Lab 2

Author: Benjamin Medicke
Topics: IPS & Anti-Virus

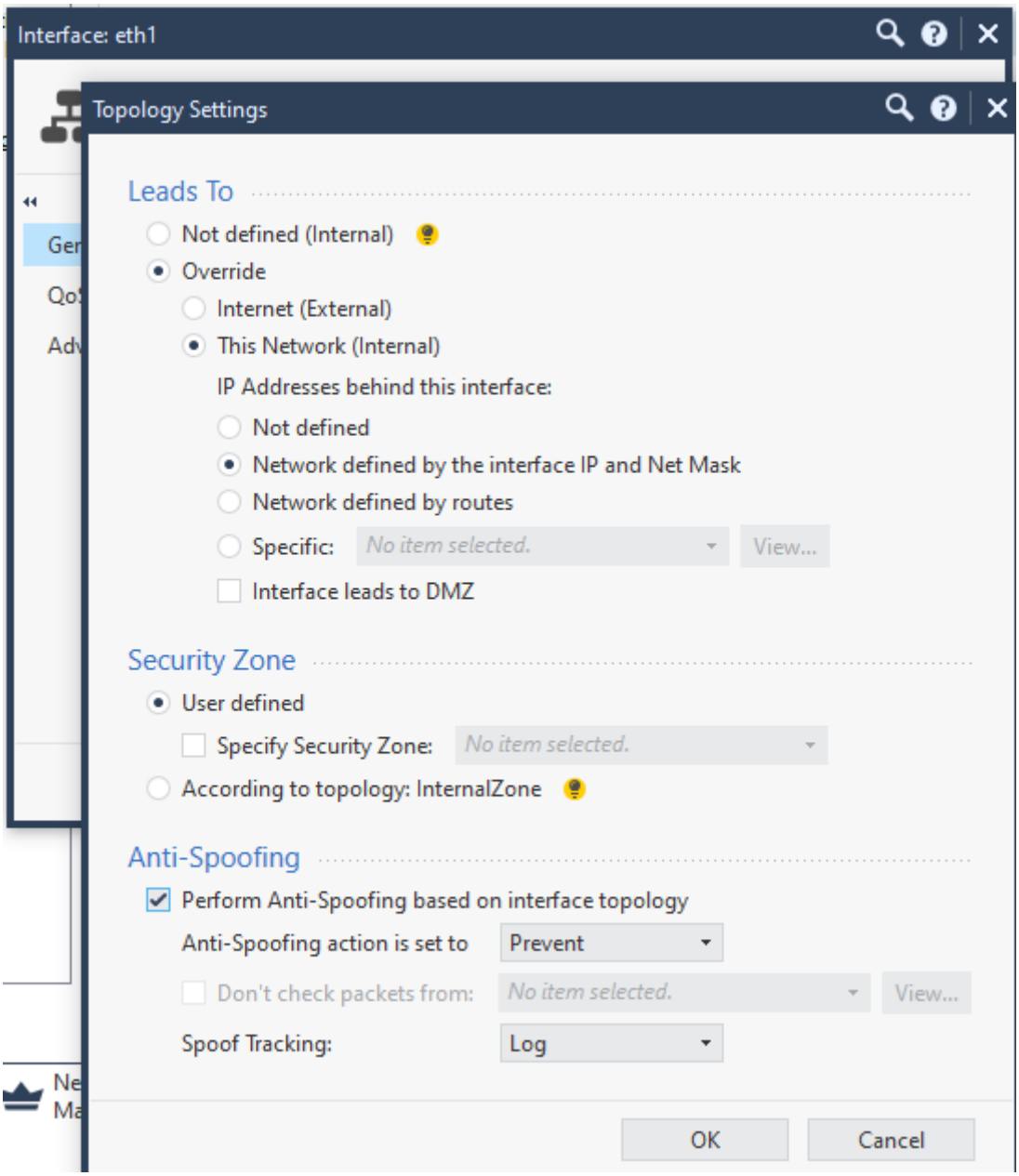
lab1 | **lab2** | lab3 | lab4

Lab 2.1 IPS

In diesem Abschnitt wurde das Intrusion Prevention System Blade aktiviert und demonstriert.

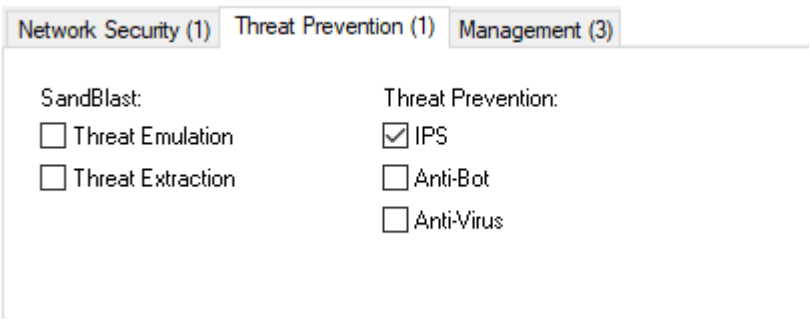
2.1.3 Topologien einstellen

Topology von eth0 auf "external" stellen.

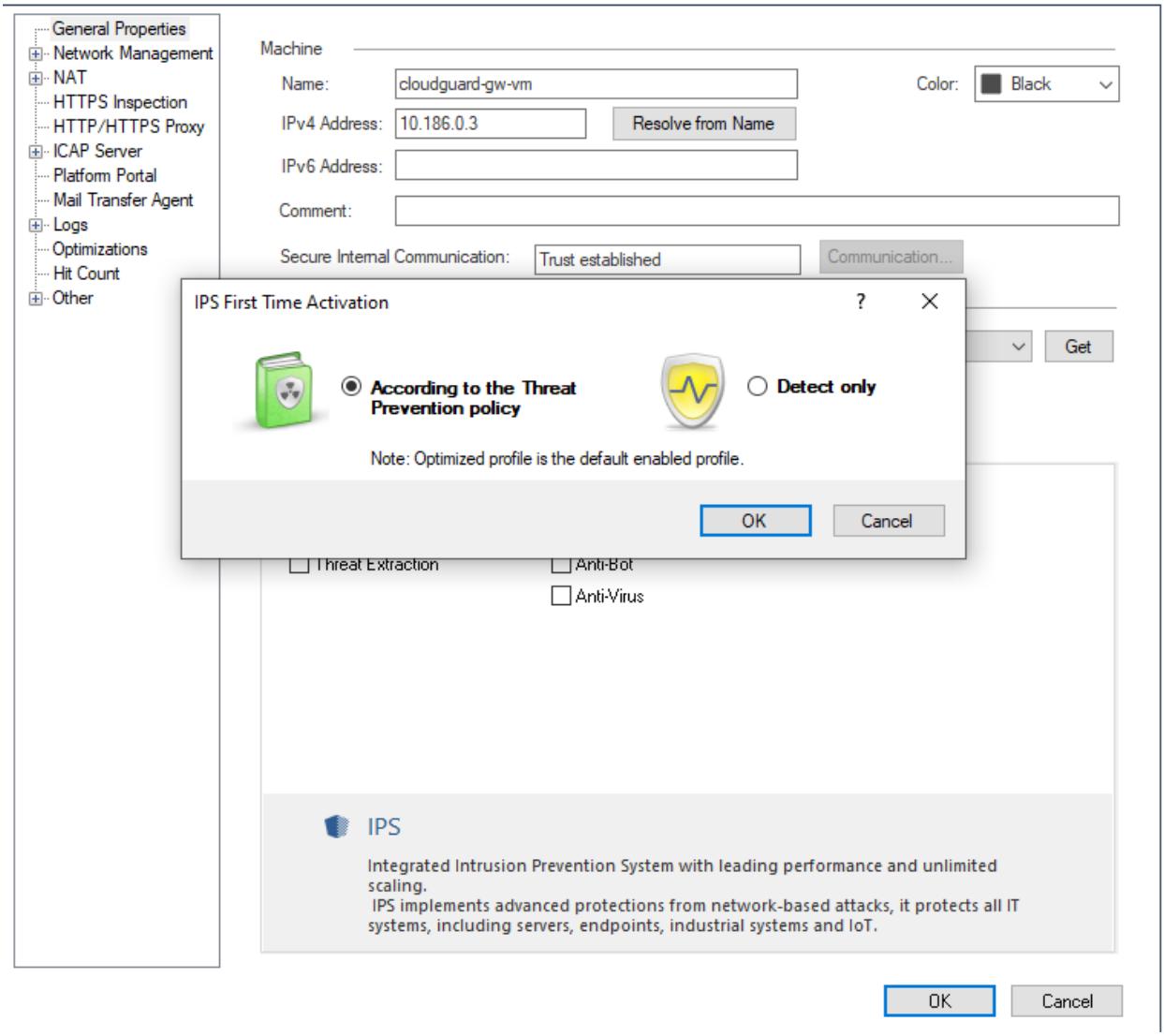


Topology von eth1 auf "internal" stellen. Aktivieren von Anti-Spoofing.

2.1.4 IPS Blade aktivieren

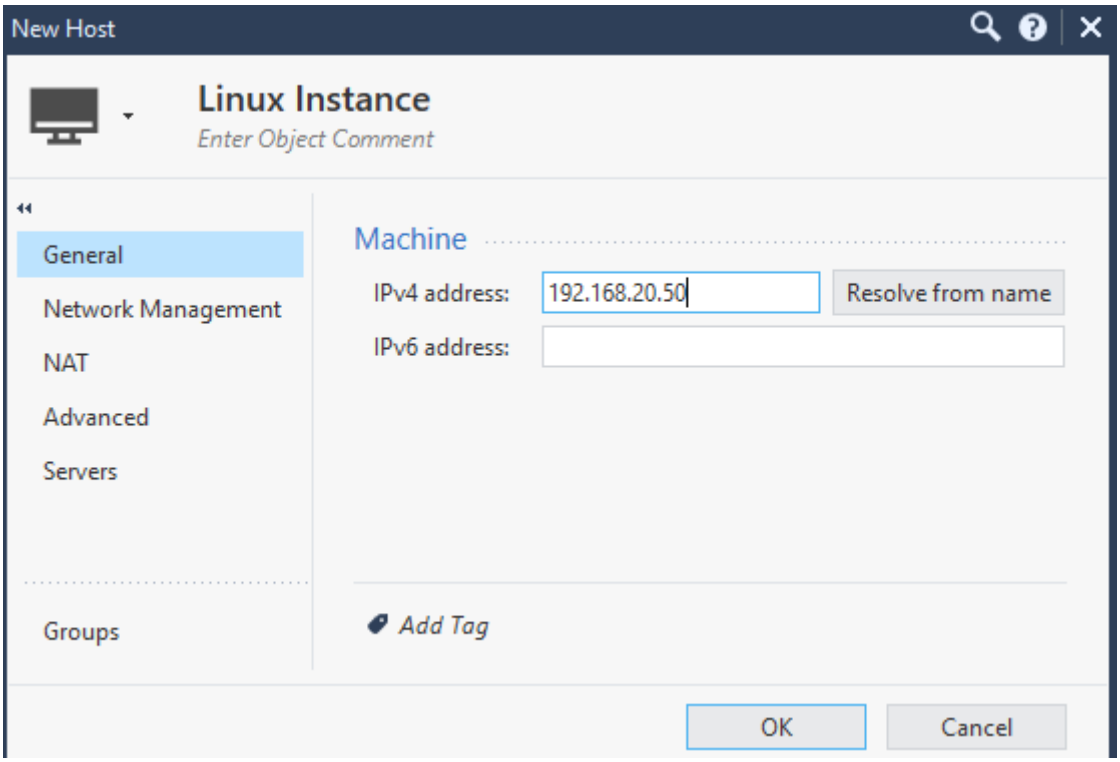


IPS blade aktiviert

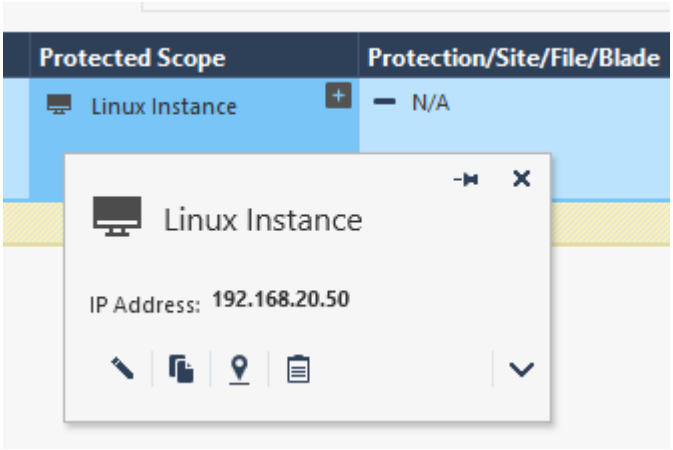


Setzten der "IPS First Time Activation" Einstellung auf "According to the Threat Prevention policy"

2.1.6 Protected Scope für die Linux Instanz

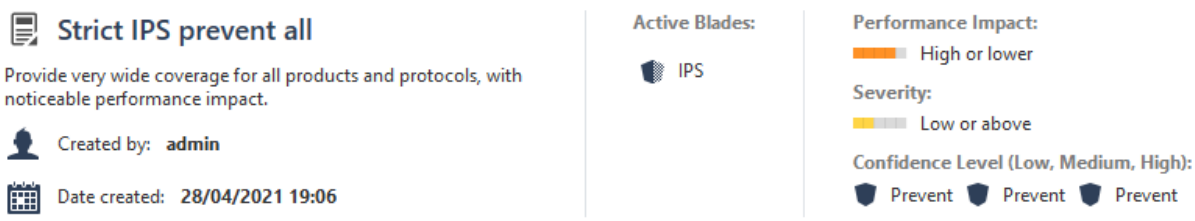


Linux Instanz



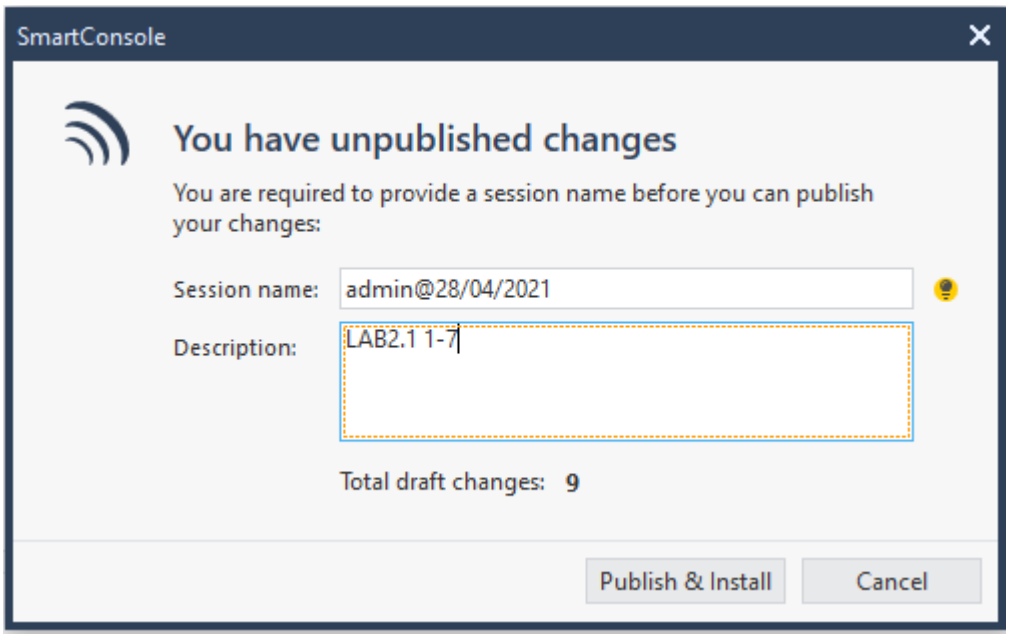
Hinzufügen der Linux Instanz zum Protected Scope

2.1.7 Profil "Strict" editieren



Kopie des "Strict" Profiles

Nur IPS Blade aktivieren, alle Aktivierungs-Szenarien auf "Prevent"

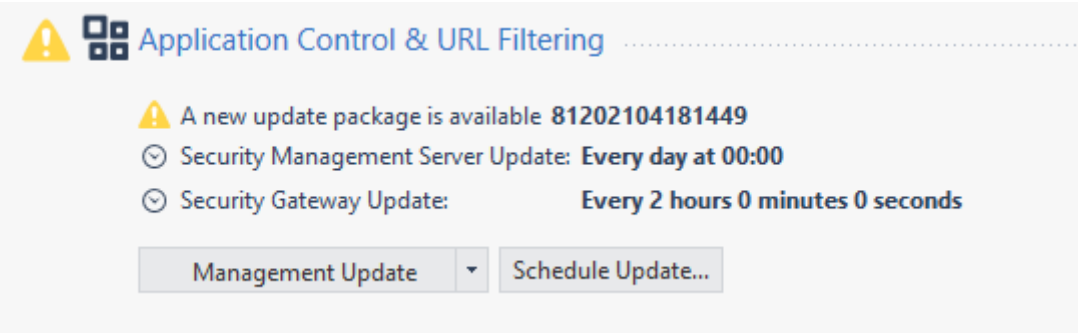


Publish & Install um die Policies anzuwenden

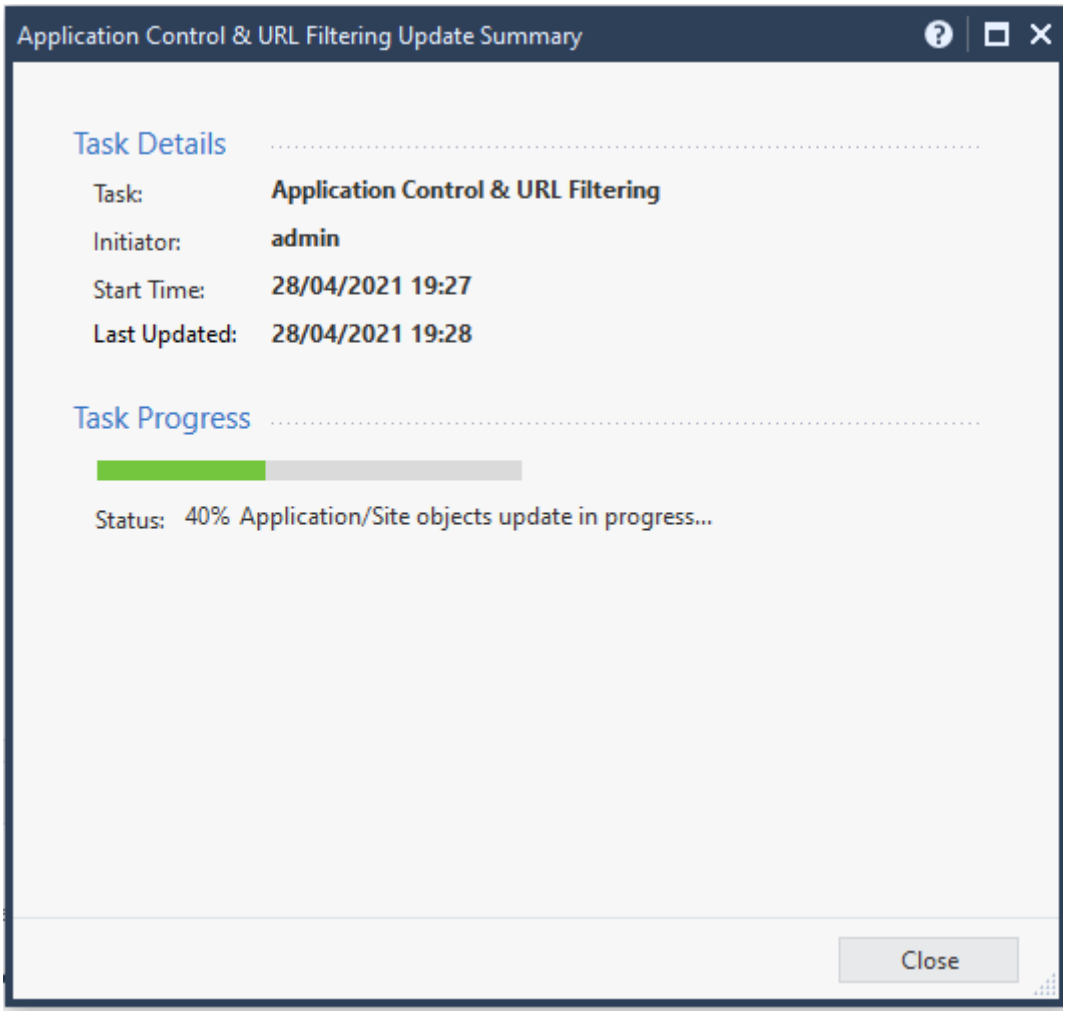
Neues Profil und zugewiesene Linux Instanz zum Protected Scope

2.1.9 Update

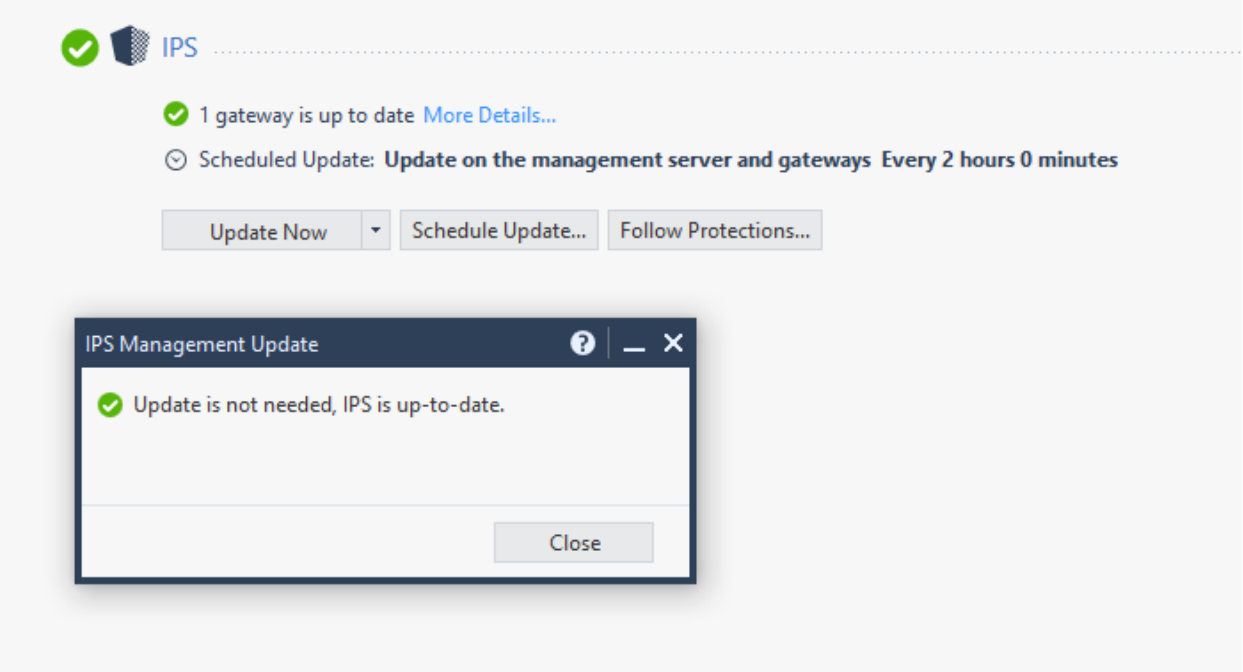
Nach der Installation des Profils wurde ein Update des IPS und des Management Servers durchgeführt.



Management Update



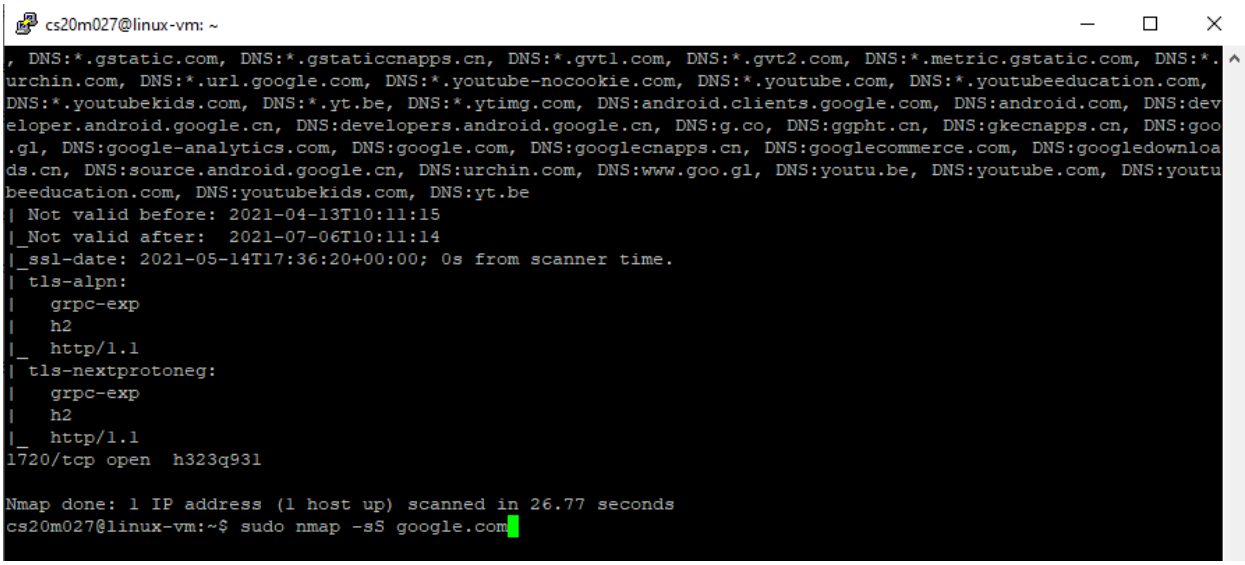
IPS Update



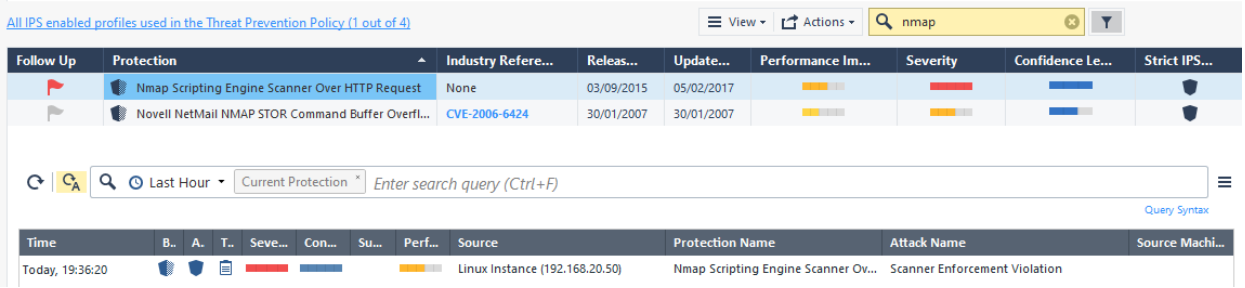
Alles up to date.

2.1.10 Traffic generieren und Logs prüfen

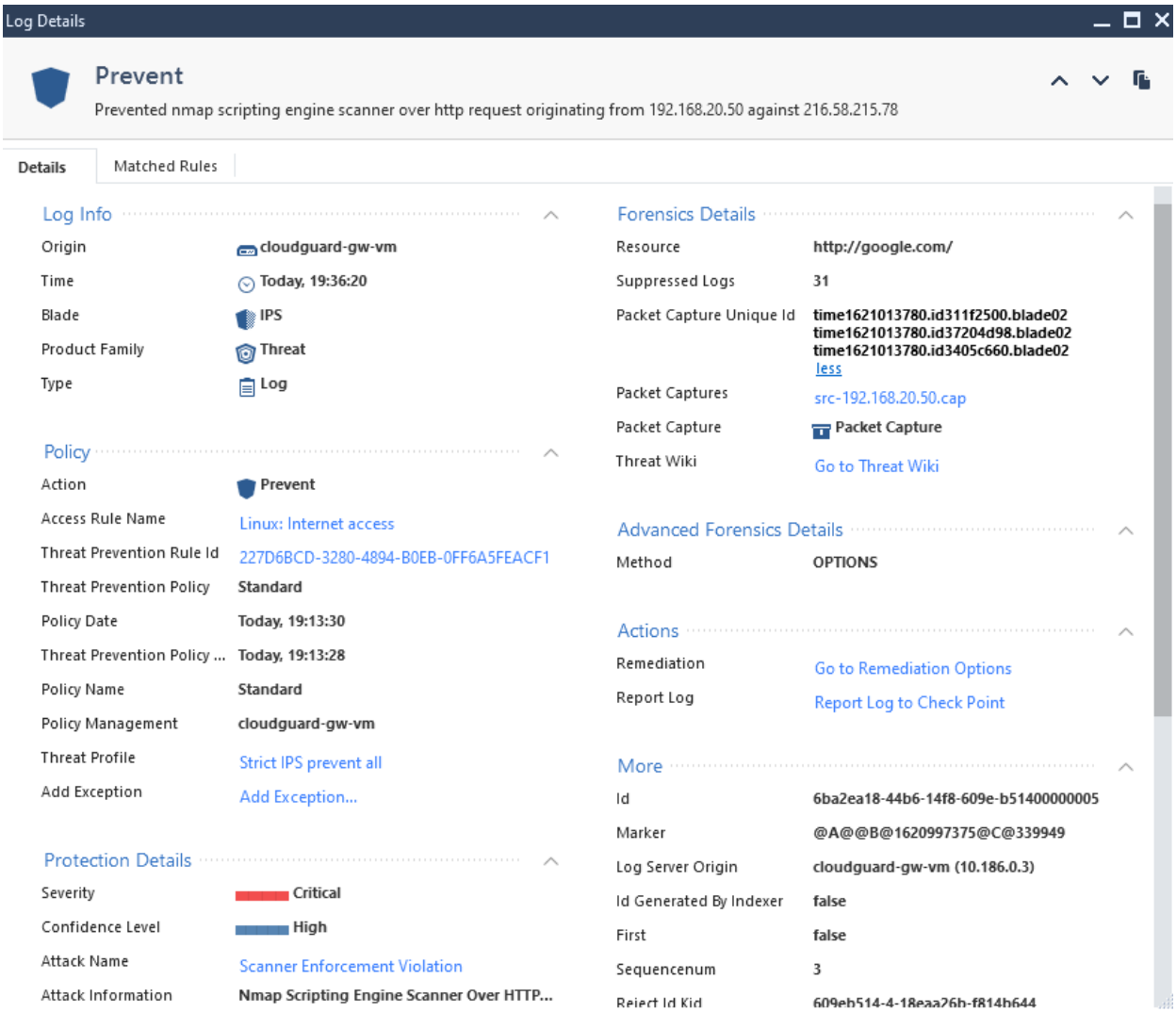
Um das IPS zu testen wurde ein (default) Nmap Script Scan durchgeführt. Die `default` Skripte sind nicht sehr aggressiv, ich hoffe Google vergiebt mir.



Start eines Nmap-Script-Scans



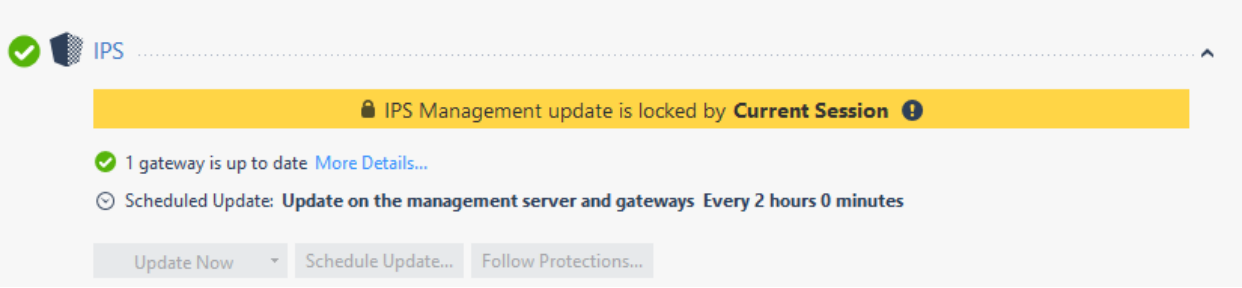
Erkannter Nmap-Script-Scan: `sudo nmap -sC google.com`



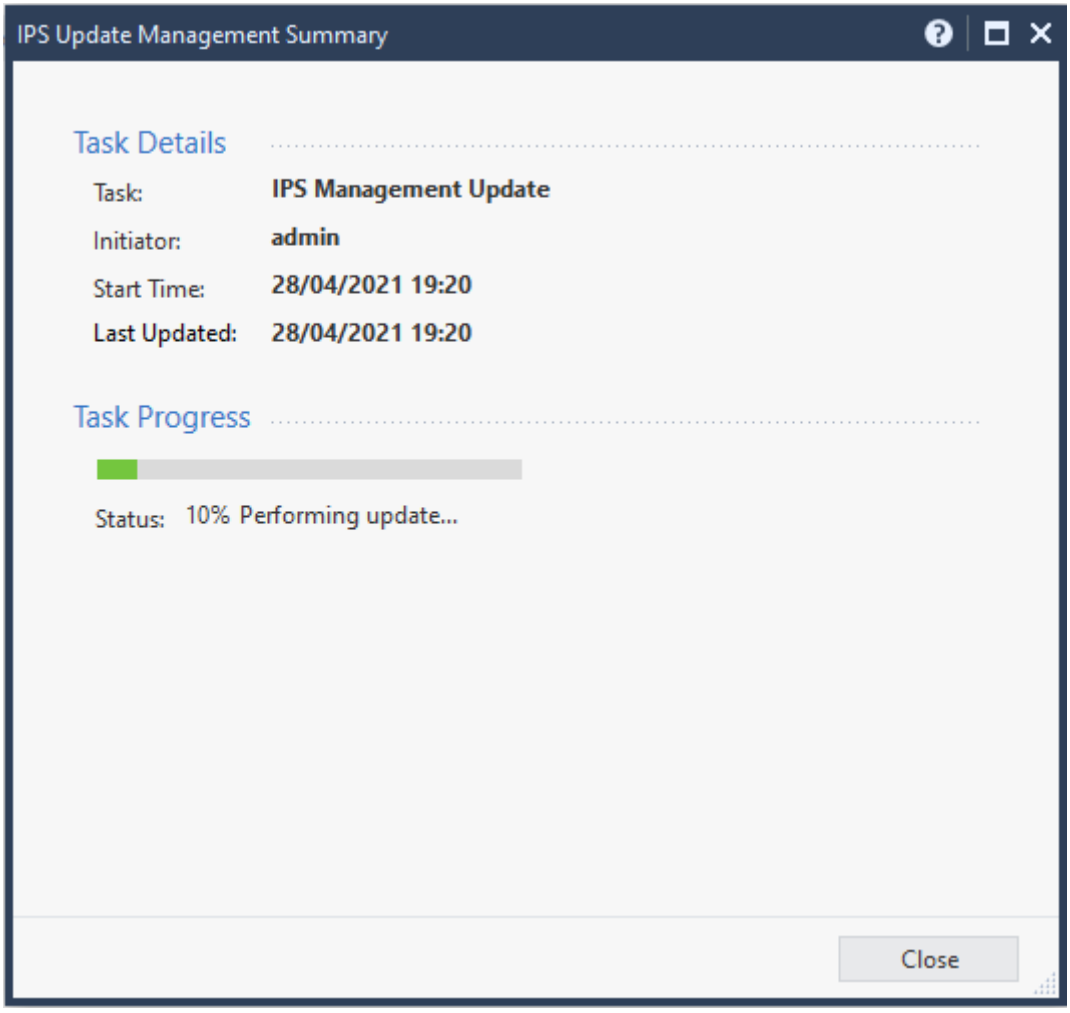
Erkannter Nmap-Script-Scan: Details

Aufgetretene Probleme

- Das Update hängt endlos.
- Gelöst durch Beenden der aktuellen Session.



Das Update blockiert bis die aktuelle Session beendet wird.

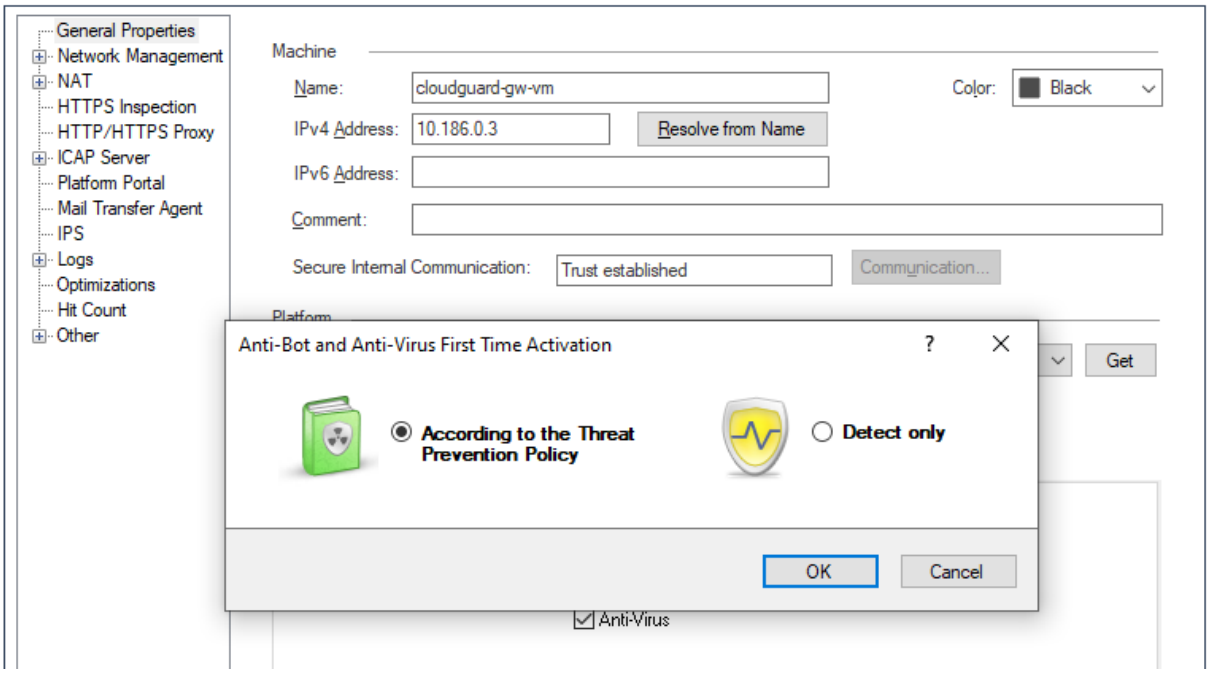


Was leider übersehen wurde, weswegen sehr lange auf die Fertigstellung gewartet wurde.

Lab 2.2 Anti-Virus

Hier wurde das Anti-Virus Blade aktiviert und mit dem eicar Anti Malware Testfile erfolgreich getestet.

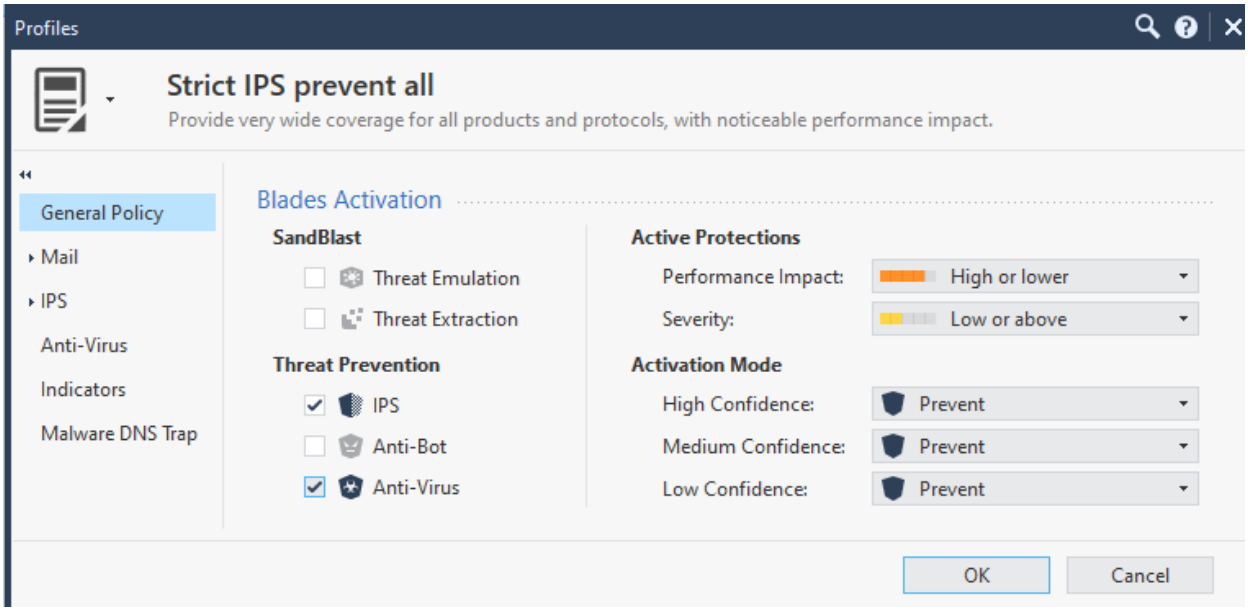
2.2.2 Aktivierung Blade: Anti-Virus



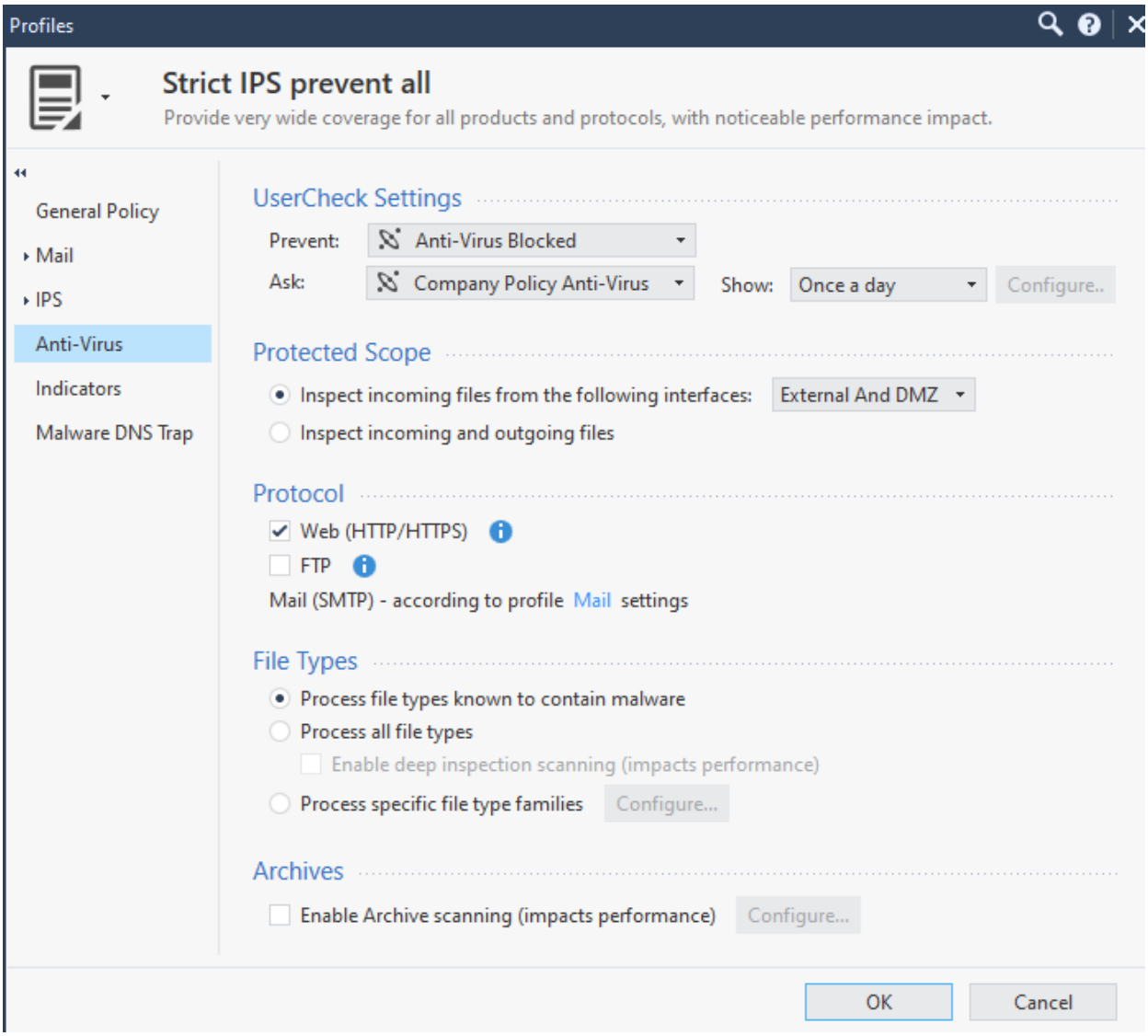
Anti-Virus Blade aktiviert "According to the Threat Prevention Policy"

2.2.5 Anpassen des zuvor angelegten Profils

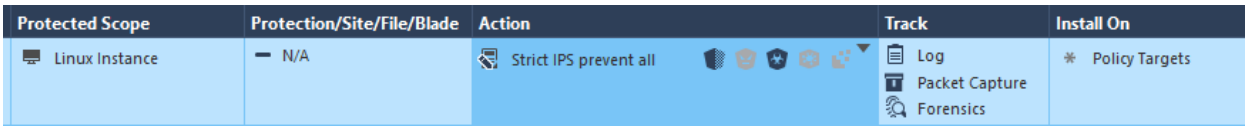
Die Linux Instanz ist bereits im Protected Scope, dieser wird nun angepasst.



Anti-Virus im vorhandenem Profil aktiviert

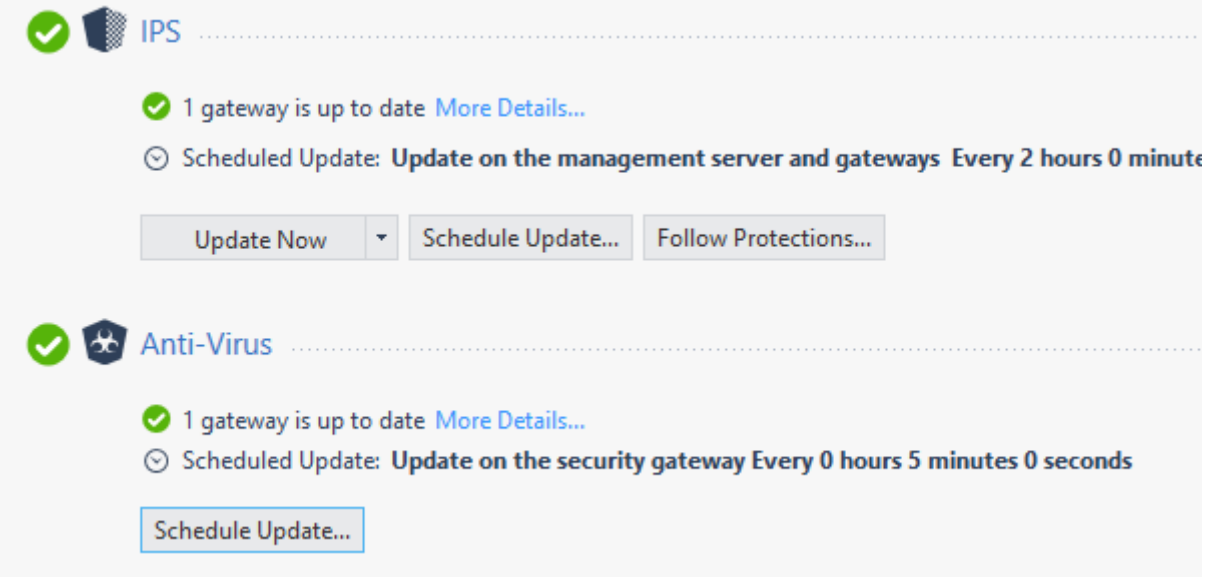


Anti-Virus Detailseite, hier wurde später auch der Archiv-Scan und Scan aller Datei-Typen aktiviert



Die aktualisierte Security Policy

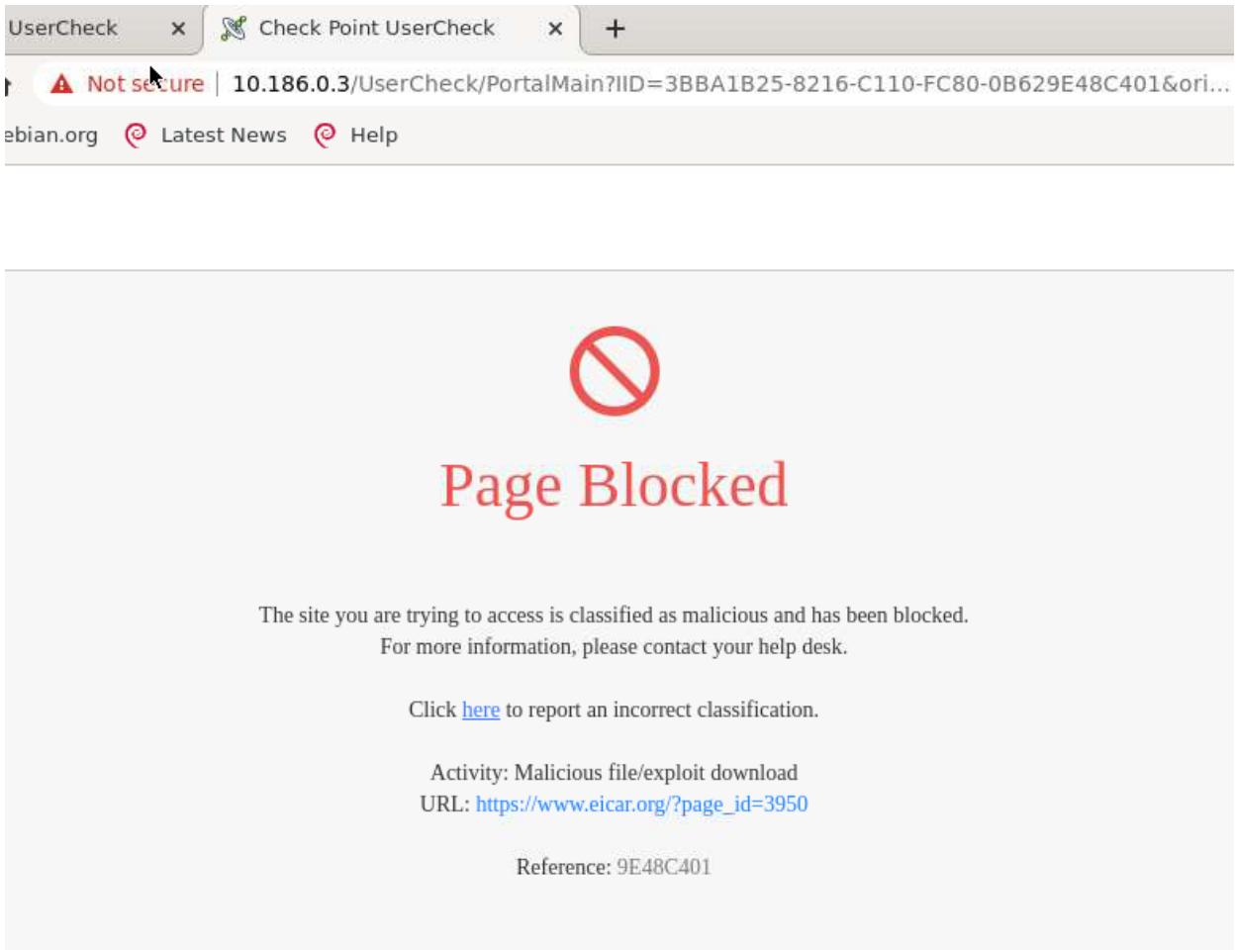
2.2.7 Update Anti-Virus



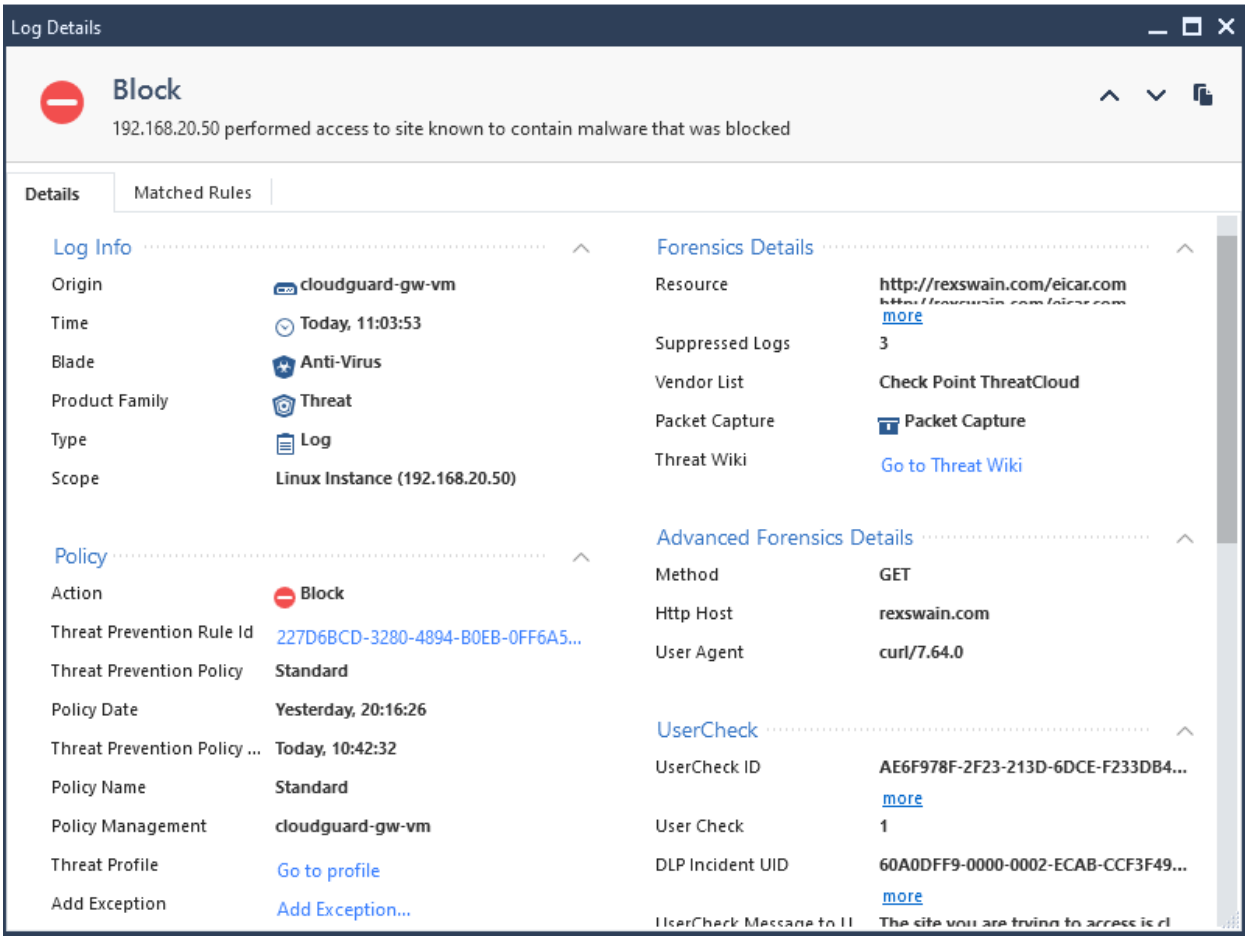
Es gibt keinen manuellen Update-Button, also wurde auf alle 5 Minuten gestellt und kurz gewartet.

2.2.8 Testlauf Anti-Virus

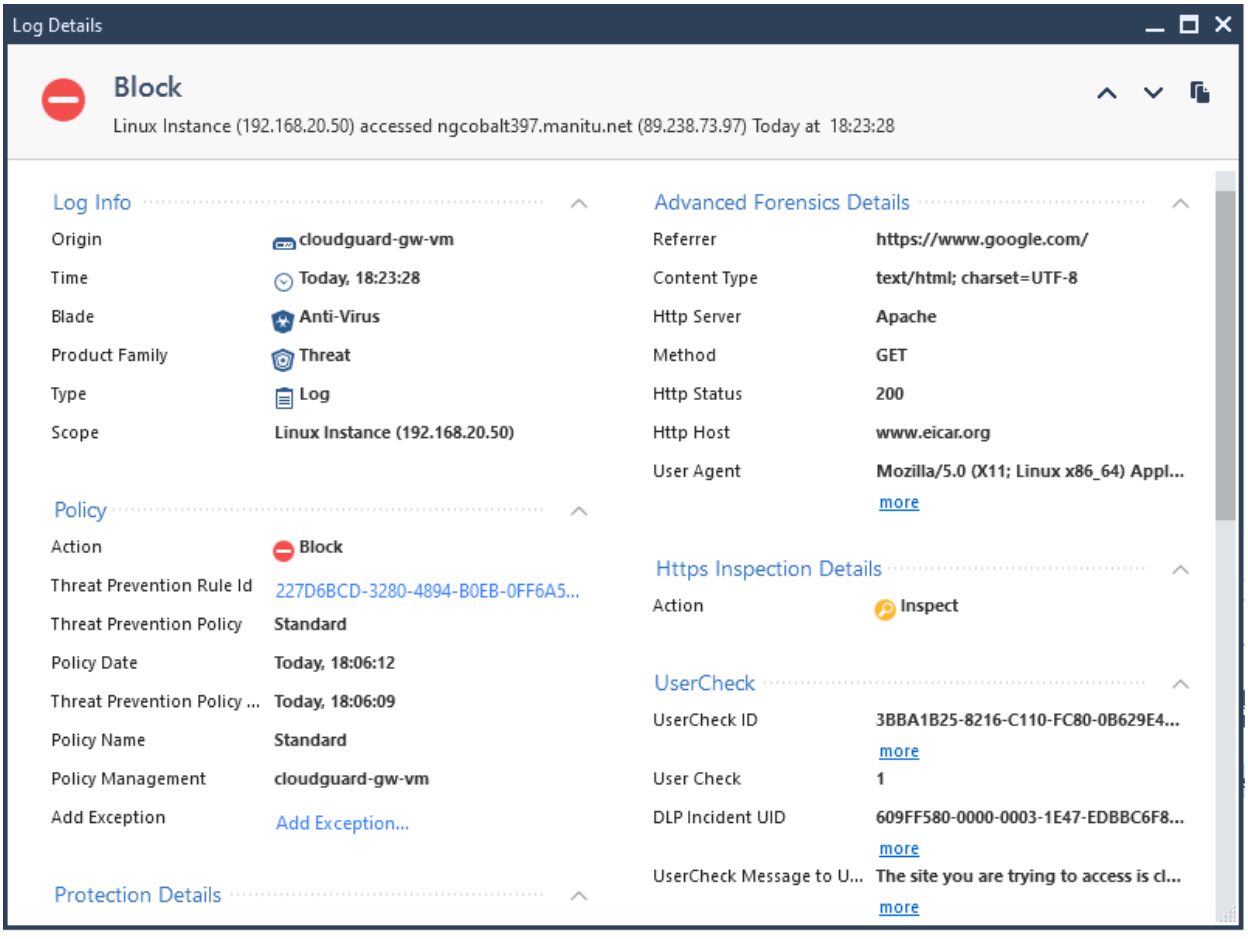
Es wurde der Eicar Download mit `curl` über HTTP versucht.



Ebenso via Browser



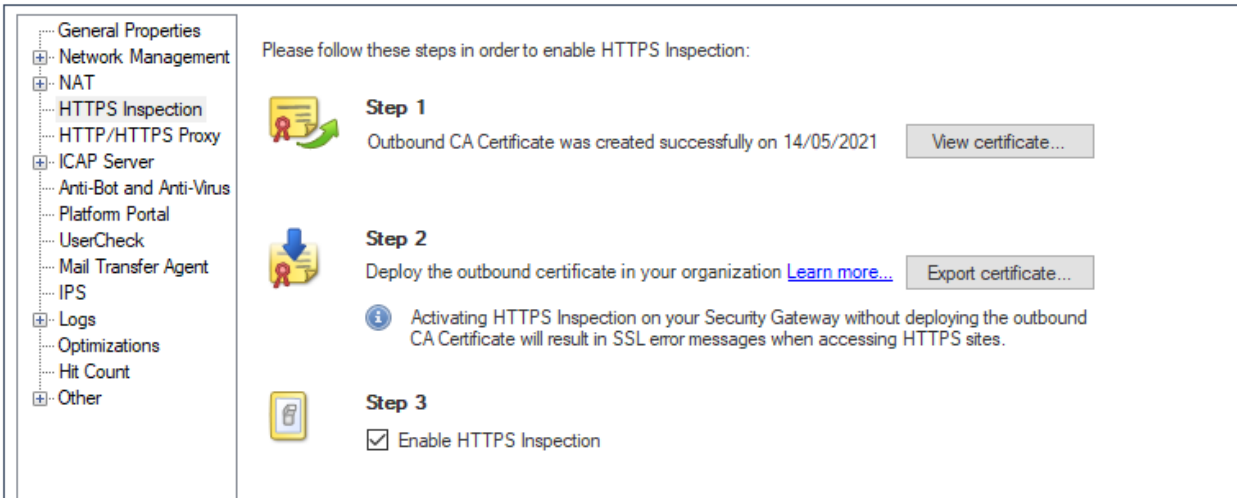
Blockierte Eicar Test-Malware über HTTP



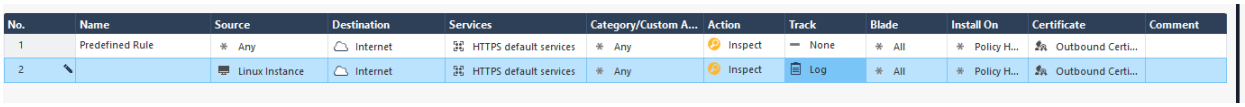
> Die Eicar Test-Malware wurde auch erfolgreich über HTTPS erkannt und der Download unterbunden. (Nach Aktivierung von HTTPS Inspection)

Lab 2.3 HTTPS Inspection

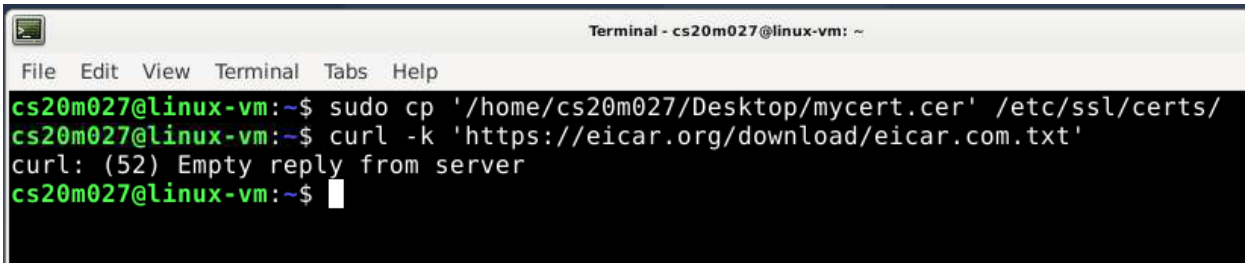
Um HTTPS aufzubrechen und zu inspizieren wurde ein selbstsigniertes Zertifikat erstellt und installiert.



Neues Zertifikat erstellt und als `mycert.cer` exportiert

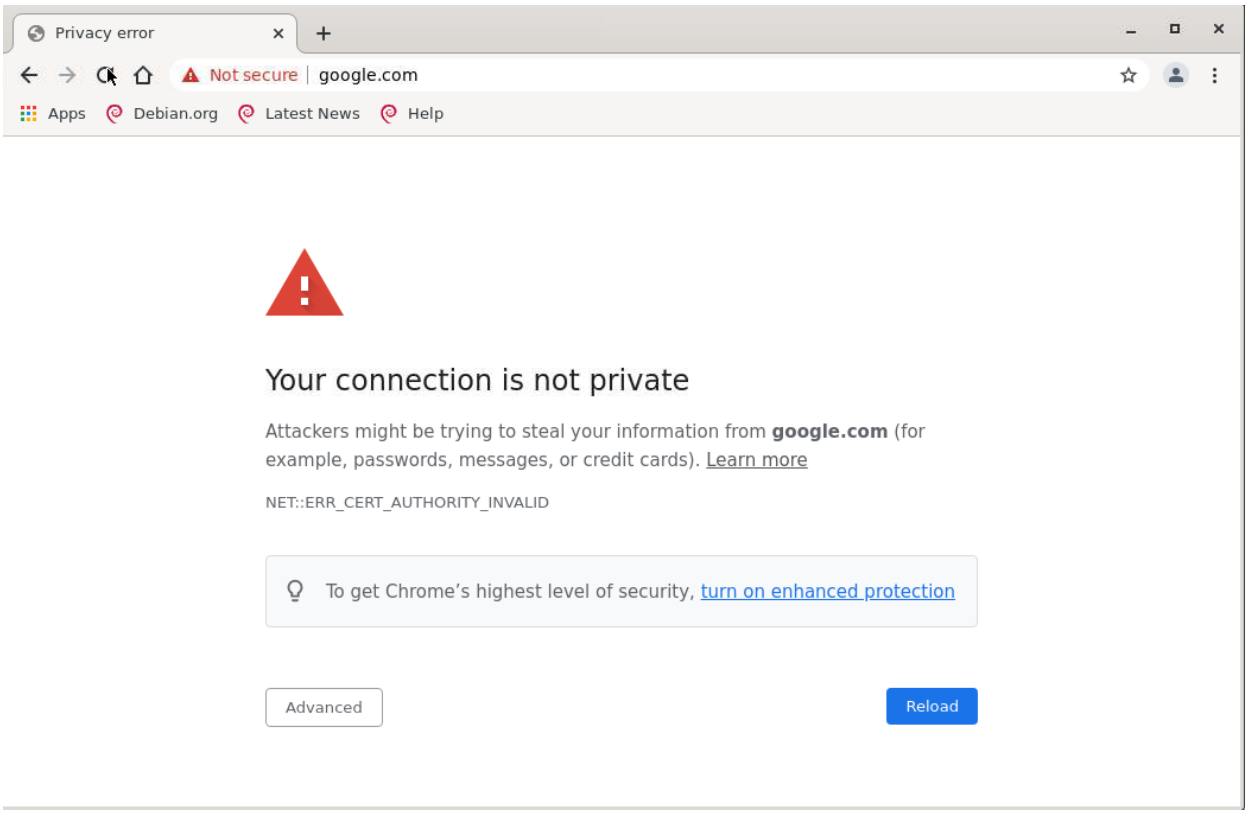


Neue HTTPS-Inspection Policy

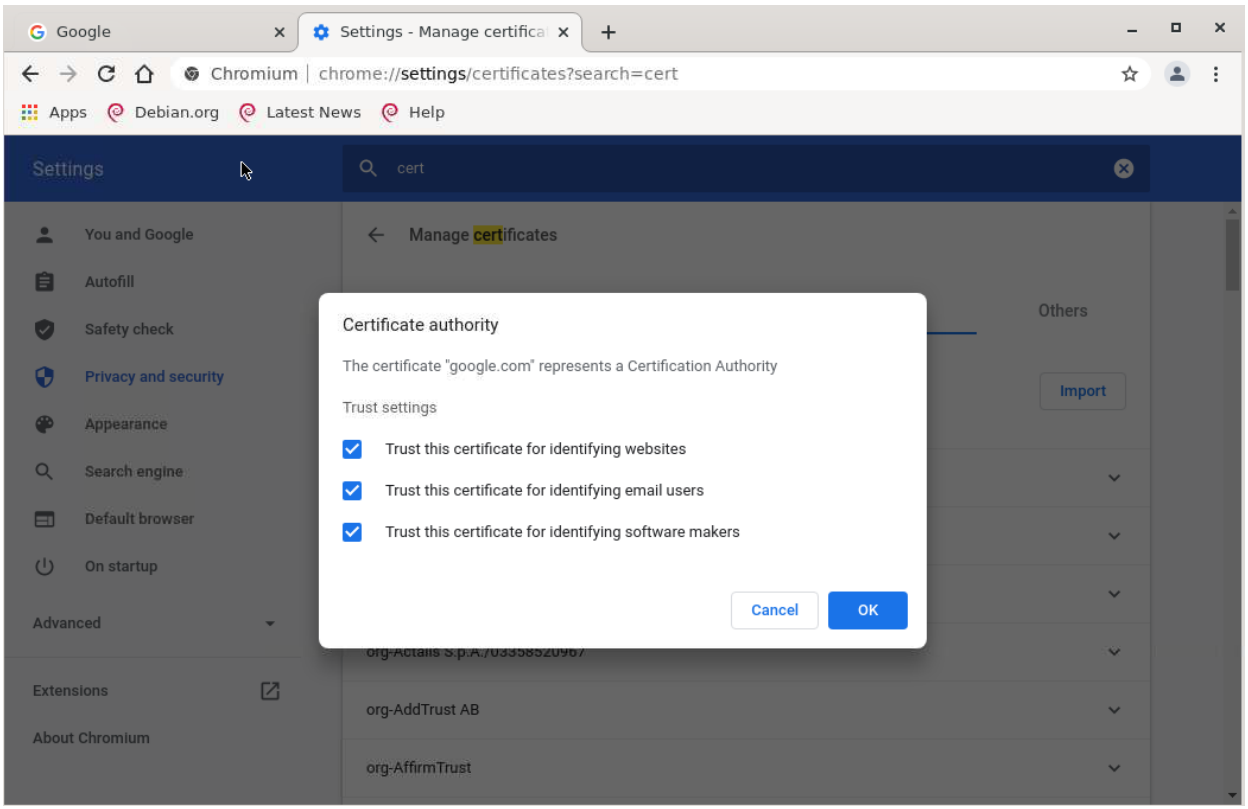


Unterbundener HTTPS Request bei Download von Eicar-Malware Testfile auch über HTTPS

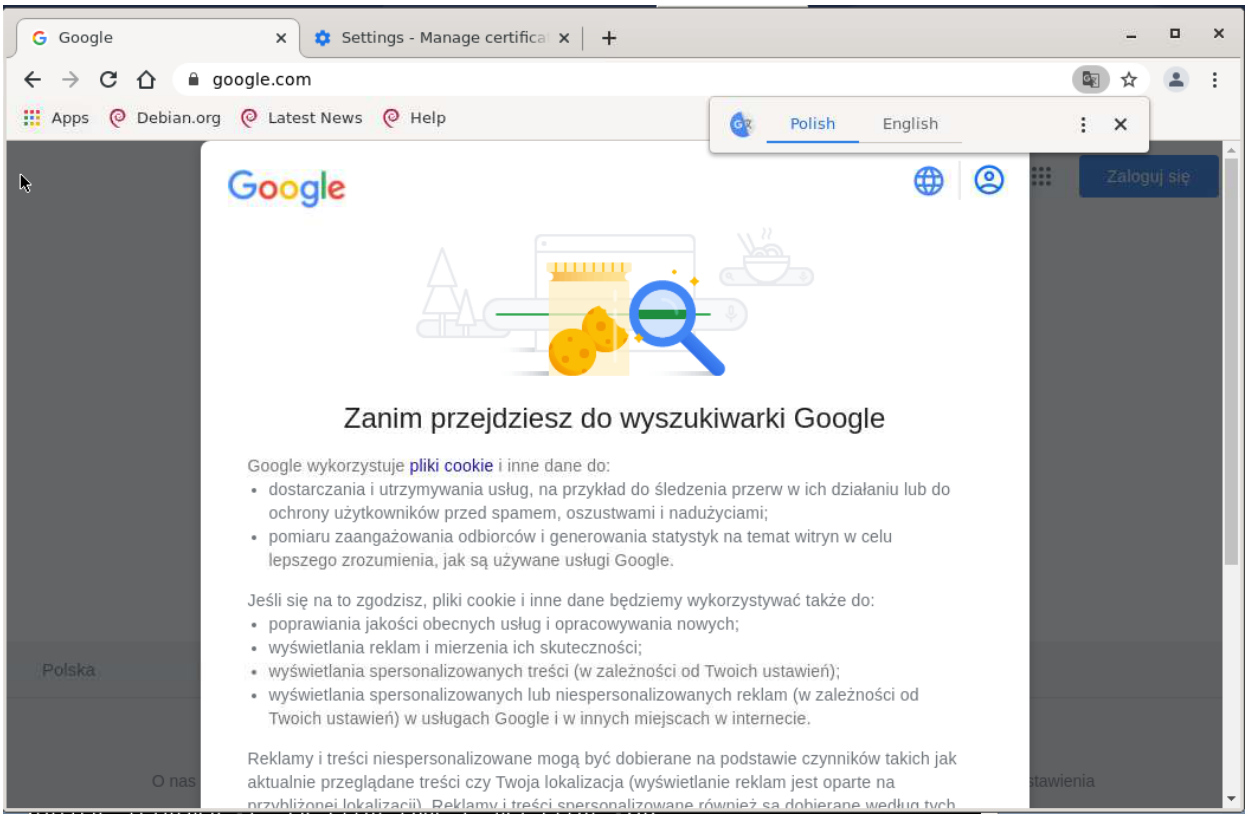
Das `-k` Flag erlaubt die Verwendung von Self-Signed Certificates. Als Browser wurde Chromium verwendet, welcher mit `apt get install chromium` installiert wurde.



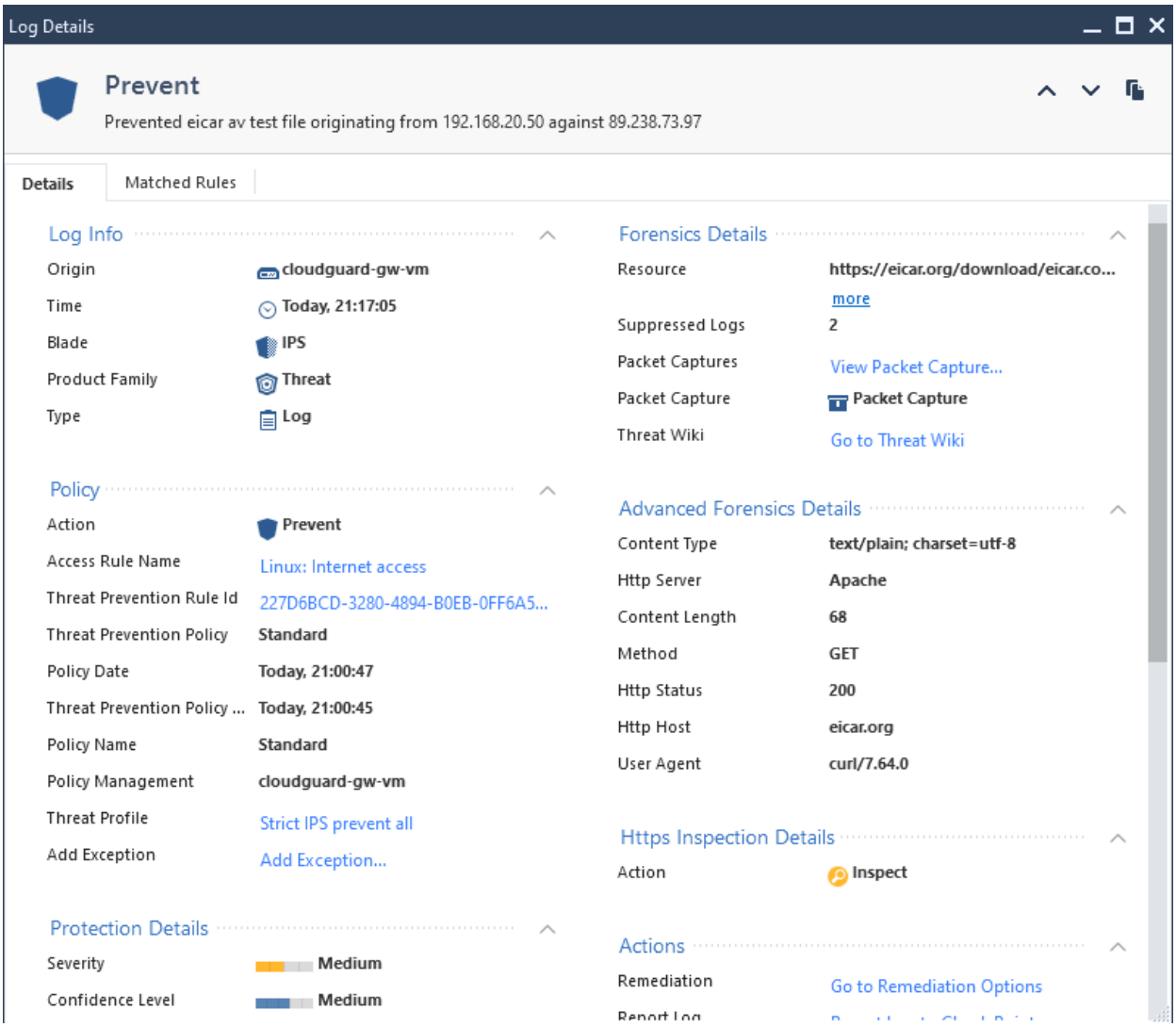
HTTPS Fehler bei Besuch einer TLS/SSL Seite



Zertifikatsimport in Chromium



Nach Import des Zertifikates wird keine Warnung generiert



Detailansicht: Erkanntes Eicar Testfile, auch über HTTPS

nächstes Lab