REPÚBLICA PORTUGUESA
ECONOMIA E TRANSIÇÃO DIGITAL

Contrato 2021/SGE/0102

Renovação da Infraestrutura de Firewall interno em Alta Disponibilidade para Compete 2020

Entre:

O **Estado Português**, através da **Secretaria-Geral** da Economia, com o número de identificação fiscal 600 081 125, sita na Avenida da República n.º 79, 1069-218 Lisboa, na qualidade de entidade que assegura o apoio logístico e administrativo do Programa Operacional Temático Competitividade e Internacionalização-COMPETE 2020, de acordo com a Resolução de Conselho de Ministros n.º 29/2016, publicada no D. R., n.º 91, série I, de 11 de maio de 2016, representada neste ato pelo mestre João Manuel Domingos da Silva Rolo, na qualidade de Secretário-Geral, no uso de competência própria, conforme despacho n.º 1243/2021, publicado no D.R. n.º 21, série II, de 1 de fevereiro de 2021, doravante designado **Primeiro Outorgante**.

e

Aroundplaces, Instalações técnicas, Lda., sede na Rua António Rodrigues Ascenso, lote 187, Bairro da Paradela, 2660-227 Santo António dos Cavaleiros, pessoa coletiva n.º 510454410, representado neste ato por Carlos Daniel de Jesus Pinheiro e Silva, titular do Cartão do Cidadão n.º [redacted], com plenos poderes para outorgar este contrato, doravante designado **Segundo Outorgante.**

E tendo em consideração que:

a) Por despacho favorável do Secretário-Geral da Economia, em 20 de abril de 2021, no uso das suas competências próprias, nos termos do n.º 1 do art.º 36 do Código dos Contratos Públicos (CCP), foi autorizada a abertura do procedimento ao abrigo da alínea c) do artigo 20º do Código dos Contrato Públicos (INF. Nº SGE/DSCPP/INF/5870/2021).

b) Igualmente pelo referido despacho datado de 20 de abril de 2021 do Secretário-Geral da Economia, no uso das suas competências próprias, foi autorizada a realização da despesa nos termos da alínea a) do nº 1 do artigo 17.º do Decreto-Lei nº 197/99.

c) A decisão de adjudicação e de aprovação da minuta do contrato foi tomada em 21.05.2021, por despacho do Secretário-Geral da Economia, no uso das suas competências próprias na INF. Nº SGE/DSCPP/INF/7611/2021.

d) A inscrição da despesa inerente ao contrato foi feita no orçamento do primeiro outorgante a satisfazer pela classificação económica D.07.01.07.A0.C0, cabimento nº DO42100626 e compromisso nº DO52100808 e elemento PEP nº 21IN42800237.

Cláusula 1.ª

Objeto

O presente contrato tem por objeto a Renovação da Infraestrutura de Firewall interno em Alta Disponibilidade para Compete 2020.

Cláusula 2.ª

Local e entrega dos bens

Os serviços a efetuar e os bens a entregar pelo segundo outorgante serão prestados e entregues, respetivamente, nas instalações da Autoridade de Gestão do COMPETE 2020 sitas no Edifício Expo 98 na Avenida Dom João II, Lote 1.07.2.1, 3.º piso em Lisboa.

Cláusula 3.ª

Prazo

1. Os serviços, bem como o fornecimento de bens e respetiva instalação inicia-se após a assinatura e vigorará por 15 (quinze) meses.
2. Os bens deverão ser entregues no primeiro mês, após a celebração do contrato.
3. O contrato manter-se-á em vigor até total cumprimento do mesmo, sem prejuízo das obrigações acessórias que devam perdurar para além da sua cessação.

Cláusula 4.ª

Preço contratual e condições de pagamento

1. Pelo fornecimento de bens e sua instalação, objeto do contrato, bem como, pelo cumprimento das demais obrigações constantes do presente contrato, o primeiro outorgante deve pagar ao segundo outorgante o preço de 44.875,00€ (quarenta e quatro mil oitocentos e setenta e cinco euros), acrescido de IVA à taxa legal em vigor.
2. Os pagamentos serão efetuados de acordo com o seguinte escalonamento:
    a. 22.437,50€ (vinte e dois mil quatrocentos e trinta e sete euros e cinquenta cêntimos), após entrega do material, que se deve verificar até ao final do primeiro mês, após celebração do contrato;
    b. 22.437,50€ (vinte e dois mil quatrocentos e trinta e sete euros e cinquenta cêntimos), após aceitação de todos os trabalhos, ou seja, 3 meses após celebração do contrato.

3. O valor referido no número anterior inclui todos os custos, encargos e despesas cuja responsabilidade não esteja expressamente atribuída ao Compete, incluindo as despesas de transporte.

4. A obrigação considera-se vencida com o efetiva entrega/ fornecimento de bens e respetiva solução que devera ter um suporte por parte do segundo outorgante pelo período de 1 ano, 24x7.

5. Desde que devidamente emitidas, as faturas serão pagas no prazo de 30 dias, após a sua receção por parte do primeiro outorgante e verificação dos formalismos legais em vigor para o processamento das despesas públicas.

6. As faturas serão emitidas em nome do Compete/SGE – GAFME, com referência ao número de identificação fiscal e remetida por meio eletrónico para o endereço de e-mail Faturacao.DSF@sgeconomia.gov.pt ou via CTT para a Av. da República, nº 79, 1069-218 Lisboa, Portugal.

7. Em caso de discordância por parte do primeiro outorgante, quanto ao valor indicado na fatura, deve este comunicar ao segundo outorgante, por escrito, os respetivos fundamentos, ficando o segundo outorgante obrigado a prestar os esclarecimentos necessários ou proceder à emissão de nova fatura corrigida.

8. Desde que devidamente emitida e observado o disposto no n.º 1, as faturas serão pagas através de transferência bancária, após a verificação dos formalismos legais, em vigor, para o processamento das despesas públicas.

9. O atraso no pagamento das faturas confere ao segundo outorgante o direito de exigir juros de mora, nos termos legais.

Cláusula 5.ª

Obrigações do segundo outorgante e especificações técnicas

1. Sem prejuízo de outras obrigações previstas na legislação aplicável e no presente contrato e respetivo anexo, constituem obrigações principais do segundo outorgante as definidas no Anexo I - Especificações Técnicas.

2. Constituem ainda obrigações do segundo outorgante:

a) Fornecer os bens ao primeiro outorgante, conforme as características técnicas e requisitos constantes do presente contrato;

b) O segundo outorgante obriga-se a recorrer a todos os meios humanos e materiais que sejam necessários e adequados à execução do contrato;

c) Comunicar antecipadamente, logo que tenha conhecimento, ao segundo outorgante, o facto que torne total ou parcialmente impossível o fornecimento de bens e sua

instalação objeto do procedimento, ou o cumprimento de qualquer outra das suas obrigações nos termos do contrato com o primeiro outorgante;

d) Não alterar as condições do fornecimento de bens e sua instalação;

e) Não subcontratar, no todo ou em parte, a execução do objeto do contrato, sem prévia autorização do primeiro outorgante;

f) Comunicar qualquer facto que ocorra durante a execução do contrato e que altere, designadamente, a sua denominação social, os seus representantes legais, a sua situação jurídica e a sua situação comercial;

g) Manter sigilo e garantir confidencialidade, não divulgando quaisquer informações que obtenham no âmbito da formação e da execução do contrato, nem utilizar as mesmas para fins alheios àquela execução, abrangendo esta obrigação todos os seus agentes, funcionários, colaboradores ou terceiros que nelas se encontrem envolvidos.

Cláusula 6.ª

Garantias a prestar pelo segundo outorgante

O segundo outorgante fica sujeito, com as devidas adaptações e no que se refere aos elementos entregues ao primeiro outorgante na execução do contrato, às exigências legais, obrigações do segundo outorgante e prazos respetivos aplicáveis aos contratos de aquisição de bens móveis, nos termos do Código dos Contratos Públicos, incluindo a respetiva garantia nos termos legais.

Cláusula 7.ª

Obrigações do primeiro outorgante

Constituem obrigações do primeiro outorgante:

a) Pagar, no prazo acordado, as faturas emitidas pelo segundo outorgante, em conformidade com as condições de pagamento estabelecidas no presente contrato.

b) Nomear um gestor de contrato, nos termos do nº 1 do artigo 290º-A do CCP, pela gestão do presente contrato, e comunicar quaisquer alterações dessa nomeação.

c) Monitorizar a presente aquisição, no que respeita às condições da prestação e aplicar as devidas sanções em caso de incumprimento.

Cláusula 8.ª

Boa-fé

As partes obrigam-se a atuar de boa-fé na execução do contrato e a não exercer os direitos nele previstos, ou na lei, de forma abusiva.

Cláusula 9.ª

Penalidades contratuais

1. Pelo incumprimento das obrigações previstas no presente contrato, o primeiro outorgante pode exigir ao segundo outorgante o pagamento de uma pena pecuniária, de montante a fixar em função da gravidade do incumprimento e cujo valor poderá ser até 20% do preço contratual.
2. Na determinação da gravidade do incumprimento, o primeiro outorgante tem em conta, nomeadamente, a duração da infração, a sua eventual reiteração, o grau de culpa do segundo outorgante e as consequências do incumprimento.
3. Os incumprimentos deverão ser denunciados por escrito no prazo máximo de 48 horas a contar do seu conhecimento, e dados a conhecer ao segundo outorgante por fax, e-mail ou através de correio em carta registada com aviso de receção.

Cláusula 10.ª

Patentes, Licenças e Marcas Registadas

1. São da responsabilidade do segundo outorgante quaisquer encargos decorrentes da utilização, no fornecimento, de patentes, licenças ou marcas registadas e direitos de autor.
2. Caso o primeiro outorgante venha a ser demandado por ter infringido, na execução do contrato, qualquer dos direitos mencionados no número anterior, o segundo outorgante indemniza-o de todas as despesas que, em consequência, haja de fazer e de todas as quantias que tenha de pagar seja a que título for.

Cláusula 11.ª

Subcontratação e Cessão da Posição Contratual

1. O contrato tem carácter *intuitu personae*, pelo que o segundo outorgante não pode subcontratar, no todo ou em parte, a execução do seu objeto.
2. Excetua-se da proibição do número anterior a subcontratação que seja objeto de autorização prévia e por escrito do primeiro outorgante.
3. Em caso de subcontratação, o segundo outorgante mantém-se plenamente responsável pelo fornecimento de bens e sua instalação.

Cláusula 12.ª

Dados Pessoais

1. O segundo outorgante obriga-se a efetuar um tratamento lícito, leal e transparente dos dados pessoais nos termos do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016 e Lei n.º 58/2019, de 8 de agosto.

2. Os dados pessoais devem ser recolhidos para finalidades determinadas, explícitas e legítimas, bem como ser adequados, pertinentes e limitados ao que é necessário, devendo ser apagados, findo o tempo necessário para a finalidade para o qual foram recolhidos, apenas podendo ser comunicados/transmitidos à Direção Superior do primeiro outorgante.

Cláusula 13ª

Gestor do Contrato

1. O primeiro outorgante designa [redacted] do Compete2020, com a função de acompanhar permanentemente a execução do contrato.
2. O gestor do contrato deverá proceder nos termos do disposto no artigo 290.º - A do Código dos Contratos Públicos, de modo a aferir os níveis de desempenho do segundo outorgante, a execução financeira, técnica e material do presente contrato.
3. Em caso de desvios, defeitos ou outras anomalias na execução do contrato, deve o gestor comunicá-los de imediato ao órgão competente, propondo em relatório fundamentado as medidas corretivas que, em cada caso, se revelem adequadas.

Cláusula 14.ª

Revisão dos preços

Não é permitida a revisão dos preços propostos, em circunstância alguma, durante a execução do contrato.

Cláusula 15.ª

Fiscalização, controlo e avaliação do serviço prestado

O primeiro outorgante tem direito à fiscalização, controlo e avaliação dos serviços e bens fornecidos, para poder aferir se os mesmos estão a ser prestados de acordo com o contrato.

Cláusula 16.ª

Outros encargos

Todas as despesas derivadas da prestação das cauções e seguros se a eles houver lugar, são da responsabilidade do segundo outorgante.

Cláusula 17.ª

Caução

Não há lugar à prestação de caução, nos termos do nº 2 do artigo 88º do CCP.

Cláusula 18.ª

Dever de sigilo

1. O segundo outorgante obriga-se a manter sigilo, sobre toda a informação de que venha a tomar conhecimento, por via direta ou indireta, no âmbito da prestação em causa e vincula-se a não utilizar essa informação para outros fins que não aqueles destinados direta e exclusivamente à execução do contrato.
2. A informação e a documentação cobertas pelo dever de sigilo não podem ser transmitidas a terceiros, nem objeto de qualquer uso ou modo de aproveitamento que não o destinado direta e exclusivamente à execução do contrato.

Cláusula 19.ª

Contagem de prazos

Os prazos previstos no contrato são contínuos correndo em sábados, domingos e dias feriados.

Cláusula 20.ª

Casos Fortuitos ou de Força Maior

1. Nenhuma das partes intervenientes incorrerá em responsabilidades se, por caso fortuito ou força maior, for impedida de cumprir as obrigações assumidas no presente contrato.
2. Entende-se por caso fortuito ou de força maior qualquer situação ou acontecimento imprevisível e excecional, independente da vontade dos intervenientes, e que não derive de falta ou negligência de qualquer deles.
3. A parte a invocar casos fortuitos ou de força maior deverá comunicar e justificar tais situações, bem como informar o prazo previsível para restabelecer a situação.

Cláusula 21.ª

Notificações e comunicações

1. Sem prejuízo de poderem ser acordadas outras regras quanto às notificações e comunicações entre as partes, estas devem ser dirigidas, nos termos do Código dos Contratos Públicos, para o domicílio ou sede contratual de cada uma das partes, indicados no contrato.
2. Qualquer alteração dos elementos de contato deve ser comunicada à outra parte.

Cláusula 22.ª

Foro Competente

Para resolução de todos os litígios decorrentes do presente contrato fica estipulada a competência do Tribunal Administrativo de Círculo de Lisboa, com expressa renúncia a qualquer outro.

Cláusula 23.ª

Legislação Aplicável

Em tudo o que for omisso e que suscite dúvidas no presente contrato, reger-se-á pela lei geral aplicável aos contratos administrativos, bem como ao regime jurídico do Código dos Contratos Públicos e demais legislação aplicável em razão da matéria.

Cláusula 24.ª

Disposições Finais

1. O presente contrato está redigido em 23 (vinte e três) folhas, que vão ser rubricadas pelos outorgantes.
2. Todas as despesas a efetuar para a legalização do presente contrato, são da responsabilidade do segundo outorgante.
3. O segundo outorgante apresentou:
   a. Declaração comprovativa da situação regularizada relativamente a contribuições para a Segurança Social;
   b. Declaração comprovativa da situação tributária regularizada emitida pela Autoridade Tributária;
   c. Certidão permanente do Registo Comercial;
   d. Certificado de registo criminal de todos os titulares dos órgãos sociais de administração, direção ou gerência que se encontrem em efetividade de funções;
   e. Certificado de registo criminal de pessoa coletiva;
   f. Declaração emitida conforme modelo constante do anexo II do CCP, de acordo com o disposto na alínea a) do nº 1 do artigo 81.º do mesmo código.

Primeiro outorgante	Segundo outorgante
Secretário-Geral da Economia	Aroundplaces, Instalações técnicas, Lda
João M. D. da Silva Rolo Assinado de forma digital por João M. D. da Silva Rolo Dados: 2021.06.09 14:30:53 +01'00'	Assinado com Assinatura Digital Qualificada por: CARLOS DANIEL DE JESUS PINHEIRO E SILVA AroundPlaces - Instalações Técnicas, Lda Data: 07-06-2021 15:31:47

Anexo I

Especificações Técnicas

1. Introdução

Pretende-se reformular e atualizar a infraestrutura de segurança beneficiando das mais recentes tecnologias que o mercado oferece e, simultaneamente, mitigando os riscos emergentes nas diversas componentes de operação, adquirindo:

- Um cluster de duas Firewall´s em Alta Disponibilidade;
- Appliance Virtual para a recolha de log´s e eventos.

2. Requisitos gerais

Com o objetivo de simplificar a gestão da infraestrutura, permitindo uma maior flexibilidade e gestão de recursos, a solução a apresentar deverá ser integralmente do mesmo fabricante, possibilitando desta forma que exista uma maior integração e correlação das soluções a implementar.

A solução a apresentar deverá prever o suporte e subscrição de todos os serviços de segurança enunciados no presente documento, por parte do fabricante, por um período mínimo de 1 ano e em regime 24x7.

Deve ser garantido o serviço de assistência técnica local com SLA 8x5 NBD.

3. Cluster de Firewall´s

Pretende-se a implementação de um cluster de duas firewall´s em alta disponibilidade, devendo cada uma das unidades possuir um conjunto de especificações e de tecnologias que enumeramos de seguida:

3.1. Integração com redes de comunicações

As seguintes funcionalidades deverão ser suportadas:

- Servidor de DHCP, NTP e DNS incluído
- Funcionalidade de DNS Proxy
- Múltiplos modos de configuração de interfaces:
    - Sniffer

  - Agregação de portas (802.3ad)
  - Loopback
  - VLANs (802.1Q e trunk)
  - Software switch
- Routing estáticos e baseado em políticas (PBR - Policy Based Routing)
- SD-WAN
  - Application Awareness & Steering (3000+ Applications Supported)
  - Dynamic WAN Path Controller
  - NGFW with SSL Inspection
  - Dynamic failover times
  - Secure VPN Overlays
  - Single Management Console for Security & SD-WAN
  - Zero-touch provisioning
- Balanceamento e redundância de múltiplos links;
- Suporte para protocolos de routing dinâmico: RIPv1, RIPv2, RIPng, OSPFv2 e OSPFv3, ISIS, BGP4+
- Suporte de trafego 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
  - NAT64
  - NAT46
  - VPN IPSec IPv6
- Suporte Dual Stack IPv4 e IPv6 em simultâneo
- Suporte VXLAN
- Controlador Wireless integrado
- Controlador Switching integrado

- Virtualização da solução em contextos.

3.2. Identificação de utilizadores e dispositivos

As seguintes funcionalidades deverão ser suportadas:

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

3.3. Firewall

As seguintes funcionalidades deverão ser suportadas:

- 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.245 I, H.245 0, H.323, MGCP, MMS, PMAP, PPTP, SIP, TFTP
- Suporte para trafego 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, STUN
- 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.

3.4. VPN

As seguintes funcionalidades deverão ser suportadas:

- IPSEC VPN:
    - Suporte para peers remotos: clientes dialup compatíveis com IPSEC, peers com IP estático ou DNS dinâmico
    - Mecanismos de autenticação: certificados ou pre-shared key
    - Opções de aceitação de peers: qualquer ID, ID específico, ID num grupo de utilizadores dialup
    - Suporte de IKEv1, IKEv2 (RFC 4306)
    - Suporte de IKE mode configuration (como servidor ou cliente)

  - Phase 1/Phase 2 Proposal encryption: DES, 3DES, AES128. AES192, AES256
  - Phase 1/Phase 2 Proposal authentication: MD5, SHA1, SHA256, SHA384, SHA512
  - Phase 1/Phase 2 Diffie-Hellman Group support: 1, 2, 5, 14
  - Suporte XAuth como cliente ou servidor
  - XAuth para clientes dialup: Server type option (PAP, CHAP, Auto), NAT Traversal option
  - Duração configurável da chave de encriptação IKE e da frequência do NAT traversal keepalive
  - Dead peer detection
  - Replay detection
  - Autokey keep-alive na Phase 2 SA
- Implementação de VPNs IPSEC nos seguintes modos: gateway-to-gateway, hub-and-spoke, full mesh, redundant-tunnel, terminação de VPNs em modo transparente
- Suporte ADVPN
- Suporte de configuração full-mesh VPN One-click
- Opções de configuração de VPNs IPSec: baseado em routing(route-based) ou baseado em politicas (policy-based)
- VPNs SSL
  - Portal de VPN SSL configurável: temas de cores, disposição, atalhos (bookmarks) mecanismos de ligação, download de cliente
  - Suporte para domínio de SSL VPN: permite a customização de múltiplos portais VPN SSL associados a grupos de utilizadores, incluindo URL do portal e desenho
  - Atalhos (bookmarks) com single sign-on: permite reutilizar um login anterior ou credenciais pré-definidas para aceder a recursos internos
  - Gestão de atalhos (bookmarks) pessoais
  - Gestão de utilizadores concorrentes
  - Controlo/limitação de múltiplos acessos VPN com as mesmas credenciais de acesso
  - Suporte de VPN SSL em modo web:
    - Para clientes remotos equipamentos apenas com um browser web
    - Disponibiliza suporte web para aplicações como: HTTP/HTTPS, FTP, Telnet, SMB/CIFS, SSH. VNC, RDP, Citrix

- Suporte para VPN SSL em modo túnel:
  - Para acesso a partir de computadores que necessitam utilizar qualquer software do tipo cliente-servidor.
  - Disponível para MAC OSX, Windows, IOS, Android e Windows Mobile
- Validação da integridade do dispositivo cliente e do sistema operativo;
- Opção para limpeza de cache aquando da terminação da sessão VPN SSL
- Opção de utilização de desktop virtual que permite isolar a sessão VPN SSL no ambiente de trabalho do computador cliente

- Monitorização de VPNs IPSec e SSL com diferentes níveis de detalhe
- Suporte para outras VPNs como L2TP (modo cliente e servidor), L2TP over IPSec, PPTP e GRE over IPSec
- Processamento de tráfego de IPSec feito em processador dedicado e desenhado para o efeito.

3.5. IPS - Deteção e prevenção de intrusões

As seguintes funcionalidades deverão ser suportadas:

- Suporte de IPS com mais de 11000 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 (IP do atacante, IP de atacante e vitima, 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 especificas 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
- Possibilidade de criar novas assinaturas

3.6. Controlo de aplicações

As seguintes funcionalidades deverão ser suportadas:

- Deteção 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
- Deteção 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 SSL

3.7. Proteção contra ameaças

As seguintes funcionalidades deverão ser suportadas:

- 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 desencriptação de sessões SSL com cópia de tráfego desencriptado para um sistema externo
- Inspeção apenas de certificado SSL ou Inspeção deep-packet com técnicas MiTM
- Deteção 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, ICQ, YM, NNTP
- Suporte de anti-vírus em modo proxy, incluindo:
    - Suporte dos seguintes protocolos: HTTP/HTTPS, STMP/SMTPS, POP3/POP3S, IMAP/IMAPS, MAPI, FTP/SFTP, ICQ, YM, NNTP
    - Suporte para análise de ficheiros em sistema baseado na cloud (OS Sandbox)

  - Listas de ficheiros autorizados/negados
  - Opção de análise heurística
- Integração com solução de Sandboxing (cloud ou on-premises)
- Deteção 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 245 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
    - 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
  - Definição de categorias customizada e sobreposição de categorização
  - 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
  - Suporte de protocolos na análise de mensagens: HTTP-POST, SMTP, POP3, IMAP, MAPI, NNTP

        - Possibilidade de executar as acções: registar, bloquear, quarentena de utilizador/IP/Interface
        - Filtros pré-difinidos incluindo cartões de crédito e número de segurança Social
    - 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
    - Utilização de mecanismos de DLP watermarking , com disponibilização de ferramentas gratuitas de watermarking para Windows e Linux
    - Fingerprinting de ficheiros
    - Arquivamento de ficheiros detetados 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 e WAF
- Feeds de ameaças por Domain Name e/ou IP Address

3.8. Alta disponibilidade

As seguintes funcionalidades deverão ser suportadas:

- 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)
    - Monitorização de portas e links (locais e remotos)
    - Sem perda de sessões
    - Failover em menos de 1 segundo
    - Notificações de eventos de failover
- Diferentes opções de arquitetura
    - HA com agregação de links
    - Full mesh HA
    - Suporte para HA com equipamento geograficamente dispersos
- Opção de sincronização de sessões em equipamentos configurados em modo Standalone ou Cluster geográfico

3.9. Administração, Monitorização e Diagnósticos

As seguintes funcionalidades deverão ser suportadas:

- 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 de Public SDN:
    - Amazon Web Services (AWS)
    - Microsoft Azure
    - Google Cloud Platform (GCP)
    - Oracle Cloud Infrastructure (OCI)
    - AliCloud
- Integração com solução de Private SDN:
    - Kubernetes
    - VMware ESXi
    - VMware NSX
    - Openstack (Horizon)
    - Application Centric Infrastructure (ACI)

- Nuage Virtualized Services Platform e Cisco ACI.

3.10. Registo de eventos e relatórios

As seguintes funcionalidades deverão ser suportadas:

- 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 trafego: 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 estatisca, com ferramentas de busca e drill-down disponível através de recurso com web browser.

3.11. Certificações

O equipamento deverá ter as seguintes certificações:

- Certificações: ICSA Labs: Firewall, IPsec, IPS, Antivirus, SSL-VPN; USGv6/IPv6

3.12. Conectividade

As seguintes interfaces mínimas deverão ser asseguradas:

- Interfaces 1GbE SFP Slots: 16
- Interfaces GbE SFP ou 10/100/1000: 16
- GE RJ45 Management: 2
- Console Port (RJ45): 1

3.13. Sistema

As seguintes características mínimas deverão ser asseguradas:

- Onboard Storage: 2x 240 GB SSD

3.14. <u>Desempenho:</u>

As seguintes características mínimas deverão ser asseguradas:

- Aceleração do tráfego de Firewall e IPSec por hardware: Hardware dedicado
- Aceleração de tráfego NGFW por hardware: Hardware dedicado
- Débito firewall IPv4 (pacotes UDP de 1518 / 512 / 64 bytes): 32 / 32 / 24 Gbps
- Débito firewall IPv6 (pacotes UDP de 1518 / 512 / 64 bytes): 32 / 32 / 24 Gbps
- Latência de firewall (pacotes UDP de 64 bytes): 2,14 µs
- Débito firewall (pacotes por segundo): 36 Mpps
- Sessões TCP concorrentes: 4 Milhões
- Novas sessões/segundo (TCP): 450.000
- Políticas de firewall: 10.000
- Débito VPN IPSec (pacotes 512 bytes): 20 Gbps
- Túneis IPsec Gateway-to-Gateway: 2.000
- Túneis IPSec cliente remoto: 50.000
- Débito VPN SSL: 4,5 Gbps
- VPN SSL - Máximo de utilizadores recomendados em simultâneos: 5.000
- Débito IPS: 7,8 Gbps
- Débito de inspeção SSL: 4,5 Gbps
- Inspeção SSL CPS (IPS, HTTPS diversas cifras): 4.000
- Débito de inspeção SSL para sessões concorrentes: 300.000
- Débito de Application Control: 12 Gbps
- Débito NGFW: 5 Gbps
- Débito Threat Protection: 5 Gbps
- Débito CAPWAP (HTTP 64K): 12 Gbps
- Domínios Virtuais (por defeito / máximo): 10 / 10
- Máximo de APs controlados (Tunnel Mode): 256
- Máximo de Switchs geridos: 72
- Máximo de Tokens: 5.000
- Licenciamento ilimitado de utilizadores: SIM

3.15. Condições ambientais

As seguintes características mínimas deverão ser suportadas:

- Temperatura de funcionamento: 0 - 40 °C
- Humidade: 10 a 90% sem condensação
- Compliance: FCC Part 15 Class A, RCM, VCCI, CE, UL/cUL, CB

3.16. Dimensões

As seguintes características deverão ser suportadas:

- Altura: 1RU

4. Plataforma de Recolha de Log's e Eventos

Pretende-se a implementação de uma appliance no formato virtual para recolha de log's e eventos centralizados da solução a implementar, devendo esta possuir um conjunto de especificações e de tecnologias que enumeramos de seguida:

4.1. Relatórios e Ferramentas de Visualização

As seguintes funcionalidades deverão ser suportadas:

- 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 repositório de logs e eventos.

4.2. APIs JSON e XML (Serviços Web)

As seguintes funcionalidades deverão ser suportadas:

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

4.3. Visualização de Logs

As seguintes funcionalidades deverão ser suportadas:

- 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
- Serviço IoC (Indicator of Comprimise)

4.4. Gestão de Eventos

As seguintes funcionalidades deverão ser suportadas:

- 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

4.5. DLP Archiving

As seguintes funcionalidades deverão ser suportadas:

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

4.6. Capacidade

As seguintes características mínimas deverão ser asseguradas:

- Devices/ ADOMs/ VDOMs Suportados (Máximo): 10.000
- Capacidade de armazenamento (Mínimo / Máximo): 500 GB / +100 TB
- GB/Dia de Logs (Mínimo / Máximo): 1 GB / +2 TB

4.7. Máquina Virtual

- Suporte de Hypervisor:

  - VMware ESX/ESXi 5.0/5.1/5.5/6.0/6.5/6.7,
  - Microsoft Hyper-V 2008 R2/2012/2012 R2/2016,
  - Citrix XenServer 6.0+ and Open Source Xen 4.1+,
  - KVM on Redhat 6.5+ and Ubuntu 17.04,
  - Nutanix AHV (AOS 5.10.5),
- Suportar vCPU (Mínimo / Máximo): 2 / Unlimited
- Suporte de Memória (Mínimo / Máximo): 4 GB / Unlimited
- Interfaces de rede (Mínimo / Máximo): 1 / 4
- Serviço Indicator of Compromise (IOC): Sim

4.8. Licenciamento

Deverá ser assegurado o licenciamento mínimo para:

- 1 GB/ Dia para Log's;
- 500 GB de capacidade de Storage.

4.9. Suporte

A solução devera ter suporte por parte do fabricante pelo período de 1 anos 24x7.