

# PRIVACYWARE

## Adaptive Security Analyzer 2.0

### User Guide

#### Published by:

Privacyware  
68 White Street, 2<sup>nd</sup> Floor  
Red Bank, NJ 07701  
Email: [info@privacyware.com](mailto:info@privacyware.com)  
URL: <http://www.privacyware.com>

#### Document Version

Adaptive Security Analyzer – User Guide, version 2.0, Privacyware. There is no warranty of any kind with respect to the completeness or accuracy of this manual. Privacyware may make improvements and/or changes to the product(s) and/or programs described in this User Guide at any time and without notice.

#### Copyright & Trademarks

Copyright ©2010 PWI, Inc./Privacyware. All rights reserved. Privacyware, Adaptive Security Analyzer Pro, Adaptive Security Analyzer, and Adaptive Security Engine are either registered trademarks or trademarks of PWI, Inc. in the United States and/or other countries. All other trademarks and trade names are the property of their respective owners.

Information in this document is subject to change without notice. The software described in this document is furnished under a license agreement or non-disclosure agreement. The software may be used or copied only in accordance with the terms of those agreements. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or any means electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's use without the written permission of Privacyware.

## Table of Contents

<b>About Privacyware</b> .....	<b>3</b>
Privacyware Products .....	3
Corporate Headquarters & Contact Information .....	3
<b>Adaptive Security Analyzer Overview</b> .....	<b>4</b>
Introduction .....	4
System Requirements .....	5
Supported Data Formats .....	5
<b>Working with Adaptive Security Analyzer</b> .....	<b>6</b>
Main Screen.....	6
Create New Analysis .....	7
Baseline Settings .....	8
Data Source Path .....	8
Trusted IP Networks .....	9
Training Period .....	9
Traffic Direction .....	10
Data Filters .....	11
Enable Sequence Analysis.....	12
Model Structure .....	13
Train .....	14
Report Settings .....	15
Data Source.....	15
Report Columns.....	16
Reporting Period.....	16
Data Filters .....	17
Other Settings.....	17
Report Distribution.....	18
Working with Reports.....	20
Table View .....	20
Table View – Right Mouse options.....	21
Event Detail View .....	22
Chart Views .....	22
Custom Models .....	25
Baseline Settings.....	25
Reports .....	32
Priors .....	34
<b>Supported Firewalls and Log Formats</b> .....	<b>35</b>
Custom Models .....	35
Check Point FireWall-1 .....	35
Cisco Pix Firewall v6 log in CiscoPIX syslog format.....	35
Juniper NetScreen (OS 5.0) .....	36
MS ISA Server Firewall Log in W3C format .....	37

## **About Privacyware**

Privacyware is the leading provider of advanced threat prevention and security intelligence solutions. The combination of advanced competencies in non-linear mathematics, neural networks and self-learning systems, and proficiency in complex software and systems development allows us to create innovative and intelligent security solutions that are distinguished by their ease of use, advanced analytic capabilities, and the value they deliver to security staff and the greater enterprise. Privacyware solutions fuel the organization's ability to make better decisions and remain a step ahead of hackers and others seeking to compromise critical systems.

### ***Privacyware Products***

#### **Adaptive Security Analyzer**

Security Data Analysis Software

#### **ThreatSentry**

IIS Web Application Firewall / IPS

#### **Privatefirewall**

Windows Client Firewall + Malware & Intrusion Defense

### ***Corporate Headquarters & Contact Information***

Privacyware

68 White Street

Red Bank, NJ 07701

Telephone: 732-212-8110

Facsimile: 732-212-9210

Web Site: [www.privacyware.com](http://www.privacyware.com)

Technical Support: <http://www.privacyware.com/support.html>

# Adaptive Security Analyzer Overview

## Introduction

Adaptive Security Analyzer (ASA) is a flexible log and data analysis application that supports almost any type of structured data. In some cases, ASA includes pre-built (out-of-the-box) analytic models that are designed to work with a particular type of data, i.e. collected from a firewall device or specific operating system. In cases where the data to be analyzed is not supported by a pre-built model, ASA provides a straight-forward set of features that enable a custom model to be rapidly created.

ASA includes pre-built models for specific data/device types. These are listed under the main Adaptive Security Analyzer MMC node. Custom Analysis can also be performed for devices and data for which no pre-built models are available.

Currently, ASA includes pre-built models in Syslog, .csv and .txt formats for data/logs generated from the following:

- Check Point Firewall-1
- Cisco PIX Firewall
- Microsoft ISA Sever
- Juniper/NetScreen Firewall

Custom Analysis can be performed using any ODBC compliant data source, including SQL, MySQL, Oracle, etc. Please refer to the Custom Models Section of this manual for more information.

Adaptive Security Analyzer allows the expertise and methods of the security specialist to be modeled so that security data can be rapidly and effectively transformed into actionable intelligence.

In the context of these models, ASA:

- Analyzes high volume security-related data.
- Freely interprets & associates event attributes to organically cluster and baseline system activity.
- Compares data sets, recognizes and quantifies the extent of abnormal events.
- Advises security personnel of the factors that contributed most to the abnormal events' classifications.
- Adapts its orientation of the relationships among event variables and event classifications based on unsupervised machine-learning and/or user-applied knowledge.

Adaptive Security Analyzer is the first security data analysis solution geared specifically for security related data that combines expert rules with concept-based artificial intelligence technology to empower network personnel challenged with monitoring and securing computing systems and managing compliance.

Adaptive Security Analyzer automatically forms contextual and conceptual associations between seemingly disparate event variables to emulate the cognitive and self-learning process of a human analyst. In this way, ASA is able to pinpoint, categorize and prioritize (score) suspicious activity and/or prevent known and unknown system threats beyond the capacity of tools which rely solely on filtering, reporting, and statistic analysis. Adaptive Security Analyzer sifts through massive volumes of logs to quickly reveal and prioritize the most critical events and advise users of the factors of highest influence to event classification.

## ***System Requirements***

To run Adaptive Security Analyzer, your system must meet the following minimum requirements:

### **Hardware**

- 1 GHz processor or faster
- 1 GB RAM or greater
- CD-ROM drive (for installation from CD)
- 5 MB of free disk space (for ASA software)

### **Software**

- One of the following operating systems:
  - Windows® Server 2008 (R2)
  - Windows® 7
  - Windows® Vista
  - Windows® Server 2000 (Service Pack 3 or later)
  - Windows® Server 2003
  - Windows XP Pro

## ***Supported Data Formats***

Adaptive Security Analyzer supports XML, CSV, ASCII, MDB, SQL, MySQL, Oracle, and any ODBC compliant data source.

## Working with Adaptive Security Analyzer

Adaptive Security Analyzer is logical and simple to use. There are several advanced options available to customize analysis and reporting, but meaningful output can be generated via primarily the default settings provided within ASA. The sections that follow will guide you through the handful of steps required to effectively use ASA.

ASA performs a unique type of analysis. It uses the data provided to it to create a complex baseline of typical behavior. The same or different sets of data are then “compared” against the baseline and reports are generated that measure and show deviant activity (events or event sequences). Each atypical event is scored based on the extent to which it departs from normal trends and patterns. The factors that contributed to the event score are also displayed, providing context and

What you'll need:

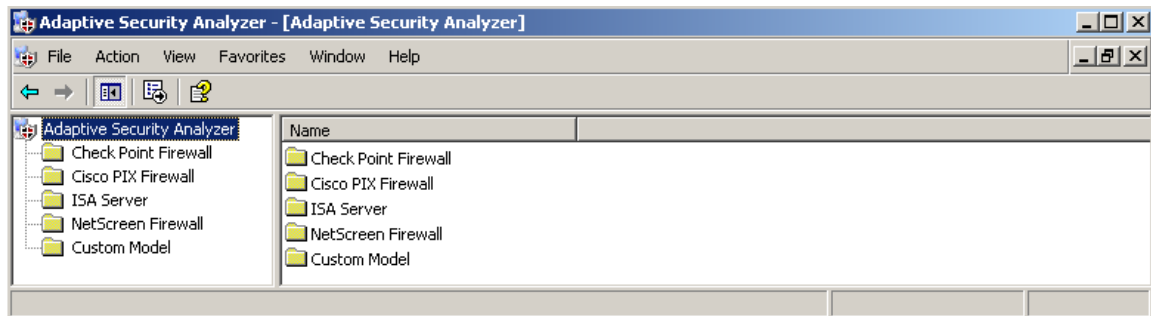
- A file or database containing the logs or data that require analysis.



The Adaptive Security Analyzer console can be opened by selecting the **Start Button->Programs ->Privacyware ->Adaptive Security Analyzer**, or by **double-clicking the Adaptive Security Analyzer desktop icon**.

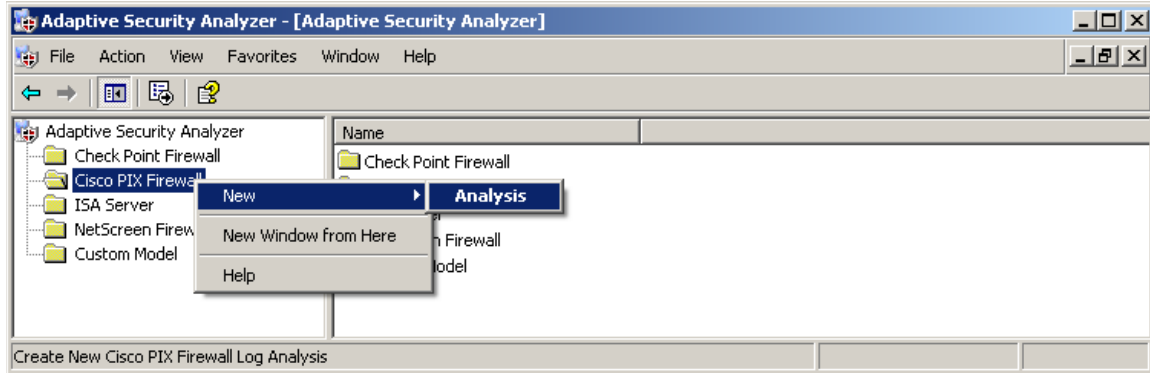
### Main Screen

Once Adaptive Security Analyzer is open, the main screen is displayed. Listed in the left panel are the default Analysis Models for various popular firewall and other security devices.

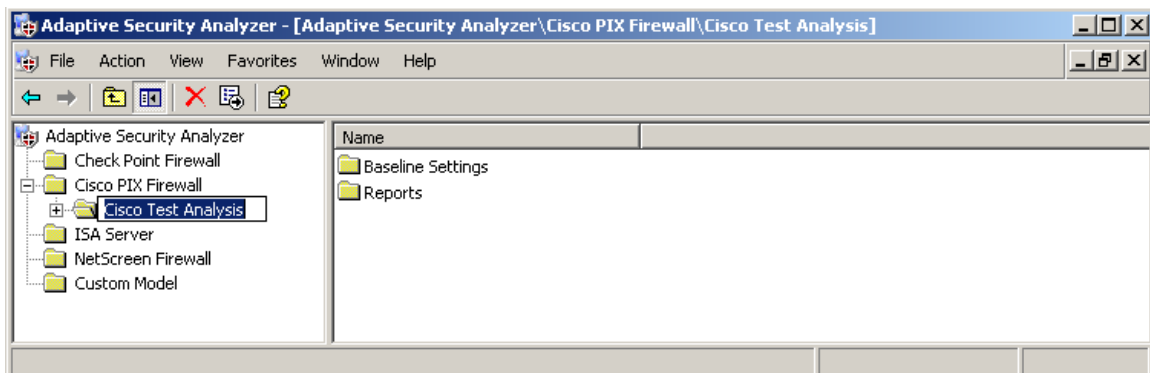


## Create New Analysis

To create a new Analysis using a pre-built model<sup>1</sup>, select and right mouse click the appropriate model name and select **New -> Analysis**.



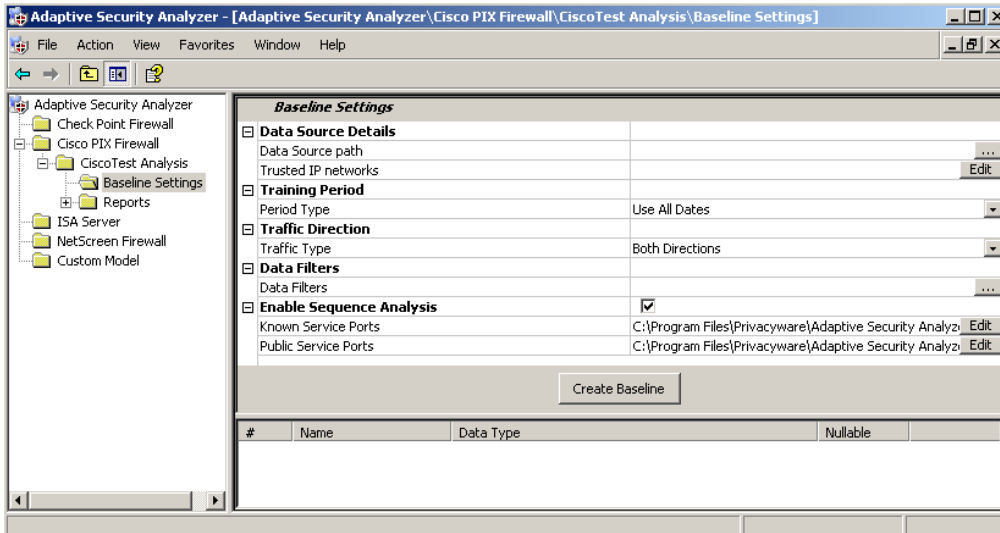
Next, provide a name for the Analysis. By default, the device root followed by Analysis1, 2, 3... will be used to name the Analysis. These defaults should be changed to reflect the nature of the analysis being conducted.



<sup>1</sup> ASA includes pre-built models for specific data/device types. These are listed under the main Adaptive Security Analyzer MMC node. Custom Analysis can also be performed for devices and data for which no pre-built models are available by right mouse clicking **Custom Model -> New -> Model**. Custom Analysis can be performed using any ODBC compliant data source, including SQL, Oracle, etc. Please refer to the Section entitled **Custom Models** of this manual for more information.

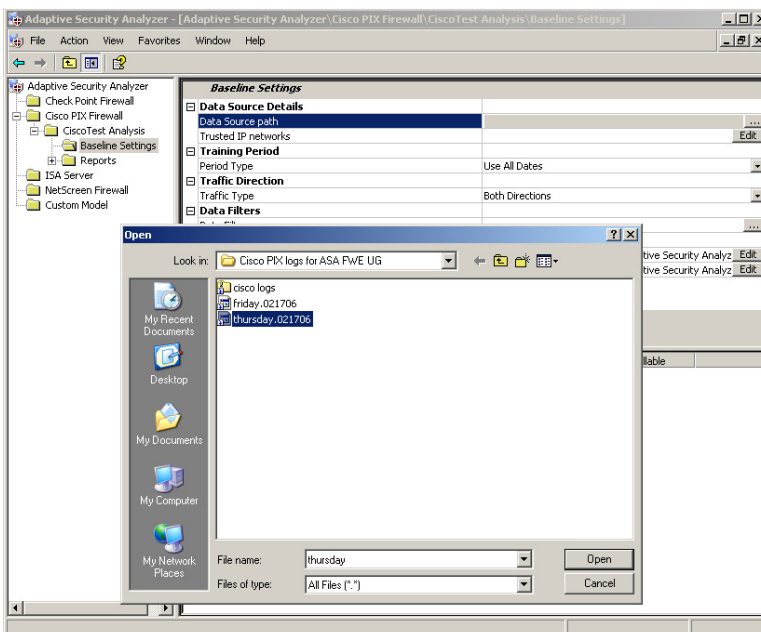
## Baseline Settings

Expand the folder of the **New Analysis** just created and select **Baseline Settings**.



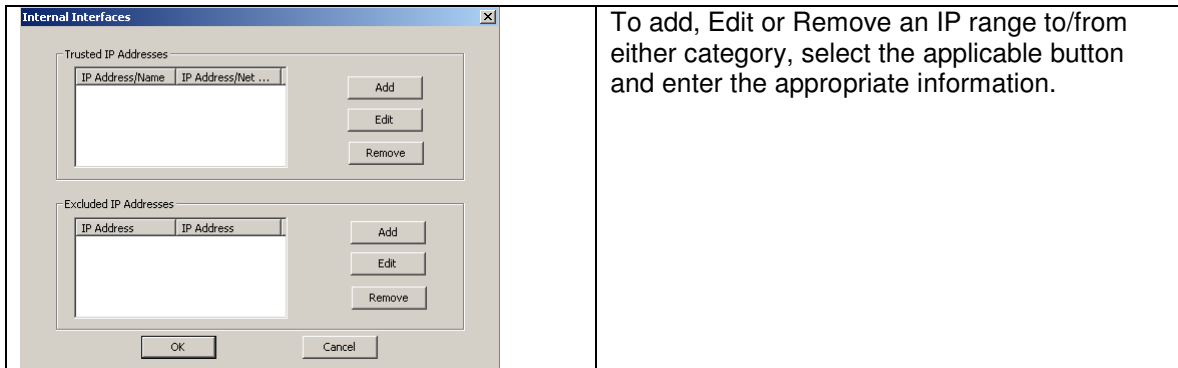
## Data Source Path

First, locate the data source that will be used to create the behavioral baseline. To do so, select the **...** button under **Data Source Details**, and browse to the appropriate file.



## Trusted IP Networks

Internal interfaces refer to IP address ranges that should be considered Trusted and/or Excluded with respect to analysis. To invoke the Trusted IP Networks screen, double-click the **Edit** button on the right of the row.

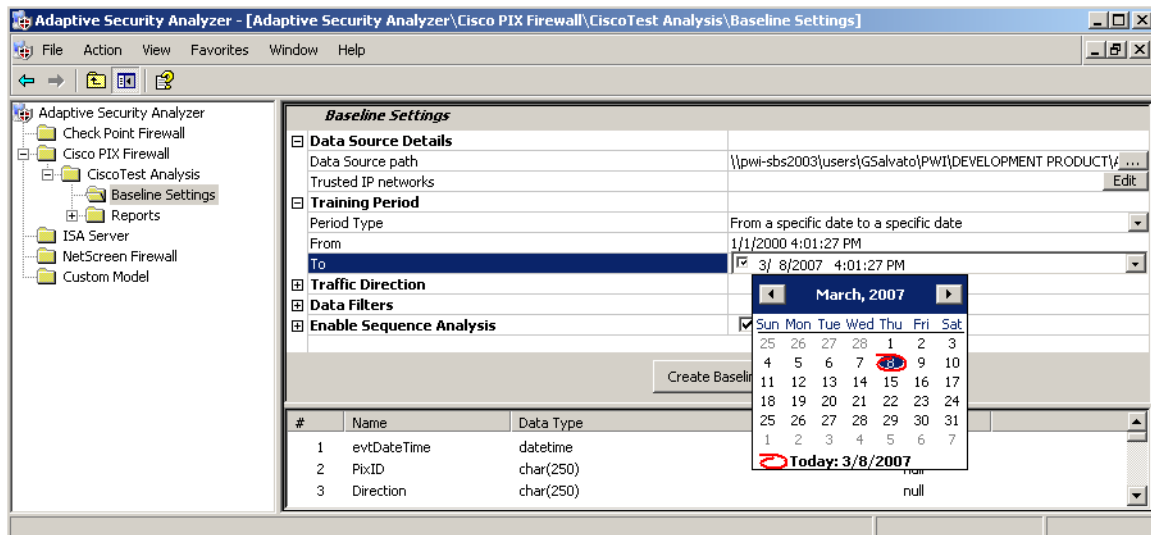


To add, Edit or Remove an IP range to/from either category, select the applicable button and enter the appropriate information.

**Note:** Trusted IP Network settings pertain to firewall log analysis specifically and not necessarily general log or data analysis that might be performed using the **Custom Model** feature. More information regarding Custom Model analysis can be found in the Custom Models section of this guide.

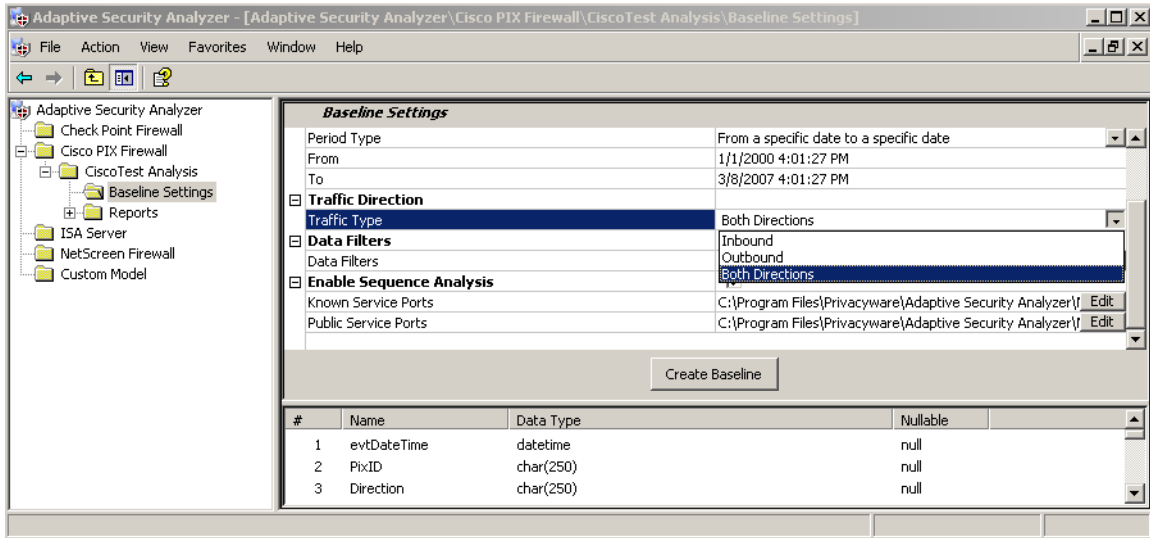
## Training Period

The baseline may be created using data spanning a defined date range, the last X number of calendar days, or the all of the data in the file.




## Traffic Direction

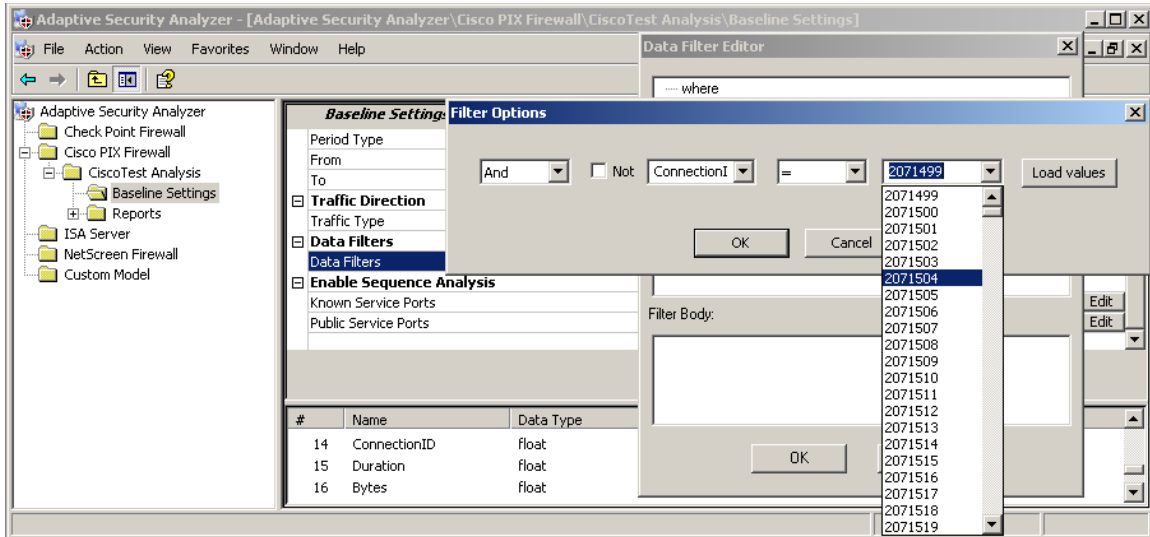
Inbound or Outbound firewall traffic can be analyzed. By default, both directions are considered.



## Data Filters

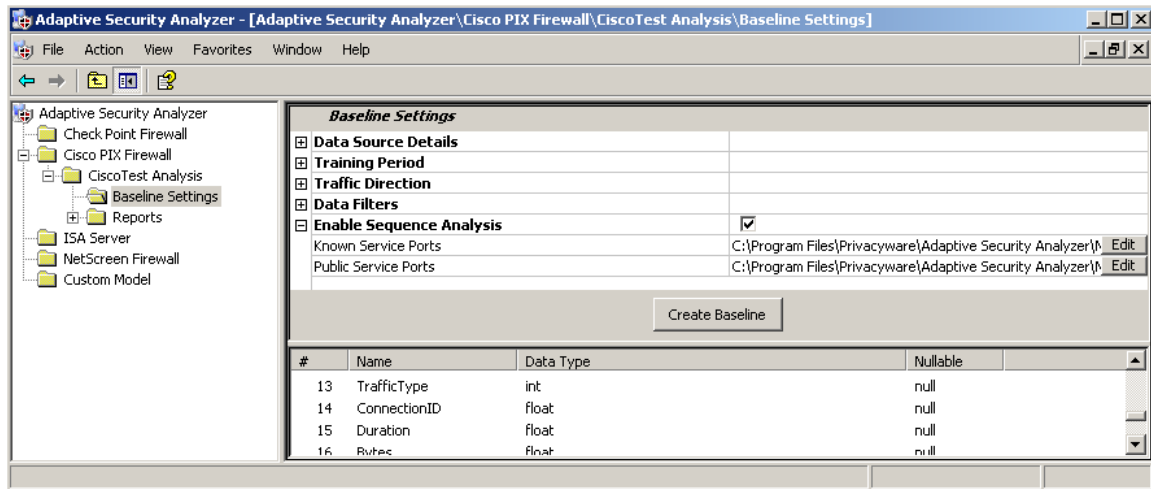
Adaptive Security Analyzer provides an ability to create custom filters so that specific events within the data set may be disregarded. For example, it may be desirable to disregard a particular day of the week or a certain IP from analysis or ConnectionID in the analysis.

Filters can be created using standard SQL query syntax. To create a filter, select the  button to invoke the Data Filter Editor. Then **Right mouse click where** and select **New Filter**. Add the filter and select **OK**.



## Enable Sequence Analysis

To effectively analyze firewall logs, event sequences as well as individual events within the log should be considered. For example, a slow port scan is generally not detectable based on analysis of a single log event, but can become apparent based on a review of event sequences. By default, the **Enable Sequence Analysis** feature is active.



Once selected, the **Enable Sequence Analysis** feature exposes a set of related configuration options to enhance analysis. These include:

### Known Service Ports

Known Service Ports are service ports that are used for typical legitimate network functions within the particular environment. It is important to explicitly identify these so that they are considered as such within the context of analysis. To invoke the Known Service Ports screen, double-click the **Edit** button on the right of the row.

	<p>To add, Edit or Remove a port, select the applicable button and enter the port information.</p> <p>To add ports from an existing file, select the <b>Import</b> button and locate the file (.csv format) that contains the ports that should be added.</p>
--	---

### Public Service Ports

Public Service Ports are the ports that are open to common network traffic. It is important to explicitly identify these so that they are considered as such within the context of analysis. To invoke the Public Service Ports screen, double-click the **Edit** button on the right of the row. A dialog screen identical to that invoked for the Known Service Ports will be displayed where you can Add, Edit, Remove or Import information. By default, Adaptive Security Analyzer includes certain ports typically used for public network traffic.

## Model Structure

The model structure is displayed in the bottom window and displays the basic elements of the pre-built (or custom-built) analytic model.

The screenshot shows the 'Baseline Settings' window in the Adaptive Security Analyzer. The window title is 'Adaptive Security Analyzer - [Adaptive Security Analyzer\Cisco PIX Firewall\CiscoTest Analysis\Baseline Settings]'. The left pane shows a tree view with 'Baseline Settings' selected. The main pane displays the following settings:

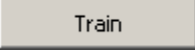
- Data Source Details**
- Training Period**
- Traffic Direction**
- Data Filters**
- Enable Sequence Analysis**

A 'Create Baseline' button is located below the settings. Below the settings is a table with the following data:

#	Name	Data Type	Nullable
1	evtDateTime	datetime	null
2	PixID	char(250)	null
3	Direction	char(250)	null
4	Protocol	char(250)	null
5	ExternalInterface	char(250)	null
6	FaddrIP	char(250)	null
7	FaddrPort	int	null
8	InternalInterface	char(250)	null
9	LaddrIP	char(250)	null
10	LaddrPort	int	null
11	GaddrIP	char(250)	null
12	GaddrPort	int	null
13	TrafficType	int	null
14	ConnectionID	float	null
15	Duration	float	null
16	Bytes	float	null
17	dstIPExists	int	null
18	DayWeek	int	null
19	Hours	int	null

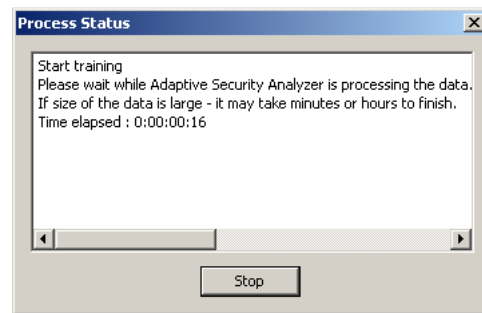
## Train

Once all of the details for the analysis have been specified, the process of creating the baseline, (upon which the comparative analysis of other data will be performed), can commence.

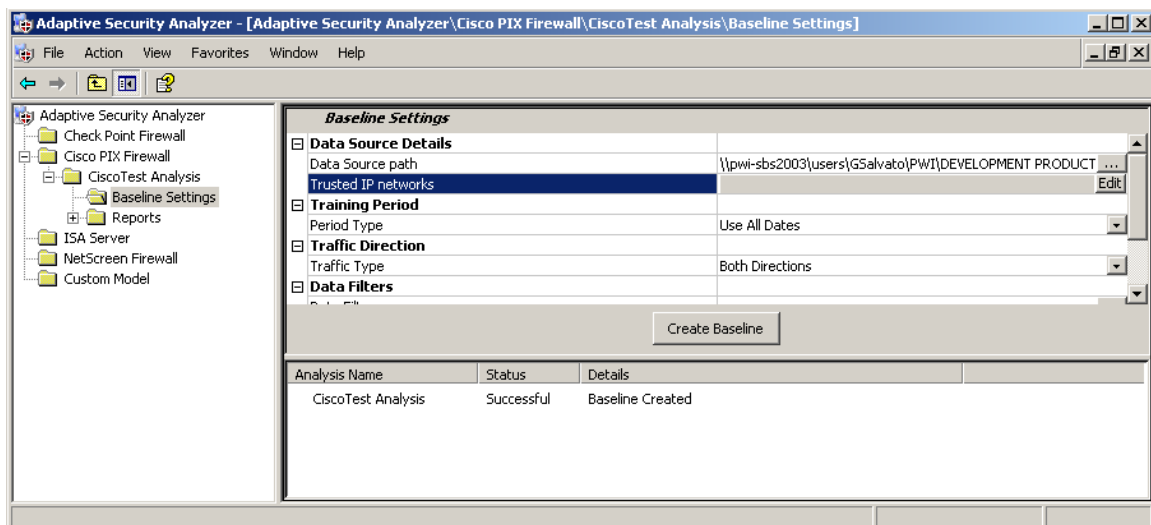
**To do so, click the  button.** Once invoked, the data identified are organized based on the underlying pre-configured analytic model as well as rules (if any) that have been specified by the end-user.

**Note:** The length of time required to complete training is primarily a function of the amount of data being processed and of course the capacity of the computer designated for the task. Creating the baseline (training) can take several minutes or hours to complete, so please be patient. If analysis will typically be performed on very large databases or files, please be sure the capacity of the computing environment is adequate for the task.

A progress status screen will be displayed during the training process.




Once the process of creating the baseline has finished, the bottom panel will display the **Successful** status and indicate that the Baseline has been created.

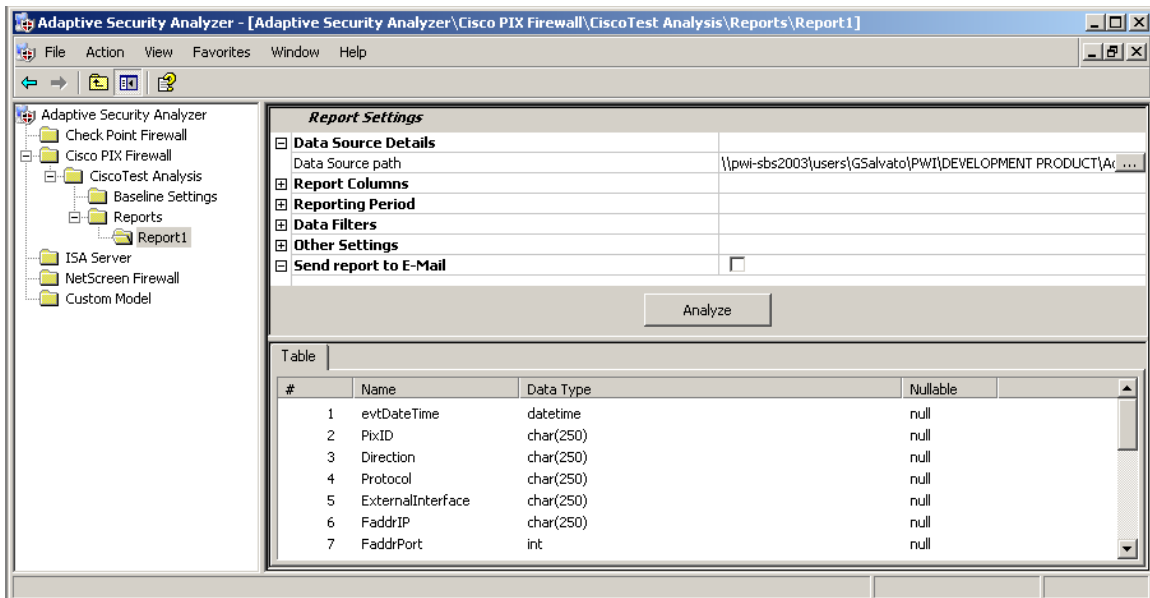


## Report Settings

Once a baseline for analysis has been created, information regarding the data to be analyzed must be specified. To start, **select** the **Report folder** that was automatically added once Training completed. The **Report name** can be changed by applying the **Right mouse function**, selecting **Rename**, and providing the name desired.

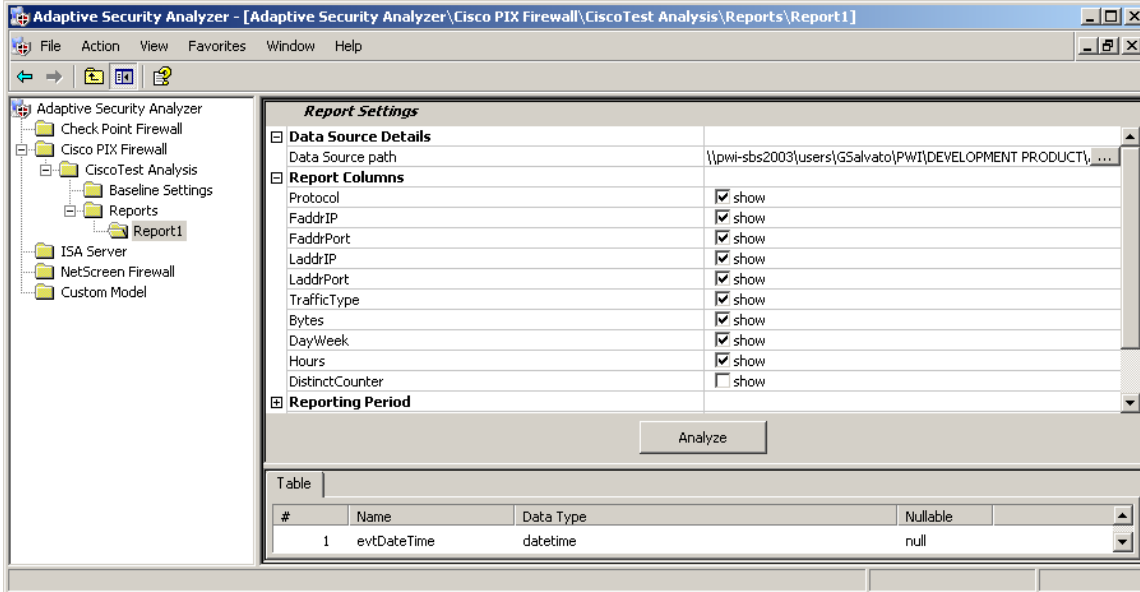
## Data Source

Locate the data source that will be used for analysis. To do so, select the  button under **Data Source**, and browse to the appropriate file.



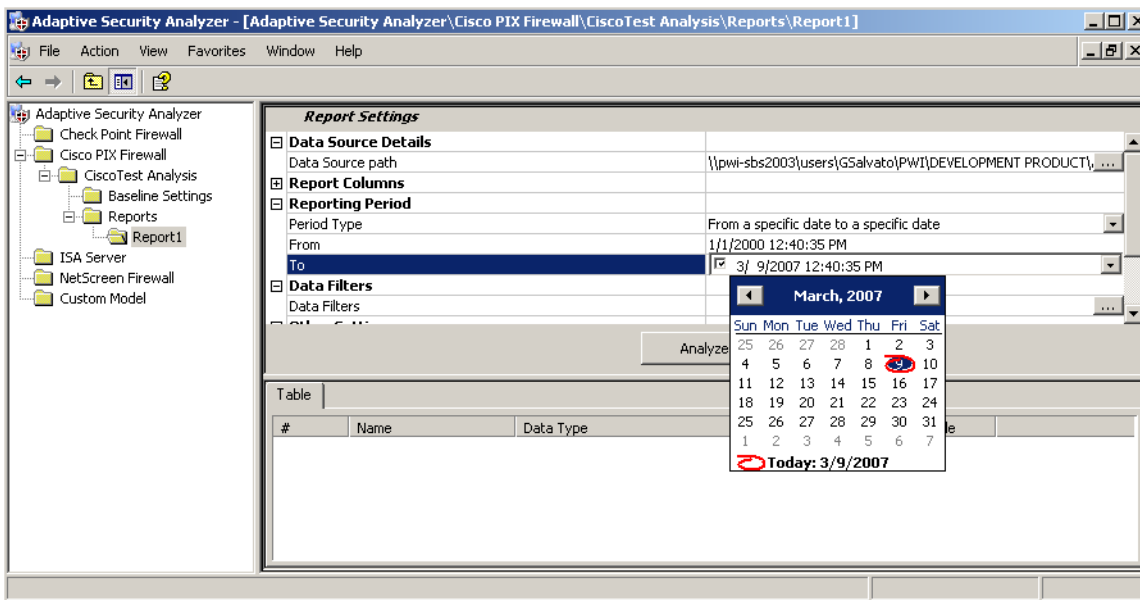
## Report Columns

Next, specify the Columns that should be displayed in the report output.



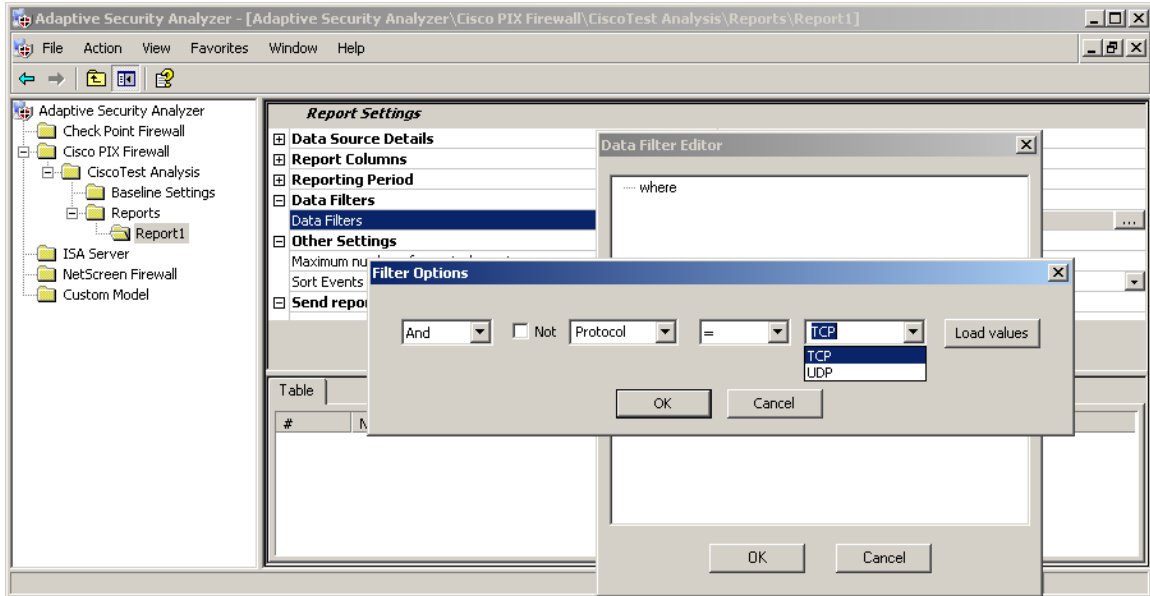
## Reporting Period

Reports can be generated using data spanning a defined date range, the last X number of calendar days, or the all of the data in the file.



## Data Filters

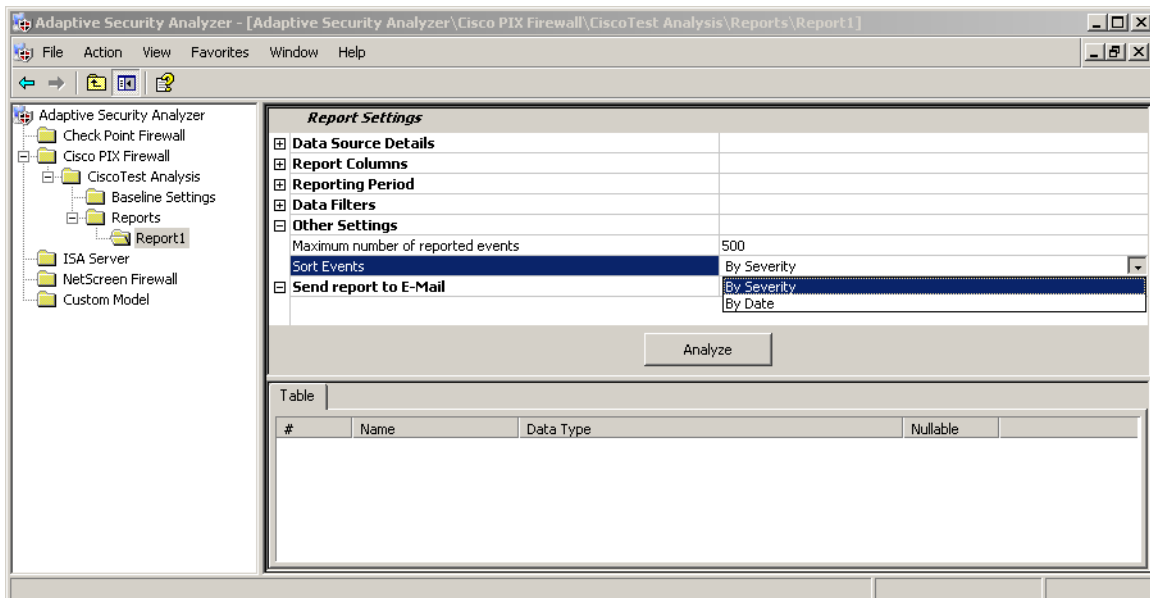
Filters can be created using standard SQL query syntax. To create a filter, select the **...** button to invoke the Data Filter Editor. Then **Right mouse click where** and select **New Filter**. Add the filter and select **OK**.



## Other Settings

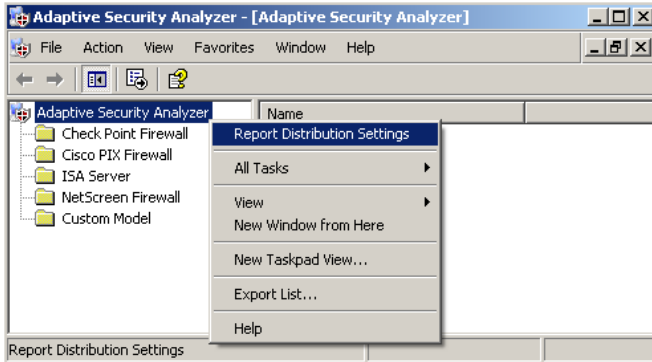
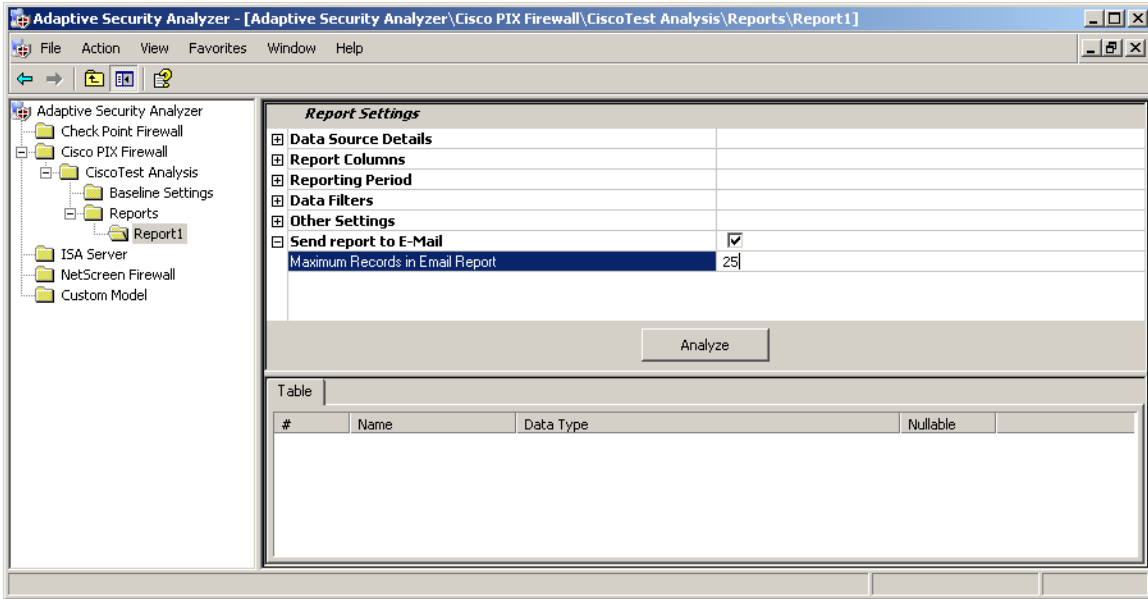
**Maximum number of reported events:** Specifies the maximum number of events to be displayed in the report.

**Sort Events:** Events may be sorted by date or the extent to which they deviate from the baseline (Severity).



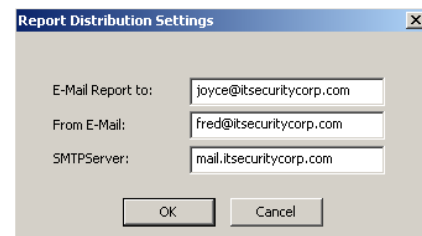
## Report Distribution

Reports can be shared with others via .csv file attachment transmitted through email. Select the check box to enable the email report feature and specify the number of events that should be included in the report.



**Note:** To configure Report Distribution Settings (email), highlight and right-click the Adaptive Security Analyzer icon in the left panel of the MMC snap-in and select Report Distribution Settings.

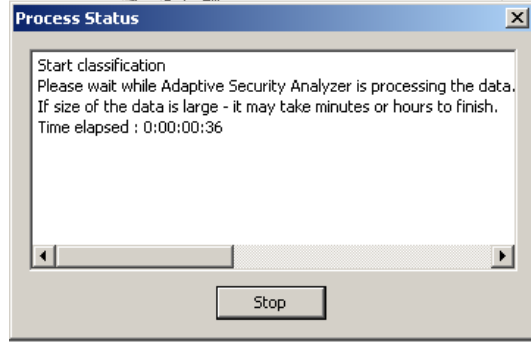
Enter the required mail server information and email address of those to whom reports should be sent as well as the name of the SMTP Server.



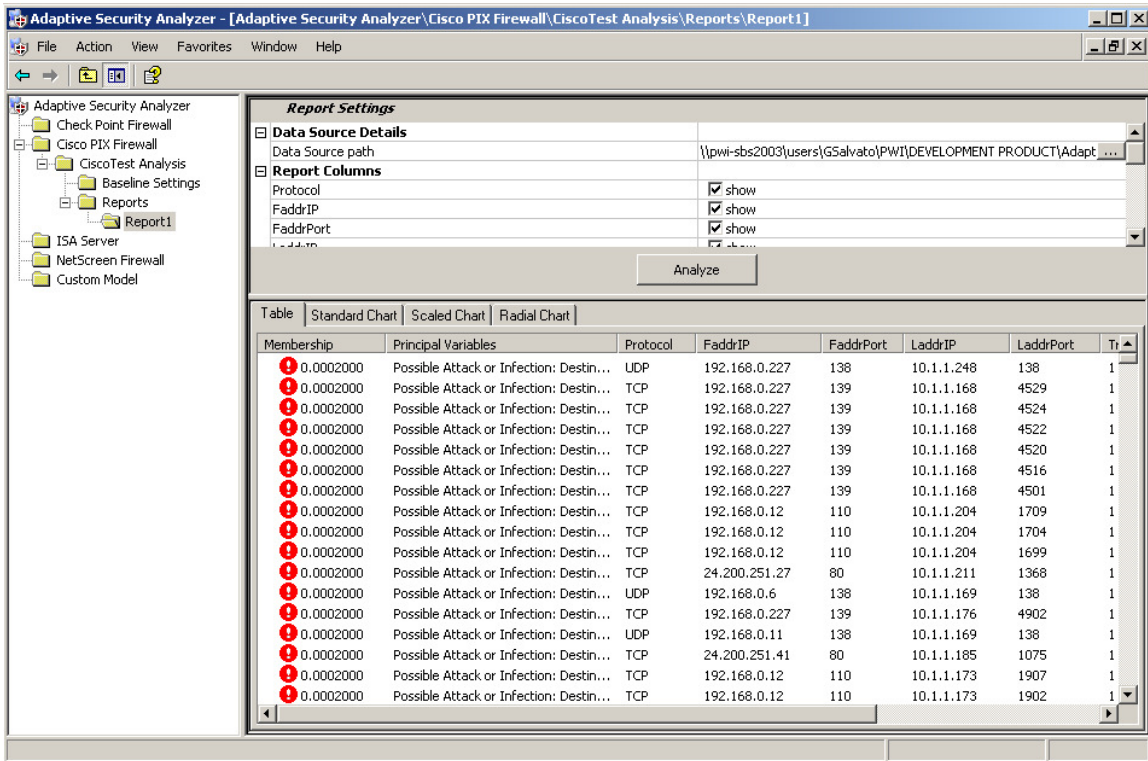
Once all of the Report Settings have been designated, click the Analyze button.



A progress status screen will be displayed as events are analyzed.



Once the analysis process has finished, reports will displayed automatically in the bottom right window or can be displayed by selecting the Report folder in the left panel (underneath the main Reports folder).



## Working with Reports

Adaptive Security Analyzer provides a flexible set of features that enable reports to be created and modified on the fly.

### Table View

The default view (displayed in the bottom right window) includes columns that reflect each of the variables in the underlying analytic model.





The screenshot shows the Adaptive Security Analyzer interface. On the left is a tree view with folders for Check Point Firewall, Cisco PIX Firewall, CiscoTest Analysis, Baseline Settings, Reports, ISA Server, NetScreen Firewall, and Custom Model. The main window is titled 'Adaptive Security Analyzer - [Cisco PIX Firewall\CiscoTest Analysis\Reports\Report1]'. It features a 'Report Settings' dialog box with sections for 'Data Source Details' (Data Source path: \\pwi-sbs2003\users\GSalvato\PWI\DEVELOPMENT PRODUCT\Adapt...) and 'Report Columns' (Protocol, FaddrIP, FaddrPort, LaddrIP, LaddrPort, Tr). Below the settings is an 'Analyze' button. At the bottom, a table view is displayed with the following columns: Membership, Principal Variables, Protocol, FaddrIP, FaddrPort, LaddrIP, LaddrPort, and Tr. The table contains 18 rows of data, each starting with a red exclamation mark icon and a membership score of 0.0002000. The Principal Variables column contains the text 'Possible Attack or Infection: Destin...'. The other columns contain various IP addresses and port numbers.

Membership	Principal Variables	Protocol	FaddrIP	FaddrPort	LaddrIP	LaddrPort	Tr
0.0002000	Possible Attack or Infection: Destin...	UDP	192.168.0.227	138	10.1.1.248	138	1
0.0002000	Possible Attack or Infection: Destin...	TCP	192.168.0.227	139	10.1.1.168	4529	1
0.0002000	Possible Attack or Infection: Destin...	TCP	192.168.0.227	139	10.1.1.168	4524	1
0.0002000	Possible Attack or Infection: Destin...	TCP	192.168.0.227	139	10.1.1.168	4522	1
0.0002000	Possible Attack or Infection: Destin...	TCP	192.168.0.227	139	10.1.1.168	4520	1
0.0002000	Possible Attack or Infection: Destin...	TCP	192.168.0.227	139	10.1.1.168	4516	1
0.0002000	Possible Attack or Infection: Destin...	TCP	192.168.0.227	139	10.1.1.168	4501	1
0.0002000	Possible Attack or Infection: Destin...	TCP	192.168.0.12	110	10.1.1.204	1709	1
0.0002000	Possible Attack or Infection: Destin...	TCP	192.168.0.12	110	10.1.1.204	1704	1
0.0002000	Possible Attack or Infection: Destin...	TCP	192.168.0.12	110	10.1.1.204	1699	1
0.0002000	Possible Attack or Infection: Destin...	TCP	24.200.251.27	80	10.1.1.211	1368	1
0.0002000	Possible Attack or Infection: Destin...	UDP	192.168.0.6	138	10.1.1.169	138	1
0.0002000	Possible Attack or Infection: Destin...	TCP	192.168.0.227	139	10.1.1.176	4902	1
0.0002000	Possible Attack or Infection: Destin...	UDP	192.168.0.11	138	10.1.1.169	138	1
0.0002000	Possible Attack or Infection: Destin...	TCP	24.200.251.41	80	10.1.1.185	1075	1
0.0002000	Possible Attack or Infection: Destin...	TCP	192.168.0.12	110	10.1.1.173	1907	1
0.0002000	Possible Attack or Infection: Destin...	TCP	192.168.0.12	110	10.1.1.173	1902	1

The key information displayed in ASA Table-style Reports includes:

- **Membership:** Membership is a numeric score that indicates the extent to which the event deviates from the baseline. In simple terms, Membership indicates how unusual an event is. The lower the number, the more deviant the event and more critical the potential threat.

Events are also color-coded to indicate their level of severity.

-  Critical
-  High
-  Medium
-  Low

- **Threat Details/Principal Variables:** Threat Details and Principal Variables refer to the nature and possible cause of a suspicious event. Specifically, Principal Variables refers

to the aspects of the event that most contributed to its classification and numeric score. This information is provided to assist the administrator in pinpointing the vulnerability, intrusion, policy violation or other threat.

- **Other Columns:** The other columns displayed correspond to the variables contained in the analysis model itself.

## Table View – Right Mouse options

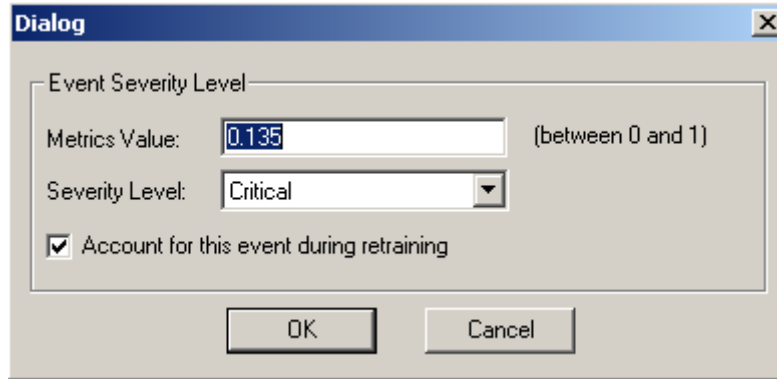
During the process of analysis, it will often be useful to impart some expert knowledge to Adaptive Security Analyzer regarding certain events. Some of these capabilities are enabled via right mouse click functionality. To invoke these options, **highlight an event in the Table View** and **apply the right mouse click**.

The screenshot shows the Adaptive Security Analyzer interface. On the left is a tree view of the configuration. The main window is titled 'Report Settings' and contains a table of events. A right-click context menu is open over the second row of the table, showing options: 'Mark as Bad', 'Mark as Good', 'Assign Severity Level...', and 'Properties'. The table has columns: Membership, Principal Variables, Protocol, FaddrIP, FaddrPort, and LaddrI.

Membership	Principal Variables	Protocol	FaddrIP	FaddrPort	LaddrI
0.0040100	Possible Port Scan: length=5, period=1	UDP	192.168.0.11	53	10.1.1
0.0040100	Possible Port Scan: length=5, period=1	TCP	192.168.0.11	135	10.1.1
0.0040100	Possible Port Scan: length=5, period=1	TCP	192.168.0.11	1026	10.1.1
0.0040100	Possible Port Scan: length=5, period=1	TCP	192.168.0.11	1026	10.1.1
0.0040100	Possible Port Scan: length=5, period=1	TCP	192.168.0.11	53	10.1.1
0.0050100	Possible IP Scan: length=6, period=1	TCP	165.254.12.106	80	10.1.1
0.0050100	Possible IP Scan: length=6, period=1	TCP	165.254.12.106	80	10.1.1
0.0050100	Possible IP Scan: length=6, period=1	TCP	165.254.12.106	80	10.1.1
0.0050100	Possible IP Scan: length=6, period=1	TCP	165.254.12.106	80	10.1.1
0.0050100	Possible IP Scan: length=6, period=1	TCP	165.254.12.115	80	10.1.1
0.0050100	Possible IP Scan: length=6, period=1	TCP	165.254.12.202	80	10.1.1
0.0057243	Possible Port Scan: length=7, period=900	UDP	192.168.0.11	53	10.1.1
0.0057243	Possible Port Scan: length=7, period=900	UDP	192.168.0.11	137	10.1.1
0.0057243	Possible Port Scan: length=7, period=900	UDP	192.168.0.11	138	10.1.1
0.0057243	Possible Port Scan: length=7, period=900	UDP	192.168.0.11	138	10.1.1

Events that have been incorrectly classified can be adjusted by assigning a correct classification in a few ways. Events that have been re-classified will be listed as such in the Threat Details/Principal Variables column as **“Reclassified Event”**.

- **Mark as Bad:** Marking an event as Bad will assign the event with a **Membership Value** of **.01**.
- **Mark as Good:** Marking an event as Good will assign the event with a **Membership Value** of **.75**.
- **Assign Severity Level:** This option allows a specific Membership value to be assigned to the event.



- **Properties:** Selecting the Properties options will invoke the Event Details screen.

## Event Detail View

Each event may be an isolated event or an event sequence. To view the details of an event, **highlight** and **double-click** an event in the Table report view.

The 'Event Properties' dialog box shows the following information:

- Schema:** Slow Scan Schema
- Membership:** 0.0000100
- Threat Type:** Possible slow Port (FaddIPort) scan: length=288, period=300
- Table:**

Name	Analyzed Event	Basis Event	Impact
Action	Built dynamic TCP ...		
FaddIP	192.168.0.7		
FaddIPort	28531		
GaddIP			
GaddIPort			
LaddIP	10.1.1.169		
LaddIPort	4960		
-----			
Action	Built dynamic TCP ...		
FaddIP	192.168.0.7		
FaddIPort	33404		
GaddIP			
GaddIPort			

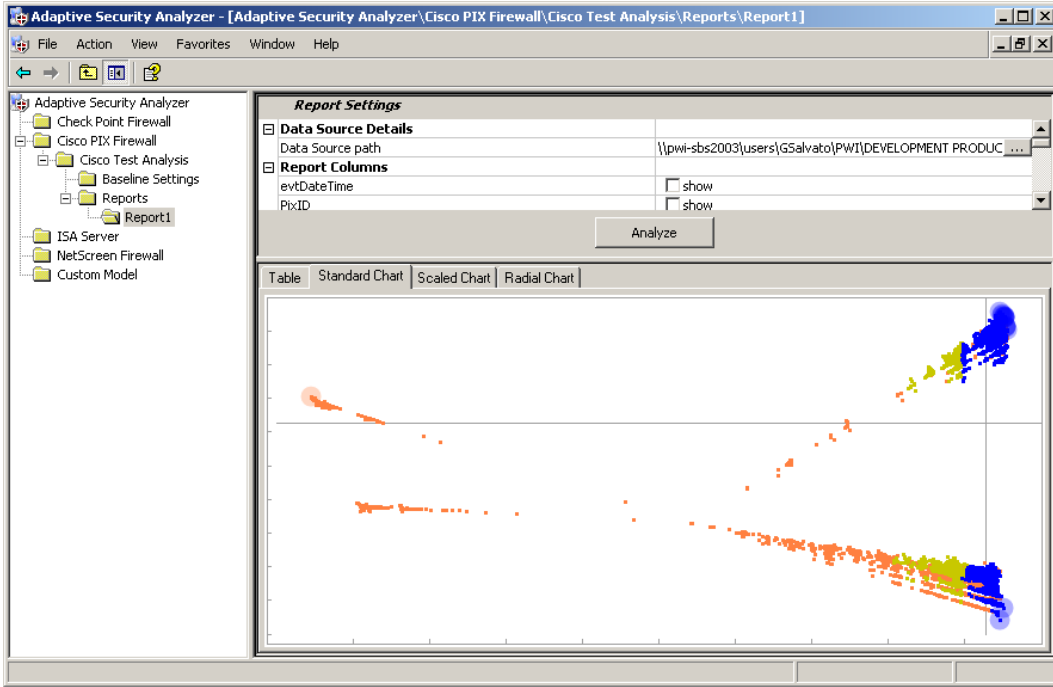
The top field in the Event Details screen indicates whether an Adaptive Security Analyzer **schema** or the **behavioral engine** detected the event. In the example to the left, the sequence of events matched the **Slow Scan Schema**.

The Membership value is displayed and the possible type of threat.

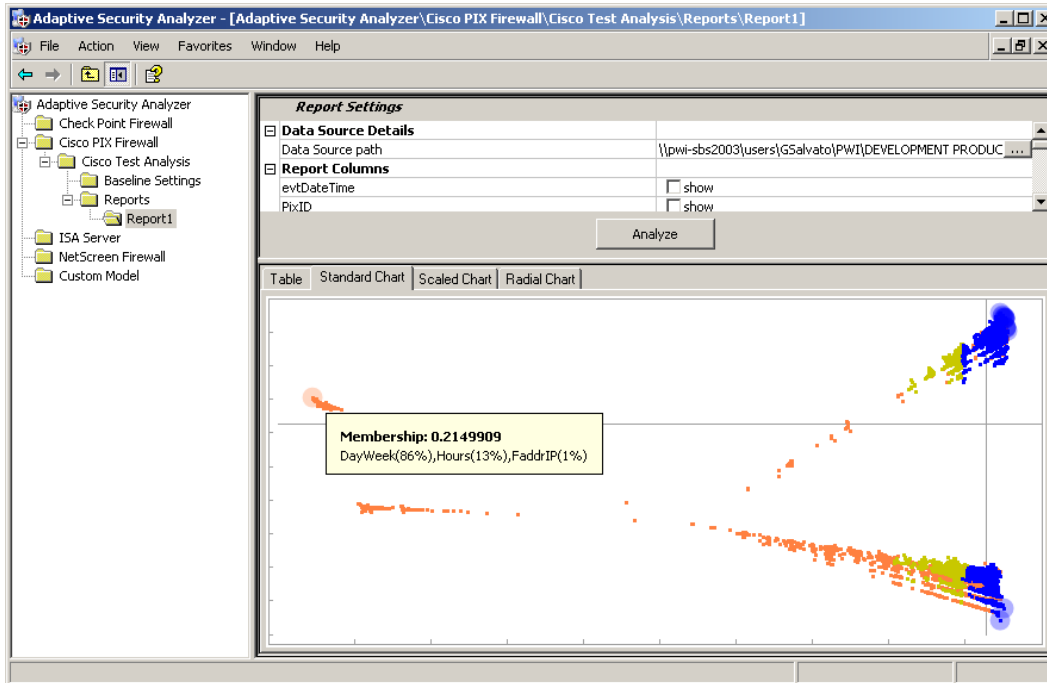
The main body of the event detail screen shows all of the events within an event sequence.

## Chart Views

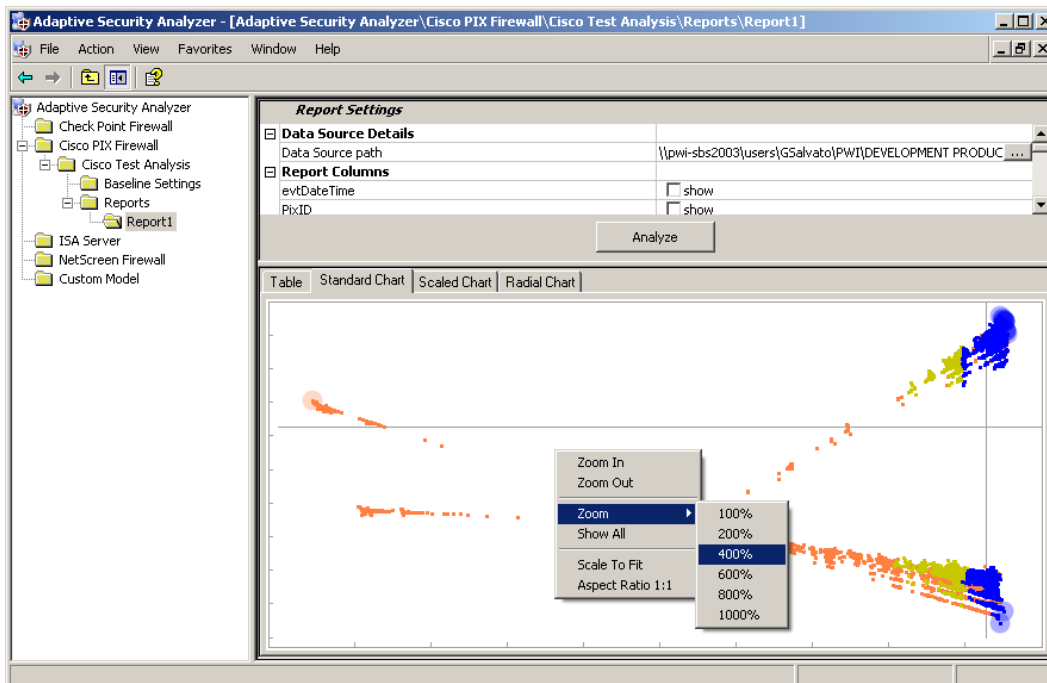
The Adaptive Security Analyzer Chart View provides a visual representation of the events displayed in the standard Table View report. The Chart View works similarly to the Table View in that specific points in the chart may be double-clicked to reveal the details regarding that event. ASA offer three different graphical displays; Standard, Scaled and Radial.



Placing the cursor focus on a single point (event) on the Chart displays the Membership Value and the Threat Details and/or Principal Variables of the event.



Placing the cursor focus on a single point (event) on the Chart and applying a right mouse click provides a **Zoom** feature that enables the Chart View to be increased or decreased.



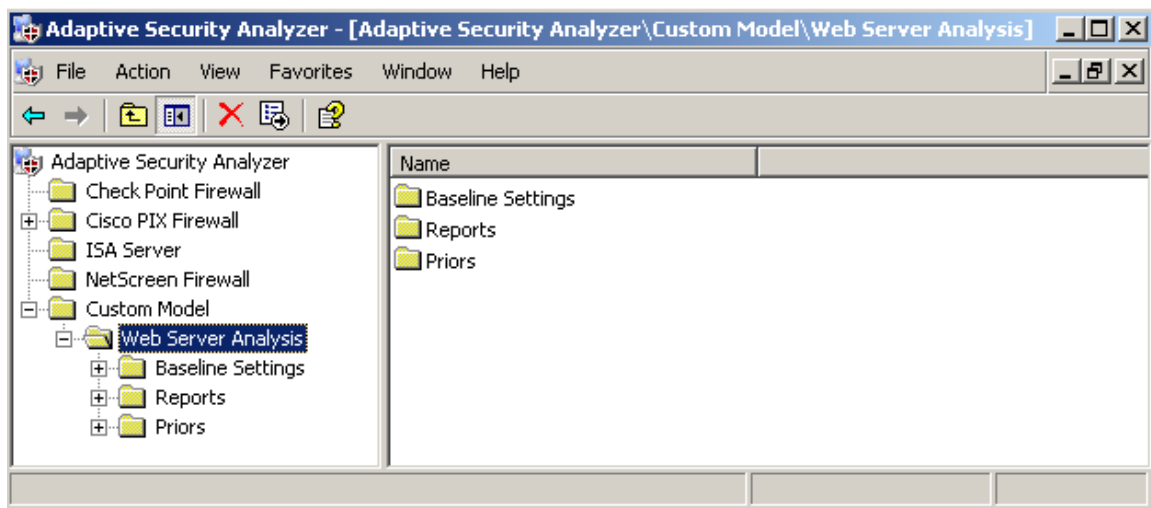
## Custom Models

Adaptive Security Analyzer includes pre-built models for specific data/device types. These are listed under the main Adaptive Security Analyzer MMC node. Custom Analysis can also be performed for devices and data for which no pre-built models are available. Custom Analysis can be performed using any ODBC compliant data source, including SQL, Oracle, etc.

The process of working with Custom Models is very similar to working with pre-built models, with some important exceptions. This Section will illustrate the fundamental steps required to create a Custom Model and conduct analysis.

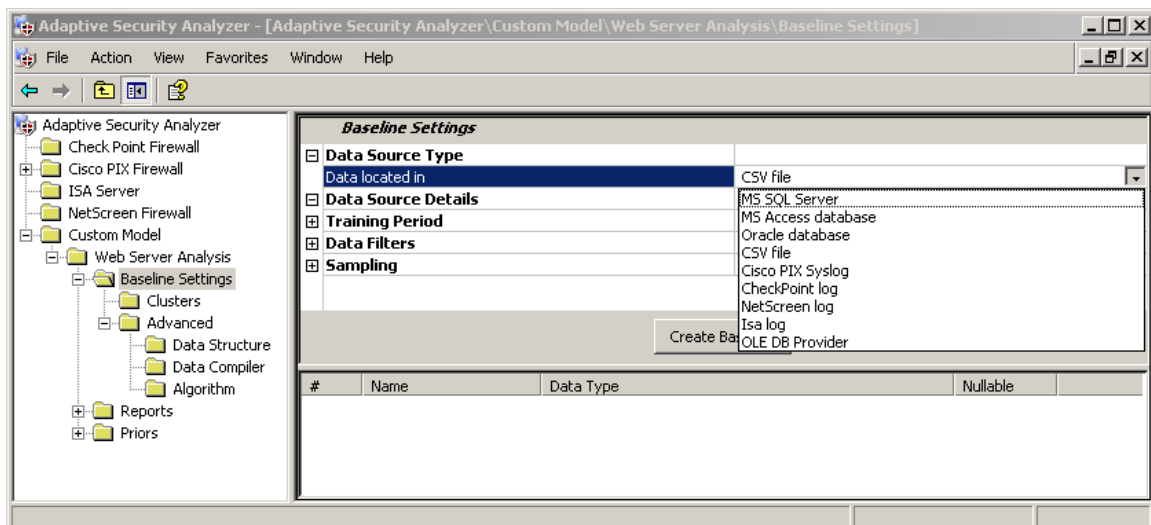
To begin, right mouse click **Custom Model -> New -> Model**.

Provide a Name for the Custom Model.

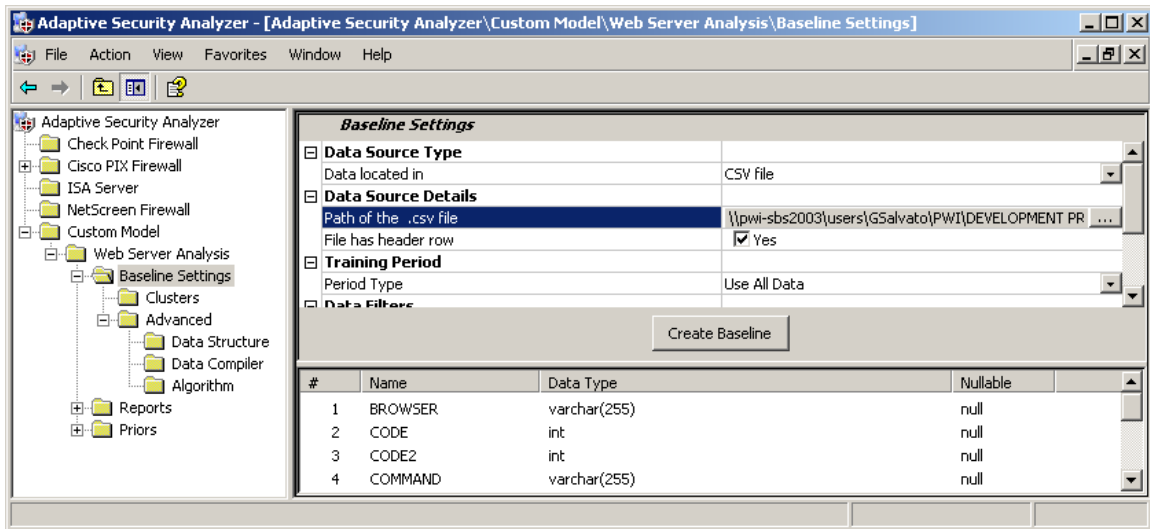


## Baseline Settings

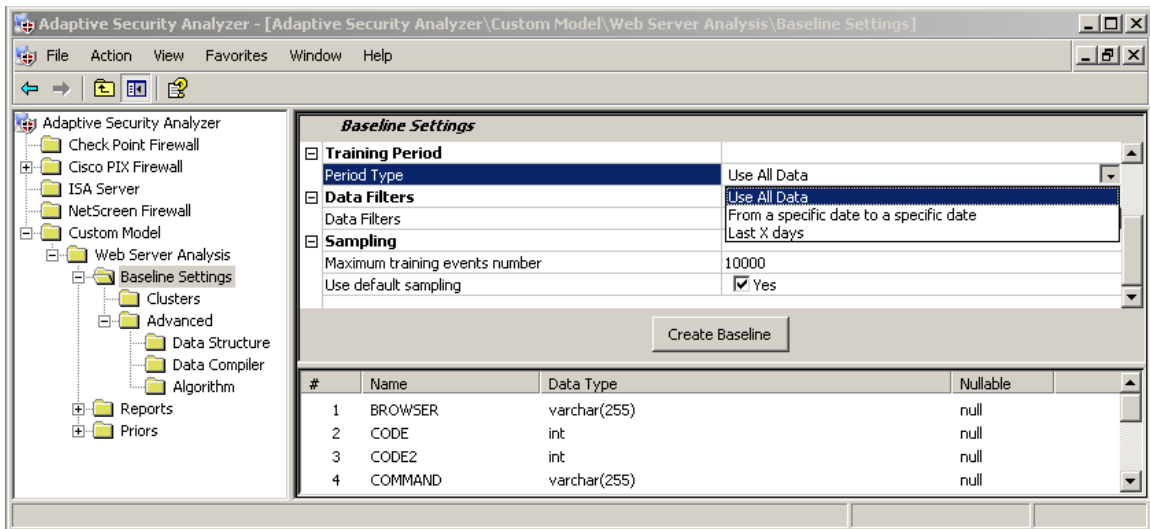
Select the **Baseline Settings** Folder. Identify the type or format of the data that will be analyzed.



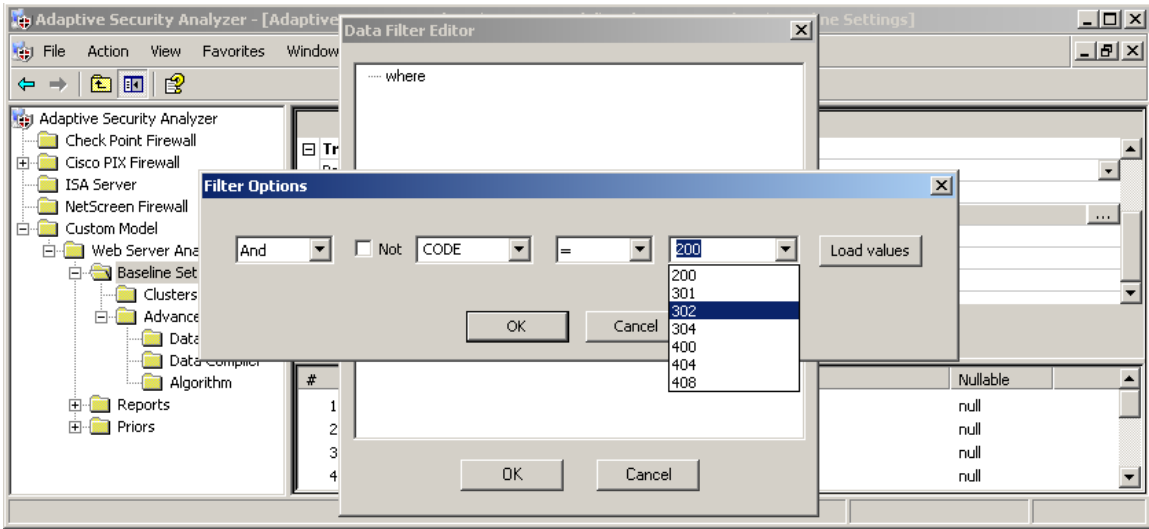
Specify the Data path and indicate whether the file has a header row.



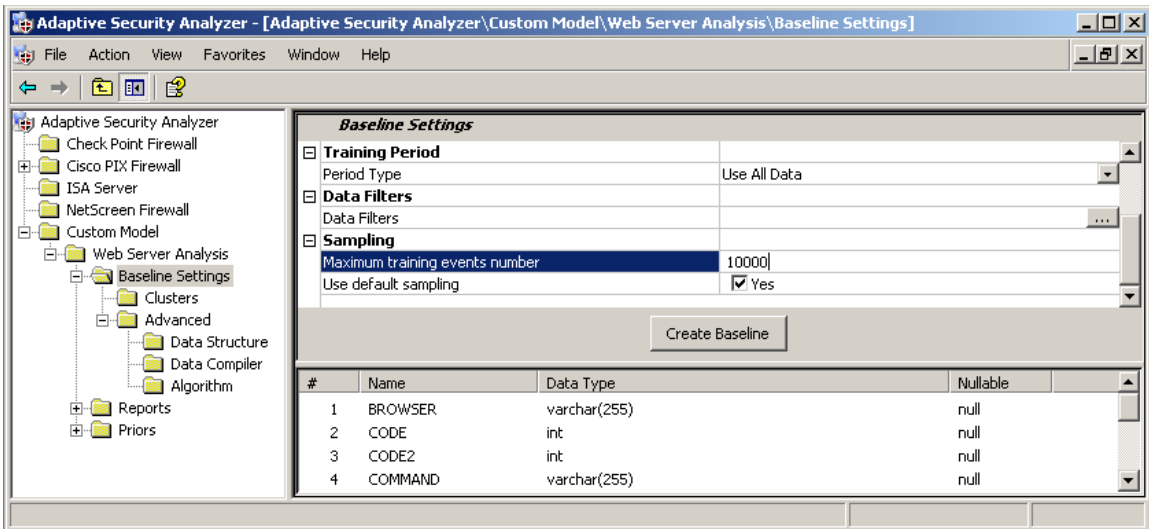
Indicate the range of data on which the baseline should be created.



Specify Data Filters.



Specify the maximum number of events to use to create the baseline and whether Sampling should be used. ASA will suggest default values for these attributes.



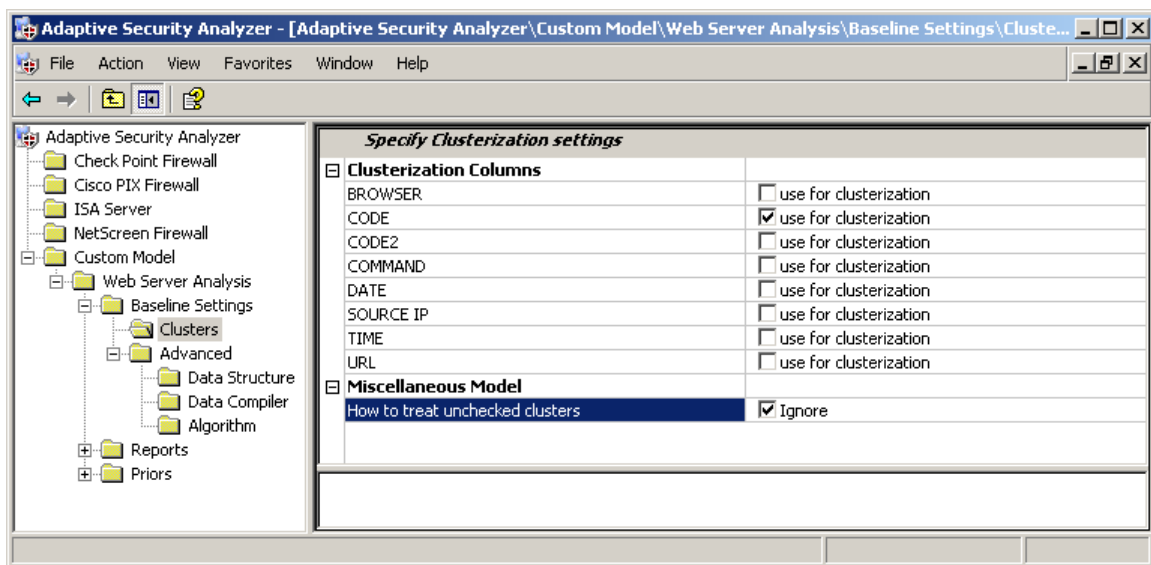
**Note:** Once these primary Baseline Settings attributes have been defined **DO NOT SELECT THE CREATE BASELINE BUTTON YET**. See next section. The Custom Model **DATA STRUCTURE** (within the **Advanced** folder) must be specified.

<p>Process Status dialog box content: Start training Please wait while Adaptive Security Analyzer is processing the data. If size of the data is large - it may take minutes or hours to finish. Cluster Web Server Analysis Train failed: Can not train this model because it does not have column Total time elapsed: 0:00:00:00</p>	<p>An error message will be displayed indicating that you have not yet specified the Custom Model columns yet.</p>
--	--

## Clusters

ASA can create a comparative baseline/s that is organized relative to all of data in aggregate or around multiple sub-groups. For example, a data source may contain log files from multiple of Web servers. By default, ASA will consider the logs from each of these servers as a single group. But it may be of interest to create separate baselines and conduct analysis for each server. In this case, the column **ServerName** can be specified in the Cluster Settings and this variable will become the central analytic element and serve as the basis from which all sub models will be created.

A separate Report folder will be created for each column selected in the Cluster Settings. For each Cluster Column (data variable), a separate Report will be created as output will be oriented around each Cluster (model center) specified. In the screen shot below, sub-models will be created for each **Code** reflected in the data file.



Once the Baseline Settings (including sub-models, if any) and the Data Structure have been specified, the baseline can be created. To do so, press the **Create Baseline** button.

Once ASA has finished creating the baseline, sub-folders reflecting each unique attribute within the column specified in **Clusters** will be created. To view details about a Cluster, highlight a folder and information will be displayed in the right panel.

The screenshot shows the Adaptive Security Analyzer interface. The left pane displays a tree view of the project structure, including folders for Check Point Firewall, Cisco PIX Firewall, ISA Server, NetScreen Firewall, Custom Model, Web Server Analysis, Baseline Settings, Clusters, Advanced, Data Structure, Data Compiler, Algorithm, Reports, Report1, and Priors. The right pane shows the 'Cluster Training Results' for CODE=200. Below the summary panel is a table of training data.

#	Membership	BROWSER	CODE	COMMAND	DATE
1	0.8378475	Mozilla/4.0 (compatible; MSIE 7.0; ...	200	GET / HTTP/1.1	2/27
2	0.7980388	Mozilla/5.0 (Windows; U; Windows...	200	GET / HTTP/1.1	2/28
3	0.7572914	Mozilla/5.0 (Macintosh; U; Intel Ma...	200	GET / HTTP/1.1	2/26
4	0.6297432	Mozilla/4.0 (compatible; MSIE 7.0; ...	200	GET /img/top_banner_left_pwi.jpg HT...	3/1/2
5	0.8244674	Mozilla/4.0 (compatible; MSIE 6.0; ...	200	GET / HTTP/1.1	2/27
6	0.7455527	Mozilla/4.0 (compatible; MSIE 7.0; ...	200	GET /img/top_banner_left_pwi.jpg HT...	2/26
7	0.7480503	Mozilla/5.0 (Macintosh; U; PPC Ma...	200	GET /img/header_gray_topright.gif H...	2/26
8	0.7398759	Mozilla/4.0 (compatible; MSIE 7.0; ...	200	GET /img/menu/home1.gif HTTP/1.1	2/26
9	0.7912432	Opera/9.10 (Windows NT 5.1; U; en)	200	GET /img/zardel.gif HTTP/1.1	2/27
10	0.799607	Mozilla/5.0 (Windows; U; Windows...	200	GET /img/pwi_top_right_banner.gif H...	2/27
11	0.7222657	Mozilla/4.0 (compatible; MSIE 6.0; ...	200	GET /img/menu/solutions1.gif HTTP/1.1	2/26
12	0.7734324	Mozilla/4.0 (compatible; MSIE 6.0; ...	200	GET /img/top_banner_left_pwi.jpg HT...	2/27
13	0.7517368	Mozilla/4.0 (compatible; MSIE 6.0; ...	200	GET /img/top_banner_left_pwi.jpg HT...	2/27
14	0.7364992	Mozilla/4.0 (compatible; MSIE 6.0; ...	200	GET / HTTP/1.1	2/28

In addition, **Report sub-folders** reflecting each unique attribute within the column specified in **Clusters** will be created. Here, general or specific criteria can be defined relevant to all or individual reports.

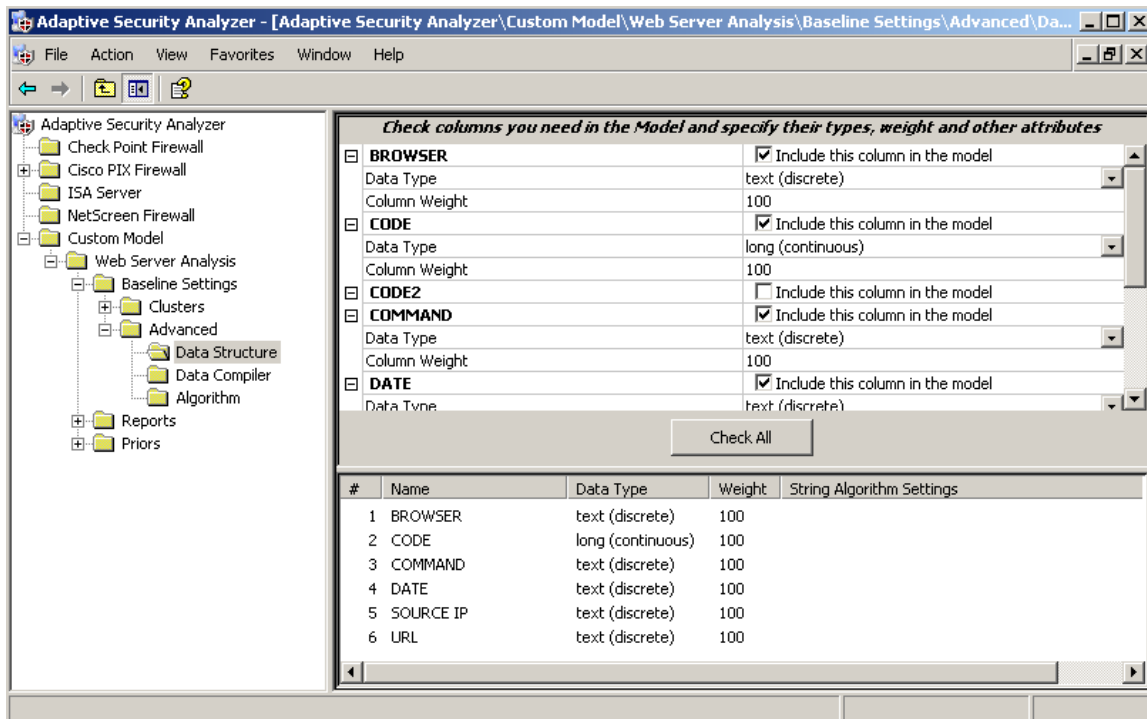
Options for Reports settings and configuration in Custom Models are identical to those in the default models with a few key differences. Refer to the Custom Models Reports section for more information.

## Advanced

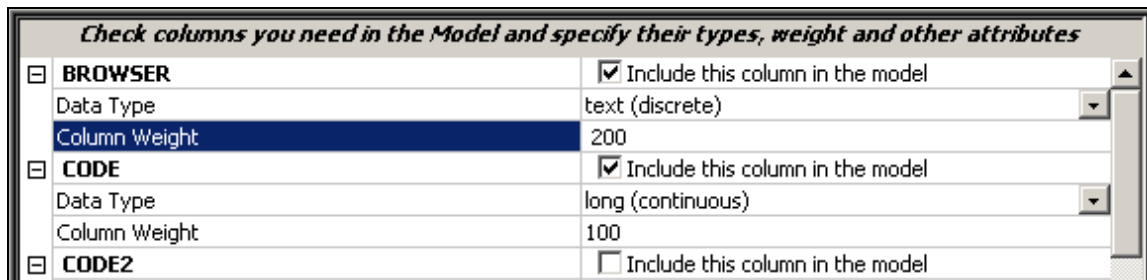
### Data Structure

One of the primary requirements for working with Custom Models that differs from working with pre-built models is selecting the columns (or variables) that will comprise the Custom Model. In the same manner as you might home in on certain columns within data for manual analysis, check the boxes next to the columns that should be considered by ASA for the purpose of creating the analysis baseline for this Custom Model.

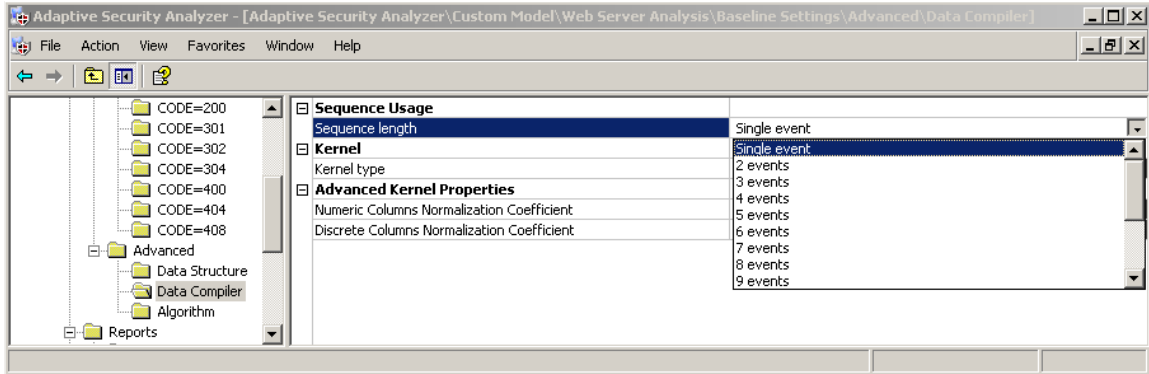
To do so, expand the **Advanced** folder and open the **Data Structure** folder. In the right panel will be displayed all of the columns within the database or file selected. Check the box next to the columns that should be included in the Custom Model.



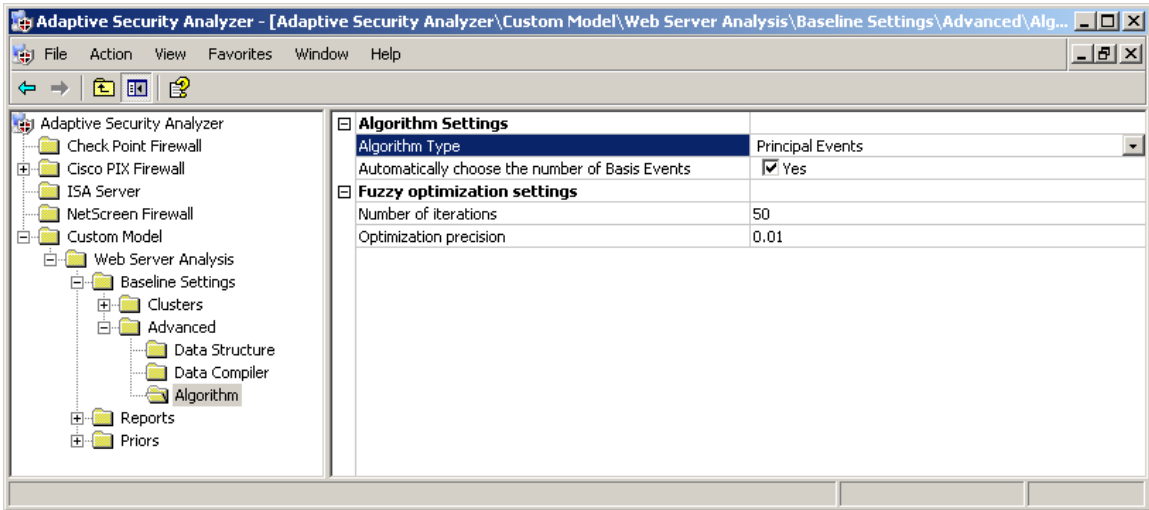
It may be appropriate to assign a weight to one or more variables that reflects a greater or lesser degree of importance than the others. To do so, highlight the **Column Weight** numeric value and enter the desired value.



## Data Compiler



## Algorithm



## Reports

Options for Reports setting and configuration in Custom Models are identical to those in the default models with a few key differences as well as additional control over report display as described below.

### Severity Level Thresholds

Severity Level thresholds can be adjusted by changing their numeric range. To do so, highlight the value associated with the appropriate Severity Level and enter the desired number.

The screenshot shows the 'Report Settings' window for a custom model. The 'Severity Level Thresholds' section is expanded, showing a table with columns for Severity Level and a numeric value. The 'Severity Levels' section is collapsed. Below the settings is a table of report data.

Severity Level	Value
High	0.15
Medium	0.3
Low	0.5

Membership	Principal Variables	BROWSER	CODE
0.1621525	BROWSER(34%),URL(33%),SOURCE IP(...)	Mozilla/4.0 (compatible; N...	200
0.1655543	BROWSER(36%),URL(36%),SOURCE IP(...)	Mozilla/4.0 (compatible; M...	200
0.1818250	URL(45%),BROWSER(37%),SOURCE IP(...)	nokia6610i/1.0 (4.10) Pro...	200
0.1844915	URL(43%),BROWSER(36%),SOURCE IP(...)	nokia6610i/1.0 (4.10) Pro...	200
0.1882460	BROWSER(43%),SOURCE IP(30%),COM...	Factbot 1.09 (see http://...	200
0.1882460	BROWSER(43%),SOURCE IP(30%),COM...	psbot/0.1 (+http://www...	200
0.1890469	BROWSER(43%),SOURCE IP(30%),COM...	Baiduspider+(+http://ww...	200

### Severity Levels

Severity Levels that should be displayed in report output can be specified by checking or unchecking the applicable box. By default, ASA displays events falling into all Severity Level categories.

The screenshot shows the 'Report Settings' window for a custom model. The 'Severity Levels' section is expanded, showing a table with columns for Severity Level and a checkbox. The 'Severity Level Thresholds' section is collapsed. Below the settings is a table of report data.

Severity Level	Value
Critical	<input checked="" type="checkbox"/> Yes
High	<input checked="" type="checkbox"/> Yes
Medium	<input checked="" type="checkbox"/> Yes
Low	<input checked="" type="checkbox"/> Yes

Membership	Principal Variables	BROWSER	CODE
0.1621525	BROWSER(34%),URL(33%),SOURCE IP(...)	Mozilla/4.0 (compatible; N...	200
0.1655543	BROWSER(36%),URL(36%),SOURCE IP(...)	Mozilla/4.0 (compatible; M...	200
0.1818250	URL(45%),BROWSER(37%),SOURCE IP(...)	nokia6610i/1.0 (4.10) Pro...	200
0.1844915	URL(43%),BROWSER(36%),SOURCE IP(...)	nokia6610i/1.0 (4.10) Pro...	200
0.1882460	BROWSER(43%),SOURCE IP(30%),COM...	Factbot 1.09 (see http://...	200

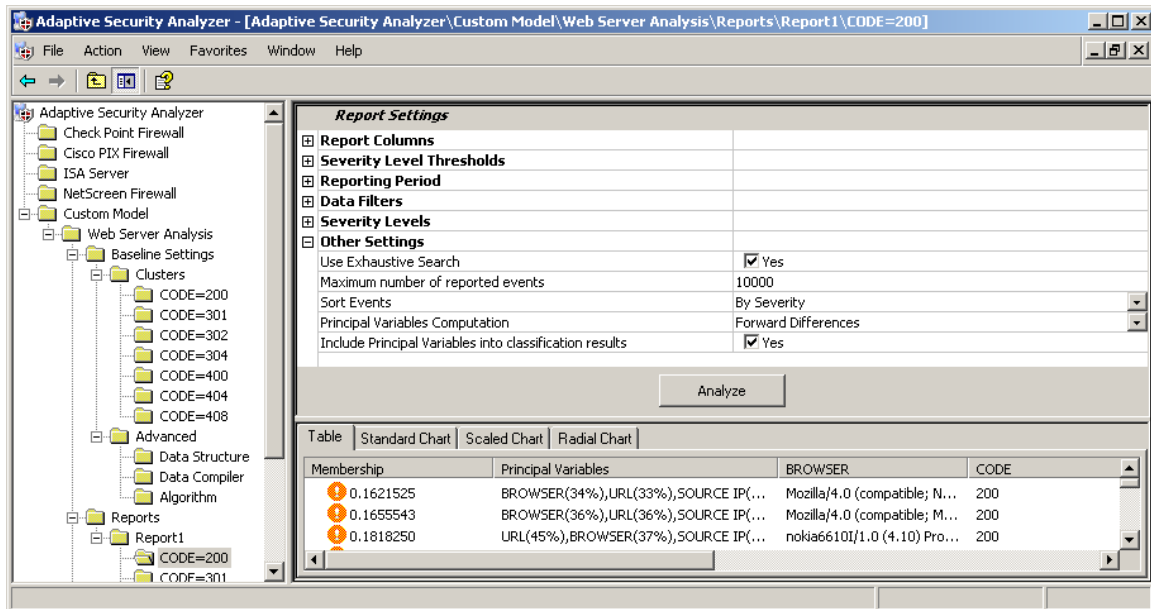
## Other Settings

Other Settings are identical to those include in pre-built models with a few exceptions.

**Use Exhaustive Search:** Enabled by default in Custom Models as well as pre-built models.

**Principal Variables Computation:** Offers computation using either Forward or Inverse Differences.

**Include Principal Variables:** By selecting this option, ASA will provide a numeric value to each attribute within an analytic model that reflects the respective contribution of the variable to an event's Membership Value.



The screenshot shows the Adaptive Security Analyzer interface with the 'Report Settings' dialog box open. The dialog is titled 'Report Settings' and contains several sections: Report Columns, Severity Level Thresholds, Reporting Period, Data Filters, Severity Levels, and Other Settings. The Other Settings section is expanded, showing options for 'Use Exhaustive Search' (checked), 'Maximum number of reported events' (10000), 'Sort Events' (By Severity), 'Principal Variables Computation' (Forward Differences), and 'Include Principal Variables into classification results' (checked). Below the settings is an 'Analyze' button. At the bottom of the dialog, there is a table view showing the results of the analysis.

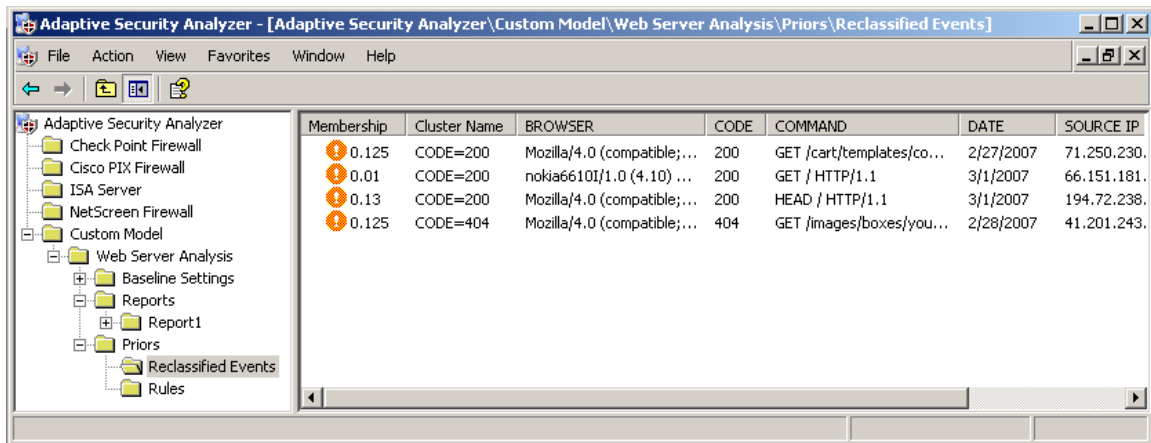
Membership	Principal Variables	BROWSER	CODE
0.1621525	BROWSER(34%),URL(33%),SOURCE IP(...)	Mozilla/4.0 (compatible; N...	200
0.1655543	BROWSER(36%),URL(36%),SOURCE IP(...)	Mozilla/4.0 (compatible; M...	200
0.1818250	URL(45%),BROWSER(37%),SOURCE IP(...)	nokia6610i/1.0 (4.10) Pro...	200

## Priors

There are two categories of Priors; Reclassified Events and Rules.

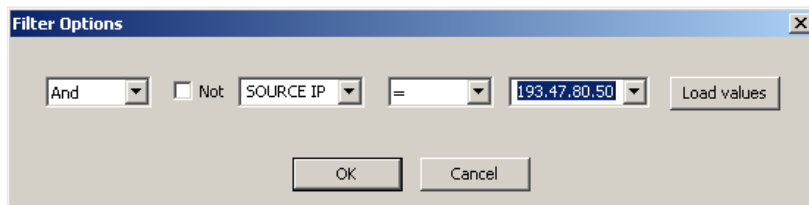
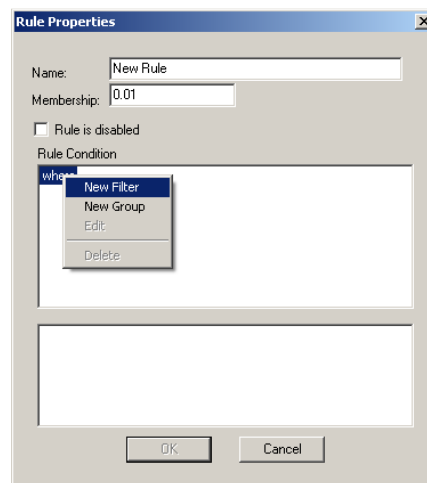
### Reclassified Events

The Reclassified Events folder displays all events where the Severity Level of classification has been manually changed.



## Rules

Rules can be created using standard SQL query syntax. To create a rule, apply the right mouse function in the right panel and select Create Rule.



The Rule Properties dialog will be displayed. Enter a rule Rule and click OK.

## Supported Firewalls and Log Formats

### *Custom Models*

Adaptive Security Analyzer supports XML, CSV, ASCII, MDB, SQL, Oracle, and ODBC compliant data source.

### *Check Point FireWall-1*

#### Log format

ID | Date | Time | Product | Interface | Firewall | Type | Action | Service | Source | Destination | Protocol | Rule | Source Port | Translation | User | Information

#### Example

```
"1" "25Dec2004" "0:00:01" "VPN-1 & FireWall-1" "eth-s5p1c0" "asi-fw1" "Log" "Accept" "ldap"
"wks-asiexchfe01" "wks-asic01" "tcp" "32" "15656" "" ""
"2" "25Dec2004" "0:00:04" "VPN-1 & FireWall-1" "eth-s4p1c0" "asi-fw1" "Log" "Accept" "snmp-
read" "wks-asiworkbench" "asi-fw1" "udp" "9" "54862" "" ""
```

#### Processed events

ASA supports Check Point Firewall-1 traffic logs. Only events with successfully established TCP and UDP sessions will be processed.

Type field should contain "Log"  
 Protocol field should be "TCP" or "UDP"  
 Action field should contain "Accept"

#### Processed Fields

Date -  
 Time -  
 Service - the service (destination port) requested by this communication;  
 Source - the source of the communication;  
 Destination - the destination of the communication;  
 Protocol - the communication protocol used;  
 Source Port -

### *Cisco Pix Firewall v6 log in CiscoPIX syslog format*

#### Log format

ID | Date | Time | Severity | Message Code | Message

There the message is:

Built {inbound | outbound} TCP connection number for interface\_name:real\_address/real\_port (mapped\_address/mapped\_port) to interface\_name:real\_address/real\_port (mapped\_address/mapped\_port) [(user)].

Teardown TCP connection number for interface\_name:real\_address/real\_port to interface\_name:real\_address/real\_port duration time bytes number [reason] [(user)]

Built {inbound | outbound} UDP connection number for interface\_name:real\_address/real\_port (mapped\_address/mapped\_port) to interface\_name:real\_address/real\_port (mapped\_address/mapped\_port) [(user)]

Teardown UDP connection number for interface\_name:real\_address/real\_port to interface\_name:real\_address/real\_port duration time bytes number [(user)]

### Example

```
<164>Feb 17 2006 20:10:37: %PIX-6-302013: Built inbound TCP connection 2095610 for
outside:192.168.5.23/193 (192.168.5.23/193) to inside:10.1.1.5/80 (10.1.1.5/80)
<164>Feb 17 2006 20:10:37: %PIX-6-302013: Built inbound TCP connection 2095650 for
outside:192.168.6.203/293 (192.168.6.203/293) to inside:10.1.1.7/80 (10.1.1.7/80)
```

### Processed events

ASA processes events with Level 6 severity (informational) only. Only events with successfully established TCP and UDP sessions will be processed by ASA.

Cisco PIX Event IDs: 302001, 302002, 302013, 302014, 302015, 302016

### Processed fields

- Date
- Time
- Real\_address - the source and the destination of the communication;
- Real\_port - the source port and the destination port of the communication;
- Bytes number – bytes transmitted

## *Juniper NetScreen (OS 5.0)*

### Log format

Date | Time | Module | Severity | Type | Message Text

There the message is:

```
May 18 15:59:26 192.168.10.1 ns204: NetScreen device_id=-0029012002000170
system notification-0025 (traffic): start_time="" duration=
policy id= service= proto= src zone={Trust | Untrust } dst zone={Trust | Untrust }
action= sent= rcvd= src= dst= src_port= dst_port= translated ip= port=
```

### Example

```
messages:Dec 17 09:35:23 10.14.93.7 ns5xp: NetScreen device_id=ns5xp system-notification-
00257(traffic): start_time="2002-12-17 09:40:13" duration=5 policy_id=0 service=dns proto=17
src zone=Trust dst zone=Untrust action=Permit sent=86 rcvd=140 src=10.14.94.221
dst=10.14.99.10 src_port=1029 dst_port=53 translated ip=10.14.93.7 port=1207
messages:Dec 17 09:35:23 10.14.93.7 ns5xp: NetScreen device_id=ns5xp system-notification-
00257(traffic): start_time="2002-12-17 09:40:13" duration=5 policy_id=0 service=tcp/port:8000
```

```

proto=6 src zone=Trust dst zone=Untrust action=Permit sent=1379 rcvd=30991 src=10.14.94.221
dst=10.14.90.217 src_port=1030 dst_port=8000 translated ip=10.14.93.7 port=1208
messages:Dec 17 09:35:25 10.14.93.7 ns5xp: NetScreen device_id=ns5xp system-notification-
00257(traffic): start_time="2002-12-17 09:40:16" duration=4 policy_id=0 service=tcp/port:8000
proto=6 src zone=Trust dst zone=Untrust action=Permit sent=720 rcvd=536 src=10.14.94.221
dst=10.14.90.217 src_port=1031 dst_port=8000 translated ip=10.14.93.7 port=1209

```

### Processed events

ASA FW process events of NetScreen Firewall with "system-notification" severity level and 00257( traffic ) type.  
events with successfully established TCP and UDP sessions will be processed by ASA FW .

Protocol should be "6" or "17"  
action=Permit

### Processed fields

Date -  
Time -  
Proto – the communication protocol used;  
Sent – bytes sent  
Rcvd – bytes received  
Src - the source of the communication;  
Src\_port -  
Dst - the destination of the communication;  
Dst\_port – the destination port requested by this communication

## MS ISA Server Firewall Log in W3C format

### Log format

Computer | Date | Time | IP protocol | Source | Destination | Original client IP | Source network | Destination network | Action | Status | Rule | Application protocol | Bidirectional | Bytes sent | Bytes sent intermediate | Bytes received | Bytes received intermediate | Connection time | Connection time intermediate | Source proxy| Destination proxy | Source name | Destination name | Username | Agent | Session ID | Connection ID | Interface | IP header | Protocol payload |

### Example

```

PWI-3KSQL1 2006-10-17 00:00:48 TCP 192.168.20.251:2990
80.231.19.81:80 192.168.20.251 Local Host External Establish
0x0 Allow HTTP/HTTPS requests from ISA Server to specified sites HTTP N
0 0 0 0 - - - - - - -
- 1859 3258 - - - - - -
PWI-3KSQL1 2006-10-17 00:00:48 UDP 192.168.20.251:1048
192.168.20.250:53 192.168.20.251 Local Host Internal Establish 0x0
Allow DNS from ISA Server to selected servers DNS Y 0 0 0
0 - - - - - - - - - 1859 3259
- - -
PWI-3KSQL1 2006-10-17 00:00:49 TCP 192.168.20.251:2991
80.231.19.81:80 192.168.20.251 Local Host External Establish

```

0x0	-	HTTP	N	0	0	0	0	-	-	-
-	-	-	-	-	1859	3260	-	-	-	-

### Processed events

ASA FW process events of ISA Server Firewall log file only with the following rules.

“Source Network” field or “Destination” field should contain “External” ;  
IP\_protocol should be "TCP" or "UDP".

### Processed fields

Date

Time

IP\_protocol – the communication protocol used;

Source - the source of the communication;

Destination- the destination of the communication;

Destination\_port – the destination port requested by this communication;

Bytes\_sent – bytes sent

Bytes\_received – bytes received

Connection\_time – the time of connection

## Adaptive Security Analyzer

### User Guide

#### **CONTACT INFORMATION**

Privacyware  
68 White Street, 2<sup>nd</sup> Flr.  
Red Bank, NJ 07701  
Email: [info@privacyware.com](mailto:info@privacyware.com)  
URL: <http://www.privacyware.com>

Email support: [support@privacyware.com](mailto:support@privacyware.com)  
Product Information: [www.privacyware.com/ASAP.html](http://www.privacyware.com/ASAP.html)

Adaptive Security Analyzer, Edition 2.01.08.10. (January, 2010) - Privacyware.

Copyright © 2002-2010 PWI, Inc./Privacyware. All rights reserved.