RADIUS Proxy How to guide

Contents

- 1 Overview
- 2 Prerequisites
- 3 Architecture
- 4 RADIUS Proxy Setup
    - 4.1 RADIUS Server Configuration
    - 4.2 RADIUS NAS Configuration
    - 4.3 Configure the RADIUS Proxy
        - 4.3.1 PINsafe RADIUS Proxy Options
    - 4.4 Testing
    - 4.5 Known Issues
    - 4.6 Troubleshooting
        - 4.6.1 Error Messages

Overview

This document outlines how to configure the RADIUS Proxy functionality of PINsafe. For information relating to RADIUS configuration see RADIUS How To Guide. The PINsafe RADIUS proxy has cyclical loop prevention to prevent RADIUS requests being continuually bounced between two RADIUS servers.

Prerequisites

PINsafe 3.7 onwards

PINsafe 3.8 onwards for Single Channel Session Proxy

Architecture

A PINsafe server can be a RADIUS Client to another RADIUS server, this may be a PINsafe server, requesting authentication information from that server.

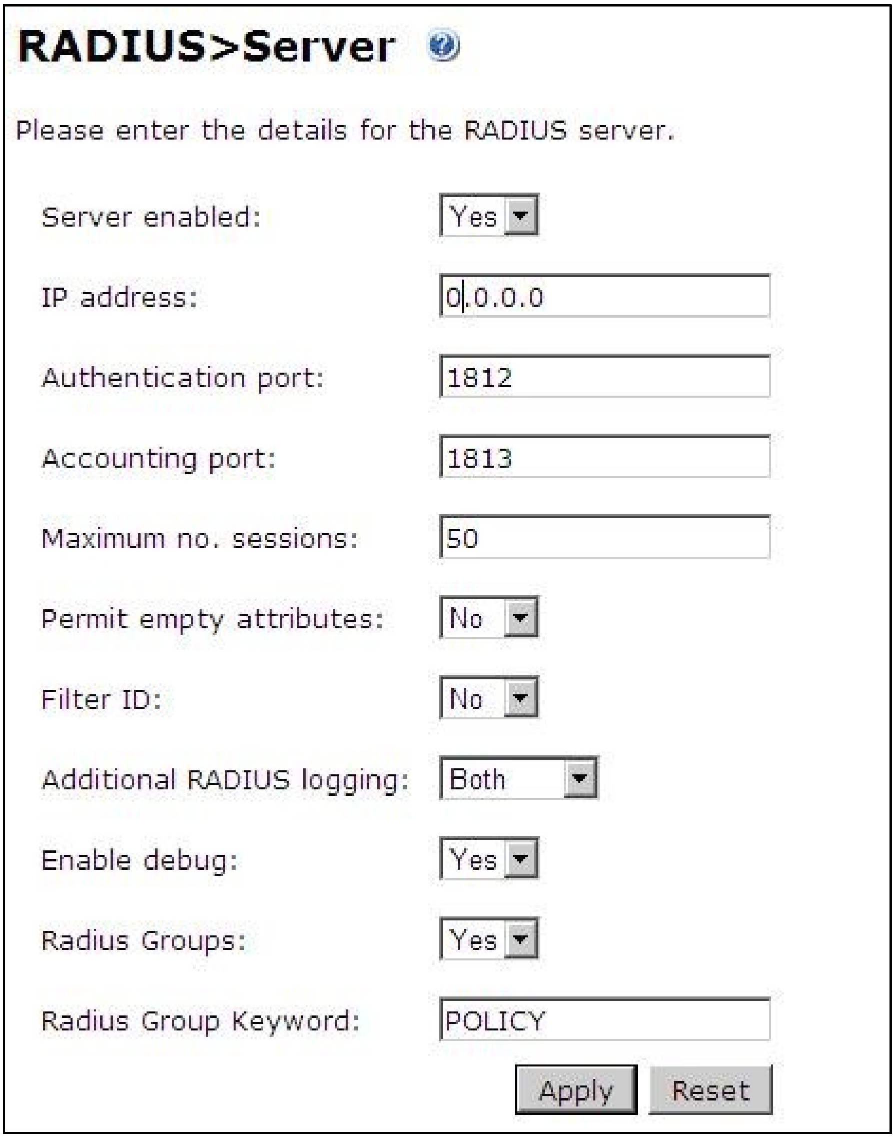
RADIUS Proxy Setup

RADIUS Server Configuration

If the remote RADIUS server is not a PINsafe RADIUS server, follow the vendor documentation for setting up and configuring the RADIUS server.

If the remote RADIUS server is a PINsafe server, configure that PINsafe server with the following. On each instance of PINsafe to be used as a RADIUS server, on the PINsafe Administration console select RADIUS/Server. Ensure Server enabled is set to yes. Leave the IP address field blank unless you wish to explicitly enter the IP address to be used for RADIUS requests (the physical IP address, but not the virtual IP if using a PINsafe HA Pair). Using a blank value or 0.0.0.0 means that the server will answer all RADIUS requests received by the server regardless of the IP address that they were sent to.

Note: for appliances, the PINsafe VIP should not be used as the server IP address, see VIP on PINsafe Appliances



RADIUS>Server

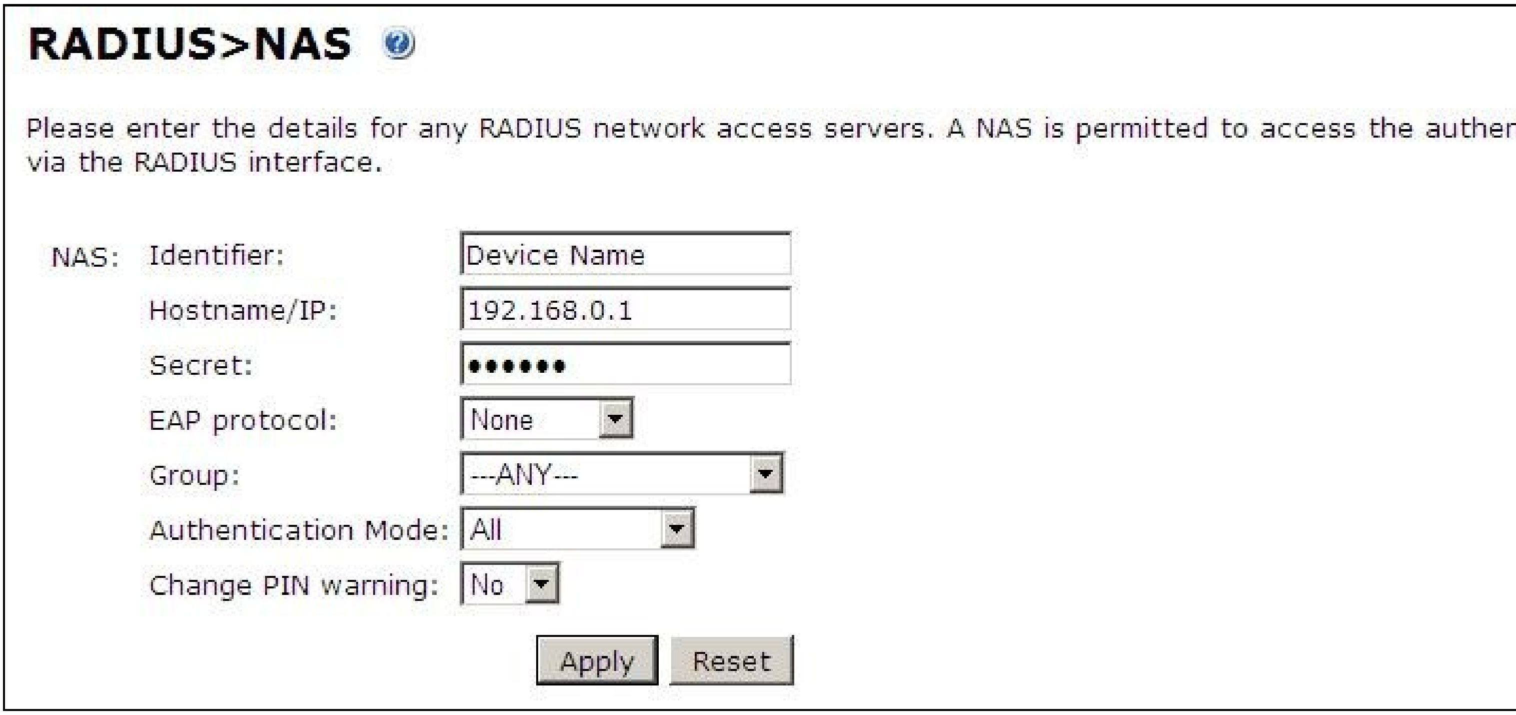
Please enter the details for the RADIUS server.

Server enabled:	Yes
IP address:	0.0.0.0
Authentication port:	1812
Accounting port:	1813
Maximum no. sessions:	50
Permit empty attributes:	No
Filter ID:	No
Additional RADIUS logging:	Both
Enable debug:	Yes
Radius Groups:	Yes
Radius Group Keyword:	POLICY

RADIUS NAS Configuration

Set up the NAS using the Network Access Servers page in the PINsafe Administration console under RADIUS/NAS. In this case the remote PINsafe server will be the client to the PINsafe server being configured. Create a New Entry and enter a descriptive name and IP address for the other instances of PINsafe that will connect for RADIUS information. The secret assigned will be used on both the PINsafe RADIUS server, and the PINsafe RADIUS Proxy.

Note: If Check Password with repository is configured on the PINsafe appliance making the RADIUS request, then the PINsafe Proxy receiving the request needs to have Check Password with repository enabled, from PINsafe 3.7 onwards this is on the NAS entry.


RADIUS>NAS

Please enter the details for any RADIUS network access servers. A NAS is permitted to access the auther
via the RADIUS interface.

NAS: Identifier: Device Name

Hostname/IP: 192.168.0.1

Secret: ●●●●●●

EAP protocol: None

Group: ---ANY---

Authentication Mode: All

Change PIN warning: No

Configure the RADIUS Proxy

On the PINsafe instance that will be the RADIUS client, configure it to talk to the remote RADIUS server. On the PINsafe Administration console select Servers/Proxy. Enter a name for the RADIUS server, IP address or hostname, RADIUS authentication port, shared secret that is entered under the RADIUS NAS, and for RADIUS Proxy the conditions that should be met to proxy the request. See the RADIUS Proxy options below.

PINsafe RADIUS Proxy Options

PINsafe 3.7 onwards can proxy RADIUS requests against other RADIUS servers. This allows PINsafe to be inserted into an existing RADIUS infrastructure such as where tokens are being used, so such solutions can be used in parallel.

The RADIUS proxy is set on the PINsafe Administration Console under Server/Peers

The RADIUS proxy functions in the following manner.

Peers: Name: Descriptive Name used for logging information

Hostname/IP: Hostname/IP address of RADIUS server to be proxied against

HTTP port: Default: 8080. Not used in RADIUS Proxy

SSL: Options: Yes/No, Default: No. Not used in RADIUS Proxy

Context: Default: pinsafe. Not used in RADIUS Proxy

RADIUS authentication port: Authentication port to be used for RADIUS server to be proxied against. Usually 1812 or 1645

RADIUS accounting port: Accounting port to be used for RADIUS server to be proxied against. Usually 1813 or 1646

Shared secret: A shared secret which must be the same as that entered on the RADIUS server to be proxied against.

RADIUS Proxy: Options Never/On Passcode/Unknown User. Default: Never. How to handle the RADIUS password that the PINsafe server receives and if it should be proxied, the options for this are:

- Never: No Proxy request is made.
- Unknown User: If the user is not in the PINsafe Database then a proxy request is made.
- On Passcode: If it sees that the user has submitted a one-time code that is at least 6 characters long and that the user: Either (a) does not have an account: Or (b) has an account but has not started a session (eg requested a TURing image or on-demand SMS) then it is treated as a third party code and passed to another RADIUS server.
- No User Session: Available in PINsafe 3.8 onwards. PINsafe can proxy RADIUS requests purely in the absence of a local session for the user making the RADIUS request. Both single channel image requests and dual channel on demand session requests can be used for this entry.

Testing

RADIUS messages should be seen in the Swivel logs

Access Request(1) LEN=192.168.1.1:1025 PROXY REQUEST to Swivel-Primary (/192.168.1.1)

Known Issues

Troubleshooting

Check the Swivel logs.

Some access devices such as the Cisco ASA have a RADIUS test tool

It may be useful to use tcpdump for troubleshooting from the command line

tcpdump -i eth0 port 1812

Check that RADIUS is listening using *netstat -a*

Error Messages

Access Request(1) LEN=192.168.1.2:1025 PACKET DROPPED - Access-Request by username REQUEST PACKET FAILED PROXY VALIDATION AccessDropException: PROXYING to Swivel-Standby FAILED - No such proxy target.

There is a problem connecting to the proxy server. On the Swivel Administration console under RADIUS/Server Stop RADIUS, then Start RADIUS. Check the logs for any error messages, such as RADIUS port cannot be bound or is already in use, if so restart Tomcat and check again.

Access Request(1) LEN=192.168.1.2:1025 PACKET DROPPED - Access-Request by username REQUEST PACKET FAILED PROXY VALIDATION AccessDropException: Packet DROPPED - Proxy target is in a Proxy Loop (Configuration error).

There is a loop whereby each RADIUS server requests RADIUS information from the other. This error usually can be ignored.