Engineering
Simplicity

Juniper Secure Analytics Managing Juniper SRX PCAP Data

Published
2022-05-02

RELEASE
7.5.0

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Juniper Secure Analytics Managing Juniper SRX PCAP Data
7.5.0

The information in this document is current as of the date on the title page.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at https://support.juniper.net/support/eula/. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

About This Guide

This guide talks about how you can configure your JSA console to integrate with the Juniper Junos OS Platform DSM, so that JSA can receive, process, and store Packet Capture (PCAP) data from a Juniper SRX-Series Services Gateway log source.

1

CHAPTER

Forwarding Syslogs with Packet Logging from SRX to JSA

Forwarding Syslogs

This section provides information on how to forward syslogs with packet logging (PCAP) from SRX to JSA. PCAPs are sent through UDP. In the example, port 5 is used. You can use any port but it must match in both the JSA and SRX configuration.

To forward syslogs with PCAP from SRX to JSA:

1. To enable packet capture and logging on the IDP policy level, run the following commands:

   ```
   set security idp idp-policy Test rulebase-ips rule 1 then notification log-attacks

   set security idp idp-policy Test rulebase-ips rule 1 then notification packet-log pre-attack 10

   set security idp idp-policy Test rulebase-ips rule 1 then notification packet-log post-attack 3

   set security idp idp-policy Test rulebase-ips rule 1 then notification packet-log post-attack-timeout 60
   ```

   > **NOTE**: You must configure match conditions and action.

2. To enable packet capture on the IDP sensor level:

   ```
   set security idp sensor-configuration packet-log total-memory 5

   set security idp sensor-configuration packet-log max-sessions 15

   set security idp sensor-configuration packet-log source-address 10.0.0.1

   set security idp sensor-configuration packet-log host 10.0.0.2

   set security idp sensor-configuration packet-log host port 5
   ```

   > **NOTE**: When the packet capture object is prepared, SRX transmits the packet captures from IP 10.0.0.1 to port 5 to device 10.0.0.2 (JSA). If the log source (SRX) IP is different from the source address configured here, JSA will not recognize the log source and will not display the log with PCAP in the WebUI. However, the PCAP is stored on JSA under the directory **/store/pcap/**.
   > The IDP option must be enabled in the firewall policy to send the traffic to the IDP module.

3. Add the log source in the JSA:

   a. Navigate to path: **Admin** > **Data Source** > **Events** > **Log Sources**.

   b. Select **Log Source Type** > **Juniper SRX-series Services Gateway**.

   c. Select **Protocol Configuration** > **PCAP Syslog Combination**.

d. Select **Incoming Port** > **5** (**Configured on SRX: set security idp sensor-configuration packet-log host port 5**).

> **NOTE**: You must configure other information such as, log source name, IP, and so on.

4. Verify the configuration on the SRX:

- Run the following command to verify packet capture configuration on the IDP sensor level:

```
root@SRX# show security idp sensor-configuration
    packet-log {
    total-memory 5;
    max-sessions 15;
    source-address 10.0.0.1;
    host {
        10.0.0.2;
        port 5;
    }
}
```

- Run the following command to verify packet capture and logging configuration on the IDP policy level:

```
root@SRX# show security idp idp-policy LAB_Test
    rulebase-ips {
    rule 1 {
        match {
            source-address any;
            destination-address any;
            application default;
            attacks {
                predefined-attacks [ ICMP:INFO:ECHO-REQUEST ICMP:INFO:ECHO-REPLY ];
            }
        }
        then {
            action {
                no-action;
            }
            notification {
                log-attacks;
                packet-log {
                    pre-attack 10;
                    post-attack 3;
                    post-attack-timeout 60;
                }
            }
        }
    }
}
```

NOTE: Other parameters such as attacks, source-address, and destination-address are for reference only.

5. Verify the configuration on the JSA:
    a. Navigate to the path: **Admin** > **Data Source** > **Events** > **Log Sources**.
    b. Verify the information below:
        - **Log Source Status** > **Success**.
        - **Protocol** > **PCAPSyslog**.
        - **Log Source Type** > **Juniper SRX-series Services Gateway**.
        - **Enabled** > **True**.
6. To display the PCAP data column on the JSA, see section *Displaying the PCAP Data Column*.

2

CHAPTER

Managing Juniper SRX PCAP Data Overview

SRX PCAP Data Overview

IN THIS SECTION

If your JSA console is configured to integrate with the Juniper Junos OS Platform DSM, JSA can receive, process, and store Packet Capture (PCAP) data from a Juniper SRX-Series Services Gateway log source. For more information about the Juniper Junos OS Platform DSM, see the *Juniper Secure Analytics Configuring DSMs.*

This section provides information on how to download and view PCAP data using the Events interface on your JSA console. Unless otherwise noted, all references to JSA refer to both JSA and JSA Log Manager.

Before you can display PCAP data in the Events interface, the Juniper SRX-Series Services Gateway log source must be configured with the PCAP Syslog Combination protocol. For more information on configuring log source protocols, see the *Log Sources Users Guide*.

This document provides information on managing PCAP data, including:

Configure the PCAP Protocol

The Juniper SRX Series appliance supports forwarding of packet capture (PCAP) and Syslog data to JSA.

Syslog data is forwarded to JSA on port 514. The IP address and outgoing PCAP port number is configured on the Juniper Networks SRX Series appliance interface. The Juniper Networks SRX Series appliance must be configured using the to forward PCAP data in the format `<IP Address>:<Port>`.

Where:

`<IP Address>` is the IP address of JSA.

`<Port>` is the outgoing port address for the PCAP data.

For more information on Configuring Packet Capture, see your Juniper Networks Junos OS documentation.

You are now ready to configure the log source and protocol in JSA. For more information see section *Configuring a New Juniper Networks SRX Log Source with PCAP*.

Configuring a New Juniper Networks SRX Log Source with PCAP

The Juniper Networks SRX Series appliance is auto discovered by JSA as a Juniper Junos OS Platform.

JSA detects the Syslog data and adds the log source automatically. The PCAP data can be added to JSA as Juniper SRX Series Services Gateway log source using the PCAP Syslog Combination protocol. Adding the PCAP Syslog Combination protocol after JSA auto discovers the Junos OS Syslog data adds an additional log source to your existing log source limit. Deleting the existing Syslog entry, then adding the PCAP Syslog Combination protocol adds both Syslog and PCAP data as single log source.

1. Log in to JSA.
2. Click the Admin tab.
3. On the navigation menu, click **Data Sources**.
4. Click the Log Sources icon.
5. Click **Add**.
6. From the Log Source Type list box, select **Juniper SRX Series Services Gateway**.
7. From the Protocol Configuration list box, select **PCAP Syslog Combination**.
8. Type the Log Source Identifier.
9. Type the Incoming PCAP Port.

   To configure the Incoming PCAP Port parameter in the log source, enter the outgoing port address for the PCAP data as configured on the Juniper Networks SRX Series appliance interface. For more information on configuring log sources, see the *Log Sources Users Guide*.
10. Click **Save**.
11. Select the auto discovered Syslog-only Junos OS log source for your Juniper Networks SRX Series appliance.
12. Click **Delete**.

    A delete log source confirmation window is displayed.
13. Click **Yes**.

The Junos OS Syslog log source is deleted from the log source list. You should now have the PCAP Syslog Combination protocol in your log source list.

14. On the **Admin** tab, click **Deploy Changes**.

Displaying the PCAP Data Column

The PCAP Data column is not displayed in the Events interface by default. When you create search criteria, you must select the PCAP Data column in the Column Definition section. You can also group your event search results by the PCAP Data column. For more information on searching and viewing events, see the *Juniper Secure Analytics Users Guide*.

To display the PCAP data column in event search results:

1. Click the **Events** tab.

   The Events interface appears.

2. Using the Search drop-down list box, select **New Search**.

   The new event search window appears.

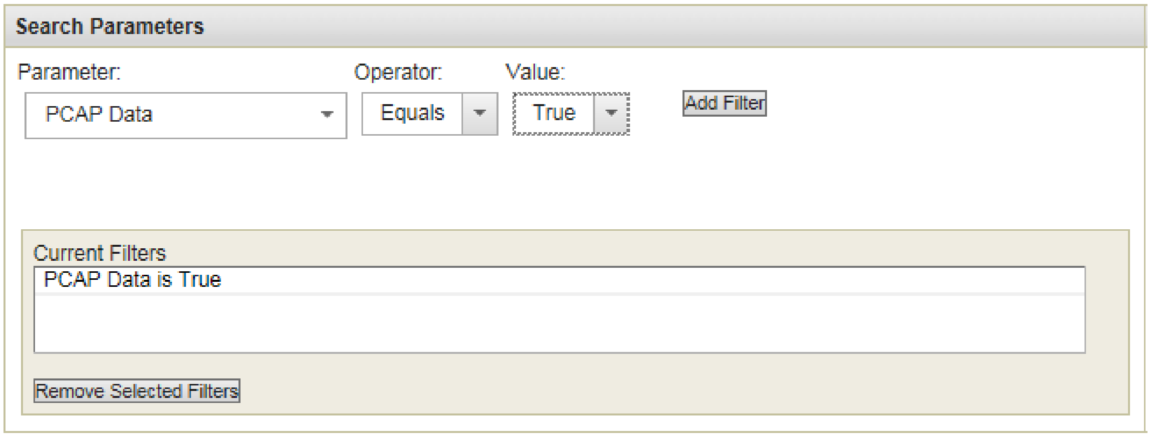
3. Optional. Configure your specific search criteria:

   NOTE: If you perform this step, the search results display only events that have PCAP data available.

   - Using the first drop-down list box, select **PCAP data**.
   - In the second drop-down list box, select **Equals**.
   - In the third drop-down list box, select **True**.

- Click **Add Filter**, as shown in Figure 1 on page 9.

Figure 1: Adding PCAP Data to the Columns List



Search Parameters

Parameter: PCAP Data

Operator: Equals

Value: True

Current Filters

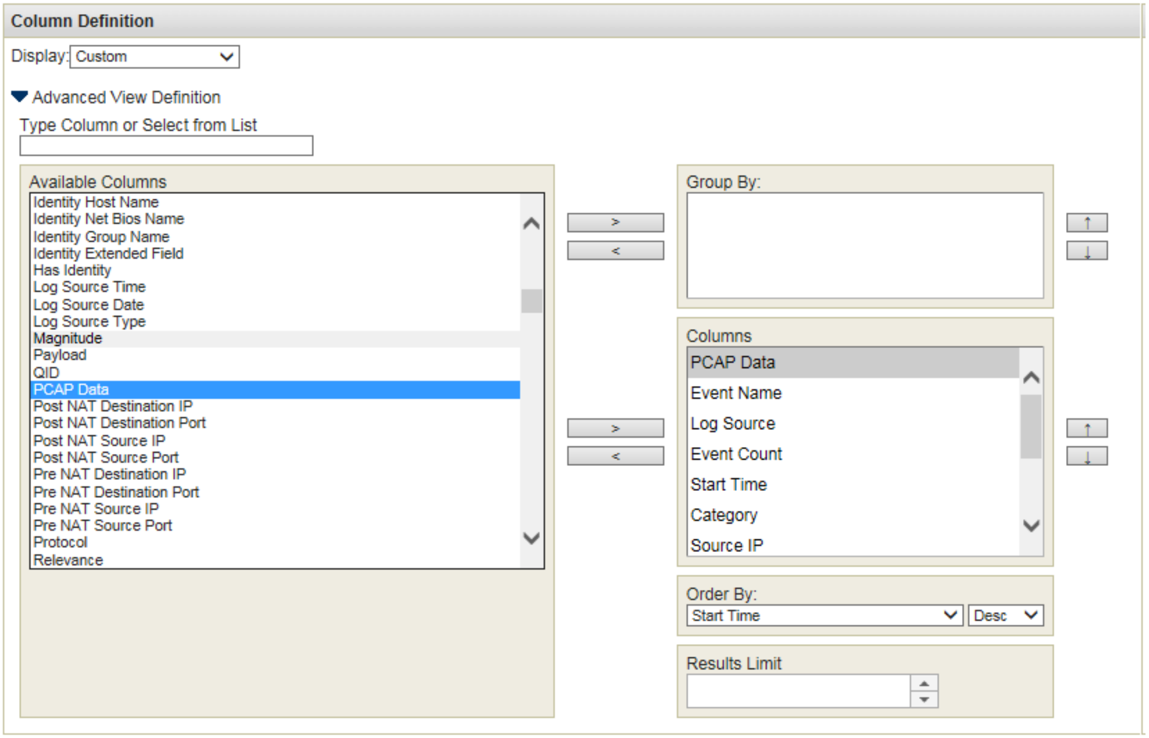
PCAP Data is True

4. Configure your column definitions:

- From the Available Columns list in the Column Definition section, click **PCAP Data**.

- Use the bottom set of Add and Remove arrow buttons to select PCAP data from the Available Columns list to add it in the Columns list, as shown in Figure 2 on page 10.

Figure 2: PCAP Data Column Search Results



Column Definition

Display: Custom

Advanced View Definition

Type Column or Select from List

Order By: Start Time Desc

- Optional. Use the top set of Add and Remove arrow buttons to move PCAP data from the Available Columns list to add it in the Group By list.

5. Click **Filter**.

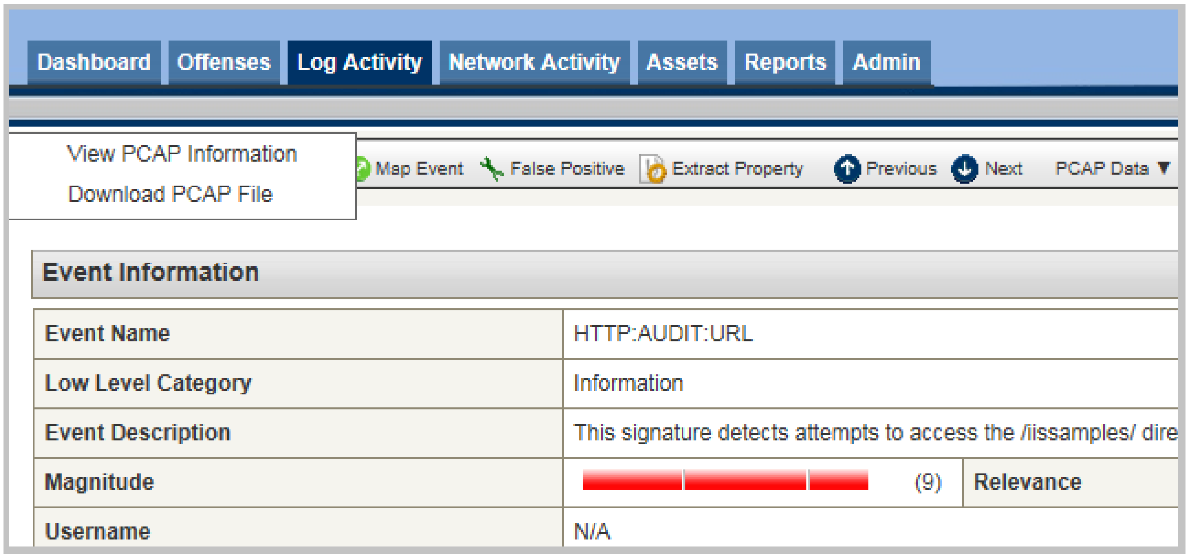
> **NOTE**: You can configure your event search using additional parameters, however, this procedure only demonstrates the required search criteria to display the PCAP data column. For more information about searching events, see the *Juniper Secure Analytics Users Guide*.

The event search results appear, displaying the PCAP Data column, as shown in Figure 3 on page 11. If PCAP data is available for an event, an icon appears in the PCAP Data column. Using the PCAP icon, you can view the PCAP data or download the PCAP file to your desktop system.

6. Double-click the event you want to investigate.

NOTE: If you are viewing events in streaming mode, you must pause streaming before you double-click an event.

Figure 3: PCAP Events Details Window



Event Information

Event Name	HTTP:AUDIT:URL		
Low Level Category	Information		
Event Description	This signature detects attempts to access the /iissamples/ dire		
Magnitude	(9)	Relevance	
Username	N/A		

The events details window appears.

From the PCAP Data toolbar option, you can view the PCAP information or download the PCAP file to your desktop system.

Viewing PCAP Information

You can view a readable version of the data in the PCAP file. To view PCAP information:

1. Click the **Events** tab.

   The Events interface appears.

2. Perform or select a search that displays the PCAP Data column. See section *Displaying the PCAP Data Column*.

   The event search results appear.

3. Choose one of the following:

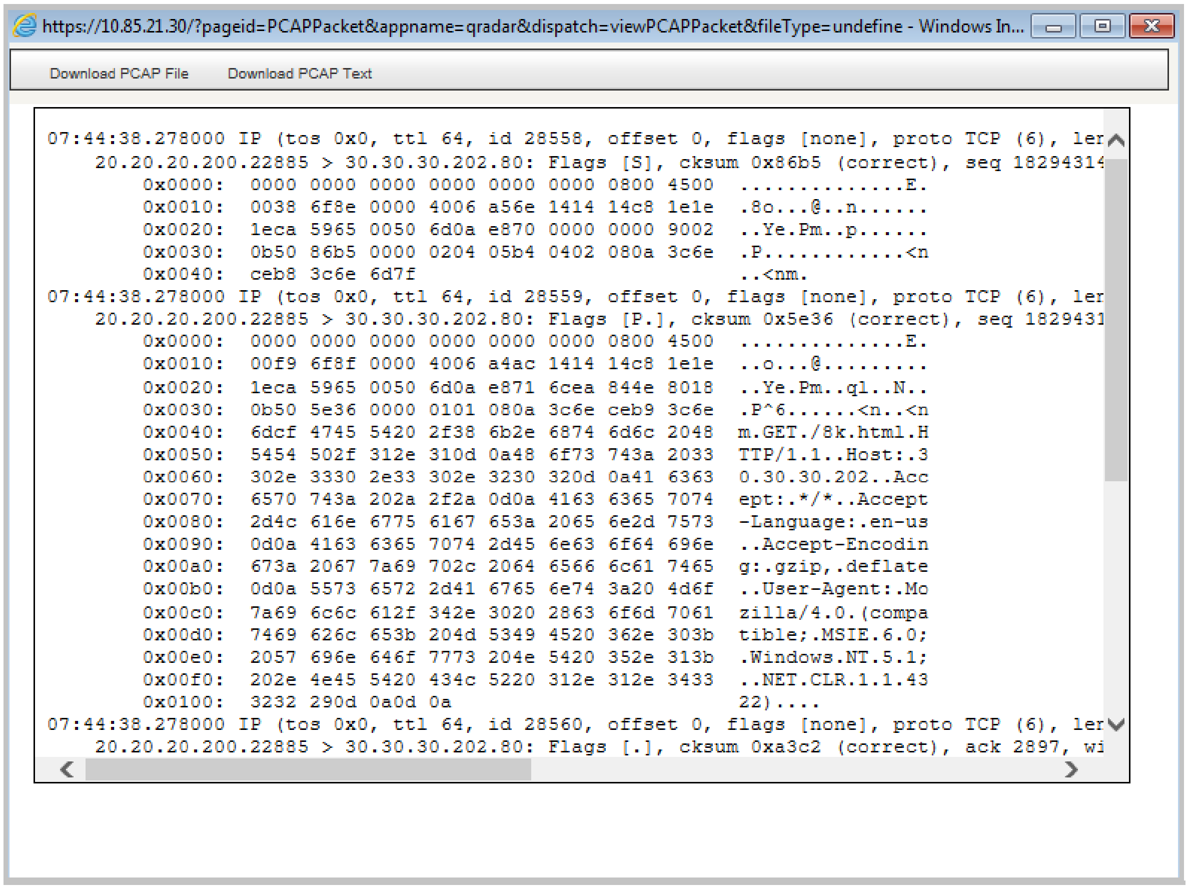
- Right-click the PCAP icon for the event you want to investigate, and then select **More Options > View PCAP Information**.

- Double-click the event you want to investigate, and then select **PCAP Data > View PCAP Information** from the event details toolbar.

> **NOTE**: If you are viewing events in streaming mode, you must pause streaming before you double-click an event.

> **NOTE**: Before PCAP data can be displayed, JSA must retrieve the PCAP file for display in the user interface. If the download process takes an extended period of time, the Downloading PCAP Packet Information window appears. In most cases, the download process is quick and this window does not appear.

Figure 4: Readable Version of the PCAP file


https://10.85.21.30/?pageid=PCAPPacket&appname=qradar&dispatch=viewPCAPPacket&fileType=undefine - Windows In...
Download PCAP File
Download PCAP Text

```
07:44:38.278000 IP (tos 0x0, ttl 64, id 28558, offset 0, flags [none], proto TCP (6), ler
    20.20.20.200.22885 > 30.30.30.202.80: Flags [S], cksum 0x86b5 (correct), seq 18294314
        0x0000:  0000 0000 0000 0000 0000 0000 0800 4500  ..............E.
        0x0010:  0038 6f8e 0000 4006 a56e 1414 14c8 1e1e  .8o...@..n......
        0x0020:  1eca 5965 0050 6d0a e870 0000 0000 9002  ..Ye.Pm..p......
        0x0030:  0b50 86b5 0000 0204 05b4 0402 080a 3c6e  .P............<n
        0x0040:  ceb8 3c6e 6d7f                           ..<nm.
07:44:38.278000 IP (tos 0x0, ttl 64, id 28559, offset 0, flags [none], proto TCP (6), ler
    20.20.20.200.22885 > 30.30.30.202.80: Flags [P.], cksum 0x5e36 (correct), seq 1829431
        0x0000:  0000 0000 0000 0000 0000 0000 0800 4500  ..............E.
        0x0010:  00f9 6f8f 0000 4006 a4ac 1414 14c8 1e1e  ..o...@.........
        0x0020:  1eca 5965 0050 6d0a e871 6cea 844e 8018  ..Ye.Pm..ql..N..
        0x0030:  0b50 5e36 0000 0101 080a 3c6e ceb9 3c6e  .P^6......<n..<n
        0x0040:  6dcf 4745 5420 2f38 6b2e 6874 6d6c 2048  m.GET./8k.html.H
        0x0050:  5454 502f 312e 310d 0a48 6f73 743a 2033  TTP/1.1..Host:.3
        0x0060:  302e 3330 2e33 302e 3230 320d 0a41 6363  0.30.30.202..Acc
        0x0070:  6570 743a 202a 2f2a 0d0a 4163 6365 7074  ept:.*/*..Accept
        0x0080:  2d4c 616e 6775 6167 653a 2065 6e2d 7573  -Language:.en-us
        0x0090:  0d0a 4163 6365 7074 2d45 6e63 6f64 696e  ..Accept-Encodin
        0x00a0:  673a 2067 7a69 702c 2064 6566 6c61 7465  g:.gzip,.deflate
        0x00b0:  0d0a 5573 6572 2d41 6765 6e74 3a20 4d6f  ..User-Agent:.Mo
        0x00c0:  7a69 6c6c 612f 342e 3020 2863 6f6d 7061  zilla/4.0.(compa
        0x00d0:  7469 626c 653b 204d 5349 4520 362e 303b  tible;.MSIE.6.0;
        0x00e0:  2057 696e 646f 7773 204e 5420 352e 313b  .Windows.NT.5.1;
        0x00f0:  202e 4e45 5420 434c 5220 312e 312e 3433  ..NET.CLR.1.1.43
        0x0100:  3232 290d 0a0d 0a                        22)....
07:44:38.278000 IP (tos 0x0, ttl 64, id 28560, offset 0, flags [none], proto TCP (6), ler
    20.20.20.200.22885 > 30.30.30.202.80: Flags [.], cksum 0xa3c2 (correct), ack 2897, wi
```

Once the file is retrieved, a pop-up window appears, displaying a readable version of the PCAP file, as shown in Figure 4 on page 12.

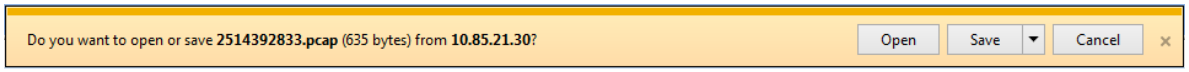
You can read the information displayed in the window, or download the information to your desktop system.

4. If you want to download the information to your desktop system, choose one of the following options:

   - Click **Download PCAP File** to download the original PCAP file to be used in an external application.
   - Click **Download PCAP Text** to download the PCAP information in .txt format.

     The Opening window appears, as shown in Figure 5 on page 13.

Figure 5: PCAP File Save or Open Window



Do you want to open or save **2514392833.pcap** (635 bytes) from **10.85.21.30**?

5. Choose one of the following options:

   - If you want to open the file for immediate viewing, select the **Open with** option and select the desired application from the drop-down list box.
   - If you want to save the list, select the **Save File** option.

6. Click **OK**.

Downloading the PCAP File to Your Desktop System

You can download the PCAP file to your desktop system for storage or for use in other applications. To download the PCAP File to your desktop system:

1. Click the **Events** tab.

   The Events interface appears.

2. Perform or select a search that displays the PCAP Data column. See section *Displaying the PCAP Data Column*.

   The event search results appear.

3. For the event you want to investigate, choose one of the following:

   - Click the PCAP icon.
   - Right-click the PCAP icon and select More **Options** > **Download PCAP File**.
   - Double-click the event you want to investigate, and then select **PCAP Data** > **Download PCAP File** from the event details toolbar.

   NOTE: If you are viewing events in streaming mode, you must pause streaming before you double-click an event.

   The Opening window appears.

4. Choose one of the following options:

   - If you want to open the file for immediate viewing, select the **Open with** option and select the desired application from the drop-down list box.
   - If you want to save the list, select the **Save File** option.

5. Click **OK**.