Resolving Cross Domain Firewall Policy Anomalies

Volume 124 - Number 14

Year of Publication: 2015

Authors:
Abdul Raziya Sultana, Amrutasagar Kavarthapu

10.5120/ijca2015905771

Abstract

For last few years, Firewall usage with regard to protected network emails is important. Its ability to process inbound and confident bundle moves and accept or eliminate those bundle in accordance with the processing is what keeps this systems and networks protected. But considering a vast organization’s protection needs with regard to firewall program guidelines, typical home solutions won’t be sufficient because such organizations are compounds of different subnets which require comfort during plan quality. The key technical restriction is that firewall program guidelines cannot be shared across different websites for easier control because a firewall program plan might include important info and this might be a potential protection cycle hole that can be utilized by harmful users. Although largest rule calculations methods help to some extent they are unsuccessful of performance in accordance with the presence of NAT (Network Address Translation) device across different subnets (domains). So here recommend improving the current solution with a quality decision tree classifier criteria applied at routers for achieving the comfort maintained firewall program plan abnormality solutions with regard to repetitive rules control. So it involves wireless router extension
recommend to imitate this event and confirm conclusion in accordance with the results.

References

13. Q. Dong, S. Banerjee, J. Wang, D. Agrawal, and A. Shukla, “Packet classifiers in ternary CAMs can be smaller,” in Proc. ACM SIGMETRICS.

Index Terms

Computer Science Security
Keywords

Firewall Optimization. Privacy, Cross Domain, Access control rule policies.