

Preporuke za analizu mrežnog saobraćaja pomoću Netflow protokola

Dokument sadrži preporuke za pripremu (konfiguraciju) uređaja kao i metode koje se koriste prilikom prikupljanja Netflow podataka u cilju efikasnog uvida u strukturu i karakteristike mrežnog saobraćaja.

AMRES BPD no	104
Tematska grupa/Working group	Nadgledanje mreže/Network management
Kategorija dokumenta/Category	Preporuka/Recommendation
Naslov originala	Preporuke za analizu mrežnog saobraćaja pomoću Netflow protokola
Originalna verzija/datum	Revizija 1 (dokumenta od 14. oktobara 2011.)/ 3. april 2012.
Originalna verzija dokumenta na srpskom jeziku	PDF
Title	Recommendations for Network Traffic Analysis Using the NetFlow Protocol
Version/date	Revision 1 (of the document dated 14 October 2011)/ 3 April 2012
English version	PDF

Rezime

Cilj ovog dokumenta je da predstavi postupke koji se koriste za analizu saobraćaja u mreži, čime se postiže jasan uvid u strukturu saobraćaja i efikasno otkrivanje eventualnih problema i anomalija. Prvo su predstavljene tehnologije za analizu mrežnog saobraćaja, kao i njihove prednosti i mane. Zatim su detaljno obrađene preporuke za analizu mrežnog saobraćaja zasnovane na statistici prikupljenoj preko NetFlow protokola. Preporuke obuhvataju primere ispravnog konfigurisanja NetFlow protokola na mrežnim uređajima kao i primere indirektnog korišćenja NetFlow protokola u situacijama kada ga mrežni uređaji ne podržavaju. Dokument obuhvata i pregled korišćenja ICmyNet.Flow sistema za analizu NetFlow statistike, koji se koristi kao jedan od Network Management sistema ne samo u Akademskoj mreži Srbije već i u drugim NREN ovima.

Summary

This document presents the procedures used for network traffic analysis, which provide a clear overview of the structure of traffic and enable the efficient detection of potential problems and irregularities. The document first presents the technologies applied in network traffic analysis, including their advantages and shortcomings. It then turns to detailed recommendations for traffic analysis based on statistics obtained through the NetFlow protocol. The recommendations include examples of the correct configuration of the NetFlow protocol on network devices, as well as examples of the indirect implementation of the NetFlow protocol in situations where network

devices do not support it. The document also includes an overview of the implementation of the ICmyNet.Flow system for analysing the NetFlow statistics, which is used as a Network Management System in the Academic Network of Serbia and in other NRENs.

From:

<http://www.bpd.amres.ac.rs/> - AMRES wiki

Permanent link:

http://www.bpd.amres.ac.rs/doku.php?id=amres_cbp_wiki:amres_bpd_104

Last update: **2012/04/03 11:32**