BARDIN GATE

نقل آمن للبيانات بين الشبكات المعزولة

AMG

AIR-GAP MAIL GATEWAY

جهاز 2U يُركب في الحامل

التشغيل والتكامل: من الحامل إلى المراقبة

لوحة التحكم، والإعدادات في ملف واحد، والتشغيل الأولي، والتحديثات، والاسترداد، وما تحتاج مؤسستك إلى توفيره، لفريق لا يريد الدخول إلى الجهاز.

في هذا الكتالوج: لوحة التحكم، والتشغيل الأولي، والتحديث والتراجع، والاسترداد، والتركيب، وقائمة التحقق قبل بدء التشغيل الفعلي

لمن: مسؤولو البريد وتقنية المعلومات

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

صُمم AMG لفريق لا يريد الدخول إلى الجهاز. كل ما يلزم يتم في لوحة التحكم في المتصفح: الإعدادات، ورؤية الطابور، وسبب التأجيل، وإجراء آمن واحد هو «أعد المحاولة الآن».

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

لوحة تحكم AMG

المجال	ما تراه وتفعله
لوحة المعلومات	ما هو مؤجل أو متوقف ولماذا؛ وما رُحِّل خلال فترة تختارها؛ وكيف يقارن الاتجاهان؛ وهل الجهتان والجهاز قادرة على العمل أصلًا. وتظهر هنا التحذيرات التي تحتاج إلى شخص.
الإعدادات	الجهة الآمنة وغير الآمنة، وأمن SMTP، والطابور، وإعادة المحاولة، والحجم، والاحتفاظ؛ كلٌّ منها إعداد محدد، لا مفتاح خام أبدًا.
مسار الإعدادات	مسودة، وتحقق، ومقارنة، وتطبيق صريح؛ وإذا رُفضت لا يتغير شيء.
الطابور	في كل صف: الحالة، والعمر، والاتجاه، والحجم، وسبب فشل ثابت منقّح. و«أعد المحاولة الآن» بتأكيد وتدقيق.
السلامة	تحذيرات السعة والتأجيل وانتهاء المدة، وسلامة الجهتين.

لا بيانات تجريبية

كل رقم في كل صفحة يُقرأ من الجهاز. ولا يوجد في هذا الإصدار عن قصد حذف أو حجز أو إفراج، ولا ملفات طابور خام، ولا تحرير حر لـ `main.cf` ؛ لا يوجد إلا «أعد المحاولة الآن».

تشغيل أولي موجَّه

١ ركّبه
ركّب جهاز 2U ووصّل الكهرباء والشبكة الآمنة وغير الآمنة وشبكة الإدارة.

٢ افتح لوحة التحكم
افتح لوحة التحكم في المتصفح. يثبت رمزٌ على شاشة الجهاز نفسه أنك أمام الوحدة.

٣ إعداد موجَّه
تجري الخطوات بالترتيب وتختبر كل خطوة نفسها: العتاد، والوقت، وعناوين الشبكة، والمسؤول الأول.

٤ الاستلام
خذ حزمة أدلة التشغيل الأولي الموقّعة؛ الجهاز جاهز للعمل.

بعد ذلك تُدخل الجهتين وTLS، وmTLS، وAUTH عند الحاجة، في لوحة التحكم وتضغط «تطبيق»؛ فيختبر الجهاز الإعدادات قبل تفعيلها.

الإعدادات ملف واحد

كل إعدادات المسؤول في ملف إعدادات واحد ذي إصدارات يُفعَّل تفعيلًا ذريًا. وملفات Postfix مشتقة منه، لا العكس، فاستبدال الجهاز يعني استيراد هذا الملف.

التحديث والتراجع

- **الحزم موقّعة وتعمل دون اتصال.** تُرفض الحزمة التي لا تحمل توقيعًا صالحًا أو تكون أقدم من تسلسل الإصدارات المسجَّل (منع الرجوع)؛ ويُمنع الرجوع العادي إلى إصدار أقدم.
- **قسمان للنظام.** يُكتب التحديث في القسم الآخر، ويُقلع منه مرة واحدة تجريبيًا، ولا يُعتمد إلا بعد نجاح فحوص السلامة؛ وإلا تعود الوحدة وحدها إلى الإصدار السابق.
- **البيانات منفصلة عن البرمجيات.** تصل تواقيع ClamAV وقواعد YARA ومخططات التحقق في حزمة بيانات فقط لا تغيّر البرمجيات أبدًا.

أثناء التحديث يتوقف القبول الجديد مؤقتًا بـ 4xx، وتنتهي المعاملات المفتوحة، ولا يُمس الطابور.

الإصلاح الذاتي

يفترض الجهاز أن أحدًا لا يستطيع الوصول إليه، فيصلح نفسه. لا محطة عمل ولا شاشة ولا SSH للعمل اليومي، ولا يجوز أن يتطلب أي تصميم للاسترداد الوصول إلى وحدة معطلة.

المستوى	ما تفعله	ما يبقى
إعادة ضبط مرنة	تعيد البرمجيات إلى آخر حالة سليمة معروفة؛ وهي الآلية نفسها التي يستخدمها رجوع التحديث.	الهوية والإعدادات والسجلات والتدقيق
إعادة ضبط كاملة	تعيد الوحدة إلى حالتها قبل التشغيل الأولي؛ فهي تمحو ولا تستعيد.	لا شيء؛ صدّر التدقيق أولًا

الاستبدال والاسترداد

الموقف	الطريق الصحيح
تعطل قرص واحد	استبدله وفق دليل التشغيل؛ تبقى وحدة التخزين سليمة أو قابلة للاسترداد.
مزوّد الطاقة أو المروحة	إجراء المورّد في وضع الصيانة، ثم إعادة التحقق من الجاهزية.
اللوحة الأم أو شريحة الأمان	يطلب الجهاز سرّ الاسترداد مرة واحدة، أمام الوحدة؛ ويحتفظ بهويته وإعداداته وترخيصه.
فقدان الجهاز بالكامل	جهاز بديل: تشغيل أولي جديد، واستيراد الإعدادات، وإدخال الأسرار من جديد، وإعادة إنشاء نقاط الاتصال. ولا تُستنسخ الهوية القديمة أبدًا.

الجهاز والتركيب

البند	ما يعنيه
الجهاز	جهاز بارتفاع 2U يُركب في الحامل، جاهز كما يُسلَّم. لا خادم ولا نظام تشغيل ولا برمجيات إضافية لاختيارها أو تثبيتها.
المساحة والكهرباء	مساحة 2U في حامل قياسي، وكهرباء.
الشبكة	اتصال بالشبكة الآمنة وغير الآمنة وشبكة الإدارة. ولا تتصل الأوليان ببعضهما أبدًا.
العمل اليومي	متصفح فقط. لوحة التحكم بأربع عشرة لغة، منها العربية.
الإنترنت	لا حاجة إليه؛ الترخيص والتحديثات والتواقيع تصل دون اتصال وموقّعة.

الاندماج في مؤسستك

الإنترنت	لا حاجة إليه؛ الترخيص والتحديثات والتواقيع كلها دون اتصال	**خوادم MTA لديك**	SMTP مع TLS مطلوب؛ وmTLS وAUTH اختياريان
نظام SIEM لديك	Syslog عبر TLS بصيغة RFC 5424 JSON أو CEF	**لغات لوحة التحكم**	أربع عشرة لغة، منها الفارسية والإنجليزية والعربية
السعة	لا سقف في الترخيص؛ الحدود يحددها العتاد والتخزين		

قائمة التحقق قبل بدء التشغيل الفعلي

1. رُكّب جهاز 2U في الحامل ووُصل بالشبكة الآمنة وغير الآمنة وشبكة الإدارة.
2. خادما بريد بعنوانَي IP ثابتين ومختلفين وشهادتَي TLS الخاصتين بهما جاهزان؛ وإن أردت mTLS أو AUTH فالأسرار في متناولك.
3. بلغ التشغيل الأولي حالة الجاهزية وصُدّرت حزمة الأدلة الموقّعة.
4. أُدخلت الجهتان وطُبّقتا في لوحة التحكم؛ وعبرت رسالة اختبار في الاتجاهين وظهرت في الطابور.
5. ضُبطت وجهة SIEM وتصل الأحداث؛ وتنبيهات التأجيل واقتراب انتهاء المدة موجودة في نظام المراقبة لديك.
6. أُخذ تصدير للإعدادات وحُفظ في عهدة شخصين؛ كرّره بعد كل تغيير ومرة في الأسبوع على الأقل.

كل رقم في لوحة التحكم يُقرأ من الجهاز؛ ولا توجد فيها بيانات تجريبية.

كتالوجات أخرى لهذا المنتج

كتالوج ١	كتالوج ٢	كتالوج ٣
نظرة عامة على المنتج	تدفق البريد والطابور	الأمن والعزل

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

قد تتغير المواصفات دون إشعار مسبق.