বিআরপিডি-২ সার্কুলার নং-০১

তারিখ : ১৫ চৈত্র ১৪৩২ / ২৯ মার্চ ২০২৬

ব্যবস্থাপনা পরিচালক/প্রধান নির্বাহী কর্মকর্তা
বাংলাদেশে কার্যরত সকল তফসিলি ব্যাংক/ফাইন্যান্স কোম্পানি/মোবাইল ফাইন্যান্সিয়াল সার্ভিস প্রোভাইডার/
পেমেন্ট সার্ভিস প্রোভাইডার/পেমেন্ট সিস্টেম অপারেটর এবং অন্যান্য আর্থিক সেবা প্রদানকারী প্রতিষ্ঠান।

প্রিয় মহোদয়,

Guidelines on Partner Network, Version 1.0 (2026)

ব্যাংক ও অন্যান্য আর্থিক সেবা প্রদানকারী প্রতিষ্ঠানের জন্য ক্লিয়ারিং ও সেটেলমেন্টসহ বিভিন্ন সেবা প্রদান ও লেনদেন সংক্রান্ত কার্যক্রমের অংশ হিসেবে বাংলাদেশ ব্যাংক তার নিকট হতে লাইসেন্স প্রাপ্ত বিভিন্ন প্রতিষ্ঠান, যেমন তফসিলি ব্যাংক, ফাইন্যান্স কোম্পানি (অ-ব্যাংক আর্থিক প্রতিষ্ঠান), মোবাইল ফাইন্যান্সিয়াল সার্ভিস প্রোভাইডার, পেমেন্ট সার্ভিস প্রোভাইডার, পেমেন্ট সিস্টেম অপারেটরসহ অন্যান্য আর্থিক সেবা প্রদানকারী প্রতিষ্ঠানের সাথে ইলেক্ট্রনিক নেটওয়ার্কের মাধ্যমে সংযুক্ত থাকে। এছাড়া, সরকারের বিভিন্ন বিভাগ বা সংস্থার সঙ্গে সংযুক্ত থেকে বাংলাদেশ ব্যাংক নাগরিকদের জন্য আইটি-এনাবেল্ড বিভিন্ন সেবা পরিচালনা করে। বাংলাদেশ ব্যাংক ও অন্যান্য প্রতিষ্ঠানের মধ্যে তথ্য আদান-প্রদান একটি এক্সট্রানেট নেটওয়ার্ক বা 'পার্টনার নেটওয়ার্ক' এর মাধ্যমে সম্পন্ন হয়। প্রযুক্তিগত অগ্রগতি ও আর্থিক পরিবেশের বিবর্তনের এই যুগে কার্যকর ও নিরাপদ ডিজিটাল যোগাযোগের গুরুত্ব অনস্বীকার্য।

২। এক্ষণে, বাংলাদেশ ব্যাংক এবং অন্যান্য প্রতিষ্ঠানের মধ্যে নিরবচ্ছিন্ন যোগাযোগ, কার্যকর সিস্টেম পরিচালনা এবং নিরাপদ তথ্য বিনিময় নিশ্চিতকল্পে পার্টনার নেটওয়ার্ক সংক্রান্ত নীতিমালা "Guidelines on Partner Network, Version 1.0, 2026" জারি করা হলো।

৩। এ নীতিমালায় বর্ণিত নির্দেশনার সার্বিক পরিপালন নিশ্চিতকরণ সাপেক্ষে ব্যাংক/ফাইন্যান্স কোম্পানি/মোবাইল ফাইন্যান্সিয়াল সার্ভিস প্রোভাইডার/পেমেন্ট সার্ভিস প্রোভাইডার/পেমেন্ট সিস্টেম অপারেটর এবং বাংলাদেশ ব্যাংক কর্তৃক নিয়ন্ত্রিত/লাইসেন্সপ্রাপ্ত অন্যান্য আর্থিক সেবা প্রদানকারী প্রতিষ্ঠানসমূহ বাংলাদেশ ব্যাংকের বিভিন্ন সেবায় সংযুক্ত হতে পারবে।

৪। পার্টনার নেটওয়ার্ক সংশ্লিষ্ট যেকোন কার্যক্রমের ক্ষেত্রে এ নীতিমালা অনুসরণের জন্য আপনাদেরকে নির্দেশনা প্রদান করা হলো।

৫। আগামী ৩১ ডিসেম্বর ২০২৬ তারিখের মধ্যে এ নীতিমালার পরিপালন নিশ্চিত করতে হবে।

৬। 'ব্যাংক কোম্পানী আইন, ১৯৯১ (২০২৩ পর্যন্ত সংশোধিত)' এর ৪৫ ধারা, 'ফাইন্যান্স কোম্পানি আইন, ২০২৩' এর ৪১ (২) (ঘ) ধারা এবং 'পরিশোধ ও নিষ্পত্তি ব্যবস্থা আইন, ২০২৪' এর ১৮(৪) ধারায় অর্পিত ক্ষমতাবলে এ সার্কুলার জারি করা হলো।

আপনাদের বিশ্বস্ত,

(মোঃ আলা উদ্দিন)
পরিচালক (বিআরপিডি-২)
ফোন ঃ ৯৫৩০০৯৫

Guidelines
on
Partner Network

Version 1.0 (2026)

Bangladesh Bank

The page is intentionally left blank

Technical committee:

Chairman:

Debdulal Roy
Executive Director (ICT)
Bangladesh Bank

Members:

Pankaj Kumar Mallick
Director (ICT)
Bangladesh Bank

Jayanta Kumar Bhowmick
Additional Director (ICT)
Bangladesh Bank

Md. Abu Shoharab
Joint Director (ICT)
Bangladesh Bank

Md. Ashek Islam
Joint Director (ICT) and Member Secretary
Bangladesh Bank

Hafiz Al Asad
Assistant Chief Information Security Officer (JD)
Bangladesh Bank

Mahmuda Fardus
Joint Director
Bangladesh Bank

Hasan Mohammed Faisal
Joint Director (ICT)
Bangladesh Bank

F.M. Faijus Salehin Rifat
Deputy Director (ICT)
Bangladesh Bank

The page is intentionally left blank

Preface

Bangladesh Bank, a cornerstone of financial operations in Bangladesh, interfaces with different entities to enforce regulatory compliance and facilitate services for the organizations. Recognizing the indispensable role of secure digital channels, Bangladesh Bank introduces guidelines for partner networks. These directives aim to streamline extranet connectivity, facilitating seamless communication and data exchange with stakeholders. By adhering to this guideline, organizations are expected to contribute to the stability and growth of the nation's financial landscape. This preface sets the tone for collaborative engagement, emphasizing shared responsibility in navigating the complexities of modern financial systems.

The page is intentionally left blank

Table of Contents

The page is intentionally left blank

Chapter-1

1.1 Introduction

Bangladesh Bank facilitates financial services and transactions, including foreign exchange operations and clearing and settlement services for banks and financial institutions. As part of its functionalities, Bangladesh Bank is connected with different Organizations, such as Banks, Finance Companies, Mobile Financial Service Providers (MFSP), Payment Service Providers (PSP), Payment System Operators (PSO) etc. Bangladesh Bank is also connected with different Government stakeholders to provide various IT-enabled services for the citizens. This exchange of information between Bangladesh Bank and other organizations is performed over an extranet network, which is defined as a Partner Network.

In an era of technological evolution and financial landscape, the importance of efficient and secure digital communication is obvious. To meet the growing importance of digital communication and collaboration among the Organizations and stakeholders, Bangladesh Bank is introducing comprehensive guidelines for partner networks. This guideline aims to establish a framework for extranet connectivity, enabling seamless communication, smooth operation and secure data exchange between Bangladesh Bank and other Organizations/stakeholders. Through collaborative engagement and adherence to this guideline, Organizations/stakeholders can individually and collectively contribute to the stability and growth of the nation's financial system.

1.2 Scope

The Guidelines on Partner Network provide a framework of connectivity for an organization to access Bangladesh Bank resources. The provisions of this Guideline apply to:

1.2.1 Bank, Finance Company, MFSP, PSP, PSO, White Label ATMs and Merchant Acquirers (WLAMA) and other financial service providers regulated/licensed by Bangladesh Bank. All these institutions shall be termed as “The Organization” throughout this guideline.

1.2.2 The Organization shall assign a Team/Committee/Entity as the focal point to implement and monitor this extranet.

1.2.3 The regulatory authority can provide observations of any non-compliance issues found.

1.2.4 The Organizations shall be grouped into two categories. Category-A shall have to ensure both security and high availability, whereas Category-B shall have to implement security and, if possible, high availability.

1.2.5 The terms Extranet and Partner Network shall be used interchangeably in this document, which shall cover network service provider links, relevant network devices, workstations, etc.

1.3 Objectives

This Guideline defines the minimum control requirements to which each Organization must adhere. The primary objectives of the Guideline are as follows:

1.3.1 To ensure minimum security standards of the Organizations to connect with Bangladesh Bank.

1.3.2 To provide requirements and ensure the infrastructure standard for extranet connectivity between Bangladesh Bank and the Organizations.

Chapter-2

2.1 Segregation of Network

2.1.1 The network shall be segregated from the Organization's LAN, WAN and other related networks.

2.1.2 There shall be firewall segregation by service or zone.

2.1.3 The Organization shall monitor and analyze abnormal traffic flow among the segregated zones within the critical infrastructure.

2.2 Change Management

2.2.1 Any changes made to the extranet shall be controlled.

2.2.2 A formal documented process, including all necessary change details, shall govern all changes to network devices implemented in the production environment.

2.2.3 Audit trails shall be maintained for extranet devices.

2.2.4 The Organization shall prepare a rollback plan before executing any changes to address unexpected situations.

2.2.5 Proper testing for changes and upgrades in the extranet shall be carried out before deployment.

2.2.6 Post-deployment tests may be carried out.

2.3 Access Restrictions

2.3.1 The internet shall not be provided to the workstations, servers, etc., at the extranet service zone under any circumstances.

2.3.2 There shall be no irrelevant applications and services other than extranet services on the workstations.

2.3.3 Only authorized officials shall have access to the service area.

2.4 Remote Connection Management

2.4.1 The Organization shall take necessary security measures to prevent any unauthorized infiltration into the partner network.

2.4.2 For remote connection management, the Organization shall ensure:

2.4.2.1 Documentation covering details such as requirement date, probable scope, and place from where remote shall take place;

2.4.2.2 Availability, authentication technique, secure message transmission, and integrity of the message;

2.4.2.3 Implementation of encryption in all network connections;

2.4.2.4 Restriction of redundant information required for remote connection;

2.4.2.5 Restriction on remote privileged access from untrusted domain; and

2.4.2.6 Recording of the logs generated from the remote access.

Chapter-3

3.1 Partner Network Connectivity Requirements

The Organizations may be grouped into two primary categories:

3.1.1 Category-A Organizations must ensure security and high availability and maintain minimum redundancy of routers, firewalls and communication links with the Data Center. In the Disaster Recovery Site, the Organizations shall deploy redundant links, one router and one firewall or one device with both firewall and router capability with filtering from layer 4 to layer 7. This category is encouraged to have redundancy in all aspects. The sample diagram is attached in Annexure A.

3.1.2 Category-B Organizations must ensure security and shall have redundant communication links, one device with both firewall and router capability with filtering from layer 4 to layer 7 in the Data Center. But separate routing and firewalling devices are recommended. In the Disaster Recovery Site, the Organizations shall have one device with both firewall and router capability with filtering from layer 4 to layer 7 or one router and one firewall. The Organizations of this Category shall establish their Disaster Recovery Site with at least one network service provider but preferably two. The sample diagram is attached herewith as Annexure A.

3.1.3 Organizations in Category-B are encouraged to be upgraded to Category-A by fulfilling requirements with the acknowledgment of Bangladesh Bank.

3.2 Extranet Management

The Organizations shall adhere to the controls specified for extranet devices for network design, access, security and management.

3.2.1 Unauthorized access and electronic tampering shall be strictly prohibited. A mechanism shall be in place to encrypt and decrypt sensitive data traveling through the Extranet.

3.2.2 The Extranet design and its security configurations shall be implemented under a documented plan.

3.2.3 The Organization shall have different security zones defined in the network design.

3.2.4 The Organization shall deploy firewalls or similar measures within internal networks to minimize the impact of internal networks on extranet services.

3.2.5 The Organization shall monitor the logs generated by extranet devices.

3.2.6 Role-based or Time-based access controls shall be implemented in extranet devices.

3.2.7 The connection of any personal devices to the extranet, including those used for vendor support, is strictly prohibited.
3.2.8 All workstations/servers connected to partner networks via VPN shall use the latest anti-virus software through push updates or offline methods.
3.2.9 The Organization shall change all default passwords of extranet devices and update them regularly.
3.2.10 Incoming and outgoing traffic shall be filtered so that unwanted traffic is not circulated in the network.
3.2.11 Unused ports of network devices shall be disabled by default unless otherwise specified.
3.2.12 The Organization must keep a backup of all configurations of extranet devices periodically.
3.2.13 The network subnet provided by Bangladesh Bank is prohibited from being advertised to the organizations' LAN or WAN in any form, including NAT.

3.3 VPN management

3.3.1 Organizations shall establish connections to Bangladesh Bank via VPN, as outlined in the sample attached in Annexure B.
3.3.2 The connections must comply with the requirements of the Cryptographic Algorithms Standard.
3.3.3 VPN gateways shall be set up and managed by the Organization's network management team.

3.4 Vulnerability Assessment

3.4.1 An assessment shall be performed before implementing extranet-based services.
3.4.2 The Organization shall run vulnerability scans on its extranet-based systems and devices periodically.
3.4.3 A process shall be established to address and remediate any gaps identified in the vulnerability assessment.

3.5 Patch Management

3.5.1 Patch updates for extranet devices shall be performed regularly.
3.5.2 The Organization shall test security patches before deploying them into production.
3.5.3 The Organization shall document the patch management procedure. The document shall include the scope, roles and responsibilities, timeline, operational guidelines, and procedures. The scope should outline which systems are covered by the patching process.

Chapter-4

4.1Extranet Administration

4.1.1 Cryptographic keys and security phrases shall not be shared.

4.1.2 Hard copies of the design, rack view diagram, cable tagging, and other physical topology-related documents, as well as configuration backups of extranet devices, shall be preserved properly.

4.1.3 Baseline/standard device hardening shall be performed on servers, terminal workstations and other devices before commissioning.

4.1.4 The Organization shall nominate an extranet focal person with appropriate authority and a fallback person.

4.1.5 The focal person with fallback shall be skilled and trained enough. If not, training shall be arranged to avoid the unavailability of services and other security breaches.

4.1.6 The Organization shall follow the controls outlined in the 'Guideline on ICT Security' circulated by Bangladesh Bank for network monitoring and auditing, account management, password management, backup and restore management, and operation management for extranet devices.

4.2 Incident Reporting

The organization shall report to the Bangladesh Bank regarding service interruptions periodically, including:

4.2.1 Detailed description of interrupted services;

4.2.2 Critical infrastructure name, focal point name and contact details;

4.2.3 The nature of the incident, the time it occurred, its cause, and details about the event; and

4.2.4 The result and effect of the incident, and if any infrastructure was affected, the details of those infrastructures.

Chapter-5

5.1 Service level agreement

5.1.1 The Organization shall ensure that contractual terms and conditions governing all contracting parties' roles, relationships, obligations and responsibilities are fully set out in written agreements.

5.1.2 The Organization shall select redundant Network Service Providers (NSPs) from the approved list. NSPs should not be changed frequently; however, under special circumstances, an NSP may be changed with prior approval from Bangladesh Bank.

Annexure-A

Network Design and Architecture

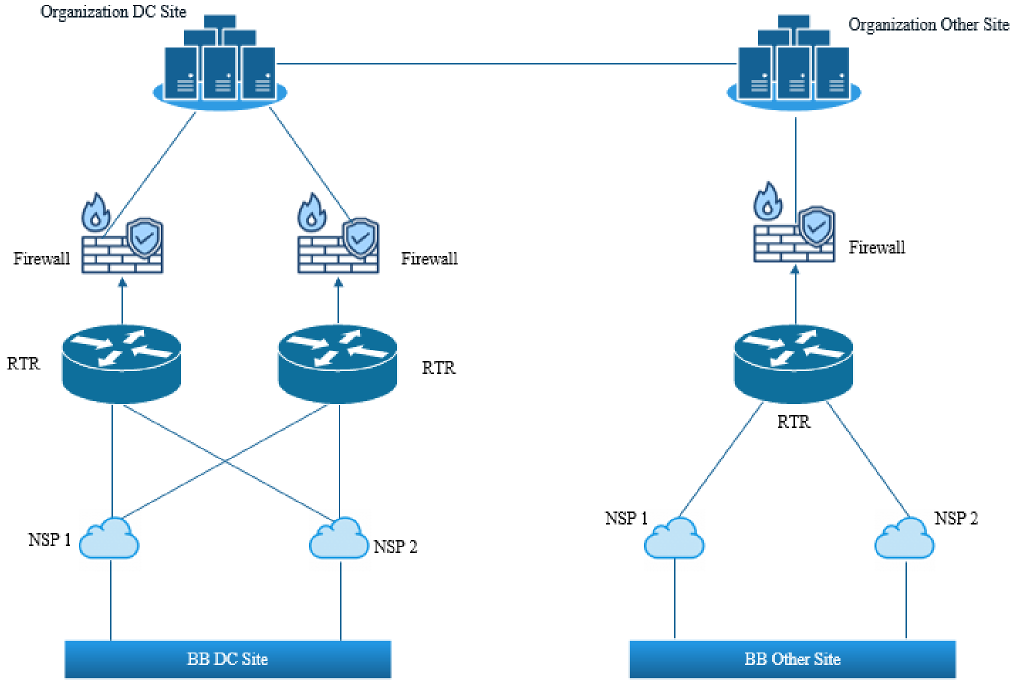

Figure 01: Ideal Connectivity diagram for Category A

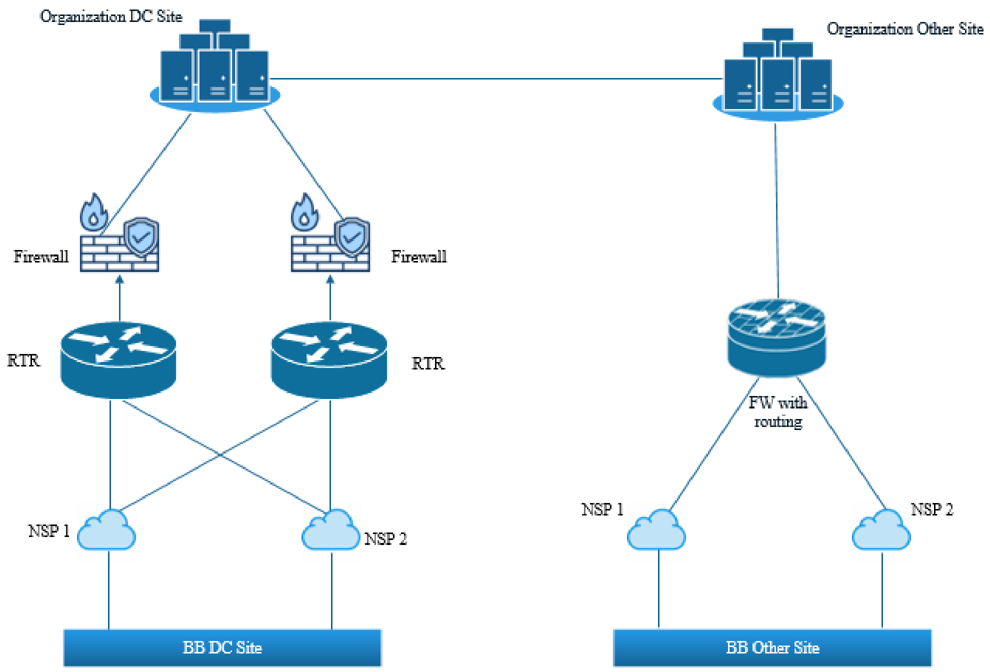

Figure 02: Basic Connectivity diagram for Category A

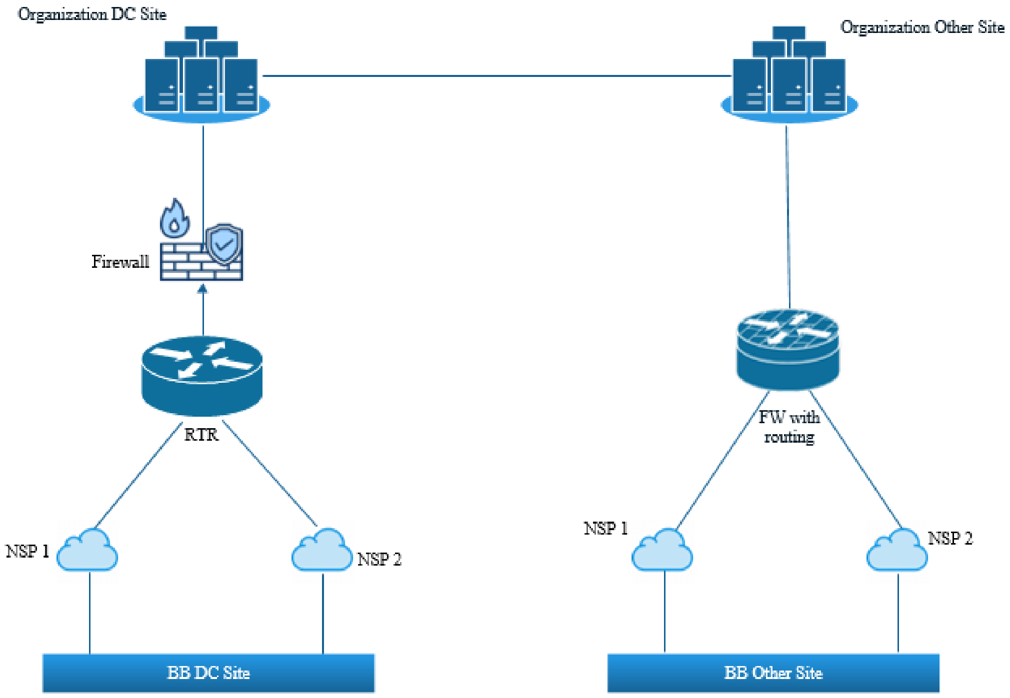

Figure 03: Ideal Connectivity diagram for Category B

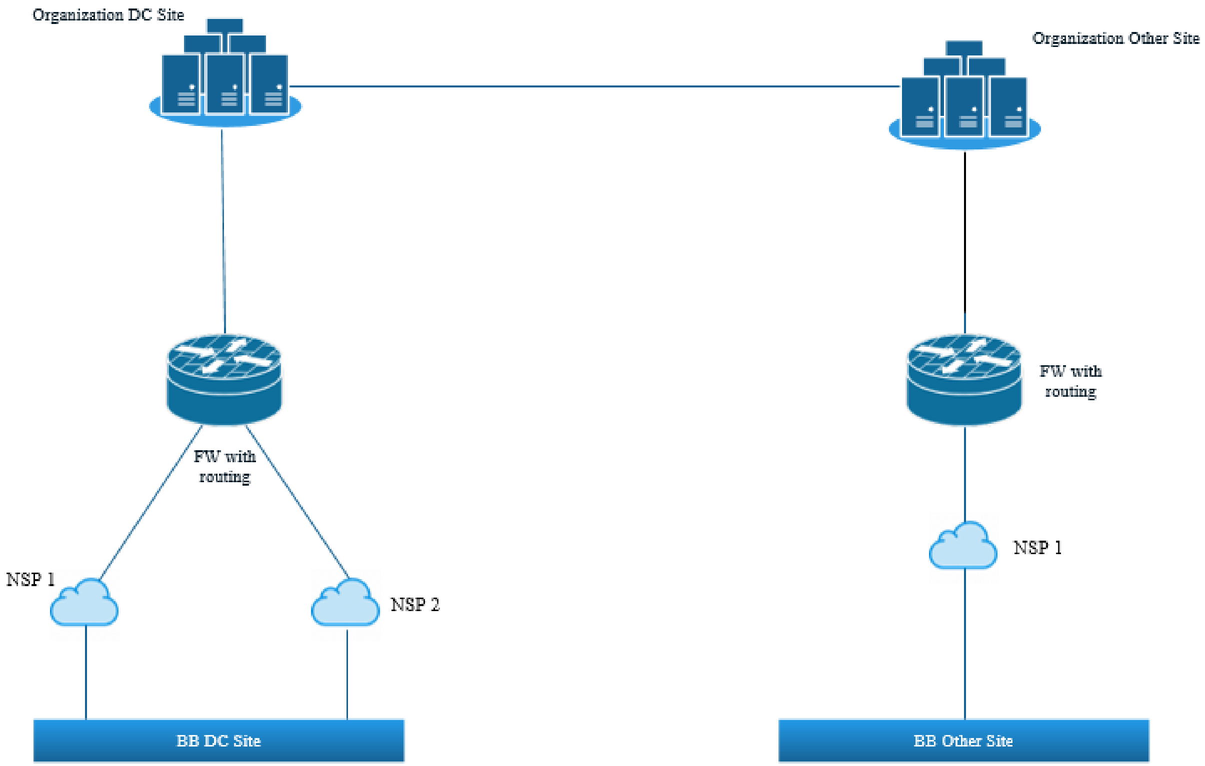

Figure 04: Basic Connectivity diagram for Category B

Annexure-B

VPN Worksheet*

VPN WORKSHEET: Bangladesh Bank			
Organization Name:			
Date Request:			
Date Start:			
Date Completed:			
Details/purpose of Connection			
Description	**BB**	**Partner**	**Comment**
Contacts:			
Details of Connection Owner/Requester:			
Name			
Designation/Department			
Email Address			
Phone			
Name (2nd Contact)			
Designation/Department			
Email Address			
Phone			
Name (3rd Contact)			
Designation/Department			
Email Address			
Phone			
Details of Network Service Provider			
Name (Primary NSP)			
Contact person Name			
Designation/Department			
Email Address			
Phone			
Name (Secondary NSP)			
Contact Person Name			
Designation/Department			
Email Address			
Phone			
Details of IT Officials:			
Name(1st Contact)			
Designation/Department			
Email Address			
Phone			
Name (2nd Contact)			
Designation/Department			
Email Address			
Phone			
VPN Gateway (VPN Gateway Configuration)			
VPN Gateway IP Address / WAN IP			**VLAN ID:**
Model/Brand			
VPN Device Location			
Service Type			
GRE Tunnel IP			
VPN Configuration			
Phase 1:			
Authentication Method			
Encryption Algorithm			
Hashing Algorithm			
Diffie-Hellman Group			
Lifetime (for renegotiation)			
Pre-Shared Key			
Phase 2:			
Encapsulation			
Encryption Algorithm			
Authentication Algorithm			
Perfect Forward Secrecy			
Tunnel Access Details:			
Local IP Block (Real IP/NAT IP if Required)			
Host IP with Port(Real IP/NAT IP if Required)			

*This format can be updated from time to time.