CADERNO DE ENCARGOS

AQUISIÇÃO DE HARDWARE PARA IMPLEMENTAÇÃO DE LIGAÇÕES DEDICADAS VPN

Capítulo I – Disposições Gerais

1. Objeto

O objeto do contrato consiste numa aquisição de bens móveis (hardware) de forma a uniformizar e interligar, utilizando a tecnologia VPN, os acessos aos diversos pontos remotos da IHM, EPERAM (Polos comunitários e Gabinetes exteriores), de acordo com as cláusulas deste Caderno de Encargos.

2. Contrato

2.1. O contrato é composto pelo respetivo clausulado contratual e eventuais anexos.

2.2. O contrato a celebrar integra ainda os seguintes elementos:

a) O suprimento dos erros e das omissões do Caderno de Encargos, identificados pelo concorrente, desde que esses erros e omissões tenham sido expressamente aceites, pelo órgão competente para a decisão de contratar;

b) Os esclarecimentos e as retificações relativos ao Caderno de Encargos;

c) O presente Caderno de Encargos;

d) A proposta adjudicada;

e) Os esclarecimentos sobre a proposta adjudicada prestados pelo adjudicatário.

2.3. Em caso de divergência entre os documentos referidos no número anterior, a respetiva prevalência é determinada de acordo com o disposto nos n.^{os} 5 e 6 do artigo 96.º do Código dos Contratos Públicos (CCP).

3. Esclarecimento de dúvidas

3.1. As dúvidas que o cocontratante tenha na interpretação dos documentos por que se rege o contrato devem ser submetidas ao gestor do contrato antes do início da entrega dos bens móveis.

3.2. O incumprimento do disposto no número anterior torna o cocontratante responsável por todas as consequências da errada interpretação que porventura haja feito, incluindo a devolução/substituição dos bens.

4. Preço base

4.1. O parâmetro base do preço contratual é **EUR 15.500,00 (S/IVA).**

4.2. A fundamentação para a fixação do preço base do procedimento, referido no número anterior, consta do n.º 1 do artigo 35.º-A do CPP, na sequência de uma consulta preliminar ao mercado.

Capítulo II – Obrigações do cocontratante

5. Obrigações principais do cocontratante

Sem prejuízo de outras obrigações previstas na legislação aplicável e no presente Caderno de Encargos, da celebração do contrato decorre para o cocontratante as seguintes obrigações principais:

a) Obrigação de entrega dos bens identificados e caracterizados no caderno de encargos e na proposta adjudicada;

b) Cumprimento do prazo de entrega;

c) Obrigação de garantia dos bens, pelo prazo de 1 ano;

d) Obrigação de suporte técnico durante 1 ano.

6. Condições de fornecimento

6.1. O cocontratante obriga-se a entregar ao contraente público os bens objeto do contrato com as características previstas no **Anexo A** ao presente Caderno de Encargos, que dele faz parte integrante e da proposta adjudicada.

6.2. Os bens objeto do contrato devem ser entregues novos, em perfeitas condições de serem utilizados para os fins a que se destinam e dotados de todo o material de apoio necessário à sua entrada em funcionamento.

6.3. É aplicável, com as necessárias adaptações, o disposto na lei que disciplina os aspetos relativos à venda de bens de consumo e das garantias a ela relativas, no que respeita à conformidade dos bens.

6.4. O cocontratante é responsável perante o contraente público, por qualquer defeito ou discrepância dos bens objeto do contrato que existam no momento em que os bens lhe são entregues.

6.5. Todas as despesas e custos com o transporte dos bens objeto do contrato e respetivos documentos para o local de entrega são da responsabilidade do cocontratante.

6.6. O contrato apenas se considera integralmente executado após o cumprimento da obrigação de garantia prevista na cláusula 12.ª do presente caderno de encargos.

7. Local de entrega

Os bens objeto do contrato celebrado devem ser entregues na sede da IHM, EPERAM, sita à Rua Dr. Pestana Júnior, n.º 6, 1.º andar, no Funchal.

8. Prazo de entrega dos bens

Os bens a adquirir, objeto do presente contrato, deverão ser entregues no **prazo máximo de 90 dias**, a contar da data da outorga do contrato, sem prejuízo das obrigações referidas nas alíneas c) e d) da cláusula 5.ª.

9. Inspeção dos bens

9.1. Efetuada a entrega dos bens objeto do contrato, dentro do prazo referido na cláusula anterior, o contraente público, por si ou através de terceiro por ele designado, procede, no prazo máximo de 3 dias, à inspeção quantitativa e qualitativa dos mesmos, com vista a verificar, respetivamente, se os mesmos correspondem às quantidades estabelecidas, e se reúnem as características definidas no **Anexo A** ao presente Caderno de Encargos e na proposta adjudicada, bem como outros requisitos exigidos por lei.

9.2. Durante a fase de realização da inspeção, a cocontratante deve prestar ao contraente público toda a cooperação e todos os esclarecimentos necessários, podendo fazer-se representar durante a realização daquela, através de pessoas devidamente credenciadas para o efeito.

10. Inoperacionalidade, defeitos ou discrepâncias

10.1. No caso da inspeção prevista na cláusula anterior não comprovar a total operacionalidade dos bens objeto do contrato, bem como a sua conformidade com as exigências legais, ou no caso de

existirem defeitos ou discrepâncias com as características definidas no **Anexo A** ao presente Caderno de Encargos e na proposta adjudicada, o contraente público deve disso informar, por escrito, o cocontratante, fixando-lhe um prazo razoável para que este proceda, à sua custa, às reparações, correções ou substituições necessárias para garantir o cumprimento do contrato.

10.2. Após a realização das reparações, correções ou substituições necessárias pelo cocontratante, no prazo respetivo, o contraente público procede à realização de nova inspeção para efeitos de aceitação, nos termos da cláusula anterior.

10.3. No caso do cocontratante não proceder à entrega ou às reparações, correções ou substituições nos termos e nos prazos referidos nos números anteriores, o contraente público pode resolver o contrato nos termos da cláusula 22.ª, sem prejuízo das eventuais sanções contratuais aplicáveis conforme disposto na cláusula 21.ª.

10.4. Para efeitos do número anterior e da consequente resolução do contrato, considera-se que a notificação efetuada nos termos do n.º 1 da presenta cláusula equivale à notificação referida no ponto 2 da cláusula 22.ª.

11. Aceitação dos bens

11.1 Caso a inspeção a que se refere a cláusula 9.ª comprove a total operacionalidade dos bens objeto do contrato, bem como a sua conformidade com as exigências legais, e neles não sejam detetados quaisquer defeitos ou discrepâncias com as características, especificações e requisitos técnicos definidos no anexo ao presente Caderno de Encargos, o contraente público notifica o cocontratante para efeitos de elaboração do auto de aceitação dos bens, o qual deverá ser assinado pelos seus representantes e do contraente público, a ocorrer no prazo máximo de 2 dias a contar do final do período de inspeção referido na cláusula 9.ª.

11.2. Com a assinatura do auto a que se refere o número anterior, ocorre a transferência da posse e da propriedade dos bens objeto do contrato para o contraente público, bem como do risco de deterioração ou perecimento dos mesmos, sem prejuízo das obrigações de garantia que impendem sobre o fornecedor.

11.3. A assinatura do auto a que se refere o n.º 11.1 não implica a aceitação de eventuais defeitos ou de discrepâncias dos bens objeto do contrato com as exigências legais ou com as características, especificações e requisitos técnicos previstos no **Anexo A** ao presente Caderno de Encargos, que não tenham sido detetados, ou que não sejam detetáveis, no momento da assinatura do referido auto.

11.4. Na eventualidade de não se entregar parte dos bens, ou de apenas se comprovar, através da inspeção referida na cláusula 9.ª, a operacionalidade e conformidade com as exigências legais e com as características definidas no **Anexo A** ao presente Caderno de Encargos, de apenas uma parte dos bens fornecidos, poderá ser elaborado e assinado um auto de receção parcial desses bens, procedendo-se de acordo com cláusula 10.ª para os restantes bens.

12. Garantia técnica

12.1. Nos termos da presente cláusula e da lei, o cocontratante garante os bens objeto do contrato, pelo **prazo de um ano a contar da data da assinatura do auto de aceitação dos bens**, contra quaisquer defeitos ou discrepâncias com as exigências legais e com características definidas no **Anexo A** ao presente Caderno de Encargos, e na proposta adjudicada, que se revelem a partir da aceitação dos bens.

12.2. A garantia prevista no número anterior abrange, nomeadamente:

a) O fornecimento, de quaisquer peças ou componentes em falta;

b) A reparação ou a substituição das peças, componentes ou bens defeituosos ou discrepantes;

c) O fornecimento das peças, componentes ou bens reparados ou substituídos;

d) O transporte do bem ou das peças ou componentes defeituosos ou discrepantes para o local da sua reparação ou substituição e a devolução daqueles bens ou a entrega das peças ou componentes em falta, reparados ou substituídos;

e) A deslocação ao local da instalação ou de entrega;

12.3. A reparação ou substituição previstas na presente cláusula devem ser realizadas dentro de um prazo razoável fixado pelo contraente público, e sem grave inconveniente para este, tendo em conta a natureza dos bens e o fim a que se destinam, sendo correspondentemente aplicável, com as devidas adaptações, o disposto nas cláusulas 21.ª e 22.ª referentes, respetivamente, às sanções contratuais e à resolução do contrato.

Capítulo III – Obrigações do contraente público

13. Preço Contratual

13.1. Pelo fornecimento dos bens objeto do contrato, a IHM, EPERAM pagará ao cocontratante o preço constante da proposta adjudicada, acrescido de IVA à taxa legal em vigor.

13.2. O preço contratual inclui todos os custos, encargos e despesas cuja responsabilidade não esteja expressamente atribuída ao contraente público, nomeadamente todos os custos com meios de transporte dos bens móveis objeto da presente aquisição até ao correspondente local de entrega.

14. Condições de pagamento

14.1. O pagamento será efetuado pelo contraente público no prazo máximo de 60 dias, após a data da receção da fatura, que corresponderá à data do correspondente registo de entrada.

14.2. Na fatura ou documento equivalente, não deverá ser feita qualquer menção à data de vencimento, mas, sim, ao prazo de vencimento mencionado no número anterior.

14.3. A fatura (ou faturas no caso de autos de aceitações parciais) apenas poderá ser emitida após a elaboração do auto de aceitação dos bens, nos termos da cláusula 11.ª do presente caderno de encargos.

15. Adiantamentos

Salvo o disposto na parte final do n.º 4 do artigo 292.º do CCP, não se prevê qualquer adiantamento de parte do preço a pagar pelo contraente público ao cocontratante.

16. Mora no pagamento

Em caso de atraso do contraente público no cumprimento das obrigações de pagamento do preço contratual, tem o cocontratante/fornecedor direito aos juros de mora sobre o montante em dívida à taxa legalmente fixada para o efeito pelo período correspondente à mora.

Capítulo IV - Condições de Modificação ao contrato

17. Disposição geral

17.1. - Sem prejuízo do disposto nas cláusulas seguintes, é aplicável à modificação objetiva do contrato em apreço (no tocante, em especial, à fonte, aos fundamentos, aos limites e respetivas consequências), o disposto nos artigos 311.º e seguintes do CCP.

17.2. – Em tudo o que não esteja especialmente previsto no presente capítulo, é aplicável o disposto no Código dos Contratos Públicos (CCP).

18. Entregas complementares

18.1.O cocontratante tem a obrigação de proceder a entregas complementares de bens que lhe sejam ordenados pelo contraente público, nos termos das disposições conjugadas dos artigos 371.º e 438.º do CCP.

18.3. A responsabilidade pelas entregas complementares é determinada nos termos do disposto no artigo 378.º, aplicável *ex vi* artigo 438.º ambos do CCP.

18.4 - Às entregas complementares de bens aplica-se o disposto nos artigos 370.º a 378.º aplicáveis *ex vi* artigo 438.º, todos do CCP.

19. Revisão de preços

Não há lugar a revisão de preços.

20. Cessão da posição contratual

Não é admitida a cessão da posição contratual.

Capítulo V – Incumprimento do contrato

21. Sanções contratuais

21.1. Pelo incumprimento imputável ao cocontratante, nomeadamente por mora ou incumprimento definitivo, de qualquer das obrigações emergentes do contrato o contraente público pode exigir do cocontratante o pagamento de uma sanção pecuniária, de montante a fixar de acordo com o seguinte:

- Em caso de mora, por cada dia de atraso no cumprimento do prazo referido na cláusula 8.ª ou na regularização de qualquer outra causa que obste ao exato cumprimento das obrigações contratuais, a sanção será de até 2% do preço contratual inicial;
- Em caso de incumprimento definitivo, a sanção aplicada será de até 5% do preço contratual inicial.

21.2. A aplicação das sanções contratuais será efetuada respeitando os limites e cumprindo as formalidades previstas na legislação aplicável, nomeadamente o disposto no artigo 329.º do CCP.

21.3. Na determinação da imputabilidade do incumprimento, para efeitos de concretização do valor da sanção aplicável nos termos referidos no número 1, o contraente público tem em conta, nomeadamente, a duração da infração, a sua eventual reiteração, o grau de culpa do fornecedor e as consequências do incumprimento.

21.4. O contraente público pode deduzir nos pagamentos devidos ao abrigo do contrato os valores das sanções contratuais aplicadas.

21.5. A aplicação das sanções contratuais nos termos previstos nos números anteriores não obsta ao poder de resolução pelo contraente público, nem à aplicação das disposições relativas à indemnização por mora e incumprimento definitivo nos termos gerais de direito.

22. Resolução do contrato pelo contraente público

22.1 À resolução do contrato pelo contraente público aplica-se, em especial, o disposto no artigo 448.º, bem como o disposto nos artigos 330.º e ss., todos do CCP.

22.2 Considerando o estabelecido no artigo 325.º do CCP, e sem prejuízo do disposto no número anterior, o contraente público pode resolver o contrato, total ou parcialmente, por incumprimento definitivo quando, após a notificação para cumprir, o cocontratante não proceda à entrega dos bens ou não proceda à regularização de qualquer outra causa que obste ao exato e cumprimento das obrigações contratuais, no prazo que razoavelmente lhe for fixado para o efeito.

22.3. O direito de resolução referido no número anterior exerce-se unilateralmente e deve ser comunicado por escrito ao cocontratante, e não obsta à aplicação das sanções contratuais previstas no presente caderno de encargos nem à aplicação das disposições relativas à indemnização por mora e incumprimento definitivo nos termos gerais de direito.

23. Resolução do contrato pelo cocontratante

23.1. O cocontratante pode resolver o contrato nos casos previstos na lei.

23.2. O direito de resolução é exercido por via judicial.

23.3. A resolução do contrato não determina a repetição das prestações já realizadas pelo cocontratante, cessando, porém, todas as obrigações deste ao abrigo do contrato, com exceção daquelas a que se refere o artigo 444.º do Código dos Contratos Públicos.

Capítulo VI – Representação das partes e controlo da execução do contrato

24. Representação do cocontratante

A execução do contrato será acompanhada, por parte do cocontratante, por quem este identificar no contrato.

25. Representação do contraente público

25.1 A execução do contrato será acompanhada, por parte do contraente público pelo gestor do contrato designado, nos termos e para os efeitos do disposto no artigo 290.º-A do CCP.

25.2 Durante os períodos em que se encontre ausente ou impedido, o gestor do contrato é substituído pela pessoa que for designada pela entidade adjudicante/contraente público para o efeito, devendo, a designação do substituto ser comunicada, por escrito, ao adjudicatário/cocontratante (esta comunicação deve ser anexa ao correspondente clausulado contratual).

26. Execução do contrato

26.1. Nos termos do disposto no artigo 7.º-A do Decreto Legislativo Regional n.º 34/2008/M, de 14 de agosto, na redação atual, durante o prazo de vigência do contrato (até à receção da totalidade dos bens fornecidos), incluindo quaisquer prorrogações do prazo de execução, o cocontratante e, caso existam, os subcontratados devem proceder à entrega dos documentos identificados na alínea a) do n.º 2 do artigo 7.º do mencionado diploma, sem prejuízo do disposto no seu n.º 5.

26.2. Nos termos do disposto no artigo 8.º-A do Decreto Legislativo Regional n.º 34/2008/M, de 14 de agosto, na redação atual, compete ao Gestor do Contrato, sem prejuízo das funções que lhe são atribuídas no artigo 290.º-A do Código dos Contratos Públicos, acompanhar o cumprimento das obrigações declarativas relativas a rendimentos gerados na Região Autónoma da Madeira, nomeadamente a entrega dos documentos identificados no artigo 7.º-A do referido diploma.

Capítulo VII – Disposições finais

27. Caução

Não é exigida a prestação de caução, nos termos do disposto no n.º 2 do artigo 88.º do CCP.

28. Deveres de colaboração recíproca e informação

As partes estão vinculadas pelo dever de colaboração mútua, designadamente no tocante à prestação recíproca de informações necessárias à boa execução do contrato, sem prejuízo dos deveres de informação previstos no artigo 290.º do CCP.

29. Sigilo

29.1. O cocontratante deve guardar sigilo sobre toda a informação e documentação, técnica e não técnica, comercial ou outra, de que possa ter conhecimento ao abrigo ou em relação com a execução do contrato.

29.2. A informação e a documentação cobertas pelo dever de sigilo não podem ser transmitidas a terceiros nem objeto de qualquer uso ou modo de aproveitamento que não o destinado direta e exclusivamente à execução do contrato.

29.3. Excluem-se do dever de sigilo previsto a informação e a documentação que sejam comprovadamente do domínio público à data da respetiva obtenção pelo cocontratante ou que este seja legalmente obrigado a revelar, por força da lei, de processo judicial ou a pedido de autoridades reguladoras ou outras entidades administrativas competentes.

30. Comunicações e notificações

30.1 - As notificações dos atos no âmbito da execução do contrato são efetuadas nos termos do disposto no artigo 467.º do CCP, preferencialmente, através de correio eletrónico, para o endereço que for indicado no contrato.

30.2 - As comunicações entre as partes no âmbito da execução do contrato são efetuadas nos termos do disposto no artigo 468.º do Código dos Contratos Públicos, preferencialmente, através de correio eletrónico, para os endereços que forem indicados no contrato.

30.3 - As notificações/comunicações que sejam realizadas por via postal, serão efetuadas para o endereço postal que for indicado no contrato.

30.4 - Qualquer alteração dos endereços constantes do contrato deve ser comunicada à outra parte.

31. Contagem dos prazos

Na fase de execução do contrato os prazos contam-se de acordo com as regras previstas no artigo 471.º do CCP.

32. Foro competente

Para resolução de todos os litígios decorrentes da execução do contrato as partes recorrerão ao tribunal administrativo competente.

PARECERES PRÉVIOS, LICENCIAMENTOS E AUTORIZAÇÕES QUE POSSAM CONDICIONAR O PROCEDIMENTO E/OU A EXECUÇÃO DO CONTRATO

Em função do objeto do contrato, foi obtida a autorização prévia do membro do Governo responsável pela área das finanças, mediante parecer prévio da Direção Regional de Informática, nos termos do n.º 1 do artigo 20.º do Decreto Regulamentar Regional n.º 5/2021/M, de 03 de maio.

Anexo A: Lista de bens a adquirir.

Funchal, 29 de junho de 2022

O Presidente do Conselho de Administração

Assinado com Assinatura Digital Qualificada por:
JOÃO PEDRO PEREIRA E SOUSA
Presidente do Conselho de Administração
IHM - INVESTIMENTOS HABITACIONAIS DA MADEIRA EPERAM
IHM - INVESTIMENTOS HABITACIONAIS DA MADEIRA EPERAM
Reunião CA de 19/04/2022, acta n.º 25, livro n.º 23
Data: 04-07-2022 17:30:48

João Pedro Sousa

ANEXO A

ESPECIFICAÇÕES TÉCNICAS : HARDWARE NEXT GEN FIREWALL

ESPECIFICAÇÕES TÉCNICAS	
CONECTIVIDADE	
INTERFACES 10/100/1000 RJ45 ACELERADAS ASIC	10X GE RJ45
INTERFACE USB CLIENT	1
INTERFACE DE CONSOLE (RJ45)	1
SISTEMA	
DISCO INTERNO	1X 128 GB SSD
DESEMPENHO	
ACELERAÇÃO DO TRÁFEGO DE FIREWALL, SSL E IPSEC POR HARDWARE	HARDWARE DEDICADO
ACELERAÇÃO DE TRÁFEGO NGFW POR HARDWARE	HARDWARE DEDICADO
DÉBITO FIREWALL (PACOTES UDP DE 1518 / 512 / 64 BYTES)	10 / 10 / 6 GBPS
LATÊNCIA DE FIREWALL (PACOTES UDP DE 64 BYTES)	3.3 MS
DÉBITO FIREWALL (PACOTES POR SEGUNDO)	9 MPPS
SESSÕES TCP CONCORRENTES	700000
NOVAS SESSÕES/SEGUNDO (TCP)	35000
POLITICAS DE FIREWALL	5000
DÉBITO VPN IPSEC (PACOTES 512 BYTES)	6.5 GBPS
TÚNEIS IPSEC GATEWAY-TO-GATEWAY	200
TÚNEIS IPSEC CLIENTE REMOTO	500
DÉBITO VPN SSL	900 MBPS
VPN SSL - MÁXIMO RECOMENDADO DE UTILIZADORES SIMULTÂNEOS	200
DÉBITO IPS	1.4 GBPS
DÉBITO DE INSPEÇÃO SSL	630 MBPS
DÉBITO DE APPLICATION CONTROL	1.8 GBPS
DÉBITO NGFW	1 GBPS
DÉBITO THREAT PROTECTION	700 MBPS
DOMÍNIOS VIRTUAIS (POR DEFEITO / MÁXIMO)	10 / 10
MÁXIMO DE FORTIAPS CONTROLADOS (TOTAL / TUNNEL MODE)	64/32
MÁXIMO DE FORTISWTICH CONTROLADOS	16
MÁXIMO DE FORTITOKENS	500
LICENCIAMENTO ILIMITADO DE UTILIZADORES	SIM
ENERGIA E ALIMENTAÇÃO	
ALIMENTAÇÃO AC	100–240V AC, 50–60 HZ
CONSUMO DE ENERGIA MÉDIO	17.2 W
CONSUMO DE ENERGIA MÁXIMO	18.7 W
DISSIPAÇÃO TÉRMICA	63.8 BTU/H
CONDIÇÕES AMBIENTAIS	
TEMPERATURA DE FUNCIONAMENTO	0 - 40 °C
FANLESS	SIM
COMPLIANCE	FCC, ICES, CE, RCM, VCCI, BSMI, UL/CUL, CB
CERTIFICAÇÕES	ICSA LABS: FIREWALL, IPSEC, IPS, ANTIVIRUS, SSL-VPN
DIMENSÕES	
ALTURA	38.5 MM
LARGURA	216 MM
PROFUNDIDADE	160 MM

ESPECIFICAÇÕES TÉCNICAS : REFERENTES AO SISTEMA OPERATIVO DA NEXT GEN FIREWALL

FUNCIONALIDADES SUPORTADAS	
SERVIDOR DHCP; NTP; DNS	
FUNCIONALIDADES DE DNS PROXY	
MÚLTIPLOS MODOS DE CONFIGURAÇÃO DE INTERFACES	SNIFFER; AGREGAÇÃO DE PORTAS (802.3AD); LOOPBACK; VLANS (802.1Q E TRUNK); SOFTWARE SWITCH
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
BALANCEAMENTO E REDUNDÂNCIA DE MÚLTIPLOS LINKS;	
SUPORTE PARA PROTOCOLOS DE ROUTING DINÂMICO: RIPV1, RIPV2, RIPNG, OSPFV2 E OSPFV3, ISIS, BGP4+	
SUPORTE DE TRAFEGO MULTICAST: PIM, SPARSE E DENSE MODE	
ROUTING BASEADO EM CONTEÚDOS: WCCP E ICAP	
PROXY EXPLÍCITO COM SUPORTE PAC E WPAD	
SUPORTE DE IPV6	GESTÃO POR IPV6 PROTOCOLOS DE ROUTING DINÂMICO COM SUPORTE PARA IPV6 TUNNELING DE IPV6 PROCESSAMENTO FIREWALL E UTM DE IPV6 NAT64 NAT46 VPN IPSEC IPV6
SUPORTE DUAL STACK IPV4 E IPV6 EM SIMULTÂNEO	
SUPORTE VXLAN	
CONTROLADOR WIRELESS INTEGRADO	
CONTROLADOR SWITCHING INTEGRADO	
VIRTUALIZAÇÃO DA SOLUÇÃO EM CONTEXTOS	
IDENTIFICAÇÃO DE UTILIZADORES E DISPOSITIVOS	
BASE DE DADOS LOCAL DE UTILIZADORES	
AUTENTICAÇÃO DE UTILIZADORES EM SERVIDORES REMOTOS	LDAP, RADIUS, TACACS+
SISTEMA DE SINGLE SIGN-ON DE UTILIZADORES	WINDOWS AD; KERBEROS; NOVELL EDIRECTORY; FORTICLIENT; CITRIX E TERMINAL SERVER; RADIUS (ACCOUNTING MESSAGE); AUTENTICAÇÃO DE UTILIZADORES NO ACESSO (802.1X, PORTAL CATIVO)
PKI E CERTIFICADOS	CERTIFICADOS X.509; SUPORTE SCEP; CRIAÇÃO DE CERTIFICATE SIGNING REQUEST (CSR); AUTO RENOVAÇÃO DE CERTIFICADOS ANTES DA DATA DE EXPIRAÇÃO; SUPORTE OCSP
AUTENTICAÇÃO DE 2 FATORES	SERVIDOR INTEGRADO DE AUTENTICAÇÃO POR TOKENS FÍSICOS, TOKENS POR SOFTWARE E SMS INTEGRAÇÃO COM TERCEIRAS PARTES
IDENTIFICAÇÃO DE DISPOSITIVOS (INCLUINDO DISPOSITIVOS IOT)	RECONHECIMENTO DE DISPOSITIVO E SISTEMA OPERATIVO; CLASSIFICAÇÃO AUTOMÁTICA DE DISPOSITIVOS; GESTÃO DE INVENTÁRIO DE DISPOSITIVOS; SUPORTE DE AUTENTICAÇÃO E BYPASS FEITOS POR MAC ADDRESS
IMPLEMENTAÇÃO DE POLÍTICAS DE SEGURANÇA COM BASE EM UTILIZADOR OU DISPOSITIVOS	
COMPONENTE DE FIREWALL	
MODOS DE OPERAÇÃO	NAT/ROUTE E TRANSPARENTE/BRIDGE
AGENDAMENTO DE POLÍTICAS	RECORRENTES OU APENAS UMA VEZ
SESSION HELPERS E ALGS	DCERPC, DNS-TCP, DNS-UDP, FTP, H.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: Office 365; Azure)	com atualização automática das gamas de IP e portos
Configuração de NAT	por política e tabela central de NAT
Suporte de NAT	NAT64, NAT46, NAT estático, NAT dinâmico, PAT, Full Cone NAT, STUN
Traffic shaping e QOS	shaping de tráfego partilhado por política, shapping por IP, largura de banda máxima e garantida, número máximo de ligações por IP, priorização de tráfego, suporte de Type of Service (TOS) e Differentiated Services (DiffServ)
Processamento de tráfego de firewall IP4 e IPv6 feito em processador dedicado e desenhado para o efeito	
Componente deVPN	
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 (MAC OSX, Windows, IOS, Android)
	Suporte para VPN SSL em modo port-forwarding; 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	
Componente ZTNA - Zero Trust Network Access	
Capacidade da Firewall de ser um proxy point de ZTNA	
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	
Componente de 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	
Componente de Controlo de aplicações	
Deteção de 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)	
Componente de Proteção contra ameaças	
Possibilidade de inspeção aplicacional de tráfego encriptado por SSL, incluindo	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	protocolos: HTTP/HTTPS, STMP/SMTPS, POP3/POP3S, IMAP/IMAPS, MAPI, FTP/SFTP, ICQ, YM, NNTP
	Suporte para análise de ficheiros em sistema baseado na cloud (OS Sandbox
	Listas de ficheiros autorizados/negados
	Opção de análise heurística
Integração com solução de Sandboxing (cloud ou on-premises)	
Deteção de sites WEB (web filtering)	Suporte de diferentes mecanismos de deteção de sites WEB (proxy-based, flow-based and DNS); Possibilidade de definição manual de 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) Mecanismos de deteção e mitigação de utilização de proxy-avoidance	Limitação a canais específicos Filtragem de conteúdo adulto 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	
Componente de 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 para gestão local e gestão centralizada em simultâneo	
Suporte para gestão centralizada com integração em plataforma específica para o efeito	
ntegração 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	
Componente de 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 3195)	
Encriptação de eventos para confidencialidade e integridade aquando da utilização de plataformas específicas	
Possibilidade de exportar relatórios em formato PDF	
Calendarização de backups de logs para sistemas externos	
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	
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
Certificações	
Certificações ICSA de Firewall, SSL VPN, IPSEc VPN, AV e IPS	
FIPS 140-2 Validated (quando a operar em FIPS mode)	
USGv6 IPv6 Certified	