Monitoring Content Security

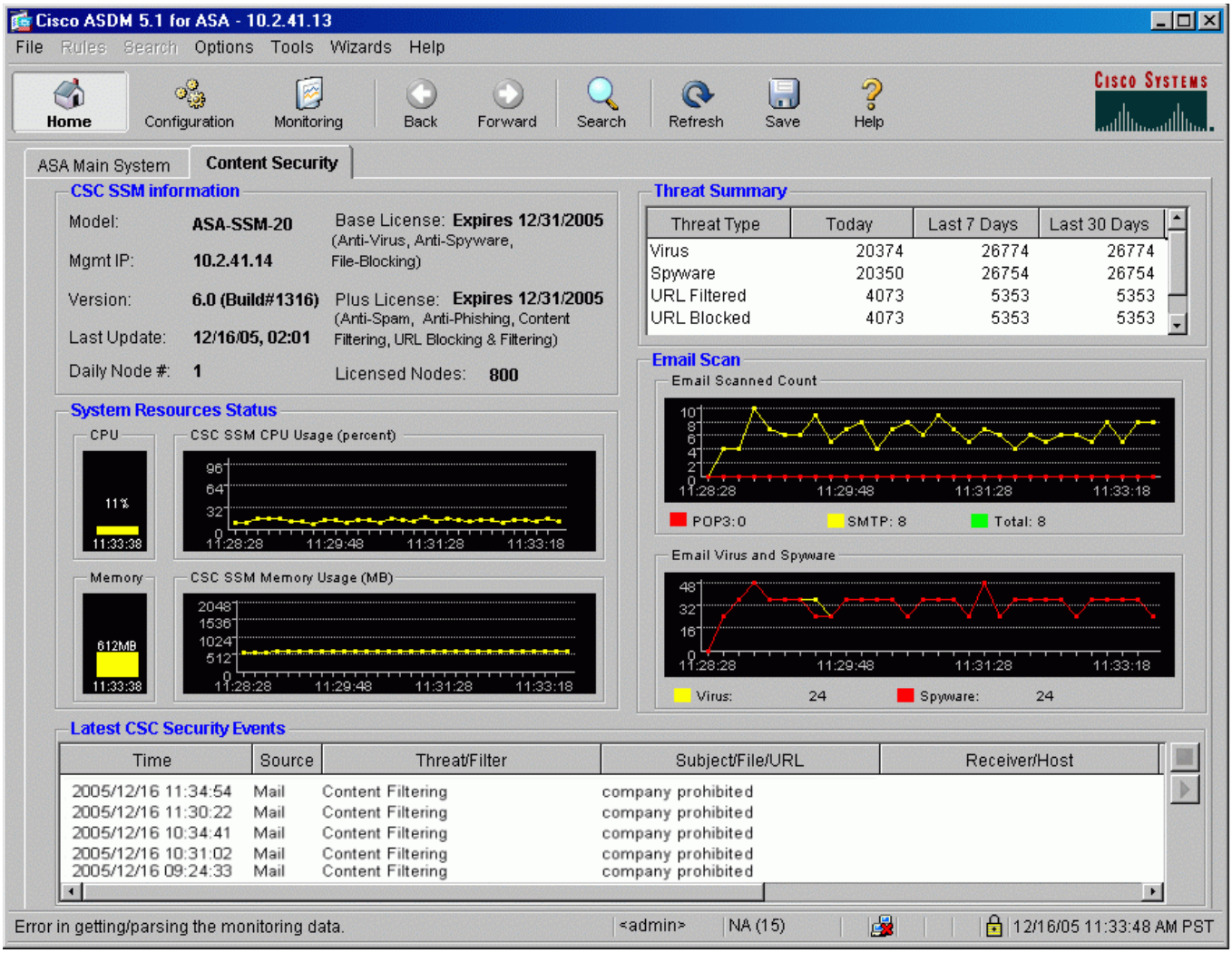
This chapter describes monitoring content security from ASDM, and includes the following sections:

Features of the Content Security Tab

After you have connected to the CSC SSM, the Content Security tab displays, as shown in Figure 7-1 on page 7-2. The Content Security tab shows you content security status at a glance, including:

- CSC SSM Information — Displays the product model number, IP address of the device, version and build number of the CSC SSM software, and important information
- Threat Summary — Displays a table summarizing threats detected today, within the last 7 days, and within the last 30 days
- System Resources Status — Allows you to view CPU and memory utilization on the SSM
- Email Scan — Provides a graphical display of number of email messages scanned and number of threats detected in the scanned email
- Latest CSC Security Events — Lists the last 25 security events that were logged

Figure 7-1 Content Security Tab



Click the Help icon to view more detailed information about the information that appears in this window.

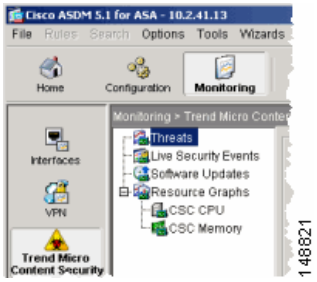
Monitoring Content Security

Click **Monitoring > Trend Micro Content Security** to display the Monitoring options. These options are:

- Threats—View graphs that display recent threat activity in the following categories:
- Live Security Events—Displays a report of recent security events (content-filtering violations, spam, virus detections, spyware detections, and so on) for monitored protocols
- Software Updates—Displays the version and last update date/time for content security scanning components (virus pattern file, scan engine, spyware/grayware pattern, and so on)
- Resource Graphs—Displays graphs of CPU utilization and memory utilization for the SSM

The appearance of the Monitoring options in ASDM is shown in Figure 7-2:

Figure 7-2 Content Security Monitoring Options in ASDM



Monitoring Threats

When you click Threats in the Monitoring pane, as shown in Figure 7-2, you can choose up to 4 categories of threats for graphing. You can display recent activity in the following categories:

- Viruses and other threats detected
- Spyware blocked
- Spam detected (this feature requires the Plus license)
- URL filtering activity and URL blocking activity (this feature requires the Plus license)

For example, assume you have both the Base and Plus license, and you choose all four threat types for monitoring. The graphs might appear as shown in Figure 7-3:

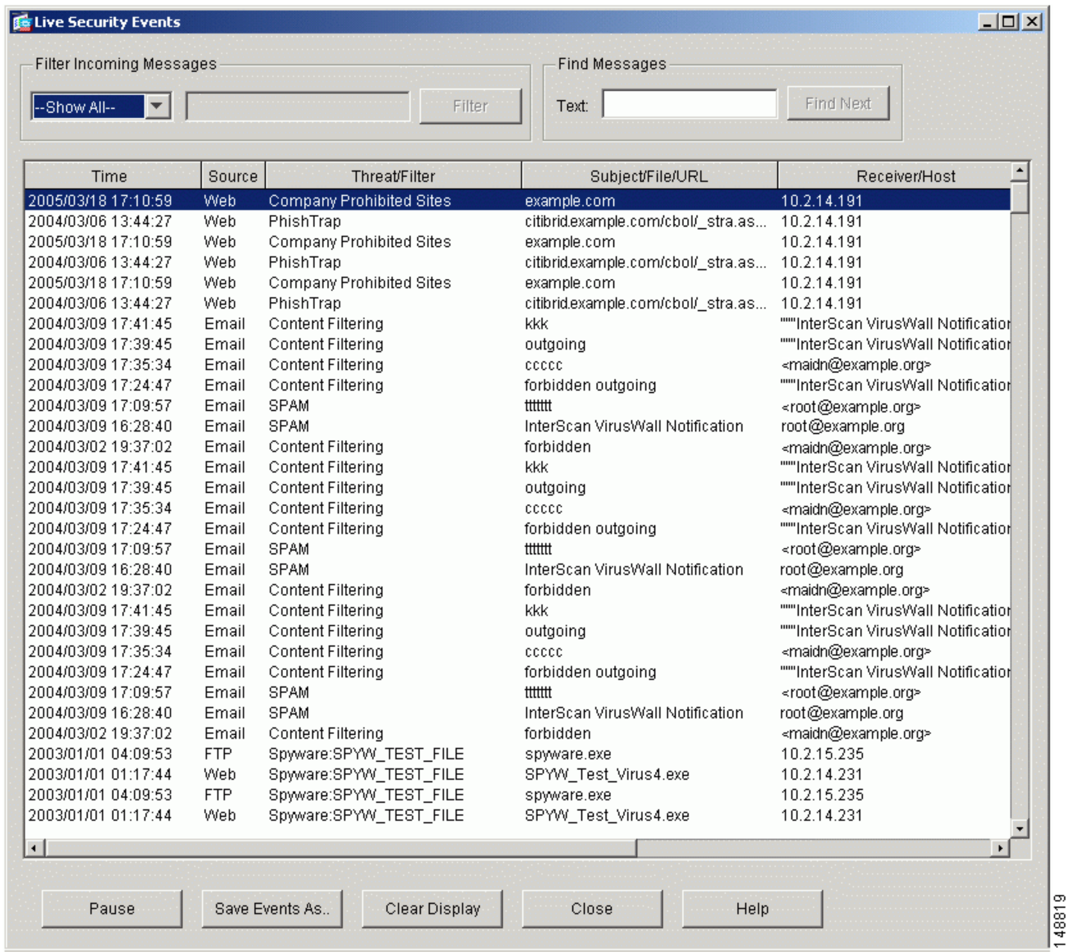
Figure 7-3 Threat Monitoring Graphs

The graphs refresh on frequent intervals (every 10 seconds), allowing you to see recent activity at a glance. See the online help for more information.

Monitoring Live Security Events

When you click Live Security Events in the Monitoring pane, after you click **View**, a report similar to the example in Figure 7-4 is created:

Figure 7-4 Live Security Events Monitoring Report

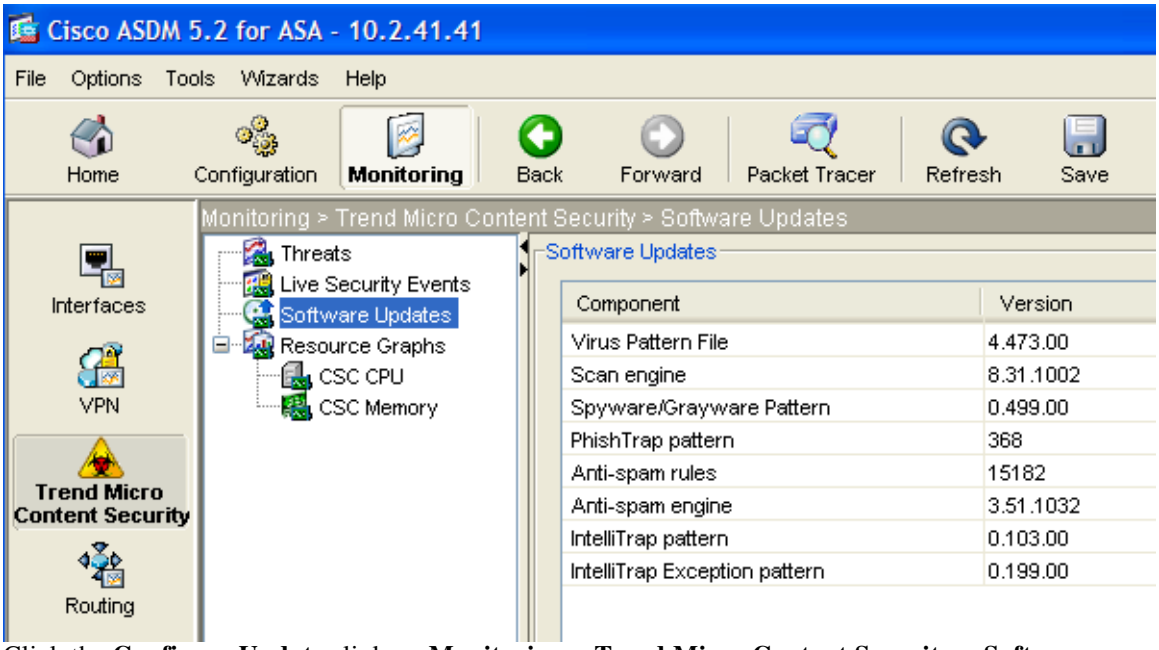


This report lists events detected by CSC SSM. The **Source** column displays “Email” for both SMTP and POP3 protocols. The horizontal and vertical scroll bars allow you to view additional report content. Filters at the top of the screen allow you to refine your search for specific events. See the online help for more information.

Monitoring Software Updates

When you click Software Updates in the Monitoring pane, as shown in Figure 7-5, the following information about the CSC SSM components displays:

Figure 7-5 Software Updates Monitoring Window



Click the **Configure Updates** link on **Monitoring > Trend Micro Content Security > Software Updates** in ASDM to display the Scheduled Update window in the CSC SSM console. See Figure 2-4 on page 2-5.

The Scheduled Update window allows you to specify the interval at which CSC SSM receives component updates from the Trend Micro ActiveUpdate server, which can be daily, hourly, or every 15 minutes.

You can also update components on demand via the Manual Update window in the SCS SSM console. See Figure 5-1 on page 5-2. Also see the online help for more information about both types of updates.

Monitoring Resources

When you click Resource Graphs in the Monitoring pane, there are two types of resources you can monitor, CPU usage, and memory. If these resources are running close to 100% usage, you might want to:

- Upgrade to ASA-SSM-20 (if you are currently using ASA-SSM-10), or
- Purchase another ASA appliance

To view CPU or memory usage, choose the information for viewing and click **Show Graphs**. For example:

Figure 7-6 Memory Monitoring Graphs