

RADIUS Duplicate packet from NAS

Contents

- 1 Overview
- 2 Prerequisites
- 3 Symptoms
- 4 Solution
 - ◆ 4.1 External interface blocking rule
 - ◆ 4.2 Group Authentication requests
 - ◆ 4.3 Authentication failure
 - ◆ 4.4 Response sent on differing IP address to receiving IP address

Overview

RADIUS duplicate packets are seen, user authentication may succeed or fail.

Prerequisites

PINsafe 3.x

Access device using RADIUS authentication

Symptoms

log message seen **PACKET DROPPED - Duplicate packet from NAS**

User authentication may succeed or fail

Solution

INFO RADIUS: <0> Access-Request(1) LEN=78 192.168.1.1:4175 PACKET DROPPED - Duplicate packet from NAS

This can be caused by the following:

External interface blocking rule

If the PINsafe server sends the reply but it is not received by the access device, the access device may try to resend the RADIUS request. This can be caused by the Access device sending a RADIUS request from an external interface, but not accepting the response through that external interface.

Group Authentication requests

Some access devices may make additional RADIUS requests for group membership checks.

Authentication failure

When an authentication fails the RADIUS client may retry sending additional authentication requests. Resolve the initial issue causing the failure.

Response sent on differing IP address to receiving IP address

If a PINsafe Virtual IP (VIP) address is used the RADIUS request may be made against the PINsafe VIP, but the RADIUS response may be sent from the real IP address of the PINsafe server, and be blocked by the access device due to IP spoofing rules, even though the PINsafe authentication has succeeded and a authentication succeeded message sent. Duplicate packets may be then seen, as the access device has not seen a response from the PINsafe server, so repeats the authentication.

Example

INFO RADIUS: <0> Access-Request(1) LEN=68 192.168.1.1:53225 PACKET DROPPED - Duplicate packet from NAS 192.168.1.2:53225 PacketId 0

INFO RADIUS: <0> Access-Request(1) LEN=68 192.168.1.1:53225 PACKET DROPPED - Duplicate packet from NAS 192.168.1.2:53225 PacketId 0

INFO RADIUS: <0> Access-Accept(2) LEN=68 192.168.1.1:53225 Access-Request by testuser succeeded

This can be resolved by using the real IP address of the PINsafe server for the RADIUS request rather than the VIP, but may impact the solution in place:

- Standalone: not affected
- Active/Passive: not affected. Only one instance of Tomcat is running, and the PINsafe RADIUS server is given the IP address of the VIP, and responds on the VIP, so does not cause an issue.
- Active/Active using dual channel only: not affected. The real IP address of the PINsafe server can be used and not the VIP.

- Active/Active with VIP and **session Sharing**: not affected. The real IP address of the PINsafe server can be used for RADIUS requests. Single channel image requests are shared so can be requested from shared server.
- Active/Active with VIP and single channel image requests, without **session Sharing**: **affected**. Single channel image requests are not being shared so the RADIUS authentication request must be made against the same server. To resolve this, use ecache, if this is not possible then use an external HA solution to route traffic.