Visualizing Remote Network Reactions with Firewall Probe

Hyuga Kobayashi[*]
The University of Tokyo

Hideya Ochiai[†]
The University of Tokyo

Hiroshi Esaki[‡]
The University of Tokyo

1 Introduction

Firewall is very common for protecting networks against cyber-attacks. However, some networks do not have firewalls, or even if they deploy a firewall, it sometimes exposes the internal network structure against administrator's intention.

This paper proposes a firewall probe to visualize global network status regarding firewall deployment. The firewall probe sends probing packets to a remote network, observes the reactions, and categorizes the network into five types from A (safe network) to E (alert-level network). By showing the network types by color, it visualizes and allows us to notice their vulnerabilities.

This paper focuses on transport-level firewall deployed at the entrance of local area networks or intra-networks. Application-layer firewall or device-level firewall are beyond the scope of this paper.

Compared to Zmap[1] or Nmap[2], our firewall probe tries to categorize the remote network type regarding firewall types based on the responses to the probing packets.

2 Firewall Probe and Visualization

This section describes the method of visualizing the remote network types obtained by our firewall probe. Let N be a large subnet. We divide N into 2^m pieces of sub-networks: i.e., N_0, N_1, N_{2^m-1}, where $m = 0, 1, 2, \cdots$. For example, N is a /16 network and N_i is a /24 network if $m = 8$. As figure 1, we can display N with Hilbert-curve mapped 2^m pieces of tiles. Each tile can show the identified remote network type by color.

For each N_i, our firewall probe sends probing packets in the following manner. First, it picks up an IP address *host* from N_i (i.e., $host \in N_i$), and sends (1) TCP SYN packet, (2) TCP SYN+ACK packet, and (3) ICMP ECHO request packet three times each to *host* with one second interval. Here, the destination port number of TCP should not be a well-known port, expecting that *host* is not servicing at the port and replying TCP RST when receiving SYN or SYN+ACK at the host level. It observes the responses from *host*, and records the packets that *host* has responded.

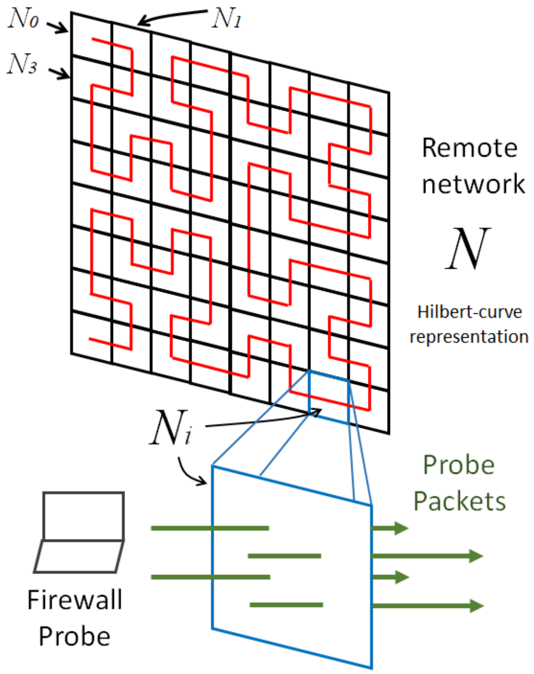

Figure 1: Firewall Probe and Visualization

The firewall probe scans for all the IP addresses in N_i in the same way, and it will get a vector of $(\text{SYN}(N_i), \text{SYNA}(N_i), \text{ICMP}(N_i))$. Here, $\text{SYN}(N_i)$ is the number of the hosts (in N_i) has responded for TCP SYN packet. The same discussions apply to $\text{SYNA}(N_i)$ and $\text{ICMP}(N_i)$.

Here, the value of $\text{SYN}(N_i)$, $\text{SYNA}(N_i)$ may contain some garbage data because of the temporal status of firewalls. So, if they are smaller than a threshold θ (e.g., 2 or 3), the firewall probe treats them as 0.

Based on the vector, the firewall probe categorizes the remote network type as follows.

Type A (safe) : the network did not respond at all. i.e., $\text{SYN}(N_i) = \text{SYNA}(N_i) = \text{ICMP}(N_i) = 0$.

Type B (ok) : the network responded only to ICMP. i.e., $\text{SYN}(N_i) = \text{SYNA}(N_i) = 0$, $\text{ICMP}(N_i) > 0$.

Type C (normal) : the network only blocked SYN. i.e., $\text{SYN}(N_i) = 0$. $\text{SYNA}(N_i) > 0, \text{ICMP}(N_i) > 0$.

Type D (warning) : the network blocked ICMP but allowed to pass SYNACK. i.e., $\text{ICMP}(N_i) =$

[*] e-mail: hyuga@hongo.wide.ad.jp
[†] e-mail: ochiai@elab.ic.i.u-tokyo.ac.jp
[‡] e-mail: hiroshi@wide.ad.jp

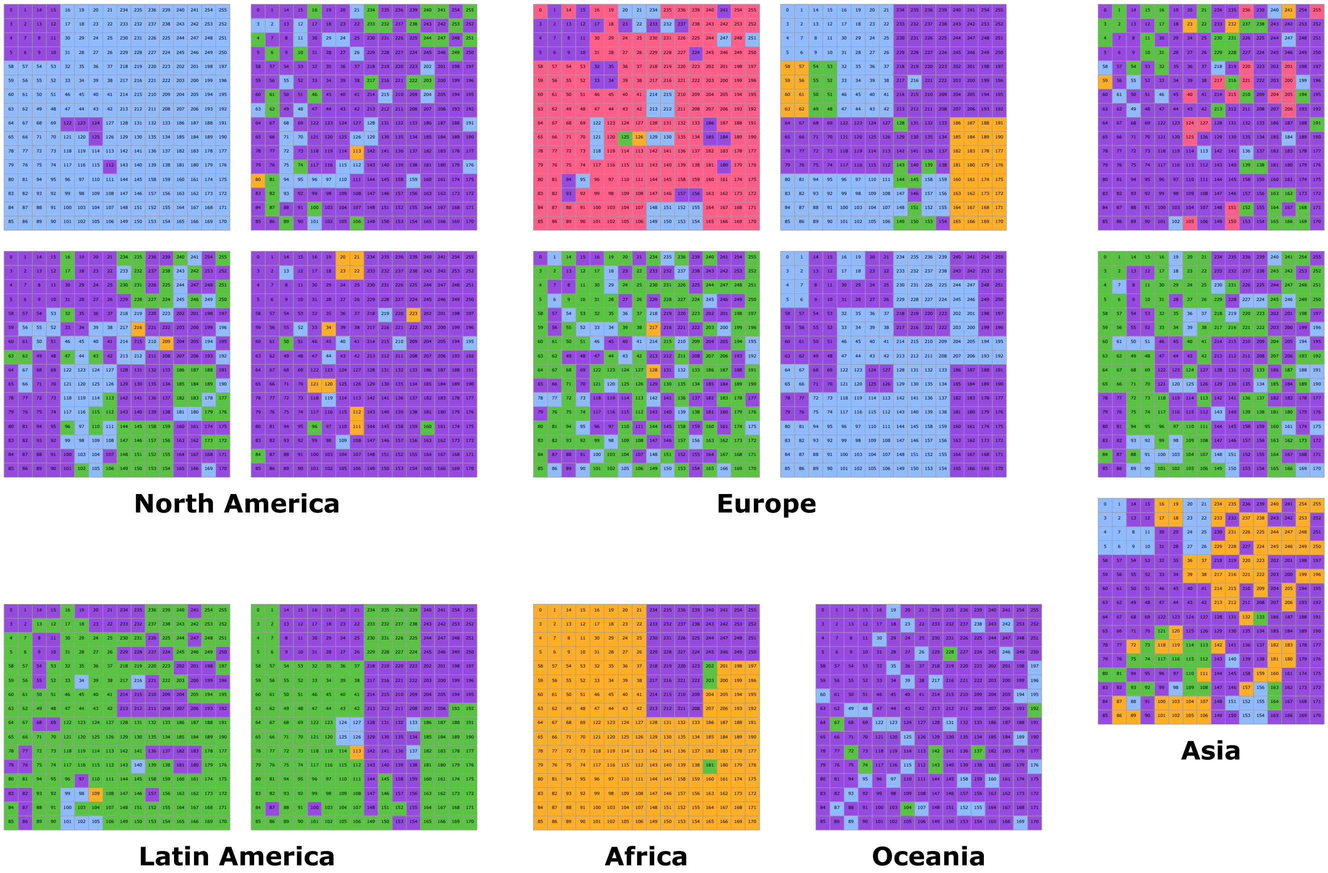

Figure 2: Visualization of remote network types with firewall probe. This figure shows fifteen /16 networks – presented as large blocks. Four for North America, two for Latin America, four for Europe, one for Africa, one for Oceania, and three for Asia. A small block in a large block corresponds to a /24 network. The meaning of the colors are – purple (A:safe), cyan (B:ok), green (C:normal), yellow (D:warning), red (E:alert).

$\mathrm{SYN}(N_i) = 0$, $\mathrm{SYNA}(N_i) > 0$. This network is sometimes vulnerable because the network operators are trying to hide the existence of hosts by blocking ICMP, but SYNACK can pass through.

Type E (alert) : the network is open to the global, potentially exposing its vulnerabilities. I.e., $\mathrm{SYN}(N_i) > 0$.

In this way, by probing N_i, we can categorize N_i and fill a color of N_i tile in a Hilbert-curve representation of N.

3 Demonstration

We selected fifteen /16 sample networks from the regions of North America, Latin America, Europe, Africa, Asia, Oceania. We scanned those networks with our firewall probe in July of 2018.

Figure 2 shows the result. Here, a small block in a large block corresponds to a /24 network. The small block is colored with one of purple, cyan, green, yellow, and red, meaning that the identified network type is A, B, C, D, and E respectively.

From the result, we can see that various network types certainly exists in the global Internet from type A to type E. We have found "type E (alert-level)" /24 networks in Europe's /16 network and Asia's /16 network, and "type D (warning-level)" /24 networks in many /16 networks. We also found some /16 networks that look well-protected; i.e., all small blocks are purple or cyan.

This result indicates that our firewall probe can work effectively for identifying the remote network types.

4 Conclusion

In this paper, we have proposed a firewall probe and demonstrated sample scanning result by visualization. Although the firewall is a well-known security mechanism, some networks still do not deploy them or are behaving against the network administrator's' intention. Our firewall probe and its visualization has demonstrated that our mechanism allows us to notice such networks.

References

[1] DURUMERIC, Zakir; WUSTROW, Eric; HALDERMAN, J. Alex. *ZMap: Fast Internet-wide Scanning and Its Security Applications.* In: USENIX Security Symposium. 2013. p. 47-53.

[2] LYON, Gordon Fyodor. Nmap network scanning: *The official Nmap project guide to network discovery and security scanning.* Insecure, 2009.