Contrato

Concurso Público n.º 13000033852025

Aquisição de Firewall

Primeira Outorgante: Unidade Local de Saúde Póvoa de Varzim/ Vila do Conde, E.P.E., Pessoa Coletiva , com sede no Largo da Misericórdia, 4490-421 Póvoa de Varzim, registada no Conservatório do Registo Comercial de Póvoa de Varzim, representado pelo Presidente do Conselho de Administração e pela Vogal Executiva,

Segunda Outorgante: Gonksys, S.A., Pessoa Coletiva , com sede na Rua António Nicolau D`Almeida, n.º 45 – 1.8 – Edifício Porto Office- Freguesia Ramalde 4100-320 Porto, conforme Certidão Permanente com o código de acesso , registada na Conservatória do Registo Comercial de Gondomar, aqui representada por , na qualidade de administrador único.

O Conselho de Administração da Unidade Local de Saúde Póvoa de Varzim/Vila do Conde, E.P.E. deliberou a adjudicação, em 12/06/2025, à representada da Segunda Outorgante, precedendo por concurso público acima identificado, cujo aviso de abertura, Anúncio de Procedimento n.º 13953/2025, publicado no Diário da República n.º 100, Série II de 26/05/2025, na Plataforma de Compras Públicas Vortal, pelo que, entre ambos os outorgantes, é celebrado e reciprocamente aceite, livremente e de boa-fé, o presente contrato que se rege pelas cláusulas seguintes, conforme minuta aprovada na data de adjudicação.

Artigo 1º

Objeto contratual

1. O contrato a celebrar na sequencia do concurso público, que tem por objeto principal a aquisição de Firewall nos termos do Anexo III e das cláusulas técnicas do caderno de encargos, pela Unidade Local de Saúde Póvoa de Varzim / Vila do Conde, E.P.E.,
2. O prazo de execução do contrato é de 60 dias, após assinatura de contrato escrito.

Artigo 2º

Gestor do contrato

Nos termos do artigo 290º-A do CCP é nomeado um Gestor do Contrato, com a função de acompanhar permanentemente a execução do mesmo o

Artigo 3º

Contrato

1. O Contrato é composto pelo respetivo clausulado contratual e seus anexos.
2. O Contrato a celebrar integra ainda os seguintes elementos:
    a. Os suprimentos dos erros e 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;
    b. Os esclarecimentos e as retificações relativos ao Caderno de Encargos;
    c. O Caderno de Encargos;
    d. A proposta adjudicada;
    e. Os esclarecimentos sobre a proposta adjudicada prestados pela Segunda Outorgante.
3. Em caso de divergência entre os documentos referidos no nº.2, a respetiva prevalência é determinada pela ordem pela qual são indicados nesse número.
4. Em caso de divergência entre os documentos no nº.2 e o clausulado do Contrato e seus anexos, prevalecem os primeiros, salvo quanto aos ajustamentos propostos de acordo com o disposto no artigo 99º do CCP e aceites pela Segunda Outorgante nos termos do disposto no artigo 101º desse mesmo diploma legal.
5. Além dos documentos indicados no n.º 2, a Segunda Outorgante obriga-se também a respeitar, no que lhe seja aplicável, as normas europeias e portuguesas, as especificações técnicas e homologações de organismos oficiais e fabricantes ou entidades detentoras de patentes.

Artigo 4º

Prazo de fornecimento

1. O contrato entra em vigor após a adjudicação ou celebração do contrato escrito com a emissão da nota de encomenda, e até 60 dias sem prejuízo das obrigações acessórias que devam perdurar para além da cessação do contrato.
2. A aquisição de bens terá início no prazo referido no n.º 1, e deverá ser executado em perfeita conformidade com as condições estabelecidas nos documentos contratuais e demais legislação em vigor.
3. Sem prejuízo do estabelecido nos números anteriores, a Primeira Outorgante poderá denunciar o presente contrato a todo o tempo, desde que comunique tal denúncia à Segunda Outorgante, com a antecedência mínima de 60 (sessenta) dias, relativamente à data a que pretende que a mesma produza os seus efeitos.
4. Ambas as Partes se obrigam a cumprir fiel e pontualmente todos os prazos acordados.

Artigo 5º

Quantidades

As quantidades indicadas no Anexo III.

Artigo 6º

Obrigações Principais da Segunda Outorgante

1. Sem prejuízo de outras obrigações previstas na legislação aplicável, no Caderno de Encargos ou nas cláusulas contratuais da celebração do contrato, decorrem para a Segunda Outorgante a obrigação principal de fornecimento de bens identificados na sua proposta, bem como todas as obrigações que se mostrem necessárias para o pontual cumprimento do objeto da presente contratação, designadamente tendo em atenção o disposto nas Condições Técnicas, constantes no Caderno de Encargos.
2. A título acessório, a Segunda Outorgante fica ainda obrigada, designadamente, a recorrer a todos os meios humanos, materiais e informáticos que sejam necessários e adequados ao fornecimento dos bens.

Artigo 7º

Conformidade e operacionalidade dos bens

1. A Segunda Outorgante obriga-se a entregar à Primeira Outorgante, na Unidade da Póvoa de Varzim, os bens objeto do contrato com as características, especificações e requisitos técnicos previstos nas cláusulas técnicas do Caderno de Encargos, mediante solicitação e através da nota de encomenda, de acordo com as necessidades da Primeira Outorgante.
2. Os bens objeto do Contrato devem ser entregues em perfeitas condições de serem utilizados para os fins a que se destinam, sendo a Segunda Outorgante a única responsável perante a Primeira Outorgante por qualquer defeito ou discrepância dos bens objeto do Contrato que existam no momento em que os bens lhe são entregues.
3. É aplicável, com as necessárias adaptações, o disposto na lei que disciplina os aspetos relativos à venda de bens de consumo e das garantias a ela relativas no que respeita à conformidade dos bens.

Artigo 8º

Entrega dos bens objeto do contrato

1. Os bens objeto do contrato devem ser entregues, nas instalações da Primeira Outorgante, mediante solicitação e através da nota de encomenda, de acordo com as necessidades da Primeira Outorgante.
2. Após a receção da nota de encomenda pela Segunda Outorgante no âmbito do presente contrato deverá entregar os bens no prazo máximo de 60 dias, sob pena de lhe poderem ser aplicadas as penalidades previstas na cláusula 21ª das cláusulas jurídicas.
3. Todas as despesas e custos associados com o transporte dos bens objeto do Contrato e respetivos documentos que acompanham os mencionados bens para o local de entrega são da responsabilidade da Segunda Outorgante.

Artigo 9º

Inspeção dos bens e rejeição por razões de qualidade

1. Efetuada a entrega dos bens do objeto do contrato, a Primeira Outorgante, por si ou através de terceiro por ele designado, procede à inspeção quantitativa e qualitativa dos mesmos,

com vista a verificar, respetivamente, se os mesmos correspondem às quantidades, características, especificações e requisitos técnicos definidos no Caderno de Encargos e se reúnem as características, especificações e requisitos técnicos e operacionais exigidos, de acordo com a proposta adjudicada, bem como, outros requisitos exigidos por lei.

2. Caso os bens fornecidos não sejam aceites pela Primeira Outorgante por razões de qualidade ou discrepâncias com as exigências legais e com as características, especificações e requisitos técnicos definidos na parte II do caderno de encargos, a Segunda Outorgante obriga-se à sua substituição, num prazo máximo de 24 horas, a contar da informação por escrito dessa não-aceitação.
3. Caso a Segunda Outorgante não tenha efetuado, em devido tempo, a substituição dos bens defeituosos ou desconformes, pode a Primeira Outorgante providenciar pela aquisição de produto idênticos junto de outro fornecedor, ficando a Segunda Outorgante responsável por todos os encargos decorrentes da situação causada.

Artigo 10º

Garantia dos bens

1. A Segunda Outorgante garantirá, sem qualquer encargo para a Primeira Outorgante, os bens fornecidos, pelo prazo de vigência do contrato, se outro prazo não for específico do bem a adquirir, a contar da entrega dos bens, contra quaisquer defeitos ou discrepâncias com as exigências legais e com características, especificações e requisitos técnicos definidos na parte II do CE, que se revelem a partir da respetiva aceitação do bem.
2. No caso de os bens entregues não comprovarem a total operacionalidade, bem como, a sua conformidade com as exigências legais, ou no caso de existirem defeitos ou discrepâncias com as características, especificações e requisitos técnicos definidos, deve informar, por escrito, a Segunda Outorgante.
3. No caso previsto no número anterior, a Segunda Outorgante deve proceder, ao seu encargo e no prazo razoável que for determinado pela Primeira Outorgante às reparações ou substituições necessárias para garantir a operacionalidade dos bens, o cumprimento das exigências legais e das características, especificações e requisitos técnicos exigidos.

Artigo 11º

Objeto do dever de sigilo

1. A Segunda Outorgante deve guardar sigilo sobre toda a informação e documentação, técnica e não técnica, relativa à atividade da Primeira Outorgante de que possa ter conhecimento ao abrigo ou em relação com a execução do Contrato.
2. A informação e documentação abrangida pelo dever de sigilo não pode ser transmitida a terceiros, nem objeto de qualquer uso ou modo de aproveitamento que o destinado direta e exclusivamente à execução do contrato.
3. Exclui-se do dever do sigilo previsto a informação e a documentação que fossem comprovadamente do domínio público à data da respetiva obtenção pela Segunda Outorgante ou que este seja legalmente obrigado a revelar, por força da lei, de processo judicial ou a pedido de autoridades reguladoras ou outras entidades administrativas competentes.

Artigo 12º

Prazo do dever do sigilo

O dever de sigilo mantém-se em vigor até ao termo do prazo de 5 (cinco) anos a contar do cumprimento ou cessação, por qualquer causa, do Contrato, sem prejuízo da sujeição subsequente a quaisquer deveres legais relativos, designadamente, á proteção de segredos comerciais ou da credibilidade, do prestígio ou da confiança devidos às pessoas coletivas.

Artigo 13º

Preço contratual

1. O encargo total do presente contrato é de 177.551,91€ (cento e setenta e sete mil quinhentos e cinquenta e um euros e noventa um cêntimo) sendo 144.351,15€ (cento e quarenta e quatro mil trezentos cinquenta e um euro e quinze cêntimos) referente ao valor contratual e 33.200,76€ (trinta e três mil e duzentos euros e setenta e seis cêntimos) relativos ao valor do IVA.
2. Pelo fornecimento dos bens objeto do contrato, bem como das demais obrigações constantes do Caderno de Encargos, a Primeira Outorgante deve pagar à Segunda Outorgante.
3. O preço referido, inclui todos os custos, encargos e despesas cuja responsabilidade não esteja atribuída à Primeira Outorgante nomeadamente os relativos ao transporte dos bens para o respetivo local de entrega, bem como, todos os bens complementares que fazem parte integrante dos bens objeto do Contrato e demais obrigações constantes do Contrato.

Artigo 14º

Condições de Pagamento

1. As quantias devidas pela Primeira Outorgante nos termos das cláusulas anteriores, devem ser pagas no prazo de 60 dias após receção pela Primeira Outorgante das respetivas faturas, as quais só podem ser emitidas após o vencimento da obrigação respetiva.
2. Para efeitos de pagamento, as faturas deverão ser apresentadas com uma antecedência de 60 dias em relação á data do seu vencimento.
3. Não sendo observado o prazo estabelecido no número anterior, considera-se que a respetiva prestação só se vence nos 60 dias subsequentes à apresentação da correspondente fatura.
4. Os pagamentos só serão devidos para as quantidades, descrição de bens e preços constantes na nota de encomenda.
5. A Primeira Outorgante não assumirá a responsabilidade do pagamento de faturas de fornecimento que não correspondam ou excedam os valores constantes na nota de encomenda.
6. Em caso de discordância, por parte da Primeira Outorgante quanto aos valores indicados nas faturas, deverá esta comunicar à Segunda Outorgante, por escrito, os respetivos fundamentos, devendo este prestar os esclarecimentos necessários ou proceder á emissão de nova fatura corrigida.

Artigo 15º

Assunção de compromisso

A informação de compromisso é efetuada nos termos do disposto no nº. 2 do artigo 8º do Decreto-Lei nº. 127/2012, de 21 de junho, alterado pelo DL nº. 99/2015. A assunção do compromisso é efetuada aquando da emissão da nota de encomenda de acordo com as necessidades assistenciais da ULSPVVC sendo aposto o número de compromisso que lhe deu origem, na data da sua realização e assinatura.

Artigo 16º

Atrasos nos Pagamentos

1. Qualquer atraso no pagamento das faturas referidas na cláusula anterior não autoriza a Segunda Outorgante a invocar a exceção de não cumprimento de qualquer das obrigações que lhe incumbem por força do contrato, salvo nos casos previstos no CCP.
2. A invocação da exceção de não cumprimento pela Segunda Outorgante depende de prévia notificação da Primeira Outorgante da intenção do exercício do direito e respetivos fundamentos, com a antecedência mínima de 60 dias.

Artigo 17º

Caução

1. Nos termos da faculdade prevista na alínea a) do n.º2 do artigo 88 do Código da Contratação Pública, na redação do Decreto-Lei n.º 111-B/2017, de 31/08, e no Programa do procedimento, não é exigida a prestação de caução.

Artigo 18º

Patentes, licenças e marcas registadas

1. São da responsabilidade da Segunda Outorgante, durante o fornecimento dos bens, quaisquer encargos ou responsabilidade civil decorrentes da incorporação em qualquer dos bens objeto do contrato, ou utilização desses mesmos bens, de elementos de construção, de hardware, de software ou de outros que respeitem a quaisquer patentes, licenças, marcas, desenhos registados e outros direitos de propriedade industrial ou direitos de autor conexos.
2. Caso à Primeira Outorgante venha a ser demandado por ter infringido, na execução do contrato, ou na posterior utilização dos bens objeto do mesmo, qualquer dos direitos mencionados no número anterior, cabe à Segunda Outorgante indemniza-la de todas as despesas que, em consequência, haja de fazer e de todas as quantias que tenha de pagar seja a que título for.

Artigo 19º

Seguros

1. É da responsabilidade do fornecedor, a cobertura, através de contratos de seguro, de todos os riscos a que sejam legalmente obrigados.

2. A Primeira Outorgante pode, sempre que entender conveniente, exigir prova documental da celebração de contratos de seguro referidos no número anterior, devendo a Segunda Outorgante fornecê-los no prazo que lhe for fixado.

Artigo 20º

Responsabilidade das Partes

Cada uma das Partes deve cumprir pontualmente as obrigações emergentes do Contrato e responde perante a outra por quaisquer danos que resultem do incumprimento ou do cumprimento defeituoso dessas obrigações, nos termos do Caderno de Encargos e da lei, sem prejuízo do disposto na cláusula seguinte.

Artigo 21º

Penalidades Contratuais

1. Pelo incumprimento de obrigações emergentes do contrato, a Primeira Outorgante, pode exigir da Segunda Outorgante o pagamento de uma sanção pecuniária, de montante a fixar em função da gravidade do incumprimento, nos seguintes termos:
    a) Pelo incumprimento das datas e prazos de entrega dos bens objeto do contrato, até 0,5% do preço contratual por cada dia de atraso;
    b) Pelo incumprimento da obrigação de garantia técnica ou deficiência dos bens entregues, até 10% do preço contratual;
    c) Pelo incumprimento da obrigação de continuidade de fabrico e de fornecimento, até 10% do preço contratual;
2. Em caso de resolução do contrato por incumprimento da Segunda Outorgante, a Primeira Outorgante pode exigir-lhe uma sanção pecuniária até 15% do preço contratual.
3. Ao valor da sanção pecuniária prevista no número anterior são deduzidas as importâncias pagas pela Segunda Outorgante ao abrigo da al. a) do n.º 1, relativamente aos bens objeto do contrato, cujo atraso na entrega tenha determinado a respetiva resolução.
4. Na determinação da gravidade do incumprimento, a Primeira Outorgante tem em conta, nomeadamente, a duração da infração, a sua eventual reiteração, o grau de culpa da Segunda Outorgante e as consequências do incumprimento.
5. A Primeira Outorgante poderá compensar os pagamentos devidos ao abrigo do contrato com as sanções pecuniárias devidas nos termos do presente artigo.
6. As penas pecuniárias previstas na presente cláusula não obstam a que a Primeira Outorgante possa exigir indemnização pelo dano excedente.
7. Não obstante a aplicação das penalidades, a Primeira Outorgante, em caso de manifesta necessidade, poderá adquirir a outros fornecedores os produtos em falta, ficando a diferença de preço, se a houver, a cargo da Segunda Outorgante.

Artigo 22º

Força maior

1. Não podem ser impostas penalidades à Segunda Outorgante, nem é havido como incumprimento, a não realização pontual das prestações contratuais a cargo de qualquer

das partes que resulte de caso de força maior, entendendo-se como tal as circunstâncias que impossibilitam a respetiva realização, alheias à vontade da parte afetada, que ela não pudesse conhecer ou prever à data da celebração do contrato e cujos efeitos não lhe fosse razoavelmente exigível contornar ou evitar.

2. Podem constituir força maior, se se verificarem os requisitos do número anterior, designadamente: tremores de terra, inundações, incêndios, epidemias, sabotagens, greves, embargos ou bloqueios internacionais, atos de guerra ou terrorismo, motins e determinações governamentais ou administrativas injuntivas.
3. Não constituem força maior, designadamente:
    a. Circunstâncias que não constituam força maior para os subcontratados da Segunda Outorgante, na parte em que intervenham;
    b. Greves ou conflitos laborais limitados às sociedades da Segunda Outorgante ou a grupos de sociedades em que este se integre, bem como a sociedades ou grupos de sociedades dos seus subcontratados.
    c. Determinações governamentais, administrativas ou judiciais de natureza sancionatória ou de outra forma resultantes do incumprimento, pela Segunda Outorgante, de deveres ou ónus que sobre ele recaiam;
    d. Manifestações populares devidas ao incumprimento, pela Segunda Outorgante, de normas legais;
    e. Incêndios ou inundações com origem nas instalações da Segunda Outorgante, cuja causa, propagação ou proporções se devam a culpa ou negligência sua ou ao incumprimento de norma de segurança.
    f. Avarias nos sistemas informáticos ou mecânicos da Segunda Outorgante não devidas a sabotagem
    g. Eventos que estejam ou devam estar cobertos por seguros.
4. A ocorrência de circunstâncias que possam consubstanciar casos de força maior deve ser imediatamente comunicada à outra parte.
5. A força maior determina a prorrogação dos prazos de cumprimento das obrigações contratuais afetadas pelo período de tempo comprovadamente correspondente ao impedimento resultante da força maior.

Artigo 23º

Resolução por parte da Primeira Outorgante

1. Sem prejuízo de outras situações de grave violação das obrigações assumidas pela Segunda Outorgante previstas na lei, a Primeira Outorgante pode resolver o Contrato a título sancionatório nos seguintes casos:
    a. O atraso, total ou parcial, na receção dos bens objeto do Contrato;
    b. Os bens entregues pela Segunda Outorgante obtenham, por duas vezes consecutivas, resultados negativos na inspeção efetuada pela Primeira Outorgante, nos termos do Caderno de Encargos;
2. O direito de resolução referido no número anterior exerce-se mediante declaração enviada à Segunda Outorgante e produz efeitos 30 dias após receção dessa declaração, mas é afastado se a Segunda Outorgante cumprir as obrigações em falta nesse prazo e proceder ao pagamento das penas pecuniárias correspondentes.

3. A resolução do Contrato nos termos dos números anteriores não determina a repetição das prestações já realizadas pela Segunda Outorgante, nem faz cessar as obrigações respeitantes a garantia técnica, à continuidade de fornecimento, à assistência técnica, e à formação para manutenção nos termos do Caderno de Encargos, a menos que tal seja determinado pela Primeira Outorgante.

Artigo 24º

Resolução por parte da Segunda Outorgante

A Segunda Outorgante só pode resolver o contrato nos termos e com os fundamentos previstos na lei.

Cláusula 25ª

Trabalhadores afetos ao serviço

Aos trabalhadores afetos à prestação do serviço é aplicável o n.º 13 do artigo 42.º do CCP, que determina a obrigatoriedade de cumprimento do disposto no artigo 419.º-A do CCP.

Artigo 26º

Subcontratação e cessão da posição contratual

A subcontratação e a cessão da posição contratual pela Segunda Outorgante dependem de prévia autorização da Primeira Outorgante, nos termos do CCP.

Cláusula 27ª

Cessão de créditos

Qualquer cessão a terceiros de créditos que o adjudicatário venha a ter direito no âmbito da execução do contrato carece de autorização prévia e escrita da Primeira Outorgante.

Artigo 28º

Visto do Tribunal de Contas

Sempre que o procedimento careça de visto prévio do Tribunal de Contas, o contrato apenas produzirá efeitos financeiros após a concessão de Visto do Tribunal de Contas.

Artigo29 º

Comunicações e notificações

Sem prejuízo de poderem ser acordadas outras regras quanto às notificações e comunicações entre as partes do contrato, estas devem ser dirigidas, nos termos do CCP, para o domicílio ou sede contratual de cada uma, identificados no contrato.

Artigo 30º

Contagem dos prazos

Na contagem dos prazos na fase de execução do contrato são aplicáveis as regras do artº. 471º do CCP.

Artigo 31º

Legislação aplicável

A tudo o que não se encontre especialmente regulado no programa do concurso e no caderno de encargos aplicam-se as disposições constantes do Código dos Contratos Públicos e demais legislação aplicável.

Artigo 32º

Proteção de dados pessoais

1. A Segunda Outorgante obriga-se, durante a vigência do contrato e mesmo após a sua cessação, a não ceder, revelar utilizar ou discutir com terceiros, todas e quaisquer informações e ou elementos que lhe hajam sido confiados pela Primeira Outorgante ou de que tenha tido conhecimento no âmbito do contrato ou por causa dele.
2. Os dados pessoais a que a Segunda Outorgante tenha acesso ou que lhe sejam transmitidos pela Primeira Outorgante ao abrigo do contrato serão tratados em estrita observância das regras e normas da Primeira Outorgante, comprometendo-se, designadamente a não os copiar, reproduzir, divulgar, adaptar, modificar, alterar, apagar, destruir, difundir, transmitir, divulgar ou por qualquer outra forma colocar à disposição de terceiros.
3. No caso em que exista autorização da Primeira Outorgante para a subcontratação de outras entidades para o fornecimento de bens/prestação de serviços, será a Segunda Outorgante responsável pela escolha das empresas subcontratadas, bem como por toda a atuação destas.
4. A Segunda Outorgante obriga-se a garantir que as empresas por ele subcontratadas cumprirão o disposto no Regulamento Geral de Proteção de Dados e na demais legislação aplicável, devendo tal obrigação constar dos contratos escritos a celebrar com as entidades por si subcontratadas:
    a. Utilizar os dados pessoais a que tenha acesso ou que lhe sejam transmitidos pela Primeira Outorgante única e exclusivamente para efeitos da prestação de serviços objeto deste contrato;
    b. Observar os termos e condições constantes dos instrumentos de legalização respeitantes aos dados tratados;
    c. Manter os dados pessoais estritamente confidenciais, cumprindo e garantindo o cumprimento do dever de sigilo profissional relativamente aos mesmos dados pessoais;
    d. Cumprir todas as regras relacionadas com o tratamento de dados pessoais a que a Primeira Outorgante esteja vinculada, desde que tais regras lhe sejam previamente comunicadas;
    e. Pôr em prática as medidas técnicas e de organização necessárias à proteção dos dados pessoais tratados por conta da Primeira Outorgante contra a respetiva destruição, acidental ou ilícita, perda acidental, a alteração, a difusão ou o acesso

não autorizado, bem como contra qualquer outra forma de tratamento ilícito dos mesmos dados pessoais

f. Assegurar que todos os seus colaboradores cumpram todas as obrigações previstas no contrato relativamente às regras de confidencialidade e proteção de dados pessoais;

g. Adotar todas as medidas exigidas nos termos do artigo 32º do RGPD.

5. A Segunda Outorgante será responsável por qualquer prejuízo em que a Primeira Outorgante venha a incorrer em consequência do tratamento, por parte do mesmo e/ou dos seus colaboradores, de dados pessoais em violação das normas legais aplicáveis e/ou do disposto no contrato.
6. Para efeitos do disposto nos números anteriores da presente cláusula, entende-se por "colaborador" toda e qualquer pessoa singular ou coletiva que preste serviços ao fornecedor de bens/prestador de serviços, designadamente, representantes legais, trabalhadores, prestadores de serviços, procuradores e consultores, independentemente da natureza e validade do vínculo jurídico estabelecido com o referido colaborador.
7. A obrigação de sigilo prevista na presente cláusula mantém-se mesmo após a cessação do presente contrato, independentemente do motivo por que ocorra.

Declaram conhecer e aceitar o clausulado que faz parte do contrato a assinar por ambas as partes.

Póvoa de Varzim,

Primeira Outorgante: _____

_____

Segunda Outorgante: _____

PARTE II

Cláusulas Técnicas

Next Generation Firewall - Especificações técnicas da Solução de Firewall

Todas as características e funcionalidades listadas são obrigatórias, devem existir dentro do mesmo equipamento e não serão aceites soluções com múltiplos equipamentos, exceto para efeitos de redundância. De seguida listam-se as características e funcionalidades por equipamento:

Hardware (obrigatório dentro do mesmo equipamento):

- Número de portas 1G/2.5G/5G/10G >= 12
- Número de portas 1G/10G SFP/SFP+ >= 10
- Número de portas 25G SFP28 >= 4
- Porta de consola RJ45
- Porta Micro USB serial consola >= 1
- Disco rígido SSD, em RAID >= 480GB
- A appliance de Firewall deverá ter uma arquitetura com recursos de hardware dedicados e independentes entre os serviços de gestão e os serviços de inspeção
- Deverá estar garantido que a appliance de FIREWALL, quando gerida localmente e perante uma sobrecarga dos serviços de inspeção de tráfego, não afete de forma alguma a performance dos serviços de gestão e vice-versa
- Fontes de alimentação redundantes

Performance:

- Performance da appliance com a funcionalidade de Firewall com identificação e controlo de aplicações (inspeção L7 de todo o tráfego) >= 19 Gbps
- Performance da appliance com as funcionalidades IDS/IPS, Antivírus e Anti-Spyware, URL Filtering e Sandboxing >= 10 Gbps
- Performance da appliance com a funcionalidade de VPN IPSec >= 9,9 Gbps
- Número de novas sessões por segundo >= 220 000
- Número máximo de sessões >= 2 200 000
- Capacidade para sistemas virtuais: até 11

Networking:

- As interfaces de rede da appliance deverão suportar os seguintes modos de funcionamento: TAP, Layer 2, Layer 3
- Suporte de IEEE 802.1Q
- Suporte de iEEE 802.1AX, suportando até 8 grupos de agregação com 8 interfaces por cada grupo
- Suporte de protocolos dinâmicos de routing: RIP, OSPF, BGP
- Suporte de routing estático
- Suporte de DHCP, NAT e PAT
- Capacidade de deteção de falhas bidirecionais entre a appliance e router para aplicar a protocolos de routing dinâmico ou rotas estáticas
- Capacidade de realizar policy based routing através do IP ou rede de origem

- Capacidade de realizar policy based routing através do utilizador ou grupo
- Capacidade de realizar policy based routing através do tipo de aplicação
- Suporte para TLS 1.3 e capacidade de desencriptar este tráfego
- Suporte de arquiteturas de alta disponibilidade do tipo ativo/passivo e ativo/ativo
- Suporte de arquiteturas de alta disponibilidade e escalar lateralmente até 6 membros dentro de um único cluster sem a necessidade de balanceadores externos

Identificação de Utilizadores:

- Possibilidade de aplicar políticas baseadas em utilizadores e grupos, em vez de por IP
- Integração com sistemas de diretórios para obtenção de utilizadores e grupos, incluindo Microsoft Active Directory, Novell eDirectory e Sun ONE Directory
- Possibilidade de integração de com sistemas multiutilizador como Citrix ou Microsoft Terminal Server para identificação de utilizadores
- Capacidade de analisar mensagens de SYSLOG com informação de LOGIN/LOGOUT para identificação de utilizadores
- Possibilidade de gerir utilizadores através de API XML
- Possibilidade de identificação de utilizadores através de portal de autenticação próprio, fazendo uso dos seguintes protocolos: Kerberos, NTLM, SAML SSO, TACACS+, RADIUS, Certificados de Cliente e autenticação local
- Capacidade de obter a identidade dos utilizadores a partir dos seguintes métodos: LDAP, Captive Portal, VPN, NACs (XML e API), Syslog, Terminal Services, XFF Headers, Server Monitoring, e client probing
- A solução a fornecer terá de suportar a interligação com um serviço SaaS, fornecido pelo fabricante das Firewalls, que permita interligar com diversas soluções de gestão de identidade, delegando neste serviço a interligação com os diversos gestores de identidade

Funcionalidades Gerais de Segurança:

- Possibilidade de agrupar interfaces da appliance em conjuntos independentes, formando diferentes zonas de segurança
- Possibilidade de definir a política de segurança por zonas de segurança, podendo incluir na mesma política várias zonas de origem e/ou destino para a análise de tráfego e processamento de regras de segurança
- Possibilidade de criar múltiplas regras de segurança entre zonas de origem e destino
- Capacidade de identificação de aplicações em L7 com um mínimo de 2400 aplicações identificadas
- Capacidade de identificação de subfunções dentro de uma aplicação
- Capacidade de aplicar e/ou excecionar qualquer das funcionalidades de inspeção (IPS, Antivírus, etc.) apenas ao tráfego de determinadas aplicações L7
- Possibilidade de agrupar aplicações por categorias de forma que as políticas de segurança sejam aplicadas por categorias de aplicações
- Possibilidade de identificar as aplicações quando estas não utilizam os portos TCP/UDP por defeito em qualquer tipo de tráfego/protocolo e não somente HTTP
- Possibilidade de identificar aplicações proprietárias que usem os protocolos HTTP e TCP
- Possibilidade de identificar aplicações que sejam transportadas em túneis encriptados SSL
- Capacidade de decifrar tráfego SSH e detetar aplicações não legítimas que utilizem este protocolo para comunicar (SSH tunneling)
- Capacidade de criar regras de QoS segundo as aplicações utilizadas no tráfego
- Possibilidade de aplicar políticas de NAT de forma independente das restantes políticas de segurança
- Capacidade de forçar o uso de MFA para acesso a aplicações internas

- Deve existir uma versão da solução que possa ser instalada como um container dentro de um ambiente de docker/kubernetes

IDS/IPS:

- Capacidade de aplicar políticas de prevenção ou de deteção contra a exploração de vulnerabilidades, tanto no tráfego que vai para a Internet como no tráfego que vem da Internet, sem incorrer numa latência superior a 1ms para não penalizar a experiência do utilizador, efetuando a análise numa única passagem do tráfego para todas as ameaças
- Possibilidade de aplicar diferentes perfis proteção contra exploração de vulnerabilidades de acordo com as aplicações identificadas
- Possibilidade de selecionar proteções contra a exploração de vulnerabilidades que se apliquem apenas a clientes ou servidores ou a ambos
- As vulnerabilidades devem estar categorizadas por tipo e por nível de risco, de forma que as aplicações de perfis de proteção se possam realizar com base nestas categorias
- Deve ser possível identificar as proteções pela identificação CVE das vulnerabilidades
- Capacidade de aplicar apenas as assinaturas necessárias para determinada aplicação identificada, através da seleção de perfis
- Deve ser possível converter e importar assinaturas snort e suricata para dentro da plataforma

Antivirus & Anti-Malware:

- Detetar equipamentos possivelmente comprometidos que tentem estabelecer comunicações com servidores de C&C
- Capacidade de habilitar mecanismos de DNS sinkholing que permitam interceptar pedidos de resolução de nomes para domínios comprometidos com malware
- Capacidade de definir políticas de antivírus, de forma que a transferência de ficheiros realizada no sentido Internet para rede interna ou vice-versa, sejam inspecionados e bloqueados se o seu conteúdo for malicioso
- Capacidade de aplicar políticas que permitam aplicar o motor de antivírus sobre protocolos como ftp, http, imap, pop3, smb ou smtp, definindo para cada um destes protocolos a ação a realizar (permitir os ficheiros, descartar os ficheiros, desconectar a sessão ou registar mediante logs)
- Possibilidade de enviar o ficheiro para serviços de inspeção adicionais na cloud que permitam analisar e emitir um veredicto para que appliance possa tomar uma ação no caso de um ficheiro malicioso
- Capacidade de aplicar políticas de antivírus de forma granular, permitindo aplicar essas políticas utilizadores ou grupos, a determinados segmentos de rede com determinada direção e a determinadas aplicações
- Capacidade de identificar ficheiros não através das suas extensões, mas sim através do tipo MIME do ficheiro, permitindo no mínimo a identificação de 100 tipos de ficheiros
- Deve-se poder aplicar políticas de bloqueio de ficheiros, de forma a poder bloquear a transferência de certo tipo de ficheiros ou que se permita após a confirmação por parte do utilizador e criando um log correspondente
- Capacidade de aplicar políticas de bloqueio de ficheiros atendendo a critérios como origem e destino do tráfego, utilizador ou grupo, tipo de aplicação ou de tráfego que inicia a transferência do ficheiro
- Possibilidade de bloquear a transferência de ficheiros quando utilizados URLs categorizados como perigosos do pondo de vista de ameaça de segurança
- Capacidade pesquisa de padrões sensíveis no tráfego, evitando a exfiltração de dados
- Deve existir a capacidade de analisar ficheiros executáveis e scripts powershell com um motor de machine learning local que permita bloquear ficheiros maliciosos localmente em tempo real sem necessidade de estabelecer ligações externas. Este motor deve

permitir bloquear malwares nunca antes observados e para os quais não existem assinaturas sem necessidade de recorrer a sandboxing

- Deve existir a capacidade de receber updates em tempo real de forma a não ter de aguardar minutos/horas/dias por determinado update. Assim que um novo malware é detetado por qualquer cliente do fabricante essa informação deve ser propagada em tempo real a todos os clientes de forma a diminuir o tempo de exposição a ameaças
- Deteção inline em tempo real para fornecer prevenção de ataques sem assinatura e ataques baseados em ficheiros ao mesmo tempo que identifica e interrompe imediatamente tentativas de phishing nunca antes vistas

Sandboxing e proteção Zero Day:

- Possibilidade de disponibilizar um serviço sandboxing na cloud capaz de analisar ficheiros do tipo desconhecido ou links recebidos em e-mails, de forma que se permita o envio desta informação para análise atendendo aos critérios: Tipo de aplicação utilizada para transferir o ficheiro, tipo de ficheiro que está a ser transferido, direção da transferência (download ou upload)
- Perante uma análise por parte do serviço de Sandboxing na cloud que categoriza a informação enviada como maliciosa, deverão ser criadas assinaturas num prazo máximo de 5 minutos, que possam ser utilizadas nos motores de Antivírus e URLF e que as descargas posteriores do mesmo ficheiro ou links sejam imediatamente bloqueadas (desta forma o malware desconhecido é transformado em malware conhecido automaticamente)
- O serviço de sandboxing na cloud deverá permitir consultar a informação enviada e avaliada e gerar os respetivos relatórios
- A tecnologia de Sandboxing tem que ser capaz de inspecionar protocolos como HTTP, HTTPS, SMTP, FTP, POP3 e IMAP
- A análise de malware deve ser inteligente o suficiente para analisar comportamentos do tipo "Call back" e IOC's durante a análise de malware e automaticamente criar assinaturas que permitam a prevenção de ameaças e que possam ser utilizadas pelas restantes funcionalidades da solução.
- Os sistemas de análise de malware devem ser capazes de detetar malware direcionado a sistemas operativos de MacOS, Windows, Android e Linux
- O malware cada vez mais utiliza técnicas de Anti-VM para detetar que está a ser executado num ambiente virtual e prevenir que seja detonado, escondendo o seu comportamento malicioso. A análise "Bare Metal" é uma funcionalidade onde o malware é executado em hardware real, o que impede que o malware utilize qualquer técnica de Anti-VM. A solução deve ter esta funcionalidade embebida
- Em termos de suporte de sistemas operativos windows emulados deve suportar: Windows XP, Windows 7 e Windows 10
- Deve ser garantido suporte para os seguintes ficheiros executáveis (EXE, DLL) e todos os tipos de ficheiros Microsoft Office, PDF, Flash, Java applets (JAR e CLASS), Android (ficheiros APK), macOS binaries (mach-O, DMG, PKG e application bundles) e Linux (ficheiros ELF)
- Deve ser garantido suporte para ficheiros comprimidos (RAR, 7Zip) e conteúdo encriptado
- Capacidade de desencriptar malware (unpacker) para utilização na análise estática e machine learning.

URL Filtering:

- Possibilidade de definir manualmente listas estáticas de URLs ou de IPs permitidos e não permitidos para a navegação, com a possibilidade de definir para os permitidos a ação a realizar (permitir, bloquear, permitir mas advertir, etc.)
- Permitir a navegação baseando-se em categorias de URL, sendo estas categorias atualizadas periodicamente através de serviço em cloud
- Possibilidade de incluir listas de URLs e IPs dinâmicas relacionadas com ameaças para que possam ser bloqueadas automaticamente (listas de reputação)
- Capacidade de detetar o envio de credenciais corporativas nas páginas de internet navegadas, de forma a poder advertir, bloquear ou permitir em função da categorização das páginas web
- A filtragem de URLs deve poder ser aplicada mediante diferentes perfis e deverá ser aplicada ao tráfego que sai para a Internet ou que vem da Internet
- A solução deve possuir um motor local de machine learning que seja aplicado às páginas web visitadas pelos utilizadores de forma a prevenir variantes maliciosas de javascript e acesso a páginas de phishing. Este motor deverá funcionar em tempo real e bloquear acesso a páginas que não estejam previamente categorizadas como maliciosas.
- Para além de fornecer proteção contra phishing, a solução deve ser capaz de identificar qualquer utilizador, que tente utilizar as suas credenciais corporativas num site externo à organização. Para além de identificar esta situação a solução tem de ser capaz de a prevenir

DNS Security:

- A solução deve disponibilizar um serviço de proteção DNS baseado na cloud que seja capaz de bloquear acesso a domínios maliciosos conhecidos e desconhecidos. Este serviço deve utilizar mecanismos de machine learning para detetar Domain Generated Algorithms (DGAs) e bloquear o acesso a estes
- A solução deve permitir bloquear tráfego de C&C através do canal de DNS assim como detetar e bloquear o uso indevido deste canal para efetuar exfiltração de dados (DNS tunneling).
- A funcionalidade de DNS Tunneling deve ser capaz de inspecionar o conteúdo dos pacotes de DNS.
- Este serviço deve permitir identificar quais as máquinas e utilizadores infetados, sem a necessidade de qualquer alteração na infraestrutura existente
- A adição deste serviço não deve obrigar a qualquer alteração na infraestrutura de DNS do cliente
- Para além da threat intelligence do fabricante, a solução deve utilizar informação proveniente de pelo menos 30 fontes distintas
- Deve ser possível criar políticas simples que bloqueiem ou façam sinkholing aos pedidos de DNS maliciosos
- Devem ser disponibilizadas as seguintes categorias para construção de políticas: Command and Control Domains, Malware Domains, Dynamic DNS Hosted Domains, Newly Registered Domains, Phishing Domains, Grayware Domains and Parked Domains
- A solução não deve necessitar de updates para estar atualizada e proteger contra as mais recentes ameaças
- A solução deve permitir a aplicações de tags a máquinas comprometidas, de forma a ser possível criar uma política de acesso diferenciada para estas.

SD-WAN:

- A plataforma deve incluir um módulo de SD-WAN
- A plataforma deve permitir adicionar um overlay de SD-WAN que permita escolher de forma inteligente e dinâmica os links mais apropriados para envio de tráfego

- Deve ser possível criar regras de SD-WAN por aplicação e definir os requisitos mínimos para cada link. No caso de os requisitos mínimos não serem cumpridos pelo link em uso, deve ser feito o failover do tráfego automaticamente
- Para os links deve ser possível monitorizar e definir regras com base em: latência, jitter e perda de pacotes
- A plataforma deve permitir fazer load-sharing através de múltiplos links de forma a melhorar o aproveitamento da largura de banda disponível
- As Firewalls devem suportar a funcionalidade de zero-touch provisioning
- A plataforma deve disponibilizar informação sobre a performance das aplicações e links
- Esta funcionalidade deve ser gerida centralmente através de uma única consola
- Deve ser suportada a funcionalidade de Packet duplication, o que permite a um equipamento enviar o mesmo pacote em links diferentes. O equipamento que recebe ambos os pacotes deverá descartar o último a chegar
- Deve ser suportada a funcionalidade de Forward Error Correction

Relatórios & Logs:

- Deve ser possível gerar relatórios tanto predefinidos ou personalizados, utilizando os logs criados pelo próprio equipamento sem necessidade de equipamentos externos adicionais
- Deve ser possível gerar relatórios de atividade por utilizador, incluindo aplicações utilizadas e páginas web visitadas
- Deve ser possível gerar relatórios de forma automática assim como agrupar vários relatório num único documento em formato pdf
- Entre os relatórios disponíveis devem constar relatórios com a largura de banda consumida pelas diferentes aplicações, relatórios sobre as origens e destinos geográficos das ameaças detetadas e relatórios sobre a análise do comportamento do tráfego observado que permita detetar equipamentos comprometidos que participem em botnets
- Deve ser possível programar o momento em que se deseja a geração do relatório pretendido e o seu envio através de e-mail, assim como o intervalo temporal que se pretende
- Possibilidade de armazenar os logs localmente tendo por única restrição a capacidade do disco do próprio equipamento
- Possibilidade de enviar logs para uma plataforma externa de gestão e processamento especializado de logs com o objetivo de manter os logs a largo prazo
- O repositório de logs externo deverá ser virtual
- O repositório de logs externo deve ter a capacidade de armazenar e gerir os logs de até 25 firewalls
- Capacidade de dispor de estatística gerada a partir de logs, personalizável por utilizador que permita fornecer informações como: utilizadores que mais geram tráfego, regras de segurança que mais utilizam, vulnerabilidades mais detetadas e bloqueadas, equipamentos que acederam a domínios maliciosos, vírus detetados, informação enviada ao serviço de sandboxing e equipamentos internos comprometidos
- Capacidade de utilizar um motor integrado de correlação de eventos dentro da própria appliance de forma que a partir dos logs criados se possa obter informações de alto nível
- Capacidade de gerar logs e reports sem necessidade de appliance ou máquina virtual adicional

Outras Funcionalidades:

- Possibilidade de definir aplicações e/ou vulnerabilidades customizadas mediante diferentes parâmetros como: Portos TCP/UDP que sejam usados na aplicação e combinação de padrões dentro dos "headers" dos pacotes ou mesmo no "payload" dos

próprios pacotes que se devam cumprir para que se reconheça a aplicação e/ou vulnerabilidade
- Possibilidade de decifrar tráfego SSL e SSH de forma que se possa estabelecer políticas de desencriptação baseadas em zonas por onde passa o tráfego, IP de origem ou destino, utilizadores geram esse tráfego, portos utilizados
- Capacidade de criar exceções à desencriptação para determinado tipo de tráfego
- Capacidade de decifrar tráfego com destino a sites web que utilizam certificados de curva elíptica (ECC)
- Possibilidade de enviar tráfego após desencriptação para uma interface de port mirror para análise de terceiras partes
- Capacidade de capturar tráfego em formato pcap, podendo ser estabelecido como critérios de captura do tráfego, uma determinada aplicação independentemente da origem ou destino desse tráfego
- Capacidade de capturar tráfego em formato pcap exclusivamente quando se deteta um vírus ou um ataque em qualquer um dos motores de proteção
- A solução apresentada deve permitir, mediante aquisição de subscrição (não incluída), ativar a funcionalidade de SD-WAN, a ser aplicada nos equipamentos adquiridos. Sem necessidade de aquisição de qualquer apliance ou outro form factor
- A solução apresentada deve permitir, mediante aquisição de subscrição (não incluída), possibilidade de permitir VPN Mobile user, que permita a análise de postura do equipamento que tenta conectar à VPN, bem como permitir configurar split tunnel baseado na aplicação de streaming de video
- A solução apresentada deve permitir, mediante aquisição de subscrição (não incluída), subscrever serviço de gestão na cloud, onde a administração dos equipamentos poderá ser feita através de um serviço SaaS disponibilizado pelo próprio fabricante. Este serviço permite ainda obter recomendações de melhoria das configurações em tempo real, bem como recomendações de atualização de software. O Serviço SaaS permite o armazenamento de logs das firewalls de forma a garantir a centralização dos logs e da visibilidade
- A solução apresentada deve permitir, mediante aquisição de subscrição (não incluída), fazer forward dos logs das firewalls para um serviço SaaS para armazenamento de logs.
- A solução apresentada deve permitir, mediante aquisição de subscrição (não incluída), integração com solução de IoT do mesmo fabricante, que permita identificar dispositivos e categorias. É necessário que a solução permita que se crie uma política de segurança na Firewall com base no dispositivo (não somente no IP)
- A solução apresentada deve permitir, mediante aquisição de subscrição (não incluída), identificar as aplicações de AI públicas (conhecidas mais de 800 aplicações de GenAI) que estão a ser utilizadas pelos utilizadores. Permite configurar políticas de bloqueio garantindo que os utilizadores não acedem a determinadas aplicações, por exemplo as de elevado risco.
- A solução a fornecer terá de suportar ser gerida por uma plataforma centralizada, que seja integralmente suportada com a gestão das Firewalls existentes na infrastrutura atual. Deve garantir que o interface de gestão centralizada é semelhante ao da Firewall em standalone

<u>Certificações/Declarações</u>:
- Parceiro Certificado - A concorrente deverá apresentar, obrigatoriamente com a proposta, uma declaração do fabricante mencionando a referência do presente concurso, em como é revendedor e prestador autorizado de serviços na implementação da solução apresentada

- Técnicos certificados - A concorrente deverá apresentar, obrigatoriamente com a proposta, evidências de que possui técnicos na sua equipa certificados na prestação de serviços na solução proposta
- Suporte - A concorrente deverá apresentar, obrigatoriamente com a proposta, uma declaração do fabricante da solução proposta, mencionando a referência do presente concurso, declarando a existência ou compromisso de compra de um contrato back-to-back com o fabricante, que garanta o correto cumprimento do suporte à solução apresentada

A concorrente deverá preencher o ANEXO V, comprovando as especificações e requisitos através de indicação do respetivo documento e nº de página. Os documentos apresentados deverão ser oficiais do fabricante e públicos.