Checkpoint Einrichtung SSL Interception

Version 1.0

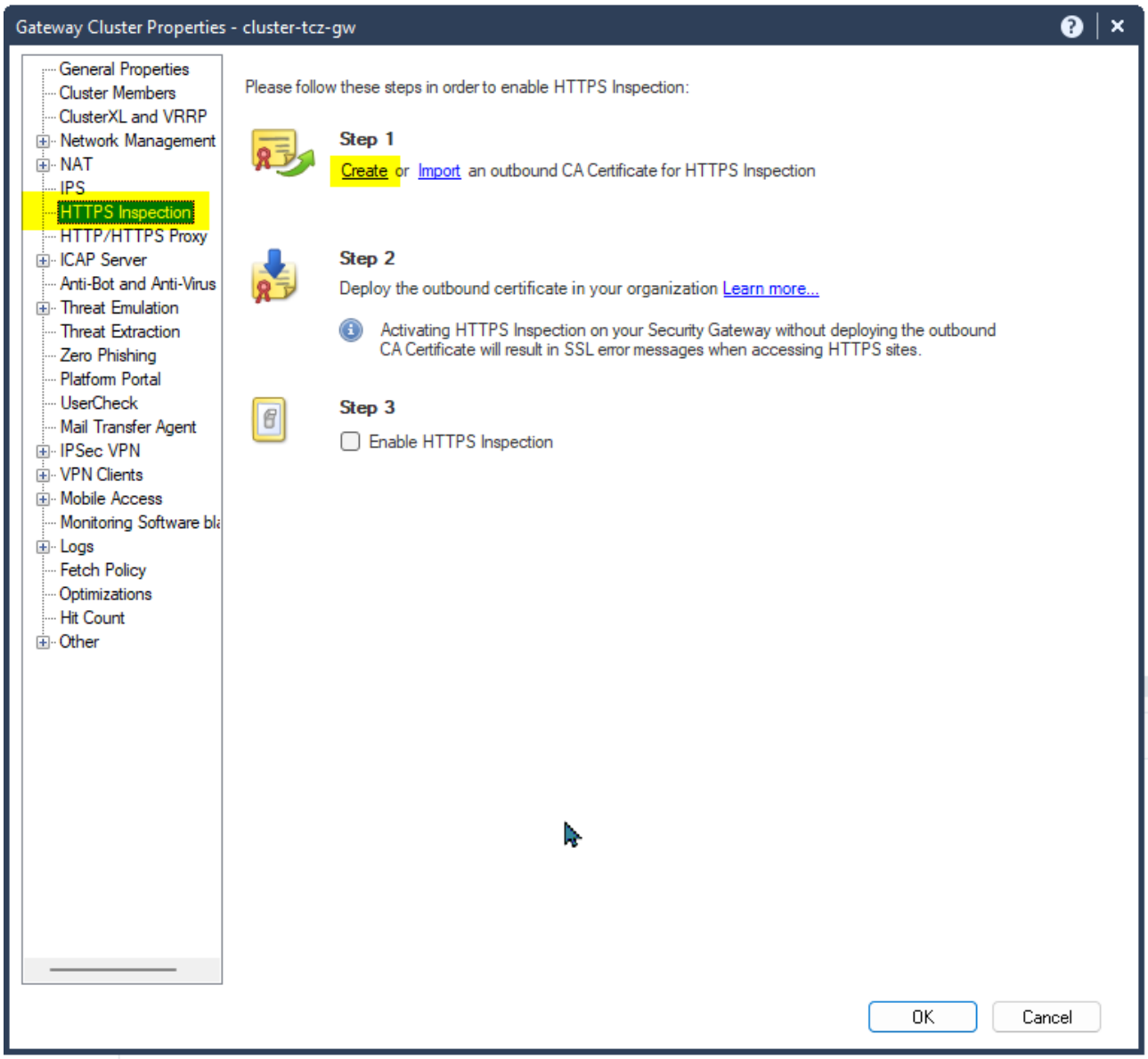
Dokument Name: Checkpoint_Einrichtung SSL Interception

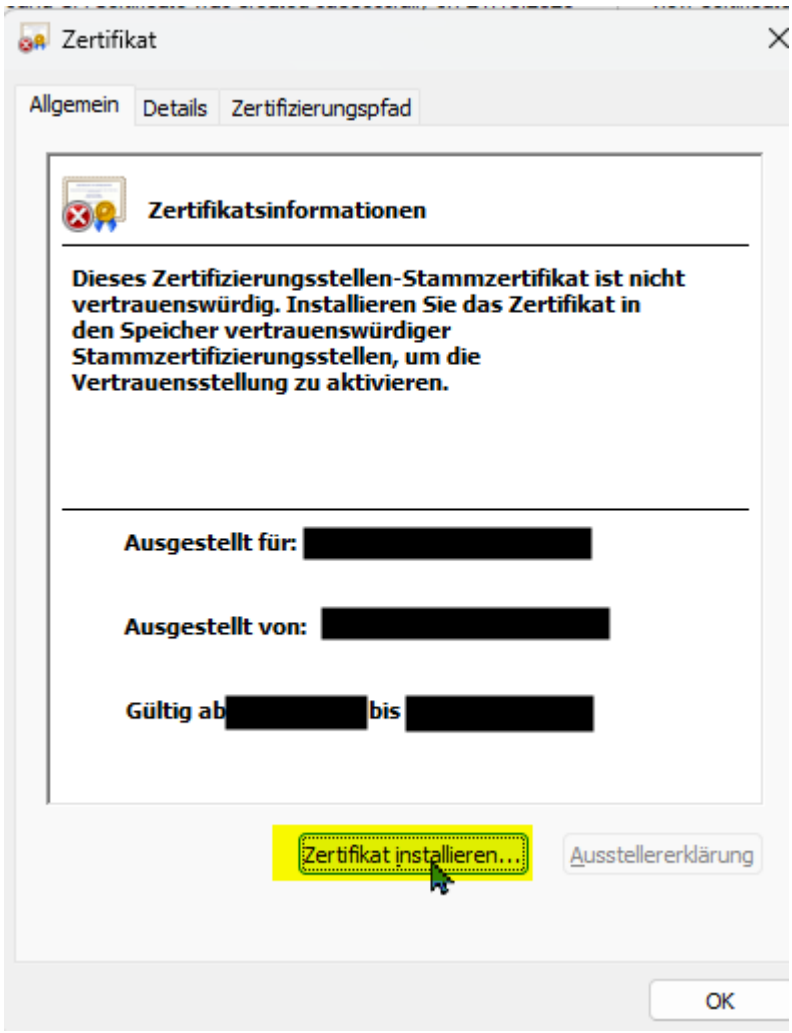
Dokumentenkontrolle

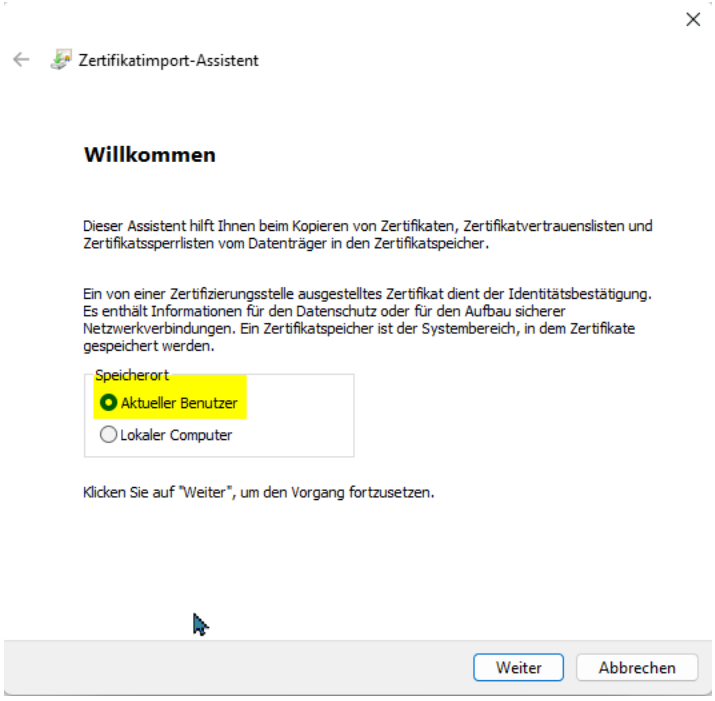
Version	Datum	Änderungsnotiz	Betroffene Seiten	Status	Author
1.0	10.07.2024				

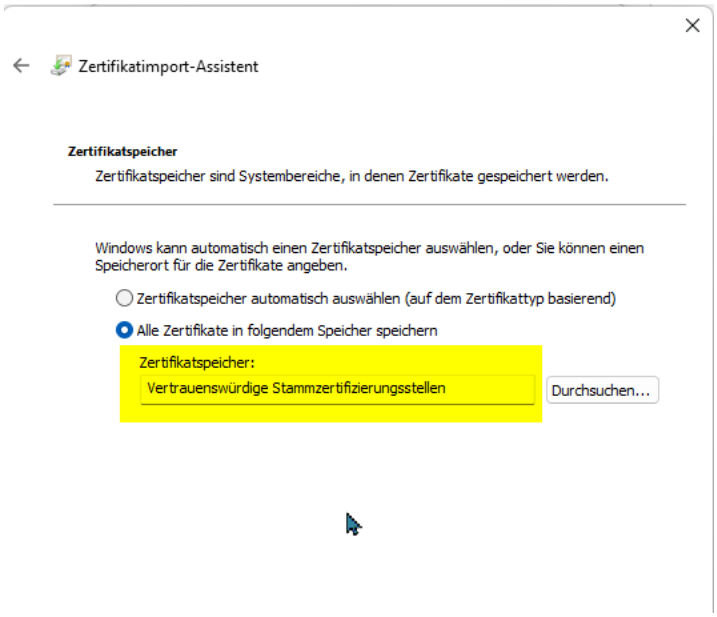
NetWyl Informatik GmbH
Täschmattstrasse 19
6015 Luzern
info@netwyl-informatik.ch
Phone: +41 41 520 73 90

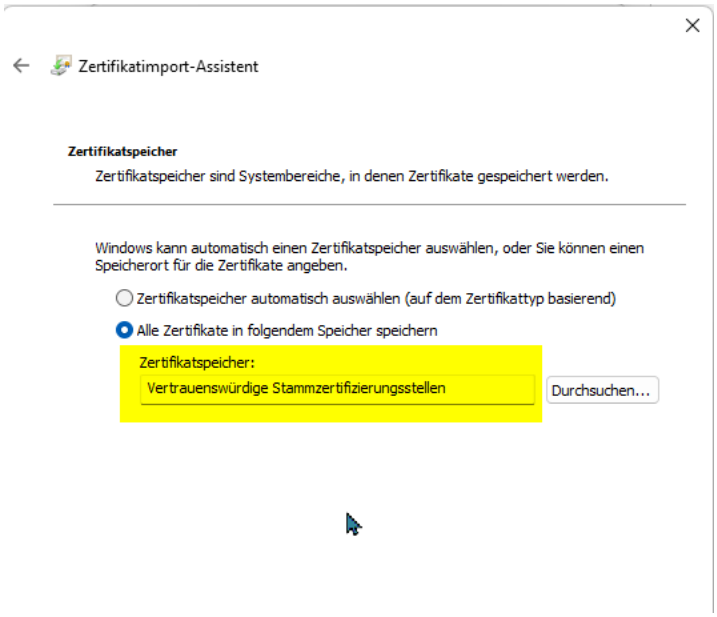
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_SecurityManagement_AdminGuide/Topics-SECMG/HTTPS-Inspection.htm

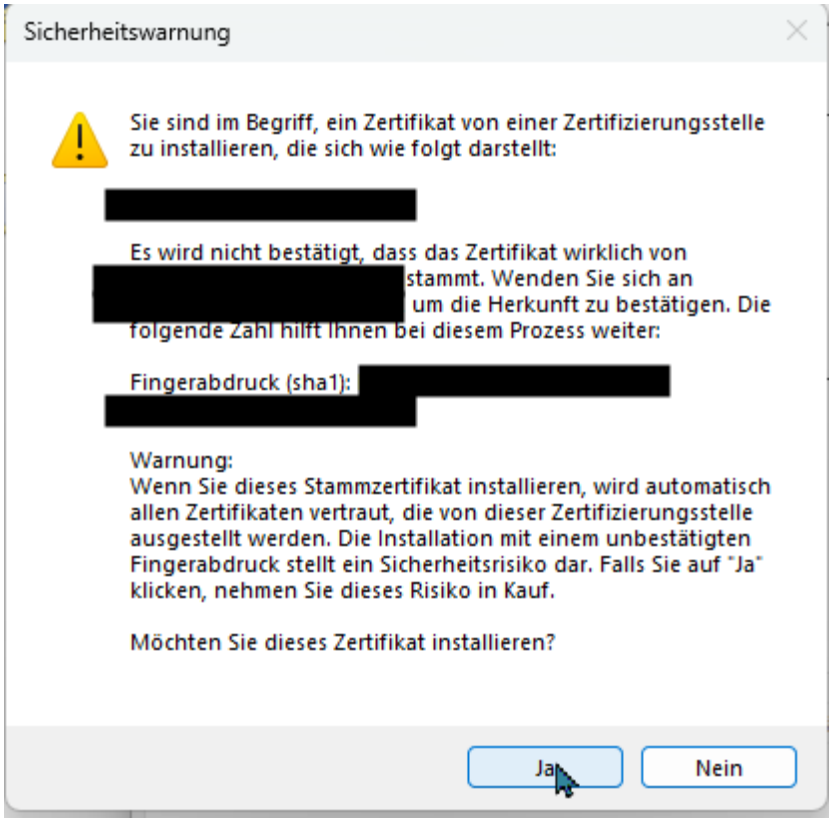

Gateway Cluster Properties - cluster-tcz-gw
General Properties
Cluster Members
ClusterXL and VRRP
Network Management
NAT
IPS
HTTPS Inspection
HTTP/HTTPS Proxy
ICAP Server
Anti-Bot and Anti-Virus
Threat Emulation
Threat Extraction
Zero Phishing
Platform Portal
UserCheck
Mail Transfer Agent
IPSec VPN
VPN Clients
Mobile Access
Monitoring Software bla
Logs
Fetch Policy
Optimizations
Hit Count
Other
Please follow these steps in order to enable HTTPS Inspection:
Step 1
Create or Import an outbound CA Certificate for HTTPS Inspection
Step 2
Deploy the outbound certificate in your organization Learn more...
Activating HTTPS Inspection on your Security Gateway without deploying the outbound CA Certificate will result in SSL error messages when accessing HTTPS sites.
Step 3
Enable HTTPS Inspection
OK
Cancel

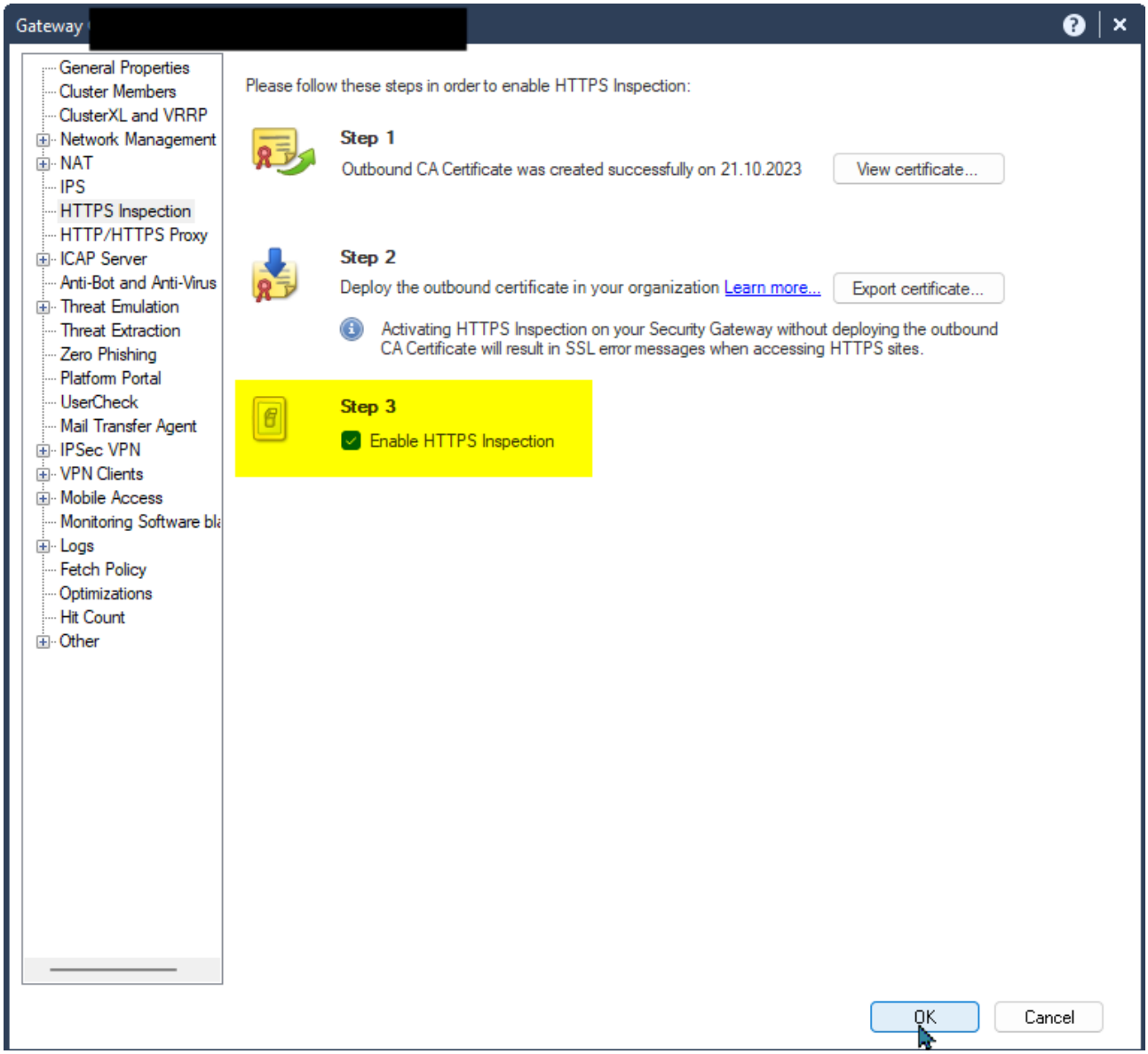

Zertifikat
Allgemein
Details
Zertifizierungspfad
Zertifikatsinformationen
Dieses Zertifizierungsstellen-Stammzertifikat ist nicht vertrauenswürdig. Installieren Sie das Zertifikat in den Speicher vertrauenswürdiger Stammzertifizierungsstellen, um die Vertrauensstellung zu aktivieren.
Ausgestellt für:
Ausgestellt von:
Gültig ab
bis
Zertifikat installieren...
Ausstellererklärung
OK

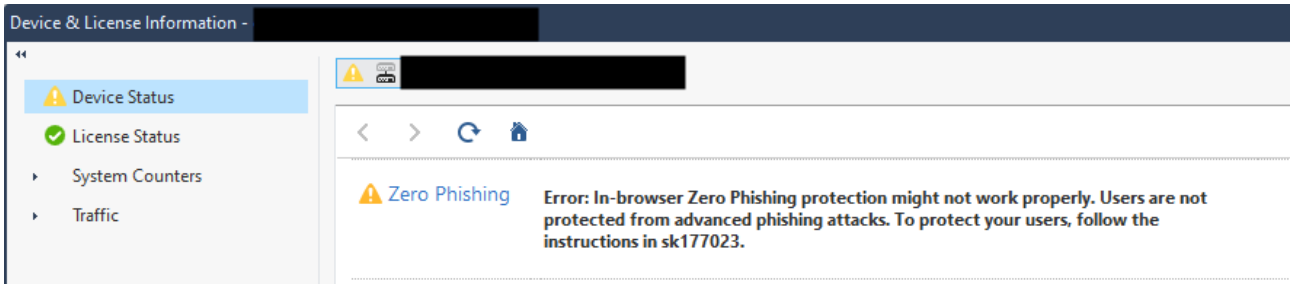

Zertifikatimport-Assistent
Willkommen
Dieser Assistent hilft Ihnen beim Kopieren von Zertifikaten, Zertifikatvertrauenslisten und Zertifikatssperrlisten vom Datenträger in den Zertifikatspeicher.
Ein von einer Zertifizierungsstelle ausgestelltes Zertifikat dient der Identitätsbestätigung. Es enthält Informationen für den Datenschutz oder für den Aufbau sicherer Netzwerkverbindungen. Ein Zertifikatspeicher ist der Systembereich, in dem Zertifikate gespeichert werden.
Speicherort
Aktueller Benutzer
Lokaler Computer
Klicken Sie auf "Weiter", um den Vorgang fortzusetzen.
Weiter
Abbrechen

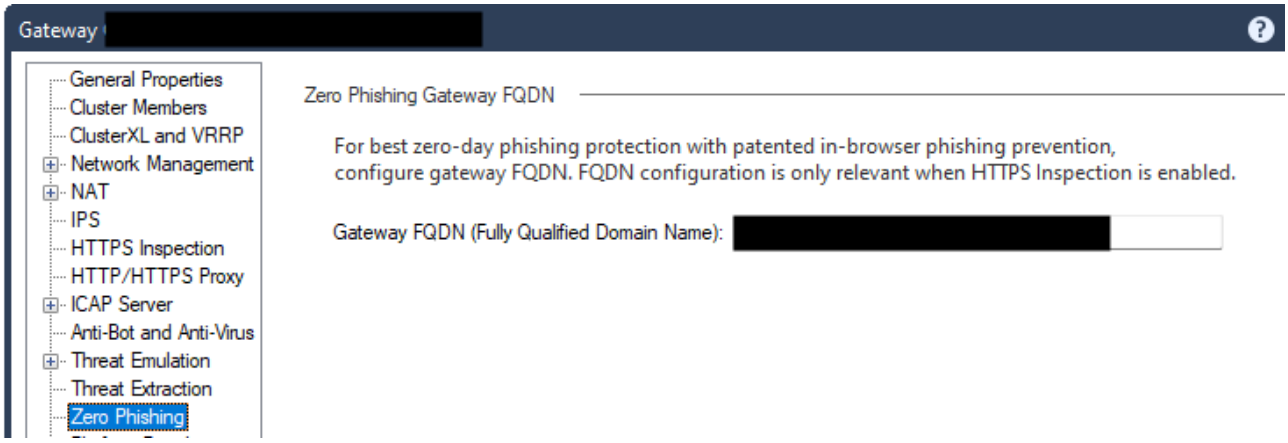

Zertifikatimport-Assistent
Zertifikatspeicher
Zertifikatspeicher sind Systembereiche, in denen Zertifikate gespeichert werden.
Windows kann automatisch einen Zertifikatspeicher auswählen, oder Sie können einen Speicherort für die Zertifikate angeben.
Zertifikatspeicher automatisch auswählen (auf dem Zertifikattyp basierend)
Alle Zertifikate in folgendem Speicher speichern
Zertifikatspeicher:
Vertrauenswürdige Stammzertifizierungsstellen
Durchsuchen...


Zertifikatimport-Assistent
Zertifikatspeicher
Zertifikatspeicher sind Systembereiche, in denen Zertifikate gespeichert werden.
Windows kann automatisch einen Zertifikatspeicher auswählen, oder Sie können einen Speicherort für die Zertifikate angeben.
Zertifikatspeicher automatisch auswählen (auf dem Zertifikattyp basierend)
Alle Zertifikate in folgendem Speicher speichern
Zertifikatspeicher:
Vertrauenswürdige Stammzertifizierungsstellen
Durchsuchen...

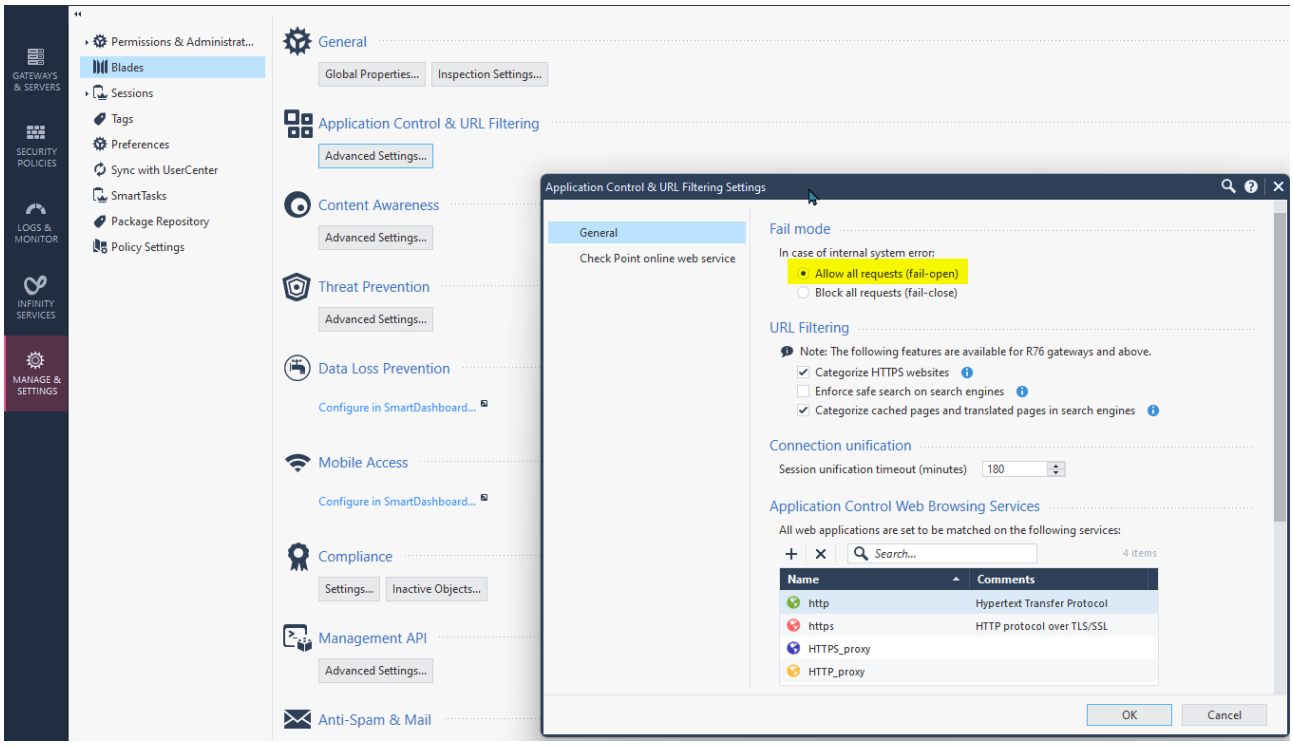

Sicherheitswarnung
Sie sind im Begriff, ein Zertifikat von einer Zertifizierungsstelle zu installieren, die sich wie folgt darstellt:
[redacted]
Es wird nicht bestätigt, dass das Zertifikat wirklich von [redacted] stammt. Wenden Sie sich an [redacted] um die Herkunft zu bestätigen. Die folgende Zahl hilft Ihnen bei diesem Prozess weiter:
Fingerabdruck (sha1): [redacted]
Warnung:
Wenn Sie dieses Stammzertifikat installieren, wird automatisch allen Zertifikaten vertraut, die von dieser Zertifizierungsstelle ausgestellt werden. Die Installation mit einem unbestätigten Fingerabdruck stellt ein Sicherheitsrisiko dar. Falls Sie auf "Ja" klicken, nehmen Sie dieses Risiko in Kauf.
Möchten Sie dieses Zertifikat installieren?
Ja
Nein

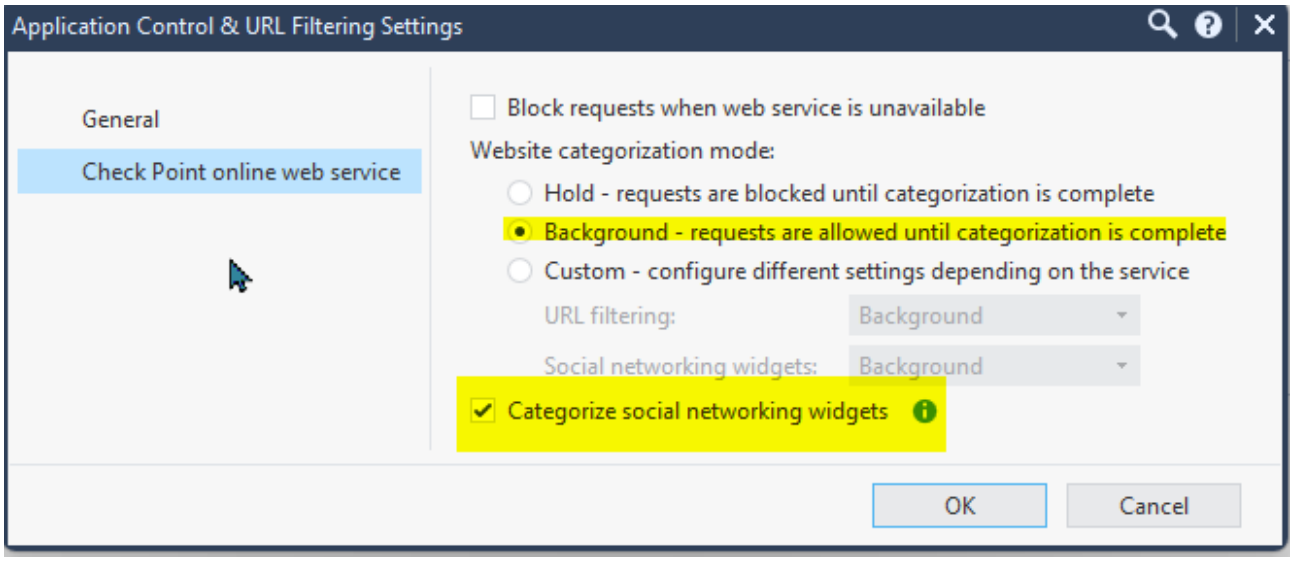

Gateway [redacted]
General Properties
Cluster Members
ClusterXL and VRRP
Network Management
NAT
IPS
HTTPS Inspection
HTTP/HTTPS Proxy
ICAP Server
Anti-Bot and Anti-Virus
Threat Emulation
Threat Extraction
Zero Phishing
Platform Portal
UserCheck
Mail Transfer Agent
IPSec VPN
VPN Clients
Mobile Access
Monitoring Software bla
Logs
Fetch Policy
Optimizations
Hit Count
Other
Please follow these steps in order to enable HTTPS Inspection:
Step 1
Outbound CA Certificate was created successfully on 21.10.2023
View certificate...
Step 2
Deploy the outbound certificate in your organization Learn more...
Export certificate...
Activating HTTPS Inspection on your Security Gateway without deploying the outbound CA Certificate will result in SSL error messages when accessing HTTPS sites.
Step 3
Enable HTTPS Inspection
OK
Cancel

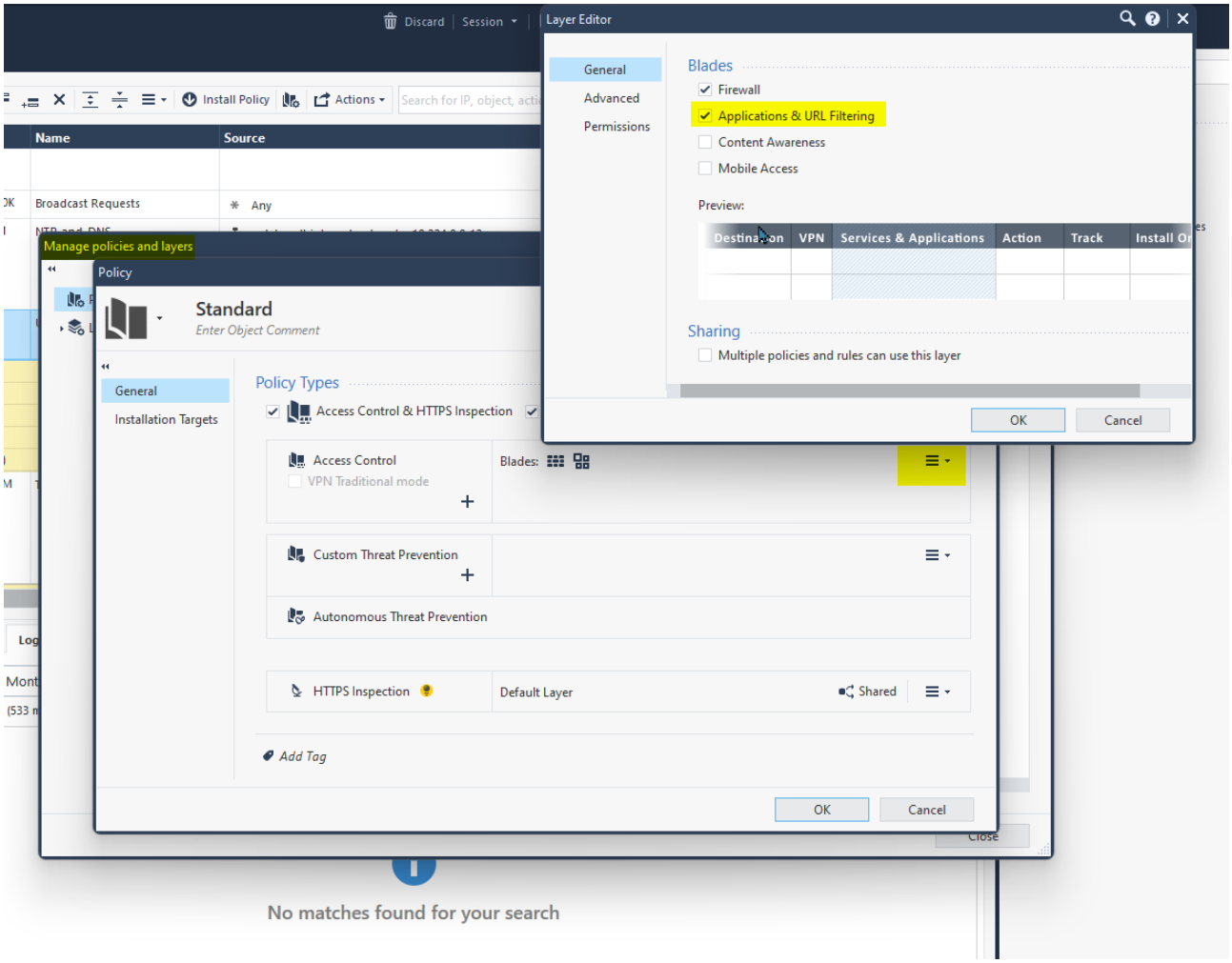

Device & License Information - [redacted]
Device Status
License Status
System Counters
Traffic
[redacted]
Zero Phishing
Error: In-browser Zero Phishing protection might not work properly. Users are not protected from advanced phishing attacks. To protect your users, follow the instructions in sk177023.



Configuring the Application Control and URL Filtering Software Blades for Monitor Mode (checkpoint.com)






Discard
Session
Layer Editor
General
Advanced
Permissions
Blades
Firewall
Applications & URL Filtering
Content Awareness
Mobile Access
Preview:
Destination
VPN
Services & Applications
Action
Track
Sharing
Multiple policies and rules can use this layer
OK
Cancel
Install Policy
Actions
Search for IP, object, acti
Name
Source
Broadcast Requests
Any
Manage policies and layers
Policy
Standard
Enter Object Comment
General
Installation Targets
Policy Types
Access Control & HTTPS Inspection
Access Control
VPN Traditional mode
Blades:
Custom Threat Prevention
Autonomous Threat Prevention
HTTPS Inspection
Default Layer
Shared
Add Tag
OK
Cancel
Close
No matches found for your search