OPNsense Firewall

Firewall > Aliases

	PrivateNetworks	HomeAssistantServer	AdminPCs
Enabled	**Checked**	**Checked**	**Checked**
Name	**PrivateNetworks**	**HomeAssistantServer**	**AdminPCs**
Type	**Network(s)**	**Host(s)**	**Host(s)**
Categories			
Content	**__lan_network, __opt1_network, __opt2_network,__opt3_network**	**192.168.120.8**	**192.168.110.16-192.168.110.24**
Statistics	**Unchecked**	**Unchecked**	**Unchecked**
Description	**All my local networks**	**Home Assistant Server for Train software**	**PC that can manage network item**

Firewall > NAT > Port Forward

!!!! These rules are only for testing at home, from my workplace, so it is easier to create documentation.
!!! Important they must be disabled or deleted during installation.

Server	**OPNsense**	**HPE 1820**	**Home Assistant**
Disabled	**Checked**	**Checked**	**Checked**
No RDR (NOT)	Unchecked	Unchecked	Unchecked
Interface	**WAN**	**WAN**	**WAN**
TCP/IP Version	**IPv4**	**IPv4**	**IPv4**
Protocol	**TCP**	**TCP**	**TCP**
Destination / Invert	Unchecked	Unchecked	Unchecked
Destination	**WAN address**	**WAN address**	**WAN address**
Destination port range from:	**HTTP**	**8080**	**8123**
Destination port range to:	**HTTP**	**8080**	**8123**
Redirect target IP	**Single host or Network**	**Single host or Network**	**Single host or Network**
	192.168.101.1	**192.168.101.2**	**192.168.120.8**

Server	OPNsense	HPE 1820	Home Assistant
Redirect target port	**HTTP**	**HTTP**	**8123**
Pool Options:	Default	Default	Default
Log	Unchecked	Unchecked	Unchecked
Category			
Description	**Nat to OPNsense**	**Nat to HPE 1820**	**Nat to Home Assistant**
Set local tag			
Match local tag			
No XMLRPC Sync	Unchecked	Unchecked	Unchecked
NAT reflection	Use system default	Use system default	Use system default
Filter rule association	**Pass**	**Pass**	**Pass**

Firewall > Rules > WAN

Only Automatically generated rules here

Firewall > Rules > LAN > Default settings

This roles wil bee disabled and replaced wit 3 new roles see below

Option	Input	Comment
Action	Pass	
Disabled	Unchecked	Disable this rule
Quick	Unchecked	Apply the action immediately on match.
Interface	LAN	
Direction	in	
TCP/IP Version	IPv4	
Protocol	any	
Source / Invert	Unchecked	Use this option to invert the sense of the match.
Source	LANviaUSB net	

Source |Destination / Invert|Unchecked|Use this option to invert the sense of the match.| |Destination|any|| |Destination port range from:|any|| |Destination port range to:|any|| |Log|Unchecked|Log packets that are handled by this rule| |Category||| |Description|Default allow LAN to any rule|| |No XMLRPC Sync|Unchecked|| |Schedule|none|| |Gateway|default||

Firewall > Rules > LAN

1.

Option	DNS	NTP Time	ICMP	HomeAssistant
Action	**Pass**	**Pass**	**Pass**	**Pass**
TCP/IP Version	**IPv4**	**IPv4**	**IPv4**	**IPv4**
Protocol	**TCP/UDP**	**UDP**	**ICMP**	**TCP**
Source	**LAN net**	**LAN net**	**LAN net**	**AdminPCs**
Destination / Invert	**Unchecked**	**Unchecked**	**Unchecked**	**Unchecked**
Destination	**LAN address**	**LAN address**	**any**	**HomeAssistantServer**
Destination port range from:	**DNS**	**NTP**	**any**	**(other) 8123**
Destination port range to:	**DNS**	**NTP**	**any**	**(other) 8123**
Description	**Allow access to DNS**	**Allow access to NTP**	**Allow ICMPv4 from LAN to all network**	**Allow access for Admins to Home Assistant server**

2.

Option	Access only to Internet
Action	**Pass**
TCP/IP Version	**IPv4**
Protocol	**any**
Source	**LAN net**
Destination / Invert	**Checked**
Destination	**PrivateNetworks**
Destination port range from:	**any**
Destination port range to:	**any**
Description	**Allow access only to Internet**

Firewall > Rules > Office

Option	DNS	NTP Time	Access only to Internet
Action	**Pass**	**Pass**	**Pass**

Option	DNS	NTP Time	Access only to Internet
TCP/IP Version	**IPv4**	**IPv4**	**IPv4**
Protocol	**TCP/UDP**	**UDP**	**any**
Source	**LAN net**	**LAN net**	**LAN net**
Destination / Invert	**Unchecked**	**Unchecked**	**Checked**
Destination	**LAN address**	**LAN address**	**PrivateNetworks**
Destination port range from:	**DNS**	**NTP**	**any**
Destination port range to:	**DNS**	**NTP**	**any**
Description	**Allow access to DNS**	**Allow access to NTP**	**Allow access only to Internet**

Firewall > Rules > Train

Option	DNS	NTP Time	Home Assistatnt
Action	**Pass**	**Pass**	**Pass**
TCP/IP Version	**IPv4**	**IPv4**	**IPv4**
Protocol	**TCP/UDP**	**UDP**	**any**
Source	**LAN net**	**LAN net**	**192.168.120.8**
Destination / Invert	**Unchecked**	**Unchecked**	**Checked**
Destination	**LAN address**	**LAN address**	**PrivateNetworks**
Destination port range from:	**DNS**	**NTP**	**any**
Destination port range to:	**DNS**	**NTP**	**any**
Description	**Allow access to DNS**	**Allow access to NTP**	**Allow HA Server access only to Internet**

Firewall > Rules > IPCam