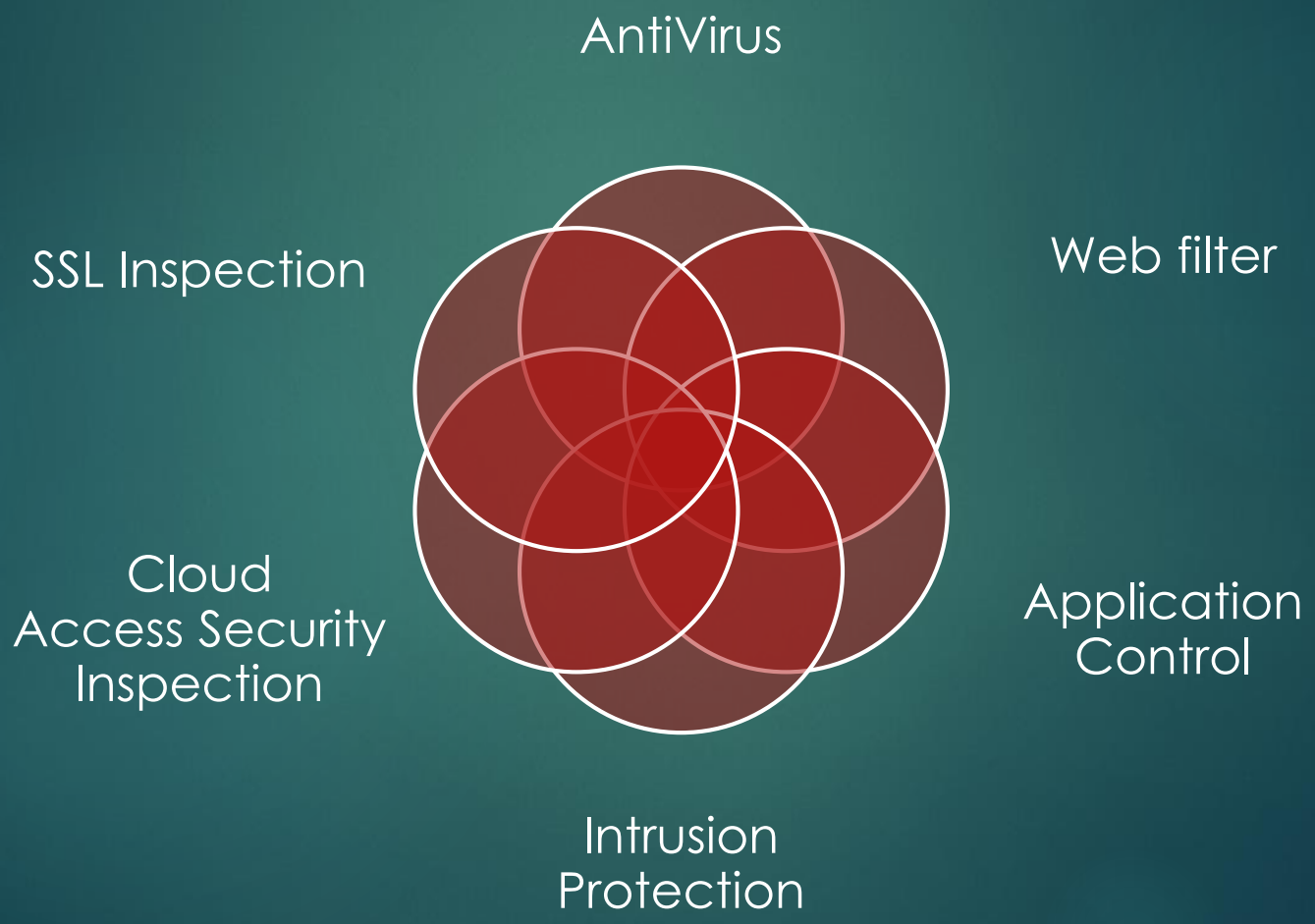
FORTINET

FortiGate 

SECURITY PROFILES CONFIGURATION

Security Profiles
Ausgewählte Features

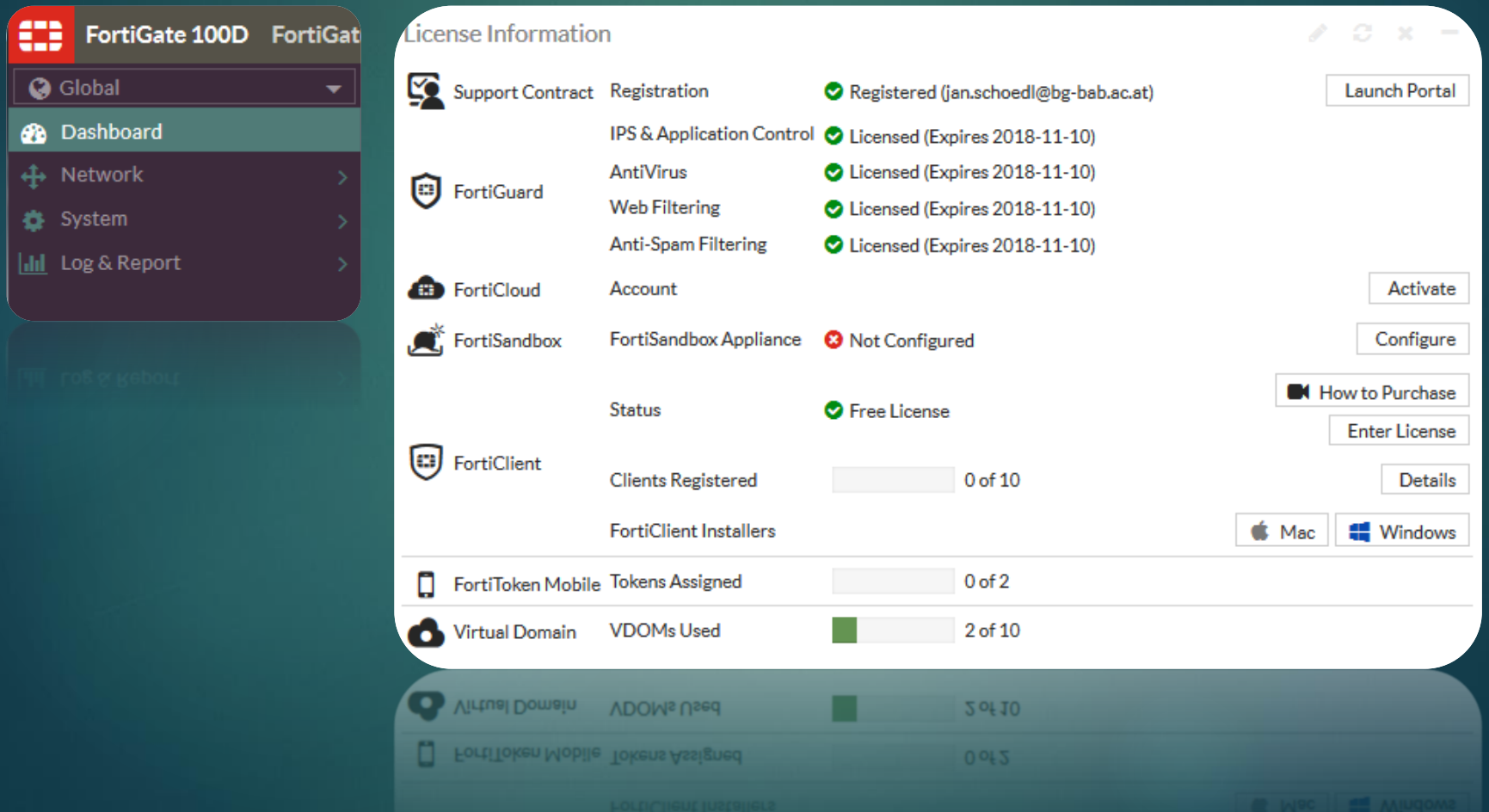


FortiGuard Supscription

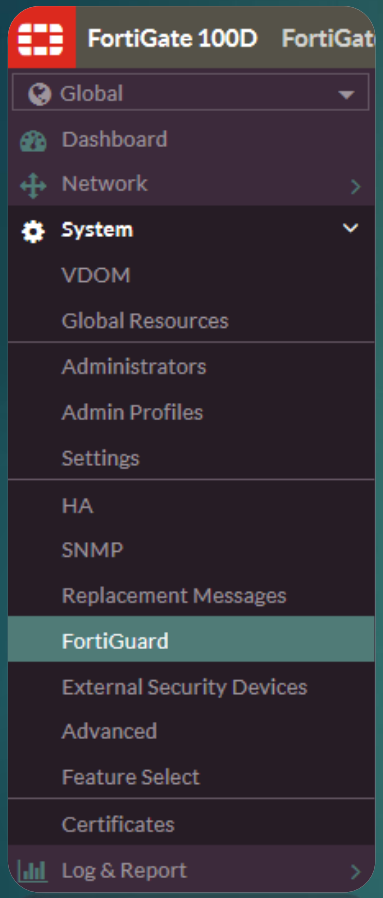
- FortiGuard Subscription für die meisten Services erforderlich
- Bei Neukauf als Bundle integriert
- Verlängerung nach Ablauf jederzeit möglich
- Relativ hohe Kosten
- ~€ 5000 - 3 Jahre Services + 8x5 HW Support für Fortigate 100D

FortiGuard Supscription

- Global Dashboard – Widget License Information



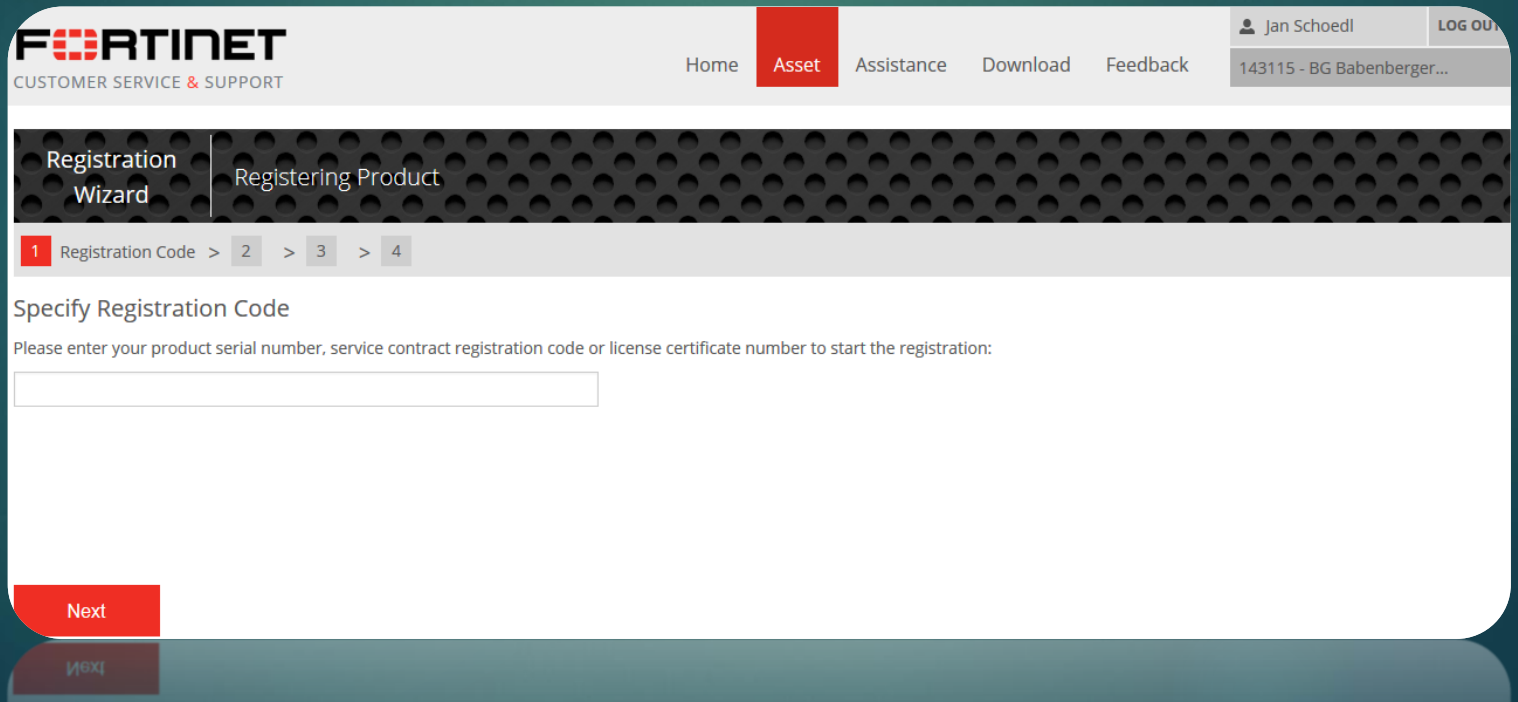
FortiGuard Supscription



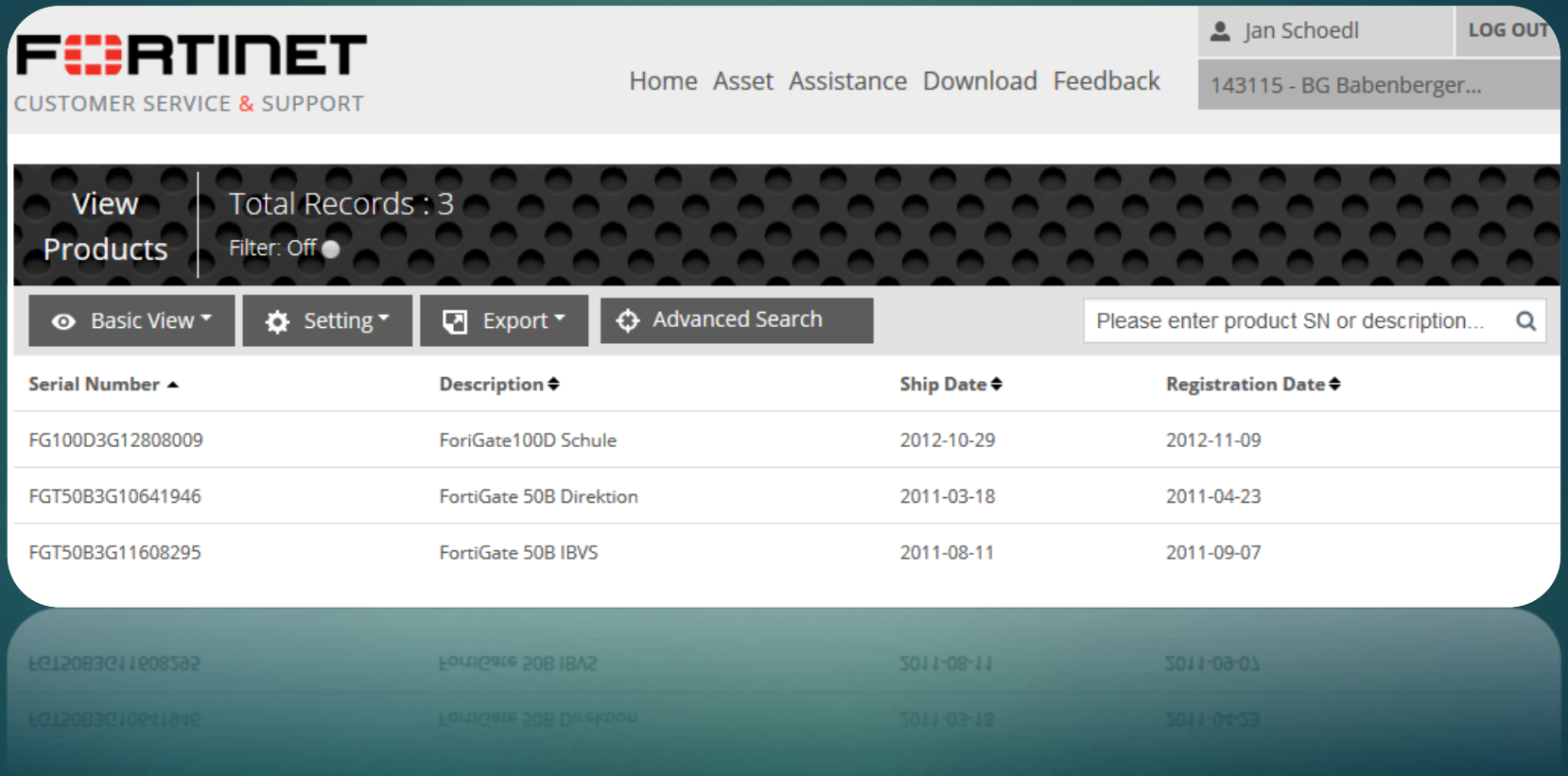
Contract	Status	
FortiCare Support	Registered (jan.schoedl@bg-bab.ac.at)	Launch Portal
Hardware Version	8 x 5 support (Expires on 2018-11-10)	
Firmware	8 x 5 support (Expires on 2018-11-10)	
Enhanced Support	8 x 5 support (Expires on 2018-11-10)	
IPS & Application Control	Licensed (Expires on 2018-11-10)	Upload Package
IPS Definitions	Version 7.00811	
IPS Engine	Version 3.00164	
AntiVirus	Licensed (Expires on 2018-11-10)	Upload Package
AV Definitions	Version 33.00284	
AV Engine	Version 5.00227	
Mobile Malware Definitions	Version 33.00284	
Botnet Definitions	Version 2.00817	View List
SSL-VPN Package	Version 4.0.2300	Upload Package
Web Filtering	Licensed (Expires on 2018-11-10)	
Anti-Spam Filtering	Licensed (Expires on 2018-11-10)	

Registrierung der Services

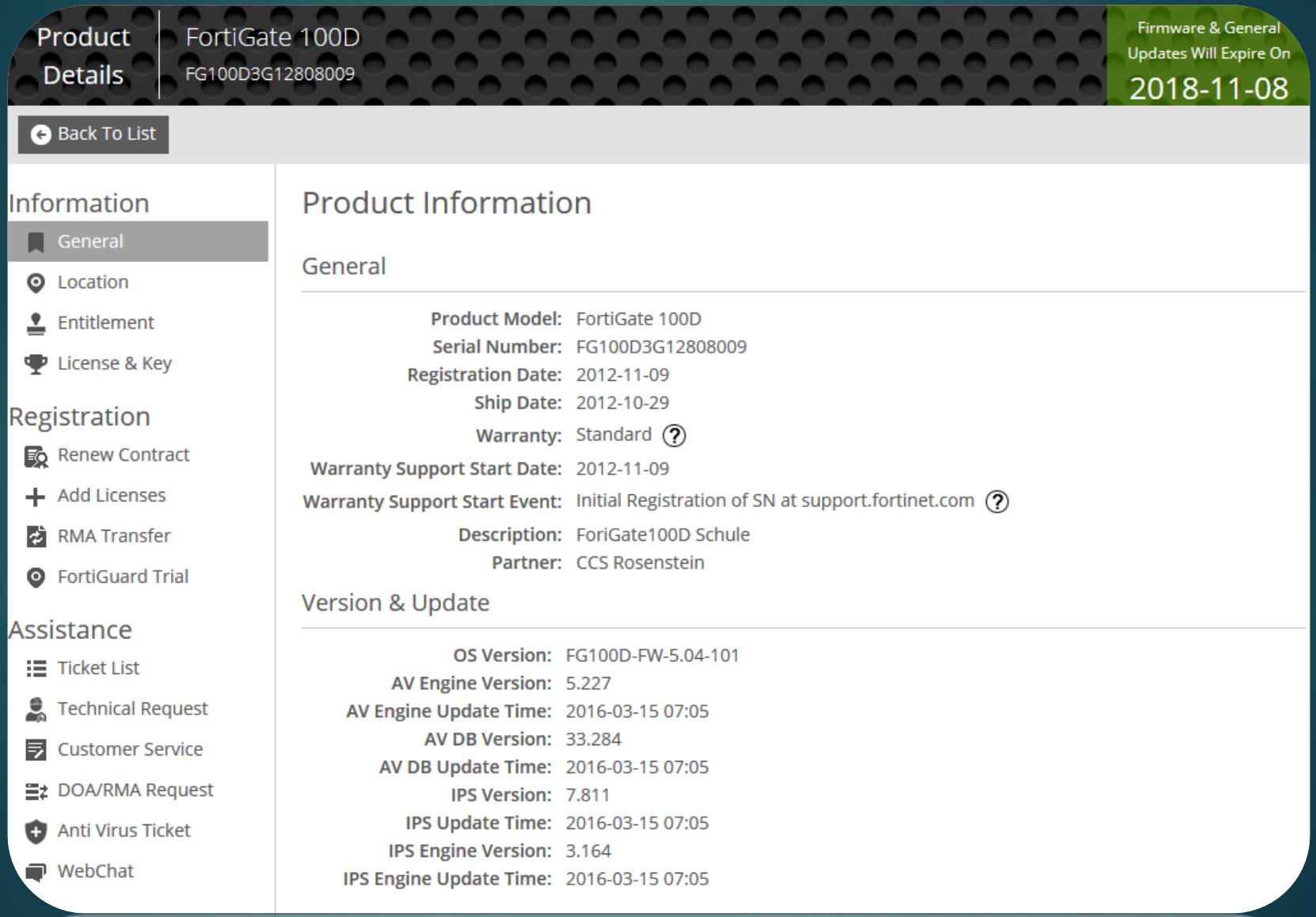
- Account auf **support.fortinet.com** erstellen
- Gerät mit SN registrieren (Bundle)
- oder Service Contract Code bei Verlängerung



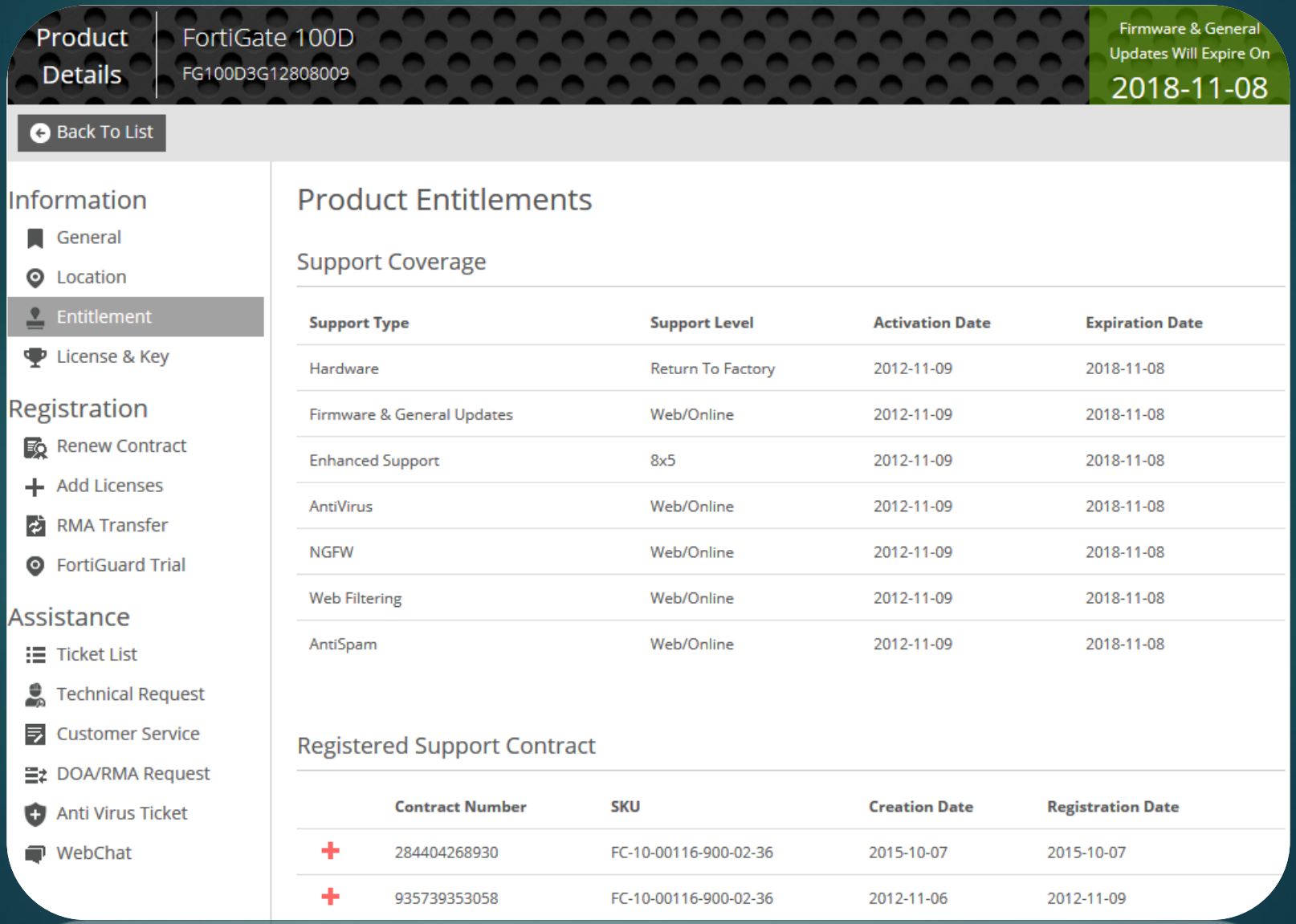
Registrierung der Services



Registrierung der Services



Registrierung der Services



Analysemethoden

Traffic Inspection

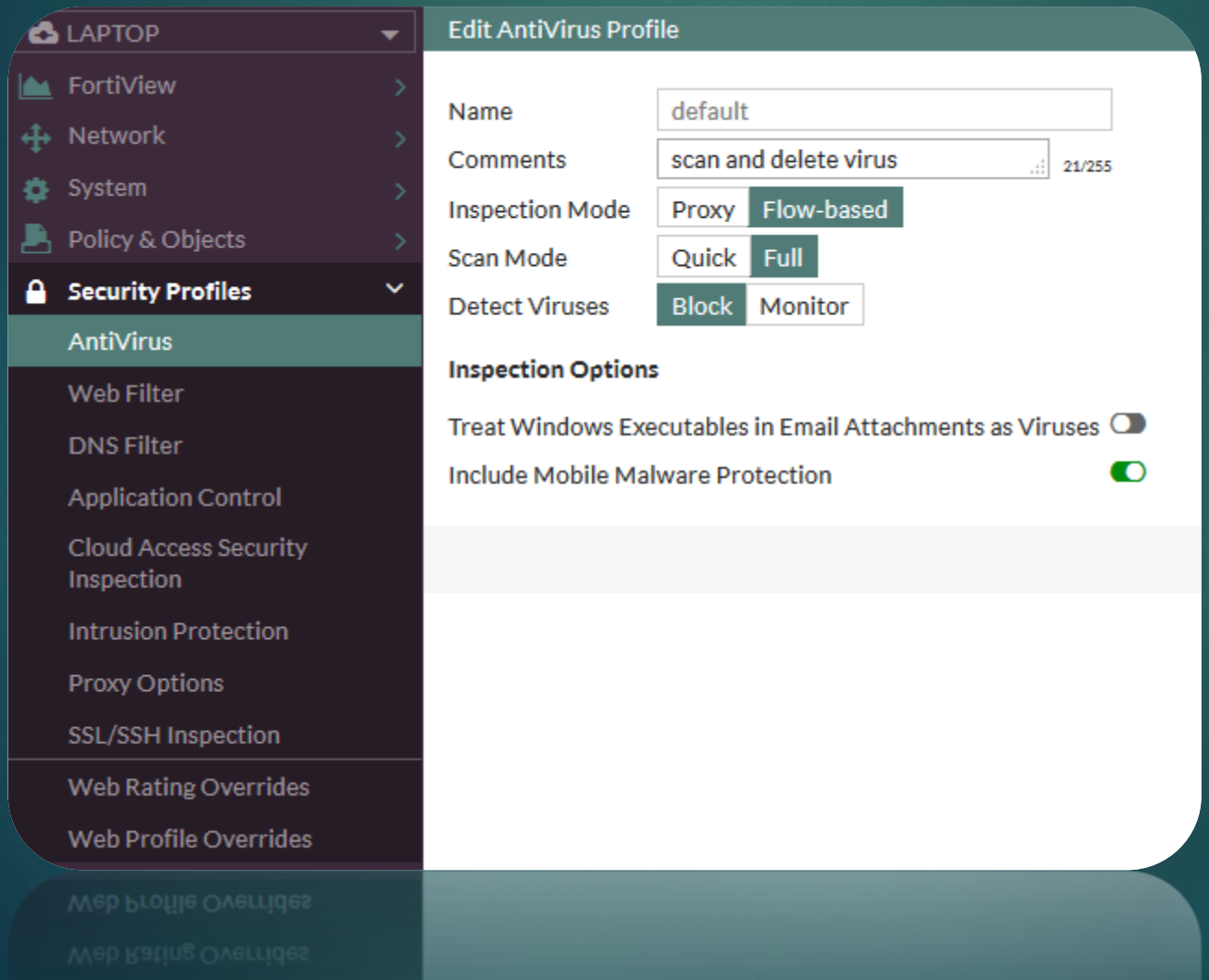
- Daten werden paketweise analysiert
- Paketfragmente werden zuerst zusammengesetzt
- IPS, Application Control, SSL Inspection

Content Inspection

- Datenpakete werden gepuffert, bis Inhalte komplett sind
- AntiVirus, Web Filter, DNS Filter, Anti Spam, DLP

AntiVirus

Allgemeine Einstellungen



Scanning Modes

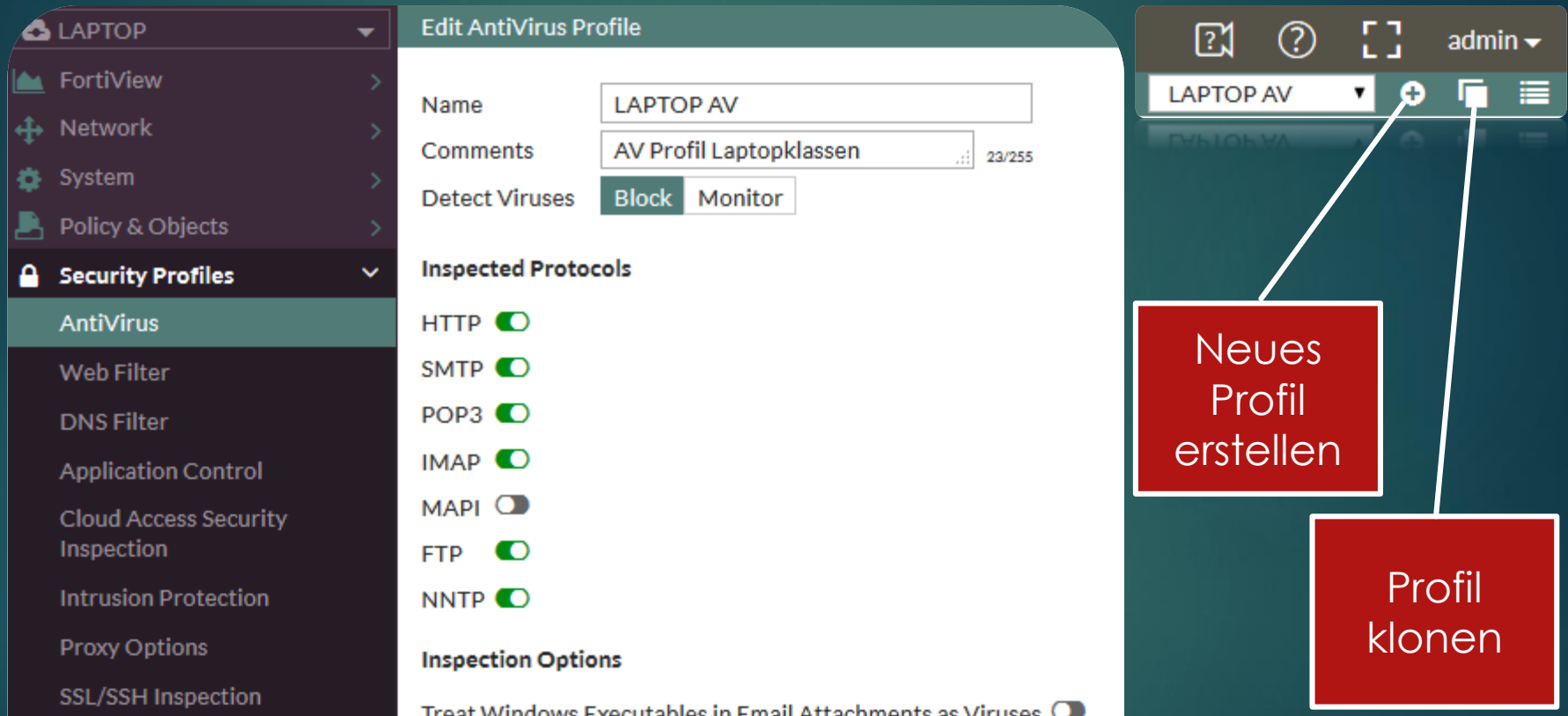
Proxy

- Gründlich, Sicher
- Gesamte Datei muss vorhanden sein
- Dateien werden gepuffert
- Puffergröße 10MB
- Wartezeit für Client
- Infektion kann nicht übersehen werden (Paketfragmentierung)

Flow-based

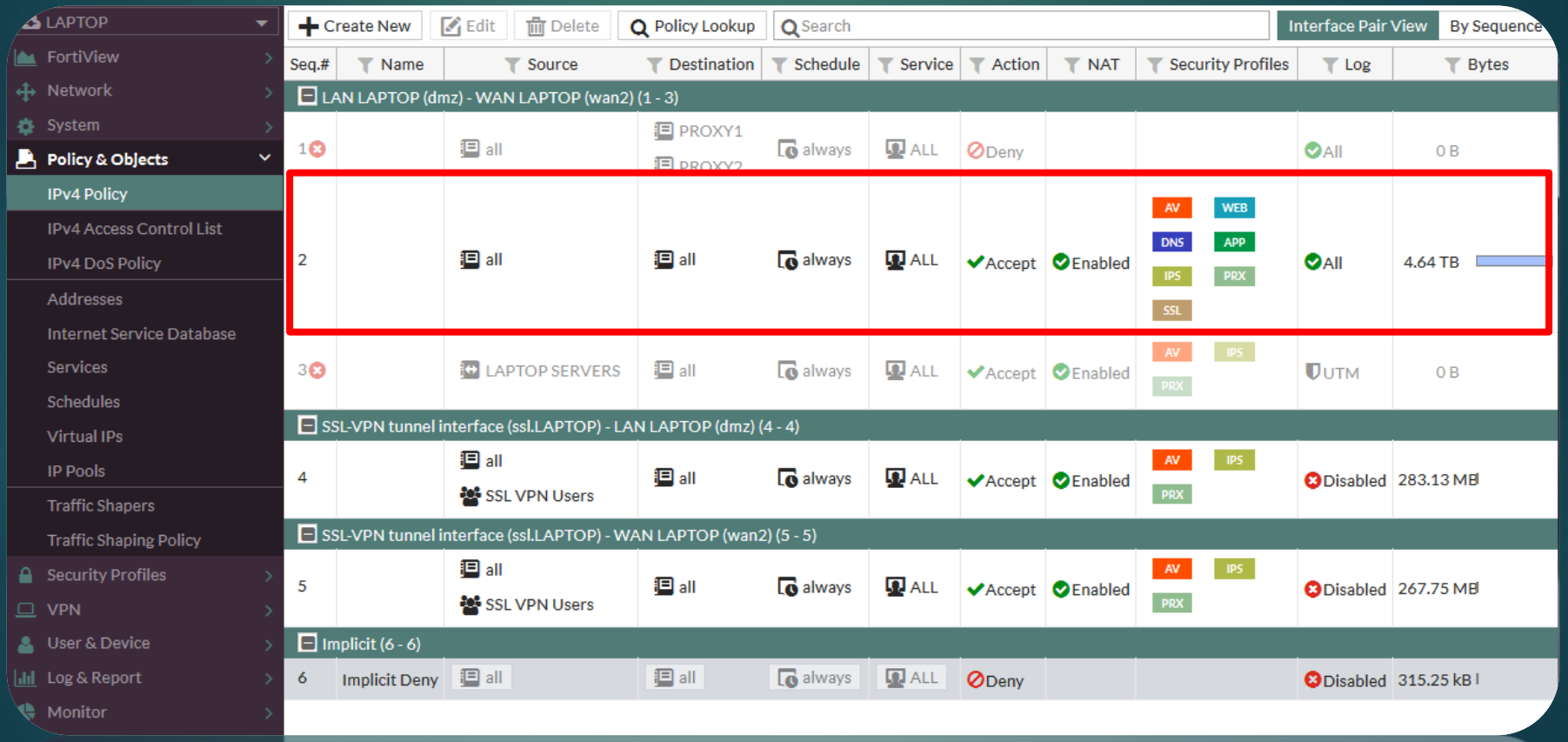
- Performanceorientiert Quick / Full Mode
- Pakete werden zum Client gestreamt
- Letztes Paket nach Abschluss des Scans
- Bei Infektion wird Paket verworfen
- Download wird abgebrochen, da Datei nicht zusammengesetzt werden kann

AntiVirus Profile

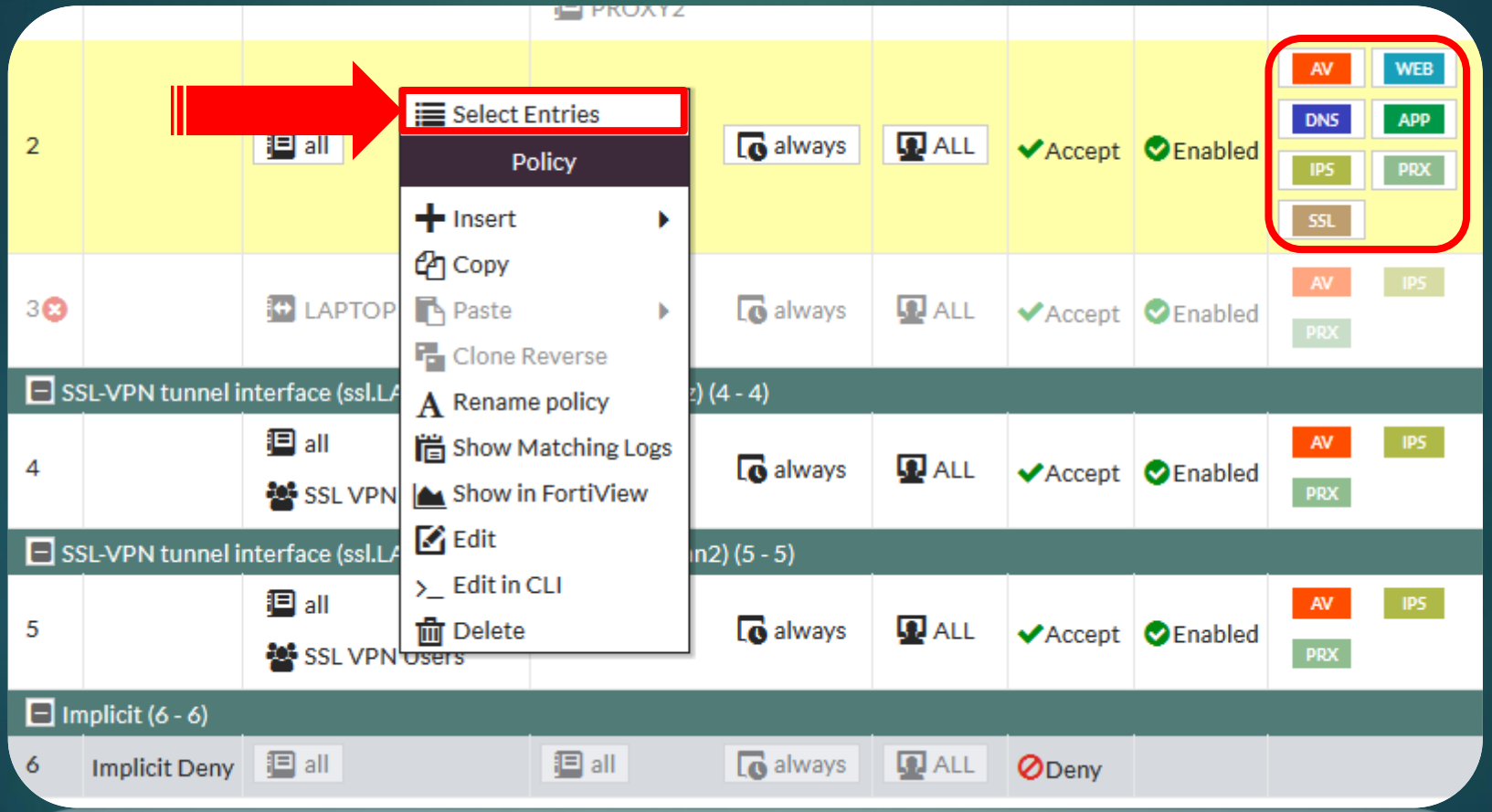


AntiVirus Profil zuweisen

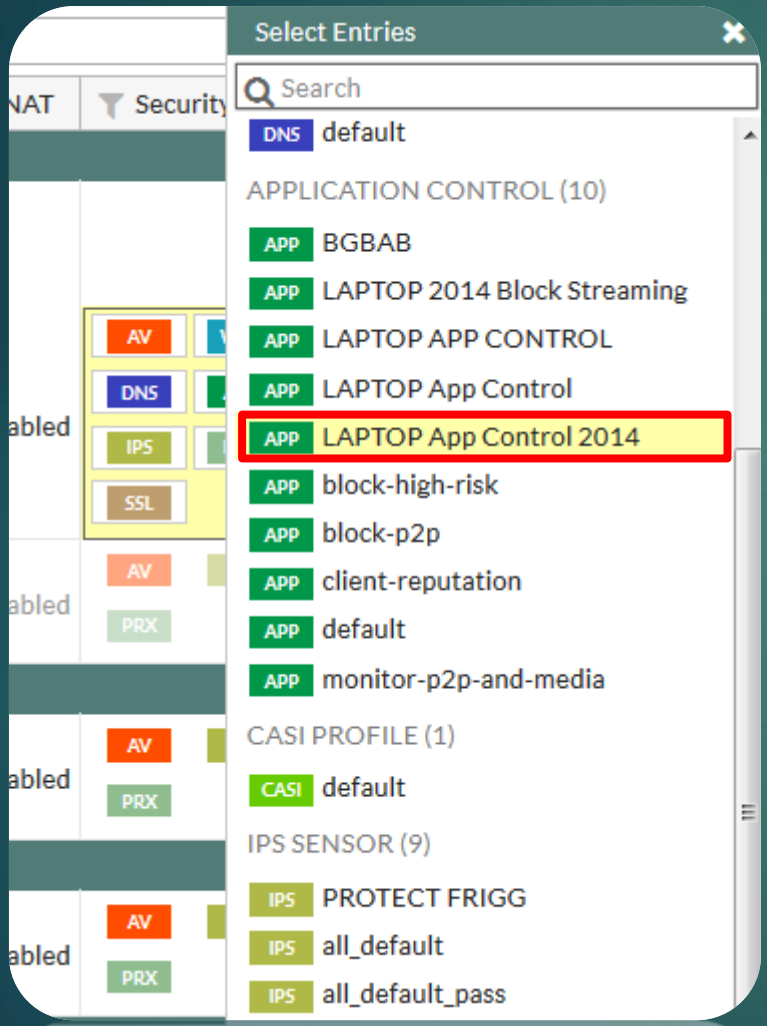
Security Profiles werden immer einer Firewall Policy zugewiesen

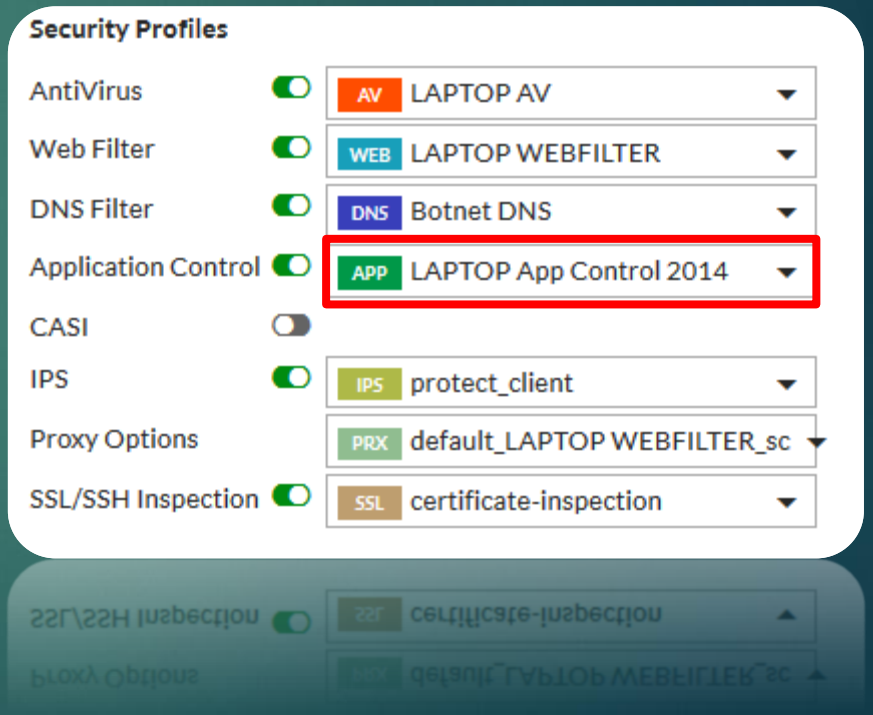


AntiVirus Profil zuweisen

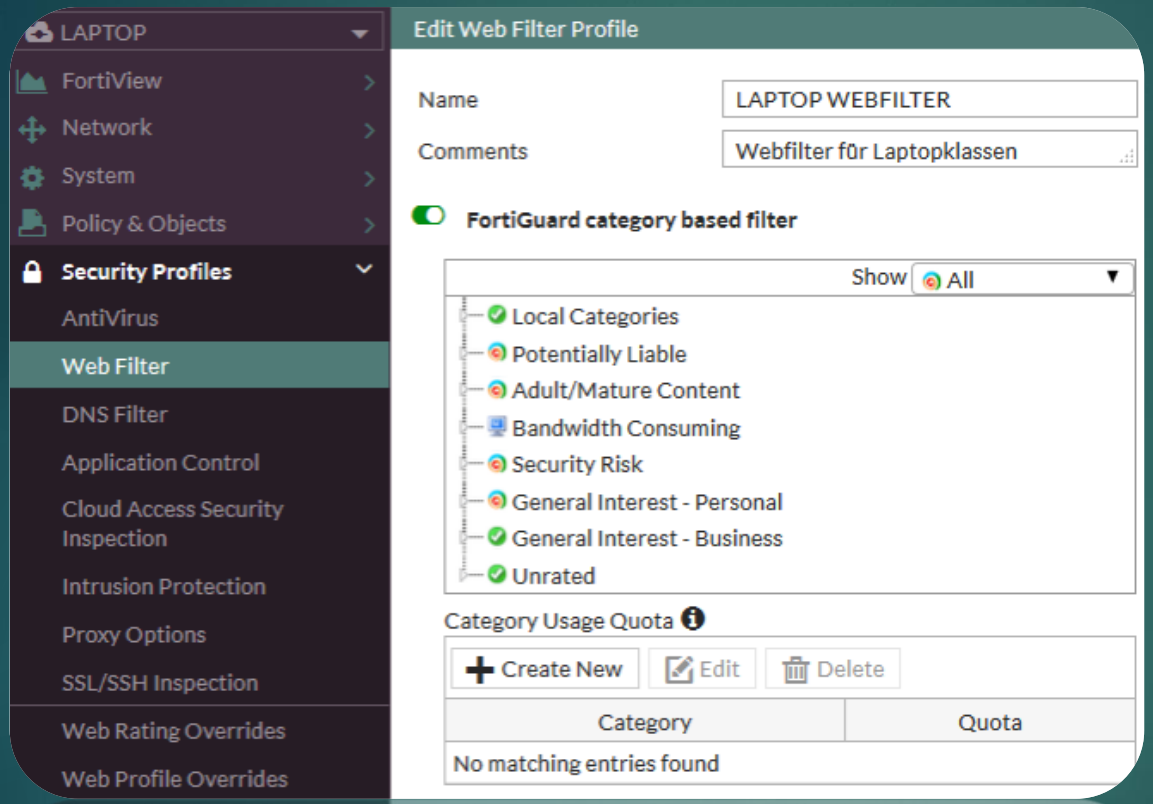


AntiVirus Profil zuweisen





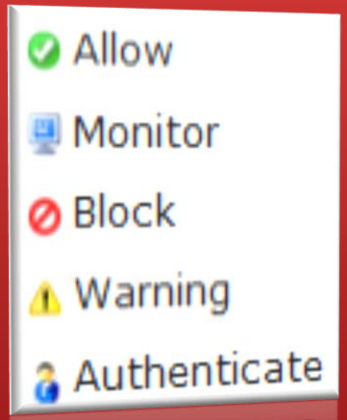
Webfilter


LAPTOP
FortiView
Network
System
Policy & Objects
Security Profiles
AntiVirus
Web Filter
DNS Filter
Application Control
Cloud Access Security Inspection
Intrusion Protection
Proxy Options
SSL/SSH Inspection
Web Rating Overrides
Web Profile Overrides
Edit Web Filter Profile
Name
LAPTOP WEBFILTER
Comments
Webfilter für Laptopklassen
FortiGuard category based filter
Show
All
Local Categories
Potentially Liable
Adult/Mature Content
Bandwidth Consuming
Security Risk
General Interest - Personal
General Interest - Business
Unrated
Category Usage Quota
Create New
Edit
Delete
Category
Quota
No matching entries found


admin
LAPTOP WEBFILTER
Neues Profil erstellen
Profil klonen

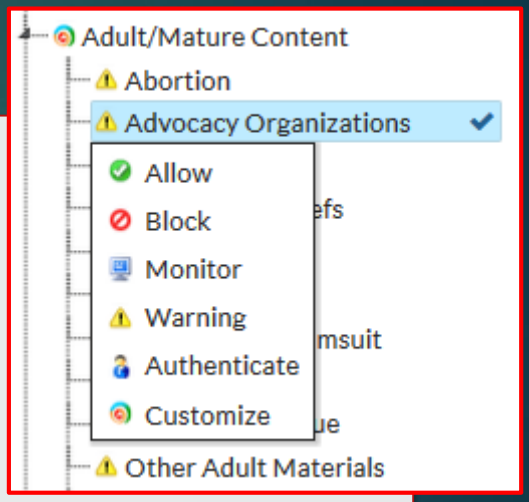
Webfilter - Reihenfolge

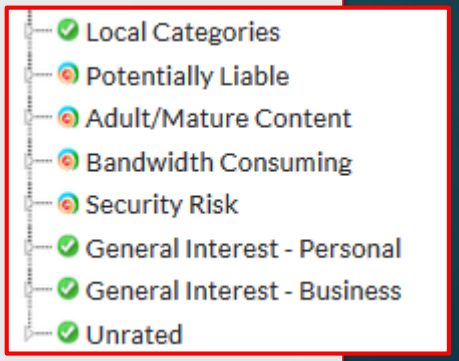
Funktionsweise Fortiguard Categories



Aktionen auswählen für

- Unterkategorien
- Kategorien





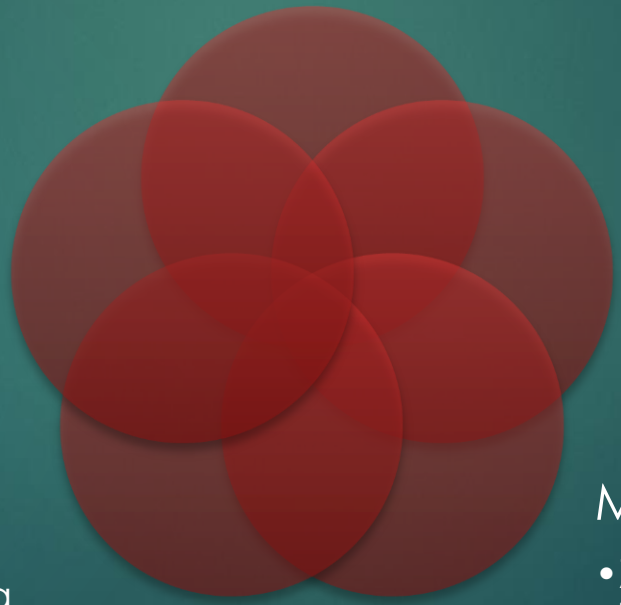
Funktionsweise Fortiguard Categories

ALLOW

- Zugriff auf Seiten der Kategorie zulassen

AUTHENTICATE

- Seiten nach Authentifizierung erlaubt



BLOCK

- Zugriff auf Seiten der Kategorie sperren

WARNING

- Warnmeldung vor Zugriff

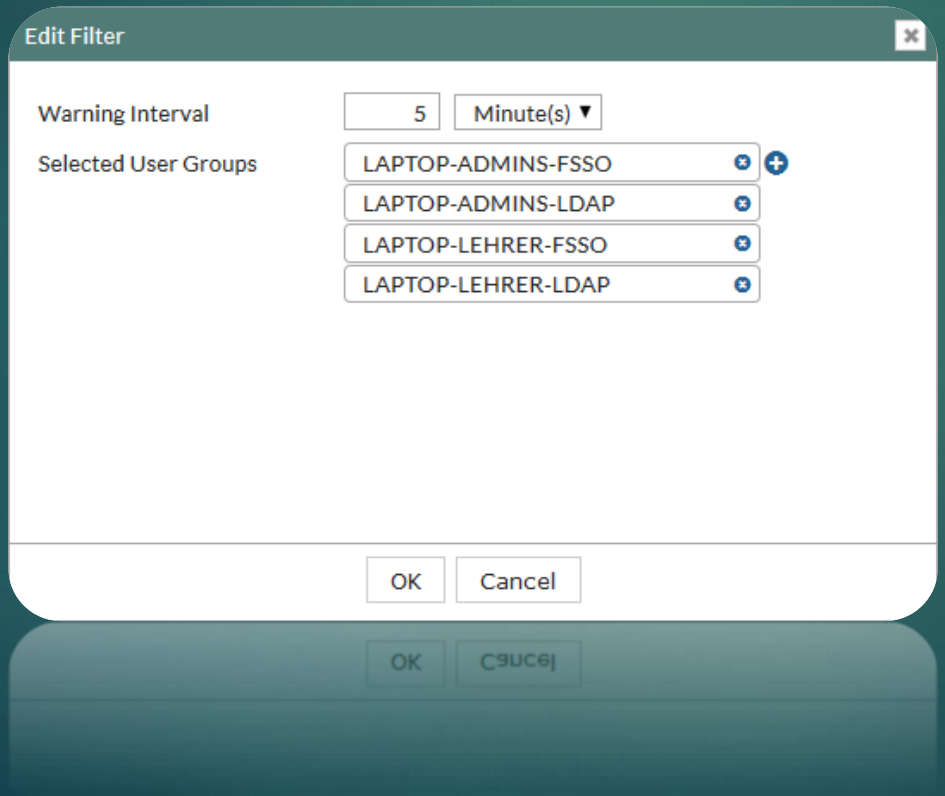
MONITOR

- Zugriff erlauben, jedoch mit Logging

AUTHENTICATE

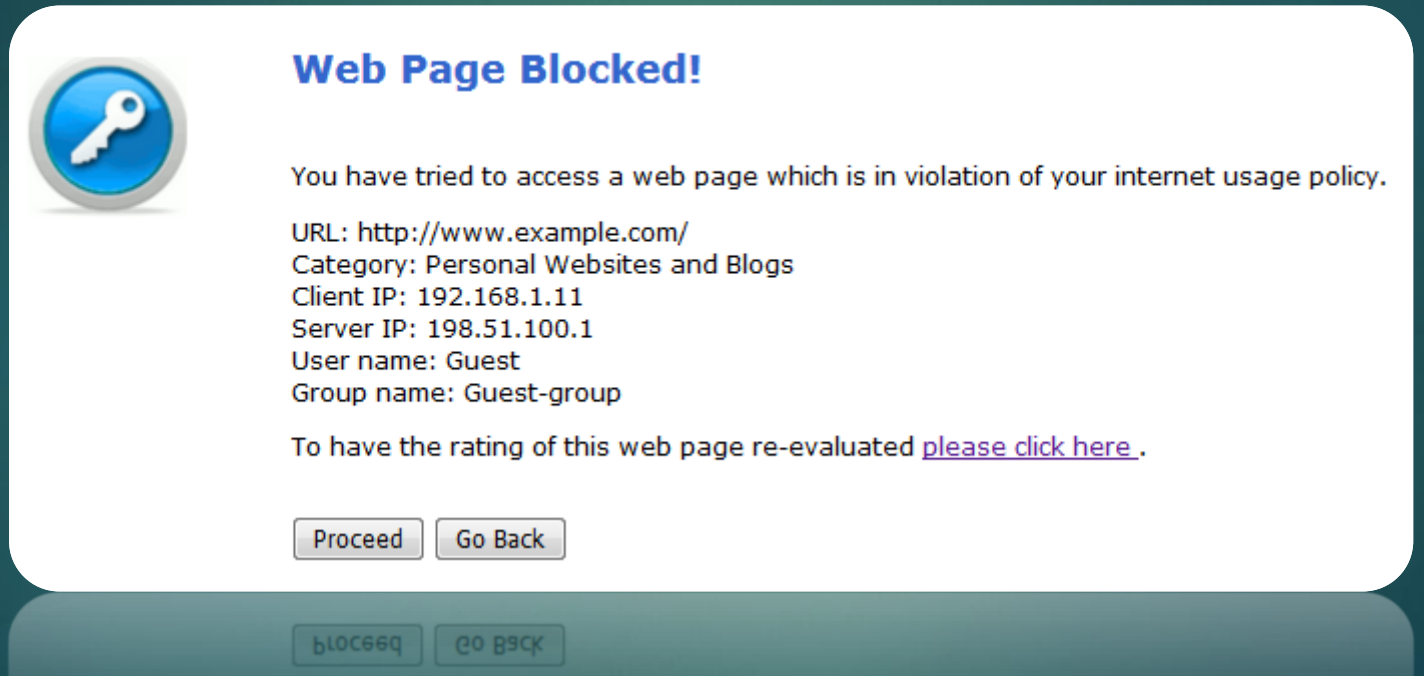
Authenticate

- Bekannten Gruppen und Usern kann Zugriff gewährt werden



AUTHENTICATE & WARNING

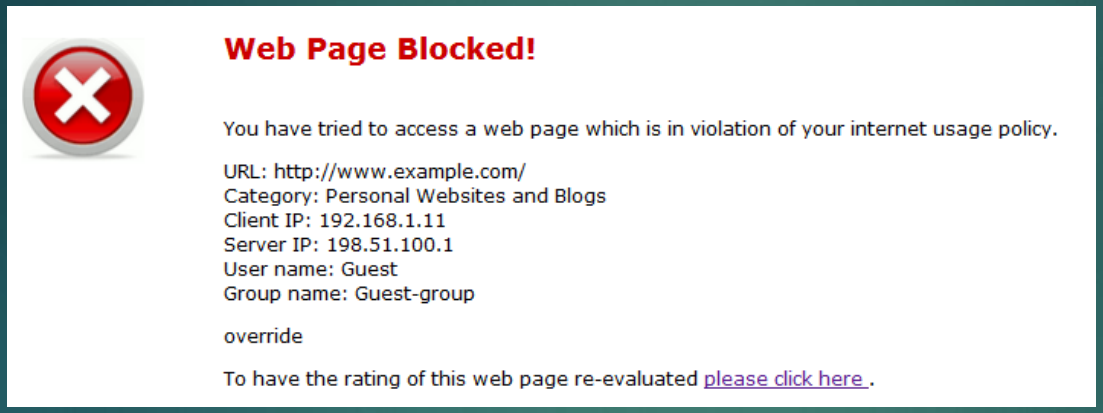
- *Authenticate / Warning* aus Sicht den Benutzers



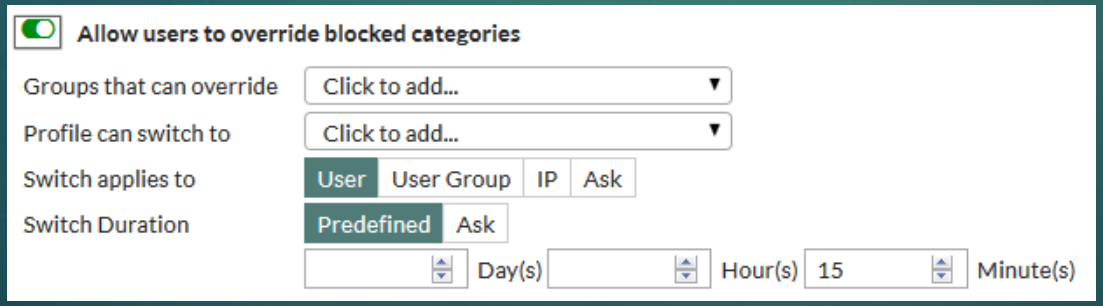
- *Warning* verlangt kein Passwort nach *Proceed*

BLOCKED

- Block erlaubt standardmäßig keinen Override



- Folgende Einstellung im Webfilter erlaubt es dennoch



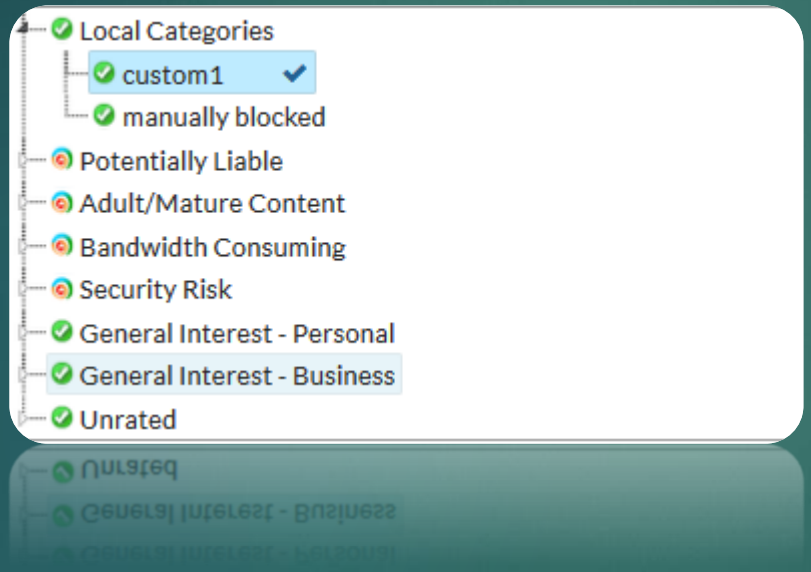
PERMANENTE OVERRIDES

- Erstellen einer lokalen Kategorie über CLI
- in FortiOS 5.4 keine Möglichkeit in WebGUI

```
config webfilter ftgd-local-cat
 edit local_category_1
  set id 140
 end
```

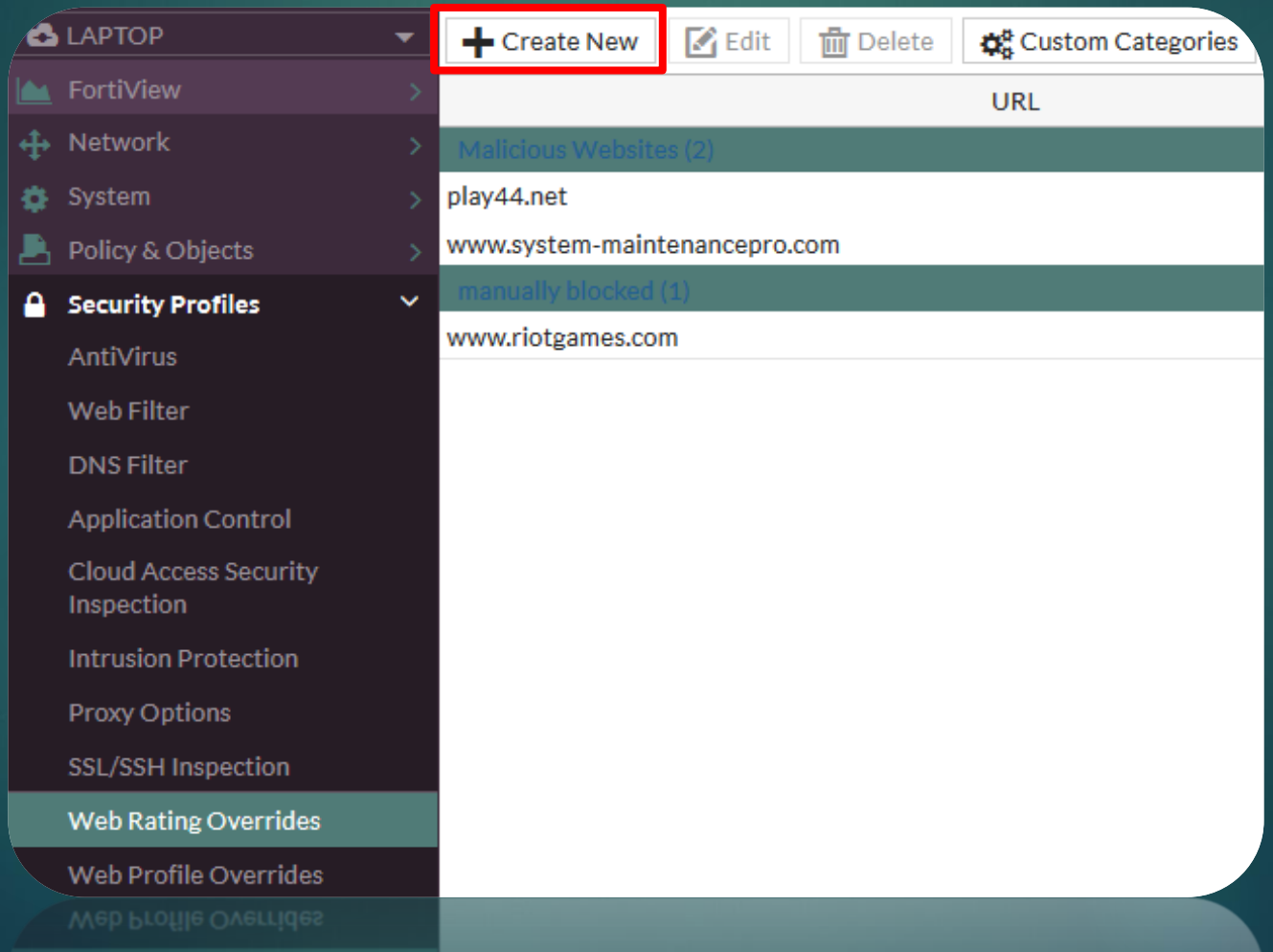
PERMANENTE OVERRIDES

- Der neuen Kategorie (*custom1*) ALLOW zuweisen



PERMANENTE OVERRIDES

- Web Rating Override – Create New



PERMANENTE OVERRIDES

- URL der Sub-Category **custom1** zuweisen