



Profile and Role-based Firewall Control for Campus Classroom Labs

Best Practice Document

Produced by the MARNET-led Campus Network

Monitoring and Security working group

Author: Vangel V. Ajanovski (FCSE/MARnet)

April 2016

© MARnet, 2016 © GÉANT, 2016. All rights reserved.

Document No:	GN4-NA3-T2-MA-BPD-6
Version / date:	V1.0 / 12-04-2016
Original language:	English
Original title:	Profile and role-based firewall control for campus classrooms labs
Original version / date:	V1.0 / 12-04-2016
Contact:	vangel.ajanovski@finki.ukim.mk

The work has been carried out by a MARnet- and FCSE-led working group on campus network monitoring and security as part of a joint-venture project within the HE sector in Macedonia.

Parts of the report may be freely copied, unaltered, provided that the original source is acknowledged and copyright preserved.

The research leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 691567 (GN4-1).

Table of Contents

Executive Summary	3
1 Introduction	4
2 Use-Cases and Priorities	5
3 Use-Case Descriptions	7
UC-FW1: Teacher - Requests the Creation of a Specific Access Profile by the Admin	7
UC-FW2: Admin - Defines New Computer Labs and New Destinations	7
UC-FW3: Admin - Configures the Monitoring and Access Control Services	7
UC-FW4: Teacher - Controls the Activation of the Pre-Made Network Access Profiles.	8
UC-FW5: Teacher - Blocks Network Access to a List of Destinations	8
4 Network Architecture	9
4.1 Initial Architecture	9
4.2 Proposed Network Architecture	10
5 Network Access Control Solution	12
5.1 Computer Labs Firewall	12
5.2 FINKI-Firewall Control Application	12
5.3 Network Access Profiles	13
Example	13
5.4 Auditing Access to Various Services	14
References	15
Glossary	16

Table of Figures

Figure 2.1 Use-case diagram denoting each user's goals.	5
Figure 4.1 Initial network architecture.	9
Figure 4.2 Proposed network architecture.	11
Figure 5.1 Screenshot showing the FINKI-Firewall control application in use.	13

Executive Summary

Computer-based teaching laboratories at the universities in Macedonia are used in three general situations: practical demonstrations of various technologies as part of the teaching process, individual work by students on their assignments and projects, and as an environment for conducting exams of many different types.

Depending on the special use-cases for each situation, different access permissions are required, different network setups are required, access to online resources should be permitted/denied, and in most situations such adjustments should be performed by the teacher, without needing any network administration knowledge or direct access to the networking equipment. In this document, the design and organizational process of the deployment of such a system is presented together with the tools that enable and ease the implementation and customization based on the needs stemming from the real environment.

This document should be considered a reference and guide to possible simple solutions, based on many years of trials at computing departments within the Ss. Cyril and Methodius University, Skopje, Macedonia.

1 Introduction

Before even starting to discuss solutions, one should have decided on the nature of the actual problems and their importance. The following problem statement tries to sum up the issues at hand that teachers and system administrators usually face in their everyday work, with regards to network access control, in order to be able to discuss and point out a solution within this BPD.

Problem statement regarding network access control

The problem of	not being able to restrict network access during classes and exams and to do it on a selective bases.
affects	teachers in larger computer labs or in situations where exams and classes are being held online.
the impact of which is	the inability of the teacher to control and evaluate whether the students have solved their assignments by themselves or with the help of external resources or other people, so the teachers sometimes revert to unplugging the network cables from the computers. Unplugging cables is sometimes the most effective and easy solution, but it creates more issues - defects in the cables, problems with computer lab monitoring software, problems with system updates, etc. When unplugging cables is not an option, the network admins will have to intervene and restrict or allow access via routing ACL tables or firewall rules, something that teachers can't do by themselves.
a successful solution would be	a software system that will enables the teacher to control and restrict network access to specific destinations, depending on the requirements at the time of the exam, without having specific system administration and network administration knowledge and access privileges.

2 Use-Cases and Priorities

The main idea in the proposed systematic solution is to enable the teacher to configure that network access is blocked or allowed to certain predefined network destinations (e.g. the course management server, e-testing server, code programming server, etc.), when needed - when starting an exam or course activity in the lab. This can be done by means of specially crafted network access profiles, created by the network administrators, unique for each computer lab, configured in the lab firewall and deployed or deactivated when the teacher needs them.

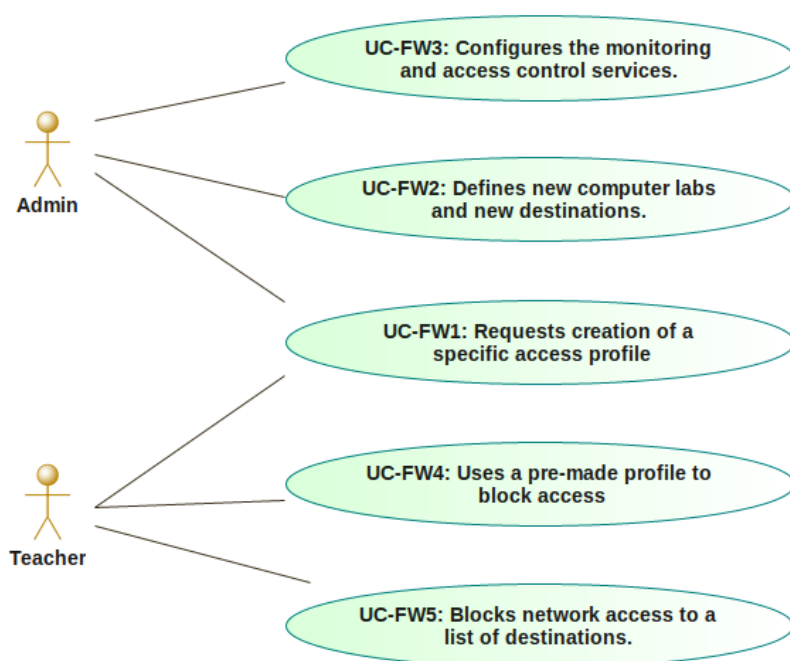


Figure 2.1 Use-case diagram denoting each user's goals.

Must have

- UC-FW1: Teacher - Requests the creation of a specific network access profile by the Admin
- UC-FW2: Admin - Defines new computer labs and new destinations.

- UC-FW3: Admin - Configures the monitoring and access control services.
- UC-FW4: Teacher - Controls the activation of the pre-made network access profiles.

Should have

- UC-FW5: Teacher - Blocks network access to a list of destinations.

Ideally, the solution would be completely automated and work as part of an integrated information and control system, so this document is presented from the viewpoint of the design and development of such a system. Business-level use-cases are presented first, to understand the general level functional requirements, and then several non-functional requirements are added. Where the solution cannot be automated, a manual process will be implemented for the same use-case scenario.

3 Use-Case Descriptions

The functional requirements, written in the form of use-cases, are given in the following paragraphs.

UC-FW1: Teacher - Requests the Creation of a Specific Access Profile by the Admin

1. The teacher accesses and opens a new profile request.
2. The teachers completes the request form with data on domains that should be allowed, domains that should be blocked, type of access to local resources and for which classrooms this profile is requested for.

The process continues manually:

3. After the admin is notified about the new request, the requirements are investigated and a new profile template is created as a configuration file.
4. After testing that the new profile template works to a satisfactory level, the profile is published in the profile selection list for further use by all teachers.

UC-FW2: Admin - Defines New Computer Labs and New Destinations

At present, this use-case depends heavily on network configuration and connections, so the profiles necessary for new labs and new destinations cannot be created automatically. The administrator manually creates groups of firewall rules that can be applied in order to allow or block access, as needed by teachers. These rules are stored as pieces of source code and are included when choosing the destinations and types of access by the teacher.

UC-FW3: Admin - Configures the Monitoring and Access Control Services

1. The admin access the monitoring service
2. The admin configures the default timeouts for resetting the firewall rules in each computer lab
3. The admin configures the scheduler for automatic invocation of the resetting process

UC-FW4: Teacher - Controls the Activation of the Pre-Made Network Access Profiles.

1. The teacher access the labs access control system.
2. The teacher chooses the lab in question.
3. The teacher selects the required access profile from the list of possible network access profiles.
4. The teacher also sets a timeout period in minutes, after which the system should remove access to all blocks. This is needed in case one forgets to remove the block and other users enter the labs without the privileges needed to modify the configurations.
5. Firewall rules to allow access to each of the needed destinations are set up, and a follow-up rule to block all other traffic originating from the chosen lab.
6. All the teacher's actions and choices are recorded in a log.

UC-FW5: Teacher - Blocks Network Access to a List of Destinations

The teacher starts an exam or activity in a lab, and depending on assignment requirements may wish to stop access to certain predefined network destinations (file management server, ...). Communication with other destinations is allowed.

1. The teacher accesses the lab's access control system.
2. The teacher chooses the lab in question.
3. The teacher marks all the destinations to be blocked.
4. The teacher sets a timeout period in minutes, after which the block is removed.
5. Firewall rules to block access to each of the selected destinations are set up, as well as a follow up rule to allow all other traffic originating from the chosen lab.
6. All the teacher's actions and choices are recorded in a log.

4 Network Architecture

4.1 Initial Architecture

Usually campuses employ a network architecture similar to the one shown in Figure 4.1. On the left is the network block with all computer labs; on the right is the publicly accessible servers block. All computer labs usually have a separate L2 switch that might be located in the room or in a network concentration point/rack/closet/room. L3 switches are sometimes used. In order to save the assigned public IP address space and protect from direct outside attacks, the labs are usually behind a small router/firewall that uses NAT/PAT, which then links them into the campus network. Sometimes, campuses isolate the labs in separate VLANs, if they have support for this in the upstream network and the main lab's router/firewall.

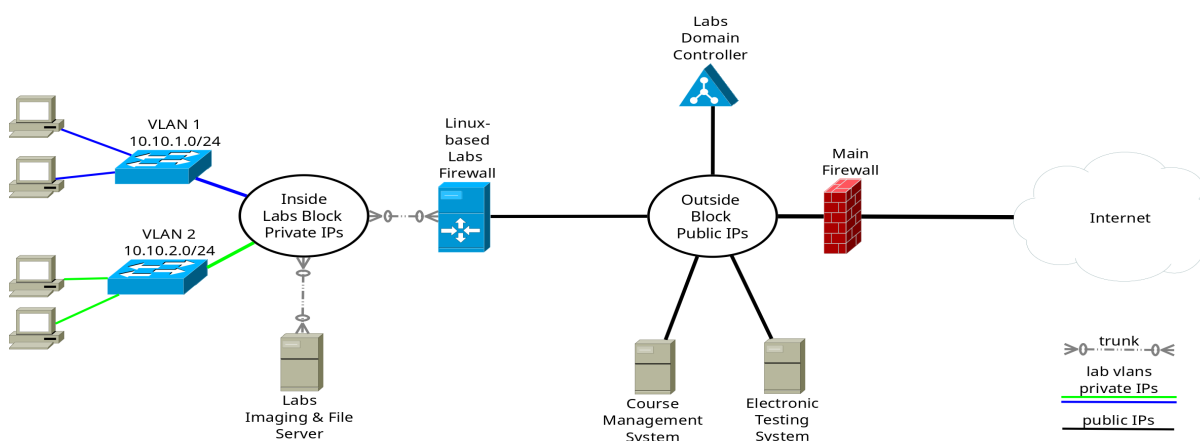


Figure 4.1 Initial network architecture.

There are several issues with the usual networking architecture, which prevent some of the use-cases we have as requirements:

- If VLANs are not used per lab, computers from different labs can communicate with each other, and there is no isolation of one lab from another, which is important when having computer exams in one lab and the other lab open for all students to use. In such a situation,

a student in the open lab can communicate and help another student taking an exam in the other lab.

- When holding some specialised classes – for example a course on Computer network design or a System services course – the students in one lab can activate a DHCP server or create loops in the network or open other services that conflict with the rest of the infrastructure.
- The Course management system / e-testing system does not know the exact IP addresses of the users accessing it from computer labs, which might be crucial when there are exams and deadlines.
- All access control is a fixed configuration usually implemented as static access lists on the routers. Teachers cannot activate or deactivate certain networking services or control access to network resources on the outside.

4.2 Proposed Network Architecture

This architecture is based on the following premises:

- The network is again split into two blocks
 - Inside a privately-addressed computer labs block with a separate VLAN and IP class for each computer lab (coloured lines).
 - Outside publicly-addressed servers block (black lines).
- The Lab's firewall, which is based on Linux, has the following responsibilities:
 - it is a static router among different parts of the computer labs block.
 - NAT/PAT hiding the network from the public internet.
 - Hosts a custom software solution for switching on/off access to various network destinations chosen by teachers.
 - DNS server for resolving the server names present in the inside block, so that all computers in the labs only get an internal IP for them.
- Computer labs have a presence only in the inside block; each lab is in a separate VLAN.
- Some servers can have a presence in both blocks, the reason is:
 - Computers in the labs should be able to access such servers even if the Internet access is disabled.
 - The servers should know the address of each lab computer that is accessing it.
 - VLAN Trunk links have to be established to each server so they can be accessed from the labs directly and only those VLANs that are allowed to pass are configured on the trunk links.
 - If higher throughput is needed, separate gigabit network interfaces are added to the respective servers and isolation is created per interface, putting each interface in a separate VLAN
- Access from the inside block to the outside block or global Internet is only possible via the Linux-based labs firewall.

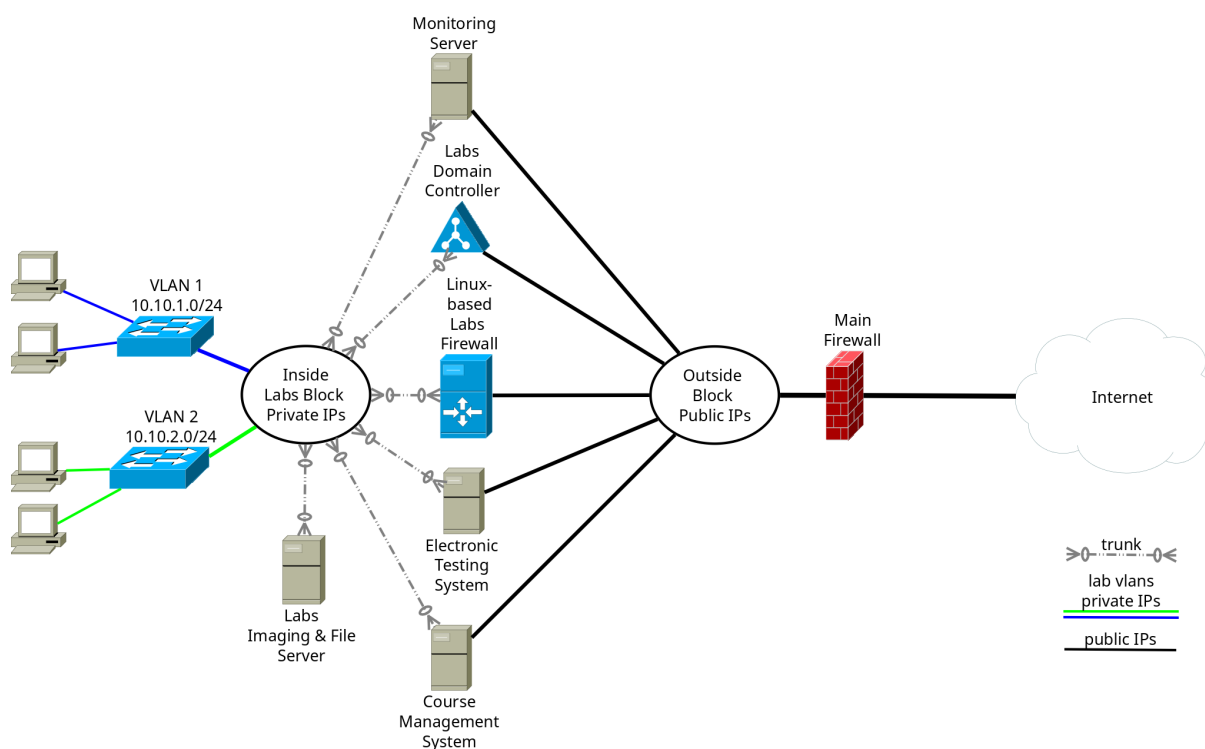


Figure 4.2 Proposed network architecture.

5 Network Access Control Solution

5.1 Computer Labs Firewall

A Linux-based server is used for the purpose of a firewall, running the ClearOS distribution. It is set up on a virtual server, with many virtual interfaces connected to various parts of the network and the respective VLANs (as seen in Figure 4.2). This enables easier manipulation of the rules of the NAT and the router in order to achieve the described use-case scenarios, by modification of the ipchains tables. Although such configurations can be prepared and loaded manually by the administrator when requested by teachers, we propose using a special application called Finki-Firewall giving an easy-to-use web interface accessible to all teachers, who can select from the pre-made network access profiles and apply them to each lab. This application is open-sourced and should be used as a basis or as an idea how to create custom solutions, although it can also be used as-is.

5.2 FINKI-Firewall Control Application

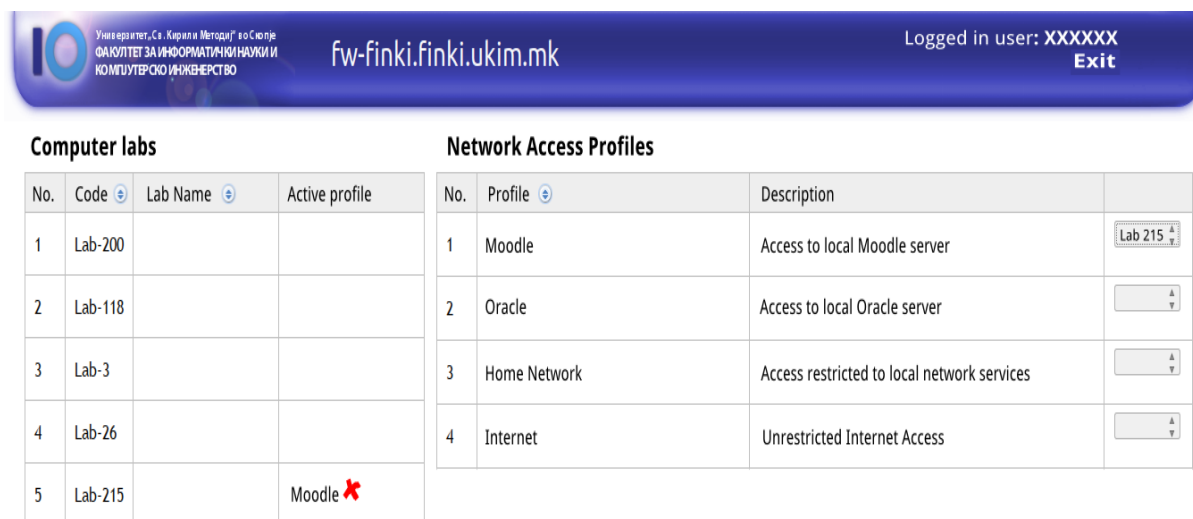
FINKI-Firewall is a Tapestry5-based Java web application initially created by Dragan Sahpaski for use at the Faculty of Computer Science and Engineering in Skopje. This application is intended to be used by teachers, enabling them to control and block network traffic in computer labs. The teachers don't need prior system administration or network administration knowledge to use the original application as it is very simple, and only enables choosing the network-access profile to be deployed from the list of pre-made profiles. [FINKI-Firewall]


The idea is simple: ready-made snippets of ipchains rules are defined in configuration files by the system administrator and, depending on the choice made by the teachers, these rules are inserted into the ipchains list and, as such, modify the firewall behaviour to block or pass traffic from certain sources to some destinations. These rules are called profiles and they are presented as simple choices for the teacher in the control application.

The application was originally created with a focus mostly on UC-FW2 and UC-FW4. After a testing setup and assurance that it works as intended, further internal development should be done to customize all the needed use-cases and prepare the application to work properly in the deployment environment.

The applications performs authentication via a CAS server for Single Sign-On, a central authentication software originally by JASIG, now Apereo, that is in use at many educational institutions and enables

the configuration of a range of authentication backends. When integration with another authentication system is requested, it should be reimplemented within the application, using the sources as an example.



No.	Code	Lab Name	Active profile
1	Lab-200		
2	Lab-118		
3	Lab-3		
4	Lab-26		
5	Lab-215		Moodle 

No.	Profile	Description
1	Moodle	Access to local Moodle server
2	Oracle	Access to local Oracle server
3	Home Network	Access restricted to local network services
4	Internet	Unrestricted Internet Access

Figure 5.1 Screenshot showing the FINKI-Firewall control application in use.

5.3 Network Access Profiles

The application for network access control uses predefined profiles, which are in fact iptables script snippets defined in a JSON file. Many such rule-sets can be prepared by the network administrator and system administrator of the labs firewall, and they can be configured within the JSON configuration files to allow activation by the teachers. When applying any profile, the previous rules are cleared and the configuration is overwritten by the new scripts.

Some of the many profiles that usually need to be configured are:

- unrestricted internet access to all resources and domains.
- restricted internet access to a certain domain only (e.g. Moodle, Oracle, Facebook, ... depending on the teacher requirements), while blocking everything else

Example

The following example shows how simple it is to configure the application - a simple profile that enables network access to a certain SITE (plus access to the domain controller, monitoring server and firewalls gateway address which are always needed), but blocks access to all other network destinations.

```
{
  "name" : "Profile",
  "description" : "Access to SITE only",
  "iptables" : [
```

```

"iptables -I FORWARD -s ${ipClass}
    -j DROP",
"iptables -I FORWARD -s ${ipClass}
    -d SITE.ADDRESS
    -j ACCEPT",
"iptables -I FORWARD -s ${ipClass}
    -d DOMAIN.CONTROLLER.INTERNAL.ADDR
    -j ACCEPT",
"iptables -I FORWARD -s ${ipClass}
    -d MONITORING.SERVER.INTERNAL.ADDR
    -j ACCEPT",
"iptables -I FORWARD -s ${ipClass}
    -d FW.INTERNAL ADDR
    -j ACCEPT"
}},

```

`${ipClass}` is a variable in the script that the application changes to the class of IPs of the selected computer lab. The application is also customisable to support many computer labs, which are also configured inside a JSON file.

5.4 Auditing Access to Various Services

The DNS server in the lab's firewall resolves the names of all services that have a presence in the inside block, so that requests for the resolution of such servers will result in a private IP address from the inside block.

All servers are connected via trunk links, so that they have a presence and IP address in all computer lab VLANs in the inside block. In that way it is ensured that:

- Access to any secured service from within the computer labs in the inside block will be served by the server daemon (service) running on an internal IP address and will be logged by the relevant service as access from the internal IP address of the precise lab computer, without hiding behind the NAT/PAT public address.
- Access to inside services will not get routed through the firewall, so will be faster.

References

- [FINKI-Firewall]** <https://github.com/dragansah/finki-firewall>
- [ClearOS]** ClearFoundation ClearOS - <http://www.clearfoundation.com>
- [Tapestry5]** Apache Tapestry 5 project - <http://tapestry.apache.org/>
- [CAS]** Apereo Foundation Central Authentication Service (known as JASIG CAS in the past) - <http://www.apereo.org/cas>
- [Tomcat]** Apache Tomcat - <https://tomcat.apache.org/>

Glossary

FCSE	Faculty of Computer Science and Engineering, University Ss Cyril and Methodius, Skopje, Macedonia
FINKI	Acronym of the FCSE official name in the Macedonian language
UC	Use-Case
VLAN	Virtual Local Area Network
DHCP	Dynamic Host Configuration Protocol
IP	Internet Protocol (used as IP address)
NAT	Network Address Translation
PAT	Protocol Address Translation
DNS	Domain Name System
JSON	JavaScript Object Notation
HTML	Hyper Text Markup Language
CAS	Central Authentication Service, a single sign-on open-source program originally by JASIG, today Apereo Foundation.
JASIG	Java in Administration Special Interest Group

