Basic Migration from Check Point to Palo Alto Network – step by step using Migration Tool 3.1

Project	Written by	Update by	Version
Migration	Guy Zwerdling		1.4

Introduction:

Hi guys, so you may ask yourself why I wrote this article, so the answer is that I search all over the NET and didn't find seriously documentation about the migration from Check Point to Palo Alto Network.

So I'm here today to make this basic article and to help you to, first of all, understand the processes of the migration and to apply it on your organization.

May god help us all.

Good luck!

Guy.zwerdling@gmail.com

Concepts

The migration from Check Point is to Palo Alto it quite a bit serially business, this is because the different between the two from the security perspective point of view and in our case we will see that in the zone configuration. As you might already know, in check point world there is no mention to zones in the policy and all the policy are based on networking, segments and sub-netting. In Palo Alto however the zone is critical because the security policy rules are applied between zones.

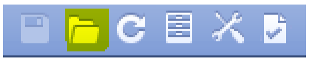
To do the migration we have a lot of stuff to cover but in this document I will show you only specifics stuff that we can do with the Migration Tool 3, we only configure in this article the Security Rules, Nat Rules and Object that we going to take from Check Point Management Machine and Routes that we will take from the Check Point Firewall.

I will specify everything stage by stage.

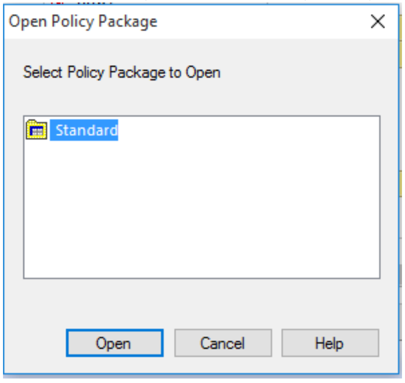
1. Preparing to the Migration

1.1 At the first stage we need to take some specific files from the Check Point FW and Mgmt, the files are:

1.1.1 <PolicyName>.W – the policy file that we setup on the Check Point machine, the name can be anything, the usual name is “Standard.w”, the name is depending on what you set on your management, if you don’t remember the name just go to the CheckPoint SmartDashboard and on the upper right side click on the **Open** icon:



And there you will see your policy file name:



Open Policy Package

Select Policy Package to Open

Standard

In my case it is **Standard**.

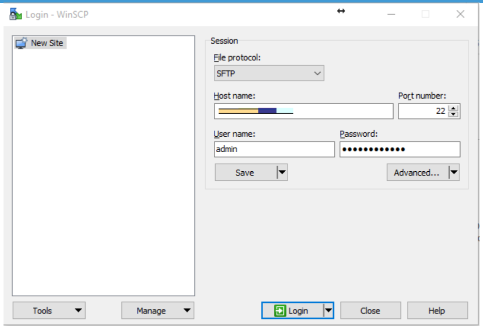
1.1.2 Object_5_0.C – this file contains the Objects in the Check Point topology.

1.1.3 Rulebases_5_0.fws – this file is the Global Rules Container, so we need it too.

1.1.4 Routes.txt – this file contains the routes in the Check Point firewall, of course you take this route only from the firewall that you want to migrate.

1.2 Now we need to take those files and save theme on our local machine for further use in the migration. I will use in WinSCP but you can use Filezila or other SFTP program that you like to use.

1.2.1 Open the WinSCP and type the IP of the Check Point Management server, type the username and the password and don’t forget to use port 22 to connect.



Session

File protocol: SFTP

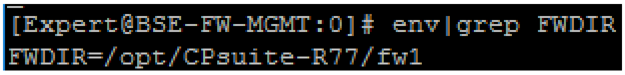
Host name: [redacted]

Port number: 22

User name: admin

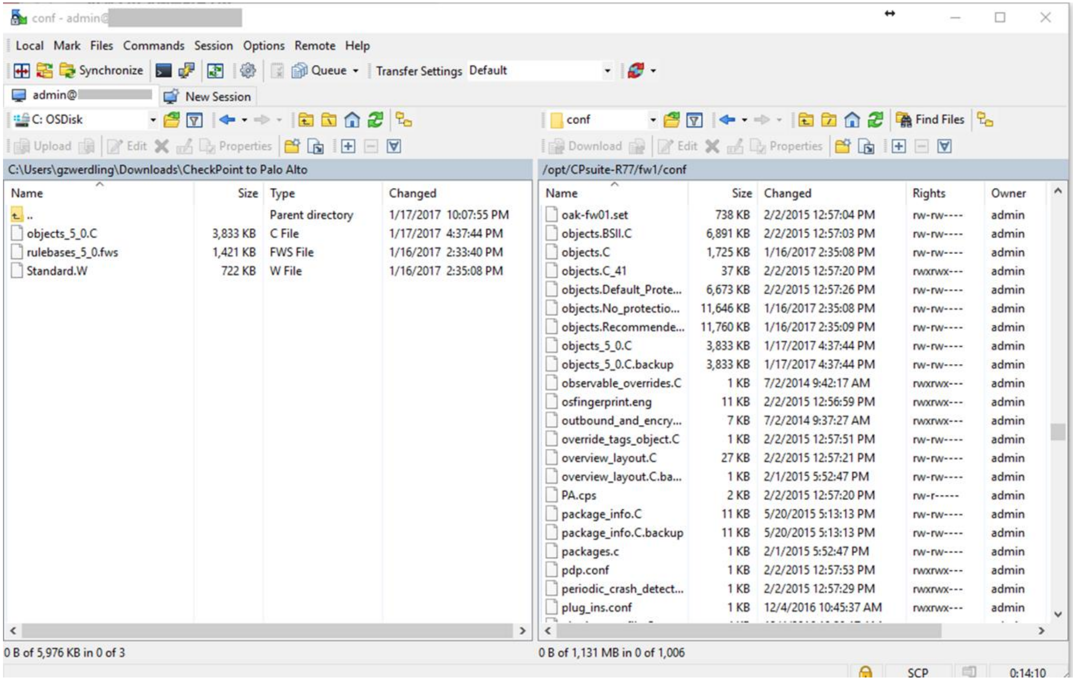
Password: ••••••••••••

1.2.2 Now according to Check Point the files are in the $FWDIR/conf, so we need to check what is the actually path that we need. Open putty and connect to your Check Point Mgmt server and on the cli type the command `env|grep FWDIR`, in my case the directory is /opt/CPsuite-R77/fw1.



```
[Expert@BSE-FW-MGMT:0]# env|grep FWDIR
FWDIR=/opt/CPsuite-R77/fw1
```

1.2.3 On WinSCP go to the directory <$FWDIR path>/conf and search the files and copy theme to your local machine.



C:\Users\gzwerdling\Downloads\CheckPoint to Palo Alto

Name	Size	Type	Changed
..		Parent directory	1/17/2017 10:07:55 PM
objects_5_0.C	3,833 KB	C File	1/17/2017 4:37:44 PM
rulebases_5_0.fws	1,421 KB	FWS File	1/16/2017 2:33:40 PM
Standard.W	722 KB	W File	1/16/2017 2:35:08 PM

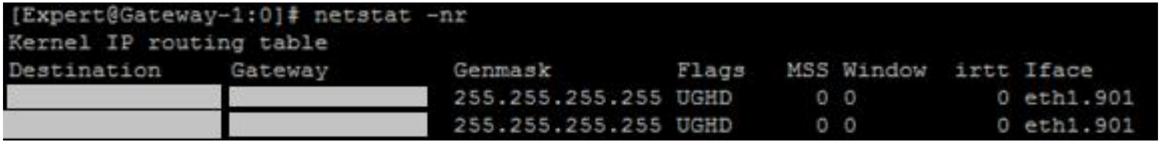
0 B of 5,976 KB in 0 of 3

/opt/CPsuite-R77/fw1/conf

Name	Size	Changed	Rights	Owner
oak-fw01.set	738 KB	2/2/2015 12:57:04 PM	rw-rw----	admin
objects.BSII.C	6,891 KB	2/2/2015 12:57:03 PM	rw-rw----	admin
objects.C	1,725 KB	1/16/2017 2:35:08 PM	rw-rw----	admin
objects.C_41	37 KB	2/2/2015 12:57:20 PM	rwxrwx---	admin
objects.Default_Prote...	6,673 KB	2/2/2015 12:57:26 PM	rw-rw----	admin
objects.No_protectio...	11,646 KB	1/16/2017 2:35:08 PM	rw-rw----	admin
objects.Recommende...	11,760 KB	1/16/2017 2:35:09 PM	rw-rw----	admin
objects_5_0.C	3,833 KB	1/17/2017 4:37:44 PM	rw-rw----	admin
objects_5_0.C.backup	3,833 KB	1/17/2017 4:37:44 PM	rw-rw----	admin
observable_overrides.C	1 KB	7/2/2014 9:42:17 AM	rwxrwx---	admin
osfingerprint.eng	11 KB	2/2/2015 12:56:59 PM	rwxrwx---	admin
outbound_and_encry...	7 KB	7/2/2014 9:37:27 AM	rwxrwx---	admin
override_tags_object.C	1 KB	2/2/2015 12:57:51 PM	rw-rw----	admin
overview_layout.C	27 KB	2/2/2015 12:57:21 PM	rw-rw----	admin
overview_layout.C.ba...	1 KB	2/1/2015 5:52:47 PM	rw-rw----	admin
PA.cps	2 KB	2/2/2015 12:57:20 PM	rw-r-----	admin
package_info.C	11 KB	5/20/2015 5:13:13 PM	rw-rw----	admin
package_info.C.backup	11 KB	5/20/2015 5:13:13 PM	rw-rw----	admin
packages.c	1 KB	2/1/2015 5:52:47 PM	rw-rw----	admin
pdp.conf	1 KB	2/2/2015 12:57:53 PM	rwxrwx---	admin
periodic_crash_detect...	1 KB	2/2/2015 12:57:29 PM	rwxrwx---	admin
plug_ins.conf	1 KB	12/4/2016 10:45:37 AM	rwxrwx---	admin

0 B of 1,131 MB in 0 of 1,006

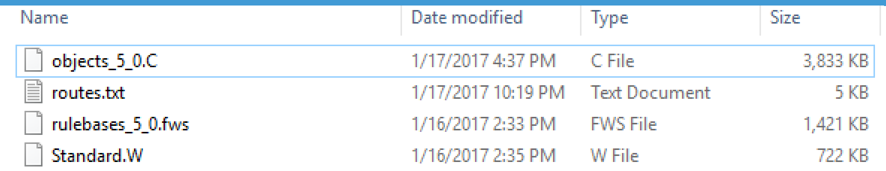
1.2.4 The route file we take directly from Check Point Firewall, so connect to him and on the command prompt type the command `netstat -nr`.



```
[Expert@Gateway-1:0]# netstat -nr
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
[redacted]      [redacted]      255.255.255.255 UGHD      0 0          0 eth1.901
[redacted]      [redacted]      255.255.255.255 UGHD      0 0          0 eth1.901
```

The output save as TXT file on your local machine (only from the titles bar, `Dest Gate Gen` etc.).

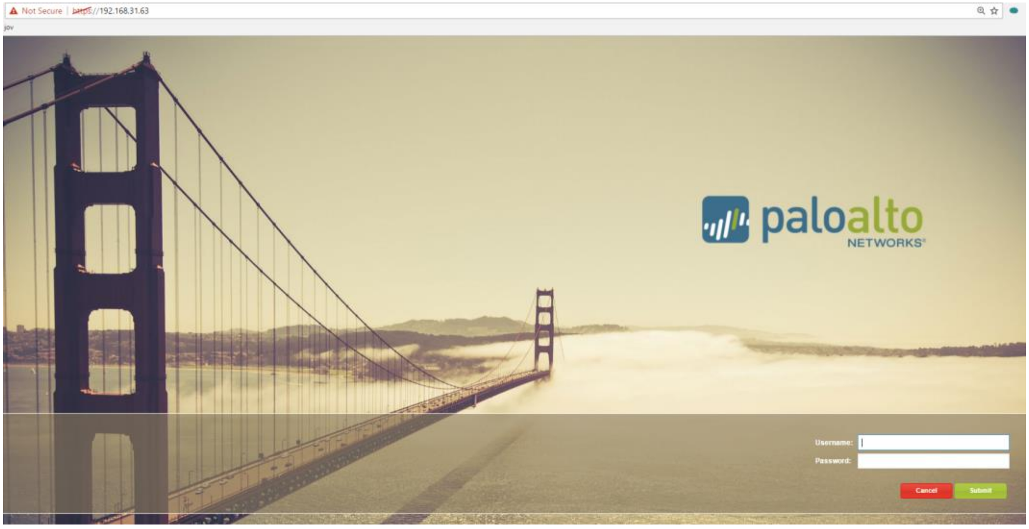
1.2.5 After that you do all this stuff correctly you end up with the files as follow:



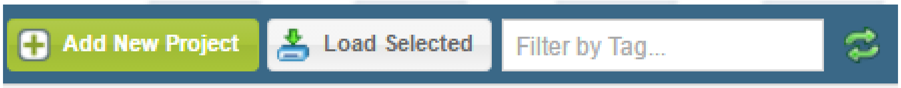
Name	Date modified	Type	Size
objects_5_0.C	1/17/2017 4:37 PM	C File	3,833 KB
routes.txt	1/17/2017 10:19 PM	Text Document	5 KB
rulebases_5_0.fws	1/16/2017 2:33 PM	FWS File	1,421 KB
Standard.W	1/16/2017 2:35 PM	W File	722 KB

1.3 Now we need to go to the migration machine and upload the files, but before that there is more stuff that we need to do.

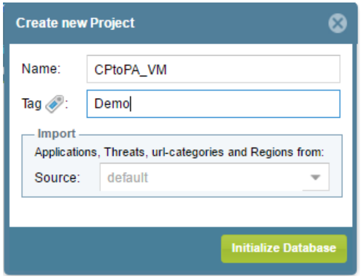
1.3.1 Connect to the migration tool, to setup the migration tool please refer to the links as follows:
https://live.paloaltonetworks.com/t5/Migration-Tool-Articles/Download-the-Migration-Tool/ta-p/56582
https://live.paloaltonetworks.com/t5/Migration-Tool-Articles/Migration-Tool-3-Info-and-Guide/ta-p/55294
https://live.paloaltonetworks.com/t5/Migration-Tool-Articles/Migration-Tool-Tutorial-Videos/ta-p/58096
And type username and password.



1.3.2 Create new project by click on **add new project**



1.3.3 Give the Project **Name** and **Tag** (the tag are used for filtering).



Create new Project

Name: CPtoPA_VM

Tag: Demo

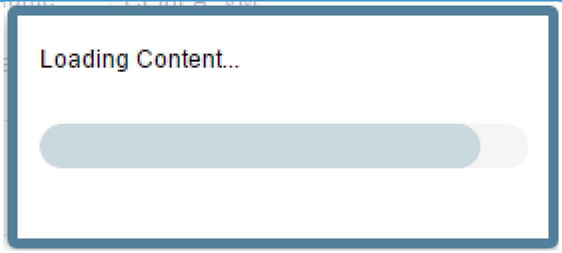
Import

Applications, Threats, url-categories and Regions from:

Source: default

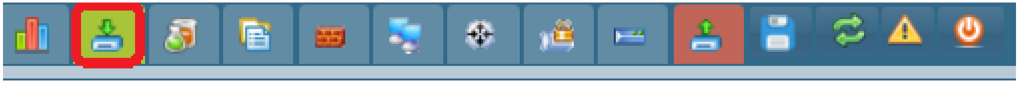
In my case it's virtual environment so the Palo Alto and Check Point machine are virtual (using VMware)

1.3.4 Click on **Initialize Database** and it will load and create new project.



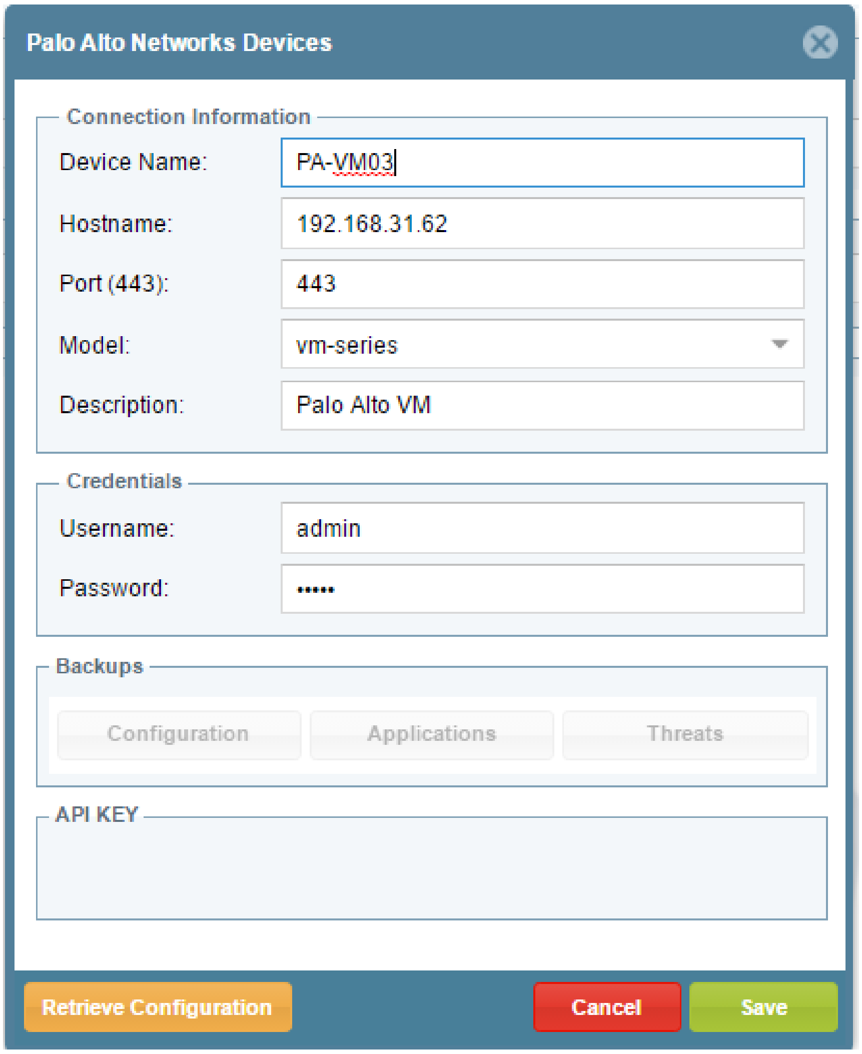
Loading Content...

1.3.5 Click on **Import Configuration** icon that appear on the upper left side on the menu.



1.3.6 Now we will import the Palo Alto device to our **Device List**. To do so click on **Add Device** on the bottom of the menu.

1.3.7 The Device menu will popup, fill up the **Connection Information** and **Credential** to allow the MT3 to connect the device.



Palo Alto Networks Devices

Connection Information

Device Name: PA-VM03

Hostname: 192.168.31.62

Port (443): 443

Model: vm-series

Description: Palo Alto VM

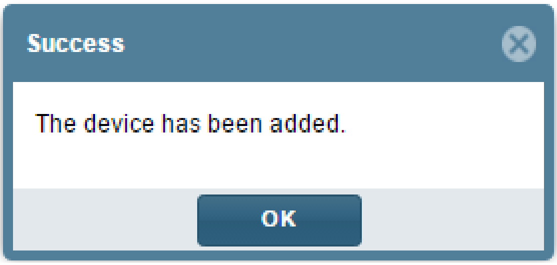
Credentials

Username: admin

Password: •••••

And click **Save**.

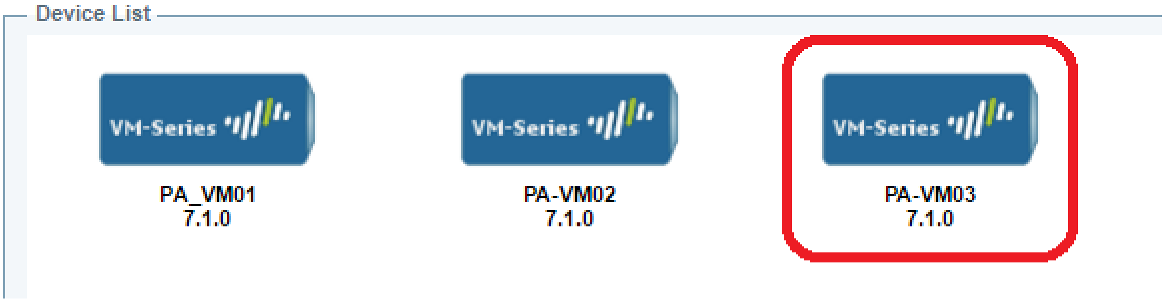
1.3.8 You should get message about the device has being added successfully, click OK.



Success

The device has been added.

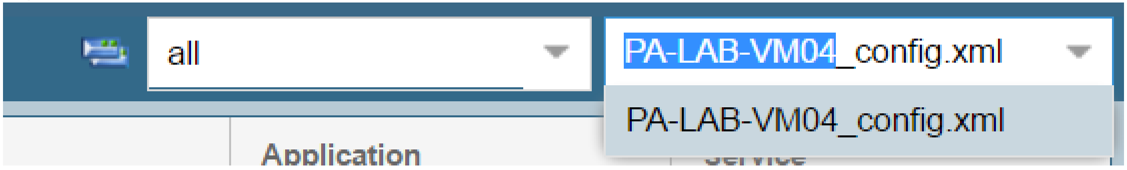
New you will see the device on the device list



Device List

In my case there is more than one device so I can see the other as well the new one.

1.3.9 Click on the device icon and it will create a XML file and you will see this file on the upper right side on the menu

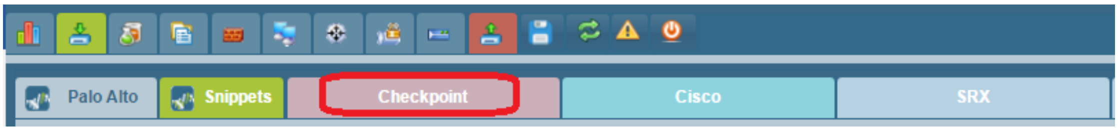


all

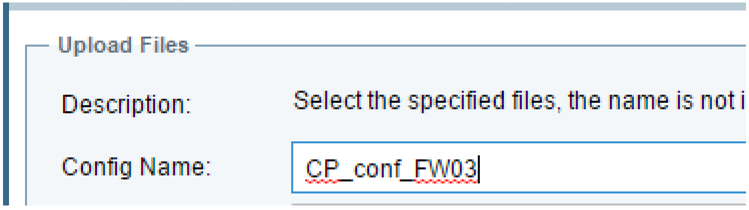
PA-LAB-VM04_config.xml

PA-LAB-VM04_config.xml

1.3.10 Now on the import configuration menu select the **Checkpoint** tab to upload the checkpoint files.



1.3.11 Now we going to give a name to the **Upload Files**, this name will serve us in the future.

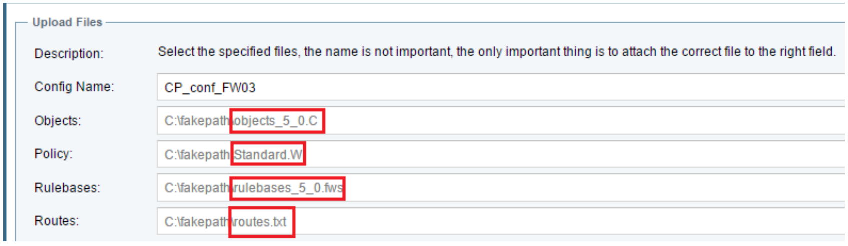


Upload Files

Description: Select the specified files, the name is not i

Config Name: CP_conf_FW03

1.3.12 On the **Checkpoint** menu upload the file that you saved as I mentioned in paragraph 1.2.5 to the correct position as follow:

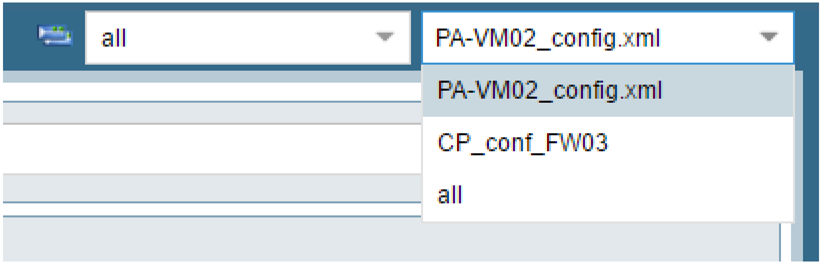


Upload Files

Description:	Select the specified files, the name is not important, the only important thing is to attach the correct file to the right field.
Config Name:	CP_conf_FW03
Objects:	C:\fakepath\objects_5_0.C
Policy:	C:\fakepath\Standard.W
Rulebases:	C:\fakepath\rulebases_5_0.fws
Routes:	C:\fakepath\routes.txt

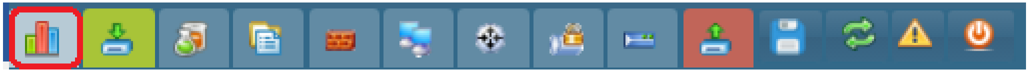
And click on the **UPLOAD** tab.

1.3.13 Now, while it's cocking, we can go and make some coffee, after it finish you will see on the upper right side of the screen the option to display the configuration of your Check Point FW and your Palo Alto FW.

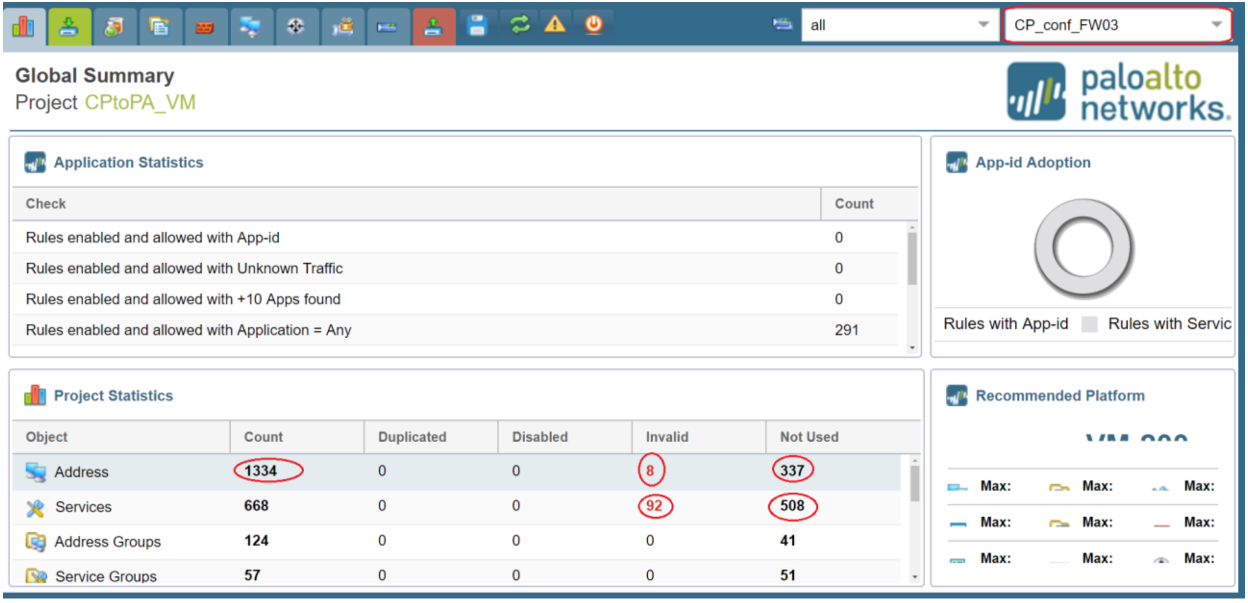


- In my case you can see that I have more than one configuration file, the CP_conf_FW03 and the PA-VM02_config.xml which was my test before.

Now go to the main menu of your project by clicking on the Global Summary icon on the upper left side of the dashboard



And while the CP_config_FW03 is chosen you will see statistic about your object that you have in your checkpoint FW and rule as well the security rule and interfaces and the **Invalid** objects and even the **Not Used** objects.



Global Summary
Project CPtoPA_VM

Application Statistics

Check	Count
Rules enabled and allowed with App-id	0
Rules enabled and allowed with Unknown Traffic	0
Rules enabled and allowed with +10 Apps found	0
Rules enabled and allowed with Application = Any	291

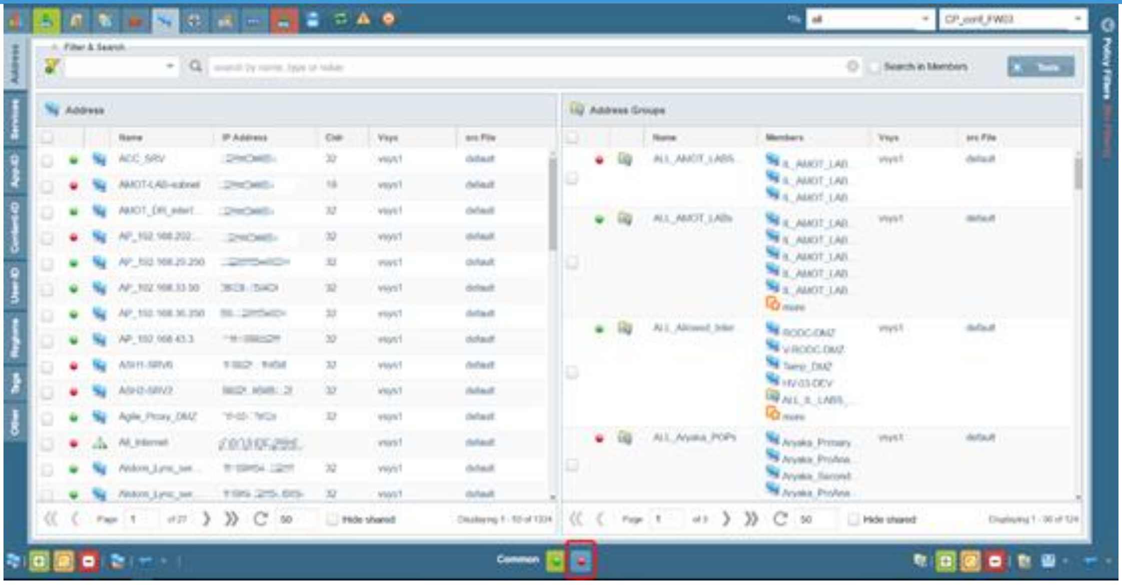
Project Statistics

Object	Count	Duplicated	Disabled	Invalid	Not Used
Address	1334	0	0	8	337
Services	668	0	0	92	508
Address Groups	124	0	0	0	41
Service Groups	57	0	0	0	51

2. Check your configuration.

2.1 Now this is the difficult part because now you need to check your policy rules and NAT rules and interfaces for preparing the configuration to the PA machine.

2.1.1 First of all, go to the **Manage Object** menu and delete every object that not being used in your policies, every object that appear in red light is doesn't used so click on the red icon on the lower menu.



Filter & Search

Address

□			Name	IP Address	Cidr	Vsys	src File
□	🟢		ACC_SRV	[redacted]	32	vsys1	default
□	🔴		AMOT-LAB-subnet	[redacted]	16	vsys1	default
□	🟢		AMOT_DR_inter...	[redacted]	32	vsys1	default
□	🔴		AP_192.168.202...	[redacted]	32	vsys1	default
□	🟢		AP_192.168.20.250	[redacted]	32	vsys1	default
□	🟢		AP_192.168.33.50	[redacted]	32	vsys1	default
□	🟢		AP_192.168.36.250	[redacted]	32	vsys1	default
□	🟢		AP_192.168.43.3	[redacted]	32	vsys1	default
□	🔴		ASH1-SRV6	[redacted]	32	vsys1	default
□	🔴		ASH2-SRV2	[redacted]	32	vsys1	default
□	🟢		Agile_Proxy_DMZ	[redacted]	32	vsys1	default
□	🔴		All_Internet	[redacted]		vsys1	default
□	🟢		Aldom_Lync_se...	[redacted]	32	vsys1	default
□	🟢		Aldom_Lync_se...	[redacted]	32	vsys1	default

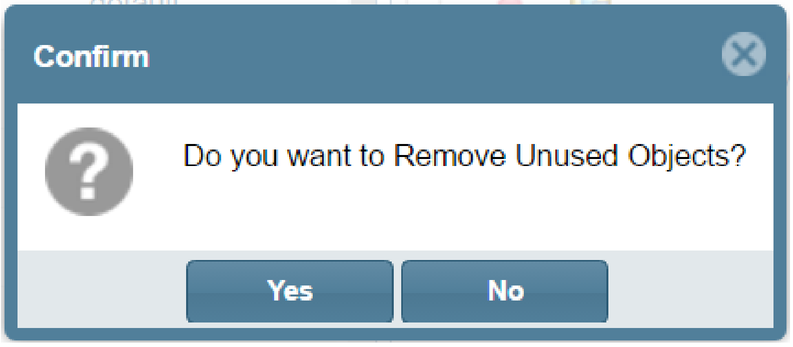
Page 1 of 27 | 50 | □ Hide shared | Displaying 1 - 50 of 1334

Address Groups

□			Name	Members	Vsys	src File
□	🔴		ALL_AMOT_LABS...	IL_AMOT_LAB... IL_AMOT_LAB... IL_AMOT_LAB...	vsys1	default
□	🟢		ALL_AMOT_LABs	IL_AMOT_LAB... IL_AMOT_LAB... IL_AMOT_LAB... IL_AMOT_LAB... IL_AMOT_LAB... more	vsys1	default
□	🟢		ALL_Allowed_Inter	RODC-DMZ V-RODC-DMZ Temp_DMZ HV-03-DEV ALL_IL_LABS_... more	vsys1	default
□	🔴		ALL_Aryaka_POPs	Aryaka_Primary Aryaka_ProAna... Aryaka_Second Aryaka_ProAna...	vsys1	default

Page 1 of 3 | 50 | □ Hide shared | Displaying 1 - 50 of 124

2.1.2 It will ask you to confirm the removing unused object.



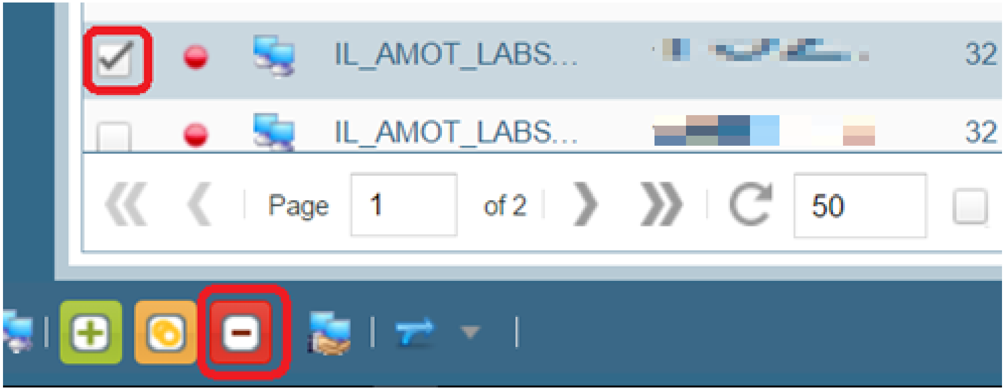
Confirm

Do you want to Remove Unused Objects?

2.1.3 And all the unused object will be deleted.

- If you don't want to delete every object at once, you can go ahead and delete object's one by one, but remember every unused **Address** object that you can't delete it because it used in unused **Address Groups,** so make sure that you delete the address group for that address before you actually delete him.

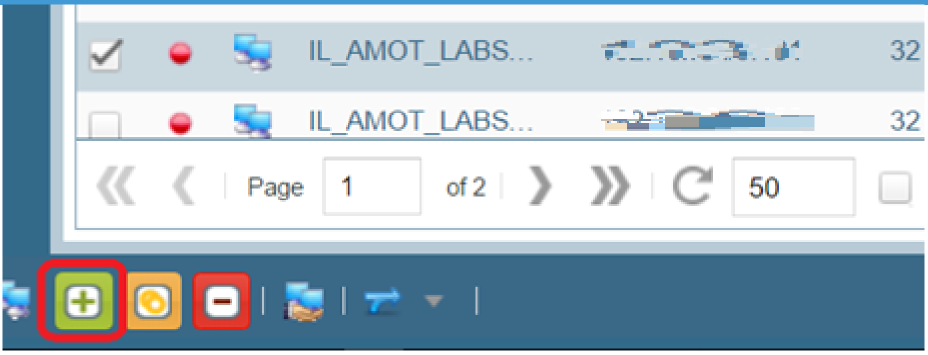
2.1.4 To delete one object just select him and delete him by the delete icon on the current side.



☑	🔴		IL_AMOT_LABS...	[redacted]	32
□	🔴		IL_AMOT_LABS...	[redacted]	32

Page 1 of 2 | 50 | □

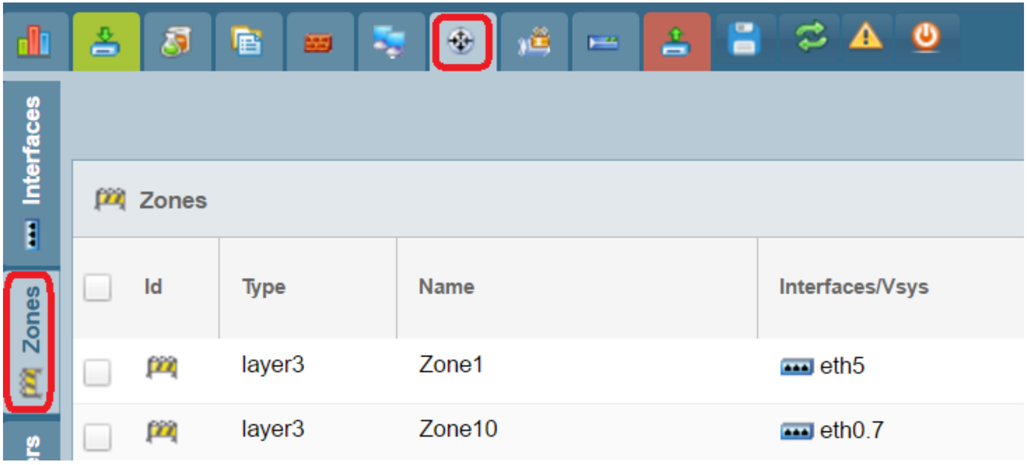
2.1.5 If you need for future use to create an object, click on the green bottom and change the object as you like.



☑	●	IL_AMOT_LABS...	[redacted]	32
□	●	IL_AMOT_LABS...	[redacted]	32

2.2 New let’s rearrange the interfaces

2.2.1 Go to the **Interfaces>Zones** menu and rename zones as you need to your topology, please remember that on Palo Alto we work with zone to setup the policy.

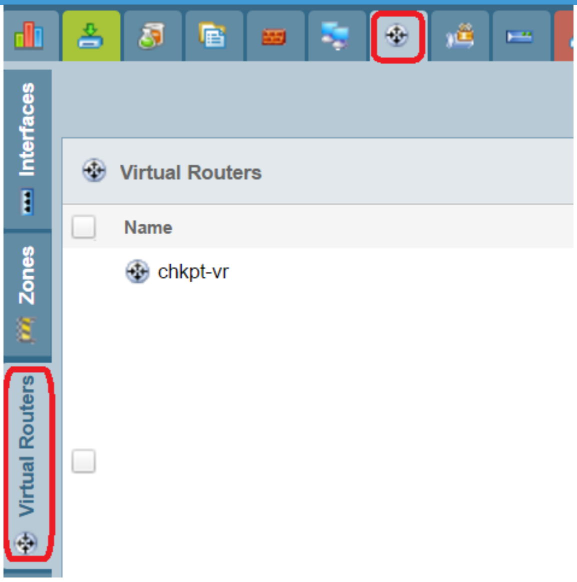


Zones

□	Id	Type	Name	Interfaces/Vsys
□		layer3	Zone1	eth5
□		layer3	Zone10	eth0.7

- <span>Please remember **do not delete zones**, just rename theme. This is because when the MT3 load the configuration for the interfaces, it creates zones for every interface and adding the zones to the policy by the routes that the FW have. It’s very critical because if you will delete the zones and create a new one, on the policy every rule will be in “any” in the zone source and zone destination.</span>

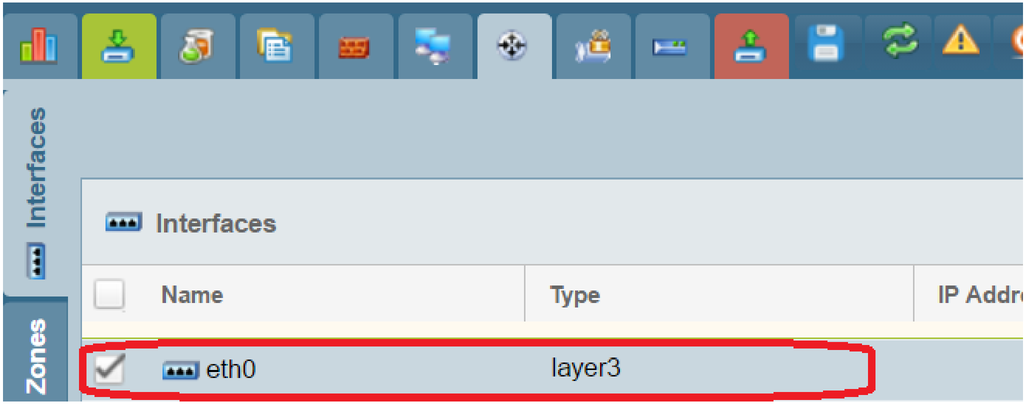
2.2.2 After it go to the Virtual Router and if you need on your topology more than one routing table, setup what you need here.



Virtual Routers

□	Name
	chkpt-vr

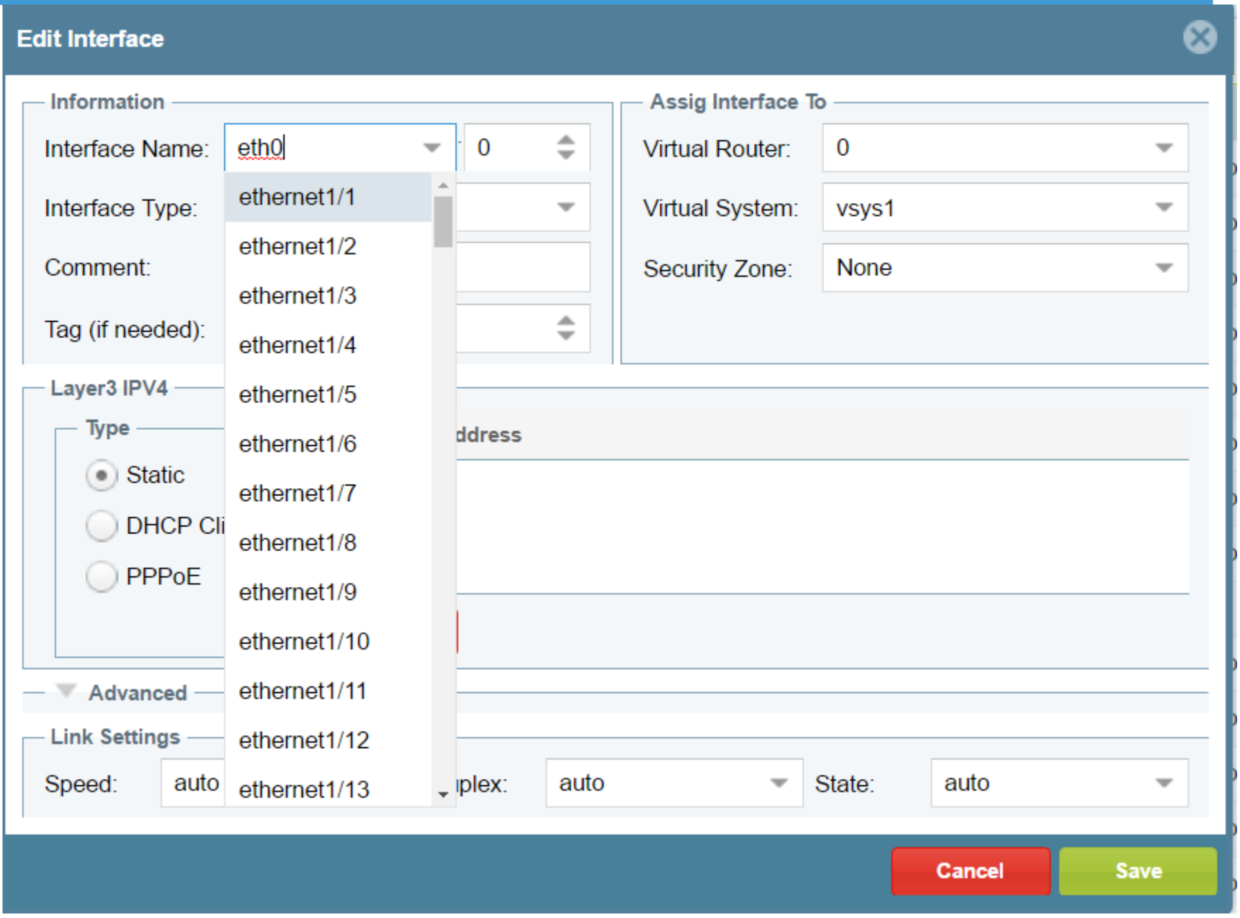
2.2.3 After you finish to setup everything that you needed, you just need to go and setup the interfaces to be in the correct syntax for the Palo Alto device. So, go to the Interfaces menu and select the interface that you want to change and double click on that interface.



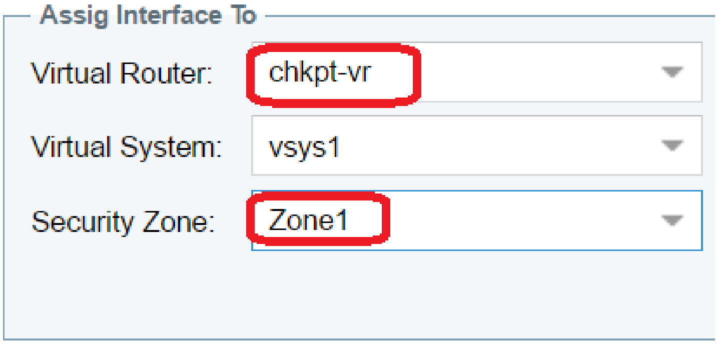
Interfaces

□	Name	Type	IP Addr
☑	eth0	layer3	

2.2.4 Now on the **Edit Interface** edit the interface name to the correct syntax, in my case eth0 become ethernet0/0.



2.2.5 Setup the **Virtual Router** for that interface and the **Security Zone** that you were created and click **Save**.

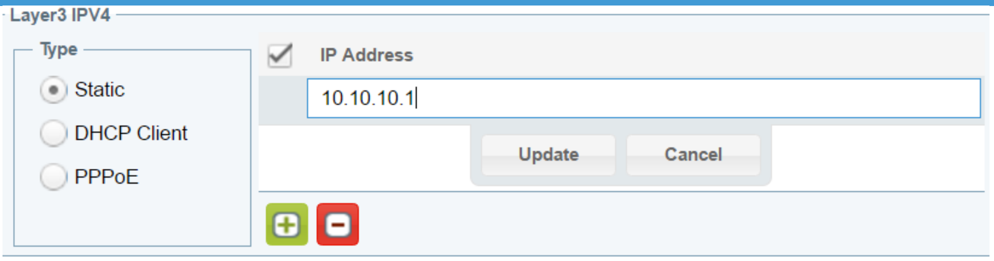

Assig Interface To

Virtual Router: chkpt-vr

Virtual System: vsys1

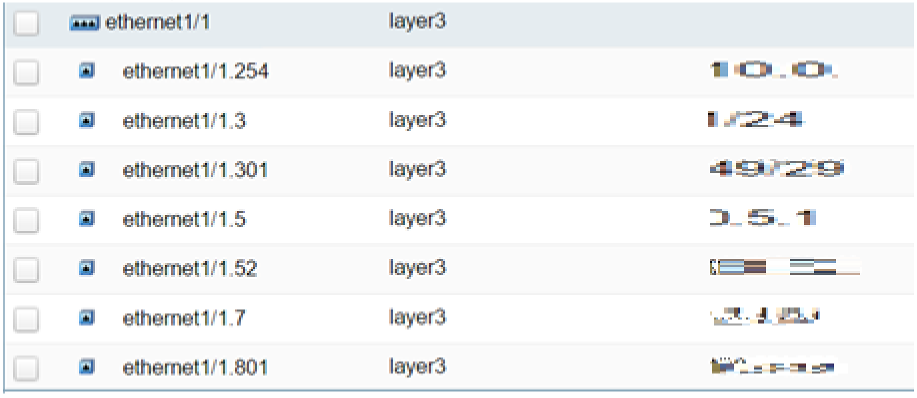
Security Zone: Zone1

2.2.6 If your **Interface Type** is setup on Layer3 this is mean that you can setup an IP address for this interface, so let’s assign an IP address for this interface.



In my case I use sub interfaces so my IP's setup on them.

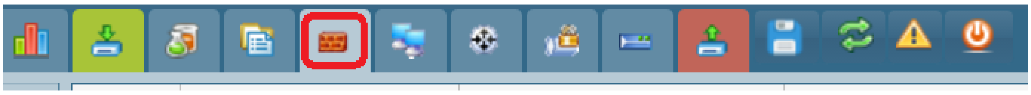
2.2.7 After you finish to rearrange the interfaces, it should be ready for the Palo Alto device with the correct syntax.



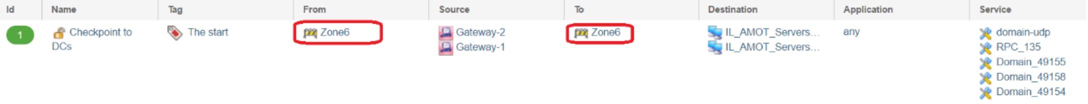
ethernet1/1	layer3	
ethernet1/1.254	layer3	[redacted]
ethernet1/1.3	layer3	[redacted]
ethernet1/1.301	layer3	[redacted]
ethernet1/1.5	layer3	[redacted]
ethernet1/1.52	layer3	[redacted]
ethernet1/1.7	layer3	[redacted]
ethernet1/1.801	layer3	[redacted]

2.3 New let's go to the rule base

2.3.1 Click on the Manage Policy icon and there you can view your policy's from your Check Point machine.



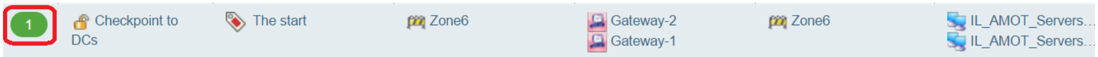
2.3.2 Now we need go and check the rules one by one to setup the correct zone for each rule.



Id	Name	Tag	From	Source	To	Destination	Application	Service
1	Checkpoint to DCs	The start	Zone6	Gateway-2 Gateway-1	Zone6	IL_AMOT_Servers... IL_AMOT_Servers...	any	domain-udp RPC_135 Domain_49155 Domain_49158 Domain_49154

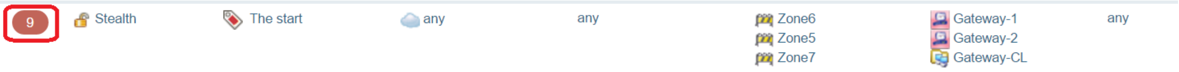
You can see that in my case the I have the default zones named Zone6 so I change them to be internal and external zones as needed.

2.3.3 Each PERMIT/ALLOW rule will be sign with green color on the ID number.



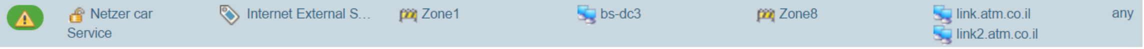
1	Checkpoint to DCs	The start	Zone6	Gateway-2 Gateway-1	Zone6	IL_AMOT_Servers... IL_AMOT_Servers...

2.3.4 Every DENAY rule will be sign with red color on the IP number.



9	Stealth	The start	any	any	Zone6 Zone5 Zone7	Gateway-1 Gateway-2 Gateway-CL	any

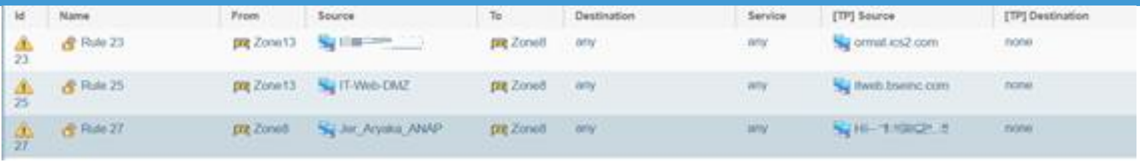
2.3.5 New we need to validate all the warnings displayed on specific rules and double check it.



⚠	Netzer car Service	Internet External S...	Zone1	bs-dc3	Zone8	link.atm.co.il link2.atm.co.il	any

2.3.6 In my case I need to check 315 rules, this is a lot of work but you must do it if you want the migration will be succeeded

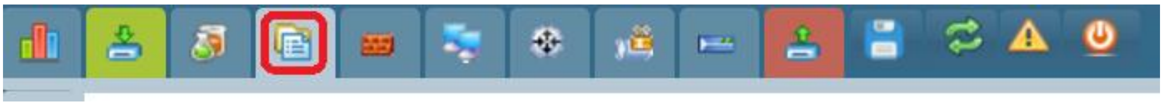
2.3.7 We also need to check the Nat rules and rearrange them as the same way we did in the policy's rules.



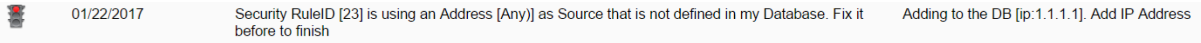
Id	Name	From	Source	To	Destination	Service	[TP] Source	[TP] Destination
23	Rule 23	Zone13	[illegible]	Zone8	any	any	ormat.ics2.com	none
25	Rule 25	Zone13	IT-Web-DMZ	Zone8	any	any	itweb.bseinc.com	none
27	Rule 27	Zone8	Jer_Aryaka_ANAP	Zone8	any	any	[illegible]	none

2.4 Logs and monitor for your rules

2.4.1 Now let’s click on the Monitor, log and Report icon to check every problem that the MT3 find for us.



2.4.2 If your setup your zone carefully and check every rule that is on the right place you will good on the logs report, however we have some thins that we need to know, in the left side we have a “traffic lights” sign, if this sign is on yellow or green you may ignor it but if it is on red color it will be better to check the error log that the MT3 find



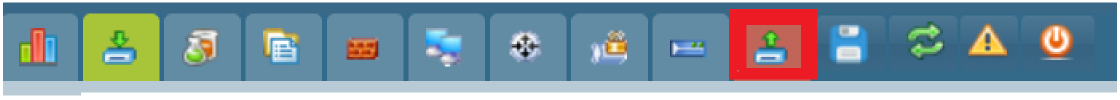
🚦	01/22/2017	Security RuleID [23] is using an Address [Any)] as Source that is not defined in my Database. Fix it before to finish	Adding to the DB [ip:1.1.1.1]. Add IP Address

In my case you can see that he says that in rule 23 I have address as source that not found in the database.

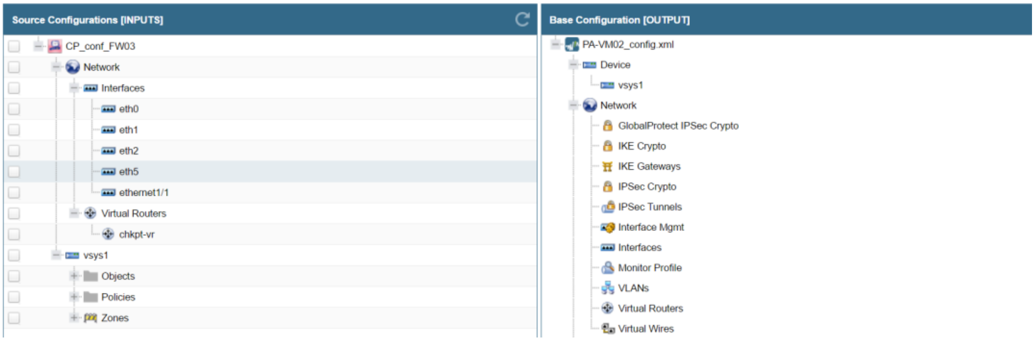
3. Prepper the XML file

3.1 After we finish to check all the critical stuff, now we need to go and setup and export the XML file for the Palo Alto FW.

3.1.1. Go to the **Create The Output** icon.



3.1.2. On the main screan you should see the following



Source Configurations [INPUTS]

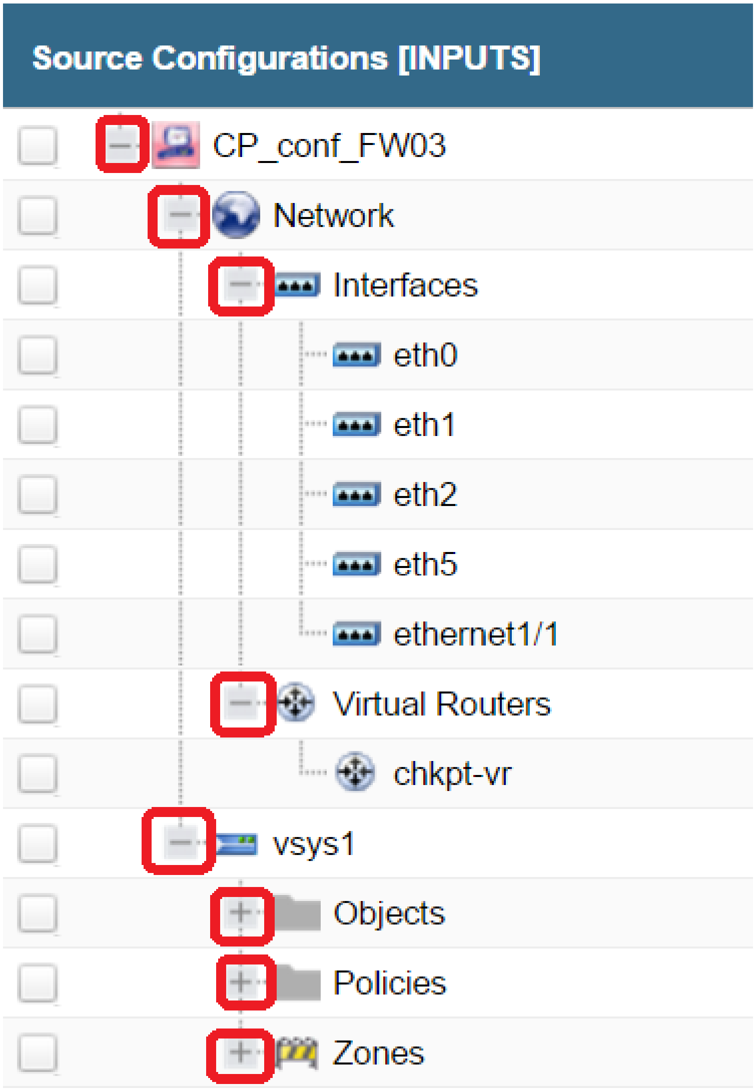
```
□ ⊟ CP_conf_FW03
□   ⊟ Network
□     ⊟ Interfaces
□         eth0
□         eth1
□         eth2
□         eth5
□         ethernet1/1
□     ⊟ Virtual Routers
□         chkpt-vr
□   ⊟ vsys1
□     ⊞ Objects
□     ⊞ Policies
□     ⊞ Zones
```

Base Configuration [OUTPUT]

```
⊟ PA-VM02_config.xml
  ⊟ Device
      vsys1
  ⊟ Network
      GlobalProtect IPSec Crypto
      IKE Crypto
      IKE Gateways
      IPSec Crypto
      IPSec Tunnels
      Interface Mgmt
      Interfaces
      Monitor Profile
      VLANs
      Virtual Routers
      Virtual Wires
```

On the right side we have Palo Alto and On the left we have CheckPoint

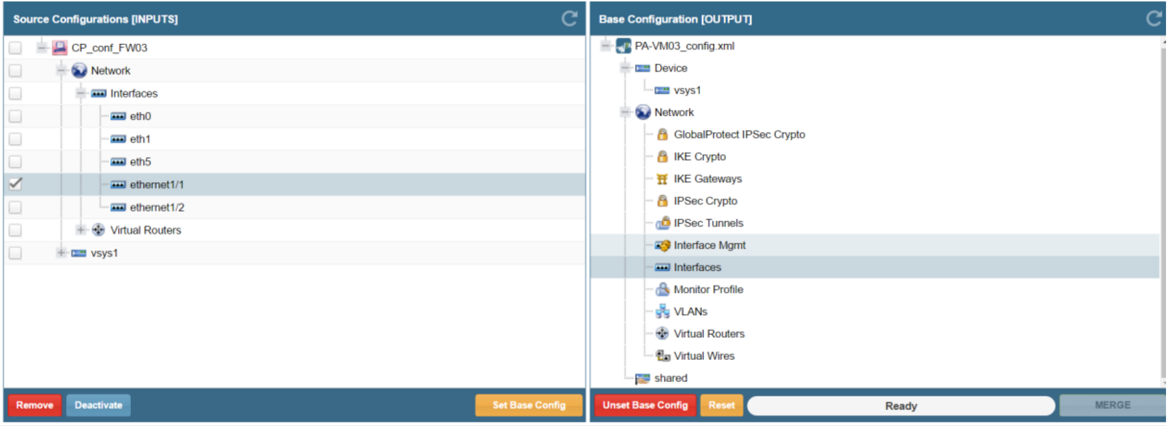
3.1.3. On the CheckPoint side click on the plus sign to open every directory

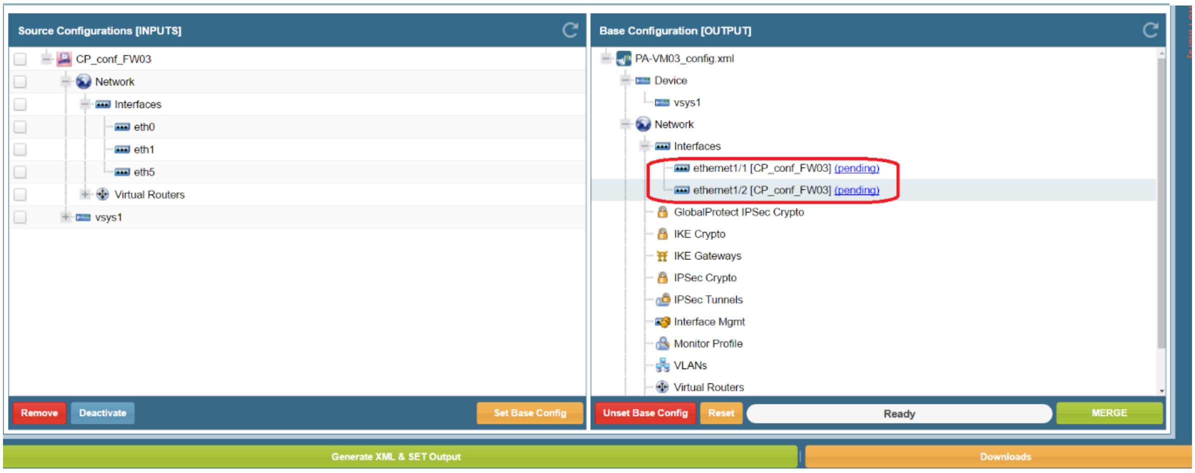


Source Configurations [INPUTS]

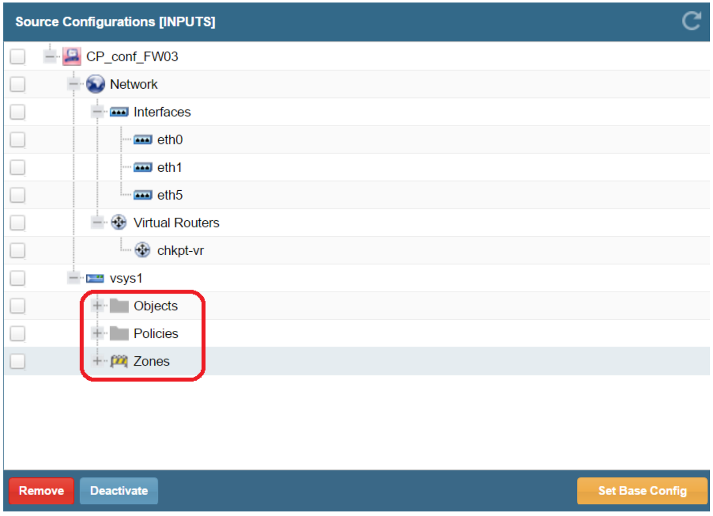
- CP_conf_FW03
  - Network
    - Interfaces
      - eth0
      - eth1
      - eth2
      - eth5
      - ethernet1/1
    - Virtual Routers
      - chkpt-vr
  - vsys1
    - Objects
    - Policies
    - Zones

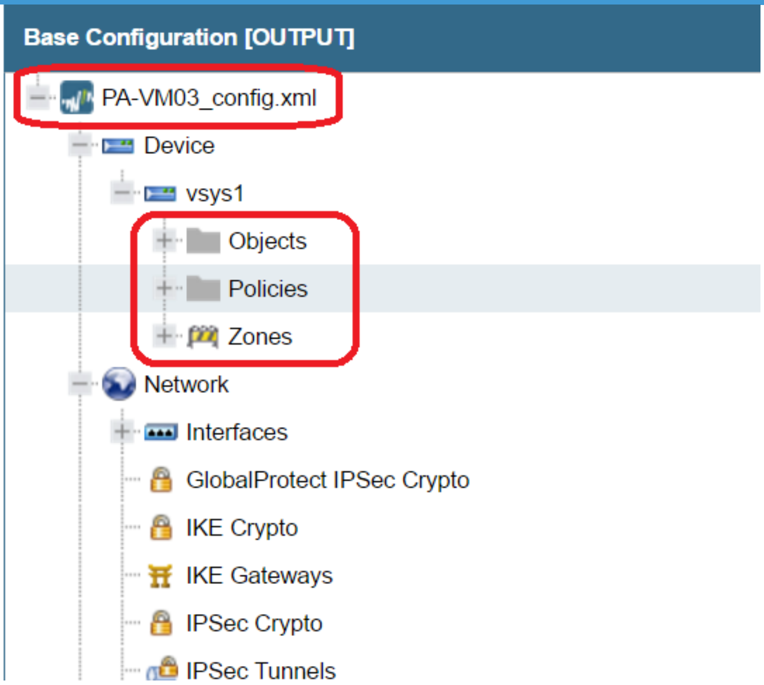
3.1.4. Now drug and drop every icon on the left to the right and place them at the correct location as example interfaces on the Check Point to the interfaces location on the Palo Alto as example in my case I need the ethernet1/1 and ethernet1/2 on the Palo Alto for my database to work so I place them in the Base Configuration on the right side





3.1.5. We need do the same for every object on the Check Point side and locate them at **Base Configuration** on the right side, the **Object**, **Policies**, **Zones** and VR if you needed.





Base Configuration [OUTPUT]

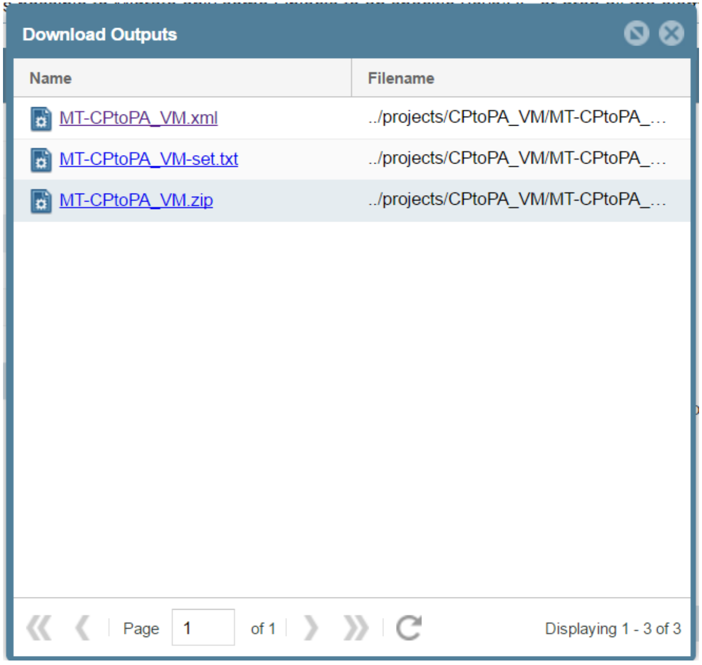
- PA-VM03_config.xml
  - Device
    - vsys1
      - Objects
      - Policies
      - Zones
  - Network
    - Interfaces
    - GlobalProtect IPSec Crypto
    - IKE Crypto
    - IKE Gateways
    - IPSec Crypto
    - IPSec Tunnels

3.2 Marge the file

3.2.1 Now click on the **MERGE** bottom.

3.2.2 Now click on **Generate XML & SET Output**, this will create a XML file that we use to import to the Palo Alto FW.

3.2.3 After it finish the **Download Output** window will popup and click on the XML file.



Download Outputs

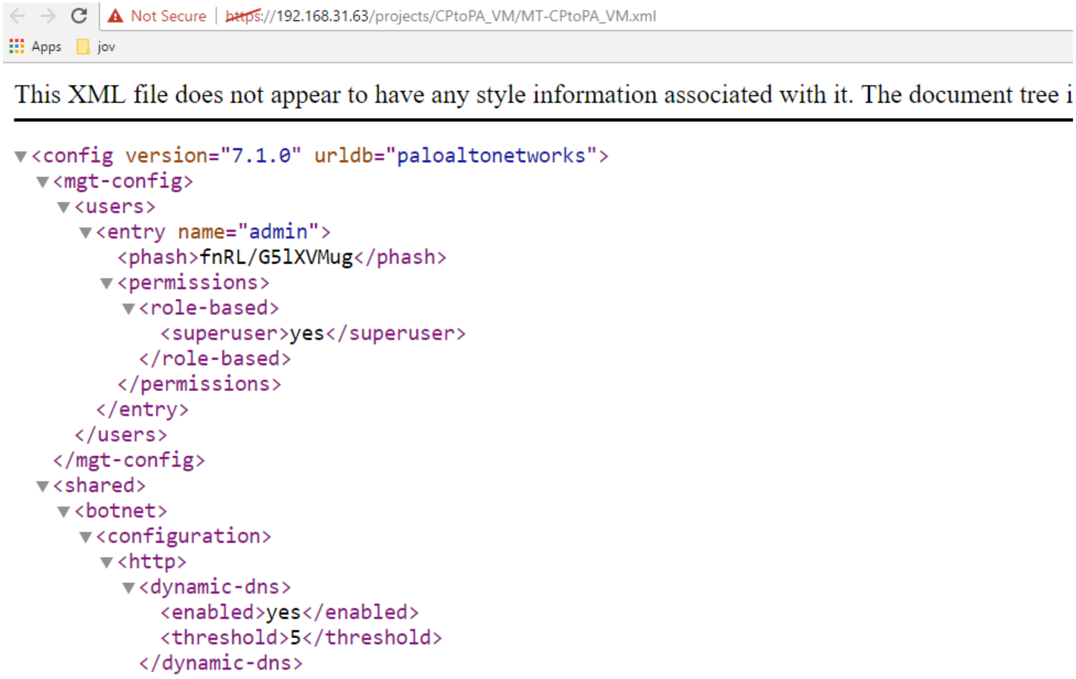
Name	Filename
MT-CPtoPA_VM.xml	../projects/CPtoPA_VM/MT-CPtoPA_...
MT-CPtoPA_VM-set.txt	../projects/CPtoPA_VM/MT-CPtoPA_...
MT-CPtoPA_VM.zip	../projects/CPtoPA_VM/MT-CPtoPA_...

Displaying 1 - 3 of 3

4 Upload the configuration file to Palo Alto FW

4.1 Now we need to import the file and load them, there is two ways to load the file, one way is to load the XML file immediately every setting and make complete change to the FW, the second way and the preferred one is to do so step by step carefully.

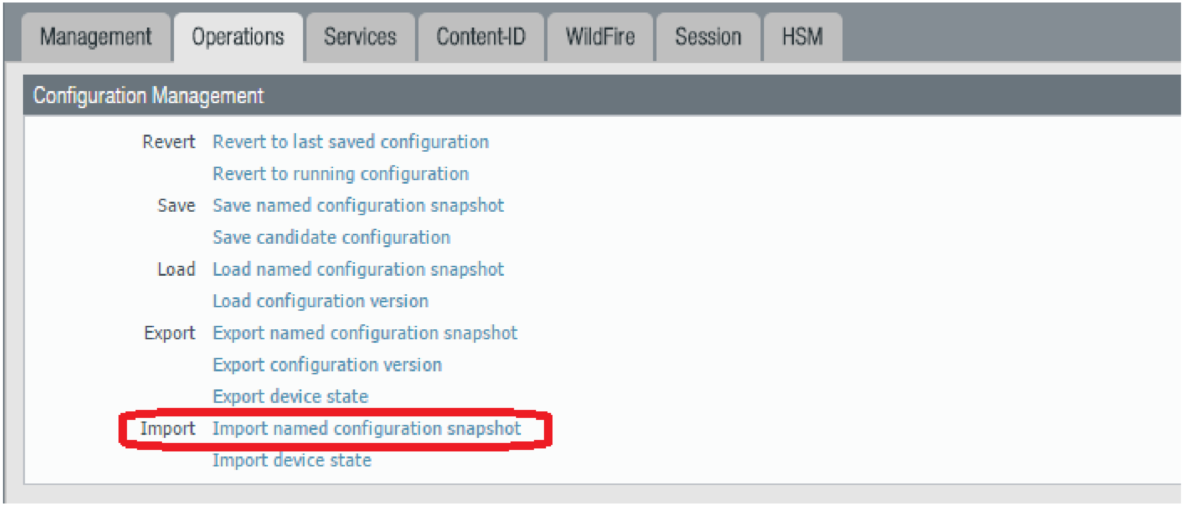
4.1.1 After you type on the XML file, it will open, so now we need to save the file on our machine.



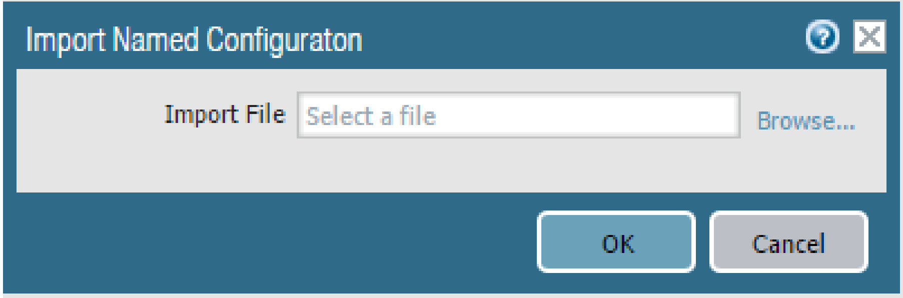
This XML file does not appear to have any style information associated with it. The document tree i

```
▼<config version="7.1.0" urldb="paloaltonetworks">
  ▼<mgt-config>
    ▼<users>
      ▼<entry name="admin">
          <phash>fnRL/G5lXVMug</phash>
        ▼<permissions>
          ▼<role-based>
              <superuser>yes</superuser>
            </role-based>
          </permissions>
        </entry>
      </users>
    </mgt-config>
  ▼<shared>
    ▼<botnet>
      ▼<configuration>
        ▼<http>
          ▼<dynamic-dns>
              <enabled>yes</enabled>
              <threshold>5</threshold>
            </dynamic-dns>
```

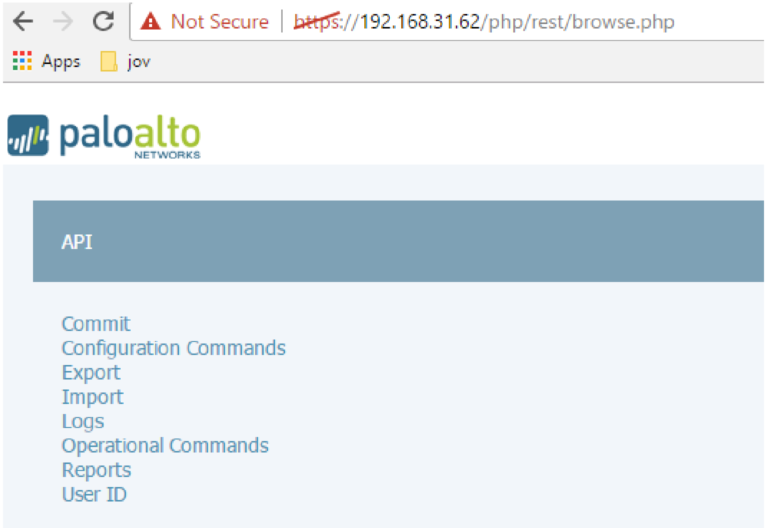
4.1.2 Now let's go to the PA FW to **Device>Setup>Operations** and click on **Import**.


Management
Operations
Services
Content-ID
WildFire
Session
HSM
Configuration Management
Revert
Revert to last saved configuration
Revert to running configuration
Save
Save named configuration snapshot
Save candidate configuration
Load
Load named configuration snapshot
Load configuration version
Export
Export named configuration snapshot
Export configuration version
Export device state
Import
Import named configuration snapshot
Import device state

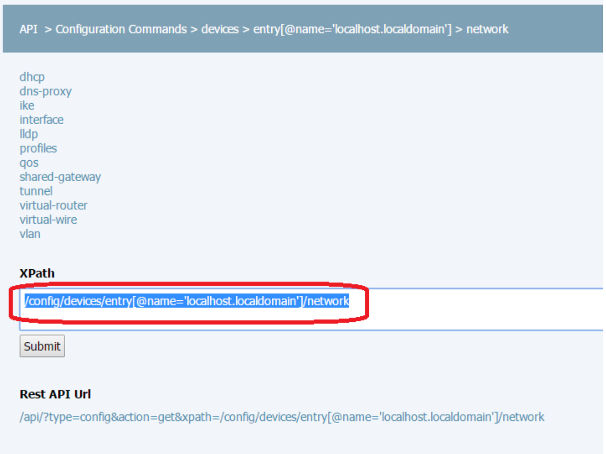
4.1.3 The **Import Named Configuration** window will popup and now browse to the CML file that we just created.



4.1.4 Now we can load the configuration to the machine, to do so just click on **Load named configuration,** but it will better if you don't load it to the machine directly because if you load it you just overload your files. Your VMs, IP address, Zones etc. so we don't want to do it, we just go to the command line and load partial configuration of that particular file and we going to put it in the FW. To do so we need to connect the API of the Palo Alto, just type the url and add **"/api"** to it:


Not Secure | ~~https~~://192.168.31.62/php/rest/browse.php

4.1.5 Now go to the configuration command to find the pieces we want to copy. In out example lets copy only the interfaces Configuration **Configuration Commands > devices > entry > network > interface > Ethernet** and copy the xPath.


API > Configuration Commands > devices > entry[@name='localhost.localdomain'] > network

XPath

/config/devices/entry[@name='localhost.localdomain']/network

Rest API Url

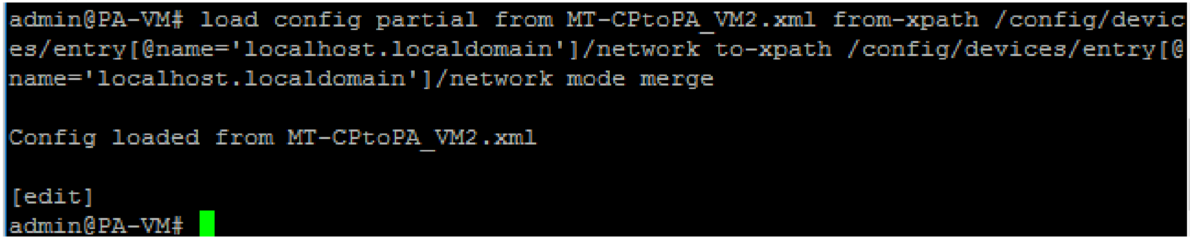
/api/?type=config&action=get&xpath=/config/devices/entry[@name='localhost.localdomain']/network

4.1.6 On the command prompt, type the command as follow:

#configure

#load config partial from <file name>.xml from-xpath <api path> to-xpath <api path> mode merge

In my case it will be:

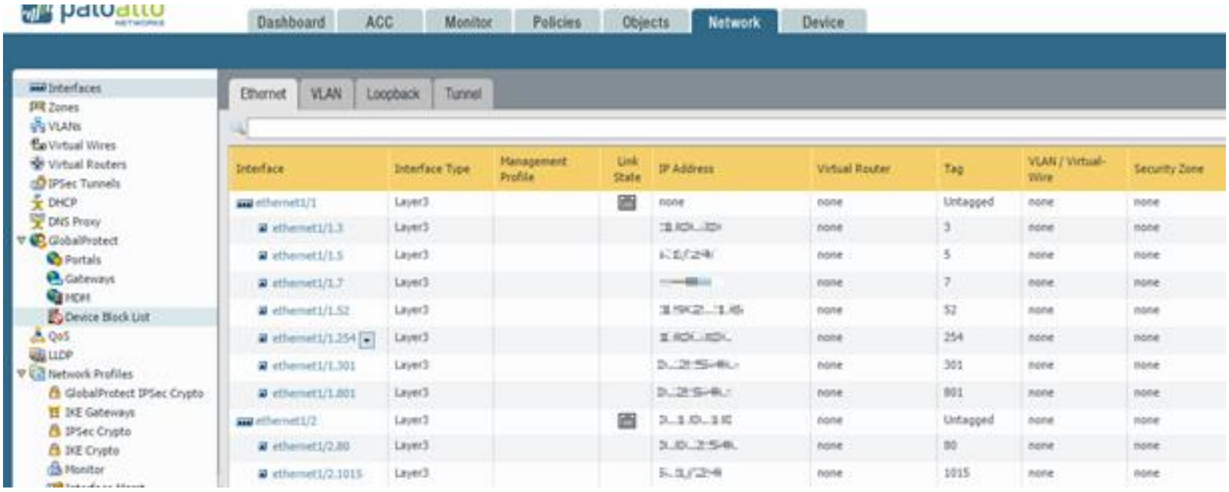


```
admin@PA-VM# load config partial from MT-CPtoPA_VM2.xml from-xpath /config/devic
es/entry[@name='localhost.localdomain']/network to-xpath /config/devices/entry[@
name='localhost.localdomain']/network mode merge

Config loaded from MT-CPtoPA_VM2.xml

[edit]
admin@PA-VM#
```

4.1.7 After it finish to load the configuration we will see them on the PA, and if it's look good we can click on commit.



Interface	Interface Type	Management Profile	Link State	IP Address	Virtual Router	Tag	VLAN / Virtual-Wire	Security Zone
ethernet1/1	Layer3		▣	none	none	Untagged	none	none
ethernet1/1.3	Layer3			[redacted]	none	3	none	none
ethernet1/1.5	Layer3			[redacted]	none	5	none	none
ethernet1/1.7	Layer3			[redacted]	none	7	none	none
ethernet1/1.52	Layer3			[redacted]	none	52	none	none
ethernet1/1.254	Layer3			[redacted]	none	254	none	none
ethernet1/1.301	Layer3			[redacted]	none	301	none	none
ethernet1/1.801	Layer3			[redacted]	none	801	none	none
ethernet1/2	Layer3		▣	[redacted]	none	Untagged	none	none
ethernet1/2.80	Layer3			[redacted]	none	80	none	none
ethernet1/2.1015	Layer3			[redacted]	none	1015	none	none

4.2 Now we do the same for every of the configuration that we created.

4.3 After you done to make the change you can do summery check on the Palo Alto FW and if it's look good I would say that you can do cut and over, please remember that there a lot of stuff that the MT3 can't do, you can read and refers to the next document, so before you do cut and over check that you apply on the PA every feature that you have on your Chack Point.

4.4 I hope this document will serve you well.