CONSULTA PRELIMINAR AO MERCADO DAG/DIRS 13/2024

Equipamentos de Firewall – Perímetro e Gestão

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 – Perímetro – Gama Alta

b) 1 Cluster de Firewall Tipo 1 – Perímetro – Gama Média

c) 1 Cluster de Firewall Tipo 2– Gestão

d) Serviços de Instalação, configuração das plataformas a concurso

e) 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), b) e c)

f) 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), b) e c)

Quantidades de equipamento a adquirir

I	**Cluster de Firewall Tipo 1 – Perímetro – Gama Alta**	1
ii	**Cluster de Firewall Tipo 1 – Perímetro – Gama Media**	1
iii	**Cluster de Firewall Tipo 2 - Gestão**	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, ii, e iii**	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, ii, e iii**	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 Perimetro

Mapa de Quantidades

Descrição	Quantidade
Appliance de Segurança em alta disponibilidade (HA) (1 Cluster) Next Generation Firewalls – Tipo 1 – Gama Alta	2 (1 Cluster)
40GE QSFP+ transceiver, short range BiDi 40GE QSFP+ transceiver module, short range BiDi for systems with QSFP+ Slots	4
10GE SFP+ transceiver module, short range 10GE SFP+ transceiver module, short range for systems with SFP+ and SFP/SFP+ slots	4
Appliance de Segurança em alta disponibilidade (HA) (1 Cluster) Next Generation Firewalls - Tipo 2 – Gama Média	2(1 Cluster)
10GE SFP+ transceiver module, short range 10GE SFP+ transceiver module, short range for systems with SFP+ and SFP/SFP+ slots	4
Plataforma de Logging & Reporting	1
Plataforma de Management	1
Licenciamento, a 36 meses, que garanta (sem limitações) a disponibilidade de todas as features definidas no ponto 2 do CE (Bens e Serviços a Fornecer)	2

Características Técnicas dos Equipamentos

I.	**Cluster de Firewall Tipo 1 – Perímetro – Gama Alta (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	
• Hardware Accelerated 100 GE QSFP28 / 40 GE QSFP+ Slots	6
• Hardware Accelerated 25 GE SFP28 / 10 GE SFP+ / GE SFP Slots (include 2 X HA Slots)	16
• Hardware Accelerated 10 GE / 5 GE / 2.5 GE / GE RJ45 Ports	16
• 10GE/ GE RJ45 Management Ports	2
• USB Ports (Client / Server)	1
• Console Port	1
• Included Transceivers	2x SFP+ (SR 10 GE)
Sistema	
• TPM (trusted platform Module)	Include
• Onboard Storage	2x 1TB SSD
Desempenho	
• Aceleração do tráfego de Firewall e IPSec por ASIC	Hardware dedicado
• Aceleração de tráfego NGFW por ASIC	Hardware dedicado
• Firewall ThroughputIPv4 (pacotes UDP 1518 / 512 / 64 byte)	397 / 389 / 221 Gbps
• Firewall ThroughputIPv6 (pacotes UDP 1518 / 512 / 64 byte)	397 / 389 / 221 Gbps
• Latência de firewall (pacotes UDP de 64 bytes)	3.92µs
• Débito firewall (pacotes por segundo)	331.5 Mpps
• Sessões TCP concorrentes	70 Milhões
• Novas sessões/segundo (TCP)	870.000
• Politicas de firewall	200 000
• Débito VPN IPSec (pacotes 512 bytes)	105 Gbps
• Túneis IPsec Gateway-to-Gateway	40 000
• Túneis IPSec cliente remoto	200 000
• Débito VPN SSL	11 Gbps
• VPN SSL - Máximo RECOMENDADO de utilizadores simultâneos	30 000
• Débito IPS	36 Gbps
• Débito de inspeção SSL (IPS, avg HTTPS)	29 Gbps
• Débito de inspeção SSL (IPS, avg HTTPS) para sessões concorrentes	7.5Milhões
• Débito de Application Control	115 Gbps
• Débito NGFW	34 Gbps
• Débito Threat Protection	33 Gbps
• Domínios Virtuais (Default / Maximum)	10 / 500
• Máximo de Tokens	20.000
• Licenciamento ilimitado de utilizadores	SIM
• Alta-disponibilidade	Active-Active, Active-Passive, Clustering
Energia e Alimentação	
• Alimentação AC	100–240V AC, 50–60 Hz
• Consumo de energia médio	>= 425 W
• Consumo de energia máximo	<= 680 W
• Dissipação Térmica	<=2356 BTU/h
• Fonte de alimentação redundante hot-swappable	SIM

Condições ambientais	
• Temperatura de funcionamento	0 - 40 °C
• Humidade	5 a 90% sem condensação
• Compliance	FCC Part 15 Class A, RCM, VCCI, CE, UL/cUL, CB
• Certificações	USGv6/IPv6
Dimensões	
• Altura	88.9 mm (2RU)
• Largura	<=443 mm
• Profundidade	5<=56 mm
• Peso	< =17.5 KG

II. Cluster de Firewall Tipo 1 – Perímetro – Gama Média (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	
• Hardware Accelerated GE RJ45 Ports	16
• Hardware Accelerated GE SFP Slots	8
• Hardware Accelerated 25 GE SFP28 / 10 GE SFP+ / GE SFP Slots	12
• Hardware Accelerated 100 GE QSFP28 / 40 GE QSFP+ Slots	4
• GE RJ45 Management Ports	2
• 10 GE SFP+ / GE SFP HA Slots	2
• USB 3.0 Port	1
• Console RJ45 Port	1
• Included Transceivers para HA	2x SFP+ (SR 10GE)
Sistema	
• Trusted Platform Module (TPM)	Sim
• Onboard Storage	2x 1 TB NVMe SSD
Desempenho	
• Aceleração do tráfego de Firewall e IPSec por hardware	Hardware dedicado
• Aceleração de tráfego NGFW por hardware	Hardware dedicado
• Débito firewall IPv4 (pacotes UDP de 1518 / 512 / 64 bytes)	198 / 197 / 140 Gbps
• Débito firewall IPv6 (pacotes UDP de 1518 / 512 / 64 bytes)	198 / 197 / 140 Gbps
• Latência de firewall (pacotes UDP de 64 bytes)	3.22 µs
• Débito firewall (pacotes por segundo)	210 Milhões
• Sessões TCP concorrentes	12 Milhões
• Novas sessões/segundo (TCP)	750.000

• Politicas de firewall	100.000
• Débito VPN IPSec (pacotes 512 bytes)	55 Gbps
• Túneis IPsec Gateway-to-Gateway	20.000
• Túneis IPSec cliente remoto	100.000
• Débito VPN SSL	11 Gbps
• VPN SSL - Máximo RECOMENDADO de utilizadores simultâneos	10.000
• Débito de inspeção SSL	12 Gbps
• Débito de Application Control	34 Gbps
• Débito IPS	22 Gbps
• Débito NGFW	17 Gbps
• Débito Threat Protection	15 Gbps
• Domínios Virtuais (base / máximo)	10 / 250
• Máximo de Tokens	20.000
• Alta-disponibilidade	Active-Active, Active-Passive, Clustering
• Licenciamento ilimitado de utilizadores	SIM
Energia e Alimentação	
• Alimentação AC	100–240V AC, 50–60 Hz
• Consumo de energia médio	<= 420 W
• Consumo de energia máximo	<= 465 W
• Dissipação Térmica	<= 1600 BTU/h
• Fonte de alimentação redundante hot-swappable	Sim / Hot Swappable
Condições ambientais	
• Temperatura de funcionamento	0 - 40 °C
• Humidade	5 a 90% sem condensação
• Compliance	FCC Part 15 Class A, RCM, VCCI, CE, UL/cUL, CB
• Certificações	USGv6/IPv6
Dimensões	
• Altura	88.4 mm (2RU)
• Largura	<= 450 mm
• Profundidade	<= 560 mm
• Peso	<= 13.8 KG

As duas tipologias de firewalls propostas têm de cumprir com os seguintes requisitos adicionais e obrigatórios:

Integração com redes de comunicações

• Servidor de DHCP, NTP e DNS incluído
• Funcionalidade de DNS Proxy
• Múltiplos modos de configuração de interfaces:
  ○ Sniffer
  ○ Agregação de portas (802.3ad)
  ○ Loopback
  ○ VLANs (802.1Q e 802.1AD)
  ○ Software switch
  ○ VLAN Switch
• Suporte a múltiplos DDNS por interface.
• Routing estático e baseado em políticas (PBR - Policy Based Routing)
• SD-WAN
  ○ Application Awareness & Steering (3000+ Applications Supported)
  ○ Dynamic WAN Path Controller
  ○ NGFW with SSL Inspection

- Dynamic failover times
- Secure VPN Overlays
- Single Management Console for Security & SD-WAN
- Zero-touch provisioning
- Tráfego Multicast por regra SD-WAN
- Route Tagging

- Balanceamento e redundância de múltiplos links;
- Suporte para protocolos de routing dinâmico: RIPv1, RIPv2, RIPng, OSPFv2 e OSPFv3, ISIS, BGP4+
- Suporte de tráfego multicast: PIM, sparse e dense mode
- Routing baseado em conteúdos: WCCP e ICAP
- Proxy explícito com suporte PAC e WPAD
- Suporte a proxy explicito seguro para ligações HTTPS entre cliente e servidor.
- Suporte de IPv6
  - Gestão por IPv6
  - Protocolos de routing dinâmico com suporte para IPv6
  - Tunneling de IPv6
  - Processamento firewall e UTM de IPv6
  - NAT64
  - NAT46
  - VPN IPSec IPv6
- Suporte Dual Stack IPv4 e IPv6 em simultâneo
- Controlador Wireless integrado
- Controlador Switching integrado
- Virtualização da solução em contextos.
- Conectores SDN (integração com soluções cloud)
- DNS, DNS over Quic, DNS over HTTP3, DNS over HTTPS e DNS over TLS

Identificação de utilizadores e dispositivos

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

Firewall

- Modos de operação NAT/route e transparente/bridge
- Agendamento de políticas:
  - recorrentes ou apenas uma vez
  - data de expiração
- Session helpers e ALGS: dcerpc, dns-tcp, dns-udp, ftp, H.323, MGCP, MMS, PMAP, PPTP, RAS, RSH, RTSP, SIP, TFTP, GTP-C, GTP-U, GTP-B, TNS (Oracle)
- Suporte para tráfego VoIP: SIP/H.323 /SCCP NAT traversal, RTP pinhole
- Suporte para diferentes tipos de protocolos: SCTP, TCP, UDP, ICMP, IP
- Visualização de políticas de forma global ou por pares de interfaces
- Definição de objetos para utilização em políticas incluindo: pré-definidos, customizados, agrupamento de objetos, tagging e definição de cor de objetos
- Definição de objetos de endereços de diferentes tipos: IP, Subnet, intervalo de IPs, Geografia e FQDN

- Utilização de objetos de serviços Internet (ex: Azure, Office365) com atualização automática das gamas de IP e portos com a possibilidade de pesquisar Ips e verificar em que categorias se inserem.
- Configuração de NAT: por política e tabela central de NAT
- Suporte de NAT: NAT64, NAT46, NAT estático, NAT dinâmico, PAT, Full Cone NAT, STUN
- Traffic shaping e QOS: shaping de tráfego partilhado por política, shapping por IP, largura de banda máxima e garantida, número máximo de ligações por IP, priorização de tráfego, suporte de Type of Service (TOS) e Differentiated Services (DiffServ)
- Processamento de tráfego de firewall IP4 e IPv6 feito em processador dedicado e desenhado para o efeito.
- Suporte para políticas em modo aprendizagem.
- Suporte Port Control Protocol (PCP), funcionando como servidor PCP.

VPN

- IPSEC VPN:
  - Suporte para peers remotos: clientes dialup compatíveis com IPSEC, peers com IP estático ou DNS dinâmico
  - Mecanismos de autenticação: certificados ou pre-shared key
  - IPSEC Phase 1 mode: aggressive e main (ID protection) mode
  - Opções de aceitação de peers: qualquer ID, ID específico, ID num grupo de utilizadores dialup
  - Suporte de IKEv1, IKEv2 (RFC 4306)
  - Suporte de IKE mode configuration (como servidor ou cliente), DHCP over IPSEC
  - Phase 1/Phase 2 Proposal encryption: DES, 3DES, AES128. AES192, AES256
  - Phase 1/Phase 2 Proposal authentication: MD5, SHA1, SHA256, SHA384, SHA512
  - Phase 1/Phase 2 Diffie-Hellman Group support: 1, 2, 5, 14
  - Suporte XAuth como cliente ou servidor
  - XAuth para clientes dialup: Server type option (PAP, CHAP, Auto), NAT Traversal option
  - Duração configurável da chave de encriptação IKE e da frequência do NAT traversal keepalive
  - Dead peer detection
  - Replay detection
  - Autokey keep-alive na Phase 2 SA
- Implementação de VPNs IPSEC nos seguintes modos: gateway-to-gateway, hub-and-spoke, full mesh, redundant-tunnel, terminação de VPNs em modo transparente
- Suporte ADVPN
- Suporte de configuração full-mesh VPN One-click
- Opções de configuração de VPNs IPSec: baseado em routing(route-based) ou baseado em políticas (policy-based)
- VPNs SSL
  - Portal de VPN SSL configurável: temas de cores, disposição, atalhos (bookmarks) mecanismos de ligação, download de cliente
  - Suporte para domínio de SSL VPN: permite a customização de múltiplos portais VPN SSL associados a grupos de utilizadores, incluindo URL do portal e desenho
  - Atalhos (bookmarks) com single sign-on: permite reutilizar um login anterior ou credenciais pré-definidas para aceder a recursos internos
  - Gestão de atalhos (bookmarks) pessoais
  - Gestão de utilizadores concorrentes
  - Controlo/limitação de múltiplos acessos VPN com as mesmas credenciais de acesso
  - Suporte de VPN SSL em modo web:
    - Para clientes remotos equipamentos apenas com um browser web
    - Disponibiliza suporte web para aplicações como: HTTP/HTTPS, FTP, Telnet, SMB/CIFS, SSH. VNC, RDP, Citrix
  - Suporte para VPN SSL em modo túnel:
    - Para acesso a partir de computadores que necessitam utilizar qualquer software do tipo cliente-servidor.
    - Disponível para MAC OSX, Windows, IOS, Android e Windows Mobile
  - Suporte para VPN SSL em modo port-forwarding:
    - Utiliza uma applet Java para permitir uma utilização alargada de aplicações do tipo cliente-servidor
  - Validação da integridade do dispositivo cliente e do sistema operativo;
  - Opção para limpeza de cache aquando do termino da sessão VPN SSL
  - Opção de utilização de desktop virtual que permite isolar a sessão VPN SSL no ambiente de trabalho do computador cliente
- Monitorização de VPNs IPSec e SSL com diferentes níveis de detalhe
- Suporte para outras VPNs como L2TP (modo cliente e servidor), L2TP over IPSec, PPTP e GRE over IPSec
- Processamento de tráfego de IPSec feito em processador dedicado e desenhado para o efeito.

ZTNA - Zero Trust Network Access

- Capacidade da Firewall de ser um proxy point de ZTNA com escalabilidade até 50 000 endpoints concorrentes
- Capacidade da Firewall de ser um enforcement point de ZTNA

- Capacidade de triar túneis TLS automáticos a partir do endpoint
- Validação da identidade do utilizador, da identidade do dispositivo, da postura de segurança do dispositivo e dos privilégios de acesso do utilizador antes de dar acesso às aplicações

IPS - Deteção e prevenção de intrusões

- Suporte de IPS com mais de 12000 assinaturas, deteção de anomalias nos protocolos, assinaturas customizadas, atualização manual ou automática das assinaturas (push ou pull), integração com enciclopédia de ameaças para melhor informação/visualização de ataques detetados
- Diferentes ações de IPS: monitorizar, bloquear, apagar sessão ou quarentena do IP de ataque com definição de duração
- Possibilidade de registo integral do pacote onde foi detetado o ataque
- Definição de diferentes perfis de IPS de forma manual ou baseada em filtro (severidade, alvo, sistema operativo, aplicação e/ou protocolo)
- Aplicação de perfis de IPS por política de firewall para maior flexibilidade
- Opção de excluir a aplicação de assinaturas de IPS especificas com base em IPs
- Proteção DoS sobre IPv4 e IPv6 com definições contra TCP Syn flood, TCP/UDP/SCTP port scan, ICMP sweep, TCP/UDP/ SCTP/ICMP session flooding (source/destination)
- Possibilidade de implementação de IDS em modo sniffer
- Possibilidade de criar novas assinaturas
- Possibilidade de incluir assinaturas específicas para proteção de comunicações e equipamentos em ambientes industriais

Controlo de aplicações

- Deteção de mais de 4150 aplicações distintas organizadas por categorias
- Definição de aplicações customizadas
- Controlo avançado de aplicações de IM e Facebook
- Definição de diferentes perfis de controlo de aplicações de forma manual ou baseada em filtro (categoria, popularidade, tecnologia, fabricante, risco e/ou protocolo)
- Aplicação de perfis de controlo de aplicações por política de firewall para maior flexibilidade
- Deteção de aplicações mesmo dentro de ligações proxy
- Diferentes ações de controlo de aplicações: bloquear, reset de sessão, monitorização ou aplicação de gestão de largura de banda
- Inspeção SSL (suporte para TLS 1.3, HTTP/3 e QUIC)

Proteção contra ameaças

- Possibilidade de inspeção aplicacional de tráfego encriptado por SSL, incluindo as seguintes funcionalidades: IPS, controlo de aplicações, anti-vírus, web filtering e DLP
- Capacidade de desencriptação de sessões SSL com cópia de tráfego desencriptado para um sistema externo
- Inspeção apenas de certificado SSL ou Inspeção deep-packet com técnicas MiTM
- Deteção e bloqueio de BOTNETs com base em listas de reputação de IPs globais;
- Excluir, de forma simples, a inspeção SSL de tráfego encriptado em determinadas categorias relevantes à manutenção da privacidade dos utilizadores
- Suporte de anti-vírus nos modos flow (pacote-a-pacote) e proxy (reconstrução de sessões)
- Suporte de inspeção de anti-vírus, em modo flow, nos seguintes protocolos: HTTP/HTTPS, SMTP/SMTPS, POP3/POP3S, IMAP/IMAPS, MAPI, FTP/SFTP, SMB, ICQ, YM, NNTP
- Suporte de anti-vírus em modo proxy, incluindo:
    - Suporte dos seguintes protocolos: HTTP/HTTPS, STMP/SMTPS, POP3/POP3S, IMAP/IMAPS, MAPI, FTP/SFTP, ICQ, YM, NNTP, SSH
    - Suporte para análise de ficheiros em sistema baseado na cloud (OS Sandbox)
    - Listas de ficheiros autorizados/negados
    - Opção de análise heurística
- Capacidade de integração com solução de Sandboxing (cloud ou on-premises) e capacidade de descarregar um relatório em PDF com o resultado da análise estática e dinâmica.
- Deteção de sites WEB (web filtering):
    - Suporte de diferentes mecanismos de deteção de sites WEB (proxy-based, flow-based and DNS)
    - Possibilidade de definição manual de filtros de sites com base em URL, conteúdo web e cabeçalho MIME
    - Categorização dinâmica em tempo real, baseada na cloud, com mais de 250 milhões de sites categorizados, de 70 idiomas e organizados em mais de 77 categorias
    - Opção para forçar a utilização de mecanismos de busca segura (safe search) disponibilizados pelos principais motores de busca, incluindo Google, Yahoo!, Bing & Yandex, e definição customizada de YouTube Education Filter

- Deverá ser possível ter a opção para activar as seguintes funcionalidades:
  - Filtrar Java Applet, ActiveX e/ou cookies
  - Bloquear HTTP Post
  - Registar termos/palavras utilizados nas pesquisas em motores de busca
  - Identificar imagens pelo URL
  - Bloquear redirect de HTTP de acordo com a categoria
  - Excluir, de forma simples, a inspeção SSL de tráfego encriptado em determinadas categorias relevantes à manutenção da privacidade dos utilizadores
  - Definição de quotas de utilização WEB com base em categorias
- Definição de categorias customizadas e sobreposição de categorização
- Mecanismos de exceção à utilização de perfis pré-definidos;

- Detecção e limitação de acesso a conteúdos video de forma granular (Video Filter)
  - Limitação a canais específicos
  - Filtragem de conteúdo adulto
- Mecanismos de deteção e mitigação de utilização de proxy-avoidance: Categorias de sites com proxy, pontar URLs por domínio e endereço IP, bloquear redirects de cache para sites com cache e tradução de sites, bloqueio de ligação a proxy com base em deteção de aplicação, bloqueio de tráfego com comportamento de proxy com base em assinaturas de IPS
- Prevenção e proteção de fugas de informação - DLP
- Suporte de protocolos na análise de mensagens: HTTP-POST, SMTP, POP3, IMAP, MAPI, NNTP
- Possibilidade de executar as acões: registar, bloquear, quarentena de utilizador/IP/Interface
- Filtros pré-difinidos incluindo cartões de crédito e número de segurança Social
- Suporte de protocolos na análise de ficheiros: HTTP-POST, HTTP=-GET,SMTP, POP3, IMAP, MAPI, FTP, NNTP
- Opções de filtro disponíveis: tipo de ficheiro, watermark, conteúdo e deteção de encriptação
- Utilização de mecanismos de DLP watermarking , com disponibilização de ferramentas gratuitas de watermarking para Windows e Linux
- Fingerprinting de ficheiros
- Armazenamento de ficheiros detetados para inspeção forense, incluindo: todo o conteúdo de e-mail, FTP, IM, NNTP e tráfego WEB
- Integração nativa com plataformas externas de filtragem de email, sandbox e WAF
- Feeds de ameaças por Domain Name e/ou IP Address

Controlo de Endpoints

- Visibilidade centralizada sobre diversos elementos de rede, nomeadamente:
  - Vulnerabilidades nos endpoints
  - Indicadores de compromisso

Alta disponibilidade

- Alta disponibilidade disponível nos modos: ativo-passivo, ativo-ativo, virtual-cluster, VRRP
- Interfaces de heartbeat redundantes
- Interfaces reservadas para gestão
- Sem custos de licenciamento para suporte de funcionalidades de alta-disponibilidade
- Reposição automática de serviço (failover)
  - Monitorização de portas e links (locais e remotos)
  - Sem perca de sessões
  - Failover em menos de 1 segundo
  - Notificações de eventos de failover
- Diferentes opções de arquitetura
  - HA com agregação de links
  - Full mesh HA
  - Suporte para HA com equipamentos geograficamente dispersos
- Opção de sincronização de sessões em equipamentos configurados em modo Standalone ou Cluster geográfico

Administração, Monitorização e Diagnósticos

- Acesso de gestão gráfica e texto: HTTPS com recurso a web browser
- Acesso de gestão em modo de texto: SSH, Telnet ou consola
- Capacidade de captura de tráfego em CLI e GUI com possibilidadde de análise em tempo real
- Sem necessidade de utilização de software cliente proprietário para gestão gráfica
- Suporte de múltiplas linguagens de administração no acesso gráfico, incluindo: português, inglês, espanhol, francês, japonês, chinês simplificado, chinês tradicional e coreano

- Suporte para gestão local e gestão centralizada em simultâneo
- Suporte para gestão centralizada com integração em plataforma específica para o efeito
- Integração com plataformas externas de gestão e monitorização, incluindo SNMP, sFlow, Syslog e Netflow
- Implementação rápida da solução incluindo mecanismos de auto instalação por USB, execução local e remota de scripts
- Visualização em tempo real do estado do equipamento através de interface gráfica (acesso HTTPS com recurso a web-browser) incluindo diversos conteúdos e funcionalidades.
- Integração com outras soluções (externas) através de scripts CLI e APIs.
- Wizards de configuração para implementação rápida da solução.
- Integração com soluções Openstack, VMWare NSX, e Cisco ACI.
- Automação, por exemplo para colocar em Quarentena um dispositivo com um elevado Indicador de Compromisso.
- Capacidade de backup para ficheiro em formato YAML
- Connectivity Fault Management (CFM)

Registo de eventos e relatórios

- Suporte para registo de eventos (logs) em diferentes repositórios, tais como: memória, disco rígido local, múltiplos servidores de syslog, múltiplos servidores específicos para registos de eventos e elaboração de relatórios, servidores do tipo WebTrends e plataformas disponíveis na cloud
- Opção de logging confiável com recurso a mecanismos TCP (RFC 5424)
- Encriptação de eventos para confidencialidade e integridade aquando da utilização de plataformas específicas;
- Possibilidade de exportar relatórios em formato PDF
- Calendarização de backups de logs para sistemas externos
- Registos detalhados de tráfego: tráfego enviado, bloqueado, sessões violadas, tráfego local, pacotes inválidos
- Organização de registos de acordo com a categoria: administração de sistema (para auditoria), routing e networking, VPN, autenticação de utilizadores, Wireless
- Opção para registo parcial ou completo de eventos
- Resolução de nomes de endereços IPs e protocolos
- Mecanismo nativo de visualização de eventos de forma estatisca, com ferramentas de busca e drill-down disponível através de recurso com web browser.
- Suporte ao envio de logs no formato JSON.

Certificações

- USGv6 IPv6 Certified

Plataforma Central de Gestão

Uma (1) plataforma, de virtualização, centralizada, do mesmo fabricante das Firewalls, que suporte as seguintes características.

• Interfaces total	4 x GE RJ45, 2 x SFP
• Porta de consola	1x RJ45
• Gestão de Devices	>=150
• Capacidade de armazenamento	32 TB (8 x 4 TB)
• GB/Dia de Logs	2GB
• Suportar Alta Disponibilidade	Sim
• Nível de RAID suportado	RAID 0/1,1s/5,5s/10
• Trusted Platform Module (TPM)	Sim
• Fonte de alimentação redundante e removíveis	Sim
• Consumo de energia médio	<=140W
• Consumo de energia máximo	<=190W
• Dissipação Térmica	<=630 BTU/h
•	

Domínios administrativos e políticas globais

Suporte obrigatório às seguintes funcionalidades:

- Permitir que o administrador principal crie grupos de firewalls para outros administradores poderem gerir e monitorizar:
  - Os administradores podem gerir firewalls no site central ou através de sites remotos
  - Multiplos contextos virtuais de firewall podem ser geridos por múltiplos contextos virtuais de administração
  - Atribuição de permissões de gestão a utilizadores por diferentes contextos virtuais de administração
  - Administradores têm acesso de gestão apenas aos contextos virtuais de firewalls assignados

- Criar modelos de configuração para novos firewalls
- Capacidade para configurar Políticas Globais

APIs JSON e XML (Serviços Web):
Suporte obrigatório às seguintes funcionalidades:
- Suporte para APIs:
  - JSON API - Permite MSSPs e grandes empresas criarem portais web personalizados para administração de políticas e objetos
  - XML API - Permite aos administradores automatizarem tarefas comuns, tais como provisionamento de novos firewalls e também configurações nos firewalls existentes

Gestão dos conteúdos de segurança aplicacional:
Suporte obrigatório às seguintes funcionalidades:
- Gestão dos conteúdos de segurança aplicacional permite ao administrador ter um maior controlo sobre as atualizações de segurança. Incluí suporte para o seguinte:
  - Atualizações de definições de antivírus
  - Atualizações de prevenção de intrusões
  - Atualizações de gestão de vulnerabilidades
  - Web Filtering
  - Antispam

Controlo e gestão:
Suporte obrigatório às seguintes funcionalidades:
- Gestão de firewalls e/ou agentes de endpoint individualmente ou em grupos lógicos
- Atualização do firmware dos firewalls
- Descobrir novos firewalls de forma automática
- Criação, implementação e monitorização de VPNs
- Delegar o controlo a diferentes utilizadores com diferentes permissões de administração
- Auditoria sobre as alterações de configuração efetuadas

Monitorização, Análise e Relatórios:
Suporte obrigatório às seguintes funcionalidades:
- Acesso às de rede e segurança
- Monitorização em tempo real e criação de relatórios básicos que fornecem visibilidade sobre a atividade da rede e dos utilizadores
- Possibilidade de integração com uma plataforma centralizada de logs e relatórios

Plataforma de Log e Reporting	
Uma (1) plataforma, de virtualização, centralizada, do mesmo fabricante das Firewalls, que suporte as seguintes características.	
• Interfaces total	4 x GE RJ45, 2 x SFP
• Porta de consola	1x RJ45
• Gestão de Devices/VDOMs (Máx)	>=800
• Capacidade de armazenamento	16TB (4x 4TB) 3.5 in SAS HDDs
• GB/Dia de Logs	200GB
• Suportar Alta Disponibilidade	Sim
• Nível de RAID suportado	RAID 0/1,1s/5,5s/10
• Trusted Platform Module (TPM)	Sim
• Fonte de alimentação redundante e removíveis	Sim
• Consumo de energia médio	<=120W
• Consumo de energia máximo	<=150W
• Dissipação Térmica	<=450 BTU/h
•	

Relatórios e Ferramentas de Visualização

Suporte obrigatório às seguintes funcionalidades:
- Visualização e filtragem dos Top Users utilização das VPNs
- Visualização dos endereços dos destinos, sites web e ameaças
- Deverá ter por omissão vários modelos de relatórios tipo
- Deverá disponibilizar mais de 60 templates de relatórios de base, incluíndo entre outros os seguintes relatórios:
- Secure SD-WAN, monitorização de VPN, análise de ameaças, indicadores de risco, consumo de largura de banda e aplicações, Compliance, UTM, tráfego
- Deverá permitir a customização, clonagem e modificação dos relatórios existentes, e calendarizar a execução de relatórios em horários determinados, e o envio automatizado de relatórios nos formatos PDF, HTML, CSV e XML
- Capacidade de monitorizar e alertar o administrador de TI sobre eventos importantes

- Capacidade de Importar/Exportar modelos de relatórios já criados em outra plataforma de Log & Reporting, do mesmo fabricante

APIs (Serviços Web):
Suporte obrigatório às seguintes funcionalidades:
- Suporte para APIs (REST API):
  - Permite MSSPs e grandes empresas manipularem os relatórios da plataforma de Log & Reporting, charts/datasets e objetos
  - Permite aos administradores aprovisionarem/configurarem a plataforma de Log & Reporting e gerar relatórios

Visualização de Logs:
Suporte obrigatório às seguintes funcionalidades:
- Visualização de Logs em tempo real ou por histórico
- Visualizar pelo tipo de tráfego ou por logs de segurança
- Visualizar pelo tipo de device, ADOM
- Filtragem de Logs
- Visualização de Logs de forma granular
- Apresentação dos Logs com pictogramas das bandeiras do países e aplicações

Gestão de Eventos:
Suporte obrigatório às seguintes funcionalidades:
- Criar alertas de forma simples
- Desencadear alertas consoante o nível de severidade, eventos específicos, por tipo de ações e destinos
- Definir vários limites pelo número de eventos por um determinado tempo
- Visualizar ou procurar alertas através do histórico
- Notificar por email, traps SNMP, envio eventos por syslog

DLP Archiving:
Suporte obrigatório às seguintes funcionalidades:
- Investigar arquivos DLP
- Suportar vários tipos de arquivo: email, HTTP, FTP, IM

IOC - Indicators of Compromise
Suporte obrigatório às seguintes funcionalidades:
- Capacidade de voltar a reanalisar eventos/logs do passado com novo conhecimento de ataques, sites maliciosos, IPs, ficheiros confirmadamente considerados maliciosos

Suporte obrigatório às seguintes funcionalidades:
- Capacidades de SIEM de forma a analisar, normalizar e correlacionar logs de produtos do fabricante e Security Event logs de hosts Windows e Linux
- Gestão de incidentes com automação via playbooks já pré-definidos ou criados pelo administrador

Outbreak Alert Service
Suporte obrigatório às seguintes funcionalidades:
- Receber automaticamente alertas de novos Outbreaks
- Criação automática de:
  - Template de Report específico para o novo Outbreak
  - Report sobre o estado actual do Outbreak
  - Gestor de eventos relevantes para o Outbreak

Firewall de Gestão

Mapa de Quantidades

Descrição	Quantidade
Appliance de Segurança em alta disponibilidade (HA) (1 Clusters) Next Generation Firewalls	2(1 Clusters)
10GE SFP+ transceiver module, short range 10GE SFP+ transceiver module, short range for systems with SFP+ and SFP/SFP+ slots	4

Licenciamento, a 36 meses, que garanta (sem limitações) a disponibilidade de todas as features definidas no pressente RFI (Bens e Serviços a Fornecer)	2
Identity and Access Management - 4x GE RJ45 ports, 2x 1 TB HDD. Base License supports up to 1500 users. Expand user support to 3500 users	3
Software one-time password tokens for iOS, Android and Windows Phone mobile devices. Perpetual licenses for 10 users. Electronic license certificate.	2
Licenciamento, a 36 meses, que garanta (sem limitações) a disponibilidade de todas as features definidas no pressente RFI (Bens e Serviços a Fornecer)	2

III. Cluster de Firewall Tipo 2 – Gestão (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	
• Hardware Accelerated GE RJ45 Ports	>=16
• Hardware Accelerated GE SFP Slots	>=8
• Hardware Accelerated 10GE SFP+ / GE SFP Slots	>=4
• Hardware Accelerated 25GE SFP28/10GE SFP+ Ultra Low Latency Slots	>=4
• GE RJ45 MGMT/HA Ports	>= 2
• USB Ports	>= 2
• RJ45 Console Port	>= 1
• Included Transceivers	>= 2x SFP (SX 1 GE)
• Onboard Storage	2x 240 GB SSD
Desempemho	
• Aceleração do tráfego de Firewall e IPSec por ASIC	Hardware dedicado
• Aceleração de tráfego NGFW por ASIC	Hardware dedicado
• Débito firewall IPv4/IPv6 (pacotes UDP 1518 /512 / 64 byte)	139 / 137.5 / 70 Gbps
• Latência de firewall (pacotes UDP de 64 bytes)	4,12µs/2,5µs in SFP28 (ULL) ports
• Débito firewall (pacotes por segundo)	>=105 Mbps
• Sessões TCP concorrentes	>=8 Milhões
• Novas sessões/segundo (TCP)	>=550 000
• Políticas de firewall	>=30 000
• Débito VPN IPSec (pacotes 512 bytes)	>=55Gbps
• Túneis IPsec Gateway-to-Gateway	>= 2 000
• Túneis IPSec cliente remoto	>=50 000
• Débito VPN SSL	>=4.3Gbps

• VPN SSL - Máximo RECOMENDADO de utilizadores simultâneos	>=10 000
• Débito IPS	>=14Gbps
• Débito de inspeção SSL	>=9Gbps
• Débito de inspeção SSL para sessões concorrentes	>=840 000
• Débito de Application Control	>=32Gbps
• Débito NGFW	>=11.5Gbps
• Débito Threat Protection	>=10.5Gbps
• Domínios Virtuais (Default / Maximum)	10 / 10
• Máximo de Tokens	>= 5000
• Licenciamento ilimitado de utilizadores	Sim
• Alta-disponibilidade	Active-Active, Active-Passive, Clustering
Energia e Alimentação	
• Alimentação AC	100–240V AC, 50–60 Hz
• Consumo de energia médio	<=175 W
• Consumo de energia máximo	<=260 W
• Dissipação Térmica	<=890 BTU/h
• Fonte de alimentação redundante hot-swappable	Sim
Condições ambientais	
• Temperatura de funcionamento	0 - 40 °C
• Humidade	5 a 90% sem condensação
• Compliance	FCC Part 15 Class A, RCM, VCCI, CE, UL/cUL, CB
• Certificações	USGv6/IPv6
Dimensões	
• Altura	44.45 mm (1RU)
• Largura	<=440 mm
• Profundidade	<=380 mm
• Peso	<=7,5 KG
Integração com redes de comunicações	
As seguintes funcionalidades deverão ser suportadas: ● Servidor de DHCP, NTP e DNS incluído ● Funcionalidade de DNS Proxy ● Múltiplos modos de configuração de interfaces: o Sniffer o Agregação de portas (802.3ad) o Loopback o VLANs (802.1Q e 802.1AD) o Software switch o VLAN Switch ● Suporte a múltiplos DDNS por interface. ● Routing estático e baseado em políticas (PBR - Policy Based Routing) ● SD-WAN o Application Awareness & Steering (3000+ Applications Supported) o Dynamic WAN Path Controller o NGFW with SSL Inspection o Dynamic failover times o Secure VPN Overlays o Single Management Console for Security & SD-WAN o Zero-touch provisioning o Tráfego Multicast por regra SD-WAN o Route Tagging ● Balanceamento e redundância de múltiplos links; ● Suporte para protocolos de routing dinâmico: RIPv1, RIPv2, RIPng, OSPFv2 e OSPFv3, ISIS, BGP4+ ● Suporte de tráfego multicast: PIM, sparse e dense mode ● Routing baseado em conteúdos: WCCP e ICAP ● Proxy explícito com suporte PAC e WPAD	

- Suporte a proxy explicito seguro para ligações HTTPS entre cliente e servidor.
- Suporte de IPv6
  - Gestão por IPv6
  - Protocolos de routing dinâmico com suporte para IPv6
  - Tunneling de IPv6
  - Processamento firewall e UTM de IPv6
  - NAT64
  - NAT46
  - VPN IPSec IPv6
- Suporte Dual Stack IPv4 e IPv6 em simultâneo
- Suporte VXLAN
- Suporte em VXLAN de MP-BGP EVPN
- Controlador Wireless integrado
- Controlador Switching integrado
- Virtualização da solução em contextos.
- Conectores SDN (integração com soluções cloud)
- DNS, DNS over Quic, DNS over HTTP3, DNS over HTTPS e DNS over TLS

Identificação de utilizadores e dispositivos
As seguintes funcionalidades deverão ser suportadas:

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

Firewall
As seguintes funcionalidades deverão ser suportadas:

- Modos de operação NAT/route e transparente/bridge
- Agendamento de políticas:
  - recorrentes ou apenas uma vez
  - data de expiração
- Session helpers e ALGS: dcerpc, dns-tcp, dns-udp, ftp, H.323, MGCP, MMS, PMAP, PPTP, RAS, RSH, RTSP, SIP, TFTP, GTP-C, GTP-U, GTP-B, TNS (Oracle)
- Suporte para trafego VoIP: SIP/H.323 /SCCP NAT traversal, RTP pinhole
- Suporte para diferentes tipos de protocolos: SCTP, TCP, UDP, ICMP, IP
- Visualização de políticas de forma global ou por pares de interfaces
- Definição de objetos para utilização em políticas incluindo: pré-definidos, customizados, agrupamento de objetos, tagging e definição de cor de objetos
- Definição de objetos de endereços de diferentes tipos: IP, Subnet, intervalo de IPs, Geografia e FQDN
- Utilização de objetos de serviços Internet (ex: Azure, Office365) com atualização automática das gamas de IP e portos com a possibilidade de pesquisar Ips e verificar em que categorias se inserem.
- Configuração de NAT: por política e tabela central de NAT
- Suporte de NAT: NAT64, NAT46, NAT estático, NAT dinâmico, PAT, Full Cone NAT, STUN
- Traffic shaping e QOS: shaping de tráfego partilhado por política, shapping por IP, largura de banda máxima e garantida, número máximo de ligações por IP, priorização de tráfego, suporte de Type of Service (TOS) e Differentiated Services (DiffServ)
- Processamento de tráfego de firewall IP4 e IPv6 feito em processador dedicado e desenhado para o efeito.
- Suporte para políticas em modo aprendizagem.
- Suporte Port Control Protocol (PCP), funcionando como servidor PCP.

VPN

As seguintes funcionalidades deverão ser suportadas:

- IPSEC VPN:
  - Suporte para peers remotos: clientes dialup compatíveis com IPSEC, peers com IP estático ou DNS dinâmico
  - Mecanismos de autenticação: certificados ou pre-shared key
  - IPSEC Phase 1 mode: aggressive e main (ID protection) mode
  - Opções de aceitação de peers: qualquer ID, ID específico, ID num grupo de utilizadores dialup
  - Suporte de IKEv1, IKEv2 (RFC 4306)
  - Suporte de IKE mode configuration (como servidor ou cliente), DHCP over IPSEC
  - Phase 1/Phase 2 Proposal encryption: DES, 3DES, AES128. AES192, AES256
  - Phase 1/Phase 2 Proposal authentication: MD5, SHA1, SHA256, SHA384, SHA512
  - Phase 1/Phase 2 Diffie-Hellman Group support: 1, 2, 5, 14
  - Suporte XAuth como cliente ou servidor
  - XAuth para clientes dialup: Server type option (PAP, CHAP, Auto), NAT Traversal option
  - Duração configurável da chave de encriptação IKE e da frequência do NAT traversal keepalive
  - Dead peer detection
  - Replay detection
  - Autokey keep-alive na Phase 2 SA
- Implementação de VPNs IPSEC nos seguintes modos: gateway-to-gateway, hub-and-spoke, full mesh, redundant-tunnel, terminação de VPNs em modo transparente
- Suporte ADVPN
- Suporte de configuração full-mesh VPN One-click
- Opções de configuração de VPNs IPSec: baseado em routing(route-based) ou baseado em politicas (policy-based)
- VPNs SSL
  - Portal de VPN SSL configurável: temas de cores, disposição, atalhos (bookmarks) mecanismos de ligação, download de cliente
  - Suporte para domínio de SSL VPN: permite a customização de múltiplos portais VPN SSL associados a grupos de utilizadores, incluindo URL do portal e desenho
  - Atalhos (bookmarks) com single sign-on: permite reutilizar um login anterior ou credenciais pré-definidas para aceder a recursos internos
  - Gestão de atalhos (bookmarks) pessoais
  - Gestão de utilizadores concorrentes
  - Controlo/limitação de múltiplos acessos VPN com as mesmas credenciais de acesso
  - Suporte de VPN SSL em modo web:
    - Para clientes remotos equipamentos apenas com um browser web
    - Disponibiliza suporte web para aplicações como: HTTP/HTTPS, FTP, Telnet, SMB/CIFS, SSH. VNC, RDP, Citrix
  - Suporte para VPN SSL em modo túnel:
    - Para acesso a partir de computadores que necessitam utilizar qualquer software do tipo cliente-servidor.
    - Disponível para MAC OSX, Windows, IOS, Android e Windows Mobile
  - Suporte para VPN SSL em modo port-forwarding:
    - Utiliza uma applet Java para permitir uma utilização alargada de aplicações do tipo cliente-servidor
  - Validação da integridade do dispositivo cliente e do sistema operativo;
  - Opção para limpeza de cache aquando do termino da sessão VPN SSL
  - Opção de utilização de desktop virtual que permite isolar a sessão VPN SSL no ambiente de trabalho do computador cliente
- Monitorização de VPNs IPSec e SSL com diferentes níveis de detalhe
- Suporte para outras VPNs como L2TP (modo cliente e servidor), L2TP over IPSec, PPTP e GRE over IPSec
- Processamento de tráfego de IPSec feito em processador dedicado e desenhado para o efeito.

ZTNA - Zero Trust Network Access

As seguintes funcionalidades deverão ser suportadas:

- Capacidade da Firewall de ser um proxy point de ZTNA com escalabilidade até 50 000 endpoints concorrentes
- Capacidade da Firewall de ser um enforcement point de ZTNA
- Capacidade de triar túneis TLS automáticos a partir do endpoint
- Validação da identidade do utilizador, da identidade do dispositivo, da postura de segurança do dispositivo e dos privilégios de acesso do utilizador antes de dar acesso às aplicações

IPS - Deteção e prevenção de intrusões

As seguintes funcionalidades deverão ser suportadas:

- Suporte de IPS com mais de 12000 assinaturas, deteção de anomalias nos protocolos, assinaturas customizadas, atualização manual ou automática das assinaturas (push ou pull), integração com enciclopédia de ameaças para melhor informação/visualização de ataques detetados
- Diferentes ações de IPS: monitorizar, bloquear, apagar sessão ou quarentena do IP de ataque com definição de duração
- Possibilidade de registo integral do pacote onde foi detetado o ataque
- Definição de diferentes perfis de IPS de forma manual ou baseada em filtro (severidade, alvo, sistema operativo, aplicação e/ou protocolo)
- Aplicação de perfis de IPS por política de firewall para maior flexibilidade
- Opção de excluir a aplicação de assinaturas de IPS especificas com base em IPs
- Proteção DoS sobre IPv4 e IPv6 com definições contra TCP Syn flood, TCP/UDP/SCTP port scan, ICMP sweep, TCP/UDP/ SCTP/ICMP session flooding (source/destination)

- Possibilidade de implementação de IDS em modo sniffer
- Possibilidade de criar novas assinaturas
- Possibilidade de incluir assinaturas específicas para proteção de comunicações e equipamentos em ambientes industriais

Controlo de aplicações

As seguintes funcionalidades deverão ser suportadas:

- Deteção de mais de 4150 aplicações distintas organizadas por categorias
- Definição de aplicações customizadas
- Controlo avançado de aplicações de IM e Facebook
- Definição de diferentes perfis de controlo de aplicações de forma manual ou baseada em filtro (categoria, popularidade, tecnologia, fabricante, risco, e/ou protocolo)
- Aplicação de perfis de controlo de aplicações por política de firewall para maior flexibilidade
- Deteção de aplicações mesmo dentro de ligações proxy
- Diferentes ações de controlo de aplicações: bloquear, reset de sessão, monitorização ou aplicação de gestão de largura de banda
- Inspeção SSL (suporte para TLS 1.3, HTTP/3 e QUIC)

Proteção contra ameaças

As seguintes funcionalidades deverão ser suportadas:

- Possibilidade de inspeção aplicacional de tráfego encriptado por SSL, incluindo as seguintes funcionalidades: IPS, controlo de aplicações, anti-vírus, web filtering e DLP
- Capacidade de desencriptação de sessões SSL com cópia de tráfego desencriptado para um sistema externo
- Inspeção apenas de certificado SSL ou Inspeção deep-packet com técnicas MiTM
- Deteção e bloqueio de BOTNETs com base em listas de reputação de IPs globais;
- Excluir, de forma simples, a inspeção SSL de tráfego encriptado em determinadas categorias relevantes à manutenção da privacidade dos utilizadores
- Suporte de anti-vírus nos modos flow (pacote-a-pacote) e proxy (reconstrução de sessões)
- Suporte de inspeção de anti-vírus, em modo flow, nos seguintes protocolos: HTTP/HTTPS, SMTP/SMTPS, POP3/POP3S, IMAP/IMAPS, MAPI, FTP/SFTP, SMB, ICQ, YM, NNTP
- Suporte de anti-vírus em modo proxy, incluindo:
  - Suporte dos seguintes protocolos: HTTP/HTTPS, STMP/SMTPS, POP3/POP3S, IMAP/IMAPS, MAPI, FTP/SFTP, ICQ, YM, NNTP, SSH
  - Suporte para análise de ficheiros em sistema baseado na cloud (OS Sandbox)
  - Listas de ficheiros autorizados/negados
  - Opção de análise heurística
- Integração com solução de Sandboxing (cloud ou on-premises) e capacidade de descarregar um relatório em PDF com o resultado da análise estática e dinâmica.
- Deteção de sites WEB (web filtering):
  - Suporte de diferentes mecanismos de deteção de sites WEB (proxy-based, flow-based and DNS)
  - Possibilidade de definição manual de filtros de sites com base em URL, conteúdo web e cabeçalho MIME
  - Categorização dinâmica em tempo real, baseada na cloud, com mais de 250 milhões de sites categorizados, de 70 idiomas e organizados em mais de 77 categorias
  - Opção para forçar a utilização de mecanismos de busca segura (safe search) disponibilizados pelos principais motores de busca, incluindo Google, Yahoo!, Bing & Yandex, e definição customizada de YouTube Education Filter
  - Deverá ser possível ter a opção para activar as seguintes funcionalidades:
    - Filtrar Java Applet, ActiveX e/ou cookies
    - Bloquear HTTP Post
    - Registar termos/palavras utilizados nas pesquisas em motores de busca
    - Identificar imagens pelo URL
    - Bloquear redirect de HTTP de acordo com a categoria
    - Excluir, de forma simples, a inspeção SSL de tráfego encriptado em determinadas categorias relevantes à manutenção da privacidade dos utilizadores
    - Definição de quotas de utilização WEB com base em categorias
  - Definição de categorias customizadas e sobreposição de categorização
  - Mecanismos de exceção à utilização de perfis pré-definidos;
- Detecção e limitação de acesso a conteúdos video de forma granular (Video Filter)
  - Limitação a canais específicos
  - Filtragem de conteúdo adulto
- Mecanismos de deteção e mitigação de utilização de proxy-avoidance: Categorias de sites com proxy, pontar URLs por domínio e endereço IP, bloquear redirects de cache para sites com cache e tradução de sites, bloqueio de ligação a proxy com base em deteção de aplicação, bloqueio de tráfego com comportamento de proxy com base em assinaturas de IPS
- Prevenção e proteção de fugas de informação - DLP
- Suporte de protocolos na análise de mensagens: HTTP-POST, SMTP, POP3, IMAP, MAPI, NNTP
- Possibilidade de executar as acções: registar, bloquear, quarentena de utilizador/IP/Interface
- Filtros pré-difinidos incluindo cartões de crédito e número de segurança Social
- Suporte de protocolos na análise de ficheiros: HTTP-POST, HTTP=-GET,SMTP, POP3, IMAP, MAPI, FTP, NNTP
- Opções de filtro disponíveis: tipo de ficheiro, watermark, conteúdo e deteção de encriptação

- Utilização de mecanismos de DLP watermarking , com disponibilização de ferramentas gratuitas de watermarking para Windows e Linux
- Fingerprinting de ficheiros
- Armazenamento de ficheiros detetados para inspeção forense, incluindo: todo o conteúdo de e-mail, FTP, IM, NNTP e tráfego WEB
- Integração nativa com plataformas externas de filtragem de email, sandbox e WAF
- Feeds de ameaças por Domain Name e/ou IP Address

Controlo de Endpoints
- Visibilidade centralizada sobre diversos elementos de rede, nomeadamente:
  - Vulnerabilidades nos endpoints
  - Indicadores de compromisso

Alta disponibilidade
As seguintes funcionalidades deverão ser suportadas:
- Alta disponibilidade disponível nos modos: ativo-passivo, ativo-ativo, virtual-cluster, VRRP
- Interfaces de heartbeat redundantes
- Interfaces reservadas para gestão
- Sem custos de licenciamento para suporte de funcionalidades de alta-disponibilidade
- Reposição automática de serviço (failover)
  - Monitorização de portas e links (locais e remotos)
  - Sem perca de sessões
  - Failover em menos de 1 segundo
  - Notificações de eventos de failover
- Diferentes opções de arquitetura
  - HA com agregação de links
  - Full mesh HA
  - Suporte para HA com equipamentos geograficamente dispersos
- Opção de sincronização de sessões em equipamentos configurados em modo Standalone ou Cluster geográfico

Administração, Monitorização e Diagnósticos
As seguintes funcionalidades deverão ser suportadas:
- Acesso de gestão gráfica e texto: HTTPS com recurso a web browser
- Acesso de gestão em modo de texto: SSH, Telnet ou consola
- Capacidade de captura de tráfego em CLI e GUI com possibilidadde de análise em tempo real
- Sem necessidade de utilização de software cliente proprietário para gestão gráfica
- Suporte de múltiplas linguagens de administração no acesso gráfico, incluindo: português, inglês, espanhol, francês, japonês, chinês simplificado, chinês tradicional e Coreano
- Suporte para gestão local e gestão centralizada em simultâneo
- Suporte para gestão centralizada com integração em plataforma específica para o efeito
- Integração com plataformas externas de gestão e monitorização, incluindo SNMP, sFlow, Syslog e Netflow
- Implementação rápida da solução incluindo mecanismos de auto instalação por USB, execução local e remota de scripts
- Visualização em tempo real do estado do equipamento através de interface gráfica (acesso HTTPS com recurso a web-browser) incluindo diversos conteúdos e funcionalidades.
- Integração com outras soluções (externas) através de scripts CLI e APIs.
- Wizards de configuração para implementação rápida da solução.
- Integração com soluções Openstack, VMWare NSX, e Cisco ACI.
- Automação, por exemplo para colocar em Quarentena um dispositivo com um elevado Indicador de Compromisso.
- Capacidade de backup para ficheiro em formato YAML
- Connectivity Fault Management (CFM)

Registo de eventos e relatórios
As seguintes funcionalidades deverão ser suportadas:
- Suporte para registo de eventos (logs) em diferentes repositórios, tais como: memória, disco rígido local, múltiplos servidores de syslog, múltiplos servidores específicos para registos de eventos e elaboração de relatórios, servidores do tipo WebTrends e plataformas disponíveis na cloud
- Opção de logging confiável com recurso a mecanismos TCP (RFC 5424)
- Encriptação de eventos para confidencialidade e integridade aquando da utilização de plataformas específicas;
- Possibilidade de exportar relatórios em formato PDF
- Calendarização de backups de logs para sistemas externos
- Registos detalhados de trafego: tráfego enviado, bloqueado, sessões violadas, tráfego local, pacotes inválidos
- Organização de registos de acordo com a categoria: administração de sistema (para auditoria), routing e networking, VPN, autenticação de utilizadores, Wireless
- Opção para registo parcial ou completo de eventos
- Resolução de nomes de endereços IPs e protocolos
- Mecanismo nativo de visualização de eventos de forma estatisca, com ferramentas de busca e drill-down disponível através de recurso com web browser.
- Suporte ao envio de logs no formato JSON.

Certificações O equipamento deverá ter as seguintes certificações: ● USGv6 IPv6 CertifiedRelatórios e Ferramentas de Visualização

Solução de autenticação e gestão de identidades com as seguintes características:

Característica base	
• Interfaces 10/100/1000 (Copper, RJ-45)	>=4
• Disco	2x 1TB Hard Disk Drive - RAID 1
• Trusted Platform Module (TPM)	Sim
• Numero de utilizadores Locais + remotos (Base / maximum)	1500 / 3000
• Tokens	>=3000
• Clientes RADIUS (NAS Devices)	>=500
• Grupos de utilizadores	>=150
• Certificados CA	>=10
• Certificados de utilizador	>=7500
• Standards suportados	10/100/1000 Base-TX (GE), IP, Telnet, HTTP 1.0/1.1, SSL, RS232, NTP Client (RFC1305), RADIUS (RFC2865), LDAP (RFC4510), x.509 (RFC5280), Certificate Revocation (RFC3280), PKCS#12 Certificate Import, PKCS#10 CSR Import (RFC2986), Online Certificate Status Protocol (RFC 2560), EAP-TLS (RFC2716), Simple Certificate Enrollment Protocol (SCEP), oAuth, OIDC, and SAML2.0
Energia e Alimentação	
• Alimentação AC	100–240V AC, 50–60 Hz
• Consumo de energia médio	<=82.5W
• Consumo de energia máximo	<=131.5W
• Dissipação Térmica	<=485 BTU/h
• Fonte de alimentação redundante	100-240 VAC, 50/60 Hz 300W Redundant (1+0)
Condições ambientais	
• Temperatura de funcionamento	0 - 40 °C
• Humidade	5 a 90% sem condensação
• Compliance	FCC Part 15 Class A, RCM, VCCI, CE, UL/cUL, CB
Dimensões	
• Altura	44.45 mm (1RU)
• Largura	<=440 mm
• Profundidade	<=425 mm
• Peso	<=8,5 KG

Funcionalidades principais
Funcionalidades principais As seguintes funcionalidades deverão ser suportadas: • Autenticação segura baseada em protocolos standard de autenticação como RADIUS e LDAP • Duplo fator de autenticação através da utilização de tokens físicos, aplicações móveis com suporte a sistemas iOS e Android, SMS e email, certificados digitais e chaves FIDO2 sem password • Diretório local de utilizadores e Integração com sistemas de diretórios externos incluindo LDAP e Active Directory de forma a reutilizar credenciais existentes • Políticas de sincronização para importação de utilizadores em diretórios externos

- Portais de registo e self-service customizáveis que permitam o registo automatizado e gestão de passwords pelos próprios utilizadores e integração com dispositivos externos
- A solução deverá ter a capacidade de funcionar como entidade certificadora, fazendo a emissão e gestão do ciclo de vida dos certificados digitais, usados para autenticação segura de dispositivos ou utilizadores em redes com e sem fios e acessos VPN
- Gestão de certificados para registo automático de dispositivos em ambientes BYOD (Bring Your Own Device)
- A solução deverá suportar o standard IEEE 802.1X de forma a permitir a autenticação de nível corporativo de dispositivos e utilizadores em redes com e sem fios. Deverão ser suportados entre outros os protocolos PEAP, EAP-MD5, EAP-TTLS, EAP-TLS e EAP-GTC. A solução deverá ainda suportar autenticação baseada no mac address dos dispositivos
- Identificação dos utilizadores de forma transparente através de pelo menos os seguintes métodos
  - Integração com controladores de domínio de Active Directory de forma a captar as credenciais dos utilizadores
  - Agente externo para instalação nas máquinas dos utilizadores com capacidade para detetar eventos e informação de login e logout e alteração de endereços IP
  - Portais disponibilizados pela própria solução para autenticação e rastreio dos utilizadores de forma a reduzir a necessidade de autenticações repetidas
  - Monitorização dos registos de login dos acessos baseados no protocolo RADIUS
- A solução deverá disponibilizar uma API de autenticação para integração com sistemas terceiros
- A solução deverá suportar o standard de autenticação e autorização SAML SP/IdP de forma a garantir mecanismos de single sign-on para acesso a aplicações através de browser

Requisitos gerais

As seguintes características deverão ser asseguradas:

- Consola de gestão com acesso via browser e protocolo seguro HTTPS ou CLI via SSH
- A solução deverá permitir a implementação em cenário de alta disponibilidade
- Deverá permitir a utilização do protocolo SNMP para queries ou envio de traps com informação do sistema
- A solução deverá ter a capacidade de mostrar graficamente, na consola de gestão, as tentativas de autenticação com e sem sucesso num período de tempo configurável
- A solução deverá ter a capacidade de guardar os logs de autenticação localmente ou enviar para um repositório externo via Syslog
- Deverá permitir o backup de toda a configuração a partir da consola de gestão e suportar calendarização e envio do ficheiro de backup para um repositório externo

Requisitos da componente de duplo fator de autenticação

As seguintes funcionalidades deverão ser suportadas:

- OATH baseada em tempo ou eventos para gerar passwords de utilização única
- Detalhes do login enviados por PUSH para o telemovel com a possibilidade de aprovar ou rejeitar
- Utilização de PIN/Impressão digital/reconhecimento facial para proteger a aplicação
- Permissão para copiar OTP (One time Password) para o clipboard
- Exibição do tempo de validade da OTP
- Gestão de tokens
- Remoção automatica de tokens em caso de ataques brute-force
- Compatibilidade com Apple Watch, iOS (iPhone, iPod Touch, iPad), Android, Windows Phone 8, 8.1, Windows 10 and Windows Universal Platform
- Licenciamento perpetúo e transferencias entre dispositivos ilimitados
- Ativar tokens over-the-air (Apenas disponível para dispositivos com WIFI)
- Especificações da OTP (RFC 6238, RFC 4226)

Software one-time password tokens com as seguintes características:

Funcionalidades Principais:

As seguintes funcionalidades deverão ser suportadas:

- Gerador OATH compliant com OTP suportando tokens baseados em tempo (TOTP) ou eventos (HOTP) para gerar passwords de utilização única.
- Detalhes do login enviados por PUSH para o telemóvel para opção de aprovar ou rejeitar.
- Utilização de PIN/Impressão digital/reconhecimento facial para proteger a aplicação.
- Permissão para copiar OTP (One time Password) para o clipboard.
- Tempo de validade da OTP.
- Gestão de tokens e da aplicação.
- Remoção automática de tokens em caso de ataques brute-force.
- Compatibilidade com iOS (iPhone, iPod Touch, iPad, Apple Watch,), Android, Windows Phone 8, 8.1, Windows 10 e Windows Universal Platform.
- Licenciamento perpetúo e transferências entre dispositivos ilimitadas.
- Ativar tokens over-the-air (Apenas disponível para dispositivos com WIFI)
- Especificações da OTP (RFC 6238, RFC 4226)

SERVIÇOS DE INSTALAÇÃO E CONFIGURAÇÃO A INCLUIR EM TODAS AS TIPOLOGIAS DE FIREWALL	
• Serviço de Instalação e Configuração Clusters Firewalles 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 13/2024– Equipamentos de Firewall – Perímetro e Gestão".**

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.**