Firewalls and their Impact on Multimedia Systems

Utz Roedig

Darmstadt University of Technology

Merckstr. 25 • D-64283 Darmstadt • Germany

Email: Utz.Roedig@KOM.tu-darmstadt.de

Firewalls are a widely used security mechanism to provide access control and auditing at the border between the Internet and private networks. The mechanisms and techniques firewalls are based on did not change much over the last years. New challenges are presented when new application types like multimedia applications are to be supported by firewalls. These applications differ in many aspects from “traditional applications”, for example in bandwidth-usage, dynamic elements and multiple data flows for one application session. Currently existing firewalls have problems supporting these new applications because they try to map the behavior of them to the manner of conventional applications which they are able to handle. To solve these problems, the protection is intentionally weakened, hazarding obvious security risks. This is usually done if such a practice seems to be the only applicable way to use a certain service at all. A typical example for which companies may decide that the service is worth to take the risks is a missing proxy support. Some applications do not support the usage of a proxy since the end systems need to communicate directly. In this case, the firewall filters may be configured to selectively pass data streams directly to the external net and vice versa. The same is necessary if no proxy is implemented for an important application. However since the firewall system has to be configured in a way that it does not provide the maximum possible protection for the internal network, such approaches can be considered as short-term hacks at best.

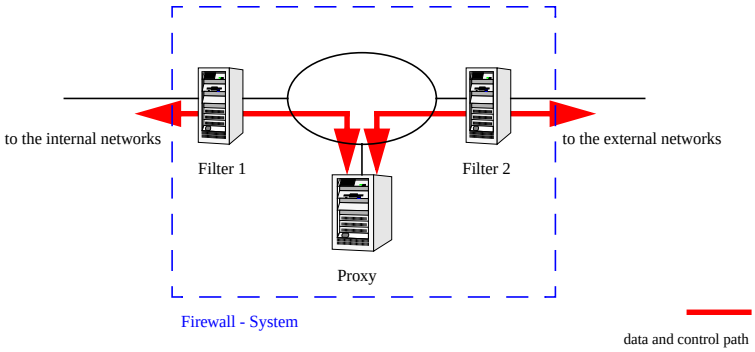
The types of applications considewherered here are multimedia applications which use continous media and discrete media data. In most cases the continuous media are audio and/or video data streams. The discrete media are often control data streams for the audio and video data streams and additional information (e.g. meta data). The client connects to the server using a straight TCP or UDP “connection”, often called control channel. After control channel setup, the multimedia application opens one or more data channels to transmit audio or video data. The port numbers used for these data channels are dynamically negotiated on the control channel. Multimedia applications differ from traditional applications in many characteristics. Especially the following issues cause problems in a network which is protected by a firewall:

- **Multiple flows for one logical session:** In most cases the audio and video content is sent using additional transport flows separate to the control data. Sender and receiver are “connected” by several flows but there is only one logical session between them.
- **Dynamic behavior:** Most of the connection parameters are unknown when the communication starts. For example, the number of audio or video streams, the bandwidth needed to transmit the streams, the transport ports used for the streams are unknown. An intermediate system like a firewall has to follow this dynamic behavior.
- **Complex protocols:** The protocols used to control multiple flows and the dynamic communication are in most cases more complex than a protocol used for one static flow. Firewalls and especially proxies have to observe the communication. Therefore, they have to interpret the communication protocols.
- **Data rate:** The increased data rate and data volume which characterizes multimedia applications demand higher network performance. A firewall has to deal with this as well.

Firewalled network environments will exist in the future, they will be enhanced but not replaced by other technologies (e.g. IPsec). Firewalls used today are not well prepared for requirements needed by multimedia applications. To reduce the problems caused by the insufficient cooperation of firewalls and multimedia applications several aspects must be taken into account:

- During the specification of multimedia protocols and the design of multimedia applications, the existance of firewalls has to be considered.
- Existing firewall techniques have to be enhanced and/or modified to support new features neeeded by multimedia applications.

To use the advantages of different firewall techniques, a combination of packet filters, proxies and stateful filters is often utilized. Such a combination of these elements and networks is called a firewall system.



As described above, multimedia applications negotiate the number and the specifications (e.g. port numbers) of the data channels dynamically. Therefore, these applications require intermediate systems which are capable to adapt to the actual communication situation. In our reference scenario, only the central component in this system, the proxy, has these capabilities. It is able to recognize the flow allocation commands of the applications in their control channels. Based on the interpretation of these commands it opens the communication paths for the communication endpoints. The filters at the border of the *demilitarized zone* (DMZ) are not involved in this dynamic adaption to the communication situation. Consequently in a standard scenario they have to be configured to pass all possible connections to and from the proxy. The filters have to be used with a configuration not providing their maximal protection functionality. From this aspect I deduce the first criteria.

> **Criteria 1:** All components of a firewall system should adapt autonomously or should allow other components to change their individual configuration to the requirements of the actual communication situation of the complete firewall system.

Another problem using multimedia applications in such a firewall system is the performance. Every packet is sent through two filters and one proxy. This reduces the performance and limits the amount of connections that can be sent through the system. To increase performance, many firewall vendors use a stateful inspection machine instead of a proxy, which has a higher throughput. However, the general problem remains, all traffic is sent through three machines. Yet, the proxy or stateful inspection machine just forwards the data channel packets without any processing. Hence these streams could be sent directly via both filters. Additionally it is usefull to achieve more flexibility using machines with special characteristics. These arguments lead to my second criteria.

> **Criteria 2:** The control channels should be separated from the data channels and should be carried on different paths through the firewall system.