

Caderno de Encargos

“Aquisição de Equipamento Segurança Informático designado por “IPT-Concurso Segurança”



GOVERNO DE
PORTUGAL

MINISTRO DA CIÊNCIA,
TECNOLOGIA E ENSINO SUPERIOR

ARTIGO 1.º

OBJECTO

1. O presente Caderno de Encargos compreende as cláusulas a incluir no contrato a celebrar entre a Fundação para a Ciência e a Tecnologia, I.P. e adjudicatário na sequência da adjudicação no âmbito da consulta para aquisição de Equipamento Segurança Informático designado por “IPT-Concurso Segurança”.

2. O **CONTRATO** a celebrar integra, para além do clausulado contratual:

- a) os suprimientos dos erros ou omissões do caderno de encargos identificados pelos concorrentes, desde que esses erros e omissões tenham sido expressamente aceites pelo órgão competente para a decisão de contratar, nos termos do artigo 50º do Código dos Contratos Públicos;
- b) os esclarecimentos e retificações relativos ao caderno de encargos que sejam emitidos ao abrigo do artigo 50º do Código dos Contratos Públicos;
- c) o caderno de encargos;
- d) a proposta adjudicada;
- e) os esclarecimentos sobre a proposta adjudicada prestados pelo adjudicatário.

3. Em caso de divergência entre os documentos referidos nas diferentes alíneas do número anterior, a prevalência obedece à ordem por que vêm enunciados nas suas diferentes alíneas.

4. Em caso de divergência entre os documentos referidos nas diferentes alíneas do nº 2 e o clausulado contratual, prevalecem os primeiros, salvo quanto aos ajustamentos propostos de acordo com o disposto no artigo 99º do Código dos Contratos Públicos e aceites pelo adjudicatário nos termos do disposto no artigo 101º do mesmo diploma.

ARTIGO 2.º

OBRIGAÇÕES DO ADJUDICATÁRIO

- 1. O adjudicatário obriga-se a executar o Contrato em termos que se conformem com o estabelecido no Caderno de Encargos, nos anexos que dele fazem parte integrante e na legislação aplicável.

2. Para além de outras obrigações previstas na lei ou no presente caderno de encargos, o adjudicatário obriga-se a:

- a) Assegurar que o objeto da prestação obedece às especificações e condições técnicas exigidas;
- b) Assegurar a manutenção;
- c) Cumprir os prazos estabelecidos, designadamente, para a execução das prestações a que se obriga;
- d) Prestar informação;
- e) Assegurar o sigilo.

ARTIGO 3.º

ESPECIFICAÇÕES TÉCNICAS

O adjudicatário obriga-se a assegurar que o objeto de aquisição obedece às especificações técnicas que constam do Anexo I ao presente Caderno de Encargos, do qual faz parte integrante.

ARTIGO 4.º

PRAZOS

O adjudicatário obriga-se ao pontual cumprimento de todos os prazos de execução das prestações objeto do contrato, os quais são os que constam do clausulado deste ou de outros documentos referidos no nº 2 do artigo 1º.

ARTIGO 5.º

ENTREGA

1. Os bens objeto de adjudicação consideram-se entregues após a respetiva aceitação por parte da FCT, I.P, a qual será comunicada por escrito ao adjudicatário.
2. O adjudicante poderá promover a realização de testes de aceitação, destinados à verificação da conformidade dos bens objeto de adjudicação com os requisitos técnicos constantes do presente Caderno de Encargos.
3. Os testes referidos no número anterior devem ocorrer no prazo de 60 dias corridos após a receção de todos os bens objeto do contrato a qual deve ocorrer nas instalações do

Instituto Politécnico de Tomar, sitas na Avenida Dr. Aurélio Ribeiro, em Tomar no prazo máximo de 30 dias corridos contados a partir da entrada em vigor do contrato.

4. Os bens consideram-se aceites na data em que a FCT, I.P. disso expressamente notificar, por escrito, o adjudicatário ou, na ausência de notificação, no dia subsequente ao fixado no número anterior como limite para a realização de testes de aceitação.

5. Se nos termos dos testes de aceitação a FCT, I.P. constatar que os bens não cumprem os requisitos técnicos constantes do presente Caderno de Encargos, disso dará conhecimento ao adjudicatário, abrindo-se um prazo de 7 (sete) dias corridos para que este desenvolva as diligências necessárias a que aqueles requisitos sejam cumpridos, e o equipamento seja de novo submetido a testes.

6. Se, estes testes de aceitação, não forem concluídos com êxito, persistindo a desadequação aos requisitos técnicos exigidos, a FCT, I.P. poderá dar ao adjudicatário novo prazo de 7 (sete) dias corridos para que este desenvolva novas diligências para que os bens ou serviços cumprem os requisitos do Caderno de Encargos, aplicando-se, com as devidas adaptações o disposto nos números anteriores ou, em alternativa, considerar incumprida a obrigação de fornecimento dos adaptadores óticos e rescindir o Contrato.

ARTIGO 6.º

OBRIGAÇÃO DE MANUTENÇÃO

Caso se verifique qualquer anomalia nos bens objeto de adjudicação que impeça ou prejudique o desempenho da sua função, o adjudicatário obriga-se a proceder, sem custos adicionais para o adjudicante, às operações necessárias à reposição deste nas mesmas condições que deram origem à aceitação nos termos e condições referidas no Anexo I ao presente Caderno de Encargos.

ARTIGO 7.º

OBRIGAÇÃO DE PRESTAÇÃO DE INFORMAÇÃO

O adjudicatário obriga-se a prestar à FCT, I.P., por escrito, toda a informação que lhe for solicitada relativa ao objeto da adjudicação ou à sua atuação em cumprimento das obrigações que para si decorrem do contrato.

ARTIGO 8.º

OBRIGAÇÃO DE SIGILO

O adjudicatário obriga-se a não divulgar informações que obtenha em virtude da execução do **CONTRATO** durante a vigência deste e por um período de dois anos contados a partir da data da sua cessação.

ARTIGO 9.º

PREÇO E CONDIÇÕES DE PAGAMENTO

1. O preço base da aquisição a que se refere o presente caderno de encargos, entendido como o preço máximo que a FCT, I.P. se dispõe a pagar pelo fornecimento dos bens que constituem o seu objeto é de 340.000 € (trezentos e quarenta mil euros), acrescido de IVA à taxa legal em vigor. sendo o preço base de cada um dos lotes objeto do concurso, entendido como o preço máximo que a FCT, I.P. se dispõe a pagar pelo fornecimento dos bens objeto de cada um desses lotes o seguinte:

Lote 1: 180.000 euros, acrescido de IVA à taxa legal em vigor

Lote 2: 160.000 euros, acrescido de IVA à taxa legal em vigor

2. Pela aquisição dos bens objeto da presente aquisição, a FCT, I.P. pagará ao adjudicatário a quantia indicada na proposta, acrescida de IVA à taxa legal em vigor nos termos do número seguinte.

3. A quantia prevista no número anterior deve ser satisfeita através do pagamento de uma fatura, emitida, após a entrega dos bens nos termos a que se refere o artigo 5º.

4. A fatura a emitir pelo adjudicatário assume a forma de fatura eletrónica, com os requisitos legais, nomeadamente os resultantes do artigo 299º-B do CCP.

5. A fatura referida no número anterior será paga no prazo máximo de trinta dias a contar da sua receção.

ARTIGO 10.º

CAUÇÃO

1. Como forma de garantir o exato e pontual cumprimento de todas as obrigações legais e contratuais, bem como a celebração do contrato, o adjudicatário deve, no caso de

o preço contratual ser igual ou superior a 200.000 €, prestar caução nos termos e condições constantes estabelecido no artigo 90º do Código dos Contratos Públicos.

2. O valor da caução a prestar é de 5% do valor contratual.
3. A caução é liberada nos termos previstos no artigo 295º do Código dos Contratos Públicos.

ARTIGO 11.º

VIGÊNCIA DO CONTRATO

1. O CONTRATO inicia a sua vigência na data da respetiva assinatura.
2. O CONTRATO cessa vigência no prazo de 5 anos¹ ou após a conclusão das tarefas para os serviços de instalação definidas no anexo técnico (Anexo I).
3. O artigo 8º cessa vigência na data em que cesse o prazo nele previsto.

ARTIGO 12.º

RESPONSABILIDADE DO ADJUDICATÁRIO

1. O adjudicatário responde pelos danos que causar à **FCT, I.P.** em razão do incumprimento culposo das obrigações que sobre ele impendam, nos termos das normas gerais de direito e do presente artigo.
2. O adjudicatário responde ainda perante a **FCT, I.P.** pelos danos causados pelos atos e omissões de terceiros, por si empregues na execução de obrigações emergentes do **CONTRATO**, como se tais atos ou omissões fossem praticados por aquele.
3. O adjudicatário responde, independentemente de culpa, pelos danos causados à **FCT, I.P.** pela execução deficiente do **CONTRATO**.

¹ A vigência do contrato de cinco anos é justificada pela criticidade do equipamento em causa que justifica uma continuidade e estabilidade na sua manutenção durante o período de vida útil do equipamento, que é de cinco anos.

4. Nenhuma das partes responde por danos causados à outra parte em virtude de incumprimento de obrigações emergentes do **CONTRATO** decorrente de caso fortuito ou força maior.

5. A parte que pretenda beneficiar-se do regime acolhido no número anterior deve, para o efeito, informar a outra parte da verificação de uma situação de incumprimento decorrente de caso fortuito ou de força maior, fazendo menção dos factos que, em seu entender, permitem atribuir esta origem ao incumprimento e, ainda, do prazo que estima necessário para cumprir a obrigação em causa.

ARTIGO 13.º

CLÁUSULA PENAL

1. Pelo incumprimento, sob a forma de mora, de obrigações emergentes do contrato, a **FCT, I.P.** pode, sem prejuízo do n.º 4 do artigo anterior, exigir do adjudicatário o pagamento de uma pena pecuniária calculada de acordo com a seguinte fórmula:

$$P = V \times A / 10$$

Sendo:

P - Montante da penalidade

V – Preço total contratualizado

A – Nº de dias de atraso no cumprimento de prazos estabelecidos para as prestações do adjudicatário

2. O valor acumulado em penalizações não pode exceder 20% do preço contratual, nos termos do nº2 do artigo 329º do CCP.

ARTIGO 14.º

RESCISÃO

1. A FCT, I.P. pode rescindir o **CONTRATO**:

a) quando, estando o adjudicatário em mora, este não realize a prestação no prazo que lhe haja razoavelmente sido fixado pela FCT, I.P.;

b) com fundamento em incumprimento das obrigações previstas no artigo 2º que determine a perda objetiva de interesse nas prestações que constituam o seu objeto;

2. A rescisão do **CONTRATO** ao abrigo do disposto no número anterior determina a perda da caução prestada pelo adjudicatário, caso esta tenha sido prestada nos termos da lei e a extinção dos créditos de que este seja titular em virtude do referido **CONTRATO**.

3. A perda da caução ao abrigo do número anterior não extingue o direito da **FCT, I.P.** de ser ressarcida da totalidade dos danos que lhe hajam sido causados pela conduta do adjudicatário que haja fundamentado a rescisão.

ARTIGO 15.º

DESPESAS

Correm por conta do adjudicatário todas as despesas em que este haja de incorrer em virtude do cumprimento de obrigações emergentes do **CONTRATO**.

ARTIGO 16.º

LEI APLICÁVEL

O **CONTRATO** rege-se pela lei portuguesa.

ARTIGO 17.º

INTERPRETAÇÃO DO CONTRATO

1. Em caso de dúvida sobre a interpretação das regras aplicáveis à execução do **CONTRATO**, o adjudicatário deve solicitar por escrito um esclarecimento à **FCT, I.P.**.

2. O adjudicatário obriga-se a ter em conta as orientações que lhe forem transmitidas por escrito pela **FCT, I.P.**, na medida em que as mesmas não colidam com as regras aplicáveis à execução do **CONTRATO**.

ARTIGO 18.º

COMUNICAÇÕES

1. Para efeitos de comunicações relativas à fase de execução do contrato, as partes podem recorrer aos seguintes meios de comunicação:

- a) correio postal, através de carta registada ou de carta registada com aviso de receção;
- b) correio eletrónico;
- c) outro meio de transmissão eletrónica de dados.

2. Todas as comunicações devem ser escritas e redigidas em língua portuguesa.

3. Para efeitos de estabelecimento das comunicações a que se refere o presente artigo, as partes identificam os seguintes contactos, através dos quais as mesmas se devem concretizar:

a) Pela FCT, I.P.:

Nome do representante:

Endereço postal: Av. do Brasil, 101 1700-066 Lisboa

Endereço eletrónico:

Número de fax:

b) Pelo adjudicatário:

Nome do representante:

Endereço postal:

Endereço eletrónico:

Número de fax:

ARTIGO 19.º

GESTOR DO CONTRATO

Para o exercício das funções de acompanhamento da execução do contrato nos termos regulados pelo artigo 290º-A do Código dos Contratos Públicos é designado Joaquim Pombo da Silva Dias.

ARTIGO 20.º

CESSÃO DA POSIÇÃO CONTRATUAL

1. A cessão da posição contratual do adjudicatário é possível nos termos do artigo 318º do Código dos Contratos Públicos.
2. Em caso de incumprimento contratual pelo adjudicatário que seja suscetível de conduzir à resolução do contrato, a sua posição contratual pode ser cedida aos concorrentes do procedimento pré-contratual classificados nas posições subsequentes à do adjudicatário, nos termos do estabelecido no artigo 318º-A do Código dos Contratos Públicos.

ARTIGO 21.º

DADOS PESSOAIS

1. No tratamento de dados pessoais por conta do adjudicante, o adjudicatário obriga-se ao escrupuloso cumprimento do Regulamento Geral sobre a Proteção de Dados (Regulamento 2016/679) e demais legislação aplicável.
2. O tratamento referido no número anterior é apenas o necessário à execução do contrato e feito durante a sua vigência, aplicando-se, em especial, o estabelecido no nº 3 do artigo 28º do Regulamento Geral sobre a Proteção de Dados.

ARTIGO 22.º

(ASSINATURA DO CONTRATO)

O contrato a celebrar entre a FCT, I.P. e o adjudicatário será celebrado com recurso preferencial, por ambas as partes, à assinatura eletrónica qualificada, tal como definida pelo Decreto-lei nº 290D/99, de 2 de agosto, com as alterações introduzidas pelos Decretos-lei n.º 62/2003, de 3 de abril, 165/2004, de 6 de julho e 116-A/2006, de 16 de junho.

ARTIGO 23.º

(TRIBUNAL DE CONTAS)

1. O contrato poderá estar sujeito a fiscalização prévia do Tribunal de contas, nos termos do disposto nº 2, do artigo 318.º da LOE 2020, conjugado com o nº 2 do artigo 48.º da Lei de Organização e Processo do Tribunal de Contas, na sua redação atual
2. Caso se verifique o previsto no número anterior, o contrato apenas produz efeitos financeiros a partir data de obtenção do referido Visto;
3. Os emolumentos devidos, no valor legal, serão suportados pelo adjudicatário.

ANEXO I

(ANEXO TÉCNICO)

IPT-Concurso Segurança

Este documento contém as especificações técnicas aplicáveis ao fornecimento de equipamentos e respetivos serviços de implementação nas instalações do Instituto Politécnico de Tomar (IPT), no âmbito do projeto RCTS100, de interligação das entidades de ensino superior em rede de alto débito.

RESUMO

O objetivo principal é dotar o Instituto Politécnico de Tomar (IPT) de uma componente de segurança ativa no edge e no datacenter que permita usufruir da ligação de 10G FCT-FCCN existente utilizando BFD, BGP e VRRP, bem como ao usar dois equipamento em ativo-passivo ou ativo-ativo, melhorar a resiliência a ataques de intrusão e consequentes latências, garantir a continuidade de serviço durante atualizações, tornar mais eficiente a gestão de políticas de segurança, implementar as políticas em degrau por forma a que nem todos os sistema rejeitem as mesmas ameaças.

Pretende-se aumentar capacidade de armazenamento, cruzamento e tratamento de informação de logs de tráfego e relacioná-lo entre os vários equipamentos Fortigate existentes usando uma solução de Gestão Centralizada de equipamentos e políticas em consola única (Fortianalyzer, Esight). Tal como com os restantes equipamentos no campus e datacenter utilizando outras ferramentas disponíveis, quer sejam proprietárias, quer sejam opensource.

CARACTERIZAÇÃO DO PROJETO

Segurança e logs

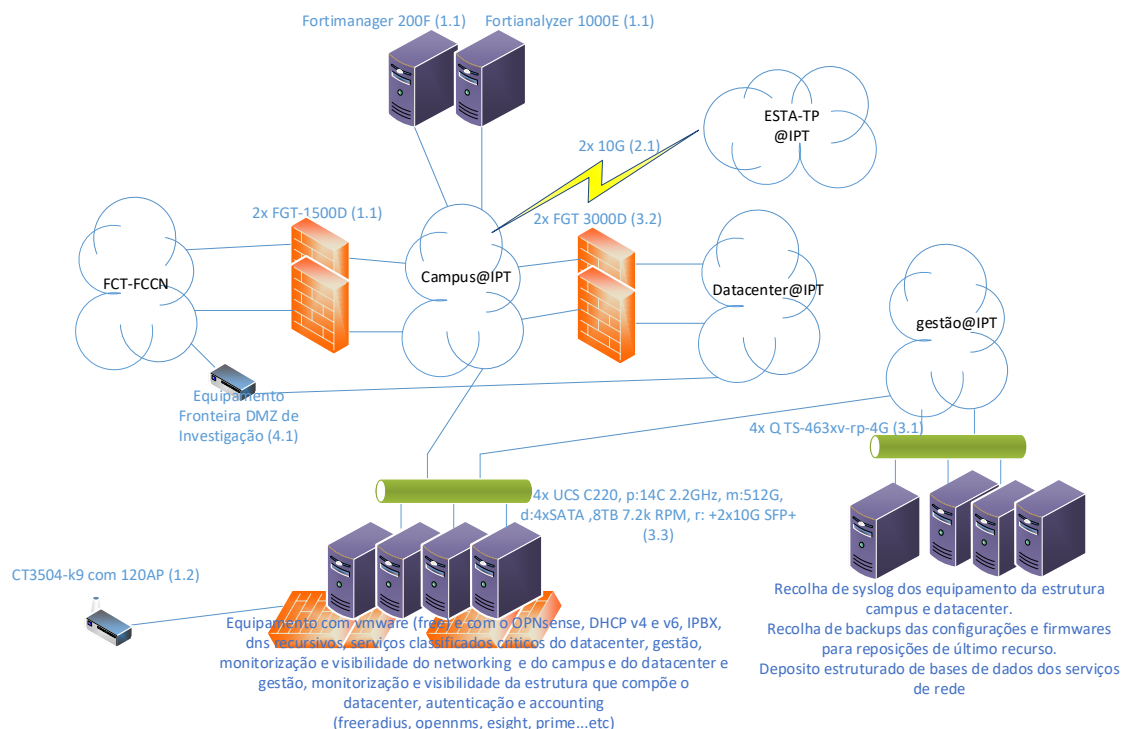


Fig.1 – Diagrama simplificado do projeto

NOTA: O diagrama não tem legenda, mas existe correspondência entre os pontos identificados no diagrama e os pontos do índice.

LOTE 1 - INTERLIGAÇÃO À FCT-FCCN

Pretende-se, usando uma solução de Gestão e visibilidade Centralizada para equipamentos e recursos em consola única, o cruzamento e tratamento de informação de logs e relacioná-la entre os vários equipamentos Fortigate existentes (FGT1KC3913801059), garantindo a existência compatibilidade na recolha e análise entre os equipamentos existentes e os equipamentos a adjudicar (Lote 1).

Equipamentos existentes em produção ou que foram retirados de produção por avaria:

Equipamento	Número de Serie	Fim de suporte	Em produção	A retirar
FortiGate 1000C	FGT1KC3913801059	2022-01-17	SIM	NÃO
FortiGate 1000A	FGT1KA2606500717	2015-02-25	SIM	SIM

FortiAnalyzer 800	FLG8002706000367	2012-10-16	NÃO	-----
-------------------	------------------	------------	-----	-------

O adjudicatário deve fornecer o seguinte equipamento:

<u>Equipamento</u>	<u>Resumo</u>	<u>Quantidade</u>
Firewall	All-in-one/ Unified Threat Management (Firewall, Threat Protection [IPS, Web-filtering, Anti-Malware, SSL inspection]) com Alta disponibilidade	2
Análise	Recolha de relatórios (obter indicadores de compromisso) e análise de logs de vários equipamentos de firewall em hardware	1
Gestor	Gestão operacional e visibilidade em hardware	1

<u>Cabos e Conversores</u>	<u>Resumo</u>	<u>Quantidade</u>
Chicotes UTP CAT7	CAT7, S/FTP, Freq. 600MHz, AWG26 e 10GBase-T velocidade com 3 metros	20
transceivers	10GE LR SFP+, 10km SMF (Huawei compatível)	2
transceivers	10GE SR SFP+MMF	4
DAC	40G QSFP+ para 4x10G de 2 mts	6
Chicotes Óticos	LC-LC OS2 2 mts	2
Chicotes Óticos	LC-LC OM3 2 mts	4

O Adjudicatário deve fornecer uma solução de interligação à FCT-FCCN composta por **2** equipamentos do tipo ***All-in-one/Unified Threat Management (Firewall, Threat Protection[IPS, Web-filtering, Anti-Malware, SSL inspection])*** em cluster e com fontes de alimentação redundantes. O OS nativo permite BFD, BGP e VRRP, bem como Firewall, Routing, Intrusion Prevention System e que a aceleração de tráfego seja por hardware dedicado no firewall/NGFWall.

Ao nível de **Firewall** deverão ser suportadas as seguintes funcionalidades:

- Modos de operação NAT/route e transparente/bridge
- Agendamento de políticas: recorrentes ou apenas uma vez

- Session helpers e ALGS: dcerpc, dns-tcp, dns-udp, ftp, H.323, MGCP, MMS, PMAP, PPTP, RAS, RSH, SIP, TFTP, TNS (Oracle)
- Suporte para tráfego VoIP: SIP/H.323 /SCCP NAT traversal, RTP pin holing
- Suporte para diferentes tipos de protocolos: SCTP, TCP, UDP, ICMP, IP
- Visualização de políticas de forma global ou por secção
- Definição de objetos para utilização em políticas incluindo: predefinidos, customizados, agrupamento de objetos, tagging e definição de cor de objetos
- Definição de objetos de endereços de diferentes tipos: IP, Subnet, intervalo de endereços IP, Geografia e FQDN
- Configuração de NAT: por política e tabela central de NAT
- Suporte de NAT: NAT64, NAT46, NAT estático, NAT dinâmico, PAT, Full Cone NAT

Traffic shaping e QOS: shaping de tráfego partilhado por política, shapping por IP, largura de banda máxima e garantida, número máximo de ligações por IP, priorização de tráfego, suporte de Type of Service (TOS) e Differentiated Services (DiffServ)

Ao nível de **IPS** deverão ser suportadas as seguintes funcionalidades:

- Suporte de IPS com mais de 7000 assinaturas, deteção de anomalias nos protocolos, assinaturas customizadas, update de assinaturas manual ou automático (push ou pull), integração com enciclopédia de ameaças para melhor informação/visualização de ataques detetados
- Diferentes ações de IPS: definido por defeito na assinatura, monitorizar, bloquear, reset de sessão ou quarentena (IP do atacante, IP de atacante e vítima, interface de entrada) com definição de duração
- Possibilidade de registo integral do pacote onde foi detetado o ataque
- Definição de diferentes perfis de IPS de forma manual ou baseada em filtro (severidade, alvo, sistema operativo, aplicação e/ou protocolo)
- Aplicação de perfis de IPS por política de firewall para maior flexibilidade
- Opção de excluir a aplicação de assinaturas de IPS específicas com base em IPs
- Proteção DOS sobre IPv4 e IPv6 com definições contra TCP Syn flood, TCP/UDP/SCTP port scan, ICMP sweep, TCP/UDP/ SCTP/ICMP session flooding (source/destination)
- Possibilidade de implementação de IDS em modo sniffer

Ao nível de **Threat Protection** deverão ser suportadas as seguintes funcionalidades:

- Possibilidade de inspeção aplicacional de tráfego encriptado por SSL, incluindo as seguintes funcionalidades: IPS, controlo de aplicações, anti-vírus, filtragem WEB e DLP
- Deteção e bloqueio de BOTNETs com base em listas de reputação de IPs globais;
- Suporte de anti-vírus nos modos flow (pacote-a-pacote) e proxy (reconstrução de sessões)
- Suporte de inspeção de anti-vírus, em modo flow, nos seguintes protocolos: HTTP/HTTPS, SMTP/SMTPS, POP3/POP3S, IMAP/IMAPS, MAPI, FTP/SFTP, SMB, NNTP
- Integração com solução de Sandboxing (cloud ou premises)
- Suporte de anti-vírus em modo proxy, incluindo:

- o Suporte dos seguintes protocolos: HTTP/HTTPS, STMP/SMTPS, POP3/POP3S, IMAP/IMAPS, MAPI, FTP/SFTP, NNTP
 - o Suporte para análise de ficheiros em sistema baseado na cloud (OS Sandbox)
 - o Listas de ficheiros autorizados/negados
 - o Opção de análise heurística
- Detecção de sites WEB (web filtering):
 - o Suporte de diferentes mecanismos de deteção de sites WEB (proxy-based, flow-based and DNS)
 - o Possibilidade de definição manual de filtragem sites com base em URL, conteúdo web e cabeçalho MIME
 - o Categorização dinâmica em tempo real, baseada na cloud, com mais de 250 milhões de sites categorizados, de 70 idiomas e organizados em mais de 77 categorias
 - o Opção para forçar a utilização de mecanismos de busca segura (safe search) disponibilizados pelos principais motores de busca, incluindo Google, Yahoo!, Bing & Yandex, e definição customizada de YouTube Education Filter
 - o Deverá ser possível ter a opção para activar as seguintes funcionalidades:
 - Filtrar Java Applet, ActiveX e/ou cookies
 - Bloquear HTTP Post
 - Registar termos/palavras utilizados nas pesquisas em motores de busca
 - Identificar imagens pelo URL
 - Bloquear redirect de HTTP de acordo com a categoria
 - Excluir, de forma simples, a inspeção SSL de tráfego encriptado em determinadas categorias relevantes à manutenção da privacidade dos utilizadores
 - Definição de quotas de utilização WEB com base em categorias
 - o Definição de categorias customizada e sobreposição de categorização
 - o Mecanismos de exceção à utilização de perfis pré-definidos;
- Mecanismos de deteção e mitigação de utilização de proxy-avoidance: Categorias de sites com proxy, apontar URLs por domínio e endereço IP, bloquear redirects de cache para sites com cache e tradução de sites, bloqueio de ligação a proxy com base em deteção de aplicação, bloqueio de tráfego com comportamento de proxy com base em assinaturas de IPS
- Prevenção e proteção de fugas de informação - DLP
 - o Suporte de protocolos na análise de mensagens: HTTP-POST, SMTP, POP3, IMAP, MAPI, NNTP
 - Possibilidade de executar as acções: registar, bloquear, quarentena de utilizar/IP/Interface
 - Filtros pré-definidos incluindo cartões de crédito e número de segurança Social
 - o Suporte de protocolos na análise de ficheiros: HTTP-POST, HTTP=-GET, SMTP, POP3, IMAP, MAPI, FTP, NNTP
 - Opções de filtragem disponíveis, tais como tamanho, tipo de ficheiro, watermark, conteúdo e deteção de encriptação
 - o Utilização de mecanismos de DLP watermarking, com disponibilização de ferramentas gratuitas de watermarking para Windows e Linux
 - o Fingerprinting de ficheiros
 - o Arquivamento de ficheiros detetado para inspeção forense, incluindo: todo o conteúdo de e-mail, FTP, IM, NNTP e tráfego WEB

Ao nível de **Alta Disponibilidade** deverão ser suportadas as seguintes funcionalidades:

- Alta disponibilidade disponível nos modos: ativo-passivo, ativo-ativo, virtual-cluster, VRRP
- Interfaces de heartbeat redundantes
- Interfaces reservadas para gestão
- Sem custos de licenciamento para suporte de funcionalidades de alta-disponibilidade
- Reposição automática de serviço (failover)
 - o Monitorização de portas e links (locais e remotos)
 - o Sem perda de sessões
 - o Failover em menos de 1 segundo
 - o Notificações de eventos de failover
- Diferentes opções de arquitetura
 - o HA com agregação de links
 - o Full mesh HA
 - o Suporte para HA com equipamento geograficamente dispersos
- Opção de sincronização de sessões em equipamentos configurações em modo Standalone

Ao nível de **Administração, Monitorização e Diagnósticos** deverão ser suportadas as seguintes funcionalidades:

- Acesso de gestão gráfica e texto: HTTPS com recurso a web browser
- Acesso de gestão em modo de texto: SSH, Telnet ou consola
- Sem necessidade de utilização de software cliente específico para gestão gráfica
- Suporte de múltiplas linguagens de administração no acesso gráfico, incluindo: Português, inglês
- Suporte para gestão local e gestão centralizada em simultâneo
- Suporte para gestão centralizada com integração em plataforma específica para o efeito
- Integração com plataformas externas de gestão e monitorização, incluindo SNMP, sFlow, Syslog
- Implementação rápida da solução incluindo mecanismos de auto instalação por USB, execução local e remota de scripts
- Visualização em tempo real do estado do equipamento através de interface gráfica (acesso HTTPS com recurso a web-browser) incluindo diversos conteúdos e funcionalidades.

Ao nível de **Registo de Eventos e Relatórios**, as seguintes funcionalidades deverão ser suportadas:

- Suporte para registo de eventos (logs) em diferentes repositórios, tais como: memória e/ou discos rígidos locais, múltiplos servidores de syslog, múltiplos servidores específicos para registos de eventos e elaboração de relatórios, servidores do tipo WebTrends e plataformas disponíveis na cloud
- Opção de logging confiável com recurso a mecanismos TCP (RFC 3195)

- Encriptação de eventos para confidencialidade e integridade aquando da utilização de plataformas específicas;
- Possibilidade de exportar relatórios em formato PDF
- Calendarização de backups de logs para sistemas externos
- Registos detalhados de tráfego: tráfego enviado, bloqueado, sessões violadas, tráfego local, pacotes inválidos
- Organização de registos de acordo com a categoria: administração de sistema (para auditoria), routing e networking, VPN, autenticação de utilizadores, wireless
- Opção para registo encurtado ou completo de eventos
- Resolução de nomes de endereços IP e protocolos

Ao nível de **Certificações**, os equipamentos deverão ter as seguintes certificações:

- Certificações ICSA de Firewall, IPsec, IPS, Antivirus, SSL-VPN
- Certificação USGv6/IPv6

All-In-One - Funcionalidades
5 anos de serviço de IPS por equipamento
4 portas a 10GE SFP+ por equipamento
4 portas a 25GE SFP28 por equipamento
2 portas HA/gestão por equipamento
8 portas GE SFP por equipamento
2 portas a 40GE QSFP+ por equipamento
960GB SSD por equipamento
Processador para funções de rede e processador para funções de conteúdo
Alta disponibilidade
Latência da firewall com pacotes de 64 bytes de 3us
Débito de tráfego ipv4 e ipv6 a 1510 bytes UDP de 80Gbps
67,5 Mpps de débito na firewall

100000 políticas de firewall
12,5Gbps de Débito no IPS
9,8Gbps de débito no NGFW
7,1Gbps de débito na proteção contra ameaças
8 milhões de sessões TCP concorrentes
10 domínios virtuais
Suporte de 24x7 a 5 anos por equipamento
Fontes de alimentação redundantes e hot swappable

Esta solução também inclui uma solução centralizada com base numa solução em hardware para gestão e outra para análise, recolha de relatórios (obter indicadores de compromisso) e análise de logs de vários equipamentos de firewall, adiante designado como **Análise**, bem como uma solução de gestão operacional e visibilidade, adiante designado por **Gestor**, do que vai acontecendo nos equipamentos de firewall.

No equipamento **Gestor** terá de ter de ser possível gerir equipamentos, políticas, bem como automatizar tarefas e configurações. Terá de ser possível otimizar a panorâmica das violações e das tentativas de violação bem como a panorâmica do incremento ou decréscimo das ameaças cibernéticas a partir de uma única consola, podendo-as detetar com precisão e automatizar a sua correlação.

No equipamento **Análise** terá de ser possível receber logs dos equipamentos **all-in-one** e **all-in-one-DC**, correlacionar eventos e indicadores de compromisso de modo a poupar tempo a identificar ameaças através de relatórios predefinidos e personalizados, como também ser possível gerá-los de forma agendada, exportá-los para pdf, csv e xml, bem como obter gráficos com os resultados. Também terá de ser possível neste equipamento reenviar os logs para outros equipamentos que pode ser um syslog ou qualquer outro compatível com o Common Event Format(CEF).

Para a componente de gestão, deverão ser suportadas as seguintes funcionalidades:

Domínios administrativos e políticas globais

- Permitir que o administrador principal crie grupos de firewalls para outros administradores poderem gerir e monitorizar:
 - o Os administradores podem gerir firewalls no site central ou através de sites remotos
 - o Múltiplos contextos virtuais de firewall podem ser geridos por múltiplos contextos virtuais de administração

- o Atribuição de permissões de gestão a utilizadores por diferentes contextos virtuais de administração
- o Administradores têm acesso de gestão apenas aos contextos virtuais de firewalls assignados
- o Criar modelos de configuração para novos firewalls
- o Capacidade para configurar Políticas Globais

APIs JSON e XML (Serviços Web)

- Suporte para APIs:
 - o JSON API - Permite MSSPs e grandes empresas criarem portais web personalizados para administração de políticas e objetos
 - o XML API - Permite aos administradores automatizarem tarefas comuns, tais como provisionamento de novos firewalls e também configurações nos firewalls existentes

Gestão dos conteúdos de segurança aplicacional

- Gestão dos conteúdos de segurança aplicacional permite ao administrador ter um maior controlo sobre as atualizações de segurança. Inclui suporte para o seguinte:
 - o Atualizações de definições de antivírus
 - o Atualizações de prevenção de intrusões
 - o Atualizações de gestão de vulnerabilidades
 - o Web Filtering
 - o Antispam

Controlo e gestão

- Gestão de firewalls e/ou agentes de endpoint individualmente ou em grupos lógicos
- Atualização do firmware dos firewalls
- Descobrir novos firewalls de forma automática
- Criação, implementação e monitorização de VPNs
- Delegar o controlo a diferentes utilizadores com diferentes permissões de administração
- Auditoria sobre as alterações de configuração efetuadas

Para a componente de Análise, as seguintes funcionalidades deverão ser suportadas:

Relatórios e Ferramentas de Visualização:

- Visualização e filtragem dos Top Users utilização das VPNs
- Visualização dos endereços dos destinos, sites web e ameaças

- Deverá ter por omissão vários modelos de relatórios tipo
- Relatórios com o sumário do UTM e Tráfego
- Capacidade de monitorizar e alertar o administrador de TI sobre eventos importantes
- Capacidade de Importar/Exportar modelos de relatórios já criados para outro equipamento de análise ou outro ADOM

APIs JSON e XML (Serviços Web):

- Suporte para APIs:
 - o JSON API - Permite MSSPs e grandes empresas manipularem os relatórios do FortiAnalyzer, charts/datasets e objetos
 - o XML API - Permite aos administradores aprovisionarem/configurarem o FortiAnalyzer e gerar relatórios

Visualização de Logs:

- Visualização de Logs em tempo real ou por histórico
- Visualizar pelo tipo de tráfego ou por logs de segurança
- Visualizar pelo tipo de device, ADOM
- Filtragem de Logs
- Visualização de Logs de forma granular
- Apresentação dos Logs com pictogramas das bandeiras do países e aplicações
- NOC View

Gestão de Eventos:

- Criar alertas de forma simples
- Desencadear alertas consoante o nível de severidade, eventos específicos, por tipo de ações e destinos
- Definir vários limites pelo número de eventos por um determinado tempo
- Visualizar ou procurar alertas através do histórico
- Notificar por email/SNMP ou enviar eventos por syslog

DLP Archiving:

- Investigar arquivos DLP
- Suportar vários tipos de arquivo: email, HTTP, FTP, IM

Análise - Funcionalidades
4 portas GE RJ45
2 interfaces SFP+
Suportar até 2000 dispositivos
36 TB (12x3TB) de armazenamento
Plataforma multi-tenant
Autenticação por AD, LDAP e RADIUS
Possibilidade de integrar com outras tecnologias (ex.SIEM)
Interface Gráfico personalizável
Filtros por users, origem, destino e ameaças, e sumários de tráfego
Suporte de APIs JSON e XML
Visualização de logs em Tempo real
Visualização por indicadores de compromisso e respetivo sumário
Filtragem e visualização de log de forma granular
Permite a recolha de logs até 1000GB/dia e 30 000 logs/seg
Suporte 24x7 a 5 anos por equipamento
Gestor- Funcionalidades
2 portas GE RJ45
8 TB (2x4 TB) de armazenamento
2GB/dia de logs
2 portas SFP+
Gerir até 300 dispositivos
Delegar a gestão de firewalls virtuais bem como outro tipo de contextos virtuais
Suporte de APIs JSON e XML

Gestão de FW, atualização de firmware, auditoria das alterações das configurações
Monitorização em tempo real
Relatórios de atividade de rede e dos utilizadores
Possibilidade de integração com plataforma Centralizada de logs e relatórios
Suporte 24x7 a 5 anos por equipamento

Transceivers, Direct attached cables e chicotes ópticos- características e quantidades
4 transceivers 10GE SR SFP+, SFP/SFP+ e Cabos Ópticos LC-LC OM3 2 mts
2 transceivers 10GE LR SFP+, 10km e Cabos Ópticos LC-LC OS2 2 mts, (Huawei compatível)
6 DAC 40G QSFP+ para 4x10G de 2 mts
20 chicotes cat7 10GBaseT, 600MHz, SFTP, AWG26 de 3 mts

LOTE 2 - MELHORAMENTOS DO DATACENTER

Pretende-se, usando uma solução de Gestão e visibilidade Centralizada para equipamentos e recursos em consola única, o cruzamento e tratamento de informação de logs e relacioná-la entre os vários equipamentos Fortigate existentes (FGT1KC3913801059), garantindo a existência compatibilidade na recolha e análise entre os equipamentos existentes e os equipamentos a adjudicar (Lote 2).

Equipamentos existentes em produção ou que foram retirados de produção por avaria:

Equipamento	Número de Serie	Fim de suporte	Em produção	A retirar
FortiGate 1000C	FGT1KC3913801059	2022-01-17	SIM	NÃO
FortiGate 1000A	FGT1KA2606500717	2015-02-25	SIM	SIM
FortiAnalyzer 800	FLG8002706000367	2012-10-16	NÃO	-----

Routing em datacenter

O adjudicatário deve fornecer equipamento de interligação da rede de datacenter à rede campus, composta por 2 equipamentos do tipo **All-in-one (Firewall, Threat Protection[IPS, Web-filtering, Anti-Malware, SSL inspection])** em cluster e com fontes de alimentação redundantes, adiante designado por **All-in-one-DC**. O Sistema Operativo(OS) permite de forma nativa domínios virtuais geridos de forma independente por segmento de rede e com firewall de baixa latência, elevado throughput e uma boa proteção contra ameaças e respetiva visibilidade no cenário de eventos de clientes (projetos académicos e corporativos distribuídos por vários HOSTs físicos ou virtuais) em datacenter.

<u>Equipamento</u>	<u>Resumo</u>	<u>Quantidade</u>
All-in-one-DC.	All-in-one/ Unified Threat Management (Firewall, Threat Protection [IPS, Web-filtering, Anti-Malware, SSL inspection]) com Alta Disponibilidade	2

<u>Ligadores</u>	<u>Resumo</u>	<u>Quantidade</u>
transceivers	10GE ZR SFP+, 80km SMF (Huawei compatível)	2
transceivers	10GE LR SFP+, 10km SMF (Huawei compatível)	2
transceivers	10GE SR SFP+ MMF	4
DAC	40G QSFP+ para 4x10G de 2 mts	4
Chicotes Óticos	LC-LC OS2 2 mts	4
Chicotes Óticos	LC-LC OM3 2 mts	4

Ao nível de **Integração com redes de comunicações** deverão ser suportadas as seguintes funcionalidades:

- Servidor de DHCP, NTP e DNS incluído
- Funcionalidade de DNS Proxy
- Múltiplos modos de configuração de interfaces:
 - o Sniffer
 - o Agregação de portas (802.3ad)
 - o Loopback
 - o VLANs (802.1Q e trunk)
- Routing estáticos e baseado em políticas (PBR - Policy Based Routing)
- SD-WAN
- Balanceamento e redundância de múltiplos links;
- Suporte para protocolos de routing dinâmico: RIPv1, RIPv2, RIPv3, OSPFv2 e OSPFv3, ISIS, BGP4+

- Suporte de tráfego multicast: PIM, sparse e dense mode
- Routing baseado em conteúdos: WCCP e ICAP
- Proxy explícito com suporte PAC e WPAD
- Suporte de IPv6:
- Gestão por IPv6
- Protocolos de routing dinâmico com suporte para IPv6
- Tunneling de IPv6
- Processamento firewall e UTM de IPv6
 - o NAT64
 - o NAT46
 - o VPN IPSec IPv6
- Suporte Dual Stack IPv4 e IPv6 em simultâneo
- Controlador Wireless integrado
- Controlador Switching integrado
- Virtualização da solução em contextos.
 - o Mínimo de 10 contextos licenciados de base
 - o Licenciamento opcional de 500 contextos.

Ao nível de **Identificação de utilizadores** e dispositivos deverão ser suportadas as seguintes funcionalidades:

- Base de dados local de utilizadores;
- Autenticação de utilizadores em servidores remotos: LDAP, RADIUS, TACACS+
- Sistema de Single Sign-on de utilizadores:
 - o Windows AD
 - o Novell eDirectory
 - o FortiClient
 - o Citrix e Terminal Server
 - o Radius (accounting message)
 - o Autenticação de utilizadores no acesso (802.1x, portal cativo)
- PKI e certificados:
 - o Certificados X.509
 - o Suporte SCEP
 - o Criação de Certificate Signing Request (CSR)
 - o Autorrenovação de certificados antes da data de expiração
 - o Suporte OCSP
- Autenticação de 2 fatores
 - o Servidor integrado de autenticação por tokens físicos, tokens por software e SMS
 - o Integração com terceiras partes
- Identificação de dispositivos
 - o Reconhecimento de dispositivo e sistema operativo
 - o Classificação automática de dispositivos
 - o Gestão de inventário de dispositivos
 - o Suporte de autenticação e bypass feitos por MAC Address
- Implementação de políticas de segurança com base em utilizador ou dispositivos

Ao nível de **Firewall** deverão ser suportadas as seguintes funcionalidades:

- Modos de operação NAT/route e transparente/bridge
- Agendamento de políticas: recorrentes ou apenas uma vez
- Session helpers e ALGS: dcerpc, dns-tcp, dns-udp, ftp, H.323, MGCP, MMS, PMAP, PPTP, RAS, RSH, SIP, TFTP, TNS (Oracle)
- Suporte para tráfego VoIP: SIP/H.323 /SCCP NAT traversal, RTP pinhole
- Suporte para diferentes tipos de protocolos: SCTP, TCP, UDP, ICMP, IP
- Visualização de políticas de forma global ou por pares de interfaces
- Definição de objetos para utilização em políticas incluindo: predefinidos, customizados, agrupamento de objetos, tagging e definição de cor de objetos
- Definição de objetos de endereços de diferentes tipos: IP, Subnet, intervalo de IPs, Geografia e FQDN
- Utilização de objetos de serviços Internet (ex: Azure, Office365) com atualização automática das gamas de IP e portos.
- Configuração de NAT: por política e tabela central de NAT
- Suporte de NAT: NAT64, NAT46, NAT estático, NAT dinâmico, PAT, Full Cone NAT
- Traffic shaping e QOS: shaping de tráfego partilhado por política, shapping por IP, largura de banda máxima e garantida, número máximo de ligações por IP, priorização de tráfego, suporte de Type of Service (TOS) e Differentiated Services (DiffServ)
- Processamento de tráfego de firewall IP4 e IPv6 feito em processador dedicado e desenhado para o efeito.

Ao nível de **IPS - Detecção e prevenção de intrusões** deverão ser suportadas as seguintes funcionalidades:

- Suporte de IPS com mais de 7000 assinaturas, deteção de anomalias nos protocolos, assinaturas customizadas, atualização manual ou automática das assinaturas (push ou pull), integração com enciclopédia de ameaças para melhor informação/visualização de ataques detetados
- Diferentes ações de IPS: definido por defeito na assinatura, monitorizar, bloquear, reset de sessão ou quarentena do IP do atacante com definição de duração
- Possibilidade de registo integral do pacote onde foi detetado o ataque
- Definição de diferentes perfis de IPS de forma manual ou baseada em filtro (severidade, alvo, sistema operativo, aplicação e/ou protocolo)
- Aplicação de perfis de IPS por política de firewall para maior flexibilidade
- Opção de excluir a aplicação de assinaturas de IPS específicas com base em IPs
- Proteção de DoS sobre IPv4 e IPv6 com definições contra TCP Syn flood, TCP/UDP/SCTP port scan, ICMP sweep, TCP/UDP/ SCTP/ICMP session flooding (source/destination)
- Possibilidade de implementação de IDS em modo sniffer

Ao nível de **Controlo de aplicações** deverão ser suportadas as seguintes funcionalidades:

- Detecção de mais de 3100 aplicações distintas organizadas por categorias
- Definição de aplicações customizadas

- Controlo avançado de aplicações de IM e Facebook
- Definição de diferentes perfis de controlo de aplicações de forma manual ou baseada em filtro (categoria, popularidade, tecnologia, fabricante, risco e/ou protocolo)
- Aplicação de perfis de controlo de aplicações por política de firewall para maior flexibilidade
- Detecção de aplicações mesmo dentro de ligações proxy
- Diferentes ações de controlo de aplicações: bloquear, reset de sessão, monitorização, aplicação de gestão de largura de banda
- Inspeção SSH

Ao nível de **Proteção contra ameaças** deverão ser suportadas as seguintes funcionalidades:

- Possibilidade de inspeção aplicacional de tráfego encriptado por SSL, incluindo as seguintes funcionalidades: IPS, controlo de aplicações, anti-vírus, filtragem WEB e DLP
- Capacidade de descriptação de sessões SSL com cópia de tráfego descriptado para um sistema externo
- Inspeção apenas de certificado SSL ou Inspeção deep-packet com técnicas MiTM
- Detecção e bloqueio de BOTNETs com base em listas de reputação de IPs globais;
- Excluir, de forma simples, a inspeção SSL de tráfego encriptado em determinadas categorias relevantes à manutenção da privacidade dos utilizadores
- Suporte de anti-vírus nos modos flow (pacote-a-pacote) e proxy (reconstrução de sessões)
- Suporte de inspeção de anti-vírus, em modo flow, nos seguintes protocolos: HTTP/HTTPS, SMTP/SMTPS, POP3/POP3S, IMAP/IMAPS, MAPI, FTP/SFTP, SMB, NNTP
- Suporte de anti-vírus em modo proxy, incluindo:
 - Suporte dos seguintes protocolos: HTTP/HTTPS, SMTP/SMTPS, POP3/POP3S, IMAP/IMAPS, MAPI, FTP/SFTP, NNTP
 - Suporte para análise de ficheiros em sistema baseado na cloud (OS Sandbox)
 - Listas de ficheiros autorizados/negados
 - Opção de análise heurística
- Detecção de sites WEB (web filtering):
 - Suporte de diferentes mecanismos de deteção de sites WEB (proxy-based, flow-based and DNS)
 - Possibilidade de definição manual de filtragem sites com base em URL, conteúdo web e cabeçalho MIME
 - Categorização dinâmica em tempo real, baseada na cloud, com mais de 250 milhões de sites categorizados, de 70 idiomas e organizados em mais de 77 categorias
 - Opção para forçar a utilização de mecanismos de busca segura (safe search) disponibilizados pelos principais motores de busca, incluindo Google, Yahoo!, Bing & Yandex, e definição customizada de YouTube Education Filter
 - Deverá ser possível ter a opção para activar as seguintes funcionalidades:
 - Filtrar Java Applet, ActiveX e/ou cookies
 - Bloquear HTTP Post
 - Registar termos/palavras utilizados nas pesquisas em motores de busca
 - Identificar imagens pelo URL
 - Bloquear redirect de HTTP de acordo com a categoria
 - Definição de quotas de utilização WEB com base em categorias

- o Definição de categorias customizada e sobreposição de categorização
 - o Mecanismos de exceção à utilização de perfis pré-definidos;
- Mecanismos de deteção e mitigação de utilização de proxy-avoidance: Categorias de sites com proxy, pontar URLs por domínio e endereço IP, bloquear redirects de cache para sites com cache e tradução de sites, bloqueio de ligação a proxy com base em deteção de aplicação, bloqueio de tráfego com comportamento de proxy com base em assinaturas de IPS
- Prevenção e proteção de fugas de informação - DLP
 - o Suporte de protocolos na análise de mensagens: HTTP-POST, SMTP, POP3, IMAP, MAPI, NNTP
 - Possibilidade de executar as acções: registar, bloquear, quarentena de utilizar/IP/Interface
 - Filtros pré-definidos incluindo cartões de crédito e número de segurança Social
 - o Suporte de protocolos na análise de ficheiros: HTTP-POST, HTTP=-GET,SMTP, POP3, IMAP, MAPI, FTP, NNTP
 - Opções de filtragem disponíveis, tais como tamanho, tipo de ficheiro, watermark, conteúdo e deteção de encriptação
 - o Utilização de mecanismos de DLP watermarking , com disponibilização de ferramentas gratuitas de watermarking para Windows e Linux
 - o Fingerprinting de ficheiros
 - o Arquivamento de ficheiros detetado para inspeção forense, incluindo: todo o conteúdo de e-mail, FTP, IM, NNTP e tráfego WEB
- Integração nativa com plataformas externas de filtragem de email, sandbox.

Ao nível de **Alta disponibilidade** deverão ser suportadas as seguintes funcionalidades:

- Alta disponibilidade disponível nos modos: ativo-passivo, ativo-ativo, virtual-cluster, VRRP
- Interfaces de heartbeat redundantes
- Interfaces reservadas para gestão
- Sem custos de licenciamento para suporte de funcionalidades de alta-disponibilidade
- Reposição automática de serviço (failover)
 - o Monitorização de portas e links (locais e remotos)
 - o Sem perda de sessões
 - o Failover em menos de 1 segundo
 - o Notificações de eventos de failover
- Diferentes opções de arquitetura
 - o HA com agregação de links
 - o Full mesh HA
 - o Suporte para HA com equipamento geograficamente dispersos
- Opção de sincronização de sessões em equipamentos configurados em modo Standalone ou Cluster geográfico

Ao nível de **Administração, Monitorização e Diagnósticos** deverão ser suportadas as seguintes funcionalidades:

- Acesso de gestão gráfica e texto: HTTPS com recurso a web browser
- Acesso de gestão em modo de texto: SSH, Telnet ou consola
- Sem necessidade de utilização de software cliente proprietário para gestão gráfica
- Suporte de múltiplas linguagens de administração no acesso gráfico, incluindo: português, inglês, espanhol, francês, japonês, chinês simplificado, chinês tradicional e coreano
- Suporte para gestão local e gestão centralizada em simultâneo
- Suporte para gestão centralizada com integração em plataforma específica para o efeito
- Integração com plataformas externas de gestão e monitorização, incluindo SNMP, sFlow, Syslog e Netflow
- Implementação rápida da solução incluindo mecanismos de auto instalação por USB, execução local e remota de scripts
- Visualização em tempo real do estado do equipamento através de interface gráfica (acesso HTTPS com recurso a web-browser) incluindo diversos conteúdos e funcionalidades.
- Integração com outras soluções (incluído de terceiras partes) através de scripts CLI e APIs.
- Wizards de configuração para implementação rápida da solução.
- Integração com soluções Openstack, VMWare NSX, e Cisco ACI.

Ao nível de **Registo de eventos e relatórios** deverão ser suportadas as seguintes funcionalidades:

- Suporte para registo de eventos (logs) em diferentes repositórios, tais como: memória, disco rígido local, múltiplos servidores de syslog, múltiplos servidores específicos para registos de eventos e elaboração de relatórios, servidores do tipo WebTrends e plataformas disponíveis na cloud
- Opção de logging confiável com recurso a mecanismos TCP (RFC 3195)
- Encriptação de eventos para confidencialidade e integridade aquando da utilização de plataformas específicas;
- Possibilidade de exportar relatórios em formato PDF
- Calendarização de backups de logs para sistemas externos
- Registos detalhados de tráfego: tráfego enviado, bloqueado, sessões violadas, tráfego local, pacotes inválidos
- Organização de registos de acordo com a categoria: administração de sistema (para auditoria), routing e networking, VPN, autenticação de utilizadores, Wireless
- Opção para registo encurtado ou completo de eventos
- Resolução de nomes de endereços IPs e protocolos
- Mecanismo nativo de visualização de eventos de forma estática, com ferramentas de busca e drill-down disponível através de recurso com web browser.
-

Ao nível de **Certificações** deverão ser suportadas as seguintes funcionalidades:

- Certificações ICSA de Firewall, SSL VPN, IPSEC VPN, AV e IPS
- USGv6 IPv6 Certified

All-In-One-DC - Funcionalidade mínimas
5 anos Fortiguard IPS por equipamento
16 portas a 10GE SFP+ por equipamento
480GB SSD por equipamento
Processador para funções de rede e processador para funções de conteúdo
Latência da firewall com pacotes de 64 bytes de 3us
Débito de tráfego ipv4 e ipv6 a 1510 bytes UDP de 80Gbps
75 Mpps de débito na firewall
200000 políticas de firewall
23Gbps de Débito no IPS
22Gbps de débito no NGFW
13Gbps de débito na proteção contra ameaças
50 milhões de sessões TCP concorrentes
Pelo menos 10 domínios virtuais
Fontes de alimentação redundantes
2 portas GE RJ45 para gestão por equipamento
Suporte 24x7 a 5 anos por equipamento

Transceivers e Direct attached cables - características e quantidades
2 transceivers 10GE ZR SFP+, 80km e Cabos Óticos LC-LC OS2 2 mts (Huawei compatível)
2 transceivers 10GE LR SFP+, 10km e Cabos Óticos LC-LC OS2 2 mts, (Huawei compatível)
4 transceivers 10GE SR SFP+, SFP/SFP+ e Cabos Óticos LC-LC OM3 2 mts
4 DAC 40G QSFP+ para 4x10G de 2 mts

Nota: Terá de se ter em atenção de que as unidades de **Análise** e **Gestão** mencionadas no **ponto anterior**, enquadram-se neste ponto.

1. SERVIÇOS DE INSTALAÇÃO

O adjudicatário obriga-se, em relação aos lotes que lhe forem adjudicados, e sem custos adicionais para o adjudicante, a assegurar:

- Levantamento de requisitos/configuração do cliente;
- Desenho Técnico e elaboração de LLD;
- Instalação dos respetivos equipamentos no local indicado pelo adjudicante na morada referido no nº 3 do artigo 5º do presente caderno de encargos;
- Colocação em Serviço;
- Passagem a produção;
- Acompanhamento dia Seguinte;
- Fornecimento de documentação do Projeto;
- Gestão de Projeto;

As tarefas serão executadas por técnicos certificados pelo fabricante nas soluções propostas pelo adjudicatário, sendo obrigatório a apresentação dos certificados que lhes reconheça capacidade para configurar, instalar, monitorizar e operacionalizar bem como implementar análises e conceitos de gestão de segurança de rede

2. SERVIÇOS DE SUPORTE

O adjudicatário obriga-se a assegurar, sem custos adicionais para o adjudicante, serviço de suporte, para todos os equipamentos fornecidos cujos requisitos mínimos são:

- Capacidade de diagnóstico remoto;
- Permitir acesso às novas versões de software lançadas pelos fabricantes;
- Substituição e/ou reparação de hardware;

3. SERVIÇOS DE MANUTENÇÃO

O adjudicatário obriga-se a assegurar, sem custos adicionais para o adjudicante, a manutenção dos equipamentos objeto do presente caderno de encargos, pelo menos, em regime de 24x7, para todos os equipamentos fornecidos.

Os requisitos mínimos pretendidos para o serviço de manutenção são:

- Serviço de apoio ao IPT, onde o proponente possa ser contactado através dos seguintes canais:
 - o Web;

- o E-mail;
 - o Telefone;
 - o Fax.
- Em caso de necessidade o proponente deve deslocar-se ao local onde estarão instalados os equipamentos, dentro dos SLAs pretendidos;
 - o Manutenção corretiva 24x7.
 - o Níveis de serviço