DBNS Offline Report

Report Overview

DBNS Overview

Data-Based Network Security system, (aka DBNS) is a network security system composed of latest opensource big data components. Within the architecture building and efficiency optimization, the DBNS system can afford various methods to analysis 1GBPS network flow within a single node server, and up to 10GBPS network flow within a three-node server cluster.

DBNS Home:https://github.com/ShengjieLuo/DBNS/

DBNS Document:http://dbnsdoc.readthedocs.io/en/latest

DBNS system is developed by Network Computing Center of Department of Computer Science and Engineering, Shanghai Jiao Tong University. You can contact luoshengjie@sjtu.edu.cn for more information.

Offline Report Overview

The offline report is built for user of DBNS and established each day. The report is composed of two parts, monitor part and probe part. The monitor serverd as netflow monitor, and the probe serverd as hazard detection. The report information:

Build Time: 2017-02-20 23:43

Component: Monitor & Probe

DBNS Version: 0.2.0

DBNS Framework: spark-based

DBNS Master: 172.16.0.104

DBNS Slaves: 172.16.0.59 172.16.0.68

DBNS Component:

DBNS Message Forwarding Component: kafka

DBNS Streaming Computation Component: spark-streaming

DBNS Online Computation Component: Python on mySQL

DBNS Offline Computation Component: Hive on Spark

DBNS Metadata Store Component: mysql::DBNS::metadata

DBNS Tempdata Store Component: mysql::web

DBNS Basic Data Store Component: HDFS

DBNS Distribution:

Streaming Task Cores: 48

Online Analysis Cores: 1

Offline Analysis Cores: 10

Conclusion of Intellegent Maintain System

Monitor Report

Monitor Function is used to monitor the network flow from the backbone router. In this report, we would include four message resources,

- **DRQ**: DNS request package

- **DRS**: DNS response package
- **HRQ**: HTTP request package
- **HRS**: HTTP response package

DRQ report

Overall situation:

DNS request report is the package sent to the DNS server to query the IP address of the URL.

Total Number of the DRQ package:{Monitor::DRQ::number}

Who send the DRQ package?

{Monitor::DRQ::table1} {Monitor::DRQ::table2} {Monitor::DRQ::image1} {Monitor::DRQ::image2}

Who receive the DRQ package?

{Monitor::DRQ::table3} {Monitor::DRQ::table4} {Monitor::DRQ::image3} {Monitor::DRQ::image4}

DRS report

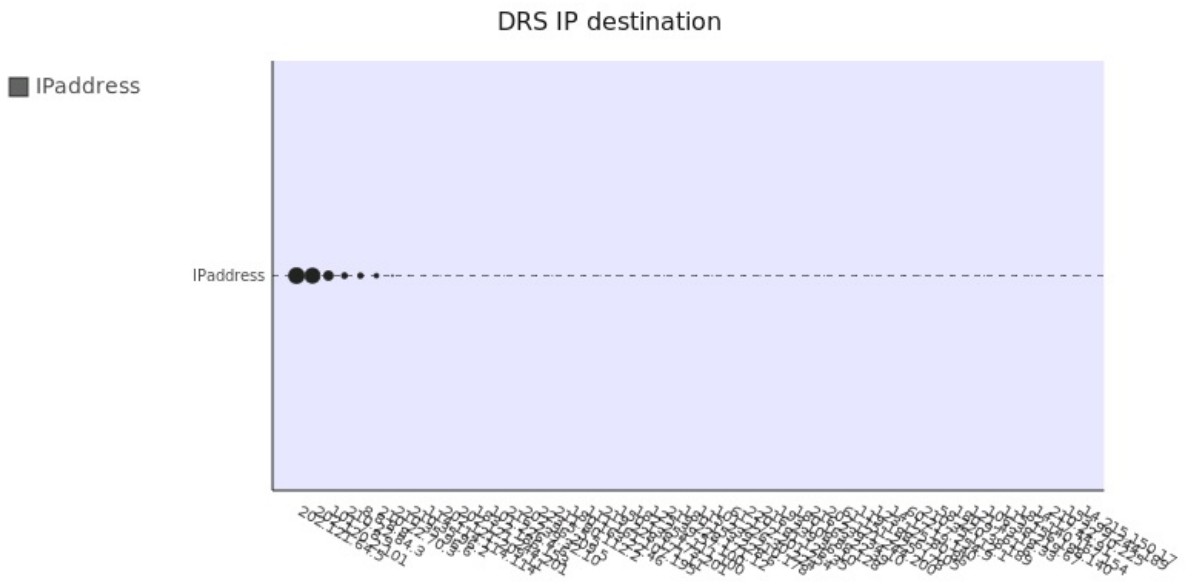
Overall situation:

DNS response report is the package reponsed by the DNS server. DNS server would inform the IP address to the server who sent the DNS query request.

Total Number of the DRS package:{Monitor::DRS::number}

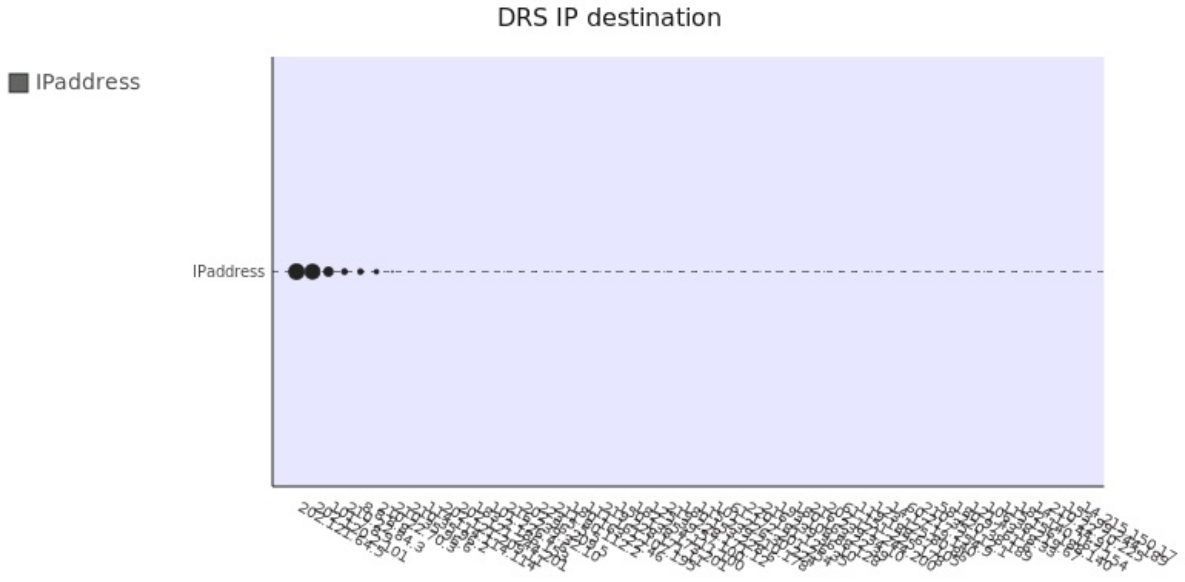
Who send the DRS package?

	First Occurred Time	IPaddress	Frequency
1	1480868217	202.121.64.5	79656
2	1480868226	192.168.2.116	55667
3	1480867249	210.35.96.6	48998
4	1480868217	202.121.209.11	46905
5	1480868217	210.35.96.2	39358
6	1480867249	202.121.64.7	33154
7	1480868218	192.168.2.215	18028
8	1480867249	202.121.64.130	17444
9	1480868221	192.168.2.223	7519
10	1480868055	202.121.223.29	5855



Who receive the DRS package?

	First Occurred Time	IPaddress	Frequency
1	1480867249	202.121.64.5	87862
2	1480867249	202.120.2.101	84712
3	1480868217	101.7.8.9	52793
4	1480867249	210.22.84.3	32207
5	1480867249	8.8.8.8	30123
6	1480867249	210.22.70.3	24833
7	1480868218	210.35.96.6	7357
8	1480868217	210.35.96.2	3454
9	1480868218	114.114.114.114	2188
10	1480868285	202.121.209.11	2149



HRQ report

Overall situation:

Http request package is one of the most popular package type in Network. For example, if you want to get a net page from www.baidu.com, you would send a HTTP request to the baidu server to fetch the net page.

Total Number of the DRQ package:{Monitor::HRQ::number}

Who send the HRQ package?

{Monitor::HRQ::table1} {Monitor::HRQ::table2} {Monitor::HRQ::image1} {Monitor::DRS::image2}

Who receive the HRQ package?

{Monitor::DRS::table3} {Monitor::DRS::table4} {Monitor::DRS::image3} {Monitor::DRS::image4}

HRS report

Overall situation:

HTTP response package is one of the most popular package type in Internet. For example, if you want to get a net page from www.baidu.com, then baidu server would send you a HTTP response package including the netpage you want.

Total Number of the DRQ package:{Monitor::HRS:number}

Who send the HRQ package?

{Monitor::HRQ::table1} {Monitor::HRQ::table2} {Monitor::HRQ::image1} {Monitor::DRS::image2}

Who receive the HRQ package?

{Monitor::DRS::table3} {Monitor::DRS::table4} {Monitor::DRS::image3} {Monitor::DRS::image4}

Probe Report