ECC Member Banks Network & Hardware Prerequisite Details

Version 1.1

June 2011

Content

1. Background

With reference to NRB Circular – Ref No C.H. ECC/95/067/68 dated 2068-01-27 and re-circular C.H. ECC/110/067/68 dated 2068-03-03 regarding ECC Member Banks Requirements (Participants HW Prerequisites) for their readiness, this document provides details of the network and other hardware.

2. Banks Network Requirements

2.1. Banks Network Devices

Each Bank should NAT its traffic when accessing NCHL network (Banks should be represented to NCHL via one IP address at each ISP) and the router/firewall should have the ability of establishing IPSec tunnels with support for certificate-based peer authentication during IPSec Phase 1.

A separate router/firewall should be configured outside the bank's network to be connected to the NCHL network.

Three cases for banks connectivity to NCHL are explained below.

Case1:- Bank is connected through two the different ISPs by two routers/firewalls:

Two routers/firewalls could be configured in Active/Standby failover mode. The active one should be connected to the Primary ISP and the standby one should be connected to the secondary ISPS. Each router/firewall can have one IP route to NCHL publishing areas according to the connected ISP.

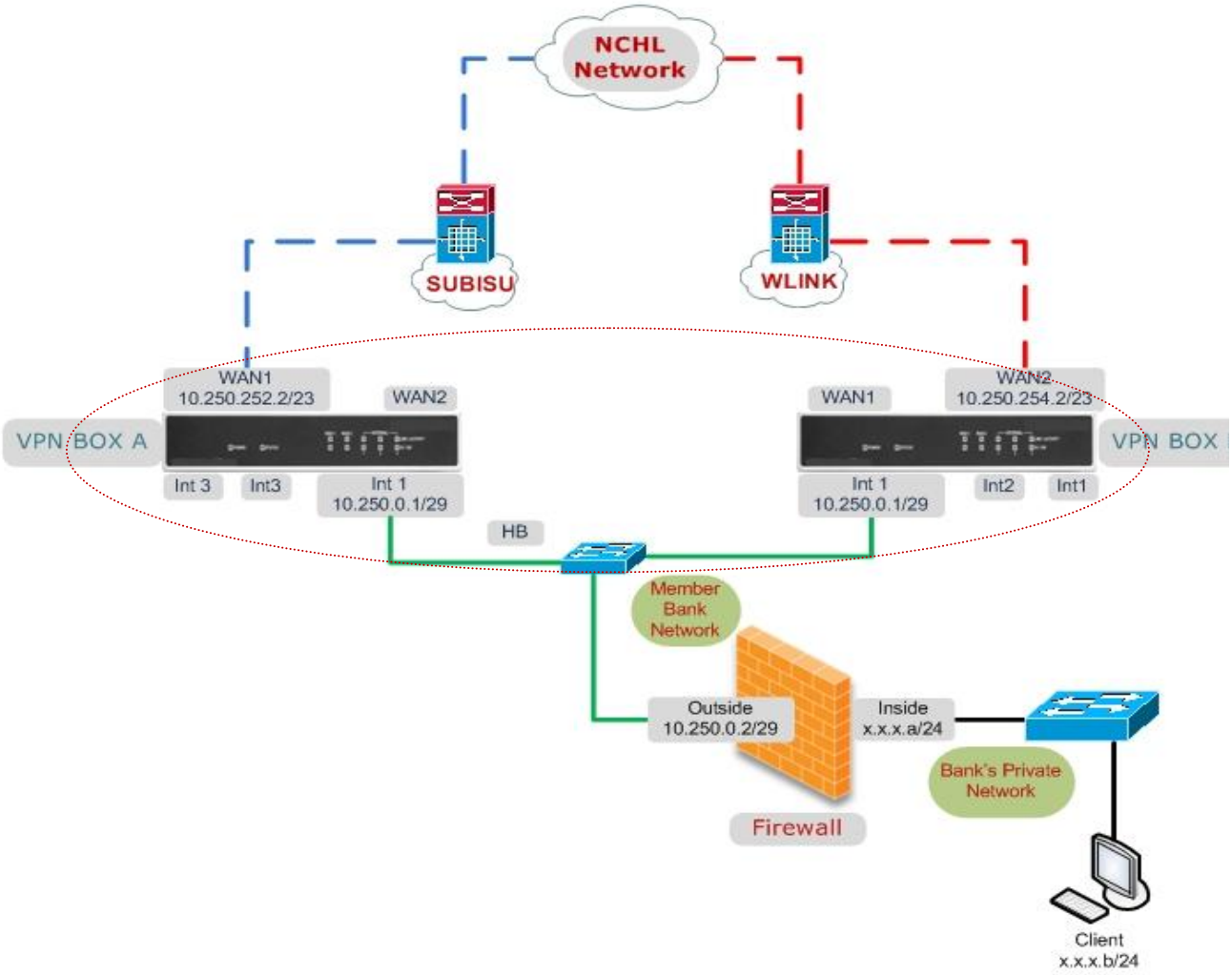

Figure 1: Case I

Symbol	Explanation	Ports
Subisu	Blue Cable	WAN 1 of VPN Box A
WLink	Red Cable	WAN 1 of VPN Box B
Heart Beat	Green Cable	INT 1 of Box A and B
Member Bank Network	Green Cable	INT 1 of VPN Box A and B
Bank's Private Network	Black Cable	

The IP addresses assigned to the three following interfaces must be on three different subnets:

- IP address assigned to WAN 1 of VPN box A must be on Subnet 1. (Example 10.250.252.2/23)
- IP address assigned to WAN 1 of VPN box B must be on Subnet 2. (Example 10.250.254.2/23)
- IP address assigned to Internal of VPN box A and B must be on Subnet 3. (Example 10.250.0.1/29)

Procedure

1. Connect VPN Box A and B and Client Firewall using Internal 1 (Green Cable in Figure 1)
2. Connect WAN 1 of VPN Box A with SUBISU (Blue Cable in Figure 1)
3. Connect WAN 1 of VPN Box B with WLINK (Red Cable in Figure 1)

Normal Packet Flow

1. The Bank's Private Network PC (x.x.x.b/24) of Client Site initiates the Packet.
2. The packet then reaches the Client Site Main Firewall (x.x.x.a/24).
    a. Here the source of Bank's Private Network PC is translated (NAT) from x.x.x.b/24 to 10.250.0.2/29
    b. NCHL Server Network recognizes 10.250.0.2/29 network.
3. The firewall analyze the packet and forwards the packet to INT1 port (10.250.0.1/29)of VPN Box A
    a. Packets are route to VPN Box A by default.
4. The packet will be analyzed in VPN Box A and will be routed to NCHL network through ISP1
    a. The packets travel securely to the NCHL Server Farm.
    b. Secure VPN Tunnel is created between NCHL FGT and VPN Box A in WAN1

Packet Flow when VPN Box A fails

1. The Bank's Private Network PC (x.x.x.b/24) of Client Site initiates the Packet.
2. The packet then reaches the Client Site Main Firewall (x.x.x.a/24).
    a. Here the source of Bank's Private Network PC is translated(NAT) from x.x.x.b/24 to 10.250.0.2/29
    b. NCHL Server Network recognizes 10.250.0.2/29 network.
3. The firewall analyze the packet and forwards the packet to INT1 port (10.250.0.1/29)of VPN Box B
    a. VPN Box A has failed
    b. The secondary route is assigned to VPN Box B
4. The packet will be analyzed in VPN Box B and will be routed to NCHL network through ISP2
    a. The packets travel securely to the NCHL Server Farm.
    b. Secure VPN Tunnel is created between NCHL FGT and VPN Box B in WAN2.

Case2:- Bank is connected through two the different ISPs by one router/firewall:

Two IP routes to NCHL publishing areas should be configured; the primary one (lowest metric route) goes through the Primary ISP and the second one goes through the Secondary ISP.

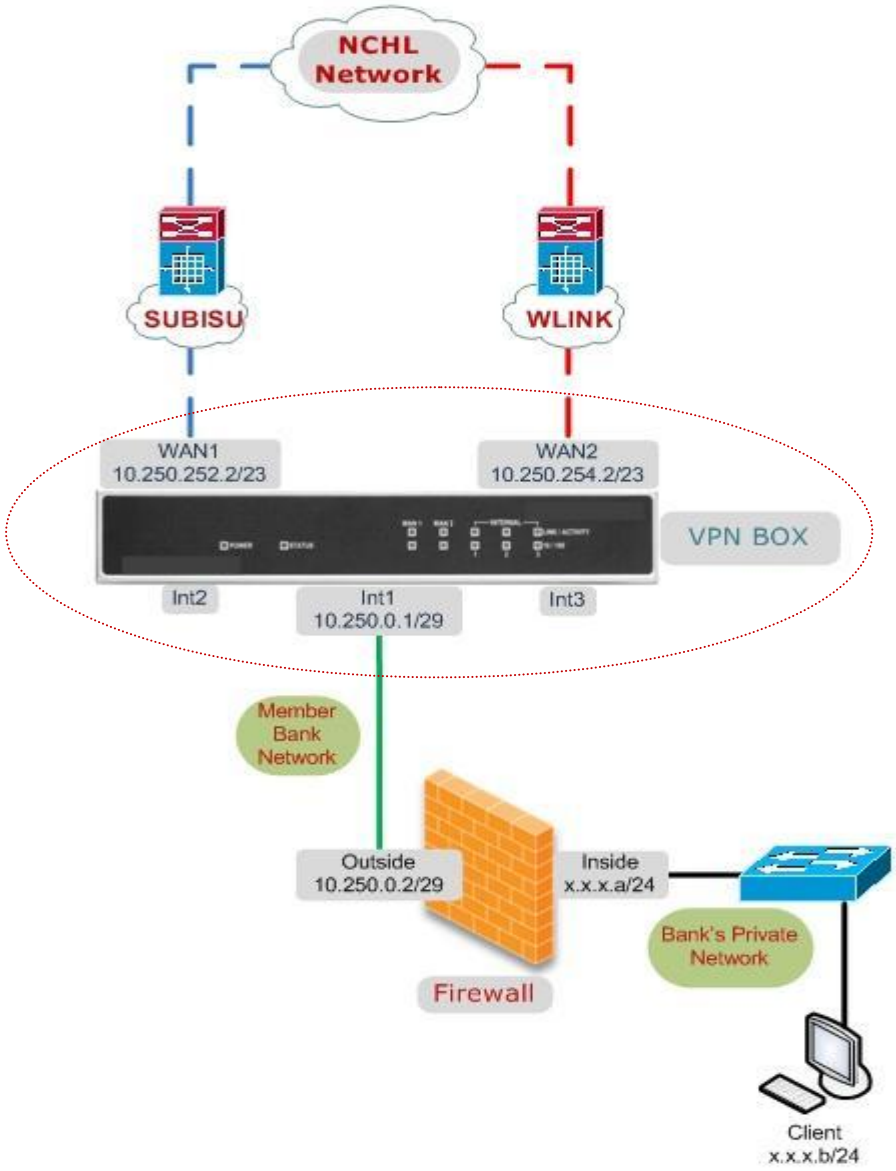

Figure 2: CaseII

Symbol	Explanation	Port
SUBISU	Blue Cable	WAN1
WLINK	Red Cable	WAN2
Member Bank Network	Green Cable	Internal
Bank's Private Network	Black Cable	

The IP addresses assigned to the three interfaces must be on three different subnets:

- IP address assigned to **WAN 1 of VPN box** must be on **Subnet 1**. (Proposed 10.250.252.2/23)
- IP address assigned to **WAN 2 of VPN box** must be on **Subnet 2**. (Proposed 10.250.254.2/23)
- IP address assigned to **Internal of VPN box A** must be on **Subnet 3**. (Proposed 10.250.0.1/29)

Procedure

1. Connect VPN Box and Client Firewall using Internal 1 (**Green Cable** in Figure 2)
2. Connect WAN 1 of VPN Box A with SUBISU (**Blue Cable** in Figure 2)
3. Connect WAN 1 of VPN Box B with WLINK (**Red Cable** in Figure 2)

Packet Flow

1. The Bank's Private Network PC (x.x.x.b/24) of Client Site initiates the Packet.
2. The packet then reaches the Client Site Main Firewall (x.x.x.a/24).
    a. Here the source of Bank's Private Network PC is translated(NAT) from x.x.x.b/24 to 10.250.0.2/29
    b. NCHL Server Network recognizes 10.250.0.2/29 network.
3. The firewall analyzes the packet and forwards the packet to internal port (10.250.0.1/29) VPN Box
4. The packet will be analyzed in VPN Box and will be routed to NCHL network through ISP1
    a. WAN 1 is made primary link to NCHL Network.
    b. Secure VPN Tunnel is created between NCHL Fortigate and VPN Box in WAN1
5. In case of failure of ISP1 the packet will be diverted to NCHL network through ISP2
    a. WAN 2 is the secondary link to NCHL Network.
    b. Secure VPN Tunnel is created between NCHL Fortigate and VPN Box in WAN2.

Case3:- Bank is connected through the Primary ISP by one router/firewall:

In this case; the router/firewall can have one IP route to NCHL publishing areas according to the Primary ISP.

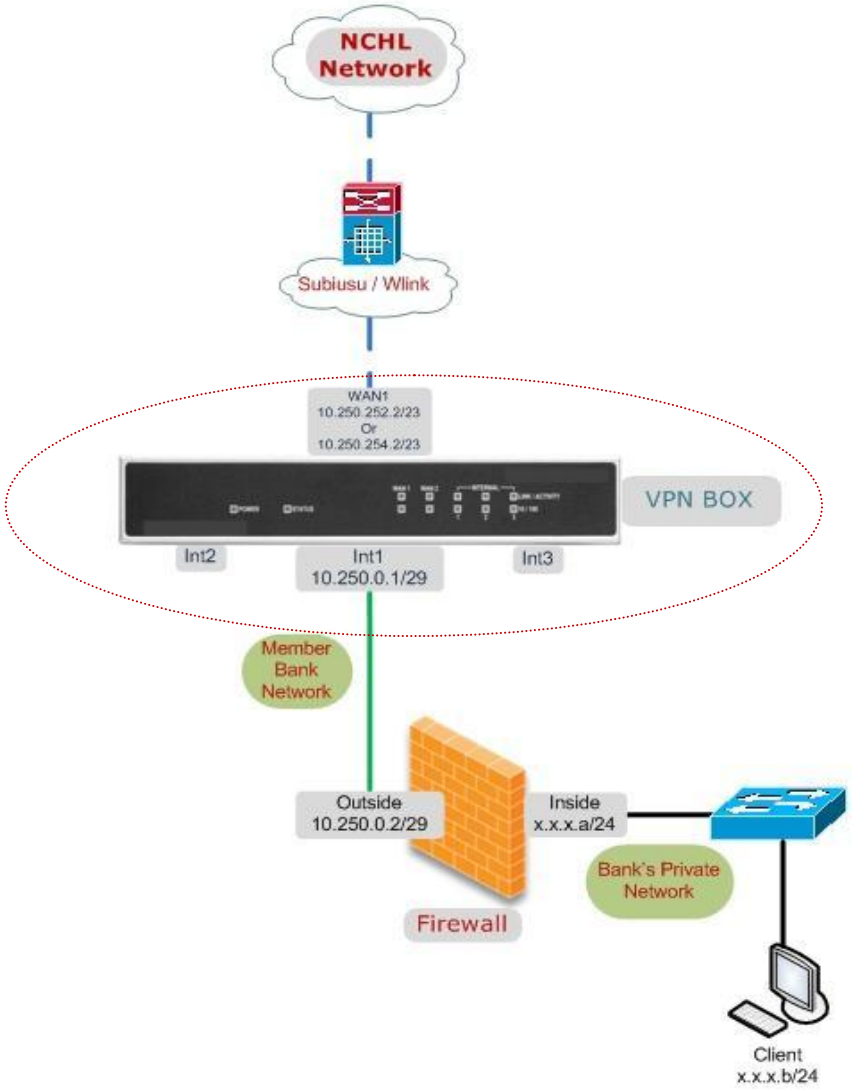

Figure 3: Case III

Symbol	Explanation	Port
SUBISU/ WLINK	Blue Cable	WAN1
Member Bank Network	Green Cable	Internal
Bank's Private Network	Black Cable	

The IP addresses assigned to the two following interfaces must be on two different subnets:

- IP address assigned to **WAN 1 of VPN box** must be on **Subnet 1**. (Proposed 10.250.252.2/23 or 10.250.254.2/23)
- IP address assigned to **Internal of VPN box A** must be on **Subnet 2**. (Example 10.250.0.1/29)

Procedure

1. Connect VPN Box and Client Firewall using Internal 1 (**Green Cable** in Figure 3)
2. Connect WAN 1 of VPN Box A with SUBISU (**Blue Cable** in Figure 3)

Packet Flow

1. The Bank's Private Network PC (x.x.x.b/24) of Client Site initiates the Packet.
2. The packet then reaches the Client Site Main Firewall (x.x.x.a/24).
   a. Here the source of Client' Private Network PC is translated(NAT) from x.x.x.b/24 to 10.250.0.2/29
   b. NCHL Server Network recognizes 10.250.0.2/29.
3. The firewall analyzes the packet and forwards the packet to internal port (10.250.0.1/29) VPN Box
4. The packet will be analyzed in VPN Box and will be routed to NCHL network through ISP1. Secure VPN Tunnel is created between NCHL Fortigate and VPN Box in WAN1

2.2. Recommended Cases

Member Type	Mandatory	Recommended
Commercial Bank	Case II	Case I
Development Bank	Case III	Case II
Finance Company	Case III	Case II

Member banks are required to reserve the IP ranges as proposed in the above cases. Individual IP for each member banks/ FI will be circulated at the time of creating VPN connections.
IPs to be reserved: 10.250.0.0/16

2.3. Minimum Specification of Router/ Firewall

1. Number of WAN Interfaces (Copper, RJ-45) : 2
2. Internal Switch Interfaces (Copper,RJ-45) : 3
3. Console (Copper, RJ-45): 1
4. IP SEC VPN (Gateway-Gateway, Client - Gateway)
5. Policy based NAT
6. Concurrent SSL VPN
7. 3DES/AES VPN
8. SSH, Telnet, SNMP and Web Based Management

3. Selected/ Recommended Devices/ Vendors

3.1. Selected Vendors for ISPs

	Vendor Name	Contact Person	Contact No
ISP 1	Subisu Cable Net	Mr. Dipak Shrestha Mr. Santosh Puri	9851088947 9802081381
ISP 2	World Link Communication	Mr. Laxman Yadav Mr. Samit Jana	9801011406 9851038795

*Member banks are required to select one or both amongst the above ISP vendors as per the Case selected. Member banks need to communicate their choice to NCHL after which NCHL will advice ISP for the connection.

3.2. Preferred Model/Vendor for router/ firewall device

	Model
Router/ Firewall	Fortigate 50B for Case II
	Or Fortigate 30B for Case III
	Or Equivalent as per Spec mentioned in2.3

*For other models, member banks are requested to consult with NCHL for detailed VPN configuration

3.3. Approved Scanner Models

S.No.	Model	Local Vendor	Contact Person	Contact No.
1	Epson TM-S1000	Mercantile Communication	Mr. Raj Prajapati	9851013336
2	Panini Vision X Series (SD, VX, AGP) Panini My Vision X 30, 60, 60X, 90 VX50.1.1F.NJ.B VX50.1.SF.NJ.B	Integrated Solution	Ms. Srijana Ghimire Mr. Kanchan Basnet	9813755595 9851026780
3	Seac Benche Zeta, Epsilon, Delta	Smart Tech Solution	Mr. Dibyesh Giri	9851118494

We are also working on adding other scanner brands and models and will be circulated as and when details are available.