Safe share

Application, installation and technical guide for General Service Slice v1.0

1. Introduction

This document is provided to the Network and Security technical teams at the Customer Client organisation to assist with the steps required to setup and implement a new Customer Client on the Safe share service.

The Safe share service is an overlay security service to facilitate Customer Clients to access or transfer data securely across the Janet network, or other network, between partners. The service utilises multiple layers of security using Juniper Networks SRX devices. To protect the transmitted data, a PKI (Public Key Infrastructure) has been design to create secure IPSec tunnels from the managed access router based on the member's site to the Secure Core network situated in the Jisc secure data centre.

The document describes the Safe share implementation steps for Customer Clients following an agreement for connection. This will include pre-staging, security assignment, installation, testing and commissioning.

The Customer Client that uses the Safe share service will be required to provide a suitable, secure location for the installation of the Access Router (Juniper Networks SRX) in order to access the General Service slice.

In order for us to configure the equipment described in this document to enable you to connect to the General Service slice we will require you to complete the accompanying questionnaire and send the completed Word document back to Jisc Operations for processing.

NB. You may require the assistance of your local technical team in filling out certain aspects of the questionnaire.

2. High Level Implementation Process

The following process highlights the steps and dependencies required to complete the implementation process to connect a customer client to the Safe share service. Customer Client actions are in Blue, Jisc actions in Orange.

Stage	Step	Description	Dependency	Time Allowance
Application to join the Safe share service	**Customer Requirements**	Complete the requirements form in this document to ensure the correct service is implemented applicable to the member	N/A	N/A
	Application check and confirmation	Jisc will perform legal entity checks, service slice eligibility and technical information requirements	All information is correctly filled out	1 week
	Agreement signature and installation date selection	Complete and sign the service agreement document and provide preferred installation dates	Application check and confirmations passing	1 week (during the 6 week initial configuration)
	Confirmation of installation date	Jisc will contact the applicant to confirm the choice of installation date	Chosen date/s being available	1 week (during the 6 week initial configuration)
Pre-installation	**Pre-Stage**	Pre-Configure Member Access Router (Junos) with: • A Pre-Shared Key Management IPSec VPN that connects back to the Core Nodes • Customer / Client allocated IP addresses • Dynamic routing configuration (BGP/OSPF) • Default Safe share system/management. configuration • Security Stanza Configuration	Customer Client Information Required IPAM	6 weeks from the application checks and confirmations being passed
	Arrange and conduct survey if required	If the Jisc engineers determine a survey is required we will arrange a suitable date with you	N/A	During the 6 week initial configuration
	Reminder	1 week before the confirmed installation date Jisc will contact you to remind you	Installation date selection	N/A

Stage	Step	Description	Dependency	Time Allowance
Installation	**Physical location/s**	Customer to escort installation engineer to location	Access to locations	1 day
	Initial Connectivity Validation	Validate the successful connection of the management IPSec VPN Liaise with the Member for any collaborated troubleshooting	Pre-Stage	
	Management Integration	Integrate the new Member Access Router into Junos Space for centralised management	Initial Connectivity Validation	
	Certificate Setup	Generate two CSRs (Certificate Signing Request) on the Member Access Router	Access to Member Access router configuration	
	Certificate Signing	Sign both CSRs per CPE with the applicable Subordinate/Intermediate CA with CA Server on SVC-A.	CA-Server	
	Certificate Implementation on SAR	Install the new signed certificates on the Member Access Router	Access to Member Access router configuration	
	Production VPN Setup	Install the Member Access Router Junos configuration to support the new x.509 Certificate-Based Production IPSec VPNs for connectivity		
	Production IPSec VPN Connectivity Validation	Confirm Certificate-Based IPSec VPN production connectivity from the Core Nodes to the Member Access Router. The production service is up after this stage but not officially online or live	Access to the Safe share Management Network and Configurations	
	Testing	• ORT (Operational Readiness Testing) to confirm all elements of the connectivity is working correctly	Management Connectivity	
		• UAT (User Acceptance Testing) in collaboration with the Member (UAT) for any Member bespoke testing as well as general traffic flow testing	Specific Test Plan of the Member	
	Go Live	Service confirmed as working	Successful testing	
	Follow up	Jisc will contact the applicant to follow up installation	Successful installation	1 week after installation

Stage	Step	Description	Dependency	Time Allowance
Post Installation	**Invoicing**	Initial invoice raised and sent to applicant	Successful installation	Within 30 days of installation
BAU	**Support**	Ongoing support as per agreement including space and Infrastructure management	N/A	N/A
	Recurrent invoicing	Annually on 1st August		

3. Technical information

The information in this section is intended to help your technical team choose a suitable physical location for your Safe share equipment and to assist with any support issues in the future.

4.1 Supplied Safe share Equipment

One or more pieces of following equipment (depending on your requirements) will need to be housed in a suitable environment with appropriate security.
It must be connected to your Internet connection and your LAN.

- High Bandwidth and High Port Density requirements – Juniper SRX 550, Juniper SRX 210 & Opengear ACM5022-FE (all three units must be housed together)
- Low Bandwidth and Low Port Density requirements – Juniper SRX 210 only

4.2 Safe share Equipment Environmental Requirements

	Juniper SRX 550	Juniper SRX 210	Opengear ACM5002-FE
Device Type	Security Appliance	Security Appliance	Access Appliance
Height (Rack Units):	2U	1U	Less than 1U/Shelf preferred
Width:	44.4 cm	28.2 cm	10.2 cm
Depth:	46.2 cm	18 cm	8.8 cm
Height:	8.8 cm	4.4 cm	2.8 cm
Weight:	9.96 kg	3.2 kg	0.34 kg
Power Device:	Internal power supply	Internal power supply	Internal power supply
Installed:	Qty2 (incl. 1 redundant)	Qty1	Integrated
Voltage Required:	AC 100/240 V (50/60 Hz)	AC 100/240 V (50/60 Hz)	AC 100/240 V (50/60 Hz)
Power Provided:	60 Watt	645 Watt	12V DC Power Adapter

The SRX access routers can be connected to existing power connectivity using either the standard type G UK "three pin" plugs/sockets or can be adapted to fit into power strips utilising C13 appliance couplers.

However, the Open gear terminal server only supports a standard UK plug and therefore will need a standard UK "three pin" socket to power the device.

4.3 SRX550 Services Gateway Front Panel

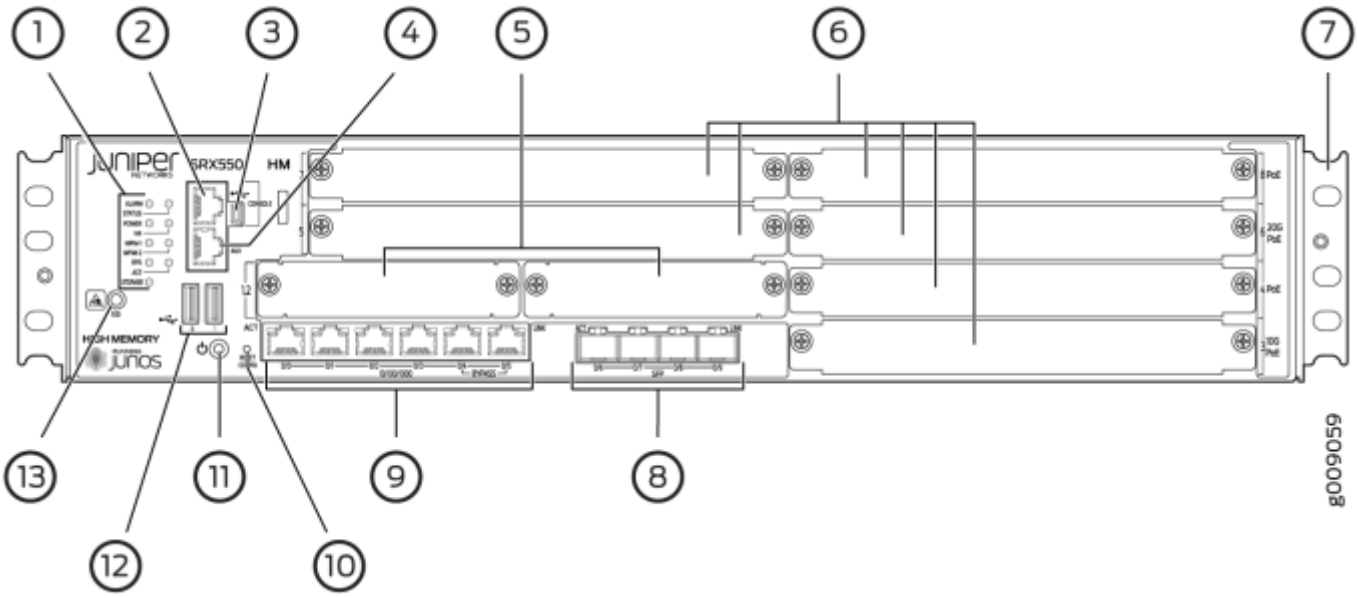

Figure 1 - Juniper Networks SRX550 Front Panel

Number	Component
1	Front panel LEDs
2	Serial Console Port
3	USB Console Port
4	Aux Port
5	2 x Mini-PIM slots numbered 1 and 2
6	6 x GPIM slots numbered 3 through 8
7	Mounting brackets
8	4 x SFP Ethernet ports (port 0/6-0/9)
9	6 x Fixed/Integrated Gigabit Ethernet ports (port 0/0 – 0/5)
10	RESET CONFIG Button
11	Power button
12	USB 0 and USB 1
13	ESD Outlet

4.4 SRX550 Services Gateway Back Panel

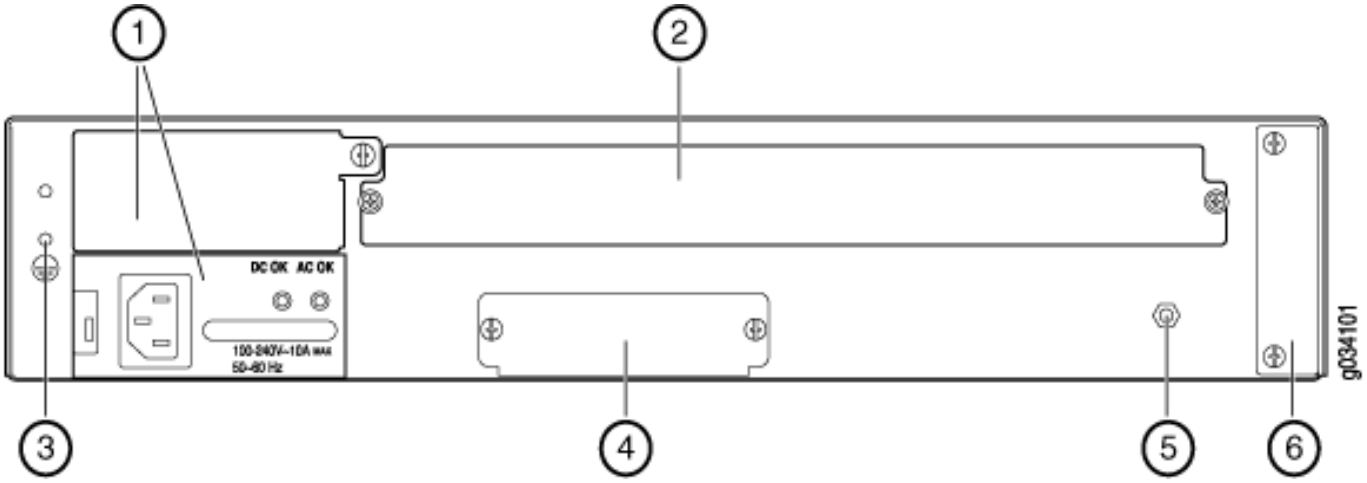

Figure 2 - SRX550 Rear Panel

Number	Component
1	Two power supply slots
2	ACE slot
3	Grounding point
4	Storage slot
5	ESD Outlet
6	Air filter cover

4.5 SRX210 Services Gateway Front Panel

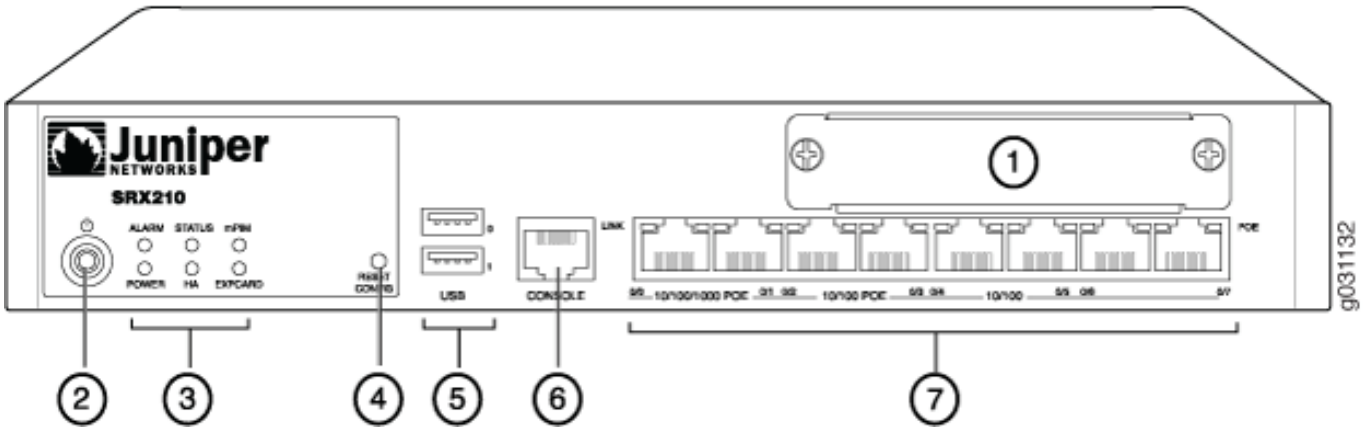

Figure 3 - Juniper Networks SRX210 Front Panel

Number	Component
1	Mini-PIM slot
2	Power button
3	LEDs: Status, Alarm, Power, 3G ExpressCard, Mini-PIM, HA
4	Reset Config button
5	Universal Serial Bus (USB) ports
6	Console port
7	Gigabit Ethernet ports and Fast Ethernet ports

4.6 SRX210 Services Gateway Back Panel

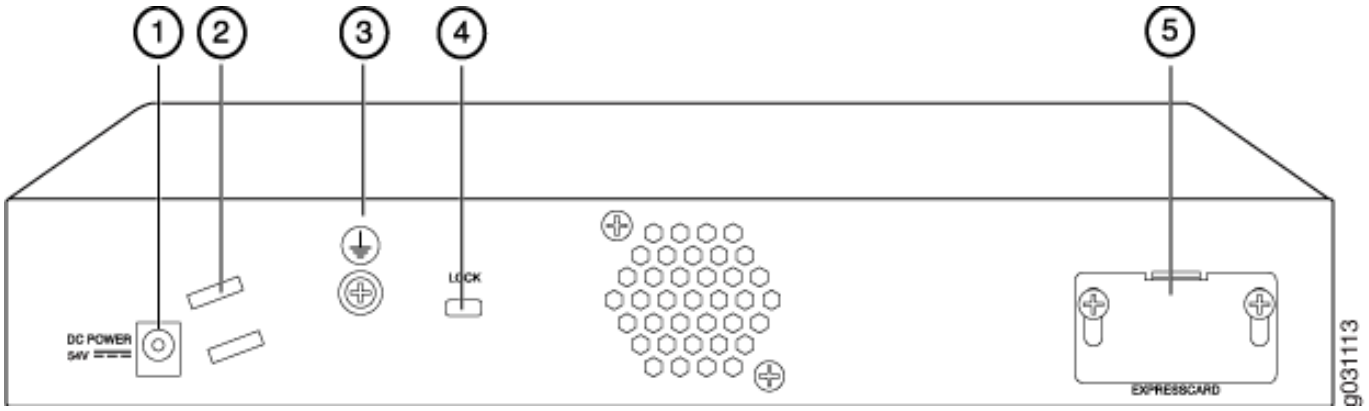

Figure 4 - Juniper Networks SRX210 Back Panel

Number	Component
1	Power supply point
2	Cable tie holder
3	Grounding point
4	Lock
5	ExpressCard slot

3.2 Opengear ACM5002-FE Front Panel

Figure 1 - Opengear ACM5002-FE Terminal Server

2 x RS-232 RJ45 serial (Cisco Straight pinout), single external power supply, 1 x 10/100 Ethernet, 1 x USB 2.0 ports, 4GB internal flash storage, 4 x TTL DIO terminals.

4. Connection Guide

4.7 High Bandwidth Connection Guide

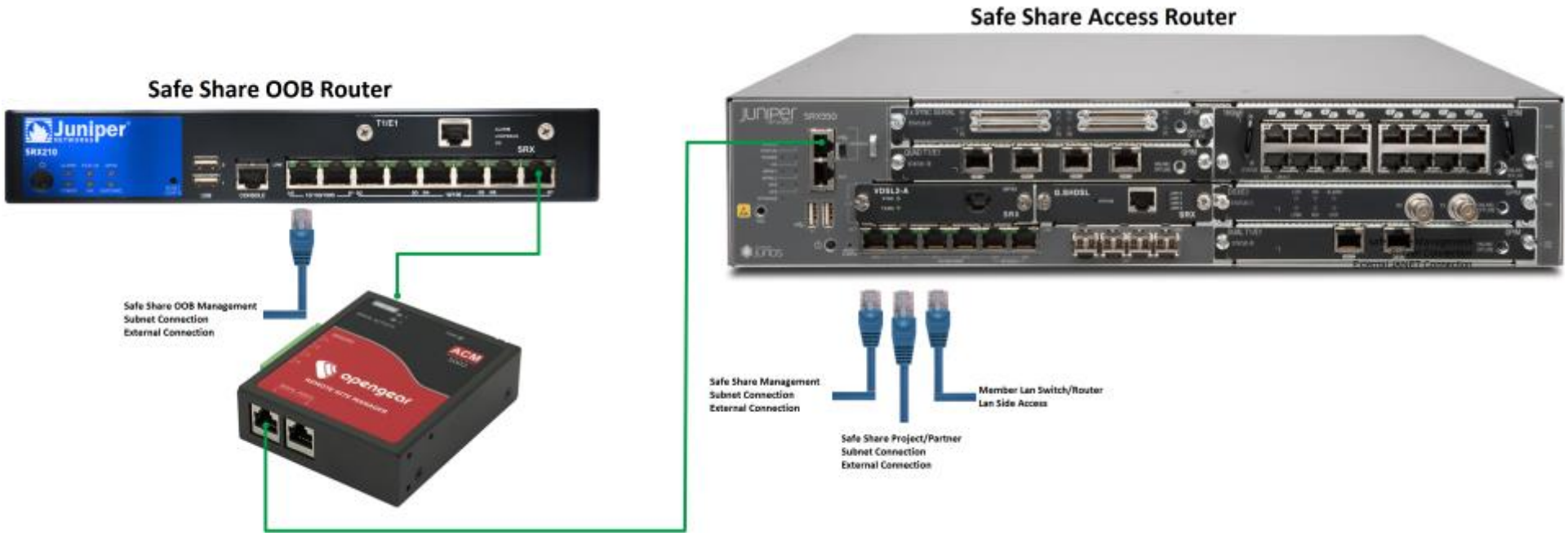

Figure 6 – High Bandwidth Access Router Connectivity Requirements

4.8 OOB Connections

The High bandwidth access router will be connected to a remote terminal service device that will be connected to the OOB router (SRX210).

The following connections as displayed in Figure 6 above are required for this connection:

- An Ethernet cable from port fe-0/0/7 on the Safe share OOB router (SRX210) to the Ethernet "LAN' port on the Opengear device.
- An Ethernet cable from the "Serial 1" port on the Opengear device to the "Console" port on the SRX550.
- An access connection from the Juniper SRX 210.

NB. External Connection may be Janet or another internet connection

4.9 Low Bandwidth Connection Guide

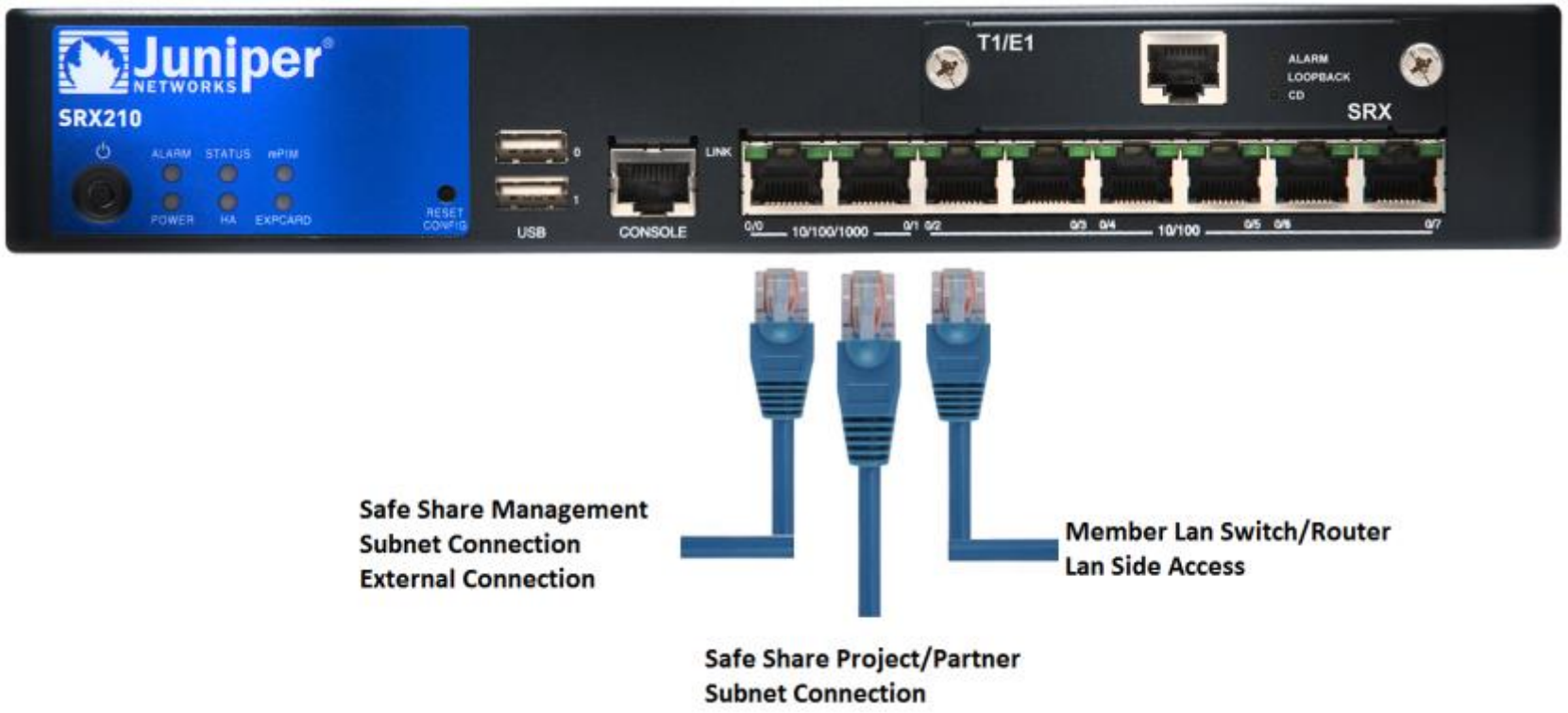

Figure 7 – High Bandwidth Access Router Connectivity Requirements

Please Note: This is a library image, therefore T1/E1 Mini-PIM module shown above will not be present in your router.

NB. External Connection may be Janet or another internet connection