INTISARI

RANCANGAN SISTEM OTOMATISASI *PACKET FILTERING* BERDASAR SINKRONISASI DATA PADA *IP PROFILE DATABASE* MENGGUNAKAN *PYTHON*

Tri Multy Rizkilina

17/410666/SV/12593

Lalu lintas data pada jaringan yang padat menjadi ancaman kejahatan dunia maya dan kerentanan yang tinggi bagi perusahaan teknologi sehingga tantangan untuk mencegahnya akan semakin beragam. Menambahkan penguatan dinding batas atau *firewall* menjadi salah satu alternatif melindungi lalu lintas yang dimiliki. Memilah data yang masuk untuk mencegah *malware* dan serangan dari luar ditingkat perangkat jaringan awamnya diatur secara manual dengan menuliskan *firewall rules* di metode *packet filtering*. Saat *traffic* padat, pintu masuk data tidak terkontrol karena pengecekan dilakukan sesekali saja. Maka penelitian ini akan membuat suatu rancangan untuk mempermudah pemilahan *packet* data yang masuk melalui seleksi berdasar *rules* yang ditentukan dan dapat berjalan secara *real-time* sehingga pencegahan kejahatan yang masuk dalam jaringan lebih sigap ditangani. Sistem berhasil berjalan dengan men-*subscribe* topik dari *IP Profile Database* melalui program MQTT *Collector* berbahasa *python* untuk mengambil data hasil *profiling*. Sistem diujicobakan pada *router* mikrotik RB951Ui-2HnD yang kemudian rekam jejak pemblokiran disimpan pada *database* di MongoDB. Hasil dari pengujian menunjukkan data hasil *profiling* yang berisi alamat IP terduga sumber *malware* dengan *average base score* diatas 20 terblokir kemudian disimpan pada *block list*. Pengecekan *collection* di *database* melalui program *blocking code* berjalan optimal pada pengaturan *delay* 30 detik. Selain itu, data pada *database* akan dicek setiap hari dalam kurun waktu 30 hari yang kemudian akan dikeluarkan dan tercatat pada *log release* di MongoDB.

Kata Kunci : *Packet Filltering, Firewall Rules, Python, Router Mikrotik.*

ABSTRACT

PACKET FILTERING AUTOMATION SYSTEM DESIGN BASED ON DATA SYNCHRONIZATION ON IP PROFILE DATABASE USING PYTHON

Data traffic on a dense network is a threat to cybercrime and a high vulnerability for technology companies so that the challenges to prevent it will be more diverse. Adding a strengthening boundary wall or firewall is an alternative to protect the traffic you have. Sorting data through packet filtering plus writing firewall rules to prevent malware and attacks from outside at the network device level is usually set manually. When heavy traffic makes data entry uncontrollable if it is monitored regularly, this research will create an automation design so that the sorting of incoming data packets through selection based on the specified rules runs in real-time so that the prevention of crime that enters the network is more swiftly handled. The system is running successfully by connecting the MQTT Collector as a subscriber that uses the python programming language to retrieve profiling data from the IP Profile Database. The system was tested on a Mikrotik router RB951Ui-2HnD which then the blocking track record will be stored in the Dynamic Firewall Data database in MongoDB. Also added a tool for controlling data in storage in the form of a program release. The results of the test show that data with an average base score above 20 is blocked and then stored in the block list in checking the collection in the database every 30 seconds. In addition, the data in the database will be checked every day within 30 days which will then be released and recorded in the release log in MongoDB.

Keyword: Packet Filltering, Firewall Rules, Python, Router Mikrotik.