Application Note

Troubleshooting Deep Inspection Update Issues

Version 1.0

Ronald Ng
AJTAC Engineer
AV/DI/UF Specialist

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089 USA
408 745 2000 or 888 JUNIPER
www.juniper.net

Part Number: 350075-001 August 2005
Contents

Contents ................................................................................................................................................... 2
Introduction ............................................................................................................................................ 3
Prerequisites ........................................................................................................................................... 3
Additional Limitations of DI on Some Devices .................................................................................. 3
Subscription Key Requirements ............................................................................................................. 4
Debugging DI Updates ........................................................................................................................... 4
Database Limitations ............................................................................................................................. 4
Introduction

Deep Inspection has been a feature that has been present in ScreenOS 5.0.0. There have been some changes to operation of some hardware devices due to memory requirements from one ScreenOS to another. This document will try to clarify the differences, requirements, and basic troubleshooting tips in obtaining the Deep Inspection updates.

Prerequisites

There are some devices that cannot run Deep Inspection, due to hardware requirements. The following devices CANNOT run Deep Inspection (DI):

- NetScreen-5XP
- NetScreen-5
- NetScreen-10
- NetScreen-100

Additionally, Deep Inspection is only supported on devices running ScreenOS 5.0.0 and higher. This automatically eliminates NetScreen-5 and NetScreen-10. However, the NetScreen-5XP and NetScreen-100 can still run ScreenOS 5.0.0. Due to hardware limitations on these platforms, DI cannot be installed.

Additional Limitations of DI on Some Devices

Even though you may have a device that is not included in the list above, you may still run into limitations into running DI on a device. For the NetScreen-25, NetScreen-50, NetScreen-204, NetScreen-208, NetScreen-500, NetScreen-5000, ISG-1000, and ISG-2000, you have the option of purchasing either the baseline version or advance version. DI requires at least running Advance license. If you have a device that uses Baseline, you need to upgrade to an Advanced license. You can determine the mode of your device by issuing a ‘get license’.

On the SSG platforms, there are additional RAM requirements. See table below:

<table>
<thead>
<tr>
<th>Platform</th>
<th>ScreenOS Required</th>
<th>RAM Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSG-5</td>
<td>5.4.0 or higher</td>
<td>256 MB</td>
</tr>
<tr>
<td>SSG-20</td>
<td>5.4.0 or higher</td>
<td>256 MB</td>
</tr>
<tr>
<td>SSG-140</td>
<td>5.4.0 or higher</td>
<td>512 MB</td>
</tr>
<tr>
<td>SSG-520</td>
<td>5.4.0 or higher</td>
<td>1024 MB</td>
</tr>
<tr>
<td>SSG-550</td>
<td>5.4.0 or higher</td>
<td>1024 MB</td>
</tr>
</tbody>
</table>
Subscription Key Requirements

A device must have the DI subscription key loaded onto the device. If the device does not have DI installed, you will see the following restriction:

- Cannot create a connection to obtain updates
- No Attack options will be available

If your device is properly entitled for DI, you can have the box retrieve its license keys directly from the server onto the device itself. You can do this in the WebUI by clicking “Retrieve Subscriptions Now”, or from the CLI using the command “exec license-key update”. Once this is complete, your DI license key has been loaded into flash, and you can begin obtaining scheduled DI updates.

Debugging DI Updates

Even after obtaining the license keys, if you are still having problems obtaining the latest DI update, make sure the following has been applied:

- System clock is up to date. Recommend having clock synchronized via NTP
- Verify the DNS is properly configured, and the DNS name services.netscreen.com can be resolved.
- Verify that services.netscreen.com is reachable. Doing a ping from the console of the NetScreen can verify this.
- Make sure there is a default route to the Internet, so that services.netscreen.com can be reached
- Make sure https traffic is allowed through to the Internet

If all the above has been checked, you should determine why the connection is not successful by running some debugs.

- Debug httpfx all
- Debug pki detail
- Debug ssl all

Debug httpfx all will show http specific details about the connection between the NetScreen and services.netscreen.com, and the actual progress of downloading the update. Debug pki detail will check if there are issues specific to the SSL certificate negotiation between the NetScreen and the web server at services.netscreen.com

Database Limitations

All NetScreen firewalls are hardware devices, and will have limitations on how large a database that can be stored. This hardware limitation is the reason why the NS-5XP and the NS-100 do not support DI, even though both can run ScreenOS 5.0.0.
Beginning with ScreenOS 5.1.0, the NetScreen-5XT was limited to only supporting Critical level signatures and anomalies. With ScreenOS 5.3.0, the NetScreen-5GT was added to the list, supporting only Critical level signatures and anomalies.

As a result of this, when upgrading NS-5XT from 5.0.0 to 5.1.0, and NS-5GT from 5.2.0 to 5.3.0, the database will be cleared out. This also means all attack group definitions that were bound to a policy will be lost. After upgrading, simply update the attack database, and add the attack groups desired to policies.

You will still see the same predefined group definitions, but you will notice it will not have any members in that group. You will only see critical groups with any attack members. Additionally, in ScreenOS 5.3.0, a new feature was introduced that would allow you to specify one of 4 possible DI update packages (to load only signatures and anomalies that would apply to this particular network environment). These packages are:

- Base
- Server
- Client
- Worm

The default on the device is to update “Base” signatures. You can specify which DI package you want to download by specifying the correct URL in the attack database:

- Base – http://services.netscreen.com/restricted/sigupdates
- Server – http://services.netscreen.com/restricted/sigupdates/server
- Client – http://services.netscreen.com/restricted/sigupdates/client
- Worm – http://services.netscreen.com/restricted/sigupdates/worm