



## INTELLIGENT EVENT MODULE BASICS

The Check Point FireWall-1 Intelligent Event Module (IEM) enables you to automate real-time monitoring of the Check Point® FireWall-1® (version R55) solution and capture the critical information you need for effective enterprise management.

The Check Point FireWall-1 IEM provides *ConsoleWorks*® with a watch-list of text messages, including error codes, system warnings, and status alerts, produced by FireWall-1. *ConsoleWorks* watches for these messages, called Events, in the data streams of your FireWall-1-secured applications.

### Events

When *ConsoleWorks* detects an Event, it alerts you to the Event as it is happening, records the circumstances surrounding the Event, and automatically performs the default or customer-configured responses associated with that Event.

### Scans

IEMs come with Events pre-arranged in logical groupings, called Scans™. Working with a Scan—or a combination of Scans—instead of hundreds of individual Events simplifies managing Events across your enterprise.

## CHECK POINT FIREWALL-1 IEM AT A GLANCE

Events:	6
Scans:	1 Master 3 Event Severity
Filename:	<code>cw_iem-checkpoint_firewall1-0002.bin</code>
License Required:	<code>CONWRKS-DB-CHECKPOINT.lic</code>
Connector Required:	Serial or Telnet

## USING THE CHECK POINT FIREWALL-1 IEM

To use this IEM, complete the following tasks:

1. Download the IEM from the TDi web site.
2. Import the IEM into *ConsoleWorks*.
3. Associate the Scans from the IEM with the applications you want to manage.

### To Download the IEM

1. Install the license for the Check Point FireWall-1 IEM. To obtain this license, contact your TDi Solutions Team Manager ([sales@tditx.com](mailto:sales@tditx.com)).
2. Move to the TDi web site ([www.tditx.com/support\\_iemdownloads.asp](http://www.tditx.com/support_iemdownloads.asp)).
3. On the Product Downloads page, locate and click **Check Point FireWall-1**.
4. In the Connect to support2.tditx.com dialog box, enter your User name and Password, and click **OK**. To obtain a User name and Password, contact TDi Support ([support@tditx.com](mailto:support@tditx.com)).
5. Save the file (`cw_iem-checkpoint_firewall1-0002.bin`) to a directory accessible from your client workstation.

### To Import the IEM

1. On the *ConsoleWorks* main menu, click **Admin > Database > Import IEM**.
2. On the Import IEM page, click **Browse**.
3. On the Choose file dialog box, locate and double-click `cw_iem-checkpoint_firewall1-0002.bin`.
4. On the Import IEM page, click **Import IEM**, and wait for the **IEM import completed** message to appear on the page before associating the IEM's Scans.

### To Associate the Scans

Associate the Scans with the FireWall-1-secured applications you want *ConsoleWorks* to monitor. When you associate Scans with an application, you are specifying that *ConsoleWorks* scan the data streams of that application for the Events contained in the Scans.

#### Example: To associate CPFW1\_WARNING Scan

1. On the *ConsoleWorks* main menu, click **Manage > Scans > Show Scans**.
2. On the Show Scans page, in the Scans column, click **CPFW1\_WARNING**.
3. On the Scan: CPFW1\_WARNING page, in the Unassociated Consoles column, select the check boxes next to the names of the managed applications you want to associate with the Scan.
4. Click **Update Scan**.



For detailed instructions on associating Scans, please refer to the *ConsoleWorks* user's guide.

## SCANS AVAILABLE IN THE CHECK POINT FIREWALL-1 IEM

---

The Check Point FireWall-1 IEM contains a Master Scan and three Event Severity Scans.

### Master Scan

The Master Scan, **CPFW1**, is the top-level Scan. It references all the other Scans in the IEM. When you associate the Master Scan with an application, you are specifying that *ConsoleWorks* scan the data streams of that application for any of the IEM's 6 Events.

### Event Severity Scans

The Check Point FireWall-1 IEM contains three Event Severity Scans. Use one or more of these Scans to monitor applications for Events based on their Severity level.

The IEM provides the following Event Severity Scans:

- CPFW1\_MINOR 2 Events
- CPFW1\_WARNING 2 Events
- CPFW1\_INFORMATIONAL 2 Events

## SAMPLE CHECK POINT FIREWALL-1 IEM EVENTS

---

The Check Point FireWall-1 IEM provides you with names, message texts, Severity ratings, and explanations for Events produced by the FireWall-1 solution.

The following section displays samples of the information you receive for each Event in the Check Point FireWall-1 IEM.

### Sample Event 1

**Name:** CPFW1\_DROP\_INCOMING  
**Message:** 4:08:15 192.16.23.32 drop product VPN-1 & Firewall-1 src 192.168.146.12 s\_port 2523 dst 192.168.10.2 service ms-sql-m proto udp rule 49>  
**Severity:** WARNING  
**Explanation:** An incoming packet was examined and dropped. The rule base indicates this packet should be ignored. No error will be returned to the packet sender.

### Sample Event 2

**Name:** CPFW1\_ACCEPT\_OUTGOING  
**Message:** 4:08:15 192.16.3.32 accept product VPN-1 & Firewall-1 src 10.5.5.1 s\_port 4523 dst 192.168.10.2 service http proto tcp xlatesrc rule 49>  
**Severity:** INFORMATIONAL  
**Explanation:** An outgoing packet was examined and accepted. The rule base indicates this is a valid packet for the system to send.

---

© 2007 TECSys Development, Inc. The information in this document is provided by TECSys Development, Inc. as-is without warranty of any kind and is subject to change without notice. The warranties for TECSys Development, Inc. solutions are set forth in the limited warranty statements accompanying such solutions. Nothing herein shall be construed as constituting an additional warranty. All products or company names mentioned in this document are trademarks or registered trademarks of their respective owners. Portions of the technology within the *ConsoleWorks* server are protected under US Patent number 6,505,245. *ConsoleWorks* is a registered trademark of TECSys Development, Inc.