AZTCOFW
CYBER SECURITY SOLUTIONS BY NOWA

الطراز

AZS8004-20

جدار الحماية من الجيل التالي (NGFW)

قارن خيارات الاتصال في أجهزة AZTCOFW واختر المنصة المناسبة بإرشادات السعة والنشر من فريقنا.

8
أنوية المعالج

32 غيغابايت
الذاكرة

حتى 1 TB SSD
تخزين SSD

أجهزة تناسب شبكتك.

الطراز	AZS8004-20
أنوية المعالج	8
الذاكرة	32 غيغابايت
تخزين SSD	حتى 1 TB SSD
واجهات الشبكة	6 × 1 GbE RJ451 × 2 ؛ GbE 10 × 4 ؛للإدارة G SFP+

تحكم دقيق عند حدود شبكتك.

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

01

تصفية الاتصالات مع تتبّع الحالة

طبّق قواعد تصفية على اتصالات IPv4 وIPv6، مع خيارات السماح أو الحظر أو الرفض. حدّد الواجهات والشبكات والمنافذ والبروتوكولات، وسجّل القواعد وراجع جدول حالات الاتصال.

02

إدارة القواعد والسياسات

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

03

NAT والخدمات المنشورة

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

04

شبكات IPv6

استخدم واجهات مزدوجة المكدس، وعناوين IPv6 ثابتة أو DHCPv6 على WAN، وتفويض البادئات وتتبع بادئة LAN، وإعلانات الموجّه وSLAAC وخدمات DHCPv6. تُضبط قواعد IPv6 بصورة مستقلة عن IPv4.

05

تقسيم الشبكة والتوجيه

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

06

اتصالات متعددة بالإنترنت

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

تحكم دقيق عند حدود شبكتك.

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

07

اتصال VPN

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

08

AZTCO HA

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

09

إدارة حركة الشبكة

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

10

خدمات الشبكة

استخدم DHCPv4 وDHCPv6 وترحيل DHCP حيث يتوفر، ومحلل DNS أو معيد توجيهه وتجاوزات DNS وDNS الديناميكي وNTP. يمكن تفعيل التحقق من DNSSEC في المحلل.

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.

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.

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

تعرّف إلى التطبيقات، وحدّد طريقة التعامل معها.

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

01

التحكم بالتطبيقات وتصنيفاتها

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

02

إجراءات التحكم

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

03

تحديد نطاق القواعد

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

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.

05

التعرّف على التطبيقات

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

06

تحديث بيانات التعرف

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

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.

08

حدود النشر

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

> من دون فحص HTTPS، يطبّق 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.

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

01

نظام AZTCO لكشف التسلل ومنعه (IDS/IPS)

افحص حركة الشبكة بحثاً عن أنماط التهديد المعروفة. خصّص القواعد والاستثناءات لكل واجهة، وراجع التنبيهات والأجهزة المحظورة. يعتمد توفر التواقيع وتحديثها وإجراءات المنع على الترخيص والإعداد.

02

حجب نطاقات DNS

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

03

WebGuard – ضبط الوصول إلى الويب

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

04

مكافحة الفيروسات

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

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.

06

مركز متابعة حركة الشبكة (Traffic Center)

راقب استخدام الرفع والتنزيل للتطبيقات والعملاء، والنشاط المباشر وإجماليات الواجهات وتقارير يومية محفوظة. صدّر CSV أو فعّل رسائل البريد اختيارياً. نطاق الجمع والاحتفاظ ظاهر؛ ولا تجمع إجمالي الواجهة وإجمالي العميل معاً.

07

مجموعات FreeRADIUS وبوابة دخول الضيوف

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

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.

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.

01

سجلات النظام وجدار الحماية

راجع أحداث جدار الحماية والنظام والمصادقة VPNg وDNSg وDHCPg والبوابات. وجّه السجلات إلى مجمّع syslog خارجي للاحتفاظ بها خارج الجهاز؛ ويستخدم التوجيه الأصلي UDP.

02

أحداث أمنية منظمة

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

03

استعلام SNMP

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

04

إشعارات SNMP

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

05

حركة المرور والبوابات

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

06

أدوات استكشاف الأعطال

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

07

التشخيص بمساعدة الذكاء الاصطناعي (AI Diagnostics)

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

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.

09

التكامل مع منصات المراقبة

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

تابع ترخيصك واحصل على الدعم عند الحاجة.

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

01

بوابة العميل

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

03

الدعم الفني

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

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.

05

التحديثات عبر الإنترنت

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

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.

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.

08

إصلاح الجهاز والاستبدال المؤقت

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

اطلب عرض سعر

تحدّث مع AZTCOFW أو الموزع عن متطلبات شبكتك. سنساعدك في اختيار البرنامج وطريقة النشر ومستوى الدعم المناسب. · **AZS8004-20**

ما المعلومات المطلوبة لإعداد عرض السعر؟

طريقة النشر

8 · AZS8004-20 أنوية المعالج · 32 غيغابايت الذاكرة · حتى 1 TB SSD

الشبكة والحماية

6 × 1 GbE RJ45؛ 2 × 1 GbE للإدارة؛ 4 × 10G SFP+. عدد المستخدمين، وسرعات الاتصال بالإنترنت، وواجهات الشبكة، واتصالات VPN ووحدات الحماية المطلوبة.

تغطية الدعم

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

اطلب تقديراً لموارد الآلة الافتراضية وتكلفتها

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

تواصل معنا

تحدث مع مختص aztcofirewall.com/ar/contact?interest=AZS8004-20

تنزيل ورقة بيانات المنتج (PDF)