MINISTÉRIO DA AGRICULTURA, PECUÁRIA E ABASTECIMENTO
SECRETARIA EXECUTIVA
SUBSECRETARIA DE TECNOLOGIA DA INFORMAÇÃO
COORDENAÇÃO-GERAL DE INFRAESTRUTURA, SEGURANÇA E SERVIÇOS DIGITAIS
COORDENAÇÃO DE CIBERSEGURANÇA E PRIVACIDADE DE DADOS

DESPACHO

Processo nº 21000.020025/2023-02

À Subsecretaria de Planejamento, Orçamento e Administração - SPOA

Senhor(a) Subsecretário,

1. Trata-se dos autos da pretensa contratação de solução de proteção de rede com características de Next Generation Firewall (NGFW), cuja sessão pública está aberta desde o dia 15/04/2024, encontrando-se na fase de julgamento da proposta preços da CLARO AS, no valor global de R$ 5.193.781,65.

2. Para atendimento ao solicitado no despacho 112 SEI Nº 34774377, na coluna " Análise do MAPA" estão as respostas/análise do MAPA quanto ao atendimento dos requisitos solicitados no termo de referência:

DESCRIÇÃO DO ITEM	**ANÁLISE DO MAPA**
A comunicação entre os appliances de segurança e o módulo de gerência deve ser através de meio criptografado.	Requisito não atendido. O link enviado não demonstra o solicitado. O Documento apontado traz informações sobre a implementação de SD-WAN. Não há qualquer informação sobre a comunicação do módulo de gerência e os *appliances*.
A solução de balanceamento deverá ser fornecida em Alta Disponibilidade do tipo Ativo/Ativo.	Requisito não atendido. O link enviado não demonstra o solicitado. O Link informado traz informações sobre como configurar um SD-WAN em FGCP HA.
12 interfaces físicas de rede do tipo 10 GE SFP 28.	Requisito não atendido. No datasheet do equipamento, não é possível concluir que cada cluster consiga compor 10 interfaces. Considerando a interface "*25GE/10GE SFP28/SFP+ ULL (ultra-low latency) Slots*" , é possível chegar, no máximo, a 08 interfaces.
02 interfaces físicas de rede do tipo 40 Gbps QSFP+ ou superior.	Requisito não atendido. No datasheet do equipamento, não é possível concluir isso. Nenhuma interface do equipamento é de 40 GE. Ademais, o equipamento não possui qualquer interface que suporte 40GE, conforme solicitado. Resta evidente, portanto, que não se trata de uma questão interpretativa. O fabricante Fortinet possui equipamentos com interfaces solicitadas no edital, contudo esses não foram ofertados pela licitante.

Deve permitir que os arquivos de log sejam baixados da plataforma para uso externo.	Requisito não atendido. No link enviado, não há como concluir tal informação. O link apontado traz informação sobre a geração automática de relatórios, logo, não há correlação entre o solicitado e enviado.
Deve permitir que o relatório seja enviado por e-mail para o destinatário específico.	Requisito não atendido. No link enviado, O link apontado traz informação de como agendar relatórios, desta forma, não há como concluir que o equipamento tenha a capacidade de de enviar o relatório por e-mail.
Deve dispor de mecanismos para analisar a requisição TLS Client hello e o cabeçalho HTTP User-Agent para determinar e controlar se a requisição está partindo de um dispositivo não passível de gerenciamento pela console central, tal como um dispositivo móvel. A comunicação de controle entre os agentes e a console central deve ser criptografada e acontecer através de TCP e TLS 1.2 e 1.3. Tanto mediante agente ou sem agente deve ser possível habilitar MFA (autenticação multifator) no processo de autenticação dos usuários.	Requisito não atendido. No link enviado, não é possível concluir que os requisitos possam ser cumpridos. Por exemplo, não foi possível localizar nenhuma referência à TLS 1.2/1.3.
A console central deve emitir, assinar e instalar automaticamente um certificado para os agentes contendo ID único de cada agente, número de série do certificado e número de série da console central. O certificado emitido deverá ser único por agente e deverá ainda ser compartilhado com o proxy de acesso.	Requisito não atendido. No link enviado, não há qualquer menção sobre o que está sendo solicitado.
A solução deve prover backup automático diariamente, permitindo que em um evento crítico seja possível restaurar os dados de até 05 dias anteriores ao ocorrido.	Requisito não atendido. Ao acessar o link fornecido, não encontramos informações claras que atendam ao pedido.
A solução deve suportar casos de uso utilizando IPv6 puro, bem como IPv6 em conjunto com IPv4. Deve ser possível agrupar agentes em grupos e atribuir grupos de agentes a perfis de políticas específicas.	Requisito não atendido. Ao acessar o link fornecido, não encontramos informações claras que atendam ao solicitado.
Suporte a, no mínimo, 1024 VLAN Tags 802.1q, agregação de links 802.3ad, policy based routing ou policy based forwarding, roteamento multicast, DHCP Relay, DHCP Server e Jumbo Frames.	Requisito não atendido. Ao acessar o link fornecido, não encontramos informações claras que atendam ao solicitado.
Deverá suportar redundância e balanceamento de links, tendo capacidade de no mínimo 3 links de internet. Deverá suportar configurar um valor de threshold baseando-se em critérios mínimos como fator de decisão nas regras de balanceamento.	Requisito não atendido. Ao acessar o link fornecido, não encontramos informações claras que atendam ao solicitado.
Deve suportar a captura de pacotes (PCAP), em assinatura de IPS e Anti-Malware, através da console de gerência centralizada.	Requisito não atendido. Ao acessar o link fornecido, não encontramos informações claras que atendam ao pedido. O termo PCAP sequer é citado ao longo conteúdo.
Solução deve proteger contra os ataques do tipo DNS Cache Poisoning, e impedir que os usuários acessem endereços de domínios bloqueados.	Requisito não atendido. Ao acessar o link fornecido, não encontramos informações claras que atendam ao solicitado. O termo "*DNS cache poisoning*" nem foi citado ao longo do documento.
Os eventos devem identificar o país de onde partiu a ameaça.	Requisito não atendido. Ao acessar o link fornecido, não encontramos informações claras que atendam ao solicitado. Nenhuma informação sobre o solicitado foi encontrado.
A funcionalidade de IPS e anY-bot, deve possuir capacidade de correlacionar em seus logs a visibilidade de acordo com o framework ATT&CK Mitre Matrix, pontuando características de técnicas de acordo com a ameaça detecada/bloqueada pela solução. Caso a solução não possua determinada capacidade, poderá ser integrada com outra solução de mercado, não sendo ela soluções abertas.	Requisito não atendido. Ao acessar o link fornecido, não encontramos informações claras que atendam ao solicitado.
A solução Antivírus deverá suportar análise de arquivos que trafegam dentro do protocolo CIFS/SMB, de forma a conter malwares se espalhando horizontalmente pela rede.	Requisito não atendido. Ao acessar o link fornecido, não encontramos informações claras que atendam ao solicitado.
Deverá possuir a função resolução de endereços via DNS, para que conexões com destino a domínios maliciosos, sejam resolvidas pelo Firewall com endereços previamente definidos, para	Requisito não atendido. Ao acessar o link fornecido, não encontramos informações claras que atendam ao solicitado.

interceptar a comunicação e bloquear o acesso do usuário.	
A solução de Anti-malware deve ser capaz de detectar e interromper o comportamento anormal suspeito da rede.	Requisito não atendido. Ao acessar o link fornecido, não encontramos informações claras que atendam ao solicitado.
A solução deve possuir funcionalidade de identificação de bloqueio de tráfego malicioso comunicando com C&C (command & Control).	Requisito não atendido. Ao acessar o link fornecido, não encontramos informações claras que atendam ao solicitado.
A solução Antivírus deverá suportar a análise de links no corpo de e-mails.	Requisito não atendido. Ao acessar o link fornecido, não encontramos informações claras que atendam ao pedido.
Suportar marcação de pacotes diffserv.	Requisito não atendido. Ao acessar o link fornecido, não encontramos informações claras que atendam ao pedido.
Suportar a identificação de arquivos compactados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos.	Requisito não atendido. Ao acessar o link fornecido, não encontramos informações claras que atendam ao pedido.
A solução de balanceamento deve possuir a capacidade de, automaticamente, por meio de definições de thresholds, executar a realocação de equipamentos entre os clusters, ou o redirecionamento do tráfego sem a necessidade de intervenção física para este redirecionamento.	Requisito não atendido. Ao acessar o link fornecido, não encontramos informações claras que atendam ao pedido.
Permitir exportar, a partir da própria console de gerenciamento da solução, o resultado das análises de malwares do tipo “Zero Day” em arquivo tabulado, como .txt; .csv ou .pdf.	Requisito não atendido. Ao acessar o link fornecido, não encontramos informações claras que atendam ao pedido.
O “offload” de cerYficado em inspeção de conexões SSL de entrada (Inbound).	Requisito não atendido. Ao acessar o link fornecido, não encontramos informações claras que atendam ao pedido.
Descriptografar sites e aplicações que utilizam certificados ECC, incluindo Elliptical Curve Digital Signature Algorithm (ECDSA);	Requisito não atendido. Ao acessar o link fornecido, não encontramos informações claras que atendam ao pedido.
Deverá permiYr o espelhamento de tráfego descriptografado (SSL e TLS) para análise por meio de soluções externas de segurança, por exemplo, soluções de análise forense de rede, ferramentas de auditoria, Data Loss Prevention, etc.	Requisito não atendido. Ao acessar o link fornecido, não encontramos informações claras que atendam ao pedido.
Deverá suportar controles por zona de segurança.	Requisito não atendido. Ao acessar o link fornecido, não encontramos informações claras que atendam ao pedido.
Permitir a criação de sub-interfaces lógicas Ethernet.	Requisito não atendido. Ao acessar o link fornecido, não encontramos informações claras que atendam ao pedido.
Suportar leitura e verificação de CRL (certificate revocation list).	Requisito não atendido. Ao acessar o link fornecido, não encontramos informações claras que atendam ao pedido.
A solução deve mostrar nos logs as seguintes informações sobre domínios DGA (Domain Generation Algorithm): • Domínio suspeito identificado; • ID de assinatura de detecção; • Usuário logado na estação/servidor que originou o tráfego; • Aplicação; • Porta de destino; • IP de origem; • Horário; • Ação do firewall; • Severidade;	Requisito não atendido. Ao acessar o link fornecido, não encontramos informações claras que atendam ao pedido.

• A solução deve possuir sistema de análise automático para detectar e bloquear encapsulamento de DNS com fins de roubo de dados e comunicações de comando e controle.	
A solução deve detectar e bloquear em tempo real (inline) os artefatos maliciosos desconhecidos (zero day) no próprio GW através de mecanismos de Machine Learning.	Requisito não atendido. Ao acessar o link fornecido, não encontramos informações claras que atendam ao pedido.
Deve permitir informar ao fabricante quanto a suspeita de ocorrências de falso-positivo e falso-negativo na análise de malwares de dia Zero a partir da própria interface de gerência.	Requisito não atendido. Ao acessar o link fornecido, não encontramos informações claras que atendam ao pedido.
Deve prevenir contra-ataques sem arquivo buscando por atividade maliciosa em pelo menos nas seguintes linguagens de scripts: Powershell e Javascript.	Requisito não atendido. Ao acessar o link fornecido, não encontramos informações claras que atendam ao pedido.
A solução de proxy de acesso deve prover suporte a um método de publicação de aplicações corpora- tivas sem necessidade de agente, tal como mediante um portal web SSL a ser acessado por cada usuário.	Requisito não atendido. Ao acessar o link fornecido, não encontramos informações claras que atendam ao pedido.
Deve dispor de mecanismos para analisar a requisição TLS Client hello e o cabeçalho HTTP User-Agent para determinar e controlar se a requisição está partindo de um dispositivo não passível de ge- renciamento pela console central, tal como um dispositivo móvel. A comunicação de controle entre os agentes e a console central deve ser criptografada e acontecer através de TCP e TLS 1.2 e 1.3. Tanto mediante agente ou sem agente deve ser possível habilitar MFA (autenticação multifator) no processo de autenticação dos usuários.	Requisito não atendido. Ao acessar o link fornecido, não encontramos informações claras que atendam ao pedido.
A console central deve emitir, assinar e instalar automaticamente um certificado para os agentes con- tendo ID único de cada agente, número de série do certificado e número de série da console central. O certificado emitido deverá ser único por agente e deverá ainda ser compartilhado com o proxy de acesso.	Requisito não atendido. Ao acessar o link fornecido, não encontramos informações claras que atendam ao pedido.
O certificado emitido deve ser utilizado no processo de autenticação via ZTNA para identificar o dis- positivo do usuário final junto ao proxy de acesso.	Requisito não atendido. Ao acessar o link fornecido, não encontramos informações claras que atendam ao pedido.
No passo de identificação do dispositivo mediante certificado deve ser possível averiguar se o identi- ficador único do agente e número do certificado coincidem com o que o proxy de acesso conhece. Caso algum desses dados esteja diferente, o acesso deverá ser bloqueado por padrão.	Requisito não atendido. Ao acessar o link fornecido, não encontramos informações claras que atendam ao pedido.
Deve ser possível configurar o idioma que o agente utiliza para, pelo menos, inglês, português, espa- nhol ou ainda usar o idioma do sistema operacional.	Requisito não atendido. Ao acessar o link fornecido, não encontramos informações claras que atendam ao pedido.
A solução deve prover backup automático diariamente, permitindo que em um evento crítico seja pos- sível restaurar os dados de até 05 dias anteriores ao ocorrido.	Requisito não atendido. Ao acessar o link fornecido, não encontramos informações claras que atendam ao pedido.

3. É possível verificar a análise de todos os itens por meio da planilha SEI Nº 34842021.

4. Após uma análise minuciosa dos documentos apresentados durante o processo de julgamento, **a CLARO não cumpre todos os requisitos necessários**.

Respeitosamente,

Thiago Pereira da Costa
Chefe da Divisão de Privacidade e Proteção de Dados

De acordo,

Alexandre Bueno Chaves
Coordenador de Cibersegurança

Marco Antônio Bittencourt Sucupira
Coordenador-Geral de Infraestrutura, Segurança e Serviços Digitais

De acordo, encaminho para a Subsecretaria de Planejamento, Orçamento e Administração para demais providências.

Camilo Mussi
Subsecretário de Tecnologia da Informação

Documento assinado eletronicamente por **THIAGO PEREIRA DA COSTA**, **Chefe da Divisão de Privacidade e Proteção de Dados**, em 19/04/2024, às 10:16, conforme horário oficial de Brasília, com fundamento no art. 4º,§ 3º, do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **ALEXANDRE BUENO CHAVES**, **Coordenador de Cibersegurança e Privacidade de Dados**, em 19/04/2024, às 10:16, conforme horário oficial de Brasília, com fundamento no art. 4º,§ 3º, do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **MARCO ANTONIO BITTENCOURT SUCUPIRA**, **Coordenador Geral de Infraestrutura, Segurança e Serviços Digitais**, em 19/04/2024, às 10:17, conforme horário oficial de Brasília, com fundamento no art. 4º,§ 3º, do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Camilo Mussi**, **Subsecretário de Tecnologia da Informação**, em 19/04/2024, às 11:58, conforme horário oficial de Brasília, com fundamento no art. 4º,§ 3º, do Decreto nº 10.543, de 13 de novembro de 2020.

A autenticidade deste documento pode ser conferida no site: https://sei.agro.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 , informando o código verificador **34840672** e o código CRC **40A8D126**.