QUESTIONAMENTO 1:

Analisando o Anexo VI – Termo de Referência, nossa equipe de engenharia em Cibersegurança constatou a exigência de funcionalidades descritas com nomenclaturas comerciais proprietárias, o que pode restringir inadvertidamente a participação de fabricantes líderes globais no segmento de *Next-Generation Firewalls* (NGFW). Destacamos os seguintes pontos:

- Sobre o "VPN Matcher" (Itens 3.3.2.5.13 e 3.3.3.5.13): O termo "VPN Matcher" não é um protocolo de rede padronizado (RFC), mas sim um serviço de nuvem proprietário e exclusivo da fabricante *DrayTek*. A finalidade técnica desse serviço é auxiliar roteadores localizados atrás de NAT (CGNAT) a estabelecerem túneis VPN. Na indústria global de cibersegurança (fabricantes como Fortinet, Sophos, Cisco, SonicWall), essa exata mesma necessidade técnica é resolvida nativamente através de protocolos e arquiteturas consagradas, tais como:
    - **NAT Traversal (NAT-T - RFC 3947)** e protocolos **STUN/TURN**;
    - **Auto-Discovery VPN (ADVPN)** ou **Dynamic Multipoint VPN (DMVPN)**;
    - **Orquestração SD-WAN em Nuvem** (ex: FortiGate Cloud, Sophos Central SD-RED).
- Sobre o "Strict Bind" (Itens 3.3.2.10.4 e 3.3.3.10.4): O edital exige "Bind-IP-to-MAC com aplicação estrita/Strict Bind". O termo "Strict Bind" é a nomenclatura literal da interface do sistema operacional *DrayOS*. A finalidade técnica é a amarração rígida de um endereço IP ao endereço MAC do dispositivo, bloqueando o tráfego de máquinas não autorizadas. Os demais fabricantes de nível *Enterprise* entregam esse exato nível de controle de acesso (ou até superior) utilizando as seguintes nomenclaturas e protocolos de mercado:
    - **IP/MAC Binding** atrelado a políticas de firewall;
    - **Dynamic ARP Inspection (DAI)** e **DHCP Snooping**;
    - **Network Access Control (NAC)** e **Port Security**.

Considerando a determinação expressa no **Item 1.7 do Edital**, que orienta os licitantes a *"Desconsiderar qualquer menção à MARCA"*, e visando garantir a seleção da proposta mais vantajosa para a Administração Pública mediante a mais ampla concorrência:

Pergunta 1: Está correto o entendimento de que a Administração **aceitará** equipamentos que realizem o fechamento e a orquestração de túneis VPN por trás de NAT (CGNAT) utilizando tecnologias de mercado equivalentes ou superiores (como NAT-T, ADVPN, DMVPN ou Orquestração SD-WAN nativa do fabricante), considerando atendida a exigência do "VPN Matcher" estipulada nos itens 3.3.2.5.13 e 3.3.3.5.13?

Pergunta 2: Está correto o entendimento de que a Administração **aceitará** equipamentos que garantam a amarração rigorosa e o controle de acesso de dispositivos na rede por meio de tecnologias equivalentes (como IP/MAC Binding padrão, Dynamic ARP Inspection, DHCP Snooping ou NAC), considerando atendida a exigência de "Bind-IP-to-MAC com aplicação estrita/Strict Bind" estipulada nos itens 3.3.2.10.4 e 3.3.3.10.4?

QUESTIONAMENTO 2:

Avaliando as especificações técnicas descritas no Anexo VI – Termo de Referência, nota-se a exigência de suporte ao protocolo **TR-069** para funcionalidades de serviços locais, atualização de firmware e gerenciamento centralizado, conforme descrito nos **itens 3.3.2.12.2, 3.3.2.12.4 e 3.3.2.12.11** (para o Modelo II) e **itens 3.3.3.12.2, 3.3.3.12.4 e 3.3.3.12.11** (para o Modelo III).

Sob a ótica da Engenharia de Cibersegurança, o TR-069 (CPE WAN Management Protocol) é um protocolo legado padronizado pelo *Broadband Forum*, concebido prioritariamente para que Provedores de Internet (ISPs) realizem o gerenciamento básico de modems e roteadores residenciais (CPEs).

No atual mercado corporativo de *Next-Generation Firewalls* (NGFW), os fabricantes líderes globais (presentes nos quadrantes de referência da indústria) aboliram o uso do TR-069 por razões de arquitetura e segurança. O gerenciamento centralizado, monitoramento de status, provisionamento *Zero-Touch* (ZTP) e atualização de firmware em soluções de borda corporativa (SD-WAN/NGFW) são realizados hoje através de protocolos muito mais seguros e nativos de cada ecossistema (tais como túneis TLS/SSL criptografados dedicados, arquiteturas baseadas em REST API, CAPWAP, entre outros protocolos proprietários de gerência em nuvem ou *on-premise*).

Considerando a determinação do **Item 1.7** do Edital, que orienta os licitantes a *"Desconsiderar qualquer menção à MARCA"*, e visando não restringir a participação aos poucos fabricantes de roteadores SMB que ainda dependem deste protocolo legado:

Pergunta: Está correto o entendimento de que a Administração **aceitará** soluções de segurança que realizem o gerenciamento centralizado, a atualização de firmware, o monitoramento e o provisionamento remoto (*Zero-Touch Provisioning*) através de protocolos seguros nativos da arquitetura de gerência do fabricante ofertado (tais como plataformas de orquestração via túneis TLS dedicados, REST API ou gerenciadores centralizados do próprio fabricante), **considerando plenamente atendidas as exigências atreladas ao protocolo TR-069 descritas nos itens 3.3.2.12.2, 3.3.2.12.4, 3.3.2.12.11, 3.3.3.12.2, 3.3.3.12.4 e 3.3.3.12.11?**

Home
Sala/Modalidades
Editais e Processos
Editais Encerrados/Arquivados
Atas e Documentos
Recursos
Relatórios
Esclarecimentos
Impugnações
Apenados / Impedidos
Contratações - PNCP
Modelos de Documento
Dados de Mercado

CONSULTAR ESCLARECIMENTO

Solicitação respondida

Nome do Usuário	Participante
Usuário Sociedade	

Solicitação

Solicitação criada às 14:57 em 20/03/2026, última edição às 11:38 em 23/03/2026

Solicitamos esclarecimentos conforme documento em anexo.

Documentos da Solicitação

DOCUMENTOS
QUESTIONAMENTO_FIREWALL_PM_TAUBATE.pdf

Nome do Usuário	Participante
Thiago Telles de Faria	Prefeitura Municipal de Taubaté

Resposta

Resposta criada às 11:38 em 23/03/2026

Prezados, Seguem os esclarecimentos para os questionamentos apresentados: QUESTIONAMENTO 01 (Perguntas 1 e 2): Sim, o entendimento está correto. QUESTIONAMENTO 02: Sim, o entendimento está correto. Era o que tínhamos a informar. Atenciosamente, Alisson Ribeiro - SEDINT-DTI Guilherme Costa De Aguiar - SEDINT-DTI-ATI-DTI

VOLTAR