Net at Work
Building IT-Excellence.

NoSpamProxy

Installationsanleitung für den Betrieb in Microsoft Azure

- Protection
- Encryption
- Large Files

Impressum

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

Handelsmarken

21. August 2018

Inhalt

1. Aufsetzen einer NoSpamProxy-Instanz in Microsoft Azure

Um NoSpamProxy in Microsoft Azure nutzen zu können, müssen Sie zuerst eine Azure-Instanz als Virtuellen Computer aufsetzen.

Melden Sie sich dazu an Ihrem Azure-Tenant unter https://portal.azure.com/ an.

Klicken Sie dann auf **Ressource erstellen** und suchen Sie nach **NoSpamProxy**.

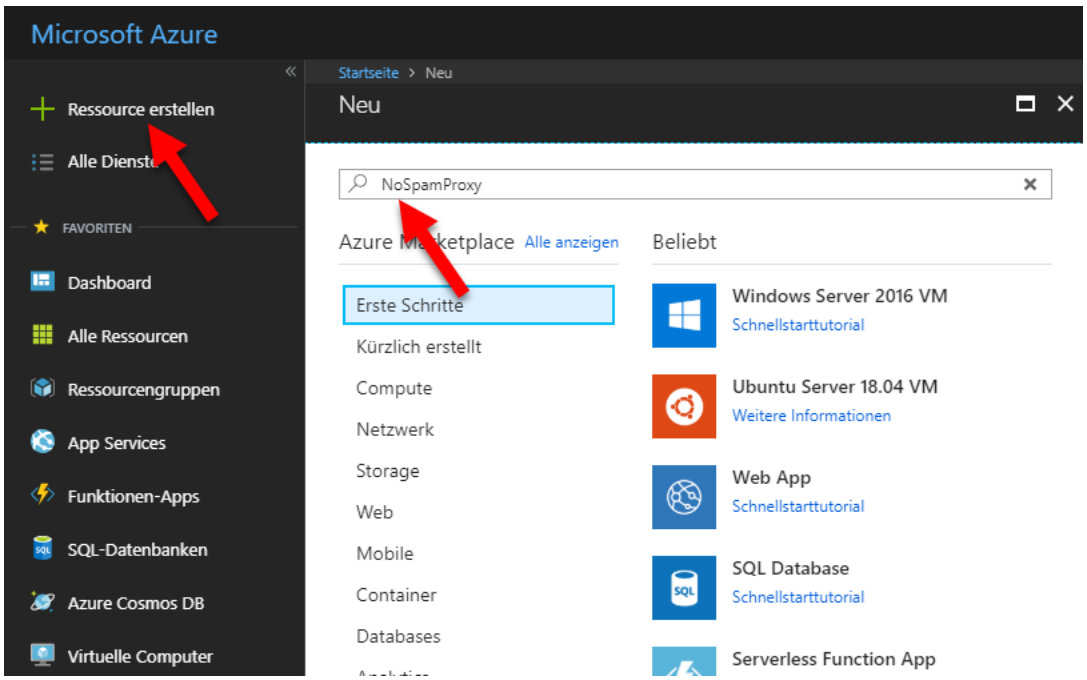

Bild 1: Der Assistent für den Azure Marketplace

Wählen Sie die **NoSpamProxy Azure Edition** aus und klicken Sie dann **Erstellen**.

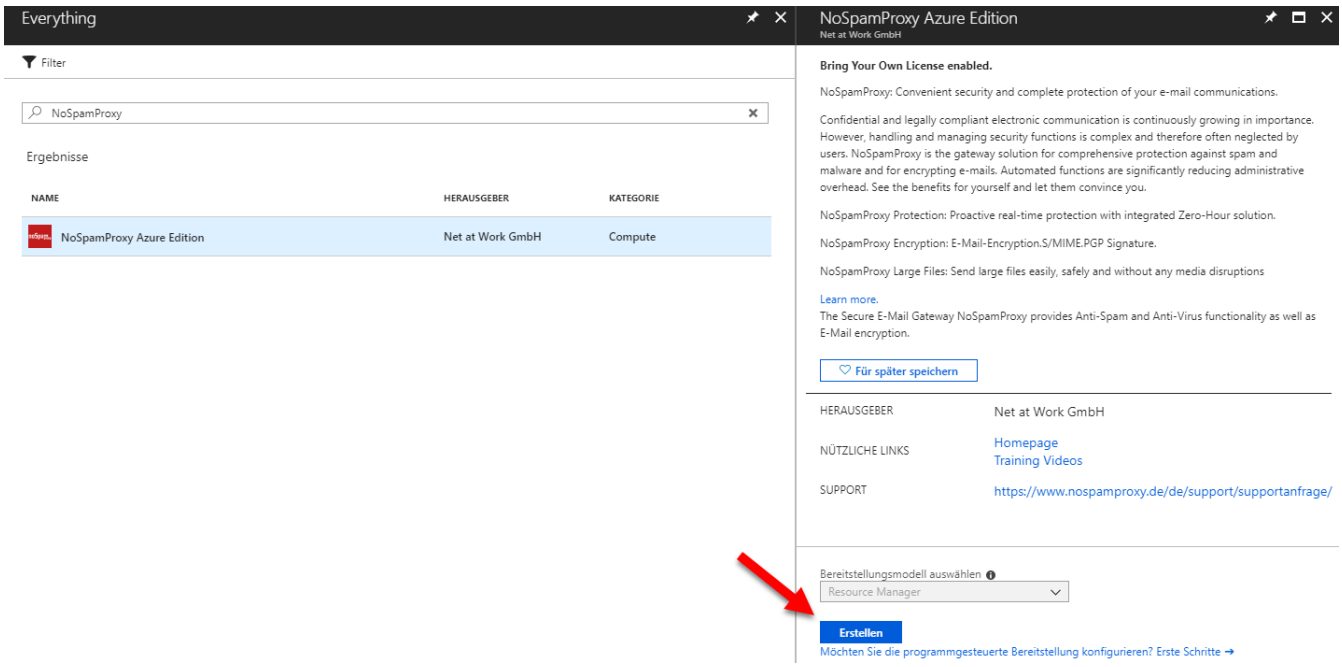

Bild 2: Eine neue Ressource in Azure erstellen

Geben Sie nun einige Details (Name, Datenträgertyp, Benutzername und Passwort) zum virtuellen Computer an, den Sie erstellen wollen. Fügen Sie danach folgende Details hinzu:

- Abonnement: Hier wird Ihr Azure-Abonnement angezeigt. Falls Sie ein weiteres Abonnement besitzen und Sie die NoSpamProxy-Instanz über ein anderes Abonnement abrechnen wollen, wählen Sie das entsprechende Abonnement über das Drop-Down-Menü aus.
- Ressourcengruppe: Wir empfehlen, die verwendeten Dienste in Ihrem Azure-Tenant in Ressourcengruppen zu ordnen, um die Übersichtlichkeit zu wahren. Falls Sie bereits eine Ressourcengruppe für NoSpamProxy angelegt haben, wählen Sie **Vorhandenes Element verwenden** aus. Wählen Sie anschließend die gewünschte Ressourcengruppe über das Drop-Down-Menü aus. Falls Sie noch keine Ressourcengruppe angelegt haben, wählen Sie **Neues Element erstellen** und geben Sie dann einen Namen für die neue Ressourcengruppe an.
- Standort: Geben Sie die Region für das Datacenter an, in dem Ihre NoSpamProxy-Instanz in Microsoft Azure betrieben wird.

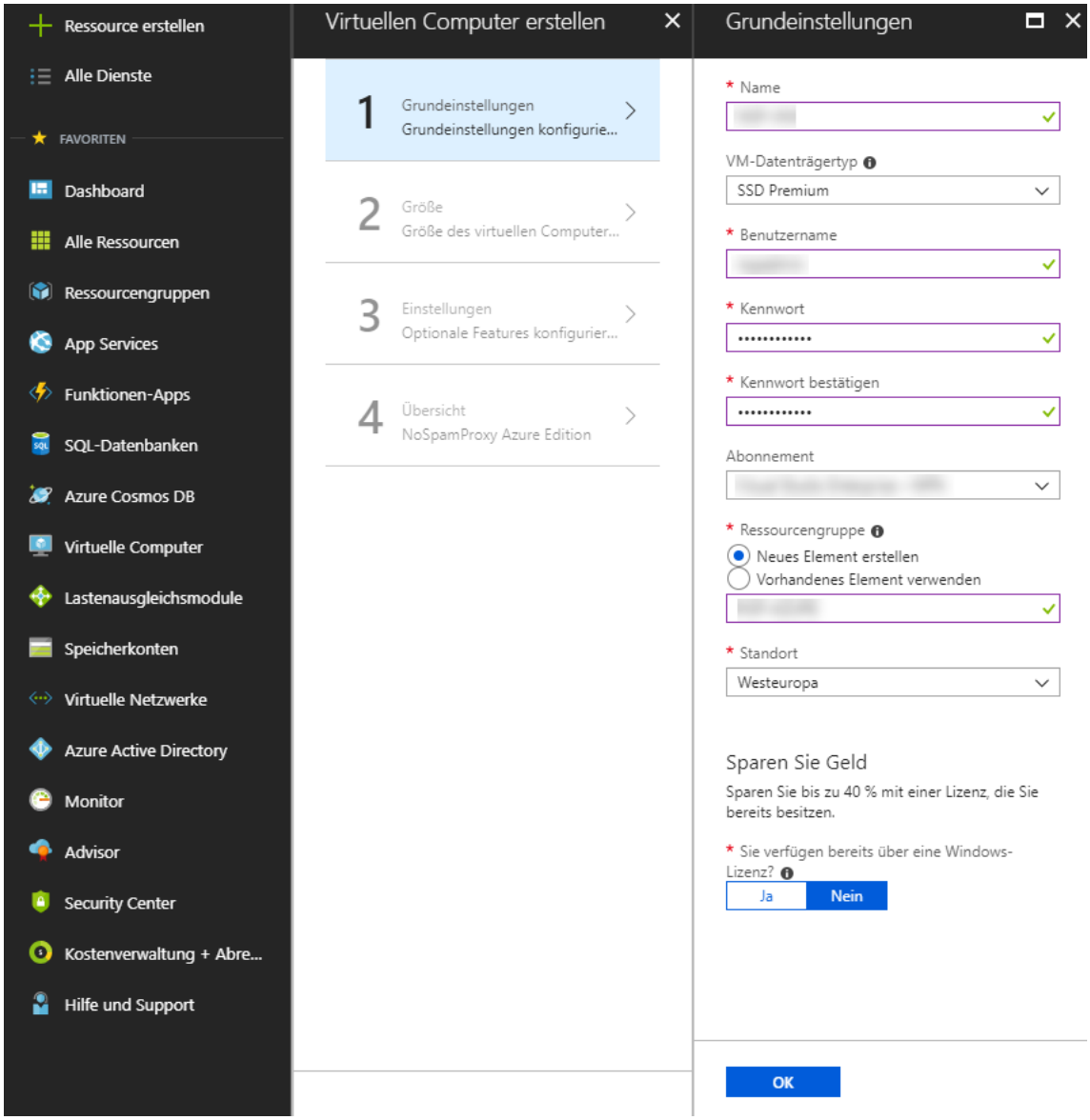

Bild 3: Grundeinstellungen für den virtuellen Computer

Klicken Sie auf OK.

Wählen Sie die Größe des virtuellen Computers. Um alle Größen zu sehen, klicken Sie auf **Zeige alle**. Die kleinstmögliche Maschine ist B1s. Für die Verarbeitung von bis zu 100 E-Mails pro Minute ist dies ausreichend, allerdings mit Einschränkungen hinsichtlich der Performanz der Verwaltungskonsole. Für den Einstieg empfehlen wir die Größe A1_V2 ; Sie können jederzeit im laufenden Betrieb auf A2_V2 wechseln.

	F8	Standard	Compute-optimiert	8
	F16	Standard	Compute-optimiert	16
	A1_v2	Standard	Allgemein	1
	A2_v2	Standard	Allgemein	2
	A4_v2	Standard	Allgemein	4

Bild 4: Die Größe des virtuellen Computers auswählen

Klicken Sie nach der Auswahl der gewünschten Größe auf **Auswählen**.

Im nächsten Schritt haben Sie die Möglichkeit, optionale Einstellungen vorzunehmen.

Wir empfehlen Ihnen, die öffentliche IP-Adresse als **statisch** einzurichten:

Falls Sie schon eine statische öffentliche IP-Adresse in Ihrem Azure-Tenant erstellt haben und Sie diese auch für die NoSpamProxy-Instanz in Microsoft Azure verwenden möchten, wählen Sie diese aus und klicken auf **OK**. Beachten Sie, dass nur die öffentlichen IP-Adressen angezeigt werden, die in der im ersten Schritt ausgewählten Ressourcengruppe erstellt wurden.

Falls Sie noch keine feste öffentliche IP-Adresse in Ihrem Azure-Tenant erstellt haben, klicken Sie auf **Öffentliche IP-Adresse** und dann auf **Neu erstellen**.

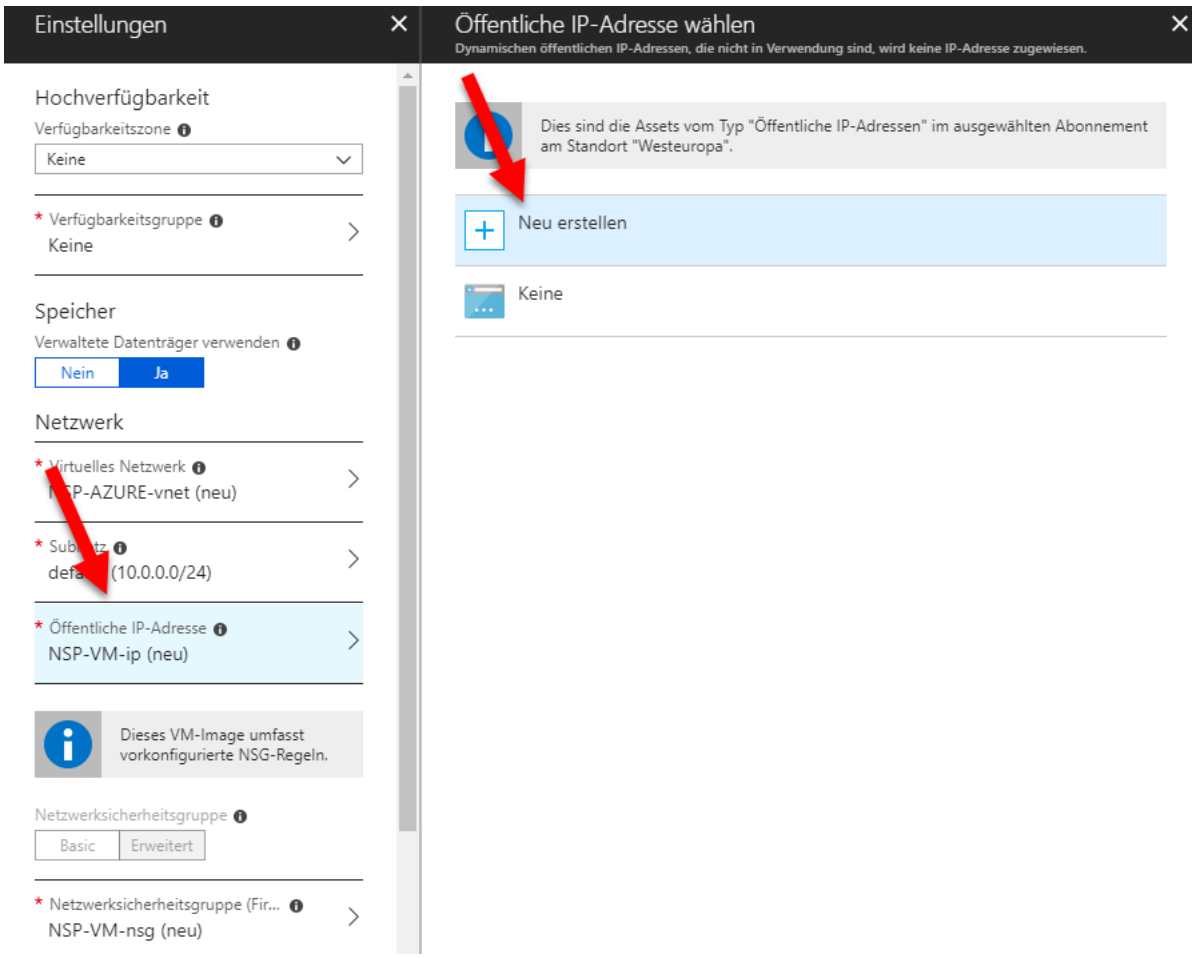

Bild 5: Erstellen einer statischen öffentlichen IP-Adresse

Vergeben Sie einen Namen für die IP-Adresse und wählen anschließend **Statisch** aus.

Klicken Sie auf **OK**.

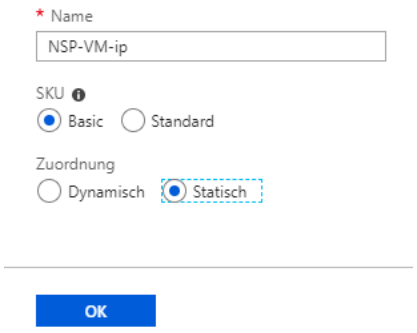

Bild 6: Eine öffentliche IP-Adresse als statisch einrichten

Überprüfen Sie die übrigen Grundeinstellungen und klicken Sie dann auf **OK**. Es wird nun eine Zusammenfassung der zuvor getroffenen Einstellungen angezeigt.

Mit **Erstellen** bestätigen Sie, dass Sie dem Kauf des virtuellen Computers zustimmen. Der virtuelle Computer wird nun bereitgestellt.

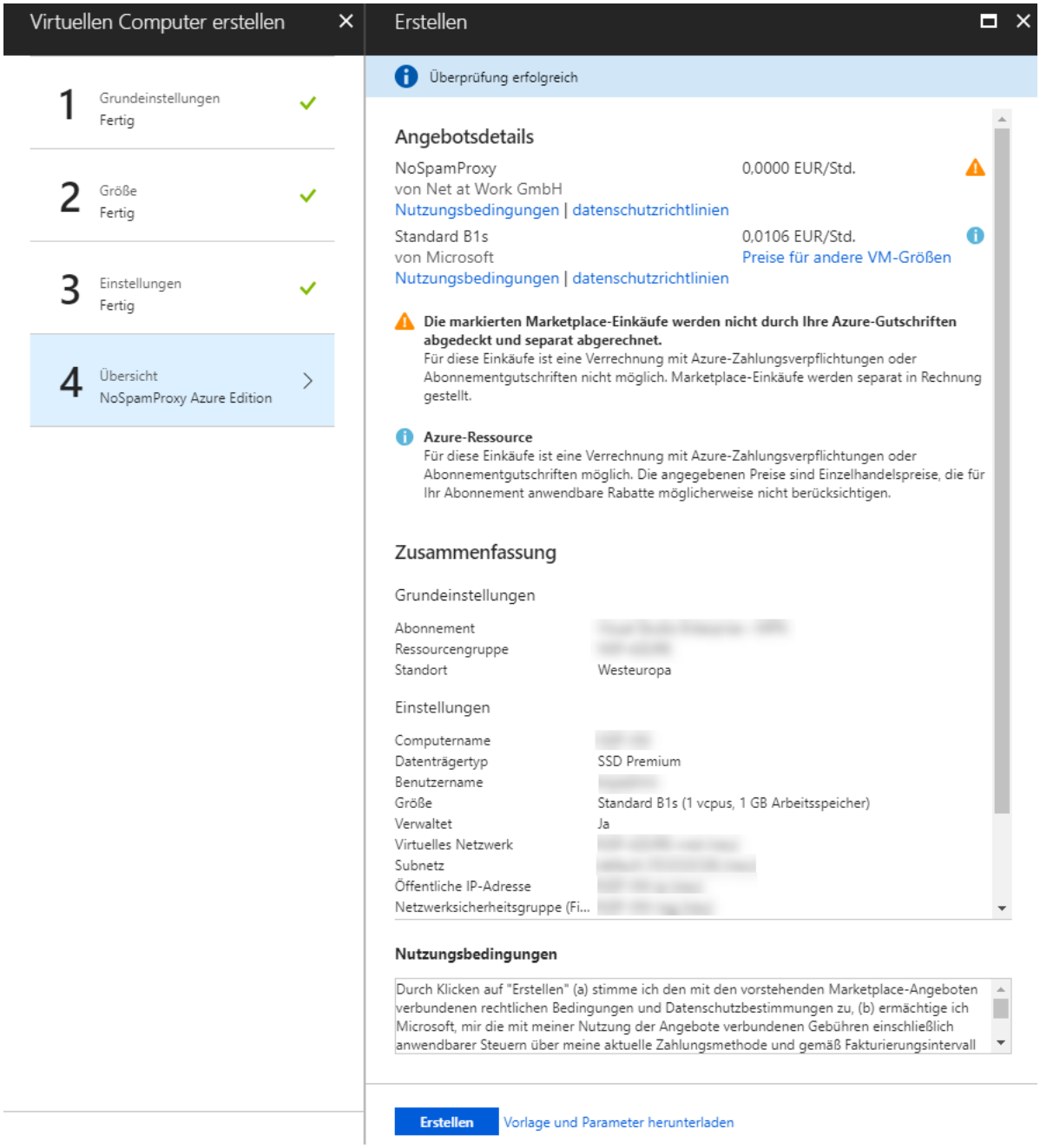

Bild 7: Dem Kauf des virtuellen Computers zustimmen

2. Notwendige Konfigurationen für den Betrieb in Microsoft Azure

Nach der Installation von NoSpamProxy in Microsoft Azure müssen Sie noch zwei Bereiche in Microsoft Azure konfigurieren.

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.

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.

Aktivieren des Azure-Proxyservers für NoSpamProxy

Da Microsoft Azure es Applikationen nicht erlaubt, E-Mails über Port 25 zu versenden, kann NoSpamProxy diesen Port nicht nutzen. Zudem werden E-Mail-Adressen durch Microsoft Azure häufig auf Blacklists gesetzt. Aus diesen Gründen stellen wir unseren Kunden einen kostenfreien Smarthost zur Verfügung, der die genannten Probleme beseitigt.

Diesen Smarthost müssen Sie über die Datei "Gateway Role.config" aktivieren. Gehen Sie dazu folgendermaßen vor:

Stoppen Sie die Gateway-Rolle.

Gehen Sie zu `C:\ProgramData\Net at Work Mail Gateway\Configuration` und öffnen Sie die Datei **Gateway Role.config**.

Suchen Sie das Tag `<netatwork.nospamproxy.proxyconfiguration>`. Fügen Sie das Tag `<smtpServicePointConfiguration isProxyTunnelEnabled="true" />` an beliebiger Stelle innerhalb des oben genannten Tags ein.

Unter Umständen ist das Tag `<smtpServicePointConfiguration>` bereits vorhanden. In diesem Fall müssen Sie nur das Attribut `isProxyTunnelEnabled="true"` hinzufügen.

Starten Sie die Gateway-Rolle.

3. Support

Bei Fragen zu NoSpamProxy oder zur Installation in Microsoft Azure steht Ihnen unser Support-Team zur Verfügung:

- per Telefon unter +49 5251304-636
- per E-Mail unter support@nospamproxy.de
- auf der NoSpamProxy-Website