

# Lab 3

**Author: Benjamin Medicke**

**Topics: Application Control, URL Filtering & HTTPS Inspection Bypass**

[lab1](#) | [lab2](#) | **[lab3](#)** | [lab4](#)

---

- Lab 3.1 Application Control
  - 3.1.1 Aktivieren der Blades: Application Control & URL Filtering
  - 3.1.3 Vorhandene Policy anpassen
  - 3.1.6 Update
  - 3.1.7 Anlegen einer Application Control Policy
  - 3.1.9 Policy auf Linux Instanz testen
  - 3.1.10 Zugriff auf Google Maps verbieten
  - Aufgetretene Probleme
- Lab 3.2 URL Filtering
  - 3.2.1 Neue Applikation erstellen
  - 3.2.3 Drop Policy für das Technikum erstellen
  - 3.2.4 Testen der Drop Policy
- Lab 3.3 HTTPS Inspection Bypass
  - Aufgetretene Probleme
  - 3.3.2 Erstellen einer Bypass Rule für das Technikum
  - 3.3.3 Testen des Zugriffs und Analyse des Zertifikates
  - 3.3.4 Welche Kategorien von Seiten kommen in einem Unternehmen in Frage?
  - Aufgetretene Probleme

## Lab 3.1 Application Control

### 3.1.1 Aktivieren der Blades: Application Control & URL Filtering

Network Security (3) Threat Prevention (2) Management (3)

Access Control:

- ☒ Firewall
- ☐ IPSec VPN
  - ☐ Policy Server
- ☐ Mobile Access
- ☒ Application Control
- ☒ URL Filtering

Advanced Networking & Clustering:

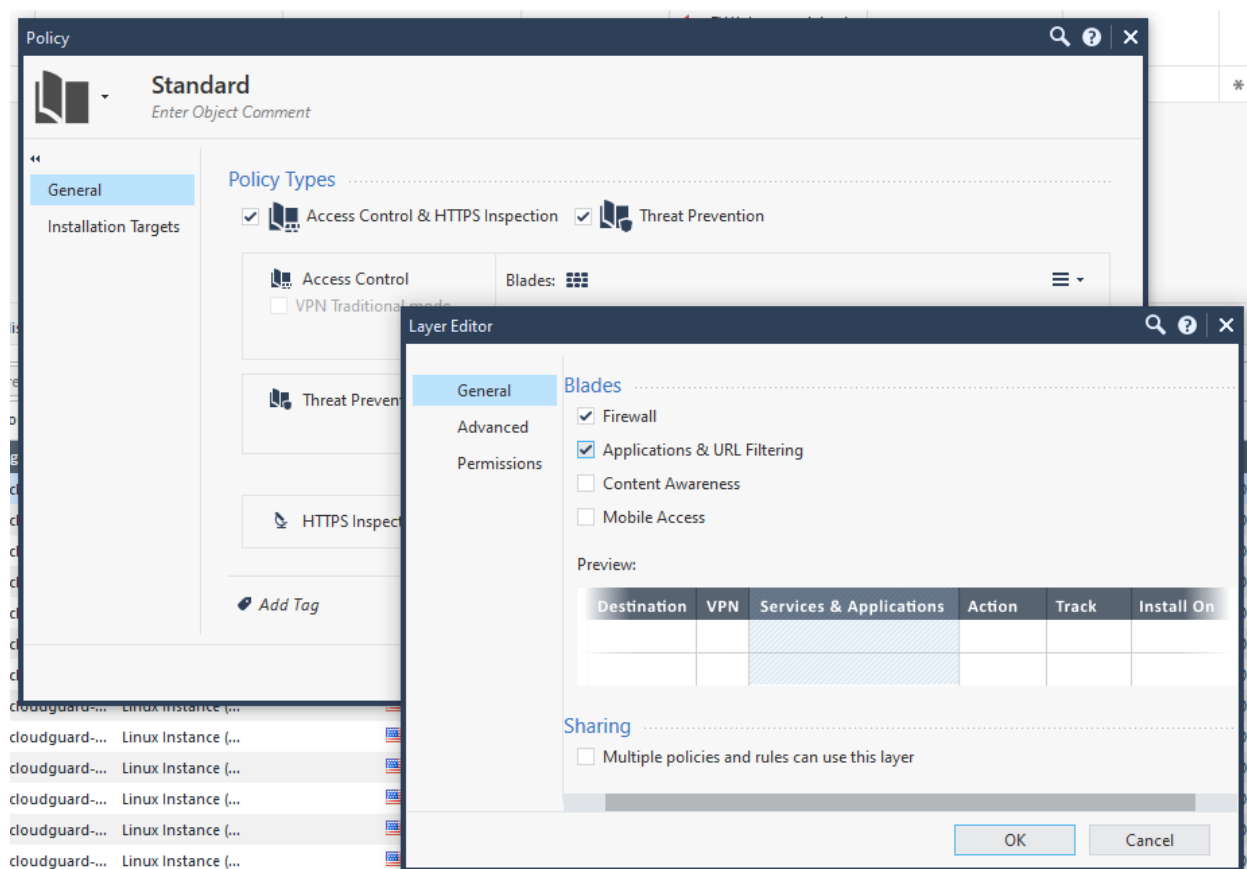
- ☒ Dynamic Routing
- ☒ SecureXL
- ☐ QoS
- ☐ Monitoring

Other:

- ☐ Data Loss Prevention

Aktivieren der "URL Filtering" und "Application Control" Blades

### 3.1.3 Vorhandene Policy anpassen



Editierter Access Control Layer

**Install Policy Details**

**Task Details**

Task: **Policy installation - Standard**  
 Initiator: **admin**  
 Start Time: **15/05/2021 17:20**  
 Last Updated: **15/05/2021 17:20**

**Task Progress**

Status: 75% Policy installation in progress

Search...

Gateway	Gateway IP	Policy Type	Policy Name	Version	Status
cloudguard-gw-vm	10.186.0.3	Access Control Policy	Standard	R80.40	Installation in progress
cloudguard-gw-vm	10.186.0.3	Threat Prevention Policy	Standard	R80.40	Succeeded

Installieren der Policy

### 3.1.6 Update

**Application Control & URL Filtering Update Summary**

**Task Details**

Task: **Application Control & URL Filtering**  
 Initiator: **admin**  
 Start Time: **15/05/2021 17:35**  
 Last Updated: **15/05/2021 17:35**

**Task Progress**

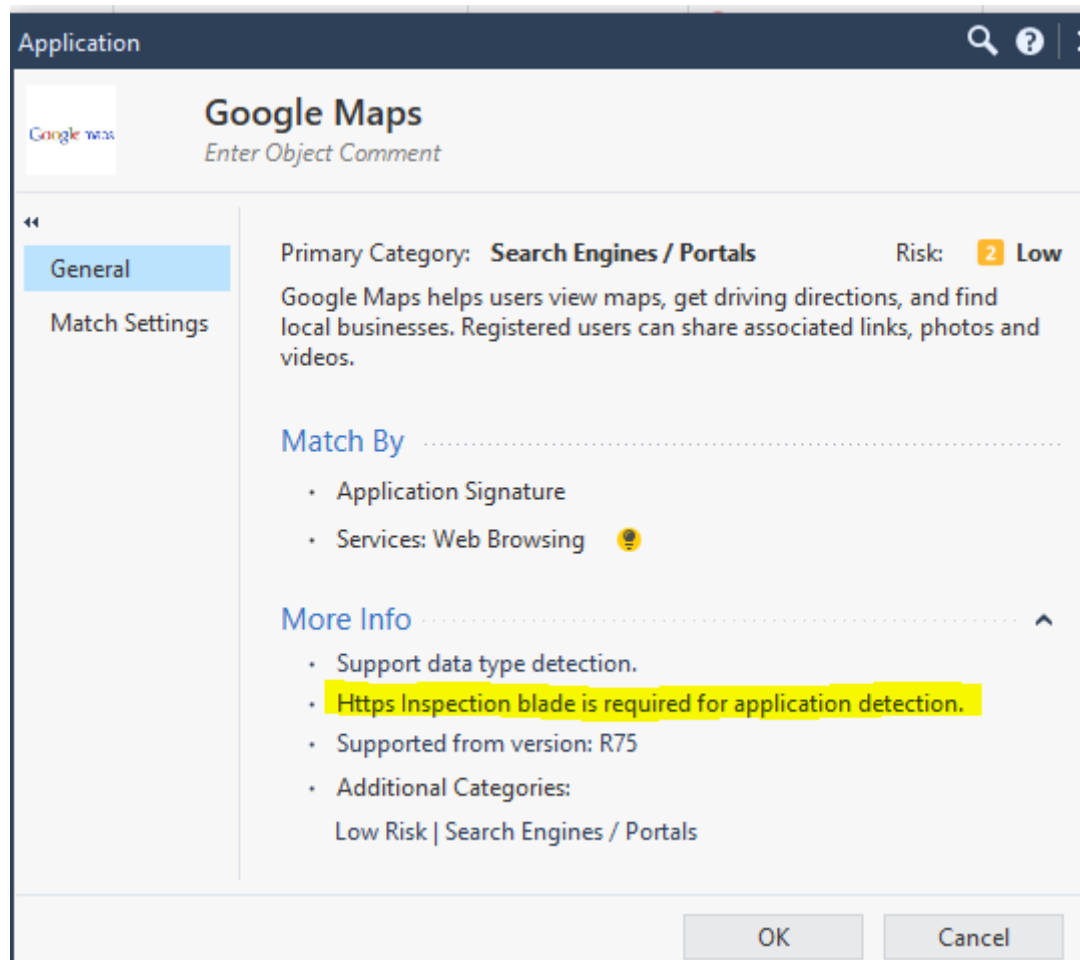
Status: 30% Downloading update package...

Update Application Control & URL Filtering

### 3.1.7 Anlegen einer Application Control Policy

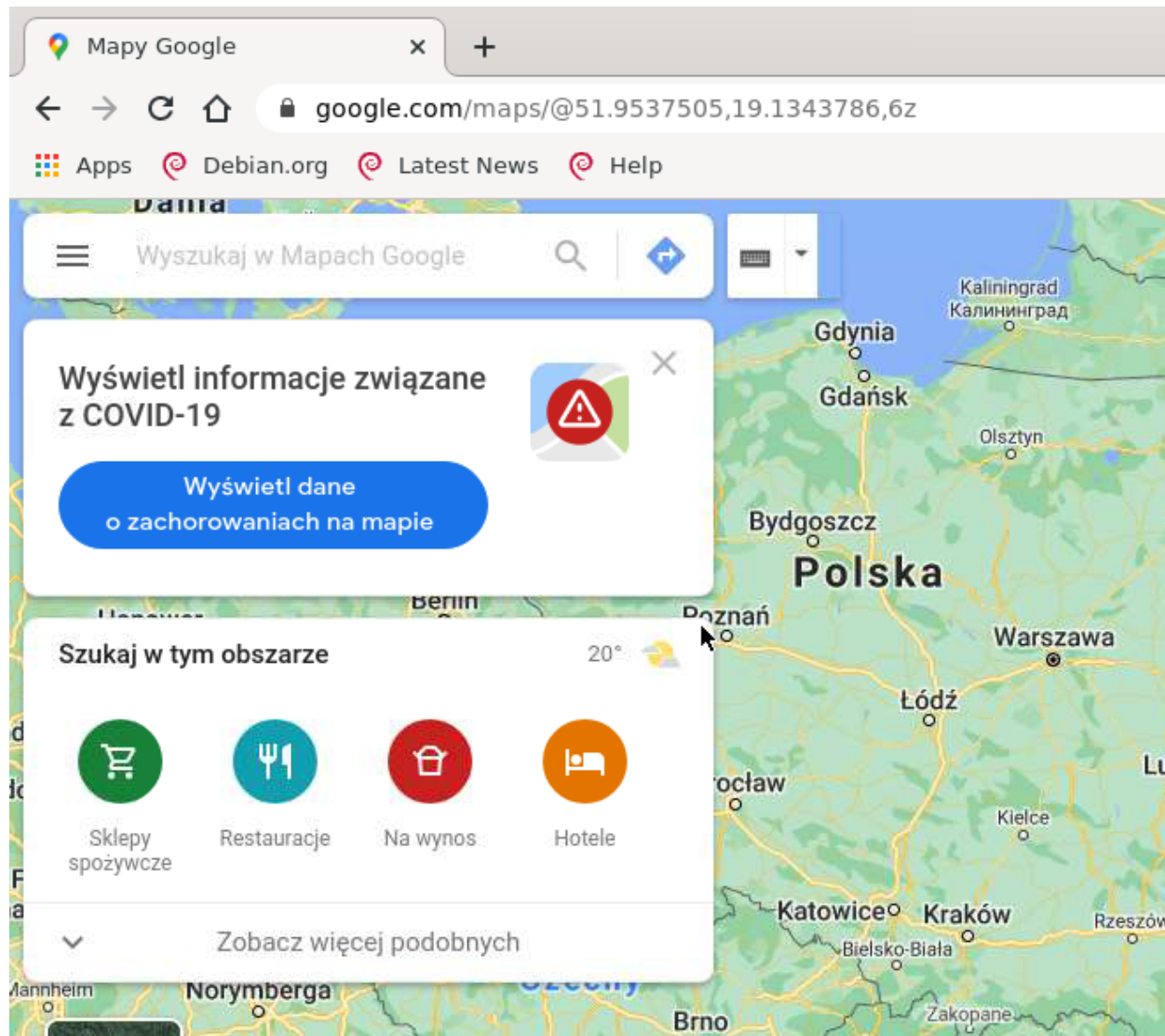
1	No Google Maps for you	Linux instance	* Any	* Any	Google Maps	Drop Blocked Message - Access C...	Log Accounting	* Policy Targets
---	------------------------	----------------	-------	-------	-------------	---------------------------------------	-------------------	------------------

Policy um Google Maps zu verbieten

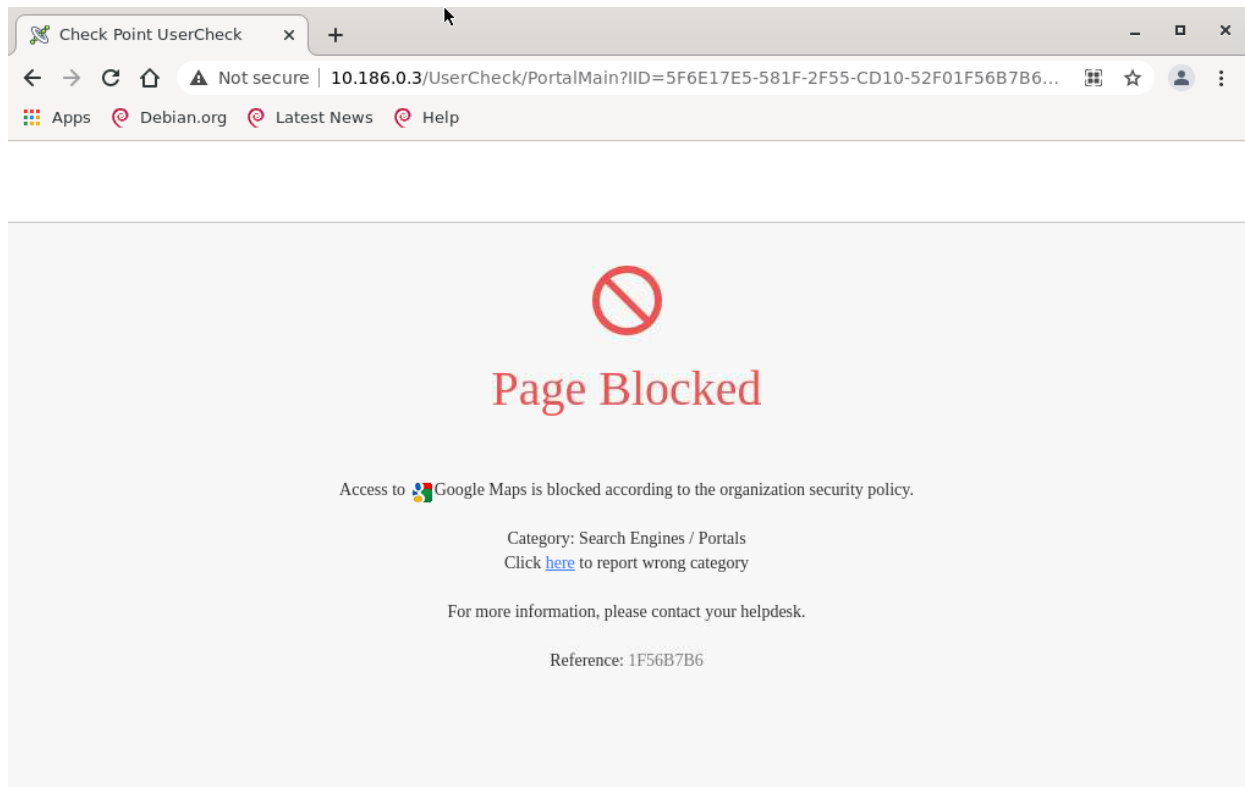


Google Maps benötigt HTTPS Inspection.

### 3.1.9 Policy auf Linux Instanz testen

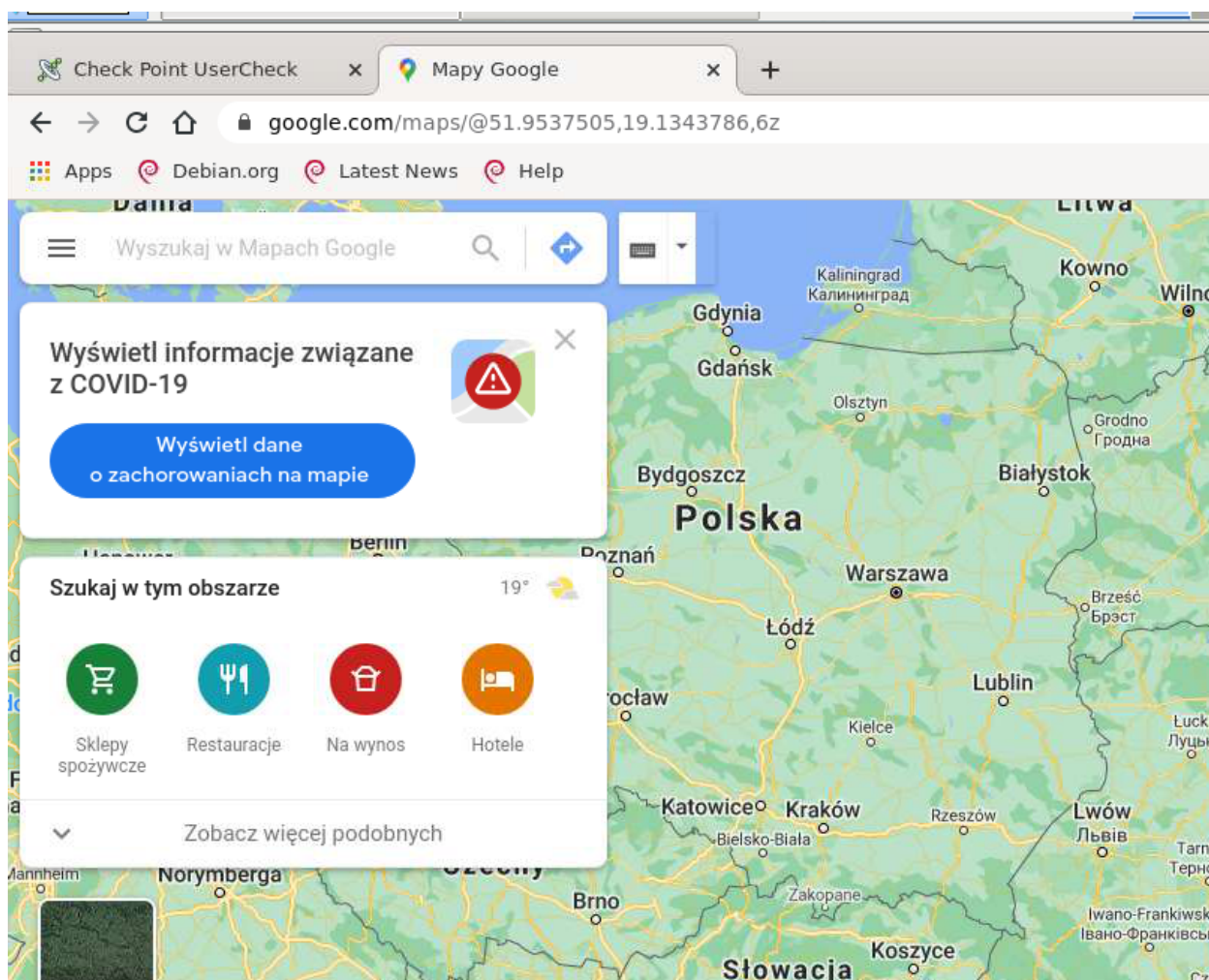


Vor Installation der Policy geht Google Maps einwandfrei



Nach Installation wird die Seite geblockt

### 3.1.10 Zugriff auf Google Maps verbieten



Nach Deaktivieren der HTTPS Inspektion ist die Seite (über HTTPS) wieder erreichbar. Dies ist der Fall, weil die Subdomain der Firewall gegenüber nicht offen gelegt wird.

## Aufgetretene Probleme

Es sind keine Probleme aufgetreten.

## Lab 3.2 URL Filtering

New Application/Site

Technikum  
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

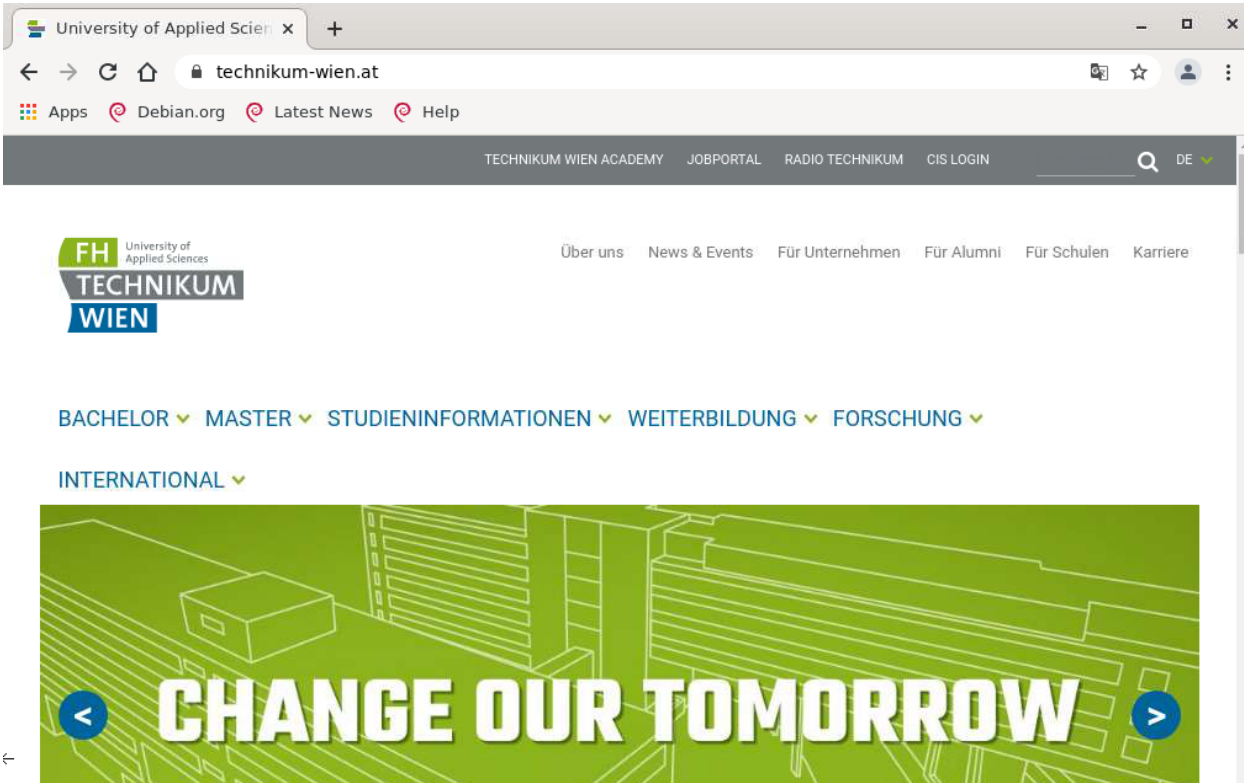
Add Tag

OK Cancel

Neues Application/Site Objekt

### 3.2.1 Neue Applikation erstellen



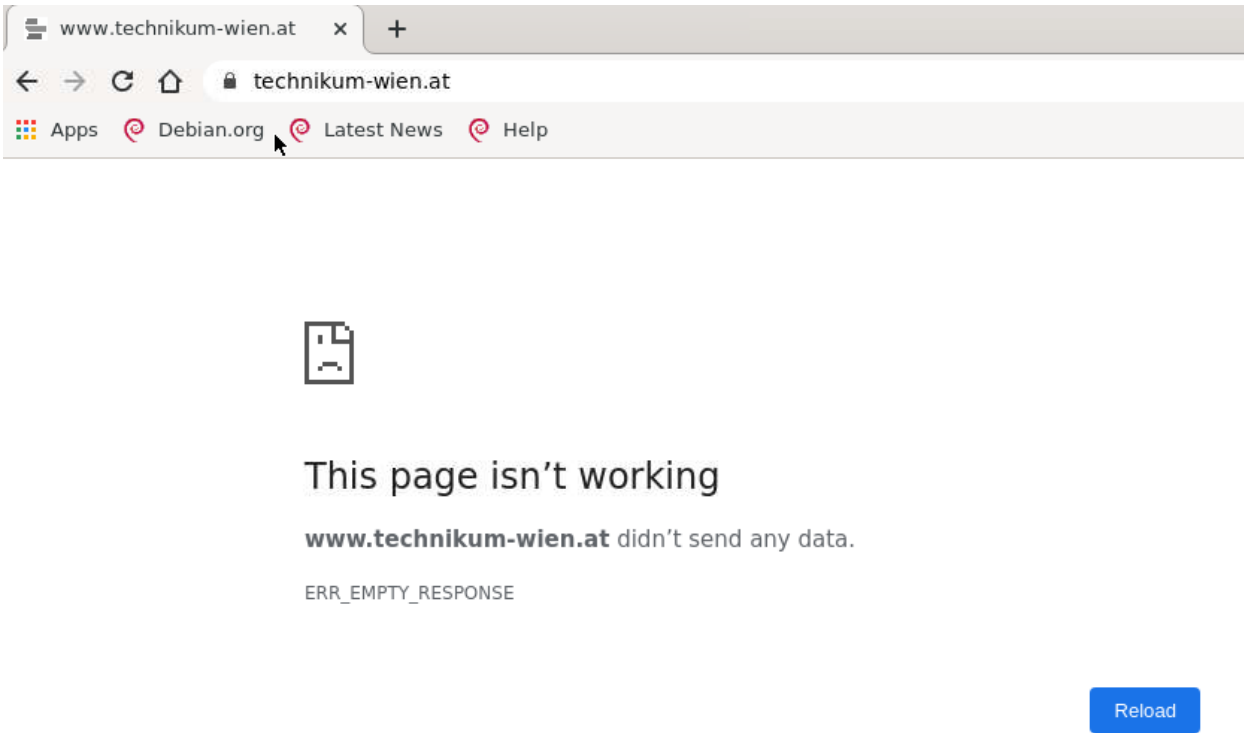


Zugriff ist noch möglich

### 3.2.3 Drop Policy für das Technikum erstellen

No.	Name	Source	Destination	VPN	Services & Applications	Action	Track	Install On
1	No Technikum for you	* Any	* Any	* Any	Technikum	Drop	Log Accounting	* Policy Targets

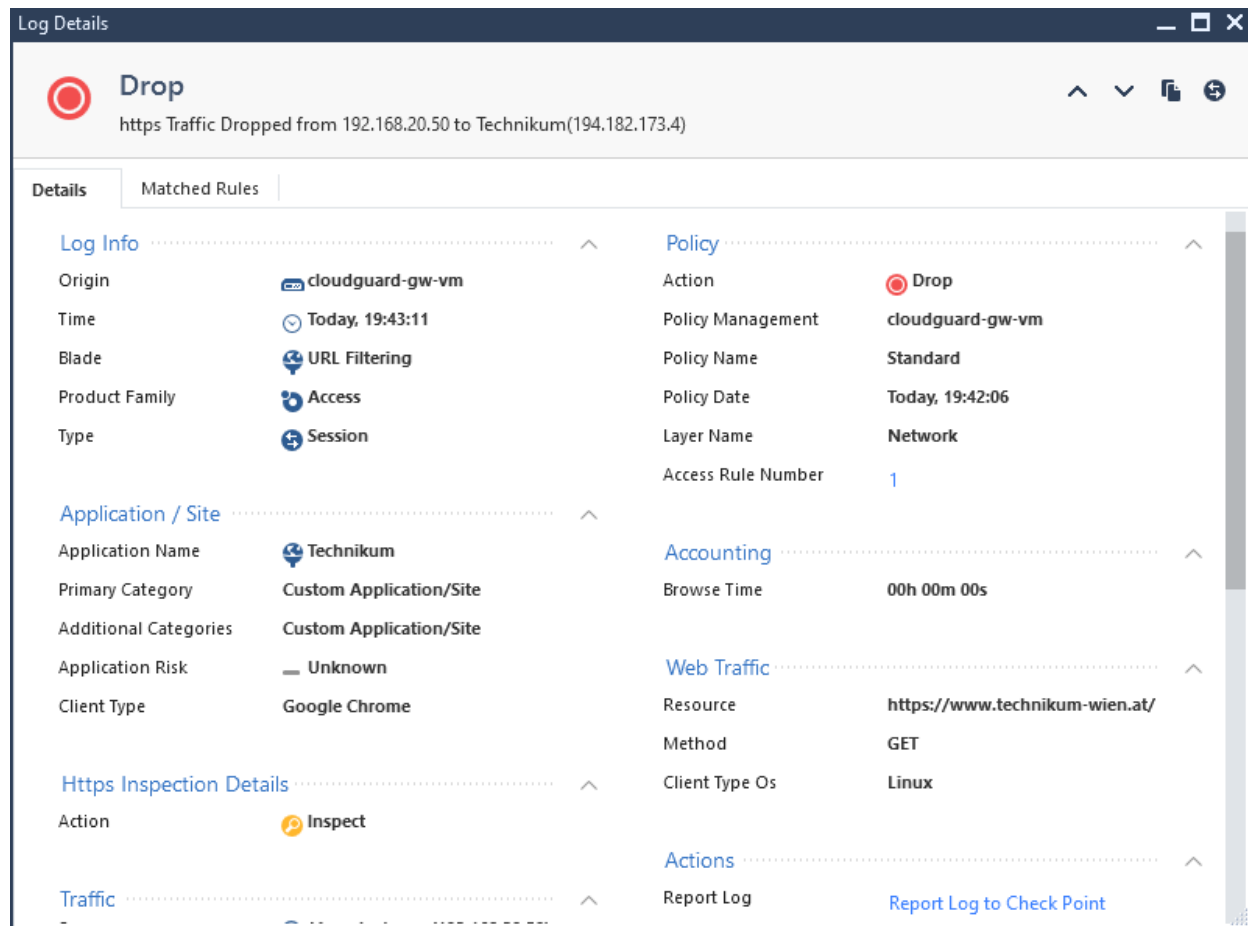
Drop Policy: Technikum





Nach Installation: Die Policy funktioniert

### 3.2.4 Testen der Drop Policy



Detailansicht des Blockeintrages

*Welche URL Kategorien von Seiten würden Sie blockieren?*

Persönlich würde ich nur Webseiten blocken, die eine sicherheitstechnische Gefahr darstellen. Aus Produktivitätsgründen kann es je nach Unternehmen gewünscht sein zusätzlich die folgenden Kategorien zu blocken:

- anstößliche Inhalte (Wettseiten, Pornographie)
- Social Media
- Spiele Seiten
- Musik/Video Streaming Seiten
- etc.

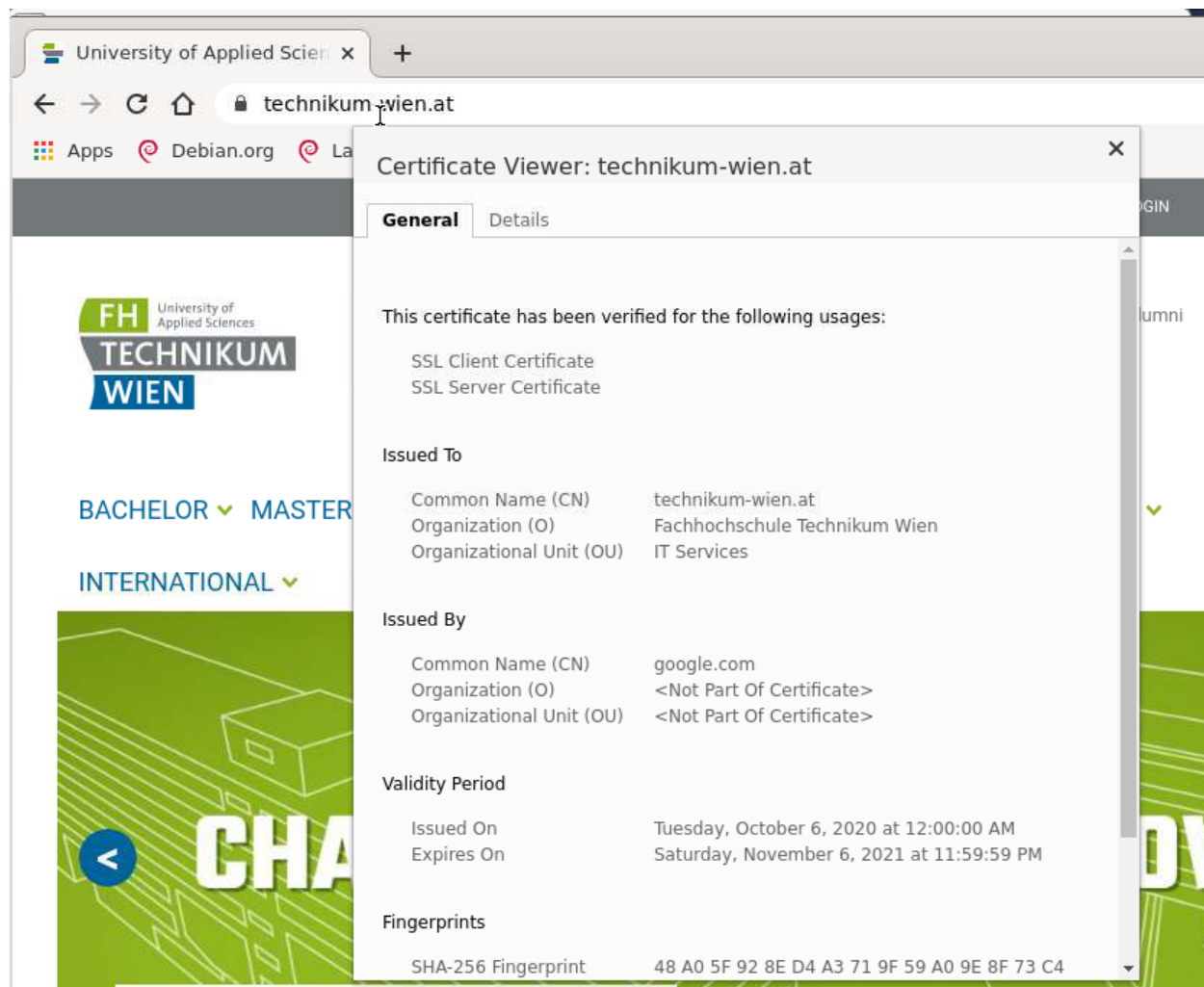
Wobei das produktivitätstechnisch vermutlich keinen positiven Einfluss hat. Geblockte Seiten haben negative Auswirkungen auf die Motivation und Moral der

Mitarbeiter. Facebook wird sonst einfach am Handy geöffnet. Im Schlimmsten Fall führt es sogar zu einer Schatten-IT.

## Aufgetretene Probleme

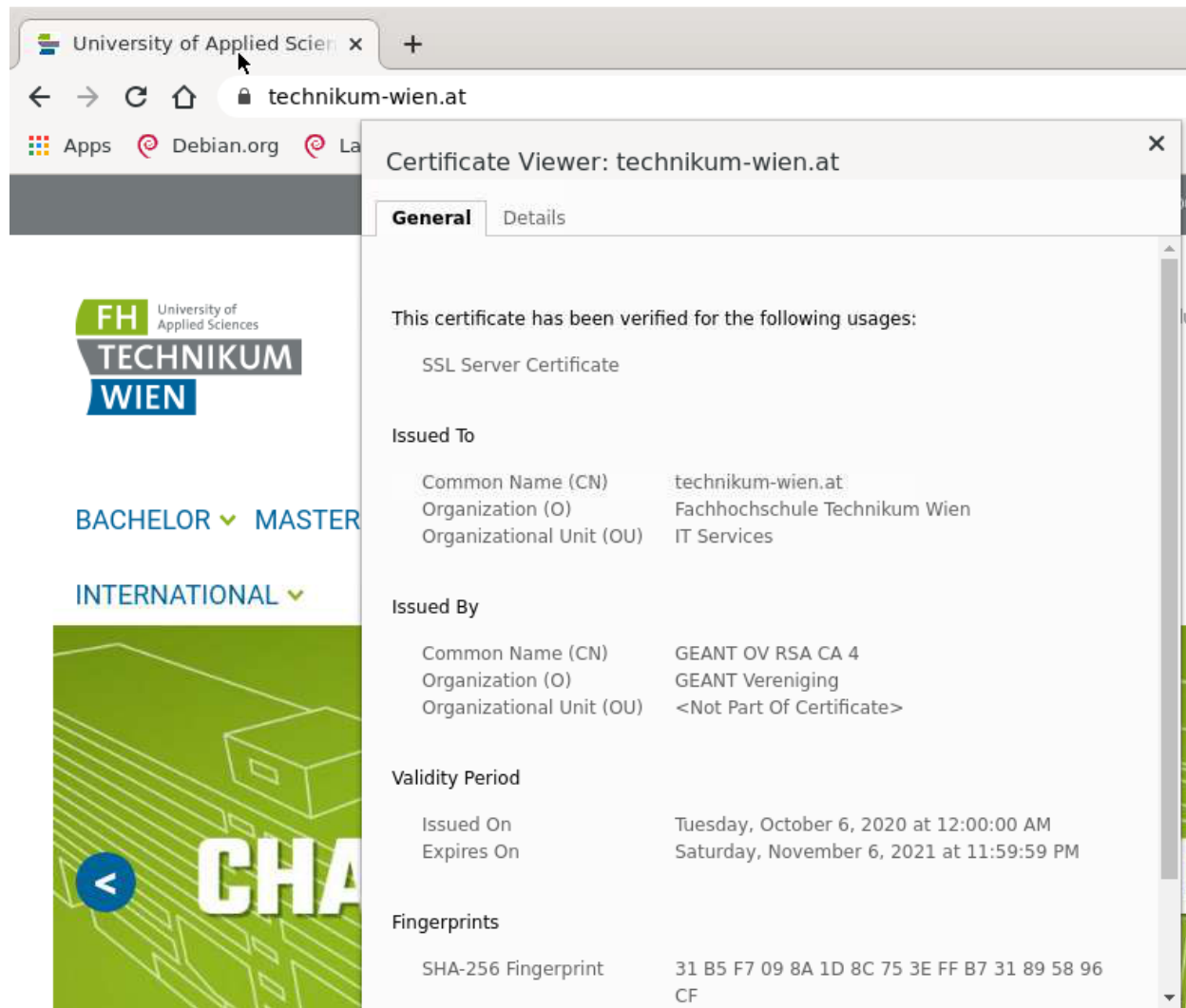
Es sind keine Probleme aufgetreten.

## Lab 3.3 HTTPS Inspection Bypass



Vor Bypass Regel. Man sieht der Issuer ist Google.com (was ich als Wert im self-signed Certificate eingestellt habe)

## 3.3.2 Erstellen einer Bypass Rule für das Technikum



Nach Bypass wird das Original Zertifikat verwendet. Vergleiche "Issued By" mit vorherigem Screenshot.

### 3.3.3 Testen des Zugriffs und Analyse des Zertifikates

**Log Details**

**HTTPS Bypass**  
HTTPS Bypassed

**Log Info**

- Log Server Origin: cloudguard-gw-vm (10.186.0.3)
- Origin: cloudguard-gw-vm
- Time: Today, 20:22:25
- Blade: HTTPS Inspection
- Product Family: Network
- Type: Log

**HTTPS Inspection**

- HTTPS Inspection Action: Bypass
- HTTPS Inspection Rule N...: Private Technikum
- HTTPS Inspection Rule ID: 8FF4450A-84C0-463D-A74C-6F76B6F... [more](#)

**Traffic**

- Source: Linux Instance (192.168.20.50)
- Source Port: 46170
- Service: https (TCP/443)
- Interface Direction: inbound
- Interface Name: eth1

**Policy**

- Action: HTTPS Bypass
- Policy Management: cloudguard-gw-vm
- Policy Name: Standard
- Policy Date: Today, 20:16:26

**Actions**

- Report Log: [Report Log to Check Point](#)

**More**

- Id: 0aba0003-6ca7-0114-60a0-1161000b0... [more](#)
- Marker: @A@@B@1621090464@C@5753
- Id Generated By Indexer: false
- First: true
- Sequencenum: 1
- Db Tag: {BE9CB3A6-84FF-6D40-90FA-7BFB48... [more](#)
- Description: HTTPS Bypassed

HTTPS Inspection Bypass für die Technikum Seite funktioniert

### 3.3.4 Welche Kategorien von Seiten kommen in einem Unternehmen in Frage?

*Welche Seiten oder Kategorien von Seiten würden Sie in der HTTPS Inspection ausnehmen, daher bypassen?*

Jegliche Seiten, die private Daten übermitteln:

- private Kommunikation
- Regierungsseiten
- Medizinische Seiten
- Finanzseiten

### Aufgetretene Probleme

Es sind (glücklicherweise ein weiteres Mal) keine Probleme aufgetreten.

nächstes Lab

