Tim Reeves
Internet Services

Email und Server-Sicherheit mit Plesk

Artikel von 2014, Anfang 2021 aktualisiert.

Inhaltsverzeichnis

Mailserver....2
IP-Ports für den Mailverkehr....2
Mail-Ports die SSL/TLS erzwingen....2
Mail-Ports die SSL/TLS nicht erzwingen....2
Was eigentlich los ist....3
Port 587 / Require TLS....3
Was die Praxis zeigt....4
Mail Display Agent: Courier oder Dovecot?....4
Dovecot konfigurieren....5
SSL-Zertifikat nachladen....5
Vorhanden in der Standard-Config....5
Unverschlüsselte Authentizierung abschalten....5
Plesk für sicheren Mailverkehr einstellen....5
Mail Transfer Agent: Postfix statt Qmail....5
Mail Server Settings....6
Outgoing Mail Control....6
Parallels Premium antivirus....7
Weitere Sicherheitsmassnahmen....8
Wichtige Maßnahmen....8
Security Policy....8
Fail2Ban....8
Watchdog....8
Optionale Maßnahmen....9
Firewall....9
ModSecurity....10
Health Monitor....10
Webserver Configurations Troubleshooter....10

Tim Reeves Internet Services
Lortzingweg 10
D-31275 Lehrte

Tel. 05132 923 35 78
Fax. 08532 923 99 51
Ust-IdNr. DE269216307

Mailserver

Eher wir zur Tat schreiten, müssen wir klären, was wir erreichen wollen – in diesem Fall müssen wir dazu die Nutzung von IP-Ports bzgl. Mailverkehr verstehen:

IP-Ports für den Mailverkehr

Mail-Ports die SSL/TLS erzwingen

- 993: der IMAP-Port ausschließlich für SSL-Verschlüsselung
- 995: der POP3-Port ausschließlich für SSL-Verschlüsselung
- 587: der SMTP-Port für Einlieferung durch Mail-Clients („Submission“ - Protokoll-Aushandlung per StartTLS, d.h. ggf. auch unverschlüsselt)
- 465: der SMTP-Port bei SSL-Verschlüsselung (Nur mit SSL/TLS und inzwischen offiziell verpönt [1,2] aber in der Praxis immer noch sehr beliebt - siehe SMTPS)

1) Auf dem Port 465 ist mittlerweile Source Specific Multicast für Audio und Video registriert. *

2) Eine Ende-zu-Ende-Sicherheit wird dadurch sowieso nicht erreicht, da alle Mailserver und Mailrelays die E-Mail im Klartext verarbeiten (müssen).

* "SMTPS wird dennoch weiterhin auf dem Port 465 angeboten, aber auch auf dem Port 587 für Message Submission nach RFC 4409. Da Message Submission sich aber nie weitreichend durchsetzen konnte und in vielen Organisationen der ausgehende und/oder eingehende SMTP-Port als Anti-SPAM Maßnahme blockiert wird, ist davon auszugehen, dass Port 465 auch in absehbarer Zukunft für Client To Server-Transfers genutzt werden wird."

Mit anderen Worten, die Ratschläge widersprechen sich: Man sollte 465 nicht nutzen, weil es offiziell schon anderweitig vergeben ist; aber 465 bietet den Vorteil, dass es auf jeden Fall verschlüsselt wird, im Gegensatz zu 587, wo die Möglichkeit besteht, dass per STARTTLS eine unverschlüsselte Verbindung ausgehandelt wird. Was tun? Münze werfen? Nein: Weiterlesen!

Mail-Ports die SSL/TLS nicht erzwingen

- 143: der IMAP-Port für IMAP-Server
  unverschlüsselt bzw. Ergebnis der StartTLS-Verhandlung
- 110: der POP3-Port für POP-Server (dito)
- 25: der SMTP-Port für Nutzung durch andere SMTP-Server,
  d.h. Weitergabe von einem Server zum anderen. Sollte daher ja nicht von Mail-Clients mitbenutzt werden (kann aber nicht im Firewall gesperrt werden, sonst gibt es keinen Austausch mit anderen SMTP-Server). Generell ohne SSL!

Also: IMAP via 993 wird auf jeden Fall verschlüsselt, aber IMAP per 143 setzt TLS-Verschlüsselung ein (weiterhin auf Port 143) nur WENN die Verschlüsselung per StartTLS vereinbart wird, d.h. es hängt auch vom Client ab, es sei denn... Weiterlesen!

Was eigentlich los ist

Lesen Sie zunächst diesen sehr guten Artikel: SSL vs TLS vs STARTTLS

"Many sites (including FastMail) now disable plain IMAP (port 143) and plain POP (port 110) altogether so people **must** use an SSL/TLS encrypted connection. By disabling ports 143 and 110, this removes completely STARTTLS as even an option for IMAP/POP connections."

Ist damit der heilige Gral gefunden? Nein – Weiterlesen!☺

Port 587 / Require TLS

Ich gehe hier davon aus, dass Postfix (nicht qmail) als SMTP-Server benutzt wird – dies lässt sich ggf. leicht über den Plesk-Installer auswählen, und ist die bessere Wahl, siehe unten Mail Transfer Agent: Postfix statt Qmail.

Lesen Sie nun diesen Blog-Beitrag: Postfix Requires TLS on Port 587

Siehe auch Parallels dazu – es hängt davon ab, ob Postfix als SMTP-Agent eingestellt ist und wie es konfiguriert ist. Siehe auch postfix.org dazu.

Plesk/Ubuntu /etc/postfix/main.cf:

```
...
smtpd_tls_security_level = may
smtp_tls_security_level = may
smtp_use_tls = no
...
```

Since we are configuring "submission" service which accepts connections, smtpd_tls_security_level should be used.

Plesk/Ubuntu /etc/postfix/master.cf:

```
...
smtp      inet  n       -       -       -       -       smtpd

smtps inet n - - - - smtpd -o smtpd_tls_wrappermode=yes

submission inet n - - - - smtpd
 -o smtpd_enforce_tls=yes
 -o smtpd_tls_security_level=encrypt
 -o smtpd_sasl_auth_enable=yes
 -o smtpd_client_restrictions=permit_sasl_authenticated,reject
 -o smtpd_sender_restrictions=
 -o smtpd_recipient_restrictions=
    permit_mynetworks,permit_sasl_authenticated,reject_unauth_destination
```

Das bedeutet im Klartext:

smtp = Port 25 :: Aktiviert (mit Standard-Werten)

smtps = Port 465 :: Aktiviert (ohne viel Config)

submission = Port 587 :: Für das Einreichen von E-Mails durch Clients auf Port 587 wird TLS-Verschlüsselung doch erzwungen!

Und wir haben somit keinen Handlungsbedarf mehr, solange Postfix in der Standard-Konfiguration von Plesk benutzt wird.

Was die Praxis zeigt

Internetseiten hier und hier listen auf, welche Provider welche Ports anbieten.

Die Fazit daraus:

- Allgemeiner Favorit für **IMAP** scheint **993** zu sein, 143 wird nur noch von wenigen Providern bevorzugt. Aber lesen Sie weiter... ☺
- Für **SMTP** sind **465** und **587** beide gängig, Aufgabe von Mails durch Mail Clients auf 25 ist längst verpönt.

Mail Display Agent: Courier oder Dovecot?

Bislang gab es mit Plesk nur Courier-IMAP als MDA (Mailserver), ab Plesk 12 kann man im Plesk-Installer stattdessen Dovecot auswählen – daraufhin entfernt Plesk Courier und installiert Dovecot, wobei die Meta-Daten über die Mailboxen, die Courier verwendet hatte, von einem Plesk-Script in Dovecot übernommen werden. Der Austausch des MDA hat in meiner Erfahrung keine Probleme verursacht – bis darauf, dass man das SSL-Zertifikat selber nachpflegen muss, was aber einfach geht.

Die Frage ist somit einfach, welches der beiden ist die bessere Wahl? Ein Artikel in Linux-Magazin testet gleich 4 MDA recht ausführlich und kommt zu folgender Bewertung:

"*So wie es allerdings zurzeit aussieht, ist mit Dovecot ein überaus ernst zu nehmender Konkurrent für alle drei Klassiker der IMAP-Szene auf den Plan getreten. Dovecot ist, verglichen mit den Konkurrenten, gut dokumentiert und verhältnismäßig leicht zu konfigurieren. Das indizierte Maildir und die Art der Implementierung gefallen durchaus. Es scheint fast, als sei seinem Erfinder der Brückenschlag von robustem Maildir zu performantem Index- und Datenbank-Ansatz gelungen.*

Eine Überarbeitung, die Dovecots indiziertes Maildir noch schneller machen soll, ist bereits erdacht und für Version 2.0 geplant. Dann müssen sich die Mitbewerber wohl wärmer anziehen. Die Sympathien der Open-Source-Gemeinde hat Dovecot wohl schon länger. Zumindest legt das eine schnelle Trendanalyse der Tester bei Google nahe".

Auch sonst im Netz liest man eine überwiegende Präferenz für Dovecot.

Und Plesk hat Dovecot nicht umsonst als Option aufgenommen:

"*We recommend that you use Dovecot instead of the default Courier IMAP server. Dovecot is faster, more secure, and it consumes fewer server resources and provides support for server-side mail filtering rules.*"

Dovecot konfigurieren

Mit Plesk 12.0.18 ist Dovecot in der Version 2.2.12 an bord.

Ferner:

"*You can customize Dovecot and Pigeonhole configuration to fit your specific needs the usual way — by adding custom configuration into /etc/dovecot/conf.d/*

Please read comments in /etc/dovecot/dovecot.conf for details."

SSL-Zertifikat nachladen

"*If you used SSL certificates with Courier IMAP, you can reuse them with Dovecot. To do this, take either /usr/share/pop3d.pem or /usr/share/imapd.pem file, and save it to /etc/dovecot/private/ under the name ssl-cert-and-key.pem. Make sure that the new file has the 0400 root:root permissions. After that restart the Dovecot service.*"

Weitere Infos auf der Dovecot-Website hier und hier.

Vorhanden in der Standard-Config

/etc/dovecot/dovecot.conf:
ssl_cert = </etc/dovecot/private/ssl-cert-and-key.pem
ssl_key = </etc/dovecot/private/ssl-cert-and-key.pem

/etc/dovecot/conf.d/10-plesk-security.conf:
disable_plaintext_auth = no

Unverschlüsselte Authentizierung abschalten

Plesk sorgt also vor dass SSL geht - erlaubt aber unverschlüsselte Authentizierung.

Das ändern wir, indem wir eine eigene Datei in /etc/dovecot/conf.d deponieren, die nach 10-plesk-security.conf ausgeführt wird und den Defaultwert "yes" von Dovecot wiederherstellt:

```
cd /etc/dovecot/conf.d
cat >50-custom-security.conf
disable_plaintext_auth = yes
^D
/etc/init.d/dovecot restart
```

Plesk für sicheren Mailverkehr einstellen

Mail Transfer Agent: Postfix statt Qmail

Qmail wird nicht weiterentwickelt, ihm fehlen Aspekte wie z.B. Anti-Spam / Anti-Virus Vorkehrungen, so dass er zunehmend von moderneren SMTP-Agenten wie Postfix. Seit Plesk 11 kann man Postfix über den Plesk-Installer als Alternative zu Qmail aus-

wählen – und das sollte man auch dringend tun; Plesk installiert immer nur ein SMTP-Agent, beim Wechsel wird der frühere entfernt:

- Install: Server | Plesk | Updates and Upgrades => Neuer Browser-Reiter
- Add/Remove Components | Mail hosting features | Different mailservers | Postfix

Der Umstieg ist schmerzlos – bis auf das vertraute Thema, dass das SSL-Zertifikat nachgepflegt werden muss – einfach nach /etc/postfix/postfix_default.pem kopieren.

Mit Postfix ist schon in der Standard-Konfiguration durch Plesk vorgesehen, dass unverschlüsselte Verbindungen zur Aufgabe neuer E-Mails ausgeschaltet ist, siehe oben Port 587 / Require TLS.

Mail Server Settings

In Plesk: Server | Tools & Settings | Mail | Mail Server Settings

- Enable mail management functions in Plesk (Häkchen, ist Standardwert)
- Maximum number of connections = 40 (entsprechend der Server-Nutzung anpassen; Std: C=40 Servers, D=1024 Users)
    - Courier: Maximum number of connections per IP address (Std: 40)
      Represents the maximum number of connections via the same protocol that the server will accept from the same IP address.
    - Dovecot: Maximum number of connections for a user per IP address (Std: 10)
      Represents the maximum number of connections via the same protocol that a mail user can establish from one IP address.
    - Fazit: Dovecot erlaubt eine genauere Kontrolle dieser Beschränkung!
    - Achtung: Dovecot „Max. connections for a user per IP“ ist mit 10 zu niedrig für IMAP-Konten mit vielen Ordnern und Zugriff von z.B. PC und Smartphone (via WLAN): Erhöhe auf z.B. 50.
- Enable message submission: Hinter dieser kryptischen Formulierung (Deutsch: Nachrichtenübermittlung aktivieren) wird geregelt, ob das Einreichen von Mails auf Port 587 erlaubt sein soll (per StartTLS). Da auch hier TLS erzwungen wird
- Relaying: authorization is required: SMTP (Standardwert)
- Wähle: Send from domain IP addresses and use domain names in SMTP greeting – siehe Plesk-Erklärung (in Plesk), aber auch hier, hier und hier!
- Used antivirus:
  Ich empfehle "Parallels Premium Antivirus" (muss ggf. extra lizensiert werden)
- Sonstige Standardwerte prüfen, ich fand sie in Ordnung.

Outgoing Mail Control

Zu Deutsch: Beschränkung der Anzahl ausgehender E-Mails einschalten. Dieses Feature ist neu in Plesk 12 - und sicherlich eine Reaktion auf die Notwendigkeit dafür. Daher sollte man es unbedingt auch nutzen!

Es handelt sich um die Möglichkeit, die Anzahl E-Mails, die pro Stunde geschickt werden können, zu begrenzen. Dies hindert effektiv, dass ein Server auf eine Blacklist kommt. Die Begrenzungswerte gibt es auf mehreren Ebenen:

- Server
- Einzelne Subscriptions
- Einzelne Domains
- Einzelne E-Mail-Adressen

Die Standardwerte für den Server werden zunächst auf allen Ebenen übernommen, da anfangs nirgends individuelle Werte eingegeben sind. Die Kunst ist, diese - eher knapp bemessene Werte - individuell anzupassen, an die tatsächliche Nutzung am Server. Sie sollen ausreichen für die übliche, legitime Nutzung - aber nicht viel höher als das liegen, damit sie ihren Job tun und Spammer erkennen.

Zum Beispiel: Ein E-Mail-Konto, das mittels Weiterleitungen als Mailingliste benutzt wird, braucht eine individuelle Einstellung die etwas höher liegt als die Anzahl Empfänger.

Das Feature muss erst in Plesk eingeschaltet werden:

Server | Tools & Settings | Mail | Mail Server Settings

und dort ein Häkchen setzen bei "Switch on limitations on outgoing email messages"

Konfiguriert wird es dann hier:

Server | Tools & Settings | Mail | Outgoing Mail Control

Die Anzeigen und Bedienerführung sind dort selbsterklärend.

- Auf dem Reiter "General" kann man über "Change Settings" die server-weiten Einstellungen anpassen.
- Auf dem Reiter "Email adresses" sieht man eine Übersicht aller Mailkonten.
- Die einzelnen Konten sind anklickbar, so erhält man Details zu dessen Nutzung und kann über "Change Limit" eine Custom-Einstellung für das Konto treffen.

Parallels Premium antivirus

Das Modul, das eigentlich eine Umverpackung des bekannten Dr. Web darstellt, kann wahlweise pro Mailkonto die ein- und/oder ausgehende Mails auf Viren prüfen.

Es soll jedenfalls gut sein, muss aber in mehreren Schritten aktiviert werden:

- Ggf. Plesk-Lizenz dafür besorgen und einspielen
- Ggf. in Plesk Installer die Komponente installieren
  Server | Plesk | Updates and Upgrades => Neuer Browser-Reiter
  Add/Remove Components | Mail hosting features | Parallels Premium antivirus
- In Plesk ggf. generell aktivieren:
  Server | Tools & Settings | Mail | mail Server Settings
  Antivirus settings: Parallels Premium Antivirus

- ABER DANN muss es für jedes vorhandene Mail-Konto extra eingeschaltet werden!
  [Power User View] Mail | Email Addresses
  Nacheinander auf jede (aktive) E-Mail Adresse klicken
  Am rechten Ende der Tab-Leiste ist hinter "Spam Filter" eine neuer Reiter "Antivirus" aufgetaucht.
  Darauf klicken und Häkchen setzen bei "Switch on antivirus protection for this email address".

Weitere Sicherheitsmassnahmen

Hier gibt es einen guten Blog-Beitrag. Und hier, wie man die Sicherheit so hochschraubt, dass der Server auch Kreditkartendaten beherbergen darf.

Wichtige Maßnahmen

Security Policy

In Plesk: Server | Security | Security Policy

- "Allow only secure FTPS connections"
- "Minimum password strength" = Strong / Very Strong

Fail2Ban

Schutz gegen Überschwemmungsangriffe („Brute Force Attacks“) – siehe Parallels dazu. Zuerst muss Fail2Ban installiert werden:

- Server | Plesk | Updates and Upgrades => Neuer Browser-Reiter
- Add/Remove Components | Mail hosting features | Fail2Ban authentication failure monitor

In Plesk:

- Server | Tools & Settings | IP Address Banning (Fail2Ban) | Settings
- Enable intrusion detection (Häkchen setzen)
- Sonst (erstmal) die Standardwerte übernehmen
- Reiter "Jails": Alle auswählen, dann "Switch On"

Watchdog

Siehe Parallels dazu:

"*The Watchdog extension is a solution that ensures that your server is clean from malware, all services are up and running and there is enough free disk space on the server.*"

Das wollen wir haben! Installieren:

- Server | Plesk | Updates and Upgrades => Neuer Browser-Reiter

- Add/Remove Components | Additional Plesk extensions | Watchdog (System monitoring extension)

In Plesk:

- Server Management | Extensions | Watchdog | Reiter "Services" | Enable
- Um einen bestimmten Service zu verwalten, auf seinen Namen klicken.
- Reiter "Security": WOW: "Scan your server for rootkits, backdoors, local exploits and other malicious code" START

Es scannt tatsächlich einiges auf dem Server - da schläft der SysAdmin ruhiger!

Update 2021: Nee, der hat doch Probleme gemacht (zu viel Last erzeugt, zu viel dazwischengefunkt, jetzt nutze ich Monit (auf dem er basierte) direkt in der Orginlaversion.

Optionale Maßnahmen

Firewall

Der Firewall ist eine Extension, die normalerweise geladen aber nicht aktiviert ist. Lesen Sie mehr dazu hier, hier, hier und hier!

Ich glaube langsam zu verstehen warum standardmäßig alles erlaubt ist: Wozu ein Port blockieren, hinter dem gar keine Software etwas entgegennimmt?

Stattdessen läuft Fail2Ban und fügt gezielt Regeln in die Kernel-IP-Tabelle ein, wo ein Angriff bzw. Missbrauch erkannt wird.

Insofern kann man wahrscheinlich tatsächlich auf die Aktivierung des "Firewalls" nun verzichten, solange kein besonderer Anlass dafür besteht. Ich habe selbst zwar einige Software-Systeme auf dem Server, aber sie sind alle als Websites realisiert (z.B. ownCloud, Mantis), die ganz normal über HTTP-Ports erreicht werden.

Achtung: Wer das Firewall aktiviert, muss anscheinend selber dafür sorgen, dass passives FTP wieder funktioniert!

Von daher habe ich schlussendlich doch auf die Firewall-Aktivierung verzichtet. Wer es dennoch machen will:

Wir müssen unterscheiden zwischen (a) Parallels Plesk Panel (PPP), und (b) das Virtuozzo Power Panel (VZPP). Es gibt anscheinend drei Möglichkeiten, den Zugang zum Server auf bestimmte IPs/Ports einzuschränken:

A) Firewall-Regeln auf der Ebene des "Containers" - Virtuozzo Power Panel (VZPP)

B) Firewall-Regeln innerhalb des "Containers", d.h.

1) Entweder der "Plesk Firewall" - Parallels Plesk Panel (PPP)

2) Oder manuelle Konfiguration der Linux-Kernel IP-Tabellen mittels /sbin/iptables

Der "Plesk Firewall" ist also nichts anderes als eine GUI (und DB-Einträge) zur bequemen Verwaltung von /sbin/iptables. Standardmäßig ist der Plesk Firewall nicht akti-

viert. Ich würde mich für B1 entscheiden, der Plesk Firewall - ich mache sonst nichts auf Container-Ebene, und manuelle Verwaltung ist zu aufwendig.

In Plesk: Server | Tools & Settings | Security | Firewall

Zur Aktivierung generiert Plesk einen Script. Zur Kontrolle dessen, was Plesk gemacht hat:

- man 8 iptables
- /etc/init.d/psa-firewall
- /opt/psa/var/modules/firewall/firewall-active.sh
- iptables -L

ModSecurity

Lesen Sie Parallels dazu:

„In order to detect and prevent attacks against web applications, the web application firewall (ModSecurity) checks all requests to your web server and related responses from the server against its set of rules. If the check succeeds, the HTTP request is passed to website content. If the check fails, the predefined actions are performed.

***ModSecurity is a module for Apache.** Thus, it can check only HTTP requests that reach Apache. Apache is supplemented with another web server - nginx. If you turn on the Process PHP by nginx option of the nginx web server for dynamic content of your website, the web application firewall will not be able to check HTTP requests because they will never reach Apache. For static content, if the Serve static files directly by nginx option is on, then HTTP requests will not reach Apache, so ModSecurity will not check them.“*

Da ich überall nur noch Nginx statt Apache einsetze, habe ich keine Erfahrung mit ModSecurity – glaube aber schon dass es gut wäre mit Apache.

Health Monitor

Das Modul fügt eine Art „Gesundheitsüberwachung“ hinzu, die eine laufende Überwachung der Dienste, Plattenplatz, Hauptspeicher- und Prozessornutzung sowie Netzwerkverfügbarkeit und -durchsatz leistet, Hierzu findet man im Netz geteilte Meinungen, auch hilfreiche Artikel.

Ich hatte es früher installiert aber einige Probleme damit gehabt, seitdem installiere es nicht mehr sondern verlasse mich auf meine eigene interne (Monit) und externe (Zabbix) Überwachung.

Webserver Configurations Troubleshooter

Diese Extension prüft auf Knopfdruck die Vollständigkeit und Richtigkeit von Webserver-Config-Dateien – sowohl für Apache als auch für Nginx. Sie kann über Plesk Installer nachgeladen und in Plesk aufgerufen werden. Nur sinnvoll wenn Sie Probleme im Bereich des Webserver-Konfigs haben, dann doch hilfreich.