IPcopv 1.3 und v1.4

Web- / Mailserver in der DMZ

Grundsätzliches

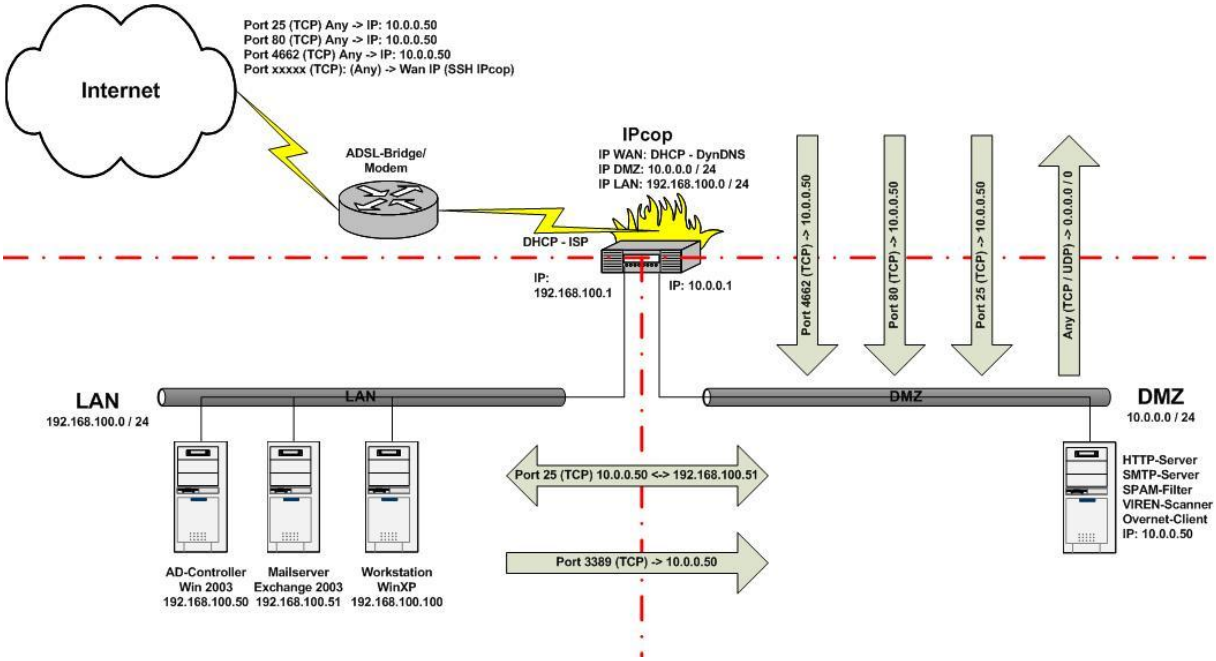
Dieses Tutorial setzt eine Grundkonfiguration wie in den Tutorials zum Basissetup des IPcop voraus. Die IP-Adressen müssen gegebenenfalls an die lokalen Vorgaben angepasst werden.
In diesem Tutorial wird Grundlagen-KnowHow über eine DMZ, auch Perimeter Netzwerk genannt, vermittelt. Ausserdem wird in einem Beispiel der IPcop für den Betrieb eines Web- / Mailservers in der DMZ konfiguriert.

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. Vorstellung, wie das Netzwerk aussehen soll

Beispiel eines Netzwerks mit DMZ



Was ist eine DMZ?

DMZ steht für **De**-**M**ilitarisierte **Z**one. In vielen Dokumentationen wird auch von „Perimeter Network“ gesprochen. Die Bedeutung ist in beiden Fällen dieselbe.

Eine DMZ bezeichnet ein Netzwerksegment, welches sowohl vom Internet, als auch vom LAN durch einen Paketfilter oder eine Firewall wie dem IPcop getrennt ist. Das LAN ist dabei nur über eine weitere Firewall erreichbar. Häufig finden sich Installationen mit 2 Firewalls, zwischen denen sich dann die DMZ befindet, s. z. B. http://de.wikipedia.org/wiki/DMZ. Der IPcop vereint diese beiden Firewalls in sich und stellt sicher, dass jedes Paket von und zum Internet seine Filter durchlaufen muss. Zu diesem Zweck existieren auf dem IPcop verschiedene Regelsätze. Einer regelt den Zugriff vom Internet zur DMZ, einer den Zugriff vom Internet zum LAN und ein Dritter regelt den Verkehr zwischen DMZ und LAN.

Warum brauche ich eine DMZ?

Der Hauptgrund für die Einrichtung einer DMZ ist die Sicherheitsvorgabe, keine direkte Verbindung vom Internet ins LAN zuzulassen. Diese Vorgabe liesse sich mit einer restriktiven Firewall und einem Proxyserver für den Webzugriff häufig noch ohne DMZ realisieren. Sobald jedoch ein eigener Mail- oder Webserver ins Spiel kommt, führt an einer DMZ kaum ein Weg vorbei. Warum, wird in den folgenden Abschnitten erläutert.

Warum sind direkte Verbindungen ins Internet gefährlich?

Die Antwort ist einfach. Sobald eine direkte Verbindung mit dem Internet besteht, können ohne Zutun des Administrators/Users schädliche Programme oder sonstiger unerwünschter Traffic die Firewall auf den geöffneten Ports passieren. Einige hervorragende Beispiele für solch unerwünschten Code liefern z. B. „W32.Blaster“ und „SQL Slammer“ (auch als „Code Red“ bekannt).
http://de.wikipedia.org/wiki/Computerwurm, Abschnitt „Geschichte“

„W32.Blaster“ verbreitete sich über TCP-Port 135, welcher auf den allermeisten Firewalls geschlossen sein sollte. „SQL Slammer“ verwendete den UDP-Port 1434, welcher normalerweise zur Kommunikation mit MS SQL-Servern verwendet wird. Da viele Datenbankanwendungen auch durch Firewalls kommunizieren müssen, war dieser Port auf vielen Firewall offen. Bis zum 25.01.2003 konnte sich jedoch niemand vorstellen, dass UDP-Port 1434 eine Gefahr darstellen könnte. Wer den Ausbruch von „SQL Slammer“ live erleben durfte, weiss spätestens seit dann, welch verheerende Wirkung läppische 376 Byte entfalten können. Die Ports wechseln, die Gefahr bleibt!

Ebenso problematisch können im Firmenumfeld aber auch „einfache“ DOS-Attacken (Denial of Service) sein, welche z. B. den lokalen Mailserver und damit in vielen modernen Firmen den Betrieb lahm legen.

Den schlimmsten Fall stellt sicher die Situation dar, dass sich eine unbefugte Person, gemeinhin als Hacker/Cracker bezeichnet, Zugang zu einem Server im LAN verschafft und dort Schaden anrichtet. Solange ein Port auf einer Firewall offen ist und hinter der Firewall ein Dienst auf diesem Port lauscht, besteht die Gefahr, dass dieser Dienst von Hackern/Crackern missbraucht wird um Zugang zum System zu bekommen.

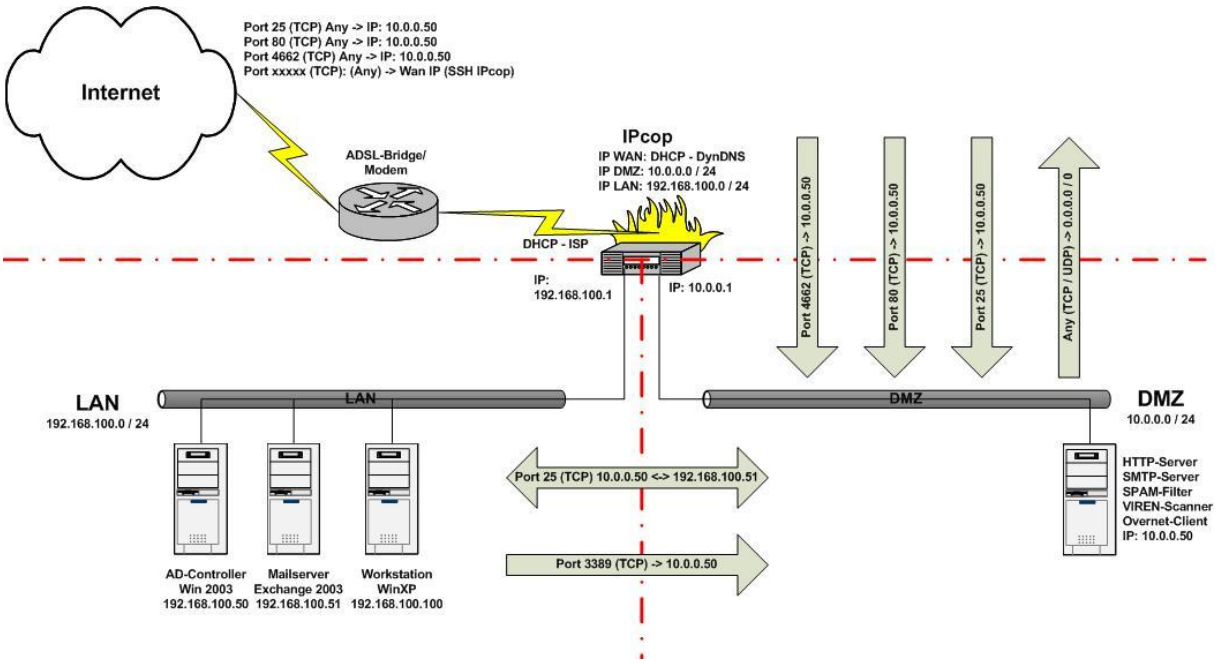
Und wie hilft mir nun die DMZ?

Sobald Dienste im Internet angeboten werden müssen, z. B. mit einem Web-Server, oder Dienste vom Internet bezogen werden müssen, z. B. mit einem Mail-Server, müssen notgedrungen Ports zum Internet hin geöffnet werden. Damit sind diese Server angreifbar und verwundbar. Dies ist eine Tatsache und lässt sich nicht vermeiden.
Ich kann jedoch dafür sorgen, dass ein erfolgreicher Hackerangriff auf einen meiner Server nicht das gesamte LAN gefährdet, oder dass ein Nachfolger von „SQL Slammer“ nicht den gesamten Datenverkehr im LAN zum erliegen bringt.
Dazu muss ich die gefährdeten Server in einem separaten Subnetz isolieren und mit einer Firewall den weiteren Zugang zum LAN regeln.

Genau dies ist die Aufgabe einer DMZ.

Das Konzept

Übersicht



Es empfiehlt sich immer, das gewünschte Ergebnis so detailliert wie möglich aufzuzeichnen und wenn möglich einer weiteren Person zur Überprüfung vorzulegen.

In dem vorliegenden Fall besteht die Aufgabe darin, einen Web- und einen Mailserver sicher mit dem Internet zu verbinden. Als Dreingabe wird der P2P-Client ebenfalls in die DMZ verbannt.

Dazu erlaube ich Jedermann vom Internet aus auf meinen Webserver, Mailserver und meinen Overnet-Client in der DMZ zu verbinden. Die dazu nötigen Portforwardings zeigen die Screenshots auf der nächsten Seite. Der Mailserver in der DMZ wird als reines Mailrelay konfiguriert, evtl. erweitert mit SPAM- und Virenfilter. Das heisst, alle Mails für die eigene Domain werden angenommen und direkt an den internen Mailserver weitergeleitet.
!!! Es werden keine Mails in der DMZ gespeichert!!!
Dadurch wird sichergestellt, dass sich in der DMZ niemals wichtige interne Daten befinden. Ebenso ist kein direkter Zugriff vom Internet auf das LAN möglich, da nun das Mailrelay in der DMZ dazwischen liegt. Selbst wenn jetzt ein Hacker den Mail- oder Webserver knackt, besteht keine direkte Gefahr für die Server und Clients im LAN, da der Hacker erst noch die zweite Firewall überwinden muss, um Zugriff auf Ressourcen im LAN zu bekommen.

Die Analyse

Als erstes muss definiert werden, welche Dienste wo benötigt werden. Anhand der Dienste lassen sich anschliessend die benötigten Portnummern festlegen. Zum Abschluss muss nun noch definiert werden **Wer, von Wo, nach Wo** über **Welchen Port** Zugriff auf **Welches System** erhält.

System	Wer	von Wo	nach Wo	Port	Bemerkungen
Firewall	Admin	GREEN, RED	Firewall	TCP xxxxx (SSH)	Konfiguration, Fernwartung
Webserver DMZ	Jeder Jeder	RED GREEN	10.0.0.50 10.0.0.50	TCP 80 TCP 80	HTTP HTTP
Mailserver DMZ	Jeder 10.0.0.50	RED ORANGE	10.0.0.50 192.168.100.51	TCP 25 TCP 25	SMTP SMTP
P2P-Client	Jeder	RED	10.0.0.50	4662	Overnet
Mailserver LAN	192.168.100.51	GREEN	10.0.0.50	TCP 25	SMTP

Diese Auflistung ist so kurz wie möglich gehalten. Eventuell müssen noch weitere Dienste wie z. B. DNS (interne Namensauflösung über AD-Integrierten DNS), HTTPS (SSL-Verschlüsselter Webtraffic), oder andere Dienste hinzugefügt werden.

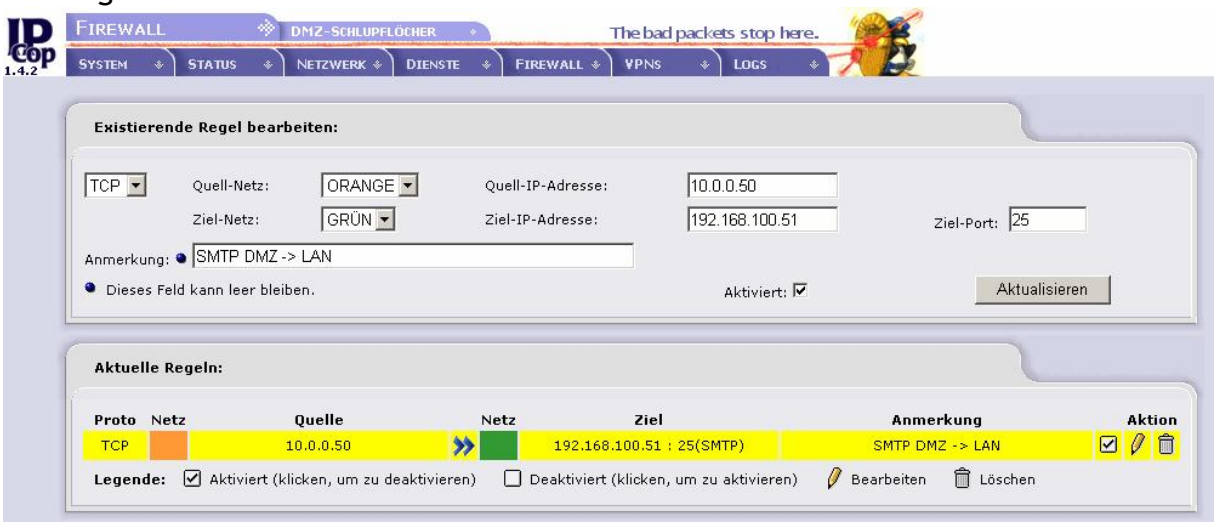
Eine Liste aller „Well Known Ports“ ist hier zu finden:
http://www.iana.org/assignments/port-numbers

Die Umsetzung

Dem Fernwartungszugriff habe ich ein eigenes Tutorial gewidmet. Hier konzentriere ich mich auf den Web- / Mailserver.

Port-Forwardings für Web, Mail und Overnet werden wie gewohnt eingerichtet, wobei die Ziel-IP nun eine IP aus dem orangenen Subnetz ist.

Um den Mailverkehr zwischen DMZ und LAN zu ermöglichen benötigen wir nun noch ein so genanntes Pinhole.



Hiermit erlaube ich dem Mailrelay (10.0.0.50) in der DMZ mit dem Exchange im LAN (192.168.100.51) via Port 25 SMTP zu kommunizieren.

Dieses Schema lässt sich auf beliebige Dienste anwenden. Egal ob ein Webserver in der DMZ Zugriff auf eine Datenbank im LAN benötigt, oder ein Webmail-Frontend Zugriff auf die eigentlichen Mails auf dem internen Mailserver. Es werden nur genau die benötigten Ports von der DMZ zum LAN geöffnet, die absolut notwendig sind. Auf diese Weise ist ein direkter Zugriff vom Internet auf Ressourcen im LAN unmöglich, es können aber trotzdem vom Internet aus Dienste in Anspruch genommen werden, die Daten aus dem LAN benötigen.

!!! Pinholes sind nur notwendig, wenn eine Verbindung von einem Server in der DMZ initiiert wird!!!

Da der IPcop per Default alles von Grün aus erlaubt, benötige ich keinerlei Firewallregeln um vom LAN aus einen Server in der DMZ zu konfigurieren.

Ebenfalls ist zu bedenken, dass ein Ping aus der DMZ heraus weder ins LAN, noch ins Internet funktioniert. Es empfiehlt sich daher zum Testen der Internetverbindung aus der DMZ z. B. ein „telnet smtp.freesurf.ch 25“ abzusetzen. Wenn sich der Mailserver meldet ist die Verbindung OK und kann mit „quit“ beendet werden.

Und jetzt?

- Wie greife ich von extern auf meine Firewall zu?

Also weiter geht’s mit dem nächsten Tutorial.