

May 22, 2021

eitan danon

see security

Yaki ben-nisan

ccsa-22.5.2021

final project

Content

***PART1***

Intro------------------------------------------------------------------------------------------------------2-3

Gaia installation ------------------------------------------------------------------------------------4-8

Firewall installation--------------------------------------------------------------------------------9-14

Browsing role --------------------------------------------------------------------------------------15-16

Second firewall installation-------------------------------------------------------------------17-20

VPN---------------------------------------------------------------------------------------------------21-25

Domain controller ------------------------------------------------------------------------------26-31

***PART2***

HTTPS inspection------------------------------------------------------------------------32-33

Identity awareness---------------------------------------------------------------------34-38

User identity check--------------------------------------------------------------------39-40

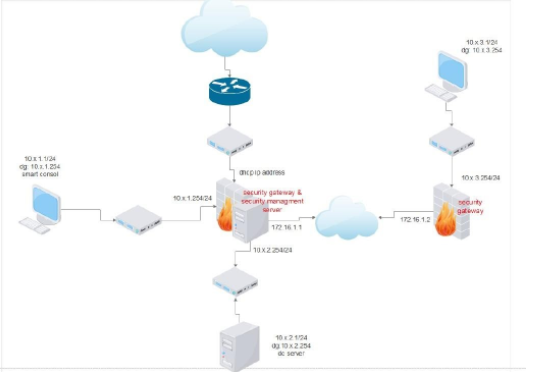
Media access--------------------------------------------------------------------------------41

Contact awareness ------------------------------------------------------------------42-43

Social media company terms --------------------------------------------------------44

ISP------------------------------------------------------------------------------------------------------45-47

**Part A – build domain topology**

**intro**

before I start explain how to build this topology, we need to understand the basic information about the system.

What is checkpoint and for what is used?

What is r80.40?

Where checkpoint product – R80 is used?

**\*Check Point** is an American-Israeli multinational provider of software and combined hardware and software products for It security.

**\*R80**.**40** Smart Console is an integrated security management solution which includes policy, logging, monitoring, event correlation and reporting – all in a single system which enables administrators to easily identify security risks across the organization

**\*Gaia** is the Check Point next generation operating system for security applications. ... The Gaia Operating System supports the full portfolio of Check Point Software Blades, Gateway and Security Management products.

**topology**

After we understand the system, we are going to work with ill explain about the topology we are going to use.

We are going to build network with 3 end devices in different Ip networks and.

**First network 10.1.1.0\24 (lan1):**

windows end device that is going to use as management pc that is connected to the Gaia operation system and to the domain controller, we are going to build

**second network 10.1.2.0\24 (lan2):**

server end device that is going to use as domain controller, webserver, DNS protocol server to our windows end devices

**third network bridge (DHCP):**

the bridge is going to path the network from the Gaia to the internet, in that way we will be able to use the internet in all the devices by our needs, after we setup few rules and protocols

**fourth network 172.16.1.0\24(connection-LAN):**

this Ip network is going to be our connection between the firewalls so the end devices will be able to contact

**fifth network 10.1.3.0\24 (lan3):**

this Ip network is for the windows we are going to join to the domain we will create from, pay attention that this network doesn’t have has connection to the domain controller or to the other windows, we will create a path with few rules and protocols that are going to help us connect it with the other devices

**part 1 install R80 product**

for our examples we are going to use VMware program.

**Create the machine:**

On VM – go to file -> new virtual machine -> costume



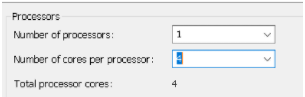
--------------------------------------------------------------------------------------------------------

Then select the operation system

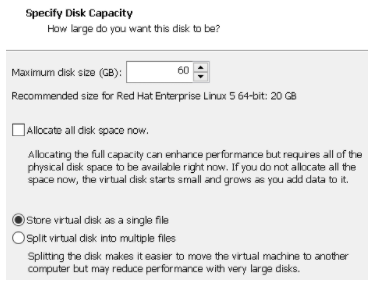


--------------------------------------------------------------------------------------------------------

Select the location of the install and name the machine, choose number of processors.



--------------------------------------------------------------------------------------------------------

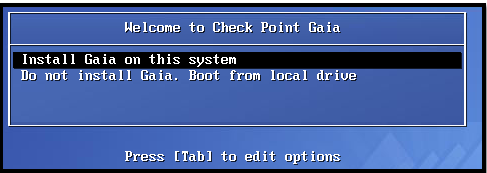
Now give the space of the hard drive and of the ram and press 4 time next.

After we created the machine, we will go to network adapter in the settings and change it from NAT to VMNET 9

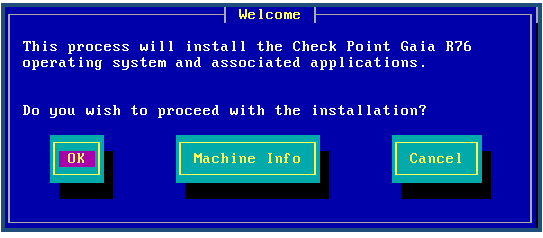
--------------------------------------------------------------------------------------------------------

***Install of Gaia:***

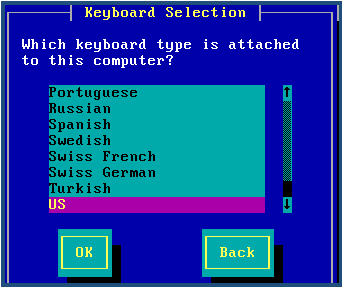
Power on the devise and install the system from the disk drive:

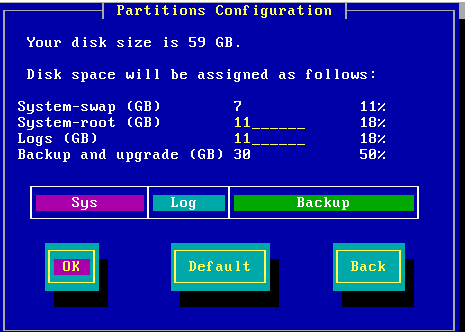


-------------------------------------------------------------------------------------------------------

Accept the beginning of the install:

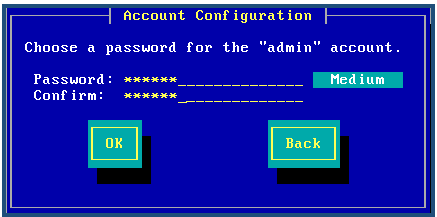
--------------------------------------------------------------------------------------------------------

Chose the keyboard language:

Split to parts the hard drive:

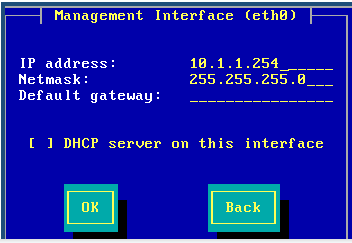
--------------------------------------------------------------------------------------------------------

Create a password to the admin account (vpn123):

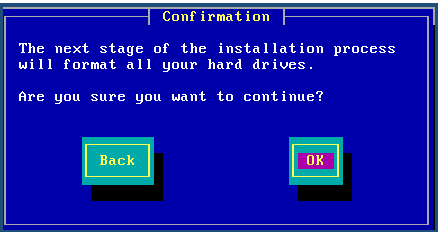


--------------------------------------------------------------------------------------------------------

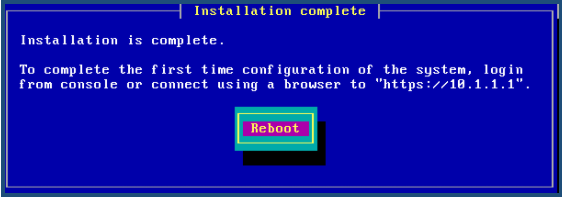
Setup a network:



Accept the delete of the hard drive and installation of the Gaia

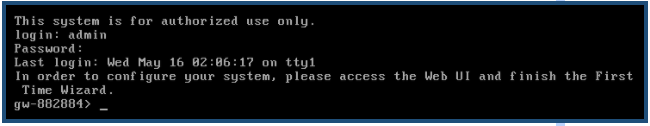


--------------------------------------------------------------------------------------------------------

Accept the restart and enter to the server from browser on another pc with https:// Ip address – (10.1.1.254) 

------------------------------------------------------------------------------------------------------

When you connected to the system with admin – vpn123 you will get massage that we need to install the Gaia from the browser



------------------------------------------------------------------------------------------------------

We will be able to turn off the Gaia system by using command (halt)

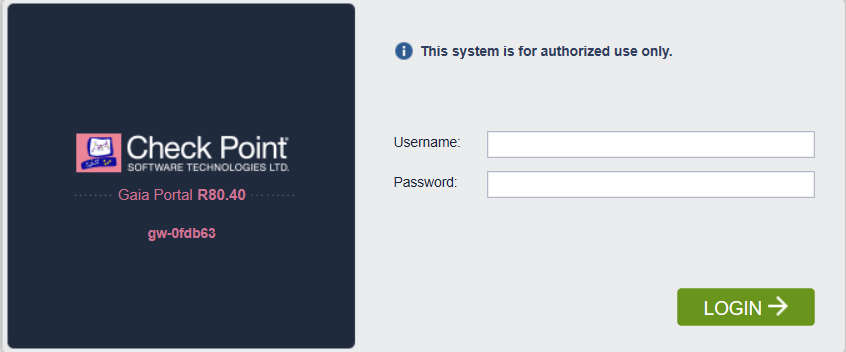
And after we turn of the system we will go to the setting and add 2 network adapters (VMNET7, bridged, VMNET5)

**VMNET7** is going to be 10.1.2.0/24 – our domain controller network

**Bridge** is going to be our exit to the network

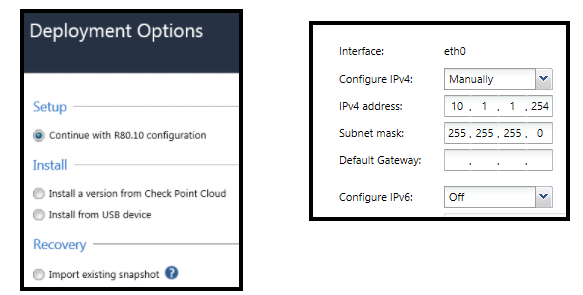
**VMNET5:** is the connection between the firewalls

After we add those two turns on the Gaia and contact by the browser

The intro to the Gaia web is: 

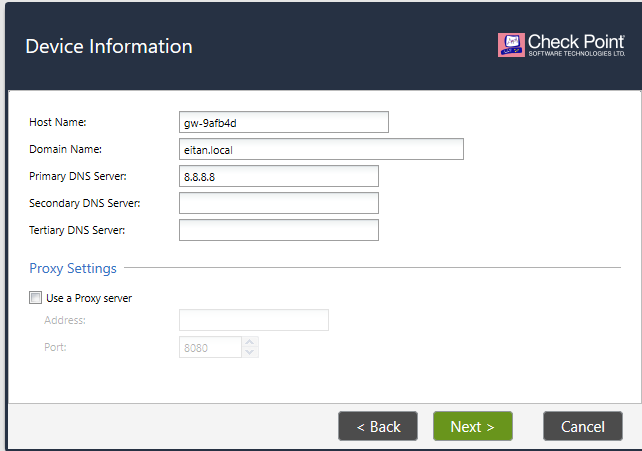
--------------------------------------------------------------------------------------------------------

Chose the operation system and the IPV4 address, setup only the VMNET9 IP

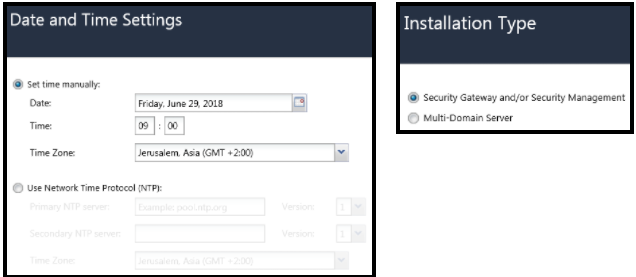


--------------------------------------------------------------------------------------------------------

Setup name to the server and setup the DNS Ip:

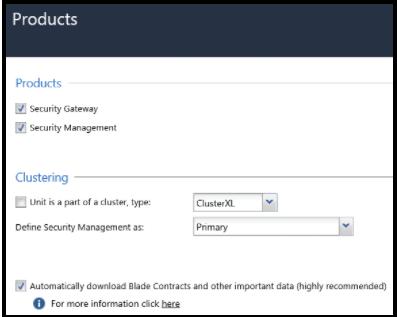


Set the NTP you chose and type of install



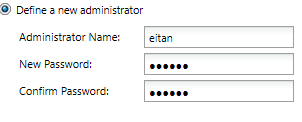
--------------------------------------------------------------------------------------------------------

Chose the type of product you want the install

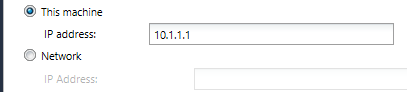


--------------------------------------------------------------------------------------------------------

Crate a user for the security management administrator:



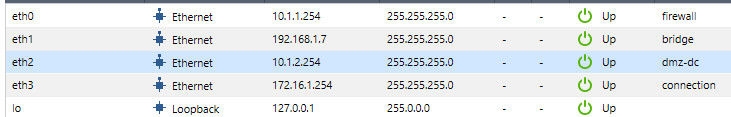
Select the machine you will be able to connect to the smart management:



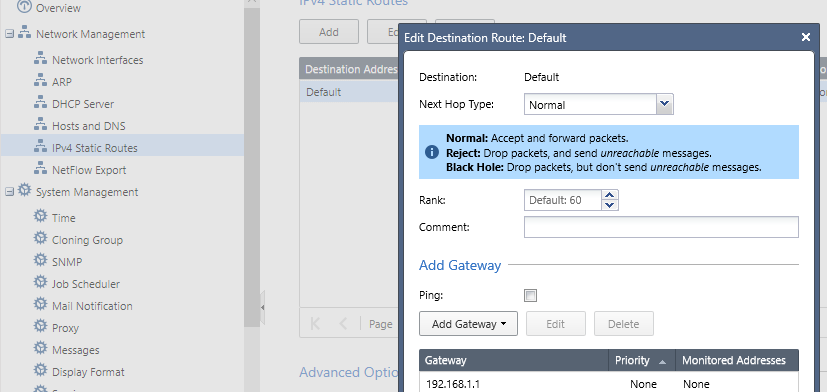
--------------------------------------------------------------------------------------------------------

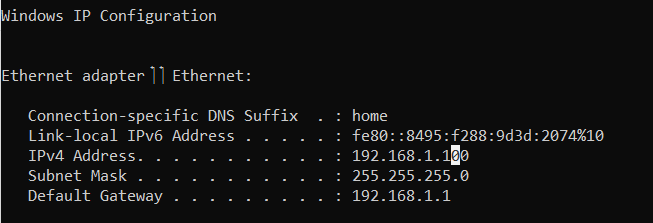
Accept the first part of the install.

Setup the interfaces by going to the network interface double click on the interface and start edit – to turn on we will put V on enable

One of the interfaces is the bridge so we can check by putting V on enable and IP address automatically

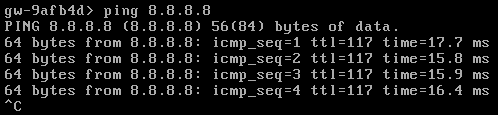
--------------------------------------------------------------------------------------------------------

Now go to the ipv4 static routs to setup the default getaway by double click on default -> add getaway

If you don’t know your D.G you can go to the CMD on your pc and use Ipconfig command

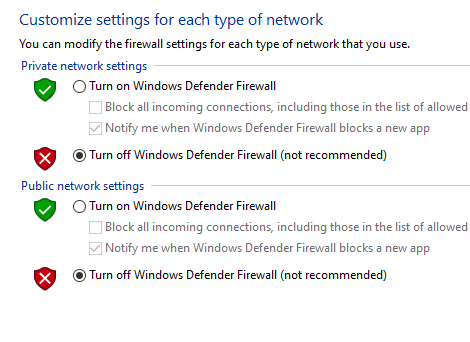
------------------------------------------------------------------------------------------------------

And like we can see my is 192.168.1.1, after we add the D.G we will go to the Gaia and check if we have Ping to 8.8.8.8 if we have, that mean we have exit to the internet

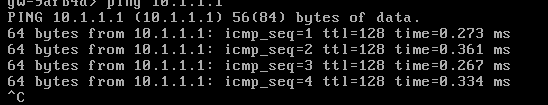


--------------------------------------------------------------------------------------------------------

Now if we want to get ping between the firewall and the win10 we need to go to the win10 and turn of the firewall settings



Only after we did that, we will be able to ping from the Gaia to the win10 – and from the win 10 to the Gaia



--------------------------------------------------------------------------------------------------------

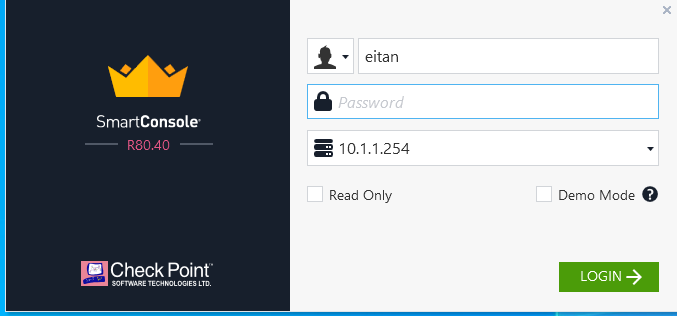
Now after we have internet on the Gaia we will go to the browser and check for updates. Status and action -> check for updates -> download and then install

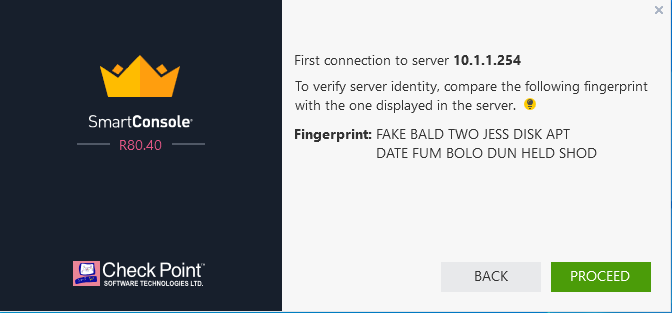
After we install the update, we will download the smart console



--------------------------------------------------------------------------------------------------------

Smart console is a program that allow as to connect the smart management, the login looks like that



After we enter with the user’s name, we created we will get warning with fingerprint text, that is for our safety from phishing attack

---------------------------------------------------------------------------------------------------

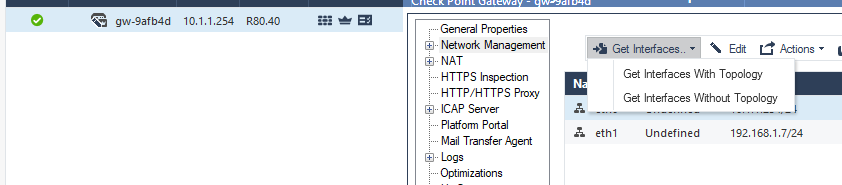
If we want to check what is our finger print, we will go to Gaia and use CPCONFIG command and then chose 8



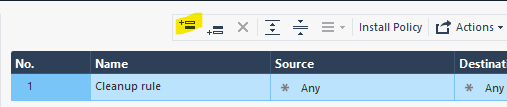
--------------------------------------------------------------------------------------------------------

Now after we enter the smart console, we need to get the topology of the interfaces by double click on the firewall(gw-9afb4d)-> network management-> get interfaces with topology-> yes-> accept/NAT -> put a V on hide internal network



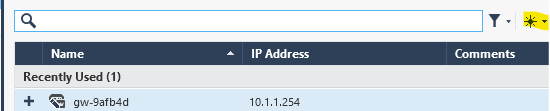


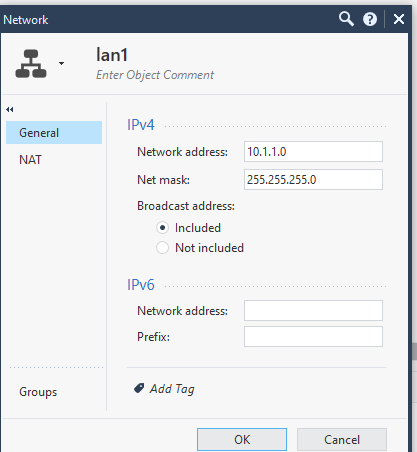
For example, of the smart console ill setup security policy that will let be brows from the win10 even if he is not connected directly to the internet. go to security policy ->add rule above



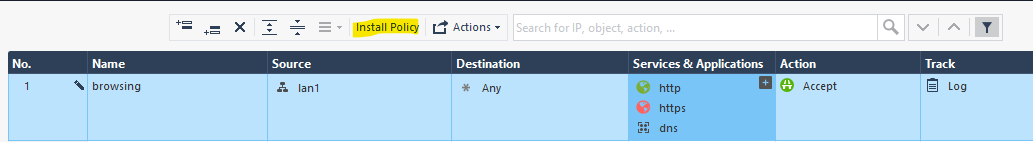
--------------------------------------------------------------------------------------------------------

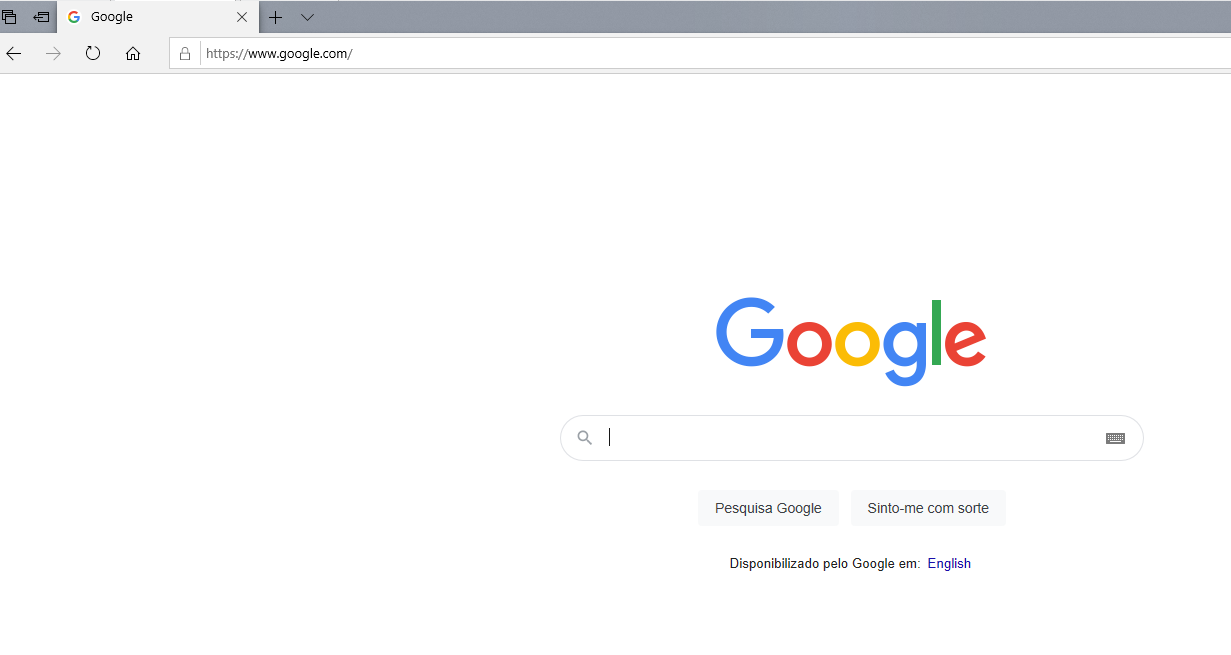
name-browsing-> source-> new-> network->name it lan1 -> 10.1.1.0/2





--------------------------------------------------------------------------------------------------------

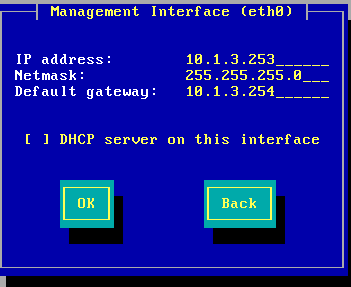
Destination-any -> services and application –(HTTP/HTTPS/DNS)-> accept->log-> install policy

And now let’s check if we have internet from the win10

--------------------------------------------------------------------------------------------------------

Now we need to add the FW2 (LAN2) to the smart management so we will have to control and to be able to add his pcs to our domain we will create.

First, we will install the firewall and give him the default getaway of the smart management because we want firewall 2 to have exit to the internet from our smart management.

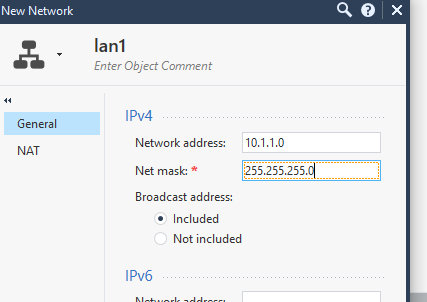


Like we see 10.1.3.254 is our smart management network IP and it is the default getaway because it’s our exit to the internet so FW2 will get 10.1.3.253 IP

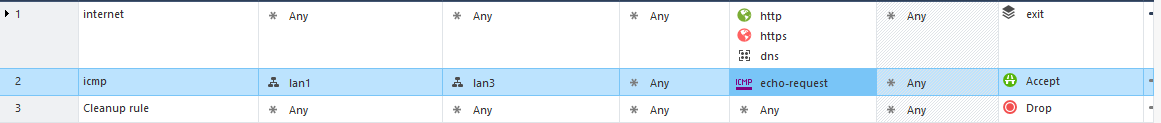
After we installed the Gaia, we need to install the fW2 but this time we will not choose smart management option but only security getaway option.

First, we need to allow PC from Lan 1 to communicate with FW2(LAN2) by adding rule ICMP in the smart management

1.create new network (LAN1, LAN3,)



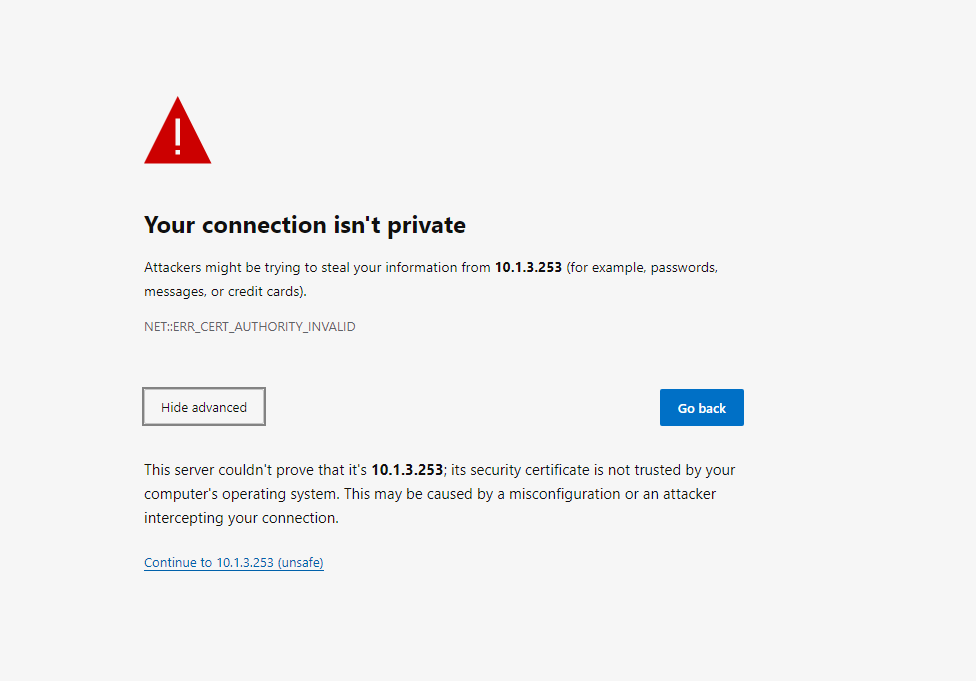
-----------------------------------------------------------------------------------------------

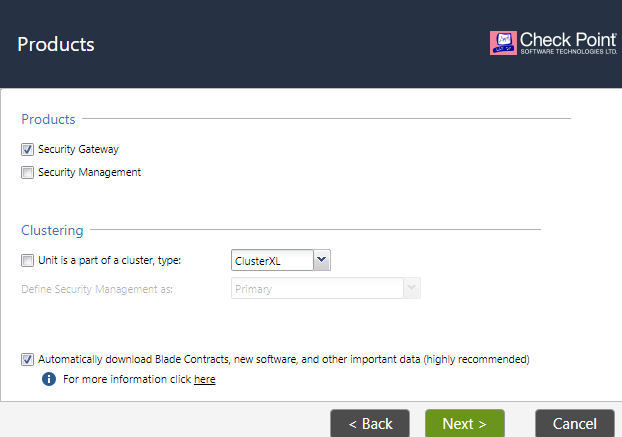
 Then create the rule ICMP

--------------------------------------------------------------------------------------------------------

Now we will try to enter the Gaia from the browser in the pc,

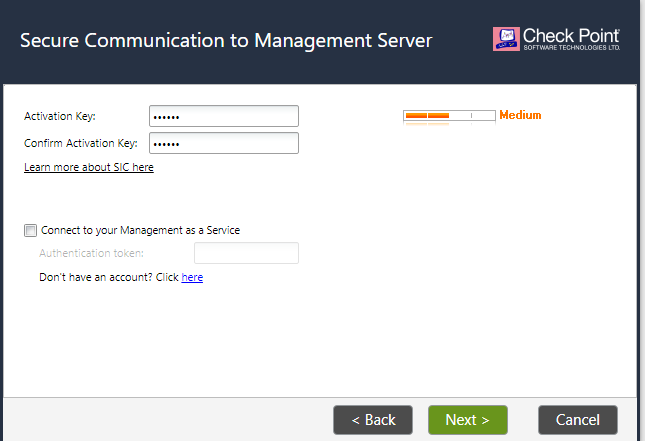
And we have connection between them, and we will start the setup

Uncheck the security management



--------------------------------------------------------------------------------------------------------

Create a key that we will use in the future



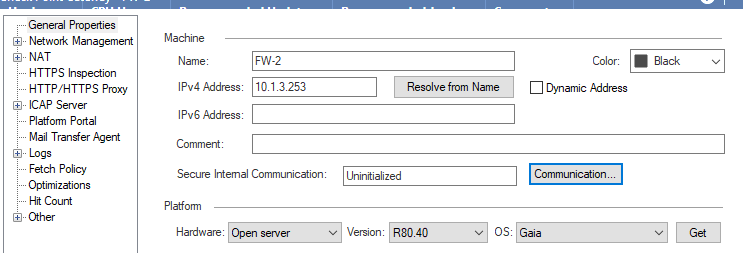
--------------------------------------------------------------------------------------------------------

And click next and finish to start the install.

After we install, we need to add the FW2(security default) to the smart management:

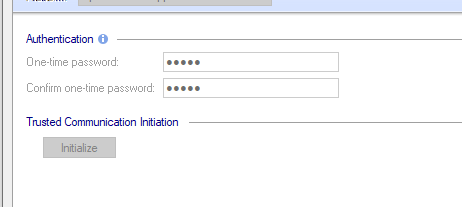


Press new🡪 more 🡪 network object 🡪 getaway and server 🡪 getaway



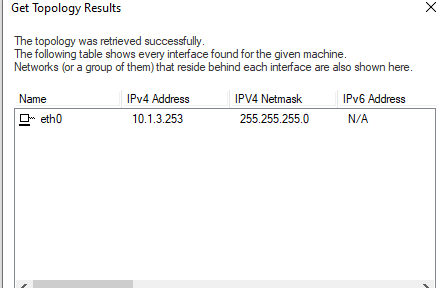
--------------------------------------------------------------------------------------------------------

Press communication and put the password we created and hit initialize

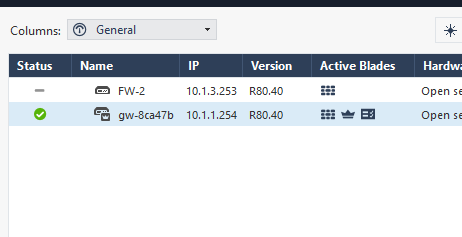


--------------------------------------------------------------------------------------------------------

Then will pop up window with topology press ok

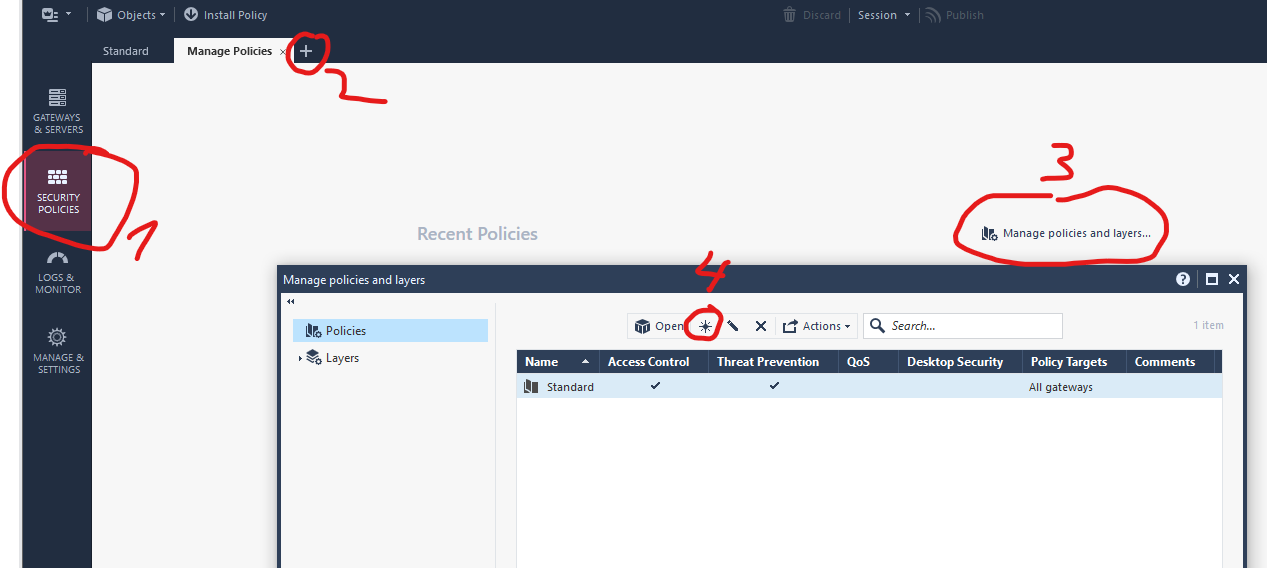


Now we see we created new FW in our smart management



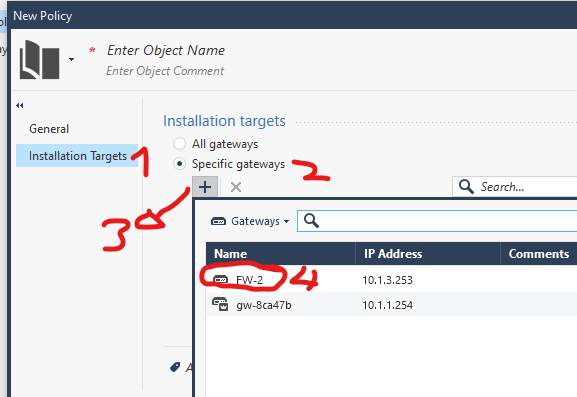
--------------------------------------------------------------------------------------------------------

So, to use SM more confutable we will edit it in a way that every getaway has his own rule page

Click security policy 🡪 + 🡪 manage 🡪 new 

-------------------------------------------------------------------------------------------------------

Target 🡪 specific 🡪 new 🡪 FW-2

And the same we do with the other FW so we will have better organize smart management.

VPN-virtual privet network

What is VPN:

VPN gives you online privacy and anonymity by creating a private network from a public internet connection

How does VPN work:

When you sign up with a VPN provider, you first log onto that service before you connect to the internet. Once you are connected, others can't see your activity. Your VPN provider will encrypt your data, scrambling it so that hackers, government agencies, and businesses can't see what websites you visit, messages you send, social media sites you use, or files you download.

What we are going to do now with VPN in this project:

In this project we have two end windows computers, those computers aren’t at the same LAN they are splatted to different LANs that every LAN has his own FW getaway,

LAN1-10.1.1.0:

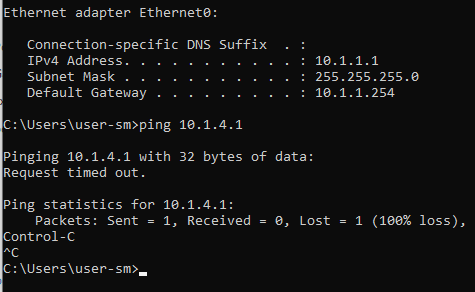
Has the main smart management FW that is the canter of the VPN we will create

LAN4- 10.1.4.0:

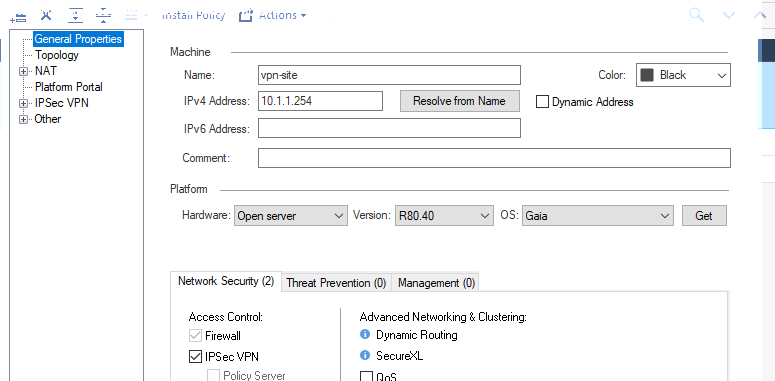
Has the second FW getaway that is connected to the smart management FW and we will provide with VPN the possibility to be able to ping to the windows at LAN1

So lets begin with the explain of the setup

Like we see here we don’t have ping from win1(10.1.1.1) to win2(10.1.4.1), so we need to setup the getaways to have VPN

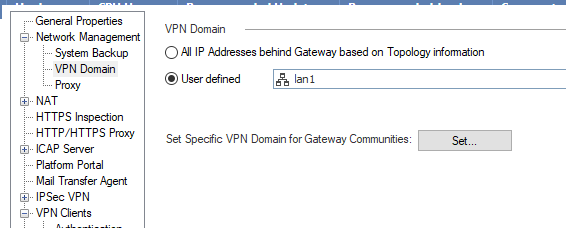


--------------------------------------------------------------------------------------------------------Now we will enter to the firewalls getaways in the smart management and select ISPec vpn in the network security

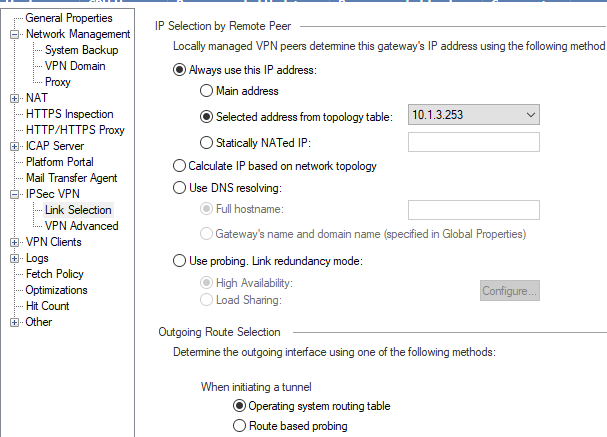


--------------------------------------------------------------------------------------------------------

Now we will go to network management 🡪 VPN domain and set the LAN each firewall belongs FW1=LAN1, FW2=LAN4

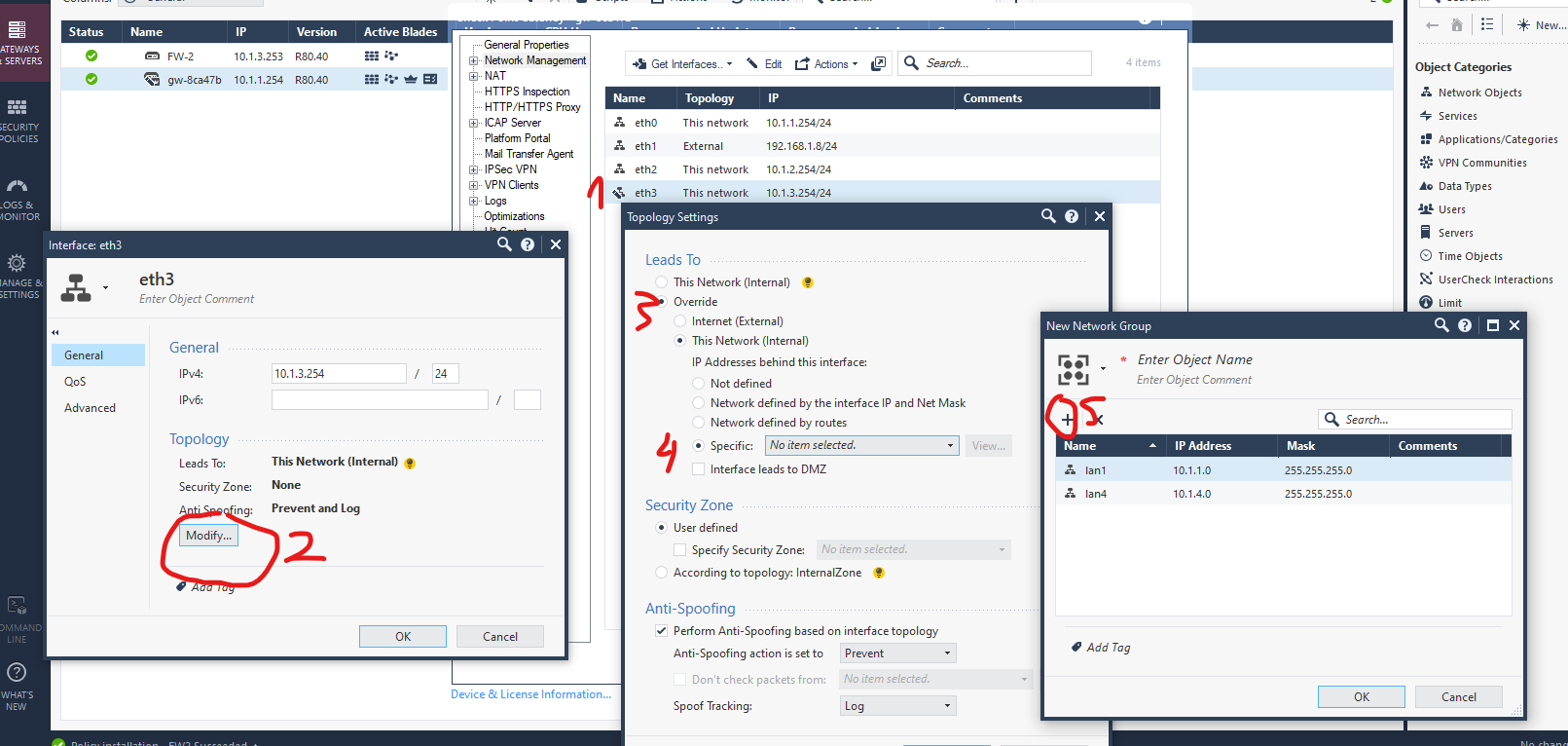


Then we go to link selection and select the address of the tunnel (interface) that connects between the FW

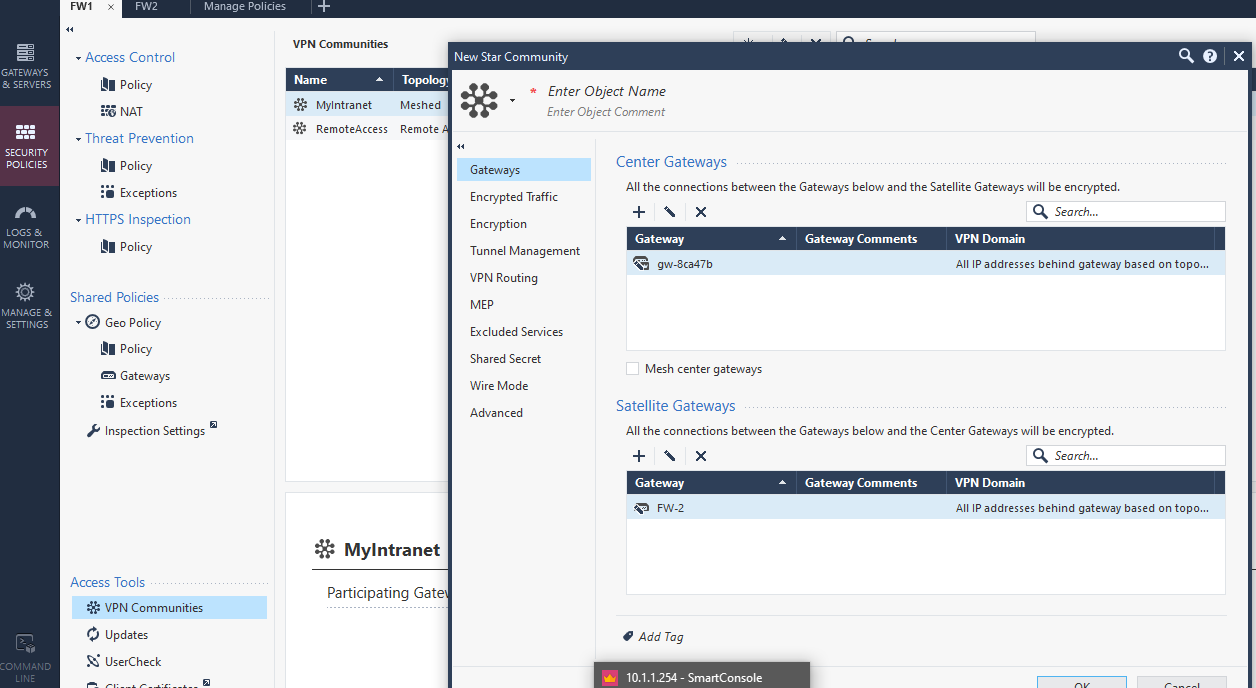


--------------------------------------------------------------------------------------------------------

Now we will enter the interface of the primary FW1 and in the tunnel interface we will choose specific LANs that we will want to have access to the VPN

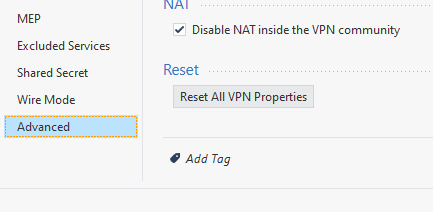


Now we will go to VPN communities in security polices and create new community

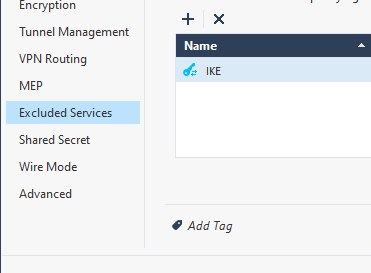


-------------------------------------------------------------------------------------------------------

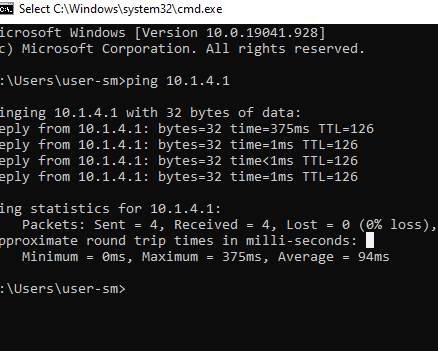
Then we go to advance and select disable NAT



--------------------------------------------------------------------------------------------------------And now we will select key for encryption that will secure the data transfer in the network



After all we will install all the policies and the settings we will check if we have ping so we will see if the VPN connection succeeded



---------------------------------------------------------------------------------------------------

Like we see we have ping between win1(LAN1) and win2(LAN2)



And here we can see the encryption between the windows and this is how we created a VPN communication

*Connecting to the domain*

What is network domain:

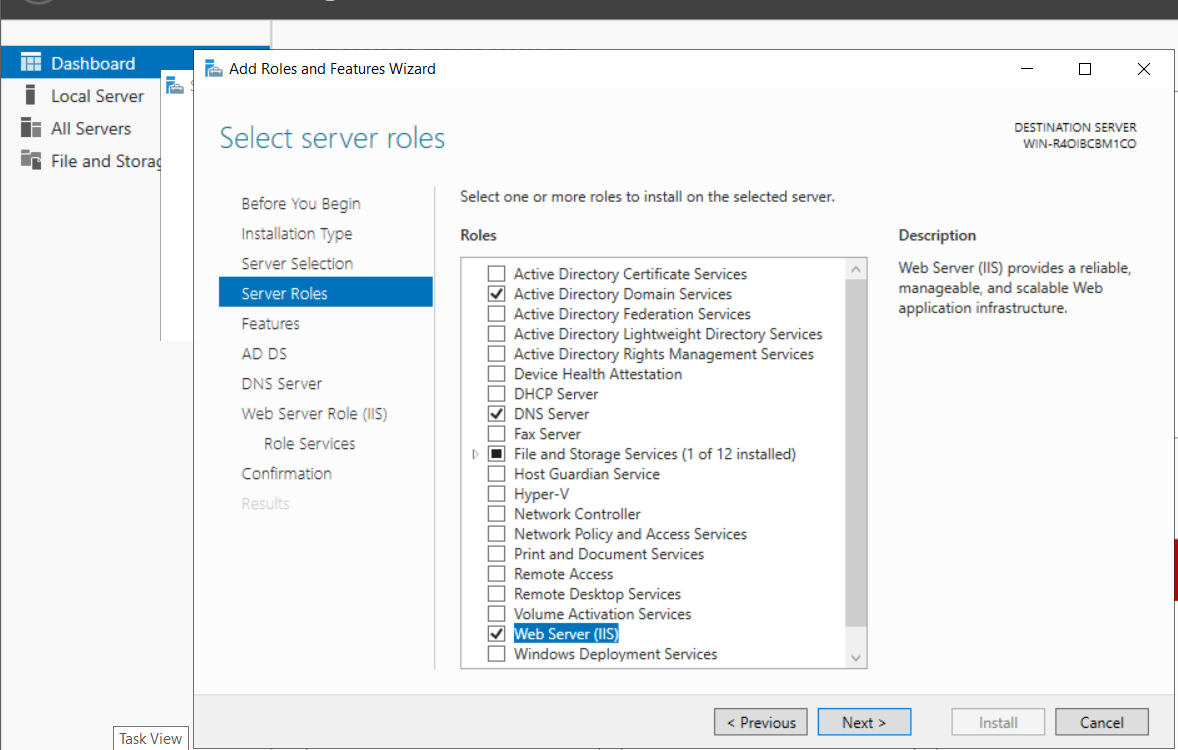
A network domain is an administrative grouping of multiple private computer networks or hosts within the same infrastructure.

 Domains can be identified using a domain name; domains which need to be accessible from the public Internet can be assigned a globally unique name within the Domain Name System (DNS).

The domain helps us to get more control in our network and to give every computer different privilege and rules, give us the opportunity to see what every computer does.

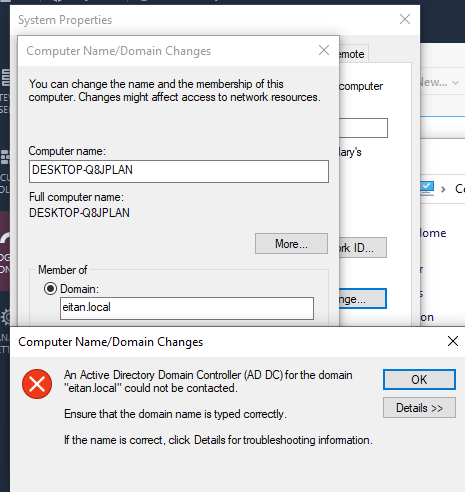
In this project ill show how to join windows end devices from different network to our domain we created with our web server

First go to the server and install those rolls

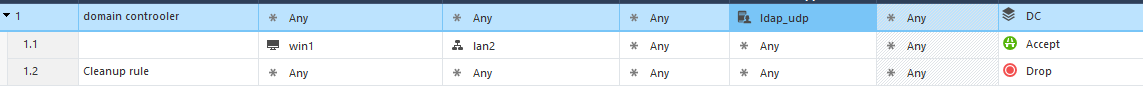


After we install those rolls, we will go to one of the windows and try to connect it to our domain and see in the log what is the drop error and, in that way, we will be able to see what port are missing and add them to the rules in the smart management.

Now ill try to join our domain eitan.local and see what is happening

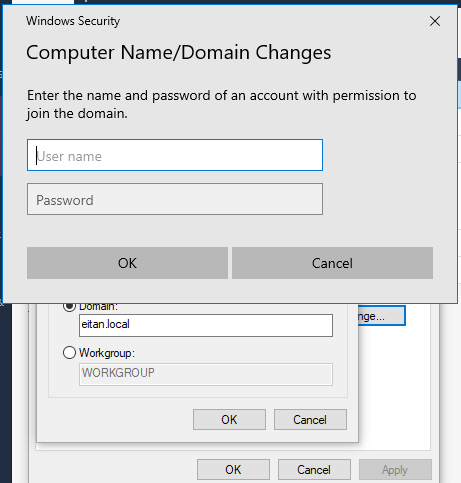


Now after I had error we will go to the log and see what is blocking the connection.

Now after we saw that we are missing LDAP\_UDP rule we will add it to our rule list and try again to join the domain

Here we can see I add the role and install it and now we will try to join

Here we can see it let me to put the user and password but it isn’t going to let me join and we will se in the log why

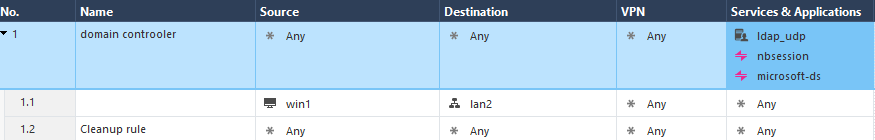


--------------------------------------------------------------------------------------------------------

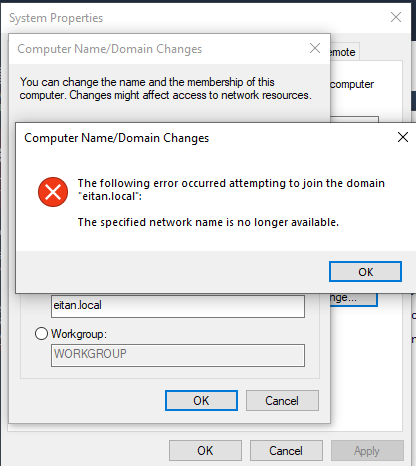
Like we see here those are the rules are missing to try join the domain so we will add them to the rule list and try join again to the domain

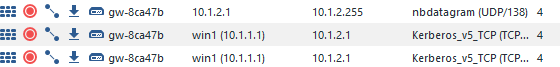


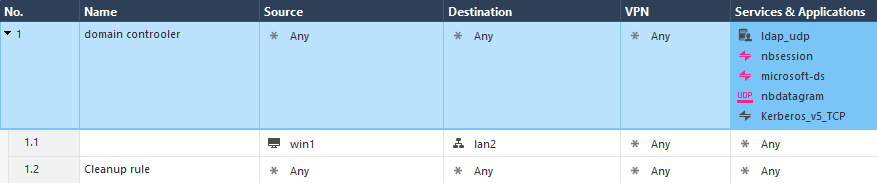
--------------------------------------------------------------------------------------------------------

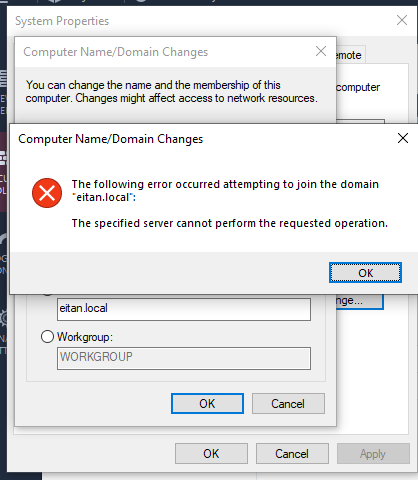
Here I add the rules

Like we see it is still something blocking, so we will go to the log and see what is missing at the rules table



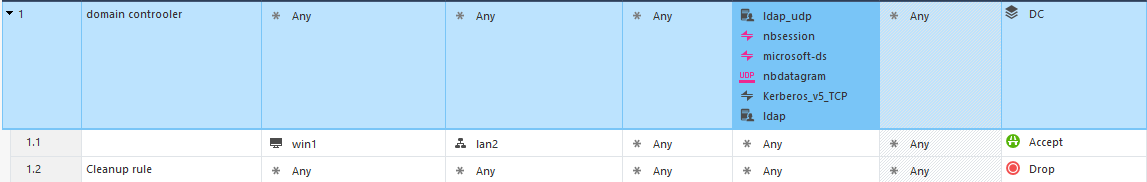
so those are the rules are missing we will add them and then try again



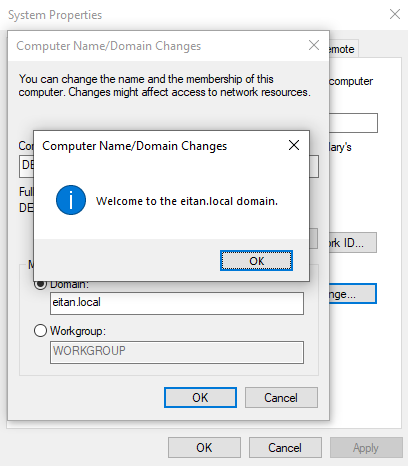
Like we see there is still something that is blocking the connection lets see at the log what it is

--------------------------------------------------------------------------------------------------------

And this is the missing rule we are going to add to the rules and check ones again if it will work



And like we see here we join successful to our domain controller with only few ports we added at the rule table



--------------------------------------------------------------------------------------------------------

There may be some problems when we will try to connect to user we created at the domain so its better if we add the port ALL\_DCE\_RPC it is allowing all RPC management and controller so we can have the trust of the domain

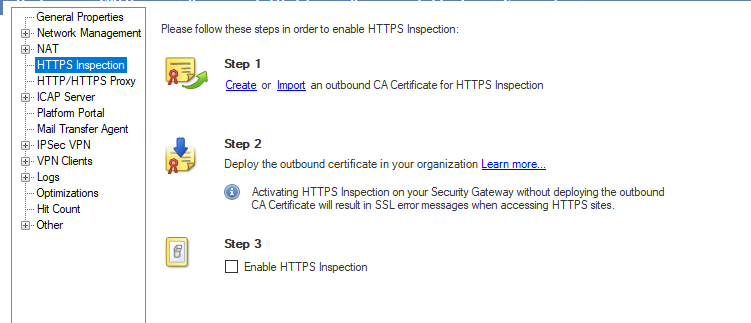
And in the same way we can add to the domain the second WIN2(LAN4) computer.

*part two*

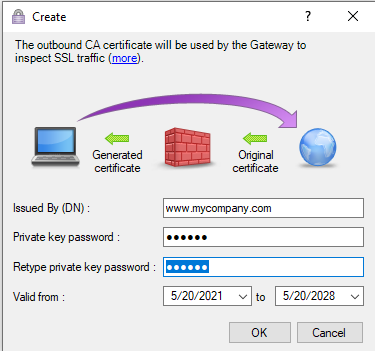
in this part of the project I will show how to control the browsing security and management of the workers, it allows me to be at control of what my workers do and enter in the internet

first, we will disable the blades from bank website so we will not be allowed to see if workers are entering their bank accounts by https inspection

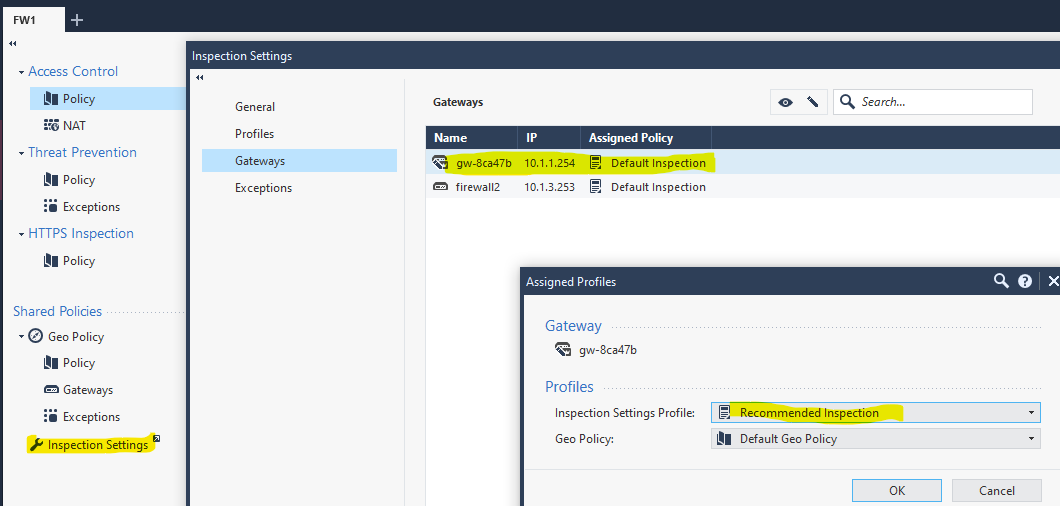
go to the firewall settings HTTPS INSPECTION and click create



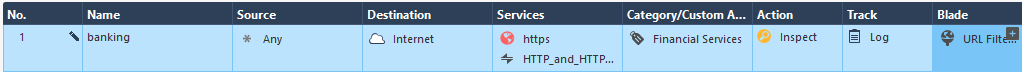
Create certificate



Then go to inspection settings in security and policy 🡪 getaway🡪 choose the getaway you want and select recommended inspection



-------------------------------------------------------------------------------------------------------

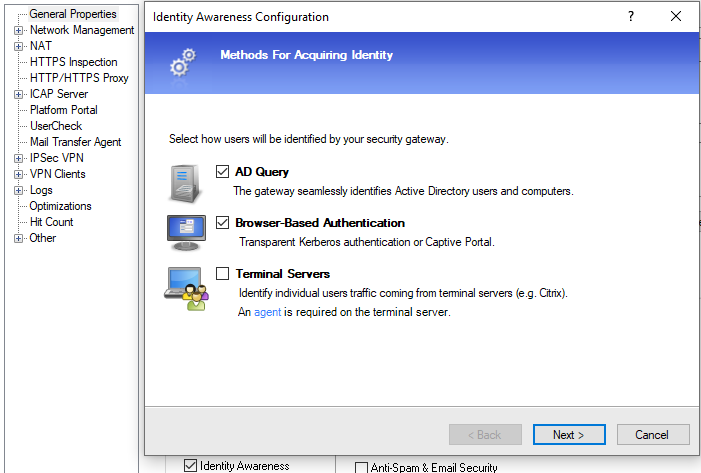
The we will crate at the HTTPS INSPETION rule that is going to inspect when people go to the bank web site

Like we see here I googled bank leumi and I got bypass with the web filter

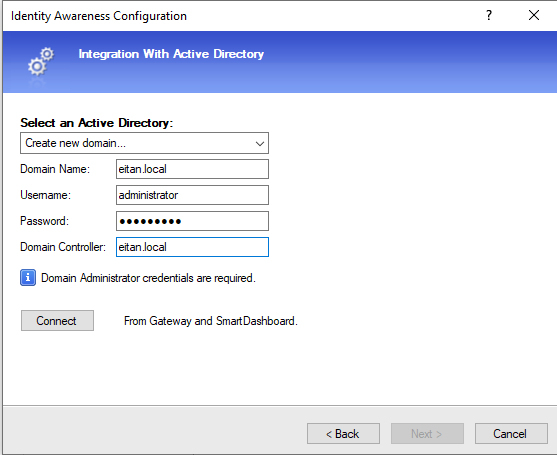


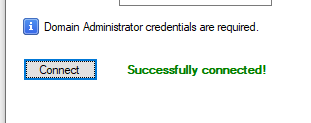
Identity awareness provide blade visibility content

Select identity awareness 🡪 then AD query and browser

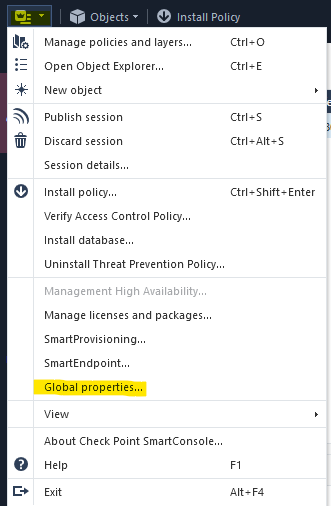


Now we will put the user name and the password of the domain we have and then click connect

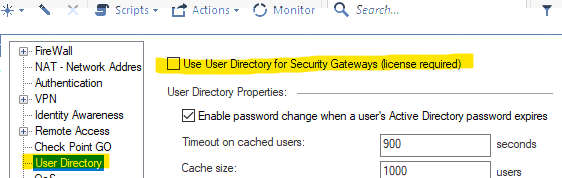


Here we see we have approved from the system we have successful connected to the domain

When we finish the install of the domain, we will go to the global properties in the up left corner of the smart management

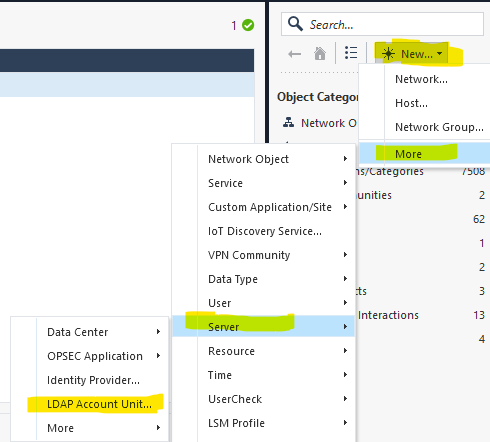


Then we will go to user directory and select use user directory for security getaway

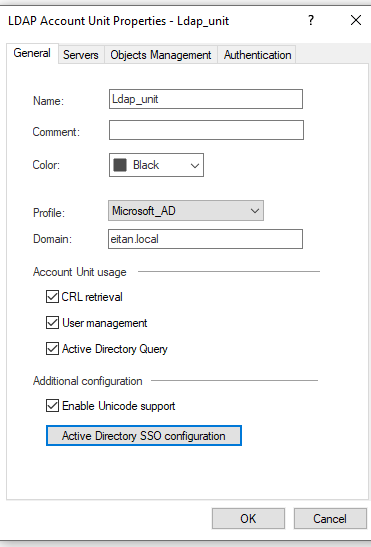


Next, we need to create LDAP account unit:

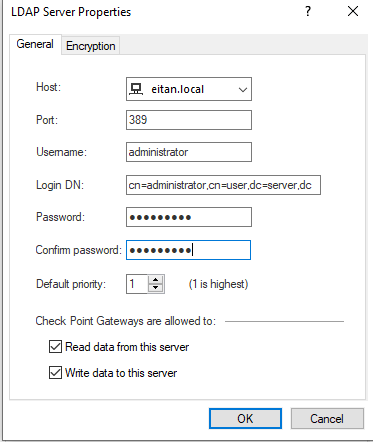
 is an open and cross platform protocol used for directory services authentication. LDAP provides the communication language that applications use to communicate with other directory services servers



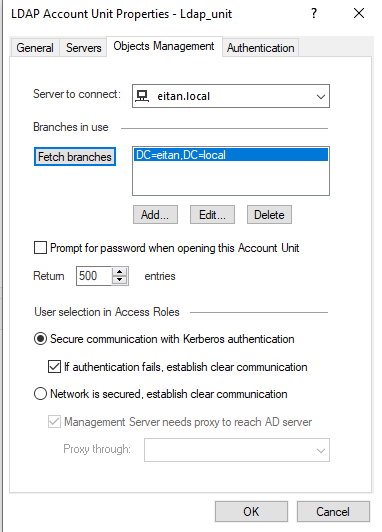
here we will enter our domain name and select all the options



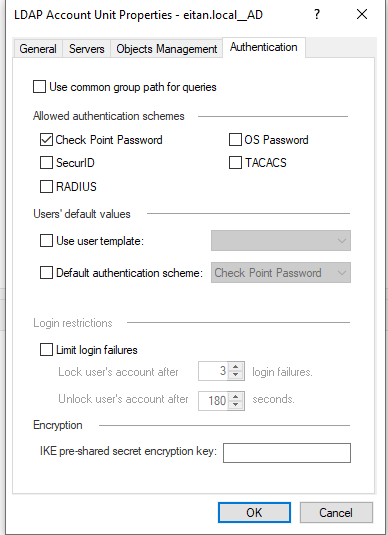
now we will add a server of the domain



Next go to object manager and hit fetch branches



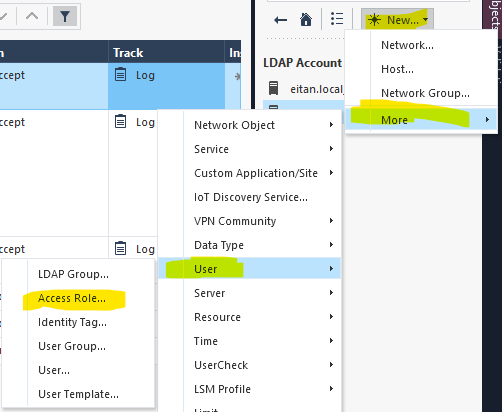
Next go to authentication and select only checkpoint password

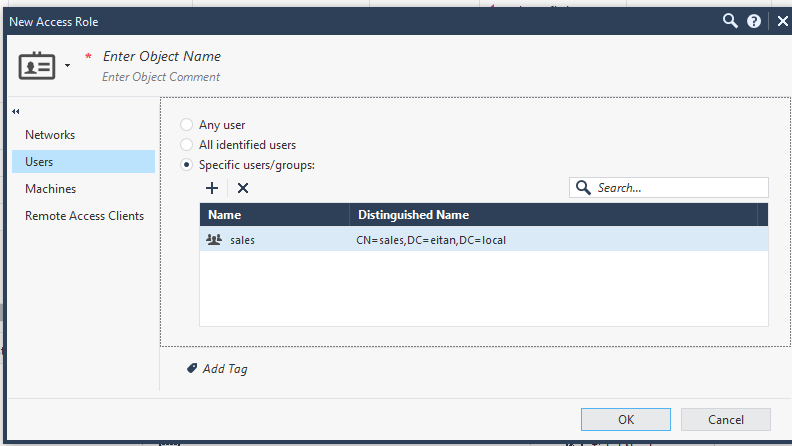


***User identity check***

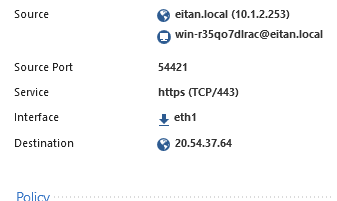
To order to allow the LANs access the portals I need to create a rule that allow it

Next ill create a group in the AD and in this group ill put WIN2 for example SALES group with WIN2





Now ill go brows and ill check if I can see where the users’ brows



Here we can see the pc we are using to get to the internet

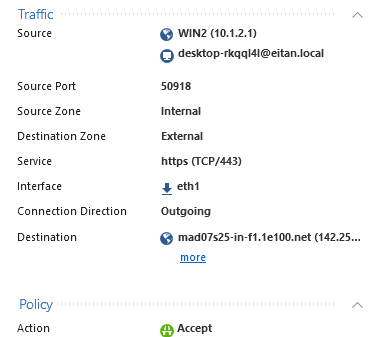
***Media access***

In this part of the project, I need to block media shearing and streaming for every one but allow LAN2 to access YouTube



Like we see here I allow LAN2 to go to YouTube and below I drop the media

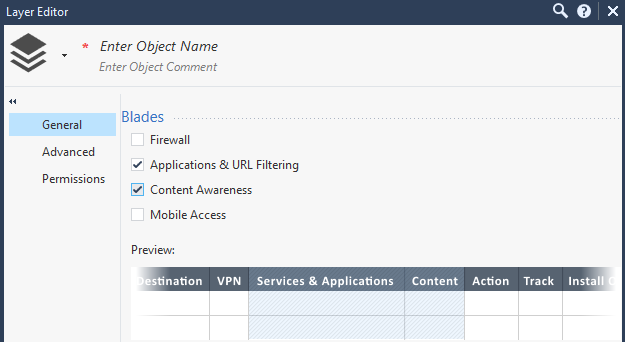
Like we see LAN1 drop YouTube, LAN2 approve YouTube

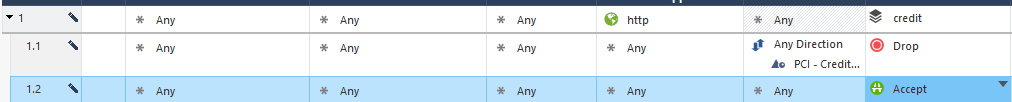


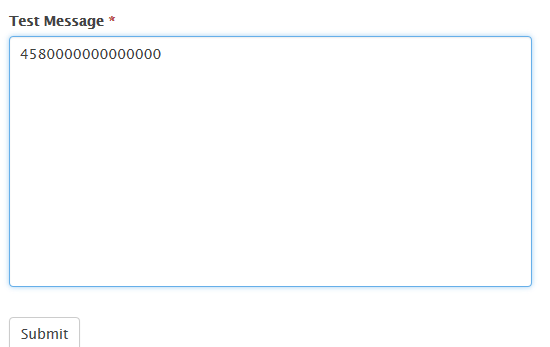
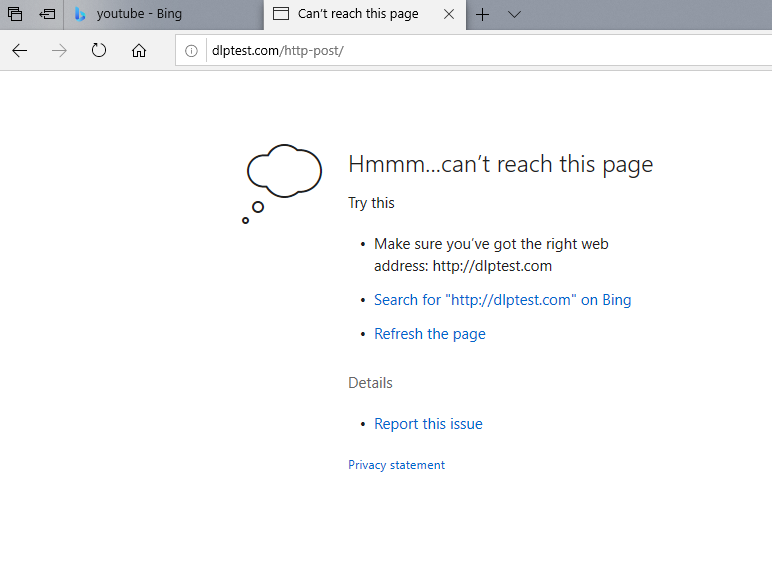
***Contact awareness***

In this part of the project ill explain how to reject credit card number on http protocol for more safety of the user

First, we will create inlayer and select contact awareness and app+url

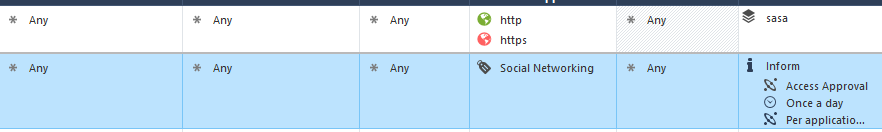


Then we will select http port in the main layer and in the inlayer, we will select in the filtering PCI-credit card and any direction

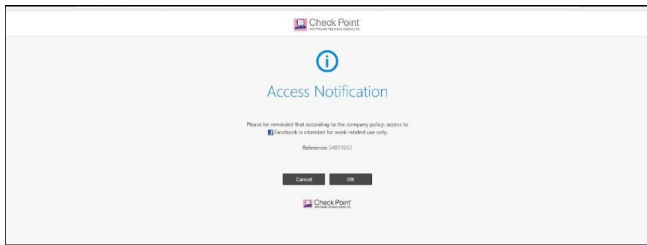
Ill go to [www.dlptest.com/http-post//](http://www.dlptest.com/http-post//) to check if it is blocking the credit card at http

We can see that we have block so it is working

Now we want to make every user that is connecting to social media to get massage that he is agree to the company terms



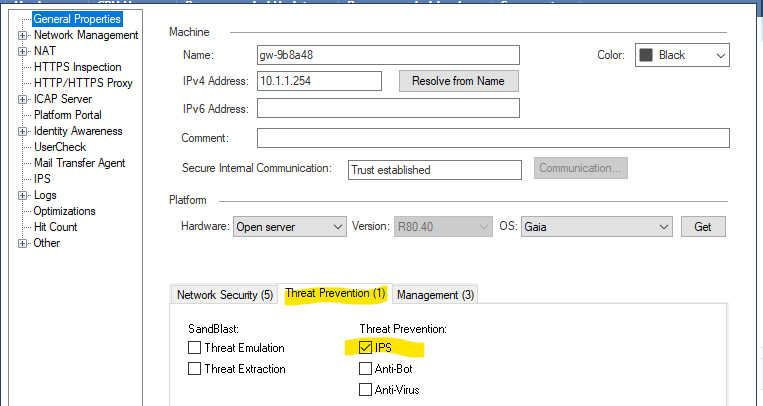
--------------------------------------------------------------------------------------------------------

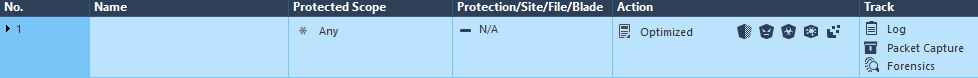
Here we can see when we enter to Facebook, we got massage and that means its working 

***IPS***

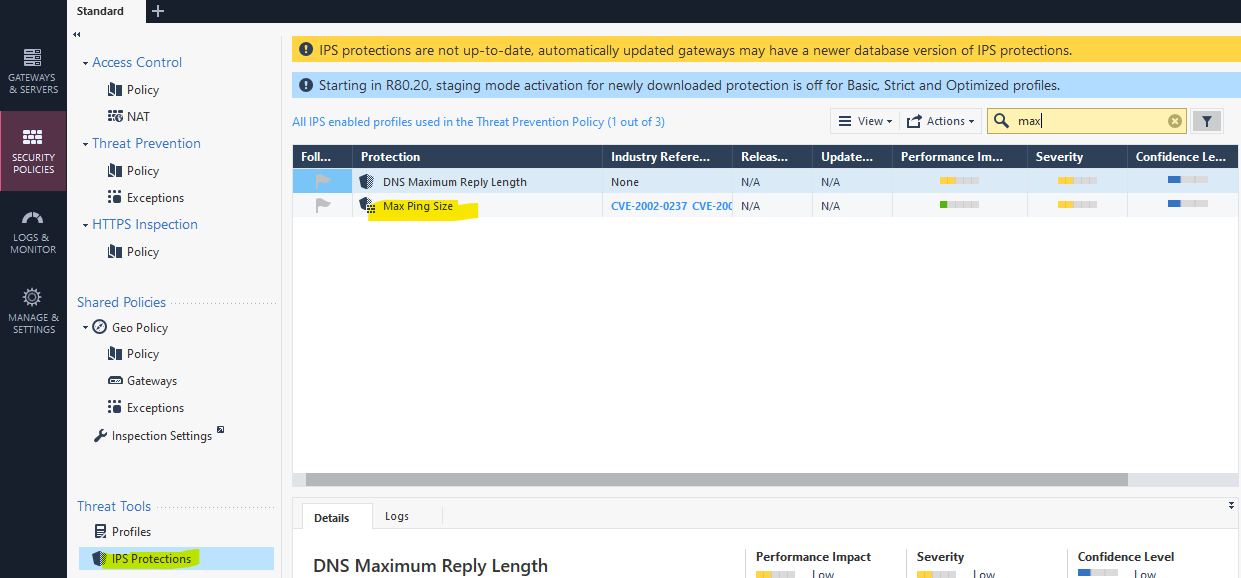
in this part of the project, I need to allow IPS and minimize the ping size to avoid attacks

select the IPS and then click OK

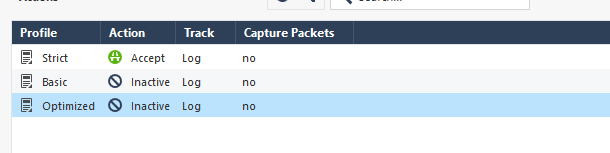


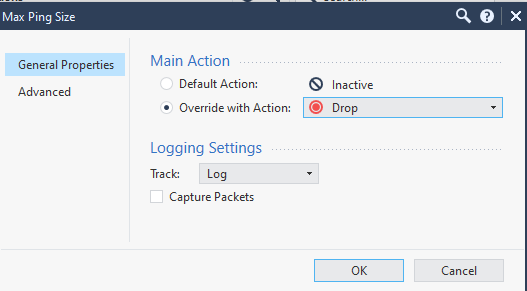
then create threat policy optimized

Then go to IPS protections and search for max ping size and click on it

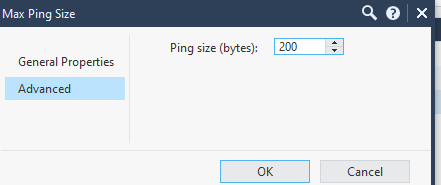


Go to the optimized and click on it

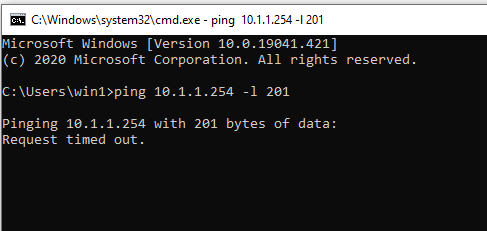


Put drop action

And in the advance maximized it only to 200 bytes ping



Then we will go to the CMD and ping with 201 bytes ping and see if its going to block it



And blocked

כתב : יקי בן-ניסן