April 20, 2017

ON-DEMAND NETWORK FIREWALL PROFILE APPLICATION

Mark Mentovai

ON-DEMAND NETWORK FIREWALL PROFILE APPLICATION

ABSTRACT

A firewall profile system allows a device to communicate its desired firewall profile upon connection establishment. The system receives the desired profile from the device and determines if the desired profile requires expanding a default profile. If the desired profile does not require expansion, the system provides network access to the device based on the default profile. If, however, the system determines that implementing the desired profile requires expansion of the default profile, the system notifies a user of a host device to allow or refuse expansion of the default profile. If the profile expansion is not allowed by the user, the system applies the default profile and the system provides network access to the device based on the default profile. Otherwise, if the profile expansion is permitted by the user, the system updates the default profile with the desired profile and provides network access to the device based on the desired profile.

PROBLEM STATEMENT

Many single-purpose devices that are connected to a network only require limited-scope access to the network. Those single-purposes devices, however, are typically granted full and unrestricted access. Under normal circumstances, they will not exercise the full extent of access that has been granted. Should such a device become compromised, it will be able to use the network for purposes not originally intended, e.g., exfiltration of data to an unwanted party or participation in a botnet. It is possible to establish a network firewall that blocks some or all

network access from a device or set of devices. Presently, it is sometimes possible, although cumbersome, to establish firewall profiles for connected devices that limit their access to the network to only the resources that are required for their operation. For example, a firewall profile might specify what network addresses a device is permitted to communicate with or what protocols it is permitted to use.

Unfortunately, it is difficult to establish such a firewall profile for many devices that are provided as black boxes. Often firewall rules are crafted based on network addresses that communication should be permitted or blocked. These addresses are not typically fixed, but change with time. Thus, it is expected that simply providing a firewall profile that allows or limits communication with specific addresses is not sufficient. It is sometimes possible to infer the desired level of access by observing a device in operation, but this is time-consuming and requires technical skill. Because of the large amount of manual work required, true tight per-device firewall profiles are seldom applied in practice. An advanced method and system for establishing a mechanism for a device to communicate its desired firewall profile upon connection to a network is described.

DETAILED DESCRIPTION

The systems and techniques described in this disclosure relate to a firewall profile system that allows a device to communicate its desired firewall profile upon connection establishment. The system can be implemented for use in an Internet, an intranet, or another client and server environment. The system can be implemented locally on a client device or implemented across a client device and server environment. The client device can be any electronic device such as a

desktop computer, a laptop computer, a mobile communication device, a tablet computer, a handheld electronic device, a printer, a personal digital assistant, any telecommunication device, a set-top boxe, a game-console, an access point, a smart applicance such as a refrigerator or clothes washer, a home automation product such as security, climate, entertainment, or lighting control, etc.

Fig. 1 illustrates an example method 100 for establishing a mechanism for a device to communicate its desired firewall profile upon connection to a network. The method 100 can be performed by a firewall profile system that can be a stand alone server or can be implemented in a host device that receives a request for connection establishment.

The system receives 102 a desired firewall profile from a device upon connection establishment. The desired firewall profile can be included in or referenced by an optional extension communicated during a Dynamic Host Configuration Protocol (DHCP) transaction. The device's desired firewall profile may be crafted tightly to request network access only to the extent required for proper operation of the device. The firewall profile includes network addresses for which communication should be permitted or blocked. The device can determine network addresses based on a Domain Name System (DNS) lookup for a known domain name, which is fixed entity unlike an IP address. Hence, the device expresses its desired firewall profile in terms of domain names rather than just IP addresses. The device can include one or more electronic devices, e.g., security cameras, home theater receivers, video streaming device, smart TVs, Blu-Ray players, cloud-connected printers, smart light bulbs, mobile phone, laptop, wearable device, headsets, etc.

The system then determines 104 if the desired profile requires expanding a default profile of the firewall profile system. The system matches the network access parameters of the desired profile against the default profile. The default profile can be one or more predetermined set of rules for providing network access to respective devices. The system can automatically define the predetermined set of rules, or a user of the host device can input the predetermined set of rules into the system via a privacy settings menu. For example, the user can input the predetermined set of rules as allowing access to host devices' media for a video streaming device. The predetermined set of rules can be stored in a memory accessible to the system, memory of the host device, in a cloud server, in an account associated with the user, etc.

A desired firewall profile requested by a connected security camera device might, for example, specify that the camera:

1. needs to send DNS requests to its configured DNS server and receive responses from the same.

    a. furthermore, the camera can specify that it only needs to look up the address of securitycamera.example.com.

2. needs to connect to and communicate with securitycamera.example.com, but only on TCP port 443.

3. accepts inbound connections on TCP port 80 from the local network, for local set-up, administration, and maintenance.

4. does not need to accept any other inbound connections.

5. needs to communicate with a DHCP server that the camera is bound for the purposes of renewing or releasing its DHCP lease, and needs the ability to broadcast to DHCP servers on the local network for the purposes of rebinding renewal failure.

Applying desired firewall profile for sub-point (1)(a) fully requires introspection into the DNS layer. (1)(a) is included in the desired profile here because usually every device specifies that it needs access to its configured DNS server. However, if access to the DNS server is not restricted in any way, this becomes a large hole through which exfiltration might occur, even if the rest of the firewall profile is tight. Hence, with the desired firewall profile in place, unwanted network access by the device and unwanted remote access of the device is prevented.

If the desired profile does not require expanding a default profile, the system applies 106 the default profile. That is, when the network access requested by the device in the desired profile is similar to the network access in the default profile. Hence, the system provides network access to the device based on the default profile. If the desired profile requires expanding a default profile, the system notifies 108 the user of the host device to allow or refuse expansion of the default profile. In an example scenario, the host device can be a server managing the network and the user can be a network administrator.

The system then receives 110 an input from the user. and accordingly checks 112 whether the user has allowed profile expansion. If the profile expansion is not allowed by the user, the system applies 106 the default profile to the device. Hence, the system provides network access to the device based on the default profile. Additionally or alternatively, the system can reject a request of the device for establishing the connection with the host device or

the network if the system automatically determines that the desired profile does not require expanding the default profile.

If the profile expansion is allowed by the user, the system updates 114 the default profile. The system can either completely erase the default profile from the host device and substitute it with the desired profile or the system can add the additional network access parameters to the existing default profile. The desired profile is applied only to the devices that require default profile expansion and the user of the device allows expansion of the default profile. The system can also use the desired profile as a default profile for future requests from similar devices. Hence, the system provides 116 network access to the device based on the desired profile. A router or other device mediating network access can then apply the desired firewall profile to all network access by the newly-connected device.

In an alternate embodiment, a device that is already connected to the network can also request expansion of network access, e.g., through a DHCP renewal. The device can similarly request 102 for the wider desired profile from the host device. However, it remains possible for a compromised device to request wider access for itself upon subsequent connection to the network. To guard against this, the system (through a router or other device mediating network access) could detect a widening of the firewall profile and refuse to allow it, possibly raising 108 an alert directed to a responsible user or the system administrator.

FIG. 2 is a block diagram of an exemplary environment that shows components of a system for implementing the techniques described in this disclosure. The environment includes client devices 210, servers 230, and network 240. Network 240 connects client devices 210 to servers 230. Client device 210 is an electronic device. Client device 210 may be capable of

requesting and receiving data/communications over network 240. Example client devices 210 are personal computers (e.g., laptops), mobile communication devices, (e.g. smartphones, tablet computing devices), handheld electronic devices, printers, personal digital assistants, set-top boxes, game-consoles, access points, smart appliances such as a refrigerator or clothes washer, a home automation product such as security, climate, entertainment, or lighting control, etc.

and other devices 210' that can send and receive data/communications over network 240. Client device 210 may execute an application, such as a web browser 212 or 214 or a native application 216. Web applications 213 and 215 may be displayed via a web browser 212 or 214. Server 230 may be a web server capable of sending, receiving and storing web pages 232. Web page(s) 232 may be stored on or accessible via server 230. Web page(s) 232 may be associated with web application 213 or 215 and accessed using a web browser, e.g., 212. When accessed, webpage(s) 232 may be transmitted and displayed on a client device, e.g., 210 or 210'. Resources 218 and 218' are resources available to the client device 210 and/or applications thereon, or server(s) 230 and/or web page(s) accessible therefrom, respectively. Resources 218' may be, for example, memory or storage resources; a text, image, video, audio, JavaScript, CSS, or other file or object; or other relevant resources. Network 240 may be any network or combination of networks that can carry data communication.

The subject matter described in this disclosure can be implemented in software and/or hardware (for example, computers, circuits, or processors). The subject matter can be implemented on a single device or across multiple devices (for example, a client device and a server device). Devices implementing the subject matter can be connected through a wired and/or wireless network. Such devices can receive inputs from a user (for example, from a

mouse, keyboard, or touchscreen) and produce an output to a user (for example, through a display). Specific examples disclosed are provided for illustrative purposes and do not limit the scope of the disclosure.

DRAWINGS

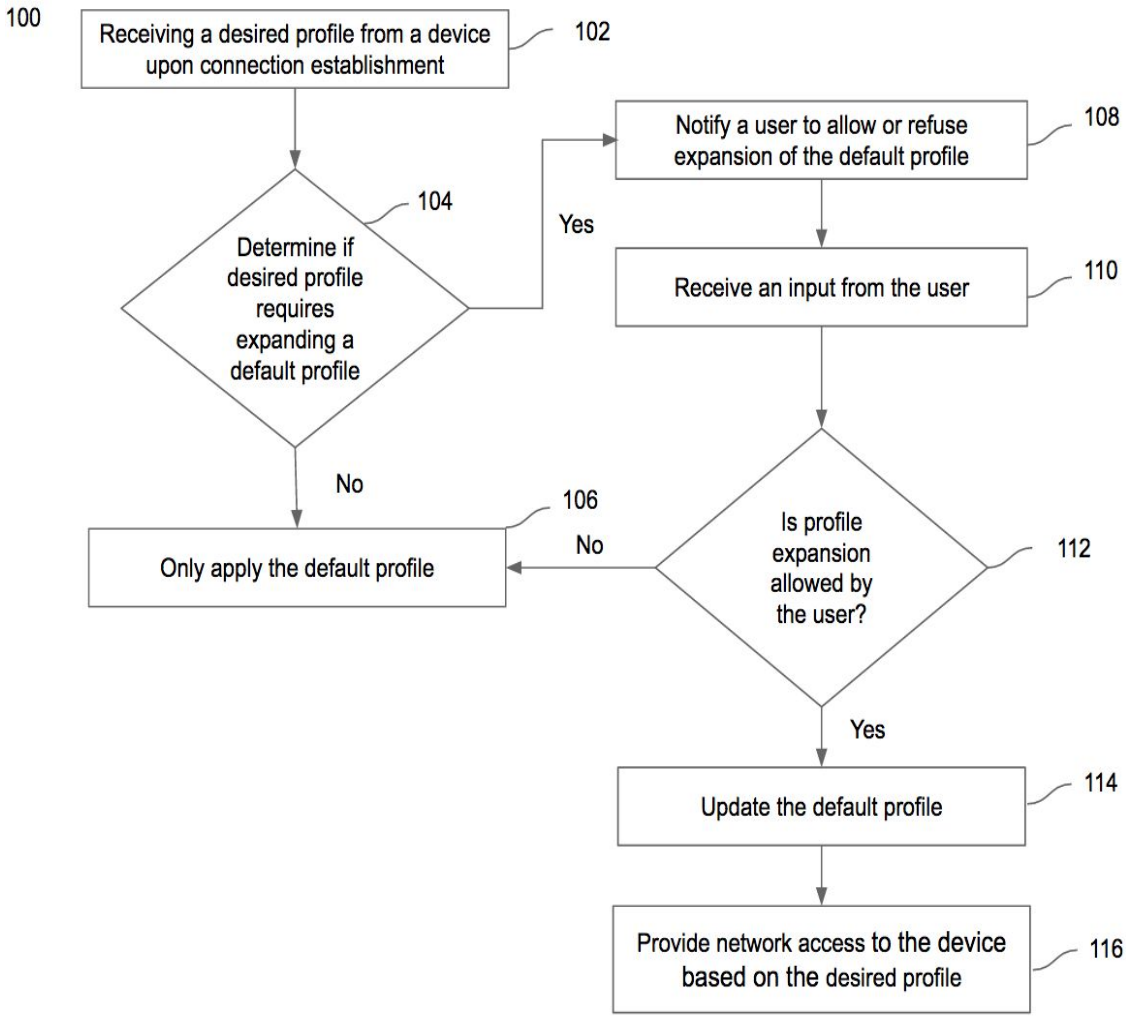

Fig. 1

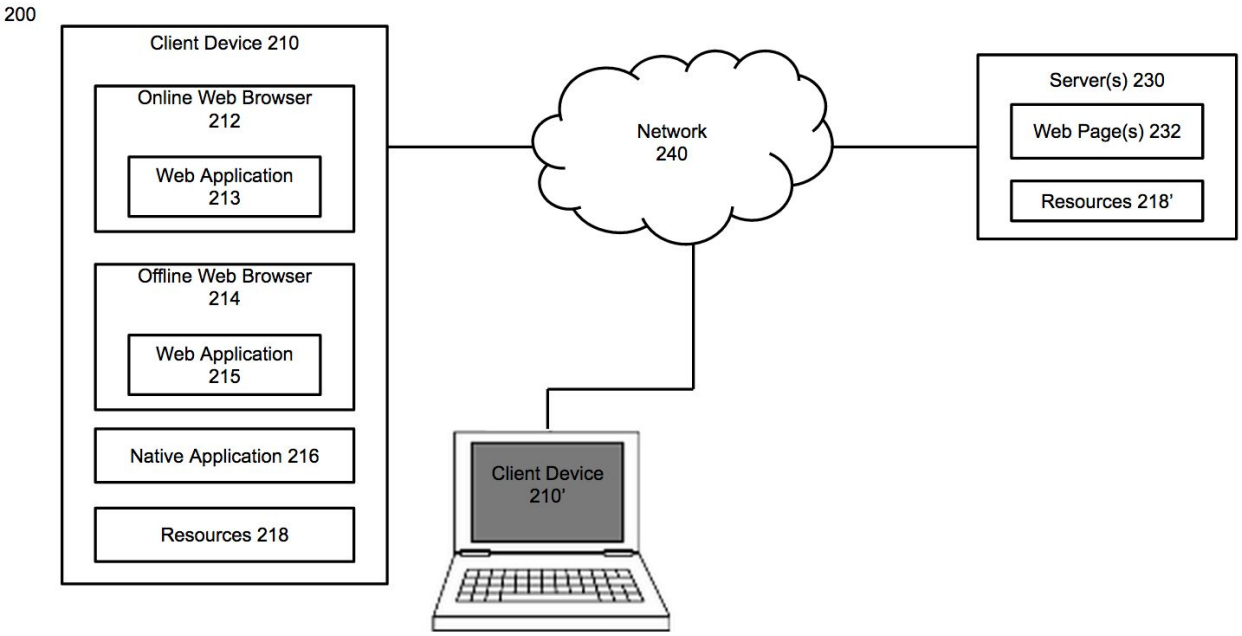
200
Client Device 210
Online Web Browser 212
Web Application 213
Offline Web Browser 214
Web Application 215
Native Application 216
Resources 218
Network 240
Server(s) 230
Web Page(s) 232
Resources 218'
Client Device 210'

Fig. 2