DynFire: Dynamic Firewalling in Heterogeneous Environments

Alexander Vensmer
University of Stuttgart
Institute of Communication Networks
and Computer Engineering
Pfaffenwaldring 47, 70569 Stuttgart
Email: alexander.vensmer@ikr.uni-stuttgart.de

Dr. Sebastian Kiesel
University of Stuttgart
Computing Center
Networks & Communications Systems Dept.
Allmandring 30A, 70569 Stuttgart
Email: sebastian.kiesel@rus.uni-stuttgart.de

***Abstract*—This paper presents "DynFire," a novel approach for the role-based, dynamic control of network firewalls. DynFire allows an individually controlled, secure access to the IT resources of a large organization, with particular focus on mobile users and users with restricted rights, such as subcontractors. The basic assumption behind DynFire is that, within a secured network domain separated from the Internet, we can establish a temporary binding between an IP address and a single user ID. Whenever a user connects to or disconnects from this secure network domain, firewalls are configured accordingly, using a centralized "Firewall Manager" and standardized signaling protocols.**

Keywords: dynamic firewall control; network security; signaling protocols; policy based network access control

I. Introduction

Firewalls are a well-understood and widely deployed means of protecting IP networks. Their use is based on the assumption that the network can be divided into distinct domains with different security requirements and threat levels. Located at domain boundaries, firewalls forward or reject network traffic between these domains, according to security policies that are usually configured statically into the firewalls. However, this assumption, and thus the applicability of firewalls, is increasingly challenged. With the widespread use of mobile wireless as well as remote access over the Internet, domain borders get more and more blurred. A mobile user changing from one access network to another usually receives a new IP address randomly chosen from an address pool. Therefore, IP packets *usually* do not carry enough information for a firewall to perform user-based access control decisions. While this puts the usefulness of firewalls into question, other developments reinforce the need for them. As the operator of a large campus network we encounter an increasing number of devices in our network, which are not "classic" telecommunications or office PC equipment. This includes, e. g., building automation systems or scientific measurement devices. While these systems are often vulnerable due to missing or outdated security mechanisms (e. g. operating system updates, virus scanners, password policies, etc.), they also have an increased need for remote access, e. g., for maintenance technicians. Placing a firewall in front of such systems may improve security, but conventional firewalls with static policies are not flexible enough for fine-grained access control.

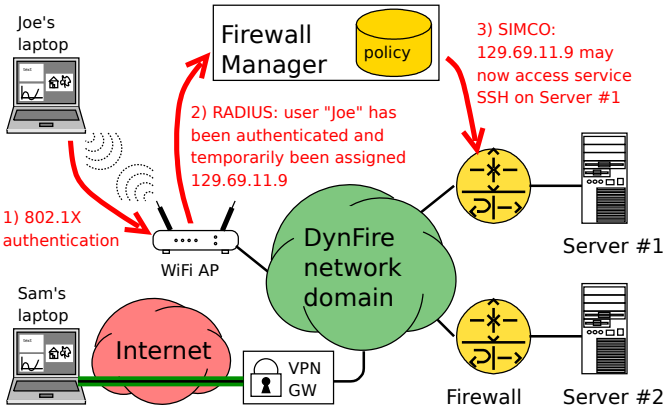

Fig. 1. DynFire scenario

In this paper we present DynFire, a new architecture for the dynamic and role-based configuration of firewalls. The rest of the paper is structured as follows. Section II summarizes related work. In Section III we present the underlying assumptions and the main ideas of our approach. In Section IV we describe the "Firewall Manager," which is the main element of our architecture. Section IV concludes the paper and summarizes further steps.

II. Related Work

Dynamic control of firewalls has been studied in detail for Voice over IP applications [1], [2], [3]. There, a signaling protocol (e. g. SIP) is used to establish a session state before media starts to flow. This signaling protocol can interact with the firewall control mechanisms. Guha and Francis [4] propose a more universal security solution targeted at the whole Internet, but it requires support in the endpoints. Cisco Systems' TrustSec technology [5] can deploy "downloadable Access Control Lists" (dACL) when a user connects to the network. However, this is currently a vendor-specific solution.

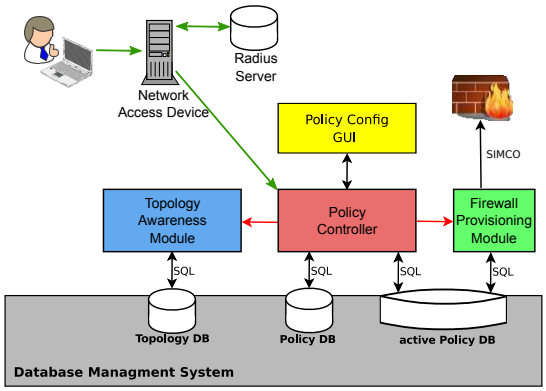

Fig. 2. DynFire architecture

III. Principles of DynFire

The goal of DynFire is to create an environment where firewalls can perform role-based access decisions, without requiring special support at the endpoints. Therefore, DynFire as such cannot be not a solution for the whole Internet. Instead, it can be used to secure the IT resources of a single organization. We assume that this organization operates a network that is protected from the Internet by firewalls. Every user has to authenticate before getting access to this network and we assume that authentication can not be bypassed. Technically, this may be realized by 802.1x/802.1ae (LAN or WiFi) or VPN access via a central VPN concentrator (Fig. 1). Consequently, an IP address observed in a packet can be mapped unambiguously to a User ID at any time. The DynFire administrators do not create firewall rules including individual IP addresses, but describe the desired communication relationship between users and services (network resources) in an administration panel. When a user logs into the network and receives a temporary IP address, these high level policies are converted to firewall rules by a centralized "Firewall Manager". In a complex network topology the Firewall Manager has to configure all firewalls on the paths between the users and the resources, respectively.

IV. Firewall Manager

The Firewall-Manager consists of several modules (Fig. 2) storing their information in a SQL database.

A. Policy Controller

When a user logs in, the Firewall Manager is notified about the temporary binding between UserID and IP address. For each resource and service the user is allowed to access, the Policy Controller creates firewall rules, based on high level policies stored in a database. Information about the concerned firewalls is retrieved from the Topology Awareness Module. Then, the rules are sent to the Firewall Provisioning Module.

B. Topology Awareness Module

The Topology Awareness Module has to find all firewalls on the path between two given hosts. Therefore, it has to know the network topology. The current version is able to work with a static topology map. Under development is an advanced version that can detect the topology automatically, based on LLDP (Link Layer Discovery Protocol) [6] and SNMP (Simple Network Management Protocol) [7]. It will also interact with the routing protocol, in order to configure firewalls on the alternative path, in case a rerouting occurs.

C. Firewall Provisioning Module

The Firewall Provisioning Module is responsible for transferring firewall rules to a set of firewalls. Several protocols for firewall control exist [2]. We have chosen the SIMCO protocol [8] for its flexibility and simplicity. Several SIMCO implementations for Linux (iptables), Cisco, and Juniper routers are currently under development or testing. Furthermore it is possible to integrate the Firewall Manager into the Astaro Command Center [9], which provides an integrated firewall solution. This multitude of supported firewalls allows DynFire to be deployed in heterogeneous network environments.

V. Conclusion and Future Work

We have presented the design and implementation of DynFire, an architecture for the dynamic control of firewalls. It enables role-based access to network resources. Particular focus is on support for legacy systems and embedded devices with poor security standards and without the ability to install special driver software. DynFire does not need specialized hardware. It uses firewalls which are already widely deployed and a central Linux server. While finishing the implementation we are also evaluating and analyzing the performance, scalability, and security of DynFire. We are planning to deploy DynFire in the campus network of the University of Stuttgart.

Acknowledgment

This work was supported by the "DynFire" project [10], a research project supported by the German Federal Ministry of Education and Research (BMBF, Foerderkennzeichen: 01BY1151). The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the DynFire project or the BMBF.

The authors would like to thank Markus Hennig and Sören Berger for contributions and feedback.

References

[1] C. Aoun, "Plan de signalisation Internet pour l'interfonctionnement entre NAT et Firewall," PhD Thesis, ENST, Paris, 2005.
[2] S. Kiesel and M. Scharf, "Modeling and performance evaluation of transport protocols for firewall control," *Computer Networks*, vol. 51, no. 11, pp. 3232–3251, Aug. 2007.
[3] ETSI TISPAN, "NGN Functional Architecture," ETSI, Standard ES 282 001 V3.4.1, 2009.
[4] S. Guha and P. Francis, "Towards a Secure Internet Architecture Through Signaling," Cornell University, Ithaca, NY, Technical Report cul.cis/TR2006-2037, 2006.
[5] Cisco Systems, Inc, "Cisco TrustSec Solution Overview," 2012.
[6] IEEE LAN/MAN Standards Committee, "Station and Media Access Control Connectivity Discovery," IEEE, Std. 802.1ab, 2009.
[7] J. Schoenwaelder and T. Jeffree, "Simple Network Management Protocol (SNMP) over IEEE 802 Networks," IETF, RFC 4789, Nov. 2006.
[8] M. Stiemerling, J. Quittek, and C. Cadar, "NEC's Simple Middlebox Configuration (SIMCO) Protocol V3.0," IETF, RFC 4540, May 2006.
[9] Astaro, a Sophos Company. [Online]. Available: http://www.astaro.com
[10] DynFire project home page. [Online]. Available: http://www.dynfire.org