ESTADO DE GOIÁS
SECRETARIA DE ESTADO DA SEGURANÇA PÚBLICA
GERÊNCIA DE TELECOMUNICAÇÕES

TERMO DE REFERÊNCIA

1. OBJETO

1.1. Aquisição de Solução de Firewall incluindo garantia de atualização contínua e suporte técnico por 30(trinta) meses para proteção dos Serviços de TI hospedados no Data Center da SSP-GO.

1.2. Solução de proteção de rede com características de Next Generation Firewall (NGFW) para segurança de informação perimetral que inclui filtro de pacote, controle de aplicação, administração de largura de banda (QoS), VPN IPSec e SSL, IPS, prevenção contra ameaças de vírus, spywares e malwares, Filtro de URL, bem como controle de transmissão de dados e acesso a internet compondo uma plataforma de segurança integrada e robusta.

1.3. Visa substituição dos Contratos 124/2015(201500016000422) no valor de R$378.000,00 e 025/2016(201500016003645) no valor de R$316.000,00 que não podem mais serem renovados.

2. JUSTIFICATIVAS

2.1. A Gerência de Telecomunicações da SSP-GO tem entre suas principais atribuições:

2.1.1. "Gestão de Segurança da Informação, definição de Política de Segurança, controle de acesso, análise e correção de vulnerabilidades em aplicações e rede corporativa."

2.1.2. "Gerência e Configuração de Servidores de Virtualização, Antivírus, Firewall, Anti-Spam, Filtro de Conteúdo Web e Sistema de Prevenção de Intrusão (IPS)."

2.1.3. "Análise e especificação de ferramentas, equipamentos e serviços de TI e de Telecomunicações para aquisição ou contratação. "

Para o correto atendimento destas atribuições é necessário a existência de infraestrutura técnica visando garantia de sigilo e integridade dos dados contra acesso indevido, fornecendo segurança para estações de trabalho, dispositivos móveis e servidores de aplicações, sejam físicos ou virtuais, conectados na Rede Corporativa da Instituição.

2.2. A Lei Geral de Proteção de Dados Pessoais (LGPD) - LEI Nº 13.709, DE 14 DE AGOSTO DE 2018, que entrará em vigor a partir de Janeiro de 2021, torna obrigatório a definição de mecanismos formais que visem auxiliar no controle sobre o tratamento de dados nas instituições conforme abaixo:

"Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

"Parágrafo único. As normas gerais contidas nesta Lei são de interesse nacional e devem ser observadas pela União, Estados, Distrito Federal e Municípios."

"Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito."

"Art. 47. Os agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento obriga-se a garantir a segurança da informação prevista nesta Lei em relação aos dados pessoais, mesmo após o seu término."

2.3. De acordo com a norma internacional ISO IEC 27001:2006, que trata da certificação para Sistemas de Gestão de Segurança da Informação e apresenta entre seus conceitos fundamentais os três atributos básicos da informação: confidencialidade, integridade e disponibilidade, é necessário que esta Gerência, responsável pela Infraestrutura de TI da SSP-GO, no exercício de suas atribuições institucionais, promova e mantenha ações que permitam identificar, analisar e qualificar riscos que possam comprometer as informações que trafegam e que são acessadas por seus usuários finais.

2.4. A solução de Firewall tem como objetivo principal proteger o ambiente de Data Center da SSP-GO, onde estão hospedados a maioria dos sistemas do Órgão, contra ataques cibernéticos e invasão dos sistemas mitigando riscos de acesso indevido a serviços policiais e roubo de informações.

2.5. Atualmente a SSP-GO possui solução de Firewall ativa. No entanto a mesma não permite mais atualizações, não possui contrato de suporte e atualização vigentes, está obsoleta e deixa o ambiente vulnerável a ameaças de ataques cibernéticos.

2.6. Com a recente contratação de novos serviços de rede corporativa(202000016003430) onde houve aumento da banda dos links utilizados por todas as unidades da SSP-GO, é necessário a aquisição de solução mais robusta que permite comportar o aumento do tráfego na rede do Órgão.

2.7. Justifica-se a duração contratual pelo período de 30(trinta) meses devido ao alto impacto e alta complexidade de ativação da solução no ambiente de Data Center da SSPO. Por isso, períodos curtos de contratos podem acarretar altos custos para substituição da arquitetura sempre que for necessário a mudança do serviço.

2.8. Visa substituição dos Contratos 124/2015(201500016000422) no valor de R$378.000,00 (Firewall) e 025/2016(201500016003645) no valor de R$316.000,00(Filtro de Conteúdo Web) que não podem mais serem renovados.

2.9. Com o recente aumento da demanda por teletrabalho é imprescindível solução de segurança da informação confiável, com assinaturas de vulnerabilidades atualizadas em tempo real, garantindo respostas imediatas a ameaças cibernéticas e que tornem seguro o acesso aos Serviços de TI a usuários fora da Rede Corporativa do Órgão.

3. ESPECIFICAÇÕES, QUANTIDADE E VALORES ESTIMADOS

Quantidades e Valores Estimados

Item	Código	Descrição	QTD	Valor Unitário	Valor Total
1	63757	Equipamento de Next Generation Firewall em alta disponibilidade incluindo IPS, prevenção contra ameaças de vírus, spywares, malwares e Filtro de URL.	2	R$ 206.460,29	R$ 412.920,58
2	63795	Licenciamento de IPS, Filtro de Conteúdo Web, Suporte técnico e garantia para equipamento de Firewall para 30 meses. Suporte técnico on-site, remoto e telefônico.	2	R$ 275.676,03	R$ 551.352,06
VALOR TOTAL ESTIMADO:					**R$ 964.272,64**
O valor total estimado pelo período de 30(trinta) meses é de R$ 964.272,64 (Novecentos e sessenta e quatro mil, duzentos e setenta e dois reais e sessenta e quatro centavos)					

4. ESPECIFICAÇÕES

4.1. DESCRIÇÃO

4.1.1. Solução de proteção de rede com características de Next Generation Firewall (NGFW) para segurança de informação perimetral que inclui filtro de pacote, controle de aplicação, administração de largura de banda (QoS), VPN IPSec e SSL, IPS, prevenção contra ameaças de vírus, spywares e malwares, Filtro de URL, bem como controle de transmissão de dados e acesso a internet compondo uma plataforma de segurança integrada e robusta.

4.1.2. Por plataforma de segurança entende-se hardware e software integrados do tipo appliance.

4.2. CARACTERÍSTICAS TÉCNICAS

4.2.1. Características de Hardware Mínimas

4.2.1.1. Deve suportar a performance considerando as funcionalidades de Next Generation firewall de no mínimo 9 Gbps, com features de threat prevention habilitadas;

4.2.1.2. Deve suportar performance de VPN de, no mínimo, 10 Gbps;

4.2.1.3. Deve suportar, no mínimo, 100.000 túneis de VPN simultâneos;

4.2.1.4. Deve suportar inspecionar, no mínimo, 10 milhões de conexões TCP;

4.2.1.5. Deve suportar 50 milhões de conexões simultâneas;

4.2.1.6. Deve suportar, no mínimo, 300.000 novas conexões TCP por segundo;

4.2.1.7. Deve permitir utilizar, no mínimo, 10 (dez) contextos virtuais e permitir expansão para 25 (vinte e cinco) contextos virtuais;

4.2.1.8. Deve ser licenciado para 10.000 clientes VPN mobile;

4.2.1.9. Deve possuir as seguintes quantidades de interfaces de rede:

4.2.1.9.1. 8 (oito) interfaces de rede 1 Gbps 10/100/1000 base-TX ou SFP;

4.2.1.9.2. 8 (oito) interfaces de rede 10 Gbps SFP+;

4.2.1.9.3. 2 (duas) interfaces de rede 40 Gbps QSFP+;

4.2.1.10. Todos os produtos ofertados devem ser novos, sem uso anterior e, estar em linha de produção e comercialização pelo fabricante dos mesmos no momento da proposta, não devendo haver anúncio de "fim de produção" (EOL - End-of-Life) nem de apresentação do fim de comercialização (EOS - End-of-Sale) até esta data;

4.2.1.11. Devem ser fornecidas todas as licenças de hardware e software necessárias à implantação das funcionalidades especificadas a serem implementadas;

4.2.1.12.A Solução deve consistir em plataforma de proteção de rede baseada em hardware dedicado, em um equipamento do tipo "appliance", possuindo sistema operacional próprio para a execução das funções especificadas. Não será aceito equipamento do tipo PC (Personal Computer) ou Servidor, com sistema operacional de uso genérico, adaptado para a função aqui especificada;

4.2.1.13. Deve possuir funcionalidade SD-WAN, podendo este item ser composto por outros players, desde que possua certificação terceira NSS Labs;

4.2.1.14. Todos os produtos ofertados devem ser entregues com a última versão de software e/ou firmware disponível no momento da aquisição;

4.2.1.15. Deve possuir 1 (uma) interface para console de acesso ao equipamento com conector RJ-45, USB e/ou serial;

4.2.1.16. Deve operar na faixa de temperatura de 0 a 40°C e umidade relativa entre 10 e 90%.

4.2.2. Funcionalidades de Segurança

4.2.2.1. Deve possuir tecnologia Stateful Inspection;

4.2.2.2. Deve possuir políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança;

4.2.2.3. Deve possuir politicas baseadas em localização geográfica;

4.2.2.4. Deve suportar os seguintes tipos de negação de tráfego nas políticas de firewall:

4.2.2.4.1. Drop sem notificação do bloqueio a origem;

4.2.2.4.2. Drop com notificação do bloqueio a origem (TCP reset ou mensagem de erro ICMP);

4.2.2.4.3. Blacklist (bloqueio de conexões por determinado período de tempo) local e distribuído com base em eventos de trafego analisados pelos firewalls gerenciados;

4.2.2.5. Deve permitir controle de acesso com suporte a aplicações, serviços e protocolos pré-definidos;

4.2.2.6. Deve permitir regras a serem aplicadas em intervalos regulares de tempo, sendo determinados dias da semana e horários e determinados dias e horários do mês;

4.2.2.7. Deve possuir integração com diretórios LDAP, RADIUS, TACACS+ e Microsoft Active Directory para a autenticação de usuários;

4.2.2.8. Deve possuir capacidade de autenticação de administradores usando base interna, RADIUS, TACACS+ e LDAP;

4.2.2.9. Deve possuir capacidade de autenticar administradores com uso de certificados X.509;

4.2.2.10. Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação. Deve possibilitar o uso deste recurso como segundo fator de autenticação através de certificados;

4.2.2.11. Deve possuir suporte a controle de aplicações do tipo multimídia, tais como, voz sobre IP, áudio e vídeo streaming;

4.2.2.12. Deve suportar os seguintes tipos de NAT:

4.2.2.12..1. NAT estático: 1-pra-1,

4.2.2.12.2. Tradução de porta (PAT) N-pra-1;

4.2.2.12.3. Suportar NAT de Origem;

4.2.2.13. Deve suportar definir o tráfego de saída baseado em aplicação web 2.0 suportando no mínimo as seguintes aplicações: Facebook, Twitter, Youtube, Salesforce, Office365 e Netflix).

4.2.3. Alta Disponibilidade

4.2.3.1. A solução deve ser escalável para no mínimo 2 (dois) e no máximo 4 (quatro) membros em um único cluster no modo ativo/ativo ou ativo/stand-by, ou seja, possibilitar a divisão de cargas entre todos os appliances, permitindo o incremento gradual ao longo do tempo;

4.2.3.2. Será permitido a utilização de balanceados de carga externos;

4.2.3.3. A solução deve permitir o agrupamento de múltiplos equipamentos (cluster) que funcionem como um único equipamento, compartilhando única configuração de política de segurança entre os componentes;

4.2.3.4. O cluster deve suportar o uso conjunto de até 4(quatro) equipamentos simultâneos;

4.2.3.5. Deve permitir que equipamentos de modelos diferentes sejam incluídos ao cluster;

4.2.3.6. Deve garantir que todas as configurações sejam replicadas entre os componentes do cluster, garantindo a continuidade das conexões mesmo se um dos equipamentos do cluster estiver indisponível;

4.2.3.7. Deve possuir mecanismos de teste de link com o objetivo de fazer com que appliances do cluster fiquem offline se houver falha de link associado aquele appliance;

4.2.3.8. Deve possuir funcionalidade de ativação do cluster mesmo em versões de softwares diferentes por equipamento;

4.2.3.9. Deve permitir que equipamentos com versões de software diferentes sejam incluídos no cluster.

4.2.4. Funcionalidades de Controle e Inspeção de Aplicações

4.2.4.1. Deve suportar a liberação e o bloqueio de aplicações sem a necessidade de liberação de portas e protocolos;

4.2.4.2. Deve possuir pelo menos 4.000 (quatro mil) aplicações diferentes, para os seguintes perfis de tráfego mínimo: tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, VoIP, áudio, vídeo, proxy, serviços de mensagens instantâneas, compartilhamento de arquivos e e-mail;

4.2.4.3. Deve identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas avançadas de evasão como por exemplo divisão do malware em partes, enviá-los fora de ordem, via diferentes canais de comunicação;

4.2.4.4. Deve analisar tráfego criptografado SSL, possibilitando a leitura de payload para checagem de assinaturas das aplicações de forma granular;

4.2.4.5. Deve reconhecer e bloquear tráfego de rede do tipo ToR;

4.2.4.6. Deve notificar o usuário quando uma aplicação for bloqueada;

4.2.4.7. Deve possibilitar que o controle de portas seja aplicado para todas as aplicações;

4.2.4.8. Deve identificar a diferença de tráfegos de Instant Messaging possuindo granularidade de controle e políticas;

4.2.4.9. Deve ser capaz de bloquear funcionalidades específicas de páginas Web ou aplicações, para no mínimo: Facebook, Facebook-chat, Facebook-Apps ou Facebook-Live, Facebook-Plugins, Google, Google-Play, GoToMeeting, Zoom, Apple-FaceTime, Apple-Game-Center, Apple-iCloud;

4.2.4.10. Deve possuir integração com Microsoft Active Directory (AD) para identificação de usuários e grupos, permitindo granularidade de controle e políticas baseadas em usuários e grupos de usuários;

4.2.4.11. Deve possuir a capacidade de criação de políticas baseadas na visibilidade e controle do usuário e de grupo de usuários que estão utilizando as aplicações, através da integração com serviços de diretório Microsoft Active Directory (AD).

4.2.5. Funcionalidades de IPS (Intrusion Prevention System)

4.2.5.1. Deve suportar o funcionamento no modo IPS no mesmo appliance;

4.2.5.2. Deve suportar implementação em camada 2 e em camada 3;

4.2.5.3. Deve inspecionar o payload de pacote de dados com o objetivo de detectar aplicações conhecidas pelo fabricante independente de porta e protocolo;

4.2.5.4. As funcionalidades de IPS e Firewall devem ser implementadas em um mesmo appliance com sua comunicação entre as funcionalidades de maneira interna, sem a necessidade de uso de qualquer interface externa;

4.2.5.5. Deve possuir o bloqueio de vulnerabilidades;

4.2.5.6. Filtrar vulnerabilidades por pelo menos uma das referências a seguir: OSVDB, MS, BID e CVE;

4.2.5.7. Deve possuir o bloqueio de exploits conhecidos;

4.2.5.8. Deve possuir proteção contra-ataques de negação de serviços;

4.2.5.9. Deve incluir mecanismos para detecção de botnets tais como:

4.2.5.9.1. Ghost

4.2.5.9.2. njRAT

4.2.5.9.3. Poisonlvy

4.2.5.9.4. Pramro

4.2.5.9.5. Pushdo

4.2.5.9.6. Ramnit

4.2.5.10. Deve reconhecer pelo menos os seguintes protocolos: Ethernet, H.323, GRE, IPv4, IPv6, ICMP, UDP, TCP, DNS, FTP, HTTP, HTTPS,IMAP, IMAPS, MGCP, MSRPC, NetBIOS Datagram, OPC UA, Oracle, MySQL, POP3, POP3S, SIP, SRP, SSH, TELNET, WINS, X11, RTSP, SMTP, NNTP, SCCP, SMB, SMB2 e TFTP;

4.2.5.11. Deve permitir a aplicação de Virtual Patching para vulnerabilidades tanto de clients como de servidores;

4.2.5.12. Deve bloquear técnicas avançadas de scan tais como: stealth scan e slow scan;

4.2.5.13. Deve suportar nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução através da utilização de expressões regulares;

4.2.5.14. Deve bloquear a origem de análises do tipo Portscan;

4.2.5.15. Deve possuir assinaturas e bloqueios contra-ataques do tipo buffer overflow;

4.2.5.16. Deve possuir pelo menos as seguintes ações de bloqueio.:

4.2.5.16.1. Bloqueio direto;

4.2.5.16.2. Reset de conexões;

4.2.5.16.3. Inclusão em Blacklist;

4.2.5.16.4. Página HTML;

4.2.5.16.5. HTTP redirect;

4.2.5.17. Deve suportar a captura e exportação de pacotes;

4.2.5.18. Deve possuir configurações de diferentes políticas de controle de ameaças baseadas no tipo de arquivos;

4.2.5.19. O mecanismo de inspeção deve receber e implementar em tempo real atualizações para os ataques emergentes sem a necessidade de reiniciar o appliance;

4.2.5.20. Deve permitir exceções baseadas na fonte, destino, serviço, dias da semana, dias do mês, horário do dia, ligar ou desligar logs ou combinação entre eles;

4.2.5.21. A solução deve possuir integração com soluções de DLP via protocolo ICAP;

4.2.5.22. Deve permitir a criação de exceções das políticas de IPS a partir do Log da solução, minimizando o impacto de falso-positivos no ambiente.

4.2.6. Funcionalidades de VPN

4.2.6.1. Deve proteger o tráfego corporativo em termos de confidencialidade através de encriptação e integridade entre os pontos finais, para estabelecer um canal virtual, através de um túnel seguro sobre uma rede tipicamente pública como a internet usando IPsec e SSL VPN;

4.2.6.2. Deve suportar os protocolos: IKEv1, IKEv2, and IPsec with IPv4 e IPv6;

4.2.6.3. Deve possuir os seguintes algoritmos de encriptação: AES-128, AES-256, AES-GCM-128, AES-GCM-256, Blowfish ou DES, 3DES;

4.2.6.4. Deve possuir os seguintes métodos de autenticação: RSA, DSS ou ECDSA signatures com certificados X.509, pre-shared key (PSK), XAUTH, EAP;

4.2.6.5. Deve possuir VPN site-to-site em topologias “Full Mesh” (cada gateway tem um link específico para os demais gateways), “Star” (gateways satélites se comunicam somente com o gateway central), “Hub and Spoke” (onde o gateway definido como Hub tem por responsabilidade redirecionar o tráfego para o seu gateway destino (spoke));

4.2.6.6. Deve suportar Main Mode e Aggressive mode em IKE Phase I;

4.2.6.7. Deve suportar CRL – Certificate Revogation Lists;

4.2.6.8. Deve suportar NAT-Transversal;

4.2.6.9. Deve suportar a criação de VPNs com base em rotas e com base em políticas;

4.2.6.10. Dever permitir a criação de políticas de controle de aplicações, IPS, anti malware e QoS para tráfego dos clientes remotos conectados na VPN, seja ela Site-to-Site ou Client-to-Site;

4.2.6.11. Deve possuir funcionalidade de acesso remoto incluindo túneis SSL VPN e portal SSL VPN (mapeando URLs internas a URLs externas disponíveis a usuários que acessam o portal);

4.2.6.12.Deve possuir funcionalidades de SSL VPN permitindo:

4.2.6.12.1. Que o usuário realize a conexão por meio de cliente instalado no sistema operacional do equipamento e por meio de interface Web;

4.2.6.12.2. Atribuição de endereço de DNS aos clientes remotos;

4.2.6.13. Deve possuir funcionalidade de acesso remoto via cliente IPSec com as seguintes características:

4.2.6.13.1. O cliente VPN deve ser compatível com pelos menos os seguintes sistemas operacionais: Android, MacOS, Windows 7 SP1, Windows 8.1 e Windows 10;

4.2.6.13.2. Deve possuir capacidade de autenticação via usuário e password (com integração a servidores externos como RADIUS e TACACS) e uso de certificados;

4.2.6.13.3. Deve permitir a configuração de MTU na VPN;

4.2.6.13.4. Deve coletar informações de diagnóstico e permitir sua exportação;

4.2.6.13.5. Deve possuir ferramenta de captura de tráfego ou diagnóstico integrada ao cliente VPN;

4.2.6.13.6. Deve possuir funcionalidade de estabelecimento e manutenção automática de conexão VPN a gateway pré-estabelecido.

4.2.7. Gerência de Tráfego WAN

4.2.7.1. Deve ser fornecida uma solução de gerência de tráfego WAN integrada;

4.2.7.2. A solução de gerência de tráfego WAN poderá ser parte integrante da solução de firewall sem fazer com que os requisitos do firewall sejam prejudicados;

4.2.7.3. O balanceamento deve ser capaz de selecionar o caminho para o destino usando pelo menos os seguintes fatores:

4.2.7.3.1. Banda Disponível

4.2.7.3.2. Jitter

4.2.7.3.3. Latência

4.2.7.3.4. Perda de Pacotes

4.2.7.4. Deve possibilitar a criação de roteamentos distintos por aplicação, nas seguintes opções:

4.2.7.4.1. Preferível: Utilizar um tipo link a não ser que outro com melhor performance esteja disponível;

4.2.7.4.2. Custo: utilizar o link de menor custo;

4.2.7.4.3. Manual: selecionar o link de forma estática;

4.2.7.5. Deve fornecer mecanismo de balanceamento de carga através de diferentes conexões VPNs;

4.2.7.6. No caso de falha de um enlace, todas as conexões existentes devem ser automaticamente transferidas (statefully) para o outro enlace que estiver ativo, sem a necessidade de intervenção do administrador;

4.2.7.7. Deve permitir acrescentar novos enlaces de comunicação ao firewall sem que haja a necessidade de alterar enlaces existentes;

4.2.7.8. Deve fornecer o recurso de balanceamento de carga e agregação da capacidade de banda de enlace;

4.2.7.9. Deve possuir funcionalidades de agregação de VPN site-to-site, baseando-se em políticas de VPN (quando a política define ser o tráfego deve ser enviado via VPN) ou com base em rotas, suportando topologias em hub e spoke, full-mesh ou malha parcial;

4.2.7.10. Deve ter a capacidade de realizar a seleção de links/agregação de links de forma dinâmica e automática;

4.2.7.11. A agregação de link deve possibilitar pelo menos dois modos:

4.2.7.11.1. Balanceamento de carga (load sharing): tráfego balanceado entre diferentes enlaces com base em medida de desempenho (tempo ao destino) ou banda relativa entre enlaces;

4.2.7.11.2. Deve ser possível controlar/priorizar em função do QoS (DSCP) associado a aplicação de rede sendo trafegada;

4.2.7.12. Deve permitir realizar a seleção do link e estado de link (ativo/standby) em função de aplicação sendo usada na rede;

4.2.7.13. Deve ser possível decidir por qual link outbound o tráfego será encaminhado em função da aplicação transportada (aplicação esta identificada através de análise de conteúdo de pacote e não simplesmente através de análise de portas UDP/TCP).

4.2.8. Funcionalidades de Filtro WEB

4.2.8.1. Deve especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);

4.2.8.2. Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs e redes;

4.2.8.3. Deve possuir a capacidade de criar políticas baseadas na visibilidade e controle de quem está utilizando os serviços de diretório, autenticação via LDAP, Active Directory;

4.2.8.4. Deve permitir popular todos os logs de URL com as informações dos usuários conforme descrito na integração com serviços de diretório;

4.2.8.5. Deve suportar a capacidade de criar políticas baseadas no controle por URL e Categoria de URL;

4.2.8.6. Deve possuir, no mínimo, 60 categorias de URLs;

4.2.8.7. Deve suportar a customização de páginas de bloqueio;

4.2.8.8. Deve permitir o bloqueio e continuação (possibilitando que o usuário acesse um site potencialmente bloqueado informando o mesmo na tela de bloqueio e possibilitando a utilização de um botão "Continuar" para permitir o usuário continuar acessando o site).

4.2.9. Sistema de Gerência Centralizada

4.2.9.1. A interface de gerência centralizada deve suportar a edição de política da mesma política segurança por mais de um usuário administrador de forma simultânea;

4.2.9.2. A interface de gerência centralizada deve suportar a edição de políticas de segurança por mais de um usuário administrador de forma simultânea;

4.2.9.3. Deve permitir o gerenciamento centralizado (interface única de gerência) dos equipamentos a suas configurações de rede, de segurança, gerência de logs, geração de relatórios e sistema de gerência de tráfego WAN;

4.2.9.4. A gerência deve permitir a busca por ativos;

4.2.9.5. Deve possuir a comparação entre a política atual e a última política;

4.2.9.6. Deve possuir o agrupamento por tipo e por geo-localização;

4.2.9.7. Deve permitir a visualização da utilização dos links por equipamento;

4.2.9.8. Deve permitir a visualização das aplicações mais utilizadas em cada link;

4.2.9.9. Possuir a visualização das VPN’s, permitindo sua configuração através de ferramenta gráfica, com técnica facilitadora de arrasta e solta para alteração da política;

4.2.9.10. Deve possuir ferramenta integrada de validação de políticas, permitindo ao administrador verificar a parte da configuração que gerou questões associadas ao processo de validação;

4.2.9.11. Deve realizar o gerenciamento centralizado das licenças dos equipamentos monitorados;

4.2.9.12. O gerenciamento deve suportar comunicação via cliente ou web (GUI), utilizando protocolo seguro (criptografado), encriptação entre equipamento e sistema de gerenciamento;

4.2.9.13. Para administração da solução de gerenciamento, deve possuir cliente com compatibilidade e homologação para os sistemas operacionais Windows e Linux ou disponibilizar interface web usando HTTPS;

4.2.9.14. Deve possuir perfis de acesso a console customizáveis, com permissões granulares, no mínimo com os seguintes perfis: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações, alteração em políticas de acesso;

4.2.9.15. Deve permitir a localização de regras em que determinado endereço IP, range de IP, sub-rede ou objeto estejam sendo utilizados;

4.2.9.16. Deve permitir a visualização do número de vezes que uma determinada regra foi usada (hits) em diferentes intervalos de tempo como dia, semana, mês e intervalo customizável como data e horário de início e de fim da contagem;

4.2.9.17. Deve permitir a exportação de logs de auditoria detalhados, no mínimo, informando alterações da configuração realizada com horário das alterações;

4.2.9.18. Deve possibilitar a coleta de estatísticas do tráfego realizado pelos dispositivos de segurança;

4.2.9.19. Deve permitir a geração de relatórios, em tempo real, para a visualização de origens e destinos do tráfego gerado na Instituição;

4.2.9.20. Deve possuir dashboard específico para gerência de tráfego WAN indicando a qualidade de links em função de perda de pacotes, atraso fim a fim e jitter (variação do atraso fim a fim);

4.2.9.21. Deve possuir a capacidade de gerar relatórios gráficos que permitam visualizar as mudanças na utilização de aplicações na rede ao longo do tempo, para permitir comparação entre os diferentes consumos realizados pelas aplicações;

4.2.9.22. Deve prover visualização sumarizada e permitir gerar relatórios de todas as ameaças (IPS, antivírus, anti-malware) e aplicações trafegadas pelos firewalls gerenciados;

4.2.9.23. Deve possuir a criação de dashboards customizados, possibilitando a visibilidade do tráfego de aplicações, usuários, ameaças identificadas pelo IPS, antivírus, malwares "Zero Day" detectados em sandbox (quando aplicável) e tráfego bloqueado;

4.2.9.24. Deve possuir mecanismo "Drill-Down" para visualização, em tempo real, das informações sumárias produzidas pela ferramenta de gerência;

4.2.9.25. Deve permitir que os relatórios sejam enviados via e-mail;

4.2.9.26. Deve permitir que os relatórios possam ser exportados em PDF, HTML e texto;

4.2.9.27. Deve possuir a capacidade de gerar alertas provenientes de eventos como:

4.2.9.27.1. Eventos do gerenciador centralizado;

4.2.9.27.2. Falhas detectadas em auto teste do firewall;

4.2.9.27.2. O uso de uma determinada regra de uma política;

4.2.9.28. Deve permitir que os logs sejam rotacionados de forma que os registros mais antigos sejam apagados quando não houver espaço de armazenamento disponível;

4.2.9.29. Deve possuir RESTful API para integração com soluções de terceiros;

4.2.9.30. Deve permitir a exibição de forma histórica e em tempo real (possibilitando a filtragem por firewall gerenciado), com atualização automática e contínua, das seguintes informações:

4.2.9.30.1. Situação do dispositivo e do cluster (geral);

4.2.9.30.2. Principais aplicações;

4.2.9.30.3. Principais aplicações por classificação (chat, redes sociais, compartilhamento de arquivos, ...);

4.2.9.30.4. Principais aplicações por volume transferido;

4.2.9.30.5. Volume de tráfego transferido nos túneis VPN;

4.2.9.31. Deve permitir a atualização dos firewalls de forma remota;

4.2.9.32. Em modo cluster o firewall deve ser atualizado sem interrupções, não havendo interferência no encaminhamento e tratamento das conexões;

4.2.9.33. Suportar a gestão de 10 dispositivos gerenciados, contextos virtuais em console única;

4.2.9.34. Caso a solução ofertada necessite de instalação de console ou algo relacionado, deve permitir a instalação do gerenciador centralizado em sistema operacional Linux;

4.2.9.35. Permitir o gerenciamento de todas os equipamentos contratados em uma console única de gerenciamento;

4.2.9.36. Permitir o recebimento de 10 GB de logs por dia, no mínimo;

4.2.9.37. Possuir armazenamento total de 10 TB, no mínimo;

4.2.10. Características de Roteamento

4.2.10.1. Suporte a 4096 (quatro mil e noventa e seis) VLANs, conforme padrão IEEE 802.1q;

4.2.10.2. Agregação de links, conforme padrão IEEE 802.3ad;

4.2.10.3. Deve suportar proxy ARP e entradas estáticas de ARP definidos em endereço ipv4;

4.2.10.4. Policy Routing permitindo que o roteamento seja baseado tanto no endereço de origem quanto no endereço de destino;

4.2.10.5. Deve suportar roteamento multicast estático, encaminhamento multicast baseado em IGMP e Roteamento Multicast utilizando PIM (Protocol-independent Multicast)

4.2.10.6. Deve suportar pelo menos 3 modalidades do PIM : PIM-SM (PIM- sparse Mode), PIM-Dense Mode e PIM-SSM (PIM source specific multicast)

4.2.10.7. Deve suportar DHCP Serve IPv4 e IPv6;

4.2.10.8. Deve suportar DHCP Relay;

4.2.10.9. Possuir proteção contra anti-spoofing;

4.2.10.10. Deve possuir roteamento estático IPv4 e, no mínimo, os seguintes protocolos de roteamento dinâmico: BGP e OSPFv2;

4.2.10.11. Deve possuir ECMP (Equal-Cost Multi-Path) suportando até 8 caminhos entre origem e destino;

4.2.10.12. Deve possuir roteamento estático IPv6 e Multicast, no mínimo, o protocolo de roteamento dinâmico OSPFv3;

4.2.10.13. Deve suportar pelo menos os seguintes serviços em ipv4 e ipv6: Dual stack IPv4/IPv6 e as seguintes aplicações:

4.2.10.13.1. NDP;

4.2.10.13.2. ICMPv6;

4.2.10.13.3. DNSv6;

4.2.10.13.4. NTP;

4.2.10.13.5. Syslog.

4.2.11. Características Gerais

4.2.11.1. Todas as funcionalidades descritas deverão estar habilitadas e prontas para uso imediato na entrega, incluindo licenças, conectores GBIC para todas as interfaces de redes e cabos de interconexão permitindo a completa integração da solução com o ambiente existente na SSP-GO;

4.2.11.2. A CONTRATADA deverá fornecer todos os itens de hardware e software para o completo funcionamento da solução no ambiente de TI da SSP-GO, sem nenhum ônus para a CONTRATANTE.

4.2.11.3. A CONTRATADA deverá fornecer ferramenta para automação de migração de regras compatível com o Firewall atualmente instalado na SSP-GO (Forcepoint 1065), ou serviço completo de migração, sem nenhum ônus para a CONTRATANTE.

4.3. OBRIGAÇÕES DA CONTRATADA

4.3.1. A CONTRATADA deverá realizar a implantação das soluções, com configuração, instalação, e testes.

4.3.2. Deverão ser apresentados os seguintes entregáveis durante a implantação:

4.3.2.1. Fase de Desenho da arquitetura:

4.3.2.1.1. Esquema detalhado de Conexão com dispositivos

4.3.2.2. Fase de Instalação:

4.3.2.2.1. Envio de resumo semanal com atividades realizadas, avanços e problemas detectados

4.3.2.3. Fase de pós instalação:

4.3.2.3.1. A CONTRATADA confeccionará relatório(s) final(is) sobre as atividades realizadas e recomendações à CONTRATANTE. Este relatório poderá ser entregue em até 25 dias úteis após a realização dos trabalhos. No relatório entregue constarão as seguintes seções:

4.3.2.3.1.1. Introdução;

4.3.2.3.1.2. Análise do ambiente;

4.3.2.3.1.3. Atividades realizadas;

4.3.2.3.1.4. Configuração de políticas aplicadas;

4.3.2.3.1.5. Resultados obtidos (Coberturas, eventos de segurança registrados);

4.3.2.3.1.6. Conclusões;

4.3.2.3.1.7. Recomendações Específicas;

4.3.2.3.1.8. Recomendações de Segurança Corporativa.

4.3.2.4. Todas as atividades envolvidas serão acompanhadas e coordenadas por técnicos da SSP-GO;

4.3.2.5. Deve abranger a instalação física e lógica da solução, em sua totalidade, com duração máxima de 60 (sessenta) dias corridos, compreendendo, mas não se limitando a essas, as seguintes atividades:

4.3.2.5.1. Instalação física dos equipamentos nas dependências do SSP-GO;

4.3.2.5.2. Identificação de conformidade com os pré-requisitos da ferramenta, de acordo com as melhores práticas ditadas pelo fabricante, no sentido de melhorar o gerenciamento e performance e aplicar os “patchs” para atualização do sistema, quando necessário;

4.3.2.5.3. Definição das funcionalidades a serem implantadas;

4.3.2.5.4. Definição da parametrização;

4.3.2.5.5. Instalação e configuração de toda a solução;

4.3.2.5.6. A instalação deve contemplar a verificação da infraestrutura elétrica e lógica existente. Eventuais problemas e necessidade de ajustes devem ser comunicados à SSP-GO o qual será responsável pela solução dos mesmos;

4.3.2.5.7. A instalação dos equipamentos e componentes da solução deverá levar em consideração o ambiente e instalações existentes (espaço físico, sistema de refrigeração e de fornecimento de energia elétrica, dutos, eletrocalhas, entre outros elementos). Os componentes fornecidos (equipamentos e acessórios) devem proporcionar condições ideais de funcionamento tanto no que diz respeito à disposição física, nas salas e nos “rack’s” evitando problemas de refrigeração e de acesso físico;

4.3.2.5.8. Após a instalação dos equipamentos, alimentação elétrica e conexões com a rede de dados e/ou voz, não poderá haver cabos sem proteção, soltos, por cima do piso elevado ou que obstruam a frente ou visibilidade dos equipamentos instalados;

4.3.2.5.9. Os serviços de instalação e configuração deverão ser prestados nas dependências da contratante;

4.3.2.5.10. Os serviços devem ser executados por técnicos autorizados e certificados na solução ofertada.

4.4. TREINAMENTO

4.4.1. Os serviços de treinamento deverão ser entregues em até 30 dias após a entrega dos sistemas ou a critério da CONTRATANTE.

4.4.2. Serviço de treinamento da equipe técnica do CONTRATANTE visando capacitá-la na operação/administração/uso da solução, contemplando, no mínimo, os seguintes tópicos:

4.4.2.1. Apresentação do projeto/solução implementado;

4.4.2.2. Descrição da arquitetura física e lógica de cada elemento da solução;

4.4.2.3. Estratégias de implementação da solução;

4.4.2.4. Procedimentos de instalação da solução;

4.4.2.5. Operação e Administração da solução;

4.4.2.6. Descrição e uso das funcionalidades da solução;

4.4.2.7. Resolução de problemas (“troubleshooting”);

4.4.2.8. Procedimentos de manutenção (atualizações de software, backup/restore, instalação de módulos de hardware, etc.);

4.4.2.9. Elaboração de Relatórios;

4.4.3. A CONTRATADA deverá providenciar material didático individual que abranja todo o conteúdo do curso. Não será exigido material oficial do fabricante, entretanto este será avaliado pela equipe técnica do CONTRATANTE antes da realização do curso, e caso seja considerado insuficiente, deverá ser readaptado para as condições exigidas pelo CONTRATANTE.

4.4.4. O período e horário de realização do curso deverão ser definidos pela CONTRATADA, em conjunto com o CONTRATANTE, para momento posterior à implantação da solução.

4.4.5. A CONTRATADA deverá providenciar local e infraestrutura para o treinamento, podendo o CONTRATANTE optar por executá-lo em seu ambiente.

4.4.6. O treinamento deve ter carga horária de no mínimo 16(dezesseis) horas.

4.4.7. A turma deverá ter no mínimo 5(cinco) alunos.

4.5. MODELO DE PLANILHA DE ATENDIMENTO A REQUISITOS

3.4.7.1. O atendimento a todos os itens deve ser comprovado através de documentação oficial do fabricante da solução, que deverá ser anexada à proposta comercial ajustada. A instituição poderá realizar diligência junto ao fabricante para comprovar a autenticidade da documentação. A localização da comprovação na(s) página(s) deverá ser clara e precisa conforme modelo abaixo. O não atendimento destes requisitos implicará na desclassificação da proposta.

Item	Documento	Página	Localização

5. QUALIFICAÇÃO TÉCNICA E SERVIÇOS ESPECIALIZADOS

5.1. Qualificação Técnica:

5.1.1. A empresa deverá apresentar Atestado de Capacidade Técnica fornecido por pessoa jurídica de direito público ou privado, declarando ter fornecido bens compatíveis com o objeto deste Termo de Referência;

5.1.2. Todos os atestados ou declarações exigidas deverão ser apresentados em original ou cópia autenticada por cartório competente, assinadas por pessoa responsável com indicação de nome e cargo exercido na empresa;

5.1.3. No caso de comprovação por mais de um atestado, os atestados somados ou não, deverão cobrir o quantitativo mínimo de 20% (vinte por cento) do objeto do Termo de Referência ou similar;

5.1.4. Para os itens nos quais o percentual requerido apresente fração, considerar-se-á o número inteiro imediatamente superior;

5.1.5. Não será aceito pela SSP-GO atestado ou declaração emitido pela própria licitante, sob pena de infringência ao princípio da moralidade, pois a licitante não possui a impessoalidade necessária para atestar sua própria capacitação técnica.

5.2. Instalação:

5.2.1. Entende-se como fase em que se dará a instalação e configuração dos produtos, ou seja, efetiva implementação do projeto especificado;

5.2.2. A instalação e testes dos produtos devem estar inclusos no custo do produto;

5.2.3. A implementação deverá ser realizada de tal forma que as interrupções no ambiente de produção sejam as mínimas possíveis e estritamente necessárias, e, ainda, não causem transtornos aos usuários finais do órgão;

5.2.4. A CONTRATADA deverá executar testes funcionais básicos para verificar o perfeito funcionamento do ambiente. Estes testes deverão ser realizados nos componentes de hardware e software envolvidos no projeto;

5.2.5. Durante a execução dos serviços, pelo menos um representante da SSP-GO participará e fará composição na equipe designada para as atividades.

5.3. Garantia e Suporte Técnico:

5.3.1. O prazo de garantia das licenças da solução ofertada deverá ser de, no mínimo, 30(trinta) meses, contados a partir da data do aceite definitivo;

5.3.2. A CONTRATADA deverá fornecer Central de Serviços para abertura de chamados técnicos em horário comercial, de 08:00 às 18:00 de segunda a sexta-feira com SLA para início de atendimento em até 12 horas após abertura do chamado;

5.3.2.3. A Central de Serviços deverá ser acionada por meio de ligação telefônica, por e-mail ou por sistema de Service Desk disponível pela Internet, para abertura dos chamados;

5.3.2.4. Os chamados deverão ser atendidos via acesso remoto utilizando-se de softwares ou atendimento via telefone. Caso seja necessário e definido pela CONTRATANTE, o atendimento deverá ser fornecido presencialmente na modalidade on-site;

5.3.2.5. Para a prestação dos serviços de suporte remoto, deverão ser utilizados os protocolos HTTP e HTTPS da Internet, SSH ou VPN;

5.3.2.6. A CONTRATADA, sendo fabricante ou não da solução ofertada, deverá disponibilizar um telefone de suporte técnico no Brasil e em Língua Portuguesa para que a SSP-GO obtenha suporte telefônico diretamente do fabricante se necessário, tantas e quantas vezes desejar durante a vigência das licenças.

5.4. Treinamento e Capacitação:

5.4.1. A capacitação deverá ser fornecida a no mínimo 04 (quatro) colaboradores da área de TI da SSP-GO;

5.4.2. A capacitação deverá consistir em treinamento oficial em acordo com as políticas do fabricante da solução fornecida;

5.4.3. Deverá ser ministrado por instrutor certificado na solução e deverá fornecer, para todos os participantes, material didático oficial impresso ou eletrônico e em português;

5.4.4. O treinamento deverá ser realizado presencialmente, em infraestrutura disponibilizada pela SSP-GO e deverá possuir carga horária mínima de 8 (oito) horas;

5.4.5. Após a realização da capacitação, a empresa deverá fornecer certificado de conclusão para cada participante;

5.4.6. O treinamento deverá ser realizado no prazo máximo até 30 (trinta) dias corridos, após a assinatura do contrato.

6. VIGÊNCIA, PRAZO E LOCAL DE ENTREGA/EXECUÇÃO DO OBJETO

6.1. O Contrato terá duração de 30(trinta) meses, podendo ser prorrogado conforme a Lei 8.666/93.

6.2. O início da execução contratual deverá ocorrer em até 60 (sessenta) dias contados da publicação da outorga do contrato no Diário Oficial do Estado de Goiás.

6.3. Os serviços e/ou equipamentos deverão ser entregues na Gerência de Telecomunicação da Secretaria da Segurança Pública do Estado de Goiás.

6.4. Endereço: Avenida Anhanguera nº 7.364 – Setor Aeroviário – CEP: 74.435-300 – Goiânia - Goiás.

6.5. A entrega e instalação dos equipamentos e/ou serviços deverá ser em horário comercial (8:00h às 18:00h), de segunda-feira a sexta-feira ou em datas e horários definidos em comum acordo entre as partes.

7. PAGAMENTO

7.1. O pagamento será realizado em até 30(trinta) dias, a contar da data de recebimento definitivo do produto e aprovado os termos das Notas Fiscais, e será efetivado por meio de crédito em conta corrente aberta exclusivamente na “Caixa Econômica Federal”, em atenção ao disposto no art. 4º da Lei nº 18.364, de 10 de janeiro de 2014.

7.2. O pagamento da(s) nota(s) fiscal(is) fica condicionado ao cumprimento dos critérios de recebimento previstos no edital.

8. RESPONSÁVEL PELA ELABORAÇÃO DO TERMO DE REFERÊNCIA

8.1. Este termo foi elaborado por Jánison Calixto dos Santos.

8.2. Dúvidas deverão ser tratadas pelo e-mail janison.calixto@ssp.go.gov.br

Documento assinado eletronicamente por **JANISON CALIXTO DOS SANTOS**, **Gerente**, em 21/10/2020, às 11:17, conforme art. 2º, § 2º, III, "b", da Lei 17.039/2010 e art. 3ºB, I, do Decreto nº 8.808/2016.

A autenticidade do documento pode ser conferida no site **http://sei.go.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=1** informando o código verificador **000016069193** e o código CRC **4F9AAEB0**.

GERÊNCIA DE TELECOMUNICAÇÕES
AVENIDA ANHANGUERA 7364 - Bairro AEROVIÁRIO - CEP 74.543-010 - GOIÂNIA - GO

Referência: Processo nº 201900016022158 SEI 000016069193