ADIB – Standard

Security Device Standard
STD-ITD-554

Date: 30th December 2023

Version: 6.1

Version Control & Change Management

Version	Issue Date	Details of Change	Reason for change
6.1	December, 2023	Document has been reviewed and no change required	Annual process review
6.0	January, 2023	Added: Access lists will be deployed on highly secured zone of DMZ and SWIFT environment Modified control: Health check shall be conducted on Quarterly basis by the respective security devices/software vendors Modified control from 'Quarterly' to 'semiannually': Health check assessment review shall be performed by Service Owner semi-annually (preferably on quarterly basis)	To align with best practices of security device
5.1	December, 2022	Republished document. Document is up to date.	Annual process review
5.0	December, 2021	Updated frequency of conducting Health check to quarterly basis	Align with current practice followed
4.0	Publishing Date	Added Security Device Operational baseline related controls Added IPS Specific Rule	To align with best practices of security device
3.1	Publishing date	Republished document. Document is up to date.	Annual process review
3.0	Publishing date	Converted into new format	ITD Process Improvement
2.1	Publishing date	NESA Security Control update	NESA Compliance
2.0	Publishing date	Security Device logon access modified. Exceptions to compliance justification requirement added. Security Patch information updated.	GARR related findings addressed
1.2	Publishing date	Streamlining of complete Standard	Process Optimization

Prepared by	Approved by	Reviewed by
IT Governance Team	Head of IT Compliance and Security Architecture Head of IT Governance and Risk Management	IT Governance Manager IT Security Analyst Security Advisor and Business Continuity Manager

Document Contents

Internal

1 Overview

The objective of this standard is to pronounce the rules for managing the Security Devices.

2 Applicability

- This standard is applicable to ADIB ITD Security Devices (Cloud & On-prem) / Software's that are listed in STD-ITD-554 Appendix A- ADIB ITD Security Devices List.
- IT respective security & networks, and GRC Teams will be responsible for maintaining the standard on the respective Security Devices (Cloud & On-prem) / software's.

3 Standard Owner

Head of Technology GRC

4 Standard Statements

4.1 Security Device logon access

4.1.1 Privileged logon access to the Security Devices (Cloud & On-prem) should be restricted to authorized users only.

4.1.2 Unprivileged (read-only) access should be granted to IT-CSA-GRC specialist for security control assurance needs.

4.1.3 Access lists will be deployed on highly secured zone of DMZ and SWIFT environment.

4.1.4 Granting privileges to Security Device should be through Service tickets and follow published process for Access Control

4.1.5 Use of default IDs shall be prohibited for security devices (Cloud & On-prem)

4.2 Security Device administrative rights

4.2.1 Security administrators have the following privileges:

- Manage Security Device accounts & Granting privileges. Add, modify, delete, disable, or reset password accounts should be documented and approved as per change management process.
- Manage Backups & Restores Process. Backup & restore process should be scheduled according to Backup and Restore policy. Restoration of backup will be only used in case of emergency cases.
- Manage Security Device configuration rules. Add, modify, delete, or disable should be as per change management process.

4.2.2 IT-CSA-GRC representative shall have the following privileges:

- Review Security Device accounts & Granting privileges.
- Review Security Device / Archiving Processes
- Review Security Device Configuration
- Review Security Device Event alerts, Traffic & Audit Logs

4.3 Security Device Password Policy

- Password policy for the Security Devices shall be enforced according to published STD-ITD-552 Password Security Standard

4.4 Security Device Operational baseline

4.4.1 The Security Devices shall be physically secured in ADIB's Data centre and approved Cloud Service Provider

4.4.2 The Security Device must be configured in High Availability (HA Mode) as per ADIB IT Standard

4.4.3 Global Super admin password needs to be stored into the CHUB in a sealed envelope. Refer: Storage and Release of Password – Master-ID's process

4.4.4 Only Security Device administrators are allowed to make changes. This includes Security Device (Cloud & On-prem) configuration, patches, and upgrades.

4.4.5 Security Device must be managed from Internal Trusted Interfaces only, All Managed services should be blocked at untrusted & DMZ Interfaces
4.4.6 The Connection between security devices and Management station should be encrypted.
4.4.7 The security devices shall be patched as per the defined patch management standard.
4.4.8 Changes to security devices would be subjected to change management process. Further, it would be tested on an identified test / development environment before applying to the production environment, if applicable
4.4.9 All ports and services that are being used for diagnostic and configuration purpose shall be identified for all security devices and Disabled / Uninstalled where not required.
4.4.10 The security device shall be managed through the privilege access management solution (PAM)
4.4.11 Security solution /device shall have valid support and maintenance contract.
4.4.12 Health check shall be conducted on Quarterly basis by the respective security devices/software vendors.
4.4.13 Health check assessment review shall be performed by Service Owner semi-annually (preferably on quarterly basis)
4.4.14 Security solution /device firmware update shall be done at least annually and there should be a plan and tracker sheet to update all running security systems.
4.4.15 No Security solution /device shall be run on absolute firmware or software.

4.5 Security Device logs and backup

4.5.1 Security Device Traffic, Alert events & Audit Logs shall be sent to Centralized Log Monitoring System.
4.5.2 Security Device Configuration backup shall be taken weekly and stored securely on secure server.
4.5.3 Security Device Configuration backup shall be taken over secure channel.
4.5.4 Security Device shall be monitored for availability and performance.

4.6 Security Device Audit & Compliance baseline

4.6.1 Changes to the security device shall be reviewed for compliance to change management process.
4.6.2 Security Device configuration shall be reviewed at least twice a year following maintenance calendar. Justification for exceptions to permitted security device rules shall be documented and approved.

4.7 Firewall Specific Rule

4.7.1 Firewall rules description shall be defined clearly including business need.
4.7.2 Perimeter firewall(s) must control all traffic into/out of the network.
4.7.3 Firewalls rules base set are implicit deny for both inbound and outbound connections.
4.7.4 Firewall(s) interfaces must prevent the following:

- IP directed broadcasts traffic.
- All source addresses spoofing.
- IP Source Routing, all IP Packet with IP Option 2,3
- Traffic on the external interface that appears to be from an internal address (spoofing)
- IP unreachable Internet Control Message Protocol (ICMP) Message

4.7.5 Redundant, duplicate, shadow, orphaned, or unused rules and objects shall be removed.
4.7.6 Conflicting rules shall be amended when discovered.
4.7.7 Naming convention for rules shall be easy to use.
4.7.8 Prioritise rules in logical order according to the security requirements.
4.7.9 Group related rules together.
4.7.10 As far as possible, avoid using "**ANY**" for port number, source, or destination. Business justification shall be required for "**ANY**" rules if it is implemented.
4.7.11 Any rules that cannot be assigned to a known product, project or service owner should be monitored for traffic for 30 days. If traffic is not detected the rule should be disabled and left in place for a minimum of 14 calendar months. If after this time a request is not made to re-enable the rule, it should be removed, and the change logged.

4.7.12 Any objects that define multiple networks should be reviewed at least annually, to ensure they remain valid.
4.7.13 Any objects that define multiple networks shall be reviewed at least annually.
4.7.14 The firewall ruleset shall be reviewed at least bi-yearly to identify any unused rules, any temporary rules and to remove defunct rules.

4.8 IPS Specific Rule

4.8.1 Tuning IPS Signatures filter should be documented and approved as per change management process.
4.8.2 IPS Signatures must be running up-to-date signatures

4.9 Firewall Traffic Filtering

4.9.1. IP spoofing MUST be blocked.
4.9.2. Deep packet inspection and threat prevention shall be enabled where is applicable.
4.9.3. All unauthorised traffic shall be blocked from entering or leaving the firewall boundary.
4.9.4. Outbound traffic with destinations that are listed on DROP filter lists shall be dropped. Similarly, inbound traffic from such destinations shall also be dropped. Allow only required traffic for Inter-VLANS communications involving external servers. Outbound client web traffic shall be allowed through the firewall based on service profiling.

5 Exceptions

Any “Exceptions” to this Standard requires business justification, compensating controls, and Standard Owner signoff. Any “Non-compliance” to this Standard shall be considered for corrective actions and corresponding corrective action/exception must be maintained by the respective team.

6 Appendixes

Annex I: Acronyms

Acronym	Explanation (Expanded Term)
ADIB	Abu Dhabi Islamic Bank
NESA	National Electronic Security Authority, Abu Dhabi also known as Signals Intelligence Agency
ITD	Information Technology Department
SWIFT CSP	Society for Worldwide Interbank Financial Telecommunications Customer Security Program
PCI DSS	Payment Card Industry Data Security Standard
CBUAE	Central Bank of the UAE
CSA	Compliance and Security Architecture

Internal