

FORTINET

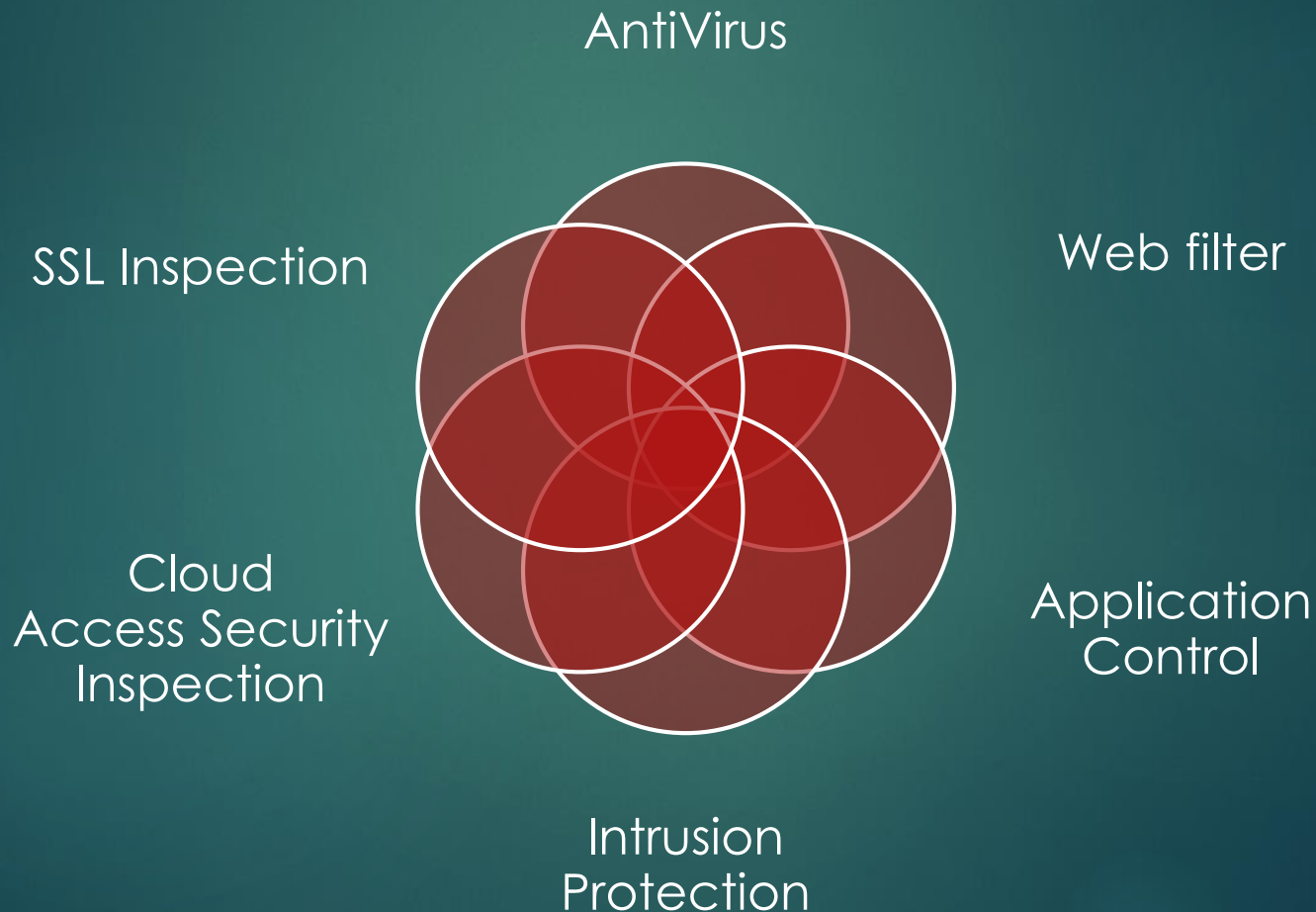
FortiGate



SECURITY PROFILES CONFIGURATION

Security Profiles

Ausgewählte Features

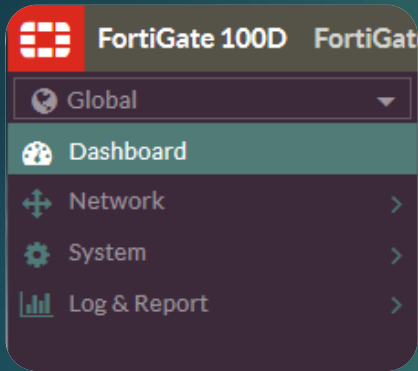


FortiGuard Subscription

- ▶ 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 Subscription

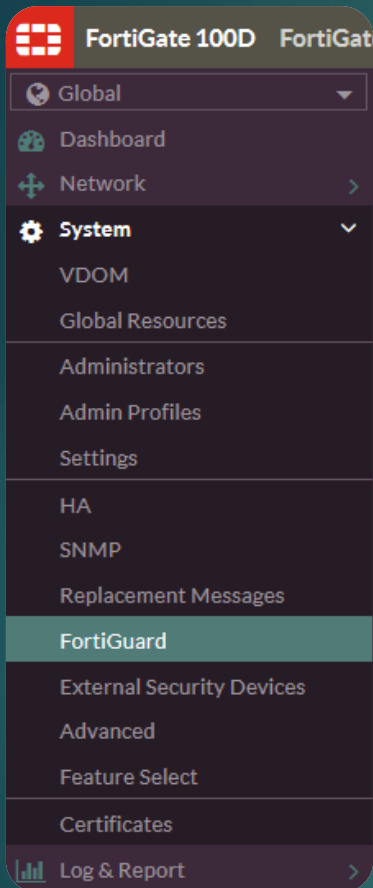
▶ Global Dashboard – Widget License Information



License Information

Support Contract	Registration	✓ Registered (jan.schoedl@bg-bab.ac.at)	Launch Portal
FortiGuard	IPS & Application Control	✓ Licensed (Expires 2018-11-10)	
	AntiVirus	✓ Licensed (Expires 2018-11-10)	
	Web Filtering	✓ Licensed (Expires 2018-11-10)	
	Anti-Spam Filtering	✓ Licensed (Expires 2018-11-10)	
FortiCloud	Account		Activate
FortiSandbox	FortiSandbox Appliance	✗ Not Configured	Configure
FortiClient	Status	✓ Free License	How to Purchase
	Clients Registered	0 of 10	Enter License
	FortiClient Installers		Details
FortiToken Mobile	Tokens Assigned	0 of 2	Mac Windows
Virtual Domain	VDOMs Used	2 of 10	

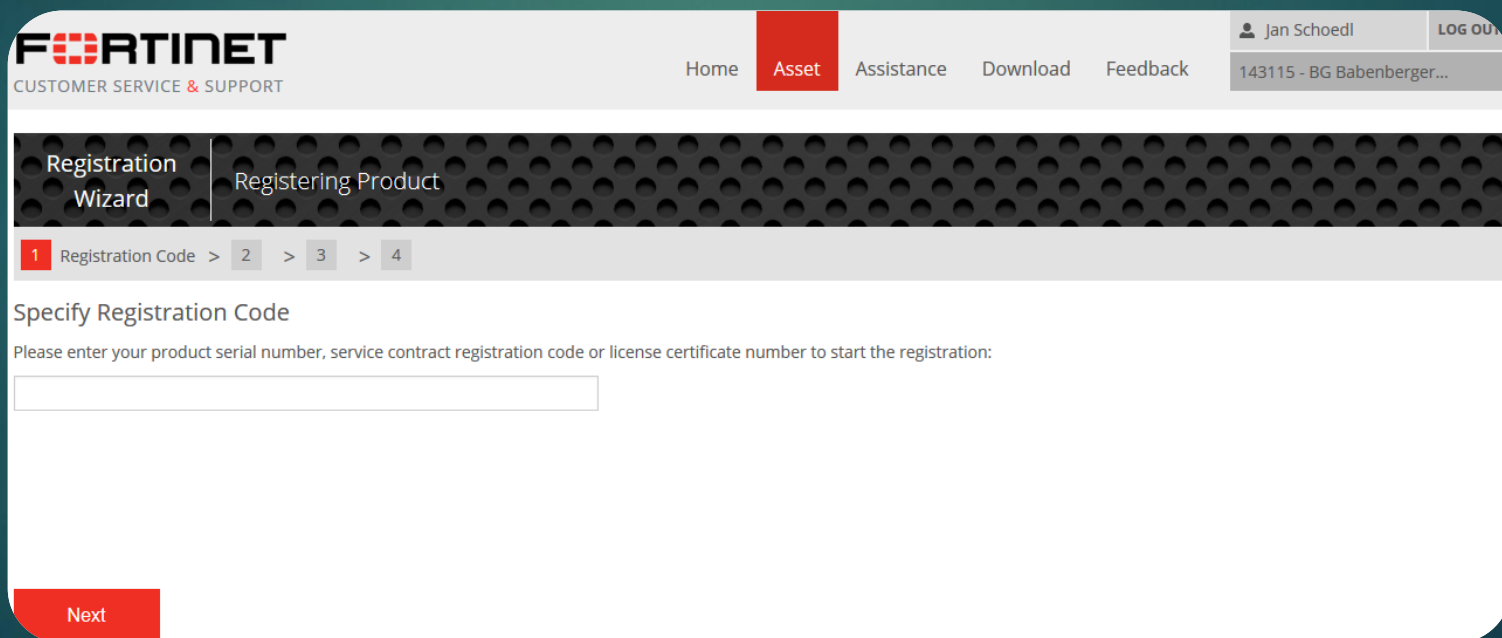
FortiGuard Subscription



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



The screenshot shows the Fortinet Customer Service & Support website. The top navigation bar includes the Fortinet logo, the text 'CUSTOMER SERVICE & SUPPORT', and links for Home, Asset, Assistance, Download, and Feedback. A user profile for 'Jan Schoedl' is visible in the top right corner, along with a 'LOG OUT' link and a location indicator '143115 - BG Babenberger...'. Below the navigation bar, the 'Registration Wizard' is active, with the current step being 'Registering Product'. A progress bar shows four steps: 1. Registration Code (active), 2, 3, and 4. The main content area is titled 'Specify Registration Code' and contains the instruction: 'Please enter your product serial number, service contract registration code or license certificate number to start the registration:'. Below this instruction is a text input field. At the bottom left of the form, there is a red 'Next' button.

Registrierung der Services

View
Products

Total Records : 3
Filter: Off

Basic View

Setting

Export

Advanced Search

Please enter product SN or description...



Serial Number ▲	Description ◆	Ship Date ◆	Registration Date ◆
FG100D3G12808009	FortiGate100D Schule	2012-10-29	2012-11-09
FGT50B3G10641946	FortiGate 50B Direktion	2011-03-18	2011-04-23
FGT50B3G11608295	FortiGate 50B IBVS	2011-08-11	2011-09-07

Registrierung der Services

Product Details FortiGate 100D
FG100D3G12808009

Firmware & General Updates Will Expire On **2018-11-08**

[Back To List](#)

Information

- General
- Location
- Entitlement
- License & Key

Registration

- Renew Contract
- + Add Licenses
- RMA Transfer
- FortiGuard Trial

Assistance

- Ticket List
- Technical Request
- Customer Service
- DOA/RMA Request
- Anti Virus Ticket
- WebChat

Product Information

General

Product Model: FortiGate 100D
Serial Number: FG100D3G12808009
Registration Date: 2012-11-09
Ship Date: 2012-10-29
Warranty: Standard ?
Warranty Support Start Date: 2012-11-09
Warranty Support Start Event: Initial Registration of SN at support.fortinet.com ?
Description: FortiGate100D Schule
Partner: CCS Rosenstein

Version & Update

OS Version: FG100D-FW-5.04-101
AV Engine Version: 5.227
AV Engine Update Time: 2016-03-15 07:05
AV DB Version: 33.284
AV DB Update Time: 2016-03-15 07:05
IPS Version: 7.811
IPS Update Time: 2016-03-15 07:05
IPS Engine Version: 3.164
IPS Engine Update Time: 2016-03-15 07:05

Registrierung der Services

Product Details FortiGate 100D
FG100D3G12808009

Firmware & General Updates Will Expire On
2018-11-08

[← Back To List](#)

Information

- General
- Location
- Entitlement**
- License & Key

Registration

- Renew Contract
- Add Licenses
- RMA Transfer
- FortiGuard Trial

Assistance

- Ticket List
- Technical Request
- Customer Service
- DOA/RMA Request
- Anti Virus Ticket
- WebChat

Product Entitlements

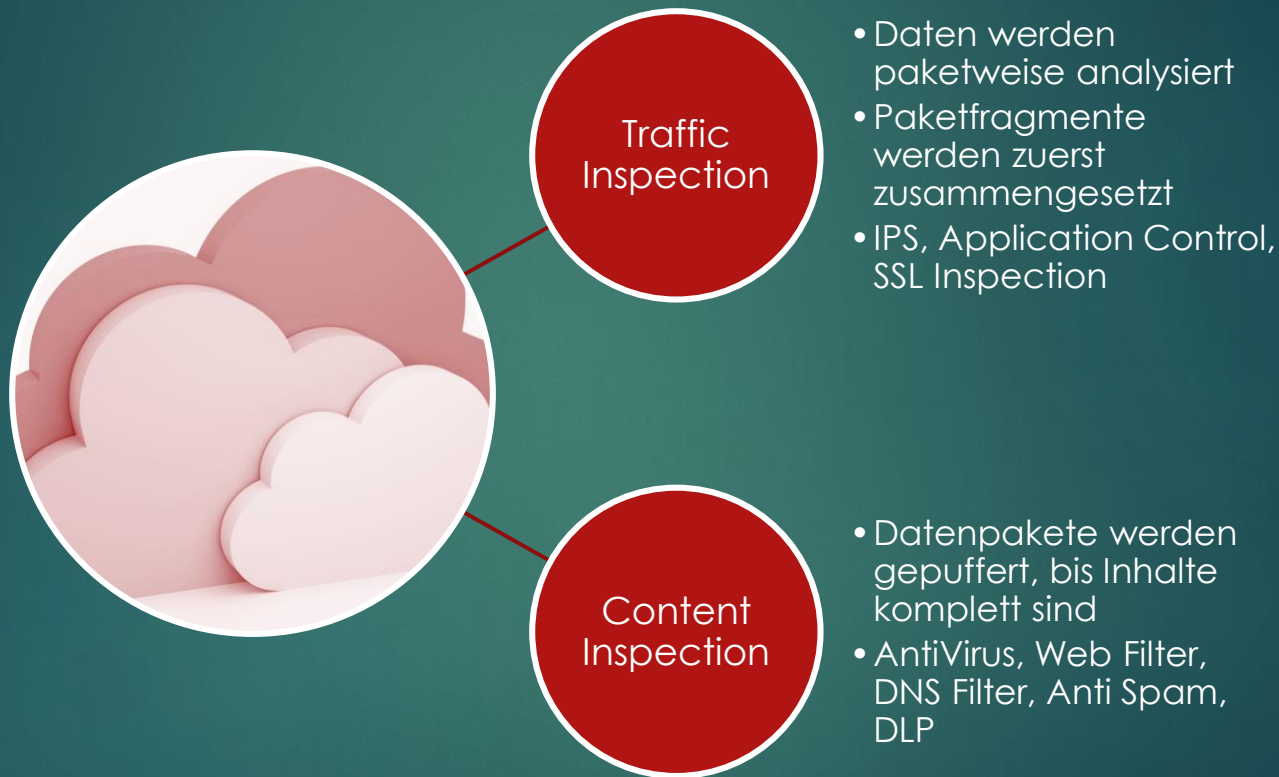
Support Coverage

Support Type	Support Level	Activation Date	Expiration Date
Hardware	Return To Factory	2012-11-09	2018-11-08
Firmware & General Updates	Web/Online	2012-11-09	2018-11-08
Enhanced Support	8x5	2012-11-09	2018-11-08
AntiVirus	Web/Online	2012-11-09	2018-11-08
NGFW	Web/Online	2012-11-09	2018-11-08
Web Filtering	Web/Online	2012-11-09	2018-11-08
AntiSpam	Web/Online	2012-11-09	2018-11-08

Registered Support Contract

	Contract Number	SKU	Creation Date	Registration Date
+	284404268930	FC-10-00116-900-02-36	2015-10-07	2015-10-07
+	935739353058	FC-10-00116-900-02-36	2012-11-06	2012-11-09

Analysemethoden



AntiVirus

Allgemeine Einstellungen

The screenshot displays the 'Edit AntiVirus Profile' configuration page in a FortiGate web interface. On the left is a dark sidebar with a menu where 'Security Profiles' is expanded and 'AntiVirus' is selected. The main content area is titled 'Edit AntiVirus Profile' and contains the following settings:

- Name:** default
- Comments:** scan and delete virus (21/255 characters)
- Inspection Mode:** Proxy and Flow-based (Flow-based is selected)
- Scan Mode:** Quick and Full (Full is selected)
- Detect Viruses:** Block and Monitor (Block is selected)
- Inspection Options:**
 - Treat Windows Executables in Email Attachments as Viruses:
 - Include Mobile Malware Protection:

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

The screenshot shows the 'Edit AntiVirus Profile' configuration page in FortiGate. The left sidebar is expanded to 'Security Profiles' > 'AntiVirus'. The main configuration area includes:

- Name:** LAPTOP AV
- Comments:** AV Profil Laptopklassen (23/255)
- Detect Viruses:** Block (selected), Monitor
- Inspected Protocols:**
 - HTTP:
 - SMTP:
 - POP3:
 - IMAP:
 - MAPI:
 - FTP:
 - NNTP:
- Inspection Options:**
 - Treat Windows Executables in Email Attachments as Viruses:
 - Include Mobile Malware Protection:

The screenshot shows the top navigation bar of the FortiGate interface. It includes a search icon, a help icon, a refresh icon, and the user name 'admin'. Below this is a dropdown menu showing 'LAPTOP AV' with a plus sign icon to its right, a square icon, and a hamburger menu icon.

Neues Profil erstellen

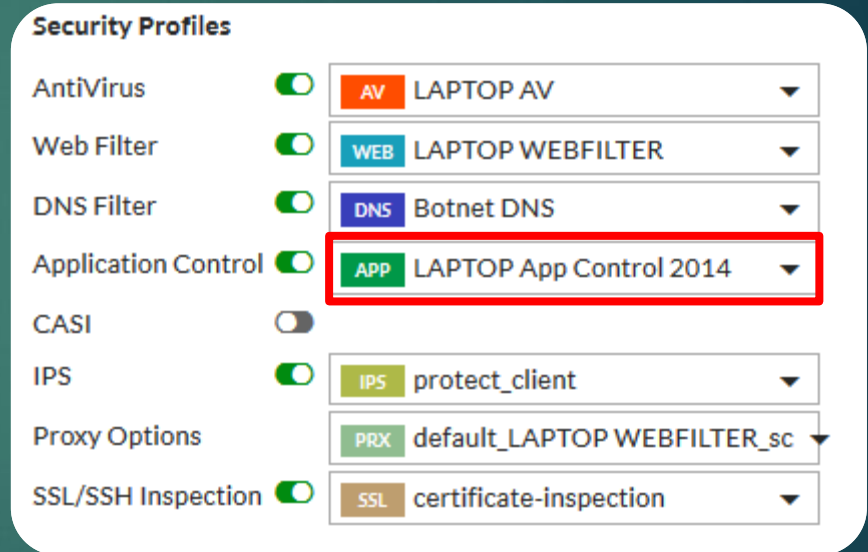
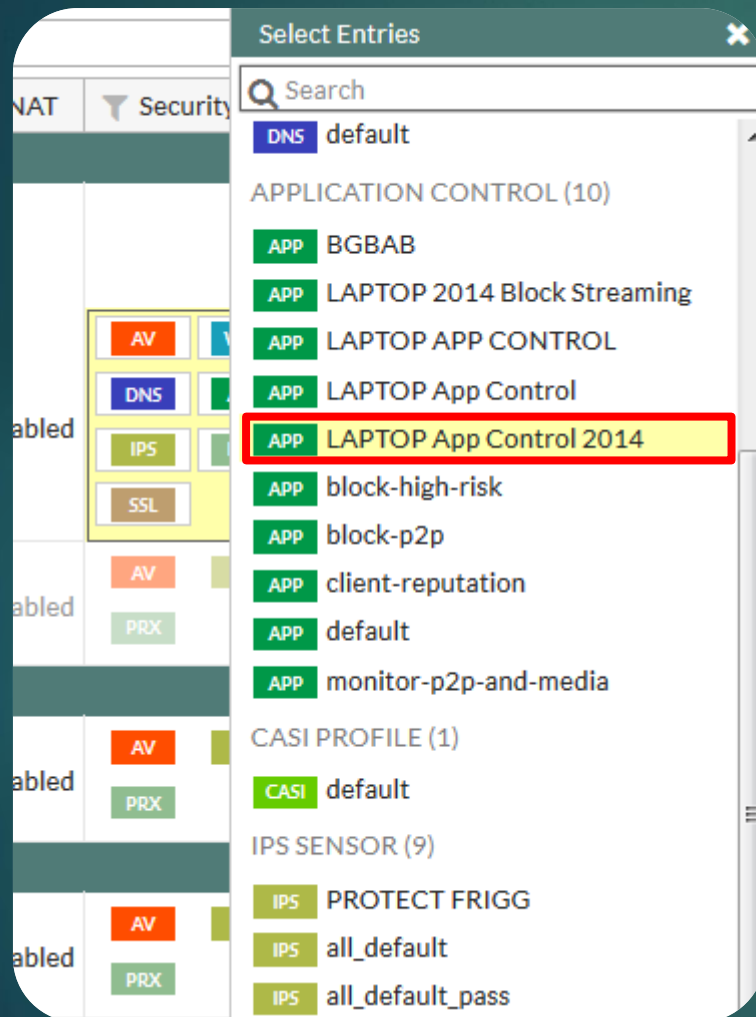
Profil klonen

AntiVirus Profil zuweisen

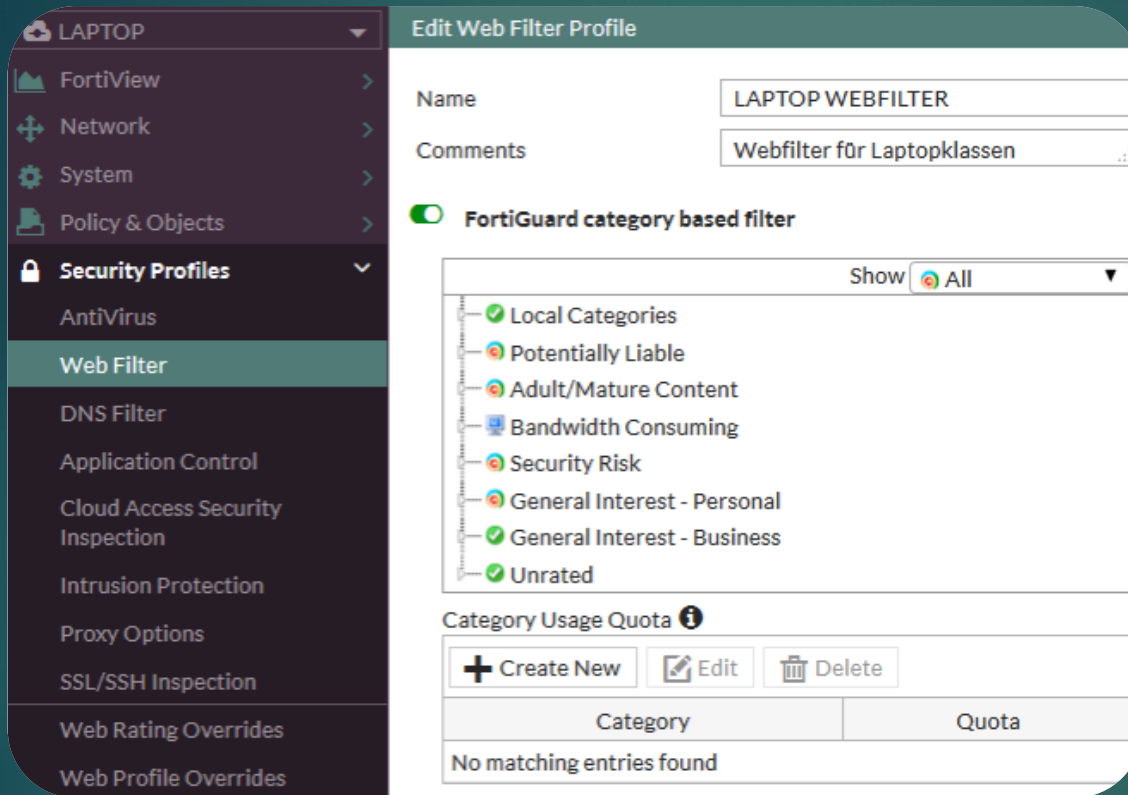
The screenshot displays the FortiGate policy configuration interface. A red arrow points to the 'Select Entries' menu, which is open over the first policy entry (ID 2). The menu options include: Insert, Copy, Paste, Clone Reverse, Rename policy, Show Matching Logs, Show in FortiView, Edit, Edit in CLI, and Delete. The 'AV' profile is highlighted in the 'Select Entries' menu. In the background, the policy configuration table is visible, showing the 'AV' profile assigned to the first policy entry (ID 2).

ID	Name	Source	Destination	Action	Status	Profiles
2	all	all	ALL	Accept	Enabled	AV, WEB, DNS, APP, IPS, PRX, SSL
3	LAPTOP	LAPTOP	ALL	Accept	Enabled	AV, IPS, PRX
4	SSL VPN	SSL VPN	ALL	Accept	Enabled	AV, IPS, PRX
5	SSL VPN Users	SSL VPN Users	ALL	Accept	Enabled	AV, IPS, PRX
6	Implicit Deny	all	ALL	Deny	Disabled	

AntiVirus Profil zuweisen

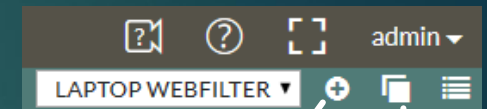


Webfilter



The screenshot shows the 'Edit Web Filter Profile' configuration page in FortiGate. The left sidebar lists various security features, with 'Web Filter' selected. The main configuration area includes:

- Name:** LAPTOP WEBFILTER
- Comments:** Webfilter für Laptopklassen
- FortiGuard category based filter:** Enabled (toggle switch)
- Category List:** A list of categories with checkboxes, including Local Categories, Potentially Liable, Adult/Mature Content, Bandwidth Consuming, Security Risk, General Interest - Personal, General Interest - Business, and Unrated.
- Category Usage Quota:** A section with 'Create New', 'Edit', and 'Delete' buttons, and a table with columns 'Category' and 'Quota'. The table currently shows 'No matching entries found'.



This screenshot shows the profile management toolbar at the top of the configuration page. It includes a search icon, a help icon, a refresh icon, and a dropdown menu showing 'LAPTOP WEBFILTER'. To the right of the dropdown are three icons: a plus sign (+) for creating a new profile, a document icon for cloning a profile, and a list icon for managing profiles.

Neues
Profil
erstellen

Profil
klonen

Webfilter - Reihenfolge

Static URL Filter

www.example.com

example.*

Example.com/news.html

FortiGuard Web Filter

Blockieren nach Fortiguard-Kategorien und Unterkategorien

Web Content Filter

Blockieren/Zulassen von Webseiten nach Schlüsselwörtern oder Mustern (RegExp, Wildcards)

Web Script Filter

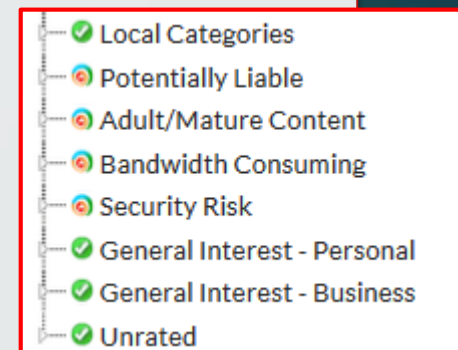
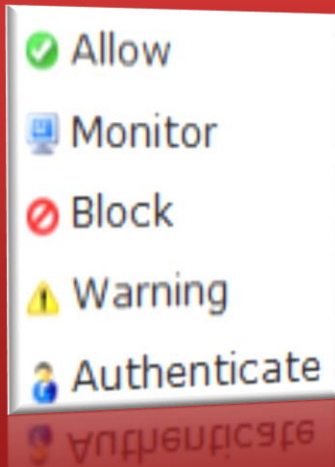
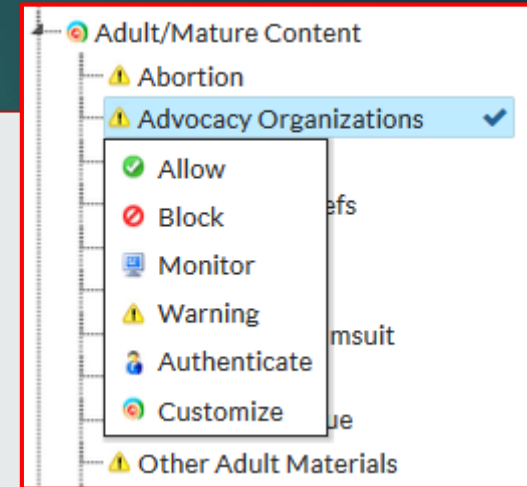
Entfernen von Java Applets, ActiveX, Cookies

Antivirus Scanning.

Funktionsweise Fortiguard Categories

Aktionen
auswählen
für

- Unterkategorien
- Kategorien



Funktionsweise Fortiguard Categories

ALLOW

- Zugriff auf Seiten der Kategorie zulassen

AUTHENTICATE

- Seiten nach Authentifizierung erlaubt

BLOCK

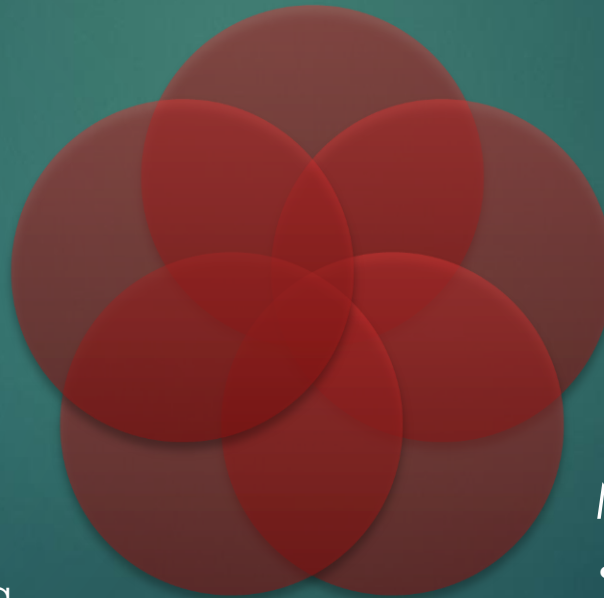
- Zugriff auf Seiten der Kategorie sperren

WARNING

- Warnmeldung vor Zugriff

MONITOR

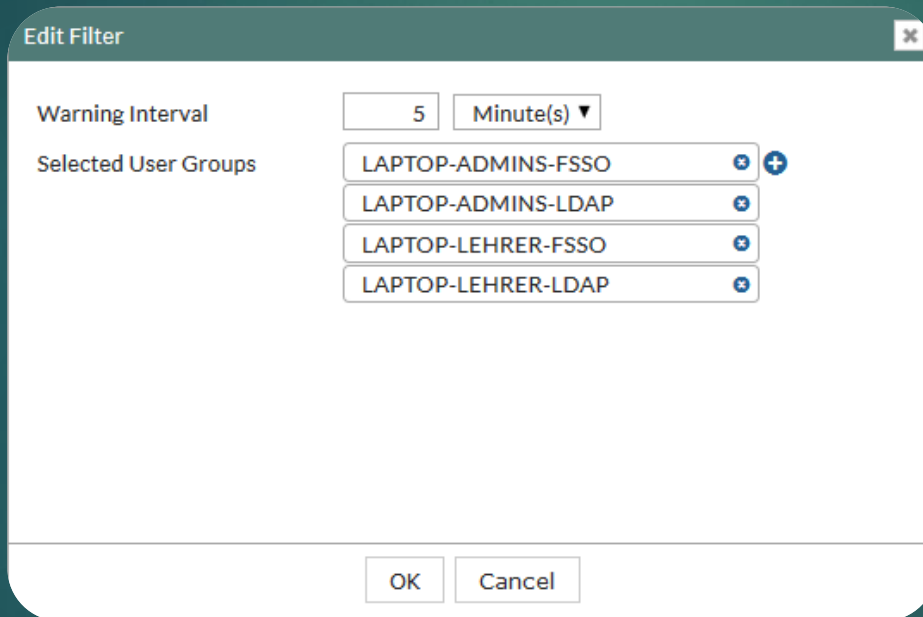
- Zugriff erlauben, jedoch mit Logging



AUTHENTICATE

Authenticate

- ▶ Bekannten Gruppen und Usern kann Zugriff gewährt werden



Edit Filter

Warning Interval: 5 Minute(s) ▼

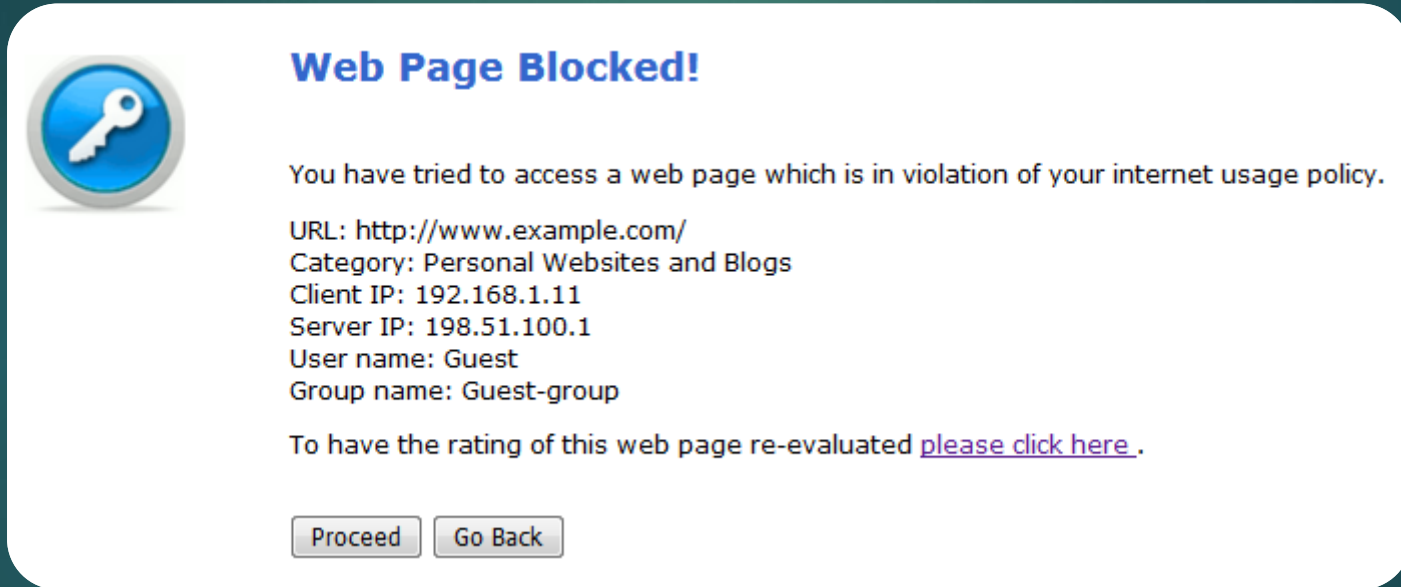
Selected User Groups:

- LAPTOP-ADMINS-FSSO
- LAPTOP-ADMINS-LDAP
- LAPTOP-LEHRER-FSSO
- LAPTOP-LEHRER-LDAP

OK Cancel

AUTHENTICATE & WARNING

- ▶ *Authenticate / Warning* aus Sicht den Benutzers



Web Page Blocked!

You have tried to access a web page which is in violation of your internet usage policy.


URL: <http://www.example.com/>
Category: Personal Websites and Blogs
Client IP: 192.168.1.11
Server IP: 198.51.100.1
User name: Guest
Group name: Guest-group

To have the rating of this web page re-evaluated [please click here](#).

- ▶ *Warning* verlangt kein Passwort nach *Proceed*

BLOCKED

- ▶ Block erlaubt standardmäßig keinen Override



Web Page Blocked!

You have tried to access a web page which is in violation of your internet usage policy.

URL: <http://www.example.com/>
Category: Personal Websites and Blogs
Client IP: 192.168.1.11
Server IP: 198.51.100.1
User name: Guest
Group name: Guest-group

override

To have the rating of this web page re-evaluated [please click here](#).

- ▶ Folgende Einstellung im Webfilter erlaubt es dennoch

Allow users to override blocked categories

Groups that can override

Profile can switch to

Switch applies to User User Group IP Ask

Switch Duration Predefined Ask

Day(s) Hour(s) Minute(s)

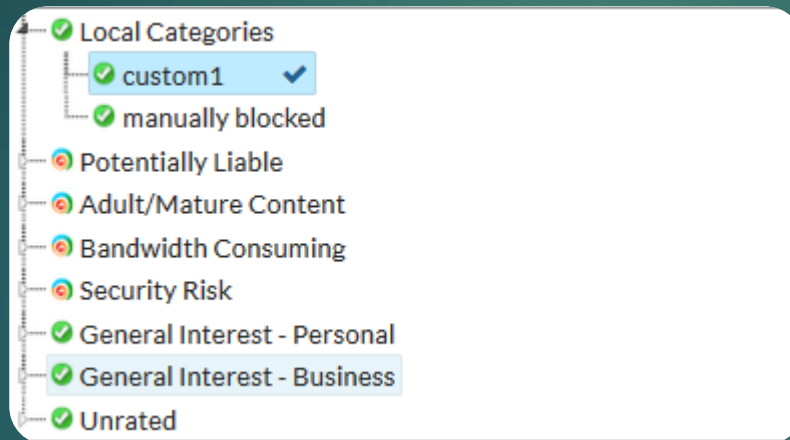
PERMANENTE OVERRIDES

- ▶ 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

The screenshot shows the FortiGate configuration interface for Web Rating Overrides. The left sidebar is expanded to 'Security Profiles' > 'Web Rating Overrides'. The main content area has a toolbar with a red box around the '+ Create New' button, along with 'Edit', 'Delete', and 'Custom Categories' buttons. Below the toolbar is a table with the following data:

URL	Action
Malicious Websites (2)	
play44.net	
www.system-maintenancepro.com	
manually blocked (1)	
www.riotgames.com	

PERMANENTE OVERRIDES

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

New Web Rating Overrides

URL

FortiGuard RatingCategory: General Interest - PersonalSub-Category: Games

Override to

Category

Sub-Category