Wachendorff Prozesstechnik GmbH & Co. KG
Industriestrasse 7
D-65366 Geisenheim
Tel.: +49 (0) 67 22 / 99 65 - 20
Fax: +49 (0) 67 22 / 99 65 - 78
www.wachendorff-prozesstechnik.de

OpenVPN Server eFive 25

Bedienungsanleitung

Stand: 17.12.2015

Copyright by Wachendorff Prozesstechnik GmbH & Co. KG, Industriestraße 7, D-65366 Geisenheim, Tel.: +49-6722/9965-20, Fax: -78.
Alle Angaben ohne Gewähr, Irrtümer und Änderungen vorbehalten.

Inhaltsverzeichnis

1 Vorwort ... 3
2 Sicherheishinweise ... 4
2.1 Allgemeine Hinweise ... 4
2.2 Bestimmungsgemäße Verwendung ... 4
2.3 Qualifiziertes Personal ... 4
2.4 Restgefahren ... 4
2.5 Haftung ... 4
2.6 CE-Konformität ... 4
3 eFive 25 ... 5
3.1 Über den Server ... 5
3.2 Anschlussdarstellung ... 6
3.2.1 Status LEDs auf der Frontseite ... 7
3.2.2 Serielle Schnittstelle ... 8
3.2.3 Netzwerke ... 9
3.3 Allgemeine Aufbaurichtlinien ... 10
3.3.1 Abmessungen ... 10
3.4 IP-Adressen ... 11
3.5 Serieller Zugang zum eFive (Neustart, Reset) ... 11
4 Konfiguration ... 14
4.1 Anschluss: PC und eFive ... 14
4.2 Webinterface öffnen ... 15
4.2.1 Startbildschirm ... 16
4.2.2 IP-Adressen ändern ... 16
4.2.3 Updates ... 17
4.2.4 eFive als DHCP-Server im LAN ... 17
4.2.5 VPN-Netzwerk aufbauen ... 17
5 Beispielaufbauten ... 18
5.1 eFive als Firewall + VPN-Server ... 18
5.2 eFive als VPN-Server in DMZ ... 18
5.3 eFive als Firewall + VPN-Server in DMZ ... 19
6 Copyright ... 20
6.1 Haftungsausschluß ... 20
7 Sonstige Bestimmungen und Standards ... 20
8 Kundenservice und Technischer Support ... 20

1 Vorwort

Verehrter Kunde!
Wir bedanken uns für Ihre Entscheidung ein Produkt unseres Hauses einzusetzen und gratulieren Ihnen zu diesem Entschluss. Die Geräte von Wachendorff Prozesstechnik GmbH & Co. KG können vor Ort für zahlreiche unterschiedliche Anwendungen eingesetzt werden.
Um die Funktionsvielfalt dieser Geräte für Sie optimal zu nutzen, bitten wir Sie folgendes zu beachten:
Jede Person, die mit der Inbetriebnahme oder Bedienung dieses Gerätes beauftragt ist, muss die Betriebsanleitung und insbesondere die Sicherheitshinweise gelesen und verstanden haben!

2 Sicherheishinweise

2.1 Allgemeine Hinweise

Zur Gewährleistung eines sicheren Betriebes darf das Gerät nur nach den Angaben in der Betriebsanleitung betrieben werden. Bei der Verwendung sind zusätzlich die für den jeweiligen Anwendungsfall erforderlichen Rechts- und Sicherheitsvorschriften zu beachten. Sinngemäß gilt dies auch bei Verwendung von Zubehör.

2.2 Bestimmungsgemäße Verwendung

Der eFive Server ist für den Verbindungsaufbau bzw. der Herstellung eines VPN-Netzwerkes geschaffen.

☞ Er darf nicht als alleiniges Mittel zur Abwendung gefährlicher Zustände an Maschinen und Anlagen eingesetzt werden. Maschinen und Anlagen müssen so konstruiert werden, das fehlerhafte Zustände nicht zu einer für das Bedienpersonal gefährlichen Situation führen können (z. B. durch unabhängige Grenzwertschalter, mechanische Verriegelungen, etc.).

2.3 Qualifiziertes Personal

Ein eFive Server darf nur von qualifiziertem Personal, ausschließlich entsprechend der technischen Daten verwendet werden.
Qualifiziertes Personal sind Personen, die mit der Aufstellung, Montage, Inbetriebnahme und Betrieb dieses Gerätes vertraut sind und die über eine ihrer Tätigkeit entsprechenden Qualifikation verfügen.

2.4 Restgefahren

Der eFive Server entspricht dem Stand der Technik und ist betriebssicher. Von dem Gerät können Restgefahren ausgehen, wenn sie von ungeschultem Personal unsachgemäß eingesetzt und bedient werden.
In dieser Anleitung wird auf Restgefahren mit dem folgenden Symbol hingewiesen:

⚠ **Dieses Symbol weist darauf hin, dass bei Nichtbeachtung der Sicherheitshinweise Gefahren für Menschen bis zur schweren Körperverletzung oder Tod und/oder die Möglichkeit von Sachschäden besteht.**

2.5 Haftung

Eine Haftung ist für Sach- und Rechtsmängel dieser Dokumentation, insbesondere für deren Richtigkeit, Fehlerfreiheit, Freiheit von Schutz- und Urheberrechten Dritter, Vollständigkeit und/oder Verwendbarkeit – außer bei Vorsatz oder Arglist –ausgeschlossen.

2.6 CE-Konformität

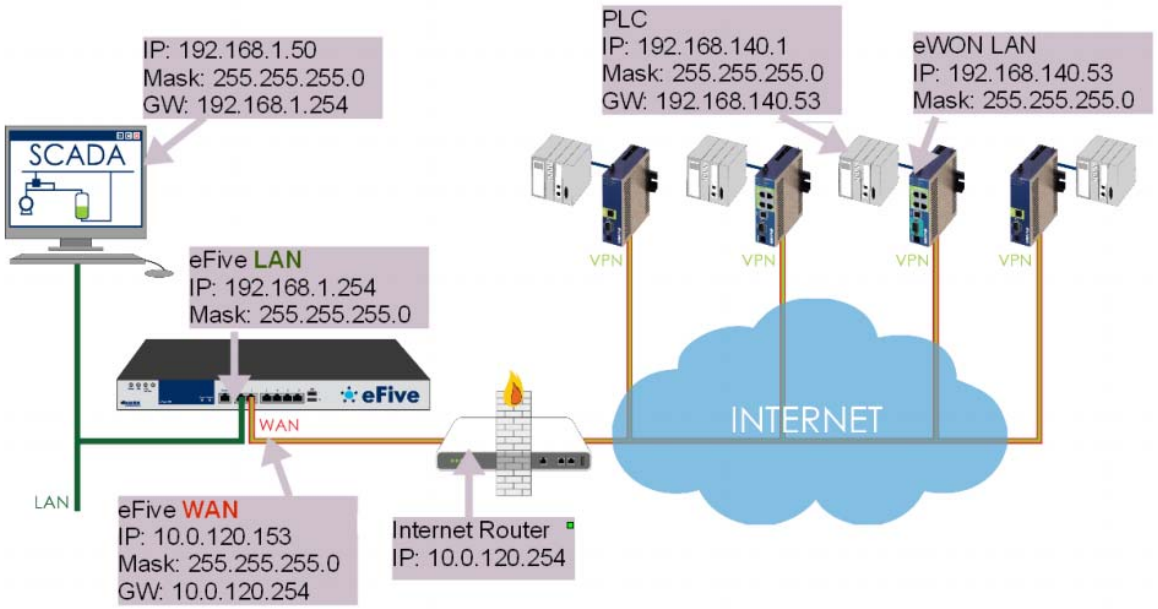
Die Konformitätserklärung liegt bei uns aus. Sie können diese gerne beziehen. Rufen Sie einfach an.

3 eFive 25

3.1 Über den Server

Der eFive ist eine kompakte, lüfterlose Hardwareplattform mit einem Virtual-Private-Network (VPN) Gateway mit OpenVPN-Verschlüsselung. Er wurde entwickelt, um mit den eWON-Routern eine optimale Verbindung zum Aufbau eines VPN-Netzwerkes herstellen zu können. Der eFive wirkt dabei als OpenVPN-Server, und die eWON-Router als OpenVPN Clients.
Der eFive 25 unterstützt bis zu 50 gleichzeitige VPN-Verbindungen. Für größere Netzwerke gibt es den eFive 100.

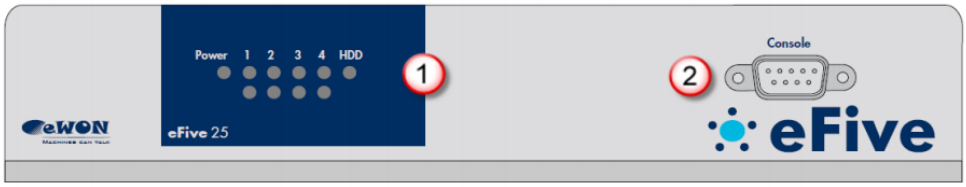
Ziel ist z. B. einen SCADA-PC mit den SPS-Geräten hinter dem eWON-Router zu verbinden. Der SCADA-PC ist Teil des LAN-Netzwerks des eFive und hat diesen als Standard Gateway. Wenn die VPN-Verbindung zwischen dem eWON-Router und dem eFive aufgebaut ist, leitet dieser die Anfragen aus dem SCADA zu dem Netzwerk hinter dem eWON. Ein Beispiel für diese typische Konfiguration wird im Bild unten angezeigt.
Weitere Aufbaubeispiele finden Sie im Kapitel 4.



3.2 Anschlussdarstellung

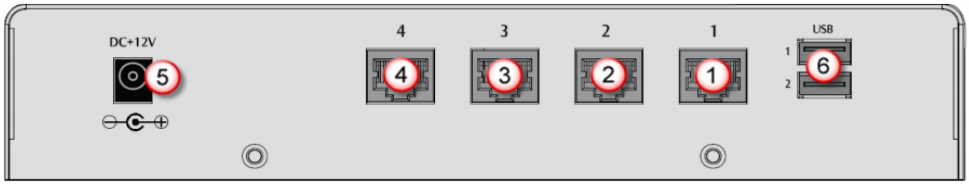
Im Folgenden sind die einzelnen Anschlüsse des Gerätes beschrieben.

Vorderseite



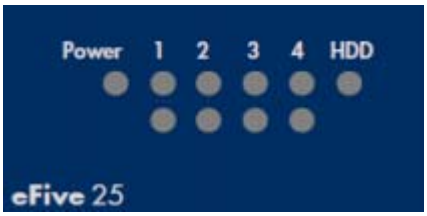
Nummer	Beschreibung
1	Status LED (Kapitel 3.2.1)
2	Serieller Anschluss für Konsolenanwendung (Kapitel 3.2.2)

Rückseite



Nummer	Beschreibung
1	Ethernet Port 1 – LAN (grün)
2	Ethernet Port 2 – WAN (rot)
3	Ethernet Port 3 – DMZ (orange)
4	Ethernet Port 4 – WLAN (blau)
5	Eingang Spannungsversorgung
6	USB Ports für Maus, Tastatur und USB-Stick zur Datensicherung

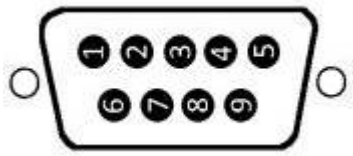
3.2.1 Status LEDs auf der Frontseite



Anzeige der LEDs	
Bezeichnung	Bedeutung
Power	Ein = Spannung vorhanden
1	LED für Ethernet Port 1 Obere LED Aus = 10 Mbps Grün = 100 Mbps Orange = 1000 Mbps Untere LED Aus = Keine Verbindung Gelb = Aktivität
2	LED für Ethernet Port 2 Bedeutung siehe LED 1
3	LED für Ethernet Port 3 Bedeutung siehe LED 1
4	LED für Ethernet Port 4 Bedeutung siehe LED 1
HDD	Ein = Aktivität auf der SSD

3.2.2 Serielle Schnittstelle

Die serielle Schnittstelle auf der Vorderseite dient für den SSH-Zugang. Damit kann u.A. der Server auf Werkseinstellung zurückgesetzt werden.



Anschlussbezeichnung Sub-D-9pol. Stecker	
Pin	RS232
1	-
2	RxD
3	TxD
4	-
5	GND
6	-
7	RTS
8	CTS
9	-

Netzwerke

eFive unterstützt vier verschiedene Arten von Netzwerken, die für jeweils verschiedene Sicherheitsstufen bzw. Zugriffswege gedacht sind.
Bei Werkseinstellung sind alle Kommunikationen zwischen den Netzwerken geblockt. Dies bedeutet, dass gezielt Firewall-Regeln freigeschaltet werden, wenn diese benötigt werden.

Folgend die Farben und Beschreibungen der vier Netzwerke:

Rot	WAN Dies ist das unsichere Netzwerk für den Internet-Anschluss am eFive. Hier kommen die VPN-Client Anfragen über das Internet rein.
Grün	LAN Dies ist das sichere Netzwerk für den lokalen Anschluss am eFive. Alle VPN-Verbindungen werden zu diesem Netzwerk geroutet.
Blau	WLAN Wird typischerweise für den einfachen Zugang in Richtung Internet genutzt. Hier kann z.B. ein WLAN-Access-Point angeschlossen werden.
Orange	DMZ (Demilitarized Zone) Dieses Netzwerk arbeitet mit mittlerem Sicherheitslevel um den Zugriff von Außen (Rot) und Innen (Grün) gleichermaßen zu erlauben.

Der Fokus des eFive liegt auf den beiden Netzwerken für WAN und LAN. Diese werden in erster Linie für den VPN Aufbau genutzt.

3.3 Allgemeine Aufbaurichtlinien

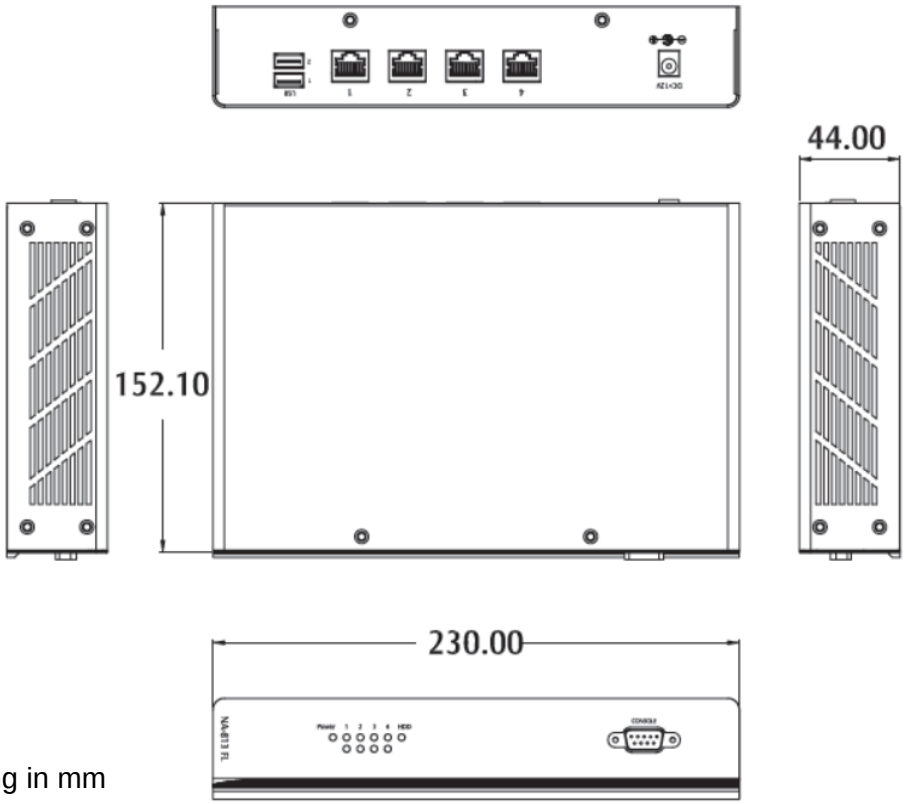
Das eFive wurde konzipiert für den Aufbau in einem geschlossen Raum.
Die Montagerichtung und die damit verbundenen zugelassenen Umgebungstemperaturen sind für den waagerechten Aufbau (0° Neigungswinkel) vorgesehen.
Folgende Freiräume sind erforderlich, um den eFive für eine ausreichende Eigenbelüftung einzubauen: 15 mm auf beiden Seiten; die Lüftungsschlitze müssen frei sein.

Die Lüftungsschlitze des Gehäuses dürfen nicht zugedeckt werden.

Das Gerät darf nur in Umgebungen der zugelassenen Schutzart verwendet werden. Beachten Sie sämtliche Sicherheitshinweise im Bezug auf Maschinen und Menschen.

Achtung! Das Gerät enthält ESD gefährdete Bauteile.

3.3.1 Abmessungen



Abmessung in mm

3.4 IP-Adressen

Mit folgenden IP-Adressen wird der eFive als Werkseinstellung ausgeliefert:

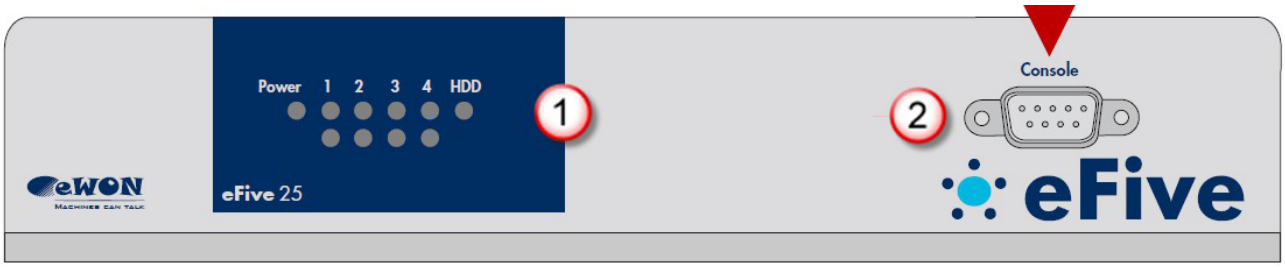
IP-Adressen	
Bezeichnung	Einstellung
LAN IP-Adresse	10.0.0.153
LAN Subnetzmaske	255.255.255.0
WAN IP-Adresse	Keine Festlegung
WAN Subnetzmaske	Keine Festlegung

3.5 Serieller Zugang zum eFive (Neustart, Reset)

Der eFive verfügt über eine serielle Schnittstelle, um sich mit der Konsole zu verbinden.
Dies ist dann sehr nützlich, wenn Sie die IP-Adresse oder das Kennwort des Servers vergessen haben.

Um diese Verbindung herzustellen, verwenden Sie das mitgelieferte serielle Kabel.

Verbinden Sie das Kabel mit dem eFive (2) und mit Ihrem seriellen Port Ihres PCs.

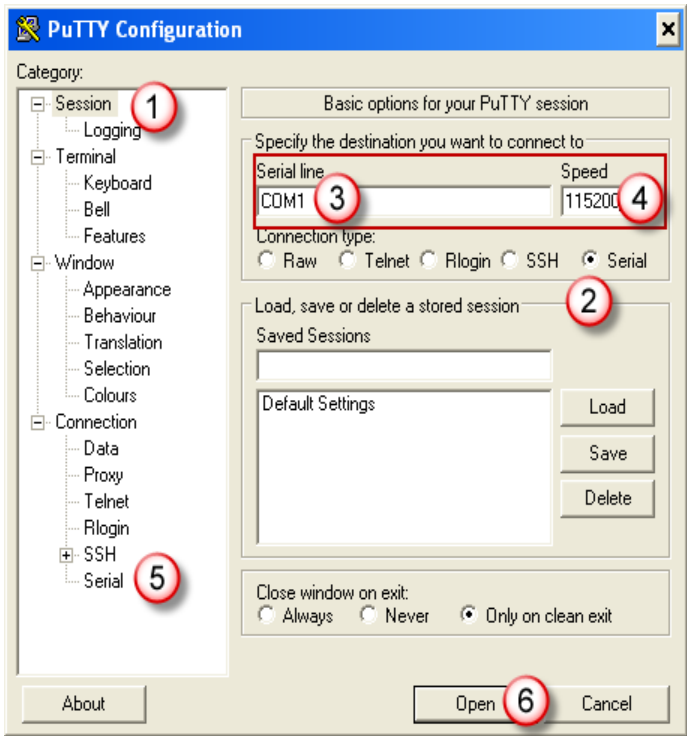


Auf Ihrem PC starten Sie nun ein Kommunikationsprogramm wie z.B. HyperTerminal oder PuTTY. Nehmen Sie nun die Einstellungen vor, um eine serielle Verbindung aufzubauen (2).

Beispiel:

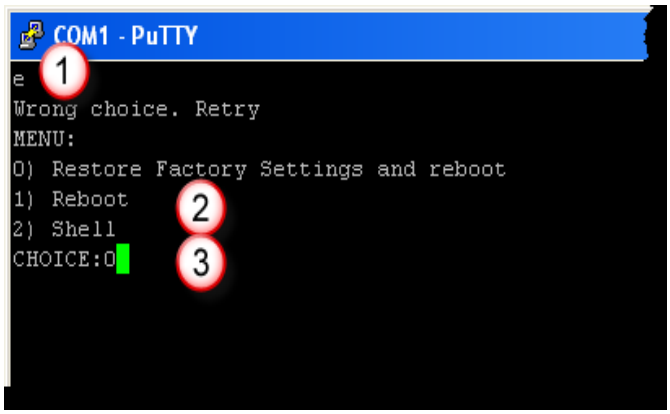
- COM-Port (3)
- Baudrate (hier 115200 bps) (4)
- Überprüfen Sie die seriellen Einstellungen: 8, n, 1; Flow Control: None (5)

- Klicken Sie nun auf Open (6)

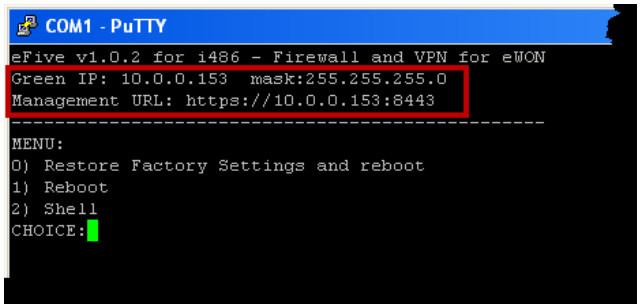


Geben Sie nun ein beliebiges Zeichen ein und drücken Enter (1). Der eFive kehrt nun ins Menü zurück (2).
Wählen Sie jetzt eine Option aus je nachdem was Sie machen wollen (3).

Um sich die aktuellen IP-Einstellungen anzeigen zu lassen, wählen Sie die 1-Reboot aus. Nach dem Neustart erscheinen die IP-Einstellungen des eFives als Überschrift in der Terminal-Schnittstelle.



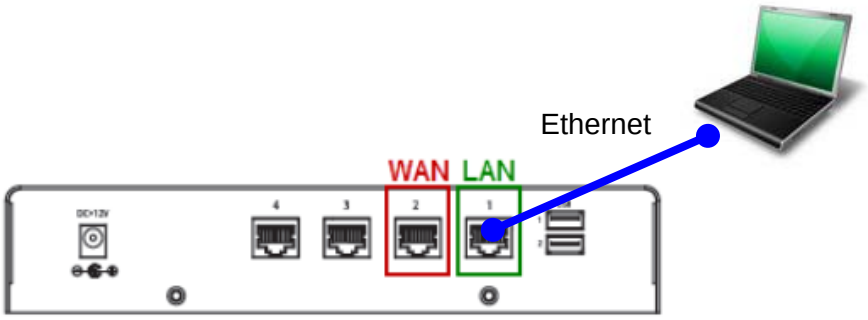
Um das Gerät in die Werkseinstellungen zurückzusetzen (IP-Adresse:10.0.0.153; Passwort: adm), geben Sie eine 0 ein und drücken Enter.
Warten Sie bis der Neustart abgeschlossen ist (dies kann einige Minuten dauern).



4 Konfiguration

4.1 Anschluss: PC und eFive

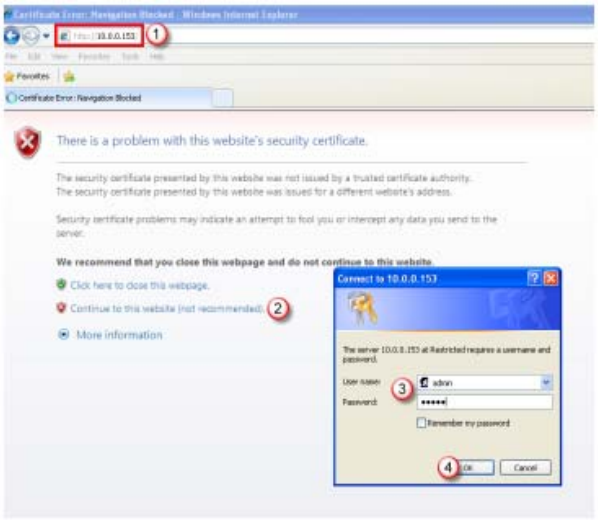
Um den eFive in Betrieb zu nehmen, müssen Sie es zunächst mit Ihrem PC/ Laptop verbinden. Grundsätzlich muss der PC mit der LAN-Schnittstelle des eFive verbunden werden.
Dafür benötigen Sie eine gekreuzte Ethernetleitung zwischen PC und eFive. Oder Sie nutzen einen externen Switch zwischen PC und eFive.



4.2 Webinterface öffnen

Damit Sie nun in die Konfigurationsoberfläche des eFive gelangen, öffnen Sie Ihren Browser und geben in der Adresszeile die IP-Adresse 10.0.0.153 des Servers ein.

Nun müssen Sie sich einloggen um in die Einstellungen zu gelangen. Bei Werkseinstellung sind Benutzername und Passwort „admin“. Übernehmen Sie die Eingabe mit **OK**.
Eine ggf. vorhandene Sicherheitsabfrage im Browser können Sie bestätigen.



Hinweis: Bitte ändern Sie auf jeden Fall das Standard Passwort!

Dazu gehen Sie in das Menü unter **System ➔ Passwords**.

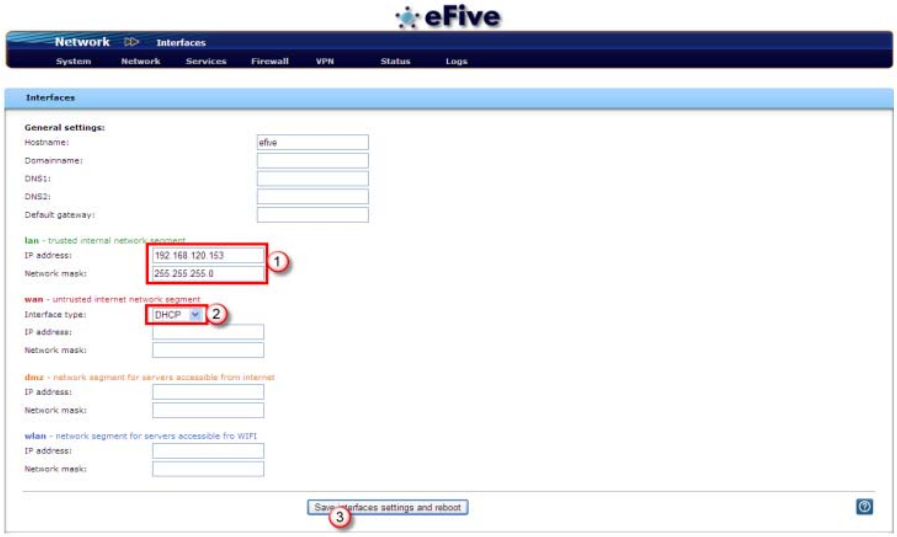
4.2.1 Startbildschirm

Als erstes wird Ihnen der Startbildschirm angezeigt.
Dieser enthält Informationen zu dem VPN-Server Status sowie den verbundenen VPN-Clients. Bei der Inbetriebnahme sind noch keine Geräte angezeigt.

4.2.2 IP-Adressen ändern

Stellen Sie die LAN und WAN IP-Adresse des eFive nach Bedarf um.

Dazu gehen Sie in das Menü unter **Network ➔ Interfaces**.
Hier können Sie nun die IP-Adressen der LAN- und WAN-Schnittstellen anpassen. Betätigen Sie nach Abschluss den Button **Save interfaces settings and reboot.**



4.2.3 Updates

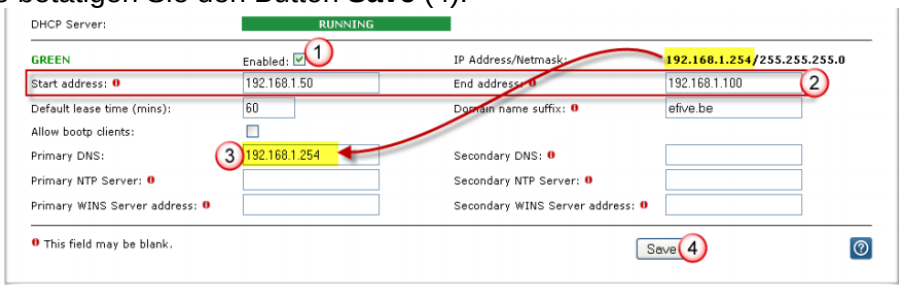
In unregelmäßigen Abständen werden Firmwareupdates zur Verfügung gestellt.
Diese können kostenlos auf den eFive geladen werden.
Dazu gehen Sie in das Menü unter **System ➔ Updates**.

Hier können Sie, eine bestehende Internet-Verbindung vorausgesetzt, sich Updates laden.
Betätigen Sie dazu den Button **Refresh update list** (1), um sich anzuschauen ob neue Updates vorhanden sind. Wurde eines gefunden (2), können Sie es sich direkt hier laden (3).

Nachdem das Update geladen wurde, können Sie es installieren (4). Die vorhandene Konfiguration bleibt dabei erhalten.

4.2.4 eFive als DHCP-Server im LAN

Wenn Sie den eFive als DHCP-Server für angeschlossene LAN-Geräte nutzen wollen, müssen Sie diesen einschalten.
Dazu gehen Sie in das Menü unter **Services ➔ DHCP Server.**
Schalten Sie zunächst den Server ein (1). Stellen Sie die Anfangs- und Endadresse für den DHCP-Bereich ein (2). Der Primäre DNS muss mit der LAN-IP des eFive identisch sein (3).
Zur Übernahme betätigen Sie den Button **Save** (4).



4.2.5 VPN-Netzwerk aufbauen

Weitere Informationen und Beispielanwendungen zu VPN-Netzwerken finden Sie in unseren Technical Notes.

5 Beispielaufbauten

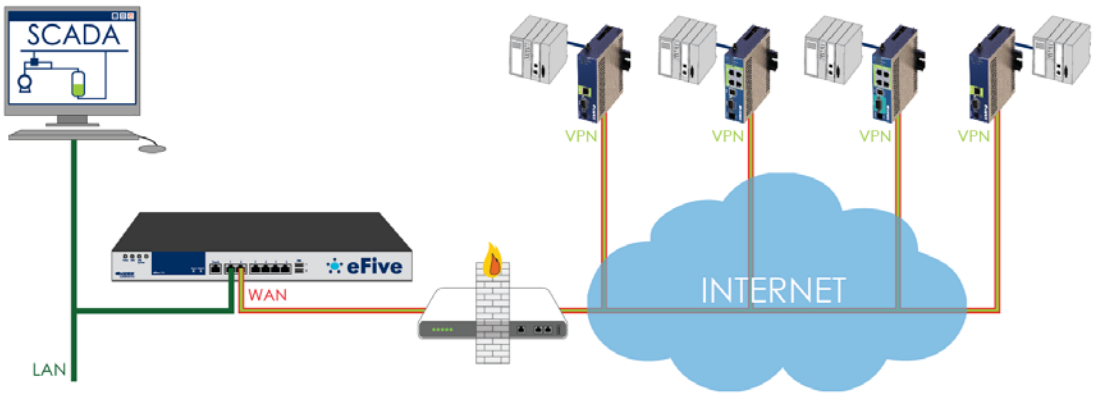
Hier finden Sie Beispiele, wie der eFive genutzt werden kann.

5.1 eFive als Firewall + VPN-Server

In diesem Beispiel dient der eFive als Firewall für den Firmenschutz sowie als VPN-Server.

Benötigt werden hier ein DSL-Router sowie eine fixe IP-Adresse am DSL-Anschluß.

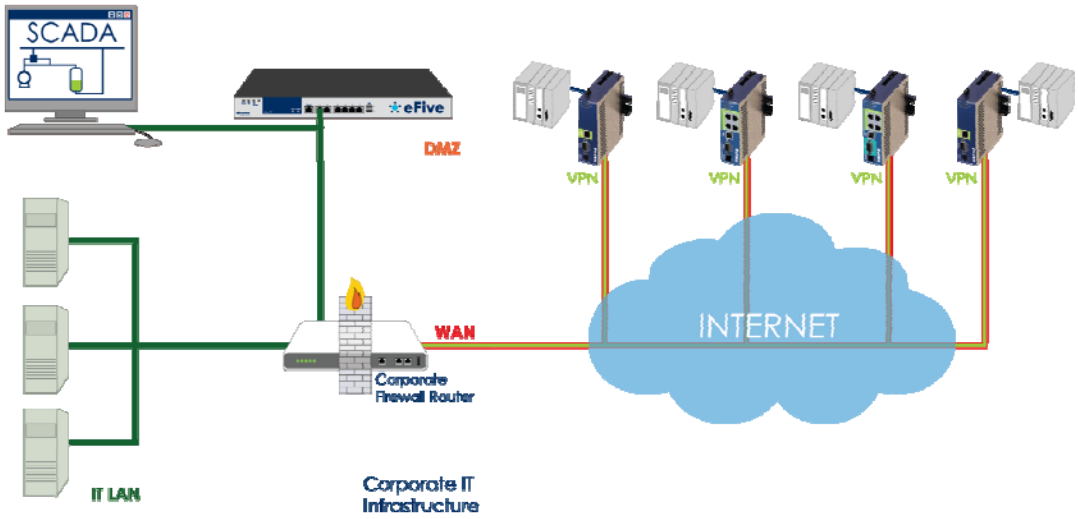
Hinweis: Bitte unternehmen Sie im Vorfeld eine Risikoabschätzung bzgl. Virenschutz u.ä., wenn Sie den eFive als alleinigen Schutz nehmen möchten!



5.2 eFive als VPN-Server in DMZ

In diesem Beispiel dient der eFive rein als VPN-Server.

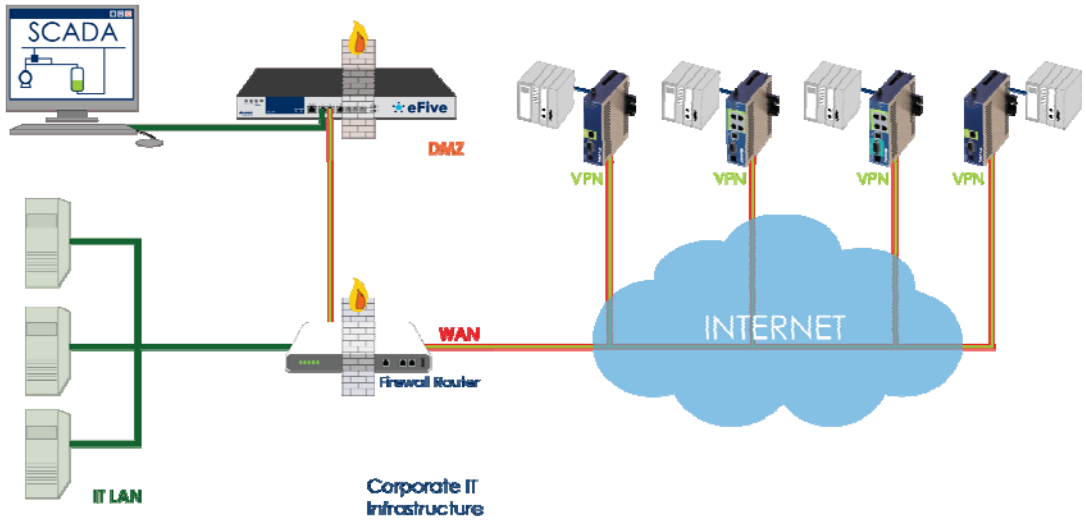
Benötigt werden hier eine Firmenfirewall mit Portweiterleitung sowie eine fixe IP-Adresse am DSL-Anschluß.



5.3 eFive als Firewall + VPN-Server in DMZ

In diesem Beispiel dient der eFive als Firewall für den SCADA-Schutz sowie als VPN-Server.

Benötigt werden hier eine Firmenfirewall mit Portweiterleitung sowie eine fixe IP-Adresse am DSL-Anschluß.



6 Copyright

Dieses Dokument ist Eigentum der Fa. Wachendorff Prozesstechnik GmbH & Co.KG. Das Kopieren und die Vervielfältigung sind ohne vorherige Genehmigung verboten. Inhalte der vorliegenden Dokumentation beziehen sich auf das dort beschriebene Gerät.

6.1 Haftungsausschluß

Alle technischen Inhalte innerhalb dieses Dokuments können ohne vorherige Benachrichtigung modifiziert werden. Der Inhalt des Dokuments ist Inhalt einer wiederkehrenden Revision.
Bei Verlusten durch Feuer, Erdbeben, Eingriffe durch Dritte oder anderen Unfällen, oder bei absichtlichem oder versehentlichem Missbrauch oder falscher Verwendung, oder Verwendung unter unnormalen Bedingungen werden Reparaturen dem Benutzer in Rechnung gestellt. Wachendorff Prozesstechnik ist nicht haftbar für versehentlichen Verlust durch Verwendung oder Nichtverwendung dieses Produkts, wie etwa Verlust von Geschäftserträgen.
Wachendorff Prozesstechnik haftet nicht für Folgen einer sachwidrigen Verwendung.

7 Sonstige Bestimmungen und Standards

CE Erklärung

Dieses Gerät wurde getestet und entspricht folgenden Anforderungen:
EMC Directive 2004/180/EC
Low Voltage Directive 2006/95/EC

WEEE Informationen

Entsorgung von alten Elektro- und Elektronikgeräten (gültig in der Europäischen Union und anderen europäischen Ländern mit separatem Sammelsystem)
Dieses Symbol auf dem Produkt oder auf der Verpackung bedeutet, dass dieses Produkt nicht wie HausmüIl behandelt werden darf. Stattdessen soll dieses Produkt zu dem geeigneten Entsorgungspunkt zum Recyceln von Elektro- und Elektronikgeräten gebracht werden. Wird das Produkt korrekt entsorgt, helfen Sie mit, negativen Umwelteinflüssen und Gesundheitsschäden vorzubeugen, die durch unsachgemäße Entsorgung verursacht werden könnten. Das Recycling von Material wird unsere Naturressourcen erhalten. Für nähere Informationen über das Recyceln dieses Produktes kontaktieren Sie bitte Ihr lokales Bürgerbüro, Ihren Hausmüll Abholservice oder das Geschäft, in dem Sie dieses Produkt gekauft haben.

8 Kundenservice und Technischer Support

Bei technischen Fragen erreichen Sie uns unter:

WACHENDORFF
Prozesstechnik GmbH & Co. KG

Industriestraße 7 • 65366 Geisenheim
Tel.: +49 6722 9966966
Fax: +49 6722 996578
E-Mail: eea@wachendorff-prozesstechnik.de
Homepage: www.wachendorff-prozesstechnik.de