finjan®
Vital Security™
securing your web

Configuring Cisco Security MARS® with Vital Security™ Syslog

July 2007

For additional information, please visit www.finjan.com or contact one of our regional offices:

USA: San Jose 2025 Gateway Place Suite 180 San Jose, CA 95110, USA Toll Free: 1 888 FINJAN 8 Tel: +1 408 452 9700 Fax: +1 408 452 9701 salesna@finjan.com	**Europe: UK** 4th Floor, Westmead House, Westmead, Farnborough, GU14 7LP, UK Tel: +44 (0)1252 511118 Fax: +44 (0)1252 510888 salesuk@finjan.com
USA: New York Chrysler Building 405 Lexington Avenue, 35th Floor New York, NY 10174, USA Tel: +1 212 681 4410 Fax: +1 212 681 4411 salesna@finjan.com	**Europe: Germany** Alte Landstrasse 27, 85521 Ottobrun, Germany Tel: +49 (0)89 673 5970 Fax: +49 (0)89 673 597 50 salesce@finjan.com
Israel/Asia Pacific Hamachshev St. 1, New Industrial Area Netanya, Israel 42504 Tel: +972 (0)9 864 8200 Fax: +972 (0)9 865 9441 salesint@finjan.com	**Europe: Netherlands** Printerweg 56 3821 AD Amersfoort Netherlands Tel: +31 334 543 555 Fax: +31 334 543 550 salesne@finjan.com

Catalog name: FD-CSMVSS-03
Email: support@finjan.com
Internet: www.finjan.com

CONTENTS

1 Introduction

Cisco Security Monitoring, Analysis, and Response System (MARS) can be configured to view Finjan's Vital Security Syslog messages. This allows MARS administrators to view log information and monitor Vital Security events on a MARS appliance.

Viewing Vital Security events is enabled by manually configuring Vital Security to send logs via Syslog messages to the MARS appliance. The MARS appliance can then be configured to receive these Syslog messages and send them to a specific Vital Security category within the appliance.

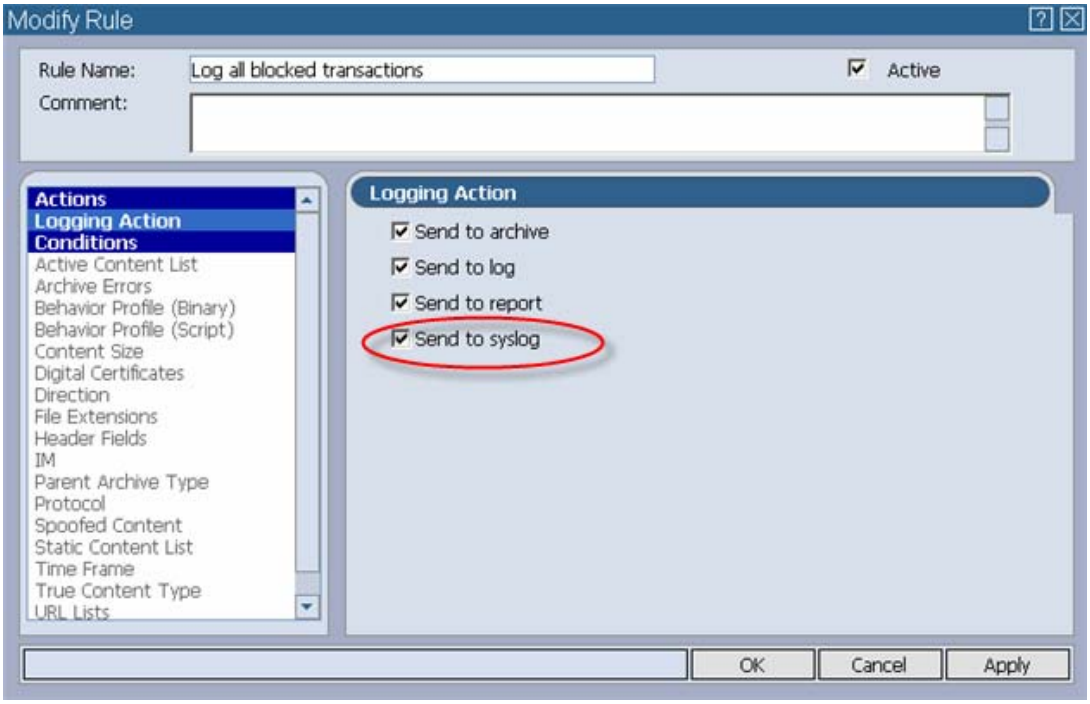
NOTE: This document was written based on Cisco Security MARS 4.2.5 and Vital Security 8.4.3.

2 Vital Security Configuration

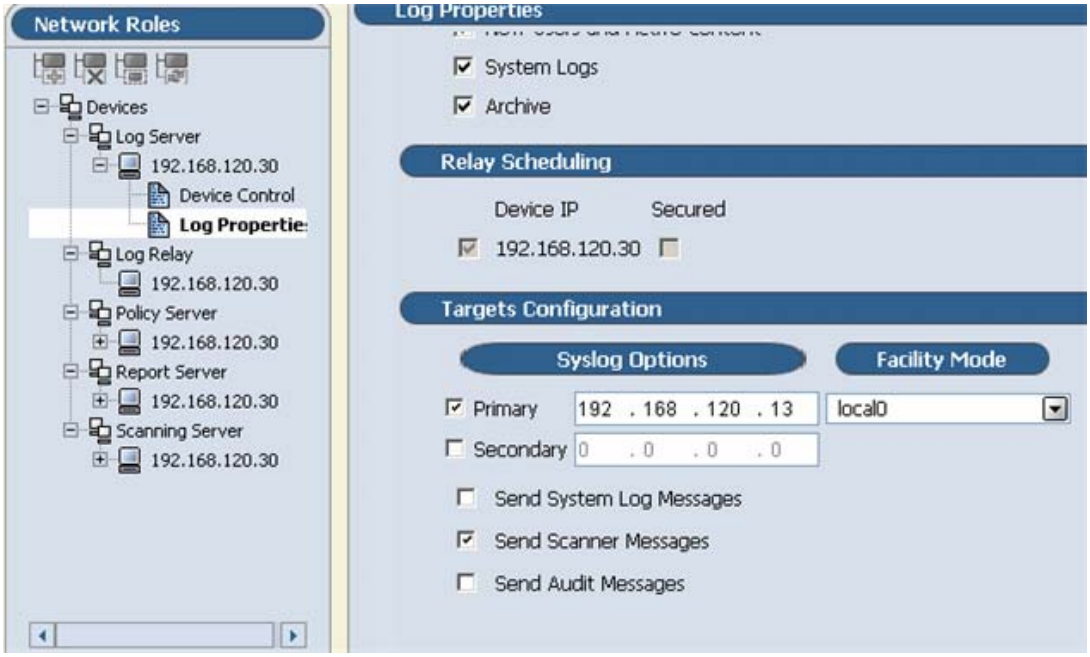
The following procedure will set up Vital Security to send Syslog files to the MARS appliance.

To configure Vital Security to send Syslog files:

1. In the Vital Security Management Console, navigate to the Policies tab.
2. Select the **Logging Block and Coach** logging policy and click on the **Duplicate** icon  .
3. Call your new policy **Log to Syslog**.
4. In your new policy, click on Web to display the rules.
5. Double-click on the **Log all blocked transactions** rule.
6. In the Logging Actions, select the **Send to Syslog** option.



7. Next, navigate to Settings → Devices → Log Server → Log Properties. In the Syslog options, enter the IP address of the MARS appliance in the Primary field. For example: **192.168.120.13**. In the Facility Mode, choose **local0**.



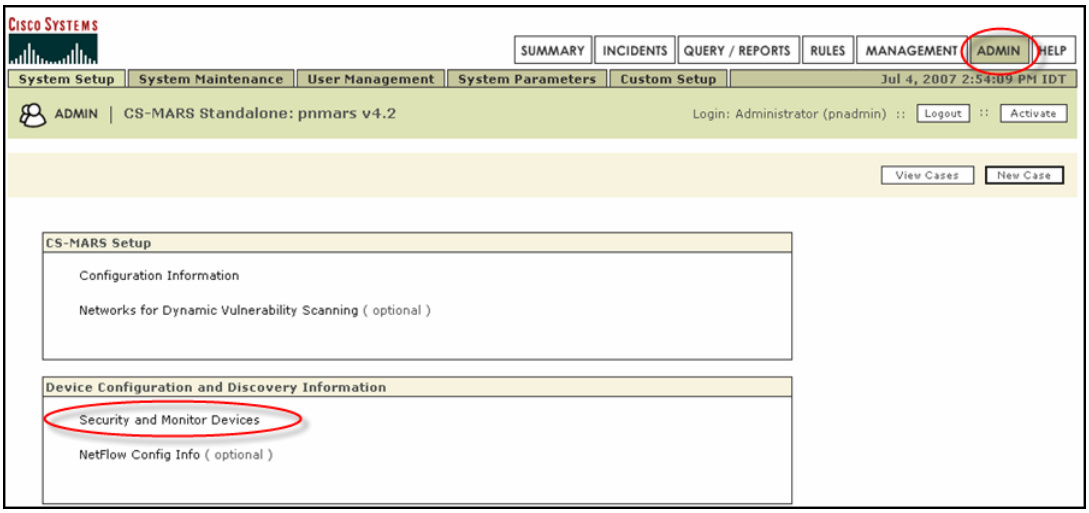
8. Click Apply and the **Commit Changes** icon. Vital Security is now set up to send logs to the MARS appliance.

3 Defining the Device Type in MARS

The next stage is to configure the Cisco MARS appliance. The first procedure involves defining the Device Type. This enables you to view Syslog messages. The second procedure involves setting up the correct Log Template which allows you to **categorize** the Syslog messages.

⇨ **To configure the MARS appliance to accept Vital Security Syslog messages:**

1. In the MARS appliance, click on **Admin** and then click on **Security and Monitor Device**s.



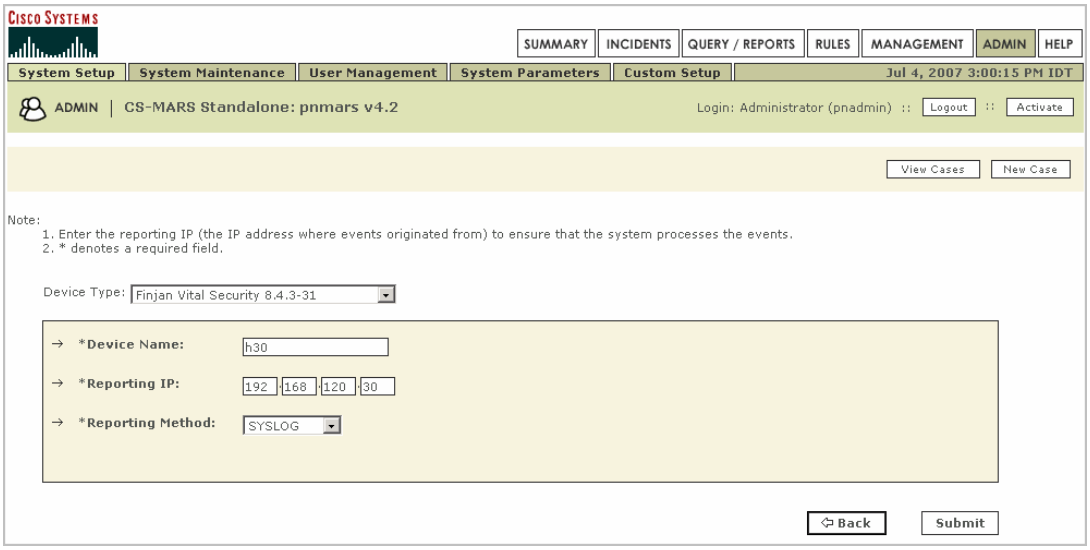
2. In the Security and Monitoring Information screen, click on **Add**.
3. In the Device Type drop-down field, choose **Finjan Vital Security 8.4.3-31**. Fill out the three fields as follows:

   Device Name: <device hostname> e.g. **h30**

   Reporting IP: <Vital Security appliance IP> e.g.**192.168.120.30**

   Reporting Method: **Syslog**

   Next, click on **Submit**.



4 Viewing the Syslog Messages

Verify that the Cisco Security MARS appliance is receiving the Vital Security Syslog messages as follows.

⇨ **To view Syslog messages in Security MARS:**

1. Navigate to **Query/Reports** and click **Edit**.
2. In the Result Format field, choose **All Matching Event Raw Messages** from the drop-down list.
3. Select the **Real Time** check box and make sure that **Raw Events** is selected.
4. Click **Apply**. Next, click **Submit**. The following is an example of the Syslog messages that will be displayed.

Query Results

Event ID	Event Type	Time	Reporting Device	Raw Message
		PM IDT		Transaction ID: 111843F1-0005-781E-EBB0-0000000000B0; Client IP: 10.194.5.95; URL: http://www.hotbar.com; Block reason: Access Denied! The requested URL is a Spyware site. The ID of the transaction is 111843F1.
207679	*Spyware Site*	Jul 16, 2007 2:25:43 PM IDT	*h30*	<134>: Vital Security Web Event - Transaction time: 07/16/2007 14:24:46; Transaction ID: 732043F2-0005-781E-EBB0-0000000000B1; Client IP: 10.194.5.95; URL: http://www.hotbar.com; Block reason: Access Denied! The requested URL is a Spyware site. The ID of the transaction is 732043F2.
207680	*Spyware Site*	Jul 16, 2007 2:25:43 PM IDT	*h30*	<134>: Vital Security Web Event - Transaction time: 07/16/2007 14:24:47; Transaction ID: 949043F2-0005-781E-EBB0-0000000000B4; Client IP: 10.194.5.95; URL: http://www.hotbar.com; Block reason: Access Denied! The requested URL is a Spyware site. The ID of the transaction is 949043F2.
207681	*Unknown Device Event Type*	Jul 16, 2007 2:25:59 PM IDT	*h30*	parsing error: <134>: Vital Security Web Event - Transaction time: 07/16/2007 14:24:53; Transaction ID: 17C843F8-0005-781E-BBB0-000000000199; Client IP: 10.194.5.95; URL: http://www.playboy.com; Block reason: Forbidden URL. URL Category is **Adult/Sexually Explicit** . The ID of the transaction is 17C843F8.
207682	*Unknown Device Event Type*	Jul 16, 2007 2:25:59 PM IDT	*h30*	parsing error: <134>: Vital Security Web Event - Transaction time: 07/16/2007 14:24:56; Transaction ID: 451843FC-0005-781E-EBB0-0000000000B7; Client IP: 10.194.5.95; URL: http://www.playboy.com; Block reason: Forbidden URL. URL Category is **Adult/Sexually Explicit** . The ID of the transaction is 451843FC.
207683	*Spyware Site*	Jul 16, 2007 2:25:59 PM IDT	*h30*	<134>: Vital Security Web Event - Transaction time: 07/16/2007 14:24:57; Transaction ID: F1D843FC-0005-781E-EBB0-0000000000B8; Client IP: 10.194.5.95; URL: http://www.hotbar.com; Block reason: Access Denied! The requested URL is a Spyware site. The ID of the transaction is F1D843FC.

5 Configuring Log Parser Templates in MARS

In order to categorize the relevant log messages, the specific Log Parser Template must be configured. The **Key Pattern** field within the Template is based on a keyword/s of your choice taken from the Syslog message.

Below are a few examples of configuring log parser templates.

5.1 Log Parser Template: Blocked Transactions

This procedure shows you how to configure the Cisco Security MARS appliance to display all Transactions that were blocked by Vital Security.

This category covers all blocked transactions – including other categories you might have specified separately in log parser templates – therefore - **it is strongly recommended to use this as a stand-alone category**.

The transactions are captured based on the Key Pattern word **Block** which appears in the phrase **Block Reason** in all Syslog messages for blocked transactions.

The following is an example of a Syslog message appearing in Cisco MARS.

```
<134>: Vital Security Web Event - Transaction time:
07/08/2007 10:35:29; Transaction ID: 1DE7EDF88EE5-
781E-FBB0-0000-0000191B; Client IP: 10.194.5.27;
URL: http://hotbar.com/favicon.ico; Block reason:
Access Denied! The requested URL is a Spyware site.
The ID of the transaction is 1DE7EDF8.
```

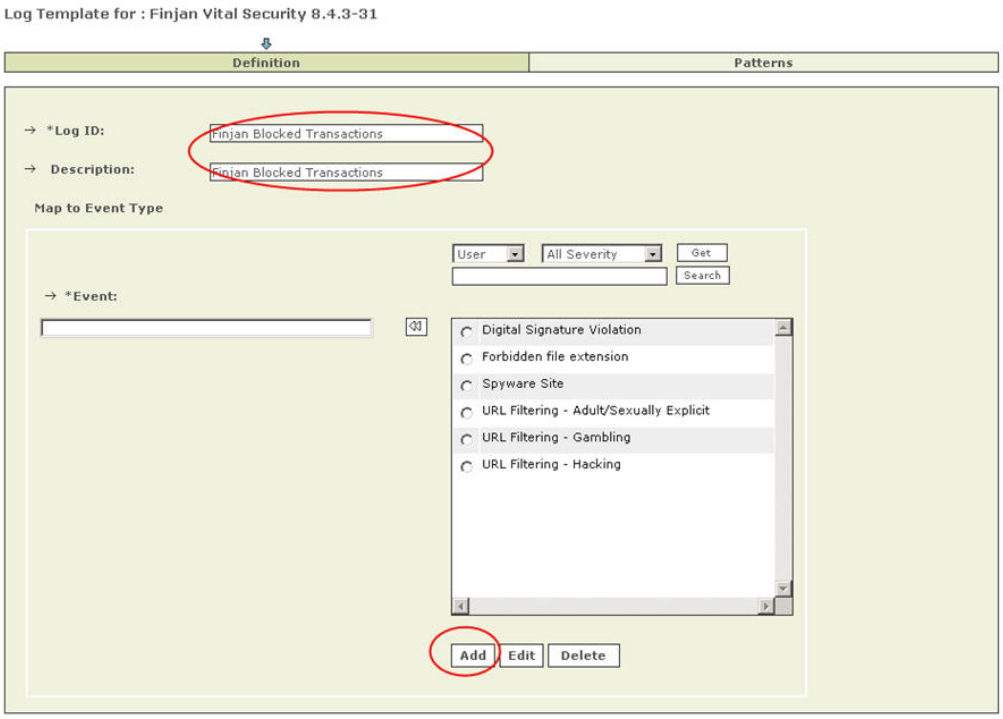
NOTE: All Syslog messages contain the word "Block". Therefore to view all blocked transactions, it is recommended to use this key pattern.

To configure Log Parser Template: Blocked Transactions:

1. Navigate to Custom Setup and click on **Custom Defined Log Parser Templates.**
2. In the Log Template screen, click on **Add** at the bottom of the screen and enter the following information:

   Log ID: **Finjan Blocked Transaction**

   Description: **Finjan Blocked Transaction**



3. Click on **Add** again. In the Event Type Definition window, enter the following information:

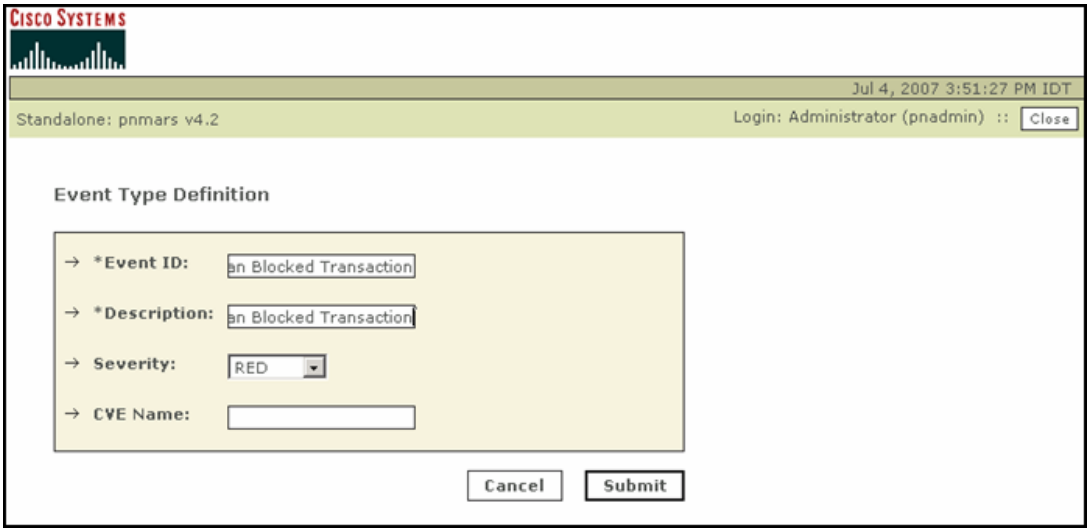
   Event ID: **Finjan Blocked Transaction**

   Description: **Finjan Blocked Transaction**

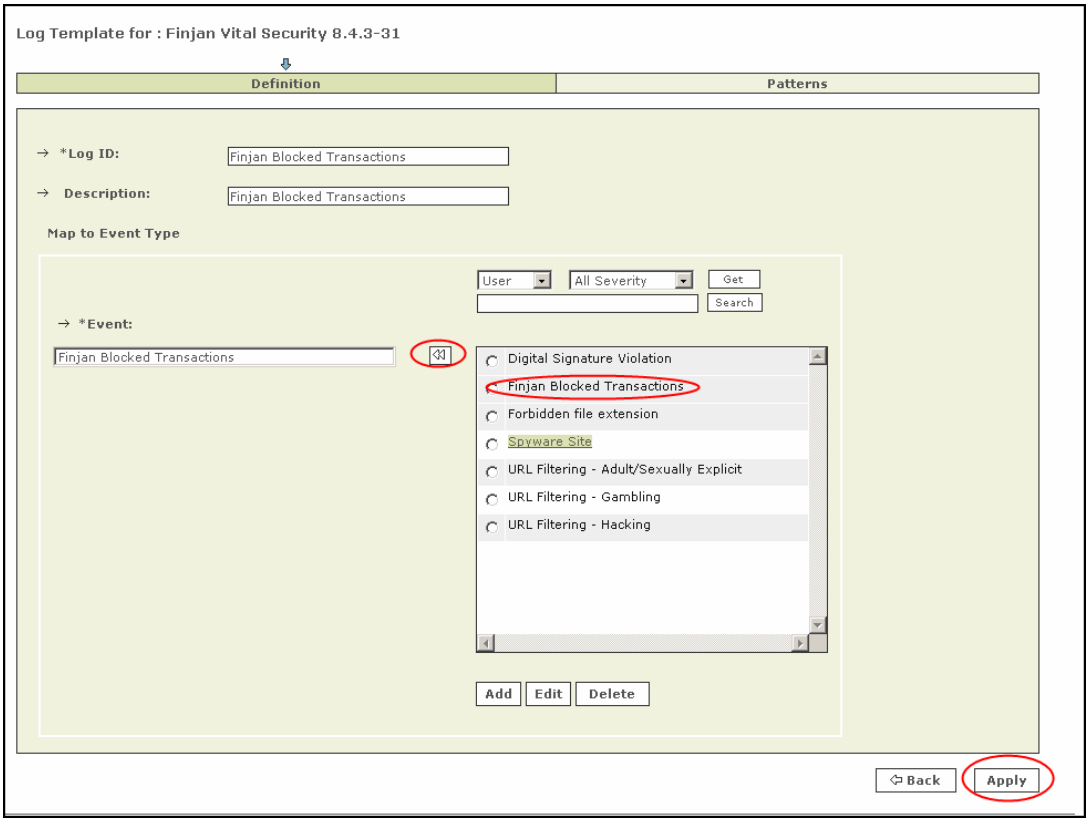
   Severity: **Red**

   CVE Name: <Leave Blank>

   Next, click on **Submit**.



4. Under the Event section, click on **Finjan Blocked Transaction**, and then click on the double arrow to move it into the Event field. Click on **Apply** at the bottom of the screen.



5. Next, click on **Patterns** at the top right of the screen.
6. In the new screen, click on **Add** and fill in the following fields:

   Key Pattern: **Block (NOTE: The key pattern chosen here must appear <u>exactly</u> as in the Syslog Message. The word Block appears in all Syslog messages)**

   Parsed Field: **None**

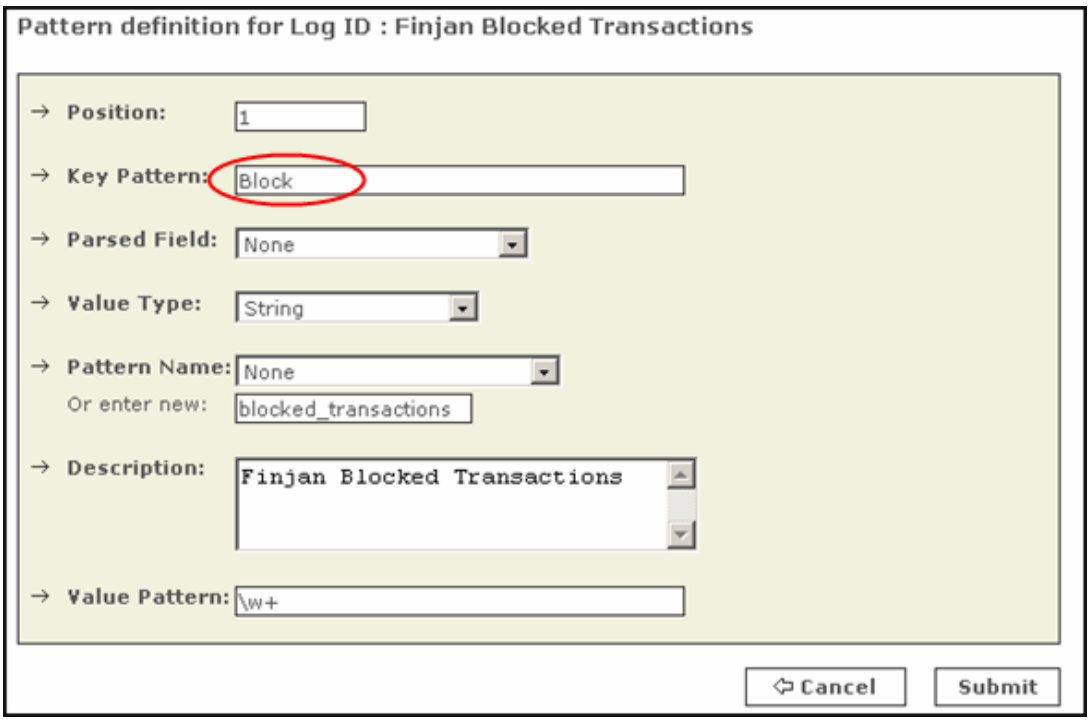
   Value Type: **String**

   Pattern (new): **finjan_blocked**

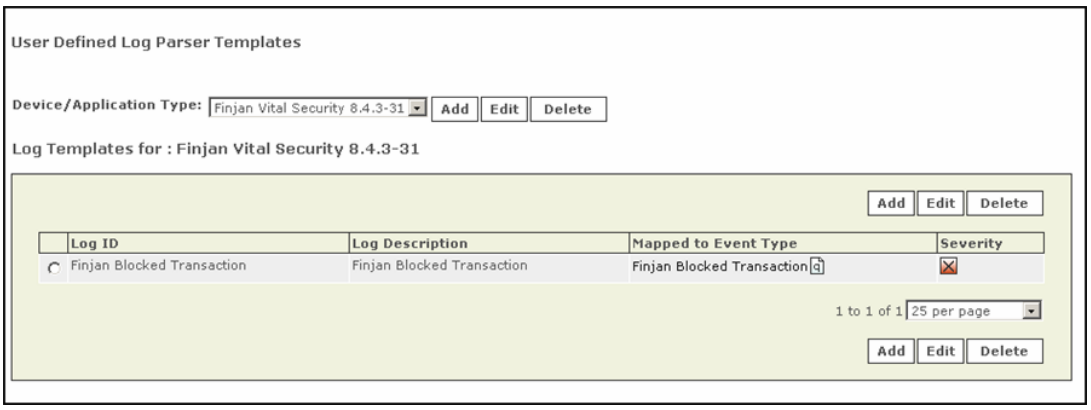
   Description: **Finjan Blocked Transaction**

   Value Pattern: **\w+**

   Click on **Submit**.



7. Click on **Submit** again. The following screen is displayed.



The MARS appliance is now configured to categorize all blocked events as Finjan Blocked Transactions.

5.2 Log Parser Template: Spyware Site

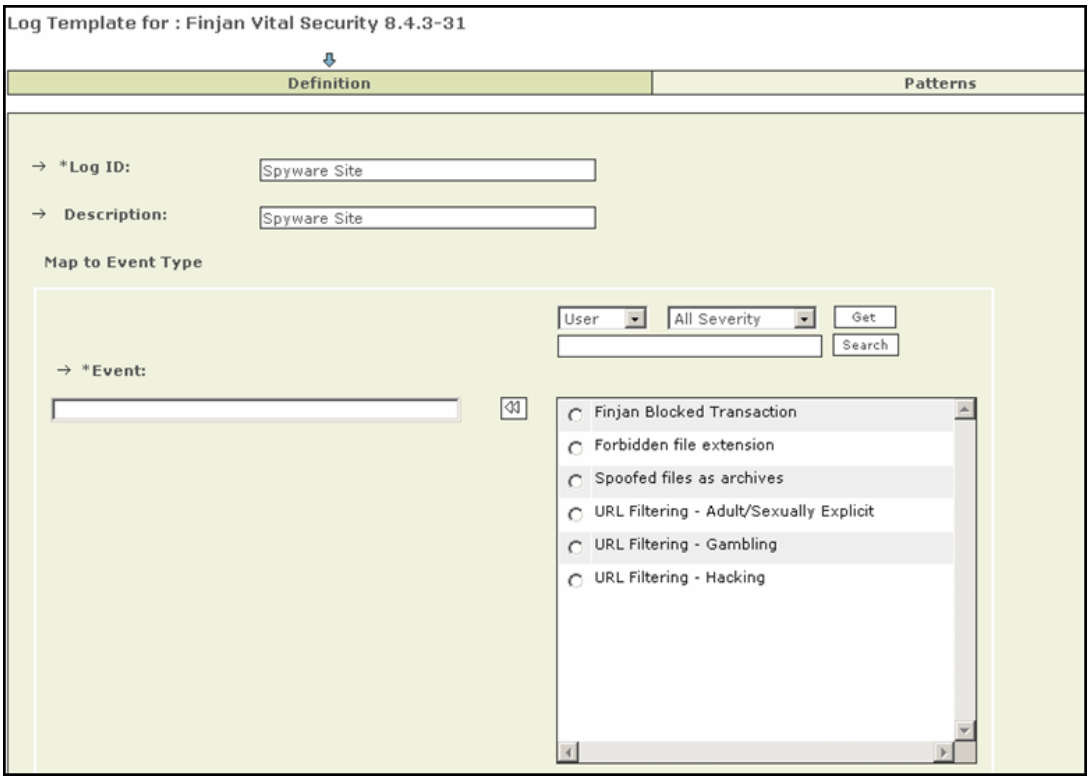
Many other log parser templates can be created to capture specific blocked transactions. This procedure shows you how to configure the Cisco Security MARS appliance to display blocked Spyware Sites by Vital Security.

⇨ **To configure Log Parser Template: Spyware Site:**

1. Navigate to Custom Setup and click on **Custom Defined Log Parser Templates.**
2. In the Log Template screen, click on **Add** at the bottom of the screen and enter the following information:

   Log ID: **Spyware Site**

Description: **Spyware Site**



3. Click on **Add** again. In the Event Type Definition window, enter the following information:

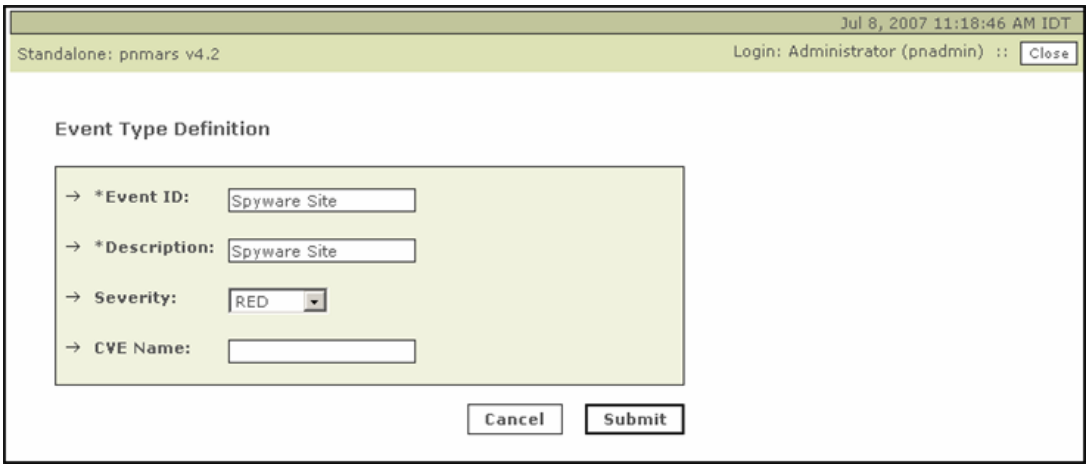
   Event ID: **Spyware Site**

   Description: **Spyware Site**

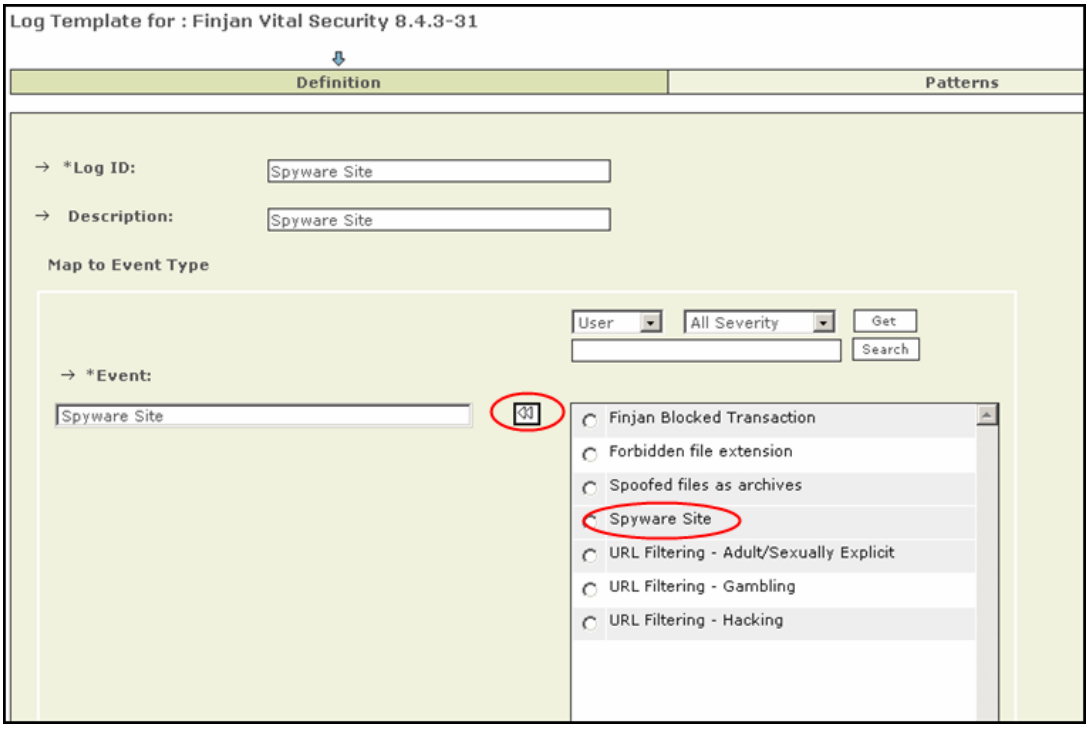
   Severity: **Red**

   CVE Name: <Leave Blank>

   Next, click on **Submit**.



4. Under the Event section, click on **Spyware Site**, and then click on the double arrow to move it into the Event field. Click on **Apply** at the bottom of the screen.



5. Next, click on **Patterns** at the top right of the screen.
6. In the new screen, click on **Add** and fill in the following fields:

   Key Pattern: **Spyware Site (NOTE: The key pattern chosen here must appear exactly as in the Syslog Message.)**

   Parsed Field: **None**

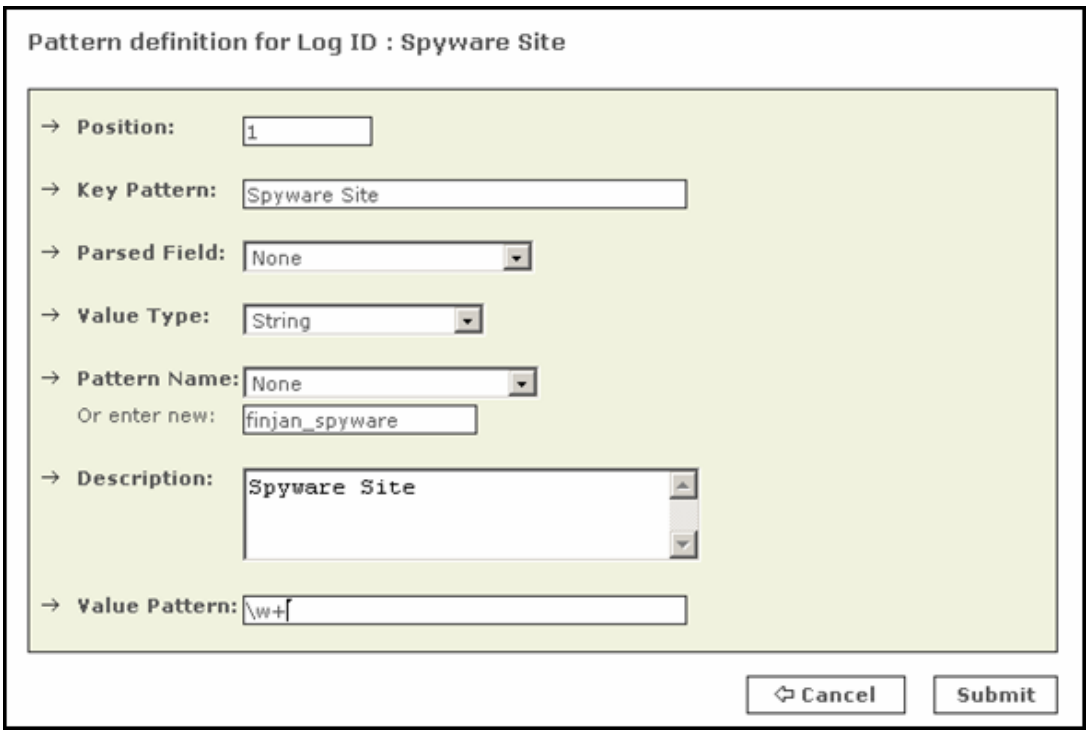
   Value Type: **String**

   Pattern (new): **finjan_spyware**

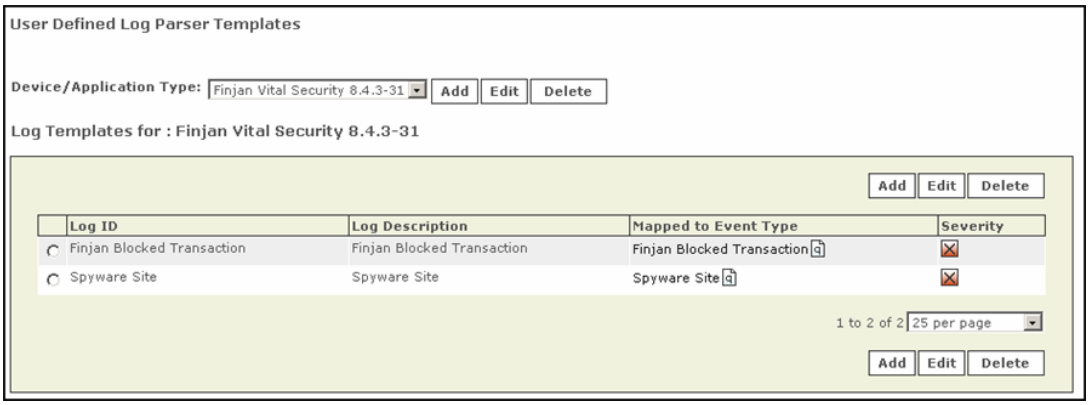
   Description: **Spyware Site**

   Value Pattern: **\w+**

   Click on **Submit**.



7. Click on **Submit** again. The following screen is displayed.



The MARS appliance is now configured to receive Syslog messages from Vital Security appliance and categorize all Spyware site events as Spyware Sites.

5.3 Log Parser Template: Digital Signature Violation

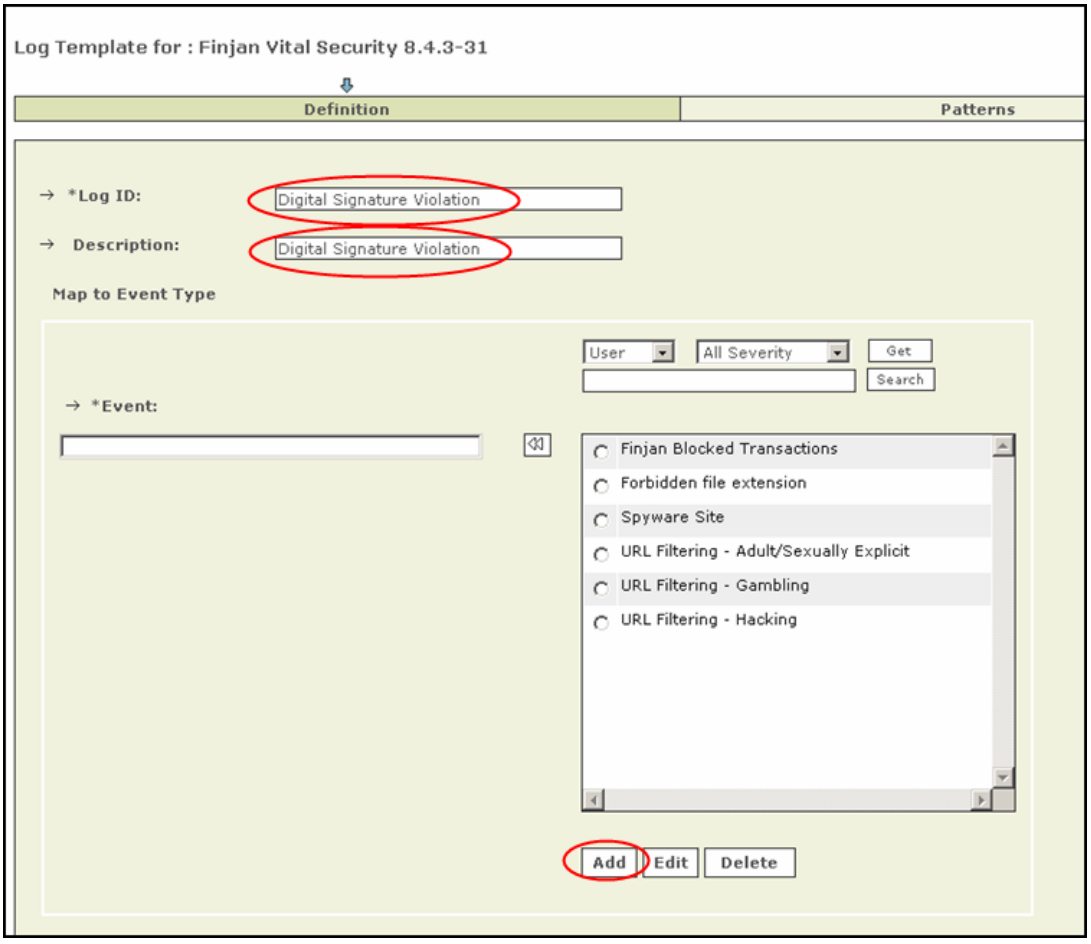
This procedure shows you how to configure the MARS appliance to display Digital Signature Violations blocked by Vital Security.

⇨ **To configure Log Parser Template: Digital Signature Violation:**

1. Navigate to Custom Setup and click on **Custom Defined Log Parser Templates.**
2. In the Log Template screen, click on **Add** at the bottom of the screen and enter the following information:

Log ID: **Digital Signature Violation**

Description: **Digital Signature Violation**



3. Click on **Add** again. In the Event Type Definition window, enter the following information:

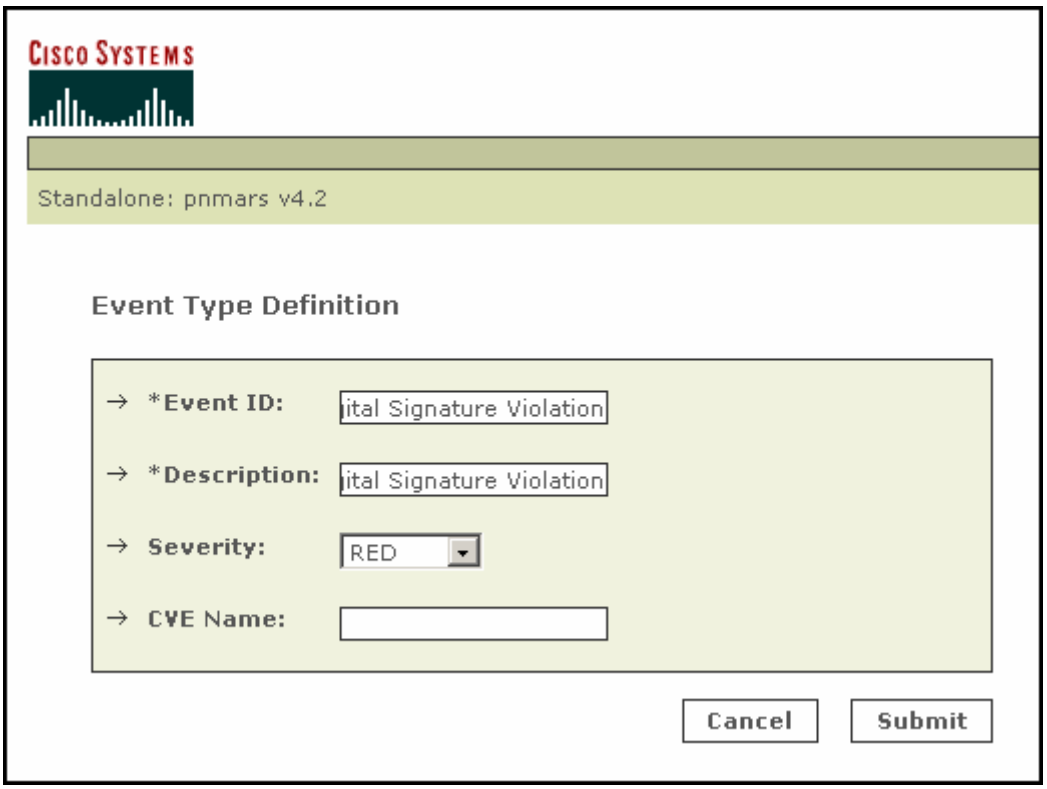
   Event ID: **Digital Signature Violation**

   Description: **Digital Signature Violation**

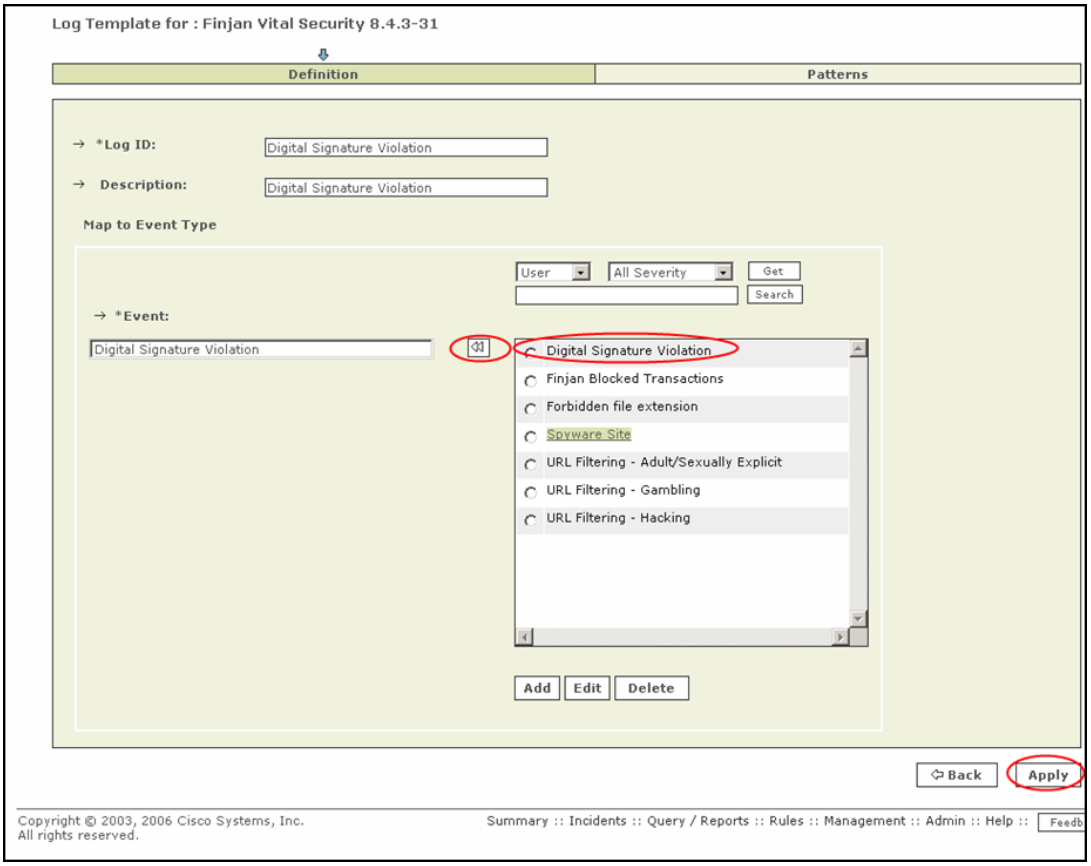
   Severity: **Red**

   CVE Name: <Leave Blank>

   Next, click on **Submit**.



4. Under the Event section, click on **Digital Signature Violation**, and then click on the double arrow to move it into the Event field. Click on **Apply** at the bottom of the screen.



5. Next, click on **Patterns** at the top right of the screen.
6. In the new screen, click on **Add** and fill in the following fields:

   Key Pattern: **digital signature violation ((NOTE: The key pattern chosen here must appear exactly as in the Syslog Message.)**

   Parsed Field: **None**

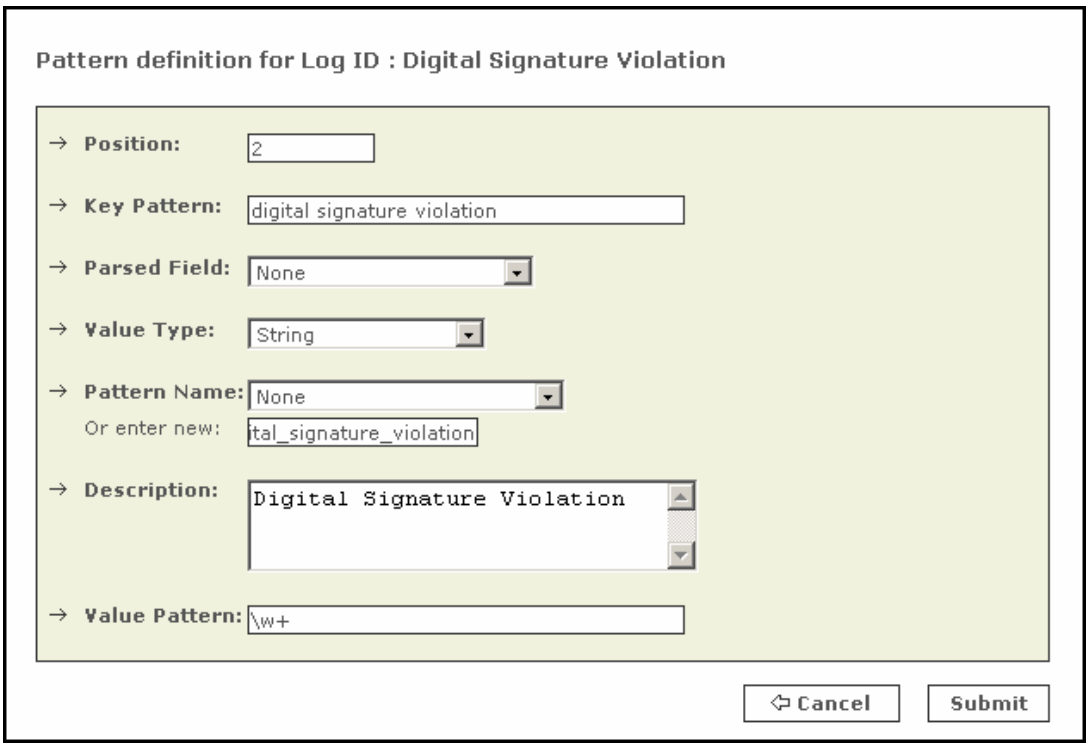
   Value Type: **String**

   Pattern (new): **digital_signature_violation**

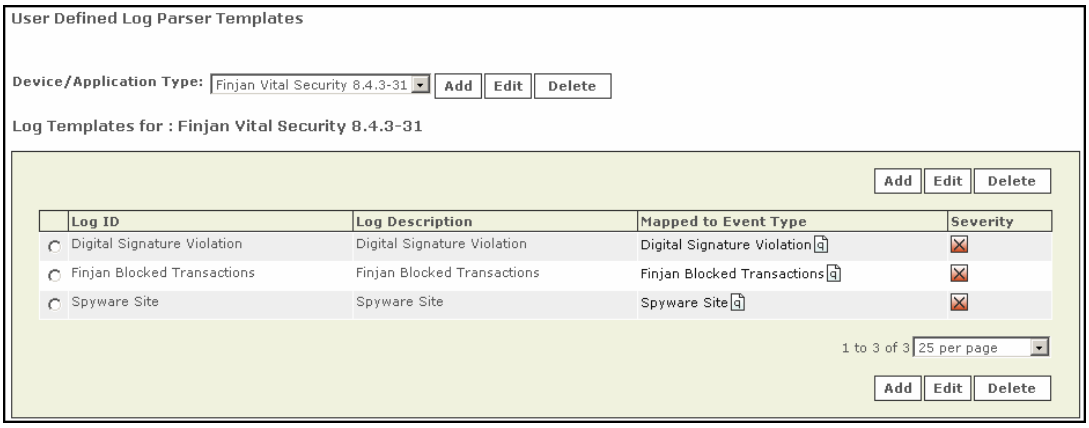
   Description: **Digital Signature Violation**

   Value Pattern: **\w+**

   Click on **Submit**.



7. Click on **Submit** again. The following screen is displayed.



The MARS appliance is now configured to categorize all Digital Signature Violation events in Finjan Syslog messages.

Continue with this procedure as many times as you like to add more categories to the Syslog messages.

6 Verifying Categorization of Syslog Messages

In order to check that you have set up the category configuration as required, you can run the appropriate report.

⇨ **To run a Report on Vital Security Syslog messages:**

1. Click on **Queries/Reports**.

2. Click on **Edit** and Filter by Time as **required**.
3. Click **Apply**.
4. Click **Submit Inline**. The report is displayed below.