



AMG

AIR-GAP MAIL GATEWAY



2U اپلاینس رک مونت

مسیر پیام و صف: قاعده‌های یک رله‌ی بی‌ابهام

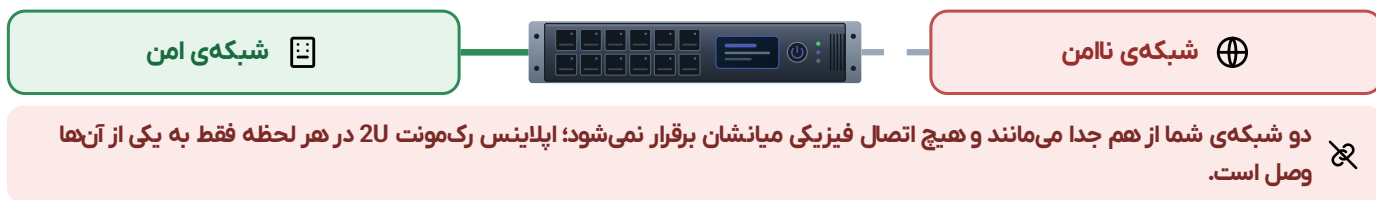
هر پیام از کجا وارد می‌شود، کجا می‌ماند، چه زمانی تحویل می‌شود و اگر نشد چه می‌شود؛ همه با قاعده‌ی روشن و نه با حدس.

<https://www.bardin.tech/fa/bardingate-amg/>

برای: راهبران ایمیل

در این کاتالوگ: نه قاعده‌ی ثابت، چرخه‌ی عمر یک
پیام، ماندگاری، صف، تنظیمات و رفتار هنگام خطا

AMG یک رله‌ی شفاف است و شفافیت یعنی هیچ تصمیمی که به محتوا یا نام‌ها وابسته باشد. جهت، مقصد و سرنوشت پیام فقط از چند قاعده‌ی ساده نتیجه می‌شود که هر کدام را می‌شود آزمایش کرد.



نه قاعده‌ی ثابت

- 1 در هر شبکه دقیقاً یک MTA تعریف می‌شود.
- 2 دو IP متفاوت‌اند. نشانی همتای امن و ناامن نمی‌تواند یکی باشد.
- 3 هر دو مستقیم وصل می‌شوند. NAT، بالانس، پراکسی SMTP و هدر نشانی منبع در نسخه‌ی کنونی نیست.
- 4 فقط همان دو IP می‌توانند پیام بدهند. AMG هرگز رله‌ی باز نیست.
- 5 گیرنده، فرستنده، دامنه، هدر و بدنه جهت را تعیین نمی‌کنند. جهت فقط از IP همتای متصل می‌آید.
- 6 پاکت چندگیرنده یک‌پارچه می‌ماند و کامل به MTA مقابل می‌رسد؛ بر پایه‌ی دامنه‌ی گیرنده تقسیم نمی‌شود.
- 7 محتوا تغییر نمی‌کند. فقط هدر ردیابی استاندارد Received اضافه می‌شود.
- 8 شکست دائمی، DSN استاندارد می‌سازد که به MTA مبدأ برمی‌گردد، نه به سوی مقصد شکست خورده.
- 9 در این نسخه هیچ صندوق نامه، بازرسی محتوا، اسکن، سیاست SPF/DKIM/DMARC یا راستی‌آزمایی گیرنده اجرا نمی‌شود.



جهت = IP، و بس

پیامی با هدرهای دستکاری شده یا گیرنده‌ی نامربوط نمی‌تواند جهتش را عوض کند؛ چون جهت از نشانی TCP مستقیم هم‌تا خوانده می‌شود، و فقط دو نشانی مجاز است.

یک تحویل موفق، گام به گام

۱

اتصال هم‌تا

MTA مبدأ وصل می‌شود و پروفایل امنیتی همان سمت را می‌گذراند: IP مجاز، TLS و در صورت تنظیم mTLS یا AUTH.

۲

پذیرش ماندگار

Postfix کل تراکنش SMTP را در صف پایدار می‌پذیرد و آنگاه پاسخ SMTP 250 می‌دهد.

۳

نگهداری امن

پیام از ری‌استارت و قطع ناگهانی برق بازیافتنی است.

۴

تلاش برای مقصد

Postfix همان پیام را به MTA‌ی مقابل، با IP و درگاه تنظیم شده، می‌فرستد.

۵

تحویل شده

با موفقیت پایین‌دست، وضعیت «تحویل شده» می‌شود و محتوا طبق نگهداری تنظیم شده می‌ماند یا حذف می‌شود.

۶

ثبت و رویداد

فراداده‌ی بدون اطلاعات حساس و ممیزی ثبت و یک رویداد ساخت‌یافته برای SIEM صادر می‌شود.

چرخه‌ی عمر یک پیام

تحویل شده

در صف ماندگار

پذیرفته شده

منقضی: DSN

شکست خورده: DSN

به تعویق افتاده

به تعویق افتادن موقت است و دلیل ثابت بدون اطلاعات حساس و زمان تلاش بعدی دارد؛ شکست و انقضا پایان‌اند و هر دو به فرستنده خبر می‌دهند.

چه می‌شود

وضعیت

پاسخ SMTP 250 فقط پس از آنکه Postfix پیام را طبق پروفایل دوام فایل سیستم ماندگار کرد.

پذیرفته شده

تلاش مجدد محدود و ماندگار. «تلاش اکنون» یک تلاش اضافه می‌خواهد، ولی هرگز مسیر، TLS، پذیرش، ظرفیت و سویچینگ را دور نمی‌زند.

به تعویق افتاده

محتوا طبق نگهداری تنظیم شده حذف می‌شود؛ فراداده‌ی صف می‌ماند.

تحویل شده

DSN استاندارد به MTA مبدأ؛ هشدار پیش از انقضا. هرگونه حذف بی‌صدا ممنوع است.

شکست یا انقضا

دوام

- پیام پذیرفته شده‌ی تحویل نشده از ری‌استارت فرایند یا کانتینر، راه‌اندازی دوباره‌ی میزبان، قطع ناگهانی برق و خرابی یک دیسک فیزیکی جان به در می‌برد؛ ذخیره‌ساز پایدار و RAID دستگاه این را می‌دهد و رمز شده است.
- لحظه‌ی «پذیرفتن» همان لحظه‌ی «ماندگار شدن» است؛ پس هیچ پیامی «تأیید شده ولی گم شده» نیست.



فشار ظرفیت و نگهداری

- **صف تحویل نشده هرگز برای رفع فشار پاک نمی شود.** نخست محتوای تحویل شده‌ی نگه‌داشته شده و قدیمی‌ترین‌ها پاک می‌شود؛ اگر ذخیره‌ی حفاظت شده هنوز کم بود، پذیرش پیام تازه موقتاً با پاسخ موقت 4xx برمی‌گردد و MTA فرستنده بعداً تلاش می‌کند.
- **نگهداری و به‌روزرسانی:** پذیرش تازه با 4xx موقتاً متوقف می‌شود، تراکنش‌های SMTP باز به مرز امن می‌رسند، صف حفظ می‌شود، به‌روزرسانی انجام و سلامت راستی‌آزمایی می‌شود، سپس ادامه یا بازگشت.

چرا «4xx» و نه حذف

پاسخ موقت 4xx به MTA فرستنده می‌گوید پیام را نگه دارد و بعداً بفرستد؛ پس نقطه‌ی گم‌شدن پیام هیچ‌گاه دستگاه نیست. حذف پیام برای باز کردن جا، AMG را به محل از دست رفتن تبدیل می‌کرد.

تنظیمات و پیش‌فرض‌ها

تنظیم	پیش‌فرض	توضیح
عمر صف	۵ روز	در بازه‌ی ایمن قابل تنظیم؛ هشدار پیش از انقضا
اندازه‌ی پیام	50 MiB	قابل تنظیم
نگهداری محتوای تحویل شده	حذف پس از تحویل	می‌توان مدت‌دار و با سقف ذخیره‌سازی فعال کرد
فرا داده‌ی صف	یک سال	قابل تنظیم در بازه‌ی ایمن
ممیزی امنیتی	پنج سال	قابل تنظیم در بازه‌ی ایمن
تلاش مجدد و هم‌زمانی	محافظه‌کارانه	تنظیمات منتخب؛ کلیدهای خام Postfix هرگز نمایش داده نمی‌شود

هیچ سقف مجوزی مصنوعی برای توان عبور، دامنه، گیرنده یا تعداد صف وجود ندارد؛ حد‌ها از سخت‌افزار و ذخیره‌ساز اعتبارسنجی شده می‌آیند.



اعمال تنظیم: گام به گام و برگشت پذیر

تأیید یا بازگشت

بررسی سلامت

بارگذاری

فعال سازی اتمی

postfix check

آماده سازی

خرابی در هر گام، از روی نسخه‌ی فعال پیکربندی، هش فایبل تولید شده و مشاهده‌ی زمان اجرا و صف بازسازی می‌شود. فایبل‌های Postfix مشتق‌اند، نه منبع.

وقتی چیزی خراب می‌شود

وضعیت	رفتار
همتای ناشناس یا IP تکراری در پیکربندی	رد؛ پیام پذیرفته نمی‌شود، پیکربندی فعال نمی‌شود
هویت TLS نامعتبر یا رمز لازم موجود نیست	ارتباط برقرار نمی‌شود؛ بدون سقوط به حالت کم‌امن
جهت مبهم یا پیکربندی مخدوش	رد پیش از اعمال
خرابی Postfix، زمان اجرا یا SIEM	پیام پذیرفته شده هرگز «تحویل شده» گزارش نمی‌شود؛ خرابی SIEM پذیرش SMTP را نمی‌بندد

آنچه آزمایش می‌شود

- هر دو جهت با یک و چند گیرنده؛ اثبات اینکه تغییر گیرنده، دامنه یا هدر جهت را عوض نمی‌کند.
- هیچ پرسش DNS در حین رله؛ TLS الزامی، فرصت طلبانه و خاموش، و mTLS و AUTH اختیاری.
- قطع برق و ری‌استارت پیرامون پاسخ SMTP 250، فعال سازی پیکربندی، تحویل و پاک سازی؛ و فشار دیسک.
- هیچ محتوا، موضوع یا رمزی در لاگ، پایگاه داده، خروجی عیب‌یابی یا SIEM نیست.

چقدر برای شما کار دارد؟

دو نشانی IP، درگاه و (اگر بخواهید) گواهی را وارد می‌کنید و «اعمال» می‌زنید. بقیه، یعنی صف، تلاش مجدد، DSN و رویدادها، خودکار است.

پیام پذیرفته شده یا تحویل می‌شود یا به صورت استاندارد و روشن پایان می‌یابد؛ حالت سومی وجود ندارد.

کاتالوگ‌های دیگر این محصول

کاتالوگ ۴

بهره‌برداری

کاتالوگ ۳

امنیت و ایزولاسیون

کاتالوگ ۱

معرفی محصول



برای مشاوره، درخواست نمایش و اطلاعات تماس:
<https://www.bardin.tech/fa/bardingate-amg/>

مشخصات ممکن است بدون اطلاع قبلی تغییر کند.