

created by: Rainer Bemsel - Version 1.0 - Dated: Mar/06/2005

Use Crannog's Netflow Tracker with PacketShaper

The purpose of this document is to describe the steps to install and configure PacketShaper to be used with Crannog's Netflow Tracker. PacketShaper is able to deliver Netflow-5 Packets to the Collector.

NetFlow Tracker is an extremely powerful new management tool from Crannog that provides a level of detail previously unavailable in any application of its type. Using Cisco's NetFlow technology (which is embedded in IOS in almost all routers and chassis based switches).

You can download a trail version of Crannog's Netflow Tracker at www.crannog-software.com

NetFlow Tracker 1.0.3a requires a minimum Java Version of 1.4.2_04, which is proofed by Installation Routine.

InstallShield Wizard
NetFlow Tracker requires that the following requirements be installed on your computer prior to installing this application. Click OK to begin installing these requirements:
Status Requirement
Pending Java(IM) 2 Huntime Environment, Standard Edition 1.4.2_04
<u> </u>

It will start to install Java first, before continuing Netflow Installation



When done with Java Installation. Netflow Tracker Installation will continueNetflow Tracker Installation will continue



Just follow the steps through the installation.

R NetFlow Tracker - Insta	hllShield Wizard 🛛 🛛 🛛	양 NetFlow Tracker - InstallShield Wizard 🛛 🛛 🔀
	Welcome to the InstallShield Wizard for NetFlow Tracker	License Agreement Please read the following license agreement carefully.
	The InstallShield(R) Wizard will instal NetFlow Tracker on your computer. To continue, click Next.	END USER SUBLICENSE AGREEMENT
	WARNING: This program is protected by copyright law and international treaties.	This is a legal agreement between you, the END USER, and CRANNOG. BY INSTALLING AND/OR RUNNING THIS SOFTWARE, YOU ARE AGREEING TO BE BOUND BY THE TERMS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, PROMPTLY RETURN THE UNOPENED DISK PACKAGE AND THE ACCOMPANYING ITEMS (INCLUDING MANUALS) TO A CRAINNOG REPRESENTATIVE FOR REFUND © I gcopt the terms in the konse agreement] do not accept the terms in the konse agreement] do not accept the terms in the konse agreement
	< gack Mest > Cancel	< gack Mext > Cancel

🔞 NetFlow Tracker - InstallShield Wizard	🔀 😼 NetFlow Tracker - InstallShield Wizard	
Customer Information Please enter your information.	Setup Type Choose the setup type that best suits your needs.	44
Ljser Name: Rainer Bensel Grganization: Evaluation	Please select a setup type. Complete All program features will be installed. (Requires the most space.)	t disk
Install this application for:	Coustom Choose which program features you want installed and will be installed. Recommended for advanced users.	where they
Install/held	Cancel Installiheid Sack Mest >	Cancel













Run Netflow Tracker by Start - Programs - NetFlow Tracker - NetFlow Tracker

	🛅 NetFlow Tracker 🛛 🔸	0	NetFlow Tracker
Programs	¥	7	User's Guide

A Webbrowser will open and connect to local host. First thing to do is verifying the License, by clicking on **SETTINGS**



	Settings
R	Licensing Examine or change your NetFlow Tracker licence
K	Listener Ports Set up the UDP ports on which the software will listen for NetFlow exports
c,	SNMP Settings Set up the community strings used to scan new devices and the retry policy
	Device Settings Rename or delete a device and edit the properties of its interfaces
	Security Settings Enable or disable password protection and edit user accounts
C	Report Settings Configure the default values used for reports
3	IP Application Names Assign names to the TCP and UDP ports appearing in reports
6	DiffServ Names Assign names to the DiffServ codepoints appearing in reports
1	Hostname Resolution Settings Configure the size of the DNS hostname cache and how long entries remain valid
	AS Names Assign names to the AS numbers appearing in reports
	Database Settings Configure options affecting database performance and the amount of storage space used
-	Memory Settings Control the amount of memory used by the software
2	Performance Counters See the amount of data the software has processed and the number of errors it has handled







DOD CompTIA.



Netflow Tracker & PacketShaper page 4 of 8

If this is a brand new installation, you will have a license for 24 hours included. I received a temp. License for a couple days, to evaluate Netflow-5 collector. This was provided in an email attachment. All to do is to load the file into licensing.

	Lice	nsing	
Current Licence			
Licensed User: Licensed Company: Expires:	3/7/05 12:22 PM		
Upload a New Licen	ce .		
	Browse	Load	
Paste in a New Lice	nce		
		95 - 110	
		Decode	
			Ok Cancel

To upload the license, just browse to the directory and file and click on LOAD

	Lice	nsing	
Current Licence			
Licensed User: Licensed Company: Expires:	Evaluation Key Only Besmel 3/17/05 11:39 AM		
Upload a New Licenc	e		
Dortalia a Mary Lizara	Browse	Loau	
		Decode	
There are unsaved cha	anges. Press Ok to con	firm them.	
			 Ok Cancel

The software must listen for NetFlow exports on at least one UDP port. You may wish to change this or have the software listen to more than one port. It is most efficient to use one port for each export-sending device. You may also wish to specify an address along with each port if the server has more than one.

The software must listen for NetFlo oftware listen to more than one po	w exports on at least one UDP port. You may wish to cha rt. It is most efficient to use one port for each export-sen	nge this or have the
ou may also wish to specify an au	dress along with each port if the server has more than on	e.
All local addresses 💽 : 988	18 📮 Add	
0.0.0.0:9888	Remove	
	×	

You can use almost any unused port. This will be the port, PAcketShaper will configured as well.



Also SNMP Setting has to be verified or set properly

When a device sends NetFlow exports to the software it must be scanned to get the names and speeds of its interfaces. You must give at least one community string to be tried on each newly-encountered device. Since the communities are tried in the order they are set here the speed of a scan can be affected by changing the order. A device is scanned again if it reboots or if the software is restarted.

Vhen a device sen nterfaces. Vou mu: communities are tr A device is scanne o rescan an existi	Is NetFlo st give at ied in the d again if ng device	w exports to t least one cor order they ar fit reboots or on the <u>devic</u>	he software it n nmunity string t e set here the s if the software i <u>e configuration</u>	nust be scanned to be tried on ea speed of a scan s restarted. You page.	I to get the na ch newly-enc can be affecte can change 1	ames and spe countered dev ed by changin the communit	eds of its ice. Since th g the order. y string used
		Add					
public	^	Remove					
	Ξ.	Up					
	~	Down					

Next, connect to your PAcketShaper and click on SETUP Tab

PacketShaper Xpress®	
top ten monitor manage report setup info feedback packetguide	
Unit: 025-10015236 Discovery: On Shaping: Off Compression: On	
	^
PACKETSHAPER INFO	
register > support site >	
Product: PacketShaper® 2500	
IP Address:	
Serial Number: 025 10015250	
Software Version: 7.1.0g1	
Shaping: Off	
Traffic Discovery: On	
Adaptive Response: 🛱 🔲 🚽 🔲 💻 📟 🔤 🖉 🔤 Settings	
Upper_Inside Interface Status: 🔔 Down	
Upper_Outside Interface Status: Δ Down	
access level utilities	
logout file browser >	
Access Level: Touch quick commands >	







DOD CompTIA.



All you do is to tell the PacketShaper the IP Address of the Netflow-5 Collector and the Port, he listens to.

-		very. On	Snaping: Off Co	Juli essio		
Choose Set	up Page: flow de flow detail recor	tail records rd settings form				
	Collector IP	Port	Record Type	Enabled	Ŕ	
Collector 1	Collector IP	Port 9888	Record Type	Enabled	l Clear	
Collector 1 Collector 2	Collector IP	Port 9888	Record Type	Enabled	l Clear Clear	
Collector 1 Collector 2 Collector 3	Collector IP	Port 9888	Record Type NetFlow-5	Enabled	clear clear clear	

Remember the Port? I configured this Port a few pages earlier. Don't forget to click on APPLY CHANGES

Now wait a few minutes and go back to Crannog's Netflow Collector. Under Devices, you should see a new entry of the PacketShaper, already sent a few packets with Netflow Data.

De	vice Settings			
o edit its properties or th	ose of its interfaces.			
Address				
192.168.10.152				
		Ok	Refresh	Cancel
	De o edit its properties or tho Address 192.168.10.152	Device Settings o edit its properties or those of its interfaces. Address 192.168.10.152	Device Settings o edit its properties or those of its interfaces. Address 192.168.10.152 Ok	Device Settings o edit its properties or those of its interfaces. Address 192.168.10.152 Ok Refresh

When you click on the Device Name, you'll get some basic information, regarding SNMP Settings.

	Device HomeSnaper (192.	168.10.152)					
By default all devices are SNMP devices. It is highly recommended that you enable SNMP on your device, and allow the monitor to query It. However, if this is not possible, you can change the SNMP Settings so that the device does not use SNMP. This means the device will create an interface for each ifIndex that it encounters, but you will have to manually set the name, speed, etc. You can also choose to keep the current settings, which mean that no further interfaces will be created, nor will the device create more interfaces if it encounters an unknown ifindex. With any of these options, you can still manually scan the device using the button on this page.							
Device Name: HomeShaper							
SNMP Mode: Use SNMP	~						
SNMP Version: SNMPv1 💌							
SNMP Community: public							
Interface	Description	Inward Speed (bps)	Outward Speed (bps)	Hidden			
Inside (ethernetCsmacd)		10000000	10000000				
Outside (ethernetCsmacd)		10000000	10000000				
Upper_Inside (ethernetCsmacd)		10000000	10000000				
Upper_Outside (ethernetCsmacd)		10000000	10000000				
			Ok Delete	Rescan			









Next, go back to the HOME page and click on DEVICES....



... and Device Name, where you can see the first stats, provided by Netflow-5 Data

Interfaces on HomeShaper (192.168.10.152)								
Timerange: Mar 6, 2005, 7:36 AM - 1:36 PM Source Device: HomeShaper (192.168.10.152)								
Interface 🛆	Description	% Utilisation	Peak Traffic In	Peak Traffic Out	Rel. Traffic	Peak Packets In	Peak Packets Out	Rel. Packets
Inside	connected to the LAN		1.5 kbps	23.49 kbps	1	2.14 /s	3.11 /s	
Outside	connected to the WAN		23.49 kbps	1.5 kbps		3.11 /s	2.14 /s	
<u>Upper Inside</u>	unused		0 bps	0 bps		0 /s	0 /s	
Upper Outside	unused		0 bps	0 bps		0 /s	0 /s	

Now, it's the time to wait a few hours and dig deeper into the possibilities of gaining information out of the data.

		Inside (ethern	etCsmacd) on Hom	eShaper (192.1	68.10.152)			
Timeran Source D Interface Speed:	ge: M Device: H e: <u>Ir</u> 11	ar 6, 2005, 11:49 . omeShaper (192.1 <u>iside</u> DO Mbps	AM - 5:49 PM 68.10.152)			୷ୡୣୣ		
Interface	e - % Utilisa	ation Traffic Rate	Packet Rate		*	**		
800 kbp: 600 kbp: 400 kbp: 200 kbp: 0 bp:	5	::30 PM	3: 20 PM Mar 6, 200 2:00 PM	<mark>3:22 РМ</mark> 15 1		<mark>ი</mark> ლესილესილე ე PM		
	Dir.	Peak			Average			
	In 51.74 kbps between 1:54 PM and 1:56 PM				2.26 kbps (5.)	2.26 kbps (5.81 MB)		
	Out	680.32 kbps bet	ween 3:20 PM and 3	3:22 PM	17.14 kbps (4	4.13 MB)		

What you also can do is highlight a range, do a right click on mouse and choose from different views.



Netflow Tracker & PacketShaper page 8 of 8

							Source Addresses
							Destination Addresses
							Address Pairs
							Protocols
ncido (othornotCer	acd) on HomoShar	oor (192 168 10	152) Crannon Sr	ftwaro NotElo	w Trackor Mo		Source Ports
Talla (admannades)	naed) on nomeenal	per (172,100,10,	(JZ) - Claimog St	ntwale Neth to	w Tracker - Mo		Destination Ports
Fait Alem Po	Bookmarks Loois H	eip					Source Applications
I • 🖒 • 🔁 🖗	3 😭 🗋 http://k	ocalhost/report.jsp?te	mplid=_if&length=216	00000&device 🔽	🔘 Go 💽		Destination Applications
Contraction Links D. Co.	and Dimed	walateles 🕞 ur	alassa ana dia 👘 mara		10.150.0-		Source Endpoints
	ee Hotmail 🔄 windows	s Marketplace 🛄 Wir	idows Media 🛄 Wind	10WS 🔲 192.168	3.10.152: Pa	"	Destination Endpoints
	Incida (athor	not(cmacd) on l	JomoShanor (10	2 160 10 15	2)		Server-Client Sessions
limerange:	Mar 6, 2005, 11:51	AM - 5:51 PM			-1	2.00	Client-Server Sessions
Source Device:	IomeShaper (192.	168.10.152)				Haa	Conversations
Interface: I Sneed	<u>nside</u> .00 Mbns						Types of Service
Interface - % Utili	ation Traffic Rate	Packet Rate			*	**	Differentiated Services
	11				1 Marcana (Carlos		Source ASs
800 kbps	9						Destination ASs
so a secolar a			· n ·				AS Pairs
600 kbps							Source Networks
1							Destination Networks
400 kbps				4 :	38 PM - 5:51 PM		Network Pairs
200 kbps		0		1010	10,2003		In Interfaces
200 1005					п	Select All	OutInterfaces
0 bps		مالے مالہ جامہ		٦٩		Zoom In	Next Hops
1:	2:30 PM	2:00 PM	3:30 F	°M	5:00 PM	Zoom Out	Source Address Dissemination
Dir.	Peak			Avera	ige	in 🕨	Destination Address Popularity
In	51.74 kbps bet	ween 1:54 PM an	d 1:56 PM	2.26	kbps (5.81 MB)	Out 🕨	
Out	680.32 kbps be	tween 3:20 PM a	nd 3:22 PM	17.1	.4 kbps (44.13 N		
et grapplet started						1.1	



This is just one example you can use. I hope this has give a quick impression on what's possible.

