Interne Verwaltung (maint)

Der Rolle *maint* obliegt die interne Verwaltung des Systems. Diese beinhaltet hauptsächlich die Benutzerverwaltung. Darüber hinaus werden mit dieser Administrationsrolle folgende Aufgaben erledigt:

- Den Server neu starten
- Systemdienste neu starten
- Die Fernwartungsverbindung öffnen, damit eine Fernwartung stattfinden kann
- Systemdienste neu starten
- Die interne Administration freigeben, sodass die Benutzer *root* und *security* per SSH zu erreichen sind.

Zusätzlich werden durch *maint* die Einstellungen für den zentralen Spamfilter *amavisd-new* und das Mail-Forwarding gesetzt.

Wartungszugang öffnen

Eine wichtige Aufgabe kommt der Rolle *maint* im Zusammenhang mit der Fernadministration per SSH zu. Mittels *SSH Admin open* kann hier der zur gesicherte Fernzugang für Wartungsarbeiten für eine Stunde geöffnet werden.

Soll ein Zugriff per SSH von extern (also über den externen Netzwerkanschluss z.B. aus dem Internet) erfolgen, so muss zusätzlich die Option *SSH open* oder ggf. *Fernwartungsverbindung auf* gewählt werden.

Systemdienste neu starten

Auf der mp-Firewall laufen diverse Systemdienste, welche einzeln durch den Administrator *maint* neu gestartet werden können. Sollte einmal ein Dienst hängen, ist es nicht unbedingt notwendig das gesamte System neu zu starten. Die Systemdienste werden direkt durch das Auswählen des jeweiligen Menüpunktes gestartet, es gibt keine weiteren Untermenüs, die aufgerufen werden. Folgende Systemdienste können neu gestartet bzw. gestoppt werden:

Systemdienst	**Beschreibung**
DSL trennen / neu starten	Falls DSL als Verbindungsweg für das Netzwerk verwendet wird oder DSL für ein Fallback-Netzwerk konfiguriert wurde, so kann der interne Administrator hier die DSL Verbindung mit dem Menüpunkt DSL trennen abbrechen und/oder die DSL-Verbindung neu starten.
DynDNS aktualisieren	Falls Sie nur eine dynamische, sich also häufig ändernde IP-Adresse haben, können Sie sich beim kostenloses DynDNS-Dienst einen Namen registrieren und diesen selber aktualisieren. Das erfolgt zwar bei der mp-Firewall automatisch, bei Bedarf kann man die Aktualisierung aber auch mit diesem Menüpunkt erzwingen.
Webserver restart	Neustart des internen Webservers.
Squid restart	Neustart des WWW/FTP-Proxy.

Systemdienst	Beschreibung
Squid3 restart	
Postfix restart	Neustart des gesamten Mail-Systems.
POP3/IMAP restart	Neustart der Mail-Abholdienste POP3/IMAP.
MySQL-Neustart	Neustart des MySQL-Server-Dienstes
MySQL-Reparatur	Reparatur der MySQL-Datenbank
OpenVPN restart	Neustart einzelner OpenVPN-Verbindungen.
Sofort Mail abholen	Mailabholung von externen Mail-Servern starten

Fallback Zugang

Die mp-Firewall bietet die Möglichkeit beim Ausfall der "normalen" Netzwerkanbindung auf eine Fallback-Anbindung umzuschalten. Die Konfiguration des Fallback Netzwerks wird von dem Benutzer *config* in den Konfigurationseinstellungen vorgenommen. Sollte der Fall eintreten, dass der Zugang zum Netzwerk über den "normalen" Verbindungsweg nicht mehr möglich ist, so kann hier über den Menüpunkt *Fallback-Modus anschalten* auf den Fallback-Zugang umgeschaltet werden.

Mit dem Menüpunkt *Fallback-Modus abschalten* kann wieder auf den "normalen" Netzwerkzugang umgeschaltet werden. Mit den Menüpunkt *Fallback-Modus Status* kann man sich jederzeit anzeigen lassen, ob der Fallback-Zugang aktiv oder abgeschaltet ist.

Hinweis: Die Menüpunkte zum Fallback-Netzwerk sind nur verfügbar, wenn das Fallback-Netzwerk eingerichtet ist.

Benutzerverwaltung

Alle Benutzer, die den Mailserver, den Webmailer, die Benutzerschnittstelle oder den Spamfilter auf der mp-Firewall nutzen wollen, müssen reguläre Benutzer sein, die als Administrator *maint* hier angelegt werden.

Es können neue reguläre Benutzer angelegt und gelöscht werden, die Passworte neu vergeben und die benutzerspezifischen Ressourcen-Einstellungen geändert werden.

Detaillierte Hinweise und Informationen zu empfohlenen Qualitätsstandards bei der Vergabe von Passworten finden Sie z.B. beim Bundesamt für Sicherheit in der Informationstechnologie unter: http://www.bsi.bund.de/gshb/deutsch/m/m02011.htm[1)]

Das Anlegen von neuen Benutzern geschieht unter dem Menüpunkt *Benutzerverwaltung*. Für das Anlegen eines neuen Benutzers ist zumindest ein Benutzername notwendig. Vor- und Nachname sind optional. Sie können folgende Menüpunkte auswählen:

Menüpunkt	Beschreibung
Ende	Verlassen des Menüs.
——-	
Info	Anzeige aller Einstellungen für die angelegten Benutzer.
Ablaufende Konten	Anzeige aller abgelaufenen oder innerhalb der nächsten 30 Tagen ablaufen werden.

Menüpunkt	Beschreibung
Ablaufende Passwörter	Anzeige aller abgelaufenen oder innerhalb der nächsten 30 Tagen ablaufenden Benutzer-Passwörter.
Quota-Engpässe	Anzeige aller Quota-Engpässe.
Show-Forwarding	Anzeige aller eingestellten E-Mail Weiterleitungen (Forwardings) für einzelne Benutzer.
Lokale Mailadressen	Anzeige aller lokalen Mailadressen inkl. aller Aliase.
Adressenliste versenden	Tragen Sie hier die Adresse ein an die die Liste versendet werden soll. Der Versand erfolgt unverschlüsselt und erfordert eine korrekte Mailkonfiguration.
Übersicht Mail-Domänen	Anzeigen der Domänen
——-	
Passwort	Unter diesem Menüpunkt können Sie das Passwort eines Benutzers ändern. Die Passwörter der Systemrollen wie *root*, *security* oder *config* können Sie als Benutzer *maint* nicht ändern. Bitte beachten Sie auch die Hinweise zu den Systembenutzern in Anschluss an diese Tabelle.
Passworte Einmal-Nutzung	Erstellung und Verwaltung von Passwörtern zur einmaligen Benutzung durch den Benutzer
Neu	Hier können Sie neue Benutzer anlegen. Dazu ist die Eingabe eines Benutzernamens zwingend erforderlich. Der Benutzername darf eine Länge von 60 Zeichen nicht überschreiten und muss mit einem Buchstaben beginnen. Ausgenommene Zeichen sind das Leerzeichen und der Schrägstrich. Die Eingabe des vollständigen Namens ist nur optional.
Name	Hier kann der volle Benutzername zu einem Konto geändert werden. Diese Angabe ist optional und dient der besseren Bestimmung von Benutzen.
Mail-Alias	Angabe unter welchen weiteren E-Mail-Namen einzelne Benutzerkonten erreichbar sein sollen.
Forwarding	Einstellung welche weiteren Empfänger die E-Mails eines Kontos bekommen sollen. Es ist ratsam für die Systembenutzer eine Weiterleitung einzurichten, damit Systemmeldungen nicht ungelesen auf der mp-Firewall verbleiben.
Löschen	Benutzer aus der Liste der Nutzungsberechtigten entfernen.
Gültigkeitsdauer	Die Gültigkeitsdauer von Benutzer-Konten begrenzen. Diese Funktion erlaubt es bei bestehenden Benutzern den Zugang zum System zeitlich zu befristen.
Quota	Festlegen des Plattenplatzes für einzelne Benutzer. Es ist sinnvoll für einzelne Benutzern die Größe des Plattenplatzes für das HOME-Verzeichnis zu beschränken, um damit den maximalen Platz für ein Postfach zu setzen. Ebenfalls macht es Sinn den Plattenplatz für den Benutzer *backuser* als zusätzlicher Schutz vor einem Überlauf der Festplatte durch Backups zu begrenzen.
Passwort entfernen	Auswahl der Benutzer, deren Passwort ungültig gemacht werden soll. Dies ist keine Änderung des Passwortes, sondern die Passworte werden ungültig gemacht. Dies ist z.B. notwendig für die ausschließliche Authentifizierung über Kerberos-v5.

Achtung: Alle Einstellungen werden ohne Neustart sofort wirksam.

Sonderfall Systembenutzer

In der Benutzerverwaltung sind im Grundsystem Systembenutzer angelegt. Diese haben spezielle Aufgaben und sind keine gewöhnlichen Benutzer der mp-Firewall. Nachfolgend wird kurz erläutert welche Aufgaben die Systembenutzer haben:

Systembenutzer	Funktion
mailadmin	Administration des webbasierten Spamfilters
ftpupload	Berechtigung Dateien in den internen FTP-Server einzuspielen.
wwwupload	Berechtigung Dateien in den internen Webserver einzuspielen

Systeminformationen

Es gibt einige System-Information die für die Analyse des Systems oder eine Fehlerdiagnose hilfreich sein können. Hierfür bieten die folgenden Optionen eine mögliche Hilfestellung.

Menüpunkt	Beschreibung
Kern-Not-Log über Netz an	Anschalten der Übertragung der kern.log Daten zu einem entfernten Rechner.
Kern-Not-Log über Netz aus	Ausschalten der Übertragung der kern.log Daten zu einem entfernten Rechner.
Festplatten-Ident	Anzeigen der Hersteller-Identifikationsdaten der Festplatte.
Hardware-Sensoren	Ausgabe der Ergebnisse von den im *config* Menü eingestellten Hardwaresensoren.

[1)]

Die m-privacy GmbH hat auf die dort dargelegten Informationen keinen direkten Einfluss, die Angabe der URL erfolgt lediglich als Hilfe für die Benutzung.