MODEL

AZS8004-20

Yeni Nesil Güvenlik Duvarı (NGFW)

AZTCOFW cihazlarının bağlantı seçeneklerini karşılaştırın. Kapasite ve kurulum rehberliğiyle platformunuzu seçin.

8
İşlemci çekirdeği

32 GB
Bellek

En fazla 1 TB SSD
SSD depolama

Ağınız için donanım.

Model	AZS8004-20
İşlemci çekirdeği	8
Bellek	32 GB
SSD depolama	En fazla 1 TB SSD
Ağ arayüzleri	6 × 1 GbE RJ45; 2 × 1 GbE yönetim; 4 × 10G SFP+

Ağ sınırınızın teknik ayrıntıları.

Seçilen sürüm ve topoloji için filtreleme, adresleme, yönlendirme, VPN ve süreklilik.

01

Durum izlemeli güvenlik duvarı

IPv4 ve IPv6 bağlantılarını durum takibiyle filtreleyin. Arayüz ve genel kurallar; izin ver, engelle ve reddet eylemleri; kaynak/hedef ağ, port ve protokoller; kural günlükleri ve durum tablosu tanılaması.

02

Politika düzeni

Yeniden kullanılabilir ana makine, ağ ve port takma adları ile URL tabloları oluşturun. Kural sırasını, zaman çizelgelerini ve desteklenen sürümlerde kural başına bağlantı/durum sınırlarını belirleyin.

03

NAT ve yayımlanan hizmetler

1:1 NAT ile bir genel adresi iç ana makineye eşleyin veya port yönlendirmeyle hizmet yayımlayın. Otomatik, hibrit ya da elle giden NAT; sanal IP ve Split DNS seçeneklerini kullanın. Erişimi kurallarla sınırlandırın.

04

IPv6 ağ iletişimi

Çift yığın arayüzleri, statik IPv6 veya WAN için DHCPv6 adreslemesi, önek devri ve izlenen LAN önekleri; Router Advertisement, SLAAC ve DHCPv6 hizmetleri. IPv6 kuralları IPv4'ten ayrı yapılandırılır.

05

Ağ bölümlendirme ve yönlendirme

802.1Q VLAN arayüzleri oluşturun, LAN ile DMZ'yi ayırın; statik rota ve ağ geçidine dayalı politika yönlendirmesi kullanın. Segmentler arası erişimi açıkça tanımlayın; sanal ve fiziksel anahtarları birlikte doğrulayın.

06

Çoklu WAN

Ağ geçidi izleme, kademeli yedeklilik ve aynı kademedeki bağlantılar arasında yük dağıtımı. Yol seçimi bağlantı başına yapılır; yol değişikliğinde mevcut oturumların yeniden bağlanması gerekebilir.

Ağ sınırınızın teknik ayrıntıları.

Seçilen sürüm ve topoloji için filtreleme, adresleme, yönlendirme, VPN ve süreklilik.

07

VPN bağlantısı

Siteler arası ve uzaktan erişim için IPsec ve OpenVPN; uyumlu paket üzerinden WireGuard kullanın. Sertifika, yerel kullanıcı, RADIUS ve LDAP desteği seçilen VPN tasarımına bağlıdır.

08

AZTCO HA

Uyumlu iki güvenlik duvarı arasında ortak sanal adresler, bağlantı durumu ve yapılandırma eşitlemesiyle devretme sağlayın. Eşitleme için ayrı bir ağ planlayın ve hizmet uyumluluğunu bayinizle doğrulayın.

09

Trafik yönetimi

Trafik şekillendirici kuyrukları ve yükleme/indirme hız sınırlayıcıları oluşturun; ayarlandığında ana makine başına paylaşım uygulayın. Desteklenen tasarım bant genişliği profillerine, arayüz sürücülerine ve paket yoluna bağlıdır.

10

Ağ hizmetleri

DHCPv4/DHCPv6, desteklenen yerde DHCP relay, DNS resolver/forwarder, DNS geçersiz kılmaları, dinamik DNS ve NTP kullanın. Resolver yapılandırmasında DNSSEC doğrulaması etkinleştirilebilir.

11

Kimlik ve misafir erişimi

Yerel yönetici kullanıcılarını ve yetkilerini, desteklenen RADIUS/LDAP kimlik doğrulamasını, captive portal bölgelerini ve yerleşik kupon/oturum kontrollerini yönetin. Misafir deneyimine AZTCO markası ekleyin.

12

Yapılandırma ve kurtarma

Web arayüzünden yönetin; yapılandırmayı yedekleyip geri yükleyin ve sürüm geçmişini inceleyin. Hizmet kontrolleri, zamanlanmış görevler ve tanılama araçları sunulur; eklenti ayarlarını geri yüklemek için uyumlu paketler gerekebilir.

> Ağınıza uygun modül ve hizmet seçeneklerini bayinizle belirleyin. Kullanılabilirlik lisansa, cihaz yapılandırmasına ve seçilen yazılım sürümüne bağlıdır.

Uygulama görünürlüğünden net erişim kurallarına.

İzlemeden denetime geçmeden önce tespiti, politika kapsamını ve uygulama davranışını inceleyin.

01

Uygulama ve kategori politikaları

Görünürlük ve erişim politikası için desteklenen uygulama veya kategorileri seçin. Algılama; şifrelemeye, uygulama değişikliklerine ve güvenlik duvarının görebildiği trafiğe göre değişir.

02

Denetim eylemleri

Uygulamaları önce izleyin; ardından desteklenen akışlara izin verin, engelleyin veya yükleme ve indirme hızını ayrı ayrı sınırlayın. Bağlantılı güvenlik duvarı kuralındaki kurallar politika sırasıyla değerlendirilir.

03

İstemci ve ağ kapsamı

Uygulama politikasını belirli IPv4 kurallarıyla ilişkilendirin; ana makine, ağ, ana makine adı veya adres takma adına göre kapsam belirleyin. Uygulamadan önce eşleşen trafik yolunu doğrulayın.

04

Güvenlik duvarı politikasıyla bütünleşme

Yerleşik kural sırası belirleyicidir. Yönetilen uygulama hedeflerini sıralı kurallar ve ağ geçitleriyle kullanın; geç algılamadan sonra uygulamanın yolu yeniden yönlendirilmez.

05

Güncel uygulama tanımları

Yönetilen ana makine alan adı tanımları, desteklenen uygulamalarda protokol algılamasını tamamlar. Ortak hedef IP'ler, CDN değişiklikleri, şifreli ana makine adları ve tüneller sınıflandırma doğruluğunu azaltabilir.

06

Algılayıcı güncellemeleri

Kimliği doğrulanmış bölgesel algılayıcı verilerini el ile veya günlük/haftalık UTC zamanlamasıyla yenileyin. Güncelleme durumu görünür; önceki veri kümesi saklanır. Zamanlama varsayılan olarak kapalıdır.

07

Operasyonel görünürlük

Gözlemlenen uygulama akışlarını, bayt ve paket sayılarını ve politika kararlarını inceleyin. Veriler uyumlu Traffic Center ve Client Risk görünümlerine aktarılır; eksiksiz trafik arşivi oluşturmaz.

08

Dağıtım sınırları

Sınıflandırma gözlemlenebilir trafik gerektirir ve ilk paketlerden sonra başlayabilir. Kısıtlamaları uygulamadan önce iş uygulamalarını, şifreli trafiği, VPN'i ve şekillendirmeyi sınayın. Güvenlik duvarı kuralına bağlı uygulama politikası IPv4 akışlarını destekler.

> HTTPS denetimi kapalıyken WebGuard, hedef politikasını istenen ana makine adına göre uygular. Antivirus taraması, denetlenen HTTPS trafiği ve istemcide güvenilen sertifika gerektirir.

Operasyonel ihtiyaçlarınıza uygun güvenlik kontrolleri.

Her modülün işlevini, ağınıza nasıl uyduğunu ve dağıtımda hangi koşulların önemli olduğunu inceleyin.

01

AZTCO IPS-IDS

İmza tabanlı inceleme, arayüz başına politikalar, seçili kural kategorileri, istisnalar, uyarılar ve engellenen ana makinelerin incelenmesi. İmza akışı, güncelleme ve önleme davranışı lisans ve yapılandırmaya bağlıdır.

02

DNS Blocker

İstenmeyen veya riskli hedefleri sınırlamak için DNS/IP itibar listeleri, akış seçimi ve izin istisnaları kullanın. Politika, yapılandırılmış resolver üzerinden geçen sorgulara uygulanır; alternatif ve şifreli DNS yolları ağ politikası gerektirir.

03

WebGuard

Sıralı alan adı kuralları, istemci kapsamı ve zamanlamayla açık HTTP/HTTPS proxy'si kurun. Uygun HTTP yanıtlarını önbelleğe alın; istemci güven sertifikası ayarlandığında isteğe bağlı HTTPS incelemesi ve alan adı istisnaları uygulayın.

04

Antivirus

WebGuard incelemesinden geçen uygun HTTPS indirmelerini tarayın ve tespit edilen zararlı yazılımı engelleyin. HTTPS denetimi ve istemcinin inceleme sertifikasına güvenmesi gerekir.

05

Client Risk

Desteklenen IPS, DNS, güvenlik duvarı ve uygulama olaylarını ilişkilendirin. 0–100 risk puanlarını, kanıt geçmişini, inceleme notlarını ve sahipliği gözden geçirin. Geçici güven, uyarı/engelleme veya kısıtlı karantina seçilebilir. Puan şüphe göstergesidir; doğrulanmış ihlal değildir.

06

Traffic Center

Gözlemlenen istemci ve uygulama yükleme/indirme kullanımını, canlı etkinliği ve arayüz toplamlarını izleyin. Günlük raporları görüntüleyin, CSV dışa aktarın ve isteğe bağlı e-posta bildirimleri alın. İstemci ve arayüz toplamları birlikte toplanmamalıdır.

07

FreeRADIUS grupları ve Captive Portal

Yerel kullanıcıları ve kayıtlı cihazları gruplandırın; IPv4 grup takma adlarını erişim kurallarında kullanın. Her bölge için içeriği düzenlenebilir, önizlenebilir ve yayımlanabilir markalı misafir sayfaları oluşturun.

08

Hotspot Guard

Seçili istemci arayüzlerinde bağlantı paylaşımı belirtilerini izleyin; kanıtları ve istisnaları inceleyip uyarı veya kaynak kısıtlaması seçin. Bulgular inceleme işaretidir, paylaşım kanıtı değildir.

09

SSL Offloading

Uyumlu HAProxy entegrasyonuyla TLS sonlandırma, ön/arka uç yapılandırması, sağlık kontrolleri, arka uç yük dağıtımı ve işlem istatistikleri içeren ters proxy üzerinden hizmet yayımlayın. WAF yerine geçmez.

Mevcut izleme iş akışınıza bağlanın.

Yerel tanı araçlarını kendi günlük toplayıcınız, SIEM ve ağ yönetim sisteminizle birleştirin.

01

Yerel sistem ve güvenlik duvarı günlükleri

Güvenlik duvarı, sistem, kimlik doğrulama, VPN, DNS/DHCP ve ağ geçidi olaylarını inceleyin. Kayıtları cihaz dışında tutmak için uzak syslog toplayıcısına iletin; yerel iletim UDP kullanır.

02

Yapılandırılmış güvenlik olayları

Client Risk güvenlik, politika ve yönetim/sağlık olaylarını UDP, TCP veya TLS syslog ile gönderir. TCP/TLS octet-counted çerçeveleme kullanır; TLS alıcı sertifikasını doğrular.

03

SNMP sorgulama

Yerleşik SNMP ile desteklenen sistem ve arayüz bilgilerini harici ağ yönetim sistemine sunun. Erişimi yetkili izleme ana makineleriyle sınırlayın ve seçili sürümdeki MIB'leri doğrulayın.

04

SNMP olay tuzakları

Client Risk; olay kimliği, istemci adresi, eylem ve risk puanı içeren SNMPv2c tuzakları gönderir. Alıcıyı, topluluk adını ve ayrılmış kurumsal OID tabanını yapılandırın. Bu özellik sorgulama OID'leri eklemez; modül SNMPv3/inform desteklemez.

05

Trafik ve ağ geçidi görünürlüğü

Arayüz grafikleri ve sayaçlarını, ağ geçidi gecikme/kayıp durumunu, güvenlik duvarı durumlarını, rotaları ve VPN bilgisini inceleyerek bağlantı, politika ve hizmet arızalarını ayırt edin.

06

Sorun giderme araçları

Paket yakalama, ping, traceroute, DNS sorgusu, rota/durum incelemesi ve uyumlu Speedtest entegrasyonuyla arızaları ayrıştırın. Üretim trafiğini gözeterek etkin test yapın.

07

AI Diagnostics

Sorun giderirken güvenlik duvarı üzerindeki yönlendirmeli kontrollerle durum, yapılandırma ve istemci kanıtlarını ilişkilendirin. Sonuçlar gözlenen sinyalleri açıklar; politikayı değiştirmeden önce operatör inceler.

08

Raporlar ve bildirimler

Client Risk kanıt/geçmişini ve CSV/yazdırma raporlarını; Traffic Center günlük kullanımını ve CSV dışa aktarımını kullanın. SMTP yapılandırıldıysa isteğe bağlı e-posta gönderilir. Rapor kapsamı gözlenen veri ve saklama ayarlarına bağlıdır.

09

Toplayıcı entegrasyonu

Desteklenen günlük ve olayları SIEM veya izleme platformunuza gönderin. Alıcıda ayrıştırma, zaman damgası, saklama ve yinelenen kayıt işlemlerini yapılandırın. UDP/tuzaklarda teslim onayı yoktur; kuyruklar sınırlıdır.

Lisans durumunuzu görün, desteğinizi planlayın.

Süre sonu ve yenileme bilgilerini kontrol edin; etkinse yapılandırma yedeklerine erişin.

01

Müşteri portalı

Güvenlik duvarı lisanslarını, sona erme tarihlerini ve yenileme bilgilerini tek yerde kontrol edin. Yapılandırma yedeklemesi etkinse saklanan yedekleri görüntüleyip hesabınızın izin verdiği kopyaları indirin.

02

Yapılandırma yedekleri

Kurtarma için yapılandırma kopyalarını cihaz dışında saklayın. Çevrimiçi güvenlik duvarında etkinleştirildiğinde zamanlanmış ve sürümlü yedekler, uyumlu sistemde kurtarma/değişim planına yardımcı olur.

03

Teknik destek

Yapılandırma, bağlantı, VPN, politika ayarı ve sorun gidermede destek alın. Uzaktan yardım, geçerli destek planı ve onayınızla ağ sorunlarını incelemeye yardımcı olur.

04

Yanıt ve eskalasyon

Operasyon ihtiyacınıza uygun hizmet saatleri, önem düzeyleri, ilk yanıt hedefleri ve eskalasyon irtibatları belirleyin. Kapsamı destek sözleşmesi tanımlar; yanıt ve çözüm süresi farklıdır.

05

Çevrimiçi güncellemeler

Mevcut yazılım düzeltmeleri ve iyileştirmeleri alın. Lisansınıza uygun sürümleri, güncelleme durumunu ve geçmişini görüntüleyip kurulumları bakım zamanlarına göre planlayın.

06

Çevrimdışı güncellemeler

İzole veya İnternet erişimi kısıtlı güvenlik duvarlarını, doğrudan indirme yapmadan çevrimdışı paketlerle güncelleyin. Seçilen sürüm için paketleri ve aktarım yöntemini doğrulayın.

07

Bakım esnekliği

Ağ politikanıza göre çevrimiçi veya çevrimdışı bakım seçin. Güncelleme ve yeniden başlatma zamanlarını ekibinizle ya da AZTCO desteğiyle planlayın; sürümünüz için paket erişimini doğrulayın.

08

Donanım onarımı ve geçici cihaz

Kapsam dahilindeki bir cihaz arızalanırsa, teşhis, onarım veya değiştirme sürecini başlatmak için destekle iletişime geçin. Onarım sırasında temel kapasiteyi sürdürmek üzere, mevcutsa geçici bir cihaz sağlanabilir. Uygunluk, gönderim ve koşullar konumunuza ve planınıza bağlıdır; satın almadan önce kapsamı doğrulayın.

Teklif isteyin

Ağınızı AZTCOFW veya bayinizle görüşün. İşletmeniz için yazılımı, dağıtım seçeneklerini ve desteği belirlemenize yardımcı olabiliriz. · **AZS8004-20**

Gereksinimlerinizi paylaşın

Dağıtım

AZS8004-20 · 8 İşlemci çekirdeği · 32 GB Bellek · En fazla 1 TB SSD

Ağ ve güvenlik

6 × 1 GbE RJ45; 2 × 1 GbE yönetim; 4 × 10G SFP+. Kullanıcılar, İnternet hızları, ağ arayüzleri, VPN bağlantıları ve gereken güvenlik modülleri.

Hizmet kapsamı

Destek ihtiyaçları, AZTCO HA veya yedek VM seçenekleri ve mevcutsa geçici cihaz kapsamı.

VM boyutlandırma ve fiyat teklifi isteyin

VM lisans bedeli gerekli CPU kaynaklarına (vCPU/çekirdek tahsisi) ve ağ arayüzü sayısına göre hesaplanır. Teklifte kaynak sınırı, lisans süresi ve seçenekler belirtilir.

İletişim

Bir uzmanla görüşün aztcofirewall.com/tr/contact?interest=AZS8004-20

Ürün teknik föyünü indirin (PDF)