

IPcop v1.3 und v1.4

Web-/Mail-Server im LAN, dynamische/fixe IP

Inhaltsverzeichnis	1
Grundsätzliches	1
Vorbereitung	1
Skizze des Netzwerks	2
Wie wird mein Server im Internet gefunden?	3
<i>Mit fixer IP</i>	3
<i>Mit dynamischer IP</i>	3
Dienst anbieten	3
<i>Mail-Server</i>	4
<i>Web-Server</i>	5
Und jetzt?	6

Grundsätzliches

Dieses Tutorial setzt eine Grundkonfiguration wie in dem Tutorial zum Basissetup des IPcop voraus. Die IP-Adressen müssen gegebenenfalls an die lokalen Vorgaben angepasst werden.

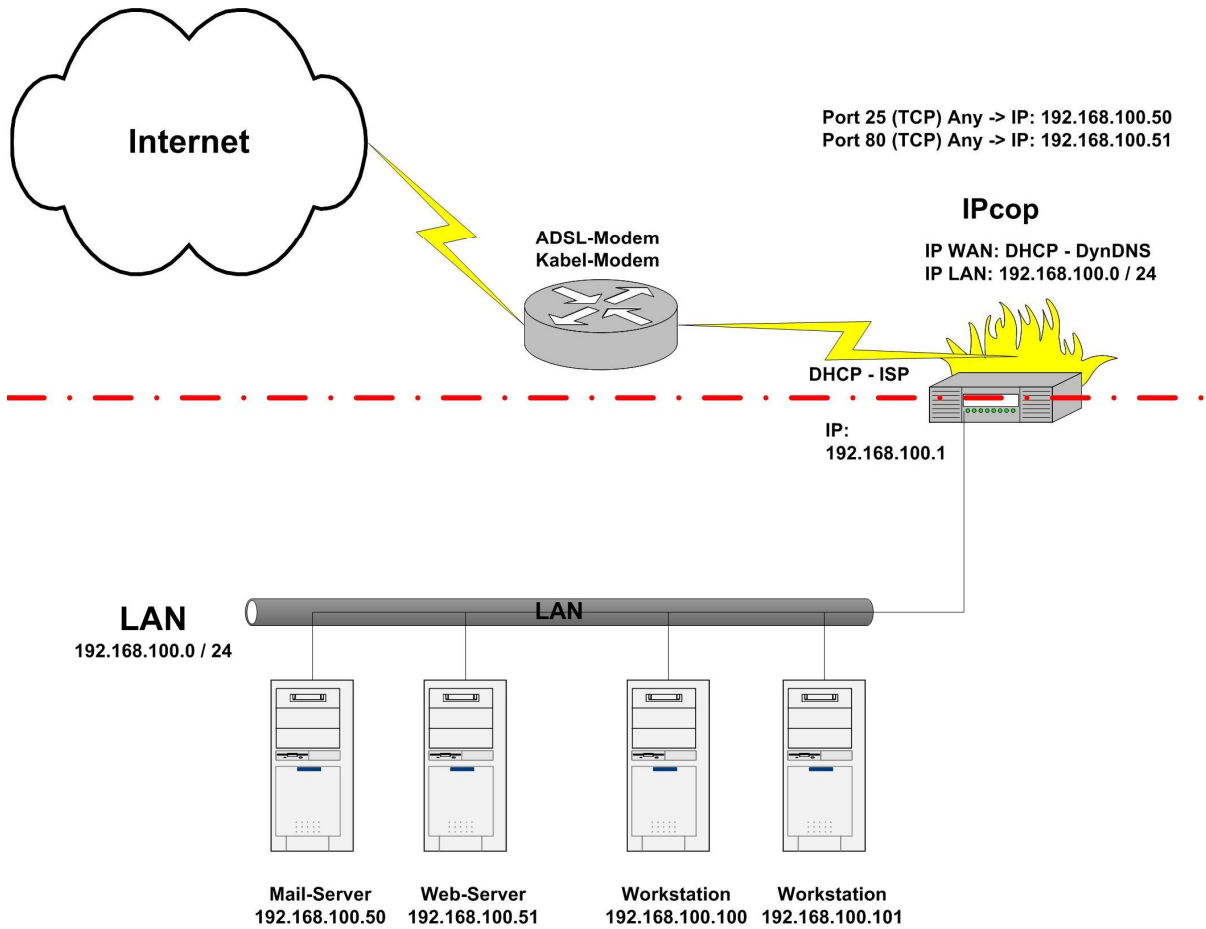
Es werden die Einstellungen besprochen, die nötig sind, um einen Web-/Mail-Server vom Internet erreichbar zu machen.

Vorbereitung

1. Grundkonfiguration des IPcop nach einem der folgenden Tutorials:
http://www.gutzeit.ch/ipcop/pdf/gr_konf_adsl_dyn.pdf
http://www.gutzeit.ch/ipcop/pdf/gr_konf_adsl_fix.pdf
http://www.gutzeit.ch/ipcop/pdf/gr_konf_kabel_dyn_fix.pdf
2. Web-Server läuft im LAN, Funktionstest erfolgreich
3. Mail-Server läuft im LAN, Funktionstest erfolgreich

Ecki's Place

Skizze des Netzwerks



Wie wird mein Server im Internet gefunden?

Mit fixer IP

Jeder Server, der vom Internet aus erreichbar sein soll, sollte über einen FQDN (Full Qualified Domain Name) wie z. B. „www.meinedomaene.ch“ verfügen. Eine Adressierung über die IP-Adresse ist zwar möglich aber denkbar unkomfortabel und stösst bei dynamischen IPs schnell an ihre Grenzen.

Wer eine fixe IP sein Eigen nennt, bekommt diese in der Regel per DHCP fix von seinem Provider zugewiesen.

IPcop (RED) bekommt z. B. immer die IP 123.123.123.123 (ist nur ein Beispiel ;-)

Des Weiteren sind in der Regel auch DNS-Dienste im Paket inbegriffen. Das heisst, dass der Provider mit Einträgen auf seinen DNS-Servern dafür sorgt, dass der Aufruf von „www.meinedomaene.ch“ zur IP 123.123.123.123 aufgelöst wird.

Mit dynamischer IP

Die meisten ADSL- und Kabelmodem-Abos werden wohl ohne fixe IPs verkauft. Da diese Adresse durch eine, häufig verwendete, Zwangstrennung nach meist 24 Stunden wechselt, funktioniert der oben genannte Ansatz nicht.

Um dieses Problem zu lösen und einem Server trotzdem einen FQDN zuweisen zu können, gibt es so genannte DynDNS-Dienste, von denen IPcop etwa ein halbes Dutzend kennt und bedienen kann.

Diese Dienste erlauben es, nach einer meist kostenlosen Registration, einem Programm oder Script, die aktuelle externe IP-Adresse auf den DNS-Servern des Anbieters zu schreiben. Bei der Registrierung kann man in der Regel den Host-Teil der Adresse frei wählen und aus einer Liste von 1st- und 2nd-Level-Domains auswählen.

Als Beispiel sei hier <http://www.dyndns.org> erwähnt. So könnte ein DynDNS FQDN z. B. so aussehen: „meinhost.dyndns.org“, oder „meinhost.homelinux.com“.

Mit den entsprechenden Accountinformationen gefüttert, ist der IPcop in der Lage, dem DynDNS DNS-Server bei einem IP-Wechsel die neue IP-Adresse zu melden und dadurch den Server praktisch ununterbrochen erreichbar zu halten.

Dienst anbieten

Da der Server nun problemlos erreichbar ist, können wir uns daran machen, unter dem FQDN Dienste im Internet anzubieten.

In diesem Tutorial geht es in erster Linie um Web- und Mail-Server. Das hier gezeigte kann jedoch problemlos auch auf andere Dienste angewandt werden.

Mail-Server

Mail-Server kommunizieren untereinander über das SMTP-Protokoll (Simple Mail Transfer Protocol) welches standardmässig den TCP-Port 25 belegt.

Um einen Mail-Server im LAN vom Internet erreichbar zu machen, muss also der TCP-Port 25 in der Firewall geöffnet werden und auf die interne, private IP-Adresse des Mail-Servers weitergeleitet werden.

Ein Screenshot zeigt die dafür notwendigen Einstellungen.

the bad packets stop here

Konfiguration der Port-Weiterleitung System: IPcopVM01 IPCOP v1.3.0

Webproxy | DHCP | Port-Weiterleitung | Externe Alias-Adressen | Fernwartungszugang | DMZ-Schlupflöcher | Dynamischer DNS

Neue Regel hinzufügen:

Protokoll: TCP Alias-IP-Adresse: DEFAULT IP Quell-Port: 25
Ziel-IP-Adresse: 192.168.100.50 Ziel-Port: 25
Anmerkung: Mail-Server LAN Aktiviert:
Quell-IP, oder Netzwerk (leer für "ALL"):
 Dieses Feld kann leer bleiben.

Aktuelle Regeln:

Proto	Quelle	Ziel	Anmerkung	Aktion
TCP	DEFAULT IP : 25(SMTP)	192.168.100.50 : 25(SMTP)	Mail-Server LAN	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>

IPcop - Your Personal Internet Police

Der fertige Eintrag sieht dann so aus

Aktuelle Regeln:

Proto	Quelle	Ziel	Anmerkung	Aktion
TCP	DEFAULT IP : 25(SMTP)	192.168.100.50 : 25(SMTP)	Mail-Server LAN	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>

Alias-IP-Adresse: Die IP des roten Interface, kann in der Regel auf „DEFAULT IP“ belassen werden. Ist nur von Bedeutung, wenn man über mehr als eine fixe IP verfügt und mehrere Alias-IPs auf Rot definiert hat.

Quell-Port: Der Port, auf dem die Anfrage aus dem Internet beim IPcop ankommt. Da der IPcop vom Internet als der Mail-Server erscheint, muss der Port 25 eingetragen werden.

! Es ist nicht der Quellport des anfragenden Clients gemeint!

Ziel-IP-Adresse: Die private IP-Adresse, des Servers im LAN

Ziel-Port: Der Port, auf dem der Mail-Server lauscht, normalerweise Port 25

Anmerkung: Eine kurze Beschreibung der Regel (optional)

Quell-IP, oder...: Wenn das Feld leer gelassen wird, kann Jedermann auf dem Port 25 auf den Mail-Server verbinden. Da die Mail-Server, von denen man Mails bekommt in der Regel nicht bekannt sind, sollte das Feld leer bleiben.

Falls Mails jedoch nur von einem definierten Mail-Server angenommen werden sollen, kann hier die IP-Adresse des Mail-Servers eingetragen werden. Anfragen auf Port 25 von anderen IPs werden dann blockiert.

Web-Server

Webserver lauschen standardmässig auf dem TCP-Port 80, HTTP (HyperText Transfer Protocol). Um einen Webserver vom Internet erreichbar zu machen, muss also der TCP-Port 80 in der Firewall geöffnet und auf die interne, private IP-Adresse des Web-Servers weitergeleitet werden.

Ein Screenshot zeigt die dafür notwendigen Einstellungen.

the bad packets stop here

Konfiguration der Port-Weiterleitung System: IPCopVM01 IPCOP v1.3.0

Webproxy | DHCP | Port-Weiterleitung | Externe Alias-Adressen | Fernwartungszugang | DMZ-Schlupflocher | Dynamischer DNS

Neue Regel hinzufügen:

Protokoll: TCP Alias-IP-Adresse: DEFAULT IP Quell-Port: 80
Ziel-IP-Adresse: 192.168.100.51 Ziel-Port: 80
Anmerkung: Web-Server LAN Aktiviert:
Quell-IP, oder Netzwerk (leer für "ALL"):
 Dieses Feld kann leer bleiben.

Aktuelle Regeln:

Proto	Quelle	Ziel	Anmerkung	Aktion
TCP	DEFAULT IP : 25(SMTP)	192.168.100.50 : 25(SMTP)	Mail-Server LAN	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
TCP	DEFAULT IP : 80(HTTP)	192.168.100.51 : 80(HTTP)	Web-Server LAN	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>

IPCop - Your Personal Internet Police

Der fertige Eintrag, incl. Mail-Server, sieht dann so aus

Aktuelle Regeln:

Proto	Quelle	Ziel	Anmerkung	Aktion
TCP	DEFAULT IP : 25(SMTP)	192.168.100.50 : 25(SMTP)	Mail-Server LAN	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
TCP	DEFAULT IP : 80(HTTP)	192.168.100.51 : 80(HTTP)	Web-Server LAN	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>

Jetzt sind sowohl der Mail- als auch der Web-Server vom Internet über den DNS-/DynDNS-Namen erreichbar. Falls der Webserver auch SSL verschlüsselte Seiten ausliefern soll, muss zusätzlich der Port 443 (HTTPS) analog zum Port 80 geöffnet werden.

Achtung bei v1.3:

Ein Test sollte NIE direkt aus dem LAN gemacht werden. Die Anfrage geht dabei durch die Firewall an die externe IP-Adresse des IPCop, da der DNS-Name in eine öffentliche IP aufgelöst wurde. Hierbei wird die Adresse „geNATted“ und erreicht dann den Server im LAN. Der Server antwortet jedoch direkt, an der Firewall vorbei, da der Client sich ja im gleichen LAN-Segment befindet. Da die Absenderadresse nun eine andere ist, als die Adresse, an die die Anfrage gesendet wurde, wird die Antwort vom Client nicht als zur vorherigen Anfrage gehörend erkannt und verworfen.

Ein Test sollte daher immer mit einem anderen Internetzugang (z. B. DialUp, etc.) erfolgen.

Bei der v1.4 wird ein [Source-NAT](#) gemacht, so dass die Anfrage aus dem LAN funktioniert.

Und jetzt?

- Wie wäre es mit dem Einrichten eines Filesharing-Clients, z. B. Overnet/eDonkey/eMule?
- Was ist eine DMZ und wofür brauche ich sie?
- Wie bringe ich meinen Webserver in der DMZ zum Laufen?

Also weiter geht's mit dem nächsten Tutorial.