NetWyl Informatik
IT-Security Experts

Checkpoint Firewall Konfiguration
NI – Home Office

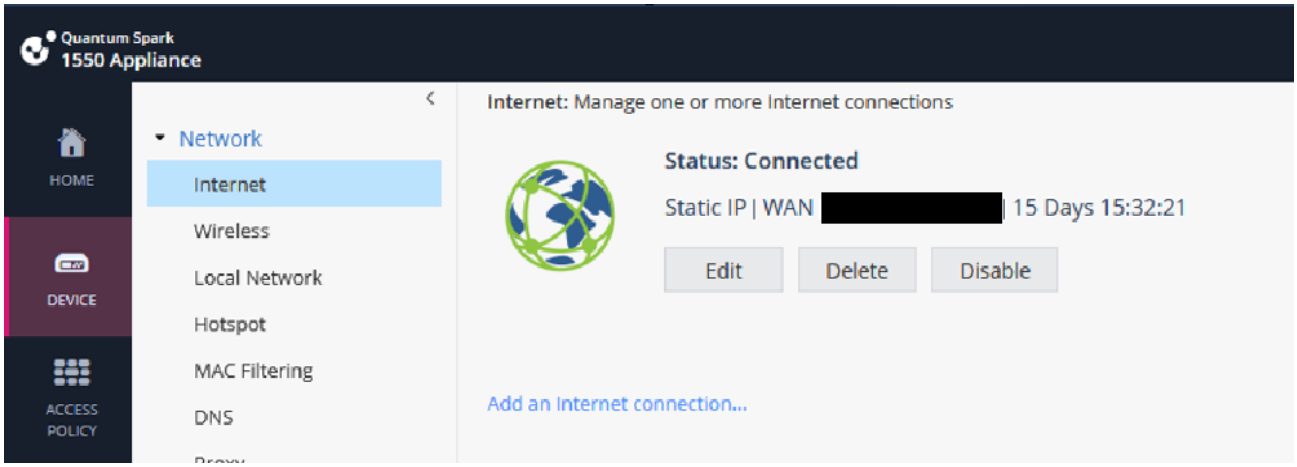
Version 1.0

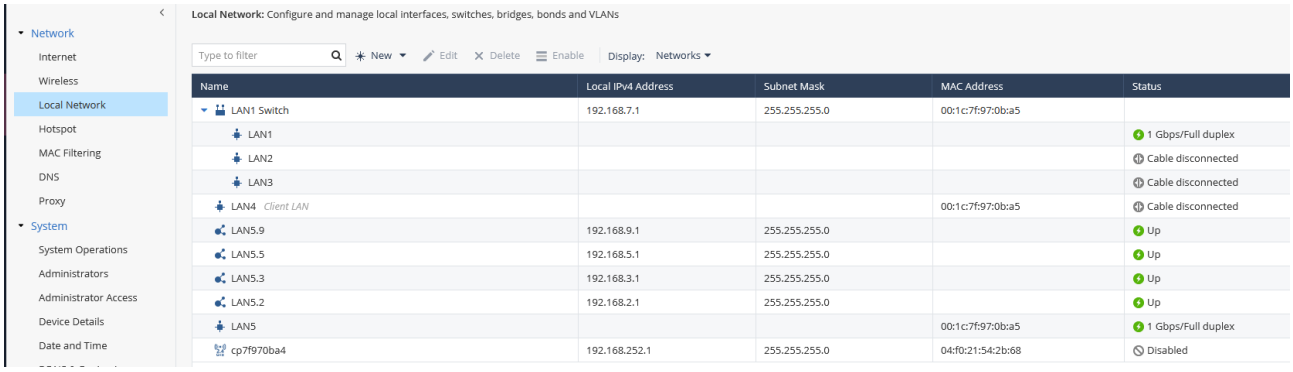
Dokument Name: Checkpoint_Firewall Konfiguration NI – Home Office

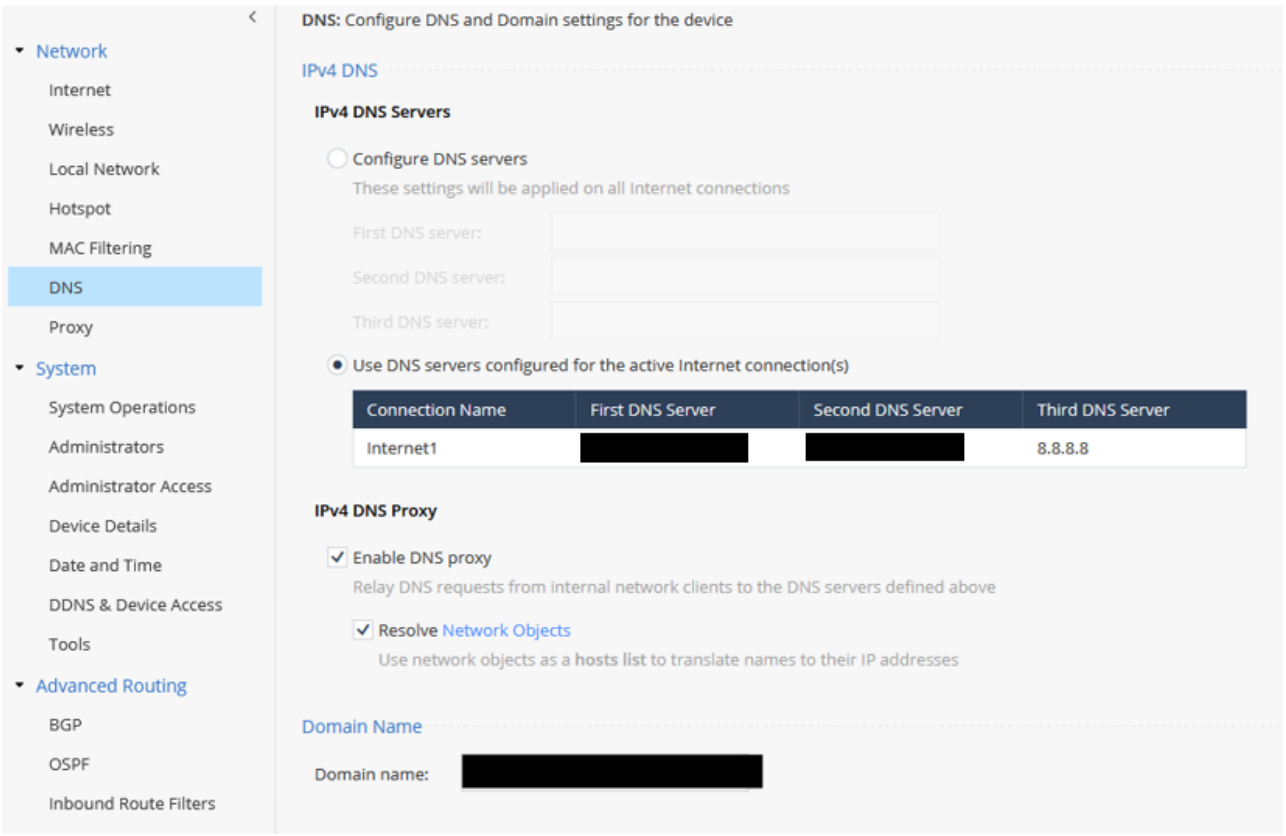
Dokumentenkontrolle

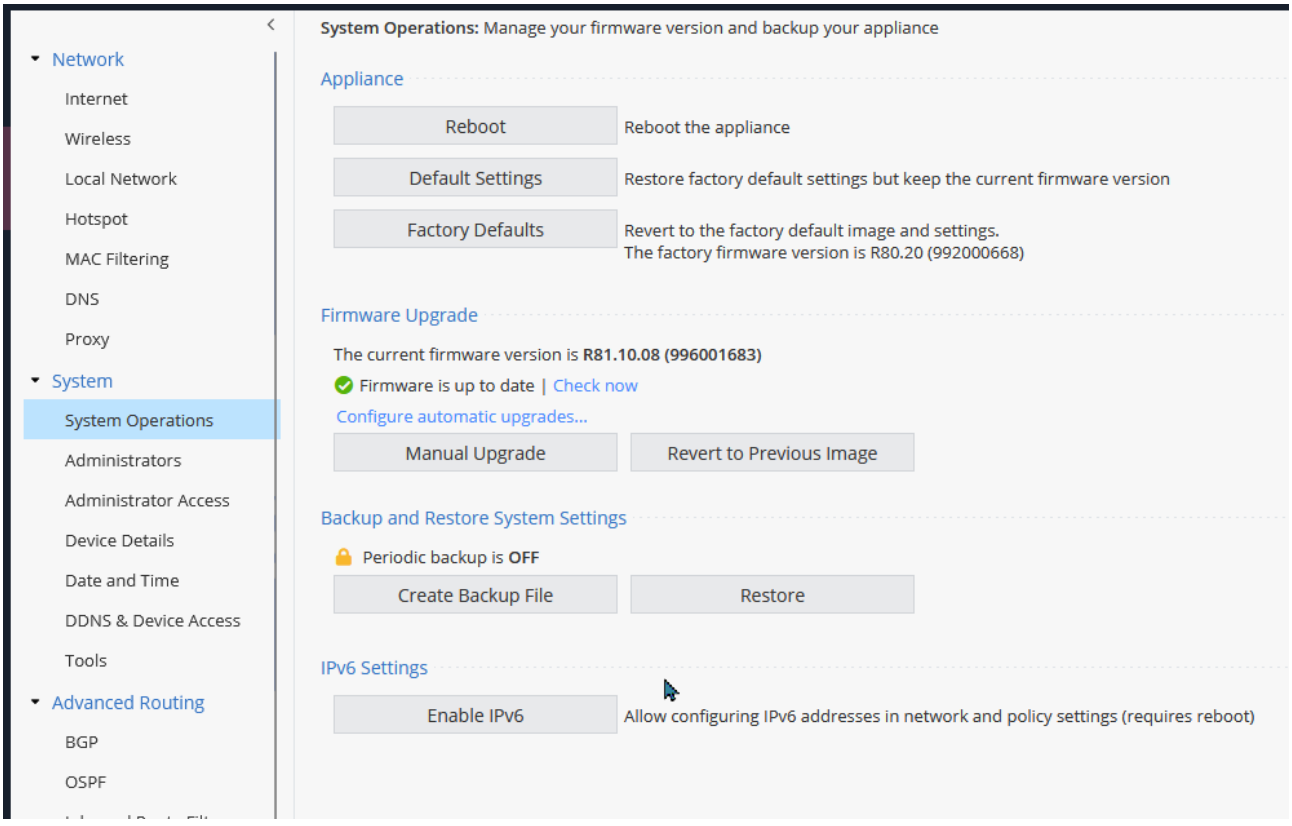
Version	Datum	Änderungsnotiz	Betroffene Seiten	Status	Author
1.0	10.07.2024				

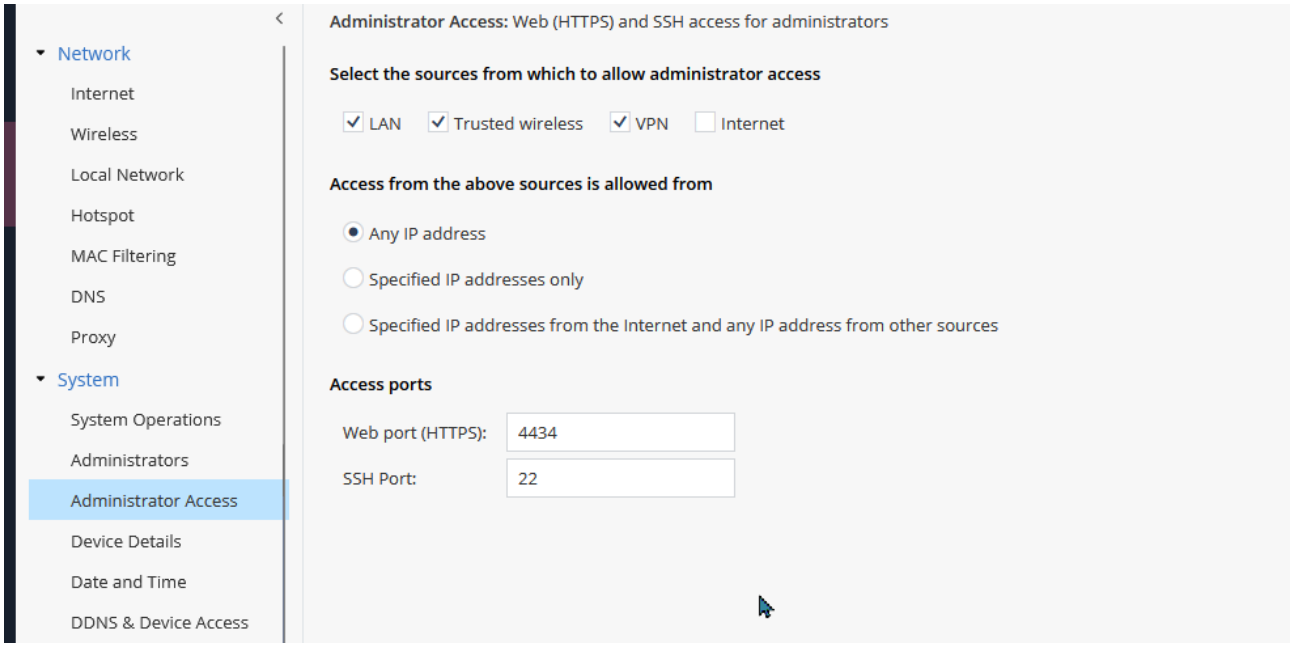
NetWyl Informatik GmbH
Täschmattstrasse 19
6015 Luzern
info@netwyl-informatik.ch
Phone: +41 41 520 73 90

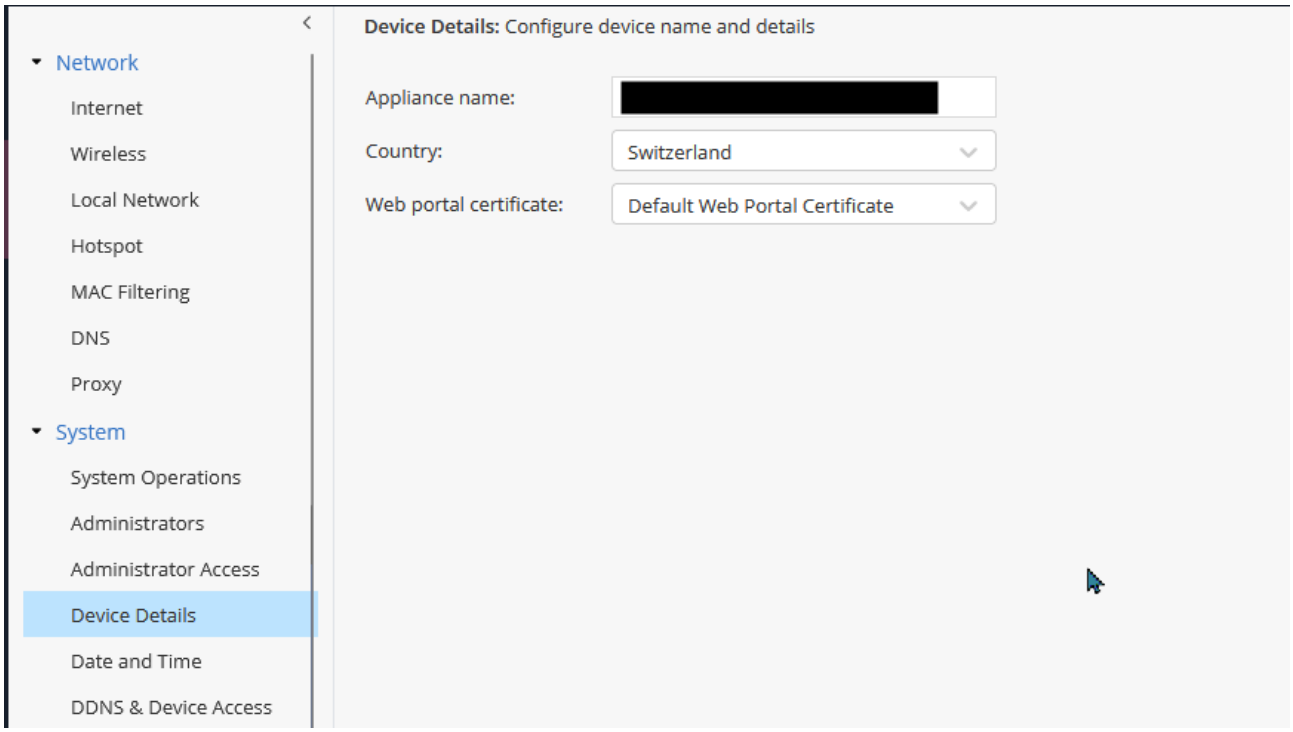

Quantum Spark
1550 Appliance
HOME
DEVICE
ACCESS POLICY
Network
Internet
Wireless
Local Network
Hotspot
MAC Filtering
DNS
Internet: Manage one or more Internet connections
Status: Connected
Static IP | WAN [redacted] | 15 Days 15:32:21
Edit
Delete
Disable
Add an Internet connection...

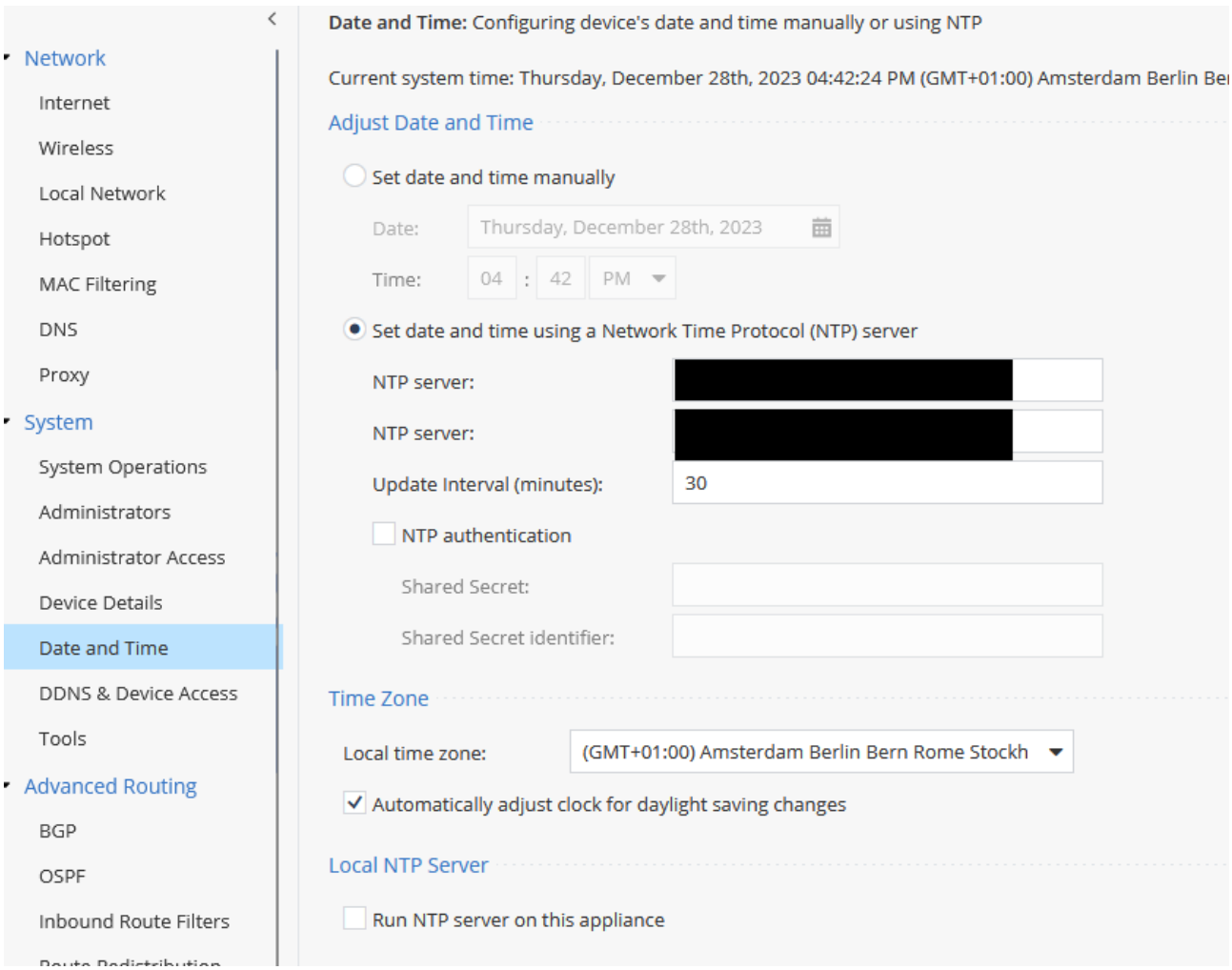

Local Network: Configure and manage local interfaces, switches, bridges, bonds and VLANs
Network
Internet
Wireless
Local Network
Hotspot
MAC Filtering
DNS
Proxy
System
System Operations
Administrators
Administrator Access
Device Details
Date and Time
Type to filter
New
Edit
Delete
Enable
Display: Networks
Name | Local IPv4 Address | Subnet Mask | MAC Address | Status
LAN1 Switch | 192.168.7.1 | 255.255.255.0 | 00:1c:7f:97:0b:a5
LAN1 | 1 Gbps/Full duplex
LAN2 | Cable disconnected
LAN3 | Cable disconnected
LAN4 Client LAN | 00:1c:7f:97:0b:a5 | Cable disconnected
LAN5.9 | 192.168.9.1 | 255.255.255.0 | Up
LAN5.5 | 192.168.5.1 | 255.255.255.0 | Up
LAN5.3 | 192.168.3.1 | 255.255.255.0 | Up
LAN5.2 | 192.168.2.1 | 255.255.255.0 | Up
LAN5 | 00:1c:7f:97:0b:a5 | 1 Gbps/Full duplex
cp7f970ba4 | 192.168.252.1 | 255.255.255.0 | 04:f0:21:54:2b:68 | Disabled

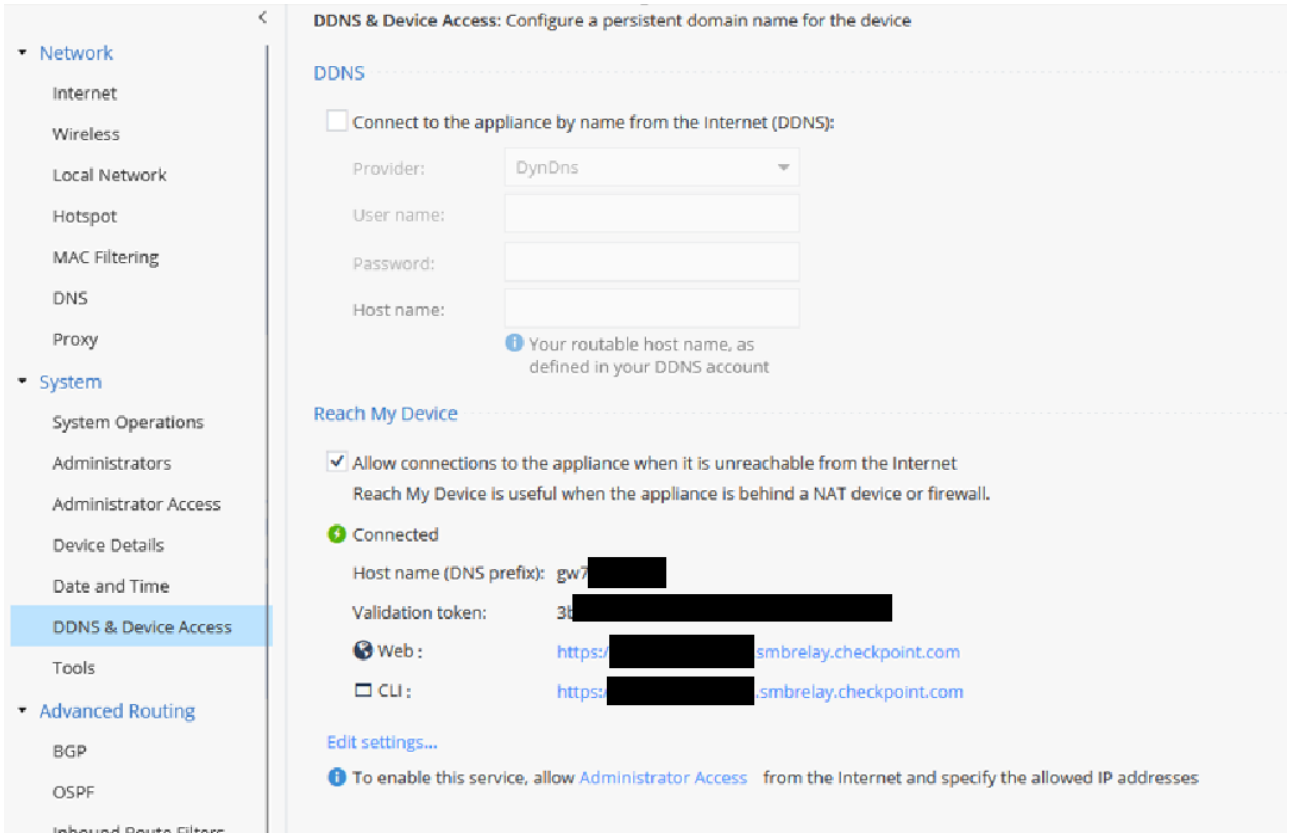

Network
Internet
Wireless
Local Network
Hotspot
MAC Filtering
DNS
Proxy
System
System Operations
Administrators
Administrator Access
Device Details
Date and Time
DDNS & Device Access
Tools
Advanced Routing
BGP
OSPF
Inbound Route Filters
DNS: Configure DNS and Domain settings for the device
IPv4 DNS
IPv4 DNS Servers
Configure DNS servers
These settings will be applied on all Internet connections
First DNS server:
Second DNS server:
Third DNS server:
Use DNS servers configured for the active Internet connection(s)
Connection Name
First DNS Server
Second DNS Server
Third DNS Server
Internet1
[redacted]
[redacted]
8.8.8.8
IPv4 DNS Proxy
Enable DNS proxy
Relay DNS requests from internal network clients to the DNS servers defined above
Resolve Network Objects
Use network objects as a hosts list to translate names to their IP addresses
Domain Name
Domain name:
[redacted]

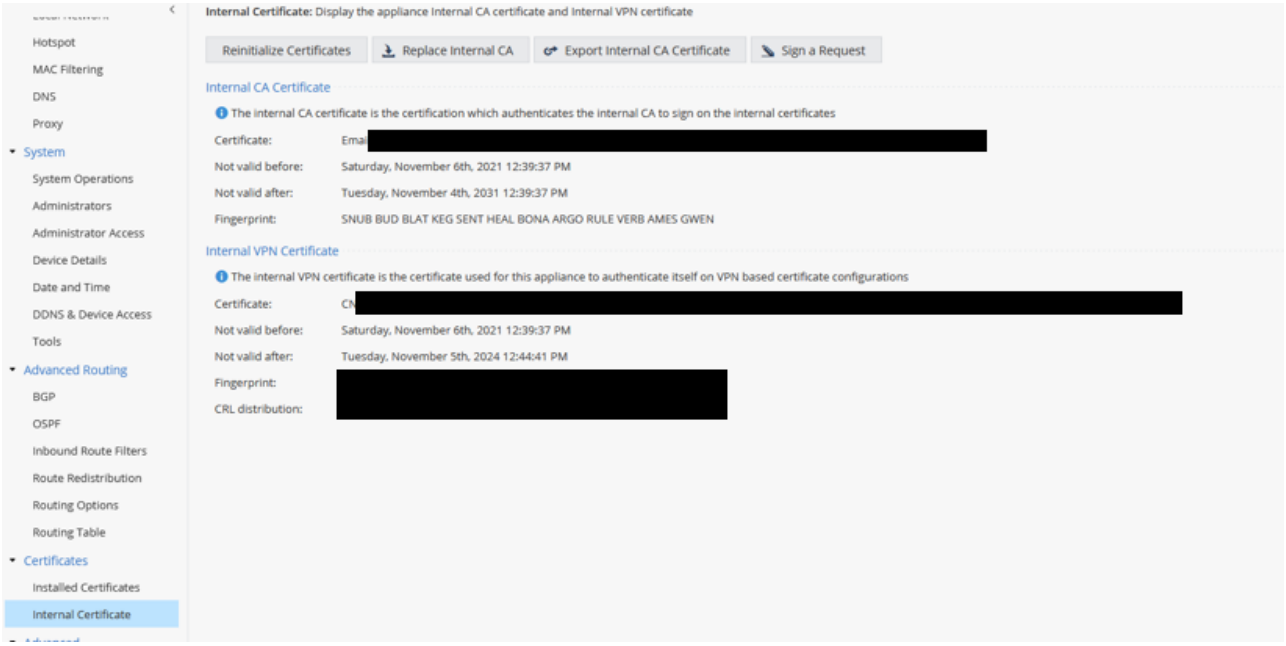

Network
Internet
Wireless
Local Network
Hotspot
MAC Filtering
DNS
Proxy
System
System Operations
Administrators
Administrator Access
Device Details
Date and Time
DDNS & Device Access
Tools
Advanced Routing
BGP
OSPF
System Operations: Manage your firmware version and backup your appliance
Appliance
Reboot
Reboot the appliance
Default Settings
Restore factory default settings but keep the current firmware version
Factory Defaults
Revert to the factory default image and settings.
The factory firmware version is R80.20 (992000668)
Firmware Upgrade
The current firmware version is R81.10.08 (996001683)
Firmware is up to date | Check now
Configure automatic upgrades...
Manual Upgrade
Revert to Previous Image
Backup and Restore System Settings
Periodic backup is OFF
Create Backup File
Restore
IPv6 Settings
Enable IPv6
Allow configuring IPv6 addresses in network and policy settings (requires reboot)

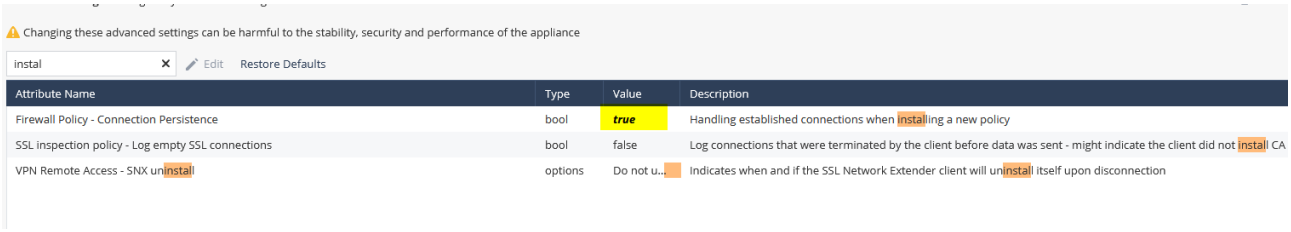

Network
Internet
Wireless
Local Network
Hotspot
MAC Filtering
DNS
Proxy
System
System Operations
Administrators
Administrator Access
Device Details
Date and Time
DDNS & Device Access
Administrator Access: Web (HTTPS) and SSH access for administrators
Select the sources from which to allow administrator access
LAN
Trusted wireless
VPN
Internet
Access from the above sources is allowed from
Any IP address
Specified IP addresses only
Specified IP addresses from the Internet and any IP address from other sources
Access ports
Web port (HTTPS): 4434
SSH Port: 22

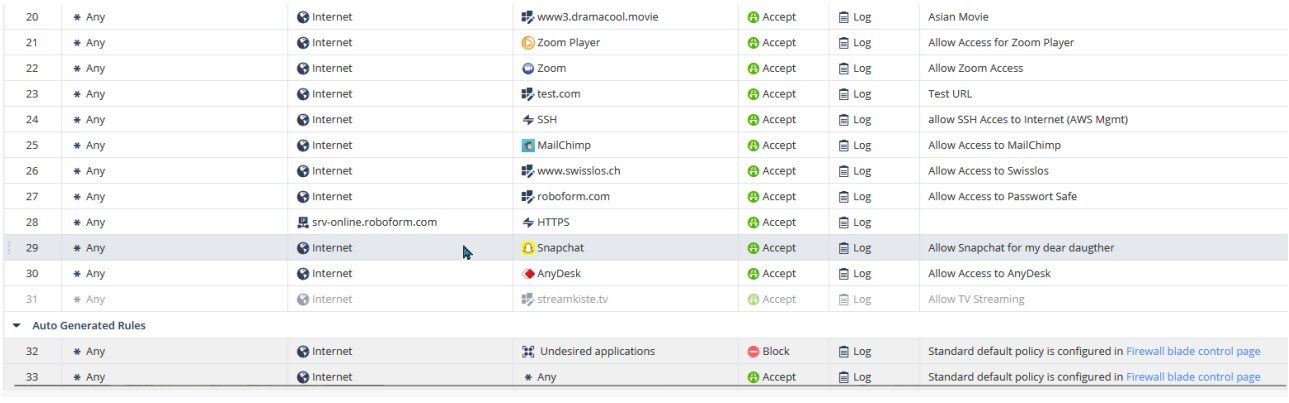

Network
Internet
Wireless
Local Network
Hotspot
MAC Filtering
DNS
Proxy
System
System Operations
Administrators
Administrator Access
Device Details
Date and Time
DDNS & Device Access
Device Details: Configure device name and details
Appliance name:
Country: Switzerland
Web portal certificate: Default Web Portal Certificate

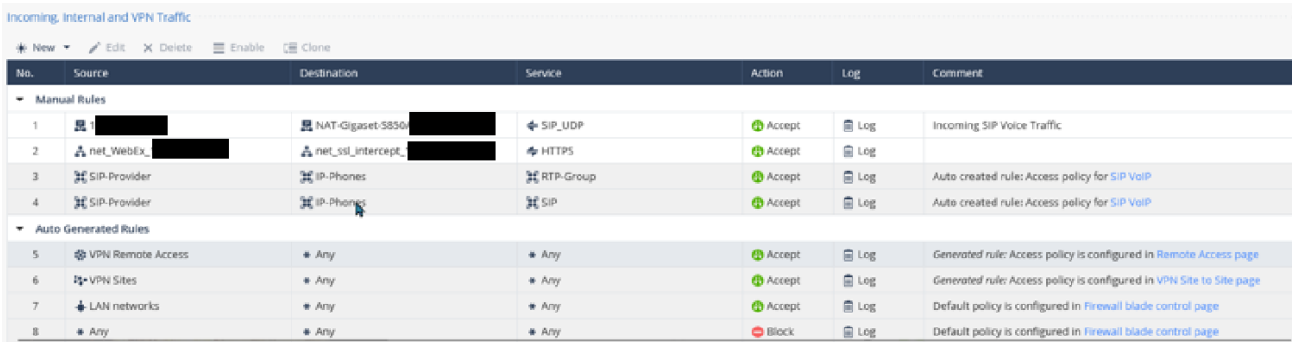

Network
Internet
Wireless
Local Network
Hotspot
MAC Filtering
DNS
Proxy
System
System Operations
Administrators
Administrator Access
Device Details
Date and Time
DDNS & Device Access
Tools
Advanced Routing
BGP
OSPF
Inbound Route Filters
Date and Time: Configuring device's date and time manually or using NTP
Current system time: Thursday, December 28th, 2023 04:42:24 PM (GMT+01:00) Amsterdam Berlin Be
Adjust Date and Time
Set date and time manually
Date: Thursday, December 28th, 2023
Time: 04 : 42 PM
Set date and time using a Network Time Protocol (NTP) server
NTP server:
NTP server:
Update Interval (minutes): 30
NTP authentication
Shared Secret:
Shared Secret identifier:
Time Zone
Local time zone: (GMT+01:00) Amsterdam Berlin Bern Rome Stockh
Automatically adjust clock for daylight saving changes
Local NTP Server
Run NTP server on this appliance


Network
Internet
Wireless
Local Network
Hotspot
MAC Filtering
DNS
Proxy
System
System Operations
Administrators
Administrator Access
Device Details
Date and Time
DDNS & Device Access
Tools
Advanced Routing
BGP
OSPF
DDNS & Device Access: Configure a persistent domain name for the device
DDNS
Connect to the appliance by name from the Internet (DDNS):
Provider: DynDns
User name:
Password:
Host name:
Your routable host name, as defined in your DDNS account
Reach My Device
Allow connections to the appliance when it is unreachable from the Internet
Reach My Device is useful when the appliance is behind a NAT device or firewall.
Connected
Host name (DNS prefix): gw7
Validation token: 3
Web : https:/ smbrelay.checkpoint.com
CLI : https: .smbrelay.checkpoint.com
Edit settings...
To enable this service, allow Administrator Access from the Internet and specify the allowed IP addresses


Internal Certificate: Display the appliance Internal CA certificate and Internal VPN certificate
Reinitialize Certificates
Replace Internal CA
Export Internal CA Certificate
Sign a Request
Internal CA Certificate
The internal CA certificate is the certification which authenticates the internal CA to sign on the internal certificates
Certificate:
Not valid before: Saturday, November 6th, 2021 12:39:37 PM
Not valid after: Tuesday, November 4th, 2031 12:39:37 PM
Fingerprint: SNUB BUD BLAT KEG SENT HEAL BONA ARGO RULE VERB AMES GWEN
Internal VPN Certificate
The internal VPN certificate is the certificate used for this appliance to authenticate itself on VPN based certificate configurations
Certificate:
Not valid before: Saturday, November 6th, 2021 12:39:37 PM
Not valid after: Tuesday, November 5th, 2024 12:44:41 PM
Fingerprint:
CRL distribution:
Hotspot
MAC Filtering
DNS
Proxy
System
System Operations
Administrators
Administrator Access
Device Details
Date and Time
DDNS & Device Access
Tools
Advanced Routing
BGP
OSPF
Inbound Route Filters
Route Redistribution
Routing Options
Routing Table
Certificates
Installed Certificates
Internal Certificate


Changing these advanced settings can be harmful to the stability, security and performance of the appliance
instal
Edit
Restore Defaults
Attribute Name
Type
Value
Description
Firewall Policy - Connection Persistence
bool
true
Handling established connections when installing a new policy
SSL inspection policy - Log empty SSL connections
bool
false
Log connections that were terminated by the client before data was sent - might indicate the client did not install CA
VPN Remote Access - SNX uninstall
options
Do not u...
Indicates when and if the SSL Network Extender client will uninstall itself upon disconnection


20 Any Internet www3.dramacool.movie Accept Log Asian Movie
21 Any Internet Zoom Player Accept Log Allow Access for Zoom Player
22 Any Internet Zoom Accept Log Allow Zoom Access
23 Any Internet test.com Accept Log Test URL
24 Any Internet SSH Accept Log allow SSH Acces to Internet (AWS Mgmt)
25 Any Internet MailChimp Accept Log Allow Access to MailChimp
26 Any Internet www.swisslos.ch Accept Log Allow Access to Swisslos
27 Any Internet roboform.com Accept Log Allow Access to Passwort Safe
28 Any srv-online.roboform.com HTTPS Accept Log
29 Any Internet Snapchat Accept Log Allow Snapchat for my dear daugther
30 Any Internet AnyDesk Accept Log Allow Access to AnyDesk
31 Any Internet streamkiste.tv Accept Log Allow TV Streaming
Auto Generated Rules
32 Any Internet Undesired applications Block Log Standard default policy is configured in Firewall blade control page
33 Any Internet Any Accept Log Standard default policy is configured in Firewall blade control page


Incoming, Internal and VPN Traffic
New
Edit
Delete
Enable
Clone
No.
Source
Destination
Service
Action
Log
Comment
Manual Rules
1 SIP_UDP Accept Log Incoming SIP Voice Traffic
2 HTTPS Accept Log
3 SIP-Provider IP-Phones RTP-Group Accept Log Auto created rule: Access policy for SIP VoIP
4 SIP-Provider IP-Phones SIP Accept Log Auto created rule: Access policy for SIP VoIP
Auto Generated Rules
5 VPN Remote Access Any Any Accept Log Generated rule: Access policy is configured in Remote Access page
6 VPN Sites Any Any Accept Log Generated rule: Access policy is configured in VPN Site to Site page
7 LAN networks Any Any Accept Log Default policy is configured in Firewall blade control page
8 Any Any Any Block Log Default policy is configured in Firewall blade control page

SSL Inspection Policy Exceptions: Configure exceptions to bypass SSL inspection policy for specific traffic

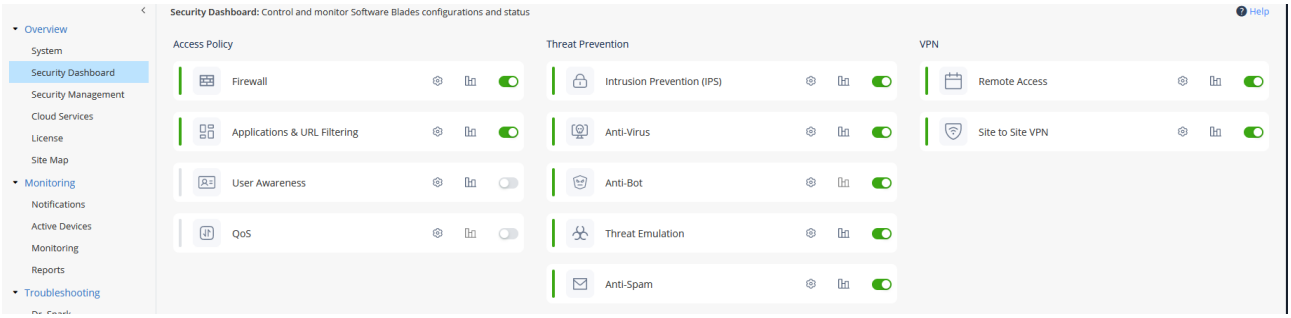
New | Edit | Delete | Enable

No.	Source	Destination	Service	Category/Custom App...	Track	Comment
1	net_192.168.7.0-24_intern	Internet	HTTPS	Any	Log	Bypass SSL Inspection
2	net_192.168.2.0-24_dmz	Internet	HTTPS	Any	Log	Bypass SSL Inspection
3	Any	Internet	Any	WebEx	Log	
4	Any	Internet	Any	WebEx-URL	Log	
5	net_ssl_intercept_192.168.9.128	net_WebEx_170.72....	RTP-Group	Any	Log	
6	net_ssl_intercept_192.168.9.128	Internet	HTTPS	APPLE-Sites	Log	
7	net_ssl_intercept_192.168.9.128	Internet	HTTPS	gdmf.apple.com	Log	
8	net_ssl_intercept_192.168.9.128	net_apple_17.0.0.0-8	HTTPS	Any	Log	
9	net_ssl_intercept_192.168.9.128	srv-online.robofor...	HTTPS	Any	Log	
10	net_ssl_intercept_192.168.9.128	Internet	HTTPS	wiildcard-checkpoi...	Log	
11	VPN Remote Access	Internet	HTTPS	Any	Log	
12	Any	lst-sg-01-outside_6...	Any	Any	Log	
13	Any	HTTPS services - by...	HTTPS	Any	Log	Predefined rule by Check Point

Network Objects: Create and edit network objects that will be used in the device's feature configuration

Type to filter | New | Edit | Delete | Used where...

Object Name	Type	Domain / IP Addresses / MAC Address
Gigaset-S850A-GO_1[redacted]	Single IP	1[redacted]
NAT-Gigaset-S850A_6[redacted]	Single IP	[redacted]
device-[redacted]	Single IP	[redacted]
Zoom-Gateway_[redacted]	Single IP	[redacted]
device-[redacted]	Single IP	[redacted]
PC-32NMTOM-Tim_192.168.7.234	Single IP	192.168.7.234
FTP_Server_192.168.3.30	Single IP	192.168.3.30
net_allianz_[redacted]	Network	[redacted]
NAT-FTP-Server_[redacted]	Single IP	[redacted]
net_192.168.1.0-24_HotelConnLAN	Network	192.168.1.0/255.255.255.0
iPhone-Seyas_192.168.7.226	Single IP	192.168.7.226
virt-mgmt01_192.168.7.40	Single IP	192.168.7.40
PC-QPP29A9-Seya_192.168.7.243	Single IP	192.168.7.243
net_192.168.2.0-24_dmz	Network	192.168.2.0/255.255.255.0
net_192.168.3.0-24_dmz	Network	192.168.3.0/255.255.255.0
net_192.168.7.0-24_intern	Network	192.168.7.0/255.255.255.0
net_192.168.9.0-24_client-lan	Network	192.168.9.0/255.255.255.0
SonosZP-Play5_192.168.7.51	Single IP	192.168.7.51
SonosZP-AMP_192.168.7.50	Single IP	192.168.7.50
SonosZP-Atelier-192.168.7.52	Single IP	192.168.7.52
SonosZP-Kueche_192.168.7.53	Single IP	192.168.7.53


Security Dashboard: Control and monitor Software Blades configurations and status
Help
Overview
System
Security Dashboard
Security Management
Cloud Services
License
Site Map
Monitoring
Notifications
Active Devices
Monitoring
Reports
Troubleshooting
Access Policy
Firewall
Applications & URL Filtering
User Awareness
QoS
Threat Prevention
Intrusion Prevention (IPS)
Anti-Virus
Anti-Bot
Threat Emulation
Anti-Spam
VPN
Remote Access
Site to Site VPN