International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 10 Issue 1 –OCTOBER 2014.

Correlation and Redundancy Firewall Optimization for Privacy Preserving

G. Bhavya[1], G. Vijaykanth[2]

[1]*M.Tech (CSE), CRIT, Affiliated to JNTUA University, ANANTAPURAMU, AP, India*

[2]*Assistant Professor in CSE, CRIT, Affiliated to JNTUA University, ANANTAPURAMU, AP, India*

[1]bhavya.gorantla@gmail.com

[2]vijay7mail@gmail.com

Abstract—Virtual Private Network (VPN) technology allows roaming users to securely use a remote computer on the public Internet. PACKET classification mechanism enables many networking devices, such as routers and firewalls, to perform services such as packet filtering, virtual private networks (VPNs), network address translation (NAT), quality of service (QoS), load balancing, etc. A firewall checks each incoming or outgoing packet to decide whether to accept or discard the packet based on its policy. Typically implemented on the network outer limits and function, firewalls clearly differentiate the trusted and untrusted regions. In this paper, we propose a cooperative firewall policy optimization protocol for cross-domain privacy. The proposed protocol identifies the rules that can be removed without either of the party disclosing the firewall rules to the other. Our protocol incurs no extra online packet processing overhead, and the offline processing time is less than a few hundred seconds.

Keywords—Firewall optimization, privacy, VPN's, Cross-Domain Privacy

I. INTRODUCTION

A firewall is defined as any device used to filter or direct the flow of traffic. Even though firewalls allow traffic from the trusted zone to the untrusted zone, with no any explicit configuration, traffic from the untrusted zone to the trusted zone must be clearly restricted. There are essentially four mechanisms used by firewalls to limit incoming and outgoing traffic -filtering, circuit- level gateway, and proxy server and application gateway. One of the core services provided by firewalls is Packet Filtering.

Packets can be permitted or denied based upon which is the:

-Source address
-Destination Address
- Protocol Type (IP, TCP, UDP, ICMP, ESP, etc.)
-Source Port and
-Destination Port

A firewall policy is usually specified as a sequence of rules, called Access Control List (ACL), where each rule has a predicate over multiple packet header fields and a decision to accept/discard the packet. The firewall rules in a firewall policy typically follow the first-match semantics, where the decision for a packet is the decision of the first rule that the packet matches in the policy. Also as the number of rules increases the performance of the firewalls decreases.

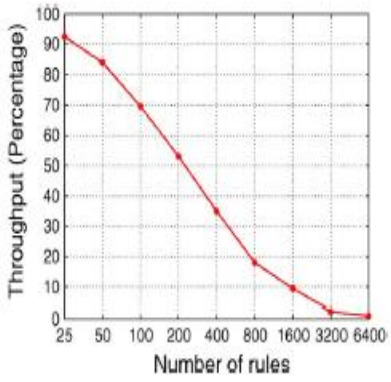

Fig. 1. Effect of the number of rules on the throughput

II. EXISTING SYSTEM

Firewall policies are kept confidential because of two reasons. First, attackers can exploit the security holes of the firewall policy. Second, a firewall policy often contains private information, e.g., the IP addresses of servers, which can be used by attackers to launch more precise and targeted attacks. The existing scheme for intrafirewall redundancy

removal aims to detect redundant rules within a single firewall. As these schemes require the knowledge of two firewall policies, hence are applicable within a single administrative domain. The collaborative firewall enforcement policies have been developed which enforce firewall policies over encrypted VPN tunnels without leaking the privacy of the remote network's policy. The former scheme preserves the privacy of the remote network's policy, whereas the latter preserves the privacy of both policies.

III. PROPOSED SYSTEM

In this work, we focus on removing interfirewall policy redundancies in a privacy-preserving manner.

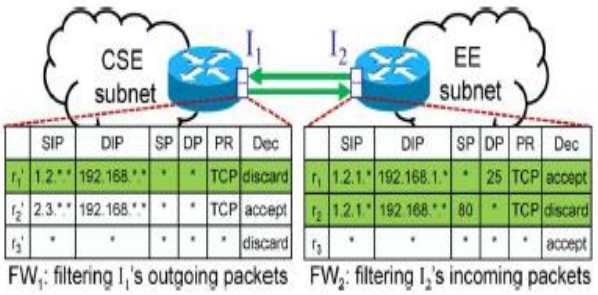

Fig. 2. Example interfirewall redundant rules.

Fig. 2 illustrates interfirewall redundancy, where two adjacent routers belong to different administrative domains CSE and EE. The rules of the two firewall policies FW1and FW2, which are used to filter the traffic flowing from CSE to EE. From the fig 2. it is clear that the Access Control List(ACL) maintains SIP, DIP, SP, DP, PR, and Dec denote source IP, destination IP, source port, destination port, protocol type, and decision, respectively. In order to perform a privacy preserving check for two adjacent firewalls, for each rule r in FW2, this solution checks whether all possible packets that match rule r in FW2 match a rule r' with the discard decision in FW1 . Since the firewalls follow the first-match semantics the above proposed solution is incorrect as there is a possibility that wrong redundant rules can be identified in FW2.

Hence, the above idea can be modified as follows: Computing a set of compact predicates for the set of packets that match r but should not match the rules above r in FW2. At the same time, we check whether all the packets that match the predicate are discarded by FW1.

Our protocol applies to both stateful and stateless firewalls. The key challenge for the design of the protocol is that it allows two adjacent firewalls to identify the interfirewall redundancy with respect to each other without knowing the policy of the other. Given two adjacent firewalls FW1, FW2 the traffic flow is from FW_1 to FW_2, a rule r in FW_2 is interfirewall redundant with respect to FW_1 if and only if all the packets in r's resolving set are discarded by FW_1.

The two adjacent firewalls are assumed to be semi-honest, which appropriate for large organizations that have many independent branches as well as for loosely connected alliances composed by multiple parties. Each firewall is converted to an equivalent sequence of non-overlapping rules. The rules for matching set are assumed to be equal to the resolving set $M(nr) = R(nr)$.Also, the problem is analyzed for single-rule coverage redundancy detection and multirule coverage redundancy detection. The first subproblem checks whether a nonoverlapping rule nr in FW_2 is covered by a nonoverlapping discarding rule nr' in FW_1, i.e., $M(nr) \subseteq M(nr')$. The second subproblem checks whether a nonoverlapping rule nr in FW_2 is covered by multiple nonoverlapping discarding rules $nr'_{i_1} \cdots nr'_{i_k}$ $(k \geq 2)$ in FW_1, i.e., $M(nr) \subseteq M(nr'_{i_1}) \cup \cdots \cup M(nr'_{i_k})$. Finally, after redundant nonoverlapping rules generated from FW_2 are identified, we map them back to original rules in FW_2 and then identify the redundant ones.

Single-Rule Coverage Redundancy Detection

For the two firewalls, in this work, it is assumed Net1 has a sequence of double encrypted no overlapping rules obtained from FW1 and d sets of double encrypted numbers obtained from FW2. The given set of predicate for matching $(F_1 \in \mathcal{T}_1) \wedge \cdots \wedge (F_d \in \mathcal{T}_d) \rightarrow discard$ denotes a double encrypted rule, where $\mathcal{T}_i$is a set of double encrypted numbers. For a nonoverlapping rule nr from FW2, if all its prefix families overlap with the same discarding rule nr'from FW1, nr is covered by nr' and, hence, nr is redundant.

Multirule Coverage Redundancy Detection

This computes all possible rules that are covered by a single or multiple nonoverlapping discarding rules among $nr'_1, \cdots, nr'_l$. All these rules form a new set $s'_1, \cdots, s'_q$.

But both the above coverage redundancy detections suffer from time and space complexities as the number of rules are huge, thereby increasing the communication and computational costs. Hence the above can be improvised as follows: A firewall rule with d fields can be denoted as a hyperrectangle over a d-dimensional space. Then, nonoverlapping discarding rules $nr'_1, \cdots, nr'_l$ are l-rectangles over a d-dimensional space.

Algorithm 1: Computation of the set of largest rules

Input: l nonoverlapping rules $nr'_1, \cdots, nr'_l$.
Output: The set of all the largest rules S

```
1  Initialize S, S := {nr'_1, ..., nr'_l};
2  while S has been changed do
3     for every two rules s'_i, s'_j (i ≠ j) in S do
4        compute the largest rules from s'_i and s'_j;
5        add the largest rules to Ŝ;
6     for each rule ŝ_i in Ŝ do
7        if there is a rule ŝ_j (j ≠ i) in Ŝ such that
   M(ŝ_j) ⊃ M(ŝ_i) then
8           remove ŝ_i from Ŝ;
9     S := Ŝ;
10    Ŝ := ∅;
11 return S;
```

Given firewall $FW_2 : \langle r_1, \cdots, r_n \rangle$ with no intrafirewall redundancy and its all-match FDD, rule ri is interfirewall redundant with respect to interfirewall redundant with respect to FW1 if and only if two conditions hold: 1) there is a redundant path whose terminal node contains sequence number i ; 2) there is no effective path whose terminal node contains as the smallest element.

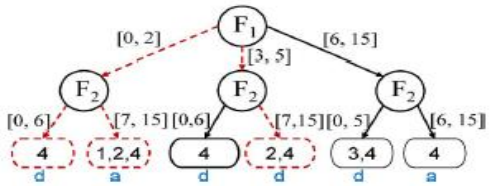

Fig 3: Identification and Removal of redundant rules

IV. CONCLUSION

The implemented work explores interfirewall optimization across different administrative domains .The protocol can identify in each firewall the rules that can be removed because of the other firewall. The cooperative computation between the two firewalls can be carried out without any party disclosing its policy to the other. From the experimental results, the communication cost is less than a few hundred kilobytes. Our protocol does not incur an extra online packet processing overhead. Our protocol applies to both stateful and stateless firewalls. i.e., having the connection table or not does not affect our protocol. Our protocol cannot be directly applied in case if there are any hosts or Network Address Translation (NAT) devices between two adjacent firewalls.

V. REFERENCES

[1] Fei Chen, Bezawada Bruhadeshwar, and Alex X. Liu, "Cross-Domain Privacy-Preserving Cooperative Firewall Optimization", IEEE/ACM TRANSACTIONS ON NETWORKING, VOL. 21, NO. 3, JUNE 2013

[2] J. Brickell and V. Shmatikov, "Privacy-preserving graph algorithms in the semi-honest model," in Proc. ASIACRYPT, 2010, pp. 236–252..

[3] A. X. Liu and F. Chen, "Collaborative enforcement of firewall policies in virtual private networks," in Proc. ACM PODC, 2008, pp. 95–104.

[4] A. X. Liu and M. G. Gouda, "Complete redundancy removal for packet classifiers in TCAMs," IEEE Trans. Parallel Distrib. Syst., vol. 21, no. 4, pp. 424–437, Apr. 2010.

[5] A. X. Liu, C. R. Meiners, and Y. Zhou, "All-match based complete redundancy removal for packet classifiers in TCAMs," in Proc. IEEE INFOCOM, 2008, pp. 574–582.

[6] C. R. Meiners, A. X. Liu, and E. Torng, "Bit weaving: A non-prefix approach to compressing packet classifiers in TCAMs," in Proc. IEEE ICNP, 2009, pp. 93–102.