Preporuke za analizu mrežnog saobra?aja pomo?u Netflow protokola

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

AMRES BPD no	104
Tematska grupa/Working group	Nadgledanje mreže/Network management
Kategorija dokumenta/Category	Preporuka/Recommendation
Naslov originala	Preporuke za analizu mrežnog saobra?aja pomo?u 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 saobra?aja u mreži, ?ime se postiže jasan uvid u strukturu saobra?aja i efikasno otkrivanje eventualnih problema i anomalija. Prvo su predstavljene tehnologije za analizu mrežnog saobra?aja, kao i njihove prednosti i mane. Zatim su detaljno obra?ene preporuke za analizu mrežnog saobra?aja zasnovanu na statistici prikupljenoj preko NetFlow protokola. Preporuke obuhvataju primere ispravnog konfigurisanja NetFlow protokola na mrežnim ure?ajima kao i primere indirektnog koriš?enja NetFlow protokola u situacijama kada ga mrežni ure?aji ne podržavaju. Dokument obuhvata i pregled koriš?enja ICmyNet.Flow sistema za analizu NetFlow statistike, koji se koristi kao jedan od Network Management sistema ne samo u Akademskoj mreži Srbije ve? 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.