

# **CADERNO DE ENCARGOS**

## **AQUISIÇÃO DE SOLUÇÃO DE FIREWALL**

NOVEMBRO 2022

## **PARTE I – CLÁUSULAS GERAIS**

### **Artigo 1.º**

#### **Objeto**

O presente Caderno de Encargos compreende as cláusulas a incluir no contrato a celebrar na sequência do procedimento que tem por objeto o fornecimento de solução firewall de nova geração.

### **Artigo 2.º**

#### **Local de entrega dos bens**

Os bens objeto deste contrato serão entregues no armazém do Município de Torres Novas, salvo outra indicação a entidade adjudicante.

### **Artigo 3.º**

#### **Entrega dos bens**

1. O fornecimento a realizar no âmbito do contrato não poderá exceder o prazo fixado no artigo 9.º do presente Caderno de Encargos.
2. O fornecimento será realizado de acordo com o Mapa de Trabalhos apresentado pelo adjudicatário, em estrito respeito pelo prazo de entrega contratado.
3. Em caso de entrega de bens com anomalias ou deficiências, o adjudicatário terá de proceder à substituição por artigo conforme no prazo máximo de 15 dias seguidos, a contar a partir do último dia da data limite para conclusão do fornecimento, conforme definido no artigo 9º.

### **Artigo 4.º**

#### **Preço Base**

O preço base do fornecimento é de 15930€ (quinze mil novecentos e trinta euros), acrescido de IVA à taxa legal em vigor.

### **Artigo 5.º**

#### **Critério de Adjudicação**

1. A adjudicação será feita segundo o critério do mais baixo preço.

### **Artigo 6.º**

#### **Contrato**

1. O contrato é composto pelo respetivo clausulado contratual (cláusulas gerais e cláusulas técnicas) constante do presente caderno de encargos.
2. O contrato a celebrar integra ainda os seguintes elementos:
  - a) Os suprimentos dos erros e das 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 presente Caderno de Encargos;
  - d) A proposta adjudicada;
  - e) Os esclarecimentos sobre a proposta adjudicada prestados pelo adjudicatário.
3. Em caso de divergência entre os documentos referidos no número anterior, a respetiva prevalência é determinada pela ordem pela qual aí são indicados.
4. Em caso de divergência entre os documentos referidos no n.º 2 e o clausulado do contrato e seus anexos, prevalecem os primeiros, salvo quanto aos ajustamentos propostos de acordo com o disposto no artigo 99.º do Código dos Contratos Públicos e aceites pelo adjudicatário nos termos do disposto no artigo 101.º desse mesmo diploma legal.

#### **Artigo 7.º**

##### **Prazo**

O contrato mantém-se em vigor até à conclusão do fornecimento dos equipamentos em conformidade com os respetivos termos e condições e o disposto na lei, sem prejuízo das obrigações acessórias que devam perdurar para além da cessação do contrato, nomeadamente prazos de garantia dos equipamentos.

#### **Artigo 8.º**

##### **Obrigações principais do prestador de serviços**

1. Sem prejuízo de outras obrigações previstas na legislação aplicável, no caderno de encargos ou nas cláusulas contratuais, da celebração do contrato decorrem para o fornecedor as seguintes obrigações principais:
  - a) Obrigação de entrega dos bens identificados na sua proposta, devidamente montados e em condições plenas de serem utilizados;
  - b) Obrigação de garantia da qualidade dos bens;
2. A título acessório, o fornecedor fica ainda obrigado, designadamente, a recorrer a todos os meios humanos, materiais e informáticos que sejam necessários e adequados ao fornecimento, bem como ao estabelecimento do sistema de organização necessário à perfeita e completa execução das tarefas a seu cargo.

#### **Artigo 9.º**

##### **Prazo de conclusão do fornecimento**

1. O fornecedor obriga-se a concluir a execução do fornecimento, cumprindo o definido no ponto 1 do artigo 8.º, com todos os elementos referidos na listagem de bens constantes das cláusulas técnicas do presente caderno de encargos, no prazo máximo de 45 dias, a contar da data da comunicação da adjudicação.
2. O prazo previsto no número anterior pode ser prorrogado por iniciativa da entidade adjudicante, ou a requerimento do adjudicatário, se previamente deferido/aceite pela entidade adjudicante.

#### **Artigo 10.º**

##### **Transferência da propriedade / Aceitação**

1. Após verificação, é emitida uma declaração de aceitação dos bens, onde ficará registada a data de aceitação dos mesmos, bem como a ocorrência de eventuais falhas ou deficiências constatadas na execução do referido fornecimento, ocorrendo assim a transferência da posse e da propriedade dos elementos a desenvolver ao abrigo do contrato para a entidade adjudicante, incluindo os direitos autorais sobre todas as criações intelectuais abrangidas pelos serviços a prestar.
2. O auto de aceitação será enviado ao adjudicatário no prazo de cinco dias úteis a contar da data da aceitação.
3. Pela cessão dos direitos a que alude o número anterior não é devida qualquer contrapartida para além do preço a pagar nos termos do presente caderno de encargos.

#### **Artigo 11.º**

##### **Conformidade e garantia técnica**

O fornecedor fica sujeito, com as devidas adaptações e no que se refere aos elementos em execução do contrato, às exigências legais, obrigações do fabricante e prazos respetivos, aplicáveis aos contratos de aquisição de bens móveis, nos termos do Código dos Contratos Públicos e demais legislações aplicáveis.

#### **Artigo 12.º**

##### **Cessão da posição contratual e subcontratação**

Ao adjudicante reserva-se o direito de autorizar a cessão da posição contratual e a subcontratação do equipamento proposto a mais do que um fornecedor, nas partes que forem economicamente mais vantajosas, nos termos dos preceitos estabelecidos no CCP (art.º 316.º a art.º 324.º).

#### **Artigo 13.º**

##### **Objeto do dever de sigilo**

1. O fornecedor deve guardar sigilo sobre toda a informação e documentação, técnica e não técnica, comercial ou outra, relativa à entidade adjudicante, de que possa ter conhecimento ao abrigo ou em relação com a 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.
3. Exclui-se do dever de sigilo previsto a informação e a documentação que fossem comprovadamente do domínio público à data da respetiva obtenção pelo prestador fornecedor 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 14.º**

##### **Preço contratual**

1. Pela prestação dos serviços objeto do contrato, bem como pelo cumprimento das demais obrigações constantes do presente caderno de encargos, a entidade adjudicante deve pagar ao prestador de serviços o preço constante da proposta adjudicada, acrescido de IVA à taxa legal em vigor, se este for legalmente devido.
2. O preço referido no número anterior inclui todos os custos, encargos e despesas cuja responsabilidade não esteja expressamente atribuída ao contraente público, incluindo-se, entre outras, as despesas de alojamento, alimentação e deslocação de meios humanos, despesas de aquisição, transporte, armazenamento e manutenção de meios materiais, bem como quaisquer encargos decorrentes da utilização de marcas registadas, patentes ou licenças.

#### **Artigo 15.º**

##### **Condições de pagamento**

- 1 – A quantia devida pelo município de Torres Novas, nos termos do artigo 14º, deve ser paga no prazo de 30 dias após a receção pelo município da respetiva fatura.
- 2 – Em caso de discordância por parte do município de Torres Novas, quanto ao valor indicado na fatura, deve este comunicar ao prestador de serviços, por escrito, os respetivos fundamentos, ficando o prestador de serviços obrigado a prestar os esclarecimentos necessários ou a proceder à emissão de nova fatura corrigida.
- 3 - O prestador dos serviços deverá remeter a fatura, em formato – PDF certificado ou ficheiro eletrónico certificado para integração direta com o SIGMA municipal.
- 4 - Se o prestador dos serviços se encontrar em condições de cumprir com o legalmente estipulado quanto à faturação eletrónica em procedimentos aquisitivos de contratação pública, nos termos e ao abrigo do disposto no Decreto-Lei n.º 28/2019, de 15 de fevereiro – artigo 12.º - faturação por via eletrónica, que regula as obrigações relativas ao processamento de faturas e outros documentos fiscalmente relevantes, e no Decreto-Lei n.º 123/2018, de 28 de dezembro, que define o modelo de governação para a implementação da faturação eletrónica nos contratos públicos, bem como os prazos previstos para a implementação explanados no Decreto-Lei n.º 104-A/2021, de 27 de novembro, a fatura deverá ser compatível com o sistema de faturação eletrónica implementado pelo Município.

- 5 - Para efeitos de cumprimento do referido no ponto anterior, será o prestador dos serviços devidamente informado, mediante pedido de esclarecimento, do procedimento a seguir para proceder à faturação dos serviços prestados.

#### **Artigo 16.º**

##### **Casos fortuitos / Força maior**

1. Não podem ser impostas penalidades ao fornecedor, nem é havida 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 impossibilitem 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 ou por outros conflitos coletivos de trabalho, 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 do fornecedor, na parte em que intervenham;
  - b) Greves ou conflitos laborais limitados às sociedades do fornecedor 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 pelo fornecedor de deveres ou ónus que sobre ele recaiam;
  - d) Manifestações populares devidas ao incumprimento pelo fornecedor de normas legais;
  - e) Incêndios ou inundações com origem nas instalações do fornecedor cuja causa, propagação ou proporções se devam a culpa ou negligência sua ou ao incumprimento de normas de segurança;
  - f) Avarias nos sistemas informáticos ou mecânicos do fornecedor 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 17.º**

##### **Patentes, licenças e marcas registadas**

1. São da responsabilidade do adjudicatário quaisquer encargos decorrentes da utilização, no fornecimento, de marcas registadas, patentes registadas ou licenças.
2. Caso a entidade adjudicante venha a ser demandada por ter infringido, na execução do contrato, qualquer dos direitos mencionados no número anterior, o adjudicatário 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.

#### **Artigo 18.º**

##### **Garantia**

1. O adjudicatário garantirá, sem qualquer encargo para a entidade adjudicante, os bens fornecidos, pelo prazo indicado na sua proposta, nunca sendo este inferior a dois anos.
2. O prazo de garantia referido no número anterior conta-se a partir da data da conclusão do fornecimento da totalidade dos bens.

3. São excluídos da garantia todos os defeitos que notoriamente resultarem de má utilização, de uma utilização abusiva ou de negligência da entidade adjudicante, bem como todos os defeitos resultantes de fraude, ação de terceiros, de caso fortuito ou de força maior.
4. Em caso de anomalia detetada no objeto do fornecimento, o adjudicatário compromete-se a intervir, sem prejuízo do direito ao pagamento dos honorários devidos se a anomalia resultar de facto não imputável ao adjudicatário.

#### **Artigo 19.º**

##### **Resolução por parte do contraente público**

1. Sem prejuízo de outros fundamentos de resolução previstos na lei, a entidade adjudicante pode resolver o contrato, a título sancionatório, no caso do prestador de serviços violar de forma grave ou reiterada qualquer das obrigações que lhe incumbem, designadamente nos seguintes casos:
  - a) Pelo atraso, total ou parcial, na entrega dos bens referentes do contrato superior a cinco dias relativos ao período estipulado no programa de fornecimentos constante da proposta ou declaração escrita do prestador de serviços de que o atraso respetivo excederá esse prazo;
2. O direito de resolução referido no número anterior exerce-se mediante declaração enviada ao fornecedor e não determina a repetição das prestações já realizadas, a menos que tal seja determinado pelo contraente público.

#### **Artigo 20.º**

##### **Resolução por parte do fornecedor**

1. Sem prejuízo de outros fundamentos de resolução previstos na lei, o fornecedor pode resolver o contrato quando:
  - a) Qualquer montante que lhe seja devido esteja em dívida há mais de 180 dias ou o montante em dívida exceda 25% do preço contratual, excluindo juros;
2. O direito de resolução é exercido por via judicial.
3. Nos casos previstos na alínea a) do n.º 1, o direito de resolução pode ser exercido mediante declaração enviada à entidade adjudicante, que produz efeitos 30 dias após a receção dessa declaração, salvo se este último cumprir as obrigações em atraso nesse prazo, acrescidas dos juros de mora a que houver lugar.

#### **Artigo 21.º**

##### **Renovação do contrato**

O contrato esgota-se com o fornecimento, salvaguardando-se os prazos de garantia.

#### **Artigo 22.º**

##### **Caução**

Não exigível nos termos do art.º 88º, do Código dos Contratos Públicos aprovado pelo D.L. nº 111/2017, conjugado com a Lei 30/2021 de 21 de maio, na sua atual redação, podendo o Município, sempre que o entender conveniente, proceder à retenção de 5% do valor dos pagamentos a efetuar.

#### **Artigo 23.º**

##### **Foro competente**

Para resolução de todos os litígios decorrentes do contrato fica estipulada a competência do Tribunal Administrativo territorialmente competente.

#### **Artigo 24.º**

##### **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 dirigidas, nos termos do Código dos Contratos Públicos, para o domicílio ou sede contratual de cada uma, identificados no contrato.
2. Qualquer alteração das informações de contacto constantes do contrato deve ser comunicada à outra parte.

**Artigo 25.º**

**Contagem dos prazos**

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

**Artigo 26.º**

**Omissões / Legislação aplicável**

Em tudo o que se encontrar omissa no presente Caderno de Encargos, o contrato é regulado pela legislação portuguesa aplicável.

## PARTE II – CLÁUSULAS TÉCNICAS

### Artigo 27.º

#### Proposta

1. As propostas têm de especificar o preço unitário por bem ou equipamento.
2. As propostas a apresentar têm, sob pena de exclusão, de responder integralmente à listagem de bens e características técnicas mínimas exigidas, conforme as cláusulas seguintes.

### Artigo 28.º

#### Mapa de quantidades

Os bens a fornecer são os que constam na tabela seguinte.

| N. | Item                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | Tipo     | Quantidades |
|----|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|-------------|
| 1  | Appliance de Segurança                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | Firewall | 1           |
| 2  | Licenciamento com subscrição por 36 meses: <ul style="list-style-type: none"><li>• Firewall aplicacional (Layer7)</li><li>• Controlo de utilizadores</li><li>• Threat prevention</li><li>• IDS/IPS</li><li>• Antivírus e Anti-Malware</li><li>• Anti-Spyware</li><li>• URL Filtering</li><li>• Sandbox</li><li>• DNS Security</li><li>• Análise de eventos</li><li>• Reporting</li><li>• Acesso remoto via agente com suporte multiplataforma (Windows 7 e posterior, macOS 10.11 e posterior, iOS 10 e posterior, Android 5 e posterior, CentOS e RHEL 7.0 até 7.7 e Ubuntu 14.04 até 19.04.)</li></ul> | Licença  | 1           |
| 3  | Equipamento de substituição (On-Site Spare)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Firewall | 1           |
| 4  | Instalação, configuração e colocação em serviço                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | Serviços | 1           |

### Artigo 29.º

#### Características técnicas

A solução a ser proposta deve ter características de *Next Generation Firewall* e tem de cumprir as seguintes especificações, para comprovar as especificações anexamos um ficheiro de excel ao procedimento onde se deve preencher o cumprimento do requisito e respetivo documento público do fabricante a fazer prova desse requisito.

#### Especificações de hardware

Número de portas Gigabit (10/100/1000) RJ45: 4 ou mais  
Número de portas Multi-Gigabit (1/2.5/5Gb) RJ45 com PoE: 4 ou mais  
Número de portas Multi-Gigabit (1/2.5/5Gb) RJ45: 4 ou mais  
Número de portas Gigabit SFP: 6 ou mais

Número de portas 10 Gigabit SFP+: 4 ou mais  
Porta dedicada para gestão 10/100/1000: 1  
Porta dedicada para alta disponibilidade 10 Gigabit: 1  
Porta de consola RJ45: 1  
Porta de consola micro USB: 1  
Porta USB: 1  
Fontes de alimentação: 2 (em redundância)  
Formato: appliance de rack (1U)

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.

### Performance

Performance da appliance com a funcionalidade de firewall com identificação e controle de aplicações (inspeção L7 de todo o tráfego - valores de produção): 6 Gbps ou superior

Performance da appliance com as funcionalidades IDS/IPS, Antivírus e Anti-Spyware: 3 Gbps ou superior

Performance da appliance com a funcionalidade de VPN IPSec: 4 Gbps ou superior

Número de novas sessões por segundo: 31 000 ou superior

Número máximo de sessões: 945 000 ou superior

### 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.

Na gestão centralizada deve existir a possibilidade de criar diferentes perfis e cargos de administração para a gestão da appliance, com diferentes níveis de privilégio.

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 efectuar 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.

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 utilizador ou grupo.

Capacidade de realizar policy based routing através do tipo de aplicação.

Suporte de arquiteturas de alta disponibilidade do tipo activo/passivo e activo/activo.

Permitir a criação de clusters de alta disponibilidade até 6 membros.

Suporte para TLS 1.3 e capacidade de descriptar este tráfego.

### **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.

### **Acessos Remotos e Gestão de Identidades**

A solução deve dar a capacidade de estender as funcionalidades da Firewalls (Módulos avançados de segurança Threat Prevention, URL Filtering e outros) aos utilizadores remotos.

A solução deve ser capaz de garantir a segurança dos acessos aos recursos internos como também às aplicações de cloud.

Capacidade de garantir a segurança também do acesso à internet do utilizador que esteja fora da rede.

Proteger os utilizadores remotos contra ataques de phishing e roubo de credenciais.

Capacidade de fazer quarentena a utilizadores remotos utilizando parâmetros e características imutáveis.

Suporte de VPNs por Aplicação e por utilizador.

Capacidade de fornecer acesso seguro e sem agente para parceiros e entidades externas às organizações.

Suporte de identificação automatizada de equipamentos que não são geridos pela entidade da firewall.

Capacidade de implementar Zero Trust efetuando uma identificação muito clara do utilizador.

Fornecer também a capacidade de efectuar a identificação de parâmetros do sistema operativo para poder criar regras de acesso do tipo NAC.

O módulo de identificação tem que obrigatoriamente ser capaz de identificar os seguintes parâmetros do equipamento que está a aceder à rede: Validar se o Patch Management está activo, Firewall local está activa, Anti-Malware está instalado, Plataforma de Backups está activa, Mecanismo de Encriptação de disco está activo, Modulo de DLP está activo e parâmetros customizados do sistema operativo como processos, registos ou property lists.

A solução deve disponibilizar um agente com suporte para os seguintes sistemas operativos: Windows 7 e posterior, macOS 10.11 e posterior, iOS 10 e posterior, Android 5 e posterior, CentOS e RHEL 7.0 até 7.7 e Ubuntu 14.04 até 19.04.

O mesmo agente de acessos remotos deve também ser possível funcionar como agente de identidades dentro da infraestrutura para identificação do utilizador e mapeamento de políticas baseadas em identidades.

### **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 excepcionar 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 detectar 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.

Capacidade de bloquear comunicações C&C desconhecidas, através de análise inline e machine learning, e em tempo real.

Capacidade de gerar assinaturas baseadas em payloads do tráfego malicioso que permitam detetar tráfego C&C mesmo que o host C&C seja desconhecido ou mude constantemente.

### **Antivírus & 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 detectado 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.

Capacidade de detetar e bloquear ameaças em todos e quaisquer portos em vez se basear em assinaturas que se limitam a um conjunto pre-definido de portos.

### **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 que 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 detectar 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 infectados, 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.

### **Sandboxing**

Possibilidade de disponibilizar um serviço na cloud capaz de analisar ficheiros do tipo desconhecido ou links recebidos em e-mails, de forma a 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 inspeccionar 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 detectar 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).

Incluir o suporte de ficheiros comprimidos (RAR, 7Zip) e conteúdo encriptado.

Capacidade de descriptar malware (unpacker) para utilização na análise estática e machine learning.

### **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**

A appliance deve ter a capacidade 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 detectadas 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 longo 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 detectadas e bloqueadas, equipamentos que acederam a domínios maliciosos, vírus detectados, 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 descriptação baseadas em: zonas por onde passa o tráfego, IP de origem ou destino, utilizadores geram esse tráfego, portos utilizados.

Capacidade de criar exceções à descriptação 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 descriptação 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 detecta um vírus ou um ataque em qualquer um dos motores de protecção.

### **Certificação**

É necessário entregar uma Declaração do fabricante fazendo prova que o mesmo tem conhecimento da proposta apresentada pelo concorrente, certificando que a empresa possui as competências necessárias para implementação e suporte da solução.

### **Formação**

Inclusão de formação de 4 dias para 2 pessoas com os seguintes conteúdos:

- Portfolio and Architecture of Firewalls
- Connect to the Management Network
- Manage Firewall Configurations
- Manage Firewall Administrator Accounts
- Connect to Production Networks
- Block Threats Using Security and NAT Policies
- Block Packet and Protocol-Based Attacks
- Block Threats from Known Bad Sources
- Block Threats by Identifying Applications
- Maintain Application-Based Policies
- Block Threats Using Custom Applications
- Block Threats by Identifying Users
- Block Unknown Threats
- Block Threats in Encrypted Traffic
- Prevent Use of Stolen Credentials
- Block Threats Using Security Profiles
- View Threat and Traffic Information
- Initial Configuration
- Adding Firewalls
- Templates
- Device Groups
- Log Collection and Forwarding
- Using Logs on Firewalls
- Vendor Administrative Accounts

- Reporting
- Troubleshooting

#### **Modelo de referência**

Palo Alto Networks PA-1410, ou equivalente.