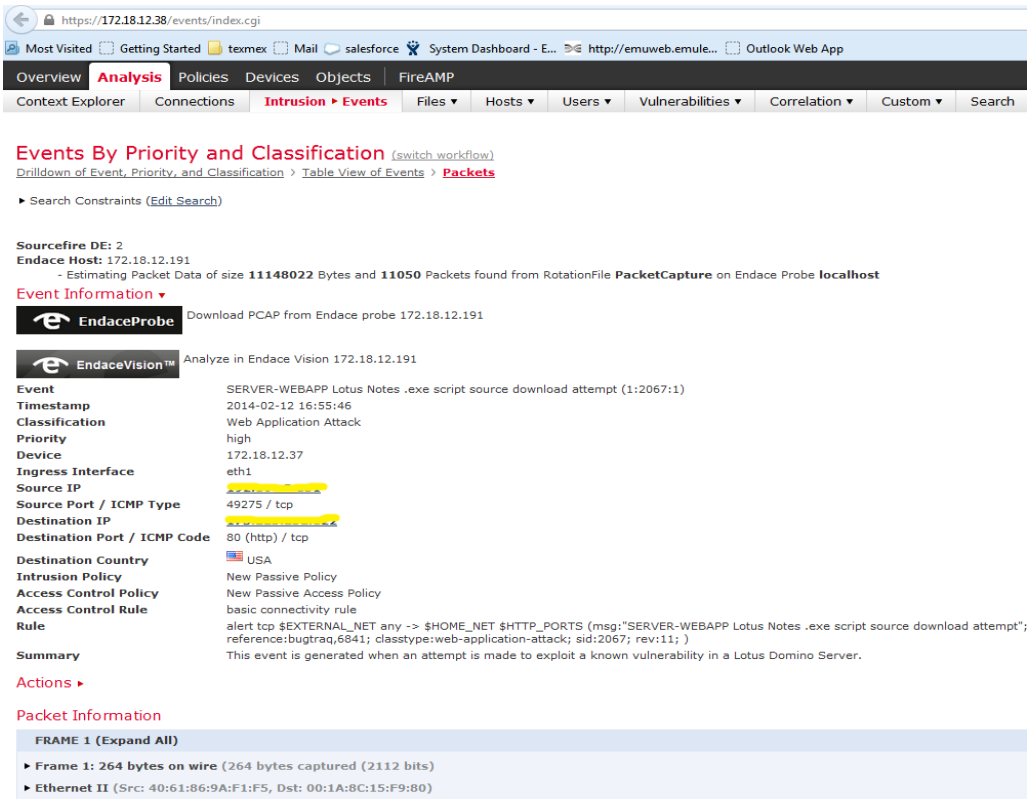
Installing and Configuring the EndaceFusion Connector for Sourcefire Defense Center

Version 8 – April 2015

Introduction

The integration between the Sourcefire Defense Center solution and EndaceProbe INR packet capture appliance provides a seamless way to perform real time security analysis. The simple click-through integration between the products make investigation of security events extremely efficient and increases the overall output of analysts by allowing them to investigate more events, more effectively.



Release Version

Endace Patch Version	Endace Osm Version	SourceFire Defense Center Version
EndacePatch2.0	OSm 5.1.3,5.2.0,6.0.2	5.2.0, 5.3.0
EndacePatch3.0	OSm 5.1.3,5.2.0,6.0.2	5.4.1

Installation

Note: Before installation, check the installer file (`installEndacePatch.sh`) for executable permission and EOL conversion. The installation file should be in "unix" format; otherwise you will get errors as shown below. "dos2unix" command on Defence Center will convert it appropriately.


```
admin@Sourcefire3D:~/EndacePatch2.0$ file installEndacePatch.sh
installEndacePatch.sh: Bourne-Again shell script, ASCII text executable, with
CRLF line terminators
admin@Sourcefire3D:~/EndacePatch2.0$ dos2unix installEndacePatch.sh
admin@Sourcefire3D:~/EndacePatch2.0$ file installEndacePatch.sh
installEndacePatch.sh: Bourne-Again shell script, ASCII text executable
```

Upgrade/Downgrade

1. Login in to the sourcefire probe as 'admin'.
2. Important – we want to preserve the contents of the configuration file named as 'endace.conf" and reuse and apply it post upgrade.

   Working copy of "endace.conf" is available at /sf/etc/endace.conf.

   ```
   #sudo cp /sf/etc/endace.conf /tmp
   ```

   User can also copy the content of the file and paste it in a local notepad.
3. Remove the existing Patch (Refer to Point 6 under New Installation)
4. Upload/copy the package (.tgz file) to the Sourcefire Defense Center at location "/var/home/admin". Copy the files using a scp client (such as openssh or putty scp).
5. Unzip the file and go to the package directory
   ```
   #cd /var/home/admin/EndacePatch2.0
   ```
6. Replace content of endace.conf with the one saved in /tmp folder or copy and paste from a local file to endace.conf.
7. Install the Patch.

New Installation

1. Upload/copy the EndacePatch2.0.tgz package to the Sourcefire Defense Center at location "/var/home/admin". Copy the files using a scp client (such as openssh or putty scp).
2. Log into the Sourcefire appliance as an "admin" user.

   ```
   login as: admin

   Using keyboard-interactive authentication.
   Password:

   Last login: Thu Jan 22 18:19:10 2015 from 172.18.5.110
   Copyright 2001-2013, Sourcefire, Inc. All rights reserved. Sourcefire is a
   registered trademark of Sourcefire, Inc. All other trademarks are property of
   their respective owners.

   Sourcefire Linux OS v5.3.0 (build 52)
   Sourcefire Virtual Defense Center 64bit v5.3.0 (build 571)
   ```

3. Unzip the file and go to the package directory

   admin@Sourcefire3D:~$ cd /var/home/admin/EndacePatch2.0/

   ```
   admin@Sourcefire3D:~/EndacePatch2.0$
   ```

4. Check the content of the patch and it should include the following files:

   ```
   admin@Sourcefire3D:~/EndacePatch2.0$ ls -l
   -rw-r--r-- 1 admin admin    339 Jun 30  2014 CHANGELOG
   -rw-r--r-- 1 admin admin 169814 Jun  9  2014 Integrating_Sourcefire_3D_v7.pdf
   -rw-r--r-- 1 admin admin  82918 Jun 30  2014 PacketView.pm
   -r--r--r-- 1 root  root   52642 Oct  6 16:59 PacketView.pm.backup.VER-
   5.3.0.1412614758
   -rw-r--r-- 1 admin admin  33486 Jun 30  2014 PacketView.pm.patch
   -rw-r--r-- 1 admin admin    185 Jun 30  2014 endace.conf
   -rw-r--r-- 1 admin admin   1852 Jun 10  2014 endace_logo.png
   -rw-r--r-- 1 admin admin   3335 Jun 10  2014 endace_vision_logo.png
   -rw-r--r-- 1 admin admin     24 Jun 10  2014 endace_viz_id.conf
   ```



```
-rwxr-xr-- 1 admin admin   5946 Jun 10  2014 installEndacePatch.sh
```

5. Check if the patch is not already installed.

```
admin@Sourcefire3D:~/EndacePatch2.0$ sudo ./installEndacePatch.sh status
Password:

 ************************************************
 * Endace Patch v2.0 for Sourcefire Defense Center *
 ************************************************
* Status
  NO  /usr/local/sf/lib/perl/5.10.1/SF/PacketView.pm is NOT patched
- NOT INSTALLED /Volume/5.2.0/sf/htdocs/img/icons/medium/endace_logo.png
- NOT INSTALLED /Volume/5.2.0/sf/htdocs/img/icons/medium/endace_vision_logo.png
- NOT INSTALLED /etc/sf/endace.conf
* Checking compatability with current release...
  Patch PacketView.pm.patch will clean apply to
/usr/local/sf/lib/perl/5.10.1/SF/PacketView.pm
1
* Looks like patch is good for 5.3.0
admin@Sourcefire3D:~/EndacePatch2.0$
```

6. Install the Patch.
   This will install the patch and copy all the necessary files as shown below:

```
admin@Sourcefire3D:~/EndacePatch2.0$ sudo ./installEndacePatch.sh install
Password:

 ************************************************
 * Endace Patch v2.0 for Sourcefire Defense Center *
 ************************************************
* Patching with Endace Patch....
  Patch PacketView.pm.patch will clean apply to
/usr/local/sf/lib/perl/5.10.1/SF/PacketView.pm
1
* Looks like patch is good for 5.3.0
- Taking backup of /usr/local/sf/lib/perl/5.10.1/SF/PacketView.pm
PacketView.pm.backup.VER-5.3.0.1412614758
* Copy files
- Installing /Volume/5.3.0/sf/htdocs/img/icons/medium/endace_logo.png
- Installing /Volume/5.3.0/sf/htdocs/img/icons/medium/endace_vision_logo.png
- Installing /etc/sf/endace.conf
admin@Sourcefire3D:~/EndacePatch2.0$
```

7. Remove the Patch – This will remove patch and other files that were part of the package.

```
admin@Sourcefire3D:~/EndacePatch2.0$ sudo ./installEndacePatch.sh remove
Password:

 ************************************************
 * Endace Patch v2.0 for Sourcefire Defense Center *
 ************************************************
* Removing Endace Patch....
  Removing - PacketView.pm.patch from
/usr/local/sf/lib/perl/5.10.1/SF/PacketView.pm
* Remove files....
  Removing /Volume/5.3.0/sf/htdocs/img/icons/medium/endace_logo.png
  Removing /Volume/5.3.0/sf/htdocs/img/icons/medium/endace_vision_logo.png
  Removing /etc/sf/endace.conf
admin@Sourcefire3D:~/EndacePatch2.0$
```

8. Configuration steps:

```
admin@Sourcefire3D:~/EndacePatch2.0$ sudo ./installEndacePatch.sh config

 ************************************************
 * Endace Patch v2.0 for Sourcefire Defense Center *
 ************************************************
* Configuration
Enter the Sourcefire DE ID: 2
Enter the IP address for the Endace probe: 172.18.12.191
Enter the User Login for the Endace probe: visiondemo
Enter the User Passwd for the Endace probe: changeme
Enter the number of seconds before the incident's time: 60
```



```
Enter the number of seconds after the incident's time: 60
Enter the number of seconds after which the old datamines will be purged from
Endace probe: 7200
```

The number of seconds before and after the incident time specifies the window of time around the event for which packets should be downloaded. Choose a period that is most appropriate for your purposes. The number of seconds that old datamines are purged should be left at the default of 7200.

9. Configuration notes:

Configuration prompts the user to fill in the required information which are added as a new entry after the "default" entry in endace.conf file

Note:
*Every time configuration script is executed; a **NEW** entry will be added at the end of the endace.conf*

Default "endace.conf" file:

```
#DE_MAP_ID,Endace_Probe_IP,EP_VisionUser,EP_VisionUserPass,Seconds_Before,Seconds_
After,Datamine_created_before
default,172.18.12.191, visionuser,changeme,30,30,7200
```

After making changes to "endace.conf" file from install script.

```
#DE_MAP_ID,Endace_Probe_IP,EP_VisionUser,EP_VisionUserPass,Seconds_Before,Seconds_
After,Datamine_created_before
default,172.18.12.191,visionuser,changeme,30,30,7200

2,172.18.12.191,visiondemo,changeme,60,60,7200
```

Note:
The "endace.conf" file can also be edited manually if necessary.

Description of fields in "endace.conf":

Field	Description
DE_MAP_ID:	Detection Engine ID - "default" or check from the Sourcefire 3D system (see the *Advanced Configuration Steps* section for instructions on how to obtain this value for each sensor).
Endace_Probe_IP:	IP Address of the EndaceProbe.
EP_VisionUser:	User ID to log into EndaceProbe.
EP_VisionUserPass:	Password for the corresponding role.
Seconds_Before:	Time before the event occurred.
Seconds_After:	Time after the event occurred.
Datamine_created_before:	This is number of seconds after which datamine urls will be purged from EndaceProbe, more like a cleanup action. Every time packet view plugin is executed, this will check the list of existing urls and their creation time. If the creation time is older than "Datamine_created_before" seconds as mentioned, than those stale download urls are deleted from EndaceProbe. This doesn't have any impact on the actual packet data or metadata on EndaceProbe.

Advanced configuration Steps

Role Based Access Control User accounts on EndaceProbes

One of the core user security capabilities of the EndaceProbe is Role-Based Access Control. User account privileges can be set by assigning individual users to one or more RBAC roles that allow access and control to different aspects of the system.

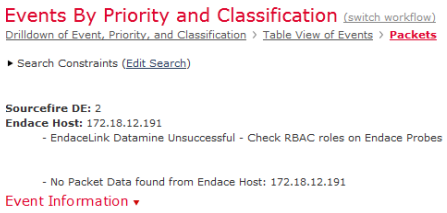
In order to best secure the EndaceProbe it is recommended that a dedicated user account is set up for access from the Sourcefire Defense Center. This account should have its own unique password with only the *app_user* role enabled. This restricts access to packet and packet metadata, which is sufficient for the use of this Fusion connector.

For information on how to set user roles, please refer to the *Setup > User > Role Based Access Control* section in *EDM09-10 EndaceProbe User Guide* or contact Endace Support via endace.support@emulex.com.

After creating a user on EndaceProbe with sufficient privileges, a user with admin privileges on Sourcefire system can either directly edit the "/etc/sf/endace.conf" to add the new user or update an existing user or the admin can choose to add a new user via the "installation script" as described in section 8 above (configuration steps).

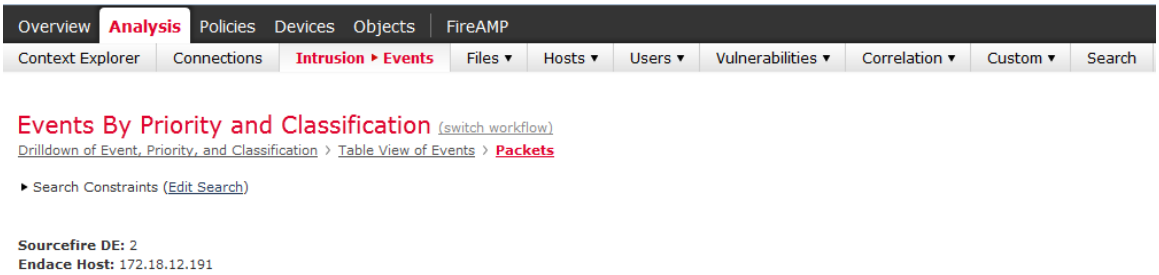
Note:
In case duplicate entries exists with same Detection Engine IDs, then only the last one is used for packet data searches and all others prior to that are ignored.

Incorrect RBAC privileges will result in failure to execute Endace REST calls and may result in errors as shown below:



Determining Sourcefire Detection Engine ID

Install the Endace Plugin and go to Sourcefire 3D system and drill down into "Events By Priority and Classification" Packets View. If the Endace plugin is installed correctly Sourcefire DE ID (Example - Sourcefire DE: 2) is displayed on the Packet view Page as seen below.



Plugin Message Output

The following messages are printed to reflect the status of the data either found or not on Endace Probe

Packet Data Found

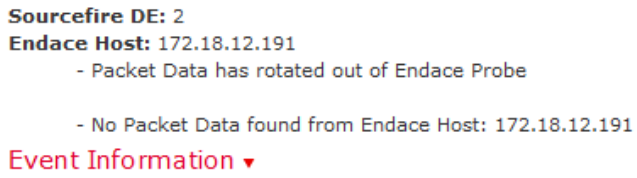

```
Sourcefire DE: 2
Endace Host: 172.18.12.191 - Estimating Packet Data of size 11148022 Bytes and
11050 Packets found from RotationFile PacketCapture on Endace Probe localhost
```

Upon clicking into the packet page for an event, an estimation of the amount of packet data related to the event is displayed. The above statement shows *Number of Bytes* and *Number of Packets* that matched this flow search query.

The idea behind these numbers is to let the user know beforehand how large the match is, so as to avoid downloading the actual file. For example, if the match resulted in couple of GB of data and the user is working behind a slow link, than he can either analyze using Endace Vision Tool or modify the search window by editing entry in the "/etc/sf/endace.conf" file, to narrow down the time window around the event search.

The two Endace Logos are links to either download PCAP file or for direct analysis on EndaceProbe Vision tool

Packet Data Rotated Out



Packet Data doesn't exist anymore on the EndaceProbe, this is typically due to the age of the packets related to the event. Check the RotationFile on the EndaceProbe and ensure that the RotationFile is sufficiently large – if packets related to recent events are repeatedly being rotated out, then the size of the RotationFile should be increased if possible. Please contact Endace Support at endace.support@emulex.com for assistance with the configuration of Endace Probes to get the maximum storage out of the probes.

Packet Data Not Found

This message is generated when no data could be found and indicates that the endace.conf file may not contain all of the EndaceProbe IP's or is incorrectly populated. This may occur either by entering incorrect IP address of the Endace probe IP or incorrect login / password. Please check the "/etc/sf/endace.conf" and correct it if required.

If the configuration is correct this message is an indication that the metadata has rotated out of storage allocated on Endace Probes. This can be corrected by increasing the retention period for EndaceVision metadata in the RotationFile configuration. Please contact Endace Support at endace.support@emulex.com for assistance.

Copyright & Disclaimer

Support

If you experience problems with any aspect of using the EndaceProbe software, please contact Endace Technical Support at endace.support@emulex.com for further assistance.

Disclaimer

Whilst every effort has been made to ensure accuracy, neither Endace Technology Limited nor any employee of the company, shall be liable on any ground whatsoever to any party in respect of decisions or actions they may make as a result of using this information. Information furnished by Endace is believed to be accurate and reliable. However, no responsibility is assumed by Endace for its use; or for any infringements of patents or other rights of third parties which may result from its use. No license is granted by implication or otherwise under any patent, copyright or related rights of Endace. Endace Technology Limited has taken great effort to verify the accuracy of this document, but nothing herein should be construed as a warranty and Endace shall not be liable for technical or editorial errors or omissions contained herein. Endace provides this user guide "as is" without any warranty of any kind, either expressed or implied, including but not limited to the implied warranties of merchantability or fitness for a particular purpose. In accordance with Endace's policy of continuing development, Endace may make improvements and changes to the product described in this document at any time and without any notice. Similarly, the information contained herein is subject to change without notice; although these changes may be incorporated into new editions of this document, Endace disclaims any undertaking to give notice of such changes.

Website

www.emulex.com/visibility/

Copyright 2014 - 2015 Endace Technology Limited. All Rights Reserved Worldwide.

Endace Technology Limited
6th Floor, KPMG Center
85 Alexandra Street
Hamilton, New Zealand, 3204