CONTRATO Nº 1643/2023

AQUISIÇÃO DE UMA SOLUÇÃO DE FIREWALL E AP'S

ASSINATURAS

Instituto Português de Oncologia de Lisboa de Francisco Gentil, EPE	**CHIEF SECURITY OFFICERS, SA**
[redacted]	[redacted]
[redacted]	[redacted]
Lisboa, 01 de junho 2023	

Entre:

Instituto Português de Oncologia de Lisboa de Francisco Gentil, EPE, com o número único de matrícula e de pessoa coletiva 506 361 616 e sede na Rua Professor Lima Basto, 1099-023 Lisboa, aqui representado por, [redacted] do Conselho de Administração, com poderes para o ato face ao disposto face ao disposto no Art.º 12º do anexo II ao D.L. 52/2022 de 4 agosto, como entidade adjudicante;

E

CHIEF SECURITY OFFICERS, SA, número de pessoa coletiva 507817842, com sede na Alfapark – Edifício F – Piso 1, Estrada de Alfragide, 67, 2610-008, aqui representada por [redacted], titular do Bilhete de Identidade nº [redacted] e [redacted], titular do Bilhete de Identidade nº [redacted], na qualidade de representantes legais, com poderes para o ato, adiante também denominada como entidade adjudicatária.

Tendo em conta:

a) A decisão de adjudicação proferida pela [redacted] do Conselho de Administração, a 30 de maio de 2023, relativa ao Procedimento PN/1643/2023;

b) O subsequente ato de aprovação da minuta do contrato proferido pela [redacted] do Conselho de Administração, a 30 de maio de 2023;

c) A despesa inerente ao contrato, no valor **de 130 561,58€ (cento trinta mil quinhentos e sessenta e um euros e cinquenta e oito cêntimos) acrescido de IVA** à taxa legal em vigor, inscrita na rubrica orçamental 62262 do orçamento económico de 2023 com o cabimento nº 16432023 e compromisso nº 3200.

e) Fazem parte integrante do presente Contrato todos os elementos previstos no n.º 2 do artigo 96.º do Código dos Contratos Públicos (CCP), aprovado pelo Decreto-Lei n.º 18/2008, de 29 de janeiro, na sua redação atual;

É celebrado o presente Contrato, nos termos das seguintes cláusulas:

Cláusula 1.ª

Objeto

O presente contrato tem por objeto a Aquisição de uma Solução de Firewall e AP's para o Instituto Português de Oncologia de Lisboa Francisco Gentil, EPE, de acordo com o definido no Caderno de Encargos, na proposta adjudicada e no anexo I, os quais dele fazem parte integrante.

Cláusula 2.ª

Preço contratual e condições de pagamento

1. Pelo fornecimento objeto do Contrato, bem como pelo cumprimento das demais obrigações constantes do presente Caderno de Encargos, o Primeiro Outorgante obriga-se a pagar ao adjudicatário o preço constante da proposta adjudicada no valor **de 130 561,58€ (cento trinta mil quinhentos e sessenta e um euros e cinquenta e oito cêntimos) acrescido de IVA** à taxa legal em vigor, se este for legalmente devido.

2. As quantias devidas pelo Primeiro Outorgante nos termos da Cláusula anterior, devem ser pagas no prazo máximo de 60 (sessenta) dias após a entrega das respetivas faturas, as quais só podem ser emitidas após o vencimento da obrigação e receção da respetiva nota de encomenda, a emitir em função dos fundos disponíveis, e onde se encontre necessariamente inscrito, sob pena de nulidade, um número de compromisso válido e sequencial.

3. O preço referido nos números anteriores inclui todos os custos, encargos e despesas cuja responsabilidade não esteja expressamente atribuída ao contraente público, nomeadamente os relativos a deslocações fora da comarca de Lisboa, taxas de justiça, injunções, custas judiciais ou a solicitadores de execução e despesas administrativas bem como quaisquer encargos decorrentes da utilização de marcas registadas, patentes ou licenças.

4. De acordo com o artigo 300º do CCP, não haverá lugar à revisão dos preços, mantendo-se o preço contratual adjudicado inalterado durante toda a vigência do contrato.

5. Para efeitos de pagamento, as faturas deverão ser apresentadas, após execução do fornecimento e com uma antecedência de 60 dias em relação à data do seu vencimento.

6. Os pagamentos só serão devidos para a quantidade e preço constante da Nota de Encomenda emitida, pelo Serviço de Gestão de Compras do IPOLFG.

7. Em caso de discordância, por parte do IPOLFG, quanto aos valores indicados nas faturas, deverá o mesmo comunicar ao fornecedor, por escrito, os respetivos fundamentos, devendo este prestar os esclarecimentos necessários ou proceder à emissão de nova fatura corrigida.

8. Desde que devidamente emitidas e observado o disposto no n.º 1 as faturas são pagas por transferência bancária para instituição de crédito indicada pelo fornecedor.

9. Sem prejuízo do definido no Diploma de execução orçamental, em caso de atraso no cumprimento das obrigações pecuniárias por parte do IPOLFG, o fornecedor tem o direito aos juros de mora sobre o montante em dívida, nos termos previstos no artigo 326.º do Código dos Contratos Públicos e da Lei n.º 3/2010, de 27 de abril.

10. O atraso em um ou mais pagamentos não determina em caso algum o vencimento das restantes obrigações de pagamento.

Cláusula 3ª

Vigência

O contrato vigora desde a data da sua assinatura até ao fornecimento do(s) bem(s) ao contraente publico, em conformidade com os respetivos termos e condições e o disposto na lei, não podendo exceder os 30 dias úteis, sem prejuízo das obrigações acessórias que devam perdurar para além da sua cessação

Cláusula 4.ª

Penalidades Contratuais

1. Pelo incumprimento de obrigações emergentes do contrato, nomeadamente em casos de mora, cumprimento defeituoso ou incumprimento de qualquer das obrigações assumidas no âmbito do Contrato a celebrar, o IPOLFG pode exigir do Prestador de serviços o pagamento de uma pena pecuniária, até ao limite de 5 % (cinco por cento) sobre o preço mensal do Contrato, calculados diariamente, até ao completo e integral cumprimento das obrigações assumidas. A sanção prevista corresponderá ao máximo aplicável, sendo que, no caso concreto, será apreciada em função da culpa do Prestador de serviços.
2. Na determinação da gravidade do incumprimento, o IPOLFG tem em conta, nomeadamente, a duração da infração, a sua eventual reiteração, o grau de culpa do Prestador e as consequências do incumprimento.
3. O IPOLFG pode compensar os pagamentos devidos ao abrigo do contrato com as penas pecuniárias devidas nos termos da presente cláusula.
4. As penas pecuniárias previstas na presente cláusula não obstam a que o IPOLFG exija uma indemnização pelo dano excedente.

Cláusula 5ª

Gestor do Contrato

Para efeitos do disposto no artigo 290.º-A do CCP, o Gestor do Contrato é o [redacted]

Anexo I

Especificações Técnicas

1. Objetivo

Pretende-se reformular e atualizar a infraestrutura de segurança beneficiando das mais recentes tecnologias que o mercado oferece e, simultaneamente, mitigar os riscos emergentes nas diversas componentes de operação, adquirindo:

- 2 x Firewall´s em Alta Disponibilidade;
- 210 x Pontos de Acesso Wireless

2. Requisitos Gerais

Com o objetivo de simplificar a gestão da infraestrutura, permitindo uma maior flexibilidade e gestão de recursos, a solução a apresentar deverá ser integralmente do mesmo fabricante, possibilitando desta forma que exista uma maior integração e correlação das soluções a implementar.

A solução a apresentar deverá prever o suporte e subscrição de todos os serviços de segurança enunciados no presente documento, por parte do fabricante por um período mínimo de 1 ano e em regime 24x7.

3. Requisitos Técnicos

Pretende-se a implementação de um cluster de duas firewall´s em alta disponibilidade, devendo cada uma das unidades possuir um conjunto de especificações e de tecnologias que enumeramos de seguida:

3.1 Integração com redes de comunicações

As seguintes funcionalidades deverão ser suportadas:

- Servidor de DHCP, NTP e DNS incluído
- Funcionalidade de DNS Proxy
- 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, 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
- Suporte Dual Stack IPv4 e IPv6 em simultâneo
- Suporte VXLAN

3.2 Identificação de utilizadores e dispositivos

As seguintes funcionalidades deverão ser suportadas:

- Base de dados local de utilizadores;
- Autenticação de utilizadores em servidores remotos: LDAP, RADIUS, TACACS+
  - Sistema de Single Sign-on de utilizadores (Windows AD, Radius, Kerberos, ...)
  - Autenticação de utilizadores no acesso (802.1x, portal cativo)
- 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

3.3 Firewall

As seguintes funcionalidades deverão ser suportadas:

- Modos de operação NAT/route e transparente/bridge
- Agendamento de políticas: recorrentes ou apenas uma vez
- 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
- 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.

3.4 VPN

As seguintes funcionalidades deverão ser suportadas:

- IPSEC VPN:
  - Suporte para peers remotos: clientes dialup compatíveis com IPSEC, peers com IP estático ou DNS dinâmico
  - Mecanismos de autenticação: certificados ou pre-shared key
  - 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 politicas (policy-based)
- VPNs SSL
  - Portal de VPN SSL configurável: temas de cores, disposição, atalhos (bookmarks) mecanismos de ligação, download de cliente
  - Suporte para domínio de SSL VPN: permite a customização de múltiplos portais VPN SSL associados a grupos de utilizadores, incluindo URL do portal e desenho
  - Atalhos (bookmarks) com single sign-on: permite reutilizar um login anterior ou credenciais pré-definidas para aceder a recursos internos
  - Gestão de atalhos (bookmarks) pessoais
  - Gestão de utilizadores concorrentes
  - Controlo/limitação de múltiplos acessos VPN com as mesmas credenciais de acesso
  - Suporte de VPN SSL em modo web:
    - Para clientes remotos equipamentos apenas com um browser web
    - Disponibiliza suporte web para aplicações como: HTTP/HTTPS, FTP, Telnet, SMB/CIFS, SSH. VNC, RDP, Citrix
  - Suporte para VPN SSL em modo túnel:
    - Para acesso a partir de computadores que necessitam utilizar qualquer software do tipo cliente-servidor.
    - Disponível para MAC OSX, Windows, IOS, Android e Windows Mobile
  - 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.

3.5 IPS - Deteção e prevenção de intrusões

As seguintes funcionalidades deverão ser suportadas:

- Suporte de IPS com mais de 11000 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: definido por defeito na assinatura, monitorizar, bloquear, reset de sessão ou quarentena (IP do atacante, IP de atacante e vitima, interface de entrada) 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

3.6 Controlo de aplicações

As seguintes funcionalidades deverão ser suportadas:

- Deteção de mais de 3100 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, aplicação de gestão de largura de banda
- Inspeção SSL

3.7 Proteção contra ameaças

As seguintes funcionalidades deverão ser suportadas:

- Possibilidade de inspeção aplicacional de tráfego encriptado por SSL, incluindo as seguintes funcionalidades: IPS, controlo de aplicações, anti-vírus, filtragem WEB e DLP
- Capacidade de desencriptação de sessões SSL com cópia de tráfego desencriptado para um sistema externo
- Inspeção apenas de certificado SSL ou Inspeção deep-packet com técnicas MiTM
- Deteção e bloqueio de BOTNETs com base em listas de reputação de IPs globais;
- Excluir, de forma simples, a inspeção SSL de tráfego encriptado em determinadas categorias relevantes à manutenção da privacidade dos utilizadores
- Suporte de anti-vírus nos modos flow (pacote-a-pacote) e proxy (reconstrução de sessões)
- Suporte de inspeção de anti-vírus, em modo flow, nos seguintes protocolos: HTTP/HTTPS, SMTP/SMTPS, POP3/POP3S, IMAP/IMAPS, MAPI, FTP/SFTP, SMB, ICQ, YM, NNTP
- Suporte de anti-vírus em modo proxy, incluindo:
    - Suporte dos seguintes protocolos: HTTP/HTTPS, STMP/SMTPS, POP3/POP3S, IMAP/IMAPS, MAPI, FTP/SFTP, ICQ, YM, NNTP
    - 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 filtragem sites com base em URL, conteúdo web e cabeçalho MIME
- Categorização dinâmica em tempo real, baseada na cloud, com mais de 245 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 customizada e sobreposição de categorização
- Mecanismos de exceção à utilização de perfis pré-definidos;

- Mecanismos de deteção e mitigação de utilização de proxy-avoidance: Categorias de sites com proxy, pontar URLs por domínio e endereço IP, bloquear redirects de cache para sites com cache e tradução de sites, bloqueio de ligação a proxy com base em deteção de aplicação, bloqueio de tráfego com comportamento de proxy com base em assinaturas de IPS
- Integração nativa com plataformas externas de filtragem de email, sandbox e WAF
- Feeds de ameaças por Domain Name e/ou IP Address

3.8 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

3.9 Administração, Monitorização e Diagnósticos

As seguintes funcionalidades deverão ser suportadas:

- Acesso de gestão gráfica e texto: HTTPS com recurso a web browser
- Acesso de gestão em modo de texto: SSH, Telnet ou consola
- 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.
- **Registo de eventos e relatórios**

As seguintes funcionalidades deverão ser suportadas:

- Suporte para registo de eventos (logs) em diferentes repositórios, tais como: memória, disco rígido local, múltiplos servidores de syslog, múltiplos servidores específicos para registos de eventos e elaboração de relatórios, servidores do tipo WebTrends e plataformas disponíveis na cloud
- Opção de logging confiável com recurso a mecanismos TCP (RFC 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
- Registos detalhados de trafego: tráfego enviado, bloqueado, sessões violadas, tráfego local, pacotes inválidos
- Organização de registos de acordo com a categoria: administração de sistema (para auditoria), routing e networking, VPN, autenticação de utilizadores, Wireless
- Opção para registo encurtado 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.

3.10 Conectividade

As seguintes interfaces mínimas deverão ser asseguradas:

- Interfaces 10Gb SFP+ >= 4
- Interfaces 10/100/1000 RJ45 >= 16
- Interfaces GbE SFP>= 8

- Interface 25Gb SFP28 >= 4
- Interface de Console (RJ45) = 1

3.11 Sistema

As seguintes características mínimas deverão ser asseguradas:

- Disco interno: 2x 240 GB SSD

3.12 Desempenho:

As seguintes características mínimas deverão ser asseguradas:

- Débito firewall (pacotes UDP 512): 135 Gbps
- Latência de firewall (pacotes UDP de 64 bytes): 4.12 µs
- Débito firewall (pacotes por segundo): 100 Mpps
- Sessões TCP concorrentes:8 Milhões
- Novas sessões/segundo (TCP): 500.000
- Débito VPN IPSec (pacotes 512 bytes): 55 Gbps
- Túneis IPsec Gateway-to-Gateway:500
- Túneis IPSec cliente remoto: 1500
- Tuneis VPN SSL: 1500
- Débito de inspeção SSL: 9 Gbps
- Débito NGFW: 11 Gbps
- Débito Threat Protection: 10 Gbps
- Domínios Virtuais: 10
- Possibilidade de controlar pontos de acesso wireless: 512
- Tokens suportados: 5.000
- Licenciamento ilimitado de utilizadores: SIM

3.13 Energia e Alimentação

- Fonte de alimentação redundante hot-swappable:Sim

3.14 Dimensões

As seguintes características deverão ser suportadas:

- Altura maxima: 1RU

4. Pontos de Acesso Wireless

Pretende-se a aquisição de Access Points de media densidade, sendo que cada uma das unidades deve possuir um conjunto de especificações e de tecnologias que enumeramos de seguida:

- Número de rádios: 3
- Número de antenas: 3 internas dual band + 1 interna BLE/Zigbee
- Antenas: 4.5dBi para 2.4 GHz, 5.5 dBi para 5 GHz
- Taxa máxima de transferência de dados:
- Radio 1: até 574 Mbps,
- Radio 2: até 1201 Mbps
- SSIDs simultâneos (Máximo): 16
- Interfaces: 2x10/100/1000 RJ45 e 1x USB 2.0
- 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 e 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, 802.1Q, 802.1X, 802.3ad, 802.3af, 802.3at, 802.3az
- OFDMA
- WIDS
- Deverá permitir funcionalidades de analise 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 e/ou gateway de segurança
- Possibilidade de monitorizar o estado do equipamento a partir de uma plataforma centralizada