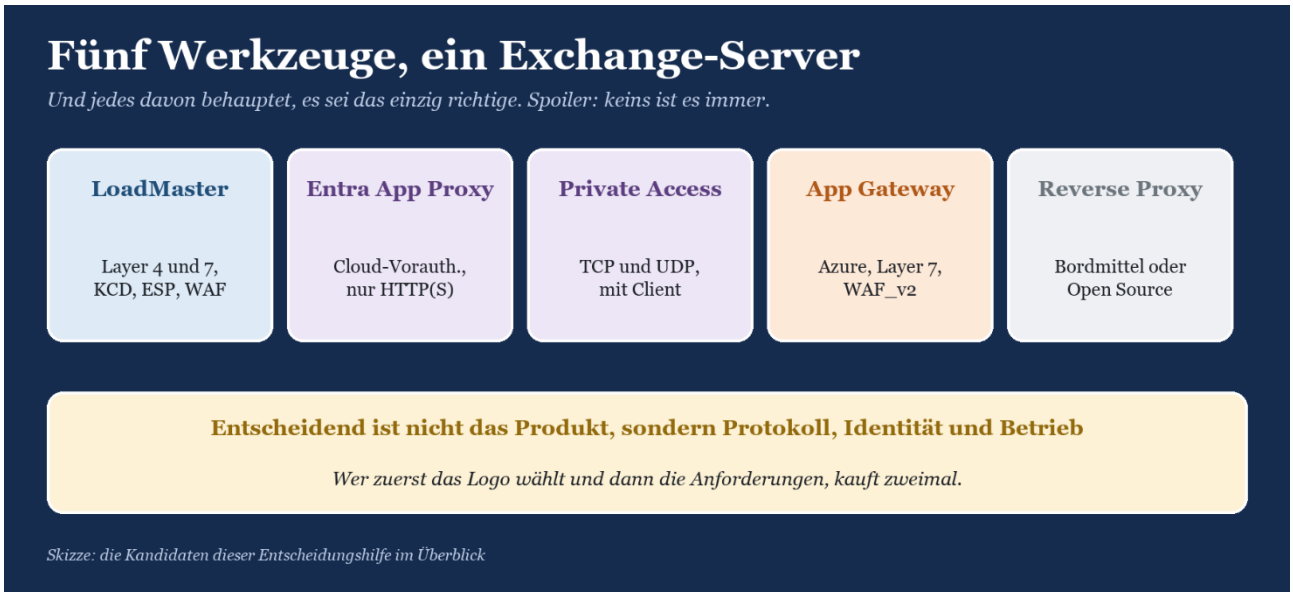
Entscheidungshilfe: LoadMaster, Entra Application Proxy, Azure Application Gateway oder Reverse Proxy?



Skizze: die Kandidaten dieser Entscheidungshilfe im Überblick

WISSEN

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

› **Kemp LoadMaster**

BERATUNG

LoadMaster behalten, ablösen oder mit Entra kombinieren? Wir prüfen mit dir jede veröffentlichte Anwendung und geben eine Empfehlung, die auch nachts um zwei hält.

› **Beratung zum Kemp LoadMaster**

SCHULUNG

Virtual Services, ESP und KCD im Labor bauen, damit du die Alternativen fair vergleichen kannst und nicht nur die Folien der Hersteller.

› **Kemp-LoadMaster-Schulung**

Irgendwann kommt die Frage. Meistens in einem Meeting, in dem jemand eine Folie mit dem Wort „Zero Trust“ zeigt, und meistens kurz bevor der Wartungsvertrag des LoadMasters verlängert werden soll. „Brauchen wir das Ding überhaupt noch? Microsoft hat doch den Application Proxy. Und Azure hat ein Application Gateway. Und der Kollege aus der Nachbarabteilung schwört auf NGINX.“ Alle Blicke wandern zu dir. Du betreibst den LoadMaster vor Exchange, SharePoint, ADFS und der Fachanwendung, die ein Dienstleister 2014 gebaut und seitdem nicht mehr angefasst hat. Du weißt, dass die Antwort nicht in eine Folie passt.

Wer nach einer kemp loadmaster alternative sucht, findet viele Vergleiche. Die meisten stammen von Herstellern, die zufällig genau das empfehlen, was sie verkaufen, oder von Cloud-Enthusiasten, die noch nie einen SMTP-Empfangsconnector hinter einem Proxy debuggt haben. Dieser Beitrag ist der Abschluss unserer Serie rund um den Kemp LoadMaster, und er versucht etwas Unbequemes: ehrlich zu sein. Es gibt Szenarien, in denen der LoadMaster die falsche Wahl ist. Es gibt mehr Szenarien, in denen die Alternativen an Stellen scheitern, die auf keiner Produktseite stehen. Und es gibt erstaunlich viele, in denen die beste Antwort „beides“ lautet.

Wir vergleichen fünf Kandidaten nach sechs Kriterien: Wie gut kommen sie mit On-Premises-Workloads zurecht? Können sie Kerberos und Constrained Delegation? Was ist mit Layer-4-Protokollen wie SMTP? Wie sieht die Vorauthentifizierung aus? Was kostet der Betrieb an Nerven? Und wie passt das Ganze zur Cloud-Strategie, die deine Geschäftsführung oder dein Ministerium

gerade verabschiedet hat? Preise lassen wir bewusst weg. Die ändern sich schneller als Produktnamen, und das will bei Microsoft etwas heißen.

FAKTEN · Das Wichtigste in 30 Sekunden

Entra Application Proxy veröffentlicht nur HTTP- und HTTPS-Anwendungen. Er kann per Kerberos Constrained Delegation an Anwendungen mit integrierter Windows-Authentifizierung weiterreichen, verteilt aber keine Last auf mehrere Backend-Server.

Der Private Network Connector baut nur ausgehende Verbindungen über die Ports 80 und 443 auf. Derselbe Connector bedient auch Entra Private Access, das TCP und UDP tunnelt, dafür aber den Global Secure Access Client auf dem Endgerät braucht.

Azure Application Gateway v1 ist seit dem 28. April 2026 abgekündigt und nicht mehr unterstützt. Der Layer-4-Proxy für TCP und TLS im v2 ist laut Microsoft noch Preview, und die WAF greift dort nicht.

Windows Server 2025 führt Network Load Balancing als nicht mehr weiterentwickelt. Der SMTP-Server ist aus Windows Server 2025 entfernt, und Forefront TMG ist seit April 2020 ohne Support.

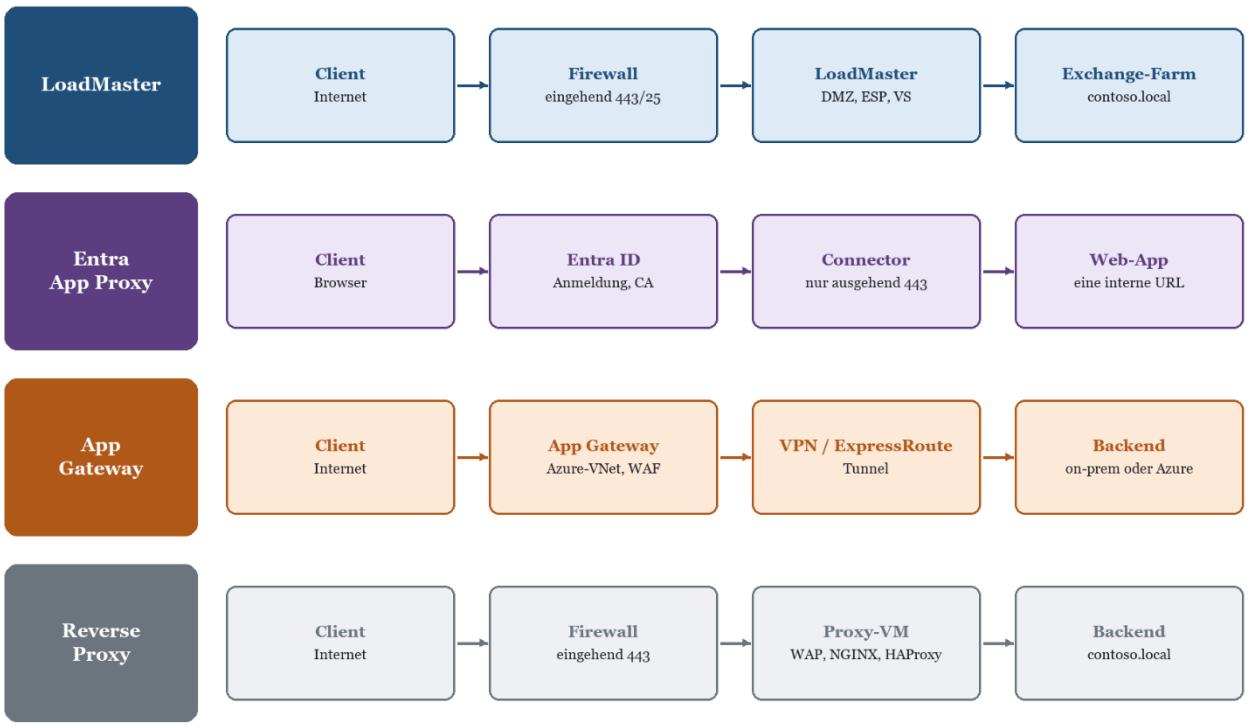
Der LoadMaster ist der einzige Kandidat in diesem Vergleich, der Layer 4, Layer 7, Vorauthentifizierung, KCD und Lastverteilung in einem Gerät vereint. Dafür betreibst du ihn selbst, mit allem, was dazugehört.

Die Kandidaten: fünf Werkzeuge, fünf Weltbilder

Bevor wir Häkchen in Tabellen setzen, lohnt ein Blick darauf, wofür die Werkzeuge eigentlich gebaut wurden. Viele Fehlentscheidungen entstehen, weil jemand ein Produkt für etwas einsetzt, das es zwar kann, für das es aber nie gedacht war. Das ist wie mit dem Schweizer Taschenmesser: Die Säge funktioniert, aber du möchtest damit keinen Dachstuhl bauen.

Vier Wege ins Rechenzentrum: wo der Verkehr wirklich entlangläuft

Gleiches Ziel, völlig unterschiedliche Wege. Und unterschiedliche Stellen, an denen es klemmt



Skizze: vereinfacht; Namen und Zonen frei gewählt, HA-Partner nicht dargestellt

Progress Kemp LoadMaster: der Allrounder im eigenen Rack

Der LoadMaster ist ein Application Delivery Controller im klassischen Sinn: ein Gerät, physisch oder virtuell, das Verbindungen annimmt, auf Real Server verteilt, deren Gesundheit prüft und dabei wahlweise auf Layer 4 durchreicht oder auf Layer 7 TLS terminiert, Header umschreibt und Inhalte inspiziert. Mit dem Edge Security Pack kommt Vorauthentifizierung hinzu, inklusive Kerberos Constrained Delegation zum Backend, mit SAML und OIDC auch gegen Entra ID. Das macht ihn zum natürlichen Erben von Forefront TMG, und genau deshalb steht er in so vielen Microsoft-Umgebungen vor Exchange.

Sein Weltbild ist das Rechenzentrum: Der Verkehr kommt von außen durch die Firewall in die DMZ, der LoadMaster entscheidet, und die Server dahinter bleiben unsichtbar. Das funktioniert hervorragend, solange du ein Rechenzentrum hast, eingehende Ports öffnen darfst und jemanden, der Firmware-Updates einspielt. In Azure läuft er als VM aus dem Marketplace, mit eigenen Eigenheiten, die wir in LoadMaster in Azure und hybriden Umgebungen beschrieben haben.

Entra Application Proxy und Entra Private Access: Microsofts Antwort ohne DMZ

Der Application Proxy dreht das Modell um. Es gibt keine eingehende Verbindung ins Unternehmensnetz mehr. Stattdessen läuft auf einem oder besser mehreren Windows Servern im internen Netz der Private Network Connector, der eine ausgehende Verbindung zum Dienst in Entra ID hält. Nutzerinnen und Nutzer melden sich bei Entra ID an, Conditional Access und MFA greifen, und erst danach holt der Connector die Anfrage ab und reicht sie an die interne URL weiter. Für Anwendungen mit integrierter Windows-Authentifizierung macht der Connector dabei Kerberos Constrained Delegation, für andere gibt es SAML, Header-basiertes SSO oder Kennworttresore.

Das Weltbild ist die Identität: Nicht das Netz entscheidet, wer reindarf, sondern Entra ID. Das ist elegant und für Webanwendungen oft genau richtig. Es hat aber zwei Grenzen, die gern übersehen werden. Erstens: nur HTTP und HTTPS. Zweitens: Der Application Proxy ist kein Load Balancer. Er kennt pro veröffentlichter Anwendung genau eine interne URL. Wenn hinter dieser URL eine Farm steht, braucht die Farm weiterhin etwas, das die Last verteilt und kranke Server aussortiert. Microsoft schreibt außerdem ausdrücklich, dass der Dienst für Remote-Zugriffe gedacht ist und nicht für interne Nutzer, die im Firmennetz sitzen.

Entra Private Access ist der jüngere Bruder mit breiterem Kreuz. Er nutzt denselben Connector, tunnelt aber beliebige TCP- und UDP-Verbindungen zu Adressen und Namen, die du als privat definierst, entweder als Quick Access oder als einzelne App mit eigenen Conditional-Access-Richtlinien. Der Preis dafür ist ein Agent: Ohne Global Secure Access Client auf dem Endgerät geht nichts. Für verwaltete Clients der eigenen Belegschaft ist das wunderbar, als VPN-Ersatz sogar ausgezeichnet. Für externe Absender, die dir eine Mail schicken wollen, oder für das Smartphone eines Partners ist es keine Lösung.

> **WICHTIG · Application Proxy ersetzt den Zugang, nicht den Load Balancer**
>
> Der häufigste Denkfehler in Projekten: „Wir machen App Proxy, dann können wir den LoadMaster abschalten." Für eine einzelne Webanwendung auf einem Server stimmt das. Für Exchange mit vier Servern, für eine SharePoint-Farm oder für RD Web Access mit mehreren Knoten stimmt es nicht. Die Connectoren selbst sind über Connector-Gruppen redundant, aber sie sprechen mit genau einer internen Adresse. Steht dort ein einzelner Server, ist er dein neuer Single Point of Failure.

Azure Application Gateway: der Layer-7-Balancer aus der Steckdose

Das Application Gateway ist ein verwalteter Layer-7-Load-Balancer in einem Azure-VNet. Es terminiert TLS, routet nach Hostnamen und Pfaden, prüft Backends per Health Probe, skaliert

automatisch und bringt mit der WAF_v2-Variante eine Web Application Firewall mit. Backends dürfen auch im eigenen Rechenzentrum stehen, sofern sie per VPN oder ExpressRoute erreichbar sind. Seit dem 28. April 2026 gibt es nur noch die v2-Generation, die alte v1 ist abgekündigt und wird laut Microsoft bereits abgebaut.

Das Weltbild ist die Azure-Landezone. Was dort wohnt, schützt das Application Gateway sehr gut. Was es nicht ist: ein Identitätsdienst. Eine Vorauthentifizierung gegen Entra ID macht es nicht selbst, und Kerberos Constrained Delegation schon gar nicht. Immerhin kann die v2-Generation inzwischen Anfragen mit NTLM- oder Kerberos-Authentifizierung durchreichen, wenn du dedizierte Backend-Verbindungen aktivierst. Der Client spricht dann direkt mit dem Backend Kerberos, das Gateway hält nur die Leitung. Für Layer 4 gibt es einen TCP- und TLS-Proxy, den Microsoft Stand Oktober 2026 in der FAQ weiterhin als Preview führt, ohne UDP und ohne WAF-Schutz.

Windows-Bordmittel: WAP, ARR und NLB

Microsoft hat über die Jahre einiges ins Betriebssystem gepackt, das irgendwie nach Reverse Proxy riecht. Der Web Application Proxy, die Rolle aus dem Remote-Access-Umfeld, ist der legitime Kern: Er veröffentlicht ADFS nach außen und kann Anwendungen mit ADFS-Vorauthentifizierung und Kerberos-Delegation publizieren. Lastverteilung kann er nicht, mehrere WAP-Server brauchen selbst wieder einen Balancer davor. Application Request Routing ist eine IIS-Erweiterung, deren letzte Hauptversion 3.0 aus dem Jahr 2013 stammt. Network Load Balancing schließlich steht in der Liste der Funktionen, die ab Windows Server 2025 nicht mehr weiterentwickelt werden.

Das Weltbild hier ist: Es war schon da. Das ist kein schlechtes Argument, solange der Bestand klein und überschaubar ist. Es wird zum schlechten Argument, wenn drei Bordmittel zusammengesteckt werden müssen, um das zu erreichen, was ein Gerät allein kann. Wie der Umzug von diesen Altlasten aussieht, steht ausführlich in Migration von Windows NLB, IIS ARR oder TMG-Erbe auf den LoadMaster.

Open-Source-Reverse-Proxys: HAProxy, NGINX, Traefik und Freunde

HAProxy und NGINX sind technisch ausgezeichnete Werkzeuge. Beide können Layer 4 und Layer 7, beide sind schnell, beide laufen auf einer kleinen Linux-VM. Traefik und Envoy spielen ihre Stärken eher in Container-Welten aus, Apache httpd mit mod_proxy hat schon mehr Rechenzentren gesehen als die meisten von uns. Das Weltbild ist der Baukasten: Du bekommst exzellente Teile und baust daraus, was du brauchst. Vorauthentifizierung gegen Entra ID? Mit Zusatzmodulen oder einem vorgeschalteten Identity-Proxy machbar. Kerberos Constrained Delegation im Namen des Nutzers? Da wird es dünn, und für Exchange-Szenarien landest du schnell in Eigenbau, den außer dir niemand versteht.

> **WARNUNG · Der Bus-Faktor ist ein Kriterium**
>
> Eine handgeschriebene HAProxy-Konfiguration vor Exchange ist so lange eine gute Idee, wie die Kollegin oder der Kollege, die sie geschrieben haben, im Haus ist. Danach ist sie ein Rätsel mit Produktionsverantwortung. Bevor du dich für den Baukasten entscheidest, frag ehrlich: Wer im Team kann das in drei Jahren noch lesen, testen und nachts reparieren? Wenn die Antwort ein einzelner Name ist, hast du keine Architektur, sondern eine Abhängigkeit.

Der Vergleich nach Kriterien

Jetzt die Häkchen. Damit die Tabelle nicht lügt, erst die Erklärung, was hinter jedem Kriterium steckt und warum es in Microsoft-Umgebungen so viel Gewicht hat.

On-Premises-Workloads: Exchange, SharePoint, ADFS, RDS

Die klassischen Microsoft-Serverprodukte haben eines gemeinsam: Sie wurden für ein Rechenzentrum mit Active Directory gebaut, sprechen mehr als ein Protokoll und erwarten, dass vor ihnen jemand die Last verteilt. Exchange braucht HTTPS für OWA, ECP, EWS, MAPI over HTTP, ActiveSync und Autodiscover, dazu SMTP, gegebenenfalls IMAP und POP. SharePoint Server ist reines HTTPS, möchte aber Lastverteilung und versteht sich am besten mit Kerberos. ADFS will eine Farm mit Probe-Endpunkt und davor WAP. RDS spricht HTTPS für RD Web, HTTPS und UDP für das RD Gateway und RDP für den Connection Broker.

Der LoadMaster deckt das komplett ab, Templates für die Microsoft-Workloads inklusive. Der Application Proxy deckt OWA, SharePoint und RD Web gut ab, alles mit Kerberos bis zum Backend. Outlook-Desktop, ActiveSync und SMTP sind dagegen nicht sein Revier, und die Lastverteilung musst du anderweitig lösen. Das Application Gateway ist stark, wenn die Anwendung in Azure läuft, und mühsam, wenn jede Anfrage durch den VPN-Tunnel zurück ins eigene Rechenzentrum muss. Die Bordmittel können das irgendwie, Open Source kann es technisch, aber mit viel Handarbeit pro Dienst.

Kerberos und KCD: das unsichtbare Kriterium

Kerberos taucht in keiner Marketingfolie auf und entscheidet trotzdem über Erfolg oder Misserfolg. Sobald ein Gerät vorauthentifiziert, also den Nutzer kennt, bevor die Anfrage das Backend erreicht, muss es dem Backend irgendwie mitteilen, wer da kommt. Bei Windows-Anwendungen heißt das: Es holt sich im Namen des Nutzers ein Kerberos-Ticket, per Constrained Delegation oder ressourcenbasierter Delegation. Das können der LoadMaster mit ESP, der Application-Proxy-Connector und der Web Application Proxy. Das Application Gateway kann es nicht, es reicht nur durch. Open-Source-Proxys können es nur mit erheblichem Zusatzaufwand.

In der Praxis knallt es dann an denselben Stellen, egal welches Produkt delegiert: SPN auf dem falschen Konto, Delegation nur auf HTTP statt auf den richtigen Dienst, und seit Windows Server 2025 RC4 als veraltet markiert ist, Keytabs oder Konten, die noch RC4 erwarten. Die Grundlagen dazu findest du auf der Seite Microsoft Kerberos, die LoadMaster-Seite der Delegation in Kerberos Constrained Delegation am LoadMaster: KCD und RBCD sauber einrichten. Wer einmal verstanden hat, warum Delegation scheitert, debuggt sie an jedem der Kandidaten.

Layer 4: SMTP, RDP und alles, was kein Browser ist

Hier trennt sich das Feld am deutlichsten. Der Application Proxy ist ein reiner HTTP-Dienst, SMTP bekommt er nicht. Private Access könnte TCP 25 tunneln, aber nur für Geräte mit Client, und der Mailserver eines Geschäftspartners wird ihn eher nicht installieren. Das Application Gateway hat den Layer-4-Proxy in Preview, ohne WAF. Windows Server 2025 hat den SMTP-Server gleich ganz entfernt, Microsoft verweist auf Exchange oder Drittprodukte. Bleiben LoadMaster und Open Source.

Und selbst dort ist SMTP kein Selbstläufer, weil Exchange für Empfangsconnectors die echte Absender-IP sehen will. Wer per SNAT verteilt, macht aus jedem Absender den Load Balancer und damit im schlimmsten Fall ein offenes Relay. Wie du das sauber löst, steht in SMTP über den LoadMaster: Relay, Empfangsconnectors und die echte Absender-IP. Für diese Entscheidungshilfe reicht: Wenn du SMTP, IMAP oder RDP-Verkehr verteilen musst, ist jede reine Web-Lösung nur die halbe Antwort.

Vorauthentifizierung: wer darf überhaupt anklopfen?

Vorauthentifizierung heißt: Unangemeldeter Verkehr erreicht das Backend nicht. Das ist der Hauptgrund, warum OWA nicht einfach nackt im Internet stehen sollte. Hier ist der Application Proxy der Klassenprimus, weil er Conditional Access, MFA, Gerätestatus und Anmelderisiko aus Entra ID ohne Zusatzaufwand mitbringt. Der LoadMaster kommt mit dem Edge Security Pack auf

ein ähnliches Niveau, entweder klassisch per Formular gegen Active Directory oder modern per SAML und OIDC mit Entra ID, wie in SAML, OIDC und Entra ID: der LoadMaster als moderner Identitätsvermittler beschrieben. Dann greifen auch dort Conditional Access und MFA, nur eben über einen Umweg, den du selbst konfigurierst.

Das Application Gateway hat keine eigene Vorauthentifizierung. Wer sie dort braucht, baut sie in die Anwendung oder schaltet etwas davor. WAP kann gegen ADFS vorauthentifizieren, das ist solide, aber an ADFS gebunden. Open Source kann alles, was du ihm beibringst.

Betriebsaufwand: wer patcht, wer haftet, wer wird angerufen?

Der ehrlichste Vorteil von Cloud-Diensten ist nicht die Technik, sondern dass jemand anderes die Firmware aktualisiert. Beim Application Proxy betreibst du nur die Connector-Server, die sich selbst aktualisieren. Beim Application Gateway betreibst du Konfiguration, Zertifikate und WAF-Regeln, aber kein Betriebssystem. Beim LoadMaster betreibst du alles: HA-Paar, Firmware, Backups, Zertifikate, Monitoring. Bei Open Source zusätzlich das Linux darunter, die Paketquellen und die Frage, wer bei einer kritischen Sicherheitslücke am Wochenende reagiert. Bei den Windows-Bordmitteln den Windows Server, und das kennst du ja.

Dafür kehrt sich das Bild bei der Fehlersuche um. Am LoadMaster hast du L7-Debug, TCP-Dump und Logs auf dem eigenen Gerät. Beim Application Proxy hast du Anmeldeprotokolle, Connector-Ereignisse und ein Supportticket. Wenn der Fehler im Dienst selbst liegt, wartest du. Das ist nicht schlimmer, aber anders, und es fühlt sich um zwei Uhr nachts deutlich schlimmer an.

Cloud-Strategie: wohin will dein Haus eigentlich?

Das letzte Kriterium ist kein technisches, aber oft das entscheidende. Ein Haus, das konsequent nach Microsoft 365 und Azure geht, Exchange Online nutzt und die letzten On-Premises-Server bis 2028 abbauen will, braucht keinen neuen Load Balancer für fünf Jahre. Ein Haus, das aus Gründen der Datenhoheit, des Vergaberechts oder schlicht der Fachverfahren auf absehbare Zeit im eigenen Rechenzentrum bleibt, fährt mit dem LoadMaster gut und ergänzt Entra punktuell. Und eine Verwaltung, die Cloud-Dienste nur für bestimmte Datenkategorien nutzen darf, muss für jede Anwendung prüfen, ob Anmeldeverkehr und Inhalte durch einen Microsoft-Dienst laufen dürfen.

Die große Vergleichstabelle

Kriterium	LoadMaster	Entra App Proxy / Private Access	Azure App Gateway	Windows-Bordmittel	Open Source
On-Prem-Workloads	vollständig, Templates für Exchange, SharePoint, ADFS, RDS	Web-Teile gut (OWA, SharePoint, RD Web), keine Lastverteilung	über VPN/ExpressRoute möglich, stark in Azure	WAP für ADFS, ARR für IIS, NLB veraltet	technisch alles, viel Handarbeit
Kerberos / KCD	ja, mit ESP (KCD und RBCD)	ja, Connector macht KCD	nur Durchreichen (v2, dedizierte Verbindung)	WAP ja, ARR und NLB nein	nur mit Zusatzaufwand
Layer 4 (SMTP, RDP)	ja, mit oder ohne Transparenz	App Proxy nein; Private Access mit Client	TCP/TLS-Proxy in Preview, kein UDP	NLB ja; SMTP-Server in WS 2025 entfernt	ja (HAProxy, NGINX stream)
Vorauthentifizierung	ESP: Formular,	Entra ID mit Conditional	keine eigene	WAP mit ADFS	über Module oder Identity-

	AD, SAML, OIDC, MFA über IdP	Access und MFA			Proxy
Lastverteilung, Health Checks	ja, fein steuerbar	nein (nur Connector-HA)	ja, Health Probes	NLB nur Knotenstatus, ARR einfach	ja
Betriebsaufwand	hoch: HA, Firmware, Backup	gering: Connector-Server	mittel: Konfig, Zertifikate, WAF	mittel bis hoch, mehrere Rollen	hoch: OS, Pakete, Know-how
Eingehende Ports nötig	ja	nein	ja, in Azure	ja	ja
Passt zu Cloud-Strategie	on-prem und hybrid	Cloud-first mit On-Prem-Rest	Azure-first	Bestand, auslaufend	beliebig, je nach Team

Was geht wo durch? Die Protokoll- und Identitätsmatrix

Grün: kann es. Gelb: mit Einschränkung oder Umweg. Rot: geht nicht oder ist nicht vorgesehen

	LoadMaster	App Proxy	Private Acc.	App Gateway	Windows	Open Source
HTTPS-Web-Apps	ja	ja	ja	ja	ja	ja
Lastverteilung Farm	ja	nein	nein	ja	bedingt	ja
Kerberos / KCD	ja	ja	ja	bedingt	bedingt	bedingt
Vorauth. Entra ID	ja	ja	ja	nein	bedingt	bedingt
SMTP, Layer 4	ja	nein	bedingt	bedingt	bedingt	ja
RDP / RD Gateway	ja	bedingt	ja	bedingt	bedingt	bedingt
ohne Client-Agent	ja	ja	nein	ja	ja	ja
ohne Eingangs-Port	nein	ja	ja	bedingt	nein	nein

Skizze: grobe Einordnung, Stand Oktober 2026; Details und Bedingungen im Text

Wo es in der Praxis knallt

Tabellen sind geduldig. Projekte nicht. Die folgenden Stolperstellen haben wir in unterschiedlichen Umgebungen gesehen, meist kurz nach dem Satz „Das ist doch nur eine Konfigurationssache“.

Application Proxy: die interne URL und das Split-DNS

Der Application Proxy kann externe und interne URL gleich benennen, etwa mail.contoso.de. Dann zeigt der Name extern auf den Proxy-Dienst und intern auf den Server oder Virtual Service. Das ist komfortabel und gleichzeitig die Quelle der meisten Überraschungen: Interne Clients, die plötzlich extern auflösen, landen beim Proxy, werden zur Entra-Anmeldung umgeleitet und rufen den Helpdesk an. Mobile Clients, die zwischen WLAN und Mobilfunk wechseln, verlieren ihre Sitzung. Und der Kerberos-SPN muss zum internen Namen passen, nicht zum externen.

AUS DER PRAXIS · Die Farm, die plötzlich ein Server war

Eine Verwaltung veröffentlicht ihr SharePoint-Intranet für das Homeoffice per Application Proxy. Als interne URL wird der Name des ersten Webservers eingetragen, weil der LoadMaster ohnehin abgelöst werden soll. Alles läuft, bis der Server für ein kumulatives Update neu startet. Zwanzig Minuten lang ist das Intranet von außen weg, während der zweite Webserver gelangweilt Däumchen dreht. Lösung: interne URL auf den Virtual Service des LoadMasters, SPN und Delegation auf dessen Namen. Der LoadMaster blieb, nur seine Rolle hat sich verschoben.

Application Gateway: Rückweg durch den Tunnel

Ein Application Gateway in Azure vor Servern im eigenen Rechenzentrum klingt modern und fühlt sich in der Praxis an wie eine Fernbeziehung. Jede Anfrage geht ins Azure-Rechenzentrum, durch den Tunnel zurück und wieder raus. Fällt das VPN, ist die Anwendung weg, obwohl Server und Nutzer im selben Gebäude sitzen. Für Anwendungen, die ohnehin nach Azure wandern, ist das ein sinnvoller Zwischenschritt. Für dauerhaft lokale Workloads ist es eine Abhängigkeit, die du dir gut überlegen solltest.

LoadMaster: der unterschätzte Betrieb

Der LoadMaster scheitert selten an Funktionen, aber gelegentlich an der Pflege. Firmware, die drei Jahre alt ist, ein HA-Partner, der seit dem letzten Update nicht mehr synchronisiert, Zertifikate, die in der Woche ablaufen, in der die zuständige Person im Urlaub ist. Wer den LoadMaster behält, sollte ihn auch so behandeln wie jedes andere Sicherheitssystem am Rand des Netzes, mit Monitoring, Update-Rhythmus und Notfallplan. Welche Edition und welches Sizing zu deinem Bestand passen, beschreibt Editionen, Lizenzierung und Sizing: welcher LoadMaster für welchen Laden.

Open Source: die Konfiguration, die keiner reviewt

Der Reiz von HAProxy und NGINX ist die Textdatei. Sie lässt sich versionieren, reviewen und automatisiert ausrollen. In der Realität vieler mittelständischer IT-Teams wird sie per SSH auf einer VM editiert, und das letzte Review war die Erstellung. Wer das Werkzeug professionell betreibt, mit Git, Pipeline und Tests, hat eine starke Lösung. Wer es betreibt wie früher den TMG, hat ein Problem mit besserem Marketing.

Ehrliche Empfehlungen je Szenario

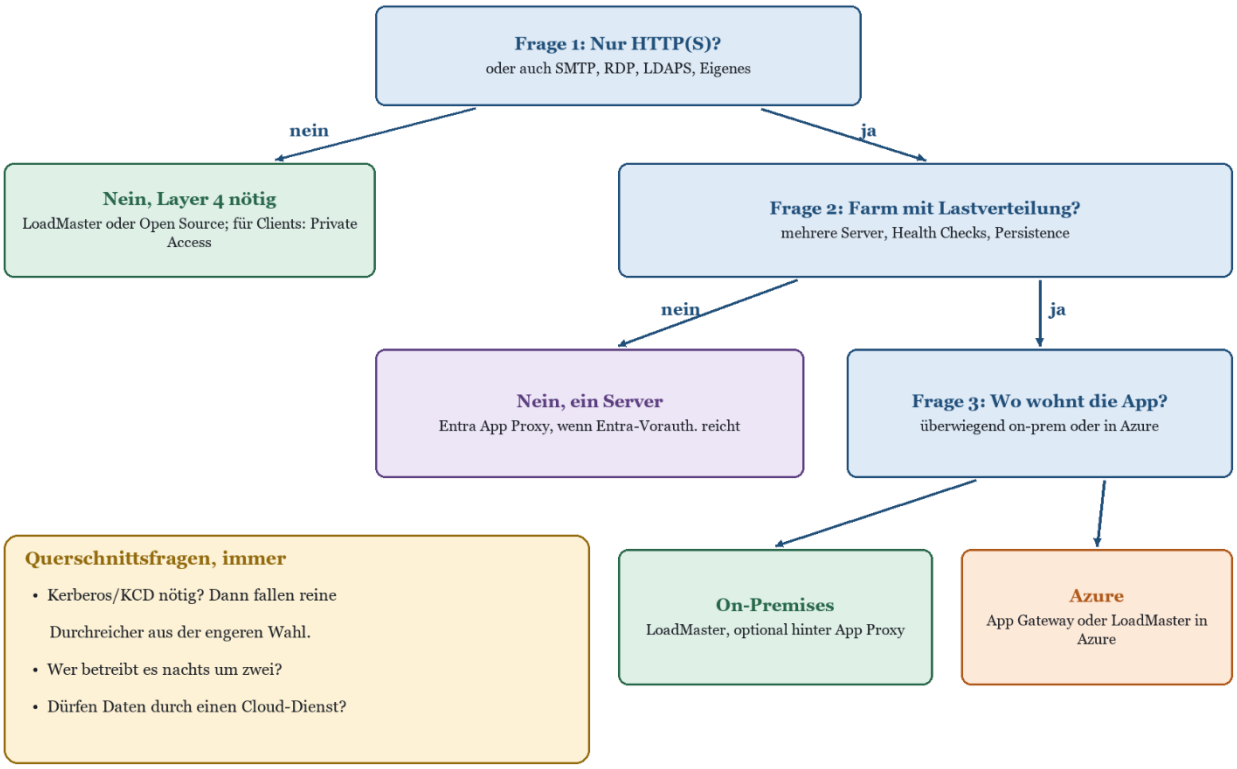
Jetzt wird es konkret. Die folgende Tabelle ist keine Herstellerempfehlung, sondern die Einschätzung, die wir einem Kunden in genau dieser Lage mitgeben würden. Ehrlich heißt auch: Manchmal ist der LoadMaster die zweitbeste Wahl.

Szenario	Empfehlung	Warum	Wann es anders aussieht
Exchange Server on-prem mit mehreren Servern, OWA, Outlook, ActiveSync, SMTP	LoadMaster	Layer 4 und 7, SMTP mit Absender-IP, ESP mit KCD, Templates	Exchange-Abbau in Richtung Online steht innerhalb von zwei Jahren an
Einzelne interne Webanwendung, nur Remote-Zugriff, ein Server	Entra Application Proxy	keine DMZ, MFA und Conditional Access ohne Zusatzaufwand	die Anwendung braucht Lastverteilung oder Nicht-HTTP-Protokolle
SharePoint-Server-Farm, intern und	LoadMaster, extern optional App Proxy	Farm braucht Lastverteilung, extern	kein externer Zugriff: App Proxy entfällt ganz

extern	davor	profitiert von Entra-Vorauth.	
VPN-Ersatz für verwaltete Clients der Belegschaft	Entra Private Access	TCP und UDP, Conditional Access je App, kein VPN-Konzentrator	unverwaltete Geräte oder externe Partner ohne Client
Neue Webanwendung in Azure, mehrere Instanzen	Azure Application Gateway (WAF_v2)	verwaltet, skaliert, nah an der Anwendung	Kerberos zum Backend oder Vorauth. in Gerät nötig
ADFS-Farm mit Extranet-Zugang	LoadMaster vor ADFS und WAP	Farm-Probe, SNI, Lastverteilung; WAP bleibt für ADFS-Spezifika	ADFS wird zugunsten von Entra ID abgebaut
RDS mit RD Gateway und RD Web	LoadMaster, App Proxy für RD Web optional	RD Gateway braucht HTTPS und UDP, Broker braucht Persistence	Umzug nach Azure Virtual Desktop geplant
Hybrid mit Rechenzentrum und Azure	LoadMaster plus App Gateway oder LoadMaster in Azure	jede Seite mit passendem Werkzeug, GSLB möglich	eine Seite wird absehbar aufgegeben
Kleines Team, wenig Netzwerk-Know-how, Cloud-first	App Proxy plus Private Access	geringster Betriebsaufwand	Exchange oder SMTP bleiben dauerhaft on-prem
Starkes Linux- und DevOps-Team, Container	Open-Source-Proxy	versionierte Konfiguration, volle Kontrolle	Kerberos-Delegation für Windows-Apps nötig
Alter Bestand mit NLB, ARR oder TMG-Resten	Migration, Ziel nach Szenario oben	Bordmittel werden nicht mehr weiterentwickelt	nur noch eine Anwendung mit Restlaufzeit

Der Entscheidungsbaum für die Kaffeepause

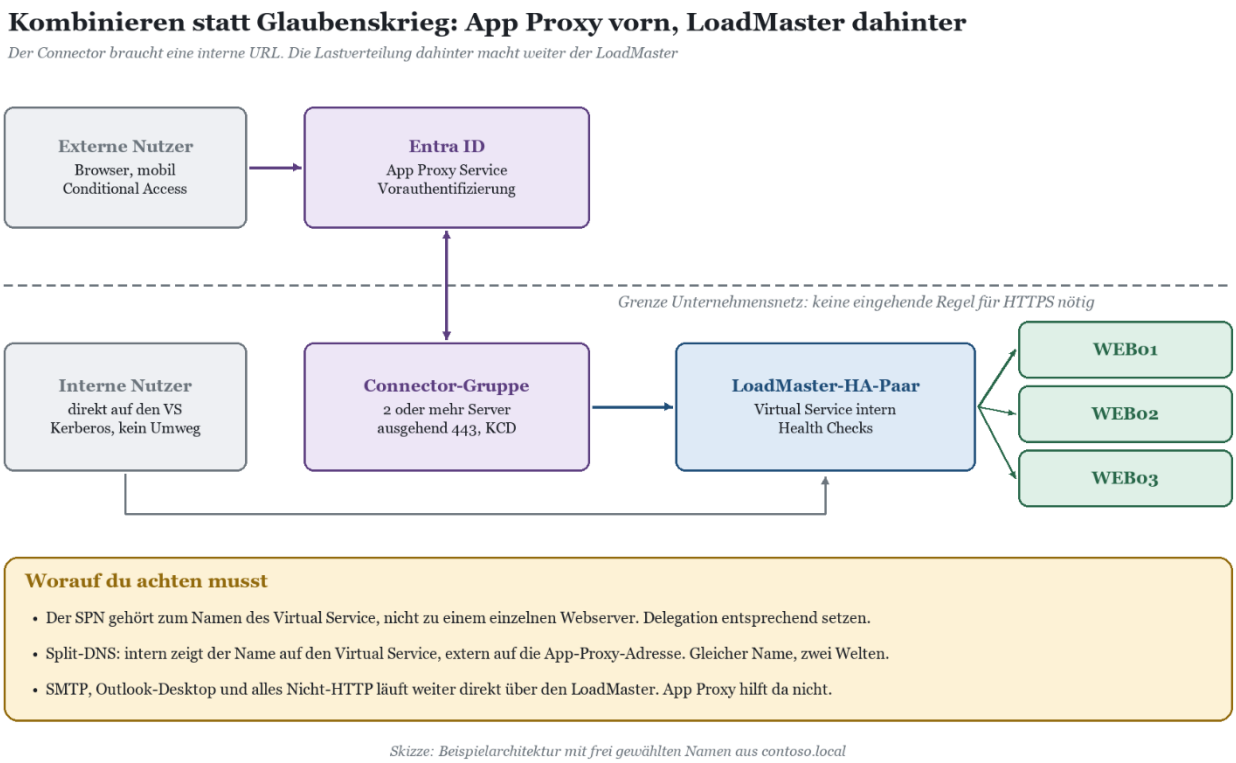
Drei Fragen, in dieser Reihenfolge. Wer mit der Cloud-Strategie anfängt, landet bei der Ausnahme



Skizze: Heuristik, keine Norm; Sonderfälle wie Behördennetze und Air-Gap ausgenommen

Kombinationen statt Glaubenskrieg

Die vielleicht wichtigste Erkenntnis dieser Serie: Die Frage „LoadMaster oder Entra?“ ist meist falsch gestellt. In vielen Umgebungen ist die beste Architektur eine Arbeitsteilung. Der Application Proxy übernimmt den Zugang für Remote-Nutzer zu Webanwendungen, mit Conditional Access und ohne eingehende Ports. Der LoadMaster übernimmt die Lastverteilung dahinter, den internen Zugriff, SMTP, Outlook-Desktop und alles, was kein Browser ist. Das Application Gateway kümmert sich um die Anwendungen, die bereits in Azure leben.



Skizze: Beispielarchitektur mit frei gewählten Namen aus contoso.local

Der Preis der Kombination ist Komplexität an den Nahtstellen: Split-DNS, zwei Orte für Zertifikate, Kerberos-Delegation an zwei Stellen, Logs in zwei Welten. Dafür bekommst du das Beste aus beiden, und du kannst Anwendungen einzeln umziehen, statt alles auf einmal zu schwenken. Für Hybrid-Szenarien mit Azure lohnt zusätzlich ein Blick in LoadMaster in Azure und hybriden Umgebungen.

BERATUNG · Unsicher, welches Szenario deins ist?

Die Tabelle oben passt auf viele Häuser, aber nie ganz auf deins. Genau dafür gibt es die Beratung zum Kemp LoadMaster: Wir gehen mit dir jede veröffentlichte Anwendung durch, prüfen Protokolle, Authentifizierung und Abhängigkeiten und liefern eine Zielarchitektur, die ehrlich sagt, wo der LoadMaster bleibt, wo Entra übernimmt und wo du Altlasten abbauen kannst. Ohne Herstellerbrille, mit Microsoft-Brille.

FAQ

Kann Entra Application Proxy den LoadMaster vollständig ersetzen?

Nur, wenn alle veröffentlichten Dienste reine Webanwendungen auf jeweils einem Server sind und du keinen internen Load Balancer brauchst. Sobald eine Farm, SMTP, Outlook-Desktop oder RDP-Verkehr im Spiel ist, ersetzt der Application Proxy den Zugang, nicht den Balancer.

Was ist der Unterschied zwischen Application Proxy und Private Access?

Der Application Proxy veröffentlicht einzelne Webanwendungen über eine URL und braucht auf dem Endgerät nur einen Browser. Private Access tunnelt beliebige TCP- und UDP-Verbindungen, setzt aber den Global Secure Access Client voraus. Beide nutzen denselben Private Network Connector.

Kann das Azure Application Gateway Kerberos Constrained Delegation?

Nein. Die v2-Generation kann Anfragen mit NTLM oder Kerberos durchreichen, wenn dedizierte Backend-Verbindungen aktiviert sind. Ein Ticket im Namen des Nutzers holt es aber nicht, eine Vorauthentifizierung mit anschließender Delegation ist damit nicht möglich.

Lohnt sich der Web Application Proxy aus Windows Server noch?

Für ADFS ja, dafür ist er gebaut. Als allgemeiner Reverse Proxy für weitere Anwendungen ist er ein Auslaufmodell, das an ADFS gebunden ist. Wer ADFS zugunsten von Entra ID abbaut, baut den WAP gleich mit ab.

Ist ein Open-Source-Reverse-Proxy vor Exchange supportet?

Microsoft schreibt keinen bestimmten Load Balancer vor, sondern beschreibt die Anforderungen an Namespaces und Persistence. Technisch geht es also. Die Frage ist eher, wer bei einem Problem die Ursache findet und ob dein Team die Konfiguration langfristig pflegen kann.

Was mache ich mit SMTP, wenn ich den LoadMaster abschaffe?

Eingehende Mail von außen kommt in vielen Umgebungen ohnehin über Exchange Online Protection oder ein Mail-Gateway. Intern brauchen Relay-Clients wie Scanner und Fachverfahren aber weiterhin einen Weg zu den Exchange-Servern. Ohne Load Balancer bleibt dir DNS-Round-Robin ohne Health Checks oder ein anderer Layer-4-Balancer.

Kann ich LoadMaster und Application Proxy parallel betreiben?

Ja, und das ist oft die beste Lösung. Der Connector spricht intern mit dem Virtual Service des LoadMasters, Kerberos-Delegation und SPN werden auf dessen Namen ausgerichtet. Intern greifen die Nutzer direkt auf den Virtual Service zu.

Fazit: Erst das Protokoll, dann das Logo

Es gibt keine universelle Kemp-Alternative, und es gibt auch keinen universellen Grund, beim LoadMaster zu bleiben. Es gibt Protokolle, Identitäten und Betriebsmodelle. Der Application Proxy ist hervorragend für Remote-Zugriff auf Webanwendungen mit Entra-Vorauthentifizierung, aber kein Load Balancer. Private Access ist ein starker VPN-Ersatz für verwaltete Geräte. Das Application Gateway gehört zu Anwendungen in Azure. Die Windows-Bordmittel sind Bestand mit Ablaufdatum, und Open Source ist ein Baukasten für Teams, die ihn wirklich beherrschen. Der LoadMaster bleibt der Allrounder für alles, was im eigenen Rechenzentrum mehrere Protokolle spricht, Kerberos braucht und verteilt werden will.

Die ehrlichste Empfehlung für die meisten Microsoft-Umgebungen im Mittelstand und in Verwaltungen lautet deshalb: nicht entweder oder, sondern bewusst kombinieren und Anwendung für Anwendung entscheiden. Wenn du dafür eine zweite Meinung brauchst, hilft dir die Beratung zum Kemp LoadMaster. Wenn du die Bausteine selbst beherrschen willst, bevor du entscheidest, ist die Kemp-LoadMaster-Schulung der richtige Ort. Und falls jemand im nächsten Meeting wieder fragt, ob man das Ding nicht einfach abschalten kann: Frag zurück, wer dann die Mail vom Scanner der Poststelle annimmt. Die Stille danach ist meistens die Antwort.

WEITERLESEN · Weiter im Thema

› LoadMaster in Azure und hybriden Umgebungen
› SAML, OIDC und Entra ID: der LoadMaster als moderner Identitätsvermittler
› Migration von Windows NLB, IIS ARR oder TMG-Erbe auf den LoadMaster
› Editionen, Lizenzierung und Sizing: welcher LoadMaster für welchen Laden
› Edge Security Pack: Vorauthentifizierung, SSO-Domänen und der TMG-Ersatz