



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: <u>benoit.rostagni@clickndecide.com</u>



Table of Contents

1.	Sc	oft-Appliance installation	. 4
2.	Pr	re-installation check list	. 4
	2.1.	Hardware Environment	. 4
	2.2.	Software Environment	. 4
3.	Ins	stall 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.	Сс	onfiguration of Click&DECiDE NSI Demo device	10
	4.1.	Enter your License Certificate	10
5.	Ru	un 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.	Re	eport Generation	20
	6.1.	Generate a Dynamic Report	21
7.	Re	eport analysis	23
	7.1.	Firewall report analysis	23
	7.2.	IPS report analysis	23
	7.3.	Proxy report analysis	23
8.	Inv	vestigation	24
	8.1.	Firewall investigation	24
	8.2.	IDS/IPS investigation	26
	8.3.	Proxy investigation	29
9.	Ac	dd 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	I.2.1. Administrator user screen access:	32
	11	1.2.2. 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

Hardware Environment 2.1.

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) 0
- 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 0
- Framework .NET 3.5 (Minimum SP1) 0
 - 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 Wild Web Services
 - a. Applications Development Features
 - i. ASP.NET
 - ii. ASP
 - b. Security
 - i. Basic Authentication
 - ii. Windows Authentication
- 7. Click OK

Download and install the Framework .NET 3.5 SP1 3.2.

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 lastest release of Click & DECiDE from our web site: http://license.clickndecide.com/downloads/cndnsi request.aspx



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

From:	sales@clickndecide.com	Sent:	Wed 12/05/2010 17:06
To:	Benoit		
Cc			
Subject:	Your Click & DECiDE - NSI Evaluation License		
🖂 Message	S license.d7cert (2 KB)		
			-
Dear Sir/N	Aadam,		
Many that	aks for registering for the Click & DECiDE - NSI		
indity that			
About t	he License Certificate		
• P	lease find your Evaluation License in the attached license.d7cert file.		
Downlo	ading Click & DECiDE - NSI		
You can o	download Click & DECiDE - NSI here:		
http://www	v.clickndecide.com/downloads/evalsetup/CnD-NSI.10.01.02.exe		
			-

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

Click and DECiDE - Network Security Intelligence - InstallShield Wizard	×
Location to Save Files Where would you like to save your files?	
Please enter the folder where you want these files saved. If the folder does not exist, it will be created for you. To continue, click Next.	
Save files in folder:	
C:\Program Files\Click and DECiDE\NSISetupFiles	
<u>C</u> hange	
InstallShield	

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

The Click and DECiDE - NSI Installation Wizard 3.4.

- 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.





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



6. Click Next.



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



- Click Next. 8
- Click Install. 9
- 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. 🙀 Click and DECiDE NSI Installer Information X



Congratulation, the installation is now finished!



4. Configuration of Click&DECiDE NSI Demo device

Enter your License Certificate 4.1.

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.

Click and I	DECIDE Configurator - License Certificate X
<u>NU</u>	This Certificate was delivered to: NET REPORT This License authorizes you to use version of: Click and DECIDE - for NSI Enterprise
	Business Application Intelligence Enterprise Edition v10.1 Builder 1 CAL user(s) WebPortal 5 CAL user(s) WebPortal 5 Concurrent user(s)(Client Access) Scheduled Tasks Yes Project Types NSI Projects (Execute only) Maintenance Agreement Valid until 1/31/2011
	Network & Security Intelligence Enterprise v10.1 Daily Records 200000 Maintenance Agreement Valid until 1/31/2011
	This Certificate will expire on: 1/31/2011 Internal Use Only
	OK Cancel Change Help



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

🚬 Click and DECiDE - Demo Usage Configurator 🛛 🔀						
* Device Ture lastelled						
Type Number of Devices	Add					
	Change					
Click and DECIDE - Demo Usage Configu	rator - Add Device					
cick and becibe being objecting						
Select the device type that you want to add.	ľ.					
	F I					
Device Tupe	Category					
Aladdin eSafe	E-mail Content Filtering					
Aladdin eSafe v5.2	Content Filtering					
- I Apache	Web Site					
ARKOON Network Security	Firewall; Proxy; Intrusion Prevention System					
Blue Loat Check Point (Real Time)	Proxy; Content Filtering					
Check Point Firewall (Command Line Flat Fil	le) Firewall					
Check Point Firewall (GUI Flat File)	Firewall					
Check Point Syslog UTM	Firewall					
Lisco Firewalls	Firewall					
Cisco IronPort-S	Proxu					
Clavister	Firewall					
Demo	Firewall; Proxy; Intrusion Prevention System					
Deny All	Intrusion Prevention System; Web Site					
	_					
OK Cancel <u>H</u> elp						
License Certificate						
View or update your current Click ar	nd DECIDE License Certificate					
	Settings					
_	UN Lancel Apply <u>H</u> elp					

- 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



Type From Type Name OK SINGLE 194.206.126.204 DMZ WebServer Cancel Internal DMZ WebServer Help external IP Add DMZ WebServer Edd 194.206.126.204 DMZ WebServer Edd 194.206.126.204 DMZ WebServer Edd 194.206.126.204 DMZ VebServer Edd 192.168.20 255.255.255 DMZ Public 192.168.00 192.168.255.255 Internal 192 Ehemove 100.0.0 10.255.255.255 Internal 10 Ehemove 172.16.00 172.31.255.255 Internal 172 Ehemove 127.0.01 Local host Move Up 255.255.255.255 Broadcast Move Up 0.0.0 255.255.255.254 External	ck and	DECiDE - Demo	Usage Configura	tor - Network Change	×	
From To/Mask Name Add 194,206,126,204 DMZ WebServer Change Change 192,168,2.0 255,255,255.0 DMZ Public Change 192,168,0.0 192,168,255,255 Internal 10 Change 172,16,0.0 172,31,255,255 Internal 172 Remove 1255,255,255 Broadcast Move Up 0,0.0 255,255,254 External Move Down	Tyr SINGI	pe LE 💌 194.20	From DMZ	Type Name WebServer nal	OK Cancel <u>H</u> elp	
From To/Mask Name 194.206.126.204 DMZ WebServer Add 192.168.20 255.255.255.0 DMZ Public Ehange 192.168.0.0 192.168.255.255 Internal 192 Ehange 100.0.0 10.255.255.255 Internal 10 Emove 172.16.0.0 172.31.255.255 Internal 172 Emove 255.255.255 Broadcast Move Up 0.0.0 255.255.255.254 External						external IP Addr
From To/Mask Name 194.206.126.204 DMZ WebServer Ehange 192.168.2.0 255.255.255 DMZ Public 192.168.0.0 192.168.255.255 Internal 192 10.0.0 10.255.255.255 Internal 10 172.16.0.0 172.31.255.255 Internal 172 127.0.01 Local host Move Up 0.0.0 255.255.254 External	c and	DECiDE - Demo	Usage Configura	tor - Network Connecti	on Settings	
Image: Product state DMZ WebServer 194.206.126.204 DMZ VebServer 192.168.20 255.255.255.0 DMZ Public 192.168.20 192.168.255.255 Internal 192 10.0.0 10.255.255.255 Internal 192 10.0.0 10.255.255 Internal 172 127.0.0.1 Local host 255.255.255 Broadcast 0.0.0 255.255.255.254 External Move Up		From	To/Mask	Name		Add
102.100.00 102.55.255 Internal 10 Remove 100.00 10255.255 Internal 10 Remove 172.16.0.0 172.31.255.255 Internal 172 127.0.0.1 Local host Move Up 0.0.0 255.255.255.254 External	Image: 194.206.126.204 DMZ WebServer 192.168.2.0 255.255.0 DMZ Public 192.168.2.0 192.168.2.0 192.168.2.0					<u>C</u> hange
127.0.0.1 Local host 255.255.255.255 Broadcast 0.0.0 255.255.255.254 External Move Down		10.0.0.0 172.16.0.0	10.255.255.255 172.31.255.255	Internal 10 Internal 172		<u>R</u> emove
Move <u>D</u> own		255.255.255.255 0.0.0.0	255.255.255.254	Local nost Broadcast External		Move <u>U</u> p
						Move <u>D</u> own
				ОК	Cancel	<u>H</u> elp

- 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_Re



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

Click and DECiDE - Demo Usage Configurator - Database Settings						
😂 🛛 Database Connection Settings						
	Please use only Case Ir	nsensitive settings.				
	Database Server:	Local SQL Server				
	Server Name:	NETREPORT-SRV1				
	Server Instance:	MSSQLSERVER				
	– Login –––––					
	Windows User:	NT AUTHORITY'Local System				
	Password:	Tear				
	Database Upda	te Setting				
	Consigure the update settings for the Successful Database connection. Delete existing data					
Database Time Zone Set						
						Use UTC offset (Coordinated Universal Time)
	Time Zone: (GMT+01	:00) Brussels, Copenhagen, Madrid, Paris 📃 📃				
	🔽 Adjust	for Daylight Saving Time (DST)				
Powered by	Click and DECiDE	OK Cancel <u>H</u> elp				

- 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.

Click and	DECiDE - for NSI Enterprise Configurator - T	asks Scheduling	×
14	Scheduling Run the Consolidation, Aggregation, Purge a	and Report Tasks everyday at 👔:00:00 AM 🚊	
	Purge Settings Detailed Data	Aggregated Data	
	 Velete al data arter treatment. Keep last 7 and days. 	Keep last 12 • months of data.	
		OK Cancel <u>H</u> elp	

- 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]
	C Windows Authentication	
	Click and DECiDE Authentication	
	Mail Server (SMTP)	1
	smtp.company.com	
	Mail Action Settings	1
	Enter the e-mail addresses to use to send Click and DECiDE alerts.	
	From: nsi@company.com	
	To: admin@company.com	
	OK Cancel <u>H</u> elp	

- 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:



Click and	Decide - D	emo Usage Configurat	or - Log Archive Settings		×
	- Log Stora Log Stora Vault. Log %NETR	ige Settings gegenerates files in Native Storage does not treat oth EPORT_STORAGE% Envi	e and/or Enriched CSV Format for temp rer Flat File Logs which can be directly ironment Variable: • C:\NetReportStor	orary storage before they are archi archived in the Archive Directory. age	ved by the Log
	The enviro	onment variable defines the	e default directory for the log storage ac	ctions.	
	- Log Vauli Verifies da	t General Settings ata integrity, compresses ar	nd encrypts logs for long-term archival.		
	Archive	e Directory:	C:\NetReportArchives	Þ	
	Archive Archive	Files from %NETREPORT Other Flat File Logs from B	[_STORAGE% Directory Older than Elsewhere Older than	2 Day(s) 2 Day(s)	
	Allo	w real-time archival	C Archive everyday at	12:00:00 AM	
	🔽 Pur	ge Archive Files Older thar	n	1 Year(s) 💌	
	🗖 Allo	w User to Delete			
	Security	Elick and DECiDE - Dem	no Usage Configurator - Add Devi	ce Logs to Archive	×
	Encry	General			
	Device L	Configuration Name:	All Logs		
	To enab the follov	Spied Directory:	•%NETREPORT_STORA	GE%	
		File Name:	× × .		
	Configur				vdd
		Security			ange
		Verity Data Inte	egnty		emove
		🔽 Encrypt Data			011070
	⊂Archive Select ≀	Transfer Archive Files After files have been ar local copy or FTP trans Archive File Tran	rchived via the Log Vault, you can mov sfer. nsfer disabled.	ve them to another location via	
			ОК	Cancel <u>H</u> elp	

- 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

View Performance counter 5.1.

- 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.

Add Counters	? ×
 Use local computer counters Select counters from computer: 	
\\RR0-W2003-32	•
Performance <u>o</u> bject: NetReport Filter Engine	
All counters	O <u>A</u> ll instances
C Select counters from list:	Select instances from list:
# nelif processed # of nelif in error queue # of nelif in queue Rate of nelif processed	NetReport Filter Engine
A <u>d</u> d <u>E</u> xplain	
	<u>C</u> lose

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



8. 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 DECiDEWSI/Error agent Storage. You can modify the destination of these files by changing the registry value: HKEY LOCAL MACHINE\SOFTWARE\WetReport\MC\Agents\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	Туре	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.

Control the database insertion 5.3.

- 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.

🖉 Click and DECiDE Web Portal - Menus	🖉 Click and DECIDE Web Portal - Menus - Windows Internet Explorer 📃 🗖 🗙							
SS v lei http://localhost/dvweb/l	Menulaspx 💽 🗟 🐓 🗙	bing Bing	₽ •					
🚖 Favorites 🛛 🄏 Click and DECiDE Web I	Portal - Menus							
M Click	DECIDE							
Web Server Configuration	Firewall Statistics Utilities	Size Modification	Creation					
	💷 <u>1 - Selected Record Details</u>	0 1/21/2010 5:14:15 PM	9/2/2004 10:43:08 AM					
🖃 🚞 NSI Utilities	🐙 <u>2 - Number of Records in the Firewall Tables</u>	0 1/21/2010 5:20:02 PM	9/2/2004 10:43:08 AM					
🖃 📾 Database Status	🗐 <u>3 - Address Definition Management</u>	0 1/21/2010 4:07:29 PM	9/2/2004 10:43:08 AM					
Firewall Statistics Utilities Click and DECIDE Audit	🕼 <u>4 - Firewall Aggregation Process Status</u>	0 4/28/2010 4:57:31 PM	9/2/2004 10:43:08 AM					
🚰 Proxy Statistics Utilities								
🗉 🚞 NSI Alert Management								
Scheduled Tasks & Tasks								
Content Builder								
Web Server Administration								

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	🖉 Click and DECiDE Web Portal - Menus - Windows Internet Explorer 📃 🗆 🗙						
COO - Attp://localhost/dvweb/f	nenu, aspx	💌 🗟 👉 🗙 🔁 Bing	₽ ▼				
🔶 Favorites 🛛 🄏 Click and DECiDE Web I	Portal - Menus						
Click& DECIDE							
Web Server Configuration	🚹 🗐 욿 🗌 Parame	ters Result Both					
	From: Today - X days To: Today - Y days Start time: Stop time: Firewall? (Ignore for all) Output Format: PDF	2 - Number of Records in the Fire 10 0 5/6/2009 12:00:00 AM 5/6/2010 11:59:59 PM 3 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	wall Tables				

7. Click Run.



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



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**.

🔮 Scheduled Tasks						_ 🗆 🗡		
Eile Edit View Favorites Iools Advanced Help								
🕓 Back 👻 🕤 👻 🏂 Searc	🔇 Back 🔻 🕘 🛩 🏂 🔎 Search 🌔 Folders 🛛 😰 🎯 🗙 🎾 🛄 -							
Address 🙆 Scheduled Tasks						💌 🄁 Go		
Name 🔺		Schedule	Next Run Time	Last Ru	Status	Last Result		
Add Scheduled Task Click and DECIDE NSI Scheduled Purge Alerts Tables SQL Firewall Alert	Run End Task Cut Copy Delete Rename Properti	0 AM 3 AM ed es	1:00:00 AM 1:23:00 AM Disabled	Never Never Never		0x0 0x0 0x0		
•						F		

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

🔮 Scheduled Tasks						
File Edit View Favorites Tools Advanced Help						
🕝 Back 👻 🕘 👻 🏂 🔎 Search 🌔 Folder	s 🔯 🎯 🕽	× 🍤 🛄-				
Address Cheduled Tasks					💌 🄁 Go	
Name 🔺	Schedule	Next Run Time	Last Ru	Status	Last Result	
🖸 Add Scheduled Task						
Click and DECiDE NSI Scheduled Dashboards	At 1:00 AM	1:00:00 AM	5:01:41	Running	0×0	
👸 Purge Alerts Tables	At 1:23 AM	1:23:00 AM	Never		0×0	
😠 SQL Firewall Alert	Disabled	Disabled	Never		0×0	
•					F	

- 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.

🖉 Click and DECiDE Web Portal - Menus - Windows Internet Explorer							
G S v I http://localhost/dvweb	/Menu.aspx	💌 🗟 👉 🗙 🄄 Bing					
🔶 Favorites 🛛 🏉 Click and DECiDE Web	Portal - Menus						
M Click	& DECi	DE					
Web Server Configuration	Firewall	Size Modification	Creation				
Menus	🔁 Firewall Daily 100505	164,630 5/6/2010 5:02:25 PM	5/6/2010 5:02:23 PM				
B Dublished Reports							
Proxy							
a Dynamic Reports							
🚔 Forensic Analysis							
🚞 My Projects							
🖃 🚞 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							

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.

Generate a Dynamic Report 6.1.

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

Select the Period or Other for a Date: Ioday Yesterday Select the Date (if Other selected): 6/Z/2010 Proxy? (Ignore for all): ISNORE P Source beginning with? (enter the first characters or full value): IGNORE P Source beginning with? (enter the first characters or full value): IGNORE P source beginning with? (enter the first characters or full value): IGNORE Vanonymous User? No User? (Ignore for all): User Group beginning with? (enter the first characters or full name): IGNORE Wester Group beginning with? (enter the first characters or full name): IGNORE Waser Group beginning with? (enter the first characters or full name): IGNORE Waser Group beginning with? (enter the first characters or full name): IGNORE Waser Group beginning with? (enter the first characters or full name): IGNORE Waser Group beginning with? (enter the first characters or full name): IGNORE Waser Group beginning with? (enter the first characters or full name): IGNORE Waser Group beginning with? (enter the first characters or full name): IGNORE Waser Group beginning with? (enter the first characters or full name): IGNORE Waser Group begin b	🔏 🗐 😫 📂	Parameters	Result Both Report Book for the Proxy Daily Reports						
Vertice 20dsy Octher 20dsy Select the Date (if Other selected): 6/2/2010 Proxy? (Ignore for all): IGNORE IP Source? (Ignore for all): IGNORE Destination? (Ignore for all): IGNORE Anonymous User? No Ver? (Ignore for all): IGNORE User? (Ignore for all): IGNORE Ver? (Ignore for all): IGNORE User? (Ignore for all): IGNORE Ver? (Ignore for all): IGNORE V	Select the Period	l or Other for a [)ate:			Today			
Select the Date (if Other selected):6/2/2010Proxy? (Ignore for all):IGNOREIP Source? (Ignore for all):IGNOREDestination? (Ignore for all):IGNOREAnonymous User?NoUser? (Ignore for all):IGNOREUser? (Ignore for all):IGNOREUser? (Ignore for all):IGNOREUser? (Ignore for all):IGNORETop N Visited Domain?IGNORETop N Visited Domain by User or IP Address?STop N Visited Domain by User or IP Address?30Top N Visited Domain?STop N Visited Domain?IOTop N Visited Domain?IOIT Top N Visited Domain?IOIT Top N Visited Categories?IOIT Top N User or IP Address by Category?IOIT Top N Visited Categories?IOIT Top N Visited Categories?IOIT Top N Visited Categories?IOIT Top N Visited Categories?IOIT Top						Other			
Select the Date (if Other selected):6/2/2010Proxy? (Ignore for all):IGNOREIP Source? (Ignore for all):IGNOREDestination? (Ignore for all):IGNOREVanoymous User?NoUser? (Ignore for all):IGNOREUser? (Ignore for all):IGNOREUser Group beginning with? (enter the first characters or full name):Prop N Visited Domain?IGNOREVanoy N Visited Domain by User or IP Address?SVanoy N User or IP Address by Visited Domain?SVanoy N Visited Domain by User or IP Address?IoVanoy N Viser?IoVanoy N Viser? <t< th=""><th></th><th></th><th></th><th></th><th></th><th>8</th><th></th></t<>						8			
Proxy? (Ignore for all): IGNORE IP Source? (Ignore for all): IGNORE Destination? (Ignore for all): IGNORE Anonymous User? No User? (Ignore for all): IGNORE User? (Ignore for all): IGNORE User? (Ignore for all): IGNORE Vser Group beginning with? (enter the first characters or full name): IGNORE Vser Group beginning with? (enter the first characters or full name): IGNORE Vser Group beginning with? (enter the first characters or full name): IGNORE Vser Group beginning with? (enter the first characters or full name): IGNORE Vser Group beginning with? (enter the first characters or full name): IGNORE Vser Group beginning with? (enter the first characters or full name): IGNORE Vser Group beginning with? (enter the first characters or full name): IGNORE Vser Group beginning with? (enter the first characters or full name): IGNORE Vser Group beginning with? (enter the first characters or full name): IGNORE Vser Group beginning with? (enter the first characters or full name): IGNORE Vser Group beginning with? II Vser Group N Visited Domain? S Vop N Visited Domain by User or IP	Select the Date (i	if Other selected	l):			6/2/2010			
IP Source? (Ignore for all): IGNORE IP Source beginning with? (enter the first characters or full value): IGNORE Destination? (Ignore for all): IGNORE Vanonymous User? No User? (Ignore for all): IGNORE User? (Ignore for all): IGNORE Vser Group beginning with? (enter the first characters or full name): IGNORE Vser Group beginning with? (enter the first characters or full name): IGNORE Vser Group beginning with? (enter the first characters or full name): IGNORE Vser Group beginning with? (enter the first characters or full name): IGNORE Vser Group beginning with? (enter the first characters or full name): IGNORE Vser Group beginning with? (enter the first characters or full name): IGNORE Vser Group beginning with? (enter the first characters or full name): IGNORE Vser Group beginning with? (enter the first characters or full name): IGNORE Vser Group beginning with? (enter the first characters or full name): IGNORE Vser Group beginning with? (enter the first characters or full name): IGNORE Vser Group N Visited Domain? 30 Image: Second image: Secon	Proxy? (Ignore for	or all):				IGNORE			
 IP Source beginning with? (enter the first characters or full value): IGNORE Destination? (Ignore for all): IGNORE Vanonymous User? User? (Ignore for all): User Group beginning with? (enter the first characters or full name): IGNORE Vaser Group beginning with? (enter the first characters or full name): IGNORE We For by IP Address or by User? IP Address Vor top N Visited Domain? Top N Visited Domain by User or IP Address? Top N Users? Top N Users? Top N Search Engine? Top N Countries? Top N Countries? Top N Operating Systems? Top N Visited Categories? Top N Visited Categories? Top N Visited Category by Category? Top N Visited Category by User or IP Address? 	IP Source? (Ignor	re for all):				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 V Top N Visited Domain? Iop N Visited Domain by User or IP Address? 5 Top N User or IP Address by Visited Domain? 30 Top N Users? 30 Top N Status? 10 Top N Keywords? 10 Top N Countries? 10 Top N Operating Systems? 10 Top N Visited Categories? 10 Top N Visited Categories? 5 Top N User or IP Address by Category? 5	IP Source beginn	ning with? (enter	the first chara	cters or full va	lue):	IGNORE			
 Anonymous User? No User? (Ignore for all): User Group beginning with? (enter the first characters or full name): IGNORE IBNORE IP Address or by User? IP Address User Top N Visited Domain? Top N Visited Domain by User or IP Address? Top N User or IP Address by Visited Domain? Top N Users? Top N Status? Top N Keywords? Top N Keywords? Top N Countries? Top N Operating Systems? Top N Visited Categories? Top N Visited Categories? Top N Visited Categories? Top N Visited Category? Top N Viser or IP Address? Top N Visited Category by User or IP Address? 	Destination? (Ign	nore for all):				IGNORE			
 User? (Ignore for all): User Group beginning with? (enter the first characters or full name): IGNORE IGNORE IP Address IP Address IP Address User IP Address User IP Address IP Ad	Anonymous Use	er?				No			
 User Group beginning with? (enter the first characters or full name): IGNORE Report by IP Address or by User? IP Address User User Top N Visited Domain? Top N Visited Domain by User or IP Address? Top N User or IP Address by Visited Domain? Top N Users? Top N Users? Top N Status? Top N Search Engine? Top N Countries? Top N Operating Systems? Top N User or IP Address by Category? Top N Visited Categories? Top N User or IP Address by Category? Top N User or IP Address? 	User? (Ignore for	r all):				IGNORE			
 Report by IP Address or by User? IP Address User Top N Visited Domain? Top N Visited Domain by User or IP Address? Top N User or IP Address by Visited Domain? Top N Users? Top N Status? Top N Search Engine? Top N Keywords? Top N Countries? Top N Operating Systems? Top N User or IP Address by Category? Top N User or IP Address? 	User Group begin	nning with? (ent	ter the first cha	racters or full	name):	IGNORE			
Image: Constraint of the sector of the didress?	Report by IP Add	dress or by User?				IP Address			
 Top N Visited Domain? Top N Visited Domain by User or IP Address? Top N User or IP Address by Visited Domain? Top N Users? Top N Status? Top N Search Engine? Top N Keywords? Top N Countries? Top N Operating Systems? Top N Visited Categories? Top N User or IP Address? 						User			
 Top N Visited Domain by User or IP Address? Top N User or IP Address by Visited Domain? Top N Users? Top N Status? Top N Search Engine? Top N Keywords? Top N Countries? Top N Operating Systems? Top N Browsers? Top N Visited Categories? Top N User or IP Address? 	🕡 Top N Visited Do	omain?				20			
 Top N User or IP Address by Visited Domain? Top N Users? Top N Status? Top N Search Engine? Top N Keywords? Top N Countries? Top N Operating Systems? Top N Browsers? Top N Visited Categories? Top N User or IP Address by Category? Top N Category by User or IP Address? 	Top N Visited Do	omain by User o	r IP Address?			5			
Image: Constraint of the second s	Top N User or IP	Address by Visit	ted Domain?			5			
Image: Constraint of the second se	Top N Users?	-				30			
Image: Constraint of the second se	Top N Status?					10			
Image: Constraint of the second se	Top N Search En	igine?				10			
Image: Construint of the second se	Top N Keywords	2 1?				10			
Image: Constraint of the second se	Top N Countries	?				10			
Image: Constraint of the second se	Top N Operating	g Systems?				10			
Image: Constraint of the second se	Top N Browsers?	?				10			
Top N User or IP Address by Category? 5 Top N Category by User or IP Address? 5	Top N Visited Ca	tegories?		10					
Top N Category by User or IP Address?	Top N User or IP	Top N User or IP Address by Category?				5			
	Top N Category	by User or IP Ad	ldress?			5			
	Output Formati @ 7	- 	Burn 💼 🖻	(m)		-			



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 (I)?
- 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

Cube Chart			
📴 🚉 🕌 🎬	Ϋ 🖳 Σ+ 🏪 👼 %, 🖛	日 🖷 🖬 🖬 🛯 🍤 🛛	🗎 🗉 🕐
Firewall Cube on D	etailed Information (lim	ited to 100 000 reco	ds) Field List
DATE YYYY MM DD	HH 🔻		
All YYYY MM DD HH	1		
		Action Group -	
		Accepted	Blocked
Source Net Area 🕶	Destination Net Area 🕶	Hits	Hits
External		12	7 4
	Internal 172	24	9 287
	Internal 192		6
Internal 192		10,97	3 166
	Internal 172		7
Grand Total		11,36	2 457



- 6. With the manipulation of sort $2 \downarrow 1$ icon, top x $12 \downarrow 1$ icon, top x $12 \downarrow 1$ icon, drag and drop of dimension \square , try to view the following :
 - a. Top 25 services by top 10 Rules and Action Group

		/ /						
Firewall C	rewall Cube on Detailed Information (limited to 100 000 records)							
DATE YYYY	MM DD HH 🔻							
AII YYYY M	IM DD HH							
	Rule V Action Group V							
	⊟ 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		
🗆 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

Sepa	ale	uie g	napri	Dy St	alus				
Cube	Chart								
83 6	a ĝ	Z I	1	Σ.	📮 %	03 iki		3 0	2)
Eirowall Cube on Detailed Information (limited to 100,000 records)									

Firewall Cube on Detailed Information (limited to 100 000 records)							
Source hierarchy 🔻							
External							
	Action Group 🔻						
			🗉 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





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

🚮 🗐 📚 🗕	arameters	Result	Both	IPS Cube on Detailed Information (limited to 100 000 records)
👽 Select the Period c	r Other for a Date	: Yesterday		
📝 Start Date and Tim	ie (Inclusive):	6/2/2010 1	2:00:00 AM	
📝 End Date and Time	e (Inclusive):	6/2/2010 1	1:59:59 PM	
👿 IPS? (Ignore for all):	harry IPS_MPL		
📄 Source? (Ignore fo	r all):	IGNORE		
📄 Destination? (Igno	re for all):	IGNORE		
Output Format: 🔘 HT	ML Run 🛅			

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





IPS Cube on Detailed Inform	ation (limited to	100 000 records	s)	
Cube Chart				DiscaTable Field is
😫 🖻 👌 🕻 🎬 👰 🗵	- 🔚 🔜 🌾 🖓	-1 +1 im im	🎽 🗎 🗉 🖉	Drag items to the PivotTable list
IPS Cube on Detailed Inform	nation (limited	to 100 000 rec	ords)	IPS Detailed
Date YYYY MM DD HH - Da	te Detailed 🔻		·	D 10 Totals
AII YYYY MM DD HH 🛛 AII	Detailed			10 Count
	Action Group	Action		⊕ 🗐 Action hierarchy
	🗄 Blocked	Accepted		Attack hierarchy
				€
Attack Category 🔻 Attack I	D Count	Count		Country Source
🗄 netbios	20	143		🗄 🗐 Date Detailed
⊞ p2p		48		🛓 🗐 Date YYYY MM DD HH
⊞ dns_decoder		25		🗄 🗐 Destination hierarchy
⊞ icmp	17	4		IPS Product
li im		15		🗄 🗐 Origin
anomaly Devial of Service	1	1		Protocol
		1		
⊞ web-mst		I		
				🛓 🗐 Source Port
				Source hierarchy
				Add to Row Area 🔻

- 6. With the manipulation of sort $2 \downarrow 1$ icon, top x 12 = 100 icon, drag and drop of dimension 12, 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

Drop Filter Fields Here									
						Action Group	 Action 		
						🖽 Blocked	Accepted		
Attack Category 🔻	Attack ID	Attack Name	IP Source 🔹	IP Destination 🔻	Date 🔻	Count	Count		
Denial of Service	□ FGT101974314	Microsoft.Works.Spreadsheet.Memory.Corruption		⊟ 192.168.0.3	19/01/2010 19:14:00	1			
🗆 netbios	□ FGT102039558	NT.NULL.Session	⊟ 66.11.102.220	目 192.168.0.52	19/01/2010 15:13:00		1		
🗆 web-misc	□ FGT103350551	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

	Date YYYY MM DD HH					
		E				
	♥19 ♥20 ♥21					
	- ▼ 22 ▼23					
ate selectior	OK Cancel	and field selection:				
ibe Chart						
	Σ• 😭 💐 🍕 💾 🍯 補	ii 🎽 🖹 🗉 🛛				
te YYYY MM DD HH -	ormation (limited to 100 00	J records)				
lultiple Items)					Action Group ⊞ Blocked	 ► Action E Accepte
Source • Attack Cat	egory 🔻 Attack ID	Attack Name	IP Destination 🔻	Date 🔻	Count	Count
192.168.0.52 ⊡ netbios	□ FGT102039613		□ 192.168.0.201	19/01/2010 15:09:00 19/01/2010 15:16:00 19/01/2010 15:21:00		
				19/01/2010 15:33:00 19/01/2010 15:41:00 19/01/2010 16:34:00		
				19/01/2010 16:34:00		
				19/01/2010 16:59:00		
				19/01/2010 17:23:00 19/01/2010 17:24:00		
				19/01/2010 17:28:00 19/01/2010 17:48:00		
				19/01/2010 18:12:00		
				19/01/2010 19:01:00		
				19/01/2010 19:26:00		
				10/01/2010 20:47:00		
				19/01/2010 20:15:00		
				19/01/2010 20:15:00 19/01/2010 20:52:00 19/01/2010 21:28:00		
				19/01/2010 20:15:00 19/01/2010 20:52:00 19/01/2010 21:28:00 19/01/2010 21:29:00 19/01/2010 21:53:00		
				19/01/2010 20:15:00 19/01/2010 20:52:00 19/01/2010 21:28:00 19/01/2010 21:29:00 19/01/2010 21:53:00 19/01/2010 22:17:00		
				19/01/2010 20:52:00 19/01/2010 20:52:00 19/01/2010 21:28:00 19/01/2010 21:29:00 19/01/2010 21:53:00 19/01/2010 22:17:00 19/01/2010 22:42:00 19/01/2010 22:06:00		
				19/01/2010 20:52:00 19/01/2010 20:52:00 19/01/2010 21:28:00 19/01/2010 21:28:00 19/01/2010 21:29:00 19/01/2010 21:29:00 19/01/2010 22:42:00 19/01/2010 23:06:00 19/01/2010 23:31:00		
	E FGT102039618		nain 139 E 192.168.0.201 E 192.168.0.204	19/01/2010 20:52:00 19/01/2010 20:52:00 19/01/2010 21:28:00 19/01/2010 21:28:00 19/01/2010 21:29:00 19/01/2010 22:17:00 19/01/2010 22:42:00 19/01/2010 23:06:00 19/01/2010 23:31:00 19/01/2010 18:05:00	1	
	E FGT102039618		nain 139 E 192 168.0.201 E 192 168.0.204	19/07/2010 20 15:00 19/07/2010 21:28:00 19/07/2010 21:28:00 19/07/2010 21:53:00 19/07/2010 21:53:00 19/07/2010 22:17:00 19/07/2010 23:06:00 19/07/2010 23:06:00 19/07/2010 18:07:00 19/07/2010 18:07:00 19/07/2010 18:07:00	1	
	⊟ FGT102039618		nain 139 = 192 168.0.201 = 192 168.0.204 = 192 168.0.59 = 192 168.0.69	19/07/2010 20 15:00 19/07/2010 21:28:00 19/07/2010 21:28:00 19/07/2010 21:53:00 19/07/2010 21:53:00 19/07/2010 22:17:00 19/07/2010 23:06:00 19/07/2010 23:06:00 19/07/2010 18:06:00 19/07/2010 18:07:00 19/07/2010 18:07:00 19/07/2010 18:07:00 19/07/2010 16:06:00	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	
0 iour	⊟ FGT102039618		nain 139 = 192 168.0.201 = 192 168.0.204 = 192 168.0.59 = 192 168.0.87	19/07/2010 20:52:00 19/07/2010 21:52:00 19/07/2010 21:28:00 19/07/2010 21:53:00 19/07/2010 21:53:00 19/07/2010 22:17:00 19/07/2010 23:06:00 19/07/2010 23:06:00 19/07/2010 23:06:00 19/07/2010 18:07:00 19/07/2010 18:07:00 19/07/2010 18:07:00 19/07/2010 16:05:00 19/07/2010 16:05:00	1 1 1 1 1 1 1	

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 Per	iod or Other for a 🛙	ate: Yesterday	
📝 Start Date and	l Time (Inclusive):	6/2/2010 12:00:00 AN	1
📝 End Date and	Time (Inclusive):	6/2/2010 11:59:59 PN	1
👿 Proxy? (Ignore	e for all):	FW-MPL IronPort-S SG-HTTP-Service	
📄 Source? (Igno	re for all):	IGNORE	
📄 User? (Ignore	for all):	George Hector Jairo Jo John Joy ken	
		6	08
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





- 6. With the manipulation of sort $2 \downarrow 1$ icon, top x $12 \downarrow 1$ icon, top x $12 \downarrow 1$ icon, drag and drop of dimension \square , try to view the following :
 - a. Check where are surfing the top 2 users in time
 - b. Check if it is during work hours! Full result:

Pro:	cy Cuk	e on Detailed Information b	y User (Limited to 100 000 records)									
Cube by	y User	Chart by User										
8 8 R	Â	↓ Z↓ 🚰 👰 Σ+ 🖍 👼	炎 三 41 前 浦 👋 🗎 🗉	2								
Ргоху	Cube	on Detailed Information	(Limited to 100 000 records)									
Drop Fi	ilter F	ields Here										
				Years 🔻 Mor	nths Days Hou	rs						
				□ 2010	-							
				🗆 January								
				⊡ 19								
				9	10	11	12	14	15	16	17	Total
User	7.	Category 🛛 🔻	Destination	7 Elapsed Time	Elapsed Time	Elapsed Time	Elapsed Time	Elapsed Time	e Elapsed Time	Elapsed Time	Elapsed Time	Elapsed Time
🗆 Jo		🗆 Business	www.villasprisme.com		3 801	9 814						13 615
			www.vente-privee.com							8 302		8 302
			🖽 www.paruvendu.com	1 127	·	14						1 141
			🖽 www.ideesmaison.com		861							861
			⊞ www.toutfaire.com					525	5			525
			🖽 guidemateriaux.toutfaire.com					483	3			483
			🗉 www.cyberarchi.com				413	1				413
		Shopping and Auction	🕀 www.maisons-avenir-tradition.com	n			3 143	1				3 143
			🗉 rcm-images.amazon.com				7					7
			🗉 www.abebooks.com				7					7
			🕀 www.eurorelais.org				7					7
		⊞ Search Engines			2 310		637			42		2 989
		Content Servers		7	189	154	1 876	i 28	3	371		2 625
		⊞ Information Technology		128	5 14	14	532			1 330		2 016
		⊟ Sports	🖽 www.lequipe.com				896	i				896
			⊞ www.handzone.net							406		406
			🖽 www.ff-handball.org							350		350
			⊞ www.sports.com							14		14
			⊞ sports.voila.com							7		7
		⊞ Travel					224					224
										7		7
🗆 Chri	8	🗆 News and Media	⊞ medias.lemonde.com	1 883	3 493				910	2 1 4 9	910	9 345
			www.liberation.com		854							854
		🗆 Sports	⊞ www.sport365.com		756							756
		E Content Servers		42	: 91				21	42	21	217
0	T	⊞ Information Technology		0.404	42	0.000	7 7 40	4.000		40.000	004	42
Grand	rota			3 185	12 411	a aae	/ /42	1 036	931	13 020	931	49 252

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:

- 1. Launch Click&DECiDE Configurator
- 2. In Device Type, select Add
- 3. 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
- 4. In the Log File Acquisition Settings window, select Log in Real-Time with Syslog Protocol. Enter the Syslog IP address of your device.
- 5. Select OK
- 6. 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
- I. 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

Data available in SQL database 11.1.

- 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

Administrator user screen access: 11.2.1.

🖉 Click and DECiDE Web Portal - Menus - Wind	lows Internet Explorer			
COO V Inttp://localhost/dvweb/Default.as	spx?NoInit=1		💌 🗲 🗙 🔽 Bing	₽ •
🚖 Favorites 🛛 🏀 Click and DECIDE Web Portal - M	Menus			
M Click&	DECiDE			
Web Server Configuration	Web Parts Yesterday Firewall Dashboard	Yesterday IPS Dashboard Yesterday Prox	y Dashboard	
Windows as:				
User: NSI-10-2\ADMINISTRATOR	Alerts	Daily Reports	Monthly	Reports
Groups: ADMINISTRATORS AUTHENTICATED USERS	Title Date Alert on Many Rejection by Tad 1/16/201	Title I Intrusion Prevention System Daily Dashboard	Date Title 1/16/2011 Proxy Monthly Dashboard	Date 1/5/2011
INTERACTIVE	Alert on Many Rejection by Victoria 1/16/201	I Proxy Daily Dashboard	1/16/2011 Intrusion Prevention System	n Monthly 1/5/2011
NTLM AUTHENTICATION	Alert on Many Rejection by Zoe 1/16/201	I Firewall Daily Dashboard	1/16/2011 (i) Firewall Monthly Dashboard	d 1/5/2011
	Alert on Hits on Accepted on firewall FW-MPL 1/16/201	I Intrusion Prevention System Daily Dashboard	1/5/2011 < Page	= 1/1 >
Your Server Administrator Credentials:	Alert on Bytes on Service 25 1/16/201	I Proxy Daily Dashboard	1/5/2011	
	Alert on Hits on Service 80 1/16/201	I Firewall Daily Dashboard	1/5/2011	
USERS	Alert on Hits on a IP 192.168.0.37 1/16/201	Page 1/1	>	
	Alert on Bytes on a IP 192.168.2.22 1/16/201	L		
WP ::1	Alert on Suspicious Port Scan 62.210.136.135 1/16/201			
Click and DECIDE	Proxy Alert on Bytes on a IP 192.168.0.37 1/16/201			
Language:	< Page 1/1	>		
I Display banner				
Add a nome Page				
# Title URL				
			Local intranet Protected Mode: Off	🖓 🕶 🔍 100% 💌 //
P		, , , , ,	· · · ·	, _ , ///



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 webPatts 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
- Click and Decide Web Parts Update 4.

🕒 Task Scheduler							
Eile Action View Help							
🗢 🔿 🔰 💽 🖬							
Task Scheduler (Local)	Name	S.,	▼ Triggers	Next Run Time	Last Run Time	Last Run Result	Author
Task Scheduler Library	Click and DECIDE NSI Scheduled Dashboards	Ready	At 1:00 AM every day	1/17/2011 1:00:00 AM	1/16/2011 4:41:45 PM	The operation completed successfully. (0x0)	Click and Decide Task M
	Click and Decide Demo Alerts	Ready	At 1:10 PM every day	1/17/2011 1:10:00 PM	1/16/2011 7:15:59 PM	The operation completed successfully. (0x0)	Click and Decide Task №
	Click and Decide Web Parts Update	Ready	At 1:20 PM eve Run	1/17/2011 1:20:00 PM	1/16/2011 7:14:00 PM	The operation completed successfully. (0x0)	Click and Decide Task M
	Purge Alerts Tables	Ready	At 1:23 AM eve End	1/17/2011 1:23:00 AM	Never		Click and Decide Task M
	🕒 SQL Firewall Alert	Disabled	At 1:30 PM eve Disable		Never		SYSTEM
	B Renew Windows 2008 Evalutation Period	Ready	At 12:30 PM ev Export	2/16/2011 12:30:00 PM	Never		W2008-32-EVAL\Admin
	(Now	Ready	At 7:14 PM on Properties		1/16/2011 7:15:33 PM	The operation completed successfully. (0x0)	Click and Decide Task M
			Delete]			Þ