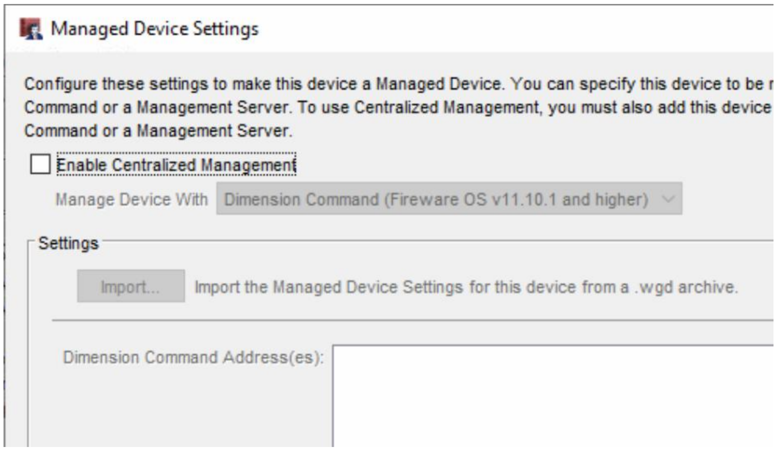
Client B - Firebox Audit

Screenshots & Comments

No CM in use.



Managed Device Settings

Configure these settings to make this device a Managed Device. You can specify this device to be r
Command or a Management Server. To use Centralized Management, you must also add this device
Command or a Management Server.

☐ Enable Centralized Management

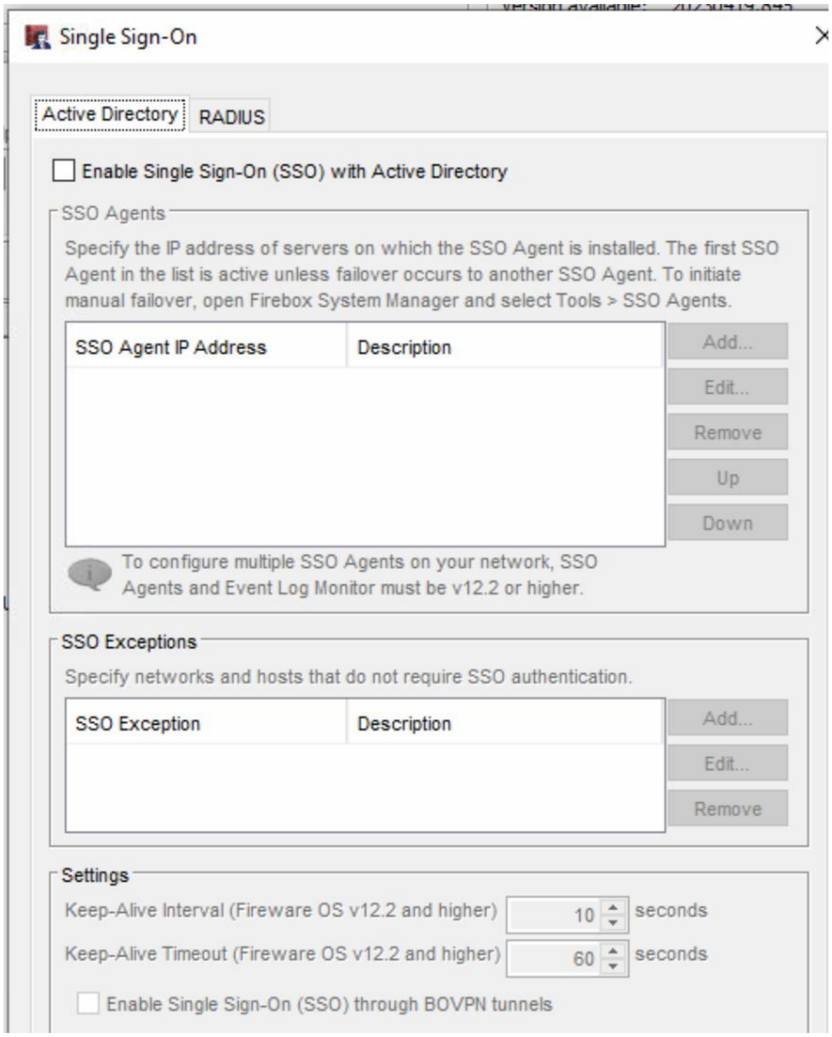
Manage Device With: Dimension Command (Fireware OS v11.10.1 and higher)

Settings

Import... Import the Managed Device Settings for this device from a .wgd archive.

Dimension Command Address(es):

Not using SSO.



Single Sign-On

Active Directory | RADIUS

☐ Enable Single Sign-On (SSO) with Active Directory

SSO Agents

Specify the IP address of servers on which the SSO Agent is installed. The first SSO Agent in the list is active unless failover occurs to another SSO Agent. To initiate manual failover, open Firebox System Manager and select Tools > SSO Agents.

SSO Agent IP Address	Description

To configure multiple SSO Agents on your network, SSO Agents and Event Log Monitor must be v12.2 or higher.

SSO Exceptions

Specify networks and hosts that do not require SSO authentication.

SSO Exception	Description

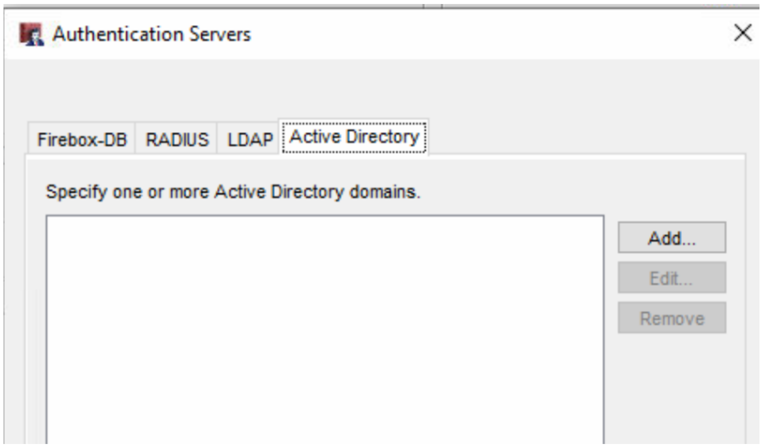
Settings

Keep-Alive Interval (Fireware OS v12.2 and higher): 10 seconds

Keep-Alive Timeout (Fireware OS v12.2 and higher): 60 seconds

☐ Enable Single Sign-On (SSO) through BOVPN tunnels

AD integration and LDAPS not implemented.



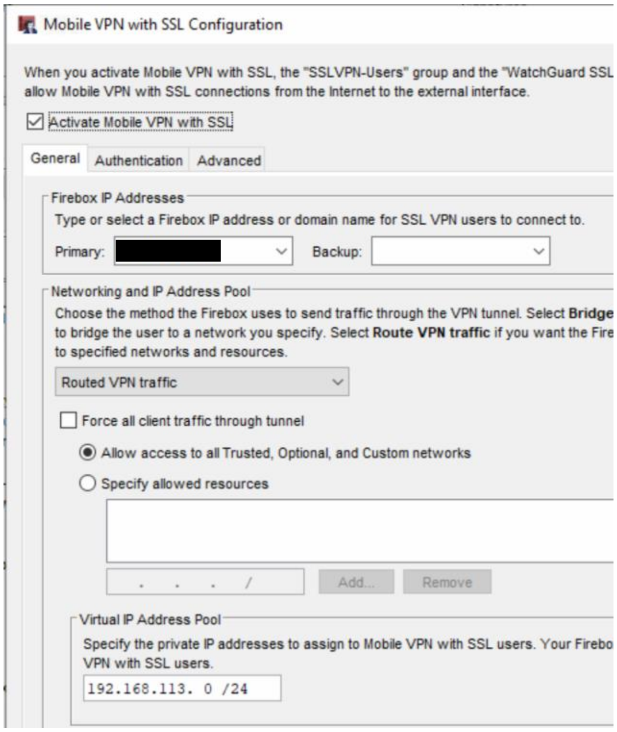
Authentication Servers

Firebox-DB | RADIUS | LDAP | Active Directory

Specify one or more Active Directory domains.

No MFA for SSL VPN and SSL VPN not configured correctly.

Force tunnel not configured.



Mobile VPN with SSL Configuration

When you activate Mobile VPN with SSL, the "SSLVPN-Users" group and the "WatchGuard SSL
allow Mobile VPN with SSL connections from the Internet to the external interface.

☑ Activate Mobile VPN with SSL

General | Authentication | Advanced

Firebox IP Addresses

Type or select a Firebox IP address or domain name for SSL VPN users to connect to.

Primary: [redacted] Backup:

Networking and IP Address Pool

Choose the method the Firebox uses to send traffic through the VPN tunnel. Select **Bridge**
to bridge the user to a network you specify. Select **Route VPN traffic** if you want the Fire
to specified networks and resources.

Routed VPN traffic

□ Force all client traffic through tunnel

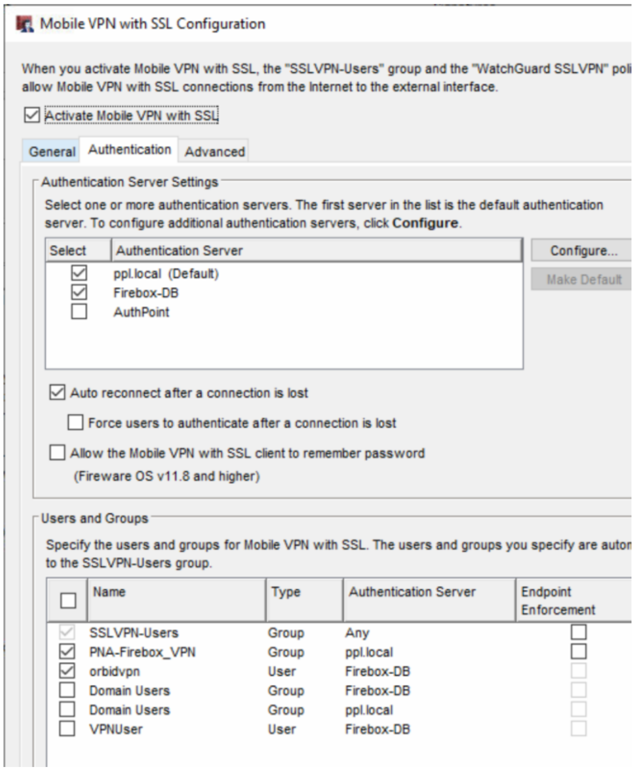
● Allow access to all Trusted, Optional, and Custom networks

○ Specify allowed resources

Virtual IP Address Pool

Specify the private IP addresses to assign to Mobile VPN with SSL users. Your Firebo
VPN with SSL users.

192.168.113. 0 /24



Mobile VPN with SSL Configuration

When you activate Mobile VPN with SSL, the "SSLVPN-Users" group and the "WatchGuard SSLVPN" poli
allow Mobile VPN with SSL connections from the Internet to the external interface.

☑ Activate Mobile VPN with SSL

Authentication Server Settings

Select one or more authentication servers. The first server in the list is the default authentication server. To configure additional authentication servers, click **Configure**.

Select	Authentication Server
☑	ppl.local (Default)
☑	Firebox-DB
□	AuthPoint

☑ Auto reconnect after a connection is lost

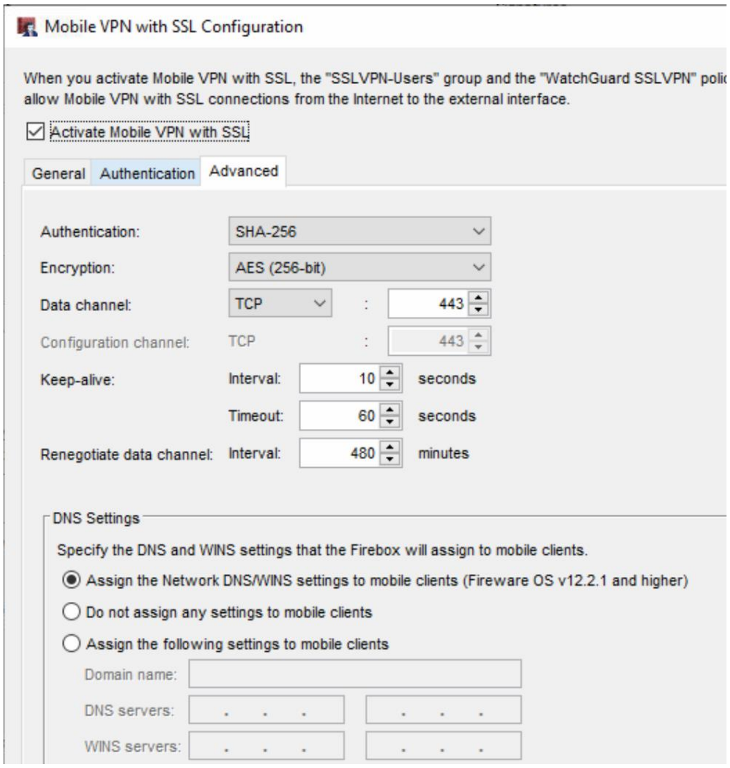
□ Force users to authenticate after a connection is lost

□ Allow the Mobile VPN with SSL client to remember password (Fireware OS v11.8 and higher)

Users and Groups

Specify the users and groups for Mobile VPN with SSL. The users and groups you specify are auton
to the SSLVPN-Users group.

□	Name	Type	Authentication Server	Endpoint Enforcement
☑	SSLVPN-Users	Group	Any	□
☑	PNA-Firebox_VPN	Group	ppl.local	□
☑	orbidvpn	User	Firebox-DB	□
□	Domain Users	Group	Firebox-DB	□
□	Domain Users	Group	ppl.local	□
□	VPNUser	User	Firebox-DB	□



Mobile VPN with SSL Configuration

When you activate Mobile VPN with SSL, the "SSLVPN-Users" group and the "WatchGuard SSLVPN" polic
allow Mobile VPN with SSL connections from the Internet to the external interface.

☑ Activate Mobile VPN with SSL

Authentication: SHA-256

Encryption: AES (256-bit)

Data channel: TCP : 443

Configuration channel: TCP : 443

Keep-alive: Interval: 10 seconds

Timeout: 60 seconds

Renegotiate data channel: Interval: 480 minutes

DNS Settings

Specify the DNS and WINS settings that the Firebox will assign to mobile clients.

● Assign the Network DNS/WINS settings to mobile clients (Fireware OS v12.2.1 and higher)

○ Do not assign any settings to mobile clients

○ Assign the following settings to mobile clients

Domain name:

DNS servers: . . . . . .

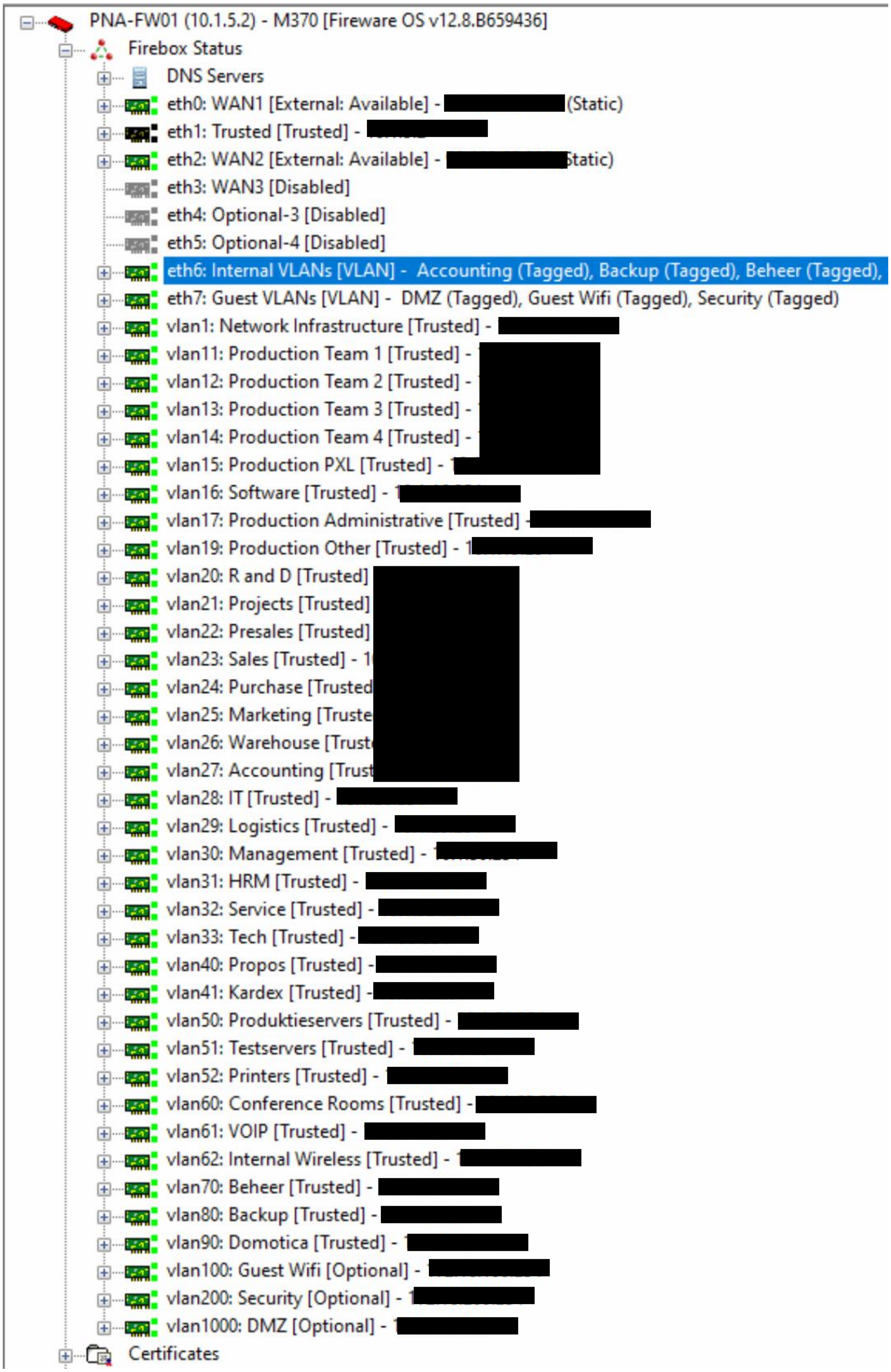
WINS servers: . . . . . .

Old security algorithms

No DNS provided

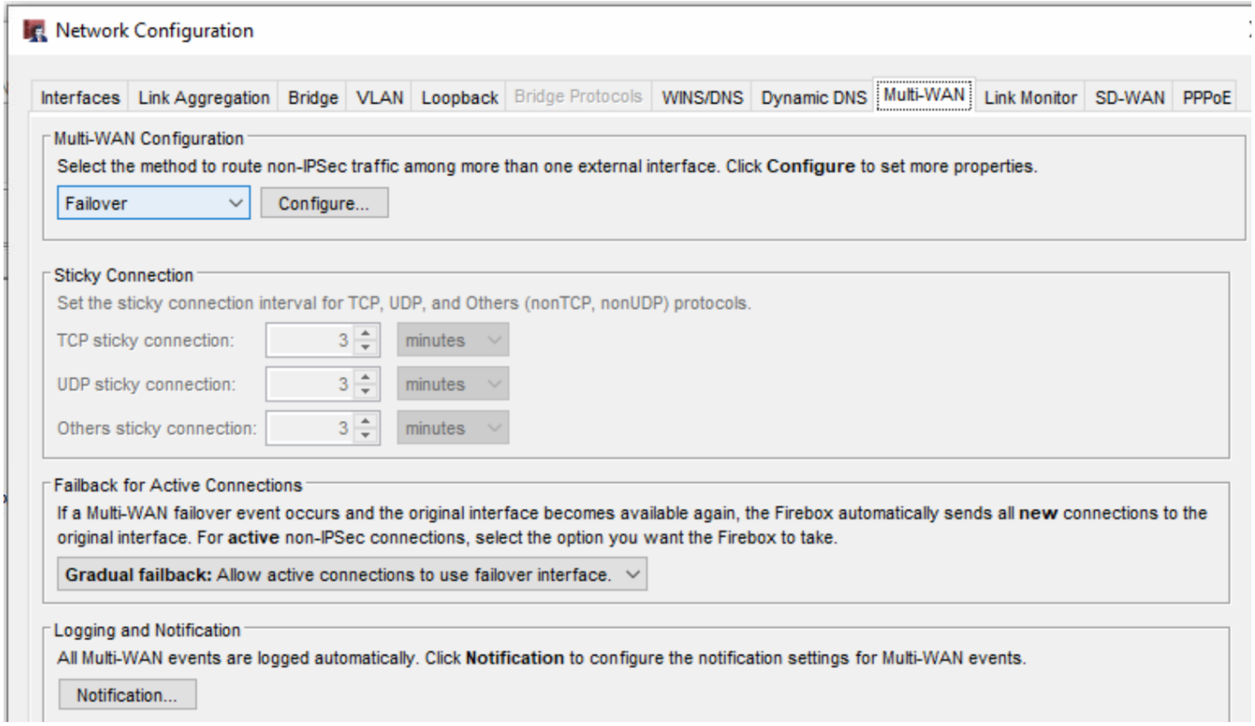
No link aggregation.

Old Fireware.



- PNA-FW01 (10.1.5.2) - M370 [Fireware OS v12.8.B659436]
  - Firebox Status
    - DNS Servers
    - eth0: WAN1 [External: Available] - [redacted] (Static)
    - eth1: Trusted [Trusted] - [redacted]
    - eth2: WAN2 [External: Available] - [redacted] tatic)
    - eth3: WAN3 [Disabled]
    - eth4: Optional-3 [Disabled]
    - eth5: Optional-4 [Disabled]
    - eth6: Internal VLANs [VLAN] - Accounting (Tagged), Backup (Tagged), Beheer (Tagged),
    - eth7: Guest VLANs [VLAN] - DMZ (Tagged), Guest Wifi (Tagged), Security (Tagged)
    - vlan1: Network Infrastructure [Trusted] - [redacted]
    - vlan11: Production Team 1 [Trusted] - [redacted]
    - vlan12: Production Team 2 [Trusted] -
    - vlan13: Production Team 3 [Trusted] -
    - vlan14: Production Team 4 [Trusted] -
    - vlan15: Production PXL [Trusted] -
    - vlan16: Software [Trusted] - [redacted]
    - vlan17: Production Administrative [Trusted] [redacted]
    - vlan19: Production Other [Trusted] - [redacted]
    - vlan20: R and D [Trusted] [redacted]
    - vlan21: Projects [Trusted]
    - vlan22: Presales [Trusted]
    - vlan23: Sales [Trusted] -
    - vlan24: Purchase [Trusted
    - vlan25: Marketing [Truste
    - vlan26: Warehouse [Trust
    - vlan27: Accounting [Trust
    - vlan28: IT [Trusted] - [redacted]
    - vlan29: Logistics [Trusted] - [redacted]
    - vlan30: Management [Trusted] - [redacted]
    - vlan31: HRM [Trusted] - [redacted]
    - vlan32: Service [Trusted] - [redacted]
    - vlan33: Tech [Trusted] - [redacted]
    - vlan40: Propos [Trusted] - [redacted]
    - vlan41: Kardex [Trusted] - [redacted]
    - vlan50: Produktieservers [Trusted] - [redacted]
    - vlan51: Testservers [Trusted] - [redacted]
    - vlan52: Printers [Trusted] - [redacted]
    - vlan60: Conference Rooms [Trusted] - [redacted]
    - vlan61: VOIP [Trusted] - [redacted]
    - vlan62: Internal Wireless [Trusted] - [redacted]
    - vlan70: Beheer [Trusted] - [redacted]
    - vlan80: Backup [Trusted] - [redacted]
    - vlan90: Domotica [Trusted] - [redacted]
    - vlan100: Guest Wifi [Optional] - [redacted]
    - vlan200: Security [Optional] - [redacted]
    - vlan1000: DMZ [Optional] - [redacted]
  - Certificates

No SDWAN configured. Failover is just wrong. It should be round robin. The Firebox should be able to use both connections simultaneously with traffic shaping.



Multi-WAN Configuration

Select the method to route non-IPSec traffic among more than one external interface. Click **Configure** to set more properties.

Failover

Sticky Connection

Set the sticky connection interval for TCP, UDP, and Others (nonTCP, nonUDP) protocols.

TCP sticky connection: 3 minutes

UDP sticky connection: 3 minutes

Others sticky connection: 3 minutes

Failback for Active Connections

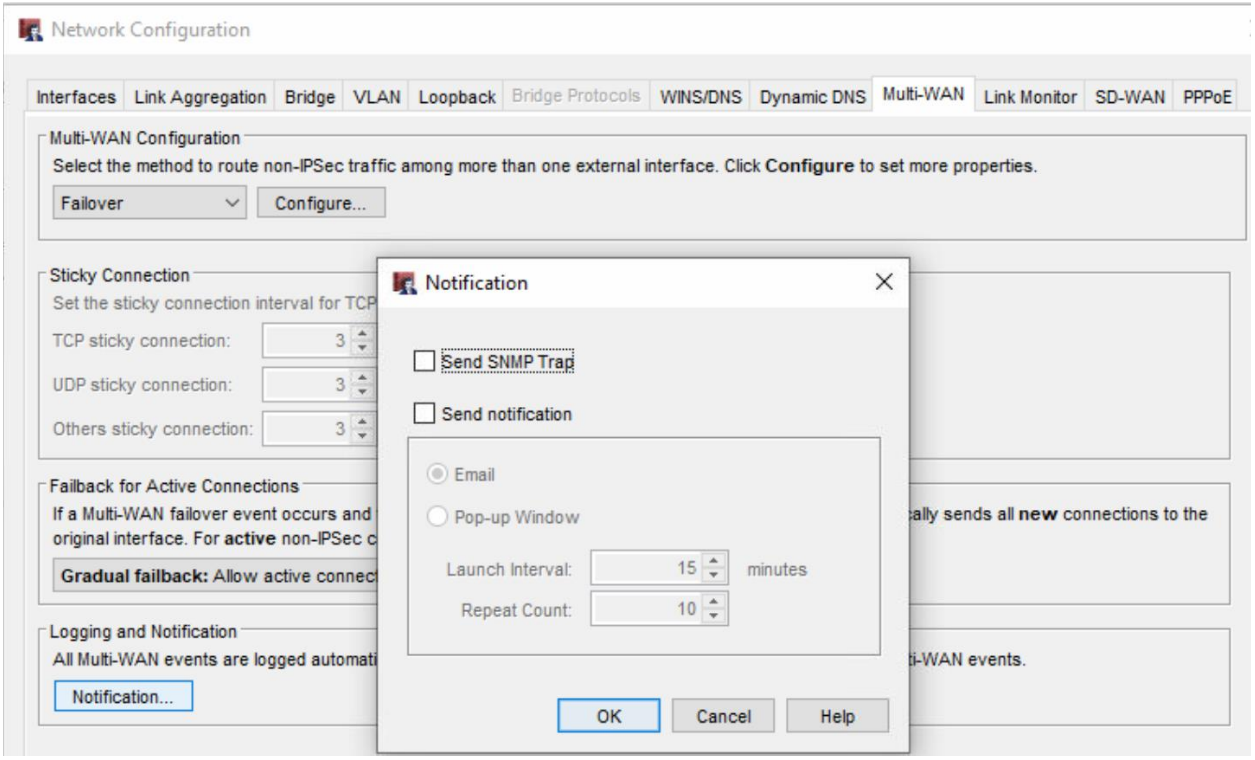
If a Multi-WAN failover event occurs and the original interface becomes available again, the Firebox automatically sends all **new** connections to the original interface. For **active** non-IPSec connections, select the option you want the Firebox to take.

Gradual failback: Allow active connections to use failover interface.

Logging and Notification

All Multi-WAN events are logged automatically. Click **Notification** to configure the notification settings for Multi-WAN events.

Why would you want a notification when the WAN link is down?



Notification

□ Send SNMP Trap

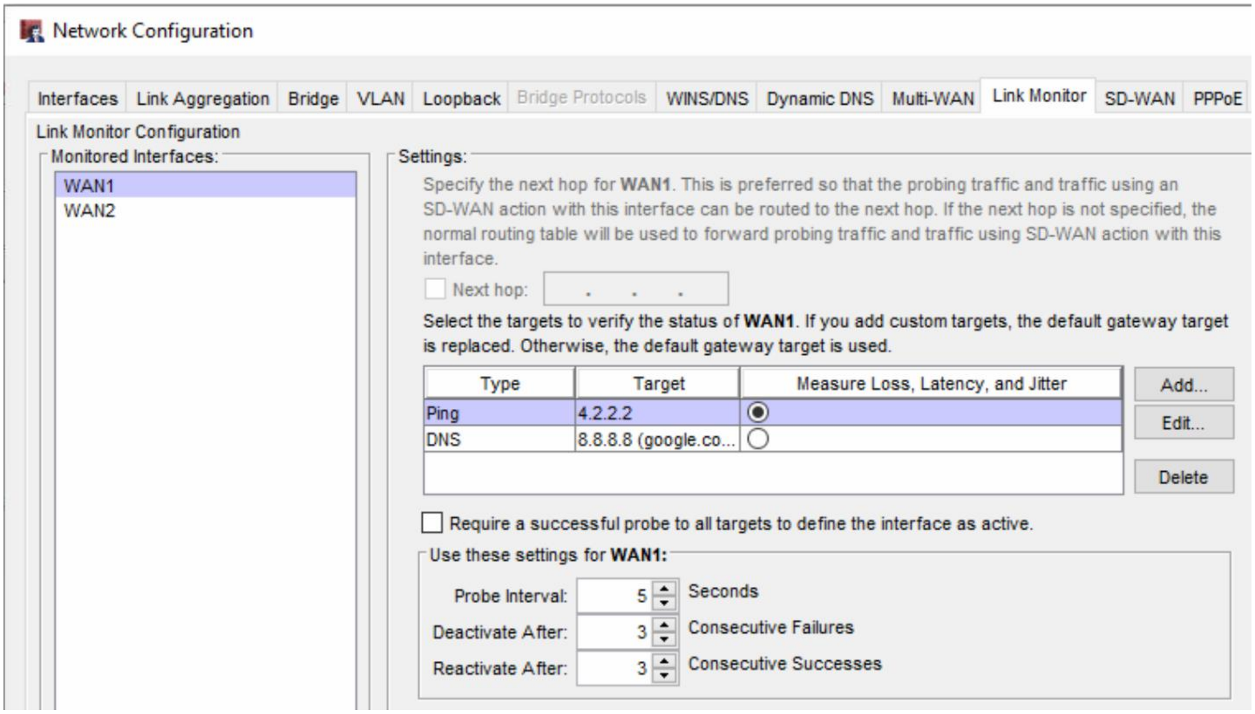
□ Send notification

● Email

○ Pop-up Window

Launch Interval: 15 minutes

Repeat Count: 10



Link Monitor Configuration

Monitored Interfaces:

- WAN1
- WAN2

Settings:

Specify the next hop for **WAN1**. This is preferred so that the probing traffic and traffic using an SD-WAN action with this interface can be routed to the next hop. If the next hop is not specified, the normal routing table will be used to forward probing traffic and traffic using SD-WAN action with this interface.

□ Next hop: . . .

Select the targets to verify the status of **WAN1**. If you add custom targets, the default gateway target is replaced. Otherwise, the default gateway target is used.

Type	Target	Measure Loss, Latency, and Jitter
Ping	4.2.2.2	●
DNS	8.8.8.8 (google.co...	○

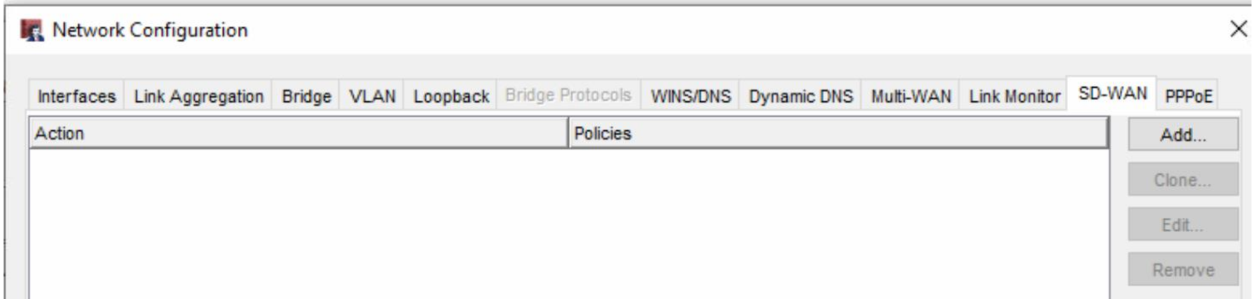
□ Require a successful probe to all targets to define the interface as active.

Use these settings for **WAN1**:

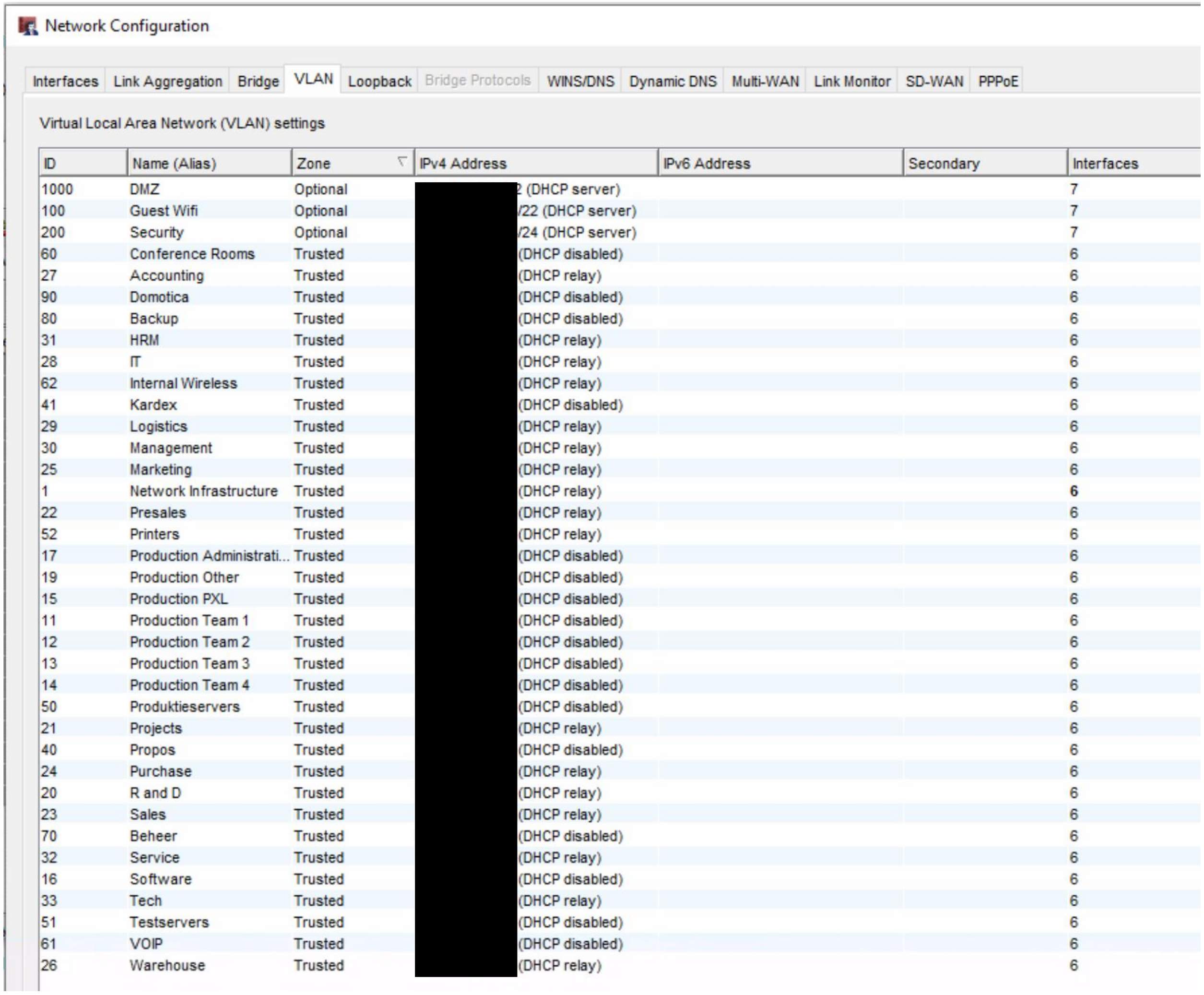
Probe Interval:	5	Seconds
Deactivate After:	3	Consecutive Failures
Reactivate After:	3	Consecutive Successes

Wrong configs

No SD WAN



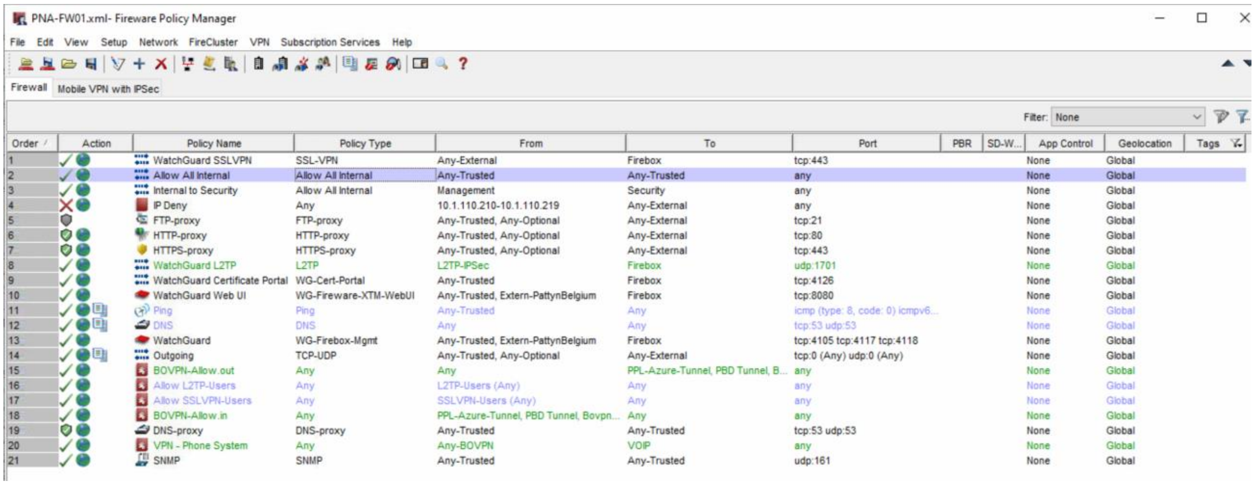
Action	Policies



Network Configuration

Virtual Local Area Network (VLAN) settings

ID	Name (Alias)	Zone	IPv4 Address	IPv6 Address	Secondary	Interfaces
1000	DMZ	Optional	[redacted] (DHCP server)			7
100	Guest Wifi	Optional	[redacted] (DHCP server)			7
200	Security	Optional	[redacted] (DHCP server)			7
60	Conference Rooms	Trusted	[redacted] (DHCP disabled)			6
27	Accounting	Trusted	[redacted] (DHCP relay)			6
90	Domotica	Trusted	[redacted] (DHCP disabled)			6
80	Backup	Trusted	[redacted] (DHCP disabled)			6
31	HRM	Trusted	[redacted] (DHCP relay)			6
28	IT	Trusted	[redacted] (DHCP relay)			6
62	Internal Wireless	Trusted	[redacted] (DHCP relay)			6
41	Kardex	Trusted	[redacted] (DHCP disabled)			6
29	Logistics	Trusted	[redacted] (DHCP relay)			6
30	Management	Trusted	[redacted] (DHCP relay)			6
25	Marketing	Trusted	[redacted] (DHCP relay)			6
1	Network Infrastructure	Trusted	[redacted] (DHCP relay)			6
22	Presales	Trusted	[redacted] (DHCP relay)			6
52	Printers	Trusted	[redacted] (DHCP relay)			6
17	Production Administrati...	Trusted	[redacted] (DHCP disabled)			6
19	Production Other	Trusted	[redacted] (DHCP disabled)			6
15	Production PXL	Trusted	[redacted] (DHCP disabled)			6
11	Production Team 1	Trusted	[redacted] (DHCP disabled)			6
12	Production Team 2	Trusted	[redacted] (DHCP disabled)			6
13	Production Team 3	Trusted	[redacted] (DHCP disabled)			6
14	Production Team 4	Trusted	[redacted] (DHCP disabled)			6
50	Produktieservers	Trusted	[redacted] (DHCP disabled)			6
21	Projects	Trusted	[redacted] (DHCP relay)			6
40	Propos	Trusted	[redacted] (DHCP disabled)			6
24	Purchase	Trusted	[redacted] (DHCP relay)			6
20	R and D	Trusted	[redacted] (DHCP relay)			6
23	Sales	Trusted	[redacted] (DHCP relay)			6
70	Beheer	Trusted	[redacted] (DHCP disabled)			6
32	Service	Trusted	[redacted] (DHCP relay)			6
16	Software	Trusted	[redacted] (DHCP disabled)			6
33	Tech	Trusted	[redacted] (DHCP relay)			6
51	Testservers	Trusted	[redacted] (DHCP disabled)			6
61	VOIP	Trusted	[redacted] (DHCP disabled)			6
26	Warehouse	Trusted	[redacted] (DHCP relay)			6



PNA-FW01.xml- Fireware Policy Manager

Filter: None

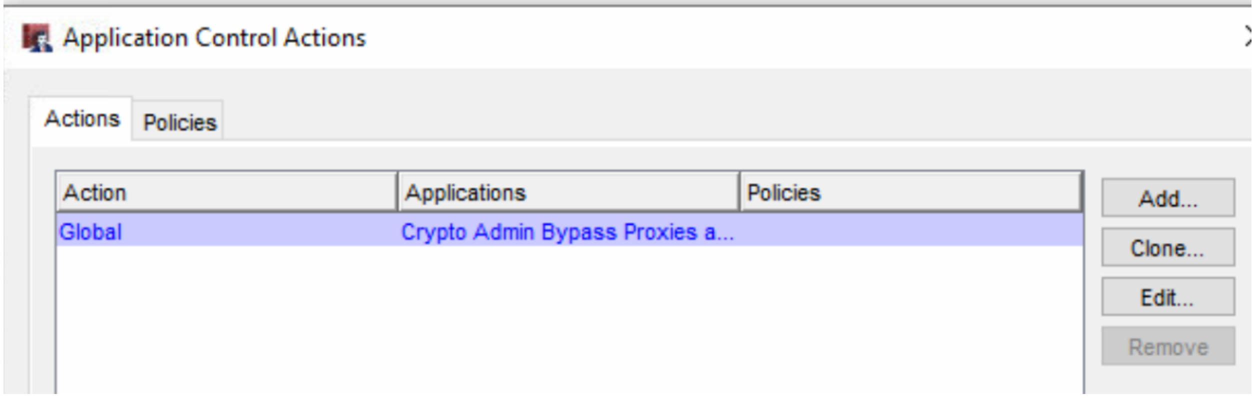
Order	Action	Policy Name	Policy Type	From	To	Port	PBR	SD-W...	App Control	Geolocation	Tags
1	✓ ●	WatchGuard SSLVPN	SSL-VPN	Any-External	Firebox	tcp:443			None	Global	
2	✓ ●	Allow All Internal	Allow All Internal	Any-Trusted	Any-Trusted	any			None	Global	
3	✓ ●	Internal to Security	Allow All Internal	Management	Security	any			None	Global	
4	✗ ●	IP Deny	Any	10.1.110.210-10.1.110.219	Any-External	any			None	Global	
5	🛡	FTP-proxy	FTP-proxy	Any-Trusted, Any-Optional	Any-External	tcp:21			None	Global	
6	🛡 ●	HTTP-proxy	HTTP-proxy	Any-Trusted, Any-Optional	Any-External	tcp:80			None	Global	
7	🛡 ●	HTTPS-proxy	HTTPS-proxy	Any-Trusted, Any-Optional	Any-External	tcp:443			None	Global	
8	✓ ●	WatchGuard L2TP	L2TP	L2TP-IPSec	Firebox	udp:1701			None	Global	
9	✓ ●	WatchGuard Certificate Portal	WG-Cert-Portal	Any-Trusted	Firebox	tcp:4126			None	Global	
10	✓ ●	WatchGuard Web UI	WG-Fireware-XTM-WebUI	Any-Trusted, Extern-PattynBelgium	Firebox	tcp:8080			None	Global	
11	✓ ●	Ping	Ping	Any-Trusted	Any	icmp (type: 8, code: 0) icmpv6...			None	Global	
12	✓ ●	DNS	DNS	Any	Any	tcp:53 udp:53			None	Global	
13	✓ ●	WatchGuard	WG-Firebox-Mgmt	Any-Trusted, Extern-PattynBelgium	Firebox	tcp:4105 tcp:4117 tcp:4118			None	Global	
14	✓ ●	Outgoing	TCP-UDP	Any-Trusted, Any-Optional	Any-External	tcp:0 (Any) udp:0 (Any)			None	Global	
15	✓ ●	BOVPN-Allow.out	Any	Any	PPL-Azure-Tunnel, PBD Tunnel, B...	any			None	Global	
16	✓ ●	Allow L2TP-Users	Any	L2TP-Users (Any)	Any	any			None	Global	
17	✓ ●	Allow SSLVPN-Users	Any	SSLVPN-Users (Any)	Any	any			None	Global	
18	✓ ●	BOVPN-Allow.in	Any	PPL-Azure-Tunnel, PBD Tunnel, Bovpn...	Any	any			None	Global	
19	🛡 ●	DNS-proxy	DNS-proxy	Any-Trusted	Any-Trusted	tcp:53 udp:53			None	Global	
20	✓ ●	VPN - Phone System	Any	Any-BOVPN	VOIP	any			None	Global	
21	✓ ●	SNMP	SNMP	Any-Trusted	Any-Trusted	udp:161			None	Global	

IntraVLAN packet inspection is not on.

BOVPN policies wide open.

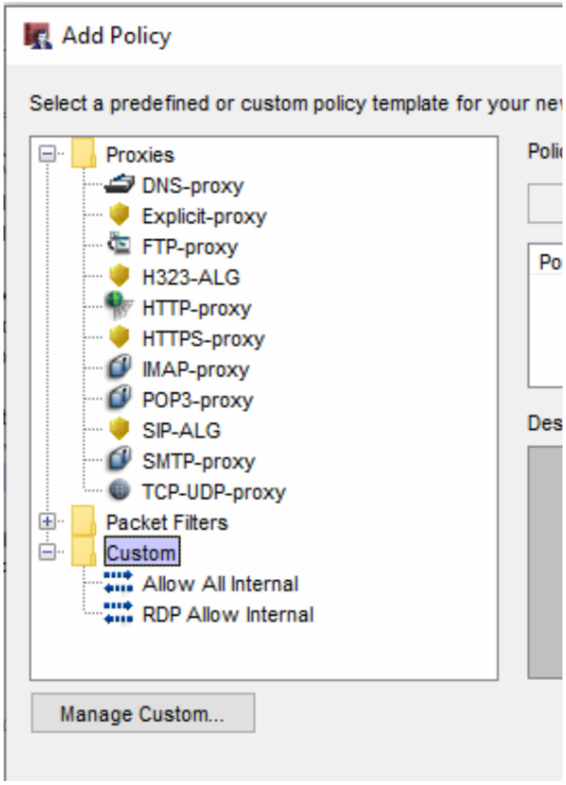
Outgoing is wide open. This should be DELETED.

Application control not even being used.



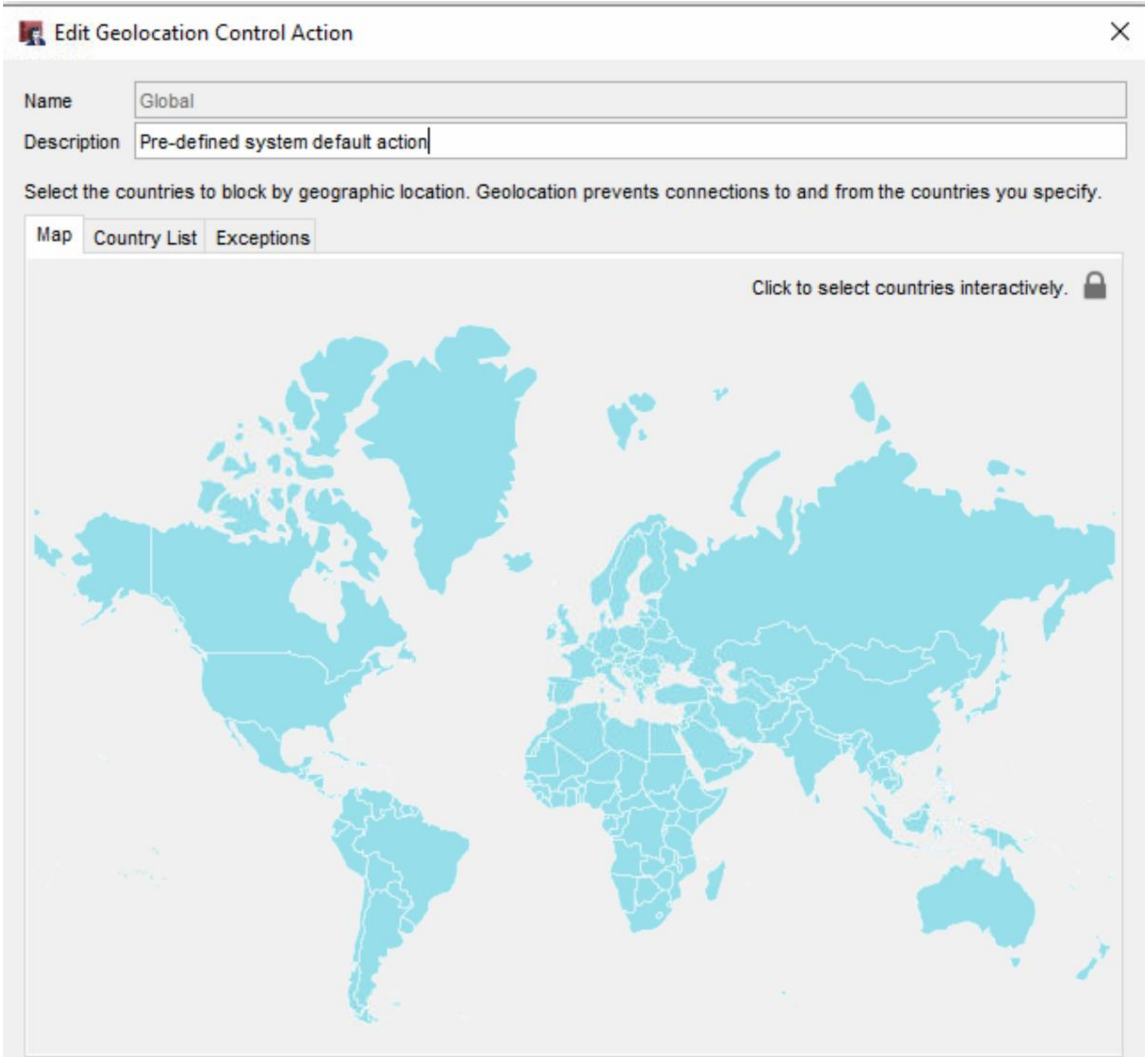
Action	Applications	Policies
Global	Crypto Admin Bypass Proxies a...	

No effective custom port collections going on. These are silly because they are an **Any** policy, which is the antithesis of security.



Select a predefined or custom policy template for your ne

Geo policy is turned on, but does absolutely nothing because it is not configured to block anything.

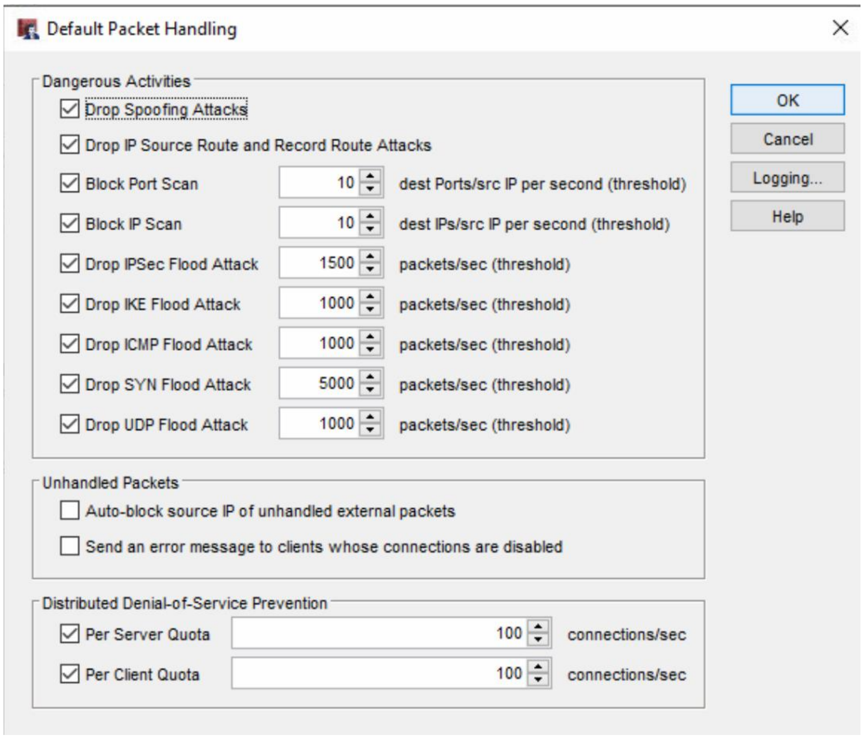


Edit Geolocation Control Action

Name: Global

Description: Pre-defined system default action

Select the countries to block by geographic location. Geolocation prevents connections to and from the countries you specify.



Default Packet Handling

Dangerous Activities

☑ Drop Spoofing Attacks

☑ Drop IP Source Route and Record Route Attacks

☑ Block Port Scan 10 dest Ports/src IP per second (threshold)

☑ Block IP Scan 10 dest IPs/src IP per second (threshold)

☑ Drop IPSec Flood Attack 1500 packets/sec (threshold)

☑ Drop IKE Flood Attack 1000 packets/sec (threshold)

☑ Drop ICMP Flood Attack 1000 packets/sec (threshold)

☑ Drop SYN Flood Attack 5000 packets/sec (threshold)

☑ Drop UDP Flood Attack 1000 packets/sec (threshold)

Unhandled Packets

□ Auto-block source IP of unhandled external packets

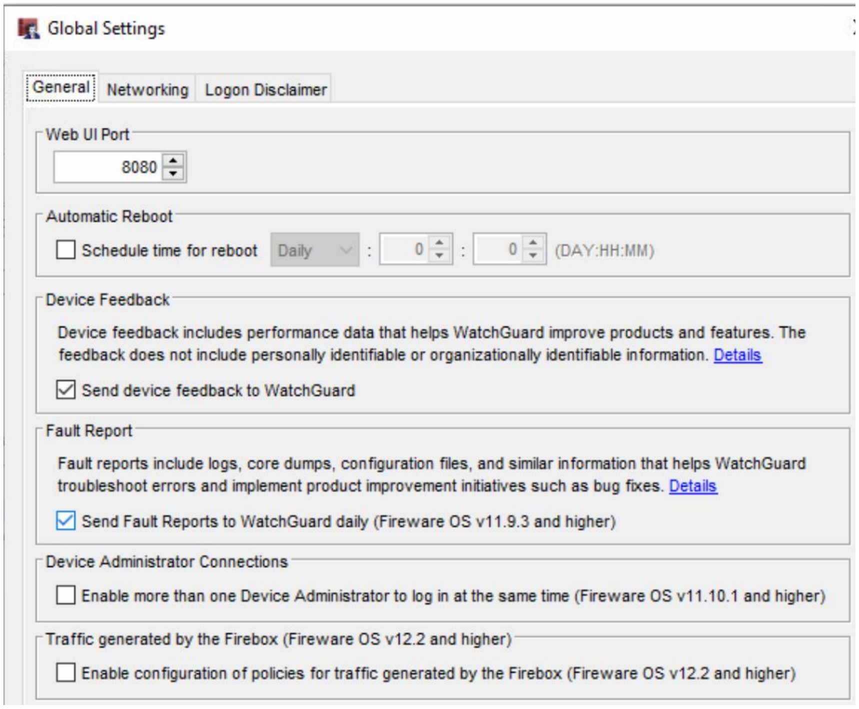
□ Send an error message to clients whose connections are disabled

Distributed Denial-of-Service Prevention

☑ Per Server Quota 100 connections/sec

☑ Per Client Quota 100 connections/sec

incorrect settings



Global Settings

Web UI Port

8080

Automatic Reboot

□ Schedule time for reboot Daily : 0 : 0 (DAY:HH:MM)

Device Feedback

Device feedback includes performance data that helps WatchGuard improve products and features. The feedback does not include personally identifiable or organizationally identifiable information. Details

☑ Send device feedback to WatchGuard

Fault Report

Fault reports include logs, core dumps, configuration files, and similar information that helps WatchGuard troubleshoot errors and implement product improvement initiatives such as bug fixes. Details

☑ Send Fault Reports to WatchGuard daily (Fireware OS v11.9.3 and higher)

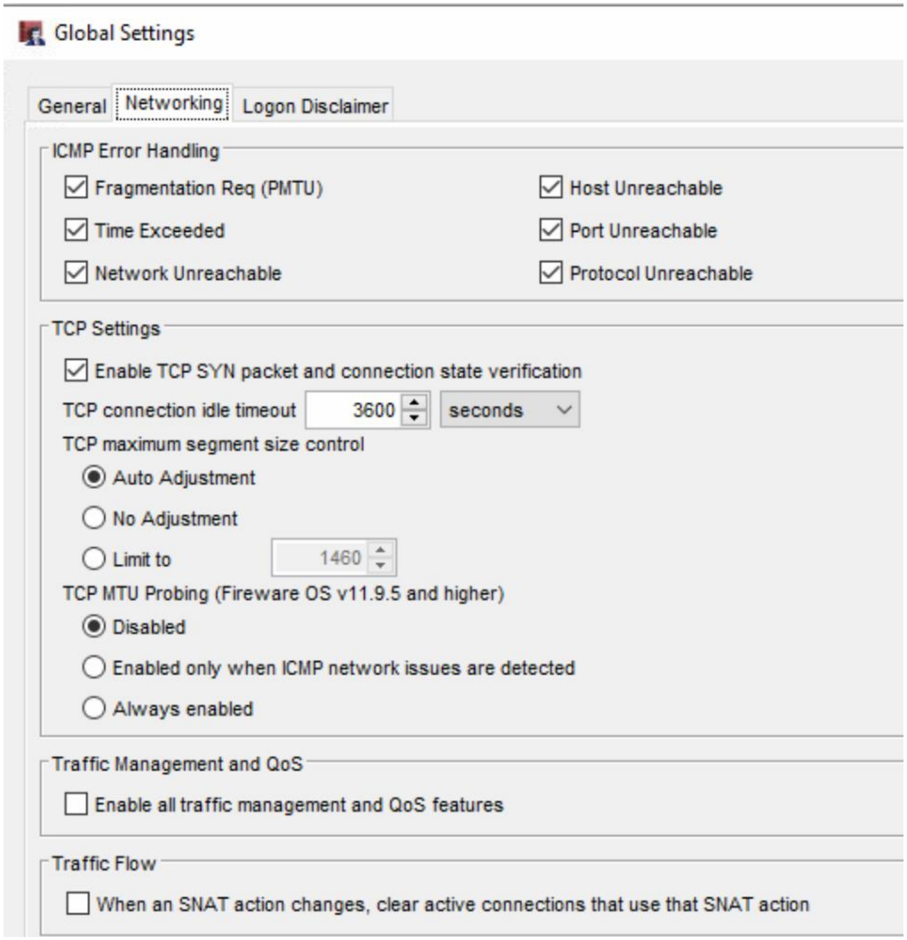
Device Administrator Connections

□ Enable more than one Device Administrator to log in at the same time (Fireware OS v11.10.1 and higher)

Traffic generated by the Firebox (Fireware OS v12.2 and higher)

□ Enable configuration of policies for traffic generated by the Firebox (Fireware OS v12.2 and higher)

incorrect settings



Global Settings

ICMP Error Handling

☑ Fragmentation Req (PMTU)
☑ Host Unreachable
☑ Time Exceeded
☑ Port Unreachable
☑ Network Unreachable
☑ Protocol Unreachable

TCP Settings

☑ Enable TCP SYN packet and connection state verification

TCP connection idle timeout 3600 seconds

TCP maximum segment size control

● Auto Adjustment
○ No Adjustment
○ Limit to 1460

TCP MTU Probing (Fireware OS v11.9.5 and higher)

● Disabled
○ Enabled only when ICMP network issues are detected
○ Always enabled

Traffic Management and QoS

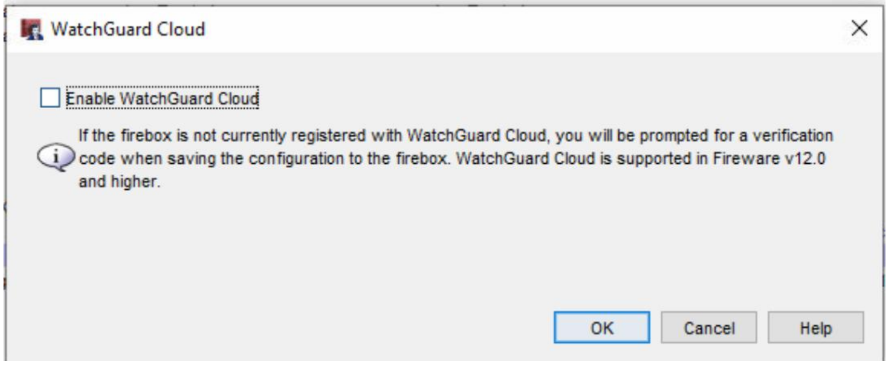
□ Enable all traffic management and QoS features

Traffic Flow

□ When an SNAT action changes, clear active connections that use that SNAT action

incorrect settings

Not even enrolled in WatchGuard Cloud.

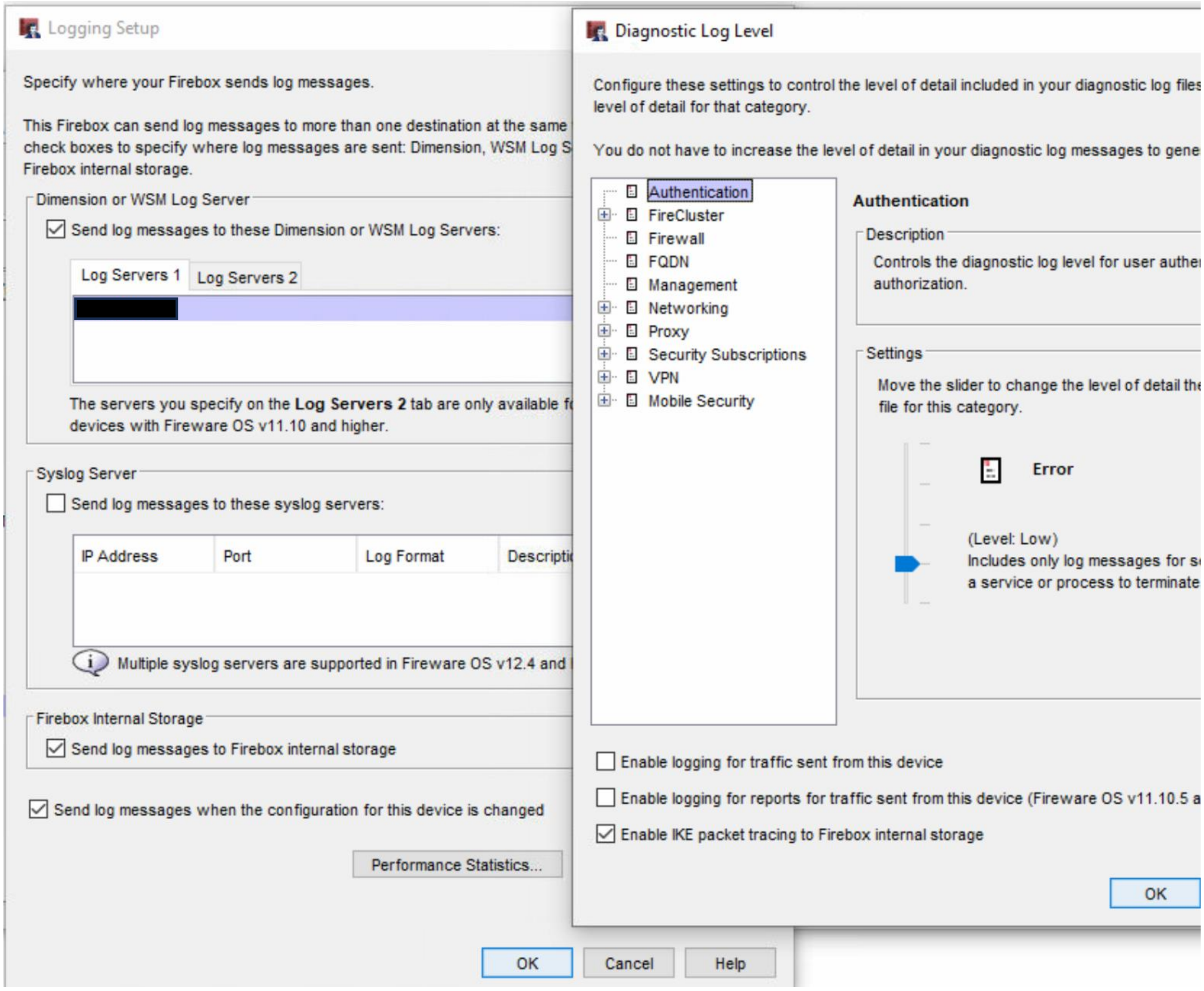


WatchGuard Cloud

□ Enable WatchGuard Cloud

If the firebox is not currently registered with WatchGuard Cloud, you will be prompted for a verification code when saving the configuration to the firebox. WatchGuard Cloud is supported in Fireware v12.0 and higher.

Logging not enabled.



Logging Setup

Specify where your Firebox sends log messages.

This Firebox can send log messages to more than one destination at the same
check boxes to specify where log messages are sent: Dimension, WSM Log S
Firebox internal storage.

Dimension or WSM Log Server

☑ Send log messages to these Dimension or WSM Log Servers:

Log Servers 1 | Log Servers 2

[redacted]

The servers you specify on the **Log Servers 2** tab are only available f
devices with Fireware OS v11.10 and higher.

Syslog Server

☐ Send log messages to these syslog servers:

IP Address	Port	Log Format	Descripti

Multiple syslog servers are supported in Fireware OS v12.4 and

Firebox Internal Storage

☑ Send log messages to Firebox internal storage

☑ Send log messages when the configuration for this device is changed

Diagnostic Log Level

Configure these settings to control the level of detail included in your diagnostic log files
level of detail for that category.

You do not have to increase the level of detail in your diagnostic log messages to gene

Authentication

Description

Controls the diagnostic log level for user authe
authorization.

Settings

Move the slider to change the level of detail the
file for this category.

Error

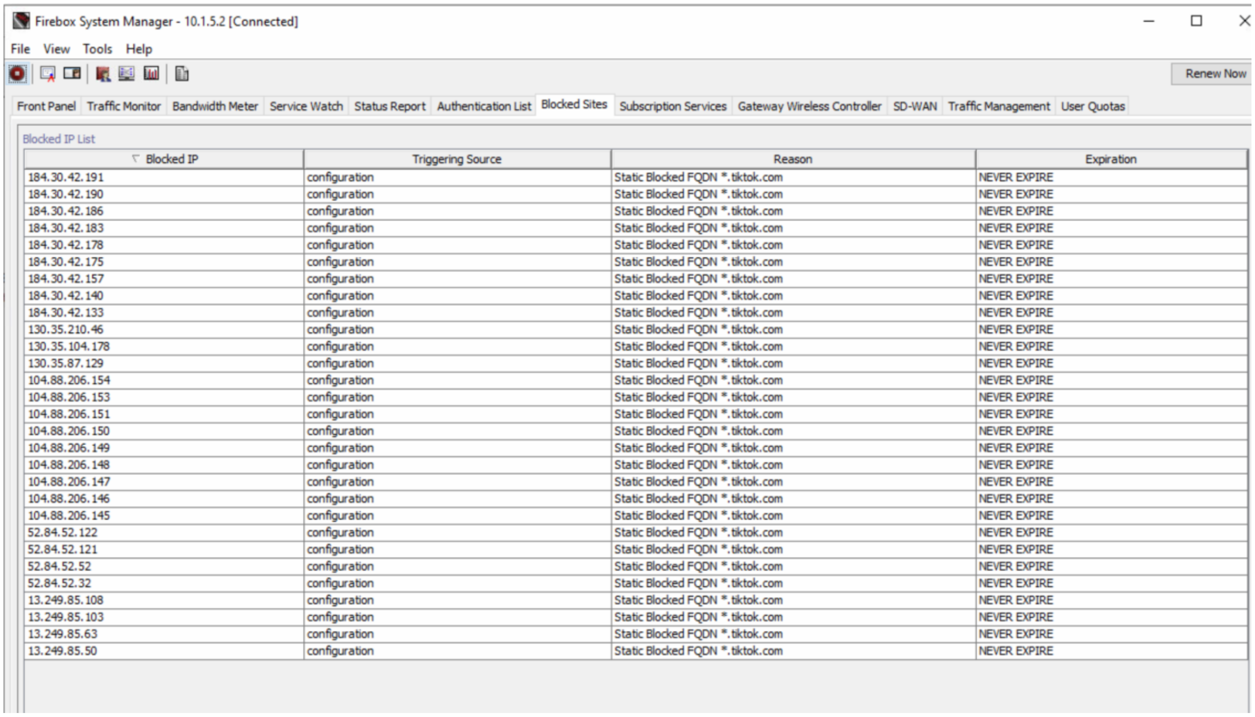
(Level: Low)
Includes only log messages for s
a service or process to terminate

☐ Enable logging for traffic sent from this device

☐ Enable logging for reports for traffic sent from this device (Fireware OS v11.10.5 a

☑ Enable IKE packet tracing to Firebox internal storage

Autoblocking not configured.



Blocked IP	Triggering Source	Reason	Expiration
184.30.42.191	configuration	Static Blocked FQDN *.tiktok.com	NEVER EXPIRE
184.30.42.190	configuration	Static Blocked FQDN *.tiktok.com	NEVER EXPIRE
184.30.42.186	configuration	Static Blocked FQDN *.tiktok.com	NEVER EXPIRE
184.30.42.183	configuration	Static Blocked FQDN *.tiktok.com	NEVER EXPIRE
184.30.42.178	configuration	Static Blocked FQDN *.tiktok.com	NEVER EXPIRE
184.30.42.175	configuration	Static Blocked FQDN *.tiktok.com	NEVER EXPIRE
184.30.42.157	configuration	Static Blocked FQDN *.tiktok.com	NEVER EXPIRE
184.30.42.140	configuration	Static Blocked FQDN *.tiktok.com	NEVER EXPIRE
184.30.42.133	configuration	Static Blocked FQDN *.tiktok.com	NEVER EXPIRE
130.35.210.46	configuration	Static Blocked FQDN *.tiktok.com	NEVER EXPIRE
130.35.104.178	configuration	Static Blocked FQDN *.tiktok.com	NEVER EXPIRE
130.35.87.129	configuration	Static Blocked FQDN *.tiktok.com	NEVER EXPIRE
104.88.206.154	configuration	Static Blocked FQDN *.tiktok.com	NEVER EXPIRE
104.88.206.153	configuration	Static Blocked FQDN *.tiktok.com	NEVER EXPIRE
104.88.206.151	configuration	Static Blocked FQDN *.tiktok.com	NEVER EXPIRE
104.88.206.150	configuration	Static Blocked FQDN *.tiktok.com	NEVER EXPIRE
104.88.206.149	configuration	Static Blocked FQDN *.tiktok.com	NEVER EXPIRE
104.88.206.148	configuration	Static Blocked FQDN *.tiktok.com	NEVER EXPIRE
104.88.206.147	configuration	Static Blocked FQDN *.tiktok.com	NEVER EXPIRE
104.88.206.146	configuration	Static Blocked FQDN *.tiktok.com	NEVER EXPIRE
104.88.206.145	configuration	Static Blocked FQDN *.tiktok.com	NEVER EXPIRE
52.84.52.122	configuration	Static Blocked FQDN *.tiktok.com	NEVER EXPIRE
52.84.52.121	configuration	Static Blocked FQDN *.tiktok.com	NEVER EXPIRE
52.84.52.52	configuration	Static Blocked FQDN *.tiktok.com	NEVER EXPIRE
52.84.52.32	configuration	Static Blocked FQDN *.tiktok.com	NEVER EXPIRE
13.249.85.108	configuration	Static Blocked FQDN *.tiktok.com	NEVER EXPIRE
13.249.85.103	configuration	Static Blocked FQDN *.tiktok.com	NEVER EXPIRE
13.249.85.63	configuration	Static Blocked FQDN *.tiktok.com	NEVER EXPIRE
13.249.85.50	configuration	Static Blocked FQDN *.tiktok.com	NEVER EXPIRE

Revision history

4/19/2023	Felicia King	First draft