποδομές επιχειρήσεων.

Ο βασικός στόχος του Terraform είναι να επιτρέπει τη διαχείριση των υποδομών ως κώδικα, δηλαδή τη δήλωση της επιθυμητής κατάστασης του συστήματος σε έναν απλό, δεκτικό σε μηχανικούς μορφή, χρησιμοποιώντας μια γλώσσα υποδομής.

Οι βασικές έννοιες και λειτουργίες του Terraform περιλαμβάνουν:

- **Διακήρυξη (*Declaration*):** Οι χρήστες δηλώνουν την επιθυμητή κατάσταση της υποδομής σε ένα αρχείο διαμόρφωσης, γνωστό ως "Terraform configuration".
- **Παρακολούθηση (*Planning*):** Το Terraform αναλύει τον κώδικα υποδομής και δημιουργεί ένα σχέδιο για τις αλλαγές που θα εφαρμοστούν στο περιβάλλον.
- **Εφαρμογή (*Application*):** Οι αλλαγές που περιέχονται στο σχέδιο εφαρμόζονται στο περιβάλλον υποδομής με την εντολή terraform apply.

- Διαχείριση Κατάστασης (State Management): Το Terraform διατηρεί ένα αρχείο κατάστασης που περιγράφει την τρέχουσα κατάσταση της υποδομής και χρησιμοποιεί αυτό το αρχείο για να διαχειριστεί και να εφαρμόσει αλλαγές.

Με το Terraform, οι ομάδες ανάπτυξης και διαχείρισης μπορούν να αυτοματοποιήσουν τη διαδικασία δημιουργίας, διαμόρφωσης και διαχείρισης της υποδομής τους, επιτρέποντάς τους να επιτύχουν μεγαλύτερη ευελιξία, επαναληψιμότητα και αξιοπιστία στις λειτουργίες τους.

2.3.3 IP Fabric

Το IP Fabric [13] είναι μια πλατφόρμα διαχείρισης δικτύων που προσφέρει ολοκληρωμένες λύσεις για τον έλεγχο, την ανάλυση και τη διαχείριση δικτύων. Με χρήση προηγμένων αλγορίθμων και τεχνολογιών αυτοματοποίησης, το IP Fabric προσφέρει ένα πλήρες εύρος λειτουργιών για την παρακολούθηση, τον έλεγχο και τη βελτιστοποίηση των δικτύων.

Οι βασικές λειτουργίες του IP Fabric περιλαμβάνουν:

- Αυτόματη Εντοπισμός Δικτυακών Συσκευών: Το IP Fabric ανιχνεύει αυτόματα όλες τις συσκευές που υπάρχουν στο δίκτυο, συμπεριλαμβανομένων router, server, switches, και τερματικών συσκευών.
- Εξαγωγή Δεδομένων Δικτύου: Παρέχει λεπτομερείς πληροφορίες για τη δικτυακή υποδομή, συμπεριλαμβανομένων των τοπολογιών, των διασυνδέσεων και των ροών κυκλοφορίας.
- Αυτόματη Ανάλυση Ασφάλειας: Επιτρέπει τον εντοπισμό ευπαθειών ασφαλείας στο δίκτυο και παρέχει συστάσεις για την ενίσχυση των μέτρων ασφαλείας.
- Παρακολούθηση Κίνησης Δικτύου: Παρέχει λεπτομερείς αναφορές και γραφικές παραστάσεις της κίνησης δεδομένων στο δίκτυο, βοηθώντας στον εντοπισμό προβλημάτων και στη βελτιστοποίηση της απόδοσης.
- Διαχείριση Αλλαγών: Παρέχει εργαλεία για την παρακολούθηση και τον έλεγχο των αλλαγών στο δίκτυο, προστατεύοντας τη σταθερότητα και την ασφάλεια του.

Με το IP Fabric, οι network administrators έχουν ένα ισχυρό εργαλείο που τους επιτρέπει να διαχειρίζονται, να παρακολουθούν και να βελτιστοποιούν την υποδομή τους με αποτελεσματικό και ασφαλή τρόπο.

2.3.4 Intential

Το Intential [14] είναι μια σουίτα λογισμικού που σχεδιάστηκε για να παρέχει λύσεις αυτοματοποίησης δικτύων και προγραμματισμού δικτύου σε επιχειρηματικά περιβάλλοντα. Αποτελεί ένα ολοκληρωμένο πλαίσιο λογισμικού που επιτρέπει στις επιχειρήσεις να αυτοματοποιούν τις διαδικασίες δικτύου και να επιτυγχάνουν την ευελιξία και την επεκτασιμότητα που απαιτούνται για τη διαχείριση σύγχρονων δικτύων.

Το Intential παρέχει μια ευέλικτη και επεκτάσιμη πλατφόρμα που ενσωματώνει συστατικά λογισμικού όπως η αυτοματοποίηση των δικτύων, η οποία επιτρέπει στους χρήστες να δημιουργούν, να εκτελούν και να διαχειρίζονται αυτοματοποιημένες διαδικασίες χρησιμοποιώντας μια ευέλικτη γραφική διεπαφή χρήστη. Αυτό επιτρέπει στις επιχειρήσεις να αυξήσουν την αποτελεσματικότητα των δικτύων τους, να μειώσουν τα σφάλματα και να επιτύχουν την ταχύτερη αντίδραση σε αλλαγές και προκλήσεις δικτύου.

Οι βασικές λειτουργίες του Itential περιλαμβάνουν:

- Αυτοματοποίηση Δικτύων: Το Itential παρέχει προηγμένες δυνατότητες αυτοματοποίησης για τη διαχείριση και την εκτέλεση διάφορων δικτυακών λειτουργιών, όπως η διαμόρφωση συσκευών, ο έλεγχος της ποιότητας των υπηρεσιών και η διαχείριση συμβάντων.
- Γραφική Διεπαφή Χρήστη: Μια ευέλικτη γραφική διεπαφή χρήστη επιτρέπει στους χρήστες να δημιουργούν, να εκτελούν και να διαχειρίζονται τις αυτοματοποιημένες διαδικασίες με άνεση και αποτελεσματικότητα.
- Ολοκληρωμένη Διαχείριση Δικτύων: Το Itential επιτρέπει στις επιχειρήσεις να διαχειρίζονται τα δίκτυά τους από μια ενιαία πλατφόρμα, εξασφαλίζοντας ομαλή λειτουργία και αυξημένη ευελιξία.
- Υποστήριξη πολλαπλών πλατφορμών: Με υποστήριξη για πολλαπλές πλατφόρμες δικτύου και πρωτόκολλα, το Itential επιτρέπει την ολοκλήρωση και τον έλεγχο δικτύων ανεξαρτήτως του περιβάλλοντος.
- Διαχείριση Πολυπλοκότητας: Με την αυτοματοποίηση διαδικασιών και την ολοκληρωμένη διαχείριση των δικτύων, το Itential βοηθά στην αντιμετώπιση της πολυπλοκότητας που συνήθως σχετίζεται με τη διαχείριση των εταιρικών δικτύων.

Συνολικά, το Itential αποτελεί μια ολοκληρωμένη και επεκτάσιμη λύση για τη διαχείριση, την αυτοματοποίηση και την εξέλιξη εταιρικών δικτύων, επιτρέποντας στις επιχειρήσεις να επιτύχουν την απαιτούμενη ευελιξία, αποτελεσματικότητα και ασφάλεια στη διαχείριση των υποδομών τους.

2.3.5 Junos Space Network Management Platform

Το Junos Space [15] είναι μια πλατφόρμα διαχείρισης δικτύων που αναπτύχθηκε από την εταιρεία Juniper Networks. Αποτελεί ένα ολοκληρωμένο σύνολο λύσεων λογισμικού που παρέχει εργαλεία για την εύκολη και αποτελεσματική διαχείριση δικτύων Juniper.

Ο κύριος στόχος του Junos Space είναι να παρέχει ένα κεντρικό σημείο διαχείρισης για δίκτυα Juniper, επιτρέποντας στους διαχειριστές να διαχειρίζονται και να παρακολουθούν τις συσκευές και τα δίκτυα τους με άνεση και αποτελεσματικότητα.

Οι βασικές λειτουργίες του Junos Space περιλαμβάνουν:

- Διαχείριση συσκευών: Το Junos Space παρέχει εργαλεία για την παρακολούθηση, διαμόρφωση και διαχείριση των συσκευών Juniper που αποτελούν το δίκτυό σας.
- Εφαρμογή πολιτικών ασφαλείας: Παρέχει δυνατότητες για τη διαχείριση και την εφαρμογή πολιτικών ασφαλείας σε επίπεδο δικτύου.
- Παρακολούθηση απόδοσης: Το Junos Space παρέχει εργαλεία παρακολούθησης για την επίβλεψη και την αξιολόγηση της απόδοσης του δικτύου.
- Ανίχνευση προβλημάτων: Παρέχει δυνατότητες ανίχνευσης προβλημάτων στο δίκτυο και παρέχει ειδοποιήσεις σε περίπτωση που προκύψουν προβλήματα.
- Αυτοματοποίηση εργασιών: Το Junos Space παρέχει εργαλεία για την αυτοματοποίηση εργασιών και διαδικασιών στο δίκτυο, επιτρέποντας στους διαχειριστές να εκτελούν εργασίες μεγάλης κλίμακας με ευκολία και αξιοπιστία.

Το Junos Space είναι σχεδιασμένο για να παρέχει μια ολοκληρωμένη λύση για τη διαχείριση δικτύων Juniper και να βοηθά τους διαχειριστές να διαχειρίζονται τα δίκτυά τους με ασφάλεια, αποτελεσματικότητα και ευκολία.

2.4 Συνεισφορά της πλατφόρμας “nimble”

Η πλατφόρμα “nimble” προσφέρει αρκετά προτερήματα έναντι των εμπορικών εφαρμογών που χρησιμοποιούνται συνήθως στη διαχείριση δικτύων και αποτελεί μια εξαιρετική λύση έναντι της παραδοσιακής προσέγγισης στην παραμετροποίηση των δικτυακών συσκευών. Ας αναλύσουμε τα κύρια πλεονεκτήματά της:

1. Απλότητα Χρήσης: Η πλατφόρμα “nimble” προσομοιώνει τον χρήστη, επιτρέποντας τη χρήση της χωρίς την ανάγκη για εκμάθηση ειδικών γλωσσών. Αυτό σημαίνει ότι οι network administrators μπορούν να επωφεληθούν αμέσως από τις λειτουργίες της χωρίς πολύπλοκες διαδικασίες εκπαίδευσης.
2. Αυτονομία και Εγκατάσταση: Η “nimble” είναι διαθέσιμη για εγκατάσταση σε τοπικό εξοπλισμό της επιχείρησης, εξασφαλίζοντας την αυτονομία και τον έλεγχο των δεδομένων της επιχείρησης χωρίς την ανάγκη πρόσβασης τρίτων στην υποδομή της επιχείρησης.
3. Ευελιξία στην Επιλογή Εξοπλισμού: Η “nimble” δεν περιορίζεται σε εξοπλισμό ενός συγκεκριμένου κατασκευαστή, προσφέροντας στους διαχειριστές τη δυνατότητα να επιλέξουν τον εξοπλισμό που ταιριάζει καλύτερα στις ανάγκες τους και το περιβάλλον τους.
4. Απουσία Αδειών Χρήσης: Δεν απαιτούνται αδειοδοτήσεις χρήσης για τη χρήση της πλατφόρμας “nimble”, προσφέροντας μια οικονομικά βιώσιμη λύση χωρίς την ανάγκη για πρόσθετες δαπάνες.
5. Ελεκτασιμότητα: Η “nimble” είναι μια πλατφόρμα και όχι ένα εργαλείο, προσφέροντας έτσι τη δυνατότητα προσθήκης νέων εργαλείων, δυνατοτήτων και λειτουργιών. Αυτό επιτρέπει στις επιχειρήσεις να προσαρμόσουν τη λύση σύμφωνα με τις ανάγκες και την ανάπτυξή τους χωρίς περιορισμούς.
6. Αυτοματοποίηση των εντολών και μαζική παραμετροποίηση: Η πλατφόρμα “nimble” επιτρέπει την αυτόματη προσαρμογή των εντολών για κάθε συσκευή και τη μαζική παραμετροποίηση συσκευών, εξοικονομώντας έτσι πολύτιμο χρόνο για τους network administrators.
7. Αποφυγή ανθρώπινων λαθών: Η αυτοματοποίηση μειώνει δραματικά την πιθανότητα ανθρώπινων λαθών, καθώς δεν απαιτούνται επαναλαμβανόμενες ανθρώπινες ενέργειες. Αυτό οδηγεί σε μια πιο ομοιόμορφη παραμετροποίηση, χωρίς ασυνέπειες και με βελτιστοποιημένα αποτελέσματα.
8. Βελτίωση των χρόνων παράδοσης: Οι χρόνοι παράδοσης είναι πλέον σαφείς, προβλέψιμοι και σύντομοι λόγω της αυτοματοποιημένης διαδικασίας, εξασφαλίζοντας την άμεση εφαρμογή των αλλαγών.

Συνολικά, η πλατφόρμα “nimble” αναδεικνύεται ως μια ευέλικτη, εύχρηστη και οικονομικά αποδοτική λύση για τη διαχείριση δικτύων, και επιτρέπει στους διαχειριστές να εστιάσουν τον χρόνο και τους πόρους τους σε εργασίες που πραγματικά απαιτούν την προσοχή τους, ενώ ταυτόχρονα εξαλείφει τα προβλήματα που σχετίζονται με την παραδοσιακή χειροκίνητη προσέγγιση, όπως ο ανθρώπινος παράγοντας και οι χρονοβόρες επαναλαμβανόμενες διαδικασίες.

2.5 Επίλογος

Σε αυτό το κεφάλαιο, εξετάσαμε λεπτομερώς την αυτοματοποιημένη παραμετροποίηση δικτυακών συσκευών. Ξεκινήσαμε με μια εισαγωγή στο θέμα, ακολουθώντας την ανάλυση του παραδοσιακού τρόπου παραμετροποίησης δικτυακών συσκευών, με έμφαση στο firewall, τους router και τα switches. Κατόπιν, εξετάσαμε τα προβλήματα που συνήθως συναντώνται με την παραδοσιακή προσέγγιση.

Έπειτα, αναλύσαμε την προσφορά της πλατφόρμας “nimble” σε σχέση με την παραδοσιακή προσέγγιση. Στη συνέχεια, αναφέραμε άλλα εμπορικά εργαλεία, όπως το Cisco Catalyst Center, το Terraform, το IP Fabric, το Intential και το Junos Space Network Management Platform, και τέλος εξετάσαμε τα πλεονεκτήματά της πλατφόρμας “nimble” σε σύγκριση με τα εμπορικά εργαλεία όσον αφορά την αυτοματοποιημένη παραμετροποίηση δικτυακών συσκευών.

Με βάση αυτές τις αναλύσεις, γίνεται προφανές ότι η πλατφόρμα “nimble” αντιπροσωπεύει μια σύγχρονη και ευέλικτη λύση για τη διαχείριση δικτύων, προσφέροντας ταυτόχρονα απλότητα χρήσης, ευελιξία, αυτονομία και επεκτασιμότητα. Αυτή η πλατφόρμα επιτρέπει στους network administrators να κάνουν ένα βήμα προς την κατεύθυνση της αποτελεσματικής και ασφαλούς διαχείρισης των δικτύων, ενισχύοντας την αυτοματοποίηση και την ασφάλεια.

Κεφάλαιο 3ο: Η Πλατφόρμα “nimble”

3.1 Εισαγωγή

Η “nimble” αποτελεί μία πλατφόρμα ειδικά σχεδιασμένη για τη διευκόλυνση των network administrator (*network administrators*) στο έργο της διαχείρισης μεγάλης κλίμακας εταιρικών δικτύων. Η κύρια αποστολή της είναι να παρέχει αυτοματοποιημένες διαδικασίες για τη δημιουργία και εφαρμογή μαζικών ρυθμίσεων σε δικτυακές συσκευές, καθώς και τη μείωση του απαιτούμενου χρόνου για την εκτέλεση αυτών των εργασιών. Λόγω του ότι αποτελεί πλατφόρμα και όχι εργαλείο, διαθέτει την ευελιξία να επιτρέπει την επέκταση της προς οποιαδήποτε κατεύθυνση.

3.2 Λειτουργία της Πλατφόρμας

Οι network administrators μπορούν να χρησιμοποιούν την “nimble”:

1. για τη έμμεση τροποποίηση πολλαπλών κανόνων σε Cisco NGFW, και
2. την παραμετροποίηση ομοειδών δικτυακών συσκευών με τρόπο μαζικό και ταυτόχρονο.

Μέσω μιας φόρμας εισαγωγής δεδομένων, οι διαχειριστές μπορούν να καθορίζουν τις απαιτούμενες ρυθμίσεις και παραμέτρους, ενώ η “nimble” αξιοποιεί τα διαθέσιμα εργαλεία για την αυτόματη δημιουργία της αντίστοιχης παραμετροποίησης (*configuration*), και έπειτα την μαζική και ταυτόχρονη εφαρμογή του στις αντίστοιχες συσκευές.

3.2.1 Εργαλεία “Objects” και “Groups” για το Cisco FMC

Ο network administrator χρησιμοποιεί την πλατφόρμα “nimble” για τη διαχείριση του Cisco Firepower Management Center (*FMC*). Μέσω φορμών, συμπληρώνει πληροφορίες για τη δημιουργία, τροποποίηση ή διαγραφή objects και object groups στο FMC, τα οποία είτε χρησιμοποιούνται ήδη, είτε πρόκειται να χρησιμοποιηθούν από κανόνες, επηρεάζοντας έτσι την συμπεριφορά του/των NGFW. Οι φόρμες παρέχουν επίσης τη δυνατότητα χρήσης μεταβλητών (*variables*), καθώς και ευρών (*ranges*), επιτρέποντας στον διαχειριστή να προσαρμόσει με ευκολία τα αποτελέσματα σύμφωνα με τις απαιτήσεις του δικτύου και του εκάστοτε έργου.

3.2.2 Εργαλείο “Bulk Configurator” για τη Μαζική Παραμετροποίηση Δικτυακών Συσκευών

Ο διαχειριστής χρησιμοποιεί επίσης την πλατφόρμα “nimble” για τη μαζική παραμετροποίηση δικτυακών συσκευών, όπως routers και switches, από διαφορετικούς κατασκευαστές όπως είναι οι Cisco, Aruba και MikroTik. Μέσω αντίστοιχων φορμών, ο διαχειριστής συμπληρώνει πληροφορίες και χρησιμοποιεί variables και ranges για να παράγει αυτόματα τις εντολές παραμετροποίησης. Στη συνέχεια, οι εντολές εφαρμόζονται μαζικά και ταυτόχρονα στις συσκευές προορισμού.

Με αυτόν τον τρόπο, ο network administrator επιτυγχάνει την αποτελεσματική και αυτοματοποιημένη διαχείριση του Cisco FMC και των δικτυακών συσκευών στο πλαίσιο της πλατφόρμας “nimble”, εξοικονομώντας χρόνο και ελαχιστοποιώντας την πιθανότητα σφαλμάτων.

3.3 Οφέλη για τους Network Administrators

Η χρήση της πλατφόρμας “nimble” προσφέρει σημαντικά οφέλη στους network administrator. Ανάμεσα στα κύρια οφέλη περιλαμβάνονται:

- **Εξοικονόμηση Χρόνου:** Η δυνατότητα δημιουργίας και εφαρμογής μαζικών ρυθμίσεων με ελάχιστη ανθρώπινη επέμβαση οδηγεί σε σημαντική μείωση του χρόνου που απαιτείται για τη διαχείριση των δικτύων.
- **Ελαχιστοποίηση Σφαλμάτων:** Η αυτοματοποιημένη διαδικασία εφαρμογής ρυθμίσεων μειώνει την πιθανότητα ανθρώπινων σφαλμάτων και τις συνέπειες που μπορεί να έχουν στην ασφάλεια και τη λειτουργία του δικτύου.
- **Βελτίωση Χρόνων Παράδοσης:** Η αυξημένη αποτελεσματικότητα και η μείωση του χρόνου ανάπτυξης, προσαρμογής και εφαρμογής ρυθμίσεων οδηγούν σε βελτίωση των χρόνων παράδοσης των έργων.
- **Προβλεψιμότητα Χρόνων Παράδοσης:** Η αυτοματοποιημένη διαδικασία εφαρμογής ρυθμίσεων εξασφαλίζει την προβλεψιμότητα των χρόνων παράδοσης των έργων, καθώς η διαδικασία γίνεται συνεπής και αξιόπιστη.

Με τη συνδυασμένη δράση αυτών των οφελών, η πλατφόρμα “nimble” επιτρέπει στους network administrator να επιτυγχάνουν υψηλό επίπεδο αποτελεσματικότητας και ασφάλειας στη διαχείριση των εταιρικών δικτύων.

3.4 Εργαλεία

Συνοψίζοντας τα εργαλεία και τις τεχνολογίες που χρησιμοποιήθηκαν για την ανάπτυξη της πλατφόρμας “nimble”, παρουσιάζουμε τα παρακάτω:

3.4.1 Django για το Front και το Back-end

Το Django [16] είναι ένα δημοφιλές open-source web framework γραμμένο σε Python. Προσφέρει ένα ολοκληρωμένο σετ εργαλείων για την ανάπτυξη WEB εφαρμογών, συμπεριλαμβανομένων λειτουργιών όπως η διαχείριση χρηστών, ο χειρισμός των URL, η ανάπτυξη προτύπων (*templates*) για τη δημιουργία δυναμικού περιεχομένου και η αλληλεπίδραση με βάσεις δεδομένων.

Το Django χρησιμοποιήθηκε για την ανάπτυξη του front-end και back-end της πλατφόρμας “nimble”. Η χρήση ενός ενιαίου framework για και τα δύο μέρη της εφαρμογής διευκόλυνε την ανάπτυξη και τη συντήρηση του κώδικα.

3.4.2 Python για την Υλοποίηση όλων των Λειτουργιών

Η Python [17] είναι μια δυναμική, υψηλού επιπέδου γλώσσα προγραμματισμού με συντακτική σύνταξη που επιτρέπει την εύκολη ανάπτυξη και αναγνώριση κώδικα. Χρησιμοποιείται ευρέως στην ανάπτυξη λογισμικού, από εφαρμογές desktop έως και εφαρμογές WEB και επεξεργασίας δεδομένων.

Η Python χρησιμοποιήθηκε για την υλοποίηση όλων των λειτουργιών της πλατφόρμας “nimble”, συμπεριλαμβανομένων των διαδικασιών αυτοματοποίησης και διαχείρισης των δικτυακών συσκευών.

3.4.3 Python API της Cisco για το FMC

Το Python API της Cisco για το FMC [18] παρέχει ένα σύνολο από βιβλιοθήκες και εργαλεία που επιτρέπουν την αυτοματοποίηση και τη διαχείριση των λειτουργιών του FMC μέσω της Python.

Χρησιμοποιήθηκε για την αυτοματοποίηση των λειτουργιών διαχείρισης των Cisco NGFW μέσω της πλατφόρμας “nimble”, επιτρέποντας τη δημιουργία και την εφαρμογή ρυθμίσεων μαζικά και αυτοματοποιημένα.

3.4.4 Paramiko

Το Paramiko [19] είναι μια Python βιβλιοθήκη που παρέχει πρόσβαση σε δικτυακές συσκευές προσομοιώνοντας τον χρήστη, διασφαλίζοντας την ασφαλή απομακρυσμένη επικοινωνία με απομακρυσμένους υπολογιστές.

Χρησιμοποιήθηκε για την αυθεντικοποίηση και την αλληλεπίδραση με τις δικτυακές συσκευές μέσω SSH [20], επιτρέποντας στην πλατφόρμα “nimble” να επικοινωνεί και να εκτελεί εντολές στις συσκευές.

3.4.5 Βιβλιοθήκη Python concurrent

Η βιβλιοθήκη concurrent [21] της Python παρέχει ένα περιβάλλον για την ασύγχρονη και παράλληλη εκτέλεση κώδικα.

Χρησιμοποιήθηκε για την αξιοποίηση της παράλληλης εκτέλεσης κώδικα, βελτιώνοντας την απόδοση των λειτουργιών που απαιτούν επικοινωνία με τις δικτυακές συσκευές και εφαρμογή του configuration.

3.4.6 Βιβλιοθήκη Bootstrap

Η βιβλιοθήκη Bootstrap [22] προσφέρει ένα σύνολο προ-διαμορφωμένων στοιχείων και εργαλείων για τη δημιουργία διεπαφών χρήστη (UI) με ελκυστικό σχεδιασμό και δίνοντας έμφαση στην ανταπόκριση. Τα κύρια χαρακτηριστικά της περιλαμβάνουν πλέγματα (*grids*), προ-διαμορφωμένα στοιχεία, στυλ συνιστωσών και αυτόματη ανταπόκριση για διαφόρων μεγεθών οθόνες.

Χρησιμοποιήθηκε για τη δημιουργία του front-end της εφαρμογής. Τα προ-διαμορφωμένα στοιχεία και τα στυλ της Bootstrap αξιοποιήθηκαν για να δημιουργηθεί ένα αποτελεσματικό και λειτουργικό περιβάλλον χρήστη. Τα πλέγματα της Bootstrap χρησιμοποιήθηκαν για τη διάταξη των στοιχείων στη σελίδα, τα προ-διαμορφωμένα στοιχεία για τη δημιουργία κουμπιών, φορμών και άλλων στοιχείων εισόδου, και τα στυλ συνιστωσών για να προσθέσουμε ενσωματωμένα στυλ στην εφαρμογή μας.

Επίσης, χρησιμοποιήθηκε η Bootstrap για να διασφαλιστεί ότι η εφαρμογή εμφανίζεται σωστά σε διάφορες συσκευές και μεγέθη οθονών. Αυτό επιτρέπει μια συνεπή εμπειρία ανεξάρτητα από τη συσκευή που χρησιμοποιεί ο χρήστης.

3.4.7 Javascript

Η JavaScript [23] είναι μια δημοφιλής γλώσσα προγραμματισμού που χρησιμοποιείται ευρέως για την ανάπτυξη διαδραστικών και δυναμικών δικτυακών εφαρμογών.

Χρησιμοποιήθηκε για την προσθήκη λειτουργικότητας και διαδραστικότητας στο front-end της εφαρμογής και των στοιχείων που δημιουργήθηκαν με τη βοήθεια της βιβλιοθήκης Bootstrap. Μέσω της JS, έγινε διαχείριση των γεγονότων, όπως κλικ κουμπιών και αποστολή φόρμας, δυναμική ενημέρωση του περιεχόμενου της σελίδας χωρίς ανανέωση της ίδιας, και επικοινωνία με τον server για την ανάκτηση ή αποστολή δεδομένων. Μέσω αυτής της προσέγγισης, δημιουργήθηκε μια διαδραστική και αποτελεσματική εμπειρία χρήστη, βελτιώνοντας έτσι την αποδοτικότητα της εφαρμογής.

3.4.8 JSON και CSV

Τα αρχεία CSV [24] (*Comma-Separated Values*) και JSON [25] (*JavaScript Object Notation*) είναι δύο δημοφιλείς μορφές αρχείων που χρησιμοποιούνται για την αποθήκευση και τη μεταφορά δεδομένων.

Το CSV είναι ένα απλό κείμενο που περιέχει δεδομένα σε μορφή πίνακα, όπου κάθε γραμμή αντιπροσωπεύει μια εγγραφή και ως διαχωριστικά των πεδίων των εγγραφών χρησιμοποιούνται κόμματα. Η μορφή CSV είναι απλή και εύκολη στην ανάγνωση από ανθρώπους και συχνά χρησιμοποιείται για την αποθήκευση δεδομένων από πίνακες ή βάσεις δεδομένων, καθώς και για τη μεταφορά δεδομένων μεταξύ διαφορετικών εφαρμογών.

Το JSON είναι ένα εύηλεκτο και διαδομένο μορφότυπο ανταλλαγής δεδομένων, βασισμένο στη σύνταξη αντικειμένων JS. Τα δεδομένα σε μορφή JSON αναπαρίστανται σε μορφή ζευγών “κλειδί-τιμή” και μπορούν να περιέχουν συμβατικούς τύπους δεδομένων όπως αριθμούς, συμβολοσειρές (*strings*), λογικές τιμές, λίστες και αντικείμενα. Το JSON είναι πιο πολύπλοκο από το CSV, αλλά προσφέρει μεγαλύτερη ευελιξία και δυνατότητα αναπαράστασης δομικών δεδομένων.

Και τα δύο αυτά αρχεία μορφοποιούνται με τέτοιον τρόπο που να επιτρέπει την εύκολη ανάγνωση και επεξεργασία των δεδομένων από τόσο ανθρώπους όσο και από υπολογιστικά συστήματα.

Το αρχείο CSV χρησιμοποιήθηκε στην εφαρμογή για την εισαγωγή δεδομένων από τον χρήστη. Αν και τα αρχεία CSV είναι αρχικά μηδενικής πολυπλοκότητας, η μορφή τους παρέχει μια οργανωμένη δομή για την εισαγωγή δεδομένων σε πίνακες ή βάσεις δεδομένων. Ο χρήστης μπορεί να δημιουργήσει ένα αρχείο CSV με τα δεδομένα που επιθυμεί να εισαγάγει στην εφαρμογή, ταξινομώντας τα σε στήλες και χρησιμοποιώντας κόμματα για να διαχωρίσει τις τιμές. Στη συνέχεια, η εφαρμογή αναλύει αυτό το αρχείο CSV και εισάγει τα δεδομένα στην κατάλληλη βάση δεδομένων ή τις δομές δεδομένων της εφαρμογής.

Αντίθετα, το αρχείο JSON χρησιμοποιήθηκε για την απεικόνιση της εξόδου (*output*) της εφαρμογής προς τον χρήστη, καθώς και για την εφαρμογή των αποτελεσμάτων στις συσκευές. Το JSON είναι ιδανικό για τη μεταφορά δομικών δεδομένων και παρέχει μια εύηλεκτη δομή που επιτρέπει την αναπαράσταση πολύπλοκων δεδομένων. Τα δεδομένα που παράγονται από την εφαρμογή, όπως αποτελέσματα επεξεργασίας ή διαμορφωμένα αποσπάσματα παραμετροποίησης (*configuration snippets*), αποτυπώνονται σε μορφή JSON για να μεταβιβαστούν από το back-end στο front-end της εφαρμογής. Επίσης, το JSON χρησιμοποιείται για την επικοινωνία μεταξύ της εφαρμογής και των συσκευών, καθώς τα δεδομένα που απαιτούνται για τη διαμόρφωση των συσκευών συνήθως μεταφέρονται σε μορφή JSON.

3.4.9 EVE-NG και VMware

Κατά την ανάπτυξη και δοκιμή της πλατφόρμας “nimble”, χρησιμοποιήθηκαν συμπληρωματικά δύο εργαλεία: το EVE-NG [26] για την προσομοίωση των δικτυακών συσκευών, και το VMware [27] για την εγκατάσταση του FMC.

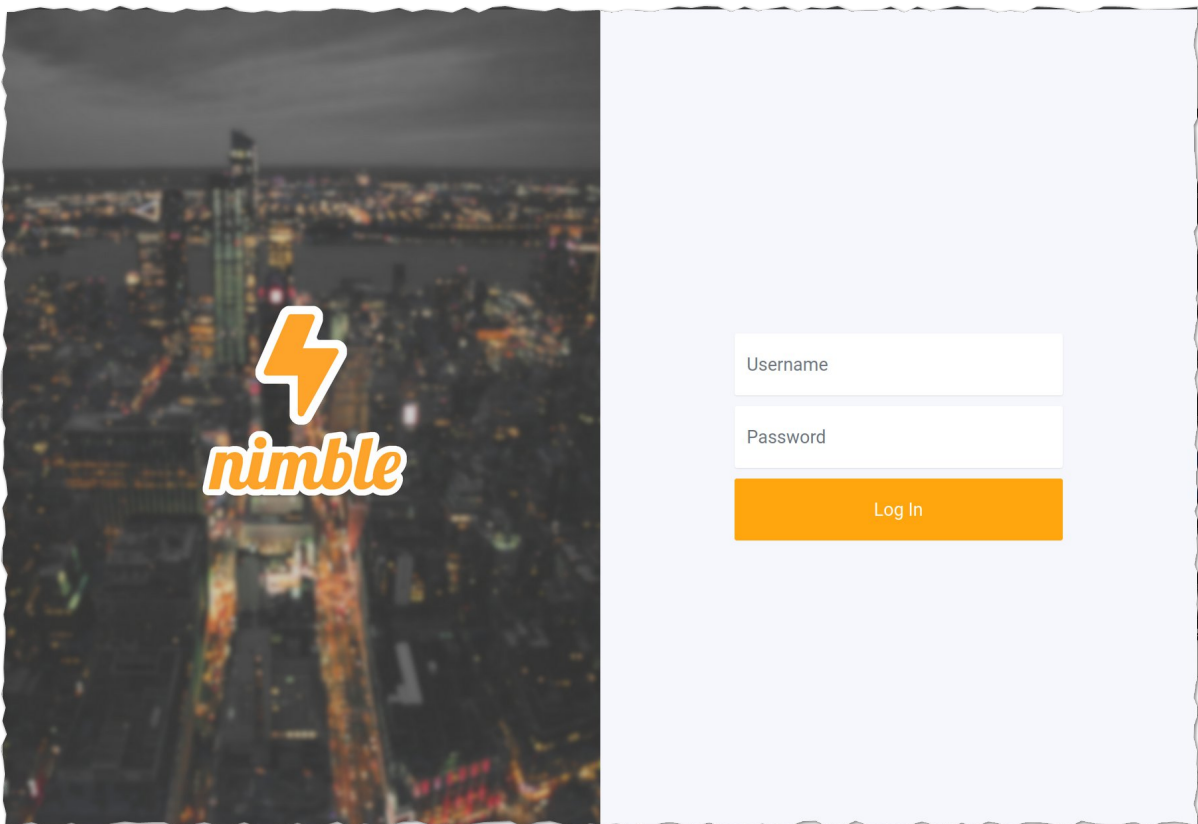
Το EVE-NG είναι μια πλατφόρμα εικονικοποίησης (*virtualization*) δικτύου [28] που επιτρέπει στους χρήστες να δημιουργήσουν περιβάλλοντα δικτύου με εικονικές συσκευές, όπως routers, switches και servers, για δοκιμές και εκπαίδευση. Χρησιμοποιώντας το EVE-NG, κατέστη δυνατή η προσομοίωση δικτυακών σεναρίων και να γίνει έλεγχος της συμπεριφοράς της πλατφόρμας σε διάφορες συνθήκες δικτύου.

Το VMware χρησιμοποιήθηκε για την εγκατάσταση του FMC. Το FMC είναι μια πλατφόρμα διαχείρισης ασφάλειας της Cisco που παρέχει λειτουργίες διαχείρισης και εποπτείας για δικτυακές συσκευές Cisco Firepower. Χρησιμοποιώντας το VMware, έγινε η εγκατάσταση και οι δοκιμές των εργαλείων που αφορούν το FMC, σε ένα ελεγχόμενο εικονικό περιβάλλον. Αυτό επέτρεψε την ανάπτυξη, το έλεγχο και την προσαρμογή της ενσωματωμένης λογικής διαχείρισης της ασφάλειας του δικτύου της πλατφόρμας.

3.5 Αρχιτεκτονική και λειτουργικότητα

3.5.1 Είσοδος στην πλατφόρμα

Ο χρήστης ανοίγει τον φυλλομετρητή (*browser*) του και εισάγει το URL της πλατφόρμας “nimble” στη γραμμή διεύθυνσης. Αφού εισαγάγει το κατάλληλο URL, ο χρήστης ανακατευθύνεται αυτόματα στη σελίδα σύνδεσης της πλατφόρμας, όπου του ζητείται να εισάγει τα στοιχεία σύνδεσής του.



Σχήμα 3.1 Είσοδος στην πλατφόρμα

Στη σελίδα σύνδεσης, ο χρήστης πρέπει να εισάγει τα κατάλληλα διαπιστευτήρια (*credentials*), το όνομα χρήστη (*username*) και τον κωδικό πρόσβασής του (*password*) στα αντίστοιχα πεδία. Μετά την εισαγωγή των στοιχείων σύνδεσης, ο χρήστης πατάει το κουμπί “Log In” για να υποβάλει τα στοιχεία του. Η εφαρμογή ελέγχει τα στοιχεία σύνδεσης που εισήχθησαν από τον χρήστη, ελέγχοντας την εγκυρότητα τους και την αντιστοιχία με τα αποθηκευμένα στοιχεία στη βάση δεδομένων. Αν τα στοιχεία σύνδεσης είναι έγκυρα, η εφαρμογή παρέχει στον χρήστη πρόσβαση στην πλατφόρμα, ανακατευθύνοντάς τον στην κύρια σελίδα της εφαρμογής. Αν τα στοιχεία είναι εσφαλμένα, εμφανίζεται ένα μήνυμα σφάλματος ζητώντας από τον χρήστη να επαναλάβει τη διαδικασία σύνδεσης με τα σωστά στοιχεία.

3.5.2 Βασικό Μενού

Το βασικό μενού αποτελεί τον πυρήνα της διαδικασίας παραμετροποίησης των δικτυακών συσκευών και περιλαμβάνει τις ακόλουθες επιλογές:

- i. **Select Vendor** (Επιλογή Κατασκευαστή):
Ο χρήστης επιλέγει τον κατασκευαστή της ή των συσκευών που επιθυμεί να παραμετροποιήσει. Αυτή η επιλογή καθορίζει το εύρος των επιλογών που θα εμφανιστούν στα επόμενα βήματα.
- ii. **Select Type** (Επιλογή Τύπου):
Μετά την επιλογή του κατασκευαστή, ο χρήστης επιλέγει τον τύπο της ή των συσκευών που θα παραμετροποιήσει. Αυτή η επιλογή διευκρινίζει περαιτέρω τα χαρακτηριστικά των συσκευών που θα επεξεργαστεί.
- iii. **Select Target** (Επιλογή Στόχου):
Αφού επιλεγεί ο τύπος των συσκευών, ο χρήστης επιλέγει τον στόχο της ενέργειας παραμετροποίησης. Αυτή η επιλογή περιλαμβάνει τη δημιουργία ενός νέου στόχου (*target device* ή *target group*) ή την επιλογή ενός ήδη υπάρχοντος.

Αφού ολοκληρωθούν οι παραπάνω επιλογές, στο μενού εμφανίζονται τα διαθέσιμα εργαλεία (*Tools*) που επιτρέπουν στον χρήστη να προχωρήσει στην παραμετροποίηση των συσκευών βάσει των επιλογών του.



Σχήμα 3.2 Βασικό Μενού

3.6 Δημιουργία νέου target

Ο χρήστης, έχοντας ήδη επιλέξει τον κατασκευαστή και τον τύπο του target, επιλέγει το “Add new target” από το βασικό μενού της εφαρμογής, και έπειτα συμπληρώνει τις απαραίτητες πληροφορίες. Ο χρήστης συμπληρώνει το όνομα και μία περιγραφή για το νέο target. Ανάλογα με τον προεπιλεγμένο τύπο του target (*device* ή *group*), η πλατφόρμα προβάλλει τα αντίστοιχα πεδία συμπλήρωσης.

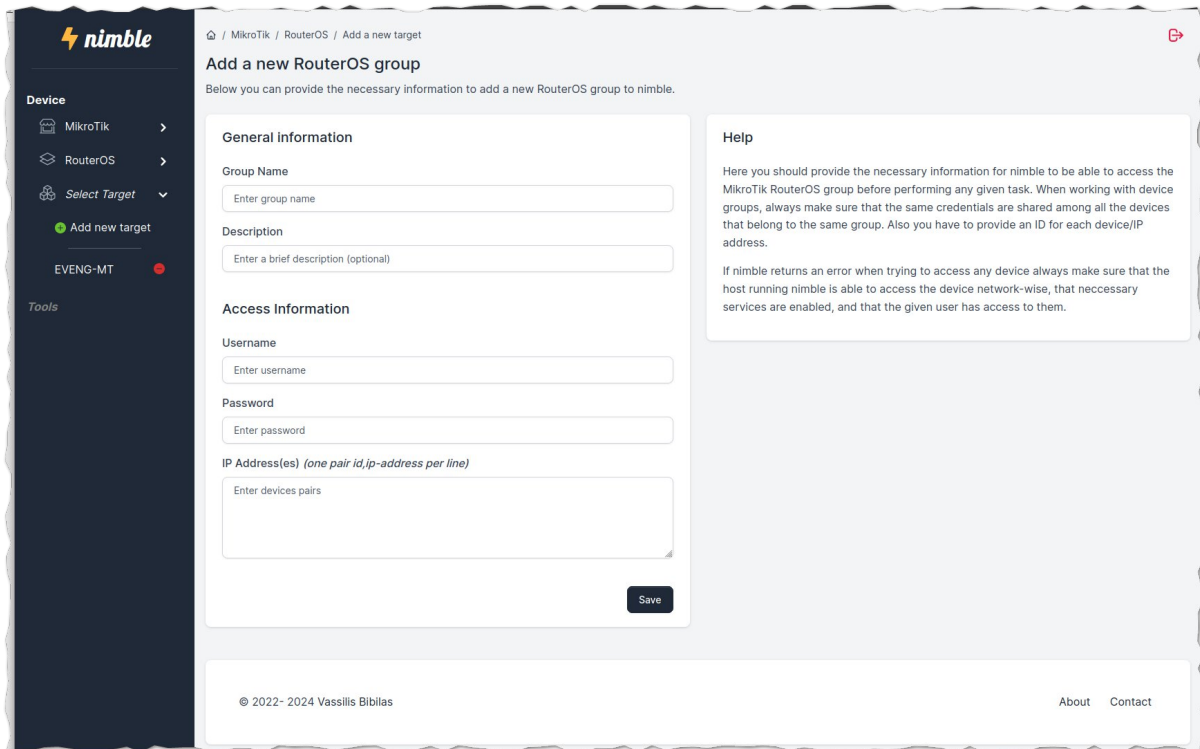
Είτε πρόκειται για target device, είτε για target group, ο χρήστης συμπληρώνει τα (κοινά μεταξύ των συσκευών στην περίπτωση του target group) username και password.

Αν πρόκειται για target device τότε ο χρήστης συμπληρώνει την IP διεύθυνση της συσκευής. Αν πρόκειται για target group τότε ο χρήστης θα πρέπει να συμπληρώσει τις IP διεύθυνση όλων των συσκευών που ανήκουν στο target group.

Αφού συμπληρώσει όλες τις απαραίτητες πληροφορίες, ο χρήστης αποθηκεύει το νέο target ή target group, επιτρέποντας έτσι στην πλατφόρμα “nimble” να χρησιμοποιήσει αυτές τις πληροφορίες για τη διαχείριση των δικτυακών συσκευών.

The screenshot shows the 'Add a new FMC device' page in the Nimble interface. The left sidebar contains a 'Device' menu with options for Cisco, FMC, and 'Add new target'. The main content area has a breadcrumb trail 'Cisco / FMC / Add a new target' and a title 'Add a new FMC device'. Below the title is a brief instruction: 'Below you can provide the necessary information to add a new FMC device to nimble.' The form is divided into two main sections: 'General information' and 'Access Information'. The 'General information' section includes a 'Device Name' field and an optional 'Description' field. The 'Access Information' section includes fields for 'Username', 'Password', and 'IP Address'. A 'Save' button is located at the bottom right of the form. To the right of the form is a 'Help' section with text explaining that users should provide necessary information for access and that services must be enabled on the device.

Σχήμα 3.3 Προσθήκη νέου target Cisco FMC



Σχήμα 3.4 Προσθήκη νέου target group Cisco IOS

3.7 Εργαλεία για το FMC

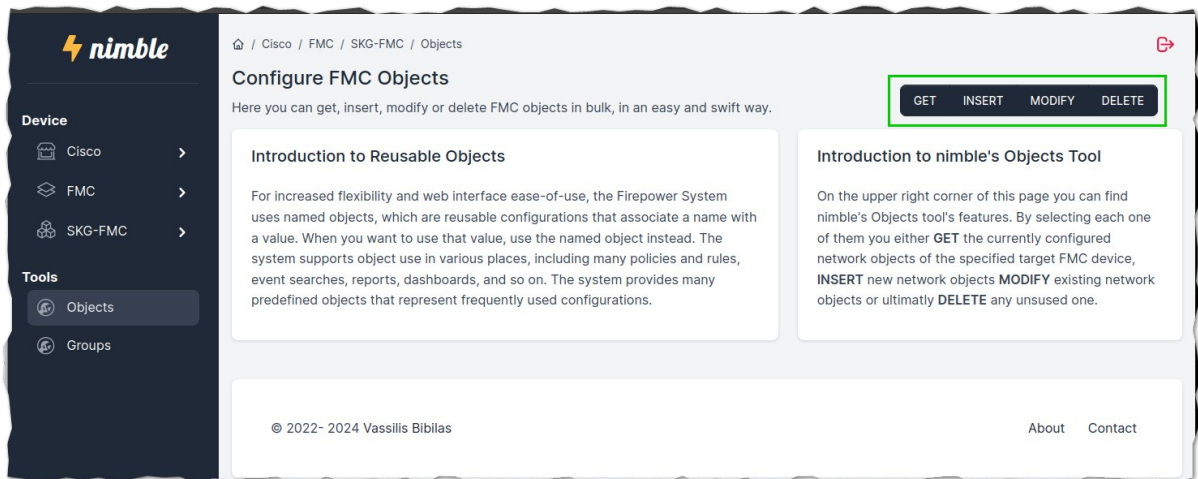
Με αυτά τα εργαλεία, ο χρήστης μπορεί να διαχειριστεί αποτελεσματικά τα object και τα object group στο Cisco FMC μέσω της πλατφόρμας “nimble”.

3.7.1 Εργαλείο “Objects” για τη διαχείριση αντικειμένων

Όταν ο χρήστης επιλέξει το εργαλείο “Objects”, του δίνεται η δυνατότητα να διαχειριστεί τα object στο Cisco FMC.

Ο χρήστης μπορεί να εκτελέσει τις ακόλουθες ενέργειες:

- i. **Λήψη (GET):** Να λάβει πληροφορίες για τα υπάρχοντα object.
- ii. **Προσθήκη (INSERT):** Να προσθέσει νέα object.
- iii. **Τροποποίηση (MODIFY):** Να τροποποιήσει τα υπάρχοντα object.
- iv. **Διαγραφή (DELETE):** Να διαγράψει υπάρχοντα object.



Σχήμα 3.5 Δυνατότητες εργαλείου Objects

3.7.1.1 Λήψη (*GET*) object

Για την λήψη των object ο χρήστης θα πρέπει να παρέχει τις παρακάτω πληροφορίες:

i. Επιλογή Τύπου Object:

Ο χρήστης επιλέγει τον τύπο των object που επιθυμεί να λάβει. Οι διαθέσιμοι τύποι είναι:

- **Network:** Δικτυακά object όπως διευθύνσεις υποδικτύων.
- **Host:** Object που αναφέρονται σε μεμονωμένες συσκευές ή υπολογιστές.
- **Range:** Εύρος διευθύνσεων IP.

ii. Περιορισμός Αποτελεσμάτων (Προαιρετικό):

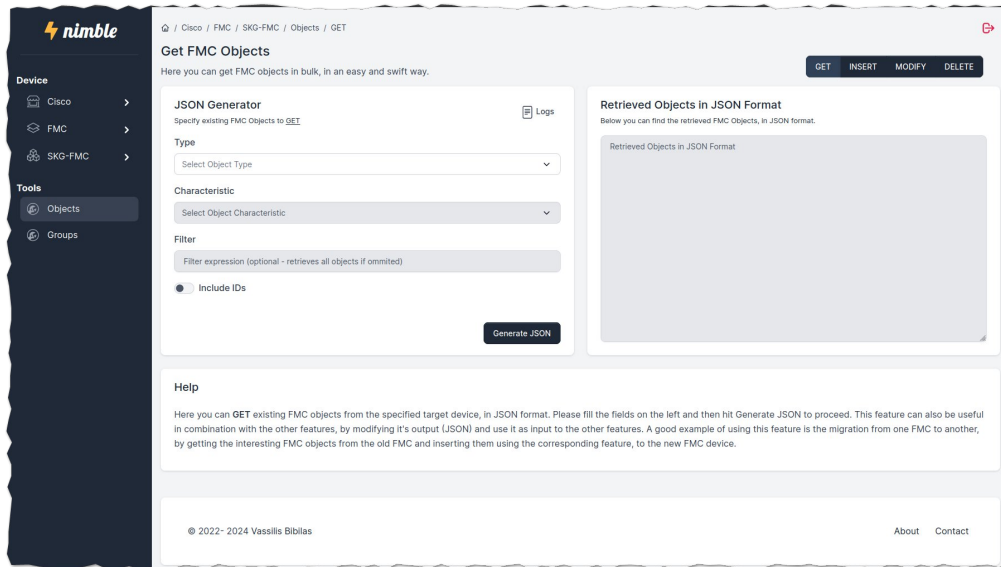
Ο χρήστης έχει τη δυνατότητα να περιορίσει τα αποτελέσματα με βάση συγκεκριμένα χαρακτηριστικά, χρησιμοποιώντας ένα filter expression. Οι επιλογές περιορισμού μπορεί να περιλαμβάνουν τα χαρακτηριστικά:

- **Name:** Αναγνωριστικό
- **Description:** Σύντομη περιγραφή
- **Value:** Τιμή

iii. Επιστροφή Αποτελεσμάτων σε JSON Μορφή:

Μετά την επιλογή των κατάλληλων παραμέτρων, το εργαλείο “Objects” επιστρέφει τα αποτελέσματα σε μορφή JSON. Αυτή η μορφή επιτρέπει στον χρήστη να επεξεργαστεί εύκολα τα δεδομένα ή να τα χρησιμοποιήσει ως είσοδο σε άλλα εργαλεία της εφαρμογής.

Με αυτόν τον τρόπο, ο χρήστης μπορεί να λαμβάνει τα object από το Cisco FMC σύμφωνα με τις προδιαγραφές που έχει ορίσει, ενώ ταυτόχρονα έχει τη δυνατότητα να προσαρμόσει τα αποτελέσματα στις ανάγκες του μέσω του φίλτρου.



Σχήμα 3.6 Δυνατότητα GET του εργαλείου Objects

3.7.1.2 Προσθήκη (INSERT) object

Για την προσθήκη object ο χρήστης θα πρέπει να παρέχει τις παρακάτω πληροφορίες:

i. Επιλογή Τύπου Object:

Ο χρήστης πρέπει να επιλέξει τον τύπο του object που επιθυμεί να προσθέσει, είτε πρόκειται για:

- **Network:** Δικτυακά object όπως διευθύνσεις υποδικτύων.
- **Host:** Object που αναφέρονται σε μεμονωμένες συσκευές ή υπολογιστές.
- **Range:** Εύρος διευθύνσεων IP.

ii. Συμπλήρωση Πεδίων:

Στη συνέχεια, ο χρήστης συμπληρώνει τα απαραίτητα πεδία για κάθε object:

- **Name:** Αναγνωριστικό
- **Description:** Σύνομη περιγραφή
- **Value:** Τιμή

iii. Χρήση Variables:

Ο χρήστης, αν επιθυμεί να προσθέσει πολλαπλά object του ίδιου τύπου, μπορεί να χρησιμοποιήσει variables. Στο πεδίο “Variables”, προσθέτει τα ονόματα των variables σε μορφή CSV στην πρώτη γραμμή και τις αντίστοιχες τιμές τους σε κάθε επόμενη γραμμή. Έπειτα, κάνει αναφορά των ονομάτων των variables ανάμεσα στα σύμβολα “<” και “>” σε οποιοδήποτε πεδίο (Name, Description, Value). Έτσι, για κάθε γραμμή με τιμές variables, δημιουργείται ένα νέο object .

iv. Χρήση Range:

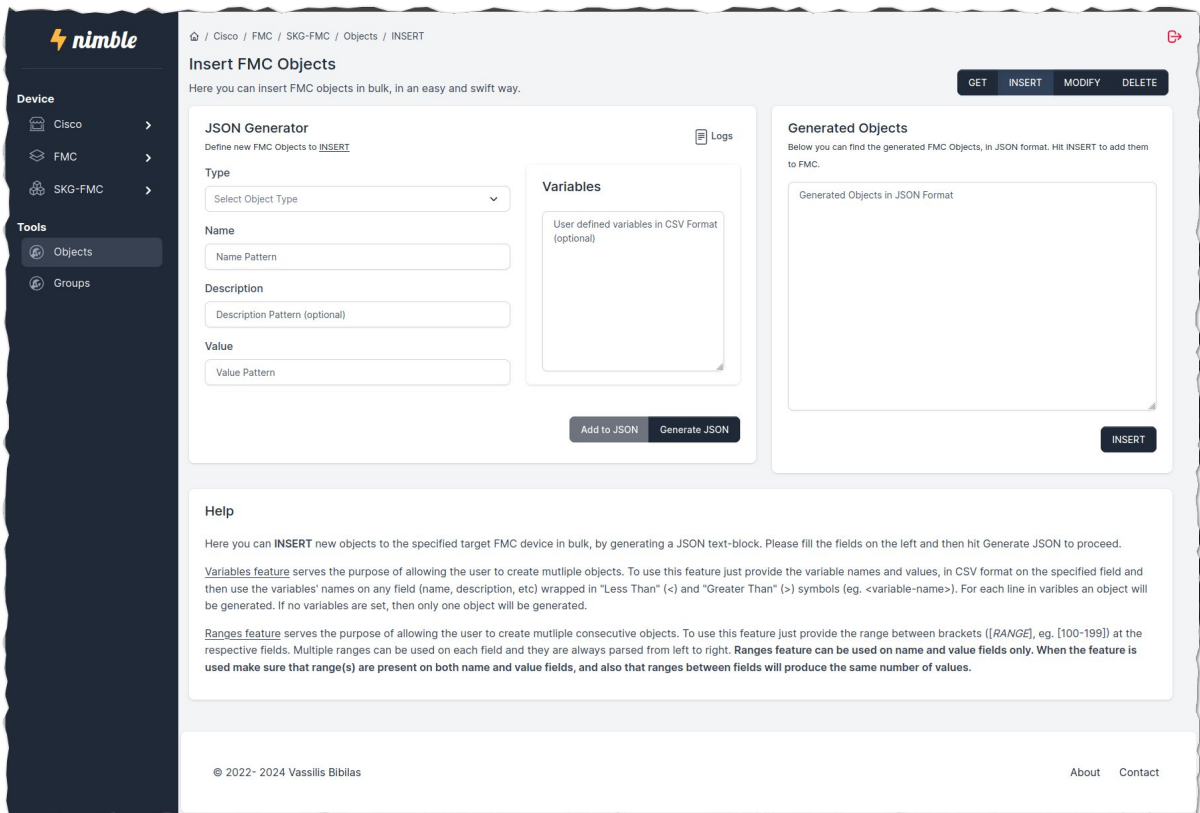
Το εργαλείο επιτρέπει τη χρήση ευρών, επιτρέποντας στον χρήστη να δημιουργήσει πολλαπλά συνεχόμενα object. Ο χρήστης προσθέτει τα range στα πεδία “Name” και “Value” εντός των συμβόλων “[” και “]”. Έπειτα, το εργαλείο δημιουργεί ένα object για κάθε τιμή του range. Είναι

σημαντικό να αναφέρουμε ότι κάθε τιμή του range αντιστοιχεί σε ένα object, και πρέπει να διατηρείται η αντιστοιχία μεταξύ των πεδίων “Name” και “Value”.

v. Πολλαπλά Εύρη (Multiple Ranges):

Υπάρχει η δυνατότητα χρήσης πολλαπλών ευρών στα πεδία, πάντα με την προϋπόθεση να τηρούνται οι παραπάνω προϋποθέσεις.

Με αυτόν τον τρόπο, ο χρήστης μπορεί να προσθέσει object με μεγάλη ευελιξία, είτε μεμονωμένα είτε σε μαζική κλίμακα χρησιμοποιώντας variables και ranges. Αφού ο χρήστης συμπληρώσει τα στοιχεία λαμβάνει ένα JSON αρχείο που περιέχει όλες τις πληροφορίες που πρόκειται να εφαρμοστούν στο FMC, παρέχοντας του έτσι τη δυνατότητα να ελέγξει και να επεξεργαστεί τις παραμέτρους πριν εφαρμοστούν στο FMC.



Σχήμα 3.7 Δυνατότητα INSERT του εργαλείου Objects

3.7.1.3 Τροποποίηση (MODIFY) object

Το εργαλείο “Objects” για την τροποποίηση υπαρχόντων object παρέχει στον χρήστη τη δυνατότητα να επεξεργαστεί τα ήδη υπάρχοντα object σύμφωνα με τις ανάγκες του.

Ο χρήστης ακολουθεί τα παρακάτω βήματα για να τροποποιήσει υπάρχοντα object:

i. Προσδιορισμός Object:

Αρχικά, ο χρήστης πρέπει να προσδιορίσει ποια object επιθυμεί να τροποποιήσει. Αυτό γίνεται συμπληρώνοντας τον τύπο του/των object που επιθυμεί να επεξεργαστεί, και έπειτα προσδιορίζοντας ένα filter expression βάσει κάποιου χαρακτηριστικού των object.

ii. Επιλογή Χαρακτηριστικού:

Έχοντας προσδιορίσει το/τα object που θέλει να τροποποιήσει, ο χρήστης πρέπει να συμπληρώσει το χαρακτηριστικό που επιθυμεί να τροποποιηθεί (π.χ. *Name, Description, Value*).

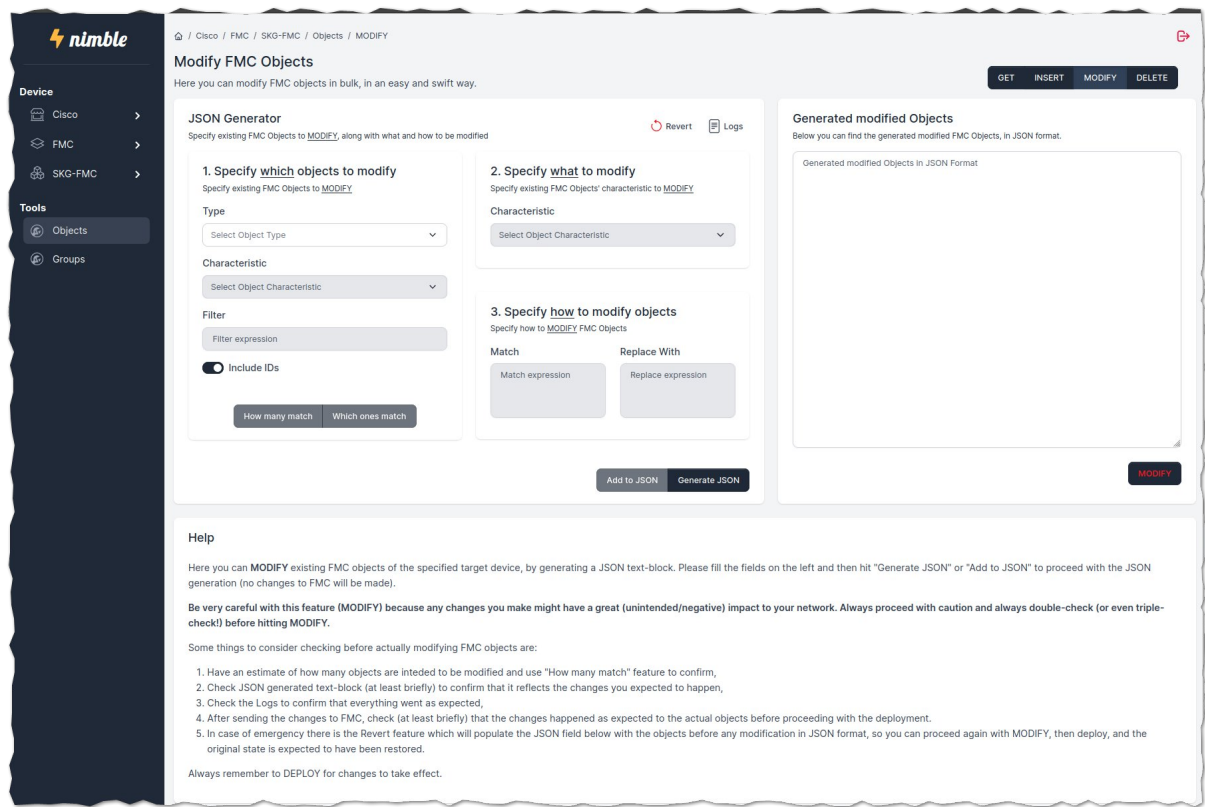
iii. Ορισμός Match Expression:

Ο χρήστης ορίζει ένα match expression, το οποίο καθορίζει ποιο τμήμα του χαρακτηριστικού θα τροποποιηθεί.

iv. Ορισμός Replace Expression:

Στη συνέχεια, ο χρήστης προσδιορίζει ένα replace expression, το οποίο καθορίζει πώς θα τροποποιηθεί το τμήμα του χαρακτηριστικού που προσδιορίστηκε από το match expression.

Με αυτόν τον τρόπο, ο χρήστης μπορεί να τροποποιήσει χαρακτηριστικά των υπάρχοντων object με πολλαπλούς και ευέλικτους τρόπους, προσαρμόζοντας τα ανάλογα με τις ανάγκες του συστήματός του. Αφού ο χρήστης συμπληρώσει τα στοιχεία λαμβάνει ένα JSON αρχείο που περιέχει όλες τις πληροφορίες που πρόκειται να εφαρμοστούν στο FMC, παρέχοντας του έτσι τη δυνατότητα να ελέγξει και να επεξεργαστεί τις παραμέτρους πριν εφαρμοστούν στο FMC.



Σχήμα 3.8 Δυνατότητα INSERT του εργαλείου Objects

3.7.1.4 Διαγραφή (DELETE) object

Το εργαλείο “Objects” για τη διαγραφή υπάρχοντων object παρέχει στον χρήστη τη δυνατότητα να αφαιρέσει object από το σύστημα σύμφωνα με τα κριτήρια που ορίζει.

Ο χρήστης ακολουθεί τα παρακάτω βήματα για τη διαγραφή υπάρχοντων object:

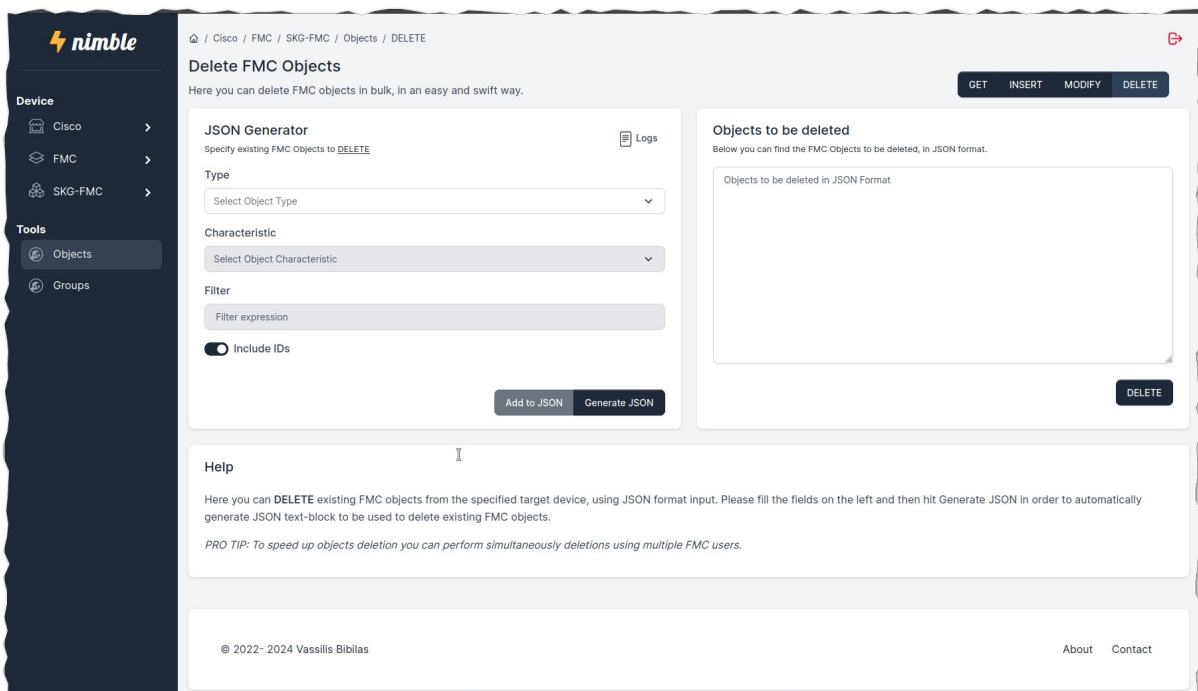
i. Προσδιορισμός Τύπου Object:

Αρχικά, ο χρήστης πρέπει να προσδιορίσει τον τύπο του/των object που επιθυμεί να διαγράψει, όπως δίκτυα (*Networks*), κόμβους (*Hosts*), ή range διευθύνσεων.

ii. Ορισμός Φίλτρου Εκφράσεων:

Έπειτα, ο χρήστης προσδιορίζει ένα filter expression βάσει κάποιου χαρακτηριστικού των object που επιθυμεί να διαγράψει. Αυτό μπορεί να είναι το όνομα του object, η περιγραφή του, ή οποιοδήποτε άλλο χαρακτηριστικό που είναι διαθέσιμο για φιλτράρισμα.

Μετά την ολοκλήρωση αυτών των βημάτων, το εργαλείο “Objects” θα διαγράψει τα object που πληρούν τα κριτήρια που ορίστηκαν από τον χρήστη. Είναι σημαντικό να προσέξει ο χρήστης κατά τη χρήση αυτού του εργαλείου, καθώς η διαγραφή object μπορεί να έχει μόνιμες επιπτώσεις στο σύστημα.



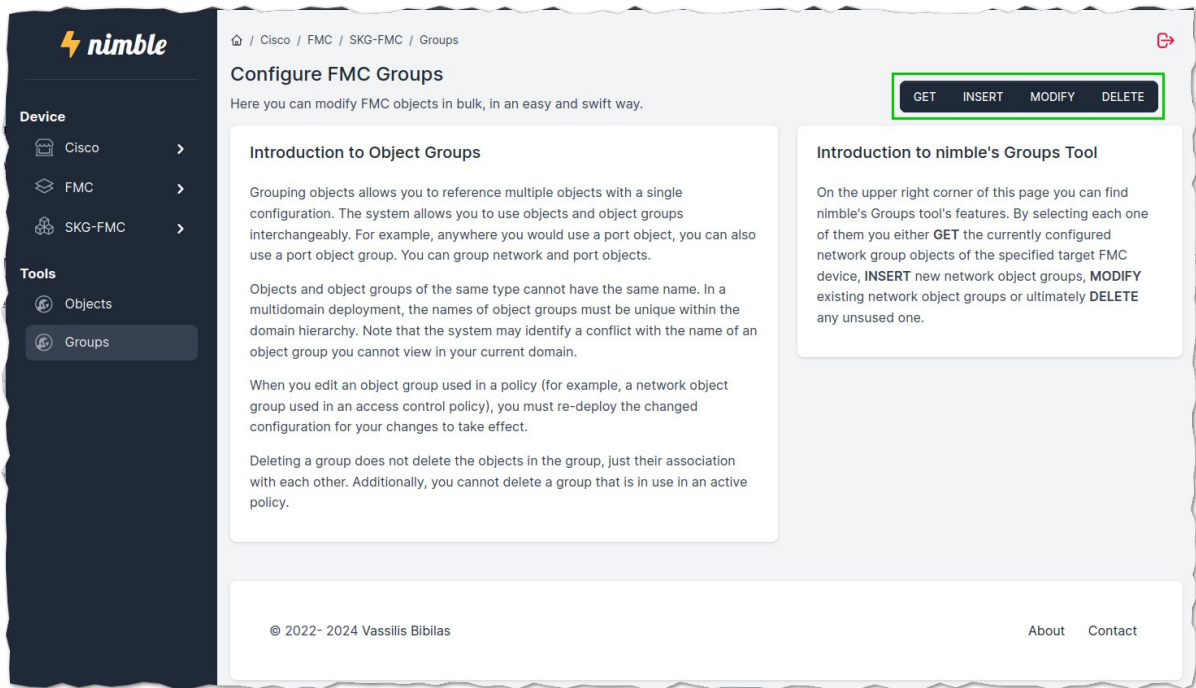
Σχήμα 3.9 Δυνατότητα DELETE του εργαλείου Objects

3.7.2 Εργαλείο “Groups” για διαχείρισης ομάδων object

Όταν ο χρήστης επιλέξει το εργαλείο “Groups”, του δίνεται η δυνατότητα να διαχειριστεί τα object group στο Cisco FMC.

Ο χρήστης μπορεί να εκτελέσει τις ακόλουθες ενέργειες:

- i. **Λήψη (GET):** Λήψη πληροφοριών για τα υπάρχοντα object group.
- ii. **Προσθήκη (INSERT):** Προσθήκη νέων object group.
- iii. **Τροποποίηση (MODIFY):** Τροποποίηση υπάρχοντων object group.
- iv. **Διαγραφή (DELETE):** Διαγραφή object group.



Σχήμα 3.10 Δυνατότητες εργαλείου Groups

3.7.2.1 Λήψη (GET) object group

Για την λήψη object group ο χρήστης θα πρέπει να παρέχει τις παρακάτω πληροφορίες:

i. Επιλογή Τύπου Object Group:

Ο χρήστης επιλέγει τον τύπο των object group που επιθυμεί να λάβει. Οι διαθέσιμοι τύποι είναι:

- **Network:** Object group που περιέχουν δικτυακά object όπως διευθύνσεις IP ή υποδίκτυα.
- **Port:** Object group που περιέχουν object θυρών που αναφέρονται σε υπηρεσίες.

ii. Περιορισμός Αποτελεσμάτων (Προαιρετικό):

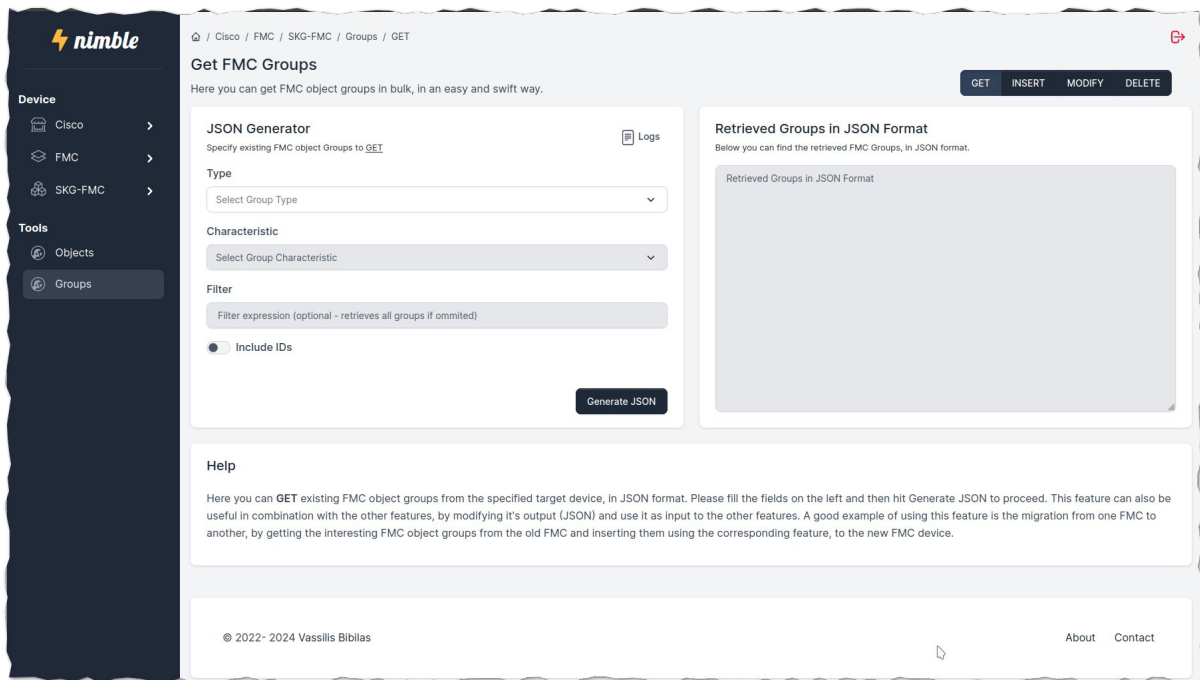
Ο χρήστης έχει τη δυνατότητα να περιορίσει τα αποτελέσματα με βάση συγκεκριμένα χαρακτηριστικά, χρησιμοποιώντας ένα filter expression. Οι επιλογές περιορισμού μπορεί να περιλαμβάνουν τα χαρακτηριστικά:

- **Name:** Αναγνωριστικό
- **Description:** Σύντομη περιγραφή
- **Members:** Μέλη του object group

iii. Επιστροφή Αποτελεσμάτων σε JSON Μορφή:

Μετά την επιλογή των κατάλληλων παραμέτρων, το εργαλείο “Groups” επιστρέφει τα αποτελέσματα σε μορφή JSON. Αυτή η μορφή επιτρέπει στον χρήστη να επεξεργαστεί εύκολα τα δεδομένα ή να τα χρησιμοποιήσει ως είσοδο σε άλλα εργαλεία της εφαρμογής.

Με αυτόν τον τρόπο, ο χρήστης μπορεί να λαμβάνει τα object group από το Cisco FMC σύμφωνα με τις προδιαγραφές που έχει ορίσει, ενώ ταυτόχρονα έχει τη δυνατότητα να προσαρμόσει τα αποτελέσματα στις ανάγκες του μέσω του φίλτρου.



Σχήμα 3.11 Δυνατότητα GET του εργαλείου Groups

3.7.2.2 Προσθήκη (INSERT) object group

Για την προσθήκη object group ο χρήστης θα πρέπει να παρέχει τις παρακάτω πληροφορίες:

i. Επιλογή Τύπου Object Group:

Ο χρήστης πρέπει να επιλέξει τον τύπο του object group που επιθυμεί να προσθέσει, είτε πρόκειται για:

- **Network:** Object group που περιέχουν δικτυακά object όπως διευθύνσεις IP ή υποδίκτυα.
- **Port:** Object group που περιέχουν object θυρών που αναφέρονται σε υπηρεσίες.

ii. Συμπλήρωση Πεδίων:

Στη συνέχεια, ο χρήστης συμπληρώνει τα απαραίτητα πεδία για κάθε object group:

- **Name:** Αναγνωριστικό
- **Description:** Σύντομη περιγραφή
- **Members:** Μέλη του object group

iii. Χρήση Variables:

Ο χρήστης, αν επιθυμεί να προσθέσει πολλαπλά object group του ίδιου τύπου, μπορεί να χρησιμοποιήσει variables. Στο πεδίο “Variables”, προσθέτει τα ονόματα των variables σε μορφή CSV στην πρώτη γραμμή και τις αντίστοιχες τιμές τους σε κάθε επόμενη γραμμή. Έπειτα, αναφέρει τα ονόματα των variables ανάμεσα στα σύμβολα “<” και “>” σε οποιοδήποτε πεδίο (*Name*, *Description*). Έτσι, για κάθε γραμμή με τιμές variables, δημιουργείται ένα νέο object group.

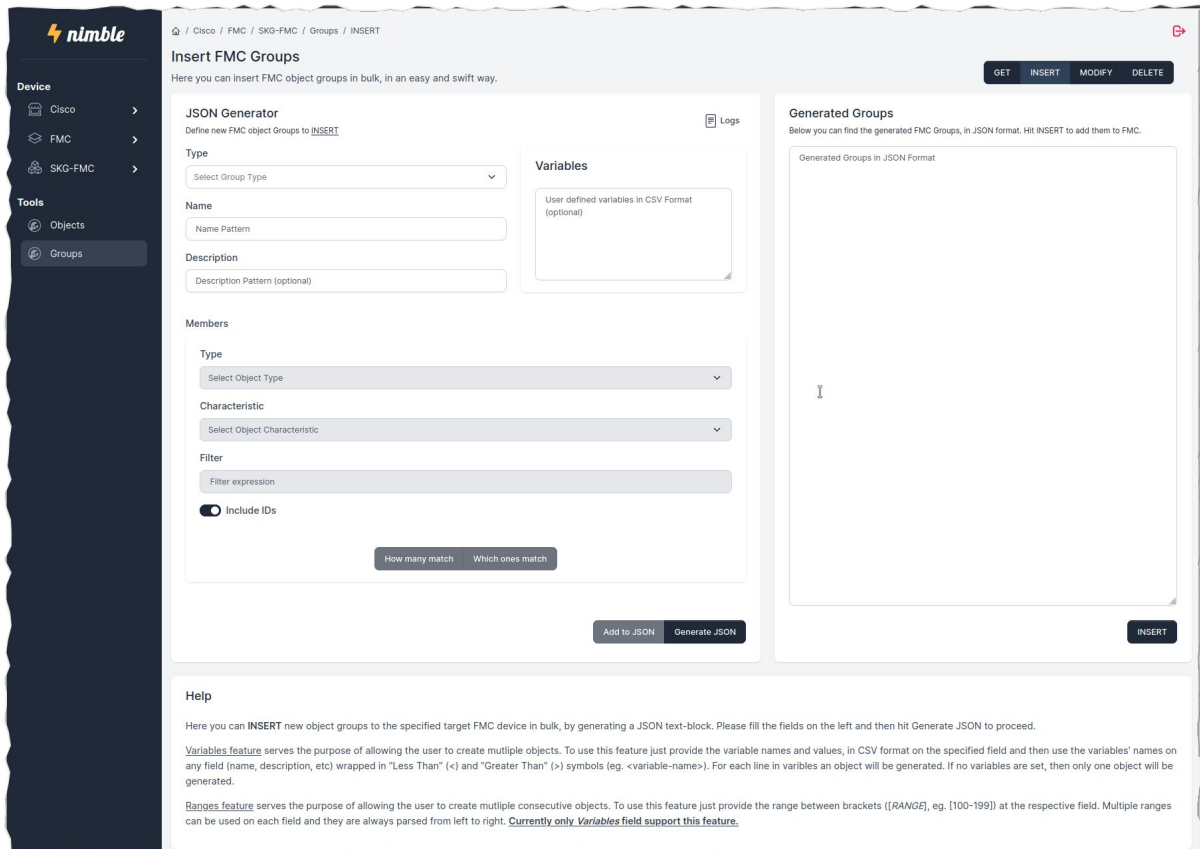
iv. Χρήση Range:

Το εργαλείο επιτρέπει τη χρήση ευρών, επιτρέποντας στον χρήστη να δημιουργήσει πολλαπλά συνεχόμενα object group. Ο χρήστης προσθέτει τα range στο πεδίο “Variables” εντός των συμβόλων “[” και “]”. Έπειτα, το εργαλείο δημιουργεί ένα object group για κάθε τιμή του range.

v. Πολλαπλά Εύρη (Multiple Ranges):

Υπάρχει η δυνατότητα χρήσης πολλαπλών ευρών στα πεδία, πάντα με την προϋπόθεση να τηρούνται οι παραπάνω προϋποθέσεις. Η διεκπεραίωση των ευρών συμβαίνει πάντα από αριστερά προς τα δεξιά.

Με αυτόν τον τρόπο, ο χρήστης μπορεί να προσθέσει object group με μεγάλη ευελιξία, είτε μεμονωμένα είτε σε μαζική κλίμακα χρησιμοποιώντας variables και ranges. Αφού ο χρήστης συμπληρώσει τα στοιχεία λαμβάνει ένα JSON αρχείο που περιέχει όλες τις πληροφορίες που πρόκειται να εφαρμοστούν στο FMC, παρέχοντας του έτσι τη δυνατότητα να ελέγξει και να επεξεργαστεί τις παραμέτρους πριν εφαρμοστούν στο FMC.



Σχήμα 3.12 Δυνατότητα INSERT του εργαλείου Groups

3.7.2.3 Τροποποίηση (MODIFY) object group

Το εργαλείο “Groups” για την τροποποίηση υπάρχοντων object group παρέχει στον χρήστη τη δυνατότητα να επεξεργαστεί τα ήδη υπάρχοντα object group σύμφωνα με τις ανάγκες του.

Ο χρήστης ακολουθεί τα παρακάτω βήματα για να τροποποιήσει τις υπάρχοντα object group:

i. Προσδιορισμός Object Group :

Αρχικά, ο χρήστης πρέπει να προσδιορίσει ποια object group επιθυμεί να τροποποιήσει. Αυτό γίνεται συμπληρώνοντας τον τύπο του/των object group που επιθυμεί να επεξεργαστεί, και έπειτα προσδιορίζοντας ένα filter expression βάσει κάποιου χαρακτηριστικού των object group.

ii. Επιλογή Χαρακτηριστικού:

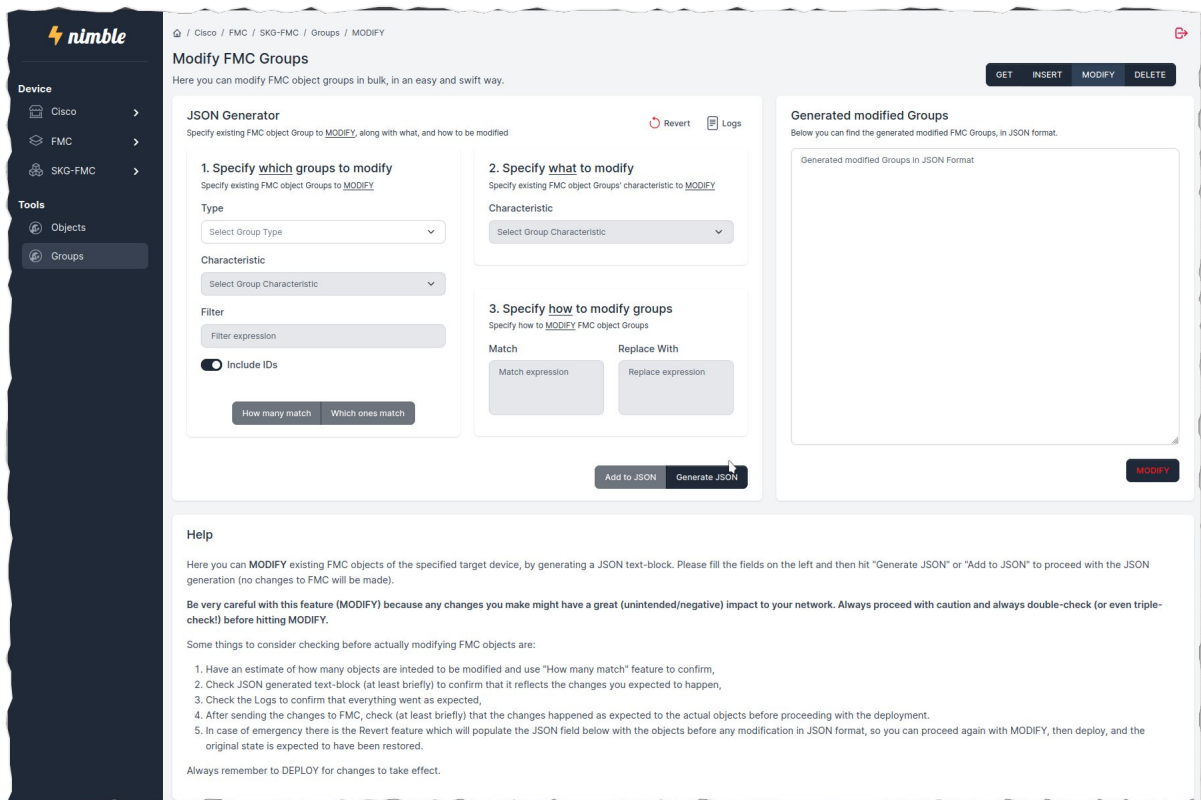
Έχοντας προσδιορίσει το/τα object group που θέλει να τροποποιήσει, ο χρήστης πρέπει να συμπληρώσει το χαρακτηριστικό που επιθυμεί να τροποποιηθεί (π.χ. *Name*, *Description*, *Members*).

iii. Ορισμός Match Expression:

Ο χρήστης ορίζει ένα match expression, το οποίο καθορίζει ποιο τμήμα του χαρακτηριστικού θα τροποποιηθεί.

iv. Ορισμός Replace Expression:

Στη συνέχεια, ο χρήστης προσδιορίζει ένα replace expression, το οποίο καθορίζει πώς θα τροποποιηθεί το τμήμα του χαρακτηριστικού που προσδιορίστηκε από το match expression.



Σχήμα 3.13 Δυνατότητα MODIFY του εργαλείου Groups

Στην περίπτωση που ο χρήστης επιθυμεί να τροποποιήσει τα μέλη (*members*) του/των object group θα πρέπει να προσδιορίσει τα παρακάτω:

i. Προσδιορισμός Ενεργείας (Action):

Αρχικά, ο χρήστης πρέπει να προσδιορίσει μία ενέργεια από τις παρακάτω που επιθυμεί να εφαρμοστεί:

- **Add members:** Προσθέτει object στα ήδη υπάρχοντα object του/των object group.
- **Remove members:** Αφαιρεί object από τα ήδη υπάρχοντα object του/των object group.
- **Re-set members:** Επαναπροσδιορίζει τα object του/των object group.

ii. Επιλογή Τύπου των μελών:

Έχοντας προσδιορίσει την ενέργεια που αφορά την τροποποίηση των μελών του/των object group, ο χρήστης πρέπει να συμπληρώσει τον τύπο των object στα οποία θέλει να εφαρμοστεί η παραπάνω ενέργεια (π.χ. *Network, Host, Range, Network-Group*).

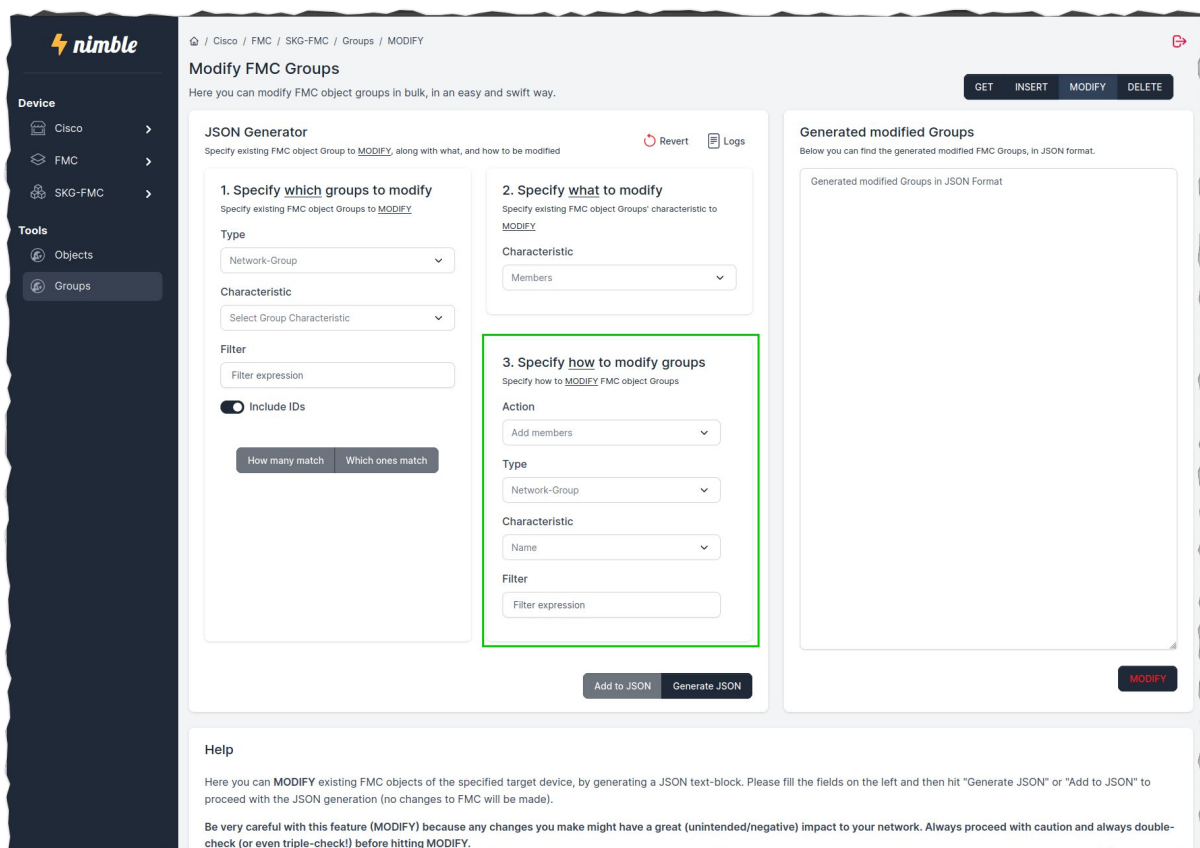
iii. Επιλογή Χαρακτηριστικού των μελών:

Έχοντας προσδιορίσει την ενέργεια και τον τύπο που αφορά την τροποποίηση των μελών του/των object group, ο χρήστης πρέπει να συμπληρώσει το χαρακτηριστικό των object στα οποία θέλει να εφαρμοστεί η παραπάνω ενέργεια (π.χ. *Name, Description, Value*).

iv. Ορισμός Φίλτρου Εκφράσεων:

Έπειτα, ο χρήστης προσδιορίζει ένα filter expression βάσει του χαρακτηριστικού των object που αφορούν την τροποποίηση των μελών του/των object group.

Με αυτόν τον τρόπο, ο χρήστης μπορεί να τροποποιήσει χαρακτηριστικά των υπάρχοντων object group με πολλαπλούς και ευέλικτους τρόπους, προσαρμόζοντας τα ανάλογα με τις ανάγκες του συστήματός του. Αφού ο χρήστης συμπληρώσει τα στοιχεία λαμβάνει ένα JSON αρχείο που περιέχει όλες τις πληροφορίες που πρόκειται να εφαρμοστούν στο FMC, παρέχοντας του έτσι τη δυνατότητα να ελέγξει και να επεξεργαστεί τις παραμέτρους πριν εφαρμοστούν στο FMC.



Σχήμα 3.14 Δυνατότητα MODIFY MEMBERS του εργαλείου Groups

3.7.2.4 Διαγραφή (DELETE) object group

Το εργαλείο “Groups” για τη διαγραφή υπάρχοντων object group παρέχει στον χρήστη τη δυνατότητα να αφαιρέσει object group από το σύστημα σύμφωνα με τα κριτήρια που ορίζει.

Ο χρήστης ακολουθεί τα παρακάτω βήματα για τη διαγραφή υπάρχοντων object group:

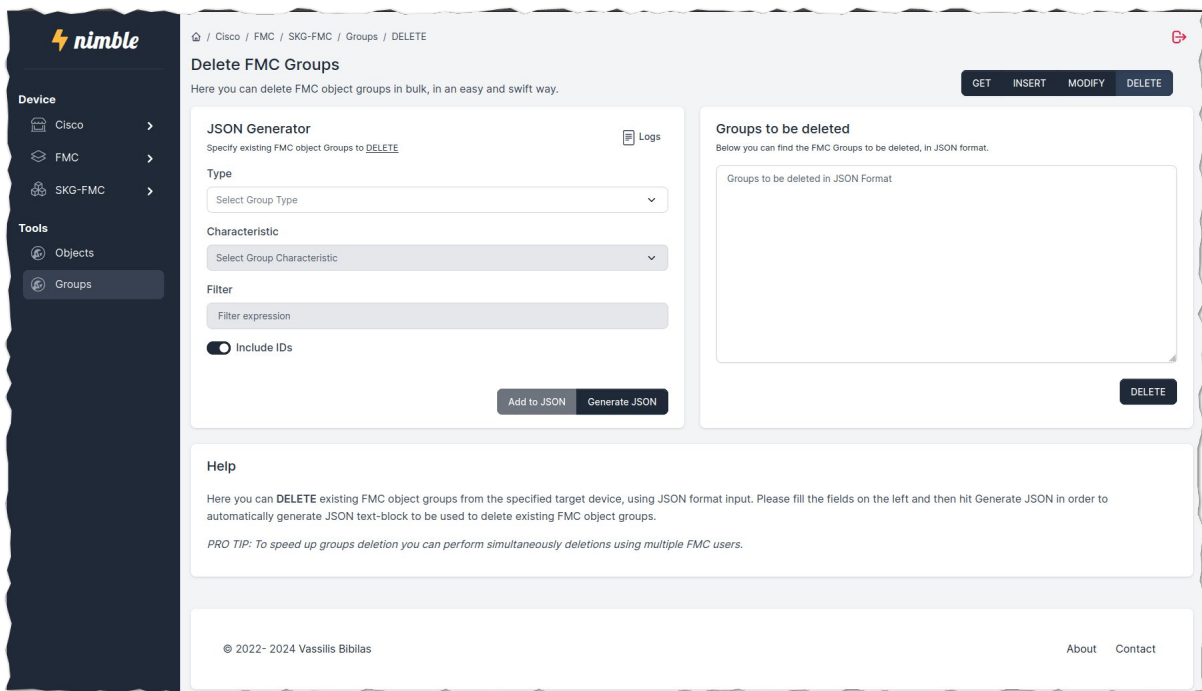
i. Προσδιορισμός Τύπου Object Group:

Αρχικά, ο χρήστης πρέπει να προσδιορίσει τον τύπο του/των object group που επιθυμεί να διαγράψει, όπως ομάδες δικτυακών αντικειμένων (*network groups*) ή ομάδες αντικειμένων θυρών (*port groups*).

ii. Ορισμός Φίλτρου Εκφράσεων:

Έπειτα, ο χρήστης προσδιορίζει ένα filter expression βάσει κάποιου χαρακτηριστικού των object group που επιθυμεί να διαγράψει. Αυτό μπορεί να είναι το όνομα του/των object group, η περιγραφή της/των, ή τα μέλη.

Μετά την ολοκλήρωση αυτών των βημάτων, το εργαλείο “Groups” θα διαγράψει τα object group που πληρούν τα κριτήρια που ορίστηκαν από τον χρήστη. Είναι σημαντικό να προσέξει ο χρήστης κατά τη χρήση αυτού του εργαλείου, καθώς η διαγραφή object group μπορεί να έχει μόνιμες επιπτώσεις στο σύστημα.



Σχήμα 3.15 Δυνατότητα DELETE του εργαλείου Groups

3.8 Εργαλείο “Bulk Configurator” για μαζική και ταυτόχρονη παραμετροποίηση

Το εργαλείο “Bulk Configurator” επιτρέπει στους χρήστες να εφαρμόσουν μαζικά και ταυτόχρονα ρυθμίσεις σε δικτυακές συσκευές, όπως routers και switches, από διάφορους κατασκευαστές, όπως Cisco, Aruba και MikroTik. Ο χρήστης έχει τη δυνατότητα να προσδιορίσει τον κατασκευαστή της ομάδας συσκευών (*target group*) καθώς και τον τύπο τους με βάση το λειτουργικό τους σύστημα. Αφού επιλέξει αυτά τα στοιχεία από το βασικό μενού, μπορεί να χρησιμοποιήσει το εργαλείο “Bulk Configurator” για να εφαρμόσει τις επιθυμητές ρυθμίσεις.

Χρησιμοποιώντας αυτό το εργαλείο, οι network administrators μπορούν να επιτύχουν τα ακόλουθα:

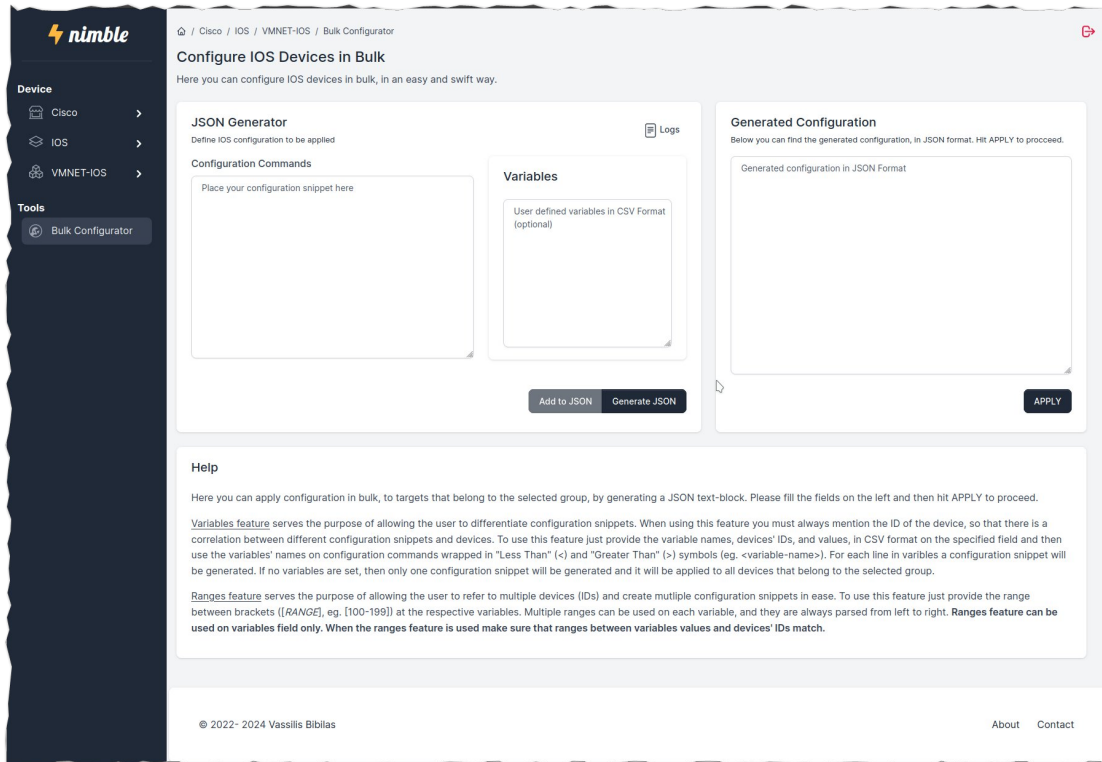
- Εξοικονόμηση Χρόνου: Αντί να πρέπει να διαχειρίζονται κάθε συσκευή ξεχωριστά, οι διαχειριστές μπορούν να εφαρμόζουν αλλαγές σε ένα σύνολο συσκευών ταυτόχρονα, εξοικονομώντας έτσι χρόνο και πόρους.
- Ενιαία Διαχείριση: Μέσω αυτού του εργαλείου, οι διαχειριστές μπορούν να επιτύχουν ενιαία διαχείριση του δικτύου τους, ανεξάρτητα από τον κατασκευαστή των συσκευών.
- Αυτοματοποίηση: Η δυνατότητα μαζικής παραμετροποίησης επιτρέπει στους διαχειριστές να αυτοματοποιήσουν διαδικασίες συντήρησης και διαχείρισης, μειώνοντας την ανθρώπινη επέμβαση και τον κίνδυνο σφαλμάτων.

Με τη βοήθεια αυτού του εργαλείου, οι network administrators μπορούν να διαχειρίζονται με αποτελεσματικό τρόπο το configuration των δικτυακών τους συσκευών, εξοικονομώντας χρόνο και προσπάθεια και βελτιστοποιώντας την επίδοση και την ασφάλεια του δικτύου. Αν ο χρήστης επιθυμεί να εφαρμόσει τις ίδιες εντολές σε όλες τις συσκευές της ομάδας συσκευών, αρκεί να συμπληρώσει τις εντολές που επιθυμεί στο αντίστοιχο πεδίο. Έπειτα, το εργαλείο παράγει το αντίστοιχο JSON για τη μαζική εφαρμογή των ρυθμίσεων. Επιπλέον, ο χρήστης μπορεί να χρησιμοποιήσει variables για να διαφοροποιήσει το configuration που προορίζεται για κάθε συσκευή. Για να το πετύχει αυτό, θα πρέπει να συμπληρώσει τα ονόματα των variables στο αντίστοιχο πεδίο και έπειτα τις τιμές αυτών σε κάθε επόμενη γραμμή. Απαραίτητη προϋπόθεση αποτελεί η αναφορά του αναγνωριστικού συσκευής (*device-id*) κάθε συσκευής, όπως το δήλωσε κατά την εισαγωγή της συσκευής στην πλατφόρμα, ώστε να γίνει η αντιστοίχιση των configuration snippet με τις συσκευές της ομάδας συσκευών (*target group*). Έτσι, δίνεται η δυνατότητα στον χρήστη να εφαρμόσει configuration σε υποσύνολο των συσκευών που ανήκουν στην ομάδα συσκευών.

Η χρήση των variables γίνεται με αναφορά του ονόματος τους εντός των συμβόλων "<" και ">", ενώ η χρήση ευρών επιτρέπεται μόνο στο πεδίο των variables. Είναι σημαντικό να ταιριάζει το πλήθος των ευρών με το πλήθος των device-id. Αυτό εξασφαλίζει την αντιστοίχιση κάθε configuration snippet με τις σωστές συσκευές. Η χρήση variables παρέχει στους χρήστες τη δυνατότητα να προσαρμόσουν το configuration για κάθε συσκευή με βάση τις ανάγκες και τις διαφορές στη διαμόρφωση των συσκευών. Με τη χρήση variables, ο χρήστης μπορεί να αναφέρει παραμέτρους όπως διευθύνσεις IP, ονόματα δικτύων ή οποιαδήποτε άλλη πληροφορία που χρειάζεται να προσαρμοστεί για κάθε συσκευή ξεχωριστά. Κάθε γραμμή με τιμές των variables στο πεδίο των variables αντιστοιχεί σε ένα configuration snippet που προορίζεται για μια συγκεκριμένη συσκευή, κάνοντας έτσι εύκολο να διαμορφωθεί το configuration για κάθε συσκευή ξεχωριστά.

Όσον αφορά τα range, αυτά επιτρέπουν στον χρήστη να ορίσει ένα range τιμών για μια variable, αντί για μια συγκεκριμένη τιμή. Αυτό είναι χρήσιμο όταν ο χρήστης θέλει να εφαρμόσει μια παρόμοια ρύθμιση σε μια ομάδα συσκευών που έχουν παρόμοιες αλλά όχι ακριβώς ίδιες παραμέτρους. Χρησιμοποιώντας ένα range, αυτή η ρύθμιση θα εφαρμοστεί αυτόματα σε όλες τις συσκευές που

πληρούν αυτό το κριτήριο, εξοικονομώντας έτσι χρόνο και προσπάθεια στον χρήστη.



Σχήμα 3.16 Εργαλείο Bulk Configurator

3.9 Βάση δεδομένων

Η βασική βάση δεδομένων της πλατφόρμας αποτελεί το κεντρικό στοιχείο που διαχειρίζεται και αποθηκεύει την πληροφορία που απαιτείται για τη λειτουργία του συστήματος. Αυτή η βάση δεδομένων περιλαμβάνει πολλούς πίνακες που είναι σχεδιασμένοι να αποθηκεύουν διαφορετικές κατηγορίες πληροφοριών, επιτρέποντας έτσι την αποτελεσματική οργάνωση και διαχείριση των δεδομένων.

Οι κύριοι πίνακες που απαρτίζουν τη βάση δεδομένων συνήθως περιλαμβάνουν πληροφορίες για τους κατασκευαστές (*Vendors*), τους τύπους συσκευών (*Types*), τα εργαλεία (*Tools*), τις εφαρμογές Django (*DjangoApps*), τους στόχους (*Targets*) και τις διευθύνσεις IP (*IP Addresses*). Κάθε πίνακας περιλαμβάνει πεδία που αντιστοιχούν σε συγκεκριμένα χαρακτηριστικά ή πληροφορίες που πρέπει να αποθηκευτούν, όπως ονόματα, περιγραφές, τύποι, διευθύνσεις IP και πολλά άλλα.

Οι πίνακες συνδέονται μεταξύ τους μέσω συσχετίσεων (*relationships*), οι οποίες ορίζουν τον τρόπο με τον οποίο οι διάφοροι τύποι πληροφοριών συσχετίζονται μεταξύ τους. Για παράδειγμα, ο πίνακας των στόχων (*Targets*) μπορεί να έχει σχέσεις με τους πίνακες των κατασκευαστών (*Vendors*) και των τύπων (*Types*) συσκευών, ώστε να καθοριστεί ποια συσκευή ανήκει σε ποιον κατασκευαστή και τύπο.

Η βάση δεδομένων παρέχει τη βάση για τη λειτουργία και τη λειτουργικότητα της πλατφόρμας, καθώς επίσης επιτρέπει την ανάκτηση, την ενημέρωση και τη διαγραφή δεδομένων με ασφάλεια και αποτελεσματικότητα. Η σωστή σχεδίαση και διαχείριση της βάσης δεδομένων είναι κρίσιμη για την ομαλή λειτουργία της πλατφόρμας και την αποτελεσματική αξιοποίηση των δεδομένων που περιέχονται σε αυτήν.

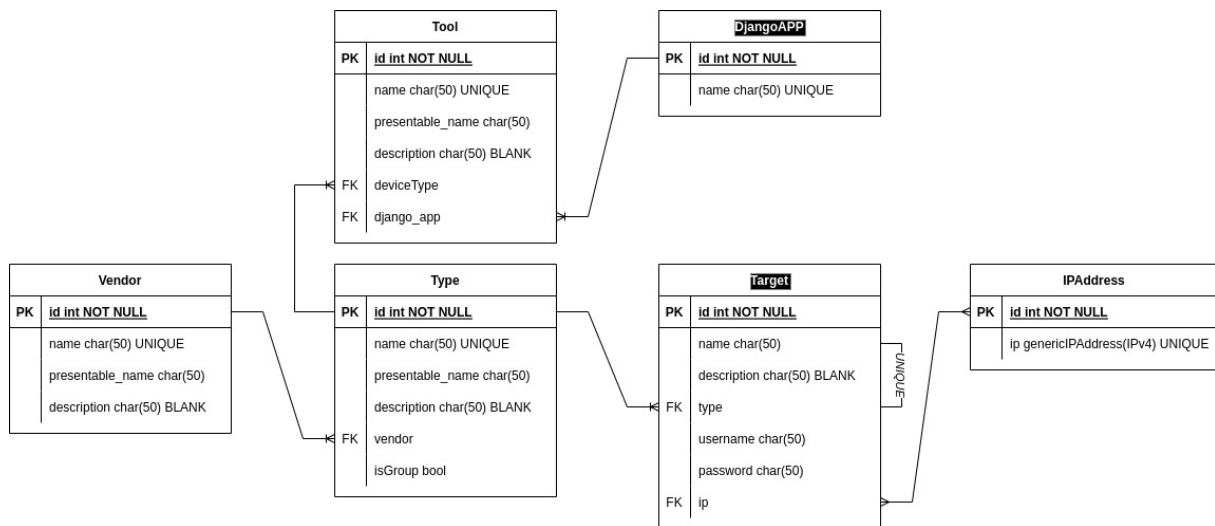
Η βασική βάση δεδομένων της πλατφόρμας αποτελεί τον πυρήνα του συστήματος, στον οποίο αποθηκεύονται οι κρίσιμες πληροφορίες που απαιτούνται για τη λειτουργία της. Ο κύριος σκοπός του

base APP είναι η σύνδεση των συσκευών (*targets*) με τις λειτουργίες της πλατφόρμας που εκφράζονται μέσω των Django-Apps.

Τα βασικά στοιχεία της βάσης αποτελούν τα στοιχεία των συσκευών (*targets*) και τις λειτουργίες της πλατφόρμας που παρέχονται μέσω των Django-Apps. Αυτά τα δύο στοιχεία είναι κρίσιμα, διότι ανεξάρτητα από τις ειδικές λειτουργίες που προσφέρει η πλατφόρμα “nimble”, πάντα αφορούν τις συσκευές (*targets*) και τις λειτουργίες (*Django-Apps*). Τα Django-Apps αντιπροσωπεύουν τη λειτουργικότητα ή τον πυρήνα (*value*) της πλατφόρμας “nimble”.

Συνολικά, η “nimble” είναι εδώ για να εξυπηρετήσει τις ανάγκες αυτοματοποίησης μέσω των διαφορετικών Django-Apps, οι οποίες αναφέρονται στις συσκευές (*targets*). Η σύνδεση των συσκευών (*targets*) με τα Django-Apps γίνεται μέσω του base APP και των αντίστοιχων μενού στο front-end, για τα οποία επίσης είναι υπεύθυνο το base APP.

Τέλος, το base APP αναλαμβάνει επίσης βασικές λειτουργίες όπως το login και το logout, προσφέροντας έτσι τη δυνατότητα στους χρήστες να προσδεθούν και να αποσυνδεθούν από την πλατφόρμα με ασφάλεια και ευκολία.



Σχήμα 3.17 Βάση δεδομένων εφαρμογής

3.10 Επίλογος

Στο κεφάλαιο αυτό μελετήσαμε την πλατφόρμα “nimble” και τον τρόπο λειτουργίας της. Ξεκινήσαμε με μια εισαγωγή στην πλατφόρμα και τα οφέλη που προσφέρει στους network administrator. Στη συνέχεια, εξετάσαμε τα εργαλεία και τις τεχνολογίες που χρησιμοποιήθηκαν για την ανάπτυξη της πλατφόρμας, όπως το Django, το Python, το Python API της Cisco, το Paramiko, η βιβλιοθήκη Bootstrap, το Javascript και οι μορφές αρχείων JSON και CSV. Αναφέραμε επίσης τη χρήση των εργαλείων EVE-NG και VMware για την προσομοίωση δικτυακών συσκευών και το στήσιμο του FMC.

Τέλος, εξετάσαμε την αρχιτεκτονική και τη λειτουργικότητα της πλατφόρμας, συμπεριλαμβανομένων των διαφόρων εργαλείων για το FMC, τη δημιουργία νέων στόχων και τον τρόπο εισόδου στην εφαρμογή. Μέσω αυτής της ανάλυσης, κατανοήσαμε τη σημασία της πλατφόρμας “nimble” για την αυτοματοποίηση δικτύων και τη διαχείριση συσκευών, καθώς και τον ρόλο που παίζουν τα διάφορα εργαλεία και τεχνολογίες στην ανάπτυξη και τη λειτουργία της. Η πλατφόρμα αυτή ανταποκρίνεται σε σύγχρονες ανάγκες δικτύων και προσφέρει ένα περιβάλλον για τη διαχείριση και την αυτοματοποίηση δικτύων.

Κεφάλαιο 4ο: Μελέτη Περίπτωσης Λειτουργίας της “nimble”

4.1 Εισαγωγή

Σε αυτήν την ενότητα θα μελετήσουμε ένα σενάριο που εστιάζει στη λειτουργία της πλατφόρμας “nimble” σε ένα εταιρικό περιβάλλον. Θα εξετάσουμε το προφίλ μιας υποθετικής εταιρίας και την τοπολογία του δικτύου της. Στη συνέχεια, θα επικεντρωθούμε στο υποθετικό σενάριο, με σκοπό να αναδείξουμε τις δυνατότητες και τα οφέλη που προσφέρει η πλατφόρμα “nimble” στην επίλυση πραγματικών προβλημάτων και στη βελτίωση της λειτουργικότητας του δικτύου.

Μέσα από αυτήν τη μελέτη περίπτωσης, θα διαπιστώσουμε πώς η πλατφόρμα “nimble” μπορεί να προσαρμοστεί αποτελεσματικά στις ανάγκες μιας επιχείρησης, προσφέροντας απλότητα χρήσης, αυτοματοποίηση εργασιών και ασφάλεια, ενώ ταυτόχρονα βελτιώνει την απόδοση και την αποτελεσματικότητα της διαχείρισης του δικτύου.

Μέσα από το πραγματικό παράδειγμα και το υποθετικό σενάριο, αυτό το κεφάλαιο θα αναδείξει πώς η πλατφόρμα “nimble” μπορεί να αποτελέσει ένα απαραίτητο εργαλείο για τη μοντερνοποίηση και τη βελτίωση των δικτύων των επιχειρήσεων.

4.2 Προφίλ Εικονικής Εταιρίας

Το προφίλ της υποθετικής εταιρίας που θα εξετάσουμε είναι εκείνο μιας εταιρίας με κεντρικά γραφεία (*headquarters*) και ένα εκτεταμένο δίκτυο υποκαταστημάτων (*branches*) που εκτείνονται σε όλη την επικράτεια της Ελλάδας. Η εταιρία δραστηριοποιείται σε έναν τομέα που απαιτεί συχνές επεμβάσεις στο δίκτυο και υπόκειται σε ειδικούς κανονισμούς του κράτους..

Το NOC της εταιρίας είναι υπεύθυνο για την εύρυθμη και συνεχή λειτουργία της δικτυακής υποδομής και των υπηρεσιών που εξαρτώνται από εκείνη. Οι *network administrators* του NOC καλούνται συχνά να προβαίνουν σε αλλαγές σε ένα μεγάλης κλίμακας δίκτυο για να ανταποκριθούν σε απαιτήσεις της εταιρίας ή να συμμορφωθούν με τους ειδικούς κανονισμούς.

Επιπλέον, η εταιρία βρίσκεται σε μια φάση έντονης ανάπτυξης και πραγματοποιεί συνεχείς και μαζικές εξαγορές μικρότερων επιχειρήσεων. Αυτό σημαίνει ότι οι *network administrators* πρέπει να είναι έτοιμοι να ενσωματώνουν νέα μικρότερα δίκτυα στην υπάρχουσα υποδομή και να αντιμετωπίζουν τις προκλήσεις της ενοποίησης δικτύων. Αυτό απαιτεί ευελιξία, αυξημένη απόδοση και ασφάλεια στη διαχείριση του δικτύου, καθώς και την ταχύτητα και την αποτελεσματικότητα στην εφαρμογή αλλαγών.

Η εταιρία, αντιμετωπίζοντας αυξημένες ανάγκες σε εργασίες που αφορούν το τμήμα NOC, αποφάσισε να προσλάβει νέους μηχανικούς πληροφορικής. Παρά την προσθήκη προσωπικού, το NOC συνεχίζει να αντιμετωπίζει προβλήματα με τους χρόνους παράδοσης των έργων και την αύξηση των σφαλμάτων λόγω του αυξημένου φόρτου εργασίας. Οι νέοι μηχανικοί πληροφορικής δεν είναι επαρκώς εκπαιδευμένοι λόγω έλλειψης χρόνου του προσωπικού για εκπαίδευση.

Επομένως, ο διευθυντής του τμήματος NOC ανέλαβε να εξετάσει εναλλακτικές λύσεις για την αποτελεσματική διαχείριση του δικτύου. Έπειτα από έρευνα, ανακάλυψε την πλατφόρμα “nimble” και αποφάσισε να την εγκαταστήσει στην υποδομή των κεντρικών γραφείων της εταιρίας. Οι λόγοι που τον οδήγησαν σε αυτήν την απόφαση είναι πολλαπλοί. Καταρχάς, η πλατφόρμα “nimble” προσφέρει εύκολη χρήση και αυτοματοποίηση εργασιών, ενώ ταυτόχρονα βελτιώνει την απόδοση και την αποτελεσματικότητα της διαχείρισης του δικτύου. Επιπλέον, η πλατφόρμα μπορεί να προσαρμοστεί

αποτελεσματικά στις ανάγκες της επιχείρησης, παρέχοντας λύσεις που ανταποκρίνονται στις ειδικές απαιτήσεις τους.

Η εγκατάσταση της πλατφόρμας “nimble” αναμένεται να επιφέρει σημαντικά οφέλη στην εταιρία, αποτελώντας ένα σημαντικό βήμα προς την επίλυση των προβλημάτων που αντιμετωπίζει το τμήμα NOC. Η επιλογή της “nimble” αντιπροσωπεύει μια σύγχρονη και ολοκληρωμένη προσέγγιση στη διαχείριση του δικτύου, ενισχύοντας την ικανότητα της εταιρίας να ανταποκρίνεται στις σύγχρονες απαιτήσεις της ψηφιακής εποχής.

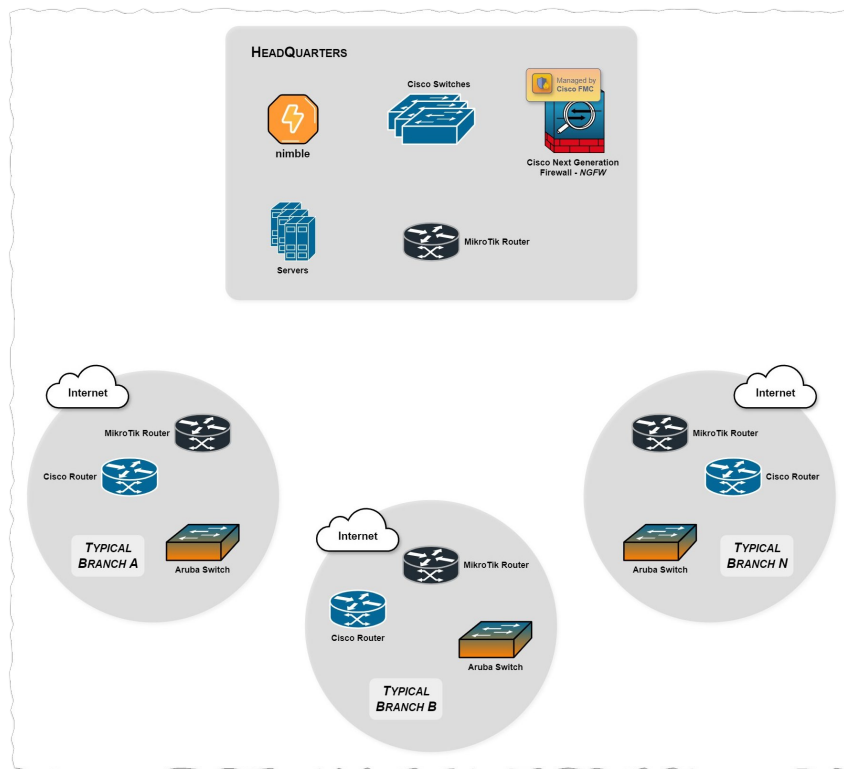
4.3 Εξοπλισμός και Τοπολογία

Στα κεντρικά γραφεία, ο δικτυακός εξοπλισμός περιλαμβάνει μια ποικιλία από συσκευές. Πιο συγκεκριμένα, χρησιμοποιούνται:

- Cisco Switches
- Cisco Next-Generation Firewall (*NGFW*)
- Firepower Management Center virtual (*FMCv*)
- MikroTik Router
- MikroTik Access Points
- Servers

Σε κάθε τυπικό υποκατάστημα, βρίσκουμε:

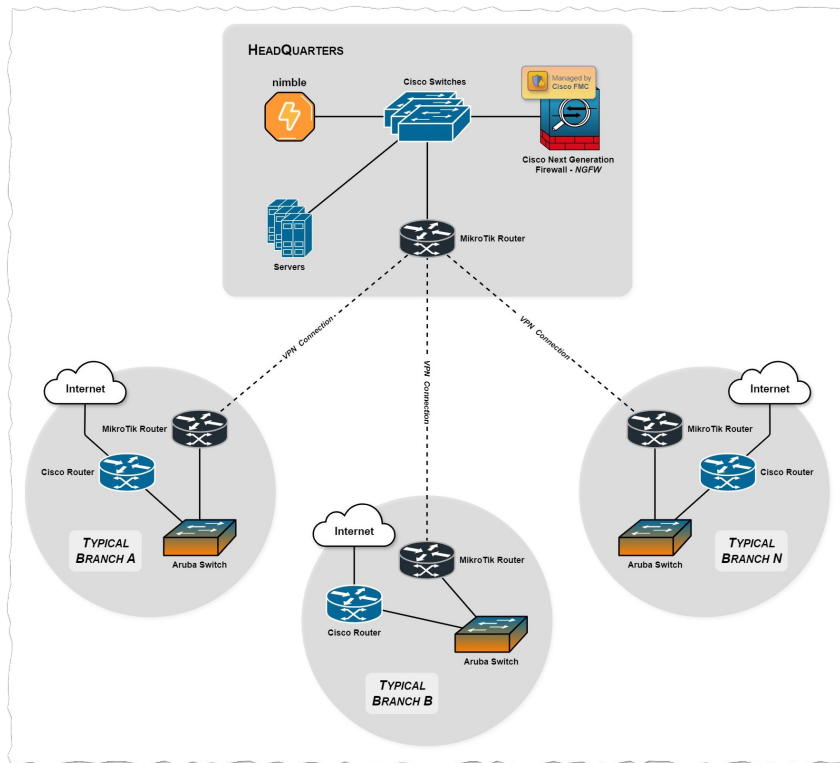
- Cisco Router
- MikroTik Router
- MikroTik Access Point
- Aruba Switch



Σχήμα 4.1 Συσκευές τοπολογίας υποκαταστημάτων

Στα κεντρικά γραφεία τα Cisco Switches χρησιμοποιούνται για την πρόσβαση των χρηστών στο δίκτυο και για τη διασύνδεση των συστημάτων μεταξύ τους. Το Cisco Next-Generation Firewall (NGFW) το οποίο διαχειρίζεται ένα FMCv έχει το ρόλο της περιφερειακής προστασίας του δικτύου και τη διαχείριση της πρόσβασης μεταξύ των διαφόρων υποδικτύων. Ο MikroTik Router αναλαμβάνει τη διασύνδεση μεταξύ των κεντρικών γραφείων και των υποκαταστημάτων μέσω Virtual Private Network (VPN). Τα MikroTik Access Points προσφέρουν ασύρματη πρόσβαση στο δίκτυο. Τέλος, οι servers προσφέρουν ποικίλες υπηρεσίες στους χρήστες και τα υποσυστήματα των κεντρικών γραφείων, καθώς και στους απομακρυσμένους χρήστες και συστήματα των υποκαταστημάτων.

Σε κάθε τυπικό υποκατάστημα, ο Cisco Router είναι υπεύθυνος για τη δρομολόγηση μεταξύ των υποδικτύων και για την πρόσβαση στο διαδίκτυο, ο MikroTik Router για τη διασύνδεση με τα κεντρικά γραφεία μέσω VPN, τα MikroTik Access Point προσφέρει ασύρματη πρόσβαση στο δίκτυο, και το Aruba Switch για τη διασύνδεση των συστημάτων του υποκαταστήματος.



Σχήμα 4.2 Τοπολογία υποκαταστημάτων

4.4 Σενάριο Χρήσης της “nimble”

Σε αυτήν την υποενότητα θα εξετάσουμε σενάριο χρήσης που αναδεικνύει τις δυνατότητες της πλατφόρμας. Ανεξάρτητα από το σενάριο, το πρώτο βήμα είναι να αποκτήσουμε πρόσβαση στην σελίδα WEB της εφαρμογής. Για να το επιτύχουμε αυτό, πρέπει να έχουμε πρόσβαση στον υπολογιστή (*host*) που φιλοξενεί το django project (“nimble”) μας. Στην περίπτωση μας, αυτός ο υπολογιστής είναι μια εικονική μηχανή (*VM*) με λειτουργικό σύστημα GNU/Linux (*Debian*). Αφού αποκτήσουμε πρόσβαση στον host μέσω της γραμμής εντολών (*CLI*) και πλοηγηθούμε στον κατάλογο που φιλοξενεί την πλατφόρμα “nimble”, αρκεί να ενεργοποιήσουμε το περιβάλλον εκτέλεσης Python (*Python virtual environment - venv*). Στη συνέχεια, με την κατάλληλη εντολή, εκτελούμε την “nimble” στη θύρα TCP 8000.

```

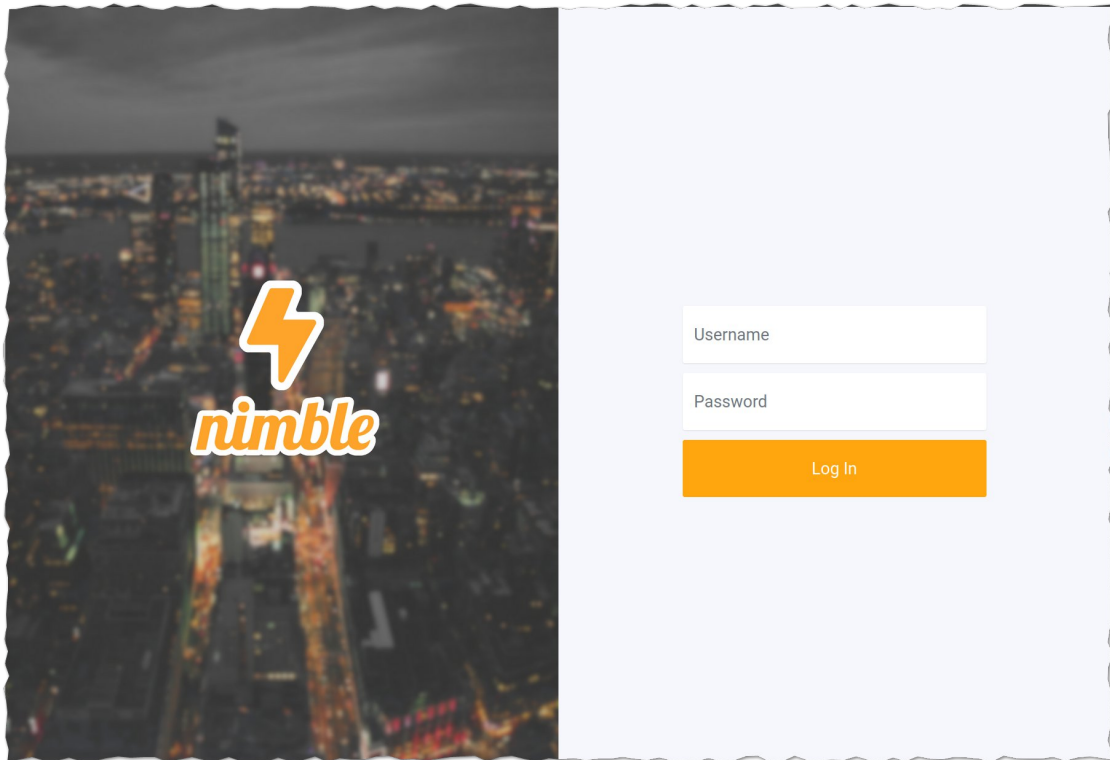
mais@greta:~/django/nimble_new_170423$
mais@greta:~/django/Nimble_new_170423$
mais@greta:~/django/Nimble_new_170423$ source venv/bin/activate
(venv) mais@greta:~/django/Nimble_new_170423$ nimble
Watching for file changes with StatReloader
Performing system checks...

System check identified no issues (0 silenced).
May 21, 2024 - 20:10:52
Django version 4.1.4, using settings 'nimble.settings'
Starting development server at http://0.0.0.0:8000/
Quit the server with CONTROL-C.

```

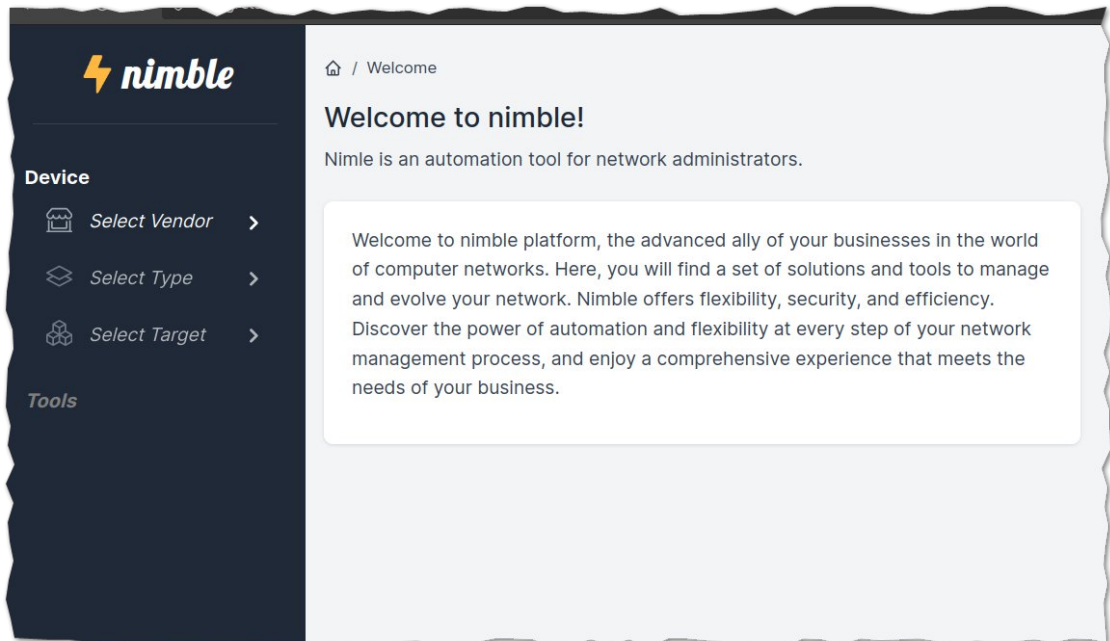
Σχήμα 4.3 VM που φιλοξενεί την πλατφόρμα

Από έναν τερματικό υπολογιστή, αρκεί να πλοηγηθούμε στο αντίστοιχο URL μέσω ενός περιηγητή (*browser*). Εκεί θα μας υποδεχτεί η σελίδα σύνδεσης (*login page*) της πλατφόρμας.



Σχήμα 4.4 Είσοδος στην πλατφόρμα

Χρησιμοποιώντας τα διαπιστευτήριά μας, αποκτούμε πρόσβαση στην πλατφόρμα, και οδηγούμαστε στην σελίδα καλωσορίσματος.

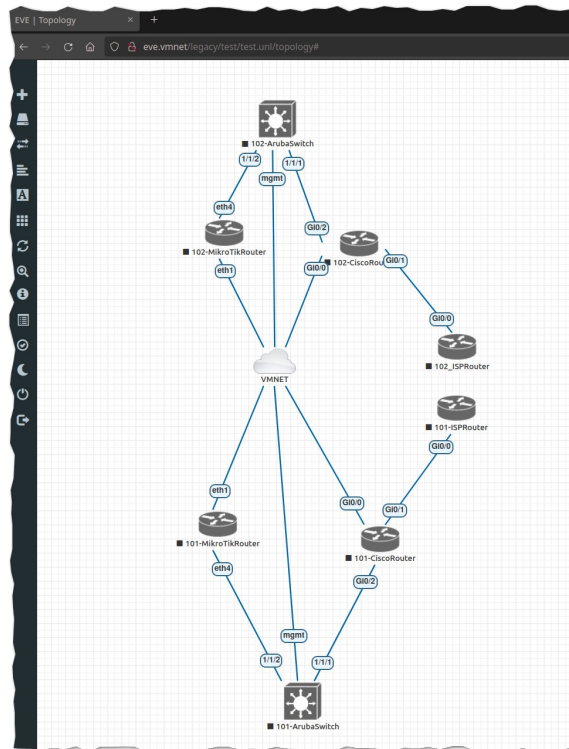


Σχήμα 4.5 Υποδοχή χρήστη από την πλατφόρμα

Στη συνέχεια, ανάλογα με τις ανάγκες κάθε σεναρίου, πλοηγούμαστε μέσω του κύριου μενού στα αντίστοιχα εργαλεία.

Κεφάλαιο 4

Για τις ανάγκες της παρούσας διατριβής, εγκαταστάθηκε το Cisco FMCv σε υποδομή εικονικοποίησης (*virtualization*), ενώ χρησιμοποιήθηκε το εργαλείο EVE-NG για την προσομοίωση των δικτυακών συσκευών των υποκαταστημάτων.



Σχήμα 4.6 Τοπολογία EVE-NG

Για τα κεντρικά γραφεία, έχουν οριστεί τα ακόλουθα IP υποδίκτυα (*IP subnets*) και VLANs:

- το υποδίκτυο **192.168.100.0/24** αντιστοιχεί στο **VLAN 100** και χρησιμοποιείται για την δικτύωση των server, ενώ
- το υποδίκτυο **192.168.50.0/24** αντιστοιχεί στο **VLAN 50** και χρησιμοποιείται για τους χρήστες του δικτύου.

Για τα υποκαταστήματα, έχει εφαρμοστεί subnetting στον private class A network (*RFC1918 [29]*) 10.0.0.0/8.

Λόγω της μεγάλης κλίμακας του δικτύου, έχουν εφαρμοστεί κάποιες συμβάσεις, ώστε να είναι ευκολότερα διαχειρίσιμο. Οι συμβάσεις αυτές περιλαμβάνουν:

- Σε κάθε υποκατάστημα αντιστοιχεί σε ένα τριψήφιο ID από το 101 έως το 999.
- Το υποδίκτυο κάθε υποκαταστήματος ακολουθεί τη μορφή 10.XY.Z.0/24, όπου XYZ είναι το τριψήφιο ID του υποκαταστήματος.
- Το υποδίκτυο κάθε υποκαταστήματος έχει διασπαστεί περαιτέρω σε δύο /25 υποδίκτυα (10.XY.Z.0/25 και 10.XY.Z.128/25), με το δεύτερο να είναι ελεύθερο για μελλοντικές επεκτάσεις
- Ο Cisco router κάθε υποκαταστήματος χρησιμοποιεί πάντα την πρώτη διαθέσιμη IP διεύθυνση του αντίστοιχου υποδικτύου (10.XY.Z.1/25).

- Το Aruba switch κάθε υποκαταστήματος χρησιμοποιεί πάντα τη δεύτερη διαθέσιμη IP διεύθυνση του αντίστοιχου υποδικτύου (10.XY.Z.2/25).
- Ο MikroTik router κάθε υποκαταστήματος χρησιμοποιεί πάντα την τελευταία διαθέσιμη IP διεύθυνση του αντίστοιχου υποδικτύου (10.XY.Z.126/25).

Store ID	Subnet
101	10.10.1.0/24
102	10.10.2.0/24
XYZ	10.XY.Z.0/24

Πίνακας 4.1 Υποδίκτυα καταστημάτων

Device	IP Address
Cisco Router	10.XY.Z.1/25
Aruba Switch	10.XY.Z.2/25
MikroTik Router	10.XY.Z.126/25

Πίνακας 4.2 Διευθύνσεις IP συσκευών

Με αυτόν τον τρόπο, επιτυγχάνεται μια οργανωμένη και εύκολη στη διαχείριση δομή του δικτύου, παρέχοντας την αναγκαία ευελιξία και αποδοτικότητα για την εταιρία.

4.4.1 Σενάριο A – Εγκατάσταση Συστημάτων Ασφαλείας

Στο πλαίσιο της συνεχούς δέσμευσης για τη διασφάλιση της ασφάλειας και της προστασίας των πελατών και του περιβάλλοντος των υποκαταστημάτων, αναδείχθηκε η ανάγκη για την εγκατάσταση συστημάτων ασφαλείας σε όλα τα υποκαταστήματα. Μετά από προσεκτική μελέτη και συνεργασία με εξειδικευμένη εταιρία, εγκαταστάθηκε ένα σύστημα καταγραφής DVR στα κεντρικά γραφεία και αποφασίστηκε η εγκατάσταση τριών (3) καμερών σε κάθε υποκατάστημα. Επιπλέον, θα πραγματοποιηθεί και η εγκατάσταση ενός συστήματος συναγερμού σε κάθε υποκατάστημα, ενισχύοντας την ασφάλεια και την προστασία των υποκαταστημάτων.

Μετά τη λήψη των παραπάνω αποφάσεων, το NOC ανέλαβε την εκπόνηση μιας λεπτομερούς μελέτης για τον προσδιορισμό του πλάνου εγκατάστασης. Η μελέτη αυτή κατέληξε στον καθορισμό των ακόλουθων επιμέρους στοιχείων:

1. Διευθυνσιοδότηση:

Απόδοση διευθύνσεων IP για τις κάμερες και το σύστημα συναγερμού σε κάθε υποκατάστημα, ώστε να διασφαλιστεί η απρόσκοπτη λειτουργία και η αποτελεσματική διαχείριση τους.

2. Ονοματοδοσία:

Απόδοση ονομάτων για τις κάμερες και το σύστημα συναγερμού σε κάθε υποκατάστημα, ώστε να διασφαλιστεί ο μοναδικός προσδιορισμός τους, η ευκολότερη αναγνώριση τους και η αποτελεσματική διαχείριση τους.

3. Σύνδεση νέου εξοπλισμού στο δίκτυο:

Προσδιορισμός των θέσεων μέσω των οποίων θα γίνει η ενσωμάτωση των καμερών και του συστήματος συναγερμού στο υπάρχον δίκτυο κάθε υποκαταστήματος, διασφαλίζοντας τη συμβατότητα και τη σταθερή λειτουργία τους.

4. Διαχείριση Πρόσβασης:

Καθορισμός κανόνων πρόσβασης, προκειμένου να διασφαλιστεί η προστασία των συστημάτων ασφαλείας από ανεπιθύμητη παρέμβαση.

5. Απαιτούμενες Εντολές και Ενέργειες:

Ανάπτυξη ενός συνόλου εντολών και ενεργειών για την εγκατάσταση, τη ρύθμιση και την επικοινωνία των συστημάτων ασφαλείας.

Με αυτόν τον τρόπο, επιτυγχάνεται η ολοκληρωμένη εγκατάσταση συστημάτων ασφαλείας σε όλα τα υποκαταστήματα, ενισχύοντας έτσι την ασφάλεια, την προστασία και τη διαχειριστική αποτελεσματικότητα της εταιρίας.

4.4.1.1 Διευθυνσιοδότηση

Η διευθυνσιοδότηση αποτελεί ένα κρίσιμο στάδιο στη διαδικασία εγκατάστασης των συστημάτων ασφαλείας σε κάθε υποκατάστημα. Η ορθή ανάθεση διευθύνσεων IP εξασφαλίζει τη σταθερή λειτουργία των συστημάτων και τη συμβατότητά τους με το υπάρχον δίκτυο, ενώ παράλληλα διασφαλίζει την ομοιομορφία στη διαχείριση των διευθύνσεων.

Στο πλαίσιο της εγκατάστασης τριών (3) καμερών, και ενός (1) συστήματος συναγερμού σε κάθε υποκατάστημα αναγνωρίζεται η ανάγκη για ανάθεση τεσσάρων (4) ελεύθερων διευθύνσεων IP για κάθε υποκατάστημα.

Μετά από προσεκτική μελέτη το τμήμα NOC, καθόρισε το ελεύθερο subnet 10.XY.Z.128/25 για τα νέα συστήματα ασφαλείας σε κάθε υποκατάστημα. Καθόρισε το εύρος διευθύνσεων 10.XY.Z.241-10.XY.Z.243 για τις κάμερες, ενώ η διεύθυνση 10.XY.Z.245 αποδόθηκε στο σύστημα συναγερμού. Αυτές οι αποφάσεις είναι αποτέλεσμα επιμελούς ανάλυσης και εξασφαλίζουν τη σταθερή λειτουργία και την ασφάλεια των συστημάτων ασφαλείας σε κάθε υποκατάστημα.

Device	IP Address
Camera 1	10.XY.Z.241/25
Camera 2	10.XY.Z.242/25
Camera 3	10.XY.Z.243/25
Alarm	10.XY.Z.245/25

Πίνακας 4.3 Διευθύνσεις IP νέων συστ. ασφαλείας

4.4.1.2 Ονοματοδοσία

Η ονοματοδοσία αναφέρεται στον καθορισμό ονομάτων για κάθε συσκευή του νέου συστήματος ασφαλείας, με σκοπό την ομοιομορφία, την ευκολότερη αναγνώριση τους και την αποτελεσματική διαχείρισή τους. Η ορθή ονοματοδοσία είναι κρίσιμη για τη διασφάλιση της διαφάνειας και της ευκολίας στην αναγνώριση των συσκευών σε ένα δίκτυο.

Στη συγκεκριμένη περίπτωση, τα συστήματα ασφαλείας αποτελούνται από τρεις (3) κάμερες και ένα (1) σύστημα συναγερμού ανά υποκατάστημα. Η ανάθεση ονομάτων στις συσκευές αυτές γίνεται με γνώμονα την ευκολότερη αναγνώριση και διαχείριση τους.

Μετά από αντίστοιχη μελέτη, το τμήμα NOC αποφάσισε να αποδώσει τα παρακάτω ονόματα:

- Για κάθε κάμερα: <storeID>_CAM<cameraID>
- Για κάθε σύστημα συναγερμού: <storeID>_ALARM

Με αυτόν τον τρόπο, κάθε συσκευή ασφαλείας συνοδεύεται από ένα μοναδικό όνομα που περιλαμβάνει τον κωδικό του υποκαταστήματος και το device-id, διευκολύνοντας έτσι την αναγνώριση και τη διαχείρισή τους.

4.4.1.3 Σύνδεση νέου εξοπλισμού στο δίκτυο

Η σύνδεση του νέου εξοπλισμού στο δίκτυο αποτελεί σημαντικό βήμα για την ομαλή λειτουργία των συστημάτων ασφαλείας σε κάθε υποκατάστημα. Κατά τον καθορισμό των θυρών είναι απαραίτητο να ληφθεί υπόψη η ομοιομορφία και η συμβατότητα με το υπάρχον δίκτυο.

Στην προκειμένη περίπτωση, η σύνδεση των νέων συστημάτων ασφαλείας απαιτεί την δημιουργία ενός νέου VLAN στα υποκαταστήματα και την ανάθεση πέντε (4) ελεύθερων θυρών Ethernet στο Aruba Switch κάθε υποκαταστήματος. Συγκεκριμένα, μία θύρα αντιστοιχεί σε κάθε ένα από τα ακόλουθα συστήματα: τρεις (3) κάμερες και ένας (1) συναγερμός.

Μετά από λεπτομερή ανάλυση το τμήμα NOC, αποφάσισε τη χρήση του νέου VLAN με ID 128 και καθόρισε το εύρος θυρών 3-5 για τις κάμερες. Επιπλέον, προέβλεψε την ανάθεση της θύρας 6 αποδόθηκε στο σύστημα συναγερμού. Αυτές οι αποφάσεις είναι αποτέλεσμα εμπειριστάτων ανάλυσης και εξασφαλίζουν την απρόσκοπτη σύνδεση και λειτουργία των συστημάτων ασφαλείας σε κάθε υποκατάστημα.

4.4.1.4 Διαχείριση Πρόσβασης

Η διαχείριση της πρόσβασης αποτελεί κρίσιμο στάδιο για την ασφάλεια και την απρόσκοπτη λειτουργία των συστημάτων ασφαλείας. Σε κάθε περίπτωση, η αναγνώριση των αναγκών σε πρόσβαση είναι καθοριστική για την επίτευξη της ισορροπίας μεταξύ ασφάλειας και λειτουργικότητας. Με γνώμονα την ασφάλεια, ο περιορισμός των προσβάσεων σημαίνει ότι τα νέα συστήματα θα έχουν πρόσβαση μόνο σε συγκεκριμένους πόρους που είναι απαραίτητοι για την εκτέλεση των καθηκόντων τους.

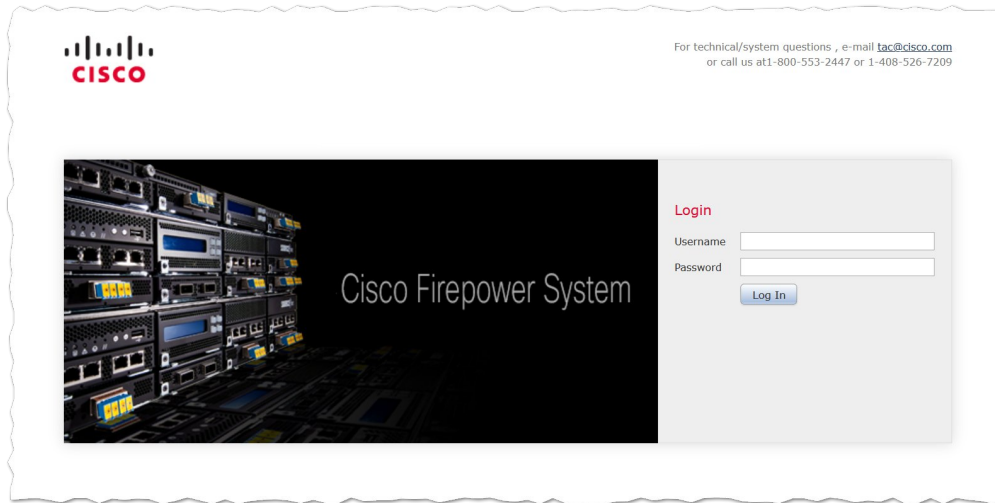
Στη συγκεκριμένη περίπτωση, από τα νέα συστήματα ασφαλείας σε κάθε υποκατάστημα οι κάμερες απαιτούν την επικοινωνία με τα κεντρικά γραφεία, και το DVR, ενώ το σύστημα συναγερμού απαιτεί μόνον πρόσβαση στο διαδίκτυο. Συνεπώς, ο περιορισμός των προσβάσεων επιδιώκει την διασφάλιση ότι τα συστήματα θα έχουν πρόσβαση μόνο σε συγκεκριμένους πόρους και υπηρεσίες. Με αυτό τον τρόπο, επιτυγχάνεται η ισορροπία μεταξύ της απαιτούμενης πρόσβασης και της ασφάλειας του δικτύου.

4.4.1.5 Απαιτούμενες Εντολές και Ενέργειες

Η διαδικασία των απαιτούμενων εντολών και ενεργειών αποτελεί βασικό βήμα για την εφαρμογή των νέων απαιτήσεων στο δίκτυο. Στόχος είναι να εφαρμοστούν οι αλλαγές με τον πιο αποτελεσματικό και ασφαλή τρόπο, ενώ διατηρείται η ομοιομορφία και ελαχιστοποιείται ο κίνδυνος πιθανών παρεμβάσεων.

Στο Cisco FMCν των κεντρικών γραφείων, η πρώτη ενέργεια αφορά τον ορισμό των νέων συστημάτων ασφαλείας, λαμβάνοντας υπόψη τη διευθυνσιοδότηση και την ονοματοδοσία που έχουν οριστεί. Έπειτα,

ακολουθεί ο κατάλληλος περιορισμός της πρόσβασης των συστημάτων σύμφωνα με τις νέες απαιτήσεις ασφαλείας.



Σχήμα 4.7 Cisco FMC

Στον Cisco router κάθε υποκαταστήματος, απαιτείται η δημιουργία ενός νέου layer-3 interface ώστε να καταστεί δυνατή η οποιαδήποτε επικοινωνία των νέων συστημάτων, καθώς και η εφαρμογή των πολιτικών περιορισμού πρόσβασης των νέων συστημάτων στο διαδίκτυο. Αυτό εξασφαλίζει ότι μόνον τα εξουσιοδοτημένα συστήματα έχουν πρόσβαση στο διαδίκτυο και διατηρεί την ασφάλεια του δικτύου.

```
1 config t
2
3 ip access-list extended 128
4 remark allow cameras to DVR
5 permit tcp host 10.XY.Z.241 host 192.168.100.249 eq 443
6 permit tcp host 10.XY.Z.242 host 192.168.100.249 eq 443
7 permit tcp host 10.XY.Z.243 host 192.168.100.249 eq 443
8 remark deny cameras to everything else
9 deny ip host 10.XY.Z.241 any
10 deny ip host 10.XY.Z.242 any
11 deny ip host 10.XY.Z.243 any
12 remark deny alarm to private
13 deny ip host 10.XY.Z.245 10.0.0.0 0.255.255.255
14 deny ip host 10.XY.Z.245 172.16.0.0 0.15.255.255
15 deny ip host 10.XY.Z.245 192.168.0.0 0.0.255.255
16 remark allow alarm to Internet
17 permit ip host 10.XY.Z.245 any
18 exit
19
20 inter g0/2.128
21 encapsulation dot1q 128
22 ip address 10.XY.Z.129 255.255.255.128
23 description ### Security ###
24 ip access-group 128 in
25 exit
26
27 exit
28
29 wr mem
```

Σχήμα 4.8 Εντολές για Cisco router καταστημάτων

Στο Aruba switch κάθε υποκαταστήματος, οι ενέργειες περιλαμβάνουν τη δημιουργία νέου VLAN και την παραμετροποίηση των θυρών που θα συνδεθεί ο νέος εξοπλισμός. Αυτό διασφαλίζει ότι ο νέος εξοπλισμός είναι σωστά ενσωματωμένος στο δίκτυο και μπορεί να λειτουργήσει σύμφωνα με τις απαιτήσεις ασφαλείας.

```

1 config t
2
3 vlan 128
4 name Security
5 exit
6
7 interface 1/1/1
8 vlan trunk native 1
9 vlan trunk allowed 1,128
10
11 inter 1/1/3
12 no shut
13 vlan access 128
14 description ### CAM-1 ###
15
16 inter 1/1/4
17 no shut
18 vlan access 128
19 description ### CAM-2 ###
20
21 inter 1/1/5
22 no shut
23 vlan access 128
24 description ### CAM-3 ###
25
26 inter 1/1/6
27 no shut
28 vlan access 128
29 description ### ALARM ###
30 exit
31
32 exit
33
34 wr mem

```

Σχήμα 4.9 Εντολές για Aruba switchr καταστημάτων

4.4.1.6 Εκτέλεση

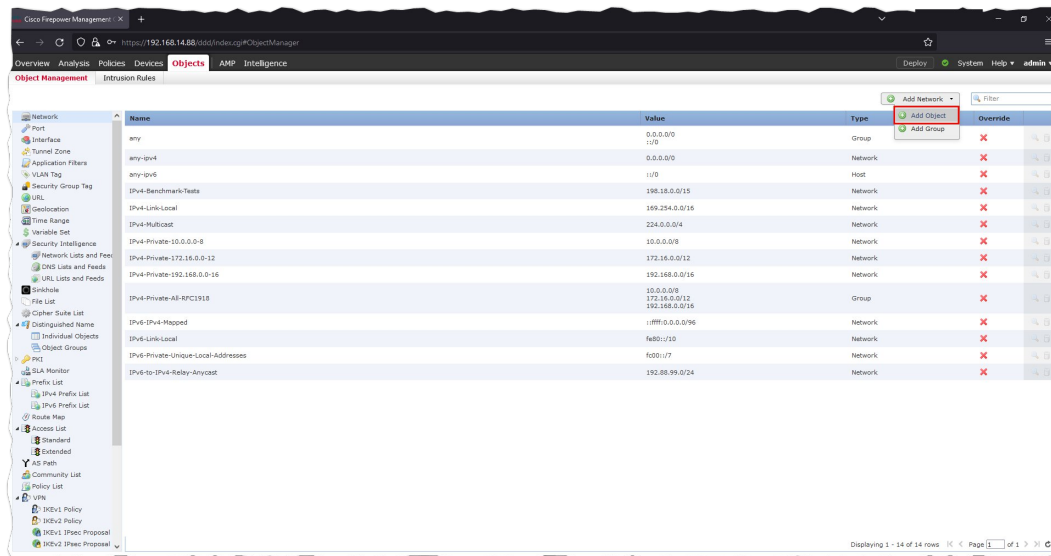
Αφού έχουν ολοκληρωθεί οι φάσεις της μελέτης και του σχεδιασμού η διαδικασία προχωρά στην φάση της εκτέλεσης. Στο πλαίσιο αυτό, αρχικά θα γίνει ανάλυση των ενεργειών που απαιτούνται χωρίς τη χρήση των εργαλείων της πλατφόρμας “nimble”, ενώ έπειτα θα εξεταστούν οι ενέργειες με τη χρήση της πλατφόρμας και των εργαλείων που διαθέτει, δίνοντας έμφαση στους μειωμένους απαιτούμενους χρόνους.

4.4.1.6.1 Εκτέλεση χωρίς το nimble

Σε περίπτωση που οι μηχανικοί του NOC δεν είχαν στη διάθεσή τους την πλατφόρμα “nimble”, θα έπρεπε να προβούν σε συγκεκριμένες επαναλαμβανόμενες χειροκίνητες ενέργειες για την ενσωμάτωση των νέων συστημάτων ασφαλείας.

Καταρχάς, ο υπεύθυνος μηχανικός χρειάζεται να συνδεθεί στο Cisco FMC και να δημιουργήσει τέσσερα (4) νέα object για κάθε ένα από τα υπάρχοντα καταστήματα. Αυτά τα object περιλαμβάνουν πληροφορίες όπως διευθύνσεις IP, περιγραφές και ονόματα συσκευών για τις κάμερες και το σύστημα συναγερμού του κάθε καταστήματος. Για μόλις 100 υποκαταστήματα, ο μηχανικός καλείται να δημιουργήσει 400 object, μια διαδικασίας η οποία εκτός από χρονοβόρα, απαιτεί μεγάλη προσοχή για την αποφυγή λαθών.

Κεφάλαιο 4

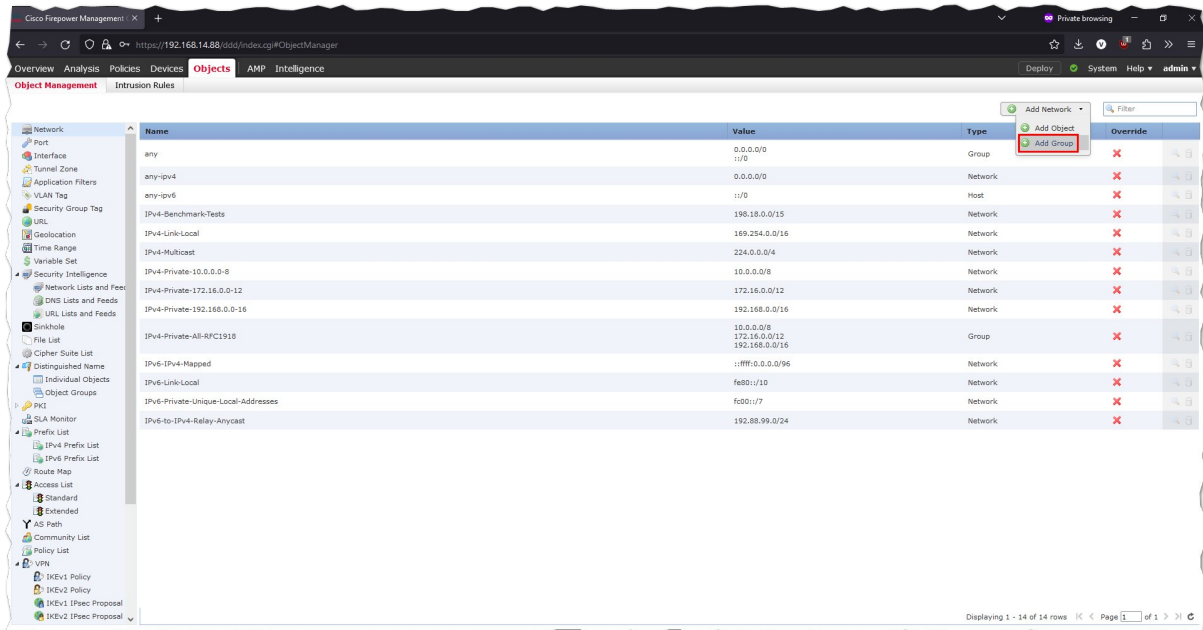


Σχήμα 4.10 Επιλογή προσθήκης νέου object στο FMC

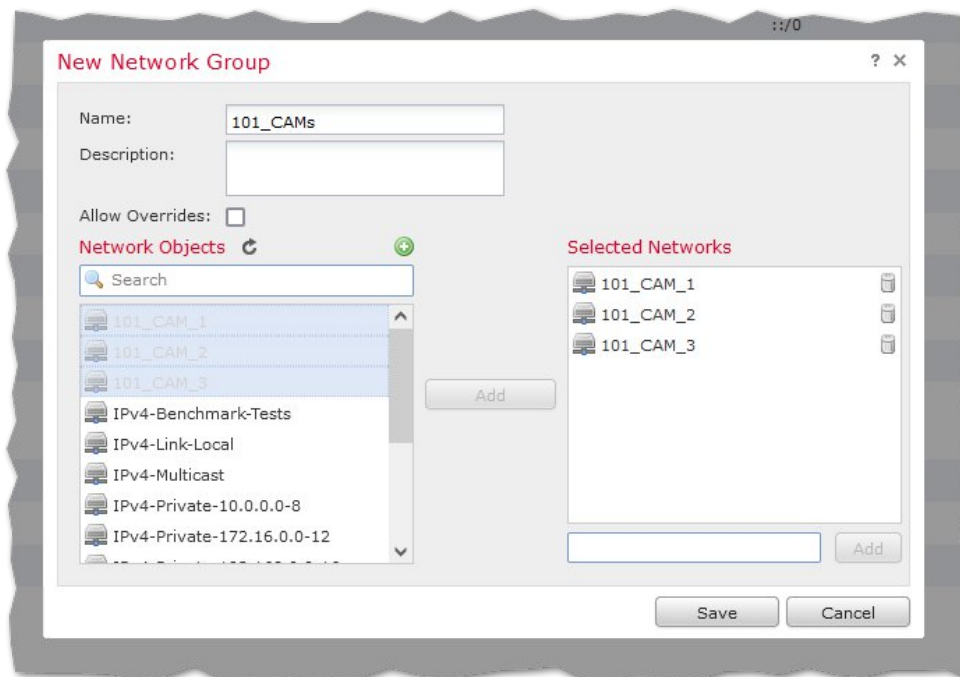


Σχήμα 4.11 Προσθήκη νέου object στο FMC

Έπειτα, ο μηχανικός θα πρέπει να ομαδοποιήσει αυτά τα object σε object group ανά κατάσταση. Αυτή η ομαδοποίηση θα επιτρέψει την οργάνωση των συσκευών σε λογικές ομάδες με βάση τη φυσική τους τοποθέτηση και λειτουργικότητα. Ο μηχανικός επίσης θα πρέπει να ομαδοποιήσει όλες αυτές τις ομάδες σε μία γενική ομάδα που θα συγκεντρώνει το σύνολο των νέων συστημάτων σε μορφή object και object group. Αυτή η τελική ομαδοποίηση θα διευκολύνει τη διαχείριση της πρόσβασης μέσω του αντίστοιχου Access Control Policy (ACP), διατηρώντας τους κανόνες που το απαρτίζουν όσο τον δυνατό λιγότερος σε πλήθος, επιτρέποντας την εφαρμογή ομαδικών περιορισμών πρόσβασης σε όλα τα νέα συστήματα ασφαλείας.



Σχήμα 4.12 Επιλογή προσθήκης νέου group στο FMC



Σχήμα 4.13 Προσθήκη object group στο FMC

Μετά την ολοκλήρωση των εργασιών στο Cisco FMC, ο υπεύθυνος μηχανικός θα πρέπει να προσαρμόσει τις εντολές που αφορούν τους Cisco router των καταστημάτων. Αυτές οι ενέργειες περιλαμβάνουν τη δημιουργία νέων layer-3 interfaces και την εφαρμογή των πολιτικών περιορισμών πρόσβασης των νέων συστημάτων ασφαλείας στο δίκτυο.

Για να επιτευχθεί αυτό, ο μηχανικός θα πρέπει να συνδεθεί σε κάθε Cisco router του κάθε υποκαταστήματος ξεχωριστά. Αφού συνδεθεί, θα εφαρμόσει τις αντίστοιχες εντολές που θα δημιουργήσουν τα απαραίτητα layer-3 interfaces για κάθε τα νέα συστήματα ασφαλείας. Κάθε εντολή

θα πρέπει να προσαρμοστεί με βάση τις συγκεκριμένες ανάγκες και παραμέτρους του κάθε υποκαταστήματος.

Μετά την ολοκλήρωση των προηγούμενων εργασιών, ο μηχανικός θα πρέπει αυτή τη φορά να προσαρμόσει τις εντολές που αφορούν τα Aruba switches των καταστημάτων. Αυτές οι ενέργειες απαιτούν τη δημιουργία του νέου VLAN που θα φιλοξενήσει τα νέα συστήματα ασφαλείας σε κάθε υποκατάστημα, καθώς επίσης και την κατάλληλη παραμετροποίηση των θυρών στις οποίες θα συνδεθεί ο νέος εξοπλισμός.

Για να επιτευχθεί αυτό, ο μηχανικός θα πρέπει να συνδεθεί σε κάθε Aruba switch του κάθε υποκαταστήματος ξεχωριστά. Αφού συνδεθεί, θα εφαρμόσει τις αντίστοιχες εντολές που θα δημιουργήσουν το νέο VLAN και θα παραμετροποιήσουν τις θύρες του switch για τη σύνδεση του νέου εξοπλισμού. Κάθε εντολή θα πρέπει να προσαρμοστεί με βάση τις συγκεκριμένες ανάγκες και προδιαγραφές του κάθε υποκαταστήματος.

Η παραπάνω ανάλυση αποκαλύπτει την χρονοβόρα φύση των ενεργειών που απαιτούνται για την ενσωμάτωση νέου εξοπλισμού στο δίκτυο, ακόμα και σε περιπτώσεις που μπορούν να θεωρηθούν απλές. Οι χειροκίνητες ενέργειες, που περιλαμβάνουν τη σύνδεση σε κάθε συσκευή ξεχωριστά και την εφαρμογή εντολών, απορροφούν αξιοσημείωτο μέρος του χρόνου των μηχανικών του NOC.

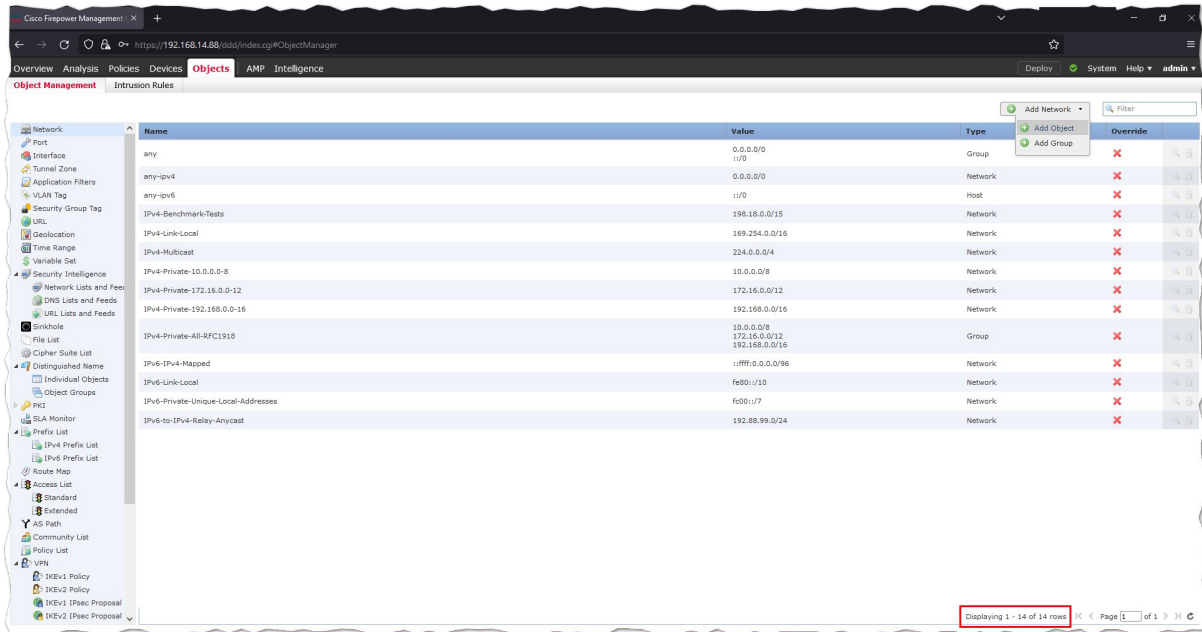
Η ανάγκη για επανάληψη αυτών των διαδικασιών σε κάθε υποκατάστημα αυξάνει τον φόρτο εργασίας και επιβαρύνει τους πόρους της εταιρίας. Οι μηχανικοί του NOC χρειάζονται συνεχή συμβολή, παρακολούθηση και επιτήρηση, ενώ η εξέλιξη των εργασιών απαιτεί αύξηση του προσωπικού ή την ανάπτυξη νέων, αποτελεσματικότερων διαδικασιών.

Για να αντιμετωπιστεί αυτή η πρόκληση, η εταιρία θα πρέπει να εξετάσει εναλλακτικές λύσεις όπως η χρήση αυτοματοποιημένων εργαλείων ή πλατφορμών, οι οποίες θα επιτρέπουν την εκτέλεση των εργασιών με μεγαλύτερη ταχύτητα και αποτελεσματικότητα, μειώνοντας τα κόστη και βελτιώνοντας την απόδοση και την ασφάλεια του δικτύου.

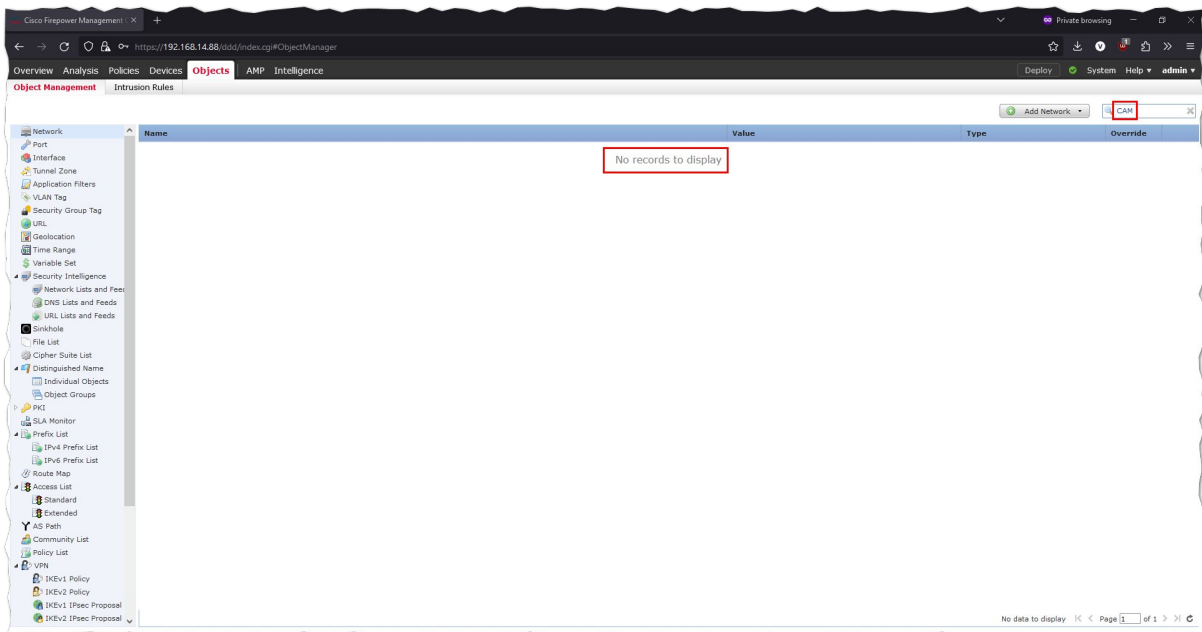
4.4.1.6.2 Εκτέλεση με το nimble

Η ενσωμάτωση των νέων συστημάτων ασφαλείας με τη χρήση της πλατφόρμας “nimble” καθιστά τη διαδικασία όχι μόνο πιο γρήγορη αλλά και πιο αποδοτική. Ας εξετάσουμε τις ενέργειες που θα εκτελέσουν οι μηχανικοί του NOC με τη βοήθεια της πλατφόρμας “nimble” και των εργαλείων που προσφέρει.

Προτού προχωρήσουμε σε παραμετροποιήσεις είναι χρήσιμο να επιβεβαιώσουμε την απουσία των απαιτούμενου configuration στο Cisco FMC, καθώς και στους Cisco router και Aruba switch. Όπως βλέπουμε στην παρακάτω εικόνα, το πλήθος των object ανέρχεται στα 14, και δεν υπάρχει κάποιο object με αναγνωριστικό αντίστοιχο της σύμβασης.



Σχήμα 4.14 Έλεγχος πλήθους object



Σχήμα 4.15 Έλεγχος απουσίας object

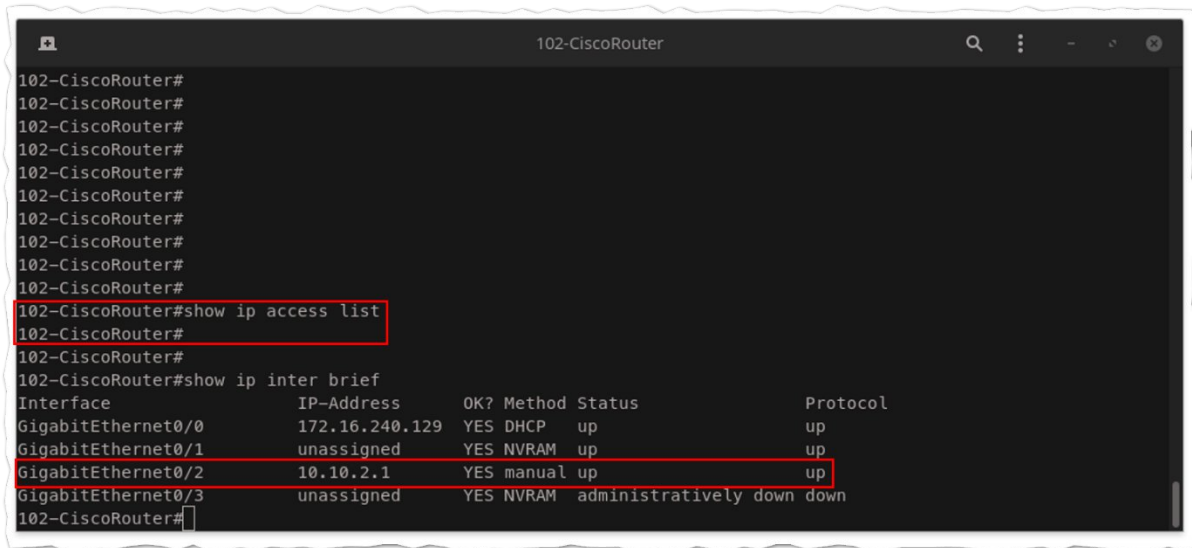
Κεφάλαιο 4

Έπειτα, επιβεβαιώνουμε ότι στους Cisco router απουσιάζουν τα subinterfaces, καθώς και οι ACL.



```
101-CiscoRouter#
101-CiscoRouter#
101-CiscoRouter#
101-CiscoRouter#
101-CiscoRouter#
101-CiscoRouter#
101-CiscoRouter#
101-CiscoRouter#
101-CiscoRouter#
101-CiscoRouter#
101-CiscoRouter#
101-CiscoRouter#
101-CiscoRouter#
101-CiscoRouter#show ip access-list
101-CiscoRouter#
101-CiscoRouter#show ip inter brief
Interface          IP-Address      OK? Method Status          Protocol
GigabitEthernet0/0 172.16.240.131 YES DHCP    up              up
GigabitEthernet0/1 unassigned      YES NVRAM    up              up
GigabitEthernet0/2 10.10.1.1       YES manual  up              up
GigabitEthernet0/3 unassigned      YES NVRAM   administratively down down
101-CiscoRouter#
```

Σχήμα 4.16 Έλεγχος απουσίας subinterface



```
102-CiscoRouter#
102-CiscoRouter#
102-CiscoRouter#
102-CiscoRouter#
102-CiscoRouter#
102-CiscoRouter#
102-CiscoRouter#
102-CiscoRouter#
102-CiscoRouter#
102-CiscoRouter#
102-CiscoRouter#
102-CiscoRouter#
102-CiscoRouter#
102-CiscoRouter#show ip access list
102-CiscoRouter#
102-CiscoRouter#
102-CiscoRouter#show ip inter brief
Interface          IP-Address      OK? Method Status          Protocol
GigabitEthernet0/0 172.16.240.129 YES DHCP    up              up
GigabitEthernet0/1 unassigned      YES NVRAM    up              up
GigabitEthernet0/2 10.10.2.1       YES manual  up              up
GigabitEthernet0/3 unassigned      YES NVRAM   administratively down down
102-CiscoRouter#
```

Σχήμα 4.17 Έλεγχος απουσίας subinterface

Τέλος, επιβεβαιώνουμε ότι στα Aruba switch απουσιάζουν το νέο VLAN και το configuration των interfaces 1/1/3-1/1/6 που πρόκειται να φιλοξενήσουν τον νέο εξοπλισμό.

```

101-ArubaSwitch#
101-ArubaSwitch#
101-ArubaSwitch#
101-ArubaSwitch# show vlan
-----
VLAN Name                Status Reason                Type    Interfaces
-----
1    DEFAULT_VLAN_1        up    ok                      default 1/1/1-1/1/6
101-ArubaSwitch#

101-ArubaSwitch# show inter brief
-----
Port      Native Mode  Type      Enabled Status Reason                Speed
          VLAN
-----
1/1/1     1     access --      yes    up
1/1/2     1     access --      yes    up
1/1/3     1     access --      no     down    Administratively down --
1/1/4     1     access --      no     down    Administratively down --
1/1/5     1     access --      no     down    Administratively down --
1/1/6     1     access --      no     down    Administratively down --
101-ArubaSwitch#

```

Σχήμα 4.18 Έλεγχος απουσίας switch configuration

```

102-ArubaSwitch#
102-ArubaSwitch#
102-ArubaSwitch#
102-ArubaSwitch#
102-ArubaSwitch#
102-ArubaSwitch#
102-ArubaSwitch# show vlan
-----
VLAN Name                Status Reason                Type    Interfaces
-----
1    DEFAULT_VLAN_1        up    ok                      default 1/1/1-1/1/6
102-ArubaSwitch# show inter brief
-----
Port      Native Mode  Type      Enabled Status Reason                Speed
          VLAN
-----
1/1/1     1     access --      yes    up
1/1/2     1     access --      yes    up
1/1/3     1     access --      no     down    Administratively down --
1/1/4     1     access --      no     down    Administratively down --
1/1/5     1     access --      no     down    Administratively down --
1/1/6     1     access --      no     down    Administratively down --
102-ArubaSwitch#

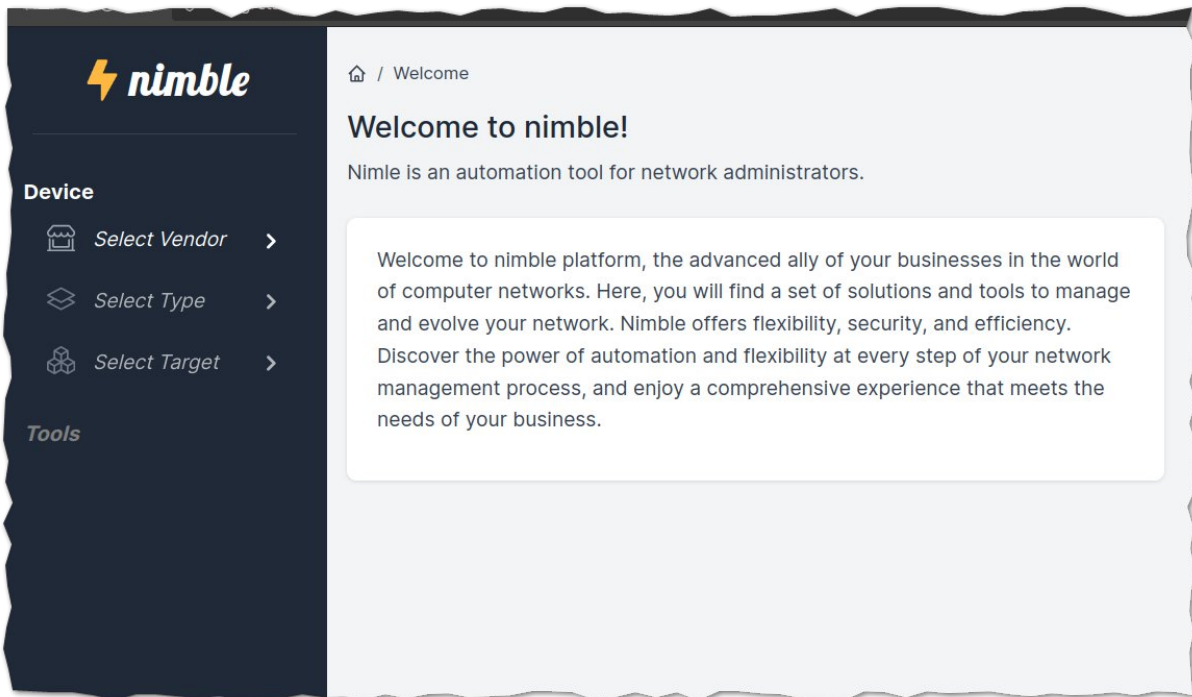
```

Σχήμα 4.19 Έλεγχος απουσίας switch configuration

4.4.1.6.2.1 Δημιουργία και Διαχείριση FMC Objects και Groups

- **Σύνδεση στην Πλατφόρμα nimble:**

Ο network administrator συνδέεται στην πλατφόρμα nimble και πλοηγείται στο βασικό μενού της εφαρμογής. Η πλατφόρμα “nimble” προσφέρει ένα ευέλικτο και εύχρηστο περιβάλλον εργασίας που διευκολύνει την πλοήγηση και την εκτέλεση σύνθετων εργασιών.



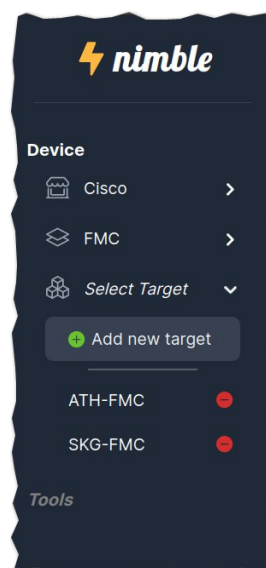
Σχήμα 4.20 Υποδοχή χρήστη από την πλατφόρμα

- **Δημιουργία Νέας Οντότητας (Target) τύπου Cisco FMC:**

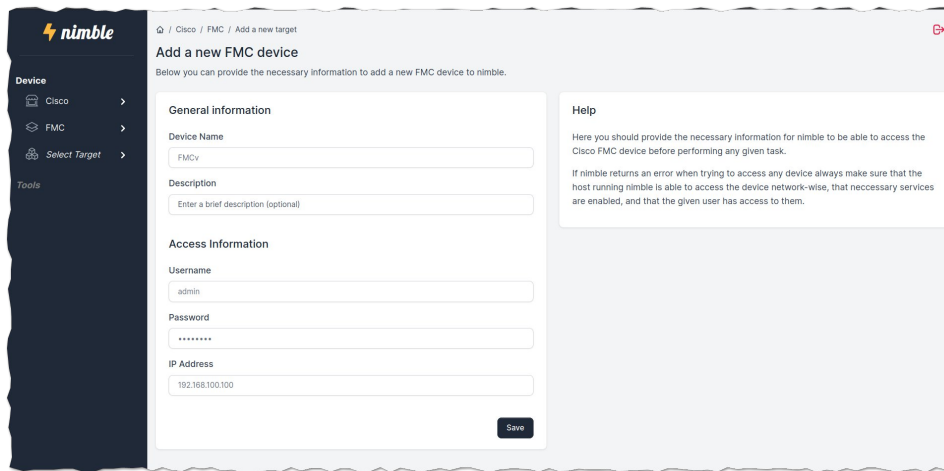
Μέσω του μενού της πλατφόρμας, ο διαχειριστής επιλέγει τη δημιουργία νέας οντότητας και ορίζει το νέο target ως τύπου FMC, συμπληρώνοντας τα παρακάτω στοιχεία:

- Target Name: Αναγνωριστικό όνομα
- Description: Σύντομη περιγραφή
- Username: Όνομα χρήστη μέσω του οποίου το εργαλείο θα εκτελέσει τις ενέργειες
- Password: Κωδικός χρήστη μέσω του οποίου το εργαλείο θα εκτελέσει τις ενέργειες
- IP Address: Η διεύθυνση IP του target FMC

Με αυτήν την ενέργεια, η πλατφόρμα “nimble” καθίσταται έτοιμη να διαχειριστεί το configuration του Cisco FMC.



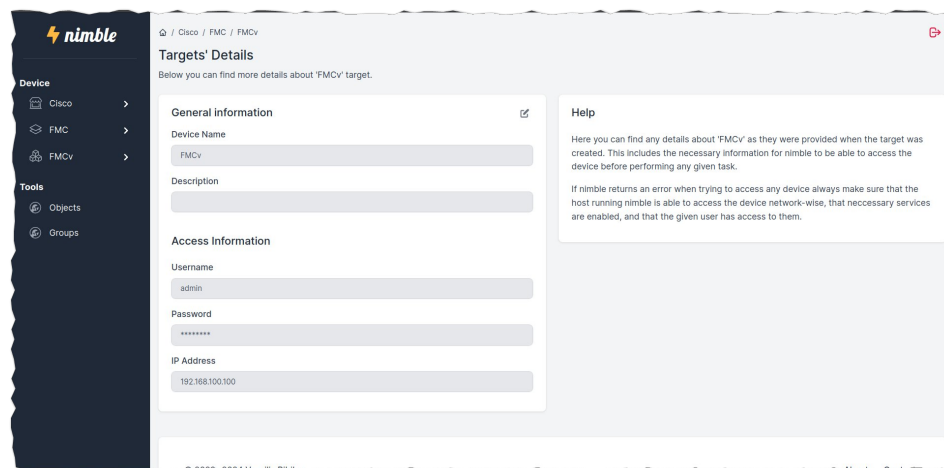
Σχήμα 4.21 Προσθήκη target FMC



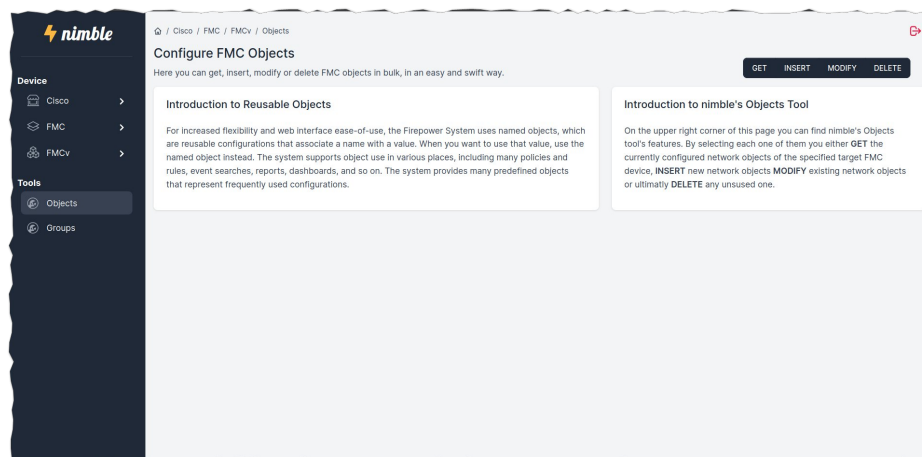
Σχήμα 4.22 Υποδοχή χρήστη από την πλατφόρμα

- **Επιλογή Εργαλείων για FMC:**

Μετά τη δημιουργία του FMC target, ο διαχειριστής επιλέγοντας το νέο target FMC έχει τη δυνατότητα να επιλέξει ανάμεσα σε δύο διαθέσιμα εργαλεία: "Objects" και "Groups". Αυτά τα εργαλεία επιτρέπουν την αποτελεσματική διαχείριση των object και των object group που απαιτούνται για την ενσωμάτωση των νέων συστημάτων ασφαλείας.



Σχήμα 4.23 Εργαλεία για FMC



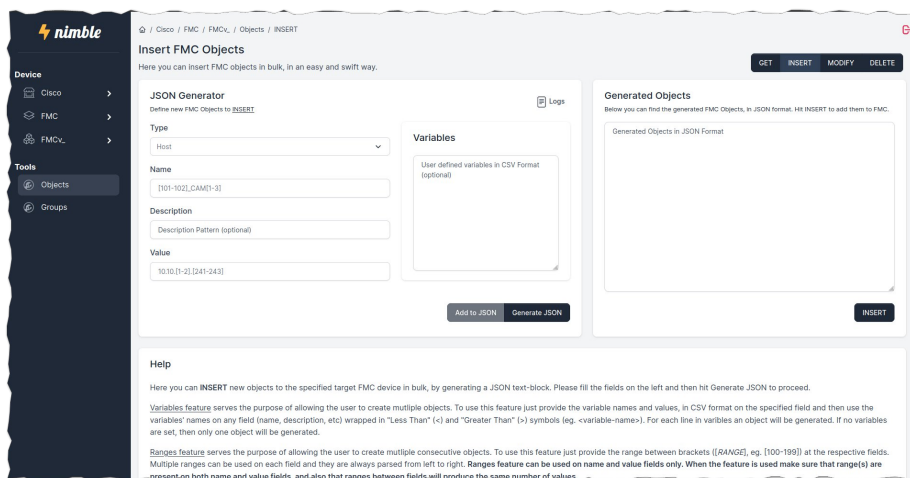
Σχήμα 4.24 Εργαλείο objects

- **Χρήση του Εργαλείου "Objects":**

Αρχικά, ο διαχειριστής επιλέγει το εργαλείο "Objects". Η πλατφόρμα nimble παρέχει ένα φιλικό προς τον χρήστη περιβάλλον που επιτρέπει τη μαζική δημιουργία και διαχείριση των object. Σε αυτή την περίπτωση, ο διαχειριστής θα δημιουργήσει τέσσερα (4) objects ανά κατάσταση. Αυτό σημαίνει ότι για παράδειγμα 100 ενεργών καταστημάτων θα δημιουργηθούν συνολικά 400 object μέσα σε ελάχιστα λεπτά, χάρη στην αυτοματοποίηση και την μαζική παραμετροποίηση που προσφέρει η πλατφόρμα.

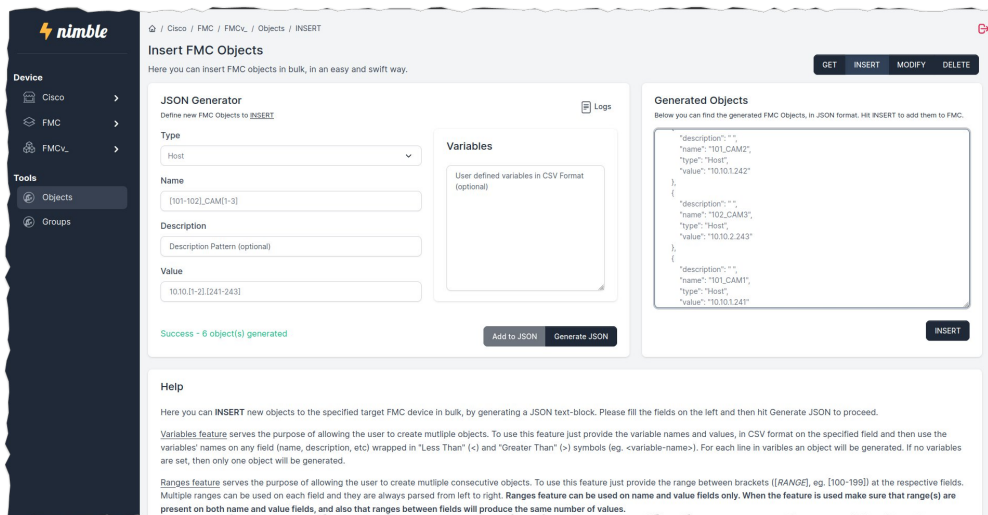
Για τη μαζική δημιουργία των χιλίων object ο μηχανικός θα συμπληρώσει τα παρακάτω πεδία στην αντίστοιχη φόρμα του εργαλείου "Objects":

- o Type
- o Name
- o Value



Σχήμα 4.25 Προσθήκη FMC objects

Έπειτα επιλέγοντας το "Generate JSON", το εργαλείο παράγει αυτόματα το απαιτούμενο configuration, το οποίο ο μηχανικός θα βρει στο πεδίο "Generated Configuration". Ακολουθώντας αυτήν την προσέγγιση το εργαλείο προσφέρει στον μηχανικό τη δυνατότητα να προβεί σε μία ανασκόπηση του configuration που πρόκειται να εφαρμοστεί, αλλά ακόμα και να τροποποιήσει, εφόσον το επιθυμεί, το προς εφαρμογή JSON αρχείο. Όταν λοιπόν ο μηχανικός το αποφασίσει αρκεί να επιλέξει το "Apply" και τότε το εργαλείο θα συνδεθεί στο target FMC και θα δημιουργήσει μαζικά τα objects, μέσα σε λίγα λεπτά, χωρίς να χρειάζεται κάποια άλλη ενέργεια από τον μηχανικό.



Σχήμα 4.26 Προσθήκη FMC objects

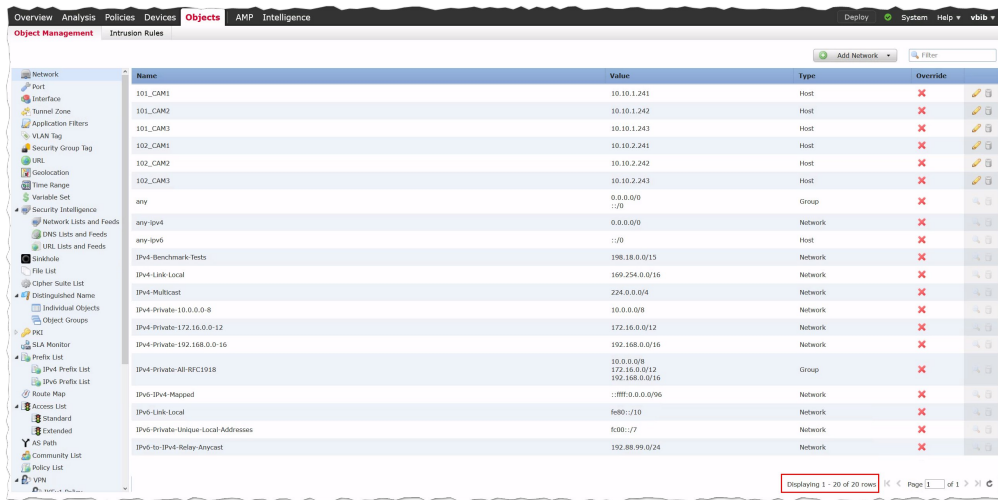
```

1  {
2    {
3      "description": " ",
4      "name": "101_CAM1",
5      "type": "Host",
6      "value": "10.10.1.241"
7    },
8    {
9      "description": " ",
10     "name": "101_CAM2",
11     "type": "Host",
12     "value": "10.10.1.242"
13   },
14   {
15     "description": " ",
16     "name": "101_CAM3",
17     "type": "Host",
18     "value": "10.10.1.243"
19   },
20   {
21     "description": " ",
22     "name": "102_CAM1",
23     "type": "Host",
24     "value": "10.10.2.241"
25   },
26   {
27     "description": " ",
28     "name": "102_CAM2",
29     "type": "Host",
30     "value": "10.10.2.242"
31   },
32   {
33     "description": " ",
34     "name": "102_CAM3",
35     "type": "Host",
36     "value": "10.10.2.243"
37   },
38 }

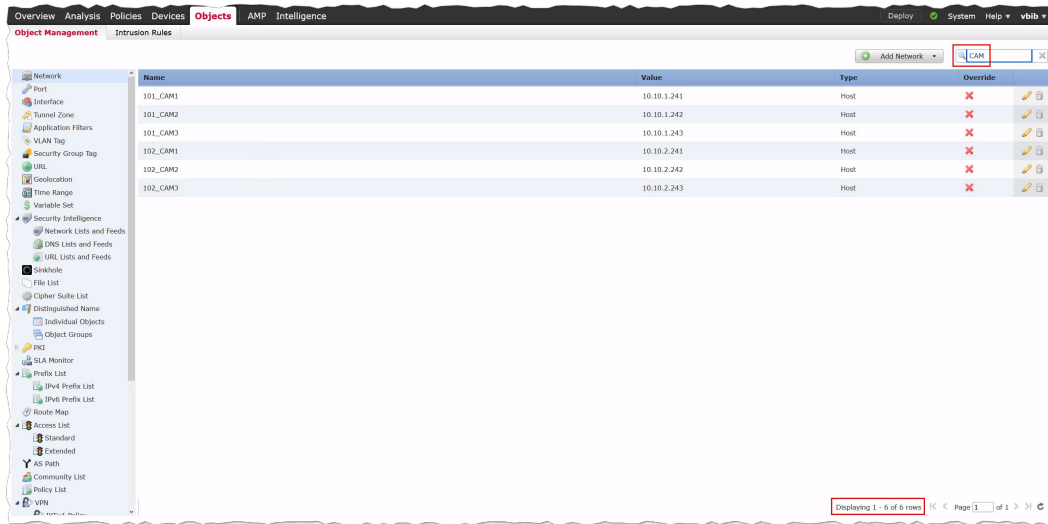
```

Σχήμα 4.27 Αρχείο JSON για FMC objects

Μετά την ολοκλήρωση της εργασίας επιβεβαιώνουμε ότι πλέον το πλήθος των object ανέρχεται στα 20, καθώς επίσης και ότι τα νέα object είναι διαθέσιμα και με τα σωστά στοιχεία.



Σχήμα 4.28 Επιβεβαίωση πλήθους object

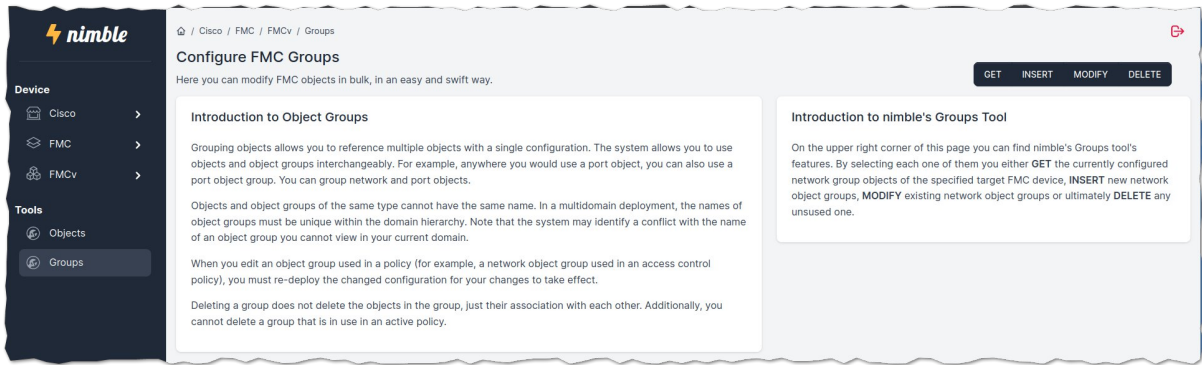


Σχήμα 4.29 Επιβεβαίωση object

Όπως είδαμε ο μηχανικός με τη χρήση του εργαλείου “Objects” για Cisco FMC, της πλατφόρμας “nimble”, κατάφερε να δημιουργήσει όλα τα απαιτούμενα objects χωρίς καμία επαναλαμβανόμενη ενέργεια, συμπληρώνοντας μία φόρμα, και αξιοποιώντας το configuration σε μορφή JSON, που παρήγαγε αυτόματα το εργαλείο. Μία διαδικασία που χωρίς τη χρήση της πλατφόρμας θα ήταν χρονοβόρα και επαναληπτική, κατέστη απλή και σύντομη κάνοντας χρήση των δυνατοτήτων της πλατφόρμας.

- **Χρήση του Εργαλείου "Groups":**

Αφού ολοκληρωθεί η δημιουργία των object, ο διαχειριστής επιλέγει το εργαλείο "Groups". Αυτό το εργαλείο επιτρέπει την ομαδοποίηση των object σε ομάδες, κάνοντας τη διαχείρισή τους πιο ευέλικτη και αποτελεσματική. Ο διαχειριστής θα δημιουργήσει object group για κάθε κατάσταση και, στη συνέχεια, θα ομαδοποιήσει όλες αυτές τις ομάδες σε μία κεντρική ομάδα που θα περιλαμβάνει το σύνολο των νέων συστημάτων ασφαλείας. Πιο συγκεκριμένα για το παράδειγμα των 100 ενεργών καταστημάτων ο μηχανικός θα δημιουργήσει 100 object groups, ένα για κάθε κατάσταση. Το κάθε object group θα περιέχει τα 3 objects που αντιστοιχούν στα νέα συστήματα ασφαλείας κάθε υποκαταστήματος.

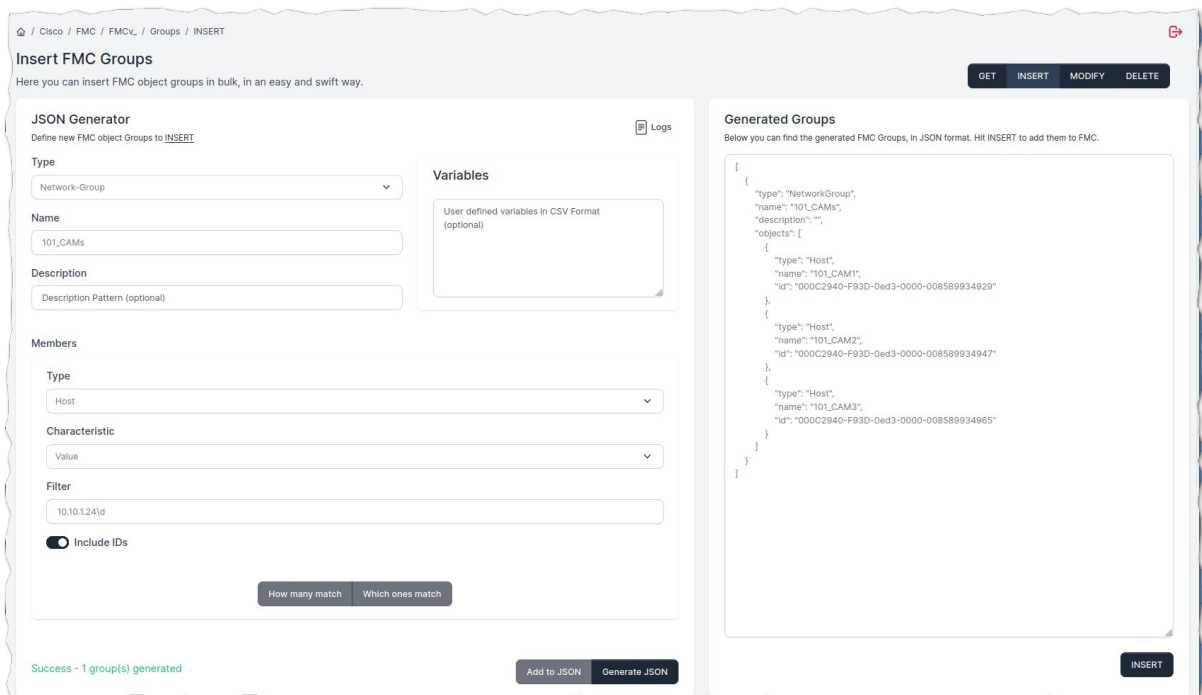


Σχήμα 4.30 Εργαλείο groups

Για τη μαζική δημιουργία των τετρακοσίων object group ο μηχανικός θα συμπληρώσει τα παρακάτω πεδία στην αντίστοιχη φόρμα του εργαλείου “Groups”:

- Type
- Name
- Members
 - Type of member(s)
 - Characteristic
 - Filter

Έπειτα επιλέγοντας το “Generate JSON”, το εργαλείο παράγει αυτόματα το απαιτούμενο configuration, το οποίο ο μηχανικός θα βρει στο πεδίο “Generated Configuration”. Ακολουθώντας αυτήν την προσέγγιση το εργαλείο προσφέρει στο μηχανικό τη δυνατότητα να προβεί σε μία ανασκόπηση του configuration που πρόκειται να εφαρμοστεί, αλλά ακόμα και να τροποποιήσει, εφόσον το κρίνει απαραίτητο, το προς εφαρμογή JSON αρχείο. Όταν λοιπόν ο μηχανικός το αποφασίσει αρκεί να επιλέξει το “Apply” και τότε το εργαλείο θα συνδεθεί στο target FMC και θα δημιουργήσει μαζικά τα object group, αντιστοιχίζοντας τα objects με τα κατάλληλα object-group μέσα σε λίγα λεπτά, χωρίς να χρειάζεται κάποια άλλη ενέργεια από τον μηχανικό.



Σχήμα 4.31 Δημιουργία νέου object group

```

1  {
2
3      "type": "NetworkGroup",
4      "name": "101_CAMs",
5      "description": "",
6      "objects": [
7          {
8              "type": "Host",
9              "name": "101_CAM1",
10             "id": "000C2940-F93D-0ed3-0000-008589934929"
11          },
12          {
13              "type": "Host",
14              "name": "101_CAM2",
15              "id": "000C2940-F93D-0ed3-0000-008589934947"
16          },
17          {
18              "type": "Host",
19              "name": "101_CAM3",
20              "id": "000C2940-F93D-0ed3-0000-008589934965"
21          }
22      ]
23  }
24

```

Σχήμα 4.32 Αρχείο JSON για FMC groups

Η τελική ομαδοποίηση διευκολύνει την εφαρμογή των ACP στο Cisco FMC. Με αυτόν τον τρόπο, οι πολιτικές ασφάλειας και οι κανόνες πρόσβασης μπορούν να εφαρμοστούν γρήγορα και με ακρίβεια, χωρίς την ανάγκη για χρονοβόρες χειροκίνητες διαδικασίες.

Μετά την ολοκλήρωση της εργασίας επιβεβαιώνουμε ότι πλέον τα νέα object-group είναι διαθέσιμα και με τα σωστά στοιχεία.

Name	Value	Type	Override
101_CAMs	101_CAM1 101_CAM2 101_CAM3	Group	✘

Σχήμα 4.33 Επιβεβαίωση object group

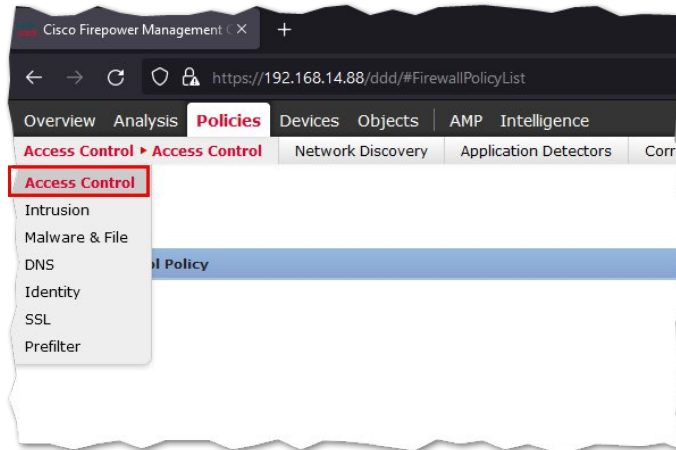
Name	Value	Type	Override
101_CAMs	101_CAM1 101_CAM2 101_CAM3	Group	✘
102_CAMs	102_CAM1 102_CAM2 102_CAM3	Group	✘
StoresCAMs	101_CAMs 102_CAMs	Group	✘

Σχήμα 4.34 Επιβεβαίωση object group

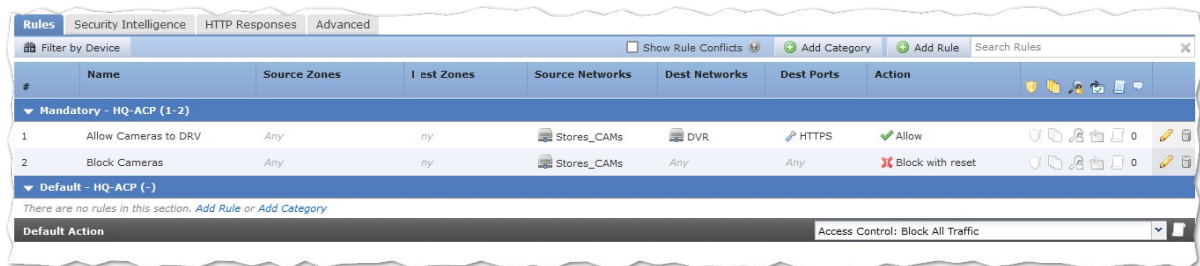
Όπως είδαμε ο μηχανικός με τη χρήση του εργαλείου “Groups” για Cisco FMC, της πλατφόρμας “nimble”, κατάφερε να δημιουργήσει όλα τα απαιτούμενα object-group χωρίς καμία επαναλαμβανόμενη ενέργεια, συμπληρώνοντας μία φόρμα, και αξιοποιώντας το configuration σε μορφή JSON, που παρήγαγε αυτόματα το εργαλείο. Μία διαδικασία που χωρίς τη χρήση της πλατφόρμας θα ήταν χρονοβόρα και επαναληπτική, κατέστη απλή και σύντομη κάνοντας χρήση των δυνατοτήτων της πλατφόρμας.

- **Χρήση των Ομάδων στο ACP:**

Για την αξιοποίηση της συγκεντρωτικού object group ο μηχανικός αρκεί να δημιουργήσει έναν νέο κανόνα στο ACP του FMC. Η ενέργεια αυτή είναι απαραίτητα ανεξαρτήτως της χρήσης ή μη της πλατφόρμας, οπότε ο υπεύθυνος network administrator θα πρέπει να πλοηγηθεί στο Cisco FMC και αφού αποκτήσει πρόσβαση στο WEB GUI χρησιμοποιώντας τα διαπιστευτήρια (*credentials*) του να δημιουργήσει έναν κανόνα στο αντίστοιχο ACP, περιορίζοντας έτσι αποτελεσματικά την πρόσβαση των συστημάτων ασφαλείας στο δίκτυο των server των κεντρικών γραφείων.



Σχήμα 4.35 FMC ACP



Σχήμα 4.36 Κανόνες ACP

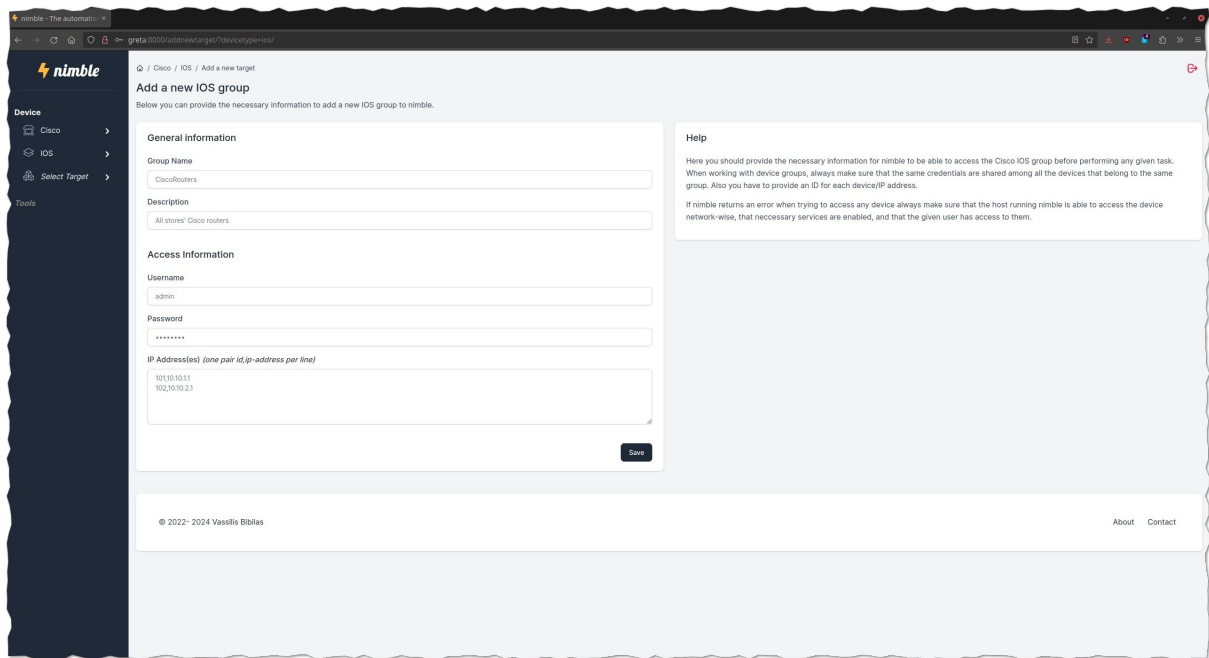
4.4.1.6.2 Δημιουργία και Εφαρμογή configuration για δικτυακές συσκευές

- **Δημιουργία Νέας Οντότητας (Target Group) τύπου Cisco IOS:**

Μέσω του μενού της πλατφόρμας, ο διαχειριστής επιλέγει τη δημιουργία νέας οντότητας και ορίζει το νέο target ως τύπου IOS, συμπληρώνοντας τα παρακάτω στοιχεία:

- Target Group Name: Αναγνωριστικό όνομα
- Description: Σύντομη περιγραφή
- Username: Όνομα χρήστη μέσω του οποίου το εργαλείο θα εκτελέσει τις ενέργειες
- Password: Κωδικός χρήστη μέσω του οποίου το εργαλείο θα εκτελέσει τις ενέργειες
- IP Addresses: Οι διευθύνσεις IP των target IOS που ανήκουν στο target group

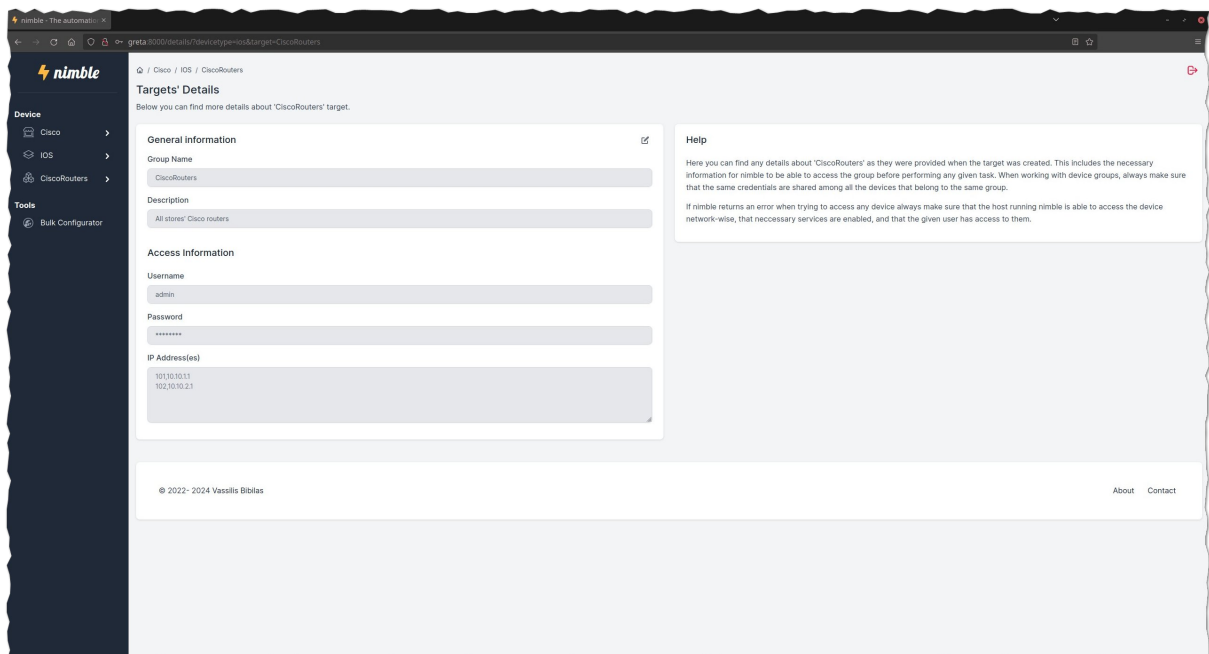
Με αυτήν την ενέργεια, η πλατφόρμα “nimble” καθίσταται έτοιμη να διαχειριστεί το configuration των Cisco IOS.



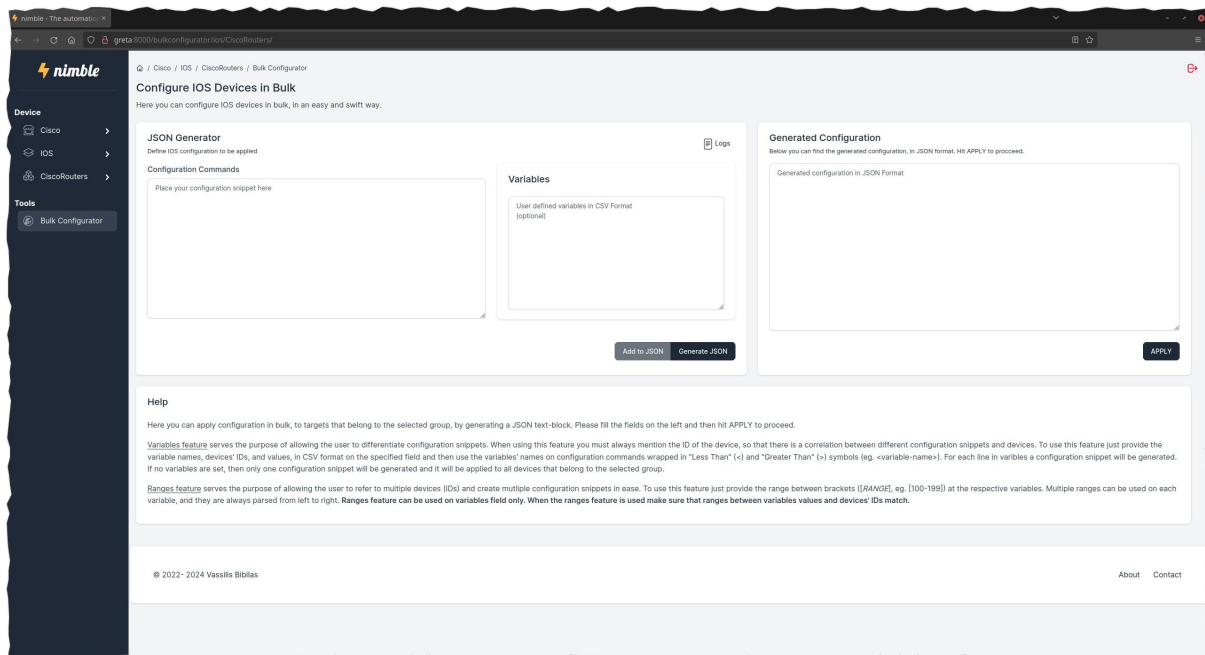
Σχήμα 4.37 Δημιουργία target group IOS

- **Επιλογή Εργαλείου για IOS:**

Μετά τη δημιουργία του IOS target group, ο διαχειριστής επιλέγοντας το νέο target group IOS έχει τη δυνατότητα να επιλέξει το εργαλείο “Bulk Configurator”. Αυτό το εργαλείο επιτρέπει την αποτελεσματική διαχείριση του configuration που απαιτείται για την ενσωμάτωση των νέων συστημάτων ασφαλείας. Πιο συγκεκριμένα, ο μηχανικός θα πρέπει να εφαρμόσει το κατάλληλο configuration για την δημιουργία νέου subinterface στις IOS συσκευές, με σκοπό να καταστεί δυνατή η επικοινωνία των νέων συστημάτων με το δίκτυο. Επίσης, θα πρέπει να δημιουργηθούν οι κατάλληλες ACL ώστε να περιορίσουν την πρόσβαση των νέων συστημάτων στο δίκτυο.



Σχήμα 4.38 Εργαλείο για Cisco IOS



Σχήμα 4.39 Εργαλείο Bulk Configurator

- **Χρήση του εργαλείου “Bulk Configurator” για Cisco IOS:**

Αρχικά, ο διαχειριστής επιλέγει το εργαλείο "Bulk Configurator". Η πλατφόρμα nimble παρέχει ένα φιλικό προς τον χρήστη περιβάλλον που επιτρέπει τη μαζική παραμετροποίηση συσκευών Cisco IOS. Σε αυτή την περίπτωση, ο διαχειριστής θα εφαρμόσει τις απαιτούμενες εντολές στους Cisco router κάθε υποκαταστήματος για όλα ενεργά καταστήματα. Αυτό σημαίνει ότι θα εφαρμοστούν 25 εντολές ανά συσκευή. Συνολικά λοιπόν ο αριθμός των εντολών αυξάνεται σημαντικά για κάθε κατάσταση που προστίθεται, μία διαδικασία που θα διαρκέσει ελάχιστα λεπτά, χάρη στην αυτοματοποίηση και την μαζική παραμετροποίηση που προσφέρει η πλατφόρμα.

Για τη μαζική παραμετροποίηση των διακοσίων πενήντα IOS συσκευών ο μηχανικός θα συμπληρώσει τα παρακάτω πεδία στην αντίστοιχη φόρμα του εργαλείου “Bulk Configurator”:

- o Configuration Commands
- o Variables

Έπειτα επιλέγοντας το “Generate JSON”, το εργαλείο παράγει αυτόματα το απαιτούμενο configuration, το οποίο ο μηχανικός θα βρει στο πεδίο “Generated Configuration”. Ακολουθώντας αυτήν την προσέγγιση το εργαλείο προσφέρει στον μηχανικό τη δυνατότητα να προβεί σε μία ανασκόπηση του configuration που πρόκειται να εφαρμοστεί, αλλά ακόμα και να τροποποιήσει, εφόσον το επιθυμεί, το προς εφαρμογή JSON αρχείο. Όταν λοιπόν ο μηχανικός το αποφασίσει αρκεί να επιλέξει το “Apply” και τότε το εργαλείο θα συνδεθεί σε όλα τα target IOS του target group παράλληλα, και θα εφαρμόσει μαζικά όλες τις εντολές, μέσα σε λίγα λεπτά, χωρίς να χρειάζεται κάποια άλλη ενέργεια από τον μηχανικό.


```

102-CiscoRouter#
102-CiscoRouter#show ip inter brief
Interface                IP-Address      OK? Method Status      Protocol
GigabitEthernet0/0      172.16.240.129 YES DHCP    up          up
GigabitEthernet0/1      unassigned      YES NVRAM   up          up
GigabitEthernet0/2      10.10.2.1       YES manual up          up
GigabitEthernet0/2.128 10.10.2.129    YES manual up          up
GigabitEthernet0/3      unassigned      YES NVRAM   administratively down down
102-CiscoRouter#show run inter g0/2.128
Building configuration...

Current configuration : 159 bytes
!
interface GigabitEthernet0/2.128
 description ### Security ###
 encapsulation dot1q 128
 ip address 10.10.2.129 255.255.255.128
 ip access-group 128 in
end
102-CiscoRouter#
    
```

Σχήμα 4.43 Επιβεβαίωση παραμετροποίησης subinterface Cisco router

```

101-CiscoRouter#
101-CiscoRouter#show ip access-list
Extended IP access list 128
 10 permit tcp host 10.10.1.241 host 192.168.100.249 eq 443
 20 permit tcp host 10.10.1.242 host 192.168.100.249 eq 443
 30 permit tcp host 10.10.1.243 host 192.168.100.249 eq 443
 40 deny ip host 10.10.1.241 any
 50 deny ip host 10.10.1.242 any
 60 deny ip host 10.10.1.243 any
 70 deny ip host 10.10.1.245 10.0.0.0 0.255.255.255
 80 deny ip host 10.10.1.245 172.16.0.0 0.15.255.255
 90 deny ip host 10.10.1.245 192.168.0.0 0.0.255.255
100 permit ip host 10.10.1.245 any
101-CiscoRouter#
101-CiscoRouter#show run | section access-list
access-list 128 remark allow cameras to DVR
access-list 128 permit tcp host 10.10.1.241 host 192.168.100.249 eq 443
access-list 128 permit tcp host 10.10.1.242 host 192.168.100.249 eq 443
access-list 128 permit tcp host 10.10.1.243 host 192.168.100.249 eq 443
access-list 128 remark deny cameras to everything else
access-list 128 deny ip host 10.10.1.241 any
access-list 128 deny ip host 10.10.1.242 any
access-list 128 deny ip host 10.10.1.243 any
access-list 128 remark deny alarm to private
access-list 128 deny ip host 10.10.1.245 10.0.0.0 0.255.255.255
access-list 128 deny ip host 10.10.1.245 172.16.0.0 0.15.255.255
access-list 128 deny ip host 10.10.1.245 192.168.0.0 0.0.255.255
access-list 128 remark allow alarm to Internet
access-list 128 permit ip host 10.10.1.245 any
101-CiscoRouter#
    
```

Σχήμα 4.44 Επιβεβαίωση παραμετροποίησης ACL Cisco router

```

102-CiscoRouter#
102-CiscoRouter#show ip access-list
Extended IP access list 128
 10 permit tcp host 10.10.2.241 host 192.168.100.249 eq 443
 20 permit tcp host 10.10.2.242 host 192.168.100.249 eq 443
 30 permit tcp host 10.10.2.243 host 192.168.100.249 eq 443
 40 deny ip host 10.10.2.241 any
 50 deny ip host 10.10.2.242 any
 60 deny ip host 10.10.2.243 any
 70 deny ip host 10.10.2.245 10.0.0.0 0.255.255.255
 80 deny ip host 10.10.2.245 172.16.0.0 0.15.255.255
 90 deny ip host 10.10.2.245 192.168.0.0 0.0.255.255
100 permit ip host 10.10.2.245 any
102-CiscoRouter#
102-CiscoRouter#show run | section access-list
access-list 128 remark allow cameras to DVR
access-list 128 permit tcp host 10.10.2.241 host 192.168.100.249 eq 443
access-list 128 permit tcp host 10.10.2.242 host 192.168.100.249 eq 443
access-list 128 permit tcp host 10.10.2.243 host 192.168.100.249 eq 443
access-list 128 remark deny cameras to everything else
access-list 128 deny ip host 10.10.2.241 any
access-list 128 deny ip host 10.10.2.242 any
access-list 128 deny ip host 10.10.2.243 any
access-list 128 remark deny alarm to private
access-list 128 deny ip host 10.10.2.245 10.0.0.0 0.255.255.255
access-list 128 deny ip host 10.10.2.245 172.16.0.0 0.15.255.255
access-list 128 deny ip host 10.10.2.245 192.168.0.0 0.0.255.255
access-list 128 remark allow alarm to Internet
access-list 128 permit ip host 10.10.2.245 any
102-CiscoRouter#
    
```

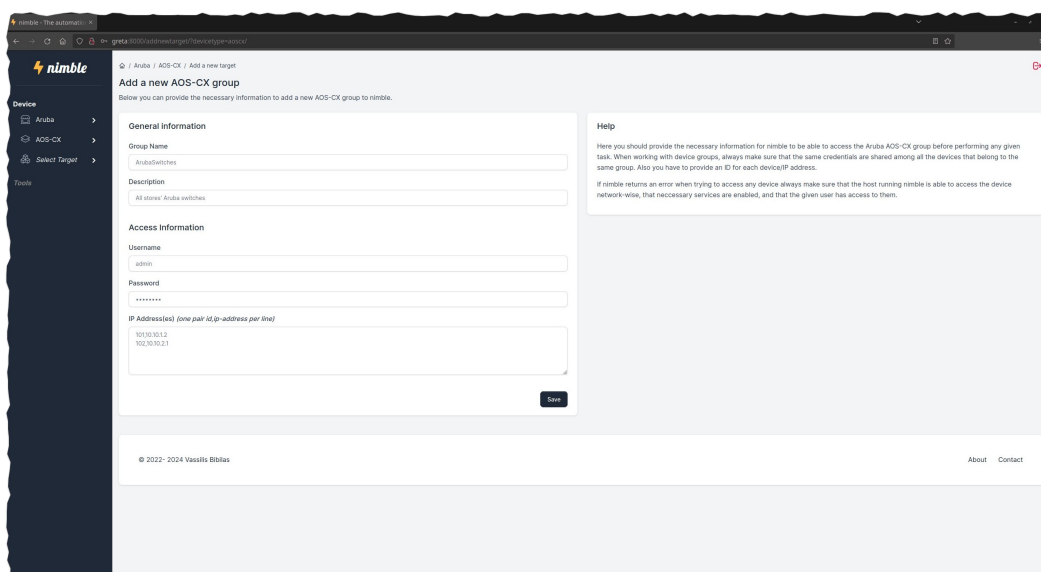
Σχήμα 4.45 Επιβεβαίωση παραμετροποίησης ACL Cisco router

- **Δημιουργία Νέας Οντότητας (Target Group) τύπου Aruba AOS-CX:**

Μέσω του μενού της πλατφόρμας, ο διαχειριστής επιλέγει τη δημιουργία νέας οντότητας και ορίζει το νέο target ως τύπου AOS-CX, συμπληρώνοντας τα παρακάτω στοιχεία:

- ο Target Group Name: Αναγνωριστικό όνομα
- ο Description: Σύντομη περιγραφή
- ο Username: Όνομα χρήστη μέσω του οποίου το εργαλείο θα εκτελέσει τις ενέργειες
- ο Password: Κωδικός χρήστη μέσω του οποίου το εργαλείο θα εκτελέσει τις ενέργειες
- ο IP Addresses: Οι διευθύνσεις IP των target IOS που ανήκουν στο target group

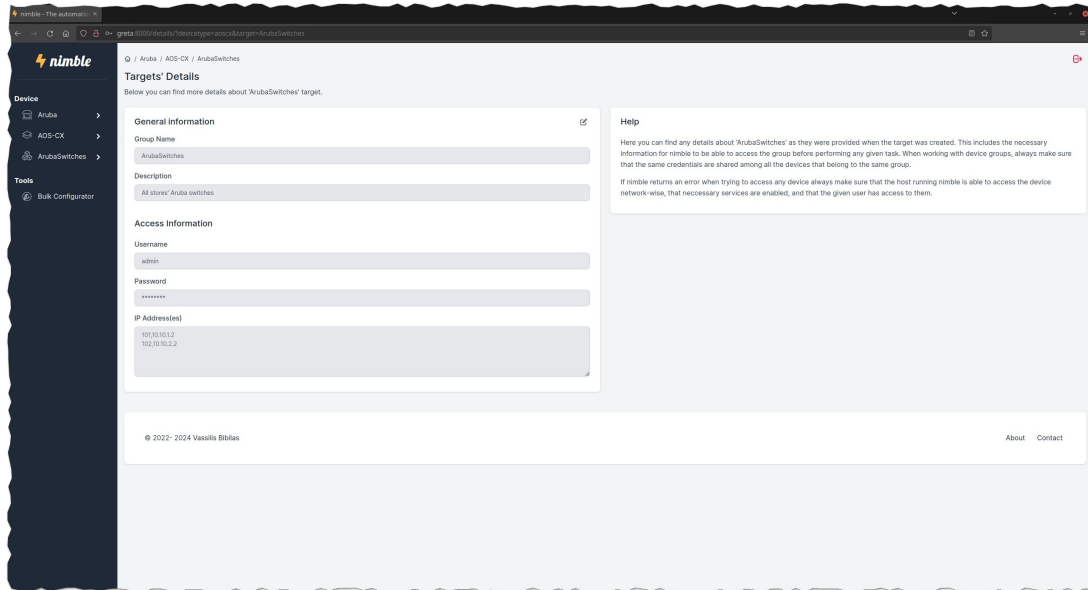
Με αυτήν την ενέργεια, η πλατφόρμα “nimble” καθίσταται έτοιμη να διαχειριστεί το configuration των Aruba AOS-CX.



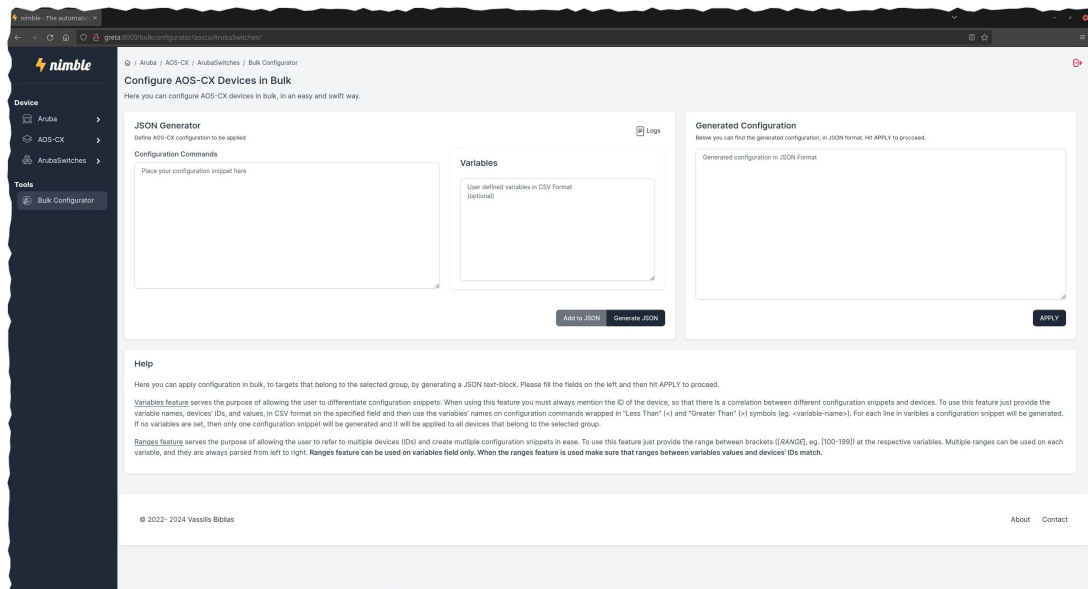
Σχήμα 4.46 Προσθήκη νέου target group AOS-CX

- **Επιλογή Εργαλείου για AOS-CX:**

Μετά τη δημιουργία του AOS-CX target group, ο διαχειριστής επιλέγοντας το νέο target group AOS-CX έχει τη δυνατότητα να επιλέξει το εργαλείο “Bulk Configurator”. Αυτό το εργαλείο επιτρέπει την αποτελεσματική διαχείριση του configuration που απαιτείται για την ενσωμάτωση των νέων συστημάτων ασφαλείας. Πιο συγκεκριμένα, ο μηχανικός θα πρέπει να εφαρμόσει το κατάλληλο configuration για την δημιουργία νέου VLAN στις AOS-CX συσκευές, με σκοπό να καταστεί δυνατή η επικοινωνία των νέων συστημάτων με το δίκτυο. Επίσης, θα πρέπει να παραμετροποιηθούν κατάλληλα οι θύρες ώστε να υποδεχτούν τα νέα συστήματα και να τους παρέχουν πρόσβαση στο δίκτυο.



Σχήμα 4.47 Εργαλείο για AOS-CX



Σχήμα 4.48 Εργαλείο Bulk Configurator

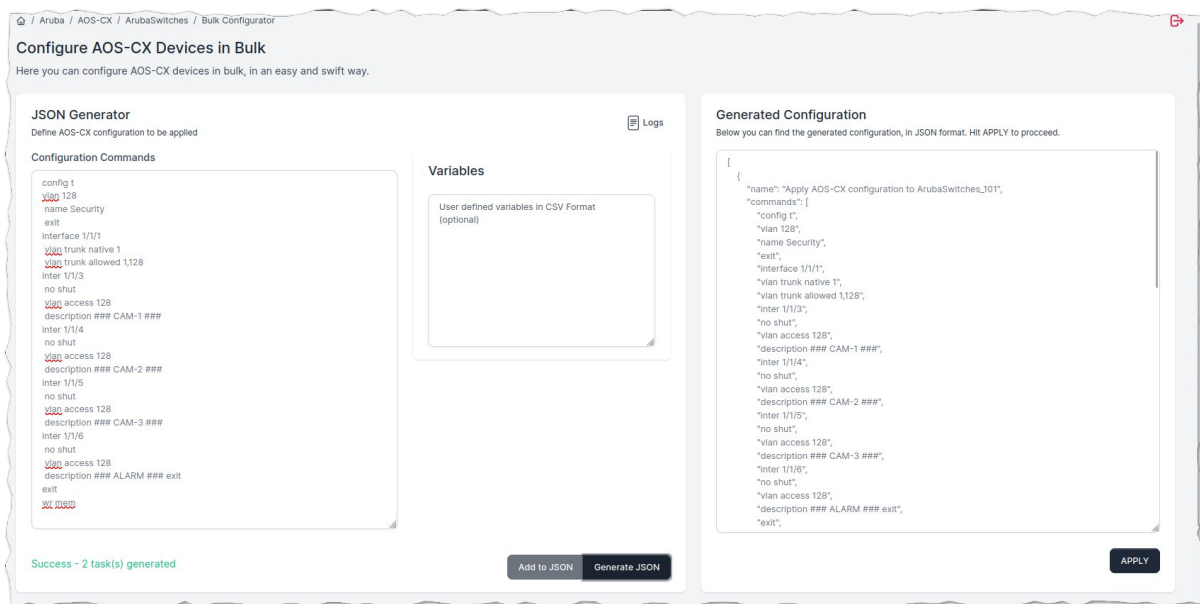
- **Χρήση του εργαλείου “Bulk Configurator” για AOS-CX:**

Αρχικά, ο διαχειριστής επιλέγει το εργαλείο "Bulk Configurator". Η πλατφόρμα nimble παρέχει ένα φιλικό προς τον χρήστη περιβάλλον που επιτρέπει τη μαζική παραμετροποίηση συσκευών Aruba AOS-CX. Σε αυτή την περίπτωση, ο διαχειριστής θα εφαρμόσει τις απαιτούμενες εντολές στα Aruba switch κάθε υποκαταστήματος για όλα τα ενεργά καταστήματα. Αυτό σημαίνει ότι θα εφαρμοστούν 26 εντολές ανά συσκευή. Συνολικά λοιπόν θα εφαρμοστεί μεγάλο πλήθος εντολών, μέσα σε λίγα λεπτά, χάρη στην αυτοματοποίηση και την μαζική παραμετροποίηση που προσφέρει η πλατφόρμα.

Για τη μαζική παραμετροποίηση των διακοσίων πενήντα AOS-CX συσκευών ο μηχανικός θα συμπληρώσει τα παρακάτω πεδία στην αντίστοιχη φόρμα του εργαλείου “Bulk Configurator”:

o Configuration Commands

Έπειτα επιλέγοντας το “Generate JSON”, το εργαλείο παράγει αυτόματα το απαιτούμενο configuration, το οποίο ο μηχανικός θα βρει στο πεδίο “Generated Configuration”. Ακολουθώντας αυτήν την προσέγγιση το εργαλείο προσφέρει στον μηχανικό τη δυνατότητα να προβεί σε μία ανασκόπηση του configuration που πρόκειται να εφαρμοστεί, αλλά ακόμα και να τροποποιήσει, εφόσον το επιθυμεί, το προς εφαρμογή JSON αρχείο. Όταν λοιπόν ο μηχανικός το αποφασίσει αρκεί να επιλέξει το “Apply” και τότε το εργαλείο θα συνδεθεί σε όλα τα target AOS-CX του target group παράλληλα, και θα εφαρμόσει μαζικά όλες τις εντολές, μέσα σε λίγα λεπτά, χωρίς να χρειάζεται κάποια άλλη ενέργεια από τον μηχανικό.



Σχήμα 4.49 Παραμετροποίηση Aruba switches

```

1
2 {
3   "name": "Apply AOS-CX configuration to ArubaSwitches_101",
4   "commands": [
5     "config t",
6     "vlan 128",
7     "name Security",
8     "exit",
9     "interface 1/1/1",
10    "vlan trunk native 1",
11    "vlan trunk allowed 1,128",
12    "inter 1/1/3",
13    "no shut",
14    "vlan access 128",
15    "description ### CAM-1 ###",
16    "inter 1/1/4",
17    "no shut",
18    "vlan access 128",
19    "description ### CAM-2 ###",
20    "inter 1/1/5",
21    "no shut",
22    "vlan access 128",
23    "description ### CAM-3 ###",
24    "inter 1/1/6",
25    "no shut",
26    "vlan access 128",
27    "description ### ALARM ### exit",
28    "exit",
29    "wr mem"
30  ],
31  "device": {
32    "host": "10.10.1.2",
33    "username": "admin",
34    "password": "password"
35  }
36 },
37 {
38   "name": "Apply AOS-CX configuration to ArubaSwitches_102",
39   "commands": [

```

Σχήμα 4.50 Αρχείο JSON για Aruba switches

Μετά την ολοκλήρωση της εργασίας επιβεβαιώνουμε ότι πλέον τα VLAN για την επικοινωνία των συστημάτων ασφαλείας είναι διαθέσιμα στα Aruba AOS-CX switch των καταστημάτων, καθώς επίσης ότι υπάρχει το κατάλληλο configuration στις θύρες για τη σύνδεση των συστημάτων στο δίκτυο.

```

101-ArubaSwitch#
101-ArubaSwitch# show vlan
-----
VLAN Name                Status Reason          Type      Interfaces
-----
1    DEFAULT_VLAN_1         up    ok                default   1/1/1-1/1/2
128  Security                up    ok                static    1/1/1,1/1/3-1/1/6
101-ArubaSwitch#
101-ArubaSwitch# show inter brief
-----
Port      Native Mode  Type      Enabled Status Reason      Speed
        VLAN
-----
1/1/1     1     trunk  --       yes    up    --          1000
1/1/2     1     access --       yes    up    --          1000
1/1/3     128  access --       yes    down  --          --
1/1/4     128  access --       yes    down  --          --
1/1/5     128  access --       yes    down  --          --
1/1/6     128  access --       yes    down  --          --
101-ArubaSwitch# show run inter 1/1/1
interface 1/1/1
no shutdow

```

Σχήμα 4.51 Επιβεβαίωση παραμετροποίησης VLAN Aruba switch

```

102-ArubaSwitch#
102-ArubaSwitch# show vlan
-----
VLAN Name                Status Reason          Type      Interfaces
-----
1    DEFAULT_VLAN_1         up    ok                default   1/1/1-1/1/2
128  Security                up    ok                static    1/1/1,1/1/3-1/1/6
102-ArubaSwitch#
102-ArubaSwitch# show inter brief
-----
Port      Native Mode  Type      Enabled Status Reason      Speed
        VLAN
-----
1/1/1     1     trunk  --       yes    up    --          1000
1/1/2     1     access --       yes    up    --          1000
1/1/3     128  access --       yes    down  --          --
1/1/4     128  access --       yes    down  --          --
1/1/5     128  access --       yes    down  --          --
1/1/6     128  access --       yes    down  --          --
102-ArubaSwitch# show run inter 1/1/1
interface 1/1/1
no shutdow

```

Σχήμα 4.52 Επιβεβαίωση παραμετροποίησης θυρών Aruba switch

```

102-ArubaSwitch# show run inter 1/1/1
interface 1/1/1
  no shutdown
  description ### to CiscoRouter ###
  no routing
  vlan trunk native 1
  vlan trunk allowed 1,128
  exit
102-ArubaSwitch# show run inter 1/1/3
interface 1/1/3
  no shutdown
  description ### CAM-1 ###
  no routing
  vlan access 128
  exit
102-ArubaSwitch# show run inter 1/1/4
interface 1/1/4
  no shutdown
  description ### CAM-2 ###
  no routing
  vlan access 128
  exit
102-ArubaSwitch# show run inter 1/1/5
interface 1/1/5
  no shutdown
  description ### CAM-3 ###
  no routing
  vlan access 128
  exit
102-ArubaSwitch# show run inter 1/1/6
interface 1/1/6
  no shutdown
  description ### ALARM ###
  no routing
  vlan access 128
  exit
102-ArubaSwitch#

102-ArubaSwitch# show run inter 1/1/1
interface 1/1/1
  no shutdown
  description ### to CiscoRouter ###
  no routing
  vlan trunk native 1
  vlan trunk allowed 1,128
  exit
102-ArubaSwitch# show run inter 1/1/3
interface 1/1/3
  no shutdown
  description ### CAM-1 ###
  no routing
  vlan access 128
  exit
102-ArubaSwitch# show run inter 1/1/4
interface 1/1/4
  no shutdown
  description ### CAM-2 ###
  no routing
  vlan access 128
  exit
102-ArubaSwitch# show run inter 1/1/5
interface 1/1/5
  no shutdown
  description ### CAM-3 ###
  no routing
  vlan access 128
  exit
102-ArubaSwitch# show run inter 1/1/6
interface 1/1/6
  no shutdown
  description ### ALARM ###
  no routing
  vlan access 128
  exit
102-ArubaSwitch#

```

Σχήμα 4.53 Επιβεβαίωση παραμετροποίησης θυρών Aruba switch

Όπως είδαμε ο μηχανικός με τη χρήση του εργαλείου “Bulk Configurator” για Cisco IOS και Aruba AOS-CX, της πλατφόρμας “nimble”, κατάφερε να δημιουργήσει και να εφαρμόσει όλες τις απαιτούμενες εντολές, προσαρμοσμένες στις απαιτήσεις κάθε υποκαταστήματος χωρίς καμία επαναλαμβανόμενη ενέργεια, συμπληρώνοντας μία φόρμα ανά τύπο συσκευής, και αξιοποιώντας το configuration σε μορφή JSON, που παρήγαγε αυτόματα το εργαλείο. Μία διαδικασία που χωρίς τη χρήση της πλατφόρμας θα ήταν χρονοβόρα, επαναληπτική, και επιρρεπής σε λάθη, κατέστη απλή, σύντομη και ακριβής κάνοντας χρήση των δυνατοτήτων της πλατφόρμας.

4.5 Επίλογος

Η ενότητα αυτή ανέδειξε τη σημασία της αυτοματοποίησης και της αποτελεσματικής διαχείρισης δικτύου μέσω της πλατφόρμας “nimble”. Συγκρίνοντας τις παραδοσιακές χειροκίνητες διαδικασίες με την αυτοματοποίηση που προσφέρει η πλατφόρμα, γίνεται εμφανής η εξοικονόμηση χρόνου και πόρων, καθώς και η αύξηση της ακρίβειας και της αποδοτικότητας.

Χωρίς την πλατφόρμα “nimble”, οι μηχανικοί του NOC θα έπρεπε να εκτελέσουν επαναλαμβανόμενες, χρονοβόρες εργασίες σε κάθε υποκατάστημα, με αυξημένο κίνδυνο για ανθρώπινα λάθη και σημαντικά λειτουργικά κόστη. Η χειροκίνητη δημιουργία object και object group στο Cisco FMC, η παραμετροποίηση των Cisco router και των Aruba switches για την ενσωμάτωση των νέων συστημάτων ασφαλείας, απαιτούν σημαντική αφοσίωση και χρόνο από τους μηχανικούς.

Αντίθετα, η χρήση της πλατφόρμας nimble επιτρέπει την ταχεία και αποδοτική ολοκλήρωση αυτών των διαδικασιών. Η δυνατότητα μαζικής δημιουργίας και διαχείρισης object και object group, καθώς και η αυτοματοποίηση των ρυθμίσεων δικτύου, εξασφαλίζουν την ομοιομορφία και την ακρίβεια. Επιπλέον, η πλατφόρμα διευκολύνει έμμεσα την κεντρική διαχείριση πολιτικών πρόσβασης, ενισχύοντας την ασφάλεια και την ευελιξία της δικτυακής υποδομής.

Σε ένα επιχειρησιακό περιβάλλον όπου η ταχύτητα και η ακρίβεια είναι κρίσιμες, η πλατφόρμα nimble αποδεικνύεται αναντικατάστατο εργαλείο. Με τη δυνατότητα αυτοματοποίησης σύνθετων διαδικασιών

και τη μείωση των λειτουργικών δαπανών, η πλατφόρμα συμβάλλει καθοριστικά στην αποδοτικότητα και την επιτυχία της εταιρίας. Το NOC μπορεί πλέον να επικεντρωθεί σε στρατηγικές δραστηριότητες υψηλότερης αξίας, βελτιώνοντας τη συνολική απόδοση και τη διαχειριστική ικανότητα του δικτύου.

Η υιοθέτηση τέτοιων σύγχρονων εργαλείων όχι μόνο εκσυγχρονίζει τις διαδικασίες αλλά και ενισχύει την ανταγωνιστικότητα της εταιρίας στον απαιτητικό τομέα της τεχνολογίας και των δικτύων.

Κεφάλαιο 5ο: Συμπεράσματα και Μελλοντικές Επεκτάσεις

5.1 Συμπεράσματα

Η διαχείριση και συντήρηση εταιρικών δικτύων αποτελεί ένα πολύπλευρο και πολλές φορές πολύπλοκο έργο, το οποίο απαιτεί συνεχή προσοχή και επαγρύπνηση από τους network administrator. Η χρήση και εφαρμογή συμβάσεων αποτελούν στοιχείο που διευκολύνει σημαντικά την διαχείριση των αναπτυσσόμενων δικτύων, και βοηθά τους διαχειριστές να είναι αποτελεσματικότεροι στο έργο τους. Επιπλέον, γεγονός αποτελεί ότι τα λάθη μπορούν να κοστίσουν ακριβά σε λειτουργικό επίπεδο, όπως επίσης και από πλευράς ασφάλειας σε μία εταιρία, επιβεβαιώνοντας την ανάγκη μείωσης τους στο ελάχιστο δυνατό.

Επίσης, οι σύντομοι και προβλέψιμοι χρόνοι παράδοσης είναι κρίσιμοι για την ομαλή λειτουργία και την αποδοτικότητα του δικτύου, και αυτό πρέπει να λαμβάνεται υπόψη κατά την επιλογή των μεθόδων διαχείρισης. Τέλος, η ανάγκη για αυτοματοποίηση επισημαίνεται ως αναγκαία, καθώς μειώνει τον απαιτούμενο χρόνο και ταυτόχρονα αυξάνει την αξιοπιστία και την ασφάλεια των όλο και αναπτυσσόμενων εταιρικών δικτύων.

Η εμπειρία μας στην ανάπτυξη και την χρήση της πλατφόρμας “nimble” μας οδήγησε στα παραπάνω συμπεράσματα και είναι ουσιώδη για την κατανόηση της σημασίας της αυτοματοποίησης στη διαχείριση των εταιρικών δικτύων.

5.2 Μελλοντικές επεκτάσεις

Η αρχιτεκτονική της πλατφόρμας “nimble” παρέχει τη βάση για την ενσωμάτωση νέων εργαλείων και λειτουργιών, επιτρέποντας τη συνεχή βελτίωση και εξέλιξη του συστήματος. Παρακάτω περιγράφονται μερικές προγραμματισμένες επεκτάσεις για την πλατφόρμα “nimble”:

- Προσθήκη δυνατότητας επαναφοράς (revert) για τις ενέργειες που πραγματοποιήθηκαν, προκειμένου να διευκολυνθεί η ανάκαμψη σε περίπτωση λάθους.
- Ενσωμάτωση εργαλείων για τον έλεγχο και την παρακολούθηση της λειτουργίας του δικτύου και των συσκευών.
- Προσθήκη σήμανσης προόδου (progress bar) ώστε να ενημερώνεται ο χρήστης για την πρόοδο των διαδικασιών.
- Πρόσβαση του χρήστη σε λεπτομερεί αρχεία καταγραφής (logs) για περαιτέρω ανάλυση και διαχείριση.
- Δυνατότητα αποθήκευσης των αρχείων παραμετροποίησης (configuration files) των συσκευών για ευκολότερη ανάκτηση και διαχείριση.
- Προσθήκη δυνατότητας σύγκρισης διαφορετικών configuration files για την εντοπισμό διαφορών και την επίλυση προβλημάτων.

Οι μελλοντικές επεκτάσεις της πλατφόρμας “nimble” αποσκοπούν στη βελτίωση της λειτουργικότητας και της χρηστικότητάς της, επιτρέποντας στους χρήστες να διαχειρίζονται και να παρακολουθούν τα δίκτυά τους με ακόμα μεγαλύτερη αποτελεσματικότητα και αξιοπιστία. Αυτές οι επεκτάσεις συμβάλλουν στη συνεχή προσαρμογή και βελτίωση της πλατφόρμας, επιτρέποντάς της να ανταποκριθεί αποτελεσματικά στις μελλοντικές ανάγκες και προκλήσεις της διαχείρισης δικτύων.

ΒΙΒΛΙΟΓΡΑΦΙΑ

- [1] Rohit Prasad, The Importance of Computer Networking: How it Shapes the Future of Business. Available: <https://www.linkedin.com/pulse/importance-computer-networking-how-shapes-future-business-prasad-1c>
- [2] Iyamuremye, Blake, and Hisato Shima. "Network security testing tools for SMEs (small and medium enterprises)." 2018 IEEE International Conference on Applied System Invention (ICASI). IEEE, 2018.
- [3] Zhou, Donghao, et al. "A survey on network data collection." Journal of Network and Computer Applications 116 (2018): 9-23.
- [4] Pras, Aiko, et al. "Key research challenges in network management." IEEE communications magazine 45.10 (2007): 104-110.
- [5] <https://www.forbes.com/advisor/business/software/what-is-network-management/> [4] Hassan, R., Razali, R., Mohseni, S., Mohamad, O., & Ismail, Z. (2010). Architecture of network management tools for heterogeneous system. arXiv preprint arXiv:1001.1967.
- [6] Claise, Benoit, Joe Clarke, and Jan Lindblad. Network programmability with YANG: the structure of network automation with YANG, NETCONF, RESTCONF, and gNMI. Addison-Wesley Professional, 2019.
- [7] Edelman, Jason, Scott S. Lowe, and Matt Oswalt. Network Programmability and Automation: Skills for the Next-Generation Network Engineer. " O'Reilly Media, Inc.", 2018.
- [8] Rose, Marshall T. The simple book: an introduction to networking management: revised second edition. Simon & Schuster Trade, 1995.
- [9] Hassan, R., Razali, R., Mohseni, S., Mohamad, O., & Ismail, Z. (2010). Architecture of network management tools for heterogeneous system. arXiv preprint arXiv:1001.1967.
- [10] [Kijazi, Ahmed, and Kisangiri Michael. "A Step on Developing Network Monitoring Tools." (2014).
- [11] Cisco, "Cisco Catalyst Center: Smarter, simpler, network management". [Online]. Available: <https://www.cisco.com/site/us/en/products/networking/catalyst-center/index.html>.
- [12] HashiCorp, "Terraform Community: Automate infrastructure on any cloud with Terraform". [Online]. Available: <https://www.terraform.io>.
- [13] IP Fabric, "IP Fabric: A world where you can ask your network anything". [Online]. Available: <https://ipfabric.io>.
- [14] Itential, "itential: Simplify & Scale Network Automation". [Online]. Available: <https://www.itential.com>.
- [15] Juniper Networks, "Junos Space Network Management Platform". [Online]. Available: <https://www.juniper.net/us/en/products/sdn-and-orchestration/junos-space-platform.html>.
- [16] Django, "Django was invented to meet fast-moving newsroom deadlines, while satisfying the tough requirements of experienced web developers.". [Online]. Available: <https://www.djangoproject.com/start/overview/>.

- [17] Python, “Python is a programming language that lets you work more quickly and integrate your systems more effectively.”. [Online]. Available: <https://www.python.org>.
- [18] Cisco, “Working with the Firepower Management Center API”. [Online]. Available: <https://developer.cisco.com/learning/modules/fmc-api>.
- [19] Paramiko, “A Python implementation of SSHv2.”. [Online]. Available: <https://docs.paramiko.org>.
- [20] OpenSSH, “Keeping your communiques secret”. [Online]. Available: <https://www.openssh.com>.
- [21] Python, “The concurrent package”. [Online]. Available: <https://docs.python.org/3.11/library/concurrent.html>.
- [22] Bootstrap, “Build fast, responsive sites with Bootstrap”. [Online]. Available: <https://getbootstrap.com>.
- [23] ECMA International, “ECMA-262, 14th edition, June 2023 ECMAScript® 2023: Language Specification”. [Online]. Available: <https://262.ecma-international.org/14.0>.
- [24] Wikipedia, “Comma-separated values”. [Online]. Available: https://en.wikipedia.org/wiki/Comma-separated_values.
- [25] ECMA International, “ECMA-404, 2nd edition, December 2017: The JSON data interchange syntax”. [Online]. Available: <https://ecma-international.org/publications-and-standards/standards/ecma-404>.
- [26] EVE-NG, “EVE - The Emulated Virtual Environment: For Network, Security and DevOps Professionals”. [Online]. Available: <https://www.eve-ng.net>.
- [27] Broadcom, “VMware”. [Online]. Available: <https://www.vmware.com>.
- [28] Chowdhury, NM Mosharaf Kabir, and Raouf Boutaba. "A survey of network virtualization." Computer Networks 54.5 (2010): 862-876
- [29] IETF, “Address Allocation for Private Internets”. [Online]. Available: <https://datatracker.ietf.org/doc/html/rfc1918>.