opsec
Internet-Draft
Intended status: Informational
Expires: August 19, 2014

F. Gont
SI6 Networks / UTN-FRH
M. Ermini
ResMed
W. Liu
Huawei Technologies
February 15, 2014

Requirements for IPv6 Firewalls
draft-gont-opsec-ipv6-firewall-reqs-00

Abstract

While there are a large number of documents discussing IP and IPv6 packet filtering, requirements for IPv6 firewalls have never been specified in the RFC series. When it comes to IPv6, the more limited experience with the protocols, and reduced variety of products has made it rather difficult to specify what are reasonable features to be expected from an IPv6 firewall. This has typically been a problem for network operators, who typically have to produce a "Request for Proposal" (from scratch) that describes such features. This document specifies a set of requirements for IPv6 firewalls, marked as "mandatory", "recommended", or "optional".

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on August 19, 2014.

Copyright Notice

Copyright (c) 2014 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. DISCLAIMER

This initial version of the document is based on a typical IPv6 firewall RFP, and is mostly meant to trigger discussion in the community, and define a direction for the document. Future versions of this document may content all, more, or a subset of the requirements present in the current version of this document. Additionally, the current version DOES NOT yet properly separate requirements among MUST/REQUIRED, SHOULD/RECOMMENDED, and MAY/ OPTIONAL.

Additionally, this version is meant to provide requirements, rather than implementation guidelines.

2. Introduction

While the IETF has published a large number of documents discussing IP and IPv6 packet filtering (see e.g. [RFC7126], requirements for firewalls have never been specified in the RFC series. When it comes to IPv4, a number of features have become common over the years, and firewall requirements have somehow become operational wisdom. When it comes to IPv6 [RFC2460], the more limited experience with the protocols, and the reduced variety of IPv6 firewalls has made it rather difficult to specify what are reasonable features to be expected of IPv6 firewall. This has typically been a problem for network operators (who typically have typically had to produce a "Request for Proposal" from scratch), but also for vendors (who lack a well defined set of requirements to comply to).

This situation has not only made the process of purchasing an IPv6 firewall harder, but at times has also meant that a number of important/basic features have remained unimplemented by major firewall vendors, or the aforementioned features have been found to contain bugs.

This document aims to provide a ser of requirements for firewall vendors, which are specified as "MUST", "SHOULD", or "MAY". An IPv6 firewall product is said to be "fully-compliant" with this specification provided it implements all requirements marked as "MUST" and "SHOULD". An IPv6 firewall product is said to be "conditionally-compliant" with this specification provided it implements all requirements marked as "MUST", but fails to implement one or more of the requirements marked as "SHOULD".

3. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

4. General Security Features

REQ GEN-1:
MUST support basic Access Control Lists (ACLs).

REQ GEN-2:
MUST support both stateless and stateful packet inspection and filtering at transport layer.

REQ GEN-3:

MUST support full-proxy for the TCP [RFC0793] connections (the handshake is validated on the firewall before reaching the target system).

REQ GEN-4:
MUST be able to enforce timeouts on TCP connections based on specific protocols (e.g. enforce DNS timeout to a specific number of seconds, or FIN-WAIT, etc.). In general, it MUST have different kind of timeout values and thresholds to be used to prevent idle established connections to saturate resources on both the device and the service that is defended.

REQ GEN-5:
MUST be able to provide anti-spoofing features (e.g. uRPF).

REQ GEN-6:
MUST be able to redirect specific traffic to a proxy server e.g. for HTTP/S protocols.

REQ GEN-7:
MUST be able to detect and reject invalid source or destination addresses (e.g. local-link addresses that try to traverse the firewall) with a single policy.

5. IPv6-Specific Features

REQ SPC-1:
MUST be able to filter ICMPv6 [RFC4443] traffic at a message type/code granularity.

REQ SPC-2:
MUST be able to block IPv6 packets that employ a Routing Header (both at the granaularity of Extension Header Type and Routing Header Type).

REQ SPC-3:
MUST be able to detect IPv6 tunnels such as SIT, 6to4, 6in4, ISATAP and Teredo (please see [RFC7123], and must be able to selectively block or allow them for specific sources, destinations, routes or interfaces.

REQ SPC-4:
MUST be able to filter ICMPv6 traffic at a message type/code granularity.

REQ SPC-5:

MUST be able to validate IPv6 Neighbor Discovery [RFC4861] packets (RS, RA, NS, NA, Redirect) according to [I-D.ietf-opsec-ipv6-nd-security].

REQ SPC-6:
MUST be able to statefully match ICMPv6 errors to TCP [RFC0793], UDP [RFC0768], and ICMPv6 [RFC4443] communication instances.

REQ SPC-7:
MUST be able to find the upper-layer protocol in an IPv6 header chain (see [RFC7112].

6. VPN Security Requirements

REQ VPN-1:
MUST implement IPsec-based [RFC4301] VPN technology.

REQ VPN-2:
MUST implement "hub-and-spoke" Dynamic Multipoint VPN-like technology, allowing creation of dynamic-meshed VPN without having to preconfigure all of possible tunnels.

REQ VPN-3:
MUST implement SSL/TLS-based [SSL-VPNs] VPN technology.

REQ VPN-4:
MUST be able to use digital certificates, including CRL and OCSP revocation checking methods, to mutually authenticate VPN peers.

REQ VPN-5:
MUST be able to disable or enable split-tunnelling feature on VPN as required.

REQ VPN-5:
MUST support the enrollment of the system in a PKI infrastructure for the regular renewal of certificates.

REQ VPN-6:
MUST be able to work indifferently on IPv4 and IPv6, and also offer both protocol in dual-stack in the same VPN connection.

REQ VPN-7:
MUST be able to apply to the tunnelled content that is terminated on the device, the same inspection policies that are possible in the non tunnelled traffic.

7. Denial of Service (DoS) Protection

REQ DoS-1:
MUST be able to protect against OS-specific attacks: nuke, ping-of-death (NOTE: this list should be expanded, and references added).

REQ DoS-2:
MUST be able to protect against IPv6 resource exhaustion attacks (e.g., fragment flooding attacks).

REQ DoS-3:
MUST be able to protect against TCP flooding attacks: connection-flooding, FIN-WAIT-1 flooding, etc. (see e.g. [CPNI-TCP])

REQ DoS-4:
MUST be able to protect against TCP resource exhaustion attacks: zero-window attacks, SYN-floods, etc. (see e.g. [CPNI-TCP])

REQ DoS-5:
MUST be able to detect and drop malformed IPv6 packets (incorrect header/option lengths, etc.).

REQ DoS-6:
MUST be able to detect and drop malformed TCP packets (incorrect segment/options lengths, etc.).

REQ DoS-7:
MUST be able to provide bandwidth management (QoS or anti-flooding) policies customisable for specific source and destination networks, or by VLAN or MPLS ID.

REQ DoS-8:
MUST be able to participate to a blackhole/sync hole routing infrastructure as per [RFC5635].

REQ DoS-9:
MUST be able to set up a maximum session setup rate, and detect hosts or networks exceeding it.

REQ DoS-10:
MUST be able to set up a maximum IPv6 source and/or destination session limit, and detect when they are exceeded.

REQ DoS-11:
For each of the previous detection controls, different configurable reactions SHOULD be possible by IPv6 address and

network sources and/or destinations. The minimum actions required are the following:

1. allow the traffic ("ignore" or "whitelist")

2. allow the traffic but log ("bypass" or "detection only" mode)

3. drop the packet (only the offending packet but do not reset

the connection)

4. drop session (drop the entire connection, but do not send a reset back)

5. "greylist" - put it in a list of blocked addresses, but remove it from the list after a configurable amount of time

6. send an email/SMS/pager text to administrator

7. send TCP reset to source only

8. send TCP reset to destination only

9. send TCP reset to both source and destination

10. perform a specific, preconfigured change on the firewall policy

11. feed a third party source such as a switch/NAC/NAP or RADIUS system, to isolate/quarantine the offending port/MAC address/ user

12. quarantine the specific traffic or source (block them for a configurable amount of time, e.g. 5 minutes, and then allow them again; eventually, the quarantine time may get longer if the offense is repeated)

8. Application Layer Firewall

REQ APP-1:
MUST be able to provide web filtering features, such as enforcing access to allowed web content and filtering high risk URLs such as anonymizers and known hostile addresses.

REQ APP-2:
MUST be able to provide email filtering features, such as mitigating spam, phishing and email harvesting, and enforce email policies.

9. Logging, Auditing and Group Security Operation Centre (GSOC)

requirements

REQ GSOC-1:
MUST generate log for all the changes performed to the system, including change of group membership for a device, new or removed devices in a group, new or removed administrators.

REQ GSOC-2:
MUST provide the following features:

1. Connection logs
2. Local log storage
3. Network logging
4. Real time log viewer
5. Attack detected
6. Per rule logging
7. Automatic log file compression
8. Log file rotation

REQ GSOC-3:
MUST be able to generate a log for:

1. all the logins, logouts and failed login attempts from administrators
2. any modifications or disabling of the firewall rules

REQ GSOC-4:
Any security event detected - malicious traffic, hit of a policy, policy violation, termination of a session and so on - MUST be able to generate a log, and be configurable to do that or not by administrators.

REQ GSOC-5:
There MUST be a mechanism to prevent log flooding from the device against the management system, such as aggregation of like events.

REQ GSOC-6:
The amount of information in the alerts MUST be configurable; it SHOULD possible to have the date/time and type of event and the

full payload of the traffic that has triggered the signature/ event.

REQ GSOC-7:
The firewall MUST minimise the number of log entries generated for a single event - e.g. when repeated similar events for a short period of time are detected, they are aggregated and the cumulative number of events is reported.

REQ GSOC-8:
The firewall MUST be able to send logs in multiple ways and formats, for instance UDP syslog, TCP syslog, SMTP, SNMP and so on. It must be possible to configure different ways and formats for different policies and configure some ways and formats as a "backup" in the case that the main way fails. Please describe the different possibilities.

10. Console and Events Visualisation requirements

REQ CON-1:
MUST provide a dashboard view, which must be customisable by user and users' group.

REQ CON-2:
The dashboard must be able to include system health monitoring information, such as the following:

1. CPU idle
2. Real and Swap memory usage
3. Disk usage
4. Number of accepted and dropped packets
5. Operating status for all supported facilities (HA, QoS, VPN)
6. VPN tunnels status
7. NIC link state

REQ CON-3:
MUST have the possibility to select a particular piece of data or individual alert, and visualise the policy that has triggered the event.

REQ CON-4:

MUST be able to create exception filters that will suppress visualisation of a specific alert (e.g. from specific sources, or specific events), without actually affecting the detection and log retention.

11. Reporting requirements

REQ REP-1:
Built in reports MUST be provided by default, such as protocol distribution, policy and rule matched, top attacks, top sources/ destinations, top targets, top geographical sources, device status including utilisations, and so on.

REQ REP-2:
MUST allow to run reporting over historical and archived logs, automatically restoring and rearchiving them.

12. IANA Considerations

There are no IANA registries within this document. The RFC-Editor can remove this section before publication of this document as an RFC.

13. Security Considerations

[TBD]

14. Acknowledgements

This initial version is based on an earier document authored by Marco Ermini.

15. References

15.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2460] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, December 1998.

[RFC4301] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, December 2005.

[RFC4443] Conta, A., Deering, S., and M. Gupta, "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification", RFC 4443, March 2006.

[RFC4861] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)", RFC 4861, September 2007.

[RFC0768] Postel, J., "User Datagram Protocol", STD 6, RFC 768, August 1980.

[RFC0793] Postel, J., "Transmission Control Protocol", STD 7, RFC 793, September 1981.

[RFC7112] Gont, F., Manral, V., and R. Bonica, "Implications of Oversized IPv6 Header Chains", RFC 7112, January 2014.

15.2. Informative References

[RFC7123] Gont, F. and W. Liu, "Security Implications of IPv6 on IPv4 Networks", RFC 7123, February 2014.

[RFC7126] Gont, F., Atkinson, R., and C. Pignataro, "Recommendations on Filtering of IPv4 Packets Containing IPv4 Options", BCP 186, RFC 7126, February 2014.

[RFC5635] Kumari, W. and D. McPherson, "Remote Triggered Black Hole Filtering with Unicast Reverse Path Forwarding (uRPF)", RFC 5635, August 2009.

[I-D.ietf-opsec-ipv6-nd-security] Gont, F., Bonica, R., and W. Will, "Security Assessment of Neighbor Discovery (ND) for IPv6", draft-ietf-opsec-ipv6-nd-security-00 (work in progress), October 2013.

[RFC6274] Gont, F., "Security Assessment of the Internet Protocol

Version 4", RFC 6274, July 2011.

[CPNI-TCP]
CPNI, , "Security Assessment of the Transmission Control Protocol (TCP)", http://www.gont.com.ar/papers/tn-03-09-security-assessment-TCP.pdf, 2009.

[SSL-VPNs]
Hoffman, P., "SSL VPNs: An IETF Perspective", IETF 72, SAAG Meeting., 2008, <http://www.ietf.org/proceedings/72/slides/saag-4.pdf>.

Authors' Addresses

Fernando Gont
SI6 Networks / UTN-FRH
Evaristo Carriego 2644
Haedo, Provincia de Buenos Aires 1706
Argentina

Phone: +54 11 4650 8472
Email: fgont@si6networks.com
URI: http://www.si6networks.com

Marco Ermini
ResMed
Fraunhoferstrasse 16
Munich, Bayern 82152
Deutschland

Phone: +49 175 4395642
Email: marco.ermini@resmed.com
URI: http://www.resmed.com

Will Liu

Huawei Technologies
Bantian, Longgang District
Shenzhen 518129
P.R. China

Email: liushucheng@huawei.com