FACULDADE DE DIREITO
UNIVERSIDADE DE LISBOA

Aprovo,

Assinado com Assinatura Digital
Qualificada por:
MARIA PAULA DOS REIS VAZ FREIRE
Diretora da Faculdade de Direito
FACULDADE DE DIREITO DA
UNIVERSIDADE DE LISBOA
Data: 26-07-2022 15:13:51

Prof.ª Doutora Paula Vaz Freire
Diretora da Faculdade de Direito - ULisboa
(nos termos do Despacho 1431/2020, de 31 de janeiro)

CONSULTA PRÉVIA

AQUISIÇÃO DE FIREWALL COM SUPORTE APLICACIONAL PARA A FACULDADE DE DIREITO DA UNIVERSIDADE DE LISBOA

CADERNO DE ENCARGOS

Procedimento n.º FDUL.2022.020

PARTE I

CLÁUSULAS JURÍDICAS

CAPÍTULO I
DISPOSIÇÕES INICIAIS

Cláusula 1.ª
Objeto

1. O presente caderno de encargos tem por objeto a aquisição de uma *appliance* de Segurança para funcionar em alta disponibilidade com *appliance* Palo Alto Networks existente (PA-3220).
2. O equipamento a fornecer deve ser totalmente integrável com o equipamento passivo já existente e configurado todo o sistema para comutação automática de funcionamento, em caso de falha.
3. No âmbito do presente procedimento e nos termos do n.º 1 do artigo 1.º do Decreto-Lei n.º 107/2012, de 18 de maio foi emitido parecer favorável pela AMA – Agência para a Modernização Administrativa, em 15/07/2022.

Cláusula 2.ª
Contrato

1. O contrato é composto pelo respetivo clausulado contratual e seus anexos e será reduzido a escrito, integrando igualmente os elementos elencados nas disposições aplicáveis do Código dos Contratos Públicos (CCP).
2. Para além dos elementos referidos pelo número anterior, o contrato integra ainda:
   a. Os suprimentos dos erros e das omissões do caderno de encargos identificados pelo concorrente, 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 pelo concorrente.
3. Em caso de divergência entre os documentos referidos no número anterior, a ordem de prevalência é a que nele se dispõe.

Cláusula 3.ª

Duração do contrato

1. O contrato entra em vigor na data da sua assinatura, considerando-se para o efeito, no caso de assinatura eletrónica, a data da última assinatura aposta no mesmo.
2. O contrato mantém-se em vigor por 1 (um) ano, podendo ser prorrogado por igual período até um máximo de 2 (duas) prorrogações, sem prejuízo das obrigações acessórias que devam perdurar para além da cessação do contrato, incluindo as de confidencialidade e de garantia.
3. Adicionalmente, sem prejuízo do disposto no número anterior, a disponibilização do bem objeto do contrato deverá ocorrer no prazo máximo de 30 (trinta) dias, contados a partir da data de assinatura do contrato.

Cláusula 4.ª

Gestor do Contrato

1. Para o acompanhamento permanente e para a garantia da boa execução do contrato, é designado um gestor.
2. O gestor detetará os desvios, defeitos ou outras anomalias na execução do contrato, identificando e propondo medidas corretivas que se revelem adequadas, ao órgão competente para a decisão de contratar.

Cláusula 5.ª

Rescisão do Contrato

1. O incumprimento, por uma das partes, dos deveres resultantes do contrato confere à outra parte, nos termos gerais de direito, o direito de rescindir o contrato, sem prejuízo das correspondentes indemnizações legais.
2. Caso se verifique que o adjudicatário não garante a correta, completa e adequada articulação entre os bens fornecidos e a finalidade a que os mesmos se destinam, bem como não dê cumprimento aos prazos definidos no presente caderno de encargos, a entidade adjudicante procederá à resolução imediata do contrato, sem obrigação de pagamento de qualquer indemnização.

Cláusula 6.ª

Patentes, licenças e marcas registadas

São da responsabilidade do adjudicatário quaisquer encargos decorrentes da utilização, na execução do contrato, de marcas registadas, patentes registadas ou licenças.

Cláusula 7.ª

Dever de sigilo

1. O adjudicatário garantirá o sigilo por parte dos elementos da sua equipa, não podendo divulgar ou facilitar a terceiros qualquer informação confidencial e/ou de circulação restrita por parte da Faculdade de Direito da Universidade de Lisboa, independentemente do âmbito da mesma.
2. O dever de sigilo abrange toda a informação e documentação, técnica e não técnica, comercial ou outra, relativa à Faculdade de Direito da Universidade de Lisboa, de que o adjudicatário fique com conhecimento ao abrigo do contrato a celebrar.
3. Exclui-se do dever de sigilo toda a informação e documentação que seja comprovadamente do domínio público à data da respetiva obtenção pelo adjudicatário ou que esta seja legalmente obrigado a revelar, por força da lei, de processo judicial ou a pedido de autoridades reguladoras ou, similarmente, por outras entidades administrativas competentes.
4. O adjudicatário não pode utilizar o logotipo ou qualquer outro sinal distintivo da entidade adjudicante sem o seu consentimento prévio.

CAPÍTULO II
ESTIPULAÇÕES CONTRATUAIS

Secção I
Obrigações

Cláusula 8.ª

Obrigações do adjudicatário

1. Sem prejuízo de outras obrigações previstas na legislação aplicável, da celebração do contrato decorre para o adjudicatário as seguintes obrigações principais para com a entidade adjudicante:
   a. Preparação e planeamento de todas as operações que são requisitos inerentes à execução e manutenção das condições do contrato a celebrar, bem como das premissas técnicas do mesmo, descritas na Parte II deste caderno de encargos;
   b. Disponibilização e instalação completa dos bens contratualizados no prazo máximo de 30 (trinta) dias, contados a partir da data de assinatura do contrato;

c. Comunicar qualquer facto que ocorra durante o período de vigência do contrato e que altere designadamente, a denominação social ou os seus representantes legais;

2. A entidade adjudicante monitorizará em contínuo a prestação do objeto contratual com vista a verificar se o mesmo reúne as características, especificações e requisitos técnicos, legal e contratualmente definidos.
3. Em caso de anomalia detetada no objeto de fornecimento e se o mesmo resultar de facto imputável ao adjudicatário, este compromete-se a intervir e a repor o seu bom funcionamento, sem o direito ao pagamento de quaisquer honorários.
4. Durante todo o período de vigência do contrato, o adjudicatário compromete-se a garantir a operacionalidade dos equipamentos, bem como a assumir todos os custos, encargos e despesas cuja responsabilidade não esteja expressamente atribuída à entidade adjudicante, incluindo encargos com pessoal, deslocação de meios humanos, despesas de aquisição, transporte, armazenamento e manutenção de meios materiais, seguros, bem como quaisquer encargos decorrentes da utilização de marcas registadas, patentes ou licenças, inerentes a esta prestação contratual.

Cláusula 9.ª

Preço e condições de pagamento

1. O preço base é de 25.000€ (vinte e cinco mil euros), acrescido de IVA à taxa legal em vigor.
2. Os preços base unitários, elencados no Anexo I do presente caderno de encargos, correspondem aos valores máximos que a entidade adjudicante se dispõe a pagar por cada um dos equipamentos, licenças e serviços.
3. No que concerne aos serviços de instalação e configuração, os quais constituem uma opção de serviços a adquirir, a apresentação de um preço unitário proposto não vincula a entidade adjudicante para efeitos de adjudicação obrigatória.
4. As propostas que apresentarem preços unitários superiores aos indicados no Anexo I do presente caderno de encargos serão excluídas.
5. A quantia devida pela entidade adjudicante, nos termos do n.º 1 da presente cláusula, deve ser paga no prazo máximo de 60 (sessenta) dias após a data de receção pela entidade adjudicante da respetiva fatura.
6. A fatura deverá fazer referência obrigatoriamente ao número de compromisso a indicar pela entidade adjudicante e só pode ser emitida após o vencimento da respetiva obrigação e verificação das conformidades.

7. Qualquer pagamento só poderá ser efetuado após a verificação dos formalismos legais em vigor para o processamento das despesas públicas.
8. São encargos do adjudicatário todos os custos, encargos e despesas cuja responsabilidade não esteja expressamente atribuída à entidade adjudicante, incluindo encargos com pessoal, deslocação de meios humanos, despesas de aquisição, transporte, armazenamento e manutenção de meios materiais, seguros, bem como quaisquer encargos decorrentes da utilização de marcas registadas, patentes ou licenças, inerentes a esta prestação contratual.

Secção II
Vicissitudes

Cláusula 10.ª
Sanções contratuais

1. Pelo incumprimento de obrigações emergentes do contrato, a entidade adjudicante pode exigir ao adjudicatário o pagamento de pena pecuniária, por cada incumprimento registado, e em função da respetiva gravidade, de valor a fixar entre 1‰ (um por mil) e 5‰ (cinco por mil) do valor global da respetiva adjudicação, sem IVA.
2. No caso de incumprimento do prazo fixado para a disponibilização do bem, por causa imputável ao adjudicatário, poderá a entidade adjudicante exigir 1‰ (um por mil) do valor global da respetiva adjudicação, sem IVA, por cada dia de atraso.

Cláusula 11.ª
Subcontratação e cessão da posição contratual

A subcontratação e a cessão da posição contratual do adjudicatário dependem de autorização do Contraente Público, nos termos do Código dos Contratos Públicos.

CAPÍTULO III
DISPOSIÇÕES FINAIS

Cláusula 12.ª
Comunicações e notificações

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

2. Qualquer alteração das informações constantes do contrato deve ser comunicada à outra parte.

Cláusula 13.ª

Contagem dos prazos

1. A contagem dos prazos na fase de formação dos contratos rege-se pelo disposto no artigo 470.º do Código dos Contratos Públicos e do Código do Procedimento Administrativo, por remissão das disposições aplicáveis.
2. A contagem dos prazos na fase de execução dos contratos é realizada nos termos do artigo 471.º do Código dos Contratos Públicos, sem prejuízo dos prazos para o cumprimento das obrigações assumidas pelas partes no âmbito do contrato.

Cláusula 14.ª

Foro competente

Para resolução de todos os litígios decorrentes do contrato fica estipulada a competência do tribunal arbitral, com sede em Lisboa, constituído por três árbitros, sendo dois designados por cada uma das partes e o terceiro cooptado pelos dois indicados, o qual decide segundo o direito constituído, nos termos da Lei de Arbitragem Voluntária.

PARTE II
ESPECIFICAÇÕES TÉCNICAS

Cláusula 15.ª
Caracterização dos equipamentos

1. Os equipamentos deverão ser novos, não sendo aceitável qualquer tipo de recondicionamento.
2. Os equipamentos a fornecer deverão assegurar as características e especificações abaixo indicadas:

Hardware (obrigatório dentro do mesmo equipamento):

- Número de portas 1Gbit/s RJ45 >= 12;
- Número de portas Gigabit SFP 1Gbit/s >= 4;
- Número de portas Gigabit SFP+ 10Gbit/s >= 4;
- Disco rígido SSD >= 240GB;
- Porta de gestão dedicada "Out of Band";
- Número de portas de alta disponibilidade 1Gbit/s >= 2;
- Número de portas de alta disponibilidade 10 Gbit/s SFP+ >= 1;
- Porta USB;
- Disco rígido SSD >= 240GB;
- Montável em rack padrão de 19" com U space <= 2U;
- 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 controle de aplicações (inspeção L7 de todo o tráfego - valores de produção) >= 4,4 Gbps;
- Performance da appliance com as funcionalidades IDS/IPS, Antivírus e Anti-Spyware (valores de produção) >= 2,3 Gbps;

- Performance da appliance com a funcionalidade de VPN IPSec >= 2,5 Gbps;
- Número de novas sessões por segundo >= 48 000;
- Número máximo de sessões >= 1 000 000;

Gestão:

- Gestão e administração da própria appliance através de interface web, linha de comandos e API XML;
- Possibilidade de criar diferentes perfis e cargos de administração para a gestão da appliance, com diferentes níveis de privilégio;
- Na gestão centralizada deve ser possível criar perfis de administração que permita segmentar a gestão em diferentes tenants (Por Firewall, por número de firewalls) - Multi-tenancy;
- Possibilidade de editar configurações pendentes que ainda não foram aplicadas;
- Possibilidade de visualizar e validar alterações à configuração antes de estas alterações serem aplicadas;
- Possibilidade de descartar alterações à configuração realizadas;
- Possibilidade de armazenar diferentes versões da configuração;
- Na gestão centralizada deve existir a capacidade de criar hierarquização da política de segurança para permitir ter políticas globais para toda infraestrutura instalada;
- Na gestão centralizada deve existir a capacidade de stacks de templates com configurações reutilizáveis para múltiplos equipamentos;
- Na gestão centralizada deve existir um ponto centralizado para efetuar upgrades e atualizações de versões e assinaturas;
- Capacidade de transformar políticas de layer4 em layer7 com machine learning e aprendizagem embebida na plataforma de gestão;
- Na gestão centralizada deve existir a capacidade de "zero touch provisioning" para simplificar o deployment de firewalls remotas;
- Deve existir a capacidade de correr a Gestão centralizada sobre hardware dedicado assim como numa Máquina Virtual em VMware ESXi™, KVM e Microsoft Hyper-V, ou então em clouds públicas incluindo Google Cloud Platform (GCP™), Amazon Web Services (AWS®), AWS GovCloud, Microsoft Azure e Azure GovCloud;
- Análise da utilização das regras para reduzir superfície de exposição e melhorar postura de segurança;
- Envio de logs via SYSLOG, FTP, SCP e TFTP para retenção e posterior tratamento;

- Possibilidade de envio seletivo de logs, de acordo com o nível de severidade ou outros atributos como por exemplo o tipo de ameaça;
- Suporte de SNMP, incluindo a possibilidade de obter estatísticas relacionadas com o processamento de logs e com as funcionalidades de alta disponibilidade.

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 tipo de aplicação;
- Suporte para TLS 1.3 e capacidade de desencriptar este tráfego;
- Possibilidade de criar Firewalls virtuais dentro de um chassis com tabela de rotas, interfaces e políticas segmentadas;
- Suporte de arquiteturas de alta disponibilidade do tipo ativo/passivo e ativo/ativo;
- Permitir a criação de clusters de alta disponibilidade até 6 membros.

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;

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 a 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 determinados recursos. Deve ser possível configurar políticas que forcem qualquer utilizador em determinada

subnet, a utilizar MFA se tentar aceder a um recurso em determinado segmento de rede da organização;

- 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 escolher 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 a que a aplicação 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 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 intercetar pedidos de resolução de nomes para domínios comprometidos com malware;
- Capacidade de definir políticas de antivírus, de forma a 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 possam 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 ponto 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 que 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.

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.

Network Packet Broker

- O equipamento deve ter capacidades de Network Packet Broker de forma a permitir filtrar e encaminhar tráfego para uma cadeia externa de dispositivos de segurança de terceiros para uma análise estendida;
- Capacidade para usar um ou mais dispositivos de segurança de terceiros (Security Chain) como parte do conjunto geral de segurança;
- Capacidade de definir o tráfego encaminhado com base em aplicações, utilizadores, zonas, dispositivos e endereços de IP;
- Capacidade para encaminhar tráfego TLS (Decryption Broker) desencriptado e sem ser desencriptado;
- Capacidade para assegurar que o caminho para a cadeia de segurança está íntegro e que tenha opções para lidar com o tráfego se a cadeia não estiver operacional;
- Capacidade para suportar tráfego unidirecional e bidirecional na cadeia (Client-to-server e Server-to-client) no mesmo par de interfaces (broker interfaces);
- Capacidade de definir múltiplos perfis e associar o perfil a uma regra/politica;
- As regras/politicas devem definir o tráfego a ser encaminhado para a cadeia de segurança e o perfil deve definir como encaminhar esse tráfego, incluindo os

interfaces para encaminhamento, monitorização da integridade da cadeia, distribuição de sessão entre várias cadeias e escolha da forma como é encaminhada Routing (Layer 3) ou Transparente Bridge (Layer 1).

Relatórios & Logs:

- A appliance deve ter a capacidade para 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 relatórios 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;
- Capacidade de dispor de um painel de instrumentos personalizável por utilizador de administração da appliance com pelo menos a seguinte informação: Aplicações mais utilizadas, Aplicações de alto risco, Informação geral do sistema, Estado das interfaces, Logs relativos às ameaças mais observadas, Logs de URLs filtrados, Recursos do sistema;
- 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 enviado ao serviço de sandboxing e equipamentos internos comprometidos;

- Capacidade de utilizar um motor integrado de correlação de eventos dentro da própria appliance de forma a que a partir dos logs criados se possa obter informações de alto nível.

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 a 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.

Anexo I

Preços Base Unitários (S/IVA)

Código de Produto	Descrição	Preço Base unitário (S/IVA)[1]
PAN-PA-3220	Palo Alto Networks PA-3220 with redundant AC power supplies	5.800 €
PAN-SVC-BKLN-3220-3YR	Partner enabled premium support 3-year prepaid, PA-3220	5.200 €
PAN-PA-3220-TP-3YR-HA2	Threat prevention subscription 3 year term for device in an HA pair, PA-3220	2.900 €
PAN-PA-3220-ADVURL-3YR-HA2	Advanced URL Filtering Subscription, 3-year, PA-3220 HA Pair	4.300 €
PAN-PA-3220-BND-LAB4-R	PA-3220 Lab Unit Renewal Service Bundle (Advanced Threat Prevention, DNS, Advanced URL Filtering, GlobalProtect, WildFire, SD-WAN, VSYS-5, Standard Support) 3-year	6.300 €
-	Serviços de instalação e configuração [2]	500 €

Preço Base (S/IVA): [3]	25.000 €

1) Valor máximo que a entidade adjudicante se dispõe a pagar por cada item
2) No que concerne aos serviços de instalação e configuração, os quais constituem uma opção de serviços a adquirir, a apresentação de um preço unitário proposto não vincula a entidade adjudicante para efeitos de adjudicação obrigatória.
3) O preço base (S/IVA) resulta do somatório (incluindo os serviços de instalação e configuração opcionais) dos preços base unitários (S/IVA) para cada item.