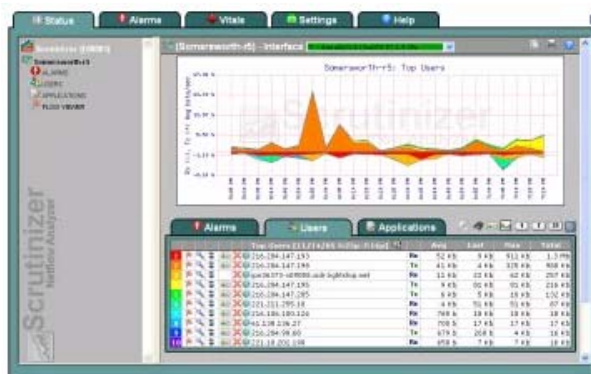




The purpose of this document is to provide you with some basic steps to install Scrutinizer Netflow collector with the use of PacketShaper providing Netflow-5 Data.

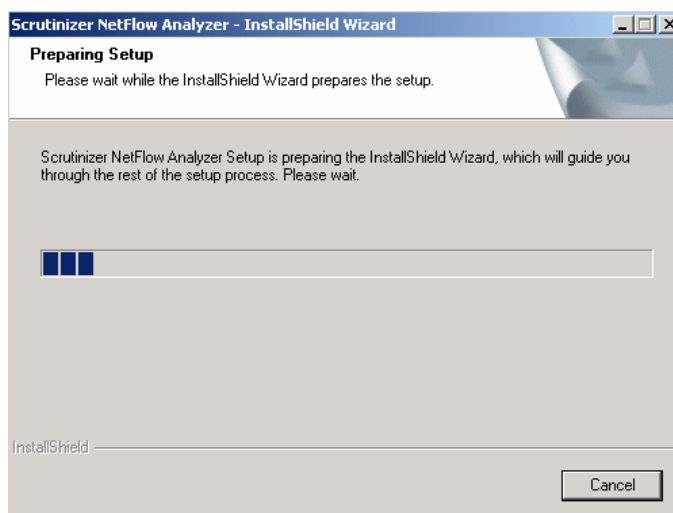
Netflow is the name of an open (but proprietary) Cisco protocol for collecting IP traffic information. Devices with netflow enabled generate netflow records, which are exported from the device in UDP packets and collected using a netflow collector.

A network flow is defined as a unidirectional sequence of packets between given source and destination endpoints. Flow endpoints are identified both by IP address as well as by transport layer application port numbers. The router will only output a flow record when it determines that the flow is finished - it does this by flow aging; when the router sees new traffic for an existing flow it resets the aging counter. The flow record contains a version number, a sequence number, the IP address of the interface upon which the flow was observed, timestamps for the flow start and finish time, the volume of traffic in the flow, and its source & destination IP addresses and source and destination port numbers. By analyzing flow data, one can build a picture of traffic flow and traffic volume in a network.



You can download the software from www.plixer.com. The installation is pretty straight forward and once the PacketShaper is configured to provide netflow-data, Scrutinizer will recognize the data and add it to the list.

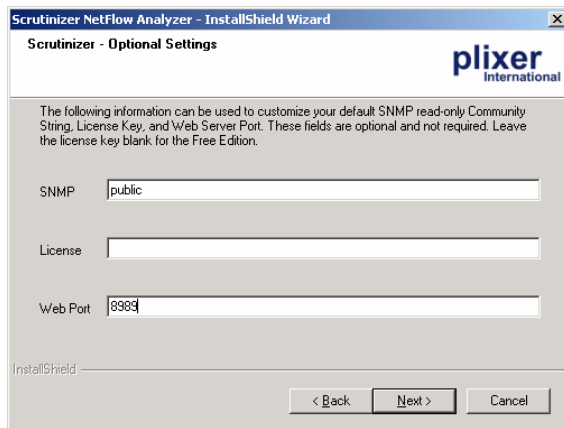
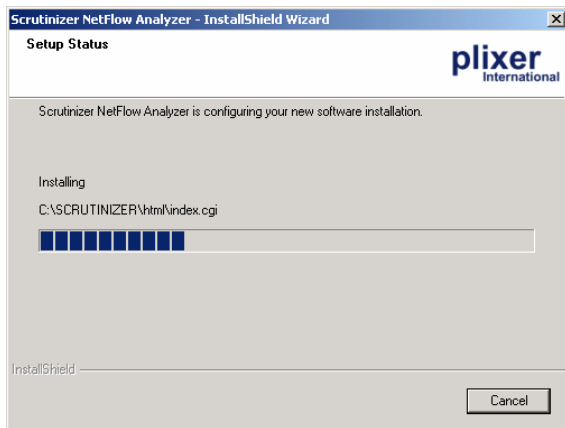
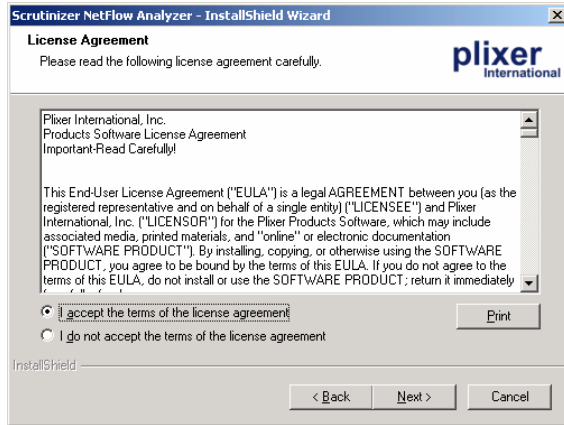
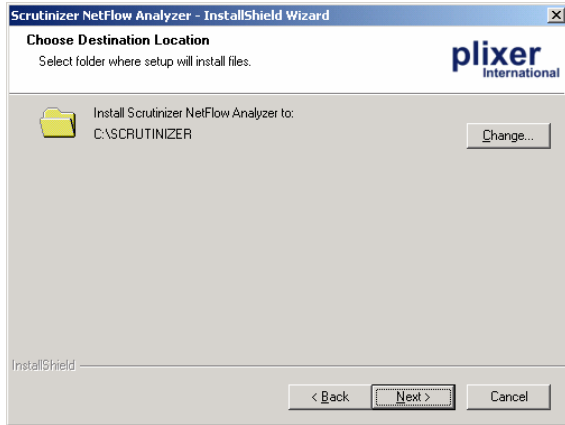
Start the executable file and Install Wizard will open



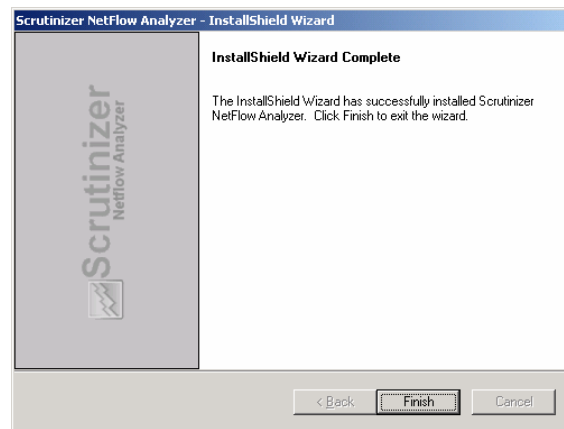
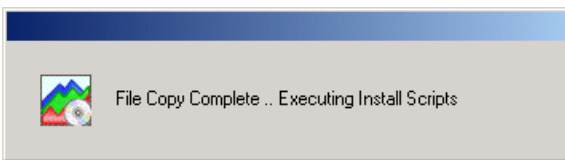
DISCLAIMER

This Technical Tip or TechNote is provided as information only. I cannot make any guarantee, either explicit or implied, as to its accuracy to specific system installations / configurations. Readers should consult each Vendor for further information or support.

Although I believe the information provided in this document to be accurate at the time of writing, I reserve the right to modify, update, retract or otherwise change the information contained within for any reason and without notice. This technote has been created after studying the material and / or practical evolution by myself. All liability for use of the information presented here remains with the user.



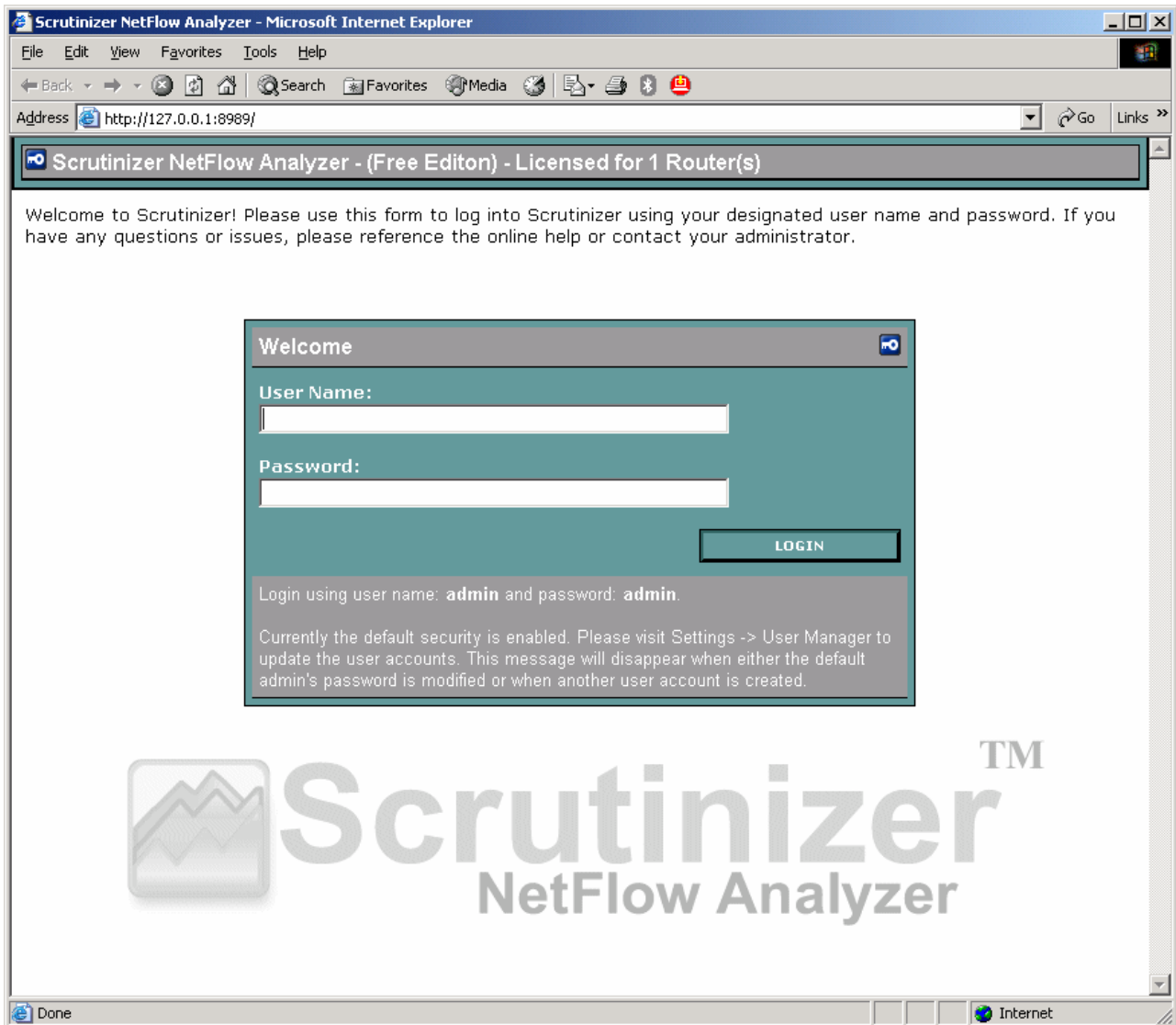
If you don't use default Web Port of 80 or SNMP community of public, in the Optional Settings, you can change the values. Because I already have a Web Server running on Port 80, I've chosen 8989.



That's pretty much the installation itself.



First time logon, will ask for a User Name and Password. Both are default **admin**



It will get you to the Settings page, where you can add an activation key.

When new netflows from the devices are detected, they are automatically added to this view.

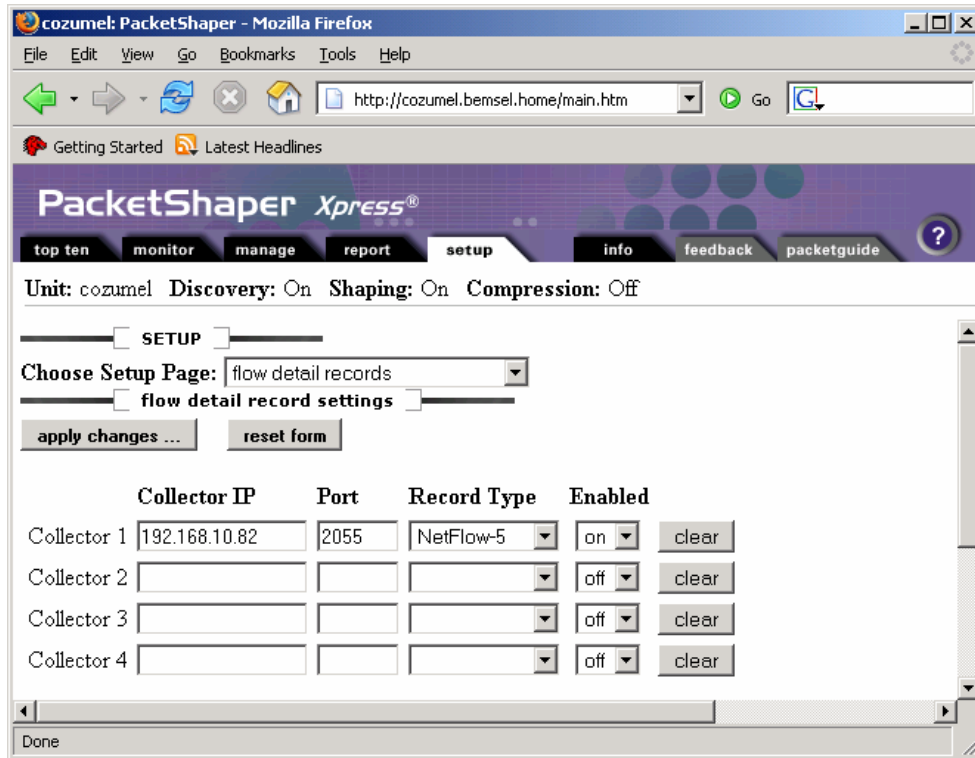
Router	Interface	Port Speed			
		Outbound	Inbound	UpTime	Port Speed
1 cozumel.bemsel.home	Upper_Inside			2h 43m 39s	100.0 Mb
2 cozumel.bemsel.home	Upper_Outside			2h 43m 39s	100.0 Mb
3 cozumel.bemsel.home	Inside			2h 43m 39s	100.0 Mb
4 cozumel.bemsel.home	Outside			2h 43m 39s	100.0 Mb

COZUMEL.BEMSEL.HOME is the DNS name of my PacketShaper and it is equipped with an additional LEM.

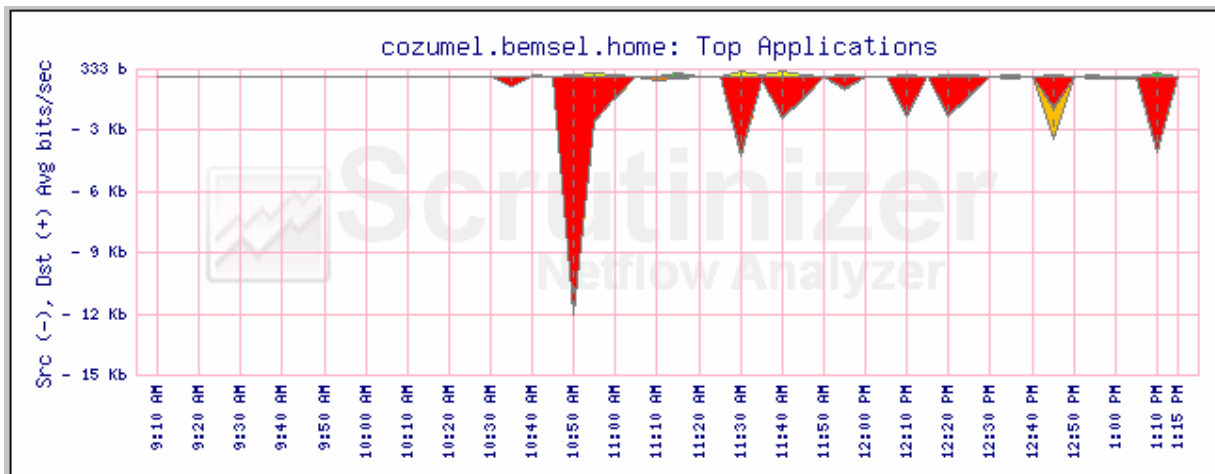


But before you will see any of those flows, you have to configure the PacketShaper to deliver Netflow-5 Data.

Connect to PacketShaper, click on SETUP Tab and choose FLOW DETAIL RECORDS page. Netflow will send packets by default on port 2055/UDP to the collector. In this example, Scrutinizer is installed on IP 192.168.10.82.



Wait a couple of minutes and see incoming packets



A quick overview of applications

			Top Applications [last 24 hrs]		Avg	Last	Max	Total
1		✗	http (TCP 80)	Dst	5 Kb	5 b	623 Kb	1.6 Mb
2		✗	http (TCP 80)	Src	5 Kb	6 b	623 Kb	1.6 Mb
3		✗	snmp (UDP 161)	Dst	22 b	0 b	273 b	6 Kb
4		✗	snmp (UDP 161)	Src	22 b	24 b	273 b	6 Kb
5		✗	DNS (UDP 53)	Src	9 b	11 b	267 b	3 Kb
6		✗	DNS (UDP 53)	Dst	9 b	0 b	267 b	3 Kb
7		✗	https (TCP 443)	Dst	3 b	91 b	127 b	898 b
8		✗	https (TCP 443)	Src	3 b	111 b	127 b	898 b
9		✗	netbios-dgm (UDP 138)	Dst	2 b	12 b	104 b	484 b
10		✗	netbios-dgm (UDP 138)	Src	2 b	0 b	104 b	484 b

As well as a quick overview of users, meaning hosts.

			Top Users [last 24 hrs]		Avg	Last	Max	Total
1		✗	192.168.10.234	Dst	5 Kb	16 b	623 Kb	1.3 Mb
2		✗	207.234.147.42	Src	4 Kb	621 Kb	621 Kb	1.2 Mb
3		✗	192.168.10.82	Dst	626 b	82 b	68 Kb	180 Kb
4		✗	63.123.36.80	Src	282 b	41 Kb	41 Kb	81 Kb
5		✗	63.123.36.89	Src	249 b	18 Kb	18 Kb	72 Kb
6		✗	192.168.10.234	Src	141 b	8 b	12 Kb	41 Kb
7		✗	207.234.147.42	Dst	80 b	12 Kb	12 Kb	23 Kb
8		✗	209.249.116.139	Src	64 b	2 Kb	7 Kb	19 Kb
9		✗	198.133.219.25	Src	57 b	8 Kb	8 Kb	16 Kb
10		✗	192.168.10.82	Src	36 b	105 b	2 Kb	10 Kb

An good feature in Scrutinizer is FLOGGING, telling you who has communicated with whom an on what service.

Date	Source	Destination	Int	Application	Bytes
11/30/05 19:00	192.168.10.233	66.135.200.141	2	TCP > https	2038
11/30/05 19:00	192.168.10.233	66.135.200.141	2	TCP > https	2038
11/30/05 19:00	192.168.10.233	192.168.10.255	3	UDP > netbi	936
11/30/05 19:00	192.168.10.233	66.135.200.141	2	TCP > https	3464
11/30/05 19:00	192.168.10.233	66.135.200.141	2	TCP > https	848

I like this tool a lot. It was easy to install and less complicated to use. Just give it a try.

