

Processo: 100000430

DE: GTEC

Para: COLIC

Assunto: Licitação Eletrônica 430/2026 – Análise Técnica de Diligências – Empresa: LIGGA TELECOMUNICAÇÕES

Prezado Pregoeiro,

Em análise à diligencia técnica apresentada pela empresa LIGGA TELECOMUNICAÇÕES S.A. verificamos os itens exigidos, conforme Edital e Termo de Referência:

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.

intermédio de seu representante legal, Sr. Camilo José Gasparetto, portador do RG nº 9.898.144-6/SSPPR e do CPF nº 007.474.119-56, **apresenta** proposta de preços conforme abaixo:

ID	TIPO	BANDA DE DADOS	QUANTIDADE	valor unitário mensal	valor total mensal	valor total 36 meses
1	MPLS FIBRA ÓPTICA	100 Mbps	5	290,00	R\$ 1.450,00	R\$ 52.200,00
2	MPLS FIBRA ÓPTICA	20 Mbps	6	157,00	R\$ 1.256,00	R\$ 45.216,00
3	MPLS FIBRA ÓPTICA	200 Mbps	1	340,55	R\$ 340,55	R\$ 12.547,00
4	MPLS FIBRA ÓPTICA	50 Mbps	5	219,00	R\$ 1.095,00	R\$ 39.420,00
5	MPLS FIBRA ÓPTICA	10 Mbps	21	78,00	R\$ 1.638,00	R\$ 58.968,00
6	MPLS FIBRA ÓPTICA	500 Mbps	3	425,00	R\$ 1.275,00	R\$ 45.900,00
7	MPLS FIBRA ÓPTICA	1000 Mbps	3	585,65	R\$ 1.756,95	R\$ 63.250,20
8	WI-FI ou SATELITE ou 5G	100 Mbps	8	150,00	R\$ 1.200,00	R\$ 43.200,00
9	RADIO ou SATELITE ou 5G	30 Mbps	11	150,00	R\$ 1.650,00	R\$ 58.400,00
10	RADIO ou SATELITE ou 5G	1000 Mbps	4	150,00	R\$ 600,00	R\$ 21.600,00
11	RADIO ou SATELITE ou 5G	50 Mbps	10	150,00	R\$ 1.500,00	R\$ 54.000,00
12	locação de equipamento SDWAN + SERVIÇO	n/a	55	R\$ 749,65	R\$ 41.230,48	R\$ 1.484.297,10
TOTAIS DO CONTRATO					R\$ 54.999,98	R\$ 1.979.999,10

- Valor Mensal: R\$ 54.999,98 (cinquenta e quatro mil, novecentos e noventa e nove reais e noventa e oito centavos).
- Valor 36 meses: R\$ 1.979.999,10 (Um milhão, novecentos e setenta e nove mil, novecentos e noventa e nove reais e dez centavos).
- Validade da proposta: 60 (sessenta) dias, contados da data de sua apresentação.
- A redundância será através da tecnologia 5G.

Nas taxas e nos preços unitários propostos para os serviços estão incluídas todas e quaisquer despesas que venham a incidir sobre os mesmos, representando a compensação integral para todas as operações, transportes, materiais, perdas, mão-de-obra, equipamentos e eventuais

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

intermédio de seu representante legal, Sr. Camilo José Gasparetto, portador do RG nº 9.898.144-6/SSPPR e do CPF nº 007.474.119-56, **apresenta** proposta de preços conforme abaixo:

ID	TIPO	BANDA DE DADOS	QUANTIDADE	valor unitário mensal	valor total mensal	valor total 36 meses
1	MPLS FIBRA ÓPTICA	100 Mbps	5	290,00	R\$ 1.450,00	R\$ 52.200,00
2	MPLS FIBRA ÓPTICA	20 Mbps	8	157,00	R\$ 1.256,00	R\$ 45.216,00
3	MPLS FIBRA ÓPTICA	200 Mbps	1	348,55	R\$ 348,55	R\$ 12.547,80
4	MPLS FIBRA ÓPTICA	50 Mbps	5	219,00	R\$ 1.095,00	R\$ 39.420,00
5	MPLS FIBRA ÓPTICA	10 Mbps	21	78,00	R\$ 1.638,00	R\$ 58.968,00
6	MPLS FIBRA ÓPTICA	500 Mbps	3	425,00	R\$ 1.275,00	R\$ 45.900,00
7	MPLS FIBRA ÓPTICA	1000 Mbps	3	585,65	R\$ 1.756,95	R\$ 63.250,20
8	RADIO ou SATELITE ou 5G	100 Mbps	8	150,00	R\$ 1.200,00	R\$ 43.200,00
9	RADIO ou SATELITE ou 5G	30 Mbps	11	150,00	R\$ 1.650,00	R\$ 58.400,00
10	RADIO ou SATELITE ou 5G	1000 Mbps	4	150,00	R\$ 600,00	R\$ 21.600,00
11	RADIO ou SATELITE ou 5G	50 Mbps	10	150,00	R\$ 1.500,00	R\$ 54.000,00
12	locação de equipamento SDWAN + SERVIÇO	n/a	55	R\$ 749,65	R\$ 41.230,48	R\$ 1.484.297,10
TOTAIS DO CONTRATO					R\$ 54.999,98	R\$ 1.979.999,10

- Valor Mensal: R\$ 54.999,98 (cinquenta e quatro mil, novecentos e noventa e nove reais e noventa e oito centavos).
- Valor 36 meses: R\$ 1.979.999,10 (Um milhão, novecentos e setenta e nove mil, novecentos e noventa e nove reais e dez centavos).
- ~~Validade da proposta: 60 (sessenta) dias, contados da data de sua apresentação.~~
- A redundância será através da tecnologia 5G.

Nas taxas e nos preços unitários propostos para os serviços estão incluídas todas e quaisquer despesas que venham a incidir sobre os mesmos, representando a compensação integral para todas as operações, transportes, materiais, perdas, mão-de-obra, equipamentos e eventuais

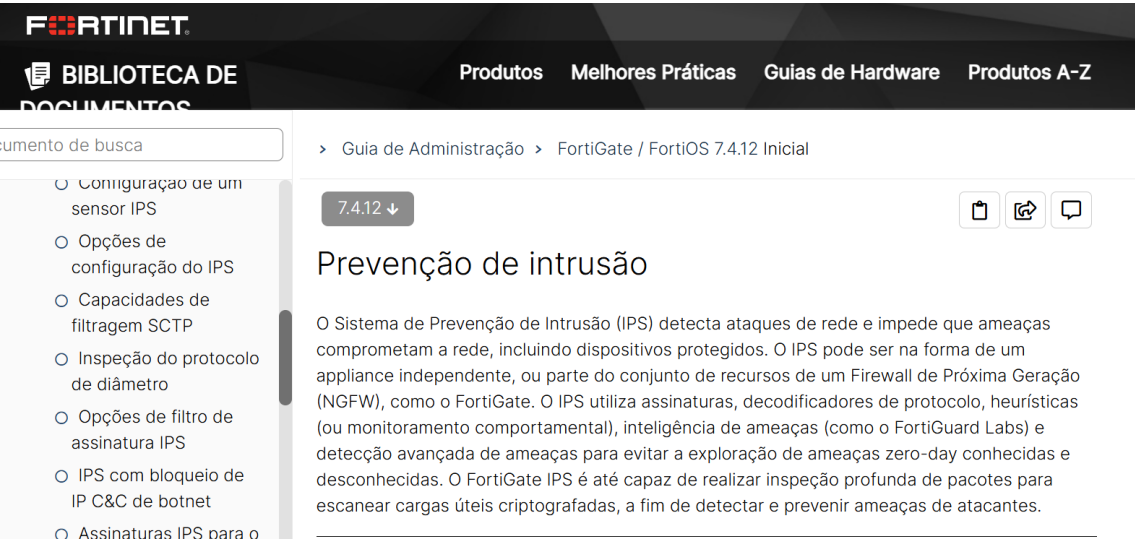
3.5 Todo o hardware e software fornecidos não podem constar, no momento da apresentação da proposta, em listas de end-of-sale, end-of-support, end-ofengineering-support ou end-of-life do fabricante, ou seja, não poderão ter previsão de descontinuidade de fornecimento, suporte ou vida, devendo estar em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

R: Atendido. Os equipamentos propostos, encontram-se ambos, em linha de produção do fabricante.



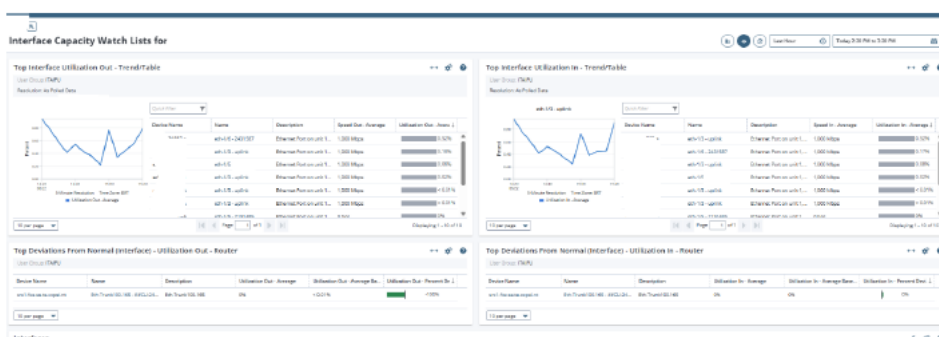
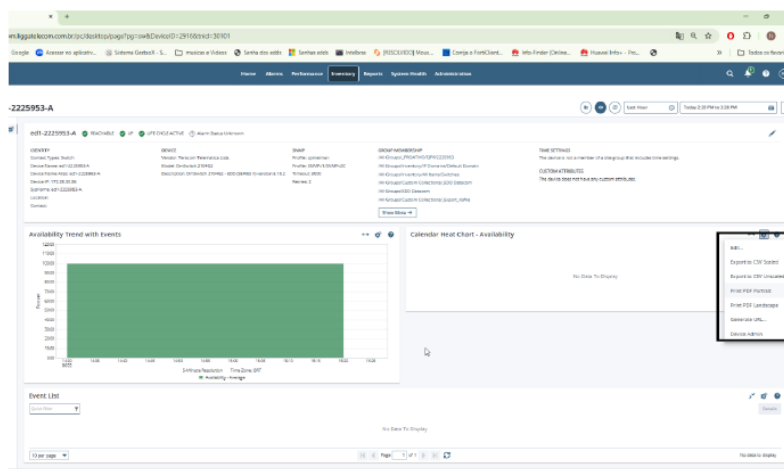
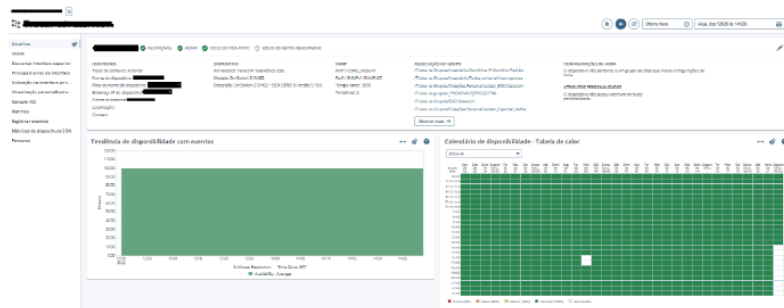
3.8 A solução deverá possuir e permitir que ferramentas de detecção e prevenção de propagação de ataques de agentes maliciosos sejam utilizados.

R: Atendido. A solução sistêmica proposta e suas funcionalidades possuem os recursos necessários através da ferramenta NGFW – Next Generation Firewall.



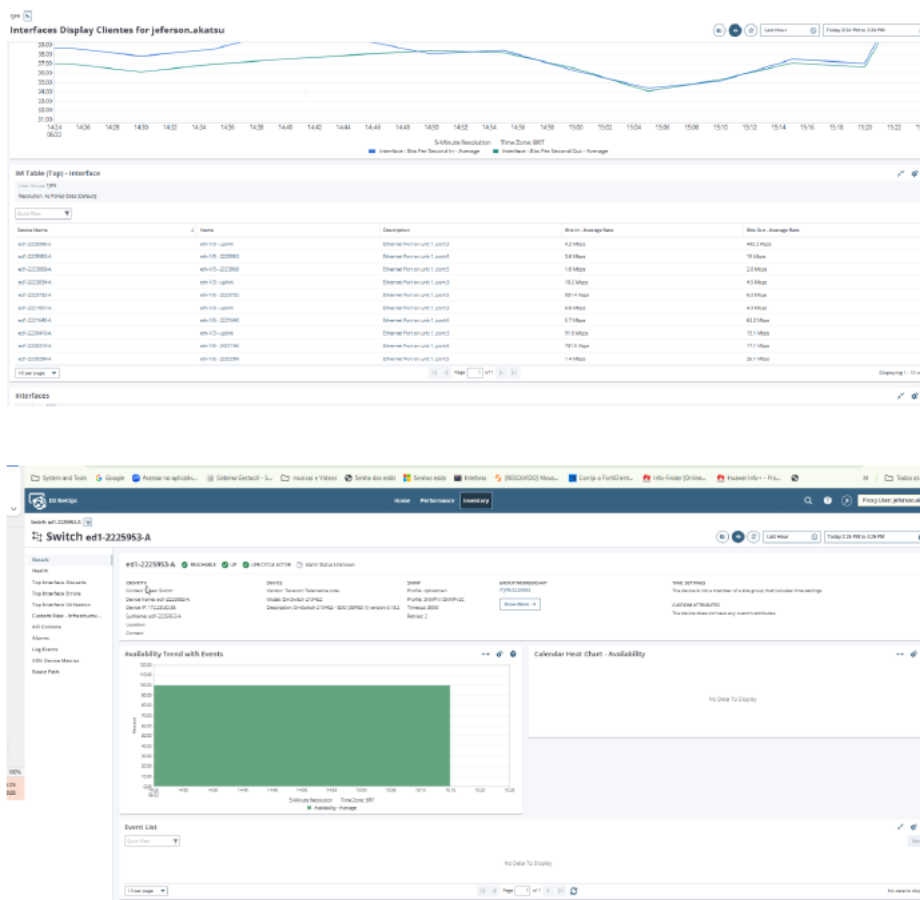
3.10 A CONTRATADA deverá prover solução de gerência de rede que contemple os módulos de gerencia de falhas, desempenho, disponibilidade, capacity planning, relatórios, tickets, e de nível de serviço.

R: Atendido.



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: Atendido.



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: Atendido. Ambos os modelos possuem funcionalidades SDWAN.

GERÊNCIA DE TECNOLOGIA DA INFORMAÇÃO

FortiGate 90G Series

Data Sheet



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 security and network services

FortiGate 40F Series

Data Sheet



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



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 da proposta tecnica

	02 Gbps	04
	03 Gbps	02
	04 Gbps	01
	12 Gbps	01
	40 Gbps.	01

1. Enlace de comunicação utilizando MULTIPROTOCOL LABEL SWITCHING(MPLS);

2. Configuração de VPNs (Virtual Private Network) distintas, distribuídas conforme definição da contratante;

3. Classificação de marcação de diferentes níveis de trafego, (QoS), aplicando classes de serviço distintas (dados prioritários e dados não prioritários);

4. Total de Circuitos: 4.826 (quatro mil, oitocentos e vinte e sei)

Serviço	Banda	Circuitos ativos
Comunicação de dados entre locais distintos, denominados Rede Privada – tipo Acesso MPLS (Multiprotocol Label Switching Ponto a Ponto) / Rede de Alta Velocidade (RAV L2):	20 Mbps	04
	30 Mbps	02
	40 Mbps	02

GERÊNCIA DE TECNOLOGIA DA INFORMAÇÃO

Ficha: 2331 - Dotação: 4.126.11.2499 - COORDENAR E MANTER AS ATIVIDADES OPERACIONAIS DA

Elemento: 3390395800 - SERVIÇOS DE TELECOMUNICAÇÕES

Grupo Fonte: 1 - Do Exercício

Fonte: 00000 - RECURSOS ORDINÁRIOS (LIVRES)

Observação:

Justificativa: Considerando a necessidade de continuidade dos serviços de telefonia móvel corporativa utilizados pela administração municipal, e que o processo licitatório definitivo para contratação do serviço encontra-se em tramitação, conforme Solicitação de Contratação nº 355/2025, justifica-se a contratação temporária, conforme proposta apresentada. O serviço inclui planos corporativos de voz e dados, gestão centralizada de contas, atendimento prioritário, portabilidade de números, fornecimento de SIM Cards e suporte técnico. Tais recursos são essenciais à manutenção das atividades administrativas e operacionais das secretarias. A interrupção do serviço causaria prejuízos à comunicação institucional e às ações de campo. Assim, a contratação possui caráter emergencial e temporário, até a conclusão do novo certame, garantindo continuidade e eficiência administrativa.

Empenho: 23187/2025

Emitido em: 29/10/2025

Fornecedor: LIGGA TELECOMUNICACOES S.A.

Cnpj/Cpf: 4368865000166

Endereço: AV VICENTE MACHADO

Cidade: CURITIBA

Fone: 4333751280

CEP: 8042001

e-felipe.marques@liggavc.com.br

IE/RG: 0

Item	Cod.	Produto	Cidade	Unid.	VI Unit	VI Total
1	554725	SERVIÇO DE TELEFONIA MOVEL PESSOAL COM ABRANGENCIA DE	4	UNIDADE	11.404,500	45.618,000
SERVIÇO DE TELEFONIA MOVEL PESSOAL SISTEMA DIGITAL POS-PAGO COM ABRANGENCIA DE COBERTURA NO MUNICIPIO DE SAO JOSE DOS PINHAIS E REGIAO METROPOLITANA DE CURITIBA PR - Assinatura mensal:400Assinatura Tarifa Zero Local:400Assinatura Tarifa Zero Nacional:1VC1 móvel móvel (mesma operadora)433.420VC1 móvel móvel (outra operadora)437.420Móvel - Fone:18.000SM5 4.000Pacote de Dados de 40 MB(velocidade: 16 Kbps e 256 kbps) Dados MM:50MBx131Dado 3G: 16 GB(velocidade: 1Mbps)460Pacote de Dados limitado para Smartphone(velocidade até 300 Kbps)476VC2 mesma operadora4250VC2 outra operadora4150VC2 fixo4150VC3 Mesma operadora4250VC3 outra operadora4150VC3 Fixo4150VC3459						

TOTAL DA SOLICITAÇÃO:

10.455.18,00

3.2.4.2 Suporte a VPN Camada 2 (Pseudowire) para conexões legadas específicas (Núcleo CELEPAR), permitindo a integração com os ambientes legados;

R: Atendido pg 155 da proposta técnica.

02 Gbps	04
03 Gbps	02
04 Gbps	01
12 Gbps	01
40 Gbps.	01

1. Enlace de comunicação utilizando MULTIPROTOCOL LABEL SWITCHING(MPLS);

2. Configuração de VPNs (Virtual Private Network) distintas, distribuídas conforme definição da contratante;

3. Classificação de marcação de diferentes níveis de tráfego, (QoS), aplicando classes de serviço distintas (dados prioritários e dados não prioritários);

4. Total de Circuitos: 4.826 (quatro mil, oitocentos e vinte e sei)

Serviço	Banda	Circuitos ativos
Comunicação de dados entre locais distintos, denominados Rede Privada – tipo Acesso MPLS (Multiprotocol Label Switching Ponto a Ponto) / Rede de Alta Velocidade (RAV L2):	20 Mbps	04
	30 Mbps	02
	40 Mbps	02

3.2.4.3 Compatibilidade nativa com protocolos de roteamento dinâmico (OSPF/BGP) utilizados pela CELEPAR.

R: Atendido. Evidenciado na documentação técnica que “O FortiGate suporta RIP, OSPF, BGP e IS-IS, que são interoperáveis com outros fornecedores.”.



3- Equipamentos

3.4.1 Todos os equipamentos fornecidos deverão ser homologados pela ANATEL.

R: Atendido. Indicados os números de homologação dos equipamentos.

Modelos Certificados						
Modelo	Nome Comercial	TipoProduto	Número de Homolo...	Certificado de Conformidade Técnica	Data do Certifi... de	Data de Validac
FG-90G		Equipamento de Rede de Dados	038302408867	BRC-23.2290.01	26/02/2024	2027-02-26 00:00
FG-91G		Equipamento de Rede de Dados	038302408867	BRC-23.2290.01	26/02/2024	2027-02-26 00:00

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.

4 R: Atendido. Ambos os modelos possuem funcionalidades SDWAN.

FortiGate 90G Series

Data Sheet

5



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 security and network services

FortiGate 40F Series

Data Sheet

6



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

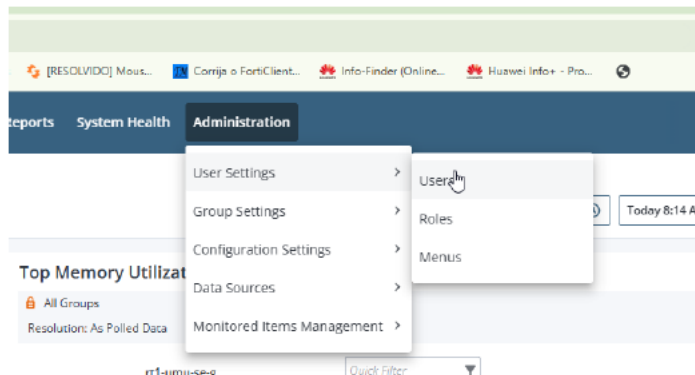
GERÊNCIA DE TECNOLOGIA DA INFORMAÇÃO



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: Atendido.



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.

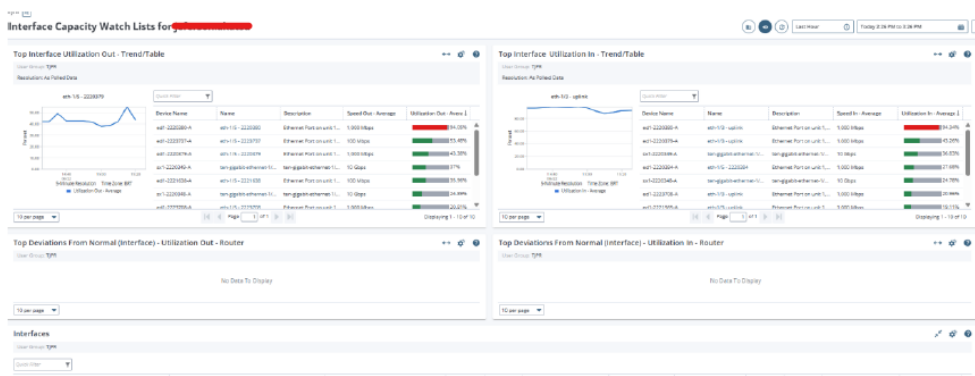
R: Atendido.

[illegible]

R: Atendido



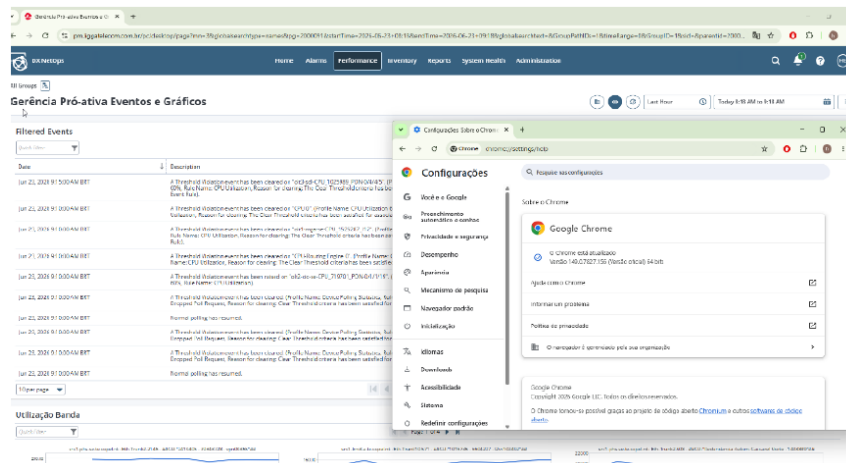
Devices						
Devices						
Device Group: VPN						
Data Filter:						
Name	Type	Address	Description	Connect Status	Current Admin State	Life Cycle State
vpn-022008a-6	Switch	172.28.181.10	EndUser 275422-820-288933 (v-version: 5.18.2)		Up	Active Switch
vpn-022008a-6	Switch	172.28.181.12	EndUser 275422-820-288933 (v-version: 5.18.2)		Up	Active Switch
vpn-022008a-6	Switch	172.28.181.7	EndUser 275422-820-288933 (v-version: 5.18.2)		Up	Active Switch
vpn-022008a-6	Switch	172.28.181.8	EndUser 275422-820-288933 (v-version: 5.18.2)		Up	Active Switch
vpn-022008a-6	Switch	172.28.181.9	EndUser 275422-820-288933 (v-version: 5.18.2)		Up	Active Switch
vpn-022008a-6	Switch	172.28.181.6	EndUser 275422-820-288933 (v-version: 5.18.2)		Up	Active Switch
vpn-022008a-6	Switch	172.28.181.4	EndUser 275422-820-288933 (v-version: 5.18.2)		Up	Active Switch
vpn-022008a-6	Switch	172.28.181.209	EndUser 275422-820-288933 (v-version: 5.18.2)		Up	Active Switch
vpn-022008a-6	Switch	172.28.181.9	EndUser 275422-820-288933 (v-version: 5.18.2)		Up	Active Switch
vpn-022008a-6	Switch	172.28.181.6	EndUser 275422-820-288933 (v-version: 5.18.2)		Up	Active Switch



GERÊNCIA DE TECNOLOGIA DA INFORMAÇÃO

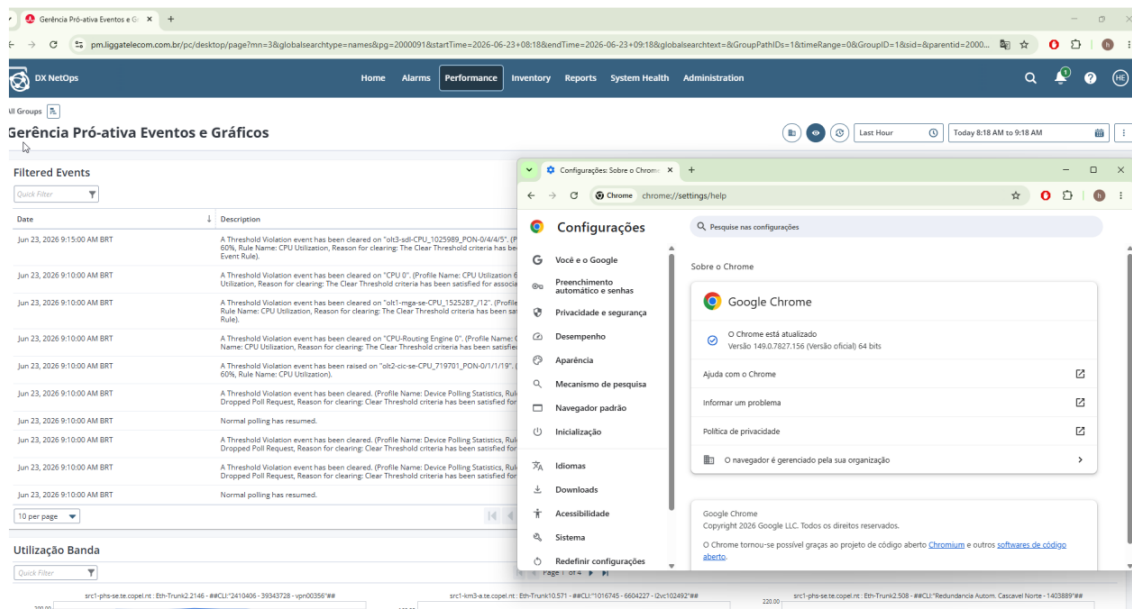
3.11.6 A solução de gerência de redes deverá ser 100% web, sem necessidade de instalação de clients específicos, portanto, não serão aceitas soluções que requeiram a instalação de agentes ou plug-ins nos desktops das estações da CONTRATANTE.

R: Atendido.



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.

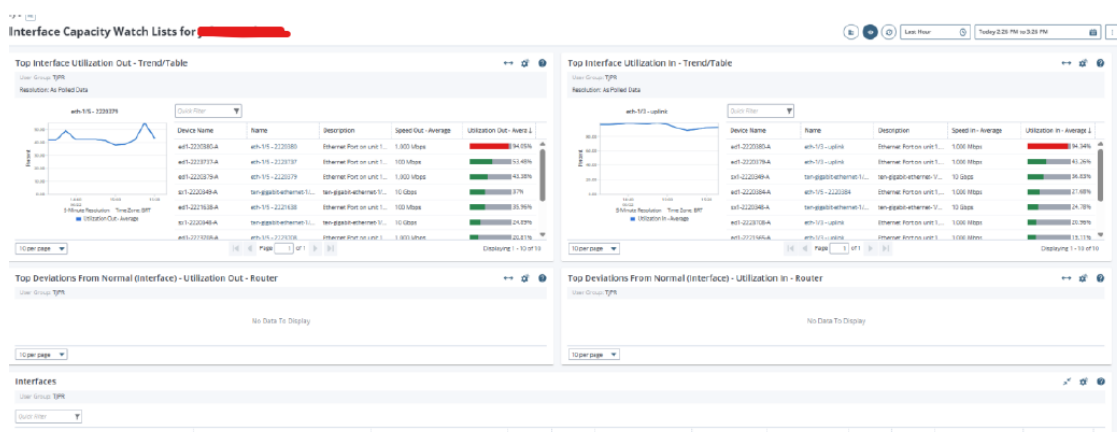
R: Atendido.



GERÊNCIA DE TECNOLOGIA DA INFORMAÇÃO

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

R: Atendido.



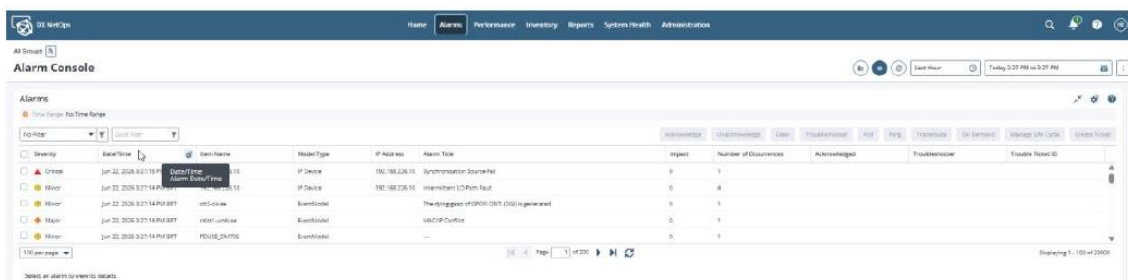
3.11.11A solução de gerência de rede deverá fornecer, através do portal, visualização de informações on-line da rede, que deverá apresentar no mínimo os seguintes itens para cada um dos elementos monitorados:

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: Atendido, através de afirmação do proponente, sendo pré-requisito a instalação física dos circuitos de rede.

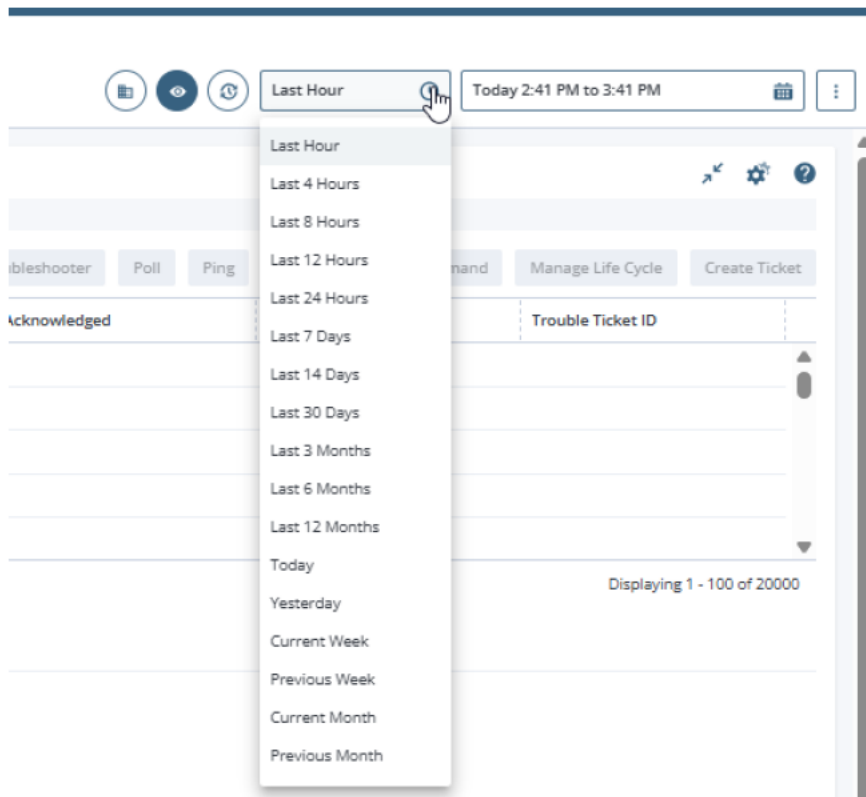
3.11.11.2 Alarmes de eventos ocorridos na rede com informações de data, hora e duração da ocorrência e identificação dos recursos gerenciados;

R: Atendido.



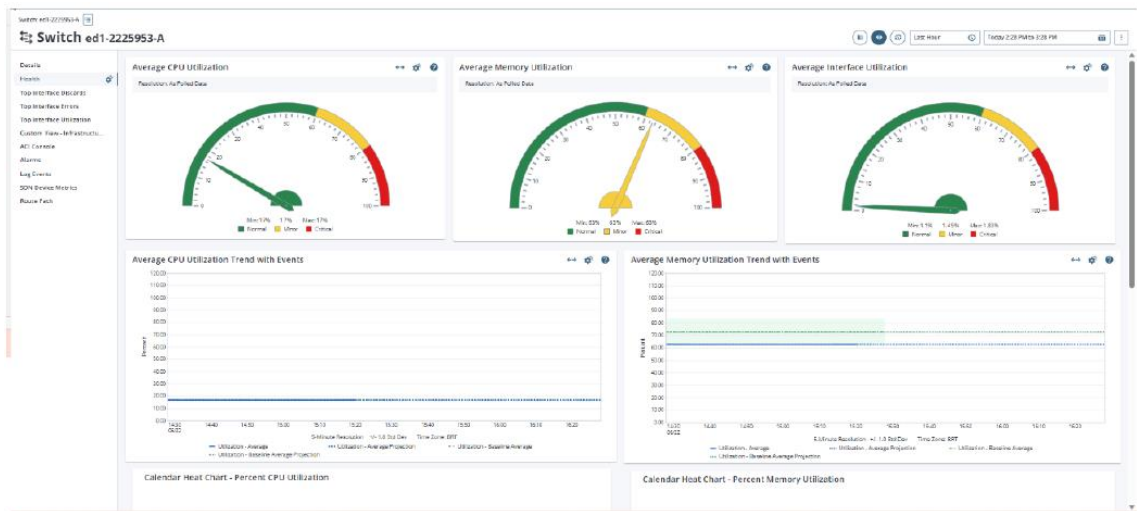
3.11.11.3 Consumo de banda dos enlaces separados por dia e mês;

R: Atendido.



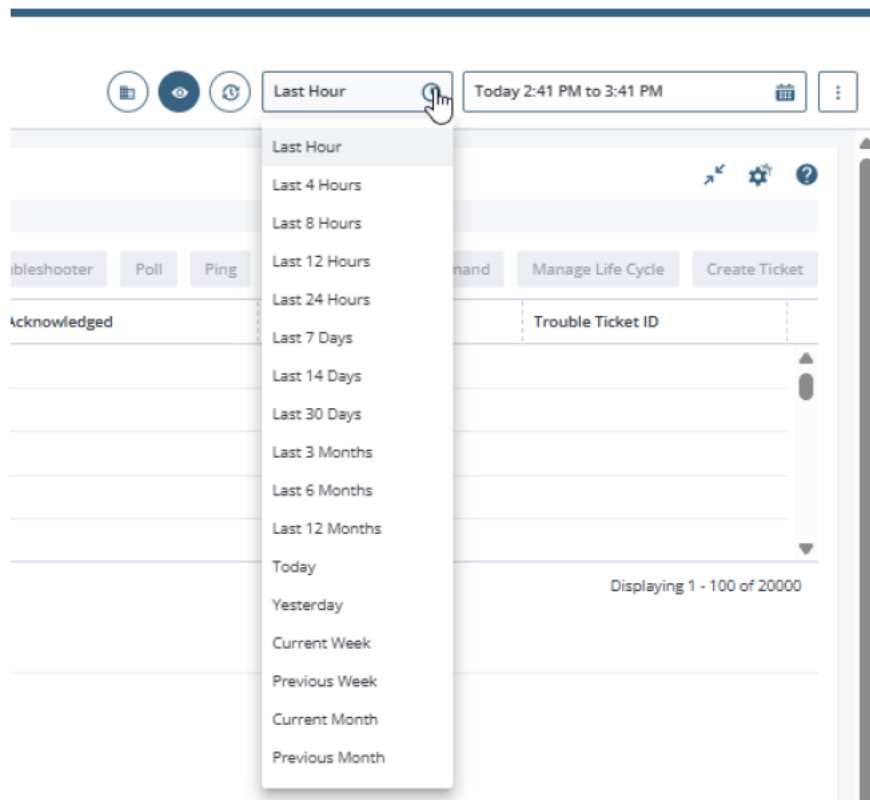
3.11.11.4 Ocupação de memória e CPU dos equipamentos CPE;

R: Atendido.



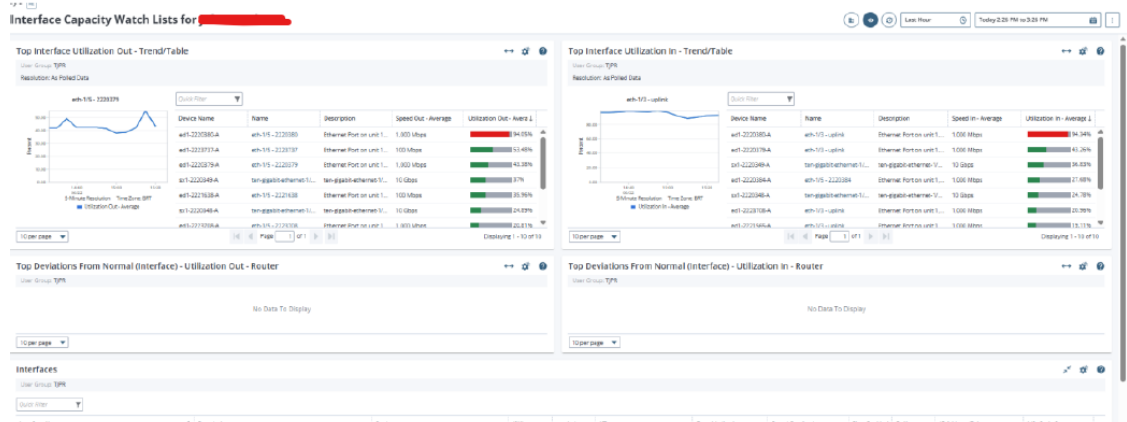
3.11.11.5 Latência dos enlaces separados por dia e mês, em Milissegundos (mS);

R: Atendido.



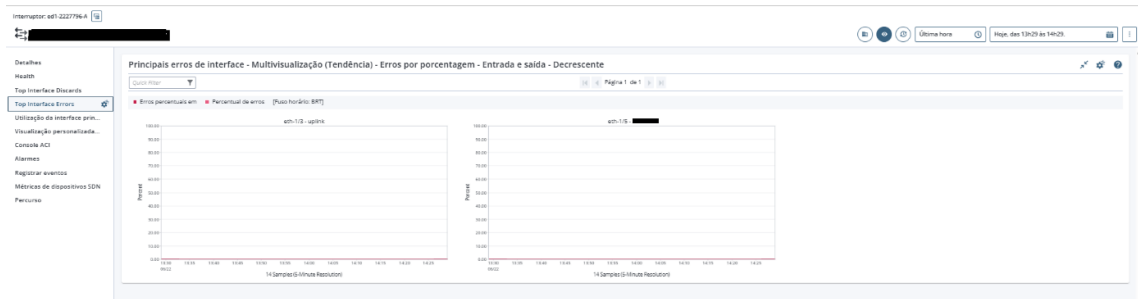
3.11.11.6 Perda de pacotes no sentido IN e OUT em %;

R: Atendido.



3.11.11.7 Taxa de erros em erros por segundo;

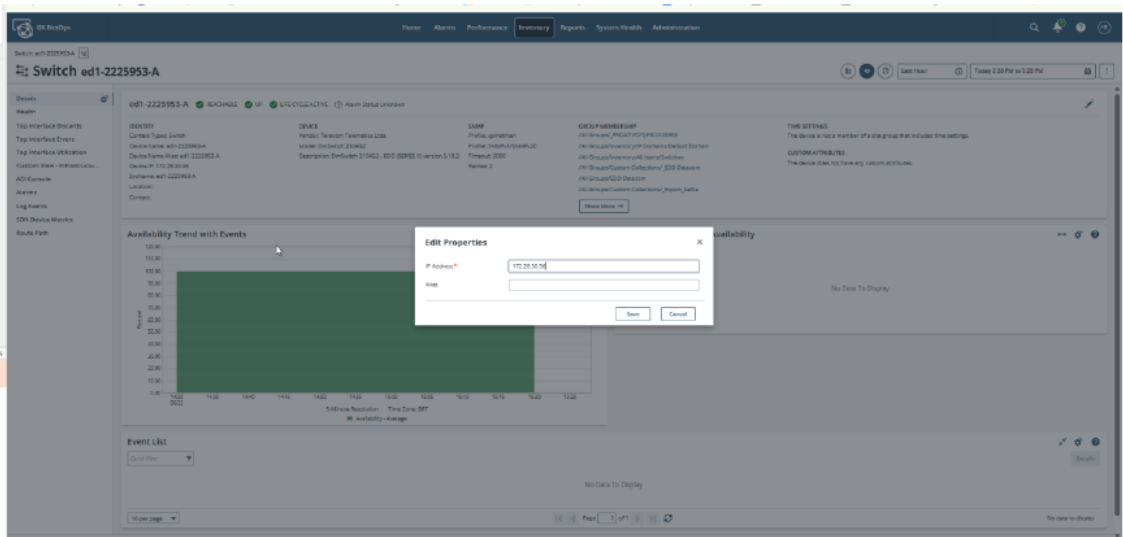
R: Atendido.



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

R: Atendido.

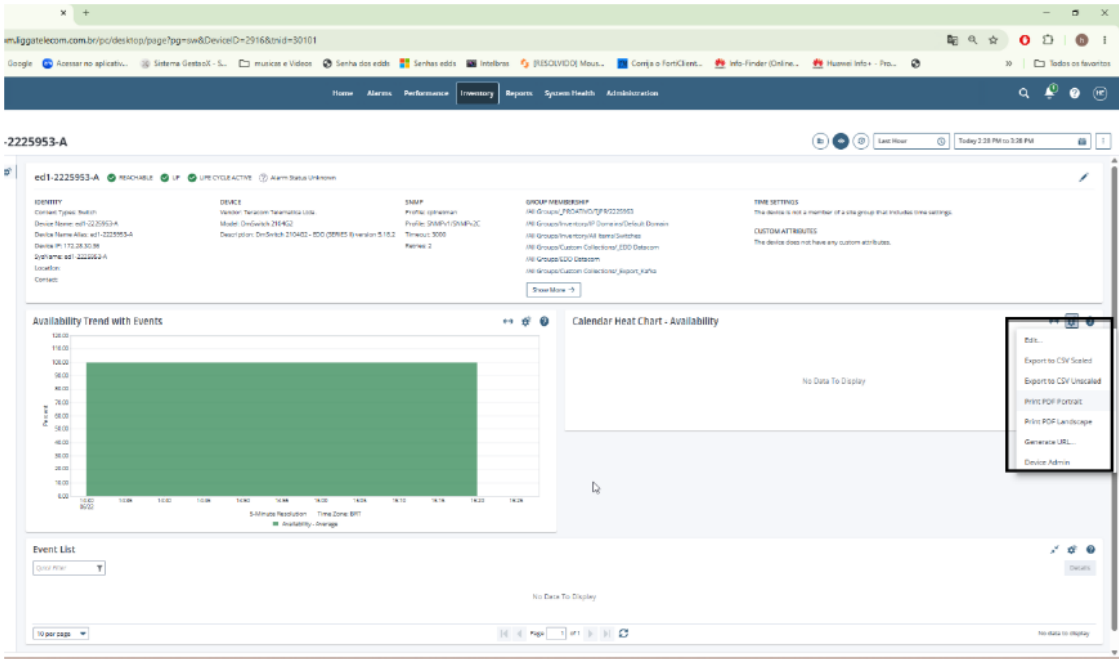
GERÊNCIA DE TECNOLOGIA DA INFORMAÇÃO



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

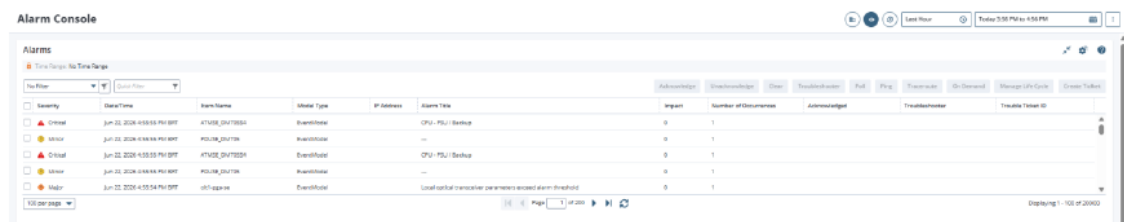
3.11.14.4 Dashboards relacionando falhas, desempenho, capacity e disponibilidade.

R: Atendido.



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.

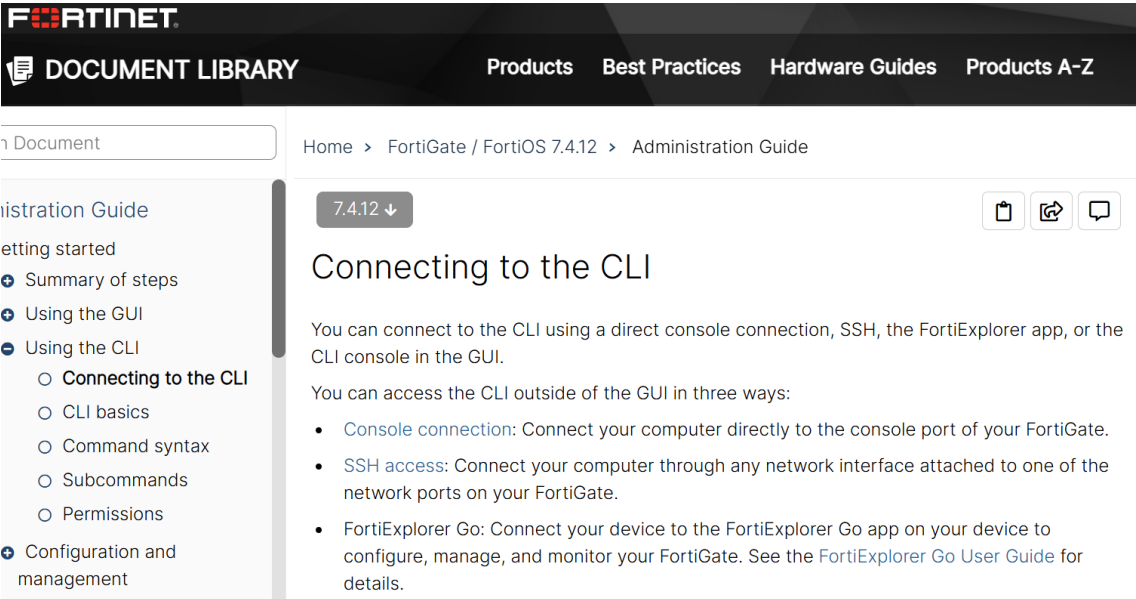


5- SD-WAN

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: Atendido.



FORTINET

DOCUMENT LIBRARY

Products

Best Practices

Hardware Guides

Products A-Z

h Document

Administration Guide

Getting started

- Summary of steps
- Using the GUI
 - Connecting using a web browser
 - Menus
 - Tables
 - Entering values
 - GUI-based global search
 - Loading artifacts from

Home > FortiGate / FortiOS 7.4.12 > Administration Guide

7.4.12 ↓

Connecting using a web browser

In order to connect to the GUI using a web browser, an interface must be configured to allow administrative access over HTTPS or over both HTTPS and HTTP. By default, an interface has already been set up that allows HTTPS access with the IP address 192.168.1.99.

Browse to <https://192.168.1.99> and enter your username and password. If you have not changed the admin account's password, use the default user name, **admin**, and leave the password field blank.

The GUI will now display in your browser, and you will be required to provide a password for the administrator account.

FORTINET

DOCUMENT LIBRARY

Products

Best Practices

Hardware Guides

Products A-Z

h Document

Configuration scripts

Workspace mode

Custom languages

RAID

FortiGate encryption algorithm cipher suites

Conserve mode

Using APIs

Configuration backups and reset

Fortinet Security Fabric

Log and Report

WAN optimization

VPN

Home > FortiGate / FortiOS 7.4.12 > Administration Guide

7.4.12 ↓

Using APIs

Administrators can use API calls to a FortiGate to:

- Retrieve, create, update, and delete configuration settings
- Retrieve system logs and statistics
- Perform basic administrative actions, such as a reboot or shut down through programming scripts.

Token-based authentication

FortiGate supports only token-based authentication for API calls. Token-based authentication requires the administrator to generate a token, which is then included in each API request for authentication. A token is automatically generated when a new API administrator is created in

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

R: Atendido.

Fortinet

DOCUMENT LIBRARY

Products

Best Practices

Hardware Guides

Products A-Z

Document

Basic configuration

+

DHCP options

DHCP addressing mode on an interface

VCI pattern matching for DHCP assignment

DHCP shared subnet

Multiple DHCP relay servers

DHCP smart relay on interfaces with a secondary IP

FortiGate DHCP works with DDNS to allow EQDN connectivity to

Home > FortiGate / FortiOS 7.4.12 > Administration Guide

7.4.12

Clipboard

Share

Comment

DHCP servers and relays

A DHCP server dynamically assigns IP addresses to hosts on the network connected to the interface. The host computers must be configured to obtain their IP addresses using DHCP. You can configure one or more DHCP servers on any FortiGate interface.

A DHCP server can be in server or relay mode. In server mode, you can define up to ten address ranges to assign addresses from, and options such as the default gateway, DNS server, lease time, and other advanced settings. In relay mode, the interface forwards DHCP requests from DHCP clients to an external DHCP server and returns the responses to the DHCP clients. The DHCP server must have appropriate routing so that its response packets to the DHCP clients arrive at the unit.

If an interface is connected to multiple networks through routers, you can add a DHCP server for each network. The IP range of each DHCP server must match the network address range. The

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: Atendido.

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

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

3.12.7 Deverá permitir o funcionamento em modo transparente tipo “bridge”.

R: Atendido.

Avenida Ayrton Senna da Silva, 161 | D. Pedro II | Paranaguá/PR | CEP 83203-800 | 41 3420.1143 / 41 3420.1114

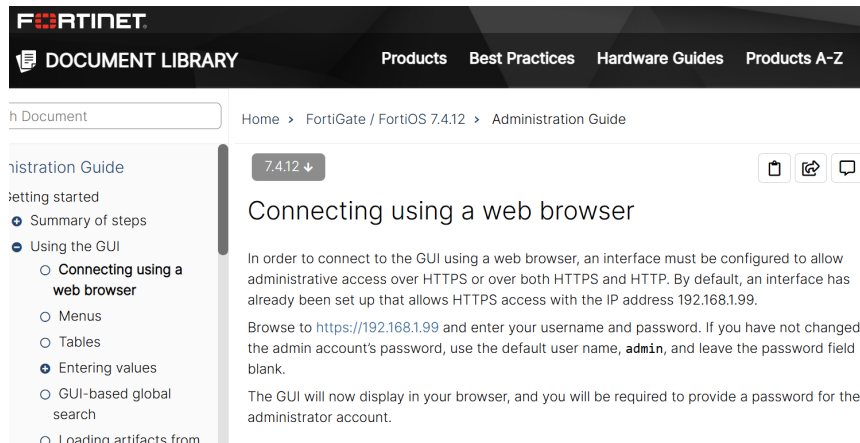
www.portosdoparana.pr.gov.br

COMUNICAÇÃO INTERNA 4746/2026. Assinatura Simples realizada por: Vinícius Rodrigo Teixeira (XXX.978.469-XX) em 07/07/2026 17:29. Inserido ao documento 2.196.631 por: Vinícius Rodrigo Teixeira em: 07/07/2026 17:29. Demais assinaturas na última folha. A autenticidade deste documento pode ser validada no endereço: https://www.eprotocolo.pr.gov.br/spiweb/validarDocumento com o código: 932d25c1054bed9d3951746e2da9a3ec



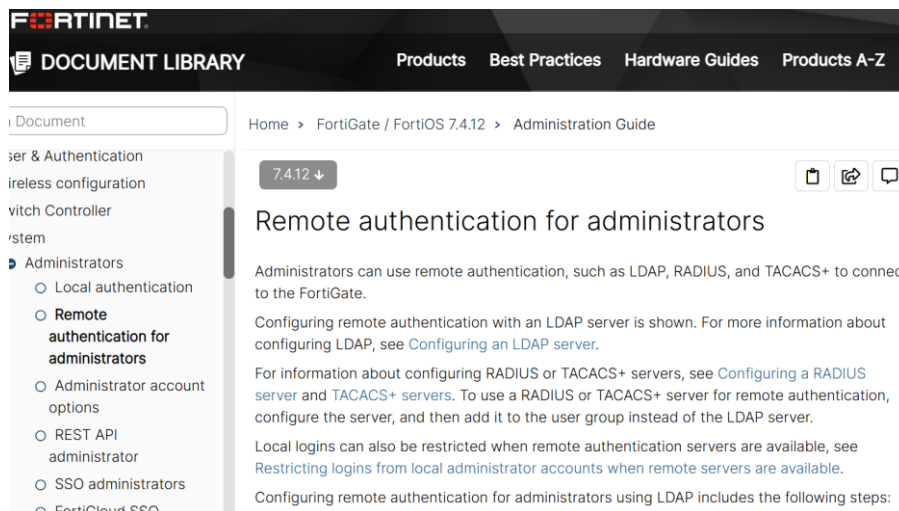
3.12.8 Deverá possuir conexão entre estação de gerência e appliance criptografada, tanto em interface gráfica, quanto CLI (Linha de Comando).

R: Atendido.



3.12.9 Deverá permitir autenticação de usuários em base local, servidor LDAP, RADIUS e TACACS+.

R: Atendido.



3.12.10 Deve 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 SD-WAN.

R: Atendido.



3.12.12 Deverá 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: Atendido.



3.12.13A configuração de alta disponibilidade deve possibilitar a monitoração de falha de link e falha de fornecimento de energia nos equipamentos CPE.

R: Atendido.



6- SOLUÇÃO SD-WAN

3.13.2 Deverá ser capaz de agregar minimamente 03 links em uma interface virtual;

R: Atendido.



3.13.3 Deverá ser capaz de adicionar e equilibrar, no mínimo, 06 interfaces de dados, entre links e tuneis VPN.

R: Atendido.



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: Atendido.

GERÊNCIA DE TECNOLOGIA DA INFORMAÇÃO

BIBLIOTECA DE DOCUMENTOS

ento de busca

SLA de desempenho

Membros e zonas da SD-WAN

SLA de desempenho

- Visão geral do SLA de desempenho
- Monitor de saúde do link
- SLA de desempenho de monitoramento
- Medição passiva de saúde de WAN
- Medição passiva de exames de saúde por serviço e aplicação de internet
- Cálculo médio de pontuação de opinião

ProdutosMelhores PráticasGuias de HardwareProdutos A-Z

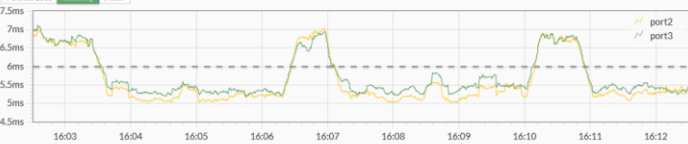
> Guia de Administração > FortiGate / FortiOS 7.4.12 Inicial

Investigue quaisquer problemas prioritários como perda de pacotes, aumento de jitter para garantir que sua rede não sofra desempenho degradado ou uma queda de energia.

Você pode monitorar o status da qualidade do link dos membros da interface SD-WAN indo para *Network > SD-WAN* e selecionando a aba de *SLAS de Desempenho*.

SD-WAN ZonesSD-WAN RulesPerformance SLAs

Packet LossLatencyJitter



Create NewEditDeleteSearch

Name	Detect Server	Packet Loss	Latency	Jitter	Failure Threshold	Recovery Threshold
Default_Office_365	https://www.office.com/				5	10
PINGSLA	8.8.8.8 9.9.9.9	port2: 0.00% port3: 0.00%	port2: 5.38ms port3: 5.34ms	port2: 0.84ms port3: 0.55ms	5	5

Os gráficos ao vivo mostram a perda de pacotes, latência ou jitter para o exame de saúde

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: Atendido.

BIBLIOTECA DE DOCUMENTOS

ento de busca

SLA de desempenho

Regras SD-WAN

- Visão geral das regras SD-WAN
- Regra implícita
- Estratégia automática
- Estratégia manual
- Estratégia de melhor qualidade
- Estratégia de menor custo (SLA)
- Estratégia de balanceamento de carga
- Modelagem de tráfego SD-WAN e QoS
- Endereços dinâmicos

ProdutosMelhores PráticasGuias de HardwareProdutos A-Z

> Guia de Administração > FortiGate / FortiOS 7.4.12 Inicial

Estratégia de melhor qualidade

Ao usar o modo de *Melhor Qualidade*, a SD-WAN escolherá o melhor link para encaminhar o tráfego comparando o *fator custo do link*. Um fator de custo de link é uma métrica específica de link(s) participante (como latência, perda de pacotes, etc.) avaliada em relação a um alvo que você define (como um servidor de verificação de saúde), por exemplo, a latência de WAN1 e WAN2 em relação ao seu datacenter. Abaixo está uma lista dos fatores de custo dos links disponíveis para você:

GUI	CLI	Descrição
Latência	Latência	Selecione um link baseado na latência.
Jitter	tremor	Selecione um link baseado no jitter.
Perda de Pacotes	Perda de pacotes	Selecione um link baseado na perda de pacotes.
A jusante	Largura de	Selecione um link com base na largura de banda

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.

Avenida Ayrton Senna da Silva, 161 | D. Pedro II | Paranaguá/PR | CEP 83203-800 | 41 3420.1143 / 41 3420.1114

www.portosdoparana.pr.gov.br

COMUNICAÇÃO INTERNA 4746/2026. Assinatura Simples realizada por: Vinícius Rodrigo Teixeira (XXX.978.469-XX) em 07/07/2026 17:29. Inserido ao documento 2.196.631 por: Vinícius Rodrigo Teixeira em: 07/07/2026 17:29. Demais assinaturas na última folha. A autenticidade deste documento pode ser validada no endereço: https://www.eprotocolo.pr.gov.br/spiweb/validarDocumento com o código: 932d25c1054bed9d3951746e2da9a3ec

R: Atendido

BIBLIOTECA DE DOCUMENTOS

ento de busca

SD-WAN Quick Start

Membros e zonas da SD-WAN

SLA de desempenho

Regras SD-WAN

- Visão geral das regras SD-WAN
- Regra implícita**
- Estratégia automática
- Estratégia manual
- Estratégia de melhor qualidade
- Estratégia de menor custo (SLA)
- Estratégia de balanceamento de carga

ProdutosMelhores PráticasGuias de HardwareProdutos A-Z

> Guia de Administração > FortiGate / FortiOS 7.4.12 Inicial

Regra implícita

As regras SD-WAN definem opções específicas de roteamento de políticas para direcionar tráfego a um membro SD-WAN. Quando nenhuma regra SD-WAN explícita é definida, ou se nenhuma das regras for correspondida, então a regra implícita padrão é usada.

Em uma configuração SD-WAN, a rota padrão geralmente aponta para a interface SD-WAN, de modo que o gateway de cada membro ativo é adicionado à rota padrão da tabela de roteamento. O FortiOS utiliza o multipath de custo igual (ECMP) para equilibrar o tráfego entre as interfaces. Um dos cinco algoritmos de balanceamento de carga pode ser selecionado:

IP de origem (source-ip-based)	O tráfego é dividido igualmente entre as interfaces, incluindo a interface SD-WAN. Sessões que começam no mesmo endereço IP de origem usam o mesmo caminho. Essa é a seleção padrão.
Sessões (weight-based)	A carga de trabalho é distribuída com base no número de sessões conectadas pela interface. O peso que você atribui a cada interface é usado para calcular a

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:

3.13.7.1 Manual: Deve permitir que as interfaces tenham as propriedades atribuídas manualmente.

R: Atendido.

FORTINET

BIBLIOTECA DE DOCUMENTOS

ento de busca

WAN

SLA de desempenho

Regras SD-WAN

- Visão geral das regras SD-WAN
- Regra implícita
- Estratégia automática
- Estratégia manual**
- Estratégia de melhor qualidade
- Estratégia de menor custo (SLA)
- Estratégia de balanceamento de carga

ProdutosMelhores PráticasGuias de HardwareProdutos A-Z

> Guia de Administração > FortiGate / FortiOS 7.4.12 Inicial

7.4.12 ↓

Estratégia manual

No modo manual, não são realizados exames de saúde. Como resultado, a tomada de decisão se assemelha mais à lógica do que à inteligência. As regras manuais SD-WAN são semelhantes às rotas regulares baseadas em políticas, mas possuem recursos adicionais de roteamento consciente da aplicação e roteamento por etiquetas BGP. Uma regra manual de estratégia é composta pelas seguintes partes:

- Definindo as interfaces a serem usadas
- Ordenar as interfaces com base na preferência, ou balanceamento de carga do tráfego a partir das interfaces especificadas usando um algoritmo de balanceamento de carga

A estratégia de maximizar largura de banda () usada antes do FortiOS 7.4.1 agora é conhecida como estratégia de balanceamento de carga. Essa

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

Avenida Ayrton Senna da Silva, 161 | D. Pedro II | Paranaguá/PR | CEP 83203-800 | 41 3420.1143 / 41 3420.1114

www.portosdoparana.pr.gov.br

COMUNICAÇÃO INTERNA 4746/2026. Assinatura Simples realizada por: **Vinícius Rodrigo Teixeira (XXX.978.469-XX)** em 07/07/2026 17:29. Inserido ao documento **2.196.631** por: **Vinícius Rodrigo Teixeira** em: 07/07/2026 17:29. Demais assinaturas na última folha. A autenticidade deste documento pode ser validada no endereço: <https://www.eprotocolo.pr.gov.br/spiweb/validarDocumento> com o código: **932d25c1054bed9d3951746e2da9a3ec**

menos um dos seguintes parâmetros com valores customizáveis: Jitter, latência, perda de pacotes ou largura de banda.

R: Atendido.

BIBLIOTECA DE DOCUMENTOS

ProdotosMelhores PráticasGuias de HardwareProdutos A-Z

imento de busca

SLA de desempenho

Regras SD-WAN

- Visão geral das regras SD-WAN
- Regra implícita
- Estratégia automática
- Estratégia manual
- Estratégia de melhor qualidade
- Estratégia de menor custo (SLA)
- Estratégia de balanceamento de carga
- Modelagem de tráfego SD-WAN e QoS
- Endereços dinâmicos

Guia de Administração > FortiGate / FortiOS 7.4.12 Inicial

Estratégia de melhor qualidade

Ao usar o modo de Melhor Qualidade, a SD-WAN escolherá o melhor link para encaminhar o tráfego comparando o fator custo do link. Um fator de custo de link é uma métrica específica de link(s) participante (como latência, perda de pacotes, etc.) avaliada em relação a um alvo que você define (como um servidor de verificação de saúde), por exemplo, a latência de WAN1 e WAN2 em relação ao seu datacenter. Abaixo está uma lista dos fatores de custo dos links disponíveis para você:

GUI	CLI	Descrição
Latência	Latência	Selecione um link baseado na latência.
Jitter	tremor	Selecione um link baseado no jitter.
Perda de Pacotes	Perda de pacotes	Selecione um link baseado na perda de pacotes.
A jusante	Largura de	Selecione um link com base na largura de banda

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: Atendido.

FORTINET

BIBLIOTECA DE DOCUMENTOS

ProdotosMelhores PráticasGuias de HardwareProdutos A-Z

imento de busca

Visão geral das regras SD-WAN

Regra implícita

Estratégia automática

Estratégia manual

Estratégia de melhor qualidade

Estratégia de menor custo (SLA)

Estratégia de balanceamento de carga

Modelagem de tráfego SD-WAN e QoS

Endereços dinâmicos

Guia de Administração > FortiGate / FortiOS 7.4.12 Inicial

7.4.12

Estratégia de menor custo (SLA)

Ao usar o modo de Menor Custo (SLA) (na linha de crédito), SD-WAN escolherá o link de menor custo que satisfaz o SLA para o tráfego encaminhado. O menor custo possível é . Se múltiplos links elegíveis tiverem o mesmo custo, a ordem de preferência de Interface será usada para selecionar um link.slaø

DMZ

192.168.100.0/24

FortiGate

wan1

wan2

ISP 1

Gateway: 172.16.20.2

Internet

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: Atendido.



Fortinet
BIBLIOTECA DE DOCUMENTOS

Produtos Melhores Práticas Guias de Hardware Produtos A-Z

Guia de Administração > FortiGate / FortiOS 7.4.12 Inicial

7.4.12

Estratégia de balanceamento de carga

A estratégia de maximizar largura de banda () usada antes do FortiOS 7.4.1 agora é conhecida como estratégia de balanceamento de carga. Essa estratégia pode ser configurada no modo manual e nas estratégias de menor custo (SLA).

- Quando a estratégia de balanceamento de carga é configurada sob a estratégia de modo manual, alvos de SLA não são usados (veja [Estratégia de balanceamento de carga sem alvos de SLA](#) para um exemplo de configuração).
- Quando a estratégia de balanceamento de carga é configurada sob a estratégia de menor custo (SLA), são usados alvos de SLA (veja [Estratégia de balanceamento de carga com alvos de SLA](#) para um exemplo de configuração).

A funcionalidade da estratégia de balanceamento de carga permanece a

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

R: Atendido.



Fortinet
BIBLIOTECA DE DOCUMENTOS

Produtos Melhores Práticas Guias de Hardware Produtos A-Z

Guia de Administração > FortiGate / FortiOS 7.4.12 Inicial

7.4.12

Use regras SD-WAN para seleção de link WAN com balanceamento de carga

Este exemplo cobre um caso de uso em que um usuário possui múltiplos links WAN e deseja otimizar a seleção e o desempenho dos links WAN, limitando o uso de interfaces mais caras que consomem largura de banda, como 5G ou LTE.

Diagrama de rede:

```
graph LR
    R[Router] --- port1
    R --- wan1
    R --- wan2
    wan1 --- ISP1[ISP1 Gateway: 172.16.200.254]
    wan2 --- ISP2[ISP2 Gateway: 10.1.100.254]
```

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

R: Atendido.

BIBLIOTECA DE DOCUMENTOS

imento de busca

redundante manual de VPN

OSPF com VPN IPsec para redundância de rede

VPN IPsec em um ambiente HA

Distribuição de pacotes e redundância para túneis agregados IPsec

Distribuição de pacotes para túneis agregados de discagem discada IPsec usando ID de localização

Distribuição de

Produtos

Melhores Práticas

Guias de Hardware

Produtos A-Z

> Guia de Administração > FortiGate / FortiOS 7.4.12 Inicial

Distribuição de pacotes e redundância para túneis agregados IPsec

Esta é uma configuração de exemplo de uma VPN IPsec múltipla site-to-site que usa uma interface agregada IPsec para configurar redundância e balanceamento de carga de tráfego. As interfaces do túnel VPN devem ter sido desativadas para serem membros do agregado IPsec.

net-device

Cada FortiGate possui duas interfaces WAN conectadas a diferentes provedores. O OSPF roda sobre o agregado IPsec nessa configuração.

Os algoritmos de balanceamento de carga suportados são: L3, L4, round-robin (padrão), round-robin ponderado e redundante. As quatro primeiras opções permitem que o tráfego seja balanceado em carga, enquanto a última opção (redundante) usa o primeiro túnel que está disponível para todo o tráfego.

O roteamento dinâmico pode rodar na interface agregada, e pode ser uma interface de membro no SD-WAN (não mostrado nesta configuração).

HQ1

172.16.200.1 port1

ISP1

172.16.202.1 port25

HQ2

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: Atendido através da tecnologia ADVPN.

BIBLIOTECA DE DOCUMENTOS

imento de busca

Regras SD-WAN

Roteamento avançado

Overlay de VPN

Descoberta de bordas e gerenciamento de caminhos ADVPN 2.0

ADVPN e caminhos de atalho

Vizinho BGP dinâmico ativo acionado por atalho ADVPN

Monitor SD-WAN em atalhos ADVPN

Tempo de espera para annciar as estratégias

Produtos

Melhores Práticas

Guias de Hardware

Produtos A-Z

> Guia de Administração > FortiGate / FortiOS 7.4.12 Inicial

ADVPN e caminhos de atalho

Este tópico fornece um exemplo de como usar SD-WAN e ADVPN juntos.

ADVPN (Auto Discovery VPN) é uma tecnologia IPsec que permite que os raios de uma VPN hub tradicional estabeleçam túneis diretos e dinâmicos sob demanda entre si, evitando o roteamento pelo dispositivo hub da topologia. A principal vantagem é que oferece capacidades completas de malha para uma topologia padrão de hub-and-spoke. Isso reduz muito o esforço de provisionamento para alcance total de raios-para-raios e baixo atraso, e resolve os problemas de escalabilidade associados a redes VPN totalmente mesh muito grandes.

Se a sede e as filiais de um cliente tiverem duas ou mais conexões de internet, ele pode construir uma rede ADVPN de hub duplo. Combinado com a tecnologia SD-WAN, o cliente pode balancear o tráfego para outros escritórios em múltiplos túneis dinâmicos, controlar tráfego específico usando conexões específicas ou escolher conexões de melhor desempenho dinamicamente.

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: Atendido através da tecnologia FEC (Forward Error Correction).

Avenida Ayrton Senna da Silva, 161 | D. Pedro II | Paranaguá/PR | CEP 83203-800 | 41 3420.1143 / 41 3420.1114

www.portosdoparana.pr.gov.br

COMUNICAÇÃO INTERNA 4746/2026. Assinatura Simples realizada por: **Vinícius Rodrigo Teixeira (XXX.978.469-XX)** em 07/07/2026 17:29. Inserido ao documento **2.196.631** por: **Vinícius Rodrigo Teixeira** em: 07/07/2026 17:29. Demais assinaturas na última folha. A autenticidade deste documento pode ser validada no endereço: <https://www.eprotocolo.pr.gov.br/spiweb/validarDocumento> com o código: **932d25c1054bed9d3951746e2da9a3ec**

Fortinet

BIBLIOTECA DE DOCUMENTOS

Produtos

Melhores Práticas

Guias de Hardware

Produtos A-Z

ento de busca

ativo acionado por atalho ADVPN

Monitor SD-WAN em atalhos ADVPN

Tempo de espera para apoiar as estratégias de serviço SD-WAN

Correção de Erros Adaptativa para Frente

Assistente de túnel de VPN dupla

Pacotes duplicados em outros membros da zona

Pacotes duplicados

> Guia de Administração > FortiGate / FortiOS 7.4.12 Inicial

7.4.12

Correção de Erros Adaptativa para Frente

A Correção de Erros Direta (FEC) é usada para controlar e corrigir erros na transmissão de dados, enviando dados redundantes pela VPN em antecipação a pacotes perdidos ocorrendo durante o trânsito. O mecanismo envia x número de pacotes redundantes para cada y número de pacotes base.

O FEC adaptativo considera as condições do enlace e ajusta dinamicamente a razão de pacotes FEC:

A relação base do FEC e do pacote redundante é ajustada dinamicamente com base nas mudanças nas métricas de SLA da rede definidas nas verificações de saúde do SLA do SD-WAN. Por exemplo, quando não há ou há baixa perda de pacotes na rede, o FEC pode funcionar em um nível redundante baixo, enviando apenas um pacote redundante para cada 10 pacotes base. À medida que a perda de pacotes aumenta, o número de pacotes

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: Atendido.

BIBLIOTECA DE DOCUMENTOS

Produtos

Melhores Práticas

Guias de Hardware

Produtos A-Z

ento de busca

Membros e zonas da SD-WAN

SLA de desempenho

Visão geral do SLA de desempenho

Monitor de saúde do link

SLA de desempenho de monitoramento

Medição passiva de saúde de WAN

Medição passiva de exames de saúde por serviço e aplicação de internet

Cálculo médio de pontuação de opinião

> Guia de Administração > FortiGate / FortiOS 7.4.12 Inicial

Investigue quaisquer problemas prolongados como perda de pacotes, atrasos ou jitter para garantir que sua rede não sofra desempenho degradado ou uma queda de energia.

Você pode monitorar o status da qualidade do link dos membros da interface SD-WAN indo para *Network > SD-WAN* e selecionando a aba de *SLAs de Desempenho*.

SD-WAN Zones

SD-WAN Rules

Performance SLAs

Packet Loss

Latency

Jitter

7.5ms

7ms

6.5ms

6ms

5.5ms

5ms

4.5ms

16:03

16:04

16:05

16:06

16:07

16:08

16:09

16:10

16:11

16:12

port2

port3

Create New

Edit

Delete

Search

Name

Detect Server

Packet Loss

Latency

Jitter

Failure Threshold

Recovery Threshold

Default_Office_365

http://www.office.com/

5

10

PINGSLA

8.8.8.8

9.9.9.9

port2: 0.00%

port2: 5.38ms

port2: 0.84ms

5

5

port3: 0.00%

port3: 5.34ms

port3: 0.55ms

100%

Os gráficos ao vivo mostram a perda de pacotes, latência ou jitter para o exame de saúde

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 experiência do usuário.

R: Atendido.

GERÊNCIA DE TECNOLOGIA DA INFORMAÇÃO

BIBLIOTECA DE DOCUMENTOS Produtos Melhores Práticas Guias de Hardware Produtos A-Z

mento de busca

> Guia de Administração > FortiGate / FortiOS 7.4.12 Inicial

monitoramento de longo prazo de problemas de tráfego em locais remotos, além de relatórios e visualizações no FortiAnalyzer.

Os intervalos de tempo em que o SLA de desempenho falha e os logs de aprovação são gerados podem ser configurados.

Para configurar o intervalo de tempo de geração dos logs de falha e aprovação:

```
config system sdwan
config health-check
edit "PingSLA"
set sla-fail-log-period 30
set sla-pass-log-period 60
next
end
end
```

Para ver o histórico de status do Performance SLA em 10 minutos:

FGDocs # diagnose svs sdwan sla-log PingSLA 1

3.13.14 Deve suportar balanceamento de tráfego por sessão e pacote.

R: Atendido.

BIBLIOTECA DE DOCUMENTOS Produtos Melhores Práticas Guias de Hardware Produtos A-Z

mento de busca

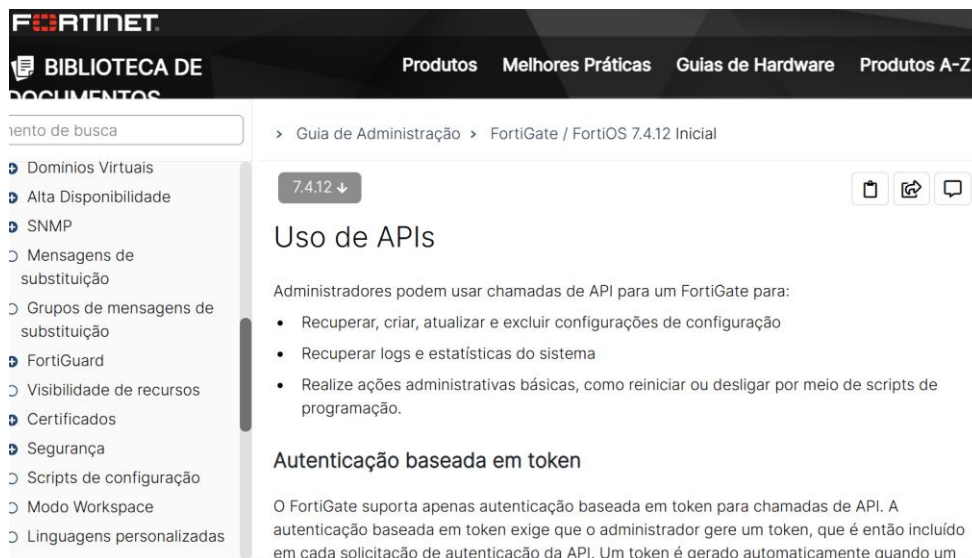
> Guia de Administração > FortiGate / FortiOS 7.4.12 Inicial

Este exemplo mostra quatro métodos para equilibrar igualmente o tráfego entre as duas conexões WAN. Vá para *Network > SD-WAN*, selecione a aba *de Regras SD-WAN* e edite a regra *SD-WAN* para selecionar o método apropriado para suas necessidades.

- IP de origem (comando CLI): source-ip-based**
Selecione essa opção para balancear o tráfego igualmente entre os membros da SD-WAN de acordo com um algoritmo de hash baseado nos endereços IP de origem.
- Sessão (:weight-based)**
Selecione essa opção para equilibrar o tráfego igualmente entre os membros da SD-WAN pela proporção de números de sessão entre seus membros. Use peso 50 para cada um dos 2 membros.
- IP de Origem-Destino (:source-dest-ip-based)**
Selecione essa opção para balancear o tráfego igualmente entre os membros SD-WAN de acordo com um algoritmo de hash baseado nos endereços IP de origem e destino.
- Volume (:measured-volume-based)**
Selecione esta opção para balancear o tráfego igualmente entre os membros SD-WAN de acordo com a razão de largura de banda entre seus membros.

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

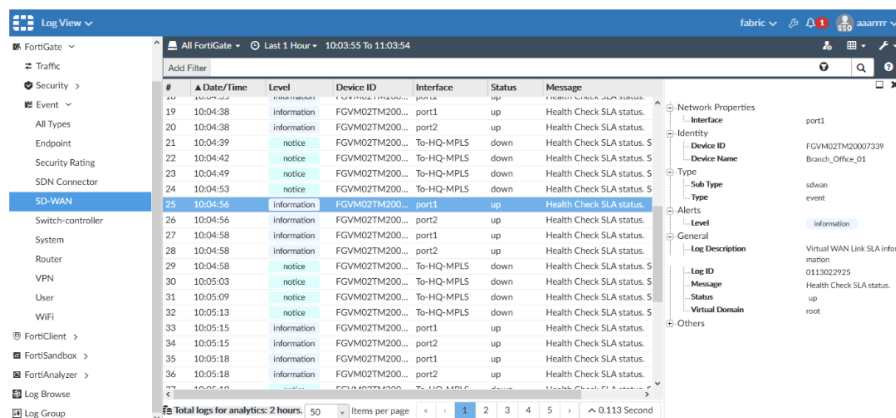
R: Atendido.



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

R: Atendido.

Na interface gráfica do FortiAnalyzer:



7- FUNCIONALIDADE VPN

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

R: atendido.

Fortinet

BIBLIOTECA DE DOCUMENTOS

Produtos

Melhores Práticas

Guias de Hardware

Produtos A-Z

ento de busca

> Guia de Administração > FortiGate / FortiOS 7.4.12 Inicial

7.4.12

Site-to-site VPN

Uma conexão VPN site-to-site permite que filiais usem a Internet para acessar a intranet do escritório principal. Uma VPN site-to-site permite que escritórios em múltiplos locais fixos estabeleçam conexões seguras entre si por meio de uma rede pública, como a Internet.

As seções a seguir fornecem instruções para configurar VPNs site-to-site:

- FortiGate-para-FortiGate
- FortiGate para-terceiros

< Anterior

Próximo >

© 2026 Fortinet, Inc.

Política de Privacidade

Legal

Fortinet

BIBLIOTECA DE DOCUMENTOS

Produtos

Melhores Práticas

Guias de Hardware

Produtos A-Z

ento de busca

> Guia de Administração > FortiGate / FortiOS 7.4.12 Inicial

7.4.12

SSL VPN

A tecnologia de Rede Privada Virtual (VPN) permite que usuários remotos se conectem a redes privadas de computadores para acessar seus recursos de forma segura. Por exemplo, um funcionário que viaja ou trabalha em casa pode usar uma VPN para acessar com segurança a rede do escritório pela internet.

Em vez de fazer login remoto em uma rede privada usando uma conexão de internet não criptografada e não segura, o uso de uma VPN garante que partes não autorizadas não possam acessar a rede do escritório nem interceptar informações que circulem entre o funcionário e o escritório. Outro uso comum de uma VPN é conectar as redes privadas de vários escritórios.

A VPN SSL utiliza o protocolo Secure Socket Layer (SSL) para criar um túnel seguro do navegador web do host para uma aplicação específica (modo web) ou para fornecer um túnel SSL entre o cliente e a rede corporativa (modo túnel). A VPN SSL opera na camada de aplicação

< Anterior

Próximo >

© 2026 Fortinet, Inc.

Política de Privacidade

Legal

3.14.2 Suportar IPsec VPN.

R: Atendido.

Avenida Ayrton Senna da Silva, 161 | D. Pedro II | Paranaguá/PR | CEP 83203-800 | 41 3420.1143 / 41 3420.1114

www.portosdoparana.pr.gov.br

COMUNICAÇÃO INTERNA 4746/2026. Assinatura Simples realizada por: Vinícius Rodrigo Teixeira (XXX.978.469-XX) em 07/07/2026 17:29. Inserido ao documento 2.196.631 por: Vinícius Rodrigo Teixeira em: 07/07/2026 17:29. Demais assinaturas na última folha. A autenticidade deste documento pode ser validada no endereço: https://www.eprotocolo.pr.gov.br/spiweb/validarDocumento com o código: 932d25c1054bed9d3951746e2da9a3ec

GERÊNCIA DE TECNOLOGIA DA INFORMAÇÃO

BIBLIOTECA DE DOCUMENTOS

imento de busca

erfis de Segurança

sec VPN

Configuração geral de VPN

IPsec

Site-to-site VPN

Acesso remoto

VPN agregada e redundante

ADVPN

Orquestrador de Sobreposição de Tecido

Outros tópicos sobre VPN

Solução de problemas de IPsec de VPN

SSL VPN

es.fortinet.com

ificação

ProdutosMelhores PráticasGuias de HardwareProdutos A-Z

> Guia de Administração > FortiGate / FortiOS 7.4.12 Inicial

IPsec VPN

A tecnologia de Rede Privada Virtual (VPN) permite que usuários remotos se conectem a redes privadas de computadores para acessar seus recursos de forma segura. Por exemplo, um funcionário que viaja ou trabalha em casa pode usar uma VPN para acessar com segurança a rede do escritório pela internet.

Em vez de fazer login remoto em uma rede privada usando uma conexão de internet não criptografada e não segura, o uso de uma VPN garante que partes não autorizadas não possam acessar a rede do escritório nem interceptar informações que circulam entre o funcionário e o escritório. Outro uso comum de uma VPN é conectar as redes privadas de vários escritórios.

A VPN IPsec utiliza o protocolo de Segurança de Protocolo de Internet (IPsec) para criar túneis criptografados na internet. O protocolo IPsec opera na camada de rede do modelo de SO e roda sobre o protocolo IP, que rotela pacotes. Todos os dados transmitidos são protegidos pelo túnel IPsec.

As seções a seguir fornecem instruções para configurar conexões VPN IPsec no FortiOS 7.4.12.

Configuração geral de VPN IPsec

Site-to-site VPN

3.14.3 Suportar SSL VPN;

R: Atendido.

FORTINET

BIBLIOTECA DE DOCUMENTOS

imento de busca

VPN SSL Quick Start

Modo túnel VPN SSL

Modo web SSL VPN

Autenticação SSL VPN

SSL VPN para IPsec VPN

Protocolos SSL VPN

Configuração do sistema operacional e verificação do host

FortiGate como Cliente VPN SSL

Suporte de dual stack para IPv4 e IPv6 para VPN SSL

Desabilite a área de

ProdutosMelhores PráticasGuias de HardwareProdutos A-Z

> Guia de Administração > FortiGate / FortiOS 7.4.12 Inicial

7.4.12 ↓

SSL VPN

A tecnologia de Rede Privada Virtual (VPN) permite que usuários remotos se conectem a redes privadas de computadores para acessar seus recursos de forma segura. Por exemplo, um funcionário que viaja ou trabalha em casa pode usar uma VPN para acessar com segurança a rede do escritório pela internet.

Em vez de fazer login remoto em uma rede privada usando uma conexão de internet não criptografada e não segura, o uso de uma VPN garante que partes não autorizadas não possam acessar a rede do escritório nem interceptar informações que circulam entre o funcionário e o escritório. Outro uso comum de uma VPN é conectar as redes privadas de vários escritórios.

A VPN SSL utiliza o protocolo Secure Socket Layer (SSL) para criar um túnel seguro do navegador web do host para uma aplicação específica (modo web) ou para fornecer um túnel SSL entre o cliente e a rede corporativa (modo túnel). A VPN SSL opera na camada de aplicação

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

R: Atendido.

BIBLIOTECA DE DOCUMENTOS

ProdutosMelhores PráticasGuias de HardwareProdutos A-Z

amento de busca

Certificados

Segurança

Scripts de configuração

Modo Workspace

Linguagens personalizadas

RAID

Conjuntos de cifras do algoritmo de criptografia FortiGate

Modo conservar

Uso de APIs

Backups de configuração e reset

Acordo de Segurança Fortinet

Registro e Relatório

Otimização WAN

Guia de Administração > FortiGate / FortiOS 7.4.12 Inicial

versão TLS	Conjuntos de cifras suportados	
TLS 1.1 ¹	ECDHE-RSA-AES256-SHA ¹	AES256-SHA ¹
	ECDHE-RSA-AES128-SHA ¹	AES128-SHA ¹
TLS 1.2	ECDHE-RSA-AES256-GCM-SHA384	AES256-GCM-SHA384 ¹
	ECDHE-RSA-AES128-GCM-SHA256	AES128-GCM-SHA256 ¹
	ECDHE-RSA-CHACHA20-POLY1305	AES256-SHA256
	ECDHE-RSA-AES256-SHA384	AES128-SHA256
	ECDHE-RSA-AES128-SHA256	AES256-SHA ¹
	ECDHE-RSA-AES256-SHA ¹	AES128-SHA ¹
	ECDHE-RSA-AES128-SHA ¹	
	TLS-AES-128-GCM-SHA256	TLS-AES-128-GCM-8-SHA256 ¹

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: Atendido.

BIBLIOTECA DE DOCUMENTOS

ProdutosMelhores PráticasGuias de HardwareProdutos A-Z

to de busca

Administração

Recependo

Resumo dos passos

Usando a interface gráfica

Conectando usando um navegador web

Menus

Tabelas

Inserimento de valores

Busca global baseada em interface gráfica

Carregando artefatos de uma CDN

Acesso a recursos de suporte adicionais

Paleta de comandos

Recuperando componentes gráficos ausentes

Usando o CLI

Configuração e gerenciamento

Registro de produtos com a FortiCare

Guia de Administração > FortiGate / FortiOS 7.4.12 Inicial

A interface gráfica contém os seguintes menus principais, que oferecem acesso às opções de configuração para a maioria dos recursos do FortiOS:

Painel	O painel exibe vários widgets e monitores que exibem informações importantes do sistema e permitem configurar algumas opções do sistema. Para mais informações, veja Dashboards e Monitores .
Rede	Opções para rede, incluindo configuração de interfaces de sistema e opções de roteamento. Para mais informações, veja Rede .
Política & Objetivos	Configure políticas de firewall, opções de protocolo e conteúdo de suporte para políticas, incluindo agendamentos, endereços de firewall e moduladores de tráfego. Para mais informações, veja Política e Objetos .
Perfis de Segurança	Configure os recursos de segurança do seu FortiGate, incluindo Antivírus, Filtro Web e Controle de Aplicações. Para mais informações, veja Perfis de Segurança .
VPN	Configure opções para redes privadas virtuais (VPNs) IPsec e SSL. Para mais informações, veja IPsec VPN e SSL VPN .
Usuário & Autenticação	Configure contas de usuário, grupos e métodos de autenticação, incluindo autenticação externa e login único (SSO).

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: Atendido.

BIBLIOTECA DE DOCUMENTOS

ProdutosMelhores PráticasGuias de HardwareProdutos A-Z

nto de busca

Prevenção de perda de dados

Patching virtual

SSL & SSH Inspeção

Assinaturas personalizadas

○ Configuração de assinaturas personalizadas

○ Bloqueando aplicações com assinaturas personalizadas

○ Filtros para grupos de controle de aplicações

○ Grupos de aplicações em políticas de modelagem de tráfego

Substituições

Proibição de IP

Grupos de perfil

ic VPN

VPN

ário & Autenticação

figuração sem fio

trolador de Switch

> Guia de Administração > FortiGate / FortiOS 7.4.12 Inicial

Para configurar uma política de modelagem de tráfego para usar um grupo de aplicações na interface gráfica:

1. Configure um grupo de aplicações para aplicações em nuvem:

a. Vá para *Perfis de Segurança > Assinaturas de Aplicação*.

b. Clique em *Criar Novo Grupo de Aplicação >*. A *página do Novo Grupo de Aplicações* se abre.

c. Insira o nome do grupo e, para *Tipo*, selecione *Aplicação*.

d. Clique no *+* para adicionar o grupo, os membros.

New Application Group

Group Namecloud app group

TypeApplicationFilter

Members

AmazonAWS

AmazonAWS_EC2

AmazonAWS_S3

GoogleCloudPlatform_AppEngi

GoogleCloudPrint

CommentsWrite a comment0/255

FortiGate

FGDES

Additional Information

API Preview

Documentation

Online Help

Video Tutorials

OK

Cancel

e. Clique em *OK*.

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

R: Atendido.

BIBLIOTECA DE DOCUMENTOS

ProdutosMelhores PráticasGuias de HardwareProdutos A-Z

nto de busca

so à Rede Zero Trust

ica e Objetivos

Políticas

Objetos de endereçamento

Opções do protocolo

Modelagem de tráfego

● Políticas de modelagem de tráfego

● Perfis de modelagem de tráfego

● Modeladores de tráfego

○ Priorização global do tráfego

○ Correspondência DSCP e marcação DSCP

● Exemplos

Serviços de Internet

is de Segurança

c VPN

VPN

ário & Autenticação

Resumo de...

> Guia de Administração > FortiGate / FortiOS 7.4.12 Inicial

Modelagem de tráfego

Um FortiGate oferece qualidade de serviço (QoS) aplicando limites de largura de banda e priorização ao tráfego de rede. O modelamento de tráfego é uma técnica usada pelo FortiGate para fornecer QoS. Uma abordagem básica para o modelamento do tráfego é priorizar o tráfego de maior prioridade em relação ao tráfego de menor prioridade durante períodos de congestionamento. Isso proporciona um efeito estabilizador para tráfego importante enquanto limita o tráfego menos importante.

O FortiGate pode ser configurado para fornecer modelagem de tráfego com policiamento ou modelagem de tráfego com fila. A diferença geral entre os dois é a seguinte:

Técnica	Descrição
Modelagem do trânsito com policiamento	Quando o tráfego excede os limites de largura de banda configurados, o tráfego é reduzido.
Modelagem de tráfego com fila	Quando o tráfego ultrapassa os limites de largura de banda configurados, o tráfego é atrasado para transporte até que a largura de banda seja liberada. O tráfego pode ser interrompido se as filas estiverem lotadas.

Policiamento e fila podem tanto priorizar o tráfego quanto garantir largura de banda e largura de banda máxima ao definir limites de largura de banda. A implementação é diferente, pois a fila usa filas, e a polícia não. Na fila, antes de um pacote sair de uma interface, ele é primeiro enfileirado em uma fila usando um algoritmo como RED ou FIFO. O kernel faz o desfile de enfileira do pacote com base no algoritmo HTB antes de enviá-lo. No policiamento, o tráfego simplesmente cai se estiver acima da largura de banda alocada.

Avenida Ayrton Senna da Silva, 161 | D. Pedro II | Paranaguá/PR | CEP 83203-800 | 41 3420.1143 / 41 3420.1114

www.portosdoparana.pr.gov.br

COMUNICAÇÃO INTERNA 4746/2026. Assinatura Simples realizada por: Vinícius Rodrigo Teixeira (XXX.978.469-XX) em 07/07/2026 17:29. Inserido ao documento 2.196.631 por: Vinícius Rodrigo Teixeira em: 07/07/2026 17:29. Demais assinaturas na última folha. A autenticidade deste documento pode ser validada no endereço: https://www.eprotocolo.pr.gov.br/spiweb/validarDocumento com o código: 932d25c1054bed9d3951746e2da9a3ec

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: Atendido.

BIBLIOTECA DE DOCUMENTOS

ProdutosMelhores PráticasGuias de HardwareProdutos A-Z

nto de busca

ssos à Rede Zero Trust
ica e Objetivos
Políticas
Objetos de endereçamento
Opções do protocolo
Modelagem de tráfego

- Políticas de modelagem de tráfego
- Perfis de modelagem de tráfego
- Modeladores de tráfego
- Priorização global do tráfego
- Correspondência DSCP e marcação DSCP
- Exemplos

Serviços de Internet
is de Segurança
c VPN
VPN
ário & Autenticação
figuração sem fio

> Guia de Administração > FortiGate / FortiOS 7.4.12 Inicial

As características da implementação de cada método são ligeiramente diferentes. A seguir, um breve resumo das características de policiamento de trânsito e da abordagem que cada método adota.

Priorização do tráfego

O FortiGate pode colocar pacotes em diferentes níveis de prioridade para priorizar determinado tráfego em relação a outros.

Método	Descrição
Perfil de modelagem de tráfego	O tráfego é dividido em categorias. Há um total de 30 aulas disponíveis. Para cada classe, o tráfego pode ser configurado em cinco níveis de prioridade.
Manipulador de tráfego	O tráfego pode ser priorizado nos níveis alto (2), médio (3) ou baixo (4). Quando o tráfego está abaixo da largura de banda garantida do shaper, o tráfego é automaticamente aplicado ao nível crítico (1).
Priorização global do tráfego	O tráfego é priorizado em alto (2), médio (3) ou baixo (4) com base no ToS (tipo de serviço) ou DSCP.

Limites garantidos e máximos de largura de banda

O propósito geral de configurar a largura de banda garantida é alocar uma certa proporção da largura de banda total para garantir o transporte para um determinado tipo de tráfego. Isso é configurado e tratado de forma diferente em cada método.

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

R: Atendido.

BIBLIOTECA DE DOCUMENTOS
Produtos
Melhores Práticas
Guias de Hardware
Produtos A-Z

> Guia de Administração > FortiGate / FortiOS 7.4.12 Inicial

taxa para traffic shapers.

Configuração da largura de banda de saída

O modelagem de tráfego geralmente é configurado para tráfego de saída que sai do FortiGate. Portanto, é necessário definir a largura de banda de saída da interface para que a priorização do tráfego ocorra em todos os métodos de configuração de modelagem de tráfego. A largura de banda de saída da interface também é necessária ao definir a largura de banda garantida e máxima em um perfil de modelagem de tráfego.

Para modeladores de tráfego, não é necessário configurar a largura de banda de saída para aplicar limites máximos de largura de banda; no entanto, a largura de banda de saída é necessária para garantir a largura de banda. Tráfego abaixo do limite de largura de banda garantida em um modelador de tráfego recebe prioridade 1. Se a largura de banda externa não estiver configurada, a priorização do tráfego não ocorre e a prioridade não tem sentido.

Política de modelagem de tráfego

Perfis de modelagem de tráfego e modeladores de tráfego são métodos de fiscalização do tráfego. Políticas de modelagem de tráfego são usadas para mapear o tráfego a um modelador de tráfego ou atribuí-los a uma classe.

Menu

- Objetos de endereçamento
- Opções do protocolo
- Modelagem de tráfego**
 - ☒ Políticas de modelagem de tráfego
 - ☒ Perfis de modelagem de tráfego
 - ☒ Modeladores de tráfego
 - ☐ Priorização global do tráfego
 - ☐ Correspondência DSCP e marcação DSCP
 - ☒ Exemplos

3.15.5 A rede deverá suportar QoS (Quality of Service) fim a fim.

GERÊNCIA DE TECNOLOGIA DA INFORMAÇÃO

R: Atendido.

Existem diferentes métodos para configurar o traffic shaping no FortiGate. A tabela a seguir lista os métodos e suas capacidades em ordem de preferência. Se os três métodos forem configurados, o primeiro será preferido em relação ao segundo, que é preferido ao terceiro.

Método	Policimento		Fila
	Priorização do tráfego	Limites garantidos e máximos de largura de banda	Fila de tráfego
Perfil de modelagem de tráfego*	Sim	Sim, com base na porcentagem da largura de banda externa	Sim
Manipulador de tráfego	Sim	Sim, baseado na taxa	Não
Priorização global do tráfego	Sim	Não	Não

* Perfis de modelagem de tráfego são configurados como tipos de policiamento ou fila. A fila permite opções adicionais ao configurar uma entrada de classe de modelagem.

As características da implementação de cada método são ligeiramente diferentes. A seguir, um breve resumo das características de policiamento de trânsito e da abordagem que cada método adota.

Priorização do tráfego

O FortiGate pode colocar pacotes em diferentes níveis de prioridade para priorizar determinado tráfego em relação a

3.15.6 A rede deverá permitir o mapeamento dos tráfegos e largura de banda de cada classe do QoS.

R: Atendido.

Existem diferentes métodos para configurar o traffic shaping no FortiGate. A tabela a seguir lista os métodos e suas capacidades em ordem de preferência. Se os três métodos forem configurados, o primeiro será preferido em relação ao segundo, que é preferido ao terceiro.

Método	Policimento		Fila
	Priorização do tráfego	Limites garantidos e máximos de largura de banda	Fila de tráfego
Perfil de modelagem de tráfego*	Sim	Sim, com base na porcentagem da largura de banda externa	Sim
Manipulador de tráfego	Sim	Sim, baseado na taxa	Não
Priorização global do tráfego	Sim	Não	Não

* Perfis de modelagem de tráfego são configurados como tipos de policiamento ou fila. A fila permite opções adicionais ao configurar uma entrada de classe de modelagem.

As características da implementação de cada método são ligeiramente diferentes. A seguir, um breve resumo das características de policiamento de trânsito e da abordagem que cada método adota.

Priorização do tráfego

O FortiGate pode colocar pacotes em diferentes níveis de prioridade para priorizar determinado tráfego em relação a

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:

SERVIÇO	QUANTIDADES ("N")
FORNECIMENTO DE "N" CIRCUITOS DE REDE PRIVATIVA MPLS (DE ALTA DISPONIBILIDADE) EM FIBRA OPTICA	22
FORNECIMENTO DE "N" CIRCUITOS DE REDE PRIVATIVA DE ALTA DISPONIBILIDADE EM RADIO LICENCIADO	15
GERENCIAMENTO DE "N" CIRCUITOS ATRAVÉS DE FERRAMENTA SD-WAN COM SERVIÇO NOC/SOC	25

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 da proposta tecnica.

CORPORATIVAS E EDUCACIONAIS – REEDIÇÃO DO EDITAL PE 2.0905/2022.
CONTRATO 303/2022
PROVIMENTO DE REDES DE TELECOMUNICAÇÃO DO TIPO MPLS E/ou SD-WAN QUE ATENDERÃO ÀS DEMANDAS DE CONECTIVIDADE CORPORATIVA.

Quantitativos:

Item	Descrição	Qtde
1	Link MPLS 15 Mbps dedicado	0
2	Link MPLS 25 Mbps dedicado	48
3	Link MPLS 50 Mbps dedicado	8
4	Link MPLS 75 Mbps dedicado	0
5	Link MPLS 100 Mbps dedicado	2
6	Link MPLS 150 Mbps dedicado	0
7	Link MPLS 300 Mbps dedicado	2
8	Link MPLS 500 Mbps dedicado	0
9	Link MPLS 700 Mbps dedicado	2
10	Link MPLS 1000 Mbps dedicado	0
10	Link MPLS 2000 Mbps dedicado	1
11	Equipamento SD-WAN Tipo 1	51
12	Equipamento SD-WAN Tipo 2	9
13	Equipamento SD-WAN Tipo 3	2

CONTRATO 312/2022
PROVIMENTO DE REDES DE TELECOMUNICAÇÃO DO TIPO MPLS E/ou SD-WAN QUE ATENDERÃO ÀS DEMANDAS DE CONECTIVIDADE EDUCACIONAL - LOTE II.

Quantitativo:

Item	Descrição	Qtde
1	Link internet 25 Mbps em SD-WAN com simetria de banda	0

GERÊNCIA DE TECNOLOGIA DA INFORMAÇÃO

Contrato nº 592.321/2022

Objeto: Contratação de empresa para a prestação de serviço de comunicação multimídia (SCM) com equipamentos de SD-WAN e suporte.

Item	Descrição	Quantidade
1	Links MPLS 100 Mbps dedicado em fibra óptica	130
2	Equipamento SD-WAN 40F	146
3	Administração de circuitos de comunicação com orquestração SD-WAN e suporte operacional e de segurança. Fazem parte de suporte: • Monitoramento contínuo de infraestrutura; • Detecção e tratamento de incidentes; • Adoção de ações de contenção e recuperação; • Análise de alertas gerados por ferramentas de supervisão; • Execução de procedimentos operacionais padronizados (POPs); • Gestão do ciclo de vida de incidentes e requisições; • Acompanhamento de mudanças planejadas; • Apoio à gestão de segurança da informação; • Atendimento a chamados de suporte de segundo nível;	146

Contrato assinado em junho/2022 e vigente.

Por ser verdade, firmamos a presente.

Maringá, 26 de maio de 2026.

Grupo Fonte: 1 - Do Exercício

Fonte: 0000 - RECURSOS ORDINÁRIOS (LIVRES)

Observação:

Justificativa: Considerando a necessidade de continuidade dos serviços de telefonia móvel corporativa utilizados pela administração municipal, e que o processo licitatório definitivo para contratação do serviço encontra-se em tramitação, conforme Solicitação de Contratação nº 365/2025, justifica-se a contratação temporária, conforme proposta apresentada. O serviço inclui planos corporativos de voz e dados, gestão centralizada de contas, atendimento prioritário, portabilidade de números, fornecimento de SIM Cards e suporte técnico. Tais recursos são essenciais à manutenção das atividades administrativas e operacionais das secretarias. A interrupção do serviço causaria prejuízos à comunicação institucional e às ações de campo. Assim, a contratação possui caráter emergencial e temporário, até a conclusão do novo certame, garantindo continuidade e eficiência administrativa.

Empenho: 23187/2025

Emitido em: 29/10/2025

Fornecedor: LIGGA TELECOMUNICACOES S.A.

Cnpj/Cpf: 4368865000166

IE/RG: 0

Endereço: AV VICENTE MACHADO

Cidade: CURITIBA

Fone: 4333751280

CEP: 8042001

e-felipe.marques@liggavc.com.br

Item	Cod.	Produto	Qtde	Unid.	VL Unit.	VL Total
1	554725	SERVICO DE TELEFONIA MOVEL PESSOAL C/ ABRANGENCIA DE	4	UNIDADE	11.404,500	45.618,000
SERVICO DE TELEFONIA MOVEL PESSOAL, SISTEMA DIGITAL POS-PAGO, COM ABRANGENCIA DE COBERTURA NO MUNICIPIO DE SAO JOSE DOS PINHAIS E REGIAO METROPOLITANA DE CURITIBA PR. Assinatura mensal&40Assinatura Tarifa Zero Local&40Assinatura Tarifa Zero Nacional&1VC1 móvel-móvel (mesma operadora)&33.420VC1 móvel-móvel (outra operadora)&37.420Móvel - Fixo&18.000SMS 4.000Pacote de Dados de 40 MB(velocidade 56 KBPS a 256 kbps) Dados M2M 50Mb&131Dados 3G (6 GB velocidade 1Mbps)&50Pacote de Dados limitado para Smartphone(velocidade até 300 Kbps)&26VC2 mesma operadora&250VC2 outra operadora&150VC2 fixo&150VC3 Mesma operadora&350VC3 outra operadora&150VC3 fixo&150MMS&50						
Total da Solicitação:					R\$ 45.618,00	

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 da proposta tecnica.

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 SD-WAN.

R: Atendido.

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

Histórico Contratual

Data Inclusão: 11/04/2025
Hora Inclusão: 11:00
Matricula 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 - 14:30 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

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

Estrangeiro

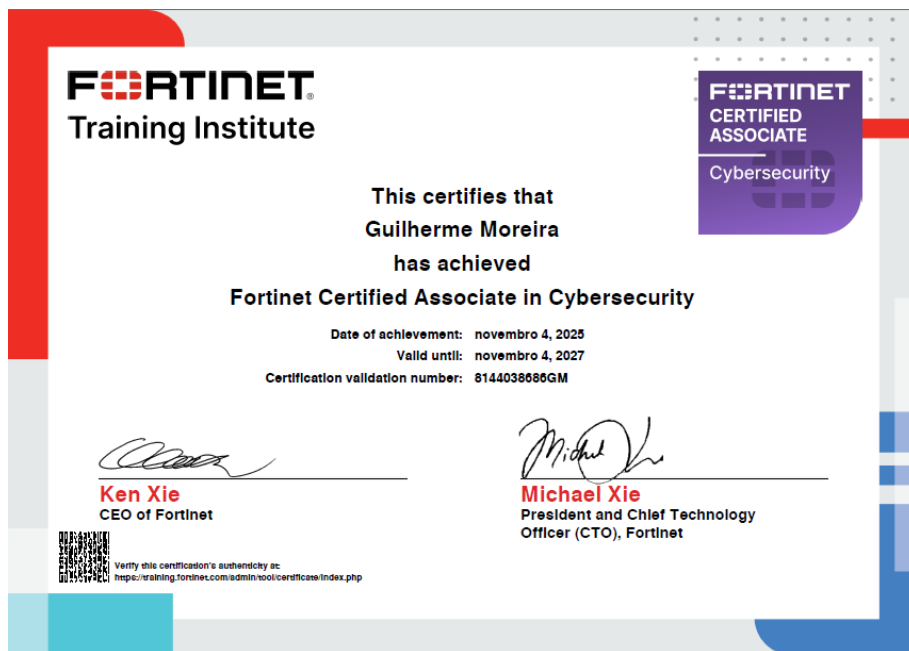
Ano Chegada:
Condição:
Nr. Carteira RNE:
Validade:
Nr/Serie Ct. Trab.:
Expedição:



Avenida Ayrton Senna da Silva, 161 | D. Pedro II | Paranaguá/PR | CEP 83203-800 | 41 3420.1143 / 41 3420.1114

www.portosdoparana.pr.gov.br

COMUNICAÇÃO INTERNA 4746/2026. Assinatura Simples realizada por: Vinícius Rodrigo Teixeira (XXX.978.469-XX) em 07/07/2026 17:29. Inserido ao documento 2.196.631 por: Vinícius Rodrigo Teixeira em: 07/07/2026 17:29. Demais assinaturas na última folha. A autenticidade deste documento pode ser validada no endereço: https://www.eprotocolo.pr.gov.br/spiweb/validarDocumento com o código: 932d25c1054bed9d3951746e2da9a3ec



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 da proposta tecnica

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 da proposta tecnica.

CONCLUSÃO

Com base na avaliação acima, a referida empresa, atendeu de forma integral os requisitos técnicos exigidos pelo Termo de Referência e Edital.

Sem mais para o momento.

Paranaguá, 06 de julho de 2026

(Assinado Eletronicamente)

Vinicius Rodrigo Teixeira

Coordenador (CINCO)

(Assinado Eletronicamente)

Wanice Carvalho Violim

Gerente de Tecnologia (GTEC)

COMUNICAÇÃO INTERNA 4746/2026.

Documento: **AnalisetecnicaDiligenciasProcesso430TIC_2026_07_06.pdf.**

Assinatura Simples realizada por: **Vinícius Rodrigo Teixeira (XXX.978.469-XX)** em 07/07/2026 17:29, **Wanice Cavalheiro Violim (XXX.934.678-XX)** em 07/07/2026 17:30 Local: APPA/GTEC.

Inserido ao documento **2.196.631** por: **Vinícius Rodrigo Teixeira** em: 07/07/2026 17:29.



Documento assinado nos termos do Art. 38 do Decreto Estadual nº 7304/2021.

A autenticidade deste documento pode ser validada no endereço:

<https://www.eprotocolo.pr.gov.br/spiweb/validarDocumento> com o código:
932d25c1054bed9d3951746e2da9a3ec