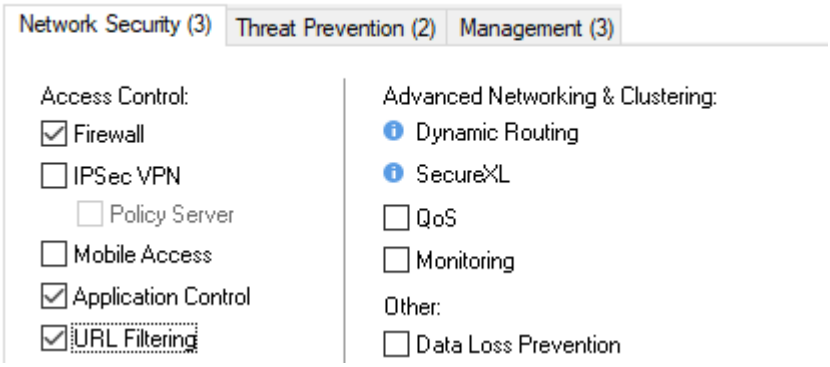
Lab 3

Author: Benjamin Medicke
Topics: Application Control, URL Filtering & HTTPS Inspection Bypass

lab1 | lab2 | **lab3** | lab4

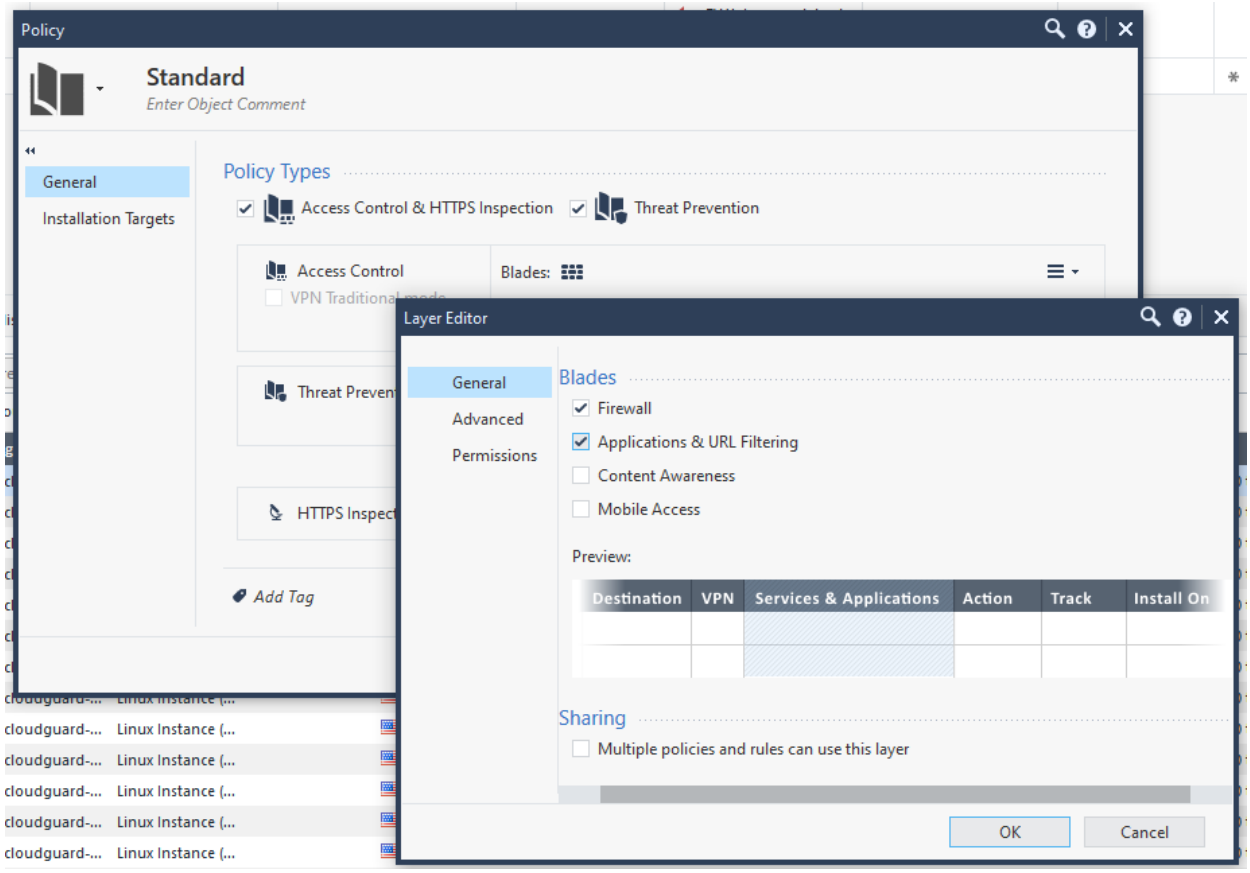
Lab 3.1 Application Control

3.1.1 Aktivieren der Blades: Application Control & URL Filtering

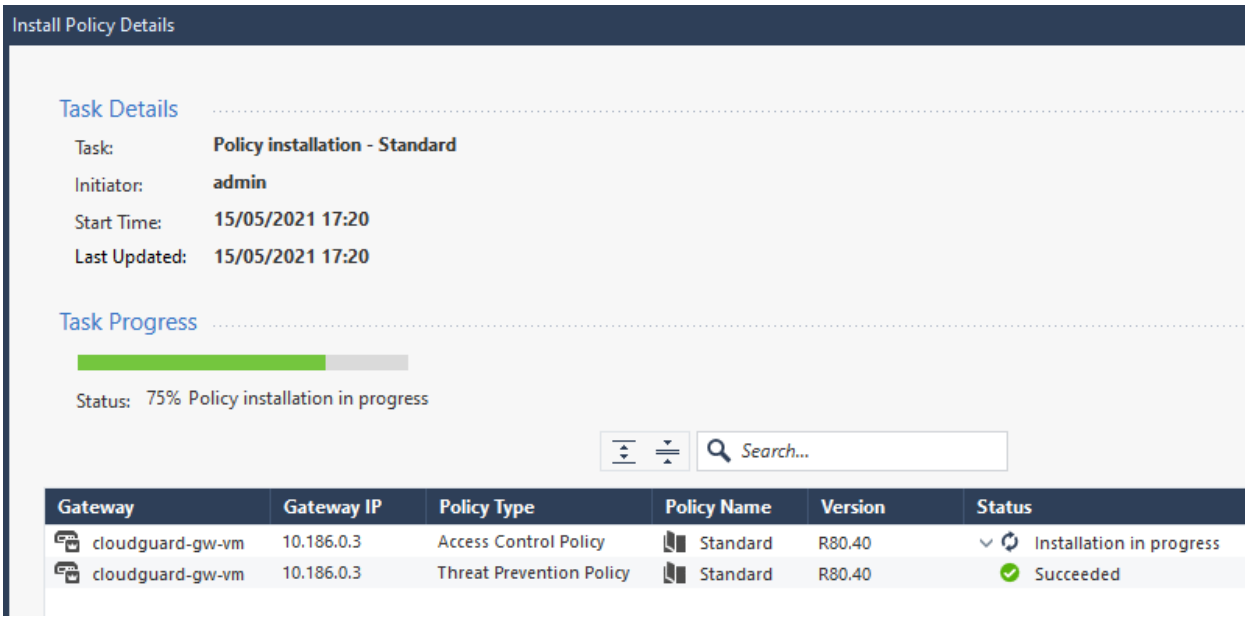


Aktivieren der "URL Filtering" und "Application Control" Blades

3.1.3 Vorhandene Policy anpassen

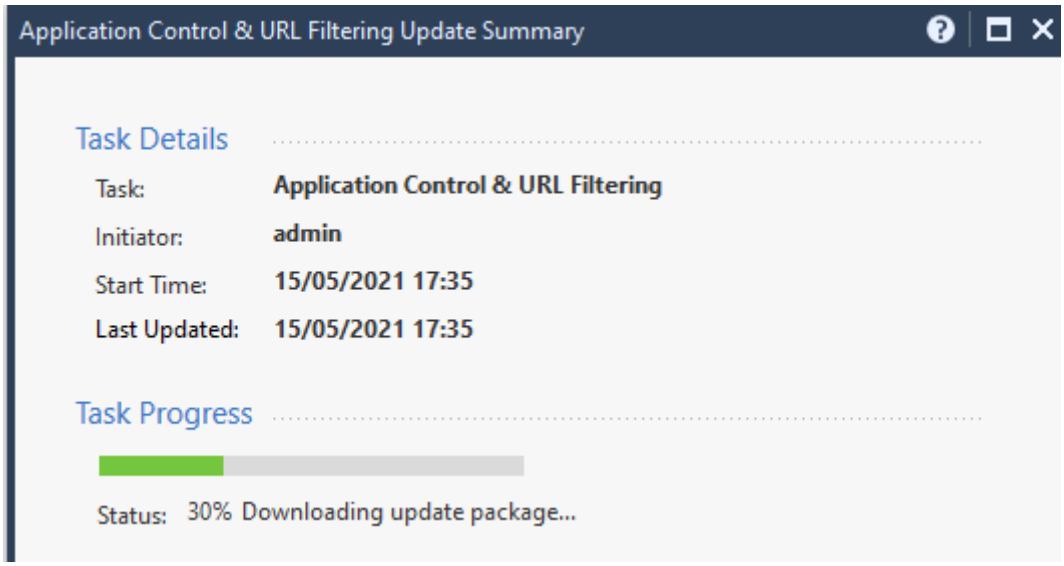


Editierter Access Control Layer



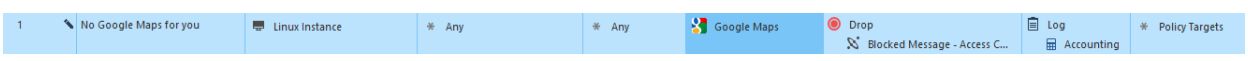
Installieren der Policy

3.1.6 Update

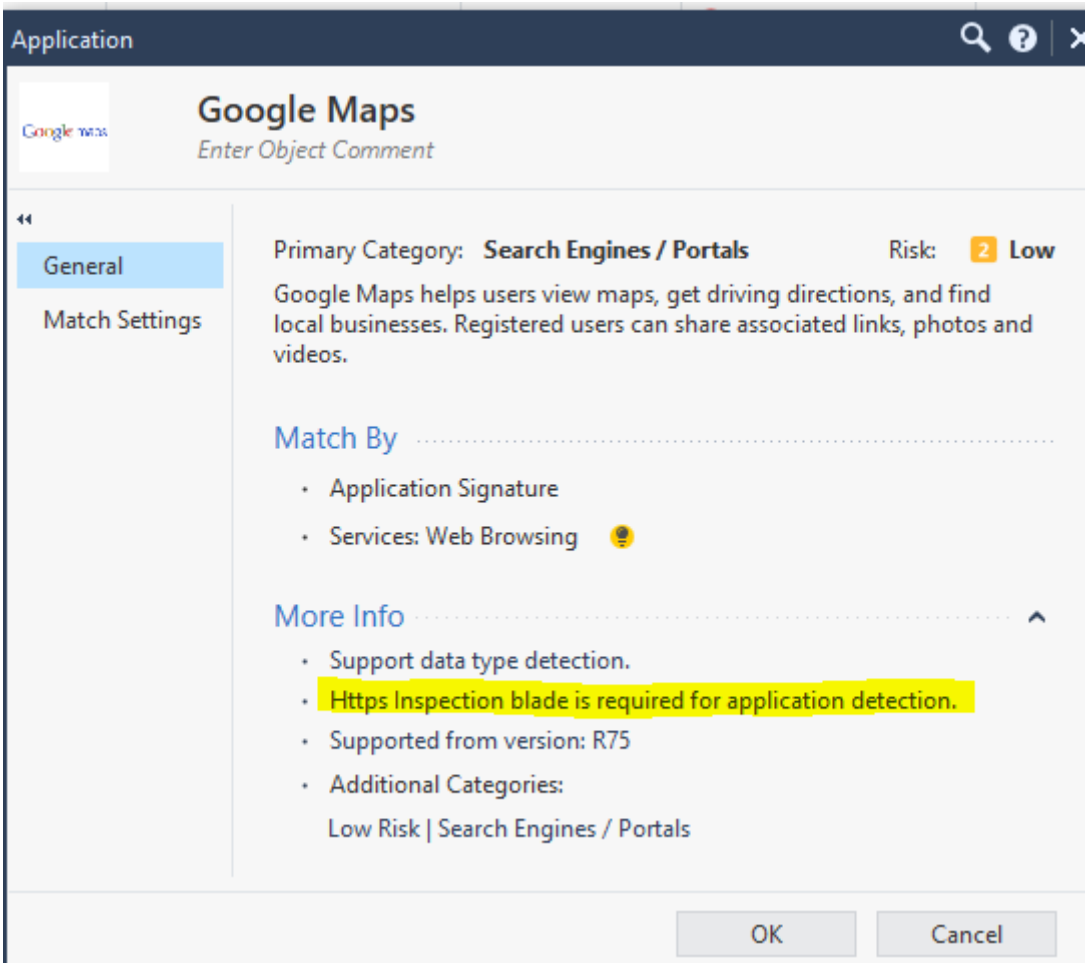


Update Application Control & URL Filtering

3.1.7 Anlegen einer Application Control Policy

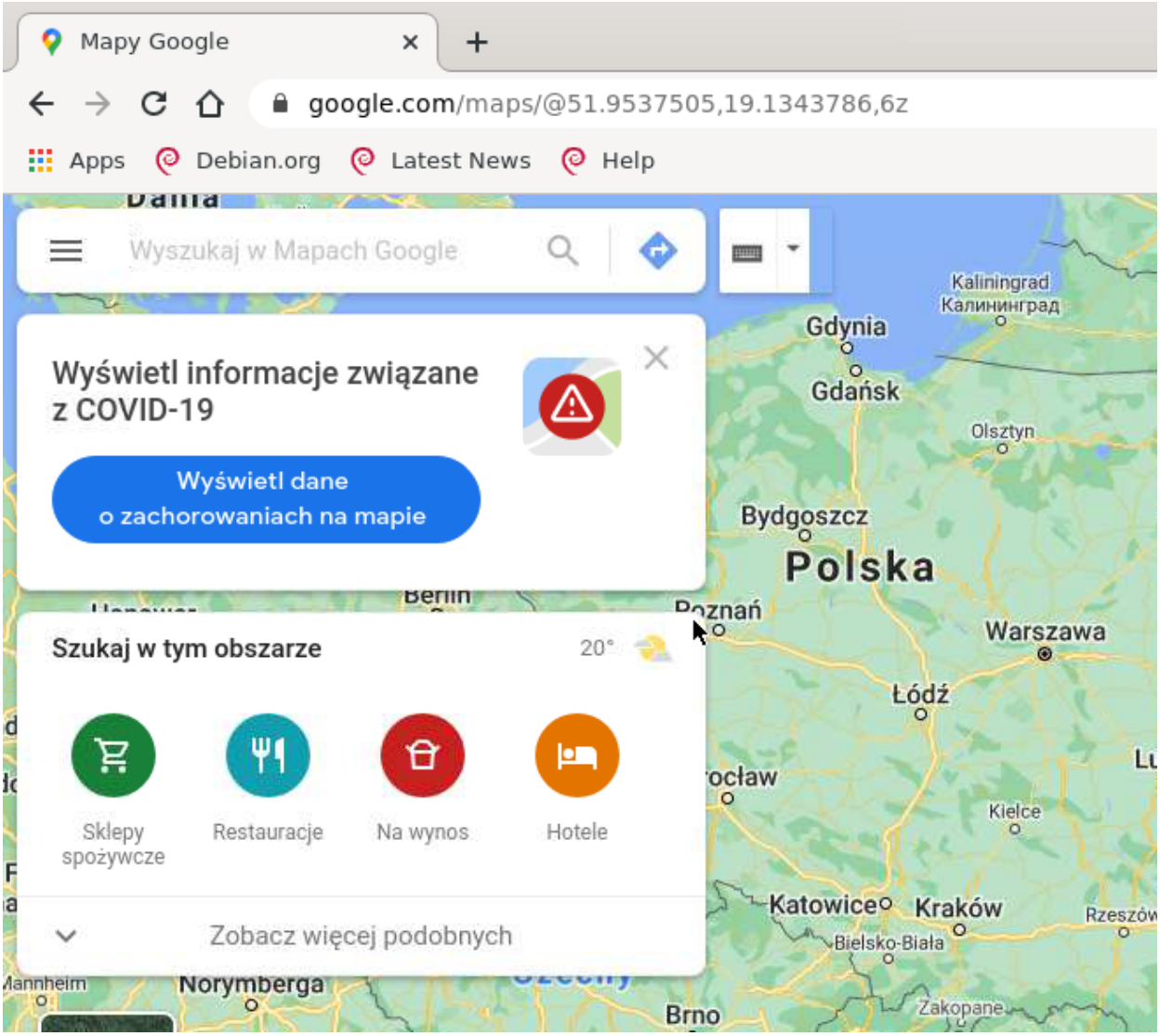


Policy um Google Maps zu verbieten

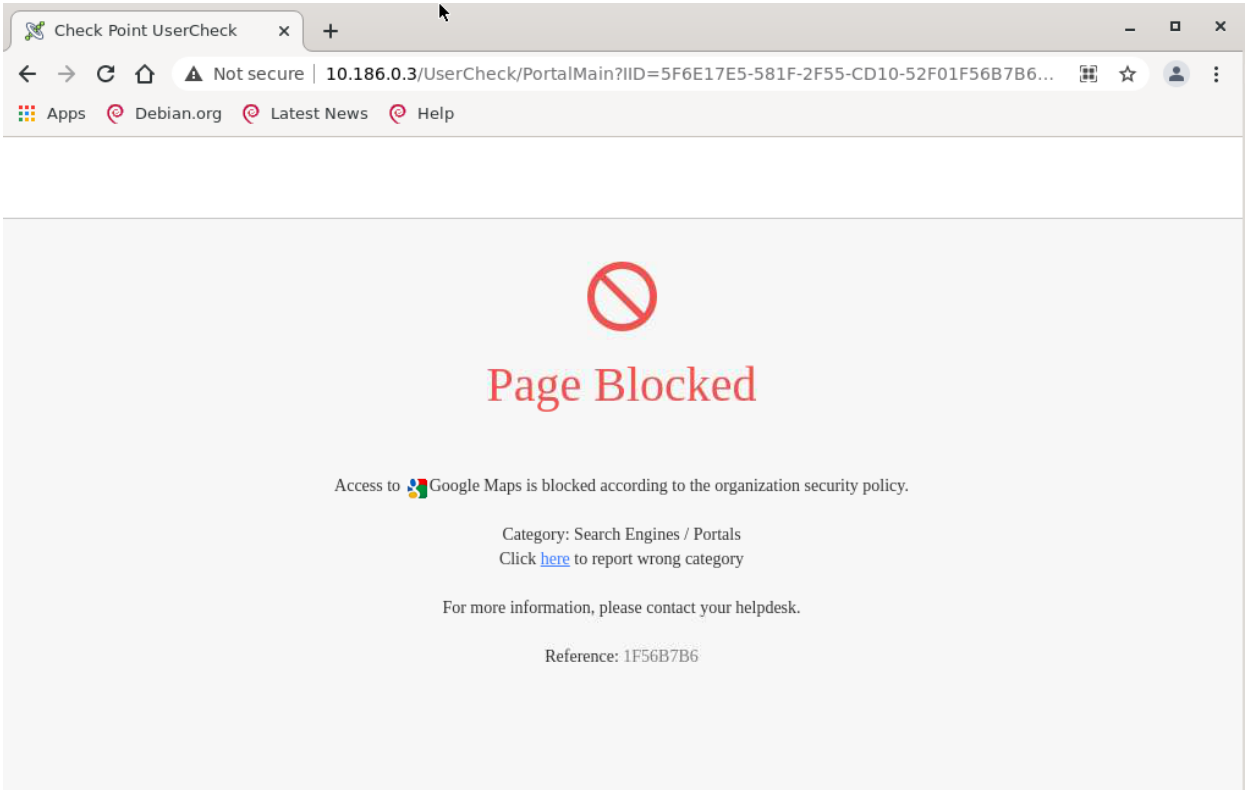


Google Maps benötigt HTTPS Inspection.

3.1.9 Policy auf Linux Instanz testen

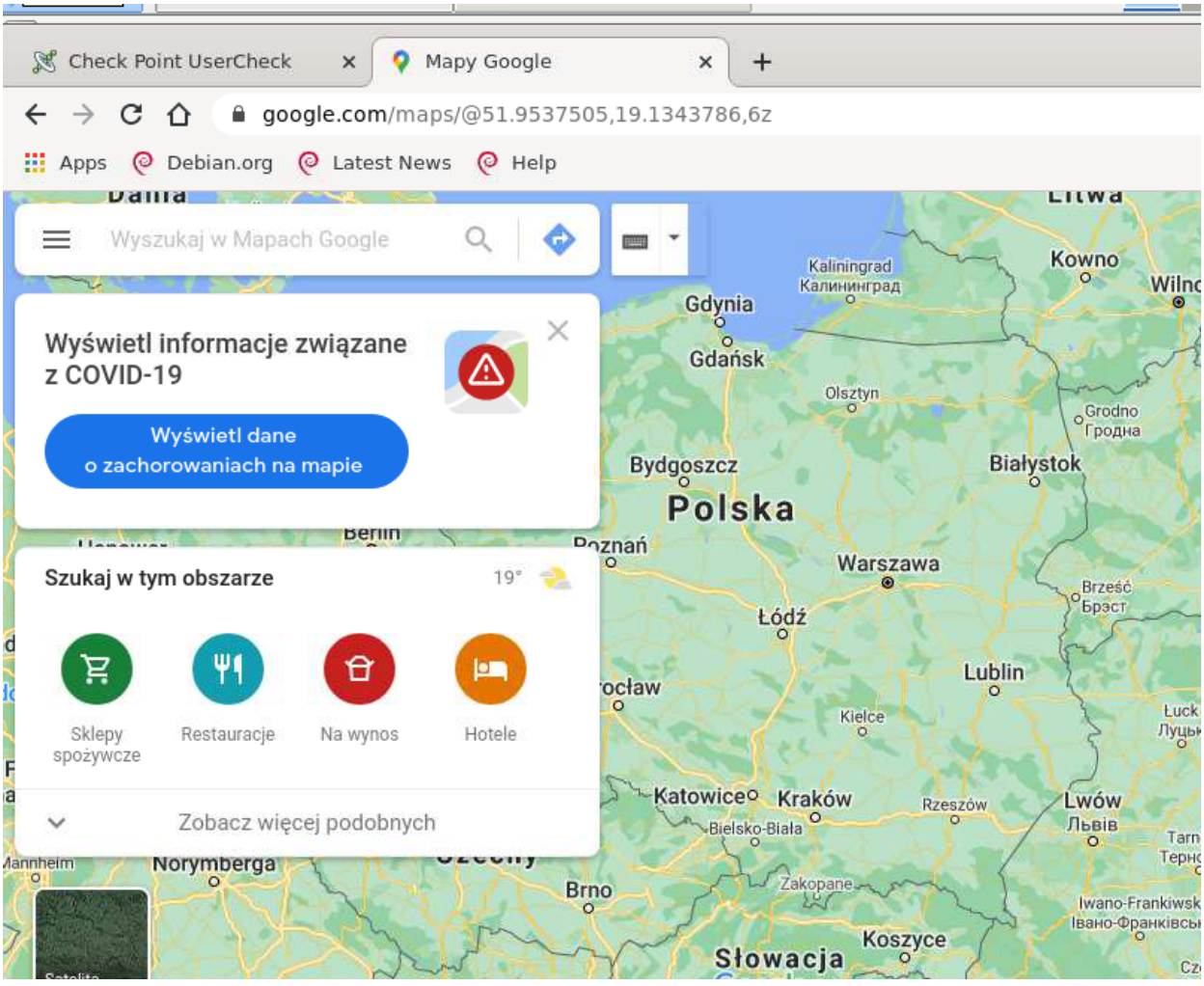


Vor Installation der Policy geht Google Maps einwandfrei



Nach Installation wird die Seite geblockt

3.1.10 Zugriff auf Google Maps verbieten

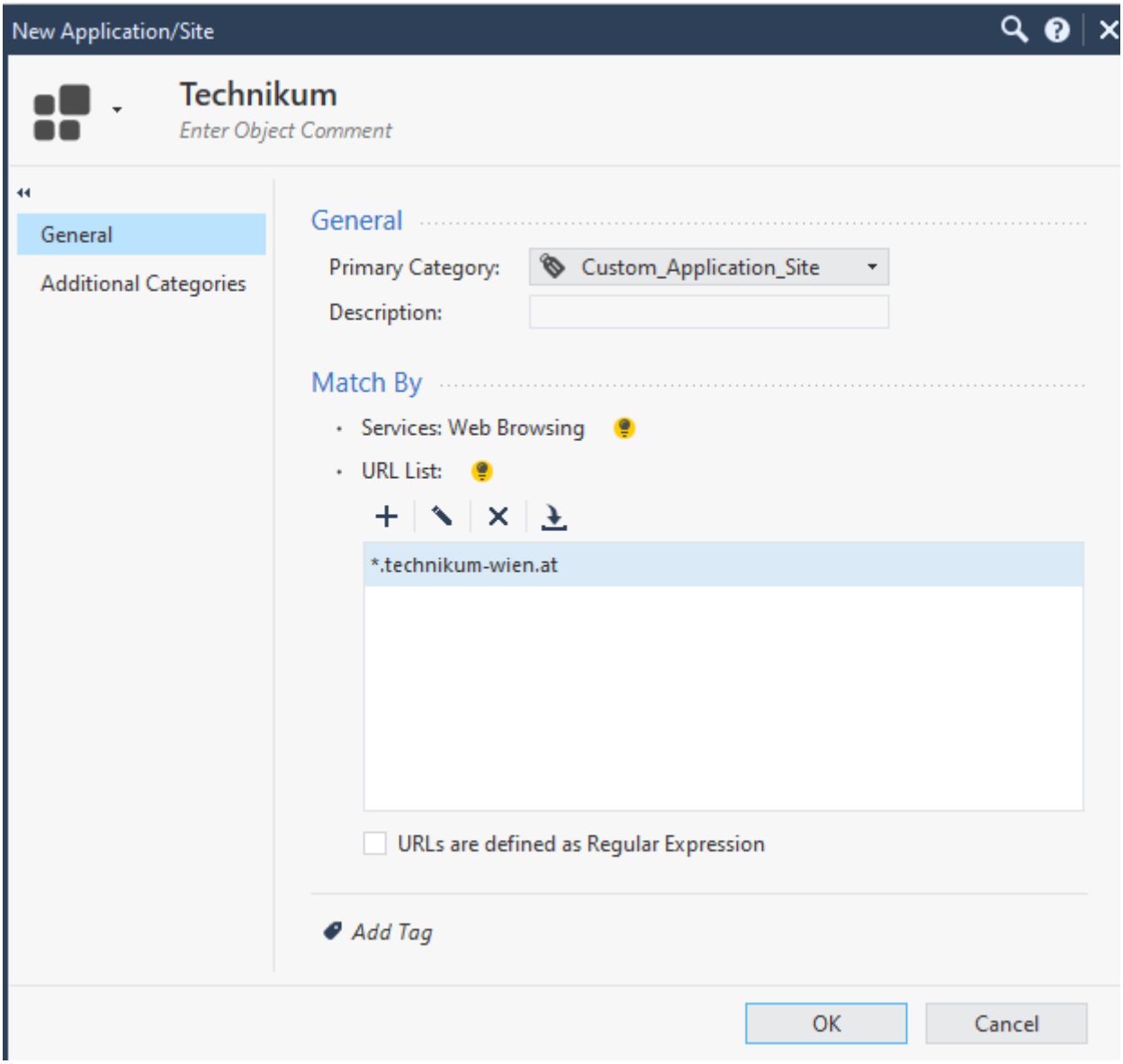


Nach Deaktivieren der HTTPS Inspektion ist die Seite (über HTTPS) wieder erreichbar. Dies ist der Fall, weil die Subdomain der Firewall gegenüber nicht offen gelegt wird.

Aufgetretene Probleme

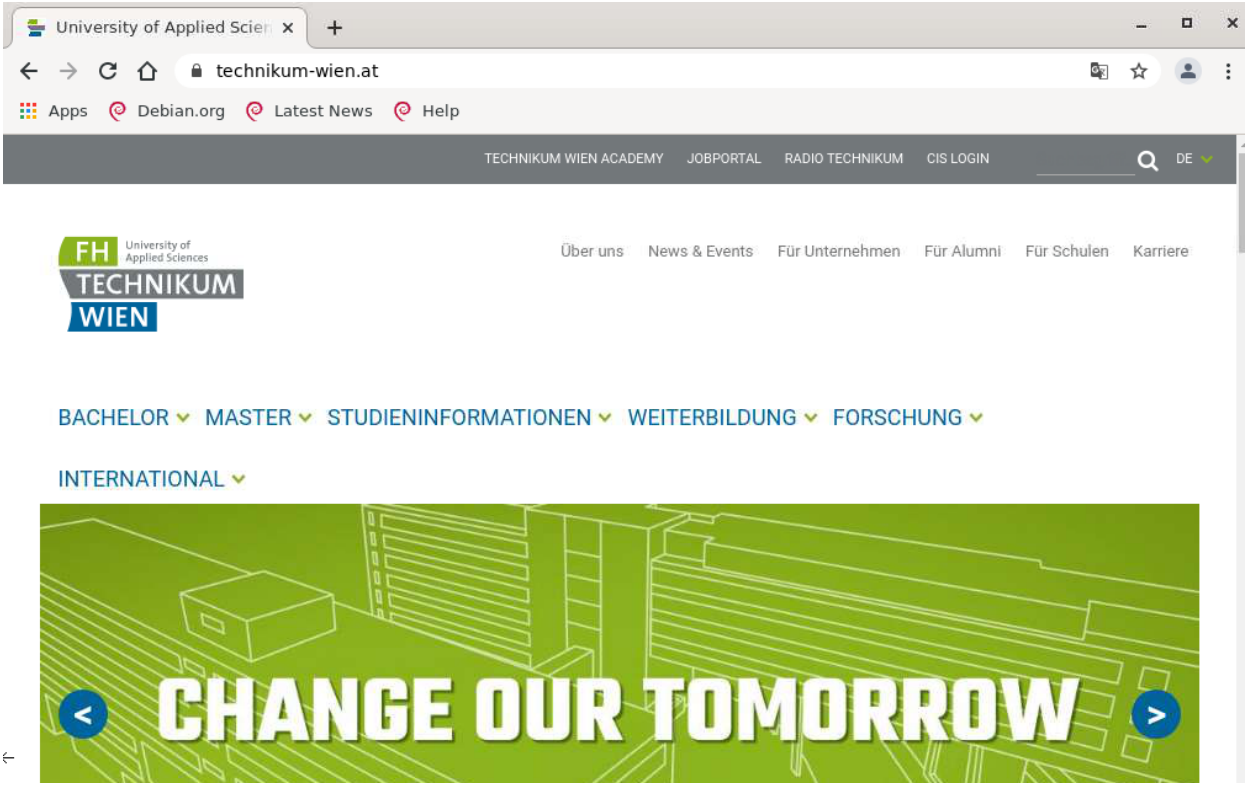
Es sind keine Probleme aufgetreten.

Lab 3.2 URL Filtering



Neues Application/Site Objekt

3.2.1 Neue Applikation erstellen

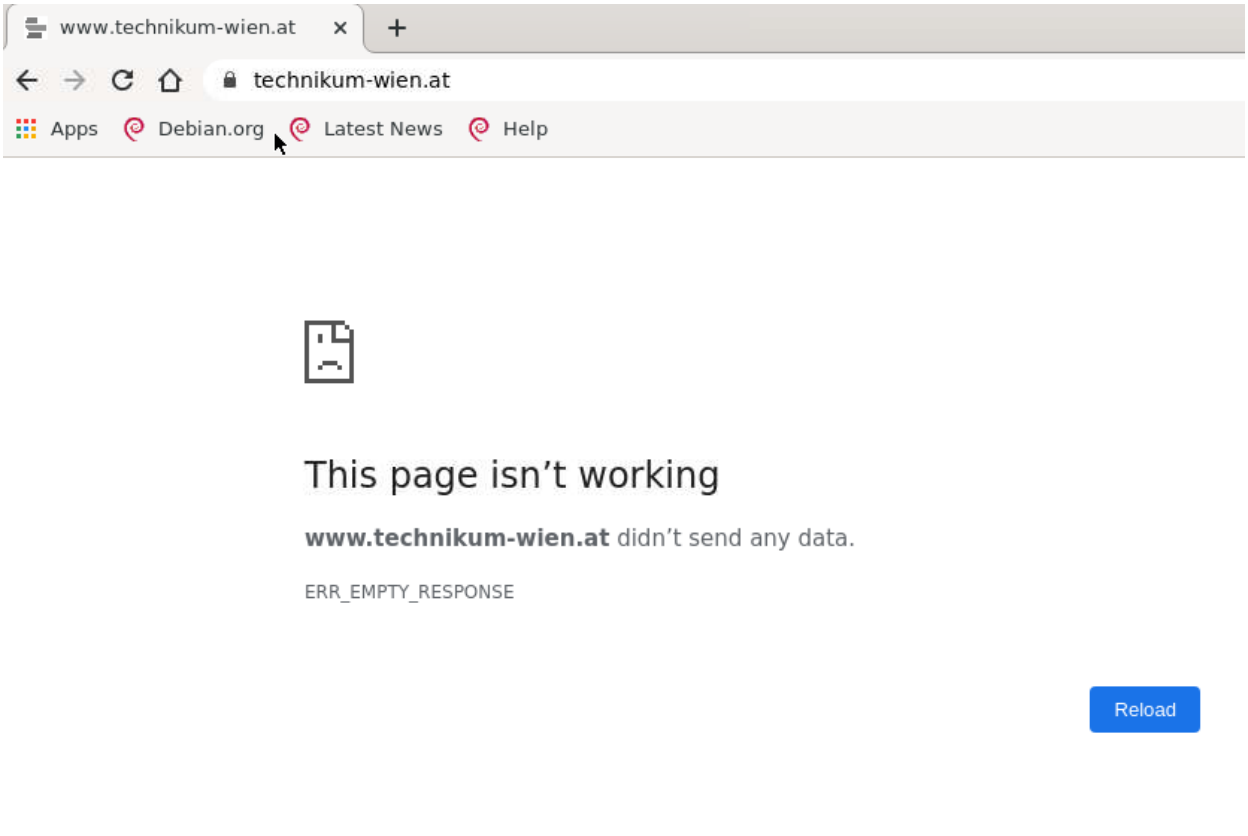


Zugriff ist noch möglich

3.2.3 Drop Policy für das Technikum erstellen

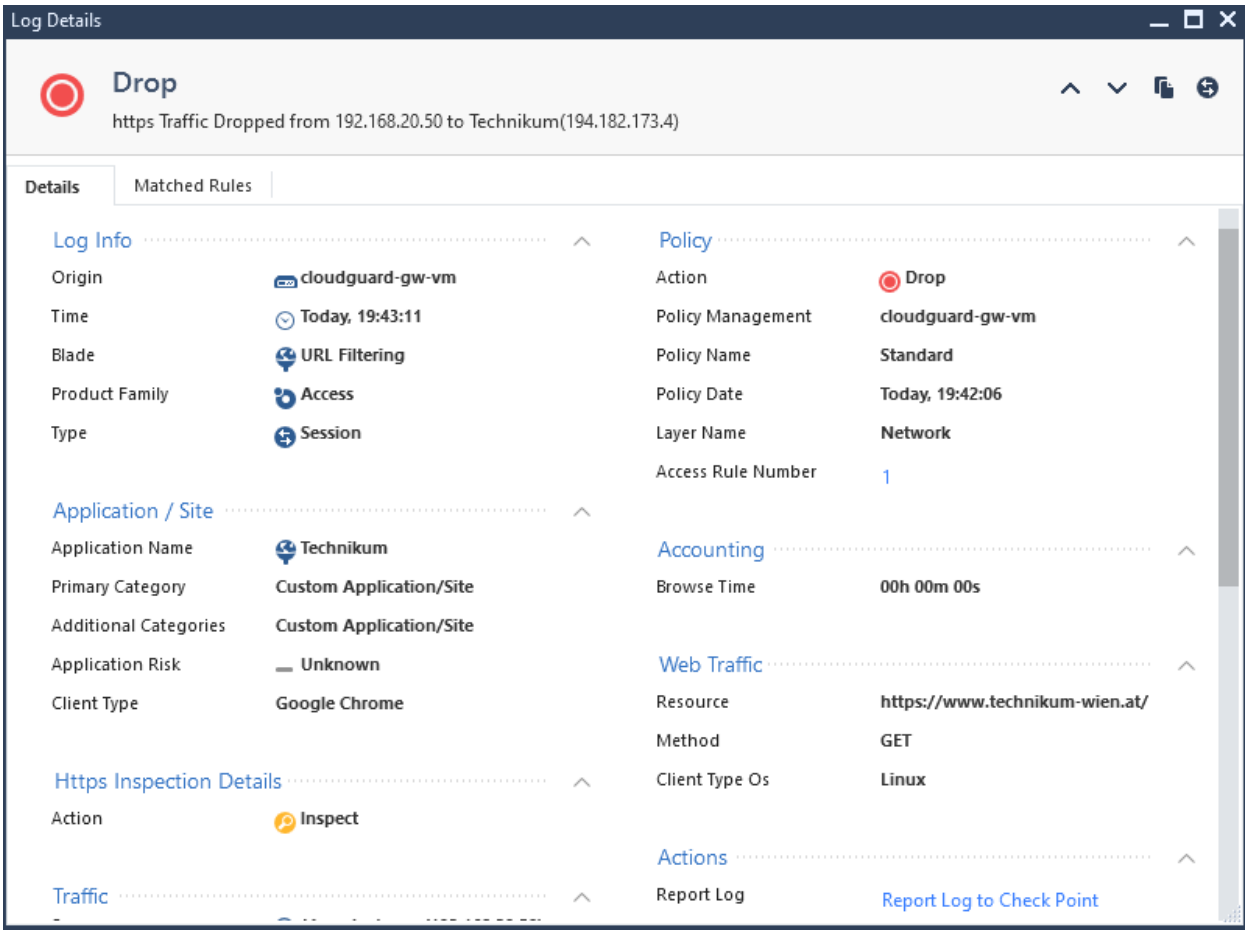
No.	Name	Source	Destination	VPN	Services & Applications	Action	Track	Install On
1	No Technikum for you	Any	Any	Any	Technikum	Drop	Log, Accounting	Policy Targets

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.

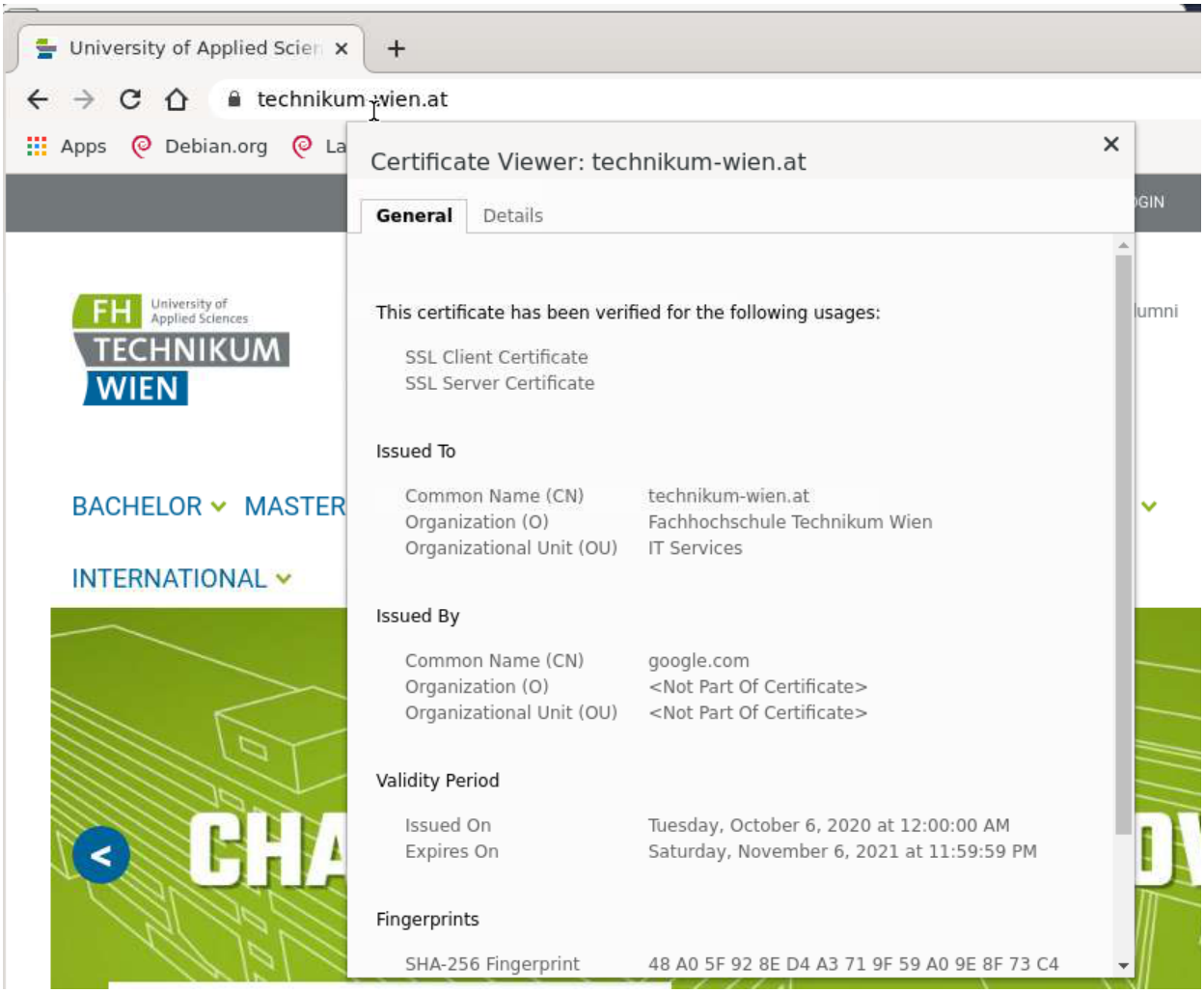
Wobei das produktivitätstechnisch vermutlich keinen positiven Einfluss hat. Geblockte Seiten haben negative Auswirkungen auf die Motivation und Moral der

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

Aufgetretene Probleme

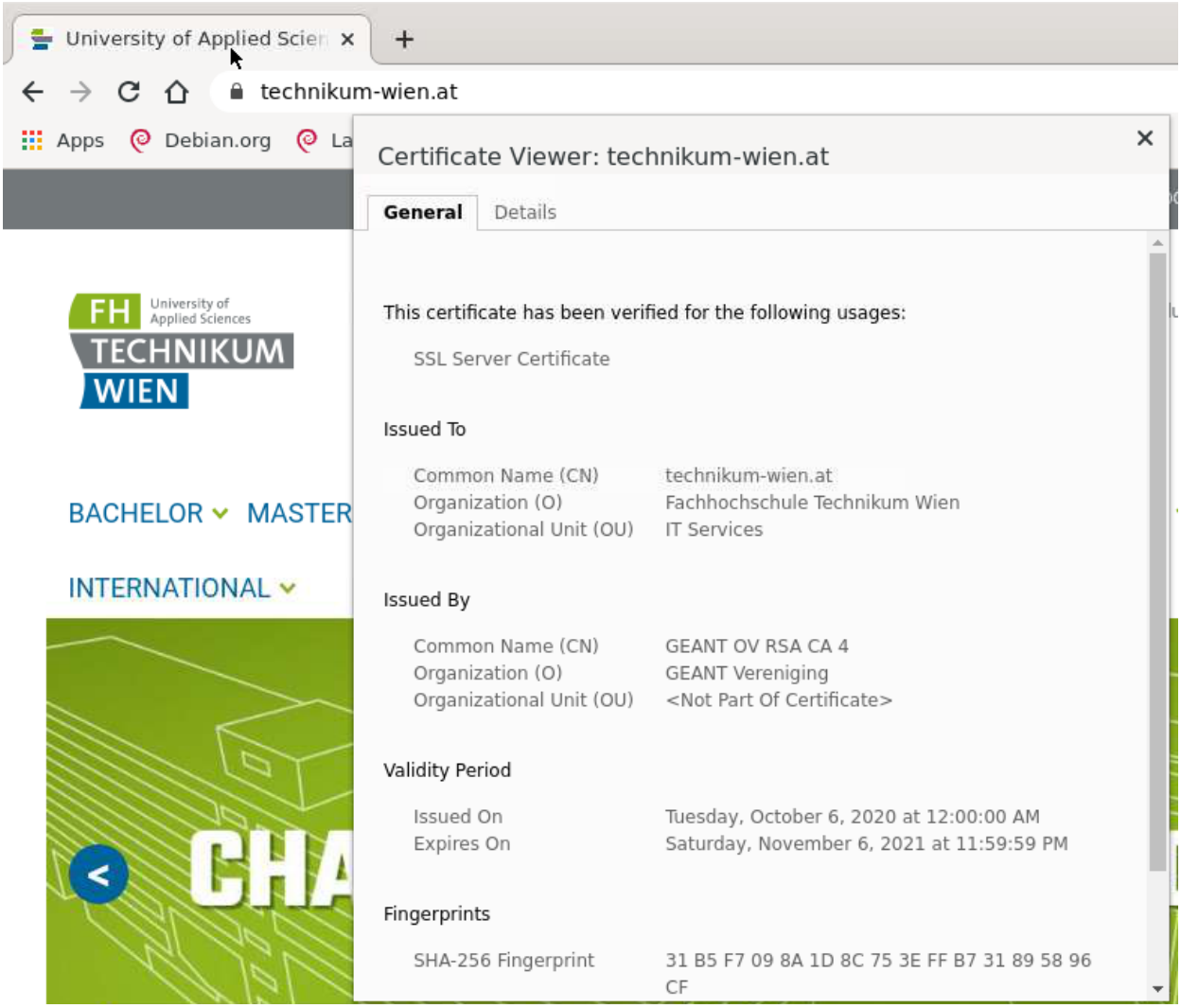
Es sind keine Probleme aufgetreten.

Lab 3.3 HTTPS Inspection Bypass



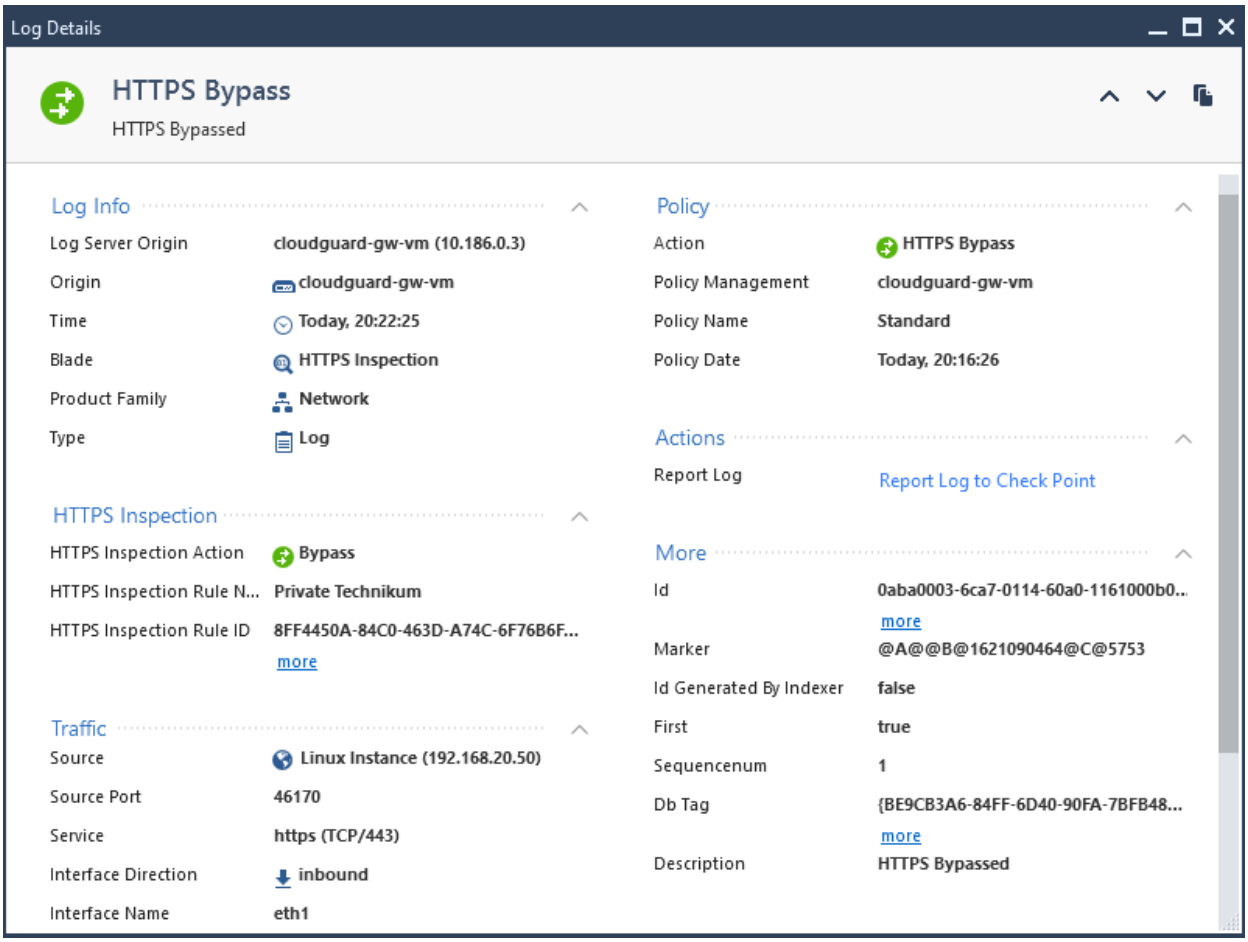
Vor Bypass Regel. Man sieht der Issuer ist Google.com (was ich als Wert im self-signed Certificate eingestellt habe)

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



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
- Medizienische Seiten
- Finanzseiten

Aufgetretene Probleme

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

nächstes Lab