

Firewall and Router Policy

Reference: PCI POL 1.1

DocumentKits Issue No: 1.1

Organisation Issue No:

DocumentKits Issue Date: 29/06/2020

Organisation Issue Date:

1. Scope

All firewalls and routers within, or connected, to Organisation Name's cardholder data environment (CDE).

The policy applies to all network devices, including but not restricted to Firewalls, routers, switches, access points, that are live or form a back-up of the GRCI International cardholder data environment. This policy must be applied prior to a network device being attached to the network. Furthermore, any third party accessing or configuring a network device, must also comply with this policy.

2. Responsibilities

2.1 The

"Enter applicable role"

is responsible for the configuration and maintenance of Organisation Name's firewall and routers and as further described in 3.8 below.

2.2 The

"Enter applicable role"

is responsible for approving configuration changes to firewall and routers.

3. Requirements

3.1 A firewall is required and is present at each internet connection and between any demilitarised zone (DMZ) and the internal network, and any untrusted connection and the internal network.

Firewalls are installed between any authorised wireless networks inside or outside the cardholder data environment and the cardholder data environment itself. These firewalls

are identified on the current network diagram (see 3.8 below). These firewalls are configured to deny, or control, any traffic (which has a valid business justification) from the wireless environment into the cardholder data environment.

3.2 Firewall & router configuration

3.2.1 Firewalls are configured, on the basis of the scope assessment and the analysis of cardholder data flows, to restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and to restrict connections between untrusted networks and trusted networks, system components in the CDE. All other inbound/outbound traffic is specifically denied, e.g. using an explicit 'deny all'.

3.2.2 Firewall and router configuration files are secured and synchronised, in that running configuration files and start-up configuration files (used during re-boot), have the same, secure configuration.

"Detail how you secure and sync these files."

3.2.3 The firewall performs stateful inspection (dynamic packet filtering) ensuring only established connections are allowed into the network.

3.2.4 IP masquerading is implemented on all firewalls and routers to prevent internal addresses and routing information from being translated and revealed on the Internet, e.g. Network Address Translation (NAT).

3.3 All proposed changes to network connections, and to firewall and router configurations, must be approved in advance and then tested after completion(s).

3.3.1 All changes must be authorised and approved by

"the Change Authority Board"

in conjunction with the change management process. These requests must describe clearly the current configuration, the proposed change, the business or technical reason for making the change, and the means by which the change will be tested to ensure that adequate security is maintained.

3.3.2 The Head of IT (CIO) is responsible for maintaining records of all tests carried out to ensure that changes have not reduced required security.

3.4 Organisation Name maintains firewall and router configurations which lists services, protocols and ports necessary for business.

"This document, which should be under formal document control, must be created to reflect the specific firewalls and routers in place in your organisation, and it should be referenced from here – i.e. where is it located?"

Justification is provided for each permitted
"service/protocol/port. "

If insecure
"services/protocols/ports"

are necessary (e.g. FTP), security features are documented.

<< 3.5 – 3.10 removed for sample purposes >>

Document Owner and Approval

The Information Security Manager is the owner of this document and is responsible for keeping it up to date.

The current version of this document is available to
"Specify which members of staff this document is intended for"

and is published
"Describe the location(s) – electronic and physical – where this document is available"

Its approval status can be viewed in the [Master List of Document Approval](#).