



CADERNO DE ENCARGOS DE PROCEDIMENTO PARA O CONCURSO PÚBLICO
AQUISIÇÃO INFRAESTRUTURAS DE EQUIPAMENTOS ATIVOS DE REDES,
FIREWALLS E PONTOS ACESSO PARA A CASA PIA DE LISBOA, I.P.

Processo n.º 5001/21/0000549



PARTE I

CLÁUSULAS GERAIS

CAPITULO I

1. OBJETO

O presente caderno de encargos compreende as cláusulas a incluir no contrato a celebrar na sequência do procedimento contratual por Concurso Público, e que tem por objecto a **aquisição infraestruturas de equipamentos ativos de redes, firewalls e pontos de acesso**, para a Casa Pia de Lisboa, I.P..

2. PREÇO BASE

O preço máximo que a entidade adjudicante se dispõe a pagar pela aquisição dos bens objeto do presente procedimento, é de € 273.599,99 € (duzentos e setenta e três mil e quinhentos e noventa e nove euros e noventa e nove cêntimos), acrescidos de IVA à taxa legal em vigor.

3. VIGENCIA E PRAZO DE EXECUÇÃO

1. O contrato a celebrar na sequência do presente procedimento contempla a aquisição infraestruturas de equipamentos ativos de redes, firewalls e pontos de acesso para a Casa Pia de Lisboa, I.P., com início a partir do dia seguinte ao da receção da Requisição Oficial de Adjudicação.
2. O presente procedimento tem em vista o fornecimento de infraestruturas de equipamentos ativos de redes, firewalls e pontos de acesso para a Casa Pia de Lisboa, I.P., iniciando-se após emissão da requisição oficial, até ao prazo máximo de 30 de Dezembro de 2021.
3. O contrato manter-se-á em vigor até total cumprimento do mesmo, sem prejuízo das obrigações acessórias que devam perdurar para além da sua cessação.
4. Em caso de denúncia, esta deverá ser efetuada através de carta registada com aviso de receção, a enviar ao outro contratante com a antecedência mínima de 90 (noventa) dias relativamente ao fim do período em curso.



CAPITULO II

OBRIGAÇÕES CONTRATUAIS

4. LOCAL DA PRESTAÇÃO DE SERVIÇO

Os bens a fornecer, deverão ser entregues, pelo Adjudicatário, nos Serviços Centrais da Casa Pia de Lisboa, com sede na Avenida do Restelo, 1, 1449-008 Lisboa.

5. CONTRATO

1. O contrato a celebrar integra sempre os seguintes elementos:

- a) Os suprimientos dos erros e omissões do caderno de encargos identificados pelos concorrentes, desde que esses erros e omissões tenham sido expressamente aceites pelo órgão competente para a decisão de contratar;
- b) Os esclarecimentos e as retificações relativos ao caderno de encargos;
- c) O presente caderno de encargos e seus anexos;
- d) A proposta adjudicada;
- e) Os esclarecimentos sobre a proposta adjudicada prestados pelo adjudicatário.

2. Em caso de divergência entre os documentos referidos no número anterior, a respetiva prevalência é determinada pela ordem pela qual aí são indicados.

6. OBRIGAÇÕES DO ADJUDICATÁRIO

1 Sem prejuízo de outras obrigações previstas na legislação aplicável, no presente caderno de encargos ou nas cláusulas contratuais, da celebração do contrato decorrem para o adjudicatário a obrigação de fornecer infraestruturas de equipamentos ativos de redes, firewalls e pontos de acesso.

- a) Obrigação de conformidade com as características, especificações e requisitos técnicos previstos neste caderno de encargos e seus anexos;
- b) Obrigação de pagamento de todas as despesas decorrentes da prestação de cauções.



2. A título acessório, o adjudicatário fica obrigado, designadamente, a recorrer a todos os meios necessários e adequados ao fornecimento das infraestruturas de equipamentos ativos de redes, firewalls e pontos de acesso.
3. Todas as despesas derivadas da prestação das cauções e seguros se a eles houver lugar, são da responsabilidade do adjudicatário.
4. Toda e qualquer alteração, no que respeita aos serviços contratados, carecem de uma aprovação prévia por parte da Casa Pia de Lisboa, I.P.

7. INTERLOCUTOR

O adjudicatário deverá indicar um interlocutor privilegiado, a quem competirá toda a articulação com a Casa Pia de Lisboa, I.P., para quaisquer esclarecimentos e resolução de situações urgentes.

8. PREÇO CONTRATUAL DE CONDIÇÕES DE PAGAMENTO

1. Pelo fornecimento de bens objeto do presente procedimento, bem como pelo cumprimento das demais obrigações constantes do presente caderno de encargos, a entidade adjudicante deve pagar à adjudicatária o preço previsto, constante da proposta adjudicada, acrescido de IVA à taxa legal em vigor, que não pode ultrapassar o preço base previamente estabelecido.
- 2 - Na proposta, para além dos preços unitários, deverá ser indicado o preço total e as condições de pagamento.
- 3 - O valor referido no número anterior inclui todos os custos, encargos e despesas cuja responsabilidade não esteja expressamente atribuída à Casa Pia de Lisboa, I.P, incluindo as despesas de transporte.
- 4 – A faturação será efetuada após ao fornecimento dos bens a que se refere.
- 5 - Desde que devidamente emitidas as faturas serão pagas no prazo de 30 dias, após a verificação dos formalismos legais em vigor para o processamento das despesas públicas.



- 6.- As faturas serão emitidas em nome da Casa Pia de Lisboa, IP, com referência ao número de identificação fiscal e entregues por mão própria ou remetidas por correio para a Avenida do Restelo, n.º1, 1449-008 Lisboa, Portugal.
- 7 - Em caso de discordância por parte da entidade adjudicante, quanto ao valor indicado na fatura, deve esta comunicar à entidade adjudicatária, por escrito, os respetivos fundamentos, ficando a entidade adjudicatária obrigada a prestar os esclarecimentos necessários ou proceder à emissão de nova fatura corrigida.
- 8 - Desde que devidamente emitida e observando o disposto no n.º1, a fatura será paga através de transferência bancária, após a verificação dos formalismos legais, em vigor, para o processamento das despesas públicas.
- 9 - Nas condições de pagamento a apresentar pelos concorrentes, não podem ser propostos adiantamentos por conta dos serviços a prestar.
- 10 - O atraso no pagamento das faturas confere ao fornecedor o direito de exigir juros de mora, nos termos legais.

9. NÍVEIS DE SERVIÇO

Os adjudicatários obrigam-se a cumprir os níveis de serviço referidos nas alíneas seguintes:

- a) É obrigação dos adjudicatários entregar/fornecer os bens em conformidade com o definido no caderno de encargos;
- b) O adjudicatário deve garantir o cumprimento de todas as normas ambientais aplicáveis, bem como garantir que todos os produtos, a fornecer, incluindo o seu embalamento e transporte, respeitam as exigências ambientais e de saúde pública em vigor, devendo o adjudicatário garantir a sua adequação às novas normas ou exigências que, eventualmente, possa entrar em vigor no período de vigência do contrato;

10. REVISÃO DE PREÇO

Durante a vigência do contrato não haverá lugar a revisão/atualização do preço contratado, exceto todas aquelas que se revistam de obrigatoriedade específica imposta pela lei.



CAPITULO III

PENALIDADES CONTRATUAIS E RESOLUÇÃO

11. SANÇÕES

1. No caso de incumprimento dos prazos fixados no contrato e por causa imputável ao adjudicatário, poderá ser aplicada uma sanção, calculada de acordo com a seguinte fórmula: $P=V \cdot A/500$, em que P corresponde ao montante da sanção, V é igual ao valor do fornecimento dos serviços e A é o número de dias em atraso, até ao limite de 20% do preço contratual.
2. Na determinação da gravidade do incumprimento, a Casa Pia de Lisboa I.P, tem em conta, nomeadamente, a duração da infração, a sua eventual reiteração, o grau de culpa do prestador de serviços e as consequências do incumprimento.
3. A Casa Pia de Lisboa, I.P., pode compensar os pagamentos devidos ao abrigo do contrato com as sanções pecuniárias devidas nos termos da presente cláusula.
4. O não cumprimento das cláusulas de execução do contrato, quando a sua gravidade o justifique pelos danos causados, poderá constituir fundamento para a sua rescisão imediata, independentemente das sanções previstas na lei e de outros procedimentos legais que se julgue conveniente adotar.

12. FORÇA MAIOR

1. Não podem ser impostas sanções ao adjudicatário, nem é havida como incumprimento, a não realização pontual das prestações contratuais a cargo de qualquer das partes que resulte de caso de força maior, entendendo-se como tal as circunstâncias que impossibilitem a respetiva realização, alheias à vontade da parte afetada, que ela não pudesse conhecer ou prever à data da celebração do contrato e cujos efeitos não lhe fosse razoavelmente exigível contornar ou evitar.
2. Podem constituir força maior, se se verificarem os requisitos do número anterior, designadamente, tremores de terra, inundações, incêndios, epidemias, sabotagens, greves, embargos ou bloqueios internacionais, atos de guerra ou terrorismo, motins e determinações governamentais ou administrativas injuntivas.
3. Não constituem força maior, designadamente:



- a) Circunstâncias que não constituam força maior para os subcontratados do fornecedor, na parte em que intervenham;
 - b) Greves ou conflitos laborais limitados às sociedades do fornecedor ou a grupos de sociedades em que este se integre, bem como a sociedades ou grupos de sociedades dos seus subcontratados;
 - c) Determinações governamentais, administrativas ou judiciais de natureza sancionatória ou de outra forma resultantes do incumprimento pelo fornecedor de deveres ou ónus que sobre ele recaiam;
 - d) Manifestações populares devidas ao incumprimento pelo fornecedor de normas legais;
 - e) Incêndios ou inundações com origem nas instalações do fornecedor cuja causa, propagação ou proporções se devam a culpa ou negligência sua ou ao incumprimento de normas de segurança;
 - f) Avarias nos sistemas informáticos ou mecânicos do fornecedor não devidas a sabotagem;
 - g) Eventos que estejam ou devam estar cobertos por seguros.
4. A ocorrência de circunstâncias que possam consubstanciar casos de força maior deve ser imediatamente comunicada à outra parte.
5. A força maior determina a prorrogação dos prazos de cumprimento das obrigações contratuais afetadas pelo período de tempo comprovadamente correspondente ao impedimento resultante da força maior.

13. RESOLUÇÃO DO CONTRATO

1. O incumprimento, por uma das partes, dos deveres resultantes do contrato confere, nos termos gerais de direito, à outra parte o direito de rescindir o contrato, sem prejuízo das correspondentes indemnizações legais.
2. Considera-se incumprimento dos deveres resultantes do contrato, para além das previstas no art.º 333.º do Código dos Contratos Públicos, a violação das especificações técnicas do presente caderno de encargos.



14. FORO COMPETENTE

Para resolução de todos os litígios decorrentes do contrato fica estipulada a competência do Tribunal Administrativo de Círculo de Lisboa, com expressa renúncia a qualquer outro.

CAPITULO IV

DISPOSIÇÕES FINAIS

15. SUBCONTRATAÇÃO E CESSÃO DA POSIÇÃO CONTRATUAL

A subcontratação pelo adjudicatário e a cessão da sua posição contratual depende da autorização prévia da entidade adjudicante, nos termos do Código dos Contratos Públicos.

16. MODIFICAÇÃO OBJETIVA DO CONTRATO

1. Qualquer alteração do contrato deverá constar de documento escrito, assinado por ambos os outorgantes e produzirá efeitos a partir da data da respetiva assinatura, e deverá obedecer ao estipulado nos artigos 311.º e seguintes do CCP.
2. A parte interessada na alteração deve comunicar, por escrito, à outra parte essa intenção, com uma antecedência mínima de 10 (dez) dias em relação à data em que pretende ver introduzida a alteração.
3. O contrato pode ser modificado por:
 - a) Acordo entre as partes, que não pode revestir forma menos solene do que a do contrato;
 - b) Decisão judicial ou arbitral;
 - c) Razões de interesse público.
4. A modificação do contrato com os fundamentos previstos no artigo 312.º do CCP, encontra-se sujeita aos limites e consequências estabelecidos nos artigos 313.º e 314.º do Código dos Contratos Públicos.
5. Caso as modificações representem um valor acumulado superior a 10% do preço contratual, devem as mesmas ser publicitadas nos termos do disposto do artigo 315.º do CCP.



17. CONTAGEM DOS PRAZOS

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

18. COMUNICAÇÕES E NOTIFICAÇÕES

1. Sem prejuízo de poderem ser acordadas outras regras quanto às notificações e comunicações entre as partes do contrato, estas devem ser dirigidas, nos termos do Código dos Contratos Públicos, para o domicílio ou sede contratual de cada uma, identificados no contrato a celebrar.
2. Qualquer alteração dos elementos de contacto deve ser comunicado à outra parte.

19. PATENTES, LICENÇAS E MARCAS REGISTRADAS

1. Caso existam encargos decorrentes da utilização, no fornecimento, de marcas registadas, patentes registadas ou licenças os mesmos são da responsabilidade da entidade adjudicatária.
2. Caso a entidade adjudicante venha a ser demandada por ter infringido, na execução do contrato, qualquer dos direitos mencionados no número anterior, a entidade adjudicatária indemniza-a de todas as despesas que, em consequência, haja de fazer e de todas as quantias que tenha de pagar seja a que título for.

20. SIGILO, CONFIDENCIALIDADE E PROTEÇÃO DADOS PESSOAIS

1. Todos os elementos entregues pela Casa Pia de Lisboa, I.P., no âmbito do presente procedimento, bem como em fase de execução do contrato, são fornecidos sob reserva de confidencialidade, não podendo ser divulgados por qualquer forma, sem prévia autorização escrita da Casa Pia de Lisboa, I.P., restringindo-se a sua utilização ao prosseguimento do fim a que se destinam.
2. O adjudicatário garantirá o sigilo quanto a informações, designadamente de carácter fiscal, que os seus trabalhadores venham a ter acesso relacionadas com a atividade da Casa Pia de Lisboa, I.P.



3. Cabe ao adjudicatário assegurar que as pessoas ou entidades que tiverem acesso à informação sujeita a sigilo referida no número anterior, assumam perante si um compromisso de confidencialidade, limitando a divulgação de informação exclusivamente às pessoas ou entidades que dela tenham de tomar conhecimento para tornar possível a sua intervenção nos processos em que intervêm.
4. O adjudicatário assumirá direta e pessoalmente a responsabilidade por qualquer dano patrimonial ou moral que a Casa Pia de Lisboa, I.P ou qualquer terceiro venha a sofrer em consequência de ato, ação ou omissão, praticado, dolosa ou negligentemente, por qualquer dos seus colaboradores, em violação do dever de sigilo a que estão obrigados.
5. O adjudicatário obriga-se ainda, durante a vigência do contrato e após a sua cessação, a cumprir toda a legislação em vigor relativa à proteção de dados pessoais e a não ceder, revelar, utilizar ou discutir, com quaisquer terceiros, todas e quaisquer informações e/ou elementos que lhe tenham sido confiados pela Entidade Adjudicante ou de que tenha tido conhecimento ou acesso no âmbito do presente contrato ou por causa dele.
6. Sempre que, no âmbito do presente contrato, o Segundo Outorgante tenha de proceder ou efetuar operações de tratamento automatizado ou manual de dados pessoais, o mesmo obriga-se a cumprir rigorosamente o disposto na legislação aplicável em matéria de tratamento de dados pessoais e nomeadamente a:
 - a) Manter a confidencialidade desses dados, podendo apenas facultá-los aos trabalhadores alocados à prestação dos serviços, na medida do estritamente necessário à referida prestação;
 - b) Tratar os dados, única e exclusivamente para efeitos da prestação dos serviços objeto deste contrato, em estrita observância das instruções transmitidas pela Casa Pia de Lisboa;
 - c) Adotar todas as medidas técnicas e organizativas apropriadas a assegurar um nível de segurança adequado à proteção dos dados, e a existência de mecanismos/processos que permitam testar, apreciar e avaliar regularmente a eficácia dessas medidas;



- d) Não copiar, reproduzir, adaptar, modificar, alterar, apagar, destruir, difundir, transmitir, divulgar ou, por qualquer outra forma, colocar à disposição de terceiros os dados, sem que para tal tenha sido expressamente autorizada;
 - e) Prestar apoio ao responsável pelo tratamento de dados da CPL em caso de exercício de direitos pelos titulares;
 - f) Exigir aos trabalhadores afetos à prestação de serviços, igual dever de confidencialidade e proteção dos dados pessoais;
 - g) Prestar assistência ao responsável pelo tratamento de dados da CPL no sentido de assegurar o cumprimento das obrigações que recaem sobre o mesmo (segurança, notificações de violações de segurança, avaliações de impacto);
 - h) Colaborar nas auditorias levadas a cabo pelo responsável pelo tratamento de dados;
 - i) Apagar ou devolver (consoante a escolha do responsável pelo tratamento de dados) todos os dados pessoais depois de concluída a prestação de serviços, apagando as cópias existentes, salvo se a conservação dos dados seja exigida ao abrigo de legislação específica na matéria;
 - j) Obter autorização expressa pela Casa Pia de Lisboa para eventual subcontratação do serviço, ficando o subcontratante sujeito às mesmas obrigações de proteção de dados a que está sujeito o Segundo Outorgante.
7. O Adjudicatário será responsável por qualquer prejuízo em que a Entidade Adjudicante venha a incorrer em consequência do tratamento, por parte da mesma e/ou dos seus trabalhadores, de dados pessoais em violação das normas legais aplicáveis e/ou do disposto no contrato.
8. Para efeitos do disposto no número anterior da presente cláusula entende-se por “trabalhador” toda e qualquer pessoa singular ou coletiva que preste serviços ao Adjudicatário, incluindo, designadamente, representantes legais, trabalhadores, prestadores de serviços, procuradores e consultores, independentemente da natureza e validade do vínculo jurídico estabelecido entre o Segundo Outorgante e o referido trabalhador.
9. A obrigação de sigilo prevista na presente cláusula mantém-se mesmo após a cessação



21. LEGISLAÇÃO APLICAVEL

Em tudo o que for omissa e que suscite dúvidas no presente contrato, reger-se-á pela lei geral aplicável aos contratos administrativos, bem como ao regime jurídico do Código dos Contratos Públicos, na sua versão atualizada e republicado pelo Decreto-Lei n.º 111-B/2017, de 31 de agosto, e retificado pelas declarações de retificação n.ºs 36-A/2017, de 30/10 e 42/2017 de 30/11, e demais legislação aplicável em razão da matéria.



PARTE II ESPECIFICAÇÕES TÉCNICAS

Especificações Técnicas

Atendendo à evolução dos modelos de ensino com crescente incorporação de diversificadas ferramentas tecnológicas e a amplificação do conceito de Escola Digital torna-se necessário ajustar a estrutura de wireless presente nos 5 Centros de Educação e Desenvolvimento (CED) da Casa Pia de Lisboa I.P. (CPL) onde ocorre ensino e formação.

São pressupostos desta implementação:

- aproveitamento de infraestrutura já presente na CPL
- simplificação da infraestrutura
- maior flexibilidade e gestão de recursos
- garantia de integração e correlação de soluções
- a solução a apresentar deverá ser integralmente do mesmo fabricante

Neste sentido pretende adquirir as seguintes soluções:

- Firewalls – 3 equipamentos
 - Firewall do Tipo 1 – 1 equipamento
 - Firewall do Tipo 2 – 2 equipamentos
- Pontos de Acesso Wireless Internos – 250 equipamentos
- Pontos de acesso Wireless Externos – 5 equipamentos
- Switch Centralizador
 - Switch de core – 2 equipamentos
 - Switch de acesso tipo 1 – 5 equipamentos
- Switch de ligação – 9 equipamentos
- Switch de ligação fibra – 5 equipamentos
 - Switch de ligação fibra tipo 1 – 1 equipamento
 - Switch de ligação fibra tipo 2 – 4 equipamentos



. **Firewalls – 3 equipamentos**

A. Firewalls tipo 1 – 1 equipamento

Pretende-se o fornecimento de uma firewall, devendo o equipamento garantir as seguintes funcionalidades e especificações técnicas:

a) Ao nível da 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 trunk)
 - Software switch
- Routing estáticos 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, RIPv6, 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 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 com capacidade para suportar até um mínimo de 120 pontos de acesso wireless
- Controlador Switching integrado com capacidade para suportar até um mínimo de 60 equipamentos de switching.
- Controlador de switch com funcionalidade de NAC.
- Controlador wireless com funcionalidade NAC.
- Virtualização da solução em contextos.

b) Ao nível da 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
 - Cliente VPN
 - 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
 - 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
- c) Ao nível de Firewall:
- Modos de operação NAT/route e transparente/bridge



- Agendamento de políticas: recorrentes ou apenas uma vez
- Suporte para tráfego VoIP: SIP/H.323 /SCCP NAT traversal
- 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: predefinidos, 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.
- 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.

d) Ao nível de 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
 - 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)
- 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
- Validação da integridade do dispositivo cliente e do sistema operativo;
- Opção para limpeza de cache aquando da terminação 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.

e) Ao nível de controlo de aplicações:

- Detecção de mais de 3000 aplicações distintas organizadas por categorias
- Definição de aplicações customizadas
- Controlo avançado de aplicações tipo 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
- Detecção de aplicações mesmo dentro de ligações proxy
- Diferentes ações de controlo de aplicações: bloquear, reset de sessão, monitorização, aplicação de gestão de largura de banda
- Inspeção SSL

f) Ao nível da 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 perda 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 equipamento geograficamente dispersos



- Opção de sincronização de sessões em equipamentos configurados em modo Standalone ou Cluster geográfico

g) Ao nível da 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
- 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 (incluído de terceiras partes) através de scripts CLI e APIs.
- Wizards de configuração para implementação rápida da solução.
- Integração com soluções de Public SDN:
 - Amazon Web Services (AWS)
 - Microsoft Azure
 - Google Cloud Platform (GCP)



- Oracle Cloud Infrastructure (OCI)
- AliCloud
- Integração com solução de Private SDN:
 - Kubernetes
 - VMware ESXi
 - VMware NSX
 - Openstack (Horizon)
 - Application Centric Infrastructure (ACI)
 - Nuage Virtualized Services Platform e Cisco ACI.
- h) Ao nível da conectividade, deverão ser asseguradas as características mínimas:
 - Interfaces 10G SFP+ Slots: 4 (deverão ser fornecidos 1 transceivers e cabo de 10G SFP+)
 - Interfaces 1GbE SFP Slots: 8 (deverão ser fornecidos 2 transceivers e cabos de 1G SFP)
 - Interfaces GbE 10/100/1000: 16
 - GE RJ45 Management / HA Ports: 1
 - Console Port (RJ45): 1
- i) Ao nível do sistema, deverão ser asseguradas as características mínimas:
 - Onboard Storage: 1x 480 GB SSD
- j) Ao nível do desempenho, deverão ser asseguradas as características mínimas:
 - 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): 27 / 27 / 11 Gbps
 - Latência de firewall (pacotes UDP de 64 bytes): 4.78 µs
 - Débito firewall (pacotes por segundo): 16.5 Mpps



- Sessões TCP concorrentes: 3 Milhões
- Novas sessões/segundo (TCP): 280.000
- Políticas de firewall: 10.000
- Débito VPN IPsec (pacotes 512 bytes): 13 Gbps
- Túneis IPsec Gateway-to-Gateway: 2.500
- Túneis IPsec cliente remoto: 16.000
- Débito VPN SSL: 2 Gbps
- Débito IPS: 5 Gbps
- Débito de inspeção SSL: 3.5 Gbps
- Inspeção SSL CPS (IPS, HTTPS diversas cifras): 3.500
- Débito de inspeção SSL para sessões concorrentes: 300.000
- Débito de Application Control: 13 Gbps
- Débito NGFW: 3.5 Gbps
- Débito Threat Protection: 3 Gbps
- Domínios Virtuais (por defeito / máximo): 10 / 10
- Máximo de Tokens: 5.000
- Licenciamento ilimitado de utilizadores: SIM

k) O equipamento deverá assegurar as seguintes certificações:

- ICSA Labs: Firewall, IPsec, IPS, Antivirus, SSL-VPN, IPv6

B. Firewalls tipo 2 - 2 equipamentos

Pretende-se o fornecimento de duas firewalls para duas localizações distintas, devendo os equipamentos garantir as seguintes funcionalidades e especificações técnicas:

a) Ao nível da 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 trunk)
 - Software switch
- Routing estáticos 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, RIPv6, 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 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 com capacidade para suportar até um mínimo de 120 pontos de acesso wireless
- Controlador Switching integrado com capacidade para suportar até um mínimo de 60 equipamentos de switching.
- Controlador de switch com funcionalidade de NAC.
- Controlador wireless com funcionalidade NAC.
- Virtualização da solução em contextos.

b) Ao nível da 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
 - Cliente VPN
 - 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
 - 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
- c) Ao nível de Firewall:
- Modos de operação NAT/route e transparente/bridge
 - Agendamento de políticas: recorrentes ou apenas uma vez
 - Suporte para tráfego VoIP: SIP/H.323 /SCCP NAT traversal,
 - 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: predefinidos, 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.
- 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.

d) Ao nível de 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
 - 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)
 - 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
- Validação da integridade do dispositivo cliente e do sistema operativo;
- Opção para limpeza de cache aquando da terminação 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.

e) Ao nível de controlo de aplicações:

- Detecção de mais de 3000 aplicações distintas organizadas por categorias
- Definição de aplicações customizadas
- Controlo avançado de aplicações tipo 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
- Detecção de aplicações mesmo dentro de ligações proxy



- Diferentes ações de controlo de aplicações: bloquear, reset de sessão, monitorização, aplicação de gestão de largura de banda
- Inspeção SSL

f) Ao nível da 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 perda 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 equipamento geograficamente dispersos
- Opção de sincronização de sessões em equipamentos configurados em modo Standalone ou Cluster geográfico

g) Ao nível da 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
- 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 (incluído de terceiras partes) através de scripts CLI e APIs.
- Wizards de configuração para implementação rápida da solução.
- Integração com soluções de Public SDN:
 - Amazon Web Services (AWS)
 - Microsoft Azure
 - Google Cloud Platform (GCP)
 - Oracle Cloud Infrastructure (OCI)
 - AliCloud
- Integração com solução de Private SDN:
 - Kubernetes
 - VMware ESXi
 - VMware NSX
 - Openstack (Horizon)



- Application Centric Infrastructure (ACI)
- Nuage Virtualized Services Platform e Cisco ACI.

h) Ao nível da conectividade, deverão ser asseguradas as características mínimas:

- Interfaces 10G SFP+ Slots: 2 (deverão ser fornecidos 1 transceivers e cabo de 10G SFP+ por equipamento)
- Interfaces 1GbE SFP Slots: 8 (deverão ser fornecidos 2 transceivers e cabo de 1G SFP por equipamento)
- Interfaces GbE 10/100/1000: 18
- GE RJ45 Management / HA Ports: 1
- Console Port (RJ45): 1

i) Ao nível do sistema, deverão ser asseguradas as características mínimas:

- Onboard Storage: 1x 480 GB SSD

j) Ao nível do desempenho, deverão ser asseguradas as características mínimas:

- 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): 20 / 18 / 10 Gbps
- Latência de firewall (pacotes UDP de 64 bytes): 4.97 µs
- Débito firewall (pacotes por segundo): 15 Mpps
- Sessões TCP concorrentes: 1.5 Milhões
- Novas sessões/segundo (TCP): 56.000
- Políticas de firewall: 10.000
- Débito VPN IPSec (pacotes 512 bytes): 11.5 Gbps
- Túneis IPsec Gateway-to-Gateway: 2.000



- Túneis IPSec cliente remoto: 16.000
- Débito VPN SSL: 1 Gbps
- Débito IPS: 2.6 Gbps
- Débito de inspeção SSL: 1 Gbps
- Débito de Application Control: 2.2 Gbps
- Débito NGFW: 1.6 Gbps
- Débito Threat Protection: 1 Gbps
- Domínios Virtuais (por defeito / máximo): 10 / 10
- Máximo de Tokens: 5.000
- Licenciamento ilimitado de utilizadores: SIM

k) O equipamento deverá assegurar as seguintes certificações:

- ICSA Labs: Firewall, IPsec, IPS, Antivirus, SSL-VPN, IPv6

. Pontos de Acesso Wireless Internos – 250

Pretende-se o fornecimento de 250 pontos de acesso wireless internos, devendo os equipamentos garantir as seguintes funcionalidades e especificações técnicas:

- 802.11ax
- Tipo de ponto de acesso: Indoor
- Número de rádios: 3 + 1 BLE
- Número de antenas: 5 internas + 1 interna BLE
- Antenas: 4 dBi para 2.4 GHz, 5 dBi para 5 GHz
- Bandas de frequência (GHz): 2.400–2.4835, 5.150–5.250, 5.250–5.350, 5.470–5.725, 5.725–5.850
- Capacidades do Radio 1: 2.4 GHz 20/40 MHz (BPSK, QPSK, QAM64, QAM256, e QAM1024)



- Capacidades do Radio 2: 5 GHz 4x4 20/40/80 MHz
- Taxa máxima de dados:
 - Radio 1: até 1100 Mbps,
 - Radio 2: até 2400 Mbps
- SSIDs simultâneos (Máximo): 16
- Suporte para os seguintes tipos EAP: EAP-TLS, EAP-TTLS/MSCHAPv2, EAPv0/EAP-MSCHAPv2, PEAPv1/EAP-GTC, EAP-SIM, EAP-AKA, EAP-FAST
- Autenticação de Utilizadores/Dispositivos: WPA, WPA2, e WPA3 com 802.1x ou Preshared key, WEP, Web Captive Portal, MAC blocklist & allowlist
- Tipos de SSID suportados: Local-Bridge, Tunnel, Mesh
- Especificações IEEE: 802.11a, 802.11b, 802.11e, 802.11g, 802.11h, 802.11i, 802.11j, 802.11k, 802.11n, 802.11r, 802.11v, 802.11ac, 802.11ax (Wi-Fi 6), 802.1X, 802.3ad, 802.3af, 802.3at, 802.3az
- Coexistência celular: Sim
- Modo LED desligado: Sim
- OFDMA
- WIDS
- Deverá permitir funcionalidades de análise de espectro
- O equipamento deverá funcionar em modo Remote Access Point
- O equipamento deverá permitir a descoberta automática de Controladores de Equipamentos Wi-Fi e efetuar o download de configurações para instalações plug-and-play
- O equipamento deverá ter suporte para SNMP
- O equipamento deverá permitir ser gerido via cloud
- Possibilidade de gerar relatórios de todos os eventos e performance através de uma plataforma centralizada
- Possibilidade de monitorizar o estado do equipamento a partir de uma



plataforma centralizada

- Certificação Wi-Fi Alliance

• **Pontos de Acesso Wireless Externos – 5**

Pretende-se o fornecimento de 5 pontos de acesso wireless externos, devendo os equipamentos garantir as seguintes funcionalidades e especificações técnicas:

- 802.11ax
- Tipo de ponto de acesso: Indoor/Outdoor
- Número de rádios: 3 + 1 BLE
- Número de antenas: 3 internas dual band + 1 interna BLE/Zigbee
- Antenas: 10dBi para 2.4 GHz, 10 dBi para 5 GHz
- Bandas de frequência (GHz): 2.400–2.4835, 5.150–5.250, 5.250–5.350, 5.470–5.725, 5.725–5.850
- Taxa máxima de dados:
 - Radio 1: até 574 Mbps,
 - Radio 2: até 1200 Mbps
- SSIDs simultâneos (Máximo): 16
- Interfaces: 2x10/100/1000 RJ45 e 1x RS232 Serial Port
- Suporte para os seguintes tipos EAP: EAP-TLS, EAP-TTLS/MSCHAPv2, EAPv0/EAP-MSCHAPv2, PEAPv1/EAP-GTC, EAP-SIM, EAP-AKA, EAP-FAST
- Autenticação de Utilizadores/Dispositivos: WPA, WPA2, e WPA3 com 802.1x ou Preshared key, WEP, Web Captive Portal, MAC blocklist & allowlist
- Tipos de SSID suportados: Local-Bridge, Tunnel, Mesh
- Especificações IEEE: 802.11a, 802.11b, 802.11d, 802.11e, 802.11g, 802.11h, 802.11i, 802.11j, 802.11k, 802.11n, 802.11r, 802.11v, 802.11w, 802.11ac, 802.11ax (Wi-Fi 6), 802.1Q, 802.1X, 802.3ad, 802.3af, 802.3at, 802.3az,



802.3bz.

- OFDMA
- WIDS
- Deverá permitir funcionalidades de análise de espectro
- O equipamento deverá funcionar em modo Remote Access Point
- O equipamento deverá permitir a descoberta automática de Controladores de Equipamentos Wi-Fi e efetuar o download de configurações para instalações plug-and-play
- O equipamento deverá ter suporte para SNMP
- O equipamento deverá permitir ser gerido via cloud
- Possibilidade de monitorizar o estado do equipamento a partir de uma plataforma centralizada.

. Switch Centralizador

A. Switch de core – 2 equipamentos

Pretende-se o fornecimento de 2 switch de core, devendo cada um dos equipamentos garantir as seguintes funcionalidades e especificações técnicas:

a) Ao nível dos requisitos de gestão:

- O equipamento deverá permitir o acesso Telnet / SSH
- O equipamento deverá permitir o acesso HTTP / HTTPS
- O equipamento deverá permitir o acesso via CLI e web GUI interface
- O equipamento deverá permitir configurar SNMP v1/v2c/v3
- O equipamento deverá permitir configurar Sntp
- O equipamento deverá suportar LLDP (802.1ab, Link Layer Discovery Protocol) (receive and transmit)
- O equipamento deverá suportar Loop-guard



- O equipamento deverá suportar software download/upload: TFTP/FTP/GUI
- O equipamento deverá suportar Auto Discovery of Multiple Switches
- O equipamento deverá suportar permitir a configuração de VLANs
- O equipamento deverá suportar Syslog Collection
- Deverá ser possível gerir o equipamento através de uma Firewall
- O equipamento deverá suportar HTTP REST APIs para configuração e monitorização

b) Ao nível da alta disponibilidade:

- Multi-Chassis Link Aggregation (MCLAG)

c) Ao nível dos requisitos de segurança:

- O equipamento deverá permitir 802.1x Port Authentication
- O equipamento deverá permitir TACACS+/RADIUS Admin Access
- O equipamento deverá permitir Port Mirroring
- O equipamento deverá permitir Admin Authentication Via RFC 2865 RADIUS
- O equipamento deverá permitir 802.1x authentication with port-based assignment
- O equipamento deverá permitir 802.1x authentication with mac-based assignment
- O equipamento deverá permitir 802.1x Guest and Fallback VLAN
- O equipamento deverá permitir 802.1x MAC Address Bypass (MAB)
- O equipamento deverá permitir 802.1x Dynamic VLAN Assignment
- O equipamento deverá permitir sFlow
- O equipamento deverá permitir ACL Tables
- O equipamento deverá permitir QOS: 802.1p support
- O equipamento deverá permitir VLAN tag by ACL
- O equipamento deverá permitir VLAN tag by MAC/IP/802.1x

d) Ao nível dos requisitos de Routing:

- O equipamento deverá permitir Inter-VLAN Routing



- O equipamento deverá permitir Static Routing (Hardware-based)
- O equipamento deverá permitir L3 Host/ARP Entries
- O equipamento deverá permitir Static BFD (Bidirectional Forwarding Detection)
- O equipamento deverá suportar OSPFv2, RIPv2, VRRP
- O equipamento deverá suportar ECMP

e) Ao nível dos requisitos de Layer 2:

- O equipamento deverá suportar Jumbo Frames
- O equipamento deverá suportar auto negociação da velocidade dos portos e duplex
- O equipamento deverá suportar IEEE 802.1D MAC Bridging/STP
- O equipamento deverá suportar IEEE 802.1w Rapid Spanning Tree Protocol
- O equipamento deverá suportar IEEE 802.1s Multiple Spanning Tree Protocol (MSTP)
- O equipamento deverá suportar Edge Port / Port Fast
- O equipamento deverá suportar IEEE 802.1Q VLAN Tagging
- O equipamento deverá suportar IEEE 802.3ad Link Aggregation com LACP
- O equipamento deverá suportar balanceamento de tráfego Unicast/Multicast sobre portos em trunk (dst-ip, dst-mac, src-dst-ip, src-dst-mac, src-ip, src-mac)
- O equipamento deverá suportar IEEE 802.1AX Link Aggregation
- O equipamento deverá suportar Spanning Tree Instances (MSTP/CST)
- O equipamento deverá suportar IEEE 802.3x Flow Control and back-pressure
- O equipamento deverá suportar IEEE 802.3 10Base-T
- O equipamento deverá suportar IEEE 802.3u 100Base-TX
- O equipamento deverá suportar IEEE 802.3z 1000Base-SX/LX
- O equipamento deverá suportar IEEE 802.3ab 1000Base-T
- O equipamento deverá suportar IEEE 802.3 CSMA/CD Access Method and Physical Layer Specifications



- O equipamento deverá suportar MAC, IP, Ethertype-based VLANs
 - O equipamento deverá suportar Virtual-Wire
- f) Ao nível dos requisitos de serviços:
- O equipamento deverá suportar IGMP Snooping
 - O equipamento deverá suportar IP conflict detection & notification
- g) Ao nível do suporte de RFC e MIB:
- RFC 2571 Architecture for Describing SNMP Framework
 - DHCP relay feature
 - DHCP Snooping
 - RFC 2865 RADIUS
 - RFC 1643 Ethernet-like Interface MIB
 - RFC 1213 MIB-II
 - RFC 1354 IP Forwarding Table MIB
 - RFC 2572 SNMP Message Processing and Dispatching
 - RFC 1573 SNMP MIB II
 - RFC 1157 SNMPv1/v2c
 - RFC 2030 SNTP
- h) Ao nível da conectividade e sistema deverão ser asseguradas as características mínimas:
- Nº total de interfaces:
 - 48x GE/10 GE SFP+ ports (deverão ser fornecidos 10 transceivers e cabos de 10G SFP+ por equipamento)
 - 6x 40GE QSPF+ ports or 4x 100 GE QSFP28 ports (deverão ser fornecidos 1 transceivers e cabo 40GE QSPF+ por equipamento)
 - Interface de gestão dedicada 10/100/1000 Mbps: 1
 - Interface Consola RJ45: 1



- Modo de gestão: Web, CLI e Firewall
- Capacidade de switching (Duplex): 1760 Gbps
- Pacotes por segundo (Duplex): 2620 Mpps
- Armazenamento de MAC addresses: 144 000
- Latência: < 800 ns
- Número de VLANs suportadas: 4000
- Tamanho do grupo Link Aggregation Group: até 48
- Capacidade da DRAM: 8 GB
- Capacidade da FLASH: 128 MBs
- Fonte de alimentação redundante: SIM (hot swappable)
- Temperatura de funcionamento: 0 - 45 °C
- Humidade: 10 ate 95% sem condensação
- Altura: 1RU

B. Switch de acesso tipo 1 – 5 equipamentos

Para garantir as necessidades de portas a cobre no CORE pretende-se a aquisição de 5 switches de acesso com PoE, devendo cada um dos equipamentos garantir as seguintes funcionalidades e especificações técnicas:

a) Ao nível dos requisitos de gestão:

- O equipamento deverá permitir o acesso Telnet / SSH
- O equipamento deverá permitir o acesso HTTP / HTTPS
- O equipamento deverá permitir o acesso via CLI e web GUI interface
- O equipamento deverá permitir configurar SNMP v1/v2c/v3
- O equipamento deverá permitir configurar SNTp
- O equipamento deverá suportar LLDP (802.1ab, Link Layer Discovery Protocol) (receive and transmit)



- O equipamento deverá suportar Loop-guard
- O equipamento deverá suportar POE-pre-standard detection
- O equipamento deverá suportar software download/upload: TFTP/FTP/GUI
- O equipamento deverá suportar Auto Discovery of Multiple Switches
- O equipamento deverá suportar permitir a configuração de VLANs
- O equipamento deverá suportar Syslog Collection
- Deverá ser possível gerir o equipamento através de uma Firewall
- O equipamento deverá suportar HTTP REST APIs para configuração e monitorização

b) Ao nível da alta disponibilidade:

- Multi-Chassis Link Aggregation (MCLAG)

c) Ao nível de requisitos de segurança:

- O equipamento deverá permitir 802.1x Port Authentication
- O equipamento deverá permitir TACACS+/RADIUS Admin Access
- O equipamento deverá permitir Port Mirroring
- O equipamento deverá permitir Admin Authentication Via RFC 2865 RADIUS
- O equipamento deverá permitir 802.1x authentication with port-based assignment
- O equipamento deverá permitir 802.1x authentication with mac-based assignment
- O equipamento deverá permitir 802.1x Guest and Fallback VLAN
- O equipamento deverá permitir 802.1x MAC Address Bypass (MAB)
- O equipamento deverá permitir 802.1x Dynamic VLAN Assignment
- O equipamento deverá permitir sFlow
- O equipamento deverá permitir ACL Tables
- O equipamento deverá permitir QOS: 802.1p support
- O equipamento deverá permitir VLAN tag by ACL
- O equipamento deverá permitir VLAN tag by MAC/IP/802.1x



d) Ao nível dos requisitos de Routing

- O equipamento deverá permitir Inter-VLAN Routing
- O equipamento deverá permitir Static Routing (Software-based only) routing (like management traffic)
- O equipamento deverá permitir Static Routing (Hardware-based)
- O equipamento deverá permitir L3 Host/ARP Entries
- O equipamento deverá permitir Static BFD (Bidirectional Forwarding Detection)

e) Ao nível dos requisitos de Layer 2

- O equipamento deverá suportar Jumbo Frames
- O equipamento deverá suportar auto negociação da velocidade dos portos e duplex
- O equipamento deverá suportar IEEE 802.1D MAC Bridging/STP
- O equipamento deverá suportar IEEE 802.1w Rapid Spanning Tree Protocol
- O equipamento deverá suportar IEEE 802.1s Multiple Spanning Tree Protocol (MSTP)
- O equipamento deverá suportar Edge Port / Port Fast
- O equipamento deverá suportar IEEE 802.1Q VLAN Tagging
- O equipamento deverá suportar IEEE 802.3ad Link Aggregation com LACP
- O equipamento deverá suportar balanceamento de tráfego Unicast/Multicast sobre portos em trunk (dst-ip, dst-mac, src-dst-ip, src-dst-mac, src-ip, src-mac)
- O equipamento deverá suportar IEEE 802.1AX Link Aggregation
- O equipamento deverá suportar Spanning Tree Instances (MSTP/CST)
- O equipamento deverá suportar IEEE 802.3x Flow Control and back-pressure
- O equipamento deverá suportar IEEE 802.3 10Base-T
- O equipamento deverá suportar IEEE 802.3u 100Base-TX
- O equipamento deverá suportar IEEE 802.3z 1000Base-SX/LX
- O equipamento deverá suportar IEEE 802.3ab 1000Base-T
- O equipamento deverá suportar 802.3 CSMA/CD Access Method and Physical Layer



Specifications

- O equipamento deverá suportar MAC, IP, Ethertype-based VLANs
 - O equipamento deverá suportar Virtual-Wire
- f) Ao nível dos requisitos de serviços
- O equipamento deverá suportar IGMP Snooping
 - O equipamento deverá suportar IP conflict detection & notification
- g) Ao nível dos requisitos do suporte de RFC e MIB
- RFC 2571 Architecture for Describing SNMP Framework
 - DHCP relay feature
 - DHCP Snooping
 - RFC 2865 RADIUS
 - RFC 1643 Ethernet-like Interface MIB
 - RFC 1213 MIB-II
 - RFC 1354 IP Forwarding Table MIB
 - RFC 2572 SNMP Message Processing and Dispatching
 - RFC 1573 SNMP MIB II
 - RFC 1157 SNMPv1/v2c
 - RFC 2030 SNTP
- h) Ao nível da conectividade e sistema deverão ser asseguradas as características mínimas:
- Nº total de interfaces:
 - 48x GE RJ45 PoE
 - 4x 10 GE SFP+ (deverão ser fornecidos 2 transceivers e cabos de 10G SFP+ por equipamento)
 - Interface de gestão dedicada 10/100 Mbps: 1



- Interface Consola RJ45: 1
- Budget de PoE mínimo: 421W
- Modo de gestão: Web, CLI e Firewall
- Capacidade de switching (Duplex): 176 Gbps
- Pacotes por segundo (Duplex): 262 Mpps
- Armazenamento de MAC addresses: 32000
- Latência: < 1µs
- Número de VLANs suportadas: 4000
- Tamanho do grupo Link Aggregation Group: até 8
- Capacidade da DRAM: 1 GB
- Capacidade da FLASH: 256 MBs
- Fonte de alimentação redundante: SIM
- Temperatura de funcionamento: 0 - 50 °C
- Humidade: 20 ate 90% sem condensação
- Altura: 1RU

. Switch de ligação – 9 equipamentos

Para garantir as ligações em diversas localizações pretende-se a aquisição de 9 switches de ligação com PoE, devendo cada um dos equipamentos garantir as seguintes funcionalidades e especificações técnicas:

a) Ao nível dos requisitos de gestão:

- O equipamento deverá permitir o acesso Telnet / SSH
- O equipamento deverá permitir o acesso HTTP / HTTPS
- O equipamento deverá permitir o acesso via CLI e web GUI interface
- O equipamento deverá permitir configurar SNMP v1/v2c/v3



- O equipamento deverá permitir configurar SNMP
- O equipamento deverá suportar LLDP (802.1ab, Link Layer Discovery Protocol) (receive and transmit)
- O equipamento deverá suportar Loop-guard
- O equipamento deverá suportar POE-pre-standard detection
- O equipamento deverá suportar software download/upload: TFTP/FTP/GUI
- O equipamento deverá suportar Auto Discovery of Multiple Switches
- O equipamento deverá suportar permitir a configuração de VLANs
- O equipamento deverá suportar Syslog Collection
- Deverá ser possível gerir o equipamento através de uma Firewall
- O equipamento deverá suportar HTTP REST APIs para configuração e monitorização

b) Ao nível da alta disponibilidade:

- Multi-Chassis Link Aggregation (MCLAG)

c) Ao nível de requisitos de segurança:

- O equipamento deverá permitir 802.1x Port Authentication
- O equipamento deverá permitir TACACS+/RADIUS Admin Access
- O equipamento deverá permitir Port Mirroring
- O equipamento deverá permitir Admin Authentication Via RFC 2865 RADIUS
- O equipamento deverá permitir 802.1x authentication with port-based assignment
- O equipamento deverá permitir 802.1x authentication with mac-based assignment
- O equipamento deverá permitir 802.1x Guest and Fallback VLAN
- O equipamento deverá permitir 802.1x MAC Address Bypass (MAB)
- O equipamento deverá permitir 802.1x Dynamic VLAN Assignment
- O equipamento deverá permitir sFlow
- O equipamento deverá permitir ACL Tables



- O equipamento deverá permitir QOS: 802.1p support
- O equipamento deverá permitir VLAN tag by ACL
- O equipamento deverá permitir VLAN tag by MAC/IP/802.1x

d) Ao nível dos requisitos de Routing

- O equipamento deverá permitir Inter-VLAN Routing
- O equipamento deverá permitir Static Routing (Software-based only) routing (like management traffic)
- O equipamento deverá permitir Static Routing (Hardware-based)
- O equipamento deverá permitir L3 Host/ARP Entries
- O equipamento deverá permitir Static BFD (Bidirectional Forwarding Detection)

e) Ao nível dos requisitos de Layer 2

- O equipamento deverá suportar Jumbo Frames
- O equipamento deverá suportar auto negociação da velocidade dos portos e duplex
- O equipamento deverá suportar IEEE 802.1D MAC Bridging/STP
- O equipamento deverá suportar IEEE 802.1w Rapid Spanning Tree Protocol
- O equipamento deverá suportar IEEE 802.1s Multiple Spanning Tree Protocol (MSTP)
- O equipamento deverá suportar Edge Port / Port Fast
- O equipamento deverá suportar IEEE 802.1Q VLAN Tagging
- O equipamento deverá suportar IEEE 802.3ad Link Aggregation com LACP
- O equipamento deverá suportar balanceamento de tráfego Unicast/Multicast sobre portos em trunk (dst-ip, dst-mac, src-dst-ip, src-dst-mac, src-ip, src-mac)
- O equipamento deverá suportar IEEE 802.1AX Link Aggregation
- O equipamento deverá suportar Spanning Tree Instances (MSTP/CST)
- O equipamento deverá suportar IEEE 802.3x Flow Control and back-pressure
- O equipamento deverá suportar IEEE 802.3 10Base-T



- O equipamento deverá suportar IEEE 802.3u 100Base-TX
 - O equipamento deverá suportar IEEE 802.3z 1000Base-SX/LX
 - O equipamento deverá suportar IEEE 802.3ab 1000Base-T
 - O equipamento deverá suportar 802.3 CSMA/CD Access Method and Physical Layer Specifications
 - O equipamento deverá suportar MAC, IP, Ethertype-based VLANs
 - O equipamento deverá suportar Virtual-Wire
- f) Ao nível dos requisitos de serviços
- O equipamento deverá suportar IGMP Snooping
 - O equipamento deverá suportar IP conflict detection & notification
- g) Ao nível dos requisitos do suporte de RFC e MIB
- RFC 2571 Architecture for Describing SNMP Framework
 - DHCP relay feature
 - DHCP Snooping
 - RFC 2865 RADIUS
 - RFC 1643 Ethernet-like Interface MIB
 - RFC 1213 MIB-II
 - RFC 1354 IP Forwarding Table MIB
 - RFC 2572 SNMP Message Processing and Dispatching
 - RFC 1573 SNMP MIB II
 - RFC 1157 SNMPv1/v2c
 - RFC 2030 SNTP
- h) Ao nível da conectividade e sistema deverão ser asseguradas as características mínimas:
- Nº total de interfaces:



- 48x GE RJ45 PoE
 - 4x 10 GE SFP+ (deverão ser fornecidos 2 transceivers e cabos de 10G SFP+ por equipamento)
- Interface de gestão dedicada 10/100 Mbps: 1
- Interface Consola RJ45: 1
- Budget de PoE mínimo: 421W
- Modo de gestão: Web, CLI e Firewall
- Capacidade de switching (Duplex): 176 Gbps
- Pacotes por segundo (Duplex): 262 Mpps
- Armazenamento de MAC addresses: 32000
- Latência: < 1µs
- Número de VLANs suportadas: 4000
- Tamanho do grupo Link Aggregation Group: até 8
- Capacidade da DRAM: 1 GB
- Capacidade da FLASH: 256 MBs
- Fonte de alimentação redundante: SIM
- Temperatura de funcionamento: 0 - 50 °C
- Humidade: 20 ate 90% sem condensação
- Altura: 1RU

• **Switch de ligação fibra – 5 equipamentos**

A. Switch de ligação fibra tipo 1 – 1 equipamento

Pretende-se a aquisição de 1 switches de ligação de fibra tipo 1 devendo cada o equipamento garantir as seguintes funcionalidades e especificações técnicas:

a) Ao nível dos requisitos de gestão:

- O equipamento deverá permitir o acesso Telnet / SSH



- O equipamento deverá permitir o acesso HTTP / HTTPS
- O equipamento deverá permitir o acesso via CLI e web GUI interface
- O equipamento deverá permitir configurar SNMP v1/v2c/v3
- O equipamento deverá permitir configurar SNTp
- O equipamento deverá suportar LLDP (802.1ab, Link Layer Discovery Protocol) (receive and transmit)
- O equipamento deverá suportar Loop-guard
- O equipamento deverá suportar POE-pre-standard detection
- O equipamento deverá suportar software download/upload: TFTP/FTP/GUI
- O equipamento deverá suportar Auto Discovery of Multiple Switches
- O equipamento deverá suportar permitir a configuração de VLANs
- O equipamento deverá suportar Syslog Collection
- Deverá ser possível gerir o equipamento através de uma Firewall
- O equipamento deverá suportar HTTP REST APIs para configuração e monitorização

b) Ao nível da alta disponibilidade:

- Multi-Chassis Link Aggregation (MCLAG)

c) Ao nível dos requisitos de segurança:

- O equipamento deverá permitir 802.1x Port Authentication
- O equipamento deverá permitir TACACS+/RADIUS Admin Access
- O equipamento deverá permitir Port Mirroring
- O equipamento deverá permitir Admin Authentication Via RFC 2865 RADIUS
- O equipamento deverá permitir 802.1x authentication with port-based assignment
- O equipamento deverá permitir 802.1x authentication with mac-based assignment
- O equipamento deverá permitir 802.1x Guest and Fallback VLAN
- O equipamento deverá permitir 802.1x MAC Address Bypass (MAB)



- O equipamento deverá permitir 802.1x Dynamic VLAN Assignment
- O equipamento deverá permitir sFlow
- O equipamento deverá permitir ACL Tables
- O equipamento deverá permitir QOS: 802.1p support
- O equipamento deverá permitir VLAN tag by ACL
- O equipamento deverá permitir VLAN tag by MAC/IP/802.1x

d) Ao nível dos requisitos de routing:

- O equipamento deverá permitir Inter-VLAN Routing
- O equipamento deverá permitir Static Routing (Software-based only) routing (like management traffic)
- O equipamento deverá permitir Static Routing (Hardware-based)
- O equipamento deverá permitir L3 Host/ARP Entries
- O equipamento deverá permitir Static BFD (Bidirectional Forwarding Detection)

e) Ao nível dos requisitos de Layer 2:

- O equipamento deverá suportar Jumbo Frames
- O equipamento deverá suportar auto negociação da velocidade dos portos e duplex
- O equipamento deverá suportar IEEE 802.1D MAC Bridging/STP
- O equipamento deverá suportar IEEE 802.1w Rapid Spanning Tree Protocol
- O equipamento deverá suportar IEEE 802.1s Multiple Spanning Tree Protocol (MSTP)
- O equipamento deverá suportar Edge Port / Port Fast
- O equipamento deverá suportar IEEE 802.1Q VLAN Tagging
- O equipamento deverá suportar IEEE 802.3ad Link Aggregation com LACP
- O equipamento deverá suportar balanceamento de tráfego Unicast/Multicast sobre portos em trunk (dst-ip, dst-mac, src-dst-ip, src-dst-mac, src-ip, src-mac)
- O equipamento deverá suportar IEEE 802.1AX Link Aggregation



- O equipamento deverá suportar Spanning Tree Instances (MSTP/CST)
 - O equipamento deverá suportar IEEE 802.3x Flow Control and back-pressure
 - O equipamento deverá suportar IEEE 802.3 10Base-T
 - O equipamento deverá suportar IEEE 802.3u 100Base-TX
 - O equipamento deverá suportar IEEE 802.3z 1000Base-SX/LX
 - O equipamento deverá suportar IEEE 802.3ab 1000Base-T
 - O equipamento deverá suportar 802.3 CSMA/CD Access Method and Physical Layer Specifications
 - O equipamento deverá suportar MAC, IP, Ethertype-based VLANs
 - O equipamento deverá suportar Virtual-Wire
- f) Ao nível dos requisitos de serviços:
- O equipamento deverá suportar IGMP Snooping
 - O equipamento deverá suportar IP conflict detection & notification
- g) Ao nível dos requisitos ao nível do suporte de RFC e MIB:
- RFC 2571 Architecture for Describing SNMP Framework
 - DHCP relay feature
 - DHCP Snooping
 - RFC 2865 RADIUS
 - RFC 1643 Ethernet-like Interface MIB
 - RFC 1213 MIB-II
 - RFC 1354 IP Forwarding Table MIB
 - RFC 2572 SNMP Message Processing and Dispatching
 - RFC 1573 SNMP MIB II
 - RFC 1157 SNMPv1/v2c
 - RFC 2030 SNTP



h) Ao nível da conectividade e sistema deverão ser asseguradas as características mínimas:

- Nº total de interfaces:
 - 48x 10 GE SFP+ (deverão ser fornecidos 40 transceivers e cabos de 10G SFP+ por equipamento, sendo 20 LR)
- Interface de gestão dedicada 10/100 Mbps: 1
- Interface Consola RJ45: 1
- Modo de gestão: Web, CLI e Firewall
- Capacidade de switching (Duplex): 1280 Gbps
- Pacotes por segundo (Duplex): 1920 Mpps
- Armazenamento de MAC addresses: 128000
- Latência: < 1µs
- Número de VLANs suportadas: 4000
- Tamanho do grupo Link Aggregation Group: até 24
- Capacidade da DRAM: 2 GB
- Capacidade da FLASH: 256 MBs
- Fonte de alimentação redundante: SIM
- Temperatura de funcionamento: 0 - 45 °C
- Humidade: 5 ate 95% sem condensação
- Altura: 1RU

B. Switch de ligação fibra tipo 2 – 4 equipamentos

Pretende-se a aquisição de 4 switches de ligação de fibra tipo 2 devendo cada o equipamento garantir as seguintes funcionalidades e especificações técnicas:

a) Ao nível dos requisitos de gestão:

As seguintes funcionalidades deverão ser suportadas:



- O equipamento deverá permitir o acesso Telnet / SSH
- O equipamento deverá permitir o acesso HTTP / HTTPS
- O equipamento deverá permitir o acesso via CLI e web GUI interface
- O equipamento deverá permitir configurar SNMP v1/v2c/v3
- O equipamento deverá permitir configurar SNTp
- O equipamento deverá suportar LLDP (802.1ab, Link Layer Discovery Protocol) (receive and transmit)
- O equipamento deverá suportar Loop-guard
- O equipamento deverá suportar POE-pre-standard detection
- O equipamento deverá suportar software download/upload: TFTP/FTP/GUI
- O equipamento deverá suportar Auto Discovery of Multiple Switches
- O equipamento deverá suportar permitir a configuração de VLANs
- O equipamento deverá suportar Syslog Collection
- Deverá ser possível gerir o equipamento através de uma Firewall
- O equipamento deverá suportar HTTP REST APIs para configuração e monitorização

b) Ao nível da alta disponibilidade:

- Multi-Chassis Link Aggregation (MCLAG)

c) Ao nível dos requisitos de segurança:

- O equipamento deverá permitir 802.1x Port Authentication
- O equipamento deverá permitir TACACS+/RADIUS Admin Access
- O equipamento deverá permitir Port Mirroring
- O equipamento deverá permitir Admin Authentication Via RFC 2865 RADIUS
- O equipamento deverá permitir 802.1x authentication with port-based assignment
- O equipamento deverá permitir 802.1x authentication with mac-based assignment
- O equipamento deverá permitir 802.1x Guest and Fallback VLAN



- O equipamento deverá permitir 802.1x MAC Address Bypass (MAB)
- O equipamento deverá permitir 802.1x Dynamic VLAN Assignment
- O equipamento deverá permitir sFlow
- O equipamento deverá permitir ACL Tables
- O equipamento deverá permitir QOS: 802.1p support
- O equipamento deverá permitir VLAN tag by ACL
- O equipamento deverá permitir VLAN tag by MAC/IP/802.1x

d) Ao nível dos requisitos de routing:

- O equipamento deverá permitir Inter-VLAN Routing
- O equipamento deverá permitir Static Routing (Software-based only) routing (like management traffic)
- O equipamento deverá permitir Static Routing (Hardware-based)
- O equipamento deverá permitir L3 Host/ARP Entries
- O equipamento deverá permitir Static BFD (Bidirectional Forwarding Detection)

e) Ao nível dos requisitos de Layer 2:

- O equipamento deverá suportar Jumbo Frames
- O equipamento deverá suportar auto negociação da velocidade dos portos e duplex
- O equipamento deverá suportar IEEE 802.1D MAC Bridging/STP
- O equipamento deverá suportar IEEE 802.1w Rapid Spanning Tree Protocol
- O equipamento deverá suportar IEEE 802.1s Multiple Spanning Tree Protocol (MSTP)
- O equipamento deverá suportar Edge Port / Port Fast
- O equipamento deverá suportar IEEE 802.1Q VLAN Tagging
- O equipamento deverá suportar IEEE 802.3ad Link Aggregation com LACP
- O equipamento deverá suportar balanceamento de tráfego Unicast/Multicast sobre portos em trunk (dst-ip, dst-mac, src-dst-ip, src-dst-mac, src-ip, src-mac)



- O equipamento deverá suportar IEEE 802.1AX Link Aggregation
 - O equipamento deverá suportar Spanning Tree Instances (MSTP/CST)
 - O equipamento deverá suportar IEEE 802.3x Flow Control and back-pressure
 - O equipamento deverá suportar IEEE 802.3 10Base-T
 - O equipamento deverá suportar IEEE 802.3u 100Base-TX
 - O equipamento deverá suportar IEEE 802.3z 1000Base-SX/LX
 - O equipamento deverá suportar IEEE 802.3ab 1000Base-T
 - O equipamento deverá suportar 802.3 CSMA/CD Access Method and Physical Layer Specifications
 - O equipamento deverá suportar MAC, IP, Ethertype-based VLANs
 - O equipamento deverá suportar Virtual-Wire
- f) Ao nível dos requisitos de serviços:
- O equipamento deverá suportar IGMP Snooping
 - O equipamento deverá suportar IP conflict detection & notification
- g) Ao nível dos requisitos ao nível do suporte de RFC e MIB:
- RFC 2571 Architecture for Describing SNMP Framework
 - DHCP relay feature
 - DHCP Snooping
 - RFC 2865 RADIUS
 - RFC 1643 Ethernet-like Interface MIB
 - RFC 1213 MIB-II
 - RFC 1354 IP Forwarding Table MIB
 - RFC 2572 SNMP Message Processing and Dispatching
 - RFC 1573 SNMP MIB II
 - RFC 1157 SNMPv1/v2c



- RFC 2030 SNMP
- h) Ao nível da conectividade e sistema deverão ser asseguradas as características mínimas:
 - Nº total de interfaces:
 - 24x GE RJ45
 - 4x 10 GE SFP+ (deverão ser fornecidos 4 transceivers e cabos de 10G SFP+ por equipamento)
 - Interface de gestão dedicada 10/100 Mbps: 1
 - Interface Consola RJ45: 1
 - Budget de PoE mínimo: 250W
 - Modo de gestão: Web, CLI e Firewall
 - Capacidade de switching (Duplex): 128 Gbps
 - Pacotes por segundo (Duplex): 204 Mpps
 - Armazenamento de MAC addresses: 16000
 - Latência: < 1µs
 - Número de VLANs suportadas: 4000
 - Tamanho do grupo Link Aggregation Group: até 8
 - Capacidade da DRAM: 1 GB
 - Capacidade da FLASH: 256 MBs
 - Fonte de alimentação redundante: SIM
 - Temperatura de funcionamento: 0 - 50 °C
 - Humidade: 10 ate 90% sem condensação
 - Altura: 1RU

Suporte



- Todos os equipamentos deverão garantir o suporte e subscrição de todos os serviços por parte do fabricante, por um período mínimo de 3 anos e em regime 24x7

Documentação técnica de suporte à proposta

O concorrente deverá submeter fichas técnicas do fabricante dos equipamentos propostos, de onde seja possível ao júri aferir todas as funcionalidades e especificações técnicas solicitadas, não sendo aceite apenas documentos que atestem o cumprimento integral da solução.