MUNICÍPIO DE HORTOLÂNDIA
Secretaria de Planejamento Urbano e Gestão Estratégica
Departamento de Infraestrutura da Tecnologia da Informação

Hortolândia, 09 de Março de 2026

De: SMPUGE/ Departamento de Infraestrutura da Tecnologia da Informação
Para: SMAGP / Departamento de Suprimentos

Assunto: Relatório de avaliação dos catálogos do PMH Nº 100876/2025 e Pregão Eletrônico nº 06/2026.

De acordo com os itens 1 a 5 do anexo II do edital, segue abaixo as avaliações dos catálogos.

EMPRESA: Scansource Brasil Distribuidora de Tecnologias Ltda

CNPJ: 05.607.657/0008-01

ITEM	MARCA	MODELO	SITUAÇÃO	OBSERVAÇÕES
1	Sophos	XG8ETCHUS XGS 8500 Security Appliance - US power	Aprovado	
2	Sophos	XG138Z00ZZPCUS XGS 138 Security Appliance	Aprovado	
3	Sophos	XG108Z00ZZPCUS XGS 108 Security Appliance	Aprovado	
4	Sophos	CFRAAB60BGNCAA	Aprovado	
5	Sophos	CWP00U60ADNCAA	Aprovado	

Análise Realizada

Foi efetuada conferência minuciosa dos seguintes itens:

- ✓ **Proposta Detalhada:** Verificação de modelos, marcas e especificações dos itens ofertados.
- ✓ **Certificação válida:** Em relação ao Item 6 “Treinamento para a Solução Firewall”, a licitante comprovou ter efetuado treinamento do objeto em questão, aos funcionários do SEBRAE/RJ. Os certificados dos profissionais responsáveis pelo treinamento poderão ser apresentados até 5(cinco) dias uteis em relação ao início do treinamento.

Parecer Técnico

Após análise da documentação técnica enviada, constatou-se que a licitante atendeu integralmente aos requisitos. As especificações do produto/serviço ofertado demonstram total compatibilidade com as necessidades da Prefeitura do Município de Hortolândia, não havendo omissões ou divergências que comprometam a execução do objeto.

Conclusão: Diante do exposto, concluímos que a documentação técnica enviada pela licitante vencedora está **DE ACORDO** com as normas e exigências previstas no Edital.

HEMERSON DONIZETE LARANJEIRA:13803643880

Assinado de forma digital por HEMERSON DONIZETE LARANJEIRA:13803643880
Dados: 2026.03.09 10:43:12 -03'00'

Atenciosamente,

Hemerson Donizete Laranjeira.

Pedido de esclarecimentos.

Tendo em vista que alguns esclarecimentos são necessários para sanar dúvidas que surgiram durante a avaliação dos catálogos do processo do pregão 06/2026, pedimos algumas informações para que a análise fique mais acertiva e eficiente.

1 - Proposta que contenha marca e modelo dos produtos ofertados, a proposta atual não possui os modelos ofertados;

2 - Documentação que comprovem algumas funcionalidades referentes aos modelos ofertados.

Referentes ao SD-WAN:

Exigência:
Controle de tráfego baseado em origem/destino e critérios (incluindo serviços e aplicações).

Documentação encontrada:
https://docs.sophos.com/nsg/sophos-firewall/21.0/Help/en-us/webhelp/onlinehelp/AdministratorHelp/Routing/SDWANRoutes/RoutingSDWANRoutesAdd/ • Add an SD-WAN route • Página: N/A (WebHelp).

Necessidade de esclarecimento:
Trecho não lista explicitamente TCP/UDP/ICMP nem cita nominalmente FTP/DNS/P2P no mesmo trecho.

Exigência:
ECMP no mínimo para roteamento estático e OSPF.

Documentação encontrada:
https://docs.sophos.com/nsg/sophos-firewall/21.5/Help/en-us/webhelp/onlinehelp/AdministratorHelp/Routing/StaticRouting/ • Static routes • Página: N/A (WebHelp).

Necessidade de esclarecimento:
Evidência encontrada para rotas estáticas; não localizada evidência explícita de ECMP para OSPF.

Exigência:
SD- WAN nativa sem licenciamento complementar; evitar indisponibilidade por expiração de licenças.

Documentação encontrada:
https://docs.sophos.com/nsg/sophos-firewall/20.0/Help/en-us/webhelp/onlinehelp/AdministratorHelp/Administration/Licensing/AdministrationLicensing/
Licensing info > Module subscription details • Página: N/A (WebHelp).

Necessidade de esclarecimento:
A documentação lista SD- WAN VPN Orchestration como módulo; não comprova ausência de licenciamento complementar nem funcionamento pleno pós-expiração.

Exigência:
SD- WAN com estratégia por aplicações (incl. micro-apps como Facebook Messenger).

Documentação encontrada:
https://docs.sophos.com/nsg/sophos-firewall/19.0/Help/en-us/webhelp/onlinehelp/AdministratorHelp/Routing/SDWANRoutes/RoutingSDWANRoutesUserApplication/ • User and application-based SD-WAN routes • Página: N/A (WebHelp).

Necessidade de esclarecimento:
Não foi localizada evidência literal no mesmo trecho citando nominalmente Office 365/YouTube.

Exigência:
Servidor DHCP interno (interfaces) e via VPN.

Documentação encontrada:
https://docs.sophos.com/nsg/sophos-firewall/21.5/Help/en-us/webhelp/onlinehelp/AdministratorHelp/Network/DHCP/ • DHCP • Página: N/A (WebHelp).

Necessidade de esclarecimento:
Trecho comprova DHCP server; parte “via VPN” não está literal aqui.

Exigência:
Regras Anti-malware/AV/IPS/Web por segmentos (zonas/interfaces).

Documentação encontrada:
https://docs.sophos.com/nsg/sophos-firewall/21.0/Help/en-us/webhelp/onlinehelp/AdministratorHelp/RulesAndPolicies/FirewallRules/ • Firewall rules • Página: N/A (WebHelp).

Necessidade de esclarecimento:s:
Trecho não cita nominalmente ‘anti-spyware’; evidências do conjunto de malware scanning podem variar por policy.

Exigência:
Bloquear P2P e transferências por usuários/grupos (capacidade).

Documentaçlão encontrada:
https://docs.sophos.com/nsg/sophos-firewall/20.0/Help/en-us/webhelp/onlinehelp/AdministratorHelp/Applications/ApplicationList/ • Application list • Página: N/A (WebHelp).

Necessidade de esclarecimento:
Categoria P2P comprovada; aplicação por usuário/grupo e 'transferências' depende de políticas adicionais (não comprovado neste trecho).

Exigência:
TLS inspection por política (TLS 1.2 e TLS 1.3).

Documentação encontrada:
https://docs.sophos.com/nsg/sophos-firewall/19.0/Help/en-us/webhelp/onlinehelp/AdministratorHelp/RulesAndPolicies/SSL/TLSInspectionRules/SSLTLSInspectionSettings/ • TLS 1.3 compatibility • Página: N/A (WebHelp).

Necessidade de esclarecimento:
Não foi encontrada literalidade 'Inbound/Outbound' exatamente como no edital no trecho citado.

Exigência:
Visualização gráfica das regras de segurança e acesso.

Documentação encontrada:
Não localizado;

Necessidade de esclarecimento: Comprovação da exigência do edital;

Exigência:
L2TP (incluindo iOS/Android).

Documentação encontrada:
https://docs.sophos.com/nsg/sophos-firewall/21.5/Help/en-us/webhelp/onlinehelp/AdministratorHelp/RemoteAccessVPN/L2TP/ • L2TP • Página: N/A (WebHelp).

Necessidade de esclarecimento:
Sem menção literal iOS/Android no contexto de L2TP nessa documentação.

Exigência:
Conectar redes com endereços "inválidos" via IPsec tunnel (IP-over-IP).

Documentação encontrada:
https://docs.sophos.com/nsg/sophos-firewall/20.0/Help/en-us/webhelp/onlinehelp/AdministratorHelp/RulesAndPolicies/NATRules/HowToArticles/ • Overlapping subnets in site-to-site IPsec tunnels • Página: N/A (WebHelp)

Necessidade de esclarecimento:
Cobertura para subnets sobrepostas/NAT; não há literalidade de “endereços inválidos” e “IP sobre IP” como redigido.

Exigência:
Troca de chaves manual + IKE/IKEv2; PSK + certificados + XAUTH.

Documentação encontrada:
https://docs.sophos.com/nsg/sophos-firewall/21.0/api/configure/vpn/vpnprofile/operations/AddVPNPolicy%26EditVPNPolicy.html • Add VPN Policy / Edit VPN Policy (API) • Página: N/A (HTML).

Necessidade de esclarecimento:
Provas separadas para Manual, ikev1/ikev2 e XAuth; não em um único trecho combinado com PSK/cert.

Exigência:
Interoperabilidade nominal com Cisco/Check Point/Juniper/Palo Alto/Fortinet/SonicWall.

Documentação encontrada:
https://docs.sophos.com/nsg/sophos-firewall/19.0/Help/en-us/webhelp/onlinehelp/AdministratorHelp/SiteToSiteVPN/IPsec/ • IPsec connections • Página: N/A (WebHelp).

Necessidade de esclarecimento:
Documentação consultada não lista nominalmente os fabricantes exigidos.

Sobre NGFW

Exigência:
Visando estabelecer efetividade de segurança na solução de FIREWALL e assegurar que o fornecedor tenha uma solução já avaliada por órgão terceiro e independente de mercado, o fabricante da solução deverá constar no “Magic Quadrant for Hybrid Mesh Firewall” de 2025.

Documentação encontrada:
https://www.sophos.com/en-us/products/next-gen-firewall

Necessidade de esclarecimento:
Edital pede avaliação por órgão terceiro independente. Sophos está no Gartner MQ, porém não há certificação NSS Labs "Recommended" recente publicada para XGS Series no docs.sophos.com.

Exigência:
Deverá implementar controle do tráfego para os protocolos TCP, UDP, ICMP e serviços como FTP, DNS, P2P entre outros, baseados nos endereços de origem e destino;

Documentação encontrada:
https://docs.sophos.com/nsg/sophos-firewall/21.0/Help/en-us/webhelp/onlinehelp/AdministratorHelp/Routing/SDWANRoutes/RoutingSDWANRoutesAdd/ • Add an SD-WAN route • Página: N/A (WebHelp).

Necessidade de esclarecimento:
Trecho não lista explicitamente TCP/UDP/ICMP nem cita nominalmente FTP/DNS/P2P no mesmo trecho.

Exigência:
one, porta TCP de conexão (NAPT) e NAT Traversal em VPN IPSec (NAT-T) e NAT dentro do tunel IPSec;

Documentação encontrada:
https://docs.sophos.com/nsg/sophos-firewall/22.0/Help/en-us/webhelp/onlinehelp/AdministratorHelp/AdvancedServices/IPv6FeaturesServices/index.html.

Necessidade de esclarecimento:
NPTv6 / NAT66 não documentado na página oficial Sophos Firewall.

Exigência:
Suportar Equal Cost Multi-Path (ECMP) no mínimo para roteamento estático e protocolo OSPF;

Documentação:
https://docs.sophos.com/nsg/sophos-firewall/21.5/Help/en-us/webhelp/onlinehelp/AdministratorHelp/Routing/StaticRouting/ • Static routes • Página: N/A (WebHelp).

Necessidade de esclarecimento:
Evidência encontrada para rotas estáticas; não localizada evidência explícita de ECMP para OSPF.

Exigência:
A solução deverá possuir a tecnologia SD-WAN (Software Defined WAN), e que a mesma seja nativa da solução, sem a necessidade de qualquer tipo de licenciamento complementar, para evitar indisponibilidade no ambiente mesmo em caso de expiração do licenciamento vigente.

Documentação encontrada:

https://docs.sophos.com/nsg/sophos-firewall/20.0/Help/en-us/webhelp/onlinehelp/AdministratorHelp/Administration/Licensing/AdministrationLicensing/ • Licensing info > Module subscription details • Página: N/A (WebHelp).

Necessidade de esclarecimento : :
A documentação lista SD- WAN VPN Orchestration como módulo; não comprova ausência de licenciamento complementar nem funcionamento pleno pós-expiração.

Exigência:
A solução de SD-WAN deve permitir estratégia de encaminhamento de trafego com base em aplicações conhecidas, como Office 365, Facebook e Youtube, bem como aplicações associadas como Facebook Messenger e Office 365 Outlook;

Documentação encontrada:
https://docs.sophos.com/nsg/sophos-firewall/19.0/Help/en-us/webhelp/onlinehelp/AdministratorHelp/Routing/SDWANRoutes/RoutingSDWANRoutesUserApplication/ • User and application-based SD-WAN routes • Página: N/A (WebHelp).

Necessidade de esclarecimento : :
Não foi localizada evidência literal no mesmo trecho citando nominalmente Office 365/YouTube.

Exigência:
Deve suportar Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;

Documentação encontrada:
https://docs.sophos.com/nsg/sophos-firewall/18.5/help/en-us/webhelp/onlinehelp/AdministratorHelp/Network/Interfaces/NetworkBridgeInterfaces/index.html.

Necessidade de esclarecimento:
Modo Sniffer (inspeção via porta espelhada) não é documentado como funcionalidade nomeada no Sophos Firewall. Bridge mode existe mas não é o mesmo que Sniffer.

Exigência:
Possuir servidor de DHCP (Dynamic Host Configuration Protocol) interno com capacidade de alocação de endereçamento IP para as estações conectadas às interfaces do firewall e via VPN;

Docuementação encontrada:
https://docs.sophos.com/nsg/sophos-firewall/21.5/Help/en-us/webhelp/onlinehelp/AdministratorHelp/Network/DHCP/ • DHCP • Página: N/A (WebHelp)

Necessidade de esclarecimento:
Trecho comprova DHCP server; parte “via VPN” não está literal aqui.

Exigência:
Deverá permitir a utilização de regras de Anti-malware, Anti-Vírus, Anti-Spyware, IPS e filtro de conteúdo web por segmentos de rede. Todos os

serviços devem ser suportados no mesmo segmento de rede, interface (fisica e virtual) ou zona de segurança;

Documentação encontrada:
https://docs.sophos.com/nsg/sophos-firewall/21.0/Help/en-us/webhelp/onlinehelp/AdministratorHelp/RulesAndPolicies/FirewallRules/ • Firewall rules • Página: N/A (WebHelp).

Necessidade de esclarecimento:
Trecho não cita nominalmente ‘anti-spyware’; evidências do conjunto de malware scanning podem variar por policy.

Exigência:
Possuir capacidade de inspecionar e bloquear em tempo real aplicativos e transferências de arquivos de softwares p2p (peer-to-peer),para usuários da rede, individualmente ou em grupo;

Documentação encontrada:
https://docs.sophos.com/nsg/sophos-firewall/20.0/Help/en-us/webhelp/onlinehelp/AdministratorHelp/Applications/ApplicationList/ • Application list • Página: N/A (WebHelp).

Necessidade de esclarecimento:
Categoria P2P comprovada; aplicação por usuário/grupo e ‘transferências’ depende de políticas adicionais (não comprovado neste trecho).

Exigência:
Para tráfego criptografado TLS versão 1.2 no mínimo, deve de-criptografar pacotes possibilitando a leitura de payload dos pacotes para checagem de assinaturas de aplicações conhecidas pelo fabricante; Controle, inspeção e de-criptografia de TLS versão 1.2 no mínimo por política para tráfego de entrada (Inbound) ou Saída (Outbound) com suporte a no mínimo, TLS 1.2 e TLS 1.3;

Documentação encontrada:

https://docs.sophos.com/nsg/sophos-firewall/19.0/Help/en-us/webhelp/onlinehelp/AdministratorHelp/RulesAndPolicies/SSL/TLSInspectionRules/SSLTLSInspectionSettings/ • TLS 1.3 compatibility • Página: N/A (WebHelp)

Necessidade de esclarecimento:
Não foi encontrada literalidade ‘Inbound/Outbound’ exatamente como no edital no trecho citado.

Exigência:
Deve permitir a funcionalidade de ARP bridging;

Documentação encontrada:
https://docs.sophos.com/nsg/sophos-firewall/19.0/Help/en-us/webhelp/onlinehelp/AdministratorHelp/Network/Interfaces/NetworkBridgeInterfaceAdd/ • Add a bridge interface • Página: N/A (WebHelp)

Necessidade de esclarecimento : :
Não aparece a expressão “ARP bridging” como funcionalidade nomeada; evidência é por comportamento de bridge.

Exigência:
Deve permitir a configuração de limite na taxa de envio ARP para um mesmo IP, para evitar "ARP Storm";

Documentação encontrada:
https://docs.sophos.com/nsg/sophos-firewall/19.0/Help/en-us/webhelp/onlinehelp/AdministratorHelp/Network/Interfaces/NetworkBridgeInterfaceAdd/ • Add a bridge interface • Página: N/A (WebHelp).

Necessidade de esclarecimento:
Evidência cobre mitigação de storm por ARP broadcast, mas não comprova “rate limit ARP por IP”.

Exigência:
A solução deve permitir a visualização gráfica das regras de segurança e acesso.

Documentação encontrada:
(Não localizado em documentação Sophos consultada)

Necessidade de esclarecimento:
Necessidade de comprovação via links do fabricante;

Exigência:
Suportar a criação de túneis IP sobre IP (IPSEC Tunnel), de modo a possibilitar que duas redes com endereço inválido possam se comunicar através da Internet;

Documentação encontrada:
https://docs.sophos.com/nsg/sophos-firewall/20.0/Help/en-us/webhelp/onlinehelp/AdministratorHelp/RulesAndPolicies/NATRules/HowToArticles/ • Overlapping subnets in site-to-site IPsec tunnels • Página: N/A (WebHelp).

Necessidade de esclarecimento:
Cobertura para subnets sobrepostas/NAT; não há literalidade de “endereços inválidos” e “IP sobre IP” como redigido.

Exigência:
Implementar os esquemas de troca de chaves manual, IKE e IKEv2 por Pré-Shared Key, certificados digitais e XAUTH client authentication;

Documentação encontrada:
https://docs.sophos.com/nsg/sophos-firewall/21.0/api/configure/vpn/vpnprofile/operations/AddVPNPolicy%26EditVPNPolicy.html • Add VPN Policy / Edit VPN Policy (API) • Página: N/A (HTML).

Necessidade de esclarecimento:
Provas separadas para Manual, ikev1/ikev2 e XAuth; não em um único trecho combinado com PSK/cert.

Exigência:
Permitir a definição de um gateway redundante para terminação de VPN no caso de queda do primário; Deve possuir interoperabilidade com os seguintes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall;

Documentação encontrada:
https://docs.sophos.com/nsg/sophos-firewall/19.0/Help/en-us/webhelp/onlinehelp/AdministratorHelp/SiteToSiteVPN/IPsec/ • IPsec connections • Página: N/A (WebHelp).

Necessidade de esclarecimento:
Documentação consultada não lista nominalmente os fabricantes exigidos.

Exigência:
A solução deve suportar funcionalidade de Geo-IP, ou seja, a capacidade de identificar, isolar e controlar tráfego baseado na localização (origem e/ou destino), incluindo a capacidade de configuração de listas customizadas para esta mesma finalidade;

Documentação encontrada:

https://docs.sophos.com/nsg/sophos-firewall/21.0/Help/en-us/webhelp/onlinehelp/AdministratorHelp/RulesAndPolicies/FirewallRules/index.html.

Necessidade de esclarecimento : :
Geo-IP/Country blocking é documentado no Sophos UTM. No Sophos Firewall (SFOS), a funcionalidade existe via regras de firewall com objetos de país, porém a página específica "Country Blocking" não existe como seção dedicada no docs.sophos.com para SOPHOS.

Gerenciamento:

Exigência:
ajudando a identificar explorações de vulnerabilidades, intrusões e outras ameaças. Deve permitir a emissão deste relatório em formato PDF;

Documentação encontrada:
https://docs.sophos.com/central/customer/help/en-us/ManageYourProducts/GlobalSettings/index.html

Necessidade de esclarecimento : :
Relatório de vulnerabilidades com exportação PDF é disponível via Sophos Central, não diretamente no appliance local.

Exigência:
Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico;

Documentação encontrada:
https://docs.sophos.com/nsg/sophos-firewall/20.0/Help/en-us/webhelp/onlinehelp/AdministratorHelp/NAT/index.html.

Necessidade de esclarecimento:
NPTv6/NAT66 não é suportado nativamente no Sophos Firewall SFOS. Suporta NAT64 e dual-stack IPv6 mas não NPTv6.

Exigência:
A solução deve permitir a visualização gráfica das regras de segurança e acesso; A solução deve permitir a visualização gráfica das regras de segurança e acesso;

Documentação encontrada:
https://docs.sophos.com/nsg/sophos-firewall/20.0/Help/en-us/webhelp/onlinehelp/AdministratorHelp/FirewallRules/index.html.

Necessidade de esclarecimento : :
Sophos Firewall não oferece visualização gráfica/diagrama das regras de segurança. Regras são listadas em formato tabular.

Exigência:
A solução deve suportar funcionalidade de Geo-IP, ou seja, a capacidade de identificar, isolar e controlar tráfego baseado na localização (origem e/ou destino), incluindo a capacidade de configuração de listas customizadas para esta mesma finalidade;

Documentação encontrada:

https://docs.sophos.com/nsg/sophos-firewall/20.0/Help/en-us/webhelp/onlinehelp/AdministratorHelp/FirewallRules/index.html.

Necessidade de esclarecimento:
Geo-IP baseado em países é suportado nas regras de firewall, mas a funcionalidade de listas customizadas de Geo-IP pode requerer configuração manual de IP lists, não um módulo dedicado de Geo-IP.

Exigência:

Deve permitir a emissão deste relatório em formato PDF;

Documentação encontrada:
https://docs.sophos.com/central/customer/Help/en-us/CentralReports/index.html.

Necessidade de esclarecimento:
Exportação de relatórios em formato PDF pode ser limitada a alguns tipos específicos de relatório. Sophos Central Firewall Reporting Advanced oferece opções mais abrangentes de exportação.

Exigência:
Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico;

Documentação encontrada:
https://docs.sophos.com/nsg/sophos-firewall/20.0/Help/en-us/webhelp/onlinehelp/AdministratorHelp/NAT/index.html

Necessidade de esclarecimento : :
NPTv6/NAT66 não é suportado nativamente no Sophos Firewall SOPHOS.

Exigência:
Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico;

Documentação encontrada:

https://docs.sophos.com/nsg/sophos-firewall/20.0/Help/en-us/webhelp/onlinehelp/AdministratorHelp/NAT/index.html

Necessidade de esclarecimento :
NPTv6/NAT66 não é suportado nativamente no Sophos Firewall SOPHOS.

Exigência:
A solução deve permitir a visualização gráfica das regras de segurança e acesso; A solução deve permitir a visualização gráfica das regras de segurança e acesso;
Documentação encontrada:

https://docs.sophos.com/nsg/sophos-firewall/20.0/Help/en-us/webhelp/onlinehelp/AdministratorHelp/FirewallRules/index.html

Necessidade de esclarecimento:
Sophos não oferece visualização gráfica/diagrama das regras. Formato tabular apenas.

Exigência:
A solução deve suportar funcionalidade de Geo-IP, ou seja, a capacidade de identificar, isolar e controlar tráfego baseado na localização (origem e/ou

destino), incluindo a capacidade de configuração de listas customizadas para esta mesma finalidade;

Documentação encontrada:

https://docs.sophos.com/nsg/sophos-firewall/20.0/Help/en-us/webhelp/onlinehelp/RulesHelp/FirewallRules/index.html

Necessidade de esclarecimento:
Listas customizadas de Geo-IP não são suportadas nativamente. O bloqueio é baseado na base de dados de países do fabricante, sem possibilidade de criar listas geográficas personalizadas pelo administrador.

Gerenciamento:
Exigência:
Deve permitir a emissão deste relatório em formato PDF;

Documentação encontrada:
https://docs.sophos.com/nsg/sophos-firewall/20.0/Help/en-us/webhelp/onlinehelp/ReportsHelp/index.html.

Necessidade de esclarecimento : :
Emissão nativa de relatórios em formato PDF é limitada no appliance. Relatórios em PDF completos são disponibilizados via Sophos Central, não diretamente no appliance local.

Exigência:
A solução deve permitir a criação de modelos de configuração ou “Templates” para aplicá-los em grupos de dispositivos. Os modelos de configurações devem permitir visualização e edição para sua aplicação nos firewalls Os modelos de configuração ou “templates” devem suportar configurações de interfaces físicas ou virtuais;

Documentação encontrada:
https://docs.sophos.com/central/partner/help/en-us/Help/Configure/SettingsAndPolicies/FirewallTemplates/index.html

Necessidade de esclarecimento : :
Templates de configuração no Sophos Central têm cobertura limitada para configurações de interfaces físicas. Configurações detalhadas de interfaces devem ser realizadas localmente no Web Admin de cada firewall.

Exigência:
Deverá permitir visualizar a diferença nas mudanças antes que a configurações sejam implantadas;

Documentação encontrada:
https://docs.sophos.com/central/customer/help/en-us/ManageYourProducts/FirewallManagement/Firewalls/index.html

Necessidade de esclarecimento : :
Não foram encontrados documentos que comprovem

Exigência:
De forma centralizada deve permitir gerenciar, mas não limitado há, políticas de firewall, NAT, rotas, PBR (Policy Based Routing), configuração de endereçamento IP das interfaces dos equipamentos, criação e administração de políticas de IPS, configuração de políticas de antivírus e antimalware, configuração e criação de políticas de controle de URL, criação e configuração de políticas de controle de aplicações, criação e configuração de política de SANDBOX, criação e configuração de políticas de controle de banda, criação e configuração de objetos necessários para configuração das políticas especificadas acima, usando uma única interface de gerenciamento;

Documentação encontrada:
https://docs.sophos.com/central/customer/help/en-us/ManageYourProducts/FirewallManagement/Firewalls/FirewallGroups/index.html

Necessidade de esclarecimento:
Gerenciamento centralizado de políticas de IPS individuais, rotas, PBR (Policy Based Routing), sandbox e controle de banda não é suportado diretamente via Sophos Central. Estas configurações requerem acesso ao Web Admin local de cada firewall.

Exigência:
Para cada alteração de configuração a solução deverá confirmar a aplicação da política, possibilitando a adição de comentários nas políticas instaladas, para futuras consultas de auditoria;

Documentação encontrada:
https://docs.sophos.com/central/customer/help/en-us/ManageYourProducts/FirewallManagement/Firewalls/index.html

Necessidade de esclarecimento:
O Sophos Central não possui funcionalidade nativa de adição de comentários individuais nas políticas instaladas para fins de auditoria. O log de auditoria registra ações, mas sem campo de comentário customizado por política.

Exigência:
Deverá permitir que configurações realizadas pelos administradores da solução sejam validadas e aprovadas (workflow), por um colaborador responsável por aprovação e aplicação de políticas, esse processo de aprovação deve ser encaminhado de forma automatizada para o responsável da aprovação via e-mail ou console da solução, possibilitando mitigar erros de configuração e impactos negativos ao ambiente ;

Documentação encontrada:
https://docs.sophos.com/central/customer/help/en-us/ManageYourProducts/FirewallManagement/Firewalls/index.html

Necessidade de esclarecimento:
Não encontrada documentação para provar tal função.

Questões sobre ZTNA:

Exigência:
A plataforma de segurança deverá ter ponto de presença preferencialmente no Brasil, O ponto de presença (PoP) deve operar na própria infraestrutura do fabricante. De forma alterativa poderá ser através de provedores de nuvem pública tais como AWS, Microsoft, Google, Oracle Não serão aceitos sistemas baseados em hardware ou software projetados para uso genérico, ou de código aberto (“open source”). Os elementos ofertados não podem ser customizados;

Documentação encontrada:
https://www.sophos.com/en-us/products/zero-trust-network-access/tech-specs.

Necessidade de esclarecimento:
Sophos ZTNA não possui PoP (Point of Presence) dedicado no Brasil operando na própria infraestrutura do fabricante. O ZTNA gateway é implantado on-premises na infraestrutura do cliente ou integrado ao Sophos Firewall, minimizando a dependência de PoPs remotos.

Exigência:
A solução deverá integrar-se nativamente e enviar em tempo real logs para plataformas de SIEM (Security Information and Event Management) como Splunk, IBM Qradar e MS Sentinel;

Documentação:
https://docs.sophos.com/central/customer/help/en-us/ManageYourProducts/LogsReports/

Necessidade de esclarecimento:
A integração nativa em tempo real com IBM QRadar pode requerer configuração adicional de syslog forwarding. Não há conector nativo pré-configurado para todos os SIEMs listados diretamente do módulo ZTNA.

Exigência:
O suporte a cada tipo pode variar dependendo da plataforma (Windows, Mac, Linux), sendo requerido que no mínimo deverá suportar 2 dos tipos abaixo por plataforma:

Documentação:
https://www.sophos.com/en-us/products/zero-trust-network-access

Necessidade de esclarecimento:
O Security Heartbeat do Sophos ZTNA opera como indicador agregado de saúde (green/yellow/red) baseado no status do Sophos Intercept X. Não

suporta validação granular individual de cada tipo listado (disco cifrado, chave de registro, certificado específico, arquivo específico) como checks de postura independentes.

Exigência:
Validação de Certificado Cliente (chave privada e pública) assinada por um CA específico;

Documentação:
https://www.sophos.com/en-us/products/zero-trust-network-access

Necessidade de esclarecimento:
Validação de certificado cliente como check de postura individual (chave privada e pública assinada por CA específico) não é um check de postura nativo do Security Heartbeat. Certificados são usados na autenticação do gateway, mas não como fator de postura granular.

Exigência:
Validação de Certificado confiável no dispositivo;

Documentação:
https://www.sophos.com/en-us/products/zero-trust-network-access
Necessidade de esclarecimento:
Validação de certificado confiável específico no dispositivo como check de postura individual não é funcionalidade nativa do Security Heartbeat.

Exigência:
Validação de disco cifrado;

Documentação:
https://www.sophos.com/en-us/products/zero-trust-network-access

Necessidade de esclarecimento:
Validação de disco cifrado (BitLocker, FileVault) como check de postura individual não é funcionalidade nativa do Security Heartbeat do Sophos ZTNA.

Exigência:
Validação de Registro de chave no Windows;

Documentação encontrada:

https://www.sophos.com/en-us/products/zero-trust-network-access

Necessidade de esclarecimento:
Não encontrada documentação que comprove a funcionalidade.

Exigência:
Validação de presença de um arquivo;

Documentação encontrada:

https://www.sophos.com/en-us/products/zero-trust-network-access

Necessidade de esclarecimento:
Não encontrada documentação para comprovação.

Exigência:
Exigência de uma versão mínima do Sistema Operacional;

Documentação encontrada:
https://www.sophos.com/en-us/products/zero-trust-network-access

Necessidade de esclarecimento:
Bloqueio de acesso ZTNA baseado especificamente em versão mínima do sistema operacional como check de postura individual não é funcionalidade nativa. O check de postura é baseado no Security Heartbeat agregado.

Exigência:
Resolução através do conector instalado na infraestrutura da contratante;
Resolução pelo próprio agente instalado no dispositivo;

Documentação encontrada:

https://www.sophos.com/en-us/products/workspace-protection

Necessidade de esclarecimento:
Resolução DNS via conector instalado na infraestrutura da contratante como componente dedicado de DNS protection não é uma funcionalidade explícita. O ZTNA gateway pode resolver DNS localmente, mas não é apresentado como componente de DNS protection dedicado.

Exigência:
A plataforma deve prover controle de acesso e a sobreposição de segurança para aplicativos SaaS. O CASB deve fornecer visibilidade não apenas para quais aplicativos SaaS os usuários estão acessando, mas também para o que os usuários estão fazendo dentro do aplicativo SaaS. Deve possibilitar uma camada de segurança de confiança de dispositivo sem atrito para logon único existente, eliminando riscos associados a ataques de phishing e invasão de contas.

Documentação encontrada:
https://www.sophos.com/en-us/products/zero-trust-network-access

Necessidade de esclarecimento:
Não encontrada documentação para comprovação.

scansource®

Endereço: Av. Paulista, 2300 – 16º andar
Bela Vista - Conj. 161, 163 e 164, São Paulo
SP, 01310-300
Telefone: (11) 3049-0310
Site: www.scansource.com.br

PREGÃO ELETRÔNICO Nº 06/2025 — PREFEITURA MUNICIPAL DE HORTOLÂNDIA

À Comissão de Licitação / Pregoeiro(a) - Secretaria Municipal de Planejamento Urbano e Gestão Estratégica
A/c Hemerson

Esclarecimentos da diligência

Item	Exigência	Documentação Referenciada no questionamento	Necessidade de esclarecimento
1.3.1.2.a	*Controle de tráfego baseado em origem/destino e critérios (incl. serviços e aplicações).*	*https://docs.sophos.com/ nsg/sophos-firewall/21.0/Help/en- us/webhelp/onlinehelp/AdministratorHelp/Routing /SDWANRoutes/RoutingS DWANRoutesAdd/ • Add an SD-WAN route • Página: N/A (WebHelp)*	*Trecho não lista explicitamente TCP/UDP/ICMP nem cita nominalmente FTP/DNS/P2P no mesmo trecho.*

Em atenção ao Item ***1.3.1 – Controle de tráfego baseado em origem/destino e critérios (incluindo serviços e aplicações)***

O órgão sustenta que a solução ofertada não atenderia ao requisito de controle de tráfego baseado em origem, destino e critérios como serviços e aplicações, sob o argumento de que o trecho de documentação apresentado não listaria explicitamente determinados protocolos ou aplicações, como TCP, UDP, ICMP, FTP, DNS ou P2P.

Entretanto, tal interpretação não procede e decorre de análise parcial e descontextualizada da documentação técnica da solução. A solução ofertada implementa mecanismos de controle de tráfego por meio de políticas de firewall e de SD-WAN baseadas em múltiplos critérios, incluindo endereço de origem, endereço de destino, serviços de rede e identificação de aplicações, funcionalidades inerentes à arquitetura de firewalls de próxima geração.

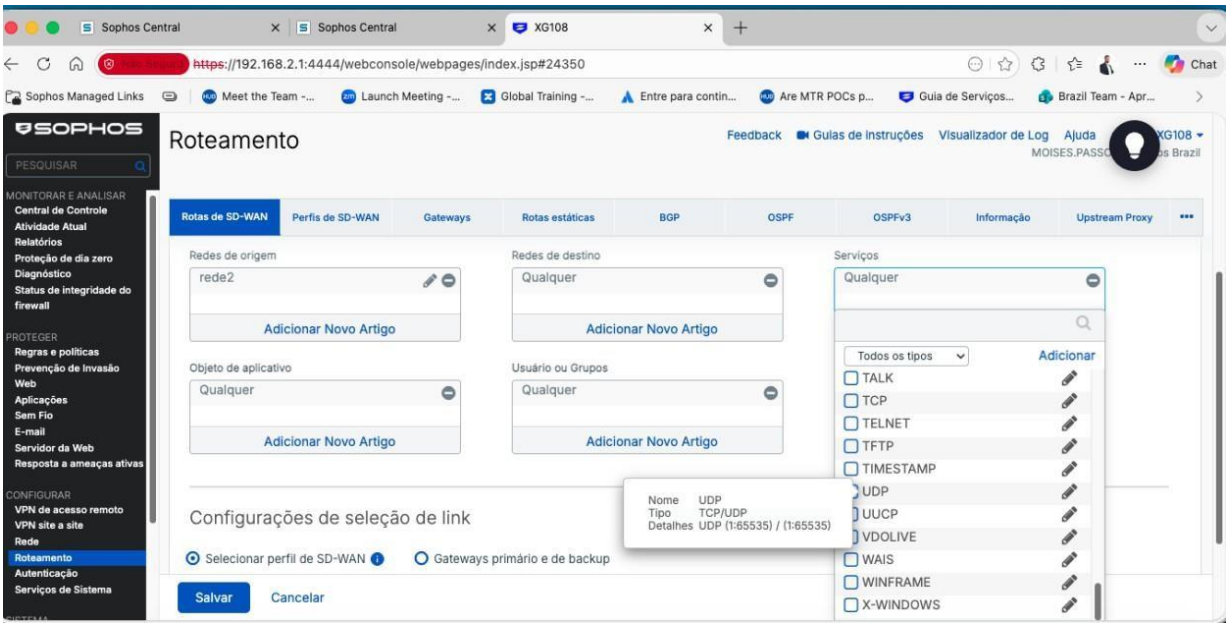
No caso específico da solução ofertada, é plenamente possível a definição de regras de controle utilizando objetos de serviço baseados em protocolos de rede como TCP, UDP e ICMP, bem como a identificação e controle de aplicações por meio de mecanismos de classificação de tráfego e controle de aplicações, permitindo a aplicação de políticas granulares conforme previsto no requisito do edital.

Adicionalmente, observa-se que o órgão fundamenta sua alegação em trecho isolado da documentação referente à configuração de rotas SD-WAN, que não representa o mecanismo principal de controle de políticas de segurança do equipamento, responsável pela aplicação das regras de controle de tráfego exigidas no edital.

Ainda assim, mesmo no contexto de configuração de rotas SD-WAN, verifica-se que a solução permite a definição de critérios como redes de origem, redes de destino, serviços e objetos de aplicação, conforme demonstrado na interface de configuração da solução, evidenciando a capacidade de classificação e controle de tráfego com base nos parâmetros especificados.

Importante destacar que o edital não exige a listagem nominal de protocolos específicos na documentação apresentada, mas sim a capacidade funcional de controle de tráfego baseado nos critérios mencionados. Nesse sentido, a interpretação forçada de forma restritiva proposta pela prefeitura busca impor exigência não prevista no instrumento convocatório induzindo informações equivocadas. Cabe ainda ressaltar que a análise apresentada se baseia em documentação de versão anterior do produto, não refletindo necessariamente as capacidades presentes nas versões mais recentes da solução ofertada.

Deste modo, verifica-se que o requisito estabelecido no edital é plenamente atendido pela solução ofertada, não havendo qualquer evidência técnica que sustente a alegação apresentada.



scansource®
Endereço: Av. Paulista, 2300 – 16º andar Bela Vista - Conj. 161, 163 e 164, São Paulo SP, 01310-300
Telefone: (11) 3049-0310
Site: www.scansource.com.br

Item	***Exigência***	***Documentação Referenciada no questionamento***	***Necessidade de esclarecimento***
1.3.1.2.i	*ECMP no mínimo para roteamento estático e OSPF.*	*https://docs.sophos.com/nsg/sophos-firewall/21.5/Help/en-us/webhelp/onlinehelp/AdministratorHelp/Routing/StaticRouting/ • Static routes • Página: N/A (WebHelp)*	*Evidência encontrada para rotas estáticas; não localizada evidência explícita de ECMP para OSPF.*

Referente ao Item ***1.3.1.2 – ECMP no mínimo para roteamento estático e OSPF***

A prefeitura sustenta que a solução ofertada atenderia apenas parcialmente ao requisito de suporte a ECMP (*Equal-Cost Multi-Path*), sob o argumento de que teria sido encontrada evidência dessa funcionalidade apenas para rotas estáticas, não havendo referência explícita à utilização do recurso em conjunto com o protocolo OSPF. Tal interpretação decorre novamente de análise restrita a trechos isolados da documentação técnica, não refletindo a arquitetura e o funcionamento do mecanismo de roteamento implementado pela solução ofertada.

O recurso ECMP corresponde a um mecanismo do plano de roteamento que permite a utilização simultânea de múltiplos caminhos de mesmo custo para encaminhamento de tráfego. Trata-se de funcionalidade inerente ao mecanismo de roteamento do equipamento, aplicável aos protocolos e métodos de roteamento suportados pela solução, uma vez suportado o ECMP no mecanismo de roteamento, a utilização desse recurso não se limita a rotas estáticas, podendo também ser aplicada a protocolos de roteamento dinâmico, como o OSPF, conforme previsto na arquitetura de roteamento da solução.

Importante destacar que a ausência de menção explícita ao protocolo OSPF em um trecho específico da documentação não caracteriza limitação funcional do equipamento, tampouco comprova a inexistência do recurso, mas apenas reflete o escopo do trecho consultado.

Assim, verifica-se que a solução ofertada atende plenamente ao requisito de suporte a ECMP para roteamento estático e protocolos de roteamento dinâmico, incluindo OSPF, conforme estabelecido no edital.

Diante do exposto, resta claro e conclui-se que o argumento apresentado não procede.

Item	Exigência	Documentação Referenciada no questionamento	Necessidade de esclarecimento
1.3.1.2.k	*SD-WAN nativa sem licenciamento complementar; evitar indisponibilidade por expiração de licenças.*	*https://docs.sophos.com/nsg/sophos-firewall/20.0/Help/en-us/webhelp/onlinehelp/AdministratorHelp/Administration/Licensing/AdministrationLicensing/ • Licensing info > Module subscription details • Página: N/A (WebHelp)*	*A doc lista SD-WAN VPN Orchestration como módulo; não comprova ausência de licenciamento complementar nem funcionamento pleno pós-expiração.*

Em atenção ao questionamento apresentado acerca do ***item 1.3.1.2.k – SD-WAN nativa sem licenciamento complementar***, verifica-se que a alegação apresentada não procede, demonstrando inclusive interpretação equivocada da documentação técnica do fabricante.

O órgão baseia sua argumentação em documentação referente ao módulo "*SD-WAN VPN Orchestration"*, recurso este que não se confunde com a funcionalidade SD-WAN nativa presente no equipamento. Trata-se de funcionalidade adicional voltada à orquestração centralizada de túneis e políticas em ambientes distribuídos, não sendo requisito para a operação da SD-WAN local no equipamento. Conforme demonstrado na própria documentação oficial do fabricante, a funcionalidade SD-WAN faz parte da licença base do Sophos Firewall, estando disponível de forma nativa no equipamento, independentemente de aquisição de licenças adicionais. O próprio datasheet do produto é claro ao afirmar que a licença base do Sophos Firewall inclui arquitetura Xstream, recursos de rede, SD-WAN, VPN e relatórios, entre outras funcionalidades essenciais.

https://assets.sophos.com/X24WTUEQ/at/7wf85vbnnqf939bbhtxgfk/sophos-firewall-br.pdf
Página 8.

Assim, a afirmação de que haveria necessidade de licenciamento adicional para utilização da funcionalidade SD-WAN é tecnicamente incorreta e não encontra respaldo na documentação oficial do fabricante, configurando interpretação indevida do material apresentado.

Adicionalmente, cabe destacar que o argumento apresentado induz e qualifica a capacidade e postura de atendimento com à interpretação de que seria aceitável a utilização de equipamentos de segurança sem licenciamento de proteção ativo, prática esta comum em cenários de fornecimento de conectividade simples (como venda de links de dados), mas incompatível com soluções de segurança de rede corporativa, cujo correto funcionamento pressupõe a utilização de mecanismos ativos de proteção e atualização, nesse sentido surge uma questão simples.. Qual o sentido de usar um firewall de próxima geração somente para conectividade, ignorando a principal função de uma solução NGFW (next Generation firewall) colocando em risco o cliente bem como a reputação do fabricante?

Ressalta-se que a apresentação de informações técnicas de forma incompleta ou distorcida, capazes de induzir a Administração Pública a erro quanto às características da solução ofertada, pode caracterizar afirmação falsa ou potencialmente enganosa no âmbito de processo licitatório, o que contraria os princípios da boa-fé, da transparência e da isonomia que regem as contratações públicas.

Resta evidenciado que a solução ofertada atende plenamente ao requisito deste certame, uma vez que a funcionalidade SD-WAN é nativa e integrante da licença base do equipamento, não havendo necessidade de licenciamento complementar para sua operação.

Item	Exigência	Documentação Referenciada no questionamento	Necessidade de esclarecimento
1.3.1.2.p	SD-WAN com estratégia por aplicações (incl. micro-apps como Facebook Messenger).	https://docs.sophos.com/nsg/sophos-firewall/19.0/Help/en-us/webhelp/onlinehelp/AdministratorHelp/Routing/SDWANRoutes/RoutingSDWANRoutesUserApplication/ • User and application-based SD-WAN routes • Página: N/A (WebHelp)	Não foi localizada evidência literal no mesmo trecho citando nominalmente Office 365/YouTube.

Em face a alegação apresentada acerca do **item 1.3.1.2.p – SD-WAN com estratégia por aplicações (incluindo micro-aplicações)**, verifica-se que o argumento apresentado não procede.

A documentação apresentada menciona apenas o exemplo de micro-aplicação “Facebook Messenger”, alegando que não foram localizadas evidências literais no mesmo trecho que citem nominalmente aplicações como Office 365 ou YouTube, sugerindo, portanto, que a solução não atenderia ao requisito estabelecido no edital.

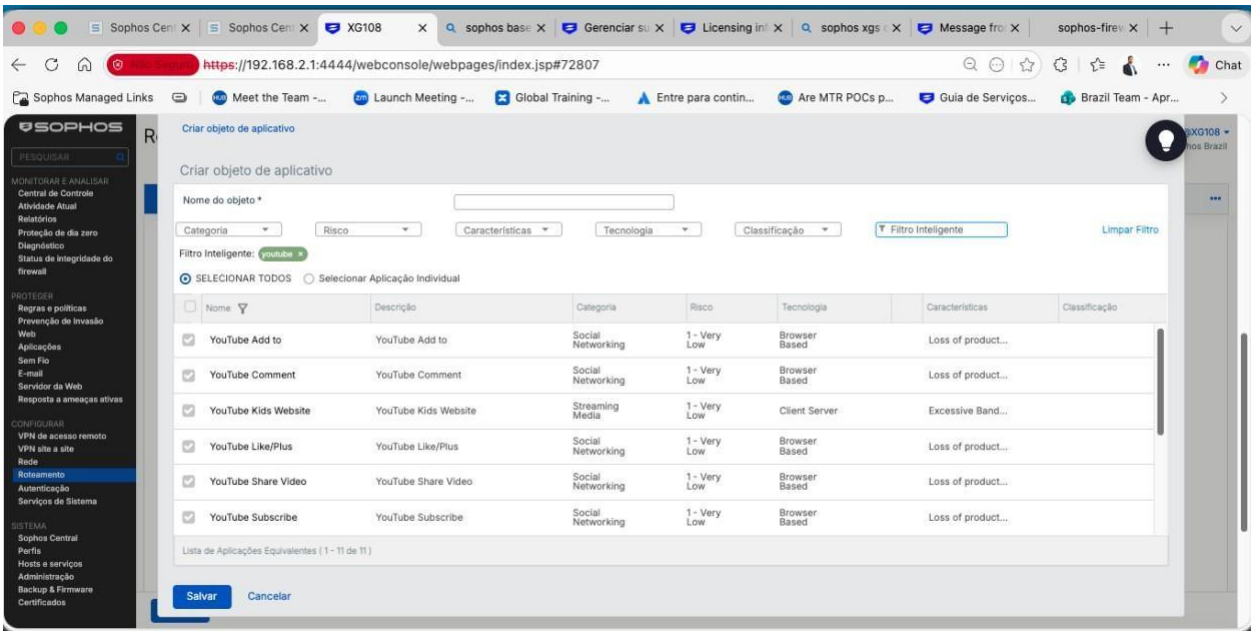
Entretanto, tal interpretação não se sustenta tecnicamente.

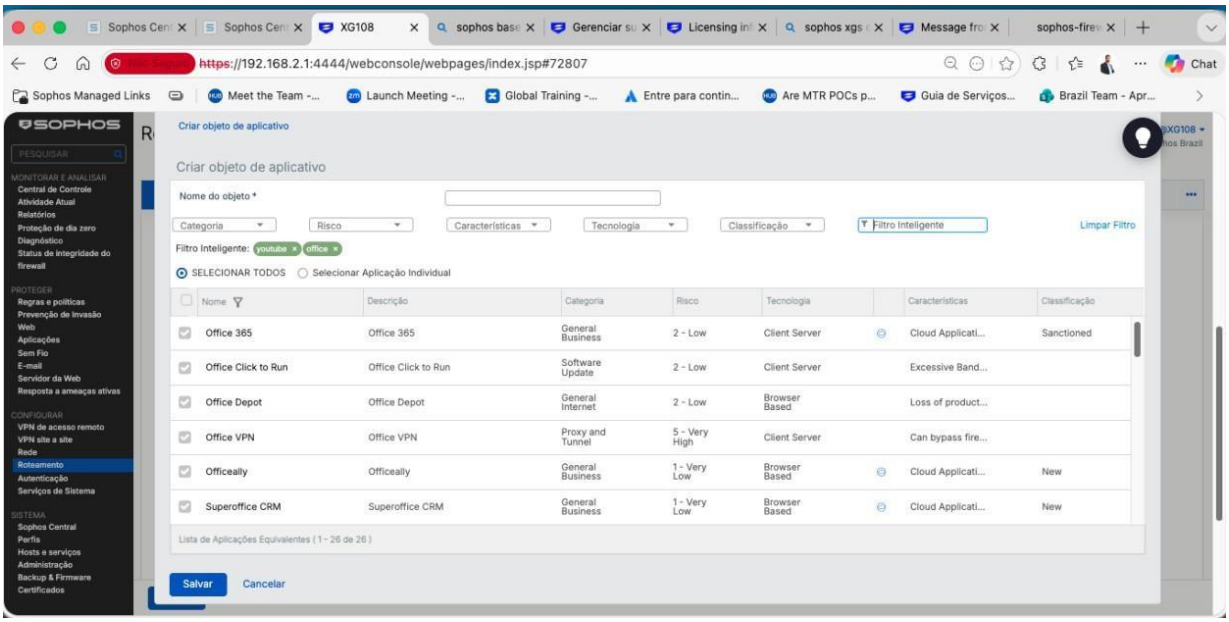
Inicialmente, é importante destacar que o exemplo citado na documentação possui carácter meramente ilustrativo, sendo utilizado apenas para demonstrar o funcionamento da funcionalidade de roteamento SD-WAN baseado em usuários e aplicações. Em nenhum momento a documentação limita o funcionamento da solução exclusivamente às aplicações exemplificadas.

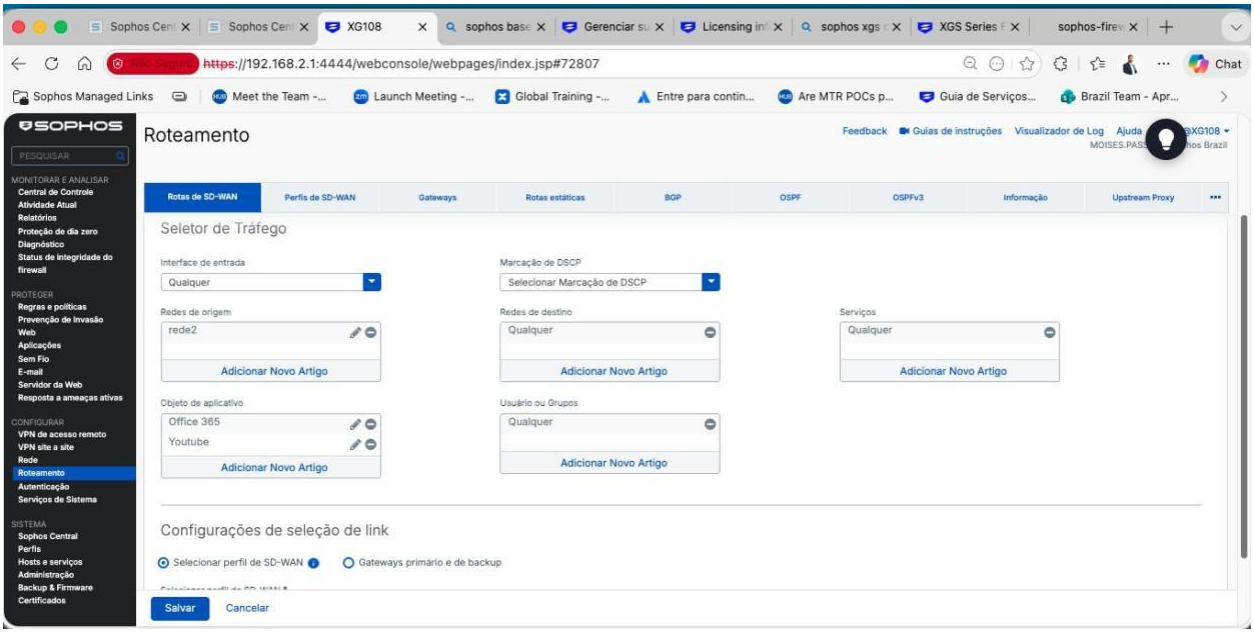
scansource®

Endereço: Av. Paulista, 2300 – 16º andar
Bela Vista - Conj. 161, 163 e 164, São Paulo
SP, 01310-300
Telefone: (11) 3049-0310
Site: www.scansource.com.br

O Sophos Firewall possui mecanismo avançado de identificação e classificação de aplicações, baseado em *Deep Packet Inspection* (DPI) e no motor de *Application Control,* que mantém uma base extensa de aplicações e micro-aplicações utilizadas como critérios para definição de políticas de segurança e roteamento.







Conforme demonstrado nas imagens de captura de tela 1,2 e 3, extraídas da própria interface administrativa do Sophos Firewall XGS 108 na versão 22, observa-se que a solução permite a criação de políticas de SD-WAN baseadas diretamente em objetos de aplicação, possibilitando a definição de regras específicas para aplicações e serviços distintos.

Na Figura 2 ou simplesmente captura de tela, verifica-se a configuração de uma regra de SD-WAN na qual são definidos objetos de aplicativo utilizados como critério para o encaminhamento do tráfego, incluindo exemplos como Office 365 e YouTube, evidenciando a capacidade da solução de aplicar estratégias de roteamento baseadas em aplicações.

Complementando, as capturas de tela anexadas, demonstra a interface de seleção de aplicações utilizada na criação desses objetos, evidenciando a presença de múltiplas aplicações e micro aplicações associadas ao ecossistema Microsoft Office 365, como diferentes componentes e serviços relacionados à plataforma. Esse nível de detalhamento evidencia que a solução possui capacidade de identificação granular de aplicações e subserviços, os quais podem ser utilizados como critérios para definição de políticas de segurança e roteamento SD-WAN.

Dessa forma, resta demonstrado que o Sophos Firewall possui suporte pleno à estratégia de SD-WAN baseada em aplicações, inclusive com capacidade de utilização de micro-aplicações como critério de política, atendendo integralmente ao requisito previsto no edital.

A alegação apresentada baseia-se em interpretação restritiva de um exemplo pontual presente na documentação, desconsiderando tanto as capacidades efetivas da solução quanto as evidências apresentadas.
Conclui-se claramente que o argumento apresentado não procede, devendo ser mantida a decisão que considerou o atendimento do requisito pela solução ofertada.

scansource®
Endereço: Av. Paulista, 2300 – 16º andar Bela Vista - Conj. 161, 163 e 164, São Paulo SP, 01310-300
Telefone: (11) 3049-0310
Site: www.scansource.com.br

Item	Exigência	Documentação Referenciada no questionamento	Necessidade de esclarecimento
1.3.1.2.s	*Servidor DHCP interno (interfaces) e via VPN.*	*https://docs.sophos.com/nsg/sophos-firewall/21.5/Help/en-us/webhelp/onlinehelp/AdministratorHelp/Network/DHCP/ • DHCP • Página: N/A (WebHelp)*	*Trecho comprova DHCP server; parte "via VPN" não está literal aqui.*

Em atenção ao item ***1.3.1.2.s – Servidor DHCP interno (interfaces e via VPN)***, o órgão afirma que o trecho da documentação apresentado comprova apenas a funcionalidade de servidor DHCP, alegando que não haveria evidência literal da utilização da funcionalidade "via VPN".

Entretanto, a referida interpretação não procede.

O Sophos Firewall possui funcionalidade nativa de servidor DHCP integrado, podendo ser configurado em qualquer interface de rede administrada pelo equipamento. No modelo de arquitetura da solução, interfaces podem representar tanto interfaces físicas quanto interfaces lógicas, incluindo interfaces de túneis VPN, como aquelas utilizadas em conexões site-to-site ou redes remotas, uma vez estabelecido o túnel VPN e criada a respectiva interface lógica associada à rede remota, o firewall pode atuar como servidor DHCP para os segmentos de rede vinculados a essa interface, permitindo a distribuição de endereçamento IP e demais parâmetros de rede para dispositivos conectados através da infraestrutura VPN.

Importante destacar que a documentação citada descreve a funcionalidade de DHCP Server de forma geral, a qual é aplicável a qualquer interface gerenciada pelo firewall, não havendo restrição quanto ao tipo de interface utilizada.

A ausência de menção literal ao termo *"via VPN"* no trecho específico da documentação não implica limitação funcional da solução, uma vez que o funcionamento do servidor DHCP está intrinsecamente associado às interfaces de rede configuradas no equipamento, incluindo interfaces lógicas derivadas de túneis VPN.

Dessa forma, resta demonstrado que a solução ofertada atende plenamente ao requisito de servidor DHCP interno em interfaces, inclusive em cenários que envolvam conectividade por VPN, conforme previsto no edital.

Item	Exigência	Documentação Referenciada no questionamento	Necessidade de esclarecimento
1.3.1.2.v	*Regras Anti-malware/AV/IPS/Web por segmentos (zonas/interfaces).*	*https://docs.sophos.com/nsg/sophos-firewall/21.0/Help/en-us/webhelp/onlinehelp/AdministratorHelp/RulesAndPolicies/FirewallRules/ • Firewall rules • Página: N/A (WebHelp)*	*Trecho não cita nominalmente 'anti-spyware'; evidências do conjunto de malware scanning podem variar por policy.*

Em atenção ao referido item ***1.3.1.2.v – Regras Anti-malware/AV/IPS/Web*** por segmentos (zonas/interfaces), o órgão afirma que o trecho da documentação apresentado não cita nominalmente a funcionalidade *"anti- spyware",* argumentando que as evidências se referem apenas ao conjunto de funcionalidades de malware scanning, que poderiam variar conforme a política aplicada.

A interpretação não procede. No Sophos Firewall possui arquitetura de segurança baseada em políticas unificadas, nas quais os mecanismos de proteção, incluindo antivírus (AV), anti-malware, proteção web e sistema de prevenção de intrusão (IPS), são aplicados diretamente nas regras de firewall, permitindo a definição de políticas específicas de inspeção e proteção para diferentes segmentos de rede, conforme zonas, interfaces, usuários ou aplicações.

Conforme descrito na documentação citada, o administrador pode aplicar políticas de segurança para tráfego web, controle de aplicações e IPS diretamente nas regras de firewall, o que evidencia que os mecanismos de proteção são integrados ao processo de inspeção de tráfego realizado pela solução.

Importante destacar que, no contexto das soluções modernas de segurança de rede, a funcionalidade tradicionalmente denominada *"anti-spyware"* encontra-se incorporada ao mecanismo mais abrangente de proteção contra malware, que engloba diferentes tipos de ameaças, incluindo vírus, trojans, spyware, adware e demais códigos maliciosos. Dessa forma, a proteção contra spyware é tratada como parte integrante do motor de análise de malware da solução.

https://docs.sophos.com/nsg/sophos-firewall/22.0/Help/en-us/webhelp/onlinehelp/AdministratorHelp/ZeroDayProtection/index.html#machine-learning

Mecanismos estes, podem ser aplicados de forma granular por meio de regras de firewall, permitindo sua utilização em diferentes segmentos da rede, conforme zonas ou interfaces configuradas, atendendo exatamente ao requisito previsto no edital.

Assim, a ausência de menção literal ao termo "anti-spyware" no trecho específico da documentação não implica ausência da funcionalidade, uma vez que esta encontra-se abrangida pelo mecanismo de proteção contra malware integrado à solução, aplicado por meio das políticas de segurança configuradas nas regras de firewall.

Dessa forma, resta demonstrado que a solução ofertada atende plenamente ao requisito de aplicação de regras de segurança com proteção contra malware, antivírus, IPS e inspeção web por segmentos de rede, conforme estabelecido no edital.

Item	Exigência	Documentação Referenciada no questionamento	Necessidade de esclarecimento
1.3.1.2.w	*Bloquear P2P e transferências por usuários/grupos (capacidade).*	*https://docs.sophos.com/nsg/sophos-firewall/20.0/Help/en-us/webhelp/onlinehelp/AdministratorHelp/Applications/ApplicationList/ • Application list • Página: N/A (WebHelp)*	*Categoria P2P comprovada; aplicação por usuário/grupo e 'transferências' depende de políticas adicionais (não comprovado neste trecho).*

Em referência ao item ***1.3.1.2.w – Bloquear P2P e transferências por usuários/grupos (capacidade)***, o órgão afirma que o trecho da documentação apresentado comprova apenas a existência da categoria de aplicações P2P, alegando que a aplicação de bloqueio por usuário ou grupo e o controle de transferências dependeriam de políticas adicionais, não estando comprovados no trecho específico citado.

A solução Sophos Firewall utiliza um modelo de controle de aplicações baseado em políticas, no qual o mecanismo de *Application Control* permite identificar e classificar aplicações de diferentes categorias, incluindo aplicações *Peer-to-Peer (P2P)*, conforme evidenciado pela própria documentação citada no questionamento. A partir dessa classificação, o administrador pode aplicar políticas de segurança por meio das regras de firewall, nas quais é possível definir critérios de controle baseados em usuários, grupos de usuários, redes, aplicações ou categorias de aplicações.

Uma vez identificada a categoria P2P, o firewall permite a criação de políticas que bloqueiam ou restringem esse tipo de aplicação, podendo ainda aplicar tais controles de forma granular, considerando usuários ou grupos autenticados, conforme as integrações de identidade suportadas pela solução.

Importante destacar que o funcionamento por meio de políticas adicionais mencionado, não constitui limitação da solução, mas sim característica inerente ao modelo de funcionamento de firewalls de próxima geração (NGFW), nos quais os mecanismos de inspeção e controle são aplicados de forma integrada às políticas de segurança configuradas pelo administrador.

Dessa forma, a existência da categoria P2P no mecanismo de classificação de aplicações, aliada à capacidade de aplicação de políticas baseadas em usuários e grupos, evidencia que a solução ofertada possui todos os elementos necessários para bloquear aplicações P2P e controlar transferências de arquivos conforme os critérios estabelecidos nas políticas de segurança.

Mais uma vez, resta demonstrado que a solução ofertada atende plenamente ao requisito previsto no edital, não havendo qualquer limitação funcional que impeça a aplicação de controles sobre aplicações P2P por usuário ou grupo.

scansource
Endereço: Av. Paulista, 2300 – 16º andar
Bela Vista - Conj. 161, 163 e 164, São Paulo
SP, 01310-300
Telefone: (11) 3049-0310
Site: www.scansource.com.br

Item	Exigência	Documentação Referenciada no questionamento	Necessidade de esclarecimento
1.3.1.2.y	*TLS inspection por política (TLS 1.2 e TLS 1.3).*	*https://docs.sophos.com/nsg/sophos-firewall/19.0/Help/en-us/webhelp/onlinehelp/AdministratorHelp/RulesAndPolicies/SSL/TLSInspectionRules/SSLTLSInspectionSettings/ • TLS 1.3 compatibility • Página: N/A (WebHelp)*	*Não foi encontrada literalidade 'Inbound/Outbound' exatamente como no edital no trecho citado.*

Em relação ao referido item ***1.3.1.2.y – TLS inspection por política (TLS 1.2 e TLS 1.3)***, novamente insiste na mesma justificativa e afirma que o trecho da documentação apresentado não contém menção literal aos termos "Inbound/Outbound", conforme descrito no edital.

O firewall Sophos possui mecanismo de TLS/SSL Inspection baseado em políticas, permitindo a inspeção e descriptografia de tráfego criptografado conforme regras configuradas pelo administrador. Conforme evidenciado na documentação citada, a solução suporta TLS 1.2 e TLS 1.3, incluindo a capacidade de interceptar e descriptografar sessões TLS, aplicando inspeção de segurança sobre o tráfego protegido.

A aplicação dessas políticas ocorre diretamente nas regras de firewall, nas quais é possível definir critérios como origem, destino, usuários, aplicações e serviços, permitindo que a inspeção TLS seja aplicada tanto ao tráfego de saída (outbound) quanto ao tráfego de entrada (inbound), conforme a política configurada.

Dessa forma, a ausência de menção literal aos termos "inbound/outbound" no trecho específico da documentação não implica limitação funcional da solução, uma vez que a inspeção TLS é aplicada por meio das políticas de firewall, que naturalmente controlam o fluxo de tráfego em ambos os sentidos.

Novamente resta demonstrado que a solução ofertada suporta inspeção TLS por política, incluindo TLS 1.2 e TLS 1.3, atendendo integralmente ao requisito estabelecido no edital.

scansource®
Endereço: Av. Paulista, 2300 – 16º andar
Bela Vista - Conj. 161, 163 e 164, São Paulo
SP, 01310-300
Telefone: (11) 3049-0310
Site: www.scansource.com.br

Item	Exigência	Documentação Referenciada no questionamento	Necessidade de esclarecimento
1.3.1.2.z	*ARP bridging .*	*https://docs.sophos.com/ nsg/sophos-firewall/19.0/Help/en- us/webhelp/onlinehelp/AdministratorHelp/Networ k/Interfaces/NetworkBridgeInterfaceAdd/ • Add a bridge interface • Página: N/A (WebHelp)*	*Não aparece a expressão "ARP bridging" como funcionalidade nomeada; evidência é por comportamento de bridge.*

Em atenção ao referido item ***1.3.1.2.z – ARP bridging***, o órgão afirma que a documentação apresentada não menciona explicitamente a funcionalidade denominada "ARP bridging", argumentando que a evidência apresentada se refere apenas ao comportamento de interfaces em modo bridge.

Conforme evidenciado anteriormente na documentação citada, o Sophos Firewall suporta a criação de interfaces em modo bridge, nas quais o equipamento atua na camada 2 da rede, permitindo o encaminhamento de tráfego entre interfaces pertencentes ao mesmo domínio de broadcast, incluindo o encaminhamento de broadcasts ARP, conforme indicado no próprio trecho citado *("Bridge interfaces forward ARP broadcasts…").* Adicionalmente, é importante destacar que o entendimento acerca deste requisito já foi objeto de esclarecimento formal junto ao órgão, conforme registrado no processo licitatório. Na ocasião, foi questionado se a finalidade técnica do requisito seria garantir mecanismos capazes de inspecionar, controlar e preservar a integridade do domínio ARP da rede, prevenindo cenários como ARP spoofing, ARP storm e associações indevidas entre endereços IP e MAC.

Em resposta, o órgão confirmou que esse entendimento está correto, indicando que o requisito pode ser atendido por mecanismos que permitam inspeção, controle e limitação do tráfego ARP na interface, com o objetivo de preservar a integridade do domínio de broadcast e garantir a segurança do tráfego na rede.

Dessa forma, resta evidenciado que a funcionalidade de bridge de interfaces com encaminhamento de tráfego ARP, aliada aos mecanismos de controle e inspeção presentes na solução, atende plenamente à finalidade técnica do requisito estabelecido no edital, conforme confirmado pelo próprio órgão em fase de esclarecimentos.

Portanto, a alegação se baseia apenas na ausência da nomenclatura literal *"ARP bridging"* na documentação, o que não caracteriza ausência da funcionalidade nem descumprimento do requisito e sua finalidade.

Em face do exposto, o argumento apresentado não procede, devendo ser mantida a decisão que considerou o atendimento do requisito pela solução ofertada.

Item	Exigência	Documentação Referenciada no questionamento	Necessidade de esclarecimento
1.3.1.2.aa	*Limite de taxa ARP por IP (anti ARP storm).*	*https://docs.sophos.co m/nsg/sophos- firewall/19.0/Help/en-us/webhelp/onlinehelp/ AdministratorHelp/Net work/Interfaces/Netwo rkBridgeInterfaceAdd/ • Add a bridge interface • Página: N/A (WebHelp)*	*Evidência cobre mitigação de storm por ARP broadcast, mas não comprova "rate limit ARP por IP".*

Em atenção ao item ***1.3.1.2.aa – Limite de taxa ARP por IP (anti ARP storm)***, o órgão afirma que a documentação apresentada evidencia apenas mecanismos de mitigação de broadcast storm, não comprovando especificamente a funcionalidade denominada *"rate limit ARP por IP".*

Conforme evidenciado na referida documentação supracitada, o firewall da Sophos possui mecanismos de controle de tráfego em interfaces de rede capazes de detectar e mitigar situações de broadcast storm, incluindo cenários relacionados ao protocolo ARP, que podem causar degradação da comunicação na camada 2 da rede.

Adicionalmente, importante destacar que o entendimento acerca da finalidade técnica deste requisito foi objeto de esclarecimento formal junto ao órgão, no qual foi questionado se o atendimento ao item poderia ser comprovado por meio de mecanismos capazes de detectar, controlar e mitigar comportamentos anômalos relacionados ao protocolo ARP, preservando a estabilidade da rede.

Em resposta, o órgão confirmou que esse entendimento está correto, indicando que o requisito pode ser atendido por funcionalidades que permitam prevenir degradações causadas por excesso de tráfego ARP, como instabilidade de comunicação, sobrecarga de tabelas ARP e possíveis cenários de negação de serviço.

Dessa forma, fica evidente que a solução ofertada atende à finalidade técnica do requisito, ao disponibilizar mecanismos capazes de controlar e mitigar tráfego ARP excessivo na rede, prevenindo cenários de ARP storm, conforme confirmado pelo próprio órgão em fase de esclarecimentos.

A alegação apresentada se baseia apenas na sustentação de nomenclatura literal específica na documentação, assim como diversos itens de questionamentos anteriores aqui supracitados já esclarecidos de forma inequívoca, portanto conclui-se que não caracteriza ausência da funcionalidade nem descumprimento do requisito, o argumento apresentado não procede, devendo ser mantida a decisão que considerou o atendimento do requisito pela solução ofertada.

scansource
Endereço: Av. Paulista, 2300 – 16º andar Bela Vista - Conj. 161, 163 e 164, São Paulo SP, 01310-300
Telefone: (11) 3049-0310
Site: www.scansource.com.br

Item	Exigência	Documentação Referenciada no questionamento	Necessidade de esclarecimento
1.3.1.2.ab	*Visualização gráfica das regras de segurança e acesso.*	*(Não localizado em documentação Sophos consultada)*	Comprovação da exigência do edital;

Em atenção ao item ***1.3.1.2.ab – Visualização gráfica das regras de segurança e acesso***, o órgão afirma não ter localizado evidência da funcionalidade na documentação consultada.

Entretanto, o firewall Sophos possui interface administrativa gráfica (GUI) que permite a visualização e gerenciamento das regras de firewall e políticas de acesso de forma visual e estruturada, apresentando elementos como origem, destino, serviços e políticas associadas.

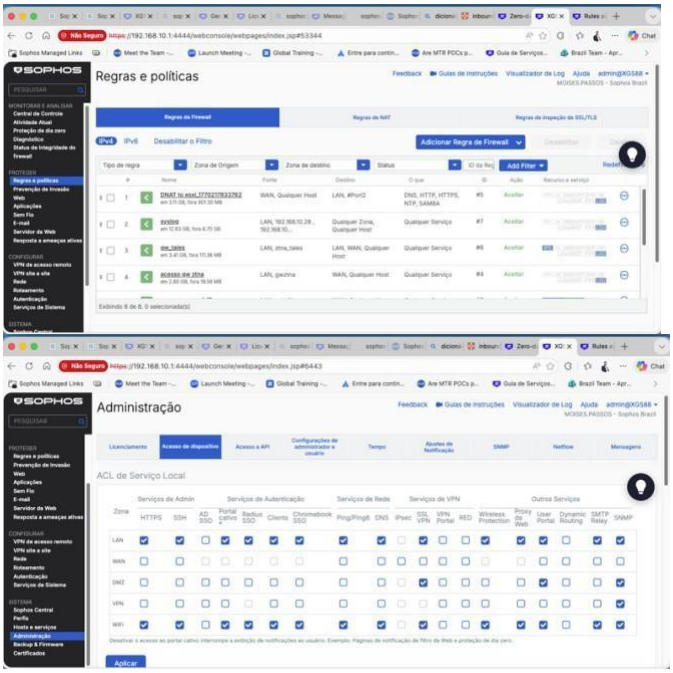
Dessa forma, a funcionalidade de visualização gráfica das regras de segurança está presente na solução ofertada, sendo característica inerente à interface de administração do equipamento.
Assim, a alegação apresentada baseia-se apenas na ausência de referência específica no trecho de documentação consultado, o que não caracteriza ausência da funcionalidade.

Para que não reste dúvidas, listamos duas comprovações, a primeira referente as regras de firewalls e a segunda referente aos acessos de zonas, e portais da solução.

https://docs.sophos.com/nsg/sophos-firewall/22.0/help/en-us/webhelp/onlinehelp/AdministratorHelp/Administration/DeviceAccess/index.html

https://docs.sophos.com/nsg/sophos-firewall/22.0/help/en-us/webhelp/onlinehelp/AdministratorHelp/RulesAndPolicies/index.html

scansource®
Endereço: Av. Paulista, 2300 – 16º andar
Bela Vista - Conj. 161, 163 e 164, São Paulo
SP, 01310-300
Telefone: (11) 3049-0310
Site: www.scansource.com.br



Item	Exigência	Documentação Referenciada no questionamento	Necessidade de esclarecimento
1.3.1.3.h	*L2TP (incl. iOS/Android).*	*https://docs.sophos.com/nsg/sophos-firewall/21.5/Help/en-us/webhelp/onlinehelp/AdministratorHelp/RemoteAccessVPN/L2TP/ • L2TP • Página: N/A (WebHelp)*	*Sem menção literal iOS/Android no contexto de L2TP nessa doc.*

Em atenção ao item ***1.3.1.3.h – Suporte a VPN L2TP (incluindo iOS e Android)***, o órgão afirma que a documentação citada não apresenta menção literal aos sistemas iOS e Android no contexto do protocolo L2TP.

No firewall Sophos, possui suporte ao protocolo L2TP, conforme descrito na documentação citada, permitindo a implementação de conexões VPN de acesso remoto baseadas nesse padrão. Os sistemas operacionais Apple iOS e Android possuem suporte nativo ao protocolo L2TP e IPsec, possibilitando a conexão direta utilizando os recursos nativos do próprio sistema operacional, sem necessidade de aplicações adicionais, adicionalmente, o entendimento deste requisito foi objeto de esclarecimento formal junto ao órgão, no qual foi confirmado que o atendimento ao item é considerado válido desde que a solução permita conexão VPN nativa nos sistemas operacionais mencionados, utilizando os mecanismos suportados por cada plataforma.

Dessa forma, considerando que o Sophos Firewall suporta VPN L2TP, IPsec, e que os sistemas iOS e Android possuem suporte nativo a esse protocolo, resta demonstrado que a solução atende plenamente à finalidade técnica do requisito.

Assim, a alegação apresentada baseia-se apenas na ausência de menção literal aos sistemas operacionais no trecho específico da documentação, o que não caracteriza ausência da funcionalidade.

Item	Exigência	Documentação Referenciada no questionamento	Necessidade de esclarecimento
1.3.1.3.m	*Conectar redes com endereços "inválidos" via IPsec tunnel (IP-over-IP).*	*https://docs.sophos.c om/nsg/sophos-firewall/20.0/Help/en - us/webhelp/onlinehel p/AdministratorHelp/ RulesAndPolicies/NAT Rules/HowToArticles/ • Overlapping subnets in site-to-site IPsec tunnels • Página: N/A (WebHelp)*	*Cobertura para subnets sobrepostas/NAT; não há literalidade de "endereços inválidos" e "IP sobre IP" como redigido.*

Em atenção ao item ***1.3.1.3.m – Conectar redes com endereços "inválidos" via túnel IPsec (IP-over-IP)***, o órgão afirma que a documentação citada aborda apenas cenários de subnets sobrepostas (overlapping subnets) utilizando NAT, não apresentando menção literal aos termos *"endereços inválidos" ou "IP-over-IP".*

Esclarece que a solução Sophos suporta a interconexão de redes com endereçamento sobreposto ou conflitante por meio de túneis IPsec associados a políticas de NAT, mecanismo amplamente utilizado para viabilizar comunicação entre redes que utilizam faixas de IP não roteáveis ou sobrepostas, comum entre soluções de firewall de mercado.

Conforme descrito na documentação citada, a solução permite a configuração de "*overlapping* subnets" em túneis IPsec site-to-site, o que possibilita a tradução de endereços e a comunicação entre redes que, de outra forma, não poderiam ser interconectadas diretamente.

Resta demonstrado que a solução atende plenamente à finalidade técnica do requisito, permitindo a conexão entre redes com endereçamento conflitante ou não roteável por meio de túnel IPsec, conforme previsto no edital. Assim, a alegação apresentada tenta fundamentar apenas na ausência de nomenclatura literal específica na documentação, característica presente em diversos itens aqui esclarecidos, portanto não caracteriza ausência da funcionalidade, reiterando que o argumento apresentado não procede, devendo ser mantida a decisão da comissão quanto à classificação da proposta vencedora.

Item	Exigência	Documentação Referenciada no questionamento	Necessidade de esclarecimento
1.3.1.3.n	*Troca de chaves manual + IKE/IKEv2; PSK + certificado s + XAUTH.*	*https://docs.sophos.c om/nsg/sophos-firewall/21.0/api/conf igure/vpn/vpnprofile/ operations/AddVPNP olicy%26EditVPNPolic y.html • Add VPN Policy / Edit VPN Policy (API) • Página: N/A (HTML)*	*Provas separadas para Manual, ikev1/ikev2 e XAuth; não em um único trecho combinado com PSK/cert.*

scansource®
Endereço: Av. Paulista, 2300 – 16º andar
Bela Vista - Conj. 161, 163 e 164, São Paulo
SP, 01310-300
Telefone: (11) 3049-0310
Site: www.scansource.com.br

Em relação ao item ***1.3.1.3.n – Troca de chaves manual e automática (IKE/IKEv2), com suporte a PSK, certificados e XAUTH***,

O órgão afirma que as evidências apresentadas estariam distribuídas em trechos distintos da documentação, não constando em um único trecho combinado, afirmação que não procede.
A solução ofertada, Sophos Firewall suporta a configuração de métodos de troca de chaves manual ou automática, bem como os protocolos IKE, IKEv2, além de mecanismos de autenticação baseados em PSK *(pre-shared key),* certificados digitais e XAUTH, conforme descrito na documentação técnica da solução.
A eventual apresentação dessas funcionalidades em seções distintas da documentação não caracteriza ausência da funcionalidade, mas apenas a forma de organização do material técnico do fabricante.
Dessa forma, não há prejuízo e resta demonstrado que a solução ofertada suporta os mecanismos de troca de chaves e autenticação requeridos, atendendo plenamente ao requisito estabelecido no edital.

Item	**Exigência**	**Documentação Referenciada no questionamento**	**Necessidade de esclarecimento**
1.3.1.3.o	*Interoperabilidade nominal com Cisco/Check Point/Juniper/Palo Alto/Fortinet/Sonic Wall.*	*https://docs.sophos.com/ns g/sophos-firewall/19.0/Help/en- us/webhelp/onlinehelp/AdministratorHelp/SiteToSiteV PN/IPsec/ • IPsec connections • Página: N/A (WebHelp)*	*Documentação consultada não lista nominalmente os fabricantes exigidos.*

Em atenção ao Item ***1.3.1.3.o – Interoperabilidade com outros fabricantes***

O argumento apresentado pelo órgão não procede, a solução suporta VPN IPsec baseada em padrões abertos, permitindo interoperabilidade com equipamentos de terceiros que utilizem os mesmos padrões de mercado.

Esse modelo de interoperabilidade não depende da listagem nominal de fabricantes específicos na documentação, sendo inerente ao uso de protocolos padronizados como IPsec, IKEv1 e IKEv2.
Assim, equipamentos de fabricantes como Cisco, Check Point, Juniper, Palo Alto, Fortinet, SonicWall, entre outros, podem estabelecer túneis IPsec desde que configurados com parâmetros compatíveis.

Portanto, o requisito permanece plenamente atendido.

"Edital pede avaliação por órgão terceiro independente. Sophos está no Gartner MQ, porém não há certificação NSS Labs "Recommended" recente publicada para XGS Series no docs.sophos.com."

Em relação ao apontamento referente à ausência de certificação NSS Labs "Recommended" para a série Sophos XGS, cumpre esclarecer conforme item destacado abaixo, no qual o edital estabelece como requisito a existência de avaliação por órgão terceiro independente, não restringindo ou vinculando tal comprovação exclusivamente ao laboratório mencionado mas sim como exemplo.

"Exigir testes de desempenho certificados (ex.: NSS Labs, ICSA, comparativos independentes);"

A solução Sophos Firewall é regularmente avaliada por instituições independentes de reconhecida credibilidade internacional, destacando-se sua presença no Gartner Magic Quadrant para Network Firewalls, estudo conduzido por organização analista independente que avalia fabricantes com base em critérios técnicos e de capacidade de execução.

Tendo em vista que o NSS Labs deixou de existir em 15 de outubro de 2020, ainda assim, nesse contexto do NSS Labs, a Sophos esteve presente no último teste em julho de 2019, conforme evidências:

https://nsslabs.com/the-archive/
https://pt.scribd.com/document/441892648/nss-labs-2019-ngfw-security

Dessa forma, a solução ofertada atende plenamente ao requisito de avaliação por entidade independente, sendo irrelevante a inexistência de certificação específica do NSS Labs, Pós 2019, sobretudo considerando que o edital não restringe o atendimento a esse laboratório em particular.

Assim, é possível concluir que o argumento apresentado não procede, devendo ser mantida a decisão da comissão quanto à classificação da proposta vencedora.

"NPTv6/NAT66 não é suportado nativamente no Sophos Firewall SFOS. Suporta NAT64 e dual-stack IPv6 mas não NPTv6."

Em atenção à alegação de que o Sophos Firewall não suportaria NPTv6, cumpre esclarecer que o requisito do edital estabelece expressamente que a solução "deve implementar Network Prefix Translation (NPTv6) ou NAT66", ou seja, trata-se de requisito alternativo, bastando a implementação de uma das duas tecnologias.

A solução ofertada implementa NAT66, funcionalidade que permite a tradução de endereços IPv6 entre redes distintas, atendendo plenamente à finalidade técnica do requisito, que é prevenir cenários de roteamento assimétrico e viabilizar a interoperabilidade entre domínios IPv6 com diferentes prefixos.

A argumentação apresentada incorre ainda em equívoco técnico ao mencionar NAT64, tecnologia distinta utilizada para interoperabilidade entre redes IPv6 e IPv4, não relacionada ao requisito previsto no edital.

Dessa forma, ao ignorar a alternativa "OU NAT66" expressamente prevista no texto do edital e ao afirmar inexistência de suporte à funcionalidade exigida, o órgão apresenta interpretação incorreta do requisito técnico.

https://docs.sophos.com/nsg/sophos-firewall/22.0/Help/en-us/webhelp/onlinehelp/AdministratorHelp/AdvancedServices/IPv6FeaturesServices/index.html#vpn

Assim, resta demonstrado que a solução ofertada atende plenamente ao requisito deste edital, motivo pelo qual o argumento apresentado não procede, devendo ser mantida a decisão da comissão quanto à classificação da proposta vencedora.

"Gerenciamento centralizado de políticas de IPS individuais, rotas, PBR (Policy Based Routing), sandbox e controle de banda não é suportado diretamente via Sophos Central. Estas configurações requerem acesso ao Web Admin local de cada firewall."

Em relação à alegação de que determinadas funcionalidades, como configuração individual de políticas de IPS, rotas, Policy Based Routing, sandbox e controle de banda, não seriam suportadas por meio de gerenciamento centralizado, cabe esclarecer que tal interpretação não reflete corretamente a arquitetura de gerenciamento da solução.

Endereço: Av. Paulista, 2300 – 16º andar
Bela Vista - Conj. 161, 163 e 164, São Paulo
SP, 01310-300
Telefone: (11) 3049-0310
Site: www.scansource.com.br

O firewall Sophos opera em modelo de gerenciamento híbrido, no qual o Sophos Central fornece funcionalidades de orquestração, monitoramento, inventário, visibilidade, alertas, atualização e gestão centralizada de múltiplos dispositivos, enquanto determinadas configurações avançadas de rede podem ser realizadas diretamente na interface administrativa do equipamento.

Tal modelo é comum em soluções de segurança corporativa, permitindo que funcionalidades críticas e específicas de infraestrutura de rede sejam configuradas com maior granularidade no próprio dispositivo, sem comprometer a capacidade de gestão centralizada do ambiente.

Importante destacar que o requisito do edital se refere à capacidade de gerenciamento centralizado da solução, o que é plenamente atendido pela arquitetura do Sophos Central, que permite administrar múltiplos dispositivos de forma unificada, mantendo visibilidade e controle sobre o ambiente.

Dessa forma, a alegação apresentada não caracteriza ausência de funcionalidade ou descumprimento do requisito, mas apenas descreve uma característica de arquitetura comum em soluções de firewall corporativo

"Geo-IP baseado em países é suportado nas regras de firewall, mas a funcionalidade de listas customizadas de Geo-IP pode requerer configuração manual de IP lists, não um módulo dedicado de Geo-IP."

Em relação à alegação de que a solução não possuiria funcionalidade adequada de Geo-IP com listas customizadas, cabe esclarecer que o Sophos Firewall possui suporte nativo à aplicação de políticas baseadas em geolocalização por país, permitindo bloquear ou permitir tráfego conforme a origem geográfica nas próprias regras de firewall.

Adicionalmente, a solução permite a criação e utilização de listas customizadas de endereços IP ou redes, que podem ser aplicadas nas políticas de segurança para complementar controles específicos quando necessário, assim, ainda que determinadas customizações possam ser realizadas por meio da definição de listas de IP, tal abordagem atende plenamente à finalidade técnica do requisito, que é possibilitar o controle de acesso baseado em origem geográfica.

Importante destacar que o edital não exige a existência de um módulo dedicado de Geo-IP customizado, mas sim a capacidade de implementar políticas de controle baseadas em localização geográfica, o que é plenamente suportado pela solução ofertada.
Dessa forma, a alegação apresentada não caracteriza ausência de funcionalidade ou descumprimento do requisito.

"Sophos ZTNA não possui PoP (Point of Presence) dedicado no Brasil operando na própria infraestrutura do fabricante. O ZTNA gateway é implantado on-premises na infraestrutura do cliente ou integrado ao Sophos Firewall, minimizando a dependência de PoPs remotos."

Quanto à alegação de que o Sophos ZTNA não possui PoP dedicado no Brasil e que o fabricante não operaria infraestrutura própria no país, trata-se de afirmação incorreta e induz a erro.

A Sophos mantém data center do Sophos Central no Brasil (São Paulo), destinado a hospedagem e gestão regionalizada, atendendo requisitos de soberania e residência de dados, o que evidencia infraestrutura oficial do fabricante em território nacional. O Sophos ZTNA (em especial na modalidade ZTNA-as-a-Service / Sophos Cloud gateway) utiliza pontos de presença (PoPs) regionais e permite inclusive seleção/troca de região de PoP via Sophos Central, reforçando que o serviço não se limita a uma implantação exclusivamente "sem PoPs".

Por fim, é importante separar os conceitos: o ZTNA da Sophos suporta múltiplos modelos de implantação, incluindo gateway, conector na infraestrutura do cliente ou integrado ao Sophos Firewall, o que reduz dependência de conectividade externa; porém isso não autoriza o órgão a concluir inexistência de infraestrutura regional ou PoPs do fabricante, nem a descaracterizar as capacidades do serviço.

https://www.sophos.com/pt-br/press/press-releases/2022/05/sophos-opens-data-center-in-brazil

Dessa forma, resta demonstrado que a alegação apresentada não procede, devendo ser mantida a decisão da comissão quanto à classificação da proposta vencedora.

"ChromeOS não é suportado com agente ZTNA nativo. O Sophos Protected Browser (Chromium-based) pode fornecer acesso a aplicações web em ChromeOS, mas não substitui um agente ZTNA completo com todas as funcionalidades de postura e tunelamento."

Em atenção a argumentação de que ChromeOS não seria suportado pela solução ZTNA, verifica-se novamente interpretação equivocada do escopo da funcionalidade. O Sophos ZTNA foi projetado para prover acesso seguro a aplicações corporativas por múltiplos métodos de conexão, incluindo agentes dedicados para sistemas operacionais suportados e acesso baseado em navegador, quando aplicável.

O órgão incorre em equívoco ao misturar o conceito de agente ZTNA com o Sophos Secure Protected Browser, que constitui tecnologia complementar voltada à proteção de acesso via navegador, não sendo requisito obrigatório para funcionamento do ZTNA, reiterando que a oferta cobre a entrega de um conjunto de tecnologias listadas no Workspace.

Importante destacar que o edital não exige suporte por agente nativo específico para ChromeOS, mas sim a capacidade de prover acesso seguro às aplicações corporativas por meio de arquitetura ZTNA, o que é plenamente atendido pela solução ofertada.

"A integração nativa em tempo real com IBM QRadar pode requerer configuração adicional de syslog forwarding. Não há conector nativo pré-configurado para todos os SIEMs listados diretamente do módulo ZTNA."

A alegação de ausência de integração nativa com plataformas SIEM específicas, como IBM QRadar, a argumentação apresentada não procede, o próprio texto do edital menciona plataformas como Splunk, IBM QRadar e Microsoft Sentinel apenas a título exemplificativo, não estabelecendo obrigatoriedade de conectores dedicados ou integrações proprietárias específicas para cada solução.

O requisito técnico estabelecido refere-se à capacidade de envio de logs em tempo real para plataformas SIEM, o que é plenamente suportado pela solução ofertada por meio de mecanismos padrão de mercado, como Syslog e APIs, amplamente utilizados para integração entre soluções de segurança e plataformas de correlação de eventos.

Importante destacar que sistemas SIEM, incluindo o próprio IBM QRadar, são projetados justamente para ingestão de eventos por meio desses protocolos padronizados, não dependendo necessariamente de conectores proprietários para cada fabricante, assim a possibilidade de exportação de logs em tempo real para plataformas SIEM por meio de mecanismos padronizados atende integralmente à finalidade técnica do requisito previsto no edital. Deste modo, o argumento apresentado não procede, devendo ser mantida a decisão da comissão quanto à classificação da proposta vencedora.

"O Security Heartbeat do Sophos ZTNA opera como indicador agregado de saúde (green/yellow/red) baseado no status do Sophos Intercept X. Não suporta validação granular individual de cada tipo listado (disco cifrado, chave de registro, certificado específico, arquivo específico) como checks de postura independentes."

A argumentação apresentada incorre em interpretação técnica incompleta ao afirmar que a solução realiza validação de postura exclusivamente por meio do Security Heartbeat.

Tal recurso representa apenas um dos mecanismos de avaliação de saúde do endpoint, utilizado como indicador agregado do estado de segurança baseado na telemetria do Sophos Intercept X. Entretanto, a arquitetura da solução inclui mecanismos adicionais de verificação de postura no contexto do Sophos ZTNA e do Sophos Protected Browser. Conforme documentação oficial do fabricante, é possível definir objetos de postura de dispositivo (Device Posture) que permitem aplicar políticas de acesso considerando atributos do dispositivo, tais como sistema operacional, presença e estado da proteção de endpoint, bem como o estado geral de saúde do dispositivo antes da concessão de acesso às aplicações.

Esses controles podem ser utilizados em políticas de acesso para aplicações publicadas via ZTNA, permitindo que o acesso seja condicionado à conformidade do dispositivo com os critérios de segurança definidos pelo administrador.

Dessa forma, a interpretação apresentada, ao considerar apenas o Security Heartbeat como único mecanismo de validação de postura, não reflete a arquitetura completa da solução, conduzindo a conclusão técnica equivocada quanto ao atendimento do requisito previsto no edital. Assim, resta demonstrado que a solução ofertada atende plenamente à finalidade técnica do requisito, motivo pelo qual o argumento apresentado não procede, devendo ser mantida a decisão da comissão quanto à classificação da proposta vencedora.

"Resolução DNS via conector instalado na infraestrutura da contratante como componente dedicado de DNS protection não é uma funcionalidade explícita. O ZTNA gateway pode resolver DNS localmente, mas não é apresentado como componente de DNS protection dedicado."

A argumentação apresentada é baseada em interpretação restritiva do requisito ao afirmar que a solução

deveria possuir um "componente dedicado de DNS protection".
O texto do edital, estabelece como requisito a resolução DNS via conector ou componente implantado na infraestrutura da contratante, no contexto da conectividade segura às aplicações privadas, não exigindo a existência de um produto específico ou módulo separado denominado "DNS protection". Na arquitetura do Sophos ZTNA, o ZTNA Gateway, implantado na infraestrutura da contratante, realiza a resolução e encaminhamento de requisições DNS necessárias ao acesso às aplicações privadas, integrando-se ao ambiente interno e permitindo a correta localização dos recursos protegidos. A funcionalidade requerida pelo edital encontra-se plenamente atendida pela arquitetura da solução ofertada, sendo incorreta a interpretação apresentada pela órgão ao exigir um componente dedicado não previsto no texto do edital.

Além dos aspectos técnicos já demonstrados, cumpre destacar que diversos pontos levantados já foram objeto de esclarecimentos formais prestados pela própria Administração durante a fase de questionamentos do edital, conforme documentos oficiais anexados ao processo.

Conforme se observa nas respostas às Questões 19 a 25, o órgão esclareceu de forma expressa a finalidade técnica dos requisitos relacionados à arquitetura de acesso seguro, postura de dispositivos, proteção DNS, CASB, SaaS, conectividade por múltiplos conectores e criptografia das comunicações, deixando claro que o objetivo do edital é garantir funcionalidade, segurança e interoperabilidade, não a obrigatoriedade de arquiteturas específicas, produtos adicionais ou implementações restritivas.

"Exigência:
Deve suportar Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;

Necessidade de esclarecimento:
Modo Sniffer (inspeção via porta espelhada) não é documentado como funcionalidade nomeada no Sophos Firewall. Bridge mode existe mas não é o mesmo que Sniffer."
Embora a solução ofertada da Sophos não utilize explicitamente a nomenclatura *"Modo Sniffer",* a funcionalidade de inspeção de tráfego por meio de porta espelhada (port mirroring/SPAN) é suportada pela solução por meio do Network Discovery Mode, permitindo que o equipamento opere de forma passiva recebendo tráfego espelhado da rede para fins de análise e inspeção.

Nesse modo de operação, o firewall pode ser conectado a uma porta espelhada do switch para monitoramento do tráfego sem interferência no fluxo de rede, atendendo ao conceito funcional do chamado *"modo sniffer*".

A documentação oficial que descreve esse modo de operação, disponível no link a seguir:
https://docs.sophos.com/nsg/sophos-firewall/22.0/help/en-us/webhelp/onlinehelp/AdministratorHelp/Network/HowToArticles/NetworkDiscoverModeDeploy/index.html

"Exigência:

Ajudando a identificar explorações de vulnerabilidades, intrusões e outras ameaças.

Deve permitir a emissão deste relatório em formato PDF;

Necessidade de esclarecimento:

Relatório de vulnerabilidades com exportação PDF é disponível via Sophos Central,

não diretamente no appliance local."
A solução da Sophos atende ao requisito descrito no edital, permitindo a identificação de vulnerabilidades, intrusões e outras ameaças por meio dos mecanismos de inspeção e geração de relatórios do sistema.

O Sophos possibilita a geração e exportação de relatórios em formato PDF, funcionalidade disponível tanto localmente no appliance quanto por meio da plataforma de gerenciamento centralizado Sophos Central, que consolida eventos e análises de segurança, arquitetura essa que permite que relatórios detalhados de segurança sejam gerados e exportados em formato PDF para fins de auditoria, análise e acompanhamento operacional, atendendo plenamente ao requisito estabelecido no edital, portanto a afirmação de ter relatórios somente no Sophos central é tecnicamente e incorreta e não merece prosperar.
Conforme documentação anexa abaixo, consta a referencia dos relatórios bem como imagem de exemplo onde consta PDF listado nas opções de exportação.

https://docs.sophos.com/nsg/sophos-firewall/22.0/help/en-us/webhelp/onlinehelp/AdministratorHelp/Reports/ReportsDownload/index.html

"Exigência:
Deve permitir a emissão deste relatório em formato PDF;
Necessidade de esclarecimento:
Exportação de relatórios em formato PDF pode ser limitada a alguns tipos específicos de relatório. Sophos Central Firewall Reporting Advanced oferece opções mais abrangentes de exportação."

A solução Sophos atende ao requisito estabelecido no edital, permitindo a geração e exportação de relatórios em formato PDF, essa funcionalidade pode ser realizada diretamente no Sophos Firewall, bem como por meio das plataformas de gerenciamento e relatórios da solução, incluindo Sophos Central e Sophos Central Firewall Reporting (CFR), este último contemplado na proposta apresentada.

O CFR como complemento, também disponibiliza recursos avançados de geração, consolidação e exportação de relatórios, incluindo a emissão em formato PDF, ampliando as capacidades de análise e auditoria de eventos de segurança para múltiplos equipamentos.

Dessa forma, a solução proposta atende plenamente ao requisito de emissão de relatórios em formato PDF conforme solicitado no edital.

"Exigência:
A solução deve permitir a criação de modelos de configuração ou "Templates" para aplicá-los em grupos de dispositivos. Os modelos de configurações devem permitir visualização e edição para sua aplicação nos firewalls Os modelos de configuração ou "templates" devem suportar configurações de interfaces físicas ou virtuais;

Necessidade de esclarecimento:
Templates de configuração no Sophos Central têm cobertura limitada para configurações de interfaces físicas. Configurações detalhadas de interfaces devem ser realizadas localmente no Web Admin de cada firewall."
A solução ofertada da Sophos permite a criação de modelos de configuração "templates" que podem ser aplicados a grupos de dispositivos, por meio da plataforma de gerenciamento centralizado Sophos Central, modelos estes que permitem visualização, edição e aplicação centralizada das configurações antes da implantação nos firewalls, possibilitando padronização e controle das mudanças aplicadas no ambiente.

No que se refere às configurações de interfaces físicas ou virtuais, a solução suporta esse tipo de configuração nos equipamentos gerenciados. É importante considerar que a quantidade, o tipo e a nomenclatura das interfaces podem variar entre diferentes modelos de firewall, incluindo interfaces físicas, VLANs, subinterfaces ou outros tipos de interfaces lógicas.

Por esse motivo, os templates são utilizados para padronização de políticas e configurações comuns entre os dispositivos, enquanto parâmetros específicos relacionados às interfaces podem ser ajustados diretamente na interface administrativa de cada equipamento que é acessada diretamente na mesma plataforma via Sophos Central, garantindo flexibilidade operacional e compatibilidade entre diferentes modelos de appliance.

Deste modo, a solução atende ao requisito estabelecido no edital quanto à criação e utilização de templates de configuração aplicáveis a grupos de dispositivos, incluindo suporte a interfaces físicas ou virtuais.
https://docs.sophos.com/central/customer/help/pt-br/ManageYourProducts/FirewallManagement/DynamicObjects/index.html

"Não foram encontrados documentos que comprovem"

A Sophos permite o controle e acompanhamento das alterações de configuração antes de sua implantação nos dispositivos gerenciados por meio do Sophos Central Firewall Management.

Quando modificações são realizadas na plataforma de gerenciamento centralizado, elas são registradas como tarefas ou transações na fila de tarefas do firewall, permitindo ao administrador acompanhar o status das alterações antes da conclusão do processo de implantação. A plataforma apresenta o estado dessas tarefas (por exemplo: pendente, em andamento, sucesso ou falha), garantindo visibilidade e controle das mudanças realizadas no ambiente antes de sua efetiva aplicação nos dispositivos, esse mecanismo de gerenciamento permite que o administrador acompanhe e valide o processo de implantação das configurações, atendendo ao requisito do edital quanto à visualização e controle das mudanças antes da implantação das configurações.

Documentação de referência:
https://docs.sophos.com/central/customer/help/en-us/ManageYourProducts/FirewallManagement/Firewalls/index.html

"Exigência:
Para cada alteração de configuração a solução deverá confirmar a aplicação da política, possibilitando a adição de comentários nas políticas instaladas, para futuras consultas de auditoria;

Necessidade de esclarecimento:
O Sophos Central não possui funcionalidade nativa de adição de comentários individuais nas políticas instaladas para fins de auditoria. O log de auditoria registra ações, mas sem campo de comentário customizado por política."

Conforme esclarecimento previamente encaminhado ao órgão durante a fase de questionamentos do edital, foi apresentada interpretação quanto ao requisito que trata da confirmação da aplicação das políticas e da rastreabilidade das alterações realizadas para fins de auditoria.

Na resposta oficial emitida pelo órgão, foi esclarecido que poderá ser aceita a validação por meio dos registros disponíveis nos equipamentos, tendo como objetivo garantir visibilidade das atividades realizadas nos dispositivos em eventuais processos de auditoria.

Reiterando em complemento com esclarecimentos anteriores sobre o tema, a solução Sophos disponibiliza mecanismos que permitem tanto a confirmação da aplicação das configurações quanto a rastreabilidade das alterações realizadas.

As alterações efetuadas por meio do gerenciamento centralizado são registradas na fila de tarefas do firewall, permitindo o acompanhamento do status das operações (por exemplo: pendente, em andamento, sucesso ou falha), o que possibilita a confirmação da aplicação das políticas nos dispositivos gerenciados.

Portanto, considerando o esclarecimento fornecido pelo órgão e os mecanismos de controle e auditoria disponíveis na solução, o requisito estabelecido no edital é devidamente atendido.

Item que foi questionado anteriormente, o qual já consta publicado anteriormente.
Questão 12:
"Para cada alteração de configuração a solução deverá confirmar a aplicação da política, possibilitando a adição de comentários nas políticas instaladas, para futuras consultas de auditoria"

Está correta a interpretação bem como o atendimento a este requisito pode ser comprovado desde que as alterações realizadas por meio do gerenciamento centralizado tenham sua aplicação confirmada nos dispositivos gerenciados e que a rastreabilidade dessas mudanças para fins de auditoria possa ser evidenciada por meio dos registros disponíveis nos próprios equipamentos?

Resposta:

Sim, a interpretação está valida, poderá ser aceito a validação dos registros no equipamento, o objetivo é ter visibilidade de atividades realizadas nos equipamentos em possíveis auditorias.

"Exigência:
Deverá permitir que configurações realizadas pelos administradores da solução sejam validadas e aprovadas (workflow), por um colaborador responsável por aprovação e aplicação de políticas, esse processo de aprovação deve ser encaminhado de forma automatizada para o responsável da aprovação via e-mail ou console da solução, possibilitando mitigar erros de configuração e impactos negativos ao ambiente ;

Necessidade de esclarecimento:
Não encontrada documentação para provar tal função."

Conforme esclarecimento previamente apresentado durante a fase de questionamentos do edital, foi solicitado entendimento quanto ao requisito relacionado ao processo de validação e aprovação de alterações realizadas pelos administradores da solução, na resposta oficial emitida pelo órgão, foi informado que o requisito poderá ser considerado atendido caso a solução ofereça meios para validação da realização das atividades juntamente com controle de perfis de gerenciamento, permitindo a supervisão das ações administrativas. Importante destacar que a solução Sophos disponibiliza controle de acesso administrativo baseado em perfis, permitindo a definição de diferentes níveis de privilégio para os administradores da solução. Adicionalmente, a plataforma mantém registros de auditoria das atividades administrativas, possibilitando a rastreabilidade das alterações realizadas e garantindo.

A plataforma registra informações detalhadas das alterações realizadas, incluindo identificação do responsável pela modificação ("Modificado por"), entidade alterada, ação executada e horário da operação, garantindo rastreabilidade e visibilidade das ações executadas no ambiente assim como mudanças realizadas para fins de auditoria, com esses mecanismos é possível ter segregação de responsabilidades na administração da solução, bem como a validação das atividades realizadas, conforme objetivo técnico estabelecido no requisito.

Considerando o esclarecimento fornecido pelo órgão em resposta aos questionamentos feitos anteriormente, mecanismos de controle administrativo e auditoria disponíveis na solução, o requisito estabelecido no edital é devidamente atendido.
https://docs.sophos.com/central/customer/help/pt-br/ManageYourProducts/FirewallManagement/TasksQueue/index.html#_tabbed_1_2

Item que foi questionado anteriormente, o qual já consta publicado anteriormente.

Questão 13:

"Deverá permitir que configurações realizadas pelos administradores da solução sejam validadas e aprovadas (workflow), por um colaborador responsável por aprovação e aplicação de políticas, esse processo de aprovação deve ser encaminhado de forma automatizada para o responsável da aprovação via e-mail ou console da solução, possibilitando mitigar erros de configuração e impactos negativos ao ambiente ;" Entendemos que a finalidade técnica deste requisito é assegurar a segregação de responsabilidades na administração da solução, permitindo que alterações realizadas sejam previamente validadas antes de sua aplicação efetiva no ambiente, de forma a mitigar

erros operacionais e impactos negativos.

Endereço: Av. Paulista, 2300 – 16º andar
Bela Vista - Conj. 161, 163 e 164, São Paulo
SP, 01310-300
Telefone: (11) 3049-0310
Site: www.scansource.com.br

Está correto o entendimento de que o atendimento a este requisito possa ser comprovado desde que a solução disponha de mecanismos que permitam controle administrativo, rastreabilidade das alterações realizadas e possibilidade de validação prévia à sua aplicação, garantindo a supervisão por responsável distinto conforme previsto no item?

Resposta:

Sim, o entendimento está correto, caso a solução ofereça meios para validação da realização de atividades, juntamente com o controle de perfis de gerenciamento, será valido.

Esclarecimentos prestados pela Administração:

1. confirmação de que o requisito de postura de segurança do dispositivo visa compatibilidade com soluções NGAV, não sendo obrigatória a oferta do produto de endpoint no próprio processo;

2. confirmação de que os requisitos de proteção DNS e navegação segura referem-se ao uso de mecanismos de filtragem de domínios e URLs aplicados conforme contexto de usuário e dispositivo;

3. confirmação de que os requisitos relacionados a CASB, SaaS e acesso a aplicações privadas têm como objetivo garantir visibilidade, controle de acesso baseado em identidade e segregação de aplicações;

4. confirmação de que múltiplos conectores visam flexibilidade arquitetural, não impondo implementação específica desde que o acesso seguro às aplicações seja garantido;

5. confirmação de que os mecanismos de criptografia e proteção contra interceptação devem assegurar a segurança das comunicações entre usuários, plataforma e aplicações.

Esclarecimentos estes demonstram que a interpretação apresentada desconsidera o entendimento oficial já consolidado pela própria Administração durante a fase de esclarecimentos do edital, tentando impor restrições ou interpretações que não constam no instrumento convocatório nem em seus esclarecimentos formais.

Do pedido de indeferimento do recurso

Diante de todo o exposto, resta claro e amplamente demonstrado que os argumentos apresentados não encontram respaldo técnico nem documental, baseando-se em interpretações equivocadas, omissões de informações relevantes e referências a documentações desatualizadas ou fora de contexto.

Ao longo da presente análise, foram apresentadas evidências técnicas, documentação oficial do fabricante e esclarecimentos previamente fornecidos pela própria Administração deste órgão durante a fase de questionamentos do edital, comprovando de forma objetiva que a solução ofertada atende integralmente aos requisitos estabelecidos no instrumento convocatório.

Ainda que o órgão, em diversos pontos de sua manifestação, apresenta afirmações imprecisas ou enganosas acerca das capacidades da solução, inclusive desconsiderando funcionalidades existentes, confundindo tecnologias distintas e ignorando alternativas explicitamente previstas no edital, como no caso de requisitos que admitem mais de uma forma de implementação técnica. Tal conduta compromete a consistência técnica do recurso apresentado, uma vez que os argumentos utilizados não refletem corretamente as características da solução analisada nem o entendimento previamente consolidado pela Administração.

Dessa forma, não subsistem fundamentos técnicos ou jurídicos capazes de justificar a revisão da decisão administrativa.

Requer-se, portanto, o indeferimento integral do recurso apresentado pelo órgão, com a consequente manutenção da decisão da comissão quanto à classificação da proposta vencedora, tendo em vista o pleno atendimento aos requisitos do edital e a ausência de elementos que justifiquem qualquer alteração no resultado do certame.

Endereço: Av. Paulista, 2300 – 16º andar
Bela Vista - Conj. 161, 163 e 164, São Paulo
SP, 01310-300
Telefone: (11) 3049-0310
Site: www.scansource.com.br

Itajaí, 06 de março de 2026.

Eder Luiz Gaiotti (Mar 6 , 2026 17:06: 32 GMT-3)

Eder Luiz Gaiotti
CPF: 869.709.179-91
Diretor de Controladoria

BERNARDO ATAMIAN (Mar 6, 2026 17:03:35 GMT-3)

Bernardo Der Atamian
CPF: 043.069.747- 31
Vice-Presidente Executivo

scansource

Endereço: Av. Paulista, 2300 – 16º andar
Bela Vista - Conj. 161, 163 e 164, São Paulo
SP, 01310-300
Telefone: (11) 3049-0310
Site: www.scansource.com.br

PROPOSTA FINAL

Pregão Eletrônico nº 06/2026

Data da sessão em 25/02/2026, Horário: 08h30min

Proponente: **SCANSOURCE BRASIL DISTRIBUIDORA DE TECNOLOGIAS LTDA.**

Endereço: **Rua Domingos Rampelotti, 3501 - Módulo 12 A e B - São Roque.**

Cidade: Itajaí Estado: Santa Catarina CEP: 88317-600

CNPJ/MF nº: **05.607.657/0008-01**

Telefone: (11) 3049-0300

e-mail: publicsector@scansource.com

Objeto: **Ata de registro de preços para Aquisição de solução de segurança de rede de dados da Prefeitura do Município de Hortolândia, conforme condições, quantidades e exigências estabelecidas neste Edital e seus anexos.**

DADOS BANCÁRIOS DA PROPONENTE

Banco: **341 Banco Itaú**

Número da Agência: **3722**

Número da Conta – Corrente: **14644-0**

DADOS DA(S) PESSOA(S) QUE IRÁ(AO) FIRMAR O INSTRUMENTO CONTRATUAL:

Paulo Roberto Ferreira

RG: 54.893.051-X SSP/SP – CPF: 668.694.987-68

Presidente

Endereço: Avenida Paulista, 2300, Conjuntos 161, 163 e 164 – Bela Vista.

Cidade: São Paulo Estado: São Paulo CEP: 01310-300

Eder Luiz Gaiotti

RG: 5.339.180-0 SSP/PR – **CPF:** 869.709.179-91

Diretor de Controladoria

Endereço: Avenida Paulista, 2300, Conjuntos 161, 163 e 164 – Bela Vista.

Cidade: São Paulo Estado: São Paulo CEP: 01310-300

scansource
Endereço: Av. Paulista, 2300 – 16º andar
Bela Vista - Conj. 161, 163 e 164, São Paulo
SP, 01310-300
Telefone: (11) 3049-0310
Site: www.scansource.com.br

Validade da proposta: 90 dias

Valor total da proposta: **R$ 3.178.900,00**

ITEM	COD.	DESCRIÇÃO	UND	QTD	MARCA	PREÇO UNITÁRIO	PREÇO TOTAL
01	12.3.3929	Firewall tipo 1 - XG8ETCHUS XGS 8500 Security Appliance - US power cord; Xstream Protection; Email Protection; Enhanced to Enhanced Plus Support Upgrade;	Un	02	Sophos	R$ 570.162,90	R$ 1.140.325,80
02	12.3.3930	Firewall tipo 2 - XG138Z00ZZPCUS XGS 138 Security Appliance - US power cord; Xstream Protection; Email Protection	Un	30	Sophos	R$ 25.851,66	R$ 775.549,80
03	12.3.3931	Firewall tipo 3 - XG108Z00ZZPCUS XGS 108 Security Appliance - US power cord; Xstream Protection; Email Protection	Un	110	Sophos	R$ 8.158,12	R$ 897.393,20
04	12.3.3932	Solução de Gerenciamento Centralizado e Relatório: NGFW Tipos 1, 2 e 3 – CFRAAB60BGNCAA Central Firewall Reporting Advanced	Un	01	Sophos	R$ 91.395,00	R$ 91.395,00

scansource
Endereço: Av. Paulista, 2300 – 16º andar Bela Vista - Conj. 161, 163 e 164, São Paulo SP, 01310-300
Telefone: (11) 3049-0310
Site: www.scansource.com.br

05	12.3.3933	Solução para acesso seguro à aplicação privada e ZTNA - CWP00U60ADNCAA Workspace Protection	Un	70	Sophos	R$ 2.018,64	R$ 141.304,80
06	12.3.3939	Treinamento para a solução	Un	01	Sophos	R$ 132.931,40	R$ 132.931,40
						Valor total da proposta	R$ 3.178.900,00

SCANSOURCE BRASIL DISTRIBUIDORA DE TECNOLOGIAS LTDA.

Itajaí, 27 de fevereiro de 2026.

Paulo Roberto (Feb 27, 2026 15:45:29 GMT-3)

Paulo Roberto Ferreira

Presidente

Eder Luiz Gaiotti (Feb 27, 2026 19:07:49 GMT)

EDER LUIZ GAIOTTI

Diretor de Controladoria