

VS-Wall

Firewall-Plattform mit vorkonfigurierter IPCop Firewall Software

Bedienungshinweise

Version 04

Inhaltsverzeichnis

1 Überblick.....	2
2 Hardware und Software - Features.....	2
2.1 Hinweise zur Hardware.....	2
2.2 Software.....	2
3 Vorkonfiguration der VS-Wall.....	3
4 Ändern der Firewallkonfiguration.....	4
4.1 Grundlegende Einstellungen.....	5
4.2 Administration der VS-Wall.....	6
4.3 Beschreibung einiger Konfigurationsmöglichkeiten.....	7
4.3.1 Dienste - Proxy-Server.....	7
4.3.2 Firewall – Verbindungen.....	7
4.3.3 Firewall – Externer Zugang.....	8
4.3.4 VPN - OpenVPN.....	8
5 Weitere Fähigkeiten: die IPCop AddOns.....	8
6 Anhang.....	9
6.1 Anhang: Betrieb der VS-Wall mit CompactFlash-Karte.....	9
6.1.1 Sichern eines CompactFlash-Images.....	9
6.1.2 Wiederherstellen eines CompactFlash-Images.....	9
6.2 Anhang: Weitere Tipps für die Konfiguration der VS-Wall.....	10
6.3 Anhang: FAQ.....	11
6.4 Anhang: Technische Daten.....	11
6.4.1 VS-Wall 5620.....	11
6.4.2 VS-Wall 9927.....	12
6.4.3 VS-Wall 860A.....	12

1 Überblick

Mit der **VS-Wall** erhalten Sie einen Firewall-Router, der die freie spezialisierte Linux-Firewall-Distribution IPCop auf einem Embedded Industrial PC ausführt. IPCop ist bereits auf der CompactFlash-Karte installiert und zum direkten Betrieb vorkonfiguriert. Die Anpassung an die individuellen Gegebenheiten muss natürlich der Benutzer selbst ausführen, was aber durch das Webkonfigurations-tool von IPCop sehr einfach ist.

In diesem Dokument finden Sie die Beschreibung der besonderen Anpassung von IPCop für die VS-Wall und einige Bedienungshinweise für die ersten Schritte. **Dieses Dokument ist kein Handbuch für IPCop!** Ein solches können Sie, so wie die neuesten Versionen von IPCop, auf den entsprechenden Internetseiten finden, z.B. unter www.ipcop-forum.de.

Lesen Sie bitte auch diese **Einschränkung der Haftung!**

Die mit der VS-Wall angebotene und dort vorkonfigurierte Software IPCop ist freie, unter der GPL stehende Software (die genauen Bedingungen finden Sie unter <http://www.gnu.org/licenses/fdl.html#SEC1>).

Für die mit der VS-Wall zur Verfügung gestellte Software IPCop und die eventuell mit installierten AddOns (siehe unten) kann VS Vision Systems keinerlei Garantie leisten. VS Vision Systems schließt jegliche Haftung für Schäden aus, die unmittelbar oder mittelbar durch den Gebrauch der Software entstanden sind.

2 Hardware und Software - Features

In diesem Abschnitt werden nur die wichtigsten Features der VS-Wall aufgeführt. Detailliertere Informationen findet man in den speziellen Dokumentationen auf beiliegender CD.

Für die Hardware:

- Technische Daten zur VS-Wall in Abschnitt [6.4. "Anhang: Technische Daten"](#)
- Manual zur Hardware-Plattform: z.B. [M5620.pdf](#) oder ähnlich.

Für die Software in den Handbüchern zu IPCop unter www.ipcop-forum.de oder auf CD:

- [IPCop-Installationshandbuch](#)
- [IPCop-Administrationshandbuch](#)

sowie an vielen Orten im Internet.

2.1 Hinweise zur Hardware

Hinweis VS-Wall 9927: Um bei Tests oder Installation die VS-Wall 9927 direkt mit Monitor und Keyboard zu steuern, muss der Monitor über den Pfostenstecker auf der Platine angeschlossen werden. Dazu muss man das Gehäuse öffnen (siehe auf CD [9927b101.pdf](#)) und es wird das Monitor-Adapterkabel benötigt. Die Tastatur wird über USB angeschlossen.

Hinweis VS-Wall 9927: Eventuell ist ein BIOS-Passwort voreingestellt: das heißt `PASSWORD`.

2.2 Software

Als Firewall-Software verwendet die VS-Wall eine Implementation der freien Linux-Distribution IP-Cop (<http://www.ipcop.org> oder www.ipcop-forum.de), die fertig auf einer 256MB CompactFlash vorinstalliert ist.

IPCop erschließt die besonderen Firewall-Fähigkeiten von Linux (iptables, ipchains, usw.) über eine sehr benutzerfreundliche Weboberfläche, so dass die Administration der VS-Wall vollständig über den Browser von Computern im lokalen Netzwerk erfolgt (es ist auch ein externer Zugang über Internet möglich).

IPCop Features

- Optionaler DHCP Client, der es IPCop erlaubt, seine IP-Adresse vom ISP zu bekommen
- DHCP Server für die Konfiguration der PC's im internen Netzwerk
- Caching DNS Proxy, um Internet Namensanfragen zu beschleunigen
- Proxyserver für Webseiten, um den Internet Webzugriff zu beschleunigen
- Intrusion-Detection („Einbruchsmelder“) um Attacken auf das Netzwerk von ausserhalb zu erkennen
- Möglichkeit, das Netzwerk in Zonen aufzuteilen.
- VPN Unterstützung (unterstützt auch x509 Zertifikate oder OpenVPN)
- Traffic shaping, um den Internetdiensten unterschiedliche Prioritäten zuzuweisen
- Von Beginn an mit der Prämisse entwickelt, Stack-Attacken auf Applikationen zu verhindern.

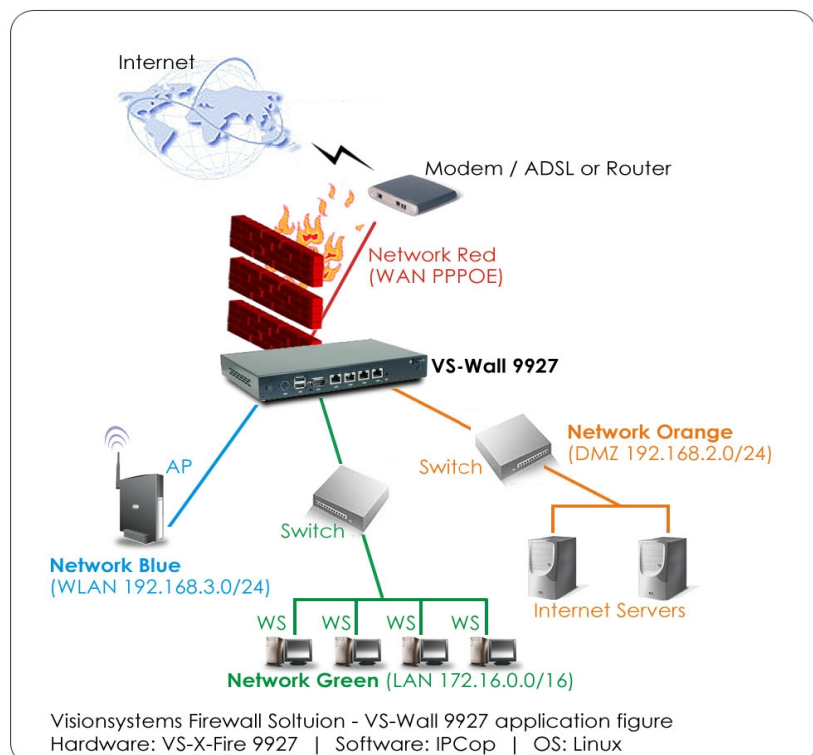
3 Vorkonfiguration der VS-Wall

Die VS-Wall hat drei oder vier physikalisch getrennte Netzwerkschnittstellen.

Jede von Ihnen hat eine bestimmte Konfiguration und individuelle Funktion im Netzwerk. Sie werden mit

- GREEN,
- BLUE,
- ORANGE
- und RED

bezeichnet. Die Abbildung rechts zeigt eine typische Konfiguration.



IPCop auf der VS-Wall ist vorkonfiguriert, um die Einbindung in das bestehende Netzwerk möglichst einfach zu machen. Die Konfiguration lässt sich durch das Setup-Tool von IPCop verändert werden (siehe unten Abschnitt [4.1 "Grundlegende Einstellungen"](#)).

	GREEN	BLUE	ORANGE	RED
	Schnittstelle zum lokalen sicheren Netz (LAN) <i>Administrations-PC, lokale Switches und lokale PCs</i>	Schnittstelle zum Wireless Netz (WLAN) <i>z.B. Access Point</i>	Schnittstelle zur demilitarisierten Zone (DMZ) <i>Betrieb öffentlicher, vom Internet erreichbarer Server</i>	Schnittstelle zum unsicheren Internet (WAN) <i>Verbindung zum ISP, oder anderes unsicheres Netz</i>
IP Cop				
	192.168.0.1/24 DHCP-Server aktiviert /dev/eth0	192.168.21.1/24 DHCP-Server nicht aktiviert /dev/eth1	192.168.11.1/24 kein DHCP-Server /dev/eth2	auto IP (DHCP) /dev/eth3
VS-Wall 5620				
	LAN 6 (GigaLAN) Verwendung der Ports LAN 4 und LAN 5 nicht fest gelegt.	LAN 1	LAN 2	LAN 3
VS-Wall 9927				
	LAN 1	LAN 2	LAN 3	LAN 4
VS-Wall 860A				
Standard:	LAN 1	nicht vorhanden*	LAN 2	LAN 3
	*Nur 3 LAN-Ports vorhanden. Durch opt. USB-LAN-Adapter kann auch BLUE verwendet werden.			
Alternative:	LAN 1	LAN 2	LAN 3	Modem (z.B USB)

Hinweis: Die Verbindung zum Internet über RED kann auch ganz anders konfiguriert werden: über statische IP (dabei ist interessant, dass mehrere IP-Adressen als Aliase möglich sind), über PPP (Modem), PPPoE (ADSL) oder PPTP (Kabelmodem). Siehe dazu den Abschnitt [5 "Grundlegende Einstellungen"](#).

Hinweis: Das Sicherheitsmodell von IPCop vertraut den Computern auf GREEN ohne Einschränkungen, egal ob die Anfragen von einem Benutzer oder etwa von Viren, Trojanern oder anderer Schadsoftware stammen. Alle werden gleichberechtigt behandelt und von IPCop zugelassen. Für jeden Netzwerkbereich kann allerdings die Einbruchdetektierung (Intrusion detection) eingeschaltet werden. Mit Hilfe des AddOns „BlockOutgoingTraffic“ (siehe Abschnitt [5. "Weitere Fähigkeiten: die IPCop AddOns"](#)) können auch die von GREEN eingehenden Anfragen eingeschränkt werden.

4 Ändern der Firewallkonfiguration

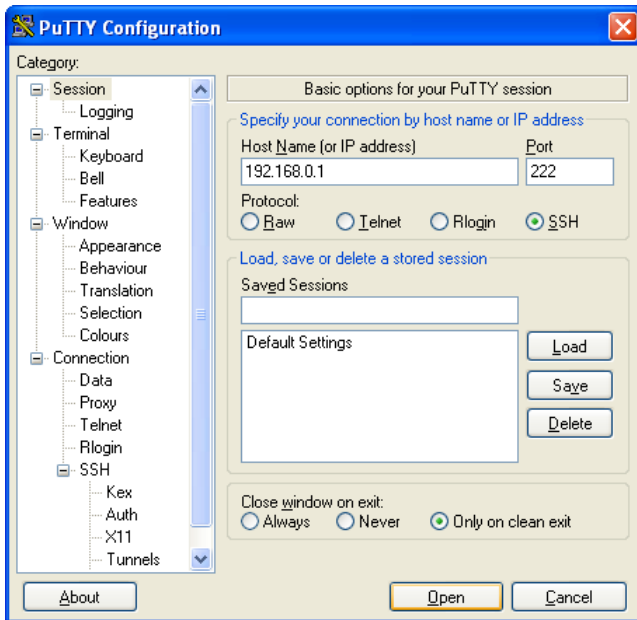
Um die Konfiguration der VS-Wall einzustellen, benötigt man einen Computer im lokalen Netz (GREEN). Dieser Computer erhält die richtige IP-Adresse über den DHCP-Server der VS-Wall. Zur Einstellung der VS-Wall gibt es zwei verschiedene Wege:

Den **IPCop Web-Server**: hier geschieht die normale Administration. Man verbindet sich mit einem Browser auf die grüne Schnittstelle auf Port 445 (<https://192.168.0.1:445>).

Die **IPCop Linux Konsole**: man verbindet sich mittels SSH (z.B. von Windows aus mit dem Tool PuTTY) auf den Port 222 (z.B. ssh 192.168.0.1 -port 222).

4.1 Grundlegende Einstellungen

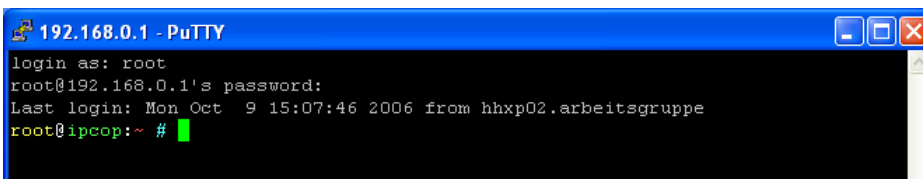
Um die grundlegenden Einstellungen von IPCop zu verändern, muss man sich aus dem lokalen Netz (GREEN) per SSH auf die VS-Wall verbinden (Port 222). Dann ruft man das IPCop Installationsstool über `setup` auf, um die grundlegenden Einstellungen wie die Netzwerkkonfiguration oder die Schnittstellenadressen zu verändern.



Wählen Sie sich über SSH auf 192.168.0.1 Port 222 (!) ein:

(Beispielanwendung Putty:

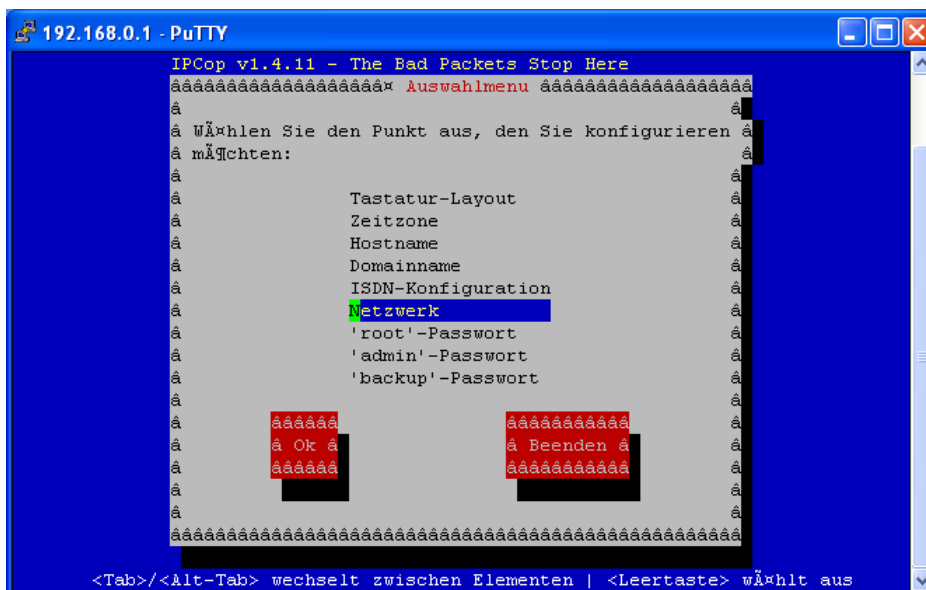
Geben Sie nur die Host IP-Adresse an und den Port ein. Mit dem Button „Open“ die Verbindung herstellen.)



Login as: **root**

Password: **vision**

Sie haben sich somit zum ersten Mal auf ihrem X-Fire eingewählt. Geben Sie `setup` ein und konfigurieren Sie Ihr Netzwerk nach Ihren Bedürfnissen.



Hinweis: Das 'root'-Passwort ist brauchen Sie für die Einwahl mit SSH und grundlegende Einstellungen von der Linux-Konsole über das Setup-Tool (siehe oben). Das 'admin'-Passwort wird für den Zugriff auf das WebGUI von IPCop benötigt (siehe unten), das 'backup'-Passwort für Sicherung und Wiederherstellung der IPCop-Einstellungen.

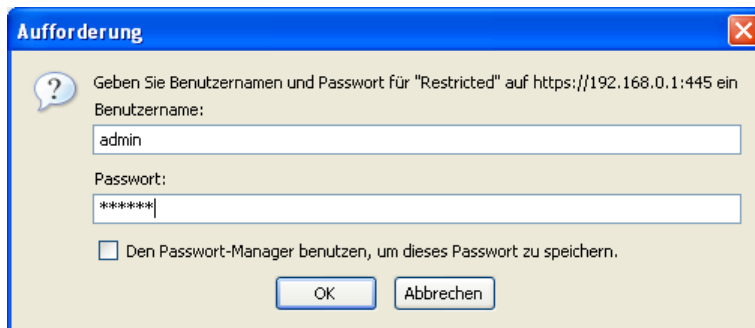
Hinweis: Wie üblich sollten Sie alle drei Passwörter sobald wie möglich geändert werden.

Hinweis: Detaillierte Beschreibung zum Setup im [IPCop-Installationshandbuch](#).

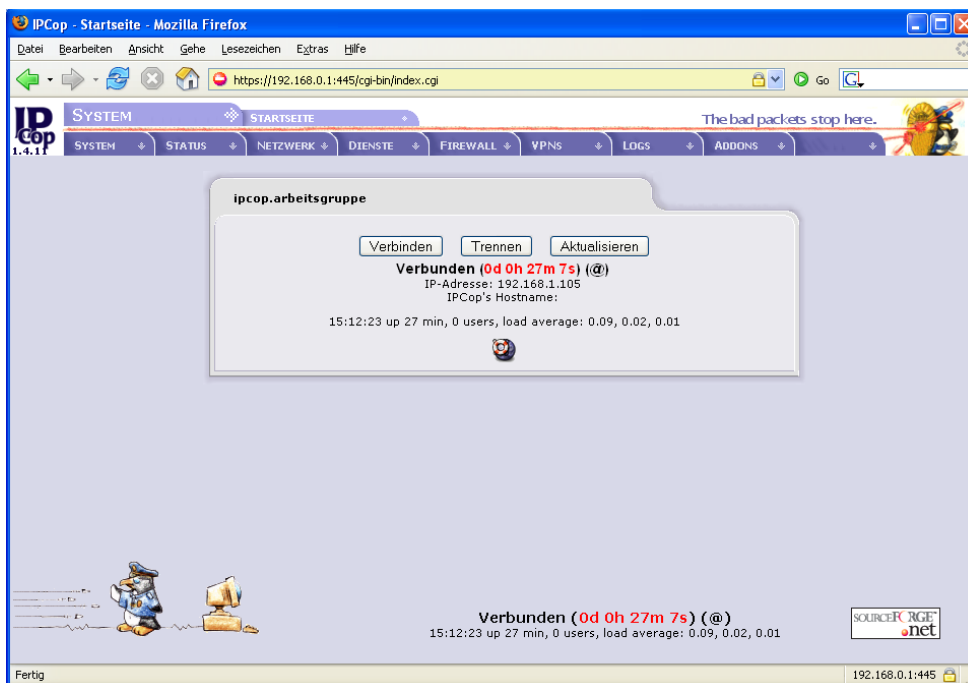
4.2 Administration der VS-Wall

Die Administration der VS-Wall geschieht über einen Browser auf einem Computer im lokalen Netz, der sich auf die grüne Schnittstelle der VS-Wall auf Port 445 verbindet (<https://192.168.0.1:445>).

Achten Sie darauf, dass Sie keine Proxy Einstellungen benutzen!



Melden Sie sich mit Benutzernamen **admin** und Passwort **vision** an (falls Sie kein anderes gesetzt haben).



dann können Sie auf die Web-Oberfläche der Firewall zugreifen.

Die folgende Tabelle zeigt die Einstellmöglichkeiten über das Menü der Web-Oberfläche:

Inhalt des Webkonfigurationstool	
System	Passwörter, Neustart-Zeitplan, SSH Zugriff, Updates
Status	System und Netzwerk Anzeigen und Diagramme
Netzwerk	Einwahl über Modem
Dienste	Proxy, DHCP, DNS, NTP und TrafficShaping
Firewall	Port Weiterleitung, DMZ Pinholes
VPNs	Virtuelle Private Netzwerke – auch OpenVPN
Logs	Einstellung und Ansicht der Logs

Hinweis: Detailliertes Manual: [IPCop-Administrationshandbuch](#).

Bei der Anpassung der Konfiguration von IPCop für die VS-Wall wurden fast alle Defaulteinstellungen übernommen. Der Benutzer muss also mit dem Webkonfigurationstool weitere Regeln und Eigenschaften hinzufügen.

Die Konfiguration der VS-Wall unterscheidet sich von den IPCop Defaults an drei Stellen:

- Aktivierung des SSH Zugangs von GREEN über Port 222
- Aktivierung des DHCP-Servers auf GREEN (voreingestellter Adressbereich für dynamische Zuordnungen: 192.168.0.100 – 192.168.0.199)
- Verkleinerung der Logs auf 7 Tage
(siehe dazu Abschnitt [6.1."Anhang: Betrieb der VS-Wall mit CompactFlash-Karte"](#))

4.3 Beschreibung einiger Konfigurationsmöglichkeiten

Im Folgenden werden einige Konfigurationsmöglichkeiten kurz erklärt. Eine detaillierte Beschreibung aller Möglichkeiten findet man in dem [Administrationshandbuch von IPCop](#).

4.3.1 Dienste - Proxy-Server

Der Betrieb eines Proxy-Servers auf der VS-Wall ist zwar im Prinzip möglich und unter IPCop sehr einfach einzurichten – allerdings in der Kombination mit einer CompactFlash nicht sinnvoll (siehe dazu auch Abschnitt [6.1. "Anhang: Betrieb der VS-Wall mit CompactFlash-Karte"](#)). Falls ein Proxy-Server auf der VS-Wall dem lokalen Netz angeboten werden soll, ist es erforderlich die CompactFlash-Karte durch eine 2,5“-Festplatte zu ersetzen.

4.3.2 Firewall – Verbindungen

Die wichtigste Fähigkeit einer Firewall ist die Weiterleitung bzw. Unterdrückung von Datenpaketen auf der Grundlage von Filterregeln. Auf der VS-Wall sind keine Filterregeln vorgegeben weil diese auf die Bedingungen der individuellen Netzwerkkonfiguration angepasst werden müssen.

Grundsätzlich werden Anfragen aus dem lokalen Netzwerk GREEN uneingeschränkt angenommen, Anfragen aus den anderen Netzen (BLUE, ORANGE/DMZ und RED/Internet) wird dagegen nicht vertraut, sie werden nicht angenommen. Diese Einschränkungen können zurückgenommen werden, z.B. durch das Einrichten von sogenannten „Schlupflöchern“ (Pinholes).

Durch das IPCop-AddOn „BlockOutgoingTraffic“ (blockouttraffic.de) lässt sich auch der Zugriff von GREEN aus einschränken. „Diese AddOn blockiert die Verbindungen, die in einer normalen IPCop Installation erlaubt sind. Über die komfortable und intuitive GUI ist es möglich, eigene Regeln zu erstellen, die eine bessere Kontrolle der Verbindungen zum und durch den IPCop ermöglichen.“ - sehr zu empfehlen!

4.3.3 Firewall – Externer Zugang

Für eine IPCop-Firewall lässt sich auch ein externer Zugang konfigurieren, so dass über RED auf den IPCop und sein Webkonfigurationstool zugegriffen werden kann. Dadurch ist Fernwartung von einem Computer möglich, der nicht notwendigerweise im lokalen Netz GREEN steht.

Durch einen externen Zugang wird aber auch die Sicherheit beeinträchtigt. Er ist deshalb nicht per Default aktiviert.

4.3.4 VPN - OpenVPN

Die Verbindung eines entfernten Computers („RoadWarrior“) oder Netze in ein lokales Netz über einen sicheren VPN-Tunnel gehört zu den verbreiteten Anwendungen einer Firewall. So können auch mit der VS-Wall und IPCop VPN-Verbindungen eingerichtet werden, deren Anzahl nur durch die Leistungsfähigkeit der Hardware beschränkt ist.

Durch Installation des AddOns [ZERINA for IPCop](#) – VPN, easy as 1, 2, 3 – kann die Unterstützung für OpenVPN in IPCop integriert werden, ebenfalls eingebunden in das Web GUI.

5 Weitere Fähigkeiten: die IPCop AddOns

IPCop lässt sich über „AddOns“ erweitern, wie oben schon zweimal erwähnt ist, z.B. durch das AddOn „BlockOutgoingTraffic“ mit dem der Zugriffs vom lokalen Netz GREEN aus kontrolliert werden kann.

Die wichtigsten AddOns werden von den IPCop-Gemeinde geprüft und sind unter www.ipcop.org - [IPCop AddOns](#) gelistet. Auch unter www.ipcop-forum.de/links.php sind viele Erweiterungsmöglichkeiten, ihre Anwendung und Konfiguration zu finden.

Eine Kopie der aktuellen ipcop.org-Liste...

- Internet Seiten Filtern mit [squidGuard](#). Einfaches Installationsmanagement mit Ipcop 1.4. Übersetzt in Französisch, Deutsch, Holländisch, Russisch, Portugisisch und Englisch. Schaut hier: <http://franck78.ath.cx>
- **Addon Server** für IPCop <http://firewalladdons.sourceforge.net/> hat ein grosses Sortiment an Modifikationen, die man zu IPCop hinzufügen kann, so wie [DansGuardian](#).
- www.ipadd.de -**Addon-Binaries** und auf PCop bezogene Links
- www.urlfilter.net - **URL filter** mit nahtloser GUI Integration und einer zeitbasierten Zugriffskontrolle.
- www.advproxy.net - **Advanced Proxy** mit verschiedenen Methoden der Benutzerauthentifizierung und anderen vielseitigen und nützlichen zusätzlichen Features.
- IPCop V1.4 **Banish** - Blockieren Sie Zugang durch IP, CDIR, Gebiet und MAC address. <http://banish.sidsolutions.net>
- blockouttraffic.de - **BlockOutTraffic (BOT)** blockiert die Verbindungen, die in einer normalen IPCop Installation erlaubt sind. Über die komfortable und intuitive GUI ist es

möglich, eigene Regeln zu erstellen, die eine bessere Kontrolle der Verbindungen zum und durch den IPCop ermöglichen.

- www.ipcop.h-loit.de - **IPCop Addons** wie z.B. UPS Server, GUIPorts, Who IS Online.
- www.supporting-role.net - Supporting Role Inoffizielle IPCop Modifikationen.
- www.ban-solms.de - **IPCop Addons** Connection Scheduler, HDDGraph, mbmongraph, Wake On LAN, COM LED, GUI Colors etc.
- www.advproxy.net/update-accelerator - der **Update Accelerator** speichert Software-Updates lokal zwischen und liefert sie mit voller LAN-Geschwindigkeit aus - sogar komplette Service Packs.
- www.sischmitz.de - **IPCop Addons** RAMCop, ADDPartition

6 Anhang

6.1 Anhang: Betrieb der VS-Wall mit CompactFlash-Karte

Idealerweise kommt die Hardwareplattform einer Firewall gänzlich ohne bewegliche Teile aus. Dies ist bei der VS-Wall durch ihre lüfterlose Hardware gegeben – deshalb sollte auch eine CompactFlash-Karte als Speichermedium gewählt werden. Allerdings ist die Anzahl der Schreibzugriffe auf die Speicherzellen einer CompactFlash-Karte beschränkt (je nach Produktqualität ca. 10.000 bis 100.000 Schreibzugriffe).

Um die Lebensdauer so gut wie möglich zu verbessern, ist auf der VS-Wall eine besonders angepasste CompactFlash-Installation von IPCop eingerichtet. Dabei werden einerseits regelmäßig beschriebene Dateien wie die Logs auf einer RamDisk gespeichert und nur in größeren Abständen in komprimierter Form auf der CompactFlash-Karte gesichert. Darüber hinaus werden die gesicherten Dateien regelmäßig auf dem Medium rotiert, so dass alle Speicherzellen gleichmäßig belastet werden.

Es ist aber nicht ratsam, auf einem solchen System einen Proxy-Server zu betreiben, der sehr intensiv Dateien zwischenspeichern muss. Falls diese Funktion gewünscht wird, sollte unbedingt eine 2,5“-Harddisk verwendet werden. Besser noch wird die Funktion auf einen Server in der DMZ ausgelagert – so verbessert sich auch die Leistungsfähigkeit der VS-Wall.

6.1.1 Sichern eines CompactFlash-Images

Schrauben Sie den ausgeschalteten X-Fire auf der Unterseite auf (3 Kreuzschrauben) und entnehmen Sie vorsichtig die Compact Flash-Karte. Erstellen Sie ein binäres Image dieser Karte auf einem PC der CompactFlash-Karten lesen kann und speichern Sie diese Datei.

R-Linux http://www.data-recovery-software.net/Linux_Recovery_Download.shtml
Anleitung: <http://www.pSIONwelt.de/workshop/cfmws/index.html>

6.1.2 Wiederherstellen eines CompactFlash-Images

Schrauben Sie den ausgeschalteten X-Fire auf der Unterseite auf (3 Kreuzschrauben) und entnehmen Sie vorsichtig die Compact Flash-Karte. Laden Sie entweder die Grundkonfiguration, die Sie auf unserer CD finden, oder ein selbst erstelltes Image von ihrem PC aus auf ihre Karte.

Hinweis: Achten Sie darauf, dass die Größe (256MB) der CompactFlash-Karte stimmt!

6.2 Anhang: Weitere Tipps für die Konfiguration der VS-Wall

Addon „BlockOutgoingTraffic“ – Zugriffsregeln

Web-Interface ► Firewall ► BlockOutgoingTraffic

-Für einen Administrator alleine:

- „Einstellungen“
- „BOT ausschalten“
- „Bearbeiten“
- „Admin MAC“ **Achtung schliessen Sie sich nicht selbst aus!!**
- „IPCop Zugriff“s Regel deaktivieren
- „BOT einschalten“

-Für mehrere Administratoren

- In aktuellen Regeln „IPCop Zugriff“ bearbeiten.
(Voreinstellung alle im grünen Netz erlaubt)

IP Adresse ändern

- SSH Einwahl mit `root` (Bsp.: Putty in [4.1. "Grundlegende Einstellungen"](#))
- `setup` Kommando ausführen
- ► Netzwerk ► Adresseinstellungen

Anschließend über das Webinterface ggf. die DHCP und BlockOutTraffic IP-Adressen ändern.

Logging (de)aktivieren

- SSH Einwahl mit `root` (Bsp.: Putty in [4.1. "Grundlegende Einstellungen"](#))
- `„cd etc/rc.d“`
- `„vi rc.sysinit“` ausführen

-aktivieren:

```
#echo "Starting syslogd"  
/usr/sbin/syslogd -u syslogd -m 0  
#echo "Starting klogd"  
/usr/sbin/klogd -u klogd -j /var/empty
```

-deaktivieren:

```
#echo "Starting syslogd"  
#/usr/sbin/syslogd -u syslogd -m 0  
#echo "Starting klogd"  
#/usr/sbin/klogd -u klogd -j /var/empty
```

6.3 Anhang: FAQ

- *Ich habe die Adresse der GRÜNEN Schnittstelle geändert und mich „ausgesperrt“*

Siehe Abschnitt [6.1.2. "Wiederherstellen eines CompactFlash-Images"](#)

- *Ich möchte meine IPCop-Konfiguration mit allen Regeln usw. sichern (z.B. vor einem Update der Software)*

Sie benötigen eine USB-Floppy oder ähnliches. Die anschließen...

> WebGUI > System > Datensicherung

USB-Floppy **einbinden** (mounten), dann auf Diskette sichern. Danach das Gerät **abmelden!**

6.4 Anhang: Technische Daten

6.4.1 VS-Wall 5620

Chassis		Connectivity	
Construction	Fullsize stainless steel Connectors and PowerSwitch on rear side	LAN	1 x GigaLAN (RTL-8169 chipset) 5 x LAN 10/100 (RTL-8139 chipset) supports PXE Boot
Cooling system	Fanless design	USB	2 x USB 1.1 supports boot function from USB
LED indicator	Power, Status, LAN access	VGA	DSUB 15 connector
Dimensions	240 x 161 x 44mm ³	Com Ports	1 x RS232 DSUB 9 connector
Hardware		Operating Conditions	
Processor	VIA Eden 1GHz	Power Adapter	external Power Adapter 27W
Front Side Bus	100, 133MHz	Operating Temp.	0°-40°C
BIOS	AMI	Storage Temp.	-20°-+80°C
Chipset	VIA VT 8601T	Ordering Information	
Memory type	256MB SDRAM, max 512MB	Art No	206
Memory socket	1 x 144-pin SoDIMM	Product Name	VS-Wall 5620
VGA controller	integrated in Chipset	Packing List	VS-EmRunner 5620, Power Supply Adapter, Compact Flash 256MB IPCop preinstalled, CD with CF-Image and manual
Expansion Slot	1 x Mini PCI Slot		
HDD	optional 2.5" HD		
Compact Flash	256MB Card in CF-Slot with ejector		
Watchdog Timer	Software programmable 1-63 sec.		
Real Time Clock	standard		
Keyboard/Mouse	PS/2 connector for Keyboard and Mouse		

6.4.2 VS-Wall 9927

Chassis	
Construction	Heavy duty steel, Connectors and PowerSwitch on rear side
Cooling system	Fanless design
LED indicator	Power on/off, LAN access
Dimensions	242 x 148.5 x 34mm ³

Hardware	
Processor	Intel Celeron 400MHz
Front Side Bus	100, 133MHz
BIOS	AMI
Chipset	VIA 8601A, VT82C686B
Memory type	128MB SDRAM, max 512MB
Memory socket	1 x 144-pin SoDIMM
VGA controller	integrated in Chipset
Expansion Slot	1 x Mini PCI Slot
HDD	optional 2.5" HD
Compact Flash	256MB Card in internal Slot
Watchdog Timer	Software programmable 1-63 sec.
Real Time Clock	standard
Keyboard/Mouse	optional USB-PS/2 Adapter cable

Connectivity	
LAN	4 x 10/100Mbps BaseTx with RJ45 connector, NS 83816 chipset, supports boot from LAN
USB	2 x USB 1.1 supports boot function from USB
VGA	internal Header Connector
Com Ports	1 x RS232 DSUB 9 connector

Operating Conditions	
Power Adapter	external Power Adapter 27W
Consumption	up to 17W
Operating Temp.	0°-55°C
Storage Temp.	-20°-+80°C

Ordering Information	
Art No	207
Product Name	VS-Wall 9927
Packing List	VS-X-Fire 9927, Power Supply Adapter, Compact Flash 256MB IPCop preinstalled, CD with CF-Image and manual
optional	VGA adapter cable, KB/MS USB PS/2 cable

6.4.3 VS-Wall 860A

Chassis	
Construction	Light aluminum casing Connectors on rear side, PowerSwitch on front
Cooling system	Fanless design
LED indicator	Power on/off, LAN access
Dimensions	220 x 165 x 49mm ³

Hardware	
Processor	VIA Eden 533MHz
BIOS	AWARD Flash BIOS
Chipset	VIA 8601A
Memory type	128MB SDRAM, max 512MB
Memory socket	Standard SDRAM
VGA controller	integrated in Chipset
Expansion Slot	--
HDD	optional 2.5" HD
Compact Flash	256MB Card in internal Slot
Watchdog Timer	--
Real Time Clock	standard
Keyboard/Mouse	PS/2 connector
Audio	AC 97 ver 2.1

Connectivity	
LAN	3 x 10/100Mbps BaseTx with RJ45 connector, Realtek chipset, supports boot from LAN
USB	2 x USB 1.1 supports boot function from USB
VGA	DSUB 15 connector
Com Ports	2 x RS232 DSUB 9 connector, 1 x LPT DSUB 25

Operating Conditions	
Power Adapter	external Power Adapter 60W
Consumption	average 11W, with power supply 22W
Operating Temp.	0°-55°C
Storage Temp.	-20°-+80°C

Ordering Information	
Art No	164
Product Name	VS-Wall 860A
Packing List	VS-FlexRunner 11, Power Supply Adapter, Compact Flash 256MB IPCop pre-installed, CD with CF-Image and manual
optional	USB-Ethernet Adapter (for 4th BLUE Network)