NetFlow Data Collection using nTop and nProbe

Kyurim Rhee

Sept-22-2010

Purpose:

To collect NetFlow data using nTop and nProbe NetFlow probe.

Lab Setup

We have set up a voice and data traffic generated by IXIA traffic generator which the traffic was passed through a designated router. The router was configured to send NetFlow data to my PC which collected the NetFlow data using nProbe. Below is a diagram of our lab layout.



Running the nProbe:

First nProbe must be initiated:

nProbe shut down
C:\Program Files\nProbe-Win32>nprobe ∕c -h Running nProbe for Win32.
Welcome to nprobe v.5.8.1 (\$Revision: 1659 \$) for Win32
Built on 08/09/10 08:49:49 Copyright 2002-10 by Luca Deri <deri@ntop.org></deri@ntop.org>
Usage: nprobe -n <host:portinone> [-i <interfaceldump file="">] [-t <lifetime timeout="">] [-d <idle timeout="">] [-l <queue timeout="">] [-s <scan cycle="">] [-h [-p <aggregation>] [-f <filter>] [-a] [-b <level>] [-P <path>] [-F <dump timeout="">] [-D <format>] [-u <in dev="" idx="">] [-Q <qut dev="" idx="">]</qut></in></format></dump></path></level></filter></aggregation></scan></queue></idle></lifetime></interfaceldump></host:portinone>

Install nProbe service and have it collect the NetFlow data at a given directory on your local machine:



Start the nProbe service:

go to Windows Control Panel-->Administrative -->Tools--> Services--> and manually Start/Stop Services

🍇 Services											
File Action View Help											
Services (Local)	Services (Local)	_									
	nprobe	Name 🔺	Description	Status	Startup Type	Log On As	A				
		Network Access Pr	Allows win		Manual	Local System					
	Start the service	🏶 Network Connections	Manages o	Started	Manual	Local System					
		🍓 Network DDE	Provides n		Disabled	Local System					
	Description:	🆓 Network DDE DSDM	Manages D		Disabled	Local System					
	nProbe v.5.8.1 - NetFlow/IPFIX Probe. http://www.ntop.org/	🖏 Network Location A	Collects an	Started	Manual	Local System					
		🆓 Network Provisionin	Manages X		Manual	Local System					
		🎭 nprobe	nProbe v.5		Automatic	Local System					
		🆓 NT LM Security Sup	Provides s		Manual	Local System					
		🆓 NVIDIA Display Driv	Provides s	Started	Automatic	Local System					
		🆓 Office Source Engine	Saves inst		Manual	Local System					
		Performance Logs	Collects pe		Manual	Network S					
		🍓 Plug and Play	Enables a c	Started	Automatic	Local System					
		🍓 Pointsec		Started	Automatic	Local System					

NetFlow Data Format

We were successful in collecting the NetFlow data. The data is delimited with " | " and contain the following parameters:

 I
 IPV4_SRC_ADDR| IPV4_DST_ADDR| IPV4_NEXT_HOP| INPUT_SNHP| OUTPUT_SNHP| IN_PKTS| IN_BYTES| FIRST_SWITCHED| LAST_SWITCHED| L4_SSC_PORT| L4_DST_PORT| TCP_FLAGS| PROTOCOL| SRC_AS| DST_AS| DST_AS| IPV4_SRC_MASK| IPV4_DST_MASK

 2
 192.168.1.109| 192.168.1.13 | 0
 1147
 0
 11
 176
 1285164039
 1285164215
 123
 116
 17
 16
 0
 0
 0
 0

IPV4_SRC_ADDR	Source IP Address
IPV4_DST_ADDR	Destination IP Address
IPV_NEXT_HOP	
INPUT_SNMP	
OUTPUT_SNMP	
IN_PKTS	Total Number of Packets received in this time frame
IN_BYTES	Total Number of Bytes received in this time frame
FIRST_SWITCHED	Start Time stamp
LAST_SWITCHED	Stop Time stamp
L4_SRC_PORT	Layer4 Source Port number
L4_DST_PORT	Layer4 Destination Port Number
TCP_FLAGS	Check Chart
PROTOCOL	Check Chart
SRC_TOS	Check Chart
SRC_AS	Source Autonomous System
DST_AS	Destination Autonomous System
IPV4_SRC_MASK	
IPV4_DST_MASK	

Collection Interval

This NetFlow data is collected in every 1 minute interval. nProbe will collect the NetFlow data and organize it by creating directories in "Year/Month/Date/Hour" manner.

The following is a snapshot of 33 minutes of NetFlow data gathered on 2010-09-22 between 10:00AM - 10:33AM.

Address C:\flows\2010\09\22\10									
Folders	x	Name 🔺	Size	Туре	Date Modified				
🞯 Desktop		🖬 00.flows	11 KB	FLOWS File	9/22/2010 10:01 AM				
		🖬 01.flows	10 KB	FLOWS File	9/22/2010 10:02 AM				
Downloads		🔟 02.flows	10 KB	FLOWS File	9/22/2010 10:03 AM				
		🖬 03.flows	12 KB	FLOWS File	9/22/2010 10:04 AM				
My Data Sources		🖬 04.flows	12 KB	FLOWS File	9/22/2010 10:05 AM				
🗉 🔂 My Music		🖬 05.flows	13 KB	FLOWS File	9/22/2010 10:06 AM				
My Personal		🔟 06.flows	14 KB	FLOWS File	9/22/2010 10:07 AM				
🗉 👜 My Pictures		🖬 07.flows	13 KB	FLOWS File	9/22/2010 10:08 AM				
My Received Files		🔟 08.flows	14 KB	FLOWS File	9/22/2010 10:09 AM				
My Videos		🔟 09.flows	14 KB	FLOWS File	9/22/2010 10:10 AM				
🗉 🧰 My WebPage		🔟 10.flows	14 KB	FLOWS File	9/22/2010 10:11 AM				
Im NetBeansProjects		🔟 11.flows	13 KB	FLOWS File	9/22/2010 10:12 AM				
🗉 🧰 OneNote Notebooks		🔟 12.flows	13 KB	FLOWS File	9/22/2010 10:13 AM				
🗉 🫅 OxygenXMLEditor		🔟 13.flows	13 KB	FLOWS File	9/22/2010 10:14 AM				
SharePoint Drafts		🛅 14.flows	14 KB	FLOWS File	9/22/2010 10:15 AM				
🖃 晃 My Computer		15.flows	15 KB	FLOWS File	9/22/2010 10:16 AM				
🖂 🧼 C-DISK (C:)		16.flows	14 KB	FLOWS File	9/22/2010 10:17 AM				
⊞		17.flows	14 KB	FLOWS File	9/22/2010 10:18 AM				
BackUp Programs		18.flows	14 KB	FLOWS File	9/22/2010 10:19 AM				
Documents and Settings		19.flows	16 KB	FLOWS File	9/22/2010 10:20 AM				
🗉 🧰 Drivers		20.flows	15 KB	FLOWS File	9/22/2010 10:21 AM				
😑 🧰 flows		21.flows	14 KB	FLOWS File	9/22/2010 10:22 AM				
E 🛅 2010		22.flows	14 KB	FLOWS File	9/22/2010 10:23 AM				
🖂 🧰 09		23.flows	14 KB	FLOWS File	9/22/2010 10:24 AM				
🗉 🛅 22		24.flows	15 KB	FLOWS File	9/22/2010 10:25 AM				
Cia 09		25.flows	14 KB	FLOWS File	9/22/2010 10:26 AM				
i 10		26.flows	14 KB	FLOWS File	9/22/2010 10:27 AM				
🗉 🧰 I386		27.flows	15 KB	FLOWS File	9/22/2010 10:28 AM				
🗉 🧰 MSOCache		28.flows	16 KB	FLOWS File	9/22/2010 10:29 AM				
표 🚞 oracle		29.flows	16 KB	FLOWS File	9/22/2010 10:30 AM				
표 🚞 Program Files		30.flows	15 KB	FLOWS File	9/22/2010 10:31 AM				
표 🛅 Radiatmp		31.flows	14 KB	FLOWS File	9/22/2010 10:32 AM				
🕀 🧰 TEMP		32.flows	13 KB	FLOWS File	9/22/2010 10:33 AM				
🗉 🚞 WINDOWS		33.flows.temp	8 KB	TEMP File	9/22/2010 10:33 AM				
🗉 🥝 DVD-RAM Drive (D:)									

For more information on nTop & nProbe, visit:

http://www.ntop.org/news.php