Anti Virus Konfiguration

Projekttitel: Little Big Topo
Auftraggeber: SDO, KUS
Auftragnehmer: Morris Tichy, Lukas Freudensprung
Schuljahr: 2024/25 **Klasse:** 5CN

VERSION	DATUM	AUTOR/IN	ÄNDERUNG
v1.0	17.02.2025	Morris Tichy	Erstellung des Dokuments

1 Konfiguration FortiGate AV

1.1 Konfiguration des AV Profiles

Der AV Profile wird so konfiguriert, dass alle Dateien blockiert werden, die als Virus erkannt werden. Der folgende Code zeigt die Konfiguration des AV Profiles.

codeblock

```
config antivirus profile
    edit "„AV_SVAL“"
        set feature-set proxy
        config http
            set av-scan block
            set outbreak-prevention block
        end
        config ftp
            set av-scan block
            set outbreak-prevention block
        end
        config imap
            set av-scan block
            set outbreak-prevention block
            set executables virus
        end
        config pop3
```

```
18              set av-scan block
19              set outbreak-prevention block
20              set executables virus
21          end
22          config smtp
23              set av-scan block
24              set outbreak-prevention block
25              set executables virus
26          end
27          config cifs
28              set av-scan block
29              set outbreak-prevention block
30          end
31      next
32  end
```

1.2 Custom-Deep-Inspection

Anschließend muss die custom deep inspection konfiguriert werden. Dafür muss auf den Ziel Clients das FortiGate Zertifikat installiert werden. Im Firefox-Browser wird das wie folgt gemacht:

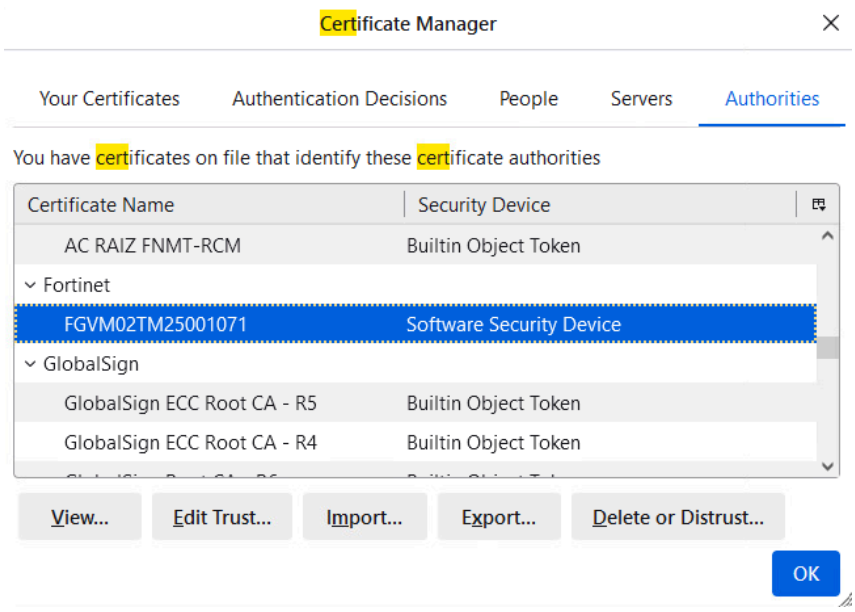

Abbildung 1: FireFox Zertifikat installieren

1.2.1 AV Testen

Damit der AV nun getestet werden kann, wird eine Datei von der Website www.eicar.org installiert. Diese Datei ist ein Testvirus und wird von den meisten AV-Programmen erkannt. Wenn der AV funktioniert, wird die Datei blockiert und der Benutzer sieht folgenden Output.

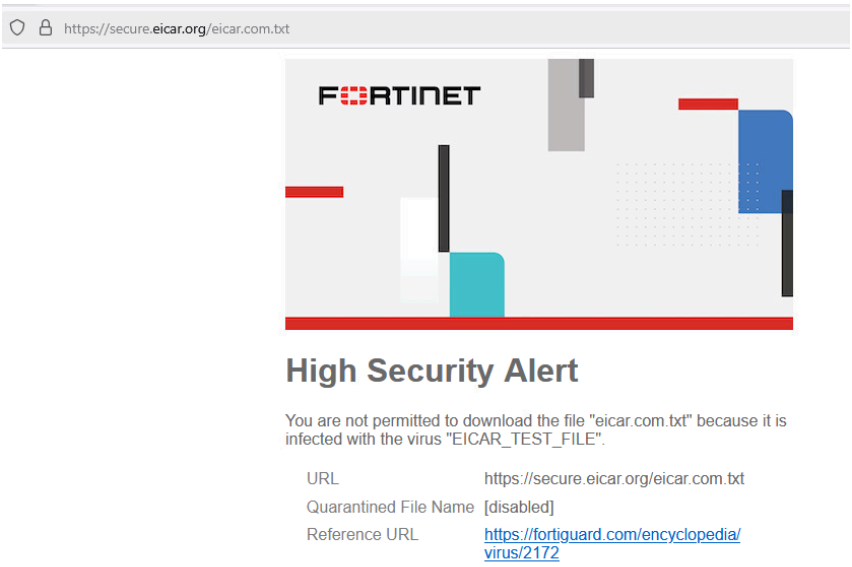

Abbildung 2: AV blockiert File