Atributo		Descrição	Limitadores Implantação	Planos			
				SD-WAN Básico	SD-WAN Seguro	SD-WAN Super Seguro	GerSec Avançado
SOC	**Gerenciamento**	O serviço de gerenciamento conta com o monitoramento de rede e uma equipe especializada, disponível 24h, conferindo agilidade e prontificada para levar soluções sob medida para o negócio.					
	Monitoramento proativo	À partir do identificação de um evento em nossa plataforma de monitoramento centralizada, dá-se início a investigação do mesmo. Confirmado um incidente, um chamado é aberto e o cliente notificado.					
	Tratativa de incidente	Mediante um incidente de segurança, o SOC deve prover o diagnóstico e dar início a tratativa. **SLA: 4h**					
	Programação de serviço	Qualquer alteração de configuração não relacionada à incidente. **SLA: 24h úteis**					
	Suporte do fornecedor	Licença de suporte técnico com o fornecedor, 24h por dia, para todos os dispositivos em operação.					
	Relatório	Disponibilizado mensalmente, podendo ser personalizado de acordo com os parâmetros abaixo.					
	Consumo de banda	Top 10 Usuários/origens por consumo de banda e sessões; Top 10 Destinos por consumo de banda; Top 10 *Websites* por consumo de banda; Top 10 Aplicações por consumo de banda; Top 10 Categorias aplicações por consumo de banda.		✘	✘		
	Tráfego bloqueado	Top 10 Categorias de *websites* acessados, por exemplo: rede social, *streaming* e P2P; Top 30 *Websites* visitados; Top 10 *Websites* bloqueados; Top 10 Bloqueio de acesso por usuário (os usuários mais bloqueados); Top 10 Categorias bloqueadas (os tipos de *websites* mais bloqueados); Top 20 Aplicações bloqueadas.		✘	✘		
	Vulnerabilidades identificadas	Listagem de *malwares*: vírus, *botnet*, *spyware* e *adware* identificados; Frequência de bloqueio por ataque de *botnet*; Listagem de terminais infectados por *botnet*; Listagem de aplicações de alto risco; Top 10 *malwares*.		✘	✘		
Dispositivo	**Múltiplos formatos**	Os equipamentos disponíveis possuem diferentes dimensões físicas ou características como: a quantidade de interfaces e fontes de alimentação. Por exemplo, alguns são de mesa (*desktop*), de pequeno porte, outros são próprios para bastidores (*rack*) e alguns podem ser modelos virtualizados. Estes parâmetros estão relacionados ao pacote do produto.					
	Pacote 1	*Hardware* FortiGate modelo FG-30E - *desktop*					
	Pacote 2	*Hardware* FortiGate modelo FG-60E - *desktop*					
	Pacote 3	*Hardware* FortiGate modelo FG-100E - 1 *Rack Unit* (RU)					
	Pacote 4	*Hardware* FortiGate modelo FG-200E - 1 *Rack Unit* (RU)					
	Virtual	*Software* FG-VM00 compatível com o *hypervisor* VMware.					
	*Public Cloud**	AWS e Azure * Sujeito a viabilidade e aprovação do projeto técnico.					
	Redundância	Para as localidades que possuem baixa tolerância à indisponibilidade, o produto prevê duas modalidades: alta disponibilidade e *spare*. Premissa: os dispositivos devem ser do mesmo modelo.					
	Alta disponibilidade (HA)	É criado um *cluster* com dois (2) dispositivos: um em modo ativo e outro passivo, em *standby*. Apenas o dispositivo ativo processa os pacotes e responde a ARP, por exemplo. Em caso de falha, a comutação entre os elementos ocorre em subsegundo e de forma *stateful*, preservando as sessões ativas.					
	Sobressalente *(spare)*	O dispositivo sobressalente é mantido armazenado na localidade e, mediante a necessidade de troca, este equipamento é instalado, configurado e licenciado. Como apenas um dispositivo é licenciado, há um menor custo com licenciamento.					
	Múltiplos acessos	Independente do provedor de acesso local, seja Algar Telecom ou terceiros.					◑

	Atributo	Descrição	Limitadores Implantação	Planos			
				SD-WAN Básico	SD-WAN Seguro	SD-WAN Super Seguro	GerSec Avançado
SD-WAN	Interface de acesso	Independente do meio de transporte como: banda larga, internet dedicada, MPLS. Obs.: ao menos um dos *links* deve prover acesso à internet, para a efetiva gestão da Algar Telecom, e as interfaces devem suportar o padrão Ethernet.	4 interfaces físicas ou virtuais (VLAN).				
	3G/4G LTE*	Acesso via rede móvel (celular). * Sujeito a viabilidade e aprovação do projeto técnico. Obs.: A Algar Telecom possui o modelo de modem USB D-Link DWM-157 (sem suporte ao 4G).	1 interface USB.				✘
	SL*A monitor (health-check*)	Monitoramento dos seguintes indicadores dos *links*: latência, *jitter*, perda de pacotes, utilização de banda e disponibilidade.	8 *probes* de monitoramento.				✘
	Rede virtual	Comunicação privada e encriptada entre as unidades de negócio, garantindo a confidencialidade e integridade dos dados utilizando-se de todos os *links* ativos. Obs.: unidades de negócio são localidades que possuem o produto SD-WAN da Algar Telecom.					
	Topologia *hub-and-spoke*	O roteamento do tráfego entre as unidades de negócio se dá por 1 ou 2 concentradores (*hubs*) instalados na infraestrutura do cliente, por exemplo, na matriz e/ou data center.	2 *hubs*.				✘
	Modo de navegação à internet	Basicamente a navegação pode ser realizada de três (3) modos: direto, indireto ou misto.		◑			◑
	Direto	A navegação direta à internet, também conhecida como *Local Internet Breakout* ou *Direct Internet Access* (DIA), permite que este tipo de tráfego seja roteado diretamente para o provedor local sem transitar pelo ponto concentrador, reduzindo a latência e melhorando a experiência do usuário.	1 modo de navegação.				
	Indireto	Na navegação indireta, o tráfego é roteado até o ponto concentrador, centralizando o controle e reduzindo a necessidade de segurança adicional nas demais unidades (*spokes*).					✘
	Misto	O modo misto é a combinação do modo direto e indireto. Assim, é possível criar regras de encaminhamento distintas para diferentes segmentos de rede ou aplicação.		✘			✘
	Balanceamento de tráfego	O algoritmo de balanceamento padrão do tráfego de rede pode ser definido em 4 categorias.					◑
	Failover	A prioridade das interfaces é atribuída manualmente e a comutação ocorre de forma automática em caso de falha do *link* principal.	1 modo de balanceamento.				
	IP de origem	O tráfego é distribuído igualmente entre todas as interfaces, porém sessões com o mesmo IP de origem utilizam a mesma rota.					✘
	Número de sessões	O tráfego é distribuído de acordo com o número de sessões em cada interface, porém sessões com o mesmo IP de origem e destino utilizam a mesma rota.					✘
	Volumétrico	O tráfego é distribuído de acordo com a banda consumida em cada interface, porém sessões com o mesmo IP de origem e destino utilizam a mesma rota.					✘
	Roteamento inteligente	Possibilita a criação de regras para melhor *performance* das aplicações e otimização dos *links*.					
	Baseado em aplicação	Definição de regras de encaminhamento baseado em: endereçamento IP (L3), serviço (L4) ou aplicação (L7) para priorização e *traffic shaping*. Suporte à milhares de protocolos, serviços e aplicações como: Dropbox, Office 365 e YouTube.	5 regras.	✘			✘

	Atributo	Descrição	Limitadores Implantação	Planos			
				SD-WAN Básico	SD-WAN Seguro	SD-WAN Super Seguro	GerSec Avançado
	Traffic shaping	Limitar e/ou reservar uma quantidade de banda para uma determinada regra de encaminhamento.	5 perfis.	✘			✘
	Priorização (QoS)	Classificação de pacotes em filas (*queues*) de alta, média e baixa prioridade e marcação de pacotes via DSCP. RFC 2474: Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers RFC 2475: An Architecture for Differentiated Services	5 perfis.	✘			✘
	Portal centralizado	Portal centralizado para consultas e monitoramento dos dispositivos, verificar a saúde dos *links* e histórico de eventos.	3 usuários.				◑
	Visibilidade do dispositivo	Acesso ao *status*, configurações e histórico de alterações do dispositivo.					
	Saúde d*o link*	*Status* e histórico dos *links* contendo informações do SLA *monitor*, dos últimos 7 dias.					✘
Rede	**Interface Ethernet**	Configurações de rede na camada 2.					
	PPPoE	Protocolo de autenticação para conexão WAN.					
	VLA*N tagging*	Padrão IEEE 802.1q.	10 interfaces VLANs.				
	Agregação Ethernet (LACP)	Padrão IEEE 802.1ax. Número máximo de 8 interfaces físicas por agregação.	Limitado pelo dispositivo.				
	Switch virtual	O *switch* virtual agrupa diferentes interfaces do dispositivo em um mesmo domínio de *broadcast*.	Limitado pelo dispositivo.				
	Endereçamento IP	Configurações de rede na camada 3.					
	IP estático	Configuração manual de endereçamento IP da interface.					
	DHC*P client*	Configuração de endereçamento IP da interface via DHCP, de forma automática.					
	DHC*P server*	O dispositivo atua como servidor DHCP.					
	DHC*P relay*	O dispositivo redireciona as requisições DHCP do cliente para um servidor.					
	Suporte IPv6	RFC 3315: Dynamic Host Configuration Protocol for IPv6 (DHCPv6) RFC 3633: IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6 RFC 3736: Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6					
	Roteamento	Suporte a roteamento estático e dinâmico, com os principais protocolos padrão de mercado.					
	Rota estática	Configuração manual de roteamento.	25 rotas.				
	RIP v2	RFC 2453: RIP Version 2 RFC 2080: RIPng for IPv6 RFC 4822: RIPv2 Cryptographic Authentication	1 protocolo dinâmico.				
	OSPF v2/3	RFC 2328: OSPF Version 2 RFC 3101: The OSPF Not-So-Stubby Area (NSSA) Option RFC 3623: Graceful OSPF Restart RFC 4812: OSPF Restart Signaling RFC 5340: OSPF for IPv6					
	BGP v4/6	RFC 2918: Route Refresh Capability for BGP-4 RFC 4271: A Border Gateway Protocol 4 (BGP-4) RFC 4360: BGP Extended Communities Attribute RFC 4456: BGP Route Reflection: An Alternative to Full Mesh Internal BGP (IBGP) RFC 4724: Graceful Restart Mechanism for BGP RFC 7911: Advertisement of Multiple Paths in BGP					
	BFD	RFC 5880: Bidirectional Forwarding Detection (BFD)					

				Planos			
Atributo		**Descrição**	**Limitadores Implantação**	**SD-WAN Básico**	**SD-WAN Seguro**	**SD-WAN Super Seguro**	**GerSec Avançado**
NGFW	***Firewall* de aplicação**	Protege o perímetro de rede inspecionando o tráfego até a camada 7 (aplicação).					
	Políticas de segurança	As *policies* definem como se dá o controle do tráfego de rede, aplicando ações como: permitir, descartar, limitar o fluxo e/ou gerar *logs* das sessões.	100 políticas.	✘			
	Objeto de endereço	Objeto associado aos elementos de rede como: *host*, *subnet*, *range*, FQDN ou país.	200 objetos.	✘			
	Objeto de serviço	O serviço pode ser associado a uma porta de origem e/ou destino dos protocolos de transporte TCP, UDP ou SCTP.		✘			
	Objeto de grupo	Agrupamento de um ou mais objetos de endereço ou serviço.		✘			
	Central NAT	A tabela NAT permite definir e controlar a tradução dos endereços. Com esta tabela, pode-se definir regras para o tráfego entrante (*ingress*) e sainte (*egress*).	25 regras.	✘			
	*Syslog** (quebra de sigilo)	Encaminhamento dos *logs* de sessão e autenticação do usuário para um servidor de *syslog*, geralmente, utilizados para quebra de sigilo na intranet. * Servidor de *syslog* administrado pelo cliente.	1 servidor.	✘			
	Gerenciamento de usuário	O controle de acesso pode ser realizado por usuários locais ou pela integração com um servidor de Active Directory (AD), por exemplo.		◑			
	Usuário local	Configuração de usuário local para uso em perfis ou grupos de acesso.	25 usuários.				
	LDAP, RADIUS ou SMB	Integração com servidor LDAP, RADIUS ou Samba (SMB) para validação de acesso.	1 servidor.				
	Grupo de autenticação	Os usuários, sejam locais ou do AD, podem ser inseridos dentro de um grupo de usuários. Posteriormente, este grupo pode ser aplicado a uma política de segurança ou de acesso a VPN, por exemplo.	5 grupos.				
	Certificado	Autenticação via certificado digital, sendo recomendado utilizar um certificado válido.	1 certificado.				
	Autenticação multifator*	Geração de *token* via *software* para aplicativo iOS ou Android. * Licenciamento à parte.	Limitado pela licença.	✘			
	VPN SSL (*client-to-site*)	Tecnologia para conexão do usuário final à rede corporativa (ambiente interno) pela internet via um terminal como: computador, *smartphone, tablet*, etc.					
	Protocolo TLS/SSL	RFC 6347: Datagram Transport Layer Security Version 1.2					
	Split tunnel	Habilita a navegação de internet, dos usuários remotos, localmente, ou seja, o tráfego não é roteado até o concentrador de VPN.					
	Protocolo IPsec	RFC 2409: The Internet Key Exchange (IKE) RFC 3706: A Traffic-Based Method of Detecting Dead Internet Key Exchange (IKE) Peers RFC 4303: IP Encapsulating Security Payload (ESP) RFC 4306: Internet Key Exchange (IKEv2) Protocol					
	VPN individual *(site-to-site)*	Túnel VPN (*site-to-site/gateway-to-gateway*). Obs.: qualquer VPN que não componha a rede virtual SD-WAN será cobrada à parte.	5 túneis grátis por Network. Túneis adicionais limitado pelo dispositivo.				
	Antivírus de perímetro	Inspeção do tráfego entrante na rede, utilizando base de dados do fabricante, para identificação e bloqueio de possíveis *malwares*.	2 perfis.				
	Protocolos	A varredura contra *malware* é suportada nos seguintes protocolos: HTTP, FTP, IMAP, POP3, SMTP, NNTP e MAPI.		✘	✘		
	Antispam de perímetro	Inspeção do tráfego de *e-mail* entrante na rede, utilizando a base de dados do fabricante, para bloquear *e-mails* identificados como *spam* ou que contenham ameaças.	2 perfis.				
	Protocolos	A varredura é suportada nos seguintes protocolos: SMTP, IMAP, POP3 e MAPI.		✘	✘		

				Planos			
Atributo		**Descrição**	**Limitadores Implantação**	**SD-WAN Básico**	**SD-WAN Seguro**	**SD-WAN Super Seguro**	**GerSec Avançado**
UTM	**Sistema de prevenção de intrusão (IPS/IDS)**	Sistema de Detecção e Prevenção de Intrusão (IPS/IDS) é uma tecnologia que examina os fluxos de tráfego de rede para detectar e prevenir exploração de vulnerabilidade. Essas ameaças, geralmente, apresentam-se na forma de entradas maliciosas em um aplicativo ou serviço alvo no qual os invasores usam para interromper e obter o controle sobre uma aplicação ou terminal.	2 perfis.				
	Bloqueio de *botnet*	Como parte do tráfego malicioso, a comunicação entre a *botnet* e o Comando e Controle (C&C) é identificada e bloqueada.		✘	✘		
	Controle de conteúdo	Restringe ou bloqueia o acesso a aplicativos ou a *websites*.					
	App control	Realiza o controle de aplicações a partir de *black/white list* gerada de acordo com perfis ou grupos de usuários previamente cadastrados.	5 perfis.	✘	✘		
	Web filter	Realiza o controle de acesso ao ambiente *web* via categorias de *websites* e/ou a partir de *black/white list* gerada de acordo com os perfis ou grupos de usuários previamente cadastrados. Primeira linha de defesa contra ataques baseados em *web* e no controle, monitoramento e bloqueio de *websites* indesejados ou maliciosos.	5 perfis.	✘	✘		
Versão	**FortiOS 6.2.3**	Funcionalidades associadas a este verão de software.					

ESTAÇÃO ALGAR TELECOM / CYBER SECURITY		Extras
Atributo		**Web Filter**
SOC	**Relatório**	◑
	Consumo de banda	
	Tráfego bloqueado	
	Vulnerabilidades identificadas	✘
UTM	**Controle de conteúdo**	
	Application control	
	Web filter	