2Cana Policy for Firewalls			
ISSUED BY	Systems Network Team	Date	2019/04/29
APPROVED BY	Management Forum		

Revision History

Date	Author	Details
2019/04/29	Neville Moonsamy	Original

HEAD OFFICE

08610 2CANA

1st Floor Ridgeview Building

1 Nokwe Avenue

Umhlanga Ridge, Durban

2Cana Solutions (Pty) Ltd.

Reg no. 2002/028673/07

HARARE

+263 867 710 4494

6 Childwall Road

Bluffhill

Harare

INTERNATIONAL

+27 31 583 3200

19 Church Street

Port Louis

Mauritius

Purpose

This Policy is approved by 2Cana Risk Management and sets out the Firewall Security Policy within the company. The purpose of this policy is to define standards to be met by all firewall gateways owned and/ or operated by 2Cana Networks & Security. These standards are designed to minimise the potential exposure to 2Cana Solutions from the loss of sensitive or company confidential data, intellectual property, damage to public image etc., which may follow from unauthorised use of 2Cana company resources. The 2Cana Networks are constantly changing to meet the needs of business and continue to expand.

2Cana Solutions has standardised on Fortigate Firewalls at the perimeter as well to segment the network into segments. The segments can be classified as:
Public DMZ, Private DMZ, Extranet, Mail and Remote Access Segments.

The policy defines the following standards:

- Ownership and Responsibilities
- Securing the Base Installations
- Implementation of Secure Default Settings
- Change Control requirement

.

Policy Scope

This policy applies to all employees of 2Cana Solutions; as well as Vendors, Contractors, 3rd Parties and any others doing business with the 2Cana Solutions will be subject to the provisions of this policy. Any other parties, who use, work on, or provide services involving 2Cana Solutions computers, technology systems, and/or data will also be subject to the provisions of this policy.

Violation of Policy

If it is suspected that this policy is not being followed, report the incident to the Head of 2Cana Systems and IT Risk Management. Any exceptions to this policy must be approved in advance by the Head of 2Cana Systems and IT Risk Management.

Policy

All Fortigate firewalls owned and/or operated by 2Cana Solutions Networks & Security and/or registered in any Domain Name System (DNS) domain owned by 2Cana Solutions must comply with this policy.

Enforcement

Any person found to have violated this policy will be subject to appropriate disciplinary action as defined by the provisions of the Company.

Ownership and Responsibility

Firewalls within the scope of this policy are administered by the 2Cana Networks & Security Department.
Networks & Security Department will be responsible for the following:

- Equipment must be documented and monitored by the Networks & Security Monitoring systems.
- Equipment must have appropriate Domain Name Server (DNS) records.
- Ensuring the implementation of the Firewall Security policy.
- Changes to existing equipment and deployment of new equipment must follow the 2Cana Solutions Change Management processes and procedures.
- To verify compliance with this policy, 2Cana Solutions Networks & Security Department will periodically audit the firewall's configuration.

Securing Base Installation

All firewalls must comply with the following configuration policy:

Physically Secure the Firewall

Physical security is the cornerstone of internetworking security. If an attacker can gain physical access to your device, all the patches, and firewall feature sets in the world cannot protect them. The attacker can cause either overt or covert damage to your network when physical access is compromised.
Overt damage is classified as immediate shutdown of the services provided by the firewall. Covert damage is much harder to find and correct. It consists of the intentional introduction of malicious information that affects the firewall's services.

Apply latest OS Patches

Installing up-to-date vendor patches and developing a procedure for keeping up with vendor patches is critical for the security and reliability of the system. 2Cana Networks & Security must patch each installed component of the Fortigate Firewalling system. Consideration must be given to the patch levels of the OS. Vendors will issue operating system updates when they become aware of security vulnerabilities and other serious functionality issues.

Create Secure Configuration of all Firewall Components

In addition to the firewall(s), Security must configure the administrator workstations securely.

Change all Default Account ID's and Passwords

Security must change the default passwords used during firewall installations.

Configure Encrypted Connections to All Firewall Devices

Ensure that SSH is running and logging and no plaintext protocols (telnet, ftp, etc) are running on the firewalls.

User Authentication and Local Account

One Local Account will exist on each Firewall.

Authorize Administrator GUI's by IP Address

Define GUI access by IP addresses or subnet range for authorised Administrators.

Ensure Network Time Protocol is Setup Correctly

Ensure NTP or an acceptable substitute is providing accurate time sourcing to the firewall devices.

Enable Secure Logging

Configure all the firewall gateways to log to the Forti-analyzer and/or configure local logging.

Secure SNMP

SNMP must be secured with an unpredictable community string (SNMP password).

Enable Firewall Stealth Rule

Create a rule to drop "Any" Service "Any" Source or "Any" VPN that attempts to connect to the firewall. The stealth rule will limit access to the firewall to the control and service connections enabled as part of the design.

Configure a Default / Cleanup Rule

Ensure that the final rule in the rule base explicitly drops all services, destinations, etc not specifically allowed in the previous rules.
It is important that any access not explicitly allowed be explicitly dropped.

Enable logging of Implied Rules

Enable the logging of implied rules.

Enable Version Control and Export of Configurations

Use database Revision Control. Regularly backup all Firewall Configurations.

Change Management

A Change Management process is invaluable for security. It assures that changes to devices are made in a logical, orderly manner and facilitates good security measures. 2Cana Networks & Security employees will adhere to the 2Cana Change Management process at all times.