Einleitung

Ausgangspunkt ist ein Univention Server Version 4.4-3 mit einem Kopano Server Version 8.7.1.0-1. Die E-Mail-Kommunikation soll zukünftig verschlüsselt erfolgen, wobei die Open Source Software CipherMail zum Einsatz kommen soll.

CipherMail bietet eine E-Mail-Verschlüsselung mittels PGP, S/MIME und PDF an und kann komfortabel über ein Webinterface administriert werden. Um die Änderungen am UCS möglichst gering zu halten und unabhängig von Updates/Upgrades des UCS zu sein, wird CipherMail in einer virtuellen Maschine auf dem UCS installiert.

Eine entsprechende virtuelle Maschine steht im vmdk Format als Download zur Verfügung und muss lediglich in das qcow2 Format konvertiert werden.

Danach wird die Konfiguration von Postfix auf dem UCS so geändert, dass ein- und ausgehende E-Mails die virtuelle Maschine mit CipherMail durchlaufen.

Voraussetzungen

Auf dem UCS wurden über das App Center die Anwendungen *Active Directory-kompatibler Domänen-Controller, Kopano Core, Fetchmail, KVM Virtualisierungsserver* und *UCS Virtual Machine Manager* installiert.

In der Benutzerverwaltung wurde mindestens ein Benutzer angelegt, der auch ein Kopano Benutzer ist und für den die E-Mail-Abholung mittels Fetchmail eingerichtet wurde.

Wenn der UCS als MX für die Domain betrieben wird, kann natürlich auf die Konfiguration von Fetchmail verzichtet werden.

Der UCS hat in dieser Dokumentation die IP-Adresse 192.168.0.242, die virtuelle Maschine die IP-Adresse 192.168.0.218, die im UCS hinterlegte Mail-Domain lautet *in-put.de* .

Kurze Steig 31
75179 Pforzheim
https://www.in-put.de/
kontakt@in-put.de
fon +49 (0) 72 31 / 44 07 85 - 0
fax +49 (0) 72 31 / 44 07 85 - 9

Installation der virtuellen Maschine

Die Installation der virtuellen Maschine erfolgt zunächst auf der Kommandozeile des UCS und beginnt mit dem Herunterladen und Entpacken der virtuellen Maschine, gefolgt von der Konvertierung in das qcow2 Format:

```
cd /tmp
wget https://www.ciphermail.info/downloads/ciphermail-community-virtual-appliance-4.6.2-0.zip
unzip ciphermail-community-virtual-appliance-4.6.2-0.zip
cd ciphermail-community-virtual-appliance-4.6.2-0/
qemu-img convert ciphermail-community-virtual-appliance-4.6.2-0-disk1.vmdk -O qcow2 \
/var/lib/libvirt/images/ciphermail-community-virtual-appliance-4.6.2-0.qcow2
```

Über das Webinterface des UCS (*System -> Virtuelle Maschinen (UVMM)*) wird die konvertierte virtuelle Maschine nun eingebunden.

Im *UCS Virtual Machine Manager* wählt man den Menüpunkt **Erstellen** und wählt danach **Erstellen einer neuen virtuellen Instanz** auf dem lokalen UCS.

Als Profil für die virtuelle Maschine wählt man die folgenden Einstellungen:

- Profil: Other (64 Bit)
- Name: CipherMail 4.6.2.0
- Größe des Arbeitsspeichers: 4096 MiB
- Anzahl der CPUs: 1
- Direktzugriff (VNC): aktiviert

Im nächsten Schritt wählt man **Hinzufügen -> Festplatte** und wechselt den Laufwerkstyp von *Erstellen einer neuen Image-Datei* auf *Auswahl einer vorhandenen Image-Datei*. Wenn die zuvor erstellte qcow2 Datei die einzige Image-Datei ist, wird sie direkt im DropDown-Menü *Laufwerk Image-Date*i angezeigt. Andernfalls muss sie hier ausgewählt werden.

Nachdem man die Konfiguration abgeschlossen hat, kann die virtuelle Maschine starten und über das Monitor Icon eine VNC Verbindung zur VM herstellen.

Kurze Steig 31
75179 Pforzheim
https://www.in-put.de/
kontakt@in-put.de
fon +49 (0) 72 31 / 44 07 85 - 0
fax +49 (0) 72 31 / 44 07 85 - 9

Innerhalb der VNC-Sitzung kann man sich am CentOS System mit dem Benutzer *sa* und dem Passwort *sa* anmelden.
Eine Anmeldung über das Netzwerk ist zu diesem Zeitpunkt noch nicht möglich. Nachdem Login in der VNC-Sitzung startet jedoch ein Konfigurationsmenü, in dem man unter *Config -> Network* die Netzwerkschnittstelle der virtuellen Maschine konfigurieren kann.

Danach sollte sowohl das Webinterface von CipherMail erreichbar sein, in unserem Beispiel unter der URL https://192.168.0.218:8443/ , als auch ein Login mit dem Benutzer sa via ssh möglich sein.

Konfiguration der virtuellen Maschine

Für die Konfiguration meldet man sich via SSH mit Benutzer sa an der virtuellen Maschine an, wählt im Konfigurationsmenü unter *File* den Eintrag *Open shell* und wechselt mittels **sudo su -** zu root.

Konfiguration der Firewall

Unter CentOS ist in der Standardinstallation die lokale Firewall aktiv, die jedoch die Kommunikation zwischen UCS und Ciphermail stört.

Der einfachste und schnellste Weg ist, die lokale Firewall komplett zu deaktivieren:

```
systemctl stop firewalld
systemctl disable firewalld
```

Alternativ schaltet man nur den Port 10025 frei, der es dem Postfix auf dem UCS ermöglicht, E-Mails an CipherMail weiterzuleiten:

```
firewall-cmd --zone=public  --add-port=10025/tcp --permanent
firewall-cmd --reload
```

In der Standard-Konfiguration befinden sich Postfix und CipherMail auf derselben Maschine, daher nimmt CipherMail Verbindungen nur auf der IP-Adresse 127.0.0.1 an und leitet E-Mails auch an diese IP-Adresse weiter.

Kurze Steig 31
75179 Pforzheim
https://www.in-put.de/
kontakt@in-put.de
fon +49 (0) 72 31 / 44 07 85 - 0
fax +49 (0) 72 31 / 44 07 85 - 9

Damit CipherMail auf der externen IP-Adresse 192.168.0.218 auf die vom UCS weitergeleiteten E-Mails wartet, ändert man die Datei */usr/share/djigzo/conf/james/SAR-INF/smtp_server_config.xml* wie folgt ab:

```
<port> 10025 </port>
<bind> 192.168.0.218 </bind>
<!--
        Default Einstellung
<bind> 127.0.0.1 </bind>
-->
```

Die von CipherMail bearbeiteten E-Mails müssen nun wieder an den Postfix auf dem UCS zurückgegeben werden. Dafür sorgt eine Änderung der Konfigurationsdatei */usr/share/djigzo/conf/james/SAR-INF/smtp_transport_config.xml:*

```
<!--
        Default Einstellung
<gateway> 127.0.0.1 </gateway>
-->
<gateway> 192.168.0.242 </gateway>
<gatewayPort> 10026 </gatewayPort>
```

Nun muss CipherMail noch mitgeteilt werden, dass die IP-Adresse des UCS vertrauenswürdig ist. Dies geschieht in der Datei *usr/share/djigzo/conf/james/SAR-INF/config.xml:*

```
<!--
        Default Einstellung
<authorizedAddresses> 127.0.0.0/8 </authorizedAddresses>
-->
<authorizedAddresses> 192.168.0.242/32 </authorizedAddresses>
```

Der Neustart von CipherMail aktiviert die Änderungen:

```
/etc/init.d/djigzo restart
```

/etc/security/packetfilter.d/50_local.sh

Kurze Steig 31
75179 Pforzheim
https://www.in-put.de/
kontakt@in-put.de
fon +49 (0) 72 31 / 44 07 85 - 0
fax +49 (0) 72 31 / 44 07 85 - 9

Konfiguration des Univention Corporate Server

Anpassen der Firewall-Konfiguration

Damit der UCS die von CipherMail weitergeleiteten E-Mails annimmt, ist der Port 10026 zu öffnen:

iptables -I INPUT 1 -p tcp --dport 10026 -s 192.168.0.218/32 -j ACCEPT

Damit diese Regel auch nach einem Neustart des UCS Bestand hat, trägt man sie in die Datei */etc/security/packetfilter.d/50_local.sh* ein.

Anpassen der Konfiguration von Postfix

CipherMail wird als so genannter Content Filter in Postfix eingebunden. Auf dem UCS ist jedoch bereits Amavis als Content Filter in Postfix eingebunden. Da es nur Sinn macht, eine entschlüsselte E-Mail auf Viren und Spam zu prüfen, deaktiviert man zunächst die Einbindung von Amavis in Postfix:

ucr set "mail/antivir"=no

Eine Einbindung von CipherMail als Content Filter ist über die UCR Variablen nicht vorgesehen. Für solch einen Fall hat Univention mit der Datei */etc/postfix/main.cf.local* eine Möglichkeit geschaffen, individuelle Änderungen an Postfix vorzunehmen. In diese Datei trägt man den Aufruf von CipherMail als Content Filter ein und aktiviert die Änderung:

content_filter=djizo:[192.168.0.218]:10025

ucr commit

Der Postfix auf dem UCS kann auch zunächst nichts mit den E-Mails anfangen, die von CipherMail zurückkommen, dazu sind Änderungen an der Datei */etc/postfix/master.cf* erforderlich. Auch diese Änderungen sind über das Webinterface oder das ucr Kommando nicht möglich, daher trägt man sie in die individuelle Änderungen vorgesehene Datei */etc/postfix/master.cf.local* ein:

```
djigzo  unix  -  -  n  -  4  smtp
  -o smtp_send_xforward_command=yes
  -o disable_dns_lookups=yes
  -o smtp_generic_maps=
```


Kurze Steig 31
75179 Pforzheim
https://www.in-put.de/
kontakt@in-put.de
fon +49 (0) 72 31 / 44 07 85 - 0
fax +49 (0) 72 31 / 44 07 85 - 9

```
:10026 inet n - n - 10 smtpd
  -o content_filter=
  -o receive_override_options=no_unknown_recipient_checks,no_header_body_checks,no_milters
  -o smtpd_helo_restrictions=
  -o smtpd_client_restrictions=
  -o smtpd_sender_restrictions=
  -o smtpd_relay_restrictions=
  -o smtpd_recipient_restrictions=permit_mynetworks,reject
  -o mynetworks=127.0.0.0/8,192.168.0.218/32
  -o smtpd_authorized_xforward_hosts=127.0.0.0/8,192.168.0.218/32
  -o smtpd_authorized_xclient_hosts=127.0.0.0/8,192.168.0.218/32
```

Auch diese Änderungen müssen aktiviert werden:

```
ucr commit
```

Damit ist die Konfiguration der beiden Systeme abgeschlossen. Durch den Aufruf des Befehls

```
tail -f /var/log/djigzo.log
```

auf dem CipherMail-System kann man sich davon überzeugen, dass die aus- und eingehenden E-Mails von CipherMail bearbeitet werden.

CipherMail und Amavis

Wie zuvor erwähnt, ist auf dem UCS bereits Amavis als Content Scanner installiert. Will man die von CipherMail entschlüsselten E-Mails an Amavis weiterleiten, um diese auf Viren und Spam zu prüfen, so sind weitere Änderungen erforderlich.

CipherMail konfiguriert man in */usr/share/djigzo/conf/james/SAR-INF/smtp_transport_config.xml* so, dass die E-Mails an Amavis und nicht Postfix geschickt werden:

```
<!--
        Default Einstellung
<gateway> 127.0.0.1 </gateway>
-->
<gateway> 192.168.0.242 </gateway>
<gatewayPort> 10024 </gatewayPort>
```


Kurze Steig 31
75179 Pforzheim
https://www.in-put.de/
kontakt@in-put.de
fon +49 (0) 72 31 / 44 07 85 - 0
fax +49 (0) 72 31 / 44 07 85 - 9

Amavis wartet auf der IP-Adresse 127.0.0.1 Port 10024 auf Verbindungen. Damit CipherMail E-Mails an Amavis weiterleiten kann, muss Amavis auf der externen IP-Adresse lauschen. Dazu editiert man die Datei */etc/univention/templates/files/etc/amavis/conf.d/60-univention* und sorgt auch gleich dafür, dass Amavis der IP-Adresse der virtuellen Maschine vertraut:

```
$inet_socket_bind = '192.168.0.242';
@inet_acl = qw( 127.0.0.1 192.168.0.218 );
```

Die Datei */etc/postfix/master.cf.local* sieht bei Verwendung von Amavis wie folgt aus:

```
smtp-amavis  unix  -  -  n  -  2  smtp
  -o smtp_data_done_timeout=1200
  -o smtp_send_xforward_command=yes
 -o disable_dns_lookups=yes

127.0.0.1:10025  inet  n  -  n  -  -  smtpd
  -o content_filter=
  -o local_recipient_maps=
  -o relay_recipient_maps=
  -o smtpd_restriction_classes=
  -o smtpd_client_restrictions=
  -o smtpd_helo_restrictions=
  -o smtpd_sender_restrictions=
  -o smtpd_recipient_restrictions=permit_mynetworks,reject
  -o mynetworks=127.0.0.0/8
  -o smtpd_authorized_xforward_hosts=127.0.0.0/8
  -o strict_rfc821_envelopes=yes
  -o smtpd_error_sleep_time=0
  -o smtpd_soft_error_limit=1001
  -o smtpd_hard_error_limit=1000
  -o receive_override_options=no_address_mappings
```

Abschließend sorgt man dafür, dass die durchgeführten Änderungen aktiviert werden:

```
ucr commit
```


Kurze Steig 31
75179 Pforzheim
https://www.in-put.de/
kontakt@in-put.de
fon +49 (0) 72 31 / 44 07 85 - 0
fax +49 (0) 72 31 / 44 07 85 - 9