Chapter 5
Enterprise Network Packet Filtering for Mobile Cryptographic Identities

Janne Lindqvist
Helsinki University of Technology, Finland

Essi Vehmersalo
Helsinki University of Technology, Finland

Miika Komu
Helsinki Institute for Information Technology, Finland

Jukka Manner
Helsinki University of Technology, Finland

ABSTRACT

Firewalls are an essential component of the Internet and enterprise network security policy enforcement today. The configurations of enterprise firewalls are typically rather static. Even if client's IP addresses can be dynamically added to the packet filtering rules, the services allowed through the firewall are commonly still fixed. In this paper, we present a transparent firewall configuration solution based on mobile cryptographic identifiers of Host Identity Protocol (HIP). HIP allows a client to protect the data transfer with IPsec ESP, and supports dynamic address changes for mobile clients. The HIP-based firewall learns the identity of a client when it communicates with the server over HIP. The firewall configures the necessary rules based on HIP control messages passing through the firewall. The solution is secure and flexible, and introduces only minimal latency to the initial HIP connection establishment.

INTRODUCTION

Remote access to corporate service is very challenging to set up and configure in a secure way. The simplest way is on a per-service basis, by using HTTP and TLS and introducing a login function to public servers. Unfortunately, this leaves the server open for various attacks, e.g., DoS, since it must be open to any remote client regardless of the source IP address, and unlawful access attempts are caught very late in the login process.
To enable better security, and to disable most forms of attacks on the services, a VPN solution can be used, together with a tightly controlled firewall configuration. Through a VPN, corporate services are available for the client only after a successful VPN login transaction. Yet, also here the VPN server needs to be available to the public, and can be attacked. Moreover, configuration of the firewall is a further cause of concern. First of all, setting up proper filtering rules for corporate firewalls is not a trivial task. Secondly, changing the connectivity provider results in network renumbering which further requires a full reconfiguration of the firewall. It is also also possible that the address of single VPN client changes due to device mobility or DHCP lease renewal. In such a case, the client has to reinitialize the VPN connection.

Two additional security concerns arise from the use of a typical VPN service. First, typically all the corporate services become available to the user when VPN gateway or firewall accepts a VPN connection. Then, a malicious user, virus or worm can try to mount an attack on any service of the corporation because VPNs do not offer protection against “internal” attacks. Second, the corporate services become vulnerable to attacks to “external” attacks if the device of a user is compromised. The attacker can route its own packets using the compromised device through the VPN tunnel to the corporate network. Hence, the attacker can practically mount any type of attack on the corporate services.

The second security concern was highlighted as part of the Microsoft Windows Vista routing compartments functionality, which was supposed to be included in the new operating system. The basic idea was that remote access from the user device is controlled per application, and not per host, making it impossible to route packets between interfaces, WLAN and VPN interfaces in our example. Yet, it is still not included, and one can only guess what the reasons are. Nevertheless, the security vulnerability still remains.

Firewalls are, unfortunately, a critical component of corporate and personal networks in the Internet today. Packet filtering is typically based on the 5-tuple of sender and receiver IP addresses and port numbers, and the transport protocol. Sophisticated firewalls can also filter based on the content of application layer protocols. Commonly, the filtering rules are quite static and constrained. The firewall passes only certain services and a known set of hosts through. In more dynamic networks, for example, offering public or subscription-based WLAN access, or nomadic enterprise environments, the firewalls are controlled and rules set up based on some authentication exchange. Typically, a client is authenticated and authorized to use a WLAN service based on a web browser login application. If the login is successful, the firewall opens predefined services for the MAC and IP address of the client device. Only then the client can start access Internet to, for example, browse the web, or initiate VPN connections.

The current situation has at least four downsides. First, authentication for network access has a number of different implementation choices, which may or may not work with the device of the user, for example, on laptop computers, PDAs, or smart mobile phones. Second, the firewall allows the client to only use certain pre-defined services even when the client is authenticated successfully and authorized to use the Internet. It would be more useful to have a separate signaling protocol dynamically manage the filtering rules associated with a given authenticated client. Third, a third party can still listen to the network communications, collect varying information, and steal the identity of an authenticated client. Fourth, network renumbering becomes a problem, because all static rules on firewalls that are based on IP address must be changed when renumbering occurs. The same problem of updating firewall rules appears in access networks, where the IP address assigned to a client can change during the session,