IT STANDARD OPERATING PROCEDURE	**DBLGROUP** **IT DEPARTMENT** **South Avenue Tower (6th Floor), House-50, Road-3, Gulshan-1, Dhaka, Bangladesh**				
TITLE:	Firewall Configuration				
SOP No.	Issue Date	Effective Date	Review Due	Copy No.	Page **1** of **6**
1.0.6					

1.0.6 Firewall Configuration

1. PURPOSE

The objective of this SOP is to establish a standardized process for configuring and maintaining firewalls to ensure the security and integrity of the DBL GROUP network.

2. SCOPE

This SOP applies to all IT personnel responsible for configuring and managing firewalls within DBL GROUP.

3. ROLES AND RESPONSIBILITIES

The IT infrastructure lead and CIO are responsible for overseeing and approving firewall configurations.

The Information Security team is responsible for cross-checking the overall security baseline.

Network Administrators are responsible for implementing firewall configurations as per the approved guidelines.

4. Procedures:

1. **Assess Network Requirements:**
   Understand the network architecture, including the number of users, servers, and the types of services being used MZ, DMZ etc.

2. **Identify Firewall Placement:**
   Determine where the firewall will be placed in the network topology, typically between the internal network and the external network (Internet).

3. **Firewall Solution:**
   We have chosen state-of-the-art next-generation Fortinet firewalls (200F, 100F, and 80F) considering our business needs, along with WAN and Core Switches.

4. **Configure Basic Settings:**
   a. Verify the device's hardware conditions by turning it on.
   b. Updated latest recommended firewall versions.
   c. Ensured that all physical connections were established.

d. Established HA connection and test.
e. Assign IP addresses to firewall interfaces.
f. Configure basic network settings such as gateway and DNS servers.

5. **Define Access Control Policies:**
   a. Create rules to allow or deny traffic based on source IP, destination IP, port, protocol, and application.
   b. Define firewall policies for inbound and outbound traffic separately.
   c. Prioritize rules based on security requirements and traffic patterns.
6. **Implement Network Address Translation (NAT):**
   a. Configure NAT to translate internal private IP addresses to external public IP addresses for outbound traffic.
   b. Define port forwarding rules for inbound traffic destined for internal servers.
   c. Configure Real IP Mapping to access the local server by defining a specific port.
   d. Set up specific firewall policies for traffic that comes from outside network to one-prem servers.
7. **Enable Intrusion Prevention System (IPS):**
   a. Enable IPS features to monitor and block suspicious network activity.
   b. Configure signatures and rulesets to match the organization's security policies.
8. **Set Up Virtual Private Network (VPN) Access:**
   a. Configure VPN tunnels for remote access or site-to-site connectivity.
   b. Implement authentication and encryption protocols to secure VPN connections.
   c. Configure IPsec and GRE Tunnels to integrate with branch office networks.
9. **Enable Logging and Monitoring:**
   a. Configure logging settings to record firewall events and traffic logs through Fortinet analyzer.
   b. Set up alerts for critical events such as intrusion attempts or policy violations or compromised hosts.
10. **Regular Maintenance and Updates:**
    a. Schedule regular maintenance tasks such as software updates, firmware upgrades, and security patches.
    b. Review firewall rules periodically to ensure they align with the organization's security policies.
    c. Test firewall configurations to verify they are functioning as expected.
11. **Document Configuration Changes:**

a. Maintain detailed documentation of firewall configurations, including rule changes, firmware upgrades, and security patches.

b. Document any exceptions or special configurations for auditing purposes.

12. **Backup Configuration:**

a. Regularly backup firewall configurations to prevent data loss in case of hardware failure or configuration errors.

13. **Testing:**

a. Conduct thorough testing of the firewall configuration to ensure it effectively filters traffic and meets security requirements without impacting network performance.

14. **Change Management:**

a. All changes to firewall configurations must go through a formal change management process, including cross checking from the IT Security Team.

DOCUMENTATION AND RECORD-KEEPING

a. Keep a record of all configuration details documented.

b. Any change or modification should also be documented.

ABBREVIATIONS

SOP - Standard Operating Procedure
IT - Information Technology
HA - High Availability

PRECAUTIONS

1. **COMPLIANCE AND SECURITY**

a. In terms of existing firewall configuration should keep backup before any operations for safety

b. Access to sensitive information will be strictly controlled and monitored.

c. Any security incidents or breaches will be reported and handled according to established protocols.

2. **INCIDENT RESPONSE**

a. Notify affected parties promptly and take corrective actions.

b. Develop an emergency response plan to handle firewall failures or security breaches, including procedures for isolating affected systems and restoring services. (See SOP- 1.0.6 Incident Response)

3. TRAINING AND CONTINIOUS IMPROVMENT

a. Provide regular training to network administrators and security personnel on managing and troubleshooting the firewall configuration.
b. Train SOP stakeholders regularly for any upgradation of SOP's.

REVIEW AND REVISION

a. This SOP will be reviewed annually or as needed to ensure relevance and effectiveness.

b. Any updates or revisions will be communicated to all relevant stakeholders.

COMMUNICATION:

Clearly communicate the SOP to all relevant stakeholders. Ensure that employees are aware of their roles and responsibilities and understand the implications of not adhering to them.

ACCESSIBILITY:

Make the SOP easily accessible to all relevant personnel. This could involve storing it in a central repository, such as an intranet or document management system.

ASSOCIATED DOCUMENTS

Firewall security policy will be created by Information Security Team

REFERENCES

a. FDA's 21 CFR Part 11: Electronic Records; Electronic Signatures
b. GAMP 5: A Risk-Based Approach to Compliant GxP Computerized
c. Company IT Policies and Procedures
d. Industry Best Practices

APPENDICES

APPENDIX-A	Incident Response Plan

REVISION HISTORY

REVISION DATE	REVISION NUMBER	DESCRIPTION OF REVISION
02 Feb' 24	01	First edition of the SOP

APPROVAL		
Prepared by:	**Signature**	**Date**
Name:		
Designation:		
Reviewed by:	**Signature**	**Date**
Name:		
Designation:		
Approved by:	**Signature**	**Date**
Name:		
Designation:		
Authorized by:	**Signature**	**Date**
Name:		
Designation:		

Distribution:

1. **IT Department**
2. **HR**
3. **Related stakeholders (Management Employee)**

CONFIDENTIALITY

IT STANDARD OPERATING PROCEDURE	**DBLGROUP** **IT DEPARTMENT** **South Avenue Tower (6th Floor), House-50, Road-3, Gulshan-1, Dhaka, Bangladesh**				
TITLE:	Firewall Configuration				
SOP No.	Issue Date	Effective Date	Review Due	Copy No.	Page **6** of **6**
1.0.6					

This document shall be treated as confidential. No additional copies (except for copy holders) shall be made without approval of Head Department designee and a record must be kept for all the copies issued by IT Department.