Juniper Networks | Engineering Simplicity

Juniper Secure Analytics Managing Juniper SRX PCAP Data

Published
2021-01-28

Release
7.4.2

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

Juniper Secure Analytics Managing Juniper SRX PCAP Data
7.4.2

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 the Documentation

IN THIS SECTION

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.

Documentation and Release Notes

To obtain the most current version of all Juniper Networks® technical documentation, see the product documentation page on the Juniper Networks website at https://www.juniper.net/documentation/.

If the information in the latest release notes differs from the information in the documentation, follow the product Release Notes.

Juniper Networks Books publishes books by Juniper Networks engineers and subject matter experts. These books go beyond the technical documentation to explore the nuances of network architecture, deployment, and administration. The current list can be viewed at https://www.juniper.net/books.

Documentation Conventions

Table 1 on page v defines notice icons used in this guide.

Table 1: Notice Icons

Icon	Meaning	Description
	Informational note	Indicates important features or instructions.
	Caution	Indicates a situation that might result in loss of data or hardware damage.
	Warning	Alerts you to the risk of personal injury or death.
	Laser warning	Alerts you to the risk of personal injury from a laser.
	Tip	Indicates helpful information.
	Best practice	Alerts you to a recommended use or implementation.

Table 2 on page v defines the text and syntax conventions used in this guide.

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents text that you type.	To enter configuration mode, type the **configure** command: user@host> **configure**
`Fixed-width text like this`	Represents output that appears on the terminal screen.	`user@host>` **show chassis alarms** `No alarms currently active`
Italic text like this	• Introduces or emphasizes important new terms. • Identifies guide names. • Identifies RFC and Internet draft titles.	• A policy *term* is a named structure that defines match conditions and actions. • *Junos OS CLI User Guide* • RFC 1997, *BGP Communities Attribute*

Table 2: Text and Syntax Conventions *(continued)*

Convention	Description	Examples
Italic text like this	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: [edit] root@# **set system domain-name** *domain-name*
Text like this	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	• To configure a stub area, include the **stub** statement at the **[edit protocols ospf area area-id]** hierarchy level. • The console port is labeled **CONSOLE**.
< > (angle brackets)	Encloses optional keywords or variables.	**stub <default-metric *metric*>;**
| (pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	**broadcast | multicast** **(*string1* | *string2* | *string3*)**
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	**rsvp { # Required for dynamic MPLS only**
[ ] (square brackets)	Encloses a variable for which you can substitute one or more values.	**community name members [*community-ids*]**

Indention and braces ({ })	Identifies a level in the configuration hierarchy.	[edit]
		routing-options {
		  static {
		  route default {
		  nexthop *address*;
		  retain;
		  }
		  }
		}

; (semicolon)	Identifies a leaf statement at a configuration hierarchy level.	
GUI Conventions		

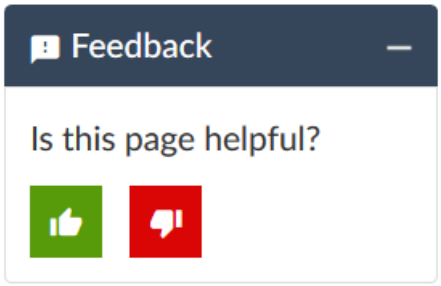
Table 2: Text and Syntax Conventions *(continued)*

Convention	Description	Examples
Bold text like this	Represents graphical user interface (GUI) items you click or select.	• In the Logical Interfaces box, select **All Interfaces**. • To cancel the configuration, click **Cancel**.
> (bold right angle bracket)	Separates levels in a hierarchy of menu selections.	In the configuration editor hierarchy, select **Protocols>Ospf**.

Documentation Feedback

We encourage you to provide feedback so that we can improve our documentation. You can use either of the following methods:

- Online feedback system—Click TechLibrary Feedback, on the lower right of any page on the Juniper Networks TechLibrary site, and do one of the following:



  - Click the thumbs-up icon if the information on the page was helpful to you.
  - Click the thumbs-down icon if the information on the page was not helpful to you or if you have suggestions for improvement, and use the pop-up form to provide feedback.
- E-mail—Send your comments to techpubs-comments@juniper.net. Include the document or topic name, URL or page number, and software version (if applicable).

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active Juniper Care or Partner Support Services support contract, or are

covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at https://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf.
- Product warranties—For product warranty information, visit https://www.juniper.net/support/warranty/.
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: https://www.juniper.net/customers/support/
- Search for known bugs: https://prsearch.juniper.net/
- Find product documentation: https://www.juniper.net/documentation/
- Find solutions and answer questions using our Knowledge Base: https://kb.juniper.net/
- Download the latest versions of software and review release notes: https://www.juniper.net/customers/csc/software/
- Search technical bulletins for relevant hardware and software notifications: https://kb.juniper.net/InfoCenter/
- Join and participate in the Juniper Networks Community Forum: https://www.juniper.net/company/communities/
- Create a service request online: https://myjuniper.juniper.net

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: https://entitlementsearch.juniper.net/entitlementsearch/

Creating a Service Request with JTAC

You can create a service request with JTAC on the Web or by telephone.

- Visit https://myjuniper.juniper.net.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see https://support.juniper.net/support/requesting-support/.

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**.

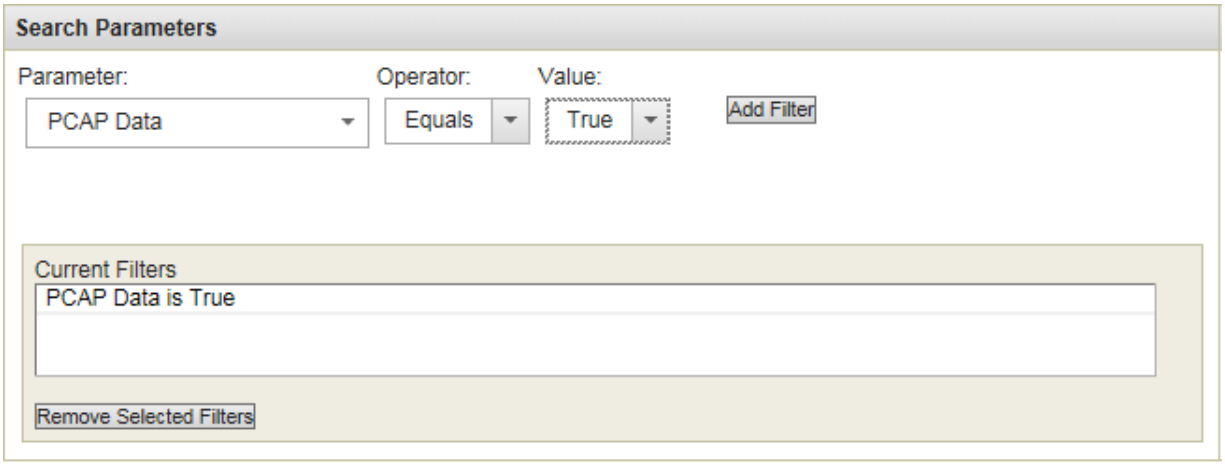
   The new event search window appears.

3. Optional. Configure your specific search criteria:

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

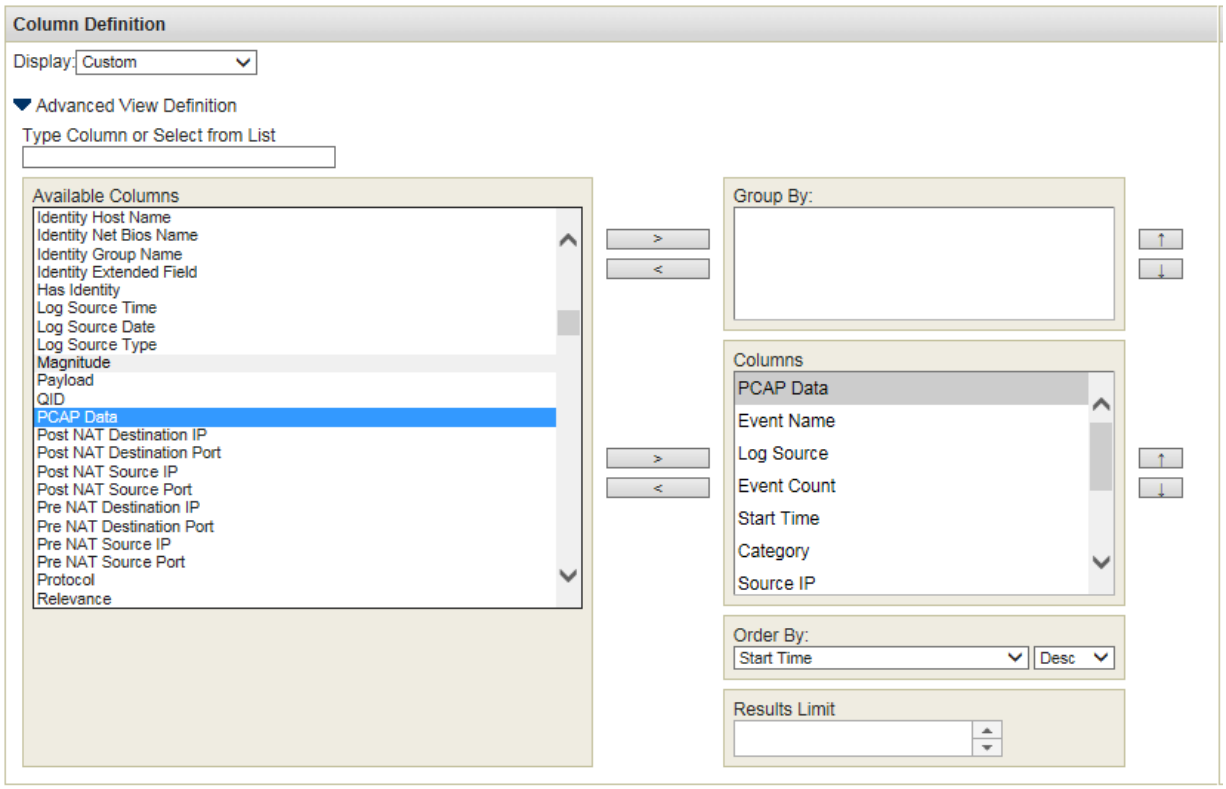
   - Using the first drop-down list box, select **PCAP data**.
   - In the second drop-down list box, select **Equals**.
   - In the third drop-down list box, select **True**.
   - Click **Add Filter**, as shown in Figure 1 on page 17.

Figure 1: Adding PCAP Data to the Columns List



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 17.

Figure 2: PCAP Data Column Search Results



- 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**.

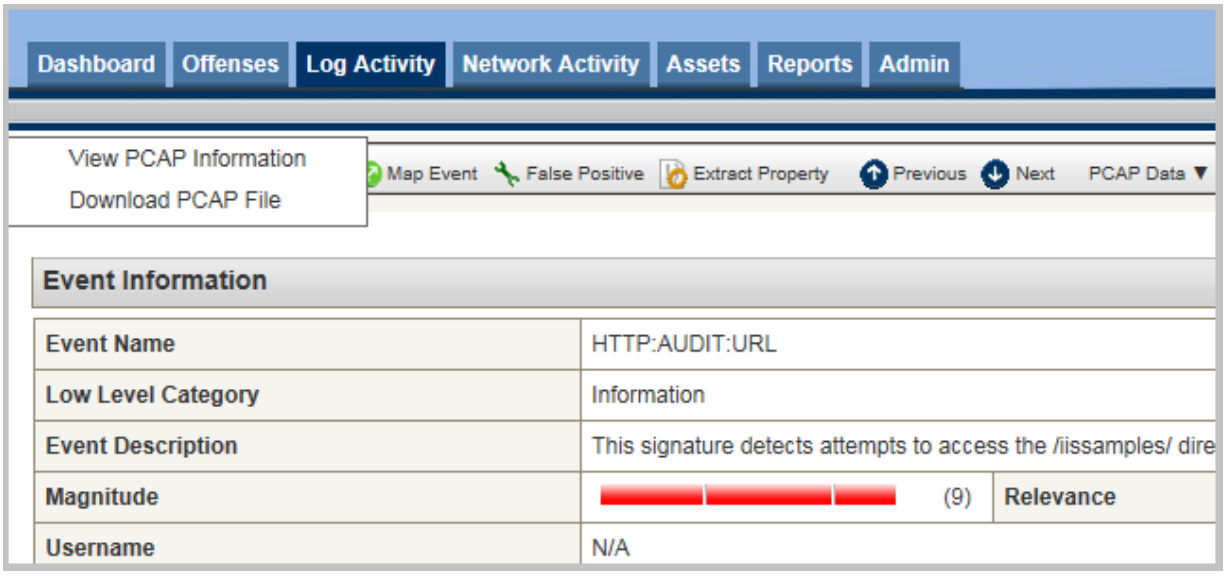
> **NOTE:** You can configure your event search using additional parameters, however, this procedure only demonstrates the required search criteria to display the PCAP data column. For more information about searching events, see the *Juniper Secure Analytics Users Guide*.

The event search results appear, displaying the PCAP Data column, as shown in Figure 3 on page 18. 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



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.

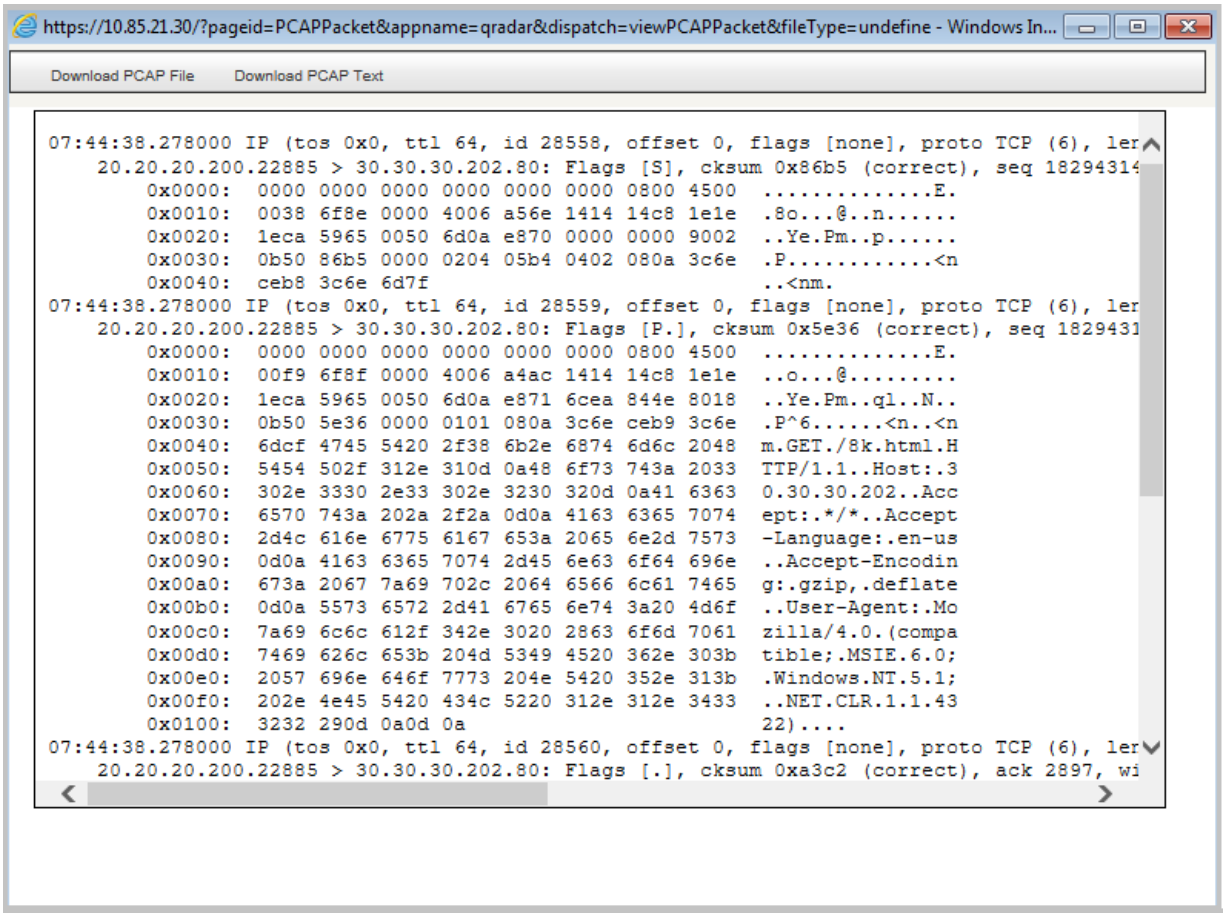
3. Choose one of the following:

   - 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



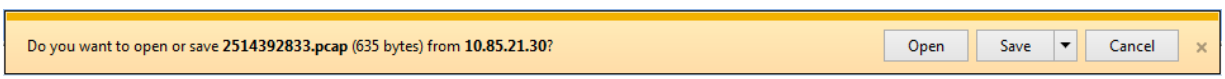
Once the file is retrieved, a pop-up window appears, displaying a readable version of the PCAP file, as shown in Figure 4 on page 20.

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 20.

Figure 5: PCAP File Save or Open Window



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**.