DEFENSORIA PÚBLICA DO ESTADO DO RIO DE JANEIRO

PROPOSTA COMERCIAL

Rio de Janeiro – RJ, 25 de outubro de 2023

A
DEFENSORIA PÚBLICA DO ESTADO DO RIO DE JANEIRO

Objeto: CONTRATAÇÃO DE SERVIÇO CONTINUADO DE CONECTIVIDADE PARA ACESSO AO DATA CENTER E À INTERNET, UTILIZANDO LINKS SIMÉTRICOS COM SERVIÇO SD-WAN (SOFTWARE-DEFINED NETWORKING IN A WIDE AREA NETWORK), LINK DEDICADO DE ACESSO À INTERNET E LINKS ASSIMÉTRICOS DE ACESSO À INTERNET.

1) IDENTIFICAÇÃO DO LICITANTE:

Dados a constar na proposta	Preenchimento pelo proponente
Razão Social	OI SOLUÇÕES S/A
CNPJ	09.719875.0001/12
Endereço	V DR CHUCRI ZAIDAN S/N COMPLEMENTO:CONJ 191 TORREA EZ TOWERS ANEXO ARQ OLAV R CAMPOS10 BAIRRO: VILA SAO FRANCISCO (ZONASUL), São Paulo-SP
Banco:	001 - Banco do Brasil
Agencia :	3132-1
Conta Corrente:	7469-1
Telefone/Fax	(31) 98584-2207
Nome dos Representantes Legais	- Tatiana Zouain - Rosalvo Oliveira Silva Junior
Identidade do Representante Legal	- 595-180 -989034
Nacionalidade dos Representantes Legais	Brasileiros
CPF dos Representantes Legais	- 873.658.127-53 - 693.002.751-00

2.1) Prazo de validade da proposta: 60 DIAS, contados da data de abertura da sessão;

2.2) Prazo de entrega: De acordo com o Termo de Referência:

2.3) Local de entrega/execução: conforme o Termo de Referência.

3) Proposta:

LOTE	ITEM	NÚMERO DE ESTOQUE (ID SIGA)	ESPECIFICAÇÃO	UNID.	QTD	MARCA	PREÇO SEM ICMS (R$)	
							UNIT.	TOTAL
1	1	0461.001.0011 (ID - 139149)	SERVICO DE LINK DE COMUNICACAO,DESCRIÇÃO: CONTRATACAO DE EMPRESA PARA IMPLANTACAO DE LINK DE COMUNICACAO DE DADOS, INCLUINDO O FORNECIMENTO DE EQUIPAMENTOS E SUPORTE TECNICO Observação: LOTE 1 - LINK SIMÉTRICO COM SERVIÇO SD-WAN	Unid	1	Oi	11.138.885,10	11.138.885,10

ITEM	ID SIGA	ESPECIFICAÇÃO	PERÍODO	FORMA DE PAGAMENTO	MEDIDA	VELOCIDADE	QUANT.	VALOR UNITÁRIO R$	VALOR TOTAL R$	VALOR GLOBAL R$
1	0461.001.0011 (ID - 139149)	LINK SIMÉTRICO COM SERVIÇO SD-WAN	30 MESES	MENSAL	UNIDADE	20 MBPS	139	963,47	133.922,33	4.017.669,90
						30 MBPS	84	1.064,63	89.428,92	2.682.867,60
						40 MBPS	46	1.127,27	51.854,42	1.555.632,60
						60 MBPS	25	1.300,63	32.515,75	975.472,50
						80 MBPS	15	1.488,61	22.329,15	669.874,50
						100 MBPS	10	1.653,14	16.531,40	495.942,00
						200 MBPS	5	2.147,43	10.737,15	322.114,50
						300 MBPS	5	2.795,41	13.977,05	419.311,50
							Total		371.296,17	11.138.885,10

Valor Global Lote 1: R$ 11.138.885,10 (onze milhões, cento e trinta e oito mil, oitocentos e oitenta e cinco reais e dez centavos).

Obs: O montante total conquistado na licitação é de R$ 11.138.886,00. Ao realizar a distribuição entre os diversos serviços e os meses do contrato, surge uma fração/dizima periódica. Para facilitar essa distribuição sem impactar o valor final, optamos por aplicar um desconto de R$ 0,90 no montante global. Assim, o valor ajustado finaliza em R$ 11.138.885,10.

Tatiana Zouain

TATIANA ZOUAIN DUTRA DO SOUTO

Executiva de Negócios

RG: 03370641602

CPF: 873.658.127-53

DEFENSORIA PÚBLICA DO ESTADO DO RIO DE JANEIRO

Anexo D - CARACTERÍSTICAS MÍNIMAS DOS EQUIPAMENTOS SD-WAN

Rio de Janeiro – RJ, 25 de outubro de 2023

A
DEFENSORIA PÚBLICA DO ESTADO DO RIO DE JANEIRO

Objeto: CONTRATAÇÃO DE SERVIÇO CONTINUADO DE CONECTIVIDADE PARA ACESSO AO DATA CENTER E À INTERNET, UTILIZANDO LINKS SIMÉTRICOS COM SERVIÇO SD-WAN (SOFTWARE-DEFINED NETWORKING IN A WIDE AREA NETWORK), LINK DEDICADO DE ACESSO À INTERNET E LINKS ASSIMÉTRICOS DE ACESSO À INTERNET.

1) IDENTIFICAÇÃO DO LICITANTE:

Dados a constar na proposta	Preenchimento pelo proponente
Razão Social	OI SOLUÇÕES S/A
CNPJ	09.719875.0001/12
Endereço	V DR CHUCRI ZAIDAN S/N COMPLEMENTO:CONJ 191 TORREA EZ TOWERS ANEXO ARQ OLAV R CAMPOS10 BAIRRO: VILA SAO FRANCISCO (ZONASUL), São Paulo-SP
Banco:	001 - Banco do Brasil
Agencia :	3132-1
Conta Corrente:	7469-1
Telefone/Fax	(31) 98584-2207
Nome dos Representantes Legais	- Tatiana Zouain - Rosalvo
Identidade do Representante Legal	- 595-180 -989034
Nacionalidade dos Representantes Legais	Brasileiros
CPF dos Representantes Legais	- 873.658.127-53 - 693.002.751-00

CARACTERÍSTICAS MÍNIMAS DOS EQUIPAMENTOS SD-WAN

CARACTERÍSTICAS MÍNIMAS DOS EQUIPAMENTOS SD-WAN DAS SEDES E ÓRGÃOS (EXCETO DO DATACENTER)				
Interface Gigabit (1000Base-T)	Quatro Interfaces Gigabit Ethernet (1000Base-T) (uma para conectar o link do LOTE 1, uma para conectar o link do LOTE 3, rede interna da respectiva sede ou órgão da DPRJ, outros links)	Atende	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-fortiwifi-40f-series.pdf	Página 6
			https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-fortiwifi-60f-series.pdf	Página 6
			https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-fortiwifi-80f-series.pdf	Página 6
			https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-100f-series.pdf	Página 6
Throughput	Deverá possuir throughtput mínimo que suporte adequadamente os serviços de SSL inspection ou NGFW ou Application Control, para tráfego VPN e para IPS	Atende	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-fortiwifi-40f-series.pdf	Página 7
			https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-fortiwifi-60f-series.pdf	Página 7
			https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-fortiwifi-80f-series.pdf	Página 7
			https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-100f-series.pdf	Página 7

Sessões simultâneas	Deverá suportar no mínimo 50.000 (cinquenta mil) sessões de firewall simultâneas	Atende	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-fortiwifi-40f-series.pdf https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-fortiwifi-60f-series.pdf https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-fortiwifi-80f-series.pdf https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-100f-series.pdf	Página 7 Página 7 Página 7 Página 7
Funcionalidade NGFW	O equipamento deverá possuir funcionalidade NGFW (Next Generation Firewall) reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões	Atende	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf	A partir da página 5
Análise de conteúdo de aplicações	A plataforma deverá ser otimizada para análise de conteúdo de aplicações em camada 7	Atende	https://docs.fortinet.com/document/fortigate/6.0.0/handbook/240599/application-control	Sem Página
Tipo de equipamento	Deverá ser do tipo appliance, não sendo aceito equipamento do tipo servidor e com sistema operacional de uso genérico	Atende	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-fortiwifi-40f-series.pdf https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-fortiwifi-60f-series.pdf https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-fortiwifi-80f-series.pdf https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-100f-series.pdf	Página 1 Página 1 Página 1 Página 1
Funcionalidades	Anti-spoofing, configurável por segmento de rede de modo que seja possível utilizar o próprio endereçamento da interface ou especificar quais redes serão utilizadas como referência para permitir/negar o ingresso de um pacote	Atende	https://docs.fortinet.com/document/fortigate/6.0.0/handbook/178055/fortios-diagnostics	Sem Página
	Deverá permitir a configuração de ISP (rota default estática) com a utilização de probe para verificar a disponibilidade do provedor	Atende	https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/626338/adding-a-static-route	Sem Página
	A probe deve permitir verificar o acesso HTTP a pelo menos 1 (um) site web e deve considerar o ISP indisponível em caso de falha	Atende	https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/723056/link-monitoring-and-failover	Sem Página
	As funcionalidades de controle de aplicações, filtro de URLs, VPN IPSec e SSL, QoS, SSL Decryption e protocolos de roteamento dinâmico deverão operar em caráter permanente, podendo ser utilizadas durante toda a vigência do contrato	Ciente	-	-
	Policy based routing ou policy based forwarding	Atende	https://docs.fortinet.com/document/fortigate/6.0.0/handbook/34912/policy-routing	Sem Página
	Jumbo Frames	Atende	https://docs.fortinet.com/document/fortigate/6.0.0/handbook/822669/interface-mtu-packet-size	Sem Página
	Servidor DHCP em IPv4 e IPv6	Atende	https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/783526/dhcp-servers-and-relays https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/776785/dhcpv6-stateful-server	Sem Página

	Suportar IGMP, v2 e v3	Atende	https://docs.fortinet.com/document/fortigate/7.2.0/new-features/64590/configure-the-frequency-of-igmp-queries-7-2-1	Sem Página
	Permitir a administração remota, protegida por autenticação usuário/senha e utilizando pelo menos os protocolos SSHv2 e HTTPS	Atende	https://docs.fortinet.com/document/fortigate/7.2.0/new-features/936614/restrict-ssh-and-telnet-jump-host-capabilities-7-2-1 https://docs.fortinet.com/document/fortigate/7.2.0/new-features/499047/new-default-certificate-for-https-administrative-access-7-2-1	Sem Página
	Roteamento IP Multicast através do protocolo PIM nas versões 1 e 2 e nos modos Sparse Mode e Dense Mode, não sendo exigida a implementação dos dois modos de forma simultânea	Atende	https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/4afb0436-a998-11e9-81a4-00505692583a/FortiOS-6.0-Handbook.pdf	Página 1737
	Roteamento estático, OSPF, BGP e PBR (Policy Base Routing)	Atende	https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/804259/static-routing https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/479509/dynamic-routing	Sem Página
	MP-BGP, ou seja, encaminhamento de tráfego IPv4 e IPv6, ou suportar VRF	Atende	https://docs.fortinet.com/document/fortigate/6.0.0/handbook/691160/routing-concepts	Sem Página
	Cliente NTP	Atende	https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/149181/date-and-time-settings	Sem Página
	SNMP nas versões 2c e 3 com restrição dos endereços para consultas	Atende	https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/62595/snmp	Sem Página
	Protocolo de informações de fluxo como Netflow, sFlow, IPFIX ou similar	Atende	https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/998643/netflow https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/505119/sflow	Sem Página
	Gateway que contenha solução de antivírus que suporte a análise de pelo menos os protocolos HTTP, FTP, IMAP, POP3 e SMTP	Atende	https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/922423/configuring-an-antivirus-profile	Sem Página
	Suportar health check ativo, passivo e misto	Atende	https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/943037/monitoring-performance-sla https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/208103/passive-wan-health-measurement	Sem Página
Deverá suportar NAT dos seguintes tipos	NAT dinâmico (Many-to-1)	Atende	https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/188051/source-nat https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/728694/destination-nat	Sem Página
	NAT dinâmico (Many-to-Many)	Atende	https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/188051/source-nat https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/728694/destination-nat	Sem Página
	NAT estático (1-to-1)	Atende	https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/188051/source-nat https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/728694/destination-nat	Sem Página
	NAT estático (Many-to-Many)	Atende	https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/188051/source-nat https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/728694/destination-nat	Sem Página
	NAT estático bidirecional 1-to-1	Atende	https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/188051/source-nat https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/728694/destination-nat	Sem Página

	Tradução de porta (PAT)	Atende	https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/188051/source-nat https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/728694/destination-nat	Sem Página
	NAT de origem	Atende	https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/188051/source-nat https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/728694/destination-nat	Sem Página
	NAT de destino	Atende	https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/188051/source-nat https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/728694/destination-nat	Sem Página
	NAT de origem e NAT de destino simultaneamente	Atende	https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/188051/source-nat https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/728694/destination-nat	Sem Página
	Network Prefix Translation (NPTv6), NAT66	Atende	https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/627219/nat66-nat46-nat64-and-dns-64	É suportado a tradução completa por endereço (NAT66), o que entendemos ser superior a tradução apenas de prefixo (NTPv6)
Controle de política de firewall	O controle de aplicações por grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias	Atende	https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/302748/application-control	Sem Página
	Controle, inspeção e descriptografia de SSL por política para trafego de entrada (inbound) e saída (outbound)	Atende	https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/669193/ssl-based-application-detection-over-decrypted-traffic-in-a-sandwich-topology	Sem Página
	Suporte offload de certificado em inspeção de conexões SSL de entrada (inbound)	Atende	https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/669193/ssl-based-application-detection-over-decrypted-traffic-in-a-sandwich-topology	Sem Página
	Permissão de bloqueio de, pelo menos, os seguintes tipos de arquivos ou extensões: bat, cab, dll, exe, pif, e reg	Atende	https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/610893/supported-file-types	Suporta extensões do tipo bat,

				cab e exe.
	Suporte a objetos e regras multicast	Atende	https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/4afb0436-a998-11e9-81a4-00505692583a/FortiOS-6.0-Handbook.pdf	Página 617
	O agendamento de políticas em horários pré-definidos, de maneira automática	Atende	https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/656084/firewall-policy	Sem Página
	Suporte a criação de políticas com data de expiração	Atende	https://docs.fortinet.com/document/fortimanager/7.0.0/administration-guide/156162/configuring-policy-details https://docs.fortinet.com/document/fortimanager/7.0.0/administration-guide/958981/schedule-a-policy-package-install	Sem Página
Controle de aplicações	Capacidade de reconhecer aplicações, independente de porta e protocolo	Atende	https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/836937/configuring-an-application-sensor	Sem Página
	A capacidade de balancear o tráfego das aplicações entre múltiplos links, simultaneamente, incluindo portanto os links disponibilizados pelo lote de links simétricos e pelo lote de links assimétricos	Atende	https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/257828/sd-wan-components-and-design-principles	Sem Página
	Capacidade de definição de qual link será utilizado em situação normal por determinada aplicação	Atende	https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/270527/specify-an-sd-wan-zone-in-static-routes-and-sd-wan-rules	Sem Página
	Liberação e o bloqueio das aplicações, sem a necessidade de especificação de portas e protocolos	Atende	https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/243446/ngfw-policy	Sem Página
	Reconhecimento das diversas aplicações diferentes, incluindo, mas não limitado: peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, audio, vídeo, proxy, mensageria instantânea, compartilhamento de arquivos, e-mail	Atende	https://www.fortiguard.com/appcontrol	Sem Página
	Habilidade de inspecionar o payload de pacote de dados com o objetivo de detectar através de expressões regulares assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo	Atende	https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/969330/proxy-mode-inspection	Sem Página
	A capacidade de identificar o uso de táticas evasivas, ou seja, visualizar e controlar as aplicações e os ataques que utilizam comunicações criptografadas, tais como Skype e ataques utilizando a porta 443	Atende	https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/4afb0436-a998-11e9-81a4-00505692583a/FortiOS-6.0-Handbook.pdf	Páginas 919 e 920
	A capacidade de decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo, incluindo, mas não limitado a Yahoo Instant Messenger ou Whatsapp usando HTTP. A decodificação de protocolo também deve identificar funcionalidades específicas dentro de uma aplicação, incluindo, mas não limitado a, compartilhamento de arquivo dentro do Webex. Além de detectar arquivos e outros conteúdos que devem ser inspecionados de acordo as regras de segurança implementadas	Atende	https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/4afb0436-a998-11e9-81a4-00505692583a/FortiOS-6.0-Handbook.pdf	Páginas 467 e 826
	A possibilidade da liberação e do bloqueio das aplicações (ou de suas funcionalidades) por	Atende	https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/4afb0436-a998-11e9-81a4-00505692583a/FortiOS-6.0-Handbook.pdf	Páginas 919 e 920

	usuário, grupo de usuários, endereço IP ou rede específica			
	Atualização automática da base de assinaturas de aplicações	Atende	https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/4afb0436-a998-11e9-81a4-00505692583a/FortiOS-6.0-Handbook.pdf	Página 110
	A possibilidade de adicionar controle de aplicações em todas as regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras	Atende	https://docs.fortinet.com/document/fortigate/6.0.0/handbook/721617/configuring-profiles	Sem Página
	A permissão de solicitação de inclusão de aplicações na base de assinaturas de aplicações do fabricante	Atende	https://www.fortiguard.com/faq/appctrlsubmit	Sem Página
	A função de alertar o usuário quando uma aplicação for bloqueada	Atende	https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/4afb0436-a998-11e9-81a4-00505692583a/FortiOS-6.0-Handbook.pdf https://kb.fortinet.com/kb/documentLink.do?externalID=FD48878	Páginas 923 e 924
	A possibilidade de diferenciação e controle de partes das aplicações como, por exemplo, permitir o Gtalk chat mas bloquear a transferência de arquivos, permitir acesso ao Facebook mas bloquear a visualização de vídeos, permitir acesso ao WhatsApp mas bloquear a transferência de arquivos	Atende	https://www.fortiguard.com/search?q=hangouts&type=app&engine=1	Sem Página
	A possibilidade de diferenciação de aplicações Proxies (ghostsurf, freegate, ultrasurf, tor, etc) possuindo granularidade de controle/políticas para os mesmos	Atende	https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/243446/ngfw-policy	Sem Página
	A possibilidade da criação de grupos estáticos de aplicações e grupos dinâmicos de aplicações baseados em características das aplicações como: tecnologia utilizada nas aplicações (client-server, browser based, network protocol, etc), nível de risco da aplicação, aplicações que usem técnicas evasivas, utilizadas por malwares, como transferência de arquivos e/ou uso excessivo de banda, etc	Atende	https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/19814/basic-category-filters-and-overrides	Sem Página
Controle de prevenção de ameaças	Módulo de IPS integrado no equipamento	Atende	https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/565562/intrusion-prevention	Sem Página
	Assinaturas de prevenção de intrusão (IPS)	Atende	https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/213498/signature-based-defense	Sem Página
	A sincronização das assinaturas de IPS quando implementado em alta disponibilidade a ativo/ativo e a ativo/passivo (quando aplicável)	Atende	https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/127856/resume-ips-scanning-of-iccp-traffic-after-ha-failover	Sem Página
	Mecanismos de inspeção de IPS por meio da análise do estado da conexão, do protocolo, de anomalias de protocolo, da fragmentação, da remontagem e da malformação de pacotes	Atende	https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/213498/signature-based-defense#Engine	Sem Página
	Capacidade de impedimento de ataques básicos e bem conhecidos como Synflood, ICMPflood, UDPflood, etc	Atende	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf	Página 11
	Detecção e bloqueio da origem de port scans	Atende	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf	Página 11

	A mitigação de ataques DoS e DDoS	Atende	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf	DDoS Página 11 - DDoS deverá ser entregue pela solução de BackBone da Operadora
	A prevenção de ataques de buffer overflow	Atende	https://www.fortiguard.com/search?q=buffer+overflow&engine=1	Sem Página
	A possibilidade de criação de assinaturas customizadas	Atende	https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/4afb0436-a998-11e9-81a4-00505692583a/FortiOS-6.0-Handbook.pdf	Página 838
	O suporte a bloqueio de arquivos por tipo	Atende	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf	Página 12
	A Identificação e o bloqueio de comunicação com botnets	Atende	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf	Página 7
	Suporte a várias técnicas de prevenção, incluindo Drop (cliente, servidor e ambos)	Atende	https://docs.fortinet.com/document/fortigate/7.4.0/hardware-acceleration/202492/config-fp-anomaly	Sem Página
	Suporte a referência cruzada com CVE (Common Vulnerabilities and Exposures)	Atende	https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/535363/ips-signature-filter-options	Sem Página
	Suporte a captura de pacotes (PCAP), por assinatura de IPS	Atende	https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/462154/using-the-packet-capture-tool	Sem Página
	Proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms	Atende	https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/610893/supported-file-types	Sem Página
	Proteção contra downloads involuntários usando HTTP ou HTTPS de arquivos executáveis	Atende	https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/610893/supported-file-types	Sem Página
	Rastreamento de vírus em pdf	Atende	https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/610893/supported-file-types	Sem Página
	Inspeção em arquivos comprimidos que uilizam o algoritmo deflate, como: zip e gzip	Atende	https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/610893/supported-file-types	Sem Página
	A configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas do firewall, considerando usuários, grupos de usuários, origem, destino, zonas de segurança, etc, ou seja, cada política de firewall poderá ter uma configuração diferente de IPS, sendo essas políticas por usuários, grupos de usuário, origem, destino, zonas de segurança	Atende	https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/243446/ngfw-policy	Sem Página
	A inspeção de arquivos incorporados em outros arquivos ou arquivos que tenham sua extensão alterada na tentativa de contornar sua detecção	Atende	https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/969330/proxy-mode-inspection	Sem Página
Controle de usuários	A capacidade de criação de políticas baseadas na visibilidade e controle de quem (usuários e grupos de usuários) está utilizando quais aplicações através da integração com serviços de	Atende	https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/656084/firewall-policy	Sem Página

	diretório, autenticação via Ldap, Microsoft Active Directory e base de dados local			
	Autenticação Kerberos	Atende	https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/771627/multiple-ldap-servers-in-kerberos-keytabs-and-agentless-ntlm-domain-controllers	Sem Página
	A capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no Domain Controller, nem nas estações dos usuários	Atende	https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/771627/multiple-ldap-servers-in-kerberos-keytabs-and-agentless-ntlm-domain-controllers	Sem Página
	Integração ao Microsoft Active Directory, permitindo identificar usuários dentro de grupos, mesmo que estejam em uma hierarquia de grupo dentro de grupo	Atende	https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/107067/enabling-active-directory-recursive-search	Sem Página
	Suporte a identificação de múltiplos usuários conectados, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão em uso	Atende	https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/29900/user-groups	Sem Página
	Atualização da identificação de um usuário caso este mude de endereço IP e mesmo que mais de um dispositivo esteja sendo utilizado de forma simultânea, evitando a necessidade de que sejam configurados endereços fixos	Atende	https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/443027/users	Sem Página
Suporte a QoS	A capacidade de controlar as aplicações por políticas de máximo de largura de banda por aplicação, tanto de áudio como de vídeo streaming	Atende	https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/275338/changing-traffic-shaper-bandwidth-unit-of-measurement	Sem Página
	A funcionalidade de configurar horários para navegação, permitindo controle por usuário e tempo	Atende	https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/243446/ngfw-policy	Sem Página
	A criação de políticas de QoS por usuário/grupo do LDAP/AD, aplicações (traffic shaping) e interface física ou lógica do equipamento	Atende	https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/371960/local-in-and-local-out-traffic-matching-new	Sem Página
	Priorização de protocolos de voz e vídeo como H323, SIP, SCCP, MGCP e aplicações como Skype, Teams, Hangout e similares	Atende	https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/933502/shared-traffic-shaper https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/867974/scanning-msrp-traffic https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/813032/dscp-matching-and-dscp-marking	Sem Página
	Suporte a conformação de tráfego com, pelo menos, os seguintes métodos: Traffic Policing e Traffic Shaping	Atende	https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/673634/traffic-shaping-policies https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/297431/traffic-shaping	Sem Página
	Classificação de tráfego com base no campo DSCP	Atende	https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/813032/dscp-matching-and-dscp-marking	Sem Página
	A marcação e priorização do tráfego previamente classificado com base no campo DSCP	Atende	https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/813032/dscp-matching-and-dscp-marking	Sem Página
Suporte à VPN	VPN client-to-site	Atende	https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/190553/remote-access	Sem Página

	Suporte IPSec VPN, com suporte a AES e autenticação via cer ficado IKE PKI	Atende	https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/526306/ike-mode-config-clients	Sem Página
	VPN IPSec com capacidade de implementar túneis site-to-site do tipo hub-and-spoke	Atende	https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/978793/advpn	Sem Página
	O estabelecimento do túnel utilizando uma "chave secreta" ou certificados digitais	Atende	https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/560886/pre-shared-key-vs-digital-certificates	Sem Página
	Implementação de IKEv1 e IKEv2	Atende	https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/167137/choosing-ike-version-1-and-2	Sem Página
	Suporte pelo menos aos seguintes algoritmos de criptografia: 3DES, AES-128, AES-192 e AES256	Atende	https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/604285/phase-2-configuration	Sem Página
	Suporte pelo menos aos seguintes algoritmos de autenticação: MD5, SHA-1, SHA-256, SHA-384, SHA-512	Atende	https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/604285/phase-2-configuration	Sem Página
	Suporte SSL VPN com as seguintes funcionalidades: Conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface WEB Funcionalidades de VPN SSL sejam atendidas sem o uso de cliente Atribuição de endereço IP nos clientes remotos de VPN Atribuição de DNS nos clientes remotos de VPN Políticas de controle de aplicações, IPS, para trafego dos clientes remotos conectados na VPN SSL Autenticação via AD/LDAP, Secure id, certificado padrão ICP-Brasil e base de usuários local Túnel VPN client-to-site do cliente a plataforma de segurança, fornecendo uma solução de single-sign-on aos usuários, integrando-se com as ferramentas de Windows-logon Aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos tuneis SSL Agente de VPN SSL client-to-site deve ser compatível com pelo menos: Windows 7, Windows 8, Windows 10 (home) e Mac Osx Suporte e licença para pelo menos 2000 conexões remotas simultâneas VPN SSL	Atende	https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/4afb0436-a998-11e9-81a4-00505692583a/FortiOS-6.0-Handbook.pdf	A partir da página 557
Controle de acesso à Internet	Filtro de URL HTTP e HTTPS	Atende	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf	Página 7
	Filtro de conteúdo HTTP	Atende	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf	Página 7
	Controle de downloads/uploads de arquivos pelo nome, tipo ou extensão do arquivo	Atende	https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/610893/supported-file-types	Sem Página
	Controle de acesso à internet por domínio	Atende	https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/1706/static-application-steering-with-a-manual-strategy	Sem Página
	Controle de acesso à internet por categorias de sites web	Atende	https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/675558/fortiguard-filter	Sem Página
	Controle de acesso à internet por lista de sites web proibidos (blacklist) customizável	Atende	https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/725397/web-content-filter	Sem Página

	Controle de acesso à internet por lista de sites web permitidos (whitelist) customizável	Atende	https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/725397/web-content-filter	Sem Página
	Mecanismo automático para detecção e bloqueio em tempo real de tráfego (inbound/outbound) originado por códigos maliciosos, tipo malwares ou spywares	Atende	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf	Página 7
	Mecanismo automático para detecção de tráfego tunelado na porta 80	Atende	https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/352916/using-custom-internet-service-in-policy	Sem Página
	Páginas de erro e bloqueio customizáveis	Atende	https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/131140/replacement-messages	Sem Página
	Compatibilidade com filtros de busca segura (safe-search filters), oferecidos por sites web de busca	Atende	https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/12534/dns-safe-search	Sem Página
	Controle de acesso por definição e aplicação das regras com expressões regulares	Atende	https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/931220/configuring-web-filter-profiles-with-hebrew-domain-names	Sem Página
	Liberação/bloqueio de componentes específicos de sites de redes sociais, tais como chat e comentários do site wwwfacebookcom ou postagem no site wwwtwittercom	Atende	https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/615462/url-filter	Sem Página
	Controle de acesso por geolocalização	Atende	https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/286826/geography-based-addresses	Sem Página
Categorização de sites web	Base de dados com no mínimo 15 (quinze) milhões de URL's cadastradas, e pelo menos 45 (quarenta e cinco) categorias previamente definidas e possibilidade de criação de novas categorias personalizadas	Atende	https://www.fortiguard.com/webfilter https://www.fortiguard.com/webfilter/categories	Sem Página
	A classificação/categorização de sites de acordo com o assunto	Atende	https://www.fortiguard.com/webfilter/categories	Sem Página
	Mecanismo de cadastro de novas URLs junto ao fabricante para a devida categorização	Atende	https://www.fortiguard.com/faq/wfratingsubmit	Sem Página
	Mecanismo de reclassificação, quando necessário	Atende	https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/408599/web-profile-override	Sem Página
Atualização da base de sites	Atualização automática da base de sites pela solução, via Internet, em dias e horários customizáveis	Atende	https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/655726/scheduled-updates	Sem Página
	Atualização transparente, sem comprometer a execução dos serviços, principalmente no caso de falhas no acesso à base de sites	Atende	https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/655726/scheduled-updates	Sem Página
	Mecanismos de manutenção da base de sites incluindo a reclassificação de sites antes "maliciosos" que foram "descontaminados", para o retorno do acesso à normalidade	Atende	https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/408599/web-profile-override	Sem Página
Definição de políticas para a modelagem do tráfego	IP de origem	Atende	https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/1706/static-application-steering-with-a-manual-strategy	Sem Página
	IP de destino	Atende	https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/1706/static-application-steering-with-a-manual-strategy	Sem Página
	Porta TCP/UDP de destino	Atende	https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/1706/static-application-steering-with-a-manual-strategy	Sem Página

	URL de destino	Atende	https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/1706/static-application-steering-with-a-manual-strategy	Sem Página
	Aplicação de camada 7	Atende	https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/1706/static-application-steering-with-a-manual-strategy	Sem Página
Gerenciamento remoto	Deve permitir o provisionamento e configuração de maneira automática, sem a necessidade de intervenção manual, quando ligado e conectado à rede	Atende	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortimanager.pdf	Sem Página
CARACTERÍSTICAS MÍNIMAS DOS EQUIPAMENTOS SD-WAN DAS SEDES E ÓRGÃOS (EXCETO DO DATACENTER)				
Interface Gigabit	Três interfaces Gigabit Ethernet (1000Base-T) que serão utilizadas para outros links ou na rede interna da DPRJ	Atende	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-400f-series.pdf	Página 6
	Três interfaces 10Gigabit Ethernet (10Gbase-SR) que serão utilizadas para outros links ou na rede interna da DPRJ	Atende	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-400f-series.pdf	Página 6
Fonte de alimentação	Deverá ter no mínimo duas fontes de alimentação (redundantes)	Atende	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-400f-series.pdf	Página 7
Throughput	Deverá possuir throughtput mínimo de 5.8 Gbps (cinco ponto oito gigabits por segundo) para SSL inspection ou NGFW ou Application Control	Atende	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-400f-series.pdf	Página 7
	Deverá possuir throughtput mínimo de 5.8 Gbps (cinco ponto oito gigabits por segundo) para tráfego VPN	Atende	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-400f-series.pdf	Página 7
	Deverá possuir throughtput mínimo de 5.8 Gbps (cinco ponto oito gigabits por segundo) para IPS	Atende	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-400f-series.pdf	Página 7
Sessões simultâneas	Deverá suportar no mínimo 2.000.000 (dois milhões) de sessões de firewall simultâneas	Atende	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-400f-series.pdf	Página 7
Funcionalidade NGFW	O equipamento deverá possuir funcionalidade NGFW (Next Generation Firewall) reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões	Atende	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-400f-series.pdf	Página 1
Análise de conteúdo de aplicações	A plataforma deverá ser otimizada para análise de conteúdo de aplicações em camada 7	Atende	https://docs.fortinet.com/document/fortigate/6.0.0/handbook/240599/application-control	Sem Página
Tipo de equipamento	Deverá ser do tipo appliance, não sendo aceito equipamento do tipo servidor e com sistema operacional de uso genérico	Atende	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-400f-series.pdf	Página 1
Funcionalidades	anti-spoofing, configurável por segmento de rede de modo que seja possível utilizar o próprio endereçamento da interface ou especificar quais redes serão utilizadas como referência para permitir/negar o ingresso de um pacote	Atende	https://docs.fortinet.com/document/fortigate/6.0.0/handbook/178055/fortios-diagnostics	Sem Página
	Deverá permitir a configuração de ISP (rota default estática) com a utilização de probe para verificar a disponibilidade do provedor	Atende	https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/626338/adding-a-static-route	Sem Página
	A probe deve permitir verificar o acesso HTTP a pelo menos 1 (um) site web e deve considerar o ISP indisponível em caso de falha	Atende	https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/723056/link-monitoring-and-failover	Sem Página
	As funcionalidades de controle de aplicações, filtro de URLs, VPN IPSec e SSL, QoS, SSL Decryption e protocolos de roteamento dinâmico deverão operar em caráter permanente,	Atende	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf	A partir da

	podendo ser utilizadas durante toda a vigência do contrato			página 5
	Policy based routing ou policy based forwarding	atende	https://docs.fortinet.com/document/fortigate/6.0.0/handbook/34912/policy-routing	Sem Página
	Jumbo Frames	Atende	https://docs.fortinet.com/document/fortigate/6.0.0/handbook/822669/interface-mtu-packet-size	Sem Página
	Servidor DHCP em IPv4 e IPv6	Atende	https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/783526/dhcp-servers-and-relays https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/776785/dhcpv6-stateful-server	Sem Página
	Suportar IGMP, v2 e v3	Atende	https://docs.fortinet.com/document/fortigate/7.2.0/new-features/64590/configure-the-frequency-of-igmp-queries-7-2-1	Sem Página
	Permitir a administração remota, protegida por autenticação usuário/senha e utilizando pelo menos os protocolos SSHv2 e HTTPS	Atende	https://docs.fortinet.com/document/fortigate/7.2.0/new-features/936614/restrict-ssh-and-telnet-jump-host-capabilities-7-2-1 https://docs.fortinet.com/document/fortigate/7.2.0/new-features/499047/new-default-certificate-for-https-administrative-access-7-2-1	Sem Página
	Roteamento IP Multicast através do protocolo PIM nas versões 1 e 2 e nos modos Sparse Mode e Dense Mode, não sendo exigida a implementação dos dois modos de forma simultânea	Atende	https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/4afb0436-a998-11e9-81a4-00505692583a/FortiOS-6.0-Handbook.pdf	Página 1737
	Roteamento estático, OSPF, BGP e PBR (Policy Base Routing)	Atende	https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/804259/static-routing https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/479509/dynamic-routing	Sem Página
	MP-BGP, ou seja, encaminhamento de tráfego IPv4 e IPv6, ou suportar VRF	Atende	https://docs.fortinet.com/document/fortigate/6.0.0/handbook/691160/routing-concepts	Sem Página
	Cliente NTP	atende	https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/149181/date-and-time-settings	Sem Página
	SNMP nas versões 2c e 3 com restrição dos endereços para consultas	Atende	https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/62595/snmp	Sem Página
	Protocolo de informações de fluxo como Netflow, sFlow, IPFIX ou similar	Atende	https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/998643/netflow https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/505119/sflow	Sem Página
Deverá suportar NAT dos seguintes tipos	NAT dinâmico (Many-to-1)	Atende	https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/188051/source-nat https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/728694/destination-nat	Sem Página
	NAT dinâmico (Many-to-Many)	Atende	https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/188051/source-nat https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/728694/destination-nat	Sem Página
	NAT estático (1-to-1)	Atende	https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/188051/source-nat https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/728694/destination-nat	Sem Página
	NAT estático (Many-to-Many)	Atende	https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/188051/source-nat https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/728694/destination-nat	Sem Página

	NAT estático bidirecional 1-to-1	Atende	https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/188051/source-nat https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/728694/destination-nat	Sem Página
	Tradução de porta (PAT)	Atende	https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/188051/source-nat https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/728694/destination-nat	Sem Página
	NAT de origem	Atende	https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/188051/source-nat https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/728694/destination-nat	Sem Página
	NAT de destino	Atende	https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/188051/source-nat https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/728694/destination-nat	Sem Página
	NAT de origem e NAT de destino simultaneamente	Atende	https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/188051/source-nat https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/728694/destination-nat	Sem Página
Controle de política de firewall	O controle de aplicações por grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias	Atende	https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/302748/application-control	Sem Página
	Controle, inspeção e descriptografia de SSL por política para trafego de entrada (inbound) e saída (outbound)	Atende	https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/669193/ssl-based-application-detection-over-decrypted-traffic-in-a-sandwich-topology	Sem Página
	Suporte offload de certificado em inspeção de conexões SSL de entrada (inbound)	Atende	https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/669193/ssl-based-application-detection-over-decrypted-traffic-in-a-sandwich-topology	Sem Página
	Permissão de bloqueio de, pelo menos, os seguintes tipos de arquivos ou extensões: bat, cab, dll, exe, pif, e reg	Atende	https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/610893/supported-file-types	Suporta extensões do tipo bat, cab e exe.
	Suporte a objetos e regras multicast	Atende	https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/4afb0436-a998-11e9-81a4-00505692583a/FortiOS-6.0-Handbook.pdf	Página 617
	O agendamento de políticas em horários pré-definidos, de maneira automática	Atende	https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/656084/firewall-policy	Sem Página
	Suporte a criação de políticas com data de expiração	Atende	https://docs.fortinet.com/document/fortimanager/7.0.0/administration-guide/156162/configuring-policy-details https://docs.fortinet.com/document/fortimanager/7.0.0/administration-guide/958981/schedule-a-policy-package-install	Sem Página
Controle de aplicações	Capacidade de reconhecer aplicações, independente de porta e protocolo	Atende	https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/836937/configuring-an-application-sensor	Sem Página
	Capacidade de balancear o tráfego das aplicações entre múltiplos links, simultaneamente	Atende	https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/257828/sd-wan-components-and-design-principles	Sem Página

	Capacidade de definição de qual link será utilizado em situação normal por determinada aplicação	Atende	https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/270527/specify-an-sd-wan-zone-in-static-routes-and-sd-wan-rules	Sem Página
	Liberação e o bloqueio das aplicações, sem a necessidade de especificação de portas e protocolos	Atende	https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/243446/ngfw-policy	Sem Página
	Reconhecimento das diversas aplicações diferentes, incluindo, mas não limitado: peer-to-peer, redes sociais, acessoremoto, update de software, protocolos de rede, voip, audio, vídeo, proxy, mensageria instantânea, compartilhamento de arquivos, e-mail	Atende	https://www.fortiguard.com/appcontrol	Sem Página
	Habilidade de inspecionar o payload de pacote de dados com o objetivo de detectar através de expressões regulares assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo	Atende	https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/969330/proxy-mode-inspection	Sem Página
	A capacidade de identificar o uso de táticas evasivas, ou seja, visualizar e controlar as aplicações e os ataques que ulizam comunicações criptografadas, tais como Skype e ataques utilizando a porta 443	Atende	https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/4afb0436-a998-11e9-81a4-00505692583a/FortiOS-6.0-Handbook.pdf	Páginas 919 e 920
	A capacidade de decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo, incluindo, mas não limitado a Yahoo Instant Messenger ou Whatsapp usando HTTP. A decodificação de protocolo também deve identificar funcionalidades específicas dentro de uma aplicação, incluindo, mas não limitado a compartilhamento de arquivo dentro do Webex. Além de detectar arquivos e outros conteúdos que devem ser inspecionados de acordo as regras de segurança implementadas	Atende	https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/4afb0436-a998-11e9-81a4-00505692583a/FortiOS-6.0-Handbook.pdf	Páginas 467 e 826
	A possibilidade da liberação e do bloqueio das aplicações (ou de suas funcionalidades) por usuário, grupo de usuários, endereço IP ou rede específica	Atende	https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/4afb0436-a998-11e9-81a4-00505692583a/FortiOS-6.0-Handbook.pdf	Páginas 919 e 920
	Atualização automática da base de assinaturas de aplicações	Atende	https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/4afb0436-a998-11e9-81a4-00505692583a/FortiOS-6.0-Handbook.pdf	Página 110
	A possibilidade de adicionar controle de aplicações em todas as regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras	Atende	https://docs.fortinet.com/document/fortigate/6.0.0/handbook/721617/configuring-profiles	Sem Página
	A permissão de solicitação de inclusão de aplicações na base de assinaturas de aplicações do fabricante	Atende	https://www.fortiguard.com/faq/appctrlsubmit	Sem Página
	A função de alertar o usuário quando uma aplicação for bloqueada	Atende	https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/4afb0436-a998-11e9-81a4-00505692583a/FortiOS-6.0-Handbook.pdf	Sem página
			https://kb.fortinet.com/kb/documentLink.do?externalID=FD48878	Páginas 923 e 924

	A possibilidade de diferenciação e controle de partes das aplicações como, por exemplo, permitir o Gtalk chat mas bloquear a transferência de arquivos, permitir acesso ao Facebook mas bloquear a visualização de vídeos, permitir acesso ao WhatsApp mas bloquear a transferência de arquivos	Atende	https://www.fortiguard.com/search?q=hangouts&type=app&engine=1	Sem Página
	A possibilidade de diferenciação de aplicações Proxies (ghostsurf, freegate, ultrasurf, tor, etc) possuindo granularidade de controle/políticas para os mesmos	Atende	https://www.fortiguard.com/search?q=hangouts&type=app&engine=1	Sem Página
	A possibilidade da criação de grupos estáticos de aplicações e grupos dinâmicos de aplicações baseados em características das aplicações como: tecnologia utilizada nas aplicações (client-server, browser based, network protocol, etc), nível de risco da aplicação, aplicações que usem técnicas evasivas, utilizadas por malwares, como transferência de arquivos e/ou uso excessivo de banda, etc	Atende	https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/19814/basic-category-filters-and-overrides	Sem Página
Controle de prevenção de ameaças	Módulo de IPS integrado no equipamento	Atende	https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/565562/intrusion-prevention	Sem Página
	Assinaturas de prevenção de intrusão (IPS)	Atende	https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/213498/signature-based-defense	Sem Página
	A sincronização das assinaturas de IPS quando implementado em alta disponibilidade a ativo/ativo e a ativo/passivo (quando aplicável)	Atende	https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/127856/resume-ips-scanning-of-iccp-traffic-after-ha-failover	Sem Página
	Mecanismos de inspeção de IPS por meio da análise do estado da conexão, do protocolo, de anomalias de protocolo, da fragmentação, da remontagem e da malformação de pacotes	Atende	https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/213498/signature-based-defense#Engine	Sem Página
	Capacidade de impedimento de ataques básicos e bem conhecidos como Synflood, ICMPflood, UDPflood, etc	Atende	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf	Página 11
	Detecção e bloqueio da origem de port scans	Atende	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf	Página 11
	A mitigação de ataques DoS e DDoS	Atende	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf	DDoS Página 11 - DDoS deverá ser entregue pela solução de BackBone da Operadora
	A prevenção de ataques de buffer overflow	atende	https://www.fortiguard.com/search?q=buffer+overflow&engine=1	Sem Página
	A possibilidade de criação de assinaturas customizadas	Atende	https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/4afb0436-a998-11e9-81a4-00505692583a/FortiOS-6.0-Handbook.pdf	Página 838
	O suporte a bloqueio de arquivos por tipo	Atende	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf	Página 12

	A Identificação e o bloqueio de comunicação com botnets	Atende	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf	Página 7
	Suporte a várias técnicas de prevenção, incluindo Drop (cliente, servidor e ambos)	Atende	https://docs.fortinet.com/document/fortigate/7.4.0/hardware-acceleration/202492/config-fp-anomaly	Sem Página
	Suporte a referência cruzada com CVE (Common Vulnerabilities and Exposures)	Atende	https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/535363/ips-signature-filter-options	Sem Página
	Suporte a captura de pacotes (PCAP), por assinatura de IPS	Atende	https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/462154/using-the-packet-capture-tool	Sem Página
	Proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms	Atende	https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/610893/supported-file-types	Sem Página
	Proteção contra downloads involuntários usando HTTP ou HTTPS de arquivos executáveis	atende	https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/610893/supported-file-types	Sem Página
	Rastreamento de vírus em pdf	Atende	https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/610893/supported-file-types	Sem Página
	Inspeção em arquivos comprimidos que uilizam o algoritmo deflate, como: zip e gzip	Atende	https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/610893/supported-file-types	Sem Página
	A configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas do firewall, considerando usuários, grupos de usuários, origem, destino, zonas de segurança, etc, ou seja, cada política de firewall poderá ter uma configuração diferente de IPS, sendo essas políticas por usuários, grupos de usuário, origem, destino, zonas de segurança	Atende	https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/243446/ngfw-policy	Sem Página
	A inspeção de arquivos incorporados em outros arquivos ou arquivos que tenham sua extensão alterada na tentativa de contornar sua detecção	Atende	https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/969330/proxy-mode-inspection	Sem Página
Controle de usuários	A capacidade de criação de políticas baseadas na visibilidade e controle de quem (usuários e grupos de usuários) está utilizando quais aplicações através da integração com serviços de diretório, autenticação via Ldap, Microsoft Active Directory e base de dados local	Atende	https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/656084/firewall-policy	Sem Página
	Autenticação Kerberos	Atende	https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/771627/multiple-ldap-servers-in-kerberos-keytabs-and-agentless-ntlm-domain-controllers	Sem Página
	A capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no Domain Controller, nem nas estações dos usuários, com expansão a portal captivo residente no próprio equipamento	Atende	https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/771627/multiple-ldap-servers-in-kerberos-keytabs-and-agentless-ntlm-domain-controllers	Sem Página
	Suporte a accounting Microsoft NPS como RSSO, Radius Accounting ou similar	Atende	https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/29900/user-groups	Sem Página
	Integração ao Microsoft Active Directory, permitindo identificar usuários dentro de grupos, mesmo que estejam em uma hierarquia de grupo dentro de grupo	Atende	https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/107067/enabling-active-directory-recursive-search	Sem Página
	Suporte a identificação de múltiplos usuários conectados, permitindo visibilidade e controle	atende	https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/29900/user-groups	Sem Página

	granular por usuário sobre o uso das aplicações que estão em uso			
	Suporte a identificação de usuários via certificados digitais ICP-Brasil para conexões a serviços via SSL VPN	Atende	https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/371626/ssl-vpn	Sem Página
	Atualização da identificação de um usuário caso este mude de endereço IP e mesmo que mais de um dispositivo esteja sendo utilizado de forma simultânea, evitando a necessidade de que sejam configurados endereços fixos	atende	https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/443027/users	Sem Página
Suporte a QoS	A capacidade de controlar as aplicações por políticas de máximo de largura de banda por aplicação, tanto de áudio como de vídeo streaming	atende	https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/275338/changing-traffic-shaper-bandwidth-unit-of-measurement	Sem Página
	A funcionalidade de configurar horários para navegação, permitindo controle por usuário e tempo	Atende	https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/243446/ngfw-policy	Sem Página
	A criação de políticas de QoS por usuário/grupo do LDAP/AD, aplicações (traffic shaping) e interface física ou lógica do equipamento	Atende	https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/371960/local-in-and-local-out-traffic-matching-new	Sem Página
	Priorização de protocolos de voz e vídeo como H323, SIP, SCCP, MGCP e aplicações como Skype, Teams, Hangout e similares	atende	https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/933502/shared-traffic-shaper https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/867974/scanning-msrp-traffic https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/813032/dscp-matching-and-dscp-marking	Sem Página
	Suporte a conformação de tráfego com, pelo menos, os seguintes métodos: Traffic Policing e Traffic Shaping	Atende	https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/673634/traffic-shaping-policies https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/297431/traffic-shaping	Sem Página
	Classificação de tráfego com base no campo DSCP	atende	https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/813032/dscp-matching-and-dscp-marking	Sem Página
	A marcação e priorização do tráfego previamente classificado com base no campo DSCP	Atende	https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/813032/dscp-matching-and-dscp-marking	Sem Página
Suporte à VPN	VPN client-to-site	Atende	https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/190553/remote-access	Sem Página
	Suporte IPSec VPN, com suporte a AES e autenticação via cer ficado IKE PKI	Atende	https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/526306/ike-mode-config-clients	Sem Página
	VPN IPSec com capacidade de implementar túneis site-to-site do tipo hub-and-spoke	Atende	https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/978793/advpn	Sem Página
	O estabelecimento do túnel utilizando uma “chave secreta” ou certificados digitais	Atende	https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/560886/pre-shared-key-vs-digital-certificates	Sem Página
	Implementação de IKEv1 e IKEv2	Atende	https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/167137/choosing-ike-version-1-and-2	Sem Página
	Suporte pelo menos aos seguintes algoritmos de criptografia: 3DES, AES-128, AES-192 e AES256	Atende	https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/604285/phase-2-configuration	Sem Página
	Suporte pelo menos aos seguintes algoritmos de autenticação: MD5, SHA-1, SHA-256, SHA-384, SHA-512	Atende	https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/604285/phase-2-configuration	Sem Página

	Suporte SSL VPN com as seguintes funcionalidades: Conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface WEB Funcionalidades de VPN SSL sejam atendidas sem o uso de cliente Atribuição de endereço IP nos clientes remotos de VPN Atribuição de DNS nos clientes remotos de VPN Políticas de controle de aplicações, IPS, para trafego dos clientes remotos conectados na VPN SSL Autenticação via AD/LDAP, Secure id, certificado padrão ICP-Brasil e base de usuários local Túnel VPN client-to-site do cliente a plataforma de segurança, fornecendo uma solução de single-sign-on aos usuários, integrando-se com as ferramentas de Windows-logon Aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos tuneis SSL Agente de VPN SSL client-to-site deve ser compatível com pelo menos: Windows 7, Windows 8, Windows 10 (home) e Mac Osx Suporte e licença para pelo menos 2000 conexões remotas simultâneas VPN SSL	Atende	https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/4afb0436-a998-11e9-81a4-00505692583a/FortiOS-6.0-Handbook.pdf	A partir da página 557
Filtro de URLs	Filtro de URL HTTP e HTTPS	Atende	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf	Página 7
	Filtro de conteúdo HTTP	Atende	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf	Página 7
	SSL Scanner	Atende	https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/669193/ssl-based-application-detection-over-decrypted-traffic-in-a-sandwich-topology	Sem Página
	Proxy transparente HTTP/HTTPS, proxy explícito e portal captivo, por segmento de rede	Atende	https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/15908/transparent-proxy	Sem Página
	Cache de dados	Atende	https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/72214/cache-service-and-video-caching	Sem Página
	Bloqueio de acesso com mensagem customizada, de forma a permitir que o usuário solicite a liberação por meio de formulário ou justificativa	Atende	https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/4afb0436-a998-11e9-81a4-00505692583a/FortiOS-6.0-Handbook.pdf	Página 838
	Monitoramento do tráfego internet independente de plataforma, sistema operacional ou aplicação	Atende	https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/379794/passive-health-check-measurement-by-internet-service-and-application	Sem Página
	Filtragem sem necessidade da instalação de agentes nas estações	Atende	https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/771627/multiple-ldap-servers-in-kerberos-keytabs-and-agentless-ntlm-domain-controllers	Sem Página
Controle de acesso à Internet	Regras baseadas tanto na requisição quanto na resposta HTTP	Atende	https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/243446/ngfw-policy	Sem Página
	Regras baseadas em horário do dia	Atende	https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/243446/ngfw-policy	Sem Página
	Controle de downloads/uploads de arquivos pelo nome, tipo ou extensão do arquivo	Atende	https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/610893/supported-file-types	

	Controle de acesso à internet por domínio	Atende	https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/1706/static-application-steering-with-a-manual-strategy	Sem Página
	Controle de acesso à internet por categorias de sites web	Atende	https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/675558/fortiguard-filter	Sem Página
	Controle de acesso à internet por lista de sites web proibidos (blacklist) customizável	Atende	https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/725397/web-content-filter	Sem Página
	Controle de acesso à internet por lista de sites web permitidos (whitelist) customizável	Atende	https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/725397/web-content-filter	Sem Página
	Mecanismo automático para detecção e bloqueio em tempo real de tráfego (inbound/outbound) originado por códigos maliciosos, tipo malwares ou spywares	Atende	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf	Página 7
	Mecanismo automático para detecção de tráfego tunelado na porta 80	Atende	https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/352916/using-custom-internet-service-in-policy	Sem Página
	Páginas de erro e bloqueio customizáveis	Atende	https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/131140/replacement-messages	Sem Página
	Compatibilidade com filtros de busca segura (safe-search filters), oferecidos por sites web de busca	Atende	https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/12534/dns-safe-search	Sem Página
	Controle de acesso por definição e aplicação das regras com expressões regulares	Atende	https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/931220/configuring-web-filter-profiles-with-hebrew-domain-names	Sem Página
	Liberação/bloqueio de componentes específicos de sites de redes sociais, tais como chat e comentários do site www.facebook.com ou postagem no site www.twitte.rcom	Atende	https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/615462/url-filter	Sem Página
	Controle de acesso por geolocalização	Atende	https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/286826/geography-based-addresses	Sem Página
Categorização de sites web	Base de dados com no mínimo 15 (quinze) milhões de URL's cadastradas, e pelo menos 45 (quarenta e cinco) categorias previamente definidas e possibilidade de criação de novas categorias personalizadas	Atende	https://www.fortiguard.com/webfilter https://www.fortiguard.com/webfilter/categories	Sem Página
	A classificação/categorização de sites de acordo com o assunto	ate nde	https://www.fortiguard.com/webfilter/categories	Sem Página
	Mecanismo de cadastro de novas URLs junto ao fabricante para a devida categorização	Atende	https://www.fortiguard.com/faq/wfratingsubmit	Sem Página
	Mecanismo de reclassificação, quando necessário	Atende	https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/408599/web-profile-override	Sem Página
Atualização da base de sites	Atualização automática da base de sites pela solução, via Internet, em dias e horários customizáveis	Atende	https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/655726/scheduled-updates	Sem Página
	Atualização transparente, sem comprometer a execução dos serviços, principalmente no caso de falhas no acesso à base de sites	Atende	https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/655726/scheduled-updates	Sem Página
	Mecanismos de manutenção da base de sites incluindo a reclassificação de sites antes "maliciosos" que foram "descontaminados", para o retorno do acesso à normalidade	Atende	https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/408599/web-profile-override	Sem Página
Definição de políticas	IP de origem	Atende	https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/1706/static-application-steering-with-a-manual-strategy	Sem Página

para a modelagem do tráfego	IP de destino	Atende	https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/1706/static-application-steering-with-a-manual-strategy	Sem Página
	Porta TCP/UDP de destino	Atende	https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/1706/static-application-steering-with-a-manual-strategy	Sem Página
	URL de destino	Atende	https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/1706/static-application-steering-with-a-manual-strategy	Sem Página
	Aplicação de camada 7	Atende	https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/1706/static-application-steering-with-a-manual-strategy	Sem Página
Gerenciamento remoto	Deve permitir o provisionamento e configuração de maneira automática, sem a necessidade de intervenção manual, quando ligado e conectado à rede	Atende	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortimanager.pdf	Página 3

TATIANA ZOUAIN DUTRA DO SOUTO

Executiva de Negócios

RG: 03370641602

CPF: 873.658.127-53

ROSALVO OLIVEIRA SILVA JUNIOR

Gerente de Vendas

RG: 989034

CPF: 693.002.751-00

_____

Assinatura do(s) representante(s) legal(is) da empresa, sobre carimbo
Nome e número da identidade do responsável pela Sociedade

Item	
CARACTERÍSTICAS MÍNIMAS DOS EQUIPAMENTOS SD-WAN DAS SEDES E ÓRGÃOS (EXCETO DO DATACENTER)	
Interface Gigabit (1000Base-T)	Quatro Interfaces Gigabit Ethernet (1000Base-T) (uma para conectar o link do LOTE 1, uma para conectar o link do LOTE 3, rede interna da respectiva sede ou órgão da DPRJ, outros links)
Throughtput	Deverá possuir throughtput mínimo que suporte adequadamente os serviços de SSL inspection ou NGFW ou Application Control, para tráfego VPN e para IPS
Sessões simultâneas	Deverá suportar no mínimo 50.000 (cinquenta mil) sessões de firewall simultâneas
Funcionalidade NGFW	O equipamento deverá possuir funcionalidade NGFW (Next Generation Firewall) reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões
Análise de conteúdo de aplicações	A plataforma deverá ser otimizada para análise de conteúdo de aplicações em camada 7
Tipo de equipamento	Deverá ser do tipo appliance, não sendo aceito equipamento do tipo servidor e com sistema operacional de uso genérico
Funcionalidades	Anti-spoofing, configurável por segmento de rede de modo que seja possível utilizar o próprio endereçamento da interface ou especificar quais redes serão utilizadas como referência para permitir/negar o ingresso de um pacote
	Deverá permitir a configuração de ISP (rota default estática) com a utilização de probe para verificar a disponibilidade do provedor
	A probe deve permitir verificar o acesso HTTP a pelo menos 1 (um) site web e deve considerar o ISP indisponível em caso de falha
	As funcionalidades de controle de aplicações, filtro de URLs, VPN IPSec e SSL, QoS, SSL Decryption e protocolos de roteamento dinâmico deverão operar em caráter permanente, podendo ser utilizadas durante toda a vigência do contrato
	Policy based routing ou policy based forwarding
	Jumbo Frames
	Servidor DHCP em IPv4 e IPv6
	Suportar IGMP, v2 e v3
	Permitir a administração remota, protegida por autenticação usuário/senha e utilizando pelo menos os protocolos SSHv2 e HTTPS
	Roteamento IP Multicast através do protocolo PIM nas versões 1 e 2 e nos modos Sparse Mode e Dense Mode, não sendo exigida a implementação dos dois modos de forma simultânea
	Roteamento estático, OSPF, BGP e PBR (Policy Base Routing)
	MP-BGP, ou seja, encaminhamento de tráfego IPv4 e IPv6, ou suportar VRF
	Cliente NTP
	SNMP nas versões 2c e 3 com restrição dos endereços para consultas
	Protocolo de informações de fluxo como Netflow, sFlow, IPFIX ou similar
	Gateway que contenha solução de antivírus que suporte a análise de pelo menos os protocolos HTTP, FTP, IMAP, POP3 e SMTP
	Suportar health check ativo, passivo e misto

Deverá suportar NAT dos seguintes tipos	NAT dinâmico (Many-to-1)
	NAT dinâmico (Many-to-Many)
	NAT estático (1-to-1)
	NAT estático (Many-to-Many)
	NAT estático bidirecional 1-to-1
	Tradução de porta (PAT)
	NAT de origem
	NAT de destino
	NAT de origem e NAT de destino simultaneamente
	Network Prefix Translation (NPTv6), NAT66
Controle de política de firewall	O controle de aplicações por grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias
	Controle, inspeção e descriptografia de SSL por política para trafego de entrada (inbound) e saída (outbound)
	Suporte offload de certificado em inspeção de conexões SSL de entrada (inbound)
	Permissão de bloqueio de, pelo menos, os seguintes tipos de arquivos ou extensões: bat, cab, dll, exe, pif, e reg
	Suporte a objetos e regras multicast
	O agendamento de políticas em horários pré-definidos, de maneira automática
	Suporte a criação de políticas com data de expiração
	Capacidade de reconhecer aplicações, independente de porta e protocolo
	A capacidade de balancear o tráfego das aplicações entre múltiplos links, simultaneamente, incluindo portanto os links disponibilizados pelo lote de links simétricos e pelo lote de links assimétricos
	Capacidade de definição de qual link será utilizado em situação normal por determinada aplicação
	Liberação e o bloqueio das aplicações, sem a necessidade de especificação de portas e protocolos
	Reconhecimento das diversas aplicações diferentes, incluindo, mas não limitado: peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, audio, vídeo, proxy, mensageria instantânea, compartilhamento de arquivos, e-mail
	Habilidade de inspecionar o payload de pacote de dados com o objetivo de detectar através de expressões regulares assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo
	A capacidade de identificar o uso de táticas evasivas, ou seja, visualizar e controlar as aplicações e os ataques que utilizam comunicações criptografadas, tais como Skype e ataques utilizando a porta 443

Controle de aplicações	A capacidade de decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo, incluindo, mas não limitado a Yahoo Instant Messenger ou Whatsapp usando HTTP. A decodificação de protocolo também deve identificar funcionalidades específicas dentro de uma aplicação, incluindo, mas não limitado a, compartilhamento de arquivo dentro do Webex. Além de detectar arquivos e outros conteúdos que devem ser inspecionados de acordo as regras de segurança implementadas
	A possibilidade da liberação e do bloqueio das aplicações (ou de suas funcionalidades) por usuário, grupo de usuários, endereço IP ou rede específica
	Atualização automática da base de assinaturas de aplicações
	A possibilidade de adicionar controle de aplicações em todas as regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras
	A permissão de solicitação de inclusão de aplicações na base de assinaturas de aplicações do fabricante
	A função de alertar o usuário quando uma aplicação for bloqueada
	A possibilidade de diferenciação e controle de partes das aplicações como, por exemplo, permitir o Gtalk chat mas bloquear a transferência de arquivos, permitir acesso ao Facebook mas bloquear a visualização de vídeos, permitir acesso ao WhatsApp mas bloquear a transferência de arquivos
	A possibilidade de diferenciação de aplicações Proxies (ghostsurf, freegate, ultrasurf, tor, etc) possuindo granularidade de controle/políticas para os mesmos
	A possibilidade da criação de grupos estáticos de aplicações e grupos dinâmicos de aplicações baseados em características das aplicações como: tecnologia utilizada nas aplicações (client-server, browser based, network protocol, etc), nível de risco da aplicação, aplicações que usem técnicas evasivas, utilizadas por malwares, como transferência de arquivos e/ou uso excessivo de banda, etc
Controle de prevenção de ameaças	Módulo de IPS integrado no equipamento
	Assinaturas de prevenção de intrusão (IPS)
	A sincronização das assinaturas de IPS quando implementado em alta disponibilidade a ativo/ativo e a ativo/passivo (quando aplicável)
	Mecanismos de inspeção de IPS por meio da análise do estado da conexão, do protocolo, de anomalias de protocolo, da fragmentação, da remontagem e da malformação de pacotes
	Capacidade de impedimento de ataques básicos e bem conhecidos como Synflood, ICMPflood, UDPflood, etc
	Detecção e bloqueio da origem de port scans
	A mitigação de ataques DoS e DDoS
	A prevenção de ataques de buffer overflow
	A possibilidade de criação de assinaturas customizadas
	O suporte a bloqueio de arquivos por tipo
	A Identificação e o bloqueio de comunicação com botnets
	Suporte a várias técnicas de prevenção, incluindo Drop (cliente, servidor e ambos)
	Suporte a referência cruzada com CVE (Common Vulnerabilities and Exposures)
	Suporte a captura de pacotes (PCAP), por assinatura de IPS
	Proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms
	Proteção contra downloads involuntários usando HTTP ou HTTPS de arquivos executáveis
	Rastreamento de vírus em pdf
	Inspeção em arquivos comprimidos que uilizam o algoritmo deflate, como: zip e gzip

	A configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas do firewall, considerando usuários, grupos de usuários, origem, destino, zonas de segurança, etc, ou seja, cada política de firewall poderá ter uma configuração diferente de IPS, sendo essas políticas por usuários, grupos de usuário, origem, destino, zonas de segurança
	A inspeção de arquivos incorporados em outros arquivos ou arquivos que tenham sua extensão alterada na tentativa de contornar sua detecção
Controle de usuários	A capacidade de criação de políticas baseadas na visibilidade e controle de quem (usuários e grupos de usuários) está utilizando quais aplicações através da integração com serviços de diretório, autenticação via Ldap, Microsoft Active Directory e base de dados local
	Autenticação Kerberos
	A capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no Domain Controller, nem nas estações dos usuários
	Integração ao Microsoft Active Directory, permitindo identificar usuários dentro de grupos, mesmo que estejam em uma hierarquia de grupo dentro de grupo
	Suporte a identificação de múltiplos usuários conectados, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão em uso
	Atualização da identificação de um usuário caso este mude de endereço IP e mesmo que mais de um dispositivo esteja sendo utilizado de forma simultânea, evitando a necessidade de que sejam configurados endereços fixos
Suporte a QoS	A capacidade de controlar as aplicações por políticas de máximo de largura de banda por aplicação, tanto de áudio como de vídeo streaming
	A funcionalidade de configurar horários para navegação, permitindo controle por usuário e tempo
	A criação de políticas de QoS por usuário/grupo do LDAP/AD, aplicações (traffic shaping) e interface física ou lógica do equipamento
	Priorização de protocolos de voz e vídeo como H323, SIP, SCCP, MGCP e aplicações como Skype, Teams, Hangout e similares
	Suporte a conformação de tráfego com, pelo menos, os seguintes métodos: Traffic Policing e Traffic Shaping
	Classificação de tráfego com base no campo DSCP
	A marcação e priorização do tráfego previamente classificado com base no campo DSCP
	VPN client-to-site
	Suporte IPSec VPN, com suporte a AES e autenticação via cer ficado IKE PKI
	VPN IPSec com capacidade de implementar túneis site-to-site do tipo hub-and-spoke
	O estabelecimento do túnel utilizando uma “chave secreta” ou certificados digitais
	Implementação de IKEv1 e IKEv2
	Suporte pelo menos aos seguintes algoritmos de criptografia: 3DES, AES-128, AES-192 e AES256
	Suporte pelo menos aos seguintes algoritmos de autenticação: MD5, SHA-1, SHA-256, SHA-384, SHA-512

Suporte à VPN	Suporte SSL VPN com as seguintes funcionalidades: Conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface WEB Funcionalidades de VPN SSL sejam atendidas sem o uso de cliente Atribuição de endereço IP nos clientes remotos de VPN Atribuição de DNS nos clientes remotos de VPN Políticas de controle de aplicações, IPS, para trafego dos clientes remotos conectados na VPN SSL Autenticação via AD/LDAP, Secure id, certificado padrão ICP-Brasil e base de usuários local Túnel VPN client-to-site do cliente a plataforma de segurança, fornecendo uma solução de single-sign-on aos usuários, integrando-se com as ferramentas de Windows-logon Aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos tuneis SSL Agente de VPN SSL client-to-site deve ser compatível com pelo menos: Windows 7, Windows 8, Windows 10 (home) e Mac Osx Suporte e licença para pelo menos 2000 conexões remotas simultâneas VPN SSL
Controle de acesso à Internet	Filtro de URL HTTP e HTTPS
	Filtro de conteúdo HTTP
	Controle de downloads/uploads de arquivos pelo nome, tipo ou extensão do arquivo
	Controle de acesso à internet por domínio
	Controle de acesso à internet por categorias de sites web
	Controle de acesso à internet por lista de sites web proibidos (blacklist) customizável
	Controle de acesso à internet por lista de sites web permitidos (whitelist) customizável
	Mecanismo automático para detecção e bloqueio em tempo real de tráfego (inbound/outbound) originado por códigos maliciosos, tipo malwares ou spywares
	Mecanismo automático para detecção de tráfego tunelado na porta 80
	Páginas de erro e bloqueio customizáveis
	Compatibilidade com filtros de busca segura (safe-search filters), oferecidos por sites web de busca
	Controle de acesso por definição e aplicação das regras com expressões regulares
	Liberação/bloqueio de componentes específicos de sites de redes sociais, tais como chat e comentários do site wwwfacebookcom ou postagem no site wwwtwittercom
	Controle de acesso por geolocalização
Categorização de sites web	Base de dados com no mínimo 15 (quinze) milhões de URL's cadastradas, e pelo menos 45 (quarenta e cinco) categorias previamente definidas e possibilidade de criação de novas categorias personalizadas
	A classificação/categorização de sites de acordo com o assunto
	Mecanismo de cadastro de novas URLs junto ao fabricante para a devida categorização
	Mecanismo de reclassificação, quando necessário
Atualização da base de sites	Atualização automática da base de sites pela solução, via Internet, em dias e horários customizáveis
	Atualização transparente, sem comprometer a execução dos serviços, principalmente no caso de falhas no acesso à base de sites
	Mecanismos de manutenção da base de sites incluindo a reclassificação de sites antes “maliciosos” que foram “descontaminados”, para o retorno do acesso à normalidade
Definição de políticas para a modelagem do tráfego	IP de origem
	IP de destino
	Porta TCP/UDP de destino
	URL de destino
	Aplicação de camada 7

Gerenciamento remoto	Deve permitir o provisionamento e configuração de maneira automática, sem a necessidade de intervenção manual, quando ligado e conectado à rede
CARACTERÍSTICAS MÍNIMAS DOS EQUIPAMENTOS SD-WAN DAS SEDES E ÓRGÃOS (EXCETO DO DATACENTER)	
Interface Gigabit	Três interfaces Gigabit Ethernet (1000Base-T) que serão utilizadas para outros links ou na rede interna da DPRJ
	Três interfaces 10Gigabit Ethernet (10Gbase-SR) que serão utilizadas para outros links ou na rede interna da DPRJ
Fonte de alimentação	Deverá ter no mínimo duas fontes de alimentação (redundantes)
Throughtput	Deverá possuir throughtput mínimo de 5.8 Gbps (cinco ponto oito gigabits por segundo) para SSL inspection ou NGFW ou Application Control
	Deverá possuir throughtput mínimo de 5.8 Gbps (cinco ponto oito gigabits por segundo) para tráfego VPN
	Deverá possuir throughtput mínimo de 5.8 Gbps (cinco ponto oito gigabits por segundo) para IPS
Sessões simultâneas	Deverá suportar no mínimo 2.000.000 (dois milhões) de sessões de firewall simultâneas
Funcionalidade NGFW	O equipamento deverá possuir funcionalidade NGFW (Next Generation Firewall) reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões
Análise de conteúdo de aplicações	A plataforma deverá ser otimizada para análise de conteúdo de aplicações em camada 7
Tipo de equipamento	Deverá ser do tipo appliance, não sendo aceito equipamento do tipo servidor e com sistema operacional de uso genérico
Funcionalidades	anti-spoofing, configurável por segmento de rede de modo que seja possível utilizar o próprio endereçamento da interface ou especificar quais redes serão utilizadas como referência para permitir/negar o ingresso de um pacote
	Deverá permitir a configuração de ISP (rota default estática) com a utilização de probe para verificar a disponibilidade do provedor
	A probe deve permitir verificar o acesso HTTP a pelo menos 1 (um) site web e deve considerar o ISP indisponível em caso de falha
	As funcionalidades de controle de aplicações, filtro de URLs, VPN IPSec e SSL, QoS, SSL Decryption e protocolos de roteamento dinâmico deverão operar em caráter permanente, podendo ser utilizadas durante toda a vigência do contrato
	Policy based routing ou policy based forwarding
	Jumbo Frames
	Servidor DHCP em IPv4 e IPv6
	Suportar IGMP, v2 e v3
	Permitir a administração remota, protegida por autenticação usuário/senha e utilizando pelo menos os protocolos SSHv2 e HTTPS
	Roteamento IP Multicast através do protocolo PIM nas versões 1 e 2 e nos modos Sparse Mode e Dense Mode, não sendo exigida a implementação dos dois modos de forma simultânea
	Roteamento estático, OSPF, BGP e PBR (Policy Base Routing)
	MP-BGP, ou seja, encaminhamento de tráfego IPv4 e IPv6, ou suportar VRF
	Cliente NTP
	SNMP nas versões 2c e 3 com restrição dos endereços para consultas
	Protocolo de informações de fluxo como Netflow, sFlow, IPFIX ou similar
	NAT dinâmico (Many-to-1)
	NAT dinâmico (Many-to-Many)
	NAT estático (1-to-1)

Deverá suportar NAT dos seguintes tipos	NAT estático (1-to-1)
	NAT estático (Many-to-Many)
	NAT estático bidirecional 1-to-1
	Tradução de porta (PAT)
	NAT de origem
	NAT de destino
	NAT de origem e NAT de destino simultaneamente
Controle de política de firewall	O controle de aplicações por grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias
	Controle, inspeção e descriptografia de SSL por política para trafego de entrada (inbound) e saída (outbound)
	Suporte offload de certificado em inspeção de conexões SSL de entrada (inbound)
	Permissão de bloqueio de, pelo menos, os seguintes tipos de arquivos ou extensões: bat, cab, dll, exe, pif, e reg
	Suporte a objetos e regras multicast
	O agendamento de políticas em horários pré-definidos, de maneira automática
	Suporte a criação de políticas com data de expiração
Controle de aplicações	Capacidade de reconhecer aplicações, independente de porta e protocolo
	Capacidade de balancear o tráfego das aplicações entre múltiplos links, simultaneamente
	Capacidade de definição de qual link será utilizado em situação normal por determinada aplicação
	Liberação e o bloqueio das aplicações, sem a necessidade de especificação de portas e protocolos
	Reconhecimento das diversas aplicações diferentes, incluindo, mas não limitado: peer-to-peer, redes sociais, acessoremoto, update de software, protocolos de rede, voip, audio, vídeo, proxy, mensageria instantânea, compartilhamento de arquivos, e-mail
	Habilidade de inspecionar o payload de pacote de dados com o objetivo de detectar através de expressões regulares assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo
	A capacidade de identificar o uso de táticas evasivas, ou seja, visualizar e controlar as aplicações e os ataques que ulizam comunicações criptografadas, tais como Skype e ataques utilizando a porta 443
	A capacidade de decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo, incluindo, mas não limitado a Yahoo Instant Messenger ou Whatsapp usando HTTP. A decodificação de protocolo também deve identificar funcionalidades específicas dentro de uma aplicação, incluindo, mas não limitado a compartilhamento de arquivo dentro do Webex. Além de detectar arquivos e outros conteúdos que devem ser inspecionados de acordo as regras de segurança implementadas
	A possibilidade da liberação e do bloqueio das aplicações (ou de suas funcionalidades) por usuário, grupo de usuários, endereço IP ou rede específica
	Atualização automática da base de assinaturas de aplicações

	A possibilidade de adicionar controle de aplicações em todas as regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras
	A permissão de solicitação de inclusão de aplicações na base de assinaturas de aplicações do fabricante
	A função de alertar o usuário quando uma aplicação for bloqueada
	A possibilidade de diferenciação e controle de partes das aplicações como, por exemplo, permitir o Gtalk chat mas bloquear a transferência de arquivos, permitir acesso ao Facebook mas bloquear a visualização de vídeos, permitir acesso ao WhatsApp mas bloquear a transferência de arquivos
	A possibilidade de diferenciação de aplicações Proxies (ghostsurf, freegate, ultrasurf, tor, etc) possuindo granularidade de controle/políticas para os mesmos
	A possibilidade da criação de grupos estáticos de aplicações e grupos dinâmicos de aplicações baseados em características das aplicações como: tecnologia utilizada nas aplicações (client-server, browser based, network protocol, etc), nível de risco da aplicação, aplicações que usem técnicas evasivas, utilizadas por malwares, como transferência de arquivos e/ou uso excessivo de banda, etc
Controle de prevenção de ameaças	Módulo de IPS integrado no equipamento
	Assinaturas de prevenção de intrusão (IPS)
	A sincronização das assinaturas de IPS quando implementado em alta disponibilidade a ativo/ativo e a ativo/passivo (quando aplicável)
	Mecanismos de inspeção de IPS por meio da análise do estado da conexão, do protocolo, de anomalias de protocolo, da fragmentação, da remontagem e da malformação de pacotes
	Capacidade de impedimento de ataques básicos e bem conhecidos como Synflood, ICMPflood, UDPflood, etc
	Detecção e bloqueio da origem de port scans
	A mitigação de ataques DoS e DDoS
	A prevenção de ataques de buffer overflow
	A possibilidade de criação de assinaturas customizadas
	O suporte a bloqueio de arquivos por tipo
	A Identificação e o bloqueio de comunicação com botnets
	Suporte a várias técnicas de prevenção, incluindo Drop (cliente, servidor e ambos)
	Suporte a referência cruzada com CVE (Common Vulnerabilities and Exposures)
	Suporte a captura de pacotes (PCAP), por assinatura de IPS
	Proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms
	Proteção contra downloads involuntários usando HTTP ou HTTPS de arquivos executáveis
	Rastreamento de vírus em pdf
	Inspeção em arquivos comprimidos que uilizam o algoritmo deflate, como: zip e gzip
	A configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas do firewall, considerando usuários, grupos de usuários, origem, destino, zonas de segurança, etc, ou seja, cada política de firewall poderá ter uma configuração diferente de IPS, sendo essas políticas por usuários, grupos de usuário, origem, destino, zonas de segurança
	A inspeção de arquivos incorporados em outros arquivos ou arquivos que tenham sua extensão alterada na tentativa de contornar sua detecção
	A capacidade de criação de políticas baseadas na visibilidade e controle de quem (usuários e grupos de usuários) está utilizando quais aplicações através da integração com serviços de diretório, autenticação via Ldap, Microsoft Active Directory e base de dados local
	Autenticação Kerberos

Controle de usuários	A capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no Domain Controller, nem nas estações dos usuários, com expansão a portal captivo residente no próprio equipamento
	Suporte a accounting Microsoft NPS como RSSO, Radius Accounting ou similar
	Integração ao Microsoft Active Directory, permitindo identificar usuários dentro de grupos, mesmo que estejam em uma hierarquia de grupo dentro de grupo
	Suporte a identificação de múltiplos usuários conectados, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão em uso
	Suporte a identificação de usuários via certificados digitais ICP-Brasil para conexões a serviços via SSL VPN
	Atualização da identificação de um usuário caso este mude de endereço IP e mesmo que mais de um dispositivo esteja sendo utilizado de forma simultânea, evitando a necessidade de que sejam configurados endereços fixos
Suporte a QoS	A capacidade de controlar as aplicações por políticas de máximo de largura de banda por aplicação, tanto de áudio como de vídeo streaming
	A funcionalidade de configurar horários para navegação, permitindo controle por usuário e tempo
	A criação de políticas de QoS por usuário/grupo do LDAP/AD, aplicações (traffic shaping) e interface física ou lógica do equipamento
	Priorização de protocolos de voz e vídeo como H323, SIP, SCCP, MGCP e aplicações como Skype, Teams, Hangout e similares
	Suporte a conformação de tráfego com, pelo menos, os seguintes métodos: Traffic Policing e Traffic Shaping
	Classificação de tráfego com base no campo DSCP
	A marcação e priorização do tráfego previamente classificado com base no campo DSCP
Suporte à VPN	VPN client-to-site
	Suporte IPSec VPN, com suporte a AES e autenticação via cer ficado IKE PKI
	VPN IPSec com capacidade de implementar túneis site-to-site do tipo hub-and-spoke
	O estabelecimento do túnel utilizando uma “chave secreta” ou certificados digitais
	Implementação de IKEv1 e IKEv2
	Suporte pelo menos aos seguintes algoritmos de criptografia: 3DES, AES-128, AES-192 e AES256
	Suporte pelo menos aos seguintes algoritmos de autenticação: MD5, SHA-1, SHA-256, SHA-384, SHA-512
	Suporte SSL VPN com as seguintes funcionalidades: Conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface WEB Funcionalidades de VPN SSL sejam atendidas sem o uso de cliente Atribuição de endereço IP nos clientes remotos de VPN Atribuição de DNS nos clientes remotos de VPN Políticas de controle de aplicações, IPS, para trafego dos clientes remotos conectados na VPN SSL Autenticação via AD/LDAP, Secure id, certificado padrão ICP-Brasil e base de usuários local Túnel VPN client-to-site do cliente a plataforma de segurança, fornecendo uma solução de single-sign-on aos usuários, integrando-se com as ferramentas de Windows-logon Aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos tuneis SSL Agente de VPN SSL client-to-site deve ser compatível com pelo menos: Windows 7, Windows 8, Windows 10 (home) e Mac Osx Suporte e licença para pelo menos 2000 conexões remotas simultâneas VPN SSL
	Filtro de URL HTTP e HTTPS
	Filtro de conteúdo HTTP
	SSL Scanner
	Proxy transparente HTTP/HTTPS, proxy explícito e portal captivo, por segmento de rede

Filtro de URLs	Cache de dados
	Bloqueio de acesso com mensagem customizada, de forma a permitir que o usuário solicite a liberação por meio de formulário ou justificativa
	Monitoramento do tráfego internet independente de plataforma, sistema operacional ou aplicação
	Filtragem sem necessidade da instalação de agentes nas estações
Controle de acesso à Internet	Regras baseadas tanto na requisição quanto na resposta HTTP
	Regras baseadas em horário do dia
	Controle de downloads/uploads de arquivos pelo nome, tipo ou extensão do arquivo
	Controle de acesso à internet por domínio
	Controle de acesso à internet por categorias de sites web
	Controle de acesso à internet por lista de sites web proibidos (blacklist) customizável
	Controle de acesso à internet por lista de sites web permitidos (whitelist) customizável
	Mecanismo automático para detecção e bloqueio em tempo real de tráfego (inbound/outbound) originado por códigos maliciosos, tipo malwares ou spywares
	Mecanismo automático para detecção de tráfego tunelado na porta 80
	Páginas de erro e bloqueio customizáveis
	Compatibilidade com filtros de busca segura (safe-search filters), oferecidos por sites web de busca
	Controle de acesso por definição e aplicação das regras com expressões regulares
	Liberação/bloqueio de componentes específicos de sites de redes sociais, tais como chat e comentários do site www.facebook.com ou postagem no site www.twitte.rcom
	Controle de acesso por geolocalização
Categorização de sites web	Base de dados com no mínimo 15 (quinze) milhões de URL's cadastradas, e pelo menos 45 (quarenta e cinco) categorias previamente definidas e possibilidade de criação de novas categorias personalizadas
	A classificação/categorização de sites de acordo com o assunto
	Mecanismo de cadastro de novas URLs junto ao fabricante para a devida categorização
	Mecanismo de reclassificação, quando necessário
Atualização da base de sites	Atualização automática da base de sites pela solução, via Internet, em dias e horários customizáveis
	Atualização transparente, sem comprometer a execução dos serviços, principalmente no caso de falhas no acesso à base de sites
	Mecanismos de manutenção da base de sites incluindo a reclassificação de sites antes “maliciosos” que foram “descontaminados”, para o retorno do acesso à normalidade
Definição de políticas para a modelagem do tráfego	IP de origem
	IP de destino
	Porta TCP/UDP de destino
	URL de destino
	Aplicação de camada 7
Gerenciamento remoto	Deve permitir o provisionamento e configuração de maneira automática, sem a necessidade de intervenção manual, quando ligado e conectado à rede

Status
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Ciente
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende

Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende

Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende

Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende

Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende

Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
atende
Atende
Atende
Atende
Atende

Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende

Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
atende
Atende
Atende
Atende
Atende
Atende

Atende
Atende
Atende
atende
Atende
atende
atende
Atende
Atende
atende
Atende
atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende

Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende
Atende

Documento
https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-fortiwifi-40f-series.pdf https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-fortiwifi-60f-series.pdf https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-fortiwifi-80f-series.pdf https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-100f-series.pdf
https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-fortiwifi-40f-series.pdf https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-fortiwifi-60f-series.pdf https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-fortiwifi-80f-series.pdf https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-100f-series.pdf
https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-fortiwifi-40f-series.pdf https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-fortiwifi-60f-series.pdf https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-fortiwifi-80f-series.pdf https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-100f-series.pdf
https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf
https://docs.fortinet.com/document/fortigate/6.0.0/handbook/240599/application-control
https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-fortiwifi-40f-series.pdf https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-fortiwifi-60f-series.pdf https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-fortiwifi-80f-series.pdf https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-100f-series.pdf
https://docs.fortinet.com/document/fortigate/6.0.0/handbook/178055/fortios-diagnostics
https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/626338/adding-a-static-route
https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/723056/link-monitoring-and-failover
-
https://docs.fortinet.com/document/fortigate/6.0.0/handbook/34912/policy-routing
https://docs.fortinet.com/document/fortigate/6.0.0/handbook/822669/interface-mtu-packet-size
https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/783526/dhcp-servers-and-relays https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/776785/dhcpv6-stateful-server
https://docs.fortinet.com/document/fortigate/7.2.0/new-features/64590/configure-the-frequency-of-igmp-queries-7-
https://docs.fortinet.com/document/fortigate/7.2.0/new-features/936614/restrict-ssh-and-telnet-jump-host-capabiliti https://docs.fortinet.com/document/fortigate/7.2.0/new-features/499047/new-default-certificate-for-https-administra
https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/4afb0436-a998-11e9-81a4-00505692583a/
https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/804259/static-routing https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/479509/dynamic-routing
https://docs.fortinet.com/document/fortigate/6.0.0/handbook/691160/routing-concepts
https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/149181/date-and-time-settings
https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/62595/snmp
https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/998643/netflow https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/505119/sflow
https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/922423/configuring-an-antivirus-profile
https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/943037/monitoring-performance-sla https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/208103/passive-wan-health-measurement

https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/188051/source-nat https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/728694/destination-nat
https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/188051/source-nat https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/728694/destination-nat
https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/188051/source-nat https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/728694/destination-nat
https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/188051/source-nat https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/728694/destination-nat
https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/188051/source-nat https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/728694/destination-nat
https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/188051/source-nat https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/728694/destination-nat
https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/188051/source-nat https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/728694/destination-nat
https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/188051/source-nat https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/728694/destination-nat
https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/188051/source-nat https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/728694/destination-nat
https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/627219/nat66-nat46-nat64-and-dns-64
https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/302748/application-control
https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/669193/ssl-based-application-detection-ove
https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/669193/ssl-based-application-detection-ove
https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/610893/supported-file-types
https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/4afb0436-a998-11e9-81a4-00505692583a/
https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/656084/firewall-policy
https://docs.fortinet.com/document/fortimanager/7.0.0/administration-guide/156162/configuring-policy-details https://docs.fortinet.com/document/fortimanager/7.0.0/administration-guide/958981/schedule-a-policy-package-inst
https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/836937/configuring-an-application-sensor
https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/257828/sd-wan-components-and-design-pr
https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/270527/specify-an-sd-wan-zone-in-static-ro
https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/243446/ngfw-policy
https://www.fortiguard.com/appcontrol
https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/969330/proxy-mode-inspection
https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/4afb0436-a998-11e9-81a4-00505692583a/

https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/4afb0436-a998-11e9-81a4-00505692583a/
https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/4afb0436-a998-11e9-81a4-00505692583a/
https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/4afb0436-a998-11e9-81a4-00505692583a/
https://docs.fortinet.com/document/fortigate/6.0.0/handbook/721617/configuring-profiles
https://www.fortiguard.com/faq/appctrlsubmit
https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/4afb0436-a998-11e9-81a4-00505692583a/
https://www.fortiguard.com/search?q=hangouts&type=app&engine=1
https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/243446/ngfw-policy
https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/19814/basic-category-filters-and-overrides
https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/565562/intrusion-prevention
https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/213498/signature-based-defense
https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/127856/resume-ips-scanning-of-iccp-traffic-
https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/213498/signature-based-defense#Engine
https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf
https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf
https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf
https://www.fortiguard.com/search?q=buffer+overflow&engine=1
https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/4afb0436-a998-11e9-81a4-00505692583a/
https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf
https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf
https://docs.fortinet.com/document/fortigate/7.4.0/hardware-acceleration/202492/config-fp-anomaly
https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/535363/ips-signature-filter-options
https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/462154/using-the-packet-capture-tool
https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/610893/supported-file-types
https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/610893/supported-file-types
https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/610893/supported-file-types
https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/610893/supported-file-types

https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/243446/ngfw-policy
https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/969330/proxy-mode-inspection
https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/656084/firewall-policy
https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/771627/multiple-ldap-servers-in-kerberos-k
https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/771627/multiple-ldap-servers-in-kerberos-k
https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/107067/enabling-active-directory-recursive-
https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/29900/user-groups
https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/443027/users
https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/275338/changing-traffic-shaper-bandwidth-
https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/243446/ngfw-policy
https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/371960/local-in-and-local-out-traffic-matchi
https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/933502/shared-traffic-shaper https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/867974/scanning-msrp-traffic https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/813032/dscp-matching-and-dscp-marking
https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/673634/traffic-shaping-policies https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/297431/traffic-shaping
https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/813032/dscp-matching-and-dscp-marking
https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/813032/dscp-matching-and-dscp-marking
https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/190553/remote-access
https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/526306/ike-mode-config-clients
https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/978793/advpn
https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/560886/pre-shared-key-vs-digital-certificate
https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/167137/choosing-ike-version-1-and-2
https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/604285/phase-2-configuration
https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/604285/phase-2-configuration

https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/4afb0436-a998-11e9-81a4-00505692583a/
https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf
https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf
https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/610893/supported-file-types
https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/1706/static-application-steering-with-a-mar
https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/675558/fortiguard-filter
https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/725397/web-content-filter
https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/725397/web-content-filter
https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf
https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/352916/using-custom-internet-service-in-po
https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/131140/replacement-messages
https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/12534/dns-safe-search
https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/931220/configuring-web-filter-profiles-with-
https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/615462/url-filter
https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/286826/geography-based-addresses
https://www.fortiguard.com/webfilter https://www.fortiguard.com/webfilter/categories
https://www.fortiguard.com/webfilter/categories
https://www.fortiguard.com/faq/wfratingsubmit
https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/408599/web-profile-override
https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/655726/scheduled-updates
https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/655726/scheduled-updates
https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/408599/web-profile-override
https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/1706/static-application-steering-with-a-mar
https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/1706/static-application-steering-with-a-mar
https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/1706/static-application-steering-with-a-mar
https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/1706/static-application-steering-with-a-mar
https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/1706/static-application-steering-with-a-mar

https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortimanager.pdf
[redacted]
https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-400f-series.pdf
https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-400f-series.pdf
https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-400f-series.pdf
https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-400f-series.pdf
https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-400f-series.pdf
https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-400f-series.pdf
https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-400f-series.pdf
https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-400f-series.pdf
https://docs.fortinet.com/document/fortigate/6.0.0/handbook/240599/application-control
https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-400f-series.pdf
https://docs.fortinet.com/document/fortigate/6.0.0/handbook/178055/fortios-diagnostics
https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/626338/adding-a-static-route
https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/723056/link-monitoring-and-failover
https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf
https://docs.fortinet.com/document/fortigate/6.0.0/handbook/34912/policy-routing
https://docs.fortinet.com/document/fortigate/6.0.0/handbook/822669/interface-mtu-packet-size
https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/783526/dhcp-servers-and-relays https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/776785/dhcpv6-stateful-server
https://docs.fortinet.com/document/fortigate/7.2.0/new-features/64590/configure-the-frequency-of-igmp-queries-7-
https://docs.fortinet.com/document/fortigate/7.2.0/new-features/936614/restrict-ssh-and-telnet-jump-host-capabiliti https://docs.fortinet.com/document/fortigate/7.2.0/new-features/499047/new-default-certificate-for-https-administra
https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/4afb0436-a998-11e9-81a4-00505692583a/
https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/804259/static-routing https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/479509/dynamic-routing
https://docs.fortinet.com/document/fortigate/6.0.0/handbook/691160/routing-concepts
https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/149181/date-and-time-settings
https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/62595/snmp
https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/998643/netflow https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/505119/sflow
https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/188051/source-nat https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/728694/destination-nat
https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/188051/source-nat https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/728694/destination-nat
https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/188051/source-nat

https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/728694/destination-nat
https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/188051/source-nat https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/728694/destination-nat
https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/188051/source-nat https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/728694/destination-nat
https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/188051/source-nat https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/728694/destination-nat
https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/188051/source-nat https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/728694/destination-nat
https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/188051/source-nat https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/728694/destination-nat
https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/188051/source-nat https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/728694/destination-nat
https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/302748/application-control
https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/669193/ssl-based-application-detection-ove
https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/669193/ssl-based-application-detection-ove
https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/610893/supported-file-types
https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/4afb0436-a998-11e9-81a4-00505692583a/
https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/656084/firewall-policy
https://docs.fortinet.com/document/fortimanager/7.0.0/administration-guide/156162/configuring-policy-details https://docs.fortinet.com/document/fortimanager/7.0.0/administration-guide/958981/schedule-a-policy-package-inst
https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/836937/configuring-an-application-sensor
https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/257828/sd-wan-components-and-design-pr
https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/270527/specify-an-sd-wan-zone-in-static-ro
https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/243446/ngfw-policy
https://www.fortiguard.com/appcontrol
https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/969330/proxy-mode-inspection
https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/4afb0436-a998-11e9-81a4-00505692583a/
https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/4afb0436-a998-11e9-81a4-00505692583a/
https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/4afb0436-a998-11e9-81a4-00505692583a/
https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/4afb0436-a998-11e9-81a4-00505692583a/

https://docs.fortinet.com/document/fortigate/6.0.0/handbook/721617/configuring-profiles

https://www.fortiguard.com/faq/appctrlsubmit

https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/4afb0436-a998-11e9-81a4-00505692583a/

https://kb.fortinet.com/kb/documentLink.do?externalID=FD48878

https://www.fortiguard.com/search?q=hangouts&type=app&engine=1

https://www.fortiguard.com/search?q=hangouts&type=app&engine=1

https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/19814/basic-category-filters-and-overrides

https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/565562/intrusion-prevention

https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/213498/signature-based-defense

https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/127856/resume-ips-scanning-of-iccp-traffic-

https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/213498/signature-based-defense#Engine

https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf

https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf

https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf

https://www.fortiguard.com/search?q=buffer+overflow&engine=1

https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/4afb0436-a998-11e9-81a4-00505692583a/

https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf

https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf

https://docs.fortinet.com/document/fortigate/7.4.0/hardware-acceleration/202492/config-fp-anomaly

https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/535363/ips-signature-filter-options

https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/462154/using-the-packet-capture-tool

https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/610893/supported-file-types

https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/610893/supported-file-types

https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/610893/supported-file-types

https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/610893/supported-file-types

https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/243446/ngfw-policy

https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/969330/proxy-mode-inspection

https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/656084/firewall-policy

https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/771627/multiple-ldap-servers-in-kerberos-k

https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/771627/multiple-ldap-servers-in-kerberos-k

https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/29900/user-groups

https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/107067/enabling-active-directory-recursive-

https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/29900/user-groups

https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/371626/ssl-vpn

https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/443027/users

https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/275338/changing-traffic-shaper-bandwidth-

https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/243446/ngfw-policy

https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/371960/local-in-and-local-out-traffic-matchi

https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/933502/shared-traffic-shaper
https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/867974/scanning-msrp-traffic
https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/813032/dscp-matching-and-dscp-marking
https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/673634/traffic-shaping-policies
https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/297431/traffic-shaping

https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/813032/dscp-matching-and-dscp-marking

https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/813032/dscp-matching-and-dscp-marking

https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/190553/remote-access

https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/526306/ike-mode-config-clients

https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/978793/advpn

https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/560886/pre-shared-key-vs-digital-certificate

https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/167137/choosing-ike-version-1-and-2

https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/604285/phase-2-configuration

https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/604285/phase-2-configuration

https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/4afb0436-a998-11e9-81a4-00505692583a/

https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf

https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf

https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/669193/ssl-based-application-detection-ove

https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/15908/transparent-proxy

https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/72214/cache-service-and-video-caching

https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/4afb0436-a998-11e9-81a4-00505692583a/

https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/379794/passive-health-check-measurement

https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/771627/multiple-ldap-servers-in-kerberos-k

https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/243446/ngfw-policy

https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/243446/ngfw-policy

https://docs.fortinet.com/document/fortigate/7.2.5/administration-guide/610893/supported-file-types

https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/1706/static-application-steering-with-a-mar

https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/675558/fortiguard-filter

https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/725397/web-content-filter

https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/725397/web-content-filter

https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf

https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/352916/using-custom-internet-service-in-po

https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/131140/replacement-messages

https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/12534/dns-safe-search

https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/931220/configuring-web-filter-profiles-with-

https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/615462/url-filter

https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/286826/geography-based-addresses

https://www.fortiguard.com/webfilter
https://www.fortiguard.com/webfilter/categories

https://www.fortiguard.com/webfilter/categories

https://www.fortiguard.com/faq/wfratingsubmit

https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/408599/web-profile-override

https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/655726/scheduled-updates

https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/655726/scheduled-updates

https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/408599/web-profile-override

https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/1706/static-application-steering-with-a-mar

https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/1706/static-application-steering-with-a-mar

https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/1706/static-application-steering-with-a-mar

https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/1706/static-application-steering-with-a-mar

https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/1706/static-application-steering-with-a-mar

https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortimanager.pdf

Observação
Página 6
Página 6
Página 6
Página 6
Página 7
Página 7
Página 7
Página 7
Página 7
Página 7
Página 7
Página 7
A partir da página 5
Sem Página
Página 1
Página 1
Página 1
Página 1
Sem Página
Sem Página
Sem Página
-
Sem Página
Sem Página
Sem Página
Sem Página
Sem Página
Página 1737
Sem Página
Sem Página
Sem Página
Sem Página
Sem Página
Sem Página
Sem Página

Sem Página
Sem Página
Sem Página
Sem Página
Sem Página
Sem Página
Sem Página
Sem Página
Sem Página
É suportado a tradução completa por endereço (NAT66), o que entendemos ser superior a tradução apenas de prefixo (NTPv6)
Sem Página
Sem Página
Sem Página
Suporta extensões do tipo bat, cab e exe.
Página 617
Sem Página
Sem Página
Sem Página
Sem Página
Sem Página
Sem Página
Sem Página
Sem Página
Páginas 919 e 920

Páginas 467 e 826
Páginas 919 e 920
Página 110
Sem Página
Sem Página
Páginas 923 e 924
Sem Página
Sem Página
Sem Página
Sem Página
Sem Página
Sem Página
Página 11
Página 11
DDoS Página 11 - DDoS deverá ser entregue pela solução de BackBone da Operadora
Sem Página
Página 838
Página 12
Página 7
Sem Página
Sem Página
Sem Página
Sem Página
Sem Página
Sem Página
Sem Página

Sem Página
Sem Página
Sem Página
Sem Página
Sem Página
Sem Página
Sem Página
Sem Página
Sem Página
Sem Página
Sem Página
Sem Página
Sem Página
Sem Página
Sem Página
Sem Página
Sem Página
Sem Página
Sem Página
Sem Página
Sem Página

A partir da página 557
Página 7
Página 7
Sem Página
Sem Página
Sem Página
Sem Página
Sem Página
Página 7
Sem Página
Sem Página
Sem Página
Sem Página
Sem Página
Sem Página
Sem Página
Sem Página
Sem Página
Sem Página
Sem Página
Sem Página
Sem Página
Sem Página
Sem Página
Sem Página
Sem Página
Sem Página

Sem Página
Página 6
Página 6
Página 7
Página 7
Página 7
Página 7
Página 7
Página 1
Sem Página
Página 1
Sem Página
Sem Página
Sem Página
A partir da página 5
Sem Página
Sem Página
Sem Página
Sem Página
Sem Página
Página 1737
Sem Página
Sem Página
Sem Página
Sem Página
Sem Página
Sem Página
Sem Página
Sem Página

Sem Página
Sem Página
Sem Página
Sem Página
Sem Página
Sem Página
Sem Página
Sem Página
Sem Página
Sem Página
Suporta extensões do tipo bat, cab e exe.
Página 617
Sem Página
Sem Página
Sem Página
Sem Página
Sem Página
Sem Página
Sem Página
Sem Página
Sem Página
Páginas 919 e 920
Páginas 467 e 826
Páginas 919 e 920
Página 110

Sem Página
Sem Página
Sem página
Páginas 923 e 924
Sem Página
Sem Página
Sem Página
Sem Página
Sem Página
Sem Página
Sem Página
Página 11
Página 11
DDoS Página 11 - DDoS deverá ser entregue pela solução de BackBone da Operadora
Sem Página
Página 838
Página 12
Página 7
Sem Página
Sem Página
Sem Página
Sem Página
Sem Página
Sem Página
Sem Página
Sem Página
Sem Página
Sem Página

Sem Página
Sem Página
Sem Página
Sem Página
Sem Página
Sem Página
Sem Página
Sem Página
Sem Página
Sem Página
Sem Página
Sem Página
Sem Página
Sem Página
Sem Página
Sem Página
Sem Página
Sem Página
Sem Página
Sem Página
A partir da página 557
Página 7
Página 7
Sem Página
Sem Página

Sem Página
Página 838
Sem Página
Sem Página
Sem Página
Sem Página
Sem Página
Sem Página
Sem Página
Sem Página
Página 7
Sem Página
Sem Página
Sem Página
Sem Página
Sem Página
Sem Página
Sem Página
Sem Página
Sem Página
Sem Página
Sem Página
Sem Página
Sem Página
Sem Página
Sem Página
Sem Página
Sem Página
Sem Página
Sem Página
Sem Página
Sem Página
Sem Página
Sem Página
Página 3

FortiGate FortiWiFi 40F Series

FG-40F, FG-40F-3G4G, FWF-40F, FWF-40F-3G4G

Highlights

Gartner Magic Quadrant Leader for both Network Firewalls and SD-WAN.

Security-Driven Networking with FortiOS delivers converged networking and security.

Unparalleled Performance with Fortinet's patented SoC processors.

Enterprise Security with consolidated AI / ML-powered FortiGuard Services.

Simplified Operations with centralized management for networking and security, automation, deep analytics, and self-healing.

Converged Next-Generation Firewall (NGFW) and SD-WAN

The FortiGate Next-Generation Firewall 40F series is ideal for building security-driven networks at distributed enterprise sites and transforming WAN architecture at any scale.

With a rich set of AI/ML-based FortiGuard security services and our integrated Security Fabric platform, the FortiGate FortiWiFi 40F series delivers coordinated, automated, end-to-end threat protection across all use cases.

FortiGate has the industry's first integrated SD-WAN and zero-trust network access (ZTNA) enforcement within an NGFW solution and is powered by one OS. FortiGate 40F automatically controls, verifies, and facilitates user access to applications, delivering consistency with a seamless and optimized user experience.

IPS	NGFW	Threat Protection	Interfaces
1 Gbps	800 Mbps	600 Mbps	Multiple GE RJ45 | WiFi variants

Available in

Appliance

Virtual

Hosted

Cloud

Container

FortiOS Everywhere

FortiOS, Fortinet's Advanced Operating System

FortiOS enables the convergence of high performing networking and security across the Fortinet Security Fabric. Because it can be deployed anywhere, it delivers consistent and context-aware security posture across network, endpoint, and multi-cloud environments.

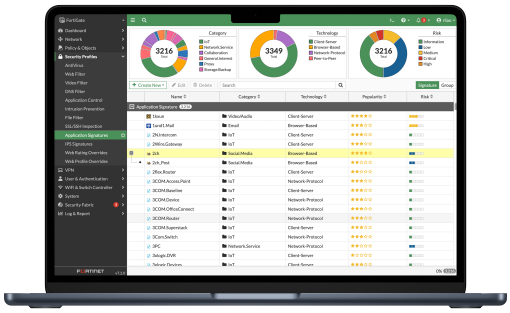
FortiOS powers all FortiGate deployments whether a physical or virtual device, as a container, or as a cloud service. This universal deployment model enables the consolidation of many technologies and use cases into organically built best-of-breed capabilities, unified operating system, and ultra-scalability. The solution allows organizations to protect all edges, simplify operations, and run their business without compromising performance or protection.

FortiOS dramatically expands the Fortinet Security Fabric's ability to deliver advanced AI/ML-powered services, inline advanced sandbox detection, integrated ZTNA enforcement, and more. It provides protection across hybrid deployment models for hardware, software, and Software-as-a-Service with SASE.

FortiOS expands visibility and control, ensures the consistent deployment and enforcement of a simplified, single policy and management framework. Its security policies enable centralized management across large-scale networks with the following key attributes:

- Interactive drill-down and topology viewers that display real-time status
- On-click remediation that provides accurate and quick protection against threats and abuses
- Unique threat score system correlates weighted threats with users to prioritize investigations

Intuitive easy to use view into the network and endpoint vulnerabilities



Visibility with FOS Application Signatures

FortiConverter Service

FortiConverter Service provides hassle-free migration to help organizations transition from a wide range of legacy firewalls to FortiGate Next-Generation Firewalls quickly and easily. The service eliminates errors and redundancy by employing best practices with advanced methodologies and automated processes. Organizations can accelerate their network protection with the latest FortiOS technology.

FortiGuard Services

Network and File Security

Services provide protection against network-based and file-based threats. This consists of Intrusion Prevention (IPS) which uses AI/M models to perform deep packet/SSL inspection to detect and stop malicious content, and apply virtual patching when a new vulnerability is discovered. It also includes Anti-Malware for defense against known and unknown file-based threats. Anti-malware services span both antivirus and file sandboxing to provide multi-layered protection and are enhanced in real-time with threat intelligence from FortiGuard Labs. Application Control enhances security compliance and offers real-time application visibility.

Web / DNS Security

Services provide protection against web-based threats including DNS-based threats, malicious URLs (including even in emails), and botnet/command and control communications. DNS filtering provides full visibility into DNS traffic while blocking high-risk domains, and protects against DNS tunneling, DNS infiltration, C2 server ID and Domain Generation Algorithms (DGA). URL filtering leverages a database of 300M+ URLs to identify and block links to malicious sites and payloads. IP Reputation and anti-botnet services prevent botnet communications, and block DDoS attacks from known sources.

SaaS and Data Security

Services address numerous security use cases across application usage as well as overall data security. This consists of Data Leak Prevention (DLP) which ensures data visibility, management and protection (including blocking exfiltration) across networks, clouds, and users, while simplifying compliance and privacy implementations. Separately, our Inline Cloud Access Security Broker (CASB) service protects data in motion, at rest, and in the cloud. The service enforces major compliance standards and manages account, user and cloud application usage. Services also include capabilities designed to continually assess your infrastructure, validate that configurations are working effectively and secure, and generate awareness of risks and vulnerabilities that could impact business operations. This includes coverage across IoT devices for both IoT detection and IoT vulnerability correlation.

Zero-Day Threat Prevention

Zero-day threat prevention entails Fortinet's AI-based inline malware prevention, our most advanced sandbox service, to analyze and block unknown files in real-time, offering sub-second protection against zero-day and sophisticated threats across all NGFWs. The service also has a built-in MITRE ATT&CK® matrix to accelerate investigations. The service focuses on comprehensive defense by blocking unknown threats while streamlining incident response efforts and reducing security overhead.

OT Security

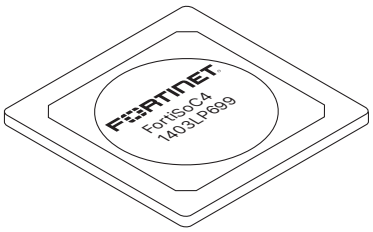
The service provides OT detection, OT vulnerability correlation, virtual patching, OT signatures, and industry-specific protocol decoders for overall robust defense of OT environments and devices.

Secure Any Edge at Any Scale

Powered by Security Processing Unit (SPU)

Traditional firewalls cannot protect against today's content- and connection-based threats because they rely on off-the-shelf hardware and general-purpose CPUs, causing a dangerous performance gap. Fortinet's custom SPU processors deliver the power you need—up to 520Gbps—to detect emerging threats and block malicious content while ensuring your network security solution does not become a performance bottleneck.

ASIC Advantage



Secure SD-WAN ASIC SOC4

- Combines a RISC-based CPU with Fortinet's proprietary Security Processing Unit (SPU) content and network processors for unmatched performance
- Delivers industry's fastest application identification and steering for efficient business operations
- Accelerates IPsec VPN performance for best user experience on direct internet access
- Enables best of breed NGFW Security and Deep SSL Inspection with high performance
- Extends security to access layer to enable SD-Branch transformation with accelerated and integrated switch and access point connectivity

FortiCare Services

Fortinet is dedicated to helping our customers succeed, and every year FortiCare Services help thousands of organizations get the most from our Fortinet Security Fabric solution. Our lifecycle portfolio offers Design, Deploy, Operate, Optimize, and Evolve services. Operate services offer device-level FortiCare Elite service with enhanced SLAs to meet our customer's operational and availability needs. In addition, our customized account-level services provide rapid incident resolution and offer proactive care to maximize the security and performance of Fortinet deployments.

Use Cases

Next Generation Firewall (NGFW)

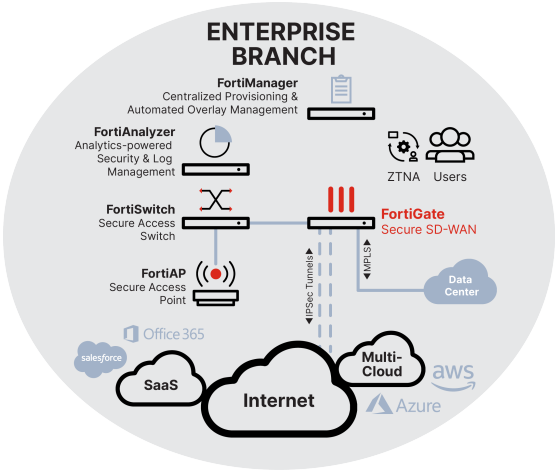
- FortiGuard Labs' suite of AI-powered Security Services—natively integrated with your NGFW—secures web, content, and devices and protects networks from ransomware and sophisticated cyberattacks
- Real-time SSL inspection (including TLS 1.3) provides full visibility into users, devices, and applications across the attack surface
- Fortinet's patented SPU (Security Processing Unit) technology provides industry-leading high-performance protection

Secure SD-WAN

- FortiGate WAN Edge powered by one OS and unified security and management framework and systems transforms and secures WANs
- Delivers superior quality of experience and effective security posture for work-from-any where models, SD-Branch, and cloud-first WAN use cases
- Achieve operational efficiencies at any scale through automation, deep analytics, and self-healing

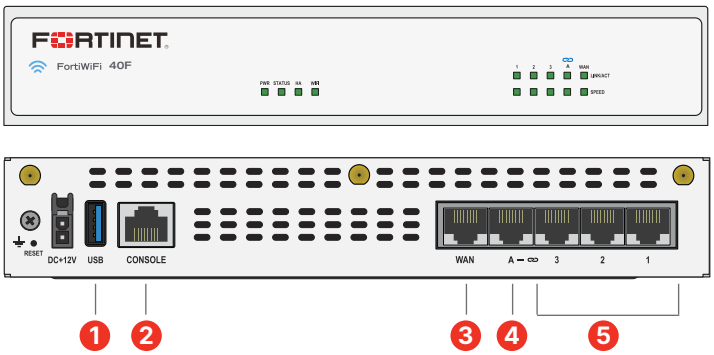
Universal ZTNA

- Control access to applications no matter where the user is and no matter where the application is hosted for universal application of access policies
- Provide extensive authentications, checks, and enforce policy prior to granting application access - every time
- Agent-based access with FortiClient or agentless access via proxy portal for guest or BYOD



Hardware

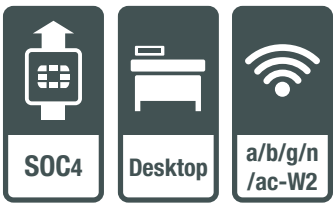
FortiGate FortiWifi 40F Series



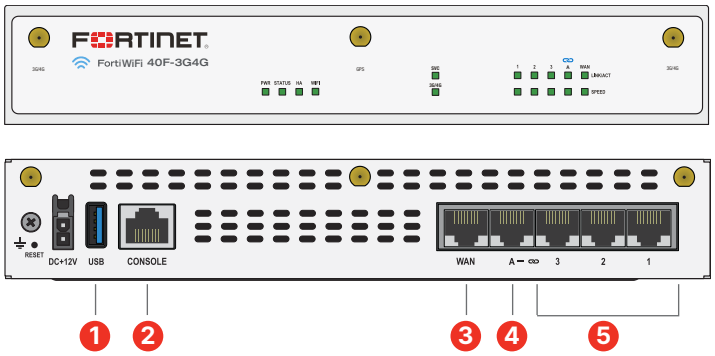
Interfaces

1. 1 x USB Port
2. 1 x Console Port
3. 1 x GE RJ45 WAN Port
4. 1 x GE RJ45 FortiLink Port
5. 3 x GE RJ45 Ethernet Ports

Hardware Features



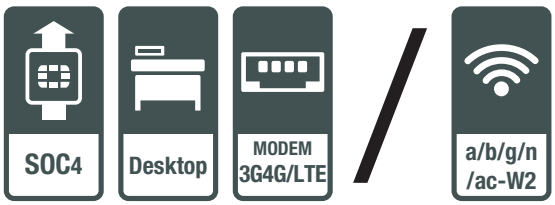
FortiGate FortiWifi 40F-3G4G



Interfaces

1. 1 x USB Port
2. 1 x Console Port
3. 1 x GE RJ45 WAN Port
4. 1 x GE RJ45 FortiLink Port
5. 3 x GE RJ45 Ethernet Ports

Hardware Features



Compact and Reliable Form Factor

Designed for small environments, you can place it on a desktop or wall-mount it. It is small, lightweight, yet highly reliable with a superior MTBF (Mean Time Between Failure), minimizing the chance of a network disruption.

Access Layer Security

FortiLink protocol enables you to converge security and the network access by integrating the FortiSwitch into the FortiGate as a logical extension of the NGFW. These FortiLink enabled ports can be reconfigured as regular ports as needed.

Specifications

	FORTIGATE 40F	FORTIWIFI 40F	FORTIGATE 40F-3G4G	FORTIWIFI 40F-3G4G
Interfaces and Modules				
Hardware Accelerated GE RJ45 WAN / DMZ Ports	1	1	1	1
Hardware Accelerated GE RJ45 Internal Ports	3	3	3	3
Hardware Accelerated GE RJ45 FortiLink Ports (Default)	1	1	1	1
Hardware Accelerated GE RJ45 PoE/+ Ports	0	0	0	0
Cellular Modem	-	-	3G4G LTE	3G4G LTE
Wireless Interface	0	Single Radio (2.4GHz/5GHz) 802.11 /a/b/g/n/ac-W2	0	Single Radio (2.4GHz/5GHz), 802.11 a/b/g/n/ac-W2
Antenna Ports (SMA)	0	3	3	6
USB Ports	1	1	1	1
Console Port (RJ45)	1	1	1	1
SIM Slots (Nano SIM)	0	0	2	2
Onboard Storage	0	0	0	0
Included Transceivers	0	0	0	0
System Performance — Enterprise Traffic Mix				
IPS Throughput [2]	1 Gbps			
NGFW Throughput [2, 4]	800 Mbps			
Threat Protection Throughput [2, 5]	600 Mbps			
System Performance and Capacity				
IPv4 Firewall Throughput (1518 / 512 / 64 byte, UDP)	5 / 5 / 5 Gbps			
Firewall Latency (64 byte, UDP)	2.97 µs			
Firewall Throughput (Packet per Second)	7.5 Mpps			
Concurrent Sessions (TCP)	700 000			
New Sessions/Second (TCP)	35 000			
Firewall Policies	5000			
IPsec VPN Throughput (512 byte) [1]	4.4 Gbps			
Gateway-to-Gateway IPsec VPN Tunnels	200			
Client-to-Gateway IPsec VPN Tunnels	250			
SSL-VPN Throughput	490 Mbps			
Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode)	200			
SSL Inspection Throughput (IPS, avg. HTTPS) [3]	310 Mbps			
SSL Inspection CPS (IPS, avg. HTTPS) [3]	320			
SSL Inspection Concurrent Session (IPS, avg. HTTPS) [3]	55 000			
Application Control Throughput (HTTP 64K) [2]	990 Mbps			
CAPWAP Throughput (HTTP 64K)	3.5 Gbps			
Virtual Domains (Default / Maximum)	10 / 10			
Maximum Number of FortiSwitches Supported	8			
Maximum Number of FortiAPs (Total / Tunnel)	16 / 8			
Maximum Number of FortiTokens	500			
High Availability Configurations	Active-Active, Active-Passive, Clustering			

Note: All performance values are “up to” and vary depending on system configuration.

[1] IPsec VPN performance test uses AES256-SHA256.

[2] IPS (Enterprise Mix), Application Control, NGFW and Threat Protection are measured with Logging enabled.

[3] SSL Inspection performance values use an average of HTTPS sessions of different cipher suites.

[4] NGFW performance is measured with Firewall, IPS and Application Control enabled.

[5] Threat Protection performance is measured with Firewall, IPS, Application Control and Malware Protection enabled.

Specifications

	FORTIGATE 40F	FORTIWIFI 40F	FORTIGATE 40F-3G4G	FORTIWIFI 40F-3G4G
Dimensions and Power				
Height x Width x Length (inches)	1.5 × 8.5 × 6.3		1.6 × 8.5 × 6.3	
Height x Width x Length (mm)	38.5 × 216 × 160		40.5 × 216 × 160	
Weight	2.2 lbs (1 kg)		2.2 lbs (1 kg)	
Form Factor (supports EIA/non-EIA standards)	Desktop		Desktop	
Input Rating	12Vdc, 3A		12Vdc, 3A	
Power Required	Powered by External DC Power Adapter, 100–240V AC, 50/60 Hz		Powered by external DC power adapter 100-240V AC, 50/60 Hz	
Current (Maximum)	100V AC / 0.2A, 240V AC / 0.1A		100V AC / 0.3A, 240V AC / 0.2A	
Power Consumption (Average / Maximum)	7.74 W / 9.46 W	14.6 W / 16.6 W	15.8 W / 18.6 W	18.6 W / 19.8 W
Heat Dissipation	52.55 BTU/h	56.64 BTU/h	63.5 BTU/h	67.6 BTU/h
Operating Environment and Certifications				
Operating Temperature	32°–104°F (0°–40°C)			
Storage Temperature	-31°–158°F (-35°–70°C)			
Humidity	10%–90% non-condensing			
Noise Level	Fanless 0 dBA			
Operating Altitude	Up to 7400 ft (2250 m)			
Compliance	FCC, ICES, CE, RCM, VCCI, BSMI, UL/cUL, CB			
Certifications	USGv6/IPv6			
Radio Specifications				
Multiple (MU) MIMO	N/A	3 × 3	N/A	3 × 3
Maximum Wi-Fi Speeds	N/A	1300 Mbps @ 5 GHz, 450 Mbps @ 2.4 GHz	N/A	1300 Mbps @ 5 GHz, 450 Mbps @ 2.4 GHz
Maximum Tx Power	N/A	20 dBm	N/A	20 dBm
Antenna Gain	N/A	3.5 dBi @ 5GHz, 5 dBi @ 2.4 GHz	N/A	3.5 dBi @ 5GHz, 5 dBi @ 2.4 GHz
Regional Compatibility				
Regions	N/A		All Regions	
Modem Model	N/A		Sierra Wireless EM7565 (2 SIM Slots, Active/Passive)	
LTE Category	N/A		CAT-12	
LTE Bands	N/A		B1, B2, B3, B4, B5, B7, B8, B9, B12, B13, B18, B19, B20, B26, B28, B29, B30, B32, B41, B42, B43, B46, B48, B66	
UMTS/HSPA+	N/A		B1, B2, B4, B5, B6, B8, B9, B19	
WCDMA	N/A		-	
CDMA 1xRTT/EV-DO Rev A	N/A		-	
GSM/GPRS/EDGE	N/A		-	
Module Certifications	N/A		FCC, ICES, CE, RCM, VCCI, BSMI, UL/cUL, CB	
Diversity	N/A		Yes	
MIMO	N/A		Yes	
GNSS Bias	N/A		Yes	

Subscriptions

Service Category	Service Offering	A-la-carte	Bundles		
			Enterprise Protection	Unified Threat Protection	Advanced Threat Protection
FortiGuard Security Services	IPS Service	•	•	•	•
	Anti-Malware Protection (AMP) — Antivirus, Mobile Malware, Botnet, CDR, Virus Outbreak Protection and FortiSandbox Cloud Service	•	•	•	•
	URL, DNS & Video Filtering Service	•	•	•	
	Anti-Spam		•	•	
	AI-based Inline Malware Prevention Service	•	•		
	Data Loss Prevention Service [1]	•	•		
	OT Security Service (OT Detection, OT Vulnerability correlation, Virtual Patching, OT Signature / Protocol Decoders) [1]	•			
	Application Control		included with FortiCare Subscription		
	CASB SaaS Control		included with FortiCare Subscription		
SD-WAN and SASE Services	SD-WAN Underlay Bandwidth and Quality Monitoring Service	•			
	SD-WAN Overlay-as-a-Service for SaaS-based overlay network provisioning	•			
	SD-WAN Connector for FortiSASE Secure Private Access	•			
	FortiSASE subscription including cloud management and 10Mbps bandwidth license [2]	•			
NOC and SOC Services	FortiGuard Attack Surface Security Service (IoT Detection, IoT Vulnerability Correlation, and Security Rating Updates) [1]	•	•		
	FortiConverter Service	•	•		
	Managed FortiGate Service	•			
	FortiGate Cloud (SMB Logging + Cloud Management)	•			
	FortiAnalyzer Cloud	•			
	FortiAnalyzer Cloud with SOCaaS	•			
	FortiGuard SOCaaS	•			
Hardware and Software Support	FortiCare Essentials	•			
	FortiCare Premium	•	•	•	•
	FortiCare Elite	•			
Base Services	Internet Service (SaaS) DB Updates	included with FortiCare Subscription			
	GeoIP DB Updates				
	Device/OS Detection Signatures				
	Trusted Certificate DB Updates				
	DDNS (v4/v6) Service				

1. Full features available when running FortiOS 7.4.1
2. Desktop Models only

FortiGuard Bundles

FortiGuard Labs delivers a number of security intelligence services to augment the FortiGate firewall platform. You can easily optimize the protection capabilities of your FortiGate with one of these FortiGuard Bundles.

FortiCare Elite

FortiCare Elite offers enhanced SLAs and quick issue resolution through a dedicated support team. It provides single-touch ticket handling, extended Extended End-of-Engineering-Support for 18 months, and access to the new FortiCare Elite Portal for a unified view of device and security health.

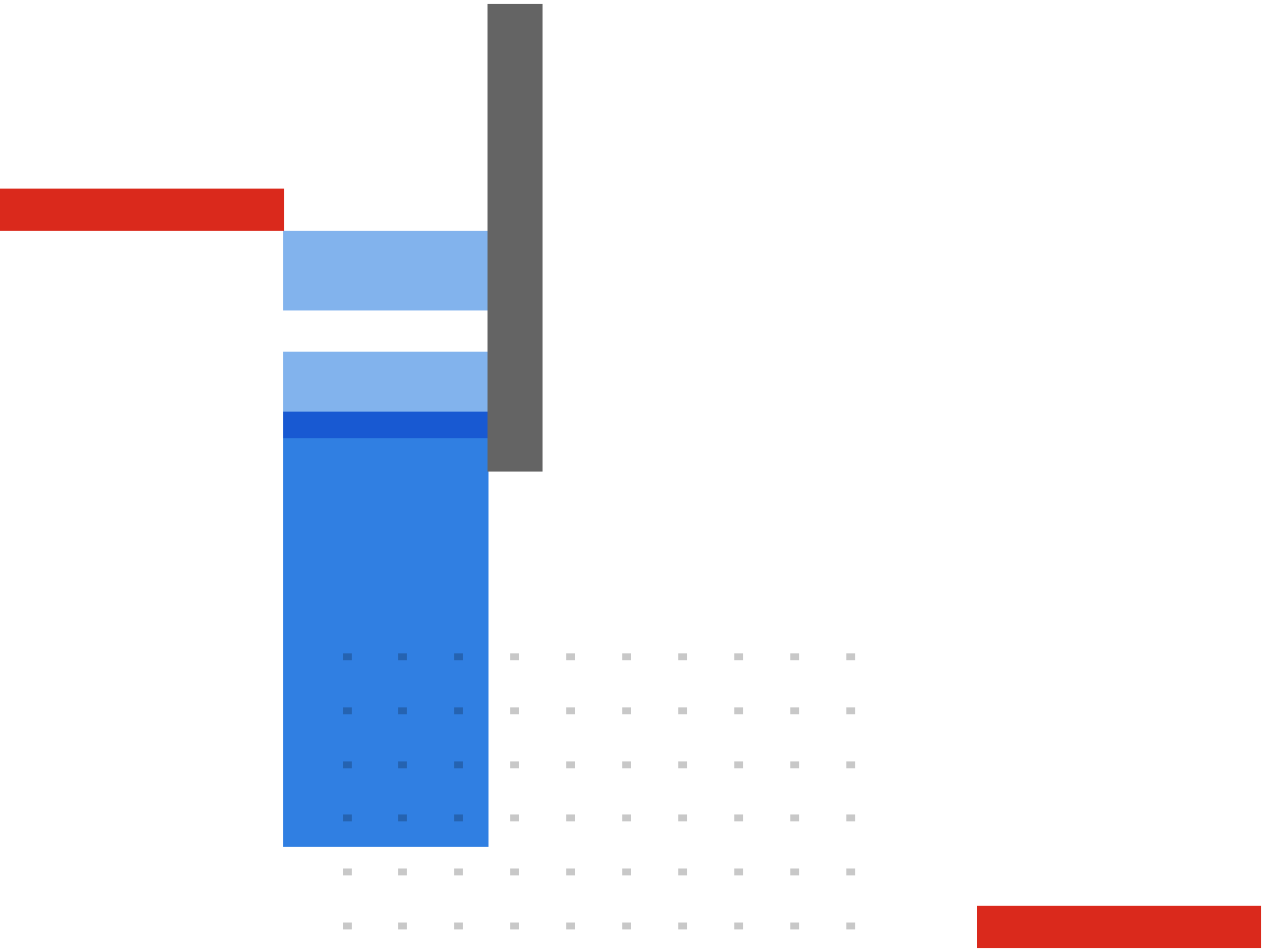
Ordering Information

Product	SKU	Description
FortiGate 40F	FG-40F	5 x GE RJ45 ports (including 4 x Internal Ports, 1 x WAN Ports).
FortiWiFi 40F	FWF-40F-[RC]	5 x GE RJ45 ports (including 4 x Internal Ports, 1 x WAN Ports), Wireless (802.11a/b/g/n/ac-W2).
FortiGate 40F-3G4G	FG-40F-3G4G	5 x GE RJ45 ports (Including 1 x WAN port, 4 x Switch ports) with Embedded 3G/4G/LTE wireless wan module, external SMA WWAN antennas included.
FortiWiFi 40F-3G4G	FWF-40F-3G4G-[RC]	5 x GE RJ45 ports (Including 1 x WAN port, 4 x Switch ports) with Embedded 3G/4G/LTE wireless wan module, Wireless (802.11a/b/g/n/ac-W2), external SMA WWAN and wireless antennas included.
Optional Accessories		
Rack Mount Tray	SP-RACKTRAY-02	Rack mount tray for all FortiGate E series and F series desktop models are backwards compatible with SP-RackTray-01. For list of compatible FortiGate products, visit our Documentation website, docs.fortinet.com
AC Power Adaptor	SP-FG-40F-PA-10(-XX)	Pack of 10 AC power adaptors for FG/FWF-40F, come with interchangeable power plugs. (XX=various countries code).
Wall Mount Kits	SP-FG60F-MOUNT-20	Pack of 20 wall mount kits for FG/FWF-40F series, FG/FWF-60F series, FG-80F, FG-81F and FG-80F-Bypass.

[RC] = regional code: A, B, D, E, F, I, J, N, P, S, V, and Y

Fortinet CSR Policy

Fortinet is committed to driving progress and sustainability for all through cybersecurity, with respect for human rights and ethical business practices, making possible a digital world you can always trust. You represent and warrant to Fortinet that you will not use Fortinet's products and services to engage in, or support in any way, violations or abuses of human rights, including those involving illegal censorship, surveillance, detention, or excessive use of force. Users of Fortinet products are required to comply with the Fortinet EULA and report any suspected violations of the EULA via the procedures outlined in the Fortinet Whistleblower Policy.



FORTINET

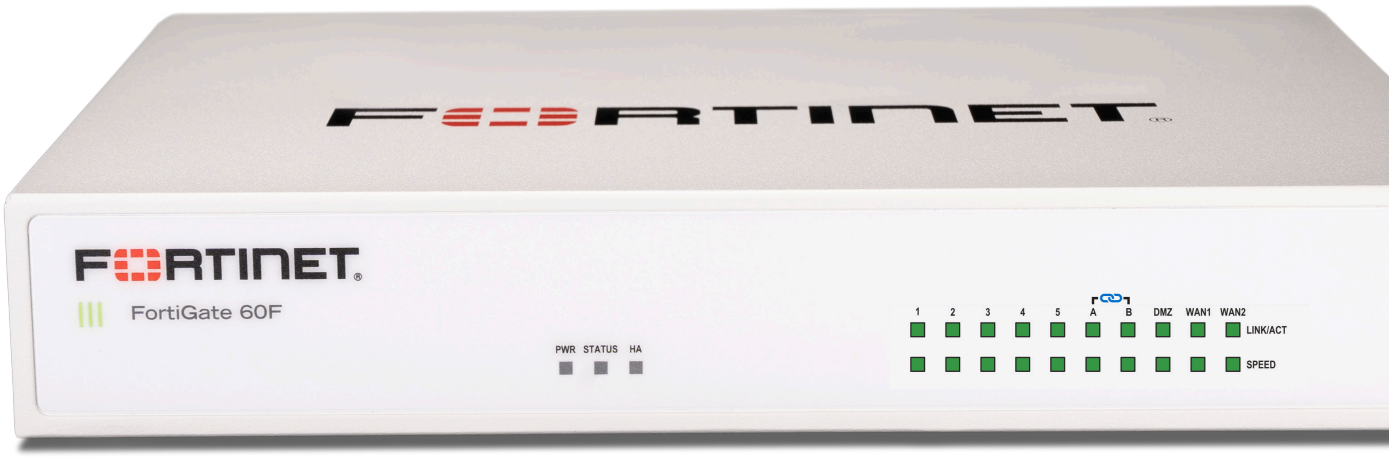
www.fortinet.com

October 17, 2023

FGFWF-40F-DAT-R30-20231017

FortiGate FortiWiFi 60F Series

FG-60F, FG-61F, FWF-60F, and FWF-61F



Highlights

Gartner Magic Quadrant Leader for both Network Firewalls and SD-WAN.

Security-Driven Networking with FortiOS delivers converged networking and security.

Unparalleled Performance with Fortinet's patented SoC processors.

Enterprise Security with consolidated AI / ML-powered FortiGuard Services.

Simplified Operations with centralized management for networking and security, automation, deep analytics, and self-healing.

Converged Next-Generation Firewall (NGFW) and SD-WAN

The FortiGate Next-Generation Firewall 60F series is ideal for building security-driven networks at distributed enterprise sites and transforming WAN architecture at any scale.

With a rich set of AI/ML-based FortiGuard security services and our integrated Security Fabric platform, the FortiGate FortiWiFi 60F series delivers coordinated, automated, end-to-end threat protection across all use cases.

FortiGate has the industry's first integrated SD-WAN and zero-trust network access (ZTNA) enforcement within an NGFW solution and is powered by one OS. FortiGate FortiWiFi 60F automatically controls, verifies, and facilitates user access to applications, delivering consistency with a seamless and optimized user experience.

IPS	NGFW	Threat Protection	Interfaces
1.4 Gbps	1 Gbps	700 Mbps	Multiple GE RJ45 | Variants with internal storage | WiFi variants

Available in

Appliance

Virtual

Hosted

Cloud

Container

FortiOS Everywhere

FortiOS, Fortinet's Advanced Operating System

FortiOS enables the convergence of high performing networking and security across the Fortinet Security Fabric. Because it can be deployed anywhere, it delivers consistent and context-aware security posture across network, endpoint, and multi-cloud environments.

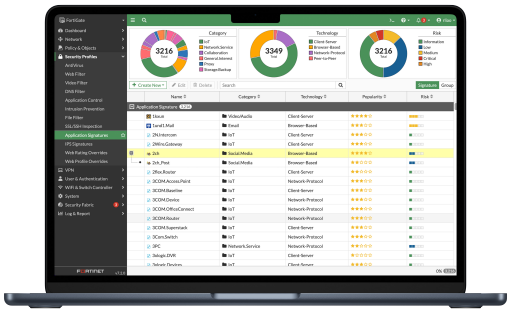
FortiOS powers all FortiGate deployments whether a physical or virtual device, as a container, or as a cloud service. This universal deployment model enables the consolidation of many technologies and use cases into organically built best-of-breed capabilities, unified operating system, and ultra-scalability. The solution allows organizations to protect all edges, simplify operations, and run their business without compromising performance or protection.

FortiOS dramatically expands the Fortinet Security Fabric's ability to deliver advanced AI/ML-powered services, inline advanced sandbox detection, integrated ZTNA enforcement, and more. It provides protection across hybrid deployment models for hardware, software, and Software-as-a-Service with SASE.

FortiOS expands visibility and control, ensures the consistent deployment and enforcement of a simplified, single policy and management framework. Its security policies enable centralized management across large-scale networks with the following key attributes:

- Interactive drill-down and topology viewers that display real-time status
- On-click remediation that provides accurate and quick protection against threats and abuses
- Unique threat score system correlates weighted threats with users to prioritize investigations

Intuitive easy to use view into the network and endpoint vulnerabilities



Visibility with FOS Application Signatures

FortiConverter Service

FortiConverter Service provides hassle-free migration to help organizations transition from a wide range of legacy firewalls to FortiGate Next-Generation Firewalls quickly and easily. The service eliminates errors and redundancy by employing best practices with advanced methodologies and automated processes. Organizations can accelerate their network protection with the latest FortiOS technology.

FortiGuard Services

Network and File Security

Services provide protection against network-based and file-based threats. This consists of Intrusion Prevention (IPS) which uses AI/M models to perform deep packet/SSL inspection to detect and stop malicious content, and apply virtual patching when a new vulnerability is discovered. It also includes Anti-Malware for defense against known and unknown file-based threats. Anti-malware services span both antivirus and file sandboxing to provide multi-layered protection and are enhanced in real-time with threat intelligence from FortiGuard Labs. Application Control enhances security compliance and offers real-time application visibility.

Web / DNS Security

Services provide protection against web-based threats including DNS-based threats, malicious URLs (including even in emails), and botnet/command and control communications. DNS filtering provides full visibility into DNS traffic while blocking high-risk domains, and protects against DNS tunneling, DNS infiltration, C2 server ID and Domain Generation Algorithms (DGA). URL filtering leverages a database of 300M+ URLs to identify and block links to malicious sites and payloads. IP Reputation and anti-botnet services prevent botnet communications, and block DDoS attacks from known sources.

SaaS and Data Security

Services address numerous security use cases across application usage as well as overall data security. This consists of Data Leak Prevention (DLP) which ensures data visibility, management and protection (including blocking exfiltration) across networks, clouds, and users, while simplifying compliance and privacy implementations. Separately, our Inline Cloud Access Security Broker (CASB) service protects data in motion, at rest, and in the cloud. The service enforces major compliance standards and manages account, user and cloud application usage. Services also include capabilities designed to continually assess your infrastructure, validate that configurations are working effectively and secure, and generate awareness of risks and vulnerabilities that could impact business operations. This includes coverage across IoT devices for both IoT detection and IoT vulnerability correlation.

Zero-Day Threat Prevention

Zero-day threat prevention entails Fortinet's AI-based inline malware prevention, our most advanced sandbox service, to analyze and block unknown files in real-time, offering sub-second protection against zero-day and sophisticated threats across all NGFWs. The service also has a built-in MITRE ATT&CK® matrix to accelerate investigations. The service focuses on comprehensive defense by blocking unknown threats while streamlining incident response efforts and reducing security overhead.

OT Security

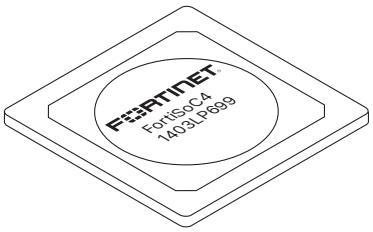
The service provides OT detection, OT vulnerability correlation, virtual patching, OT signatures, and industry-specific protocol decoders for overall robust defense of OT environments and devices.

Secure Any Edge at Any Scale

Powered by Security Processing Unit (SPU)

Traditional firewalls cannot protect against today's content- and connection-based threats because they rely on off-the-shelf hardware and general-purpose CPUs, causing a dangerous performance gap. Fortinet's custom SPU processors deliver the power you need—up to 520Gbps—to detect emerging threats and block malicious content while ensuring your network security solution does not become a performance bottleneck.

ASIC Advantage



Secure SD-WAN ASIC SOC4

- Combines a RISC-based CPU with Fortinet's proprietary Security Processing Unit (SPU) content and network processors for unmatched performance
- Delivers industry's fastest application identification and steering for efficient business operations
- Accelerates IPsec VPN performance for best user experience on direct internet access
- Enables best of breed NGFW Security and Deep SSL Inspection with high performance
- Extends security to access layer to enable SD-Branch transformation with accelerated and integrated switch and access point connectivity

FortiCare Services

Fortinet is dedicated to helping our customers succeed, and every year FortiCare Services help thousands of organizations get the most from our Fortinet Security Fabric solution. Our lifecycle portfolio offers Design, Deploy, Operate, Optimize, and Evolve services. Operate services offer device-level FortiCare Elite service with enhanced SLAs to meet our customer's operational and availability needs. In addition, our customized account-level services provide rapid incident resolution and offer proactive care to maximize the security and performance of Fortinet deployments.

Use Cases

Next Generation Firewall (NGFW)

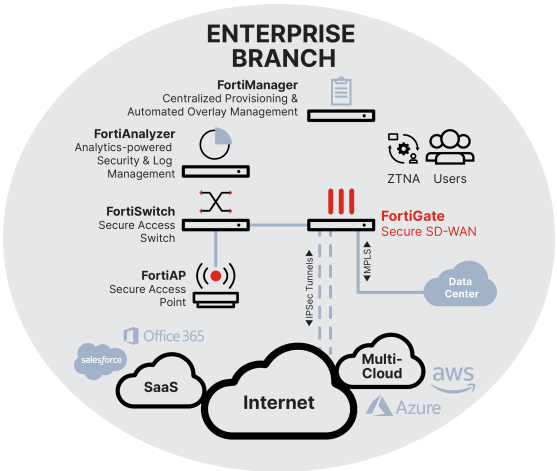
- FortiGuard Labs' suite of AI-powered Security Services—natively integrated with your NGFW—secures web, content, and devices and protects networks from ransomware and sophisticated cyberattacks
- Real-time SSL inspection (including TLS 1.3) provides full visibility into users, devices, and applications across the attack surface
- Fortinet's patented SPU (Security Processing Unit) technology provides industry-leading high-performance protection

Secure SD-WAN

- FortiGate WAN Edge powered by one OS and unified security and management framework and systems transforms and secures WANs
- Delivers superior quality of experience and effective security posture for work-from-any where models, SD-Branch, and cloud-first WAN use cases
- Achieve operational efficiencies at any scale through automation, deep analytics, and self-healing

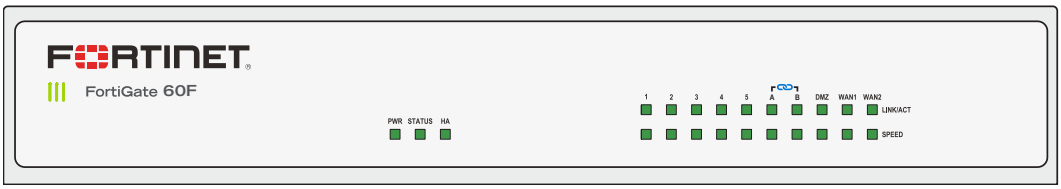
Universal ZTNA

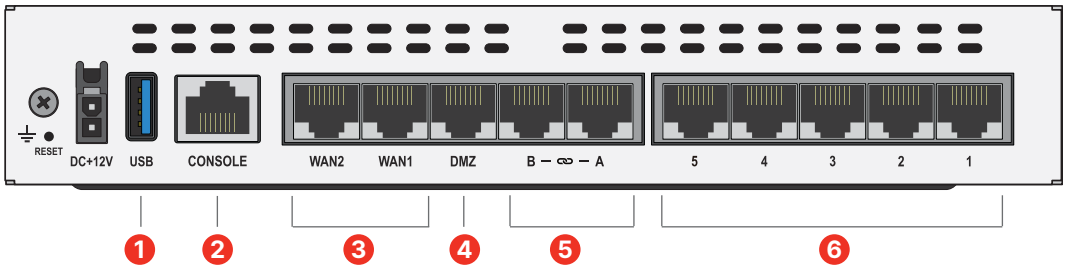
- Control access to applications no matter where the user is and no matter where the application is hosted for universal application of access policies
- Provide extensive authentications, checks, and enforce policy prior to granting application access - every time
- Agent-based access with FortiClient or agentless access via proxy portal for guest or BYOD



Hardware

FortiGate FortiWiFi 60F/61F

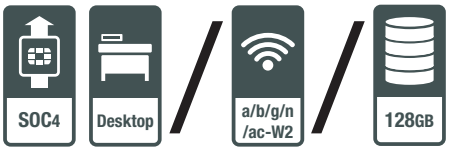




Interfaces

1. 1 x USB Port
2. 1 x Console Port
3. 2 x GE RJ45 WAN Ports
4. 1 x GE RJ45 DMZ Port
5. 2 x GE RJ45 FortiLink Ports
6. 5 x GE RJ45 Internal Ports

Hardware Features



Compact and Reliable Form Factor

Designed for small environments, you can place it on a desktop or wall-mount it. It is small, lightweight, yet highly reliable with a superior MTBF (Mean Time Between Failure), minimizing the chance of a network disruption.

Access Layer Security

FortiLink protocol enables you to converge security and the network access by integrating the FortiSwitch into the FortiGate as a logical extension of the NGFW. These FortiLink enabled ports can be reconfigured as regular ports as needed.

Specifications

	FORTIGATE 60F	FORTIGATE 61F	FORTIWIFI 60F	FORTIWIFI 61F
Hardware Specifications				
GE RJ45 WAN / DMZ Ports	2 / 1	2 / 1	2 / 1	2 / 1
GE RJ45 Internal Ports	5	5	5	5
GE RJ45 FortiLink Ports (Default)	2	2	2	2
Wireless Interface	–	–	Single Radio (2.4GHz/5GHz), 802.11 a/b/g/n/ac-W2	Single Radio (2.4GHz/5GHz), 802.11 a/b/g/n/ac-W2
USB Ports	1	1	1	1
Console (RJ45)	1	1	1	1
Internal Storage	–	1 × 128 GB SSD	–	1 × 128 GB SSD
System Performance — Enterprise Traffic Mix				
IPS Throughput [2]	1.4 Gbps			
NGFW Throughput [2, 4]	1 Gbps			
Threat Protection Throughput [2, 5]	700 Mbps			
System Performance				
Firewall Throughput (1518 / 512 / 64 byte UDP packets)	10/10/6 Gbps			
Firewall Latency (64 byte UDP packets)	3.3 µs			
Firewall Throughput (Packets Per Second)	9 Mpps			
Concurrent Sessions (TCP)	700 000			
New Sessions/Second (TCP)	35 000			
Firewall Policies	5000			
IPsec VPN Throughput (512 byte) [1]	6.5 Gbps			
Gateway-to-Gateway IPsec VPN Tunnels	200			
Client-to-Gateway IPsec VPN Tunnels	500			
SSL-VPN Throughput	900 Mbps			
Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode)	200			
SSL Inspection Throughput (IPS, avg. HTTPS) [3]	630 Mbps			
SSL Inspection CPS (IPS, avg. HTTPS) [3]	400			
SSL Inspection Concurrent Session (IPS, avg. HTTPS) [3]	55 000			
Application Control Throughput (HTTP 64K) [2]	1.8 Gbps			
CAPWAP Throughput (HTTP 64K)	8 Gbps			
Virtual Domains (Default / Maximum)	10 / 10			
Maximum Number of FortiSwitches Supported	24			
Maximum Number of FortiAPs (Total / Tunnel Mode)	64 / 32			
Maximum Number of FortiTokens	500			
High Availability Configurations	Active-Active, Active-Passive, Clustering			
Dimensions				
Height x Width x Length (inches)	1.5 × 8.5 × 6.3			
Height x Width x Length (mm)	38.5 × 216 × 160 mm			
Weight	2.23 lbs (1.01 kg)			
Form Factor	Desktop			
Radio Specifications				
Multiple User (MU) MIMO	–	–	3×3	
Maximum Wi-Fi Speeds	–	–	1300 Mbps @ 5 GHz, 450 Mbps @ 2.4 GHz	
Maximum Tx Power	–	–	20 dBm	
Antenna Gain	–	–	3.5 dBi @ 5 GHz, 5 dBi @ 2.4 GHz	

Note: All performance values are "up to" and vary depending on system configuration.

[1] IPsec VPN performance test uses AES256-SHA256.

[2] IPS (Enterprise Mix), Application Control, NGFW and Threat Protection are measured with Logging enabled.

[3] SSL Inspection performance values use an average of HTTPS sessions of different cipher suites.

[4] NGFW performance is measured with Firewall, IPS and Application Control enabled.

[5] Threat Protection performance is measured with Firewall, IPS, Application Control and Malware Protection enabled.

Specifications

	FORTIGATE 60F	FORTIGATE 61F	FORTIWIFI 60F	FORTIWIFI 61F
Operating Environment and Certifications				
Power Rating	12Vdc, 3A			
Power Required	Powered by External DC Power Adapter, 100–240V AC, 50/60 Hz			
Maximum Current	100Vac/1.0A, 240Vac/0.6A			
Power Consumption (Average / Maximum)	10.17 W / 12.43 W	17.2 W / 18.7 W	17.2 W / 18.7 W	17.5 W / 19.0 W
Heat Dissipation	42.4 BTU/hr	42.4 BTU/hr	63.8 BTU/hr	64.8 BTU/hr
Operating Temperature	32°–104°F (0°–40°C)			
Storage Temperature	-31°–158°F (-35°–70°C)			
Humidity	Humidity 10%–90% non-condensing			
Noise Level	Fanless 0 dBA			
Operating Altitude	Up to 7400 ft (2250 m)			
Compliance	FCC, ICES, CE, RCM, VCCI, BSMI, UL/cUL, CB			
Certifications	USGv6/IPv6			

Subscriptions

Service Category	Service Offering	A-la-carte	Bundles		
			Enterprise Protection	Unified Threat Protection	Advanced Threat Protection
FortiGuard Security Services	IPS Service	•	•	•	•
	Anti-Malware Protection (AMP) — Antivirus, Mobile Malware, Botnet, CDR, Virus Outbreak Protection and FortiSandbox Cloud Service	•	•	•	•
	URL, DNS & Video Filtering Service	•	•	•	
	Anti-Spam		•	•	
	AI-based Inline Malware Prevention Service	•	•		
	Data Loss Prevention Service [1]	•	•		
	OT Security Service (OT Detection, OT Vulnerability correlation, Virtual Patching, OT Signature / Protocol Decoders) [1]	•			
	Application Control		included with FortiCare Subscription		
	CASB SaaS Control		included with FortiCare Subscription		
SD-WAN and SASE Services	SD-WAN Underlay Bandwidth and Quality Monitoring Service	•			
	SD-WAN Overlay-as-a-Service for SaaS-based overlay network provisioning	•			
	SD-WAN Connector for FortiSASE Secure Private Access	•			
	FortiSASE subscription including cloud management and 10Mbps bandwidth license [2]	•			
NOC and SOC Services	FortiGuard Attack Surface Security Service (IoT Detection, IoT Vulnerability Correlation, and Security Rating Updates) [1]	•	•		
	FortiConverter Service	•	•		
	Managed FortiGate Service	•			
	FortiGate Cloud (SMB Logging + Cloud Management)	•			
	FortiAnalyzer Cloud	•			
	FortiAnalyzer Cloud with SOCaaS	•			
	FortiGuard SOCaaS	•			
Hardware and Software Support	FortiCare Essentials	•			
	FortiCare Premium	•	•	•	•
	FortiCare Elite	•			
Base Services	Internet Service (SaaS) DB Updates	included with FortiCare Subscription			
	GeoIP DB Updates				
	Device/OS Detection Signatures				
	Trusted Certificate DB Updates				
	DDNS (v4/v6) Service				

1. Full features available when running FortiOS 7.4.1
2. Desktop Models only

FortiGuard Bundles

FortiGuard Labs delivers a number of security intelligence services to augment the FortiGate firewall platform. You can easily optimize the protection capabilities of your FortiGate with one of these FortiGuard Bundles.

FortiCare Elite

FortiCare Elite offers enhanced SLAs and quick issue resolution through a dedicated support team. It provides single-touch ticket handling, extended Extended End-of-Engineering-Support for 18 months, and access to the new FortiCare Elite Portal for a unified view of device and security health.

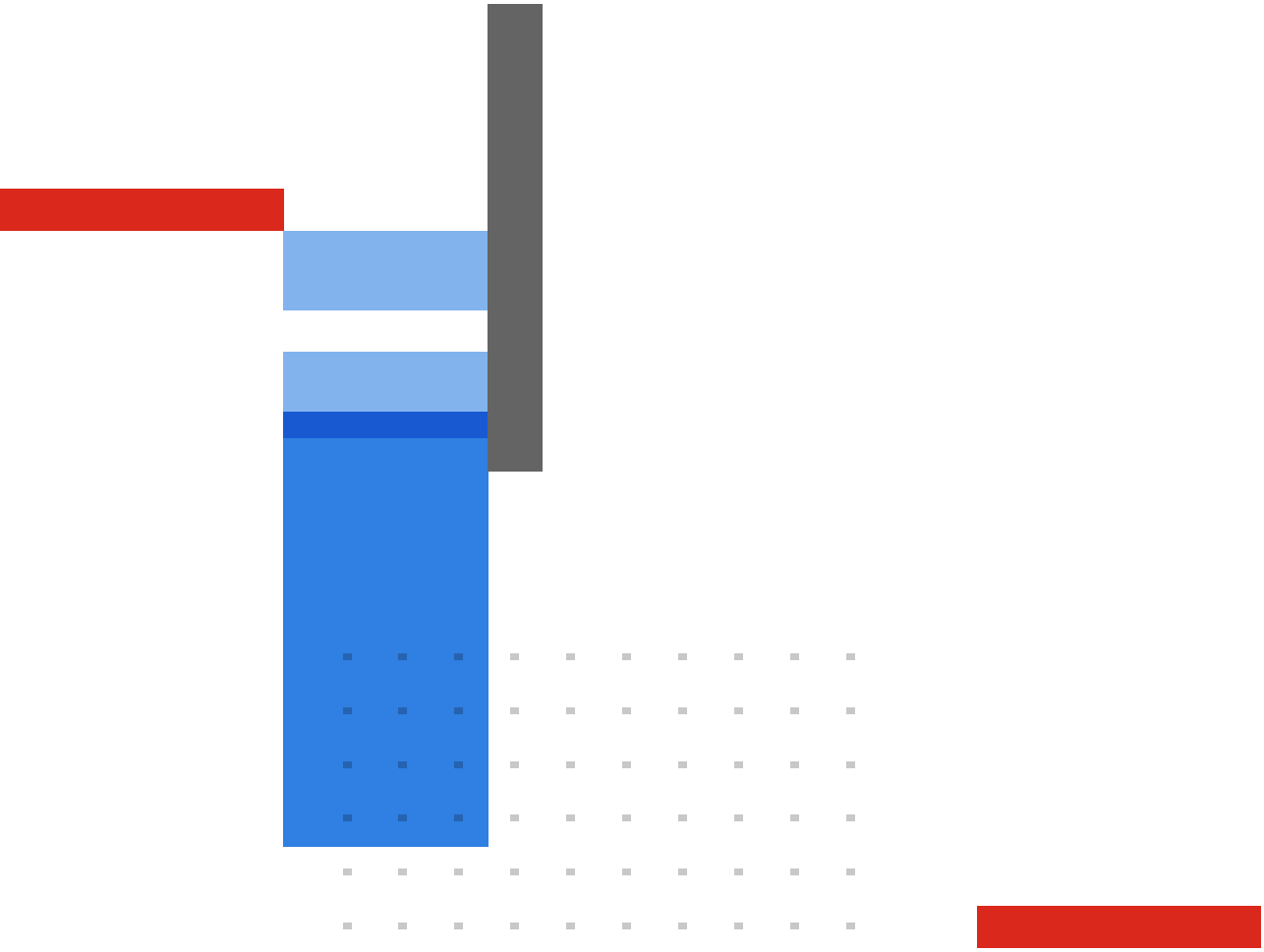
Ordering Information

Product	SKU	Description
FortiGate 60F	FG-60F	10x GE RJ45 ports (including 7x Internal ports, 2x WAN ports, 1x DMZ port)
FortiGate 61F	FG-61F	10x GE RJ45 ports (including 7x Internal ports, 2x WAN ports, 1x DMZ port), 128 GB SSD onboard storage
FortiWiFi 60F	FWF-60F-[RC]	10x GE RJ45 ports (including 7x Internal Ports, 2x WAN Ports, 1x DMZ Port), Wireless (802.11 a/b/g/n/ac-W2)
FortiWiFi 61F	FWF-61F-[RC]	10x GE RJ45 ports (including 7x Internal Ports, 2x WAN Ports, 1x DMZ Port), Wireless (802.11 a/b/g/n/ac-W2), 128GB SSD onboard storage
Optional Accessories		
Rack Mount Tray	SP-RACKTRAY-02	Rack mount tray for all FortiGate E series and F series desktop models are backwards compatible with SP-RackTray-01. For list of compatible FortiGate products, visit our Documentation website, docs.fortinet.com
AC Power Adaptor	SP-FG60E-PDC-5	Pack of 5 AC power adaptors for FG/FWF 60E/61E, 60F/61F, and 80E/81E
Wall Mount Kit	SP-FG60F-MOUNT-20	Pack of 20 wall mount kits for FG/FWF-60F and FG/FWF-80F series

[RC] = regional code: A, B, D, E, F, I, J, N, P, S, V, and Y

Fortinet CSR Policy

Fortinet is committed to driving progress and sustainability for all through cybersecurity, with respect for human rights and ethical business practices, making possible a digital world you can always trust. You represent and warrant to Fortinet that you will not use Fortinet's products and services to engage in, or support in any way, violations or abuses of human rights, including those involving illegal censorship, surveillance, detention, or excessive use of force. Users of Fortinet products are required to comply with the Fortinet EULA and report any suspected violations of the EULA via the procedures outlined in the Fortinet Whistleblower Policy.



FORTINET

www.fortinet.com

October 17, 2023

FGFWF-60F-DAT-R37-20231017

FortiGate FortiWiFi 80F Series

FG-80F, FG-80F-POE, FG-80F-Bypass, FG-81F, FG-81F-POE, FG-80F-DSL, FWF-81F-2R-POE, FWF-81F-2R-3G4G-POE, FWF-80F/81F-2R, and FWF-80F/81F-2R-3G4G-DSL

Highlights

Gartner Magic Quadrant Leader for both Network Firewalls and SD-WAN.

Security-Driven Networking with FortiOS delivers converged networking and security.

Unparalleled Performance with Fortinet's patented SoC processors.

Enterprise Security with consolidated AI / ML-powered FortiGuard Services.

Simplified Operations with centralized management for networking and security, automation, deep analytics, and self-healing.

Converged Next-Generation Firewall (NGFW) and SD-WAN

The FortiGate Next-Generation Firewall 80F series is ideal for building security-driven networks at distributed enterprise sites and transforming WAN architecture at any scale.

With a rich set of AI/ML-based FortiGuard security services and our integrated Security Fabric platform, the FortiGate FortiWiFi 80F series delivers coordinated, automated, end-to-end threat protection across all use cases.

FortiGate has the industry's first integrated SD-WAN and zero-trust network access (ZTNA) enforcement within an NGFW solution and is powered by one OS. FortiGate FortiWiFi 80F automatically controls, verifies, and facilitates user access to applications, delivering consistency with a seamless and optimized user experience.

IPS	NGFW	Threat Protection	Interfaces
1.4 Gbps	1 Gbps	900 Mbps	Multiple GE RJ45 | Variants with PoE, DSL, 3G4G, WiFi and/or storage

Available in

Appliance

Virtual

Hosted

Cloud

Container

FortiOS Everywhere

FortiOS, Fortinet's Advanced Operating System

FortiOS enables the convergence of high performing networking and security across the Fortinet Security Fabric. Because it can be deployed anywhere, it delivers consistent and context-aware security posture across network, endpoint, and multi-cloud environments.

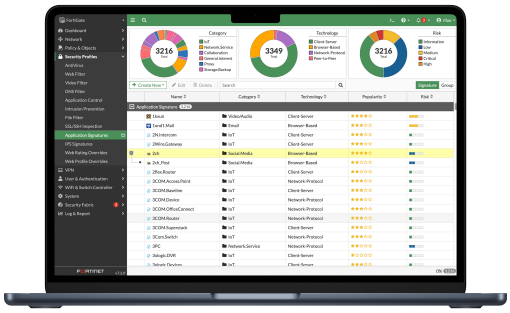
FortiOS powers all FortiGate deployments whether a physical or virtual device, as a container, or as a cloud service. This universal deployment model enables the consolidation of many technologies and use cases into organically built best-of-breed capabilities, unified operating system, and ultra-scalability. The solution allows organizations to protect all edges, simplify operations, and run their business without compromising performance or protection.

FortiOS dramatically expands the Fortinet Security Fabric's ability to deliver advanced AI/ML-powered services, inline advanced sandbox detection, integrated ZTNA enforcement, and more. It provides protection across hybrid deployment models for hardware, software, and Software-as-a-Service with SASE.

FortiOS expands visibility and control, ensures the consistent deployment and enforcement of a simplified, single policy and management framework. Its security policies enable centralized management across large-scale networks with the following key attributes:

- Interactive drill-down and topology viewers that display real-time status
- On-click remediation that provides accurate and quick protection against threats and abuses
- Unique threat score system correlates weighted threats with users to prioritize investigations

Intuitive easy to use view into the network and endpoint vulnerabilities



Visibility with FOS Application Signatures

FortiConverter Service

FortiConverter Service provides hassle-free migration to help organizations transition from a wide range of legacy firewalls to FortiGate Next-Generation Firewalls quickly and easily. The service eliminates errors and redundancy by employing best practices with advanced methodologies and automated processes. Organizations can accelerate their network protection with the latest FortiOS technology.

FortiGuard Services

Network and File Security

Services provide protection against network-based and file-based threats. This consists of Intrusion Prevention (IPS) which uses AI/M models to perform deep packet/SSL inspection to detect and stop malicious content, and apply virtual patching when a new vulnerability is discovered. It also includes Anti-Malware for defense against known and unknown file-based threats. Anti-malware services span both antivirus and file sandboxing to provide multi-layered protection and are enhanced in real-time with threat intelligence from FortiGuard Labs. Application Control enhances security compliance and offers real-time application visibility.

Web / DNS Security

Services provide protection against web-based threats including DNS-based threats, malicious URLs (including even in emails), and botnet/command and control communications. DNS filtering provides full visibility into DNS traffic while blocking high-risk domains, and protects against DNS tunneling, DNS infiltration, C2 server ID and Domain Generation Algorithms (DGA). URL filtering leverages a database of 300M+ URLs to identify and block links to malicious sites and payloads. IP Reputation and anti-botnet services prevent botnet communications, and block DDoS attacks from known sources.

SaaS and Data Security

Services address numerous security use cases across application usage as well as overall data security. This consists of Data Leak Prevention (DLP) which ensures data visibility, management and protection (including blocking exfiltration) across networks, clouds, and users, while simplifying compliance and privacy implementations. Separately, our Inline Cloud Access Security Broker (CASB) service protects data in motion, at rest, and in the cloud. The service enforces major compliance standards and manages account, user and cloud application usage. Services also include capabilities designed to continually assess your infrastructure, validate that configurations are working effectively and secure, and generate awareness of risks and vulnerabilities that could impact business operations. This includes coverage across IoT devices for both IoT detection and IoT vulnerability correlation.

Zero-Day Threat Prevention

Zero-day threat prevention entails Fortinet's AI-based inline malware prevention, our most advanced sandbox service, to analyze and block unknown files in real-time, offering sub-second protection against zero-day and sophisticated threats across all NGFWs. The service also has a built-in MITRE ATT&CK® matrix to accelerate investigations. The service focuses on comprehensive defense by blocking unknown threats while streamlining incident response efforts and reducing security overhead.

OT Security

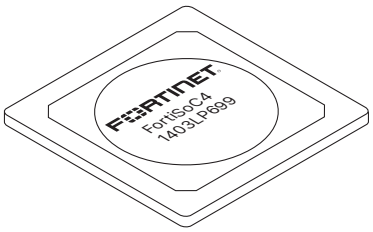
The service provides OT detection, OT vulnerability correlation, virtual patching, OT signatures, and industry-specific protocol decoders for overall robust defense of OT environments and devices.

Secure Any Edge at Any Scale

Powered by Security Processing Unit (SPU)

Traditional firewalls cannot protect against today's content- and connection-based threats because they rely on off-the-shelf hardware and general-purpose CPUs, causing a dangerous performance gap. Fortinet's custom SPU processors deliver the power you need—up to 520Gbps—to detect emerging threats and block malicious content while ensuring your network security solution does not become a performance bottleneck.

ASIC Advantage



Secure SD-WAN ASIC SOC4

- Combines a RISC-based CPU with Fortinet's proprietary Security Processing Unit (SPU) content and network processors for unmatched performance
- Delivers industry's fastest application identification and steering for efficient business operations
- Accelerates IPsec VPN performance for best user experience on direct internet access
- Enables best of breed NGFW Security and Deep SSL Inspection with high performance
- Extends security to access layer to enable SD-Branch transformation with accelerated and integrated switch and access point connectivity

FortiCare Services

Fortinet is dedicated to helping our customers succeed, and every year FortiCare Services help thousands of organizations get the most from our Fortinet Security Fabric solution. Our lifecycle portfolio offers Design, Deploy, Operate, Optimize, and Evolve services. Operate services offer device-level FortiCare Elite service with enhanced SLAs to meet our customer's operational and availability needs. In addition, our customized account-level services provide rapid incident resolution and offer proactive care to maximize the security and performance of Fortinet deployments.

Use Cases

Next Generation Firewall (NGFW)

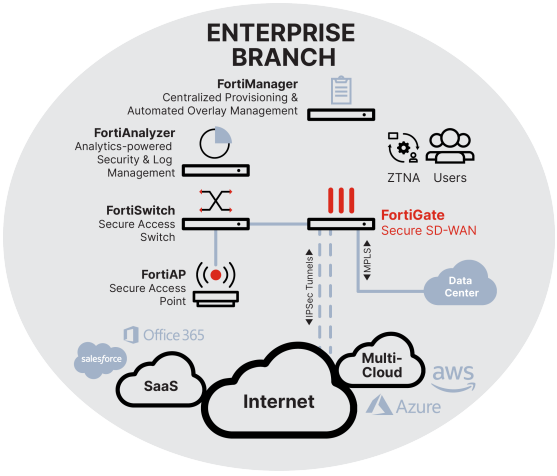
- FortiGuard Labs' suite of AI-powered Security Services—natively integrated with your NGFW—secures web, content, and devices and protects networks from ransomware and sophisticated cyberattacks
- Real-time SSL inspection (including TLS 1.3) provides full visibility into users, devices, and applications across the attack surface
- Fortinet's patented SPU (Security Processing Unit) technology provides industry-leading high-performance protection

Secure SD-WAN

- FortiGate WAN Edge powered by one OS and unified security and management framework and systems transforms and secures WANs
- Delivers superior quality of experience and effective security posture for work-from-any where models, SD-Branch, and cloud-first WAN use cases
- Achieve operational efficiencies at any scale through automation, deep analytics, and self-healing

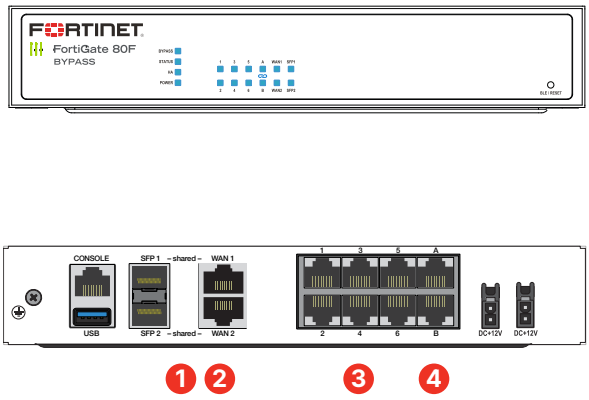
Universal ZTNA

- Control access to applications no matter where the user is and no matter where the application is hosted for universal application of access policies
- Provide extensive authentications, checks, and enforce policy prior to granting application access - every time
- Agent-based access with FortiClient or agentless access via proxy portal for guest or BYOD

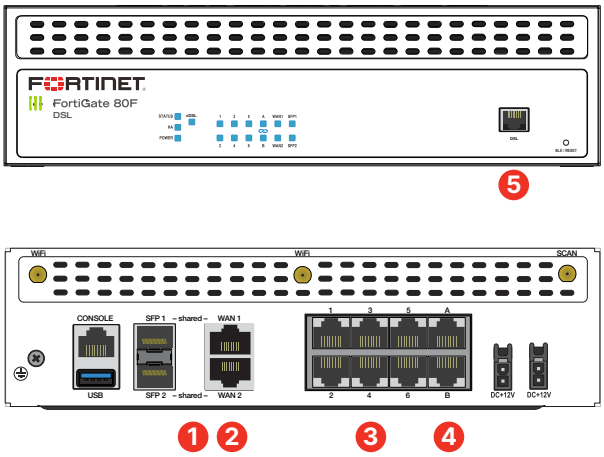


Hardware

FortiGate 80F/81F
FortiGate 80F-Bypass



FortiGate 80F-DSL
FortiGate 80F/81F-POE
FortiWiFi 80F/81F-2R
FortiWiFi 81F-2R-POE

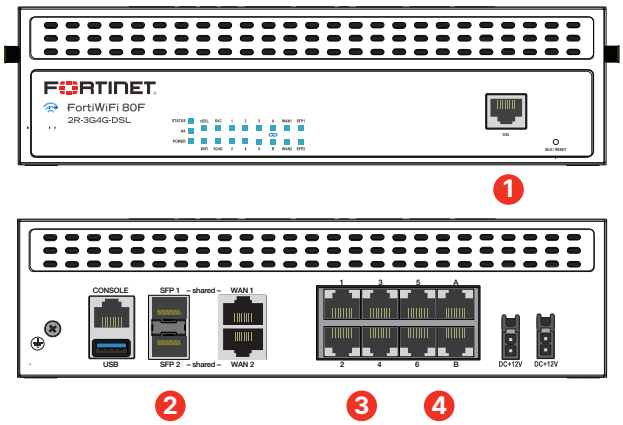


Interfaces

1. 2 x GE RJ45/SFP Shared Media Ports
2. 2 x WAN GE RJ45 Ports, FG-80F-Bypass model only: 1x Bypass GE RJ45 Port Pair (WAN1 and Port1, default configuration)
3. 6 x GE RJ45* Ports
4. 2 x GE RJ45* FortiLink Ports
5. 1 x DSL RJ11 Port (for 80F-DSL only)

* POE/+ ports for POE Variants

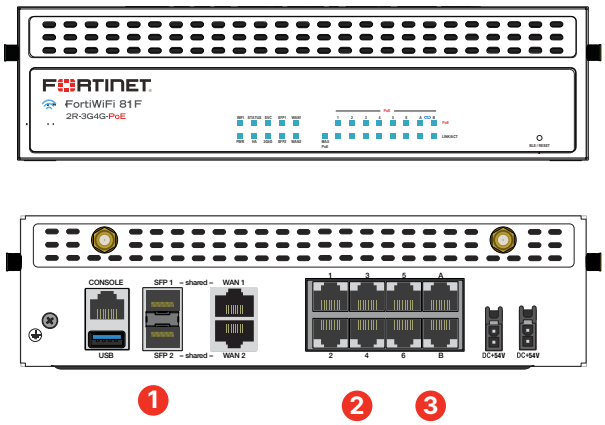
FortiWiFi 80F/81F-2R-3G4G-DSL



Interfaces

1. 1 x DSL Port (RJ11)
2. 2 x GE RJ45/SFP Shared Media Ports
3. 6 x GE RJ45 Ports
4. 2 x GE RJ45 FortiLink Ports

FortiWiFi 81F-2R-3G4G-POE



Interfaces

1. 2 x GE RJ45/SFP Shared Media Ports
2. 6 x GE RJ45 POE/+ Ports
3. 2 x GE RJ45 POE/+ FortiLink Ports

Hardware Features

Superior Wireless Coverage

A built-in dual-band, dual-stream access point is integrated on the FortiWiFi 80F series which provides the industry's latest high-speed WiFi-6 (802.11ax) wireless access.

Trusted Platform Module (TPM)

The FortiGate 80F Series features a dedicated module that hardens physical networking appliances by generating, storing, and authenticating cryptographic keys. Hardware-based security mechanisms protect against malicious software and phishing attacks.

Bypass WAN/LAN Mode

The FortiGate 80F Series offers a pair of bypass ports that help organizations avoid network communication interruption due to device faults and improve network reliability.

Access Layer Security

FortiLink protocol enables you to converge security and the network access by integrating the FortiSwitch into the FortiGate as a logical extension of the NGFW. These FortiLink enabled ports can be reconfigured as regular ports as needed.

Specifications

	FG-80F	FG-81F	FG-80F-BYPASS	FG-80F-POE	FG-81F-POE
Interfaces and Modules					
GE RJ45/SFP Shared Media Pairs	2	2	2	2	2
GE RJ45 Internal Ports	6	6	6	—	—
GE RJ45 FortiLink Ports (Default)	2	2	2	—	—
GE RJ45 PoE/+ Ports	—	—	—	6	6
GE RJ45 PoE/+ FortiLink Ports (Default)	—	—	—	2	2
Bypass GE RJ45 Port Pair (WAN1 & Port1, default configuration)	—	—	Yes	—	—
Wireless Interface	—	—	—	—	—
USB Ports 3.0	1	1	1	1	1
Console (RJ45)	1	1	1	1	1
Internal Storage		1× 128 GB SSD			1× 128 GB SSD
Trusted Platform Module (TPM)	Yes	Yes	Yes	Yes	Yes
Bluetooth Low Energy (BLE)	Yes	Yes	Yes	Yes	Yes
System Performance — Enterprise Traffic Mix					
IPS Throughput [2]			1.4 Gbps		
NGFW Throughput [2, 4]			1 Gbps		
Threat Protection Throughput [2, 5]			900 Mbps		
System Performance and Capacity					
IPv4 Firewall Throughput (1518 / 512 / 64 byte, UDP)			10 / 10 / 7 Gbps		
Firewall Latency (64 byte, UDP)			3.23 µs		
Firewall Throughput (Packet per Second)			10.5 Mpps		
Concurrent Sessions (TCP)			1.5 Million		
New Sessions/Second (TCP)			45 000		
Firewall Policies			5000		
IPsec VPN Throughput (512 byte)[1]			6.5 Gbps		
Gateway-to-Gateway IPsec VPN Tunnels			200		
Client-to-Gateway IPsec VPN Tunnels			2500		
SSL-VPN Throughput			950 Mbps		
Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode)			200		
SSL Inspection Throughput (IPS, avg HTTPS)[3]			715 Mbps		
SSL Inspection CPS (IPS, avg. HTTPS)[3]			700		
SSL Inspection Concurrent Session (IPS, avg HTTPS)[3]			100 000		
Application Control Throughput (HTTP 64K)[2]			1.8 Gbps		
CAPWAP Throughput (HTTP 64K)			9 Gbps		
Virtual Domains (Default / Maximum)			10 / 10		
Maximum Number of FortiSwitches Supported			24		
Maximum Number of FortiAPs (Total /Tunnel)			96 / 48		
Maximum Number of FortiTokens			500		
High Availability Configurations			Active-Active, Active-Passive, Clustering		

Note: All performance values are “up to” and vary depending on system configuration.

[1] IPsec VPN performance test uses AES256-SHA256.

[2] IPS (Enterprise Mix), Application Control, NGFW and Threat Protection are measured with Logging enabled.

[3] SSL Inspection performance values use an average of HTTPS sessions of different cipher suites.

[4] NGFW performance is measured with Firewall, IPS and Application Control enabled.

[5] Threat Protection performance is measured with Firewall, IPS, Application Control and Malware Protection enabled.

Specifications

	FG-80F	FG-81F	FG-80F-BYPASS	FG-80F-POE	FG-81F-POE
Dimensions and Power					
Height x Width x Length (inches)	1.6 × 8.5 × 7.0	1.6 × 8.5 × 7.0	1.6 × 8.5 × 7.0	2.4 × 8.5 × 7.0	2.4 × 8.5 × 7.0
Height x Width x Length (mm)	40 × 216 × 178	40 × 216 × 178	40 × 216 × 178	60 × 216 × 178	60 × 216 × 178
Weight	2.4 lbs (1.1 kg)	2.4 lbs (1.1 kg)	2.6 lbs (1.2 kg)	3.1 lbs (1.4 kg)	3.1 lbs (1.4 kg)
Form Factor (supports EIA/non-EIA standards)	Desktop/ Wall Mount/ Rack Tray				
Operating Environment and Certifications					
Input Rating	12V DC, 3A (dual redundancy optional)	12V DC, 3A (dual redundancy optional)	12V DC, 3A (dual redundancy optional)	+54V DC, 3A (dual redundancy optional)	+54V DC, 3A (dual redundancy optional)
Power Required (Redundancy Optional)	Powered by up to 2 External DC Power Adapters (1 adapter included), 100–240V AC, 50/60 Hz				
Maximum Current	115VAC/0.4A, 230VAC/0.2A	115VAC/0.4A, 230VAC/0.2A	115VAC/0.4A, 230VAC/0.2A	115VAC/2.2A, 230VAC/1.1A	115VAC/1.2A, 230VAC/0.6A
Total Available PoE Power Budget*	—	—	—	96W	96W
Power Consumption (Average / Maximum)	12.69 W / 15.51 W	13.5 W / 16.5 W	12.6 W / 15.4 W	96 W / 118 W	98 W / 137 W
Heat Dissipation	52.55 BTU/h	56.30 BTU/h	52.55 BTU/h	402.26 BTU/h	467.5 BTU/h
Operating Temperature	32°–104°F (0°–40°C)				
Storage Temperature	-31°–158°F (-35°–70°C)				
Humidity	10%–90% non-condensing				
Noise Level	Fanless 0 dBA	Fanless 0 dBA	Fanless 0 dBA	31.56 dBA	31.56 dBA
Operating Altitude	Up to 7400 ft (2250 m)				
Compliance	FCC, ICES, CE, RCM, VCCI, BSMI, UL/cUL, CB				
Certifications	USGv6/IPv6				

* Maximum loading on each PoE/+ port is 30 W (802.3at).

Specifications

	FORTIWIFI 80F-2R	FORTIWIFI 81F-2R	FORTIWIFI 81F-2R-POE
Hardware Specifications			
GE RJ45/SFP Shared Media Pairs	2	2	2
GE RJ45 Internal Ports	6	6	—
GE RJ45 FortiLink Ports (Default)	2	2	—
GE RJ45 PoE/+ Ports	—	—	6
GE RJ45 PoE/+ FortiLink Ports (Default)	—	—	2
Bypass GE RJ45 Port Pair (WAN1 and Port1, default configuration)	—	—	—
Wireless Interface	Dual WiFi Radio (5 GHz, 2.4 GHz) 802.11a/b/g/n/ac/ax + 1 Scanning Radio		
Antenna Ports (SMA)	3	3	3
USB Ports 3.0	1	1	1
Console (RJ45)	1	1	1
Internal Storage	—	1× 128 GB SSD	1× 128 GB SSD
Trusted Platform Module (TPM)	Yes	Yes	Yes
Bluetooth Low Energy (BLE)	Yes	Yes	Yes
Radio Specifications			
Multiple User (MU) MIMO	2×2		
Maximum Wi-Fi Speeds	574 Mbps @ 2.4 GHz, 1201 Mbps @ 5 GHz		
Maximum Tx Power	23 dBm @ 2.4 GHz, 22 dBm @ 5 GHz		
Antenna Gain	4.5dBi @ 2.4Ghz, 5.5dBi @ 5GHz		
System Performance — Enterprise Traffic Mix			
IPS Throughput [2]	1.4 Gbps		
NGFW Throughput [2, 4]	1 Gbps		
Threat Protection Throughput [2, 5]	900 Mbps		
System Performance			
Firewall Throughput (1518 / 512 / 64 byte UDP packets)	10/10/7 Gbps		
Firewall Latency (64 byte UDP packets)	3.23 µs		
Firewall Throughput (Packets Per Second)	10.5 Mpps		
Concurrent Sessions (TCP)	1.5 Million		
New Sessions/Second (TCP)	45 000		
Firewall Policies	5000		
IPsec VPN Throughput (512 byte) [1]	6.5 Gbps		
Gateway-to-Gateway IPsec VPN Tunnels	200		
Client-to-Gateway IPsec VPN Tunnels	2500		
SSL-VPN Throughput	950 Mbps		
Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode)	200		
SSL Inspection Throughput (IPS, avg. HTTPS) [3]	715 Mbps		
SSL Inspection CPS (IPS, avg. HTTPS) [3]	700		
SSL Inspection Concurrent Session (IPS, avg. HTTPS) [3]	100 000		
Application Control Throughput (HTTP 64K) [2]	1.8 Gbps		
CAPWAP Throughput (HTTP 64K)	9 Gbps		
Virtual Domains (Default / Maximum)	10 / 10		
Maximum Number of FortiSwitches Supported	24		
Maximum Number of FortiAPs (Total / Tunnel Mode)	96 / 48		
Maximum Number of FortiTokens	500		
High Availability Configurations	Active-Active, Active-Passive, Clustering		

Note: All performance values are "up to" and vary depending on system configuration.

[1] IPsec VPN performance test uses AES256-SHA256.

[2] IPS (Enterprise Mix), Application Control, NGFW and Threat Protection are measured with Logging enabled.

[3] SSL Inspection performance values use an average of HTTPS sessions of different cipher suites.

[4] NGFW performance is measured with Firewall, IPS and Application Control enabled.

[5] Threat Protection performance is measured with Firewall, IPS, Application Control and Malware Protection enabled.

Specifications

	FORTIWIFI 80F-2R	FORTIWIFI 81F-2R	FORTIWIFI 81F-2R-POE
Dimensions			
Height x Width x Length (inches)	2.4 × 8.5 × 7.0	2.4 × 8.5 × 7.0	2.4 × 8.5 × 7.0
Height x Width x Length (mm)	60 × 216 × 178	60 × 216 × 178	60 × 216 × 178
Weight	3.3 lbs (1.5 kg)	3.3 lbs (1.5 kg)	3.3 lbs (1.5 kg)
Form Factor	Desktop/ Wall Mount/ Rack Tray		
Operating Environment and Certifications			
Input Rating	12V DC, 5A (dual redundancy optional)	12V DC, 5A (dual redundancy optional)	+54V DC, 5A (dual redundancy optional)
Power Required (Redundancy Optional)	Powered by up to 2 External DC Power Adapters (1 adapter included), 100–240V AC, 50/60 Hz		
Maximum Current	115VAC/0.42A, 230VAC/0.21A	115VAC/0.42A, 230VAC/0.28A	115VAC/0.9A, 230VAC/0.6A
Total Available PoE Power Budget*	—	—	96W
Power Consumption (Average / Maximum)	22.9 W / 27.9 W	24.79 W / 30.29 W	107.4 W / 131.3 W
Heat Dissipation	95.26 BTU/h	103.29 BTU/h	441.4 BTU/h
Operating Temperature	32°–104°F (0°–40°C)		
Storage Temperature	-31°–158°F (-35°–70°C)		
Humidity	10%–90% non-condensing		
Noise Level	24.14 dBA	24.14 dBA	31.56 dBA
Operating Altitude	Up to 7400 ft (2250 m)		
Compliance	FCC, ICES, CE, RCM, VCCI, BSMI, UL/cUL, CB		
Certifications	USGv6/IPv6		

* Maximum loading on each PoE/+ port is 30 W (802.3at).

Specifications

	FG-80F-DSL	FWF-80F-2R-3G4G-DSL	FWF-81F-2R-3G4G-DSL	FWF-81F-2R-3G4G-POE
Interfaces and Modules				
GE RJ45/SFP Shared Media Pairs	2	2	2	2
GE RJ45 Internal Ports	6	6	6	–
GE RJ45 FortiLink Ports (Default)	2	2	2	–
GE RJ45 POE/+ Ports	–	–	–	6
GE RJ45 POE/+ FortiLink Ports (Default)	–	–	–	2
DSL RJ11 Port	1	1	1	–
Cellular Modem	–	3G4G / LTE	3G4G / LTE	3G4G / LTE
Wireless Interface	–	Single Radio (2.4GHz/5GHz), 802.11a/b/g/n/ac-W2 Dual WiFi Radio (5 GHz, 2.4 GHz) 802.11a/b/g/n/ac/ax + 1 Scanning Radio	Dual WiFi Radio (5 GHz, 2.4 GHz) 802.11a/b/g/n/ac/ax + 1 Scanning Radio	Dual WiFi Radio (5 GHz, 2.4 GHz) 802.11a/b/g/n/ac/ax + 1 Scanning Radio
Antenna Ports (SMA)	–	6	6	6
USB Ports	1	1	1	1
Console Port (RJ45)	1	1	1	1
SIM Slots (Nano SIM)	–	2	2	2
Internal Storage	–		128 GB	128 GB
Trusted Platform Module (TPM)	–	Yes	Yes	Yes
Bluetooth Low Energy (BLE)	–	Yes	Yes	Yes
System Performance — Enterprise Traffic Mix				
IPS Throughput [2]	1 Gbps			
NGFW Throughput [2, 4]	800 Mbps			
Threat Protection Throughput [2, 5]	600 Mbps			
System Performance and Capacity				
IPv4 Firewall Throughput (1518 / 512 / 64 byte, UDP)	5 / 5 / 5 Gbps			
Firewall Latency (64 byte, UDP)	2.97 µs			
Firewall Throughput (Packet per Second)	7.5 Mpps			
Concurrent Sessions (TCP)	700 000			
New Sessions/Second (TCP)	35 000			
Firewall Policies	5 000			
IPsec VPN Throughput (512 byte) [1]	4.4 Gbps			
Gateway-to-Gateway IPsec VPN Tunnels	200			
Client-to-Gateway IPsec VPN Tunnels	250			
SSL-VPN Throughput	490 Mbps			
Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode)	200			
SSL Inspection Throughput (IPS, avg. HTTPS) [3]	310 Mbps			
SSL Inspection CPS (IPS, avg. HTTPS) [3]	320			
SSL Inspection Concurrent Session (IPS, avg. HTTPS) [3]	55 000			
Application Control Throughput (HTTP 64K) [2]	990 Mbps			
CAPWAP Throughput (HTTP 64K)	3.5 Gbps			
Virtual Domains (Default / Maximum)	10 / 10			
Maximum Number of FortiSwitches Supported	8			
Maximum Number of FortiAPs (Total / Tunnel)	16 / 8			
Maximum Number of FortiTokens	500			
High Availability Configurations	Active-Active, Active-Passive, Clustering			

Note: All performance values are “up to” and vary depending on system configuration.

[1] IPsec VPN performance test uses AES256-SHA256.

[2] IPS (Enterprise Mix), Application Control, NGFW and Threat Protection are measured with Logging enabled.

[3] SSL Inspection performance values use an average of HTTPS sessions of different cipher suites.

[4] NGFW performance is measured with Firewall, IPS and Application Control enabled.

[5] Threat Protection performance is measured with Firewall, IPS, Application Control and Malware Protection enabled.

Specifications

	FG-80F-DSL	FWF-80F-2R-3G4G-DSL	FWF-81F-2R-3G4G-DSL	FWF-81F-2R-3G4G-POE
Dimensions and Power				
Height x Width x Length (inches)	2.4 × 8.5 × 7.0	2.4 × 8.5 × 7.0	2.4 × 8.5 × 7.0	2.4 × 8.5 × 7.0
Height x Width x Length (mm)	60 × 216 × 178	60 × 216 × 178	60 × 216 × 178	60 × 216 × 178
Weight	3.07 lbs (1.39 kg)	3.5 lbs (1.6 kg)	3.5 lbs (1.6 kg)	3.5 lbs (1.6 kg)
Form Factor (supports EIA/non-EIA standards)	Desktop / Wallmount (optional)			
Input Rating	12V DC, 5A	12V DC, 5A	12V DC, 5A	54V DC, 2.78A
Power Required (Redundancy Optional)	Powered by up to two external DC power adapters (one adapter included), 100-240V AC, 50/60 Hz			
Current (Maximum)	115Vac/0.9A, 230Vac/0.6A			
Total Available PoE Power Budget*	–	—	—	96W
Power Consumption (Average / Maximum)	28.0 W / 31.6 W	28.07 W / 34.31 W	29.2 W / 35.6 W	109.3 W / 133.6 W
Heat Dissipation	108 BTU/h	117.0 BTU/h	121.5 BTU/h	455.6 BTU/h
Operating Environment and Certifications				
Operating Temperature	32°–104°F (0°–40°C)			
Storage Temperature	-31°–158°F (-35°–70°C)			
Humidity	10%–90% non-condensing	20%–90% non-condensing	20%–90% non-condensing	20%–90% non-condensing
Noise Level	24.14 dBA	24.14 dBA	24.14 dBA	31.56 dBA
Operating Altitude	Up to 7400 ft (2250 m)			
Compliance	FCC, ICES, CE, RCM, VCCI, BSMI, UL/cUL, CB			
Certifications	USGv6/IPv6			
Radio Specifications				
Multiple (MU) MIMO	N/A	3×3		
Maximum Wi-Fi Speeds	N/A	1300 Mbps @ 5 GHz, 450 Mbps @ 2.4 GHz		
Maximum Tx Power	N/A	20 dBm		
Antenna Gain	N/A	3.5 dBi @ 5 GHz, 5 dBi @ 2.4 GHz		
3G4G Modem				
Regions Supported	N/A	All Regions		
Modem Model	N/A	Sierra Wireless EM7565 (2 SIM Slots, Active/Passive)		
LTE Category	N/A	CAT-12		
LTE Bands	N/A	B1, B2, B3, B4, B5, B7, B8, B9, B12, B13, B18, B19, B20, B26, B28, B29, B30, B32, B41, B42, B43, B46, B48, B66		
UMTS/HSPA+	N/A	B1, B2, B4, B5, B6, B8, B9, B19		
WCDMA	N/A	—		
CDMA 1xRTT/EV-DO Rev A	N/A	—		
GSM/GPRS/EDGE	N/A	—		
Module Certifications	N/A	FCC, ICES, CE, RCM, VCCI, BSMI, UL/cUL, CB		
Diversity	N/A	Yes		
MIMO	N/A	Yes		
GNSS Bias	N/A	Yes		
xDSL Modem - Supported Mode				
VDSL2	✓	✓	✓	N/A
ADSL2	✓	✓	✓	N/A
ADSL2+	✓	✓	✓	N/A
G.DMT	✓	✓	✓	N/A
T1.413	✓	✓	✓	N/A
G.Lite	✓	✓	✓	N/A
xDSL Modem - Supported Type				
Annex A, B, I,J, M & L	✓	✓	✓	N/A

* Maximum loading on each PoE/+ port is 30 W (802.3at).

Subscriptions

Service Category	Service Offering	A-la-carte	Bundles: Enterprise Protection	Bundles: Unified Threat Protection	Bundles: Advanced Threat Protection
FortiGuard Security Services	IPS Service	•	•	•	•
	Anti-Malware Protection (AMP) — Antivirus, Mobile Malware, Botnet, CDR, Virus Outbreak Protection and FortiSandbox Cloud Service	•	•	•	•
	URL, DNS & Video Filtering Service	•	•	•	
	Anti-Spam		•	•	
	AI-based Inline Malware Prevention Service	•	•		
	Data Loss Prevention Service [1]	•	•		
	OT Security Service (OT Detection, OT Vulnerability correlation, Virtual Patching, OT Signature / Protocol Decoders) [1]	•			
	Application Control		included with FortiCare Subscription		
	CASB SaaS Control		included with FortiCare Subscription		
SD-WAN and SASE Services	SD-WAN Underlay Bandwidth and Quality Monitoring Service	•			
	SD-WAN Overlay-as-a-Service for SaaS-based overlay network provisioning	•			
	SD-WAN Connector for FortiSASE Secure Private Access	•			
	FortiSASE subscription including cloud management and 10Mbps bandwidth license [2]	•			
NOC and SOC Services	FortiGuard Attack Surface Security Service (IoT Detection, IoT Vulnerability Correlation, and Security Rating Updates) [1]	•	•		
	FortiConverter Service	•	•		
	Managed FortiGate Service	•			
	FortiGate Cloud (SMB Logging + Cloud Management)	•			
	FortiAnalyzer Cloud	•			
	FortiAnalyzer Cloud with SOCaaS	•			
	FortiGuard SOCaaS	•			
Hardware and Software Support	FortiCare Essentials	•			
	FortiCare Premium	•	•	•	•
	FortiCare Elite	•			
Base Services	Internet Service (SaaS) DB Updates	included with FortiCare Subscription			
	GeoIP DB Updates				
	Device/OS Detection Signatures				
	Trusted Certificate DB Updates				
	DDNS (v4/v6) Service				

1. Full features available when running FortiOS 7.4.1
2. Desktop Models only

FortiGuard Bundles

FortiGuard Labs delivers a number of security intelligence services to augment the FortiGate firewall platform. You can easily optimize the protection capabilities of your FortiGate with one of these FortiGuard Bundles.

FortiCare Elite

FortiCare Elite offers enhanced SLAs and quick issue resolution through a dedicated support team. It provides single-touch ticket handling, extended Extended End-of-Engineering-Support for 18 months, and access to the new FortiCare Elite Portal for a unified view of device and security health.

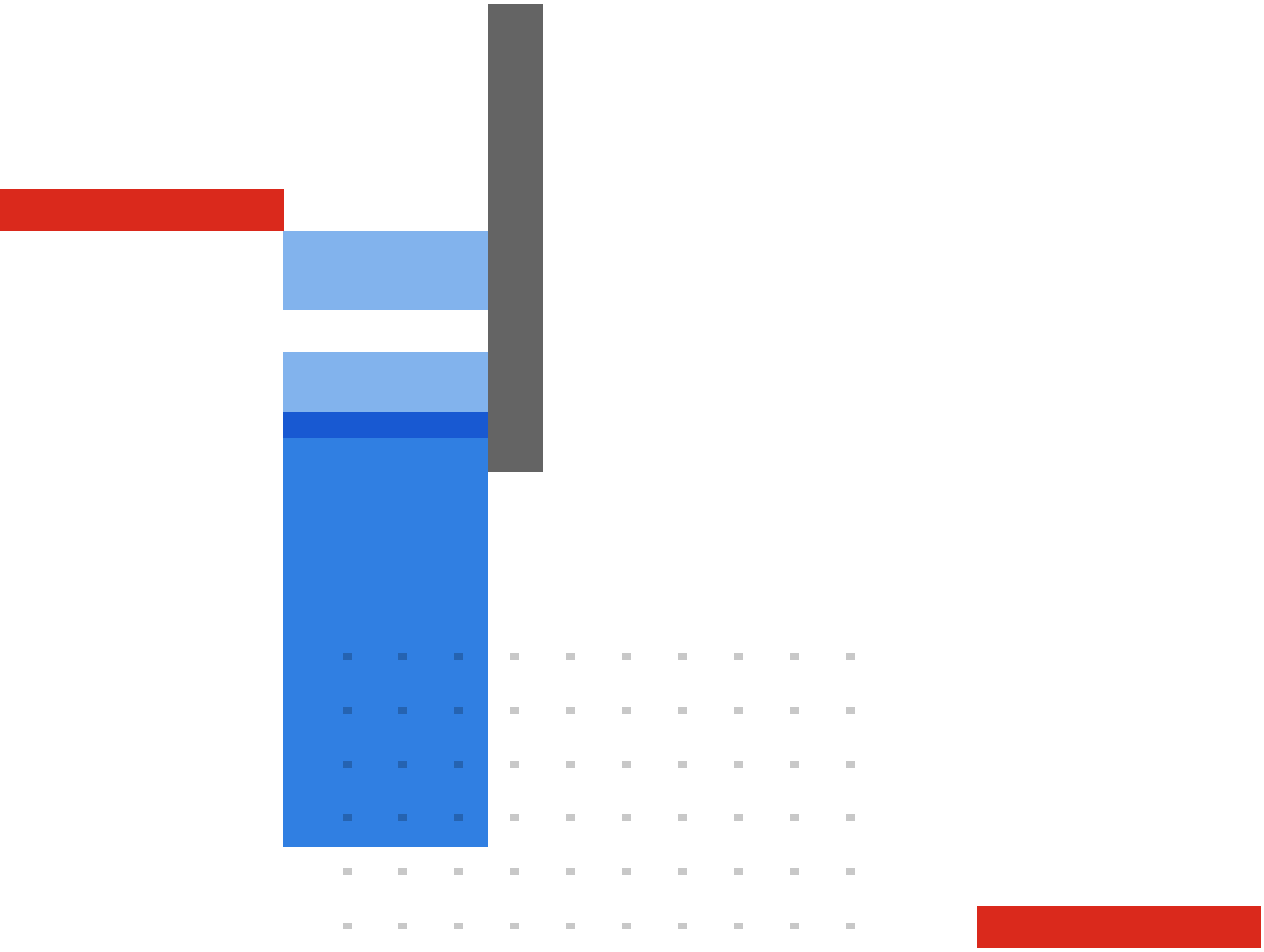
Ordering Information

Product	SKU	Description
FortiGate 80F	FG-80F	8 x GE RJ45 ports, 2 x RJ45/SFP shared media WAN ports.
FortiGate 81F	FG-81F	8 x GE RJ45 ports, 2 x RJ45/SFP shared media WAN ports, 128GB onboard storage.
FortiGate 80F-Bypass	FG-80F-Bypass	8 x GE RJ45 ports, 2 x RJ45/SFP shared media WAN ports, may be configured with 1 pair of LAN bypass.
FortiGate 80F-POE	FG-80F-POE	8 x GE PoE ports, 2 x RJ45/SFP shared media WAN ports
FortiGate 81F-POE	FG-81F-POE	8 x GE RJ45 PoE ports, 2 x RJ45/SFP shared media WAN ports, 128GB SSD.
FortiGate 80F-DSL	FG-80F-DSL	8 x GE RJ45 Ports, 2 x RJ45/SFP shared media WAN ports, with embedded DSL module.
FortiWiFi 80F-2R	FWF-80F-2R-[RC]	8 x GE RJ45 ports, 2 x RJ45/SFP shared media WAN ports, dual WiFi radio.
FortiWiFi 81F-2R	FWF-81F-2R-[RC]	8 x GE RJ45 ports, 2 x RJ45/SFP shared media WAN ports, dual WiFi radio, 128GB SSD.
FortiWiFi 81F-2R-POE	FWF-81F-2R-POE-[RC]	8 x GE RJ45 RJ45 PoE ports, 2 x RJ45/SFP shared media WAN ports, dual WiFi radio, 128GB SSD.
FortiWiFi-80F-2R-3G4G-DSL	FWF-80F-2R-3G4G-DSL-[RC]	8 x GE RJ45 Ports, 2 x GE RJ45 WAN Ports, dual WiFi radio, with embedded DSL and 3G/4G/LTE modules
FortiWiFi-81F-2R-3G4G-DSL	FWF-81F-2R-3G4G-DSL-[RC]	8 x GE RJ45 Ports, 2 x GE RJ45 WAN Ports, dual WiFi radio, with embedded DSL and 3G/4G/LTE modules, 128GB SSD onboard storage.
FortiWiFi-81F-2R-3G4G-PoE	FWF-81F-2R-3G4G-PoE-[RC]	8 x GE RJ45 PoE/+ Ports, 2 x RJ45/SFP shared media WAN ports, dual WiFi radio, with embedded 3G/4G/LTE modules, 128GB SSD onboard storage.
Accessories	**SKU**	**Description**
AC Power Adaptor	SP-FG60E-PDC-5	Pack of 5 AC power adaptors for FG/FWF 60E/61E, 60F/61F, 80E/81E and 80F/81F.
AC Power Adaptor	SP-FWF80F-PDC-5	Pack of 5 AC power adaptors for FWF-80/81F-2R, power cable SP-FG60CPCOR-XX sold separately.
AC Power Adaptor	SP-FG80E-POE-PDC	AC power adaptor for FG-60E-POE, FG-80E-POE, FG-81E-POE, FG-80/81F-POE, FWF-81F-2R-POE power cable SP-FG60CPCOR-XX sold separately.
Rack Mount Tray	SP-RACKTRAY-02	Rack mount tray for all FortiGate E series and F series desktop models.
Wall Mount Kit	SP-FG60F-MOUNT-20	Pack of 20 wall mount kits for FG/FWF-40F series, FG/FWF-60F series, FG-80F, FG-81F and FG-80F-Bypass.
Transceivers	**SKU**	**Description**
1 GE SFP RJ45 Transceiver Module	FN-TRAN-GC	1 GE SFP RJ45 transceiver module for all systems with SFP and SFP/SFP+slots.
1 GE SFP SX Transceiver Module	FN-TRAN-SX	1 GE SFP SX transceiver module for all systems with SFP and SFP/SFP+ slots.
1 GE SFP LX Transceiver Module	FN-TRAN-LX	1 GE SFP LX transceiver module for all systems with SFP and SFP/SFP+ slots.
1GE SFP Transceiver, 90km Range, -40°/85°C Operation	FR-TRAN-ZX	1G SFP transceivers, -40°/85°C operation, 90km range for all systems with SFP Slots.

RC (regional code): A, B, D, E, F, I, J, N, P , S, V, and Y

Fortinet CSR Policy

Fortinet is committed to driving progress and sustainability for all through cybersecurity, with respect for human rights and ethical business practices, making possible a digital world you can always trust. You represent and warrant to Fortinet that you will not use Fortinet's products and services to engage in, or support in any way, violations or abuses of human rights, including those involving illegal censorship, surveillance, detention, or excessive use of force. Users of Fortinet products are required to comply with the Fortinet EULA and report any suspected violations of the EULA via the procedures outlined in the Fortinet Whistleblower Policy.



FORTINET

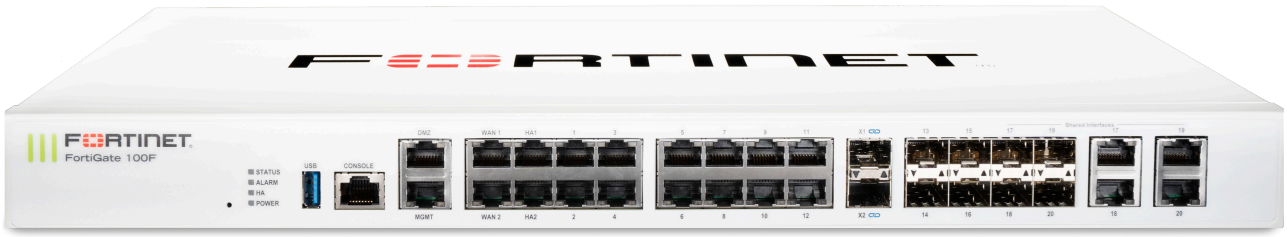
www.fortinet.com

October 18, 2023

FG-80F-DAT-R33-20231018

FortiGate 100F Series

FG-100F and FG-101F



Highlights

Gartner Magic Quadrant Leader for both Network Firewalls and WAN Edge Infrastructure.

Security-Driven Networking FortiOS delivers converged networking and security.

State-of-the-Art Unparalleled Performance with Fortinet's patented / SPU / vSPU processors.

Enterprise Security with consolidated AI / ML-powered FortiGuard Services.

Deep Visibility into applications, users, and devices beyond traditional firewall techniques.

AI/ML Security and Deep Visibility

The FortiGate 100F Series NGFW combines AI-powered security and machine learning to deliver Threat Protection at any scale. Get deeper visibility into your network and see applications, users, and devices before they become threats.

Powered by a rich set of AI/ML security capabilities that extend into an integrated security fabric platform, the FortiGate 100F Series delivers secure networking that is broad, deep, and automated. Secure your network end to end with advanced edge protection that includes web, content, and device security, while network segmentation and secure SD-WAN reduce complexity and risk in hybrid IT networks.

Universal ZTNA automatically controls, verifies, and facilitates user access to applications, reducing lateral threats by providing access only to validated users. Ultra-fast Threat Protection and SSL Inspection provides security at the edge you can see without impacting performance.

IPS	NGFW	Threat Protection	Interfaces
2.6 Gbps	1.6 Gbps	1 Gbps	Multiple GE RJ45, GE SFP and 10 GE SFP+ slots

Available in

Appliance

Virtual

Hosted

Cloud

Container

FortiOS Everywhere

FortiOS, Fortinet's Advanced Operating System

FortiOS enables the convergence of high performing networking and security across the Fortinet Security Fabric. Because it can be deployed anywhere, it delivers consistent and context-aware security posture across network, endpoint, and multi-cloud environments.

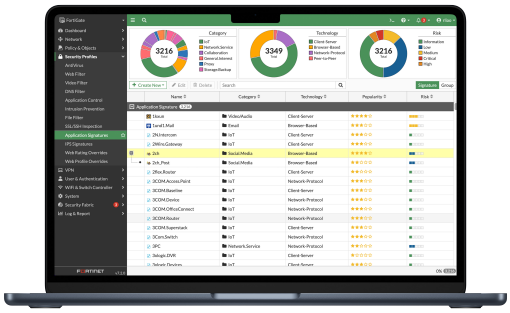
FortiOS powers all FortiGate deployments whether a physical or virtual device, as a container, or as a cloud service. This universal deployment model enables the consolidation of many technologies and use cases into a simplified, single policy and management framework. Its organically built best-of-breed capabilities, unified operating system, and ultra-scalability allows organizations to protect all edges, simplify operations, and run their business without compromising performance or protection.

FortiOS dramatically expands the Fortinet Security Fabric's ability to deliver advanced AI/ML-powered services, inline advanced sandbox detection, integrated ZTNA enforcement, and more, provides protection across hybrid deployment models for hardware, software, and Software-as-a-Service with SASE.

FortiOS expands visibility and control, ensures the consistent deployment and enforcement of security policies, and enables centralized management across large-scale networks with the following key attributes:

- Interactive drill-down and topology viewers that display real-time status
- On-click remediation that provides accurate and quick protection against threats and abuses
- Unique threat score system correlates weighted threats with users to prioritize investigations

Intuitive easy to use view into the network and endpoint vulnerabilities



Visibility with FOS Application Signatures

FortiConverter Migration Service

FortiConverter Service provides hassle-free migration to help organizations transition from a wide range of legacy firewalls to FortiGate Next-Generation Firewalls quickly and easily. The service eliminates errors and redundancy by employing best practices with advanced methodologies and automated processes. Organizations can accelerate their network protection with the latest FortiOS technology.

FortiGuard Services

Network and File Security

Services provide protection against network-based and file-based threats. This consists of Intrusion Prevention (IPS) which uses AI/M models to perform deep packet/SSL inspection to detect and stop malicious content, and apply virtual patching when a new vulnerability is discovered. It also includes Anti-Malware for defense against known and unknown file-based threats. Anti-malware services span both antivirus and file sandboxing to provide multi-layered protection and are enhanced in real-time with threat intelligence from FortiGuard Labs. Application Control enhances security compliance and offers real-time application visibility.

Web / DNS Security

Services provide protection against web-based threats including DNS-based threats, malicious URLs (including even in emails), and botnet/command and control communications. DNS filtering provides full visibility into DNS traffic while blocking high-risk domains, and protects against DNS tunneling, DNS infiltration, C2 server ID and Domain Generation Algorithms (DGA). URL filtering leverages a database of 300M+ URLs to identify and block links to malicious sites and payloads. IP Reputation and anti-botnet services prevent botnet communications, and block DDoS attacks from known sources.

SaaS and Data Security

Services address numerous security use cases across application usage as well as overall data security. This consists of Data Leak Prevention (DLP) which ensures data visibility, management and protection (including blocking exfiltration) across networks, clouds, and users, while simplifying compliance and privacy implementations. Separately, our Inline Cloud Access Security Broker (CASB) service protects data in motion, at rest, and in the cloud. The service enforces major compliance standards and manages account, user and cloud application usage. Services also include capabilities designed to continually assess your infrastructure, validate that configurations are working effectively and secure, and generate awareness of risks and vulnerabilities that could impact business operations. This includes coverage across IoT devices for both IoT detection and IoT vulnerability correlation.

Zero-Day Threat Prevention

Zero-day threat prevention entails Fortinet's AI-based inline malware prevention, our most advanced sandbox service, to analyze and block unknown files in real-time, offering sub-second protection against zero-day and sophisticated threats across all NGFWs. The service also has a built-in MITRE ATT&CK® matrix to accelerate investigations. The service focuses on comprehensive defense by blocking unknown threats while streamlining incident response efforts and reducing security overhead.

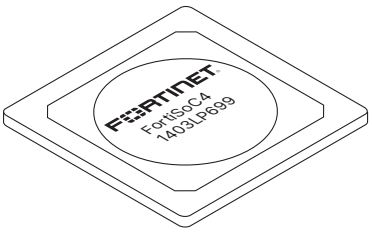
OT Security

The service provides OT detection, OT vulnerability correlation, virtual patching, OT signatures, and industry-specific protocol decoders for overall robust defense of OT environments and devices.

Secure Any Edge at Any Scale

Powered by Security Processing Unit (SPU)

Traditional firewalls cannot protect against today's content- and connection-based threats because they rely on off-the-shelf hardware and general-purpose CPUs, causing a dangerous performance gap. Fortinet's custom SPU processors deliver the power you need—up to 520Gbps—to detect emerging threats and block malicious content while ensuring your network security solution does not become a performance bottleneck.



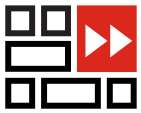
Powered by Purpose-Built Secure SD-WAN ASIC SOC4

- Combines a RISC-based CPU with Fortinet's proprietary Security Processing Unit (SPU) content and network processors for unmatched performance
- Delivers industry's fastest application identification and steering for efficient business operations
- Accelerates IPsec VPN performance for best user-experience on direct internet access
- Enables best of breed NGFW Security and deep SSL inspection with high performance
- Extends security to access layer to enable SD-Branch transformation with accelerated and integrated switch and access point connectivity
- Reduces environmental footprint by saving on average over 60% in power consumption compared to previous generation of FortiGate models

FortiCare Services

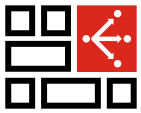
Fortinet is dedicated to helping our customers succeed, and every year FortiCare Services help thousands of organizations get the most from our Fortinet Security Fabric solution. Our lifecycle portfolio offers Design, Deploy, Operate, Optimize, and Evolve services. Operate services offer device-level FortiCare Elite service with enhanced SLAs to meet our customer's operational and availability needs. In addition, our customized account-level services provide rapid incident resolution and offer proactive care to maximize the security and performance of Fortinet deployments.

Use Cases



Next Generation Firewall (NGFW)

- FortiGuard Labs' suite of AI-powered Security Services—natively integrated with your NGFW—secures web, content, and devices and protects networks from ransomware and sophisticated cyberattacks
- Real-time SSL inspection (including TLS 1.3) provides full visibility into users, devices, and applications across the attack surface
- Fortinet's patented SPU (Security Processing Unit) technology provides industry-leading high-performance protection



Secure SD-WAN

- FortiGate WAN Edge powered by one OS and unified security and management framework and systems transforms and secures WANs
- Delivers superior quality of experience and effective security posture for work-from-any where models, SD-Branch, and cloud-first WAN use cases
- Achieve operational efficiencies at any scale through automation, deep analytics, and self-healing

Universal ZTNA

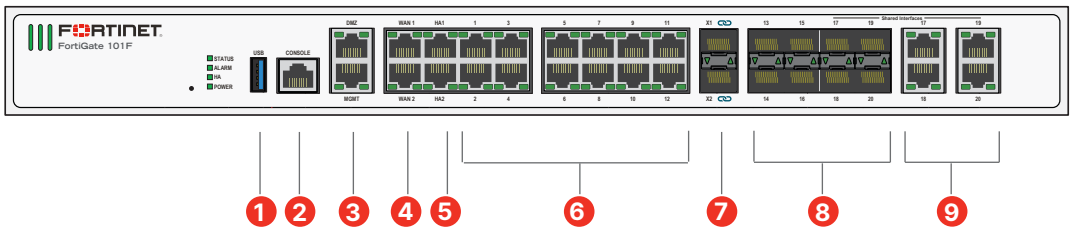
- Control access to applications no matter where the user is and no matter where the application is hosted for universal application of access policies
- Provide extensive authentications, checks, and enforce policy prior to granting application access—every time
- Agent-based access with FortiClient or agentless access via proxy portal for guest or BYOD

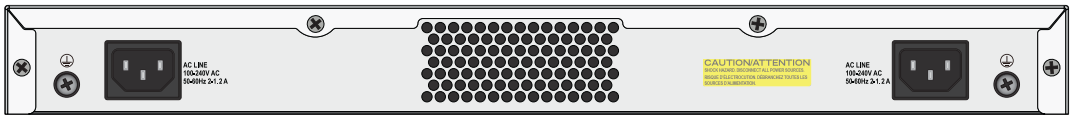
Segmentation

- Dynamic segmentation adapts to any network topology to deliver true end-to-end security—from the branch to the datacenter and across multi-cloud environments
- Ultra-scalable, low latency, VXLAN segmentation bridges physical and virtual domains with Layer 4 firewall rules
- Prevents lateral movement across the network with advanced, coordinated protection from FortiGuard Security Services detects and prevents known, zero-day, and unknown attacks

Hardware

FortiGate 100F Series

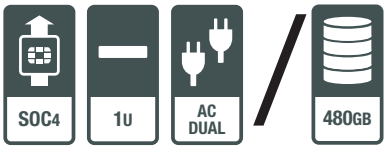




Interfaces

1. 1 x USB Port
2. 1 x Console Port
3. 2 x GE RJ45 MGMT/DMZ Ports
4. 2 x GE RJ45 WAN Ports
5. 2 x GE RJ45 HA Ports
6. 12 x GE RJ45 Ports
7. 2 × 10 GE SFP+ FortiLink Slots
8. 4 x GE SFP Slots
9. 4 x GE RJ45/ SFP Shared Media Pairs

Hardware Features



Dual Power Supplies

Power supply redundancy is essential in the operation of mission-critical networks. The FortiGate 100F Series offers dual built-in non-hot swappable power supplies.

Access Layer Security

FortiLink protocol enables you to converge security and the network access by integrating the FortiSwitch into the FortiGate as a logical extension of the NGFW. These FortiLink enabled ports can be reconfigured as regular ports as needed.

Specifications

	FORTIGATE 100F	FORTIGATE 101F
Interfaces and Modules		
Hardware Accelerated GE RJ45 Ports	12	
Hardware Accelerated GE RJ45 Management/ HA/ DMZ Ports	1 / 2 / 1	
Hardware Accelerated GE SFP Slots	4	
Hardware Accelerated 10 GE SFP+ FortiLink Slots (default)	2	
GE RJ45 WAN Ports	2	
GE RJ45 or SFP Shared Ports *	4	
USB Port	1	
Console Port	1	
Onboard Storage	0	1× 480 GB SSD
Included Transceivers	0	
System Performance — Enterprise Traffic Mix		
IPS Throughput [2]	2.6 Gbps	
NGFW Throughput [2, 4]	1.6 Gbps	
Threat Protection Throughput [2, 5]	1 Gbps	
System Performance and Capacity		
IPv4 Firewall Throughput (1518 / 512 / 64 byte, UDP)	20 / 18 / 10 Gbps	
Firewall Latency (64 byte, UDP)	4.97 µs	
Firewall Throughput (Packet per Second)	15 Mpps	
Concurrent Sessions (TCP)	1.5 Million	
New Sessions/Second (TCP)	56 000	
Firewall Policies	10 000	
IPsec VPN Throughput (512 byte) [1]	11.5 Gbps	
Gateway-to-Gateway IPsec VPN Tunnels	2000	
Client-to-Gateway IPsec VPN Tunnels	16 000	
SSL-VPN Throughput	1 Gbps	
Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode)	500	
SSL Inspection Throughput (IPS, avg. HTTPS) [3]	1 Gbps	
SSL Inspection CPS (IPS, avg. HTTPS) [3]	1800	
SSL Inspection Concurrent Session (IPS, avg. HTTPS) [3]	135 000	
Application Control Throughput (HTTP 64K) [2]	2.2 Gbps	
CAPWAP Throughput (HTTP 64K)	15 Gbps	
Virtual Domains (Default / Maximum)	10 / 10	
Maximum Number of FortiSwitches Supported	32	
Maximum Number of FortiAPs (Total / Tunnel)	128 / 64	
Maximum Number of FortiTokens	5000	
High Availability Configurations	Active-Active, Active-Passive, Clustering	

	FORTIGATE 100F	FORTIGATE 101F
Dimensions and Power		
Height x Width x Length (inches)	1.73 × 17 × 10	
Height x Width x Length (mm)	44 × 432 × 254	
Weight	7.25 lbs (3.29 kg)	7.56 lbs (3.43 kg)
Form Factor (supports EIA/non-EIA standards)	Rack Mount, 1 RU	
AC Power Supply	100–240V AC, 50/60 Hz	
Power Consumption (Average / Maximum)	26.5 W / 29.5 W	35.3 W / 39.1 W
Current (Maximum)	100V / 1A, 240V / 0.5A	
Heat Dissipation	100.6 BTU/h	121.13 BTU/h
Redundant Power Supplies	Yes (Default dual non-swappable AC PSU for 1+1 Redundancy)	
Power Supply Efficiency Rating	80Plus Compliant	
Operating Environment and Certifications		
Operating Temperature	32°–104°F (0°–40°C)	
Storage Temperature	-31°–158°F (-35°–70°C)	
Humidity	10%–90% non-condensing	
Noise Level	40.4 dBA	
Forced Airflow	Side to Back	
Operating Altitude	Up to 10 000 ft (3048 m)	
Compliance	FCC Part 15B, Class A, CE, RCM, VCCI, UL/cUL, CB, BSMI	
Certifications	USGv6/IPv6	

* Latency based on Ultra Low Latency (ULL ports)

Note: All performance values are "up to" and vary depending on system configuration.

[1] IPsec VPN performance test uses AES256-SHA256.

[2] IPS (Enterprise Mix), Application Control, NGFW and Threat Protection are measured with Logging enabled.

[3] SSL Inspection performance values use an average of HTTPS sessions of different cipher suites.

[4] NGFW performance is measured with Firewall, IPS and Application Control enabled.

[5] Threat Protection performance is measured with Firewall, IPS, Application Control and Malware Protection enabled.

[6] Uses RSA-2048 certificate.

Ordering Information

Product	SKU	Description
FortiGate 100F	FG-100F	22x GE RJ45 ports (including 2x WAN ports, 1x DMZ port, 1x Mgmt port, 2x HA ports, 16x switch ports with 4 SFP port shared media), 4 SFP ports, 2× 10 GE SFP+ FortiLinks, dual power supplies redundancy.
FortiGate 101F	FG-101F	22x GE RJ45 ports (including 2x WAN ports, 1x DMZ port, 1x Mgmt port, 2x HA ports, 16x switch ports with 4 SFP port shared media), 4 SFP ports, 2× 10 GE SFP+ FortiLinks, 480GB onboard storage, dual power supplies redundancy.
Optional Accessories	**SKU**	**Description**
1 GE SFP RJ45 Transceiver Module	FN-TRAN-GC	1 GE SFP RJ45 transceiver module for all systems with SFP and SFP/SFP+slots.
1 GE SFP SX Transceiver Module	FN-TRAN-SX	1 GE SFP SX transceiver module for all systems with SFP and SFP/SFP+ slots.
1 GE SFP LX Transceiver Module	FN-TRAN-LX	1 GE SFP LX transceiver module for all systems with SFP and SFP/SFP+ slots.
10 GE SFP+ RJ45 Transceiver Module	FN-TRAN-SFP+GC	10 GE SFP+ RJ45 transceiver module for systems with SFP+ slots.
10 GE SFP+ Transceiver Module, Short Range	FN-TRAN-SFP+SR	10 GE SFP+ transceiver module, short range for all systems with SFP+ and SFP/SFP+ slots.
10 GE SFP+ Transceiver Module, Long Range	FN-TRAN-SFP+LR	10 GE SFP+ transceiver module, long range for all systems with SFP+ and SFP/SFP+ slots.
10 GE SFP+ Transceivers, Extended Range	FN-TRAN-SFP+ER	10 GE SFP+ transceiver module, extended range for all systems with SFP+ and SFP/SFP+ slots.
10GE SFP+ Transceiver Module, 30 km Long Range	FN-TRAN-SFP+BD27	10GE SFP+ transceiver module, 30KM long range single BiDi for systems with SFP+ and SFP/SFP+ slots (connects to FN-TRAN-SFP+BD33, ordered separately).
10GE SFP+ Transceiver Module, 30 km Long Range	FN-TRAN-SFP+BD33	10GE SFP+ transceiver module, 30KM long range single BiDi for systems with SFP+ and SFP/SFP+ slots (connects to FN-TRAN-SFP+BD27, ordered separately).
10 GE SFP+ Passive Direct Attach Cable 1m	FN-CABLE-SFP+1	10 GE SFP+ passive direct attach cable, 1m for systems with SFP+ and SFP/SFP+ slots.
10 GE SFP+ Passive Direct Attach Cable 3m	FN-CABLE-SFP+3	10 GE SFP+ passive direct attach cable, 3m for systems with SFP+ and SFP/SFP+ slots.
10 GE SFP+ Passive Direct Attach Cable 5m	FN-CABLE-SFP+5	10 GE SFP+ passive direct attach cable, 5m for systems with SFP+ and SFP/SFP+ slots.

Subscriptions

Service Category	Service Offering	A-la-carte	Bundles		
			Enterprise Protection	Unified Threat Protection	Advanced Threat Protection
FortiGuard Security Services	IPS Service	•	•	•	•
	Anti-Malware Protection (AMP) — Antivirus, Mobile Malware, Botnet, CDR, Virus Outbreak Protection and FortiSandbox Cloud Service	•	•	•	•
	URL, DNS & Video Filtering Service	•	•	•	
	Anti-Spam		•	•	
	AI-based Inline Malware Prevention Service	•	•		
	Data Loss Prevention Service [1]	•	•		
	OT Security Service (OT Detection, OT Vulnerability correlation, Virtual Patching, OT Signature / Protocol Decoders) [1]	•			
	Application Control		included with FortiCare Subscription		
	CASB SaaS Control		included with FortiCare Subscription		
SD-WAN and SASE Services	SD-WAN Underlay Bandwidth and Quality Monitoring Service	•			
	SD-WAN Overlay-as-a-Service for SaaS-based overlay network provisioning	•			
	SD-WAN Connector for FortiSASE Secure Private Access	•			
	FortiSASE subscription including cloud management and 10Mbps bandwidth license [2]	•			
NOC and SOC Services	FortiGuard Attack Surface Security Service (IoT Detection, IoT Vulnerability Correlation, and Security Rating Updates) [1]	•	•		
	FortiConverter Service	•	•		
	Managed FortiGate Service	•			
	FortiGate Cloud (SMB Logging + Cloud Management)	•			
	FortiAnalyzer Cloud	•			
	FortiAnalyzer Cloud with SOCaaS	•			
	FortiGuard SOCaaS	•			
Hardware and Software Support	FortiCare Essentials	•			
	FortiCare Premium	•	•	•	•
	FortiCare Elite	•			
Base Services	Internet Service (SaaS) DB Updates	included with FortiCare Subscription			
	GeoIP DB Updates				
	Device/OS Detection Signatures				
	Trusted Certificate DB Updates				
	DDNS (v4/v6) Service				

1. Full features available when running FortiOS 7.4.1
2. Desktop Models only

FortiGuard Bundles

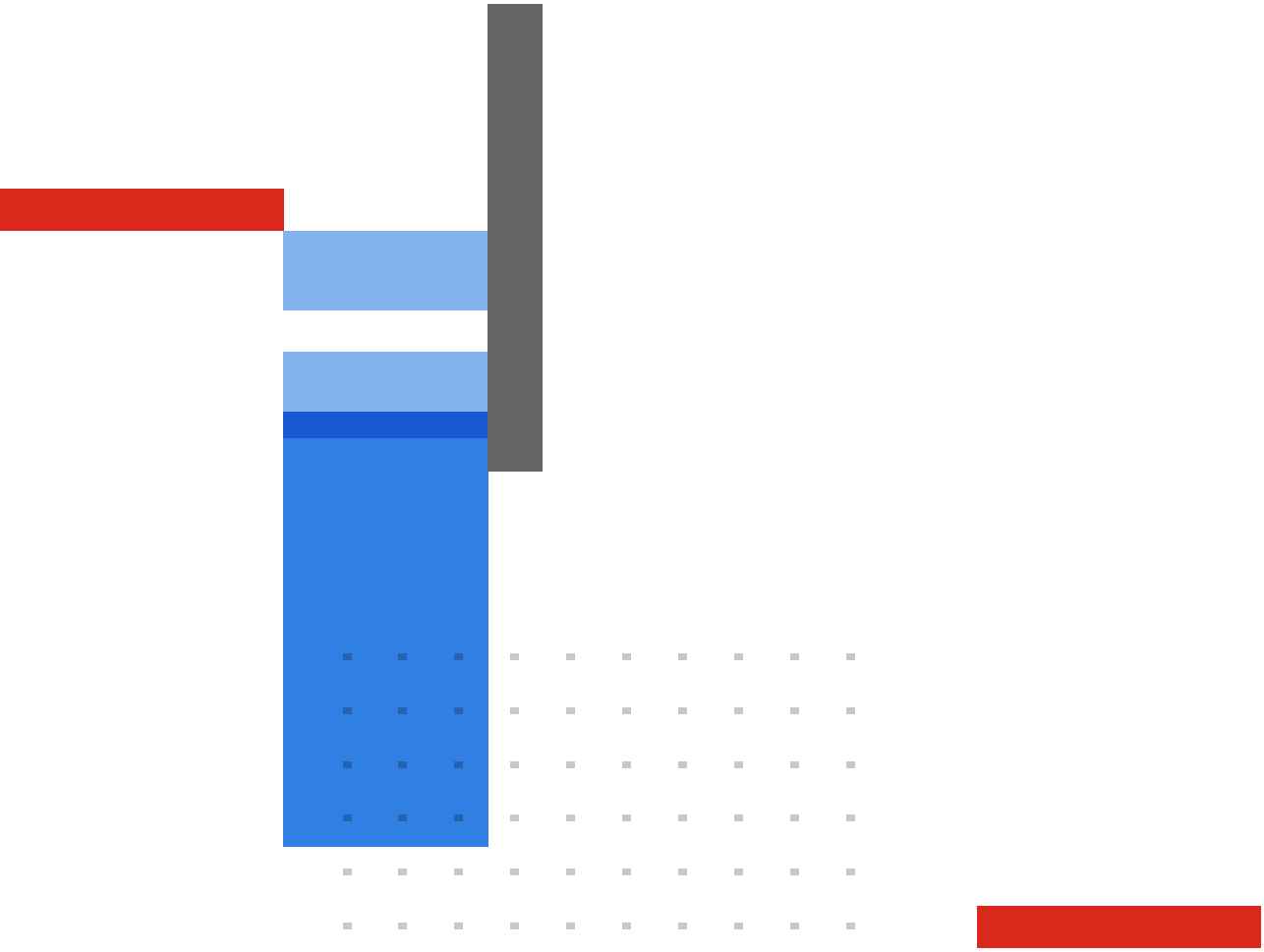
FortiGuard Labs delivers a number of security intelligence services to augment the FortiGate firewall platform. You can easily optimize the protection capabilities of your FortiGate with one of these FortiGuard Bundles.

FortiCare Elite

FortiCare Elite offers enhanced SLAs and quick issue resolution through a dedicated support team. It provides single-touch ticket handling, extended Extended End-of-Engineering-Support for 18 months, and access to the new FortiCare Elite Portal for a unified view of device and security health.

Fortinet CSR Policy

Fortinet is committed to driving progress and sustainability for all through cybersecurity, with respect for human rights and ethical business practices, making possible a digital world you can always trust. You represent and warrant to Fortinet that you will not use Fortinet's products and services to engage in, or support in any way, violations or abuses of human rights, including those involving illegal censorship, surveillance, detention, or excessive use of force. Users of Fortinet products are required to comply with the Fortinet EULA and report any suspected violations of the EULA via the procedures outlined in the Fortinet Whistleblower Policy.



FORTINET

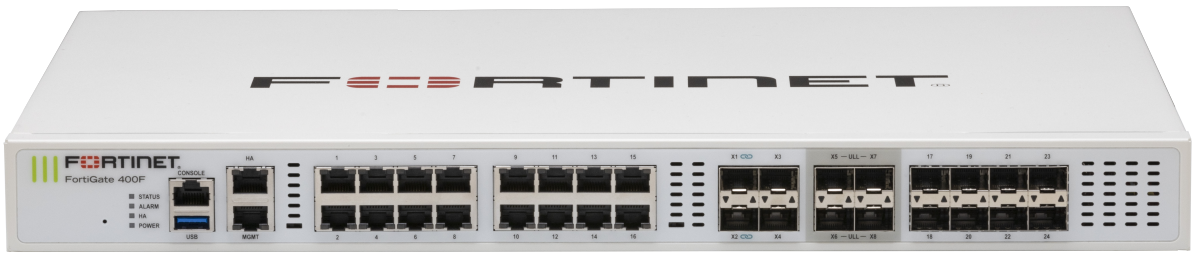
www.fortinet.com

October 17, 2023

FG-100F-DAT-R34-20231017

FortiGate 400F Series

FG-400F and FG-401F



Highlights

Gartner Magic Quadrant Leader for both Network Firewalls and WAN Edge Infrastructure.

Security-Driven Networking FortiOS delivers converged networking and security.

State-of-the-Art Unparalleled Performance with Fortinet's patented / SPU / vSPU processors.

Enterprise Security with consolidated AI / ML-powered FortiGuard Services.

Deep Visibility into applications, users, and devices beyond traditional firewall techniques.

AI/ML Security and Deep Visibility

The FortiGate 400F Series NGFW combines AI-powered security and machine learning to deliver Threat Protection at any scale. Get deeper visibility into your network and see applications, users, and devices before they become threats.

Powered by a rich set of AI/ML security capabilities that extend into an integrated security fabric platform, the FortiGate 400F Series delivers secure networking that is broad, deep, and automated. Secure your network end to end with advanced edge protection that includes web, content, and device security, while network segmentation and secure SD-WAN reduce complexity and risk in hybrid IT networks.

Universal ZTNA automatically controls, verifies, and facilitates user access to applications, reducing lateral threats by providing access only to validated users. Ultra-fast Threat Protection and SSL Inspection provides security at the edge you can see without impacting performance.

IPS	NGFW	Threat Protection	Interfaces
12 Gbps	10 Gbps	9 Gbps	Multiple GE RJ45, 10GE SFP+ Slots, GE SFP Slots

Available in

Appliance

Virtual

Hosted

Cloud

Container

FortiOS Everywhere

FortiOS, Fortinet's Advanced Operating System

FortiOS enables the convergence of high performing networking and security across the Fortinet Security Fabric. Because it can be deployed anywhere, it delivers consistent and context-aware security posture across network, endpoint, and multi-cloud environments.

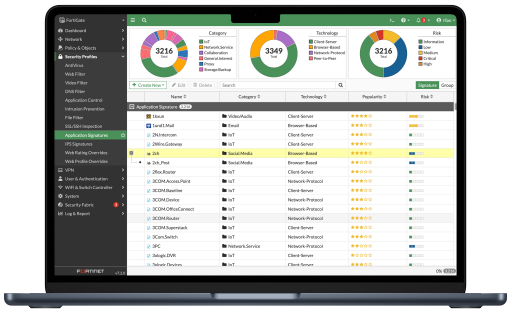
FortiOS powers all FortiGate deployments whether a physical or virtual device, as a container, or as a cloud service. This universal deployment model enables the consolidation of many technologies and use cases into a simplified, single policy and management framework. Its organically built best-of-breed capabilities, unified operating system, and ultra-scalability allows organizations to protect all edges, simplify operations, and run their business without compromising performance or protection.

FortiOS dramatically expands the Fortinet Security Fabric's ability to deliver advanced AI/ML-powered services, inline advanced sandbox detection, integrated ZTNA enforcement, and more, provides protection across hybrid deployment models for hardware, software, and Software-as-a-Service with SASE.

FortiOS expands visibility and control, ensures the consistent deployment and enforcement of security policies, and enables centralized management across large-scale networks with the following key attributes:

- Interactive drill-down and topology viewers that display real-time status
- On-click remediation that provides accurate and quick protection against threats and abuses
- Unique threat score system correlates weighted threats with users to prioritize investigations

Intuitive easy to use view into the network and endpoint vulnerabilities



Visibility with FOS Application Signatures

FortiConverter Migration Service

FortiConverter Service provides hassle-free migration to help organizations transition from a wide range of legacy firewalls to FortiGate Next-Generation Firewalls quickly and easily. The service eliminates errors and redundancy by employing best practices with advanced methodologies and automated processes. Organizations can accelerate their network protection with the latest FortiOS technology.

FortiGuard Services

Network and File Security

Services provide protection against network-based and file-based threats. This consists of Intrusion Prevention (IPS) which uses AI/M models to perform deep packet/SSL inspection to detect and stop malicious content, and apply virtual patching when a new vulnerability is discovered. It also includes Anti-Malware for defense against known and unknown file-based threats. Anti-malware services span both antivirus and file sandboxing to provide multi-layered protection and are enhanced in real-time with threat intelligence from FortiGuard Labs. Application Control enhances security compliance and offers real-time application visibility.

Web / DNS Security

Services provide protection against web-based threats including DNS-based threats, malicious URLs (including even in emails), and botnet/command and control communications. DNS filtering provides full visibility into DNS traffic while blocking high-risk domains, and protects against DNS tunneling, DNS infiltration, C2 server ID and Domain Generation Algorithms (DGA). URL filtering leverages a database of 300M+ URLs to identify and block links to malicious sites and payloads. IP Reputation and anti-botnet services prevent botnet communications, and block DDoS attacks from known sources.

SaaS and Data Security

Services address numerous security use cases across application usage as well as overall data security. This consists of Data Leak Prevention (DLP) which ensures data visibility, management and protection (including blocking exfiltration) across networks, clouds, and users, while simplifying compliance and privacy implementations. Separately, our Inline Cloud Access Security Broker (CASB) service protects data in motion, at rest, and in the cloud. The service enforces major compliance standards and manages account, user and cloud application usage. Services also include capabilities designed to continually assess your infrastructure, validate that configurations are working effectively and secure, and generate awareness of risks and vulnerabilities that could impact business operations. This includes coverage across IoT devices for both IoT detection and IoT vulnerability correlation.

Zero-Day Threat Prevention

Zero-day threat prevention entails Fortinet's AI-based inline malware prevention, our most advanced sandbox service, to analyze and block unknown files in real-time, offering sub-second protection against zero-day and sophisticated threats across all NGFWs. The service also has a built-in MITRE ATT&CK® matrix to accelerate investigations. The service focuses on comprehensive defense by blocking unknown threats while streamlining incident response efforts and reducing security overhead.

OT Security

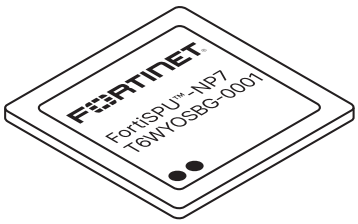
The service provides OT detection, OT vulnerability correlation, virtual patching, OT signatures, and industry-specific protocol decoders for overall robust defense of OT environments and devices.

Secure Any Edge at Any Scale

Powered by Security Processing Unit (SPU)

Traditional firewalls cannot protect against today's content- and connection-based threats because they rely on off-the-shelf hardware and general-purpose CPUs, causing a dangerous performance gap. Fortinet's custom SPU processors deliver the power you need—up to 520Gbps—to detect emerging threats and block malicious content while ensuring your network security solution does not become a performance bottleneck.

ASIC Advantage



Network Processor 7 NP7

Network Processors operate inline to deliver unmatched performance and scalability for critical network functions. Fortinet's breakthrough SPU NP7 network processor works in line with FortiOS functions to deliver:

- Hyperscale firewall, accelerated session setup, and ultra-low latency
- Industry-leading performance for VPN, VXLAN termination, hardware logging, and elephant flows

Content Processor 9 CP9

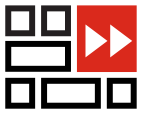
Content Processors act as co-processors to offload resource-intensive processing of security functions. The ninth generation of the Fortinet Content Processor, the CP9, accelerates resource-intensive SSL (including TLS 1.3) decryption and security functions while delivering:

- Pattern matching acceleration and fast inspection of real-time traffic for application identification
- IPS pre-scan/pre-match, signature correlation offload, and accelerated antivirus processing

FortiCare Services

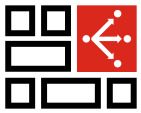
Fortinet is dedicated to helping our customers succeed, and every year FortiCare Services help thousands of organizations get the most from our Fortinet Security Fabric solution. Our lifecycle portfolio offers Design, Deploy, Operate, Optimize, and Evolve services. Operate services offer device-level FortiCare Elite service with enhanced SLAs to meet our customer's operational and availability needs. In addition, our customized account-level services provide rapid incident resolution and offer proactive care to maximize the security and performance of Fortinet deployments.

Use Cases



Next Generation Firewall (NGFW)

- FortiGuard Labs' suite of AI-powered Security Services—natively integrated with your NGFW—secures web, content, and devices and protects networks from ransomware and sophisticated cyberattacks
- Real-time SSL inspection (including TLS 1.3) provides full visibility into users, devices, and applications across the attack surface
- Fortinet's patented SPU (Security Processing Unit) technology provides industry-leading high-performance protection



Secure SD-WAN

- FortiGate WAN Edge powered by one OS and unified security and management framework and systems transforms and secures WANs
- Delivers superior quality of experience and effective security posture for work-from-any where models, SD-Branch, and cloud-first WAN use cases
- Achieve operational efficiencies at any scale through automation, deep analytics, and self-healing

Universal ZTNA

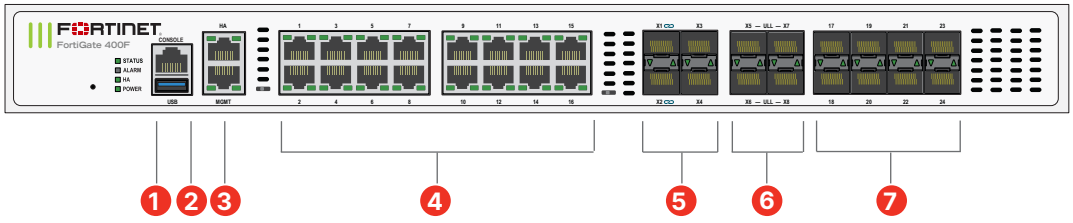
- Control access to applications no matter where the user is and no matter where the application is hosted for universal application of access policies
- Provide extensive authentications, checks, and enforce policy prior to granting application access—every time
- Agent-based access with FortiClient or agentless access via proxy portal for guest or BYOD

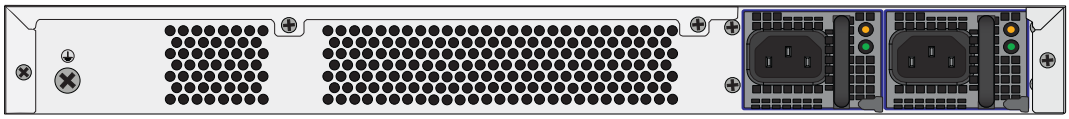
Segmentation

- Dynamic segmentation adapts to any network topology to deliver true end-to-end security—from the branch to the datacenter and across multi-cloud environments
- Ultra-scalable, low latency, VXLAN segmentation bridges physical and virtual domains with Layer 4 firewall rules
- Prevents lateral movement across the network with advanced, coordinated protection from FortiGuard Security Services detects and prevents known, zero-day, and unknown attacks

Hardware

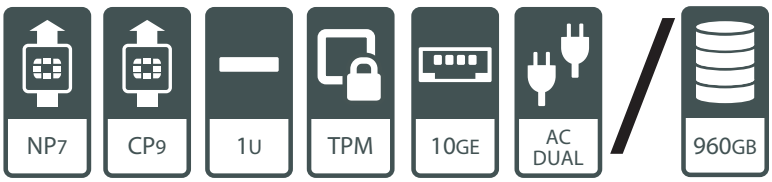
FortiGate 400F/401F Series





Interfaces

1. 1 x USB Port
2. 1 x Console Port
3. 2 x GE RJ45 MGMT/HA Ports
4. 16 x GE RJ45 Ports
5. 4 × 1GE/10GE SFP+ Slots
6. 4 × 10GE SFP+ Ultra Low Latency Slots
7. 8× 1GE SFP Slots



Trusted Platform Module (TPM)

The FortiGate 400F Series features a dedicated module that hardens physical networking appliances by generating, storing, and authenticating cryptographic keys. Hardware-based security mechanisms protect against malicious software and phishing attacks.

Access Layer Security

FortiLink protocol enables you to converge security and the network access by integrating the FortiSwitch into the FortiGate as a logical extension of the NGFW. These FortiLink enabled ports can be reconfigured as regular ports as needed.

Specifications

	FG-400F	FG-401F
Interfaces and Modules		
Hardware Accelerated GE RJ45 Interfaces	16	
Hardware Accelerated GE SFP Slots	8	
Hardware Accelerated 10GE SFP+ Slots	4	
Hardware Accelerated 10GE SFP+ Ultra Low Latency Slots	4	
GE RJ45 Management Ports	2	
USB Ports	1	
RJ45 Console Port	1	
Onboard Storage	0	2× 480 GB SSD
Trusted Platform Module (TPM)	Yes	Yes
Included Transceivers	2x SFP (SX 1 GE)	
System Performance — Enterprise Traffic Mix		
IPS Throughput [2]	12 Gbps	
NGFW Throughput [2, 4]	10 Gbps	
Threat Protection Throughput [2, 5]	9 Gbps	
System Performance and Capacity		
IPv4 Firewall Throughput (1518 / 512 / 64 byte, UDP)	79.5 / 78.5 / 70 Gbps	
IPv6 Firewall Throughput (1518 / 512 / 64 byte, UDP)	79.5 / 78.5 / 70 Gbps	
Firewall Latency (64 byte, UDP)	4.19 µs / 2.5 µs*	
Firewall Throughput (Packet per Second)	105 Mpps	
Concurrent Sessions (TCP)	7.8 Million	
New Sessions/Second (TCP)	500 000	
Firewall Policies	10 000	
IPsec VPN Throughput (512 byte) [1]	55 Gbps	
Gateway-to-Gateway IPsec VPN Tunnels	2000	
Client-to-Gateway IPsec VPN Tunnels	50 000	
SSL-VPN Throughput [6]	3.6 Gbps	
Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode)	5000	
SSL Inspection Throughput (IPS, avg. HTTPS) [3]	8 Gbps	
SSL Inspection CPS (IPS, avg. HTTPS) [3]	6000	
SSL Inspection Concurrent Session (IPS, avg. HTTPS) [3]	800 000	
Application Control Throughput (HTTP 64K) [2]	28 Gbps	
CAPWAP Throughput (HTTP 64K)	65 Gbps	
Virtual Domains (Default / Maximum)	10 / 10	
Maximum Number of FortiSwitches Supported	72	
Maximum Number of FortiAPs (Total / Tunnel)	512 / 256	
Maximum Number of FortiTokens	5000	
High Availability Configurations	Active-Active, Active-Passive, Clustering	

	FG-400F	FG-401F
Dimensions and Power		
Height x Width x Length (inches)	1.75 × 17.0 × 15.0	
Height x Width x Length (mm)	44.45 × 432 × 380	
Weight	14.11 lbs (6.4 kg)	14.33 lbs (6.5 kg)
Form Factor (supports EIA/non-EIA standards)	Rack Mount, 1 RU	
AC Power Consumption (Average / Maximum)	154.8 W / 189.2 W	161.1 W / 196.9 W
AC Power Input	100–240V AC, 50/60Hz	
AC Current (Maximum)	6A	
Heat Dissipation	645.58 BTU/h	671.85 BTU/h
Power Supply Efficiency Rating	80Plus Compliant	
Redundant Power Supplies (Hot Swappable)	Yes (Default dual AC PSU for 1+1 Redundancy)	
Operating Environment and Certifications		
Operating Temperature	32°–104°F (0°–40°C)	
Storage Temperature	-31°–158°F (-35°–70°C)	
Humidity	5%–90% non-condensing	
Noise Level	LPA 48 dBA / LWA 55 dBA	
Airflow	Side and Front to Back	
Operating Altitude	Up to 10 000 ft (3048 m)	
Compliance	FCC Part 15 Class A, RCM, VCCI, CE, UL/cUL, CB	
Certifications	USGv6/IPv6	

* Latency based on Ultra Low Latency (ULL ports)

Note: All performance values are "up to" and vary depending on system configuration.

[1] IPsec VPN performance test uses AES256-SHA256.

[2] IPS (Enterprise Mix), Application Control, NGFW and Threat Protection are measured with Logging enabled.

[3] SSL Inspection performance values use an average of HTTPS sessions of different cipher suites.

[4] NGFW performance is measured with Firewall, IPS and Application Control enabled.

[5] Threat Protection performance is measured with Firewall, IPS, Application Control and Malware Protection enabled.

[6] Uses RSA-2048 certificate.

Subscriptions

Service Category	Service Offering	A-la-carte	Bundles		
			Enterprise Protection	Unified Threat Protection	Advanced Threat Protection
FortiGuard Security Services	IPS Service	•	•	•	•
	Anti-Malware Protection (AMP) — Antivirus, Mobile Malware, Botnet, CDR, Virus Outbreak Protection and FortiSandbox Cloud Service	•	•	•	•
	URL, DNS & Video Filtering Service	•	•	•	
	Anti-Spam		•	•	
	AI-based Inline Malware Prevention Service	•	•		
	Data Loss Prevention Service [1]	•	•		
	OT Security Service (OT Detection, OT Vulnerability correlation, Virtual Patching, OT Signature / Protocol Decoders) [1]	•			
	Application Control		included with FortiCare Subscription		
	CASB SaaS Control		included with FortiCare Subscription		
SD-WAN and SASE Services	SD-WAN Underlay Bandwidth and Quality Monitoring Service	•			
	SD-WAN Overlay-as-a-Service for SaaS-based overlay network provisioning	•			
	SD-WAN Connector for FortiSASE Secure Private Access	•			
	FortiSASE subscription including cloud management and 10Mbps bandwidth license [2]	•			
NOC and SOC Services	FortiGuard Attack Surface Security Service (IoT Detection, IoT Vulnerability Correlation, and Security Rating Updates) [1]	•	•		
	FortiConverter Service	•	•		
	Managed FortiGate Service	•			
	FortiGate Cloud (SMB Logging + Cloud Management)	•			
	FortiAnalyzer Cloud	•			
	FortiAnalyzer Cloud with SOCaaS	•			
	FortiGuard SOCaaS	•			
Hardware and Software Support	FortiCare Essentials	•			
	FortiCare Premium	•	•	•	•
	FortiCare Elite	•			
Base Services	Internet Service (SaaS) DB Updates	included with FortiCare Subscription			
	GeoIP DB Updates				
	Device/OS Detection Signatures				
	Trusted Certificate DB Updates				
	DDNS (v4/v6) Service				

1. Full features available when running FortiOS 7.4.1
2. Desktop Models only

FortiGuard Bundles

FortiGuard Labs delivers a number of security intelligence services to augment the FortiGate firewall platform. You can easily optimize the protection capabilities of your FortiGate with one of these FortiGuard Bundles.

FortiCare Elite

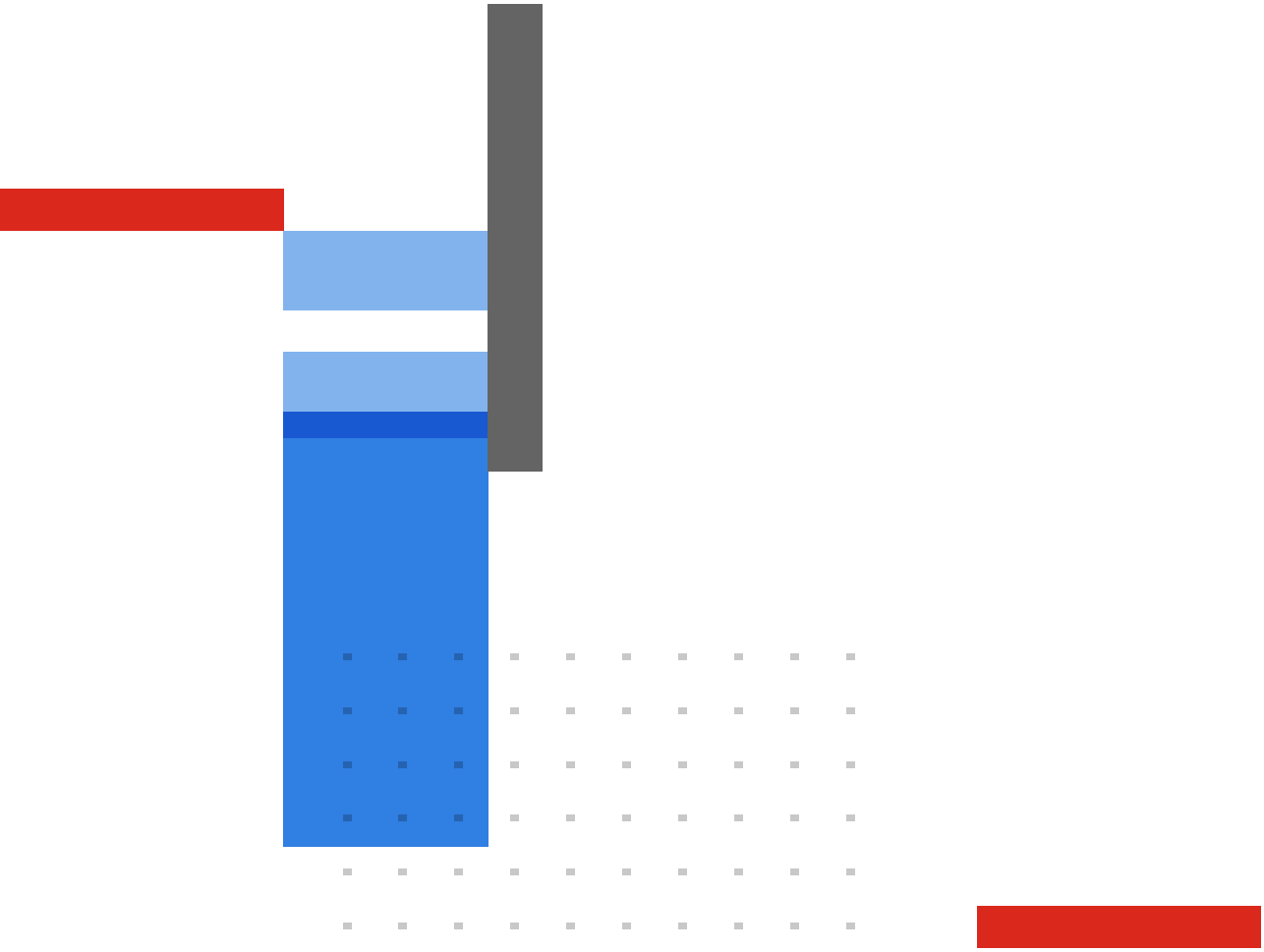
FortiCare Elite offers enhanced SLAs and quick issue resolution through a dedicated support team. It provides single-touch ticket handling, extended Extended End-of-Engineering-Support for 18 months, and access to the new FortiCare Elite Portal for a unified view of device and security health.

Ordering Information

Product	SKU	Description
FortiGate 400F	FG-400F	18 x GE RJ45 ports (including 1 x MGMT port, 1 X HA port, 16 x switch ports), 8 x GE SFP slots, 8 × 10GE SFP+ slots, SPU NP7 and CP9 hardware accelerated, dual AC power supplies.
FortiGate 401F	FG-401F	18 x GE RJ45 ports (including 1 x MGMT port, 1 X HA port, 16 x switch ports), 8 x GE SFP slots, 8 × 10GE SFP+ slots, SPU NP7 and CP9 hardware accelerated, 2× 480GB onboard SSD storage, dual AC power supplies.
Optional Accessories	**SKU**	**Description**
1 GE SFP LX Transceiver Module	FN-TRAN-LX	1 GE SFP LX transceiver module for all systems with SFP and SFP/SFP+ slots.
1 GE SFP RJ45 Transceiver Module	FN-TRAN-GC	1 GE SFP RJ45 transceiver module for all systems with SFP and SFP/SFP+slots.
1 GE SFP SX Transceiver Module	FN-TRAN-SX	1 GE SFP SX transceiver module for all systems with SFP and SFP/SFP+ slots.
10 GE SFP+ RJ45 Transceiver Module	FN-TRAN-SFP+GC	10 GE SFP+ RJ45 transceiver module for systems with SFP+ slots.
10 GE SFP+ Transceiver Module, Short Range	FN-TRAN-SFP+SR	10 GE SFP+ transceiver module, short range for all systems with SFP+ and SFP/SFP+ slots.
10 GE SFP+ Transceiver Module, Long Range	FN-TRAN-SFP+LR	10 GE SFP+ transceiver module, long range for all systems with SFP+ and SFP/SFP+ slots.
10 GE SFP+ Transceiver Module, Extended Range	FN-TRAN-SFP+ER	10 GE SFP+ transceiver module, extended range for all systems with SFP+ and SFP/SFP+ slots.
AC Power Supply	SP-FG400F-PS	AC power supply for FG-400/401F, FG-600/601F, power cable SP-FGPCOR-XX sold separately.

Fortinet CSR Policy

Fortinet is committed to driving progress and sustainability for all through cybersecurity, with respect for human rights and ethical business practices, making possible a digital world you can always trust. You represent and warrant to Fortinet that you will not use Fortinet's products and services to engage in, or support in any way, violations or abuses of human rights, including those involving illegal censorship, surveillance, detention, or excessive use of force. Users of Fortinet products are required to comply with the Fortinet EULA and report any suspected violations of the EULA via the procedures outlined in the Fortinet Whistleblower Policy.



FORTINET

www.fortinet.com

October 17, 2023

FG-400F-DAT-R09-20231017

ATESTADO DE CAPACIDADE TÉCNICA

Declaramos para os devidos fins que a empresa a Oi Soluções SA., CNPJ: 09.719.875/0001-12, sediada à Avenida das Nações Unidas, nº 13.947, Andar 9, Conj 91, Vila Gertrudes, São Paulo – SP, CEP 04794-000 –presta os serviços abaixo relacionados para *CASSI – Caixa de Assistência dos Funcionários do Banco do Brasil*, com sede em SIG, Quadra 4, Lote 575, Zona Industrial – Brasília (DF), CEP: 70610-910, inscrita Cadastro Nacional de Pessoa Jurídica do Ministério da Fazenda (CNPJ/MF) sob o número 33.719.485/0001-27, RJ vem executando os serviços de ativação, manutenção e suporte do fornecimento de link dedicado de internet, roteadores, Serviço de Gerenciamento Proativo dos links (ora denominado GIS) e firewalls conforme detalhamento abaixo:

Nº do contrato: **0265/2018**

Período de contratação: **60 meses**

SERVIÇOS CONTRATADOS:

Circuito IP CONNECT

O IP CONNECT é um serviço de acesso à Internet dedicado, através de acesso via Fibra Óptica com fornecimento de Roteadores e Gerenciamento Proativo, que oferece aos clientes a confiabilidade, qualidade e performance necessárias para o uso da Internet.

Gerencia e Gerenciamento Proativo (Gis)

Gestão Integrada de Serviços é um serviço gerenciado que inclui todos os itens necessários para o gerenciamento do ambiente WAN de nossos clientes pela Oi, através de um Portal Único via Web com visões consolidadas e on-line, processos baseados nas melhores práticas de mercado e profissionais altamente qualificados.

FUNCIONALIDADES – GESTÃO INTEGRADA DE SERVIÇOS	Avançado
Acesso Relatórios via WEB	✓
Abrangência NACIONAL	✓
Qtde. de USUÁRIOS logados simultaneamente	5 (cinco) usuários
Relatórios online de DESEMPENHO da Rede/Circuitos	✓
Visão Técnica da TOPOLOGIA da Rede com o status operacional de cada circuito	✓
INVENTÁRIO do CPE	✓
Gestão de SLA /SLM e Control Book	✓
Gerência PROATIVA de Falhas	✓
Link de Demonstração	✓
SLA de ATIVAÇÃO	30 (trinta) dias
Período de Armazenamento dos Relatórios no Portal	6 (seis) Meses

- Portal único com acesso seguro (Https) e acessível de dispositivos móveis com atualizações em tempo real das informações relevantes para a tomada de decisão;
- Utiliza ferramentas World Class, baseadas em processos ITIL (Information Technology Infrastructure Library);
- Visibilidade do comportamento da rede através do acesso via web dos relatórios de desempenho de todos os circuitos gerenciados;
- Garantia da continuidade do serviço;
- Acompanhamento de diversos indicadores via web;
- Torna-se viável investir o tempo dos recursos de TI e Telecom em outras atividades, como implantação de novas tecnologias, ou mesmo dedicar-se ainda mais ao seu core business;
- Reduzir custos da empresa podendo ao mesmo tempo ampliar o alcance do gerenciamento do ambiente;
- Suporte contínuo através de um gerenciamento proativo e consultivo fornecido pela equipe técnica especializada da Oi altamente qualificada (apenas na modalidade Qualifying);
- Mitigar e/ou Identificar indisponibilidades e atuar de forma rápida e eficaz na infra de TI e Telecom (apenas na modalidade Qualifying).
- Certificação CMSP Master
- Gerencia proativa
    - O nosso Centro de Gerência de Serviços (CGS) foi construído exclusivamente para o gerenciamento de redes corporativas com objetivo de administrar redes de longa distância (WAN) que tenham necessidade de gerenciamento de maneira integrada e proativa, com serviços de qualidade, a fim de concentrarem as atenções para seu core business.
    - O atendimento, providos a partir do nosso CGS, possui as seguintes características:
    - Atendimento em regime 24 x 7 x 365
    - Serviços telefônicos 0800 (toll free)
    - Dois contingentes internos: NOC e Help Desk

Solução de Segurança de Perímetro (MSS)/SDWAN - Firewall

Serviço de Segurança Gerenciada responsável pela monitoração e operação da solução de Segurança de Perímetro, sendo atendido pela equipe do SOC Oi, através do aluguel de equipamentos do tipo UTM Next Generation Firewall, com os seguintes serviços:

- Controle de Acesso (Firewall)
- Intrusion Detection System (IDS)
- Intrusion Prevention System (IPS)
- Filtro de Conteúdo e Filtro de Aplicação
- Antivírus de Gateway
- High Availability (Alta Disponibilidade)
- AntiSpam
- Integração base de usuários (AD, LDAP e RADIUS)
- IPSec VPN
- VPN SSL
- Policy Based Forward
- Policy Based Routing
- Fail-over de links e Roteamento
- LOG de Dados – Registro de eventos em um sistema
- Web Caching

Serviços
Emissão de alertas e relatórios
Atualização de licenças do equipamento
Configuração de regras/políticas de segurança
Levantamento de regras para ativação
Operação 24x7x365 do SOC Oi
Controle de sites e aplicações para melhoria de produtividade dos funcionários

Atestamos, ainda, que os serviços prestados pela CONTRATADA encontram-se em conformidade com todas as obrigações contratuais assumidas, sendo prestado com boa qualidade, não havendo fatos que desabonem a presente prestação de serviço.

Local: Brasília, 08 de dezembro de 2022

gov.br
Documento assinado digitalmente
IVAN ALMEIDA DA SILVA
Data: 12/12/2022 19:04:05-0300
Verifique em https://verificador.iti.br

Nome: Ivan Almeida da Silva
RG: 1.747.884
CPF: 893.038.061-15
Cargo: Analista de TI
Empresa: CASSI
Contatos: ivan.almeida@cassi.com.br

GERÊNCIA DE APOIO CORPORATIVO
(Compras, Contratações e Patrimônio)

CONTRATO DE PRESTAÇÃO DE SERVIÇOS – Nº 265/2018

Pelo presente instrumento de Contrato de Prestação de Serviços, de um lado, a **CAIXA DE ASSISTÊNCIA DOS FUNCIONÁRIOS DO BANCO DO BRASIL - CASSI**, pessoa jurídica de direito privado, associação de natureza assistencial sem fins lucrativos com Sede no Setor de Grandes Áreas Sul 613, Conjunto E, Bloco A, L2 Asa Sul – Brasília/DF, CEP: 70.200-903, inscrita no CNPJ/MF sob no. 33.719.485/0001-27, neste ato representada por seu Gerente Executivo Cesar Augusto Jacinto Teixeira, portador da cédula de identidade nº 320344526 SSP/SP, inscrito no CPF/MF sob nº 218.688.948-00, doravante simplesmente "**CASSI**" e, de outro lado a **OI S.A**, estabelecida rua do Lavradio, 71 – 02º andar - Centro, CEP 20230-070 – Rio de Janeiro, RJ, inscrita no CNPJ nº 76.535.764/0001-43, bem como a **OI MOVEL S.A** estabelecida no Setor Comercial Norte, Quadra 03 – Bloco A – andar térreo – Edifício Estação Telefônica Centro Norte – Brasília – DF – CEP: 70713-900, inscrita no CNPJ nº 05.423.963/0001-11 e a **TELEMAR NORTE LESTE S.A** estabelecida rua do Lavradio, 71 – 02º andar - Centro, CEP 20.230-070 – Rio de Janeiro, RJ, inscrita no CNPJ nº 33.000.118/0001-79, representada aqui pelo senhor Bruno Rudolfo Engelhardt – RG: 1488177 SSP-DF e CPF: 896.995.054-00 e pelo senhor Jamil Calixto Netto – RG: 38216340 SSP-SP e CPF: 363.105.488-24, doravante simplesmente "**CONTRATADA**", têm entre si justo e contratado o que se segue:

CLÁUSULA PRIMEIRA – OBJETO DO CONTRATO E SEUS ANEXOS

1.1- O presente Contrato tem por objeto a prestação dos serviços de comunicação de dados, por meio de uma rede IP*(Internet Protocol) Connect*, permitindo a comunicação de longa distância entre as dependências da **CASSI**, com o ponto central de processamento de dados no *Data Center* da **CASSI**, em Brasília/DF, conforme especificação nos Anexos deste Contrato, incluindo o fornecimento de roteadores e equipamentos de Firewall, bem como treinamento para os usuários da **CASSI**, tudo de acordo com o disposto neste Contrato e nos anexos abaixo relacionados, observada a legislação em vigor.

Anexo I –Especificação Técnica
Anexo II – Acordo de Nível de Serviço
Anexo III – Cronograma de Implantação (Macro)
Anexo IV – Disposição dos links e Valores

1.2- A execução dos serviços ora contratados estará condicionada ao início da vigência deste contrato.

1.3- O Contrato ajustado entre as **Partes** não tem caráter de exclusividade e não estabelece vínculo empregatício entre elas ou qualquer relação de subordinação pessoal entre seus administradores, diretores e/ou empregados.

CLÁUSULA SEGUNDA – DO VALOR DO CONTRATO

2.1- Pela prestação dos serviços, a **CASSI** pagará à **CONTRATADA**, para todos os serviços objeto deste contrato o valor mensal de **R$ 80.000,00** (oitenta mil reais), conforme tabela de preços unitários detalhados por dependência da **CASSI** no **Anexo IV,** totalizando **R$ 4.800.000,00 (quatro milhões e oitocentos mil reais)**. O valor mensal estipulado para cada dependência da **CASSI** será cobrado a partir da efetivação da sua instalação, mediante ateste da **CASSI**.

2.2- Os valores mensais constantes no **Anexo IV** serão fixos e irreajustáveis durante o período de vigência de 60 (sessenta) meses deste contrato.

2.3- A remuneração prevista no Contrato engloba todos os impostos e custos ou despesas de qualquer natureza a serem realizadas pela **CONTRATADA** para a execução dos serviços ora contratados de forma a cumprir as disposições do Contrato.

2.4- A **CONTRATADA** declara haver levado em conta na apresentação de sua proposta todos os tributos (impostos, taxas, emolumentos, contribuições fiscais e para-fiscais) incidentes sobre os serviços durante o período de vigência do Contrato, não cabendo qualquer reivindicação devido a erro nessa avaliação para efeito de solicitar revisão de preço ou reembolso em função de recolhimentos determinados pelas autoridades competentes.

2.5- A execução por parte da **CONTRATADA** de qualquer atividade não prevista no Contrato que ocasione aumento de custo e/ou prazo, sem a prévia e expressa autorização por escrito da **CASSI**, será de inteira responsabilidade da **CONTRATADA**, não respondendo a **CASSI**, seja a que título for, pelos custos e despesas ou por eventuais compensações.

CLÁUSULA TERCEIRA – DAS CONDIÇÕES DE PAGAMENTO E DA EMISSÃO DE NOTAS FISCAIS

3.1- O pagamento referente aos serviços efetivamente prestados pela **CONTRATADA**, e aceitos pela **CASSI**, será realizado mensalmente, no 10º (décimo) dia útil do mês subsequente ao da prestação dos serviços, após apresentação pela **CONTRATADA** de toda a documentação de cobrança à **CASSI**.

3.2- O início do faturamento se dará a partir da data de ativação do circuito na respectiva localidade e mediante confirmação da área técnica da **CASSI** dos serviços finalizados. Os valores da primeira e última mensalidade de cada circuito serão cobrados *pro rata die*.

3.3- Sendo identificada cobrança indevida após o pagamento da nota fiscal/fatura, a **CASSI** informará a **CONTRATADA** para que seja providenciado ajuste/desconto no valor correspondente ao próximo documento de cobrança.

3.4- Os pagamentos estão condicionados à satisfação de todas as obrigações oriundas e/ou decorrentes do Contrato e seus Anexos, e deverão ocorrer mediante depósito bancário em conta corrente formalmente indicada e de titularidade da **CONTRATADA**.

3.5- Havendo descumprimento das garantias de desempenho do serviço, a **CONTRATADA** deverá conceder na fatura mensal desconto de 1% (hum por cento) para cada hora passada além das 4 (quatro) horas totais acordadas de SLA.

3.6- Salvo acordo formal entre as **PARTES**, os prazos do Contrato e dos documentos dele integrantes vencem nas datas fixadas, independentemente de notificação ou interpelação judicial ou extrajudicial. A aceitação por uma das partes de pedidos de prorrogação de prazos não eximirá a parte contrária da aplicação das penalidades cabíveis por atraso no cumprimento dos novos prazos fixados para o fornecimento dos bens e/ou a execução dos serviços.

3.7- A **CONTRATADA** deverá arcar com o recolhimento de todos os tributos e encargos incidentes sobre os serviços ora contratados e devidos na forma da lei, obrigando-se a apresentar à **CASSI**, sempre que solicitado, os respectivos comprovantes de pagamento/recolhimento.

3.8- A **CONTRATADA** torna-se responsável pelas indenizações e reparação dos prejuízos eventualmente causados à **CASSI** ou a terceiros no descumprimento da legislação tributária.

3.9- A **CASSI** recolherá os tributos e encargos determinados por Lei e descontará tais valores de quantias que forem devidas à **CONTRATADA** por força do presente instrumento.

3.10- A **CONTRATADA** deverá observar, no momento da emissão das faturas/notas fiscais, faturas e recibos, o correto preenchimento destes documentos, devendo neles obrigatoriamente constar as informações relacionadas nos itens a seguir. A totalidade das cobranças deverá estar suportada pelas respectivas notas fiscais, faturas ou recibos.

(i) A dependência da **CASSI** indicada como destinatária na Discriminação dos Serviços, de acordo com a disposição dos links no **Anexo IV** deste Contrato, observando a localidade de prestação dos serviços;
(ii) As alíquotas dos impostos incidentes, conforme legislação Estadual e Municipal, e os respectivos valores;
(iii) A descrição dos serviços de forma clara, para que não haja nenhuma dúvida quanto à aplicação da legislação tributária;
(iv) O destaque no campo descrição dos serviços, quando aplicável, das retenções dos tributos e contribuições federais (IR Fonte, PIS, COFINS, CSLL e outros eventualmente aplicáveis);

CONFERIDO CONTRATADO

(v) O destaque no campo descrição dos serviços, quando aplicável, da retenção para a Seguridade Social – INSS. Além do destaque deverão ser discriminados os materiais e equipamentos previstos e/ou relacionados em contrato, que foram deduzidos da base de cálculo do INSS.

3.11- A **CONTRATADA** deverá enviar à **CASSI**, impreterivelmente até o dia 20 (vinte) de cada mês, todas as Notas Fiscais (NFs) de serviços emitidas no mês, sob pena de postergação nos prazos de pagamentos e troca (reemissão) da referida documentação. Caso a data limite para entrega das NFs coincida com sábados, domingos e feriados, as mesmas deverão ser entregues até o último dia útil anterior à data limite estabelecida.

3.11.1. - Quando se tratar de Notas Fiscais Eletrônicas (NFe's), a **CONTRATADA** deverá enviar os documentos para o e-mail nfefornecedores@cassi.com.br, impreterivelmente, até a data estipulada nesta Cláusula.

3.12- O não atendimento pela **CONTRATADA** de quaisquer das situações previstas nesta Cláusula, no que se refere à emissão correta dos documentos de cobrança, reservará à **CASSI** o direito de devolvê-los para a **CONTRATADA** para a devida reemissão, sem que isso acarrete qualquer ônus à **CASSI.**

3.13- A **CASSI** poderá suspender o pagamento de todo e qualquer valor devido à **CONTRATADA**, por força do Contrato, desde que autorizado pela **CONTRATADA**, enquanto existirem obrigações não cumpridas e/ou multas aplicadas, podendo, ainda, compensar todo e qualquer valor devido à **CASSI**.

3.14- A **CASSI** poderá, ainda, glosar os valores de retenções tributárias não realizadas pela **CONTRATADA** em notas fiscais de serviços processadas anteriormente.

3.15- A devolução da fatura/nota fiscal não aprovada, em nenhuma hipótese autorizará a **CONTRATADA** a suspender ou a deixar de efetuar os pagamentos devidos aos seus empregados.

3.16- As notas fiscais/faturas não poderão, em nenhuma hipótese, ser objeto de negócios, garantias, ou transações financeiras.

CLÁUSULA QUARTA - DAS OBRIGAÇÕES DA CONTRATADA

4.1- Sem prejuízo das disposições lançadas neste instrumento, a **CONTRATADA** se obriga a:

(i) prestar os serviços de acordo com o modo e prazos definidos neste instrumento;
(ii) enviar à **CASSI**, antes do início das atividades estabelecidas no Contrato, relação nominal de todos os empregados que irão prestar os serviços, destacando aqueles que deverão ter acesso aos sistemas computacionais e/ou às dependências físicas ou em quaisquer de suas instalações da **CASSI**, bem como indicando a pessoa responsável pela atualização, através dos sistemas disponibilizados pela **CASSI**, dos dados de tal relação. A relação e a indicação do responsável deverão ser firmadas pelo responsável legal da **CONTRATADA**. Em hipótese alguma os serviços objeto do Contrato poderão ser iniciados pela **CONTRATADA** antes do cumprimento das exigências deste item;
(iii) promover a atualização, num prazo máximo de 24 (vinte e quatro) horas, da relação nominal ou da pessoa responsável de que trata o item (ii), supra, sempre que houver qualquer tipo de alteração, seja de inclusão ou exclusão, temporária ou permanente de empregados, devendo nestas hipóteses, quando solicitado pela **CASSI**, indicar o motivo justificador da respectiva alteração;
(iv) solicitar crachás de identificação para todos os seus empregados designados a prestar serviços nas dependências físicas e/ou quaisquer instalações da **CASSI**, responsabilizando-se pelos custos decorrentes da confecção dos mesmos;
(v) treinar os empregados e/ou prepostos designados pela **CASSI**, quando for o caso, para a prestação dos serviços, sem qualquer custo ou ônus adicional para esta;
(vi) providenciar as informações e condições necessárias para a execução dos testes de aceitação a serem realizados, a critério da **CASSI**;

(vii) fornecer todos os equipamentos em regime de comodato, sendo 63 (sessenta e três) roteadores da marca HP modelo MSR1002-4 (Part number JG875A) para os circuitos de 20 Mbps e 10 Mbps, 1 (hum) roteador HP modelo MSR2003 (Part number JG411A) para o circuito de 300 Mbps, 1 (hum) Firewall FORTINET Fortigate 500E para o circuito de 300 Mbps e 63 (sessenta e três) Firewall FORTINET Fortigate 30E para os circuitos de 20 Mbps e 10 Mbps. A **CONTRATADA** deverá garantir o funcionamento dos equipamentos afim de que não haja interrupções no fornecimento dos serviços objeto deste instrumento contratual, e realizar a substituição sem ônus para a **CASSI** sempre que necessário, a fim de que o serviço não tenha interrupções.

(viii) informar à **CASSI** com antecedência de 5 (cinco) dias caso a **CONTRATADA** necessite realizar atividades de atualização e manutenção na sua plataforma de prestação de serviços, tais como reconfigurações, atividades de manutenção, entre outros, sendo necessária a interrupção do serviço;

(ix) garantir que a **CASSI** poderá retirar ou adicionar circuitos de sua dependência (relação Anexo IV) de acordo com a sua necessidade. Não haverá ônus para circuitos retirados/desativados após 12 (doze) meses da sua data de ativação;

(x) possibilitar o aumento ou a diminuição da velocidade dos circuitos de Internet, em incrementos/decrementos de 10 Mbps, com alteração no valor mensal proporcional ao custo unitário do Mbps.

(xi) caso seja identificado um roteador ou firewall com uso de CPU ou memória superior a 70%, este deverá ser substituído ou atualizado sem ônus adicional para a **CASSI**.

4.2- A **CONTRATADA** declara, reconhece e garante que tem experiência, qualificação técnica e capacidade econômica, necessárias para executar com eficiência e qualidade o objeto contratual, por sua conta e risco, de acordo com as condições e requisitos contratuais.

CLÁUSULA QUINTA - DAS OBRIGAÇÕES DA CASSI

5.1- Sem prejuízo das demais disposições do Contrato e de seus Anexos, constituem obrigações e responsabilidades da **CASSI**:

(i) efetuar os pagamentos devidos à **CONTRATADA** de acordo com o estabelecido neste instrumento;

(ii) informar à **CONTRATADA**, por escrito, as razões que motivaram eventual rejeição dos serviços executados;

(iii) garantir o acesso às suas dependências dos empregados e prepostos indicados pela **CONTRATADA** para execução do objeto do Contrato.

CLÁUSULA SEXTA – DA VIGÊNCIA E RESCISÃO

6.1- O presente Contrato de Prestação de Serviços terá vigência de 60 (sessenta) meses, contados da data de assinatura, extinguindo-se de pleno direito ao final deste prazo, salvo celebração de termo aditivo de prorrogação.

6.2- O presente Contrato poderá ser rescindido por qualquer das partes, após 12 meses contados do início de sua vigência, a qualquer tempo, mediante prévia e expressa comunicação à parte contrária, com antecedência mínima de **90 (noventa)** dias, resguardada a obrigação da **CONTRATADA** de executar os serviços em aberto e o direito aos créditos proporcionais até a efetiva data de rescisão.

6.3- Caso a **CASSI** opte pela desativação de circuito antes de 12 (doze) meses de vigência de contrato, poderá pagar à **CONTRATADA**, multa rescisória equivalente a 10% das próximas 12 parcelas vincendas deste circuito, contados do mês posterior ao mês do pedido de desativação.

CONTRATOS CONFERIDO

6.4- **A CASSI** poderá rescindir o presente instrumento, sem necessidade de prévia notificação ou dever de qualquer indenização, na hipótese de a **CONTRATADA** ou o **GRUPO EMPRESARIAL** ao qual pertença:

(i) incorrer no descumprimento da Cláusula Décima Primeira – DA PREVENÇÃO E COMBATE À CORRUPÇÃO;
(ii) incorrer na prática de atos lesivos à Administração Pública Nacional ou Estrangeira;
(iii) for incluído no Cadastro Nacional de Empresas Inidôneas e Suspensas - CEIS (http://www.portaldatransparencia.gov.br/sancoes/ceis);
(iv) for incluído no Cadastro Nacional das Empresas Punidas – CNEP; (http://www.portaldatransparencia.gov.br/sancoes/cnep);
(v) incorrer no recebimento de sanção pela prática de ato tipificado no Artigo 5º, caput e incisos, da Lei nº 12.846, de 01.08.2013.

6.5- A rescisão também poderá ocorrer, quando a **CONTRATADA:**

(i) motivar a suspensão dos serviços por parte de autoridades competentes. Neste caso, a **CONTRATADA** responderá por eventual aumento de custo daí decorrentes e por perdas de danos que a **CASSI,** como consequência, venha sofrer;
(ii) deixar de comprovar sua regularidade fiscal e trabalhista, inclusive contribuições previdenciárias e depósitos de FGTS, para com seus empregados;
(iii) for responsável por operações em curso anormal junto a qualquer dependência da **CASSI**, desde que o endividamento venha a comprometer a execução do Contrato;
(iv) vier a ser declarada inidônea por qualquer órgão da Administração Pública;
(v) vier a ser atingida por protesto de título, execução fiscal ou outros fatos que comprometam a sua capacidade econômico-financeira; e
(vi) utilizar em seu benefício próprio ou de terceiros informações sigilosas às quais tenha acesso por força de suas atribuições contratuais.

6.6- Os casos de rescisão contratual serão formalmente motivados nos autos do processo, assegurado o contraditório e a ampla defesa.

6.7- As responsabilidades imputadas à **CONTRATADA**, por prejuízos decorrentes de ações delitivas perpetuadas contra a **CASSI**, não cessam com a rescisão do Contrato.

6.8- A rescisão do presente Contrato não liberará a **CASSI** da obrigação de pagar remuneração devida pelos serviços já prestados.

6.9- Os direitos e obrigações de ambas as partes relativos à confidencialidade, garantias, preço e pagamentos, sobreviverão à rescisão deste Contrato.

CLÁUSULA SÉTIMA – DA MULTA

7.1- Os atos praticados pela **CONTRATADA**, prejudiciais à execução do contrato, sujeitam-na às seguintes sanções:

(i) advertência/notificação;
(ii) multa.

7.2- Nenhuma sanção será aplicada sem o devido processo administrativo. A aplicação das penalidades ocorrerá após defesa prévia do interessado, no prazo de 5 (cinco) dias úteis a contar da intimação do ato. A **CONTRATADA** terá o prazo de 5 (cinco) dias úteis para apresentação de recurso a contar da intimação do ato.

7.3- A advertência poderá ser aplicada quando ocorrer:

(i) descumprimento devidamente comprovado das obrigações contratuais, especialmente aquelas relativas às características dos bens, qualidade, quantidade, prazo de atendimento de suporte ou cronograma de implantação, recusa do fornecimento ou entrega, ressalvados os casos fortuitos ou de força maior e aqueles que não acarretem prejuízos para a **CASSI**;
(ii) execução insatisfatória ou pequenos transtornos ao desenvolvimento do contrato desde que sua gravidade não recomende a aplicação da suspensão temporária ou declaração de inidoneidade.

7.4- A **CASSI** poderá aplicar à **CONTRATADA** multa por inexecução total ou parcial do Contrato, no valor de 10% das últimas 6 (seis) faturas ou, no primeiro semestre do contrato, das faturas dos meses já decorridos, que deverá ser paga após encerramento do processo administrativo.

(i) Aplicar multa moratória, não compensatória, caso haja atraso por parte da **CONTRATADA** no cumprimento das garantias do prazo estabelecido para a recuperação/restabelecimento dos serviços conforme **Anexo II, itens 2.3, 3.4 e 4.4**, por hora de atraso de 0,5% sobre o valor mensal do contrato.

7.5- O valor da multa estipulada na cláusula anterior será elevado em 1% (um por cento) a cada reincidência, até o limite de 20% (vinte por cento) do valor das últimas 6 (seis) faturas.

7.6- A multa poderá ser aplicada cumulativamente com as demais sanções, não terá caráter compensatório, e a sua cobrança não isentará a **CONTRATADA** da obrigação de indenizar eventuais danos na extensão das disposições dessa Cláusula.

7.7- A multa aplicada à **CONTRATADA** e os danos diretos por ela provadamente causados à **CASSI** serão deduzidos de qualquer crédito a ela devido, cobrados diretamente ou judicialmente, respeitando o limite indicado nesta Cláusula.

CLÁUSULA OITAVA - COMUNICAÇÃO ENTRE AS PARTES:

8.1- Todas as comunicações entre as **Partes** relativas ao Contrato deverão ser feitas por escrito e encaminhadas aos destinatários listados neste Instrumento e somente serão consideradas como efetivamente realizadas mediante o recebimento da Parte destinatária.

(i) Para a **CASSI**:

CAIXA DE ASSISTÊNCIA DOS FUNCIONÁRIOS DO BANCO DO BRASIL – CASSI
SGAS 613, Conjunto E, Bloco A, L2 Sul, Brasília (DF) – CEP 70.200.903.

Para assuntos relacionados à parte operacional/técnica do Contrato:
At.: Sr. Rodrigo da Silva Leite – e-mail: gti.construcao@cassi.com.br – Tel: (61) 3212-5191.

Para assuntos comerciais do Contrato e demais comunicados/notificações:
At.: Juliana Sousa - e-mail:contratos@cassi.com.br Tel: (61) 3212-5371.

(ii) Para a **CONTRATADA**:

OI MÓVEL S/A, OI S/A E TELEMAR NORTE LESTE S/A:
Setor Comercial Norte, Quadra 03, Bloco A - Andar Térreo - Parte 02 Edifício Estação Telefônica Centro Norte
At.: Sr.: Frederico Rodrigues Moreira - e-mail: frederico.moreira@oi.net.br – Tel: (61) 3131-3152.

CONFERIDO CONTRATOS

CLÁUSULA NONA – DAS DISPOSIÇÕES GERAIS

9.1- As **PARTES** se obrigam a tratar de forma confidencial, pelo prazo de 5 (cinco) anos após o termino deste contrato, todos os dados e ou informações, bem como materiais, plantas e croquis, segredos comerciais, marcas, criações, desenhos, especificações técnicas e comerciais da outra **Parte** e/ou dos usuários ("Informações Confidenciais"), aos quais venham a ter acesso por força deste instrumento, obrigando-se a não permitir que nenhum de seus empregados ou terceiros sob a sua responsabilidade façam uso destas informações confidenciais.

9.2- As **PARTES** reconhecem que não se estabelecerá qualquer vínculo empregatício entre a **CASSI** e os prepostos da **CONTRATADA** que trabalham na execução dos serviços objeto deste contrato. A **CONTRATADA** assume a obrigação de suportar espontânea e integralmente todos os ônus decorrentes de quaisquer processos administrativos ou judiciais de qualquer natureza, inclusive reclamações trabalhistas, que sejam instauradas contra a **CASSI** pelos referidos trabalhadores, tais como: condenações a qualquer título, custas judiciais, honorários de perito, assistentes técnicos e advogados, inclusive patrono da **CASSI.**

9.3- Na hipótese de fusão, cisão, incorporação ou associação da **CONTRATADA** com outrem, a **CASSI** reserva-se ao direito de rescindir o contrato ou continuar sua execução com a empresa resultante da alteração social, desde que mantidas as condições contratuais então vigentes.

9.4- A não utilização, pelas partes, de qualquer dos direitos assegurados neste contrato, ou na lei em geral, não implica em novação, não devendo ser interpretada como desistência de ações futuras. Todos os meios postos à disposição neste contrato são cumulativos e não alternativos, inclusive com relação a dispositivos legais.

9.5- A omissão ou tolerância das partes em exigir o estrito cumprimento das disposições contratuais, não constituirá novação ou renúncia, nem lhes afetará o direito de, a qualquer tempo, exigir o fiel cumprimento do avençado.

9.6- A **CASSI** se exime da responsabilidade do pagamento de qualquer serviço executado pela **CONTRATADA** sem a sua devida autorização ou conhecimento.

9.7- Cada **Parte** será a única responsável pelas infrações que cometer quanto ao direito de uso de materiais, equipamentos, *softwares* ou processos de execução protegidos por registros de marcas e concessão de patentes, respondendo diretamente por indenizações, taxas ou comissões que forem devidas, bem como por reclamações resultantes de sua utilização inadequada.

9.8- Nenhuma das **PARTES** poderá ceder ou transferir, no todo ou em parte, ainda que em função de reestruturação societária, fusão, cisão e incorporação, os direitos e obrigações decorrentes do Contrato, inclusive seus créditos, sem a prévia e expressa autorização por escrito da outra **PARTE**.

9.9- Em caso de conflito de interpretação de cláusulas deste instrumento e seus anexos, prevalecerão as disposições do contrato.

CLÁUSULA DÉCIMA – RESPONSABILIDADE SOCIOAMBIENTAL

10.1 A **CONTRATADA** se obriga durante toda a vigência do presente contrato, sob pena de rescisão imediata do mesmo a:

10.1.1 cumprir os preceitos e determinações legais concernentes às normas de Segurança e Medicina no Trabalho, bem como as convenções e acordo trabalhistas e sindicais referentes às categorias de trabalhadores empregados pelas partes;

10.1.2 não contratar ou permitir que seus subcontratados contratem mão-de-obra que envolva a exploração de trabalhos forçados ou trabalho infantil;

10.1.3 não empregar trabalhadores menores de 16 (dezesseis) anos de idade, salvo na condição de aprendiz a partir dos 14 (quatorze) anos de idade, conforme estabelecido na Constituição Federal, artigo 7º, inciso XXXIII e na Lei nº 10.097, de 19.12.2000 e da Consolidação das Leis do Trabalho;

10.1.4 não empregar adolescentes até 18 anos em locais prejudiciais à sua formação, ao seu desenvolvimento físico, psíquico, moral e social, bem como em locais e serviços perigosos ou insalubres, em horários que não permitam a frequência à escola e, ainda, em horário noturno, considerado este o período compreendido entre as 22:00 e 05 horas;

10.1.5 não adotar práticas de discriminação negativa e limitativas ao acesso, ao emprego ou à sua manutenção.

10.1.6 As partes se obrigam ainda a divulgar entre seus fornecedores, o compromisso assumido nesta cláusula, incentivando sempre a sua adoção.

CLÁUSULA DÉCIMA PRIMEIRA- DA PREVENÇÃO E COMBATE À CORRUPÇÃO:

11.1- A **CONTRATADA** declara ter ciência e compromete-se a observar integralmente os preceitos da Lei 12.846/2013, no exercício de seu relacionamento com a **CASSI** e, notadamente, não incorrer em qualquer das situações previstas no Artigo 5º da Lei 12.846/2013.

11.2- A **CONTRATADA** declara conhecer e compromete-se a respeitar a Política de Relacionamento com Fornecedores e Prestadores de Serviços Assistenciais da **CASSI**, disponível na Internet, no endereço www.cassi.com.br.

11.3- A **CONTRATADA** compromete-se a não utilizar o negócio jurídico objeto do presente Contrato como meio para cometimento de infração prevista na Lei 12.846/2013.

CONFERIDO CONTRATOS

CLÁUSULA DÉCIMA SEGUNDA – DO FORO

12.1- As **PARTES** elegem o Foro da cidade de Brasília/DF, como o único competente para dirimir as questões decorrentes do presente Contrato, renunciando a qualquer outro por mais privilegiado que seja.

E, por estarem justas e contratadas, as partes assinam o presente instrumento em 2 (duas) vias de igual teor e forma, na presença das testemunhas abaixo indicadas.

Brasília (DF), 18 de agosto de 2019.

Pela **CASSI**:

Nome: Cesar Augusto Jacinto Teixeira
CPF: 218.688.948-00

Pela **CONTRATADA**:

Nome: Bruno Rudolfo Engelhardt
CPF: 896.995.054-00

Nome: Jamil Calixto Netto
CPF: 363.105.488-24

Testemunhas:

Nome: Frederico Rodrigues
CPF: 053.492.537-51

Nome: Juliana Sousa
CPF: 725.551.061-20

ANEXO I – ESPECIFICAÇÃO TÉCNICA

1. Solução IP Connect:

A solução IP CONNECT proposta pela **CONTRATADA** está considerando o fornecimento de Roteadores e o Gerenciamento dos Circuitos de maneira proativa, por meio da ferramenta OI GIS – Gestão Integrada de Serviços, e ainda o fornecimento de treinamento para a funcionalidade, conforme detalhamento a seguir:

1.1. Roteadores

Banda dos Circuitos	Marca	Modelo	Part Number
10Mb e 20Mb	HP	MSR1002-4	JG875A
300 Mbps	HP	MSR2003	JG411A

1.2. OI GIS – Gestão Integrada de Serviços

A Gestão Integrada de Serviços é um serviço gerenciado que inclui todos os itens necessários para o gerenciamento do ambiente WAN da **CASSI** pela **CONTRATADA**, através de um Portal Único via Web com visões consolidadas e on-line, processos baseados nas melhores práticas de mercado e profissionais altamente qualificados.

1.2.1. Descrição do Serviço

O produto OI Gestão Integrada de Serviços ofertada nesta cotação refere-se à modalidade Avançado. Nesta modalidade, a **CASSI** possuirá:

(i) Visibilidade da topologia, da disponibilidade da rede e do inventário online;
(ii) Acompanhamento do histórico dos chamados de falhas;
(iii) Proatividade quanto à falha de seus enlaces e CPE.

O atendimento, provido a partir do Centro de Gerência de Serviços CGS da **CONTRATADA**, possui as seguintes características:

(i) Atendimento em regime 24 x 7 x 365;

(ii) Serviços telefônicos 0800 (toll free);

(iii) Dois contingentes internos: NOC e Help Desk.

Este atendimento está estruturado com os seguintes níveis operacionais:

Primeiro Nível: Help Desk, responsável pela interação remota com o cliente principalmente nas ocorrências detectadas pró-ativamente e também pela abertura via Sistema de Atendimento de casos, tais como: pedidos de informações, incidentes, problemas ou solicitações de mudanças; e notificações automáticas.

Segundo Nível: NOC, responsável pela triagem e detecção de problemas, acionamento/acompanhamento/resolução de problemas e eventual escalonamento ao Terceiro Nível (Field Support). Os analistas do NOC interagem com o Help Desk e o Field Support via Sistema de Atendimento.

Terceiro Nível: *Field Support*, responsável pelo gerenciamento de resolução de problemas in loco que inclui a atividade de coordenação remota dos serviços de campo, dos serviços que foram previamente contratados pela **CASSI**. Os tempos de resolução são registrados no sistema para controle do Nível de Serviço contratado.

O Sistema de Gerência de Falhas, acessado via portal web, disponibiliza o acompanhamento no gerenciamento de ocorrências/falhas permitindo:

(i) Tratamento histórico da informação, no sistema ou via relatórios.
(ii) Histórico de ocorrência de falhas por equipamento/link.

Características:

São funcionalidades disponíveis na modalidade Avançado:

FUNCIONALIDADES – GESTÃO INTEGRADA DE SERVIÇOS	Avançado
Acesso Relatórios via WEB	✓
Abrangência NACIONAL	✓
Qtde. de USUÁRIOS logados simultaneamente	**5 (cinco) usuários**
Relatórios online de DESEMPENHO da Rede/Circuitos	✓
Visão Técnica da TOPOLOGIA da Rede com o status operacional de cada circuito	✓
INVENTÁRIO do CPE	✓
Gestão de SLA /SLM e Control Book	✓
Gerência PROATIVA de Falhas	✓
Link de Demonstração	✓
SLA de ATIVAÇÃO	**30 (trinta) dias**
Período de Armazenamento dos Relatórios no Portal	**6 (seis) Meses**

1.3. Oi Gestão Segurança com FIREWALL

O produto OI Gestão Segurança a ser fornecido pela **CONTRATADA** refere-se à modalidade PREMIUM, conforme detalhamento a seguir:

SERVIÇOS	PREMIUM
Monitoração de detecção de intrusos*	✓
Relatórios gerenciais mensais	✓
Atualização de **licenças** do equipamento	✓
Limite de configuração de 50 **regras/políticas** de segurança	✓
Levantamento de **regras** para ativação	✓
Serviço de Gerenciamento Proativo do SOC Oi **Firewall /IDS**	✓
Proteção contra ataques maliciosos e intrusos	✓
Controle de sites e aplicações para melhoria de produtividade dos funcionários **Filtro de conteúdo e Anti-Vírus Gateway**	✓

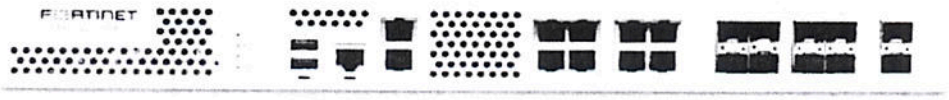
Característica deste atendimento:

(i) Proteção contínua, com gerenciamento e monitoração 24 x 7 X 365;

(ii) Disponibilização de relatórios mensais enviados pelo SOC.

Equipamentos a serem fornecidos:

Circuito 300Mb: FORTIGATE 500E:



https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_500E.pdf

Part Number	Descrição RFI (Resumo) Informar
FG-500E	2 x 10GE SFP+ slots, 10 x GE RJ45 ports (including 1 x MGMT port, 1 X HA port, 8 x switch ports), 8 x GE SFP slots, SPU NP6 and CP9 hardware accelerated
FC-10-0500E-950-02-12	UTM Protection (24x7 FortiCare plus Application Control, IPS, AV, Web Filtering and Antispam Services)

Circuitos de 10Mb e 20Mb: FORTIGATE 30E:

https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_FortiWiFi_30E.pdf

Part Number	Descrição RFI (Resumo) Informar
FG-30E	5 x GE RJ45 ports (Including 1 x WAN port, 4 x Switch ports), Max managed FortiAPs (Total / Tunnel) 2 / 2
FC-10-0030E-950-02-12	UTM Bundle (24x7 FortiCare plus NGFW, AV, Web Filtering and Antispam Services)

Os firewalls contemplarão as seguintes funcionalidades:

(i) VPN IPSEC e SSL.
(ii) QoS.
(iii) Filtro WEB.
(iv) Controle de aplicações (Application Control).
(v) IPS (Intrusion Prevention System).
(vi) Antivírus/Anti-malware.
(vii) SDWAN (Software-Defined WAN).
(viii) Procotolos de roteamento dinâmico OSPF e BGP.
(ix) Certificação do "ICSA Labs" para os itens de Firewall, IPsec, IPS, Antivírus e SSL-VPN.

1.4. Treinamento FIREWALL FORTINET

A **CONTRATADA** fornecerá treinamento oficial dos equipamentos FORTINET, conforme detalhamento a seguir:

Treinamento	Part Number	Duração	Participantes
FortiGate (I) Security v6	WCA-AC-OR-Flex-FTN-OT-NSE4-1	3 dias/24 horas	5
FortiGate (II) Infrastructure v6	WCA-AC-OR-Flex-FTN-OT-NSE4-2	2 dias/16 horas	5

Nos serviços a serem prestados pela **CONTRATADA** estão inclusos:

(i) Despesas com deslocamento do instrutor (Passagem aérea, hospedagem e traslado);

(ii) Laboratório virtual oficial do fabricante;

(iii) Material oficial (E-book).

Itens de responsabilidade da **CASSI**:

(i) Sala de aula – Localidade: Brasília/DF;

(ii) Coffee Break;

(iii) Computadores para os participantes;

(iv) Internet de no mínimo 5mb sem controle de portas, Windows 8.1 ou 10 com permissões de administrator, Switch especifico para a sala de treinamento;

(v) Data show e FlipChart.

A data de realização do curso deverá ser solicitada pela área técnica da **CASSI** com no mínimo 60 (sessenta) dias de antecedência ao interesse, visando avaliar a disponibilidade de agenda do instrutor.

1.5. Prazo de Ativação

Para ativação do serviço Oi Gestão Segurança, será necessário o fornecimento das informações de regras de Firewall e políticas de segurança por parte da **CASSI**, responsável por essas informações.

Na ausência de envio das informações técnicas necessárias para configuração dos Equipamentos de Segurança de Rede em até 30 (trinta) dias corridos após a solicitação do serviço, a Oi realizará a ativação do equipamento em modo de detecção de ataques (IDS).

As demais funcionalidades contratadas serão aplicadas quando a **CONTRATADA** receber a documentação necessária por parte do cliente, de modo o configurar as regras de Firewall e políticas de segurança. Durante este período de aguardo, a **CONTRATADA** não poderá ser responsabilizada quanto à prevenção de ataques às portas de acesso LAN/WAN (Firewall e IPS).

Para ativação do serviço, a área técnica da **CASSI** deverá encaminhar os seguintes documentos:

(i) topologia lógica detalhada;

CONTRATOS CONFERIDO

(ii) topologia física detalhada;

(iii) inventário lógico detalhado (relação de softwares, configurações e informações que constam em cada um dos ativos que compreendem o escopo do serviço contratado);

(iv) inventário físico detalhado (relação de ativos e informações de ativos que compreendem o escopo do serviço contratado);

(v) formulário de regras de firewall (se aplicável) contendo as regras iniciais a serem configuradas no ambiente, conforme escopo de serviços contratado;

(vi) formulário de regras de IPS contendo as regras iniciais a serem configuradas no ambiente, conforme escopo de serviços contratado;

(vii) contatos (limite de 5 pontos de contato) e escalation, contendo informações, como nome, telefone fixo, telefone celular, e-mail, ordem de escalation e condição para escalation. Estes contatos serão os responsáveis por realizar solicitações ao SOC OI, assim como serão o ponto de contato do SOC OI para o caso de resolução de algum problema.

Após realizadas todas as configurações necessárias, é agendada uma data para o teste de ativação junto a **CONTRATADA**.

1.6. Restrições

(i) não inclui suporte de campo (exceto em caso de atualização de firmware, quando pode ser necessário);

(ii) tarefas que não necessitem, obrigatoriamente, de acesso local às dependências da **CASSI** serão realizadas remotamente;

(iii) atividades com necessidade de realizar *in loco* tais como, alteração do cabeamento, energização dos equipamentos ou mudança física, não terão cobertura, exceto na instalação;

(iv) a **CONTRATADA** não realizará configuração das estações de trabalho dos usuários, bem como em nenhum outro equipamento, que não o objeto desta proposta comercial.

(v) não haverá nenhuma programação ou desenvolvimento de códigos, por parte da **CASSI**;

(vi) não está contemplado fornecimento de switches, servidores e quaisquer outros dispositivos de TI ficando de responsabilidade da **CASSI**, com exceção dos já descritos neste instrumento contratual como roteadores e os equipamentos de Firewall para o funcionamento adequado da solução.

(vii) nos casos onde houver a necessidade de configuração de VPN IPSEC com terceiros, a **CONTRATADA** enviará formulário de criação de VPN para o contato técnico da **CASSI**, para que este encaminhe ao responsável.

1.7. Tabela RACI – Matriz de Responsabilidade

Serviços Gerenciados de Segurança Oi	OI	CASSI
Administração de equipamentos (Firewalls, IPS e NGFW/UTM)	R	IC
Configuração de regras de firewall (inclusão, exclusão e alteração)	R	ICA
Configuração de regras de IPS/IDS (inclusão, exclusão e alteração)	R	ICA
Configuração de filtro de URL/Conteúdo	R	ICA
Monitoração e gestão de alarmes 24 x 7 x 365	R	-
Resolução de Incidentes, Requisições e Dúvidas para os aplicativos do escopo do Contrato	R	ICA
Retorno do chamado/ticket	R	I
Atualizações de firmware e sistema operacional	R	IA
Reporte mensal do acompanhamento da operação	R	I
Interface de contato e relacionamento com o fabricante para resolução de problemas, incidentes, atualizações e demais necessidades de operação dos Firewalls de UR	R	C
Resolução dos Problemas registrados	R	ICA
Relatórios mensais de nível de serviço, capacidade e desempenho	R	I
Contrato de licenças de suporte com fabricante da solução de segurança em vigência e com RMA incluso (troca de equipamento defeituoso em garantia)	R	-
RMA on-site para os casos de falhas de hardware/software	R	-
Fornecimento de acesso a página de licenciamento do fabricante, com usuário e senha para a CASSI realizar gestão de licenças, abertura de tickets e para acionamento de RMA	R	-
Perfil de acesso leitura e escrita no CPE / Appliance	R	-
Entrega de topologia de rede e documentação referente a ativos e ambientes considerados críticos	I	R

R – Responsável; A – Responsável pela Aprovação; C – Consultado; I – Informado;

1.8. Início do projeto pela CONTRATADA:

(i) Análise da infraestrutura de rede para confirmar a possibilidade de acesso ao dispositivo a ser gerenciado (plataforma);

(ii) Update em firmware, versão de software e demais alterações que forem pertinentes, a serem realizadas pela **CASSI**;

(iii) Avaliação inicial de risco das regras vigentes (avaliar possibilidade);

(iv) Identificação de alterações se pertinente (avaliar possibilidade);

(v) Definição de perfis de usuários. A **CASSI** terá usuário somente de consulta e a **CONTRATADA** de administração;

(vi) Definição dos pontos de contato na **CASSI** – lista de recorrências.

2. Matriz de Validação Técnica

Item	DESCRIÇÃO DO ITEM	VALIDAÇÃO DA CONTRATADA	
1.	**O serviço deve contemplar as seguintes características:**		
1.1	Circuito de comunicação com a Internet, banda simétrica (download = upload) e no mínimo 6 endereços IPv4 válidos.	Atende Totalmente	-
1.2	Roteador: Fornecimento de Roteadores para cada um dos circuitos de acesso à Internet.	Atende Totalmente	-
	Dimensionado os roteadores para operar com carga máxima de CPU e memória de 70% (setenta por cento) quando a utilização do circuito for igual à capacidade contratada.	Atende Totalmente	-
	Deve possuir no mínimo 2 (duas) interfaces GigabitEthernet (1000Base-T) para conexão com a rede interna da **CASSI** .	Atende Totalmente	-
	Deve permitir acesso da **CASSI** com no mínimo privilégio de leitura (read-only), via porta console, telnet, SSH e SNMP.	Atende Totalmente	-
1.3	Firewall: Deve ser do tipo NGFW (Next-Generation Firewall).	Atende Totalmente	-
	Deve ser da marca Fortinet dimensionado para operar com carga máxima de CPU e memória de 70% (setenta por cento) quando a utilização de "VPN IPSEC" for igual à capacidade do circuito contratado. Modelos de referência:	Atende Totalmente	-
	Datacenter: Fortigate 500E	Atende Totalmente	-
	Demais localidades: Fortigate 30E	Atende Totalmente	-
	Deve possuir no mínimo 4 (quatro) interfaces GigabitEthernet (1000Base-T) para conexão com a rede interna da **CASSI** .	Atende Totalmente	-
	Deve permitir acesso da **CASSI** com privilégio de escrita (write), via porta console, telnet, SSH, HTTP, HTTPS e SNMP.	Atende Parcialmente	Será avaliado com o SOC da **CONTRATADA** a regra de liberação de acesso, posteriormente a assinatura do contrato.
1.4	Gerenciamento proativo do circuito: Monitoração da disponibilidade, abertura automática de incidentes em caso de indisponibilidade ou degradação do desempenho, acompanhamento da recuperação do incidente.	Atende Totalmente	-
1.5	Gerenciamento proativo da segurança: Prevenção, detecção, gestão e resposta a incidentes, avaliação de vulnerabilidades e monitoramento e demais itens relacionados à segurança da informação.	Atende Totalmente	-
2.	**Os firewalls devem contemplar as seguintes funcionalidades:**		
2.1	VPN IPSEC e SSL.	Atende Totalmente	-
2.2	QoS.	Atende Totalmente	-
2.3	Filtro WEB.	Atende Totalmente	-
2.4	Controle de aplicações (Application Control).	Atende Totalmente	-
2.5	IPS (Intrusion Prevention System).	Atende Totalmente	-
2.6	Antivírus/Anti-malware.	Atende Totalmente	-
2.7	SDWAN (Software-Defined WAN).	Atende Totalmente	-

CONFERIDO CONTRATOS

2.8	Procotolos de roteamento dinâmico OSPF e BGP.	Atende Totalmente	-
2.9	Certificação do "ICSA Labs" para os itens de Firewall, IPsec, IPS, Antivírus e SSL-VPN.	Atende Totalmente	-
3	**A solução completa (circuitos internet + firewalls) deve contemplar as seguintes características:**		
3.1	Console centralizada de gerenciamento e configuração dos firewalls: Permitir visualização consolidada do status de diversos equipamentos e possibilitar que configurações sejam implantadas de forma simples em diversos equipamentos simultaneamente. Serão aceitos equipamentos físicos (appliances) ou equipamentos virtuais (virtual appliances).	Atende Parcialmente	Esta atividade será realizada pelo SOC da **CONTRATADA**, com solução para atender os pontos solicitados. Não previsto fornecimento de um portal para visualização pela **CASSI**.
3.2	Console centralizada de análise de segurança da informação: Permitir coleta, análise e correlação de eventos de segurança de todos os equipamentos em uma visualização consolidada. Serão aceitos equipamentos físicos (appliances) ou equipamentos virtuais (virtual appliances).	Atende Parcialmente	Esta atividade será realizada pelo SOC da **CONTRATADA**, com solução para atender os pontos solicitados. Não previsto fornecimento de um portal para visualização pela **CASSI**.
3.3	Instalação: Instalação física dos equipamentos, configuração inicial compreendendo conexão VPN com o datacenter e demais configurações necessárias para o pleno funcionamento da comunicação entre a localidade e o Datacenter **CASSI** .	Atende Parcialmente	-
3.4	Treinamento: Deverá ser ministrado treinamento "Hands On" (oficial ou similar) com duração de no mínimo 20 horas de operação dos firewalls para cinco alunos da **CASSI**. O treinamento poderá ser ministrado dentro do ambiente da **CASSI**, devendo ser oferecido com material didático atualizado e realização de atividades práticas das funcionalidades do equipamento.	Atende Totalmente	Fornecimento de treinamento Oficial com acesso ao Laboratório virtual do fabricante.
4	**Garantias de desempenho do serviço:**		
4.1	Latência média mensal dentro do backbone do fornecedor: < 50ms.	Atende Parcialmente	A depender da região de atendimento do circuito IP, a Latência média no Backbone poderá ser de até 65ms.
4.2	Perda de Pacote: < 1%.	Atende Totalmente	-
4.3	Disponibilidade Mensal: > 99,7%. (Backbone IP)	Atende Totalmente	-
4.4	Tempo de recuperação operacional (TRO): até 4 horas.	Atende Totalmente	-
4.5	Tempo de resposta do suporte técnico de segurança: até 4 horas.	Atende Parcialmente	O SLA para o suporte técnico de segurança dependerá do tipo de acionamento, vide tabela SLA ATENDIMENTO A SOLICITAÇÕES descrito no item 1 do **Anexo II**.
4.6	Todos os serviços contratados pela **CASSI**, incluindo-se o atendimento técnico, devem estar disponíveis em regime 24x7 (vinte e quatro horas por dia em sete dias por semana) por todo o período do contrato.	Atende Totalmente	-
4.7	No caso de indisponibilidade reincidente num período inferior a 3 (três) horas, contado a partir do restabelecimento da última indisponibilidade, será considerado como tempo de indisponibilidade do circuito o início da primeira indisponibilidade até o final da última indisponibilidade, quando o circuito estiver totalmente operacional.	Atende Totalmente	-

5	**O serviço deve contemplar as seguintes características:**		
5.1	Possibilidade de remover ou incluir localidades durante a vigência do contrato.	Atende Totalmente	Confirmada possibilidade de desativação/retirada ou ativação estabelecida na cláusula 4.1, inciso (ix). A inclusão de novos pontos se dará mediante estudo de viabilidade técnica, com prazo de atendimento a ser negociado entre as partes. A retirada de pontos deverá considerar a condição estabelecida na cláusula 6.2.
5.2	Possibilidade de aumento ou diminuição da velocidade dos circuitos de Internet, em incrementos/decrementos de 10 Mbps, com alteração no valor mensal proporcional ao custo unitário do Mbps.	Atende Totalmente	O Upgrade de banda dos circuitos será realizado mediante estudo de viabilidade técnica, com prazo de atendimento a ser negociado entre as partes. O valor mensal está condicionado à viabilidade financeira do contrato para os casos de bandas não previstas nesta cotação.
5.3	Caso seja identificado um roteador ou firewall com uso de CPU ou memória superior a 70%, este deverá ser substituído ou atualizado sem ônus adicional para a **CASSI**.	Atende Totalmente	-
5.4	Havendo descumprimento das garantias de desempenho serviço, o fornecedor deverá conceder na fatura mensal desconto de 1% para cada hora passada além das 4 horas acordadas.	Atende Totalmente	-

ANEXO II – ACORDO DE NÍVEL DE SERVIÇO

1. SLA ATENDIMENTO A SOLICITAÇÕES:

SERVIÇOS	SOLICITAÇÕES ABERTAS EM HORÁRIO COMERCIAL (9 ÀS 19HS)	SOLICITAÇÕES ABERTAS EM DIAS NÃO ÚTEIS
Indisponibilidade total de componentes críticos do serviço	2 HORAS*	2 HORAS*
Indisponibilidade parcial de componentes críticos do serviço	4 HORAS*	8 HORAS*
Criação, alteração ou exclusão de regras, Firewall, IPS, Filtro de Conteúdo, Controle de Aplicação e Antivírus	12 HORAS	24 HORAS
Criação, alteração ou exclusão de regras, de VPN Site-to-site / Client-to-Client	36 HORAS	72 HORAS
Analise Investigação / troubleshooting Firewall e IPS/IDS	72 HORAS	72 HORAS
Requisições de Logs, relatórios ou alterações de configurações e mudanças que não impactem na disponibilidade do ambiente	72 HORAS	72 HORAS
Analise Investigação / troubleshooting Anti-vírus de Gateway / Malware	120 HORAS	120 HORAS

* Em caso de necessidade de visita no local, deverá ser adicionado 6 horas ao SLA acima. Caso seja necessário abrir um ticket com o fabricante, o SLA acima é substituído pelo SLA do fabricante

2. SLA DE ENVIO DE RELATÓRIOS

2.1 Relatórios de incidentes: em até 5 dias úteis após o incidente;
2.2 Relatórios mensais: 35 dias após a data de ativação do produto (30 dias para fechar o ciclo mensal e 05 dias para preparar o relatório). A data fica fixada todos os meses a partir da ativação.
2.3 Tempo de Recuperação/restabelecimento dos serviços WAN/SDWAN: 4 horas.

3. Garantias de desempenho dos serviços WAN/SDWAN:

3.1. Latência média mensal dentro do backbone da **CONTRATADA**: < 50ms.
3.2. Perda de Pacote: < 1%.
3.3. Disponibilidade Mensal: > 99,7%.
3.4. Tempo de recuperação operacional (TRO): até 4 horas.
3.5. Tempo de resposta do suporte técnico de segurança: até 4 horas.
3.6. Todos os serviços contratados pela **CASSI**, incluindo-se o atendimento técnico, devem estar disponíveis em regime 24 x 7 (vinte e quatro horas por dia em sete dias por semana) por todo o período do contrato.
3.7. No caso de indisponibilidade reincidente num período inferior a 3 (três) horas, contado a partir do restabelecimento da última indisponibilidade, será considerado como tempo de indisponibilidade do circuito o início da primeira indisponibilidade até o final da última indisponibilidade, quando o circuito estiver totalmente operacional.

4. Padrão de Qualidade:

4.1. Disponibilidade do Backbone IP: 99,9%;
4.2. Latência média mensal do Núcleo do Backbone IP: 65 ms;
4.3. Perda de Pacotes Média Mensal do Núcleo do Backbone IP: 1,0%;
4.4. Tempo de Recuperação: 4 horas.

CONTRATOS CONFERIDO

5. Nível mínimo de serviço exigido (NMSE)

5.1. Central de Atendimento:

(i) A **CONTRATADA** deverá atender atender, no mínimo, às seguintes especificações ao suporte técnico para os serviços contratados:

a) disponibilizar uma Central de Atendimento, acessada por um serviço telefônico gratuito (0800), podendo oferecer, adicionalmente , opção de registro de chamados pela Internet;
b) possuir uma estrutura de atendimento especializada, adequada para suportar o volume total de chamadas para suporte aos serviços contratados, contemplando recursos humanos, hardware, software, telefonia, estação de gerenciamento proativo e demais complementos que garantam o pleno funcionamento da solução de Central de Atendimento, dentro das suas próprias instalações;
c) a Central de Atendimento deverá dar suporte a chamados referentes à rede física (recuperação), à configuração equipamentos de sua responsabilidade, ao roteamento.
d) a Central de Atendimento deverá atender, no mínimo, 90% das chamadas a ela direcionada, facultando-se à **CASSI** a solicitação de relatórios para comprovação.
e) a **CONTRATADA** deverá dar suporte a chamados referentes à rede física (instalação, alteração e remoção), à configuração equipamentos de sua responsabilidade, ao roteamento.
f) quanto à segurança (incidentes de segurança, senhas, certificados), considerando-se todos os serviços contratados, de maneira a assegurar a integridade dos circuitos, o atendimento via SOC da **CONTRATADA**.

6. Gerenciamento da Disponibilidade:

(i) A Contratante manterá os serviços disponíveis durante as 24 (vinte e quatro) horas do dia, 7 (sete) dias por semana.
(ii) A Contratante deverá utilizar ferramentas, instrumentos e procedimentos de avaliação e monitoração capazes de avaliar e reportar o desempenho dos serviços em relação aos níveis de serviços estabelecidos.

7. Gerenciamento de Incidente:

(i) Havendo descumprimento de qualquer nível de serviço estabelecido, a **CASSI** deverá:

a) investigar e relatar as causas do incidente;
b) tomar medidas preventivas apropriadas para evitar reincidência do incidente.

8. Gerenciamento de Mudanças:

(i) As paradas programadas para manutenção da solução estarão sujeitas à aprovação pela **CASSI** e não serão contabilizadas como período de indisponibilidade, desde que comunicadas com antecedência mínima de 15 (quinze) dias e que a **CASSI** efetue a concordância com a manutenção.

ANEXO III – CRONOGRAMA DE IMPLANTAÇÃO (MACRO)

Os prazos informados a seguir são contados a partir da data de início do projeto técnico, após assinatura deste instrumento contratual.

a) **Região NORTE**: em até 85 (oitenta e cinco) dias a partir do início do projeto técnico a ser celebrado entre a **CONTRATADA** e **CASSI** após assinatura do contrato.
b) **Região NORDESTE:** em até 80 (oitenta) dias a partir do início do projeto técnico a ser celebrado entre a **CONTRATADA** e **CASSI** após assinatura do contrato.
c) **Região CENTRO OESTE:** em até 80 (oitenta) dias a partir do início do projeto técnico a ser celebrado entre a **CONTRATADA** e **CASSI** após assinatura do contrato.
d) **Região SUDESTE:** em até 80 (oitenta) dias a partir do início do projeto técnico a ser celebrado entre a **CONTRATADA** e **CASSI** após assinatura do contrato.
e) **Região SUL** em até 80 (oitenta) dias a partir do início do projeto técnico a ser celebrado entre a **CONTRATADA** e **CASSI** após assinatura do contrato.
f) **Estado de São Paulo Especificamente:** em até 90 (noventa) dias a partir do início do projeto técnico a ser celebrado entre a **CONTRATADA** e **CASSI** após assinatura do contrato.

ANEXO IV – DISPOSIÇÃO DOS LINKS E VALORES

	LOCALIDADE	Velocidade Internet (Mbps)	Vlr. Mensal (R$)	ENDEREÇO	CNPJ
1	DATACENTER	300	9.313,84	Parque Tecnológico Capital Digital, Lote 03, Granja do Torto, Sala Telemática 6 - Brasília/DF - CEP 70635-810	33.719.485/0001-27
2	SEDE	20	1.508,25	SGAS 613, Conjunto E, Bloco A, L2, Asa Sul, Brasília (DF) - CEP 70.200-903	33.719.485/0001-27
3	UNIDADE CE	20	1.542,89	Avenida Dom Luís, 1233 - 2º andar - Ed. Harmony Medical Center - Meireles - Fortaleza (CE) - CEP 60160-230	33.719.485/0014-41
4	UNIDADE GO	20	1.525,31	Rua T-50, 566, Setor Bueno - Goiânia (GO) - CEP 74.215-200	33.719.485/0013-60
5	UNIDADE PE	20	1.542,89	Avenida Conselheiro Rosa e Silva, 1.460, Executive Trade Center - 5º, 6º e 7º andares, Aflitos - Recife (PE) - CEP 52.050-020	33.719.485/0008-01
6	UNIDADE PR	20	1.525,31	Rua Mateus Leme, 937 - Bairro São Francisco - Curitiba (PR) - CEP 80.510-192	33.719-485/0021-70
7	UNIDADE RS	20	1.542,89	Avenida Cristóvão Colombo nº 2240, 5º andar – Bairro Floresta – Porto Alegre (RS) CEP 90.560-002	33.719.485/0022-51
8	UNIDADE SC	20	1.459,92	Rua Professor Hermínio Jacques - Nº229 - Centro - Florianópolis (SC) – CEP 88.015-180	33.719.485/0026-85
9	UNIDADE AC	10	1.042,30	Rua Quintino Bocaiúva, 1790 - Bosque - Rio Branco (AC) - CEP 69.900-670	33.719.485/0044-67
10	UNIDADE AL	10	1.093,80	Avenida Dr. Antônio Gomes de Barros (antiga Avenida Amélia Rosa), 625, Edf. The Square, Sala 101, Bairro Jatiúca, Maceió (AL) - CEP 57036-000	33.719.485/0017-94
11	UNIDADE AM	10	1.093,80	Avenida Senador Álvaro Maia, 1286 - Praça 14 - Manaus (AM) - CEP 69020-210	33.719.485/0016-03
12	UNIDADE AP	10	1.082,89	Rodovia Duca Serra, S/Nº, KM 1 – Alvorada - Macapá (AP) - CEP 68.906-698	33.719.485/0042-03
13	UNIDADE ES	10	1.042,30	Avenida N.S. dos Navegantes, 955, 9º andar, sala 908, Edifício Global Tower - Enseada do Suá - Vitória (ES) - CEP 29.050-335	33.719.485/0025-02
14	UNIDADE MA	10	1.082,89	Avenida dos Holandeses, QD-09, 13 – Calhau - São Luís (MA) – CEP 65.075-480	33.719.485/0027-66
15	UNIDADE MS	10	1.082,89	Rua Pedro Celestino, 2670 - São Francisco - Campo Grande (MS) – CEP 79.002-372	33.719.485/0011-07
16	UNIDADE MT	10	1.116,64	Rua Rui Barbosa, 444 – Bairro Goiabeiras - Cuiabá (MT) - CEP 78.032-040	33.719.485/0012-80
17	UNIDADE PA	10	1.093,80	Avenida Duque de Caxias, 277 – Marco - Belém (PA) - CEP 66.093-400	33.719.485/0024-13
18	UNIDADE PB	10	1.093,80	Avenida Júlia Freire, 1200 - Edifício Metropolitan, 7º andar – Expedicionários – João Pessoa (PB) CEP - 58.041-000	33.719.485/0023-32
19	UNIDADE PI	10	1.093,80	Avenida Miguel Rosa, 3260, Centro-Sul - Teresina (PI) - CEP 64.001-490	33.719.485/0007-12
20	UNIDADE RN	10	1.093,80	Edifício Corporate Tower Center -CTC-Av. Amintas Barros, 3700–Torre Business-Lagoa Nova - 14º e 15º Andares -Natal (RN) - CEP 59.075-810	33.719.485/0009-84

21	UNIDADE RO	10	1.062,01	Rua Tenreiro Aranha, 2862 – Olaria - Porto Velho (RO) – CEP 76.801-254	33.719.485/0006-31
22	UNIDADE RR	10	1.042,30	Rua Professor Diomedes Souto Maior, nº 81, Centro, Boa Vista (RR) - CEP 69301-260	33.719.485/0054-39
23	UNIDADE SE	10	1.093,80	Avenida Tancredo Neves, 242 - Grageru - Aracaju (SE) - CEP 49025-620	33.719.485/0005-50
24	UNIDADE TO	10	1.082,89	Quadra 103 Norte, Avenida LO-2, Lote 74 – Plano Diretor Norte – Palmas (TO) - CEP 77001-022	33.719.485/0055-10
25	CLINICASSI BA Feira de Santana	10	1.072,30	Rua Barão do Rio Branco, 1309, SL 901, Edifício Metropolitan Center - Centro - Feira de Santana - BA - 44001-205	33.719.485/0065-91
26	CLINICASSI BA Itabuna	10	1.072,30	Rua Pernambuco, 324 - Jardim Vitória - Itabuna - BA - 45605-510	33.719.485/0036-57
27	CLINICASSI BA Vitória da Conquista	10	1.072,30	Rua Siqueira Campos, 450 - Térreo/sala 02 – Centro Empresarial DMA - Recreio - Vitória da Conquista - BA - 45020-800	33.719.485/0071-30
28	CLINICASSI MG Juiz de Fora	10	1.062,01	Avenida Francisco Bernardino, 165 - Sala 508 a 512 – 5º andar - Centro - Juiz de Fora - MG - 36013-100	33.719.485/0032-23
29	CLINICASSI MG Montes Claros	10	1.062,01	Rua São Sebastião, 150 - Todos os Santos - Montes Claros - MG - 39400-120	33.719.485/0033-04
30	CLINICASSI MG Uberaba	10	1.062,01	Rua Cunha Campos, 83 - Nossa Senhora da Abadia - Uberaba - MG - 38020-025	33.719.485/0062-49
31	CLINICASSI MG Uberlândia	10	1.062,01	Rua Arthur Bernardes, 240 - Martins - Uberlândia - MG - 38412-224	33.719.485/0034-95
32	CLINICASSI PB Campina Grande	10	1.093,80	Rua Duque de Caxias, 523 - Edifício San Raphael - Prata - Campina Grande - PB - 58400-506	33.719.485/0043-86
33	CLINICASSI PE Recife Boa Viagem	10	1.093,80	Rua Ribeiro de Brito, 618 - Boa Viagem - Recife - PE - 51020-310	33.719.485/0061-68
34	CLINICASSI PR Londrina	10	1.082,89	Rua Borba Gato, 976 - Jardim Ipiranga - Londrina - PR - 86010-630	33.719.485/0031-42
35	CLINICASSI PR Maringá	10	1.082,89	Rua Visconde de Nácar, 863 - Zona 04 - Maringá - PR - 87014-300	33.719.485/0069-15
36	CLINICASSI RJ Campos dos Goytacazes	10	1.116,64	Avenida Treze de Maio, 286 - Sala 401 - Edifício Medical Center - Centro - Campos - RJ - 28010-260	33.719.485/0066-72
37	CLINICASSI RJ Copacabana	10	1.116,64	Rua Siqueira Campos, 93 - 4º andar - Copacabana - Rio de Janeiro - RJ - 22031-071	33.719.485/0004-70
38	CLINICASSI RJ Niterói	10	1.116,64	Rua da Conceição, 188 - salas 319 parte, 320, 328 e 329 - Niterói Shopping - Centro - Niterói - RJ - 24020-087	33.719.485/0059-43
39	CLINICASSI RJ Petrópolis	10	1.116,64	Rua do Imperador, 288 - Sala 903 - Centro - Petrópolis - RJ - 25620-000	33.719.485/0073-00
40	CLINICASSI RJ Tijuca	10	1.116,64	Rua General Rocca, 836 - 2º e 3º andares - Tijuca - Rio de Janeiro - RJ - 20521-070	33.719.485/0056-09
41	CLINICASSI RS Caxias do Sul	10	1.093,80	Rua Garibaldi, 791 salas 103 e 104 – Centro – Caxias do Sul (RS) – CEP 95.080-190	33.719.485/0068-34
42	CLINICASSI RS Passo Fundo	10	1.093,80	Rua XV de Novembro, 885 - Salas 85 e 86 – Edifício Hawai - Centro - Passo Fundo - RS - 99010-090	33.719.485/0063-20
43	CLINICASSI RS Pelotas	10	1.093,80	Rua Sete de Setembro, 160 - Sala 201 - Centro - Pelotas - RS - 96015-300	33.719.485/0067-53
44	CLINICASSI RS Porto Alegre Sul	10	1.093,80	Avenida Padre Cacique, 320 - 2° Andar - Menino Deus - Porto Alegre - RS - 90810-240	33.719.485/0074-82
45	CLINICASSI RS Santa Maria	10	1.093,80	Rua Duque de Caxias, 1668 - Sala 701 - Centro - Santa Maria - RS - 97010-200	33.719.485/0064-00
46	CLINICASSI SC Balneário Camboriú	10	1.042,30	Avenida Palestina, 1510 - Nações - Balneário Camboriú - SC - 89338-010	33.719.485/0072-10

47	CLINICASSI SC Blumenau	10	1.042,30	Rua João Pessoa, 185 - Velha - Blumenau - SC - 89012-472	33.719.485/0039-08
48	CLINICASSI SC Joinville	10	1.042,30	Rua Dr. Marinho Lobo, 101 - 1º Andar - Centro - Joinville - SC - 89201-020	33.719.485/0038-19
49	CLINICASSI SP ABC	10	1.042,30	Rua Das Palmeiras, 530 - Casa - Jardim - Santo André - SP - 09080-360	33.719.485/0047-00
50	CLINICASSI SP Araçatuba	10	1.042,30	Rua Marconi, 125 - Casa - Higienópolis - Araçatuba - SP - 16010-645	33.719.485/0051-96
51	CLINICASSI SP Bauru	10	1.042,30	Rua Aviador Gomes Ribeiro, 16-48 - Casa - Vila Santa Tereza - Bauru - SP - 17012-010	33.719.485/0049-71
52	CLINICASSI SP Campinas	10	1.042,30	Avenida Jose de Souza Campos, 2021/2029 - prédio - Nova Campinas - Campinas - SP - 13025-320	33.719.485/0002-08
53	CLINICASSI SP Leste (Tatuapé)	10	1.042,30	Rua Serra de Botucatu, 1455 - Casa - Tatuapé - São Paulo - SP - 03317-000	33.719.485/0046-29
54	CLINICASSI SP Norte (Santana)	10	1.042,30	Rua Dr. Olavo Egídio, 287 - 2º Andar - Santana - São Paulo - SP - 02037-000	33.719.485/0048-90
55	CLINICASSI SP Oeste (Pacaembu)	10	1.042,30	Rua Almirante Pereira Guimarães, 248 - Casa - Pacaembu - São Paulo - SP - 01250-000	33.719.485/0058-62
56	CLINICASSI SP Piracicaba	10	1.042,30	Rua do Rosário, 153 - Casa - Centro - Piracicaba - SP - 13400-180	33.719.485/0075-63
57	CLINICASSI SP Ribeirão Preto	10	1.042,30	Av Cel. Fernando Ferreira Leite, 1520 - 4º Andar - Jardim Nova Aliança - Ribeirão Preto - SP - 14026-020	33.719.485/0035-76
58	CLINICASSI SP S. J. do Rio Preto	10	1.042,30	Rua Piracicaba, 1850 - Casa - Santos Dumont - São José do Rio Preto - SP - 15020-120	33.719.485/0040-33
59	CLINICASSI SP S. J. dos Campos	10	1.042,30	Rua Esperança, 282 - Sala 36, 3º Andar - Vila Adyana - São José dos Campos - SP - 12243-700	33.719.485/0053-58
60	CLINICASSI SP Santos	10	1.042,30	Rua Marcilio Dias, 27 - 6º andar - Gonzaga - Santos - SP - 11060-210	33.719.485/0045-48
61	CLINICASSI SP Sorocaba	10	1.042,30	Rua Eulália Silva, 243 - Casa - Jardim Faculdade - Sorocaba - SP - 18030-230	33.719.485/0052-77
62	AMBULATÓRIO BA Salvador	10	1.072,30	Avenida Estados Unidos 561, 4º andar - Comércio - Salvador/BA - CEP 40010-904	33.719.485/0015-22
63	AMBULATÓRIO PR São José dos Pinhais	10	1.082,89	Rua Joinville 3816 - São Pedro – São José dos Pinhais/PR - 83020-000	33.719-485/0021-70
64	AMBULATÓRIO SP São Paulo - Verbo Divino	10	1.042,30	Rua Verbo Divino 1830, 1º andar - Chácara Santo Antônio (Zona Sul) - São Paulo/SP - CEP 04719-002	33.719.485/0018-75

Os valores acima apresentados para cada localidade serão distribuído na seguinte proporção dos itens contratados:

- Circuito de acesso: 65% do valor;
- Roteador: 03% do valor;
- Equipamento de segurança/Treinamento: 15% do valor;
- Gerenciamento: 17% do valor.

CONTRATOS CONFERIDO

3º TERMO DE ADITAMENTO AO CONTRATO DE PRESTAÇÃO DE SERVIÇOS N° 265/2018 QUE ENTRE SI CELEBRAM, DE UM LADO, OI S/A – EM RECUPERAÇÃO JUDICIAL & CAIXA DE ASSISTÊNCIA DOS FUNCIONÁRIOS DO BANCO DO BRASIL TODAS DEVIDAMENTE ABAIXO QUALIFICADAS.

São Partes no presente instrumento:

OI S.A. – EM RECUPERAÇÃO JUDICIAL, (sucessora por incorporação das empresas: **OI MÓVEL S.A. - EM RECUPERAÇÃO JUDICIAL e TELEMAR NORTE LESTE S.A. - EM RECUPERAÇÃO JUDICIAL**) sociedade anônima, com sede à Rua do Lavradio, nº 71, 2º Andar, Centro, CEP: 20.230-070, Cidade e Estado do Rio de Janeiro, inscrita no CNPJ/ME sob o nº 76.535.764/0001-43, neste ato devidamente representada na forma prevista em seu Estatuto Social, doravante denominada "**CONTRATADA"**; e do outro lado,

CAIXA DE ASSISTÊNCIA DOS FUNCIONÁRIOS DO BANCO DO BRASIL – CASSI, pessoa jurídica de direito privado, associação de natureza assistencial sem fins lucrativos com Sede no Setor de Grandes Áreas Sul 613, Conjunto E, Bloco A, L2 Asa Sul – Brasília/DF, CEP: 70.200-903, inscrita no CNPJ/MF sob nº 33.719.485/0001-27, neste ato devidamente representada na forma prevista em seu Estatuto Social, doravante denominada "**CONTRATANTE**";

E ainda denominadas isoladamente como "**PARTE"** ou coletivamente como "**PARTES**".

OI SOLUÇÕES S.A., sociedade anônima, com sede Cidade e Estado de São Paulo, na Avenida Dr. Chucri Zaidan, S/N, Conjunto 191, Torre Ez Towers, Anexo Arquiteto Olavo Redig de Campo, nº 105, CEP: 04711-130, inscrita no CNPJ/ME sob o nº 09.719.875/0001-12, neste ato representada na forma de seu Estatuto Social, doravante denominada "**INTERVENIENTE ANUENTE**",

CONSIDERANDO que em 18 de abril de 2019, as **PARTES** firmaram um CONTRATO DE PRESTAÇÃO DE SERVIÇOS, tendo por objeto a prestação de serviços de comunicação de dados por meio de rede de IP (*Internet Protocol) Connect*, com vigência por 60 meses contados a partir da assinatura do Contrato.

Considerando o interesse das **PARTES** em incluir a **INTERVENIENTE ANUENTE** como **PARTE CONTRATADA**.

Este documento foi assinado digitalmente por Daniele Ramos Oliveira. Este documento foi assinado eletronicamente por Angélica Cristina Souza, Marcelo Augusto Leite de Moraes, Denise Cristina Paranhos Melchiades e Frederico Rodrigues Moreira.
Para verificar as assinaturas vá ao site https://cassi.portaldeassinaturas.com.br:443 e utilize o código 1FC9-2B0F-D01E-1849.

RESOLVEM as **PARTES** acima qualificadas celebrar o presente 3° Termo de Aditamento ao **CONTRATO** doravante denominada simplesmente como **"*Termo de Aditamento*",** que se regerá com base nas seguintes cláusulas e condições:

CLÁUSULA PRIMEIRA – DAS ALTERACÕES DO CONTRATO

1.1 O objeto do presente instrumento é incluir a empresa **OI SOLUÇÕES S.A. ("INTERVENIENTE ANUENTE")**, como "**CONTRATADA"**, sendo **PARTE** do Termo, de modo que a partir da formalização deste Instrumento a qualificação das **PARTES** passará a ter a seguinte redação:

> **OI S.A. – EM RECUPERAÇÃO JUDICIAL**, sociedade anônima, com sede à Rua do Lavradio, nº 71, 2º Andar, Centro, CEP: 20.230-070, Cidade e Estado do Rio de Janeiro, inscrita no CNPJ/ME sob o nº 76.535.764/0001-43, neste ato devidamente representada na forma prevista em seu Estatuto Social, doravante denominada "**OI S/A"**;
>
> **OI SOLUÇÕES S.A.**, sociedade anônima com sede Cidade e Estado de São Paulo, na Avenida Dr. Chucri Zaidan, S/N, Conjunto 191, Torre Ez Towers, Anexo Arquiteto Olavo Redig de Campo, nº 105, CEP: 04711-130, inscrita no CNPJ/ME sob o nº 09.719.875/0001-12, neste ato representada na forma de seu Estatuto Social, doravante denominada "**OI SOLUÇÕES**", quando em conjunto doravante denominadas "**CONTRATADAS**"; de um lado e, do outro lado,
>
> **CAIXA DE ASSISTÊNCIA DOS FUNCIONÁRIOS DO BANCO DO BRASIL – CASSI**, pessoa jurídica de direito privado, associação de natureza assistencial sem fins lucrativos com Sede no SIG, Quadra 4, Lote 417, Brasília/DF - CEP: 70.610-910, inscrita no CNPJ/MF sob nº 33.719.485/0001-27
>
> E ainda denominadas isoladamente como **"PARTE"** ou coletivamente como **"PARTES"**,

CLÁUSULA SEGUNDA – DAS DISPOSIÇÕES GERAIS

2.1 O presente Termo de Aditamento entrará em vigor a contar da data de sua assinatura e permanecerá vigente até o fim da vigência do Contrato.

Este documento foi assinado digitalmente por Daniele Ramos Oliveira. Este documento foi assinado eletronicamente por Angélica Cristina Souza, Marcelo Augusto Leite de Moraes, Denise Cristina Paranhos Melchiades e Frederico Rodrigues Moreira.
Para verificar as assinaturas vá ao site https://cassi.portaldeassinaturas.com.br:443 e utilize o código 1FC9-2B0F-D01E-1849.

2.2 Ficam mantidas e inalteradas todas as cláusulas contratuais que não forem objeto de alteração pelo presente Termo de Aditamento, sendo para todos os efeitos legais ratificados pelas **PARTES**.

O presente instrumento será firmado mediante assinatura eletrônica, em conformidade com a Medida Provisória 2.200-02/01, pelo representante legal das **PARTES** e testemunhas, que declaram, de forma inequívoca, a concordância, bem como o reconhecimento de validade e aceite integral do presente documento.

Brasília, 12 de setembro de 2022.

Pela **OI S.A. – EM RECUPERAÇÃO JUDICIAL (“CONTRATADA”)**

Marcelo Augusto Leite de Moraes CPF: 182.752.898-23	Frederico Rodrigues Moreira CPF: 053.492.537-51

Pela **OI SOLUÇÕES S.A(“CONTRATADA”)**

Marcelo Augusto Leite de Moraes CPF: 182.752.898-23	Frederico Rodrigues Moreira CPF: 053.492.537-51

Pela **CASSI (“CONTRATANTE”)**

Daniele Ramos Oliveira
CPF: 877.538.121-49

TESTEMUNHAS

Denise Cristina Paranhos Melchiades CPF: 963.522.210-68	Angélica Cristina Souza CPF: 994.092.081-49

Este documento foi assinado digitalmente por Daniele Ramos Oliveira. Este documento foi assinado eletronicamente por Angélica Cristina Souza, Marcelo Augusto Leite de Moraes, Denise Cristina Paranhos Melchiades e Frederico Rodrigues Moreira.
Para verificar as assinaturas vá ao site https://cassi.portaldeassinaturas.com.br:443 e utilize o código 1FC9-2B0F-D01E-1849.

PROTOCOLO DE ASSINATURA(S)

O documento acima foi proposto para assinatura digital na plataforma CASSI - CAIXA DE ASSISTÊNCIA DOS FUNCIONÁRIOS DO BANCO DO BRASIL. Para verificar as assinaturas clique no link: https://cassi.portaldeassinaturas.com.br/Verificar/1FC9-2B0F-D01E-1849 ou vá até o site https://cassi.portaldeassinaturas.com.br:443 e utilize o código abaixo para verificar se este documento é válido.

Código para verificação: 1FC9-2B0F-D01E-1849

Hash do Documento

43F4B3671A477BB298974FFEA3B38D958EF75DC2F6ADC3E044C770882B7A5442

O(s) nome(s) indicado(s) para assinatura, bem como seu(s) status em 13/09/2022 é(são) :

- Daniele Ramos Oliveira (Signatário - CASSI Sede - Divisão de Compras) - 877.538.121-49 em 13/09/2022 15:29 UTC-03:00
  Tipo: Certificado Digital
- Angélica Cristina Souza (Testemunha - CASSI Sede - Divisão de Compras) - 994.092.081-49 em 12/09/2022 17:51 UTC-03:00
  Tipo: Assinatura Eletrônica
  Identificaçao: Autenticação de conta

  Evidências

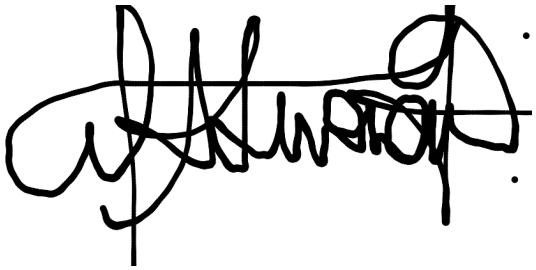
  Client Timestamp Mon Sep 12 2022 17:51:12 GMT-0300 (GMT-03:00)
  Geolocation Latitude: -21.2922457 Longitude: -50.3428431 Accuracy: 332609.67797423486
  IP 189.75.117.190
  Assinatura:

  Hash Evidências:
  9AC51DA2721BBED19BDD511C2DE03500EAEC88A9084A8264313B0BCF9AD59161
- Marcelo Augusto Leite de Moraes (Signatário - OI SOLUCOES SA) - 182.752.898-23 em 12/09/2022 17:43 UTC-03:00
  Tipo: Assinatura Eletrônica
  Identificaçao: Por email: marcelo.leite@oi.net.br

Evidências

Client Timestamp Mon Sep 12 2022 17:43:38 GMT-0300 (-03)
Geolocation Latitude: -15.788393335631062 Longitude: -47.88529260072783 Accuracy: 22.712221507798443
IP 191.219.33.184
Assinatura:



Hash Evidências:
D86FDCCA6944BDB179404BFFFA8B16DACBD9C3E48A251EA5E6461B5CA41E0DC7

☑ Denise Cristina Paranhos Melchiades (Testemunha - OI SOLUCOES SA) - 963.522.210-68 em 12/09/2022 17:41 UTC-03:00
Tipo: Assinatura Eletrônica
Identificaçao: Autenticação de conta

Evidências

Client Timestamp Mon Sep 12 2022 17:45:17 GMT-0300 (Horário Padrão de Brasília)
Geolocation Latitude: -15.7826 Longitude: -47.9354 Accuracy: 7602
IP 191.176.144.37
Assinatura:

Hash Evidências:
30F7F1D1154E82DEF79E9E0CF8244A5ECDBADBEBD6312C88A4A0BA9B409D2CAB

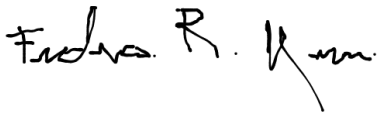
☑ Frederico Rodrigues Moreira (Signatário - OI SOLUCOES SA) - 053.492.537-51 em 12/09/2022 16:39 UTC-03:00
Tipo: Assinatura Eletrônica
Identificaçao: Por email: frederico.moreira@oi.net.br

Evidências

Client Timestamp Mon Sep 12 2022 16:38:59 GMT-0300 (Horário Padrão de Brasília)
Geolocation Location not shared by user.

IP 200.140.127.80

Assinatura:



Hash Evidências:

5CF8E21645C92A80DDDDF2FAB0C2F7A4E11789D2F19501162D428A0FEA6C1FD6