



The Versatile BI Solution!

## Click & DECiDE Quick Installation Guide

*For Proof of Concept*

*For Demonstrations*

*For Free Evaluation Licenses*

In this document, we are going to study how to install Click&DECiDE for a proof of concept, or a demonstration

Should you have any question about this document, or would you like some help, please contact:

**Benoît Rostagni**

**Tel: +33 1 79 71 84 22**

**GSM: +33 6 82 88 94 17**

**email: [benoit.rostagni@clickndecide.com](mailto:benoit.rostagni@clickndecide.com)**

## Table of Contents

1.	Soft-Appliance installation .....	4
2.	Pre-installation check list .....	4
2.1.	Hardware Environment .....	4
2.2.	Software Environment .....	4
3.	Install Click & DECiDE - NSI .....	5
3.1.	Turning on the Required IIS Features .....	5
3.2.	Download and install the Framework .NET 3.5 SP1 .....	5
3.3.	Download and extract the Click & DECiDE - NSI setup .....	5
3.4.	The Click and DECiDE - NSI Installation Wizard .....	6
4.	Configuration of Click&DECiDE NSI Demo device .....	10
4.1.	Enter your License Certificate .....	10
5.	Run the first Demo test logs .....	16
5.1.	View Performance counter .....	16
5.2.	Log Acquisition .....	18
5.3.	Control the database insertion.....	18
6.	Report Generation .....	20
6.1.	Generate a Dynamic Report.....	21
7.	Report analysis.....	23
7.1.	Firewall report analysis .....	23
7.2.	IPS report analysis.....	23
7.3.	Proxy report analysis .....	23
8.	Investigation .....	24
8.1.	Firewall investigation .....	24
8.2.	IDS/IPS investigation .....	26
8.3.	Proxy investigation.....	29
9.	Add you own devices .....	30
10.	Exercise solutions .....	31
11.	Data and Users available in Click&DECiDE Soft Appliance.....	32
11.1.	Data available in SQL database .....	32
11.2.	Users available .....	32
11.2.1.	Administrator user screen access: .....	32
11.2.2.	Demonstration user screen access: .....	33



## 1. Soft-Appliance installation

If you are using a Soft Appliance, please refer to the following guide:

Click&DECiDE\_NSI\_Soft\_Appliance\_Quick\_Installation\_Guide

*After installation of the soft Appliance, go directly to chapter 4 and validate the DEMO device installation before using it on your own equipments.*

## 2. Pre-installation check list

### 2.1. Hardware Environment

The hardware expected to test the solution can be a physical hardware or a logical hardware i.e. a virtual machine (Microsoft Virtual Server or VmWare).

Configuration expected:

- Single Processor Dual or Quad Core
- 2 to 4 Gb RAM
- 80 Gb usable disk, depending on test volume.

*Note that if you use a virtual server, you may experience a lower quality of the response time due to the virtual disk architecture.*

### 2.2. Software Environment

The software environment expected is server type system. For test purpose, you may also use a workstation environment:

Systems & Database

- Windows ® 7 32bit
  - Microsoft SQL Express 2005 (SP3) 32bit
  - Microsoft SQL Express 2008 (SP1) 32bit (preferred to 2005)
- Windows ® 7 64bit
  - Microsoft SQL Express 2008 (SP1) 64bit
- Windows ® 2003 (minimum SP2) 32bit
  - Microsoft SQL Server 2005 (SP3) 32bit
  - Microsoft SQL Express 2005
- Windows ® 2008 (minimum SP1) 32bit
  - Microsoft SQL Server 2008 (SP1) 32bit
- Windows ® 2008 (minimum SP1) 64bit
  - Microsoft SQL Server 2008 (SP1) 64bit

*Note that if you use Microsoft SQL Express 2005, you will be limited in concurrent access to the database and also in quantity of data for your tests (less than 500.000 EPD [Event Per Day]).*

- Other Software requested:
  - Adobe Acrobat Reader (Minimum v7)



- IIS (Internet Information Service)
- Internet Explorer 7.0 (Minimum SP1) or higher version of IE
- Framework .NET 3.5 (Minimum SP1)

**IIS must be installed before .NET**

*If not, or if you are not sure, please run the following command for the .NET directory:*

.NET Directory: **C:\Windows\Microsoft.NET\Framework\v2.0.50727**

Command to run: **aspnet\_regiis -i**

## 3. Install Click & DECiDE - NSI

*Note: the operations described in this article require a full access to the computer. Be sure to be logged as an Administrator.*

### 3.1. Turning on the Required IIS Features

IIS is a Windows feature, to launch the Turn Windows Features On or Off module please follow the steps below:

1. Select Start> Control Panel.
2. Click Programs and Features.
3. Click Turn Windows Features On or Off
4. Select the following Internet Information Services features:
5. Web Management Tools
  - a. IIS Management Console
  - b. IIS Management Scripts and Tools
  - c. IIS Management Service
6. World Wide Web Services
  - a. Applications Development Features
    - i. ASP.NET
    - ii. ASP
  - b. Security
    - i. Basic Authentication
    - ii. Windows Authentication
7. Click OK

### 3.2. Download and install the Framework .NET 3.5 SP1

Click&DECiDE need the Framework .NET to work properly. We recommend you to install the latest version before installing Click&DECiDE. Follow the link and install the framework:

<http://www.microsoft.com/downloads/details.aspx?familyid=AB99342F-5D1A-413D-8319-81DA479AB0D7&displaylang=en>

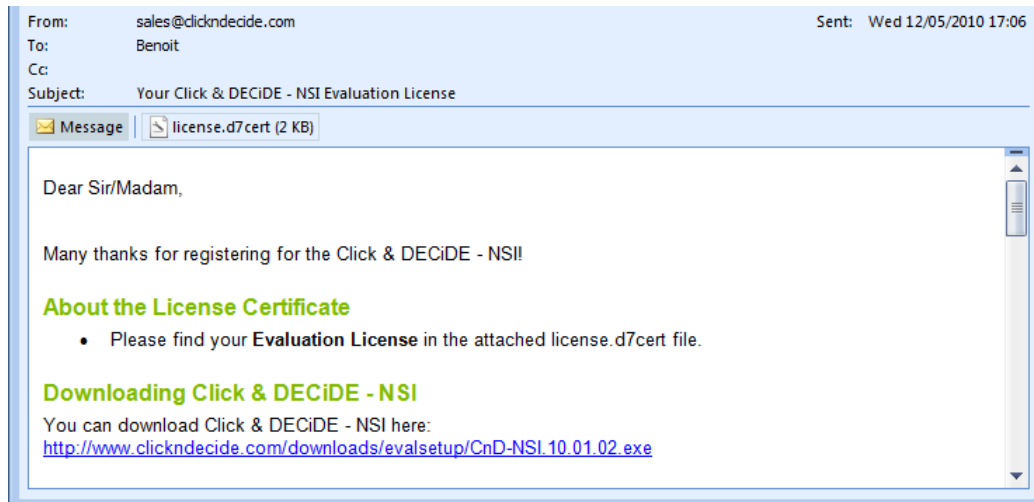
### 3.3. Download and extract the Click & DECiDE - NSI setup

1. Check that you have downloaded the latest version of Click & DECiDE NSI. If you are not sure, please download the latest release of Click & DECiDE from our web site:

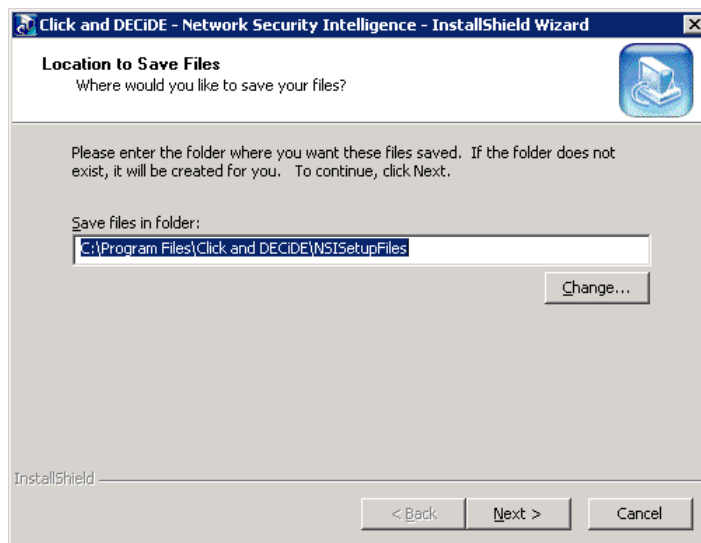
[http://license.clickndecide.com/downloads/cndnsi\\_request.aspx](http://license.clickndecide.com/downloads/cndnsi_request.aspx)



2. Download from the received email link, the latest release of Click&DECiDE.



3. Save the license file on the disk.
4. Choose where you want to extract the files required for the installation.



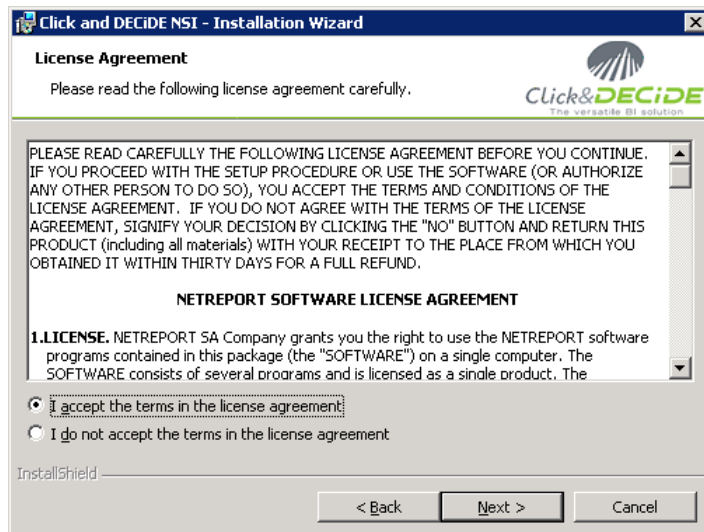
5. Click **Next**.
6. Wait for the extraction to complete. The **Click and DECiDE - NSI Installation Wizard** will launch.

## 3.4. The Click and DECiDE - NSI Installation Wizard

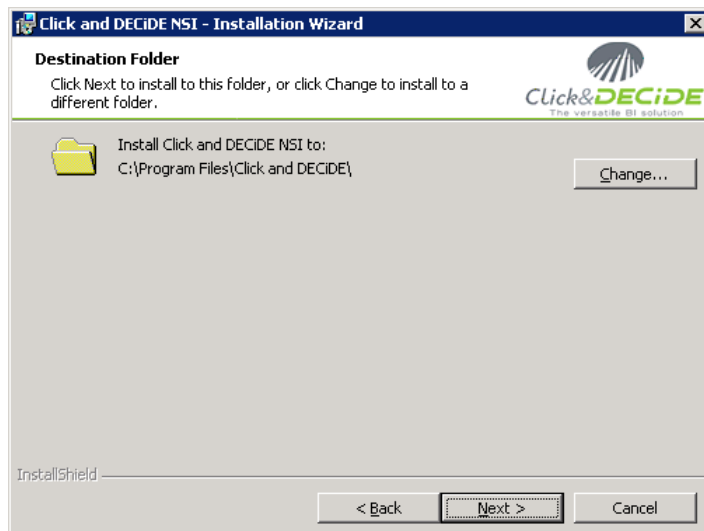
1. If you have any prerequisites, click **Install** to install them.
2. On the **Welcome to Installshield Wizard for Click and DECiDE - NSI** dialog, click **Next**.



3. On the **License Agreement** dialog, read the license agreement and select **I accept the terms in the license agreement** to continue.



4. Click **Next**.
5. On the **Destination Folder** dialog, select a folder on a partition with enough hard disk space. See recommendations:  
[http://www.clickndecide.com/downloads/WebDoc/Support/ClicknDECiDE\\_NSI\\_Database\\_Archive\\_Disk\\_Size.zip](http://www.clickndecide.com/downloads/WebDoc/Support/ClicknDECiDE_NSI_Database_Archive_Disk_Size.zip)

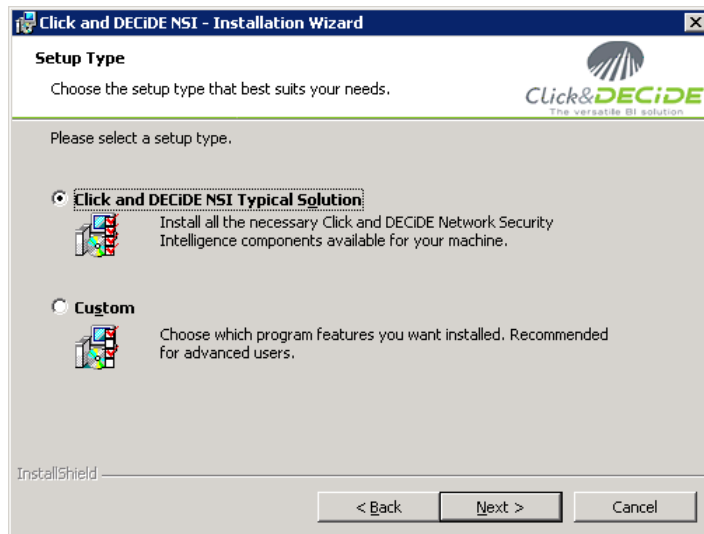


6. Click **Next**.

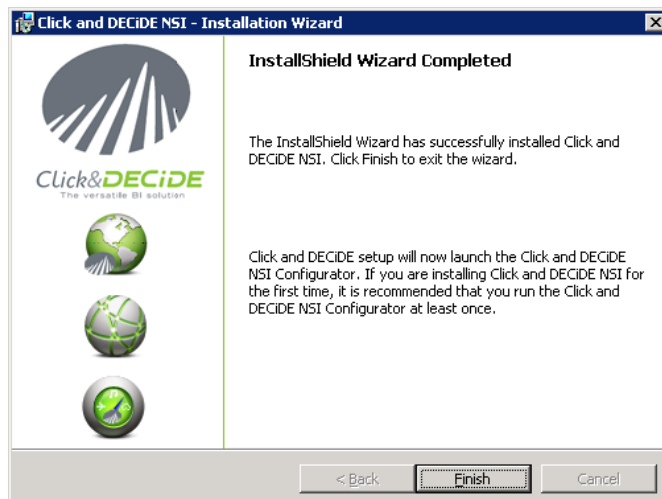




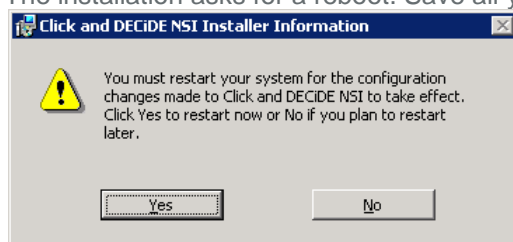
7. On the **Setup Type** dialog, choose **Click and DECiDE NSI Typical Solution**.



8. Click **Next**.
9. Click **Install**.
10. Wait for the installation to complete.
11. On the **InstallShield Wizard Completed** dialog, Click **Finish**.



12. The installation asks for a reboot. Save all your documents and close all your application and click **Yes**.



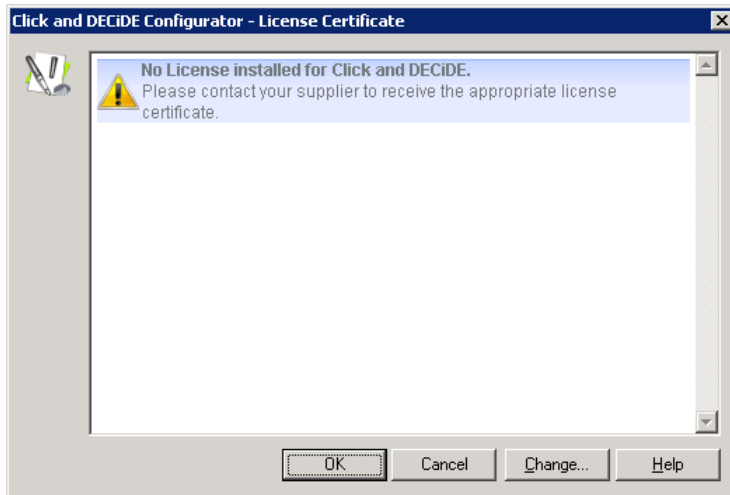
Congratulation, the installation is now finished!



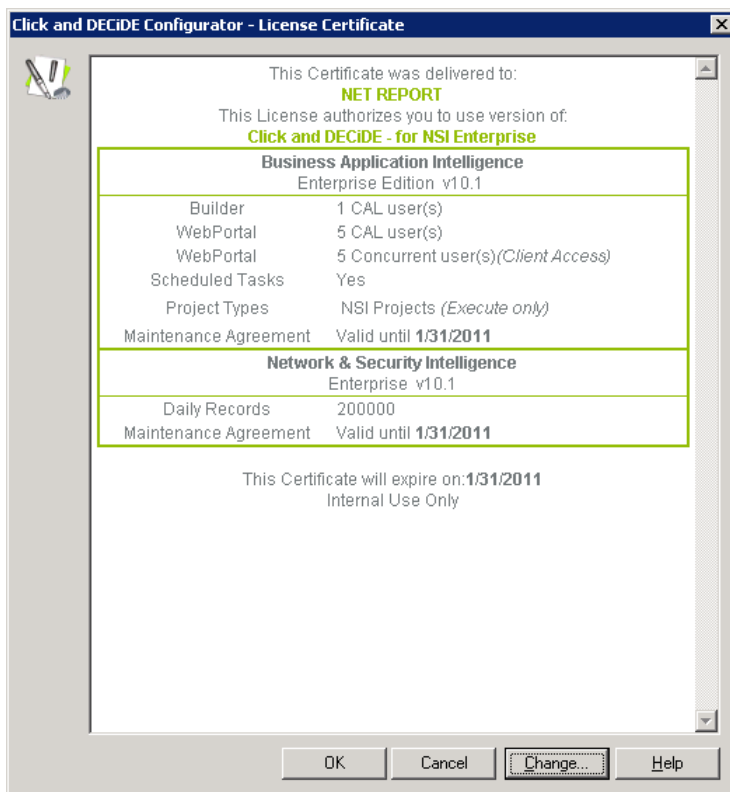
## 4. Configuration of Click&DECiDE NSI Demo device

### 4.1. Enter your License Certificate

1. After rebooting your machine, the **Log Source Configuration** launches and asks for a License Certificate.

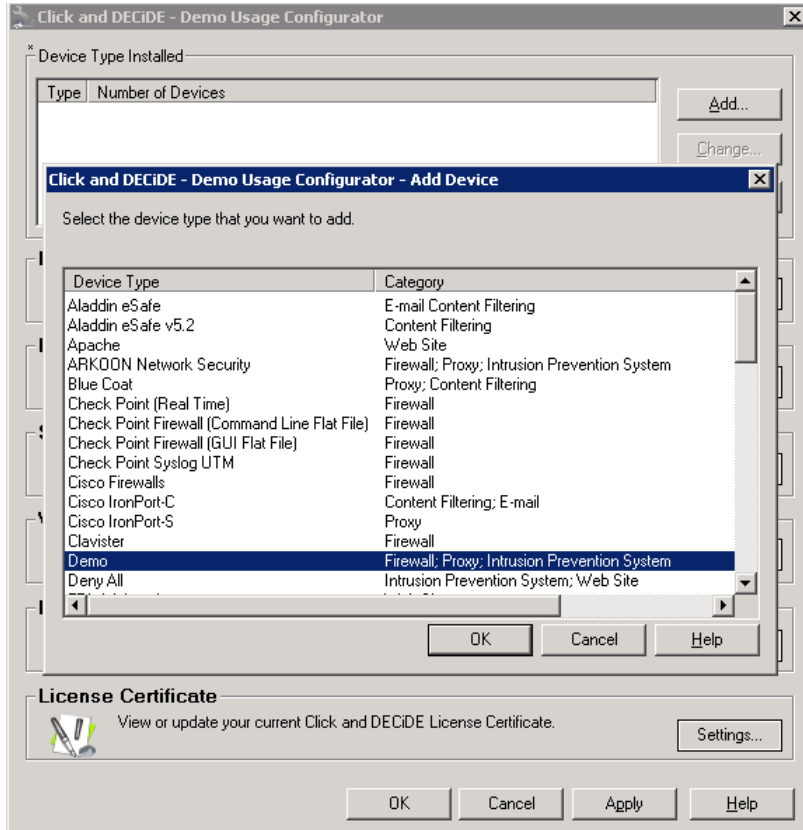


2. Click **Change...**
3. Select the License Certificate we sent you for Click & DECiDE - NSI 10.1.2.





4. Click **OK**.
5. Select the **Demo** device



6. Click **Ok** and **OK** again, than **Finish**.
7. Click **Settings...** in the **Network** section.
8. Configure the section by adding :
  - a. A single DMZ web server at IP 194.206.126.204
  - b. A public DMZ network 192.168.2.0 / 255.255.255.0
  - c. If you are connected to internet, and only if you wish to view the IP resolution, you may Enable the Global Reverse DNS resolution



The image shows two overlapping dialog boxes from the Click and DECiDE software. The top dialog, titled "Click and DECiDE - Demo Usage Configurator - Network Change", has fields for "Type" (set to SINGLE), "From" (194.206.126.204), "Type" (set to DMZ), and "Name" (WebServer). It includes OK, Cancel, and Help buttons. The bottom dialog, titled "Click and DECiDE - Demo Usage Configurator - Network Connection Settings", features a table with network rules, a checkbox for "Enable Global Reverse DNS", a warning message, and OK, Cancel, and Help buttons.

From	To/Mask	Name
194.206.126.204		DMZ WebServer
192.168.2.0	255.255.255.0	DMZ Public
192.168.0.0	192.168.255.255	Internal 192
10.0.0.0	10.255.255.255	Internal 10
172.16.0.0	172.31.255.255	Internal 172
127.0.0.1		Local host
255.255.255.255		Broadcast
0.0.0.0	255.255.255.254	External

☒ Enable Global Reverse DNS

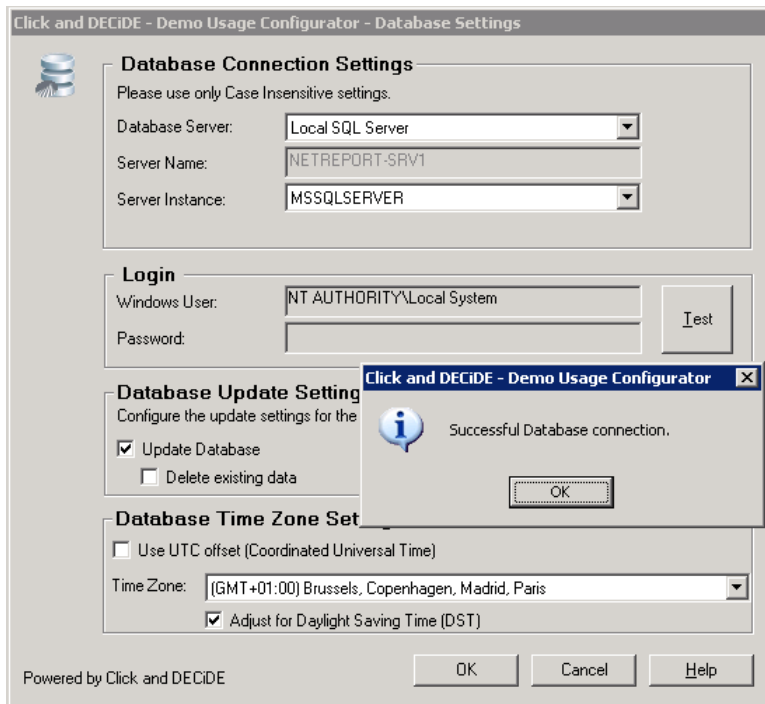
Warning: selecting to Enable Global Reverse DNS may cause a drop in the performance of the Filter Engine and an overload of your network traffic.

9. Click **OK**.
10. Click **Settings...** in the **Database** section.
11. Select your database and test your database connection.

**Note:** Click and DECiDE - NSI uses Windows Authentication to connect to the database. For a remote database connection, additional steps are required. Please refer to the Knowledge Base Article: [How to Connect to Remote SQL Server at: http://www.clickndecide.com/downloads/WebDoc/CnDRnD/KBA/KBA200\\_How\\_to\\_Connect\\_to\\_Remote\\_SQL\\_Server.pdf](http://www.clickndecide.com/downloads/WebDoc/CnDRnD/KBA/KBA200_How_to_Connect_to_Remote_SQL_Server.pdf)



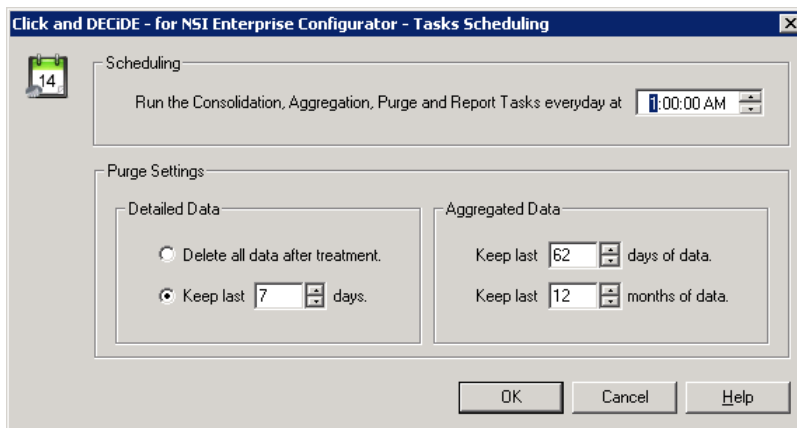
12. Note that the Log Source Configuration tool will perform an update of your database.



13. Click **OK**.

14. Click **Settings...** in the **Scheduled Tasks** section.

15. Configure the purge parameters and the start time of the Click & DECiDE - NSI scheduled task.



16. Click **OK**.

17. Click **Settings...** in the **Web Portal** section.

18. Select **Click and DECiDE Authentication**.



19. Enter your SMTP server as well as the email address for mail alerts.

Click and DECIDE - for NSI Enterprise Configurator - Web Portal Settings

Web Portal Authentication Mode

☐ Windows Authentication

☒ Click and DECIDE Authentication

Mail Server (SMTP)

smtp.company.com Test

Mail Action Settings

Enter the e-mail addresses to use to send Click and DECIDE alerts.

From: nsi@company.com

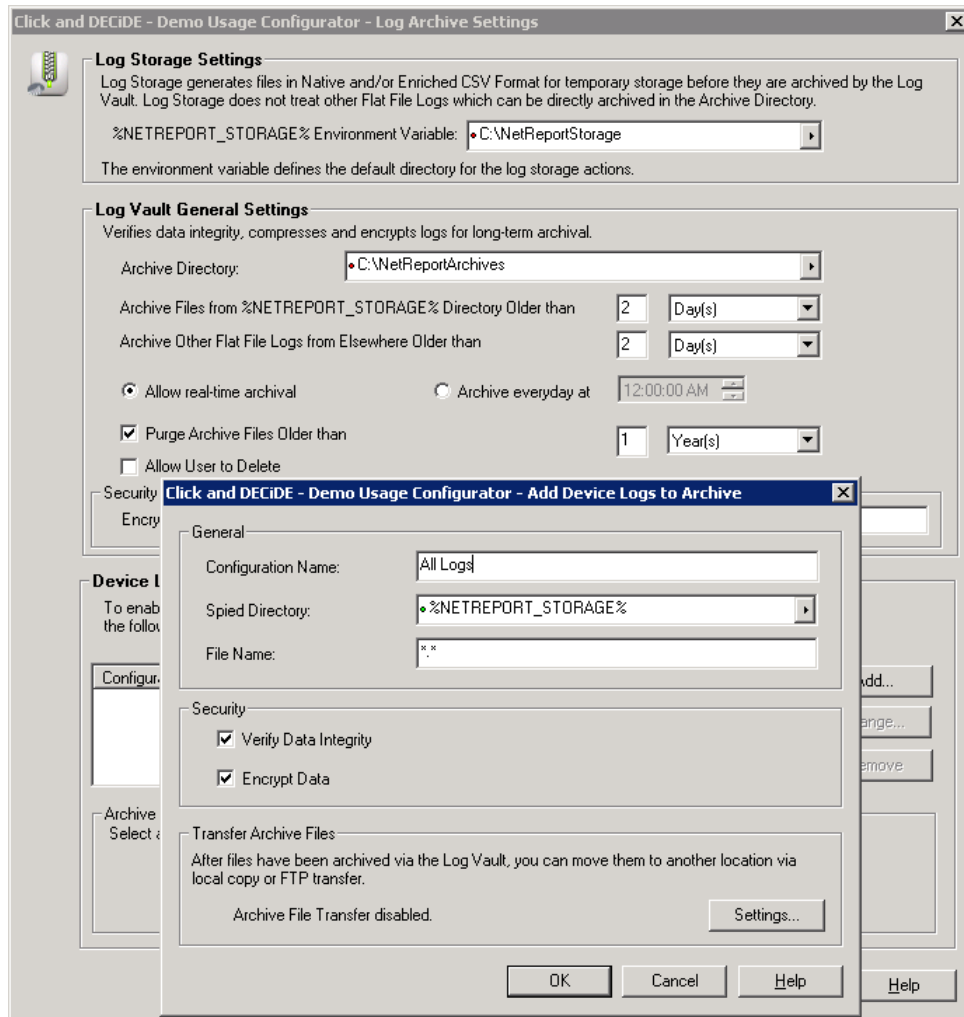
To: admin@company.com

OK Cancel Help

20. Click **OK**.

21. Click **Settings...** in the **Log Archive** section.

22. Configure your Log Archive settings. A simple “All Logs” configuration can be set-up as shown:



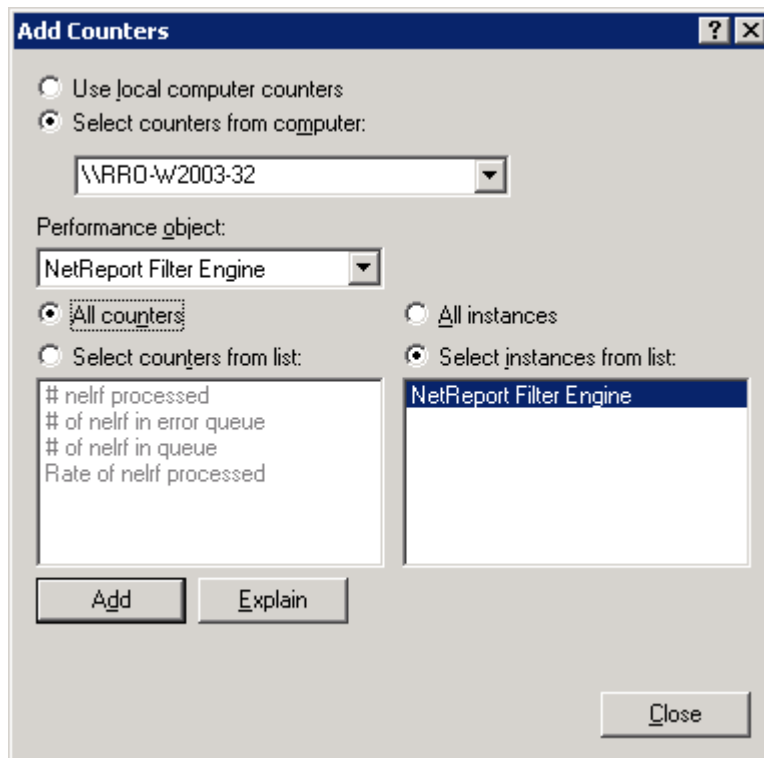
23. Click **OK**.
24. Click **OK** to apply your configuration.
25. Confirm your choice and wait for the **Log Source Configuration** tool to complete the process.
26. Close the **Log Source Configuration**.



## 5. Run the first Demo test logs

### 5.1. View Performance counter

1. Start the log treatment.
2. Open the Performance Counters: Start>Administrative Tools>Performance.
3. Click the + in the toolbar.
4. Select the **NetReport Filter Engine** Performance object and select **All counters**.

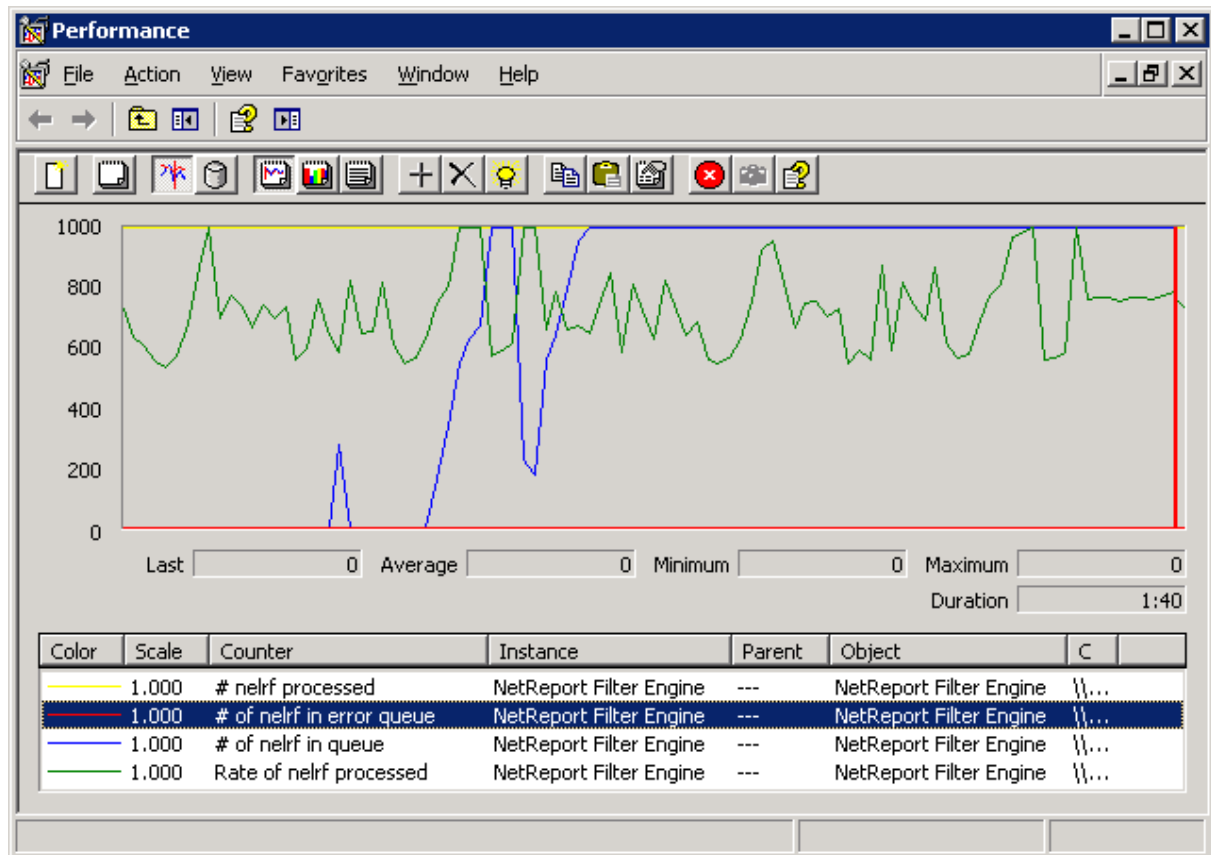


5. Click **Add**.
6. Click **Close**.
7. Save the performance Counter on your Desktop under the name **ClicknDECiDE Perfmon**





- Check that you don't have any nelrf (Click And DECiDE events) in the error queue.



**Note:** the engine queues are stored in the folder `C:\Program Files\Click and DECiDE\Error agent Storage`. You can modify the destination of these files by changing the registry value:  
**HKEY\_LOCAL\_MACHINE\SOFTWARE\NetReport\MCAgents\Error\StoragePath.**  
 You have to restart the Click & DECiDE Filter Engine service after any change

Note that the “rate of nelrf processed” varies from an average of 100 to more than 5.000 depending on hardware (processors, numbers of cores, memory and HD speed) and also the software (windows 7, 2003, 2008, architecture 32b or 64b, MS SQL express, standard, enterprise... and also 2005 – 2008...)



## 5.2. Log Acquisition

1. Open an disk explorer to the directory  
**D:\Program Files\Click and DECiDE\NSI\Logs\Engine\Flatfile\Demo**
2. Copy and paste the 3 files into new files name

Name	Date modified	Type	Size
1 - ips.csv	20/05/2009 14:27	CSV File	31 KB
2 - firewall.csv	20/05/2009 14:27	CSV File	820 KB
3 - proxy.csv	20/05/2009 14:27	CSV File	3,935 KB
Copy of 1 - ips.csv	20/05/2009 14:27	CSV File	31 KB
Copy of 2 - firewall.csv	20/05/2009 14:27	CSV File	820 KB
Copy of 3 - proxy.csv	20/05/2009 14:27	CSV File	3,935 KB

3. Check with the Performance Counter that log are processed  
You will get information there in the 10 second following the copy of the files.

## 5.3. Control the database insertion

1. Open **Web Portal: Start>All Programs>Click and DECiDE>Web Portal**.
2. If not in windows authentication mode, login as a member of **NetReport Admin group**, in Click&DECiDE authentication mode.

*The default ID/PWD is admin/admin*

3. Navigate to **NSI Utilities/Database Status**.
4. Open the project for the category of the log you have acquired. For example: **Firewall Statistics Utilities**.

	Size	Modification	Creation
1 - Selected Record Details	0	1/21/2010 5:14:15 PM	9/2/2004 10:43:08 AM
2 - Number of Records in the Firewall Tables	0	1/21/2010 5:20:02 PM	9/2/2004 10:43:08 AM
3 - Address Definition Management	0	1/21/2010 4:07:29 PM	9/2/2004 10:43:08 AM
4 - Firewall Aggregation Process Status	0	4/28/2010 4:57:31 PM	9/2/2004 10:43:08 AM

5. Open the report **2 - Number of Records in the Firewall Tables**.



6. Enter the time interval corresponding to the date of your logs. For example, if you are parsing logs from 10 days ago, enter 10 in the first text box.

Click and DECIDE Web Portal - Menus - Windows Internet Explorer

http://localhost/dvweb/Menu.aspx

Click and DECIDE Web Portal - Menus

Web Server Configuration  
Menus

- NSI Reports and Analysis
- NSI Utilities
  - Database Status
  - Firewall Statistics Utilities
  - Click and DECIDE Audit
  - Proxy Statistics Utilities
- NSI Alert Management
- Scheduled Tasks & Tasks
- Web Part Configuration
- Content Builder
- Web Server Administration

Parameters Result Both

2 - Number of Records in the Firewall Tables

☒ From: Today - X days 10

☒ To: Today - Y days 0

☒ Start time: 5/6/2009 12:00:00 AM

☒ Stop time: 5/6/2010 11:59:59 PM

☐ Firewall? (Ignore for all): IGNORE

Output Format: PDF Run

7. Click **Run**.

Click and DECIDE Web Portal - Menus - Windows Internet Explorer

http://localhost/dvweb/Menu.aspx

Click and DECIDE Web Portal - Menus

Web Server Configuration  
Menus

- NSI Reports and Analysis
- NSI Utilities
  - Database Status
  - Firewall Statistics Utilities
  - Click and DECIDE Audit
  - Proxy Statistics Utilities
- NSI Alert Management
- Scheduled Tasks & Tasks
- Web Part Configuration
- Content Builder
- Web Server Administration

Parameters Result Both

2 - Number of Records in the Firewall Tables

Number of records in the Firewall tables

This report presents the total number of records existing in the different tables from the oldest to the most recent date and time with the aggregation status associated from within the Wednesday May 6, 2009 at 00:00:00 AM until the Thursday May 6, 2010 at 11:59:59 PM

Raw Data					
fw_rawdata	fw_rawdata_dup	fw_details	From	To	Status
1 Firewall(s)	32,858 row(s)	0 row(s)	From: 5/17/2010 0:00:01 AM	To: 5/17/2010 0:00:01 AM	Not aggregated
0 Firewall(s)	0 row(s)	0 row(s)	From:	To:	In Process
0 Firewall(s)	0 row(s)	0 row(s)	From:	To:	Aggregated

Aggregated Data					
fw_hourly_main	fw_daily_main	fw_monthly_main	From	To	Period
0 Firewall(s)	0 row(s)	0 row(s)	From:	To:	0 Hour(s)
0 Firewall(s)	0 row(s)	0 row(s)	From:	To:	0 Day(s)
0 Firewall(s)	0 row(s)	0 row(s)	From:	To:	0 Month(s)

Dimension Data					
fw_device	fw_ip	fw_service	fw_user	fw_action	fw_device
1 row(s)	9 row(s)	65,836 row(s)	1 row(s)	3 row(s)	276 row(s)

Report printed on Thursday May 6, 2010 at 10:49

Dashboard created with © Click&DECIDE

Page 1/1

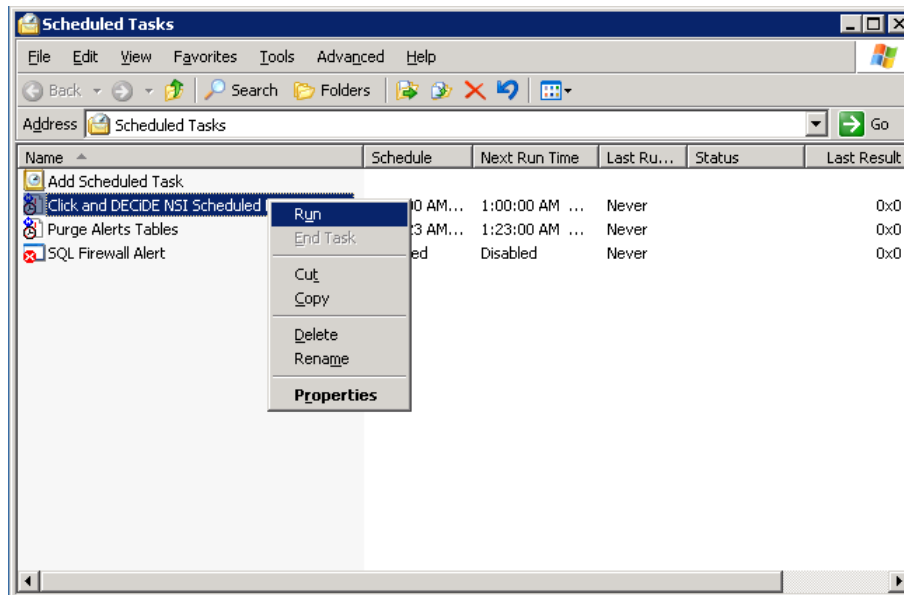
8. Check that logs are inserted into the rawdata table.



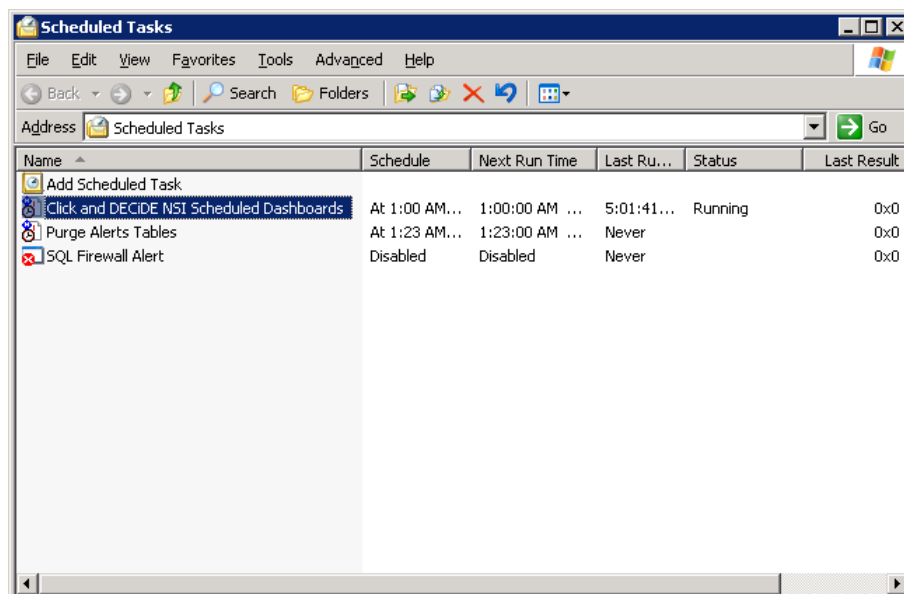
## 6. Report Generation

Reports are generated automatically at 1 AM. To speed up the process, we will force an immediate task that will generate the Dashboards.

1. Open the **Scheduled Tasks** panel: **Start>Control Panel>Scheduled Tasks**.
2. Right Click on **Click and DECiDE Scheduled Dashboards** and select **Run**.



3. Wait for the task to complete (it may take some time depending on the volume of your logs).



4. Return to **Web Portal** (see Chapter 5.3).
5. Navigate to **NSI Reports and Analysis/Published Report**.



6. Select the category of the log you have acquired. For example: **Firewall**.

Firewall	Size	Modification	Creation
Firewall Daily_100505	164,630	5/6/2010 5:02:25 PM	5/6/2010 5:02:23 PM

7. Check that a report has been generated. If you have inserted yesterday's logs, the reports should contain some data.

**Note: the DEMO device is always generating logs at YESTERDAY.**

8. Look at other reports generated with the demo devices: IDS/IPS report and Proxy Reports.

## 6.1. Generate a Dynamic Report

Generate a Dynamic Report by user on yesterday

1. Open the **Web Portal** (see Chapter 5.3).
2. Navigate to **NSI Reports** → **Dynamic Reports** → **Report Book for the Proxy Daily Reports**
3. **Select the Yesterday**
4. **Select the Report by User?**



## 5. Run the report in PDF

Report Book for the Proxy Daily Reports

☒ Select the Period or Other for a Date: Today  
Yesterday  
Other

☒ Select the Date (if Other selected): 6/2/2010

☐ Proxy? (Ignore for all): IGNORE

☐ IP Source? (Ignore for all): IGNORE

☐ IP Source beginning with? (enter the first characters or full value): IGNORE

☐ Destination? (Ignore for all): IGNORE

☒ Anonymous User? No

☐ User? (Ignore for all): IGNORE

☐ User Group beginning with? (enter the first characters or full name): IGNORE

☒ Report by IP Address or by User? IP Address  
User

☒ Top N Visited Domain? 30

☒ Top N Visited Domain by User or IP Address? 5

☒ Top N User or IP Address by Visited Domain? 5

☒ Top N Users? 30

☒ Top N Status? 10

☒ Top N Search Engine? 10

☒ Top N Keywords? 10

☒ Top N Countries? 10

☒ Top N Operating Systems? 10

☒ Top N Browsers? 10

☒ Top N Visited Categories? 10

☒ Top N User or IP Address by Category? 5

☒ Top N Category by User or IP Address? 5

Output Format: ☒ PDF ☐ HTML Run

## 7. Report analysis

### 7.1. Firewall report analysis

Find in the report:

- The unwanted accepted service (a)?
- The targeted Network Area of the unwanted accepted service (b)?
- At what time was the peak of block traffic (c)?
- What is the most used rule (d)?
- What % of the traffic in KB the top 1 Accepted Internal User is using (e)?
- Is this number [e] normal (f)?
- A non-resolved IP spend 37:44 minutes getting inside your network. Where it came from (g)?
- An incoming IP was blocked more than 30% of total blocks hit. What is the organization name we need to contact in case of legal action (h)?
- A port scan was done. From witch IP? How many hit? How many distinct services (i)?

### 7.2. IPS report analysis

Find in the report:

- What is the top attack detected (j)?
- Was it an incoming- outgoing or internal attack (k)?
- Was it blocked (l)?
- At what time did the only inbound blocked attack occurs (m)?
- What was it (n)?

### 7.3. Proxy report analysis

Find in the report:

- His the Proxy Filtered Traffic - Hourly Activity normal (o)?
- To witch user belongs the PC that stay ON all night (p)?
- Percentage of the most visited domain (q)?
- Most active Internet user and % of the total hit (r)?
- Is it a normal % (s)?
- Who are the users that are using the most the internet (t)?
- Are they professional or personal web access (u)?

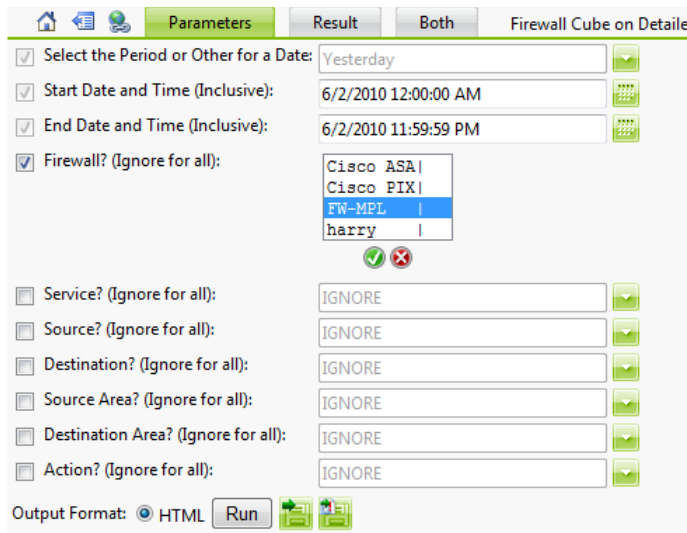
## 8. Investigation

With our Cube investigation tool, you can manipulate data to solve problems, find answers to direct questions, and discover abnormal behavior.

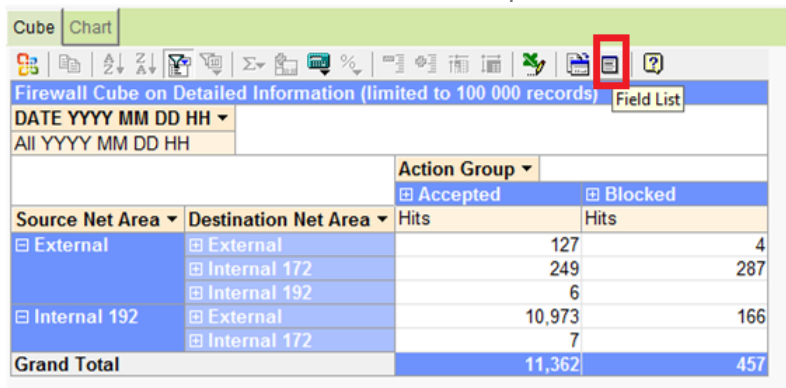
### 8.1. Firewall investigation

Generate a Dynamic Cube by user on yesterday

1. Open the **Web Portal** (see Chapter 5.3).
2. Navigate to **NSI Reports → Forensic Analysis → Firewall Cubes → Firewall Cube on Detailed Information**  
you can either select Daily cubes to have several days or Monthly Cube to manipulate a full month of data.
3. Select the firewall you want (or Ignore for all), and do the same for all other filters






4. Run the Cube.
5. Use the Field List Button to show available pivot table dimension to manipulate the data



DATE YYYY MM DD HH ▾		Action Group ▾	
All YYYY MM DD HH		Accepted	Blocked
Source Net Area ▾	Destination Net Area ▾	Hits	Hits
External	External	127	4
	Internal 172	249	287
	Internal 192	6	
Internal 192	External	10,973	166
	Internal 172	7	
<b>Grand Total</b>		<b>11,362</b>	<b>457</b>





6. With the manipulation of sort  icon, top x  icon, drag and drop of dimension , try to view the following :

- a. Top 25 services by top 10 Rules and Action Group

Firewall Cube on Detailed Information (limited to 100 000 records)							
DATE YYYY MM DD HH							
All YYYY MM DD HH							
Rule Action Group							
0 1 2 3 4 Grand Total							
Accepted Blocked Accepted Accepted Accepted Blocked							
Service	Hits	Hits	Hits	Hits	Hits	Hits	Hits
80		4	9,005	100			9,109
53			1,273	25			1,298
0	24	419	563				1,006
25			51		244		295
443	1		65	2			68
23		6					6
137			5				5

Check also the graphic view.

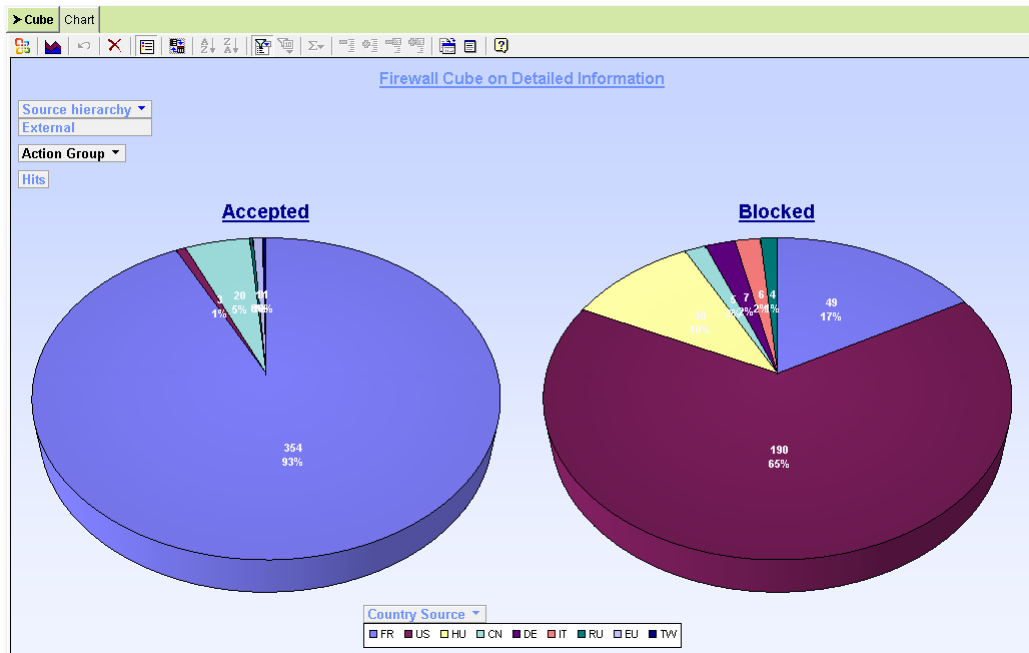
- b. Identify the Ports scan user and check the hour of the scan :

Firewall Cube on Detailed Information (limited to 100 000 records)							
Source hierarchy							
62.210.136.135							
Action Group Rule							
Accepted Blocked Grand Total							
1 4							
Country Source	Service	DATE	Hits	Hits	Hits	Hits	Hits
FR	100	19/01/2010 01:49:00			1		1
	101	19/01/2010 01:49:00			1		1
	102	19/01/2010 01:49:00			1		1

- c. Draw a graph with the top 10 country entering the firewall.  
Separate the graph by status

Cube Chart			
Firewall Cube on Detailed Information (limited to 100 000 records)			
Source hierarchy			
External			
Action Group			
Accepted Blocked Grand Total			
Country Source	Hits	Hits	Hits
FR	354	49	403
US	3	190	193
HU		30	30
CN	20	5	25
DE		7	7
IT		6	6
RU	1	4	5
EU	3		3
TW	1		1
Grand Total	382	291	673

Multiple Graph View



## 8.2. IDS/IPS investigation

Generate a Dynamic Cube by IP on yesterday

1. Open the **Web Portal** (see Chapter 5.3).
2. Navigate to **NSI Reports → Forensic Analysis → IPS Cubes → IPS Cube on Detailed Information** you can either select Daily cubes to have several days or Monthly Cube to manipulate a full month of data.
3. Select the IPS you want (or Ignore for all), and do the same for all other filters

The screenshot shows the 'Parameters' tab of the 'IPS Cube on Detailed Information (limited to 100 000 records)' configuration window. The 'Result' tab is also visible.

- ☒ Select the Period or Other for a Date: Yesterday
- ☒ Start Date and Time (Inclusive): 6/2/2010 12:00:00 AM
- ☒ End Date and Time (Inclusive): 6/2/2010 11:59:59 PM
- ☒ IPS? (Ignore for all): harry (selected), IPS MPL (available)
- ☐ Source? (Ignore for all): IGNORE
- ☐ Destination? (Ignore for all): IGNORE
- Output Format: ☒ HTML
- Buttons: Run, [Export], [Refresh]

4. Run the Cube.
5. Use the Field List Button to show available pivot table dimension to manipulate the data



IPS Cube on Detailed Information (limited to 100 000 records)

Cube Chart

IPS Cube on Detailed Information (limited to 100 000 records)

Date YYYY MM DD HH Date Detailed

All YYYY MM DD HH All Detailed




Attack Category	Attack ID	Action Group Action	
		Blocked	Accepted
netbios		20	143
p2p			48
dns_decoder			25
icmp		17	4
im			15
anomaly			1
Denial of Service		1	
web-misc			1

PivotTable Field List

Drag items to the PivotTable list

- IPS Detailed
- Totals
- Count
- Action hierarchy
- Attack hierarchy
- Country Destination
- Country Source
- Date Detailed
- Date YYYY MM DD HH
- Destination hierarchy
- IPS Product
- Origin
- Protocol
- Service
- Severity
- Source Port
- Source hierarchy

Add to Row Area

6. With the manipulation of sort  icon, top x  icon, drag and drop of dimension , try to view the following :
- a. Select the external source, dangerous Attack Category (Denial of Service, netbios, web-miscTop) and see who's internal target was and at what time

IPS Cube on Detailed Information (limited to 100 000 records)

Drop Filter Fields Here

Attack Category	Attack ID	Attack Name	IP Source	IP Destination	Date	Action Group Action	
						Blocked	Accepted
Denial of Service	FGT101974314	Microsoft Works Spreadsheet Memory Corruption	66.111.102.220	192.168.0.3	19/01/2010 19:14:00	1	
netbios	FGT102039558	NT NULL Session	66.11.102.220	192.168.0.52	19/01/2010 15:13:00		1
web-misc	FGT103390551	Prozilla Location BufferOverflow	216.52.17.116	192.168.0.52	19/01/2010 15:00:00		1



- b. Check if the target did an attack after the potential successful attack

**IPS Cube on Detailed Information**  
Date YYYY MM DD HH

2010  
January  
19  
0  
1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23

OK Cancel

Date selection: and field selection:

Cube Chart

IPS Cube on Detailed Information (limited to 100 000 records)  
Date YYYY MM DD HH  
(Multiple Items)

IP Source	Attack Category	Attack ID	Attack Name	IP Destination	Date	Action Group		Action	
						Blocked	Count	Accepted	Count
192.168.0.52	netbios	FGT102039613	SMB.DCERPC.Registry.OpenHkLM.139	192.168.0.201	19/01/2010 15:09:00				2
					19/01/2010 15:16:00				2
					19/01/2010 15:21:00				2
					19/01/2010 15:33:00				2
					19/01/2010 15:41:00				2
					19/01/2010 16:34:00				1
					19/01/2010 16:35:00				1
					19/01/2010 16:43:00				2
					19/01/2010 16:59:00				2
					19/01/2010 17:23:00				1
					19/01/2010 17:24:00				1
					19/01/2010 17:28:00				2
					19/01/2010 17:48:00				2
					19/01/2010 18:12:00				2
					19/01/2010 18:37:00				2
					19/01/2010 19:01:00				2
					19/01/2010 19:26:00				2
					19/01/2010 19:50:00				2
					19/01/2010 20:15:00				2
					19/01/2010 20:52:00				2
					19/01/2010 21:28:00				1
					19/01/2010 21:29:00				1
					19/01/2010 21:53:00				2
					19/01/2010 22:17:00				2
					19/01/2010 22:42:00				2
192.168.0.59	icmp	FGT102039618	SMB.DCERPC.SamrEnumerateAliasesInDomain.139	192.168.0.204	19/01/2010 18:05:00		1		
					19/01/2010 18:02:00		1		
					19/01/2010 18:07:00		1		
					19/01/2010 19:06:00		1		
192.168.0.87	icmp				19/01/2010 16:05:00		1		
					19/01/2010 16:06:00		1		
Grand Total							16	22	52

There are a lot of internal attacks after the first external one!



## 8.3. Proxy investigation

Generate a Dynamic Cube by user on yesterday

1. Open the **Web Portal** (see Chapter 5.3).
2. Navigate to **NSI Reports → Forensic Analysis → Proxy Cubes → Proxy Cube on Detailed Information by User**  
you can either select Daily cubes to have several days or Monthly Cube to manipulate a full month of data.
3. Select the proxy you want (or Ignore for all), and do the same for all other filters

Parameters Result Both Proxy Cube on Detailed Information by User (Limited to 100 000 records)

☒ Select the Period or Other for a Date: Yesterday

☒ Start Date and Time (Inclusive): 6/2/2010 12:00:00 AM

☒ End Date and Time (Inclusive): 6/2/2010 11:59:59 PM

☒ Proxy? (Ignore for all): FW-MPL, IronPort-S, SG-HTTP-Service

☐ Source? (Ignore for all): IGNORE

☐ User? (Ignore for all): George, Hector, Jairo, Jo, John, Joy, ken

☐ Destination? (Ignore for all): IGNORE

☐ Result Group? (Ignore for all): IGNORE

Output Format: ☒ HTML Run

4. Run the Cube.
5. Use the Field List Button to show available pivot table dimension to manipulate the data

Proxy Cube on Detailed Information by User (Limited to 100 000 records)

Cube by User Chart by User

Proxy Cube on Detailed Information (Limited to 100 000 records)




DATE YYYY MM DD HH DATE Detailed

All YYYY MM DD HH All Detailed

Result Group Result Code

User	Hits	Bytes	Elapsed Time	Accepted passthrough	Error blocked	Bytes	Elapsed Time
Jo	8 361	142 137	58 527	206	0	0	0
Chris	1 747	29 699	12 229	34	0	0	0
Xavier	1 130	19 210	7 910	1	0	0	0
Luc	932	15 844	6 524	28	0	0	0
Alan	656	11 152	4 592	13	0	0	0
George	643	10 931	4 501	70	0	0	0
Nancy	535	9 095	3 745	16	0	0	0
Hector	25	425	175				
Victoria	17	289	119				
Pam	14	238	98				
Victor	6	102	42				
Zoe	1	17	7				
Joy				44	0	0	0
Grand Total	18 371	312 307	128 597	686	0	0	0



6. With the manipulation of sort  icon, top x  icon, drag and drop of dimension , try to view the following :

- Check where are surfing the top 2 users in time
- Check if it is during work hours!

Full result:

Proxy Cube on Detailed Information by User (Limited to 100 000 records)												
Cube by User		Chart by User										
<div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div>&lt;</div>												

## 9. Add you own devices

Using the same function that you use to add the Demo device (12 point 5), you can now add your own equipments.

Example with a Cisco ASA in syslog:

- Launch **Click&DECiDE Configurator**
- In **Device Type**, select **Add**
- In the list, select the device you want to collect the log from. For example here **Cisco Firewall** for all type of Cisco's firewalling devices
- In the **Log File Acquisition Settings** window, select **Log in Real-Time with Syslog Protocol**. Enter the Syslog IP address of your device.
- Select **OK**
- In the **Log Treatment** windows select the action you want to be done on this device:

- ☒ **Generate Daily and Monthly Report**  
to generate, at 1 AM the previous day report
  - ☒ **Archive logs in enriched CSV format**  
to prepare a contextual copy of the log, that will be securely archived
  - ☒ **Archive logs in Native format**  
to prepare the legal and regulatory collection of the log, that will be securely archived
7. Click on **Finish**, than **Apply**. The new configuration is applied.
  8. Go to your device, and configure the log to be sent in syslog to the Click&DECiDE server IP.
  9. Check with the Perform monitor (see Chapter 5.1) that you received the event and that they are correctly processed.
  10. The next day, open the **Web Portal** (see Chapter 5.3) and look at your reports.

## 10. Exercise solutions

- a. Port 50010
- b. Internal 172
- c. 10 AM
- d. 1
- e. 39.57%
- f. It really depends on your architecture
- g. Click on the [58.53.60.225](#) link on page 10 and you get the correct WHOIS information whatever NIC is used. Result is "CHINANET Hubei province network"
- h. AT&T Global Network Services, LLC
- i. 62.210.136.135, 29 hit , 29 distinct services
- j. SMB.DCERPC.Registry.OpenHKLM.139
- k. Internal
- l. Detected but not blocked
- m. 19:00 to 19:59
- n. Microsoft.Works.Spreadsheet.Memory.Corruption
- o. Yes, but there is traffic at midnight that may indicate automatic updates on PC's that stay switched ON all night
- p. Eric, Peter and Eva with almost 24 hours cumulated internet session during a day. (HP update live ticker! [isee.europe.hp.com](#) page 4-5-6)
- q. [www.google.com](#) with 9.77%
- r. Jo with 45.51% hits
- s. No. A single user should not be at almost 50% of the total number of hit in the proxy of any company.
- t. Chris with 2:50 hours and Jo with 2:09 hours of internet during the day (are they paid for that?)
- u. Jo is doing Business... but home Business! (selling his house) and Chris is reading news and media (is he working in PR ?)



## 11. Data and Users available in Click&DECiDE Soft Appliance

### 11.1. Data available in SQL database

- **Firewall:** a CISCO ASA 5505 Firewall data has been installed from January 2010 to December 2010.
- **ActivIdentity:** an ActivIdentity AAA database as been setup to provide data from January 2010 to December 2010.

You can use those data for long term tests and manipulation.

A full set of all standard product logs is available in  
C:\Program Files\Click and DECiDE\NSI\Logs\Engine\Flatfile

You can use them to test device reports.

All logs there are at the date of 17 January 2010.

### 11.2. Users available

Two users have been setup in Click&DECiDE Soft Appliance.

- **Administrator** with **cnd-nsi-10** password  
This user as full access to all logs
- **Demonstration** with **cnd-nsi-10** password  
This user as restricted access in cube only to the demo logs from DEMO device (FW-MPL)
- **BI** with **cnd-nsi-10** password  
This user as menu for Business Intelligence tool

#### 11.2.1. Administrator user screen access:

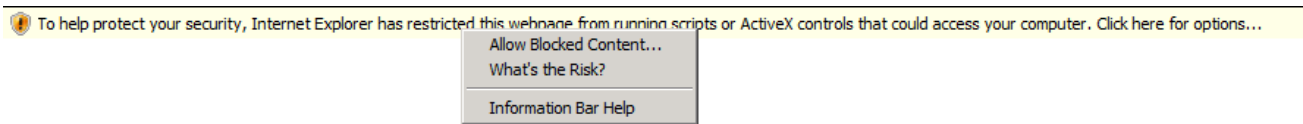
The screenshot shows the Click&DECiDE Web Portal interface. The browser window title is "Click and DECiDE Web Portal - Menus - Windows Internet Explorer". The address bar shows "http://localhost:dvweb/Default.aspx?NoInit=1". The interface includes a sidebar with navigation options like "Web Server Configuration", "Web Parts", "Yesterday Firewall Dashboard", "Yesterday IPS Dashboard", and "Yesterday Proxy Dashboard". The main content area displays three tables: "Alerts", "Daily Reports", and "Monthly Reports", each with columns for "Title", "Date", and a list of items.

Alerts	Daily Reports	Monthly Reports
Title	Title	Title
Alert on Many Rejection by Tad	Intrusion Prevention System Daily Dashboard	Proxy Monthly Dashboard
Alert on Many Rejection by Victoria	Proxy Daily Dashboard	Intrusion Prevention System Monthly Dashboard
Alert on Many Rejection by Zoe	Firewall Daily Dashboard	Firewall Monthly Dashboard
Alert on Hits on Accepted on firewall FW-MPL	Intrusion Prevention System Daily Dashboard	
Alert on Bytes on Service 25	Proxy Daily Dashboard	
Alert on Hits on Service 80	Firewall Daily Dashboard	
Alert on Hits on a IP 192.168.0.37		
Alert on Bytes on a IP 192.168.2.22		
Alert on Suspicious Port Scan 62.210.136.135		
Proxy Alert on Bytes on a IP 192.168.0.37		

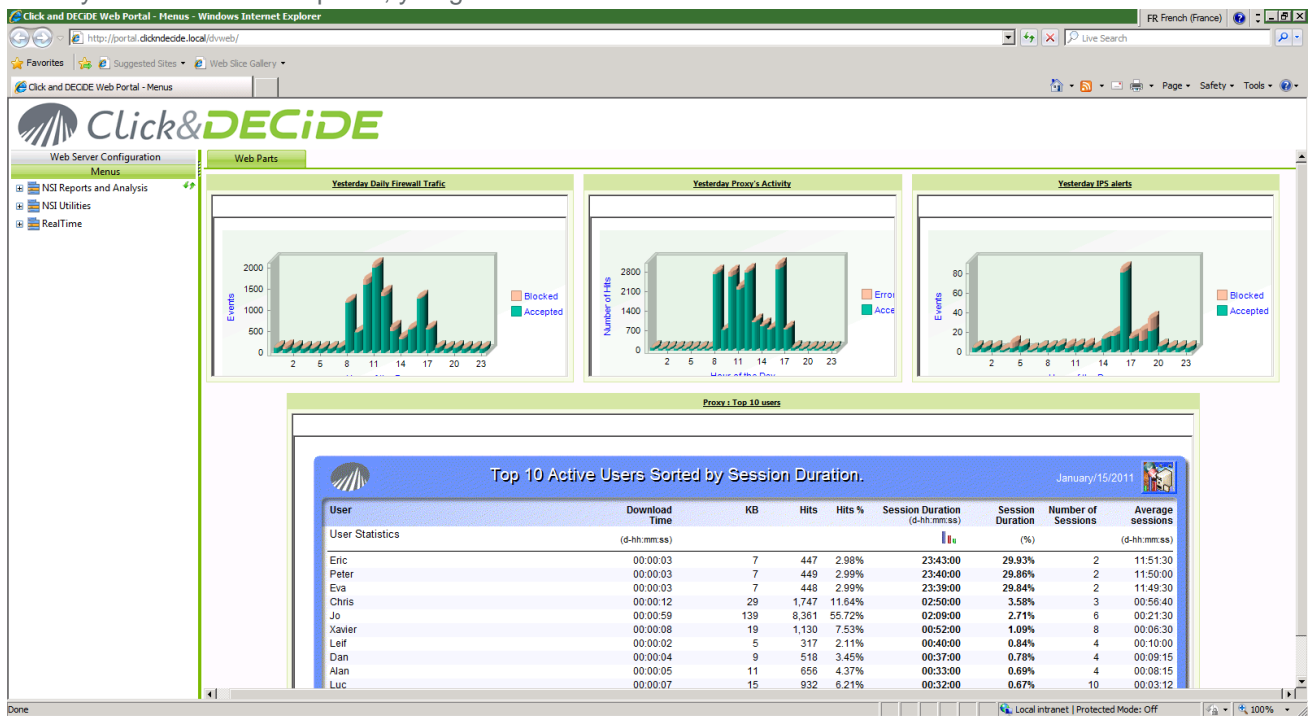


## 11.2.2. Demonstration user screen access:

When the user Demonstration is accessing his screen, the Click&DECiDE supervision screen is shown. You need to allow the access to make it work.



When you launch the web portal, you get the screen with Web Parts:



(note: if the graphic are not fully shown, please click on **Web Parts** tab for screen synchronization)

The data shown here are at the date of 15 January 2011.

If you run DEMO logs again, and wishes to update the graphics and the alarm, run the Schedule Tasks, has they should be programmed to run automatically at night in a production environment. Log in with Administrator to launch them:

1. Click and DECiDE NSI Scheduled Dashboards
2. Wait 10 minutes
3. Click and Decide Demo Alerts
4. Click and Decide Web Parts Update

