

## Jose Aparecido Flor de Souza

---

**De:** Leandro Dos Santos Vieira <leandro.svieira@telefonica.com>  
**Enviado em:** terça-feira, 29 de agosto de 2023 12:55  
**Para:** DTI - Licitação  
**Cc:** Eduardo Alex Peixoto Ruiz; Nelson Nogueira Buzeto; Guilherme Marques Miranda; Joao Cesar de Oliveira; Rosenilda Da Costa  
**Assunto:** RES: Diligência em análise de proposta G1 - Pregão 002-2023 DTI/PF

Prezado Pregoeiro, bom dia!  
Tudo bem?

### Segunda parte quanto aos esclarecimentos:

- indicar ou comprovar a homologação válida da ANATEL para os equipamentos ofertados, conforme subitem 1.4.4 do Anexo 1 do TR;  
**1.4.4. Os equipamentos (pontos de acesso e controladora) deverão possuir certificado válido referente à homologação da Agência Nacional de Telecomunicações (ANATEL) no momento da apresentação das propostas. Não serão aceitos documentos provisórios ou de entrada para obtenção da certificação.**  
→ Resposta: Segue comprovação de que os equipamentos ofertados possuem certificação da Anatel através do link: <https://fortinet.egnyte.com/fl/0swsjZpNMu>. Password: Ju9E7BJq
- apontar a comprovação de que o modelo de Power injector apresentado funciona em multigiga, conforme determina o subitem 12.4 do Anexo 1 do TR e para atender aos AP nos Itens 2 e 3 do objeto;  
**12.4. Deve possuir 2 portas RJ-45 fêmea, uma para conectar ao switch não PoE, outra para fornecer energia e dados para o ponto de acesso. Ambas as portas devem operar em compatibilidade com o AP fornecido (multigiga nos casos necessários);**  
→ Resposta: Item atendido conforme consta na página 1(um) do link: <https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortiap-accessories.pdf>.  
O modelo do Power Injector considerado para os tipos 2 e 3 de Access Points foi o modelo GPI-130 possui suporte ao 802.3at conforme descrito na página 1 do link <https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortiap-accessories.pdf>.  
A escolha do modelo GPI 130 que possui suporte a 802.3at, conforme descrito no link anteriormente informado, foi realizada por ser o padrão utilizado pelos FortiAP 431F (tipo 2) e FortiAP 831F-N (Tipo 3) descritos na página 39 do link <https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortiap-series.pdf>
- esclarecer se a proposta da licitante, segundo a lista de *Part-Number* e para cada equipamento nos Itens 1 a 4 e nos termos do subitem 2.9 do Anexo 1 do TR, é para fornecimento de Power Injector ou de adaptador de alimentação elétrica;  
**2.9. A alimentação dos Pontos de Acesso descritos nos itens 1 a 4, deverá, a princípio, ser através do dispositivo Power Injector com as configurações mínimas especificadas no item 08;**  
→ Resposta: Os modelos GPI-130 possuem suporte ao 802.3at conforme descrito na página 1 do link <https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortiap-accessories.pdf>
- indicar a comprovação de que os equipamentos nos Itens 1 a 4, em conjunto com a controladora (Item 5), suportam no mínimo o protocolo SNMPv2c e suporte a MIB para obtenção no mínimo de informações de capacidade e desempenho, conforme subitens 2.20, 2.21 e 7.42 a 7.44, todos do Anexo 1 do TR;

**2.20. Implementar, em conjunto com a controladora *wireless* (item 5), padrões abertos de gerência de rede no mínimo no protocolo SNMPv2c, e suporte a MIB (*Management Information Base*).**

**7.42. Implementar, pelo menos, os padrões abertos de gerência de rede SNMPv2c e SNMPv3, incluindo a geração de *traps***

**7.44. Implementar a MIB privativa que forneça informações relativas ao funcionamento do equipamento e disponibilizar descrição completa da mesma.**

à Resposta: No ponto a ponto foi apresentado o suporte dos Access Points as versões de SNMPv2c e SNMPv3, e também ao suporte a queries e mensagens de traps, pelo link

<https://docs.fortinet.com/document/fortiap/7.4.0/fortiwifi-and-fortiap-configuration-guide/930384/monitoring-fortiap-with-snmp>, como descrito:

#### FortiAP SNMP implementation



Simple Network Management Protocol (SNMP) queries and trap messages based on wireless-controller SNMP settings configured on FortiGate is supported on the following:

- FortiAP-S and FortiAP-W2 version 6.2.0 and later.
- FortiAP 6.4.3 and later.
- FortiAP-U 6.0.4 and later.

All SNMP versions (v1, v2, and v3) are supported.

Também está disponível as MIBs privativas, para os Access Points, como observado no mesmo link:

The SNMP manager requires the following management information base (MIB) files:

- FortiAP MIB
- Fortinet Core MIB

E também para a controladora via link <https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/608160/mib-files>, onde se apresenta todas as MIBs disponíveis.

- esclarecer a comprovação da implementação do MRC nos Access Points (itens 1 a 4), conforme subitem 2.22 do Anexo 1 do TR;

**2.22. Implementar *Maximum Ratio Combining* (MRC) no *Access Point*, ou equivalente**

- ➔ Resposta: Maximum-Ratio Combining (MRC) é definido dentro do PHY layer do padrão 802.11n ou (802.11n-2009 HT-Clause 20) e todos os modelos de access points ofertados possuem suporte a 802.11n, o que pode ser comprovado no link

<https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortiap-series.pdf>

- esclarecer a comprovação da implementação de cliente DHCP para os AP nos Itens 1 a 4, assim como endereçamento IP estático, conforme subitem 2.23 do Anexo 1 do TR;

**2.23. Implementar cliente DHCP, para configuração automática do seu endereço IP assim como endereçamento IP estático.**

- ➔ Resposta: No ponto a ponto foi apresentado as forma que o Access Point possui para sua descoberta e autorização pela controladora. O link da documentação pode ser observado por <https://docs.fortinet.com/document/fortiap/7.4.0/fortiwifi-and-fortiap-configuration-guide/540137/discovering-authorizing-and-deauthorizing-fortiap-units>, onde as forma de Descoberta podem ser tanto como IP estático “Static” como via DHCP, entre outros.

For a FortiGate acting as an AP controller (AC) to discover a FortiAP unit, the FortiAP must be able to reach the AC. A FortiAP with the factory default configuration has various ways of acquiring an AC's IP address to reach it.

WTP Configuration

AC Discovery Type: ☒ Auto ☐ Static ☐ DHCP ☐ DNS ☐ FortiCloud ☐ Broadcast ☐ Multicast

AC IP Address 1: 10.0.0.5

AC IP Address 2:

AC IP Address 3:

AC Host Name 1: \_capwap-control.\_udp.exam

AC Host Name 2:

AC Host Name 3:

AC Discovery Multicast Address: 224.0.1.140

AC Discovery DHCP Option Code: 138

FortiCloud Account:

FortiCloud Password:

AP Data Channel Security: ☒ Clear Text ☒ IPsec Enabled ☒ DTLS Enabled

Apply

AC discovery type	Description
Auto	The FortiAP attempts to be discovered in the below ways sequentially within an endless loop.
Static	The FortiAP sends discover requests to a preconfigured IP address that an AC owns.
DHCP	The FortiAP acquires the IP address of an AC in DHCP option 138 (the factory default) of a DHCP offer, which the FortiAP acquires its own IP address from.

- esclarecer a comprovação do quantitativo de VLAN suportadas para os AP nos Itens 1 a 5, conforme subitens 3.4, 4.8, 5.8, 6.10 e 7.71, todos do Anexo 1 do TR;

**3.4. Suportar, no mínimo, 8 (oito) VLANs**

**4.8. Suportar, no mínimo, 16 (dezesseis) VLANs.**

**5.8. Suportar, no mínimo, 16 (dezesseis) VLANs.**

**6.10. Suportar, no mínimo, 8 (oito) VLANs.**

**7.71. Suportar a configuração de até 4000 (quatro mil) VLANs ativas.**

- ➔ Resposta: A solução ofertada como controladora, o modelo FortiGate 1101E, pode ser observado pela documentação o suporte a 16384 interfaces, onde estas pode ser VLANs. Dessa forma é comprovada que o equipamento suporta as quatro mil VLANs ativas. O link para a documentação é <https://docs.fortinet.com/max-value-table>, onde é possível filtrar por modelo e verificar o número de interfaces, como na figura abaixo:

Show 10 entries Search: system.interface

Object	FortiGate 1101E
system.interface	16384
system.interface.mac	600
system.interface:dhcp-snooping-server-list	2048
system.interface:ipv6:ip6-prefix-list	32
system.interface:secondaryip	256

Showing 1 to 5 of 5 entries (filtered from 341 total entries) Previous 1 Next

Para os Access Points, não existe um número de VLANs suportados para cada AP. Pela documentação, é possível observar que clientes da rede Wifi são capazes de se conectarem a uma rede e serem atribuídos a uma VLAN <https://docs.fortinet.com/document/fortiap/7.4.0/fortiwifi-and-fortiap-configuration-guide/376326/configuring-dynamic-user-vlan-assignment>. Como exemplo, cada cliente pode ser atribuído a um pool de VLAN, como observado pela documentação <https://docs.fortinet.com/document/fortiap/7.4.0/fortiwifi-and-fortiap-configuration->

[guide/084238/vlan-assignment-by-vlan-pool](https://docs.fortinet.com/guide/084238/vlan-assignment-by-vlan-pool). A controladora ofertada é capaz de suportar até 64 pools de VLANs por SSID, como observado pelo link <https://docs.fortinet.com/max-value-table>, também filtrando pelo modelo FG-1101E.

Show 10 entries	Search: vlan-pool
Object	FortiGate 1101E
wireless-controller.vap:vlan-pool	64

Atenciosamente,



**Leandro dos Santos Vieira**

Gerente de Negócios  
Gerência Governo Federal  
Diretoria Governo B2B Vendas Diretas  
SMAS Trecho 1 - Guará, Ed. ParkShopping Corporate  
Torre 1 - 1º Andar - Brasília – DF CEP 71215-300  
+55 11 61 9 9639 -5804

**De:** Leandro Dos Santos Vieira

**Enviada em:** terça-feira, 29 de agosto de 2023 11:15

**Para:** DTI - Licitação <cpl.selic.dad.dti@pf.gov.br>

**Cc:** Eduardo Alex Peixoto Ruiz <eduardoalex.eapr@pf.gov.br>; Nelson Nogueira Buzeto <nelson.nnb@pf.gov.br>; Guilherme Marques Miranda <miranda.gmm@pf.gov.br>; Joao Cesar de Oliveira <cesar.jco@pf.gov.br>; Rosenilda Da Costa <rosenilda.costa@telefonica.com>

**Assunto:** ENC: Diligência em análise de proposta G1 - Pregão 002-2023 DTI/PF

Prezado Pregoeiro, bom dia!  
Tudo bem?

**Primeira parte:**

Em anexo segue o certificado de parceria junto ao fabricante Fortinet e Anexo Técnico porém, como os arquivos são muito grandes, o restante serão enviados em outros e-mails.

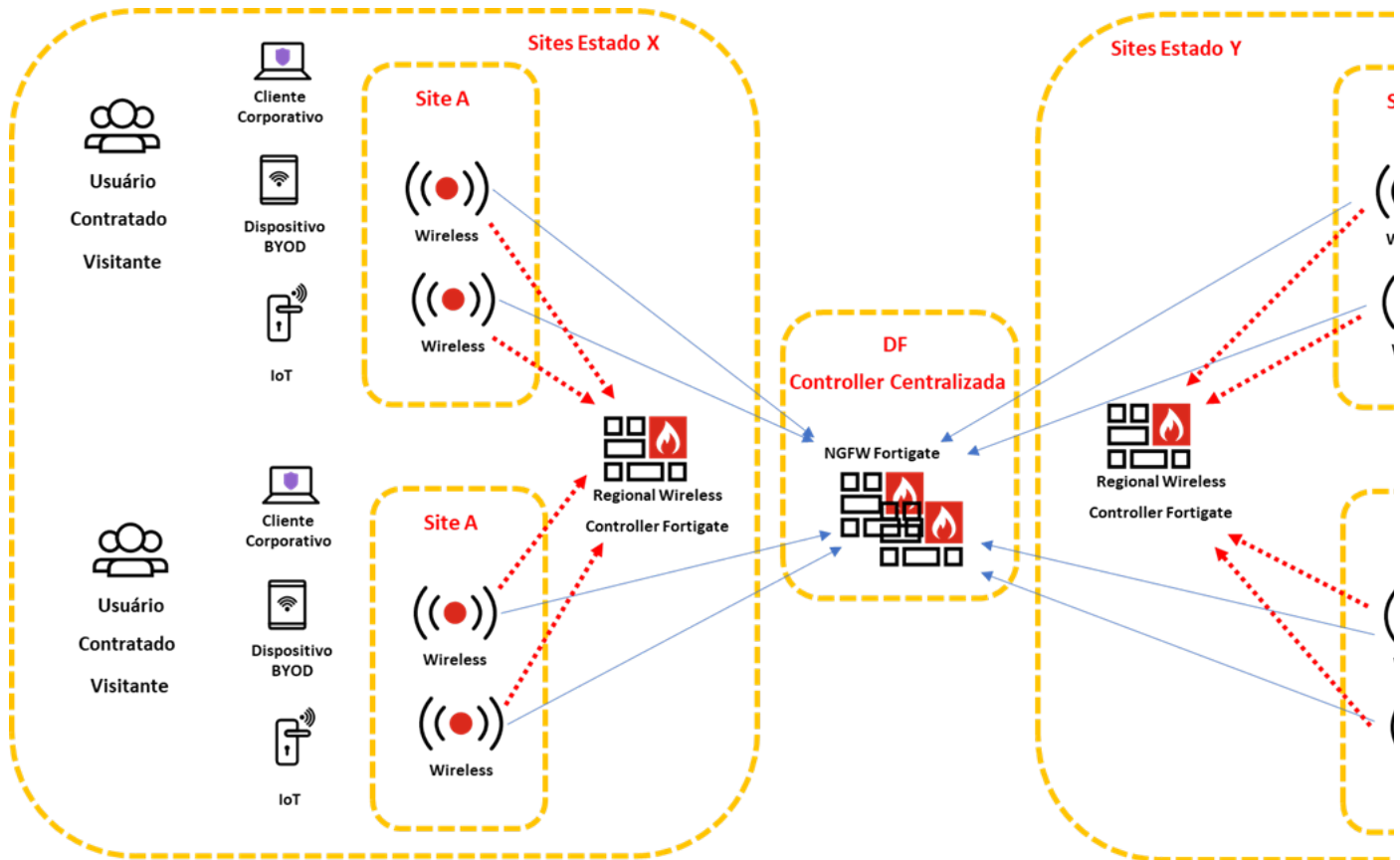
Peço a gentileza de aceitar tendo em vista que algumas documentações já foram enviadas no momento do cadastro da proposta e estamos confirmando para indicar os itens que foram apresentados.

- indicar ou comprovar a homologação válida da ANATEL para os equipamentos ofertados, conforme subitem 1.4.4 do Anexo 1 do TR;
- 1.4.4. Os equipamentos (pontos de acesso e controladora) deverão possuir certificado válido referente à homologação da Agência Nacional de Telecomunicações (ANATEL) no momento da apresentação das propostas. Não serão aceitos documentos provisórios ou de entrada para obtenção da certificação.**
- ➔ Resposta: Segue em anexo (Arquivo: “Anatel”) comprovação de que os equipamentos ofertados possuem certificação da Anatel

- apontar a aderência dos AP (Itens 1 a 4) ao subitem 2.5 do Anexo 1 do TR, no que tange ao Access Points operarem como controladoras;

**2.5. Os Pontos de Acesso fornecidos deverão possuir capacidade de operar como controladores *wireless*, sendo possível gerenciar, no mínimo, 24 Pontos de Acesso;**

→ Resposta: Com objetivo de prover a redundância dos Access Points em caso de falha de comunicação com a Controladora Wireless central uma controladora wireless regionalizada em cada estado esta sendo ofertada. Essa mesma controladora wireless regional, além permitir a redundância adicional aos sites de uma particular região, permite a implementação de funcionalidades como SDWAN adicionalmente, conforme descrito na topologia abaixo. Item atendido conforme item 2.2 do Anexo Técnico (anexo).



- apontar o atendimento ao subitem 6.4 do anexo 1, em que prevê uma porta SFP para o AP tipo 4, outdoor;

**6.4. Para equipamentos *outdoor* deverá possuir pelo menos 1(uma) interface 1000 Base T Ethernet, auto-sensing, auto MDI/MDX, com conector RJ-45, para conexão com a rede local – LAN e deverá possuir pelo menos 1 (um) slot SFP (*Small Form-factor Pluggable*) para operação em 1Gbps e para conexão de *transceiver* de fibra óptica multimodo para possível implementação do AP em distâncias superiores a 100m do *switch* de acesso, caso não possua slot SFP deverá ser fornecido conversor de mídia junto do equipamento;**

→ Resposta: Conforme item 2.7.1 do Anexo Técnico (anexo), foram considerados a utilização de conversores de media de fibra para RJ-45

- apontar, conforme subitem 7.16 do Anexo 1 do TR, a capacidade de conexão simultânea de 34.000 (trinta e quatro mil) dispositivos ou clientes à controladora;

**7.16. Cada *cluster* de controladoras deve permitir a conexão simultânea de, no mínimo, 34.000 (trinta e quatro mil) clientes (dispositivos) *wireless*, mesmo em caso de indisponibilidade de uma das controladoras. O número mínimo de conexões foi baseado nas estruturas de (wi-fi) já existentes na Polícia Federal, onde, no pico, temos uma média de 10 acessos simultâneos por Pontos de Acesso. Cabe ressaltar que os acessos simultâneos envolvem não só usuários mas também equipamentos que podem ser conectados na rede (wi-fi), como celulares, impressoras, *notebooks*, etc.**

Resposta: A Controller Proposta não possui uma limitação de número de usuários e possui suporte a 8 milhões de conexões simultâneas conforme indicado no item Concurrent Sessions (TCP) descrito na página 8 do link (<https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-1100e-series.pdf>). Utilizando a média de 10 acessos simultâneos por usuários a controladora deveria suportar de 340000, as 8 milhões de conexões suportadas atendem à demanda das 340000.

- indicar o ponto de comprovação da atuação da gerência conforme especificado no item 8.26, do anexo 1 do TR, abstendo de informar endereço de internet indisponível;

**8.26. Identificação de áreas sem cobertura de sinal (*coverage holes*) com capacidade para efetuar os devidos ajustes para a correção automática das áreas de sombras.**

→ Resposta: O FortiAP permite que o administrador determinar a área de cobertura de um Access Points conforme descrito no link (<https://docs.fortinet.com/document/fortiap/7.4.0/fortiwifi-and-fortiap-configuration-guide/821879/determining-the-coverage-area-of-a-fortiap>) adicionalmente existem funcionalidades adicionais para ambientes de alta densidade para mitigar possíveis gaps de cobertura conforme link <https://docs.fortinet.com/document/fortiap/7.4.0/fortiwifi-and-fortiap-configuration-guide/702421/features-for-high-density-deployments>

- demonstrar em documentação oficial do fabricante, conforme subitem 2.1.4 do Anexo 1 do TR, a comprovação de que os equipamentos, produtos ou softwares ofertados não constam em listas do tipo end-of-sale, end-of-support ou end-of-life do fabricante;

**2.1.4. Não serão aceitos equipamentos, produtos ou *softwares* que, no momento de entrega ao CONTRATANTE, constem em listas do tipo *end-of-sale*, *end-of-support* ou *end-of-life* do fabricante, ou seja, produtos que em breve serão descontinuados, perderão suporte e garantia oficiais do fabricante.**

→ Resposta: Item atendido conforme Certificado de Parceria anexo.

- apontar onde consta que a controladora no Item 5 comuta, entre controladoras, em modo de alta disponibilidade, em menos de dois segundos de tempo de interrupção de serviço, e sincroniza automaticamente as configurações entre as controladoras, quando em modo de operação de alta disponibilidade, conforme subitens 7.24 e 7.25 do Anexo 1 do TR;

**7.24. Comutação entre controladoras, em modo de alta disponibilidade, inferior a dois segundos de tempo de interrupção de serviço da rede sem fio;**

→ Resposta: No ponto a ponto foi apresentado a configuração de Failover da alta disponibilidade da solução, onde é possível observar a possibilidade de configuração de timing de heartbeat, exemplo 100 milissegundos ou 10 milissegundos.

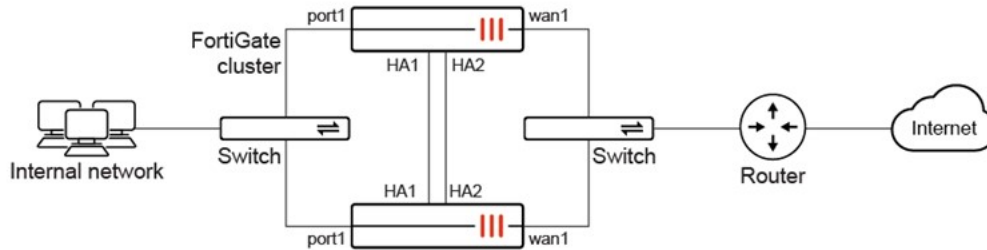


## Configuring HA failover time

On supported models, the HA heartbeat interval unit can be changed from the 100ms default to 10ms. This allows for a failover time of less than 50ms, depending on the configuration and the network.

```
config system ha
    set hb-interval-in-milliseconds {100ms | 10ms}
end
```

In this example, the HA heartbeat interval unit is changed from 100ms to 10ms. As the default heartbeat interval is two, this means that a heartbeat is sent every 20ms. The number of lost heartbeats that signal a failure is also changed to two. So, after two consecutive heartbeats are lost, a failover will be detected in 40ms.



Como descrito na documentação, no exemplo onde o intervalo do heartbeat for alterado para 10ms, o failover irá ser detectado e acontecer em 40 milissegundos. Este é só um exemplo dos timers que pode ser utilizados. Sobre sincronização, toda a configuração é sincronizada, com exceção de alguns pontos específicos como hostname, prioridades dos membros de HÁ, como observado do documento pelo link <https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/62403/fgcp>, como na figura abaixo:

### Synchronizing the configuration

FGCP uses a combination of incremental and periodic synchronization to make sure that the configuration of all cluster units is synchronized to that of the primary unit.

The following settings are not synchronized between cluster units:

- The FortiGate host name
- GUI Dashboard widgets
- HA override
- HA device priority
- The virtual cluster priority
- The HA priority setting for a ping server (or dead gateway detection) configuration
- The system interface settings of the HA reserved management interface
- The HA default route for the reserved management interface, set using the `ha-mgmt-interface-gateway` option of the `config system ha` command

Most subscriptions and licenses are not synchronized, as each FortiGate must be licensed individually. FortiToken Mobile is an exception; they are registered to the primary unit and synchronized to the secondary units.

The primary unit synchronizes all other configuration settings, including the other HA configuration settings.

- indicar onde consta que a controladora no Item 5 permitir que os SSID operem em modo de comutação de tráfego local, conforme subitem 7.31 do Anexo 1 do TR;

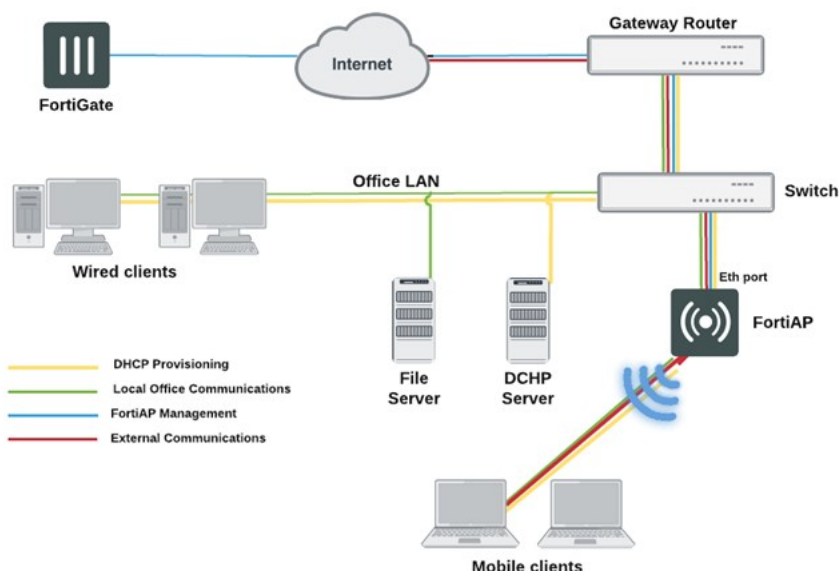
### 7.31. Permitir que os SSIDs operem em modo de tunelamento de tráfego remoto ou comutação de tráfego local.

- ➔ Resposta: No ponto a ponto foi apresentado a configuração de um SSID onde é possível a configuração do modo do tráfego entre modo "Tunnel" e modo "Bridge". Segue o link para <https://docs.fortinet.com/document/fortiap/7.4.0/fortiwifi-and-fortiap-configuration-guide/307228/defining-a-wireless-network-interface-ssid>, onde pode ser observado:

Traffic Mode	<p><i>Tunnel</i> — (Tunnel to Wireless Controller) Data for WLAN passes through WiFi Controller. This is the default.</p> <p><i>Bridge</i> — (Local bridge with FortiAP Interface) FortiAP unit Ethernet and WiFi interfaces are bridged.</p> <p><i>Mesh</i> — (Mesh Downlink) Radio receives data for WLAN from mesh backhaul SSID.</p>
--------------	--

Em modo bridge, a comutação do tráfego é feita de forma local, como observado pelo link de configuração <https://docs.fortinet.com/document/fortiap/7.4.0/fortiwifi-and-fortiap-configuration-guide/442078/how-to-configure-a-fortiap-local-bridge-private-cloud-managed-ap>,

Remotely-managed FortiAP providing WiFi access to local network:



- esclarecer a comprovação da implementação de DHCP *relay* e de mobilidade entre VLANs para *roaming* pelo menos na camada 2, para a controladora no Item 5, conforme subitens 7.70 e 7.72 do Anexo 1 do TR;

#### 7.70. Deverá implementar DHCP *relay*

- ➔ Resposta: Foi apresentado no ponto a ponto o link para a documentação do fabricante onde apresenta que na solução ofertada é capaz de ser configurada como DHCP Server e Relay. Para maior esclarecimento do item, apresentado outro link da documentação onde é possível observar a configuração necessária para a configuração do DHCP relay dentro da configuração do SSID, pelo link <https://docs.fortinet.com/document/fortiap/7.4.0/fortiwifi-and-fortiap-configuration-guide/307228/defining-a-wireless-network-interface-ssid>, onde pode ser observado:

DHCP Server	<p>To assign IP addresses to clients, enable DHCP server. You can define IP address ranges for a DHCP server on the FortiGate unit or <b>relay</b> DHCP requests to an external server.</p> <p>Note: If the unit is in transparent mode, the DHCP server settings will be unavailable.</p> <p>For more information, see <a href="#">Configuring DHCP for WiFi clients</a>.</p>
-------------	--

- esclarecer a comprovação de que a controladora no Item 5 implementa os padrões IEEE 802.11d, 802.11h, 802.11i, 802.11j, 802.11k e 802.11v, conforme subitens 7.99, 7.100 e 7.105 do Anexo 1 do TR;
- 7.99. Deve implementar os padrões IEEE 802.11d, IEEE 802.11h e IEEE 802.11i;**



→ Resposta: A solução ofertada suporta o padrão IEEE 802.11d com observado pelo documento [https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS\\_Wireless.pdf](https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS_Wireless.pdf), em sua página 8.

IEEE Standard Compliance	802.11ax, 802.11a, 802.11b, <b>802.11d</b> , 802.11g, 802.11k, 802.11n, 802.11r, 802.11v, 802.11w, 802.11ac, 802.1Q, 802.3ad, 802.3af, 802.3at, 802.3az, 802.11ax, 802.3bz
--------------------------	--

A solução ofertada suporta o padrão IEEE 802.11h como pode ser observado pelo documento <https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortiap-series.pdf>, em suas páginas 12, 16, 24 e 28.

IEEE Standards	802.11a, 802.11b, 802.11d 802.11i, 802.11j, 802.11k, 802.11l, 802.11n, 802.11p, 802.11q, 802.11r, 802.11s, 802.11t, 802.11u, 802.11v, 802.11w, 802.11x, 802.11y, 802.11z
----------------	---

A solução ofertada suporta o padrão IEEE 802.11i, com observado pelo documento [https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS\\_Wireless.pdf](https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS_Wireless.pdf), em sua página 8.

Roaming	Layer 3 roaming capable
	<b>802.11i</b> fast-roam back
	802.11i fast-associate in advance
	PMK caching

- indicar a comprovação de que a controladora no Item 5 tem conformidade com a RFC 3576/5176 (Change of Authorization), conforme subitem 7.112 do Anexo 1 do TR.

**7.112. Conformidade com a RFC 3576/5176 (Change of Authorization).**

→ Resposta: A solução ofertada suporta tanto as RFCs 3576 como 5176 como observado pelo link:

<https://docs.fortinet.com/document/fortigate/7.4.0/supported-rfcs/357205/radius>

→

Atenciosamente,



**Leandro dos Santos Vieira**

Gerente de Negócios  
Gerência Governo Federal  
Diretoria Governo B2B Vendas Diretas  
SMAS Trecho 1 - Guará, Ed. ParkShopping Corporate  
Torre 1 - 1º Andar - Brasília – DF CEP 71215-300  
+55 11 61 9 9639 -5804

**De:** DTI - Licitação <[cpl.sellic.dad.dti@pf.gov.br](mailto:cpl.sellic.dad.dti@pf.gov.br)>

**Enviada em:** terça-feira, 29 de agosto de 2023 08:47

**Para:** Leandro Dos Santos Vieira <[leandro.svieira@telefonica.com](mailto:leandro.svieira@telefonica.com)>

**Cc:** Eduardo Alex Peixoto Ruiz <[eduardoalex.eapr@pf.gov.br](mailto:eduardoalex.eapr@pf.gov.br)>; Nelson Nogueira Buzeto <[nelson.nnb@pf.gov.br](mailto:nelson.nnb@pf.gov.br)>;

Guilherme Marques Miranda <[miranda.gmm@pf.gov.br](mailto:miranda.gmm@pf.gov.br)>; Joao Cesar de Oliveira <[cesar.jco@pf.gov.br](mailto:cesar.jco@pf.gov.br)>

**Assunto:** ENC: Diligência em análise de proposta G1 - Pregão 002-2023 DTI/PF

**ATENÇÃO/WARNING:** Esta mensagem de e-mail se originou de fora da empresa. Não clique em links ou abra qualquer arquivo ao menos que reconheça o remetente e tenha certeza que o conteúdo é seguro.

Srs Licitante, **TELEFONICA BRASIL S.A./02.558.157/0001- 62 (Leandro dos Santos Vieira);**

Trata-se de **1ª DILIGÊNCIA TÉCNICA (Complementar) à PROPOSTA** apresentada ao G1 de ITENS do **Pregão Eletrônico SRP 002-2023 – WIFI** processo administrativo 08206.000155/2022-65;

Da análise dos documentos apresentados, a EQUIPE DE APOIO TÉCNICA DA DTI/PF apresentou as seguintes questões (abaixo) para manifestação da **TELEFONICA**, **considerando serem informações complementares que já deveriam constar dos documentos apresentados inicialmente**, SERÁ DADO PRAZO DE ATÉ 11h DE HOJE (29/08) para manifestação da empresa (envio das informações/documentos ao endereço [cpl.sellic.dad.dti@pf.gov.br](mailto:cpl.sellic.dad.dti@pf.gov.br)), **sob pena de RECUSA DA PROPOSTA APRESENTADA;**

#### **INFORMAÇÕES QUE DEVEM SER PRESTADAS PELA EMPRESA**

**Assunto:** Diligência em análise de proposta

Prezado Pregoeiro,

A EPC no Pregão 2/2023 entende ser necessária a seguinte diligência, na forma do item 8.6 do Edital, para que a licitante TELEFÔNICA BRASIL S/A esclareça inequivocamente, na documentação oficial da fabricante e anexa à Proposta, os seguintes pontos:

- indicar ou comprovar a homologação válida da ANATEL para os equipamentos ofertados, conforme subitem 1.4.4 do Anexo 1 do TR;
- apontar a aderência dos AP (Itens 1 a 4) ao subitem 2.5 do Anexo 1 do TR, no que tange ao Access Points operarem como controladoras;
- apontar o atendimento ao subitem 6.4 do anexo 1, em que prevê uma porta SFP para o AP tipo 4, outdoor;
- apontar, conforme subitem 7.16 do Anexo 1 do TR, a capacidade de conexão simultânea de 34.000 (trinta e quatro mil) dispositivos ou clientes à controladora;
- indicar o ponto de comprovação da atuação da gerência conforme especificado no item 8.26, do anexo 1 do TR, abstendo de informar endereço de internet indisponível;
- apontar a comprovação de que o modelo de Power injector apresentado funciona em multigiga, conforme determina o subitem 12.4 do Anexo 1 do TR e para atender aos AP nos Itens 2 e 3 do objeto;
- demonstrar em documentação oficial do fabricante, conforme subitem 2.1.4 do Anexo 1 do TR, a comprovação de que os equipamentos, produtos ou softwares ofertados não constam em listas do tipo end-of-sale, end-of-support ou end-of-life do fabricante;
- esclarecer se a proposta da licitante, segundo a lista de *Part-Number* e para cada equipamento nos Itens 1 a 4 e nos termos do subitem 2.9 do Anexo 1 do TR, é para fornecimento de Power Injector ou de adaptador de alimentação elétrica;
- indicar a comprovação de que os equipamentos nos Itens 1 a 4, em conjunto com a controladora (Item 5), suportam no mínimo o protocolo SNMPv2c e suporte a MIB para obtenção no mínimo

de informações de capacidade e desempenho, conforme subitens 2.20, 2.21 e 7.42 a 7.44, todos do Anexo 1 do TR;

- esclarecer a comprovação da implementação do MRC nos Access Points (itens 1 a 4), conforme subitem 2.22 do Anexo 1 do TR;
- esclarecer a comprovação da implementação de cliente DHCP para os AP nos Itens 1 a 4, assim como endereçamento IP estático, conforme subitem 2.23 do Anexo 1 do TR;
- esclarecer a comprovação do quantitativo de VLAN suportadas para os AP nos Itens 1 a 5, conforme subitens 3.4, 4.8, 5.8, 6.10 e 7.71, todos do Anexo 1 do TR;
- apontar onde consta que a controladora no Item 5 comuta, entre controladoras, em modo de alta disponibilidade, em menos de dois segundos de tempo de interrupção de serviço, e sincroniza automaticamente as configurações entre as controladoras, quando em modo de operação de alta disponibilidade, conforme subitens 7.24 e 7.25 do Anexo 1 do TR;
- indicar onde consta que a controladora no Item 5 permitir que os SSID operem em modo de comutação de tráfego local, conforme subitem 7.31 do Anexo 1 do TR;
- esclarecer a comprovação da implementação de DHCP *relay* e de mobilidade entre VLANs para *roaming* pelo menos na camada 2, para a controladora no Item 5, conforme subitens 7.70 e 7.72 do Anexo 1 do TR;.
- esclarecer a comprovação de que a controladora no Item 5 implementa os padrões IEEE 802.11d, 802.11h, 802.11i, 802.11, 802.11r, 802.11k e 802.11v, conforme subitens 7.99, 7.100 e 7.105 do Anexo 1 do TR;
- indicar a comprovação de que a controladora no Item 5 tem conformidade com a RFC 3576/5176 (Change of Authorization), conforme subitem 7.112 do Anexo 1 do TR.

Por se tratar de apontamentos técnicos certamente já de conhecimento da licitante, e que devem constar da documentação em sua proposta, sugere-se a concessão, à licitante TELEFÔNICA BRASIL S/A, do prazo razoável de até 2 horas, improrrogável, para cumprimento desta requisição em diligência.

Atenciosamente,

Nelson N. Buzeto

*Perito Criminal Federal*

*Integrante Técnico da EPC*

---

Este mensaje y sus adjuntos se dirigen exclusivamente a su destinatario, puede contener información privilegiada o confidencial y es para uso exclusivo de la persona o entidad de destino. Si no es usted, el destinatario indicado, queda notificado de que la lectura, utilización, divulgación y/o copia sin autorización puede estar prohibida en virtud de la legislación vigente. Si ha recibido este mensaje por error, le rogamos que nos lo comunique inmediatamente por esta misma vía y proceda a su destrucción.

The information contained in this transmission is confidential and privileged information intended only for the use of the individual or entity named above. If the reader of this message is not the intended recipient, you are hereby notified that any dissemination, distribution or copying of this communication is strictly prohibited. If you have received this transmission in error, do not read it. Please immediately reply to the sender that you have received this communication in error and then delete it.

Esta mensagem e seus anexos se dirigem exclusivamente ao seu destinatário, pode conter informação privilegiada ou confidencial e é para uso exclusivo da pessoa ou entidade de destino. Se não é vossa senhoria o destinatário indicado, fica notificado de que a leitura, utilização, divulgação e/ou cópia sem autorização pode estar proibida em virtude da legislação vigente. Se recebeu esta mensagem por erro, rogamos-lhe que nos o comunique imediatamente por esta mesma via e proceda a sua destruição