OPSWAT

AGD Documentation

OPSWAT NetWall Unidirectional Security Gateway Evaluation Assurance Level (EAL): 4 augmented with ALC_DVS.2, ALC_FLR.2, and AVA_VAN.5

TOE Reference:	OPSWAT NetWall USG-100
Version	v1.2
Date	2024-04-18
Classification:	PUBLIC

Version history

Version	Date	Author	Description
v1.0	2023-10-30	OPSWAT	The first version of the AGD documentation.
v1.1	2024-02-23	OPSWAT	Amendments based on the 1st analysis cycle
V1.2	2024-04-18	OPSWAT	Section 3.5.1 included Amendments based on the 2nd analysis cycle

Table of Contents

1 Introduction

The Target of Evaluation (TOE) consists of a TX Module that connects with a sending or trusted network and a RX Module that connects to a receiving or untrusted network. Both modules enforce a one-way information flow control policy on network traffic flowing through the TOE.

This document was created to fulfil the following assurance requirements of [CC_P3]:

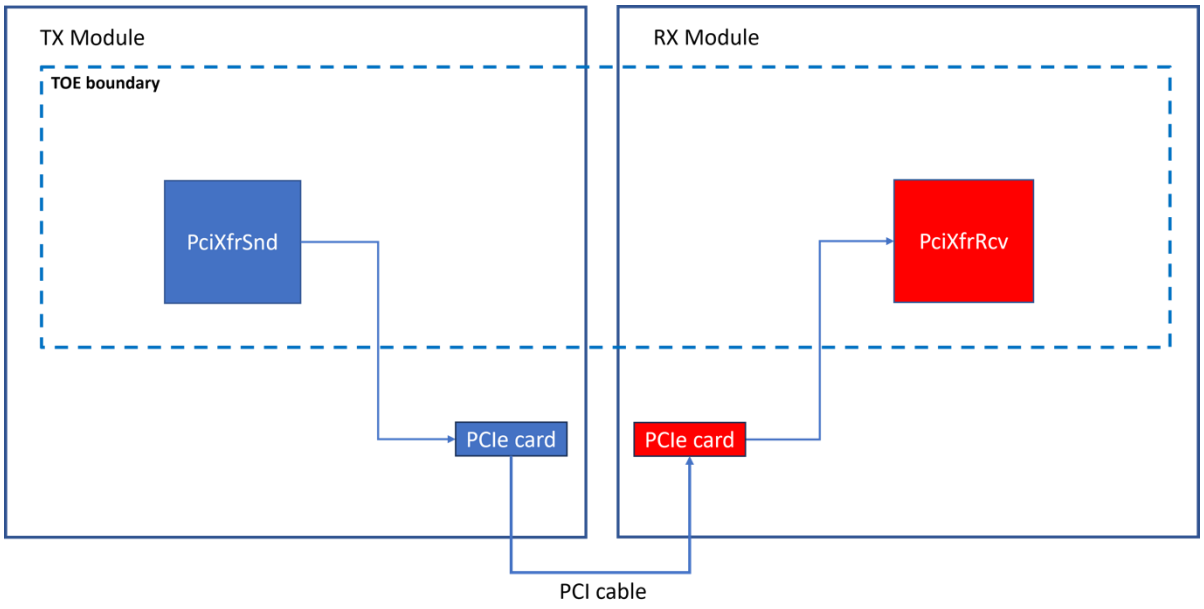
- Operational user guidance (AGD_OPE.1)
- Preparative procedures (AGD_PRE.1)

1.1 Purpose

This document provides guidance on the secure installation and secure use of the TOE for the Common Criteria (CC) Evaluation Assurance Level 4 Evaluated Configuration. This should be used as the guiding document for the installation and administration of the TOE in the CC-evaluated configuration. The official OPSWAT NetWall Unidirectional Security Gateway documentation should be referred to and followed only as directed within this document.

1.2 TOE Configuration

Figure 1 - TOE Subsystems and modules



1.3 TX Module Subsystem

- **PciXfrSnd Module**: PciXfrSnd module reads network frames from the sending network, transforms them into internal data representation and sends that to the PciXfrRcv module over a single PCI cable.

1.4 RX Module Subsystem

- **PciXfrRcv Module**: PciXfrRcv module receives the internal data sent by PciXfrSnd module over a PCI cable, extracts the network frames from the data, ensuring data integrity over both pairs is intact and recreates the network payload into the receiving network by injecting that data into the newly created network connections.

1.5 TOE Security Functional Interfaces

- The blue and red brackets outlined in the diagram mark the TOE boundaries for the TX and RX Modules.
- PciXfrSnd and PciXfrRcv can be notified of a config update by terminating the process. This will trigger the Read Config function for updating the configuration from the Config Database.
- PciXfrSnd and PciXfrRcv upon startup will query the configuration from the Config Database via the Read Config Interface using the Read config function to retrieve the configuration for TCP Connector Stream(s) and UDP Connector Stream(s).
- PciXfrSnd based on its configuration can create a TCP (or UDP) Connector Stream socket on a specific port sending the received TCP/UDP data from the Connectors.
- PciXfrRcv based on its configuration can create a TCP (or UDP) Connector Stream socket via the TCP and UDP Connector Stream interface and send TCP/UDP data received from PciXfrSnd to the Connector(s).

Figure 2 - TOE boundary and architecture

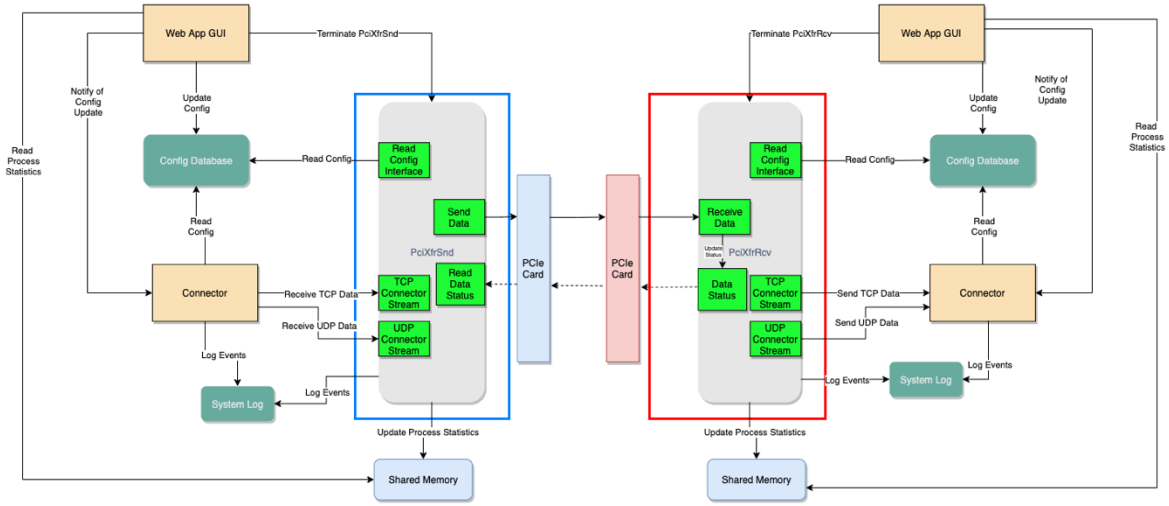


Figure 2 shows the TOE architecture containing the TOE and non-TOE components. The blue and red brackets are indicating the TOE itself. The TSFIs can be found in the green (inside PciXfrSnd or PciXfrRcv) and white boxes in the blue and red brackets.

2 Operational User's Guide

2.1 Functions, privileges, and appropriate warnings

The product has only one available role, the Admin. The users can log in to the Web App GUI or CLI interfaces of the product, but they cannot change any configuration without a plugged-in security dongle.

Product functions

- Security Dongle Management
- File Transfer
- Advanced Menu
- User Accounts

- Port Scan Detect
- System Log
- Backups
- Statistics
- Software Updates

TOE functions

- Read Config
- Notify of Config Update
- TCP/UDP streaming
    - Data transfer (it is not a separate function; data transfer is done within the TCP/UDP streams)
- Read Status
- Update Status

The following table describes the functions and appropriate TSFI mapped together.

Table 1 – TOE available functions

TSFI	Function	Warning
Read Config Interface	Read Config	N/A
Notify Interface	Notify of Config Update	N/A
TCP Connector Stream	TCP Streaming	N/A
UDP Connector Stream	UDP Streaming	N/A
Send Data	Data Transfer	N/A
Read Data status	Read Data Status	N/A
Receive Data	Data Transfer	N/A
Update Data status	Data Status	N/A

There are no warning messages from the TOE to the users since there is no direct communication between the TOE and the users.

2.2 Product functions

Brief introduction of the product functions which are out the TOE scope.

2.2.1 Security Dongle Management

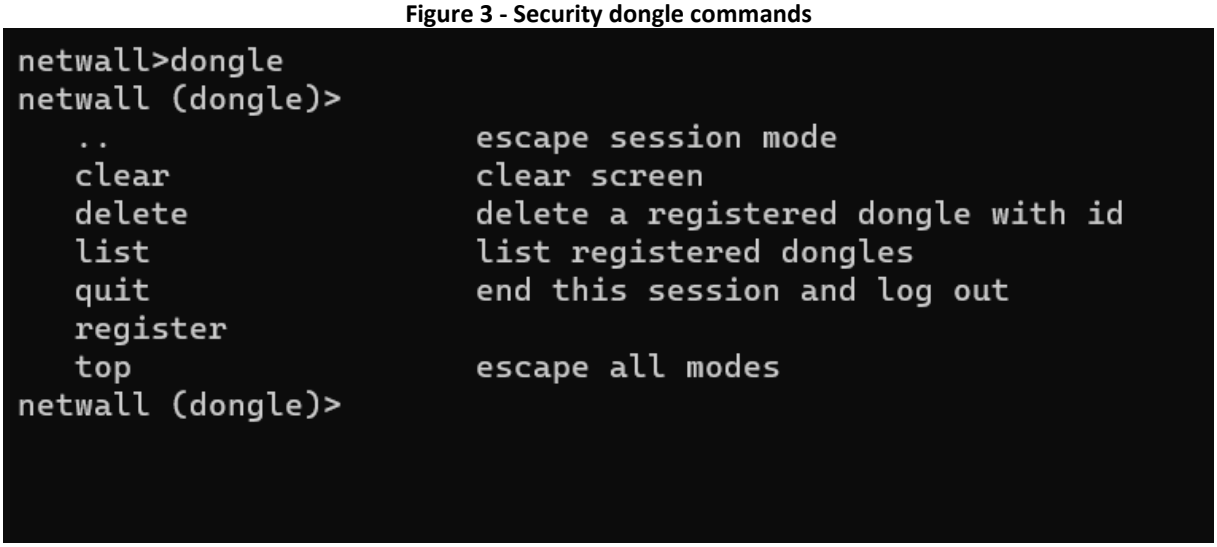
Admin can access the security dongle registration function by the CLI connecting a display and a keyboard in the desired appliance and using the command *dongles*. Before doing that, admin must input right credentials.

Commands: There are several specific commands for dongle registration:

- delete: this command deletes a registered dongle, parameters:
- list: this command displays a list of registered dongles

- register: this command registers a plugged dongle to be used with that appliance

Figure 3 - Security dongle commands



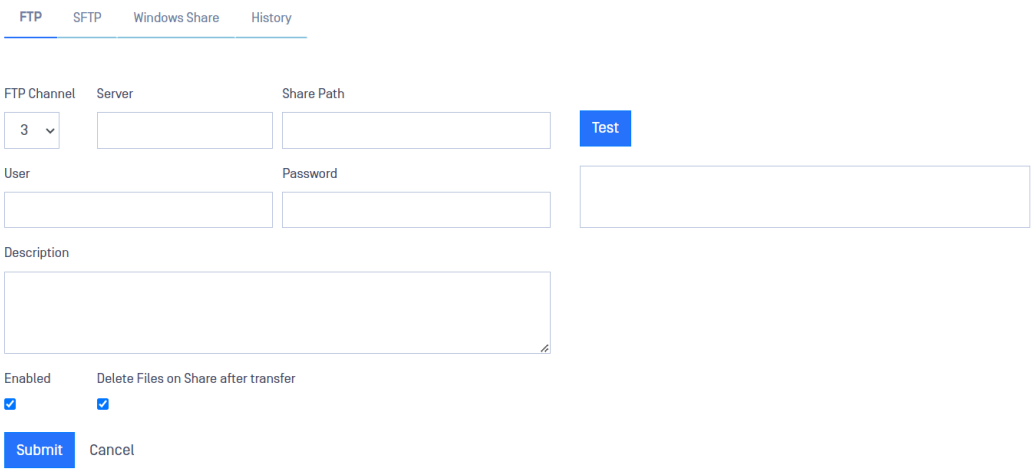
The rest of the commands are not specific for dongle registration function.

2.2.2 File Transfer

Admin can access the Web App GUI to configure File transfer functions. To do that, Admin must input right credentials and to have a security dongle registered and plugged in. Once properly configured it would be possible to transfer files from the sending to the receiving network using the following protocols:

- FTP: Files will be copied in a folder placed in the sending network and the file will be transferred to a folder placed in the receiving network. To do so, a customer-owned FTP server is needed to be configured in the sending network and a customer-owned FTP server configured in the receiving network.
- SFTP: Files will be copied in a folder placed in the sending network and the file will be transferred to a folder placed in the receiving network. To do so, a customer-owned SFTP server is needed to be configured in the sending network and a customer-owned SFTP server configured in the receiving network.
- Windows File Share: Files will be copied in a shared folder placed in the sending network and the file will be transferred to a shared folder placed in the receiving network.

Figure 4 - File Transfer



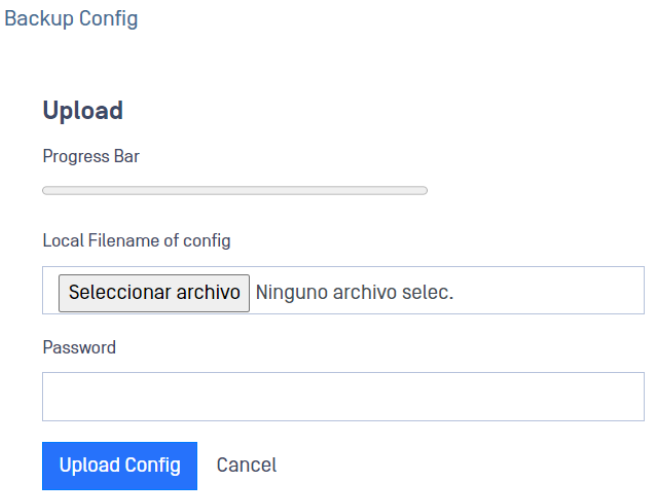
2.2.3 Backups

Admin can access the Web App GUI to store and apply backups. To do that, Admin must input the right credentials and have a security dongle registered and plugged in.

Operations:

- Comment: when a backup is stored by clicking on Snapshot Running Config, the user can include a comment in a free text box.
- Upload: admin can upload a previously stored backup to apply it after that.

Figure 5 - Backups



2.2.4 System Logs

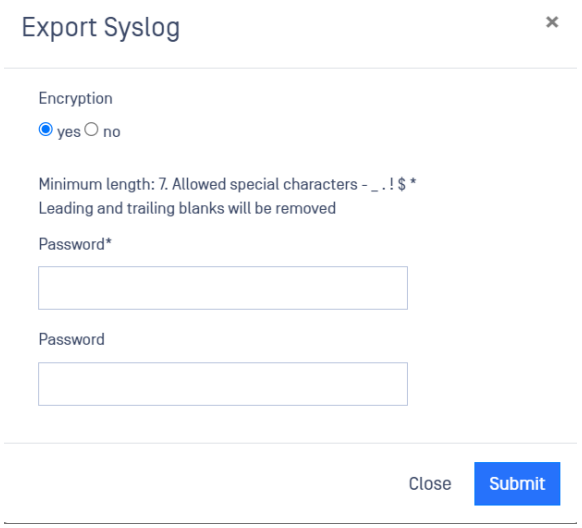
Admin can access the Web App GUI to check and export the system log. To do that, Admin must input right credentials. Also, system log can be checked in the CLI using the command *taillog*. When exporting the log from the Web App GUI, there are a couple of parameters to be filled in.

Figure 6 - System logs

```
Last login: Thu Feb  1 09:07:54 2024 from 10.15.52.10
OPSWAT Shell
Type question mark (?) to see a list of available commands.
License is Valid.
No blocked IPs
NetWall USG (Unidirectional)
USG-100 Version: 1.0.0 Config Version: 5.5.0
netwall-usg-mxh914-blue>taillog
Feb  1 09:08:20 netwall-usg-mxh914-blue Dnp3Blue[3310]: MasterStation::MainThread stationId = 5, Event = WAIT_AFTER_FAIL
ED_CONNECT
Feb  1 09:08:20 netwall-usg-mxh914-blue Dnp3Blue[3310]: MasterStation::MainThread stationId = 6, Event = CONNECTING
Feb  1 09:08:20 netwall-usg-mxh914-blue Dnp3Blue[3310]: MasterStation::MainThread stationId = 6, Event = WAIT_AFTER_FAIL
ED_CONNECT
Feb  1 09:08:20 netwall-usg-mxh914-blue Dnp3Blue[3310]: MasterStation::MainThread stationId = 7, Event = CONNECTING
Feb  1 09:08:20 netwall-usg-mxh914-blue Dnp3Blue[3310]: MasterStation::MainThread stationId = 7, Event = WAIT_AFTER_FAIL
ED_CONNECT
Feb  1 09:08:20 netwall-usg-mxh914-blue UaClientBlue[3265]: UaClientBlue ArTcp.SendData  Connected: 127.0.0.1 port 61090
Feb  1 09:08:20 netwall-usg-mxh914-blue UaClientBlue[3265]: UaClientBlue DataSendBrowse.SendBrowserData  Header and Brow
ser Data Send Resume count 0
Feb  1 09:08:20 netwall-usg-mxh914-blue UaClientBlue[3265]: UaClientBlue DataSendBrowse.SendBrowserData  Send last Brows
er Record, count 942
Feb  1 09:08:22 netwall-usg-mxh914-blue UaClientBlue[3265]: UaClientBlue DataSendValues.PostAllValues  Send all values t
o Red
Feb  1 09:08:22 netwall-usg-mxh914-blue UaClientBlue[3265]: UaClientBlue ArTcp.SendData  Connected: 127.0.0.1 port 61091
Feb  1 09:08:29 netwall-usg-mxh914-blue mwatchd[3059]: msg=memory.ok mt=16622235648 mf=14190657536 bu=14393344 ca=154600
2432 fa=0.052411
Feb  1 09:08:30 netwall-usg-mxh914-blue Dnp3Blue[3310]: MasterStation::MainThread stationId = 1, Event = CONNECTING
Feb  1 09:08:30 netwall-usg-mxh914-blue Dnp3Blue[3310]: MasterStation::MainThread stationId = 1, Event = WAIT_AFTER_FAIL
```

The encryption check box to indicate if the exported log should be encrypted or not, if the log is encrypted the password is required for decrypt.

Figure 7 - Export logs



Password must be at least 7 characters and can be comprised of alphanumeric values and the following special characters - _ . ! $ *.

2.2.5 Advanced Menu

Admin can access the Web App GUI to check and edit Advanced settings like Diagnostics tools or Networking configuration, among others. To change these settings, the Admin must input the right credentials and a security dongle must be plugged in the appliance.

2.2.6 User Accounts

Admin can access the Web App GUI to check and edit the current users accounts to access NetWall Unidirectional Security Web App GUI and CLI. To change these settings, the Admin must input the right credentials and a security dongle must be plugged in the appliance.

Parameters:

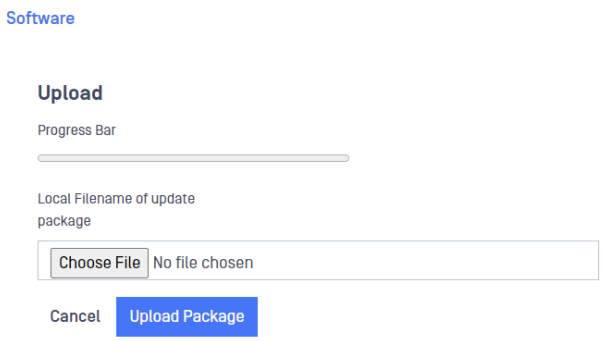
- Username: username of the user account being created or edited
- Password: Password to access the appliance using the Web App GUI or the CLI.
- Password confirm: Confirmation of the previously indicated password.
- Description: Optional description for the user account being created/edited.
- Email address: Optional email address associated to the user account.
- Force Password reset: Checkbox to indicate if it is required to change the password of the user account the first time it is used.
- Enabled: Checkbox to enable/disable the User account.

2.2.7 Software Update

Admin can access the Web App GUI to Upload and Apply software updates. To do that, Admin must input the right credentials and have a security dongle registered and plugged in. Also, previously uploaded software updates can be applied from the CLI.
From the Web App GUI:

- Select File: User needs to load the update software package before applying it. This button will be used to search for this file and select it. Once selected, the package needs to be uploaded to the appliance by pressing the Upload Package button.
- After that, the new software can be applied by pushing the apply button.

Figure 8 - Software update



From the CLI:

- list: provides a list of all the software packages uploaded to NetWall appliance, including the update number of each package
- apply: Apply one of the software updates present in the list. User needs to indicate the update number of the corresponding package.

- delete: Delete one of the software updates present in the list. User needs to indicate the update number of the packet needed to deletion.

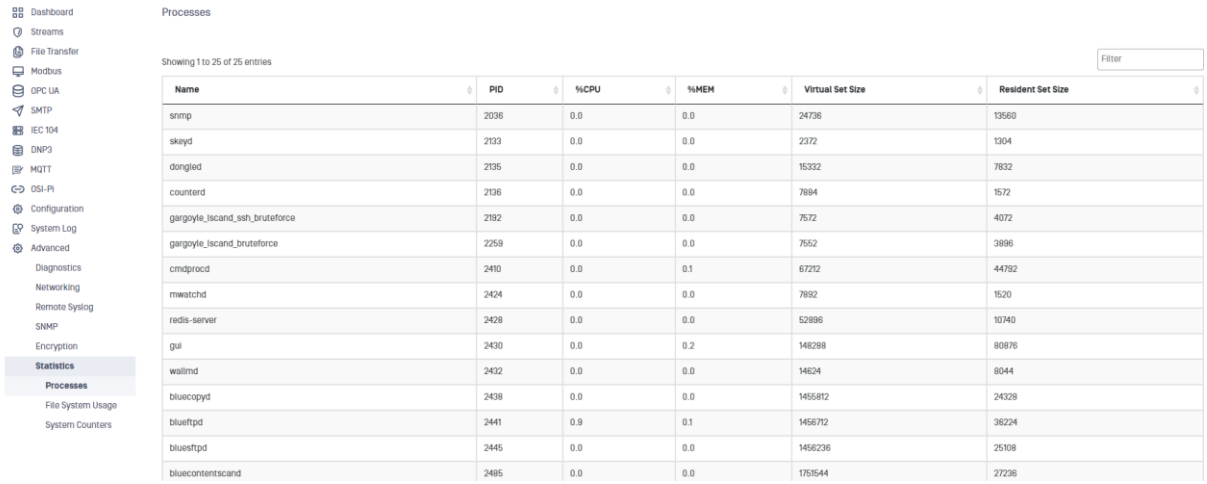
Figure 9 - Software update operations

```
netwall (software)>
   ..                    escape session mode
   apply                 apply an update
   clear                 clear screen
   delete                delete a software update
   list                  show available software updates on device
   quit                  end this session and log out
   top                   escape all modes
netwall (software)>
```

2.2.8 Statistics

Admins can access the Web App GUI to view the statistics produced by the product. An admin must authenticate to view the statistics.

Figure 10 - Statistics table in Web App GUI



Admin can check the following statistics:

- Processes: Statistics of the processes of the system.
- File System usage: Statistics of the File System.
- System Counters: Statistics sent by PciXfrSnd/PciXfrRcv.

2.2.9 Port Scan Detect

The Port Scan Detect feature protects against malicious port scan detection attacks. IP addresses that conduct overt scans (FIN/XMAS/NULL scans) are blocked immediately.

2.3 TOE Functions

2.3.1 TCP streaming and Data transfer

Once the TOE is configured, the Sending (BLUE) side of OPSWAT NetWall USG-100 establishes a Read TCP connection with the specified TCP data source on the Sending network and reads data from the data source. That data is transmitted across the data link in a proprietary non-routable packet format to the Receiving (RED) side of USG-100. The RED side of USG-100

establishes a Write TCP connection with the specified TCP data destination on the Receiving network and then streams the data from BLUE via TCP to the specified destination.

2.3.2 UDP streaming and Data transfer

Once the TOE is configured, the Sending (BLUE) side of OPSWAT NetWall USG-100 starts to read UDP data from the specified UDP data source on the Sending network. That data is transmitted across the data link in a proprietary non-routable packet format to the Receiving (RED) side of USG-100. Then the RED side of USG-100 streams the UDP data to the specified UDP data destination on the Receiving network.

2.3.3 Read Config

Read Config occurs in two distinct scenarios: during the TOE initialization (PciXfrSnd/PciXfrRcv start-up process) or if the TOE process is terminated via SIGKILL. Such process termination re-enacts the process startup sequence. During the process start-up all internal structures for the TOE TCP/UDP streams are initially empty. The TOE (PciXfrSnd/PciXfrRcv) utilizes the Read Config interface to initialize these from the database.

The Read Config interface opens the local database file. The database is opened using sqlite3 C/C++ Interface. Data read from the sqlite3 database, corresponds to the Web GUI App's configuration as defined above. There is no user input. An internal representation of this data is generated and used during the TOE's life cycle.

2.3.4 Read Data Status

Read Data Status is a function of PciXfrSnd that is reading a remote memory segment from PciXfrRcv over the PCIe Card and validating the status of the sent data by SendData function.

2.3.5 Data Status

Data Status is a function of PciXfrRcv that is updating a local memory segment with the status data received by ReceiveData function.

2.4 Security Relevant Events

This chapter describes each type of security-relevant event relative to the TOE functions and operation following failures or operational errors.

Table 2 – Security relevant events

Security relevant Event	User function	Action to take
Create TCP/UDP stream	Create a TCP/UDP Stream	Update the configuration database. Log the event to system log. Notify PciXfrSnd/PciXfrRcv of the configuration update.
Update TCP/UDP stream	Update a TCP/UDP Stream	Update the configuration database. Log the event to system log.

		Notify PciXfrSnd/PciXfrRcv of the configuration update.
Delete TCP/UDP stream	Delete a TCP/UDP Stream	Update the configuration database. Log the event to system log. Notify PciXfrSnd/PciXfrRcv of the configuration update.
Configuration failure	The read configuration cannot be initialized	There is no user required action. The TOE loads the previous working configuration if there is any error in the newly read and loaded configuration.

2.5 Modes of Operation

There is only one mode of operation for the TOE, if there is any operational error or failure the TOE will restart to revert to the same mode of operation.

2.6 Security Measures to be Followed

OE.PHYSICAL: The TOE and the PCI cable connecting the sending and receiving sides must be physically protected, within secure and controlled access facilities.

OE.ADMIN: Administrators with physical access to the TOE must follow the TOE guidance documentation to operate the TOE.

OE.NETWORK: Between sending and receiving networks the TOE must be the only interconnection.

3 Preparative Guidance

3.1 Acceptance of the TOE

The Customer can check in the invoice the Serial Number of the appliances sent to them. This Serial Number is also indicated on a label added to the appliances. This Serial Number can be compared with the Serial Number indicated in the invoice. Regarding software, OPSWAT will inform the users about the Software reference that needs to be installed to be compliant with the current certification in OPSWAT NetWall Unidirectional Security Gateway USG-100 Common Criteria Evaluated Configuration Guide. The customers will be able to check the different hashes of the update packages we provide to them by comparing it with the recommended version. In that way, the user can check if the installed software is the correct one.

The customer receives the following components:

- NetWall USG-100 BLUE with TX Module and TX Connector installed.
- NetWall USG-100 RED with the RX Module and RX Connector installed.
- Data Link cable
- Two security dongles
- Mounting rail kits and power cables

The TOE is delivered with all the necessary software components already installed, but the customer can download the evaluated version of the TOE from the https://my.opswat.com/portal/products page and the integrity of the downloaded files can be validated using the HASH values available for every version.

The documentation management can be found in section 3.2 Documentation Management and the acceptance procedures of the documents can be found in section 5.2.1 Documentation acceptance procedures of [ALC].

The common criteria related documentation is available at https://docs.opswat.com/netwall/netwall for download in PDF format with the corresponding hash values for integrity check.

3.2 TOE Installation

3.2.1 The preparative procedures

In chapter USG-100 Setup in [USG-UM] the prerequisites and the hardware requirements with the installation process can be found.

3.2.2 The TOE installation steps

By default, the TOE will be preinstalled for every customer. The users have the option to install the Common Criteria evaluated version of the TOE through the Device Updates functionality of the TOE. The description of the process can be found in chapter Software Updates of [P-UM] document.

3.3 Initial configuration

Chapter USG-100 Initial Configuration of [USG-UM] contains all the necessary configuration that should be done during the first start-up of the TOE.

3.4 Security Dongles

The TOE security dongles are USB devices that enable the user to change the configuration. I no dongle is inserted a user can login in the TOE using the Web App GUI or the CLI for either side (RED or BLUE) but cannot do any configuration changes. For details see chapter NetWall Unidirectional Security Gateway dongles of [P-UM] document.

3.5 Configure TCP/UDP Streaming from BLUE to RED

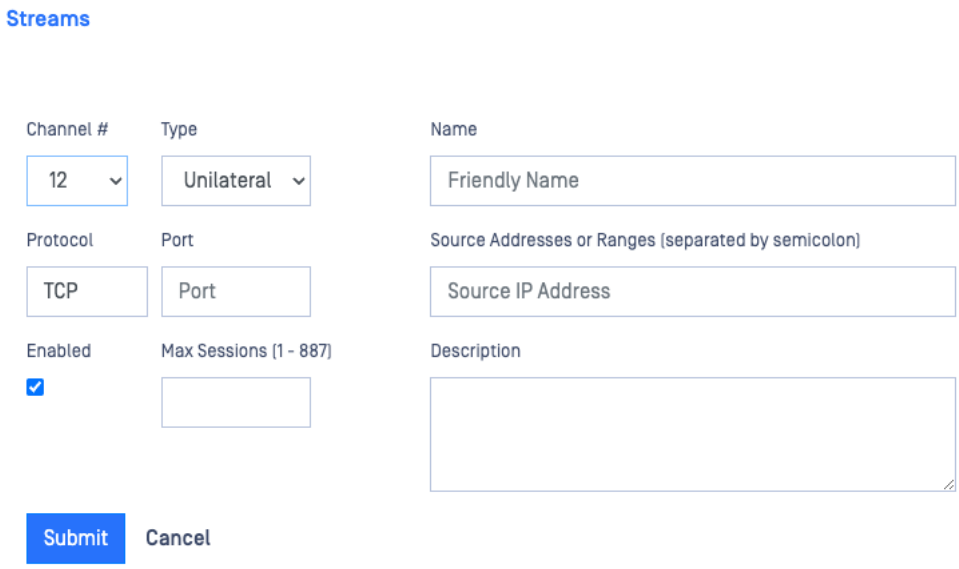
Every communication between the two sides of the TOE will be either through a TCP or UDP stream. The detailed description of the required configuration can be found in chapter TCP/UDP Streaming of [USG-UM] document and below.

Admin can access the Web App GUI to configure TCP/UDP Streaming functions. To do that, Admin must input right credentials and to have a security dongle registered and plugged in. There are several input fields needed to configure data transfer on BLUE and RED side:

- TCP BLUE:
  - Channel #: indicated the channel where the TCP streaming is performed, needs to be the same in BLUE and RED sides.
  - Type: Predefined to Unilateral.
  - Protocol: Predefined to TCP for TCP streaming.

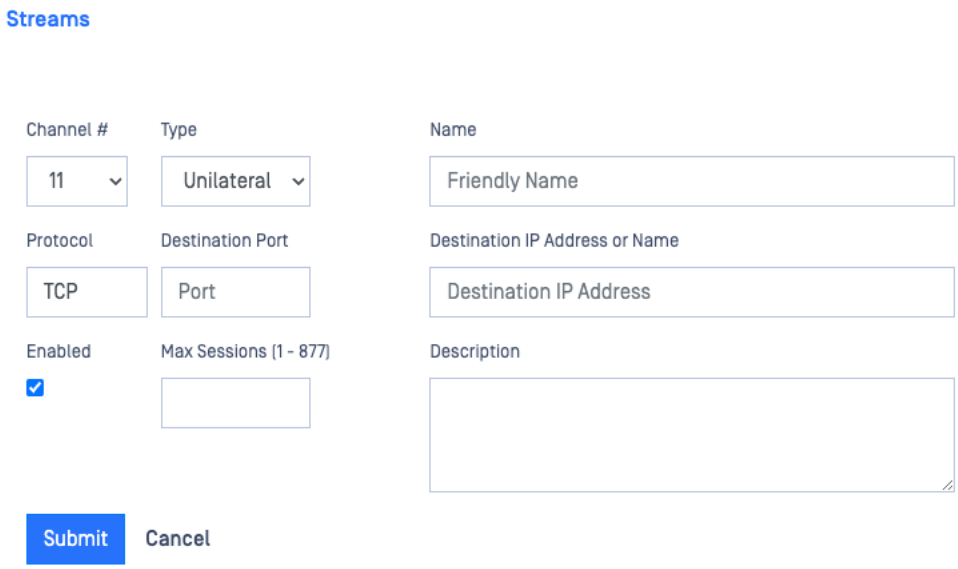
- Port: Port for the TCP source in BLUE side.
- Name: Friendly name to identify the stream.
- Source Addresses or Ranges (separated by semicolon): Source addresses or range of addresses where the TCP stream is originated.
- Max Sessions (1 - 191): Maximum number of TCP sessions to handle this stream.
- Description: Free text box for the user to include a description.
- Enabled: Check box to enable/disable the file transfer.

Figure 11 - TCP BLUE configuration via Web App GUI



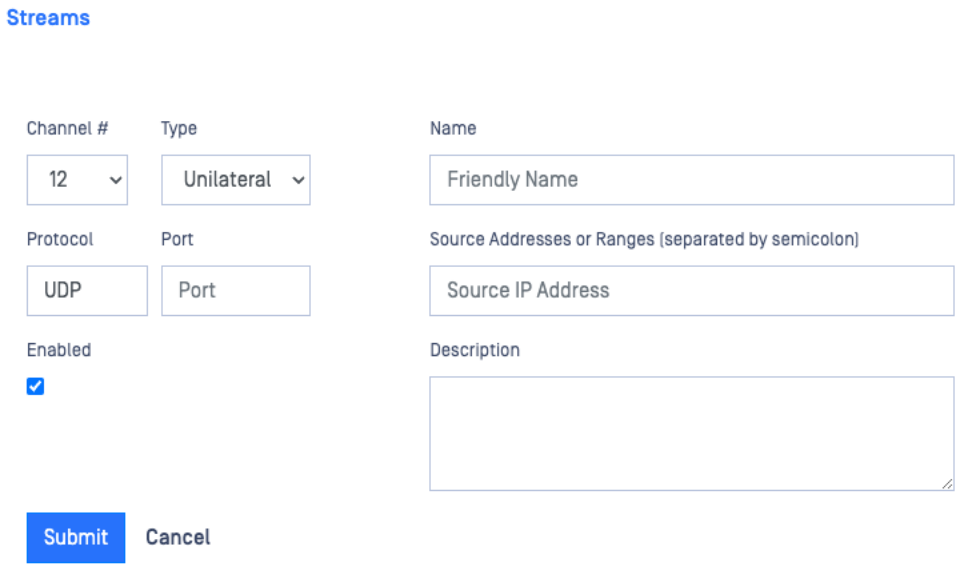
- TCP RED:
  - Channel #: indicated the channel where the TCP streaming is performed, needs to be the same in BLUE and RED sides.
  - Type: Predefined to Unilateral.
  - Protocol: Predefined to TCP for TCP streaming.
  - Destination Port: Port for the TCP destination in RED side.
  - Name: Friendly name to identify the stream.
  - Destination IP Addresses or Name: Destination addresses or range of addresses where the TCP stream is finished.
  - Max Sessions (1 - 191): Maximum number of TCP sessions to handle this stream
  - Description: Free text box for the user to include a description.
  - Enabled: Check box to enable/disable the file transfer.

Figure 12 - TCP RED configuration via Web App GUI



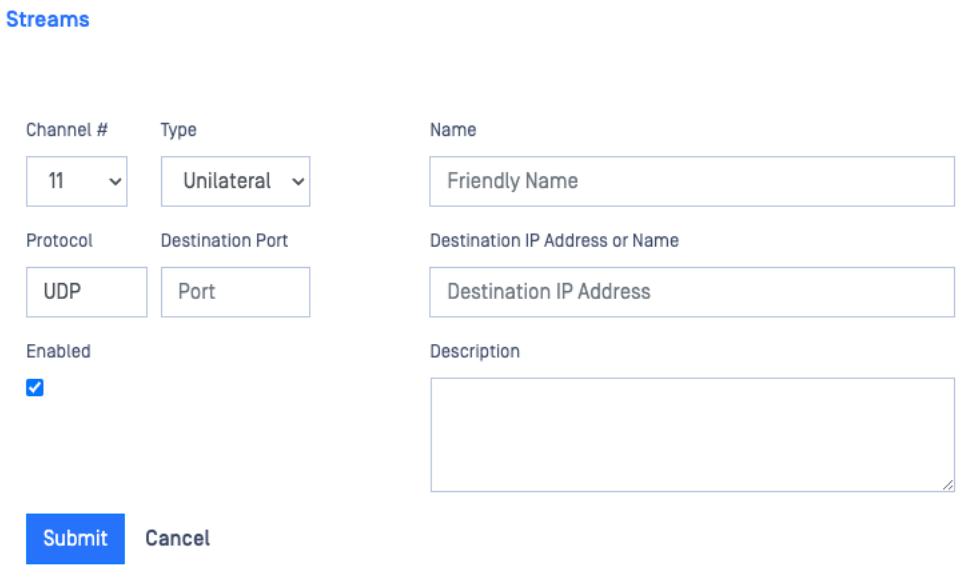
- UDP BLUE:
  - Channel #: indicated the channel where the UDP streaming is performed, needs to be the same in BLUE and RED sides.
  - Type: Predefined to Unilateral.
  - Protocol: Predefined to UDP for UDP streaming.
  - Port: Port for the UDP source in BLUE side.
  - Name: Friendly name to identify the stream.
  - Source Addresses or Ranges (separated by semicolon): Source addresses or range of addresses where the UDP stream is originated.
  - Description: Free text box for the user to include a description.
  - Enabled: Check box to enable/disable the file transfer.

Figure 13 - UDP BLUE configuration via Web App GUI



- UDP RED:
  - Channel #: indicated the channel where the UDP streaming is performed, needs to be the same in BLUE and RED sides.
  - Type: Predefined to Unilateral for NetWall USG.
  - Protocol: Predefined to UDP for UDP streaming.
  - Destination Port: Port for the UDP destination in RED side.
  - Name: Friendly name to identify the stream.
  - Destination IP Addresses or Name: Destination addresses or range of addresses where the UDP stream is finished.
  - Description: Free text box for the user to include a description.
  - Enabled: Check box to enable/disable the file transfer.

Figure 14 - UDP RED configuration via Web App GUI



3.5.1 Configuration parameters

3.5.1.1 BLUE side (TX Module)

The following configuration values determine which traffic is allowed from the BLUE network. It does not determine how the traffic is sent to the RX Module.

Table 3 – BLUE side parameters

Web UI TCP/UDP BLUE(AGD 3.5)	Database (DiodeSend)	Description
Channel #	channelnumber INTEGER	Unique Identifier between Blue/Red to correlate streams
Port	Port INTEGER	Single Port to listen for data
Protocol	is_tcp INTEGER	0 = udp 1 = tcp
Max Sessions	max_Sessions INTEGER	Max allowed concurrent connections
Enabled	active INTEGER	0 = off. 1 = on. Enable/disable flag

3.5.1.2 RED side (RX Module)

The configuration values determine where traffic is forwarded to on the RED network. It does not determine how the traffic is received from the TX Module.

Table 4 - RED side parameters

Web UI TCP/UDP RED (AGD 3.5)	Database (DiodeReceive)	Description
Channel #	channelnumber INTEGER	Unique Identifier between Blue/Red to correlate streams
Destination IP Address or Name	ipaddress TEXT	Destination IP
Destination port	port INTEGER	Single Port to send data to (destination port)
Protocol	is_tcp INTEGER	0 = udp

		1 = tcp
max Sessions	max_Sessions INTEGER	Max allowed concurrent connections
Enabled	active INTEGER	0 = off. 1 = on. Enable/disable flag

3.6 Port Scan Detect

The Port Scan Detect feature protects against malicious port scan detection attacks. IP addresses that conduct overt scans (FIN/XMAS/NULL scans) are blocked immediately. Malicious activity can be configured for obscure scans. These can consist of a source IP scanning anomalous number of ports or the scanning of one specific port an irregular number of times. Users can manually block IP addresses by adding them to a blacklist or unblock them by adding them to a whitelist. IPs that have been blocked past a specific amount of time can be unblocked via a clean-up process.

The steps of the configuration can be found in chapter Port Scan Detect of [P-UM], but the product is delivered with this function turned on by default.

4 Bibliography

[CC_P1] Common Criteria, Part 1: Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, Version 3.1, Revision 5, April 2017, CCMB-2017-04-001

[CC_P2] Common Criteria, Part 2: Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 5, April 2017, CCMB-2017-04-002

[CC_P3] Common Criteria, Part 3: Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components, Version 3.1, Revision 5, April 2017, CCMB-2017-04-003

[CEM] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, Revision 5, April 2017, CCMB-2017-04-004

[USG-UM] OPSWAT NetWall Unidirectional Security Gateway USG-100 Common Criteria Evaluated Configuration Guide v1.1, 2023-12-15

[P-UM] NetWall v5.5.0 (NetWall – v5.5.0.pdf)

[ALC] OPSWAT NetWall Unidirectional Security Gateway ALC documentation v1.2, version: v1.2, date: 2024-04-18

