سیسکو به پارسی

آشنایی با NetFlow

نوشته:

شفق زندی

سایت سیسکو به پارسی http://blog.shafagh.com/persian

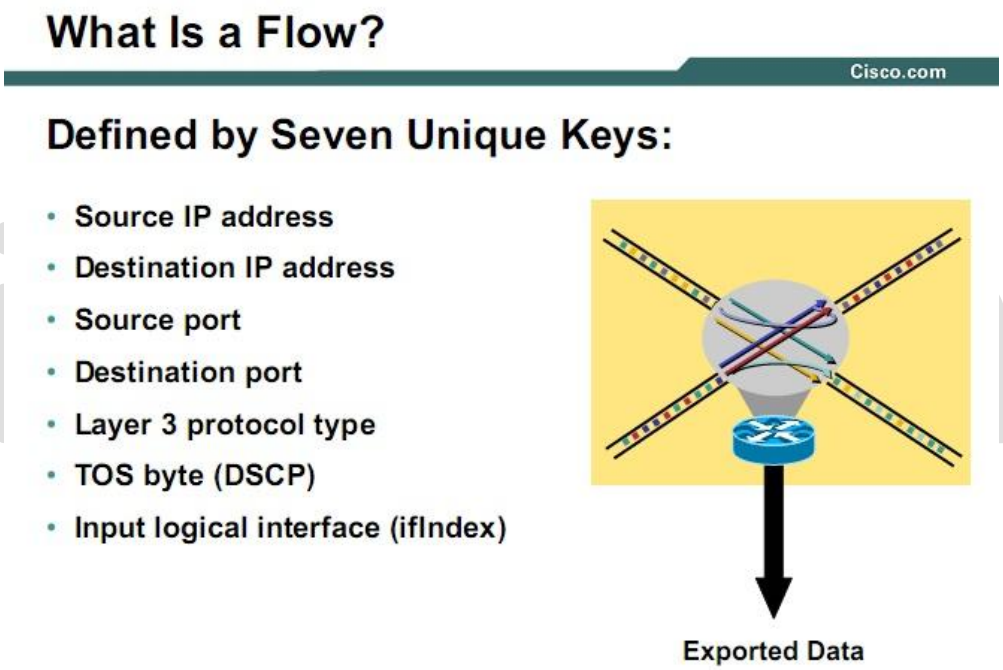
انجمن سیسکو به پارسی http://forum.shafagh.com

NetFlow

پروتکل NetFlow در سال ۱۹۹۶ توسط دو مهندس سیسکو بنامهای Darren Kerr و Barry Bruins ایجاد شد. یک پروتکل مدیریتی که اطلاعات Flow هایی که از روتر یا سوییچ عبور میکنند را به سرور ارسال میکند. بدین صورت میتوان از Flow ها و ترافیک در حال عبور مطلع شد و آنها را مانیتور (نظارت) کرد.

NetFlow به پنج سوال رایج در ترافیک شبکه پاسخ میدهد: کی، چه، کجا، چه زمانی و چطور یک بسته منتقل شده است.

Who, What, When, Where and How?



چه فرستنده ای به کدام گیرنده در زمان مشخص چه دیتایی را در چه حجمی ارسال میکند.

- Source IP address
- Destination IP address
- Source port for UDP or TCP, 0 for other protocols
- Destination port for UDP or TCP, type and code for ICMP, or 0 for other protocols
- IP protocol
- Ingress interface
- IP Type of Service

از این پروتکل در سرویس دهنده ها و Backbone های اینترنت جهت Accounting براساس ترافیک IP (Peering Arrangement) استفاده میشود. بر این اساس Backbone ها میتوانند ترافیک مورد Exchange خود با یکدیگر را حساب کنند. از دیگر موارد استفاده آن Network Planning و بررسی منابع مورد نیاز شبکه است.

از مصارف جدیدتر NetFlow، NBA یا Network Behavior Analysis است که در امنیت شبکه و برای تشخیص حملات و Denial of Service – DOS مورد استفاده قرار میگیرد.

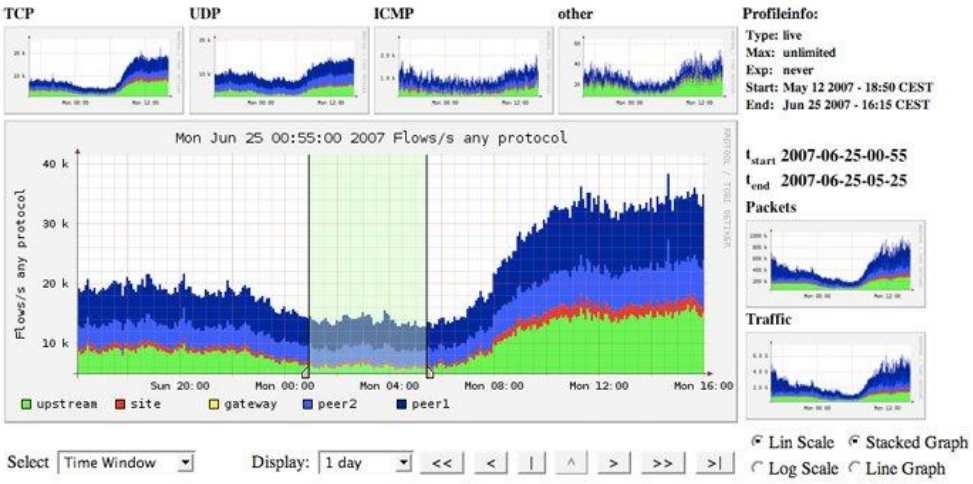
اطلاعات جمع آوری شده در زمان های مشخصی توسط UDP به سرور NetFlow Collector ارسال میگردد. عموما ۲۰ تا ۵۰ Flow در هر بسته گزارش، گنجانده میشود روی اکثر روتر های سیسکو و سوییچ های ۶۵۰۰ و ۴۵۰۰ پشتیبانی شده و جدیدا در نسخه ۸.۲ سیستم عامل ASA روی فایروال نیز گنجانده شده است که به آن NSEL یا NetFlow Security Event Logging گفته میشود و برای ارسال Flow ها به CS-MARS در نظر گرفته شده است.

آخرین نسخه NetFlow v9 است که اجازه تعریف اطلاعات ارسالی را بصورت Template به فرستنده و گیرنده میدهد. مثل MPLS و IPv6. همچنین IETF نسخه ای بنام IPFIX را که Version 10 آن اطلاق میشود براساس v9 استاندارد کرده است.RFC5101, RFC5102

Cisco in Persian

از NetFlow تولیدکنندگان دیگر شبکه نظیر جونیپر ، HP و Brocade تحت عنوان sFlow استفاده میکنند. (استاندارد و Open Source)

برنامه های Collector متعددی برای NetFlow وجود دارد که قابلیت های زیاد و متنوعی را ارائه میکنند.



بطور مثال در Scrutinizer میتوان کاربر تعریف کرد و براساس هر کاربر سطح دسترسی مشخص کرد. نسخه رایگان آن را از وب سایت Plixer میتوان Download کرد. که البته نسخه حرفه ای آن رایگان نیست:

http://www.plixer.com/products/scrutinizer.php

نحوه تنظیم NetFlow

```
Router#configure terminal
Router(config)#interface FastEthernet 0/1
Router(config-if)#ip route-cache flow
Router(config-if)#exit
Router(config)#ip flow-export destination 192.168.0.101 9996
Router(config)#ip flow-export source FastEthernet 0/1
Router(config)#ip flow-export version 5
Router(config)#ip flow-cache timeout active 1
Router(config)#ip flow-cache timeout inactive 15
Router(config)#snmp-server ifindex persist
```

```
Router#show ip flow export

Router#show ip cache flow
```

Cisco in Persian

از دیگر برنامه های Collector :

- Adventnet Netflow analyzer
- Solarwinds
- Linux, FlowScan – http://net.doit.wisc.edu/~plonka/FlowScan
- Netscout
- Fluke Netflow Tracker
  http://www.flukenetworks.com/fnet/en-us/products/NetFlow+Tracker

همچنین:

http://www.switch.ch/tf-tant/floma/software.html

http://www.networkuptime.com/tools/netflow