Title: Stateful Traffic Filter Firewall Essential Security Requirements
Maintained by: CCDB Work Group for Stateful Traffic Filter Firewall
Version: 0.2
Date of issue: *2014-May-1*
Supersedes: *Version 0.2*

Status

The CCDB Working Group has been requested to develop an Essential Security Requirements (ESR) specifies the essential requirements for Stateful Traffic Filter Firewalls. This initial draft contains material that was provided by the requestor, the United Kingdom, for a cPP.

Background and Purpose

This document describes the high-level set of security requirements that a Stateful Traffic Filtering Firewall (hereafter 'Firewall') will satisfy when evaluated against the cPP written for such technology.

A firewall is a network device connected to one or more distinct networks, which filters layer 3 and layer 4 (IP and TCP/UDP) network traffic, optimised through the use of stateful packet inspection) based on an administrator-provided set of rules – whether to allow, deny or log particular packet flows. This provides control on the flow of information between attached networks based on the configured rules based on network layer 3 and 4 traffic attributes (i.e., addresses and ports) and derived session state information.

Use Case(s)

- A firewall is a network device which provides at least two physical network interfaces for connecting to two or more distinct networks; firewalls may also provide one or more logical interfaces to enable a wide range of configuration options.
- The firewall will operate as part of an enterprise infrastructure; an administrator will configure a set of rules to permit, deny, and/or log particular data flows between physical or logical network interfaces. This then helps the enterprise manage information risk by reducing the attack surface of protected networks, and reducing the ability of inadvertent information disclosure from within such networks.

Resources to be protected

- Network devices/subnets associated with a network interface of the firewall
- Any network-facing management interfaces, including traffic to and from the device, including any critical data (e.g., audit data).
- Updates to the device.

Attacker access

- An attacker can send arbitrary packets to network interfaces.
- An attacker can intercept and arbitrarily modify or drop packets within existing traffic flows.

Attacker Resources

- An arbitrary amount of time to study traffic flows to/from a device
- Many sample devices to test and attack

Boundary of Device

- The hardware, firmware and software of the firewall define the physical boundary.
- All of the security functionality is contained and executed within the physical boundary of the firewall.

Essential Security Requirements

- The firewall shall have the ability to filter IPv4 and IPv6 network traffic.
- The firewall shall implement administrator configurable rules for traffic flow, giving the ability to allow, deny or log traffic flows according to the rules.
- The firewall rules shall allow the specification of a source IP address, destination IP address, transport layer protocol, source port, and destination port.
- The firewall shall employ stateful packet inspection when determining whether the network packet should be allowed to flow.
- The firewall shall deny, and be capable of logging, packets which are invalid fragments and fragmented IP packets which cannot be re-assembled completely.
- The firewall shall apply rules to network packets where the source address of the network packet is equal to the address of the network interface where the network packet was received, and where the source address of the network packet does not belong to the networks associated with the network interface where the network packet was received.
- The firewall shall apply rules to network packets where the source address of the network packet is defined as being on a broadcast or multicast network, or is defined as being a loopback address.
- The firewall shall apply rules to network packets where the source or destination address of the network packet is a link-local address.
- The firewall shall apply rules to network packets where the source or destination address of the network packet is defined as being an address “reserved for future use” as specified in RFC 5735 for IPv4, or is defined as an “unspecified address” or an address “reserved for future definition and use” as specified in RFC 3513 for IPv6
- The firewall shall reject, and be capable of logging, network packets with the IP options: Loose Source Routing, Strict Source Routing, or Record Route specified.
- The firewall shall reject, and be capable of logging, any network packets for which the source or destination address is inconsistent with its configured interfaces.
- The remote administration functions shall use cryptography to protect this communication path.

- The device shall be capable of auditing administrative actions, including any configuration changes and rebooting of the device.
- The device shall provide an authentication mechanism for local and remote administrators.
- The device shall provide an authentication mechanism for local and remote administrators, as well as the device itself (e.g., the device maintains an authentication credential that can be used to authenticate it to an administrator's client)
- The device shall provide a cryptographic means to validate the source of updates to be installed on the device.
- The device shall require any default passwords / other credentials to be changed.
- The device shall protect keys, key material, and authentication credentials from unauthorized disclosure.
- The device is robust against malformed network packets, including denial-of-service attacks.
- The device shall provide self-tests to ensure the security functions it implements are operating correctly.

Assumptions

- There are no general purpose computing or storage repository capabilities (e.g., compilers, debugging tools, editors, web servers, database servers or user applications) available on the device, unless they are directly related to the security functionality of the device (e.g., webserver to facilitate remote administration).
- The device is protected from physical attacks by the wider environment

Optional Extensions

Requirements captured in this section may already be realized in some products in this technology class, but this ESR is not mandating these capabilities exist in "baseline" level products.

- The device shall be able to assign which interface(s) remote administration may take place

Objective Requirements

Requirements captured in this section specify security-relevant behaviour that is not expected to be realized currently in products, but are capabilities that may be mandated in future versions of the ESR and resulting cPPs.

- The device shall have internal security features to make the device more resilient to security breaches.
- The device shall provide two-factor authentication natively on the device (i.e., does not rely on a separate device to provide this capability).

Outside the Scope of Evaluation

- Filtering at layer 2 of the network stack.
- Virus scanning, including email scanning.

- Intrusion detection/prevention capabilities
- Network Address Translation (NAT) as a security function..
- Virtualized network functions.