Abstract

Management of a network is a challenging task without accurate traffic statistics. Through this paper the security benefits of implementing a Netflow [1] based analysis system and then a novel open source application useful in Netflow analysis and management of flow records is proposed. Netflow data provides important information about network conversations and behavior. Netflow statistics are generated by Cisco and Juniper routers and switches, as well as server software Netflow probes. Netflow data provides enough information to serve the needs of several different applications such as billing, network planning and most importantly traffic engineering, which we specifically analyze to assess the state of the network. The flow records are UDP packets lacking payload data which still provides enough data to the network administrator to be a valuable analysis tool. Netflow profiling is a good moderation which strikes a balance between detail and summary and provides a real-time analysis of traffic flows, connection information and abnormal network behavior. Netflow data on the router is sampled at a variable rate which actually satisfies the conditions which have been set to monitor the incoming traffic, and then compared periodically to test if an incoming sequence is a DOS or a possible threat to the network by examining the packet sequences. Through this paper the performance of a network is gauged by using a parameter called unexpectedness [2], which is a method to gauge the amount of traffic flowing through a network.
Usage of Netflow in Security and Monitoring of Computer Networks

Refer

ences

- Cisco, Cisco IOS Net Flow Technology Data Sheet.

Index Terms

Computer Science

Computer Networks

Keywords

Netflow Cisco Packet Tracer GNS3 Virtual Box Virtual Router

Unexpectedness

Decoding Netflow Packets