Firewall Policy

1.Introduction

Gemporia recognises that payment card information is a valuable asset. Managing security systems and the information they contain is vital to maintain Gemporia’s reputation and the ability to continue trading successfully.

Gemporia considers the security of its cardholder data environment (CDE) and cardholder data to be a crucial element of its business and, to this end, has created a well-defined set of policies, standards and procedures to support secure operations

The aim of this policy document is to lay out how Gemporia will operate its Firewalls in order to uphold security standards required and desired for this role.

2.Scope

This policy applies to the people, processes and technology that interact directly or indirectly with firewall or security appliance hardware within the CDE.

This policy document is designed to be used in conjunction with the appropriate implementation standards as defined by Gemporia in accordance with best practices.

3.Policy Statement

3.1 Network Design

1. The CDE shall be restricted to a minimum within a DMZ to discard direct traffic communication from trusted to untrusted network zones
2. Logical firewalls will segregate the DMZ from all other networks, including but not limited to trusted networks and untrusted networks
3. A firewall must segregate trusted and untrusted networks
4. All traffic must flow through the firewall before changing from one zone to another

3.2 Configuration

1. Firewalls must be stateful and only permit established connections
2. Router startup configurations must be synchronized with the running configuration file as soon as reasonably possible
3. An explicit default policy of deny / drop must be defined, even if an implicit rule exists
4. Direct connections from untrusted networks to trusted or DMZ networks must be prohibited
5. Direct connections from trusted or DMZ network to untrusted networks must be prohibited
6. Router configurations must be backed up securely and transmitted over secure channels

7. All configuration must be performed over a secure connection using suitably robust encryption techniques
8. Firewall logs must be stored on an external device as soon as possible and stored for 1 year
9. Sufficient efforts must be made to prevent brute-force attacks against the firewall
10. All management sessions must disconnect after a timeout period of no longer than 10 minutes
11. All vendor supplied defaults must be changed before device is connected to the network
12. All unnecessary default accounts and credentials must be removed or disabled

3.3 Documentation

1. All business justification shall be documented for each firewall configuration beyond what is considered best practice / vanilla setup.
2. The Standard will be followed when configuring routers / firewalls
3. A network diagram (
   PDF
   VSD
) will reflect the current CDE at all times
4. Existing rules in firewalls are to be reviewed at least once every six months to confirm the business need / justification still exists and that allowed protocols are still classed as secure.
5. The firewall standards will describe the user management groups

Revision History

Date	Who	Description
12/08/2015	Andrew Smith	Original Document
13/10/2015	Andrew Smith	Added 3.2.9
02/12/2015	Andrew Smith	Added 3.3.5
5th April 2016	Andrew Smith	Review: no change
19th September 2016	Andrew Smith	Added new PCI network diagram, now contained in this document for simplicity