



## ANEXO TÉCNICO

**Título: fornecimento de equipamentos Fortinet**

**Cliente: MINISTERIO DA JUSTIÇA**

**Data: 29/08/2023**

**SFA: 2818360**



<b>1. VIVO.....</b>	<b>3</b>
1.1. INSTITUCIONAL .....	3
1.2. CERTIFICAÇÕES .....	3
<b>2. ESCOPO DO PROJETO.....</b>	<b>4</b>
2.1. FORTIAP .....	4
2.2. FORTIGATE.....	6
2.3. FORTIANALYZER .....	8
2.4. FORTIMANAGER .....	10
2.5. FORTIAUTHENTICATOR .....	14
2.6. FORTINAC.....	17
2.6.1. <i>Lista de Materiais</i> .....	21
2.6.2. <i>Garantia do fabricante</i> .....	23
2.7. PRESTADORAS DE SERVIÇOS CONTRATADAS PELA VIVO EMPRESAS .....	23
2.8. RESPONSABILIDADES DO CLIENTE .....	23
<b>3. CONSIDERAÇÕES FINAIS .....</b>	<b>24</b>
3.1. CONFIDENCIALIDADE .....	24

## 1. VIVO

### 1.1. Institucional

A Vivo é a marca comercial da Telefônica Brasil, empresa líder em telecomunicações no País, com 97,8 milhões de acessos (1T18). A operadora atua na prestação de serviços de telecomunicações fixa e móvel em todo o território nacional e conta com um portfólio de produtos completo e convergente para clientes B2C e B2B - banda larga fixa e móvel, ultra banda larga (over fiber), voz fixa e móvel e TV por assinatura. A empresa está presente em 4,3 mil cidades, sendo 4,1 mil com rede 3G e mais de 2,7 mil com 4G, segmento em que é líder de Market Share. A operadora ainda oferece o 4G+, internet duas vezes mais rápida que o 4G. No segmento móvel, a Vivo tem 75,1 milhões de clientes e responde pela maior participação de mercado do segmento (31,9%) no país, de acordo com resultados do balanço trimestral (1T18).

Guiada pela constante inovação e a alta qualidade dos seus serviços, a Vivo está no centro de uma transformação Digital, que amplia a autonomia, a personalização e as escolhas em tempo real dos seus clientes, colocando-os no comando de sua vida digital, com segurança e confiabilidade. A Telefônica Brasil faz parte do Grupo Telefônica, um dos maiores conglomerados de comunicação do mundo, com presença em 21 países, 356,9 milhões de acessos, 122,8 mil colaboradores e receita de 52,0 bilhões de euros em 2017.

Ciente de sua responsabilidade de retribuir à sociedade a confiança que recebe na utilização dos seus serviços, a empresa conta com a Fundação Telefônica Vivo. Desde 1999, a Fundação atua na formação da nova geração, apontando os caminhos para o desenvolvimento do país ao aplicar inovação à educação, empreendedorismo e cidadania, com diferentes projetos sociais nessas áreas.

### 1.2. Certificações

A **Vivo** utiliza um conjunto de metodologias e melhores práticas reconhecidas pelo mercado para a prestação dos seus serviços.

A empresa tem como política e diretriz empresarial realizar forte investimento em processos e certificações para o aprimoramento da capacitação de seus profissionais e processos internos, melhoria da eficiência e, conseqüentemente, o aumento da qualidade dos serviços prestados. A **Vivo** entende que o sucesso na implementação dos processos de negócios está baseado em três dimensões: **Atitude, Tecnologia e Metodologia**.



## 2. ESCOPO DO PROJETO

Fornecimento de equipamentos e licenciamento Fortinet para o projeto de fornecimento de pontos de acesso, controladores, Software de gerenciamento licenças e suporte para 60 meses.

### 2.1. FortiAP



#### Pontos de acesso gerenciados em nuvem FortiLAN ou FortiGate

Os pontos de acesso FortiAP™ são gerenciados centralmente pelo controlador WLAN integrado de qualquer dispositivo de segurança FortiGate® ou por meio do portal de provisionamento e gerenciamento FortiLAN Cloud. Com a integração da funcionalidade do controlador sem fio no dispositivo FortiGate líder de mercado, esses APs são perfeitos para implantações em campus e filiais. O Security Fabric da Fortinet permite que você gerencie facilmente a segurança com e sem fio a partir de um console de gerenciamento de painel único e protege sua rede das ameaças de segurança mais recentes.

Esses APs internos Wi-Fi 6E de banda de frequência estendida de classe empresarial de alto desempenho fornecem três rádios e quatro fluxos espaciais. Esses pontos de acesso suportam a banda de 6 GHz, OFDMA e uma porta Ethernet de 5 Gigabit. Os APs podem fornecer varredura 24 horas por dia, 7 dias por semana em todas as bandas enquanto ainda fornecem acesso nas bandas de 2,4 GHz e 5 GHz ou 2,4 GHz e serviço duplo de 5 GHz ou o AP pode ser configurado para fornecer acesso simultâneo em 2,4 GHz, 5 GHz e as bandas de 6 GHz. O rádio integrado BLE/ZigBee pode ser usado para beacons e aplicações de localização.

#### Especificações Técnicas

Radio 1 Radio 2 802.11ax 4x4 802.11ax				Radio3			
4x4				4x4 Tri band Service and			
Tx power/chain Rx Sensitivity Tx power/chain Rx Sensitivity				2x2 Scanning radio			
(dBm) (dBm) (dBm) (dBm)				Tx power/chain Rx Sensitivity			
				(dBm) (dBm)			
1 Mbps	21	-99					-99
11 Mbps	21	-91					-91

2.4GHz, 802.11g						
6 Mbps	21	-93				-95
54 Mbps	21	-77				-78
2.4GHz, 802.11n HT20						
MCS0	21	-95				-92
MCS7	19	-77				-74
2.4GHz, 802.11n HT40						
MCS0	20	-92				-90
MCS7	18	-74				-72
2.4GHz, 802.11ax HE20						
MCS0	21	-94				-90
MCS11	19	-64				-71
2.4GHz, 802.11ax HE40						
MCS0	21	-91				-91
MCS11	19	-62				-72
5.0GHz, 802.11a						
6 Mbps			23	-93	22	-93
54 Mbps			21	-76	21	-76
5.0GHz, 802.11n HT20						
MCS0			22	-93	21	-93
MCS7			20	-75	18	-73
5.0GHz, 802.11n HT40						
MCS0			21	-93	21	-90
MCS7			18	-78	18	-71
5.0GHz, 802.11ac VHT20						
MCS0			22	-93	21	-93

## Espectro de banda



## 2.2. FortiGate



Figura Meramente Ilustrativa 1

### Alto desempenho com flexibilidade

A série FortiGate permite que as organizações criem redes orientadas à segurança que podem incorporar a segurança profundamente seu datacenter e em sua arquitetura de TI híbrida para proteger qualquer aresta em qualquer escala.

Alimentado por um rico conjunto de serviços FortiGuard baseados em AI/ML e uma estrutura de segurança integrada a plataforma, o FortiGate oferece ameaça coordenada, automatizada e proteção de ponta a ponta em todos os casos de uso.

A primeira aplicação integrada de Zero Trust Network Access (ZTNA) do setor em um Solução NGFW, a solução FortiGate controla, verifica e facilita automaticamente o acesso do usuário a aplicativos que fornecem convergência consistente com uma experiência de usuário perfeita.

### FortiOS em todos os lugares

FortiOS, o sistema operacional avançado da Fortinet O FortiOS permite a convergência de rede e segurança de alto desempenho em todo o Tecido de segurança Fortinet. Como pode ser implantado em qualquer lugar, ele oferece suporte consistente e postura de segurança sensível ao contexto em ambientes de rede, endpoint e multinuvem.

O FortiOS capacita todas as implantações do FortiGate, seja um dispositivo físico ou virtual, como um contêiner, ou como um serviço de nuvem. Este modelo de implantação universal permite a consolidação de muitas tecnologias e casos de uso em uma estrutura de gerenciamento e política única e simplificada. Isso é recursos de ponta construídos organicamente, sistema operacional unificado e ultraescalabilidade permite que as organizações protejam todas as arestas, simplifiquem as operações e administrem seus negócios sem comprometer o desempenho ou a proteção.

O FortiOS expande drasticamente a capacidade do Fortinet Security Fabric de fornecer AI/Serviços baseados em ML, detecção de sandbox avançada em linha, imposição de ZTNA integrada, e mais, fornece proteção em modelos de implantação híbrida para hardware, software e Software como serviço com SASE.

O FortiOS expande a visibilidade e o controle, garante a implantação e aplicação consistente de políticas de segurança e permite o gerenciamento centralizado em redes de grande escala com os seguintes atributos-chave:

- Drill-down interativo e visualizadores de topologia que exibem o status em tempo real
- Remediação com um clique que fornece proteção precisa e rápida contra ameaças e abusos
- Sistema exclusivo de pontuação de ameaças correlaciona ameaças ponderadas com usuários para priorizar investigações

### Serviços FortiGuard

FortiGuard AI-Powered Security o rico conjunto de serviços de segurança do FortiGuard combate ameaças em tempo real usando inteligência artificial, proteção coordenada projetada por pesquisadores de ameaças de segurança do FortiGuard Labs, engenheiros, e especialistas forenses.

### Segurança Web

URL avançado fornecido pela nuvem, DNS (Domain Name System) e filtragem de vídeo fornecendo proteção completa contra phishing e outros ataques originados na Web, atendendo à conformidade.

Além disso, seu serviço CASB (Cloud Access Security Broker) dinâmico inline é focado em protegendo os dados SaaS de negócios, enquanto a inspeção de tráfego ZTNA em linha e a verificação de postura ZTNA fornecer controle de acesso por sessão aos aplicativos. Também se integra com o FortiClient

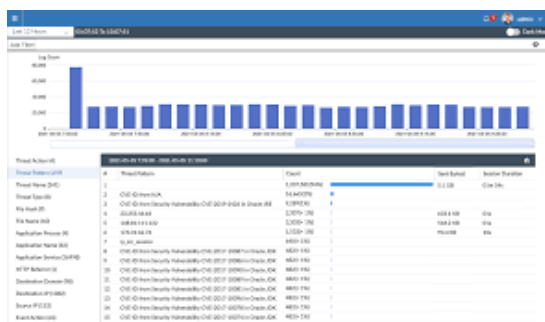
Fabric Agent para estender a proteção a usuários remotos e móveis.

## Specifications

	FG-3200F	FG-3201F
<b>Interfaces and Modules</b>		
Hardware Accelerated 400 GE QSFP-DD / 200 GE QSFP56 / 100 GE QSFP28 / 40 GE QSFP+ Ports	4	
Hardware Accelerated 50 GE SFP56 / 25 GE SFP28 / 10 GE SFP+ Slots	10	
Hardware Accelerated 25 GE SFP28 / 10 GE SFP+ / GE SFP ULL Slots	4	
Hardware Accelerated 50 GE SFP56 / 25 GE SFP28 / 10 GE SFP+ HA1/HA2 Slots	2	
10GE / GE RJ45 Management Ports	2	
USB 3.0 Port	1	
Console RJ45 Port	1	
Onboard Storage	2x 1 TB SSD	
Trusted Platform Module (TPM)	Yes	
Included Transceivers	2x SFP+ (SR 10 GE)	
<b>System Performance — Enterprise Traffic Mix</b>		
IPS Throughput <sup>2</sup>	63 Gbps	
NGFW Throughput <sup>2,4</sup>	47 Gbps	
Threat Protection Throughput <sup>2,5</sup>	45 Gbps	
<b>System Performance and Capacity</b>		
IPv4 Firewall Throughput (151B / 512 / 64 byte, UDP)	387/385/178.5 Gbps	
IPv6 Firewall Throughput (151B / 512 / 86 byte, UDP)	387/385/178.5 Gbps	
Firewall Latency (64 byte, UDP)	3.42 µs	
Firewall Throughput (Packet per Second)	267.75 Mpps	
Concurrent Sessions (TCP)	70 Million	
New Sessions/Second (TCP)	800 000	
Firewall Policies	200 000	
IPsec VPN Throughput (512 byte) <sup>1</sup>	105 Gbps	
Gateway-to-Gateway IPsec VPN Tunnels	40 000	
Client-to-Gateway IPsec VPN Tunnels	200 000	
SSL-VPN Throughput	11 Gbps	
Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode)	30 000	
SSL Inspection Throughput (IPS, avg HTTPS) <sup>3</sup>	29 Gbps	
SSL Inspection CPS (IPS, avg. HTTPS) <sup>3</sup>	30 000	
SSL Inspection Concurrent Session (IPS, avg HTTPS) <sup>3</sup>	7.4 Million	
Application Control Throughput (HTTP 64K) <sup>2</sup>	109 Gbps	
CAPWAP Throughput (HTTP 64K)	65 Gbps	
Virtual Domains (Default / Maximum)	10 / 500	
Maximum Number of FortiSwitches Supported	300	
Maximum Number of FortiAPs (Total / Tunnel)	4096 / 2048	
Maximum Number of FortiTokens	20 000	
Maximum Number of Registered FortiClients	20 000	
High Availability Configurations	Active-Active, Active-Passive, Clustering	

	FG-3200F	FG-3201F
Dimensions and Power		
Height x Width x Length (inches)	3.5 x 17.44 x 23.9	
Height x Width x Length (mm)	88.9 x 443 x 607.1	
Weight	43.9 lbs (20 kg)	45.5 lbs (20.7 kg)
Form Factor (supports EIA/non-EIA standards)	Rack Mount, 2RU	
AC Power Supply	100-240VAC, 60/50 Hz	
Power Consumption (Average / Maximum)	520W / 865 W	527 W / 870 W
Current (Maximum)	12@100V, 9A@240V	
Heat Dissipation	2955 BTU/h	2971 BTU/h
Redundant Power Supplies (Hot Swappable)	Yes (Default dual AC PSU for 1+1 Redundancy)	
Power Supply Efficiency Rating	80Plus Compliant	
Operating Environment and Certifications		
Operating Temperature	32~104°F (0~40°C)	
Storage Temperature	-31~-158°F (-35~-70°C)	
Humidity	5%-90% non-condensing	
Noise Level	71 dBA	
Forced Airflow	Front to Back	
Operating Altitude	Up to 10 000 ft (3048 m)	
Compliance	FCC Part 15 Class A, RCM, VCCI, CE, UL/cUL, CB	
Certifications	USGv6/IPv6	

## 2.3. FortiAnalyzer



O FortiAnalyzer é um poderoso gerenciador de logs, análises e relatórios plataforma que fornece às organizações um único console para gerenciar, automatize, orquestre e responda, permitindo segurança simplificada operações, identificação proativa e correção de riscos, e visibilidade completa de todo o cenário de ataque.



Integrado com o Fortinet Security Fabric, o FortiAnalyzer permite Equipes de operações de rede e segurança com detecção em tempo real recursos, análise de segurança centralizada e segurança de ponta a ponta consciência da postura para ajudar os analistas a identificar a persistência avançada ameaças (APTs) e mitigar os riscos antes que uma violação possa ocorrer.

## **Capacidades**

**Detecção e Resposta a Incidentes** Visibilidade NOC/SOC Centralizada para a Superfície de Ataque O FortiAnalyzer fornece Security Fabric Analytics em todos os logs do dispositivo com correlação de eventos e detecção em tempo real de Ameaças Persistentes Avançadas (APTs), vulnerabilidades e Indicadores de compromisso (IOC) para FortiGate NGFWs, FortiClient, FortiSandbox, FortiWeb, FortiMail e outros produtos Fortinet, para visibilidade profunda e insights críticos de rede. Orquestração simplificada e fluxos de trabalho automatizados fornecem às equipes de operações de segurança de rede informações em tempo real notificações, relatórios e painéis para visibilidade de painel único e resultados acionáveis.

## **Gestão de Incidentes e Eventos**

As equipes de segurança podem monitorar e gerenciar alertas e logs de eventos de dispositivos Fortinet, com eventos processados e correlacionados em um formato que os analistas podem entender facilmente. Investigar padrões de tráfego suspeitos e pesquisa usando filtros em manipuladores de eventos predefinidos ou personalizados para gerar notificações e monitoramento em tempo real para operações NOC e SOC, SD-WAN, SSL VPN, sem fio, Shadow IT, IPS, reconhecimento de rede, FortiClient e muito mais.

O componente Incidentes permite que os analistas gerenciem o tratamento de incidentes e o ciclo de vida, com incidentes gerados por eventos que mostram ativos, endpoints, usuários e cronogramas afetados.

## **Automação de Rede**

Os playbooks do FortiAnalyzer aumentam as habilidades da equipe de segurança de uma organização para simplificar a investigação esforços por meio de resposta automatizada a incidentes, liberando recursos e permitindo que os analistas foco em tarefas críticas. Modelos de playbook prontos para uso permitem que os analistas de SOC personalizar seus casos de uso, definir processos personalizados, interagir com outros Security Fabric dispositivos como FortiOS e EMS, edite playbooks e tarefas no editor de playbook visual e use o Playbook Monitor para investigação de hosts comprometidos, infecções e incidentes críticos, enriquecimento de dados para exibições de ativos e identidade, bloqueio de malware, IPs C&C e muito mais.

## **Análise de rede de segurança**

### **Análise e relatórios**

A análise orientada à automação do FortiAnalyzer capacita as equipes de operações de segurança de rede a concluir uma avaliação rápida de dispositivos de rede, sistemas e usuários,

com dados de log correlacionados e inteligência de ameaças FortiGuard para análise de eventos históricos e em tempo real.

- Os monitores e exibições do FortiView fornecem insights profundos com contexto e significado da rede atividade, riscos, vulnerabilidades, tentativas de ataque, indicadores de comprometimento e anomalias, atividade do usuário sancionada e não sancionada.

- A visualização de log permite que os analistas expandam sua investigação e utilizem filtros de pesquisa em logs de dispositivos gerenciados, detalhamento de logs, com exibições personalizadas e grupos de log, incluindo um Banco de dados SIEM com logs normalizados para dispositivos Fortinet em Fabric ADOMs.

## FortiAnalyzer VM

A Fortinet oferece o licenciamento FortiAnalyzer-VM em um modelo de licença permanente empilhável com suporte técnico à la carte e serviços de assinatura.

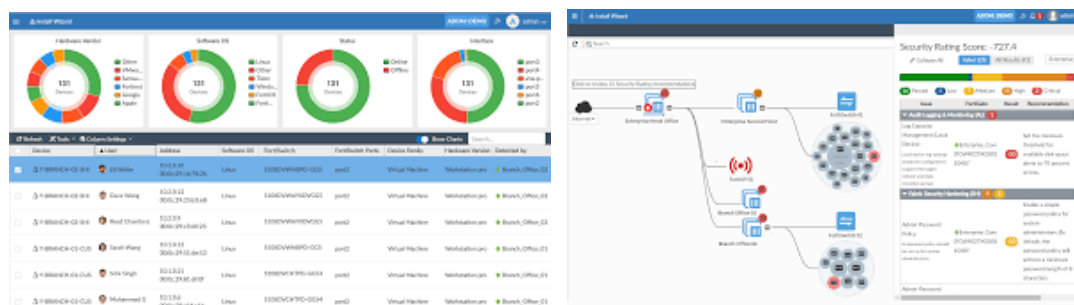
Esta versão baseada em software do dispositivo de hardware FortiAnalyzer foi projetada para ser executada em várias plataformas de virtualização, que permite que você expanda sua solução virtual à medida que seu ambiente se expande.

FORTIANALYZER VIRTUAL APPLIANCES	FAZ-VM-GB1	FAZ-VM-GB5	FAZ-VM-GB25	FAZ-VM-GB100	FAZ-VM-GB500	FAZ-VM-GB2000
Capacity						
GB/ day of Logs *	+1	+5	+25	+100	+500	+2,000
Devices/VDOMs Maximum	10 000	10 000	10 000	10 000	10 000	10 000
Chassis Management	✓	✓	✓	✓	✓	✓
FortiGuard IOC Service				✓		
Security Automation Service				✓		
Hypervisor Support	Up-to-date hypervisor support can be found in the release note for each FortiAnalyzer version. Visit <a href="https://docs.fortinet.com/product/fortianalyzer/">https://docs.fortinet.com/product/fortianalyzer/</a> and find the Release Information at the bottom section. Go to "Product Integration and Support" → "FortiAnalyzer [version] support" → "Virtualization"					
vCPU Support (Minimum / Maximum)	4 / Unlimited					
Network Interface Support (Min / Max) **	1 / 12					
Memory Support (Minimum / Maximum)	8 GB / Unlimited for 64-bit					

\* Unlimited GB/ day when deployed in collector mode

\*\* VM supports up to 12 vNIC interfaces/ports. Applicable to 6.4.3+. Actual consumable numbers vary depending on cloud platforms.

## 2.4. Fortimanager



O FortiManager fornece gerenciamento centralizado orientado à automação de gerenciamento de seus dispositivos Fortinet a partir de um único console.

Este processo permite a administração completa e visibilidade de seus dispositivos de rede por meio de provisionamento simplificado e ferramentas de automação inovadoras.

Integrado com o Fortinet Security Fabric avançado arquitetura de segurança e rede orientada a automação capacidades de operações fornecem uma base sólida para garantir e otimizar a segurança da sua rede.

## **Destaques**

### **Gerenciamento e provisionamento de painel único**

O gerenciamento e o provisionamento de painel único simplificam a política e o objeto centralizados gerenciamento e provisionamento, histórico e controle de revisão automática e recursos aprimorados de controle de acesso baseado em função (RBAC) para gerenciamento de script e gerenciamento IPS com função separação.

### **Automação de rede**

Fabric Automation simplifica o processo de implantação de provisionamento zero-touch (ZTP) para SDBranch (FortiGate e dispositivos de acesso) com modelos poderosos que utilizam metavariáveis diretamente para provisionamento escalável para milhares de sites.

### **Monitoramento e Visibilidade**

Monitoramento e visibilidade para inventário de dispositivos, aplicativos, SD-WAN, borda de LAN, gerenciamento aplicativos de extensão (MEAs), tráfego, nuvem pública e muito mais.

### **Características principais**

- Gerencie centralmente as políticas de rede e segurança para milhares de FortiGate NGFWs e SD-WAN seguro mais FortiSwitches, FortiAP e FortiExtender. Fornecer atualizações de assinatura para FortiGate, FortiMail, FortiSandbox e FortiClient
- Obtenha distribuição centralizada de conteúdo de segurança e assinaturas por meio do uso do built-in Módulo FortiGuard
- Simplifique a configuração, implantação e manutenção para Secure SD-WAN em escala.
- Acelere a conectividade FortiExtender Wireless WAN com gerenciamento centralizado em sites distribuídos
- Reduza a complexidade e os custos aproveitando a API REST automatizada, scripts, conectores e pontos de automação

- Automatize fluxos de trabalho e configurações para firewalls, switches e redes sem fio Fortinet a infraestrutura
- Separe os dados do cliente e gerencie domínios aproveitando ADOMs para estar em conformidade e operacionalmente eficaz
- Alta disponibilidade para automatizar backups para até cinco nós com software simplificado e atualizações de segurança para todos os dispositivos gerenciados

## **Gerenciamento e provisionamento de painel único**

### **Configuração e provisionamento de dispositivos**

O FortiManager expande os recursos do administrador de rede com um rico conjunto de ferramentas para gerencie centralmente até 100.000 dispositivos, incluindo FortiGate NGFWs, FortiExtender, FortiSwitch switches, pontos de acesso FortiAP, Fortinet Secure SD-WAN e muito mais.

Defina coletivamente as configurações do dispositivo usando modelos aprimorados com suporte a variáveis, em preparação para provisão sem toque para implantações em massa, imposição de versão de firmware para instalações e atualizações, modelos para atribuir pacotes de política e revisão de política e objeto histórico para auditoria e um modelo de autorização de malha provisiona e autoriza automaticamente Dispositivos Lan Edge nos FortiGates gerenciados.

O FortiManager inclui SSL estendido e suporte a certificado para perfil ssl-ssh aprimorado configuração, perfis IPS Admin restritos para suportar a transição e atualização de soluções IPS dedicadas, comandos personalizados no FortiSwitch e configuração do MCLAG a partir do FortiSwitch Manager.

Backups automatizados de configuração de dispositivos e controle de revisão tornam as tarefas administrativas diárias fácil. Rastreie as alterações na exibição aprimorada do Log de eventos para revisar as atualizações de configuração para auditoria e conformidade.

## **SD-WAN segura**

O FortiManager oferece recursos poderosos de gerenciamento de SD-WAN usando fluxos de trabalho intuitivos e provisionamento simplificado em escala. Aproveite as políticas de negócios SD-WAN centradas em aplicativos para ajustar as decisões de direcionamento de tráfego com base em metas de contrato de nível de serviço (SLA) de desempenho para cada provedor de WAN.

Simplifique e acelere a configuração de SD-WAN em escala global com SD-WAN automatizada provisionamento de sobreposição. Utilize esquemas de dispositivos para grandes implantações de SD-WAN com suporte para importe modelos CSV e atribua variáveis de metadados.

## Máquinas Virtuais do FortiManager

As máquinas virtuais FortiManager são uma versão virtual do dispositivo de hardware e são projetadas para rodar em muitas plataformas de virtualização, oferecendo todos os recursos mais recentes do FortiManager utensílio. Eles permitem que as organizações gerenciem centralmente qualquer número de rede Fortinet dispositivos de segurança e escala de vários a milhares, suportando gerenciamento centralizado, conformidade com as melhores práticas e fluxos de trabalho automatizados para fornecer proteção superior contra ameaças. FortiManager-VMs estão disponíveis em uma assinatura e oferta perpétua.

### FortiManager-VM-S

O novo modelo de licença de assinatura FortiManager-VM consolida o SKU do produto VM e o FortiCare Premium Support SKU em um único SKU para simplificar a compra do produto, atualização e renovação.

Os SKUs FortiManager-VM S Series vêm em assinaturas empilháveis para gerenciar 10, 100 e 1000 dispositivos/VDOMs. Várias unidades deste SKU podem ser compradas de uma só vez para aumentar o número de dispositivos/VDOMs conforme necessário. Este SKU também pode ser adquirido com outros FortiManager-VM-S SKUs para expandir o número total de dispositivos/VDOMs.

### FortiManager-VM

A Fortinet oferece o FortiManager-VM em um modelo de licença empilhável. Este software baseado A versão do dispositivo de hardware FortiManager foi projetada para rodar em muitos sistemas de virtualização plataformas, o que permite expandir sua solução virtual à medida que seu ambiente se expande.

A família de dispositivos virtuais FortiManager minimiza o esforço necessário para monitorar e manter sua rede e oferece todos os recursos do dispositivo de hardware FortiManager.

## Specifications

FORTIMANAGER VIRTUAL APPLIANCES	FMG-VM-10-UG	FMG-VM-100-UG	FMG-VM-1000-UG	FMG-VM-5000-UG
Capacity				
Devices/VDOMs (Default) <sup>1,3</sup>	10 +	100 +	1000 +	5000 +
GB/ day of Logs <sup>2</sup>	2	5	10	25
Chassis Management	✓	✓	✓	✓
Virtual Machine				
Hypervisor Support	Up-to-date hypervisor support can be found in the release notes for each FortiManager version. Visit <a href="https://docs.fortinet.com/product/fortimanager/">https://docs.fortinet.com/product/fortimanager/</a> and find the Release Information at the bottom section. Go to "Product Integration and Support" → "FortiManager [version] support" → "Virtualization"			
vCPU Support (Min / Max)	4 / Unlimited			
Network Interface Support (Min / Max) <sup>4</sup>	1 / 12			
Memory Support (Min / Max)	8 GB / Unlimited for 64-bit			
High Availability Support	Yes			

1 Each virtual domain (VDOM) operating on a physical or virtual device counts as one (1) licensed network device.

2 GB/ day of logs are not stackable. These values represent the maximum available with purchased license.

3 VM SKUs are stackable up to 100 000 Devices/VDOMs.

4 VM supports up to 12 vNIC interfaces/ports. Applicable to 6.4.3+. Actual consumable numbers vary depending on cloud platforms.

## 2.5. FortiAuthenticator



### Política de Identidade de Rede Corporativa

O acesso à rede e à Internet é essencial para quase todas as funções dentro da empresa; no entanto, esse requisito deve ser ponderado com o risco que ele traz. A chave objetivo de toda empresa é fornecer acesso à rede seguro, mas controlado permitindo à pessoa certa o acesso certo na hora certa, sem comprometer sobre segurança.

O Fortinet Single Sign-On é o método de fornecer identidade segura e acesso à rede conectada Fortinet. Através da integração com o Active existente Sistemas de autenticação de diretório ou LDAP, permite que o usuário corporativo baseado em identidade segurança sem atrapalhar o usuário ou gerar trabalho para administradores de rede.

O FortiAuthenticator se baseia nas bases do Fortinet Single Sign-on, adicionando uma gama maior de métodos de identificação do usuário e maior escalabilidade.

O FortiAuthenticator é o guardião da autorização no Fortinet protegido rede corporativa identificando usuários, consultando permissões de acesso de terceiros sistemas partidários e comunicar essas informações aos dispositivos FortiGate para uso em Políticas baseadas em identidade.

O FortiAuthenticator oferece identificação transparente por meio de uma ampla variedade de métodos:

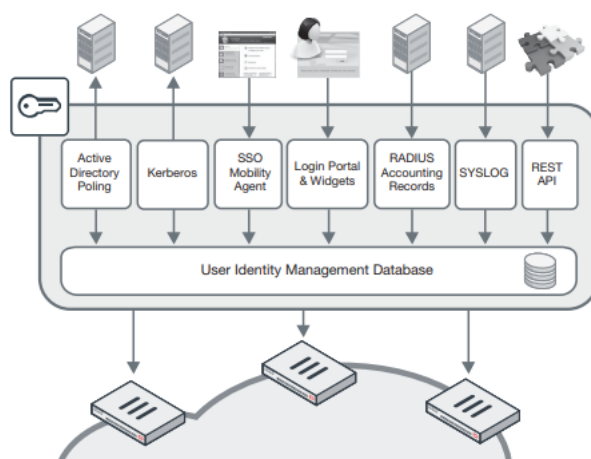
- Sondagem de um controlador de domínio do Active Directory
- Integração com o FortiAuthenticator Single Sign-On Mobility Agent que detecta login, alterações de endereço IP e logout
- Autenticação baseada em Portal FSSO com widgets de rastreamento para reduzir a necessidade de autenticações repetidas
- Monitoramento de registros de início de contabilidade RADIUS

## Usuário de logon único do FortiAuthenticator

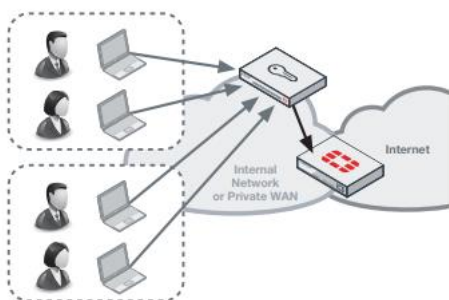
### Métodos de Identificação

FortiAuthenticator pode identificar usuários através de um intervalo variado de métodos e integrar com LDAP de terceiros ou Active Sistemas de diretório para aplicar dados de grupo ou função ao usuário e comunique-se com o FortiGate para uso em identidade baseada políticas. O FortiAuthenticator é completamente flexível e pode utilizar esses métodos em combinação. Por exemplo, em um grande empresa, sondagem AD ou FortiAuthenticator SSO Mobility

Agente pode ser escolhido como o método principal para transparência autenticação com fallback para o portal para não domínio sistemas ou usuários convidados.



### Sondagem do Active Directory

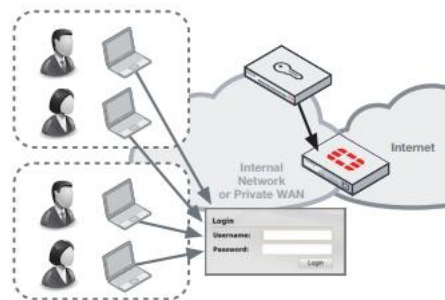


A autenticação do usuário em um diretório ativo é detectada pelo domínio de pesquisa regular controladores. Quando um login de usuário é detectado, o nome de usuário, IP e detalhes do grupo são inseridos no banco de dados de gerenciamento de identidade do usuário FortiAuthenticator e de acordo com a política local, pode ser compartilhado com vários dispositivos FortiGate.



## Portal FortiAuthenticator e Widgets

Para sistemas que não suportam polling de AD ou onde um cliente não é viável, FortiAuthenticator fornece um portal de autenticação explícita. Este portal permite os usuários se autenticarem manualmente no FortiAuthenticator e, posteriormente, na rede. Para minimizar o impacto de logins repetidos necessários para autenticação, um conjunto de widgets é fornecido para incorporação em uma organização intranet que conecta automaticamente os usuários com cookies do navegador sempre que eles acessar a página inicial da intranet



## Funcionalidade adicional

Identidade de usuário forte com autenticação multifator FortiAuthenticator estende a autenticação multifator capacidade para vários dispositivos FortiGate e para terceiros soluções que suportam autenticação RADIUS ou LDAP.

Informações de identidade do usuário do FortiAuthenticator combinadas com informações de autenticação do FortiToken e/ou O serviço de autenticação FIDO2 garante que apenas autorizados os indivíduos têm acesso aos recursos da sua organização informação sensível. Essa camada adicional de segurança reduz muito a possibilidade de vazamentos de dados enquanto ajuda empresas atendem aos requisitos de auditoria associados a regulamentos de privacidade do governo e dos negócios.

O FortiAuthenticator oferece a mais ampla gama de multifatores autenticação possível incluindo FIDO2 sem senha serviço de autenticação para atender às suas necessidades de usuário. Com o FortiToken 200 baseado em tempo físico, FortiToken Mobile (para iOS, Android e Windows), e-mail/SMS OTP, bem como FIDO2, FortiAuthenticator tem fortes opções de autenticação para todos os usuários e cenários.

A autenticação multifator pode ser usada para controlar o acesso a aplicativos como gerenciamento FortiGate, SSL e VPN IPsec, login Wireless Captive Portal e terceiros,

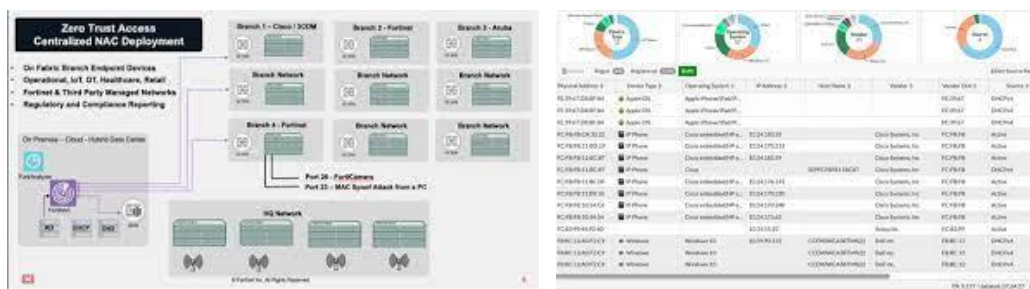
Equipamento de rede compatível com RADIUS e Serviço SAML Provedores. O FortiAuthenticator também oferece uma API REST que pode ser usado para adicionar MFA a qualquer aplicativo baseado na web.



## SPECIFICATIONS

FORTIAUTHENTICATOR MODEL NO.	FAC-300F	FAC-800F
Hardware		
10/100/1000 Interfaces (Copper, RJ-45)	4	4
SFP Interfaces	0	2
Local Storage	2× 1TB Hard Disk Drive	2× 2 TB Hard Disk Drive
Trusted Platform Module (TPM)	Yes	Yes
Power Supply	300W Redundant Auto Ranging (100V-240V), Optional Dual (1+1)	Dual (1+1) 300W Redundant Auto Ranging (100V-240V)
System Capacity		
Local + Remote Users (Base / Upper Limit)	1500 / 3500	8000 / 18 000
FortiTokens	3000	16 000
RADIUS Clients (NAS Devices)	500	2666
User Groups	150	800
CA Certificates	10	50
User Certificates	7500	40 000
Dimensions		
Height x Width x Length (inches)	1.75 x 17.0 x 15.04	1.75 x 17.0 x 27.61
Height x Width x Length (mm)	44 x 438 x 422	44 x 438 x 701.2
Weight	18.0 lbs (8.2 kg)	33.0 lbs (15.0 kg)
Environment		
Form Factor	Rack Mountable (1RU)	Rack Mountable (1RU)
Power Source	100-240 VAC, 50/60 Hz 300W Redundant (1+0)	100-240V AC, 50/60 Hz
Maximum Current	5A /100V, 2.5A /240V	5A /100V, 2.5A /240V
Power Consumption (Average / Maximum)	82.35 W / 131.23 W	154 W / 196.04 W
Heat Dissipation	482 BTU/h	703 BTU/h
Forced Airflow	Front to back	Front to back
Operating Temperature	32°-104°F (0°-40°C)	32°-104°F (0°-40°C)
Storage Temperature	-4°-158°F (-20°-70°C)	-4°-158°F (-20°-70°C)
Humidity	5%-90% non-condensing	5%-95% non-condensing
System		
Standards Supported	10/100/1000 Base-TX (GE), IP, Telnet, HTTP 1.0/1.1, SSL, RS232, NTP Client (RFC1305), RADIUS (RFC2865), LDAP (RFC4510), x.509 (RFC5280), Certificate Revocation (RFC3280), PKCS#12 Certificate Import, PKCS#10 CSR Import (RFC2986), Online Certificate Status Protocol (RFC 2560), EAP-TLS (RFC2716), Simple Certificate Enrollment Protocol (SCEP), oAuth, OIDC, and SAML2.0	
Management	CLI, Direct Console DB9 CLI, HTTPS	
High Availability	Active-Passive HA and Config Sync HA	
Compliance		
Safety	FCC Part 15 Class A, RCM, VCCI, CE, UL/cUL, CB	FCC Part 15 Class A, RCM, VCCI, CE, BSMI, KC, UL/cUL, CB, GOST

## 2.6. FortiNAC



FortiNAC™ é uma solução de controle de acesso à rede que permite organizações gerenciarem facilmente suas políticas de acesso à rede e garantir a conformidade com as políticas de segurança. Ele oferece um abrangente visualização de todos os dispositivos e usuários na rede, permitindo granular controle de acesso com base em funções de usuário, tipos de dispositivos e rede

### Localizações.

A solução fornece integração automatizada de novos endpoints, bem como como monitoramento contínuo e correção de dispositivos não compatíveis.

O FortiNAC também se integra a soluções de segurança de terceiros e oferece recursos avançados de relatórios e análises para maior visibilidade e relatórios de conformidade. Com o FortiNAC, as organizações podem proteger sua rede contra acesso não autorizado e ameaças potenciais.

## **Destaques**

### **Visibilidade do dispositivo**

Fundamental para a segurança de uma rede em constante mudança é a compreensão de sua inventar. O FortiNAC vê tudo na rede, fornecendo visibilidade completa. FortiNACGenericName verifica sua rede para descobrir cada usuário, aplicativo e dispositivo. Com até 21 diferentes técnicas, o FortiNAC pode então perfilar cada elemento com base nas características observadas e respostas, além de chamar os Serviços de IoT do FortiGuard, um banco de dados baseado em nuvem para pesquisas de identificação.

A varredura pode ser feita ativa ou passivamente e pode utilizar agentes permanentes, solúveis agentes, ou nenhum agente. Além disso, o FortiNAC pode avaliar um dispositivo para ver se ele corresponde perfis, observando a necessidade de atualizações de software para corrigir vulnerabilidades. Com o FortiNAC implantado, toda a rede é conhecida.

Além de conhecer toda a rede, a visibilidade aprimorada do FortiNAC também pode usar passiva análise de tráfego, aproveitando os dispositivos Fortinet FortiGate como sensores, para identificar anomalias padrões de tráfego, uma possível indicação de comprometimento que pode ser acompanhada pela equipe SOC.

### **Controle Dinâmico de Rede**

Uma vez que os dispositivos são classificados e os usuários são conhecidos, o FortiNAC permite segmentação da rede para permitir que dispositivos e usuários acessem os recursos necessários enquanto bloqueando o acesso não autorizado. O FortiNAC usa controle dinâmico de acesso à rede baseado em função para criar logicamente segmentos de rede agrupando aplicativos e dados semelhantes para limitar acesso a um grupo específico de usuários e/ou dispositivos. Desta forma, se um dispositivo for comprometido, sua capacidade de viajar na rede e atacar outros ativos será limitada. O FortiNAC ajuda a proteger dados críticos e ativos confidenciais, garantindo a conformidade com as normas internas, do setor e regulamentos e mandatos governamentais.

Garantir a integridade dos dispositivos antes de se conectarem à rede minimiza o risco e a possível disseminação de malware. O FortiNAC valida a configuração de um dispositivo à medida que ele tenta ingressar a rede. Se a configuração não for compatível, o dispositivo pode ser manipulado apropriadamente, como por uma VLAN de acesso isolado ou limitado que não tem acesso a recursos.

### **Resposta automática**

O FortiNAC monitorará a rede continuamente, avaliando os endpoints para garantir que eles de acordo com seu perfil. O FortiNAC verificará novamente os dispositivos para garantir que a falsificação de endereço MAC não ignore sua segurança de acesso à rede. Além disso, o FortiNAC pode observar anomalias nos padrões de tráfego. Essa detecção passiva de anomalias funciona em conjunto com o FortiGate aparelhos. Depois que um endpoint comprometido ou vulnerável é detectado como uma ameaça, o FortiNAC aciona uma resposta automatizada para conter o terminal em tempo real.

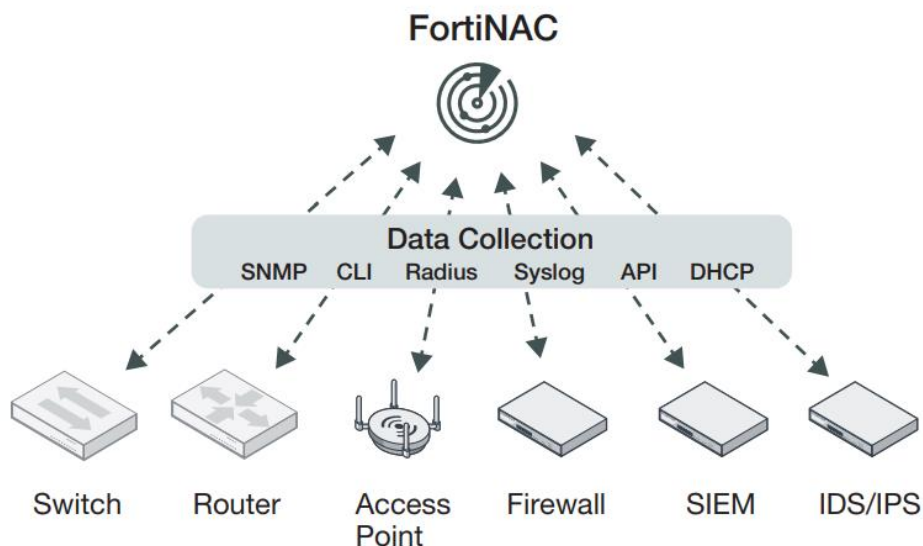
### Arquitetura centralizada

O FortiNAC é uma solução 'fora da banda', o que significa que não fica em linha com o tráfego do usuário.

A arquitetura permite que o FortiNAC seja implantado centralmente e gerencie muitos locais remotos. Visibilidade, controle e resposta são alcançados integrando e alavancando o capacidades da infra-estrutura de rede. O controle pode ser aplicado no ponto de conexão, na borda da rede, enquanto as integrações de dispositivos de segurança permitem que o FortiNAC processe alertas de segurança e tratá-los como gatilhos para mitigação automatizada de ameaças por meio de fluxos de trabalho.

A coleta de dados é coletada de várias fontes usando uma variedade de métodos. SNMP, CLI,

As impressões digitais RADIUS, SYSLOG, API e DHCP podem ser usadas para obter a visibilidade detalhada de ponta a ponta necessária para criar um ambiente verdadeiramente seguro.



## Licensing

		FORTINAC LICENSE TYPES	BASE	PLUS	PRO	
Visibility	Network	Network Discovery	✓	✓	✓	
		Rogue Identification	✓	✓	✓	
		Device Profiling and Classification	✓	✓	✓	
	Endpoint	Enhanced Visibility	✓	✓	✓	
		Anomaly Detection	✓	✓	✓	
		MDM Integration	✓	✓	✓	
		Persistent Agent	✓	✓	✓	
	User	Authentication		✓	✓	
		Captive Portal		✓	✓	
	Automation / Control		Network Access Policies	✓	✓	✓
		IoT Onboarding with Sponsor	✓	✓	✓	
		Rogue Device Detection and Restriction	✓	✓	✓	
		Firewall Segmentation	✓	✓	✓	
		MAC Address Bypass (MAB)	✓	✓	✓	
		Full RADIUS (EAP)	✓	✓	✓	
		BYOD / Onboarding		✓	✓	
		Guest Management		✓	✓	
		Endpoint Compliance		✓	✓	
		Web and Firewall Single Sign-on	✓	✓	✓	
Incident Response			Event Correlation			✓
			Extensible Actions and Audit Trail			✓
		Alert Criticality and Routing			✓	
		Guided Triage Workflows			✓	
		Inbound Security Events			✓	
Integrations		Outbound Security Events	✓	✓	✓	
		REST API	✓	✓	✓	
Reporting		Customizable Reports	✓	✓	✓	

## Specifications

	FNC-M-550C	FNC-CA-600C	FNC-CA-500C
System			
CPU	Intel Xeon Silver 4210 2.2G, 10C/20T, 9.6GT/s, 13.75M Cache, Turbo, HT (85W) DDR4-2400 (Qty 2)		Intel Xeon E-2124 3.3GHz, 8M cache, 4C/4T, turbo (71W) (Qty 1)
Memory	8GB RDIMM, 3200MT/s, Single Rank (Qty 4)		8GB 2666MT/s DDR4 ECC UDIMM (Qty 2)
Hard Disk	1TB 7.2K RPM SATA 6 Gbps 2.5in Hot-plug Hard Drive (Qty 2)		1TB 7.2K RPM SATA 6 Gbps 3.5in Hot-plug Hard Drive RAID1 (Qty 2)
BMC	iDRAC9 Express, integrated (Qty 1)		iDRAC8 Express (Qty 1)
Network Interface	4x 10/100/1000 Ethernet, RJ45		4x 10/100/1000 Ethernet, RJ45
RAID Card	PERC H330 Integrated RAID Controller (Qty 1)		PERC H330 Integrated RAID Controller (Qty 1)
RAID Configuration	RAID 1		RAID 1
Console Access	Yes *		Yes *
Form Factor	1U Rack Mountable		1U Rack Mountable
Dimensions			
Height x Width x Length (inches)	1.68 x 18.9 x 29.73		1.68 x 17.08 x 24.60
Height x Width x Length (mm)	42.8 x 482.4 x 755.12		42.8 x 434.0 x 625.0
Weight	43.056 lbs (19.76 kg)		43.87 lbs (19.9 kg)
Environment			
Power Supply	Dual 550W Hot Plug Power Supply		Dual 350W Hot Plug Power Supplies
Input Power	100-240V AC Autoranging		100-240V AC Autoranging
Input Current	6.25 A		3.0 A
Cooling	7 fans		4 fans
Panel Display	No LCD		20 Char LCD
Heat Dissipation	2559 BTU/hr		1357.1 BTU/hr
Operation Temperature Range	50°~95°F (10°~35°C)		50°~95°F (10°~35°C)
Storage Temperature Range	-40°~149°F (-40°~65°C)		-40°~149°F (-40°~65°C)
Humidity (Operating)	10%~80% non-condensing		10%~80% non-condensing
Humidity (Non-operating)	5%~95% non-condensing		5%~95% non-condensing
Certification			
Safety	Certified as applicable by Product Safety authorities worldwide, including United States (NRTL), Canada (SCC), European Union (CE).		
Electromagnetic (EMC)	Certified as applicable by EMC authorities worldwide, including United States (FCC), Canada (ICES), European Union (CE).		
Materials	Certified as applicable by Materials authorities worldwide, including European Union (ROHS) and China (ROHS).		

### 2.6.1. Lista de Materiais

Part Number	Description	Qty
FAP-231F-N	Indoor Wireless AP - Tri radio (802.11 b/g/n/ax 2x2 MU-MIMO, 802.11 a/n/ac/ax 2x2 MU-MIMO and 1x 802.11 a/b/g/n/ac Wave 2, 1x1 ), internal antennas, 2x 10/100/1000 RJ45 port, BT/BLE, 1x Type A USB, 1x RS-232 RJ45 Serial Port. Ceiling/wall mount kit included. For power order: 802.3at PoE injector GPI-130 or AC adapter SP-FAP250-PA-10. Region Code N	2331
FC-10-PF231-247-02-60	FortiCare Premium Support	2331
FAP-431F-N	Indoor Wireless FortiAP - Tri radio (2x 802.11 a/b/g/n/ac/ax, 4x4 MIMO and 1x 802.11 a/b/g/n/ac Wave 2, 2x2 MU-MIMO), internal antennas, 1x 100/1000/2500 Base-T RJ45, 1x 10/100/1000 Base-T RJ45, BT/BLE, 1x Type A USB, 1x RS-232 RJ45 Serial Port. Ceiling/wall mount kit included. For power order: 802.3at PoE injector GPI-130 or AC power adaptor SP-FAP400-PA. Region Code N	732
FC-10-F431F-247-02-60	FortiCare Premium Support	732
FAP-831F-N	Indoor Wireless AP - Tri radio (802.11 b/g/n/ax 4x4 MU-MIMO, 802.11 a/n/ac/ax 8x8 MU-MIMO and 1x 802.11 a/b/g/n/ac Wave 2, 2x2 ), internal antennas, 1x 100/1000/2500/5000 Base-T RJ45, 1x 10/100/1000 Base-T RJ45, BT / BLE, 1x RS-232 RJ45 Serial Port. Ceiling/wall mount kit included. For power order: 802.3at PoE injector GPI-130 or AC adapter SP-FAP400-PA. Region Code N	111

FC-10-P831F-247-02-60	FortiCare Premium Support	111
FAP-234F-N	Outdoor Wirelss AP - Tri radio (802.11 b/g/n/ax 2x2 MU-MIMO, 802.11 a/n/ac/ax 2x2 MU-MIMO and 1x 802.11 a/b/g/n/ac Wave 2, 1x1 ), internal antennas, 2x 10/100/1000 RJ45 port, BT/BLE, 1x Type A USB, 1x RS-232 RJ45 Serial Port. Pole/wall mount kit and PoE injector included. Region Code N	187
FC-10-P234F-247-02-60	FortiCare Premium Support	187
FG-1101E	2x 40GE QSFP+ slots , 4x 25GE SFP28 slots, 4x 10GE SFP+ slots, 8x GE SFP slots, 18x GE RJ45 ports (including 16x ports, 2x management/HA ports) SPU NP6 and CP9 hardware accelerated, 960GB SSD onboard storage, and 2 AC power supplies	2
FC-10-F11E1-247-02-60	FortiCare Premium Support	2
FN-TRAN-SFP+SR	10GE SFP+ transceiver module, short range for systems with SFP+ and SFP/SFP+ slots	8
FG-61F	10 x GE RJ45 ports (including 2 x WAN Ports, 1 x DMZ Port, 7 x Internal Ports), 128GB SSD onboard storage.	6
FC-10-0061F-247-02-60	FortiCare Premium Support	6
FG-81F	8 x GE RJ45 ports, 2 x RJ45/SFP shared media WAN ports, 128GB SSD	11
FC-10-0081F-247-02-60	FortiCare Premium Support	11
FG-101F	22 x GE RJ45 ports (including 2 x WAN ports, 1 x DMZ port, 1 x Mgmt port, 2 x HA ports, 16 x switch ports with 4 SFP port shared media), 4 SFP ports, 2x 10G SFP+ FortiLinks, 480GB onboard storage, dual power supplies redundancy.	3
FC-10-F101F-247-02-60	FortiCare Premium Support	3
FG-201F	18 x GE RJ45 (including 1 x MGMT port, 1 X HA port, 16 x switch ports), 8 x GE SFP slots, 4 x 10GE SFP+ slots, NP6X Lite and CP9 hardware accelerated, 480GB onboard SSD storage.	2
FC-10-F201F-247-02-60	FortiCare Premium Support	2
FG-401F	18 x GE RJ45 ports (including 1 x MGMT port, 1 X HA port, 16 x switch ports), 8 x GE SFP slots, 8 x 10GE SFP+ slots, SPU NP7 and CP9 hardware accelerated, 960GB onboard SSD storage, dual AC power supplies	3
FC-10-0401F-247-02-60	FortiCare Premium Support	3
FG-601F	4x 25G SFP28 slots, 4 x 10GE SFP+ slots, 18 x GE RJ45 ports (including 1 x MGMT port, 1 X HA port, 16 x switch ports), 8 x GE SFP slots, SPU NP7 and CP9 hardware accelerated, 480GB onboard SSD storage, dual AC power supplies	1
FC-10-0601F-247-02-60	FortiCare Premium Support	1
FMG-VM-10-UG	Upgrade license for adding 10 Fortinet devices/Virtual Domains; allows for total of 2 GB/Day of Logs and 200 GB storage capacity.	6
FC2-10-M3004-248-02-60	FortiCare Premium Support (1 - 110 devices/Virtual Domains)	2
FAZ-VM-GB100	Upgrade license for adding 100 GB/Day of Logs.	2
FC-10-L01KF-247-02-60	FortiCare Premium Support	2
FAC-VM-BASE	VM Base License supports 100 users. Expand user support to 1 million plus users by using FortiAuthenticator VM Upgrade License. Unlimited vCPU. Supporting VMware ESXi / ESX, Microsoft Hyper-V, Linux Kernel-based Virtual Machine (KVM) on Virtual Machine Manager and QEMU 2.5.0, and Xen Virtual Machine platforms	2
FAC-VM-10000-UG	FortiAuthenticator-VM 10000 users license upgrade	6
FAC-VM-1000-UG	FortiAuthenticator-VM 1000 users license upgrade	6
FAC-VM-100-UG	FortiAuthenticator-VM 100 users license upgrade	14
FC5-10-0ACVM-248-02-60	FortiCare Premium Support (1 - 50100 USERS)	2
FNC-CAX-VM	FortiNAC Control and Application next-gen VM Server (VMWare/Hyper-V/AWS/Azure/KVM).	2
FC-10-FNVXA-248-02-60	FortiCare Premium Support	2



LIC-FNAC-PLUS-10K	FortiNAC PLUS License for 10K concurrent endpoint devices. All the functionality of BASE with more advanced Network Access Controls and automated provisioning for users, guests, and devices.	3
LIC-FNAC-PLUS-1K	FortiNAC PLUS License for 1K concurrent endpoint devices. All the functionality of BASE with more advanced Network Access Controls and automated provisioning for users, guests, and devices.	3
LIC-FNAC-PLUS-100	FortiNAC PLUS License for 100 concurrent endpoint devices. All the functionality of BASE with more advanced Network Access Controls and automated provisioning for users, guests, and devices.	7
FC2-10-FNAC0-240-02-60	FortiCare Premium Support (100 Endpoints) for FortiNAC PLUS deployments.	337
GPI-130	GPI-130 Gigabit PoE Injector 1-Port Gigabit PoE Power Injector, 802.3at up to 30W for GPI-130 Gigabit PoE Injector	3174
FN-TRAN-SX	1GE SFP SX transceiver module 1GE SFP SX transceiver module for systems with SFP and SFP/SFP+ slots	374
CABO-PWR-NBR	Cabo de alimentação padrão Brasil	3174
CONVERSOR DE MIDIA	Conversor de Midia ótico-RJ45	748

### 2.6.2. Garantia do fabricante

Esta proposta contempla o serviço de garantia do fabricante para todos os equipamentos e softwares ofertados por um período de **60 (Sessenta) meses** contados da data de entrega dos mesmos na modalidade 24x7x4.

Durante esse período os Serviços de Manutenção e Suporte Técnico serão prestados sem qualquer ônus pelo Fabricante. Inclui-se na Garantia a cobertura completa de todos os defeitos de fabricação e excluindo-se todo e qualquer defeito decorrente de mau uso do equipamento.

### 2.7. Prestadoras de serviços contratadas pela vivo empresas

A **Vivo Empresas** poderá subcontratar serviços para a execução do contrato sendo totalmente responsável pelos mesmos.

### 2.8. Responsabilidades do cliente

- Informar à **Vivo Empresas** sobre qualquer mudança com relação à prestação dos serviços, com a devida antecedência, permitindo que a mesma tenha tempo suficiente para preparar e implementar as alterações necessárias, conforme tais alterações ou mudanças afetem a prestação dos serviços. O cliente deverá fornecer informações suficientes com relação às suas necessidades.
- Zelar pela conservação e correto manuseio da infraestrutura disponibilizada pela **Vivo Empresas**, responsabilizando-se pelos eventuais danos, pessoais e materiais, decorrentes de ações e utilizações indevidas por parte de seu pessoal ou de seus equipamentos.
- Toda e qualquer infraestrutura interna às suas unidades relacionadas com a solução ora apresentada, tais como: fornecimento de espaço e/ou ambiente, racks, rede interna, dutos e tubulações, obras civis, tomadas e energia, climatização etc. exceto menção contrária contida nesta Proposta.

### 3. CONSIDERAÇÕES FINAIS

A **Vivo Empresas** agradece e coloca-se à disposição da **MINISTERIO DA JUSTIÇA** para esclarecer quaisquer dúvidas referentes a esta Proposta e, desde já, se compromete em fornecer os melhores produtos/serviços e atendimento de alta qualidade em todas as etapas do processo de forma a atingir os objetivos desta solicitação.

Para garantir o sucesso da implementação da solução ofertada nesta Proposta, a **Vivo Empresas** ressalta que é imprescindível que os pré-requisitos e premissas do Projeto, constantes desta Proposta, sejam atendidos.

Quaisquer serviços, atividades ou produtos não previstos nesta Proposta, ou seja, modificações de escopo, mas que venham a se mostrar indispensáveis, necessárias ou convenientes no decorrer dos trabalhos, deverão ser objeto de renegociação entre a **Vivo Empresas**, e a **MINISTERIO DA JUSTIÇA** devendo ser revisto o planejamento das demais atividades e dimensionados os recursos adicionais e acordados junto ao responsável solicitante. De modo que a **Vivo Empresas** se reserva o direito de alterar sua Proposta Técnica e Comercial, caso posteriormente sejam constatadas relevantes informações e/ou *baselines* diferentes dos fornecidos inicialmente pelo Cliente.

Desde já a **MINISTERIO DA JUSTIÇA** aceita e concorda que a **Vivo Empresas** poderá dar publicidade do presente Projeto, a qualquer tempo, em mídia impressa e eletrônica, no território brasileiro ou fora dele, exclusivamente para divulgação de case, sem que se caracterize uso indevido de marca, nome comercial, imagem e/ou de quaisquer direitos do Cliente.

Demais condições deverão ser regidas nos termos de Contrato específico a ser firmado entre as partes.

#### 3.1. Confidencialidade

A **Vivo Empresas** está ciente que as informações contidas neste documento são confidenciais e não deverão ser divulgadas fora do âmbito desta sem uma prévia autorização da **MINISTERIO DA JUSTIÇA** ao mesmo tempo em que solicitamos a **MINISTERIO DA JUSTIÇA** tal consideração para as informações contidas nesta Proposta.