

Lab 2

Author: Benjamin Medicke

Topics: IPS & Anti-Virus

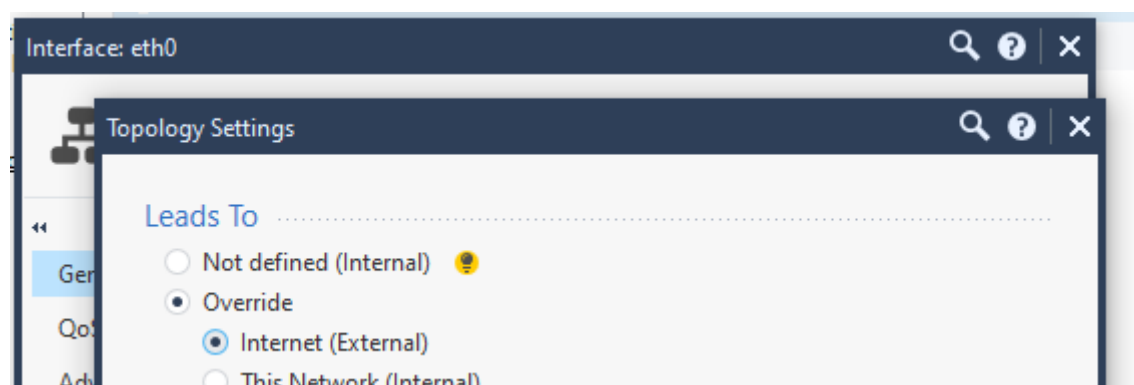
lab1 | **lab2** | lab3 | lab4

- Lab 2.1 IPS
 - 2.1.3 Topologien einstellen
 - 2.1.4 IPS Blade aktivieren
 - 2.1.6 Protected Scope für die Linux Instanz
 - 2.1.7 Profil "Strict" editieren
 - 2.1.9 Update
 - 2.1.10 Traffic generieren und Logs prüfen
 - Aufgetretene Probleme
- Lab 2.2 Anti-Virus
 - 2.2.2 Aktivierung Blade: Anti-Virus
 - 2.2.5 Anpassen des zuvor angelegten Profils
 - 2.2.7 Update Anti-Virus
 - 2.2.8 Testlauf Anti-Virus
- Lab 2.3 HTTPS Inspection

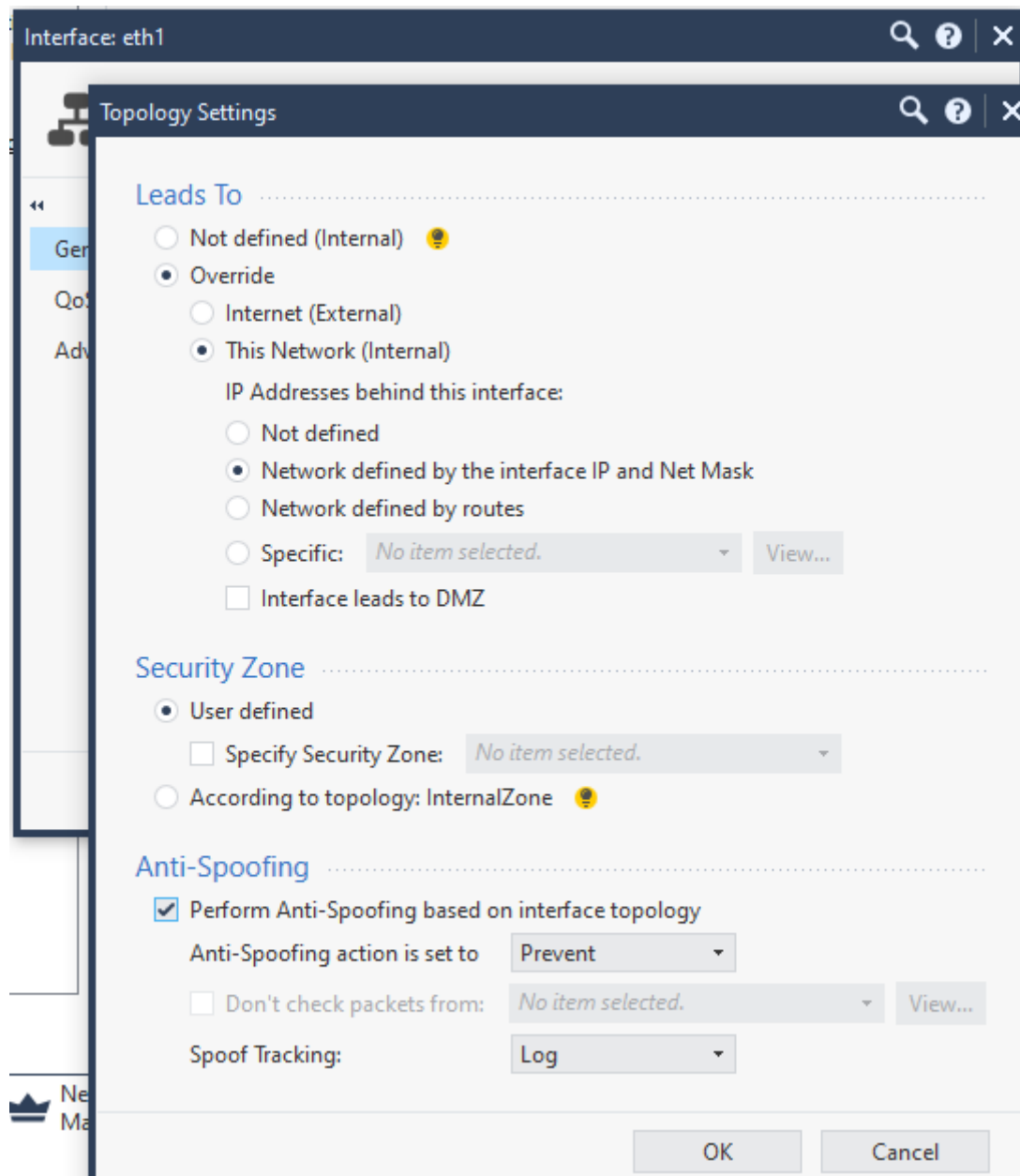
Lab 2.1 IPS

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

2.1.3 Topologien einstellen

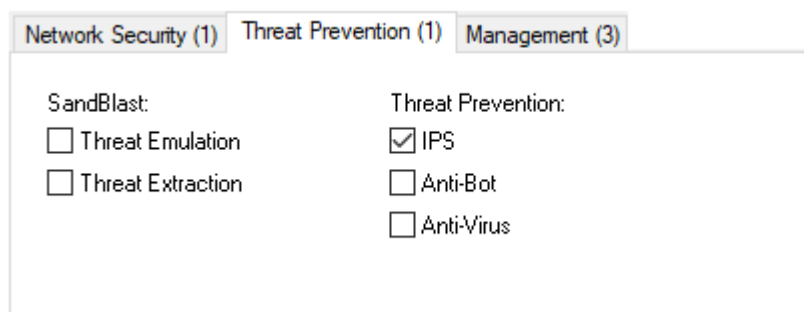


Topology von eth0 auf "external" stellen.

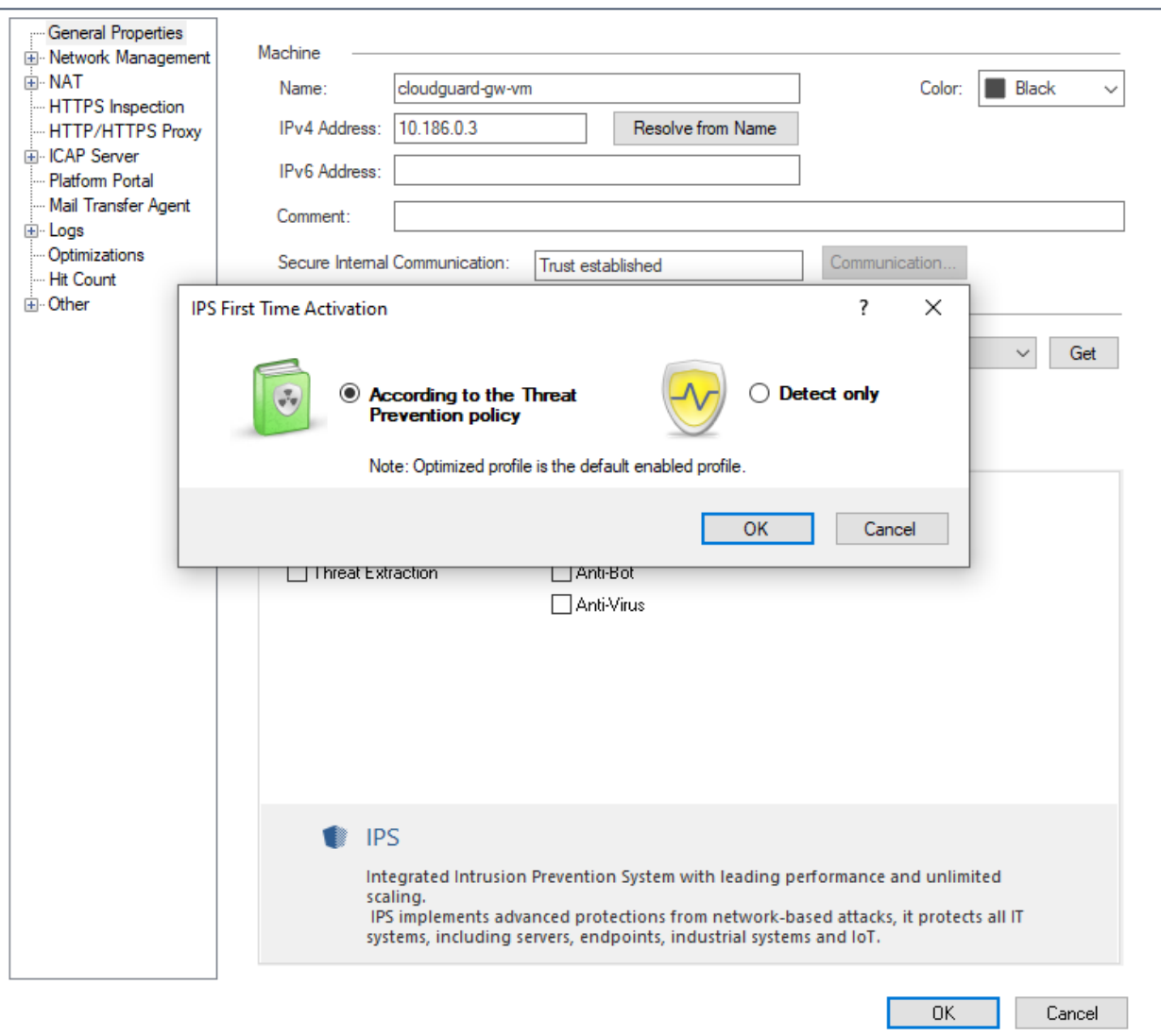


Topology von eth1 auf "internal" stellen. Aktivieren von Anti-Spoofing.

2.1.4 IPS Blade aktivieren



IPS blade aktiviert



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

2.1.6 Protected Scope für die Linux Instanz

New Host

Linux Instance
Enter Object Comment

General

Machine

IPv4 address: 192.168.20.50 Resolve from name

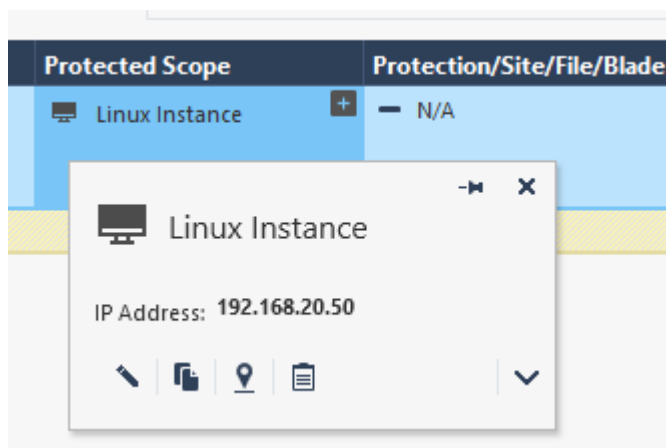
IPv6 address:

Groups

Add Tag

OK Cancel

Linux Instanz



Hinzufügen der Linux Instanz zum Protected Scope

2.1.7 Profil "Strict" editieren

Strict IPS prevent all

Provide very wide coverage for all products and protocols, with noticeable performance impact.

Created by: admin

Date created: 28/04/2021 19:06

Active Blades:

IPS

Performance Impact:

High or lower

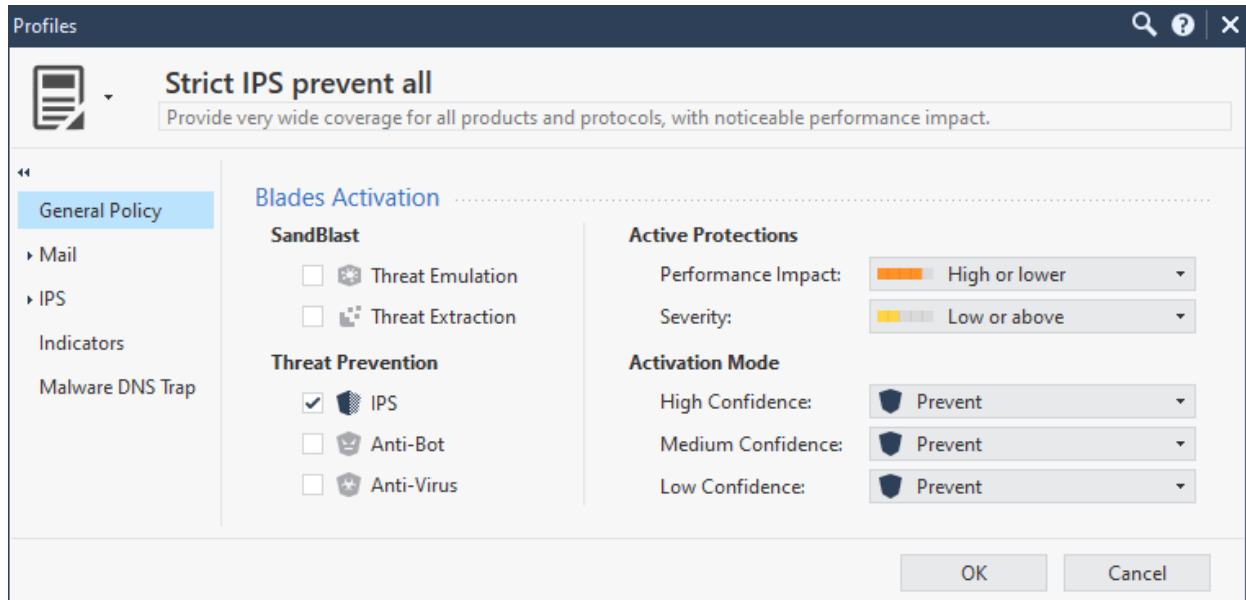
Severity:

Low or above

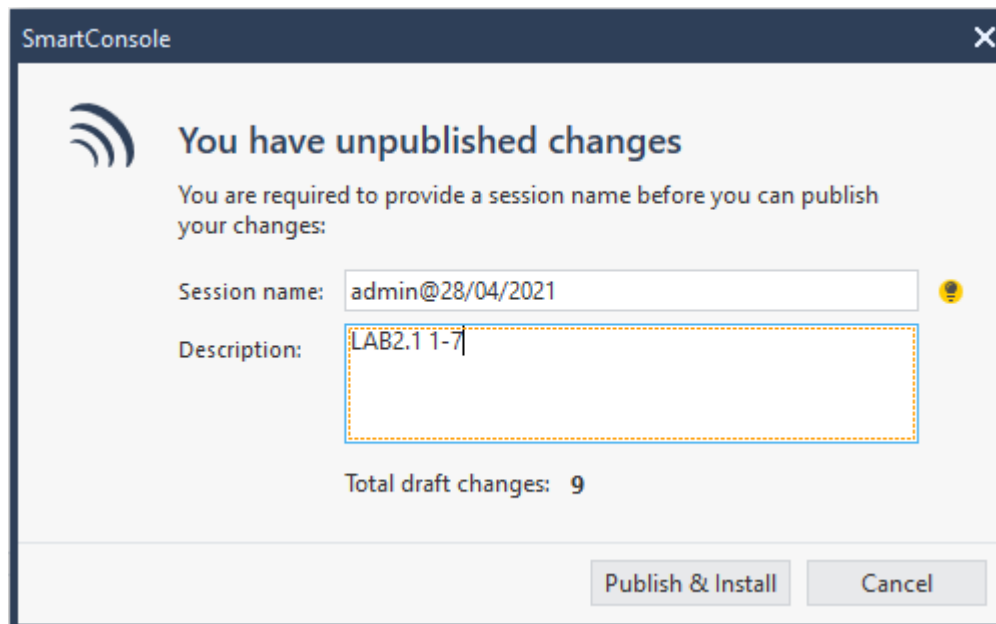
Confidence Level (Low, Medium, High):

Prevent Prevent Prevent

Kopie des "Strict" Profiles



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



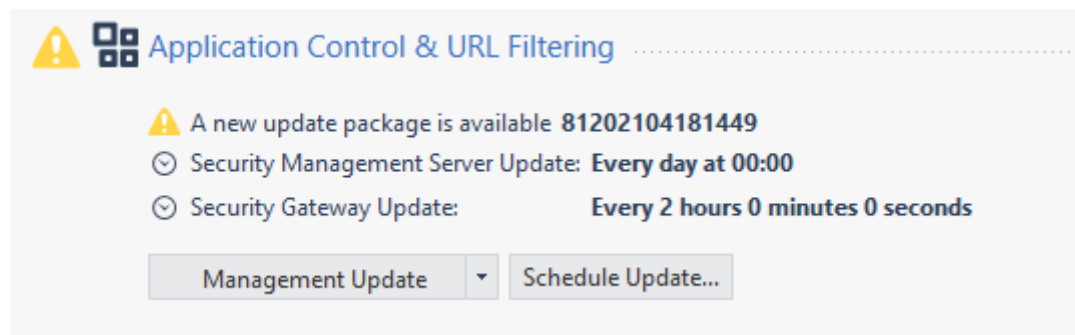
Publish & Install um die Policies anzuwenden

Protected Scope	Protection/Site/File/Blade	Action
Linux Instance	N/A	Strict IPS preve...

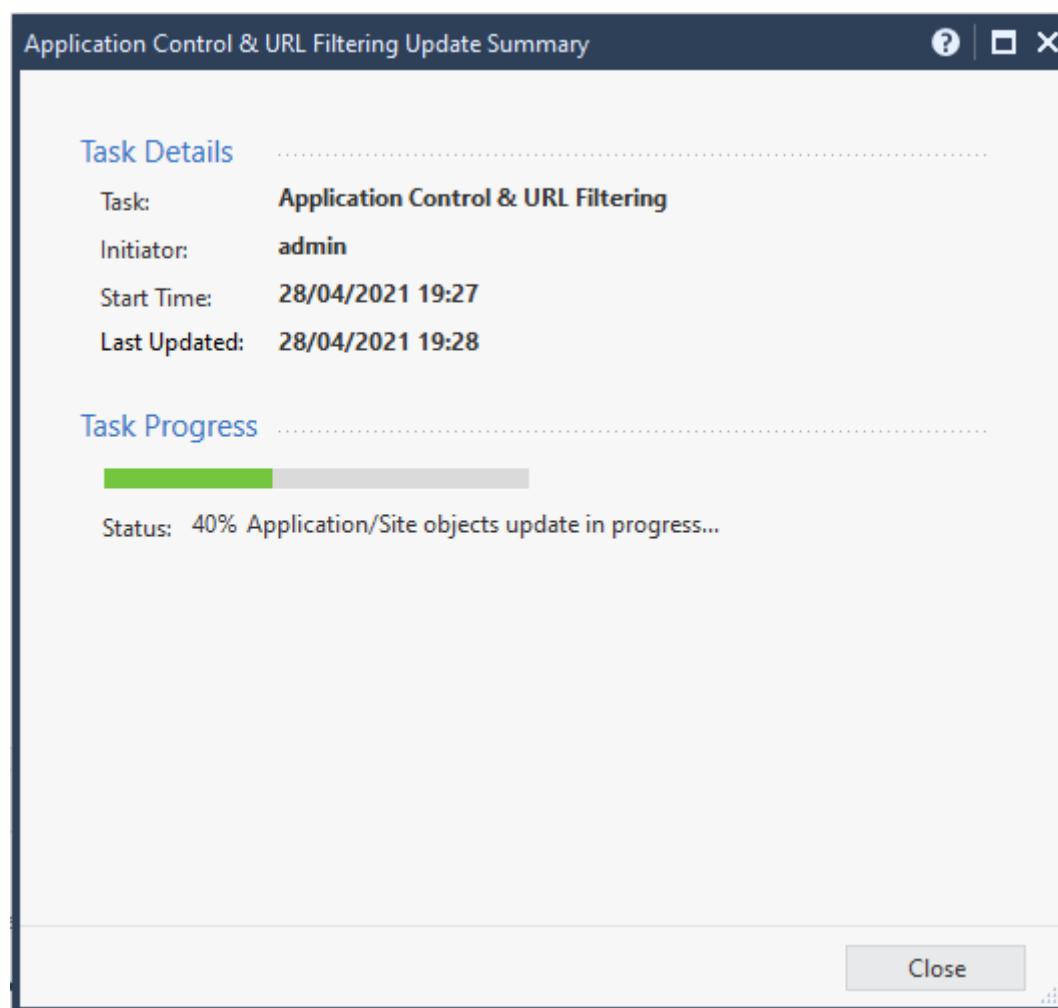
Neues Profil und zugewiesene Linux Instanz zum Protected Scope

2.1.9 Update

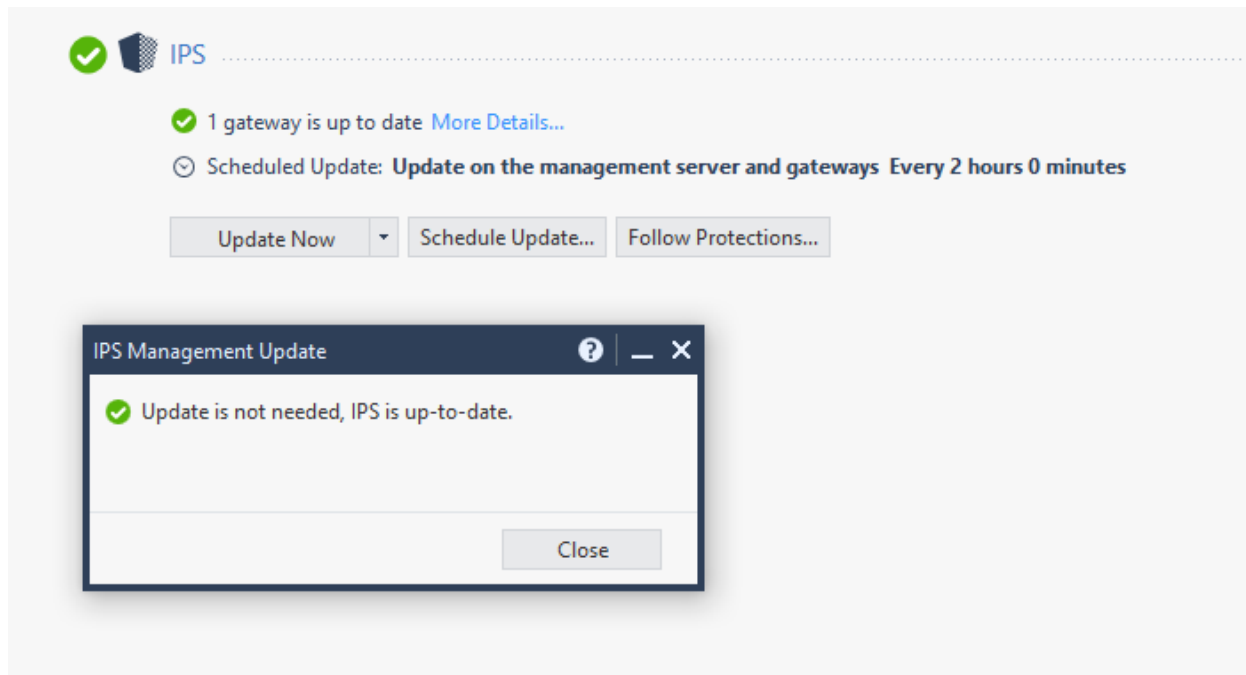
Nach der Installation des Profils wurde ein Update des IPS und des Management Servers durchgeführt.



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.

```
cs20m027@linux-vm: ~
, DNS:*.gstatic.com, DNS:*.gstaticcnapps.cn, DNS:*.gvt1.com, DNS:*.gvt2.com, DNS:*.metric.gstatic.com, DNS:*.
urchin.com, DNS:*.url.google.com, DNS:*.youtube-nocookie.com, DNS:*.youtube.com, DNS:*.youtubeeducation.com,
DNS:*.youtubekids.com, DNS:*.yt.be, DNS:*.yimg.com, DNS:android.clients.google.com, DNS:android.com, DNS:dev
eloper.android.google.cn, DNS:developers.android.google.cn, DNS:g.co, DNS:ggpht.cn, DNS:gkecnapps.cn, DNS:goo
.gl, DNS:google-analytics.com, DNS:google.com, DNS:googlecnapps.cn, DNS:googlecommerce.com, DNS:googledownloa
ds.cn, DNS:source.android.google.cn, DNS:urchin.com, DNS:www.goo.gl, DNS:youtu.be, DNS:youtube.com, DNS:youtu
beeducation.com, DNS:youtubekids.com, DNS:yt.be
|_ Not valid before: 2021-04-13T10:11:15
|_ Not valid after: 2021-07-06T10:11:14
|_ ssl-date: 2021-05-14T17:36:20+00:00; 0s from scanner time.
|_ tls-alpn:
|   grpc-exp
|   h2
|   http/1.1
|_ tls-nextprotoneg:
|   grpc-exp
|   h2
|   http/1.1
1720/tcp open  h323q931

Nmap done: 1 IP address (1 host up) scanned in 26.77 seconds
cs20m027@linux-vm:~$ sudo nmap -sS google.com
```

Start eines Nmap-Script-Scans

All IPS enabled profiles used in the Threat Prevention Policy (1 out of 4)

View Actions nmap

Follow Up	Protection	Industry Refere...	Releas...	Update...	Performance Im...	Severity	Confidence Le...	Strict IPS...
	Nmap Scripting Engine Scanner Over HTTP Request	None	03/09/2015	05/02/2017				
	Novell NetMail NMAP STOR Command Buffer Overfl...	CVE-2006-6424	30/01/2007	30/01/2007				

Last Hour Current Protection Enter search query (Ctrl+F)

Query Syntax

Time	B...	A...	T...	Seve...	Con...	SU...	Perf...	Source	Protection Name	Attack Name	Source Machi...
Today, 19:36:20								Linux Instance (192.168.20.50)	Nmap Scripting Engine Scanner Ov...	Scanner Enforcement Violation	

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

Log Details

Prevent

Prevented nmap scripting engine scanner over http request originating from 192.168.20.50 against 216.58.215.78

Details Matched Rules

Log Info

Origin: cloudguard-gw-vm

Time: Today, 19:36:20

Blade: IPS

Product Family: Threat

Type: Log

Policy

Action: Prevent

Access Rule Name: Linux: Internet access

Threat Prevention Rule Id: 227D6BCD-3280-4894-B0EB-0FF6A5FEACF1

Threat Prevention Policy: Standard

Policy Date: Today, 19:13:30

Threat Prevention Policy ...: Today, 19:13:28

Policy Name: Standard

Policy Management: cloudguard-gw-vm

Threat Profile: Strict IPS prevent all

Add Exception: Add Exception...

Protection Details

Severity: Critical

Confidence Level: High

Attack Name: Scanner Enforcement Violation

Attack Information: Nmap Scripting Engine Scanner Over HTTP...

Forensics Details

Resource: http://google.com/

Suppressed Logs: 31

Packet Capture Unique Id: time1621013780.id311f2500.blade02
time1621013780.id37204d98.blade02
time1621013780.id3405c660.blade02
[less](#)

Packet Captures: src-192.168.20.50.cap

Packet Capture: Packet Capture

Threat Wiki: [Go to Threat Wiki](#)

Advanced Forensics Details

Method: OPTIONS

Actions

Remediation: [Go to Remediation Options](#)

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

More

Id: 6ba2ea18-44b6-14f8-609e-b51400000005

Marker: @A@@B@1620997375@C@339949

Log Server Origin: cloudguard-gw-vm (10.186.0.3)

Id Generated By Indexer: false

First: false

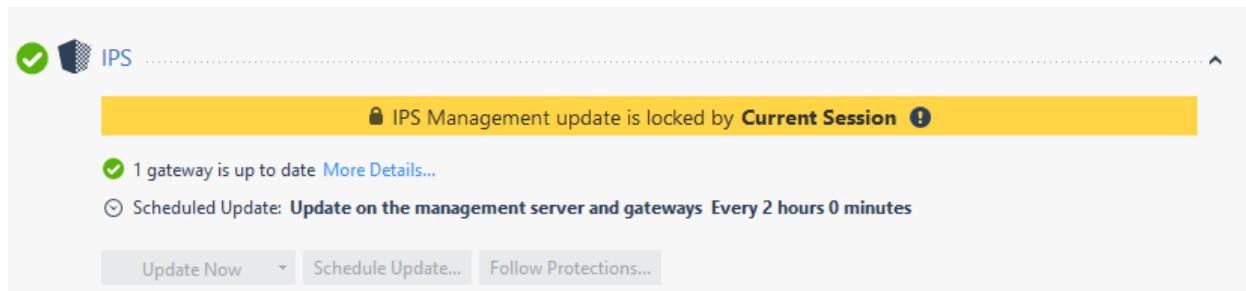
Sequencenum: 3

Reiert Id Kid: 609eh514-4-18eaa26h-f814h644

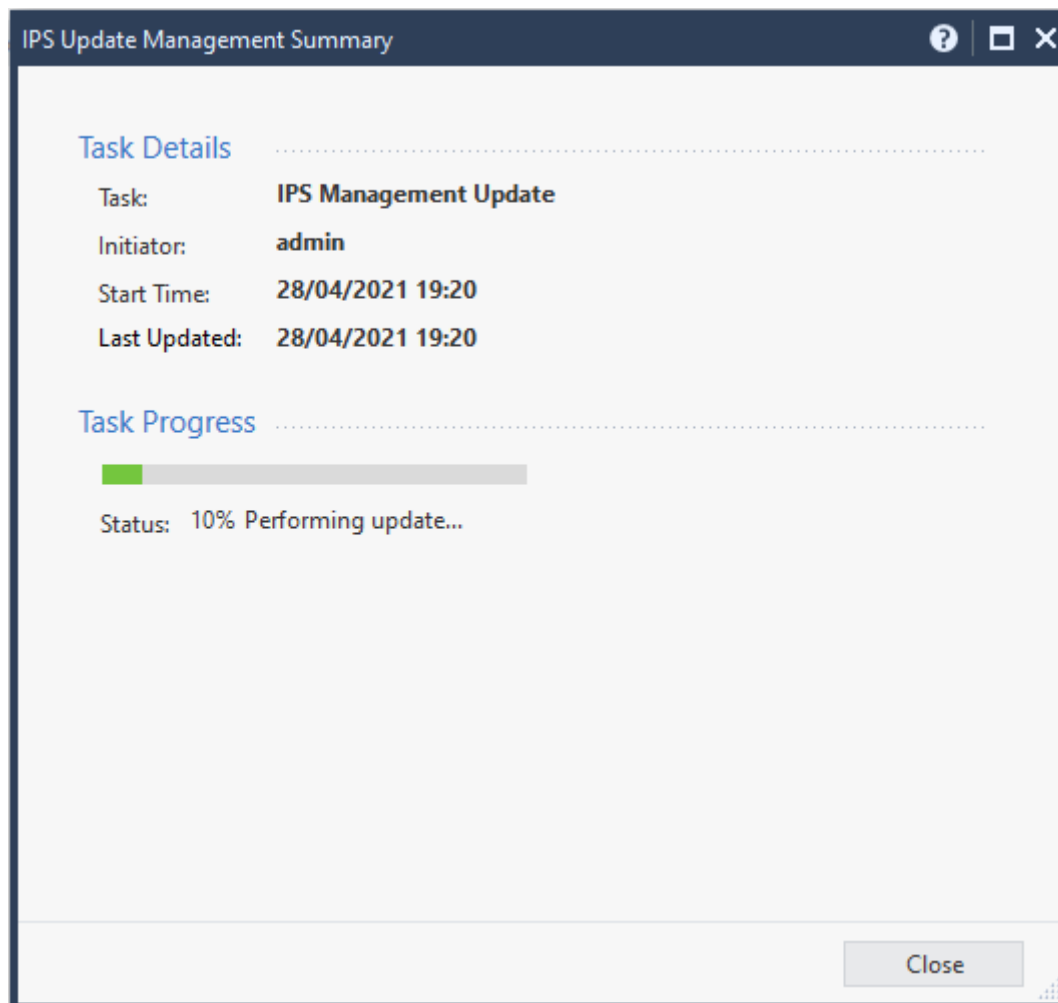
Erkannter Nmap-Script-Scan: Details

Aufgetretene Probleme

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



Das Update blockiert bis die aktuelle Session beendet wird.

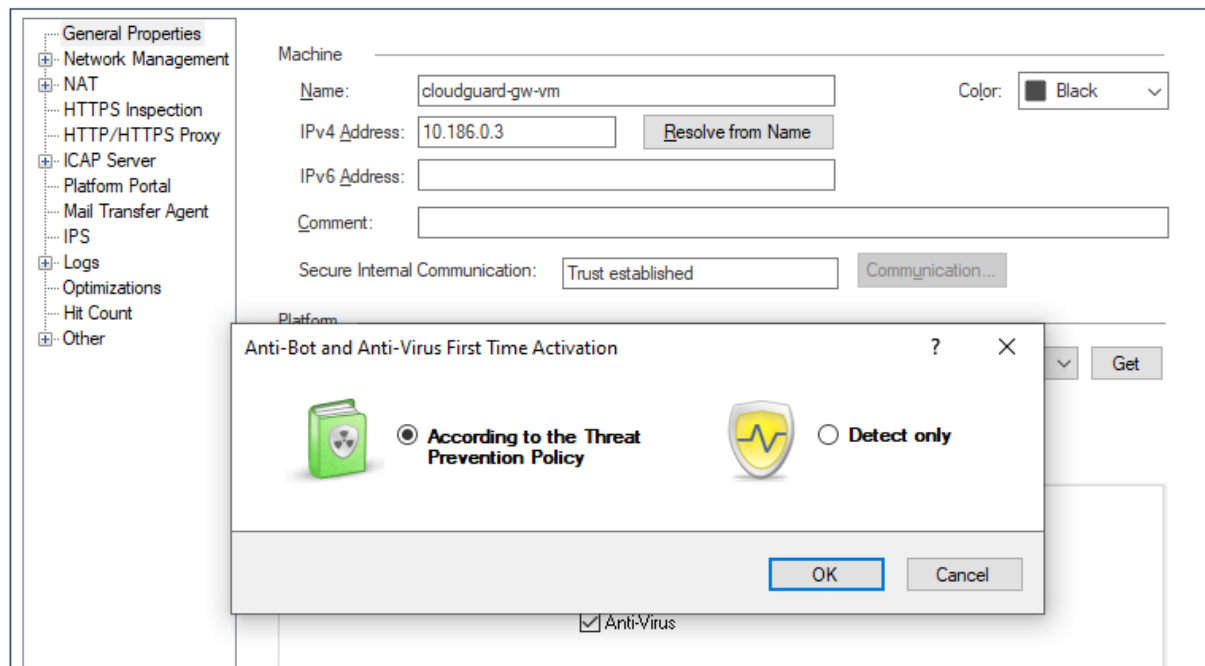


Was leider übersehen wurde, weswegen sehr lange auf die Fertigstellung gewartet wurde.

Lab 2.2 Anti-Virus

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

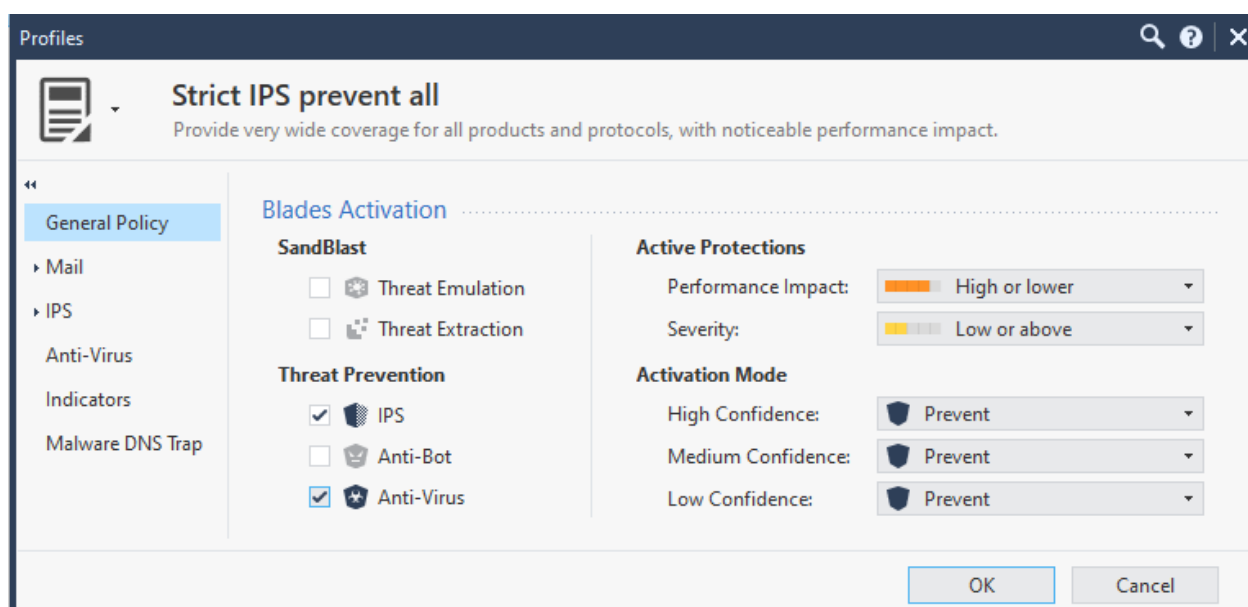
2.2.2 Aktivierung Blade: Anti-Virus



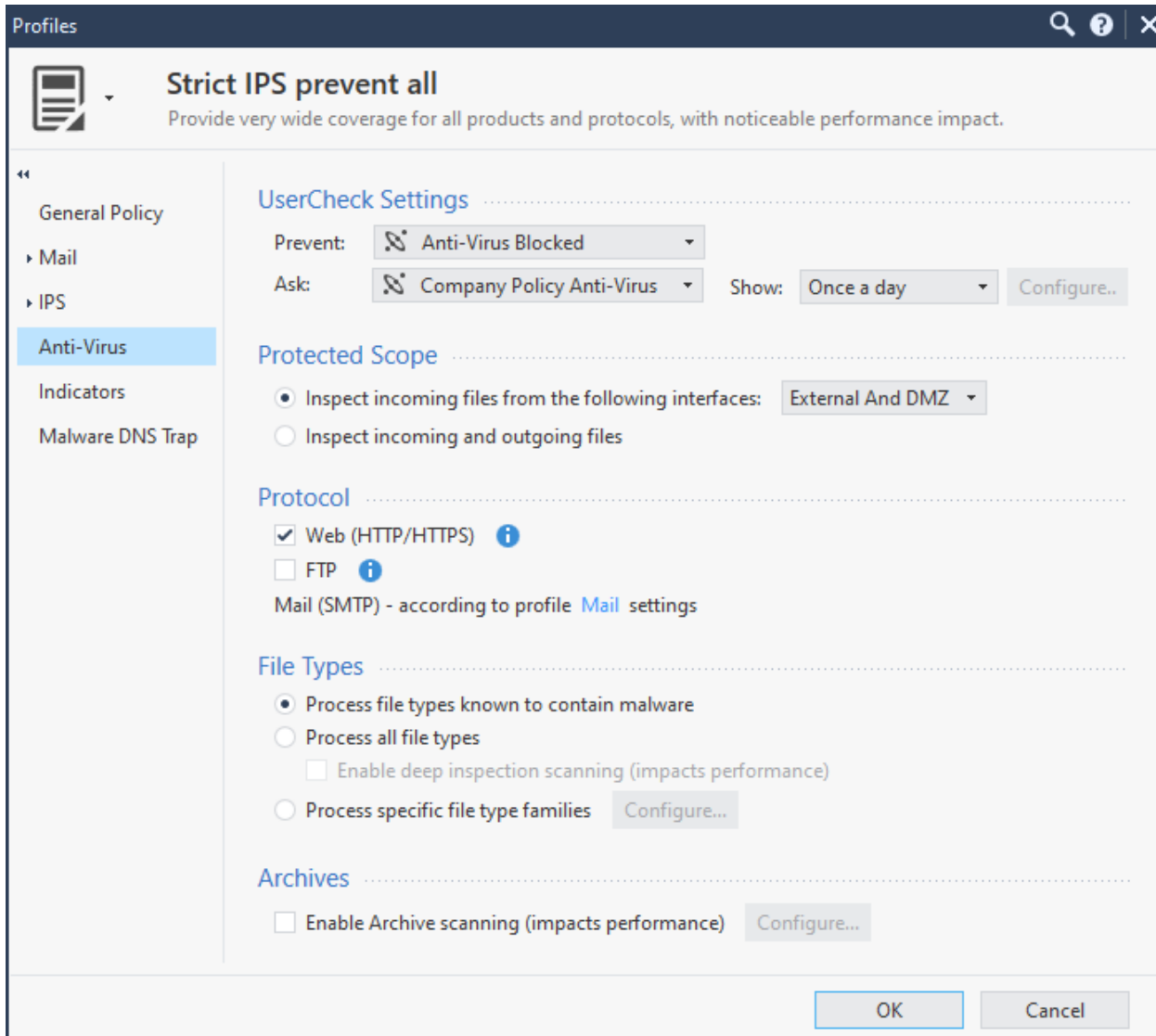
Anti-Virus Blade aktiviert "According to the Threat Prevention Policy"

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

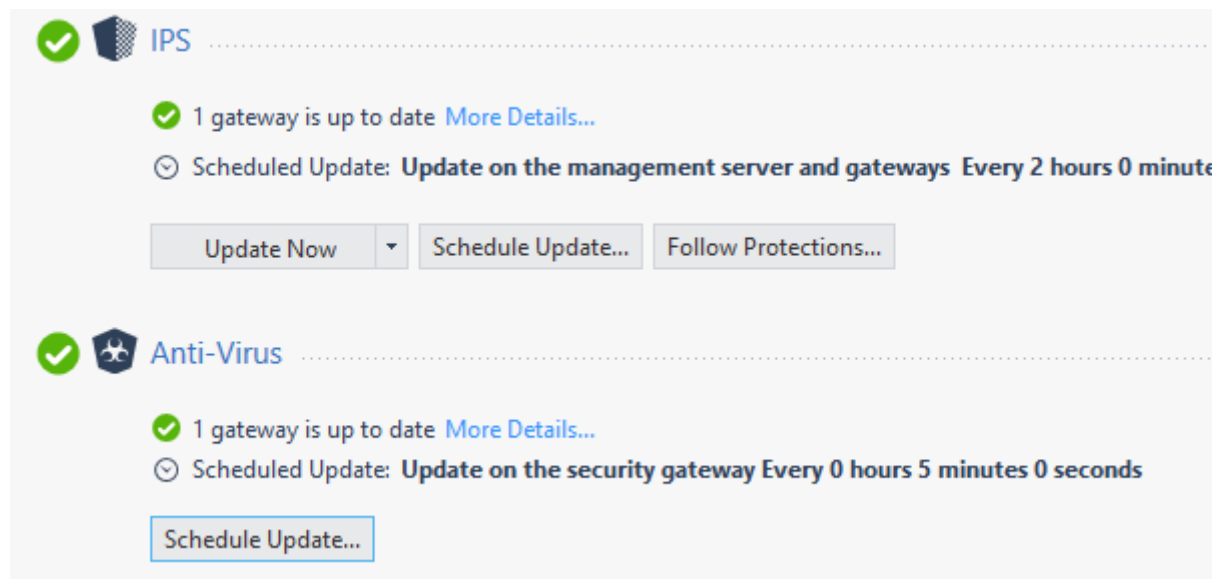


Anti-Virus Detailseite, hier wurde später auch der Archiv-Scan und Scan aller Datei-Typen aktiviert

Protected Scope	Protection/Site/File/Blade	Action	Track	Install On
Linux Instance	N/A	Strict IPS prevent all	Log Packet Capture Forensics	* Policy Targets

Die aktualisierte Security Policy

2.2.7 Update Anti-Virus

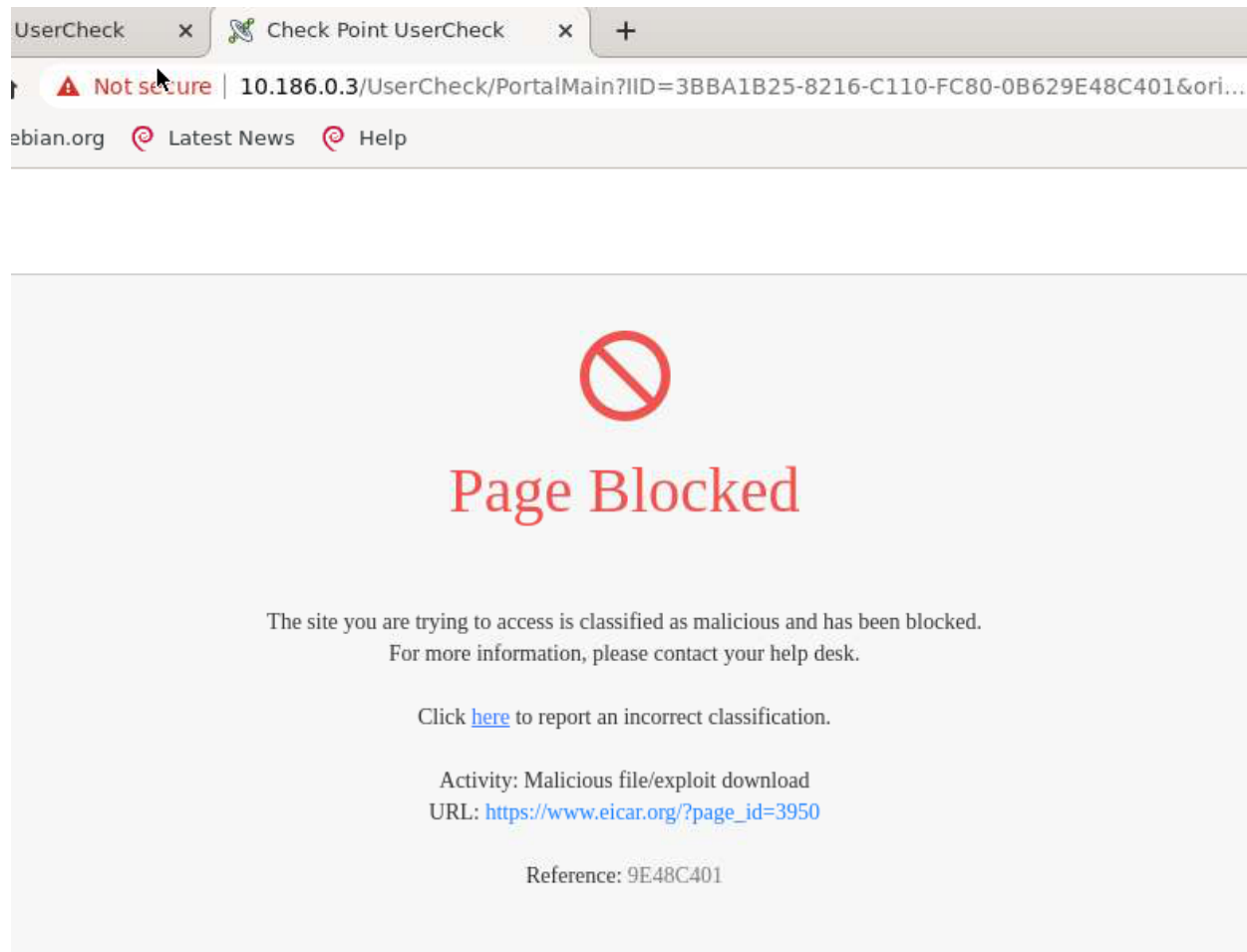


Es gibt keinen manuellen Update-Button, also wurde auf alle 5 Minuten gestellt und kurz gewartet.

2.2.8 Testlauf Anti-Virus

```
Terminal - cs20m027@linux-vm: ~
File Edit View Terminal Tabs Help
cs20m027@linux-vm:~$ curl -O http://rexswain.com/eicar.com
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
           %             Dload  Upload  Total   Spent    Left     Speed
100    5    0    5    0    0    13    0  --:--:-- --:--:-- --:--:--    13
cs20m027@linux-vm:~$ cat eicar.com
cs20m027@linux-vm:~$
```

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



Ebenso via Browser

Log Details

Block
192.168.20.50 performed access to site known to contain malware that was blocked

Details | **Matched Rules**

Log Info

Origin	cloudguard-gw-vm
Time	Today, 11:03:53
Blade	Anti-Virus
Product Family	Threat
Type	Log
Scope	Linux Instance (192.168.20.50)

Forensics Details

Resource	http://rexswain.com/eicar.com http://rexswain.com/eicar.com more
Suppressed Logs	3
Vendor List	Check Point ThreatCloud
Packet Capture	Packet Capture
Threat Wiki	Go to Threat Wiki

Policy

Action	Block
Threat Prevention Rule Id	227D6BCD-3280-4894-B0EB-OFF6A5...
Threat Prevention Policy	Standard
Policy Date	Yesterday, 20:16:26
Threat Prevention Policy ...	Today, 10:42:32
Policy Name	Standard
Policy Management	cloudguard-gw-vm
Threat Profile	Go to profile
Add Exception	Add Exception...

Advanced Forensics Details

Method	GET
Http Host	rexswain.com
User Agent	curl/7.64.0

UserCheck

UserCheck ID	AE6F978F-2F23-213D-6DCE-F233DB4... more
User Check	1
DLP Incident UID	60A0DFF9-0000-0002-ECAB-CCF3F49... more
UserCheck Message to U...	The site you are trying to access is d...

Blockierte Eicar Test-Malware über HTTP

Log Details

Block
Linux Instance (192.168.20.50) accessed ngcobalt397.manitu.net (89.238.73.97) Today at 18:23:28

Log Info

Origin	cloudguard-gw-vm
Time	Today, 18:23:28
Blade	Anti-Virus
Product Family	Threat
Type	Log
Scope	Linux Instance (192.168.20.50)

Advanced Forensics Details

Referrer	https://www.google.com/
Content Type	text/html; charset=UTF-8
Http Server	Apache
Method	GET
Http Status	200
Http Host	www.eicar.org
User Agent	Mozilla/5.0 (X11; Linux x86_64) Appl... more

Https Inspection Details

Action	Inspect
--------	---------

UserCheck

UserCheck ID	3BBA1B25-8216-C110-FC80-0B629E4... more
User Check	1
DLP Incident UID	609FF580-0000-0003-1E47-EDBBC6F8... more
UserCheck Message to U...	The site you are trying to access is cl... more

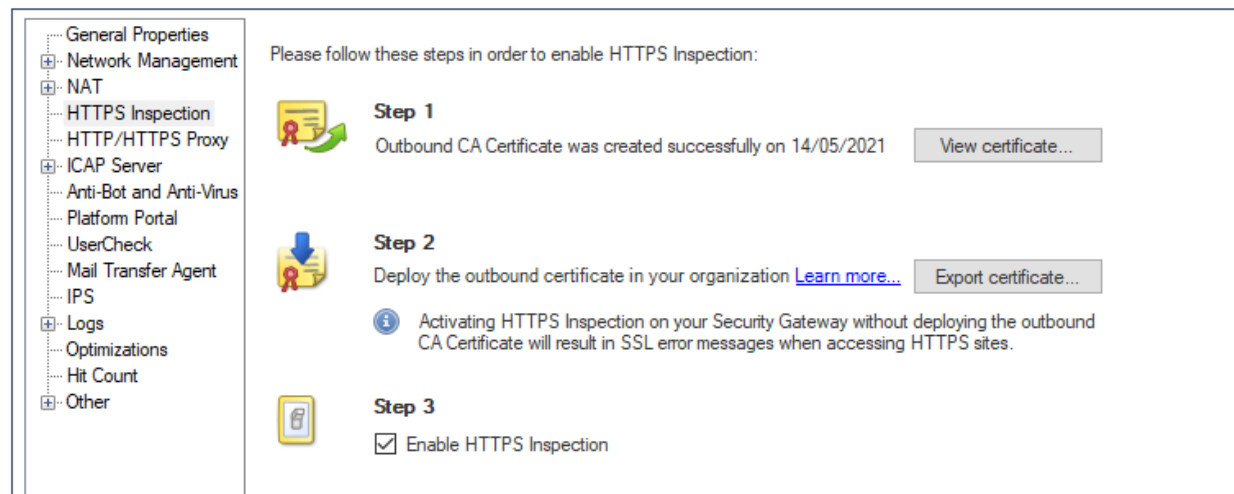
Protection Details

Action	Block
Threat Prevention Rule Id	227D6BCD-3280-4894-B0EB-OFF6A5...
Threat Prevention Policy	Standard
Policy Date	Today, 18:06:12
Threat Prevention Policy ...	Today, 18:06:09
Policy Name	Standard
Policy Management	cloudguard-gw-vm
Add Exception	Add Exception...

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

No.	Name	Source	Destination	Services	Category/Custom A...	Action	Track	Blade	Install On	Certificate	Comment
1	Predefined Rule	* Any	Internet	HTTPS default services	* Any	Inspect	None	* All	* Policy H...	Outbound Certi...	
2		Linux Instance	Internet	HTTPS default services	* Any	Inspect	Log	* All	* Policy H...	Outbound Certi...	

Neue HTTPS-Inspection Policy

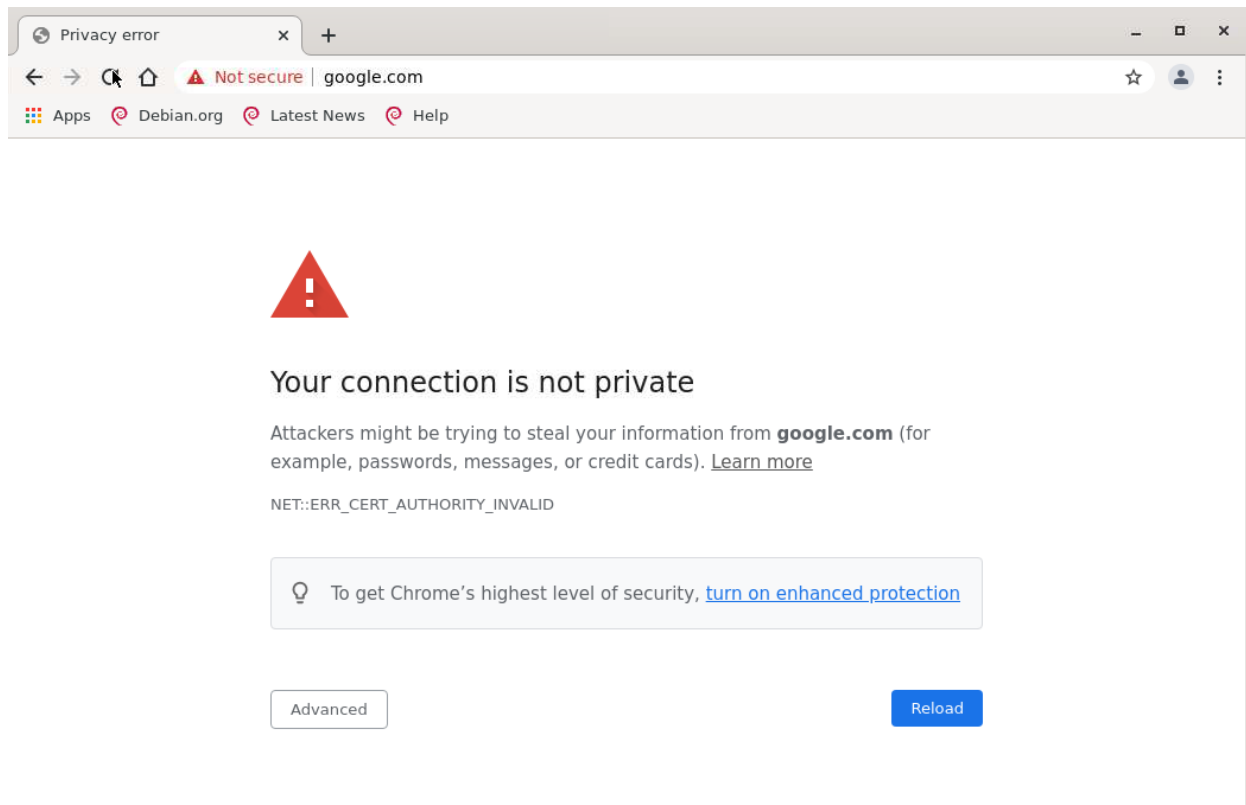
```

Terminal - cs20m027@linux-vm: ~
File Edit View Terminal Tabs Help
cs20m027@linux-vm:~$ sudo cp '/home/cs20m027/Desktop/mycert.cer' /etc/ssl/certs/
cs20m027@linux-vm:~$ curl -k 'https://eicar.org/download/eicar.com.txt'
curl: (52) Empty reply from server
cs20m027@linux-vm:~$

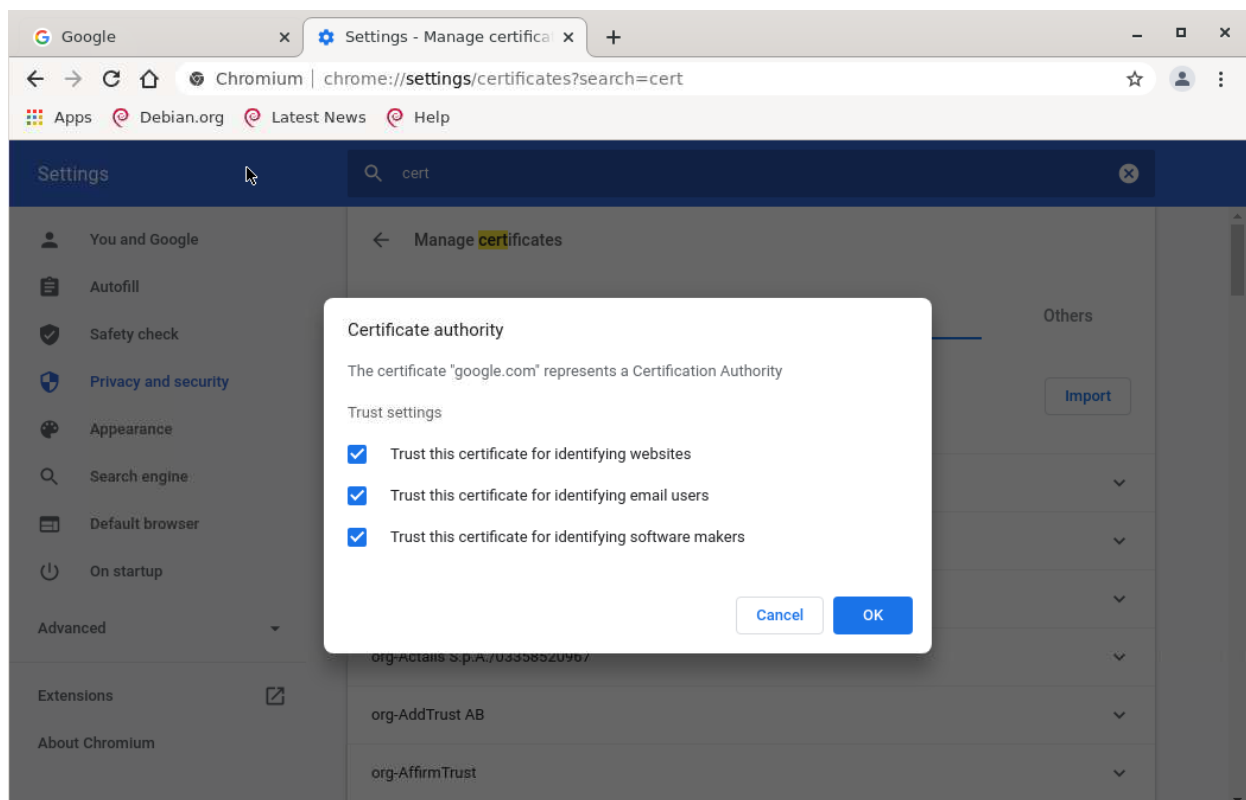
```

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

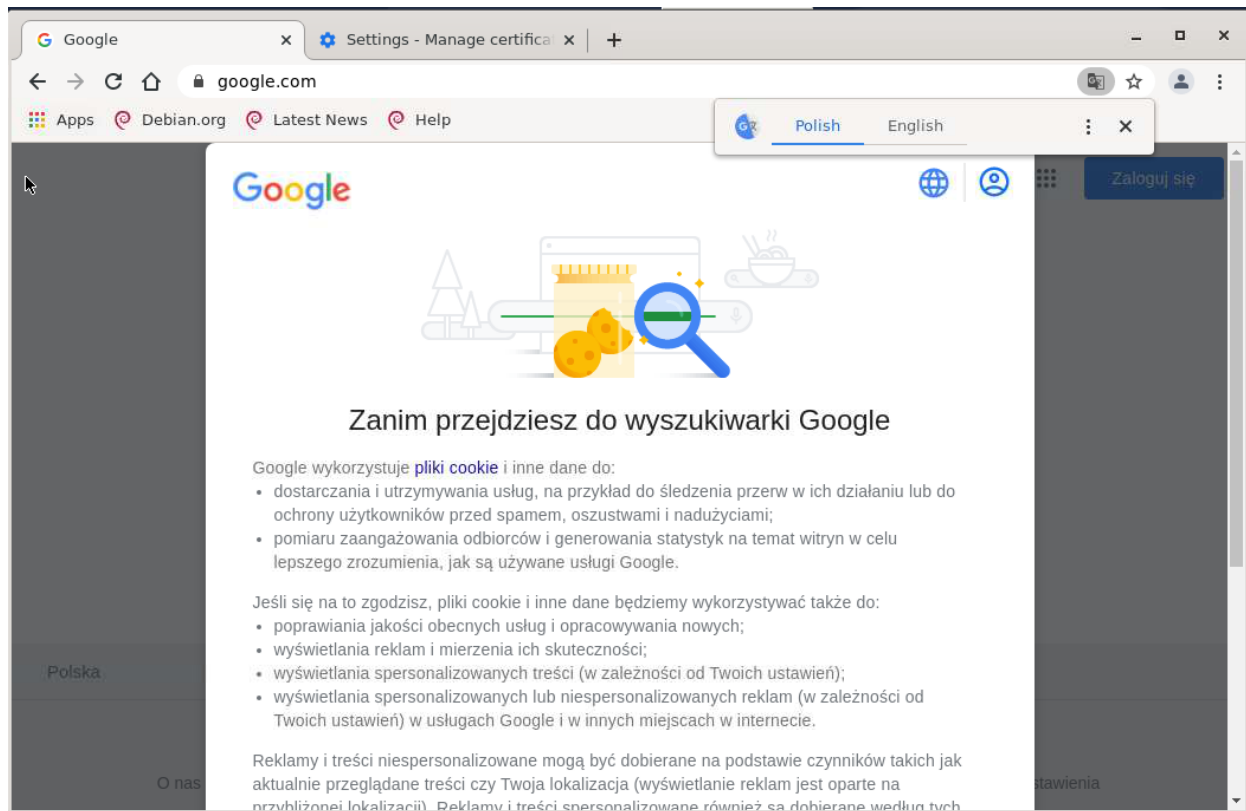
Das `-k` Flag erlaubt die Verwendung von Self-Signed Certificates. Als Browser wurde Chromium verwendet, welcher mit `apt get install chromium` installiert wurde.



HTTPS Fehler bei Besuch einer TLS/SSL Seite



Zertifikatsimport in Chromium



Nach Import des Zertifikates wird keine Warnung generiert

Log Details

Prevent

Prevented eicar av test file originating from 192.168.20.50 against 89.238.73.97

Details | Matched Rules

Log Info

Origin: cloudguard-gw-vm

Time: Today, 21:17:05

Blade: IPS

Product Family: Threat

Type: Log

Policy

Action: Prevent

Access Rule Name: [Linux: Internet access](#)

Threat Prevention Rule Id: 227D6BCD-3280-4894-B0EB-0FF6A5...

Threat Prevention Policy: Standard

Policy Date: Today, 21:00:47

Threat Prevention Policy ...: Today, 21:00:45

Policy Name: Standard

Policy Management: cloudguard-gw-vm

Threat Profile: [Strict IPS prevent all](#)

Add Exception: [Add Exception...](#)

Protection Details

Severity: Medium

Confidence Level: Medium

Forensics Details

Resource: <https://eicar.org/download/eicar.co...>

Suppressed Logs: 2

Packet Captures: [View Packet Capture...](#)

Packet Capture: [Packet Capture](#)

Threat Wiki: [Go to Threat Wiki](#)

Advanced Forensics Details

Content Type: text/plain; charset=utf-8

Http Server: Apache

Content Length: 68

Method: GET

Http Status: 200

Http Host: eicar.org

User Agent: curl/7.64.0

Https Inspection Details

Action: [Inspect](#)

Actions

Remediation: [Go to Remediation Options](#)

Report Log: [Report Log](#)

Detailansicht: Erkanntes Eicar Testfile, auch über HTTPS

nächstes Lab