UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
WACO DIVISION

DATAMONITOR SYSTEMS LLC, Plaintiff v. CISCO SYSTEMS, INC. Defendant	**Case No. 6:24-cv-00186** **JURY TRIAL DEMANDED**

ORIGINAL COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff Datamonitor Systems LLC ("Plaintiff" or "Datamonitor") hereby files this Original Complaint for Patent Infringement against Defendant Cisco Systems, Inc. ("Defendant" or "Cisco"), and alleges, on information and belief, as follows:

THE PARTIES

1. Datamonitor Systems LLC is a limited liability company organized and existing under the laws of the State of Delaware.

2. On information and belief, Cisco Systems, Inc. ("Cisco") is a corporation organized under the laws of Delaware and maintains a regular place of business at 12515 Research Blvd Bldg 3, Austin, Texas 78759.

JURISDICTION AND VENUE

3. This action arises under the patent laws of the United States, 35 U.S.C. § 1, *et seq*. This Court has subject matter jurisdiction under 28 U.S.C. §§ 1331 and 1338(a).

4. Defendant has committed acts of infringement in this judicial district.

5. On information and belief, Defendant maintains regular and systematic business interests in this district and throughout the State of Texas including through their representatives, employees, and physical facilities.

6. On information and belief, the Court has personal jurisdiction over Defendant because Defendant has committed, and continue to commit, acts of infringement in the State of Texas, have conducted business in the State of Texas, and/or have engaged in continuous and systematic activities in the State of Texas. On information and belief, Defendant's accused instrumentalities that are alleged herein to infringe were and continue to be used, imported, offered for sale, and/or sold in the Western District of Texas.

7. On information and belief, Defendant voluntarily conducts business and solicit customers in the State of Texas and within this District, including, but not limited to, its offices located at 12515 Research Blvd Bldg 3, Austin, Texas 78759.

8. On information and belief, Defendant generates substantial revenue within this District and from the acts of infringement as carried out in this District. As such, the exercise of jurisdiction over Defendant would not offend the traditional notions of fair play and substantial justice.

9. Venue is proper in the Western District of Texas pursuant to 28 U.S.C. § 1400(b) and 28 U.S.C. § 1391(c)(3).

ASSERTED PATENT

10. On September 22, 2009, United States Patent No. 7,594,009 ("the '009 Patent") was duly and legally issued for "Monitoring Network Activity." A copy may be obtained at: https://patents.google.com/patent/US7594009B2/en.

ACCUSED PRODUCT

11. On information and belief, Defendant makes, uses, imports, sells, and/or offers for sale the Firewall Management Center (FMC) formerly Firepower Management Center. https://www.cisco.com/c/en/us/Product/collateral/security/firesight-management-center/datasheet-c78-736775.html. https://www.cisco.com/c/en/us/td/docs/security/firepower/650/configuration/guide/fpmc-config-guide-v65.pdf.

12. On information and belief, at all times Defendant owns and controls the operation of the Accused Instrumentalities in accordance with an end user license agreement.

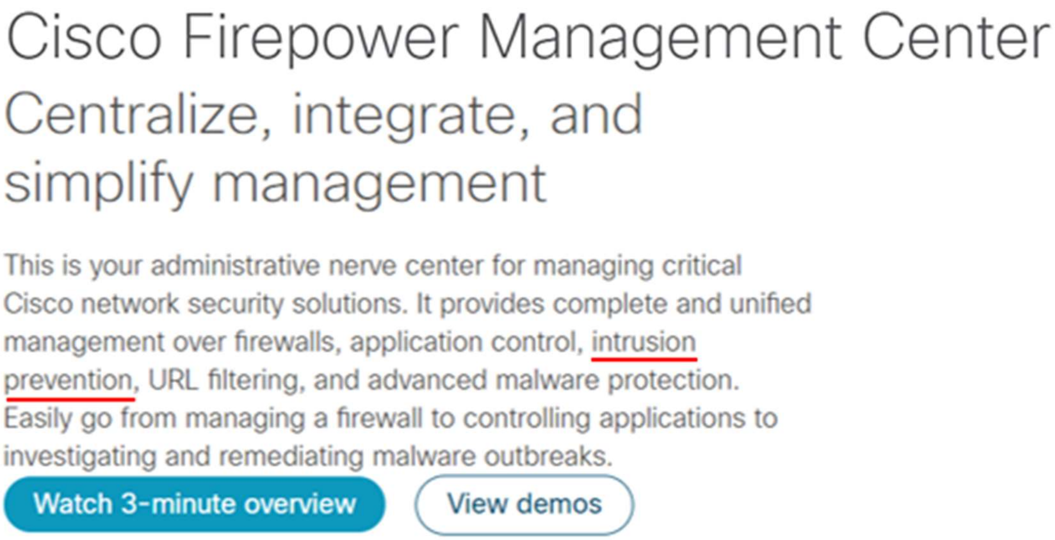
COUNT I
(Infringement of U.S. Patent No. 7,594,009)

13. Datamonitor incorporates the above paragraphs by reference.

14. Defendant has been and is now infringing one or more claims of the ’009 patent under 35 U.S.C. § 271 by making and/or using the Accused Product in the United States without authority.

15. More particularly, the Accused Product is an intrusion detection and prevention system (IDS) for analyzing network traffic. On information and belief, Defendant employs this system to perform the operations described herein.

16. More particularly, the Accused Product is a system for analyzing network traffic.

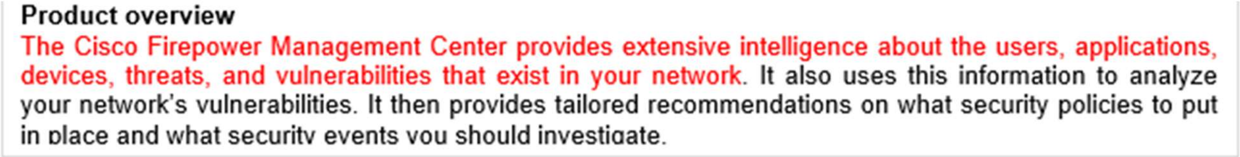


Cisco Firepower Management Center

Centralize, integrate, and simplify management

This is your administrative nerve center for managing critical Cisco network security solutions. It provides complete and unified management over firewalls, application control, intrusion prevention, URL filtering, and advanced malware protection. Easily go from managing a firewall to controlling applications to investigating and remediating malware outbreaks.

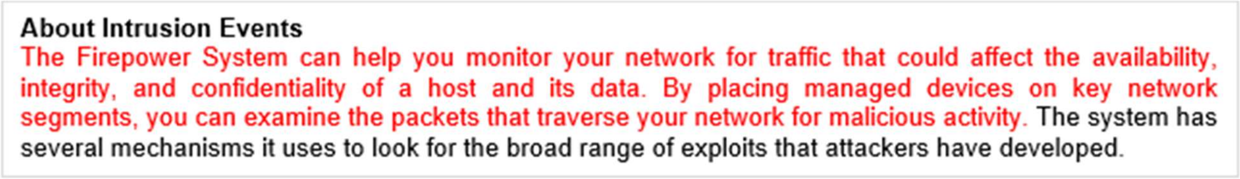
Source: https://www.cisco.com/c/en/us/products/security/firepower-management-center/index.html



Product overview

The Cisco Firepower Management Center provides extensive intelligence about the users, applications, devices, threats, and vulnerabilities that exist in your network. It also uses this information to analyze your network's vulnerabilities. It then provides tailored recommendations on what security policies to put in place and what security events you should investigate.

Source: https://www.cisco.com/c/en/us/products/collateral/security/firesight-management-center/datasheet-c78-736775.html

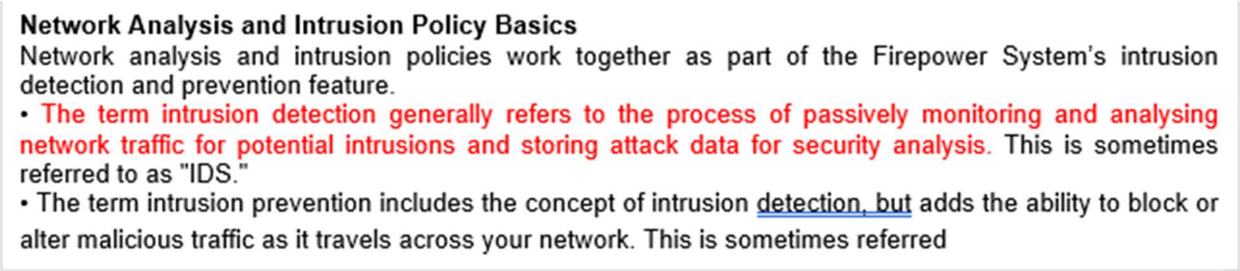


About Intrusion Events

The Firepower System can help you monitor your network for traffic that could affect the availability, integrity, and confidentiality of a host and its data. By placing managed devices on key network segments, you can examine the packets that traverse your network for malicious activity. The system has several mechanisms it uses to look for the broad range of exploits that attackers have developed.

Source: https://www.cisco.com/c/en/us/td/docs/security/firepower/650/configuration/guide/fpmc-config-guide-v65.pdf Page 2467 of 2706

17. In operation, the Accused Product uses a detecting means including a tap which receives and selects packets of data from network traffic and packet creating means which, for each packet selected by the tap, creates a modified selected packet for analysis which consists of the selected packet and a unique identifier for the selected packet which distinguishes that selected packet from all other selected packets,

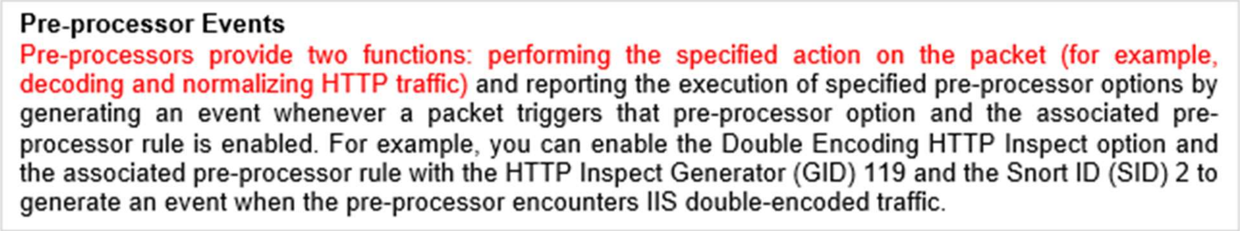


Network Analysis and Intrusion Policy Basics

Network analysis and intrusion policies work together as part of the Firepower System's intrusion detection and prevention feature.

- The term intrusion detection generally refers to the process of passively monitoring and analysing network traffic for potential intrusions and storing attack data for security analysis. This is sometimes referred to as "IDS."
- The term intrusion prevention includes the concept of intrusion detection, but adds the ability to block or alter malicious traffic as it travels across your network. This is sometimes referred

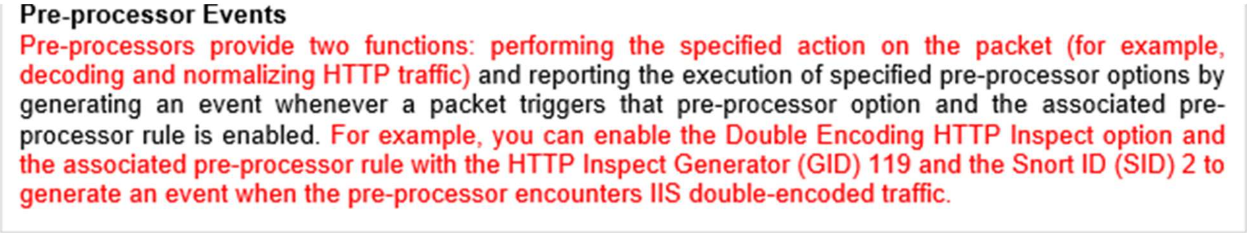
Source: https://www.cisco.com/c/en/us/td/docs/security/firepower/650/configuration/guide/fpmc-config-guide-v65.pdf Page 1623 of 2706



Pre-processor Events

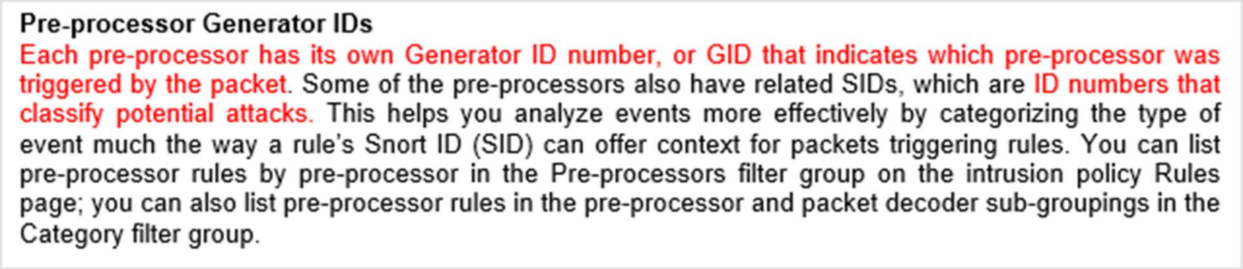
Pre-processors provide two functions: performing the specified action on the packet (for example, decoding and normalizing HTTP traffic) and reporting the execution of specified pre-processor options by generating an event whenever a packet triggers that pre-processor option and the associated pre-processor rule is enabled. For example, you can enable the Double Encoding HTTP Inspect option and the associated pre-processor rule with the HTTP Inspect Generator (GID) 119 and the Snort ID (SID) 2 to generate an event when the pre-processor encounters IIS double-encoded traffic.

Source: https://www.cisco.com/c/en/us/td/docs/security/firepower/650/configuration/guide/fpmc-config-guide-v65.pdf Page 2483 of 2706



Pre-processor Events

Pre-processors provide two functions: performing the specified action on the packet (for example, decoding and normalizing HTTP traffic) and reporting the execution of specified pre-processor options by generating an event whenever a packet triggers that pre-processor option and the associated pre-processor rule is enabled. For example, you can enable the Double Encoding HTTP Inspect option and the associated pre-processor rule with the HTTP Inspect Generator (GID) 119 and the Snort ID (SID) 2 to generate an event when the pre-processor encounters IIS double-encoded traffic.

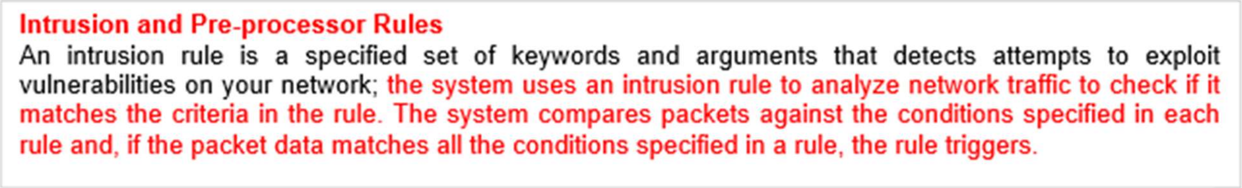


Pre-processor Generator IDs

Each pre-processor has its own Generator ID number, or GID that indicates which pre-processor was triggered by the packet. Some of the pre-processors also have related SIDs, which are ID numbers that classify potential attacks. This helps you analyze events more effectively by categorizing the type of event much the way a rule's Snort ID (SID) can offer context for packets triggering rules. You can list pre-processor rules by pre-processor in the Pre-processors filter group on the intrusion policy Rules page; you can also list pre-processor rules in the pre-processor and packet decoder sub-groupings in the Category filter group.

Source: https://www.cisco.com/c/en/us/td/docs/security/firepower/650/configuration/guide/fpmc-config-guide-v65.pdf Page 2483 and 2484 of 2706

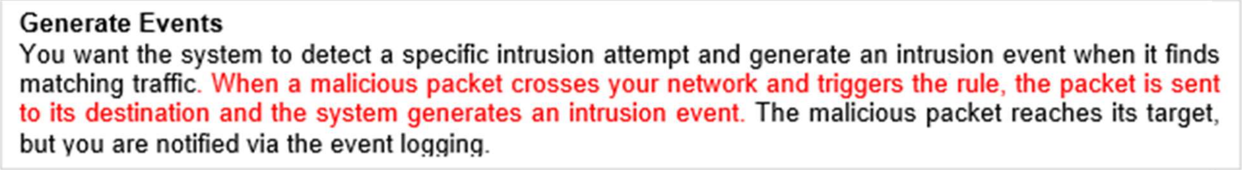
18. In operation, the Accused Product the detecting means analyzes the modified selected packets to detect suspect modified data packets which meet criteria defined by one or more functions in the detecting means, the criteria being indicative of potentially damaging traffic on the network.



Intrusion and Pre-processor Rules

An intrusion rule is a specified set of keywords and arguments that detects attempts to exploit vulnerabilities on your network; the system uses an intrusion rule to analyze network traffic to check if it matches the criteria in the rule. The system compares packets against the conditions specified in each rule and, if the packet data matches all the conditions specified in a rule, the rule triggers.

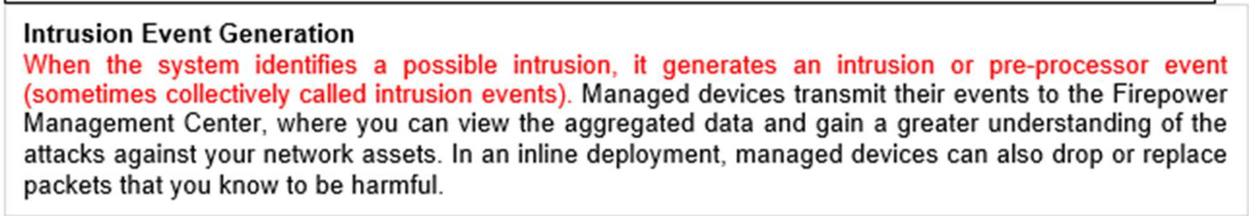
Source: https://www.cisco.com/c/en/us/td/docs/security/firepower/650/configuration/guide/fpmc-config-guide-v65.pdf Page 1627 of 2706



Generate Events

You want the system to detect a specific intrusion attempt and generate an intrusion event when it finds matching traffic. When a malicious packet crosses your network and triggers the rule, the packet is sent to its destination and the system generates an intrusion event. The malicious packet reaches its target, but you are notified via the event logging.

Source: https://www.cisco.com/c/en/us/td/docs/security/firepower/650/configuration/guide/fpmc-config-guide-v65.pdf Page 1678 of 2706

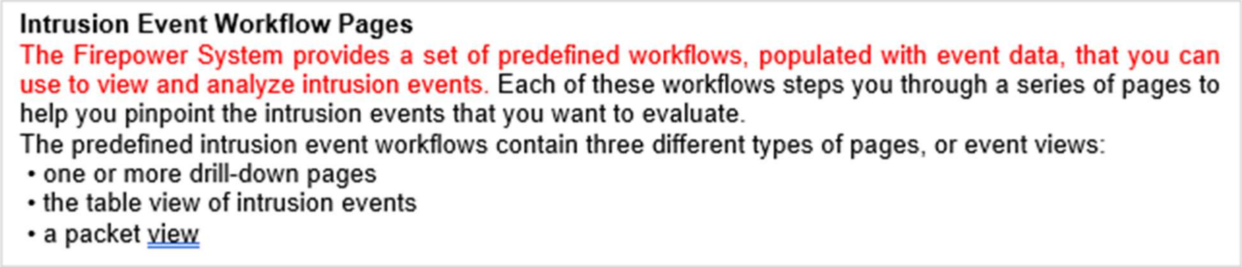


Intrusion Event Generation

When the system identifies a possible intrusion, it generates an intrusion or pre-processor event (sometimes collectively called intrusion events). Managed devices transmit their events to the Firepower Management Center, where you can view the aggregated data and gain a greater understanding of the attacks against your network assets. In an inline deployment, managed devices can also drop or replace packets that you know to be harmful.

Source: https://www.cisco.com/c/en/us/td/docs/security/firepower/650/configuration/guide/fpmc-config-guide-v65.pdf Page 1628 of 2706

19. In operation, the Accused Product forwards details of each detected suspect modified data packet to data processing means.



Intrusion Event Workflow Pages

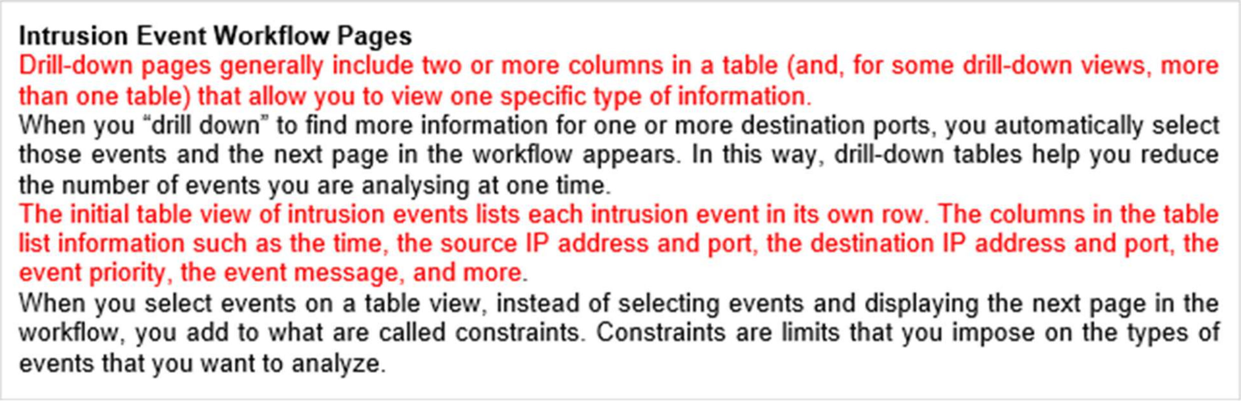
The Firepower System provides a set of predefined workflows, populated with event data, that you can use to view and analyze intrusion events. Each of these workflows steps you through a series of pages to help you pinpoint the intrusion events that you want to evaluate.

The predefined intrusion event workflows contain three different types of pages, or event views:

- one or more drill-down pages
- the table view of intrusion events
- a packet view

Source: https://www.cisco.com/c/en/us/td/docs/security/firepower/650/configuration/guide/fpmc-config-guide-v65.pdf Page 2486 of 2706

20. In operation, the Accused Product stores details of each detected suspect modified data packet so as to be accessible for use in analysis by the data processing means in conjunction with the details of other detected modified suspect packets.



Intrusion Event Workflow Pages

Drill-down pages generally include two or more columns in a table (and, for some drill-down views, more than one table) that allow you to view one specific type of information.

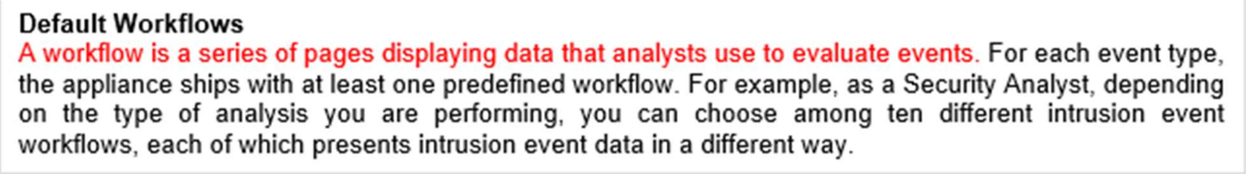
When you "drill down" to find more information for one or more destination ports, you automatically select those events and the next page in the workflow appears. In this way, drill-down tables help you reduce the number of events you are analysing at one time.

The initial table view of intrusion events lists each intrusion event in its own row. The columns in the table list information such as the time, the source IP address and port, the destination IP address and port, the event priority, the event message, and more.

When you select events on a table view, instead of selecting events and displaying the next page in the workflow, you add to what are called constraints. Constraints are limits that you impose on the types of events that you want to analyze.

Source: https://www.cisco.com/c/en/us/td/docs/security/firepower/650/configuration/guide/fpmc-config-guide-v65.pdf Page 2486 of 2706

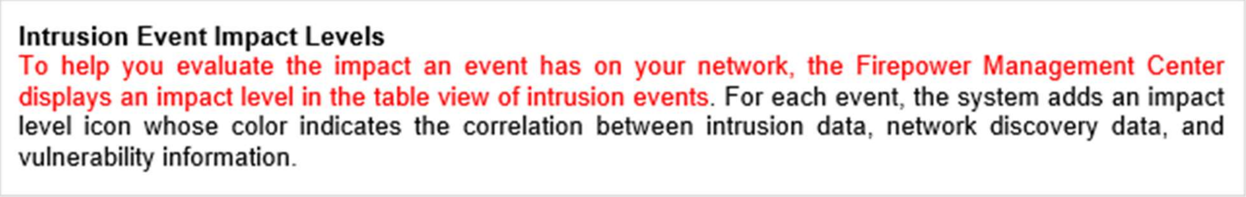
21. In operation, the Accused Product uses the data processing means to analyze the stored suspect modified data packets.



Default Workflows

A workflow is a series of pages displaying data that analysts use to evaluate events. For each event type, the appliance ships with at least one predefined workflow. For example, as a Security Analyst, depending on the type of analysis you are performing, you can choose among ten different intrusion event workflows, each of which presents intrusion event data in a different way.

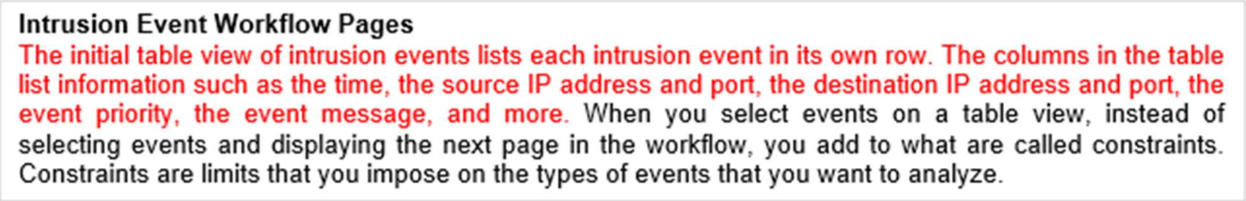
Source: https://www.cisco.com/c/en/us/td/docs/security/firepower/650/configuration/guide/fpmc-config-guide-v65.pdf Page 133 of 2706



Intrusion Event Impact Levels

To help you evaluate the impact an event has on your network, the Firepower Management Center displays an impact level in the table view of intrusion events. For each event, the system adds an impact level icon whose color indicates the correlation between intrusion data, network discovery data, and vulnerability information.

Source: https://www.cisco.com/c/en/us/td/docs/security/firepower/650/configuration/guide/fpmc-config-guide-v65.pdf Page 2479 of 2706



Intrusion Event Workflow Pages

The initial table view of intrusion events lists each intrusion event in its own row. The columns in the table list information such as the time, the source IP address and port, the destination IP address and port, the event priority, the event message, and more. When you select events on a table view, instead of selecting events and displaying the next page in the workflow, you add to what are called constraints. Constraints are limits that you impose on the types of events that you want to analyze.

Source: https://www.cisco.com/c/en/us/td/docs/security/firepower/650/configuration/guide/fpmc-config-guide-v65.pdf Page 2486 of 2706

22. Datamonitor has been damaged by Defendant's infringement of the '009 Patent.

PRAYER FOR RELIEF

WHEREFORE, Datamonitor respectfully requests the Court enter judgment against Defendant:

1. declaring that the Defendant have infringed the ’009 Patent;

2. awarding Datamonitor its damages suffered as a result of Defendant’s infringement of the Patents-in-Suit;

3. awarding Datamonitor its costs, attorneys’ fees, expenses, and interest;

4. awarding Datamonitor ongoing post-trial royalties; and

5. granting Datamonitor such further relief as the Court finds appropriate.

JURY DEMAND

Datamonitor demands trial by jury, under Fed. R. Civ. P. 38.

Dated: April 11, 2024

Respectfully Submitted

/s/ Raymond W. Mort, III
Raymond W. Mort, III
Texas State Bar No. 00791308
raymort@austinlaw.com
THE MORT LAW FIRM, PLLC
111 Congress Ave, Suite 500
Austin, Texas 78701
Tel/Fax: (512) 865-7950

ATTORNEYS FOR PLAINTIFF