BARDIN GATE

نقل آمن للبيانات بين الشبكات المعزولة

AMG

AIR-GAP MAIL GATEWAY

جهاز 2U يُركب في الحامل

الأمن والعزل: مُرحِّل لا يترك شيئًا مفتوحًا

الجهات المسموح بها، وأمن النقل، والأسرار، وتحصين Postfix، وخصوصية المحتوى، على جهاز يبقي الشبكتين منفصلتين ماديًا.

في هذا الكتالوج: أمن النقل، والتوقف التام عند أي فشل، وخصوصية المحتوى، والأحداث لنظام SIEM لديك

لمن: متخصصو الأمن

https://www.bardin.tech/ar/bardingate-amg/

AMG نقطة دخول للبريد، لذلك يطرح أصعب أسئلة الأمن أولًا: من يحق له الاتصال بي؟ والجواب: عنوانا IP لا أكثر. وبقية التصميم يُبقي هذا الجواب صحيحًا طوال عمر الجهاز.

تبقى شبكتاك منفصلتين ولا تتصلان ببعضهما ماديًا أبدًا؛ وجهاز 2U متصل بإحداهما فقط في أي لحظة.

عزل مادي

مفتاح مادي داخل الجهاز يصله بإحدى الشبكتين في كل مرة، ويفصل الأولى تمامًا قبل أن يصل الأخرى. عند كل تشغيل يُفصل كل شيء أولًا، وتُثبت الحالة بتغذية راجعة من المفتاح نفسه.

إقلاع موثوق

UEFI Secure Boot، وإقلاع مقيس في شريحة TPM 2.0، ونظام للقراءة فقط يُتحقق منه كتلةً كتلة.

طابور مشفّر

يقع الطابور الدائم على وحدة البيانات المشفّرة في الجهاز (LUKS2 وAES-256-XTS)، ويتحمّل RAID تعطل قرص واحد.

Postfix محصّن ومستقل

Podman دون صلاحيات root، وجذر للقراءة فقط، وAppArmor، وseccomp، دون امتيازات نظام إضافية ومع سقوف للموارد؛ عملية منفصلة عن بقية برمجيات الجهاز.

التشفير

لا تعمل لوحة التحكم إلا بـ TLS 1.3؛ والتواقيع ECDSA على P-256 مع SHA-256؛ وكلمات المرور بـ Argon2id. ولا تُستخدم MD5 وSHA-1 و3DES وRC4 أبدًا.

الجهات المسموح بها وأمن النقل

الضابط	كيف يعمل
قائمة عناوين IP المسموح بها	لا يُقبل إلا الاتصال المباشر من العنوانين المضبوطين. وكل منهما عنوان IPv4 أو IPv6 مكتوب بالأرقام؛ ويُرفض اسم المضيف في حقل العنوان.
لا DNS ولا MX	تذهب الاتصالات دائمًا مباشرة إلى عنوان IP ذاك. واسم المضيف ليس إلا هوية الجهة الأخرى والاسم المتوقع في شهادتها.
نمط TLS	REQUIRED هو الافتراضي ويتحقق من شهادة الجهة الأخرى دون استثناء. أما OPPORTUNISTIC وOFF فيتطلبان تحذيرًا صريحًا وتطبيقًا مسجَّلًا في التدقيق.
mTLS وSMTP AUTH	اختياريان ويُضبطان لكل جهة؛ والشهادات والمفاتيح وكلمات المرور محفوظة فقط كمراجع إلى مخزن الأسرار.
الاتجاه	من عنوان IP للجهة الأخرى فقط؛ وتعديل الرسالة لا يستطيع تغييره.

> **الأسرار لا تعيش في أي مكان آخر**
>
> لا تدخل المفاتيح الخاصة وكلمات المرور أبدًا ملف الإعدادات أو السجلات أو قاعدة البيانات أو التشخيص أو SIEM. فالملف لا يحمل إلا مواضعها في مخزن الأسرار.

أي فشل يوقف التدفق

- تُرفض كلها: الجهة غير المعروفة، والعنوان نفسه في الجهتين، وهوية TLS غير الصالحة، والسرّ المطلوب المفقود، والاتجاه الملتبس، والإعدادات المشوّهة.
- تُفحص الإعدادات أولًا (`postfix check`)، ولا تُفعَّل إلا إذا كانت سليمة، وإلا يُتراجع عنها.

خصوصية المحتوى

- لا تظهر نصوص الرسائل ومرفقاتها وموضوعاتها أبدًا في السجلات أو المقاييس أو البيانات الوصفية في قاعدة البيانات أو أحداث SIEM.
- في SIEM تكون عناوين المرسل والمستلم افتراضيًا اسمًا مستعارًا ثابتًا بمفتاح مع عرض مُقنَّع. والعرض الكامل والإغفال بديلان صريحان، والعرض الكامل يحمل تحذيرًا وسجل تدقيق.
- الاسم المستعار هو HMAC بمفتاح مخصص لهذا الغرض في مخزن الأسرار؛ ويُمنع التجزئة البسيطة دون ملح، وتدوير المفتاح يبدأ جيلًا جديدًا.

الوضع الأمني في لمحة

الجهات المسموح بها	اثنتان بالضبط، بعنوانين ثابتين ومختلفين	**TLS**	مطلوب افتراضيًا، مع التحقق من الشهادة
مُرحِّل مفتوح	أبدًا	**DNS وMX**	لا استعلامات أثناء الترحيل
الأسرار	مراجع فقط في الإعدادات	**محتوى الرسالة**	دون تغيير، وليس في أي سجل أو حدث
تشغيل Postfix	دون root، وللقراءة فقط، مع AppArmor وseccomp	**وصل الشبكتين**	أبدًا؛ لا اتصال مادي بينهما

الهوية والوصول

- **الجهاز هو السلطة الوحيدة.** المتصفح والملفات المستوردة وكل ما عداها تأتي بادعاءات؛ ولا يستطيع أي منها منح سلطة.
- **الافتراضي هو المنع.** تحمل الأدوار نطاقًا صريحًا، والصلاحية غير المكتوبة رفض.
- **كلمة المرور، ثم كلمة المرور مرة أخرى.** الإجراءات عالية الخطورة (الأدوار، وسياسة الأمن، واستيراد الترخيص والتحديثات، وتصحيح الوقت، والاسترداد، واستيراد الإعدادات) تطلبها مرة أخرى.
- **لا باب خلفي.** لا كلمة مرور رئيسية للمورّد، ولا حساب مخفي، ولا استعادة عبر البريد، ولا تجاوز غير مسجَّل. واسترداد آخر مسؤول إجراء مادي أمام الوحدة.
- **لا يصل SSH إلا إلى حساب دعم مقيَّد.** يعيد التقارير والسجلات والحالة فقط؛ ولا دخول لـ root عبر SSH، ولا سطر أوامر للعمل اليومي ولا وصول مباشر إلى قاعدة البيانات.

أحداث لنظام SIEM لديك

الحدث	متى يصدر
MAIL_ACCEPTED	قُبلت رسالة وحُفظت حفظًا دائمًا
MAIL_DELIVERED	قبلها MTA المقابل
MAIL_DEFERRED	فشل التسليم مؤقتًا، مع سبب ثابت وموعد المحاولة التالية
MAIL_FAILED	فشل دائم أو انتهاء مدة؛ وصدر إشعار DSN

الإرسال إلى SIEM في اتجاه واحد، وعطل SIEM لا يوقف SMTP أبدًا. وتُصدَّر أيضًا جميع أحداث الأمن والتدقيق افتراضيًا.

أمن دون عمل إضافي

كل هذه الضوابط هي إعدادات الجهاز الافتراضية وتعمل كما يُسلَّم؛ لا تُدخل إلا عنوانَي الجهتين وشهاداتك.

مُرحِّل لا يتحدث إلا إلى عنوانين، بشهادات صالحة فقط، ولا يحكم على المحتوى أبدًا.

كتالوجات أخرى لهذا المنتج

كتالوج ١ — نظرة عامة على المنتج

كتالوج ٢ — تدفق البريد والطابور

كتالوج ٤ — التشغيل والتكامل

للاستشارة وطلب عرض توضيحي ومعلومات الاتصال:
https://www.bardin.tech/ar/bardingate-amg/

قد تتغير المواصفات دون إشعار مسبق.