

جدار الحماية من الجيل التالي

جدار حماية من الجيل التالي لشبكة أعمالك.

يجمع برنامج AZTCOFW بين التحكم في حركة الشبكة والاتصال الآمن ومتابعة حالة التشغيل. اختر نشره على جهاز AZTCO، أو آلة افتراضية، أو عتاد متوافق تملكه.

منصة واحدة. ثلاثة خيارات للنشر.

اختر جهاز AZTCO أو آلة افتراضية أو عتاداً متوافقاً تملكه. أضف وحدات الحماية والدعم التي تلائم احتياجات شبكتك.

03

تابع ما يجري في الشبكة

راجع حركة البيانات ومؤشرات الأجهزة وحالة النظام لدعم قرارات التشغيل.

02

حافظ على اتصال فرقك

اربط الفروع والمستخدمين عن بُعد، وعزز استمرارية الاتصال باستخدام عدة مزودي إنترنت وميزة AZTCO HA.

01

تحكم في الوصول

حدّد الاتصالات المسموح بها، وافصل الشبكات والخدمات، واستفد من فحص التهديدات.

الشركات والفروع / قطاع التعليم / مزودو الاستضافة

جهاز AZTCO / آلة افتراضية لجدار الحماية / عتاد متوافق يملكه العميل

تحكم دقيق عند حدود شبكتك.

تصفية الاتصالات والعنونة والتوجيه وVPN واستمرارية الخدمة، وفق الإصدار وتصميم الشبكة.

02

إدارة القواعد والسياسات

أنشئ مجموعات قابلة لإعادة الاستخدام للأجهزة والشبكات والمنافذ وعناوين URL. رتب القواعد وجدول أوقات تفعيلها، وحدد حدود الاتصالات لكل قاعدة وفقاً لما يدعمه الإصدار.

01

تصفية الاتصالات مع تتبع الحالة

طبّق قواعد تصفية على اتصالات IPv4 و IPv6، مع خيارات السماح أو الحظر أو الرفض. حدّد الواجهات والشبكات والمنافذ والبروتوكولات، وسجّل القواعد وراجع جدول حالات الاتصال.

04

شبكات IPv6

استخدم واجهات مزدوجة المكس، وعناوين IPv6 ثابتة أو DHCPv6 على WAN، وتفويض البادئات وتتبع بادئة LAN، وإعلانات الموجه و SLAAC وخدمات DHCPv6. تُضبط قواعد IPv6 بصورة مستقلة عن IPv4.

03

NAT والخدمات المنشورة

اربط عنواناً عاماً بمضيف داخلي باستخدام NAT 1:1، أو انشر خدمة عبر تحويل المنافذ. اختر NAT المصدر التلقائي أو الهجين أو اليدوي، واستخدم العناوين الافتراضية و Split DNS، مع قصر الوصول على ما تسمح به القواعد.

06

اتصالات متعددة بالإنترنت

راقب البوابات، واضبط التحويل إلى اتصال احتياطي أو وزّع الاتصالات الجديدة بين بوابات المستوى نفسه. يُحدّد المسار لكل اتصال، وقد يلزم إنشاء الجلسات القائمة من جديد عند تغييره.

05

تقسيم الشبكة والتوجيه

أنشئ واجهات VLAN وفق 802.1Q وافصل LAN عن DMZ، ثم أضف المسارات الثابتة والتوجيه بحسب البوابة. حدّد مراحة الاتصالات بين القطاعات وراجع إعدادات المحولات الافتراضية والمادية معاً.

تحكم دقيق عند حدود شبكتك.

تصفية الاتصالات والعنونة والتوجيه وVPN واستمرارية الخدمة، وفق الإصدار وتصميم الشبكة.

08

AZTCO HA

وَمَرَّ التحويل الاحتياطي بين جهازين متوافقين مع عناوين افتراضية مشتركة ومزامنة لحالات الاتصالات والإعدادات. خصص شبكة للمزامنة وتحقق من توافق الخدمات مع الموزع.

07

اتصال VPN

أنشئ اتصالات IPsec و OpenVPN بين المواقع أو للمستخدمين عن بُعد، واستخدم WireGuard عبر الحزمة المتوافقة. يعتمد دعم الشهادات والمستخدمين المحليين و RADIUS أو LDAP على تصميم VPN والإصدار المختار.

10

خدمات الشبكة

استخدم DHCPv4 و DHCPv6 و ترحيل DHCP حيث يتوفر، ومحلل DNS أو معيد توجيهه وتجاوزات DNS و DNS الديناميكي و NTP. يمكن تفعيل التحقق من DNSSEC في المحلل.

09

إدارة حركة الشبكة

اضبط أولوية الحركة وحدود سرعات الرفع والتنزيل، مع توزيع السعة بين الأجهزة عند تهيئته. نعتد الخيارات المتاحة على ملفات النطاق الترددي وتعريفات الواجهات ومسارات الحزم.

12

إدارة الإعدادات واستعادتها

أدر جدار الحماية من واجهة الويب، واحفظ نسخة من الإعدادات أو استعدها، وراجع سجل النسخ والإصدارات. تتوفر أدوات لإدارة الخدمات والمهام المجدولة والتشخيص؛ وقد تتطلب استعادة إعدادات بعض الإضافات تثبيت حزم متوافقة.

11

إدارة المستخدمين وشبكات الضيوف

أدر حسابات المستخدمين وصلاحيات الإدارة، واستخدم RADIUS أو LDAP للمصادقة حيثما كان ذلك مدعوماً. أنشئ بوابات دخول للضيوف وقسائم اتصال، وأضف هوية AZTCO إلى صفحاتها.

اختر الوحدات وخيارات الخدمة المناسبة لشبكتك مع الموزع. يعتمد التوفر على الترخيص وتكوين الجهاز وإصدار البرنامج المختار.

تعرف إلى التطبيقات، وحدد طريقة التعامل معها.

راجع التطبيقات التي يمكن التعرف إليها، ونطاق القواعد وآلية تطبيقها قبل تفعيل الحظر أو تحديد السرعة.

02

إجراءات التحكم

ابدأ بالمراقبة قبل تطبيق السياسة. اسمح بالتدفقات المدعومة أو امنعها أو حدّد سرعات رفعها وتنزيلها كل على حدة. تُقيّم القواعد المرتبطة بقاعدة جدار حماية وفق ترتيب السياسات.

04

التكامل مع سياسات جدار الحماية

يبقى ترتيب قواعد جدار الحماية هو المرجع. يمكن استخدام وجهات التطبيقات المعروفة ضمن قواعد وبوابات مرتبة؛ ولا يعيد النظام توجيه التطبيق بعد اكتشافه المتأخر.

06

تحديث بيانات التعرف

استخدم التحديث اليومي أو الجداول اليومية والأسبوعية بتوقيت UTC للحصول على بيانات إقليمية موثقة. تظهر حالة التحديث وتبقى مجموعة البيانات السابقة محفوظة؛ وتكون الجداول معطلة افتراضياً.

08

حدود النشر

يتطلب التصنيف حركة يمكن للجدار الناري رؤيتها وقد يبدأ بعد الحزم الأولى. اختر تطبيقات العمل والحركة المشفرة وVPN وتشكيل الحركة قبل فرض القيود. ربط السياسة بقواعد جدار الحماية يدعم تدفقات IPv4.

01

التحكم بالتطبيقات وتصنيفاتها

راقب استخدام التطبيقات المدعومة أو أنشئ قواعد تحدد الوصول إليها. تختلف دقة التعرف بحسب التشفير وتغيّرات التطبيق ونوع الحركة التي يمكن لجدار الحماية فحصها.

03

تحديد نطاق القواعد

اربط قواعد التطبيقات بقواعد IPv4 محددة، وطبقها على أجهزة أو شبكات أو أسماء مضيفين أو مجموعات عناوين. تحقق من مسار الحركة المطابق قبل تفعيل الحظر.

05

التعرف على التطبيقات

تدعم قوائم أسماء النطاقات والمضيفين المُدارة التعرف على التطبيقات المتوافقة. وقد تتأثر الدقة عند مشاركة عناوين IP أو تغيّر شبكات CDN أو تشفير أسماء المضيفين أو استخدام الأنفاق.

07

الرؤية التشغيلية

اعرض التطبيقات المرصودة والحركة والبايتات والحزم وقرارات السياسات. تتكامل البيانات مع Client Riskg Traffic Center المتوافقين؛ لكنها عدادات ومشاهدات محدودة وليست أرشيفاً كاملاً للحركة.

من دون فحص HTTPS، يطبق WebGuard سياسة الوجهات استناداً إلى اسم المضيف المطلوب. يتطلب فحص مكافحة الفيروسات حركة HTTPS مفحوصة وشهادة عميل موثوقة.

حماية شبكتك، مع تحكم يناسب طريقة عملها.

تعرف إلى وظائف كل وحدة، وكيفية دمجها في الشبكة، وما يلزم لنشرها.

02

حجب نطاقات DNS

استخدم قوائم موثوقة نطاقات DNS وعناوين IP لتقييد الوصول إلى الوجهات غير المرغوبة أو عالية المخاطر، مع إمكانية إضافة استثناءات. تسري القواعد على الاستعلامات التي تمر عبر محلل DNS المحدد؛ أما المسارات البديلة أو المشفرة فتحتاج إلى ضوابط شبكية.

04

مكافحة الفيروسات

افحص تنزيلات HTTPS المؤهلة عبر فحص WebGuard واحظر البرمجيات الخبيثة المكتشفة. يتطلب ذلك فحص HTTPS وثقة جهاز العميل بشهادة الفحص.

06

مركز متابعة حركة الشبكة (Traffic Center)

راقب استخدام الرفع والتنزيل للتطبيقات والعملاء، والنشاط المباشر وإجماليات الواجهات وتقارير يومية محفوظة. صَدْر CSV أو فُغْل رسائل البريد اختياريًا. نطاق الجمع والاحتفاظ ظاهر؛ ولا تجمع إجمالي الواجهة وإجمالي العميل معًا.

08

مراقبة مشاركة الاتصال (Hotspot Guard)

راقب واجهات العملاء المحددة لرصد مؤشرات مشاركة الاتصال. راجع التفاصيل والاستثناءات، ثم اختر إرسال تنبيه أو تقييد المصدر. هذه المؤشرات تستدعي التحقق ولا تثبت حدوث المشاركة.

01

نظام AZTCO لكشف التسلل ومنعه (IDS/IPS)

افحص حركة الشبكة بحثاً عن أنماط التهديد المعروفة. خصص القواعد والاستثناءات لكل واجهة. راجع التنبيهات والأجهزة المحظورة. يعتمد توفر التوقييع وتحديثها وإجراءات المنع على الترخيص والإعداد.

03

WebGuard – ضبط الوصول إلى الويب

استخدم وكيلًا صريحاً لاتصالات HTTP وHTTPS، مع قواعد مرتبة حسب النطاق وتحديد الأجهزة وأوقات العمل. يمكن تخزين استجابات HTTP المؤهلة مؤقتاً، كما يمكن تفعيل فحص HTTPS اختياريًا بعد تثبيت شهادة الثقة على أجهزة العملاء.

05

تقييم مخاطر الأجهزة (Client Risk)

اجمع مؤشرات IPS وDNS وجدار الحماية والتطبيقات المدعومة في سجل واحد. راجع درجة المخاطر (من 0 إلى 100) والأدلة وملاحظات التحقيق والمسؤول عن المتابعة. يمكن ضبط التنبيه أو الحظر أو العزل بصلاحيات محددة. الدرجة مؤشر للمراجعة وليست دليلاً قاطعاً على اختراق الجهاز.

07

مجموعات FreeRADIUS وبوابة دخول الضيوف

نظم المستخدمين والأجهزة المسجلة في مجموعات، واستخدم مجموعات عناوين IPv4 ضمن قواعد الوصول. أنشئ لكل منطقة صفحة دخول للضيوف بهوية علامتك التجارية، مع أدوات لتحديثها ومعاينتها ونشرها.

09

إنهاء TLS وموازنة الخوادم (SSL Offloading)

انشر الخدمات عبر وكيل عكسي ينهي اتصالات TLS، مع إعداد الخوادم الأمامية والخلفية وفحوص الحالة وتوزيع الحركة وإحصاءات التشغيل عبر تكامل HAProxy المتوافق. هذه الوظيفة لا تحل محل جدار حماية تطبيقات الويب.

أدرج جدار الحماية ضمن منظومة المراقبة لديك.

استخدم أدوات التشخيص المدمجة، وأرسل السجلات إلى مجمّعك أو منصة SIEM ونظام إدارة الشبكة.

02

أحداث أمنية منظمة

أرسل أحداث Client Risk عبر syslog باستخدام UDP أو TCP أو TLS. يستخدم TCP و TLS تأطير octet-counted، ويتحقق TLS من شهادة المستقبل. اختر أحداث الأمن والسياسات والإدارة والحالة.

04

إشعارات SNMP

يرسل Client Risk إشعارات SNMPv2c تتضمن معرّفات الأحداث وعنوان العميل والإجراء ودرجة المخاطر. اضبط المستقبل واسم المجتمع وقاعدة OID المخصصة. لا تضيف الإشعارات معرّفات استعلام جديدة؛ ولا يدعم هذا المكوّن SNMPv3 أو informs.

06

أدوات استكشاف الأعطال

استخدم التقاط الحزم و ping و traceroute و استعلام DNS وفحص المسارات والحالات وتكامل Speedtest المتوافق لعزل الأعطال. راع حمل الإنتاج عند تنفيذ الاختبارات.

08

التقارير والتنبيهات

راجع الأدلة والسجل في Client Risk وتقارير CSV والطباعة وتقارير Traffic Center اليومية. يمكن إرسال البريد عبر SMTP عند تفعيله؛ ويعتمد نطاق التقرير على البيانات والاحتفاظ المحددين.

01

سجلات النظام وجدار الحماية

راجع أحداث جدار الحماية والنظام والمصادقة وVPN و DNS و DHCP والبوابات. وّجه السجلات إلى مجمّع syslog خارجي للاحتفاظ بها خارج الجهاز؛ ويستخدم التوجيه الأصلي UDP.

03

استعلام SNMP

وفّر معلومات النظام والواجهات المدعومة لنظام إدارة الشبكة الخارجي عبر SNMP الأصلي. قيّد الاستعلامات بمضيقي المراقبة المصرّح لهم وتحقق من ملفات MIB للإصدار المختار.

05

حركة المرور والبوابات

استخدم الرسوم والعدادات وحالة زمن الاستجابة وفقد الحزم للبوابات وحالات جدار الحماية والمسارات وVPN للتمييز بين أعطال الوصلة والسياسة والخدمة.

07

التشخيص بمساعدة الذكاء الاصطناعي (AI) (Diagnostics)

نفّذ فحوصاً إرشادية محلية تربط الحالة والإعدادات وأدلة الأجهزة أثناء التشخيص. تعرض النتائج للإشارات المرصودة، ويراجعها المشغل قبل تغيير السياسة.

09

التكامل مع منصات المراقبة

أرسل السجلات والأحداث المدعومة إلى SIEM أو منصة مراقبة. أعدّ التحليل والطوابع الزمنية والاحتفاظ ومنع التكرار عند المستقبل. لا يضمن UDP والإشعارات وصولاً مؤكداً، كما أن الطوابع محدودة.

بنيتك التحتية، مع جدار حماية افتراضي مخصص.

شغل AZTCOFW على آلة افتراضية مخصصة. تُحسب تكلفة الترخيص وفق موارد المعالج وعدد واجهات الشبكة المطلوبة.

جدار حماية افتراضي

02

ترخيص بحسب الموارد

يُحتسب سعر ترخيص الآلة الافتراضية بحسب موارد CPU المطلوبة (vCPU أو الأنوية) وعدد واجهات الشبكة. يحدد العرض الموارد المسموح بها والمدة والخيارات.

01

النشر على آلة افتراضية

شغل نسخة مخصصة من جدار الحماية على منصة افتراضية متوافقة. تحقق من دعم بطاقات الشبكة الافتراضية vSwitch و VLAN، ومن تخطيط التخزين وموارد المعالج وصورة البرنامج.

04

خيارات التكرار

اسأل الموزع عن تصميم آلة ثانية أو AZTCO HA حيث يتوفر. راع نطاقات أعطال المحاكى والشبكة والتخزين؛ ويتفق منفصلاً على الاستحقاق والتوافق.

03

تحديد السعة والتغيير

حدّد CPU و RAM والتخزين وفق الجلسات المتزامنة وتشفير VPN والفحص وأحمال الوكيل/الذاكرة المؤقتة والاحتفاظ بالتقارير. تحقق من احتساب الواجهات و VLAN للتخصيص، واطلب مراجعة قبل زيادة الموارد.

حلول لمزودي الإنترنت والاستضافة

02

آلة العميل الافتراضية

شغل AZTCOFW في آلة افتراضية مخصصة لبيئة كل عميل. يُحتسب ترخيص كل آلة وفق موارد المعالج المطلوبة وعدد واجهات الشبكة.

01

AZTCO Edge

وحدة حماية لمحيط شبكة مزود الخدمة، بترخيص خاص لمزودي الإنترنت والاستضافة يساعد على إبقاء التكلفة مناسبة مع التوسع.

تابع ترخيصك واحصل على الدعم عند الحاجة.

تحقق من صلاحية الترخيص وموعد تجديده. وعند تفعيل النسخ الاحتياطي، اطلع على النسخ المتاحة من خلال حسابك.

02

نسخ الإعدادات الاحتياطية

احتفظ بنسخ إعدادات خارج الجهاز لدعم الاستعادة. عند تفعيل الخدمة لجدار متصل، تساعد النسخ المجدولة والإصدارات المحفوظة على الاستعادة أو الاستبدال بنظام متوافق.

04

الاستجابة والتصعيد

اختر التغطية وفق احتياج التشغيل، مع ساعات الخدمة ومستويات الخطورة وأهداف زمن الاستجابة الأولية وجهات التصعيد المتفق عليها. تحدد اتفاقية الدعم النطاق؛ وزمن الاستجابة يختلف عن زمن الحل.

06

التحديثات دون اتصال

حدّث جدران الحماية المؤهلة والمعزولة أو المقيدة بالإنترنت عبر حزم غير متصلة، من دون تنزيل مباشر من جدار الحماية. تحقق من توفر الحزم وطريقة نقلها لإصدارك.

08

إصلاح الجهاز والاستبدال المؤقت

إذا تعطل جهاز مشمول بالتغطية، تواصل مع الدعم لبدء التشخيص والإصلاح أو الاستبدال وفق اتفاقية الخدمة. قد يحتاج جهاز مؤقت للحفاظ على السعة الأساسية أثناء الإصلاح. يعتمد التوفر والشحن والشروط على موقعك وخطتك؛ تحقق من التغطية قبل الشراء.

01

بوابة العميل

تابع تراخيص جدار الحماية وتواريخ انتهائها وتجديدها من بوابة العميل. وإذا كانت ميزة النسخ الاحتياطي مفعلة، يمكنك الاطلاع على النسخ المحفوظة وتنزيل ما تسمح به صلاحيات حسابك.

03

الدعم الفني

احصل على المساعدة في الإعداد والاتصال وVPN وضبط السياسات واستكشاف الأعطال. تتوفر المساعدة عن بُعد وفق خطة الدعم وموافقتك لمساعدة فريقك على التحقيق في مشكلات الشبكة.

05

التحديثات عبر الإنترنت

ثبّت إصلاحات البرامج والتحسينات المتاحة، وراجع الإصدارات المؤهلة ودالة التحديث وسجله وفق الترخيص. خطط التثبيت حول نوافذ الصيانة المناسبة.

07

مرونة الصيانة

اختر صيانة متصلة أو دون اتصال بما يلائم سياسة الشبكة. خطط نوافذ التحديث وإعادة التشغيل مع فريقك أو دعم AZTCO، وتحقق من توفر الحزم للإصدار.

الأساس المناسب. لخطوتك القادمة.

شغل برنامج AZTCOFW على جهاز AZTCO. قارن أنوية المعالج والذاكرة وتخزين SSD وواجهات الشبكة، ثم حدّد التهيئة المناسبة مع الموزع.

الطرز	أنوية المعالج	الذاكرة	تخزين SSD	واجهات الشبكة
AZS400-20	4	8 غيغابايت	GB SSD 128	4 × 1 GbE RJ45
AZS600-20	4	حتى 16 غيغابايت	GB SSD 265	6 × 1 GbE RJ45
AZS8001-21	8	حتى 32 غيغابايت	GB SSD 512	8 × 1 GbE RJ451 × 4 مع خيار 4 × 10 G SFP+ أو 4 × 10 G SFP
AZS8004-20	8	32 غيغابايت	حتى 1 TB SSD	6 × 1 GbE RJ451 × 2 : 4 × 10 GbE SFP+ للإدارة

تشير كلمة «حتى» إلى الحد الأقصى للسعة. يوضّح عرض السعر التهيئة الفعلية للجهاز. تحقّق من توافق العتاد مع الموزع قبل شراء ترخيص البرنامج.

اطلب عرض سعر

تحدّث مع AZTCOFW أو الموزع عن متطلبات شبكتك. سنساعدك في اختيار البرنامج وطريقة النشر ومستوى الدعم المناسب.

ما المعلومات المطلوبة لإعداد عرض السعر؟

الشبكة والحماية

عدد المستخدمين، وسرعات الاتصال بالإنترنت، وواجهات الشبكة، واتصالات VPN ووحدات الحماية المطلوبة.

طريقة النشر

جهاز AZTCO أو آلة افتراضية أو عتاد متوافق تملكه، وعدد المواقع والموعد المتوقع للتنفيذ.

تغطية الدعم

متطلبات الدعم، وخيارات AZTCO HA أو الآلة الافتراضية الاحتياطية، وإمكانية توفير جهاز بديل مؤقت عند الحاجة.

تواصل معنا

تحدّث مع مختص aztcofirewall.com/ar/contact

تحميل ورقة بيانات المنتج (PDF)