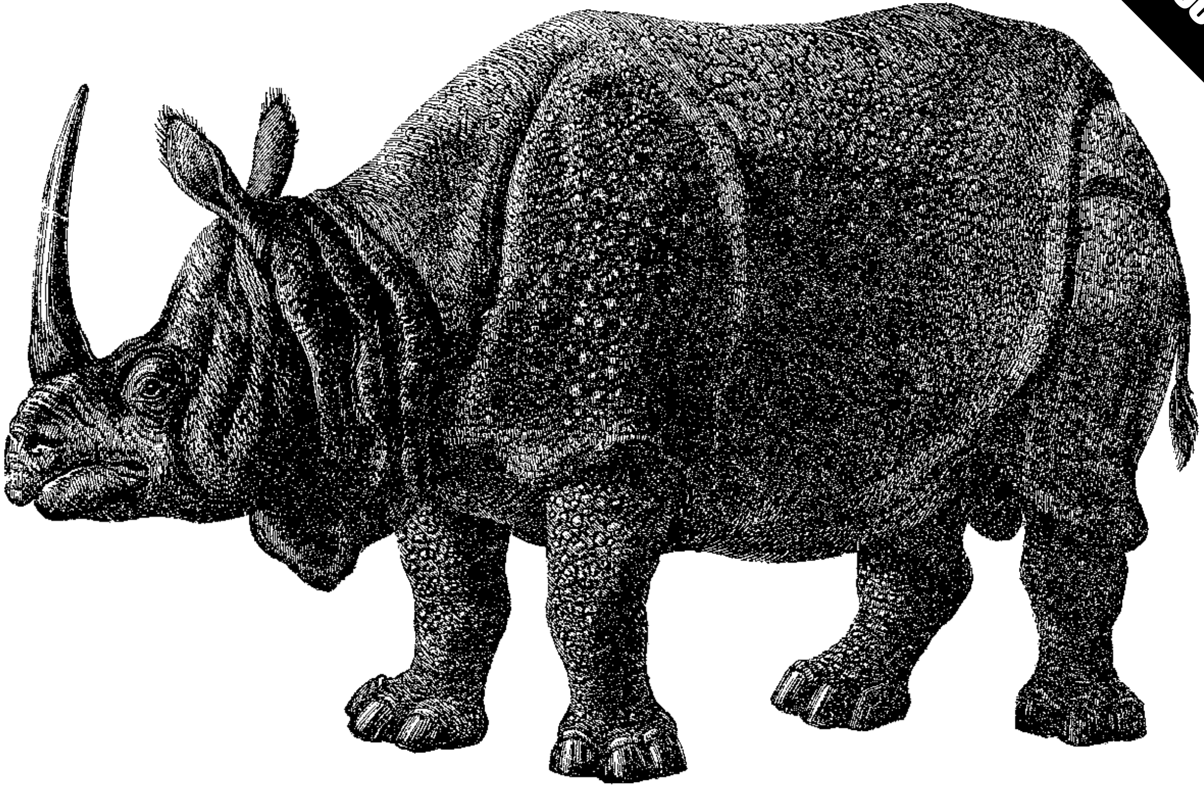
The lean security administrators favorite tool

GAiA EDITION
Updated for R77.30



Always updated firewall documentation with

UNIfw1doc

i2

Niels Thomas Haugård
& Nicolai Ernst

Table of Contents

Table of Contents 1
Introduction 2
How does UNIfw1doc work 2
What not to expect from UNIfw1doc 2
Using UNIfw1doc 3
Known problems and limitations 6
How to solve problems 6
Note 6

Introduction

UNIfw1doc - *UNI•C FireWall-1 automated documentation tool* - is a simple automated firewall documentation tool for Check Point firewall-1 made by UNI•C.

UNIfw1doc version 1.0 is compatible with GAiA and has been tested on Check Point R77.10, R77.20 and R77.30, and should work with all later R77.x versions, both appliances and open servers.

UNIfw1doc should be installed on the management station. It uses Check Point's Web visualization tool (SK64501) and a number of other utilities.

UNIfw1doc is free software and released under a modified BSD License, see LICENSE. Using the software requires a valid support contract with Check Point Technologies. **UNIfw1doc** is installed as an rpm package .

UNIfw1doc requires an application to render the Check Point configuration, and works with both *cpdb2web* from Check Point and *CPrules*. Either has to be installed separately, as described in the installation documentation.

Check Point **cpdb2web** may be download from supportcenter.checkpoint.com, search for **sk64501** and download *R77.x for Gaia / SecurePlatform / Linux* .

cpdb2web does not require a separate license, but may fail to execute if an GUI is open.

Create the directory `/var/opt/UNIfw1doc/cp_webviz_tool`, unpack the archive there with `tar xvfpz cpdb2web*gz`.

Notice the documentation created with cpdb2web requires Firefow for best viewing. (not html but xml files)

CPrules may be downloaded from here Create the directory `/var/opt/UNIfw1doc/CPrules`, unpack CPRules.tar.gz and move all files to `/var/opt/UNIfw1doc/CPrules`.

How does UNIfw1doc work

UNIfw1doc has two components:

- A SSL enabled Web Service (the server is part of the base operating system) for serving the documentation.
- An application that every 15 min. test for changes to the rule base and generates new documentation, while keeping track of all past changes and versions.

Please notice that the documentation cannot be directly converted back to the firewall, and that all changes made within 15 min. is documented as one final change not a set of individual changes.

What not to expect fromUNIfw1doc

UNIfw1doc is a simple *audit tool*, visualizing information already available through the firewall GUI, while keeping track of historical changes. It is not a tool for roll-back. It processes the available information and relies on it. If you do not trust your firewall administrator **UNIfw1doc** will not help you.

Using UNIfw1doc

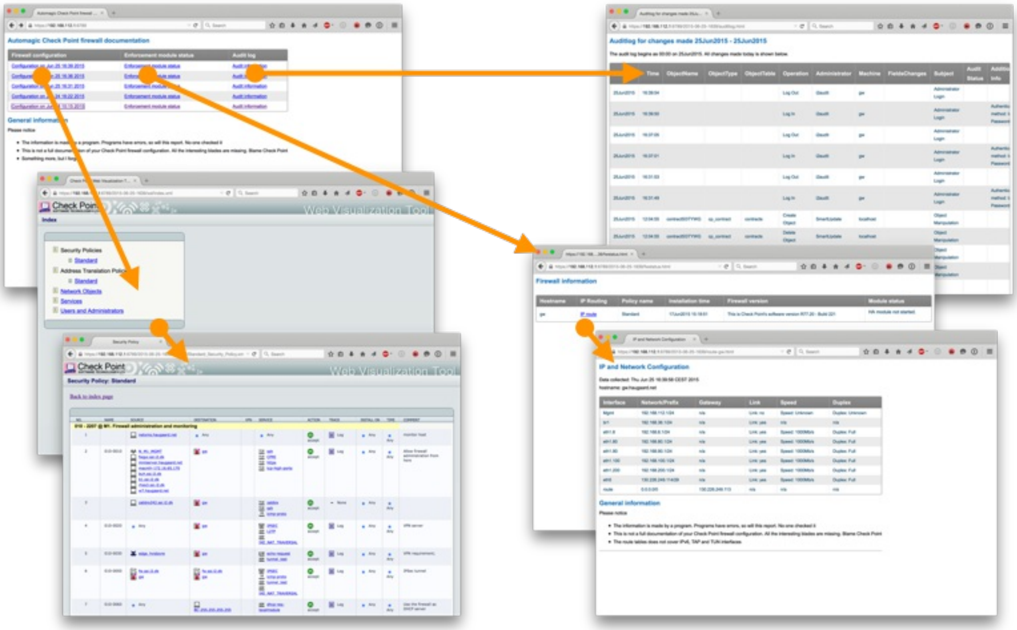
UNIfw1doc is accessed though a browser with SSL on TCP port **6789** on the management station's IP address:

```
https://a.b.c.d:6789
```

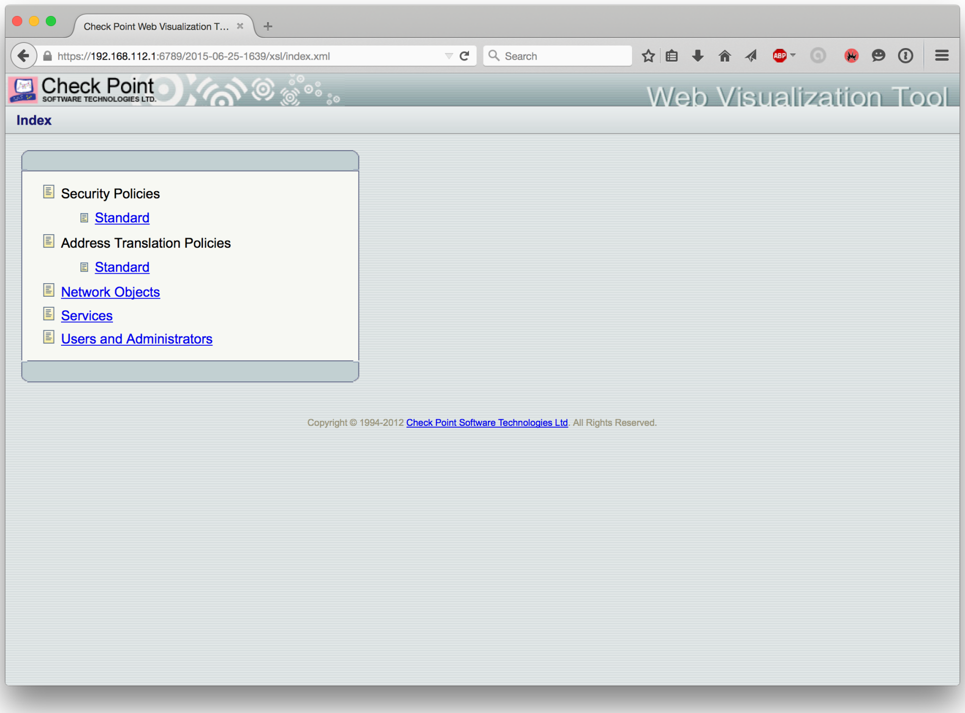
The server uses the firewall's certificate (usually a self-signed SSL certificate which will cause a browser warning).

The **main page** shows documentation for each detected change, with the newest changes at the top. Each line in the table has tree links describing how the firewall was configured at a specific point in time.

- The **Firewall Configuration** (first field) links to the firewall configuration (rule base etc.)
- The **Enforcement module status** (second field) links to firewall version, IP and route info, installed rule base and installation time, while
- The **Audit log** (third field) shows the exported audit information.


Automagic Check Point firewall documentation
Firewall configuration
Enforcement module status
Audit log
General information
Check Point
Web Visualization Tool
Index
Security Policies
Standard
Address Translation Policy
Auditlog for changes made 25Jun2015 - 25Jun2015
Firewall information
IP and Network Configuration
General information

The time stamp in the first column - Firewall configuration - links to a HTML version of the defined rule bases, with NAT, objects, users and administrators. The documentation is made with Check Point's Web Visualization Tool (see SK64501).

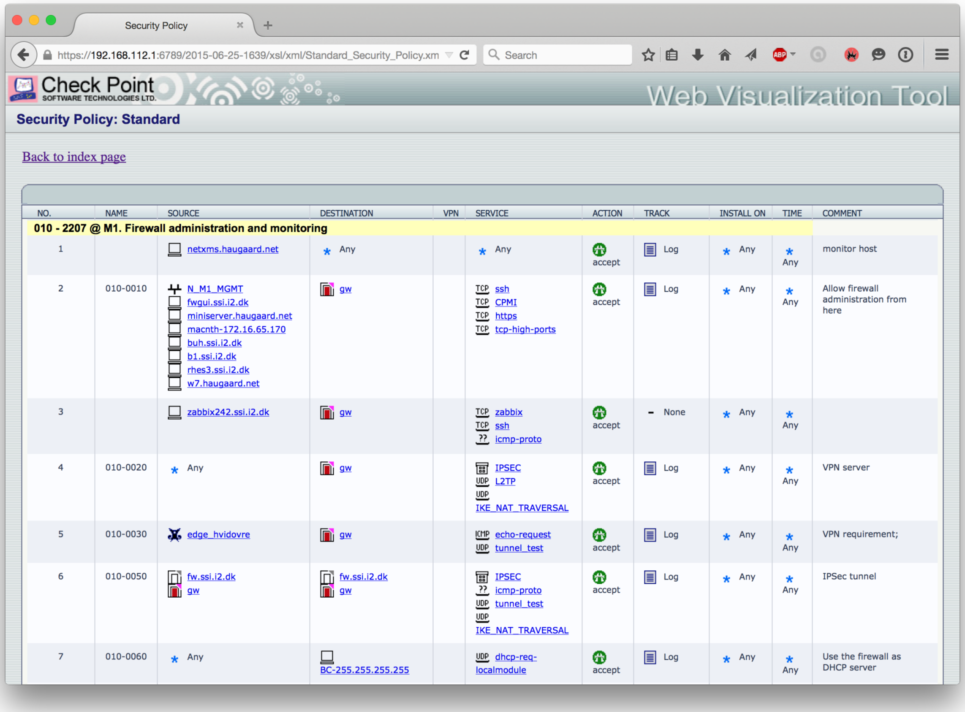

Check Point Web Visualization T...
https://192.168.112.1:6789/2015-06-25-1639/xsl/index.xml
Search
Check Point
SOFTWARE TECHNOLOGIES LTD.
Web Visualization Tool

Index

- Security Policies
  - Standard
- Address Translation Policies
  - Standard
- Network Objects
- Services
- Users and Administrators

Copyright © 1994-2012 Check Point Software Technologies Ltd. All Rights Reserved.

The rule base may look like this example.


Security Policy
https://192.168.112.1:6789/2015-06-25-1639/xsl/xml/Standard_Security_Policy.xm
Search
Check Point
SOFTWARE TECHNOLOGIES LTD.
Web Visualization Tool

Security Policy: Standard

Back to index page

NO.	NAME	SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK	INSTALL ON	TIME	COMMENT
010 - 2207 @ M1. Firewall administration and monitoring										
1		netxms.haugaard.net	* Any		* Any	accept	Log	* Any	* Any	monitor host
2	010-0010	N_M1_MGMT fwgui.ssi.i2.dk miniserver.haugaard.net macnth-172.16.65.170 buh.ssi.i2.dk b1.ssi.i2.dk rhes3.ssi.i2.dk w7.haugaard.net	gw		TCP ssh TCP CPMI TCP https TCP tcp-high-ports	accept	Log	* Any	* Any	Allow firewall administration from here
3		zabbix242.ssi.i2.dk	gw		TCP zabbix TCP ssh ?? icmp-proto	accept	- None	* Any	* Any	
4	010-0020	* Any	gw		IPSEC UDP L2TP UDP IKE_NAT_TRAVERSAL	accept	Log	* Any	* Any	VPN server
5	010-0030	edge_hvidovre	gw		ICMP echo-request UDP tunnel_test	accept	Log	* Any	* Any	VPN requirement;
6	010-0050	fw.ssi.i2.dk gw	fw.ssi.i2.dk gw		IPSEC ?? icmp-proto UDP tunnel_test UDP IKE_NAT_TRAVERSAL	accept	Log	* Any	* Any	IPSec tunnel
7	010-0060	* Any	BC-255.255.255.255		UDP dhcp-req-localmodule	accept	Log	* Any	* Any	Use the firewall as DHCP server

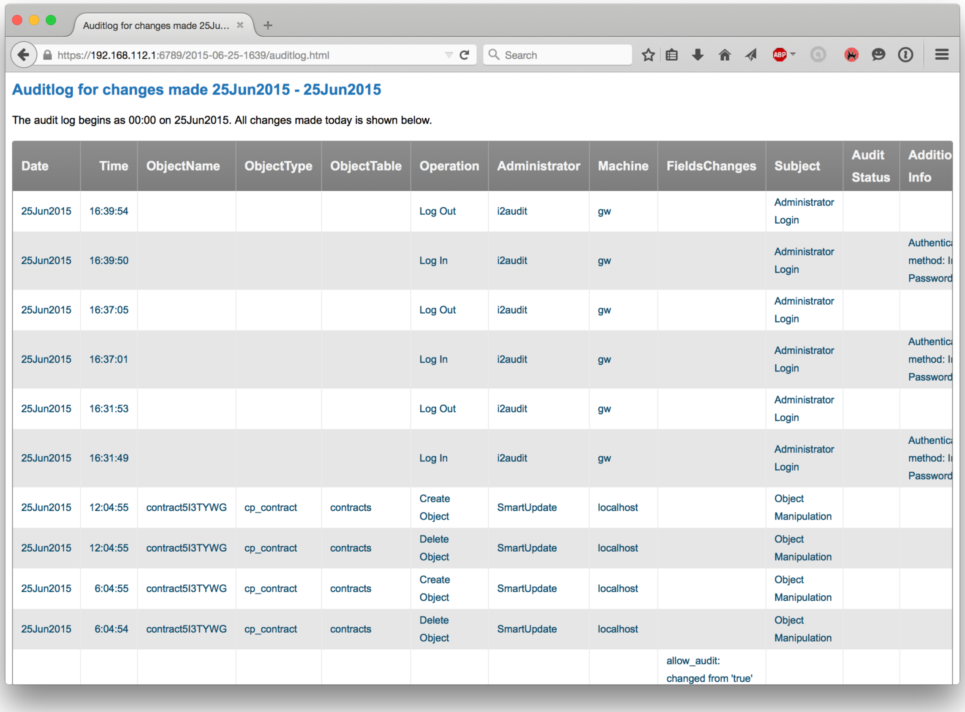
Configuration changes are tracked in the *audit log*, and the changes between different configurations are shown - exported to a HTML table.

The minimum audit time is one day.

The following information can usually be ignored:

- Automatic tasks done by the firewall software, where the column Machine is localhost.
- Automatic documentation by UNIfw1doc where the user i2audit logs in and out and column

Machine is the management station.

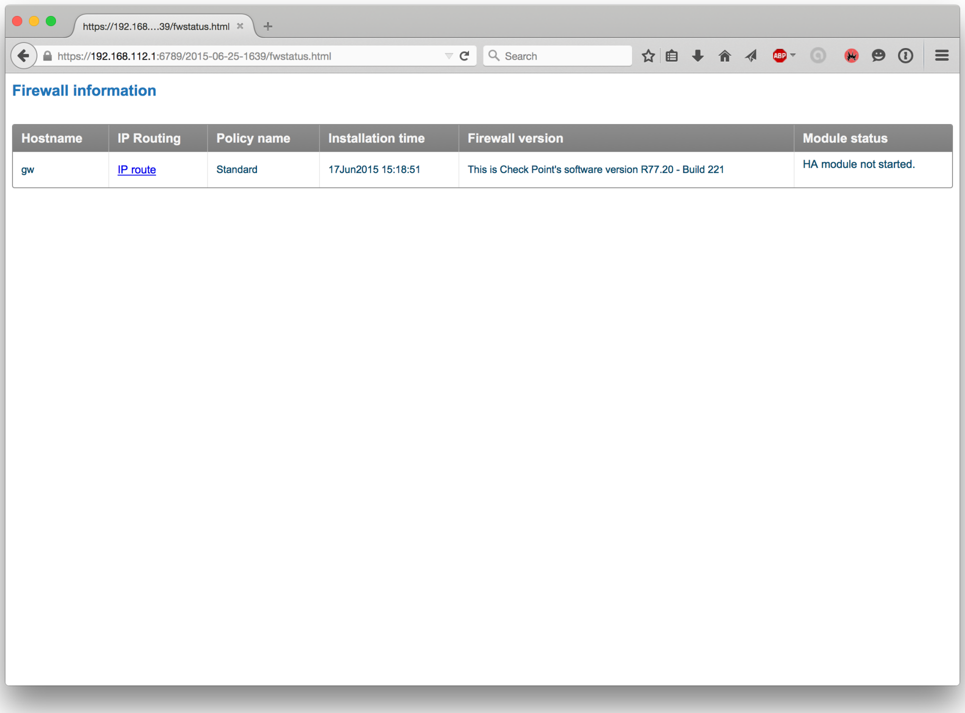

Auditlog for changes made 25Ju...
https://192.168.112.1:6789/2015-06-25-1639/auditlog.html
Search

Auditlog for changes made 25Jun2015 - 25Jun2015

The audit log begins as 00:00 on 25Jun2015. All changes made today is shown below.

Date	Time	ObjectName	ObjectType	ObjectTable	Operation	Administrator	Machine	FieldsChanges	Subject	Audit Status	Additio Info
25Jun2015	16:39:54				Log Out	i2audit	gw		Administrator Login		
25Jun2015	16:39:50				Log In	i2audit	gw		Administrator Login		Authentica method: I Password
25Jun2015	16:37:05				Log Out	i2audit	gw		Administrator Login		
25Jun2015	16:37:01				Log In	i2audit	gw		Administrator Login		Authentica method: I Password
25Jun2015	16:31:53				Log Out	i2audit	gw		Administrator Login		
25Jun2015	16:31:49				Log In	i2audit	gw		Administrator Login		Authentica method: I Password
25Jun2015	12:04:55	contract5I3TYWG	cp_contract	contracts	Create Object	SmartUpdate	localhost		Object Manipulation		
25Jun2015	12:04:55	contract5I3TYWG	cp_contract	contracts	Delete Object	SmartUpdate	localhost		Object Manipulation		
25Jun2015	6:04:55	contract5I3TYWG	cp_contract	contracts	Create Object	SmartUpdate	localhost		Object Manipulation		
25Jun2015	6:04:54	contract5I3TYWG	cp_contract	contracts	Delete Object	SmartUpdate	localhost		Object Manipulation		
								allow_audit: changed from 'true'			

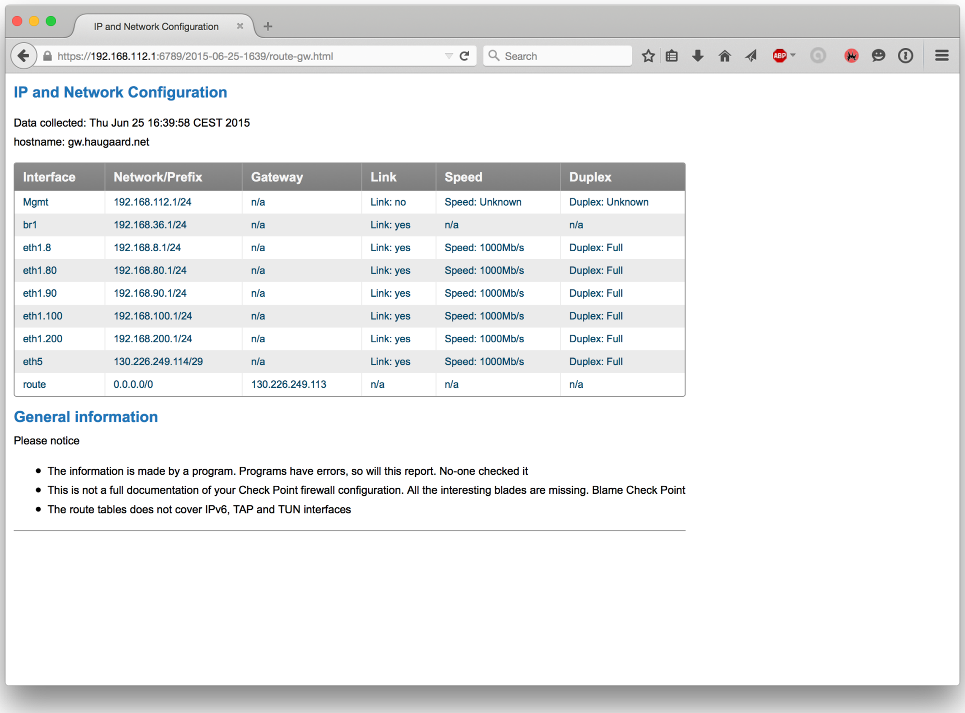
The *firewall status* shows hostname, policy name, installation date, firewall software version, cluster status (for check point clusters) and a link to a page with the static routing.


https://192.168....39/fwstatus.html
https://192.168.112.1:6789/2015-06-25-1639/fwstatus.html
Search

Firewall information

Hostname	IP Routing	Policy name	Installation time	Firewall version	Module status
gw	IP route	Standard	17Jun2015 15:18:51	This is Check Point's software version R77.20 - Build 221	HA module not started.

Example of *static routing* on the *enforcement modules*.


IP and Network Configuration
https://192.168.112.1:6789/2015-06-25-1639/route-gw.html
Search

IP and Network Configuration

Data collected: Thu Jun 25 16:39:58 CEST 2015
hostname: gw.haugaard.net

Interface	Network/Prefix	Gateway	Link	Speed	Duplex
Mgmt	192.168.112.1/24	n/a	Link: no	Speed: Unknown	Duplex: Unknown
br1	192.168.36.1/24	n/a	Link: yes	n/a	n/a
eth1.8	192.168.8.1/24	n/a	Link: yes	Speed: 1000Mb/s	Duplex: Full
eth1.80	192.168.80.1/24	n/a	Link: yes	Speed: 1000Mb/s	Duplex: Full
eth1.90	192.168.90.1/24	n/a	Link: yes	Speed: 1000Mb/s	Duplex: Full
eth1.100	192.168.100.1/24	n/a	Link: yes	Speed: 1000Mb/s	Duplex: Full
eth1.200	192.168.200.1/24	n/a	Link: yes	Speed: 1000Mb/s	Duplex: Full
eth5	130.226.249.114/29	n/a	Link: yes	Speed: 1000Mb/s	Duplex: Full
route	0.0.0.0/0	130.226.249.113	n/a	n/a	n/a

General information

Please notice

- The information is made by a program. Programs have errors, so will this report. No-one checked it
- This is not a full documentation of your Check Point firewall configuration. All the interesting blades are missing. Blame Check Point
- The route tables does not cover IPv6, TAP and TUN interfaces

Known problems and limitations

- The Web Visualization Tool is made by Check Point and sets the limits for what can be visualized.
- If the servers certificate expires, changes (the path changes with major firewall upgrade) or the servers IP address changes, then the configuration for **UNIfw1doc** must be changed as well. The configuration file is `/var/opt/UNIf1doc/etc/cp_httpd.conf`

How to solve problems

Please contact fwsupport@i2.dk in case of problems.

Note

UNI•C does not exist any more and the security devision has been transferred to DEiC/i2.dk logo and images has been updated accordingly together with new images showing cpdb2web not CPrules.