PREGÃO ELETRÔNICO Nº: 52/2022

Razão Social: Algar Multimídia S/A
CNPJ: 04.622.116/001-13
Endereço: Rua José Alves Garcia, nº 415 – Bairro Brasil – Uberlândia/MG
Contatos: Raissa Rizza Andrade Costa (34) 98855-0825
E-mail: raissarac@algartelecom.com.br

ATENDIMENTO ÀS ESPECIFICAÇÕES TÉCNICAS

Demonstramos, em atendimento ao previsto no subitem 4.3.1, 4.3.2 e 4.3.3 do Anexo II do Pregão Eletrônico nº 52/2022 o atendimento às especificações dos itens e subitens obrigatórios, especificando a localização exata das informações comprobatórias inseridas em nossa Proposta Comercial apresentada.

Item	Documento	Status	Página	Obs.
1.2. Appliance Firewall (item 1)				
1.2.1. Características Gerais				
1.2.1.1.	Datasheet_v2.4.0	Atende	6	NGFW Throughput (IMIX) 350 MBPS
1.2.1.2	Datasheet_v2.4.0	Atende	6	Firewall Throughput (UDP) 6GBPS
1.2.1.3	Datasheet_v2.4.0	Atende	6	IPSEC VPN Throughput (AES-256 +SHA256) 500 mbps
1.2.1.4	Datasheet_v2.4.0	Atende	6	SSL Inspection Throughput 200 mbps
1.2.1.5	Datasheet_v2.4.0	Atende	6	Conexões Simultâneas 6.000.000
1.2.1.6	Datasheet_v2.4.0	Atende	6	Conexões Novas por segundo 38.000
1.2.1.7	Datasheet_v2.4.0	Atende	16	VLAN (IEEE 802.lq) até 4094 por interface
1.2.1.8	Blockbit_Networks_Compatibility_Matrix	Atende	1	Max G/W to G/W IPSEC Tunnels – 50
1.2.1.9	Blockbit_Networks_Compatibility_Matrix	Atende	1	Max Client to G/W IPSEC Tunnels – 150
1.2.1.10	Datasheet_v2.4.0	Atende	6	Interface de Rede 4 X GE RJ45
1.2.2. Funcionalidades Específicas				
1.2.2.1. Arquitetura				
I	Proposta Comercial	Atende	-	-
II	Proposta Comercial	Atende	-	-
III	Proposta Comercial	Atende	-	-
1.2.2.2. Licenciamento				
I	Proposta Comercial	Atende	-	-
1.2.2.3. Hardware				
I	Proposta Comercial	Atende	-	-
II	Proposta Comercial	Atende	-	-
III	Proposta Comercial	Atende	-	-
IV	Datasheet_v2.4.0	Atende	6	Temperatura ideal de Operação - |0° (14°F) – 60°C (140°F)
V	Proposta Comercial	Atende	-	-
VI	Datasheet_v2.4.0	Atende	6	1 x USB FOTO EQUIPAMENTO
VII	Proposta Comercial	Atende	-	-
VIII	Datasheet_v2.4.0	Atende	3	O Blockbit NGFW (Next-Generation Firewall) simplifica a

				criação de políticas e regras de segurança complexas, podendo ser implementado como gateway ou inline, otimizada para análise de conteúdo de aplicação na camada 7
1.2.2.4 Funcionalidades Básicas				
I	Blockbit+NGFW+PT+2.4.0	Atende	121-122	System Resource
II	Datasheet_v2.4.0	Atende	16	Suporte ao protocolo SNMP vl, v2 e v3
III	Datasheet_v2.4.0	Atende	16	Gerenciamento (LAN ou WAN) via WEB (HTTPS por browser) e SSH
IV	Blockbit+NGFW+PT+2.4.0	Atende	108-110/121-122	Traffic Monitor/Network System Resources
V	Blockbit+NGFW+PT+2.4.0	Atende	223-225/262-266/196-199/185-188/107-110	UTM – Application Control/UTM – Threat Protection/NGFW – Web Filter/UTM – Firewall/Traffic Monitor – Network
VI	Blockbit+NGFW+PT+2.4.0	Atende	1406 / 1364	Remote Syslog / Gerenciamento Global – Analyzer
1.2.2.5. Rede				
I	Datasheet_v2.4.0	Atende	14	Suporta 1Pv4 e 1Pv6
II	Datasheet_v2.4.0	Atende	16	VLAN (IEEE 802.lq) até 4094 por interface
III	Datasheet_v2.4.0	Atende	16	DHCP (dynamic host configuration protocol) IPv4 e IPv6 – Relay, Server e Client
IV	Blockbit+NGFW+PT+2.4.0	Atende	999	Para habilitar esta opção, marque a caixa de checagem. Este campo define o MTU da interface virtual, os valores possíveis estão entre 1280 e 9000 (JUMBO FRAME)
V	Datasheet_v2.4.0	Atende	16	Suporta sub-interfaces ethernet lógicas
VI	Datasheet_v2.4.0	Atende	16	Suporte a servidores NTP (Network Time Protocol) para atualização de data e hora
VII	Datasheet_v2.4.0	Atende	14	NAT dinâmico (Many-to-Many e Many-to-1) – Nat estático (1:1 e Many-to-Many) e bidirecional 1:1
VIII	Blockbit+NGFW+PT+2.4.0	Atende	133-135	Events – Query Editor – Create query
IX	Datasheet_v2.4.0	Atende	14	NAT (SNAT e DNAT), 1:1, N:I, NAT65, NAT46, NAT44 e NAT66, PAT, NAT de Origem e NAT de Destino e simultaneamente.
X	Datasheet_v2.4.0	Atende	15/16	Roteamento dinâmico: BGP/BGP4+, OSPFv2/v3/ RIPv2 e PIM-SM Roteamento estático (IPv4 e IPv6) com suporte a ECMP. Suporta roteamento estático, dinâmico (OSPF, BGP) IPv4/IPv6
XI	Datasheet_v2.4.0	Atende	16	Roteamento dinâmico: BGP4/BGP4+ OSPFv2/v3, RIPv2 e PIM-SM
XII	Blockbit+NGFW+PT+2.4.0	Atende	14	Roteamento Avançado e Dinâmico; BGPv4+; OSPFv2 e v3; RIPv1, v2 e RIPng; IGMP; Roteamento multicast (PIM-SM)
XIII	Datasheet_v2.4.0	Atende	20	RFC 3768: Virtual Router Redundancy Protocol (VRRP)

XIV	Datasheet_v2.4.0	Atende	16	Suporte ao protocolo SNMP vl, v2 e v3.
XV	Datasheet_v2.4.0	Atende	16	Monitoramento
XVI	Datasheet_v2.4.0	Atende	16	Roteamento baseado em política (PBR – Policy Based Routing ou PBF – Policy Based Forwarding)
1.2.2.6. Autenticação e Identificação de Usuários				
I	Datasheet_v2.4.0	Atende	16	Autenticação
II	Datasheet_v2.4.0	Atende	16	Sincronismo de usuários e grupos e hosts com servidores Windows AD e servidores LDAP com replicação de sessões estabelecidas dos usuários
III	Datasheet_v2.4.0	Atende	17	Permite o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (Captive Portal)
IV	Datasheet_v2.4.0	Atende	17	Permite criar políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através de integração com serviços de diretório, autenticação via LDAP, Active Directory e base de dados local
V	Datasheet_v2.4.0	Atende	16	Monitor – Security Events – Este painel possui alguns recursos que permitem uma análise profunda mais detalhada: Através deste painel é possível efetuar busca de acordo com queries personalizadas, analisar incidentes e eventualidades específicas, perm.
VI	Blockbit+NGFW+PT+2.4.0	Atende	86/90	Monitor – Live Sessions
VII	Datasheet_v2.4.0	Atende	16	Granularidade (perfis de leitura e leitura/escrita, aplicações de configurações etc.) de acesso administrador na Interface Web com sessões simultâneas
1.2.2.7. Geolocalização				
I	Datasheet_v2.4.0	Atende	3	Suporta criar políticas de bloqueio ou liberação por geolocalização e informam nos logs e país de origem e/ou destino com a bandeira para facilitar a identificação do tráfego
II	Blockbit+NGFW+PT+2.4.0	Atende	352/353	COUNTRY
III	Datasheet_v2.4.0	Atende	3	Suporta criar políticas de bloqueio ou liberação de geolocalização e informam nos logs o país de origem e/ou destino com a bandeira para facilitar a identificação do tráfego.
IV	Datasheet_v2.4.0	Atende	3	Informam nos logs o país de origem e/ou destino com a bandeira para facilitar a identificação do tráfego.
1.2.2.8. VPN				
I	Datasheet_v2.4.0	Atende	15	VPN túnel (LAN to LAN) VPN Site-to-Site e Client-to-Site
II	Datasheet_v2.4.0	Atende	15	AES(128, 192 e 156), 3DES
III	Blockbit+NGFW+PT+2.4.0	Atende	898	Authentication Algorithm MD5/SHA1/SHA256

IV	Datasheet_v2.4.0	Atende	15	IKEvL e IKEv2 (para fase 1 e fase 2) e ESP
V	Datasheet_v2.4.0	Atende	15	DH (Diffie-Hellman – Grupo 1, Grupo 2, Grupo 4, Grupo 14; Grupo 15, Grupo 16, Grupo 17, Grupo 18, Grupo 19, Grupo 20, Grupo 21, Grupo 22, Grupo23, Grupo24, Grupo25, Grupo 26, Grupo27, Grupo28, Grupo29, Grupo30) RSA key Generation, DAS parameter.
VI	Datasheet_v2.4.0	Atende	16	VPN SSL com suporte a certificado digital X.509 v3/Gerenciamento de certificado SSL (X.509)
VII	Datasheet_v2.4.0	Atende	15	NAT-5 (encapsulamento UDP)
VIII	Blockbit+NGFW+PT+2.4.0	Atende	852	UTM Services VPN IPSEC / VPN SSL
IX	Blockbit+NGFW+PT+2.4.0	Atende	885	VPN IPSEC Acesso Remoto
X	Datasheet_v2.4.0	Atende	15	VPN RAS/SSL (remote access permite acesso por cliente de VPN ou suporte direto na estação sem cliente – Interface Web), ou seja, pode utilizar a VPN SSL com ou sem agente. Cliente VPN compatível com Win7, 8/8.1, 10 e 11 (32 e 64 bits), Linux MacOS.
XI	Blockbit+NGFW+PT+2.4.0	Atende	972	Acessando Portal de Autenticação (VPN SSL Portal)
XII	Blockbit+NGFW+PT+2.4.0	Atende	986	Acesso Remoto Rede
XIII	Datasheet_v2.4.0	Atende	15	Permite atribuir DNS nos clientes
XIV	Datasheet_v2.4.0	Atende	15	Suporta roteamento estático, dinâmico (OSPF, BGP). IPv4/IPv6
XV	BLOCKBIT_CLIENT_PT_V2.1.0rev00.Manual_do_Usuário	Atende	53	Windows Login
XVI	BLOCKBIT_CLIENT_PT_V2.1.0rev00.Manual_do_Usuário	Atende	51	Simple Login + Certificate
XVII	Datasheet_v2.4.0	Atende	4	Crie políticas de controle de aplicações, IPS, Antivírus, Antspyware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL/IPSEC
XVIII	Datasheet_v2.4.0	Atende	15	Suporte a certificados emitidos por autoridade certificadora o padrão ICP-Brasil
XIX	BLOCKBIT_CLIENT_PT_V2.1.0rev00.Manual_do_Usuário	Atende	53	Windows Login
XX	BLOCKBIT_CLIENT_PT_V2.1.0rev00.Manual_do_Usuário	Atende	2	Documentação Blockbit Client_PT_v2.1.0
XXI	Blockbit+NGFW+PT+2.4.0	Atende	1499	.p12 PKCS-(Public Key Cryptography Stadards) #12 Data File
XXII	Datasheet_v2.4.0	Atende	15	Suporta a inclusão (enrollment) de autoridades certificadoras mediante SCEP (Simple Certificate Enrollment Protocol)
XXIII	Datasheet_v2.4.0	Atende	15	Suporte a verificação de certificate revocation list (CRL)
XXIV	Datasheet_v2.4.0	Atende	4	Crie políticas de controle de aplicações, IPS, Antivírus, Antispyware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL/IPSEC
1.2.2.9. Qualidade de Serviço (QoS)				
I	Datasheet_v2.4.0	Atende	4	A Blockbit Platform conta com recurso de QoS exclusivo que permite, via interface gráfica centralizada e local, priorizar

				tráfego e controlar a largura de banda de acordo com as políticas de segurança e conformidades configuradas, além da classificação de pacotes (Shaping). O recurso de QoS avançado categoriza conexões de acordo com sua importância e possibilita priorizar pacotes através da marcação de DSCP e TOS. Defina banda máxima e garantida por aplicação, suporta o match em categoria de URL, IPs, de origem e destino, logins e portas. Regras de QoS podem ser habilitadas por horários ou intervalo de tempo.
II	Datasheet_v2.4.0	Atende	14	Controle de tráfego e garantia de banda por política (aplicações, usuários ou grupos de usuários sincronizados com o Windows AD ou LDAP), zona de rede, host específico ou origem/destino.
III	Datasheet_v2.4.0	Atende	16	Suporta VoIP (SIP/H323)
IV	Datasheet_v2.4.0	Atende	19	• RFC 3260: New Termology and Clarifications for Diffserv; • RFC 2597: Assured Forwarding PHB Group • RFC 2475: An Architucture for Differentiated Services • RFC 2474: Definition ofthe Differentiated Services Field (OS Field) in the IPv4 and IPv6 Headers
V	Blockbit+NGFW+PT+2.4.0	Atende	223	UTM – Application Control
1.2.2.10 Balanceamento de Links				
I	Datasheet_v2.4.0	Atende	15	Suporta balanceamento de link por hash do IP de origem e destino, pro peso com configuração do percentual e podendo utilizar de 2 a 9 links
II	Datasheet_v2.4.0	Atende	15	Suporte a múltiplos perfis de configuração e permite habilitar em qualquer interface WAN (DSL, MPLS, 3G/4G LTE)
III	Datasheet_v2.4.0	Atende	15	Definição de envio de tráfego por interface selecionada, suporta Policy Based Routing
IV	Blockbit+NGFW+PT+2.4.0	Atende	741	SDWAN-Failover
V	Datasheet_v2.4.0	Atende	15	Failback do link personalizável de 1 a 100 e persistência de Links
VI	Datasheet_v2.4.0	Atende	15	Roteamento baseado em aplicação e política para múltiplos caminhos WAN, com bloqueio de app
VII	Datasheet_v2.4.0	Atende	04/05	SD-WAN
VIII	Datasheet_v2.4.0	Atende	15	Verificação de falha do link por protocolo TCP/UDP Echo, ICMP (ping)
1.2.2.11. Recursos de Segurança				
I	Datasheet_v2.4.0	Atende	4	ATP – Proteção Avançada Contra Ameaças (Antivírus e Anti-Spyware)/IPS – Sistema de Prevenção de Intrusos/

				Filtragem de Conteúdo/ Controle de Aplicações.
II	Datasheet_v2.4.0	Atende	14	Suporta modo transparente (camada 2), modo gateway (camada 3) e espelhamento de porta
III	Blockbit+NGFW+PT+2.4.0	Atende	65	UTM – Fila de Comandos
IV	Blockbit+NGFW+PT+2.4.0	Atende	1374	Atualização de bases de assinaturas (IPS, WEB FILTER, APPLICATION CONTROL e ATP) são realizadas de forma automática sem a necessidade de reboot no Appliance Blockbit ou no módulo de gerência.
V	Blockbit+NGFW+PT+2.4.0	Atende	1381	Update bases automatically
VI	Datasheet_v2.4.0	Atende	14	Prevenção contra ataques do tipo Worm, Trojan, Backdoors, Portscans (detecta e bloqueia a origem), IP Spoofing, SYN-ICMP-UDP flood e Spywares/ Prevenção DoS, DDoS (Flood, Scan, Session e Sweep), PORTSCAN, Reconnaissence, Evasione e ICMP
VII	Datasheet_v2.4.0	Atende	3	A Blockbit Platform conta com descriptografia de SSL para inspeção de tráfego de saída (Outbound), garantindo o controle total de acesso e aplicando recursos avançados, como ATP, Filtro de Conteúdo, Controle de Aplicação e Antimalware, Suporta TLS 1.2 e TLS 1.3
VIII	Datasheet_v2.4.0	Atende	3	A Blockbit Platform conta com descriptografia de SSL para inspeção de tráfego de saída (Outbound), garantindo o controle total de acesso e aplicando recursos avançados, como ATP, Filtro de Conteúdo, Controle de Aplicação e Antimalware, Suporta TLS 1.2 e TLS 1.3
IX	Blockbit+NGFW+PT+2.4.0	Atende	533-534	Exceptions
X	Datasheet_v2.4.0	Atende	16	Snapshot e Backup do Sistema Criptografado Disaster recovery (backup/restore) pela interface Web
XI	Blockbit+GSM+PT+2.4.0	Atende	199	Aba Backups
XII	Datasheet_v2.4.0	Atende	16	Antivírus e Anti-Malware com análise em tempo real – HTTP, HTTPS, FTP, SMB, CIFS, POP3 e SMTP (nativo na solução)
1.2.2.12 Filtro de Pacotes				
I	Datasheet_v2.4.0	Atende	14	Suporta modo transparente (camada 2), modo gateway (camada 3) e espelhamento de porta
II	Blockbit+NGFW+PT+2.4.0	Atende	436	O Firewall opera no modo "Stateful" e dispõe de ferramentas que parametrizam os "Níveis de segurança" e os "Controle das conexões", além das políticas de "Filtro de Pacotes" e "Redirecionamento – DNAT" e análise de padrões de estado de conexões, bem

				como análise de decodificação de protocolo, análise de detecção de anomalias de protocolo, IP Deframentation, remontagem de pacotes de TCP e bloqueio de pacotes malformados e Controle de Tráfego.
III	Blockbit+NGFW+PT+2.4.0	Atende	1577	Services – Em sua configuração inicial, por padrão, o sistema traz alguns objetos (portas/protocolos) pré-cadastrados, os objetos referentes aos protocolos e serviços mais comuns: Exemplo: "DHCP", "DNS", "HTTP", "HTTPS".
IV	Datasheet_v2.4.0	Atende	16	Suporta VoIP (SIP/H323)
V	Datasheet_v2.4.0	Atende	14	Proteção Ati-Spoofing
VI	Datasheet_v2.4.0	Atende	14	Suporta IPv4 e IPv6
VII	Datasheet_v2.4.0	Atende	14	IP de Origem/Destino, Porta e Protocolo/(política de filtragem) com possibilidade de agendamento/criação de políticas por usuários ou grupos.
VIII	Blockbit+NGFW+PT+2.4.0	Atende	647	CUSTOM CATEGORIES
IX	Datasheet_v2.4.0	Atende	17	Suporta granularidade as políticas de IPS, Antivírus e Anti-Spyware, possibilita a criação de diferentes políticas de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens
1.2.2.13. Filtro de Conteúdo				
I	Datasheet_v2.4.0	Atende	4	A Blockbit é capaz de reconhecer aplicações independentemente de porta e protocolo, portanto é possível liberar a aplicação sem precisar liberar porta e/ou protocolos
II	Datasheet_v2.4.0	Atende	3	Capaz de detectar aplicações encapsuladas e validar se o tráfego corresponde com a especificação do protocolo. O recurso também identifica funcionalidade específica dentro de uma aplicação
III	Datasheet_v2.4.0	Atende	3	A maioria das informações que trafegam na web usam conexões criptografadas. A Blockbit Platform conta com descriptografia de SSL para inspeção de tráfego de saída (Outbound), garantindo o controle total de acesso e aplicando recursos avançados, como ATP, Filtro de Conteúdo, Controle de Aplicação e Antimalware.
IV	Blockbit+NGFW+PT+2.4.0	Atende	557	Application Control – Lista de Categorias Email; Proxy; Social; Remote; Ads; VoIP; Storage;

				Collaboration; Mobile; Update; Protocol; Games; Business; Streaming; Cloud; Web; Portal; P2P; Download.
V	Blockbit+NGFW+PT+2.4.0	Atende	20	Definitions: Armazena dados de inteligência e definições de sistema, como regras de compliance e assinaturas maliciosas, entre outras.
VI	Blockbit+NGFW+PT+2.4.0	Atende	550/557	Application Control – Lista de Categorias Email; Proxy; Social; Remote; Ads; VoIP; Storage; Collaboration; Mobile; Update; Protocol; Games; Business; Streaming; Cloud; Web; Portal; P2P; Download
VII	Blockbit+NGFW+PT+2.4.0	Atende	557	Application Control – Lista de Categorias Email; Proxy; Social; Remote; Ads; VoIP; Storage; Collaboration; Mobile; Update; Protocol; Games; Business; Streaming; Cloud; Web; Portal; P2P; Download
VIII	Datasheet_v2.4.0	Atende	17	Suporta a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular por usuários sobre o uso das aplicações que estão nestes serviços.
IX	Blockbit+NGFW+PT+2.4.0	Atende	15	Suporte granularidade nas políticas de IPS, Antivírus e Anti-Spyware, possibilita a criação de diferentes políticas

				por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens.
X	Blockbit+NGFW+PT+2.4.0	Atende	353-354	Identification
XI	Datasheet_v2.4.0	Atende	16	Registro de usuários os eventos de autenticação, acesso, bloqueio e ameaças.
XII	Datasheet_v2.4.0	Atende	14	Controle de tráfego e garantia de banda por política (aplicações, usuários ou grupos de usuários sincronizados com o Windows AD ou LDAP), zona de rede, host específico ou origem/destino
XIII	Blockbit+NGFW+PT+2.4.0	Atende	150	Diagnostic – Cetogory Lookup
XIV	Datasheet_v2.4.0	Atende	15	88 categorias (incluindo Governo, Webmail, Instituição de Saúde, Noticias, Pornografia, Restaurante, Redes Sociais, Esporte e Educação, Jogos, Compras), +49 milhões de URLs catalogadas, controle de login, por domínio no Google, integração SafeSearch (busca segura), Google, Bing e Yahoo, mensagem de bloqueio para o usuário final.
XV	Datasheet_v2.4.0	Atende	15	Lista personalizadas (whitelist e blacklist)
XVI	Blockbit+NGFW+PT+2.4.0	Atende	20	Definitions: Armazena dados de inteligência e definições de sistema, como regras de compliance e assinaturas maliciosas, entre outras;
XVII	Blockbit+NGFW+PT+2.4.0	Atende	219	Web Filter – Top users
XVIII	Datasheet_v2.4.0	Atende	14/17	Suporta granularidade nas políticas possibilita a criação de diferentes políticas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens.
XIX	Datasheet_v2.4.0	Atende	657	Este item permite customizar a página de bloqueio que é devolvida aos usuários da rede referente aos acessos "Não Autorizados" do tráfego Web (interceptados pelo Proxy).
XX	Blockbit+NGFW+PT+2.4.0	Atende	127	Monitor – Security Events
XXI	Datasheet_v2.4.0	Atende	14	Suporta política por tempo, horário e/ou período (dia, mês, ano, dia da semana e hora). Suporta grupos de usuários, IPs, rede e/ou zonas de segurança.
XXII	Datasheet_v2.4.0	Atende	15	Integração SafeSearch (busca segura), Google, Bing e Yahoo.
XXIII	Datasheet_v2.4.0	Atende	14	Habilitação de web cache de conteúdos dinâmicos (Facebook, Google Maps, MSN Vídeo, Sourceforge Downloads, Windows Updare, YouTube).
1.2.2.14. Prevenção de Intrusão (IPS)				
I	Datasheet_v2.4.0	Atende	4	O IPS conta com milhares de assinaturas para identificação

				de ameaças em um banco de dados atualizado diariamente
II	Datasheet_v2.4.0	Atende	14	Detecção e prevenção de ataques e intrusões baseada em +80 mil assinaturas agrupadas como Client (Aplicações) e Server (Servidores)
III	Datasheet_v2.4.0	Atende	4	A Blockbit é capaz de reconhecer aplicações independentemente de porta e protocolo, portanto é possível liberar a aplicação sem precisar liberar porta e/ou protocolos. Identifica o uso de táticas evasivas para controlar aplicações que tentam usar conexões criptografadas (por exemplo Skype ou rede TOR).
IV	Datasheet_v2.4.0	Atende	14	Reconhecimento de padrões, analise de protocolos e anomalias e bloqueia vulnerabilidade/Proteção contra ameaças na camada de aplicação (Exploit/Níveis de impacto: Baixo, Médio e Alto/Fragmentação e desfragmentação IP)
V	Datasheet_v2.4.0	Atende	3	A Blockbit Platform conta com descriptografia de SSL para inspeção de tráfego de saída (Outbound) garantindo o controle total de acesso e aplicando recursos avançados, como ATP, Filtro de Conteúdo, Controle de Aplicação e Antimalware. Suporta TLS 1.2 e TLS 1.3. Suporta aplicação de políticas de segurança e visibilidade para as aplicações que circulam.
VI	Blockbit+NGFW+PT+2.4.0	Atende	436	O firewall opera no modo "Stateful" e dispõe de ferramentas que parametrizam os "Níveis de segurança" e os "Controles das conexões", além das políticas de "Filtros de Pacotes" e "Redirecionamento – DNAT" e análise de padrões de estado de conexões.
VII	Datasheet_v2.4.0	Atende	17	Registra na console de monitoração as seguintes informações sobre ameaças identificadas: o nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo.
VIII	Datasheet_v2.4.0	Atende	17	Registra na console de monitoração as seguintes informações sobre ameaças: o nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além, da ação tomada pelo dispositivo
IX	Datasheet_v2.4.0	Atende	14	Permite ativar ou desativar as assinaturas, ou habilitar em modo de monitoração

X	Datasheet_v2.4.0	Atende	17	Permite a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas de firewall considerando usuários, grupos de usuários, origem, destino, zonas de segurança, MAC Address, cada politica de firewall poderá ter um configuração diferente de IPS, sendo essas políticas por Usuários, Grupos de usuários, origem, destino, zonas de segurança
XI	Datasheet_v2.4.0	Atende	14	Log de registro das incidências para cada tipo de ataque identificado.
XII	Datasheet_v2.4.0	Atende	15	Identifica, classifica e bloqueia malware tais como, trojan, spyware, adware, keyloggers, highjackers, Worms, vírus, conexões do tipo C&C (Command and Control) e Anti-Bot (Botnet)
XIII	Datasheet_v2.4.0	Atende	14	Prevenção contra anomalias de protocolos (HTTP, SMTP, POP, IMAP, Sendmail, NTP, NetBIOS, HTIPS, FTP, DNS, SMB, CIFS, RPC, RDP, CHARGEN, SSDP, SNMP, TCP highjacking SSH e Telnet)
XIV	Datasheet_v2.4.0	Atende	17	Possui proteção contra vírus em conteúdo HTML e Javascript, software espião (spyware) e Worms
XV	Datasheet_v2.4.0	Atende	4	Blockbit Platform pode detectar malware avançados como trojans e vírus, ameaças persistentes avançadas e ataques de call-backs maliciosos. O ATP também pode bloquear IPs com má reputação em diferentes categorias (abusers, anonymizers, attackers, malware, spam) além de ataques por geolocalização. Bloqueia arquivos pela extensão e também identifica pelo tipo MIME (mesmo mudando a extensão).
XVI	Blockbit+NGFW+PT+2.4.0	Atende	20	Armazena dados de inteligência e definições de sistema, como regras de compliance e assinaturas maliciosas, entre outras.
XVII	Datasheet_v2.4.0	Atende	20	RFC 7541: HPACK: Header Compression for HTTP/2 RFC 7540: Hypertext Transfer Protocol Version 2 (HTTP/2)
1.3. CONSOLE DE GERENCIAMENTO CETRALIZADO PARA FIREWALL (Item 2)				
1.3.1 Características Gerais				
1.3.1.1	Proposta Comercial	Atende	-	-
1.3.1.2	Proposta Comercial	Atende	-	-
1.3.1.3	Blockbit+GSM+PT+2.4.0	Atende	14	Plataforma de virtualização: VMware, XenServer, KMV e ProxMox
1.3.1.4	Proposta Comercial	Atende	-	-

1.3.1.5	Proposta Comercial	Atende	-	-
1.3.2. Gerenciamento				
1.3.2.1	Blockbit+GSM+PT+2.4.0	Atende	50	GSM – INTERFACE WEB
1.3.2.2	Proposta Comercial	Atende	-	-
1.3.2.3	Proposta Comercial	Atende	-	-
1.3.2.4	Blockbit+GSM+PT+2.4.0	Atende	16	Ao conectar um dispositivo Blockbit UTM ao Blockbit GSM é estabelecido um Túnel seguro utilizando comunicação criptografada, possibilitando a aplicação das configurações geradas.
1.3.2.5	Blockbit+GSM+PT+2.4.0	Atende	10	GSM – Introdução
1.3.2.6	Blockbit+GSM+PT+2.4.0	Atende	10	Para melhor compreensão, segue um exemplo: Supondo que você é administrador de uma rede de 1.000 lojas e necessita bloquear o acesso a determinado domínio de rede social para cada loja, sem o Blockbit GSM será necessário configurar o Firewall de cada loja para realizar o bloqueio de todas as lojas ao mesmo tempo, basta apenas fazer a configuração adequada no Blockbit GSM e executar o deploy para todas as lojas, simples, rápido e prático.
1.3.2.7	Blockbit+GSM+PT+2.4.0	Atende	11	Permite a criação de políticas e grupos de políticas para controlar os acessos das redes protegidas pelas devices, de forma rápida, fácil e sem erros;
1.3.2.8	Datasheet_v2.4.0	Atende	5	Gerenciamento Centralizado
1.3.2.9	Datasheet_v2.4.0	Atende	5	Gerenciamento Centralizado
1.3.2.10	Blockbit+GSM+PT+2.4.0	Atende	818	Administration – Aba "Auth Servers"
1.3.2.11	Blockbit+GSM+PT+2.4.0	Atende	810 – 812	User Profiles – Menu de Ações – Create Profile
1.3.2.12	Blockbit+GSM+PT+2.4.0	Atende	837	Administration – Aba "Audit Log"
1.3.2.13	Blockbit+GSM+PT+2.4.0	Atende	443	Identificação
1.3.2.14	Blockbit+GSM+PT+2.4.0	Atende	325/336	Objects / Create Group
1.3.2.15	Blockbit+GSM+PT+2.4.0	Atende	341	Objet / Mapping
1.3.2.16	Blockbit+GSM+PT+2.4.0	Atende	442	Tempo / Agendamento
1.3.2.17	Blockbit+GSM+PT+2.4.0	Atende	10	O Blockbit GSM – Global Security Management ou Gerenciamento Global de Segurança, foi desenvolvido para gerenciar as múltiplas soluções da Blockbit. Através dele é possível administrar os perfis de dispositivos, gerenciamento e automação de inventário, Monitoramento, realizar upgrade remotamente e muitas outras soluções que serão devidamente detalhadas posteriormente.
1.3.2.18	Blockbit+GSM+PT+2.4.0	Atende	108	Status da conexão entre o Blockbit GSM e o Blockbit UTM
1.3.2.19	Blockbit+NGFW+PT+2.4.0	Atende	107	Monitor – Traffic Monitor
1.3.2.20	Blockbit+NGFW+PT+2.4.0	Atende	1430	System – Aba High Availability
1.3.2.21	Blockbit+GSM+PT+2.4.0	Atende	341	Objects – Address – Object Mapping

1.3.2.22	Blockbit+NGFW+PT+2.4.0	Atende	397	IPv4 – Menu de ações – Validate Policies
1.3.2.23	Blockbit+NGFW+PT+2.4.0	Atende	1415	System – Aba Notifications
1.3.2.24	Blockbit+GSM+PT+2.4.0	Atende	79	Proporciona o monitoramento através de gráficos do status do seu gateway em aspectos gerais, tais como: sistema operacional, utilização CPU, tuneis ativos, conexões concorrentes e casos de desconexão de gateway com o GSM
1.3.2.25	Blockbit+GSM+PT+2.4.0	Atende	50	GSM – Interface WEB/Acesso remoto (SSH e Console)
1.3.3. Relatórios				
1.3.3.1	Blockbit+GSM+PT+2.4.0	Atende	469	O Blockbit GSM – Analyzer atua recebendo os dados emitidos pelas UTMs, que são administrados nas opções do menu Blockbit GSM – Management, gerando diversos tipos de relatórios e logs
1.3.3.2	Blockbit+GSM+PT+2.4.0	Atende	618	A função desta opção é administrar a criação automática e periódica de relatórios personalizados, permitindo seleção de características específica dos devices selecionados. Suporta também a distribuição automática de relatórios por e-mail através de agenda pré-determinada
1.3.3.3	Blockbit+GSM+PT+2.4.0	Atende	469	O GSM também prove uma visualização sumarizada de todas as aplicações, ameaças (IPS, antivírus, anti-malware) e URLs analisadas pelo firewall;
1.3.3.4	Blockbit+GSM+PT+2.4.0	Atende	622	Aba Custom
1.3.3.5	Blockbit+GSM+PT+2.4.0	Atende	620	Analysis: Permite a criação dos seguintes relatórios na aba Datasets: Network Traffic
1.3.3.6	Blockbit+GSM+PT+2.4.0	Atende	837	Administration – Audit Logs
1.3.3.7	Blockbit+GSM+PT+2.4.0	Atende	621	Scheduled: Exibe a data de agendamento para quando esse relatório será executado;
1.3.3.8	Blockbit+GSM+PT+2.4.0	Atende	627	Events
1.3.3.9	Blockbit+GSM+PT+2.4.0	Atende	469	O Blockbit GSM – Aalyzer é um módulo de avaliação e criação de relatórios avançados, proporcionando uma perspectiva holística a detecção, ao executar monitoramento de tráfego de rede em tempo real em múltiplos pontos e segmentos de rede, o analyzer possibilita e investigação e execução de ações orientadas no combate a ameaças, tentativas de intrusão e utilização de aplicações não autorizadas.
1.3.4 Logs				
1.3.4.1	Blockbit+GSM+PT+2.4.0	Atende	621	Analysis: Permite a criação dos seguintes relatórios na aba Datasets: Network Traffic; Policy Usage; Web Filter; Application Control; Intrusion

				Prevention; Threat Protection; User Behavior
1.3.4.2	Blockbit+GSM+PT+2.4.0	Atende	469	O GSM também prove uma visualização sumarizada de todas as aplicações, ameaças (IPS, antivírus, anti-malware) e URLs analisadas pelo firewall.
1.3.4.3	Blockbit+GSM+PT+2.4.0	Atende	469	O Blockbit GSM – Analyzer atua recebendo os dados emitidos pelos UTMs, que são administrados nas opções do menu Blockbit GSM – Management, gerando diversos tipos de relatórios e logs
1.3.4.4	Blockbit+GSM+PT+2.4.0	Atende	627-630	Este painel possui alguns recursos que permitem uma análise profunda mais detalhada: Através deste painel é possível efetuar uma busca de acordo com queries personalizadas, analisar incidentes e eventualidades específicas, permitindo uma administração muito mais precisa e eficiente
1.3.4.5	Blockbit+GSM+PT+2.4.0	Atende	627-630	EVENTS – Este painel possui alguns recursos que permitem uma análise profunda mais detalhada: Através deste painel é possível efetuar uma busca de acordo com queries personalizadas, analisar incidentes e eventualidades específicas, permitindo uma administração muito amis precisa e eficiente.
1.3.4.6	Blockbit+GSM+PT+2.4.0	Atende	626	Status – Visualize ou Dowload

Uberlândia, 11 de agosto de 2023

Assinado de forma digital por RAISSA RIZZA ANDRADE COSTA:09769230685

Raissa Rizza Andrade Costa
CPF: 097.692.306-85
RG: MG 15.511-899

Algar Telecom

MARINGÁ
PREFEITURA DA CIDADE

ATESTADO DE CAPACIDADE TÉCNICA

Atestamos para os devidos fins que a empresa **ALGAR MULTIMÍDIA S/A**, empresa Autorizatária pela ANATEL para a prestação do Serviço de Comunicação Multimídia – SCM, devidamente inscrita no CNPJ/MF sob o nº 04.622.116/0001-13, estabelecida na Rua José Alves Garcia, 415 – bairro Brasil, CEP: 38.400-668, na cidade de Uberlândia-MG, está executando os serviços citados através do(s) contrato(s) **493-2020 celebrado em 28/07/2020** que se encontra-se vigentes até a presente data com a **PREFEITURA DO MUNICÍPIO DE MARINGÁ**, regularmente inscrito no **CNPJ/MF sob n° 76.282.656/0001-06**, e estabelecida no endereço Av. XV de Novembro, nº 701 – Bairro Centro – CEP 87013-230 – Maringá/PR

- **SERVIÇOS COM ACESSO MPLS (MULTI-PROTOCOL LABEL SWITCHING):**

Com conectividade dedicada, e velocidade simétrica com 100% da capacidade concentrada com equipamentos certificados e homologados ANATEL acordo de nível de serviço (ANS) de 99,7% ao mês com tempo de reparo de até 4 horas. Configuração através de Redes Privativas Virtuais (VPN – Virtual Private Network) formando uma única rede com comunicação direta entre si, em uma topologia, full-mesh, com Qualidade de Serviço (QoS) através da arquitetura DiffServ, incluindo DifServ sobre MPLS e no mínimo 6 filiais.

- **Links MPLS Concentrador:**

Quantidade	Velocidade
2	2 Gbps

- **Links MPLS Acessos Remotos:**

Quantidade	Velocidade
05	500 Mbps
04	100 Mbps
08	50 Mbps
04	30 Mbps
164	20 Mbps
200	10 bps

- **Serviço de Clean Pipe (Anti-DDoS)**:

Proteção do acesso Internet disponibilizado no Backbone fornecendo proteção contra ataques de negação de serviço DOS (Denial of Service) e DDOS (Distributed Denial of Service), realizando as mitigações nos Centros de Limpeza Nacionais e Centros de Limpeza nos EUA com capacidade mínima de 100 Gbps monitorada por uma equipe SOC própria (Security Operation Center).

- **SERVIÇOS DE GERENCIAMENTO DE REDE:**

Proativos (NOC – Network Operation Service) com funcionamento 24 horas por dia, 7 (sete) dias na semana, com capacidade de detecção proativa de falhas ocorridas nos circuitos (serviços e equipamentos) com permissão do acompanhamento dos registros de problemas e das ações executadas para a recuperação dos serviços com fornecimento de portal web para efetuar e acompanhar solicitações de serviço, visualizar histórico de relatórios, análises e recomendações de gerência de rede, reports periódicos e emissão de relatórios gerenciais.

MARINGÁ
PREFEITURA DA CIDADE

- **LINKS DEDICADOS DE ACESSO À INTERNET:**

Links dedicados de Acesso à internet simétricas com 100% da capacidade contratada, entregues com acesso em Fibra Óptica com equipamentos certificados e homologados na ANATEL, acordo de nível de serviço (ANS) de 99,7% ao mês com tempo de reparo de até 4 horas e latência ≤ 80 milissegundos, suporte técnico, prefixos IPv4 e IPv6 no concentrador. O Backbone está conectado a pelo menos 10 Autonomuos System (AS) e pontos de troca de tráfego (PTT) no Brasil com capacidade total mínima de 300 Gbps e Backbone IP com saída internacional com destino direto para os Estados Unidos da América (EUA) com no mínimo 100 Gbps.

Quantidade de Links	Velocidade
54	10 Mbps
04	20 Mbps
02	30 Mbps
04	100 Mbps
02	500 Mbps
02	2 Gbps

- **SERVIÇO DE GERENCIAMENTO DE SEGURANÇA (SOC – Security Operation Center):**

Com funcionamento 24 horas por dia, 7 (sete) dias na semana com monitoração permanente do ambiente, regras de segurança e de controle de tráfego, notificação de falhas em Rede WAN, contemplando Instalação, Operação e Manutenção de Firewall UTM provendo proteção de rede com características de Next Generation Firewall (NGFW) para segurança de informação perimetral, que inclui: Filtro de pacote, controle de aplicação, administração de largura de Banda (QoS), VPN IPSec e SSL, IPS, prevenção contra ameaças de vírus, Spywares e Malwares, Filtro URL, e acesso à internet.

Quantidades de Pontos (Hardware/Licença) Fortinet	02

Informamos, outrossim, que o referido serviço acima descrito, têm sido prestados dentro dos padrões de qualidade técnica exigidos, não havendo nada que possa desabonar a empresa.

Por ser verdade firmamos.

Maringá, 19 de janeiro de 2023.

Jose Thadeu S. da Silva
José Thadeu S. da Silva (19 de Janeiro de 2023 13:18 GMT-3)

Nome: José Thadeu Siqueira Silva
Cargo: Gerente de Infraestrutura
Contato: (44) 3221-1603

JS

ASUN
SUPERMERCADOS

ATESTADO DE CAPACIDADE TÉCNICA

Atestamos para os devidos fins que a empresa **ALGAR MULTIMÍDIA S/A**, empresa Autorizatária pela ANATEL para a prestação do Serviço de Comunicação Multimídia – SCM, devidamente inscrita no CNPJ/MF sob o nº 04.622.116/0001-13, estabelecida na Rua José Alves Garcia, 415 – bairro Brasil, CEP: 38.400-668, na cidade de Uberlândia-MG, está executando os serviços citados através do(s) contrato(s) **202104070943-1 e 202104062950-1 celebrados em 26/06/2021 e 1-T6YXBCG celebrado em 28/11/2019** que se encontram-se vigentes até a presente data com a **ASUN COMERCIO DE GENEROS ALIMENTICIOS EIRELI**, regularmente inscrito no **CNPJ/MF sob n° 92.091.891/0001-57**, e estabelecida no endereço Rua Acylino Francisco Medeiros, nº 657 – Bairro Distrito Industrial – CEP 94045-410 – Gravataí/RS

- **DA TECNOLOGIA SD-WAN:**
  - A solução convergente é executada através de dispositivos no qual parte dos serviços poderão ser implementados diretamente pelo hardware, com a solução SD-WAN embarcada no dispositivo;
  - Funcionalidade de redundância e failover para todos os acessos físicos, permitindo que quando um dos links apresentar falhas, o outro acesso ligado na estrutura assuma a transmissão dos dados;
  - Balanceamento de tráfego entre os links ativos, baseado em volumetria, com roteamento inteligente para a priorização de tráfego;
  - Controle de caminho automático, baseado em políticas previamente aplicadas, com recursos para comutação dinâmica dos caminhos automaticamente, selecionando o melhor caminho, no mínimo, a partir dos seguintes parâmetros, simultâneos ou não:

    - ➔ Tipo de aplicação;
    - ➔ Prioridade de negócio;
    - ➔ Banda;
    - ➔ Latência;
    - ➔ Jitter;
    - ➔ Perda de pacotes.

  - Prover visibilidade fim-a-fim dos fluxos de comunicação das aplicações sobre a rede SD-WAN;
  - Prover visibilidade do desempenho da rede em tempo real, baseada nas aplicações e nos parâmetros de uso de banda, perda de pacote e latência;
  - Prover visualização de todas as configurações, políticas e status dos terminais da solução SD-WAN;
  - Preservar todas as licenças permanentes necessárias para suportar os requisitos de SD-WAN, de modo que todas as funções sejam plenamente atendidas.
  - Suporte do Técnico e do Fabricante;
  - Entre outras funcionalidades inerentes à tecnologia.

Quantidades de Pontos (Hardware/Licença) Fortinet	34

AM
AM

- **Serviço Gerenciamento de Segurança (SOC – Security Operation Center)** - com funcionamento 24 horas por dia, 7 (sete) dias na semana com monitoração permanente do ambiente, regras de segurança e de controle de tráfego, notificação de falhas em Rede WAN, contemplando instalação, operação e manutenção de Firewall UTM provendo proteção de rede com características de Next Generation Firewall (NGFW) para segurança de informação perimetral, que inclui: Filtro de pacote, controle de aplicação, administração de largura de banda (QoS), VPN IPSec e SSL, IPS, prevenção contra ameaças de vírus, Spyrewares e Malwares, Filtro de URL, e acesso à internet.

Quantidades de Pontos (Hardware/Licença) Fortinet	34

Informamos, outrossim, que o referido serviço acima descrito, têm sido prestados dentro dos padrões de qualidade técnica exigidos, não havendo nada que possa desabonar a empresa.

Por ser verdade firmamos.

Gravataí/RS, 21 de setembro de 2022.

Antonio Martins
Antonio Martins (21 de Setembro de 2022 16:39 ADT)

Nome: Antônio Martins
Cargo: TI
Contato: amartins@asun.com.br – 51 98206-0106

Assinatura:

Email: juliost@algartelecom.com.br

Eletrozema
A rede que faz sua Família Feliz.

DS DHDAP

ATESTADO DE CAPACIDADE TÉCNICA

Atestamos para os devidos fins que a empresa **ALGAR MULTIMÍDIA S/A**, empresa Autorizatária pela ANATEL para a prestação do Serviço de Comunicação Multimídia – SCM, devidamente inscrita no CNPJ/MF sob o nº 04.622.116/0001-13, estabelecida na Rua José Alves Garcia, 415 – bairro Brasil, CEP: 38.400-668, na cidade de Uberlândia-MG, está executando os serviços citados através do(s) contrato(s) **DR URA—5560-2010 celebrado em 05/10/2010 e Contrato(s) Aditivo(s) 51CE2B4A-0F1D-4F93-BF3A-8A260726D831 e 8DB8FD32-432E-4A3B-9542-F733252D19A1** que se encontram-se vigentes até a presente data com a **ELETROZEMA S.A**, regularmente inscrito no **CNPJ/MF sob n° 26.404.731/0001-96**, e estabelecida no endereço Av. José Ananias de Aguiar, nº 5005 – Bairro Conjunto Habitacional Boa Vista – CEP 38184-200 – Araxá/MG

- **LINKS DEDICADOS DE ACESSO À INTERNET:**

Links dedicados de Acesso às internets simétricas com 100% da capacidade contratada, entregues com acesso em Fibra Óptica com equipamentos certificados e homologados na ANATEL, acordo de nível de serviço (ANS) de 99/5% ao mês com tempo de reparo de até 4 horas e latência ≤ 80 milissegundos, suporte técnico, prefixos IPv4 e IPv6 no concentrador. O Backbone está conectado a pelo menos 10 Autonomuos System (AS) e pontos de troca de tráfego (PTT) no Brasil com capacidade total mínima de 300 Gbps e Backbone IP com saída internacional com destino direto para os Estados Unidos da América (EUA) com no mínimo 100 Gbps.

Quantidade de Links	Velocidade
1	1 Gbps

- **BANDA LARGA:**

Serviço que utiliza tecnologia de comunicação Banda Larga, tendo como meio a linha telefônica comum (SFTC) par metálico e fibra óptica, com acesso à rede mundial de computadores, a serem prestados para o órgão.

Quantidade de Links	Velocidade
109	100 Mbps
2	360 Mbps
1	140 Mbps
2	260 Mbps
1	380 Mbps

- **VPN NODE:**

Com instalação de conectividade dedicada, permanente e velocidades simétricas com 100% da capacidade contratada, entregues com acesso em Fibra Óptica com equipamentos certificado e homologados ANATEL, acordo de nível de serviços (ANS) 99,5% ao mês com tempo de reparo de até 4 horas. O Backbone está conectado a pelo menos 5 Autonomous System (AS) e pontos de troca de tráfego (PTT) no Brasil com capacidade total mínima de 200 Gbps e 2 Autonomous System (AS) e ponto de troca de tráfego (PTT) com capacidade total mínima de 100 Gbps.

Quantidade	Velocidade
1	500 Mbps
119	10 Mbps

DS ACA

DS DiDAP

- **DA TECNOLOGIA SD-WAN + SOC:**

• A solução convergente é executada através de dispositivos no qual parte dos serviços poderão ser implementados diretamente pelo hardware, com a solução SD-WAN embarcada no dispositivo;
• Funcionalidade de redundância e failover para todos os acessos físicos, permitindo que quando um dos links apresentar falhas, o outro acesso ligado na estrutura assuma a transmissão dos dados;
• Balanceamento de tráfego entre os links ativos, baseado em volumetria, com roteamento inteligente para a priorização de tráfego;
• Controle de caminho automático, baseado em políticas previamente aplicadas, com recursos para comutação dinâmica dos caminhos automaticamente, selecionando o melhor caminho, no mínimo, a partir dos seguintes parâmetros, simultâneos ou não:

- ➔ Tipo de aplicação;
- ➔ Prioridade de negócio;
- ➔ Banda;
- ➔ Latência;
- ➔ Jitter;
- ➔ Perda de pacotes.

• Prover visibilidade fim-a-fim dos fluxos de comunicação das aplicações sobre a rede SD-WAN;
•Prover visibilidade do desempenho da rede em tempo real, baseada nas aplicações e nos parâmetros de uso de banda, perda de pacote e latência;
• Prover visualização de todas as configurações, políticas e status dos terminais da solução SD-WAN;
• Preservar todas as licenças permanentes necessárias para suportar os requisitos de SD-WAN, de modo que todas as funções sejam plenamente atendidas.
• Suporte do Técnico e do Fabricante;
• Entre outras funcionalidades inerentes à tecnologia.
• Gerenciamento centralizado da Solução
• Contemplando instalação, operação e manutenção de Firewall UTM provendo proteção de rede com características de Next Generation Firewall (NGFW) para segurança de informação perimetral, que inclui: Filtro de pacote, controle de aplicação, administração de largura de banda (QoS), VPN IPSec e SSL, IPS, prevenção contra ameaças de vírus, Spyrewares e Malwares, Filtro de URL, e acesso à internet.

Quantidades de Pontos (Hardware/Licença) Fortinet	119

- **SERVIÇO DE GERENCIAMENTO DE SEGURANÇA ANTI-DDOS:**
Com proteção dos acessos Internet disponibilizado no backbone fornecendo proteção contra ataques de negação de serviço em momentos de ataques DOS (Denial of Service) e DDOS (Distributed Denial of Service), através de 2 (dois) Centros de Limpeza Nacionais com capacidade de 80 Gbps e 1 (um) Centro de Limpeza nos EUA com capacidade de 40 Gbps monitorada por uma equipe SOC própria (Security Operation Center).

DS ACA

Eletrozema
A rede que faz sua Família Feliz.

DS DHDAP

- **SERVIÇO DE ATENDIMENTO PREMIUM**
  Canal de relacionamento dedicado, com equipe de profissionais especializados para atuar de forma proativa em alarmes e/ou problemas. Uma equipe especial - Gestor de Prestação de Serviços (SDM) – acompanhamento 24 horas por dia a empresa de serviços. Além disso, o serviço oferece um trabalho proativo que identifica as oportunidades que o cliente tem para telefonar para os melhores resultados com o seu negócio. Monitoramento dedicado e especializado para fornecer feedback, análise de relatórios de desempenho da rede. Emissão de documentos como relatórios, gráficos e analise a respeito da rede que está sendo monitorada além do fornecimento de portal web para solicitações/acompanhamentos entre outras funções.

    - **Relatórios Mensais de performance da rede incluindo:**
        - Gráfico de Indisponibilidade;
        - Relatório de tráfego de qualidade;
        - Relatório de conexões de rede e visualização de portas;
        - Relatório de configuração de equipamentos de rede;
        - Relatório de consumo de banda;
        - Relatório de eventos;
        - Relatório de Localidades;
        - Tráfego simples;
        - Visualização de portas;
        - Entre outras.

- **SERVIÇOS DE REDE SEM FIO (Wi-Fi) COM A SEGUINTES CARACTERÍSTICAS:**
    - Frequência de operação para os pontos de acesso sem fio (Access Point Wireless – AP) 2,4 GHz e 5,0 GHz;
    - Tecnologias suportadas – 802.11 a / b / g / n / ac;
    - Controle e gerenciamento centralizado em nuvem, visualização de equipamentos e dispositivos em tempo real, fornecimento de relatórios gerenciais, segmentação de redes, controle de acesso, conteúdo, aplicações e banda, firewall, cobertura com prevenção de intrusos, processo de autenticação, logs de acesso etc;
    - Suporte técnico remoto e presencial para APs Indoor/Outdoor

MODELO	QUANTIDADE
MR20	465
MR44	40

Informamos, outrossim, que o referido serviço acima descrito, têm sido prestados dentro dos padrões de qualidade técnica exigidos, não havendo nada que possa desabonar a empresa.

Por ser verdade firmamos.

Araxá-MG, 19 de agosto de 2022.

DocuSigned by:
Diego Henrique de Almeida Pereira
F6D0379TF1CD4FA...

Nome: DIEGO HENRIQUE DE ALMEIDA PEREIRA
Cargo: COORDENADOR DE REDES E INFRAESTRUTURA T.I
Contato: (34) 3669-1895 ■ (34) 98871-0592

DS JGAJ

DS ACA

ANGELONI

ATESTADO DE CAPACIDADE TÉCNICA

Atestamos para os devidos fins que a empresa **ALGAR MULTIMÍDIA S/A**, empresa Autorizatária pela ANATEL para a prestação do Serviço de Comunicação Multimídia – SCM, devidamente inscrita no CNPJ/MF sob o nº 04.622.116/0001-13, estabelecida na Rua José Alves Garcia, 415 – bairro Brasil, CEP: 38.400-668, na cidade de Uberlândia-MG, está executando os serviços citados através do(s) contrato(s) **e66c6a26-2b52-4ab5-866e-28f4c1013bd4 celebrado em 17/05/2021** que se encontra-se vigentes até a presente data com a **A. ANGELONI & CIA. LTDA**, regularmente inscrito no **CNPJ/MF sob n° 83.646.984/0006-14**, e estabelecida no endereço Av. Centenário, nº 7521 – Bairro Nossa Senhora da Salete – CEP 88115-900 – Criciúma/SC

- **LINKS DEDICADOS DE ACESSO À INTERNET:**

Links dedicados de Acesso à internet simétricas com 100% da capacidade contratada, entregues com acesso em Fibra Óptica com equipamentos certificados e homologados na ANATEL, acordo de nível de serviço (ANS) de 99/5% ao mês com tempo de reparo de até 4 horas e latência ≤ 80 milissegundos, suporte técnico, prefixos IPv4 e IPv6 no concentrador. O Backbone está conectado a pelo menos 10 Autonomuos System (AS) e pontos de troca de tráfego (PTT) no Brasil com capacidade total mínima de 300 Gbps e Backbone IP com saída internacional com destino direto para os Estados Unidos da América (EUA) com no mínimo 100 Gbps.

Quantidade de Links	Velocidade
39	100 Mbps
1	250 Mbps
1	500 Mbps

- **SERVIÇOS DE GERENCIAMENTO DE REDE:**

Proativos (NOC – Network Operation Service) com funcionamento 24 horas por dia, 7 (sete) dias na semana, com capacidade de detecção proativa de falhas ocorridas nos circuitos (serviços e equipamentos) com permissão do acompanhamento dos registros de problemas e das ações executadas para a recuperação dos serviços com fornecimento de portal web para efetuar e acompanhar solicitações de serviço, visualizar histórico de relatórios, análises e recomendações de gerência de rede, reports periódicos e emissão de relatórios gerenciais.

- **LAN TO LAN NODE:**

Com instalação de conectividade dedicada, permanente e velocidades simétricas com 100% da capacidade contratada, entregues com acesso em Fibra Óptica com equipamentos certificado e homologados ANATEL, acordo de nível de serviços (ANS) 99,5% ao mês com tempo de reparo de até 4 horas. O Backbone está conectado a pelo menos 5 Autonomous System (AS) e pontos de troca de tráfego (PTT) no Brasil com capacidade total mínima de 200 Gbps e 2 Autonomous System (AS) e ponto de troca de tráfego (PTT) com capacidade total mínima de 100 Gbps.

Quantidade de Links	Velocidade
4	500 Mbps

ANGELONI

- **DA TECNOLOGIA SD-WAN:**

• A solução convergente é executada através de dispositivos no qual parte dos serviços poderão ser implementados diretamente pelo hardware, com a solução SD-WAN embarcada no dispositivo;
• Funcionalidade de redundância e failover para todos os acessos físicos, permitindo que quando um dos links apresentar falhas, o outro acesso ligado na estrutura assuma a transmissão dos dados;
• Balanceamento de tráfego entre os links ativos, baseado em volumetria, com roteamento inteligente para a priorização de tráfego;
• Controle de caminho automático, baseado em políticas previamente aplicadas, com recursos para comutação dinâmica dos caminhos automaticamente, selecionando o melhor caminho, no mínimo, a partir dos seguintes parâmetros, simultâneos ou não:

→ Tipo de aplicação;
→ Prioridade de negócio;
→ Banda;
→ Latência;
→ Jitter;
→ Perda de pacotes.

• Prover visibilidade fim-a-fim dos fluxos de comunicação das aplicações sobre a rede SD-WAN;
• Prover visibilidade do desempenho da rede em tempo real, baseada nas aplicações e nos parâmetros de uso de banda, perda de pacote e latência;
• Prover visualização de todas as configurações, políticas e status dos terminais da solução SD-WAN;
• Preservar todas as licenças permanentes necessárias para suportar os requisitos de SD-WAN, de modo que todas as funções sejam plenamente atendidas.
• Suporte do Técnico e do Fabricante;
• Entre outras funcionalidades inerentes à tecnologia.

Quantidades de Pontos (Hardware/Licença) Fortinet	02

- **Serviço Gerenciamento de Segurança (SOC – Security Operation Center)**

Com funcionamento 24 horas por dia, 7 (sete) dias na semana com monitoração permanente do ambiente, regras de segurança e de controle de tráfego, notificação de falhas em Rede WAN, contemplando instalação, operação e manutenção de Firewall UTM provendo proteção de rede com características de Next Generation Firewall (NGFW) para segurança de informação perimetral, que inclui: Filtro de pacote, controle de aplicação, administração de largura de banda (QoS), VPN IPSec e SSL, IPS, prevenção contra ameaças de vírus, Spyrewares e Malwares, Filtro de URL, e acesso à internet.

Quantidades de Pontos (Hardware/Licença) Fortinet	39

ANGELONI

Informamos, outrossim, que o referido serviço acima descrito, têm sido prestados dentro dos padrões de qualidade técnica exigidos, não havendo nada que possa desabonar a empresa.

Por ser verdade firmamos.

Criciúma - SC, 21 de setembro de 2022.

Nome: Jean Bitencourt
Cargo: TI
Contato: jean.bitencourt@angeloni.com.br – 48 99931-1368

Assinatura:

Email: juliost@algartelecom.com.br

Blockbit Networks Compatibility Matrix

Specifications

Model	BB 2	BB 5	BB 10	BB 30	BB 50	BB 100	BB 200	BB 500	BB 1000	BB 2000	BB 10000	BB 15000	BB 20000	BB 30000
Firewall Throughput (UDP)	3.7 Gbps	4 Gbps	6 Gbps	6 Gbps	8 Gbps	10 Gbps	15 Gbps	20 Gbps	35 Gbps	55 Gbps	80 Gbps	100 Gbps	160 Gbps	200 Gbps
Concurrent Connections	3.5 MM	4 MM	6 MM	6 MM	7 MM	8.2 MM	10.2 MM	12 MM	18 MM	22 MM	30 MM	45 MM	55 MM	70 MM
New Connections Per Second	35.000	37.000	38.000	38.000	42.000	55.000	75.000	80.000	120.000	200.000	300.000	400.000	520.000	700.000
NGFW Throughput (IMIX)[1]	150 Mbps	200 Mbps	350Mbps	350Mbps	1 Gbps	1.6 Gbps	1.8 Gbps	2 Gbps	2.8 Gbps	5 Gbps	7 Gbps	12 Gbps	20 Gbps	30 Gbps
Web Filter Throughput	300 Mbps	400 Mbps	600 Mbps	600 Mbps	1.5 Gbps	2 Gbps	3 Gbps	4 Gbps	6 Gbps	10 Gbps	12 Gbps	15 Gbps	25 Gbps	35 Gbps
SSL Inspection Throughput	100 Mbps	150 Mbps	200 Mbps	200 Mbps	750 Mbps	1 Gbps	1.2 Gbps	1.4 Gbps	2.2 Gbps	4.5 Gbps	6 Gbps	8 Gbps	12 Gbps	20 Gbps
IPS Throughput	500 Mbps	700 Mbps	1 Gbps	1 Gbps	1.5 Gbps	2 Gbps	3 Gbps	4 Gbps	6 Gbps	9 Gbps	12 Gbps	15 Gbps	23 Gbps	30 Gbps
Application Control Throughput	70 Mbps	100 Mbps	200 Mbps	200 Mbps	700 Mbps	1 Gbps	1.4 Gbps	1.6 Gbps	2 Gbps	5 Gbps	7 Gbps	10 Gbps	16 Gbps	24 Gbps
Threat Protection Throughput	100 Mbps	150 Mbps	200 Mbps	200 Mbps	500 Mbps	700 Mbps	950 Mbps	1 Gbps	1.5 Gbps	4.5 Gbps	6 Gbps	9.6 Gbps	12 Gbps	18 Gbps
IPSEC VPN Throughput (AES-256+SHA256)	250 Mbps	280 Mbps	500 Mbps	500 Mbps	1.5 Gbps	2 Gbps	3 Gbps	4 Gbps	5 Gbps	10 Gbps	15 Gbps	18 Gbps	25.6 Gbps	30 Gbps
SSL VPN Throughput (AES-256)	100 Mbps	140 Mbps	250 Mbps	250 Mbps	1 Gbps	1.5 Gbps	1.5 Gbps	1.6 Gbps	2 Gbps	6.5 Gbps	7 Gbps	8 Gbps	11 Gbps	15 Gbps
Network Interfaces (Gigabit Ethernet – RJ45)	4X	4X	4X	6X	6X	6X	8X	8X	8X	8X	8X	8X	8X	8X
Max G/W to G/W IPSEC Tunnels	10	20	50	50	200	250	300	400	500	700	1000	1500	2000	3000
Max Client to G/W IPSEC Tunnels	20	50	150	150	500	550	600	700	1000	1300	2000	3000	4000	5000
Physical characteristics	1U for Desktop	1U for Desktop	1U for Desktop	1U for Desktop	1U for Rack 19″	1U for Rack 19″	1U for Rack 19″	1U for Rack 19″	1U for Rack 19″	1U for Rack 19″	2U for Rack 19″	2U for Rack 19″	2U for Rack 19″	2U for Rack 19″

Optional

Model	BB 2	BB 5	BB 10	BB 30	BB 50	BB 100	BB 200	BB500	BB 1000	BB 2000	BB 10000	BB 15000	BB 20000	BB 30000
Solid State Drive (SSD)	64/120 GB	64/120 GB	120/240 GB	120/240 GB	240 GB	240 GB	480 GB	480 GB	480 GB	480 GB	600 GB	600 GB	2 TB	2 TB
LTE 3G/4G	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	–	–	–	–	–
RAID 0/1	–	–	–	–	–	–	–	–	–	–	Yes	Yes	Yes	Yes
40GbE Network Module - 2 QSFP + Ports	–	–	–	–	–	–	–	–	–	–	Yes	Yes	Yes	Yes
10GbE Network Module - 4 SFP + Ports	–	–	–	–	–	–	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
1GbE Network Module - 4 SFP Ports	–	–	–	–	–	–	Yes	Yes	Yes	–	–	–	–	–
1GbE Network Module - 8 SFP Ports	–	–	–	–	–	–	–	–	–	Yes	Yes	Yes	Yes	Yes
10GbE Network Module - 2 SFP + Ports With Bypass	–	–	–	–	–	–	–	–	–	–	Yes	Yes	Yes	Yes
1GbE Network Module - 4 SFP + Ports With Bypass	–	–	–	–	–	–	–	–	–	Yes	Yes	Yes	Yes	Yes
1GbE Network Module - 8 RJ45 Ports	–	–	–	–	–	–	–	–	–	Yes	Yes	Yes	Yes	Yes
1GbE Network Module - 8 RJ45 Ports With Bypass	–	–	–	–	–	–	–	–	–	Yes	Yes	Yes	Yes	Yes
10GbE Network Module - 2 SFP + Ports	–	–	–	–	Yes	Yes	–	–	–	–	–	–	–	–
1GbE Network Module - 2 SFP Ports	–	–	–	–	Yes	Yes	–	–	–	–	–	–	–	–
Redundant Power Source	–	–	–	–	–	–	–	Yes	Yes	–	–	–	–	–
Available Slots	–	–	–	–	1x	1x	1x	1x	1x	3x	7x	7x	7x	7x

All **Blockbit** models come with a power cable in the NBR 14136 standard.

[1] NGFW IS MEASURED WITH FIREWALL ENABLED, IPS AND APPLICATION CONTROL, IMIX TRAFFIC

Blockbit

Blockbit Networks Compatibility Matrix

Virtual Appliances

Model	BB 2	BB 5	BB 10	BB 30	BB 50	BB 100	BB 200	BB 500	BB 1000	BB 2000	BB 10000	BB 15000	BB 20000	BB 30000
Firewall Throughput (UDP)	3.7 Gbps	4 Gbps	6 Gbps	6 Gbps	8 Gbps	10 Gbps	15 Gbps	20 Gbps	35 Gbps	55 Gbps	80 Gbps	100 Gbps	160 Gbps	200 Gbps

Features by Subscription

Features	BASIC	STANDART	ADVANCED
Next-Generation Firewall (NGFW)	√	√	√
Secure SD-WAN	√	√	√
Proxy WEB	√	√	√
VPN IPSEC	√	√	√
VPN SSL	√	√	√
QoS	√	√	√
Cluster	√	√	√
Captive Portal	√	√	√
DHCP server/relay	√	√	√
Hardware Warranty	√	√	√
URL Category Base	–	√	√
Intrusion Prevention System (IPS)	–	√	√
Gateway Antivirus	–	√	√
Threat Protection	–	√	√
Remote Support - 04 hours / month	–	–	√

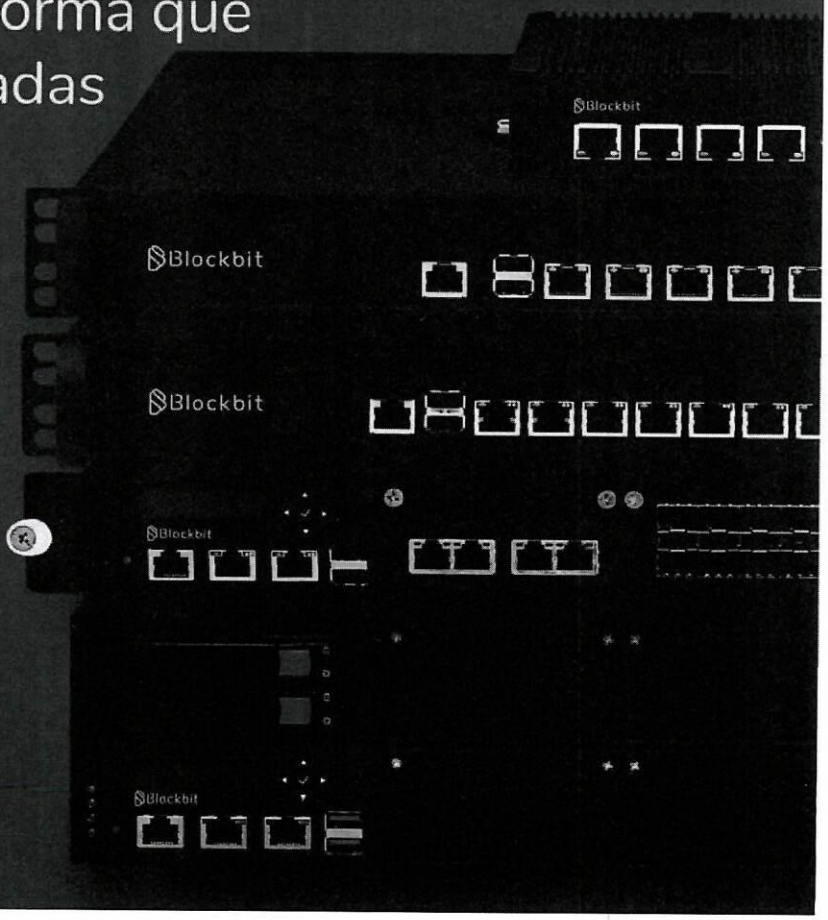
TESTS WERE CARRIED OUT IN LABORATORY USING IXIA BREAKINGPOINT IN, BLOCKBIT PLATFORM 2.0, IPS AND SERVICES, DISABLED APPLICATION DETECTORS, FIREWALL THROUGHPUT UDP 1518 BYTES PACKAGES, FIREWALL THROUGHPUT HTTP GET 1280 Kb AND PUT 1280 K, IPS / ATP THROUGHPUT WITH STANDARD FACTORY SUBSCRIPTIONS ENABLED, WITHOUT SUMMARIZATION BY USERS.

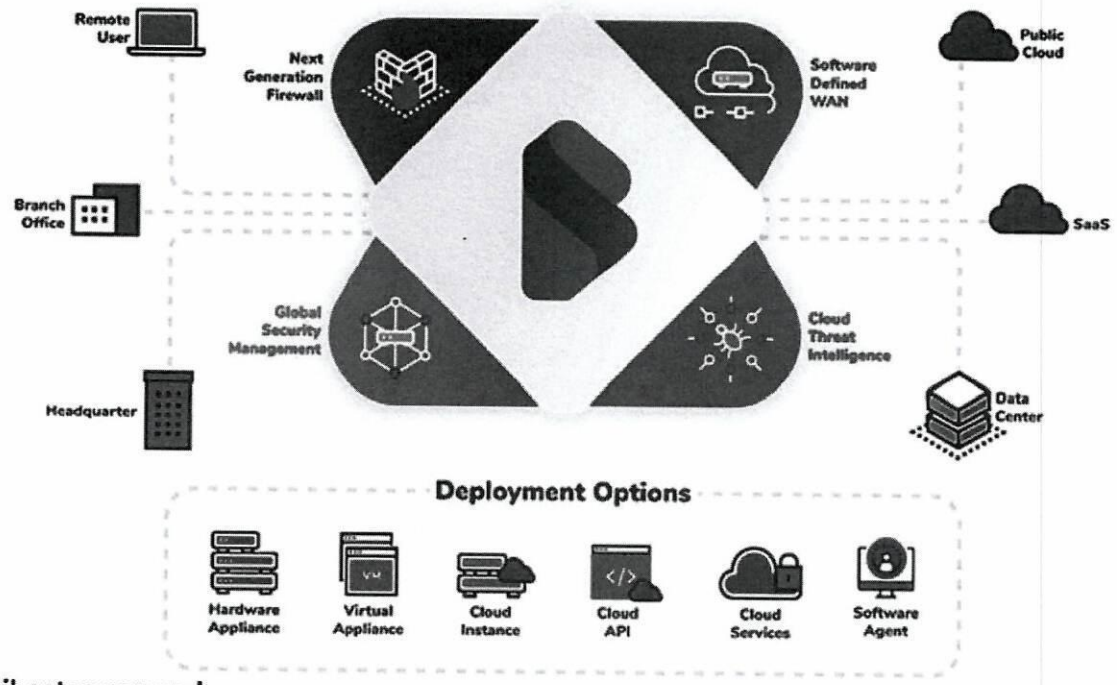
Blockbit

Blockbit Platform 2.4.0

É fácil estar seguro!

Proteja a arquitetura da sua rede com uma única plataforma que integra diversas camadas de segurança digital, sem custo de módulos adicionais.





É fácil estar seguro!

Proteja a arquitetura da sua rede com uma única plataforma que integra diversas camadas de segurança digital, sem custo de módulos adicionais.

Como fabricante global de cibersegurança, a **Blockbit oferece** uma plataforma de gestão unificada e abrangente à todas as empresas. **A Blockbit Platform** foi desenvolvida especificamente para ser um Firewall com total integração para facilitar o gerenciamento e a usabilidade do usuário final. O sistema operacional é desenvolvido pela Blockbit para garantir estabilidade e o melhor desempenho, com o que há de mais novo no mercado, nossas soluções integradas protegem todo o perímetro de rede e suas redes distribuídas.

Alterações na solução de ATP ou quaisquer outras apenas impactam no recurso alterado sem interferir nas demais regras de segurança.

Permite configuração totalmente transparente para o usuário final e usuários externos, sem a necessidade de configuração de proxies, rotas estáticas e qualquer outro mecanismo de redirecionamento de tráfego;

Plataforma integrada da cibersegurança: dinâmica, moderna e funcional;

- Configure políticas de segurança, implemente recursos e ative múltiplos dispositivos automaticamente com o Zero-touch;
- Identifique e bloqueie intrusos e aplicações suspeitas antes mesmo que entrem em sua rede;
- Simplifique a gestão e a proteção de redes, usuários, conexões e múltiplos ativos;
- Bloqueie ataques sofisticados e ameaças avançadas a partir de uma única plataforma;
- Controle navegação web e promova mais produtividade para sua equipe;
- Defina políticas de segurança, conformidade e níveis de acesso;
- Habilite comunicação entre dispositivos remotos com sua rede de forma segura e criptografada.

DESTAQUES

Controle e Roteamento Avançado de Aplicações:
Gerencie facilmente o acesso à Aplicações Web como Facebook, LinkedIn, Google, Twitter, Dropbox, entre outros.

Proteção Avançada Contra Ameaças:
Segurança inovadora contra malware avançado e call-back.

Gerenciamento Centralizado:
Gerencie facilmente múltiplos dispositivos com o Blockbit GSM (Global Security Management), que tem integração nativa com o Blockbit Next-Generation Firewall.

Decodificação de Protocolo
Capaz de detectar aplicações encapsuladas e validar se o tráfego corresponde com a especificação do protocolo. O recurso também identifica funcionalidades específicas dentro de uma aplicação.

Atualizações Transparente:
As atualizações automáticas de patches de correções e subscriptions são transparentes para o cliente sem causar interrupção na rede. Possui ferramenta com os hotfixes de segurança e upgrade simplificado e sem interrupção do ambiente.

Reduza o custo e o tempo na implementação:
Centralize configurações e as distribua automaticamente para os ativos remotos. Com o recurso ZTP (Zero-Touch Provisioning) é possível reduzir tempo e custo com a implementação.

Principais Recursos

Next-Generation Firewall
A Blockbit Platform é muito mais que um firewall. Unindo a mais avançada tecnologia de gestão de redes à capacidade avançada de detecção e proteção contra ataques e ameaças digitais. O Blockbit NGFW (Next-Generation Firewall) simplifica a criação de políticas e regras de segurança complexas, podendo ser implementado como gateway ou inline, otimizada para análise de conteúdo de aplicação na camada 7, utilizando endereços, usuários, grupos de usuários, aplicações, ameaças e serviços em suas configurações, que podem ser nomeados para facilitar a compreensão das políticas e garantir controle total do seu ambiente. Possibilita a criação de regras de saída de rede baseado em endereço IP e faixa de rede de origem, endereço IP e faixa de rede de destino e porta de destino. O licenciamento é de uso perpétuo para todos os recursos NGFW, SD-WAN, App control e stateful firewall. Suporta VDOM (Virtual Domain) em todos os modelos de hardware. Suporta criar políticas de bloqueio ou liberação por geolocalização e informam nos logs o país de origem e/ou destino com a bandeira para facilitar a identificação do tráfego.

Zero-Touch Provisioning
Com o recurso ZTP (Zero-Touch Provising) é possível pré-configurar as políticas de segurança e implementá-las automaticamente no dispositivo remoto vinculado, assim que receber uma conexão de rede. Isso reduz a complexidade da instalação e, consequentemente, a economia de recursos financeiros e técnicos.

Inspeção SSL
A maioria das informações que trafegam na web usam conexões criptografadas. A Blockbit Platform conta com descriptografia de SSL para inspeção de tráfego de saída (Outbound), garantindo o controle total de acesso e aplicando recursos avançados, como ATP, Filtro de Conteúdo, Controle de Aplicação e Antimalware. Suporta TLS 1.2 e TLS 1.3. Suporta aplicação de políticas de segurança e visibilidade para as aplicações que circulam

Filtragem de Conteúdo

A Blockbit Platform possui milhões de endereços classificados em categorias específicas. Estas informações, em conjunto com a inspeção SSL, permitem controlar totalmente o acesso ao conteúdo online e na visibilidade, o que pode ser configurado por usuário, grupos de usuários, (AD ou base local) IPs, largura de banda, prioridade de conexão, links, diferentes navegadores e suas versões. Você também pode determinar limites para tamanho de arquivos para download e upload, execução de aplicações web, tempo permitido de navegação e muito mais. Permite a filtragem de arquivos e dados pré-definidos, controle de arquivos compactados e aplicar politicas no conteúdo destes.

Controle de Aplicações

O avanço da Internet permitiu a criação de aplicações como Facebook, Youtube, Google Apps, Twitter, LinkedIn e Dropbox, que se tornaram muito populares e podem impactar a produtividade de suas equipes se não utilizadas corretamente. A Blockbit Platform permite que você controle totalmente as Aplicações Web (podendo bloquear, limitar e aplicar controle de QoS) executadas com integração a diversos métodos de autenticação, restringindo ou permitindo acesso de acordo com as regras do seu negócio. Suporta controlar o uso de aplicativos por políticas e grupos estáticos de aplicações. A Blockbit é capaz de reconhecer aplicações independemente de porta e protocolo, portanto é possível [illegible]rar a aplicação sem precisar liberar porta e/ou protocolos. Identifica o uso de táticas evasivas para controlar aplicações que tentam usar conexão criptografadas (por exemplo Skype ou rede TOR).

IPS - Sistema de Prevenção de Intrusos

A Blockbit Platform protege continuamente sua rede contra o número crescente de ameaças digitais. O IPS conta com milhares de assinaturas para identificação de ameaças em um banco de dados atualizado diariamente. É possível criar múltiplos perfis de proteção para aplicá-los em diferentes tipos de tráfego de rede. Além disto, o dashboard exibe informações sobre as ameaças detectadas de maneira detalhada, permitindo uma rápida e eficiente análise de risco. São suportados as seguintes proteções: Permite analisar e gerar logs, bloqueia e envia para quarentena o IP do atacante por um período de tempo.

ATP - Proteção Avançada Contra Ameaças (Antívirus e Anti-Spyware)

A Blockbit Platform conta com tecnologias sofisticadas de segurança e inteligência que detectam e protegem sua empresa contra ameaças conhecidas e desconhecidas, inclusive em tráfego SSL. A Blockbit Platform pode detectar malware avançados como trojans e vírus, ameaças persistentes avançadas e ataques de callbacks maliciosos. O ATP também pode bloquear IPs com má reputação em diferentes categorias (abusers, anonymizers, attackers, malware, spam) além de ataques por geolocalização. Bloqueia arquivos pela extensão e também indentifica pelo tipo MIME (mesmo mudando a extensão).

VPN SSL e IPSec

A Blockbit Platform permite criar acesso seguro às aplicações de sua rede através de um portal web que pode ser configurado rapidamente e executado em qualquer navegador. A plataforma também suporta conexão do tipo client-to-site. A Blockbit Platform permite criar redes privadas virtuais com criptografia de tunelamento nativa, que garante a interoperabilidade com outros produtos e aumenta a segurança. Suporta arquitetura de VPN hub and spoke IPSec, tanto para topologias site-to-site como para client-to-site (remote access). Permite que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais como proxies. Crie políticas de controle de aplicações, IPS, Antivírus, Antispyware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL/IPSEC

QoS & Traffic Shapping

A Blockbit Platform conta com recurso de QoS exclusivo que permite, via interface gráfica centralizada e local, priorizar tráfego e controlar a largura de banda de acordo com as políticas de segurança e conformidades configuradas, além da classificação de pacotes (Shaping). O recurso de QoS avançado categoriza conexões de acordo com sua importância e possibilita priorizar pacotes através da marcação de DSCP e TOS. Defina banda máxima e garantida por aplicação, suporta o match em categorias de URL, IPs de origem e destino, logins e portas. Regas de QoS podem ser habilitadas por horários ou intervalo de tempo.

SD-WAN

A Blockbit Platform oferece um serviço de balanceamento dinâmico de 2 até 9 links para conexão de longa distância, que permite conectar a sua empresa a qualquer local – filiais, datacenters, nuvem etc. Suporta interface física, sub-interfaces VLAN e IPSec. Suporta conexões WAN: ADSL/DSL, Cable Modem com Ethernet ou fibra, LT /3G/4G/5G, MPLS, Link de rádio e Link satélite (a terminação da conectividade deve permitir conectividade com interfaces ethernet).

Você tem mais visibilidade sobre todas as atividades em qualquer local e ainda integra o SD-WAN com todos os recursos de segurança da Blockbit, podendo gerenciar todo o ambiente a partir de uma única interface, facilitando a análise de resultados e a tomada de decisões sobre otimizações na rede, em localidades remotas, proporcionando visibilidade do tráfego, seleção de caminho dinâmico baseado em políticas de QoS, aplicação ou performance e utilização de túneis VPN para comunicação entre os sites remoto. Os appliances Blockbit possuem entrada USB compatível com modem 3G/4G permitindo que o link WAN seja utilizado nas regras de SD-WAN. Suporta o roteamento por aplicação. Permite escolher o melhor link, menor custo e definição de níveis máximos de qualidade a serem aceitos para que tais links possam ser utilizados em um determinado roteamento de aplicação. Utilize VPN IPSec para balancear o tráfego por round robin na agregação de tráfego e definição de peso de cada túnel.

Alta Disponibilidade

A Blockbit Platform tem suporte nativo a implementações H.A. (high availability). O recurso mantém um appliance em modo backup, que entra em operação imediatamente caso o appliance primário sofra uma falha. Tamém suporta monitorar se ocorre falha no link. O suporte H.A. espelha sessões de firewall, autenticação de usuário e sincroniza todas configurações, seções, certificados para Inspenção SSL, SA (Associações de Segurança) de VPN IPSsec e todas as assinaturas de ATP, Application Control, IPS e WEB Filter, entre os dispositivos primário e secundário para que o switch over seja transparente e rápido.

Captive Portal

A Blockbit Platform facilita o gerenciamento do acesso de visitantes por meio da autenticação que o navegador web utiliza. O Captive Portal permite auto registro, personalização de políticas de acesso, controle de conteúdo, gestão de usuários, troca de senhas de acesso e relatórios personalizados. Além disso, é possível autenticar via contas de mídias sociais (Facebook, Google e Twitter), Windows AD, LDAP e RADIUS.

Gerenciamento Centralizado

O Blockbit NGFW tem integração nativa com o GSM (Global Security Management), que possibilita gerenciar múltiplos dispositivos, com conexão criptografada e autenticada por meio de um ponto central. Permite o gerenciamento centralizado e local das funcionalidades de Políticas de encaminhamento, Proxy WEB, IPS/IDS e Antimalware, monitorando seus eventos de forma integrada. Suporta envio automático dos logs para servidor externo por NFS. Dashboards customizados para visibilidades do tráfego de aplicativos, categorias de URL, ameaças, serviços, origem e destino. Página com Indicador de Comprometimento. Usuários com utilização web suspeita: endereço IP do terminal do usuário, hostname, sistema operacional, veredito (classificação geral de ameaça) e número de ameaças detectadas.

Recursos Habilitados*

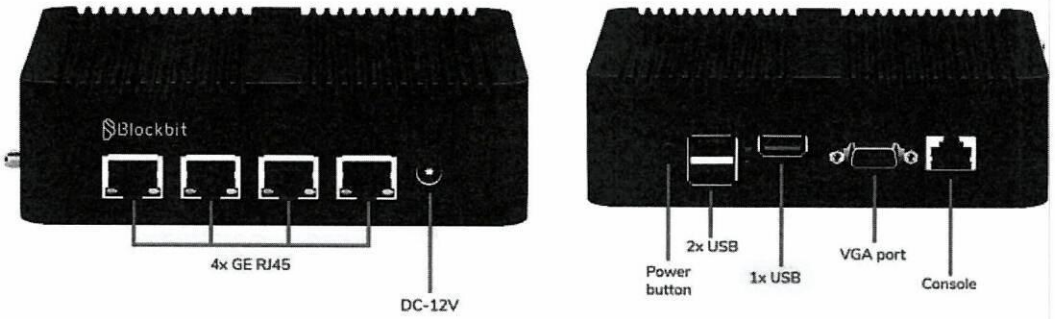
Features	Basic	Standard	Advanced
Next-Generation Firewall (NGFW)	✓	✓	✓
Secure SD-WAN	✓	✓	✓
Proxy WEB	✓	✓	✓
VPN IPSEC	✓	✓	✓
VPN SSL	✓	✓	✓
QoS	✓	✓	✓
Cluster	✓	✓	✓
Captive Portal	✓	✓	✓
DHCP SERVER/RELAY	✓	✓	✓
Garantia de Hardware	✓	✓	✓
Base de Categoria de URL		✓	✓
Intrusion Prevention System (IPS)		✓	✓
Antivírus de Gateway		✓	✓
Threat Protection		✓	✓
Suporte Remoto - 04 horas mês			✓

*LICENCIAMENTO DOS EQUIPAMENTOS DA BLOCKBIT NÃO LIMITA A QUANTIDADE DE USUÁRIOS, EQUIPAMENTO E/OU FUNCIONALIDADE.

MODELOS EQUIPAMENTOS

Pequenas Empresas

MODELO: BB2 | BB5 | BB10



Especificações de Desempenho e Opcionais

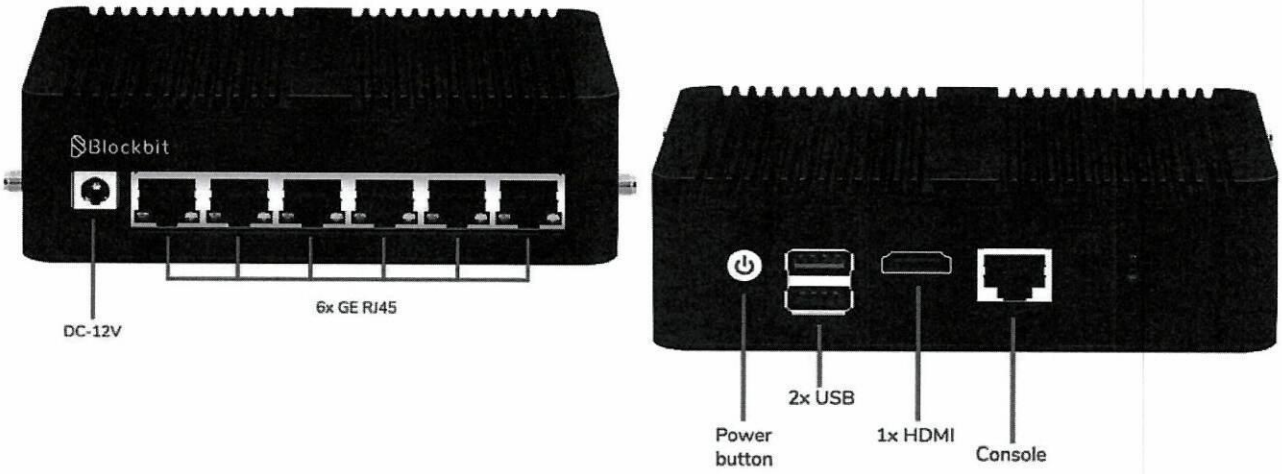
	BB2	BB5	BB10
Firewall Throughput (UDP)	3.7Gbps	4 Gbps	6 Gbps
Conexões Simultâneas	3.500.000	4.000.000	6.000.000
Conexões Novas Por Segundo	35.000	37.000	38.000
NGFW Throughput (IMIX)[1]	150 Mbps	200 Mbps	350Mbps
Web Filter Throughput	300 Mbps	400 Mbps	600 Mbps
SSL Inspection Throughput	100 Mbps	150 Mbps	200 Mbps
IPS Throughput	500 Mbps	700 Mbps	1 Gbps
Application Control Throughput	70 Mbps	100 Mbps	200 Mbps
Threat Protection Throughput	100 Mbps	150 Mbps	200 Mbps
IPSEC VPN Throughput (AES-256 + SHA256)	250 Mbps	280 Mbps	500 Mbps
SSL VPN Throughput (AES-256)	100 Mbps	140 Mbps	250 Mbps
Interfaces de Rede	4 X GE RJ45	4 X GE RJ45	4 X GE RJ45
Armazenamento	32 GB	32 GB	32 GB
Característica Física / Alimentação	1U p/ Desktop / DC 100-220V AC, 50-60hz		
Dimensões (Largura x Profundidade x Altura)	230mm x 300mm x 46mm		
Temperatura Ideal de Operação	-10°C (14 °F) ~ 60°C (140 °F)		

Opcionais

Unidade de Estado Sólido (SSD)	64/120 GB	64/120 GB	120/240 GB
LTE 3G/4G	Sim	Sim	Sim

Médias Empresas

MODELO: BB30



Especificações de Desempenho e Opcionais

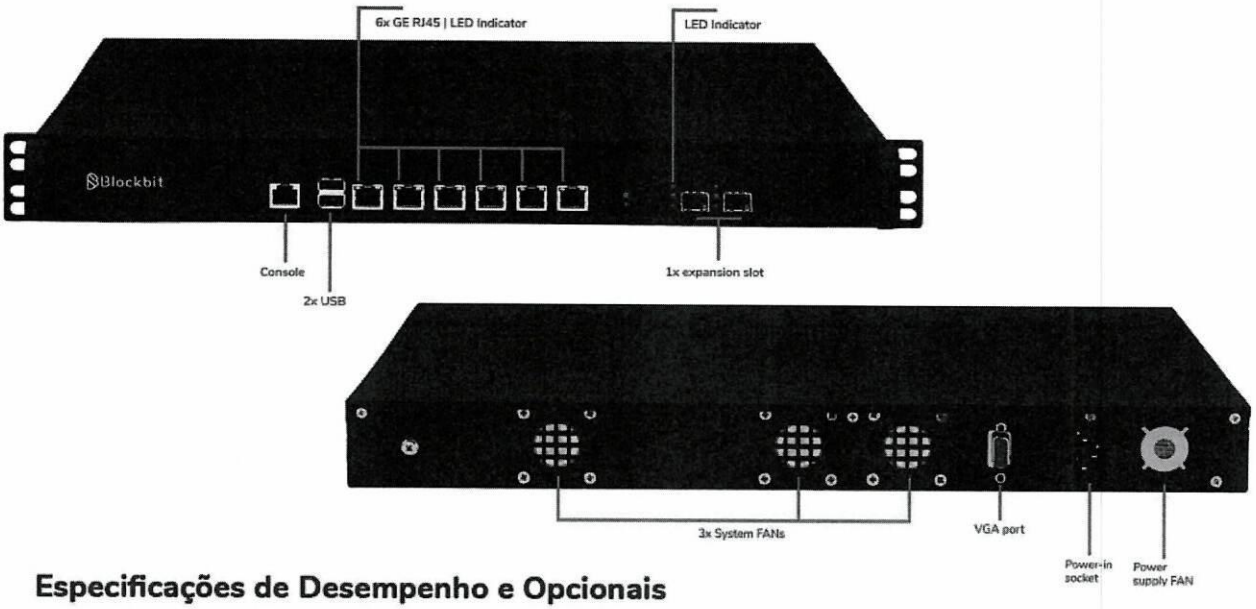
	BB30
Firewall Throughput (UDP)	6 Gbps
Conexões Simultâneas	6.000.000
Conexões Novas por Segundo	38.000
NGFW Throughput (IMIX)[1]	350 Mbps
Web Filter Throughput	600 Mbps
SSL Inspection Throughput	200 Mbps
IPS Throughput	1 Gbps
Application Control Throughput	200 Mbps
Threat Protection Throughput	200 Mbps
IPSEC VPN Throughput (AES-128 + SHA256)	500 Mbps
SSL VPN Throughput (AES-128)	250 Mbps
Interfaces de Rede	6X GE RJ45
Armazenamento	32 GB
Característica Física	1U para Desktop
Dimensões (Largura x Profundidade x Altura)	230mm x 300mm x 46mm
Temperatura Ideal de Operação	-10°C (14 °F) ~ 60°C (140 °F)

Opcionais

Unidade de Estado Sólido (SSD)	120/240 GB
LTE 3G/4G	Sim

Grandes Empresas

MODELO: BB50 | BB100



Especificações de Desempenho e Opcionais

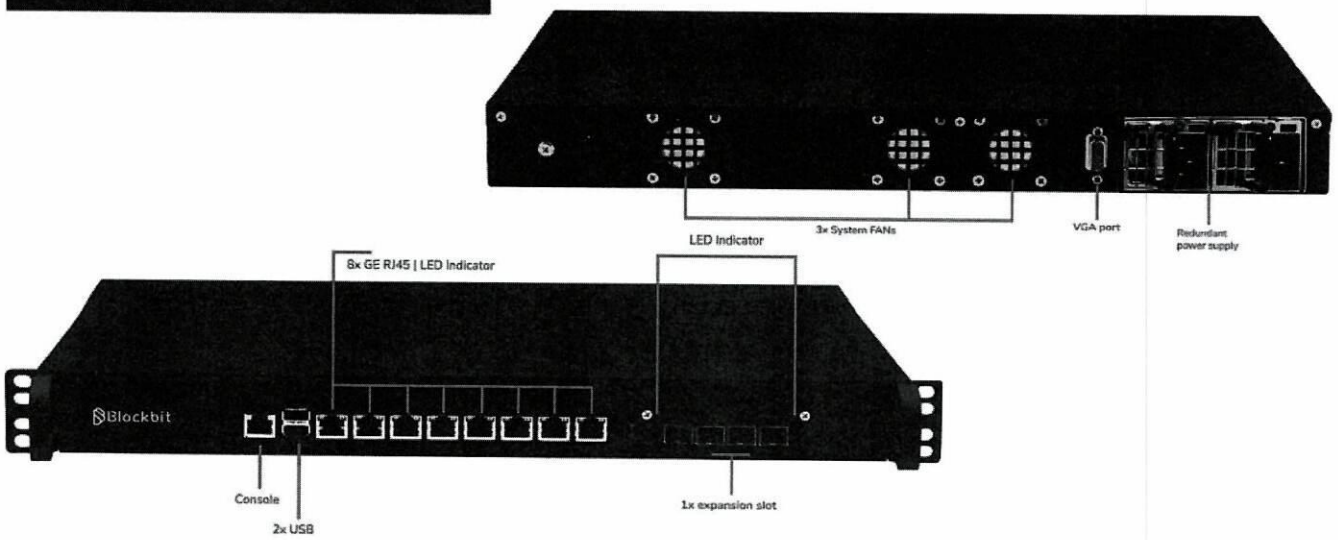
	BB50	BB100
Firewall Throughput (UDP)	8 Gbps	10 Gbps
Conexões Simultâneas	7.000.000	8.200.000
Conexões Novas Por Segundo	42.000	55.000
NGFW Throughput (IMIX)[1]	1 Gbps	1.6 Gbps
Web Filter Throughput	1.5 Gbps	2 Gbps
SSL Inspection Throughput	750 Mbps	1 Gbps
IPS Throughput	1.5 Gbps	2 Gbps
Application Control Throughput	700 Mbps	1 Gbps
Threat Protection Throughput	500 Mbps	700 Mbps
IPSEC VPN Throughput (AES-256 + SHA256)	1.5 Gbps	2 Gbps
SSL VPN Throughput (AES-256)	1 Gbps	1.5 Gbps
Interfaces de Rede	6 X GE RJ45	6X GE RJ45
Armazenamento	120 GB	120 GB
Característica Física	1U para Rack 19″	1U para Rack 19″
Alimentação	100-240V AC	
Dimensões (Largura x Profundidade x Altura)	380mm x 430mm x 46mm	
Temperatura Ideal de Operação	-20 °C (-4 °F) ~ 70 °C (158 °F)	

Opcionais

Unidade de Estado Sólido (SSD)	240 GB	240 GB
LTE 3G/4G	Sim	Sim
Módulo Rede 10GbE - 2 portas SFP+	Sim	Sim
Módulo Rede 1GbE - 2 portas SFP	Sim	Sim
Slots disponíveis	1x	1x

Grandes Empresas

MODELO: BB200



Especificações de Desempenho e Opcionais

	BB200
Firewall Throughput (UDP)	15 Gbps
Conexões Simultâneas	10.200.000
Conexões Novas Por Segundo	75.000
NGFW Throughput (IMIX)[1]	1.8 Gbps
Web Filter Throughput	3 Gbps
SSL Inspection Throughput	1.2 Gbps
IPS Throughput	3 Gbps
Application Control Throughput	1.4 Gbps
Threat Protection Throughput	950 Mbps
IPSEC VPN Throughput (AES-256 + SHA256)	3 Gbps
SSL VPN Throughput (AES-256)	1.5 Gbps
Interfaces de Rede	8X GE RJ45
Armazenamento	120 GB
Característica Física	1U para Rack 19″
Alimentação	100-240 AC
Dimensões (Largura x Profundidade x Altura)	380mm x 430mm x 46mm
Temperatura Ideal de Operação	-20 °C (-4 °F) ~ 70 °C (158 °F)

Opcionais

Unidade de Estado Sólido (SSD)	240 GB
LTE 3G/4G	Sim
Módulo Rede 10GbE - 2 portas SFP+	Sim
Módulo Rede 1GbE - 2 portas SFP	Sim
Fonte Redundante - Hot Swappable 110~240VAC, 60 Hz	Sim
Slots disponíveis	1x