



Installationsanleitung
CGM MANAGED TI
– CGM FIREWALL

Installationsanleitung CGM MANAGED TI mit CGM FIREWALL M oder L

Stand: In Erstellung

Datum: 31.01.2024

Version: 1.8

Autor: Michael Heigl

Dokumentenhistorie			
Version	Autor	Datum	Grund der Änderung
1.0	Michael Heigl	26.01.2023	Erstellung
1.1	Dominik Rosch	30.01.2023	Formatierung und redaktionelle Überarbeitung
1.2	Dominik Rosch	14.02.2023	Finalisierung
1.3	Dominik Rosch	14.03.2023	Redaktionelle Änderungen
1.4	Dominik Rosch	07.06.2023	Anpassung um zertifikatsbasierten Verbindungsaufbau
1.5	Michael Heigl	03.07.2023	Netzwerkkonfiguration CGM Firewall als Gateway für Kartenterminals
1.6	Michael Heigl	14.08.2023	Workaround für WebUI Einschränkung Kapitel 6
1.7	Dominik Rosch	22.09.2023	Anpassungen nach Feedback
1.8	Michael Heigl	29.09.2023	Anpassungen nach Feedback
1.9	Dominik Rosch	29.01.2024	Anpassungen nach Feedback

Inhalt

1	PRÄAMBEL	4
2	VORAUSSETZUNGEN.....	5
2.1	SYSTEMVORAUSSETZUNGEN	5
2.2	DOWNLOAD DER CGM-MANAGED-TI-KONFIGURATIONSDATEIEN	6
3	EINRICHTUNG DER CGM-MANAGED-TI-VERBINDUNG	7
3.1	CA-ZERTIFIKAT HINZUFÜGEN	7
3.2	GERÄTE-ZERTIFIKAT AUF DER CGM FIREWALL HINZUFÜGEN.....	10
3.3	VPN-EINRICHTUNG	14
3.4	ÜBERPRÜFUNG DES VERBINDUNGSaufbaus	18
4	EINRICHTUNG DER ZUGRIFFE AUF DIE TI-BESTANDSNETZE.....	19
4.1	EINRICHTUNG DER BESTANDSNETZE.....	19
4.2	ÜBERPRÜFEN DER EINSTELLUNGEN	24
5	KARTENTERMINAL-KONFIGURATION	26
5.1	IP-KONFIGURATION DER KARTENTERMINALS.....	26
5.2	NETZWERKKONFIGURATION DER CGM FIREWALL.....	26
6	ANPASSUNGEN FÜR DIE EVENTSCHNITTSTELLE VON PRIMÄRSYSTEMEN	28

1 Präambel

Diese Installationsanleitung richtet sich an Dienstleister vor Ort (DVO) für CGM MANAGED TI. Ziel der Anleitung ist die Beschreibung der notwendigen Schritte, um eine CGM FIREWALL mit dem TI-Zugang im CGM-MANAGED-TI-Rechenzentrum zu verbinden.

2 Voraussetzungen

2.1 Systemvoraussetzungen

Die zu konfigurierende CGM-Firewall muss auf dem aktuellen Software-Stand und über die WatchGuard-Cloud konfigurierbar sein. ([WatchGuard Cloud URLs and Network Access Requirements](#))

Zudem müssen in etwaigen zusätzlichen Firewalls die ausgehenden UDP-Ports 500 und 4500 freigeschaltet werden.

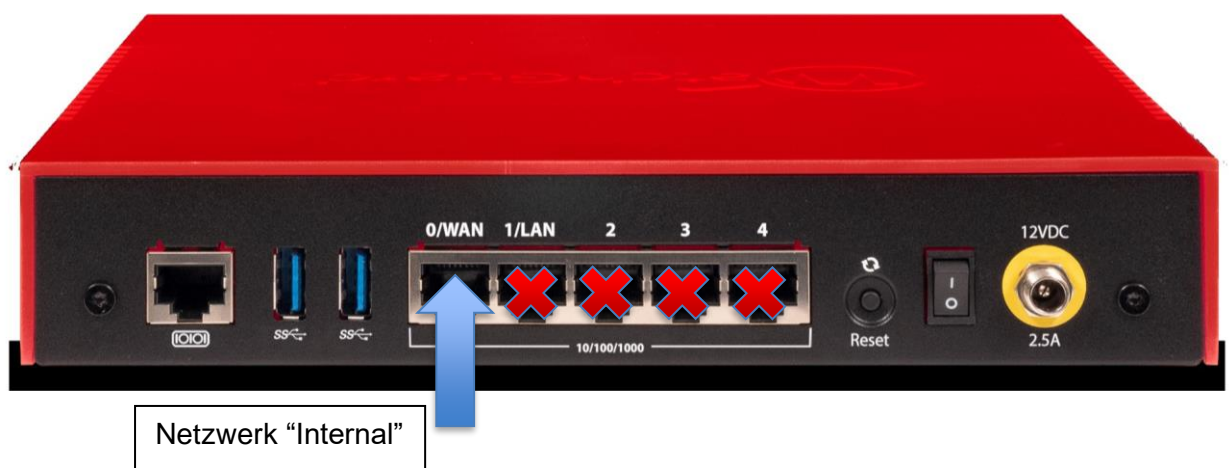
Die Standardkonfiguration ordnet die Schnittstelle 0/WAN dem Netzwerk „External“ und die Schnittstelle 1/LAN, 2, 3, 4 dem Netzwerk „Internal“ zu. Wird diese Zuordnung verändert, muss auch die im folgenden Abschnitt beschriebene Anbindungsart angepasst werden.

Die zu konfigurierende CGM-Firewall muss in einem von zwei Betriebsmodi eingesteckt und verkabelt sein:

- **Paralleler Modus**

Im parallelen Modus fungiert die CGM-Firewall nur als VPN-Router und hat daher keinerlei Firewalling-Funktionen. In diesem Modus muss die Firewall ausschließlich per WAN-Schnittstelle angebunden werden. Die WAN-Dose muss daher mit der Praxis-Infrastruktur verbunden werden.

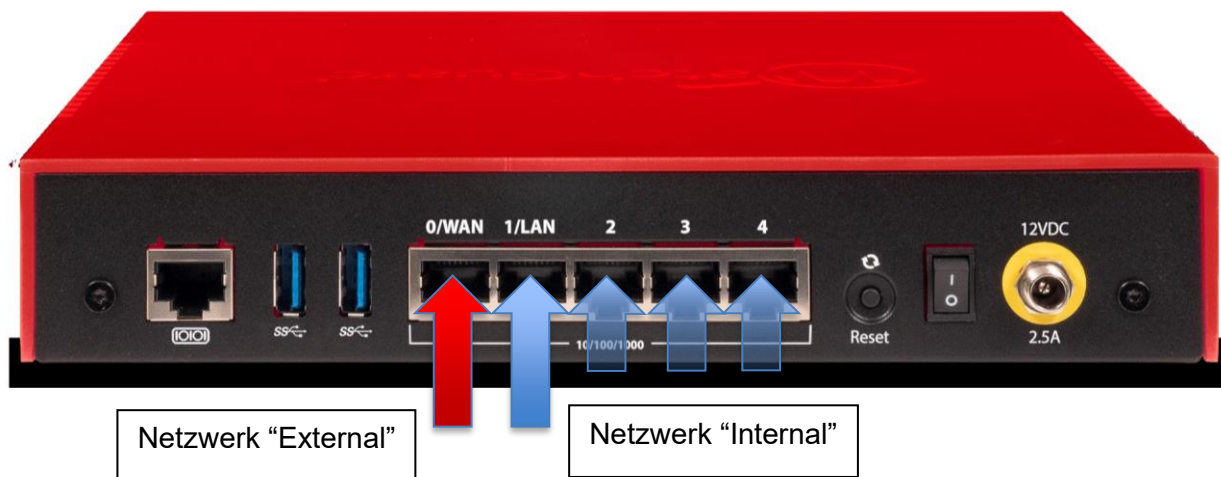
-



Installationsanleitung CGM MANAGED TI mit CGM FIREWALL M oder L

- Serieller Modus

Im seriellen Modus ist die CGM-Firewall als Standard-Gateway eingerichtet. Dafür muss sie mit einer LAN-Schnittstelle an die Praxisinfrastruktur angebunden sein und die WAN-Schnittstelle muss mit dem Praxisrouter bspw. der Fritzbox verbunden werden.



2.2 Download der CGM-MANAGED-TI-Konfigurationsdateien

Im Rahmen der Auftragsverarbeitung ist in TEO ein Download-Link je Installation hinterlegt, in dem sich eine ZIP-Datei findet. Diese umfasst folgende Dateien:

- **Ordner: wg_config.zip**
 - **Ordner: certificates**
Dieser Ordner enthält alle notwendigen Zertifikate, um eine zertifikatsbasierte Anbindung an den VPN-Endpunkt von CGM MANAGED TI abzubilden.
 - **Datei: Login-Daten.txt**
Diese Datei enthält alle notwendigen Informationen zur Anbindung an den VPN-Endpunkt von CGM MANAGED TI sowie alle Informationen zum Routing und SNAT und wird für die folgenden Schritte benötigt.

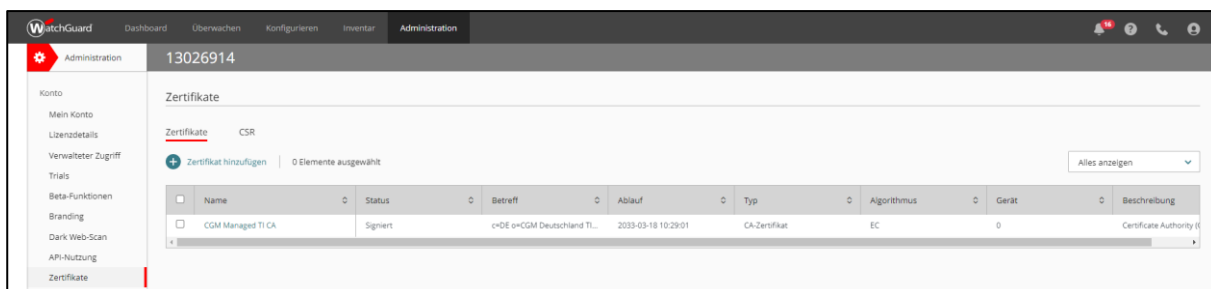
3 Einrichtung der CGM-MANAGED-TI-Verbindung

Die folgenden Schritte finden in der WatchGuard-Cloud statt.

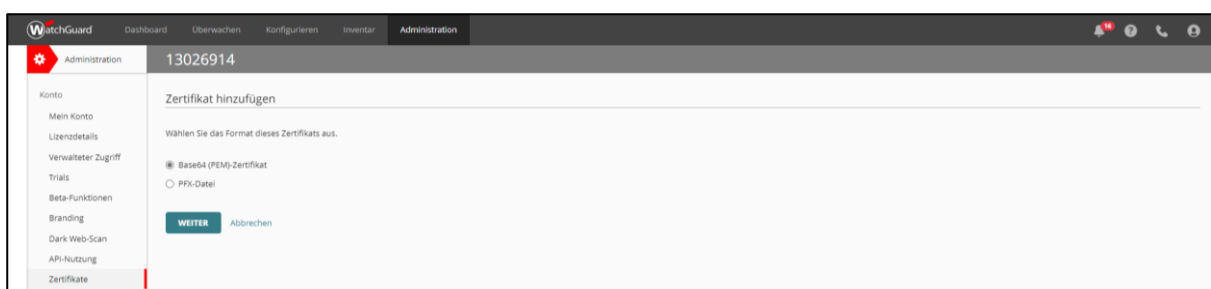
3.1 CA-Zertifikat hinzufügen

Die in 3.1 definierten Schritte müssen je Zugang zur WatchGuard-Cloud nur einmalig ausgeführt werden. Im Hauptmenü muss „Administration“ ausgewählt werden. Es öffnet sich eine neue Ansicht mit einem seitlichen Menü, in dem der Menüpunkt „Zertifikate“ ausgewählt werden muss, damit sich der Zertifikatsmanager öffnet.

Im Register „Zertifikate“ kann über die Schaltfläche „Zertifikat hinzufügen“ das mitgelieferte TlaaS-CA-Cert.txt hinzugefügt werden.

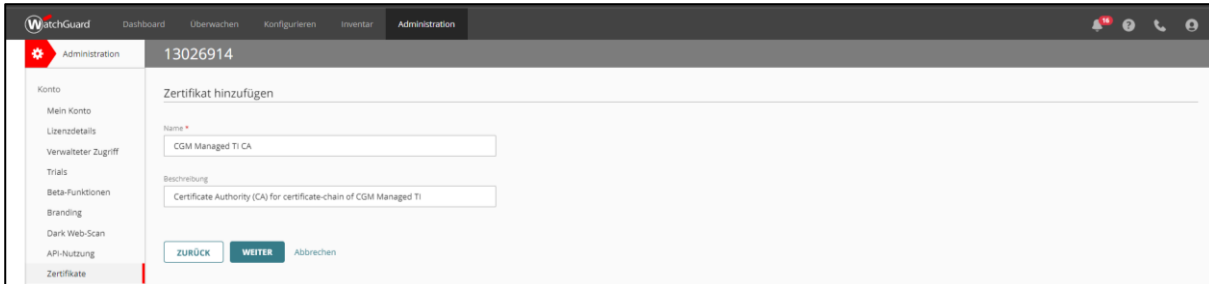


Die Zertifikatsdatei wird mit der Auswahl „Base64 (PEM)-Zertifikat“ hinzugefügt.

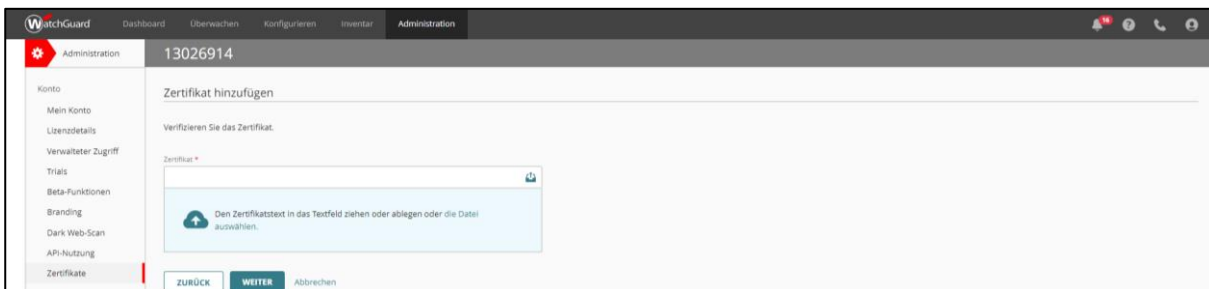


Es sollte ein entsprechender Name gewählt werden, der die Zuordnung im späteren Verlauf erleichtert. Wir empfehlen den Namen „CGM Managed TI CA“

Installationsanleitung CGM MANAGED TI mit CGM FIREWALL M oder L

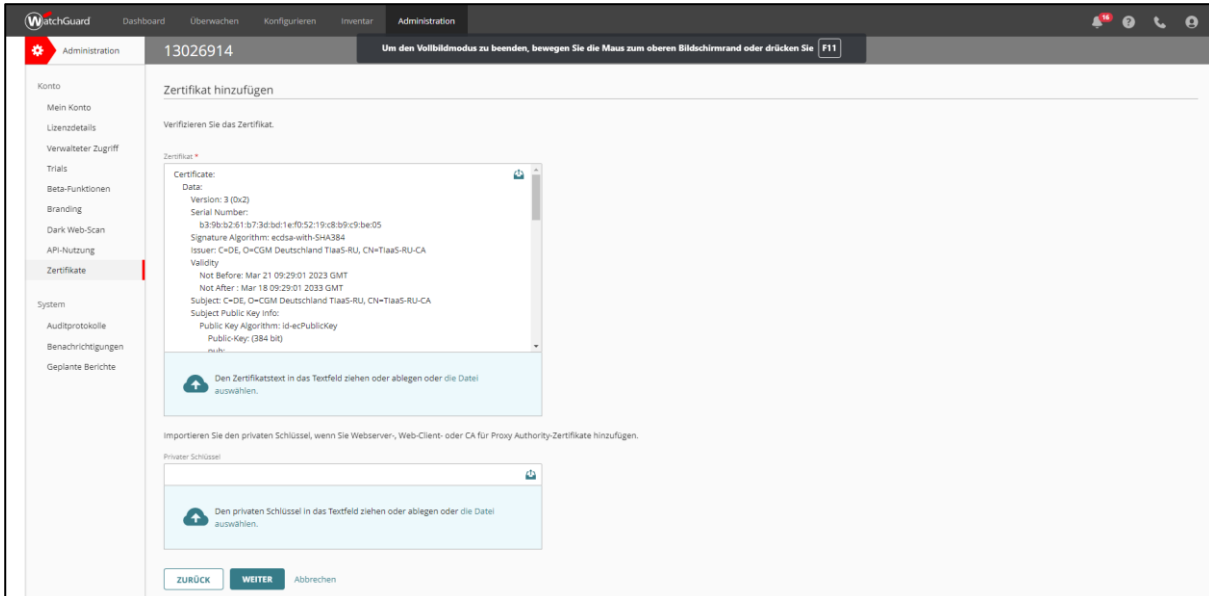


Es muss nun das mitgelieferte Zertifikat ausgewählt werden. Dazu muss die Datei „TlaaS-CA-Cert.txt“ ausgewählt oder mit Drag&Drop auf die markierte Oberfläche gezogen werden. Bei etwaigen Fehlermeldungen ist die Datei „TlaaS-CA-Cert.txt“ zu öffnen und nur der Teil des Dokuments, der sich zwischen „-----BEGIN CERTIFICATE-----“ und „-----END CERTIFICATE-----“ (inkl. der beiden genannten Zeilen) in das Eingabefeld der WG-Cloud zu kopieren.



Die Konfigurationsseite zeigt nun das hinzugefügte Zertifikat an und es kann gespeichert werden. Ein privater Schlüssel wird bei diesem Schritt nicht hinzugefügt, sodass dieses Feld leer bleibt.

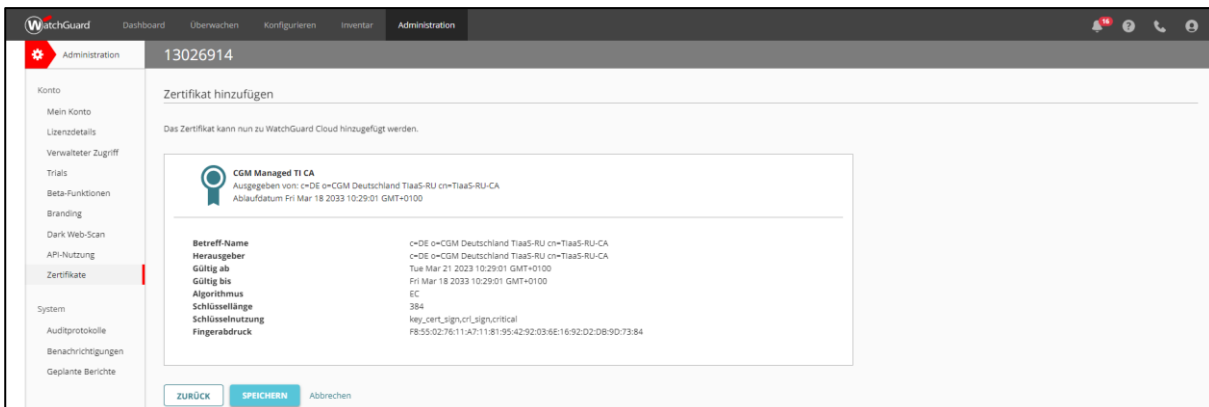
Installationsanleitung CGM MANAGED TI mit CGM FIREWALL M oder L



Mit der „Weiter“ Schaltfläche wird die Bestätigungsseite angezeigt.

Wurde der gesamte Arbeitsvorgang in der Vergangenheit bereits erfolgreich durchgeführt, so wird nun eine Fehlermeldung „Ein Zertifikat mit demselben Fingerabdruck existiert bereits“ eingeblendet.

Es kann nun die Richtigkeit des Zertifikates überprüft werden, bevor es mit der Schaltfläche „Speichern“ für Ihren Administrationsbereich hinzugefügt wird.

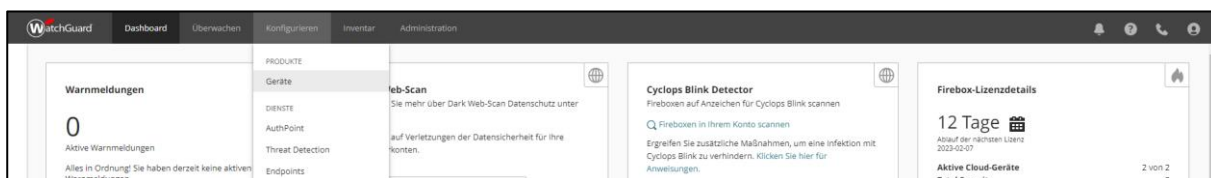


Installationsanleitung CGM MANAGED TI mit CGM FIREWALL M oder L

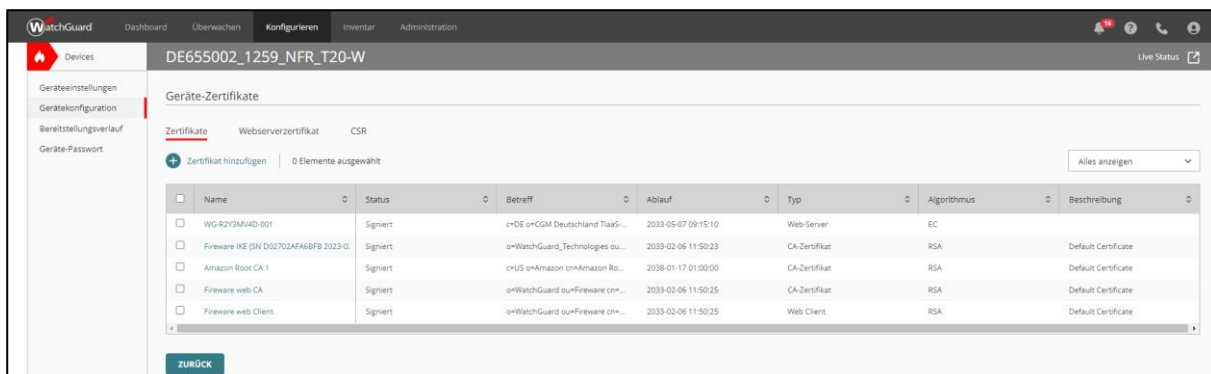
3.2 Geräte-Zertifikat auf der CGM FIREWALL hinzufügen

In unserer Anleitung verwenden wir die Zertifikatdateien mit dem Namen „WG-R2Y3MV4D-001“

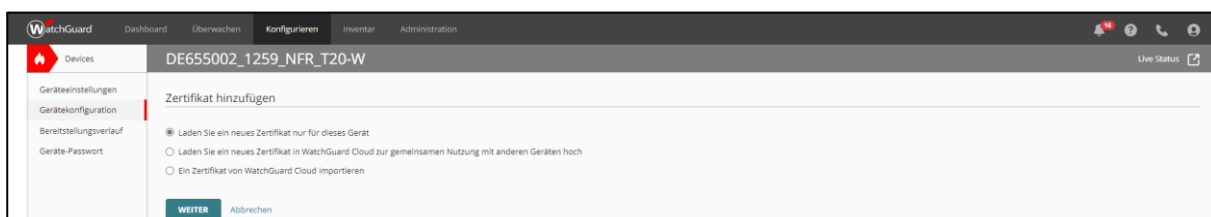
Im Hauptmenü muss im Register „Konfigurieren“ nun die Option „Geräte“ ausgewählt werden. Dort ist die einzurichtende Firebox auszuwählen.



Im Menüpunkt „Gerätekonfiguration“ ist die Option „Zertifikate“ auszuwählen. Dort muss nun mit der Aktion „Zertifikat hinzufügen“ das mitgelieferte Geräte-Zertifikat abgelegt werden.

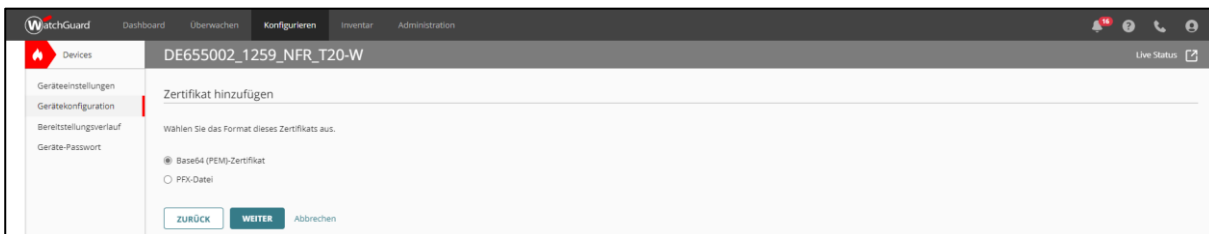


Im nächsten Schritt muss „Laden Sie ein neues Zertifikat nur für dieses Gerät“ ausgewählt werden, damit das Zertifikat nur für das gewählte Gerät verfügbar ist.



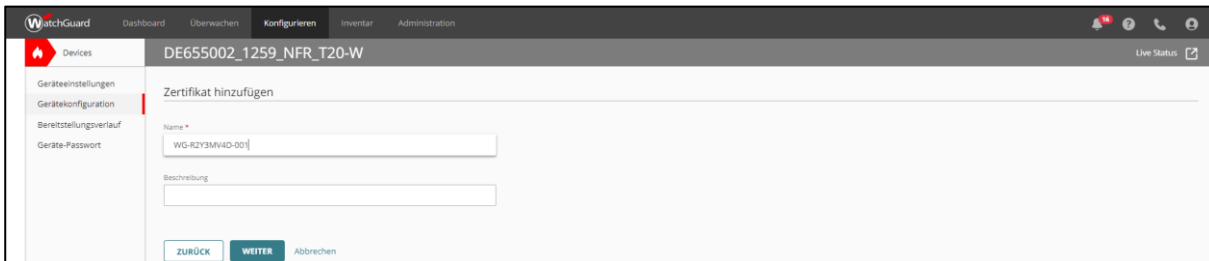
Installationsanleitung CGM MANAGED TI mit CGM FIREWALL M oder L

Wie beim Hinzufügen des CA-Zertifikates muss die Option “Base64 (PEM)-Zertifikat” gewählt werden.



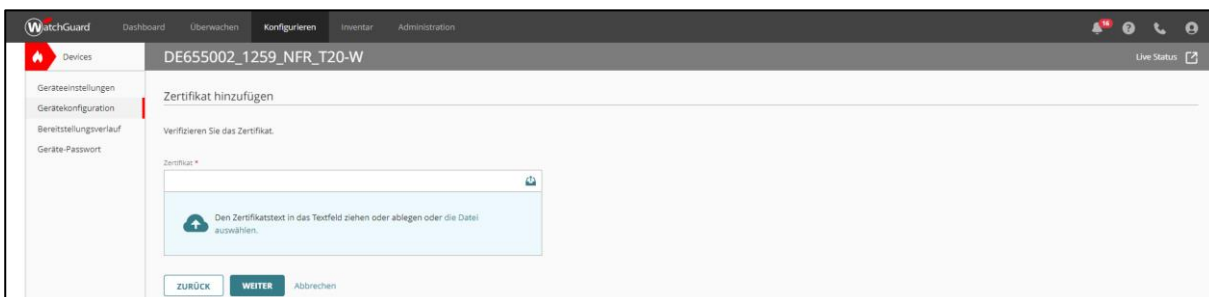
The screenshot shows the WatchGuard configuration interface for device DE655002_1259_NFR_T20-W. The 'Konfigurieren' (Configure) tab is active, and the 'Zertifikat hinzufügen' (Add Certificate) page is displayed. The left sidebar shows the navigation menu with 'Gerätekonfiguration' (Device Configuration) selected. The main content area has the heading 'Zertifikat hinzufügen' and a sub-heading 'Wählen Sie das Format dieses Zertifikats aus.' (Select the format of this certificate). Two radio buttons are present: 'Base64 (PEM)-Zertifikat' (selected) and 'PKIX-Datei'. At the bottom are buttons for 'ZURÜCK' (Back), 'WEITER' (Next), and 'Abbrechen' (Cancel).

Es muss ein eindeutiger Name gewählt werden. Es bietet sich an, den Namen des mitgelieferten Zertifikates hier einzugeben. Wir verwenden den Profil-Namen aus der Login-Daten.txt, in unserer Anleitung WG-R2Y3MV4D-001.



The screenshot shows the WatchGuard configuration interface for device DE655002_1259_NFR_T20-W. The 'Konfigurieren' (Configure) tab is active, and the 'Zertifikat hinzufügen' (Add Certificate) page is displayed. The left sidebar shows the navigation menu with 'Gerätekonfiguration' (Device Configuration) selected. The main content area has the heading 'Zertifikat hinzufügen'. Below the heading, there are two input fields: 'Name' (filled with 'WG-R2Y3MV4D-001') and 'Beschreibung' (empty). At the bottom are buttons for 'ZURÜCK' (Back), 'WEITER' (Next), and 'Abbrechen' (Cancel).

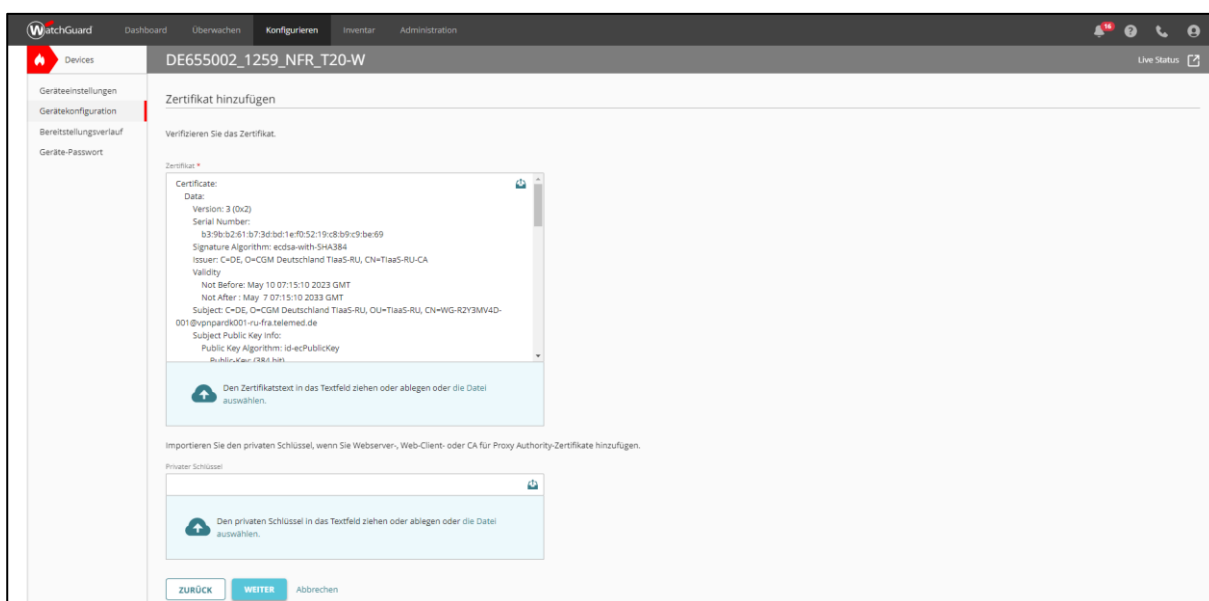
In der nächsten Eingabemaske werden die zwei Bestandteile des Geräte-Zertifikates eingegeben.



The screenshot shows the WatchGuard configuration interface for device DE655002_1259_NFR_T20-W. The 'Konfigurieren' (Configure) tab is active, and the 'Zertifikat hinzufügen' (Add Certificate) page is displayed. The left sidebar shows the navigation menu with 'Gerätekonfiguration' (Device Configuration) selected. The main content area has the heading 'Zertifikat hinzufügen' and a sub-heading 'Verifizieren Sie das Zertifikat.' (Verify the certificate). Below the heading, there is a 'Zertifikat' (Certificate) input field. A blue提示 box with a cloud icon and text says: 'Den Zertifikatstext in das Textfeld ziehen oder ablegen oder die Datei auswählen.' (Drag the certificate text into the text field or drop it or select the file). At the bottom are buttons for 'ZURÜCK' (Back), 'WEITER' (Next), and 'Abbrechen' (Cancel).

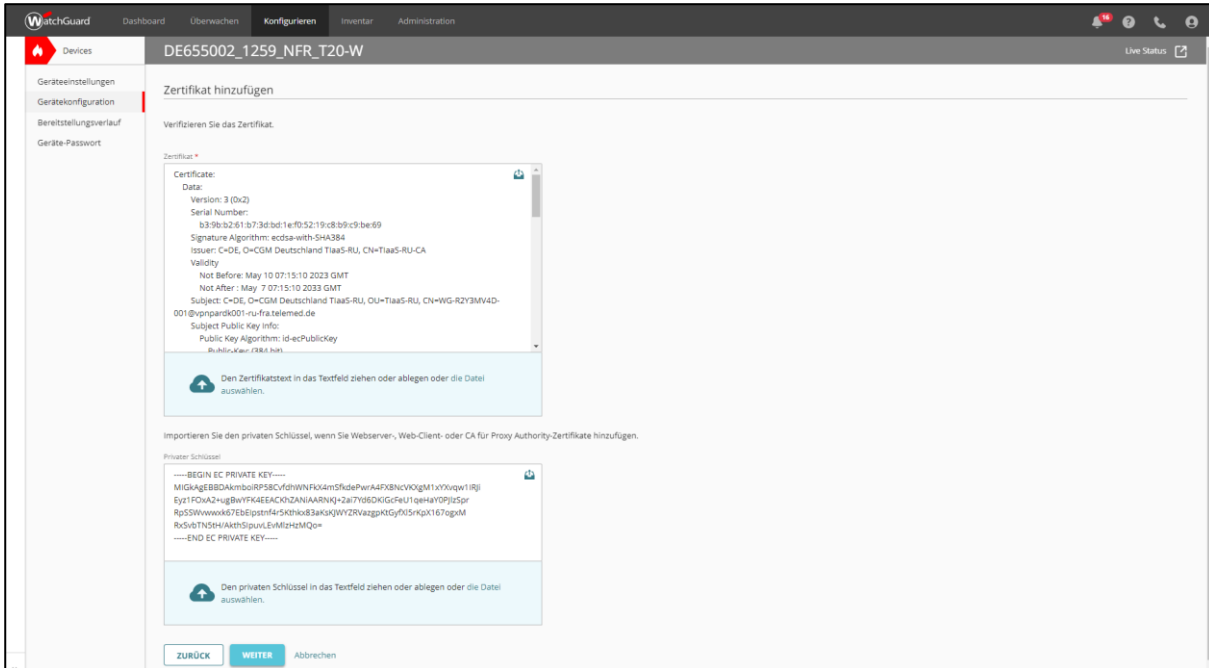
Installationsanleitung CGM MANAGED TI mit CGM FIREWALL M oder L

Es muss zuerst das Zertifikat über die mitgelieferte CRT-Datei entweder über Drag&Drop oder die Dateiauswahl hinzugefügt werden. Bei etwaigen Fehlermeldungen ist die Datei „<Profilname>_cert.txt“ zu öffnen und nur der Teil des Dokuments, der sich zwischen „-----BEGIN CERTIFICATE-----“ und „-----END CERTIFICATE-----“ (inkl. der beiden genannten Zeilen) in das Eingabefeld der WG-Cloud zu kopieren.



Nach Eingabe der CRT-Datei bzw. nach Einkopieren des Zertifikats verändert sich die Eingabemaske und ermöglicht das Hinzufügen des privaten Schlüssels mit der mitgelieferten KEY-Datei auf die gleiche Art und Weise.

Installationsanleitung CGM MANAGED TI mit CGM FIREWALL M oder L



Zertifikat hinzufügen

Verifizieren Sie das Zertifikat.

Zertifikat *

Certificate:
 Data:
 Version: 3 (0x2)
 Serial Number:
 Signature Algorithm: ecdsa-with-SHA384
 Issuer: C=DE, O=CGM Deutschland T1aa5-RU, CN=T1aa5-RU-CA
 Validity
 Not Before: May 10 07:15:10 2023 GMT
 Not After: May 7 07:15:10 2023 GMT
 Subject: C=DE, O=CGM Deutschland T1aa5-RU, OU=T1aa5-RU, CN=WG-R2Y3MV4D-001@vnpardk001-ru-fra.telemed.de
 Subject Public Key Info:
 Public Key Algorithm: id-ecPublicKey
 Public Key: -----BEGIN EC PUBLIC KEY-----

Den Zertifikatstext in das Textfeld ziehen oder ablegen oder die Datei auswählen.

Importieren Sie den privaten Schlüssel, wenn Sie Webserven-, Web-Client- oder CA für Proxy Authority-Zertifikate hinzufügen.

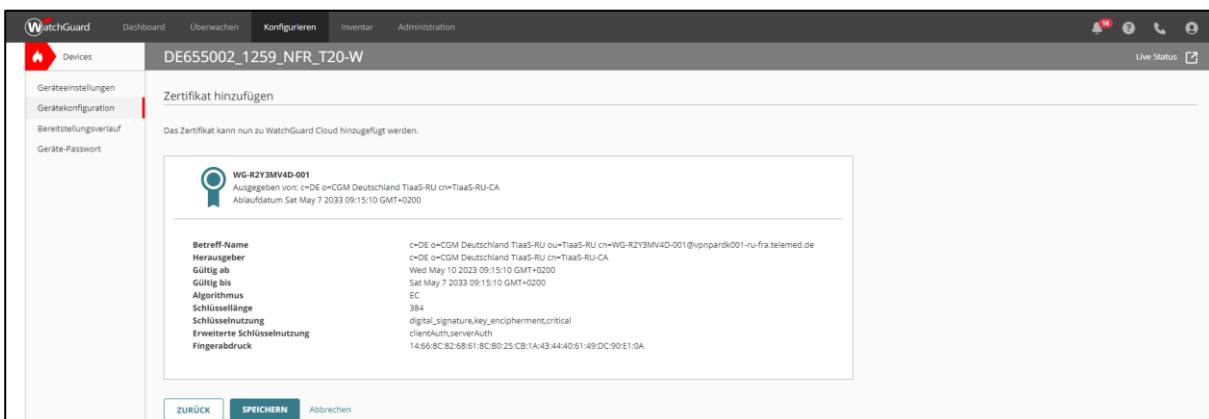
Privater Schlüssel

-----BEGIN EC PRIVATE KEY-----
 MIGKAgEBBDAKmbolRPS8CvfdhWfKdAmSfdePwA4FXBNcyOGM1xyVqv1IRj
 Eyt1FOx2+ug8WvYK4EEACkZANIAARhVQ+2a7Y0S0KGCFeU1qehAYOPj2Spr
 Rg5SWwwak5T8dtpstefarSR9kx3BakxjWY2Rvazgpxtyf9f5nkpX167gpm
 Rk5vdtN5H4AmthdipunLvmZhtzMQo=

Den privaten Schlüssel in das Textfeld ziehen oder ablegen oder die Datei auswählen.

ZURÜCK **WEITER** Abbrechen

Anschließend wird das Zertifikat zur Kontrolle angezeigt und man kehrt mit „Speichern“ zur nun aktualisierten Zertifikatsliste zurück, wo nun auch das neu hinzugefügte Zertifikat zu finden ist.



Zertifikat hinzufügen

Das Zertifikat kann nun zu WatchGuard Cloud hinzugefügt werden.

WG-R2Y3MV4D-001

Ausgegeben von: C=DE, O=CGM Deutschland T1aa5-RU, CN=T1aa5-RU-CA
 Ablaufdatum: Sat May 7 2023 09:15:10 GMT+0200

Betreff-Name	C=DE, O=CGM Deutschland T1aa5-RU, OU=T1aa5-RU, CN=WG-R2Y3MV4D-001@vnpardk001-ru-fra.telemed.de
Herausgeber	C=DE, O=CGM Deutschland T1aa5-RU, CN=T1aa5-RU-CA
Gültig ab	Wed May 10 2023 09:15:10 GMT+0200
Gültig bis	Sat May 7 2023 09:15:10 GMT+0200
Algorithmus	EC
Schlüssellänge	384
Schlüsselnutzung	digitalSignature, keyEncipherment, critical
Erweiterte Schlüsselnutzung	clientAuth, serverAuth
Fingerabdruck	14:86:8C:82:68:61:8C:80:25:CB:1A:43:44:40:61:49:DC:90:E1:0A

ZURÜCK **SPEICHERN** Abbrechen

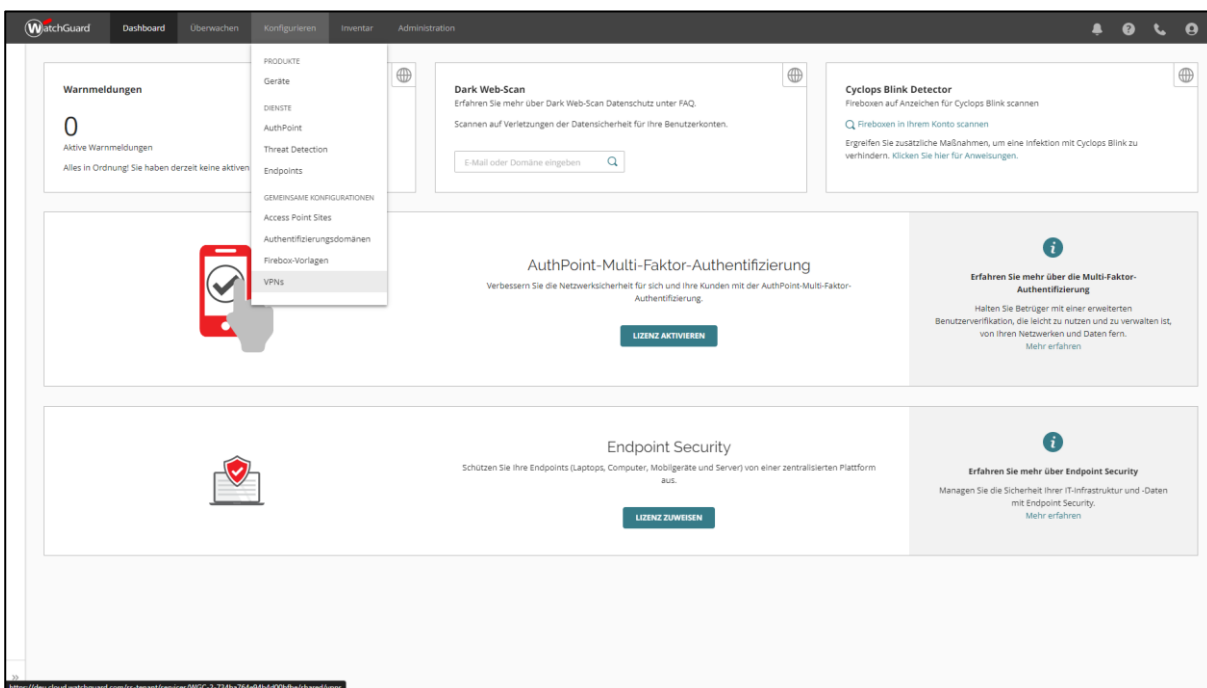
Installationsanleitung CGM MANAGED TI mit CGM FIREWALL M oder L

3.3 VPN-Einrichtung

In unserem Anleitungsbeispiel verwenden wir das Profil mit dem Namen „WG-R2Y3MV4D-001“ und den Endpunkt „vpnpardk001-ru-fra.telemed.de“ der Referenzumgebung.

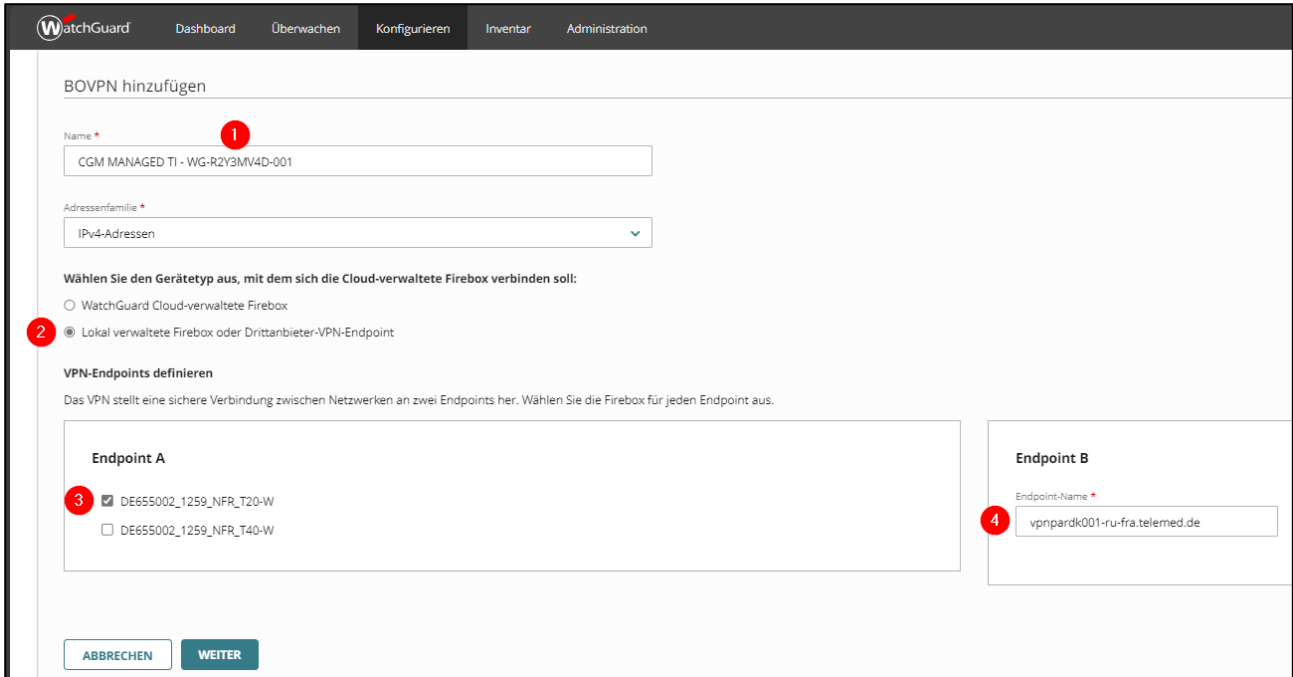
Bei Ihrer Installation müssen immer die Daten aus der Login-Daten.txt verwendet werden!

Im Register „Konfigurieren“ muss die Option „VPNs“ ausgewählt werden:



Im sich danach öffnenden Dialog muss über die Schaltfläche „BOVPN hinzufügen“ ein beliebiger Name (bspw. „CGM MANAGED TI - <Profil-Name>“ (1) aus der Login-Daten.txt) vergeben, die Adressenfamilie „IPv4-Adressen“ und die Option „lokal verwaltete Firebox oder Drittanbieter-VPN-Endpoint“ (2) ausgewählt werden.

Installationsanleitung CGM MANAGED TI mit CGM FIREWALL M oder L

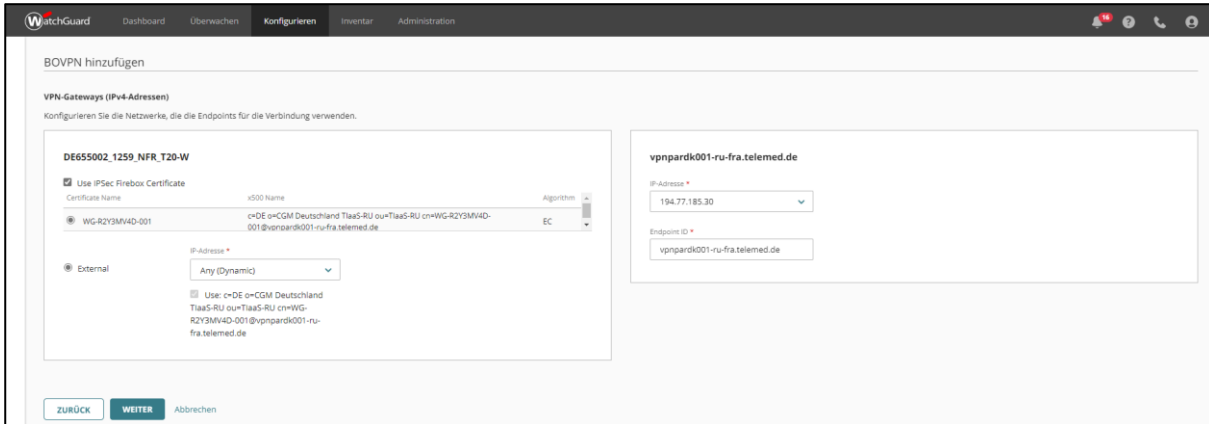


Auf der gleichen Seite muss im Abschnitt „VPN-Endpoints definieren“ zunächst bei „Endpoint A“ (3) die zu verbindende Firebox ausgewählt werden. Im Freitextfeld von „Endpoint B“ (4) muss der in der Login-Daten.txt angegebene VPN Endpunkt eingetragen werden.

Der Klick auf die Schaltfläche „weiter“ bestätigt die Eingaben.

Daraufhin muss im Abschnitt „VPN-Gateways (IPv4-Adressen)“ auf der linken Seite für die im vorherigen Schritt ausgewählte Firebox nun die Option „Use IPsec Firebox Certificate“ gesetzt werden. Das zuvor hinzugefügte Geräte-Zertifikat wird nun angezeigt und muss ausgewählt werden. Auf der rechten Seite muss die IP-Adresse und der *VPN-Endpunkt* aus der Datei *Login-Daten.txt* für die Pflichtfelder „IP-Adresse“ und „Endpoint ID“ eingetragen werden. Sollte die IP-Adresse nicht in der „Login-Daten.txt“ vorhanden sein, kann sie über einen Ping auf den VPN-Endpunkt in einer Kommandozeile ermittelt werden.

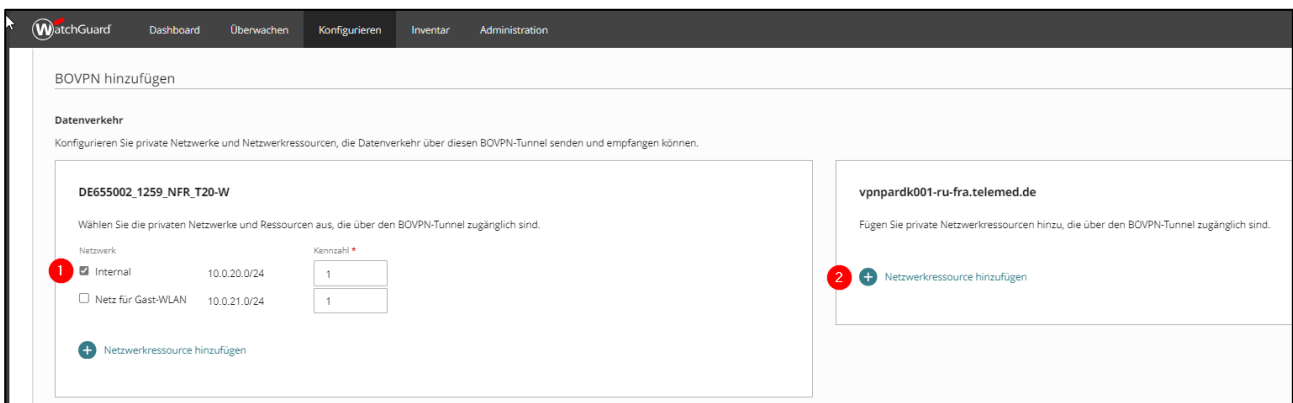
Installationsanleitung CGM MANAGED TI mit CGM FIREWALL M oder L



Im Abschnitt „Datenverkehr“ muss auf der linken Seite die Checkbox „Internal“ (1) aktiviert und die Kennzahl 1 vergeben werden.

Im rechten Bereich müssen die Bestandsnetze, die sich vollständig in der Datei *Login-Daten.txt* unter *Liste der Bestandsnetze* befinden, über die Schaltfläche „Netzwerkressource hinzufügen“ (2) hinzugefügt werden.

Zuletzt muss über die gleiche Schaltfläche die *Konnektor IP* aus der Datei *Login-Daten.txt* als 32er-Netz in CIDR-Notation (Beispieladresse: 192.168.100.1/32) hinzugefügt werden. Der Klick auf die Schaltfläche „weiter“ bestätigt die Eingaben.



Im Abschnitt „Sicherheit“ können die Einstellungen, die beim Aufruf der Seite vorbelegt wurden, übernommen werden.

Der Klick auf die Schaltfläche „Hinzufügen“ schließt die Konfiguration ab.

Installationsanleitung CGM MANAGED TI mit CGM FIREWALL M oder L

BOVPN hinzufügen

Sicherheit

Authentifizierungs- und Verschlüsselungseinstellungen für VPN-Verhandlung konfigurieren.

Gemeinsame Phase 1-Einstellungen

Diese Einstellungen werden von allen VPNs gemeinsam genutzt, die einen Remote-Endpoint mit einem Domänennamen konfiguriert haben.

+

 Phase 1-Einstellungen hinzufügen

Authentifizierung	Verschlüsselung	Diffie-Hellman-Gruppe	SA Life	
<div>SHA2-256</div>	AES-CBC (256-Bit)	Diffie-Hellman-Gruppe14	24 Stunden	

Phase 2-Einstellungen

Authentifizierung *

SHA2-256

Verschlüsselung

AES-CBC (256-Bit)

☒ Perfect Forward Secrecy (PFS) verwenden

PFS-Gruppe *

Diffie-Hellman-Gruppe14

Ablauf des Schlüssels

Wählen Sie aus, wann der VPN-Schlüssel abläuft. Der Ablauf des Schlüssels kann zeitabhängig oder abhängig vom Datenverkehr durch den Tunnel sein.

Zeit *

8 hours

☐ Datenverkehr

↺

 Standard wiederherstellen

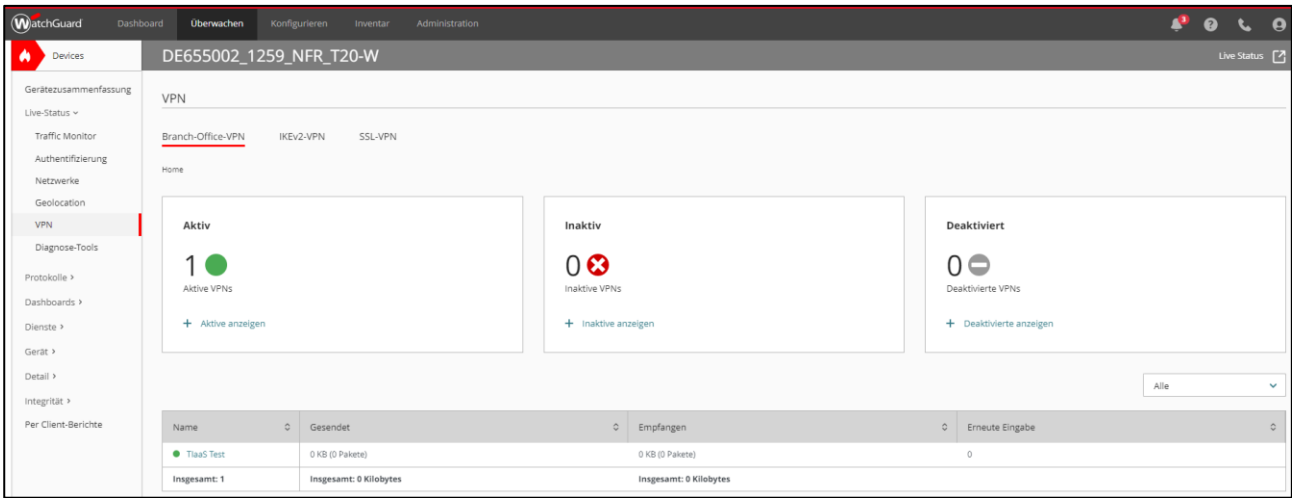
ZURÜCK

HINZUFÜGEN

Abbrechen

3.4 Überprüfung des Verbindungsaufbaus

Nach der Durchführung der Schritte aus Abschnitt 3.1 kann im Register „Überwachen“ nach Auswahl des konfigurierten Geräts unter der Option „VPN“ im Menü „Live-Status“ die VPN-Verbindung überprüft werden. Wenn die Verbindung erfolgreich war, wird mindestens ein aktives VPN angezeigt.

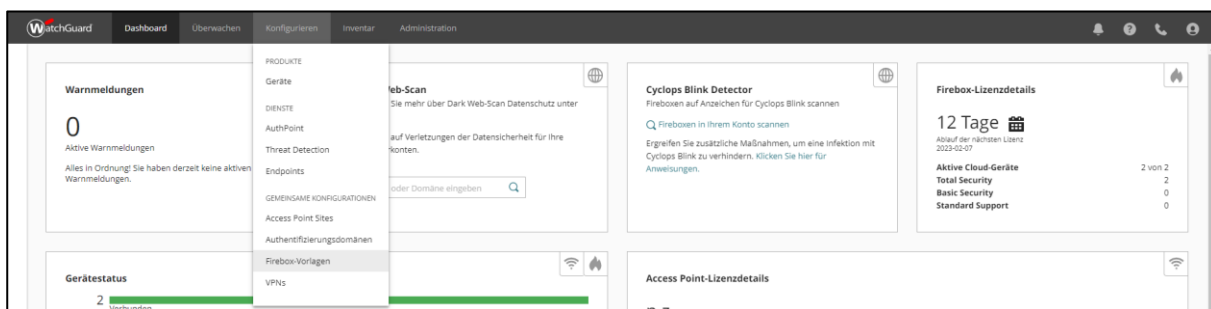


4 Einrichtung der Zugriffe auf die TI-Bestandsnetze

Um den Zugriff auf die TI-Bestandsnetze (bspw. KVSafeNet) zu ermöglichen, müssen die folgenden Schritte durchgeführt werden. Dazu muss die bereitgestellte Vorlage „CGM Managed TI“ abonniert werden. Um IP-Adresskonflikte in der CGM Managed TI Umgebung zu verhindern, werden die Einrichtungsnetze durch NAT verborgen.

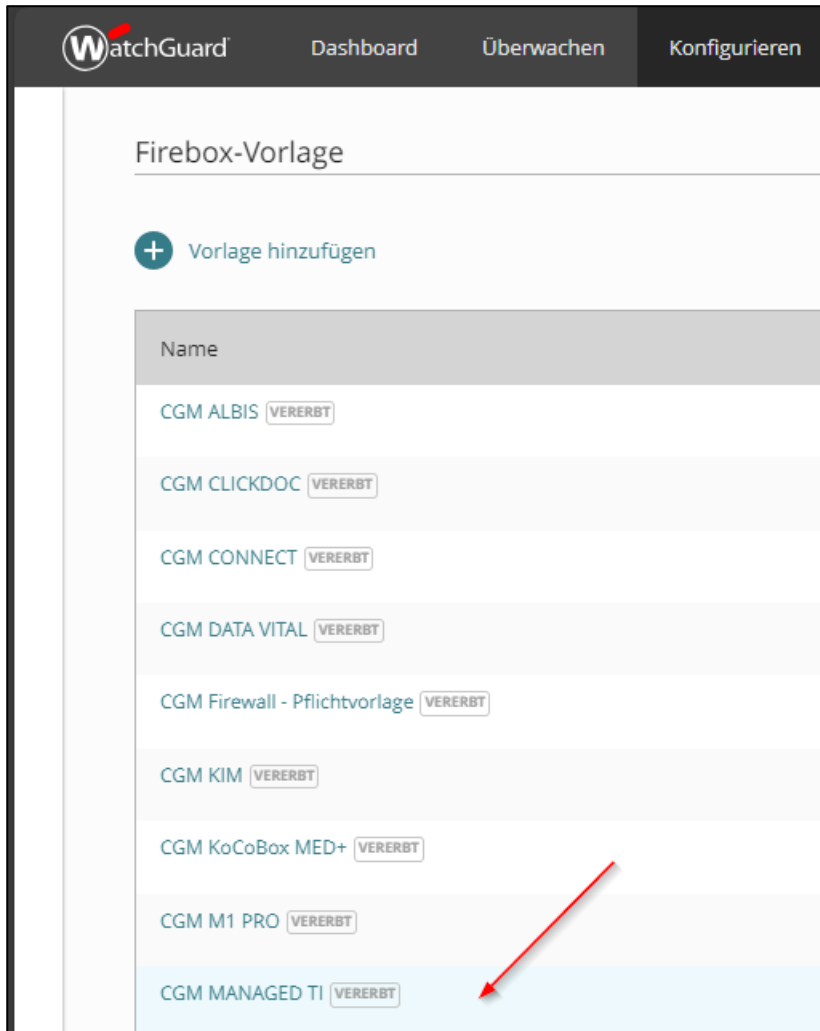
4.1 Einrichtung der Bestandsnetze

Im Hauptmenü muss im Register „Konfigurieren“ die Option „Firebox-Vorlagen“ ausgewählt werden.

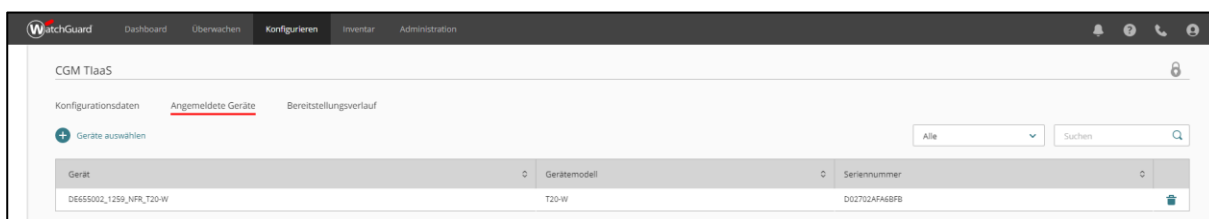


In der Liste ist die Vorlage „CGM MANAGED TI“ auszuwählen.

Installationsanleitung CGM MANAGED TI mit CGM FIREWALL M oder L



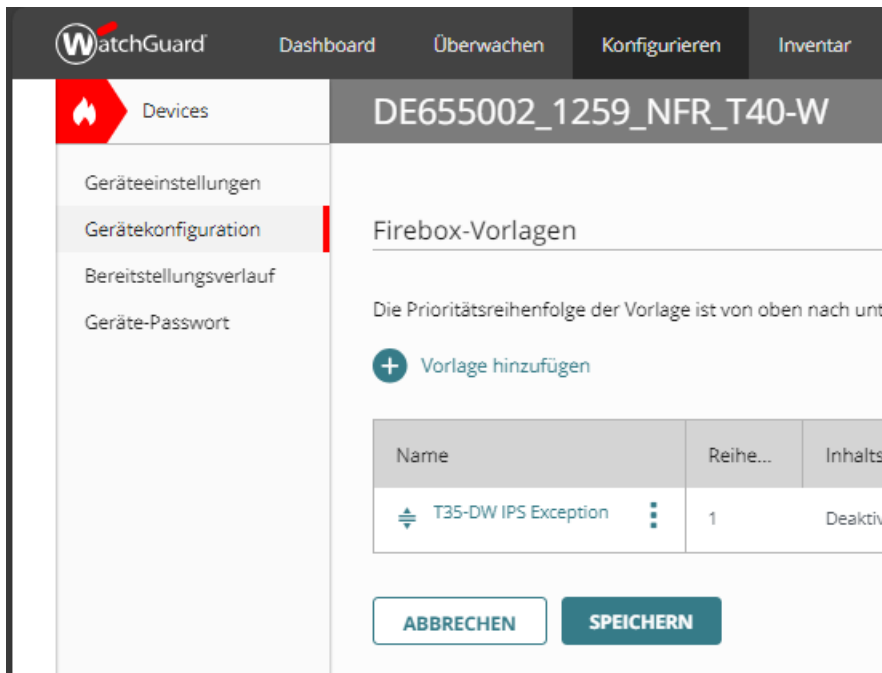
Im Reiter „Angemeldete Geräte“ muss über die Schaltfläche „Geräte auswählen“ die einzurichtende Firebox hinzugefügt werden.



Alternativ kann man die Zuweisung der Vorlage unter „Konfigurieren → Geräte → Gerätekonfiguration“ in der Kachel „Vorlagen“ unten rechts zuweisen. Dort sind alle auf dem Gerät

Installationsanleitung CGM MANAGED TI mit CGM FIREWALL M oder L

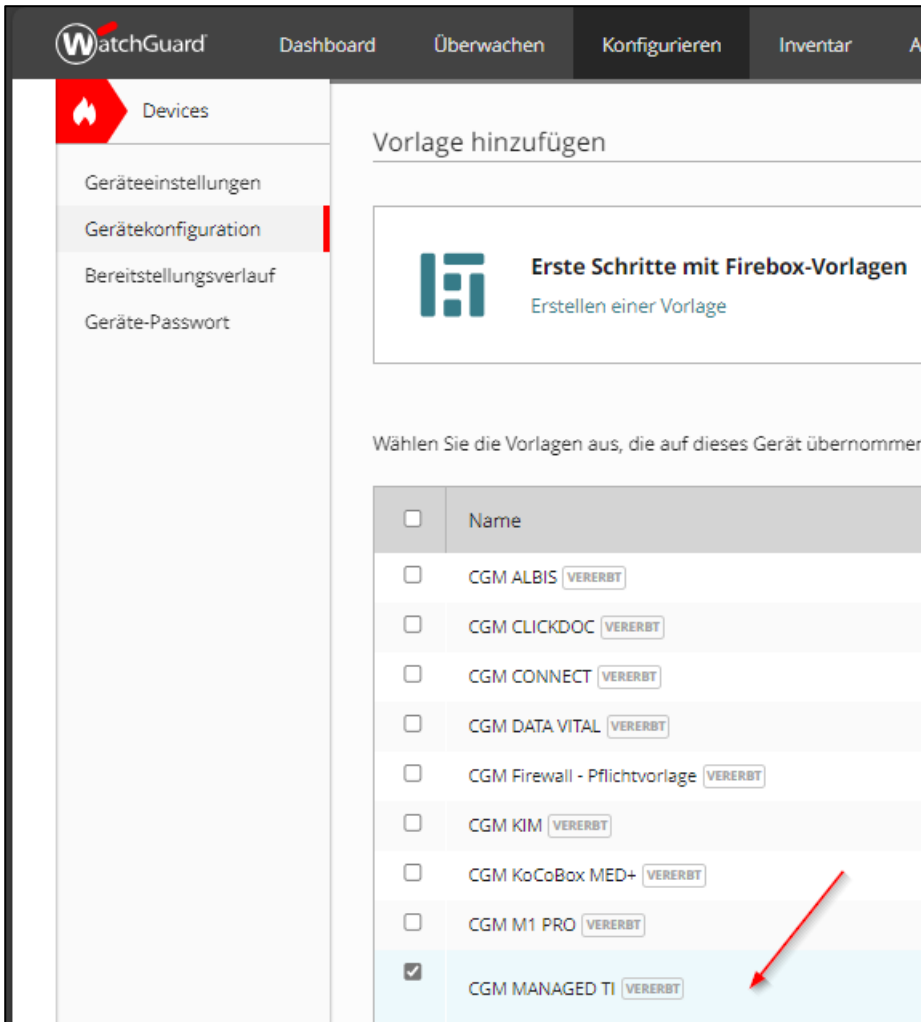
zugewiesenen Vorlagen aufgelistet und es kann hier die Vorlage „CGM MANAGED TI“ ebenfalls über die Schaltfläche „Vorlage hinzufügen“ zugewiesen werden.



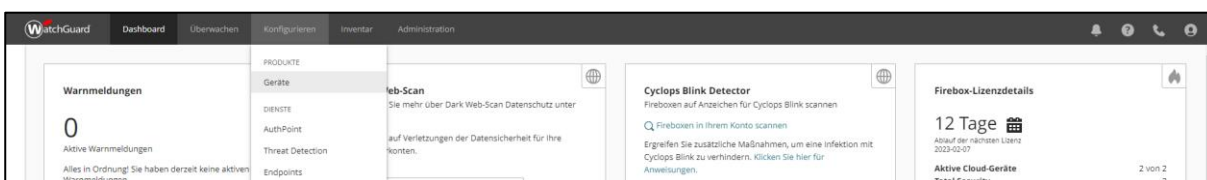
Es muss die Checkbox für die Vorlage markiert werden, damit anschließend über den Button „Hinzufügen“ die Vorlage hinzugefügt wird.

Vorsicht! Es ist keine Bereitstellung nötig! Die Änderungen in den Vorlagen sind sofort wirksam!

Installationsanleitung CGM MANAGED TI mit CGM FIREWALL M oder L



Im Hauptmenü muss im Register „Konfigurieren“ nun die Option „Geräte“ ausgewählt werden. Dort ist die einzurichtende Firebox auszuwählen.



Im Menüpunkt „Gerätekonfiguration“ ist die Option „Firewall-Regeln“ auszuwählen. Dort muss eine „Outbound-Core-Regel“ mit der Schaltfläche „Firewall-Regel hinzufügen“ erstellt werden.

Die folgenden Schritte sind im Unterregister „Einstellungen“ durchzuführen.

Als Name ist „CGM MANAGED TI – TI-Bestandsnetze-Zugriff mit NAT“ (1) zu hinterlegen.

Installationsanleitung CGM MANAGED TI mit CGM FIREWALL M oder L

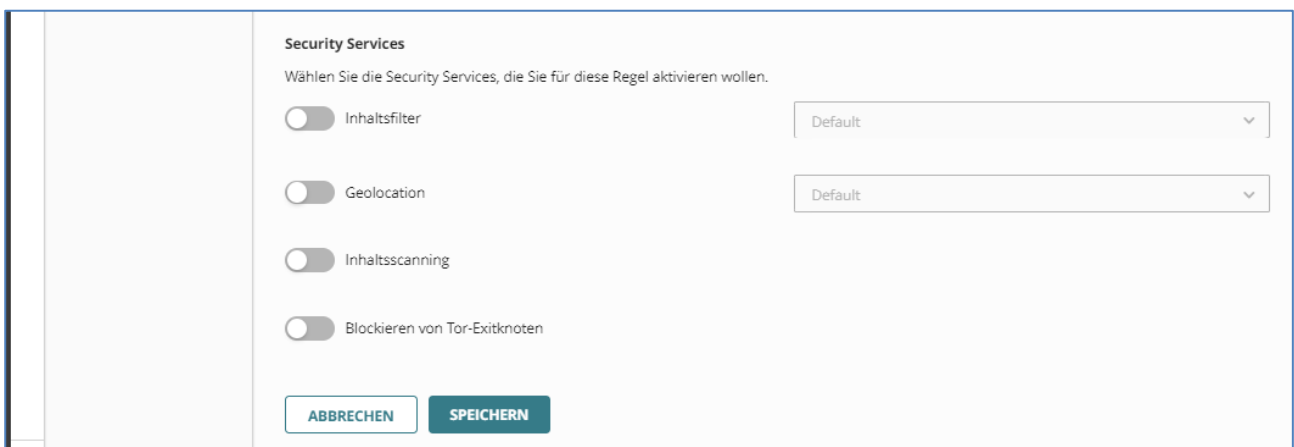
Web-Datenverkehr (Ports 80, 443) muss deaktiviert werden (2).

Es muss „Any“ über die Schaltfläche „Datenverkehrstypen hinzufügen“ hinzugefügt werden (3).

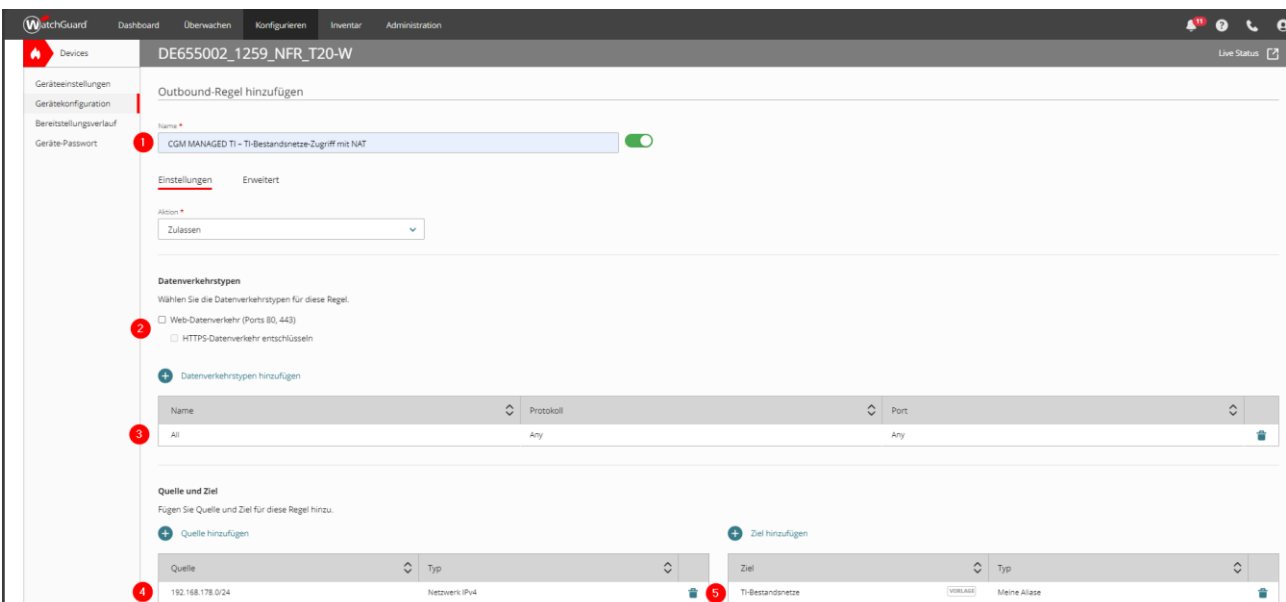
Als Quelle ist das in der Praxis genutzte IP-Netzwerk mit „Netzwerk IPv4“ über die Schaltfläche „Quelle hinzufügen“ hinzuzufügen (4).

Als Ziel ist die Vorlage „TI-Bestandsnetze VORLAGE“ unter „Meine Aliase“ auszuwählen (5).

Im unteren Bereich „Security Services“ müssen alle Schalter deaktiviert werden.



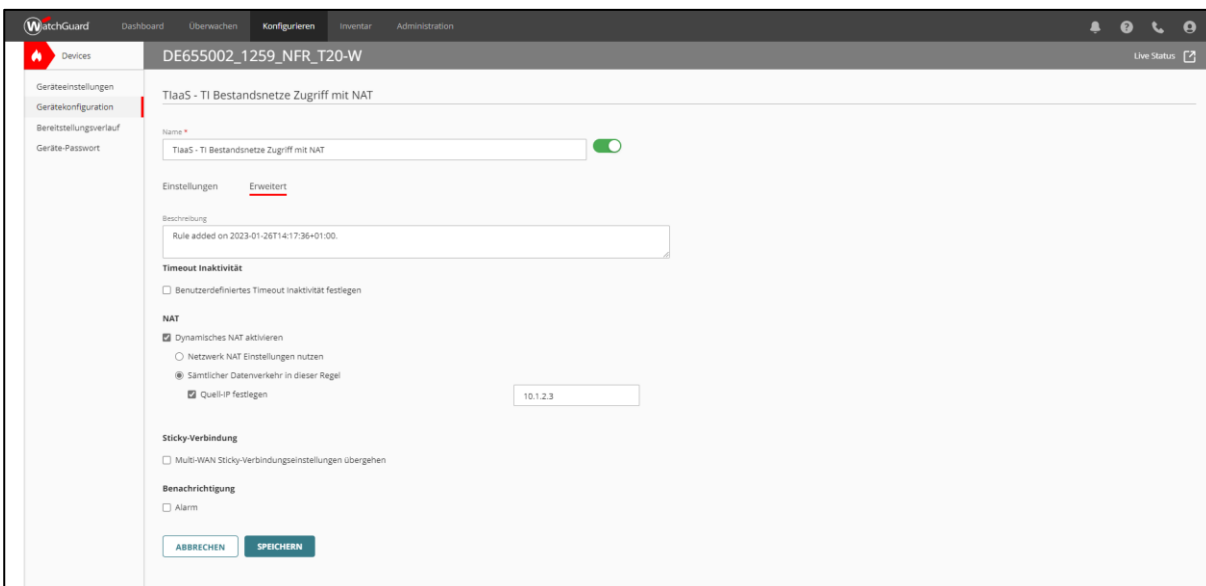
Das Ergebnis der Konfiguration sollte aussehen, wie in der nachfolgenden Abbildung dargestellt:



Installationsanleitung CGM MANAGED TI mit CGM FIREWALL M oder L

Anschließend muss in das Unterregister „Erweitert“ gewechselt werden.

Dort muss im Abschnitt „NAT“ die Option „Dynamisches NAT aktivieren“ aktiviert werden. Danach müssen die Optionen „Sämtlicher Datenverkehr in dieser Regel“ und „Quell-IP festlegen“ aktiviert werden. Im Eingabefeld auf der rechten Seite muss die *NAT-IP* aus der Datei *Login-Daten.txt* eingetragen werden. Mit Klick auf die Schaltfläche „Speichern“ wird die Konfiguration abgeschlossen.



Die Änderungen werden erst nach der Bereitstellung aktiv.

4.2 Überprüfen der Einstellungen

Die korrekte Funktionsfähigkeit der TI-Verbindung sollte nun gegeben sein. Überprüfbar ist das beispielsweise durch einen Ping auf den Konnektor von einem beliebigen Endgerät aus dem Praxis-LAN. Dazu ist in einer Kommandozeile folgender Befehl, ergänzt mit der *Konnektor-IP* aus der Datei *Login-Daten.txt*, auszuführen:

```
ping <Konnektor-IP>
```

Wenn die Funktion gegeben ist, kommen nach der Ausführung des Befehls vier Antworten zurück. Falls die Funktion nicht gegeben ist, werden hier nur vier Zeitüberschreitungen angezeigt und die vorher getätigten Einstellungen müssen überprüft werden.



Installationsanleitung CGM MANAGED TI mit CGM FIREWALL M oder L

Hinweis: Im parallelen Modus müssen an den Endgeräten im Praxis-LAN oder am Standardgateway der Praxis die Routen für die Bestandsnetze und die Konnektor-IP über die CGM-Firewall hinzugefügt werden, damit ein Ping beantwortet werden kann.

5 Kartenterminal-Konfiguration

5.1 IP-Konfiguration der Kartenterminals

Zur Vermeidung von IP-Adresskonflikten müssen die Kartenterminals im LAN der Einrichtung des Leistungserbringers in einem festgelegten Adressbereich konfiguriert werden. Eine Liste der möglichen IP-Adressen befindet sich unter *IPs für Arbeitsplätze und Kartenterminals* in der Datei *Login-Daten.txt*. Die Anzahl der IP-Adressen ergibt sich aus der Bestellung. Aufgelistet sind zunächst die IP-Adressen der Arbeitsplätze, danach die IP-Adressen der Kartenterminals. Es empfiehlt sich demnach, bei der Zuteilung rechts in der Liste zu beginnen. Andere KT-IP-Adressen können nicht akzeptiert und hinzugefügt werden.

5.2 Netzwerkkonfiguration der CGM FIREWALL

Die Kartenterminals haben nun die zugewiesenen IP-Adressen erhalten und die CGM FIREWALL ist im Praxisnetzwerk angebunden.

Damit die Kartenterminals die Verbindung zu Managed TI aufbauen können, muss das jeweils richtige Interface mit einer Adresse aus diesem Netz zur Verwendung als Standard-Gateway versorgt werden.

Nun werden, abhängig vom Netzwerklayout, zwei Fälle unterschieden:

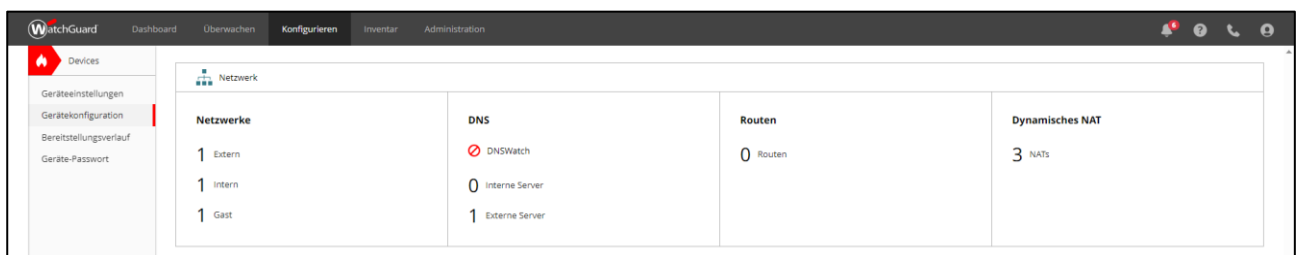
- **Firewall ist im Parallelbetrieb angebunden**
Hier muss ein sekundäres Netzwerk am externen Interface der Firewall konfiguriert werden. Eine Anpassung des Netzwerks „Internal“ wird nicht benötigt.
- **Firewall ist im seriellen Betrieb angebunden**
Hier muss ein sekundäres Netzwerk am internen Interface der Firewall konfiguriert werden.

Als Netz-IP muss eine beliebige IP-Adresse aus dem Netzbereich /24 der KT-IP-Adressen als /24-Netz eingetragen werden. Diese IP-Adresse ist bei allen Kartenterminals als Gateway einzutragen und stellt damit auf Layer-2-Ebene die Verbindung zur Firewall dar. Das muss so modelliert werden, damit die KT-IPs nicht geNATtet werden.

Beispiel: Eine Bestellung enthält IP-Adressen für 2 KTs: 10.0.0.2 und 10.0.0.3. Als sekundäres Netz wird nun 10.0.0.100/24 gewählt, um Adresskonflikte mit anderen Bestellungen definitiv aus dem Weg zu gehen und den Kartenterminals als Gateway angeboten.

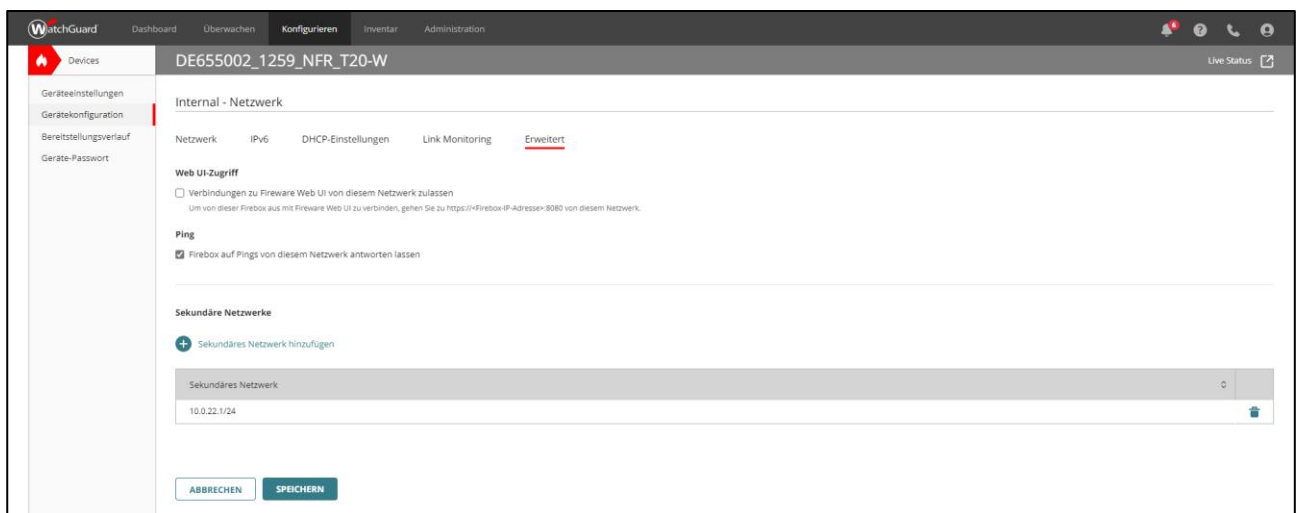
Installationsanleitung CGM MANAGED TI mit CGM FIREWALL M oder L

Im „Konfigurieren“-Bereich der Firewall muss im Untermenü „Gerätekonfiguration“ im Bereich „Netzwerk“ auf die Kachel „Netzwerke“ geklickt werden.



Dort wird entsprechend der Betriebsart, wie oben beschrieben, das richtige Netzwerk ausgewählt. Im Register „Erweitert“ kann unter „Sekundäre Netzwerke“ das in der Login-Daten.txt unter „Lokale Ips“ zugewiesene Netzwerk hinzugefügt werden und die IP 10.x.x.254/24 angegeben werden.

Diese Adresse ist für die Kartenterminals das zu konfigurierende Standardgateway.



Die Änderungen werden erst nach der Bereitstellung aktiv.

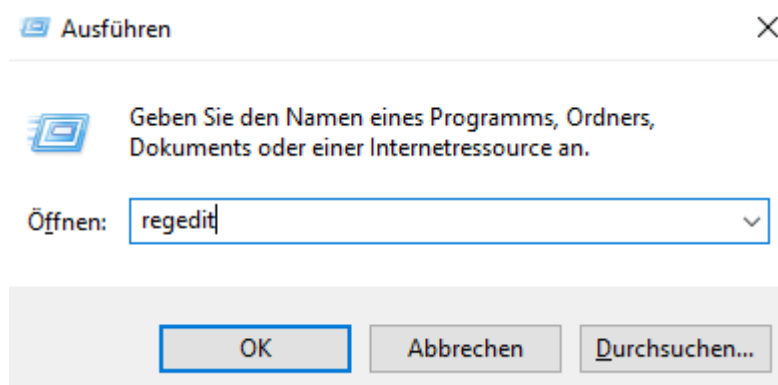
6 Anpassungen für die Eventschnittstelle von Primärsystemen

Damit das Karteneinlesen per Konnektor-Event funktioniert, müssen einige Schritte zusätzlich erfolgen. Abhängig vom zu installierenden Primärsystem muss jedem Arbeitsplatz zusätzlich eine weitere IP aus der IP-Range *IPs für Arbeitsplätze und Kartenterminals* der Datei „Login-Daten.txt“ zugeteilt werden. Dies gilt nach aktuellem Stand der Dinge für folgende Primärsysteme der CGM sowie ggf. für weitere Primärsysteme:

- CGM MEDISTAR
- CGM TURBOMED
- CGM ALBIS
- CGM M1/M1.Pro
- CGM Z1/Z1.Pro

Dazu ist dem LAN-Interface jedes anzubindenden Arbeitsplatzes konfliktfrei jeweils eine zweite IP-Adresse aus dem o.g. Netzbereich (vordefiniert durch die *IPs für Arbeitsplätze und Kartenterminals* der Datei „Login-Daten.txt“) zuzuordnen und mit der Subnetzmaske 255.255.255.0 zu belegen. In CGM MEDISTAR muss nun jedem betroffenen Task die jeweilige zweite IP-Adresse aus der Datei „Login-Daten.txt“ zugewiesen werden.

In allen anderen Systemen ist per STRG + R die Funktion „regedit“ aufzurufen:



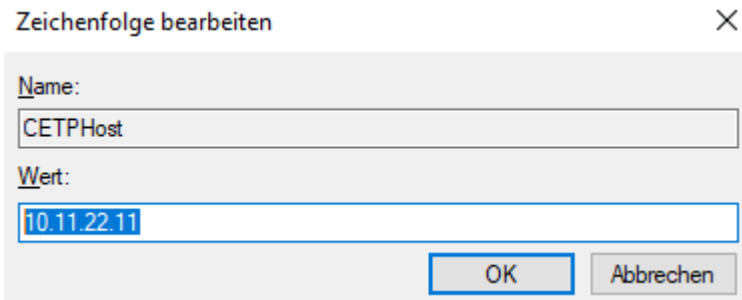
Falls noch nicht vorhanden muss im Pfad

„HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\CompuGROUP“ über die rechte Maustaste → Neu → Schlüssel ein Schlüssel mit dem Namen „Kocops“ erstellt werden.

Für diesen Schlüssel muss nun auf der rechten Seite des Fensters über die rechte Maustaste → Neu → Zeichenfolge eine neue Zeichenfolge angelegt werden, die den Namen „CETPHost“ trägt.

Installationsanleitung CGM MANAGED TI mit CGM FIREWALL M oder L

Der Wert der Zeichenfolge ist nun die IP-Adresse, die auf diesem Rechner angelegt wurde. Im Screenshot ist das beispielsweise die 10.11.22.11:



Zeichenfolge bearbeiten X

Name:
CETPHost

Wert:
10.11.22.11

OK Abbrechen

Danach muss das Primärsystem neugestartet werden.