

# Efficient Embedded Firewall for Communication Appliances

Sachin Garg  
Avaya Labs Research  
Basking Ridge, NJ, USA  
sgarg@avaya.com

Navjot Singh  
Avaya Labs Research  
Basking Ridge, NJ, USA  
singh@avaya.com

**Abstract**—Denial-of-Service attacks are a major concern in VoIP deployments. IP phones are especially vulnerable because of their inherent imbalance in network capacity and processing power. In other words, a packet flood can easily bring an IP Phone down long before the network saturation point is reached. In this work, we present the ideas behind the design of an efficient firewall to protect against DoS attacks. The main contribution lies in the novelty of packet classification heuristics by leveraging the behavior specific to VoIP. These include 1) State based rule-partitioning and 2) Flow-rate based rule update. The ideas and the evident contrast to generic firewalls should also facilitate firewall design for other applications.

## I. INTRODUCTION AND PROBLEM STATEMENT

Voice-over-IP (VoIP) devices such as IP Phones have low CPU and memory resources whereas their network connectivity is typically high bandwidth 10/100 Mbps Ethernet<sup>1</sup>. They are the first victims in a network based Denial-of-Service attack since their CPU/memory resources get overwhelmed long before network saturation limit is reached. A full-duplex 10 Mbps Ethernet pipe has a theoretic maximum receive rate of 14881 frames/second. At this rate, in a typical VoIP phone with a 60 MHz CPU, less than 4000 cycles are available to process each frame. This includes interrupt handling, stack and packet processing, buffer management and audio play-out. As an example, just the SHA-1 hash required in Secure Reliable Transport Protocol (SRTP) [2] involves 4560 logical operations [1]. Under normal operation, the receive rate of the SRTP stream is only 50 packets/second, which leaves plenty of spare CPU cycles. However, if a phone were to be flooded with fake SRTP packets, the per packet SHA-1 processing is more than sufficient to overwhelm the CPU. Similar calculations can be carried out for other VoIP protocols such as H.323 or SIP. Therefore, it is imperative that these devices be made robust against such flooding based attacks. This leads us to the problem statement, which is to *design a firewall, which can discard illegitimate packets before they travel up the network stack and overwhelm the CPU. The device based firewall itself consumes some CPU cycles underscoring the need for efficient packet classification.* In Section II, we describe the heuristics for efficient packet classification. The contrast between traditional firewalls [3] and application specific ones is brought out in the design. Section III concludes the article.

<sup>1</sup>For WLAN 802.11 based appliances, the bandwidth is 54Mbps in 802.11a and 100Mbps+ with MIMO technology.

## II. PACKET CLASSIFICATION HEURISTICS

Application specific network devices such as H.323 IP phones have the following distinguishing characteristics compared to generic network devices such as routers.

- 1) *Traffic to/from small set of IP addresses:* Less than a dozen well-known IP addresses engage in message exchanges with the phone. These include the media server (RAS, H.248), the media gateway (RTP, RTCP) and another IP phone during a call. Support servers such as DHCP, SNMP, TFTP and HTTP are also involved. In contrast, a router/switch, being a pass-through device rather than a source or a sink of packets, typically sees an order of magnitude more IP addresses and ranges.
- 2) *Small set of ports and Protocols:* The phone uses RTP, RTCP, H.323 suite, SIP, SNMP, TFTP, HTTP etc. It is never expected to receive IP datagrams, arbitrary UDP packets, TCP packets not belonging to above protocols etc. Routers and switches do not have this property.
- 3) *Distinct Operational States:* The phone has three distinct states of operation. 1) Booting and network configuration where it only engages in DHCP and TFTP exchanges, 2) Discovery and Registration, where the only legitimate exchange is H.225 and H.228 protocol with the well known media-server and 3) Operational state, which can be further divided into on-hook and off-hook state.
- 4) *Known expected traffic behavior:* In each state, since the protocol, packet format and packet data is known a priori, the expected ingress rate is completely known. For instance, with RTP, exactly 50 frames per second are received with a G.711 codec and 20 millisecond audio payload per packet. This is clearly a distinct property from routers and the one we leverage. In fact, modulo network induced delay/jitter, deviations from the expected behavior provide a strong measure for intrusion-detection in VoIP systems.

In the following, we describe the two key ideas in the firewall design for IP Phones.

### A. State based Rule Partitioning

In firewall design, there are two ways to increase the speed of packet classification. One is to increase the efficiency of rule processing by algorithms or heuristics which perform

better than simple linear search. The second is to reduce the number of rules themselves. We leverage the latter by segmenting all rules into subsets, each subset containing rules for a particular state of the appliance. This significantly reduces the number of rules the classification engine has to match at any time. For instance, once an IP-Phone reboots, it undergoes a DHCP and TFTP exchange sequence for network configuration. During this state, only DHCP and TFTP packets should be allowed. In other words, rules which match DHCP and TFTP protocols along with the known TFTP server IP address should suffice to discard any illegitimate packets. While we have drawn heavily upon the operation of an IP phone to illustrate the technique of rule-segmentation, the technique itself is orthogonal to the device and can be applied generically.

### B. Rate based Rule Update

The primary function of firewall in a router/switch is to block unwanted traffic while maximizing throughput of legitimate network packets up to the capacity limit. For a firewall in an IP Phone, while the requirement of blocking illegitimate packets is the same, maximizing throughput is not an issue. In an IP phone, in normal operation, the most network intensive traffic the phone receives is RTP packets while in a call. If G711 codec is being used, with 160 bytes packets, the data bandwidth of the RTP stream is 64 kbps. Assuming 20 millisecond audio per packet, this translates to 87.2 kbps at the Ethernet layer. This is more than two orders of magnitude lower than the capacity of the full-duplex 10 Mbps Ethernet port of the IP phone. This leads us to the underlying thesis of our heuristic. If the ingress traffic rate at the phone indeed exceeds this rate, some packets have to be illegitimate. In other words, rate monitoring is a strong measure for intrusion detection. When an increased rate is witnessed, we propose that only packets deemed critical are allowed to pass while the rest of the packets are dropped. In normal off-hook state of the phone, for instance, H.225 heartbeats between the phone and the media server are deemed critical to avoid timeouts and re-registration cycles. The criticality is a policy decision which involves a trade-off between packet classification speed and the number of rules. Once the ingress rate falls below the upper bound, the rule-base updates again to the original so as to allow all legitimate traffic and not just the critical. In the following we briefly describe the control-flow for rate based rule update.

**Rate based Update Control flow:** As shown in Figure 1, each packet arrival marks an event. A simple time based or packet count based condition is evaluated at each packet arrival. If the condition holds true then the ingress rate is calculated, following which two conditions are checked. The calculated ingress rate has to be higher than the threshold and the detection condition has to be met before the firewall rulebase can be updated by the policy rules administered by a human operator. The detection condition is based on a simple heuristic. Once the rulebase is updated, only policy determined critical traffic is allowed to reach the IP phone protocol layers and the rest is discarded. The reduced number of rules enables the phone to tolerate the DoS flooding attack without the CPU getting overwhelmed. In this degraded state,

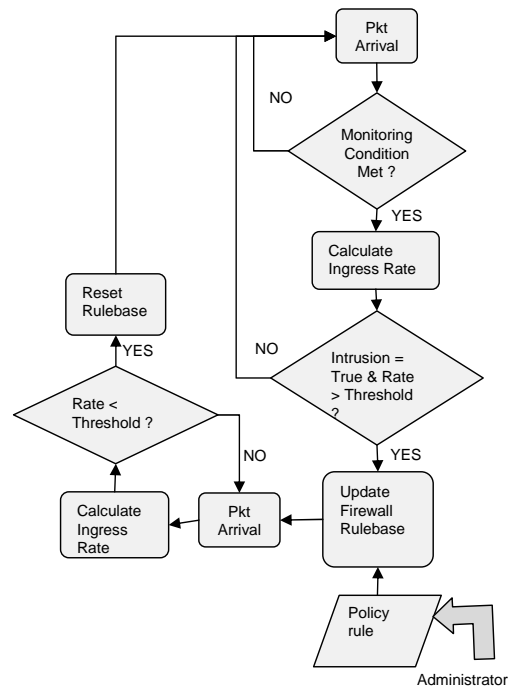


Fig. 1. Flowchart of the firewall control flow

ingress rate monitoring is continued to determine the stoppage in the intrusion. Once the rate falls below the established threshold, the rule-base is reset to its original state where all legitimate traffic is allowed to reach the phone. The control flow then returns to the initial state. Various parameters need to be optimized to fine tune the performance of the firewall. These include ingress-rate metric and measurement, ingress rate threshold, intrusion condition etc. In most cases, there would be a trade-off between the CPU cycles spent and the accuracy. We are currently validating our design ideas via a prototype.

### III. CONCLUSION

Given the critical importance of Security in VoIP system deployments, the communication appliances need a defense mechanism, which can provide protection in the face of flooding based DoS attacks. In this paper, we presented key technical elements of a light-weight firewall which can be embedded in such devices. We highlighted the difference in characteristics of communication appliances and those of general purpose network devices. We leverage the differences to design efficient heuristics for firewalling. These include 1) State based rule partitioning and 2) rate-based rule update. While the techniques were presented for IP Phones, they are general enough to be applied in firewall design for other applications.

### REFERENCES

- [1] S. Garg, N. Singh, T. Tsai, "Schemes for enhancing the denial-of-service tolerance of SRTP", Avaya Labs Technical Report, December 2004.
- [2] M. Baugher, D. McGrew, E. Carrara, M. Naslund, and K. Norrman. "The secure real-time transport protocol". IETF RFC 3711. <http://www.ietf.org/rfc/rfc3711.txt?number=3711>
- [3] W. R. Cheswick, S. M. Bellovin, A. D. Rubin, Firewalls and Internet Security: Repelling the Wily Hacker, Addison-Wesley Professional, 2 edition, February, 2003