DornerWorks, Ltd.
Technology Solutions Delivered

3445 Lake Eastbrook Blvd. SE
Grand Rapids, MI 49546
616.245.8369
www.DornerWorks.com

High Level Requirements

C_ROCKWELL_COLLINS-INSPECTA

18 NOVEMBER 2025

Table of Contents

1.0 RX_Firewall

1.1 Rx_firewall: Copy through any ARP frame to VMM output (*RC_INSPECTA_00-HLR-5*)))

The RX firewall shall copy a frame from an input port to its VMM output port if that frame has a wellformed ethheader, the ethernet type is ARP, and the ARP packet is wellformed.

- An ethernet header is wellformed if the ethernet type is valid and the destination address is valid.
    - The ethernet type is valid if bytes 12-13 of the frame are 0x0800 or 0x0806 or 0x86DD.
    - The destination address is valid if bytes 0-5 of the frame are not 0x0000000000.
- An ethernet type is ARP if bytes 12-13 of the frame are 0x0806.
- An ARP packet is wellformed if the ARP Operation is valid and the ARP hardware type is valid and the ARP protocol type is valid.
    - The ARP Operation is valid if bytes 20-21 of the frame are 0x0001 or 0x0002.
    - The ARP hardware type is valid if bytes 14-15 of the frame are 0x0001.
    - The ARP protocol type is valid if bytes 16-17 of the frame are 0x0800 or 0x86DD.

1.2 Rx_firewall: Copy through allowed UDP port frames to VMM output (*RC_INSPECTA_00-HLR-13*)))

The RX firewall shall copy a frame from an input port to its VMM output port's message if that frame has a wellformed ethheader, the ethernet type is IPv4, the IPv4 packet is wellformed, the IPv4 packet uses the UDP protocol, the UDP source port is not from GCS , and the UDP destination port is in the UDP port whitelist.

- An ethernet header is wellformed if the ethernet type is valid and the destination address is valid.
    - The ethernet type is valid if bytes 12-13 of the frame are 0x0800 or 0x0806 or 0x86DD.
    - The destination address is valid if bytes 0-5 of the frame are not 0x0000000000.
- An IPv4 packet is wellformed if the IPv4 protocol is valid, the version is 4, the IHL indicates no IPv4 options in the header, and the IPv4 length is valid.
    - The IPv4 protocol is valid if byte 23 of the frame is 0x00 or 0x01 or 0x02 or 0x06 or 0x11 or 0x2B or 0x2C or 0x3A or 0x3B or 0x3C.
    - The IPv4 length is valid if bytes 16-17 of the frame are <= 9000.
    - The IPv4 version is 4 and the IHL indicates no IPv4 options in the header if byte 14 is 0x45.
- An IPv4 packet uses the UDP protocol if byte 23 of the frame is 0x11.
- The UDP source port is not from a GCS if it is not 14550.

- The UDP destination port is in the whitelist if bytes 36-37 of the frame are one of the following:
    - [68]

A maximum IPv4 length of 9000 is selected since it is the standard JUMBO frame size for Maximum Transmission Unit (MTU). In most cases it will be closer to 1500.

1.3 Rx_firewall: Copy through mavlink UDP port frames to the mavlink_firewall output (*RC_INSPECTA_00-HLR-18*))

The RX firewall shall copy a frame from an input port to its mavlink_firewall output port's message if that frame has a wellformed ethheader, the ethernet type is IPv4, the IPv4 packet is wellformed, the IPv4 packet uses the UDP protocol, and the UDP source port is 14550.

- An ethernet header is wellformed if the ethernet type is valid and the destination address is valid.
    - The ethernet type is valid if bytes 12-13 of the frame are 0x0800 or 0x0806 or 0x86DD.
    - The destination address is valid if bytes 0-5 of the frame are not 0x0000000000.
- An IPv4 packet is wellformed if the IPv4 protocol is valid, the version is 4, the IHL indicates no IPv4 options in the header, and the IPv4 length is valid.
    - The IPv4 protocol is valid if byte 23 of the frame is 0x00 or 0x01 or 0x02 or 0x06 or 0x11 or 0x2B or 0x2C or 0x3A or 0x3B or 0x3C.
    - The IPv4 length is valid if bytes 16-17 of the frame are <= 9000.
    - The IPv4 version is 4 and the IHL indicates no IPv4 options in the header if byte 14 is 0x45.
- An IPv4 packet uses the UDP protocol if byte 23 of the frame is 0x11.
- The UDP packet contains a mavlink payload if the UDP source port (bytes 34-35) is 14550.

  A maximum IPv4 length of 9000 is selected since it is the standard JUMBO frame size for Maximum Transmission Unit (MTU). In most cases it will be closer to 1500.

1.4 Rx_firewall: Do not copy disallowed frame (*RC_INSPECTA_00-HLR-15*))

The RX firewall shall not copy any frame originating from an input port to any of its output ports if it does not match a valid frame as defined in the other HLRs.

1.5 Rx_firewall: No output on empty input (*RC_INSPECTA_00-HLR-17*))

The RX firewall shall not place any data in any output port when its corresponding input port does not have any data available.

2.0TX_Firewall

2.1 Tx_firewall: Copy through any ARP frame (*RC_INSPECTA_00-HLR-7*))

The TX firewall shall copy a frame from an input port to its output port's message if that frame has a wellformed ethheader, the ethernet type is ARP, and the ARP packet is wellformed. A size of 64 is provided in the output port's size.

- An ethernet header is wellformed if the ethernet type is valid and the destination address is valid.
    - The ethernet type is valid if bytes 12-13 of the frame are 0x0800 or 0x0806 or 0x86DD.
    - The destination address is valid if bytes 0-5 of the frame are not 0x0000000000.
- An ethernet type is ARP if bytes 12-13 of the frame are 0x0806.
- An ARP packet is wellformed if the ARP Operation is valid and the ARP hardware type is valid and the ARP protocol type is valid.
    - The ARP Operation is valid if bytes 20-21 of the frame are 0x0001 or 0x0002.
    - The ARP hardware type is valid if bytes 14-15 of the frame are 0x0001.
    - The ARP protocol type is valid if bytes 16-17 of the frame are 0x0800 or 0x86DD.

2.2 Tx_firewall: Copy through any IPv4 frame (*RC_INSPECTA_00-HLR-12*))

The TX firewall shall copy a frame from an input port to its output port's message if that frame has a wellformed ethheader, the ethernet type is IPv4, and the IPv4 packet is wellformed. The sum of the total size provided by the IPv4 header and the 14 bytes of the ethernet header is provided in the output port's size.

- An ethernet header is wellformed if the ethernet type is valid and the destination address is valid.
    - The ethernet type is valid if bytes 12-13 of the frame are 0x0800 or 0x0806 or 0x86DD.
    - The destination address is valid if bytes 0-5 of the frame are not 0x0000000000.
- An ethernet type is IPv4 if bytes 12-13 of the frame are 0x0800.
- An IPv4 packet is wellformed if the IPv4 protocol is valid, the version is 4, the IHL indicates no IPv4 options in the header, and the IPv4 length is valid.
    - The IPv4 protocol is valid if byte 23 of the frame is 0x00 or 0x01 or 0x02 or 0x06 or 0x11 or 0x2B or 0x2C or 0x3A or 0x3B or 0x3C.
    - The IPv4 length is valid if bytes 16-17 of the frame are <= 9000.
    - The IPv4 version is 4 and the IHL indicates no IPv4 options in the header if byte 14 is 0x45.

A maximum IPv4 length of 9000 is selected since it is the standard JUMBO frame size for Maximum Transmission Unit (MTU). In most cases it will be closer to 1500.

2.3 Tx_firewall: Do not copy disallowed frame (*RC_INSPECTA_00-HLR-14*)))

The TX firewall shall not copy any frame originating from an input port to its output port if it does not match a valid copy frame as defined in other HLRs.

2.4 Tx_firewall: No output on empty input (*RC_INSPECTA_00-HLR-16*)))

The TX firewall shall not place any data in an output port when its corresponding input port does not have any data available.

3.0 Mavlink_Firewall

3.1 Mavlink_Firewall: Drop flash_bootloader mav_command message (*RC_INSPECTA_00-HLR-19*)))

The Mavlink firewall shall drop a frame from an input port if the mavlink message of the payload has a message id of CommandInt or CommandLong and the message payload's command is MAV_CMD_FLASH_BOOTLOADER.

- The mavlink protocol is v2 if byte 0 is 0xFD
  - The mavlink message, bytes 7-9, has the ID of CommandInt: 75
    - The message payload's mav command, bytes 13-14, has MAV_CMD_FLASH_BOOTLOADER: 42650

OR

- The mavlink protocol is v2 if byte 0 is 0xFD
  - The mavlink message, bytes 7-9, has the ID of CommandLong: 76
    - The message payload's mav command, bytes 12-13, has MAV_CMD_FLASH_BOOTLOADER: 42650

OR

- The mavlink protocol is v1 if byte 0 is 0xFE
  - The mavlink message, byte 5, has the ID of CommandInt: 75
    - The message payload's mav command, bytes 9-10, has MAV_CMD_FLASH_BOOTLOADER: 42650

OR

- The mavlink protocol is v1 if byte 0 is 0xFE
  - The mavlink message, byte 5, has the ID of CommandLong: 76

- The message payload's mav command, bytes 8-9, has MAV_CMD_FLASH_BOOTLOADER: 42650

3.2 Mavlink_Firewall: Drop malformed mavlink messages (*RC_INSPECTA_00-HLR-20*))

The Mavlink firewall shall drop an input frame if the mavlink message of the payload is malformed.

3.3 Mavlink_firewall: No output on empty input (*RC_INSPECTA_00-HLR-21*)))

The Mavlink firewall shall not place any data in an output port when its corresponding input port does not have any data available.

3.4 Mavlink_Firewall: Copy through well-formed, not-blacklisted messages (*RC_INSPECTA_00-HLR-22*))

The Mavlink firewall shall copy through a mavlink message from an input port to its corresponding output port if it is well-formed and it is not in the blacklist.