MODEL

AZS8004-20

Next-Generation Firewall (NGFW)

Compare connectivity across the AZTCOFW appliance range. Choose your platform with capacity and deployment guidance from the team.

8
CPU cores

32 GB
RAM

Up to 1 TB SSD
SSD storage

Hardware for your network.

Model	AZS8004-20
CPU cores	8
RAM	32 GB
SSD storage	Up to 1 TB SSD
Network interfaces	6 × 1 GbE RJ45; 2 × 1 GbE management; 4 × 10G SFP+

The technical detail behind your network edge.

Filtering, addressing, routing, VPN and resilience for the selected release and topology.

01

Stateful firewall

IPv4 and IPv6 stateful packet filtering; interface and floating rules; pass, block and reject actions; source/destination networks, ports and protocols; rule logging and state-table diagnostics.

02

Policy organisation

Reusable host, network and port aliases; URL-table aliases; ordered rule evaluation; time-based schedules; per-rule connection and state limits where supported.

03

NAT and public services

IPv4 port forwards, 1:1 NAT and automatic, hybrid or manual outbound NAT; virtual IPs and split-DNS designs. Publish only the services required by policy.

04

IPv6 networking

Dual-stack interfaces, static IPv6 and DHCPv6 WAN addressing, prefix delegation and tracked LAN prefixes; Router Advertisements, SLAAC and DHCPv6 services. IPv6 rules are configured independently from IPv4.

05

Segmentation and routing

802.1Q VLAN interfaces, LAN/DMZ separation, static routes and gateway-based policy routing. Define inter-segment access explicitly; review virtual-switch and physical-switch configuration together.

06

Multi-WAN

Gateway monitoring, tiered failover and same-tier connection load balancing using gateway groups. Selection applies to connections; existing sessions may need to reconnect after a path change.

The technical detail behind your network edge.

Filtering, addressing, routing, VPN and resilience for the selected release and topology.

07

VPN connectivity

IPsec and OpenVPN for site-to-site and remote access; WireGuard through the compatible package. Certificates, local users and supported RADIUS/LDAP authentication depend on the selected VPN design.

08

AZTCO HA

Firewall failover with shared virtual addresses, connection-state synchronisation and configuration synchronisation between compatible firewall pairs. Plan a dedicated synchronisation network and confirm the selected services with your reseller.

09

Traffic management

Traffic-shaper queues and upload/download limiters, including per-host sharing where configured. Bandwidth profiles, interface drivers and packet paths determine the supported shaping design.

10

Network services

DHCPv4/DHCPv6, DHCP relay where supported, DNS resolver/forwarder, DNS overrides, dynamic DNS and NTP. Use DNSSEC validation where configured in the resolver.

11

Identity and guest access

Local administrative users and privileges, supported RADIUS/LDAP authentication, captive-portal zones and native voucher/session controls. AZTCO branding extends the guest experience.

12

Configuration and recovery

Web administration, native configuration backup/restore and revision history; service controls, scheduled tasks and diagnostic tools. A compatible package set is required when restoring addon settings.

> Select the modules and service options suited to your network with your reseller. Availability depends on the licence, appliance configuration and selected software release.

From application visibility to explicit policy.

Review detection, policy scope and enforcement before moving from observation to control.

01

Application and category policies

Select supported applications or categories for visibility and access policy. Detection varies with encryption, application changes and the traffic the firewall can observe.

02

Control actions

Monitor decisions before enforcement; allow, block or apply separate upload/download limits to supported device/application flows. Rules sharing a linked firewall rule are evaluated in policy order.

03

Client and network scope

Link application policies to selected IPv4 firewall rules and scope them by hosts, networks, hostnames or address aliases. Confirm the matching traffic path before enabling enforcement.

04

Native policy integration

Native firewall ordering remains authoritative. Managed domain/IP application destinations can be used with ordered native rules and gateways; this does not reroute an application after late detection.

05

Modern application definitions

Managed hostname/domain definitions supplement protocol detection for supported applications. Shared destination IPs, CDN changes, encrypted hostnames and tunnels can reduce classification precision.

06

Detector maintenance

Authenticated regional detector delivery, manual refresh requests and daily/weekly UTC refresh schedules, with visible update status and retained previous datasets. Schedules start disabled.

07

Operational visibility

Observed application flows, bytes, packets and policy decisions feed the application view and compatible Traffic Center/Client Risk integrations. Runtime counters and bounded observations are not a lossless traffic archive.

08

Deployment boundaries

Classification needs observable traffic and may occur after initial packets. Test your business applications, encrypted traffic, VPNs and shaping before enforcing policy. Firewall-linked application policy supports IPv4 flows.

> Without HTTPS inspection, WebGuard applies HTTPS destination policy using the requested hostname. Antivirus scanning requires inspected HTTPS traffic and trusted client certificates.

Security controls with operational context.

Explore what each module does, how it fits your network and which conditions matter for deployment.

01

AZTCO IPS-IDS

Signature-based inspection, per-interface policies, selected rule categories, suppressions, alerts and blocked-host review. Feed access, update method and prevention behaviour depend on licence and configuration.

02

DNS Blocker

DNS and IP reputation lists, allow exceptions and feed selection for unwanted or known-risk destinations. DNS policy is effective for queries using the configured resolver; alternate DNS and encrypted bypass paths need network policy.

03

WebGuard

Explicit HTTP/HTTPS proxy with ordered domain rules, client scopes and schedules. Cache eligible HTTP responses and apply optional HTTPS inspection with domain exceptions when client trust is configured.

04

Antivirus

Scan eligible HTTPS downloads through WebGuard inspection and block detected malware. Scanning requires HTTPS inspection and client trust in the inspection certificate.

05

Client Risk

Correlate supported IPS, DNS, firewall and application events; review 0–100 risk scores, evidence history, investigation notes and ownership. Configure temporary trust, notification/block modes or restricted-access quarantine. Scores indicate suspicion, not confirmed compromise.

06

Traffic Center

Observed client/application upload and download usage, live activity, separate interface totals, saved daily reports, CSV exports and opt-in administrator email. Collector coverage and retention limits are visible; interface and client totals must not be added together.

07

FreeRADIUS Groups and Captive Portal

Organise local users and registered devices into groups, then use managed IPv4 group aliases in access rules. Create branded guest pages for each zone with editable content, preview and publishing controls.

08

Hotspot Guard

Monitor selected client interfaces for signs of connection sharing, review the supporting evidence and exceptions, and choose alerts or source restrictions. Findings are indicators for review, not proof of a shared connection.

09

SSL Offloading

Reverse-proxy service publishing, TLS termination, frontend/backend configuration, health checks, backend balancing and operational statistics through the compatible HAProxy integration. This is not a substitute for a separately scoped web application firewall.

Connect to your monitoring workflow.

Combine local diagnostics with your own log collector, SIEM and network-management system.

01

Native system and firewall logs

Review firewall, system, authentication, VPN, DNS/DHCP and gateway events. Configure remote system logging to a syslog collector for off-appliance retention; native forwarding uses UDP.

02

Structured security events

Client Risk exports structured events using UDP, TCP or TLS syslog. TCP/TLS use octet-counted framing; TLS verifies the receiver certificate. Select security, policy and administrator/health events.

03

SNMP polling

Native SNMP monitoring exposes supported system/interface information for an external network-management system. Restrict access to authorised monitoring hosts and verify available MIBs on the selected release.

04

SNMP event traps

Client Risk supports SNMPv2c traps with event identifiers, client address, action and risk score. Configure a receiver, community and allocated enterprise OID base. These traps do not add polling OIDs; SNMPv3/informs are not implemented by this module.

05

Traffic and gateway visibility

Interface traffic graphs and counters, gateway latency/loss status, firewall states, routes and VPN status help distinguish link, policy and service faults.

06

Troubleshooting tools

Packet capture, ping, traceroute, DNS lookup, route/state inspection and compatible Speedtest integration support fault isolation. Run active tests with regard to the production workload.

07

AI Diagnostics

Use guided, firewall-local checks to connect status, configuration and client evidence during troubleshooting. Results explain the observed signals; an operator reviews them before changing policy.

08

Reports and notifications

Client Risk evidence/history and CSV/print reports; Traffic Center daily usage and CSV exports; opt-in email using configured SMTP. Report scope depends on observed data and selected retention.

09

Collector integration

Send supported logs/events to your SIEM or monitoring platform. Configure parsing, timestamps, retention and duplicate handling at the receiver. UDP/traps have no delivery acknowledgement; event queues are bounded.

Know your licence status. Plan your support.

Check expiry and renewal information, and access configuration backups when enabled.

01

Customer portal

Check your firewall licences, expiration dates and renewal information in one place. When configuration backup is enabled, view retained backups and download available copies according to your account permissions.

02

Configuration backups

Protect your recovery options with configuration copies stored outside the appliance. When enabled for an online firewall, scheduled backups and retained versions help you prepare for recovery or replacement on a compatible system.

03

Technical support

Get help with configuration, connectivity, VPN, policy tuning and troubleshooting. Remote assistance is available with the applicable support plan and your agreement, helping your team investigate network issues.

04

Response and escalation

Choose support coverage for your operational needs, with agreed service hours, severity levels, initial-response targets and escalation contacts. Your support agreement defines the scope; response and resolution times are distinct.

05

Online updates

Keep your firewall current with available software fixes and feature improvements. View eligible releases, plan installations around your maintenance needs, and review update status and history with the applicable licence.

06

Offline updates

Update eligible isolated or Internet-restricted firewalls with offline packages, without direct downloads from the firewall. Confirm package availability and transfer procedures for your selected release.

07

Maintenance flexibility

Choose connected or offline maintenance to suit your network policies. Plan update windows and required restarts with your team or AZTCO support. Confirm offline package availability for your selected release.

08

Hardware repair and temporary replacement

If a covered appliance fails, contact support to start diagnosis and repair or replacement under your service agreement. Where available, a temporary appliance may be arranged to maintain essential capacity during repair. Availability, shipping and terms depend on your location and plan; confirm coverage before purchase.

Request a quotation

Discuss your network with AZTCOFW or your reseller. We can help you select software, deployment options and support for your business. · **AZS8004-20**

Tell us about your requirements

Deployment

AZS8004-20 · 8 CPU cores · 32 GB RAM · Up to 1 TB SSD

Network and security

6 × 1 GbE RJ45; 2 × 1 GbE management; 4 × 10G SFP+. Users, Internet speeds, network interfaces, VPN connections and security modules required.

Service coverage

Support requirements, AZTCO HA or redundant VM options, and temporary replacement coverage, where available.

Request VM sizing and pricing

VM licence pricing is calculated from the required CPU resources (vCPU/core allocation) and number of network interfaces. The quotation states the agreed resource allowance, licence term and selected options.

Contact

Talk to a specialist aztcofirewall.com/en/contact?interest=AZS8004-20

Download product datasheet (PDF)