ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ
ΚΑΙ ΗΛΕΚΤΡΟΝΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Σχεδίαση και υλοποίηση ενσύρματης και ασύρματης δικτυακής υποδομής μιας επιχείρησης μεσαίου μεγέθους

Του φοιτητή
Καρβουνά Αρχοντή
Αρ. Μητρώου: 144238

Επιβλέπων
Δημήτριος Αμανατιάδης

Μάιος 2025

Τίτλος Π.Ε.
Σχεδίαση και υλοποίηση ενσύρματης και ασύρματης δικτυακής υποδομής μιας επιχείρησης μεσαίου μεγέθους
Κωδικός Π.Ε.
23296
Ονοματεπώνυμο φοιτητή
Αρχοντής Καρβουνάς
Ονοματεπώνυμο εισηγητή
Δημήτριος Αμανατιάδης
Ημερομηνία ανάληψης Π.Ε.
01-11-23
Ημερομηνία περάτωσης Π.Ε.
30-05-25

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

Πρόλογος

Ο λόγος που επιλέχθηκε το παρόν θέμα είναι η μελέτη και η παραμετροποίηση μιας δικτυακής υποδομής μιας επιχείρησης μεσαίου μεγέθους η οποία παρουσιάζει ιδιαίτερο ενδιαφέρον ειδικά στην παραμετροποίηση των next generation firewalls τα οποία καλούνται να αντιμετωπίσουν πρωτοεμφανιζόμενες απειλές ασφάλειας. Σκοπός της είναι να αναδείξει τις βασικές γνώσεις και ρυθμίσεις που απαιτούνται για να έχουμε ένα παραγωγικό δίκτυο ξεκινώντας από τους μεταγωγείς και καταλήγοντας στα εταιρικά firewall.

Περίληψη

Στην εργασία θα γίνει εξήγηση και ανάλυση βασικών εννοιών δικτύωσης και των διαφόρων πρωτοκόλλων και συσκευών που χρησιμοποιούνται σε ένα εταιρικό δίκτυο. Θα γίνει παραμετροποίηση βασικών ρυθμίσεων δικτύωσης σε μεταγωγείς Cisco για να εξασφαλιστεί η επικοινωνία μεταξύ των υπολογιστών του δικτύου όχι μόνο μεταξύ τους αλλά και προς το Ιντερνετ.
Για την ασφάλεια των εν λόγω συσκευών καθώς και για τον έλεγχο τους και την προστασία τους από κακόβουλο λογισμικό θα παρουσιαστεί η ανάλυση και η παραμετροποίηση ενός next generation firewall της Cisco το οποίο θα αναλάβει και το ρόλο του δρομολογητή στο δίκτυο.

Design and implementation of a wired and wireless network infrastructure for a medium-sized company

Archontis Karvounas

Abstract

The paper will explain and analyze basic networking concepts and the various protocols and devices used in a corporate network. Basic networking settings will be configured on Cisco switches to ensure that the computers on the network communicate not only with each other but also to the Internet. In order to secure these devices as well as to control and protect them from malware, the analysis and configuration of a Cisco next generation firewall will be presented which will also take on the role of a router in the network.

Περιεχόμενα

Πρόλογος iii
Περίληψη iv
Abstract v
Περιεχόμενα vi
Κεφάλαιο 1ο: Βασικές γνώσεις δικτύων 1
1.1 Εισαγωγή 1
1.2 Μοντέλο Δικτύωσης TCP/IP 1
1.3 Επίπεδο εφαρμογών TCP/IP 2
1.3.1 Μηχανισμοί πρωτοκόλλου HTTP 2
1.4 Επίπεδο μεταφοράς TCP/IP 3
1.4.1 Βασικά στοιχεία της αποκατάστασης σφαλμάτων TCP 3
1.4.2 UDP και TCP ports(θύρες) 4
1.5 Επίπεδο δικτύου TCP/IP 4
1.5.1 Βασικά στοιχεία διευθυνσιοδότησης πρωτοκόλλου διαδικτύου 5
1.5.2 Βασικά στοιχεία δρομολόγησης IP 6
1.6 TCP/IP Data-Link και Physical Layers 6
1.6.1 Ορολογία ενθυλάκωσης δεδομένων(Data Encapsulation) 7
1.7 Επίλογος 8
Κεφάλαιο 2ο: Βασικές αρχές των Ethernet LANs 9
2.1 Εισαγωγή 9
2.2 Τυπικά τοπικά δίκτυα SOHO(Small office/Home Office) 9
2.3 Τυπικά εταιρικά LANs(Enterprise LANs) 10
2.4 Διευθυνσιοδότηση Ethernet 10
2.5 Δρομολόγηση IP(IP Routing) 11
2.5.1 Λογική δρομολόγησης (προώθησης) επιπέδου δικτύου 11
2.5.2 Πώς η δρομολόγηση επιπέδου δικτύου χρησιμοποιεί τα LANs και τα WANs 12
2.5.3 Κανόνες IP (δίκτυα και υποδίκτυα) 14
2.5.4 IP Header 14
2.6 Άλλες σημαντικές λειτουργίες πρωτοκόλλων 14
2.6.1 DNS 15
2.6.2 ARP-Address Resolution Protocol 15
2.6.3 Dynamic Host Configuration Protocol (DHCP) 16

2.6.4 ICMP Echo και η εντολή ping 17
2.6.5 Επίλογος 17
Κεφάλαιο 3ο: Βασικές ρυθμίσεις Cisco switches 18
3.1 Εισαγωγή 18
3.2 Πληροφορίες για τα switches και το CLI 18
3.3 Καλωδίωση της σύνδεσης της κονσόλας 19
3.4 Πρόσβαση στο CLI με Telnet και SSH 21
3.5 Κωδικός πρόσβασης για πρόσβαση στο CLI από την κονσόλα 22
3.6 Οι εντολές debug και show 22
3.7 Διαμόρφωση του λογισμικού Cisco IOS 23
3.7.1 Υπολειτουργίες και πλαίσια διαμόρφωσης 24
3.7.2 Αντιγραφή και διαγράφη αρχείων διαμόρφωσης 24
3.8 Επισκόπηση της λογικής μεταγωγής(Switching Logic) 24
3.8.1 Σύνοψη LAN Switching 25
3.9 Διαμόρφωση βασικής διαχείρισης του switch 25
3.9.1 Ασφάλιση του CLI του switch 26
3.9.2 Διασφάλιση της πρόσβασης στο user mode και στο privileged mode με απλούς κωδικούς πρόσβασης 26
3.9.3 Διασφάλιση της πρόσβασης στο user mode με τοπικά ονόματα χρήστη 27
3.9.4 Διασφάλιση απομακρυσμένης πρόσβασης με Secure Shell 28
3.10 Ενεργοποίηση IPv4 για απομακρυσμένη πρόσβαση 29
3.10.1 Ρύθμιση IPv4 σε έναν μεταγωγέα 30
3.10.2 Επαλήθευση του IPv4 σε ένα μεταγωγέα 31
3.11 Επίλογος 31
Κεφάλαιο 4ο: VLANs 32
4.1 Virtual LAN Concepts 32
4.2 Vlan trunking 33
4.3 VLAN Tagging 34
4.4 Τα πρωτόκολλα 802.1Q και ISL VLAN Trunking 34
4.5 Προώθηση δεδομένων μεταξύ VLANs 35
4.5.1 Η ανάγκη για δρομολόγηση μεταξύ VLANs 35
4.5.2 Διαμόρφωση και επαλήθευση LAN και VLAN Trunking Configuration 35
4.5.3 Δημιουργία VLANs και εκχώρηση access VLANs πρόσβασης σε interface 35
4.5.4 Διαμόρφωση trunk links 36
4.6 Υλοποίηση διεπαφών που συνδέονται με τηλέφωνα 36

4.6.1 Διαμόρφωση και επαλήθευση VLAN δεδομένων και φωνής 37
4.7 Επίλογος 37
Κεφάλαιο 5ο: Next Generation Firewall 38
5.1 Εισαγωγή 38
5.2 Network-based και host-based firewalls 38
5.3 Υλοποίηση και διαχείριση Next-Generation Firewall της Cisco 40
5.4 Αρχιτεκτονική λογισμικού και υλικού 41
5.5 Καταχώρηση Συσκευής(Device Registration) 42
5.5.1 Παραμετροποιήσεις στο FTD μέσω CLI 43
5.5.2 Χρήση firewall σε router ή σε transparent mode 44
5.6 Παραμετροποιήσεις FMC μέσω GUI 45
5.7 Διαμόρφωση των routed interfaces 47
5.7.1 Διαμόρφωση των interfaces με στατικές διευθύνσεις IP. 48
5.8 DHCP Server 50
5.9 Access Control Policy-Πολιτική ελέγχου Πρόσβασης 51
5.9.1 Βασικά στοιχεία πολιτικής ελέγχου πρόσβασης 51
5.9.2 Access control policy editor- Συντάκτης πολιτικής 51
5.9.3 Rule Editor-Συντάκτης κανόνων 53
5.9.4 Βέλτιστες πρακτικές για την πολιτική ελέγχου πρόσβασης 54
5.10 Διαμόρφωση πολιτικής ελέγχου πρόσβασης 55
5.11 Network Analysis και Intrusion Policies 60
5.11.1 Intrusion Prevention System 61
5.11.2 Malware και File Policy 61
5.11.3 Διαμόρφωση μιας πολιτικής αρχείων 62
5.12 Μετάφραση διευθύνσεων δικτύου (NAT) 64
5.12.1 Βασικά στοιχεία NAT 64
5.12.2 Τεχνικές NAT 64
5.12.3 Τύποι κανόνων NAT 65
5.12.4 Βέλτιστες πρακτικές για το NAT 66
5.12.5 Ρύθμιση του NAT 67
5.12.6 Επίλογος 70
Κεφάλαιο 6ο: Συμπεράσματα ή/και προτάσεις βελτίωσης 71
Βιβλιογραφία 72

Κεφάλαιο 1ο: Βασικές γνώσεις δικτύων

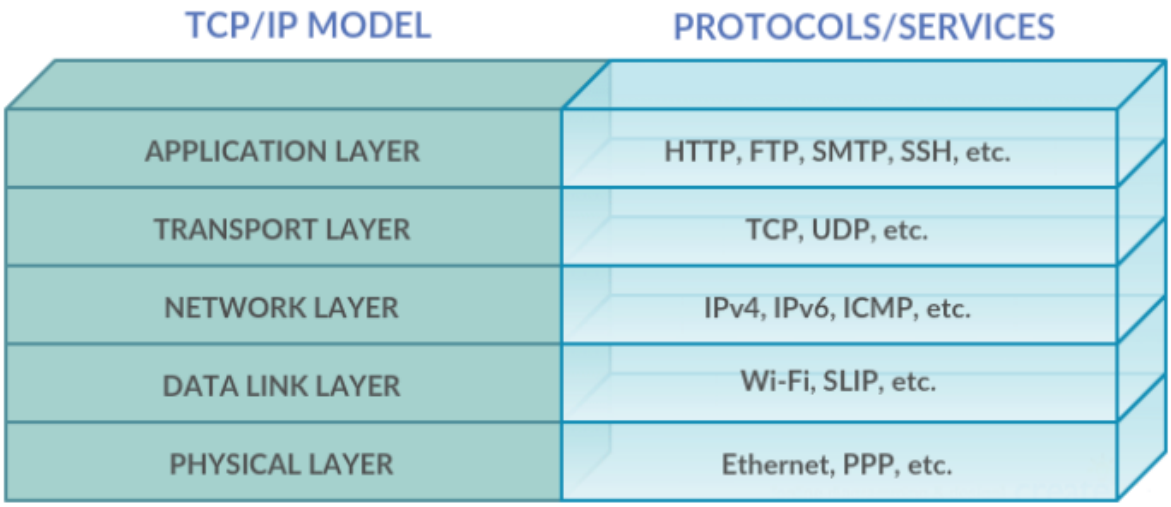
1.1 Εισαγωγή

Τα δίκτυα λειτουργούν σωστά επειδή οι διάφορες συσκευές και το λογισμικό ακολουθούν τους κανόνες. Αυτοί οι κανόνες έχουν τη μορφή προτύπων και πρωτοκόλλων, τα οποία είναι συμφωνίες για ένα συγκεκριμένο μέρος του τρόπου λειτουργίας ενός δικτύου.

Τα μοντέλα δικτύωσης ορίζουν μια δομή και διάφορες κατηγορίες (επίπεδα) προτύπων και πρωτοκόλλων. Σήμερα, οι κανόνες Transmission Control Protocol/IP Protocol(TCP/IP) αποτελούν το πιο διαδεδομένο μοντέλο δικτύωσης που χρησιμοποιείται. Μπορείτε να βρείτε υποστήριξη για το TCP/IP σχεδόν σε κάθε λειτουργικό σύστημα υπολογιστή (OS) που υπάρχει σήμερα, από κινητά τηλέφωνα έως κεντρικούς υπολογιστές. Κάθε δίκτυο που κατασκευάζεται σήμερα με προϊόντα της Cisco υποστηρίζει το TCP/IP.

1.2 Μοντέλο Δικτύωσης TCP/IP

Για την ευκολότερη κατανόηση ενός μοντέλου δικτύωσης, κάθε μοντέλο χωρίζει τις λειτουργίες σε έναν μικρό αριθμό κατηγοριών που ονομάζονται επίπεδα. Κάθε στρώμα περιλαμβάνει πρωτόκολλα και πρότυπα που σχετίζονται με τη συγκεκριμένη κατηγορία λειτουργιών, όπως δείχνει η παρακάτω εικόνα.



Εικόνα 1.1 Τα στρώματα του TCP/IP και κάποια από τα πρωτόκολλα κάθε στρώματος

Το μοντέλο TCP/IP δείχνει τους πιο συνηθισμένους όρους και τα επίπεδα που χρησιμοποιούνται όταν οι άνθρωποι μιλούν για το TCP/IP σήμερα. Το κατώτερο επίπεδο επικεντρώνεται στον τρόπο μετάδοσης των bits σε κάθε μεμονωμένη σύνδεση. Το επίπεδο σύνδεσης δεδομένων επικεντρώνεται στην αποστολή δεδομένων μέσω ενός τύπου φυσικής σύνδεσης: για παράδειγμα, τα δίκτυα χρησιμοποιούν διαφορετικά πρωτόκολλα σύνδεσης δεδομένων για τα τοπικά δίκτυα Ethernet σε σχέση με τα ασύρματα τοπικά δίκτυα. Το επίπεδο δικτύου επικεντρώνεται στην παράδοση δεδομένων σε ολόκληρη τη διαδρομή από τον αρχικό υπολογιστή αποστολής στον τελικό υπολογιστή προορισμού. Δύο ανώτερα στρώματα εστιάζουν περισσότερο στις εφαρμογές που πρέπει να στέλνουν και να λαμβάνουν δεδομένα.

Ένα μοντέλο δικτύωσης, που μερικές φορές ονομάζεται επίσης αρχιτεκτονική δικτύωσης αναφέρεται σε ένα ολοκληρωμένο σύνολο εγγράφων. Μεμονωμένα, κάθε έγγραφο περιγράφει μια μικρή λειτουργία

που απαιτείται για ένα δίκτυο, συλλογικά αυτά τα έγγραφα καθορίζουν όλα όσα πρέπει να συμβαίνουν για να λειτουργήσει ένα δίκτυο υπολογιστών. Ορισμένα έγγραφα ορίζουν ένα πρωτόκολλο, το οποίο είναι ένα σύνολο λογικών κανόνων που πρέπει να ακολουθούν οι συσκευές για να επικοινωνούν. Άλλα έγγραφα ορίζουν ορισμένες φυσικές απαιτήσεις για τη δικτύωση. Για παράδειγμα, ένα έγγραφο μπορεί να ορίζει τα επίπεδα τάσης και ρεύματος που χρησιμοποιούνται σε ένα συγκεκριμένο καλώδιο κατά τη μετάδοση δεδομένων. Το μοντέλο TCP/IP ορίζει και παραπέμπει σε μια μεγάλη συλλογή πρωτοκόλλων που επιτρέπουν στους υπολογιστές να επικοινωνούν. Για τον ορισμό ενός πρωτοκόλλου, το TCP/IP χρησιμοποιεί έγγραφα που ονομάζονται RFC(Request for Comments) [1]

Το μοντέλο TCP/IP δημιουργεί ένα σύνολο κανόνων που επιτρέπει σε όλους εμάς να βγάλουμε έναν υπολογιστή (ή μια κινητή συσκευή) από το κουτί, να συνδέσουμε όλα τα σωστά καλώδια, να τον ενεργοποιήσουμε και να συνδεθούμε και να χρησιμοποιήσουμε το δίκτυο. Μπορείτε να χρησιμοποιήσετε ένα πρόγραμμα περιήγησης ιστού για να συνδεθείτε στον αγαπημένο σας ιστότοπο, να χρησιμοποιήσετε σχεδόν οποιαδήποτε εφαρμογή και όλα λειτουργούν. Το λειτουργικό σύστημα του υπολογιστή υλοποιεί τμήματα του μοντέλου TCP/IP. Η κάρτα Ethernet ή η κάρτα ασύρματου Local Area Network(LAN) που είναι ενσωματωμένη στον υπολογιστή υλοποιεί ορισμένα πρότυπα LAN που αναφέρονται στο μοντέλο TCP/IP. Εν ολίγοις, οι προμηθευτές που δημιούργησαν το υλικό και το λογισμικό υλοποίησαν το TCP/IP.

1.3 Επίπεδο εφαρμογών TCP/IP

Τα πρωτόκολλα επιπέδου εφαρμογών TCP/IP παρέχουν υπηρεσίες στο λογισμικό εφαρμογών που εκτελείται σε έναν υπολογιστή. Το επίπεδο εφαρμογής δεν ορίζει την ίδια την εφαρμογή, αλλά ορίζει τις υπηρεσίες που χρειάζονται οι εφαρμογές. Για παράδειγμα, το πρωτόκολλο εφαρμογής HTTP ορίζει τον τρόπο με τον οποίο οι φυλλομετρητές ιστού μπορούν να αντλήσουν το περιεχόμενο μιας ιστοσελίδας από έναν διακομιστή ιστού. Το επίπεδο εφαρμογής παρέχει μια διεπαφή μεταξύ του λογισμικού που εκτελείται σε έναν υπολογιστή και του ίδιου του δικτύου.

Αναμφισβήτητα, η πιο δημοφιλής εφαρμογή TCP/IP σήμερα είναι ο περιηγητής ιστού. Πολλοί μεγάλοι προμηθευτές λογισμικού είτε έχουν ήδη αλλάξει είτε αλλάζουν το λογισμικό εφαρμογών τους ώστε να υποστηρίζουν την πρόσβαση από ένα πρόγραμμα περιήγησης ιστού. Η χρήση ενός προγράμματος περιήγησης ιστού είναι εύκολη: Ξεκινάτε ένα πρόγραμμα περιήγησης ιστού στον υπολογιστή σας και επιλέγετε έναν ιστότοπο πληκτρολογώντας το όνομα του ιστότοπου και εμφανίζεται η ιστοσελίδα.

Φανταστείτε ότι ο χρήστης Α ανοίγει το πρόγραμμα περιήγησης. Το πρόγραμμα περιήγησής του έχει ρυθμιστεί ώστε να ζητάει αυτόματα την προεπιλεγμένη ιστοσελίδα ή αρχική σελίδα του διακομιστή ιστού του χρήστη Β. Το αρχικό αίτημα του χρήστη Α ζητά από τον χρήστη Β να στείλει την αρχική του σελίδα πίσω στον χρήστη Α. Το λογισμικό του διακομιστή ιστού του χρήστη Β έχει ρυθμιστεί ώστε να γνωρίζει ότι η προεπιλεγμένη ιστοσελίδα περιέχεται σε ένα αρχείο που ονομάζεται home.html. Ο χρήστης Α λαμβάνει το αρχείο από τον χρήστη Β και εμφανίζει τα περιεχόμενα του αρχείου στο παράθυρο του προγράμματος περιήγησης ιστού του.

1.3.1 Μηχανισμοί πρωτοκόλλου HTTP

Το παράδειγμα δείχνει πώς οι εφαρμογές σε κάθε υπολογιστή τελικού σημείου -συγκεκριμένα, η εφαρμογή του προγράμματος περιήγησης ιστού και η εφαρμογή του διακομιστή ιστού- χρησιμοποιούν ένα πρωτόκολλο επιπέδου εφαρμογής TCP/IP. Για να κάνουν την αίτηση για μια ιστοσελίδα και να επιστρέψουν τα περιεχόμενα της ιστοσελίδας, οι εφαρμογές χρησιμοποιούν το πρωτόκολλο μεταφοράς υπερκειμένου (HTTP).

Η πλήρης έκδοση των περισσότερων διευθύνσεων ιστού -που ονομάζεται επίσης Ενιαίοι Εντοπιστές Πόρων (URL, Uniform Resource Locator)- αρχίζει με τα γράμματα http, πράγμα που σημαίνει ότι το HTTP χρησιμοποιείται για τη μεταφορά των ιστοσελίδων.

Για να λάβει την ιστοσελίδα από τον χρήστη Β, ο χρήστης Α στέλνει ένα μήνυμα με επικεφαλίδα HTTP. Γενικά, τα πρωτόκολλα χρησιμοποιούν επικεφαλίδες για να τοποθετούν πληροφορίες που χρησιμοποιούνται από το πρωτόκολλο. Αυτή η επικεφαλίδα HTTP περιλαμβάνει το αίτημα για «λήψη» ενός αρχείου. Το αίτημα περιέχει συνήθως το όνομα του αρχείου (home.html, στην προκειμένη περίπτωση), ή αν δεν αναφέρεται όνομα αρχείου, ο διακομιστής ιστού υποθέτει ότι ο χρήστης Α θέλει την προεπιλεγμένη ιστοσελίδα.

Η απάντηση από τον διακομιστή ιστού του χρήστη Β αρχίζει με μια επικεφαλίδα HTTP, με έναν κωδικό επιστροφής (200), που σημαίνει κάτι τόσο απλό όσο το «OK» που επιστρέφεται στην επικεφαλίδα. Το HTTP ορίζει και άλλους κωδικούς επιστροφής, ώστε ο διακομιστής να μπορεί να ενημερώσει το πρόγραμμα περιήγησης αν το αίτημα λειτούργησε. Το δεύτερο μήνυμα περιλαμβάνει επίσης το πρώτο μέρος του ζητούμενου αρχείου.

1.4 Επίπεδο μεταφοράς TCP/IP

Αν και υπάρχουν πολλά πρωτόκολλα επιπέδου εφαρμογής TCP/IP, το επίπεδο μεταφοράς TCP/IP περιλαμβάνει μικρότερο αριθμό πρωτοκόλλων. Τα δύο πιο συχνά χρησιμοποιούμενα πρωτόκολλα επιπέδου μεταφοράς είναι το Πρωτόκολλο Ελέγχου Μετάδοσης (TCP) και το Πρωτόκολλο Δεδομένων Χρήστη (User Datagram Protocol-UDP).

Τα πρωτόκολλα επιπέδου μεταφοράς παρέχουν υπηρεσίες στα πρωτόκολλα επιπέδου εφαρμογής που βρίσκονται ένα επίπεδο υψηλότερα στο μοντέλο TCP/IP. Αυτή η ενότητα εισάγει αυτή τη γενική έννοια εστιάζοντας σε μια μόνο υπηρεσία που παρέχει το TCP: την αποκατάσταση σφαλμάτων.

1.4.1 Βασικά στοιχεία της αποκατάστασης σφαλμάτων TCP

Για να κατανοήσετε τι κάνουν τα πρωτόκολλα του επιπέδου μεταφοράς, πρέπει να σκεφτείτε το επίπεδο πάνω από το επίπεδο μεταφοράς, το επίπεδο εφαρμογής. Κάθε στρώμα παρέχει μια υπηρεσία στο στρώμα που βρίσκεται πάνω από αυτό, όπως η υπηρεσία ανάκτησης σφαλμάτων που παρέχεται στα πρωτόκολλα του επιπέδου εφαρμογής από το TCP.

Για παράδειγμα, ο χρήστης Α και ο χρήστης Β χρησιμοποίησαν το HTTP για να μεταφέρουν την αρχική σελίδα από τον διακομιστή ιστού του χρήστη Β στο πρόγραμμα περιήγησης ιστού του χρήστη Α. Τι θα συνέβαινε όμως αν η αίτηση HTTP GET του χρήστη Α είχε χαθεί κατά τη μεταφορά της μέσω του δικτύου TCP/IP; Ή, τι θα συνέβαινε αν είχε χαθεί η απάντηση του χρήστη Β η οποία περιλάμβανε τα περιεχόμενα της αρχικής σελίδας; Σε κάθε περίπτωση, η σελίδα δεν θα εμφανιζόταν στο πρόγραμμα περιήγησης του χρήστη Α.

Το TCP/IP χρειάζεται έναν μηχανισμό που να εγγυάται την παράδοση δεδομένων σε ένα δίκτυο. Επειδή πολλά πρωτόκολλα επιπέδου εφαρμογής πιθανόν να θέλουν έναν τρόπο να εγγυώνται την παράδοση δεδομένων σε ένα δίκτυο, οι δημιουργοί του TCP συμπεριέλαβαν μια λειτουργία ανάκτησης σφαλμάτων. Για την ανάκτηση από σφάλματα, το TCP χρησιμοποιεί την έννοια των επιβεβαιώσεων. Για να επανέλθουμε στο προηγούμενο παράδειγμα ο διακομιστής ιστού του χρήστη Β στέλνει μια ιστοσελίδα στον περιηγητή ιστού του χρήστη Α χρησιμοποιώντας τρία ξεχωριστά μηνύματα. Η επικεφαλίδα TCP έχει έναν αριθμό ακολουθίας (SEQ) με κάθε μήνυμα. Σε αυτό το παράδειγμα, το δίκτυο έχει πρόβλημα και το δίκτυο αποτυγχάνει να παραδώσει το μήνυμα TCP (που ονομάζεται τμήμα-

segment) με αριθμό ακολουθίας 2. Όταν ο χρήστης Α λαμβάνει μηνύματα με αριθμούς ακολουθίας 1 και 3, αλλά δεν λαμβάνει μήνυμα με αριθμό ακολουθίας 2, αντιλαμβάνεται ότι το μήνυμα 2 χάθηκε. Αυτή η συνειδητοποίηση από τη λογική TCP του χρήστη Α τον αναγκάζει να στείλει ένα τμήμα TCP πίσω στον χρήστη Β, ζητώντας από τον χρήστη Β να στείλει ξανά το μήνυμα 2. [2]

Για κάθε μετάδοση δεδομένων αναθέτει ένα sequence number και ζητάει να λάβει ένα ACK από τον παραλήπτη για να επιβεβαιώσει ότι η παράδοση έγινε επιτυχώς. Αν δεν το λάβει, αναμεταδίδει το segment.

1.4.2 UDP και TCP ports(θύρες)

Αριθμοί θυρών (port numbers): Το TCP και το UDP χρησιμοποιούν αριθμούς θυρών για να διακρίνουν μεταξύ διαφορετικών τύπων δικτυακής κίνησης. Κάθε εφαρμογή ή υπηρεσία που εκτελείται σε μια συσκευή ακούει σε μια συγκεκριμένη θύρα:

Γνωστές θύρες (well-known ports): Οι αριθμοί θυρών από 0 έως 1023 θεωρούνται «γνωστές θύρες» και εκχωρούνται σε κοινές υπηρεσίες (π.χ. το HTTP χρησιμοποιεί τη θύρα 80, το HTTPS χρησιμοποιεί τη θύρα 443, το FTP χρησιμοποιεί τις θύρες 20 και 21).

Εγγεγραμμένες θύρες (registered ports): Οι θύρες από 1024 έως 49151 είναι γνωστές ως «καταχωρημένες θύρες» και μπορούν να χρησιμοποιηθούν από εφαρμογές λογισμικού.

Δυναμικές/ιδιωτικές θύρες (dynamic/private ports): Οι θύρες από 49152 έως 65535 είναι γνωστές ως «δυναμικές» ή «ιδιωτικές» θύρες και χρησιμοποιούνται συνήθως για εφήμερες συνδέσεις

1.5 Επίπεδο δικτύου TCP/IP

Το επίπεδο εφαρμογής περιλαμβάνει πολλά πρωτόκολλα. Το επίπεδο μεταφοράς περιλαμβάνει λιγότερα πρωτόκολλα, τα TCP και UDP. Το στρώμα δικτύου TCP/IP περιλαμβάνει μικρό αριθμό πρωτοκόλλων, αλλά μόνο ένα σημαντικό πρωτόκολλο: το Πρωτόκολλο Διαδικτύου (IP). Το IP παρέχει αρκετές δυνατότητες, με σημαντικότερες τη διευθυνσιοδότηση και τη δρομολόγηση.

Τα επίπεδα εφαρμογής και μεταφοράς του TCP/IP λειτουργούν όπως το άτομο που στέλνει επιστολές μέσω της ταχυδρομικής υπηρεσίας. Αυτά τα ανώτερα στρώματα λειτουργούν με τον ίδιο τρόπο, ανεξάρτητα από το αν οι υπολογιστές-hosts των τελικών σημείων βρίσκονται στο ίδιο LAN ή αν τους χωρίζει ολόκληρο το Διαδίκτυο. Για να στείλουν ένα μήνυμα, αυτά τα ανώτερα στρώματα ζητούν από το στρώμα που βρίσκεται κάτω από αυτά, το στρώμα δικτύου, να παραδώσει το μήνυμα.

Τα κατώτερα στρώματα του μοντέλου TCP/IP ενεργούν περισσότερο σαν την ταχυδρομική υπηρεσία για να παραδώσουν αυτά τα μηνύματα στους σωστούς προορισμούς. Για να το κάνουν αυτό, αυτά τα κατώτερα στρώματα πρέπει να κατανοήσουν το υποκείμενο φυσικό δίκτυο, επειδή πρέπει να επιλέξουν πώς θα παραδώσουν καλύτερα τα δεδομένα από τον έναν κεντρικό υπολογιστή στον άλλο.

Το επίπεδο δικτύου του μοντέλου δικτύωσης TCP/IP, το οποίο ορίζεται κυρίως από το Πρωτόκολλο Διαδικτύου (IP), λειτουργεί όπως η ταχυδρομική υπηρεσία. Το IP ορίζει ότι κάθε κεντρικός υπολογιστής πρέπει να έχει διαφορετική διεύθυνση IP, όπως ακριβώς η ταχυδρομική υπηρεσία ορίζει τη διευθυνσιοδότηση που επιτρέπει μοναδικές διευθύνσεις για κάθε σπίτι, διαμέρισμα και επιχείρηση. Ομοίως, το IP ορίζει τη διαδικασία δρομολόγησης, ώστε οι συσκευές που ονομάζονται δρομολογητές να μπορούν να λειτουργούν όπως το ταχυδρομείο, προωθώντας πακέτα δεδομένων ώστε να παραδίδονται στους σωστούς προορισμούς. Ακριβώς όπως η ταχυδρομική υπηρεσία δημιούργησε την απαραίτητη υποδομή για την παράδοση επιστολών - ταχυδρομεία, μηχανές διαλογής, φορτηγά,

αεροπλάνα και προσωπικό - το επίπεδο δικτύου ορίζει τις λεπτομέρειες για το πώς πρέπει να δημιουργηθεί μια δικτυακή υποδομή, ώστε το δίκτυο να μπορεί να παραδίδει δεδομένα σε όλους τους υπολογιστές του δικτύου.

1.5.1 Βασικά στοιχεία διευθυνσιοδότησης πρωτοκόλλου διαδικτύου

Το IP ορίζει διευθύνσεις για διάφορους σημαντικούς λόγους. Κάθε συσκευή που χρησιμοποιεί το TCP/IP χρειάζεται μια μοναδική διεύθυνση ώστε να μπορεί να αναγνωριστεί στο δίκτυο. Το IP ορίζει επίσης τον τρόπο ομαδοποίησης των διευθύνσεων, όπως ακριβώς το ταχυδρομικό σύστημα ομαδοποιεί τις διευθύνσεις με βάση τους ταχυδρομικούς κώδικες.

Στο επίπεδο δικτύου του TCP/IP, υπάρχουν δύο επιλογές για το κύριο πρωτόκολλο γύρω από το οποίο περιστρέφονται όλες οι άλλες λειτουργίες του επιπέδου δικτύου: IP έκδοση 4 (IPv4) και IP έκδοση 6 (IPv6). Τόσο το IPv4 όσο και το IPv6 ορίζουν τα ίδια είδη λειτουργιών του επιπέδου δικτύου, αλλά με διαφορετικές λεπτομέρειες. Θα γίνει μελέτη μόνο του IPv4 και των λεπτομερειών του.

Η μάσκα υποδικτύου (subnet mask) είναι ένας αριθμός 32 bit που χρησιμοποιείται για να διαιρέσει μια διεύθυνση IP σε τμήματα δικτύου (network) και συσκευής εντός δικτύου (host). Βοηθά τις συσκευές δικτύου, όπως οι δρομολογητές, να καθορίσουν αν ένα πακέτο πρέπει να δρομολογηθεί τοπικά ή να σταλεί σε διαφορετικό δίκτυο. Για παράδειγμα, μια διεύθυνση IP (π.χ. 192.168.1.10) είναι ένας αριθμός 32 bit που προσδιορίζει μοναδικά μια συσκευή σε ένα δίκτυο. Μια μάσκα υποδικτύου βοηθάει στο σπάσιμο αυτού του αριθμού σε δύο μέρη: το τμήμα δικτύου (το οποίο προσδιορίζει το δίκτυο στο οποίο ανήκει μια συσκευή) και το τμήμα που προσδιορίζει τη συγκεκριμένη συσκευή εντός αυτού του δικτύου. Μια μάσκα υποδικτύου 255.255.255.0 σημαίνει ότι οι τρεις πρώτες οκτάδες της διεύθυνσης IP καθορίζουν το δίκτυο και η τελευταία οκτάδα τον κεντρικό υπολογιστή. Για παράδειγμα, όλες οι συσκευές με διευθύνσεις IP στην περιοχή 192.168.1.0 έως 192.168.1.255 θα θεωρούνταν μέρος του ίδιου δικτύου (υποδικτύου) όταν χρησιμοποιείται αυτή η μάσκα υποδικτύου.

Η διαδικασία διαίρεσης ενός μεγαλύτερου δικτύου σε μικρότερα, πιο διαχειρίσιμα δίκτυα (υποδίκτυα) ονομάζεται υποδικτύωση. Οι μάσκες υποδικτύου είναι ζωτικής σημασίας για τη διαδικασία αυτή, επιτρέποντας την αποδοτικότερη χρήση των διευθύνσεων IP και την καλύτερη τμηματοποίηση του δικτύου.

Οι δρομολογητές είναι συσκευές δικτύωσης που συνδέουν τα μέρη του δικτύου TCP/IP μεταξύ τους με σκοπό τη δρομολόγηση (προώθηση) των πακέτων IP στο σωστό προορισμό. Οι δρομολογητές κάνουν το ισοδύναμο της εργασίας που κάνει κάθε θέση του ταχυδρομείου: Λαμβάνουν πακέτα IP σε διάφορες φυσικές διεπαφές, λαμβάνουν αποφάσεις με βάση τη διεύθυνση IP που περιλαμβάνεται στο πακέτο και στη συνέχεια προωθούν φυσικά το πακέτο σε κάποια άλλη διεπαφή δικτύου

Οι δρομολογητές χρησιμοποιούν τη μάσκα υποδικτύου για να προσδιορίσουν αν η διεύθυνση IP προορισμού ενός πακέτου βρίσκεται στο ίδιο δίκτυο ή σε διαφορετικό δίκτυο. Εάν οι διευθύνσεις IP βρίσκονται στο ίδιο δίκτυο (βάσει της μάσκας υποδικτύου), ο δρομολογητής θα προωθήσει το πακέτο απευθείας στη συσκευή προορισμού. Εάν βρίσκονται σε διαφορετικά δίκτυα, ο δρομολογητής θα προωθήσει το πακέτο σε έναν άλλο δρομολογητή που μπορεί να το δρομολογήσει στο σωστό δίκτυο.

Ας ανατρέξουμε πάλι στον χρήστη Α και τον χρήστη Β αλλά τώρα, χωρίς να αγνοείται το δίκτυο μεταξύ αυτών των δύο υπολογιστών.

Κάθε διεύθυνση IP αποτελείται από τέσσερις αριθμούς που χωρίζονται με τελείες. Σε αυτή την περίπτωση, ο χρήστης Β χρησιμοποιεί τη διεύθυνση IP 1.1.1.1 και ο χρήστης Α χρησιμοποιεί τη

διεύθυνση 2.2.2.2. Αυτό το στυλ αριθμού ονομάζεται dotted decimal notation (DDN). Για να επικοινωνήσει ο χρήστης A με τον χρήστη B δεδομένου ότι ανήκουν σε διαφορετικά δίκτυα χρησιμοποιούνται δρομολογητές (routers).

1.5.2 Βασικά στοιχεία δρομολόγησης IP

Το επίπεδο δικτύου TCP/IP, χρησιμοποιώντας το πρωτόκολλο IP, παρέχει μια υπηρεσία προώθησης πακέτων IP από μια συσκευή σε μια άλλη. Οποιαδήποτε συσκευή με διεύθυνση IP μπορεί να συνδεθεί στο δίκτυο TCP/IP και να στέλνει ή να λαμβάνει πακέτα. Παρουσιάζεται ένα βασικό παράδειγμα δρομολόγησης IP

Στην γνωστή περίπτωση στην οποία ο διακομιστής ιστού του χρήστη B θέλει να στείλει μέρος μιας ιστοσελίδας στον χρήστη A αλλά τώρα με λεπτομέρειες που σχετίζονται με το IP. Ο διακομιστής έχει τα γνωστά δεδομένα εφαρμογής, την επικεφαλίδα HTTP και την επικεφαλίδα TCP έτοιμα για αποστολή. Επιπλέον, το μήνυμα περιέχει τώρα μια επικεφαλίδα IP. Η επικεφαλίδα IP περιλαμβάνει μια διεύθυνση IP πηγής της διεύθυνσης IP του χρήστη B (1.1.1.1) και μια διεύθυνση IP προορισμού της διεύθυνσης IP του χρήστη A (2.2.2.2). Ξεκινάμε με τον χρήστη B να είναι έτοιμος να στείλει ένα πακέτο IP. Η διεργασία IP του χρήστη B επιλέγει να στείλει το πακέτο σε κάποιο δρομολογητή - έναν κοντινό δρομολογητή στο ίδιο LAN - με την προσδοκία ότι ο δρομολογητής θα ξέρει πώς να προωθήσει το πακέτο. Ο χρήστης B δεν χρειάζεται να γνωρίζει τίποτα περισσότερο για την τοπολογία ή τους άλλους δρομολογητές.

Ο δρομολογητής R1 λαμβάνει το πακέτο IP και η διεργασία IP του R1 λαμβάνει μια απόφαση. Ο R1 εξετάζει τη διεύθυνση προορισμού (2.2.2.2), συγκρίνει αυτή τη διεύθυνση με τις γνωστές διαδρομές IP και επιλέγει να προωθήσει το πακέτο στον δρομολογητή R2. Αυτή η διαδικασία προώθησης του πακέτου IP ονομάζεται δρομολόγηση IP (ή απλώς δρομολόγηση).

Έπειτα ο δρομολογητής R2 επαναλαμβάνει το ίδιο είδος λογικής που χρησιμοποιείται από τον δρομολογητή R1. Η διαδικασία IP του R2 θα συγκρίνει τη διεύθυνση IP προορισμού του πακέτου (2.2.2.2.2) με τις γνωστές διαδρομές IP του R2 και θα επιλέξει να προωθήσει το πακέτο στον χρήστη A.

1.6 TCP/IP Data-Link και Physical Layers

Τα data-link και physical layers του μοντέλου TCP/IP καθορίζουν τα πρωτόκολλα και το υλικό που απαιτούνται για την παράδοση δεδομένων σε κάποιο φυσικό δίκτυο. Τα δύο αυτά στρώματα συνεργάζονται αρκετά στενά- στην πραγματικότητα, ορισμένα πρότυπα ορίζουν τόσο τις λειτουργίες του data link όσο και του physical layer. Το φυσικό επίπεδο ορίζει την καλωδίωση και την ενέργεια (για παράδειγμα, ηλεκτρικά σήματα) που ρέει μέσω των καλωδίων. Υπάρχουν ορισμένοι κανόνες και συμβάσεις κατά την αποστολή δεδομένων μέσω του καλωδίου, οι κανόνες αυτοί υπάρχουν στο επίπεδο σύνδεσης δεδομένων του μοντέλου TCP/IP.

Εστιάζοντας για λίγο στο επίπεδο σύνδεσης δεδομένων, όπως κάθε επίπεδο σε οποιοδήποτε μοντέλο δικτύωσης, το επίπεδο σύνδεσης δεδομένων TCP/IP παρέχει υπηρεσίες στο επίπεδο που βρίσκεται πάνω από αυτό στο μοντέλο (το επίπεδο δικτύου). Όταν η διεργασία IP ενός κεντρικού υπολογιστή ή δρομολογητή επιλέγει να στείλει ένα πακέτο IP σε έναν άλλο δρομολογητή ή κεντρικό υπολογιστή, ο εν λόγω κεντρικός υπολογιστής ή δρομολογητής χρησιμοποιεί στη συνέχεια λεπτομέρειες του επιπέδου σύνδεσης για να στείλει το πακέτο στον επόμενο κεντρικό υπολογιστή/δρομολογητή.

Κάθε επίπεδο παρέχει μια υπηρεσία στο επίπεδο που βρίσκεται πάνω από αυτό. Σε αυτό το παράδειγμα, η διεργασία IP του host χρήστη Β επιλέγει να στείλει το πακέτο IP σε έναν κοντινό δρομολογητή (R1). Ακολουθούν τα τέσσερα βήματα που συμβαίνουν στο επίπεδο σύνδεσης για να μπορέσει ο χρήστης Β να στείλει το πακέτο IP στον R1.

Βήμα 1. Ενθυλακώνει το πακέτο IP μεταξύ μιας επικεφαλίδας Ethernet και ενός τρέιλερ Ethernet, δημιουργώντας ένα πλαίσιο Ethernet.

Βήμα 2. Μεταδίδει φυσικά τα bits αυτού του πλαισίου Ethernet, χρησιμοποιώντας ηλεκτρική ενέργεια(σε άλλες περιπτώσεις φως) που ρέει μέσω της καλωδίωσης Ethernet.

Βήμα 3. Ο δρομολογητής R1 λαμβάνει φυσικά το ηλεκτρικό σήμα μέσω ενός καλωδίου και δημιουργεί εκ νέου τα ίδια bits ερμηνεύοντας τη σημασία των ηλεκτρικών σημάτων.

Βήμα 4. Ο δρομολογητής R1 αποενθυλακώνει το πακέτο IP από το πλαίσιο Ethernet αφαιρώντας επικεφαλίδα και το τρέιλερ Ethernet.

Στο τέλος αυτής της διαδικασίας, ο χρήστης Β και ο R1 έχουν συνεργαστεί για να παραδώσουν το πακέτο από τον χρήστη Β στον δρομολογητή R1.

Τα φυσικά επίπεδα TCP/IP και τα επίπεδα σύνδεσης δεδομένων περιλαμβάνουν δύο διαφορετικές λειτουργίες, λειτουργίες που σχετίζονται με τη φυσική μετάδοση των δεδομένων, καθώς και τα πρωτόκολλα και τους κανόνες που ελέγχουν τη χρήση του φυσικού μέσου.

1.6.1 Ορολογία ενθυλάκωσης δεδομένων(Data Encapsulation)

Τα HTTP, TCP, IP και Ethernet, όταν στέλνουν δεδομένα, κάθε επίπεδο προσθέτει τη δική του επικεφαλίδα (και για τα πρωτόκολλα σύνδεσης δεδομένων, επίσης ένα trailer) στα δεδομένα που παρέχονται από το ανώτερο επίπεδο. Ο όρος ενθυλάκωση αναφέρεται στη διαδικασία τοποθέτησης επικεφαλίδων (και στο 2^{ο} επίπεδο και trailer) γύρω από κάποια δεδομένα.

Πολλά από τα παραδείγματα παρουσιάζουν τη διαδικασία ενθυλάκωσης. Για παράδειγμα, ο διακομιστής ιστού του χρήστη Β ενθυλάκωσε τα περιεχόμενα της αρχικής σελίδας μέσα σε μια επικεφαλίδα HTTP. Το επίπεδο TCP ενθυλάκωσε τις επικεφαλίδες HTTP και τα δεδομένα μέσα σε μια επικεφαλίδα TCP. Το επίπεδο IP ενθυλάκωσε τις επικεφαλίδες TCP και τα δεδομένα μέσα σε μια επικεφαλίδα IP. Τέλος, το επίπεδο σύνδεσης Ethernet ενθυλάκωσε τα πακέτα IP μέσα σε μια επικεφαλίδα και ένα τρέιλερ.

Η διαδικασία με την οποία ένας κεντρικός υπολογιστής TCP/IP στέλνει δεδομένα μπορεί να θεωρηθεί ως μια διαδικασία πέντε βημάτων [3]. Τα τέσσερα πρώτα βήματα αφορούν την ενθυλάκωση που πραγματοποιείται από τα τέσσερα επίπεδα TCP/IP και το τελευταίο βήμα είναι η πραγματική φυσική μετάδοση των δεδομένων από τον κεντρικό υπολογιστή. Στην πραγματικότητα, αν χρησιμοποιήσετε το μοντέλο TCP/IP πέντε επιπέδων, ένα βήμα αντιστοιχεί στο ρόλο κάθε επιπέδου. Τα βήματα κατά την αποστολή συνοψίζονται:

Βήμα 1. Δημιουργία και ενθυλάκωση των δεδομένων της εφαρμογής με τις απαιτούμενες επικεφαλίδες επιπέδου εφαρμογής. Για παράδειγμα, το μήνυμα HTTP OK μπορεί να επιστραφεί σε μια επικεφαλίδα HTTP, ακολουθούμενη από μέρος του περιεχομένου μιας ιστοσελίδας.

Βήμα 2. Ενθυλάκωση των δεδομένων που παρέχονται από το επίπεδο εφαρμογής μέσα σε μια επικεφαλίδα επιπέδου μεταφοράς. Για εφαρμογές τελικού χρήστη, χρησιμοποιείται συνήθως μια επικεφαλίδα TCP ή UDP.

Βήμα 3. Ενθυλάκωση των δεδομένων που παρέχονται από το επίπεδο μεταφοράς μέσα σε μια επικεφαλίδα επιπέδου δικτύου (IP). Το IP ορίζει τις διευθύνσεις IP που προσδιορίζουν μοναδικά κάθε υπολογιστή.

Βήμα 4. Ενθυλάκωση των δεδομένων που παρέχονται από το επίπεδο δικτύου μέσα σε μια επικεφαλίδα και ένα trailer του επιπέδου σύνδεσης δεδομένων.

Βήμα 5. Μετάδοση των bits. Το φυσικό στρώμα κωδικοποιεί ένα σήμα στο μέσο για τη μετάδοση του πλαισίου.

1.7 Επίλογος

Σε αυτό το κεφάλαιο είδαμε το μοντέλο TCP/IP, τα επιμέρους επίπεδα του και τις διεργασίες που γίνονται σε κάθε επίπεδο.

Κεφάλαιο 2ο: Βασικές αρχές των Ethernet LANs

2.1 Εισαγωγή

Τα περισσότερα δίκτυα υπολογιστών επιχειρήσεων μπορούν να διαχωριστούν σε δύο γενικούς τύπους τεχνολογίας: τοπικά δίκτυα (LANs) και δίκτυα ευρείας περιοχής (WANs). Τα LAN συνήθως συνδέουν κοντινές συσκευές: συσκευές στο ίδιο δωμάτιο, στο ίδιο κτίριο ή σε μια πανεπιστημιούπολη. Αντίθετα, τα WAN συνδέουν συσκευές που βρίσκονται συνήθως σε σχετικά μεγάλη απόσταση μεταξύ τους. Μαζί, τα LAN και τα WAN δημιουργούν ένα πλήρες δίκτυο υπολογιστών της επιχείρησης, συνεργαζόμενα για να κάνουν τη δουλειά ενός δικτύου υπολογιστών: να παραδίδουν δεδομένα από τη μια συσκευή στην άλλη.

Με την πάροδο των ετών έχουν υπάρξει πολλοί τύποι LAN, αλλά τα σημερινά δίκτυα χρησιμοποιούν δύο γενικούς τύπους LAN: Τα ενσύρματα τοπικά δίκτυα και τα ασύρματα τοπικά δίκτυα. Τα ενσύρματα τοπικά δίκτυα χρησιμοποιούν καλώδια για τις συνδέσεις μεταξύ των κόμβων. Υπάρχουν πολλοί τύποι καλωδίων, τα τοπικά δίκτυα Ethernet που χρησιμοποιούν χάλκινα καλώδια συχνά αποκαλούνται ενσύρματα τοπικά δίκτυα. Τα τοπικά δίκτυα Ethernet κάνουν επίσης χρήση καλωδίωσης οπτικών ινών, η οποία περιλαμβάνει έναν πυρήνα από γυαλί που χρησιμοποιούν οι συσκευές για την αποστολή δεδομένων με τη χρήση φωτός. Σε σύγκριση με το Ethernet, τα ασύρματα τοπικά δίκτυα δεν χρησιμοποιούν καλώδια , αλλά ραδιοκύματα για τις συνδέσεις μεταξύ των κόμβων.

Ο όρος Ethernet αναφέρεται σε μια οικογένεια προτύπων τοπικών δικτύων που μαζί καθορίζουν τα επίπεδα σύνδεσης δεδομένων της πιο δημοφιλούς παγκοσμίως τεχνολογίας ενσύρματων τοπικών δικτύων. Τα πρότυπα, που ορίζονται από το Ινστιτούτο Ηλεκτρολόγων και Ηλεκτρονικών Μηχανικών (IEEE), καθορίζουν την καλωδίωση, τους συνδέσμους στα άκρα των καλωδίων, τους κανόνες πρωτοκόλλου και ό,τι άλλο απαιτείται για τη δημιουργία ενός τοπικού δικτύου Ethernet. [4]

2.2 Τυπικά τοπικά δίκτυα SOHO(Small office/Home Office)

Αν σκεφτεί κανείς πρώτα ένα τοπικό δίκτυο μικρού γραφείου/οικιακού γραφείου (SOHO) σήμερα, συγκεκριμένα ένα τοπικό δίκτυο που χρησιμοποιεί μόνο την τεχνολογία Ethernet LAN. Πρώτον, το LAN χρειάζεται μια συσκευή που ονομάζεται μεταγωγέας Ethernet LAN(switch), ο οποίος παρέχει πολλές φυσικές θύρες στις οποίες μπορούν να συνδεθούν καλώδια. Ένα Ethernet καλώδιο είναι μια γενική αναφορά σε οποιοδήποτε καλώδιο που συμμορφώνεται με οποιοδήποτε από τα διάφορα πρότυπα Ethernet. Το τοπικό δίκτυο χρησιμοποιεί καλώδια Ethernet για να συνδέσει διάφορες συσκευές ή κόμβους σε μία από τις θύρες του μεταγωγέα.

Μια σύνηθης μορφή είναι η εξής: Ένας μοναδικός μεταγωγέας LAN, πέντε καλώδια και πέντε άλλους κόμβους Ethernet: τρεις υπολογιστές, έναν εκτυπωτή και μια συσκευή δικτύου που ονομάζεται δρομολογητής(ο δρομολογητής συνδέει το LAN με το WAN). Πολλά SOHO Ethernet LAN συνδυάζουν σήμερα το δρομολογητή και το μεταγωγέα σε μία μόνο συσκευή. Οι προμηθευτές πωλούν ολοκληρωμένες συσκευές δικτύωσης που λειτουργούν ως δρομολογητής και μεταγωγέας Ethernet, καθώς και άλλες λειτουργίες. Αυτές οι συσκευές συνήθως αναγράφουν «δρομολογητής» στη συσκευασία, αλλά πολλά μοντέλα διαθέτουν επίσης θύρες μεταγωγέα Ethernet LAN τεσσάρων ή οκτώ θυρών ενσωματωμένες στη συσκευή.

Τα τυπικά LAN SOHO σήμερα υποστηρίζουν επίσης ασύρματες συνδέσεις LAN. Μπορείτε να δημιουργήσετε ένα ενιαίο SOHO LAN που περιλαμβάνει τόσο την τεχνολογία Ethernet LAN όσο και την τεχνολογία ασύρματου LAN, η οποία επίσης ορίζεται από το IEEE. Τα ασύρματα LAN, που ορίζονται από το IEEE χρησιμοποιώντας πρότυπα που αρχίζουν με το 802.11, χρησιμοποιούν ραδιοκύματα για την αποστολή των bits από τον ένα κόμβο στον άλλο.

Τα περισσότερα ασύρματα τοπικά δίκτυα βασίζονται σε μια ακόμη συσκευή δικτύωσης, ένα σημείο πρόσβασης(Access Point AP) ασύρματου τοπικού δικτύου. Το AP λειτουργεί σαν switch καθώς όλοι οι κόμβοι του ασύρματου LAN επικοινωνούν με το ασύρματο AP. Εάν το δίκτυο χρησιμοποιεί ένα AP που είναι μια ξεχωριστή φυσική συσκευή, το AP χρειάζεται τότε μια μοναδική σύνδεση Ethernet για να συνδέσει το AP με το τοπικό δίκτυο Ethernet,

Ωστόσο, τα περισσότερα δίκτυα SOHO σήμερα χρησιμοποιούν μία μόνο συσκευή, που συχνά χαρακτηρίζεται ως «ασύρματος δρομολογητής», η οποία εκτελεί όλες αυτές τις λειτουργίες.

2.3 Τυπικά εταιρικά LANs(Enterprise LANs)

Τα δίκτυα επιχειρήσεων έχουν παρόμοιες ανάγκες σε σύγκριση με ένα δίκτυο SOHO, αλλά σε πολύ μεγαλύτερη κλίμακα. Για παράδειγμα, τα επιχειρησιακά τοπικά δίκτυα Ethernet ξεκινούν με μεταγωγείς LAN που εγκαθίστανται σε μια ντουλάπα καλωδίωσης πίσω από μια κλειδωμένη πόρτα σε κάθε όροφο ενός κτιρίου. Οι ηλεκτρολόγοι εγκαθιστούν την καλωδίωση Ethernet από αυτή την ντουλάπα καλωδίωσης στα γραφεία και τις αίθουσες συνεδριάσεων όπου οι συσκευές μπορεί να χρειαστεί να συνδεθούν στο LAN. Ταυτόχρονα, οι περισσότερες επιχειρήσεις υποστηρίζουν επίσης ασύρματα LAN στον ίδιο χώρο, για να επιτρέπουν στους ανθρώπους να περιφέρονται και να εξακολουθούν να εργάζονται και για να υποστηρίζουν έναν αυξανόμενο αριθμό συσκευών που δεν διαθέτουν διασύνδεση Ethernet LAN.

Έστω ένα τυπικό εταιρικό LAN σε ένα τριώροφο κτίριο:

Κάθε όροφος διαθέτει έναν μεταγωγέα Ethernet και ένα ασύρματο Access Point. Για να επιτρέπεται η επικοινωνία μεταξύ των ορόφων, κάθε μεταγωγέας ανά όροφο συνδέεται με έναν κεντρικό μεταγωγέα διανομής (distribution switch). Για παράδειγμα, ο PC3 μπορεί να στείλει δεδομένα στον PC2, αλλά αυτά θα πρέπει πρώτα να περάσουν από τον μεταγωγέα SW3 στον πρώτο όροφο στον μεταγωγέα διανομής και στη συνέχεια να επιστρέψουν πίσω.

Ο τυπικός τρόπος σύνδεσης ενός LAN σε ένα WAN γίνεται με τη χρήση ενός δρομολογητή. Οι μεταγωγείς LAN και τα σημεία ασύρματης πρόσβασης λειτουργούν για τη δημιουργία του ίδιου του LAN. Οι δρομολογητές συνδέονται τόσο στο LAN όσο και στο WAN. Για να συνδεθεί στο LAN, ο δρομολογητής χρησιμοποιεί απλώς μια διασύνδεση Ethernet LAN και ένα καλώδιο Ethernet.

2.4 Διευθυνσιοδότηση Ethernet

Τα πεδία διευθύνσεων Ethernet πηγής και προορισμού παίζουν τεράστιο ρόλο στον τρόπο λειτουργίας των τοπικών δικτύων Ethernet. Η γενική ιδέα για το καθένα είναι σχετικά απλή: ο κόμβος αποστολής τοποθετεί τη δική του διεύθυνση στο πεδίο διεύθυνσης πηγής και τη διεύθυνση της συσκευής Ethernet προορισμού στο πεδίο διεύθυνσης προορισμού. Ο αποστολέας μεταδίδει το πλαίσιο, αναμένοντας ότι το Ethernet LAN, στο σύνολό του, θα παραδώσει το πλαίσιο σε αυτόν τον σωστό προορισμό.

Οι διευθύνσεις Ethernet, που ονομάζονται επίσης MAC addresses, είναι δυαδικοί αριθμοί μήκους 6 byte (48 bit) [5]. Για λόγους ευκολίας, οι περισσότεροι υπολογιστές παραθέτουν τις διευθύνσεις MAC ως 12ψήφιους δεκαεξαδικούς αριθμούς. Οι συσκευές της Cisco συνήθως προσθέτουν μερικές τελείες στον

αριθμό για ευκολότερη αναγνωσιμότητα- για παράδειγμα, ένα μεταγωγέας Cisco μπορεί να καταγράφει μια διεύθυνση MAC ως 0000.0A12.3456.

Οι περισσότερες διευθύνσεις MAC αντιπροσωπεύουν μία μόνο Network Interface Card (NIC) ή άλλη θύρα Ethernet, οπότε αυτές οι διευθύνσεις συχνά αποκαλούνται unicast. Ο όρος unicast είναι απλώς ένας επίσημος τρόπος για να αναφερθούμε στο γεγονός ότι η διεύθυνση αντιπροσωπεύει μία διασύνδεση στο τοπικό δίκτυο Ethernet. Σημαντικό είναι ότι η διεύθυνση που αποδίδεται σε μια NIC από έναν κατασκευαστή πρέπει να είναι μοναδική μεταξύ όλων των διευθύνσεων MAC στο κόσμο.

Εκτός από τις διευθύνσεις unicast, το Ethernet χρησιμοποιεί επίσης διευθύνσεις ομάδας(group addresses). Οι διευθύνσεις ομάδας προσδιορίζουν περισσότερες από μία κάρτες διασύνδεσης LAN. Ένα πλαίσιο που αποστέλλεται σε μια διεύθυνση ομάδας μπορεί να παραδοθεί σε ένα μικρό σύνολο συσκευών στο LAN ή ακόμη και σε όλες τις συσκευές στο LAN. Στην πραγματικότητα, το IEEE ορίζει δύο γενικές κατηγορίες διευθύνσεων ομάδας για το Ethernet:

Broadcast Address: Τα πλαίσια που αποστέλλονται σε αυτή τη διεύθυνση θα πρέπει να παραδίδονται σε όλες τις συσκευές στο LAN Ethernet. Έχει την τιμή FFFF.FFFF.FFFF.

Multicast Address: Τα πλαίσια που αποστέλλονται σε μια multicast διεύθυνση θα αντιγραφούν και θα προωθηθούν σε ένα υποσύνολο των συσκευών στο LAN που δέχονται πλαίσια που αποστέλλονται σε μια συγκεκριμένη διεύθυνση πολλαπλής διανομής.

2.5 Δρομολόγηση IP(IP Routing)

Το Πρωτόκολλο Διαδικτύου (IP) επικεντρώνεται στην εργασία της δρομολόγησης δεδομένων, με τη μορφή πακέτων IP, από τον κεντρικό υπολογιστή προέλευσης στον κεντρικό υπολογιστή προορισμού. Το IP δεν ασχολείται με τη φυσική μετάδοση των δεδομένων, αλλά βασίζεται στα κατώτερα στρώματα TCP/IP για τη φυσική μετάδοση των δεδομένων. Αντίθετα, η IP ασχολείται με τις λογικές λεπτομέρειες, και όχι με τις φυσικές λεπτομέρειες, της παράδοσης δεδομένων. Ειδικότερα, το επίπεδο δικτύου καθορίζει τον τρόπο με τον οποίο τα πακέτα ταξιδεύουν από άκρο σε άκρο σε ένα δίκτυο TCP/IP, ακόμη και όταν το πακέτο διασχίζει πολλούς διαφορετικούς τύπους συνδέσεων LAN και WAN.

2.5.1 Λογική δρομολόγησης (προώθησης) επιπέδου δικτύου

Οι δρομολογητές και οι υπολογιστές τελικού χρήστη (που ονομάζονται hosts σε ένα δίκτυο TCP/IP) συνεργάζονται για την εκτέλεση της δρομολόγησης IP. Το λειτουργικό σύστημα (OS) του κεντρικού υπολογιστή διαθέτει λογισμικό TCP/IP, συμπεριλαμβανομένου του λογισμικού που υλοποιεί το επίπεδο δικτύου. Οι κεντρικοί υπολογιστές χρησιμοποιούν αυτό το λογισμικό για να επιλέξουν πού θα στείλουν πακέτα IP, συχνά σε έναν κοντινό δρομολογητή. Αυτοί οι δρομολογητές κάνουν επιλογές για το πού θα στείλουν το πακέτο IP στη συνέχεια. Μαζί, οι κεντρικοί υπολογιστές και οι δρομολογητές παραδίδουν το πακέτο IP στον σωστό προορισμό. [6]

Έστω ότι έχουμε έναν υπολογιστή (PC1) ο οποίος έχει την IP 192.168.1.5 ο οποίος έχει προεπιλεγμένο δρομολογητή τον R1 και θέλει να επικοινωνήσει με έναν υπολογιστή (PC2) ο οποίος έχει την IP 192.168.2.5.Ανάμεσα τους υπάρχουν 3 δρομολογητές.

Ο R1 έχει ένα ethernet interface στο δίκτυο 192.168.1.0 με την IP 192.168.1.1 και ένα ethernet link με τον R2 με την IP 192.168.3.1.

Ο R2 με την IP 192.168.3.2 έχει ένα ethernet link με τον R1 και ένα ethernet link(Ethernet over MPLS, EoMPLS) με τον R3 με IP 192.168.4.1

Ο R3 έχει ένα ethernet interface στο δίκτυο 192.168.2.0 με την IP 192.168.2.1 και αντίστοιχα ένα ethernet link(Ethernet over MPLS, EoMPLS) με τον R2 με την IP 192.168.4.2

Σε αυτό το παράδειγμα, ο PC1 κάνει κάποια βασική ανάλυση και στη συνέχεια επιλέγει να στείλει το πακέτο IP στο δρομολογητή, έτσι ώστε ο δρομολογητής να προωθήσει το πακέτο. Ο PC1 αναλύει τη διεύθυνση προορισμού και συνειδητοποιεί ότι η διεύθυνση του PC2 (192.168.2.5) δεν βρίσκεται στο ίδιο LAN με τον PC1. Έτσι, η λογική του PC1 του λέει να στείλει το πακέτο σε μια συσκευή της οποίας η δουλειά είναι να γνωρίζει πού να δρομολογήσει τα δεδομένα: έναν κοντινό δρομολογητή, στο ίδιο LAN, που ονομάζεται προεπιλεγμένος δρομολογητής του PC1.

Για να στείλει το πακέτο IP στον προεπιλεγμένο δρομολογητή, ο αποστολέας στέλνει ένα data link frame μέσω του καλωδίου στον κοντινό δρομολογητή, αυτό το πλαίσιο περιλαμβάνει το πακέτο στο τμήμα δεδομένων του πλαισίου. Αυτό το πλαίσιο χρησιμοποιεί διευθυνσιοδότηση Layer 2 στην επικεφαλίδα σύνδεσης δεδομένων για να διασφαλίσει ότι ο κοντινός δρομολογητής λαμβάνει το πλαίσιο.

Η λογική των R1 και R2: Δρομολόγηση δεδομένων στο δίκτυο

Και οι δύο δρομολογητές χρησιμοποιούν την ίδια γενική διαδικασία για τη δρομολόγηση του πακέτου. Κάθε δρομολογητής διατηρεί έναν πίνακα δρομολόγησης IP (routing table). Αυτός ο πίνακας απαριθμεί ομαδοποιήσεις διευθύνσεων IP, που ονομάζονται δίκτυα IP και υποδίκτυα IP. Όταν ένας δρομολογητής λαμβάνει ένα πακέτο, συγκρίνει τη διεύθυνση IP προορισμού του πακέτου με τις καταχωρήσεις στον πίνακα δρομολόγησης και πραγματοποιεί μια αντιστοίχιση. Αυτή η εγγραφή αντιστοίχισης παραθέτει επίσης κατευθύνσεις που λένε στο δρομολογητή πού να προωθήσει το πακέτο στη συνέχεια.

Ο R1 θα είχε ταιριάξει τη διεύθυνση προορισμού (192.168.2.5) με μια καταχώρηση του πίνακα δρομολόγησης, η οποία με τη σειρά της θα έλεγε στον R1 να στείλει το πακέτο στον R2 ως επόμενο. Ομοίως, ο R2 θα είχε αντιστοιχίσει μια καταχώρηση στον πίνακα δρομολόγησης που θα έλεγε στον R2 να στείλει το πακέτο, μέσω μιας σύνδεσης Ethernet WAN, στον R3.

Η λογική του R3: Ο τελευταίος δρομολογητής της διαδρομής, ο R3, χρησιμοποιεί σχεδόν την ίδια λογική με τους R1 και R2, αλλά με μια μικρή διαφορά. Ο R3 πρέπει να προωθήσει το πακέτο απευθείας στον PC2 και όχι σε κάποιον άλλο δρομολογητή.

2.5.2 Πώς η δρομολόγηση επιπέδου δικτύου χρησιμοποιεί τα LANs και τα WANs

Ενώ η λογική δρομολόγησης επιπέδου δικτύου αγνοεί τις φυσικές λεπτομέρειες μετάδοσης, τα bits εξακολουθούν να πρέπει να μεταδίδονται. Για να γίνει αυτή η εργασία, η λογική δρομολόγησης του επιπέδου δικτύου σε έναν κεντρικό υπολογιστή ή δρομολογητή πρέπει να παραδώσει το πακέτο στα πρωτόκολλα του επιπέδου σύνδεσης δεδομένων, τα οποία, με τη σειρά τους, στέλνουν στο φυσικό επίπεδο να μεταδώσει τα πραγματικά δεδομένα. Το επίπεδο σύνδεσης δεδομένων προσθέτει την κατάλληλη επικεφαλίδα και το κατάλληλο τρέιλερ στο πακέτο, δημιουργώντας ένα πλαίσιο, πριν στείλει τα πλαίσια σε κάθε φυσικό δίκτυο.

Η διαδικασία δρομολόγησης προωθεί το πακέτο του επιπέδου δικτύου από άκρο σε άκρο μέσω του δικτύου, ενώ κάθε πλαίσιο σύνδεσης δεδομένων πραγματοποιεί μόνο ένα μικρότερο μέρος του ταξιδιού. Κάθε διαδοχικό πλαίσιο επιπέδου σύνδεσης δεδομένων μεταφέρει το πακέτο στην επόμενη συσκευή που διαχειρίζεται τη λογική δρομολόγησης του επιπέδου δικτύου.

Βήμα 1. Χρησιμοποιήστε το πεδίο FCS (Frame Check Sequence) του data link frame για να βεβαιωθείτε ότι το πλαίσιο δεν είχε σφάλματα- αν υπάρχουν σφάλματα, απορρίψτε το πλαίσιο.

Βήμα 2. Υποθέτοντας ότι το πλαίσιο δεν απορρίφθηκε στο Βήμα 1, απορρίψτε την παλιά επικεφαλίδα και το τρέιλερ σύνδεσης δεδομένων, αφήνοντας το πακέτο IP.

Βήμα 3. Συγκρίνετε τη διεύθυνση IP προορισμού του πακέτου IP με τον πίνακα δρομολόγησης και βρείτε τη διαδρομή που ταιριάζει καλύτερα με τη διεύθυνση προορισμού. Αυτή η διαδρομή προσδιορίζει την εξερχόμενη διασύνδεση του δρομολογητή και ενδεχομένως τη διεύθυνση IP του επόμενου δρομολογητή στην πορεία(next hop).

Βήμα 4. Ενθυλακώστε το πακέτο IP μέσα σε μια νέα επικεφαλίδα σύνδεσης δεδομένων και ένα τρέιλερ, κατάλληλα για την εξερχόμενη διασύνδεση, και προωθήστε το πλαίσιο.

Η παρακάτω λίστα εξηγεί τη λογική προώθησης σε κάθε δρομολογητή, εστιάζοντας στον τρόπο με τον οποίο η δρομολόγηση επιδρά με το data link.

Βήμα Α. Ο PC1 στέλνει το πακέτο στον προεπιλεγμένο δρομολογητή του. Η λογική του επιπέδου δικτύου του PC1 κατασκευάζει το πακέτο IP, με διεύθυνση προορισμού τη διεύθυνση IP του PC2 (192.168.2.5). Το επίπεδο δικτύου εκτελεί επίσης την ανάλυση για να αποφασίσει ότι η διεύθυνση 192.168.2.5 δεν βρίσκεται στο τοπικό υποδίκτυο IP, οπότε ο PC1 πρέπει να στείλει το πακέτο στον R1 (τον προεπιλεγμένο δρομολογητή του PC1). Ο PC1 τοποθετεί το πακέτο IP σε ένα πλαίσιο σύνδεσης δεδομένων Ethernet, με διεύθυνση Ethernet προορισμού τη διεύθυνση Ethernet του R1. Ο PC1 στέλνει το πλαίσιο στο Ethernet.

Βήμα Β. Ο R1 επεξεργάζεται το εισερχόμενο πλαίσιο και προωθεί το πακέτο στον R2. Επειδή το εισερχόμενο πλαίσιο Ethernet έχει MAC προορισμού τη MAC Ethernet του R1, ο R1 αποφασίζει να επεξεργαστεί το πλαίσιο. Ο R1 ελέγχει το FCS του πλαισίου για σφάλματα, και αν δεν υπάρχουν, ο R1 απορρίπτει την επικεφαλίδα Ethernet και το τρέιλερ. Στη συνέχεια, ο R1 συγκρίνει τη διεύθυνση προορισμού του πακέτου (192.168.2.5) με τον πίνακα δρομολόγησης και βρίσκει την καταχώρηση για το υποδίκτυο 192.168.2.0/24. Επειδή η διεύθυνση προορισμού 192.168.2.5 βρίσκεται σε αυτό το υποδίκτυο, ο R1 προωθεί το πακέτο από τη διασύνδεση που αναφέρεται στην αντίστοιχη διαδρομή στον δρομολογητή R2. Ο R1 πρέπει πρώτα να ενθυλακώσει το πακέτο IP σε ένα πλαίσιο ethernet.

Βήμα Γ. Ο R2 επεξεργάζεται το εισερχόμενο πλαίσιο και προωθεί το πακέτο στον R3. Ο R2 επαναλαμβάνει την ίδια γενική διαδικασία με τον R1 όταν ο R2 λαμβάνει το πλαίσιο ethernet. Ο R2 ελέγχει το πεδίο FCS και διαπιστώνει ότι δεν υπάρχουν σφάλματα και στη συνέχεια απορρίπτει την επικεφαλίδα ethernet και το τρέιλερ. Στη συνέχεια, ο R2 συγκρίνει τη διεύθυνση προορισμού του πακέτου (192.168.2.5) με τον πίνακα δρομολόγησης και βρίσκει την καταχώρηση για το υποδίκτυο 192.168.2.0, μια διαδρομή που κατευθύνει τον R2 να στείλει το πακέτο από τη διασύνδεση στον δρομολογητή R3 του επόμενου βήματος. Αλλά πρώτα, ο R2 πρέπει να ενθυλακώσει το πακέτο σε μια κεφαλίδα Ethernet. Αυτή η επικεφαλίδα χρησιμοποιεί τη διεύθυνση MAC του R2 και τη διεύθυνση MAC του R3 στη σύνδεση Ethernet WAN ως διεύθυνση MAC πηγής και προορισμού, αντίστοιχα.

Βήμα Δ. Ο R3 επεξεργάζεται το εισερχόμενο πλαίσιο και προωθεί το πακέτο στον PC2. Όπως και οι R1 και R2, ο R3 ελέγχει το FCS, απορρίπτει την παλιά επικεφαλίδα και το τρέιλερ της σύνδεσης δεδομένων και ταιριάζει τη δική του διαδρομή για το υποδίκτυο 192.168.2.0. Η καταχώρηση στον πίνακα δρομολόγησης του R3 για το 192.168.2.5 δείχνει ότι η εξερχόμενη διασύνδεση είναι η διασύνδεση Ethernet του R3, αλλά δεν υπάρχει δρομολογητής επόμενου άλματος(next hop), επειδή ο R3 συνδέεται απευθείας στο υποδίκτυο 192.168.2.0. Το μόνο που έχει να κάνει ο R3 είναι να ενθυλακώσει το πακέτο μέσα σε μια νέα επικεφαλίδα Ethernet και ένα τρέιλερ, αλλά με διεύθυνση Ethernet προορισμού τη διεύθυνση MAC του PC2.

Επειδή οι δρομολογητές δημιουργούν νέες επικεφαλίδες και trailers και επειδή οι νέες επικεφαλίδες περιέχουν διευθύνσεις συνδέσμου δεδομένων, οι υπολογιστές και οι δρομολογητές πρέπει να έχουν κάποιο τρόπο να αποφασίζουν ποιες διευθύνσεις συνδέσμου δεδομένων θα χρησιμοποιήσουν. Ένα παράδειγμα του τρόπου με τον οποίο ο δρομολογητής καθορίζει ποια διεύθυνση σύνδεσης δεδομένων θα χρησιμοποιήσει είναι το πρωτόκολλο επίλυσης διευθύνσεων IP (ARP, address resolution protocol). Το ARP μαθαίνει δυναμικά τη mac address ενός κεντρικού υπολογιστή IP που είναι συνδεδεμένος σε ένα LAN. Για παράδειγμα, στο τελευταίο βήμα ο δρομολογητής R3 θα χρησιμοποιήσει το ARP μία φορά για να μάθει τη διεύθυνση MAC του PC2 πριν στείλει οποιαδήποτε πακέτα στον PC2.

2.5.3 Κανόνες IP (δίκτυα και υποδίκτυα)

Το TCP/IP ομαδοποιεί τις διευθύνσεις IP έτσι ώστε οι διευθύνσεις IP που χρησιμοποιούνται στο ίδιο φυσικό δίκτυο να αποτελούν μέρος της ίδιας ομάδας. Το IP αποκαλεί αυτές τις ομάδες διευθύνσεων δίκτυο IP ή υποδίκτυο IP. Ορίζονται συγκεκριμένοι κανόνες σχετικά με το ποια διεύθυνση IP πρέπει να βρίσκεται στο ίδιο δίκτυο IP ή υποδίκτυο IP. Αριθμητικά, οι διευθύνσεις στην ίδια ομάδα έχουν την ίδια τιμή στο πρώτο μέρος των διευθύνσεων. Από την άποψη της δρομολόγησης IP, η ομαδοποίηση των διευθύνσεων IP σημαίνει ότι ο πίνακας δρομολόγησης μπορεί να είναι πολύ μικρότερος. Ένας δρομολογητής μπορεί να καταχωρίσει μία καταχώρηση στον πίνακα δρομολόγησης για κάθε δίκτυο ή υποδίκτυο IP, αντί για μία καταχώρηση για κάθε μία διεύθυνση IP.

Ουσιαστικά υπάρχουν δύο θεμελιώδης κανόνες:

Δύο διευθύνσεις IP, που δεν διαχωρίζονται μεταξύ τους με δρομολογητή, πρέπει να ανήκουν στην ίδια ομάδα (υποδίκτυο).

Δύο διευθύνσεις IP, που χωρίζονται μεταξύ τους από τουλάχιστον έναν δρομολογητή, πρέπει να ανήκουν σε διαφορετικές ομάδες (υποδίκτυα).

2.5.4 IP Header

Η διαδικασία δρομολόγησης χρησιμοποιεί επίσης την επικεφαλίδα IPv4. Η επικεφαλίδα παραθέτει μια διεύθυνση IP πηγής 32-bit, καθώς και μια διεύθυνση IP προορισμού 32-bit. Η επικεφαλίδα, φυσικά, έχει και άλλα πεδία, αλλά πρέπει να γνωρίζει την επικεφαλίδα IP των 20 byte και την ύπαρξη των πεδίων διεύθυνσης IP πηγής και προορισμού. Στα μέχρι τώρα παραδείγματα, ενώ οι δρομολογητές αφαιρούν και προσθέτουν επικεφαλίδες συνδέσεων δεδομένων κάθε φορά που δρομολογούν ένα πακέτο, η επικεφαλίδα IP παραμένει, με τις διευθύνσεις IP αμετάβλητες από τη διαδικασία δρομολόγησης IP.

2.6 Άλλες σημαντικές λειτουργίες πρωτοκόλλων

Το επίπεδο δικτύου TCP/IP ορίζει πολλές λειτουργίες πέραν της IP. Σίγουρα, η IP παίζει τεράστιο ρόλο στη δικτύωση σήμερα, καθορίζοντας τη διευθυνσιοδότηση IP και τη δρομολόγηση IP. Ωστόσο, άλλα πρωτόκολλα και πρότυπα, τα οποία ορίζονται σε άλλες αιτήσεις για σχόλια (RFC), παίζουν επίσης σημαντικό ρόλο στις λειτουργίες του επιπέδου δικτύου. Για παράδειγμα, πρωτόκολλα δρομολόγησης όπως το Open Shortest Path First (OSPF) υπάρχουν ως ξεχωριστά πρωτόκολλα, που ορίζονται σε ξεχωριστά RFC. Θα αναφερθούν περιληπτικά τρία σημαντικά το Domain Name System (DNS), το Address Resolution Protocol (ARP) και το Internet Control Message Protocol(ICMP)-Ping.

2.6.1 DNS

Οι άνθρωποι θυμούνται πιο εύκολα ονόματα και όχι αριθμούς. Στο Ίντερνετ χρησιμοποιούνται εύκολα ονόματα όπως google.com ή facebook.com, ενώ θα έπρεπε ο χρήστης να θυμάται και να πληκτρολογεί διευθύνσεις IP, όπως 64.233.177.100. Σίγουρα, το να ζητάμε από τους χρήστες να θυμούνται διευθύνσεις IP δεν θα ήταν φιλικό προς το χρήστη και θα μπορούσε να απομακρύνει ορισμένους ανθρώπους από τη χρήση υπολογιστών.

Το TCP/IP ορίζει έναν τρόπο χρήσης των ονομάτων για την αναγνώριση άλλων υπολογιστών. Ο χρήστης είτε δεν σκέφτεται ποτέ τον άλλο υπολογιστή είτε αναφέρεται στον άλλο υπολογιστή με το όνομά του. Στη συνέχεια, τα πρωτόκολλα ανακαλύπτουν δυναμικά όλες τις απαραίτητες πληροφορίες για να επιτρέψουν την επικοινωνία με βάση αυτό το όνομα.

Για παράδειγμα, όταν ανοίγετε ένα πρόγραμμα περιήγησης στο web και πληκτρολογείτε το όνομα κεντρικού υπολογιστή υπηρεσίας ιστού www.google.com, ο υπολογιστής σας δεν στέλνει ένα πακέτο IP με διεύθυνση IP προορισμού www.google.com, αλλά ένα πακέτο IP σε μια διεύθυνση IP που χρησιμοποιείται από τον διακομιστή web για το Google. Το TCP/IP χρειάζεται έναν τρόπο για να μπορέσει ένας υπολογιστής να βρει τη διεύθυνση IP που χρησιμοποιείται από το καταχωρημένο όνομα κεντρικού υπολογιστή, και αυτή η μέθοδος χρησιμοποιεί το σύστημα DNS.

Γενικά χρησιμοποιείται η διαδικασία DNS για την επίλυση των ονομάτων στην αντίστοιχη διεύθυνση IP. Ας υποθέσουμε πως το PC1, πρέπει να συνδεθεί σε έναν διακομιστή που ονομάζεται Server1. Σε κάποιο σημείο, ο χρήστης είτε πληκτρολογεί το όνομα Server1 είτε κάποια εφαρμογή στο PC1 αναφέρεται στον εν λόγω διακομιστή με το όνομα.

Στο βήμα 1, ο PC1 στέλνει ένα ένα ερώτημα DNS στον διακομιστή DNS.

Στο βήμα 2, ο διακομιστής DNS στέλνει πίσω μια απάντηση DNS που παραθέτει τη διεύθυνση IP του Server1.

Στο Βήμα 3, ο PC1 μπορεί τώρα να στείλει ένα πακέτο IP στη διεύθυνση προορισμού 1.2.3.4, τη διεύθυνση που χρησιμοποιείται από τον Server1.

Οι λεπτομέρειες του δικτύου, συμπεριλαμβανομένων των δρομολογητών, δεν έχουν σημασία για τη διαδικασία επίλυσης ονομάτων. Οι δρομολογητές αντιμετωπίζουν τα μηνύματα DNS όπως κάθε άλλο πακέτο IP, δρομολογώντας τα με βάση τη διεύθυνση IP προορισμού.

Το DNS ορίζει πρωτόκολλα, καθώς και πρότυπα για τα ονόματα κειμένου που χρησιμοποιούνται σε όλο τον κόσμο, καθώς και ένα παγκόσμιο σύνολο κατανεμημένων διακομιστών DNS. [7] Τα ονόματα τομέων που χρησιμοποιούν καθημερινά οι άνθρωποι κατά την περιήγηση στο διαδίκτυο, τα οποία μοιάζουν με το www.example.com, ακολουθούν τα πρότυπα ονοματοδοσίας DNS. Επίσης, κανένας μεμονωμένος διακομιστής DNS δεν γνωρίζει όλα τα ονόματα και τις αντίστοιχες διευθύνσεις IP, αλλά οι πληροφορίες κατανέμονται σε πολλούς διακομιστές DNS. Έτσι, οι διακομιστές DNS του κόσμου συνεργάζονται, προωθώντας ερωτήματα ο ένας στον άλλο, μέχρι ο διακομιστής που γνωρίζει την απάντηση να παράσχει τις επιθυμητές πληροφορίες για τις διευθύνσεις IP.

2.6.2 ARP-Address Resolution Protocol

Η λογική δρομολόγησης IP απαιτεί από τους κεντρικούς υπολογιστές και τους δρομολογητές να ενθυλακώνουν πακέτα IP μέσα σε πλαίσια επιπέδου σύνδεσης δεδομένων. Για τις διασυνδέσεις Ethernet, το ARP χρησιμοποιείται στην ερώτηση «πώς γνωρίζει ένας δρομολογητής ποια διεύθυνση MAC να χρησιμοποιήσει για τον προορισμό;»

Στα τοπικά δίκτυα Ethernet, κάθε φορά που ένας κεντρικός υπολογιστής ή δρομολογητής χρειάζεται να ενθυλακώσει ένα πακέτο IP σε ένα νέο πλαίσιο Ethernet, ο κεντρικός υπολογιστής ή ο δρομολογητής γνωρίζει όλα τα σημαντικά στοιχεία για τη δημιουργία αυτής της επικεφαλίδας(εκτός από τη διεύθυνση MAC προορισμού). Ο κεντρικός υπολογιστής γνωρίζει τη διεύθυνση IP της επόμενης συσκευής, είτε τη διεύθυνση IP ενός άλλου κεντρικού υπολογιστή είτε την προεπιλεγμένη διεύθυνση IP του δρομολογητή. Ο δρομολογητής γνωρίζει τη διαδρομή IP που χρησιμοποιείται για την προώθηση του πακέτου IP, η οποία παραθέτει τη διεύθυνση IP του επόμενου δρομολογητή. Ωστόσο, οι κεντρικοί υπολογιστές και οι δρομολογητές δεν γνωρίζουν εκ των προτέρων τις διευθύνσεις MAC αυτών των γειτονικών συσκευών.

Το TCP/IP ορίζει το πρωτόκολλο επίλυσης διευθύνσεων (ARP) ως τη μέθοδο με την οποία οποιοσδήποτε κεντρικός υπολογιστής ή δρομολογητής σε ένα LAN μπορεί να μάθει δυναμικά τη διεύθυνση MAC ενός άλλου κεντρικού υπολογιστή ή δρομολογητή IP στο ίδιο LAN. Το ARP περιλαμβάνει το ARP Request, το οποίο είναι ένα μήνυμα που κάνει το απλό αίτημα «αν αυτή είναι η διεύθυνση IP σας, παρακαλώ απαντήστε με τη διεύθυνση MAC σας». Το ARP ορίζει επίσης το μήνυμα ARP Reply, το οποίο πράγματι παραθέτει τόσο την αρχική διεύθυνση IP όσο και την αντίστοιχη διεύθυνση MAC. [8]

Σημειώστε ότι οι κεντρικοί υπολογιστές και οι δρομολογητές θυμούνται τα αποτελέσματα του ARP, διατηρώντας τις πληροφορίες στην προσωρινή μνήμη ARP ή στον πίνακα ARP. Ένας κεντρικός υπολογιστής ή δρομολογητής χρειάζεται να χρησιμοποιεί το ARP μόνο περιστασιακά, για να δημιουργήσει την προσωρινή μνήμη ARP την πρώτη φορά. Κάθε φορά που ένας κεντρικός υπολογιστής ή δρομολογητής χρειάζεται να στείλει ένα πακέτο ενθυλακωμένο σε ένα πλαίσιο Ethernet, ελέγχει πρώτα την προσωρινή μνήμη ARP για τη σωστή διεύθυνση IP και την αντίστοιχη διεύθυνση MAC. Οι κεντρικοί υπολογιστές και οι δρομολογητές αφήνουν τις καταχωρήσεις της προσωρινής μνήμης ARP να λήξουν για να καθαρίσουν τον πίνακα, έτσι ώστε να εμφανίζονται περιστασιακά αιτήματα ARP.

2.6.3 Dynamic Host Configuration Protocol (DHCP)

Το DHCP είναι ένα πρωτόκολλο διαχείρισης δικτύου που χρησιμοποιούμε σε δίκτυα TCP/IP. Ο διακομιστής DHCP, εκχωρεί αυτόματα διευθύνσεις IP και άλλες ρυθμίσεις δικτύου, όπως μάσκα υποδικτύου, προεπιλεγμένη πύλη, διακομιστή DNS και άλλα στις συνδεδεμένες συσκευές, ώστε να μπορούν να ανταλλάσσουν πληροφορίες. Το DHCP επιτρέπει στους κεντρικούς υπολογιστές να λαμβάνουν τα απαραίτητα δεδομένα διαμόρφωσης TCP/IP από το διακομιστή DHCP.

Μια συσκευή κάνει αίτηση για μια διεύθυνση IP αν θέλει να αποκτήσει πρόσβαση σε ένα δίκτυο που χρησιμοποιεί το DHCP. Ο διακομιστής απαντά και παρέχει μια διεύθυνση IP στη συσκευή. Στη συνέχεια, όταν λήξει μια καθορισμένη περίοδος ή η συσκευή κλείσει, την επαναφέρει στη δεξαμενή των διαθέσιμων διευθύνσεων IP. Διατηρείται μέχρι να πρέπει να εκχωρηθεί εκ νέου σε μια άλλη συσκευή που θέλει να αποκτήσει πρόσβαση στο δίκτυο.

Χρησιμοποιώντας αυτό το πρωτόκολλο, οι διαχειριστές του δικτύου δεν χρειάζεται να ορίζουν μια στατική IP για κάθε συσκευή και αργότερα να την αναθέτουν εκ νέου σε άλλη και να παρακολουθούν όλες τις διαθέσιμες IP. Θα ρυθμίσουν απλώς τον διακομιστή DHCP με όλες τις πρόσθετες πληροφορίες δικτύου και αυτός θα εκχωρεί δυναμικά τις διευθύνσεις.

2.6.4 ICMP Echo και η εντολή ping

Το κύριο εργαλείο για τον έλεγχο της βασικής συνδεσιμότητας δικτύου είναι η εντολή ping. Η εντολή ping (Packet Internet Groper) χρησιμοποιεί το πρωτόκολλο μηνυμάτων ελέγχου του Διαδικτύου (ICMP), στέλνοντας ένα μήνυμα που ονομάζεται αίτηση ηχούς ICMP σε μια άλλη διεύθυνση IP. Ο υπολογιστής με αυτή τη διεύθυνση IP θα πρέπει να απαντήσει με μια απάντηση ICMP echo reply. Εάν αυτό λειτουργεί, έχετε δοκιμάσει επιτυχώς το δίκτυο IP. Με άλλα λόγια, γνωρίζετε ότι το δίκτυο μπορεί να παραδώσει ένα πακέτο από τον έναν υπολογιστή στον άλλο και πίσω. Η ICMP δεν βασίζεται σε καμία εφαρμογή, οπότε στην πραγματικότητα απλώς δοκιμάζει τη βασική συνδεσιμότητα IP - τα επίπεδα 1, 2 και 3. [9]

2.6.5 Επίλογος

Κλείνοντας το κεφάλαιο έχει γίνει ανάλυση των βασικών πρωτόκολλων που χρησιμοποιούνται για την επικοινωνία των συσκευών ενός δικτύου με παραδείγματα για καλύτερη κατανόηση, επίσης έγινε παρουσίαση κάποιων σημαντικών λειτουργιών όπως DHCP, DNS ,ACP και του ping

Κεφάλαιο 3ο: Βασικές ρυθμίσεις Cisco switches

3.1 Εισαγωγή

Η πρώτη δεξιότητα που πρέπει να γίνει εμπειρία πριν από την εκτέλεση όλων των εργασιών διαμόρφωσης και να εξασφαλιστεί η πρόσβαση και να χρησιμοποιηθεί το περιβάλλον εργασίας χρήστη του μεταγωγέα, το οποίο ονομάζεται διεπαφή γραμμής εντολών (Command Line Interface CLI).

Αυτή η ενότητα ξεκινά αυτή τη διαδικασία παρουσιάζοντας τα βασικά στοιχεία για την πρόσβαση στο CLI του μεταγωγέα. Αυτές οι δεξιότητες περιλαμβάνουν τον τρόπο πρόσβασης στο CLI και τον τρόπο έκδοσης εντολών επαλήθευσης για τον έλεγχο της κατάστασης του τοπικού δικτύου. Αυτή η ενότητα περιλαμβάνει επίσης τις διαδικασίες για το πώς να ρυθμίζετε τις παραμέτρους του μεταγωγέα και πώς να αποθηκεύετε αυτές τις παραμέτρους.

3.2 Πληροφορίες για τα switches και το CLI

Η Cisco χρησιμοποιεί την έννοια της διεπαφής γραμμής εντολών με τα προϊόντα δρομολογητών της και τα περισσότερα από τα προϊόντα switches LAN Catalyst. Το CLI είναι μια διεπαφή βασισμένη σε κείμενο στην οποία ο χρήστης, συνήθως ένας μηχανικός δικτύου, εισάγει μια εντολή κειμένου και πατάει Enter. Το πάτημα του Enter στέλνει την εντολή στο μεταγωγέα, ο οποίος λέει στη συσκευή να κάνει κάτι. Ο μεταγωγέας κάνει αυτό που λέει η εντολή και σε ορισμένες περιπτώσεις, ο μεταγωγέας απαντά με κάποια μηνύματα που αναφέρουν τα αποτελέσματα της εντολής.

Τα switches Cisco Catalyst υποστηρίζουν και άλλες μεθόδους παρακολούθησης και διαμόρφωσης. Για παράδειγμα, ένα switch μπορεί να παρέχει μια διεπαφή web, ώστε ένας μηχανικός να μπορεί να ανοίξει ένα πρόγραμμα περιήγησης στο web για να συνδεθεί σε έναν web server που εκτελείται στο switch. Οι μεταγωγείς μπορούν επίσης να ελέγχονται και να λειτουργούν με τη χρήση λογισμικού διαχείρισης δικτύου.

Τα switches Cisco Catalyst 1000 Series είναι Gigabit Ethernet και Fast Ethernet εταιρικής κατηγορίας Layer 2, σχεδιασμένοι για μικρές επιχειρήσεις και υποκαταστήματα. Πρόκειται για απλούς, ευέλικτους και ασφαλείς μεταγωγείς, ιδανικούς για δικτυακές εγκαταστάσεις και κρίσιμες εγκαταστάσεις Internet of Things (IoT). Τα Cisco Catalyst 1000 λειτουργούν με το λογισμικό Cisco IOS Software και υποστηρίζουν απλή διαχείριση συσκευών και δικτύου μέσω CLI καθώς και μέσω ενός ενσωματωμένου web UI. Αυτοί οι μεταγωγείς παρέχουν βελτιωμένη ασφάλεια δικτύου, αξιοπιστία δικτύου και λειτουργική αποδοτικότητα για μικρούς οργανισμούς. [10]

Η Cisco αναφέρεται στις φυσικές συνδέσεις ενός μεταγωγέα είτε ως διασυνδέσεις είτε ως θύρες, με έναν τύπο διασύνδεσης και έναν αριθμό διασύνδεσης. Ο τύπος διασύνδεσης, όπως χρησιμοποιείται στις εντολές του μεταγωγέα, είναι είτε Ethernet, Fast Ethernet, Gigabit Ethernet κ.ο.κ. για μεγαλύτερες ταχύτητες. Για τις διασυνδέσεις Ethernet που υποστηρίζουν τη λειτουργία σε πολλαπλές ταχύτητες, το μόνιμο όνομα της διασύνδεσης αναφέρεται στην ταχύτερη υποστηριζόμενη ταχύτητα. Για παράδειγμα, μια διασύνδεση 10/100/1000 (δηλαδή μια διασύνδεση που λειτουργεί στα 10 Mbps, 100 Mbps ή 1000 Mbps) θα ονομάζεται Gigabit Ethernet ανεξάρτητα από την ταχύτητα που χρησιμοποιείται αυτή τη στιγμή.

Για τη μοναδική αρίθμηση κάθε διαφορετικής διασύνδεσης, ορισμένοι μεταγωγείς Catalyst χρησιμοποιούν έναν διψήφιο αριθμό διασύνδεσης (x/y), ενώ άλλοι έχουν έναν τριψήφιο αριθμό (x/y/z). Για παράδειγμα, δύο θύρες 10/100/1000 σε πολλούς παλαιότερους μεταγωγείς Cisco Catalyst θα

ονομάζονταν GigabitEthernet 0/0 και GigabitEthernet 0/1, ενώ στη νεότερη σειρά, οι δύο διασυνδέσεις θα ήταν GigabitEthernet 1/0/1 και GigabitEthernet 1/0/2.

Όπως κάθε άλλο κομμάτι υλικού υπολογιστή, οι μεταγωγείς Cisco χρειάζονται κάποιο λογισμικό λειτουργικού συστήματος. Η Cisco ονομάζει αυτό το λειτουργικό σύστημα Internetwork Operating System (IOS).

Το λογισμικό Cisco IOS για μεταγωγείς Catalyst υλοποιεί και ελέγχει τη λογική και τις λειτουργίες που εκτελεί ένας μεταγωγέας Cisco. Το Cisco IOS CLI επιτρέπει στον χρήστη να χρησιμοποιεί ένα πρόγραμμα εξομοίωσης τερματικού, το οποίο δέχεται κείμενο που εισάγει ο χρήστης. Όταν ο χρήστης πατήσει το Enter, ο εξομοιωτής τερματικού στέλνει το κείμενο αυτό στο μεταγωγέα. Το switch επεξεργάζεται το κείμενο σαν να πρόκειται για εντολή, εκτελεί ό,τι λέει η εντολή και στέλνει το κείμενο πίσω στον εξομοιωτή τερματικού.

Η πρόσβαση στο CLI του μεταγωγέα μπορεί να γίνει μέσω τριών δημοφιλών μεθόδων - της κονσόλας, του Telnet και του Secure Shell (SSH). Δύο από αυτές τις μεθόδους (Telnet και SSH) χρησιμοποιούν το δίκτυο IP στο οποίο βρίσκεται το μεταγωγέας για να προσεγγίσουν το μεταγωγέα. Η κονσόλα είναι μια φυσική θύρα που έχει κατασκευαστεί ειδικά για να επιτρέπει την πρόσβαση στο CLI.

Η πρόσβαση στην κονσόλα απαιτεί τόσο μια φυσική σύνδεση μεταξύ ενός υπολογιστή (ή άλλης συσκευής χρήστη) και της θύρας κονσόλας του μεταγωγέα, όσο και κάποιο λογισμικό στον υπολογιστή. Το Telnet και το SSH απαιτούν λογισμικό στη συσκευή του χρήστη, αλλά βασίζονται στο υπάρχον δίκτυο TCP/IP για τη μετάδοση δεδομένων.

3.3 Καλωδίωση της σύνδεσης της κονσόλας

Η φυσική σύνδεση της κονσόλας, τόσο η παλιά όσο και η νέα, χρησιμοποιεί τρία βασικά στοιχεία: τη φυσική θύρα κονσόλας στο μεταγωγέα, μια φυσική σειριακή θύρα στον υπολογιστή και ένα καλώδιο. Ωστόσο, οι λεπτομέρειες της φυσικής καλωδίωσης έχουν αλλάξει αργά με την πάροδο του χρόνου, κυρίως λόγω των εξελίξεων και των αλλαγών με τις σειριακές διεπαφές στο υλικό του υπολογιστή.

Οι περισσότεροι υπολογιστές σήμερα χρησιμοποιούν ένα γνωστό τυπικό καλώδιο USB για τη σύνδεση της κονσόλας. Η Cisco έχει συμπεριλάβει θύρες USB ως θύρες κονσόλας στους νεότερους δρομολογητές και μεταγωγείς. Μπορεί να χρησιμοποιηθεί οποιαδήποτε θύρα USB στον υπολογιστή, με ένα καλώδιο USB, συνδεδεμένο στη θύρα κονσόλας USB του μεταγωγέα ή του δρομολογητή.

Οι παλαιότερες συνδέσεις κονσόλας χρησιμοποιούν μια σειριακή θύρα υπολογιστή που προϋπήρχε της USB, ένα καλώδιο UTP και μια θύρα κονσόλας RJ-45 στο μεταγωγέα. Η σειριακή θύρα PC έχει συνήθως έναν σύνδεσμο σχήματος D (περίπου ορθογώνιο) με εννέα ακίδες (συχνά ονομάζεται DB-9). Η θύρα κονσόλας μοιάζει με οποιαδήποτε θύρα Ethernet RJ-45 (αλλά συνήθως έχει μπλε χρώμα και τη λέξη console δίπλα της στο μεταγωγέα).

Η καλωδίωση για αυτή τη σύνδεση κονσόλας παλαιότερου τύπου μπορεί να είναι απλή ή να απαιτεί κάποια προσπάθεια, ανάλογα με το καλώδιο που χρησιμοποιείτε. Μπορεί να χρησιμοποιηθεί το ειδικά κατασκευασμένο καλώδιο κονσόλας που συνοδεύει τους νέους μεταγωγείς και δρομολογητές της Cisco. Μπορεί να φτιαχτεί το δικό σας καλώδιο με ένα τυπικό σειριακό καλώδιο (με σύνδεσμο που ταιριάζει με τον υπολογιστή), ένα τυπικό βύσμα μετατροπής RJ-45 σε DB-9 και ένα καλώδιο UTP. Το καλώδιο UTP δεν χρησιμοποιεί τα ίδια pinouts με το Ethernet- αντίθετα, το καλώδιο χρησιμοποιεί τα pinouts του καλωδίου rollover και όχι κάποιο από τα τυπικά pinouts της καλωδίωσης Ethernet. Η συνδεσμολογία rollover χρησιμοποιεί οκτώ καλώδια, κυλώντας το καλώδιο στον ακροδέκτη 1 στον ακροδέκτη 8, τον ακροδέκτη 2 στον ακροδέκτη 7, τον ακροδέκτη 3 στον ακροδέκτη 6 κ.ο.κ.

Οι θύρες USB διαδόθηκαν στους υπολογιστές πριν η Cisco αρχίσει να χρησιμοποιεί συνήθως τις θύρες USB για τις θύρες κονσόλας της. Έτσι, θα πρέπει επίσης να είστε έτοιμοι να χρησιμοποιήσετε ένα PC που διαθέτει μόνο θύρα USB και όχι μια παλιά σειριακή θύρα, αλλά ένα δρομολογητή ή μεταγωγέα που διαθέτει την παλαιότερη θύρα κονσόλας RJ-45 (και όχι θύρα κονσόλας USB). Για να συνδέσετε έναν τέτοιο υπολογιστή σε μια κονσόλα δρομολογητή ή μεταγωγέα, χρειάζεστε έναν μετατροπέα USB που μετατρέπει το παλαιότερο καλώδιο κονσόλας σε υποδοχή USB και ένα καλώδιο UTP rollover

Η σειρά 2960-XR, για παράδειγμα, υποστηρίζει τόσο την παλαιότερη θύρα κονσόλας RJ-45 όσο και μια θύρα κονσόλας USB, θα πρέπει να χρησιμοποιήσετε μόνο τη μία ή την άλλη. Σημειώστε ότι η θύρα κονσόλας USB χρησιμοποιεί μια θύρα mini-B και όχι την πιο συνηθισμένη ορθογώνια τυπική θύρα USB τύπου A.

Εικόνα 3.1 Ένα C1000 switch

Αφού ο υπολογιστής συνδεθεί φυσικά στη θύρα κονσόλας, πρέπει να εγκατασταθεί και να ρυθμιστεί στον υπολογιστή ένα πακέτο λογισμικού εξομοιωτή τερματικού. Το λογισμικό εξομοιωτή τερματικού αντιμετωπίζει όλα τα δεδομένα ως κείμενο. Δέχεται το κείμενο που πληκτρολογεί ο χρήστης και το στέλνει μέσω της σύνδεσης κονσόλας στο μεταγωγέα. Ομοίως, όλα τα bit που εισέρχονται στον υπολογιστή μέσω της σύνδεσης κονσόλας εμφανίζονται ως κείμενο για να τα διαβάσει ο χρήστης.

Ο εξομοιωτής πρέπει να διαμορφωθεί ώστε να χρησιμοποιεί τη σειριακή θύρα του υπολογιστή με τις κατάλληλες ρυθμίσεις. Οι προεπιλεγμένες ρυθμίσεις θύρας κονσόλας σε ένα μεταγωγέα είναι οι παρακάτω. Προσέξτε ότι οι τρεις τελευταίες παράμετροι αναφέρονται συνολικά ως 8N1: [11]

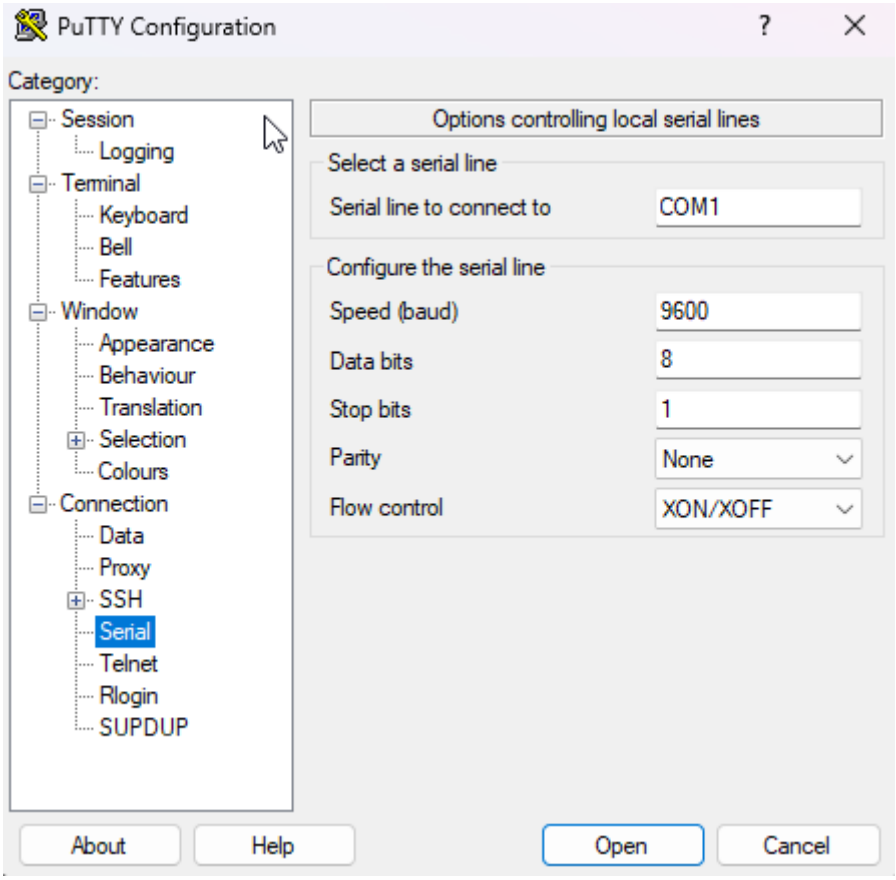
9600 bits/second

No hardware flow control

8-bit ASCII

No parity bits

1 stop bit



Εικόνα 3.2 Ρυθμίσεις σειριακής σύνδεσης στον εξομοιωτή Putty

3.4 Πρόσβαση στο CLI με Telnet και SSH

Για πολλά χρόνια, οι εφαρμογές εξομοιωτών τερματικών υποστηρίζουν πολύ περισσότερα από τη δυνατότητα επικοινωνίας μέσω μιας σειριακής θύρας με μια τοπική συσκευή (όπως η κονσόλα ενός switch). Οι εξομοιωτές τερματικών υποστηρίζουν επίσης μια ποικιλία εφαρμογών TCP/IP, συμπεριλαμβανομένων των Telnet και SSH. Τόσο το Telnet όσο και το SSH επιτρέπουν στο χρήστη να συνδεθεί στο CLI μιας άλλης συσκευής, αλλά αντί να συνδέεται μέσω ενός καλωδίου κονσόλας στη θύρα κονσόλας, η κυκλοφορία ρέει μέσω του δικτύου.

Το Telnet χρησιμοποιεί την έννοια ενός πελάτη Telnet (η τερματική εφαρμογή) και ενός διακομιστή Telnet (το switch σε αυτή την περίπτωση). Ο πελάτης Telnet, η συσκευή που βρίσκεται μπροστά από τον χρήστη, δέχεται εισόδους από το πληκτρολόγιο και στέλνει αυτές τις εντολές στον διακομιστή Telnet. Ο διακομιστής Telnet δέχεται το κείμενο, ερμηνεύει το κείμενο ως εντολή και απαντάει.

Οι μεταγωγείς Cisco Catalyst ενεργοποιούν έναν διακομιστή Telnet από προεπιλογή, αλλά οι μεταγωγείς χρειάζονται μερικές ακόμη ρυθμίσεις διαμόρφωσης προτού μπορέσετε να χρησιμοποιήσετε με επιτυχία το Telnet για να συνδεθείτε σε έναν μεταγωγέα.

Η χρήση του Telnet για δοκιμές έχει νόημα, αλλά το Telnet ενέχει σημαντικό κίνδυνο ασφάλειας σε δίκτυα παραγωγής. Το Telnet στέλνει όλα τα δεδομένα (συμπεριλαμβανομένου οποιουδήποτε ονόματος χρήστη και κωδικού πρόσβασης για σύνδεση στο μεταγωγέα) ως δεδομένα καθαρού κειμένου. Το SSH μας δίνει μια πολύ καλύτερη επιλογή κρυπτογραφώντας τα περιεχόμενα όλων των μηνυμάτων, συμπεριλαμβανομένων των κωδικών πρόσβασης.

Modes

Οι συνδέσεις με κονσόλα, Telnet και SSH τοποθετούν τον χρήστη σε μια περιοχή του CLI που ονομάζεται λειτουργία EXEC χρήστη. Η λειτουργία User EXEC mode, που μερικές φορές ονομάζεται επίσης user mode, επιτρέπει στο χρήστη να κοιτάξει γύρω του αλλά να μην παραβιάσει τίποτα. Το μέρος του ονόματος «EXEC mode» αναφέρεται στο γεγονός ότι σε αυτή τη λειτουργία, όταν εισάγετε μια εντολή, το switch εκτελεί την εντολή και στη συνέχεια εμφανίζει μηνύματα που περιγράφουν τα αποτελέσματα της εντολής.

Το Cisco IOS υποστηρίζει μια πιο ισχυρή λειτουργία EXEC που ονομάζεται λειτουργία enable (επίσης γνωστή ως privileged mode).Οταν δωθεί η εντολή **enable**, στο CLI μπορούν να εκτελεστούν ισχυρές (ή προνομιακές) εντολές. Για παράδειγμα, μπορείτε να χρησιμοποιήσετε την εντολή **reload**, η οποία λέει στο μεταγωγέα να κάνει επανεκκίνηση, μόνο από τη λειτουργία enable

3.5 Κωδικός πρόσβασης για πρόσβαση στο CLI από την κονσόλα

Ένας μεταγωγέας Cisco, με τις προεπιλεγμένες ρυθμίσεις, παραμένει σχετικά ασφαλής όταν είναι κλειδωμένος μέσα σε μια ντουλάπα καλωδίωσης, επειδή από προεπιλογή, ένας μεταγωγέας επιτρέπει μόνο την πρόσβαση στην κονσόλα. Από προεπιλογή, η κονσόλα δεν απαιτεί κανέναν κωδικό πρόσβασης, ούτε κωδικό πρόσβασης για την πρόσβαση σε κατάσταση ενεργοποίησης για τους χρήστες που έτυχε να συνδεθούν από την κονσόλα. Ο λόγος είναι ότι αν έχετε πρόσβαση στη φυσική θύρα κονσόλας του μεταγωγέα, έχετε ήδη σχεδόν πλήρη έλεγχο του μεταγωγέα. Θα μπορούσατε να αποσυνδέσετε το ρεύμα, ή να ακολουθήσετε δημοσιευμένες διαδικασίες για την ανάκτηση του κωδικού πρόσβασης για να εισέλθετε στο CLI και στη συνέχεια να ρυθμίσετε οτιδήποτε θέλετε να ρυθμίσετε.

Πολλοί άνθρωποι προχωρούν και ρυθμίζουν απλή προστασία με κωδικό πρόσβασης για τους χρήστες της κονσόλας. Οι απλοί κωδικοί πρόσβασης μπορούν να ρυθμιστούν σε δύο σημεία από την κονσόλα: όταν ο χρήστης συνδέεται στην κονσόλα και όταν οποιοσδήποτε χρήστης μεταβαίνει σε κατάσταση ενεργοποίησης (χρησιμοποιώντας την εντολή **enable**).

Η εντολή ρύθμισης **enable secret arch123**(όπου arch123 είναι ο κωδικός πρόσβασης) ορίζει τον κωδικό πρόσβασης που πρέπει να χρησιμοποιούν όλοι οι χρήστες για να εισέλθουν στο privileged mode. Έτσι, ανεξάρτητα από το αν οι χρήστες συνδέονται από την κονσόλα, το Telnet ή το SSH, θα χρησιμοποιούν τον κωδικό πρόσβασης arch123 όταν τους ζητείται κωδικός πρόσβασης μετά την πληκτρολόγηση της εντολής **enable**.

Τέλος, οι παρακάτω εντολές από config mode ρυθμίζουν τον κωδικό πρόσβασης της κονσόλας. Η **line console 0** είναι η εντολή που προσδιορίζει την κονσόλα, που ουσιαστικά σημαίνει ότι «αυτές οι επόμενες εντολές ισχύουν μόνο για την κονσόλα». Η εντολή **login** λέει στο IOS να εκτελέσει απλό έλεγχο του κωδικού πρόσβασης (στην κονσόλα). Από προεπιλογή, το switch δεν ζητά κωδικό πρόσβασης για τους χρήστες της κονσόλας. Τέλος, η εντολή **password arch1234** ορίζει τον κωδικό πρόσβασης που πρέπει να πληκτρολογήσει ο χρήστης της κονσόλας όταν του ζητηθεί.

3.6 Οι εντολές debug και show

Μακράν η πιο δημοφιλής εντολή του Cisco IOS είναι η εντολή **show**. Η εντολή **show** διαθέτει μεγάλη ποικιλία επιλογών και με αυτές τις επιλογές μπορείτε να βρείτε την κατάσταση σχεδόν κάθε δυνατότητας του Cisco IOS. Ουσιαστικά, η εντολή **show** παραθέτει τα επί του παρόντος γνωστά στοιχεία σχετικά με τη λειτουργική κατάσταση του μεταγωγέα. Η μόνη εργασία που εκτελεί το switch

ως αντίδραση στις εντολές **show** είναι να βρει την τρέχουσα κατάσταση και να παραθέσει τις πληροφορίες σε μηνύματα που αποστέλλονται στον χρήστη.

Για παράδειγμα, θεωρήστε την έξοδο από την εντολή **show mac address-table dynamic**

```
C1000-48P-1-CR#show mac address-table dynamic
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
   1    0000.5e00.0101    DYNAMIC     Gi1/0/52
   1    0c27.24cf.5e47    DYNAMIC     Gi1/0/52
   1    1006.edd6.0178    DYNAMIC     Gi1/0/52
   1    1006.edd6.58c4    DYNAMIC     Gi1/0/52
   1    1006.edd6.8188    DYNAMIC     Gi1/0/52
   1    1006.edd6.8750    DYNAMIC     Gi1/0/52
   1    1006.edd6.a5f4    DYNAMIC     Gi1/0/52
```

Εικόνα 3.3 Έξοδος εντολής **show mac address-table dynamic**

Αυτή η εντολή **show**, που εκδίδεται από τη λειτουργία χρήστη, παραθέτει τον πίνακα που χρησιμοποιεί ο μεταγωγέας για να λαμβάνει αποφάσεις προώθησης. Ο πίνακας διευθύνσεων MAC ενός μεταγωγέα ουσιαστικά παραθέτει τα δεδομένα που χρησιμοποιεί ένας μεταγωγέας για να κάνει την κύρια εργασία του.

Η εντολή **debug** λέει επίσης στον χρήστη λεπτομέρειες σχετικά με τη λειτουργία του μεταγωγέα. Ενώ η εντολή **show** παραθέτει πληροφορίες κατάστασης σε μια χρονική στιγμή η εντολή **debug** δείχνει τι συμβαίνει εκείνη την στιγμή στο switch. Μόλις εκδώσετε μια εντολή εντοπισμού σφαλμάτων, το IOS τη θυμάται, εκδίδοντας μηνύματα που μπορεί να επιλέξει να δει οποιοσδήποτε χρήστης του μεταγωγέα. Η κονσόλα βλέπει αυτά τα μηνύματα από προεπιλογή.

3.7 Διαμόρφωση του λογισμικού Cisco IOS

Θα θελήσετε να διαμορφώσετε κάθε μεταγωγέα σε ένα δίκτυο Enterprise, παρόλο που οι μεταγωγείς θα προωθήσουν την κυκλοφορία ακόμη και με προεπιλεγμένη διαμόρφωση. Οι βασικές διαδικασίες διαμόρφωσης, συμπεριλαμβανομένης της έννοιας του αρχείου διαμόρφωσης και των τοποθεσιών στις οποίες μπορούν να αποθηκευτούν τα αρχεία διαμόρφωσης.

Η λειτουργία διαμόρφωσης είναι μια άλλη λειτουργία για το Cisco CLI, παρόμοια με τη λειτουργία χρήστη και την προνομιακή λειτουργία. Η λειτουργία χρήστη επιτρέπει να εκδίδετε non disruptive εντολές και να εμφανίζετε ορισμένες πληροφορίες. Η προνομιακή λειτουργία υποστηρίζει ένα υπερσύνολο εντολών σε σύγκριση με τη λειτουργία χρήστη, συμπεριλαμβανομένων εντολών που ενδέχεται να διαταράξουν τις λειτουργίες του switch. Ωστόσο, καμία από τις εντολές στην κατάσταση λειτουργίας χρήστη ή στην προνομιακή κατάσταση λειτουργίας δεν αλλάζει τη διαμόρφωση του switch. Η λειτουργία διαμόρφωσης δέχεται εντολές διαμόρφωσης - εντολές που λένε στο μεταγωγέα τις λεπτομέρειες για το τι πρέπει να κάνει και πώς να το κάνει.

Οι εντολές που εισάγονται στη λειτουργία διαμόρφωσης ενημερώνουν το ενεργό αρχείο διαμόρφωσης. Αυτές οι αλλαγές στη διαμόρφωση πραγματοποιούνται αμέσως κάθε φορά που πατάτε το πλήκτρο Enter στο τέλος μιας εντολής οπότε χρειάζεται ιδιαίτερη προσοχή.

3.7.1 Υπολειτουργίες και πλαίσια διαμόρφωσης

Η ίδια η λειτουργία διαμόρφωσης περιέχει πλήθος εντολών. Για να βοηθήσει στην οργάνωση της διαμόρφωσης, το IOS ομαδοποιεί ορισμένα είδη εντολών διαμόρφωσης μαζί. Για να το κάνετε αυτό, όταν χρησιμοποιείτε τη λειτουργία διαμόρφωσης, μεταβαίνετε από την αρχική λειτουργία - τη γενική λειτουργία διαμόρφωσης (global configuration mode) - σε υπολειτουργίες εντολών. Οι εντολές καθορισμού πλαισίου σας μετακινούν από μια κατάσταση λειτουργίας υποεντολών διαμόρφωσης, σε μια άλλη. Αυτές οι εντολές ρύθμισης πλαισίου δηλώνουν στο switch το θέμα για το οποίο θα εισαγάγετε τις επόμενες εντολές διαμόρφωσης. Το πιο σημαντικό είναι ότι το context-πλαίσιο λέει στο μεταγωγέα το θέμα που σας ενδιαφέρει αυτή τη στιγμή, οπότε όταν χρησιμοποιείτε το ? για να λάβετε βοήθεια, ο μεταγωγέας σας δίνει βοήθεια μόνο για αυτό το θέμα.

Η εντολή **interface** είναι μία από τις πιο συχνά χρησιμοποιούμενες εντολές διαμόρφωσης πλαισίου. Για παράδειγμα, ο χρήστης του CLI θα μπορούσε να εισέλθει σε κατάσταση διαμόρφωσης διασύνδεσης εισάγοντας την εντολή διαμόρφωσης **interface FastEthernet 0/1**. Η αναζήτηση βοήθειας στη λειτουργία διαμόρφωσης διασύνδεσης εμφανίζει μόνο τις εντολές που είναι χρήσιμες κατά τη διαμόρφωση διασυνδέσεων Ethernet. Οι εντολές που χρησιμοποιούνται σε αυτό το πλαίσιο ονομάζονται υποεντολές -ή, στη συγκεκριμένη περίπτωση, υποεντολές διασύνδεσης.

3.7.2 Αντιγραφή και διαγράφη αρχείων διαμόρφωσης

Η διαδικασία διαμόρφωσης ενημερώνει το αρχείο running-config, το οποίο χάνεται εάν ο δρομολογητής χάσει την τροφοδοσία ή επανεκκινηθεί. Είναι σαφές ότι το IOS πρέπει να μας παρέχει έναν τρόπο να αντιγράψουμε την τρέχουσα διαμόρφωση ώστε να μην χαθεί, ώστε να χρησιμοποιηθεί την επόμενη φορά που ο μεταγωγέας θα επανεκκινηθεί.

Εν ολίγοις, η εντολή EXEC **copy running-config startup-config** δημιουργεί αντίγραφα ασφαλείας του running-config στο αρχείο startup-config. Αυτή η εντολή αντικαθιστά το τρέχον αρχείο startup-config με ό,τι υπάρχει αυτή τη στιγμή στο αρχείο running-configuration.

Μπορεί επίσης να θέλετε απλώς να απαλλαγείτε από όλες τις υπάρχουσες ρυθμίσεις και να ξεκινήσετε από την αρχή με μια καθαρή ρύθμιση. Για να το κάνετε αυτό, μπορείτε να διαγράψετε το αρχείο startup-config χρησιμοποιώντας τρεις διαφορετικές εντολές: **write erase**, **erase startup-config** και **erase nvram:**.

3.8 Επισκόπηση της λογικής μεταγωγής(Switching Logic)

Ο ρόλος ενός μεταγωγέα LAN είναι η προώθηση πλαισίων Ethernet. Τα τοπικά δίκτυα υπάρχουν ως ένα σύνολο συσκευών χρηστών, διακομιστών και άλλων συσκευών που συνδέονται σε μεταγωγείς, με τους μεταγωγείς να είναι συνδεδεμένοι μεταξύ τους. Ο μεταγωγέας LAN έχει μία κύρια εργασία: να προωθεί τα πλαίσια στη σωστή διεύθυνση προορισμού (MAC). Για την επίτευξη αυτού του στόχου, οι μεταγωγείς επεξεργάζονται την διεύθυνση MAC πηγής και προορισμού στην επικεφαλίδα Ethernet κάθε πλαισίου.

Οι μεταγωγείς LAN λαμβάνουν πλαίσια Ethernet και στη συνέχεια λαμβάνουν μια απόφαση μεταγωγής: είτε προωθούν το πλαίσιο σε κάποιες άλλες θύρες είτε αγνοούν το πλαίσιο. Για την εκπλήρωση αυτής της πρωταρχικής αποστολής, οι μεταγωγείς εκτελούν τρεις ενέργειες:

1. Αποφασίζουν πότε να προωθήσει ένα πλαίσιο ή πότε να φιλτράρει (να μην προωθήσει) ένα πλαίσιο, με βάση τη διεύθυνση MAC προορισμού

2. Προετοιμασία για προώθηση πλαισίων με εκμάθηση διευθύνσεων MAC εξετάζοντας τη διεύθυνση MAC προέλευσης κάθε πλαισίου που λαμβάνει ο μεταγωγέας

3. Προετοιμασία για την προώθηση μόνο ενός αντιγράφου του πλαισίου στον προορισμό με τη δημιουργία ενός loop free περιβάλλοντος μεταξύ των switches με την χρήση του πρωτοκόλλου Spanning Tree Protocol (STP)

Η πρώτη ενέργεια είναι η κύρια εργασία του switch, ενώ τα άλλα δύο στοιχεία είναι γενικές λειτουργίες.

3.8.1 Σύνοψη LAN Switching

Οι μεταγωγείς χρησιμοποιούν τη λογική επιπέδου 2, εξετάζοντας το data link header για να επιλέξουν τον τρόπο επεξεργασίας των πλαισίων. Συγκεκριμένα, οι μεταγωγείς λαμβάνουν αποφάσεις για την προώθηση/φιλτράρισμα πλαισίων, την εκμάθηση διευθύνσεων MAC και τη χρήση του STP για την αποφυγή βρόχων, ως εξής:

Προώθηση/φιλτράρισμα πλαισίων: Οι μεταγωγείς προωθούν πλαίσια με βάση τη διεύθυνση MAC προορισμού:

> **A.** Εάν η διεύθυνση MAC προορισμού είναι broadcast, multicast ή unknown destination unicast (μια unicast που δεν περιλαμβάνεται στον πίνακα MAC), το μεταγωγέας διοχετεύει το πλαίσιο παντού(flooding).
>
> **B.** Εάν η διεύθυνση MAC προορισμού είναι μια γνωστή διεύθυνση unicast (μια διεύθυνση unicast που βρίσκεται στον πίνακα MAC):
>
> > **i.** Εάν η εξερχόμενη διασύνδεση που περιλαμβάνεται στον πίνακα διευθύνσεων MAC είναι διαφορετική από τη διασύνδεση στην οποία ελήφθη το πλαίσιο, ο μεταγωγέας προωθεί το πλαίσιο από την εξερχόμενη διασύνδεση.
> >
> > **ii.** Εάν η εξερχόμενη διασύνδεση είναι η ίδια με τη διασύνδεση στην οποία ελήφθη το πλαίσιο, ο μεταγωγέας φιλτράρει το πλαίσιο, πράγμα που σημαίνει ότι ο μεταγωγέας απλώς αγνοεί το πλαίσιο και δεν το προωθεί.

Εκμάθηση διευθύνσεων MAC: Οι μεταγωγείς χρησιμοποιούν την ακόλουθη λογική για να μάθουν τις καταχωρήσεις του πίνακα διευθύνσεων MAC:

> **A.** Για κάθε λαμβανόμενο πλαίσιο, εξετάστε τη διεύθυνση MAC προέλευσης και σημειώστε τη διασύνδεση από την οποία ελήφθη το πλαίσιο.
>
> **B.** Εάν δεν υπάρχει ήδη στον πίνακα, προσθέστε τη διεύθυνση MAC και τη διασύνδεση από την οποία μαθαίνεται.

Αποφυγή βρόχων: Οι μεταγωγείς χρησιμοποιούν το STP για να αποτρέψουν τους βρόχους, προκαλώντας το μπλοκάρισμα ορισμένων διασυνδέσεων, δηλαδή τη μη αποστολή ή λήψη πλαισίων.

3.9 Διαμόρφωση βασικής διαχείρισης του switch

Οι εργασίες που εκτελεί μια συσκευή δικτύωσης μπορούν να χωριστούν σε τρεις μεγάλες κατηγορίες. Η πρώτη και πιο προφανής, που ονομάζεται επίπεδο δεδομένων, είναι η εργασία που κάνει ένας μεταγωγέας για την προώθηση πλαισίων που παράγονται από τις συσκευές που είναι συνδεδεμένες στο μεταγωγέα. Με άλλα λόγια, το επίπεδο δεδομένων είναι ο κύριος σκοπός του μεταγωγέα. Δεύτερον, το επίπεδο ελέγχου αναφέρεται στη διαμόρφωση και τις διαδικασίες που ελέγχουν και αλλάζουν τις επιλογές που γίνονται από το επίπεδο δεδομένων του μεταγωγέα. Ο μηχανικός δικτύου μπορεί να

ελέγξει ποιες διασυνδέσεις ενεργοποιούνται και απενεργοποιούνται, ποιες θύρες εκτελούνται σε ποιες ταχύτητες, πώς το Spanning Tree μπλοκάρει ορισμένες θύρες για την αποφυγή βρόχων κ.ο.κ.

Η τρίτη κατηγορία, είναι το επίπεδο διαχείρισης. Το επίπεδο διαχείρισης ασχολείται με τη διαχείριση της ίδιας της συσκευής και όχι με τον έλεγχο του τι κάνει η συσκευή. Στη συνέχεια εξετάζονται οι πιο βασικές λειτουργίες διαχείρισης που μπορούν να ρυθμιστούν σε ένα μεταγωγέα της Cisco.

3.9.1 Ασφάλιση του CLI του switch

Από προεπιλογή, ένα Cisco Catalyst switch επιτρέπει σε οποιονδήποτε να συνδεθεί στη θύρα κονσόλας, να αποκτήσει πρόσβαση στη λειτουργία χρήστη και να μεταβεί στο enable mode και στην λειτουργία διαμόρφωσης χωρίς κανενός είδους ασφάλεια. Αυτή η προεπιλογή είναι λογική, δεδομένου ότι αν μπορείτε να συνδεθείτε στη θύρα κονσόλας του μεταγωγέα, έχετε ήδη τον έλεγχο του μεταγωγέα με φυσικό τρόπο. Ωστόσο, όλοι πρέπει να χειρίζονται μεταγωγείς εξ αποστάσεως και το πρώτο βήμα σε αυτή τη διαδικασία είναι να ασφαλίσετε τον μεταγωγέα έτσι ώστε μόνο οι κατάλληλοι χρήστες να μπορούν να έχουν πρόσβαση στη CLI του μεταγωγέα.

Η προστασία του user mode είναι επίσης σημαντική, επειδή οι επιτιθέμενοι μπορούν να δουν την κατάσταση του μεταγωγέα, να μάθουν για το δίκτυο και να βρουν νέους τρόπους επίθεσης στο δίκτυο.

Όλα τα πρωτόκολλα απομακρυσμένης πρόσβασης και διαχείρισης απαιτούν να έχει ολοκληρωθεί και να λειτουργεί η διαμόρφωση IP του switch. Η διαμόρφωση IPv4 ενός μεταγωγέα δεν έχει καμία σχέση με τον τρόπο με τον οποίο ένας μεταγωγέας επιπέδου 2 προωθεί τα πλαίσια Ethernet. Αντίθετα, για να υποστηριχθούν το Telnet και το Secure Shell σε ένα μεταγωγέα, ο μεταγωγέας πρέπει να έχει διαμορφωθεί με μια διεύθυνση IP

3.9.2 Διασφάλιση της πρόσβασης στο user mode και στο privileged mode με απλούς κωδικούς πρόσβασης

Από προεπιλογή, οι μεταγωγείς Cisco Catalyst επιτρέπουν πλήρη πρόσβαση από την κονσόλα, αλλά όχι πρόσβαση μέσω Telnet ή SSH. Χρησιμοποιώντας τις προεπιλεγμένες ρυθμίσεις, ένας χρήστης της κονσόλας μπορεί να μεταβεί σε λειτουργία χρήστη και στη συνέχεια σε προνομιακή λειτουργία χωρίς να απαιτούνται κωδικοί πρόσβασης. ωστόσο, οι προεπιλεγμένες ρυθμίσεις εμποδίζουν την πρόσβαση απομακρυσμένων χρηστών ακόμη και στη λειτουργία χρήστη.

Οι προεπιλογές λειτουργούν άψογα για ένα ολοκαίνουργιο μεταγωγέα, αλλά στην παραγωγή, θα θέλετε να εξασφαλίσετε την πρόσβαση μέσω της κονσόλας καθώς και να ενεργοποιήσετε την απομακρυσμένη σύνδεση μέσω Telnet ή/και SSH, ώστε να μπορείτε να κάθεστε στο γραφείο σας και να συνδέεστε σε όλους τους μεταγωγείς στο LAN. Δεν πρέπει να ανοίξετε το switch για να συνδεθεί ο οποιοσδήποτε και να αλλάξει τις ρυθμίσεις, οπότε θα πρέπει να χρησιμοποιηθεί κάποιος τύπος ασφαλούς σύνδεσης.

Αυτή η μέθοδος χρησιμοποιεί μόνο έναν κωδικό πρόσβασης -χωρίς όνομα χρήστη- με έναν κωδικό πρόσβασης για τους χρήστες της κονσόλας και έναν διαφορετικό κωδικό πρόσβασης για τους χρήστες Telnet. Οι χρήστες της κονσόλας πρέπει να παρέχουν τον κωδικό πρόσβασης κονσόλας, όπως έχει ρυθμιστεί στη λειτουργία διαμόρφωσης γραμμής κονσόλας. Οι χρήστες Telnet πρέπει να παρέχουν τον κωδικό πρόσβασης Telnet, που ονομάζεται επίσης κωδικός πρόσβασης vty, επειδή η διαμόρφωση βρίσκεται στη λειτουργία διαμόρφωσης γραμμής vty.

Επιπλέον, οι μεταγωγείς της Cisco προστατεύουν το privileged mode με έναν ακόμη κοινόχρηστο κωδικό πρόσβασης που ονομάζεται enable password. Από τη σκοπιά του μηχανικού δικτύου που συνδέεται στο CLI του μεταγωγέα, μόλις εισέλθει σε κατάσταση λειτουργίας χρήστη, ο χρήστης

πληκτρολογεί την εντολή **enable**. Αυτή η εντολή ζητάει από τον χρήστη αυτόν τον κωδικό πρόσβασης enable αν ο χρήστης πληκτρολογήσει τον σωστό κωδικό πρόσβασης, το IOS μετακινεί τον χρήστη στην κατάσταση λειτουργίας enable.

Για να ρυθμίσετε τους κοινόχρηστους κωδικούς πρόσβασης για την κονσόλα, το Telnet και για τη λειτουργία ενεργοποίησης, πρέπει να ρυθμίσετε διάφορες εντολές.

Αυτές είναι οι εξής

Για κωδικό στην console:

line console 0

login

password test

Για κωδικό στο ssh/telnet

line vty 0 15

login

password test1234

Για κωδικό πρόσβασης στο enable mode **enable secret test12345**

Το "login": Λέει στο IOS να ενεργοποιήσει τη χρήση ενός απλού κοινόχρηστου κωδικού πρόσβασης (χωρίς όνομα χρήστη) σε αυτή τη γραμμή (console ή vty), έτσι ώστε το switch να ζητά από το χρήστη έναν κωδικό πρόσβασης

Ο κωδικός πρόσβασης enable, ισχύει για όλους τους χρήστες, ανεξάρτητα από το αν συνδέονται στη λειτουργία χρήστη μέσω της κονσόλας, του Telnet ή με άλλο τρόπο. Η εντολή για τη διαμόρφωση του κωδικού πρόσβασης είναι μια εντολή **enable secret password-value** και δίνεται απο configuration mode

3.9.3 Διασφάλιση της πρόσβασης στο user mode με τοπικά ονόματα χρήστη

Οι μεταγωγείς της Cisco υποστηρίζουν και άλλη μέθοδο σύνδεσης, όπου στην οποία χρησιμοποιούνται ζεύγη ονόματος χρήστη/κωδικού πρόσβασης ανά χρήστη αντί ενός κοινού κωδικού πρόσβασης χωρίς όνομα χρήστη. Οι μεταγωγείς υποστηρίζουν αυτή την επιλογή τοπικού ονόματος χρήστη/κωδικού πρόσβασης για την κονσόλα, για το Telnet και ακόμη και για το SSH, αλλά δεν αντικαθιστούν τον κωδικό πρόσβασης που χρησιμοποιείται για την πρόσβαση στο enable mode
Η ρύθμιση παραμέτρων για τη μετάβαση από τη χρήση των απλών κοινών κωδικών πρόσβασης στη χρήση τοπικών ονομάτων χρήστη/κωδικών πρόσβασης απαιτεί μόνο μερικές μικρές αλλαγές στις ρυθμίσεις,

Πρώτα, το switch πρέπει φυσικά να γνωρίζει τη λίστα των ζευγών ονόματος χρήστη/κωδικού πρόσβασης. Για να τα δημιουργήσετε αυτά, χρησιμοποιήστε επανειλημμένα την εντολή στο global configuration **username name secret password**. Στη συνέχεια, για να ενεργοποιήσετε αυτόν τον διαφορετικό τύπο ασφάλειας της κονσόλας ή του Telnet, απλώς ενεργοποιήστε αυτή τη μέθοδο ασφάλειας σύνδεσης με τη γραμμή **login local**. Βασικά, αυτή η εντολή σημαίνει «χρησιμοποιήστε την τοπική λίστα ονομάτων χρήστη για την είσοδο». Μπορείτε επίσης να χρησιμοποιήσετε την εντολή **no password** (χωρίς καν να πληκτρολογήσετε τον κωδικό πρόσβασης) για να καθαρίσετε όλες τις

υποεντολές κωδικού πρόσβασης που έχουν απομείνει από τη λειτουργία κονσόλας ή vty, επειδή αυτές οι εντολές δεν χρειάζονται όταν χρησιμοποιούνται τοπικά ονόματα χρηστών και κωδικοί πρόσβασης.

Όταν ένας χρήστης Telnet συνδέεται στο μεταγωγέα που έχει ρυθμιστεί έτσι, ο χρήστης θα κληθεί πρώτα να δώσει ένα όνομα χρήστη και στη συνέχεια έναν κωδικό πρόσβασης. Το ζεύγος ονόματος χρήστη/κωδικού πρόσβασης πρέπει να είναι από τη λίστα των τοπικών ονομάτων χρήστη- διαφορετικά, η σύνδεση απορρίπτεται.

3.9.4 Διασφάλιση απομακρυσμένης πρόσβασης με Secure Shell

Το Telnet έχει ένα σοβαρό μειονέκτημα, οποιοσδήποτε μπορεί να καταγράψει τα μηνύματα μεταξύ του χρήστη και του switch (χρησιμοποιώντας μια επίθεση τύπου man-in-the-middle)και μπορεί να δει τους κωδικούς πρόσβασης. Το SSH κρυπτογραφεί όλα τα δεδομένα που μεταδίδονται μεταξύ του πελάτη και του διακομιστή SSH, προστατεύοντας τα δεδομένα και τους κωδικούς πρόσβασης.

Παρατίθεται ενδεικτικά μια διαμόρφωση για την πρόσβαση με SSH.

Από το configuration mode του switch δίνονται οι παρακάτω εντολές

hostname SW1

ip domain-name sindos.com

crypto key generate rsa modulus 2048

Για τους χρήστες

username testuser 1 secret test1

username testuser2 secret test2

Στην γραμμή vty

line vty 0 15

login local

Το IOS χρησιμοποιεί τις τρεις ειδικές εντολές διαμόρφωσης SSH για τη δημιουργία των κλειδιών κρυπτογράφησης SSH. Ο διακομιστής SSH χρησιμοποιεί το πλήρως προσδιορισμένο όνομα τομέα (Fully Qualified Domain Name FQDN) του switch ως είσοδο για τη δημιουργία αυτού του κλειδιού. Ο μεταγωγέας δημιουργεί το FQDN από το hostname και το domain name.. Στη συνέχεια, η τρίτη εντολή, η εντολή **crypto key generate rsa,** δημιουργεί τα κλειδιά κρυπτογράφησης SSH.

Το IOS εκτελεί έναν διακομιστή SSH από προεπιλογή. Επιπλέον, το IOS επιτρέπει από προεπιλογή συνδέσεις SSH στις γραμμές vty.

Μια χρήσιμη προεπιλογή ήταν ότι το switch υποστηρίζει τόσο το SSH όσο και το Telnet στις γραμμές vty. Ωστόσο, επειδή το Telnet αποτελεί κίνδυνο για την ασφάλεια, θα μπορούσατε να απενεργοποιήσετε το Telnet για να επιβάλλετε μια αυστηρότερη πολιτική ασφαλείας.

Για να ελέγξετε ποια πρωτόκολλα υποστηρίζει ένα switch στις γραμμές vty, χρησιμοποιήστε την υποεντολή **transport input {all | none | telnet | ssh}** στη λειτουργία vty, με τις ακόλουθες επιλογές:

transport input all: Υποστήριξη Telnet και SSH

transport input none: Δεν υποστηρίζει κανένα από τα δύο

transport input telnet: Υποστήριξη μόνο του Telnet

transport input ssh: Υποστήριξη μόνο SSH

Ακολουθεί η λίστα ελέγχου διαμόρφωσης που περιγράφει λεπτομερώς τα βήματα για μια μέθοδο διαμόρφωσης ενός μεταγωγέα Cisco για την υποστήριξη του SSH με χρήση τοπικών ονομάτων χρήστη.

Βήμα 1. Διαμορφώστε το μεταγωγέα για τη δημιουργία ενός ζευγαριού δημόσιου και ιδιωτικού κλειδιού που θα χρησιμοποιηθεί για κρυπτογράφηση:

A. Εάν δεν έχει ήδη ρυθμιστεί, χρησιμοποιήστε **hostname** στη λειτουργία global configuration για να διαμορφώσετε ένα όνομα για αυτό το μεταγωγέα.

B. Εάν δεν έχει ήδη ρυθμιστεί, χρησιμοποιήστε το **ip domain-name name** στην κατάσταση λειτουργίας global configuration για να διαμορφώσετε ένα όνομα τομέα για το μεταγωγέα, συμπληρώνοντας το FQDN του μεταγωγέα.

C. Χρησιμοποιήστε την εντολή **crypto key generate rsa** σε κατάσταση λειτουργίας global configuration (ή την εντολή **crypto key generate rsa modulus modulus-value** για να αποφύγετε την ερώτηση για το modulus του κλειδιού) για να δημιουργήσετε τα κλειδιά. (Χρησιμοποιήστε τουλάχιστον ένα κλειδί 768 bit για να υποστηρίξετε την έκδοση 2 του SSH).

Βήμα 2. (Προαιρετικό) Χρησιμοποιήστε την εντολή **ip ssh version 2** στη λειτουργία global configuration για να παρακάμψετε την προεπιλογή της υποστήριξης και των εκδόσεων 1 και 2, ώστε να επιτρέπονται μόνο οι συνδέσεις SSHv2.

Βήμα 3. (Προαιρετικά) Εάν δεν έχει ήδη ρυθμιστεί με τη ρύθμιση που θέλετε, ρυθμίστε τις γραμμές vty για να δέχονται SSH και αν θα επιτρέπουν επίσης το Telnet:

A. Χρησιμοποιήστε την εντολή **transport input ssh** στη λειτουργία διαμόρφωσης γραμμής vty για να επιτρέπετε μόνο το SSH.

B. Χρησιμοποιήστε την εντολή **transport input all** (προεπιλογή) ή την εντολή **transport input telnet ssh** στη λειτουργία διαμόρφωσης γραμμής vty για να επιτρέψετε τόσο το SSH όσο και το Telnet.

Βήμα 4. Χρησιμοποιήστε διάφορες εντολές στη λειτουργία διαμόρφωσης γραμμής vty για να ρυθμίσετε τον τοπικό έλεγχο ταυτότητας σύνδεσης με όνομα χρήστη.

Δύο βασικές εντολές παρέχουν κάποιες πληροφορίες σχετικά με την κατάσταση του SSH στο μεταγωγέα. Η εντολή **show ip ssh** παραθέτει πληροφορίες κατάστασης για τον ίδιο το διακομιστή SSH. Στη συνέχεια, η εντολή **show ssh** παραθέτει πληροφορίες για κάθε πελάτη SSH που είναι συνδεδεμένος αυτή τη στιγμή στο μεταγωγέα.

3.10 Ενεργοποίηση IPv4 για απομακρυσμένη πρόσβαση

Για να επιτραπεί η πρόσβαση Telnet ή SSH στο μεταγωγέα και για να επιτραπεί η λειτουργία άλλων πρωτοκόλλων διαχείρισης που βασίζονται σε IP (για παράδειγμα, Simple Network Management Protocol ή SNMP), ο μεταγωγέας χρειάζεται μια διεύθυνση IP, καθώς και μερικές άλλες σχετικές ρυθμίσεις. Η διεύθυνση IP δεν έχει καμία σχέση με τον τρόπο με τον οποίο οι μεταγωγείς προωθούν τα πλαίσια Ethernet- υπάρχει απλώς για να υποστηρίζει την κίνηση διαχείρισης.

Ένας μεταγωγέας χρειάζεται το ίδιο είδος ρυθμίσεων IP όπως ένας υπολογιστής με μία μόνο διασύνδεση Ethernet. Για παράδειγμα, ένας υπολογιστής διαθέτει μια CPU, με το λειτουργικό σύστημα να εκτελείται στην CPU. Διαθέτει μια κάρτα διασύνδεσης δικτύου Ethernet (NIC). Οι ρυθμίσεις του

λειτουργικού συστήματος περιλαμβάνουν μια διεύθυνση IP που σχετίζεται με τη NIC, η οποία είτε έχει ρυθμιστεί είτε έχει ληφθεί δυναμικά με DHCP.

Ένας μεταγωγέας χρησιμοποιεί τις ίδιες ιδέες, με τη διαφορά ότι ο μεταγωγέας πρέπει να χρησιμοποιεί μια εικονική NIC. Όπως ένας υπολογιστής, ένα switch διαθέτει μια πραγματική CPU, η οποία εκτελεί ένα λειτουργικό σύστημα (που ονομάζεται IOS). Ο μεταγωγέας προφανώς διαθέτει πολλές θύρες Ethernet, αλλά αντί να εκχωρήσει τη διεύθυνση IP διαχείρισης σε οποιαδήποτε από αυτές τις θύρες, ο μεταγωγέας χρησιμοποιεί στη συνέχεια μια έννοια που μοιάζει με NIC και ονομάζεται εικονική διεπαφή μεταγωγής (SVI-switched virtual interface), ή συνηθέστερα, VLAN interface, η οποία ενεργεί σαν την NIC του μεταγωγέα. Οι ρυθμίσεις στο μεταγωγέα μοιάζουν κάπως με έναν κεντρικό υπολογιστή, με το interface στο vlan να παίρνει την κατάλληλη IP

Για παράδειγμα

interface vlan 1

ip address 192.168.1.10 255.255.255.0

Χρησιμοποιώντας τη διασύνδεση VLAN 1 για τη διαμόρφωση IP, ο μεταγωγέας μπορεί στη συνέχεια να στέλνει και να λαμβάνει πλαίσια σε οποιαδήποτε από τις θύρες του VLAN 1. Σε ένα μεταγωγέα Cisco, από προεπιλογή, όλες οι θύρες αντιστοιχίζονται στο VLAN 1.

Στα περισσότερα δίκτυα, οι μεταγωγείς διαμορφώνουν πολλά VLAN, οπότε ο μηχανικός δικτύου έχει τη δυνατότητα να επιλέξει πού θα διαμορφώσει τη διεύθυνση IP. Δηλαδή, η διεύθυνση IP διαχείρισης δεν χρειάζεται να διαμορφωθεί στη διασύνδεση VLAN 1

Ένας μεταγωγέας LAN επιπέδου 2 της Cisco χρειάζεται μόνο μία διεύθυνση IP για σκοπούς διαχείρισης. Ωστόσο, μπορείτε να επιλέξετε να χρησιμοποιήσετε οποιοδήποτε VLAN στο οποίο συνδέεται ο μεταγωγέας. Η διαμόρφωση περιλαμβάνει τότε μια διασύνδεση VLAN για αυτόν τον αριθμό VLAN, με μια κατάλληλη διεύθυνση IP.

Προσοχή, δεν θα πρέπει να προσπαθήσετε να χρησιμοποιήσετε μια διασύνδεση VLAN για την οποία δεν υπάρχουν φυσικές θύρες εκχωρημένες στο ίδιο VLAN. Εάν το κάνετε, η διασύνδεση VLAN δεν θα φτάσει σε κατάσταση up/up και ο μεταγωγέας δεν θα έχει τη φυσική δυνατότητα να επικοινωνεί εκτός του μεταγωγέα.

Η διαμόρφωση της διεύθυνσης IP (και της μάσκας) σε μια διασύνδεση VLAN επιτρέπει στο μεταγωγέα να στέλνει και να λαμβάνει πακέτα IP με άλλους κεντρικούς υπολογιστές σε ένα υποδίκτυο που υπάρχει σε αυτό το VLAN ωστόσο, ο μεταγωγέας δεν μπορεί να επικοινωνήσει εκτός του τοπικού υποδικτύου χωρίς μια άλλη ρύθμιση διαμόρφωσης που ονομάζεται προεπιλεγμένη πύλη. Ο λόγος για τον οποίο ένας μεταγωγέας χρειάζεται μια ρύθμιση προεπιλεγμένης πύλης είναι ο ίδιος λόγος για τον οποίο οι κεντρικοί υπολογιστές χρειάζονται την ίδια ρύθμιση εξαιτίας του τρόπου με τον οποίο οι κεντρικοί υπολογιστές σκέφτονται όταν στέλνουν πακέτα IP. Συγκεκριμένα:

Για να στείλετε πακέτα IP σε κεντρικούς υπολογιστές στο ίδιο υποδίκτυο, στείλτε τα απευθείας

Για να στείλετε πακέτα IP σε κεντρικούς υπολογιστές σε διαφορετικό υποδίκτυο, στείλτε τα στον τοπικό δρομολογητή, δηλαδή στην προεπιλεγμένη πύλη.

3.10.1 Ρύθμιση IPv4 σε έναν μεταγωγέα

Ένας μεταγωγέας διαμορφώνει τη διεύθυνση και τη μάσκα IPv4 σε αυτή την ειδική διασύνδεση VLAN που μοιάζει με NIC. Τα παρακάτω βήματα παραθέτουν τις εντολές που χρησιμοποιούνται για τη

διαμόρφωση του IPv4 σε ένα μεταγωγέα, υποθέτοντας ότι η διεύθυνση IP έχει ρυθμιστεί ώστε να ανήκει στο VLAN 1

Λίστα ελέγχου διαμόρφωσης:

Βήμα 1. Χρησιμοποιήστε την εντολή **interface vlan 1** στην κατάσταση global configuration mode για να εισέλθετε στη λειτουργία διαμόρφωσης της διασύνδεσης VLAN 1.

Βήμα 2. Χρησιμοποιήστε την εντολή **ip address ip-address mask** στη λειτουργία διαμόρφωσης διασύνδεσης για να εκχωρήσετε μια διεύθυνση IP και μια μάσκα.

Βήμα 3. Χρησιμοποιήστε την εντολή **no shutdown** στη λειτουργία διαμόρφωσης διασύνδεσης για να ενεργοποιήσετε τη διασύνδεση VLAN 1, εάν δεν είναι ήδη ενεργοποιημένη.

Βήμα 4. Προσθέστε την εντολή **ip default-gateway ip-address** στη λειτουργία global configuration για να ρυθμίσετε την προεπιλεγμένη πύλη.

Βήμα 5. (Προαιρετικό) Προσθέστε την εντολή **ip name-server ip-address1 ip-address2** ... σε κατάσταση λειτουργίας global configuration για να ρυθμίσετε το μεταγωγέα ώστε να χρησιμοποιεί το σύστημα Domain Name System (DNS) για την επίλυση ονομάτων στην αντίστοιχη διεύθυνση IP.

Αυτό το παράδειγμα δείχνει μια ιδιαίτερα σημαντική και κοινή εντολή: την εντολή **[no] shutdown**. Για να ενεργοποιήσετε μια διασύνδεση σε ένα μεταγωγέα, χρησιμοποιήστε την υποεντολή **no shutdown interface.** Για να απενεργοποιήσετε μια διασύνδεση, χρησιμοποιήστε την υποεντολή **shutdown interface.** Αυτή η εντολή μπορεί να χρησιμοποιηθεί στις φυσικές διασυνδέσεις Ethernet που χρησιμοποιεί ο μεταγωγέας για τη μεταγωγή μηνυμάτων Ethernet εκτός από τη διασύνδεση VLAN που παρουσιάζεται εδώ σε αυτό το παράδειγμα.

3.10.2 Επαλήθευση του IPv4 σε ένα μεταγωγέα

Η διαμόρφωση IPv4 του μεταγωγέα μπορεί να ελεγχθεί σε διάφορα σημεία. Πρώτον, μπορείτε πάντα να δείτε την τρέχουσα διαμόρφωση χρησιμοποιώντας την εντολή **show running-config**. Δεύτερον, μπορείτε να δείτε τις πληροφορίες διεύθυνσης IP και μάσκας χρησιμοποιώντας την εντολή **show interfaces vlan x**, η οποία εμφανίζει λεπτομερείς πληροφορίες κατάστασης για τη διασύνδεση VLAN στο VLAN x. Τέλος, αν χρησιμοποιείτε DHCP, χρησιμοποιήστε την εντολή **show dhcp lease** για να δείτε την (προσωρινά) μισθωμένη διεύθυνση IP και άλλες παραμέτρους. (Σημειώστε ότι ο μεταγωγέας δεν αποθηκεύει τη διαμόρφωση IP που μαθαίνει το DHCP στο αρχείο running-config).
Η έξοδος της εντολής **show interfaces vlan 1** παραθέτει δύο πολύ σημαντικές λεπτομέρειες που σχετίζονται με τη διευθυνσιοδότηση IP του μεταγωγέα. Πρώτον, αυτή η εντολή **show** παραθέτει την κατάσταση διασύνδεσης της διασύνδεσης VLAN 1. Εάν η διασύνδεση VLAN 1 δεν είναι ενεργή, ο μεταγωγέας δεν μπορεί να χρησιμοποιήσει τη διεύθυνση IP της για να στείλει και να λάβει κίνηση διαχείρισης. Ειδικότερα, εάν ξεχάσετε να εκδώσετε την εντολή **no shutdown**, η διασύνδεση VLAN 1 παραμένει στην προεπιλεγμένη κατάσταση τερματισμού λειτουργίας και αναφέρεται ως «administratively down» στην έξοδο της εντολής **show**

3.11 Επίλογος

Κλείνοντας το κεφάλαιο έχουν πραγματοποιηθεί οι βασικές ρυθμίσεις πρόσβασης και διαχείρισης ενός μεταγωγέα καθώς και επισκόπηση της λογικής μεταγωγής και θα ακολουθήσουν προηγμένες ρυθμίσεις στους μεταγωγείς.

Κεφάλαιο 4ο: VLANs

Τα VLAN επιτρέπουν σε έναν μηχανικό δικτύου να δημιουργήσει ξεχωριστά τοπικά δίκτυα Ethernet μέσω απλών επιλογών διαμόρφωσης. Η δυνατότητα διαχωρισμού ορισμένων θυρών μεταγωγής σε ένα VLAN A και άλλων θυρών μεταγωγής σε ένα άλλο VLAN B δίνει στους σχεδιαστές δικτύων ένα ισχυρό εργαλείο για τη δημιουργία δικτύων. Μόλις δημιουργηθούν, τα VLANs έχουν επίσης τεράστιο αντίκτυπο στον τρόπο λειτουργίας ενός μεταγωγέα, ο οποίος στη συνέχεια επηρεάζει τον τρόπο επαλήθευσης και αντιμετώπισης προβλημάτων της λειτουργίας ενός campus LAN.

Με τη χρήση δύο VLAN, ένας μόνο μεταγωγέας μπορεί να επιτύχει την δημιουργία δύο τομέων μετάδοσης, με έναν μόνο μεταγωγέα. Με τα VLANs, ένας μεταγωγέας μπορεί να ρυθμίσει ορισμένες διασυνδέσεις σε ένα πεδίο εκπομπής και ορισμένες σε ένα άλλο, δημιουργώντας πολλαπλά πεδία εκπομπής. Αυτά τα μεμονωμένα πεδία εκπομπής που δημιουργούνται από το μεταγωγέα ονομάζονται εικονικά τοπικά δίκτυα (VLAN).

Το STP -και το σχετικό και παρόμοιο Rapid STP (RSTP)- δρα για να αποτρέπει την περιδίνηση πλαισίων σε ένα LAN. Χωρίς το STP ή το RSTP, σε LANs με πλεονάζουσες συνδέσεις, broadcasts και ορισμένα άλλα πλαίσια θα προωθούνταν γύρω-γύρω στο LAN, με αποτέλεσμα τελικά να φράξουν το LAN τόσο πολύ, ώστε να το καταστήσουν άχρηστο.

Οι μεταγωγείς Ethernet λαμβάνουν πλαίσια Ethernet, λαμβάνουν αποφάσεις και στη συνέχεια προωθούν (μεταβιβάζουν) αυτά τα πλαίσια Ethernet. Αυτή η βασική λογική περιστρέφεται γύρω από τις διευθύνσεις MAC, τη διασύνδεση στην οποία φτάνει το πλαίσιο και τις διασυνδέσεις από τις οποίες ο μεταγωγέας προωθεί το πλαίσιο.

Αυτή η λογική παραλείπει κάθε εξέταση των εικονικών τοπικών δικτύων (VLAN). Τα VLANs επηρεάζουν τη λογική μεταγωγής για κάθε πλαίσιο, επειδή κάθε VLAN λειτουργεί ως υποσύνολο των θυρών μεταγωγής σε ένα LAN Ethernet. Οι μεταγωγείς πιστεύουν ότι κάθε πλαίσιο Ethernet λαμβάνεται σε ένα αναγνωρίσιμο VLAN, προωθείται με βάση τις καταχωρήσεις του πίνακα MAC για αυτό το VLAN και προωθείται από τις θύρες σε αυτό το VLAN.

4.1 Virtual LAN Concepts

Προτού κατανοήσετε τα VLANs, πρέπει πρώτα να έχετε κατανοήσει τον ορισμό ενός τοπικού δικτύου. Για παράδειγμα, ένα LAN περιλαμβάνει όλες τις συσκευές χρηστών, τους διακομιστές, τους μεταγωγείς, τους δρομολογητές, τα καλώδια και τα σημεία ασύρματης πρόσβασης σε μια τοποθεσία. Ωστόσο, ένας εναλλακτικός στενότερος ορισμός ενός LAN μπορεί να βοηθήσει στην κατανόηση της έννοιας ενός εικονικού LAN:

Ένα τοπικό δίκτυο περιλαμβάνει όλες τις συσκευές στον ίδιο τομέα εκπομπής(broadcast domain).

Ένας τομέας εκπομπής περιλαμβάνει το σύνολο όλων των συσκευών που είναι συνδεδεμένες στο LAN, έτσι ώστε όταν κάποια από τις συσκευές στέλνει ένα πλαίσιο εκπομπής, όλες οι άλλες συσκευές λαμβάνουν ένα αντίγραφο του πλαισίου. Έτσι, από μια άποψη, μπορείτε να θεωρήσετε ότι ένα LAN και ένας τομέας εκπομπής είναι ουσιαστικά το ίδιο πράγμα.

Χρησιμοποιώντας μόνο τις προεπιλεγμένες ρυθμίσεις, ένας μεταγωγέας θεωρεί ότι όλες οι διασυνδέσεις του βρίσκονται στον ίδιο τομέα εκπομπής. Δηλαδή, για ένα μεταγωγέα, όταν ένα πλαίσιο εκπομπής εισέλθει σε μια θύρα του μεταγωγέα, ο μεταγωγέας προωθεί αυτό το πλαίσιο εκπομπής σε όλες τις

άλλες θύρες(αν υπάρχει η mac address του προορισμού στο mac address table το προωθεί στο κατάλληλο interface). Με αυτή τη λογική, για να δημιουργήσετε δύο διαφορετικούς τομείς εκπομπής LAN, έπρεπε να αγοράσετε δύο διαφορετικούς μεταγωγείς Ethernet LAN .

Ο σχεδιασμός των τοπικών δικτύων για τη χρήση περισσότερων VLAN, το καθένα με μικρότερο αριθμό συσκευών, συχνά βοηθά στη βελτίωση του τοπικού δικτύου με πολλούς τρόπους. Για παράδειγμα, μια εκπομπή που αποστέλλεται από έναν υπολογιστή σε ένα VLAN θα ληφθεί και θα επεξεργαστεί από όλους τους άλλους υπολογιστές στο VLAN - αλλά όχι από υπολογιστές σε διαφορετικό VLAN. Ο περιορισμός του αριθμού των κεντρικών υπολογιστών που λαμβάνουν ένα ενιαίο πλαίσιο εκπομπής μειώνει τον αριθμό των κεντρικών υπολογιστών που σπαταλούν προσπάθεια για την επεξεργασία μη αναγκαίων εκπομπών. Επίσης, μειώνει τους κινδύνους ασφαλείας, επειδή λιγότεροι κεντρικοί υπολογιστές βλέπουν τα πλαίσια που αποστέλλονται από οποιονδήποτε κεντρικό υπολογιστή. Αυτοί είναι μερικοί μόνο λόγοι για το διαχωρισμό των κεντρικών υπολογιστών σε διαφορετικά VLAN. Η ακόλουθη λίστα συνοψίζει τους πιο συνηθισμένους λόγους για την επιλογή της δημιουργίας μικρότερων περιοχών εκπομπής (VLAN):

> Μείωση της επιβάρυνσης της CPU σε κάθε συσκευή, βελτιώνοντας την απόδοση του κεντρικού υπολογιστή, μειώνοντας τον αριθμό των συσκευών που λαμβάνουν κάθε πλαίσιο εκπομπής.

> Μείωση των κινδύνων ασφαλείας, μειώνοντας τον αριθμό των κεντρικών υπολογιστών που λαμβάνουν αντίγραφα των πλαισίων που κατακλύζουν οι μεταγωγείς (broadcasts, multicasts και unknown unicasts).

> Βελτίωση της ασφάλειας για τους κεντρικούς υπολογιστές μέσω της εφαρμογής διαφορετικών πολιτικών ασφαλείας ανά VLAN

> Δημιουργία πιο ευέλικτων σχεδίων που ομαδοποιούν τους χρήστες ανά τμήμα ή ανά ομάδες που συνεργάζονται, αντί για φυσική τοποθεσία

> Ταχύτερη επίλυση προβλημάτων, επειδή ο τομέας αποτυχίας για πολλά προβλήματα είναι το ίδιο σύνολο συσκευών με εκείνες που βρίσκονται στον ίδιο τομέα εκπομπής

> Μείωση του φόρτου εργασίας για το πρωτόκολλο Spanning Tree Protocol (STP) με τον περιορισμό ενός VLAN σε ένα μόνο μεταγωγέα πρόσβασης.

4.2 Vlan trunking

Η διαμόρφωση των VLANs σε ένα ενιαίο switch απαιτεί μόνο λίγη προσπάθεια: απλά ρυθμίζετε κάθε θύρα ώστε να του πείτε τον αριθμό VLAN στον οποίο ανήκει η θύρα. Με πολλούς μεταγωγείς, πρέπει να εξετάσετε πρόσθετες έννοιες σχετικά με τον τρόπο προώθησης της κυκλοφορίας μεταξύ των μεταγωγέων.

Όταν χρησιμοποιείτε VLANs σε δίκτυα που έχουν πολλαπλά διασυνδεδεμένα μεταγωγείς, οι μεταγωγείς πρέπει να χρησιμοποιούν VLAN trunking στις συνδέσεις μεταξύ των μεταγωγέων. Το trunking αναγκάζει τα μεταγωγείς να χρησιμοποιούν μια διαδικασία που ονομάζεται VLAN tagging, με την οποία ο αποστέλλων μεταγωγέας προσθέτει μια άλλη επικεφαλίδα στο πλαίσιο πριν το στείλει μέσω του trunk. Αυτή η πρόσθετη επικεφαλίδα trunking περιλαμβάνει ένα πεδίο αναγνώρισης VLAN (VLAN ID), έτσι ώστε το μεταγωγέας αποστολής να μπορεί να συσχετίσει το πλαίσιο με ένα συγκεκριμένο VLAN ID και ο μεταγωγέας λήψης να γνωρίζει στη συνέχεια σε ποιο VLAN ανήκει κάθε πλαίσιο.

4.3 VLAN Tagging

Το VLAN trunking δημιουργεί μια σύνδεση μεταξύ μεταγωγέων που υποστηρίζει όσα VLAN χρειάζεστε. Ως VLAN trunk, οι μεταγωγείς αντιμετωπίζουν τη σύνδεση σαν να ήταν μέρος όλων των VLANs. Ταυτόχρονα, το trunk διατηρεί την κυκλοφορία VLAN ξεχωριστά, έτσι ώστε τα πλαίσια στο VLAN 10 να μην πηγαίνουν σε συσκευές στο VLAN 20 και το αντίστροφο, επειδή κάθε πλαίσιο αναγνωρίζεται από τον αριθμό VLAN καθώς διασχίζει το trunk link.
Η χρήση του επιτρέπει στους μεταγωγείς να προωθούν πλαίσια από πολλαπλά VLANs μέσω μιας μόνο φυσικής σύνδεσης, προσθέτοντας μια μικρή επικεφαλίδα στο πλαίσιο Ethernet. Για παράδειγμα, το PC10 στέλνει ένα πλαίσιο εκπομπής στη διασύνδεση Fa0/1. Για να προωθήσει το πλαίσιο, ο μεταγωγέας SW1 πρέπει να προωθήσει το πλαίσιο εκπομπής στο μεταγωγέα SW2. Ωστόσο, το SW1 πρέπει να ενημερώσει το SW2 ότι το πλαίσιο είναι μέρος του VLAN 10, έτσι ώστε μετά τη λήψη του πλαισίου, το SW2 να στείλει το πλαίσιο μόνο στο VLAN 10 και όχι στο VLAN 20. Έτσι, πριν από την αποστολή του πλαισίου, ο SW1 προσθέτει μια επικεφαλίδα VLAN στο αρχικό πλαίσιο Ethernet, με την επικεφαλίδα VLAN να αναφέρει ένα αναγνωριστικό VLAN 10 σε αυτή την περίπτωση. Όταν το SW2 λαμβάνει το πλαίσιο, καταλαβαίνει ότι το πλαίσιο ανήκει στο VLAN 10. Στη συνέχεια, το SW2 αφαιρεί την επικεφαλίδα VLAN, προωθώντας το αρχικό πλαίσιο από τις διασυνδέσεις του στο VLAN 10.

4.4 Τα πρωτόκολλα 802.1Q και ISL VLAN Trunking

Η Cisco έχει υποστηρίξει δύο διαφορετικά trunking πρωτόκολλα με την πάροδο των ετών: Inter-Switch Link (ISL) και IEEE 802.1Q. Η Cisco δημιούργησε το ISL χρόνια πριν από το 802.1Q, εν μέρει επειδή το IEEE δεν είχε ακόμη ορίσει ένα πρότυπο trunking VLAN. Σήμερα, το 802.1Q έχει γίνει το πιο δημοφιλές πρωτόκολλο trunking, με τη Cisco να μην μπαίνει καν στον κόπο να υποστηρίξει το ISL σε πολλά από τα μοντέλα μεταγωγέων της σήμερα.

Ενώ τόσο το ISL όσο και το 802.1Q επισημαίνουν κάθε πλαίσιο με το αναγνωριστικό VLAN, οι λεπτομέρειες διαφέρουν. Το 802.1Q εισάγει μια επιπλέον επικεφαλίδα 802.1Q VLAN 4 byte στην αρχική επικεφαλίδα Ethernet του πλαισίου.Όσον αφορά τα πεδία στην επικεφαλίδα 802.1Q, μόνο το πεδίο 12-bit VLAN ID μέσα στην επικεφαλίδα 802.1Q έχει σημασία. Αυτό το πεδίο των 12 bit υποστηρίζει θεωρητικά το μέγιστο των 4096 VLANs, αλλά στην πράξη υποστηρίζει το μέγιστο των 4094. (Τόσο το 802.1Q όσο και το ISL χρησιμοποιούν 12 bit για την επισήμανση του αναγνωριστικού VLAN, με δύο δεσμευμένες τιμές [0 και 4095]).

Οι μεταγωγείς της Cisco χωρίζουν το εύρος των αναγνωριστικών VLAN (1-4094) σε δύο περιοχές: την κανονική περιοχή και την εκτεταμένη περιοχή. Όλοι οι μεταγωγείς μπορούν να χρησιμοποιούν VLANs κανονικής εμβέλειας με τιμές από 1 έως 1005. Μόνο ορισμένοι μεταγωγείς μπορούν να χρησιμοποιούν VLANs εκτεταμένης εμβέλειας με αναγνωριστικά VLAN από 1006 έως 4094. Οι κανόνες για το ποιοι μεταγωγείς μπορούν να χρησιμοποιήσουν VLANs εκτεταμένης εμβέλειας εξαρτώνται από τη διαμόρφωση του πρωτοκόλλου trunking VLAN (VTP).

Το 802.1Q ορίζει επίσης ένα ειδικό αναγνωριστικό VLAN σε κάθε trunk ως το native VLAN (με προεπιλογή τη χρήση του VLAN 1). Εξ ορισμού, το 802.1Q απλώς δεν προσθέτει επικεφαλίδα 802.1Q στα πλαίσια στο native VLAN. Όταν ο μεταγωγέας στην άλλη πλευρά του trunk λαμβάνει ένα πλαίσιο που δεν έχει επικεφαλίδα 802.1Q, ο παραλήπτης μεταγωγέας γνωρίζει ότι το πλαίσιο ανήκει στο native VLAN. Σημειώστε ότι εξαιτίας αυτής της συμπεριφοράς, και οι δύο μεταγωγείς πρέπει να συμφωνήσουν σχετικά με το ποιο VLAN είναι το native VLAN.

Το native VLAN 802.1Q παρέχει ορισμένες ενδιαφέρουσες λειτουργίες, κυρίως για την υποστήριξη συνδέσεων με συσκευές που δεν κατανοούν το trunking. Για παράδειγμα, ένας μεταγωγέας Cisco θα μπορούσε να συνδεθεί με καλώδιο σε έναν μεταγωγέα που δεν κατανοεί το 802.1Q trunking. Ο μεταγωγέας Cisco θα μπορούσε να στέλνει πλαίσια στο native VLAN - που σημαίνει ότι το πλαίσιο δεν έχει επικεφαλίδα trunking - έτσι ώστε ο άλλος μεταγωγέας να καταλαβαίνει το πλαίσιο. Η έννοια του native VLAN δίνει στους μεταγωγείς τη δυνατότητα να περνούν τουλάχιστον την κυκλοφορία σε ένα VLAN (το native VLAN), το οποίο μπορεί να επιτρέψει ορισμένες βασικές λειτουργίες, όπως η προσβασιμότητα για telnet σε ένα μεταγωγέα.

4.5 Προώθηση δεδομένων μεταξύ VLANs

Εάν δημιουργήσετε ένα τοπικό δίκτυο που περιέχει πολλά VLANs, συνήθως εξακολουθείτε να χρειάζεστε όλες οι συσκευές να μπορούν να στέλνουν δεδομένα σε όλες τις άλλες συσκευές. Αυτό το επόμενο θέμα εξετάζει ορισμένες έννοιες σχετικά με τον τρόπο δρομολόγησης δεδομένων μεταξύ αυτών των VLAN.

4.5.1 Η ανάγκη για δρομολόγηση μεταξύ VLANs

Όταν συμπεριλαμβάνετε VLANs σε ένα εταιρικό LAN, οι συσκευές σε ένα VLAN πρέπει να βρίσκονται στο ίδιο υποδίκτυο. Ακολουθώντας την ίδια λογική σχεδιασμού, οι συσκευές σε διαφορετικά VLAN πρέπει να βρίσκονται σε διαφορετικά υποδίκτυα.

Για την προώθηση πακέτων μεταξύ των VLAN, το δίκτυο πρέπει να χρησιμοποιεί μια συσκευή που λειτουργεί ως δρομολογητής. Μπορείτε να χρησιμοποιήσετε έναν πραγματικό δρομολογητή, καθώς και κάποιους άλλους μεταγωγείς που μπορούν να εκτελέσουν ορισμένες λειτουργίες όπως ένας δρομολογητής. Αυτοί οι μεταγωγείς που εκτελούν επίσης λειτουργίες δρομολόγησης επιπέδου 3 φέρουν την ονομασία μεταγωγέας πολλαπλών επιπέδων ή μεταγωγέας επιπέδου 3.

Για παράδειγμα, έστω ένας δρομολογητής που μπορεί να δρομολογήσει πακέτα μεταξύ των υποδικτύων 10 και 20. Ο δρομολογητής R1 έχει μια φυσική διεπαφή LAN συνδεδεμένη στο μεταγωγέα και εκχωρημένη στο VLAN 10, μια δεύτερη φυσική διεπαφή συνδεδεμένη στο μεταγωγέα και εκχωρημένη στο VLAN 20. Με μια διασύνδεση συνδεδεμένη σε κάθε υποδίκτυο, ο μεταγωγέας επιπέδου 2 μπορεί να συνεχίσει να κάνει τη δουλειά του-προώθηση πλαισίων εντός ενός VLAN, ενώ ο δρομολογητής μπορεί να κάνει τη δουλειά του-δρομολόγηση πακέτων IP μεταξύ των υποδικτύων.

4.5.2 Διαμόρφωση και επαλήθευση LAN και VLAN Trunking Configuration

Οι μεταγωγείς της Cisco δεν απαιτούν καμία διαμόρφωση για να λειτουργήσουν. Μπορείτε να αγοράσετε μεταγωγείς Cisco, να εγκαταστήσετε συσκευές με τη σωστή καλωδίωση, να ενεργοποιήσετε τους μεταγωγείς και αυτοί θα λειτουργήσουν. Δεν θα χρειαστεί ποτέ να διαμορφώσετε τον μεταγωγέα και θα λειτουργούσε άψογα, ακόμη και αν συνδέατε μεταγωγείς μεταξύ τους, μέχρι να χρειαστείτε περισσότερα από ένα VLAN. Αλλά αν θέλετε να χρησιμοποιήσετε VLANs -και τα περισσότερα δίκτυα επιχειρήσεων το κάνουν- πρέπει να προσθέσετε κάποια διαμόρφωση.

4.5.3 Δημιουργία VLANs και εκχώρηση access VLANs πρόσβασης σε interface

Για να προωθήσει ένα μεταγωγέας Cisco πλαίσια σε ένα συγκεκριμένο VLAN, ο μεταγωγέας πρέπει να ρυθμιστεί ώστε να πιστεύει ότι το VLAN υπάρχει. Επιπλέον, ο μεταγωγέας πρέπει να διαθέτει διασυνδέσεις που δεν είναι trunk (ονομάζονται access interfaces) που έχουν εκχωρηθεί στο VLAN. Τα βήματα διαμόρφωσης για τις διεπαφές πρόσβασης είναι τα εξής:

Βήμα 1. Για να ρυθμίσετε τις παραμέτρους ενός νέου VLAN, ακολουθήστε τα παρακάτω βήματα:

A. Από τη λειτουργία διαμόρφωσης, χρησιμοποιήστε την εντολή **vlan vlan-id** στην κατάσταση global configuration για να δημιουργήσετε το VLAN και να μεταβείτε σε κατάσταση διαμόρφωσης VLAN.

B. (Προαιρετικά) Χρησιμοποιήστε την εντολή **name** στη λειτουργία διαμόρφωσης VLAN για να καταχωρίσετε ένα όνομα για το VLAN. Εάν δεν έχει ρυθμιστεί, το όνομα VLAN είναι VLANZZZZ, όπου ZZZZ είναι το τετραψήφιο δεκαδικό αναγνωριστικό VLAN.

Βήμα 2. Για κάθε διασύνδεση πρόσβασης, ακολουθήστε τα παρακάτω βήματα:

A. Χρησιμοποιήστε την εντολή **interface type number** (αριθμός τύπου διασύνδεσης) στην κατάσταση global configuration για να μεταβείτε στη λειτουργία διαμόρφωσης διασύνδεσης για κάθε επιθυμητή διασύνδεση.

B. Χρησιμοποιήστε την εντολή **switchport access vlan id-number** στη λειτουργία διαμόρφωσης διασύνδεσης για να καθορίσετε τον αριθμό VLAN που σχετίζεται με τη συγκεκριμένη διασύνδεση.

C. (Προαιρετικά) Χρησιμοποιήστε την εντολή **switchport mode access** στη λειτουργία διαμόρφωσης διασύνδεσης για να κάνετε αυτή τη θύρα να λειτουργεί πάντα σε λειτουργία πρόσβασης (δηλαδή να μην είναι trunk).

Για παράδειγμα, αν θέλετε να τοποθετήσετε τις θύρες του μεταγωγέα σε τρία VLAN-11, 12 και 13, προσθέτετε πρώτα τρεις εντολές vlan: **vlan 11, vlan 12 και vlan 13**. Στη συνέχεια, για κάθε διασύνδεση, προσθέστε μια εντολή **switchport access vlan 11** (ή 12 ή 13) για να αναθέσετε τη διασύνδεση αυτή στο κατάλληλο VLAN.

Ο όρος native VLAN αναφέρεται στην προεπιλεγμένη ρύθμιση στην εντολή **switchport access vlan vlan-id**, και αυτή η προεπιλογή είναι το VLAN ID 1. Με άλλα λόγια, από προεπιλογή, κάθε θύρα εκχωρείται στο VLAN πρόσβασης 1.

4.5.4 Διαμόρφωση trunk links

Η διαμόρφωση του trunking μεταξύ δύο μεταγωγέων Cisco μπορεί να είναι πολύ απλή, αν απλά ρυθμίσετε στατικά τη διακλάδωση. Θα μπορούσατε κυριολεκτικά να προσθέσετε μία υποεντολή διασύνδεσης για τη διασύνδεση του μεταγωγέα σε κάθε πλευρά της σύνδεσης (**switchport mode trunk**) και θα δημιουργούσατε ένα trunk VLAN που θα υποστήριζε όλα τα VLAN που είναι γνωστά σε κάθε μεταγωγέα.

Δεν θα γίνει αναφορά στο Dynamic Trunking Protocol(DTP) γιατί προτείνεται η απενεργοποίηση του για λόγους ασφαλείας, Αναφορικά μόνο, το DTP μπορεί να διαπραγματευτεί αν οι δύο συσκευές στη σύνδεση συμφωνούν να κάνουν trunk.

4.6 Υλοποίηση διεπαφών που συνδέονται με τηλέφωνα

Στον κόσμο της τηλεφωνίας IP, τα τηλέφωνα χρησιμοποιούν θύρες Ethernet για να συνδεθούν σε ένα δίκτυο Ethernet, ώστε να μπορούν να χρησιμοποιούν IP για να στέλνουν και να λαμβάνουν κίνηση φωνής που αποστέλλεται μέσω πακέτων IP. Για να λειτουργήσει αυτό, η θύρα Ethernet του μεταγωγέα ενεργεί ως θύρα πρόσβασης, αλλά ταυτόχρονα, η θύρα ενεργεί ως trunk με κάποιους τρόπους. Οι τοποθεσίες που χρησιμοποιούν τηλεφωνία IP, στις οποίες περιλαμβάνεται σχεδόν κάθε εταιρεία

σήμερα, έχουν πλέον δύο συσκευές από κάθε θύρα πρόσβασης. Επιπλέον, οι βέλτιστες πρακτικές της Cisco για το σχεδιασμό της IP τηλεφωνίας μας λένε να τοποθετούνται τα τηλέφωνα σε ένα VLAN και οι υπολογιστές σε ένα διαφορετικό VLAN. Για να συμβεί αυτό, η θύρα του μεταγωγέα λειτουργεί λίγο σαν access port (για την κίνηση του υπολογιστή) και σαν trunk port (για την κίνηση του τηλεφώνου). Η διαμόρφωση ορίζει δύο VLAN σε αυτή τη θύρα, ως εξής:

Data VLAN: Ίδια ιδέα και διαμόρφωση με το access VLAN, αλλά ορίζεται ως το VLAN σε αυτή τη σύνδεση για την προώθηση της κυκλοφορίας για τη συσκευή που είναι συνδεδεμένη στο τηλέφωνο στο γραφείο (συνήθως ο υπολογιστής του χρήστη).

Voice VLAN: Το VLAN που ορίζεται στη σύνδεση για την προώθηση της κυκλοφορίας του τηλεφώνου. Η κυκλοφορία σε αυτό το VLAN είναι συνήθως επισημασμένη με επικεφαλίδα 802.1Q.

4.6.1 Διαμόρφωση και επαλήθευση VLAN δεδομένων και φωνής

Η διαμόρφωση μιας θύρας μεταγωγέα για την υποστήριξη τηλεφώνων IP, αφού γνωρίζετε τα προγραμματισμένα αναγνωριστικά VLAN φωνής και δεδομένων, απαιτεί μόνο μερικές εύκολες εντολές. Η κατανόηση των εντολών **show** μόλις διαμορφωθεί, ωστόσο, μπορεί να αποτελέσει πρόκληση. Η θύρα ενεργεί όπως μια θύρα πρόσβασης με πολλούς τρόπους. Ωστόσο, με τις περισσότερες επιλογές διαμόρφωσης, τα πλαίσια φωνής ρέουν με επικεφαλίδα 802.1Q, έτσι ώστε η σύνδεση να υποστηρίζει πλαίσια και στα δύο VLANs της σύνδεσης. Αυτό όμως κάνει την έξοδο της εντολής show διαφορετική.

Η λίστα περιγράφει λεπτομερώς τα βήματα διαμόρφωσης για ευκολότερη ανασκόπηση και μελέτη:

Βήμα 1. Χρησιμοποιήστε την εντολή **vlan vlan-id** σε κατάσταση λειτουργίας global configuration για να δημιουργήσετε τα VLAN δεδομένων και φωνής, εάν δεν υπάρχουν ήδη στο μεταγωγέα.

Βήμα 2. Διαμορφώστε το VLAN δεδομένων όπως ένα VLAN πρόσβασης, ως συνήθως:

> **A.** Χρησιμοποιήστε την εντολή **interface type number** για να μεταβείτε σε κατάσταση διαμόρφωσης διασύνδεσης.
>
> **B.** Χρησιμοποιήστε την εντολή **switchport access vlan id-number** στη λειτουργία διαμόρφωσης διασύνδεσης για να ορίσετε το VLAN δεδομένων.
>
> **C.** Χρησιμοποιήστε την εντολή **switchport mode access** στη λειτουργία διαμόρφωσης διασύνδεσης για να κάνετε αυτή τη θύρα να λειτουργεί πάντα σε λειτουργία πρόσβασης (δηλαδή να μην κάνει trunk).

Βήμα 3. Χρησιμοποιήστε την εντολή **switchport voice vlan id-number** στη λειτουργία διαμόρφωσης διασύνδεσης για να ορίσετε το αναγνωριστικό VLAN φωνής.

4.7 Επίλογος

Κλείνοντας το κεφάλαιο έχουμε πραγματοποιήσει τις βασικές ρυθμίσεις για την πρόσβαση στους μεταγωγείς καθώς και για την μεταγωγή των δεδομένων και θα προχωρήσουμε στην ρύθμιση του δρομολογητή που είναι ένα next generation firewall

Κεφάλαιο 5ο: Next Generation Firewall

5.1 Εισαγωγή

Στη δικτύωση υπολογιστών, το firewall είναι λογισμικό ή υλικό που επιτρέπει το φιλτράρισμα της ανεπιθύμητης κίνησης και τον περιορισμό της πρόσβασης από έναν υπολογιστή σε έναν άλλο ή από ένα δίκτυο σε ένα άλλο. Διαδραματίζει ζωτικό ρόλο στην ασφάλεια μιας δικτυακής υποδομής. Ένα τείχος προστασίας μπορεί να είναι είτε host-based ή network-based. [12]

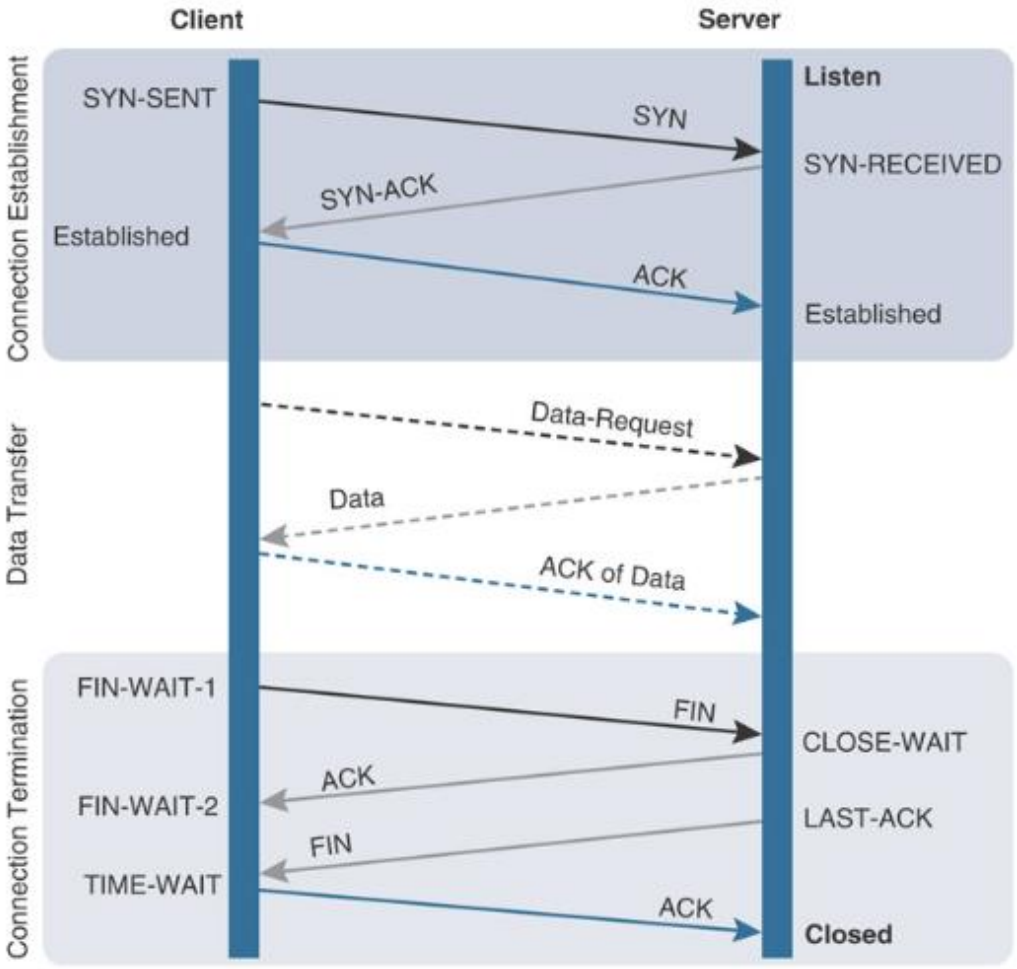
5.2 Network-based και host-based firewalls

Η πρώτη γενιά firewall μπορούσε να επιτρέπει ή να αποκλείει πακέτα μόνο με βάση τα στατικά στοιχεία ενός πακέτου, όπως source IP, destination IP, source port, destination port και πληροφορίες πρωτοκόλλου. Όταν ένα firewall εξέταζε ένα συγκεκριμένο πακέτο, δεν γνώριζε τα προηγούμενα πακέτα που είχαν περάσει από αυτό πριν, επειδή δεν γνώριζε τις καταστάσεις του πρωτοκόλλου ελέγχου μετάδοσης (TCP states). Λόγω της φύσης της λειτουργίας του, αυτό το firewall ονομάζεται stateless. Ένα stateless firewall δεν είναι σε θέση να διακρίνει την κατάσταση ενός συγκεκριμένου πακέτου. Για παράδειγμα, δεν μπορεί να προσδιορίσει αν ένα πακέτο αποτελεί μέρος ενός υπάρχων TCP connection ή αν προσπαθεί να δημιουργήσει ένα νέο connection ή αν το πακέτο είναι ένα manipulated, rogue πακέτο.

Ένα statefull firewall αναπτύχθηκε για να ξεπεράσει αυτούς τους περιορισμούς . Κατά τη διάρκεια του, κάθε TCP connection περνάει από μια σειρά καταστάσεων(states), οι οποίες μπορούν να χρησιμοποιηθούν από ένα statefull firewall για το φιλτράρισμα της κίνησης. Μπορεί να κρατήσει το state του tcp connection στη μνήμη του για ορισμένο χρονικό διάστημα, γεγονός που επιτρέπει στο firewall να παρακολουθεί τα στάδια μιας χειραψίας TCP και στη συνέχεια να αναλαμβάνει δράση με βάση την κατάσταση των τρεχόντων και των προηγούμενων πακέτων, αντί να βασίζεται απλώς σε έναν στατικό περιορισμό κανόνα ελέγχου πρόσβασης.

Για περισσότερες πληροφορίες σχετικά με το πρωτόκολλο TCP, προτείνεται η ανάγνωση του RFC 793. [13]

Παρακάτω μια εικόνα που αναφέρει περιληπτικά τα TCP states



Εικόνα 5.1 TCP States

Ωστόσο, ένα παραδοσιακό firewall - είτε stateless είτε stateful - έχει αποδειχθεί αναποτελεσματικό στην παρεμπόδιση κυβερνοεπιθέσεων τη σήμερον ημέρα. Χρειάζεται ένα τείχος προστασίας που μπορεί όχι μόνο να φιλτράρει την κυκλοφορία αλλά και να παρέχει ορατότητα και έλεγχο των εφαρμογών(application and visibility control), να εκτελεί deep packet inspection, να αποτρέπει τις απόπειρες εισβολής, να αποκρυπτογραφεί κρυπτογραφημένη κυκλοφορία, να ανιχνεύει ανωμαλίες στα πρωτόκολλα και να συσχετίζει συμβάντα ασφαλείας μεταξύ τους.
Πέρα από όλα αυτά θα πρέπει να μπορεί να επιτελέσει και κλασσικές λειτουργίες ενός layer 3 device όπως routing, QoS(Quality of service, υπηρεσίες όπως traffic shaping για παράδειγμα) και NAT(Network Address Translation).

Ένα **host-based firewall** εγκαθίσταται τοπικά σε έναν υπολογιστή. Στην περίπτωση αυτή, ο υπολογιστής του τελικού χρήστη αναλαμβάνει την τελική δράση - να επιτρέψει ή να αρνηθεί την κυκλοφορία. Καταναλώνει τους πόρους ενός τοπικού υπολογιστή για την εκτέλεση των υπηρεσιών firewalling, γεγονός που μπορεί να επηρεάσει τις άλλες εφαρμογές που εκτελούνται στον συγκεκριμένο υπολογιστή. Επιπλέον, σε ένα host-based firewall, η κίνηση διασχίζει όλα τα μέρη του δικτύου και μπορεί να καταναλώσει τους υποκείμενους πόρους του δικτύου έως ότου η κίνηση φτάσει στον στόχο της.

Ένα **network-based** firewall από την άλλη πλευρά, μπορεί να είναι εντελώς διαφανές για τον τελικό χρήστη. Συνήθως, τοποθετείται στην άκρη ή περιμετρικά του δικτύου, για να αποτρέψει την ανεπιθύμητη κίνηση πριν εισέλθει στο δίκτυο. Ο υπολογιστής του τελικού χρήστη παραμένει

ανυποψίαστος όσον αφορά τον έλεγχο της κίνησης από κάποια ενδιάμεση συσκευή. Σε μια εγκατάσταση που έχει network-based firewall, δεν χρειάζεται να εγκατασταθεί κανένα πρόσθετο λογισμικό και έτσι έχουμε και εξοικονόμηση πόρων.

Ιδανικά στα πλαίσια της ασφάλειας θα πρέπει να υπάρχουν και τα δύο, δηλαδή και ένα next-generation firewall που θα καλύπτει τις ανάγκες της εταιρείας όσον αφορά την περιμετρική ασφάλεια του δικτύου αλλα και ένα host-based firewall όπου θα κάνει έλεγχο και το ίδιον τον υπολογιστή του τελικού χρήστη για κακόβουλες ενέργειες. Στα επόμενα κεφάλαια θα γίνει ανάλυση της παραμετροποίησης και της λειτουργίας ενός network based firewall μιας μεσαίας επιχείρησης.

5.3 Υλοποίηση και διαχείριση Next-Generation Firewall της Cisco

Η υλοποίηση next generation firewall αποτελείται κυρίως από δύο στοιχεία: ένα manager και έναν sensor. Χρησιμοποιούμε έναν manager για την διαμόρφωση όλων των πολιτικών ασφαλείας και στη συνέχεια τις κάνουμε deploy σε έναν sensor. Ανάλογα με τις πολιτικές ασφαλείας, ένας sensor ενεργεί στην εισερχόμενη και εξερχόμενη κίνηση σε πραγματικό χρόνο και παράγει συμβάντα. Ένας manager λαμβάνει αυτά τα συμβάντα από τους sensors που διαχειρίζεται, τα συσχετίζει με διάφορα δεδομένα της υποδομής και τα εμφανίζει σε μια γραφική διεπαφή χρήστη (GUI) για εύκολη εξέταση

Για να καλύψει τις ανάγκες διαφορετικών τύπων επιχειρήσεων, η Cisco προσφέρει πολλαπλές λύσεις. Η διαχείριση μπορεί να γίνει τοπικά, απομακρυσμένα ή από το cloud. Οι τρέχουσες λύσεις διαχείρισης (managers) είναι οι εξής:

Secure Firewall Device Manager (FDM): Το FDM επιτρέπει την διαχείριση ενός firewall τοπικά χωρίς την καταχώρηση του σε οποιαδήποτε απομακρυσμένη πλατφόρμα διαχείρισης. Είναι ένα web based application που συνοδεύει εξ ορισμού το πακέτο λογισμικού που εγκαθίσταται. Μόλις γίνει η εγκατάσταση του λειτουργικού συστήματος ενεργοποιείται μέσω εντολών CLI και είναι διαθέσιμο μέσω ενός browser. Είναι η απλουστευμένη μορφή και από θέμα δυνατοτήτων αλλά και από θέμα παραμετροποιήσεων του FMC.

Secure Firewall Management Center (FMC): Το FMC επιτρέπει την διαχείριση πολλαπλών firewall από μια κεντρική τοποθεσία. Εάν πρέπει να γίνει τοποθέτηση πολλαπλών firewall σε διάφορες γεωγραφικές τοποθεσίες, χρησιμοποιείται ως ένα κέντρο διαχείρισης για την διαμόρφωση και την ανάπτυξη πολιτικών ασφαλείας σε όλα τα firewall. Επιτρέπει την παράλληλη διαχείριση πολλαπλών firewall και την ανάλυση των συμβάντων ασφαλείας τους ”from a single panel of glass”.Τα παραδείγματα και οι παραμετροποιήσεις που θα γίνουν παρακάτω θα βασιστούν στην χρήση του.

Cisco Defense Orchestrator (CDO): Το Cisco Defense Orchestrator είναι μια cloud πλατφόρμα διαχείρισης. Παρέχει την δυνατότητα ρύθμισης και διαχείρισης πολιτικών ταυτόχρονα για πολλαπλές πλατφόρμες ασφαλείας της Cisco. Επειδή η εφαρμογή CDO φιλοξενείται στο cloud της Cisco σε ένα μοντέλο Software as a Service (SaaS), η Cisco φροντίζει τακτικά για τις εργασίες συντήρησής της και διασφαλίζει τη διαθεσιμότητα της. Έτσι είναι πάντα ενημερωμένη και προσβάσιμη απο παντού.

Εικόνα 5.2 – Το login page του FMC

5.4 Αρχιτεκτονική λογισμικού και υλικού

Η Cisco ενσωμάτωσε τις τεχνολογίες ασφάλειας next generation της Sourcefire (εταιρεία που αγοράστηκε απο την Cisco) στις υπάρχουσες λύσεις τείχους προστασίας της Cisco, που ονομάζονται Adaptive Security Appliances (ASA). Σε αυτή την πρώιμη εφαρμογή, οι τεχνολογίες Sourcefire έτρεχαν ως ένα ξεχωριστό module στο ASA. Αργότερα, η Cisco σχεδίασε νέες πλατφόρμες για την εγγενή υποστήριξη των τεχνολογιών Sourcefire. Ονομάστηκαν Cisco Firepower, η οποία αργότερα μετονομάστηκε σε Cisco Secure Firewall. Σε αυτήν τη νέα υλοποίηση, η Cisco συγκεντρώνει τα χαρακτηριστικά ασφαλείας επόμενης γενιάς του Sourcefire, το Snort ανοικτού κώδικα και τις λειτουργίες τείχους προστασίας του ASA σε μία ενιαία εικόνα ενοποιημένου λογισμικού. Αυτό το ενοποιημένο λογισμικό ονομάζεται Firepower Threat Defense (FTD). Μετά την αλλαγή της ονομασίας, το λογισμικό αυτό είναι πλέον γνωστό ως Cisco Secure Firewall Threat Defense ή εν συντομία, threat defense. Έτσι πλέον έχουμε ένα ενοποιημένο λογισμικό το οποίο αποτελείται από τα παρακάτω

Core Software and Operating System (OS): Το βασικό μέρος του λογισμικού περιλαμβάνει το λειτουργικό σύστημα, το inspection engine ονόματι Snort για την ανίχνευση και την πρόληψη εισβολών, έναν διακομιστή ιστού για το γραφικό περιβάλλον εργασίας χρήστη, μια βάση δεδομένων για την αποθήκευση συμβάντων, firmware για τα hardware components κ.ο.κ.

Η Cisco δημοσιεύει τακτικά **maintenance releases** και **patches** για την παροχή διορθώσεων για τυχόν ελαττώματα του λογισμικού Secure Firewall και για την αντιμετώπιση τυχόν ευπαθειών ασφαλείας που ενδέχεται να βρεθούν σε μια δημόσια έκδοση.

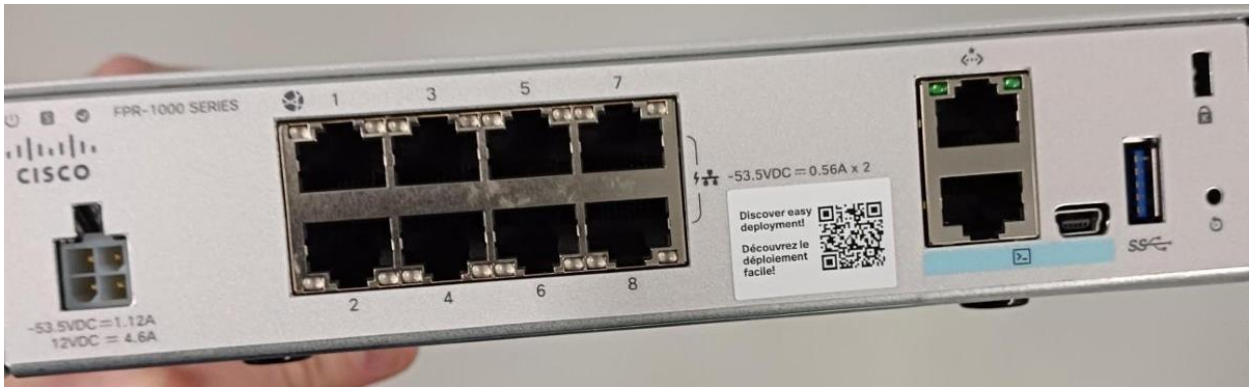
Rule Update: Η μηχανή ελέγχου (inspection engine) του Secure Firewall χρησιμοποιεί κανόνες εισβολής (intrusion rules), βασισμένους στο Snort, για να ανιχνεύει και να αποτρέπει προσπάθειες

εισβολής. Η ομάδα πληροφοριών απειλών της Cisco, γνωστή ως Talos, αναπτύσσει τους κανόνες εισβολής για να παρέχει κάλυψη στις πιο πρόσφατες απειλές και ευπάθειες ασφαλείας και πακετάρει το σύνολο κανόνων ξεχωριστά για διαφορετικές εκδόσεις του Snort. Το πακέτο ενημέρωσης κανόνων για το Snort 2 είναι γνωστό ως Cisco Secure Rule Update (SRU). Στο Snort 3, αυτό το πακέτο ενημέρωσης κανόνων ονομάζεται Lightweight Security Package (LSP). Σε ένα πρόσφατα εγκατεστημένο Secure Firewall με έκδοση λογισμικού 7.0 ή νεότερη, το Snort 3 είναι η προεπιλεγμένη μηχανή ελέγχου.

Vulnerability Database(VDB): Αυτή η βάση δεδομένων αποθηκεύει πληροφορίες για τις ευπάθειες και τα αποτυπώματα διαφόρων εφαρμογών, υπηρεσιών και λειτουργικών συστημάτων. Το Secure Firewall χρησιμοποιεί τις πληροφορίες αυτής της βάσης δεδομένων για την αναγνώριση ενός υπολογιστή δικτύου προσδιορίζοντας την εφαρμογή, την υπηρεσία ή το λειτουργικό σύστημα.

Geolocation Database (GeoDB): Αυτή η βάση δεδομένων αποθηκεύει τις γεωγραφικές πληροφορίες μιας διεύθυνσης IP. Για παράδειγμα, όταν ένα Secure Firewall εμφανίζει ένα συμβάν εισβολής στο GUI, η GeoDB σας επιτρέπει να δείτε το όνομα και τη σημαία της χώρας από την οποία προήλθε αυτή η απόπειρα εισβολής. Σας βοηθά να αναγνωρίζετε και να ενεργείτε στην κυκλοφορία με βάση τη γεωγραφική τοποθεσία.

Το FTD όπως αναφέρθηκε είναι το ενοποιημένο image, η εγκατάσταση του οποίου γίνεται σε κάποιο chassis-hardware.Υπάρχουν διαφορετικές επιλογές hardware ανάλογα τις απαιτήσεις κάθε επιχείρησης. Θα γίνει ανάλυση για την σειρά FPR 1000 η οποία συνίσταται για επιχειρήσεις μικρού και μεσαίου μεγέθους



Εικόνα 5.3 Ένα FPR1010

5.5 Καταχώρηση Συσκευής(Device Registration)

Για να ολοκληρωθεί η εγγραφή ενός FTD στο FMC, θα πρέπει να έχετε πρόσβαση στο CLI του FTD και στο GUI του κέντρου διαχείρισης. Κάποια βασικά στοιχεία τα οποία προτείνονται είναι τα εξής:

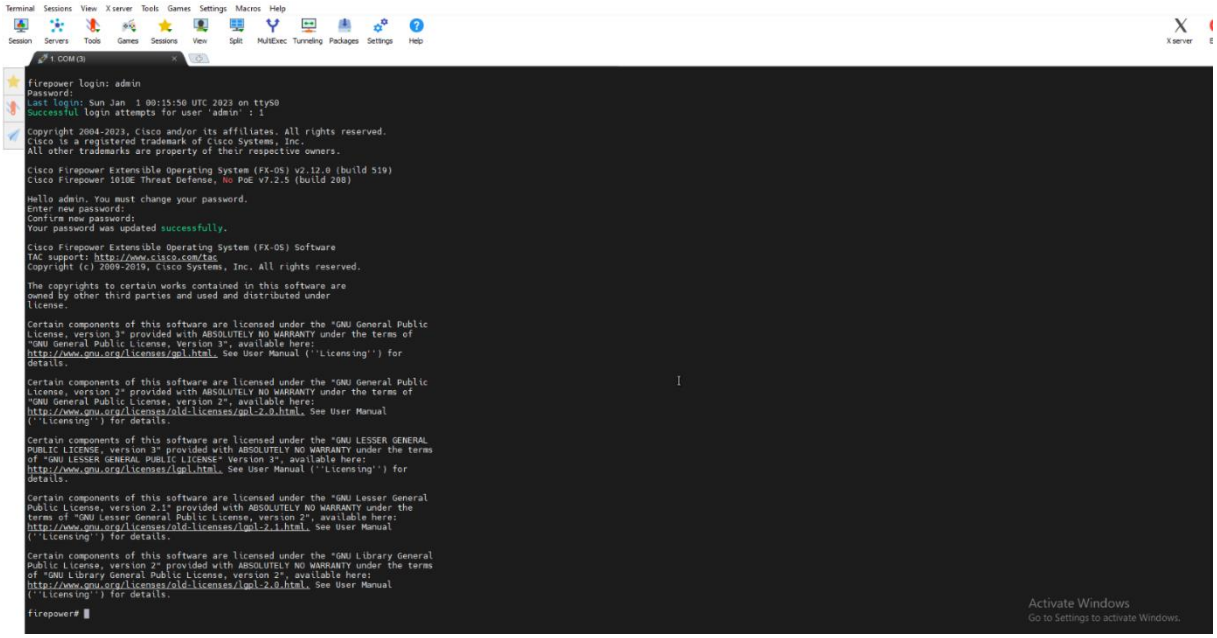
1. Πρέπει να ξεκινήσετε τη διαδικασία εγγραφής από το FTD. Αρχικά, καταχωρείτε τις πληροφορίες του κέντρου διαχείρισης στο CLI του FTD και στη συνέχεια παρέχετε τις λεπτομέρειες του, στο GUI του κέντρου διαχείρισης.

2. Αντί να χρησιμοποιείτε το hostname ή το FQDN, χρησιμοποιήστε απευθείας τη διεύθυνση IP. Αυτό διασφαλίζει ότι μια αποτυχία της διαδικασίας εγγραφής δεν οφείλεται σε αποτυχία DNS.

3. Εάν υπάρχει μία ενδιάμεση συσκευή ανάμεσα στο firewall και στο FMC η οποία κάνει NAT, χρησιμοποιήστε ένα μοναδικό αναγνωριστικό NAT κατά τη διαδικασία εγγραφής τους.

5.5.1 Παραμετροποιήσεις στο FTD μέσω CLI

Αφού ολοκληρωθεί η αρχικοποίηση του συστήματος καταλήγουμε στο Firepower eXtensible Operating System. Το FXOS είναι το υποκείμενο λειτουργικό σύστημα στις πλατφόρμες Firepower ή Secure Firewall. Χρησιμοποιείται κυρίως για advanced troubleshooting και δεν θα μας απασχολήσει ιδιαίτερα.



Εικόνα 5.4 After bootup screen του FTD

Για την παραμετροποίηση του FTD θα πρέπει από το FXOS να δώσουμε την εντολή **connect ftd**

Εικόνα 5.5 Wizard ρύθμισης management interface του FTD

Έπειτα θα τρέξει ένας wizard με τον οποίο μπορούμε να ρυθμίσουμε το management interface του firewall για να εξασφαλίσουμε την επικοινωνία του με το FMC. Οι ρυθμίσεις που μας απασχολούν άμεσα είναι η IP address και το default gateway, έχει επιλεχθεί η ανάθεση μέσω DHCP έτσι ώστε όταν το firewall συνδεθεί με το CPE(Customer Premises Equipment-Routerακι παρόχου)να πάρει μια IP

address απο το dhcp pool που έχει το ρουτεράκι του παρόχου και να αποκτήσει σύνδεση στο Internet, επίσης στο τέλος του wizard μας δίνεται και η επιλογή για routed ή transparent mode.

5.5.2 Χρήση firewall σε router ή σε transparent mode

Μπορείτε να χρησιμοποιήσετε το firewall ως default gateway για το δίκτυό σας, ώστε οι τελικοί χρήστες να μπορούν να το χρησιμοποιούν για να επικοινωνούν με ένα διαφορετικό υποδίκτυο ή για να συνδέονται στο Διαδίκτυο. Μπορείτε επίσης να το χρησιμοποιήσετε σε transparent mode, ώστε να παραμένει αόρατο στους κεντρικούς υπολογιστές του δικτύου σας και να επιτελεί απλή παρακολούθηση της κίνησης(monitoring).

Στη λειτουργία δρομολόγησης(routed mode), ένα firewall ενεργεί σαν ένα hop επιπέδου 3. Κάθε interface στο firewall μπορεί να είναι συνδεδεμένο σε διαφορετικό υποδίκτυο και να ενεργεί ως προεπιλεγμένη πύλη(default gateway) για αυτό το υποδίκτυο. Το firewall μπορεί επίσης να δρομολογήσει την κυκλοφορία μεταξύ διαφορετικών υποδικτύων, όπως ένας δρομολογητής επιπέδου 3.

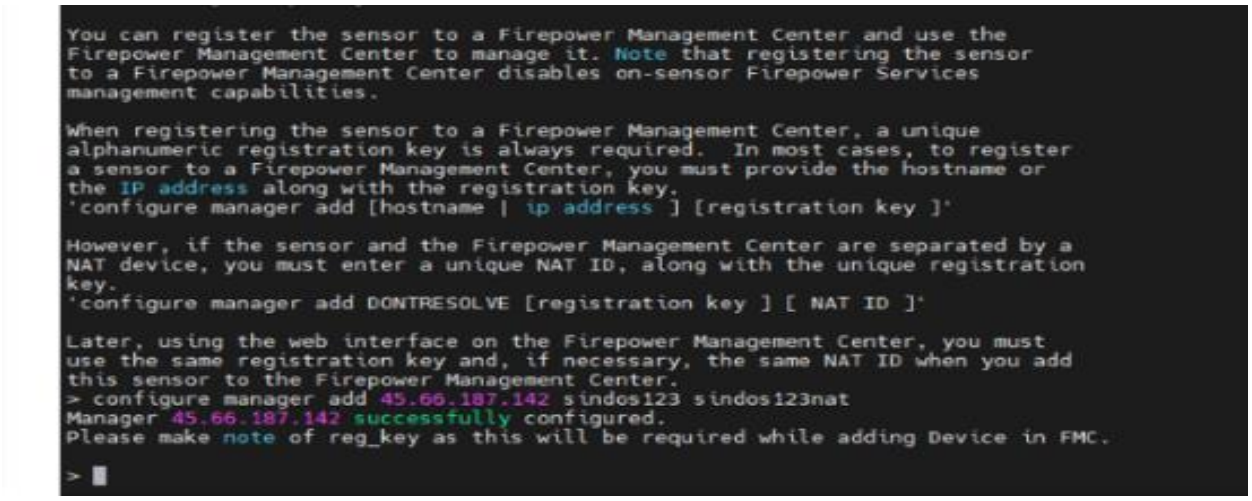
Σε διαφανή λειτουργία(transparent mode), το firewall γεφυρώνει τα εσωτερικά και εξωτερικά interface σε ένα ενιαίο δίκτυο επιπέδου 2 και παραμένει διαφανές στους κεντρικούς υπολογιστές. Το FMC δεν σας επιτρέπει να εκχωρήσετε μια διεύθυνση IPv4 στα interfaces. Ως αποτέλεσμα, οι υπολογιστές δεν μπορούν να επικοινωνήσουν με τα interfaces του firewall και προφανώς δεν μπορούμε να τα χρησιμοποιήσουμε και ως default gateway για τα εσωτερικά υποδίκτυα.

Η επιλογή του mode του firewall γίνεται μέσω CLI και χρησιμοποιώντας την εντολή **configure firewall routed/transparent.** Κάθε φορά που αλλάζουμε mode, οι υπάρχουσες ρυθμίσεις χάνονται και το firewall θέλει εκ νέου ρύθμιση. Για τις ανάγκες αυτής της υλοποίησης θα επιλέξουμε το routed mode μιας και θέλουμε το firewall να είναι και δρομολογητής του εσωτερικού δικτύου

Αφού ολοκληρωθεί η αρχικοποίηση του συστήματος και η ρύθμιση του management interface, θα εμφανιστεί η προεπιλεγμένη προτροπή CLI: >.

Για να προστεθεί το FMC, εκτελέστε την εντολή **configure manager add** μαζί με τη διεύθυνση IP διαχείρισης του κέντρου διαχείρισης. Πρέπει επίσης να δώσετε ένα κλειδί εγγραφής μιας χρήσης, το οποίο χρησιμοποιείται μόνο κατά τη διαδικασία εγγραφής. Ένα μοναδικό αναγνωριστικό NAT είναι απαραίτητο εάν υπάρχει μια ενδιάμεση συσκευή δικτύωσης η οποία κάνει NAT(όπως ένα ρουτεράκι παρόχου που αναφέρθηκε πιο πάνω). Η σύνταξη της εντολής έχει ως εξής:

configure manager add IP_Address_of_management_center Registration_Key NAT_ID

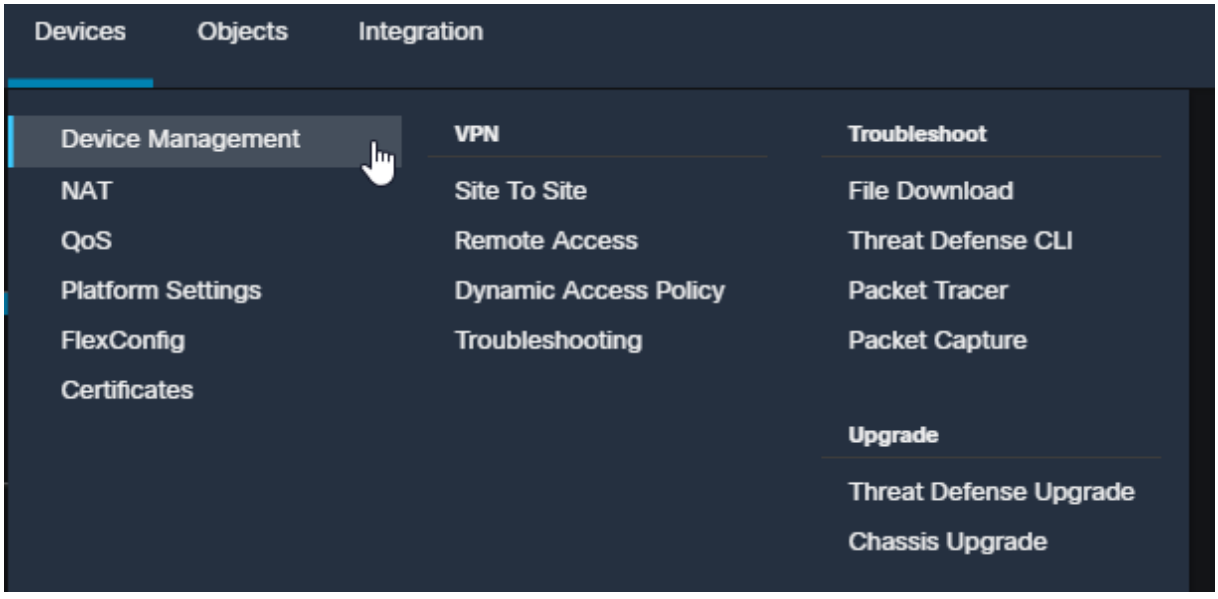


Εικόνα 5.6 Output από το CLI του FTD με την εντολή εγγραφής

5.6 Παραμετροποιήσεις FMC μέσω GUI

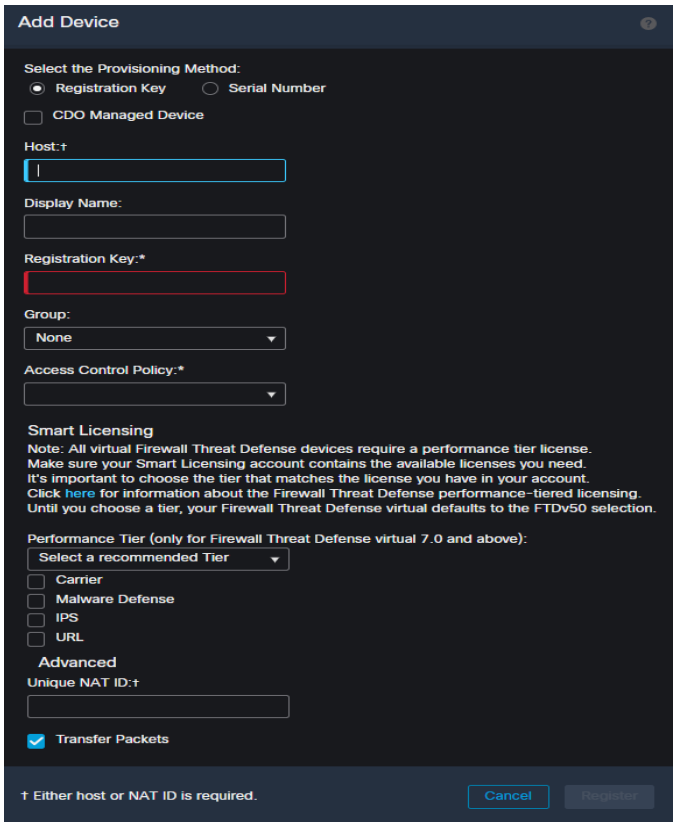
Το επόμενο βήμα της διαδικασίας εγγραφής είναι η εισαγωγή των λεπτομερειών του FTD στο GUI του FMC. Όταν παρέχετε τα στοιχεία, πρέπει να χρησιμοποιήσετε το ίδιο κλειδί εγγραφής (και το ίδιο αναγνωριστικό NAT, εάν χρησιμοποιείται) που διαμορφώσατε προηγουμένως στο FTD. Ακολουθούν τα βήματα που πρέπει να ακολουθήσετε:

1. Συνδεθείτε στο FMC. Επιλέξτε Devices > Devices Management. Εμφανίζεται η σελίδα διαχείρισης των συσκευών.



Εικόνα 5.7 Οι επιλογές του tab Devices στο GUI του FMC

2. Add Device (Προσθήκη συσκευής). Εδώ, εισάγετε τα στοιχεία του FTD.



Εικόνα 5.8 Το παράθυρο προσθήκης συσκευής του FMC

3. Στο πεδίο Host, εισαγάγετε τη διεύθυνση IP του management interface του firewall

4. Στο πεδίο Device Name, δώστε ένα όνομα που θα εμφανίζεται στο GUI του FMC για να αντιπροσωπεύει αυτό το firewall

5. Στο πεδίο Registration Key, εισαγάγετε το ίδιο κλειδί εγγραφής που χρησιμοποιήσατε νωρίτερα στο CLI του FTD.

6. Επιλέξτε μια πολιτική ελέγχου πρόσβασης που θέλετε να εφαρμόσετε αρχικά στο FTD. Εάν πρόκειται για νέα εγκατάσταση, το FMC ενδέχεται να μην έχει προρυθμίσει μια πολιτική ελέγχου πρόσβασης. Μπορείτε, ωστόσο, να δημιουργήσετε μια πολιτική εν κινήσει επιλέγοντας Δημιουργία νέας πολιτικής από το αναπτυσσόμενο μενού.

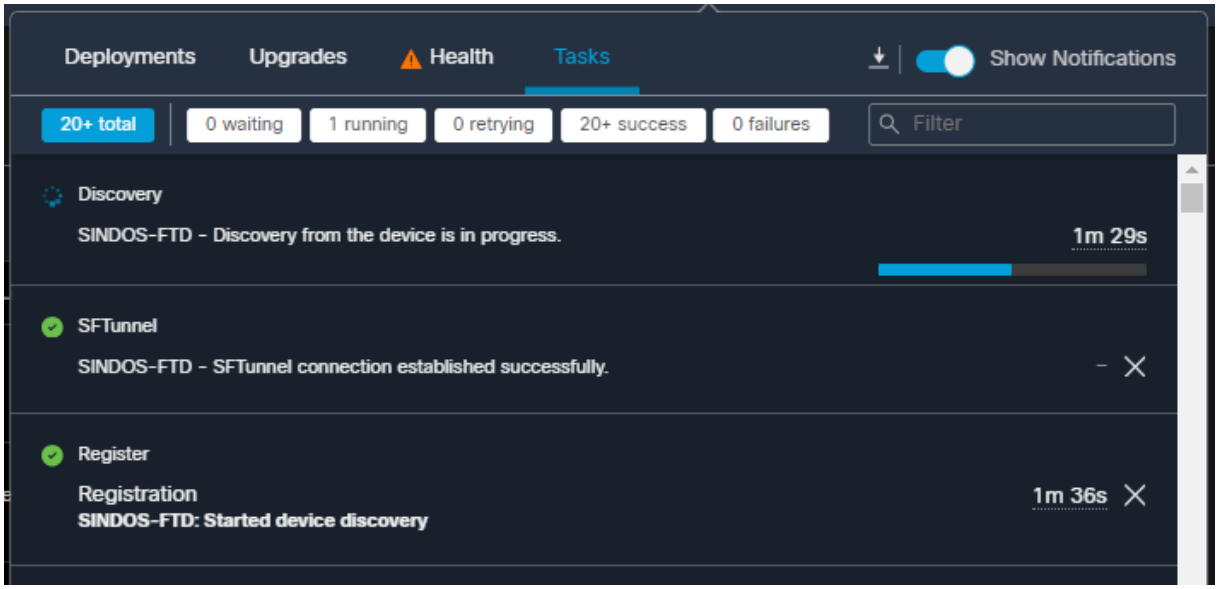
7. Στην ενότητα Smart Licensing, το performance tier δεν θα μας απασχολήσει μιας και δεν έχουμε vFTD (δηλαδή το firewall ως εικονική μηχανή). Για την χρήση όλων των δυνατοτήτων του firewall όπως Malware, Threat, URL Filtering κ.ο.κ. απαιτούνται κάποια license τα οποία τα προσθέτουμε σε αυτό το σημείο.

8. Στην ενότητα Advanced (Για προχωρημένους), δώστε ένα μοναδικό αναγνωριστικό NAT, εάν υπάρχει μια ενδιάμεση συσκευή μεταξύ του FMC και του FTD που κάνει NAT.

9. Η επιλογή Transfer Packets (Μεταφορά πακέτων) επιτρέπει ένα FTD να στέλνει τα σχετικά πακέτα στο κέντρο διαχείρισης όταν δημιουργούνται συμβάντα ασφαλείας. Αυτή η επιλογή είναι ενεργοποιημένη, από προεπιλογή.

10. Κάντε κλικ στο κουμπί Register (Εγγραφή) για να ξεκινήσει η διαδικασία εγγραφής. Όλες οι επικοινωνίες μεταξύ του κέντρου διαχείρισης και της άμυνας απειλής πραγματοποιούνται μέσω ενός κρυπτογραφημένου tunnel, γνωστου και ως sftunnel.

Κατά τη διάρκεια της διαδικασίας εγγραφής, το σύστημα περνάει από μια φάση εντοπισμού της συσκευής. Όταν ολοκληρωθεί, το σύστημα εφαρμόζει αυτόματα τις πολιτικές ασφαλείας.



Εικόνα 5.9 Διαδικασία εγγραφής συσκευής στο FMC

Εάν η διαδικασία εγγραφής είναι επιτυχής, υπάρχει ένα health status το οποίο εμφανίζεται ως υγιές στη σελίδα διαχείρισης της συσκευής. Εναλλακτικά μπορούμε και μέσω CLI να δώσουμε την εντολή show managers για να το επιβεβαιώσουμε.

5.7 Διαμόρφωση των routed interfaces

Στο firewall, μπορείτε να διαμορφώσετε ένα interface με στατική διεύθυνση IP. Επίσης μπορεί να λειτουργήσει ως DHCP client και να λάβει μια διεύθυνση IP από έναν διακομιστή DHCP. Επιπλέον, μπορεί και το ίδιο το firewall να λειτουργήσει ως DHCP server για τους υπολογιστές στα διάφορα υποδίκτυα.

Στην υποδομή μας έχουμε το δίκτυο 10.148.0.0/16 το οποίο έχει χωριστεί σε διάφορα υποδίκτυα για να καλύψεις τις ανάγκες συνδεσιμότητας της επιχείρησης.

Αυτά είναι τα παρακάτω.

Όνομα	Vlan	Υποδίκτυο
SINDOS-MGMNT	1	10.148.1.0/24
SINDOS-USERS	2	10.148.2.0/24
SINDOS-SCANNERS	3	10.148.3.0/24
SINDOS-CCTV	4	10.148.4.0/24
SINDOS-WIFI-USERS	5	10.148.5.0/24
SINDOS-GUESTS	60	10.148.60.0/24
SINDOS-VOIP	100	10.148.100.0/24

5.7.1 Διαμόρφωση των interfaces με στατικές διευθύνσεις IP.

Για την διαμόρφωση του interface με στατική διεύθυνση IP, ακολουθήστε τα παρακάτω βήματα:

1. Πλοηγηθείτε στην επιλογή Συσκευές > Διαχείριση συσκευών. Εμφανίζεται μια λίστα με τις διαχειριζόμενες συσκευές.

2. Κάντε κλικ στο εικονίδιο με το μολύβι που βρίσκεται δίπλα στο όνομα του firewall που θέλετε να διαμορφώσετε. Εμφανίζεται η σελίδα επεξεργασίας , στην οποία εμφανίζονται όλα τα interfaces

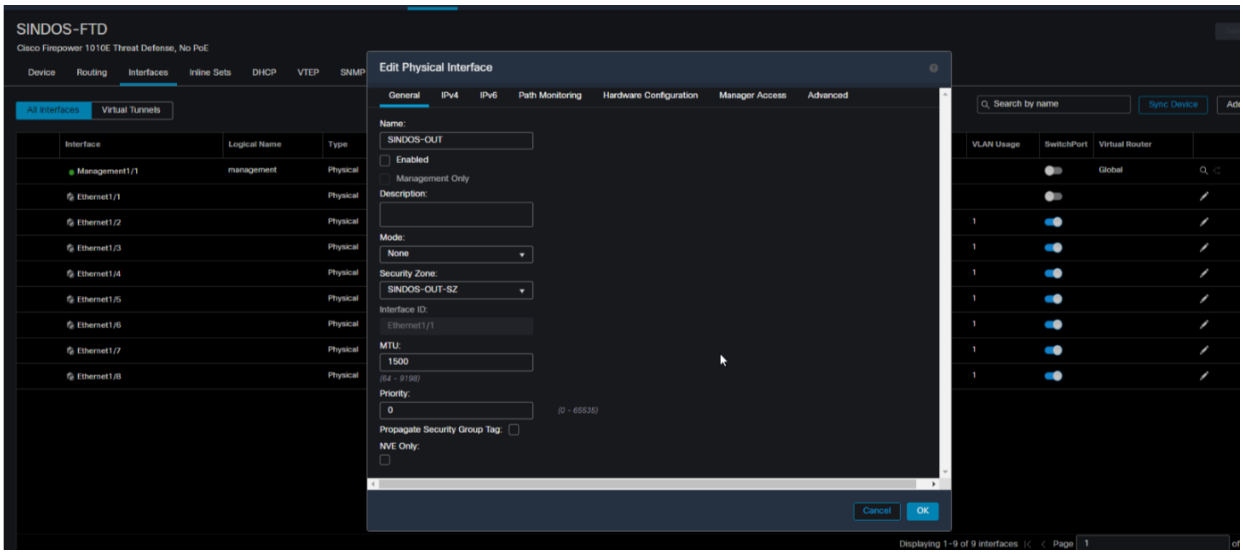
3. Στην καρτέλα Interfaces , κάντε κλικ στα εικονίδια μολυβιού δίπλα στα Ethernet1/1 και Ethernet1/2 για να ρυθμίσετε τις παραμέτρους αυτών των διασυνδέσεων για το εξωτερικό και το εσωτερικό δίκτυο, αντίστοιχα.

Στην περίπτωση που εξετάζουμε:

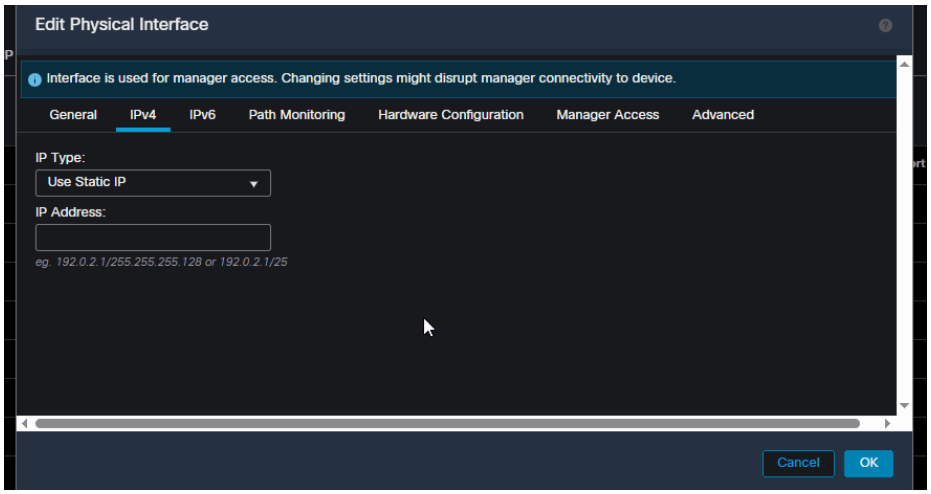
Το interface Ethernet 1/1 θα πρέπει να συνδεθεί με ένα καλώδιο ethernet στο CPE (customer premises equipment δηλαδή το ρουτεράκι παρόχου Ιντερνετ). Στο interface αυτό θα αναθέσουμε μια public IP απο ένα /30 υποδίκτυο που μας έχει δώσει ο πάροχος και για να εξασφαλίσουμε την πρόσβαση στο Ιντερνετ, next hop θα είναι το ρουτεράκι του παρόχου μέσω της ρύθμισης ενός στατικού route. Αυτό αποτελεί το εξωτερικό μας δίκτυο.

Το interface Ethernet1/2 θα συνδεθεί με ένα switch της τοπικής υποδομής, στο interface αυτό θα δημιουργηθούν τα κατάλληλα sub-interfaces βάση των υποδικτύων της υποδομής και αυτά θα αποτελέσουν το default gateway για τα υποδίκτυα της υποδομής Αυτό αποτελεί το εσωτερικό μας δίκτυο.

Για να ενεργοποιήσετε ένα interface, πρέπει να του δώσετε ένα όνομα. Ωστόσο, η διαμόρφωση μιας ζώνης ασφαλείας είναι ένα προαιρετικό βήμα. Εδώ, στο παράθυρο Edit Physical Interface μπορείτε να δημιουργήσετε μια ζώνη ασφαλείας (**Security Zone).** Μια ζώνη ασφαλείας είναι μια ομαδοποίηση διασυνδέσεων. Οι ζώνες χωρίζουν το δίκτυο σε τμήματα για να σας βοηθήσουν στη διαχείριση και ταξινόμηση της κίνησης)και να τη συσχετίσετε με ένα interface εν κινήσει. Στο μέλλον, θα μπορούσατε να χρησιμοποιήσετε τη σελίδα Objects -> Object Management -> Interfaces για τη διαχείριση των ζωνών ασφαλείας.



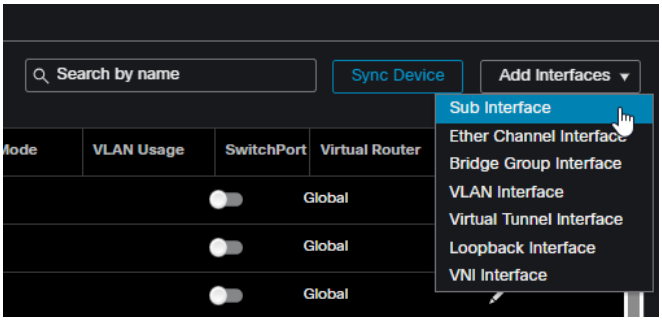
Εικόνα 5.10 Ρύθμιση του interface Ethernet1/1, η ανάθεση IP γίνεται στην καρτέλα IPv4



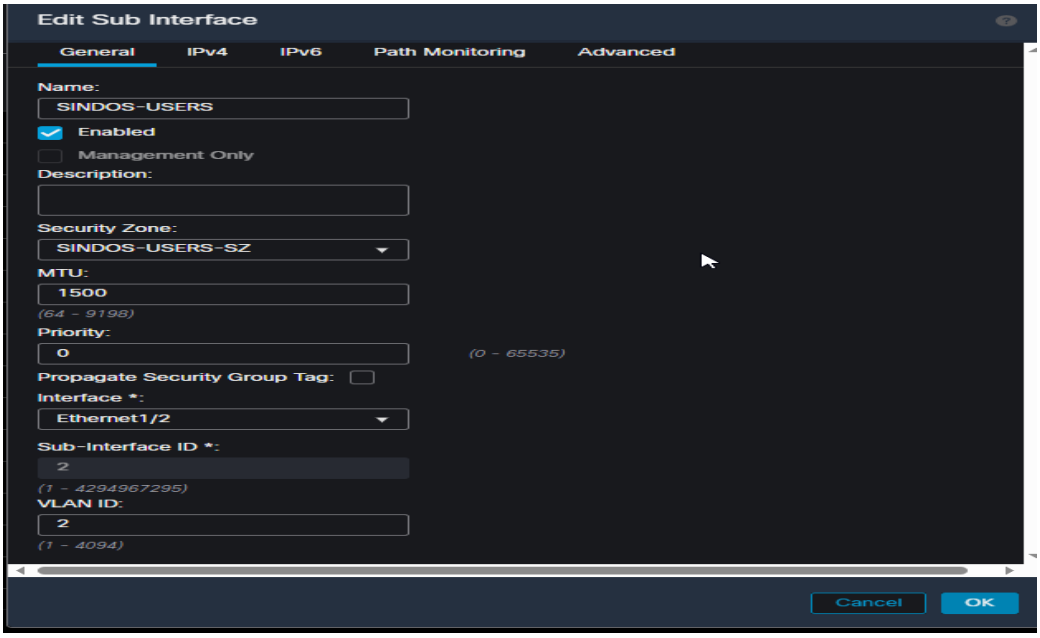
Εικόνα 5.11 Η καρτέλα IPv4 για την ρύθμιση IPv4 διεύθυνσης στο interface

Αντίστοιχα θα γίνει και η ρύθμιση του Ethernet1/2,με την διαφορά ότι σε αυτό το interface θα προσθέσουμε subinterfaces μέσω του μενού Add Interfaces->Sub Interface.

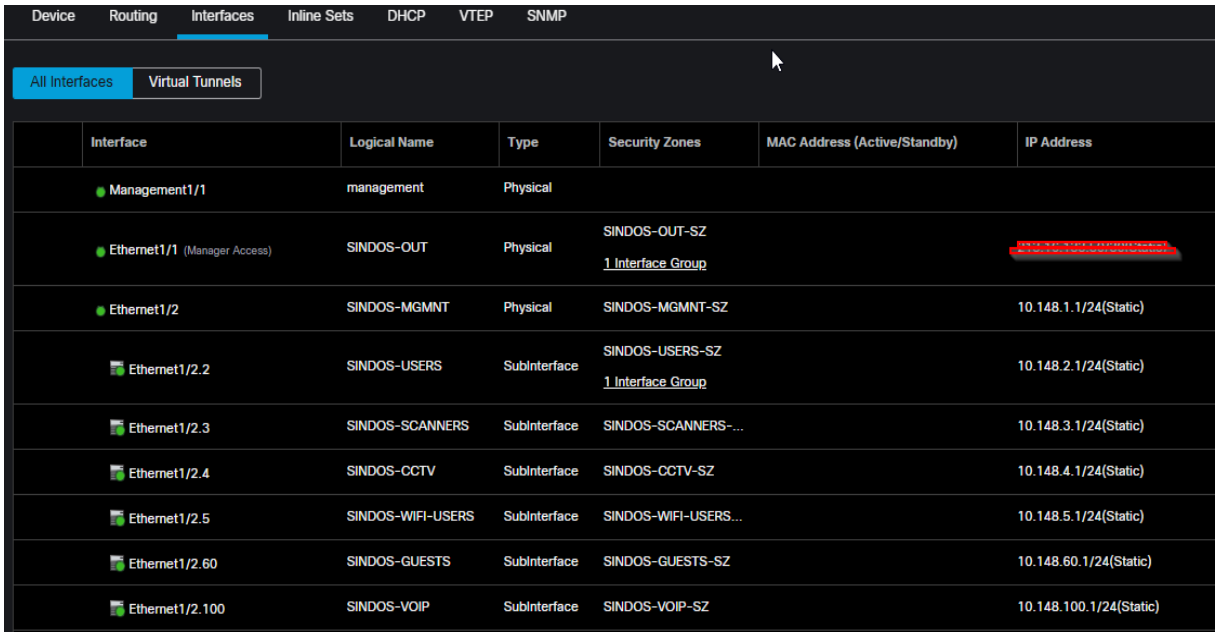
Αυτά τα subinterfaces θα είναι tagged στο κατάλληλο vlan και θα πάρουν μια IP διεύθυνση στο αντίστοιχο υποδίκτυο για να λειτουργήσουν ως default gateway στο εκάστοτε υποδίκτυο



Εικόνα 5.12 Εισαγωγή sub interface στο device

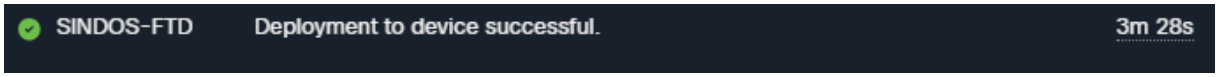


Εικόνα 5.13 Ενδεικτική ρύθμιση του sub interface για τους SINDOS-USERS



Εικόνα 5.14 Συγκεντρωτική εικόνα με όλα τα interfaces και τα sub interfaces

4. Αποθήκευση των αλλαγών και deployment στο firewall



Εικόνα 5.15- Επιτυχές deployment πολιτικής στο firewall

5.8 DHCP Server

Ενα firewall μπορεί να ενεργεί ως διακομιστής DHCP και να παρέχει δυναμικά διευθύνσεις IPv4 στους υπολογιστές που επιθεωρεί.Τα παρακάτω βήματα περιγράφουν τον τρόπο διαμόρφωσης του firewall με υπηρεσίες DHCP

1. Μεταβείτε στην ενότητα Devices > Device Management και κάντε κλικ στο εικονίδιο μολυβιού για να επεξεργαστείτε τη διαμόρφωση

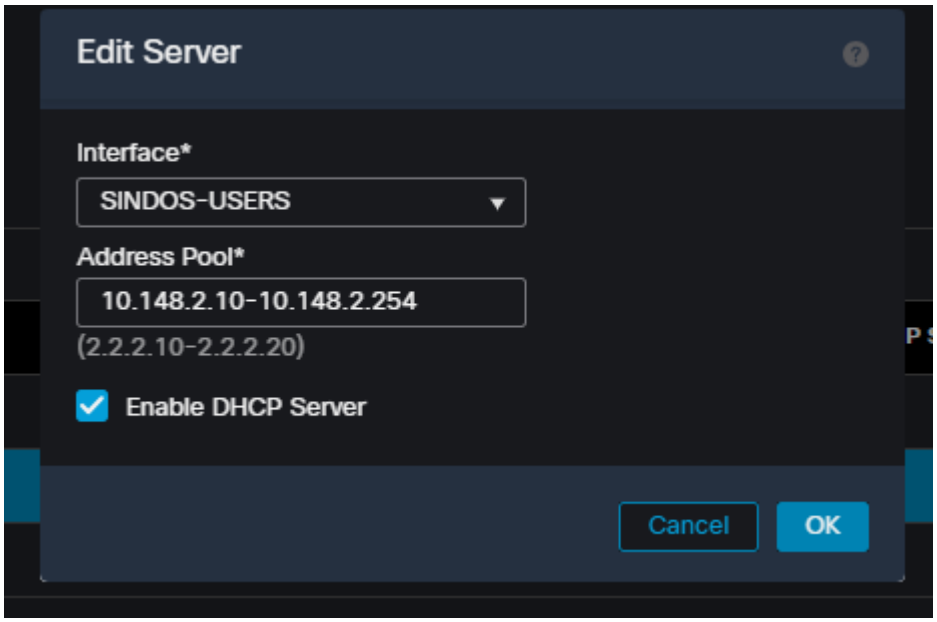
2. Εκχωρήστε μια στατική διεύθυνση IP στο interface(έστω την 10.148.2.1/24), οι τελικοί σας χρήστες (DHCP clients) θα χρησιμοποιούν αυτή τη διεύθυνση IP ως προεπιλεγμένη πύλη.

3. Μεταβείτε στην καρτέλα DHCP. Από προεπιλογή, εμφανίζεται η σελίδα DHCP Server (Διακομιστής DHCP).

4. Εδώ θα ρυθμίσουμε και DNS Servers που θα ισχύουν για όλα τα DHCP Pools. Κάντε κλικ στην επιλογή Server και μετά στο κουμπί Add. Εμφανίζεται το παράθυρο Add Server

5. Στο παράθυρο Add Server, επιλέξτε το interface από την αναπτυσσόμενη λίστα, επειδή αυτό θα προσφέρει διευθύνσεις IP στο εσωτερικό δίκτυο.

6. Δημιουργήστε ένα DHCP pool για τον διακομιστή DHCP. Θυμηθείτε ότι οι διευθύνσεις θα πρέπει να βρίσκονται στο ίδιο υποδίκτυο με το interface. Για παράδειγμα, αν αναθέσετε 10.148.2.1/24 στην εσωτερική διασύνδεση, το DHCP pool θα πρέπει να βρίσκεται μεταξύ 10.148.2.2 και 10.148.2.254.



Εικόνα 5.16 Ρύθμιση DHCP server για το δίκτυο SINDOS-USERS

5.9 Access Control Policy-Πολιτική ελέγχου Πρόσβασης

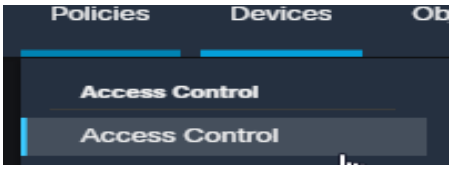
Μια πολιτική ελέγχου πρόσβασης σας επιτρέπει να δημιουργείτε κανόνες ελέγχου πρόσβασης για την αντιστοίχιση της κίνησης-traffic και να εφαρμόζετε μια ενέργεια στην αντίστοιχη κίνηση σύμφωνα με τις επιχειρηματικές απαιτήσεις. Χρησιμοποιείτε κανόνες ελέγχου πρόσβασης για να συσχετίσετε πολιτικές ασφαλείας, όπως πολιτικές αρχείων και πολιτικές εισβολής, με την αντίστοιχη κίνηση. Μια πολιτική ελέγχου πρόσβασης είναι το κεντρικό σημείο για την επίκληση όλων των πολιτικών ασφαλείας που δημιουργείτε στο Firewall. Πριν εμβαθύνουμε στις διάφορες πολιτικές ασφάλειας , ας δούμε τα διάφορα συστατικά στοιχεία μιας πολιτικής ελέγχου πρόσβασης και τον τρόπο διαμόρφωσης μιας τέτοιας πολιτικής.

5.9.1 Βασικά στοιχεία πολιτικής ελέγχου πρόσβασης

Για να δημιουργήσετε μια απλή πολιτική ελέγχου πρόσβασης, βασικά εργάζεστε σε δύο τύπους επεξεργαστών: τον επεξεργαστή πολιτικής ελέγχου πρόσβασης(access control policy editor) και τον επεξεργαστή κανόνων ελέγχου πρόσβασης(access control rule editor). Οι άλλες πολιτικές ασφαλείας, όπως οι πολιτικές εισβολής(intrusion policy) και οι πολιτικές αρχείων(file policy), έχουν τους δικούς τους συντάκτες πολιτικής. Αφού ρυθμίσετε τις παραμέτρους των άλλων πολιτικών χρησιμοποιώντας τους αντίστοιχους συντάκτες πολιτικών, πρέπει να τις επικαλεστείτε σε μια πολιτική ελέγχου πρόσβασης που θα γίνει deploy στο firewall. Οι ακόλουθες ενότητες παρουσιάζουν εν συντομία και τους δύο συντάκτες.

5.9.2 Access control policy editor- Συντάκτης πολιτικής

Για να πλοηγηθείτε στη σελίδα επεξεργασίας πολιτικής ελέγχου πρόσβασης, μεταβείτε στην επιλογή Policies > Access Control στο κέντρο διαχείρισης. Όταν εμφανιστεί η λίστα με τις υπάρχουσες πολιτικές ελέγχου πρόσβασης, κάντε κλικ στο εικονίδιο με το μολύβι δίπλα από το όνομα μιας πολιτικής για να την ανοίξετε στον συντάκτη πολιτικής. Εάν δεν έχει δημιουργηθεί ακόμη πολιτική ελέγχου πρόσβασης, μπορείτε να δημιουργήσετε μια νέα πολιτική ανά πάσα στιγμή κάνοντας κλικ στο κουμπί New Policy.



Εικόνα 5.17 Η καρτέλα access control στο FMC

Όταν ανοίγετε μια πολιτική ελέγχου πρόσβασης σε έναν συντάκτη πολιτικής, θα βρείτε πολλές επιλογές για τη βελτίωση της πολιτικής ασφαλείας. Ακολουθεί μια περίληψη ορισμένων από τις επιλογές:

Εικόνα 5.18 Τα διάφορα tabs επιλογών ενός ACP

Policy Assignment: Για να επιλέξετε το firewall στο οποίο θα γίνει deploy η πολιτική. Ενώ μπορείτε να δημιουργήσετε και να αποθηκεύσετε πολλές πολιτικές ελέγχου πρόσβασης στο κέντρο διαχείρισης, μπορείτε να κάνετε deploy μόνο μία πολιτική ελέγχου πρόσβασης στο firewall ανά πάσα στιγμή.

Rules: Για να προβάλετε τους κανόνες ελέγχου πρόσβασης με τις συνθήκες τους. Η κίνηση αξιολογείται σε σχέση με τους κανόνες ελέγχου πρόσβασης με σειρά από πάνω προς τα κάτω.

Security Intelligence: Για να αποκλείσετε συνδέσεις με βάση τη φήμη(reputation), το Talos είναι ένα σύστημα της Cisco όπου μεταξύ άλλων κατηγοριοποιεί τις ιστοσελίδες ανάλογα με το πόσο ασφαλής είναι πάνω σε μια κλίμακα reputation, με τις πιο ασφαλής να είναι υψηλά σε αυτήν την κλίμακα

HTTP Response: Για την εμφάνιση μιας σελίδας απάντησης όταν μια άμυνα απειλής ανιχνεύει μια προσπάθεια πρόσβασης σε έναν ιστότοπο.

Logging: Για να ορίσετε προορισμούς για τα μηνύματα syslog που θα παράγονται από όλα τα στοιχεία της πολιτικής ελέγχου πρόσβασης.

Για προχωρημένους: Για να ρυθμίσετε τις επιλογές για προχωρημένους που μπορούν να επηρεάσουν την απόδοση μιας άμυνας απειλής. Στις περισσότερες περιπτώσεις, οι προεπιλεγμένες ρυθμίσεις δεν απαιτούν αλλαγές.

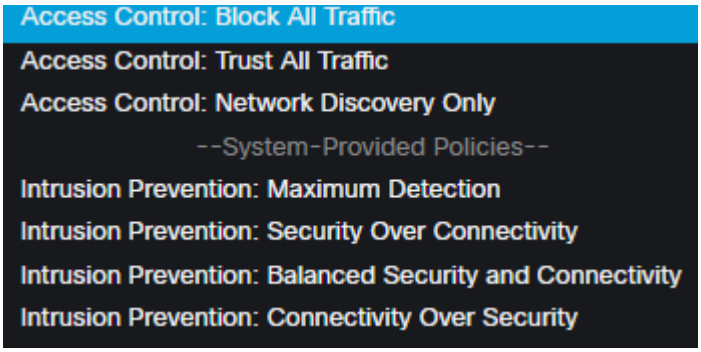
Προεπιλεγμένη ενέργεια: Για να καθορίσετε τον τρόπο με τον οποίο η κυκλοφορία που δεν ταιριάζει με καμία από τις υπάρχουσες συνθήκες κανόνα ελέγχου πρόσβασης χειρίζεται από το firewall. Μπορείτε να επιλέξετε να εφαρμόσετε μία από τις ακόλουθες ενέργειες στην υπόλοιπη κυκλοφορία που δεν ταιριάζει:

>Αποκλεισμός της κίνησης που δεν υπάγεται σε κάποιον συγκεκριμένο κανόνα.

>Να επιτρέπεται η κίνηση που δεν υπάγεται σε κάποιον συγκεκριμένο κανόνα.

>Ανακάλυψη των στοιχείων του κεντρικού υπολογιστή, του χρήστη και της εφαρμογής που δημιουργούν την κίνηση

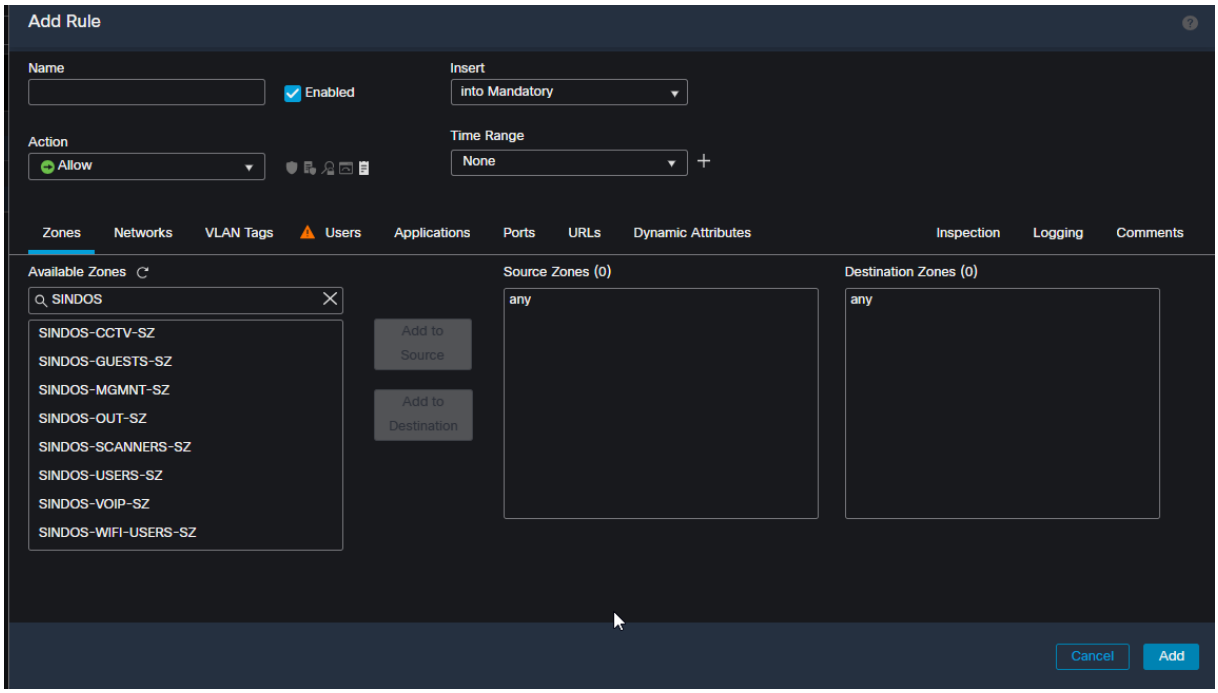
>Έλεγχος της κίνησης με βάση μια πολιτική εισβολής.



Εικόνα 5.19 Προεπιλεγμένες ενέργειες στο ACP

5.9.3 Rule Editor-Συντάκτης κανόνων

Μπορείτε να δημιουργήσετε ή να τροποποιήσετε κανόνες ελέγχου πρόσβασης χρησιμοποιώντας τον συντάκτη κανόνων. Για να ανοίξετε το παράθυρο του επεξεργαστή κανόνων, κάντε κλικ στο κουμπί Προσθήκη κανόνα στον συντάκτη πολιτικής. Ομοίως, για να ανοίξετε έναν υπάρχοντα κανόνα ελέγχου πρόσβασης στον συντάκτη κανόνων, κάντε κλικ στο εικονίδιο μολυβιού δίπλα σε έναν κανόνα. Το παράθυρο προσθήκη κανόνα εμφανίζεται όταν κάνετε κλικ στο κουμπί προσθήκη κανόνα στη σελίδα επεξεργασίας πολιτικής.



Εικόνα 5.20 Προσθήκη κανόνα στο ACP

Ένας κανόνας ελέγχου πρόσβασης μπορεί να έχει μία ή περισσότερες συνθήκες αντιστοίχισης. Μπορείτε να χρησιμοποιήσετε διάφορα κριτήρια δικτύωσης ως συνθήκες, όπως security zones, διευθύνσεις δικτύου, θύρες, χρήστες, εφαρμογές και διευθύνσεις URL. Μπορείτε επίσης να καθορίσετε οποιεσδήποτε ημέρες και ώρες κατά τις οποίες ένας κανόνας θα γίνεται ενεργός. Όταν ένα πακέτο ταιριάζει με μια συνθήκη του κανόνα, το firewall χειρίζεται την κίνηση με βάση την ενέργεια που επιλέγετε στον κανόνα ελέγχου πρόσβασης. Οι διαθέσιμες επιλογές είναι να επιτρέψετε, να εμπιστευτείτε, να παρακολουθήσετε ή να αποκλείσετε μια σύνδεση.

Όπως γνωρίζετε, μια πολιτική ελέγχου πρόσβασης είναι το κεντρικό σημείο για την επίκληση όλων των άλλων πολιτικών ασφαλείας. Μπορείτε να συσχετίσετε μια προκαθορισμένη πολιτική αρχείων και μια πολιτική εισβολής με κάθε κανόνα ξεχωριστά. Οι άλλες πολιτικές ασφαλείας, όπως οι πολιτικές προφιλτραρίσματος, οι πολιτικές Secure Socket Layer (SSL) και οι πολιτικές ταυτότητας, καλούνται συνολικά στη σελίδα επεξεργασίας πολιτικής ελέγχου πρόσβασης.

5.9.4 Βέλτιστες πρακτικές για την πολιτική ελέγχου πρόσβασης

Η τοποθέτηση των κανόνων ελέγχου πρόσβασης σε μια πολιτική ελέγχου πρόσβασης μπορεί να επηρεάσει τη χρήση της CPU και της μνήμης του firewall. Οι κανόνες ελέγχου πρόσβασης αξιολογούνται διαδοχικά από πάνω προς τα κάτω. Επομένως, λάβετε υπόψη τις ακόλουθες βέλτιστες πρακτικές όταν διαμορφώνετε μια πολιτική ελέγχου πρόσβασης:

Αρχικά, τοποθετήστε τους κανόνες με ενέργειες αποκλεισμού στην κορυφή της πολιτικής ελέγχου πρόσβασης. Αυτό επιτρέπει στο firewall να αρνείται την κυκλοφορία ταχύτερα. Κατά τη διαδικασία αξιολόγησης κανόνων, όταν ένα πακέτο ταιριάζει με τους περιορισμούς του κανόνα και βρίσκει έναν κανόνα με ενέργεια αποκλεισμού, σταματά η περαιτέρω αξιολόγηση του πακέτου σε σχέση με τους υπόλοιπους κανόνες της πολιτικής.

Στη συνέχεια, τοποθετήστε τους επακριβώς καθορισμένους κανόνες πριν από έναν ευρύτερο κανόνα. Όταν η κυκλοφορία ταιριάζει πρώτα με έναν ευρύτερο κανόνα, δεν θα αξιολογηθεί περαιτέρω έναντι οποιουδήποτε κανόνα με πιο συγκεκριμένες προϋποθέσεις.

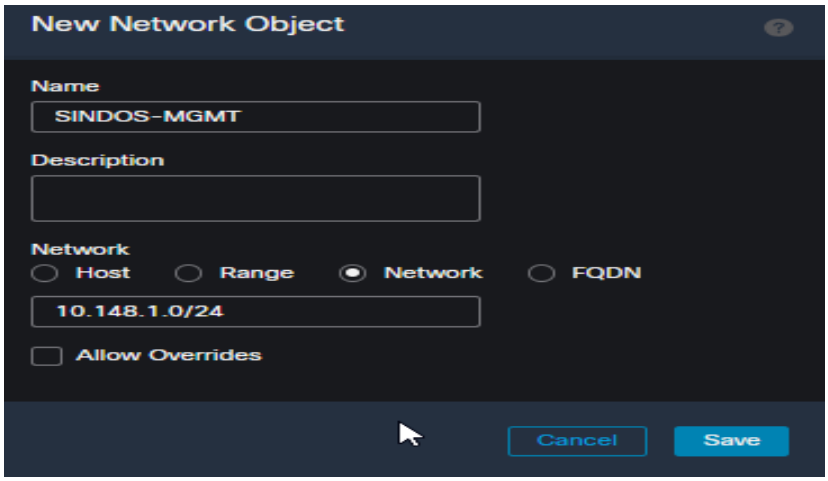
Οι κανόνες που δεν σχετίζονται με μια πολιτική εισβολής ή μια πολιτική αρχείων θα πρέπει να τοποθετούνται πριν από τους κανόνες που σχετίζονται με αυτούς.

Η διαχείριση των κανόνων με τη χρήση διευθύνσεων IP μπορεί να είναι δύσχρηστη όταν έχετε μια πολιτική ελέγχου πρόσβασης με χιλιάδες κανόνες. Ωστόσο, αν χρησιμοποιείτε αντικείμενα σε έναν κανόνα, δεν χρειάζεται να καταργήσετε τον παλιό κανόνα και να προσθέσετε έναν νέο για να αντικατοπτρίσετε τις νέες διευθύνσεις IP. Αντίθετα, απλώς επεξεργάζεστε και ενημερώνετε την τιμή του σχετικού αντικειμένου. Αφού κάνετε deploy εκ νέου την πολιτική ασφαλείας, οι νέες τιμές των αντικειμένων εφαρμόζονται αυτόματα στο σύνολο κανόνων.

Η δημιουργία αντικειμένων για τους πόρους του δικτύου και η επαναχρησιμοποίησή τους στον έλεγχο πρόσβασης είναι προαιρετική- ωστόσο, σας βοηθάει στη διαχείριση των ρυθμίσεων μακροπρόθεσμα.

Το FMC σάς επιτρέπει να δημιουργείτε αντικείμενα για διευθύνσεις δικτύου, αριθμούς θυρών, διευθύνσεις URL, FQDN και πολλά άλλα μεταβλητά στοιχεία μιας πολιτικής. Μπορείτε επίσης να ομαδοποιήσετε πολλαπλά αντικείμενα σε μια ενιαία διαμόρφωση, η οποία ονομάζεται ομάδα αντικειμένων (object group).

Μπορείτε να προσθέσετε, να διαγράψετε και να τροποποιήσετε ένα αντικείμενο μεταβαίνοντας στην επιλογή Objects > Object Management στο GUI. Ένα FMC έρχεται με προκαθορισμένα αντικείμενα που βασίζονται σε γνωστές διευθύνσεις ή αριθμούς θυρών. Μπορείτε να τα χρησιμοποιήσετε σε μια πολιτική, αλλά δεν μπορείτε να τροποποιήσετε τις τιμές τους.



Εικόνα 5.21 Δημιουργία object τύπου network

Εάν θέλετε να επιτρέψετε ή να αποκλείσετε την κυκλοφορία αποκλειστικά βάσει διεύθυνση IP πηγής, διεύθυνση IP προορισμού, αριθμός θύρας πηγής, αριθμός θύρας προορισμού και πρωτόκολλο, εξετάστε το ενδεχόμενο να χρησιμοποιήσετε έναν κανόνα προφιλτραρίσματος για αυτούς. Βελτιώνει την απόδοση του συστήματος. [14]

5.10 Διαμόρφωση πολιτικής ελέγχου πρόσβασης

Ένας κανόνας ελέγχου πρόσβασης μπορεί να δημιουργηθεί με μεγάλη ποικιλία συνθηκών. Θα επικεντρωθούμε κυρίως στην έννοια της δημιουργίας κανόνων και όχι στη δημιουργία πολλών κανόνων με κάθε πιθανό συνδυασμό.

Όπως αναφέραμε έχουμε τα εξής δίκτυα:

Όνομα	Vlan	Υποδίκτυο
SINDOS-MGMNT	1	10.148.1.0/24
SINDOS-USERS	2	10.148.2.0/24
SINDOS-SCANNERS	3	10.148.3.0/24
SINDOS-CCTV	4	10.148.4.0/24
SINDOS-WIFI-USERS	5	10.148.5.0/24
SINDOS-GUESTS	60	10.148.60.0/24
SINDOS-VOIP	100	10.148.100.0/24

Ο πελάτης έχει ζητήσει τους παρακάτω περιορισμούς όσον αφορά την επικοινωνία μεταξύ τους αλλά και την πρόσβαση κάθε συσκευής στο διαδίκτυο.

1. Τα MGMNT,USERS,SCANNERS,VOIP και WIFI-USERS δίκτυα να επικοινωνούν μεταξύ τους και να έχουν πρόσβαση στο διαδίκτυο.

2. Το δίκτυο που αφορά τις κάμερες CCTV και τους GUESTS να έχει πρόσβαση στο διαδίκτυο αλλά να μην έχει επικοινωνία με τα προαναφερθέντα δίκτυα

3. Να υπάρχει εξωτερική πρόσβαση στο MGMNT από ένα συγκεκριμένο δίκτυο για την απομακρυσμένη διαχείριση του firewall και των switches.

4. Να απαγορεύεται η πρόσβαση σε εφαρμογές peer to peer(πχ utorrent) καθώς και σε ιστοσελίδες με περιεχόμενο μόνο για ενήλικες.

5. Να απαγορευτεί η πρόσβαση στο TikTok.

Δημιουργία κανόνων

Για να δημιουργήσετε έναν κανόνα ελέγχου πρόσβασης, ακολουθήστε τα παρακάτω βήματα:

Βήμα 1. Πλοηγηθείτε στο Policies > Access Control > Access Control. Εμφανίζεται μια λίστα με τις διαθέσιμες πολιτικές ελέγχου πρόσβασης

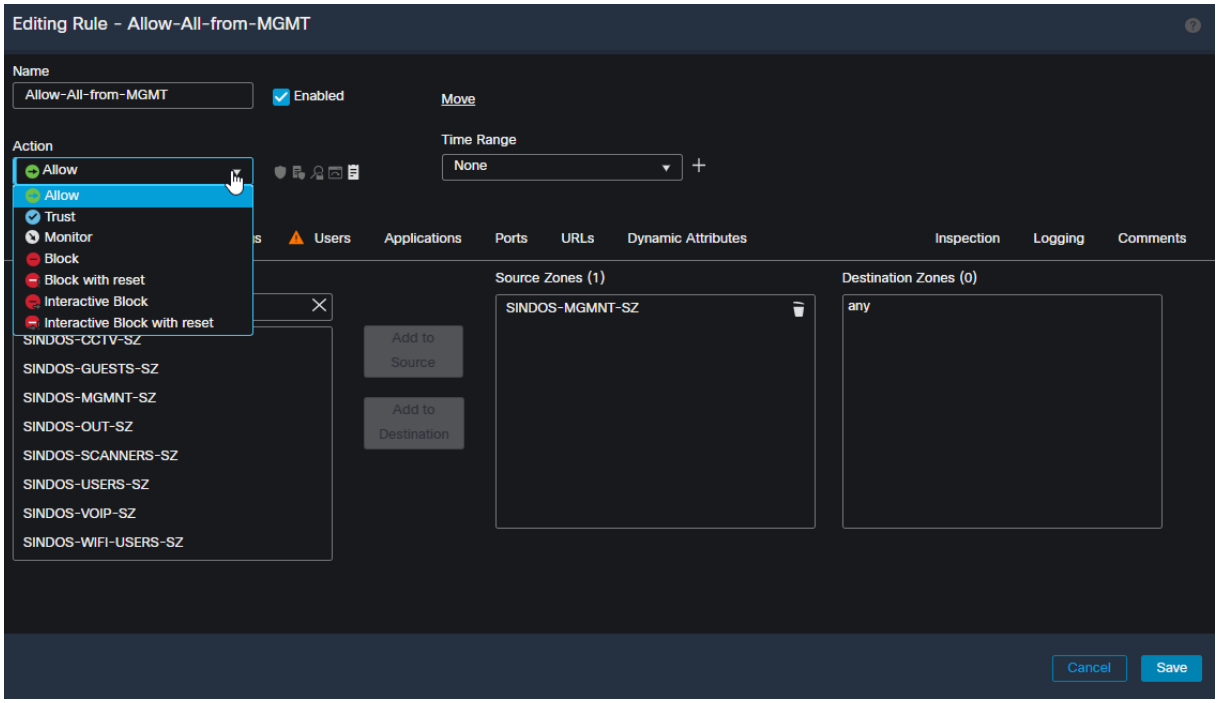
Βήμα 2. Χρησιμοποιήστε το εικονίδιο μολυβιού δίπλα στο όνομα της πολιτικής για να ανοίξετε τον επεξεργαστή πολιτικής. Εμφανίζεται η σελίδα επεξεργασίας πολιτικής ελέγχου πρόσβασης. Εάν θέλετε να χρησιμοποιήσετε μια νέα πολιτική, κάντε κλικ στο κουμπί New Policy για να δημιουργήσετε μια νέα πολιτική.

Βήμα 3. Στον συντάκτη πολιτικής, κάντε κλικ στο κουμπί Add Rule (Προσθήκη κανόνα). Ανοίγει το παράθυρο Add Rule

Βήμα 4. Τώρα έχουμε τα ακόλουθα

α) Δώστε ένα όνομα στον κανόνα.

β) Χρησιμοποιήστε το αναπτυσσόμενο πλαίσιο Action για να επιλέξετε αν θέλετε να αποκλείσετε η να επιτρέψετε την κίνηση. Υπάρχουν τέσσερις τύποι ενεργειών αποκλεισμού.



Εικόνα 5.22 Παράθυρο επεξεργασίας κανόνα

Όλες αποκλείουν την κίνηση που ταιριάζει χωρίς περαιτέρω έλεγχο, αλλά έχουν διαφορετικές προσεγγίσεις:

Επιλέξτε **Block** για να αποκλείσετε την κίνηση.

Επιλέξτε **Block with Reset** για να αρνηθείτε την κυκλοφορία καθώς και για να στείλετε ένα TCP RST στον αιτούντα έτσι ώστε να γίνει reset του tcp connection και να μην καταναλώνονται πόροι.

Επιλέξτε **Interactive Block** για να στείλετε ένα διαδραστικό μήνυμα απάντησης στον αιτούντα.

Επιλέξτε **Interactive Block with Reset** για να στείλετε ένα μήνυμα απάντησης πριν από την αποστολή TCP RST στον αιτούντα.

Όσον αφορά τις επιλογές που έχουμε για να επιτρέψουμε την κίνηση, αυτές είναι οι **Allow, Trust** και **Monitor**

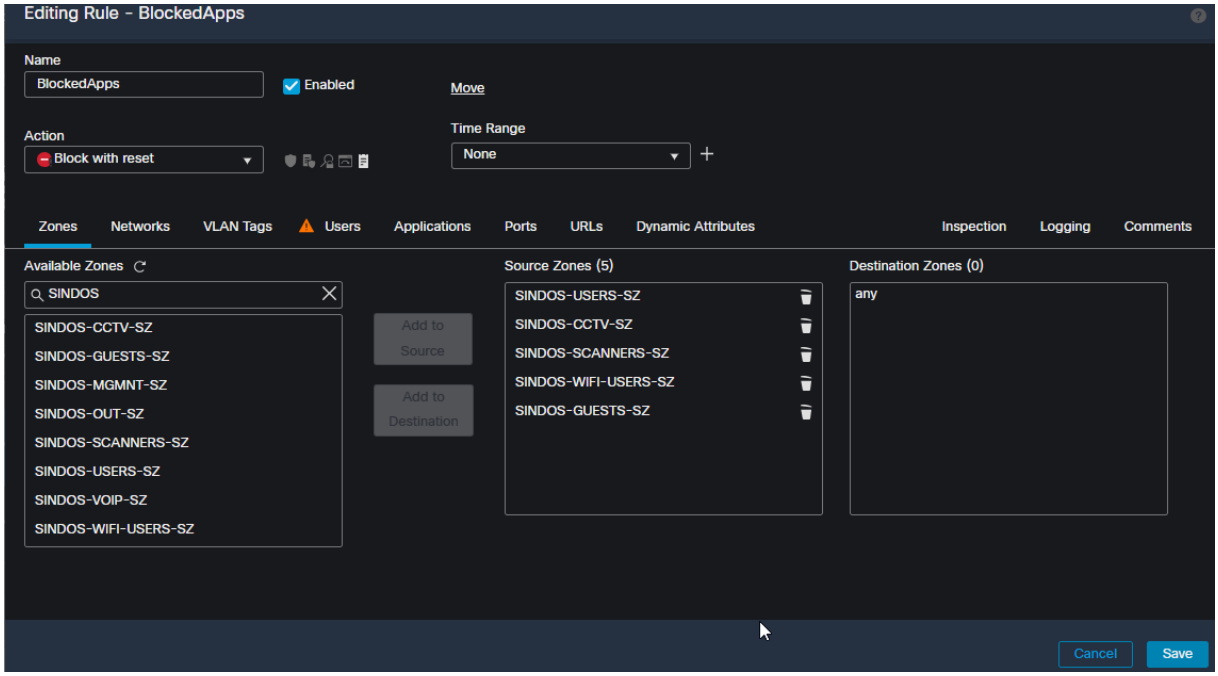
Η επιλογή **Allow** επιτρέπει την κίνηση, αλλά και πάλι θα περάσει από την πολιτική εισβολής(Intrusion Policy) και αρχείων(File Policy).

Η επιλογή **Trust** σημαίνει επιτρέπω την κίνηση χωρίς καμία περαιτέρω επιθεώρηση. Η επιλογή **Monitor** σημαίνει καταγραφή της κίνησης(πολύ χρήσιμο αν θέλουμε να ελέγξουμε για false positives πριν κάνουμε deploy έναν νεο κανόνα) και στη συνέχεια συνέχιση των υπόλοιπων κανόνων.

Οι επιλογές βάση των οποίων μπορεί να γίνει το φιλτράρισμα της κίνησης είναι οι εξής:

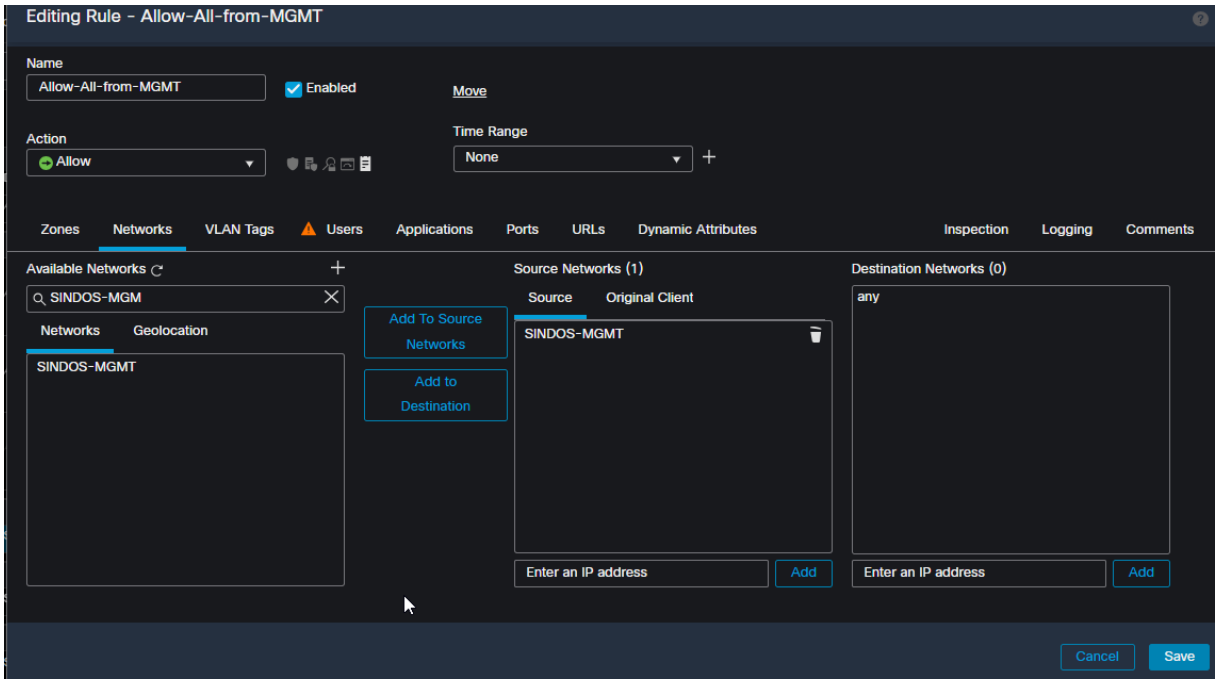
Security Zone:

Μια ζώνη ασφαλείας είναι μια ομαδοποίηση interfaces όπως έχουμε αναφέρει. Οι ζώνες χωρίζουν το δίκτυο σε τμήματα για να σας βοηθήσουν στη διαχείριση και ταξινόμηση της κυκλοφορίας.



Εικόνα 5.23 Ρύθμιση κανόνα με βάση τα security zones της υποδομής

Networks: Φιλτράρισμα της κίνησης βάση δικτύου. Έστω ότι θέλουμε να φιλτράρουμε την κίνηση που προέρχεται από το δίκτυο 10.148.1.0/24, θα μπορούσαμε να το χρησιμοποιήσουμε την IPv4 διεύθυνση του, αλλά θα ήταν καλύτερο να δημιουργήσουμε ένα αντικείμενο τύπου network με όνομα SINDOS-MGMT και να του αποδώσουμε την τιμή 10.148.1.0/24.



Εικόνα 5.24 Ρύθμιση κανόνα ο οποίος επιτρέπει την κίνηση που ξεκινάει από το management δίκτυο.

Users:

Αν γίνει σύνδεση του firewall με τον domain controller(συνήθως ένας windows server που έχει τους χρήστες της υποδομής) της υποδομής, μπορεί να γίνει φιλτράρισμα της κίνησης βάση του χρήστη του υπολογιστή στον οποίο ανήκει

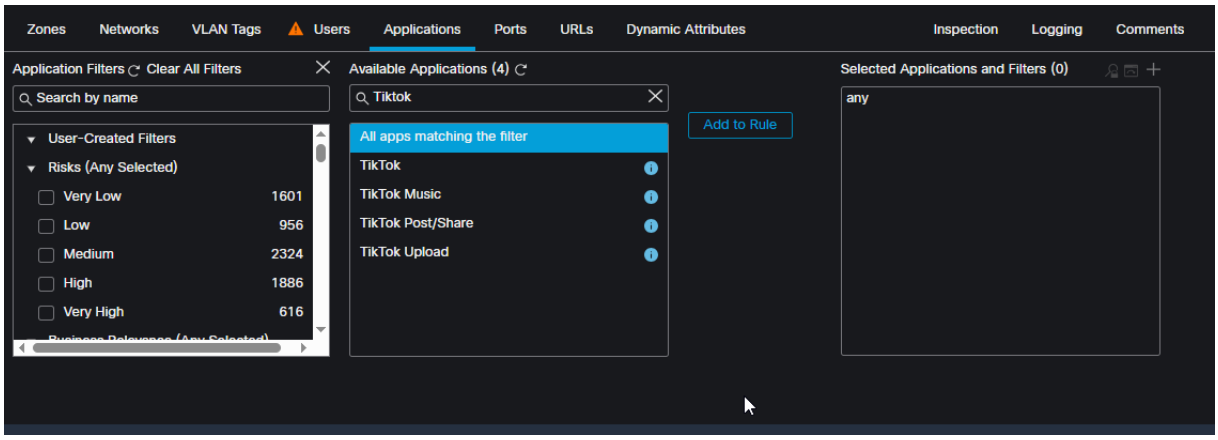
Applications:

Δεδομένου ότι το firewall κάνει ανάλυση της κίνησης μπορεί να εντοπίσει και να ταξινομήσει τις κοινά χρησιμοποιούμενες εφαρμογές στο δίκτυό σας.

Για παράδειγμα, θα μπορούσατε να δημιουργήσετε έναν κανόνα ελέγχου πρόσβασης που να εντοπίζει και να αποκλείει όλες τις υψηλού κινδύνου, χαμηλής επιχειρηματικής δραστηριότητας εφαρμογές. Εάν ένας χρήστης επιχειρήσει να χρησιμοποιήσει μια από αυτές τις εφαρμογές, η συνεδρία μπλοκάρεται.

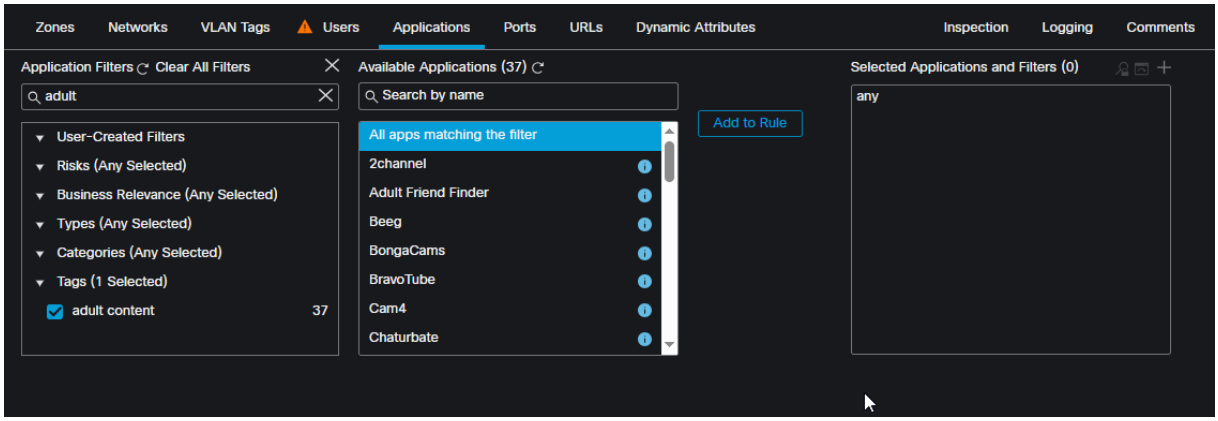
Οι τρόποι με τους οποίους μπορείτε να καθορίσετε εφαρμογές των οποίων την κυκλοφορία θέλετε να ελέγξετε είναι οι εξής:

- Μπορείτε να επιλέξετε μεμονωμένες εφαρμογές πχ TikTok.



Εικόνα 5.25 Ρύθμιση κανόνα φιλτραρίσματος της εφαρμογής TikTok

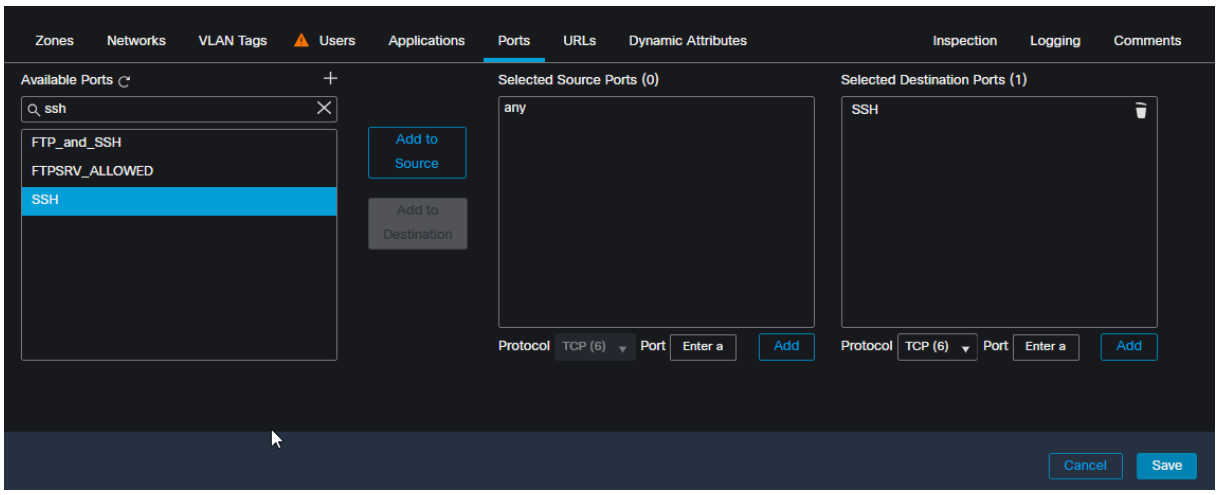
- Μπορείτε να χρησιμοποιήσετε φίλτρα εφαρμογών που παρέχονται από το σύστημα, τα οποία είναι ονομαστικά σύνολα εφαρμογών οργανωμένα με γνώμονα τα βασικά χαρακτηριστικά των εφαρμογών: Τύπος εφαρμογής, Κίνδυνος, επιχειρησιακή συνάφεια, κατηγορίες και ετικέτες. Πχ μια ετικέτα είναι το ενήλικο περιεχόμενο όπου επιλέγοντας την θα μπλοκάρει όλες τις εφαρμογές που περιέχουν ενήλικο περιεχόμενο



Εικόνα 5.26 Ρύθμιση κανόνα φιλτράρισματος adult περιεχόμενου

Ports:

Δίνεται και δυνατότητα φιλτραρίσματος βάση πορτών TCP/UDP έτσι θέλετε να μπλοκάρετε ένα συγκεκριμένο πρωτόκολλο πχ SSH αρκεί να θέσετε ως destination port την θύρα 22



Εικόνα 5.27 Παραμετροποίηση κανόνα βάση πορτών προορισμού

URL Filtering:

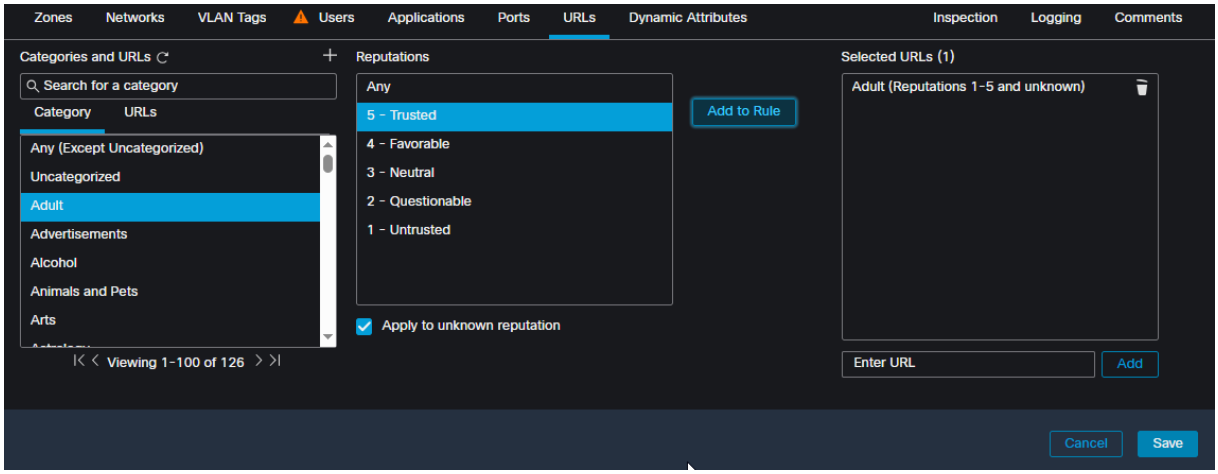
Η λειτουργία Φιλτραρίσματος URL μπορεί να κατηγοριοποιήσει εκατομμύρια διευθύνσεις URL και domains. Μπορείτε να ενεργοποιήσετε αυτή τη λειτουργία για να αποτρέψετε τους κεντρικούς υπολογιστές του δικτύου σας από την πρόσβαση σε έναν συγκεκριμένο τύπο URL.

Κατηγορία και φήμη(Category and Reputation)

Μπορείτε να χρησιμοποιήσετε το GUI του κέντρου διαχείρισης για να κατεβάσετε τη βάση δεδομένων URL απευθείας από το cloud της Cisco. Το cloud περιέχει την ανάλυση εκατομμυρίων URL, τα οποία κατηγοριοποιούνται σε περίπου εκατό διαφορετικές κατηγορίες. Η βάση δεδομένων URL Web Reputation Index - WRI, ο οποίος υπολογίζεται δυναμικά με βάση σημεία δεδομένων από διάφορες

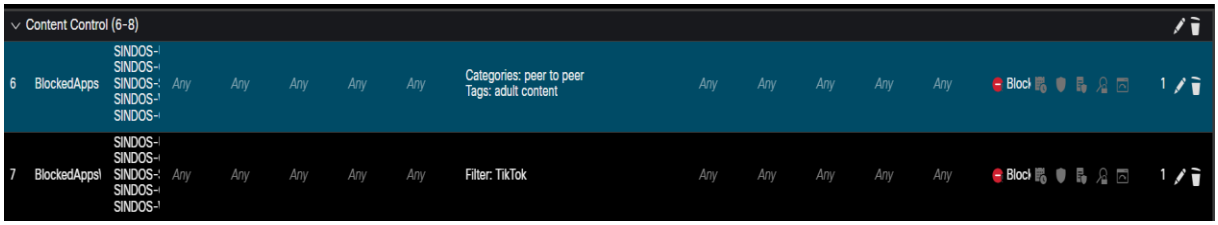
πηγές, όπως η ηλικία και το ιστορικό του ιστότοπου, η φήμη και η τοποθεσία της διεύθυνσης IP, καθώς και το θέμα και το πλαίσιο του περιεχομένου.

Με βάση την ενέργεια -Allow ή Block- που έχει ρυθμιστεί, το κέντρο διαχείρισης προσθέτει αυτόματα επιπλέον επίπεδα φήμης URL μαζί με την αρχική σας επιλογή. Για παράδειγμα, όταν επιλέγετε την ενέργεια Allow για ένα συγκεκριμένο επίπεδο φήμης, το κέντρο διαχείρισης επιτρέπει όλες τις διευθύνσεις URL αυτού του επιπέδου καθώς και τις διευθύνσεις URL που είναι πιο καλοήθεις από το επιλεγμένο επίπεδο. Ομοίως, αν επιλέξετε την ενέργεια Αποκλεισμός για ένα συγκεκριμένο επίπεδο φήμης, το κέντρο διαχείρισης αποκλείει όλες τις διευθύνσεις URL αυτού του επιπέδου μαζί με όλες τις διευθύνσεις URL που είναι πιο επικίνδυνες από το επίπεδο που επιλέξατε.



Εικόνα 5.28 Παράδειγμα κατηγορίας Adult το οποίο θα γίνει block

Ακολουθούν οι ρυθμίσεις μπλοκαρίσματος των εφαρμογών peer-to-peer, ο αποκλεισμός της κίνησης του TikTok και του adult περιεχομένου, όπως έχει ζητηθεί από τον πελάτη



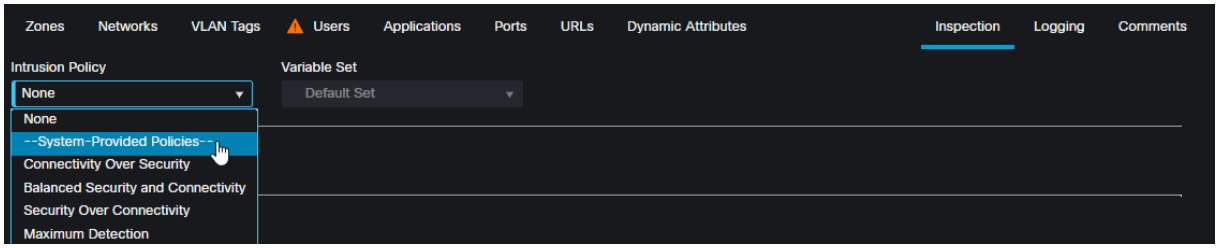
Εικόνα 5.29 Κανόνες αποκλεισμού μη επιθυμητών URL και εφαρμογών

5.11 Network Analysis και Intrusion Policies

Ένα κύριο χαρακτηριστικό του Cisco Secure Firewall είναι ότι μπορεί να λειτουργήσει ως σύστημα ανίχνευσης εισβολών (IDS) καθώς και ως σύστημα πρόληψης εισβολών (IPS). Η λειτουργία IDS/IPS βασίζεται στο Snort, ένα IPS ανοικτού κώδικα. Μπορείτε να γράψετε κανόνες Snort για να παρακολουθείτε πακέτα δικτύου, να ανιχνεύετε κακόβουλες δραστηριότητες, να δημιουργείτε ειδοποιήσεις για τους χρήστες ή ακόμη και να αποκλείετε την είσοδο επιβλαβών πακέτων σε ένα δίκτυο. Στο Secure Firewall, ένας κανόνας Snort είναι επίσης γνωστός ως κανόνας εισβολής. Η λειτουργία των κανόνων εισβολής διέπεται από δύο πολιτικές: μια πολιτική εισβολής (intrusion policy) και μια πολιτική ανάλυσης δικτύου (network analysis policy).

5.11.1 Intrusion Prevention System

Για να απλοποιήσει και να επιταχύνει την αρχική διαμόρφωση του συστήματος, το firewall διαθέτει πολλές ενσωματωμένες πολιτικές εισβολής. Μπορείτε να επιλέξετε μία από αυτές μέσω ενός κανόνα ελέγχου πρόσβασης, access control rule. Επίσης υπάρχει η επιλογή προεπιλεγμένης ενέργειας αν η κίνηση δεν κάνει match σε κάποιον κανόνα (Εικόνα 5.19).



Σχήμα 5.30 Επιλογές Intrusion Policy

Βασικές πολιτικές που παρέχονται από το σύστημα

Το firewall συνοδεύεται από διάφορες προκαθορισμένες πολιτικές ανάλυσης δικτύου και εισβολής. Μπορείτε να χρησιμοποιήσετε μία από αυτές απευθείας ή να αποτελέσουν την βάση για τη δική σας προσαρμοσμένη πολιτική εισβολής:

> Ισορροπημένη ασφάλεια και συνδεσιμότητα (**Balanced Security and Connectivity**): Αυτή η βασική πολιτική είναι το καλύτερο σημείο εκκίνησης για να δημιουργήσετε τη δική σας πολιτική εισβολής που μπορεί να αντιμετωπίσει τα κρίσιμα τρωτά σημεία, διατηρώντας παράλληλα την απόδοση του συστήματος.

> Συνδεσιμότητα έναντι ασφάλειας (**Connectivity over Security**): Αυτή η πολιτική δίνει προτεραιότητα στην ταχύτητα σύνδεσης μειώνοντας την ανίχνευση παλαιότερων ή λιγότερο κρίσιμων ευπαθειών.

> Ασφάλεια έναντι συνδεσιμότητας (**Security over Connectivity**): Αυτή η πολιτική δίνει προτεραιότητα στην ασφάλεια του δικτύου έναντι της συνδεσιμότητας, ενεργοποιώντας μεγαλύτερο αριθμό κανόνων και ορίζοντας περισσότερους κανόνες για την απόρριψη της παραβατικής κυκλοφορίας σε σχέση με τις άλλες προεπιλεγμένες πολιτικές.

> Μέγιστη ανίχνευση (**Maximum Detection**): Η ασφάλεια έχει ύψιστη προτεραιότητα έναντι της επιχειρησιακής συνέχειας. Λόγω της βαθύτερης επιθεώρησης των πακέτων με αυτή την πολιτική, οι τελικοί χρήστες ενδέχεται να αντιμετωπίσουν καθυστέρηση και το firewall ενδέχεται να απορρίψει κάποια νόμιμη κυκλοφορία.

5.11.2 Malware και File Policy

Παρόλο που επιτρέπετε στους χρήστες σας να επισκέπτονται τους περισσότερους ιστότοπους, ενδέχεται να θέλετε να μπλοκάρετε τις προσπάθειές τους να κατεβάζουν κακόβουλα αρχεία από τους ιστότοπους που επισκέπτονται ή να μεταφορτώνουν εσωτερικά αρχεία σε εξωτερικούς ιστότοπους. Οι μη ασφαλείς λήψεις μπορούν να εξαπλώσουν ιούς, κακόβουλο λογισμικό, κιτ εκμετάλλευσης και άλλους κινδύνους στο δίκτυό σας και μπορούν να καταστήσουν ολόκληρο το δίκτυο ευάλωτο σε διάφορους τύπους επιθέσεων. Ομοίως, για να συμμορφωθείτε με τις πολιτικές του οργανισμού σας, μπορεί να μην θέλετε οι χρήστες σας να μεταφορτώνουν συγκεκριμένους τύπους αρχείων στο Διαδίκτυο από το εταιρικό σας δίκτυο. Το firewall σας επιτρέπει να αποκλείετε τη λήψη και τη μεταφόρτωση αρχείων με βάση τον τύπο αρχείου (.png, .pdf, .exe και άλλα) και τη διάθεση του αρχείου (κακόβουλο λογισμικό).

File Policy Essentials

Για την παρακολούθηση και τον έλεγχο της μεταφοράς αρχείων μέσω δικτύου, το firewall προσφέρει μια αυτόνομη πολιτική γνωστή ως πολιτική αρχείων. Μια πολιτική αρχείων σας επιτρέπει να ανιχνεύετε οποιονδήποτε τύπο αρχείου, όπως αρχεία πολυμέσων (.mp3, .mpeg) και εκτελέσιμα αρχεία (.exe, .rpm). Επιπλέον, μπορεί να αναλύσει ένα αρχείο για πιθανό κακόβουλο λογισμικό όταν το αρχείο διασχίζει ένα δίκτυο ή να ανιχνεύει και να αποκλείει αρχεία με βάση τον τύπο τους, προτού εκτελέσει αναζητήσεις για κακόβουλο λογισμικό.

Ανίχνευση τύπου αρχείου

Το firewall χρησιμοποιεί μια ακολουθία μοναδικών δεκαεξαδικών χαρακτήρων που κωδικοποιούνται στις επικεφαλίδες των αρχείων για την αναγνώριση της μορφής αρχείου. Όταν ένα αρχείο διασχίζει ένα δίκτυο, ένα firewall μπορεί να βρει τους αριθμούς αυτούς στη ροή των πακέτων για να προσδιορίσει τη μορφή του αρχείου. Για παράδειγμα, για ένα εκτελέσιμο αρχείο της Microsoft (MSEXE), ο αριθμός αρχείου είναι 4D 5A και βρίσκεται στην αρχή του αρχείου.

Malware Analysis

Για την προστασία ενός δικτύου από το πιο πρόσφατο κακόβουλο λογισμικό, το firewall είναι εξοπλισμένο με την τεχνολογία άμυνας κακόβουλου λογισμικού (επίσης γνωστή ως προηγμένη προστασία από κακόβουλο λογισμικό ή AMP). Αυτή η τεχνολογία του επιτρέπει να αναλύει ένα αρχείο για πιθανό κακόβουλο λογισμικό και ιούς, ενώ το αρχείο διατρέχει ένα δίκτυο. Για την επιτάχυνση της διαδικασίας ανάλυσης και την εξοικονόμηση πόρων, μπορεί να εκτελεί τόσο τοπική όσο και δυναμική ανάλυση. Το firewall υπολογίζει το hash value χρησιμοποιώντας τον SHA-256 (Secure Hash Algorithm with 256 bits) ενός αρχείου και χρησιμοποιεί την τιμή για να καθορίσει τη πρόθεση(disposition) ενός αρχείου (κακόβουλο λογισμικό, καθαρό, άγνωστο, μη διαθέσιμο). Το κέντρο διαχείρισης στέλνει ένα ερώτημα στο νέφος ανάλυσης κακόβουλου λογισμικού για να δει αν έχει πληροφορίες σχετικά με την πρόθεση του αρχείο και αποθηκεύει στην προσωρινή του μνήμη προηγούμενες αναζητήσεις για να παρέχει ταχύτερο αποτέλεσμα αναζήτησης και να βελτιώσει τη συνολική απόδοση.

5.11.3 Διαμόρφωση μιας πολιτικής αρχείων

Η διαμόρφωση μιας πολιτικής αρχείων είναι μια διαδικασία πολλών βημάτων. Αρχικά, πρέπει να δημιουργήσετε μια πολιτική αρχείων και να προσθέσετε κανόνες αρχείων σε αυτήν. Ένας κανόνας αρχείου σας επιτρέπει να επιλέξετε την κατηγορία τύπου αρχείου, το πρωτόκολλο εφαρμογής, την κατεύθυνση μεταφοράς και την ενέργεια. Ωστόσο, δεν μπορείτε να προσθέσετε λεπτομέρειες πηγής ή προορισμού σε έναν κανόνα αρχείου. Για να εκχωρήσετε διευθύνσεις IP πηγής και προορισμού, δημιουργήστε έναν κανόνα ελέγχου πρόσβασης στην πολιτική ελέγχου πρόσβασης και επικαλεστείτε την πολιτική αρχείου εντός του κανόνα ελέγχου πρόσβασης.

Δημιουργία πολιτικής αρχείου

Για να δημιουργήσετε μια πολιτική αρχείου, ακολουθήστε τα παρακάτω βήματα:

1. Πλοηγηθείτε στις Policies >Access Control > Malware & File.

2. Κάντε κλικ στο κουμπί New File Policy και δώστε ένα όνομα

3. Ονομάστε την πολιτική και κάντε κλικ στο κουμπί Αποθήκευση. Εμφανίζεται ο επεξεργαστής πολιτικής αρχείου.

4. Κάντε κλικ στο κουμπί Add Rule. Εμφανίζεται ο επεξεργαστής κανόνων αρχείων.

5. Επιλέξτε Any (Οποιοδήποτε) από το αναπτυσσόμενο μενού Application Protocol (Πρωτόκολλο εφαρμογής) για να ανιχνεύσετε αρχεία μέσω πολλαπλών πρωτοκόλλων εφαρμογής.

6. Κάντε μια επιλογή από το αναπτυσσόμενο πλαίσιο Κατεύθυνση μεταφοράς. Ανάλογα με το υποκείμενο πρωτόκολλο εφαρμογής για μια μεταφορά αρχείου, η κατεύθυνση μπορεί να είναι περιορισμένη. Για παράδειγμα, τα πρωτόκολλα HTTP, FTP και NetBIOS-ssn (SMB) μπορούν να παρακολουθούνται για μεταφορές αρχείων σε οποιαδήποτε κατεύθυνση - φόρτωση ή λήψη. Ωστόσο, το SMTP (μόνο μεταφόρτωση) και το POP3/IMAP (λήψη) υποστηρίζουν μόνο μεταφορές αρχείων προς μία κατεύθυνση.

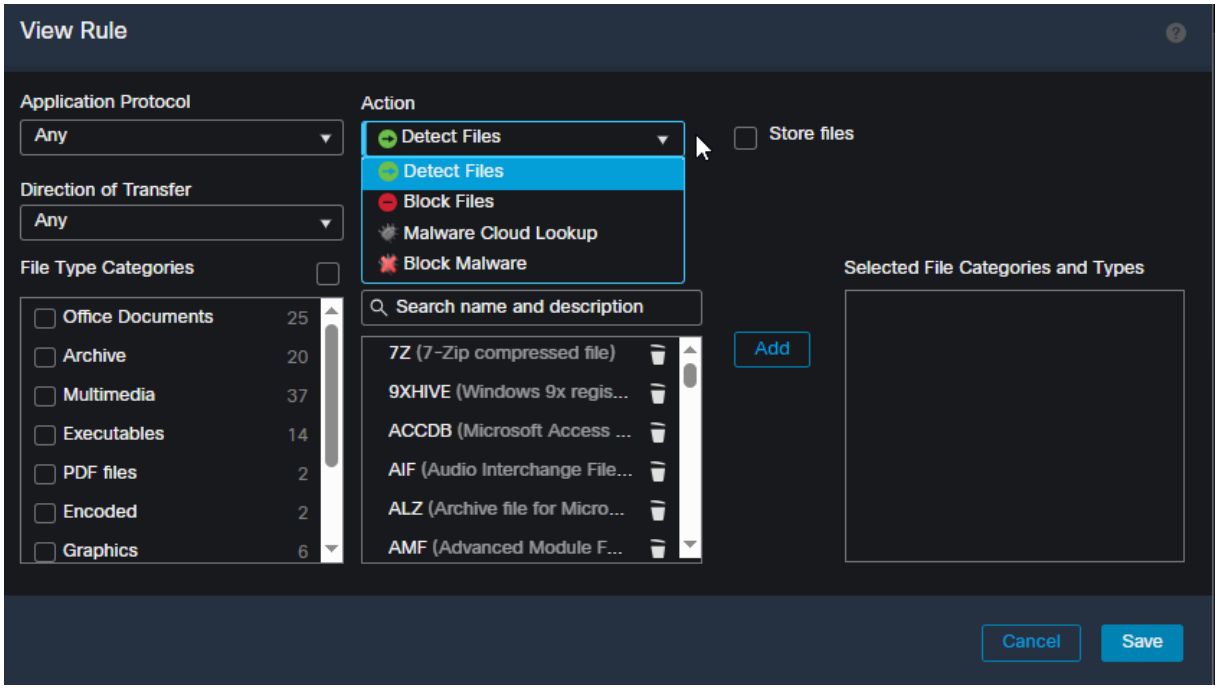
7. Επιλέξτε τις κατηγορίες τύπων αρχείων που θέλετε να επεξεργαστείτε και κάντε κλικ στο κουμπί Προσθήκη για να τις προσθέσετε στον κανόνα. Μπορείτε επίσης να αναζητήσετε συγκεκριμένους τύπους αρχείων απευθείας στο πεδίο αναζήτησης.

8. Επιλέξτε μια ενέργεια από το αναπτυσσόμενο πλαίσιο Action (Ενέργεια). Θα βρείτε τέσσερις επιλογές στο αναπτυσσόμενο μενού:

> Ανίχνευση αρχείων: Αυτή η ενέργεια ανιχνεύει μια μεταφορά αρχείου και την καταγράφει ως συμβάν αρχείου, χωρίς να διακόπτει τη μεταφορά.

> Αποκλεισμός αρχείων: Αυτή η ενέργεια μπλοκάρει τα αρχεία με βάση τους τύπους αρχείων που έχουν επιλεγεί στον κανόνα.

Όταν μπλοκάρετε ένα αρχείο, μπορείτε προαιρετικά να επιλέξετε την επιλογή επαναφορά σύνδεσης. Επιτρέπει στη μπλοκαρισμένη περίοδο λειτουργίας της εφαρμογής να κλείσει πριν η σύνδεση τερματιστεί από μόνη της, κάτι που μπορεί να διαρκέσει αρκετά λεπτά ανάλογα με την εφαρμογή.



Εικόνα 5.31 - Επιλογές κανόνα πολιτικής αρχείων

> Malware Cloud Lookup: Αυτή η ενέργεια επιτρέπει στο firewall να εκτελεί ανάλυση κακόβουλου λογισμικού τοπικά και απομακρυσμένα. Το firewall επιτρέπει την αδιάλειπτη μεταφορά αρχείων ανεξάρτητα από τη διάθεση του αρχείου.

> Block Malware: Αυτή η ενέργεια είναι παρόμοια με την ενέργεια Malware Cloud Lookup, αλλά επιτρέπει στην άμυνα απειλών να μπλοκάρει αρχεία που επιστρέφουν τη διάθεση κακόβουλου λογισμικού.

Με λίγα λόγια, οι δύο πρώτες επιλογές - Εντοπισμός αρχείων και Αποκλεισμός αρχείων - σας επιτρέπουν να ελέγχετε τα αρχεία με βάση τον τύπο τους. Οι δύο τελευταίες επιλογές - Malware Cloud Lookup και Block Malware - σας επιτρέπουν να ελέγχετε αρχεία με βάση τη διάθεση το disposition .

5.12 Μετάφραση διευθύνσεων δικτύου (NAT)

Κάθε εξωτερικός χρήστης, είτε πρόκειται για επιτιθέμενο είτε για νόμιμο χρήστη του Διαδικτύου, δεν πρέπει να έχει ορατότητα στο εσωτερικό σας δίκτυο. Μπορείτε να αποκρύψετε τις εσωτερικές διευθύνσεις του δικτύου σας μεταμορφώνοντάς τες σε δημόσιες διευθύνσεις. Ωστόσο, η εκχώρηση μιας αποκλειστικής δημόσιας διεύθυνσης σε κάθε έναν από τους εσωτερικούς κεντρικούς υπολογιστές δεν είναι εφικτή επιλογή. Μπορείτε να επιλύσετε αυτή την πρόκληση ενεργοποιώντας τη λειτουργία Μετάφρασης διευθύνσεων δικτύου (Network Adress Translation NAT) στο firewall.

Οι όροι μετάφραση και μεταμφίεση αναφέρονται στην ίδια λειτουργία και είναι εναλλάξιμοι. Με άλλα λόγια, η μετάφραση μιας διεύθυνσης και η μεταμφίεση μιας διεύθυνσης αναφέρονται στην ίδια τεχνολογία NAT.

5.12.1 Βασικά στοιχεία NAT

Το NAT επιτρέπει στο firewall να μεταφράζει μια εσωτερική διεύθυνση IP σε μια διεύθυνση από ένα διαφορετικό υποδίκτυο. Η διαδικασία NAT είναι διαφανής τόσο για τους εσωτερικούς όσο και για τους εξωτερικούς υπολογιστές. Όταν το NAT είναι σε λειτουργία, ένας εσωτερικός κεντρικός υπολογιστής δεν γνωρίζει ότι η αρχική του διεύθυνση IP μεταφράζεται ή μεταμφιέζεται σε μια δημόσια διεύθυνση, ενώ ο εξωτερικός κεντρικός υπολογιστής θεωρεί ότι η δημόσια διεύθυνση είναι η πραγματική διεύθυνση του εσωτερικού κεντρικού υπολογιστή.

Ένα άλλο πλεονέκτημα του NAT είναι η δυνατότητα δρομολόγησης ιδιωτικής κυκλοφορίας στο Διαδίκτυο. Οι εσωτερικοί κεντρικοί υπολογιστές ενός οργανισμού χρησιμοποιούν ιδιωτικές διευθύνσεις IP για εσωτερική επικοινωνία, όπως ορίζεται στο RFC 1918 . Οι ιδιωτικές διευθύνσεις IP δεν μπορούν να δρομολογηθούν στο Διαδίκτυο, εκτός αν τις αντιστοιχίσετε ή τις μεταφράσετε σε δημόσιες διευθύνσεις. Στην πραγματικότητα, αυτός ο «περιορισμός» του χώρου των ιδιωτικών διευθύνσεων επιτρέπει σε διαφορετικούς οργανισμούς να επαναχρησιμοποιούν τις ίδιες διευθύνσεις στα εσωτερικά τους δίκτυα και να τις διατηρούν ανεξάρτητα από τυχόν αλλαγές στη δημόσια διεύθυνση IP. Έτσι, διατηρείται η χρήση των δημόσιων διευθύνσεων IP. Η Αρχή Εκχώρησης Αριθμών Διαδικτύου (Internet Assigned Numbers Authority IANA) διατηρεί επιπλέον μη δρομολογήσιμες διευθύνσεις IP που μπορείτε να χρησιμοποιήσετε σε ένα δοκιμαστικό δίκτυο και στην τεκμηρίωση που περιγράφονται στο RFC 5737.

5.12.2 Τεχνικές NAT

Το NAT σας επιτρέπει να μεταμφιέσετε διευθύνσεις IP σε διάφορα σενάρια, όπως ένα προς ένα, ένα προς πολλά, πολλά προς ένα, πολλά προς πολλά, λίγα προς πολλά και πολλά προς λίγα. Ωστόσο, πριν ενεργοποιήσετε το NAT, πρέπει να απαντήσετε στις ακόλουθες ερωτήσεις:

- Πώς ένα firewall επιλέγει μια μεταμφιεσμένη ή μεταφρασμένη διεύθυνση; Είναι προκαθορισμένη στατικά ή κατανέμεται δυναμικά;

- Πόσες εξωτερικές ή δημόσιες διευθύνσεις είναι διαθέσιμες για επιλογή; Μία ή περισσότερες;

Οι απαντήσεις σας σε αυτά τα ερωτήματα μπορούν να σας βοηθήσουν να καθορίσετε τους τύπους μεταφράσεων που πρέπει να ενεργοποιήσετε. Μπορείτε να κατηγοριοποιήσετε το NAT κυρίως σε τρεις τύπους:

> **Στατικό NAT:** Ένα firewall αντιστοιχίζει μόνιμα την αρχική διεύθυνση IP με μια μεταφρασμένη διεύθυνση IP. Επειδή η αντιστοίχιση είναι μόνιμη, είτε ο εσωτερικός είτε ένας εξωτερικός κεντρικός υπολογιστής είναι σε θέση να ξεκινήσει μια σύνδεση.

> **Δυναμικό NAT:** Αντί για μόνιμη αντιστοίχιση, το firewall επιλέγει μια διεύθυνση IP από μια προκαθορισμένη δεξαμενή διευθύνσεων και μεταφράζει μια αρχική εσωτερική διεύθυνση στην επιλεγμένη διεύθυνση IP. Η επιλογή μιας διεύθυνσης γίνεται με σειρά προτεραιότητας.

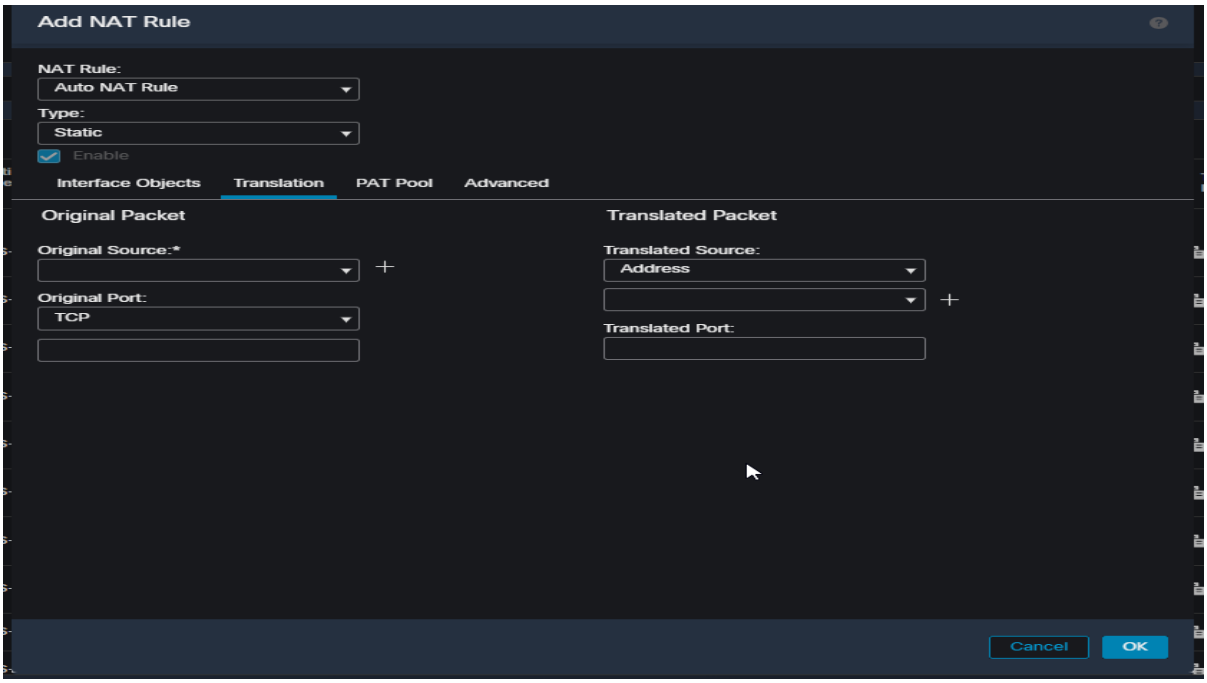
> **Μετάφραση διεύθυνσης θύρας (PAT):** Εάν μια δυναμική δεξαμενή διευθύνσεων έχει λιγότερες εξωτερικές διευθύνσεις από ό,τι εσωτερικούς κεντρικούς υπολογιστές, είναι αδύνατο για όλους τους εσωτερικούς κεντρικούς υπολογιστές να συνδεθούν ταυτόχρονα σε εξωτερικά δίκτυα. Για να αντιμετωπιστεί αυτό το ζήτημα, το firewall μπορεί να μεταφράσει τόσο τη διεύθυνση IP όσο και τον αριθμό θύρας μιας σύνδεσης (σε αντίθεση με τη διεύθυνση IP μόνο) και μπορεί να πολλαπλασιάσει πάνω από 65.000 συνδέσεις σε μία μόνο διεύθυνση IP. Τα έγγραφα RFC περιγράφουν αυτό το χαρακτηριστικό ως Network Address and Port Translation (NAPT), αλλά λόγω της φύσης της λειτουργίας του, αυτό το χαρακτηριστικό είναι επίσης γνωστό ως Port Address Translation (PAT), NAT overload και IP masquerading.

Το firewall μπορεί να χρησιμοποιήσει τη διεύθυνση IP της διεπαφής εξόδου(egress interface) για τη λειτουργία PAT. Αυτό σημαίνει ότι όταν οποιοσδήποτε εσωτερικός υπολογιστής συνδέεται σε έναν πόρο μέσω του Διαδικτύου, η διεύθυνση IP προέλευσης της σύνδεσης εμφανίζεται ως η διεπαφή εξόδου του firewall αντί της αρχικής διεύθυνσης του εσωτερικού υπολογιστή. Ωστόσο, εάν ο αριθμός των ταυτόχρονων συνδέσεων υπερβεί το όριό του, τυχόν πρόσθετοι κεντρικοί υπολογιστές δεν μπορούν να συνδεθούν στο εξωτερικό δίκτυο. Για να αντιμετωπίσετε αυτό το ζήτημα, μπορείτε να συνδυάσετε τη λειτουργία PAT με μια δυναμική δεξαμενή διευθύνσεων. Αυτό επιτρέπει στο firewall να επιλέγει μια νέα διεύθυνση IP από τη δεξαμενή όταν η πρώτη επιλογή από τη δεξαμενή δεν είναι πλέον διαθέσιμη για νέα σύνδεση.

5.12.3 Τύποι κανόνων NAT

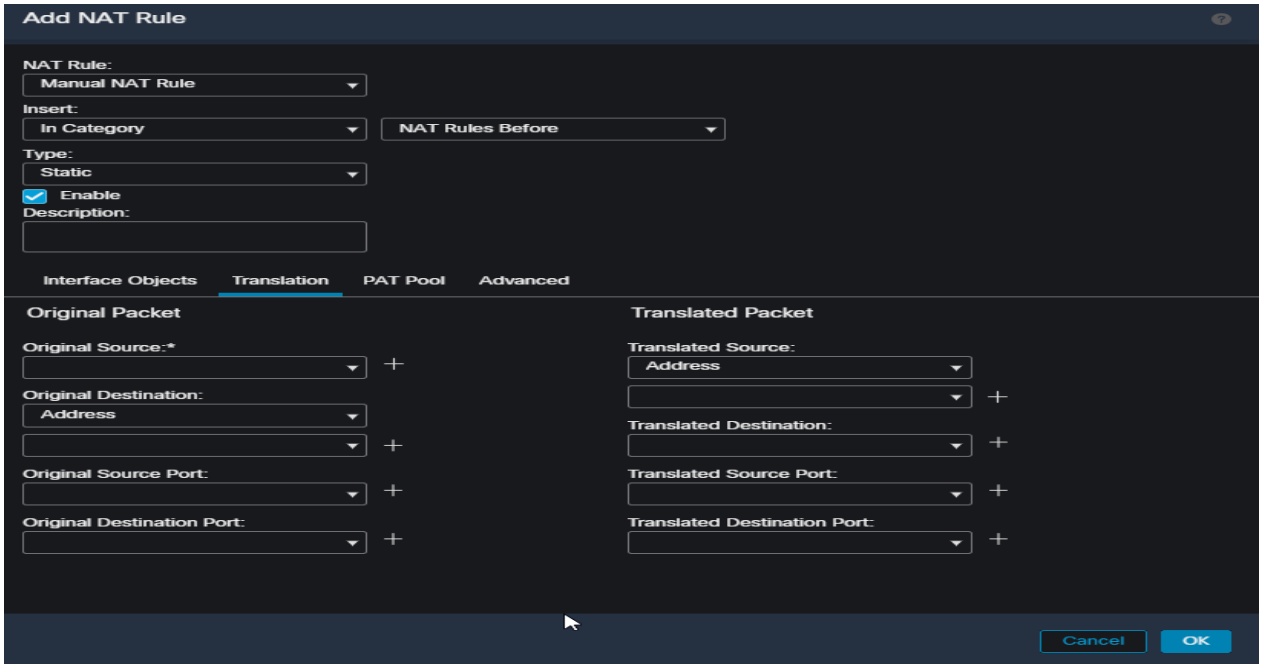
Το firewall προσφέρει δύο επιλογές για τη διαμόρφωση μιας συνθήκης κανόνα NAT:

Ένας κανόνας **Auto NAT** μπορεί να μεταφράσει μία διεύθυνση - είτε μια διεύθυνση πηγής είτε μια διεύθυνση προορισμού - σε έναν μόνο κανόνα. Αυτό σημαίνει ότι για τη μετάφραση τόσο της διεύθυνσης πηγής όσο και της διεύθυνσης προορισμού απαιτούνται δύο ξεχωριστοί κανόνες Auto NAT.



Εικόνα 5.32 Προσθήκη Auto-NAT rule

Manual Nat: Ένας κανόνας **Manual NAT** επιτρέπει τη μετάφραση τόσο των διευθύνσεων πηγής όσο και των διευθύνσεων προορισμού μέσα στον ίδιο κανόνα. Ένας κανόνας Manual NAT μπορεί να είναι απαραίτητος όταν θέλετε να κάνετε μια εξαίρεση για τη μετάφραση.



Εικόνα 5.33 Προσθήκη Manual NAT Rule

5.12.4 Βέλτιστες πρακτικές για το NAT

Βέλτιστες πρακτικές όταν σχεδιάζετε να ενεργοποιήσετε το NAT στο firewall:

> Η διαμόρφωση ενός κανόνα **Auto NAT** είναι απλούστερη από τη διαμόρφωση ενός κανόνα **Manual NAT**. Η Cisco συνιστά να επιλέξετε έναν κανόνα Auto NAT, επειδή μπορείτε εύκολα να υλοποιήσετε

τα περισσότερα από τα κοινά σενάρια NAT με αυτόν. Ένας χειροκίνητος κανόνας NAT μπορεί να είναι απαραίτητος όταν θέλετε να κάνετε μια εξαίρεση για τη μετάφραση.

> Εάν τροποποιήσετε έναν υπάρχοντα κανόνα NAT ή επανατοποθετήσετε μια νέα πολιτική NAT, ενδέχεται να διαπιστώσετε ότι η νέα πολιτική δεν τίθεται σε λειτουργία μέχρι να λήξουν οι υπάρχουσες συνδέσεις. Για να ενεργήσει το firewall με την τελευταία πολιτική NAT αμέσως, μπορείτε να διαγράψετε τις τρέχουσες μεταφράσεις εκτελώντας την εντολή **clear xlate** στην άμυνα απειλής.

> Όσο μεγαλύτερος είναι ο πίνακας μεταφράσεων, τόσο μεγαλύτερη είναι η επιβάρυνση επεξεργασίας. Εάν ο αριθμός των μεταφρασμένων συνδέσεων αυξηθεί υπερβολικά, μπορεί να επηρεάσει τη χρήση της CPU και της μνήμης του firewall.

> Για να βελτιώσετε την απόδοση, προτιμήστε το στατικό NAT από το δυναμικό NAT ή το PAT.

> Ελέγξτε προσεκτικά τις διευθύνσεις στους κανόνες δυναμικού και στατικού NAT πριν τους εφαρμόσετε. Αποφύγετε τη δημιουργία κανόνων με επικαλυπτόμενες διευθύνσεις IP.

5.12.5 Ρύθμιση του NAT

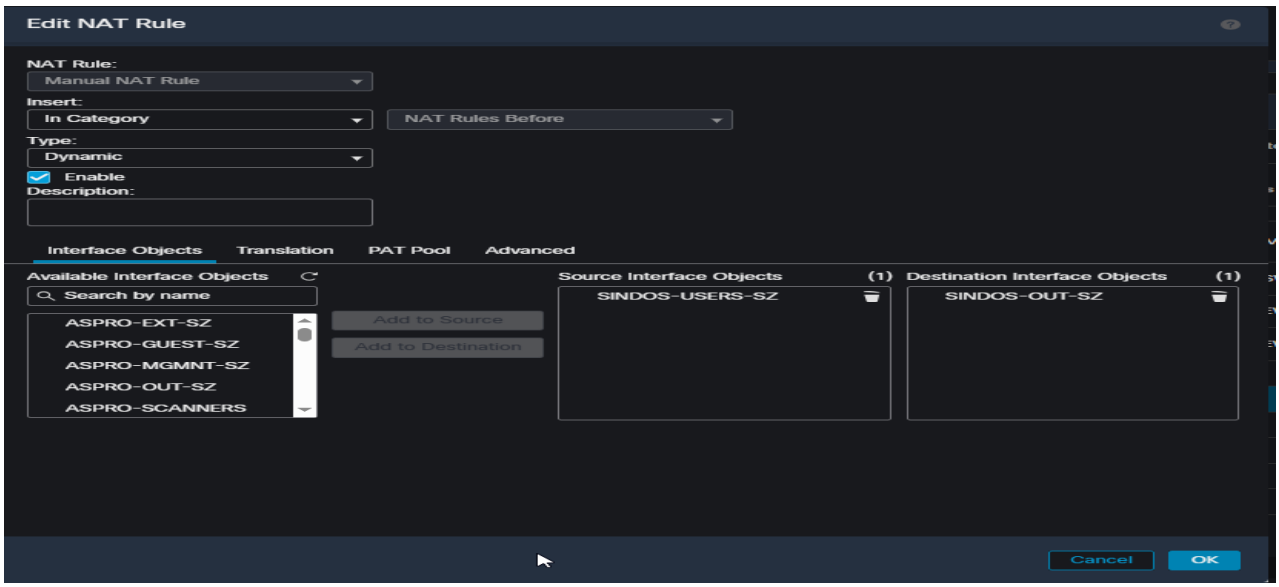
Το firewall σας δίνει τη δυνατότητα να πραγματοποιήσετε τη μετάφραση με διάφορους τρόπους. Μπορείτε να επιλέξετε οποιονδήποτε τύπο (στατικό έναντι δυναμικού) με οποιονδήποτε συνδυασμό κανόνα NAT (Αυτόματο έναντι χειροκίνητου).

> Μεταμφίεση μιας διεύθυνσης πηγής όταν ένας εσωτερικός κεντρικός υπολογιστής ξεκινά μια σύνδεση με έναν εξωτερικό διακομιστή

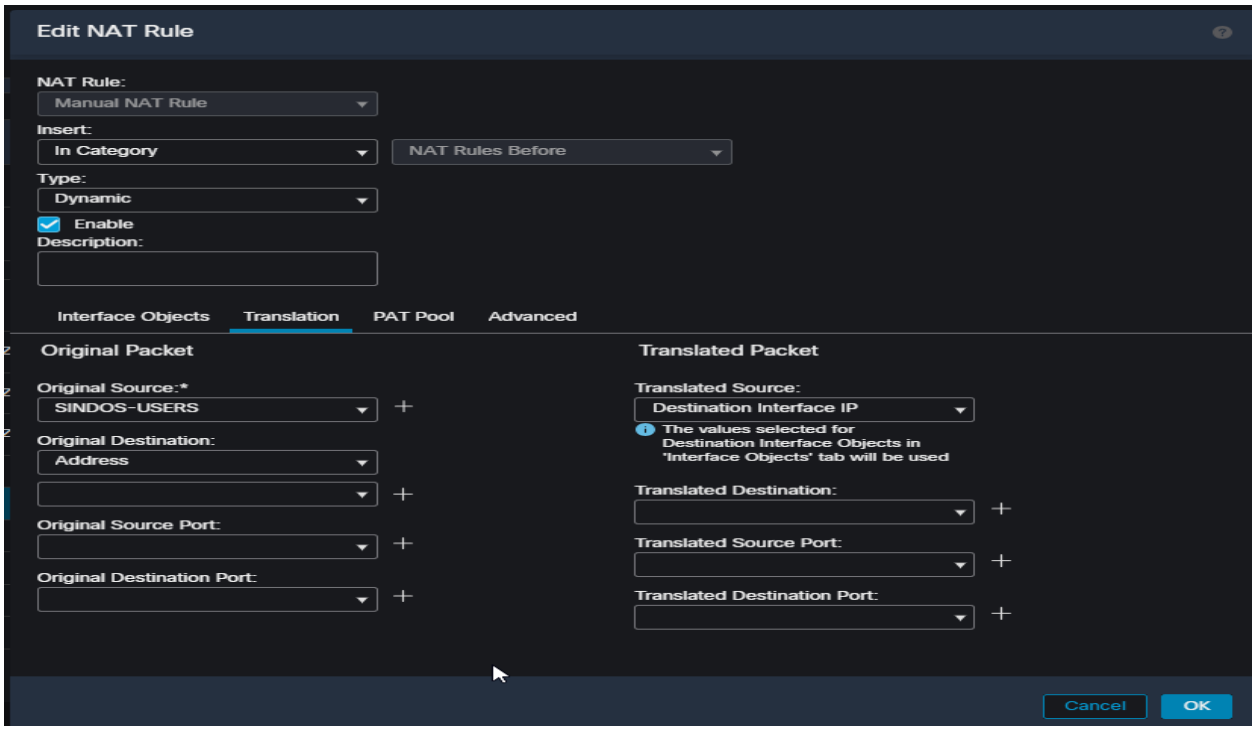
> Επιτρέποντας σε έναν εξωτερικό κεντρικό υπολογιστή να συνδεθεί σε έναν εσωτερικό κεντρικό υπολογιστή όταν ένας εξωτερικός κεντρικός υπολογιστής χρησιμοποιεί μια μεταμφιεσμένη διεύθυνση προορισμού

Μεταμφίεση μιας διεύθυνσης πηγής (Source NAT για εξερχόμενη σύνδεση)

Όταν ένας εσωτερικός κεντρικός υπολογιστής ξεκινά μια σύνδεση στο Internet, το firewall μπορεί να μεταφράσει την εσωτερική διεύθυνση IP σε μια δημόσια διεύθυνση IP. Πιο συγκεκριμένα για τα δίκτυα μας επιθυμούμε οι χρήστες να έχουν πρόσβαση στο Ίντερνετ οπότε θα κάνουμε τον εξής κανόνα:



Εικόνα 5.34 Καθορισμός των Security Zones που ανήκουν τα interfaces



Εικόνα 5.35 Καθορισμός αρχικού πακέτου και της μετάφρασης του για το manual NAT

Ο κανόνας αυτός περιγράφει την εξής διαδικασία

Μετάφρασε την κίνηση που καταφθάνει από το δίκτυο των χρηστών της Σίνδου στην διεύθυνση που έχει το interface του firewall(outside).

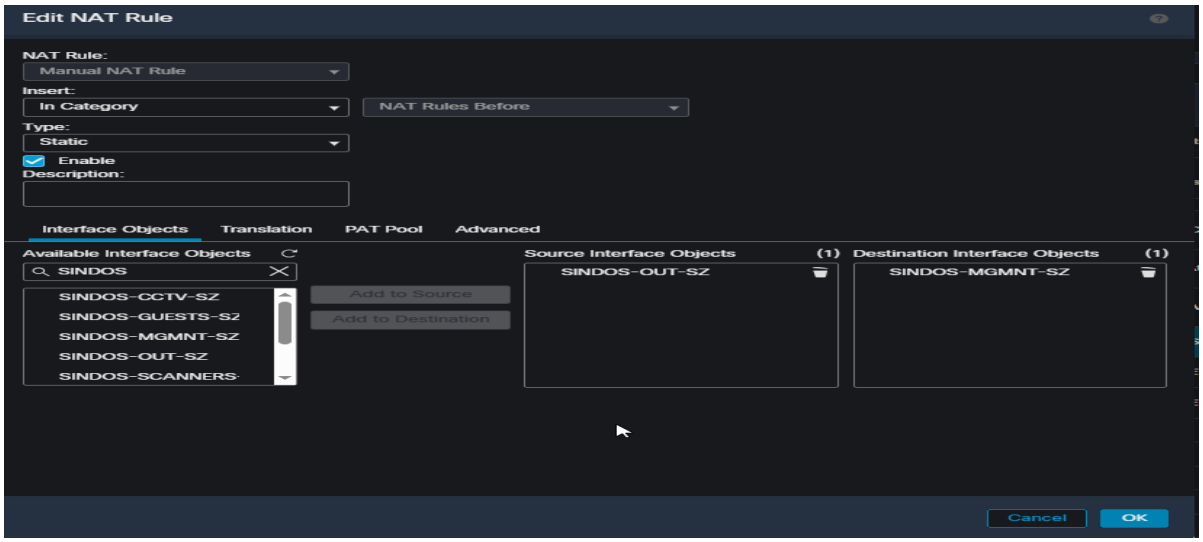
Η μεταγωγή της κίνησης θα έχει την εξής κατεύθυνση, ξεκινάει από το security zone του εσωτερικού δικτύου(SINDOS-USERS-SZ) και καταλήγει στο security zone SINDOS-OUT-SZ στο οποίο ανήκει και το outside interface(Ethernet 1/1).

Σύνδεση σε έναν προορισμό ο οποίος έχει μεταφραστεί (Destination NAT για εισερχόμενη σύνδεση)

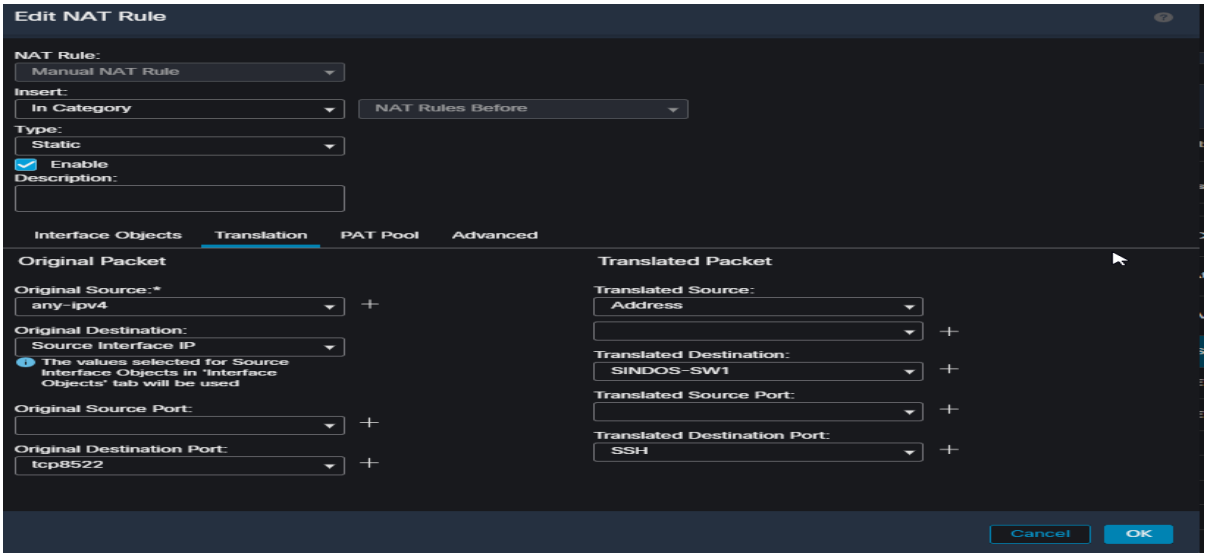
Αν εξωτερικοί υπολογιστές θέλουν να έχουν πρόσβαση σε οποιεσδήποτε υπηρεσίες της εταιρείας σας, θα πρέπει να έχουν πρόσβαση μέσω της δημόσιας διεύθυνσης IP του οργανισμού σας. Οποιοδήποτε σύστημα εσωτερικής διευθυνσιοδότησης πρέπει να είναι αόρατο για τους εξωτερικούς χρήστες.

Παρουσιάζεται το σενάριο όπου ένας εξωτερικός συνεργάτης θα θέλει να έχει πρόσβαση στο switch της εταιρείας μέσω του πρωτοκόλλου SSH για την απομακρυσμένη διαχείριση του.

Σε αυτήν την περίπτωση θα χρειαστούμε ένα στατικό NAT όπου θα μεταφράζει όλη την κίνηση που καταφθάνει στην δημόσια διεύθυνση IP και σε μια συγκεκριμένη θύρα(tcp 8522) στην εσωτερική ιδιωτική διεύθυνση που έχει το switch και στο πρωτόκολλο ssh(tcp 22).



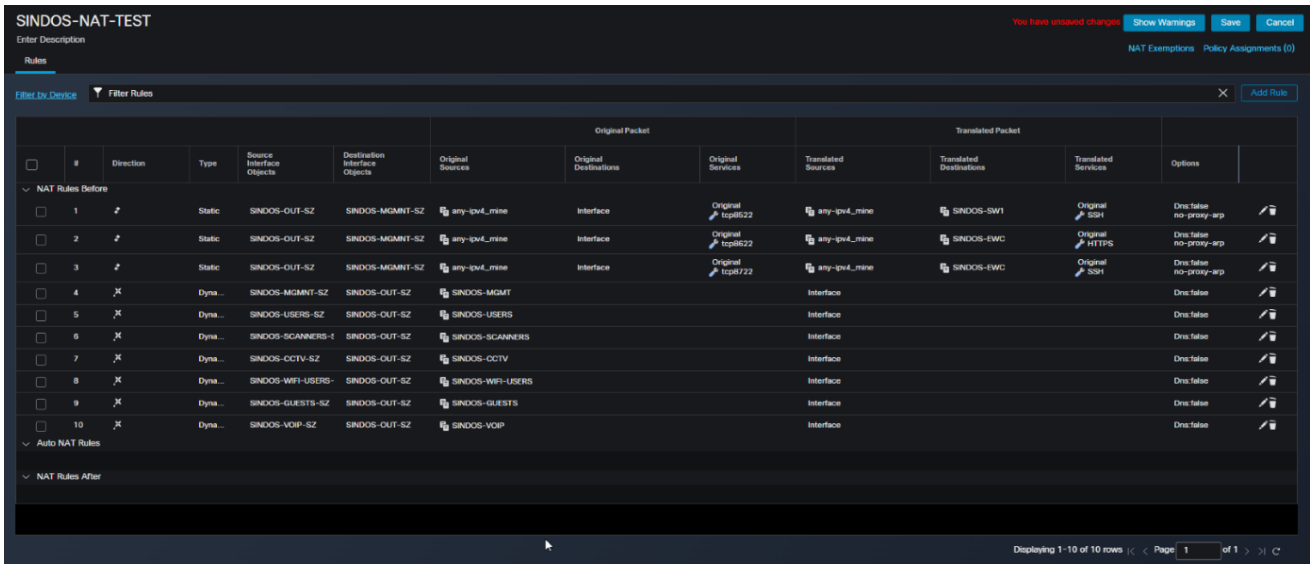
Εικόνα 5.36 Καθορισμός των Security Zones που ανήκουν τα interfaces



Εικόνα 5.37 Καθορισμός αρχικού πακέτου και της μετάφρασης του για το manual NAT

Η μεταγωγή της κίνησης αυτή την φορά θα έχει την εξής κατεύθυνση, θα φτάσει στο outside interface του firewall δηλαδή στην SINDOS-OUT security zone και θα κατευθυνθεί στο εσωτερικό δίκτυο δηλαδή προς την SINDOS-USERS security zone

Βάση των παραπάνω ολοκληρώνουμε την ρύθμιση NAT και για τα υπόλοιπα δίκτυα.



Εικόνα 5.38 Συγκεντρωτικά, οι ρυθμίσεις NAT για το firewall.

5.12.6 Επίλογος

Ολοκληρώνοντας το κεφάλαιο έχει γίνει ανάλυση των βασικών λειτουργιών ενός firewall και ρύθμιση του με τους απαραίτητους κανόνες και πολιτικές ασφαλείας, ενώ έχουμε εξασφαλίσει την πρόσβαση στο Internet για τους υπολογιστές του δικτύου μας με την ρύθμιση του NAT.

Κεφάλαιο 6ο: Συμπεράσματα ή/και προτάσεις βελτίωσης

Αναλύθηκαν τα βασικά πρωτόκολλα που χρησιμοποιούνται για την επικοινωνία των συσκευών ενός δικτύου και αναφέρθηκαν σημαντικές λειτουργίες όπως DHCP, DNS ,ACP και ping. Εξετάστηκε η παραμετροποίηση εταιρικών switches όσον αφορά την διαχείριση τους και την μεταγωγή της κίνησης μεταξύ των επιμέρους δικτύων καθώς και η διαμόρφωση ενός next generation firewall στο οποίο διαμορφώθηκαν πολιτικές ασφαλείας και κανόνες συνδεσιμότητας στο Internet για τους εταιρικούς χρήστες. Εν κατακλείδι, η πρόσβαση στο Internet αποτελείται από πολλά επιμέρους τμήματα όπως σωστή παραμετροποίηση vlans στον μεταγωγέα, ορθή διαμόρφωση πολιτικών ασφαλείας στο firewall και άλλα, τα οποία οφείλουν να λειτουργούν αρμονικά για να εξασφαλίσουμε την απρόσκοπτη και ασφαλής σύνδεση.

Βιβλιογραφία

[1] «About RFCs» [Online].
Available: https://www.ietf.org/process/rfcs/.

[2] «Transmission Control Protocol» [Online].
Available: https://www.ietf.org/rfc/rfc793.txt.

[3] «Data Encapsulation and the TCP/IP Protocol Stack» [Online].
Available: https://docs.oracle.com/cd/E19455-01/806-0916/ipov-32/index.html.

[4] «802.3-IEEE Standard for Ethernet» [Online].
Available: https://ieeexplore.ieee.org/document/9844436.

[5] « IANA Considerations and IETF Protocol and Documentation Usage for IEEE 802
meters» [Online]. Available: https://datatracker.ietf.org/doc/html/rfc7042.

[6] « Requirements for IP Version 4 Routers» [Online].
Available: https://datatracker.ietf.org/doc/html/rfc1812.

[7] « DNS Terminology» [Online].
Available: https://www.rfc-editor.org/rfc/rfc9499.

[8] « An Ethernet Address Resolution Protocol,» [Online].
Available: https://datatracker.ietf.org/doc/html/rfc826.

[9] « Internet Control Message Protocol» [Online].
Available: https://datatracker.ietf.org/doc/html/rfc792.

[10] «Cisco Catalyst 1000 Series Switches Data Sheet » [Online].
Available: https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-1000-series-switches
/nb-06-cat1k-ser-switch-ds-cte-en.html.

[11] «Configuring the Switch »[Online].
Available: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst1000/hardware/installation
/8_16_port_hig/b_c1000_8_16_hig/configuring_the_switch.html.

[12] « Difference between network-based and host-based firewalls» [Online].
Available: https://community.fortinet.com/t5/FortiGate
/Technical-Tip-Difference-between-network-based-and-host-based/ta-p/378866.

[13] « Transmission Control Protocol » [Online]. Available: https://www.rfc-editor.org/rfc/rfc793.html.

[14] «Configure and Operate FTD Prefilter Policies» [Online].
Available: https://www.cisco.com/c/en/us/support/docs/security
/firepower-management-center/212700-configuration-and-operation-of-ftd-prefi.html.

[15] « What Is a Network Firewall?» [Online].
Available: https://www.paloaltonetworks.com/cyberpedia/what-is-a-network-firewall.