

# Project G-Cloud Setup

Name	value
Project	SAWFT
Project ID	sawft-275017
Cloudguard Admin User	admin
Cloudguard Admin PW	MesvQPH5h95c
Cloudguard internalIP(default)	10.128.0.2
Cloudguard internalIP(my-vpc)	192.168.23.2
Cloudguard externalIP	34.71.14.71

## Lab 3.1: Application Control

Ein Hindernis bei dieser Uebung war, dass das Update fuer "Application Control & URL Filtering" sehr lange gebraucht hat.

Folgende Regeln wurden angelegt:

2	block some services with message	* Any	* Any	* Any	Google Maps Google Accounts Google Search Twitter	Drop Blocked Messa...	Log Accounting	* Policy Targets
3	block facebook	* Any	* Any	* Any	Facebook Facebook Messenger	Drop	Log Accounting	* Policy Targets

Die "block facebook"-Regel wurde zur Kontrolle angelegt um auch eine Seite geblockt zu haben , ohne Block Message.

Sonstige Vorgehensweise laut Anweisung.

Die Tests wurden im Lynx-Terminal Browser durchgefuehrt da es durchwegs Probleme mit VNC gab.

Dass die Services als geblockt markiert wurden zeigt der HitCount der Regel:

2	block some services with message	* Any	* Any	* Any	Google Maps Google Accounts Google Search Twitter	Drop Blocked Messa...	Log	* Policy Targets
3	block facebook	* Any	* Any	* Any	Facebook Facebook Messenger	Drop	Log	* Policy Targets
4	allow vnc	* Any	cloudguard-gw-vm	* Any	VNCLINUX	Accept	Log	* Policy Targets
5	allow internet traffic LINUXVM	LinuxHost	All_internet	* Any	* Any	Accept	Log	* Policy Targets
6	allowsSH	* Any	cloudguard-gw-vm	* Any	ssh_version_2 Service1	Accept	Log	* Policy Targets
7	Cleanup rule	* Any	* Any	* Any	* Any	Drop	Log	* Policy Targets

SummaryDetailsLogsHistory

Drop Rule 2

block some services with message

Created by: admin

Date created: 5/13/2020 12:00 PM

Expiration time: Never

Hit Count: 44 (1%, Low)

Additional Rule Info:

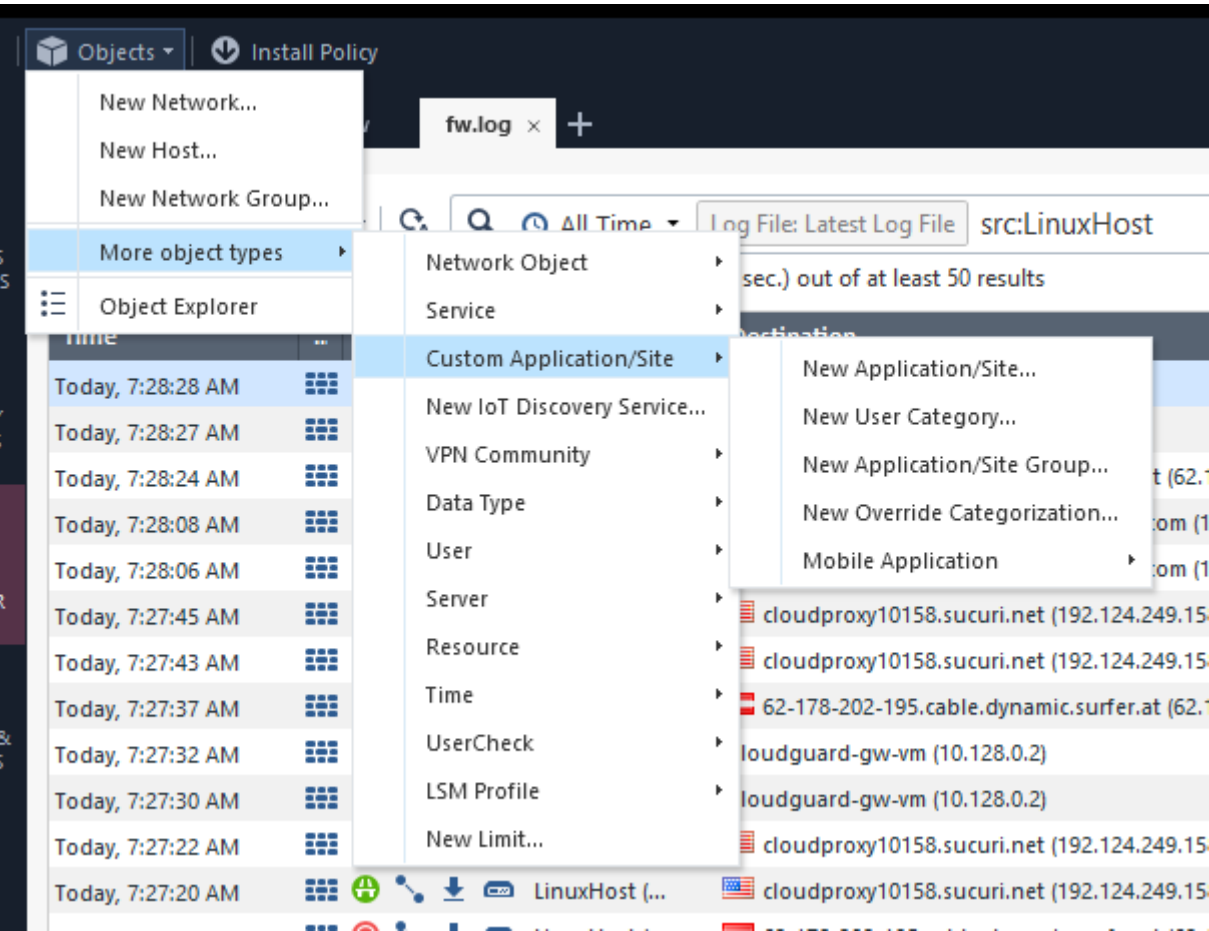
Ticket Number:

Ticket Requester:

Mit HTTPS-Inspection werden die Seiten wie gewuenscht geblockt. Ohne HTTPS-Inspection werden die Seiten angezeigt, im Log wird jedoch ein "drop" hinterlegt. Ohne HTTPS-Inspection ist das Blockieren von Webseiten nicht zuverlaesslich moeglich.

### 3.2: URL Filtering

Unter Objects



wurde folgendes Obejkt erstellt

New Application/Site

Technikum Wien  
Enter Object Comment

General

Additional Categories

General

Primary Category: Custom\_Application\_Site

Description:

Match By

- Services: Web Browsing
- URL List: \*

+ - X

\* ,technikum-wien.at

☐ URLs are defined as Regular Expression

Add Tag

OK Cancel

Man kann nicht sagen, dass man gewisse Kategorien generell blocken wuerde. Es kommt immer auf das Unternehmen und den Wirtschaftszweig in dem man sich befindet. Beispielsweise wuerde ich bei einem Unternehmen wie der Novomatic "Gambling" nicht verbieten aber "Fashion" schon. Umgekehrt waere das bei einem Konzern wie H&M.

Bei einem Antivirus/Antispam Hersteller wie der Ikarus war nichts dergleichen geblockt um den Mitarbeitern ihre Arbeit zu ermoeeglichen.

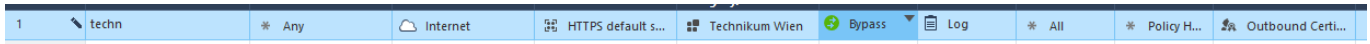
In einem "normalen" Umfeld wuerde ich auf jedenfall alle Kategorien in Betracht ziehen und dann diese freigeben welche in das Geschaeftsfeld des Unternehmens passt. Folgende Auflistung wird jedoch fast immer geblockt:

- Alcohol & Tobacco
- Anonymizer
- Hate /Racism
- Illegal
- Pornography
- Sex
- Spam
- Spyware

- URL Filtering
- Violence

## 3.3 HTTPS Inspection Bypass

Es wurde folgende Bypass Policy erstellt:



Mit dieser Policy kann die Technikumseite wieder aufgerufen werden:

```

#alternat alternate
IFRAME: //www.googletagmanager.com/ns.html?id=GTM-WLP7L7

Direkt zum Inhalt

Technikum Wien Academy Academy Jobportal Jobportal Radio Technikum Radio CIS Login CIS

Search this site
(<i class="fa fa-search"></i>)

* Deutsch
* English

DE

Startseite

Technikum Wien

* Aktuelle Info Coronavirus
* Über uns
* News & Events
* Für Unternehmen
* Für Alumni
* Für Schulen
* Karriere

(BUTTON)
Menu

* Bachelor
  + Biomedical Engineering
  + Elektronik

(NORMAL LINK) Use right-arrow or <return> to activate.
Arrow keys: Up and Down to move. Right to follow a link; Left to go back.
H)elp O)ptions P)rint G)o M)ain screen Q)uit /=search [delete]=history list
[0] 0:lynx*

```

Leider kann mit diesem Browser das Zertifikat nicht angezeigt werden. Es wurde jedoch das Technikum eigene Zertifikat angezeigt und nicht mehr das Proxyzertifikat der Firewall.

Ausnahmen wurde ich externe essentielle Services, besonders wenn diese mit Certificate Pinning arbeiten. Das sind Zum Beispiel Security Systeme (AntiVirus, EDR, ...) oder Mirosoft Services wie Sharepoint oder Office364 zusaetzlich zu Cloudsystemen wie AWS, G-Cloud und Azure.