AZTCOFW
CYBER SECURITY SOLUTIONS BY NOWA

MODÈLE

AZS400-20

Pare-feu de nouvelle génération (NGFW)

Comparez la connectivité de la gamme AZTCOFW. Choisissez votre plateforme avec nos conseils de dimensionnement et de déploiement.

4
Cœurs CPU

8 GB
Mémoire vive

128 GB SSD
Stockage SSD

Du matériel pour votre réseau.

Modèle	AZS400-20
Cœurs CPU	4
Mémoire vive	8 GB
Stockage SSD	128 GB SSD
Interfaces réseau	4 × 1 GbE RJ45

Les détails techniques de votre frontière réseau.

Filtrage, adressage, routage, VPN et continuité selon la version et la topologie retenues.

01

Pare-feu à suivi d'état

Filtrage avec suivi d'état des connexions IPv4 et IPv6. Configurez des règles par interface ou globales, leurs actions (autoriser, bloquer, rejeter), les réseaux, ports et protocoles, la journalisation et le diagnostic de la table d'états.

02

Organisation des politiques

Réutilisez des alias d'hôtes, de réseaux et de ports, ainsi que des tables d'URL. Ordonnez les règles, planifiez leur application et définissez des limites par règle lorsque la version le permet.

03

NAT et services publiés

Associez une adresse publique à un hôte interne avec le NAT 1:1, ou publiez un service par redirection de port. Choisissez le NAT sortant automatique, hybride ou manuel et utilisez des IP virtuelles ou le split DNS. Les règles restent déterminantes.

04

Réseau IPv6

Utilisez des interfaces double pile, des adresses IPv6 statiques ou DHCPv6 sur le WAN, la délégation et le suivi de préfixes LAN, les annonces de routeur, SLAAC et DHCPv6. Les règles IPv6 se configurent séparément d'IPv4.

05

Segmentation et routage

Créez des VLAN 802.1Q, séparez LAN et DMZ et configurez les routes statiques ou le routage par passerelle. Définissez explicitement les échanges entre segments et vérifiez ensemble les commutateurs virtuels et physiques.

06

Multi-WAN

Surveillez les passerelles, configurez le basculement par niveaux et répartissez les nouvelles connexions entre passerelles d'un même niveau. Le choix s'applique aux connexions ; une session existante peut devoir se reconnecter après un changement de chemin.

Les détails techniques de votre frontière réseau.

Filtrage, adressage, routage, VPN et continuité selon la version et la topologie retenues.

07

Connectivité VPN

Déployez IPsec et OpenVPN pour l'interconnexion de sites ou l'accès distant ; utilisez WireGuard via le paquet compatible. Certificats, comptes locaux et authentification RADIUS/LDAP dépendent du VPN retenu.

08

AZTCO HA

Assurez le basculement entre deux pare-feu compatibles grâce aux adresses virtuelles partagées et à la synchronisation des états de connexion et de configuration. Prévoyez un réseau dédié et vérifiez la compatibilité des services auprès de votre revendeur.

09

Gestion du trafic

Configurez les files de mise en forme et les limiteurs de débit montant/descendant, avec partage par hôte si nécessaire. La conception dépend des profils de bande passante, pilotes d'interface et chemins de paquets.

10

Services réseau

Utilisez DHCPv4/6, le relais DHCP lorsqu'il est pris en charge, le résolveur ou relais DNS, les substitutions DNS, le DNS dynamique et NTP. La validation DNSSEC peut être activée dans le résolveur.

11

Identité et accès invités

Gérez les comptes et privilèges locaux, l'authentification RADIUS/LDAP prise en charge, les zones de portail captif et les codes d'accès natifs. Personnalisez l'expérience invités aux couleurs d'AZTCO.

12

Configuration et restauration

Administrez via le Web, sauvegardez et restaurez la configuration et consultez son historique. Des outils gèrent les services, tâches planifiées et diagnostics ; les paramètres des extensions peuvent nécessiter des paquets compatibles.

> Choisissez avec votre revendeur les modules et services adaptés au réseau. La disponibilité dépend de la licence, de la configuration matérielle et de la version logicielle retenues.

De la visibilité des applications à des règles explicites.

Examinez la détection, le périmètre des règles et leur application avant d'activer le contrôle.

01

Politiques par application ou catégorie

Choisissez les applications ou catégories prises en charge pour observer l'activité et définir les accès. La détection varie selon le chiffrement, les évolutions des applications et le trafic visible par le pare-feu.

02

Actions de contrôle

Commencez par observer, puis autorisez, bloquez ou limitez séparément le débit montant et descendant des flux pris en charge. Les règles liées à une règle pare-feu sont évaluées dans l'ordre de la politique.

03

Périmètre client et réseau

Associez la politique applicative à des règles IPv4 précises et ciblez des hôtes, réseaux, noms d'hôte ou alias d'adresse. Vérifiez le chemin du trafic correspondant avant d'appliquer un blocage.

04

Intégration aux règles du pare-feu

L'ordre natif des règles reste prioritaire. Les destinations applicatives gérées peuvent servir dans des règles et passerelles ordonnées ; une détection tardive ne redirige pas le trafic déjà engagé.

05

Définitions d'applications actuelles

Les définitions gérées de noms d'hôte et domaines complètent la détection protocolaire pour les applications prises en charge. IP partagées, CDN changeants, noms chiffrés et tunnels peuvent réduire la précision.

06

Mise à jour des détecteurs

Actualisez les données régionales authentifiées manuellement ou selon un calendrier quotidien/hebdomadaire UTC. L'état est visible et le jeu précédent conservé. Les calendriers sont désactivés par défaut.

07

Visibilité opérationnelle

Consultez les flux détectés, octets, paquets et décisions de politique. Les données alimentent les vues compatibles Traffic Center et Client Risk ; elles ne constituent pas une archive exhaustive du trafic.

08

Limites de déploiement

La classification nécessite un trafic observable et peut commencer après les premiers paquets. Testez applications métier, trafic chiffré, VPN et mise en forme avant d'appliquer les restrictions. Les politiques liées au pare-feu prennent en charge IPv4.

> Sans inspection HTTPS, WebGuard applique la règle de destination selon le nom d'hôte demandé. L'analyse antivirus nécessite le trafic HTTPS inspecté et un certificat d'inspection approuvé par les postes.

Des contrôles de sécurité avec une vision opérationnelle.

Découvrez le rôle de chaque module, son intégration au réseau et les conditions à prévoir au déploiement.

01

AZTCO IPS-IDS

Inspection par signatures, politiques par interface, catégories de règles sélectionnées, exceptions, alertes et examen des hôtes bloqués. L'accès aux signatures, la méthode de mise à jour et la prévention dépendent de la licence et de la configuration.

02

DNS Blocker

Utilisez des listes de réputation DNS/IP, des exceptions autorisées et le choix des flux pour limiter les destinations indésirables ou risquées. La politique s'applique aux requêtes passant par le résolveur choisi ; DNS alternatif et chiffré nécessitent des règles réseau.

03

WebGuard

Contrôlez le Web via un proxy explicite HTTP/HTTPS, avec règles de domaine ordonnées, périmètres clients et horaires. Mettez en cache les réponses HTTP éligibles et activez l'inspection HTTPS avec exceptions si le certificat de confiance est installé sur les postes.

04

Antivirus

Analysez les téléchargements HTTPS éligibles par l'inspection WebGuard et bloquez les logiciels malveillants détectés. L'inspection HTTPS et la confiance du poste dans le certificat sont requises.

05

Client Risk

Corrélez les événements IPS, DNS, pare-feu et applicatifs pris en charge. Examinez les scores de risque de 0 à 100, les preuves, l'historique d'enquête et le responsable. Configurez confiance temporaire, notification/blocage ou quarantaine à accès restreint. Un score signale un soupçon, pas une compromission confirmée.

06

Traffic Center

Suivez les usages montant/descendant observés par client et application, l'activité en direct, les totaux par interface et les rapports quotidiens. Exportez en CSV et activez éventuellement les courriels. Ne cumulez pas totaux client et interface.

07

Groupes FreeRADIUS et portail captif

Organisez les comptes locaux et appareils enregistrés en groupes, puis utilisez les alias de groupes IPv4 dans les règles d'accès. Créez des pages invités à votre marque par zone, avec contenu modifiable, aperçu et publication.

08

Hotspot Guard

Surveillez les interfaces choisies pour repérer des indices de partage de connexion, examinez les éléments et exceptions, puis choisissez alertes ou restrictions de source. Ces indices appellent une vérification ; ils ne prouvent pas le partage.

09

Déchargement SSL

Publiez des services par proxy inverse avec terminaison TLS, configuration frontend/backend, contrôles de santé, équilibrage backend et statistiques via l'intégration HAProxy compatible. Cette fonction ne remplace pas un WAF.

Intégrez votre environnement de supervision.

Associez les diagnostics locaux à votre collecteur, SIEM et système de gestion réseau.

01

Journaux système et pare-feu

Consultez les événements du pare-feu, du système, de l'authentification, VPN, DNS/DHCP et des passerelles. Transférez les journaux vers un collecteur syslog externe ; le transfert natif utilise UDP.

02

Événements de sécurité structurés

Envoyez les événements Client Risk par syslog UDP, TCP ou TLS. TCP/TLS utilisent le cadrage octet compté ; TLS vérifie le certificat du récepteur. Sélectionnez événements sécurité, politique, administration et état.

03

Interrogation SNMP

Exposez les informations système et interfaces prises en charge à un outil externe de gestion réseau via SNMP natif. Limitez l'accès aux hôtes de supervision autorisés et vérifiez les MIB de la version choisie.

04

Traps SNMP

Client Risk envoie des traps SNMPv2c avec identifiant d'événement, adresse client, action et score de risque. Configurez récepteur, communauté et base d'OID d'entreprise attribuée. Les traps n'ajoutent pas d'OID de polling ; ce module ne prend pas en charge SNMPv3/informs.

05

Trafic et passerelles

Les graphiques et compteurs d'interface, la latence/perte des passerelles, les états du pare-feu, routes et VPN aident à distinguer les pannes de liaison, de politique et de service.

06

Outils de diagnostic

Capturez des paquets et utilisez ping, traceroute, recherche DNS, inspection des routes/états et Speedtest compatible pour isoler les incidents. Tenez compte de la charge de production lors des tests actifs.

07

AI Diagnostics

Utilisez des contrôles guidés exécutés sur le pare-feu pour rapprocher état, configuration et éléments client pendant le diagnostic. Les résultats décrivent les signaux observés ; l'opérateur les examine avant toute modification.

08

Rapports et alertes

Consultez les éléments/historiques Client Risk, rapports CSV/imprimables, usages quotidiens Traffic Center et exports CSV. Des courriels sont possibles via SMTP configuré. La portée dépend des données et de la rétention.

09

Intégration des collecteurs

Transmettez journaux et événements pris en charge à votre SIEM ou outil de supervision. Configurez parsing, horodatage, conservation et dédoublonnage côté récepteur. UDP et traps ne confirment pas la livraison ; les files sont limitées.

Suivez votre licence et organisez le support.

Consultez l'échéance et le renouvellement, ainsi que les sauvegardes de configuration si activées.

01

Portail client

Consultez licences, échéances et renouvellements de vos pare-feu. Si la sauvegarde est activée, affichez les copies conservées et téléchargez celles autorisées par votre compte.

02

Sauvegardes de configuration

Conservez les copies de configuration hors de l'équipement pour préparer la restauration. Une fois activées sur un pare-feu connecté, les sauvegardes planifiées et leurs versions facilitent la reprise sur un système compatible.

03

Assistance technique

Obtenez de l'aide pour la configuration, la connectivité, VPN, réglage des politiques et diagnostic. L'assistance à distance dépend du contrat et de votre accord.

04

Réponse et escalade

Choisissez des horaires de service, niveaux de gravité, objectifs de première réponse et contacts d'escalade convenus. Le contrat précise la couverture ; délai de réponse et délai de résolution sont distincts.

05

Mises à jour en ligne

Installez les correctifs et améliorations disponibles ; consultez versions admissibles, état et historique selon la licence. Planifiez l'installation dans vos fenêtres de maintenance.

06

Mises à jour hors ligne

Mettez à jour les équipements isolés ou à Internet restreint à l'aide de paquets hors ligne, sans téléchargement direct depuis le pare-feu. Vérifiez la disponibilité et la procédure de transfert pour votre version.

07

Souplesse de maintenance

Choisissez une maintenance connectée ou hors ligne selon vos règles réseau. Planifiez les mises à jour et redémarrages avec l'équipe ou le support AZTCO, et vérifiez la disponibilité des paquets pour votre version.

08

Réparation et équipement temporaire

En cas de panne d'un équipement couvert, contactez le support pour engager le diagnostic puis la réparation ou le remplacement selon votre contrat. Si le service est disponible, un équipement temporaire peut maintenir la capacité essentielle pendant la réparation. Disponibilité, expédition et conditions dépendent de votre région et de votre contrat ; vérifiez la couverture avant l'achat.

Demander un devis

Échangez avec AZTCOFW ou votre revendeur sur votre réseau. Nous pouvons vous aider à choisir le logiciel, le déploiement et le support adaptés. · **AZS400-20**

Précisez vos besoins

Déploiement

AZS400-20 · 4 Cœurs CPU · 8 GB Mémoire vive · 128 GB SSD

Réseau et sécurité

4 × 1 GbE RJ45. Utilisateurs, débits Internet, interfaces réseau, connexions VPN et modules requis.

Couverture de service

Besoins de support, AZTCO HA ou VM redondante et couverture de remplacement temporaire, si disponible.

Demander le dimensionnement et le prix de la VM

Le prix de la licence VM dépend des ressources CPU requises (vCPU/cœurs alloués) et du nombre d'interfaces réseau. Le devis précise allocation, durée et options.

Contact

Parler à un spécialiste aztcofirewall.com/fr/contact?interest=AZS400-20

Télécharger la fiche produit (PDF)