GOVERNO DO ESTADO DA BAHIA
Companhia de Processamento de Dados do Estado da Bahia
Diretoria de Infraestrutura Tecnológica e Conectividade - PRODEB/DTC

INFORMAÇÕES PARA PROCESSO

PROCESSO Nº 065.10933.2026.0003946-61

Interessado: Diretoria de Infraestrutura Tecnológica e Conectividade

Assunto: Resposta ao Questionamento - Empresa 01

EMPRESA 01

QUESTIONAMENTO 01 – Monitoramento de tráfego (sFlow)

Item 1.2.26.36 (e correlatos nos demais Tipos do LOTE 01 e LOTE 02)

"Deve suportar a funcionalidade de monitoramento de tráfego utilizando o protocolo sFlow."

NetFlow e IPFIX oferecem as mesmas capacidades funcionais de monitoramento de tráfego (coleta de estatísticas de fluxo, amostragem e exportação para coletores), sendo amplamente adotados e padronizados por RFCs do IETF (RFC 3954 – NetFlow v9; RFC 7011 – IPFIX). A exigência exclusiva do protocolo sFlow restringe injustificadamente o universo de fabricantes participantes, sem agregar valor funcional diferenciado, uma vez que ferramentas de coleta e análise de tráfego do mercado (incluindo as soluções de gerenciamento centralizado já existentes na PRODEB) suportam de forma nativa os três protocolos.

Desta forma solicitamos que o texto seja alterado para: **"Deve suportar a funcionalidade de monitoramento de tráfego utilizando o protocolo sFlow ou NetFlow ou IPFIX."**

A nossa solicitação será aceita?

RESPOSTA

Não. Mantido conforme Edital.

O requisito foi definido com base nas necessidades técnicas específicas da arquitetura pretendida, considerando uma rede WAN com mais de 4 mil pontos de acesso.

Em razão das características técnicas de funcionamento dos protocolos de telemetria, observa-se que o sFlow utiliza mecanismo de amostragem estatística, enviando menor quantidade de registros ao coletor. Tal característica proporciona redução no consumo de banda, armazenamento e processamento associados à telemetria da rede

QUESTIONAMENTO 02 – Roteamento WCCP e ICAP

Item 1.2.28.40 (e correlatos nos demais Tipos do LOTE 01 e LOTE 02)

“Deve implementar roteamento WCCP e ICAP.”

WCCP (Web Cache Communication Protocol) e ICAP (Internet Content Adaptation Protocol) são tecnologias legadas concebidas para arquiteturas baseadas em encadeamento externo de proxies e de appliances dedicados de inspeção de conteúdo. Os NGFWs modernos integram nativamente, no próprio dataplane, todas as funções que historicamente justificavam esses protocolos: inspeção SSL, filtragem web, antivírus, IPS e controle de aplicações.

A obrigatoriedade desses protocolos, na forma atual, não traz benefício funcional ao cenário desenhado pelo TR (NGFW + SD-WAN com inspeção ativa) e, na prática, atua como restrição ao universo de fabricantes participantes, sem ganho de segurança real.

Desta forma solicitamos que o texto seja alterado para: **“Deve implementar roteamento WCCP e ICAP ou dispor de proxy integrado nativamente ao NGFW, com modos de operação transparente e explícito, atendendo às mesmas funções de inspeção e adaptação de conteúdo.”**

A nossa solicitação será aceita?

RESPOSTA

Não. Mantido conforme Edital.

O requisito visa garantir interoperabilidade e flexibilidade em ambiente heterogêneo, possibilitando a integração com soluções externas de proxy e inspeção de conteúdo.

Mesmo com funcionalidades nativas em NGFW, o suporte a WCCP e ICAP assegura padronização no encadeamento de serviços e compatibilidade com diferentes cenários operacionais.

QUESTIONAMENTO 03

Item 1.2.30.15 (e correlatos nos demais Tipos do LOTE 01 e LOTE 02)

“Possuir agente de IPSEC client-to-site compatível com dispositivos móveis Android ou IOS;”

Os sistemas operacionais Android e IOS possuem clientes VPN nativos que suportam IPsec/IKEv2 de forma robusta, segura e amplamente utilizada em ambientes corporativos e governamentais. A exigência de agente proprietário do fabricante introduz custo adicional de distribuição, atualização e gestão (especialmente em frota heterogênea de dispositivos BYOD) sem agregar valor funcional. Adicionalmente, a interoperabilidade nativa via IKEv2 é hoje a melhor prática recomendada pelo NIST e pela comunidade de segurança, por reduzir superfície de ataque e simplificar a operação.

Desta forma solicitamos que o texto seja alterado para: **“Possuir agente de IPSEC client-to-site compatível com dispositivos móveis Android ou IOS, ou suportar conexão VPN IPsec/IKEv2 utilizando os clientes VPN nativos dos sistemas operacionais Android e IOS;”**

A nossa solicitação será aceita?

RESPOSTA

Não. Mantido conforme edital.

A utilização de múltiplos clientes VPN, associados a diferentes fabricantes, modelos e versões de dispositivos, eleva a complexidade operacional da solução, dificultando a padronização e a gestão do ambiente. além de dificultar o suporte técnico em razão da diversidade de plataformas e versões existentes.

QUESTIONAMENTO 04 – Restrição de tenants em aplicações SaaS via inserção de cabeçalhos HTTP

Item 1.2.31.15 (e correlatos nos demais Tipos do LOTE 01 e LOTE 02)

“A solução deve efetuar restrição de acesso a tenants/domínios específicos de aplicações SaaS, como Office 365 e Google Workspace, interceptando as solicitações de acesso dos usuários e inserindo cabeçalhos que indiquem ao serviço SaaS aplicar restrições de a tenants/domínios conforme uma lista pré-aprovada em cada serviço.”

A exigência de interceptar conexões HTTPS e inserir cabeçalhos específicos (Restrict-Access-To-Tenants, X-GoogApps-Allowed-Domains) para controle de tenants em aplicações SaaS não se alinha às melhores práticas atuais de segurança. Esse tipo de controle é nativamente tratado pelas próprias plataformas SaaS (Microsoft Entra ID Conditional Access, Google Context-Aware Access) e por soluções de identidade (IdP/IAM/SSO), sendo mais eficaz, seguro e auditável quando implementado na camada de autenticação.

A obrigatoriedade da implementação via NGFW restringe o universo de fabricantes a um número muito reduzido de soluções proprietárias, sem ganho de segurança real, uma vez que o objetivo (restrição de acesso a tenants/domínios pré-aprovados) é plenamente atendido por meio de políticas nativas de controle de aplicações e de filtragem de URL/domínio.

Desta forma solicitamos que o texto seja alterado para: **"A solução deve efetuar restrição de acesso a tenants/domínios específicos de aplicações SaaS, como Office 365 e Google Workspace, interceptando as solicitações de acesso dos usuários e inserindo cabeçalhos que indiquem ao serviço SaaS aplicar restrições de a tenants/domínios conforme uma lista pré-aprovada em cada serviço, ou por meio de políticas de controle de aplicações e filtragem de URL/domínio."**

A nossa solicitação será aceita?

RESPOSTA

Não. Mantido conforme Edital

Políticas baseadas exclusivamente em controle de aplicações e filtragem de URL/domínio não oferecem o mesmo nível de validação e restrição de acesso a tenants específicos em aplicações SaaS. A funcionalidade requerida visa garantir controle centralizado, transparente e aderente à camada de segurança da rede, assegurando que o acesso ocorra exclusivamente a tenants/domínios previamente autorizados.

QUESTIONAMENTO 05 – Filtros do YouTube por Channel ID e Categoria

Item 1.2.31.28 (e correlatos nos demais Tipos do LOTE 01 e LOTE 02)

"Deve permitir realizar filtros no YouTube baseado no ID do canal e na categoria;"

A redação atual exige cumulativamente o filtro por Channel ID E por categoria, o que é tecnicamente excessivo. Na prática operacional, qualquer uma das duas funcionalidades, isoladamente, atende ao objetivo de controle granular sobre o tráfego do YouTube em ambiente corporativo/governamental: o Channel ID permite bloqueio/liberação de canais específicos e a categoria permite controle por temática. A substituição da conjunção "e" por "ou" preserva o objetivo funcional do requisito e amplia o universo de fabricantes que podem competir no certame.

Desta forma solicitamos que o texto seja alterado para: **"Deve permitir realizar filtros no YouTube baseado no ID do canal ou na categoria;"**

A nossa solicitação será aceita?

RESPOSTA

Não. Mantido conforme edital.

As funcionalidades de filtragem por ID de canal e por categoria possuem finalidades complementares, permitindo diferentes níveis de granularidade e controle sobre o acesso ao conteúdo do YouTube. A exigência conjunta visa assegurar maior flexibilidade operacional e aderência aos requisitos de controle de conteúdo

QUESTIONAMENTO 06 – Segmentação de rede sobre "único overlay"

Item 1.2.32.29 (e correlatos nos demais Tipos do LOTE 01 e LOTE 02)

"Deverá possuir, garantir, implementar e permitir a segmentação de rede sobre um único overlay, possibilitando a criação de múltiplos segmentos de rede isolados logicamente, cada um com suas próprias políticas de roteamento, segurança e QoS, enquanto compartilham a mesma infraestrutura física subjacente;"

O termo “overlay”, no contexto de SD-WAN/NGFW, está historicamente associado a tecnologias específicas de determinados fabricantes (VXLAN, GRE, IPsec sobre overlay proprietário). O objetivo funcional pretendido pelo requisito – isolamento lógico de múltiplos segmentos de rede, cada um com suas próprias políticas de roteamento, segurança e QoS, sobre a mesma infraestrutura física – é plenamente atendido por mecanismos consolidados e padronizados como Zonas de Segurança, VLANs 802.1Q e interfaces virtuais (VDOMs/Contextos). A retirada do termo “overlay” torna o requisito tecnologicamente neutro e mais aderente à diversidade de arquiteturas NGFW disponíveis no mercado.

Desta forma solicitamos que o texto seja alterado para: **“Deverá possuir, garantir, implementar e permitir a segmentação de rede, possibilitando a criação de múltiplos segmentos de rede isolados logicamente, cada um com suas próprias políticas de roteamento, segurança e QoS, enquanto compartilham a mesma infraestrutura física subjacente;”**

RESPOSTA

Não. Mantido conforme Edital.

O conceito de overlay é amplamente adotado pelos principais fabricantes do mercado e visa garantir segmentação lógica fim a fim de forma transparente, abstraindo a necessidade de segmentação na infraestrutura do cliente.

Documento assinado eletronicamente por **Elmo dos Santos Sales**, **Assessor Especial**, em 25/05/2026, às 14:46, conforme horário oficial de Brasília, com fundamento no art. 13º, Incisos I e II, do Decreto nº 15.805, de 30 de dezembro de 2014.

A autenticidade deste documento pode ser conferida no site https://seibahia.ba.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **00140908057** e o código CRC **8321C4F4**.

Referência: Processo nº 065.10933.2026.0003946-61 SEI nº 00140908057