ExpressoLivre - ExpressoMail

Remetente:	"Camilo Jose Gasparetto" <camilo.gasparetto@liggavc.com.br>
Para:	"Comissao Permanente de Licitacoes" <cplc.appa@appa.pr.gov.br>
Com Cópia:	"Licitação - Ligga Telecom" <licitacao@liggavc.com.br>
Data:	26/06/2026 14:09 (07 minutos atrás)
Assunto:	RES: ENC: Diligência LE SAP 430/2026
Anexos:	image001.png (6.42 KB) image002.png (610 B) fortigate-90g-series.pdf#page=6.pdf (1.54 MB) fortigate-fortiwifi-40f-series.pdf#page=6.pdf (5.18 MB) Resposta_a_Diligencia_-_APPA_assinado.pdf (2 MB)

Prezado pregoeiro, Sr. Délcio Chicora.

Boa tarde!

Segues as respostas, tempestivamente, ao diligenciamento bem como manuais dos equipamentos que serão utilizados na entrega da solução licitada e foram citados nas respostas.

Permanecemos à disposição.

Atenciosamente

Camilo Gasparetto
B2B - Governo
camilo.gasparetto@liggavc.com.br
41 996.097.491

Chamados Técnicos: 0800 604 3939

Pós-Vendas: 41 992.833.849

Contratos e Aditivos: 41 998.560.180
LIGGAVC.COM.BR

De: Comissao Permanente de Licitacoes <cplc.appa@appa.pr.gov.br>
Enviada em: terça-feira, 23 de junho de 2026 09:20
Para: Camilo Jose Gasparetto <camilo.gasparetto@liggavc.com.br>
Assunto: Re: ENC: Diligência LE SAP 430/2026

Bom dia,

Pedido de dilação de prazo concedido.

Seu novo prazo de entrega da documentação é até o final do dia 26/06/2026.

COMISSÃO PERMANENTE DE LICITAÇÃO E CADASTRO - CPLC

COORDENADORIA DE LICITAÇÕES | DAF

PORTOS DO PARANÁ
LOGÍSTICA INTELIGENTE

+55 (41) 3420-1127 - (41) 3420-1373

cplc.appa@appa.pr.gov.br

www.portosdoparana.pr.gov.br

Palácio Taguaré - Avenida Ayrton Senna da Silva, 161

DOM PEDRO II - Paranaguá/PR

Em 22/06/2026 às 15:36 horas, "Camilo Jose Gasparetto" <camilo.gasparetto@liggavc.com.br> escreveu:

> Boa tarde.
>
> Por meio deste e-mail, venho solicitar a dilação do prazo referente a Diligência LE SAP 430/2026, atualmente previsto para até o final do dia 23/06/2026.
>
> Para fundamentação do pedido, segue em anexo documento contendo a respectiva justificativa e informações complementares.

Permaneço à disposição para quaisquer esclarecimentos adicionais e aguardamos retorno sobre o nosso pleito.

Atenciosamente,

Camilo Gasparetto
B2B - Governo
camilo.gasparetto@liggavc.com.br
41 996.097.491

Chamados Técnicos: 0800 604 3939

Pós-Vendas: 41 992.833.849

Contratos e Aditivos: 41 998.560.180
LIGGAVC.COM.BR

De: Comissao Permanente de Licitacoes <cplc.appa@appa.pr.gov.br>
Enviada em: quinta-feira, 18 de junho de 2026 11:14
Para: Camilo Jose Gasparetto <camilo.gasparetto@liggavc.com.br>
Cc: Licitação - Ligga Telecom <licitacao@liggavc.com.br>
Assunto: Diligência LE SAP 430/2026

Referente LE Nº 430/2026,

Protocolo SAP nº 10000000430

Bom dia,

Realizada a competente análise da habilitação técnica pelo setor requisitante, conforme documento em anexo, foi identificado que a empresa não atendeu integralmente aos requisitos técnicos do edital e termo de referência, para o que solicitamos, em diligência os esclarecimentos / documentos necessários ao prosseguimento do certame.

Prazo de resposta: 03 (três) dias úteis ou seja até até o final do dia 23/06/2026.

Colocamo-nos à disposição para eventuais esclarecimentos.

Délcio Chicora

Pregoeiro

COMISSÃO PERMANENTE DE LICITAÇÃO E CADASTRO - CPLC

COORDENADORIA DE LICITAÇÕES | DAF

PORTOS DO PARANÁ
LOGÍSTICA INTELIGENTE

+55 (41) 3420-1127 - (41) 3420-1373

cplc.appa@appa.pr.gov.br

www.portosdoparana.pr.gov.br

Palácio Taguaré - Avenida Ayrton Senna da Silva, 161

DOM PEDRO II - Paranaguá/PR

Curitiba, 26 de junho de 2026.

À Administração dos Portos de Paranaguá e Antonina – APPA

À Gerência de Tecnologia da Informação

Ref. a Licitação Eletrônica n.º 430/2026

Protocolo SAP nº 10000000430

A **LIGGA TELECOMUNICAÇÕES S.A.** vem, em atendimento à **Diligência Complementar** encaminhada no âmbito da **Licitação Eletrônica nº 430/2026**, apresentar os esclarecimentos e documentos complementares solicitados, nos termos a seguir expostos.

Inicialmente, registra-se que a presente manifestação tem por finalidade prestar todos os esclarecimentos requeridos pela Administração, demonstrando o pleno atendimento das exigências constantes do Edital, Termo de Referência e demais documentos que compõem o certame.

1- Requisitos Técnicos Gerais

3.2.1 Meio físico do link principal: Obrigatória a entrega via fibra óptica para garantir a robustez e imunidade a interferências eletromagnéticas presentes no ambiente portuário;
R: Atendido através da proposta técnica na página 01.

3.2.2 Meio físico dos links redundantes: Os circuitos de redundância devem apresentar trajetória geográfica independente do primário, com distância mínima de 500 metros entre rotas (quando aplicável), e meio físico não terrestre. Serão aceitos para redundância: Rádio Digital Licenciado (Microwave), 5G Corporativo (Network Slicing) ou Satélite LEO (Low Earth Orbit), podendo ser apresentada proposta com qualquer das soluções citadas, desde que atendidos os requisitos técnicos.
R: Atendido através da proposta técnica, na página 01, onde afirma que a tecnologia utilizada será 5G.

3.5 Todo o hardware e software fornecidos não podem constar, no momento da apresentação da proposta, em listas de end-of-sale, end-of-support, end-ofengineering-support ou end-of-life do fabricante, ou seja, não poderão ter previsão de descontinuidade de fornecimento, suporte ou vida, devendo estar em linha de produção e sendo oferecidos no mercado pelo fabricante.

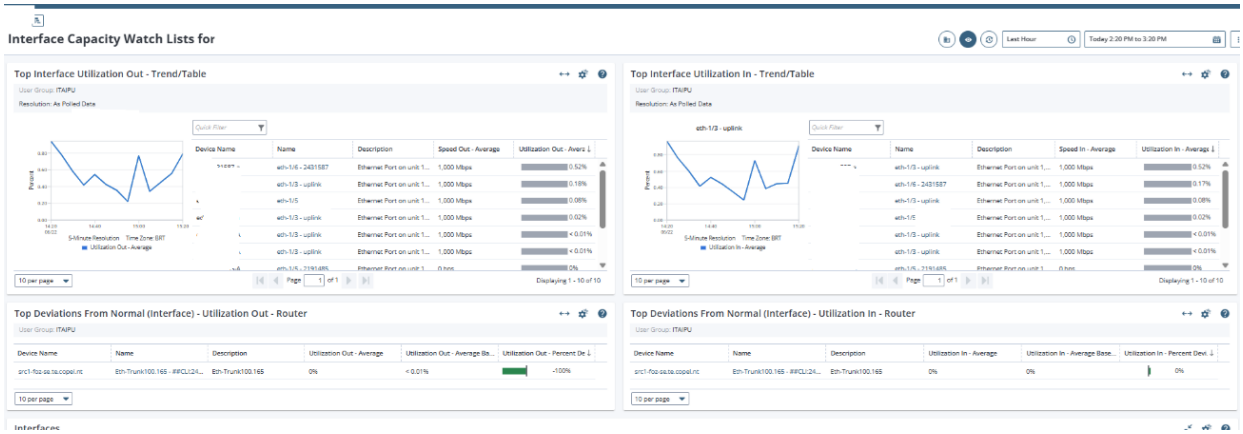
R: R: SD-WAN: Fortigate 40F e Fortigate 90G ambos sem end-of-sale, end-of-support, end-of-engineering-support e end-of-life pelo fabricante (https://support.fortinet.com/welcome/#/lifecycle)

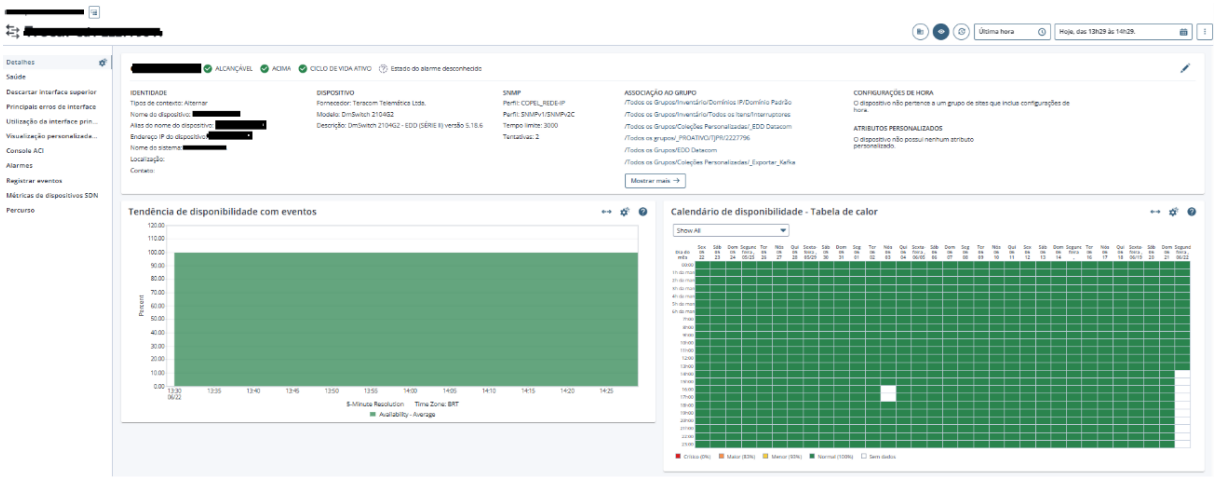
3.8 A solução deverá possuir e permitir que ferramentas de detecção e prevenção de propagação de ataques de agentes maliciosos sejam utilizados.

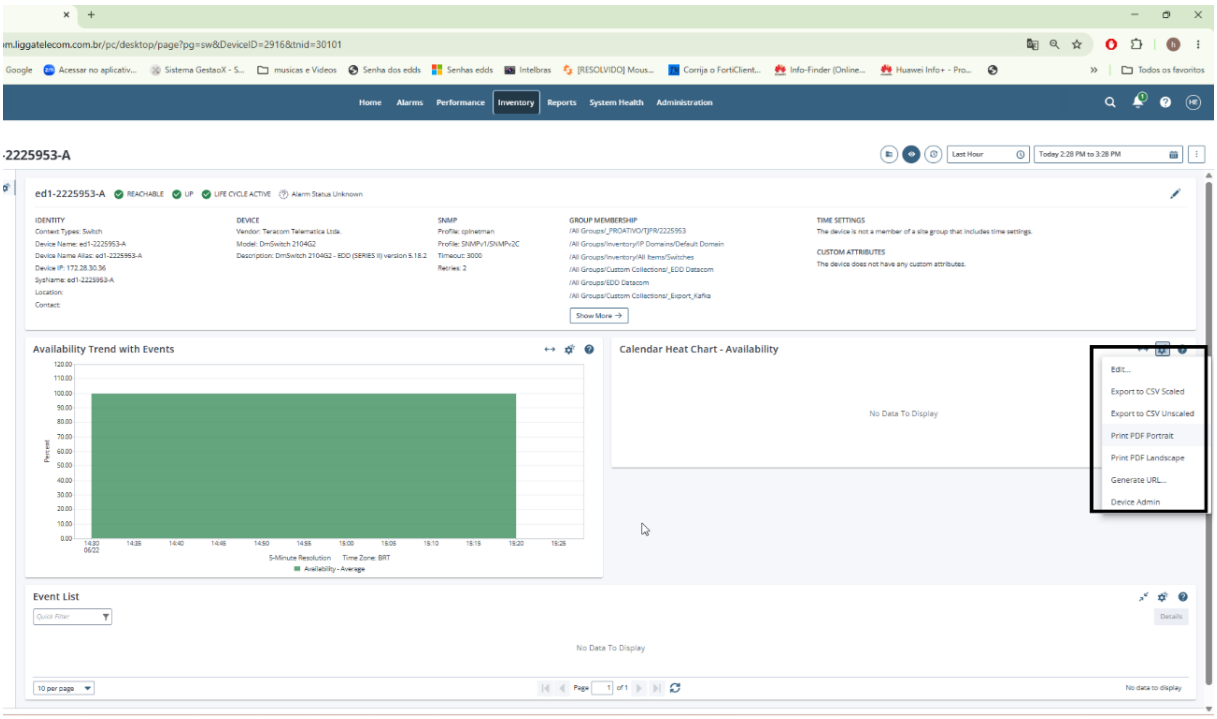
R: O FortiOS integra nativamente recursos avançados de Next-Generation Firewall (NGFW), possuindo ferramentas para detecção e prevenção de ameaças, como o Sistema de Prevenção de Intrusões (IPS), Sistema de Detecção de Intrusões (IDS) e o Antivírus (AV). Esses perfis de segurança podem ser aplicados diretamente nas políticas de firewall, inspecionando os pacotes em tempo real para bloquear efetivamente a propagação de agentes maliciosos. (https://docs.fortinet.com/document/fortigate/7.4.12/administration-guide/411317/intrusion-prevention e https://docs.fortinet.com/document/fortigate/7.4.12/administration-guide/862660/antivirus)

3.10 A CONTRATADA deverá prover solução de gerência de rede que contemple os módulos de gerencia de falhas, desempenho, disponibilidade, capacity planning, relatórios, tickets, e de nível de serviço.

R: Segue telas com a comprovação:

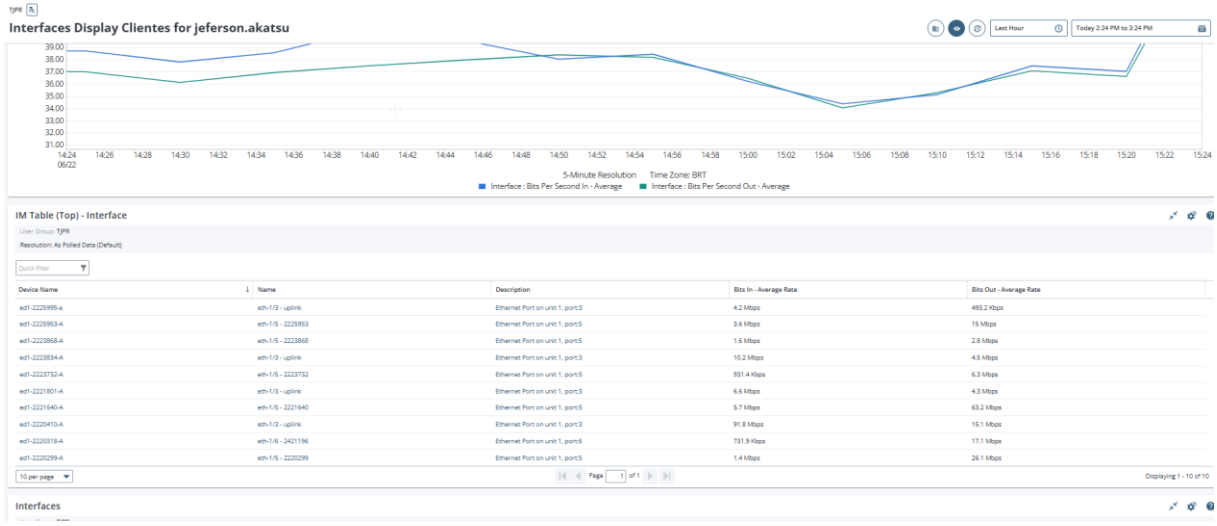


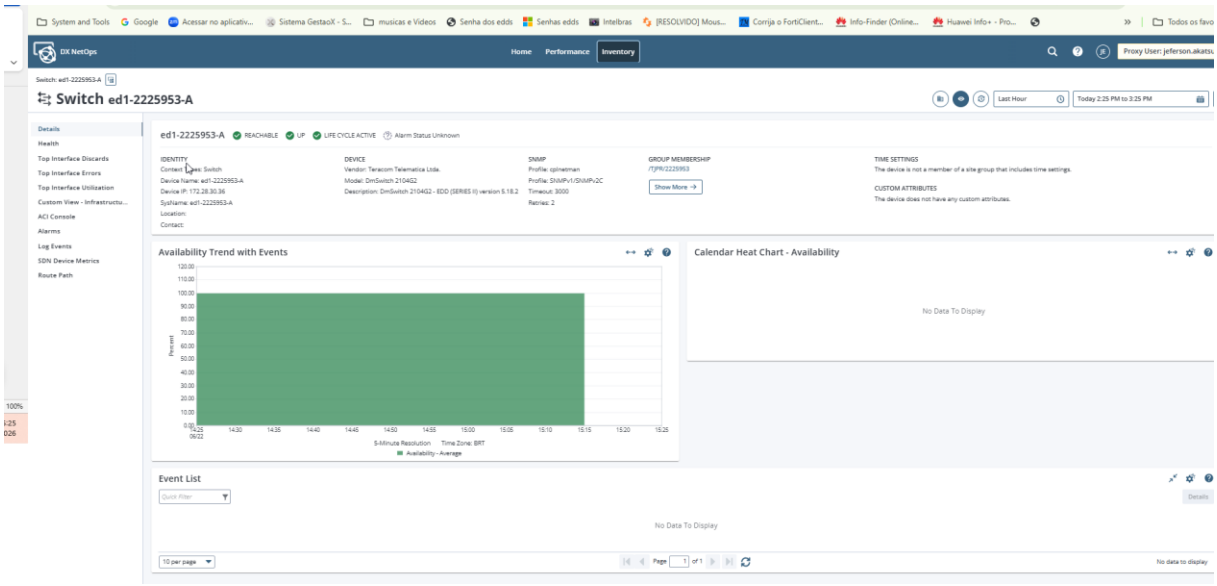




3.10.1 A solução de gerência de rede deverá disponibilizar a visualização de informações on-line (de forma gráfica) da rede para o acompanhamento e monitoração do estado global e detalhado do ambiente;

R: Atende conforme telas abaixo:





3.27 Para garantia da entrega dos serviços, os equipamentos fornecidos devem atuar com o intuito de consolidar todos os enlaces WAN das localidades, tais como links de internet, MPLS via Fibra Optica, Radio, entre outros para a utilização da engenharia de tráfego do SD-WAN, provendo ainda de modo integrado a conectividade segura, viabilizando o acesso local a internet de modo seguro.

R: SD-WAN: Fortigate 40F e Fortigate 90G com licenciamento UTP possuem funcionalidade de SD-WAN capaz de consolidar os links.

Datasheet 40F: Tópicos “Perimeter Protection” e “Secure SD-WAN” página 2

Datasheet 90G: Tópicos “Perimeter Protection” e “Secure SD-WAN” página 2

2- Tecnologia e protocolos para os links principais e de redundância

3.2.4.1 Suporte a MPLS (Multiprotocol Label Switching) em camada 3 com QoS (Quality of Service), permitindo assim a definição de rotas pré-definidas, mais eficientes que o roteamento tradicional, e utilizando a classificação e priorização de pacotes;
R: Atendido pg. 26 e 31

3.2.4.2 Suporte a VPN Camada 2 (Pseudowire) para conexões legadas específicas (Nucleo CELEPAR), permitindo a integração com os ambientes legados;
R: Atendido pg 155.

3.2.4.3 Compatibilidade nativa com protocolos de roteamento dinâmico (OSPF/BGP) utilizados pela CELEPAR.
R: : SD-WAN: Fortigate 40F e Fortigate 90G possuem nativamente os protocolos de roteamento dinâmico OSPF e BGP com a utilização do FortiOS (https://docs.fortinet.com/document/fortigate/7.4.12/administration-guide/479509/dynamic-routing)

3 - Equipamentos

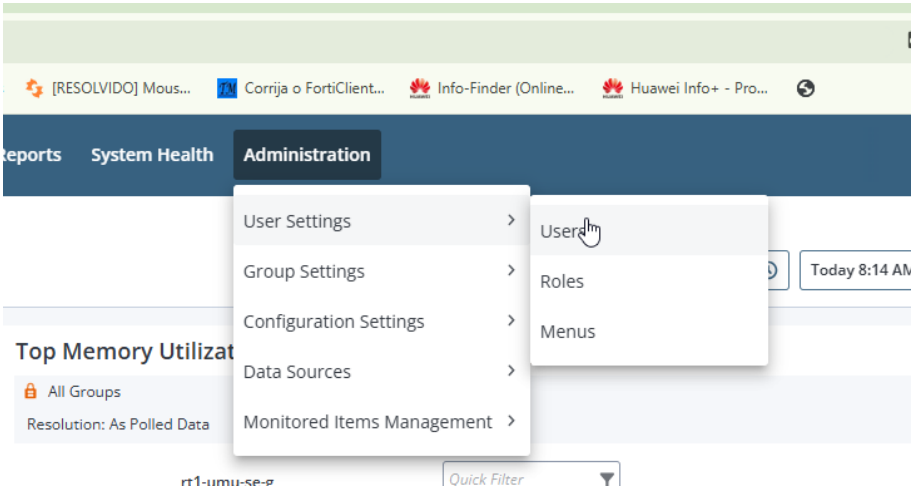
3.4.1 Todos os equipamentos fornecidos deverão ser homologados pela ANATEL.
R: SD-WAN: Fortigate 40F: Registro Anatel 035152008867. Fortigate 90G: Registro Anatel 038302408867.

3.4.2 Os equipamentos fornecidos deverão ser capazes de integrar diferentes tecnologias WAN, provedores e meios de acesso à internet, permitindo a evolução tecnológica e situacional dos circuitos.
R: R: SD-WAN: Fortigate 40F e Fortigate 90G com licenciamento UTP possuem funcionalidade de SD-WAN capaz de consolidar os links.
Datasheet 40F: Tópicos “Perimeter Protection” e “Secure SD-WAN” página 2
Datasheet 90G: Tópicos “Perimeter Protection” e “Secure SD-WAN” página 2

4- Gerenciamento de Rede

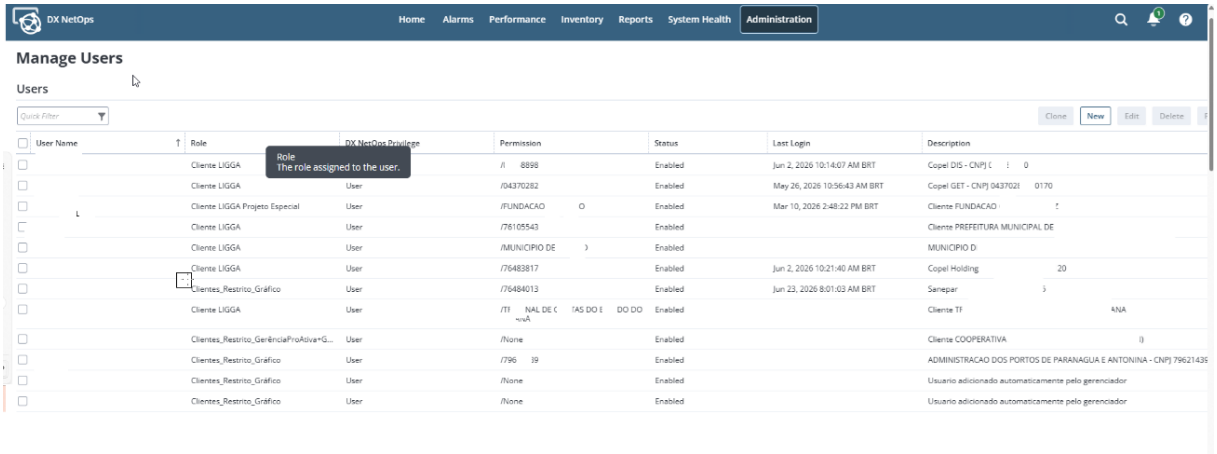
3.11.3 Deverá permitir acesso de usuários com perfis diferenciados com limitação de acesso a consoles, dispositivos, menus, alarmes, indicadores, etc.

R: Atende: Após a instalação dos links os perfis podem ser configurados conforme as premissas.



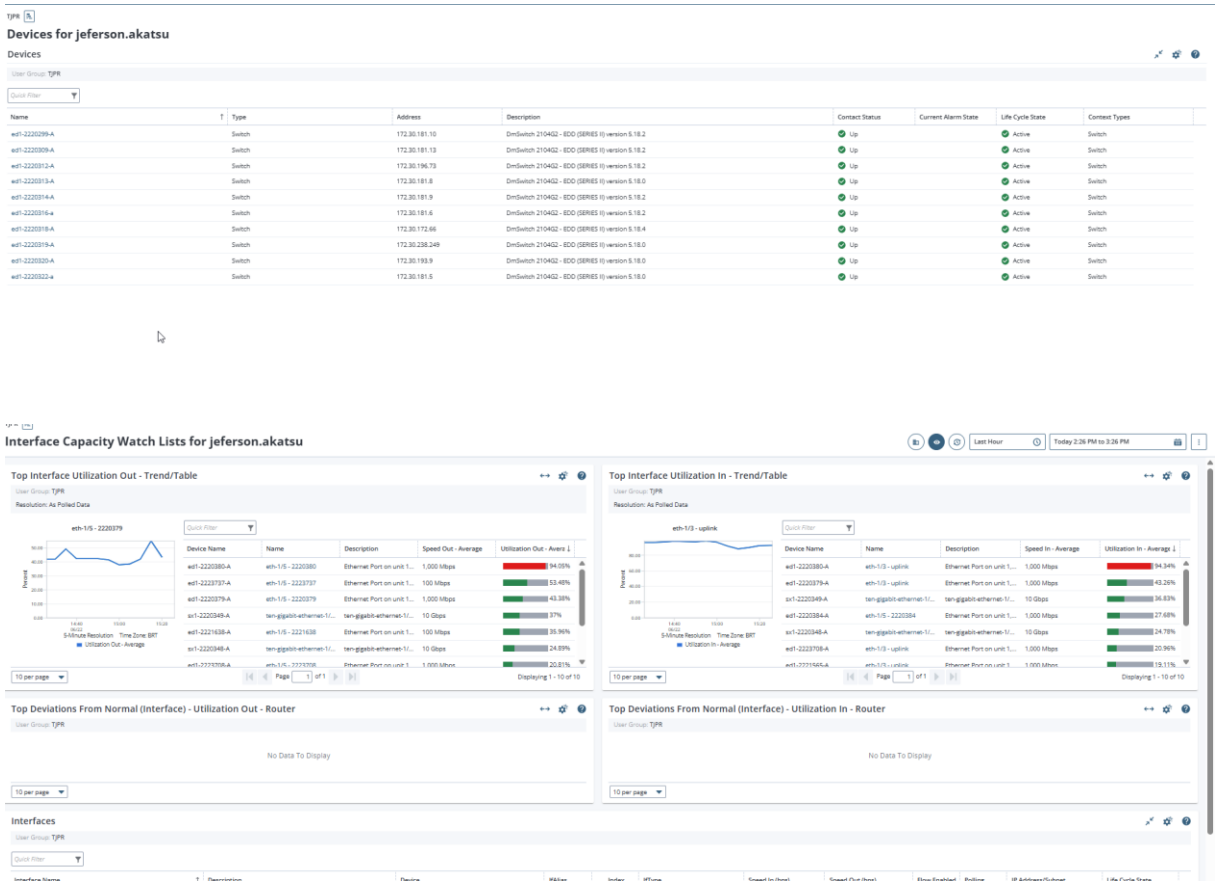
3.11.4 A solução de gerência de rede deverá permitir ainda a criação de grupos de perfis de acesso, que serão associados a tipos de usuários.

R: Atende: Após a instalação dos links os perfis e grupos podem ser configurados conforme as premissas.



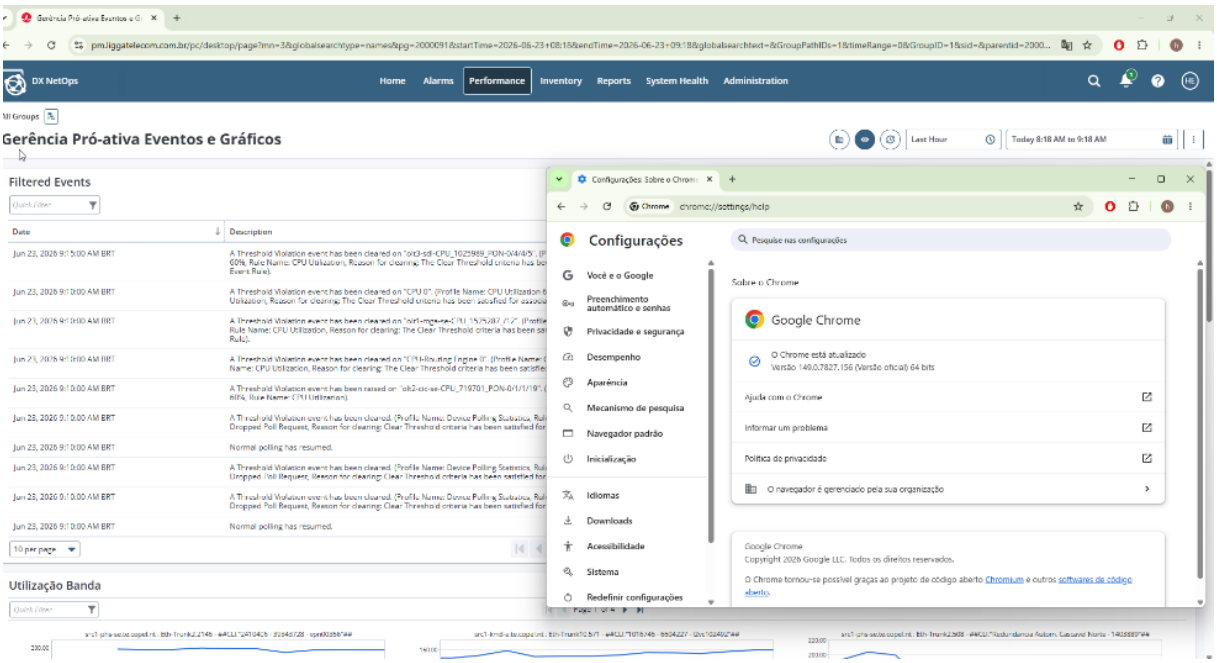
3.11.5 Os perfis deverão prever configurações de níveis de alertas, equipamentos, interfaces, aplicações, funcionalidades de monitoração, capacity planning, inventário, etc.

R: Atende conforme telas abaixo



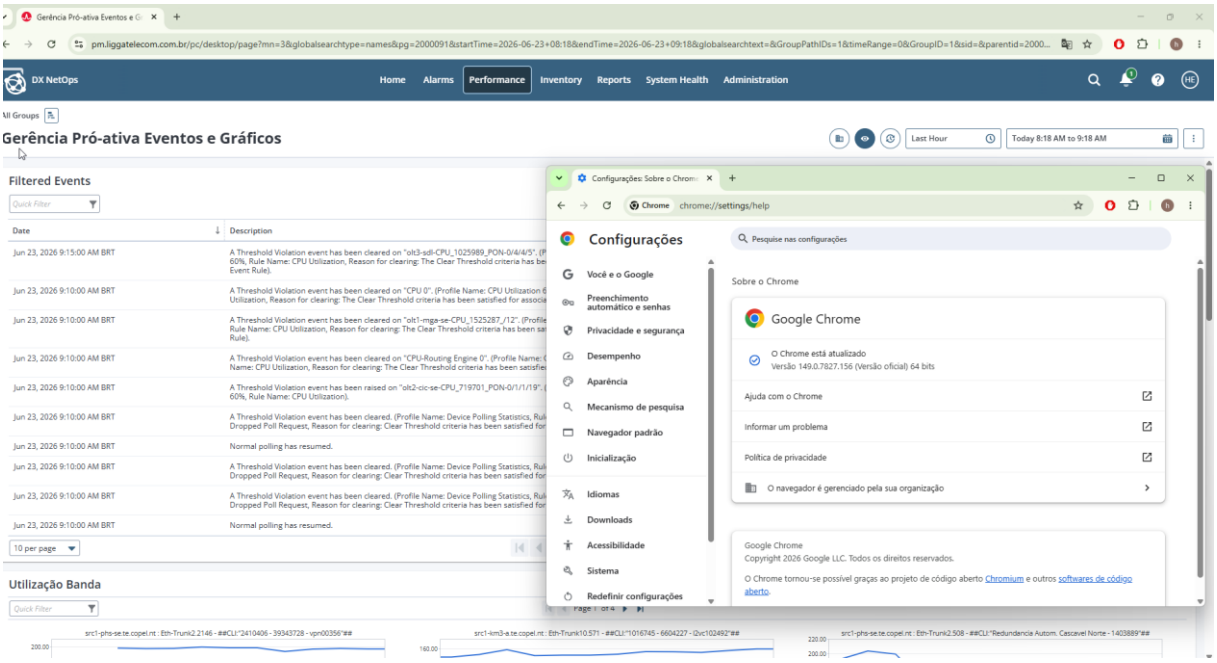
3.11.6 A solução de gerência de redes deverá ser 100% web, sem necessidade de instalação de clientes específicos, portanto, não serão aceitas soluções que requeiram a instalação de agentes ou plug-ins nos desktops das estações da CONTRATANTE.

R: Atende plenamente.



3.11.8 A solução de gerenciamento de rede deve ser acessível através dos principais browsers do mercado tais como, Firefox, Google Chrome e Safari.

R: Atende Plenamente



3.11.10A solução de gerenciamento deverá possuir funcionalidade de geração de alertas para uso excessivo ou incomum dos recursos de dados.

R: Atende: Após a instalação dos links é possível criar alertas conforme premissas.

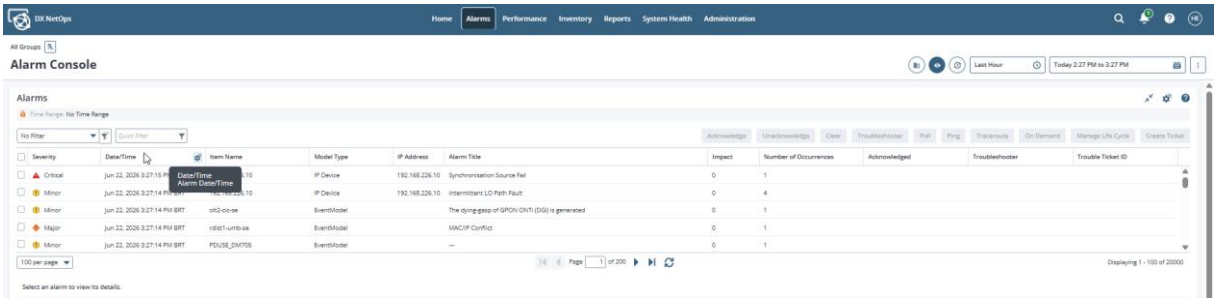
3.11.11A solução de gerência de rede deverá fornecer, através do portal, visualização de informações on-line da rede, que deverá apresentar no mínimo os seguintes itens para cada um dos elementos monitorados:

3.11.11.1 Topologia da rede, incluindo os CPEs e seus enlaces, com visualização do estado operacional de todos os elementos da rede. O estado operacional dos elementos da rede deverá ser atualizado automaticamente na Solução de Gerência da Rede, sempre que os mesmos sofrerem alterações;

R: Atende: Após a instalação dos links a topologia é criada e atualizada automaticamente em caso de alteração ao acréscimo.

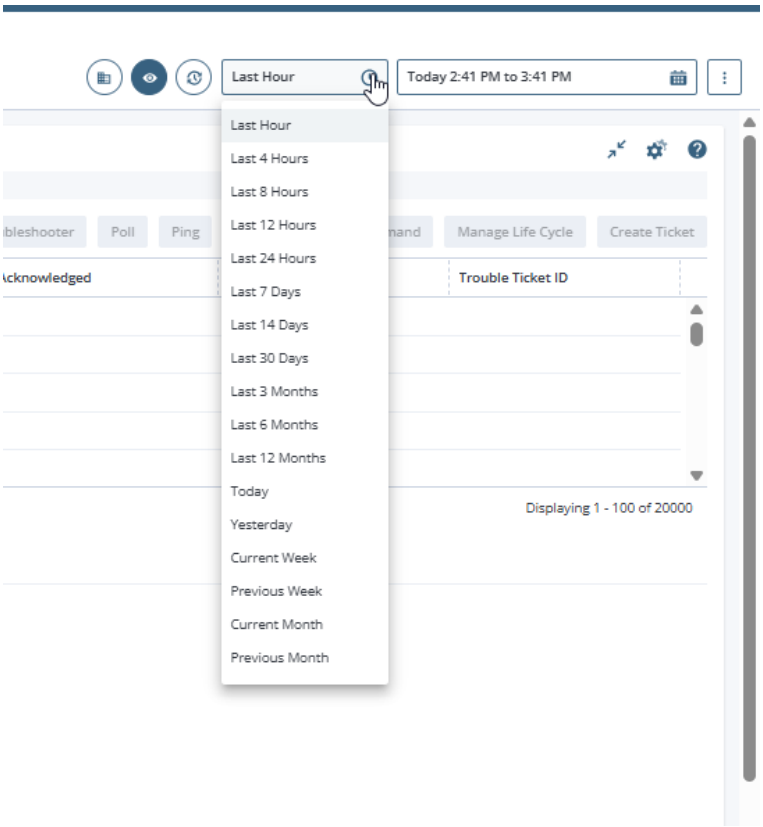
3.11.11.2 Alarmes de eventos ocorridos na rede com informações de data, hora e duração da ocorrência e identificação dos recursos gerenciados;

R: Atende conforme tela abaixo:



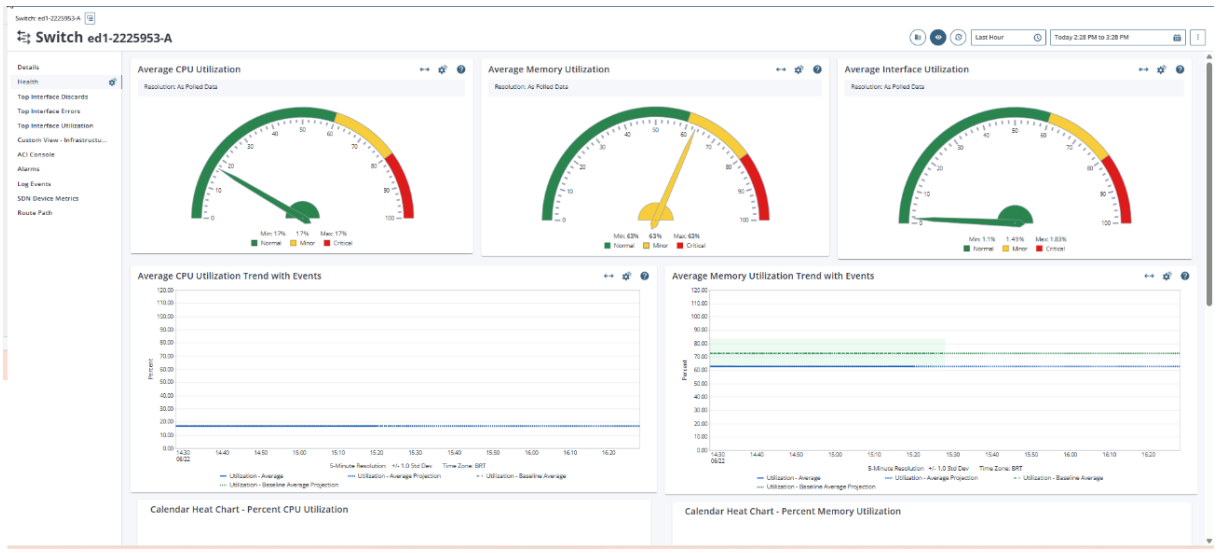
3.11.11.3 Consumo de banda dos enlaces separados por dia e mês;

R: Atende conforme tela abaixo:



3.11.11.4 Ocupação de memória e CPU dos equipamentos CPE;

R: Atende conforme telas abaixo:



3.11.11.5 Latência dos enlaces separados por dia e mês, em Milissegundos (mS);

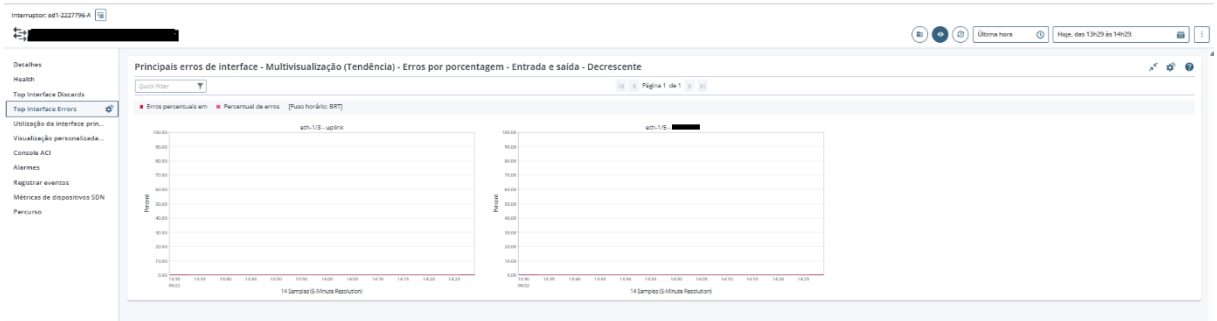
R: Atende através do portal apresentado nas imagens anteriores

3.11.11.6 Perda de pacotes no sentido IN e OUT em %;

R: Atende através do portal apresentado nas imagens anteriores

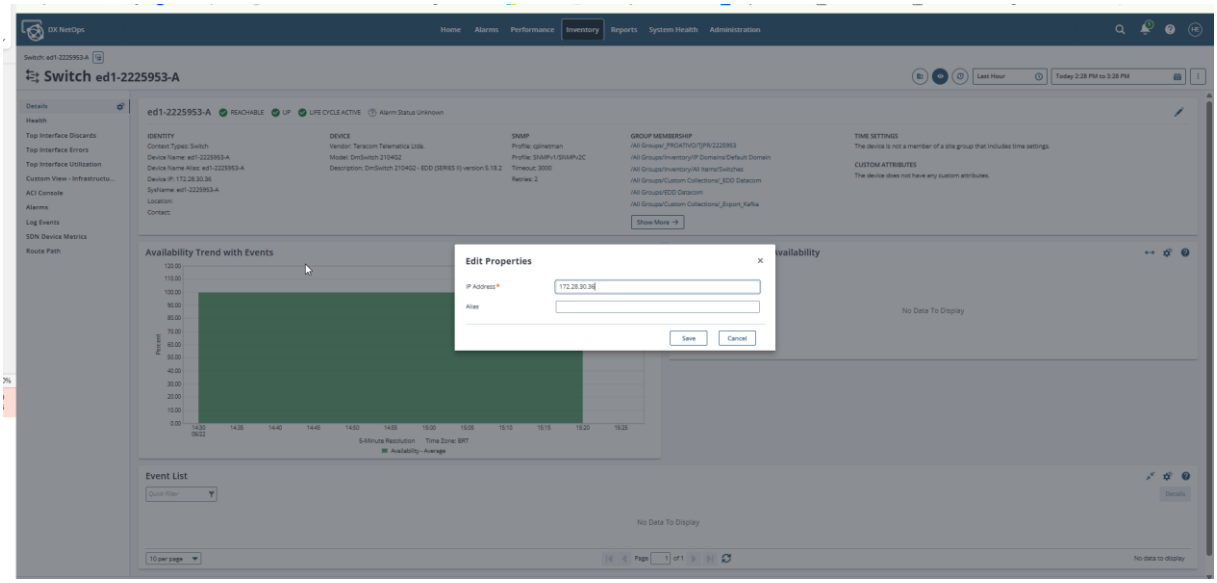
3.11.11.7 Taxa de erros em erros por segundo;

R: Atende conforme tela abaixo



3.11.13 A solução de gerenciamento de rede deverá permitir adição de nomenclatura conhecida pela CONTRATANTE para os recursos gerenciados.

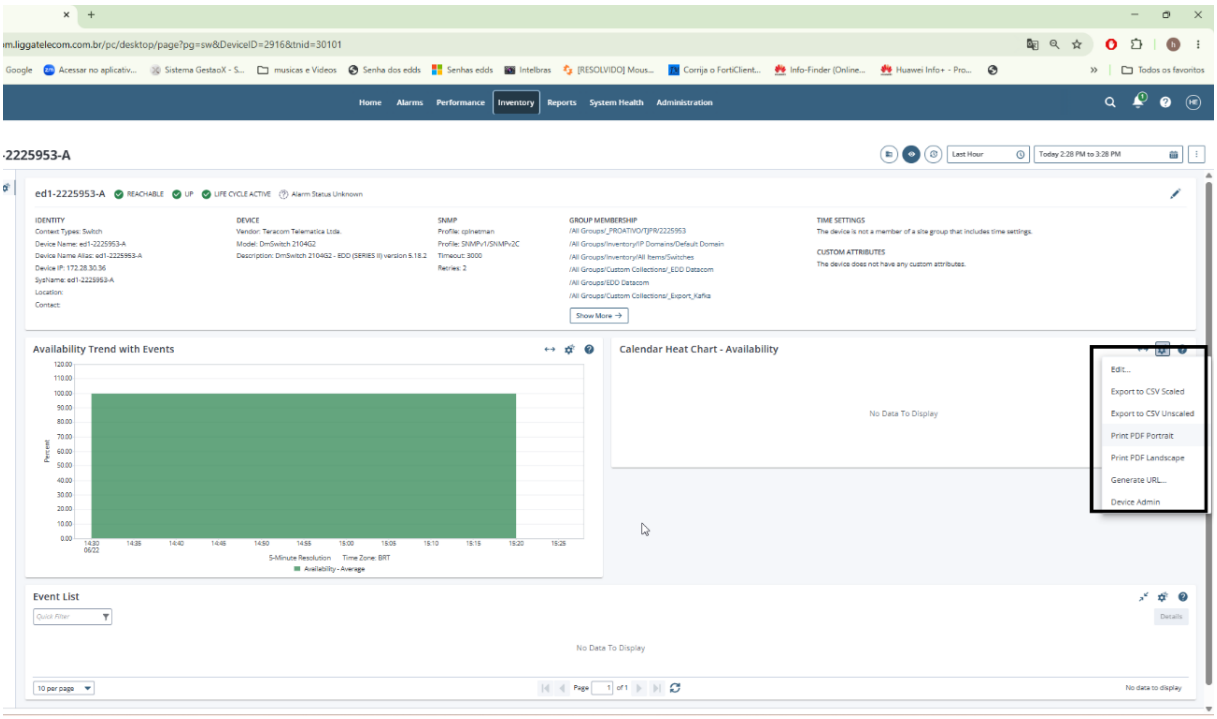
R: Atende conforme tela abaixo



3.11.14A solução de gerenciamento de rede deverá permitir a criação de relatórios (exportáveis conforme os principais métodos (PDF, CSV, pacote office)) como:

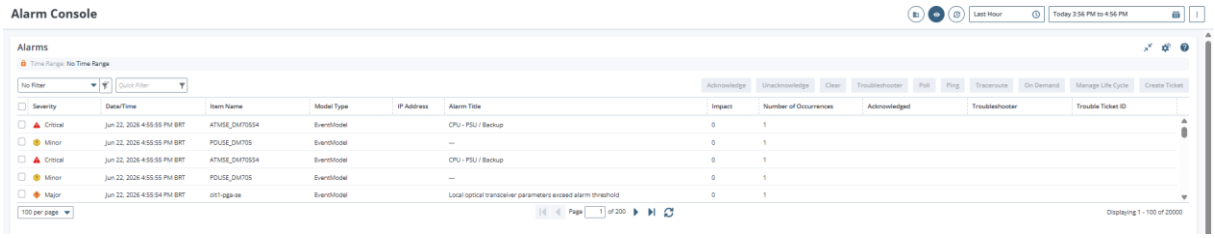
3.11.14.4 Dashboards relacionando falhas, desempenho, capacity e disponibilidade.

R: Atende conforme tela abaixo



3.11.15A solução deverá realizar registro de todas as ocorrências, alarmes e eventos em log de históricos ou base de dados contendo informações de data/hora da ocorrência, identificando os recursos gerenciados.

R: Atendido conforme tela abaixo



5 - SD-WAN

3.12 A solução de SD-WAN deverá ser composta pelos dispositivos SD-WAN (concentradores e equipamentos de borda (CPEs)) e pelo gerenciamento da solução SD-WAN, possuindo as seguintes características:

3.12.4 O gerenciamento da solução deve suportar acesso via SSH, WEB (HTTPS) e via API.

R: O FortiOS permite acesso via SSH (https://docs.fortinet.com/document/fortigate/7.4.12/administration-guide/901037/connecting-to-the-cli), WEB (https://docs.fortinet.com/document/fortigate/7.4.12/administration-guide/241541/connecting-using-a-web-browser) e API (https://docs.fortinet.com/document/fortigate/7.4.12/administration-guide/940602/using-apis)

3.12.5 Deverá possuir a funcionalidade de DHCP Cliente, Servidor e Relay.

R: O FortiOS possui a funcionalidade de DHCP: https://docs.fortinet.com/document/fortigate/7.4.12/administration-guide/783526/dhcp-servers-and-relays

3.12.6 A solução deverá suportar mecanismo de alta disponibilidade compatível com a criticidade do ambiente, podendo operar no modo Ativo-Passivo e também ativo ativo.

R: Foritigate 40F página 8 do datasheet: High Availability Configurations: Active-Active, Active-Passive, Clustering.

Fortigate 90G página 8 do datasheet: High Availability Configurations: Active-Active, Active-Passive, Clustering.

3.12.7 Deverá permitir o funcionamento em modo transparente tipo “bridge”.
R: O FortiOS permit o funcionamento em modo transparente: https://docs.fortinet.com/document/fortigate/7.4.12/administration-guide/402940/vlan

3.12.8 Deverá possuir conexão entre estação de gerência e appliance criptografada, tanto em interface gráfica, quanto CLI (Linha de Comando).
R: O FortiOS suporta e impõe criptografia na comunicação de gerência nativamente, utilizando o protocolo HTTPS para acesso seguro à interface gráfica (WEB) e SSH para a interface de linha de comando (CLI). (https://docs.fortinet.com/document/fortigate/7.4.12/administration-guide/901037/connecting-to-the-cli e https://docs.fortinet.com/document/fortigate/7.4.12/administration-guide/241541/connecting-using-a-web-browser)

3.12.9 Deverá permitir autenticação de usuários em base local, servidor LDAP, RADIUS e TACACS+.
R: O FortiOS permite autenticação em base local, servidor LDAP, RADIUS e TACACS+: https://docs.fortinet.com/document/fortigate/7.4.12/administration-guide/766272/remote-authentication-for-administrators

3.12.10Deve permitir monitorar via SNMP o uso de CPU, memória, espaço em disco, VPN, situação do Cluster, eventos de segurança e estatística das verificações de saúde da camada SDWAN.
R: O FortiOS permite monitorar via SNMP:
https://docs.fortinet.com/document/fortigate/7.4.12/administration-guide/62595/snmp e
https://docs.fortinet.com/document/fortigate/7.4.12/administration-guide/608160/mib-files

3.12.12Deverá possuir a capacidade de criar automações possibilitando uma atuação mais proativa através de gatilhos e ações como execução de scripts, envio de emails, WebHooks e APIs mediante ocorrência de hosts comprometidos, agendamentos, mudanças de configuração e ocorrência de eventos de rede e segurança pré-definidos.

R: FortiOS possui o recurso de Automation Stitches (Security Fabric), que permite a criação de gatilhos baseados em logs de sistema, agendamentos, mudanças de configuração ou comprometimento de hosts (IOC). Estes gatilhos podem acionar ações automatizadas em tempo real, como envio de alertas por e-mail, WebHooks, execução de scripts via CLI e chamadas de API. https://docs.fortinet.com/document/fortigate/7.4.12/administration-guide/139441/automation-stitches

3.12.13 A configuração de alta disponibilidade deve possibilitar a monitoração de falha de link e falha de fornecimento de energia nos equipamentos CPE.
R: O FortiOS possibilita a monitoração do link e energia
https://docs.fortinet.com/document/fortigate/7.4.12/administration-guide/666376/high-availability

6 - Solução SD-WAN

3.13.2 Deverá ser capaz de agregar minimamente 03 links em uma interface virtual;
R: O FortiOS permite agregar múltiplos links (físicos e virtuais) em uma única interface lógica do tipo SD-WAN Zone, superando com facilidade o mínimo exigido de 03 links e centralizando a gestão de roteamento de todo o circuito.
https://docs.fortinet.com/document/fortigate/7.4.12/administration-guide/523215/sd-wan-zones

3.13.3 Deverá ser capaz de adicionar e equilibrar, no mínimo, 06 interfaces de dados, entre links e tuneis VPN.
R: A solução FortiGate suporta a adição de dezenas de membros (SD-WAN Members), permitindo gerenciar e equilibrar simultaneamente links físicos de internet, MPLS e diversos túneis VPN IPsec em sua zona de SD-WAN. O limitador serão as interfaces físicas dos equipamentos.
https://docs.fortinet.com/document/fortigate/7.4.12/administration-guide/523215/sd-wan-zones

3.13.4 A solução deverá ser capaz de medir o status de qualidade do link baseando-se em critérios mínimos de latência, jitter e perda de pacotes, onde deve ser possível configurar um

valor limite para cada um destes itens que será utilizado como gatilho para fator de decisão nas regras de tráfego de saída e balanceamento inteligente.

R: O FortiOS permite medir a qualidade do link por latência, jitter e perda de pacotes e é possível configurar limites de SLA para cada parâmetro e efetuar o balanceamento: https://docs.fortinet.com/document/fortigate/7.4.12/administration-guide/943037/monitoring-performance-sla

3.13.5 A solução deve ser capaz de monitorar a qualidade e identificar falhas nos links, enviando sinais por meio de cada link para servidores ou aplicações, permitindo utilizar protocolos como BGP, IPsec e TWAMP para monitoramento ativo dos links.
R: O FortiOS permite o monitoramento de qualidade e identifica falha no link: https://docs.fortinet.com/document/fortigate/7.4.12/administration-guide/22371/best-quality-strategy

Também permite a utilização de protocolos como BGP (https://docs.fortinet.com/document/fortigate/7.4.12/administration-guide/722590/using-multiple-members-per-sd-wan-neighbor-configuration), IPSec (https://docs.fortinet.com/document/fortigate/7.4.12/administration-guide/050631/sla-link-monitoring-for-dynamic-ipsec-and-ssl-vpn-tunnels) e TWAMP (https://docs.fortinet.com/document/fortigate/7.4.12/administration-guide/76624/link-monitor) para monitorar os links.

3.13.6 A solução deve possibilitar o balanceamento de tráfego entre conexões WAN, de forma em que o algoritmo de balanceamento de carga utilizado possa ser configurado usando os seguintes parâmetros: sessões, volume de trafego, IP de origem e destino, transbordo de link, entre outros.
R: O FortiOS permite o balanceamento de tráfego e possui diversos parâmetros para o balanceamento de carga:
https://docs.fortinet.com/document/fortigate/7.4.12/administration-guide/716691/sd-wan-rules e https://docs.fortinet.com/document/fortigate/7.4.12/administration-guide/683285/selecting-the-implicit-sd-wan-algorithm

3.13.7 A solução deve possibilitar a criação de regras para políticas de roteamento com seleção das interfaces de saída e suas prioridades que será utilizada para encaminhar o tráfego de saída de rede, considerando os seguintes critérios:
R: Atendido através das respostas abaixo

3.13.7.1 Manual: Deve permitir que as interfaces tenham as propriedades atribuídas manualmente.
R: O FortiOS permite propriedade atribuídas manualmente:
https://docs.fortinet.com/document/fortigate/7.4.12/administration-guide/723448/manual-strategy

3.13.7.2 Melhor qualidade: Deve permitir que as interfaces recebam uma prioridade com base na qualidade do link no qual a interface está conectada, considerando o monitoramento de pelo menos um dos seguintes parâmetros com valores customizáveis: Jitter, latência, perda de pacotes ou largura de banda.
R: O FortiOS permite a prioridade por melhor qualidade:
https://docs.fortinet.com/document/fortigate/7.4.12/administration-guide/22371/best-quality-strategy

3.13.7.3 Menor custo: Deve permitir que as interfaces recebam uma prioridade com base no custo atribuído a interface, considerando a satisfação dos parâmetros de qualidade do link no qual a interface está conectada.
R: O FortiOS possui estratégia de menor custo:
https://docs.fortinet.com/document/fortigate/7.4.12/administration-guide/342836/lowest-cost-sla-strategy

3.13.7.4 Balanceamento da carga: Deve permitir que o tráfego seja distribuído entre todas as interfaces disponíveis com base em algoritmos de balanceamento de carga e satisfação dos parâmetros customizados de qualidade do link no qual a interface está conectada.
R: O FortiOS permite estratégia por balanceamento de carga:
https://docs.fortinet.com/document/fortigate/7.4.12/administration-guide/708464/load-balancing-strategy

3.13.8 A solução SD-WAN deve possuir suporte a Policy Based Routing ou Policy Based Forwarding.

R: O FortiOS suporta nativamente o Policy Based Routing (PBR), que é configurado diretamente através das SD-WAN Rules, permitindo o roteamento dinâmico de tráfego com base em aplicações, serviços, usuários e indicadores de qualidade (SLA). https://docs.fortinet.com/document/fortigate/7.4.12/administration-guide/716691/sd-wan-rules

3.13.9 Deve possibilitar a agregação de túneis IPSec, realizando balanceamento por pacotes entre os mesmos.

R: O FortiOS permite agregação de túneis IPSec: https://docs.fortinet.com/document/fortigate/7.4.12/administration-guide/779544/packet-distribution-and-redundancy-for-aggregate-ipsec-tunnels

3.13.10A solução deve possibilitar a descoberta, criação e uso de tuneis VPN de forma automática e dinâmica entre os locais de instalação, para aplicações sensíveis.

R: A solução suporta a tecnologia ADVPN (Auto-Discovery VPN), que estabelece dinamicamente túneis IPsec "spoke-to-spoke" (entre localidades) de forma automática e sob demanda. Isso garante caminhos mais curtos, reduzindo a latência para as aplicações sensíveis. https://docs.fortinet.com/document/fortigate/7.4.12/administration-guide/985659/advpn-and-shortcut-paths

3.13.11A solução deve possuir recursos para controlar e corrigir erros na transmissão de dados, enviando dados redundante através de túnel VPN em antecipação à perda de pacotes que pode ocorrer durante a transmissão.

R: O FortiOS possui recursos avançados de remediação de WAN, incluindo suporte nativo a Forward Error Correction (FEC) para recuperar pacotes corrompidos/perdidos e Packet Duplication (duplicação de pacotes) que transmite o mesmo tráfego crítico em múltiplos túneis simultâneos, mitigando falhas na rede.

https://docs.fortinet.com/document/fortigate/7.4.12/administration-guide/779544/packet-distribution-and-redundancy-for-aggregate-ipsec-tunnels

3.13.12A solução deve prover estatísticas em tempo real na interface web a respeito da ocupação de banda (upload e download) e desempenho das verificações de saúde dos links (perda de pacotes, jitter e latência)

R: Através do painel do FortiOS (Dashboards e SD-WAN Monitor), a solução fornece estatísticas gráficas em tempo real demonstrando a ocupação de banda (upload/download), além das métricas vitais medidas pelo Performance SLA de cada link (latência, jitter e perda de pacotes). https://docs.fortinet.com/document/fortigate/7.4.12/administration-guide/943037/monitoring-performance-sla

3.13.13A solução deve permitir a customização do intervalo de tempo em que é feita a verificação da situação de um link, assim como, permitir definir a quantidade de falhas encontradas no link antes de declará-lo inativo, com o objetivo de identificar oscilações nos links que possam impactar os serviços e a experiencia do usuário.

R: O FortiOS permite total customização nas regras de Performance SLA (Health Checks), possibilitando definir o intervalo exato entre as sondagens (Probe Interval), a quantidade de falhas consecutivas aceitas antes de o link ser marcado como inativo (Failures before inactive) e o número de sucessos necessários para restaurá-lo. https://docs.fortinet.com/document/fortigate/7.4.12/administration-guide/943037/monitoring-performance-sla

3.13.14Deve suportar balanceamento de tráfego por sessão e pacote.

R: O FortiOS suporta múltiplos algoritmos de balanceamento no SD-WAN, permitindo distribuição baseada em sessão (Source IP, Source-Destination IP, Sessions, Spillover) e também baseada em volume de tráfego/pacotes na agregação de túneis e links. https://docs.fortinet.com/document/fortigate/7.4.12/administration-guide/683285/selecting-the-implicit-sd-wan-algorithm

3.13.15Deve permitir a extração de informações de desempenho das verificações de saúde mediante REST API, permitindo assim a consolidação de tais informações em aplicações externas.

R: O FortiOS conta com uma poderosa REST API que permite a consulta, configuração e extração estruturada de dados do sistema, incluindo todas as estatísticas de desempenho e logs de saúde dos links (SLA), facilitando a integração nativa com aplicações e monitoramentos externos.

https://docs.fortinet.com/document/fortigate/7.4.12/administration-guide/940602/using-apis

3.13.16Deve gerar log de eventos que registrem alterações no estado dos links SD-WAN monitorados pela verificação de saúde.

R: A solução gera automaticamente alertas e System Event Logs detalhados que registram toda e qualquer mudança de estado (Up/Down) dos links de rede e violações de latência/jitter estipuladas no SD-WAN Performance SLA.

https://docs.fortinet.com/document/fortigate/7.4.12/administration-guide/943037/monitoring-performance-sla

7 - Funcionalidade VPN

3.14.1 Suportar VPN Site-to-Site e Client-to-Site;

R: O FortiOS suporta VPN Site-to-Site (https://docs.fortinet.com/document/fortigate/7.4.12/administration-guide/202791/site-to-site-vpn) e Client-to-Site (https://docs.fortinet.com/document/fortigate/7.4.12/administration-guide/371626/ssl-vpn)

3.14.2 Suportar IPsec VPN.

R: O FortiOS suporta IPSec VPN

https://docs.fortinet.com/document/fortigate/7.4.12/administration-guide/520377/ipsec-vpn

3.14.3 Suportar SSL VPN;

R: O FortiOS suporta SSL VPN

https://docs.fortinet.com/document/fortigate/7.4.12/administration-guide/371626/ssl-vpn

3.14.4 Deve possuir algoritmos de criptografia para tuneis VPN, tais como AES-256 e SHA-2;

R: O FortiOS suporta os algoritmos AES-256 e SHA-2, além de outras cifras:

https://docs.fortinet.com/document/fortigate/7.4.12/administration-guide/484445/fortigate-encryption-algorithm-cipher-suites

3.14.5 Deve permitir habilitar e desabilitar túnel de VPN IPsec através da interface gráfica da solução, facilitando o processo de resolução de problemas.

R: O FortiOS permite desabilitar túneis IPSec via interface gráfica (GUI).

8- QoS e Priorização de Tráfego

3.15.1 Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo (como youtube) e ter alto consumo de largura de banda, se requer que a solução além de poder permitir ou negar esse tipo de aplicação, deva ter a capacidade de controlá-las por meio de políticas de largura de banda máxima quando forem solicitadas por diferentes aplicações.

R: O FortiOS permite a configuração de políticas de largura de banda para aplicações específicas como o YouTube (https://docs.fortinet.com/document/fortigate/7.4.12/administration-guide/666067/application-groups-in-traffic-shaping-policies)

3.15.2 Deve suportar a criação de políticas de QoS e Traffic Shaping:

R: O FortiOS permite a criação de políticas de QoS e Traffic Shaping:
https://docs.fortinet.com/document/fortigate/7.4.12/administration-guide/297431/traffic-shaping

3.15.3 O QoS deve possibilitar a definição de tráfego com banda garantida, como por exemplo, banda mínima disponível para aplicações do negócio, e banda máxima permitida para aplicações não corporativas, tais como youtube, facebook entre outros.

R: Através dos perfis de Traffic Shaping, o FortiOS permite estabelecer uma "Banda Garantida" (Guaranteed Bandwidth) que reserva recursos para as aplicações essenciais de negócio, e configurar um limite de "Banda Máxima" (Maximum Bandwidth) para restringir o consumo de aplicações recreativas (como YouTube e mídias sociais).
https://docs.fortinet.com/document/fortigate/7.4.12/administration-guide/297431/traffic-shaping

3.15.4 O QoS deve possibilitar a definição de fila de prioridade.

R: O recurso de Traffic Shaping do FortiOS suporta o enfileiramento de pacotes por prioridade de tráfego (Alta, Média, Baixa), organizando os fluxos nas filas correspondentes na saída da

interface de rede. https://docs.fortinet.com/document/fortigate/7.4.12/administration-guide/297431/traffic-shaping

3.15.5 A rede deverá suportar QoS (Quality of Service) fim a fim.
R: A solução garante a marcação e o repasse de QoS fim a fim, permitindo classificar, ler e remarcar os pacotes em trânsito com os valores padrões de indústria para priorização, como os campos DSCP (Differentiated Services Code Point) e 802.1p (CoS). https://docs.fortinet.com/document/fortigate/7.4.12/administration-guide/297431/traffic-shaping

3.15.6 A rede deverá permitir o mapeamento dos tráfegos e largura de banda de cada classe do QoS.
R: O painel de monitoramento do FortiOS (FortiView Traffic Shaping) exibe em tempo real o tráfego de rede classificado, permitindo mapear visualmente a largura de banda consumida e as limitações aplicadas individualmente por cada classe de QoS (Shaper). https://docs.fortinet.com/document/fortigate/7.4.12/administration-guide/706509/fortiview-monitors-and-widgets

9- Requisitos de Habilitação

14.1 Atestado(s) de capacidade técnica, fornecido(s) por pessoa(s) jurídica(s) de direito público ou privado, comprovando que a empresa executou ou está executando serviços de fornecimento de link de dados privativos, com sistema de gerenciamento SD-WAN, pertinentes e compatíveis em características com o objeto do presente Termo de Referência, no mínimo, nas quantidades apresentadas na tabela a seguir:
R. Atendido. Experiência com circuitos de redundância no meio proposto (5G) através de serviços M2M em 5G, conforme evidenciado nas páginas 26, 28, 29, 31.

14.2 Apresentar o documento de Atestado de Visita Técnica emitido e assinado pela APPA, ou, caso tenha optado em não realizar a visita técnica, deverá apresentar em substituição ao Atestado de Visita Técnica, uma Declaração Formal assinada pelo representante da empresa, sob as penalidades da Lei, que tem pleno conhecimento das condições de peculiaridades inerentes à natureza dos trabalhos, que assume total responsabilidade por este fato, e que não

utilizará deste para quaisquer questionamentos futuros que ensejem questões técnicas ou financeiras, o qual deverá fazer parte do processo licitatório. A ausência destes documentos inabilitará a Proponente.

R: Atendido através de declaração evidenciada na página 172.

14.3 Apresentar documento que comprove que a PROPONENTE possui em seu quadro funcional no mínimo 1 (um) profissional com capacitação comprovada junto ao fabricante da solução SDWAN.

R: Atendido: Ficha do colaborador abaixo:

0008 - LIGGA SERVICOS EM TELECOM S.A.

Registro de Empregados

Portaria 41 MTE, de 28/03/2007 DOU 30/03/2007

22/06/2026 16:23

Ficha.: 1989 — **1989 - GUILHERME MOREIRA**

Empregador

Razão Social: LIGGA SERVICOS EM TELECOM S.A.
Filial: 1 - LIGGA SERVICOS
CNPJ: 65.649.511/0001.84
Ativid. CNAE Fiscal: 6110803
Endereço: AV VICENTE MACHADO, 1001
Bairro: BATEL
Município: 41.06902 - Curitiba - PR
CEP: 80.420-011

Colaborador

Data Nascimento: 21/06/1984
Naturalidade: Curitiba - PR
Nacionalidade: 010 - Brasileiro

Filiação

Pai: DILERMANO MOREIRA
Mãe: ELISABETE MOREIRA

Documentos

CPF: 043.126.349-39
CTPS/Série/UF: 431263 - 4939 - - PR
PIS/PASEP: 127.44180.51.5

Histórico Contratual

Data Inclusão: 11/04/2025
Hora Inclusão: 11:00
Matrícula eSocial: SELIGGASER00000000000000000506
Nr. Ficha Registro: 000001989
Data Admissão: 14/04/2025
Cargo: 000001110 ANALISTA CENTRO OPERACOES PL

Período Pagto: M - Mensal
% Insalubridade: 0,00
% Periculosidade: 0,00
Jornada Trabalho: 08:00 às 12:00 - 14:00 às 18:00
DSR: Domingo
Data Desligamento: 00/00/0000
Data Final do Aviso: 00/00/0000
Escala: 9199 - FLEXIVEL-CURITIBA (032)
Local: 01.02.04.01.01 - CENTRO SERV CORPORATIVO

Estrangeiro

Ano Chegada:
Condição:
Nr. Carteira RNE:
Validade:
Nr/Serie Ct. Trab.:
Expedição:

14.4 Apresentar comprovação de que possui Licença própria e válida para execução das atividades objeto desta contratação (SCM- Sistema de Comunicação Multimídia), estando licenciada pela ANATEL - Agência Nacional de Telecomunicações, conforme previsto no Regulamento Geral de Outorgas.

R. Atendido pg. 268

10 - Requisitos de Sustentabilidade

7.1 A empresa CONTRATADA deverá demonstrar seu compromisso com a sustentabilidade, em alinhamento com as diretrizes da Portos do Paraná, os requisitos previstos no RILC. A comprovação poderá ser feita por meio da apresentação de políticas, programas, certificações ambientais, ou, alternativamente, através de evidências concretas de projetos e práticas sustentáveis implementadas.
R: Atendido através do Eixo Ambiental do relatório ESG apresentado nas páginas 228 a 232.

CONSIDERAÇÕES FINAIS

Diante dos esclarecimentos apresentados, a **LIGGA TELECOMUNICAÇÕES S.A.** entende ter atendido integralmente a diligência, demonstrando o pleno atendimento aos requisitos técnicos, operacionais e de habilitação previstos no instrumento convocatório.

Por fim, a LIGGA se coloca à inteira disposição para prestar quaisquer esclarecimentos adicionais que eventualmente se façam necessários.

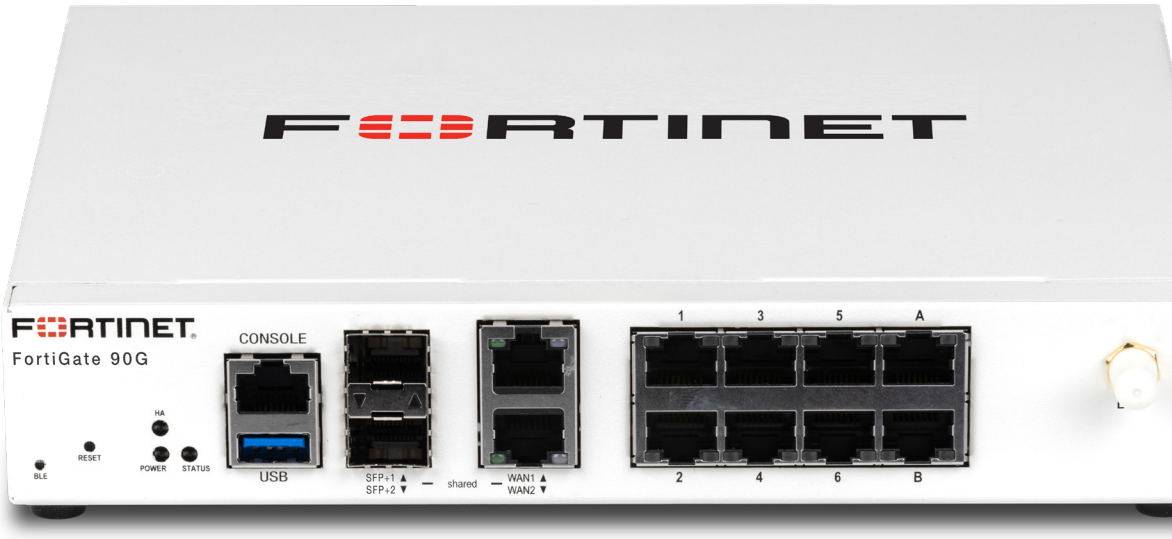
Nessa hipótese, visando assegurar a plena observância dos princípios do contraditório, da ampla defesa, da razoabilidade e da busca da proposta mais vantajosa para a Administração, requer desde já que seja concedido prazo adicional para manifestação e apresentação dos esclarecimentos ou documentos eventualmente solicitados.

Nossos votos de elevada consideração.

gov.br Documento assinado digitalmente
CAMILO JOSE GASPARETTO
Data: 26/06/2026 11:31:26-0300
Verifique em https://validar.iti.gov.br

LIGGA TELECOMUNICAÇÕES S.A.
CNPJ/MF n.º 04.368.865/0001-66

FortiGate 90G Series



Highlights

Leader in the Gartner® Magic Quadrant™ for Hybrid Mesh Firewall

Unparalleled performance enabled by Fortinet's patented ASIC and the AI-enriched FortiOS operating system

Enterprise-grade protection with FortiGuard AI-Powered Security Services

Simplified operations with centralized management for networking and security, automated workflows, deep analytics, and self-healing

Inclusive SD-WAN and network controller in every FortiGate appliance at no extra cost

Rich portfolio for any business budget and need

Converged Next-Generation Firewall and SD-WAN

The FortiGate 90G series integrates firewalling, SD-WAN, network controller, and security in one appliance, making them perfect for building secure networks at distributed enterprise sites and transforming WAN architecture at any scale.

The 90G series runs on FortiOS, a converged networking and security platform with secure AI controls and quantum-safe protection. This single OS approach enables businesses to gain benefits of operational efficiency and unified protection from the seamless integration of Fortinet solutions within a hybrid mesh firewall architecture.

As a cornerstone of the Fortinet Security Fabric platform, the FortiGate NGFW works seamlessly with FortiGuard AI-Powered Security Services to deliver coordinated, automated, end-to-end threat protection in real time.

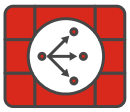
The 90G family is built on the patented SD-WAN-based ASIC, which delivers unmatched performance over traditional CPUs with lower cost and reduced power consumption. This application-specific design and embedded multi-core processor further accelerate the convergence of networking and security functions in the 90G family to optimize secure connections and deliver a robust user experience at branch locations.

IPS	NGFW	Threat Protection	Interfaces
4.5 Gbps	2.5 Gbps	2.2 Gbps	Multiple GE RJ45, 10 GE RJ45, and SFP+ Share Media Slots | Variants with internal storage

Use Cases

Perimeter Protection

- Protect networks from malicious traffic, guard against file-based threats, block web-based attacks, and secure applications and data with natively integrated FortiGuard AI-Powered Security Services
- Inspect and control incoming and outgoing traffic based on defined security policies
- Perform real-time SSL inspection (including TLS 1.3) with full visibility into users, devices, and applications across the attack surface
- Accelerate performance, protection, and energy efficiency with Fortinet's patented SPU with converged security and networking technologies



Secure SD-WAN

- FortiGate enables best-of-breed WAN edge with integrated SD-WAN, WAN optimization, security, and unified management from a single FortiOS operating system
- FortiGate, built on a patented SD-WAN-based ASIC, delivers faster application identification to avoid delays in accessing applications and accelerates overlay performance regardless of location
- Enhances hybrid working with a comprehensive SASE solution by integrating cloud-delivered SD-WAN with security service edge (SSE)
- Achieves operational efficiencies at any scale through automation, deep analytics, and self-healing

Secure Branch

- The Fortinet Security Fabric platform enables FortiGate NGFWs to automatically discover and secure IoT devices for faster branch onboarding
- Fully integrated with FortiSwitch secure Ethernet switches and FortiAP access points, FortiGate easily extends security to WAN, LAN, and WLAN at branch offices for unified protection and reliable connectivity
- FortiGate and Fortinet products work seamlessly with FortiManager to centralize visibility and simplify management across locations for IT teams
- FortiGate HA support ensures continuous network protection and minimizes downtime in the event of hardware failures or network disruptions

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

Available in

Appliance

Virtual

Hosted

Cloud

Container

FortiOS Everywhere

FortiOS, Fortinet's Real-Time Quantum-Safe Network Security Operating System

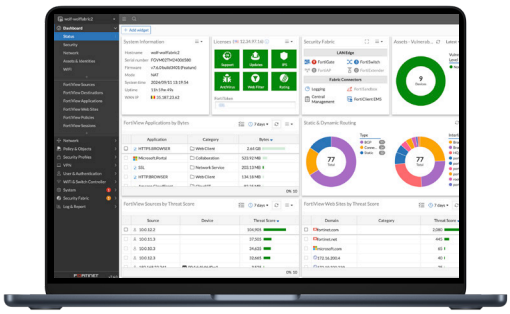
FortiOS is Fortinet's natively AI-powered and quantum-safe operating system (OS) that powers the Fortinet Security Fabric platform, enabling enforcement of security policies and holistic visibility across the entire attack surface. It provides a unified framework for securing networks across on-premises, cloud, hybrid environments, and the convergence of IT, OT, and IoT.

By converging networking and security functions into a single operating system, organizations can manage network and security more effectively to detect, investigate, and respond to incidents faster. This unified architecture simplifies operations, eliminates security silos, and allows organizations to scale securely without multiple tools or management complexity.

FortiOS also incorporates AI-driven capabilities that enhance threat detection, automate network activity analysis, and deliver more precise remediation guidance. Together, FortiGate firewalls and FortiOS provide intelligent, adaptive protection that reduces complexity, improves operational efficiency, and strengthens security across modern hybrid environments.

Learn more about what's new in FortiOS. https://www.fortinet.com/products/fortigate/fortios

Intuitive easy to use view into the network and endpoint vulnerabilities



Comprehensive view of network performance, security, and system status

FortiGuard AI-Powered Security Services

FortiGuard AI-Powered Security Services is part of Fortinet's layered defense and tightly integrated into our FortiGate NGFWs and other products. Powered by real-time AI enhanced threat intelligence from FortiGuard Labs, these services protect organizations against modern attack vectors and threats, including zero days and evasive, sophisticated AI-powered attacks.

Network and file security

Network and file security services protect against network and file-based threats. Consists of intrusion prevention system (IPS) which uses AI/ML models for deep packet/SSL inspection, detecting and blocking malicious content, uncovers hidden command-and-control activity, and applies virtual patches for newly discovered vulnerabilities. Application control improves security compliance and provides real-time visibility into applications and usage including generative AI (GenAI) applications.

Web/DNS security

Web/DNS security services protect against DNS-based attacks, malicious URLs (including those in emails), and botnet communications. DNS filtering blocks the full spectrum of DNS-based attacks while URL filtering uses a database of millions of URLs to identify and block malicious links. Meanwhile, IP reputation and anti-botnet services guard against botnet activity and DDoS attacks.

SaaS and data security

SaaS and data security services cover key security needs for application use and data protection. This service includes data loss/leakage prevention in files, GenAI applications and Images via OCR (optical character recognition). This ensures visibility, management, and protection (blocking exfiltration) of data in motion across networks, clouds, and users. The inline CASB service, secures SaaS applications in use, providing broad visibility and granular control over SaaS access, usage, and data.

Zero-day threat prevention

Zero-day threat prevention is achieved through AI-powered inline malware prevention to analyze file content to identify and block unknown and zero-day malware in real time, delivering sub-second protection across all NGFWs. Integrated into FortiGate NGFWs, the service provides comprehensive defense by blocking unknown threats, streamlining incident response, and reducing security overhead.

Attack surface visibility and compliance

The FortiGuard Attack Surface Security Service provides continuous, compliance-ready monitoring of your Fortinet Security Fabric infrastructure. It calculates your overall security posture rating by scoring controls against vulnerabilities, misconfigurations, and sub-optimal settings, while offering specific remediation guidelines for devices found out of configuration. It maintains continuous compliance with PCI DSS, CIS Controls, and Fortinet security best practices.

OT security

With over 2400 virtual patches, 1600+ OT applications, and 3500+ protocol rules, integrated OT security capabilities detect threats targeting OT infrastructure, perform vulnerability correlation, apply virtual patching, and utilize industry-specific protocol decoders for robust defense of OT environments and devices.

Unified Management for Optimal Security and Efficiency

Whether you are a small business or a large enterprise, Fortinet provides centralized control, visibility, and automation for your security infrastructure.

FortiManager: AI-powered, automation-driven, enterprise-class centralized management at scale

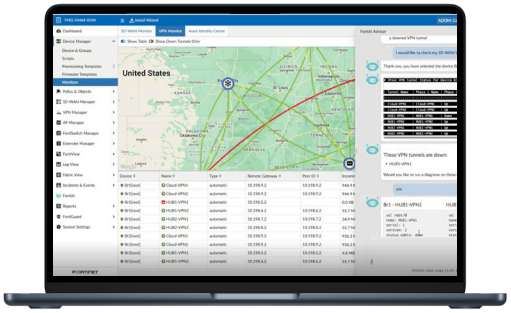
FortiManager, powered by FortiAI-Assist, provides centralized, single-pane management for the Fortinet Security Fabric, unifying configuration, policy, and responses across thousands of devices. It converges networking and security management, enabling consistent policy enforcement across SD-WAN, ZTNA, SASE, and branch environments while delivering real-time visibility and automated network operations.

FortiAI-Assist helps with Day 0–1 provisioning and Day N troubleshooting and maintenance. AI agents collaborating via a unified Model Context Protocol (MCP) framework automates goal-driven tasks toward a self-healing operation.

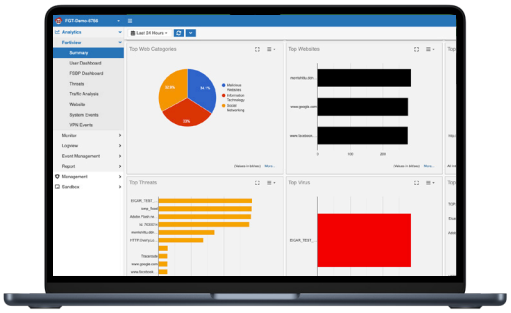
FortiManager integrates with FortiSOC for contextual insights and fabric-wise response. It also supports ecosystem integrations, and open APIs for extended automation. ADOM-based administration and FortiManager clusters enables resilient control across distributed networks.

FortiGate Cloud: Simplified management for small and mid-size businesses

FortiGate Cloud is a SaaS service offering simplified management, security analytics, and reporting for Fortinet FortiGate NGFWs to help you more efficiently manage your devices and reduce cyber risk. It simplifies the initial deployment, setup, and ongoing management of FortiGates and downstream connected devices such as FortiAP, FortiSwitch, and FortiExtender, with zero-touch provisioning. It provides real-time and historical visibility into traffic analytics and security threats to reduce risks and improve security posture. View various threats, web traffic, and system events stored in the cloud for up to a year, with predefined reports to meet compliance and deliver actionable insights.



GenAI in FortiManager helps manage networks effortlessly—generate configuration and policy scripts, troubleshoot issues, and execute recommended actions.



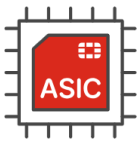
FortiGate Cloud provides intuitive management and analytics solution with end-to-end visibility, logging and reporting for SMB.

FortiConverter Service

Migration to FortiGate NGFW made easy

The FortiConverter Service provides hassle-free migration to help organizations transition quickly and easily from a wide range of legacy firewalls to FortiGate NGFWs. 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.

Fortinet ASICs: Unrivaled Security, Unprecedented Performance



Powered by the only purpose-built SPU

Traditional firewalls cannot protect against today's content and connection-based threats because they rely on off-the-shelf general-purpose central processing units (CPUs), leaving a dangerous security gap. Fortinet's custom SPUs deliver the power you need to radically increase speed, scale, and efficiency while greatly improving user experience and reducing footprint and power requirements. Fortinet's SPUs deliver up to 520 Gbps of protected throughput to detect emerging threats and block malicious content while ensuring your network security solution does not become a performance bottleneck.

Fortinet ASICs are designed to be energy-efficient, leading to lower power consumption and improved TCO. They deliver industry-leading throughput, handle more traffic and perform security inspections faster, reduce latency for quicker packet processing and minimize network delays.

Fortinet SPUs are designed with integrated security functions like zero trust, SSL, IPS, and VXLAN to name but a few, dramatically improving the performance of these functions that competitors traditionally implement in software.

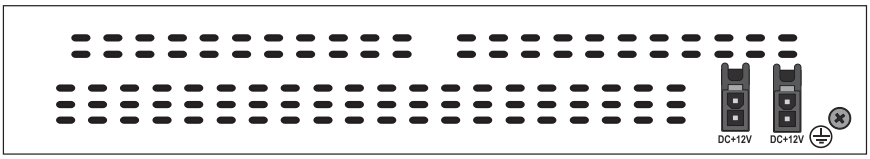
Secure SD-WAN ASIC SP5

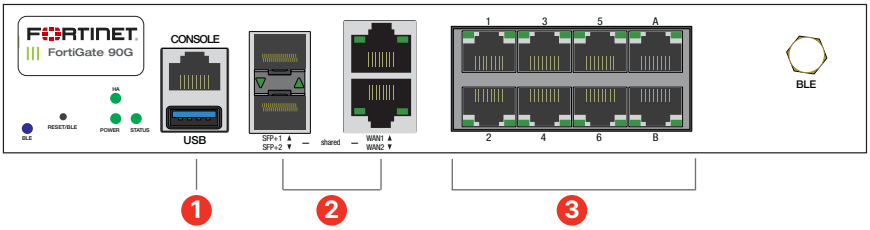
- Combines a RISC-based CPU with Fortinet's proprietary SPU content and network processors for unmatched performance
- Delivers the industry's fastest application identification and steering for efficient business operations
- Accelerates IPsec VPN performance for the best user experience on direct internet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

Hardware

FortiGate 90G/91G

SP5 DESKTOP 120GB





Interfaces

1. 1x RJ45 Console and 1x USB Management Port
2. 2× 10/5/2.5/ GE RJ45 or 10GE/GE SFP+/SFP Shared Media Ports
3. 8x GE RJ45 Ports

Hardware Features

Trusted Platform Module (TPM)

The FortiGate 90G 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.

Compact and reliable form factor

Designed for small environments, the FortiGate can be on a desktop or wall-mounted. It is small, lightweight, yet highly reliable with superior meantime between failures, minimizing the chance of network disruption.

Third-party verified Environmental Product Declaration

The FortiGate 90G/91G is EPD compliant with ISO 14025 Type III (externally verified), ensuring data accuracy and full transparency on the product environmental impacts throughout its life cycle. For more information please visit https://www.environdec.com/library/epd21562

EPD
INTERNATIONAL EPD SYSTEM

Specifications

	FORTIGATE 90G	FORTIGATE 91G
Hardware Specifications		
10/5/2.5/GE RJ45 or 10GE/GE SFP+/ SFP Shared Media pairs	2	2
GE RJ45 Internal Ports	8	8
Wireless Interface	—	—
USB Ports	1	1
Console (RJ45)	1	1
Internal Storage	–	1 × 120 GB SSD
Trusted Platform Module (TPM)	✓	✓
Bluetooth Low Energy (BLE)	✓	✓
Signed Firmware Hardware Switch	—	—
System Performance* — Enterprise Traffic Mix		
IPS Throughput [2]	4.5 Gbps	
NGFW Throughput [2, 4]	2.5 Gbps	
Threat Protection Throughput [2, 5]	2.2 Gbps	
System Performance and Capacity		
Firewall Throughput (1518 / 512 / 64 byte UDP packets)	28 / 28 / 27.9 Gbps	
Firewall Latency (64 byte UDP packets)	3.23 µs	
Firewall Throughput (Packets Per Second)	41.85 Mpps	
Concurrent Sessions (TCP)	3 M	
New Sessions/Second (TCP)	124 000	
Firewall Policies	5000	
IPsec VPN Throughput (512 byte) [1]	25 Gbps	
Gateway-to-Gateway IPsec VPN Tunnels	200	
Client-to-Gateway IPsec VPN Tunnels	2500	
SSL-VPN Throughput [6]	1.4 Gbps	
Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode)	200	
SSL Inspection Throughput (IPS, avg. HTTPS) [3]	2.6 Gbps	
SSL Inspection CPS (IPS, avg. HTTPS) [3]	1400	
SSL Inspection Concurrent Session (IPS, avg. HTTPS) [3]	300 000	
Application Control Throughput (HTTP 64K) [2]	6.7 Gbps	
CAPWAP Throughput (HTTP 64K)	23.6 Gbps	
Virtual Domains (Default / Maximum)	10 / 10	
Maximum Number of FortiSwitches Supported	24	
Maximum Number of FortiAPs (Total / Tunnel Mode)	128 / 64	
Maximum Number of FortiTokens	500	
High Availability Configurations	Active-Active, Active-Passive, Clustering	

	FORTIGATE 90G	FORTIGATE 91G
Dimensions		
Height x Width x Length (inches)	1.65 × 8.5 × 7.0	
Height x Width x Length (mm)	42 × 216 × 178	
Weight	2.47 lbs (1.12 kg)	
Form Factor	Desktop	
Operating Environment and Certifications		
Input Rating	12V 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	
Power Supply Efficiency Rating	80Plus Compliant	
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	
Power Consumption (Average / Maximum)	19.9 W / 20.53 W	22.4 W / 23.5 W
Heat Dissipation	70.0 BTU/hr	80.1 BTU/hr
Operating Temperature	32°F to 104°F (0°C to 40°C)	
Storage Temperature	-31°F to 158°F (-35°C to 70°C)	
Humidity	10% to 90% non-condensing	
Noise Level	21.73 dBA	
Operating Altitude	Up to 10 000 ft (3048 m)	
Compliance	FCC, ICES, CE, RCM, VCCI, BSMI, UL/cUL, CB	
Certifications	USGv6/IPv6	

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] SSL VPN only supported between 7.0.12 and 7.0.15

Subscriptions

Service Category	Service Offering	A-la-carte	Bundles			
			Enterprise Protection	Unified Threat Protection	Advanced Threat Protection	SD-WAN
FortiGuard Security Services	IPS — IPS, Malicious/Botnet URLs	•	•	•	•	
	Anti-Malware Protection (AMP)—AV, Botnet Domains, Mobile Malware, Virus Outbreak Protection, Content Disarm and Reconstruct[1], AI-based Heurestic AV, FortiGate Cloud Sandbox	•	•	•	•	
	URL, DNS and Video Filtering — URL, DNS and Video[1] Filtering, Malicious Certificate	•	•	•		
	Anti-Spam		•	•		
	AI-based Inline Malware Prevention	•	•			
	Data Loss Prevention (DLP) [2]	•	•			
	Attack Surface Security — IoT Device Detection, IoT Vulnerability Correlation and Virtual Patching, Security Rating, Outbreak Check		•			•
	OT Security—OT Device Detection, OT Vulnerability Correlation and Virtual Patching, OT Application Control and IPS [2]	•				
	Application Control		----------included with FortiCare Subscription----------			
	Inline CASB[1]		----------included with FortiCare Subscription----------			
SD-WAN and SASE Services	SD-WAN SLA Database					•
	SD-WAN Underlay and Application Monitoring Service					•
	SD-WAN Overlay Orchestration Service					•
	SD-WAN Connector for FortiSASE Secure Private Access					•
	FortiSASE Starter Kit for n* Users[3]					•
	FortiGate Cloud One Year Cloud-based Log Retention					•
	FortiTelemetry Cloud					•
NOC and SOC Services	FortiConverter Service for One Time Configuration Conversion	•	•			
	Managed FortiGate Service—Available 24×7, with Fortinet NOC Experts Performing Device Setup, Network, And Policy Change Management	•				
	FortiGate Cloud—Management, Analysis, and One Year Log Retention	•				
	FortiManager Cloud	•				
	FortiAnalyzer Cloud	•				
	FortiGuard SOCaaS—24×7 Cloud-Based Managed Log Monitoring, Incident Triage, and SOC Escalation Service	•				
Hardware and Software Support	FortiCare Essentials	Desktop models only				
	FortiCare Premium	•	•	•	•	•
	FortiCare Elite	•				
Base Services	Device/OS Detection, GeoIPs, Trusted CA Certificates, Internet Services and Botnet IPs, DDNS (v4/v6), Local Protection, PSIRT Check, Anti-Phishing		----------included with FortiCare Subscription----------			

1. Not available for FortiGate/FortiWiFi 40F, 60E, 60F, 80E, and 90E series from 7.4.4 onwards. Not available for FortiGate/FortiWiFi 30G and 50G series in any OS build.
2. Full features available when running FortiOS 7.4.1.
3. Only supported on FortiGate models from the 100F onwards (F-series and all later series).
See the FortiSASE Ordering Guide for supported models and corresponding user license allocations.

FortiGuard AI-Powered Security Bundles for FortiGate

FortiGuard AI-Powered Security Bundles provide a comprehensive and meticulously curated selection of security services to combat known, unknown, zero-day, and emerging AI-based threats. These services are designed to prevent malicious content from breaching your defenses, protect against web-based threats, secure devices throughout IT/OT/IoT environments, and ensure the safety of applications, users, and data. All bundles include FortiCare Premium Services featuring 24×7×365 availability, one-hour response for critical issues, and next-business-day response for noncritical matters.

FortiCare Services

Fortinet prioritizes customer success through FortiCare Services, optimizing the Fortinet Security Fabric solution. Our comprehensive life-cycle services include Design, Deploy, Operate, Optimize, and Evolve. The FortiCare Elite, one of the service offerings, provides heightened SLAs and swift issue resolution with a dedicated support team. This advanced support option includes an extended end-of-engineering support of 18 months, providing flexibility and access to the intuitive FortiCare Elite portal for a unified view of device and security health, streamlining operational efficiency and maximizing Fortinet deployment performance.

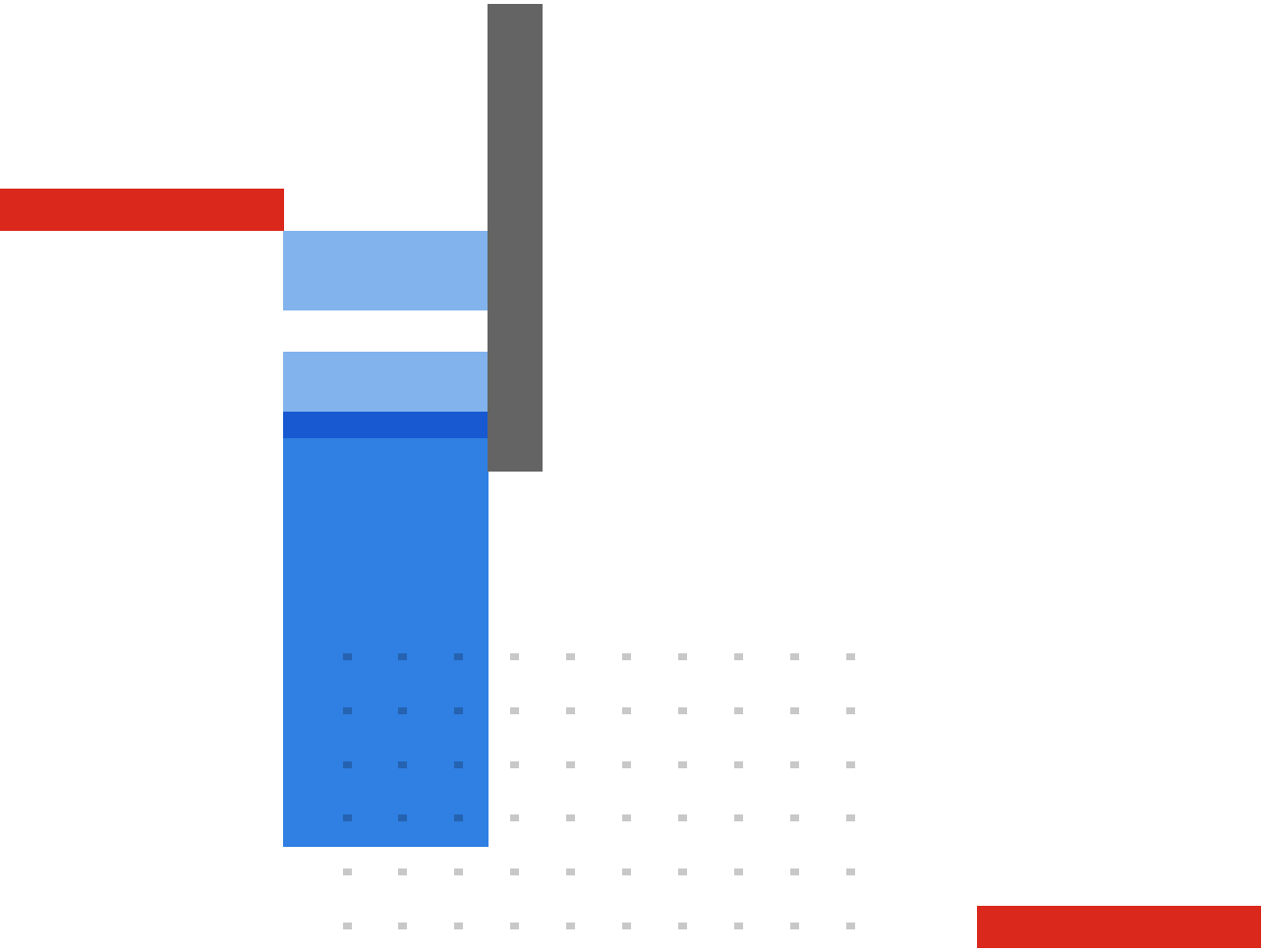
Ordering Information

Product	SKU	Description
FortiGate 90G	FG-90G	8x GE RJ45 ports, 2× 10GE RJ45/SFP+ shared media WAN ports.
FortiGate 91G	FG-91G	8x GE RJ45 ports, 2× 10GE RJ45/SFP+ shared media WAN ports with 120GB SSD.
Optional Accessories		
AC Power Adaptor	SP-FG60E-PDC-5	Pack of 5 AC power adaptors for FG/FWF 60E/61E, 60F/61F, 70/71F, 70/71G, 80E/81E, 80/81F, 90/91G and FDC-100G. Power cable SP-FG60CPCOR-XX sold separately
Wall Mount Kit	SP-FG60F-MOUNT-20	Pack of 20 wall mount kits for FG/FWF-60F, FG-90G/91G and FG/FWF-80F series.
Rack Mount Tray	SP-RACKTRAY-02	Rack mount tray for all FortiGate E, F, and G series desktop models.
Mounting Ear Bracket	SP-EAR-FG90G-10	Mounting Ear brackets for FG-90/91G 10 pairs pack.
Transceivers		
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.
1 GE SFP transceivers, 90km range, -40/85c operation	FR-TRAN-ZX	1 GE SFP transceiver module, long range 90km, LC connector, SMF, 1550nm, -40°C to 85°C, for systems with 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.
10 GE SFP+ Transceiver Module, 30km Long Range	FN-TRAN-SFP+BD27	10 GE SFP+ transceiver module, 30km long range single BiDi for systems with SFP+ and SFP/SFP+ slots (connects to FN-TRAN-SFP+BD33, ordered separately).
10 GE SFP+ Transceiver Module, (connects to FN-TRAN-SFP+BD27, ordered separately)	FN-TRAN-SFP+BD33	10 GE SFP+ transceiver module, 30km long range single BiDi for systems with SFP+ and SFP/SFP+ slots (connects to FN-TRAN-SFP+BD27, ordered separately).
Cables		
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.

Visit https://www.fortinet.com/resources/ordering-guides for related ordering guides.

Fortinet Corporate Social Responsibility 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

Copyright © 2026 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's SVP Legal and above, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

April 15, 2026

FG-90G-DAT-R16-20260415

FortiGate 40F Series

Highlights

Leader in the Gartner® Magic Quadrant™ for Hybrid Mesh Firewall

Unparalleled performance enabled by Fortinet's patented ASIC and the AI-enriched FortiOS operating system

Enterprise-grade protection with FortiGuard AI-Powered Security Services

Simplified operations with centralized management for networking and security, automated workflows, deep analytics, and self-healing

Inclusive SD-WAN and network controller in every FortiGate appliance at no extra cost

Rich portfolio for any business budget and need

Converged Next-Generation Firewall and SD-WAN

The FortiGate 40F series integrates firewalling, SD-WAN, network controller, and security in one appliance, making them perfect for building secure networks at distributed enterprise sites and transforming WAN architecture at any scale.

The 40F series runs on FortiOS, a converged networking and security platform with secure AI controls and quantum-safe protection. This single OS approach enables businesses to gain benefits of operational efficiency and unified protection from the seamless integration of Fortinet solutions within a hybrid mesh firewall architecture.

As a cornerstone of the Fortinet Security Fabric platform, the FortiGate NGFW works seamlessly with FortiGuard AI-Powered Security Services to deliver coordinated, automated, end-to-end threat protection in real time.

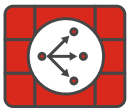
The 40F family is built on the patented SD-WAN-based ASIC, which delivers unmatched performance over traditional CPUs with lower cost and reduced power consumption. This application-specific design and embedded multi-core processor further accelerate the convergence of networking and security functions in the 40F family to optimize secure connections and deliver a robust user experience at branch locations.

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

Use Cases

Perimeter Protection

- Protect networks from malicious traffic, guard against file-based threats, block web-based attacks, and secure applications and data with natively integrated FortiGuard AI-Powered Security Services
- Inspect and control incoming and outgoing traffic based on defined security policies
- Perform real-time SSL inspection (including TLS 1.3) with full visibility into users, devices, and applications across the attack surface
- Accelerate performance, protection, and energy efficiency with Fortinet's patented SPU with converged security and networking technologies



Secure SD-WAN

- FortiGate enables best-of-breed WAN edge with integrated SD-WAN, WAN optimization, security, and unified management from a single FortiOS operating system
- FortiGate, built on a patented SD-WAN-based ASIC, delivers faster application identification to avoid delays in accessing applications and accelerates overlay performance regardless of location
- Enhances hybrid working with a comprehensive SASE solution by integrating cloud-delivered SD-WAN with security service edge (SSE)
- Achieves operational efficiencies at any scale through automation, deep analytics, and self-healing

Secure Branch

- The Fortinet Security Fabric platform enables FortiGate NGFWs to automatically discover and secure IoT devices for faster branch onboarding
- Fully integrated with FortiSwitch secure Ethernet switches and FortiAP access points, FortiGate easily extends security to WAN, LAN, and WLAN at branch offices for unified protection and reliable connectivity
- FortiGate and Fortinet products work seamlessly with FortiManager to centralize visibility and simplify management across locations for IT teams
- FortiGate HA support ensures continuous network protection and minimizes downtime in the event of hardware failures or network disruptions

Available in

Appliance

Virtual

Hosted

Cloud

Container

FortiOS Everywhere

FortiOS, Fortinet's Real-Time Quantum-Safe Network Security Operating System

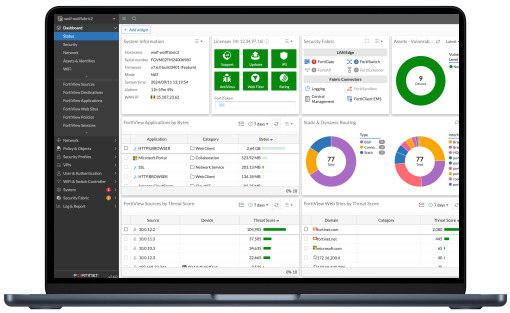
FortiOS is Fortinet's natively AI-powered and quantum-safe operating system (OS) that powers the Fortinet Security Fabric platform, enabling enforcement of security policies and holistic visibility across the entire attack surface. It provides a unified framework for securing networks across on-premises, cloud, hybrid environments, and the convergence of IT, OT, and IoT.

By converging networking and security functions into a single operating system, organizations can manage network and security more effectively to detect, investigate, and respond to incidents faster. This unified architecture simplifies operations, eliminates security silos, and allows organizations to scale securely without multiple tools or management complexity.

FortiOS also incorporates AI-driven capabilities that enhance threat detection, automate network activity analysis, and deliver more precise remediation guidance. Together, FortiGate firewalls and FortiOS provide intelligent, adaptive protection that reduces complexity, improves operational efficiency, and strengthens security across modern hybrid environments.

Learn more about what's new in FortiOS. https://www.fortinet.com/products/fortigate/fortios

Intuitive easy to use view into the network and endpoint vulnerabilities



Comprehensive view of network performance, security, and system status

FortiGuard AI-Powered Security Services

FortiGuard AI-Powered Security Services is part of Fortinet's layered defense and tightly integrated into our FortiGate NGFWs and other products. Powered by real-time AI enhanced threat intelligence from FortiGuard Labs, these services protect organizations against modern attack vectors and threats, including zero days and evasive, sophisticated AI-powered attacks.

Network and file security

Network and file security services protect against network and file-based threats. Consists of intrusion prevention system (IPS) which uses AI/ML models for deep packet/SSL inspection, detecting and blocking malicious content, uncovers hidden command-and-control activity, and applies virtual patches for newly discovered vulnerabilities. Application control improves security compliance and provides real-time visibility into applications and usage including generative AI (GenAI) applications.

Web/DNS security

Web/DNS security services protect against DNS-based attacks, malicious URLs (including those in emails), and botnet communications. DNS filtering blocks the full spectrum of DNS-based attacks while URL filtering uses a database of millions of URLs to identify and block malicious links. Meanwhile, IP reputation and anti-botnet services guard against botnet activity and DDoS attacks.

SaaS and data security

SaaS and data security services cover key security needs for application use and data protection. This service includes data loss/leakage prevention in files, GenAI applications and Images via OCR (optical character recognition). This ensures visibility, management, and protection (blocking exfiltration) of data in motion across networks, clouds, and users. The inline CASB service, secures SaaS applications in use, providing broad visibility and granular control over SaaS access, usage, and data.

Zero-day threat prevention

Zero-day threat prevention is achieved through AI-powered inline malware prevention to analyze file content to identify and block unknown and zero-day malware in real time, delivering sub-second protection across all NGFWs. Integrated into FortiGate NGFWs, the service provides comprehensive defense by blocking unknown threats, streamlining incident response, and reducing security overhead.

Attack surface visibility and compliance

The FortiGuard Attack Surface Security Service provides continuous, compliance-ready monitoring of your Fortinet Security Fabric infrastructure. It calculates your overall security posture rating by scoring controls against vulnerabilities, misconfigurations, and sub-optimal settings, while offering specific remediation guidelines for devices found out of configuration. It maintains continuous compliance with PCI DSS, CIS Controls, and Fortinet security best practices.

OT security

With over 2400 virtual patches, 1600+ OT applications, and 3500+ protocol rules, integrated OT security capabilities detect threats targeting OT infrastructure, perform vulnerability correlation, apply virtual patching, and utilize industry-specific protocol decoders for robust defense of OT environments and devices.

Unified Management for Optimal Security and Efficiency

Whether you are a small business or a large enterprise, Fortinet provides centralized control, visibility, and automation for your security infrastructure.

FortiManager: AI-powered, automation-driven, enterprise-class centralized management at scale

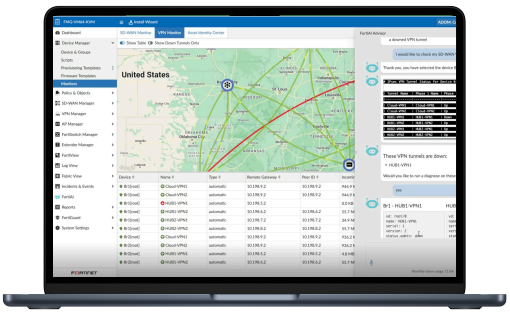
FortiManager, powered by FortiAI-Assist, provides centralized, single-pane management for the Fortinet Security Fabric, unifying configuration, policy, and responses across thousands of devices. It converges networking and security management, enabling consistent policy enforcement across SD-WAN, ZTNA, SASE, and branch environments while delivering real-time visibility and automated network operations.

FortiAI-Assist helps with Day 0–1 provisioning and Day N troubleshooting and maintenance. AI agents collaborating via a unified Model Context Protocol (MCP) framework automates goal-driven tasks toward a self-healing operation.

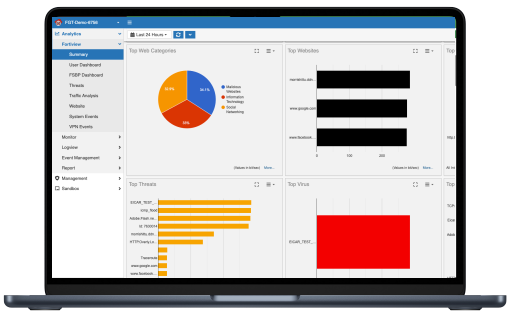
FortiManager integrates with FortiSOC for contextual insights and fabric-wise response. It also supports ecosystem integrations, and open APIs for extended automation. ADOM-based administration and FortiManager clusters enables resilient control across distributed networks.

FortiGate Cloud: Simplified management for small and mid-size businesses

FortiGate Cloud is a SaaS service offering simplified management, security analytics, and reporting for Fortinet FortiGate NGFWs to help you more efficiently manage your devices and reduce cyber risk. It simplifies the initial deployment, setup, and ongoing management of FortiGates and downstream connected devices such as FortiAP, FortiSwitch, and FortiExtender, with zero-touch provisioning. It provides real-time and historical visibility into traffic analytics and security threats to reduce risks and improve security posture. View various threats, web traffic, and system events stored in the cloud for up to a year, with predefined reports to meet compliance and deliver actionable insights.



GenAI in FortiManager helps manage networks effortlessly—generate configuration and policy scripts, troubleshoot issues, and execute recommended actions.



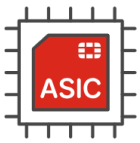
FortiGate Cloud provides intuitive management and analytics solution with end-to-end visibility, logging and reporting for SMB.

FortiConverter Service

Migration to FortiGate NGFW made easy

The FortiConverter Service provides hassle-free migration to help organizations transition quickly and easily from a wide range of legacy firewalls to FortiGate NGFWs. 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.

Fortinet ASICs: Unrivaled Security, Unprecedented Performance



Powered by the only purpose-built SPU

Traditional firewalls cannot protect against today's content and connection-based threats because they rely on off-the-shelf general-purpose central processing units (CPUs), leaving a dangerous security gap. Fortinet's custom SPUs deliver the power you need to radically increase speed, scale, and efficiency while greatly improving user experience and reducing footprint and power requirements. Fortinet's SPUs deliver up to 520 Gbps of protected throughput to detect emerging threats and block malicious content while ensuring your network security solution does not become a performance bottleneck.

Fortinet ASICs are designed to be energy-efficient, leading to lower power consumption and improved TCO. They deliver industry-leading throughput, handle more traffic and perform security inspections faster, reduce latency for quicker packet processing and minimize network delays.

Fortinet SPUs are designed with integrated security functions like zero trust, SSL, IPS, and VXLAN to name but a few, dramatically improving the performance of these functions that competitors traditionally implement in software.

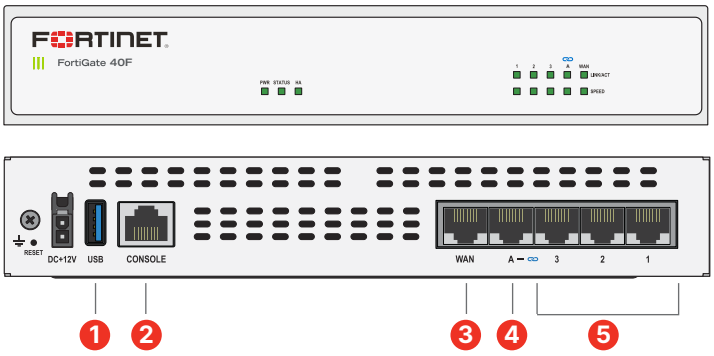
Secure SD-WAN ASIC SP4

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

Hardware

FortiGate 40F Series

SoC4 DESKTOP

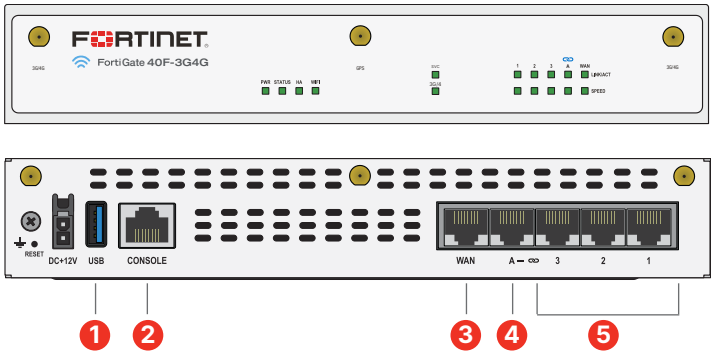


Interfaces

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

FortiGate 40F-3G4G

SoC4 DESKTOP 3G4G/LTE a/b/g/n/ac-W2



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

Access layer security

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

Compact and reliable form factor

Designed for small environments, the FortiGate can be on a desktop or wall-mounted. It is small, lightweight, yet highly reliable with superior meantime between failures, minimizing the chance of network disruption.

Specifications

	FORTIGATE 40F	FORTIGATE 40F-3G4G
Interfaces and Modules		
Hardware Accelerated GE RJ45 WAN / DMZ Ports	1	1
Hardware Accelerated GE RJ45 Internal Ports	3	3
Hardware Accelerated GE RJ45 FortiLink Ports (Default)	1	1
Hardware Accelerated GE RJ45 PoE/+ Ports	0	0
Cellular Modem	—	3G4G LTE
Wireless Interface	0	0
Antenna Ports (SMA)	0	3
USB Ports	1	1
Console Port (RJ45)	1	1
SIM Slots (Nano SIM)	0	2
Onboard Storage	0	0
Included Transceivers	0	0
Trusted Platform Module (TPM)	—	—
Bluetooth Low Energy (BLE)	—	—
Signed Firmware Hardware Switch	—	—
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	2000	
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[6]	490 Mbps	
Concurrent SSL-VPN Users[6] (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.

[6] SSL VPN not supported on FortiOS 7.6.0 and above.

Specifications

	FORTIGATE 40F	FORTIGATE 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	15.8 W / 18.6 W
Heat Dissipation	52.55 BTU/h	63.5 BTU/h
Operating Environment and Certifications		
Operating Temperature	32°F to 104°F (0°C to 40°C)	
Storage Temperature	-31°F to 158°F (-35°C to 70°C)	
Humidity	10% to 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	N/A
Maximum Wi-Fi Speeds	N/A	N/A
Maximum Tx Power	N/A	N/A
Antenna Gain	N/A	N/A
3G4G Modem		
Maximum Tx Power	N/A	20 dBm
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

EPD
INTERNATIONAL EPD SYSTEM

Third-party verified Environmental Product Declaration

The FortiGate 40F is EPD compliant with ISO 14025 Type III (externally verified), ensuring data accuracy and full transparency on the product environmental impacts throughout its life cycle. For more information please visit https://www.environdec.com/library/epd21558

Subscriptions

Service Category	Service Offering	A-la-carte	Bundles			
			Enterprise Protection	Unified Threat Protection	Advanced Threat Protection	SD-WAN
FortiGuard Security Services	IPS — IPS, Malicious/Botnet URLs	•	•	•	•	
	Anti-Malware Protection (AMP)—AV, Botnet Domains, Mobile Malware, Virus Outbreak Protection, Content Disarm and Reconstruct[1], AI-based Heurestic AV, FortiGate Cloud Sandbox	•	•	•	•	
	URL, DNS and Video Filtering — URL, DNS and Video[1] Filtering, Malicious Certificate	•	•	•		
	Anti-Spam		•	•		
	AI-based Inline Malware Prevention	•	•			
	Data Loss Prevention (DLP) [2]	•	•			
	Attack Surface Security — IoT Device Detection, IoT Vulnerability Correlation and Virtual Patching, Security Rating, Outbreak Check		•			•
	OT Security—OT Device Detection, OT Vulnerability Correlation and Virtual Patching, OT Application Control and IPS [2]	•				
	Application Control		----------included with FortiCare Subscription----------			
	Inline CASB[1]		----------included with FortiCare Subscription----------			
SD-WAN and SASE Services	SD-WAN SLA Database					•
	SD-WAN Underlay and Application Monitoring Service					•
	SD-WAN Overlay Orchestration Service					•
	SD-WAN Connector for FortiSASE Secure Private Access					•
	FortiSASE Starter Kit for n* Users[3]					•
	FortiGate Cloud One Year Cloud-based Log Retention					•
	FortiTelemetry Cloud					•
NOC and SOC Services	FortiConverter Service for One Time Configuration Conversion	•	•			
	Managed FortiGate Service—Available 24×7, with Fortinet NOC Experts Performing Device Setup, Network, And Policy Change Management	•				
	FortiGate Cloud—Management, Analysis, and One Year Log Retention	•				
	FortiManager Cloud	•				
	FortiAnalyzer Cloud	•				
	FortiGuard SOCaaS—24×7 Cloud-Based Managed Log Monitoring, Incident Triage, and SOC Escalation Service	•				
Hardware and Software Support	FortiCare Essentials	Desktop models only				
	FortiCare Premium	•	•	•	•	•
	FortiCare Elite	•				
Base Services	Device/OS Detection, GeoIPs, Trusted CA Certificates, Internet Services and Botnet IPs, DDNS (v4/v6), Local Protection, PSIRT Check, Anti-Phishing		----------included with FortiCare Subscription----------			

1. Not available for FortiGate/FortiWiFi 40F, 60E, 60F, 80E, and 90E series from 7.4.4 onwards. Not available for FortiGate/FortiWiFi 30G and 50G series in any OS build.
2. Full features available when running FortiOS 7.4.1.
3. Only supported on FortiGate models from the 100F onwards (F-series and all later series).
See the FortiSASE Ordering Guide for supported models and corresponding user license allocations.

FortiGuard AI-Powered Security Bundles for FortiGate

FortiGuard AI-Powered Security Bundles provide a comprehensive and meticulously curated selection of security services to combat known, unknown, zero-day, and emerging AI-based threats. These services are designed to prevent malicious content from breaching your defenses, protect against web-based threats, secure devices throughout IT/OT/IoT environments, and ensure the safety of applications, users, and data. All bundles include FortiCare Premium Services featuring 24×7×365 availability, one-hour response for critical issues, and next-business-day response for noncritical matters.

FortiCare Services

Fortinet prioritizes customer success through FortiCare Services, optimizing the Fortinet Security Fabric solution. Our comprehensive life-cycle services include Design, Deploy, Operate, Optimize, and Evolve. The FortiCare Elite, one of the service offerings, provides heightened SLAs and swift issue resolution with a dedicated support team. This advanced support option includes an extended end-of-engineering support of 18 months, providing flexibility and access to the intuitive FortiCare Elite portal for a unified view of device and security health, streamlining operational efficiency and maximizing Fortinet deployment performance.

Ordering Information

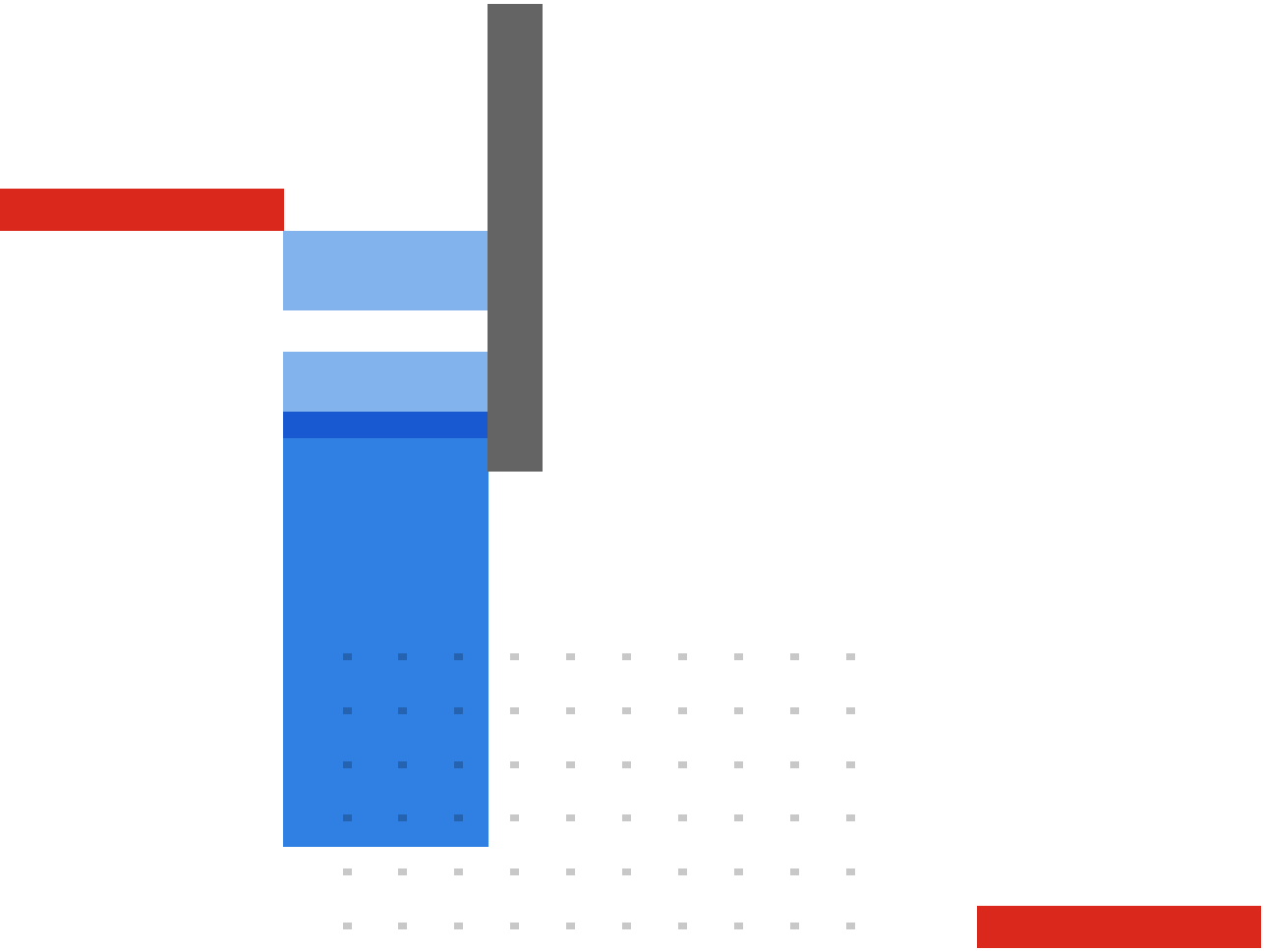
Product	SKU	Description
FortiGate 40F	FG-40F	5x GE RJ45 ports (including 4x Internal Ports, 1x WAN Ports).
FortiGate 40F	FG-40F-HA	5 x GE RJ45 ports (including, 1 x WAN Port, 4 x Internal Ports). FG-XX-HA SKUs must to be bought in pairs and entitle HA pair to leverage single service contracts.
FortiGate 40F-3G4G	FG-40F-3G4G	5x GE RJ45 ports (Including 1x WAN port, 4x Switch ports) with Embedded 3G/4G/LTE wireless wan module, external SMA WWAN antennas included.
FortiGate 40F-3G4G	FG-40F-3G4G-HA	5 x GE RJ45 ports (including 1 x WAN Port, 4 x Internal Ports) with Embedded 3G/4G/LTE wireless wan module, 3 external SMA WWAN antennas included. FG-XX-HA SKUs must to be bought in pairs and entitle HA pair to leverage single service contracts.
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-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-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

Visit https://www.fortinet.com/resources/ordering-guides for related ordering guides.

Fortinet Corporate Social Responsibility 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

Copyright © 2026 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's SVP Legal and above, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

April 21, 2026

FG-40F-DAT-R48-20260421