**Process Document - 10**

**Firewall Management Procedure**

|  |  |
| --- | --- |
| **Document Control Sheet** | |
| **For Airtel Money Environment only** | |
| Document Name | Firewall Management Procedure |
| Document Owner | Venkatachal Hegde |
| Effective Date | xx-04-2013 |
| Review Date | 15-04-2013 |
| Review Remarks |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Document Version Control** | | | | |
| **Version** | **Date** | **Prepared By** | **Reviewed By** | **Approved By** |
| 1.0 | 08-04-2013 |  |  |  |
|  |  |  |  |  |

**Table of contents**

[1. Firewall Management Overview 3](#_Toc353370038)

[2. Firewall Management Procedure 5](#_Toc353370039)

[3. Firewall Management Procedure-II 9](#_Toc353370040)

[4. Key Performance Indicator 11](#_Toc353370041)

1. **Firewall Management Overview**
2. Introduction

Firewalls are an integral part of defense-in-depth strategy. At the perimeter, they prevent malicious traffic and attacker from entering the corporate network; while internally they help to control access on a need-to-know and need-to-do basis.

With varying architectures and configuration, it’s very important to define a structured way of managing and interacting with firewalls. The objective of this procedure is to define procedures and essential rules regarding the management and maintenance of firewalls at Airtel Money environment.

1. Definitions

**Change Management -** It is an organized, systematic application of the knowledge, tools, as resources change state from current to a desired.

**Configuration -** Selection of one of the sets of possible combinations of features of a system.

**Encryption -** Process by which data is temporarily re-arranged into an unreadable or unintelligible form for confidentiality, transmission, or other security purposes.

**Firewall** - A system designed to prevent unauthorized access to or from a private network.

**FTP -** File Transfer Protocol, a standard Internet protocol, is the simplest way to exchange files between computers on the Internet.

**Logging -** The process of recording events at the time they occur.

**Network Address Translation -** Re-writing the source and/or destination addresses of IP packets as they traverse (internal to external & vice versa) through a router or firewall.

**Remote Access -** Ability to get access to a computer or a network from a remote distance.

**Virtual Local Area Networks -** Work stations connected to an intelligent device which provides the capabilities to define LAN membership.

**Virtual Private Networks -** A virtual private network is a logical network that is established, at the application layer of the Open Systems Interconnection model, over an existing physical network and typically does not include every node present on the physical network

1. Applicability

This procedure is applicable to management of all firewall appliances deployed within Airtel Money environment.

This procedure serves the following purpose:

* Guidelines for secure configuration of the firewall appliance.
* Steps to follow for carrying administrative activities like privileged user registration, policy (rule base) creation and change, configuration backup, third party connection, remote administration, OS update etc.
* Exceptions from this procedure will be permitted only, if approved in advance, and in writing by the Airtel Money Central Security Team.

1. Dependencies

This procedure has dependencies on other procedures and guidelines and should be read in conjunction with the following documents:

* Asset Management Procedure
* Audit Logging Procedure
* Backup & Restore Management Process
* Change Management Procedure
* Information Labeling and Handling Guidelines

1. Central Security Team

Security Operations Center (SOC) shall be assigned with the responsibility for installing, configuring and maintaining all firewall appliances and its configuration.

1. Labelling

Every firewall should be physical tagged in-accordance with the ‘Information labelling and Handling’ Guideline. The physical identification tag pasted on the firewall appliance should detail the following items:

* Identification Tag in the format: Comviva\<OpCo>\<Asset Type>\<Asset No>
* Name of the Owner
* EMP ID of the Owner
* Name of Custodian
* Issued Date
* Asset Class

1. **Firewall Management Procedure**
   1. Baseline Security Set

The firewall MUST be primarily used for the purpose of access control only. Enabling of secondary functions like DHCP, proxy, URL filtering, AAA server, Content filtering etc on the firewall is NOT authorized.

* The operating system and the firewall application should be secured based on the baseline configuration document prepared for the respective firewall type and base operating system. It is mandatory that all configuration settings listed in the baseline document are applied to the firewall before releasing it to production. Due approval should be obtained from the Central Security Team before production release.
* The firewall should not have any additional services running, that can be accessed remotely. Any additional service like SMTP, DNS running on the firewall machine would present the attackers with an opportunity to compromise the firewall by exploiting vulnerabilities associated with the service.
* The hostname of the firewall should confirm to the Airtel Money Naming Convention as documented in Information Security Policy
* A deterrent banner conforming to Information Security Policy should be displayed to the user upon successful logon.
* All default vendor supplied user accounts should be disabled after setting their password to a complex value.
  1. Firewall Interfaces

The firewall should segment the network based on the risk levels. Systems with similar risk level should be put into one segment. For example if the firewall is segregating the internal network from the Internet there should be a minimum of three segments- one for Internet, one for internal network and one for machines that are accessed from both internal network and Internet.

* Central Security Team will be responsible for determining the number of segments and the servers that will be located in each segment. Due approval should be obtained from the Central Security Team before adding or removing servers / applications to / from a Firewall segment.
* Listed below are guidelines to adhere while determining the number of firewall segments and servers/ application to be hosted within that segment:

Sensitive and critical applications/ servers that are accessed only internally should be hosted on the most protected segment of the firewall.

* System accessed internally as well as by external sources should be hosted on a separate segment of the firewall, preferably the De-militarized Zone (DMZ). Additionally, for better manageability, these systems can further be classified into business application and infrastructure support applications with each category hosted in a separate DMZ.
* Connection links from third parties, contractors etc. should terminate on a separate interface of the firewall.
* Wide Area Network (WAN) links connecting various circle offices to the central Data Center should terminate on a separate interface of the firewall.
* Administrators normally require unrestricted access to systems and networks they manage. In case these administrators have their machines configured as part of the user LAN, there is strong possibility that malicious user may sniff the administrative communication and thereby gain unauthorized administrative access. To avoid this, it is necessary to group all administration terminals on to a separate interface of the firewall with access restricted to only administrators. Additional security measures like dual factor authentication should be considered for protecting these terminals
  1. Rule-base Creation

SOC will be responsible for designing and testing the firewall rule-base before deployment in production. SOC should get the required inputs from the respective application owner for designing the rulebase. Following guidelines should be adhered while adding or modifying rulebase:

* By default the firewall MUST have a DENY ALL policy, with access granted on a need to do basis. Firewall should have a rule to deny all access that is not explicitly allowed.
* Only required services/ ports MUST be opened between specific source and destination IP addresses/ subnets. Use of the ‘ANY’ literal either in the source, destination or service/ ports MUST be strictly avoided.
* Firewall rulebase should restrict access to required ports on the target machine. The source field in the rulebase should be restricted to specific IP addresses/Subnet addresses wherever feasible. In the case of applications where the number of individual IP addresses/subnets is very large the source address can be made generic to make the rule base more manageable.
* Servers which are directly accessed from a public network like Internet should be moved to a separate segment (De-Militarized Zone) of the firewall. The IP address of the server should be NATed with a public IP addresses.
* For connections with third parties NATing should be performed using any available private/ public address slot.
* Access to administrative ports including SSH and Microsoft Windows Terminal services on protected servers should have user ID based authentication at the firewall in addition to source IP address. User authentication provides additional security and also provides facility for authenticating roaming users.
* Firewall user-database, needed for rules that are configured for user-authentication, can be stored either locally on the firewall or in an external directory server. Enforce password policy for these user accounts including password expiry, password history, and password complexity. Account lockout should be configured to prevent password cracking attempts. It should be ensured that these user credentials are transmitted in encrypted format from the user desktop to the firewall.
* The rulebase should be approved by application owner and should come through PCR form (Policy Change request) prior to deployment. CST should give a copy of the tested rulebase pertaining to the application to the respective application owners. This will ensure that application owners are aware of the services that will be allowed through the firewall prior to deployment. This will also help in reducing troubleshooting efforts when the firewall goes into production.
* Certain applications like Oracle; Active FTP uses random ports for data transfer between the client & server, after the initial handshake has taken place over a standard port. Using such applications demands opening all ports between the client and server for successful communication. For such access requirements the following service group should be created to avoid exposing all standard TCP/UDP ports.

Create a service group for the application consisting of the standard port for initial

communication and all higher end TCP/UDP ports (1024 & above)

* Service Group = Standard port + (1024 – 65536)

Open access for the service group between the desired client and server.

* As enabling logging will generate voluminous data, enable logging on the individual rules judiciously.
* The comments column for each rule MUST have the following information duly entered:-

The request number

* + Purpose of the rule
  + Expiry date, for temporary rules.
* The LAST rule for each segment MUST be a ‘DENY ALL’ rule denying all traffic not explicitly allowed. Logging should be enabled on this rule.
  1. Rule-base Change
* After the firewall goes into production, all changes to the rulebase should be done after proper authorization, to ensure that the security level is maintained at all times. User should contact the application owner for any access requirement. Application owner should validate the request, translate the user request to specific IP address and port numbers and pass it to SOC.
* The SOC should analyze the request and conduct a security impact analysis.
* A backup/ recovery strategy should be in place to ensure that an implementation failure does not adversely impact availability of other systems and firewall, in general.
* Situation where the exact access requirements are not known (for e.g. exact ports to open between source and destination IPs) changes can be implemented by initially enabling more access and enabling logging. The logs should then be used to verify the exact port requirements. The activity of fine-tuning the ports based on firewall logs should be completed within 6 hours of enabling, as there is risk of unauthorized access during this time.
  1. Administrative Access
* Administrative access to firewall is required for activities including rule base modification, firewall-user account management, firewall-administrator account management and log monitoring. Super-user privileges should be provided to members of the SOC on a need to have and need to do basis.
* Default passwords for all vendor-supplied user accounts should be changed to complex combination in-accordance with ‘Password Management Standard’. Logical access to the firewall should be limited to the SOC. Each administrator should have separate account within for management. Local system administrators should not have access to firewall application. Administrator accounts on the firewall should have password policy and account lockout configured.
* Access to firewall administration programs should be through encrypted channels. If the firewall software itself does not provide this facility, then additional mechanisms like IPSEC should be used for this purpose.

1. **Firewall Management Procedure-II**

* 1. Logging
* Logging needs to be enabled to ensure that all critical access is tracked. Logging should be enabled for rules enabling administrative access (e.g. SSH access to Airtel Money web server). Logging should not be enabled for normal user access (e.g. HTTP access to Airtel Money web server).
* Logging should be enabled for the last rule that blocks all access that is not explicitly allowed by the other rules.
* Logging should be enabled to track any changes done to firewall configuration including changes to rule base. This will ensure that all changes can be tracked for trouble shooting as well as for audit purposes.
* The SOC should monitor the logs periodically for the following activities:
  + Port scans
  + Authentication failures
  + Denial of service attempts
  + Failed connections
  1. Performance Monitoring

Resource utilization should be tracked to ensure that firewall is performing at optimum level. SOC should monitor the critical system parameters on a continuous basis. Any surge in utilization of any of these parameters might be an indication of a system under attack. SOC should determine threshold levels for peak and average usage for the following parameters.

* CPU utilization
* Memory utilization
* Hard disk free space
* Concurrent Connections
  1. Change Control
* Changes to the following should adhere to change management process:
* OS Upgrade / installing a new patch on the firewall
* Firewall Application upgrade
* Installation or removal of additional component
* Integration of Firewall with third party components
* Adding a new segment or modifying existing segment
* Central Security team will be responsible for approving the changes. The SOC should be responsible for implementing the changes on the firewall.
  1. Virtual Private Network

Following guidelines should be followed for establishing a Virtual Private Network (VPN) with trusted third parties which include Strategic partners, support vendors, third party service providers, application development group requiring permanent connection to Airtel Money network, remote/ international branches, business groups like contractors & other institution with whom Airtel Money has business relations/ ties.

* Ideally, a separate VPN management device (Concentrator) should be deployed for establishing, configuring and managing VPN connection. Use of a firewall appliance for setting up VPN connections should be avoided to prevent performance bottlenecks. Also, there is possibility that a vulnerability in either the access control or VPN module can be exploited by adversary to gain un-authorized access.
* The preferred methodology for setting up VPN with a trusted party is IP Security (IPSEC), as if offers reliable level of security, interoperability and control over the tunnel parameters. Use of other methodologies like Layer 2 Tunneling Protocol (L2TP) or Point to Point Tunneling Protocol (PPTP) should be considered only if setting up an IPSEC tunnel is not practically feasible.
* The nature of VPN to set namely Site-to-Site or Client-to-Site (Remote access VPN) will depend upon the purpose and number of clients behind the VPN gateway on either side.

* 1. VPN creation request and approval
* The Application/ Business group requiring the VPN setup should send a formal VPN creation request detailing the following information to SOC:-
* Requestor Name
  + - Application/ Business group
    - Name of the Third Party
    - Need/ Justification
    - Nature of the Tunnel – Temporary/ Permanent& Time frame
    - Airtel Money Server/ Client IP addresses or Hostname
    - Number of third party client accessing the infrastructure (this will help to decide whether to set up a Site-to-Site or Remote access VPN).
* SOC should conduct a security risk analysis based on the following parameters and forward the request along with their recommendations to Central Security team for approval:
  + - Criticality of Application/ Business unit
    - Business Impact
    - Nature of services
    - Extent/ Type of data being shared
    - Third party status
* The Central Security team based on SOC recommendations will approve/ dis-approve the creation of the VPN tunnel.
* Post-approval a designated Point of Contact should be identified from each side namely Application/ Business group, SOC and Third party for coordination and troubleshooting.
* Upon completion of the time frame, the VPN tunnel should be initially disabled and if no subsequent errors or requests are received, it can be deleted. VPN tunnels of recurrent nature can be maintained in a disabled state for a period of one month. If a re-establishment request is not received within this period, the tunnel should be deleted. Thereafter any request for establishing the same tunnel should follow the VPN creation/ approval process afresh.
  1. VPN tunnel parameters
* The section documents the standard values for various tunnel parameters for IPSEC VPN. These should be negotiated with the third party and consent obtained before setting up the tunnel.

|  |  |
| --- | --- |
| Parameter | Value |
| Authentication | Pre-share/ Digital Certificate/ Group Password/ Individual Password |
| Hashing | SHA1 / MD5 / HMAC |
| Encryption | DES / 3DES / AES |
| IKE Security Association | 86400 seconds (24 hours) |
| Mode of Operation | Main Mode |
| **IPSEC Phase II Parameters** | |
| Hashing | SHA1 / MD5 / HMAC |
| Encryption | DES / 3DES / AES |
| IPSec Security Association | 28800 seconds (8 hours) |
| IPSec Security Protocol | Encapsulated Security Payload (ESP) |
| **Key Generation** | |
| Algorithm | Diffie-Hellman Group 5 |

* Digital Certificates should be the preferred method for authentication. Use of pre-shared key shall be allowed in the event of practical difficulties with digital certificates. The minimum length for the pre-share key should be 32 byte.
* For remote access VPN, group password should be the preferred method of authentication. The group password should be minimum 12 characters in length.
* Message Digest 5 (MD5) / Hashed Message Authentication Code (HMAC) should be preferred message hashing/ integrity checking method.
* Main mode should be the preferred mode of operation for Internet Key Exchange (IKE).
* Encapsulated Security Payload (ESP) should be the preferred security protocol for IPSec phase II as it offers message encryption & integrity both.
* By default, the encryption parameters should be configured with the maximum number of bits available for the selected encryption algorithm.
  1. Backup & Recovery

The SOC will be responsible for backup and recovery of the firewall. The following should be backed up soon after installation and successful testing of the firewall and securely stored:

* Firewall OS files
* Firewall application files
* Configuration files

Firewall rule base

* Routing Table
* Firewall logs
* A full backup of firewall application/operating system files should be taken before any major changes to firewall including:
* Upgrade of Firewall OS /Application
* Installation of any additional component on Firewall (e.g. VPN)
* Integration of Firewall with third party components (e.g. Integration of Firewall with RSA for authentication)
* Adding a new firewall interface
* Backup of firewall logs and audit trails should be taken on a daily basis and archived for a period of six months to meet statutory requirements and for forensic analysis.
* Backup of firewall policy / rule base should be taken before and after addition of new rules or modification to any existing rule.
* By default, a backup of firewall configuration and policies should be taken on a monthly basis, irrespective of whether changes are made to the firewall or not
  1. High Availability
* Firewall redundancy should be configured based on the criticality of the applications and network segments/ zones being protected. For critical applications/ zones firewalls should be configured in high availability mode to ensure minimum downtime for the respective applications.
* All communication between the primary and secondary firewall appliance should be secure using supported encryption technologies and dedicated communication channels like cross-over cables
  1. Documentation

The SOC should maintain detailed documentation of the firewall architecture and administration tasks.

Firewall architecture documentation should include the following:

* Network diagram with firewall segments/ interfaces

IP addresses of firewall interface and network devices connected to the firewall

* Routing table of firewall and connected devices

Documentation on firewall administration tasks should include the following:

* Installation and configuration of the firewall
* Adding/Deleting/Modifying firewall rule base
* Adding/Deleting/Modifying firewall routing table
* Adding/Deleting/Modifying firewall Users
* Adding/Deleting/Modifying firewall Administrators
* Backup/Recovery of firewall OS/Application files
* Backup/Recovery of firewall Rule base
* Backup/Recovery of log files
* Backup/Recovery of user database

1. **Key Performance Indicator**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **SlNo.** | **CTQ** | **KPI** | **Reports/Logs** | **Acceptable Limits** | **Accountability** |
| 1 | Ensuring Baseline Security configuration settings are done on all Firewalls | Number of Firewalls wherein secondary functions like DHCP, proxy, VPN, URL filtering, AAA server and/or Content filtering were enabled other then basic purpose of access control v/s total number of Firewalls installed | Monthly Report to be prepared by SOC on % such Firewalls installed |  | Central Security Team |
| Number of Firewalls released in to production Environment wherein due approval was not taken by Central Security team about configuration settings listed in the baseline document v/s total number of Firewalls released | Monthly Report to be prepared by SOC on % such Firewalls released in to production environment |  | Central Security Team |



Annexure :

1. Contact Details :

|  |  |  |
| --- | --- | --- |
|  | **Contact Person** | **Contact details** |
| Security Operations Center |  |  |
| Business Head |  |  |
| Business Head |  |  |