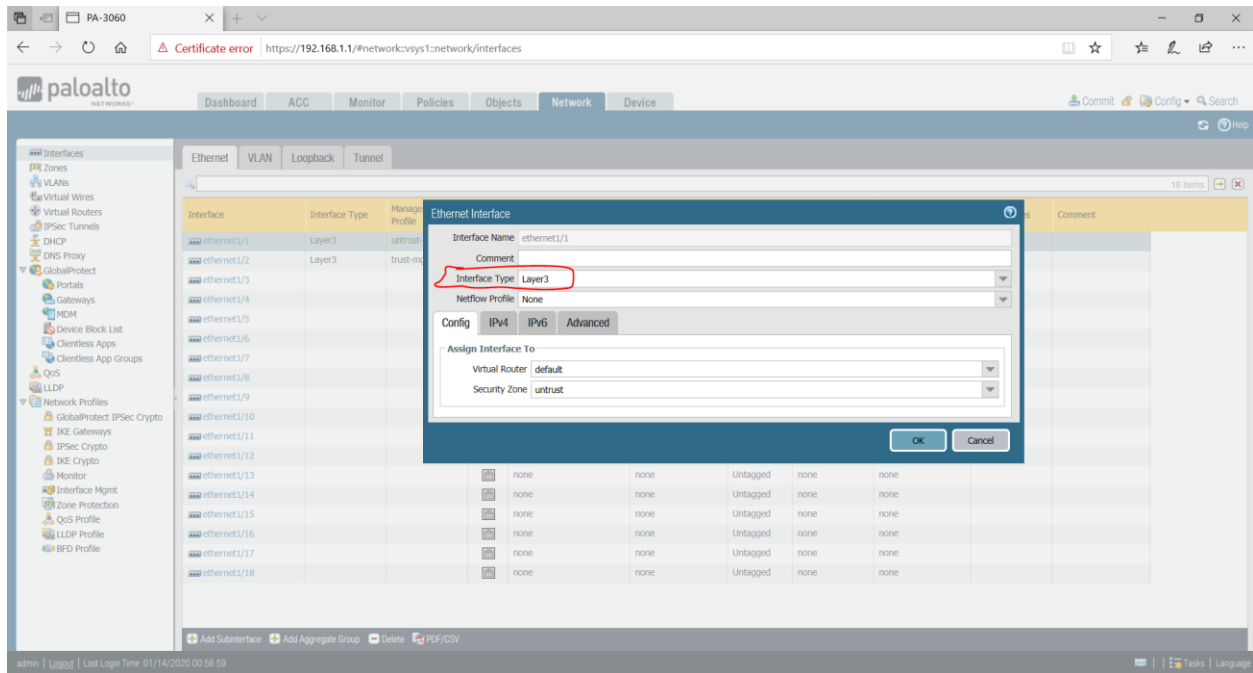
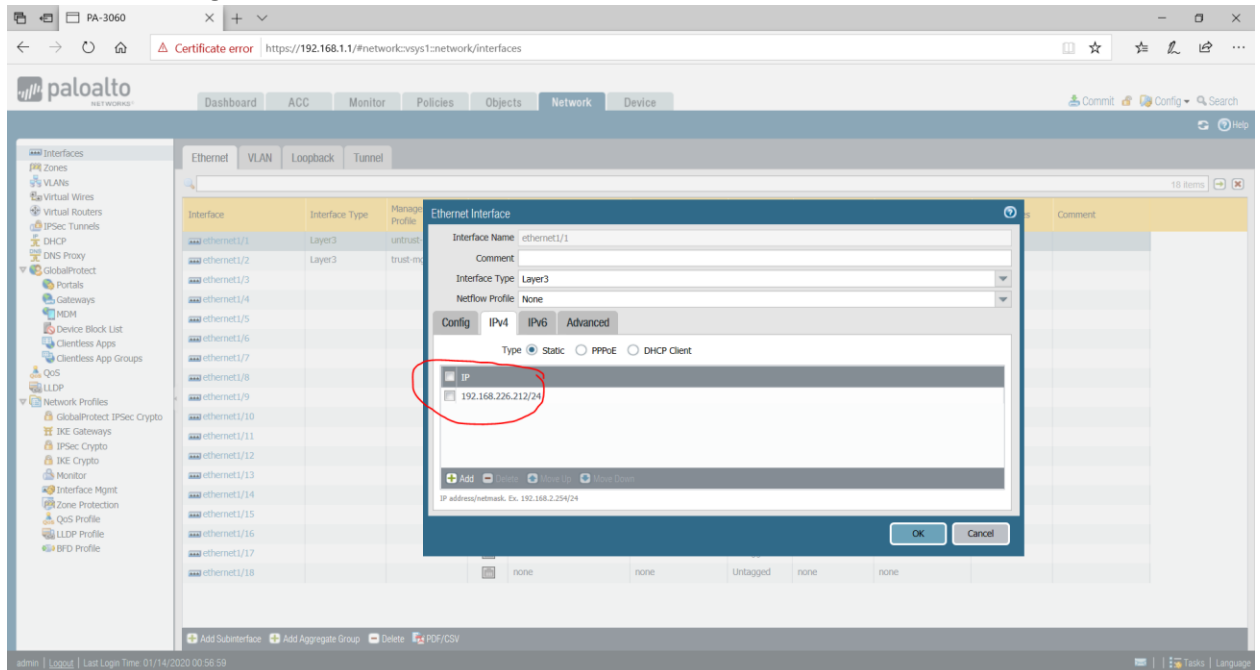


Palo Alto Firwall

1. Eerste wat moet wij doen is instellen van de WAN in de port 1

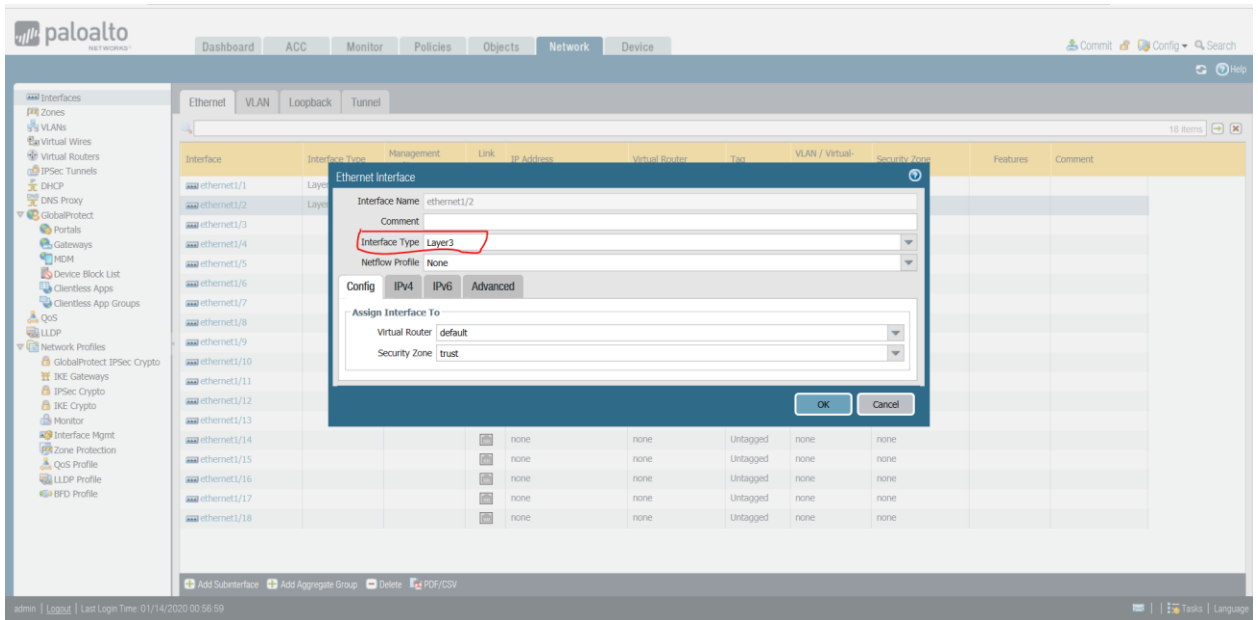


2. Static IP address geven:

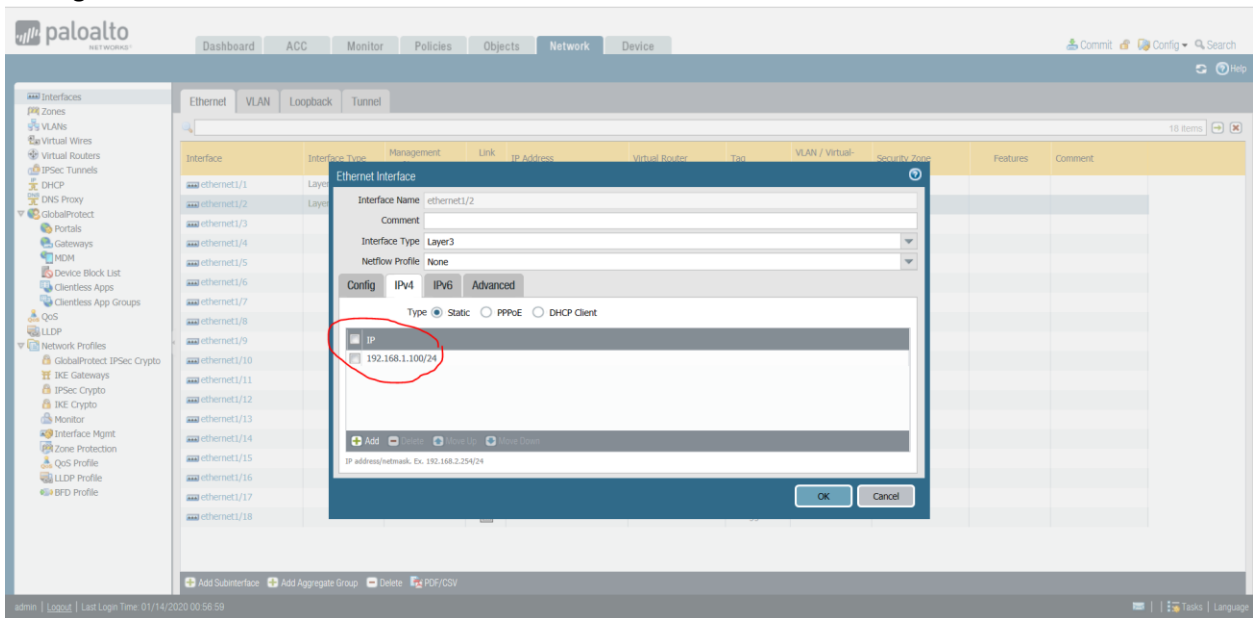


3. WAN instelleren in port 2:

Palo Alto Firewall

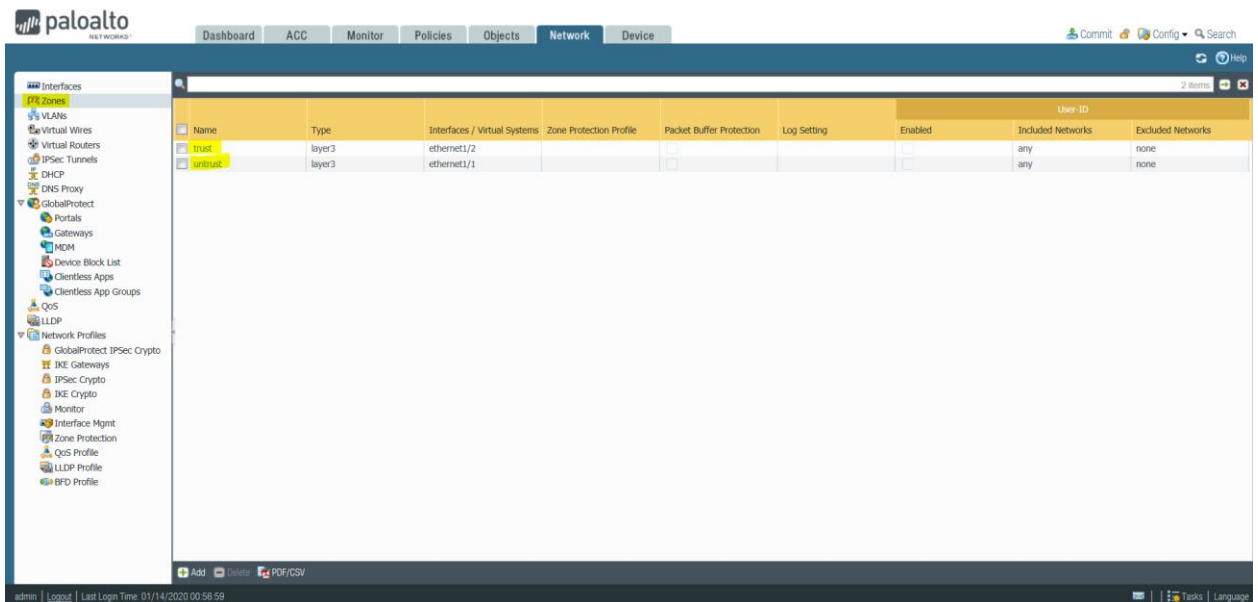


4. En nog een static IP address in stellen:

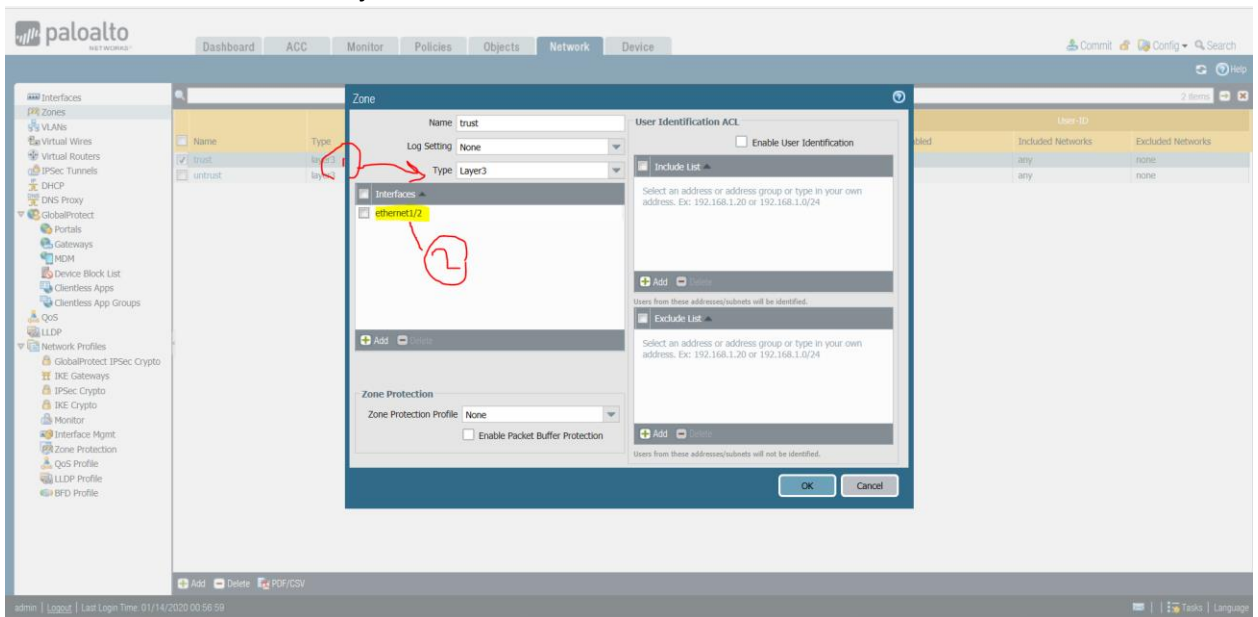


Palo Alto Firwall

5. Daar na begin wij met een zones te maken en wij maken een twee zonen in Trust en untrust:

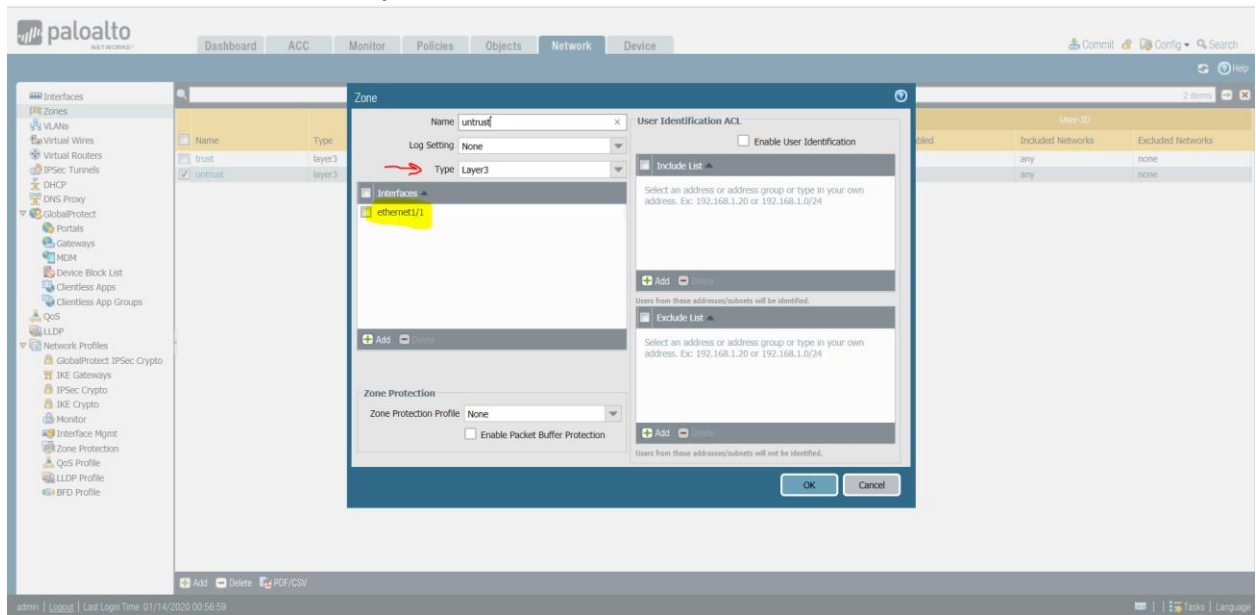


6. Voor die twee zonenhet staat default in en door dat kunnen wij het gewoon aanpassen :
7. Voor trust zone: hier zitten wij de LAN interface



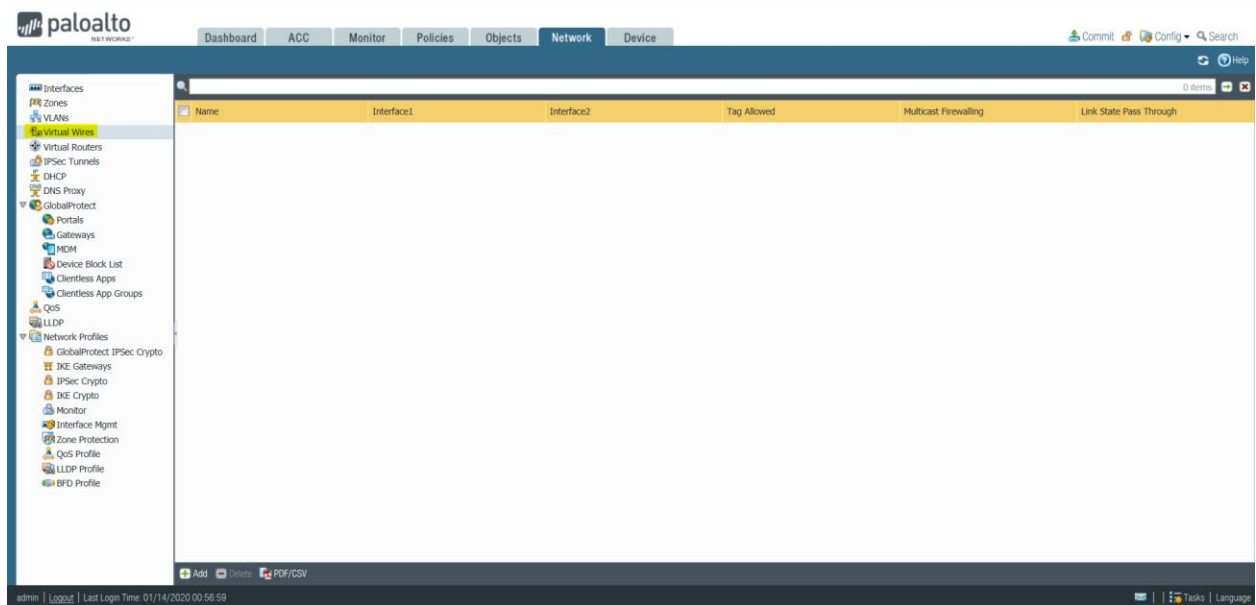
Palo Alto Firwall

8. Voor untrust zone: hier zitten wij de bese internet interface



9. Daarna zitten wij de zonen in de interface's voor trust zitten wij het in de interface ethernet 1/2 en voor utrust zitten wij het in de interface 1/1

10. Een belangrijk step die moet gedaan heb is de virtual wires deleten



11. En nu moeten wij een default gateway intellen en die :

Palo Alto Firewall

The screenshot displays the Palo Alto Networks management console interface. The left sidebar contains a navigation menu with categories like Interfaces, Virtual Wires, Virtual Routers (selected), IPSec, DHCP, DNS Proxy, GlobalProtect, Portals, Gateways, MDM, Device Block List, Clientless Apps, Clientless App Groups, QoS, LLDP, Network Profiles, GlobalProtect IPSec Crypto, IKE Gateways, IPSec Crypto, IKE Crypto, Monitor, Interface Mgmt, Zone Protection, QoS Profile, LLDP Profile, and BFD Profile. The main content area shows the 'Virtual Routers' configuration page. A table lists the configuration for a router named 'default'. The table has columns for Name, Interfaces, Configuration, RIP, OSPF, OSPFv3, BGP, Multicast, and Runtime Stats. The 'default' router is configured with interfaces ethernet1/1, ethernet1/2, and loopback. The configuration shows Static Routes: 1 and ECHP status: Disabled. The bottom status bar shows the user is 'admin' and the last login time was '01/14/2020 00:58:59'.

Name	Interfaces	Configuration	RIP	OSPF	OSPFv3	BGP	Multicast	Runtime Stats
default	ethernet1/1 ethernet1/2 loopback	Static Routes: 1 ECHP status: Disabled						More Runtime Stats

admin | [Logout](#) | Last Login Time: 01/14/2020 00:58:59

Palo Alto Firewall

The screenshot shows the Palo Alto Firewall configuration interface. The left sidebar contains a tree view of configuration objects, including Interfaces, Zones, Virtual Wires, Virtual Routers, IPsec Tunnels, DHCP, DNS Proxy, GlobalProtect, Portals, Gateways, MDM, Device Block List, Clientless Apps, Clientless App Groups, QoS, LLDP, Network Profiles, GlobalProtect IPsec Crypto, IKE Gateways, IPsec Crypto, IKE Crypto, Monitor, Interface Mgmt, Zone Protection, QoS Profile, LLDP Profile, and BFD Profile. The main pane displays the 'Virtual Router - default' configuration. The 'Static Routes' tab is selected, showing a list of static routes. The 'Administrative Distances' tab is also visible, showing a list of administrative distances for various protocols.

Virtual Router - default

Router Settings

Static Routes

Redistribution Profile

RIP

OSPF

OSPFv3

BGP

Multicast

General

ECMP

Administrative Distances

Static 10

Static IPv6 10

OSPF Int 30

OSPF Ext 110

OSPFv3 Int 30

OSPFv3 Ext 110

IBGP 200

EBGP 20

RIP 120

The screenshot shows the Palo Alto Firewall configuration interface. The left sidebar contains a tree view of configuration objects, including Interfaces, Zones, Virtual Wires, Virtual Routers, IPsec Tunnels, DHCP, DNS Proxy, GlobalProtect, Portals, Gateways, MDM, Device Block List, Clientless Apps, Clientless App Groups, QoS, LLDP, Network Profiles, GlobalProtect IPsec Crypto, IKE Gateways, IPsec Crypto, IKE Crypto, Monitor, Interface Mgmt, Zone Protection, QoS Profile, LLDP Profile, and BFD Profile. The main pane displays the 'Virtual Router - default' configuration. The 'Static Routes' tab is selected, showing a list of static routes. The 'IPv4' tab is also visible, showing a list of static routes. The 'IPv6' tab is also visible, showing a list of static routes.

Virtual Router - default

Router Settings

Static Routes

Redistribution Profile

RIP

OSPF

OSPFv3

BGP

Multicast

IPv4

IPv6

Name	Destination	Interface	Type	Value	Admin Distance	Metric	BFD	Route Table
DC	0.0.0.0/0		ip-address	192.168...	default	10	None	unicast

Palo Alto Firewall

Virtual Router - Static Route - IPv4

Name

Destination

Interface

Next Hop

Admin Distance

Metric

Route Table

BFD Profile

☐ Path Monitoring

Failure Condition ☒ Any ☐ All Preemptive Hold Time (min)

<input type="checkbox"/>	Name	Enable	Source IP	Destination IP	Ping Interval(sec)	Ping Count

De next hop IP address is de virtual IP address die alle gebruiker die willen naar de internet surfen , krijgen die IP address om te surfen

12. En daar na maken wij twee interface mangement door:

Palo Alto Firewall

The screenshot shows the Palo Alto Firewall configuration interface. The top navigation bar includes tabs for Dashboard, ACC, Monitor, Policies, Objects, **Network**, and Device. The left sidebar contains a tree view of configuration objects, with 'Interface Mgmt' highlighted. The main content area displays a table of interface configurations.

Name	Ping	Telnet	SSH	HTTP	HTTP OCSP	HTTPS	SNMP	Response Pages	User-ID	User-ID Syslog Listener-SSL	User-ID Syslog Listener-UDP	Permitted IP Addresses
trust-mgt	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
untrust-mgt	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

Below the table, the 'Interface Management Profile' configuration window is open for the 'trust-mgt' interface. It shows the following settings:

- Name:** trust-mgt
- Administrative Management Services:**
 - ☒ HTTP
 - ☒ HTTPS
 - ☐ Telnet
 - ☒ SSH
- Network Services:**
 - ☒ Ping
 - ☐ HTTP OCSP
 - ☐ SNMP
 - ☐ Response Pages
 - ☐ User-ID
 - ☐ User-ID Syslog Listener-SSL
 - ☐ User-ID Syslog Listener-UDP
- Permitted IP Addresses:** (Empty list)

At the bottom of the configuration window, there are 'Add' and 'Delete' buttons, and a text box showing examples of IP addresses: 'Ex. IPv4 192.168.1.1 or 192.168.1.0/24 or IPv6 2001:db8:123:1::1 or 2001:db8:123:1::/64'. The window has 'OK' and 'Cancel' buttons at the bottom right.

Bij deze interface zitten wij alle diens die mogen de gebruiker in trust zone maken

Palo Alto Firewall

Interface Management Profile

Name

Administrative Management Services

☐ HTTP

☐ HTTPS

☐ Telnet

☐ SSH

Network Services

☒ Ping

☐ HTTP OSCP

☐ SNMP

☐ Response Pages

☐ User-ID

☐ User-ID Syslog Listener-SSL

☐ User-ID Syslog Listener-UDP

Permitted IP Addresses

Ex. IPv4 192.168.1.1 or 192.168.1.0/24 or IPv6 2001:db8:123:1::1 or 2001:db8:123:1::/64

+ Add - Delete

OK Cancel

Bij deze interface zitten wij alle diens die mogen de gebruiker in untrust zone maken
13. En nu meten wij configureren het in de interfaces en die gebeurt :

paloalto NETWORKS

Dashboard ACC Monitor Policies Objects **Network** Device

Interfaces

Ethernet VLAN Loopback Tunnel

Interface ethernet1/1

Interface Name ethernet1/1

Comment

Interface Type Layer3

Netflow Profile None

Config IPv4 IPv6 **Advanced**

Link Settings

Link Speed auto Link Duplex auto Link State auto

Other Info ARP Entries ND Entries NDP Proxy LLDP

Management Profile untrust-mgt

MTU 1576 - 1500

☐ Adjust TCP MSS

IPv4 MSS Adjustment 40

IPv6 MSS Adjustment 60

☐ Untagged Subinterface

OK Cancel

admin | Logout | Last Login Time: 01/14/2020 00:56:59

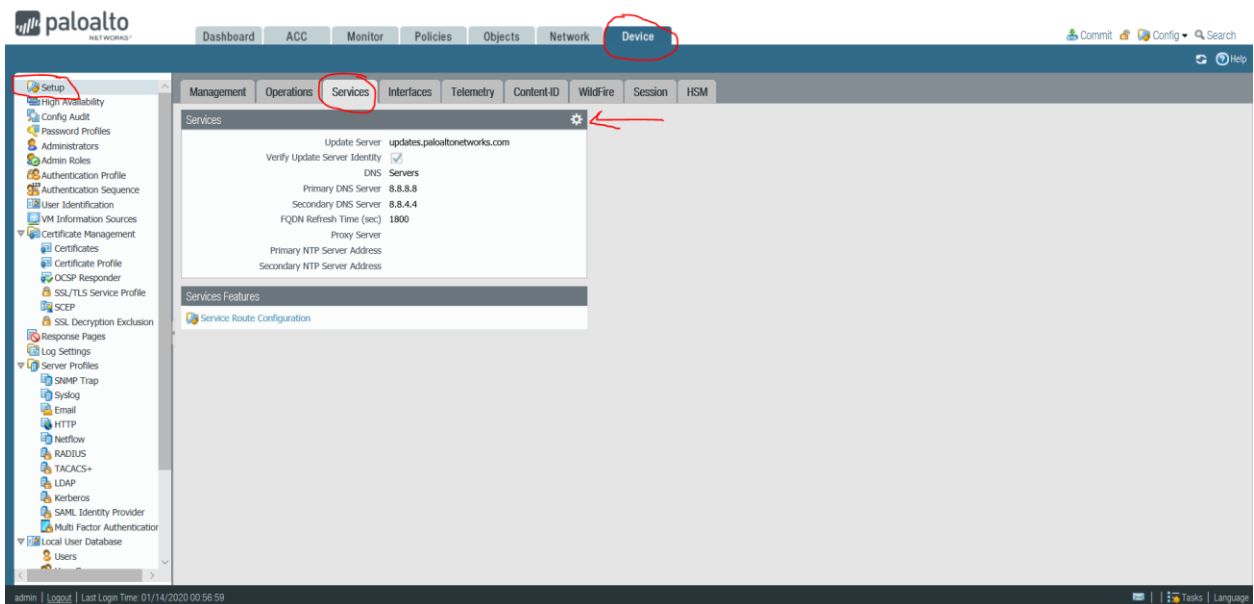
Tasks Language

Palo Alto Firewall

Nu alle gebruiker die zitten in de untrust zone (de gebruiker die zitten in de bese internet) kunnen allen de netwerk pingen en kunnen zij niks ander.

The screenshot shows the 'Ethernet Interface' configuration page. The 'Interface Name' is 'ethernet1/2'. The 'Interface Type' is 'Layer3'. The 'Netflow Profile' is 'None'. The 'Advanced' tab is selected, showing 'Link Settings' with 'Link Speed' set to 'auto', 'Link Duplex' set to 'auto', and 'Link State' set to 'auto'. Below this, the 'Other Info' tab is selected, showing 'Management Profile' set to 'trust-mgt' and 'MTU' set to '[576 - 1500]'. There are checkboxes for 'Adjust TCP MSS' (unchecked), 'IPv4 MSS Adjustment' (set to 40), and 'IPv6 MSS Adjustment' (set to 60). There is also an unchecked checkbox for 'Untagged Subinterface'. At the bottom right are 'OK' and 'Cancel' buttons.

14. Voor update de system moeten wij eerste een DNS instellen:



Palo Alto Firewall

Services

Services NTP

Update Server updates.paloaltonetworks.com

☒ Verify Update Server Identity

DNS Settings

DNS ☒ Servers ☐ DNS Proxy Object

Primary DNS Server 8.8.8.8

Secondary DNS Server 8.8.4.4

FQDN Refresh Time (sec) 1800

Proxy Server

Server

Port [1 - 65535]

User

Password

Confirm Password

OK Cancel

In de primary DNS server kunnen wij de IP address van de Actiev Directory server zitten en in de secondary de google ip address.