Single Channel Session Cache

PINsafe Security String Session Cache

Session Cache

Contents

Introduction

From version 3.9.5 onwards, Session sharing is included as part of Appliance Synchronisation which supercedes the Single Channel Session Cache and session Sharing. The Single Channel session cache should be disabled if the Appliance Synchronisation is to be used. Appliance Synchronisation and Session sharing are not enabled by default. See Also Session Sharing

PINsafe version 3.5 or newer has the facility to use session caching. The session cache allows security strings generated on one appliance to be communicated to other PINsafe appliances on the same network. Session Caching uses multicast to communicate the generated strings. The benefit of session caching is to allow all PINsafe appliances to be aware of all issued security strings. This is particularly important in Active/Active HA environments and SMS authentication. Active/Passive environments would not require session sharing.

The instructions contained in this document have been tested on a V2.x appliance. If you find that they are not applicable to your appliance, please contact Swivel Secure support (support@swivelsecure.com) for assistance.

It is assumed that the appliance is already configured, and has a valid IP address on your network.

Please Note: Session cache traffic is designed to go over the trusted interface, this interface would be the 2nd NIC using a cross over cable or a dedicated LAN/VLAN that allows multicast traffic.

Swivel Multicast is configured using the RFC implementation with Multicast and IGMP joins for a specific group or groups.

Note also that PINsafe RADIUS Proxy may also be used in PINsafe 3.8 onwards as an alternative to Session Sharing.

Pre-requisites

PINsafe 3.5 onwards

multicast enabled between pair of PINsafe appliances using the primary interface (ETH0 on PINsafe appliances)

Enabling Session cache

1. Login to the appliance using the console or an SSH client (Using SSH and SFTP)
2. Select "Advanced Options" from the Main Menu.
3. Select "Admin menu" from the Advanced Menu.
4. Select "Ehcache" from the Admin Menu.
5. Select the option to enable Session Caching.

Disable Session cache

1. Login to the appliance using the console or an SSH client (Using SSH and SFTP)
2. Select "Advanced Options" from the Main Menu.
3. Select "Admin menu" from the Advanced Menu.
4. Select "Ehcache" from the Admin Menu.
5. Select the option to disable Session Caching.

Troubleshooting

1. Check that the IP address is the correct IP for the appliance.
2. Check that multicast messages are allowed across the network between appliances, i.e. are the switches capable of multicast, or does multicast need to be enabled on them.
3. Check that UDP port 4446 is open and able to communicate between appliances.

If any error messages are reported after the rpm command please contact Swivel Secure support (support@swivelsecure.com) for assistance.

Known issues

After enabling session caching from the CMI, a bug in the CMI may prevent the session cache being enabled, if it is not working, check that:

/webapps/pinsafe/WEB-INF/classes/multicast-cache.xml has been changed to /webapps/pinsafe/WEB-INF/classes/cache.xml

and

Within config.properties file which will be found in one of the following locations:

- Swivel 3.9.2 and later on appliance: /home/swivel/.swivel/conf
- Swivel 3.9.2 and later on software: USER_HOME/.swivel/conf
- Swivel 3.5 to 3.9.1 or earlier: /usr/local/tomcat/webapps/pinsafe/WEB-INF/conf
- Swivel 3.5 to 3.9.1 or earlier on software: <path to Tomcat>/webapps/pinsafe/WEB-INF/conf

SECURITY_STRING_GENERATOR = com.swiveltechnologies.pinsafe.server.utility.SecurityString

SESSION_MANAGER = com.swiveltechnologies.pinsafe.server.session.DistributedCacheSessionManager

SESSION_MANAGER = com.swiveltechnologies.pinsafe.server.session.LocalSessionManager

it should look like the above, with SESSION_MANAGER having been changed to DistributedSessionManager...

Error Messages

PINsafe Session Caching is not available

This error can be seen on the CMI 0.9z-17 and CMI 0.9z-17rc2, the session cache details are set, but the error message is incorrectly displayed. Restart Tomcat for the settings to take effect.