noSpamProxy® SERVER

Version 13.2

Integration von NoSpamProxy Encryption

- in Office 365
- in Microsoft Azure
- als On-Premises-Lösung

ENCRYPTION PROTECTION LARGE FILES DISCLAIMER

Net at Work
Building IT-Excellence.

Rechtliche Hinweise

Net at Work GmbH
Am Hoppenhof 32a
D-33104 Paderborn
Deutschland

DIESES DOKUMENT WURDE ZULETZT AM 05. NOVEMBER 2020 ÜBERARBEITET.

Inhalt

Einleitung

Seit Version 10 ist NoSpamProxy® vollständig in Microsoft Office 365 integrierbar. Dieses Handbuch beschreibt die Konfigurationsschritte sowohl für NoSpamProxy und Office 365 als auch für die eingesetzte Serverumgebung.

Die beschriebene Konfiguration gilt dabei ebenso für den Einsatz von NoSpamProxy als On-Premises-Lösung und in Microsoft Azure.

HINWEIS: Die spezifischen Konfigurationsschritte für den Einsatz in Microsoft Azure werden unter Notwendige Konfigurationen für den Betrieb in Microsoft Azure beschrieben.

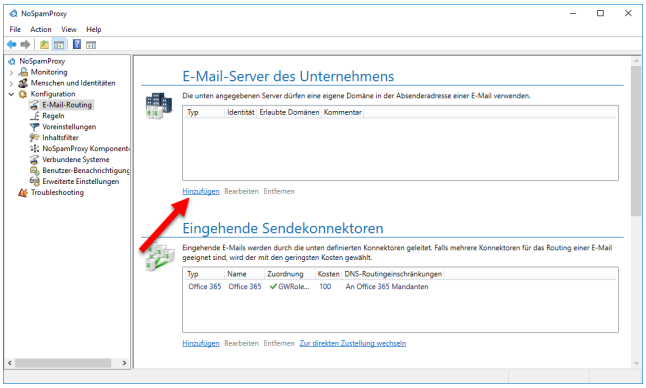
Office 365 als Relayhost freigeben

In diesem Schritt lassen Sie Office 365 in der NoSpamProxy®-Konfiguration als Relayhost zu, damit E-Mails aus Office 365 heraus durch NoSpamProxy an externe Kommunikationspartner verschickt werden können.

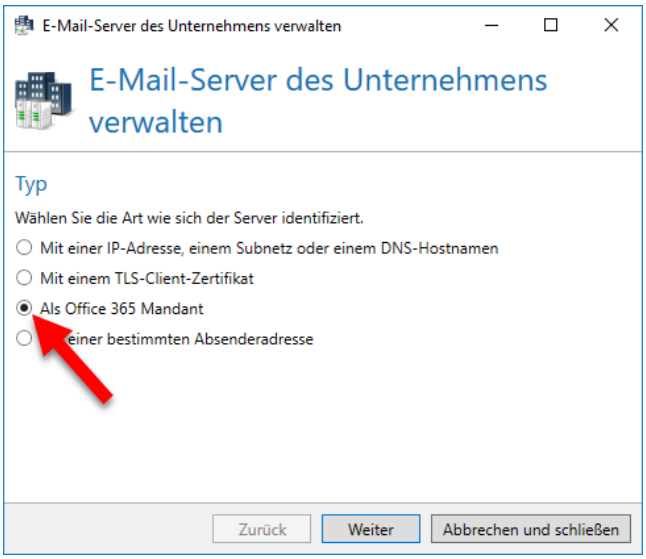
Ohne diese Konfiguration wird NoSpamProxy E-Mails als Relay-Missbrauchsversuch bewerten und abweisen.

> **HINWEIS:** Stellen Sie sicher, dass Sie mindestens eine Unternehmensdomäne eingerichtet haben, bevor Sie mit der Konfiguration beginnen.

1. Wechseln Sie in der NoSpamProxy-Managementkonsole in das Menü **Konfiguration > E-Mail-Routing**. Der Dialog **E-Mail-Server des Unternehmens verwalten** öffnet sich.

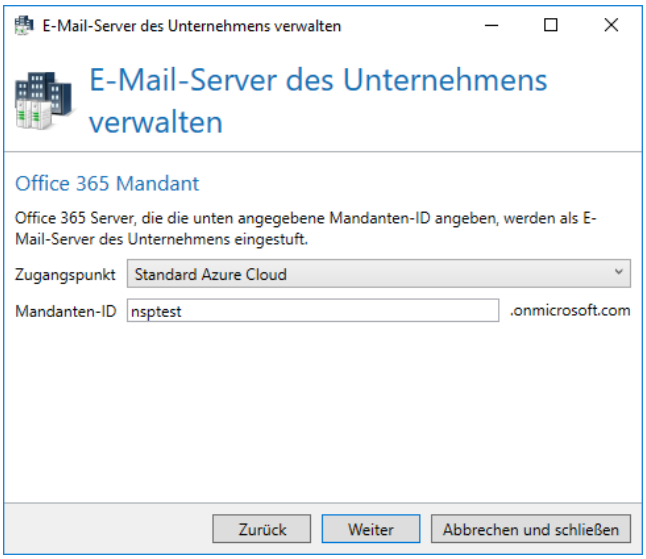


2. Wählen Sie den Typ **Als Office 365 Mandant** und klicken Sie danach **Weiter**.



3. Treffen Sie unter **Zugangspunkt** die für Ihre Organisationsumgebung passende Auswahl.
4. Geben Sie ihre Mandanten-ID ein. Achten Sie darauf, dass Sie den Namen der ID eingeben (nicht die ID in hexadezimaler Schreibweise).

5. Klicken Sie **Weiter**.



6. Wählen Sie unter **Zugeordnete Unternehmensdomänen** die Domänen aus, die Sie in Office 365 hinterlegt haben und die in der Absenderadresse für ausgehende E-Mails vorkommen werden.

> **HINWEIS:** Wenn Sie hier nicht alle Domänen vorfinden, müssen Sie die fehlenden Domänen unter **Menschen und Identitäten > Domänen und Benutzer > Unternehmensdomänen** hinzufügen. Dies ist auch zu einem späteren Zeitpunkt möglich.

7. Klicken Sie **Weiter**.
8. Geben Sie bei Bedarf einen Kommentar ein und klicken Sie dann **Fertigstellen**.

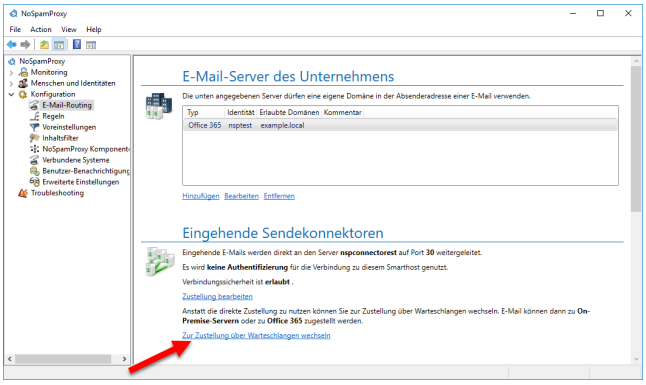
Der E-Mail-Server ist nun angelegt.

Weiterleitung an Office 365 einrichten

In diesem Schritt konfigurieren Sie NoSpamProxy® so, dass alle eingehenden und ausgehenden E-Mails an Office 365 weitergeleitet werden. Dazu müssen Sie die entsprechenden Sendekonnektoren bearbeiten.

Den eingehenden Sendekonnektor anlegen

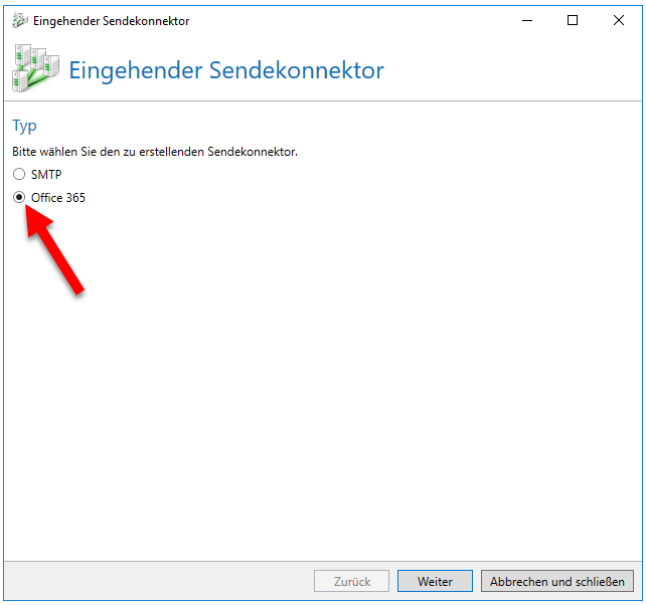
1. Wechseln Sie zu **Konfiguration > E-Mail-Routing**.
2. Klicken Sie unter **Eingehende Sendekonnektoren** auf **Zur Zustellung über Warteschlangen wechseln**.



3. Wählen Sie im Dialog **Zustellung ändern** die Option **Zustellung ersetzen**.

> **HINWEIS:** Ab Version 13 entfällt dieser Schritt, da die direkte Zustellung ab dieser Version nicht mehr unterstützt wird.

4. Wählen Sie im dann folgenden Dialog **Office 365** und klicken Sie **Weiter**.

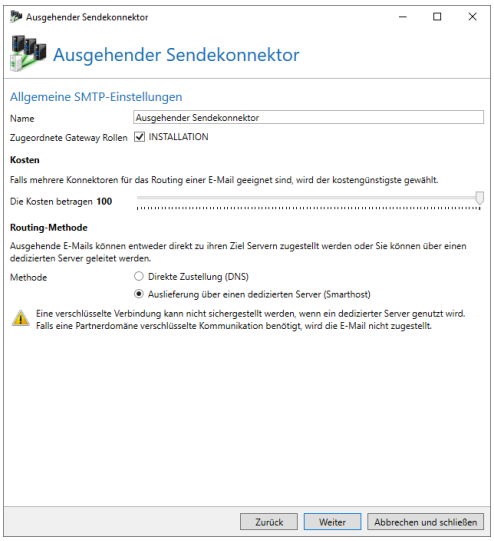


5. Geben Sie einen beliebigen Namen für den eingehenden Sendekonnektor ein und wählen Sie danach die Gateway-Rolle(n) aus, die E-Mails an Office 365 verarbeiten sollen.
6. Klicken Sie **Weiter** und dann **Fertigstellen**.

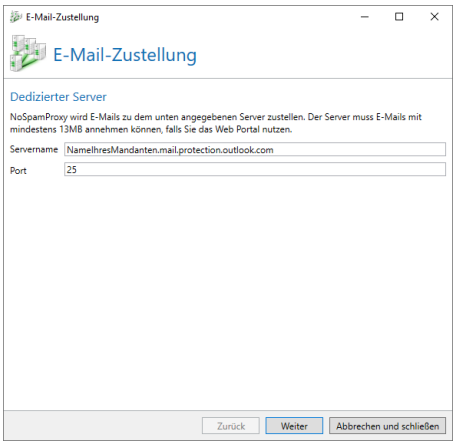
Den ausgehenden Sendekonnektor anlegen

1. Gehen Sie zu **Konfiguration > E-Mail-Routing**.
2. Klicken Sie unter **Ausgehende Sendekonnektoren** auf **Hinzufügen**, wählen Sie **SMTP** und klicken Sie **Weiter**.
3. Geben Sie einen beliebigen Namen für den ausgehenden Sendekonnektor ein, wählen Sie danach die Gateway-Rolle(n) aus, die ausgehende E-Mails

verarbeiten sollen und bestimmen Sie die Kosten.



4. Wählen Sie unter **Routing-Methode** die Option **Auslieferung über einen dedizierten Server (Smarthost)** und klicken Sie **Weiter**.
5. Klicken Sie unter **Zustellung** auf **Hinzufügen** und geben Sie als Servernamen den entsprechenden Namen nach dem Muster **NamelhresMandanten.mail.protection.outlook.com** an.



6. Wählen Sie die Option **Keine Authentifizierung verwenden** und klicken Sie **Weiter**.
7. Bestimmen Sie die Verbindungssicherheit, wählen Sie gegebenenfalls ein Zertifikat und klicken Sie **Fertigstellen** und dann **Weiter**.
8. Belassen Sie die Einstellung unter **DNS-Routingeinschränkungen**.
9. Klicken Sie **Fertigstellen**.

Die Konfiguration für NoSpamProxy ist nun abgeschlossen.

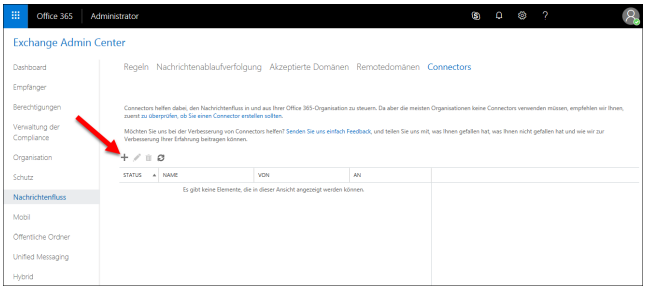
Office 365 konfigurieren

Einen Konnektor für ausgehende E-Mails anlegen

In diesem Schritt konfigurieren Sie den Office-365-Mandanten so, dass ausgehende E-Mails nicht direkt an den Empfängerserver, sondern zunächst an NoSpamProxy® zugestellt werden. Melden Sie sich dazu in an Ihrem Office-365-Mandanten unter https://outlook.office365.com/ecp an.

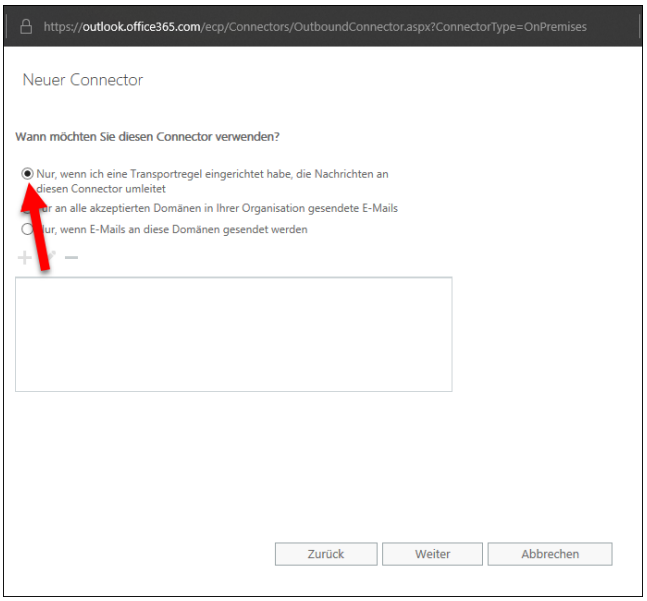
> **HINWEIS:** Verwenden Sie für die Anmeldung einen Benutzer, der über Administrationsrechte verfügt.

1. Wechseln Sie im Exchange Admin Center zu **Nachrichtenfluss > Connectors**; klicken Sie danach das **Plus-Zeichen**. Der Assistent zum Anlegen eines neuen Connectors öffnet sich.

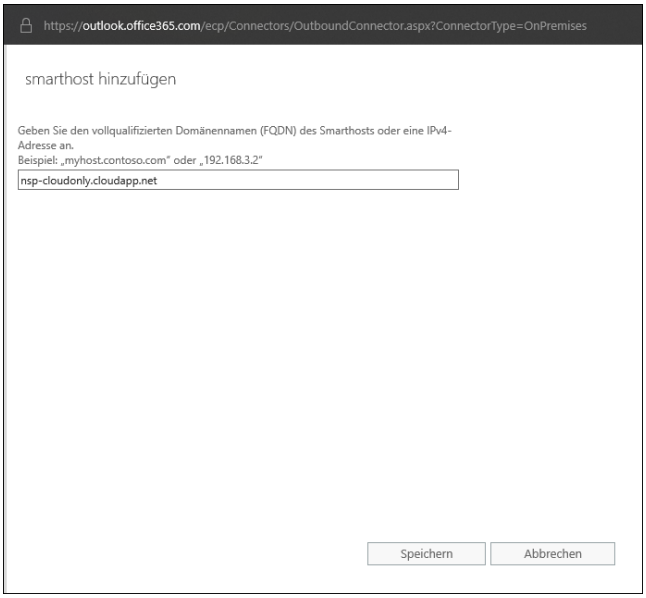


2. Wählen Sie auf der ersten Seite im Feld **Von** die Option **Office 365** aus; wählen Sie im Feld **An** die Option **Partnerorganisation** aus.

3. Klicken Sie **Weiter**. Mit dieser Einstellung werden ausgehende E-Mails vom Office-365-Mandanten an NoSpamProxy gesendet.
4. Geben Sie auf der dann folgenden Seite einen beliebigen Namen für den Connector ein.
5. Geben Sie bei Bedarf eine Beschreibung ein und klicken Sie **Weiter**.
6. Wählen Sie auf der dann folgenden Seite die Option **Nur, wenn ich eine Transportregel eingerichtet habe, die Nachrichten an diesen Konnektor umleitet**.
7. Klicken Sie **Weiter**.

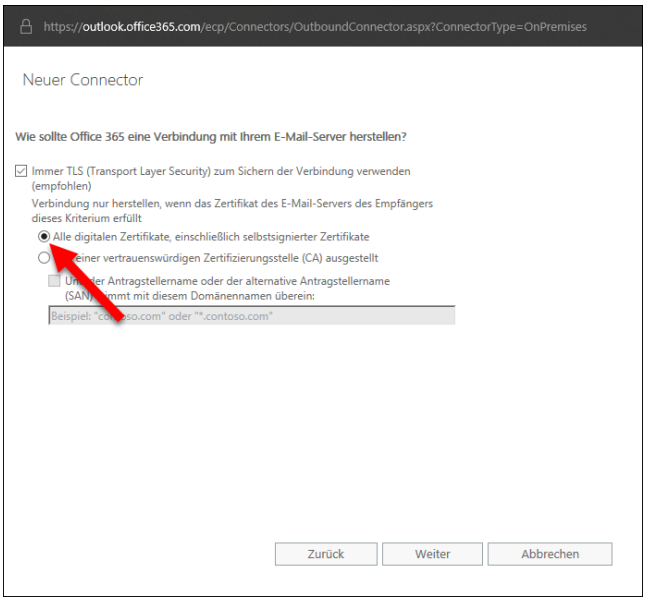


8. Geben Sie den Namen oder die IP-Adresse des Servers (Smarthost) an, auf dem die Gateway-Rolle installiert ist und klicken Sie danach **Speichern**.



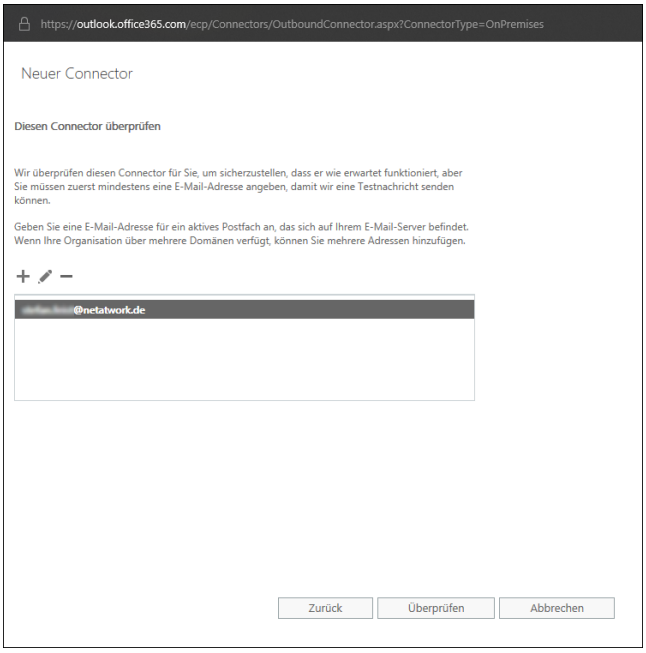
9. Aktivieren Sie im folgenden Dialogfenster die Option **Immer TLS zum Sichern der Verbindung verwenden**. Im darunterliegenden Dialogfenster wählen Sie den Punkt **Alle digitalen Zertifikate, einschließlich selbstsignierter**

Zertifikate aus und klicken **Weiter**.



10. Kontrollieren Sie die Zusammenfassung Ihrer Angaben auf Richtigkeit und klicken Sie **Weiter**.

11. Geben Sie im folgenden Dialog eine oder mehrere E-Mail-Adressen ein, die Sie für die Überprüfung dieses Konnektors verwenden möchten.



12. Klicken Sie **Überprüfen**.

> **HINWEIS:** Es werden nun eine oder mehrere Test-Nachrichten gesendet. Nach Abschluss der Prüfung erhalten Sie ein Überprüfungsergebnis. Die Test-Nachricht schlägt in der Regel fehl; dies können Sie zunächst ignorieren.

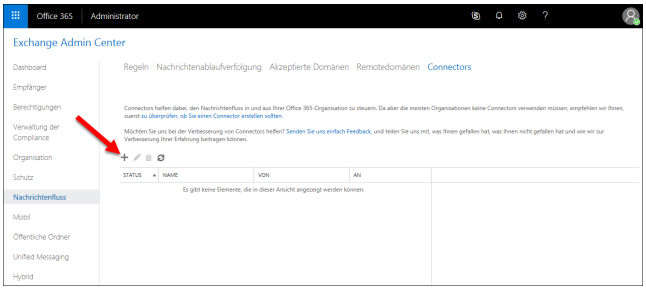
13. Klicken Sie **Speichern**, um den Dialog zu schließen.

Einen Konnektor für eingehende E-Mails anlegen

In diesem Schritt konfigurieren Sie den Office-365-Mandanten so, dass eingehende E-Mails nicht direkt an den Empfängerserver, sondern zunächst an NoSpamProxy® zugestellt werden. Melden Sie sich dazu in an Ihrem Office-365-Mandanten unter https://outlook.office365.com/ecp an.

> **HINWEIS:** Verwenden Sie für die Anmeldung einen Benutzer, der über Administrationsrechte verfügt.

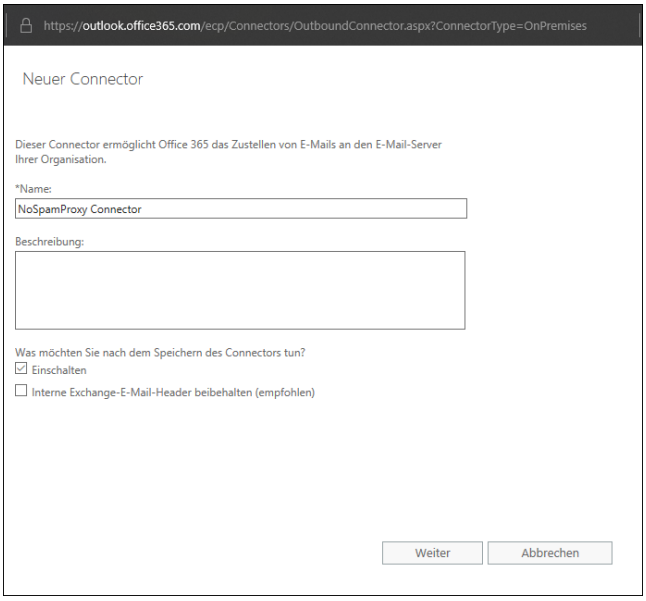
1. Wechseln Sie im Exchange Admin Center zu **Nachrichtenfluss > Connectors**; klicken Sie danach das **Plus-Zeichen**. Der Assistent zum Anlegen eines neuen Connectors öffnet sich.



2. Wählen Sie auf der ersten Seite im Feld **Von** die Option **E-Mail-Server Ihrer Organisation** aus; wählen Sie im Feld **An** die Option **Office 365** aus.
3. Klicken Sie **Weiter**.
4. Geben Sie auf der dann folgenden Seite einen beliebigen Namen für den Konnektor ein.

> **HINWEIS:** Entfernen Sie unbedingt das Häkchen neben **Interne Exchange-Email-Header beibehalten (empfohlen)**.

5. Geben Sie bei Bedarf eine Beschreibung ein und klicken Sie **Weiter**.

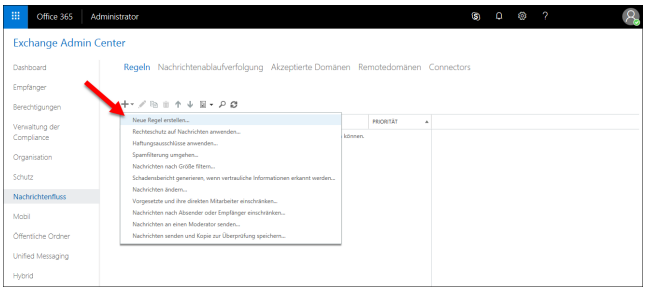


6. Wählen Sie auf der dann folgenden Seite die Option **Durch Überprüfen, ob die IP-Adresse [...]**, klicken Sie das **Plus-Zeichen** und geben Sie die IP-Adresse des NoSpamProxy-Servers an.
7. Klicken Sie **OK**, **Weiter** und dann **Speichern**.

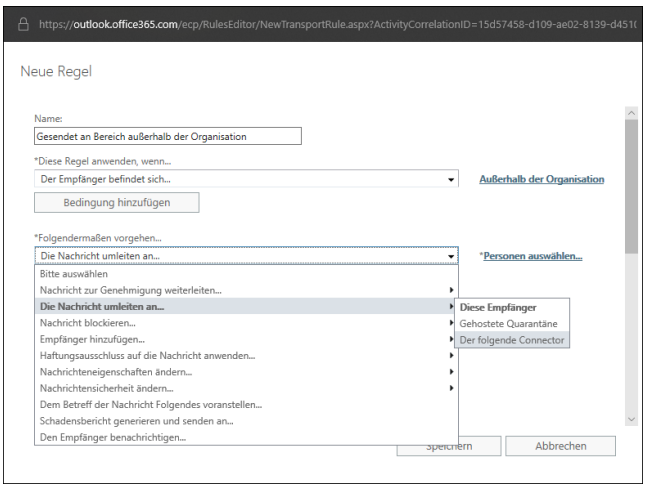
Die Transportregeln erstellen

Die ausgehende Transportregel erstellen

1. Gehen Sie in der Office-365-Verwaltungsoberfläche zu **Nachrichtenfluss > Regeln**.
2. Klicken Sie das **Plus-Symbol**.



3. Wählen Sie danach die Option **Neue Regel erstellen**. Der Assistent für die Erstellung einer neuer Transportregel öffnet sich.



4. Geben Sie einen beliebigen Namen für die Regel ein.

5. Stellen Sie unter **Diese Regel anwenden wenn** die folgenden Optionen ein:
    - **Der Empfänger befindet sich** sowie
    - **Außerhalb der Organisation**.
6. Stellen Sie unter **Folgendermaßen vorgehen** die Option **Folgenden Connector verwenden** ein.
7. Geben Sie danach den vorher erstellten Konnektor für ausgehende E-Mails an und klicken Sie **Aktion hinzufügen**.

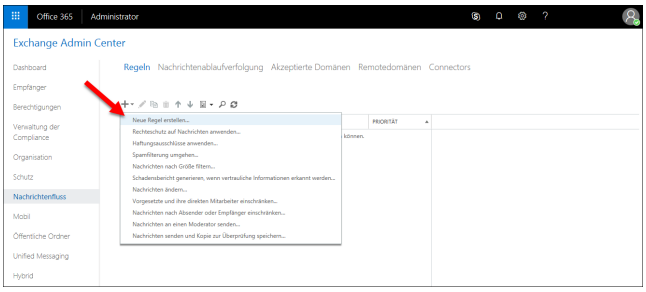
> **HINWEIS:** Falls Sie an dieser Stelle nur **Personen** auswählen können, klicken Sie im unteren Abschnitt **Weitere Optionen**. Dort können Sie unter **Die Nachricht umleiten an** die Option **Folgenden Connector verwenden** auswählen. Anschließend können Sie den zuvor erstellten Konnektor verwenden.

8. Klicken Sie **Ausnahme hinzufügen** und dann **Absender** sowie **IP liegt in einem dieser Bereiche oder stimmt genau überein mit**.
9. Fügen Sie die von NoSpamProxy genutzte IP-Adresse hinzu, klicken Sie **OK** und dann **Speichern**.

Die eingehende Transportregel erstellen

1. Gehen Sie in der Office-365-Verwaltungsoberfläche zu **Nachrichtenfluss > Regeln**.

2. Klicken Sie das **Plus-Symbol**.



3. Wählen Sie danach die Option **Neue Regel erstellen**. Der Assistent für die Erstellung einer neuer Transportregel öffnet sich.
4. Geben Sie einen beliebigen Namen für die Regel ein.
5. Stellen Sie unter **Diese Regel anwenden wenn** die folgenden Optionen ein:
   - **Der Empfänger befindet sich** sowie
   - **Innerhalb der Organisation**.
6. Stellen Sie unter **Folgendermaßen vorgehen** die Option **Folgenden Connector verwenden** ein.
7. Geben Sie danach den vorher erstellten Connector für eingehende E-Mails an und klicken Sie **Aktion hinzufügen**.

> **HINWEIS:** Falls Sie an dieser Stelle nur **Personen** auswählen können, klicken Sie im unteren Abschnitt **Weitere Optionen**. Dort können Sie unter **Die Nachricht umleiten an** die Option **Folgenden Connector verwenden** auswählen. Anschließend können Sie den zuvor erstellten Connector verwenden.

8. Klicken Sie **Ausnahme hinzufügen** und dann **Absender** sowie **IP liegt in einem dieser Bereiche oder stimmt genau überein mit**.
9. Fügen Sie die von NoSpamProxy genutzte IP-Adresse hinzu, klicken Sie **OK** und dann **Speichern**.

Notwendige Konfigurationen für den Betrieb in Microsoft Azure

Nach der Integration von NoSpamProxy in Office 365 und der Installation von NoSpamProxy in Microsoft Azure werden E-Mails nicht mehr durch Office 365 zugestellt, sondern direkt durch NoSpamProxy.

Um das Versenden von E-Mails durch NoSpamProxy zu ermöglichen, müssen Sie Ihre NoSpamProxy-Installation in Microsoft Azure entsprechend konfigurieren. Diese Konfiguration umfasst drei Bereiche.

Einbinden des TCP Proxy für NoSpamProxy

Der NoSpamProxy-Server kann in Microsoft Azure keine E-Mails über Port 25 schicken. Zudem werden E-Mail-Adressen durch Microsoft Azure häufig auf Blacklists gesetzt.

Aus diesen Gründen stellen wir unseren Kunden einen kostenfreien Proxyserver zur Verfügung, der die genannten Probleme beseitigt. Diesen TCP Proxy müssen Sie über die Datei **Gateway Role.config** aktivieren.

Gehen Sie dazu folgendermaßen vor:

1. Stoppen Sie den Dienst der Gateway-Rolle über die NoSpamProxy-Konsole oder die Windows-Dienste
2. Öffnen Sie als Administrator einen Texteditor auf dem System, auf dem die Gateway-Rolle installiert ist.

3. Öffnen Sie die Konfigurationsdatei **Gateway Role.config** aus dem Verzeichnis **C:\ProgramData\Net at Work Mail Gateway\Configuration**.
4. Suchen Sie in der Datei nach `<smtpServicePointConfiguration>` und ändern/fügen Sie den Wert `isProxyTunnelEnabled="true" proxyTunnelAddress="proxy.nospamproxy.com"` als Attribute hinzu.

   > **HINWEIS:** Falls `<smtpServicePointConfiguration` nicht vorhanden ist, suchen Sie nach `<netatwork.nospamproxy.proxyconfiguration` und fügen Sie `<smtpServicePointConfiguration isProxyTunnelEnabled="true" proxyTunnelAddress="proxy.nospamproxy.com" />`direkt unter diesem Wert hinzu.

5. Speichern Sie die Datei ab und schließen Sie den Editor.
6. Legen Sie das Root CA Zertifikat im Zertifikatsspeicher von Microsoft im Computerkonto unter **Vertrauenswürdige Stammzertifizierungsstellen > Zertifikate** auf dem Server mit der Gateway Rolle ab.
7. Bearbeiten Sie in der NoSpamProxy-Konsole unter **Konfiguration > NoSpamProxy Komponenten > Gateway Rollen** die entsprechende Gateway Rolle und ändern Sie den Wert für **SMTP Servername** auf den Wert **proxy.nospamproxy.de**.
8. Starten Sie den Gateway-Rollen-Dienst wieder

9. Öffnen Sie die Datei **Gateway Role.config** erneut und prüfen Sie, ob der Wert beim Start erhalten geblieben ist.

Einrichten einer statischen IP-Adresse für den NoSpamProxy-Server

> **HINWEIS:** Diese Einstellung nehmen Sie auf dem virtuellen Computer in Microsoft Azure vor, auf dem NoSpamProxy installiert ist.

1. Öffnen Sie die Webseite portal.azure.com.
2. Klicken Sie unter **Home > Virtuelle Computer** auf den virtuellen Computer, auf dem NoSpamProxy installiert ist.
3. Gehen Sie zu **Netzwerk > Netzwerkschnittstelle > IP-Konfigurationen** und wählen Sie die für NoSpamProxy relevante Konfiguration.
4. Aktivieren Sie die Option **Öffentliche IP-Adresse** und klicken sie danach **Neu erstellen**.
5. Geben Sie einen Namen ein und wählen Sie die Option **Statisch** aus.
6. Klicken Sie **OK**.

Die IP-Adresse wird nun unter dem angegebenen Namen angezeigt.

Anpassen des Reverse-DNS-Eintrags für den NoSpamProxy-Server

Um den Reverse-DNS-Eintrag zu konfigurieren, folgen Sie den Anweisungen im Abschnitt Reverse-DNS für öffentliche IP-Adressressourcen der Microsoft Azure-Dokumentation.

> **HINWEIS:** Falls SPF-Einträge (Sender Policy Framework-Einträge) vorliegen, müssen Sie die IP-Adresse des NoSpamProxy-Servers als erlaubten Absender eintragen. Alternativ können Sie auch den Domänennamen - also **proxy.nospamproxy.de** - eintragen.

> **HINWEIS:** Falls Sie NoSpamProxy in Microsoft Azure betreiben und den TCP Proxy einsetzen, muss der SPF-Eintrag zwingend um den Eintrag **a:proxy.nospamproxy.de** erweitert werden. Nur wenn der TCP Proxy nicht verwendet wird **und** ein SPF Eintrag vorhanden ist, müssen dort die IP-Adresse(n) der Azure-Maschine eingetragen werden.

> **HINWEIS:** Wir empfehlen dringend den Einsatz eines SPF-Eintrags.

Hilfe und Unterstützung

Knowledge Base

Die Knowledge Base enthält weiterführende technische Informationen zu unterschiedlichen Problemstellungen.

Website

Auf der NoSpamProxy-Website finden Sie Handbücher, Whitepaper, Broschüren und weitere Informationen zu NoSpamProxy.

NoSpamProxy-Forum

Das NoSpamProxy-Forum gibt Ihnen die Gelegenheit, sich mit anderen NoSpamProxy-Anwendern auszutauschen, sich zu informieren sowie Tipps und Tricks zu erhalten und diese mit anderen zu teilen.

Blog

Das Blog bietet technische Unterstützung, Hinweise auf neue Produktversionen, Änderungsvorschläge für Ihre Konfiguration, Warnungen vor Kompatibilitätsproblemen und vieles mehr. Die neuesten Nachrichten aus dem Blog werden auch auf der Startseite der NoSpamProxy-Managementkonsole angezeigt.

YouTube

In unserem YouTube-Kanal finden Sie Tutorials, How-Tos und andere Produktinformationen, die Ihnen das Arbeiten mit NoSpamProxy erleichtern.

NoSpamProxy-Support

Unser Support-Team erreichen Sie

- per Telefon unter +49 5251304-636
- per E-Mail unter support@nospamproxy.de.