



Bundesamt
für Sicherheit in der
Informationstechnik

ICC

JULIA MailOffice Betriebskonzept

ICC GmbH, 30.05.07

Version 2.0

Zusammenfassung

JULIA MailOffice ist ein System, das Verschlüsselung und Signatur von E-Mails an zentraler Stelle erlaubt. Als Gateway-Lösung kann JULIA MailOffice nahtlos in die bestehende Mail-Infrastruktur integriert werden. Dieses Dokument soll helfen, die notwendigen Voraussetzungen zu schaffen, damit JULIA MailOffice in den Regelbetrieb übernommen werden kann. Folgende für einen Regelbetrieb relevanten Aspekte werden behandelt:

- Planung der Infrastruktur
- Implementation von Hochverfügbarkeitsmechanismen
- Auswirkungen von JULIA MailOffice auf die bestehende Infrastruktur und die Konfiguration dieser Komponenten
- Systemvoraussetzungen
- Wichtige Betriebsaktivitäten

Die Installation von JULIA MailOffice ist in diesem Dokument *nicht* beschrieben.



© 2004 BSI Bundesamt für Sicherheit in der Informationstechnologie, Bonn
ICC GmbH, Köln

Version 2.0, Freigabe Juni 2005

Erstellt von:
ICC GmbH, Köln

Dieses Dokument kann bezogen werden über:
Bundesamt für Sicherheit in der Informationstechnik
Referat 111
Postfach 200363
D 53133 Bonn

E-Mail: vps@bsi.bund.de

ICC Solutions GmbH
Luxemburger Straße 79 - 83
D 50354 Hürth

Tel.: +49 (22 33) 9 46 96-0
Fax: +49 (22 33) 9 46 96-33
E-Mail: sales@iccsec.com

Weitere Informationen finden Sie unter:

<http://www.bsi.de/fachthem/vps>

<http://www.iccsec.com>

Inhaltsverzeichnis

| | |
|---|----|
| 1 Überblick..... | 1 |
| 2 Funktionalität von JULIA MailOffice..... | 2 |
| 2.1 Überblick..... | 2 |
| 2.2 Arbeitsweise von JULIA MailOffice..... | 3 |
| 2.3 Eingang verschlüsselter/signierter Mails (MailOffice-Modus)..... | 6 |
| 2.4 Eingang verschlüsselter/signierter Mails (Gateway-Modus)..... | 7 |
| 2.5 Versand verschlüsselter/signierter Mails | 8 |
| 2.6 Ermittlung der privaten Schlüssel ohne die VPS..... | 9 |
| 3 Implementationen von JULIA MailOffice..... | 11 |
| 3.1 Überblick..... | 11 |
| 3.2 Beispielumgebung für JULIA MailOffice und die VPS..... | 11 |
| 3.3 Alternativen zur Beispielumgebung..... | 13 |
| 3.3.1 Überblick..... | 13 |
| 3.3.2 JULIA MailOffice als externes Relay..... | 13 |
| 3.3.3 Betrieb eines Virens scanners und des internen Relays auf nur einem Server..... | 14 |
| 3.4 JULIA MailOffice als Gateway..... | 15 |
| 3.5 Hochverfügbarkeit..... | 16 |
| 3.5.1 Überblick..... | 16 |
| 3.5.2 Load-Balancing und Failover durch entsprechende MX-Records..... | 17 |
| 3.5.3 Verwendung von IP-Loadbalancer-Komponenten..... | 19 |
| 3.6 Firewall Konfiguration..... | 21 |
| 3.6.1 Überblick..... | 21 |
| 3.6.2 SMTP-Regeln..... | 21 |
| 3.6.3 LDAP(s)-Regeln..... | 21 |
| 3.6.4 HTTPS-Regeln..... | 21 |
| 3.6.5 Regeln für Extended Mail Header..... | 22 |
| 3.6.6 Besonderheiten bei Verwendung von Load-Balancern..... | 22 |
| 3.7 Änderungen der Konfigurationen der vorhandenen Mail-Server..... | 22 |
| 3.7.1 Überblick..... | 22 |
| 3.7.2 Änderungen an der Konfiguration des externen Relays..... | 23 |
| 3.7.3 Änderungen an der Konfiguration des Virens scanners..... | 23 |
| 3.7.4 Änderungen an der Konfiguration des internen Relays..... | 23 |
| 3.8 Anwendungsfälle..... | 24 |
| 3.8.1 Überblick..... | 24 |
| 3.8.2 Verwendung eines Behördenzertifikats..... | 24 |
| 3.8.3 Verwendung eines Behördenzertifikats und einiger benutzerbezogenen Zertifikate..... | 25 |
| 3.8.4 Verwendung von benutzerbezogenen Zertifikaten..... | 25 |
| 3.8.5 Implementierung für mehrere Mandanten..... | 26 |
| 3.8.5.1 Überblick..... | 26 |
| 3.8.5.2 Mehrere Mandanten auf verschiedenen Servern..... | 27 |
| 3.8.5.3 Mehrere Mandanten auf einem Server..... | 27 |
| 4 Inbetriebnahme von JULIA MailOffice..... | 30 |

| | |
|--|----|
| 4.1 Überblick..... | 30 |
| 4.2 Zu erfüllende Voraussetzungen..... | 30 |
| 4.2.1 Überblick..... | 30 |
| 4.2.2 Systemvoraussetzungen für das JULIA MailOffice-System..... | 30 |
| 4.2.2.1 Hardware..... | 30 |
| 4.2.2.2 Betriebssystem..... | 31 |
| 4.2.2.3 Weitere Software-Voraussetzungen..... | 31 |
| 4.2.2.4 Installation des VPS-Dispatchers..... | 31 |
| 4.2.2.5 Sicherungs- und Archivierungsmechanismen..... | 31 |
| 4.2.2.5.1 Konfiguration von JULIA MailOffice | 31 |
| 4.2.2.5.2 Protokolldaten..... | 32 |
| 4.2.2.6 Verfügbarkeit der Mailsysteme im DNS..... | 32 |
| 4.2.3 Organisatorische Voraussetzungen..... | 32 |
| 4.2.3.1 Klärung der datenschutzrelevanten Aspekte mit den entsprechenden Gremien..... | 32 |
| 4.2.3.2 Einrichtung eines Mail-Verteilers für die JULIA MailOffice-Administration..... | 33 |
| 4.3 Protokolldaten..... | 33 |
| 4.3.1 Ergebnisse der Zertifikatsprüfung..... | 33 |
| 4.3.2 Protokollierung der Aktivitäten von JULIA MailOffice..... | 34 |
| 4.4 Besondere Betriebsaktivitäten..... | 34 |
| 4.4.1 Überblick..... | 34 |
| 4.4.2 Anschauen der Mail-Queues von JULIA MailOffice | 34 |
| 4.4.3 Manuelle Zustellung von Mails..... | 35 |
| 4.4.4 Veröffentlichung eines Schlüssels..... | 35 |
| 4.4.5 Einem Zertifikat immer vertrauen..... | 35 |
| 4.4.6 Einem Zertifikat nie vertrauen..... | 35 |
| 4.4.7 Fehlersuche..... | 36 |
| 4.4.7.1 Überblick..... | 36 |
| 4.4.7.2 Prüfung des Mail-Routings..... | 36 |
| 4.4.7.3 Prüfung des VPS-Dispatchers..... | 36 |
| 4.4.7.4 Prüfung der Erreichbarkeit des Kernsystems..... | 36 |
| 4.4.7.5 Prüfung des Status des Kernsystems..... | 36 |
| 4.4.7.6 Prüfung der Operation IDs..... | 37 |
| 4.4.8 Protokoll-Information von JULIA MailOffice..... | 37 |
| 4.4.9 Protokoll-Informationen des VPS-Dispatchers..... | 37 |
| 5 Literatur..... | 38 |

Abbildungsverzeichnis

| | |
|--|----|
| Abbildung 1 Eingang verschlüsselter/signierter Mails (MailOffice-Modus)..... | 6 |
| Abbildung 2 Eingang verschlüsselter/signierter Mails (Gateway-Modus)..... | 7 |
| Abbildung 3 Versand verschlüsselter/signierter E-Mail..... | 8 |
| Abbildung 4 Mechanismen zur Ermittlung privater Schlüssel..... | 9 |
| Abbildung 5 Beispielumgebung von JULIA MailOffice zusammen mit der VPS..... | 10 |
| Abbildung 6 JULIA MailOffice als externes Relay..... | 13 |
| Abbildung 7 Virens Scanner und internes Mail-Relay zusammengefasst..... | 14 |
| Abbildung 8 JULIA MailOffice als Gateway..... | 15 |
| Abbildung 9 Verwendung mehrerer MX-Records..... | 17 |
| Abbildung 10 Einsatz eines Load-Balancers..... | 17 |
| Abbildung 11 Einsatz mehrerer Ketten..... | 18 |

1 Überblick

JULIA MailOffice ist ein zentraler Verschlüsselungs- und Signaturproxy für die kryptographische Behandlung ein- und ausgehender E-Mails und operiert als eigenständiges SMTP-Gateway. JULIA MailOffice kann deshalb nahtlos in eine bestehende SMTP-Umgebung integriert werden. Die Installation von JULIA MailOffice ist in [JULIA 02/2003] beschrieben, an dieser Stelle wird darauf deshalb nicht eingegangen. In diesem Dokument werden für den Betrieb von JULIA MailOffice relevante Aspekte beschrieben.

In Abschnitt 2 wird die Funktionalität von JULIA MailOffice beschrieben. Mögliche Implementierungen von JULIA MailOffice, insbesondere hochverfügbar ausgelegte Systeme, werden in Abschnitt 3 beschrieben. Voraussetzungen für eine Inbetriebnahme von JULIA MailOffice sowie besondere Betriebsaufgaben im Regelbetrieb, wie zum Beispiel

- Manuelle Weiterleitung von E-Mails
- Einem abgelaufenen Zertifikat vertrauen
- Starten und Stoppen des VPS-Dispatchers

sind in Abschnitt 4 beschrieben.

2 Funktionalität von JULIA MailOffice

2.1 Überblick

JULIA MailOffice kann sowohl stand-alone als auch zusammen mit der Virtuellen Poststelle (VPS) eingesetzt werden. Wird JULIA MailOffice nicht stand-alone sondern zusammen mit der VPS betrieben, werden alle kryptographischen Operationen, wie zum Beispiel "verschlüsseln einer Mail", "Prüfung von Zertifikaten", etc. vom Kernsystem der VPS durchgeführt. Die Funktionsweise von JULIA MailOffice ist in beiden Varianten gleich, jedoch bestehen Unterschiede in der Betriebsumgebung. Damit unterscheiden sich auch die Mechanismen für die Verwaltung der Komponenten, die von JULIA MailOffice benutzt werden. Die wichtigsten Unterschiede sind in nachfolgender Tabelle zusammen gefasst.

| <i>Komponente</i> | <i>JULIA MailOffice stand-alone</i> | <i>JULIA MailOffice zusammen mit der VPS</i> |
|--|--|---|
| Schlüsselverwaltung | Liegt innerhalb von JULIA MailOffice | Liegt im Kernsystem und OCSP-/CRL-Relay der VPS |
| Zertifikat-Prüfung | Liegt innerhalb von JULIA MailOffice | Liegt im Kernsystem und OCSP-/CRL-Relay der VPS |
| OCSP-/CRL-Relay | Kann mit Hilfe des JULIA MailOffice Moduls 'moducc' via SOAP angebunden werden | Wird vom Kernsystem via Document Interface angesprochen |
| VPS-Dispatcher | Wird nicht benötigt | Wird für Kommunikation mit dem Kernsystem der VPS benötigt |
| Regelwerk für Mails | Liegt innerhalb von JULIA MailOffice | Liegt innerhalb von JULIA MailOffice |
| Rudimentäre Verwaltungsfunktionen für eine PKI | Die Web-Administrationsschnittstelle kann für diesen Zweck verwendet werden | Müssen mit Hilfe separater Werkzeuge implementiert oder in das Kernsystem der VPS integriert werden |
| Auto-CA | Steht zur Verfügung | Steht nicht zur Verfügung da Schlüssel und Zertifikate in der VPS verwaltet werden |

2.2 Arbeitsweise von JULIA MailOffice

JULIA MailOffice ist in einen Mail Transfer Agent (MTA) eingebettet. Beim Empfang einer E-Mail wird JULIA MailOffice aufgerufen und unten angegebener Workflow abgearbeitet. "Externe Aktivitäten" sind die Aktivitäten, die nicht vom JULIA MailOffice-Kern sondern von den JULIA MailOffice-Modulen ausgeführt werden.

1. Empfang der E-Mail
2. Ermittlung der Transportrichtung:
 1. Internet -> Unternehmen
 1. Externe Aktivität:: Ermittlung der benötigten Schlüssel
 2. Externe Aktivität: Prüfung der Zertifikate
 3. Externe Aktivität: Gegebenenfalls Entschlüsselung
 4. Weiterleitung der Mail an internes Relay
 2. Unternehmen -> Internet
 1. Darf Mail transportiert werden? Automatische Verschlüsselung und/oder Signatur darf nur von den Mailsystemen aus verwendet werden, die in JULIA MailOffice als intern definiert sind.
 2. Externe Aktivität: Für jeden Empfänger: Ermittlung der benötigten Schlüssel
 3. Externe Aktivität: Für jeden Empfänger: Prüfung mit Hilfe des Regel-Moduls von JULIA MailOffice, ob Signatur/Verschlüsselung notwendig oder gewünscht ist.
 4. Externe Aktivität: Für jeden Empfänger: Ermittlung und Prüfung der Zertifikate
 5. Abhängig vom Regelwerk und den Ergebnissen der Zertifikatprüfung gegebenenfalls Versand der E-Mail(s)

Der Workflow ist unabhängig von der eingesetzten Verschlüsselungstechnologie und den Prüffunktionen.

Die externen Aktivitäten werden von separaten Komponenten (JULIA MailOffice-Modulen) implementiert. Die Kommunikation zwischen dem JULIA MailOffice-Kern und den JULIA MailOffice-Modulen erfolgt mit Hilfe von XML.

Um verschlüsselte Mails auf Viren prüfen zu können, müssen diese zunächst entschlüsselt werden. Dazu muss JULIA MailOffice Zugriff auf die entsprechenden Schlüsselpaare (öffentliche und private Schlüssel der Benutzer) haben. Diese werden im Kernsystem der VPS verwaltet. JULIA MailOffice fordert die benötigten Objekte und Operationen beim Kernsystem mit Hilfe des so genannten VPS-Dispatchers an. Der VPS-Dispatcher ist ein eigenständiger, multi-threaded Server, der Anfragen von JULIA MailOffice entgegennimmt und an das Kernsystem der VPS weiterleitet. Die Antworten und Ergebnisse nimmt der VPS-Dispatcher vom Kernsystem entgegen und stellt sie JULIA MailOffice zur Verfügung.

Wird JULIA MailOffice ohne die VPS eingesetzt, stehen folgende Mechanismen zur Verfügung:

- Bezug der Schlüsselpaare von einem LDAP-Server oder einer ähnlichen Backend-Komponente (HSM, Datenbank, etc.)
- Bezug des öffentlichen Schlüssels vom lokalen Dateisystem
- Bezug des zugehörigen privaten Schlüssels von einer Crypto-Card oder einem anderen externen Gerät (Smart Card, PDA, Memory-Stick, etc.)

Die privaten Schlüssel können sowohl durch ein Passwort geschützt als auch ungeschützt gespeichert werden.

In den folgenden Abschnitten sind die einzelnen Schritte für den Versand und den Empfang verschlüsselter Mails durch JULIA MailOffice dargestellt sowie die beteiligten Komponenten beschrieben.

Senden von verschlüsselten Mails Schickt ein Benutzer eine Mail an einen Empfänger außerhalb des Unternehmens, wird diese Mail über den Mail-Server (MTA) des Unternehmens geführt. Dieser MTA sendet die Mail ohne weitere Prüfung an den Empfänger.

Empfang verschlüsselter Mails Empfangene verschlüsselte Mails werden über einen zentralen Mail-Server geführt. Dort wird die erste JULIA MailOffice-Komponente als Mail-Programm gestartet. Um die Mail entschlüsseln zu können, wird der private Schlüssel des Empfängers ermittelt. Dieser ist im Kernsystem der VPS angelegt. Wird JULIA MailOffice Stand-alone eingesetzt, befindet sich der private Schlüssel entweder in einer Datei im lokalen Dateisystem, in einem LDAP-Server oder auf einer Crypto-Card abgelegt.

JULIA MailOffice zusammen mit der VPS:

Alle vom Kernsystem implementierten Mechanismen für die Verwaltung von privaten Schlüsseln können verwendet werden. JULIA MailOffice bezieht diese mit Hilfe des VPS-Dispatchers bei Bedarf. Tritt beim Bezug eines privaten Schlüssels ein Fehler auf (Schlüssel nicht verfügbar, etc.), meldet dies das Kernsystem. Der VPS-Dispatcher leitet die Fehlermeldung weiter an JULIA MailOffice.

JULIA MailOffice stand-alone:

JULIA MailOffice kann den für die Entschlüsselung der Mail benötigten privaten Schlüssel aus einer Datei oder von einem LDAP-Server direkt beziehen. Befindet sich der Schlüssel auf einer Crypto-Card, wird die zu entschlüsselnde Mail von JULIA MailOffice "zwischengelagert". Der Empfänger erhält eine Mail mit der Aufforderung, die Karte in das Lesegerät einzuführen und anschließend auf einen in der Mail angegebenen Link zu klicken. Durch Klicken auf diesen Link wird ein Applet gestartet, das den privaten Schlüssel des Empfängers liest.

Die entschlüsselte Mail wird dem Viren-Scanner zugeführt. Enthält die Mail keine Viren wird sie

zugestellt. Abhängig von der Konfiguration von JULIA MailOffice wird diese Mail unverschlüsselt oder verschlüsselt ausgeliefert. Soll sie verschlüsselt an den Empfänger ausgeliefert werden, wird das verschlüsselte Original an den Empfänger gesendet. Es ist auch möglich, die Mail unverschlüsselt an den Empfänger auszuliefern, sofern die Mailsysteme sich in einer entsprechend abgesicherten Zone befinden und der unverschlüsselte Versand als solcher nicht bereits als Verlust der Vertraulichkeit eingestuft wird.

2.3 Eingang verschlüsselter/signierter Mails (MailOffice-Modus)

Der MailOffice-Modus ist der "normale" Betriebsmodus von JULIA MailOffice. Die Aufgabe von JULIA MailOffice in diesem Modus ist, eingehende Mails falls erforderlich zu entschlüsseln und ausgehende Mails bei Bedarf zu signieren und/oder zu verschlüsseln.

Die Abbildung 1 zeigt den Ablauf beim Eingang einer verschlüsselten und/oder signierten Mail. Eine Mail wird vom außen liegenden SMTP-Relay entgegengenommen. JULIA MailOffice entschlüsselt die Mail und prüft falls erforderlich die Signatur. Die benötigten Objekte wie Zertifikate und/oder private Schlüssel werden von der VPS bezogen. Danach leitet JULIA MailOffice die unverschlüsselte Mail an ein internes Mail-Relay weiter.

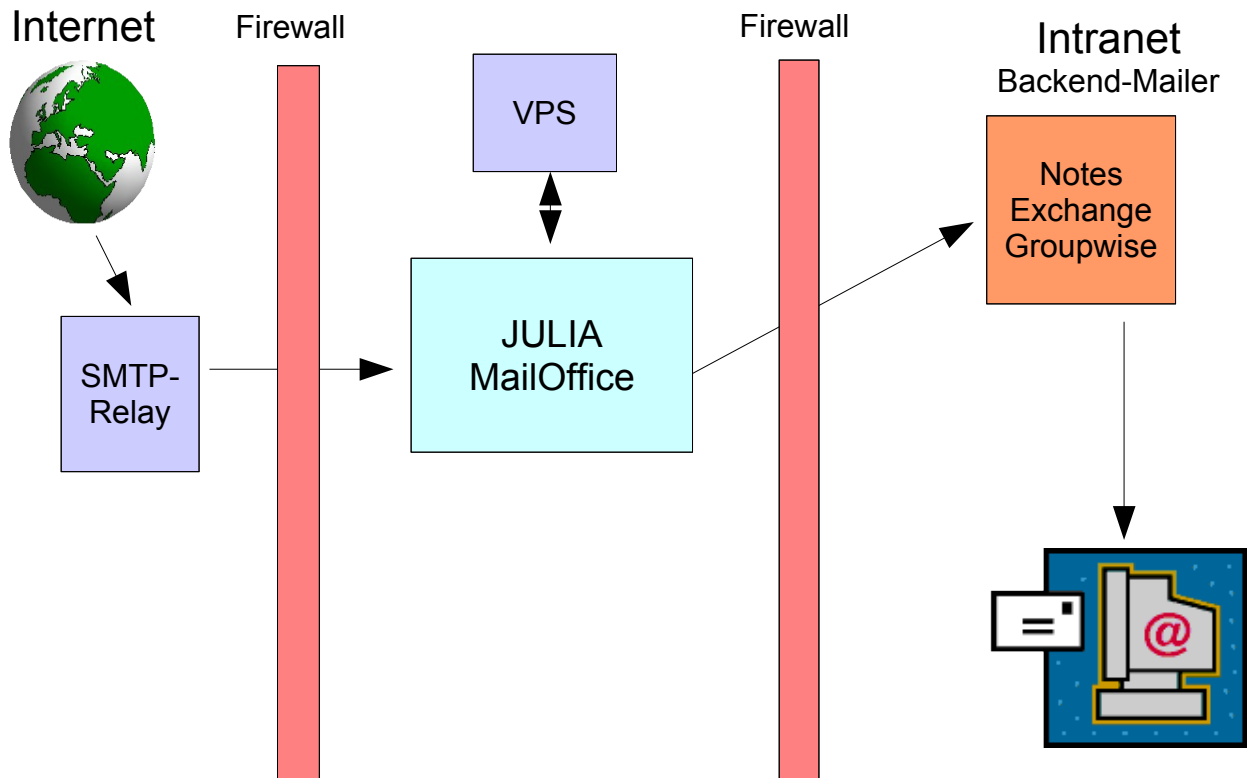


Abbildung 1 Eingang verschlüsselter/signierter Mails (MailOffice-Modus)

2.4 Eingang verschlüsselter/signierter Mails (Gateway-Modus)

Der "Gateway-Modus" von JULIA MailOffice ist eine spezielle Betriebsart, in der JULIA MailOffice die Hauptaufgabe hat, eingehende Mails auf Viren prüfen zu lassen.

Die Abbildung 2 zeigt den Ablauf beim Eingang einer verschlüsselten und/oder signierten Mail.

Eine Mail wird vom außen liegenden SMTP-Relay entgegengenommen. JULIA MailOffice entschlüsselt die Mail und prüft falls erforderlich die Signatur. Die privaten Schlüssel und Zertifikate werden von der VPS bezogen. Danach leitet JULIA MailOffice die unverschlüsselte Mail an den Virenschanner zur Prüfung weiter. Ist die Prüfung der Mail erfolgreich, leitet der Virenschanner die unverschlüsselte Mail an die internen Mailsysteme weiter. Durch entsprechende Konfiguration kann JULIA MailOffice auch veranlasst werden, die verschlüsselte Originalmail an die internen Systeme zu schicken (siehe [JULIA 2003/02]).

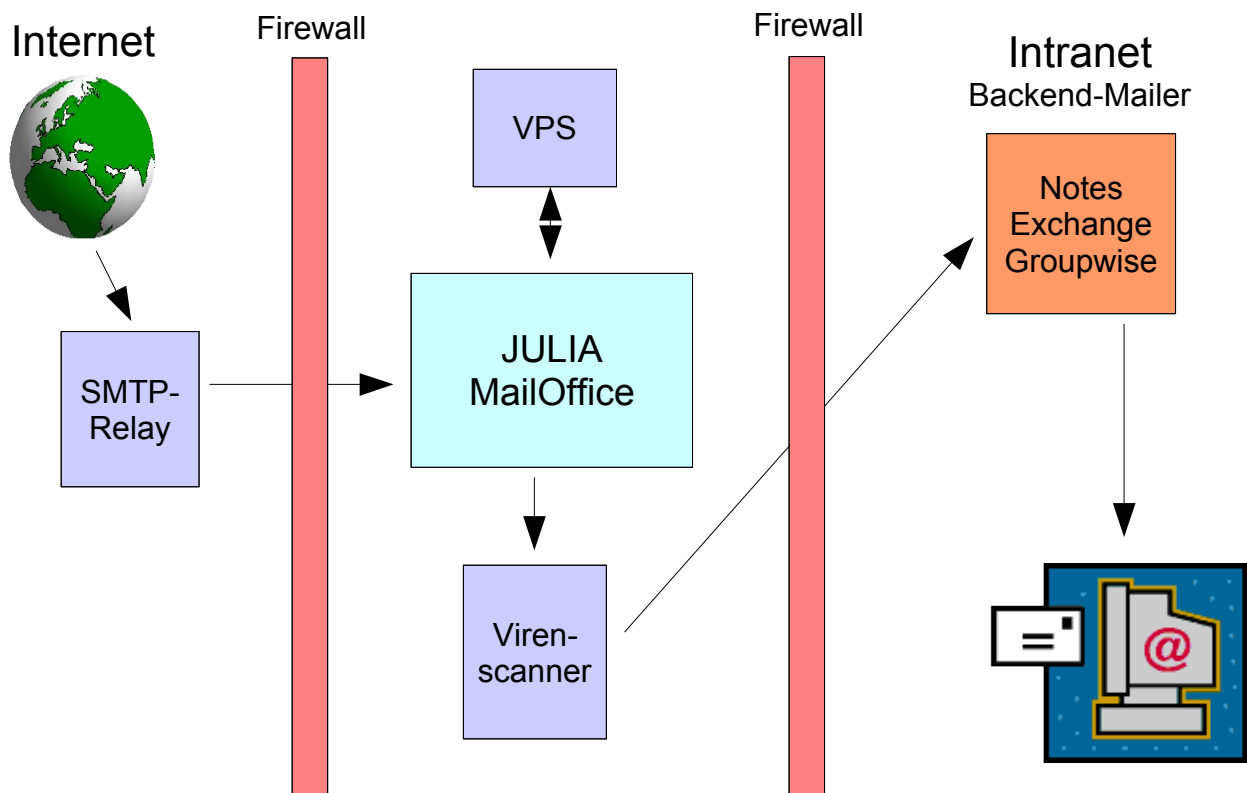


Abbildung 2 Eingang verschlüsselter/signierter Mails (Gateway-Modus)

2.5 Versand verschlüsselter/signierter Mails

Der Versand verschlüsselter und/oder signierter E-Mail ist in Abbildung 3 beschrieben. Eine Mail wird über die internen Systeme an den Virenschanner geschickt. Enthält die Mail keine Viren, wird sie an JULIA MailOffice zur weiteren Bearbeitung weitergeleitet. Anhand des Regelwerks und/oder der Betreffzeile der Mail entscheidet JULIA MailOffice, ob diese Mail verschlüsselt und/oder signiert werden muss. Abhängig von der entsprechenden Konfiguration bezieht JULIA MailOffice für die Entscheidung, ob eine Mail verschlüsselt oder signiert werden soll, die Betreffzeile der aktuellen Mail und ihr statisches Regelwerk ein. Dabei kann einer der beiden Mechanismen oder es

können beide Mechanismen verwendet werden (siehe [JULIA 2003/02]). Danach wird die Mail gegebenenfalls verschlüsselt und signiert und zur endgültigen Zustellung an das SMTP-Relay weitergeleitet. Schlüssel und Zertifikate werden jeweils von der VPS bezogen.

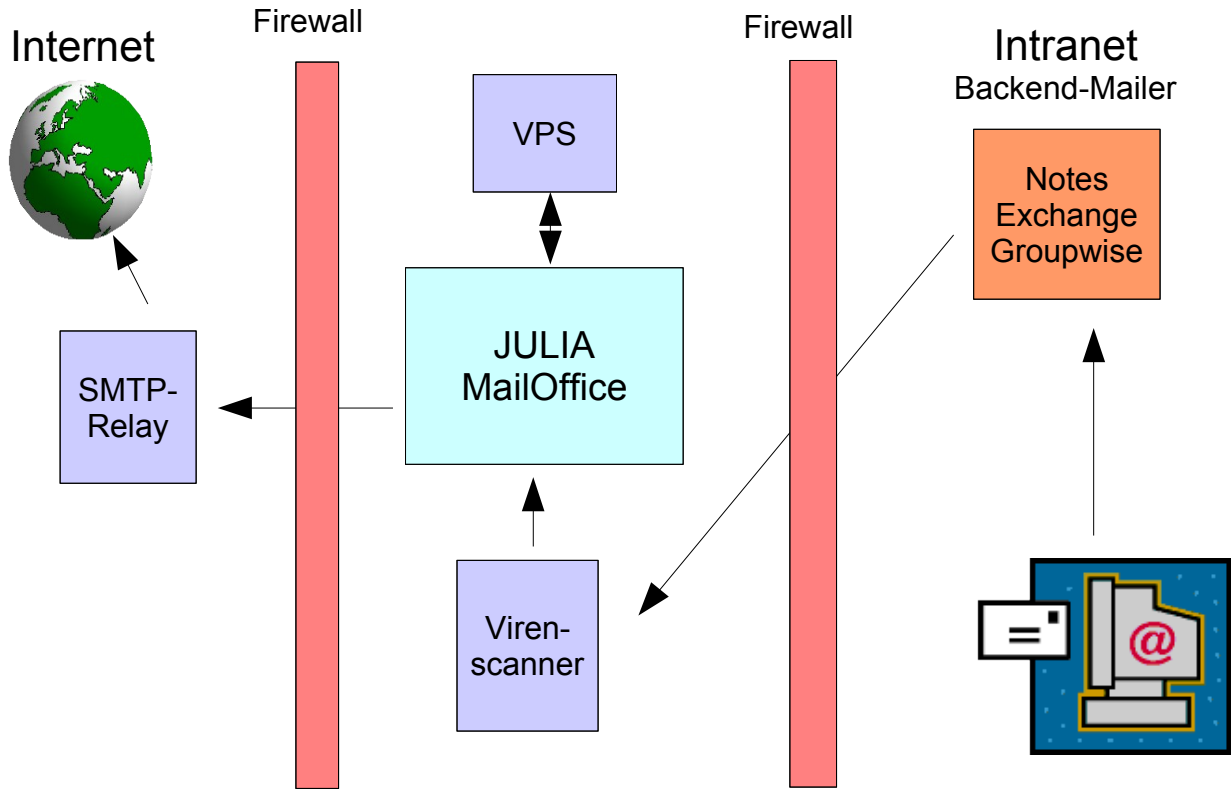


Abbildung 3 Versand verschlüsselter/signierter E-Mail

2.6 Ermittlung der privaten Schlüssel ohne die VPS

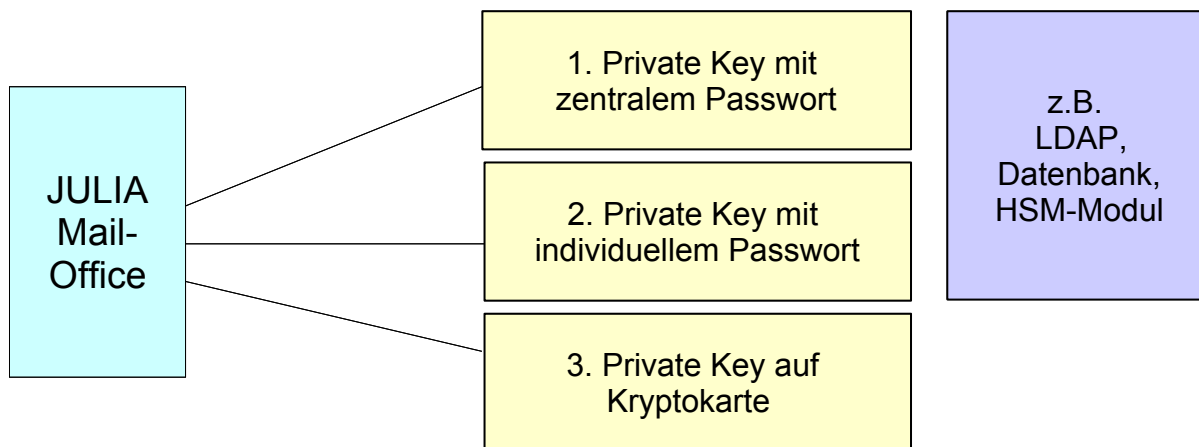


Abbildung 4 Mechanismen zur Ermittlung privater Schlüssel

Die Abbildung 4 zeigt die verschiedenen Varianten zur Speicherung und Ermittlung der privaten Schlüssel.

Variante 1: Speicherung der privaten Schlüssel, die alle durch ein zentral hinterlegtes Passwort gesichert sind.

In diesem Fall kennt JULIA MailOffice das Passwort und kann die Schlüssel, ohne mit dem Anwender in Interaktion treten zu müssen, verwenden. Die Schlüssel können im Dateisystem, auf einem LDAP-Server, in einer Datenbank oder einem HSM abgelegt werden. Der Zugriff auf die Speichermedien wird durch entsprechende JULIA MailOffice-Module implementiert.

Variante 2: Speicherung der privaten Schlüssel, die durch individuelle Passwörter gesichert sind.

Werden individuelle Passwörter für die Absicherung der privaten Schlüssel verwendet, muss JULIA MailOffice mit dem Benutzer in Interaktion treten. Dies geschieht mit Hilfe eines Web-Formulars. Benötigt JULIA MailOffice zum Beispiel für die Signatur einer Mail den privaten Schlüssel eines Benutzers, erhält dieser eine Mail, die einen Link auf ein Web-Formular enthält. Dort wird der Benutzer aufgefordert, das Passwort einzugeben. Der private Schlüssel wird so für JULIA MailOffice nutzbar und anschließend für die Signatur der Mail verwendet. Auch bei dieser Variante können die Schlüssel im Dateisystem, auf einem LDAP-Server, in einer Datenbank oder einem HSM abgelegt werden.

Variante 3: Speicherung der privaten Schlüssel auf Cryptokarten.

Auch bei dieser Variante muss JULIA MailOffice in Interaktion mit dem Schlüsselbesitzer in Interaktion treten. Der Benutzer erhält eine Mail, die einen Link auf ein signiertes Applet enthält. Durch Anwählen dieses Links wird das Applet gestartet, das den Datenstrom zwischen JULIA MailOffice, der Arbeitsstation und dem dort angeschlossenen Kartenleser kontrolliert.

3 Implementationen von JULIA MailOffice

3.1 Überblick

In den folgenden Abschnitten werden mögliche Implementationen von JULIA MailOffice beschrieben. Auch die verschiedenen Varianten für die Speicherung der privaten Schlüssel so wie hochverfügbar ausgelegte Systeme werden beschrieben.

3.2 Beispielumgebung für JULIA MailOffice und die VPS

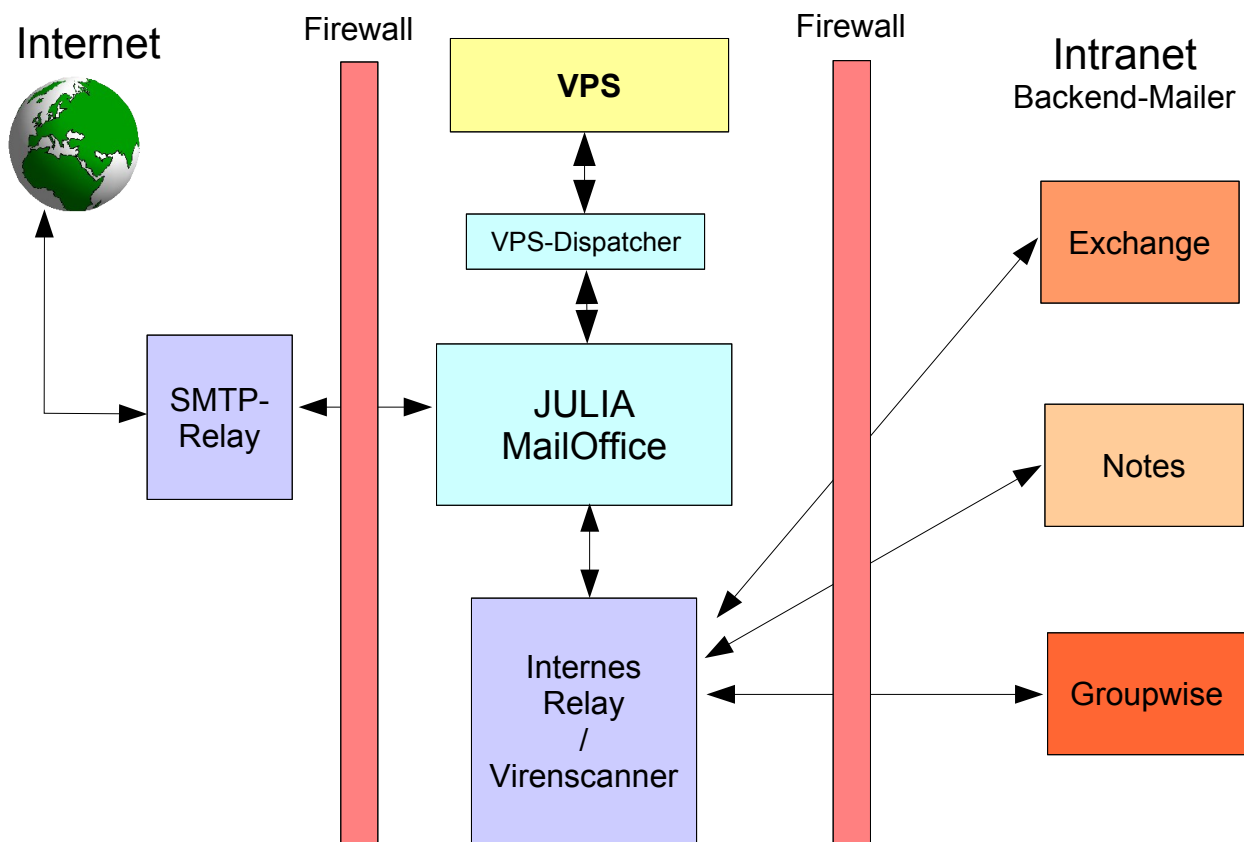


Abbildung 5 Beispielumgebung von JULIA MailOffice zusammen mit der VPS

Abbildung 5 zeigt schematisch eine Beispielumgebung für Mailsysteme. Üblicherweise werden Mails aus dem Internet durch ein entsprechendes SMTP-Relay entgegengenommen. Auf diesem dem Internet zugewandten Relay werden zum Beispiel Komponenten betrieben wie

- SPAM-Filter
- Mail-Blocker

Sowohl das Kernsystem der VPS als auch JULIA MailOffice steht in einer durch zwei Firewalls gesicherten Zone. So ist das System vor nicht autorisierten Zugriffen sowohl von innen als auch von außen geschützt. Wenn verschlüsselte Emails auf Viren geprüft werden sollen, werden diese Mails von JULIA MailOffice entschlüsselt und unverschlüsselt zur Prüfung an den Virenschanner weitergeleitet. Aus diesem Grund muss sich der für die Virenprüfung zuständige Server in der selben Zone wie JULIA MailOffice selbst befinden. Die Entschlüsselungsoperation wird mit Hilfe des VPS-Dispatchers veranlasst und vom Kernsystem durchgeführt. Der VPS-Dispatcher kann auf jedem beliebigen Rechner innerhalb der selben Zone betrieben werden. Da es sich bei dem VPS-Dispatcher um einen eigenständigen multi-threaded Server handelt, der in Java implementiert ist, werden alle Plattformen unterstützt, auf der eine Java-Laufzeitumgebung der Version 1.4.02 oder aktueller betrieben werden kann. Muss JULIA MailOffice eine kryptographische Operation durchführen (zum Beispiel eine ausgehende Mail verschlüsseln), richtet JULIA MailOffice diese Anfrage an den VPS-Dispatcher. Dieser verbindet sich mit dem Kernsystem der VPS über das so genannte Document Interface.

Im inneren Bereich können verschiedene Mailsysteme, wie zum Beispiel

- Exchange
- Notes
- Groupwise

eingesetzt werden. Wichtige Voraussetzung ist jedoch, dass diese die Mails zwischen dem internen Relay (bzw. Virenschanner) und JULIA MailOffice via SMTP transportiert werden. Zwischen Virenschanner und den Backend-Mailern können auch andere Mail-Protokolle als SMTP eingesetzt werden.

JULIA MailOffice selbst wird in einen SMTP-Server eingebettet und von diesem als so genannter "local-Mailer" aufgerufen. Dieser SMTP-Server agiert als "Trägersystem" und muss sich auf einer Linux- oder Solaris-Plattform befinden. Wird von diesem SMTP-Server eine Mail transportiert, ruft dieser für den eigentlichen Transport JULIA MailOffice auf. Für die aktuell zu bearbeitende Mail führt JULIA MailOffice die notwendigen Aktionen durch und terminiert danach wieder. JULIA MailOffice verschickt selbst keine Mails sondern ruft stattdessen neue Instanzen des SMTP-Servers auf. Für jedes der drei möglichen Ziele

- Externes Relay
- Virenschanner
- Internes Relay

existieren eigene Konfigurationsdateien. Zur Zeit werden folgende SMTP-Server unterstützt:

- Sendmail und
- Postfix.

3.3 Alternativen zur Beispielumgebung

3.3.1 Überblick

Die in Abschnitt 3.2 beschriebene Beispielumgebung stellt die maximale Ausbaustufe dar. Die Infrastruktur kann vereinfacht werden, indem einige Komponenten zusammengelegt werden. Mögliche Varianten sind in den folgenden Abschnitten beschrieben.

3.3.2 JULIA MailOffice als externes Relay

Soll JULIA MailOffice als externes Relay eingesetzt werden, fällt das äußere Relay weg. Der Nachteil dieser Vorgehensweise ist, dass bei dieser Architektur SPAM-Mails auf den JULIA MailOffice-Server gelangen, wenn keine weiteren vorgelagerten Filter verwendet werden. Das bedeutet, dass eine höhere Last auf dem JULIA MailOffice-Server erzeugt wird und dieser so potentiell einer größeren Gefährdung von Denial-of-Service-Attacken unterliegt. Die Abbildung 6 zeigt diese Variante.

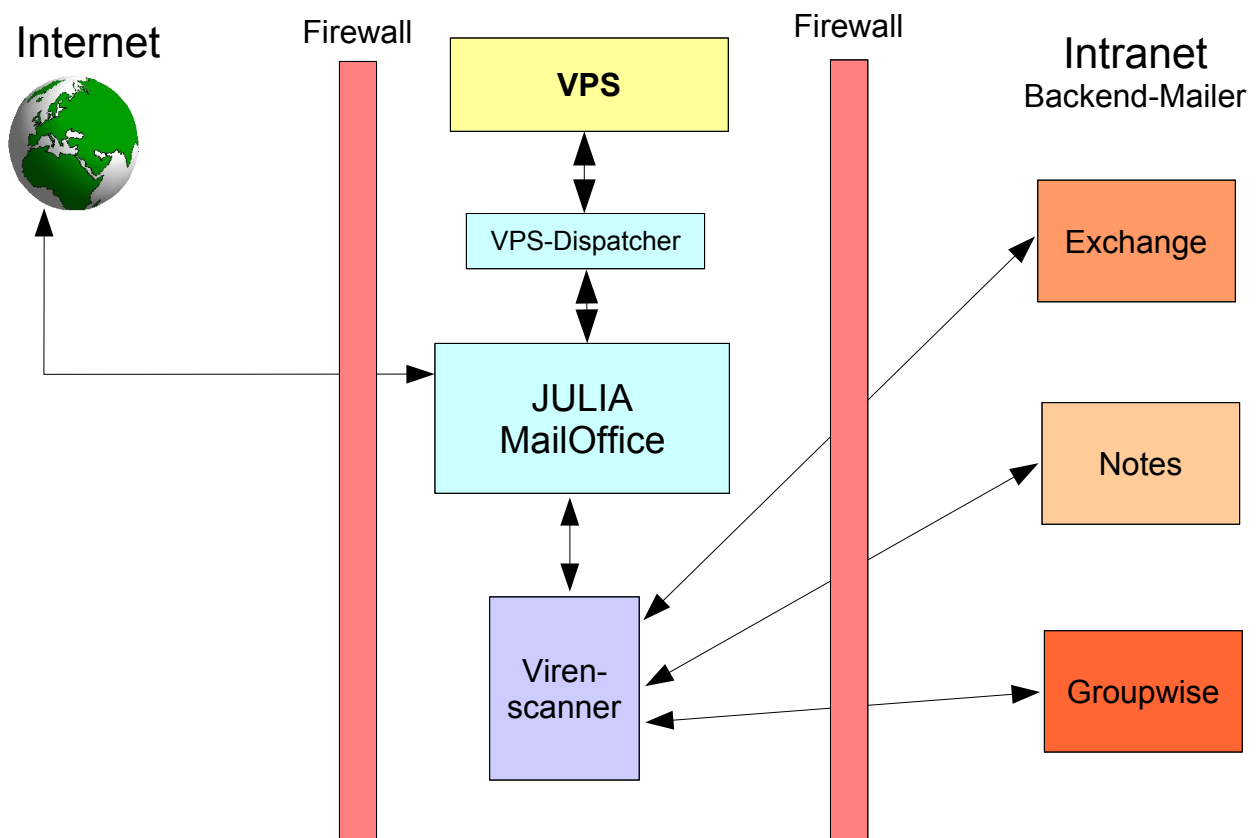


Abbildung 6 JULIA MailOffice als externes Relay

3.3.3 Betrieb eines Virencanners und des internen Relays auf nur einem Server

Mails werden von JULIA MailOffice an ein internes Mail-Gateway gesendet. Ist dieses Gateway ein Virencanner, leitet dieser als nicht gefährlich eingestufte Mails wiederum an das innere Mail-Relay weiter. Es liegt daher nahe, den Virencanner und das innere Mail-Relay zusammenzufassen und auf der selben Hardware zu betreiben.

Auch in dieser Variante werden die kryptographischen Operationen vom Kernsystem der VPS durchgeführt und mit Hilfe des VPS-Dispatchers angestoßen.

Diese Variante kann nur gewählt werden, wenn die eingegangenen verschlüsselten Mails unverschlüsselt im Unternehmen ausgeliefert werden sollen. Besteht die Forderung, dass verschlüsselt gesendete Mails verschlüsselt an die Empfänger ausgeliefert werden sollen, müssen Virencanner und internes Relay voneinander getrennt werden (siehe Abschnitt "JULIA MailOffice als Gateway"), damit verschlüsselt eingegangene Mails nur innerhalb der Mail-Zone unverschlüsselt verschickt werden. Abbildung 7 zeigt die Variante mit zusammengefasstem Virencanner und internem Relay.

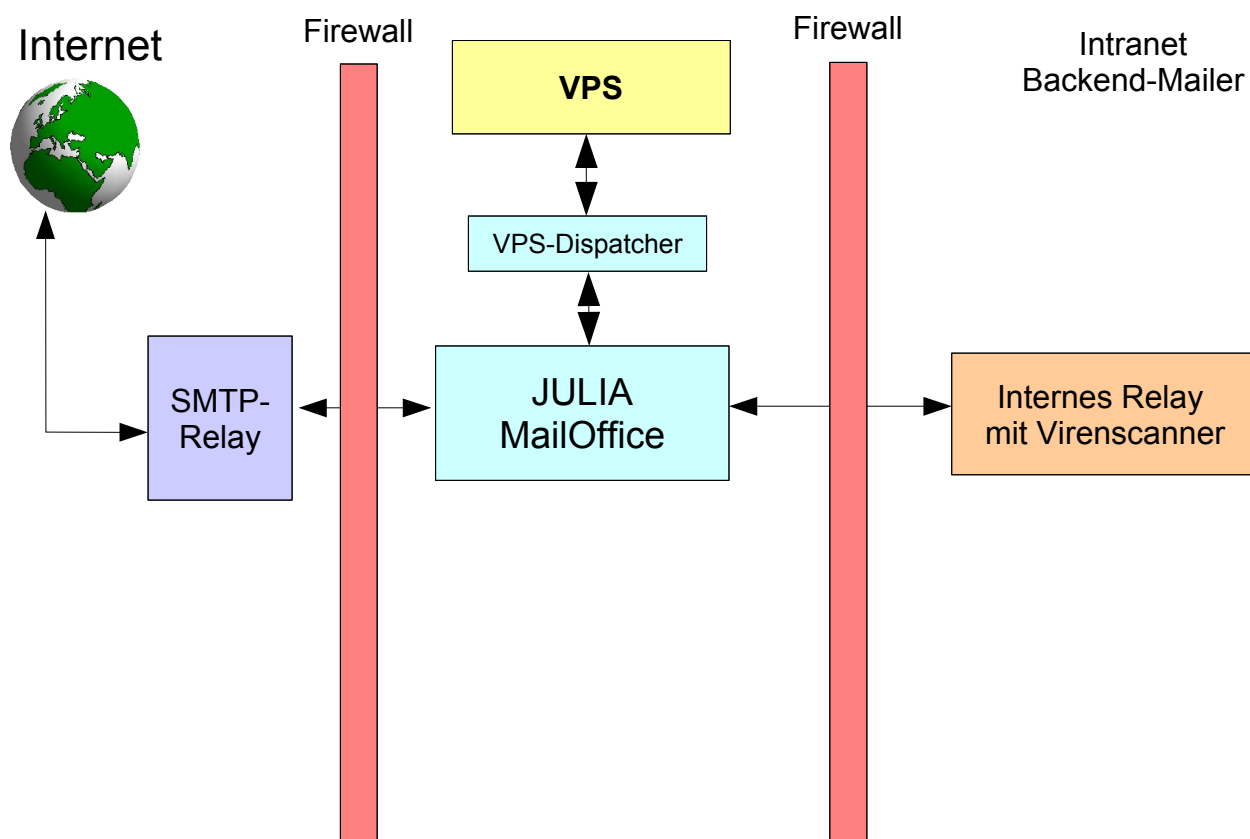


Abbildung 7 Virencanner und internes Mail-Relay zusammengefasst

3.4 JULIA MailOffice als Gateway

In der Variante "JULIA MailOffice als Gateway" ist die Hauptaufgabe von JULIA MailOffice, verschlüsselte Mails entgegen zu nehmen, an einen Virenschanner zu schicken und Mails mit ungefährlichem Inhalt an einen internen Mail-Server weiterzuleiten. Abhängig von der Konfiguration kann JULIA MailOffice die Mails an den internen Mail-Server wie folgt senden:

- Die Mails werden unverschlüsselt nach innen gesendet.
- Mails werden von JULIA MailOffice mit einem eigenen Schlüssel erneut verschlüsselt.
- JULIA MailOffice leitet die verschlüsselte Original-Mail weiter.

Kryptographische Operationen, wie zum Beispiel Entschlüsselung einer Mail, Signatur einer Mail, etc. werden vom Kernsystem der VPS durchgeführt. Der VPS-Dispatcher leitet entsprechende Anfragen von JULIA MailOffice an die VPS weiter und sendet deren Antwort an JULIA MailOffice zurück.

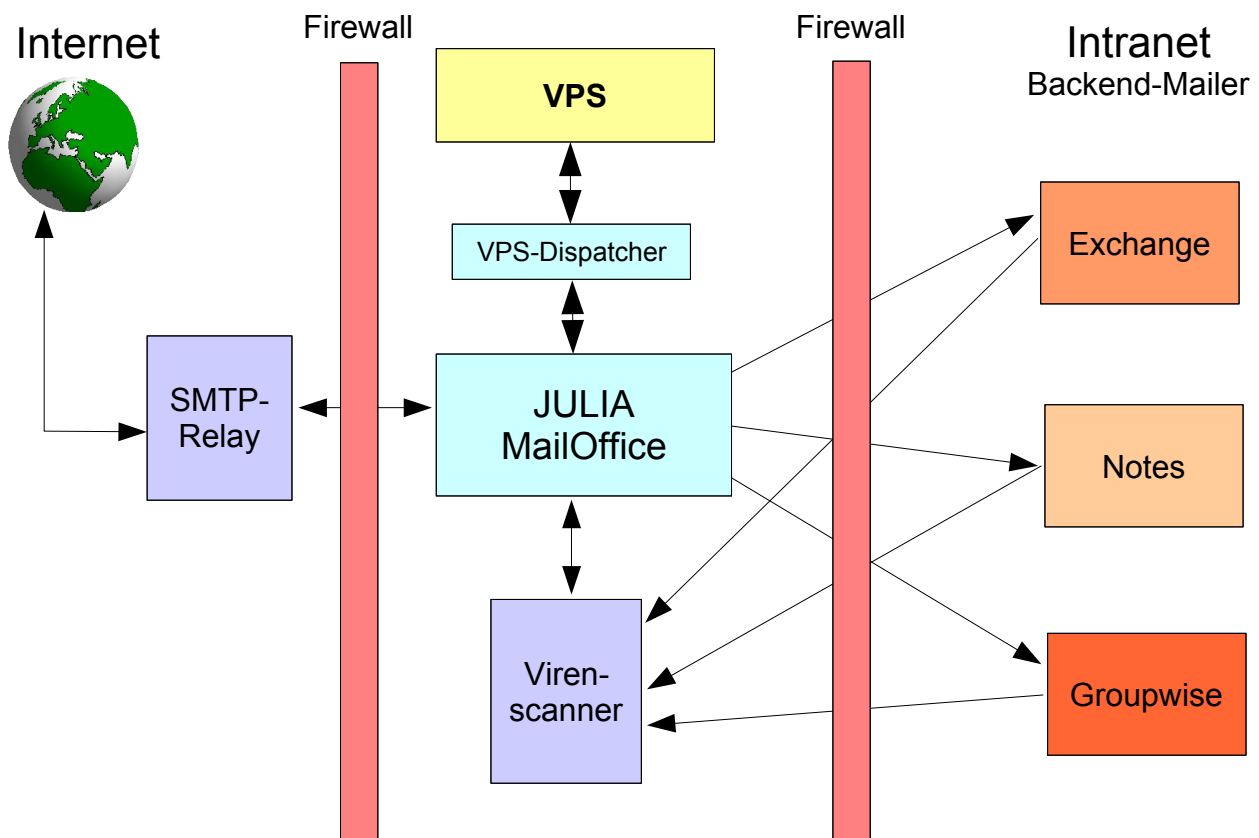


Abbildung 8 JULIA MailOffice als Gateway

3.5 Hochverfügbarkeit

3.5.1 Überblick

Um die Verfügbarkeit des Mail-Systems zu erhöhen, können mehrere JULIA MailOffice-Server parallel eingesetzt werden. Es können zwei Ansätze verfolgt werden:

- Verwendung entsprechender MX-Records in den Name-Servern
- Verwendung von Load-Balancer-Komponenten und Betrieb von JULIA MailOffice im Cluster

Beide Ansätze sind in den folgenden Abschnitten beschrieben.

Jeder JULIA MailOffice-Server in einem Cluster wird als Knoten bezeichnet. Die Synchronisation zwischen den Julia-MailOffice-Knoten sowohl der Konfigurationsdaten als auch der Zertifikate, Schlüssel, etc. kann zeitgesteuert erfolgen oder vom Webfrontend aus angestoßen werden. Jeder der einzelnen JULIA MailOffice-Knoten enthält die kompletten Konfigurationsdaten des JULIA MailOffice-Clusters und kann als Ausgangspunkt für die Verteilung der Daten innerhalb des Clusters dienen. Auf diese Art und Weise wird kein Master benötigt, was die Ausfallsicherheit erhöht. Mögliche Implementationen eines JULIA MailOffice-Clusters sind in den Abbildungen 10 und 11 dargestellt. Zu beachten ist, dass auch die Komponenten VPS-Dispatcher, die VPS und der Virenschanner hoch-verfügbar ausgelegt werden müssen, damit keine Single-Point-Of-Failure existieren.

3.5.2 Load-Balancing und Failover durch entsprechende MX-Records

Damit ein Server Mails zustellen kann, müssen den Empfänger-Domains entsprechende Mail-Server zugeordnet werden. Dies geschieht durch entsprechende Einträge, so genannte MX-Records, im verwendeten Name-Server (DNS). Ein MX-Record besitzt folgenden Aufbau:

MX <IP-Adresse> <Priorität> <Domain>

Die IP-Adresse ist die Adresse des Mail-Servers, der für die genannte Domain die Mails verarbeiten soll. Der Wert für "Priorität" ist eine natürliche Zahl. Je kleiner diese Zahl ist, desto höher ist die Priorität für den entsprechenden Mail-Server, für die angegebene Domain den Mailverkehr zu behandeln. Werden für eine Domain mehrere MX-Records angegeben, wird der Mailverkehr in Abhängigkeit der gewählten Prioritäten für die einzelnen Mail-Server auf diese verteilt. Sind die Werte für die Prioritäten für alle Server gleich, erhalten alle Server gleich viele Mails.

Vorteile:

- Es wird keine zusätzliche Hardware neben den Mail-Servern benötigt.
- Komplexität des IP-Routings bleibt gleich

Nachteile:

- Man muss Zugriff auf den entsprechenden Name-Server haben

- Unter Umständen hohe Latenz bei Konfigurationsänderungen: Soll ein Mailserver aus der Verarbeitung herausgenommen werden, muss der entsprechende MX-Record aus der Name-Server-Konfiguration entfernt und dieser "durchgestartet" werden. Die Propagierung der veränderten Daten zu anderen Name-Servern kann mehrere Minuten und sogar Stunden dauern.

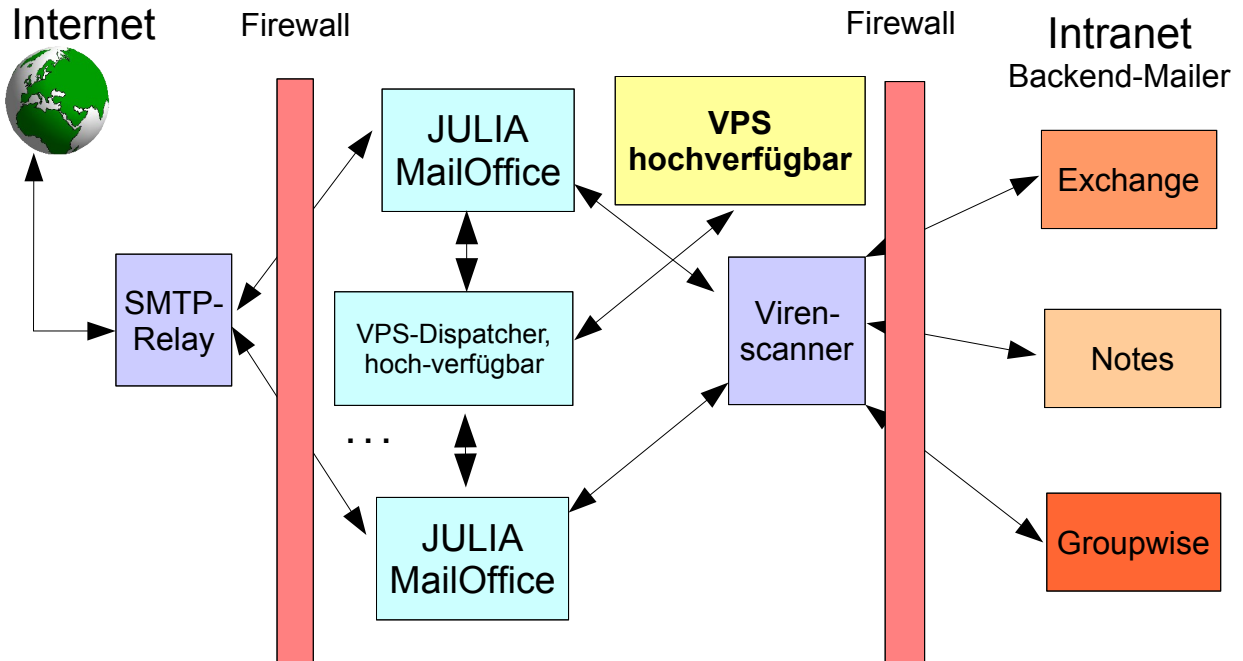


Abbildung 9 Verwendung mehrerer MX-Records

3.5.3 Verwendung von IP-Loadbalancer-Komponenten

Die Abbildung 10 zeigt einen Aufbau unter Verwendung eines Load-Balancers. Damit der Load-Balancers seinerseits keinen Single-Point-Of-Failure darstellt, ist dieser hochverfügbar auszulegen. Das selbe gilt sowohl für den VPS-Dispatcher als auch für die VPS.

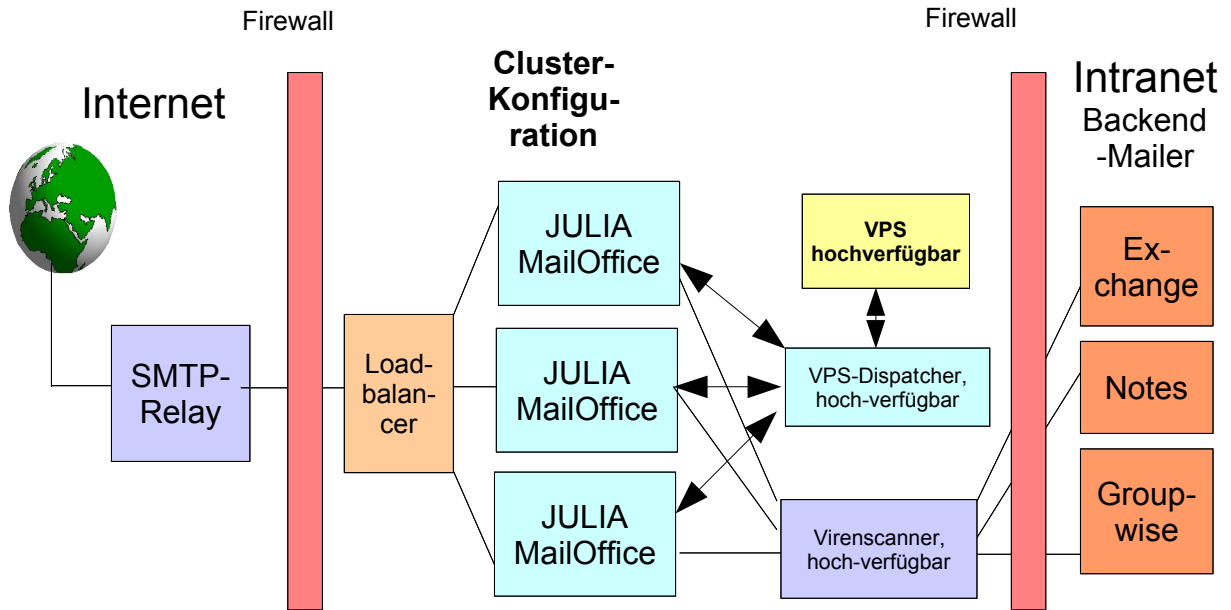


Abbildung 10 Einsatz eines Load-Balancers

In der Abbildung 10 sind nur die JULIA-MailOffice-Server mehrfach vorhanden und die Komponenten Virens scanner, VPS-Dispatcher und VPS hoch verfügbar. Bei hoher Last ist es sinnvoll, die Virens scanner ebenfalls auf mehrere Server zu verteilen werden, so dass mehrere JULIA-Virens scanner-Ketten implementiert werden. Diese Variante ist in Abbildung 11 dargestellt.

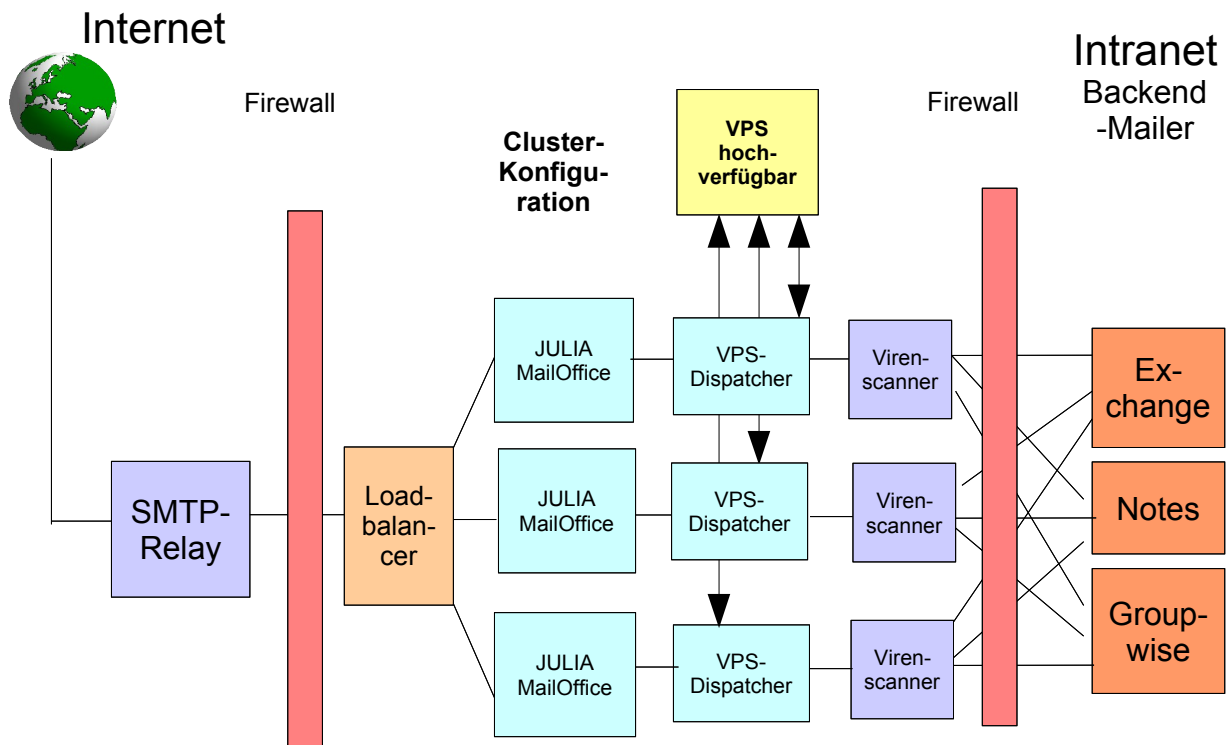


Abbildung 11 Einsatz mehrerer Ketten

Vorteile:

- Generische Lösung: Load-Balancer können auch für andere Protokolle als SMTP eingesetzt werden
- Automatisches Fail-Over: Die meisten Load-Balancer-Komponenten prüfen die Erreichbarkeit der angeschlossenen Komponenten. So ist es im Störfall nicht notwendig, in die Konfiguration manuell einzugreifen. Nicht erreichbare Server werden vom Load-Balancer nicht mehr angesteuert.

Nachteile:

- Für die Load-Balancer wird zusätzliche, hochverfügbare Hardware benötigt.
- Die Komplexität des IP-Routings steigt: Alle von einem Load-Balancer angesteuerten Server liegen in einem separaten logischen Netzwerk.
- Die Komplexität der Firewall-Regeln steigt: Auf den Load-Balancern müssen eigene Regeln implementiert werden

3.6 Firewall Konfiguration

3.6.1 Überblick

Da JULIA MailOffice mit sensitiven Daten operiert, muss das System besonders geschützt werden. Insbesondere wenn sich die privaten Schlüssel im lokalen Dateisystem des JULIA MailOffice-Servers befinden, müssen besondere Vorkehrungen getroffen werden. JULIA MailOffice wird daher in einer durch Firewalls geschützten Zone betrieben. Die zu JULIA MailOffice bestehenden Kommunikationsbeziehungen müssen im Regelwerk dieser Firewall-Systeme berücksichtigt werden. Möglicherweise betroffene Firewall-Regeln sind in den Abschnitten 3.6.2 bis 3.6.5 beschrieben.

3.6.2 SMTP-Regeln

Ein- und ausgehende Mails werden von JULIA MailOffice mit Hilfe von SMTP transportiert. Folgende Kommunikationsbeziehungen bestehen im allgemeinen:

- Internes Relay -> JULIA MailOffice SMTP
- Externes Relay -> JULIA MailOffice SMTP
- JULIA MailOffice -> Virenschanner SMTP
- Virenschanner -> Internes Relay SMTP oder anderes
 Mail-Protokoll

3.6.3 LDAP(s)-Regeln

Werden die Zertifikate in einem LDAP-Server gespeichert, besteht folgende Kommunikationsbeziehung:

- JULIA MailOffice -> LDAP-Server LDAP(s)

3.6.4 HTTPS-Regeln

Sowohl für die Konfiguration von JULIA MailOffice als auch bei der Interaktion mit Benutzern, zum Beispiel bei der Ermittlung der privaten Schlüssel für die Signierung einer Mail, wird eine Web-Anwendung verwendet. Folgende Kommunikationsbeziehungen bestehen:

- Arbeitsstation(en) Administration -> JULIA MailOffice HTTPS
- Arbeitsstationen der Benutzer -> JULIA MailOffice HTTPS

3.6.5 Regeln für Extended Mail Header

JULIA MailOffice legt während der Verarbeitung der Mails Informationen in den Extended-Mail-Header-Feldern ab. Einige Firewall-Systeme erlauben, Extended-Mail-Header-Felder aus dem Datenstrom zu entfernen. Damit soll erreicht werden, dass die Infrastruktur des Unternehmens nach außen hin verborgen wird. Befindet sich zum Beispiel der Virens Scanner nicht in derselben Zone wie JULIA MailOffice, müssen die betroffenen Firewalls so konfiguriert werden, dass Extended-Mail-Header-Felder nicht entfernt werden.

3.6.6 Besonderheiten bei Verwendung von Load-Balancern

Werden Load-Balancer-Komponenten für JULIA MailOffice eingesetzt, befinden sich die JULIA MailOffice-Server in einem separaten Netzwerk "hinter" dem Load-Balancer. Das bedeutet, dass anstatt der JULIA MailOffice-Server der Load-Balancer als Quelle oder Ziel in den Firewall-Regeln auftreten.

Auf den Load-Balancern selbst müssen entsprechende Routen gesetzt und NAT-Mechanismen konfiguriert werden, damit die JULIA MailOffice-Server mit den anderen Mail-Komponenten kommunizieren können.

3.7 Änderungen der Konfigurationen der vorhandenen Mail-Server

3.7.1 Überblick

Soll das JULIA MailOffice in eine vorhandene Infrastruktur integriert werden, hat dies einige Auswirkungen auf die Konfiguration der bereits existierenden Mail-Komponenten. Zum Beispiel muss das externe Relay Mails zum Entschlüsseln an JULIA MailOffice weiterleiten, die internen Relays müssen zu verschlüsselnde oder zu signierenden Mails ebenfalls an JULIA MailOffice senden. Mögliche Änderungen der vorhandenen Mail-Komponenten sind in den folgenden Abschnitten beschrieben.

3.7.2 Änderungen an der Konfiguration des externen Relays

Damit eingehende Mails entschlüsselt werden können, müssen diese an JULIA MailOffice geschickt werden. Außerdem muss das externe Relay so konfiguriert werden, dass es Mails von JULIA MailOffice annimmt.

3.7.3 Änderungen an der Konfiguration des Virens Scanners

Werden ausgehende Mail auf Viren geprüft, so wird ohne JULIA MailOffice entweder der Virens Scanner die Mails direkt an die Empfänger verschicken oder mit Hilfe des externen Relays an

die Empfänger zustellen. Die Konfiguration des Virenschanners ist so zu ändern, dass dieser die Mails in jedem Fall zunächst an JULIA MailOffice schickt.

3.7.4 Änderungen an der Konfiguration des internen Relays

Werden ausgehende Mails auf Viren geprüft, werden die Mails zunächst an den Virenschanner weitergeleitet. In diesem Fall ist keine Änderung vorzunehmen.

Werden ausgehende Mails direkt verschickt, müssen diese über JULIA MailOffice geführt werden. Besser ist jedoch, auch ausgehende Mails auf Viren zu prüfen und die Mails an den Virenschanner zu schicken.

Im Normalfall erhält das interne Relay eingehende Mails vom Virenschanner. Für verschlüsselte Mails bedeutet dies, dass diese entschlüsselt zum internen Relay und zu den Empfängern geschickt werden. Ist dies nicht erwünscht, muss JULIA MailOffice die Originalmail, sofern diese vom Virenschanner als ungefährlich eingestuft wurde, an das interne Relay schicken. Das interne Relay muss so konfiguriert sein, dass es Mails von JULIA MailOffice annimmt.

3.8 Anwendungsfälle

3.8.1 Überblick

In den folgenden Abschnitten werden folgende Anwendungsfälle für die Implementierung von verschlüsselter E-Mail in einer Behörde und deren Auswirkung auf die Konfiguration von JULIA MailOffice betrachtet:

- Verwendung eines Behördenzertifikats
- Verwendung eines Behördenzertifikats und einiger benutzerbezogenen Zertifikate
- Verwendung von benutzerbezogenen Zertifikaten

3.8.2 Verwendung eines Behördenzertifikats

Im einfachsten Fall wird ein einziges Zertifikat für die gesamte Behörde verwendet. Kommunikationspartner erhalten den öffentlichen Schlüssel und können so mit der Behörde kommunizieren. Innerhalb der Behörde kann jeder eine verschlüsselte Mail entschlüsseln, auch wenn sie nicht an ihn gerichtet ist. Diese Variante ist für Behörden interessant, die mit geringstem Aufwand automatisch signierte Mails verschicken möchten, zum Beispiel um so "authentische Mails" von nicht-authentischen Mails unterscheiden zu können.

Die Regeldatei von JULIA MailOffice für den Anwendungsfall "Verwendung eines Behördenzertifikats" nur für die Signatur sieht wie folgt aus:

```
#
# Julia Rules
#
#
# From          To          Rules
#-----
.                (to) .          (do) FS@mail@behoerde.de
```

Unabhängig vom Absender oder Empfänger einer Mail (". (to) .") wird die Signatur der Mail mit dem Schlüssel von "mail@behoerde.de" signiert. Für diesen Anwendungsfall werden keine Backend-Mechanismen, wie zum Beispiel LDAP-Server für die Speicherung der Zertifikate, benötigt.

Soll darüber hinaus zum Beispiel zu den Domains "partner-1.com" und "partner-2.com" der Mailverkehr verschlüsselt werden, müssen folgende Zeilen ergänzt werden:

```

# Julia Rules
#
#
# From          To          Rules
#-----
.              (to) .          (do) FS=mail@behoerde.de
.              (to) partner-1.com (do) FE,FS
.              (to) partner-2.com (do) FE,FS

```

3.8.3 Verwendung eines Behördenzertifikats und einiger benutzerbezogenen Zertifikate

Um die Vertraulichkeit gegenüber dem einfachsten Szenario "Verwendung eines Behördenzertifikats" zu erhöhen, erhalten die Benutzer, die unbedingt verschlüsselt kommunizieren müssen, eigene Zertifikate. Alle übrigen Benutzer verwenden das Behördenzertifikat für die automatische Signatur von Mails. Folgende Regeln von JULIA MailOffice implementieren ein solches Szenario:

```

# Julia Rules
#
#
# From          To          Rules
#-----
.              (to) .          (do) FS=mail@behoerde.de
.              (to) partner-1.com (do) FE,FS
.              (to) partner-2.com (do) FE,FS
user_1@behoerde.de (to) .          (do) EIP, FS
user_2@behoerde.de (to) .          (do) EIP, FS

```

3.8.4 Verwendung von benutzerbezogenen Zertifikaten

Um ein Maximum an Vertraulichkeit innerhalb des Unternehmens zu gewährleisten, werden benutzerbezogene Zertifikate verwendet. Dies bedeutet, dass unter Umständen viele Zertifikate verwaltet werden müssen, ein geeignetes Backend-System sollte zur Verfügung stehen (zum Beispiel LDAP-Server und geeignete Verwaltungswerkzeuge). Das unten angegebene Regelwerk definiert folgende Policy:

- Für jeden Benutzer wird die Signatur erzwungen (Zeile 1, Befehl "FS")
- Mails zu den Kommunikationspartnern "partner-1" und "partner-2" werden immer verschlüsselt und signiert (Zeilen 2 und 3)

```

# Julia Rules
#
#

```

```

# From          To          Rules
#-----
.              (to) .          (do) FS
.              (to) partner-1.com (do) FE,FS
.              (to) partner-2.com (do) FE,FS
  
```

3.8.5 Implementierung für mehrere Mandanten

3.8.5.1 Überblick

Soll JULIA MailOffice für mehrere Mandanten implementiert werden, kann dies durch Abbildung auf mehrere JULIA MailOffice-Instanzen erreicht werden. Jeder Mandant hat seine eigene JULIA MailOffice-Instanz und somit seine eigene Administrationsumgebung.

Die Mandanten werden anhand ihrer Mail-Domains (eine oder mehrere) identifiziert. Die zugehörigen inneren und äußeren Mail-Relays müssen so konfiguriert werden, dass diese auf den entsprechenden JULIA MailOffice-Server für die Auslieferung von Mails verweisen.

Grundsätzlich bestehen zwei Möglichkeiten:

- Jeder Mandant erhält seinen eigenen JULIA MailOffice-Server
- Alle Mandanten teilen sich einen JULIA MailOffice-Server

Diese beiden Ansätze mit den Auswirkungen auf die Konfiguration sind in den folgenden Abschnitten beschrieben.

3.8.5.2 Mehrere Mandanten auf verschiedenen Servern

Die einfachste Variante ist, jedem Mandanten einen eigenen Server zuzuweisen. In dieser Variante erhält man die geringsten Wechselwirkungen zwischen den einzelnen Mandanten, da die Administrationsumgebungen der einzelnen Mandanten auf verschiedenen Servern liegen. Für jeden dieser Server sind entsprechende Firewall-Regeln zu definieren (siehe Abschnitt 3.6.2ff).

Vorteile:

- Geringe Wechselwirkungen zwischen den einzelnen Administrationsumgebungen:
 - Wartungsaktivitäten für einen Mandanten beeinflussen den Betrieb der anderen JULIA MailOffice-Installationen nicht
 - Erhöhter Plattenbedarf eines Mandanten hat keinen Einfluß auf den Betrieb der anderen JULIA MailOffice-Installationen
- Große Flexibilität bei der Umsetzung mandantenspezifischer Anforderungen
 - Hoch-Verfügbarkeit für einen Teil der Mandanten, Nutzung nur eines Servers für die übrigen Mandanten ist möglich
 - Ressourcen für einen Mandanten können separat ausgebaut werden, nur für diesen Mandanten entstehen Kosten (Transparenz der Kosten)

Nachteile:

- Höhere Kosten durch separate Server
- Höhere Komplexität bei hoch-verfügbaren Systemen (Server-Anzahl verdoppelt, verdreifacht, ..., sich für jeden Mandanten)
- Höhere Komplexität des Firewall-Regelwerks

3.8.5.3 Mehrere Mandanten auf einem Server

Sollen mehrere Mandanten auf einem Server betrieben werden, müssen die JULIA MailOffice-Installationen auf entsprechende Verzeichnisse verteilt werden, zum Beispiel

```
/opt/julia-mandant-1, ..., /opt/julia-mandant-n)
```

Darüber hinaus werden für jeden der Mandanten ein entsprechender Mailer im MTA definiert, zum Beispiel

```
Mjulia-1,      P=/opt/julia-mandant-1/bin/julia, F=sDFmMoqeu9, D=$z:/,
               T=X-Unix/X-Unix/X-Unix,
               A=/opt/julia-mandant-1/bin/julia -c /opt/julia-mandant-1/etc/julia.conf -client
${client_addr} -readmail $u
```

...

```
Mjulia-n,      P=/opt/julia-mandant-n/bin/julia, F=sDFmMoqeu9, D=$z:/,  
              T=X-Unix/X-Unix/X-Unix,  
              A=/opt/julia-mandant-n/bin/julia -c /opt/julia-mandant-n/etc/julia.conf -client  
${client_addr} -readmail $u
```

(siehe auch [JULIA 03/02]).

Der MTA, welcher als Trägersystem für die verschiedenen JULIA MailOffice-Systeme fungiert, ist so zu konfigurieren, dass dieser alle Mails akzeptiert, die an alle den Mandanten gehörenden Mail-Domains gerichtet sind. Ferner sind alle Mail-Relay-Systeme der Mandanten so zu parametrisieren, dass diese auf den JULIA MailOffice-Server für die Auslieferung der Mails verweisen. Für jeden Mandanten sind ebenfalls entsprechende Firewall-Regeln (siehe Abschnitt 3.6.2ff) einzurichten.

Vorteile:

- Geringere Hardware-/Systemkosten als bei der Variante "Mandanten auf eigenen Servern"
- Geringere Komplexität für die Implementation einer Hoch-Verfügbarkeitslösung für alle Mandanten (nur ein Server muss verdoppelt, verdreifacht, ..., werden)

Nachteile:

- Hohe Wechselwirkungen zwischen den Administrationsbereichen:
 - Eine Erhöhung des Ressourcenbedarf bei einem Mandanten hat Auswirkungen auf die übrigen JULIA MailOffice-Installationen
 - Höhere Komplexität der Konfiguration des Träger-MTA
 - Administrationsaktivitäten (Sicherung, etc.) haben Auswirkungen auf die übrigen JULIA MailOffice-Installationen
- Geringe Flexibilität bei der Umsetzung mandantenspezifischer Anforderungen:
 - Die Hardware/das System kann nicht nur für einen Mandanten ausgebaut werden
 - Hoch-Verfügbarkeit kann nur für alle oder für keinen Mandanten implementiert werden
 - Geringere Kostentransparenz: Wenn ein Mandant einen größeren Plattenplatz benötigt, profitieren die übrigen JULIA MailOffice-Installationen zumindest temporär von einem Plattenausbau. Wer trägt die Kosten für einen Ausbau?

4 Inbetriebnahme von JULIA MailOffice

4.1 Überblick

Bevor JULIA MailOffice in den Regelbetrieb überführt werden kann, müssen gewisse Voraussetzungen erfüllt sein. Diese sind in Abschnitt 4.2 beschrieben. Die Behandlung der Protokolldaten von JULIA MailOffice ist in Abschnitt 4.3 erläutert. In Abschnitt 4.4 sind besondere Betriebsaktivitäten genannt.

4.2 Zu erfüllende Voraussetzungen

4.2.1 Überblick

In den folgenden Abschnitten werden die Voraussetzungen aus den Bereichen

- Systemvoraussetzungen (Hard- und Software)
- Organisatorische Voraussetzungen

beschrieben, die für die Aufnahme des Regelbetriebs erfüllt sein müssen.

4.2.2 Systemvoraussetzungen für das JULIA MailOffice-System

4.2.2.1 Hardware

Zur Zeit werden Intel/Linux- und SUN/Solaris-Systeme von JULIA MailOffice unterstützt. Die einzusetzenden Hardware sollte folgende Voraussetzungen erfüllen:

- SUN/Solaris
 - Prozessor Sparc, 700 MHz oder schneller
 - 1 GB RAM
 - Plattenkapazität Netto 20 GB
 - Netzwerk-Interface 100 Mbit/s
- Intel/Linux
 - Prozessor Intel Pentium III, 750 MHz oder schneller
 - 1 GB RAM
 - Plattenkapazität Netto 20 GB
 - Netzwerk-Interface 100 Mbit/s

Folgende Eigenschaften sind für den Regelbetrieb wünschenswert:

- RAID-Plattensystem
- Platten "Hot-Swappable"

4.2.2.2 Betriebssystem

Folgende Betriebssysteme werden unterstützt:

- Linux ab Kernel-Version 2.4 und glibc-Version 2.2, die eingesetzte Distribution ist unerheblich. Im Einsatz befinden sich die Linux-Distributionen
 - RedHat ab Version 8.x
 - SuSE und SuSE Enterprise ab Version 8.x
- SUN Solaris ab Version 8

4.2.2.3 Weitere Software-Voraussetzungen

- Unterstützte MTAs:
 - sendmail (Version aktueller als 8.8)
 - postfix
- OpenSSL V0.97 oder aktueller
- Für den VPS-Dispatcher: JDK 1.4.2_04 bzw. die selbe Version, die für die VPS verwendet wird

4.2.2.4 Installation des VPS-Dispatchers

Der VPS-Dispatcher kann auf jedem beliebigen Server installiert werden, der sich in der selben Zone befinden wie der JULIA MailOffice Server.

4.2.2.5 Sicherungs- und Archivierungsmechanismen

4.2.2.5.1 Konfiguration von JULIA MailOffice

Die Konfiguration von JULIA MailOffice sollte bei Änderungen gesichert werden. Da diese nur wenige und kleine Dateien umfasst, kann jedes beliebige Sicherungsverfahren gewählt werden. Besonderheiten brauchen nicht berücksichtigt zu werden. Die einfachste Möglichkeit, die Konfigurationsdaten zu sichern ist, das komplette Verzeichnis `/opt/julia/etc` zu sichern.

4.2.2.5.2 Protokolldaten

Protokolldaten von JULIA MailOffice sind im Verzeichnis `/opt/julia/logs` gespeichert. Der Einfachheit halber sollte das gesamte Verzeichnis gesichert werden, wenn eine Archivierung gewünscht wird. Es ist jedoch vorher unbedingt abzustimmen, inwiefern die Speicherung der JULIA MailOffice-Protokolldaten konform mit den aktuellen Datenschutzbestimmungen ist. Gegebenenfalls müssen auch die Genehmigung des Betriebsrats für die Archivierung der JULIA MailOffice-Protokolldaten eingeholt und die Protokolldaten vor deren Archivierung anonymisiert

werden. Die Speicherung personenbezogener Daten ist nur bis zu einem Zeitraum von 60 bzw. 80 Tagen zulässig. Es muss nachgewiesen werden, dass die Daten nach Ablauf dieses Zeitraums vernichtet werden. Dies geschieht im allgemeinen durch entsprechende Verfahrens- und Arbeitsanweisungen. Die Einhaltung des abgestimmten Verfahrens muss durch entsprechende Revisionsmaßnahmen geprüft werden.

4.2.2.6 Verfügbarkeit der Mailsysteme im DNS

Viele MTAs identifizieren die Zielsysteme mit Hilfe von entsprechenden DNS-Anfragen. Dies bedeutet, dass alle von diesen MTAs angesteuerten Ziele in dem von ihnen verwendeten Name-Server bekannt sein müssen. Dies ist vor der Inbetriebnahme zu prüfen.

4.2.3 Organisatorische Voraussetzungen

4.2.3.1 Klärung der datenschutzrelevanten Aspekte mit den entsprechenden Gremien

Die Implementation von JULIA MailOffice berührt einige datenschutzrelevante Aspekte. Diese sind zum Beispiel:

- Inhalt der Log-Dateien: Werden Benutzernamen protokolliert?
- Sicherung und/oder Archivierung der Log-Dateien: Welche besonderen Maßnahmen müssen umgesetzt werden (Speicherung der Daten auf nicht-veränderbaren Medien, Revisionsicherheit, Vernichtung der Datenträger nach Ablauf der Aufbewahrungsfrist etc.)
- Mechanismen für die Absicherung der privaten Schlüssel
- Unverschlüsselter Datenverkehr: Gibt es Netzwerk-Strecken, auf denen unverschlüsselt kommuniziert wird? Beispiel: Kommunikation zwischen JULIA MailOffice und Viren-Scanner. Falls ja, ist dies tragbar oder müssen zusätzliche Maßnahmen (JULIA MailOffice und Viren-Scanner auf derselben Hardware, Einsatz von Kanal-Verschlüsselung etc.) ergriffen werden?

Um eine Freigabe für die Implementation von JULIA MailOffice in einem Unternehmen zu bekommen, sind die oben genannten Aspekte mit den entsprechenden Gremien zu diskutieren. Diese sind unter anderen

- Datenschutzbeauftragte(r)
- Betriebsrat
- Corporate Security (Zugangskontrolle, etc.)

4.2.3.2 Einrichtung eines Mail-Verteilers für die JULIA MailOffice-Administration

Wichtige Nachrichten, wie zum Beispiel

- Probleme beim Entschlüsseln einer Mail
- Virenbefall einer Mail

werden an eine in JULIA MailOffice zu konfigurierende E-Mail-Adresse geschickt. Sollen mehrere Administratoren diese Nachrichten erhalten, ist ein entsprechender Verteiler im Mail-System des Unternehmens zu definieren. Dieser Verteiler-Name ist dem Parameter ADMIN in JULIA MailOffice zuzuweisen (siehe [JULIA 03/02]).

4.3 Protokolldaten

4.3.1 Ergebnisse der Zertifikatsprüfung

Die Ergebnisse der Zertifikatsprüfung werden in der Datei

```
/opt/julia/logs/verify.log
```

gespeichert. Wenn Benutzer Probleme bei Versand verschlüsselter oder signierter E-Mail melden, sind in dieser Datei Hinweise für das aktuelle Problem zu finden.

4.3.2 Protokollierung der Aktivitäten von JULIA MailOffice

Alle Aktivitäten und Fehlermeldungen von JULIA MailOffice werden in der Datei

```
/opt/julia/logs/julia.log
```

protokolliert. Zu beachten ist, dass auch die Namen der Absender und der Empfänger protokolliert werden. Unter Umständen sind diese Log-Daten für weitere Auswertungen vorher zu anonymisieren.

4.4 Besondere Betriebsaktivitäten

4.4.1 Überblick

In den folgenden Abschnitten werden besondere Betriebsaktivitäten genannt, die zum Beispiel für die Bearbeitung von Störungen wichtig sind. Diese Aktivitäten sind in [JULIA 02/03] genauer beschrieben.

4.4.2 Anschauen der Mail-Queues von JULIA MailOffice

Für jedes der drei für JULIA MailOffice relevanten Mail-Systeme

- Externes Relay

- Virens Scanner
- Internes Relay

existiert eine Mail-Queue in JULIA MailOffice. Mit Hilfe des Befehls `mailq-all` zeigt den Inhalt aller Mailqueues an:

```
bash-2.03# /opt/julia/bin/mailq-all
-----
Mails from the Universe to JULIA
Mail queue is empty
-----
Mailq from JULIA to the VIRUSSCANNER
Mail queue is empty
-----
Mailq from JULIA to the final RELAY
Mail queue is empty
-----
bash-2.03#
```

Normalerweise sollten die Queues stets leer sein. Lediglich während der kurzen Zeit der Verarbeitung durch JULIA MailOffice befinden sich Mails in diesen Queues. Sollte eine Mail sich länger (länger als fünf Minuten) in einer Queue befinden, besteht mit dieser Mail ein Problem.

4.4.3 Manuelle Zustellung von Mails

Damit Mails, die nicht sofort ausgeliefert werden konnten, nicht in den Queues liegen bleiben, werden die Warteschlangen periodisch abgearbeitet. Dazu dient der Befehl `deliver-all`, der versucht, nacheinander Mails aus allen Warteschlangen auszuliefern. Sollte die Zustellung der Mails wiederum nicht funktionieren, da zum Beispiel ein beteiligtes System nicht verfügbar ist, verbleibt die Nachricht in der Schlange und wird beim nächsten Aufruf von `deliver-all` erneut bearbeitet.

4.4.4 Veröffentlichung eines Schlüssels

Damit ein öffentlicher Schlüssel eines Benutzers für die Verschlüsselung genutzt werden kann, muss dieser innerhalb von JULIA MailOffice bekannt sein. Dies kann von einem Administrator durch Kopieren eines bereits erfolgreich geprüften Zertifikats in den so genannten Public-Bereich ([JULIA 02/03, Abschnitt 5.4.5.2.1) erreicht werden. Dies ist nicht notwendig, wenn öffentliche Schlüssel von einem LDAP-Server bezogen werden.

4.4.5 Einem Zertifikat immer vertrauen

Es kommt in der Praxis vor, dass man Zertifikaten vertrauen möchte, obwohl dieses von der Zertifikatsprüfung als nicht vertrauenswürdig eingestuft wurde. Zum Beispiel:

- Das Zertifikat eines Partners ist abgelaufen, ein neues steht noch nicht zur Verfügung

Um einem Zertifikat immer zu vertrauen, muss dieses in den Trusted-Bereich ([JULIA 02/03, Abschnitt 5.4.5.3.1) kopiert werden.

4.4.6 Einem Zertifikat nie vertrauen

Soll einem Zertifikat niemals vertraut werden, zum Beispiel, wenn bekannt wurde, dass Dritte das Zertifikat unrechtmäßig erhalten haben, muss dieses in den Untrusted-Bereich ([JULIA 02/03, Abschnitt 5.4.5.4) kopiert werden.

4.4.7 Fehlersuche

4.4.7.1 Überblick

In den folgenden Abschnitten werden kleine Hilfestellungen zur Fehlersuche gegeben. Die für diese Abschnitte gewählte Reihenfolge entspricht der, die auch in der Praxis in einem Fehlerfall gewählt werden sollte.

4.4.7.2 Prüfung des Mail-Routings

Setzen sie die Variable `SMIME_ENGINE` in JULIA MAILOffice auf "0". Dies kann entweder mit Hilfe des Web-Interfaces und des Menüpunkts Basiskonfiguration erfolgen. Anschließend führen Sie die in [JULIA 03/03] beschriebenen Tests durch und senden jeweils eine unverschlüsselte Mail von innen nach aussen und von aussen nach innen. Kommen beide Mails an, ist das Mailrouting korrekt. Die Variable `SMIME_ENGINE` sollten nun wieder auf "2" gesetzt werden.

4.4.7.3 Prüfung des VPS-Dispatchers

Ob der VPS-Dispatcher korrekt eingebunden wurde, kann wie folgt getestet werden:

- Senden einer verschlüsselten und/oder signierten Mail (Transportrichtung ist irrelevant)
- Beobachten der Datei `/opt/vps-dispatcher/logs/dispatcher.log`: Werden dort neue Meldungen erzeugt, arbeitet der VPS-Dispatcher korrekt.

4.4.7.4 Prüfung der Erreichbarkeit des Kernsystems

Durch das Kommando `ping <ip-adresse-Kernsystem>` auf dem Server, auf dem der VPS-Dispatcher betrieben wird, kann die Erreichbarkeit des Kernsystems auf IP-Ebene geprüft werden.

4.4.7.5 Prüfung des Status des Kernsystems

Ob das Kernsystem korrekt arbeitet, kann nur mit den Monitoring-Werkzeugen des Kernsystems ermittelt werden, und ist daher bei den entsprechenden Administratoren des Kernsystems zu erfragen.

4.4.7.6 Prüfung der Operation IDs

Bitte prüfen Sie, ob alle benötigten Operation IDs definiert und in [JULIA 04/04] beschriebenen Einstellungen für die Operation IDs vorgenommen wurden.

4.4.8 Protokoll-Information von JULIA MailOffice

Die Protokoll-Informationen speichert JULIA MailOffice in einer entsprechenden Log-Datei (in der Standard-Installation `/opt/julia/logs/julia.log`). Diese Log-Datei kann mit einem Editor oder mit Hilfe des Web-Frontends eingesehen werden. Alternativ kann JULIA MailOffice so konfiguriert werden, dass der `syslog`-Daemon des JULIA MailOffice Servers für die Speicherung der Protokollinformationen verwendet wird. Der lokale `syslog`-Daemon kann so konfiguriert werden, dass alle JULIA MailOffice relevanten Meldungen an einen Log-Server weitergeleitet werden. (siehe auch [JULIA 02/03]).

4.4.9 Protokoll-Informationen des VPS-Dispatchers

Der VPS-Dispatcher speichert Protokoll-Informationen in Abhängigkeit der Konfiguration in `<Basispfad>/logs/dispatcher.log`. Diese Datei wird auch nach einem Neustart fortgeschrieben und niemals durch den VPS-Dispatcher gelöscht. Entsprechende Rotationsmechanismen müssen in der Betriebsumgebung implementiert werden.

5 Literatur

- [JULIA 03/02] JULIA MailOffice Benutzerhandbuch, ICC GmbH, Februar 2003
[JULIA 04/04] JULIA MailOffice Installation mit VPS, ICC GmbH, November 2004