NetFlow on the ASA

Why the Reports Look Strange

Nov 18th, 2009
www.plixer.com
Scrutinizer Supports Flexible NetFlow

If you click here, a trend for the last 24 hours will appear using all flows from all templates that include the data necessary for the selected report.

If you click on Graph, you get the most recent 1 hour of flows in a trend for this template.
Bidirectional Flows

Bidirectional flows means that returning bytes from 74.125.113.132 are added to the same flow. In traditional NetFlow, a 2nd flow should have been created on interface 2 going back to 10.1.7.8 and appear in the Outbound table.

Adding what should be two flows together in one flow can be confusing to a person used to looking at conventional NetFlow.
No Active Timeout

No active timeout for long lived flows means that they are exported when they are torn down. This causes spikes in the trends of many reporting tools and results in under stated prior intervals.
Apparently “Flow Creation” templates only include startup bytes. “Teardown” templates include all flow bytes and include the bytes in “Flow Creation”. This can cause a slight duplication of data when reporting using multiple templates.
Using All Templates vs. just the Teardown template shows a considerable discrepancy. Notice below that something is over stating or understating.
These are flows that were denied. Notice that this appears to be a lot of traffic for denied flows.
We provide a text interface to the NSEL events so you can see Flows that do not have octetTotalCount in them. We provide this view for any Netflow Template we receive via our Flow View interface.

Problem 1, ACL names: An option template with ACL name is necessary to provide the information your (i.e. our) customers are looking for. As it is we can only provide numbers.

Problem 2, Extended event descriptions: These extended event codes are in the 1000 range so we can translate per Cisco’s documentation. If the extended event codes are in the 2000 range we can only display the number because the docs do not provide definitions.

If the extended event codes are static across devices, documentation would suffice. If these numbers mean different things on different devices, an option template is required to provide useful data to our customers.
NetFlow ASA and Scrutinizer

- Bidirectional flows are unique and require a different understanding as inbound includes some outbound traffic and vice versa.
- The template architecture is exciting but, different: Creation Flows, Teardown Flows, etc. contain duplicate entries and often result in inaccurate reports when combined in Scrutinizer.
- No active timeout for long lived connections causes spikes in the trend (i.e. large TCP downloads).
- No ToS field being exported
- No TCP flags being exported
- No ACL Names
- No Extended Event Descriptions
- Interface instances do not match up with the SNMP instances causing problems in the reporting interface.
Many Cisco ASA customers are excited about the ability to collect NetFlow.

Most NetFlow Reporting tools like Scrutinizer are seeing the same odd patterns with the ASA.

Cisco is aware of the differences we pointed out in this presentation and is very receptive to suggestions.

Please contact Plixer and/or Cisco if you have any questions.