[Airbus Amber]

Network Packet Filtering Revision for A858P1S1

Timo Warns

AIRBUS

Overview

- Egress and ingress filtering - proposal for PP858 update
- Stateful vs. stateless filtering - no update
- Additional filtering criteria
  - Application knowledge - no update
  - ROHC - no update
  - RFC 4890 “Recommendations for Filtering ICMPv6 Messages in Firewalls” - proposal for PP858 update
  - RFC 9099 “Operational Security Considerations for IPv6 Networks” - proposal for PP858 update

Ingress and Egress Filtering

4.3.2.1 Packet Filtering

Packet filtering at Layer 3 is the process of controlling traffic to/from the Airborne IPS System by monitoring all incoming or outgoing packets and allowing only those packets that comply with predefined security policies. The filtering functions described in the following sub-sections may be implemented via one or more firewall applications.

The Airborne IPS System shall perform both, ingress and egress filtering on air-ground interfaces as well as interfaces with other avionics. With ingress filtering, the Airborne IPS System validates the IP source address of an incoming IP packet against the interface on which the packet was received. For example, the system should not accept packets that are incoming on an air-ground interface with a source IP allocated to the aircraft itself. Ingress filtering helps to ensure that only legitimate IPS traffic is allowed to enter preventing some denial-of-service and IP spoofing attacks.

With egress filtering, the Airborne IPS System validates the IP source address of an outgoing IP packet. For example, the system should not accept packets that are outgoing on an air-ground interface with a source IP not allocated to the aircraft itself. Egress filtering helps to ensure that only legitimate traffic is allowed to leave preventing attacks on the ground or on native IP applications. Note that, for the Airborne IPS System case, there may not be a clear delineation between ingress and egress filtering. For example, rejecting packets to ground from a native IP application with a source address not allocated to the aircraft may be considered ingress or egress filtering depending on perspective.

RFC 4890 “Recommendations for Filtering ICMPv6 Messages in Firewalls”

In networks supporting IPv6, the Internet Control Message Protocol version 6 (ICMPv6) plays a fundamental role with a large number of functions, and a correspondingly large number of message types and options. ICMPv6 is essential to the functioning of IPv6, but **there are a number of security risks associated with uncontrolled forwarding of ICMPv6 messages.** Filtering strategies designed for the corresponding protocol, ICMP, in IPv4 networks are not directly applicable, because these strategies are intended to accommodate a useful auxiliary protocol that may not be required for correct functioning.

This document provides some recommendations for ICMPv6 firewall filter configuration that will allow propagation of ICMPv6 messages that are needed to maintain the functioning of the network but drop messages that are potential security risks. [...]

This section suggests some common considerations that should be borne in mind when designing filtering rules and then categorizes the rules for each class. The categories are:

- **Messages that must not be dropped**: usually because establishment or maintenance of communications will be prevented or severely impacted.
- **Messages that should not be dropped**: administrators need to have a very good reason for dropping this category.
- **Messages that may be dropped in firewall/routers**, but these messages may already be targeted to drop for other reasons (e.g., because they are using link-local addresses) or because the protocol specification would cause the messages to be rejected if they had passed through a router. Special considerations apply to transit traffic if the firewall is not a router as discussed in Section 4.2.
- **Messages that administrators may or may not want to drop depending on local policy**.
- **Messages that administrators should consider dropping** (e.g., ICMP node information name lookup queries).

Proposal for ARINC 858 Update on RFC 4890

IPv6 Filtering

The Airborne IPS System shall implement IPv6 packet filtering of all IPS dataflows. The IPv6 filtering implementation should be configurable to filter by the following items, as a minimum:

- Source and destination IPv6 addresses (e.g., allow only specified global-unique or care-of-addresses)
- Payload length (e.g., allow only if the payload length in the IPv6 header matches the actual payload data length)
- Next Header type (e.g., allow only if ICMP, UDP, or TCP (if enabled)),
- ICMPv6 (e.g., allow only supported packets per the IPS Profiles in RTCA DO-379 and EUROCAE ED-262; additional guidance for filtering ICMPv6 is available in RFC 4890)
- IPv6 Extension Headers (e.g., allow only supported extension headers, per the IPS Profiles in RTCA DO-379 and EUROCAE ED-262)

RFC 9099 “Operational Security Considerations for IPv6 Networks”

Knowledge and experience on how to operate IPv4 networks securely is available, whether the operator is an Internet Service Provider (ISP) or an enterprise internal network. However, IPv6 presents some new security challenges. RFC 4942 describes security issues in the protocol, but network managers also need a more practical, operations-minded document to enumerate advantages and/or disadvantages of certain choices.

This document analyzes the operational security issues associated with several types of networks and proposes technical and procedural mitigation techniques. This document is only applicable to managed networks, such as enterprise networks, service provider networks, or managed residential networks.

2. Generic Security Considerations
2.1. Addressing
2.2. Extension Headers
2.3. Link-Layer Security
2.4. Control Plane Security
2.5. Routing Security
2.6. Logging/Monitoring
2.7. Transition/Coexistence Technologies
2.8. General Device Hardening

3. Enterprises-Specific Security Considerations

4. Service Provider Security Considerations
4.1. BGP
4.2. Transition/Coexistence Mechanism
4.3. Lawful Intercept

5. Residential Users Security Considerations

RFC 9099, Section 2.2 “Extension Headers”

2.2. Extension Headers [...]
A clarification on how intermediate nodes should handle packets with existing or future extension headers is found in [RFC7045]. [...] Sections 5.2 and 5.3 of [RFC8504] provide more information on the processing of extension headers by IPv6 nodes.

Vendors of filtering solutions and operations personnel responsible for implementing packet filtering rules should be aware that the 'Next Header' field in an IPv6 header can both point to an IPv6 extension header or to an upper-layer protocol header. This has to be considered when designing the user interface of filtering solutions or during the creation of filtering rule sets.

[IPV6-EH-FILTERING] discusses filtering rules for those extension headers at transit routers.

2.2.1. Order and Repetition of Extension Headers [...]

A firewall or edge device should be used to enforce the recommended order and the maximum occurrences of extension headers by dropping nonconforming packets.

2.2.3. Fragment Header [...]
Firewall and security devices should drop first fragments that do not contain the entire IPv6 header chain (including the transport-layer header). Destination nodes should discard first fragments that do not contain the entire IPv6 header chain (including the transport-layer header). If those requirements are not met, stateless filtering could be bypassed by a hostile party.

Proposal for ARINC 858 Update on RFC 9099

IPv6 Filtering

The Airborne IPS System shall implement IPv6 packet filtering of all IPS dataflows. The IPv6 filtering implementation should be configurable to filter by the following items, as a minimum:

- Source and destination IPv6 addresses (e.g., allow only specified global-unique or care-of-addresses)
- Payload length (e.g., allow only if the payload length in the IPv6 header matches the actual payload data length)
- Next Header type (e.g., allow only if ICMP, UDP, or TCP (if enabled)),
- ICMPv6 (e.g., allow only supported packets per the IPS Profiles in RTCA DO-379 and EUROCAE ED-262; additional guidance is available in RFC 4890)
- IPv6 Extension Headers (e.g., allow only supported extension headers, per the IPS Profiles in RTCA DO-379 and EUROCAE ED-262; drop packets with non-conforming order or number of extension headers)

Implementers are recommended to consider RFC 9099 for further guidance on defining appropriate filter rules.

Thank you

AIRBUS