CONSULTA PRELIMINAR AO MERCADO DAG/DIRS 12/2024

Equipamentos de Firewall

Nota legal:

Esta apresentação é apenas uma versão preliminar do projeto pretendido, partilhada apenas para fins de informação geral, não podendo ser considerada versão final, nem vinculativa.

As informações contidas neste documento podem estar sujeitas a alterações, não comprometendo nem vinculando os Serviços Partilhados do Ministério da Saúde, EPE e/ou quaisquer outros serviços e/ou órgãos do Ministério da Saúde ou do Serviço Nacional de Saúde.

I. ENQUADRAMENTO

A SPMS tem por missão a prestação de serviços partilhados nas áreas de compras e logística, serviços financeiros, recursos humanos e sistemas e tecnologias de informação e comunicação às entidades com atividade especifica na área da saúde, de forma a "*centralizar, otimizar e racionalizar*" a aquisição de bens e serviços no Serviço Nacional de Saúde.

Os Sistemas de Informação na Saúde permitem a cooperação, a partilha de conhecimentos e informação, bem como o desenvolvimento de atividades de prestação de serviços nas áreas dos sistemas e tecnologias de informação e comunicação. Desempenham um papel importante na reforma do sistema de saúde, tendo como principais objetivos a melhoria da acessibilidade, eficiência, qualidade e continuidade dos cuidados e o aumento da satisfação dos profissionais e cidadãos.

À SPMS cabe, ainda, a garantia da operacionalidade e segurança das infraestruturas tecnológicas e dos sistemas de informação do Ministério da Saúde, promovendo a definição e a utilização de normas, metodologias e requisitos que garantam a interoperabilidade e interconexão dos sistemas de informação da saúde entre si, e com os sistemas de informação transversais à Administração Pública, visando desenvolver e proteger a saúde dos cidadãos.

II. OBJETIVO

Pretende assim a SPMS, EPE vir a adquirir equipamentos e instalação que permitam a ampliação e modernização da capacidade de salvaguarda de dados nos seus centros de processamento de dados, pelo

que com vista à preparação do respetivo procedimento aquisitivo, e fazendo uso do disposto no artigo 35.º-A do Código dos Contratos Públicos, a SPMS, EPE vem, nos termos da denominada "consulta preliminar ao mercado", solicitar informações sobre o objeto do contrato.

Assim, na presente consulta preliminar ao mercado, pretende-se identificar:

1. O preço base a considerar pela entidade adjudicante face aos equipamentos pretendidos;
2. O preço base a considerar pela entidade adjudicante para os serviços de instalação;
3. Análise da viabilidade para os operadores económicos do procedimento, alocar os equipamentos a um adjudicatário, e os serviços a adjudicatário diferente;
4. Prazo considerado necessário para a entrega dos equipamentos e informação da necessidade de entregas faseadas;
5. Prazo considerado necessário para a instalação dos equipamentos;

A consulta preliminar será constituída por:

a) 1 Cluster de Firewall Tipo 1 – Datacenter

b) 1 Cluster de Firewall Tipo 2 – Serviços de VPN

c) Serviços de Instalação, configuração das plataformas a concurso

d) Serviços de Assistência Técnica Preventiva e Corretiva durante o período de 12 meses com cobertura 24 x 7 com 4h de tempo de resposta para os equipamentos referidos em a) e b)

e) Serviços de Assistência Técnica Preventiva e Corretiva durante o período de 36 meses com cobertura 24 x 7 com 4h de tempo de resposta para os equipamentos referidos em a) e b)

Quantidades de equipamento e serviços:

I	**Cluster de Firewall Tipo 1 - Datacenter**	1
ii	**Cluster de Firewall Tipo 2 - Serviços de VPN**	1
iii	**Serviços de Instalação, configuração das plataformas a concurso – valores separados para i e ii**	1
iv	**Serviços de Assistência Técnica Preventiva e Corretiva o período de 12 meses com cobertura 24 x 7 com 4h de tempo de resposta, - valores separados para i e ii**	1

v	**Serviços de Assistência Técnica Preventiva e Corretiva o período de 12 meses com cobertura 24 x 7 com 4h de tempo de resposta, - valores separados para i e ii**	1

a) Cumprir as alíneas a) a g) do n.º 5 da Deliberação n.º 1/2023 da Comissão de Avaliação de Segurança, disponível em https://www.gns.gov.pt/docs/cas-1-2023.pdf.

Firewall Datacenter

Mapa de Quantidades

Descrição	Quantidade
Appliance de Segurança em alta disponibilidade (HA) Chassi Modular, Base AC Hardware Bundle. Includes Chassis, 2xAC power supplies, 4xFans, Base Card, Management Processing Card, and Networking Card, includes 4 post rack mount kit	2 (1 Clusters)
Network Card	**4**
Data Processor Card	**8**
SFP 10G SR original do Fabricante (SFP+ form factor, SR 10Gb optical transceiver, short reach 300m, OM3 MMF, duplex LC, IEEE 802.3ae 10GBASE-SR compliant)	4
SFP 40G SR original do Fabricante (QSFP+ form factor, 40Gb Bidirectional optical transceiver, 100m reach over OM3 MMF, 150m over OM4 MMF, duplex LC)	12
Licenciamento em HA com subscriçao por 36 meses:	2 (1 Clusters)
Firewall Aplicacional (Layer 7)	
Controlo de utilizadores	
Advanced Threat Prevention	
IDS/IPS	
Antivirus & Anti-Malware	
AntiSpyware	
Sandboxing	
DNS Security	

Advanced URL Filtering	
SD-WAN	
Reporting	
AIOps and Cloud Manager for NGFW subscription, 3-year (Minimo de 1TB de retenção)	12
Data Lake with 1TB of storage, 3-year, includes Premium Support	22
Software de gestão centralizada, gestão de logs e automação Licenciamento 25 Devices por 36 meses	1

I. Cluster de Firewall Tipo 1 – Datacenter (2 nós)

Requisitos de Segurança da Autoridade Nacional de Segurança (GNS)	• O fabricante do equipamento deverá cumprir as deliberações da Comissão de Avaliação de Segurança nomeadamente os critérios objetivos de segurança, assim como o seu âmbito técnico de aplicação, que justificam e fundamentam medidas destinadas a garantir um elevado nível comum de segurança da informação na União Europeia

Requisitos Mínimos Por nó de Cluster

Característica base	
Para uma carta de Networking, suporte de:	
○ Número de portas 10Gbit/s RJ45	>=4
○ Número de portas Gigabit SFP+ 10Gbit/s	>=12
○ Número de portas Gigabit QSFP28 40/100 Gbit/s	>=2
Para o agregado de 2 cartas de Networking (incluídas), suporte de:	
○ Número de portas 10Gbit/s RJ45	>=8
○ Número de portas Gigabit SFP+ 10Gbit/s	>=24
○ Número de portas Gigabit QSFP28 40/100 Gbit/s	>=4
• Porta de consola RJ45	>=1
• Porta USB serial consola	>=1
• Disco rígido SSD, em RAID	>=480GB
• Discos rígido SSD para Log	>=4TB
• Ocupação máxima	<=5 Rack Units
• Arquitetura com recursos de hardware dedicados e independentes entre os serviços de gestão e os serviços de inspeção	Obrigatório
• 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	Obrigatório
• Fontes de alimentação redundantes.	Sim
Performance	
Suporte de, no mínimo, 4 cartas de Data Processing (incluídas na solução), com os seguintes requisitos de performance por carta:	
○ Performance da appliance com a funcionalidade de firewall com identificação e controle de aplicações (inspeção L7 de todo o tráfego - valores de produção)	>= 70 Gbps

○ Performance da appliance com as funcionalidades IDS/IPS, Antivírus e Anti-Spyware, Sandboxing, DNS Security, file blocking, e logging (valores de produção)	>= 38 Gbps
○ Performance da appliance com a funcionalidade de VPN IPSec	>= 17 Gbps
○ Número de novas sessões por segundo	>= 725 000
○ Número máximo de sessões	>= 20 000 000
O agregado de 4 cartas de Data Processing deve processar:	
○ Performance da appliance com a funcionalidade de firewall com identificação e controle de aplicações (inspeção L7 de todo o tráfego - valores de produção)	>= 200 Gbps
○ Performance da appliance com as funcionalidades IDS/IPS, Antivírus e Anti-Spyware, Sandboxing, DNS Security, file blocking, e logging (valores de produção)	>= 150 Gbps
○ Performance da appliance com a funcionalidade de VPN IPSec	>= 85 Gbps
○ Número de novas sessões por segundo	>= 3 600 000
○ Número máximo de sessões	>= 100 000 000

Software Gestão Centralizado

- 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
- Na gestão centralizada deve ser possível gerir até 25 firewalls num único servidor de gestão
- 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 a 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 utilizador ou grupo
- Capacidade de realizar policy based routing através do tipo de aplicação
- Suporte de arquitecturas de alta disponibilidade do tipo activo/passivo e activo/activo

- Permitir a criação de clusters de alta disponibilidade até 6 membros dentro de um único cluster sem necessidade de balanceadores externos
- Suporte para TLS 1.3 e capacidade de desencriptar 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

Funcionalidades Gerais de Segurança

- Possibilidade de agrupar interfaces da appliance em conjuntos independentes, formando diferentes zonas de segurança
- Possibilidade de definir a política de segurança por zonas de segurança, podendo incluir na mesma política várias zonas de origem e/ou destino para a análise de tráfego e processamento de regras de segurança
- Possibilidade de criar múltiplas regras de segurança entre zonas de origem e destino
- Capacidade de identificação de aplicações em L7 com um mínimo de 2400 aplicações identificadas
- Capacidade de identificação de subfunções dentro de uma aplicação
- Capacidade de aplicar e/ou excecionar qualquer das funcionalidades de inspeção (IPS, Antivírus, etc) apenas ao tráfego de determinadas aplicações L7
- Possibilidade de agrupar aplicações por categorias de forma que as políticas de segurança sejam aplicadas por categorias de aplicações
- Possibilidade de identificar as aplicações quando estas não utilizam os portos TCP/UDP por defeito em qualquer tipo de tráfego/protocolo e não somente HTTP
- Possibilidade de identificar aplicações proprietárias que usem os protocolos HTTP e TCP
- Possibilidade de identificar aplicações que sejam transportadas em túneis encriptados SSL
- Capacidade de decifrar tráfego SSH e 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 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

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.
- 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.

Sandboxing e protecção Zero Day

- Possibilidade de disponibilizar um serviço na cloud capaz de analisar ficheiros do tipo desconhecido ou links recebidos em e-mails, de forma que se permita o envio desta informação para análise atendendo aos critérios: Tipo de aplicação utilizada para transferir o ficheiro, tipo de ficheiro que está a ser transferido, direção da transferência (download ou upload)
- Perante uma análise por parte do serviço de Sandboxing na cloud que categoriza a informação enviada como maliciosa, deverão ser criadas assinaturas num prazo máximo de 5 minutos que possam ser utilizadas nos motores de Antivírus e URLF e que as descargas posteriores do mesmo ficheiro ou links sejam imediatamente bloqueadas (desta forma o malware desconhecido é transformado em malware conhecido automaticamente)
- O serviço de sandboxing na cloud deverá permitir consultar a informação enviada e avaliada e gerar os respetivos relatórios
- A tecnologia de Sandboxing tem que ser capaz de 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 desencriptar malware (unpacker) para utilização na análise estática e machine learning.
DNS
• A solução deve incluir um serviço de proteção DNS baseado na cloud que seja capaz de bloquear acesso a domínios maliciosos conhecidos e desconhecidos • Este serviço deve utilizar mecanismos de machine learning para detetar Domain Generated Algorithms (DGAs) e bloquear o acesso a estes • A solução deve permitir bloquear tráfego de C&C através do canal de DNS assim como detetar e bloquear o uso indevido deste canal para efetuar exfiltração de dados (DNS tunneling) • A funcionalidade de DNS Tunneling deve ser capaz de inspecionar o conteúdo dos pacotes de DNS • Este serviço deve permitir identificar qual as máquinas e utilizadores infetados, sem a necessidade de qualquer alteração na infraestrutura existente • A adição deste serviço não deve obrigar a qualquer alteração na infraestrutura de DNS do cliente • Para além da threat intelligence do fabricante, a solução deve utilizar informação proveniente de pelo menos 30 fontes distintas • Deve ser possível criar políticas simples que bloqueiem ou façam sinkholing aos pedidos de DNS maliciosos • A solução não deve necessitar de updates para estar atualizada e proteger contra as mais recentes ameaças • A solução deve permitir a aplicações de tags a máquinas comprometidas, de forma a ser possível criar uma política de acesso diferenciada para estas
SD-Wan
● A plataforma deve incluir um módulo de SD-WAN. ● A plataforma deve permitir adicionar um overlay de SD-WAN que permita escolher de forma inteligente e dinâmica os links mais apropriados para envio de tráfego. ● Deve ser possível criar regras de SD-WAN por aplicação e definir os requisitos mínimos para cada link. No caso de os requisitos mínimos não serem cumpridos pelo link em uso, deve ser feito o failover do tráfego automaticamente. ● Para os links deve ser possível monitorizar e definir regras com base em: latência, jitter e perda de pacotes. ● A plataforma deve permitir fazer load-sharing através de múltiplos links de forma a melhorar o aproveitamento da largura de banda disponível. ● As firewalls devem suportar a funcionalidade de zero-touch provisioning. ● A plataforma deve disponibilizar informação sobre a performance das aplicações e links. ● Esta funcionalidade deve ser gerida centralmente através de uma única consola ● Deve ser suportada a funcionalidade de Packet duplication, o que permite a um equipamento enviar o mesmo pacote em links diferentes. O equipamento que recebe ambos os pacotes deverá descartar o último a chegar. ● Deve ser suportada a funcionalidade de Forward Error Correction.
Relatórios & Logs
• 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 actividade 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 detectar 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 objectivo de manter os logs a largo prazo
- O repositório de logs externo, em hardware dedicado, deverá suportar cerca de 12 spares de 8TB RAID Certified HDD, para um máximo de 48 TB de armazenamento RAID.
- O repositório de logs externo deve ter a capacidade de armazenar e gerir os logs de até 25 firewalls.
- O repositório de logs externo deverá incluir:
  - Número de portas 1Gbit/s RJ45 >= 4
  - Número de portas Gigabit SFP+ 10Gbit/s >= 2
  - Fontes redundantes
- 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 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 enviada ao serviço de sandboxing e equipamentos internos comprometidos
- Capacidade de utilizar um motor integrado de correlação de eventos dentro da própria appliance de forma a que a partir dos logs criados se possa obter informações de alto nível.

Network 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 as 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)

AIOps

- A solução deve incluir um módulo de AIOps que utiliza os dados de telemetria das firewalls, e aos quais serão aplicados algoritmos de machine learning para produzir recomendações e detectar anomalias.
- A solução AIOps deverá ser totalmente cloud-based, sem necessidade de instalação de produtos adicionais.
- A solução deverá disponibilizar uma visão abrangente de ameaças detetas nas firewalls, assinaturas de segurança e tráfego de rede.
- A solução deverá prever e detetar anomalias e falhas de segurança nas configurações das firewalls, com base em machine learning.
- A solução deverá disponibilizar boas práticas de segurança recomendadas por forma a melhor a postura de segurança da organização.

• A solução deverá ter a capacidade de detetar problemas de hardware e de software. • A solução deverá, proativamente, corrigir e implementar boas práticas antes de serem submetidas alterações na política de segurança. • A solução deverá permitir planear upgrades com base nas versões de software instaladas. • Deverão ser enviadas notificações de alertas via email ou através da integração com o serviceNow. • Deverá permitir a criação fácil de tickets de suporte com apenas um clique para questões de sistema e operacionais.
Funcionalidades adicionais licenciáveis (o equipamento deverá ter a capacidade de no futuro suportar as seguintes funcionalidades de segurança através de licenciamento adicional):
Data Loss Prevention
• A plataforma deve disponibilizar um módulo completo de Data Loss Prevention • Esta funcionalidade deve ser disponibilizada como um serviço cloud que utilize supervised machine learning para identificar documentos sensíveis e atribuir-lhes uma categoria automaticamente como por exemplo: Financeiros, Legais, Saúde, informação pessoal,etc. A solução deverá também permitir controlar este tipo de documentos de forma evitar a sua exposição ou extravio • Este serviço deverá permitir proteger estes documentos das seguintes formas: • Prevenir o upload de ficheiros com informação confidencial e/ou sensível para aplicações web não permitidas pela organização • Monitorizar o upload de documentos para aplicações externas permitidas pela organização • O serviço deve disponibilizar out-of-the-box pelo menos 380 “data patterns” e deve também disponibilizar perfis que agrupam determinados padrões de forma a simplificar a criação de políticas. Por exemplo, deverá existir um perfil associado com o GDPR de forma a facilitar a monitorização de documentos que possam contêm informação pessoal de utilizadores • Deverão existir os seguintes perfis out-of-the-box: Bulk CCN, CCPA, Corporate FInancial docs, Financial information, GDPR, GLBA, Healthcare, Intellectual Property, Legal, Malware, Personally-Identifiable Information, Profanity, Self Harm e Sensitive content • A solução deverá ser constantemente atualizada com novos padrões e perfis • De forma a melhorar o rácio de detecção e eliminar falsos positivos a solução deverá permitir especificar: proximity keywords, níveis de confiança e expressões regulares básicas ou “weighted” • Este serviço deve poder ser consumido por diferentes plataformas do fabricante, nomeadamente, firewalls, serviço SASE(Secure Access Service Edge), CASB(Cloud Access Security Broker) e CSPM(Cloud Security Posture Management). Isto permitirá aplicar políticas de DLP transversais à organização
IOT
• A plataforma deve disponibilizar um serviço cloud de segurança para dispositivos IOT. • A firewall deve colecionar metadados do tráfego de rede dos dispositivos IoT, gerar logs com estas informações e enviá-los para um Data Lake na Cloud. O Serviço de IOT deve ter capacidade de analisar estes metadados através de um motor patenteado baseado em algoritmos de inteligência artificial e machine learning para detetar e identificar os dispositivos IoT e OT na rede. • A identificação de dispositivos não se deve basear em fingerprinting, como por exemplo identificação de MAC addresses. • O motor de identificação deve possuir 3 níveis: identificação da categoria do dispositivo (ex: camara de vigilancia), identificação do seu perfil (ex: fabricante, modelo e versão) e identificação de cada instância do dispositivo • Após a identificação dos dispositivos, a solução deve criar um padrão de comportamento para cada um e detetar automaticamente comportamentos anormais que possam sugerir que o dispositivo está comprometido. Para este tipo de eventos, devem ser gerados alertas no dashboard da solução. Deve ser possível receber estes alertas via email e sms também. • Quando é observado um comportamento anormal a solução deve sugerir automaticamente políticas de segurança a aplicar na firewall que permitam o correto funcionamento do dispositivo, mas bloqueie qualquer ligação anormal. • A firewall deve permitir a criação de regras baseadas em tipos de dispositivos que devem ser identificados através da marca, modelo e versão. Não sendo assim necessário criar regras com base em IPs ou zonas. • Este serviço deve observar mais de 200 parâmetros nos metadados do tráfego de rede, incluindo parâmetros de DHCP (option 55), HTTP user agent IDs, protocolos, headers dos protocolos,etc. • O serviço deve identificar vulnerabilidades presentes no software a correr nos respetivos dispositivos e diferenciar entre dispositivos vulneráveis e potencialmente vulneráveis. O serviço deve identificar vulnerabilidades de

software assim como vulnerabilidades associadas os uso/configuração incorreta dos mesmos. Exemplo: uso de credenciais default. • Deve existir a possibilidade do Data Lake ser utilizado para outro conjunto de use cases através de licenciamento adicional, nomeadamente: NTA (Network Traffic Analysis), UEBA (User Entity Behavior Analytics), shadow IT e integração com CASB(Cloud Access Security Broker). • O repositório de dados, na cloud, com capacidade de armazenamento de logs de 1 TB.

II. Cluster de Firewall Tipo 2 – Serviços de VPN (2 nós)

Requisitos de Segurança da Autoridade Nacional de Segurança (GNS)	• O fabricante do equipamento deverá cumprir as deliberações da Comissão de Avaliação de Segurança nomeadamente os critérios objetivos de segurança, assim como o seu âmbito técnico de aplicação, que justificam e fundamentam medidas destinadas a garantir um elevado nível comum de segurança da informação na União Europeia

Requisitos Mínimos Por nó de Cluster

Característica base	
Número de portas 1G/2.5G/5G/10 Gbit/s RJ45	>= 12
Número de portas Gigabit SFP+ 10 Gbit/s	>= 10
Número de portas Gigabit SFP28 25 Gbit/s	>= 4
Porta de gestão dedicada "Out of Band"	Sim
Número de portas de alta disponibilidade 1Gbit/s	>= 2
Número de portas de alta disponibilidade 10 Gbit/s SFP+	>= 1
Porta USB	>= 1
Disco rígido SSD	>= 480GB
A appliance de FW deverá ter uma arquitectura com recursos de hardware dedicados e independentes entre os serviços de gestão e os serviços de inspeção	Obrigatório
Garantido que a appliance de FW quando gerida localmente e perante uma sobrecarga dos serviços de inspeção de tráfego não afecte de forma alguma a performance dos serviços de gestão e vice-versa.	Obrigatório
Fontes de alimentação redundantes.	Obrigatório
Performance	
● Performance da apiance com a funcionalidade de firewall com identificação e controle de aplicações (inspeção L7 de todo o tráfego	>= 14 Gbps
● Performance da appliance com as funcionalidades IDS/IPS, Antivírus e Anti-Spyware, DNS Security, URL Filtering e Sandboxing	>= 7,5 Gbps
● Performance da appliance com a funcionalidade de VPN IPSec	>= 6,6 Gbps
● Número de novas sessões por segundo >= 145 000	>= 145 000
● Número máximo de sessões	>= 1 400 000

Especificações técnicas das Subscrições

Gestão Centralizada:

- 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
- Na gestão centralizada deve ser possível gerir até 25 firewalls num único servidor de gestão
- 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 a 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 utilizador ou grupo
- Capacidade de realizar policy based routing através do tipo de aplicação
- Suporte de arquitecturas 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 desencriptar 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

Funcionalidades Gerais de Segurança:

- Possibilidade de agrupar interfaces da appliance em conjuntos independentes, formando diferentes zonas de segurança

- Possibilidade de definir a política de segurança por zonas de segurança, podendo incluir na mesma política várias zonas de origem e/ou destino para a análise de tráfego e processamento de regras de segurança
- Possibilidade de criar múltiplas regras de segurança entre zonas de origem e destino
- Capacidade de identificação de aplicações em L7 com um mínimo de 2400 aplicações identificadas
- Capacidade de identificação de subfunções dentro de uma aplicação
- Capacidade de aplicar e/ou excecionar qualquer das funcionalidades de inspeção (IPS, Antivírus, etc) apenas ao tráfego de determinadas aplicações L7
- Possibilidade de agrupar aplicações por categorias de forma que as políticas de segurança sejam aplicadas por categorias de aplicações
- Possibilidade de identificar as aplicações quando estas não utilizam os portos TCP/UDP por defeito em qualquer tipo de tráfego/protocolo e não somente HTTP
- Possibilidade de identificar aplicações proprietárias que usem os protocolos HTTP e TCP
- Possibilidade de identificar aplicações que sejam transportadas em túneis encriptados SSL
- Capacidade de decifrar tráfego SSH e 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 assianturas baseadas em payloads do tráfego malicioso que permitam detetar tráfego C&C mesmo que o host C&C seja desconhecido ou mude constantemente

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 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.

Sandboxing e protecção Zero Day:

- Possibilidade de disponibilizar um serviço na cloud capaz de analisar ficheiros do tipo desconhecido ou links recebidos em e-mails, de forma que se permita o envio desta informação para análise atendendo aos critérios: Tipo de aplicação utilizada para transferir o ficheiro, tipo de ficheiro que está a ser transferido, direção da transferência (download ou upload)
- Perante uma análise por parte do serviço de Sandboxing na cloud que categoriza a informação enviada como maliciosa, deverão ser criadas assinaturas num prazo máximo de 5 minutos que possam ser utilizadas nos motores de Antivírus e URLF e que as descargas posteriores do mesmo ficheiro ou links sejam imediatamente bloqueadas (desta forma o malware desconhecido é transformado em malware conhecido automaticamente)
- O serviço de sandboxing na cloud deverá permitir consultar a informação enviada e avaliada e gerar os respetivos relatórios
- A tecnologia de Sandboxing tem que ser capaz de 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 desencriptar malware (unpacker) para utilização na análise estática e machine learning.

DNS:

- A solução deve incluir um serviço de proteção DNS baseado na cloud que seja capaz de bloquear acesso a domínios maliciosos conhecidos e desconhecidos
- Este serviço deve utilizar mecanismos de machine learning para detetar Domain Generated Algorithms (DGAs) e bloquear o acesso a estes
- A solução deve permitir bloquear tráfego de C&C através do canal de DNS assim como detetar e bloquear o uso indevido deste canal para efetuar exfiltração de dados (DNS tunneling)
- A funcionalidade de DNS Tunneling deve ser capaz de inspecionar o conteúdo dos pacotes de DNS
- Este serviço deve permitir identificar qual as máquinas e utilizadores infetados, sem a necessidade de qualquer alteração na infraestrutura existente
- A adição deste serviço não deve obrigar a qualquer alteração na infraestrutura de DNS do cliente
- Para além da threat intelligence do fabricante, a solução deve utilizar informação proveniente de pelo menos 30 fontes distintas
- Deve ser possível criar políticas simples que bloqueiem ou façam sinkholing aos pedidos de DNS maliciosos
- 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

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.

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.

Solução de 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 caractisticas 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 efectuando 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 modulo de identificação tem que obrigatoriamente ser capaz de identificar os seguintes parâmetros do equipamento que está 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 politicas baseadas em identidades.

Acessos VPN:

- Suporte de IKEv1 e IKEv2
- Suporte de criptografia para 3DES e AES-256 para IKE Phase I e II IKEv2
- Suporte de pelo menos os seguintes grupos de Diffie-Hellman: Group 1, Group 2, Group 5, Group 14, Group 19 and Group 20

- IKE Phase2 - Encriptação de dados (DES, 3DES, AES-128, AES-192, AES-256) e suporte de integridade dos dados (MD5, SHA1, SHA256, SHA384, SHA512)
- VPNs Site to Site: Full Mesh (all to all) ou Star (Remote to center)
- Suporte de IKE com PKI e pre-shared Secret
- Aprovisionamento automático de VPNs site-to-site
- Gestão automática de túneis IPSec de backup
- Suporte de routing dinâmico em VPN IPSec
- Clientes VPN para Windows, MacOS e iOS, Android
- Suporte de OTP para VPN sem recurso a terceiros fabricantes ou servidores adicionais
- Aplicação de políticas e restrições de acesso por utilizador ou por grupo de utilizadores
- Single Sign On VPN
- Portal HTML5 para maior compatibilidade com todo tipo de dispositivos
- Administração a partir da consola central

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 actividade 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 detectar 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 objectivo 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 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 enviada ao serviço de sandboxing e equipamentos internos comprometidos
- Capacidade de utilizar um motor integrado de correlação de eventos dentro da própria appliance de forma a que a partir dos logs criados se possa obter informações de alto nível.

Network 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 as 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)

Outras Funcionalidades:

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

- Possibilidade de decifrar tráfego SSL e SSH de forma que se possa estabelecer políticas de desencriptação baseadas em: zonas por onde passa o tráfego, IP de origem ou destino, utilizadores geram esse tráfego, portos utilizados
- Capacidade de criar exceções à desencriptação para determinado tipo de tráfego
- Capacidade de decifrar tráfego com destino a sites web que utilizam certificados de curva elíptica (ECC)
- Possibilidade de enviar tráfego após desencriptação para uma interface de port mirror para análise de terceiras partes
- Capacidade de capturar tráfego em formato pcap, podendo ser estabelecido como critérios de captura do tráfego, uma determinada aplicação independentemente da origem ou destino desse tráfego
- Capacidade de capturar tráfego em formato pcap exclusivamente quando se detecta um vírus ou um ataque em qualquer um dos motores de proteção

AIOps:

- A solução deve incluir um módulo de AIOps que utiliza os dados de telemetria das firewalls, e aos quais serão aplicados algoritmos de machine learning para produzir recomendações e detectar anomalias.
- A solução AIOps deverá ser totalmente cloud-based, sem necessidade de instalação de produtos adicionais.
- A solução deverá disponibilizar uma visão abrangente de ameaças detetas nas firewalls, assinaturas de segurança e tráfego de rede.
- A solução deverá prever e detetar anomalias e falhas de segurança nas configurações das firewalls, com base em machine learning.
- A solução deverá disponibilizar boas práticas de segurança recomendadas por forma a melhor a postura de segurança da organização.
- A solução deverá ter a capacidade de detetar problemas de hardware e de software.
- A solução deverá, proativamente, corrigir e implementar boas práticas antes de serem submetidas alterações na política de segurança.
- A solução deverá permitir planear upgrades com base nas versões de software instaladas.
- Deverão ser enviadas notificações de alertas via email ou através da integração com o serviceNow.
- Deverá permitir a criação fácil de tickets de suporte com apenas um clique para questões de sistema e operacionais.

Funcionalidades adicionais licenciáveis (o equipamento deverá ter a capacidade de no futuro suportar as seguintes funcionalidades de segurança através de licenciamento adicional):

Data Loss Prevention:

- A plataforma deve disponibilizar um módulo completo de Data Loss Prevention
- Esta funcionalidade deve ser disponibilizada como um serviço cloud que utilize supervised machine learning para identificar documentos sensíveis e atribuir-lhes uma categoria automaticamente como por exemplo: Financeiros, Legais, Saúde, informação pessoal,etc. A solução deverá também permitir controlar este tipo de documentos de forma evitar a sua exposição ou extravio
- Este serviço deverá permitir proteger estes documentos das seguintes formas:

Prevenir o upload de ficheiros com informação confidencial e/ou sensível para aplicações web não permitidas pela organização
Monitorizar o upload de documentos para aplicações externas permitidas pela organização

- O serviço deve disponibilizar out-of-the-box pelo menos 380 “data patterns” e deve também disponibilizar perfis que agrupam determinados padrões de forma a simplificar a criação de políticas. Por exemplo, deverá existir um perfil associado com o GDPR de forma a facilitar a monitorização de documentos que possam contêm informação pessoal de utilizadores
- Deverão existir os seguintes perfis out-of-the-box: Bulk CCN, CCPA, Corporate FInancial docs, Financial information, GDPR, GLBA, Healthcare, Intellectual Property, Legal, Malware, Personally-Identifiable Information, Profanity, Self Harm e Sensitive content
- A solução deverá ser constantemente atualizada com novos padrões e perfis
- De forma a melhorar o rácio de detecção e eliminar falsos positivos a solução deverá permitir especificar: proximity keywords, níveis de confiança e expressões regulares básicas ou “weighted”
- Este serviço deve poder ser consumido por diferentes plataformas do fabricante, nomeadamente, firewalls, serviço SASE(Secure Access Service Edge), CASB(Cloud Access Security Broker) e CSPM(Cloud Security Posture Management). Isto permitirá aplicar políticas de DLP transversais à organização

IOT:

- A plataforma deve disponibilizar um serviço cloud de segurança para dispositivos IOT.
- A firewall deve colecionar metadados do tráfego de rede dos dispositivos IoT, gerar logs com estas informações e enviá-los para um Data Lake na Cloud. O Serviço de IOT deve ter capacidade de analisar estes metadados através de um motor patenteado baseado em algoritmos de inteligência artificial e machine learning para detetar e identificar os dispositivos IoT e OT na rede.
- A identificação de dispositivos não se deve basear em fingerprinting, como por exemplo identificação de MAC addresses.

• O motor de identificação deve possuir 3 níveis: identificação da categoria do dispositivo (ex: camara de vigilância), identificação do seu perfil (ex: fabricante, modelo e versão) e identificação de cada instância do dispositivo • Após a identificação dos dispositivos, a solução deve criar um padrão de comportamento para cada um e detetar automaticamente comportamentos anormais que possam sugerir que o dispositivo está comprometido. Para este tipo de eventos, devem ser gerados alertas no dashboard da solução. Deve ser possível receber estes alertas via email e sms também. • Quando é observado um comportamento anormal a solução deve sugerir automaticamente políticas de segurança a aplicar na firewall que permitam o correto funcionamento do dispositivo, mas bloqueie qualquer ligação anormal. • A firewall deve permitir a criação de regras baseadas em tipos de dispositivos que devem ser identificados através da marca, modelo e versão. Não sendo assim necessário criar regras com base em IPs ou zonas. • Este serviço deve observar mais de 200 parâmetros nos metadados do tráfego de rede, incluindo parâmetros de DHCP (option 55), HTTP user agent IDs, protocolos, headers dos protocolos, etc. • O serviço deve identificar vulnerabilidades presentes no software a correr nos respetivos dispositivos e diferenciar entre dispositivos vulneráveis e potencialmente vulneráveis. O serviço deve identificar vulnerabilidades de software assim como vulnerabilidades associadas os uso/configuração incorreta dos mesmos. Exemplo: uso de credentials default. • Deve existir a possibilidade do Data Lake ser utilizado para outro conjunto de use cases através de licenciamento adicional, nomeadamente: NTA (Network Traffic Analysis), UEBA (User Entity Behavior Analytics), shadow IT e integração com CASB(Cloud Access Security Broker). • O repositório de dados, na cloud, com capacidade de armazenamento de logs de 1 TB.

SERVIÇOS DE INSTALAÇÃO E CONFIGURAÇÃO A INCLUIR EM TODAS AS TIPOLOGIAS DE FIREWALL	
• Serviço de Instalação e Configuração Clusters Firewalls com instalação na infraestrutura existente.	Chave-na-mão

Serviço de operacionalização on site para aplicações críticas (incluindo manutenção de todo o software proposto) para 12 Meses 24x7	
• Nível de Serviço	24x7
• Tempo de resposta	4 horas
• Tempo de resposta para incidentes críticos	30 minutos
• Solução de suporte que permita a abertura automática de chamadas, no caso de incidentes de falha ou pré-falha de algum componente de hardware	Sim
• Os serviços de reparação deverão ser realizados apenas por técnicos de equipas residentes em Portugal e devidamente credenciados pelo fabricante do equipamento	Sim
• A reparação de Hardware deverá apenas ser realizada com peças genuínas do fabricante dos equipamentos	Sim
• Deverá ser disponibilizado um portal/ferramenta que permita uma visão global e em tempo real do estado de suporte de todos os equipamentos registados. Deverá também permitir a abertura de chamadas de suporte e o acompanhamento de todos os casos abertos	Sim
• Suporte disponibilizado sempre em português durante todo o horário de cobertura (24x7) e através de um único ponto de contacto para todo o tipo de incidentes de Hardware	Sim
• Deverá ser atribuído um responsável pela coordenação e planeamento das atividades de suporte preventivo e que, semanalmente, esteja presente em reuniões presenciais para apoio às ações proativas a serem executadas e a revisão de ações que estejam planeadas	Sim
• Declaração do fabricante onde conste o conhecimento técnico da infraestrutura e responsabilidade pela solução apresentada na proposta	Sim

Serviços Profissionais de Fabricante:
Toda a solução terá de estar coberta com garantia/suporte de fabricante A garantia/suporte tem de incluir: - Suporte remoto de fabricante 24x7 - Suporte a diagnóstico e acesso a todos os softwares updates - Acesso a portal de suporte do fabricante - Substituição avançada de hardware (inclui Chassis, power supplies, módulos, fans e transceivers) - Capacidade de abertura de casos diretamente no fabricante, sem ter de recorrer a qual processo que envolva terceiras partes - Duração mínima de 3 anos (com data de início de garantia/suporte a coincidir com a data de início de projeto) - Serviços de consultoria de Fabricante

Secção II – Instalação, Configuração, Manutenção

1. **Nos valores a apresentar, devem estar previstos os seguintes trabalhos de instalação e configuração:**
   i. Plano de projeto detalhado, incluindo metodologia de gestão de projeto, plano de trabalhos, mecanismos de acompanhamento e entregáveis de projeto, tendo em consideração os elementos a entregar pelo ADJUDICATÁRIO;
   ii. O projeto de instalação deverá ter os seguintes milestones:
      a) Atribuição de um gestor de projeto dedicado
      b) Recolha de informação relacionada com o ambiente de produção;
      c) Elaboração e desenvolvimento da arquitetura técnica e funcional a implementar, com recomendações de melhorias e melhores práticas
      d) Planeamento de execução de tarefas para implementação da solução
      e) Elaboração do High Level Design e Low Level Design
      f) Planeamento de tarefas para testes de aceitação e validação da solução implementada
      g) Instalação física de todos os componentes em rack (é obrigatório o fornecimento de todo o material por forma a garantir a instalação física dos equipamentos e sua interligação à estrutura de switching)
      h) Updates e upgrades para versões de software recomendadas
      i) Testes de failover (redundância física e lógica)

j) Configuração dos novos equipamentos de acordo com o planeado em sede de projeto
k) Migração dos serviços para os novos equipamentos (devido à criticidade das aplicações, deverá ser feito em várias fases para diminuir probabilidade de riscos associados à migração)
l) Testes de aceitação em cada uma das fases da migração
m) Acompanhamento da solução implementada por, pelo menos, 12 meses após o fecho do projeto
n) Todos os trabalhos de planeamento, instalação, configuração, migração e testes têm de ser realizados on-site
o) Entrega de documentação do projeto, passagem de conhecimento, e formação certificada pelo fabricante a 2 elementos da equipa da SPMS
p) Relatório com todas as configurações da solução;

iii. Todas as tarefas que impliquem paragem de serviços ou indisponibilidade de recursos IT críticos da SPMS devem ser obrigatoriamente contempladas fora do horário normal de trabalho, ou seja, após as 20h.

2. Nos valores a apresentar, deve estar prevista garantia nos seguintes termos:

i. Prazo de mínimo de 3 (três) anos a contar da data de entrega dos equipamentos.

III. FORMA DA CONSULTA

É imperativo que a consulta preliminar ao mercado seja conduzida com transparência e não haja tratamento desigual de operadores económicos, conforme dispõe o artigo 35.º-A do Código dos Contratos Públicos.

Tendo em conta a prossecução destes princípios, a informação da consulta preliminar é publicitada no portal Internet público da SPMS, da qual faz parte integrante o presente documento, em: http://www.spms.min-saude.pt e no respetivo LinkedIn.

IV. PRESTAÇÃO DE INFORMAÇÃO PELOS OPERADORES ECONÓMICOS

A prestação voluntária de informação pelos operadores económicos, deverá ser efetuada para o correio eletrónico consulta.preliminar@spms.min-saude.pt até à data-limite de 26 de julho de 2024, devendo os

interessados indicar claramente no assunto do email a referência **"Consulta Preliminar n.º 12/2024 – "Equipamentos de Firewall".**

V. INFORMAÇÃO PRETENDIDA

A informação a prestar voluntariamente pelos operadores económicos, considerada por eles como oportuna e relevante, é a seguinte:

- Informação do equipamento, serviço ou do seu portefólio, com os detalhes que considerar relevante para o objeto da consulta preliminar;
- Os operadores económicos deverão apresentar o ficheiro Excel em anexo à presente Consulta Preliminar, devidamente preenchido.

VI. PRAZO DA CONSULTA

A informação prestada pelos operadores económicos será aceite até à data de **26/07/2024.**