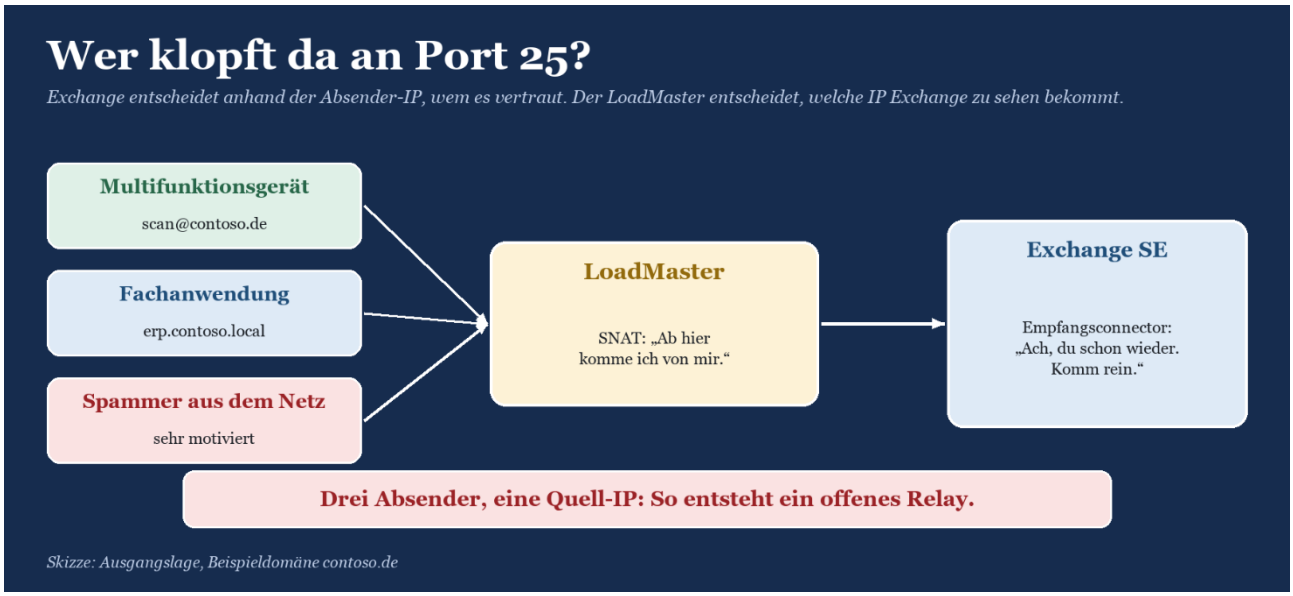
SMTP über den LoadMaster: Relay, Empfangsconnectors und die echte Absender-IP



WISSEN

Alles zum Kemp LoadMaster mit Microsoft-Brille: Exchange, SharePoint, ADFS, RDS und Kerberos an einem Ort.

› **Kemp LoadMaster**

BERATUNG

SMTP-Relay hinter dem LoadMaster aufräumen, ohne dass am Montag die Scanner schweigen? Wir prüfen Connectors und Virtual Services mit dir.

› **Beratung zum Kemp LoadMaster**

SCHULUNG

Transparenz, SNAT, Relay-Connectors und Protokollprotokolle im Labor durchspielen, bevor es die Produktion für dich tut.

› **Kemp-LoadMaster-Schulung**

Es gibt zwei Sorten von Exchange-Administratoren: die, die schon einmal ein offenes Relay betrieben haben, und die, die es noch nicht wissen. Der schnellste Weg in die erste Gruppe führt erstaunlich oft über einen Load Balancer. Die Geschichte geht immer gleich: Die HTTPS-Dienste laufen längst sauber über den LoadMaster, also zieht man Port 25 „der Einheitlichkeit halber" gleich mit um. Danach melden sich die Multifunktionsgeräte mit „550 5.7.54 Unable to relay", jemand trägt eilig die IP-Adresse des LoadMasters in den Relay-Connector ein, die Scanner sind glücklich, und drei Wochen später steht die eigene Domäne auf einer Blockliste. Die Scanner sind übrigens immer noch glücklich.

Der Grund liegt nicht im LoadMaster und nicht in Exchange, sondern in der Fuge zwischen beiden. Exchange entscheidet bei SMTP anhand der Quell-IP-Adresse, welcher Empfangsconnector eine Verbindung bekommt und welche Rechte damit verbunden sind. Der LoadMaster entscheidet, welche Quell-IP-Adresse Exchange überhaupt zu sehen bekommt. Wenn diese beiden Entscheidungen nicht zueinander passen, hast du entweder ein Relay für alle oder für niemanden. Dazwischen gibt es erstaunlich wenig.

Dieser Beitrag gehört zur Serie rund um den Kemp LoadMaster und baut auf Exchange Server hinter dem LoadMaster: Templates, Namespaces, Health Checks auf. Dort geht es um HTTPS, Namespaces und healthcheck.htm. Hier geht es um das Protokoll, das älter ist als die meisten Leser dieses Textes und sich entsprechend benimmt: SMTP. Du erfährst, warum SNAT und Empfangsconnectors sich beißen, wann Transparenz die Lösung ist und wann ein Albtraum, wie

getrennte VIPs das Problem elegant umgehen und warum die beste SMTP-Lastverteilung manchmal gar keine ist.

FAKTEN · SMTP und Exchange in Zahlen

Port 25: Frontend-Transport-Dienst, Connector „Default Frontend <Server>“, nimmt anonym Mail für die eigenen akzeptierten Domänen an.

Port 587: Connector „Client Frontend <Server>“ für authentifizierte Clients.

Port 2525: Transport-Dienst auf demselben Server, nur für Exchange-interne Kommunikation. Gehört nie hinter einen Load Balancer.

Connector-Auswahl: lokale Bindung (IP und Port) plus RemoteIPRanges, der spezifischste Treffer gewinnt.

Gilt für Exchange 2016, 2019 und Exchange Server SE gleichermaßen.

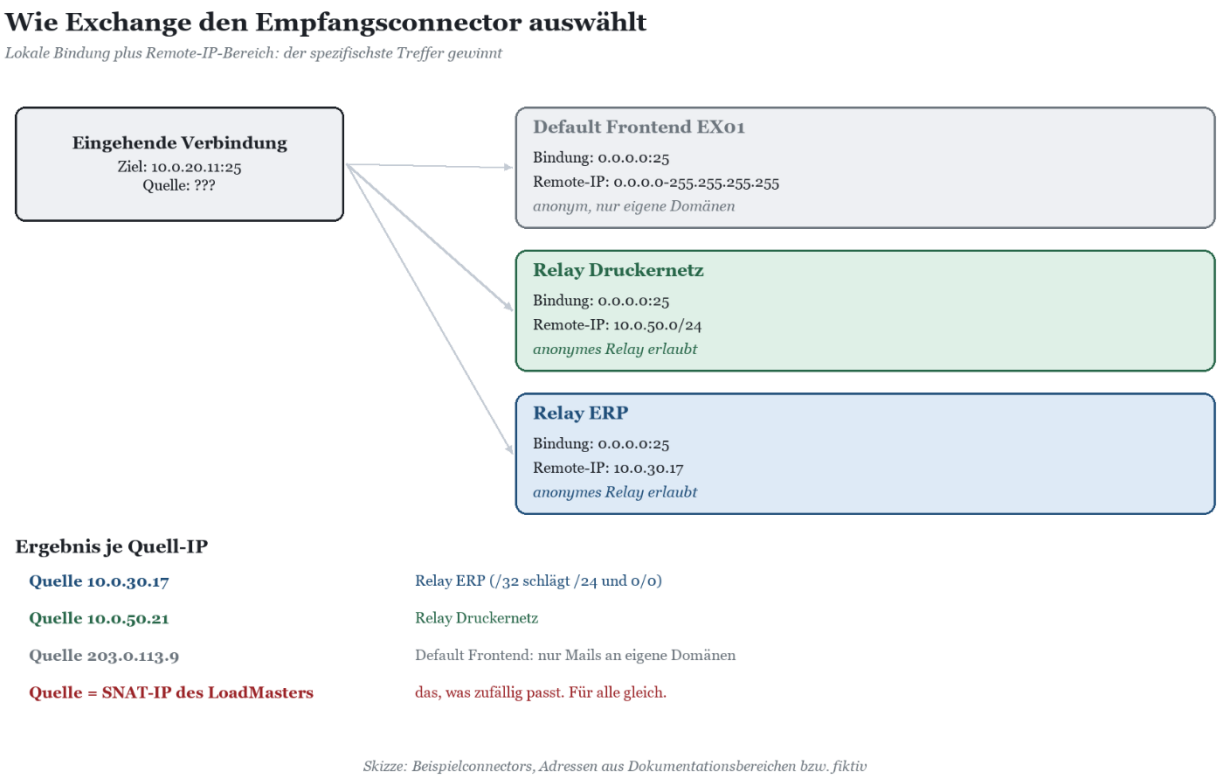
Warum SMTP anders tickt als HTTPS

Bei HTTPS ist dem Exchange-Server ziemlich egal, woher eine Verbindung kommt. Wer OWA öffnet, muss sich anmelden, und die Anmeldung entscheidet über die Rechte. Die Quell-IP-Adresse landet höchstens im IIS-Log, und wer sie dort sehen will, hilft sich mit X-Forwarded-For. SMTP dagegen stammt aus einer Zeit, in der man sich im Internet noch gegenseitig vertraut hat. Anonyme Verbindungen sind der Normalfall, nicht die Ausnahme, und die einzige Information, die Exchange über einen anonymen Absender sicher kennt, ist seine IP-Adresse.

Folgerichtig ist die IP-Adresse bei SMTP kein Logdetail, sondern ein Sicherheitsmerkmal. Exchange vergibt Rechte an Empfangsconnectors, und ob eine Verbindung auf dem harmlosen Default-Connector landet oder auf dem Relay-Connector, der Mail an beliebige Empfänger weiterleiten darf, entscheidet allein die Kombination aus Ziel-IP, Port und Quell-IP. Wer die Quell-IP verändert, verändert die Rechte. So einfach ist das, und so gefährlich.

Die Connector-Auswahl: der spezifischste Treffer gewinnt

Jeder Empfangsconnector hat zwei Eigenschaften, die über seine Zuständigkeit entscheiden: Bindings, also die lokalen IP-Adressen und Ports, auf denen er lauscht, und RemoteIPRanges, also die Absenderadressen, für die er gilt. Exchange erlaubt mehrere Connectors auf derselben Bindung, solange sich die Remote-Bereiche unterscheiden. Kommt eine Verbindung herein, gewinnt der Connector mit der genauesten Übereinstimmung: Eine einzelne Adresse schlägt ein /24-Netz, ein /24-Netz schlägt den Bereich 0.0.0.0 bis 255.255.255.255 des Default-Connectors.



Skizze: Beispielconnectors, Adressen aus Dokumentationsbereichen bzw. fiktiv

Genau so empfiehlt Microsoft auch das anonyme Relay: einen eigenen Connector im Frontend-Transport-Dienst anlegen, die erlaubten Geräte möglichst eng als RemoteIPRanges eintragen und dann die Rechte vergeben. Die Default-Connectors fasst man dabei ausdrücklich nicht an. Das Modell ist elegant, solange eine Annahme gilt: Die Quell-IP-Adresse, die Exchange sieht, ist die Adresse des Geräts. Der LoadMaster ist das Bauteil, das diese Annahme beiläufig zerlegen kann.

Zwei Wege zum Relay und ihr Preis

Für die Rechte auf dem Relay-Connector kennt Microsoft zwei Methoden, und beide verhalten sich hinter einem Load Balancer unterschiedlich gefährlich. Die Tabelle fasst zusammen, was du dir jeweils einhandelst.

Methode	Was Exchange daraus macht	Risiko hinter SNAT
Anonym plus Recht Ms-Exch-SMTP-Accept-Any-Recipient für ANONYMOUS LOGON	Absender bleibt anonym, Antispam und Größenlimits greifen weiter, minimale Rechte	Falsche Quell-IP öffnet das Relay, Spam wird aber noch gefiltert, sofern Antispam aktiv ist
Permission-Gruppe ExchangeServers plus Authentifizierung ExternalAuthoritative (im EAC „Extern gesichert“)	Absender gilt als vollständig vertrauenswürdig, umgeht Antispam und Größenlimits, Absender wird gegen die GAL aufgelöst	Falsche Quell-IP macht jeden Absender zum internen Exchange-Server. Schlimmer geht nicht.

WICHTIG · Extern gesichert ist ein Vertrauensversprechen

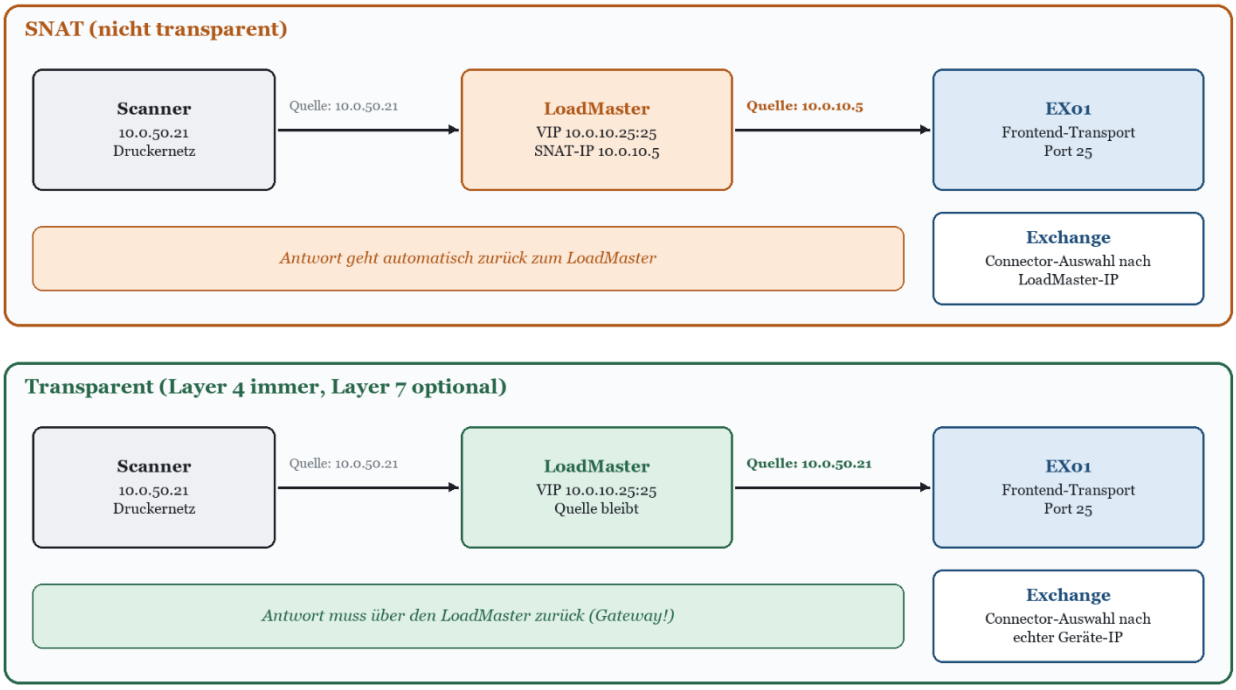
Die Option heißt im EAC „Extern gesichert (z. B. mit IPsec)“. Gemeint ist eine Leitung, die du kryptografisch oder physisch absicherst. Ein Load Balancer, der alle Absender auf eine Adresse zusammenfaltet, ist das Gegenteil davon. Wenn du hinter einem LoadMaster mit SNAT relayen musst, nimm die anonyme Variante und begrenze den Zugang woanders.

SNAT oder Transparenz: wer steht im Absenderfeld?

Der LoadMaster kann eine Verbindung auf zwei Arten an einen Real Server weiterreichen. Bei SNAT, also Source NAT, baut er eine eigene Verbindung zum Exchange-Server auf und verwendet dabei seine eigene Adresse als Quelle. Bei Transparenz lässt er die Quell-IP-Adresse des Clients stehen und ändert nur das Ziel. Für HTTPS ist das eine Frage der Protokollierung, im Detail beschrieben in Client-IP sichtbar machen: Transparenz, SNAT und X-Forwarded-For. Für SMTP ist es eine Frage der Sicherheit.

SNAT gegen Transparenz: welche Quell-IP Exchange sieht

Gleiche Verbindung, zwei Betriebsarten, zwei völlig verschiedene Empfangsconnectors



Skizze: Adressen frei erfunden, Prinzipdarstellung

SNAT: bequem, routingneutral und blind

SNAT ist der Modus, in dem die meisten Layer-7-Dienste am LoadMaster laufen, und er hat gute Gründe auf seiner Seite. Der Exchange-Server antwortet an den LoadMaster, weil die Verbindung von dort kam. Am Routing musst du nichts ändern, Clients im selben Subnetz wie die Server funktionieren, und der Default-Gateway der Exchange-Server bleibt, wo er war. Der Preis: Exchange sieht für jede Verbindung über die VIP dieselbe Adresse, nämlich die des LoadMasters. Für den Empfangsconnector sind Scanner, ERP-System, Mail-Gateway und Spammer damit ein und derselbe Absender.

Daraus folgen genau zwei Zustände. Steht die LoadMaster-Adresse in keinem Relay-Connector, landen alle auf dem Default-Connector und dürfen nur an die eigenen Domänen zustellen. Die Multifunktionsgeräte, die Scans an externe Empfänger schicken sollen, scheitern mit „550 5.7.54 SMTP; Unable to relay recipient in non-accepted domain“. Steht die Adresse dagegen in einem Relay-Connector, darf jeder relayen, der die VIP erreicht. Ein drittes Ergebnis kennt die Logik nicht.

WARNUNG · Offenes Relay in drei Klicks

Die IP-Adresse des LoadMasters, seine SNAT-Adresse oder gar das ganze Subnetz des LoadMasters in die RemoteIPRanges eines Relay-Connectors einzutragen, ist der Klassiker schlechthin. Es funktioniert sofort, und genau das ist das Problem.

Ist dieselbe VIP oder ein anderer Virtual Service mit SNAT auf Port 25 aus dem Internet erreichbar, betreibst du ab diesem Moment ein offenes Relay. Spammer finden das schneller als dein Monitoring. Die Quittung kommt als Blocklisteneintrag, als Warteschlange mit zehntausenden Nachrichten und als Gespräch mit der Geschäftsführung über die Frage, warum Rechnungen nicht mehr ankommen.

Auch intern ist das riskant: Jeder kompromittierte Client im Netz kann dann im Namen beliebiger Absender Mail nach außen schicken. Phishing mit Absender der eigenen Buchhaltung, zugestellt von deinem eigenen Exchange. Teste nach jeder Änderung von außen und von einem beliebigen Client aus, ob ein RCPT TO an eine fremde Domäne mit 550 abgelehnt wird.

Transparenz: die echte IP, aber mit Bedingungen

Im transparenten Modus reicht der LoadMaster die Verbindung mit der echten Quell-IP-Adresse durch. Exchange sieht den Scanner als Scanner, den Spammer als Spammer, und die Connector-Auswahl funktioniert, als gäbe es keinen Load Balancer. Layer-4-Dienste sind beim LoadMaster grundsätzlich transparent, und SMTP braucht in aller Regel kein Layer 7, weil der LoadMaster im Datenstrom nichts zu tun hat. Bei Layer-7-Diensten lässt sich Transparenz pro Virtual Service einschalten.

Die Physik verlangt dafür eine Gegenleistung. Wenn der Exchange-Server eine Antwort an 10.0.50.21 schickt, muss diese Antwort über den LoadMaster laufen, sonst sieht der Scanner ein Paket von einer Adresse, mit der er nie gesprochen hat, und verwirft es. Progress formuliert die Bedingungen nüchtern: Der LoadMaster muss Default-Gateway der Real Server sein, im HA-Paar die gemeinsame Adresse, und die Clients dürfen nicht im selben Subnetz wie die Real Server liegen. Beides hat Folgen, die weit über SMTP hinausgehen.

Kriterium	SNAT	Transparenz
Quell-IP in Exchange	Adresse des LoadMasters	echte Adresse des Absenders
Connector-Auswahl nach Gerät	nicht möglich	funktioniert wie ohne Load Balancer
Routing der Real Server	unverändert	Default-Gateway über den LoadMaster oder gezielte Routen für die Client-Netze
Clients im Server-Subnetz	unproblematisch	funktionieren nicht ohne Zusatzaufwand
Protokolle und Message Tracking	zeigen nur den LoadMaster	zeigen den echten Absender
IP-basierter Spamschutz	wirkungslos oder gefährlich	funktioniert
Auswirkung auf andere Dienste	keine	alle Antworten des Servers laufen über den LoadMaster, auch HTTPS und Ausgehendes

Wo Transparenz in der Praxis knallt

Der Default-Gateway ist kein SMTP-Detail, sondern eine Eigenschaft des ganzen Servers. Wird der LoadMaster zum Gateway der Exchange-Server, läuft ab sofort auch der ausgehende Internetverkehr, der Verkehr zu Domänencontrollern in anderen Netzen, Windows Update, die Sicherung und der Send-Connector zum Mail-Gateway über den LoadMaster. Der muss das alles routen können und im HA-Fall sauber übergeben. Wie sich das HA-Paar mit gemeinsamer Adresse verhält, steht in HA-Paar, Failover und Konfig-Sync: zwei LoadMaster, ein Gedanke.

Der zweite Stolperstein ist das Subnetz. Viele Umgebungen haben Fachanwendungen, Monitoring-Server oder sogar Scanner im selben Netz wie die Exchange-Server. Diese Clients schicken ihre Anfrage an die VIP, bekommen die Antwort aber direkt vom Exchange-Server, weil der sein eigenes Subnetz nicht über einen Gateway erreicht. Die TCP-Verbindung kommt nie zustande, und das Fehlerbild sieht im ersten Moment aus wie eine Firewall. Typischer Satz im Ticket: „Von meinem Rechner aus geht es, vom Applikationsserver nicht."

AUS DER PRAXIS · Halb transparent ist auch kaputt

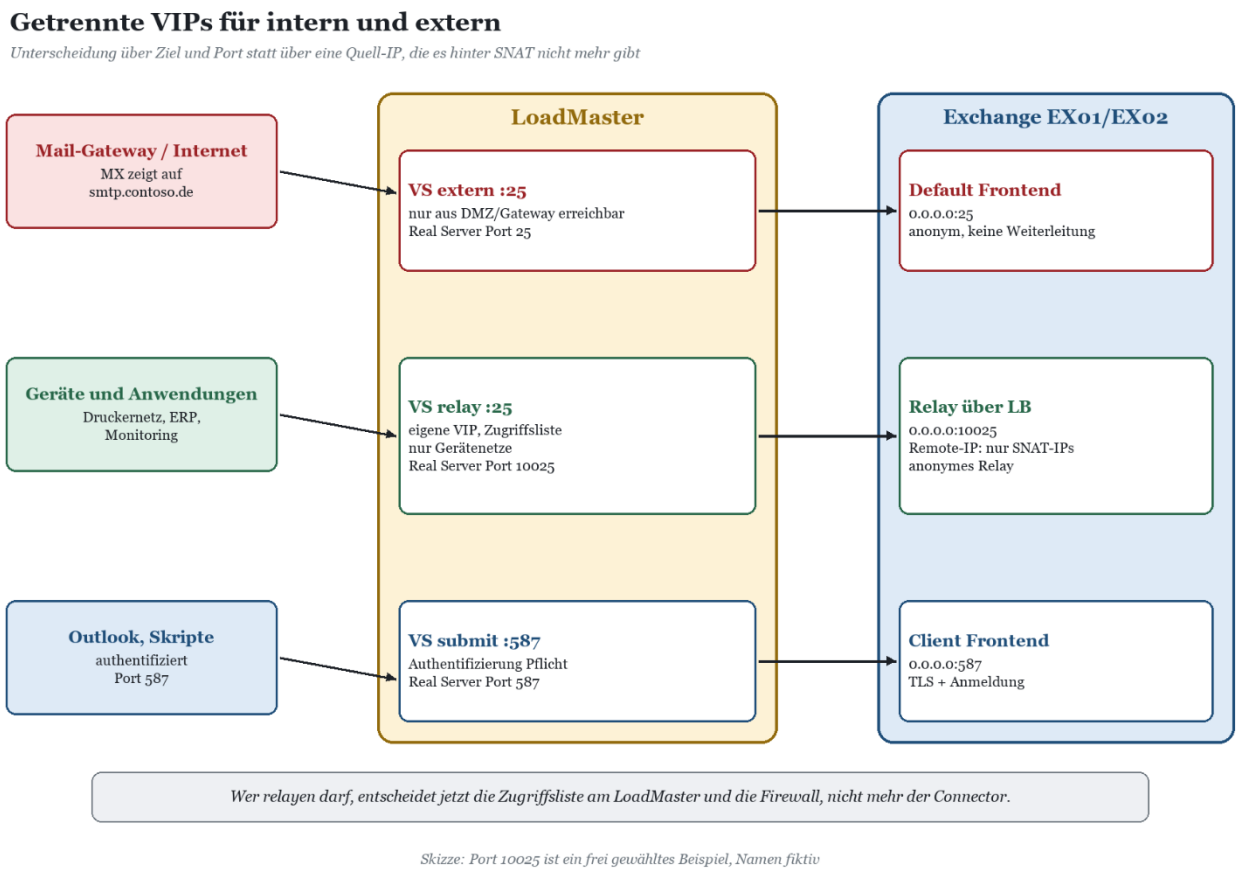
In einer Verwaltung mit zwei Exchange-Servern lief SMTP transparent über Layer 4. Die Scanner im Druckernetz funktionierten tadellos, das Ticketsystem im Servernetz verschickte dagegen sporadisch keine Mails. Sporadisch deshalb, weil das Ticketsystem bei einem Timeout auf einen hinterlegten zweiten Server direkt auswich. Die Lösung war kein LoadMaster-Schalter, sondern Ehrlichkeit: Das Ticketsystem spricht seitdem direkt mit beiden Exchange-Servern, ganz ohne VIP. Der LoadMaster bedient nur noch, wer ihn wirklich braucht.

TIPP · Kein Proxy-Protokoll für Exchange

Bei HTTPS hilft X-Forwarded-For, bei manchen Mailservern das PROXY-Protokoll, das die Client-Adresse vor den eigentlichen Datenstrom setzt. Exchange kennt für SMTP weder das eine noch das andere. Was der Empfangsconnector als Quelle sieht, ist die IP-Adresse im TCP-Header, Punkt. Für SMTP gibt es deshalb nur Transparenz, getrennte Wege oder SNAT mit einem Sicherheitskonzept, das ohne die Absender-IP auskommt.

Getrennte VIPs: intern, extern und alles dazwischen

Wenn Transparenz nicht in Frage kommt, weil niemand das Routing der Exchange-Server umbauen will, bleibt die Frage: Wie unterscheidet Exchange erlaubte Relay-Absender von allen anderen, wenn alle mit derselben Adresse ankommen? Die Antwort: Gar nicht mehr über die Quelle, sondern über das Ziel. Du baust für jede Vertrauensstufe einen eigenen Virtual Service und lässt jeden davon auf einem anderen Port oder einer anderen Server-IP landen. Der Connector entscheidet dann nach Bindung statt nach Absender.



Das Muster im Detail

- **VS extern auf Port 25:** nimmt Mail vom Mail-Gateway oder aus dem Internet an und leitet auf Port 25 der Exchange-Server weiter. Dort landet sie auf dem Default-Connector, der nur an eigene Domänen zustellt. Hier darf SNAT laufen, denn auf diesem Weg soll ohnehin niemand relayen.
- **VS relay mit eigener VIP:** nur aus den Gerätenetzen erreichbar, abgesichert per Zugriffsliste am Virtual Service und per Firewall. Der LoadMaster leitet auf einen eigenen Port der Exchange-Server weiter, etwa 10025. Der LoadMaster erlaubt pro Real Server einen anderen Zielport als den der VIP.
- **Relay-Connector auf dem eigenen Port:** Bindung 0.0.0.0:10025, RemoteIPRanges nur die SNAT-Adressen des LoadMasters, Rechte anonym mit Accept-Any-Recipient. Wer diesen Port erreicht, kommt per Definition durch die Relay-VIP.
- **VS submit auf Port 587:** für Clients und Anwendungen, die sich anmelden können. Hier ist SNAT harmlos, weil die Anmeldung über die Rechte entscheidet und nicht die Adresse.

```
# Relay-Connector auf eigenem Port, erreichbar nur über die Relay-VIP
New-ReceiveConnector -Name "Relay via LoadMaster" -Server EX01 `
  -TransportRole FrontendTransport -Custom `
  -Bindings 0.0.0.0:10025 -RemoteIPRanges 10.0.10.5,10.0.10.6
Set-ReceiveConnector "EX01\Relay via LoadMaster" -PermissionGroups AnonymousUsers
Get-ReceiveConnector "EX01\Relay via LoadMaster" |
  Add-ADPermission -User "NT AUTHORITY\ANONYMOUS LOGON" `
  -ExtendedRights "Ms-Exch-SMTP-Accept-Any-Recipient"
```

Der Trick dabei: Die Sicherheitsgrenze wandert vom Exchange-Server zum LoadMaster und zur Firewall. Wer bisher im Connector gepflegt hat, welcher Scanner relayen darf, pflegt das jetzt in der Zugriffsliste des Virtual Service. Das ist kein Nachteil, solange es jemand weiß und dokumentiert.

Es ist ein gewaltiger Nachteil, wenn der nächste Kollege die Exchange-Connectors prüft, dort nur „SNAT-Adressen“ findet und daraus schließt, alles sei eng begrenzt.

WARNUNG · Port 10025 darf nur der LoadMaster erreichen

Der zusätzliche Port ist auf dem Exchange-Server für jeden offen, der ihn im Netz erreicht. Weil RemoteIPRanges nur die SNAT-Adressen enthält, landet ein direkter Zugriff von einem anderen Rechner zwar nicht auf dem Relay-Connector. Wenn aber kein anderer Connector auf diesem Port passt, lehnt Exchange die Verbindung ab, und das ist gewollt. Lege auf Port 10025 deshalb niemals einen zweiten Connector mit großem Remote-Bereich an und sperre den Port zusätzlich in der Windows-Firewall für alles außer den LoadMaster.

Health Checks für SMTP

Für SMTP reicht ein reiner TCP-Check fast nie. Ein Frontend-Transport-Dienst, der hängt, nimmt Verbindungen gelegentlich noch an und antwortet dann nicht mehr. Der LoadMaster bringt einen SMTP-Check mit, der das Begrüßungsbanner des Servers auswertet. Das ist besser als ein offener Port, sagt aber nichts über volle Warteschlangen oder eine Back-Pressure-Situation, in der Exchange Nachrichten mit temporären Fehlern abweist. Prüfe deshalb im Monitoring zusätzlich die Warteschlangen, und nimm einen Server vor Wartungsarbeiten auch am LoadMaster aus dem Pool. Was ein guter Check prüft und was nicht, beschreibt Health Checks, die wirklich prüfen: warum „Port 443 offen“ nicht reicht.

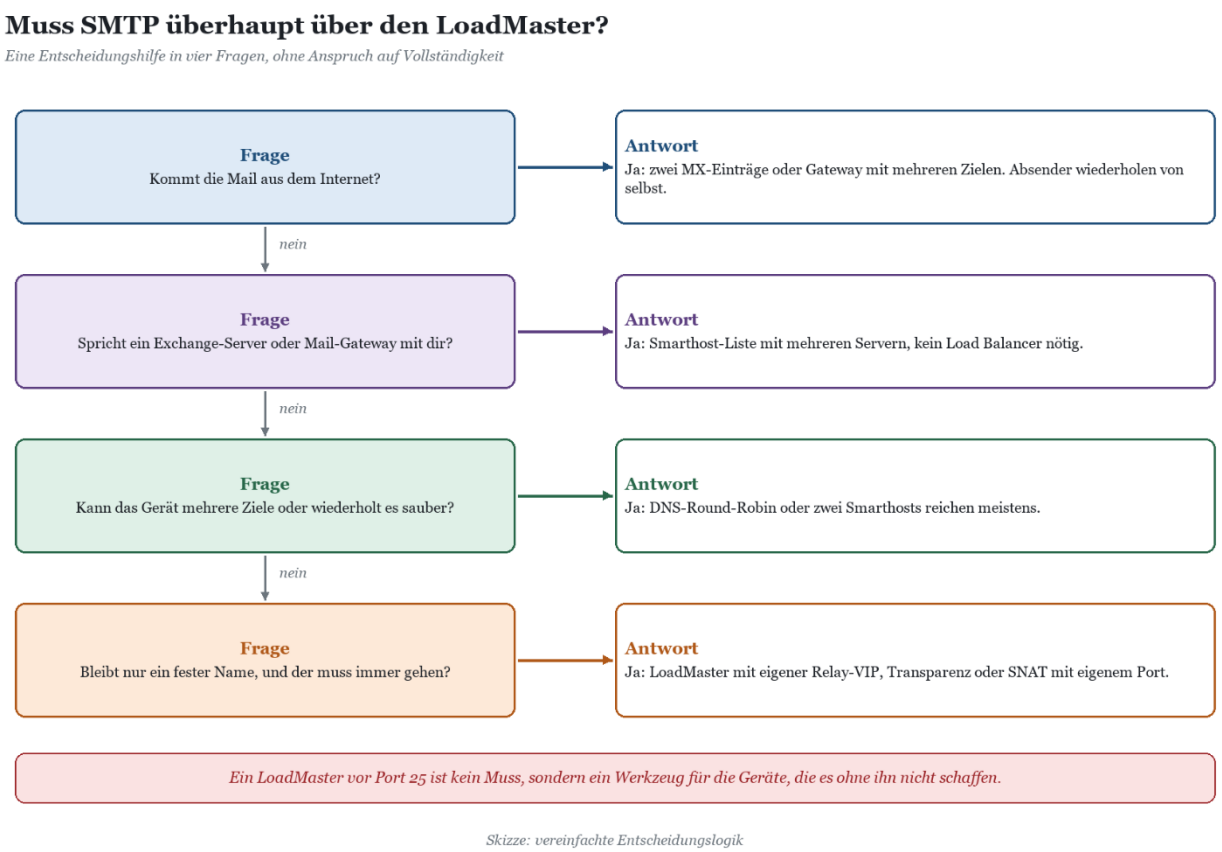
Virtual Service	Zielport Exchange	SNAT	Zugang	Connector
smtp-extern	25	ja, unkritisch	nur Mail-Gateway oder MX-Eingang	Default Frontend
smtp-relay	10025 (Beispiel)	ja, gewollt	nur Gerätenetze per Zugriffsliste	Relay via LoadMaster
smtp-submit	587	ja, unkritisch	intern, Anmeldung Pflicht	Client Frontend
smtp-relay-transparent	25	nein, Layer 4	Gerätenetze, Routing über LoadMaster	Relay-Connector je Gerätenetz

TLS gehört an den Exchange-Server

Bei HTTPS ist es normal, dass der LoadMaster TLS auspackt. Bei SMTP solltest du das lassen. STARTTLS ist ein Teil der SMTP-Unterhaltung, der Exchange-Server bietet es mit seinem eigenen Zertifikat an, und gerade Verbindungen mit Exchange Online in Hybridumgebungen hängen an genau diesem Zertifikat. Ein SMTP-Virtual-Service auf Layer 4, der den Datenstrom unangetastet durchreicht, ist hier die robuste Wahl. Alles andere erhöht nur die Zahl der Stellen, an denen ein abgelaufenes Zertifikat einen Freitagnachmittag ruiniert.

Alternativen: SMTP ohne Load Balancer verteilen

Ein Satz, den Load-Balancer-Verkäufer ungern hören: SMTP ist von Haus aus redundant. Ein Mailserver, der einen Empfänger nicht erreicht, versucht es später erneut und probiert dabei auch weitere MX-Einträge. Exchange-Server verteilen untereinander selbst. Viele Probleme rund um SMTP und LoadMaster verschwinden, wenn man sich ehrlich fragt, welcher Absender den Load Balancer überhaupt braucht.



Skizze: vereinfachte Entscheidungslogik

Direkte Zustellung per MX und Smarthost-Liste

Für eingehende Internet-Mail sind zwei MX-Einträge mit gleicher Priorität, die auf zwei Exchange-Server oder zwei Gateway-Knoten zeigen, die älteste und zuverlässigste Form der Lastverteilung. Absendende Server wählen selbst, wiederholen selbst und brauchen keinen Health Check, weil sie einen nicht antwortenden Server schlicht überspringen. Steht ein Mail-Gateway davor, trägt man dort mehrere Exchange-Server als Zustellziel ein. Das Gateway merkt Ausfälle selbst und liefert die echte Quell-IP gleich mit, weil es direkt mit Exchange spricht.

DNS-Round-Robin für Geräte

Für interne Relay-Absender ist ein Name wie relay.contoso.local mit zwei A-Einträgen die einfachste Lösung. Exchange sieht die echte Geräte-IP, die Relay-Connectors funktionieren wie dokumentiert, und der LoadMaster hat Feierabend. Die Schwäche ist bekannt: DNS weiß nicht, ob ein Server lebt. Gute Absender probieren die nächste Adresse, schlechte, und dazu zählen erschreckend viele Multifunktionsgeräte, bleiben an der ersten hängen, bis jemand den Drucker neu startet.

Variante	Echte Absender-IP	Erkennt Ausfälle	Aufwand	Passt für
MX-Einträge / Gateway-Zielliste	ja	ja, durch den Absender	gering	Internet-Mail, Mail-Gateways
DNS-Round-Robin	ja	nein	gering	Geräte und Anwendungen mit Wiederholung
Mehrere Smarthosts im Gerät	ja	meist ja	gering bis mittel	Anwendungen mit konfigurierbarem Fallback
LoadMaster	ja	ja, per Health	hoch, Routing	Gerätenetze, wenn

transparent (L4)		Check		Routing ohnehin über LoadMaster
LoadMaster SNAT mit eigenem Port	nein	ja, per Health Check	mittel	Geräte mit festem Namen, ohne Routing-Umbau
LoadMaster SNAT auf Port 25 mit LB-IP im Relay	nein	ja	gering	niemanden. Wirklich niemanden.

Wie du herausfindest, was Exchange wirklich sieht

Bevor du an Connectors drehst, schau nach, welche Adressen tatsächlich ankommen. Das SMTP-Protokollprotokoll des Frontend-Transport-Dienstes zeigt pro Verbindung die Remote-Adresse und den Connector, der sie angenommen hat. Es liegt unterhalb des Exchange-Installationspfads unter TransportRoles\Logs\FrontEnd\ProtocolLog\SmtpReceive und muss pro Connector eingeschaltet sein.

```
# Welche Connectors gibt es, worauf lauschen sie, für wen gelten sie?
Get-ReceiveConnector -Server EX01 | Format-Table Name,Bindings,RemoteIPRanges -Auto

# Protokollierung für die Fehlersuche einschalten
Set-ReceiveConnector "EX01\Default Frontend EX01" -ProtocolLoggingLevel Verbose
```

Taucht im Protokoll bei Verbindungen von Scannern die Adresse des LoadMasters auf, läuft der Virtual Service mit SNAT, egal was in der Konfigurationsdokumentation steht. Taucht die Scanner-Adresse auf, aber die Verbindung bricht ab, schau auf Routing und Subnetze. Wie du am LoadMaster selbst mitschneidest, um die andere Seite der Leitung zu sehen, erklärt Troubleshooting am LoadMaster: Logs, L7-Debug und TCP-Dump.

TIPP · Der Fünf-Minuten-Relay-Test

Baue von einem Rechner außerhalb der erlaubten Netze eine SMTP-Verbindung zur VIP auf, sende EHLO, MAIL FROM mit einer eigenen Adresse und RCPT TO an eine externe Domäne. Die richtige Antwort ist 550 5.7.54. Wiederhole den Test aus einem erlaubten Gerätenetz, dort muss 250 kommen. Und dann ein drittes Mal von außerhalb des Firmennetzes. Wer diesen Test nach jeder Änderung am LoadMaster oder an den Connectors macht, schläft ruhiger.

FAQ: Häufige Fragen zu SMTP über den Kemp LoadMaster

Warum bekommen meine Multifunktionsgeräte plötzlich „550 5.7.54 Unable to relay“?

Weil Exchange sie seit der Umstellung auf den LoadMaster nicht mehr an ihrer Adresse erkennt. Mit SNAT kommt jede Verbindung von der LoadMaster-Adresse, landet auf dem Default-Connector und darf nur an eigene Domänen zustellen. Die Lösung ist Transparenz, ein eigener Relay-Port oder der direkte Weg zum Exchange-Server, nicht die LoadMaster-Adresse im Relay-Connector.

Darf ich die IP-Adresse des LoadMasters in den Relay-Connector eintragen?

Nur, wenn ausschließlich ein Virtual Service mit strikter Zugriffsliste diese Adresse als Quelle nutzen kann und dieser Weg auf einem eigenen Port landet. Auf Port 25, über den auch andere Absender kommen, ist es ein offenes Relay mit Ankündigung.

Ist ein Layer-4-Virtual-Service am LoadMaster automatisch transparent?

Ja. Layer-4-Dienste reichen die Client-Adresse beim LoadMaster grundsätzlich durch. Damit das funktioniert, muss die Antwort des Exchange-Servers wieder über den LoadMaster laufen, in der Regel als Default-Gateway, und die Clients dürfen nicht im Subnetz der Exchange-Server liegen.

Kann Exchange die echte Absender-IP aus einem Header lesen, wie X-Forwarded-For bei HTTPS?

Nein. Der Empfangsconnector wählt anhand der IP-Adresse der TCP-Verbindung. Exchange unterstützt für SMTP weder einen solchen Header noch das PROXY-Protokoll.

Brauche ich für eingehende Internet-Mail überhaupt einen Load Balancer?

Meistens nicht. Mehrere MX-Einträge oder ein Mail-Gateway mit mehreren Zustellzielen verteilen zuverlässig und behalten die echte Absender-IP. Ein LoadMaster lohnt sich hier vor allem, wenn ohnehin nur eine öffentliche Adresse zur Verfügung steht.

Was passiert mit Port 587, wenn ich SNAT verwende?

Funktional nichts, weil sich Clients dort anmelden und die Anmeldung über die Rechte entscheidet. Beachte aber, dass fehlgeschlagene Anmeldungen und Drosselungen in Exchange dann alle derselben Adresse zugeordnet werden.

Soll der LoadMaster bei SMTP TLS terminieren?

In aller Regel nicht. STARTTLS gehört zur SMTP-Sitzung mit dem Exchange-Server, und gerade der Mailfluss mit Exchange Online in Hybridumgebungen hängt am Zertifikat des Exchange-Servers. Reiche SMTP auf Layer 4 durch.

Fazit: Bei SMTP ist die Absender-IP ein Schlüssel

SMTP über den LoadMaster ist kein schwieriges Thema, aber eines mit einer einzigen, gemeinen Falle. Exchange vertraut bei anonymen Verbindungen der Quell-IP-Adresse, und der LoadMaster kann diese Adresse mit SNAT durch seine eigene ersetzen. Wer das übersieht, landet zuverlässig in einer von zwei Ecken: abgewiesene Scanner oder offenes Relay. Die Ecke mit dem offenen Relay ist die teurere, auch ohne Preisschild.

Saubere Lösungen gibt es drei. Transparenz auf Layer 4, wenn du das Routing der Exchange-Server bewusst über den LoadMaster führst und keine Clients im Server-Subnetz hast. Getrennte Virtual Services mit eigenem Port, wenn SNAT bleiben soll und die Sicherheitsgrenze an den LoadMaster wandern darf. Und, häufiger als gedacht: gar kein Load Balancer, sondern MX-Einträge, Gateway-Zielliste, Smarthost-Listen oder DNS. Welche Variante du wählst, ist weniger wichtig als die Gewissheit, dass du weißt, welche IP-Adresse in deinem Protokollprotokoll steht. Und dass du den Relay-Test nach jeder Änderung wiederholst. Das ist langweilig. Langweilig ist bei Port 25 ein Kompliment.

TIPP · Unterstützung bei Planung und Umsetzung

Wenn du SMTP-Relay und Empfangsconnectors hinter dem LoadMaster neu ordnen oder ein gewachsenes Setup auf offene Türen prüfen willst, hilft dir die Beratung zum Kemp LoadMaster. Wer Transparenz, SNAT und Relay-Tests mit dem eigenen Team im Labor durchspielen will, findet das in der Kemp-LoadMaster-Schulung.

WEITERLESEN · Weiter im Thema

› Exchange Server hinter dem LoadMaster: Templates, Namespaces, Health Checks

› Client-IP sichtbar machen: Transparenz, SNAT und X-Forwarded-For

› Health Checks, die wirklich prüfen: warum „Port 443 offen“ nicht reicht
› Troubleshooting am LoadMaster: Logs, L7-Debug und TCP-Dump