INSTITUTO DE HIGIENE E MEDICINA TROPICAL
DESDE 1902

Assinado por : **FILOMENO DE JESUS PIRES COELHO FORTES**
Num. de Identificação: 12237173
Data: 2021.09.29 18:23:07+01'00'

CARTÃO DE CIDADÃO

Despacho:
Aprovo o caderno de encargos.
Data:

O Diretor

(Professor Doutor Filomeno Fortes)

CADERNO DE ENCARGOS

Renovação e ampliação de toda a Infraestrutura de Tecnologias de Informação do Edifício do Biotério/VIASEF

Procedimento de Consulta Prévia com Ref.ª 09/CPrv/2021

Em conformidade com os n.ºs 1 a 4, do artigo 42.º do Código dos Contratos Públicos (CCP), na sua atual redação, abaixo se discriminam as especificações técnicas e demais aspetos essenciais à execução do contrato a celebrar.

Artigo 1.º

Objeto

O presente caderno de encargos tem por objeto a renovação e ampliação de toda a Infraestrutura de Tecnologias de Informação do Edifício do Biotério/VIASEF, em conformidade com as especificações técnicas em anexo.

Artigo 2.º

Forma e documentos contratuais

1- O contrato será reduzido a escrito através da elaboração de um clausulado em suporte informático com a aposição de assinaturas eletrónicas, nos termos do n.º 1 do artigo 94.º do CCP.

2- Fazem parte integrante do contrato os seguintes documentos:

a) Os suprimentos dos erros e omissões do caderno de encargos identificados pelas entidades convidadas, desde que esses erros e omissões tenham sido expressamente aceites pelo órgão competente para a decisão de contratar;

b) Os esclarecimentos e as retificações relativas ao caderno de encargos;

c) O presente caderno de encargos;

d) A proposta adjudicada;

e) Os esclarecimentos à proposta adjudicada prestados pelo adjudicatário.

3- Em caso de divergência entre os documentos referidos no n.º 2, a prevalência é determinada pela ordem que nele se dispõe.

4- Em caso de divergência entre os documentos referidos no n.º 2 e o clausulado do contrato, prevalecem os primeiros, salvo quanto aos ajustamentos ao conteúdo do contrato propostos pelo órgão competente para a decisão de contratar e aceites pelo adjudicatário.

Artigo 3.º

Vigência

O contrato mantém-se em vigor até à conclusão e aceitação da implementação, em conformidade com os respetivos termos e condições e o disposto na lei, sem prejuízo das obrigações acessórias que devam perdurar para além da cessação do contrato.

Artigo 4.º

Obrigações e responsabilidade do adjudicatário

1- O adjudicatário obriga-se a executar o objeto do contrato de forma profissional e competente, utilizando os conhecimentos técnicos, o *know-how*, a diligência, o zelo e a pontualidade próprios das melhores práticas.

2- Constituem ainda obrigações do adjudicatário:

a) Apresentar os documentos de habilitação a que estão obrigados, nos termos do artigo 81.º do CCP;

b) Fornecer e implementar a solução à entidade adjudicante, conforme as especificações técnicas em anexo ao presente caderno de encargos;

c) Garantir o bom funcionamento em todas as fases da solução implementada;

d) Disponibilizar, sempre que necessário, manuais de utilizador e apoio técnico;

e) Disponibilizar os drivers de instalação e software utilizados na solução implementada;

f) Possuir todas as autorizações, consentimentos, aprovações, registos e licenças necessários para o pontual cumprimento das obrigações assumidas no contrato;

g) Comunicar antecipadamente, logo que tenha conhecimento, à entidade adjudicante, o facto que torne total ou parcialmente impossível o fornecimento e a implementação da solução,

objeto do procedimento, ou o cumprimento de qualquer outra das suas obrigações nos termos do contrato celebrado com a entidade adjudicante;

h) Manter sigilo e garantir a confidencialidade, não divulgando quaisquer informações que obtenham no âmbito da formação e da execução do contrato, nem utilizar as mesmas para fins alheios àquela execução, abrangendo esta obrigação todos os seus agentes, funcionários, colaboradores ou terceiros que nelas se encontrem envolvidos;

i) Não alterar as condições do fornecimento e implementação da solução fora dos casos previstos de acordo com as especificações do presente caderno de encargos;

j) O adjudicatário obriga-se a recorrer a todos os meios humanos, materiais e informáticos que sejam necessários e adequados à execução do contrato.

3- O adjudicatário é responsável:

a) Por todos os serviços necessários à correta definição, implementação e disponibilização da solução, incluindo a configuração e otimização de todos os componentes incluídos;

b) Por todos os prejuízos e danos causados à entidade adjudicante ou a terceiros que, por qualquer motivo, resultem da execução do contrato, da atuação do seu pessoal ou do deficiente comportamento da solução implementada, incluindo a sua interligação com os equipamentos da entidade adjudicante ou de terceiros.

Artigo 5.º

Obrigações da entidade adjudicante

Constitui obrigação da entidade adjudicante, pagar, no prazo acordado, as faturas emitidas pelo adjudicatário.

Artigo 6.º

Preço base

O preço base para efeitos do presente procedimento pré-contratual é de 26.167,84€ (vinte e seis mil, cento e sessenta e sete euros e oitenta e quatro cêntimos), acrescido de IVA à taxa legal em vigor.

Artigo 7.º

Condições e prazo de pagamento

1- As faturas devem ser emitidas em nome de Universidade Nova de Lisboa - Instituto de Higiene e Medicina Tropical e entregues na Divisão de Gestão Financeira e Patrimonial deste Instituto.

2- As faturas devem ser emitidas faseadamente do seguinte modo:

a) 40% do valor adjudicado – após implementação da solução;

b) 20% do valor adjudicado – após 60 dias da data da implementação da solução;

c) 20% do valor adjudicado – após 90 dias da data da implementação da solução;

d) 20% do valor adjudicado – após 120 dias da data da implementação da solução;

3- Os pagamentos são realizados por transferência bancária para a conta a indicar pelo adjudicatário.

Artigo 8.º

Patentes, licenças e marcas registadas

São da responsabilidade do adjudicatário quaisquer encargos decorrentes da obtenção ou utilização, no âmbito do contrato, de patentes, licenças ou marcas registadas.

Artigo 9.º

Inspeção e testes

1- Concluída a implementação da solução objeto do contrato, a entidade adjudicante procede, no prazo de 30 (trinta) dias, à inspeção quantitativa e qualitativa da mesma, com vista a verificar, respetivamente, se os mesmos correspondem às características, especificações e requisitos técnicos e operacionais definidos no presente caderno de encargos e na proposta adjudicada, bem como outros requisitos exigidos por lei.

2- A inspeção qualitativa a que se refere o número anterior incide sobre os serviços realizados, sendo efetuada através da verificação do cumprimento das especificações técnicas que constam do presente caderno de encargos.

3- Durante a fase da realização de testes, o adjudicatário deve prestar à entidade adjudicante, toda a cooperação e todos os esclarecimentos necessários, podendo fazer-se representar durante a realização daqueles, através de pessoas devidamente credenciadas para o efeito.

Artigo 10.º

Inoperacionalidade, defeitos ou discrepâncias

1- No caso de os testes previstos no artigo anterior não comprovarem a total operacionalidade da solução implementada, bem como a sua conformidade com as exigências legais, ou no caso de existiram defeitos ou discrepâncias com as características, especificações e requisitos técnicos definidos no presente caderno de encargos, a entidade adjudicante deve informar, por escrito, o adjudicatário.

2- No caso previsto no número anterior, o adjudicatário deve proceder, à sua custa e no prazo razoável que for determinado pela entidade adjudicante, às reparações ou substituições necessárias para garantir a operacionalidade dos serviços objeto do contrato e o cumprimento das exigências legais e das características, especificações e requisitos técnicos exigidos.

3- Após a realização das reparações ou substituições necessárias pelo adjudicatário, no prazo respetivo, a entidade adjudicante procede à realização de novos testes de aceitação, nos termos do artigo anterior.

Artigo 11.º

Aceitação dos serviços objeto do contrato

1- Caso os testes a que se refere o artigo 9.º comprovem a total operacionalidade dos serviços objeto do contrato, bem como a sua conformidade com as exigências legais, e neles não sejam detetadas quaisquer defeitos ou discrepâncias com as características, especificações e requisitos técnicos definidos no presente caderno de encargos, deve ser emitida pela entidade adjudicante, no prazo máximo de 10 (dez) dias a contar do final da realização dos testes, um auto de aceitação da solução implementada.

2- A assinatura do auto a que se refere o número anterior não isenta o adjudicatário das obrigações relativas à solução implementada, nos termos da lei que disciplina os aspetos relativos à venda de bens de consumo e das garantias a ela relativas no que respeita à responsabilidade e obrigações do adjudicatário e do produtor e aos direitos do consumidor.

Artigo 12.º

Local e prazo

1- Os serviços objeto do contrato a celebrar serão efetuados no Instituto de Higiene e Medicina Tropical, sito na Rua da Junqueira n.º 100, 1349-008 Lisboa.

2- O adjudicatário obriga-se a concluir a execução dos serviços objeto do contrato a celebrar no prazo máximo de 30 (trinta) dias a contar da data de notificação de adjudicação.

Artigo 13.º

Resolução do contrato

O incumprimento, por uma das partes, das obrigações resultantes do contrato, confere à outra parte o direito de rescindir o contrato, sem prejuízo das correspondentes indemnizações legais.

Artigo 14.º

Foro Competente

Para todas as questões emergentes do contrato será competente o Tribunal Administrativo e Fiscal de Lisboa, com renúncia a qualquer outro.

Artigo 15.º

Subcontratação e cessão da posição contratual

1- A subcontratação pelo adjudicatário e a cessão da posição contratual por qualquer das partes depende da autorização da outra, nos termos do CCP.

2- O adjudicatário não poderá subcontratar, sem o consentimento prévio e escrito da entidade adjudicante, total ou parcialmente, qualquer uma das obrigações que para si decorrem do contrato.

3- A subcontratação de qualquer entidade por parte do adjudicatário não o desvinculará de qualquer responsabilidade ou obrigação para si decorrente do contrato.

Artigo 16.º

Gestor do contrato

1- Será nomeado um gestor do contrato por parte da entidade adjudicante, com a função de acompanhamento permanente da execução do contrato.

2- Caso o gestor detete desvios, defeitos ou outras anomalias, pode o mesmo adotar medidas corretivas que, em cada caso, se revelem adequadas, com exceção das respeitantes a matérias de modificação e cessação do contrato.

Artigo 17.º

Comunicações e notificações

Em sede de execução contratual, todas as comunicações do adjudicatário dirigidas à entidade adjudicante são efetuadas por escrito e enviadas através de correio registado ou correio eletrónico, de acordo com os seguintes elementos:

Divisão de Gestão Financeira e Patrimonial

Universidade Nova de Lisboa – Instituto de Higiene e Medicina Tropical

Rua da Junqueira 100, 1349-008 Lisboa

E-mail: financeira.ihmt@ihmt.unl.pt

Artigo 18.º

Legislação Aplicável

Em tudo o que for omisso no presente caderno de encargos, observar-se-á o disposto no CCP e demais legislação em vigor.

ANEXO I

Especificações Técnicas

Os Equipamentos e Serviços a adquirir deverão reunir as seguintes características técnicas:

LAN Switch Core

Pretende-se o fornecimento de 2 Switches de rede para interligação dos atuais equipamentos existentes no IHMT.

Cada equipamento deverá cumprir com os seguintes requisitos mínimos:

1 Switch de 12 Portas com a seguinte configuração:

- Altura Máxima de 1U com guias para fixação em Rack de 19”
- Mínimo de 12 portos SFP+ 10Gb/s, 3 portos QSFP28
- 1 Cabo QSFP28 para QSFP28 para interligação dos switches
- 1 Cabo QSFP+ para QSFP+ para interligação dos 2 switches;
- 3 Transceivers 1Gb SFP SR

1 Switch de 12 Portas com a seguinte configuração:

- Altura Máxima de 1U com guias para fixação em Rack de 19”
- Mínimo de 12 portos SFP+ 10Gb/s, 3 portos QSFP28
- 1 Cabo QSFP28 para QSFP28 para interligação dos switches
- 1 Cabo QSFP+ para QSFP+ para interligação dos 2 switches;
- 2 Transceivers 1Gb SFP SR
- 1 Transceiver

Características Genéricas:

- Capacidade de switching mínima de 840Gbps
- Throughput mínimo de 625Mpps
- 1 Porto Consola/Gestão com sinal RS232
- 1 Porto Consola RJ45 micro-USB-B
- 1 Porto RJ45 10/100/1000 Base-T para Gestão
- 2 Fontes de alimentação Redudantes
- Packet buffer memory: 12MB
- CPU memory: 4GB
- MAC addresses: 272K (in Scaled L2 mode)
- PVST: 128 instances
- ARP table 200K (in Scaled L3 host mode)
- IPv4 routes: 200K (in Scaled L3 routes mode)

- IPv6 hosts: 64K
- IPv6 routes: 130K (in Scaled L3 routes mode)
- Multicast hosts: 8K
- Link aggregation: 32 links per group, 128 groups
- Layer 2 VLANs: 4K
- Layer3 VLANs: 500
- MSTP: 32 instances
- LAG load balancing: Based on layer 2, IPv4 or IPv6 headers
- L2 Ingress ACL: 6K
- L2 Egress ACL: 1K
- IPv4 Ingress ACL: 6K
- IPv4 Egress ACL: 1K
- IPv6 Ingress ACL: 3K
- IPv6 Egress ACL: 500
- IEEE Compliance
- 802.1AB LLDP
- TIA-1057 LLDP-MED
- 802.1s MSTP
- 802.1w RSTP
- 802.3ab Gigabit Ethernet (1000Base-T)
- 802.3ad Link Aggregation with LACP
- 802.3ae 10 Gigabit Ethernet (10GBase-X)
- 802.3ba 40 Gigabit Ethernet (40GBase-X)
- 802.3i Ethernet (10Base-T)
- 802.3u Fast Ethernet (100Base-TX)
- 802.3z Gigabit Ethernet (1000BaseX)
- 802.1D Bridging, STP
- 802.1p L2 Prioritization
- 802.1Q VLAN Tagging, GVRP
- 802.1Qbb PFC
- 802.1Qaz ETS
- 802.1s MSTP
- 802.1w RSTP
- PVST+
- 802.1X Network Access Control

- 802.3ab Gigabit Ethernet (1000BASE-T) or breakout
- 802.3ac Frame Extensions for VLAN Tagging
- 802.3ad Link Aggregation with LACP
- 802.3ae 10 Gigabit Ethernet (10GBase-X)
- 802.3ba 40 Gigabit Ethernet (40GBase- SR4, 40GBase-CR4, 40GBase-LR4, 100GBase-SR10, 100GBase-LR4, 100GBase-ER4) on optical ports
- 802.3bj 100 Gigabit Ethernet
- 802.3u Fast Ethernet (100Base-TX) on mgmt. ports
- 802.3x Flow Control
- 802.3z Gigabit Ethernet (1000Base-X) with QSA
- ANSI/TIA-1057 LLDP-MED
- Jumbo MTU support 9,416 bytes
- 802.1D Compatible
- 802.1p L2 Prioritization
- 802.1Q VLAN Tagging
- 802.1s MSTP
- 802.1w RSTP
- 802.1t RPVST+
- 802.3ad Link Aggregation with LACP
- VLT Enhancements
- Minloss Upgrades
- VLT Proxy Gateway
- RVPST over VLT
- DCB, FSB, iSCSI over VLT
- RSPAN over VLT
- SNMPv1/2
- SSHv2
- FTP, TFTP, SCP
- Syslog
- Port Mirroring
- RADIUS
- 802.1X
- Support Assist (Phone Home)
- Netconf APIs
- XML Schema

- CLI Commit (Scratchpad)
- sFlow
- Automation
- Control Plane Services APIs
- Linux Utilities and Scripting Tools
- Quality of Service
- Access Control Lists
- Prefix List
- Route-Map
- Rate Shaping (Egress)
- Rate Policing (Ingress)

Suporte e Manutenção:

O suporte e manutenção de todo o equipamento fornecido, deve ser assegurado diretamente pelo fabricante com suporte ao nível local e preferencialmente em língua portuguesa.

A manutenção pretendida é a seguinte:

Manutenção de 36 meses incluindo peças e mão-de-obra.

- SLA 24x7 com tempo de resposta nas instalações no dia útil seguinte
- Prestação de assistência contínua até à solução da avaria
- O suporte deverá ser dado diretamente pelo fabricante localmente

Serviços de Instalação:

Pretende-se o fornecimento dos seguintes serviços:

LAN Switch Core

- Instalação física dos equipamentos em Bastidores
- Configuração dos equipamentos na rede do cliente
- Configuração Stack\VLT
- Configuração VLAN, Uplink, LAG
- Testes de funcionamento

LAN Switch Distribuição

Pretende-se o fornecimento de 2 Switches de rede para interligação dos atuais equipamentos existentes no IHMT.

1 Switch de 24 Portos com a seguinte configuração mínima:

- Altura Máxima de 1U com guias para fixação em Rack de 19”

- Mínimo de 24 portos 10/100/1000BASE-T PoE-Plus, 4 portos SFP 1Gb com possibilidade de upgrade para 10Gb por Licença
- Mínimo de 1 Processador 1Ghz 64-bit MIPS Single Core
- Mínimo de 1GB ECC DDR3 DRAM
- Mínimo de 4GB eMMC Flash
- 1 Porto Consola/Gestão com sinal RS232
- 1 Porto RJ45 10/100/1000 Base-T para Gestão
- 1 Fonte de alimentação
- Capacidade de switching mínima de 128Gbps
- Throughput mínimo de 95.2Mpps
- Packet buffer memory: 1.5 MB
- 1 Transceiver 1000BASE-SX SFP MMF 220 550 meters LC connector Industrial Temp

1 Switch de 48 Portos com a seguinte configuração mínima:

- Altura Máxima de 1U com guias para fixação em Rack de 19”
- Mínimo de 48 portos 10/100/1000BASE-T PoE-Plus, 4 portos SFP 1Gb com possibilidade de upgrade para 10Gb por Licença
- Mínimo de 1 Processador 1Ghz 64-bit MIPS Single Core
- Mínimo de 1GB ECC DDR3 DRAM
- Mínimo de 4GB eMMC Flash
- 1 Porto Consola/Gestão com sinal RS232
- 1 Porto RJ45 10/100/1000 Base-T para Gestão
- 1 Fonte de alimentação
- Capacidade de switching mínima de 176Gbps
- Throughput mínimo de 130.9Mpps
- Packet buffer memory: 1.5 MB
- 1 Transceiver 1000BASE-SX SFP MMF 220 550 meters LC connector Industrial Temp

Características Genéricas:

- Menos de 4 microssegundos de latência (64-byte)
- Layer 2/MAC Addresses: 16K
- IPv4 LPM Entries: 480
- IPv4 Hosts: 1000
- IPv6 LPM (64-bit) Entries: 240
- 4096 user-created VLAN/VMANs
- 9216 Byte Max Packet Size (Jumbo Frame)

- 128 load sharing trunks, up to 8 members per trunk
- 1,024 ingress bandwidth meters, 256 egress meters
- Ingress and egress bandwidth policing/rate limiting per flow/ACL
- 8 QoS egress queues/port
- Egress bandwidth rate shaping per egress queue and per port.
- Rate Limiting Granularity: 8 Kbps
- Half-duplex 10/100 supported on the following 10/100/1000 ports:
- 12 port switches: Ports 1-12
- 24 port switches: Ports 1-16
- 48 port switches: Ports 1-16 and Ports 25-40
- LRM support on rear-panel SFP/SFP+ ports on all
- 48-port switches
- Policy Capabilities
- Policy Profiles: 63
- Rules per Profile: Up to 440
- Authenticated Policy Users per Switch: Up to 1,536
- Authenticated Policy Users per Port: Up to 1,536
- Unique Permit/Deny Rules per switch: 440
- MAC Rules: N/A
- IPv4 Rules: 256
- IPv6 Rules: N/A
- L2 Rules: 184
- Rate Limiting: Per Class of Service

Suporte e Manutenção:

Manutenção de 36 meses incluindo peças e mão-de-obra.

- SLA 24x7 com tempo de resposta nas instalações no dia útil seguinte
- Prestação de assistência contínua até à solução da avaria
- O suporte deverá ser dado diretamente pelo fabricante localmente

Serviços de Instalação:

Pretende-se o fornecimento dos seguintes serviços:

- Instalação física dos equipamentos em Bastidores
- Configuração dos equipamentos na rede do cliente
- Configuração VLAN, Uplink, LAG
- Testes de funcionamento

Solução Wifi

Pretende-se o fornecimento de 9 Pontos de Acesso wifi para cobertura do edifício do Biotério com rede wifi 6.

Os equipamentos a fornecer terão que cumprir os seguintes requisitos mínimos:

- Incluir Base de fixação em teto
- 1 Porto 10\100\1000 Base-T PoE 802.3af
- 1 USB2.0 Tipo A
- Suporte para 802.11 a, b, g, n, ac, ax
- Suporte para BLE 5
- Suporte um mínimo de 8 SSID por tecnologia de Radio
- Suporte as seguintes tecnologias de Radio
  - ✓ 5 GHz 2x2:2
  - ✓ 2.4 GHz 2x2:2
- Suporte para os seguintes modos de Radio
  - ✓ 5 GHz/2.4 GHz - Fixed
  - ✓ 5 GHz/5 GHz - Dual 5 GHz
- Plataforma de gestão em cloud gratuita
- Suporte a WPA3
- Filtro de Coexistência Celular

Suporte e Manutenção:

Manutenção de 12 meses incluindo peças e mão-de-obra.

- SLA 24x7 com tempo de resposta nas instalações no dia útil seguinte
- Prestação de assistência contínua até à solução da avaria
- O suporte deverá ser dado diretamente pelo fabricante localmente

Serviços de Instalação:

Pretende-se o fornecimento dos seguintes serviços:

- Fixação dos Pontos de Acessos nos locais definidos
- Configuração dos acessos a plataforma de gestão em Cloud
- Adição dos Pontos de acessos a Plataforma e criação dos SSID e respetivas políticas de acessos
- Testes de funcionamento

Firewall:

Pretende-se o fornecimento de uma firewall que incorpora uma plataforma de gestão capaz de gerir e monitorizar outros equipamentos instalados local ou geograficamente dispersos. Toda a componente de reporting da solução a adquirir no âmbito deste procedimento deverá ser parte integrante da solução. Cada equipamento a propor deverá cumprir os seguintes requisitos:

- O fabricante deverá ter no mínimo 20 anos de experiência no mercado da segurança, e desenvolver em exclusivo, apenas soluções de segurança;
- O fabricante deverá comprovar a sua liderança em soluções de segurança (UTM, Firewall e prevenção de intrusões) ano após ano, em análises/relatórios de entidades independentes;
- O fabricante deverá endereçar todos os requisitos de um equipamento de segurança (Firewall), tais como processamento de largura de banda, número de ligações, capacidade de securização de aplicações de nova geração em todas as vertentes da rede (escritório, centro de dados) num único equipamento;
- O fabricante deverá disponibilizar as mesmas funcionalidades de inspeção avançada (Firewall, intrusion prevention, application control, URL filtering, Anti-Bot, Anti-Virus, Sandboxing) em modelo físico e virtual, quaisquer destas geridas por uma única consola central e dedicada;
- A solução proposta, deverá endereçar todas as funcionalidades que se seguem, de forma unificada, suportadas e desenvolvidas somente pelo mesmo fabricante (single vendor):
    - ✓ Statefull Inspection Firewall - A gateway deverá inspecionar end-to-end (não apenas “half-way” ou “header”) todos os fluxos de comunicação desde o estabelecimento da sessão (3-way handshake TCP), durante a transferência de informação (payload), até que esta seja terminada;
    - ✓ Intrusion Prevention System;
    - ✓ User Identity Acquisition
    - ✓ Application Control and URL filtering
    - ✓ Anti – Bot / Anti – Virus
    - ✓ Threat Emulation (Sandboxing)
    - ✓ Threat Extraction (scrubbing)
    - ✓ Anti – Spam and Email Security
    - ✓ IPSec VPN
    - ✓ Remote Access VPN (Mobile Access)
    - ✓ Data Loss Prevention
    - ✓ Logging and Status

- ✓ Event Correlation and Reporting

- A solução proposta, não poderá em momento algum "sacrificar" a segurança em detrimento da performance (desabilitar inspeção end-to-end em cenários de "carga" na plataforma)
- A solução proposta deverá conter uma plataforma de gestão dedicada com:
  - ✓ Centralização de políticas, logs, reports;
  - ✓ Sem limite de storage com base em requisitos de licenciamento;
  - ✓ O servidor de gestão deverá ter a capacidade de obter detalhes de configuração diretamente das gateways de firewall (fetch de informação de routing, interfaces, etc.) de forma "automática", e não apenas se estas forem instanciadas previamente via template, a partir do servidor de gestão;
- Requisitos mínimos de Performance:
  - ✓ Threat Prevention/Extraction >=1.7 Gbps
  - ✓ NextGen Firewall >=3.7 Gbps
  - ✓ Intrusion Prevention System >= 4.6 Gbps
  - ✓ VPN Throughput >= 2.5 Gbps
  - ✓ Firewall Throughput >= 8.5 Gbps
  - ✓ Connections per second 67 k
  - ✓ Concurrent Connections 2 M
- Requisitos físicos mínimos:
  - ✓ Disco de 240Gb
  - ✓ 8GB de Memoria
  - ✓ 10 Interfaces 10/100/100
  - ✓ Interface de Gestão dedicado
- Possibilidade de expandir a memória até 32 GB
- Modularidade de interfaces
  - ✓ Deverá ser flexível quanto o número/tipos de interfaces a aplicar ao chassis:
    - 8x1GE UTP (até 18 portas);
    - 4x1GE SFP (até 4 Portas);
    - 4x10GE SFP+ (até 4 Portas);
- Possibilidade de Interface LOM (Lights Out Management)
- Possibilidade de Fontes de Alimentação Redundantes
- Dimensões: 17.2 x 20 x 1.73 in.(438 x 508 x 44mm)
- Peso (Base/Plus): 14.9/16.5 lbs. (6.75/7.5 kg)

Requisitos - Funcionalidades de rede:

- Suporte para 1024 interfaces vlan;
- Suporte para 4096 interfaces vlan (em cenário de contextos virtuais de firewall);
- Suporte para protocolos de agregação de links (LACP 802.3ad);
- Suporte para funcionamento em modo L2 (bridging) e L3 (routing);
- Suporte de NAT
  - ✓ Static, Hide, PAT
  - ✓ NAT44, NAT46, NAT64, NAT66
- Suporte para routing estático;
- Suporte para Policy Based Routing (PBR);
- Suporte para protocolos de routing dinâmico:
  - ✓ BGP, OSPF (v2 | v3), RIP
  - ✓ Suporte para multicast
- Routing Multicast
  - ✓ L2 (IGMP v1 | v2)
  - ✓ L3 (PIM-SM, PIM-SSM, PIM-DM)

Requisitos técnicos/lógicos:

- O equipamento de segurança, deve utilizar a tecnologia de Stateful Inspection, para construir e manter a tabela de sessões (fluxos de comunicação);
- O Equipamento de segurança deve ser capaz de suportar o debito, número de novas ligações e manutenção das mesmas de acordo com as necessidades do cliente;
- A solução deve identificar/controlar o acesso de pelo menos 150 serviços/protocolos;
- Na interface da plataforma de gestão deve ser possível visualizar número de acessos por regra;
- A solução tem de suportar que se apliquem regras em intervalos de tempo, para que seja possível definir o tempo útil das mesmas;
- A comunicação entre a firewall e a solução de gestão, tem de ser encriptada e autenticada com recurso a infraestrutura própria de PKI;
- A Firewall tem de suportar métodos de autenticação por sessão, utilizadores e clientes;
- Os seguintes métodos de autenticação de utilizadores têm de ser suportados pelos módulos de VPN e Firewall:
  - ✓ Tokens (ie -SecureID)
  - ✓ TACACS
  - ✓ RADIUS
  - ✓ Certificados Digitais

- A solução tem de ter base de dados de utilizadores local, para permitir a autenticação e autorização dos mesmos sem recurso a um dispositivo externo;
- A solução tem de suportar as funções de DHCP server e Relay;
- A solução tem de suportar o suportar a função de proxy em HTTP e HTTPS;
- A solução tem de ter capacidade de trabalhar em modo transparente/Bridge (L2).

Sistema de prevenção de intrusões (IPS):

- O fabricante deve fornecer evidências da sua posição de liderança, ano após ano, no Quadrante Mágico do Gartner para:
  - ✓ Soluções de Prevenção de Intrusão
  - ✓ Soluções de Firewall Enterprise
- O IPS deve ser baseado nos seguintes mecanismos de deteção:
  - ✓ Assinaturas
  - ✓ Anomalias no protocolo
  - ✓ Controlo Aplicacional
  - ✓ Análise de comportamento
- Os Módulos de IPS e firewall devem estar integrados na mesma plataforma;
- O administrador deve ter a possibilidade de configurar a inspeção para proteção apenas da rede interna;
- O IPS deve ter opções para criar perfis com base em assinaturas para proteção de Clientes ou servidores. Também deve ser possível criar um perfil para proteção de ambos;
- O IPS deve fornecer pelo menos dois perfis/políticas predefinidas que podem ser utilizados no deployment da solução;
- O IPS deve ter um mecanismo fail-open baseado em software, ajustável com base em limites do gateway, CPU ou utilização de memória;
- O IPS deve ter mecanismo automático para ativar ou gerir as novas assinaturas após atualizações;
- O IPS deve suportar exceções com base em origem, destino, protocolo, ou uma combinação dos três;
- O IPS deve permitir mudar para o modo de deteção, sem alterar parâmetros individuais, por forma a facilitar as ações de troubleshooting;
- O IPS deve possuir uma solução centralizada de correlação e relatório de eventos;
- O administrador deve poder ativar de forma automática novas proteções, com base em parâmetros configuráveis:
  - ✓ Impacto no desempenho
  - ✓ Grau de severidade da ameaça

- ✓ Nível de confiança
- ✓ Proteções do cliente
- ✓ Proteções do servidor

- O IPS deve ser capaz de detetar e prevenir os seguintes tipos de ameaça:
  - ✓ Uso indevido de protocolo
  - ✓ Comunicações de malware
  - ✓ Tentativas de uso de protocolos de tunneling
  - ✓ Tipos genéricos de ataque sem assinaturas predefinidas
- Para cada proteção, a solução deve incluir o tipo de proteção (relativamente a servidor ou cliente):
  - ✓ Gravidade da ameaça
  - ✓ Impacto no desempenho
  - ✓ Nível de confiança
  - ✓ Referência - (ie CVE)
- O IPS deve ser capaz de capturar pacotes/evidencias para proteções específicas;
- O IPS deve ser capaz de detetar e bloquear ataques nas layers de network e application layer, protegendo pelo menos os seguintes tipos de serviços:
  - ✓ Serviços de email
  - ✓ DNS
  - ✓ FTP
  - ✓ Serviços do Windows (Microsoft Networking)
- O fornecedor deve fornecer evidências de liderança na proteção de vulnerabilidades Microsoft;
- O IPS e/ou o Application Control deve incluir a capacidade de detetar e bloquear aplicações P2P e evasivas (Anonymizers);
- O administrador deve poder definir exclusões a plataforma de IPS, baseadas em redes ou hosts;
- A solução deve proteger DNS Cache Poisoning e impedir o acesso dos utilizadores a endereços de domínio bloqueados;
- Solução deve fornecer proteções para protocolos VOIP;
- O IPS e/ou o Application Control devem detetar e bloquear aplicações que permitam controlo remotos, incluindo as que são capazes de realizar tunneling sobre o tráfego HTTP;
- IPS deve ter proteções SCADA;
- IPS deve possibilitar a conversão de assinaturas SNORT;

- A solução deve permitir ao administrador bloquear de forma fácil o tráfego de entrada e/ou saída com base em países, sem a necessidade de gerir manualmente os intervalos de IP correspondentes ao país.

Aquisição de identidade de utilizadores (User ID Acquisition):

- Deve ser capaz de adquirir a identidade dos utilizadores, com base na consulta dos eventos de segurança da Microsoft Active Directory;
- Deve ser possível a autenticação através de uma browser, numa base de dados local, para utilizadores ou dispositivos que não pertençam ao domínio;
- Deve ter um agente que possa ser instalado nos endpoints, para reportar a firewall as identidades dos utilizadores;
- A solução deve integrar-se perfeitamente com Microsoft Active Directory, IF-MAP e Radius;
- O impacto do uso da solução de aquisição de identidade no CPU das AD, deve ser inferior a 3%;
- A solução de aquisição de identidade deve suportar soluções de Terminal server e citrix;
- A solução deve permitir a identificação de utilizadores que acedem através de um proxy (exemplo: X-forwarded headers);
- Deve ser capaz de adquirir a identidade de um utilizador presente numa Microsoft Active Directory sem qualquer tipo de agente instalado no controlador de domínio;
- Deve suportar autenticação Kerberos para single sign on;
- Deve suportar LDAP nested groups;
- Deve ser capaz de partilhar identidades de utilizadores entre vários gateways de segurança;
- Deve ser capaz de criar identity roles (grupos de identidades) para serem invocados em diferentes aplicações da solução.

Filtragem de URL e Controlo de Aplicações:

- A solução deve reconhecer e controlar mais de 8000 aplicações conhecidas;
- A base de dados da solução deve conter mais de 200 milhões de URL's categorizados, abrangendo mais de 85% da Alexa's top 1M sites;
- A solução deve permitir criar uma regra de filtragem de conteúdos com várias categorias;
- A solução deve permitir filtrar conteúdos de URL's baseada em HTTPS sem efetuar inspeção de SSL;

- A solução deve ser capaz de filtrar um único site sendo este identificado em várias categorias;
- A solução deve permitir criar regras de segurança por utilizador ou grupo de utilizadores;
- A solução, após 4 semanas de produção, deve ter em cache cerca de 99% das solicitações de categorização;
- A solução deve ter uma interface fácil de pesquisa de aplicações e URL's;
- A solução deve categorizar aplicações e URL's por fator de risco;
- A política de URLF e Application Control deve poder ser definida por identidade do utilizador;
- A base de dados de URLF e Application Control devem ser atualizados por um serviço Cloud;
- A solução deve ter o controlo de aplicações e URLF unificado na mesma política;
- A solução deve ter mecanismos para informar ou perguntar ao utilizador em tempo real, para os educar ou para confirmarem as suas ações com base na política de segurança;
- A solução deve ter mecanismo que permita limitar o uso de aplicações com base no consumo de largura de banda;
- A solução deve permitir exceções com base em objetos de rede previamente definidos;
- A solução deve fornecer a opção de modificar a página de Bloqueio e redirecionar o utilizador para uma página de remediação;
- A solução deve incluir um mecanismo de Black e White List, para permitir que se negue ou permita URL's específicos, independentemente da categoria;
- A solução deve fornecer um mecanismo de substituição na categorização de URL.

Anti-bot e Anti-Virus:

- O fornecedor deve ter solução de Anti-Bot e Anti-Virus integrado na firewall;
- A Solução de Anti-Bot deve ser capaz de detetar e parar comportamentos de rede suspeitos;
- O aplicativo Anti-Bot deve usar um mecanismo de detecção baseado em varias pontos. Reputação de endereços IP, URLs e DNS e detectar padrões de comunicação de bots;
- A proteção Anti-Bot deve ter capacidade de efetuar Scan a ações de bot;
- A solução deve apoiar a detecção e prevenção de vírus e variantes de Cryptors & ransomware (por exemplo, Wannacry, Cryptlocker, CryptoWall ...) através do uso de análise estática e/ou dinâmica;
- A solução deve ter suporte para proteção contra-ataques de spear phishing;

- DNS based attacks - A solução deve ter recursos de deteção e prevenção para C&C DNS hideouts:
  - ✓ Pesquisa de padrões de tráfego de C & C, não apenas no destino de DNS
  - ✓ Reverse engineer do Malware para descobrir seu DGA (Domain Name Generation)
  - ✓ DNS Trap, como parte da politica de ameaças, interceta e analisa tentativas de comunicações do endpoint com C&C
  - ✓ A solução deve detetar e prevenir ataques de DNS tunneling
- A política de Anti-Bot e Anti-Virus deve ser gerida a partir de uma consola central;
- A solução de Anti-Bot e Anti-Virus deve ter um mecanismo centralizado de correlação e relatório de eventos;
- A solução de antivírus deve ser capaz de impedir o acesso a sites maliciosos;
- A solução de antivírus deve poder inspecionar o tráfego SSL;
- O Anti-Bot e o Anti-Virus devem ter atualizações em tempo real na cloud;
- O Antivírus deve ser capaz de impedir a entrada de arquivos maliciosos;
- O Antivírus deve ser capaz de analisar arquivos compactados;
- Políticas antivírus e Anti-Bot devem ser geridas centralmente e ser possível a parametrização das mesmas;
- O Antivírus deve suportar a analise de links dentro de emails;
- O antivírus deve analisar os ficheiros que estão passam no protocolo CIFS.

Emulação e Extração de Ameaças

- A solução deve ter a capacidade de proteger contra ataques desconhecidos (malware Zero Day) antes que proteções de assinatura estática sejam criadas:
  - ✓ Proteção em Tempo Real para malware desconhecido na navegação Web
  - ✓ Proteção em Tempo Real para malware desconhecido em email
- Cenários de implantação:
  - ✓ A solução deve fazer parte da arquitetura de prevenção de ameaças (com IPS, AV, AB, URLF, APP FW)
  - ✓ A solução deve fornecer solução de implementação On Prem e Cloud Based
  - ✓ Solução de Cloud pura
  - ✓ A solução deve suportar integração com 3rd party (public API)
  - ✓ A solução deve suportar implementação em modo in-line
  - ✓ A solução deve suportar a implementação modo MTA (Mail Transfer Agent)
  - ✓ A solução deve suportar implementação em modo de porta TAP / SPAN

- ✓ A solução não deve exigir infraestrutura separada para proteção email e proteção Web
- ✓ A solução deve suportar a implementação em modo cluster

- Tipos de ficheiros Suportados - A solução deve ser capaz de emular executáveis, arquivos, documentos, JAVA e flash especificamente:
  - ✓ 7z, cab, csv, doc, docm, docx, dot, dotm, dotx, exe, jar, pdf, potx, pps, ppsm, ppsx, ppt, pptm, pptx, rar, rtf, scr, swf, tar, xla, xls, xlsb, xlsm, xlsx, xlt, xltm, xltx, xlw, zip, pif, com, gz, bz2, tgz, apk(android), ipa (iphone), ISO, js, cpl, vbs, jse, vba, vbe, wsf, wsh
- A solução deve ser capaz de emular executáveis, arquivos, documentos, JAVA e flash, que sejam transmitidos pelos protocolos:
  - ✓ HTTP
  - ✓ HTTPS
  - ✓ FTP
  - ✓ SMTP
  - ✓ CIFS (SMB)
  - ✓ TLS SMTP
- OS support:
  - ✓ O mecanismo de emulação deve suportar vários sistemas operativos, como XP e Windows7, 8,10 32/64 bits, incluindo imagens personalizadas
  - ✓ A solução deve suportar cópias LICENCIADAS de Microsoft WINDOWS e Microsoft Office através de um contrato com a Microsoft
  - ✓ A solução deve detectar chamadas API, alterações em ficheiros, system registry, ligações de rede e processos do sistema
  - ✓ A solução deve suportar análise estática para windows, mac OS-X, Linux ou qualquer plataforma x86
- O mecanismo de emulação deve ser capaz de inspecionar, emular, prevenir e compartilhar os resultados do evento de sandbox na infraestrutura de anti-malware;
- A solução deve permitir a emulação de ficheiros maiores que 10 Mb, em todos os tipos suportados;
- A solução deve suportar automated machine learning based detection engines;
- A solução deve detectar o ataque na fase de exploitation - ou seja, antes que o código seja executado e antes que se tenha concluído o download do malware;
- A solução deve detectar ROP e outras técnicas de exploitation (por exemplo, elevação de privilégios), analizando o CPU;

- A solução deve suportar a analise de links no corpo do e-mail para deteção de Malware Zero Day;
- A solução deve ser capaz de verificar o histórico de URLs registrados nos últimos X e-mails e verificar se a classificação foi alterada (por exemplo: de Clean para malicious);
- Tempo médio de emulação, para um veredito de malware suspeito como benigno não deve ser muito superior a 1 minuto;
- Tempo médio de emulação, para um veredito de malware suspeito como maligno não deve ser muito superior a 3 minutos;
- A solução de emulação de ameaças deve permitir "Geo Restriction", que permite que as emulações sejam restritas a um país;
- A solução deve possuir um mecanismo automático de partilha de informação com outros gateways em meio a atualizações de assinaturas etc, por forma a partilhar informações sobre novos ataques;
- O mecanismo de emulação deve exceder 90% na taxa de captura nos testes do Total de vírus em que os PDFs e os arquivos maliciosos conhecidos são modificados com cabeçalhos "não usados" para demonstrar a capacidade das soluções de detetar malwares desconhecidos;
- A solução deve detetar o tráfego de C & C de acordo com a reputação dinâmica de ip / url;
- A solução deve ser capaz de emular e extrair arquivos incorporados em documentos;
- A solução deve ser capaz de analisar documentos com URL's;
- Na funcionalidade de Sandboxing/Scrubbing, a solução proposta deverá ter a capacidade de suportar deteção de ameaças e técnicas de evasão (com tentativas de explorar vulnerabilidades de S.O.) ao nível do CPU – CPU-Level detection;

Deteção de atividades em sistema

- A solução deve ter a capacidade de detetar atividades fora de "padrão de utilização/protocolo":
  - ✓ Chamadas de API
  - ✓ Alterações no sistema de arquivos
  - ✓ Alterações de Registo
  - ✓ Ligações de rede
  - ✓ Em Processos do sistema Operativo
  - ✓ Criar e eliminar arquivos
  - ✓ Modificação de arquivos
  - ✓ Adição de código ao kernel
  - ✓ Detetar tentativas de elevação de privilégios

- ✓ Alterações no kernel (Alterações de memória realizadas pelo código do kernel, não o fato de que um driver ser carregado - isso é controlado pelo item acima)
- ✓ Analise de comportamento do kernel (analisar a atividade do código, não as alterações efetuadas pelo utilizador)
- ✓ Contornar UAC (user access control)

Mecanismos Anti-evasão

- A solução proposta deverá ter capacidade de deteção de técnicas de evasão (emulação/sandboxing) para posterior reação e mitigação de ameaças;
- A solução deverá ser resiliente e identificar casos onde a execução de código malicioso (malware/shell-code) não ocorra mediante a deteção de um ambiente virtualizado (técnica de evasão para contornar mecanismos de deteção por sandboxing);
- A solução deverá ser resiliente e detetar delays implementados na execução de código malicioso (malware/shell-code);
- A solução deverá ser resiliente a situações em que a execução de código malicioso (malware/shell-code) apenas ocorre após um restart/shutdown da workstation/endpoint infetado;

Extração de ameaças (File Scrubbing/Flattening)

- A solução proposta deverá ter a capacidade de eliminar ameaças existentes em conteúdos dinâmicos/objetos embebidos em ficheiros;
- A solução proposta deverá ter a capacidade de reconstrução dos ficheiros, excluindo os conteúdos ativos, e mantendo apenas conteúdos seguros;
- A solução proposta deverá ter a capacidade de converter ficheiros reconstruídos (em que os conteúdos ativos foram excluídos) em formato PDF, para serem entregues em tempo real ao utilizador, de forma a melhorar a experiencia de utilização;
- A solução proposta deverá ser configurável e flexível, de forma a possibilitar manter o formato do ficheiro original, especificando o tipo de conteúdo a ser removido;

Anti-Spam & Email Security

- A solução deverá ser agnóstica em relação ao conteúdo, e ter a capacidade de classificar ameaças em tempo real, protegendo a infraestrutura com base padrões comportamentais, e não com base em conteúdo;
- A solução proposta deverá incluir mecanismos de proteção com base em serviços online de IP reputation, de forma a evitar falsos positivos;

- A solução deverá incluir mecanismos de proteção imediata (Dia Zero) para novos vírus propagados por email.

IPsec VPN

- A solução deverá suportar implementações de VPN (domain based, e route based com protocolos de routing dinâmico e virtual tunnel interfaces), com utilização de Internal Certificate Authority ou External 3rd party Certificate Authority;
- A solução deverá suportar criptografia 3DES e AES-256 para IKE Phase 1 e 2;
- A solução deverá suportar criptografia IKEv2 plus "Suite-B-GCM-128" e "Suite-B-GCM-256" for IKE Phase 2;
- A solução deverá suportar os seguintes grupos Diffie-Hellman: Group 1 (768 bit), Group 2 (1024 bit), Group 5 (1536 bit), Group 14 (2048 bit), Group 19 and Group 20;
- A solução deverá suportar os seguintes tipos de mecanismos de integridade de dados: md5, sha1, SHA-256, SHA-384 and AES-XCBC;
- A solução proposta deverá suportar as seguintes funcionalidades VPN:
  - ✓ Site-to-site:
    - Full Mesh (todos para todos)
    - Estrela (Sites remotos para Site principal)
    - Hub&Spoke (Site remotoA para Site RemotoB, através de site principal)
    - Suporte para configuração através de GUI, com opção de drag&drop de objetos nas comunidades VPN
  - ✓ Suporte para VPN's de acesso remoto "clientless" e "client based"
  - ✓ Suporte para aplicação de políticas de segurança específicas, para controlo de tráfego associado à comunidade VPN
  - ✓ A solução proposta deverá incluir licenciamento para 50 VPN´s simultâneas

Security Management

- A solução deverá possibilitar a segmentação da política de segurança numa estrutura de subpolíticas;
- A solução deverá possibilitar a segmentação da política de segurança numa estrutura de layers;
- A solução deverá possibilitar a integração de logs e audit logs numa única consola, para contextualizar o administrador ao efetuar alterações sobre a política de segurança;
- A solução de gestão deverá suportar role based access control, para segregar acessos de administração para gestão de política e visualização de logs;

- A solução deverá implementar um mecanismo de comunicação segura, assente em certificados, entre todas as componentes de segurança integradas no sistema de gestão centralizada;
- A solução deverá incluir um Certificate Authority x.509 com capacidade para gerir/gerar certificados internos, para autenticação de utilizadores em acessos VPN remotos;
- A solução deverá disponibilizar um mecanismo de pesquisa para facilitar a utilização e identificação de objetos, com base no seu endereço IP;
- A solução deverá disponibilizar métricas de "hit count" nas regras presentes na política de segurança;
- A solução deverá possibilitar a utilização de etiquetas (labels) ou secções (tabs) para melhor organização da política de segurança;
- A solução deverá permitir gravar a política de forma integral ou parcial;
- A solução deverá disponibilizar um mecanismo de validação da política de segurança, antes da sua instalação nas gateways de firewall;
- A solução deverá disponibilizar um mecanismo de backup e revisão da política de segurança, possibilitando comparar versões da política e reverter para versões anteriores, se necessário;

Logging e Monitorização

- A solução de logging, deverá estar integrada na componente de gestão centralizada, e possibilitar a visualização de logs afetos a políticas específicas, sem ser necessário recorrer a uma nova janela, ou aplicação;
- A solução deverá poder ser integrada na componente de gestão centralizada, ou numa appliance/máquina virtual dedicada;
- A solução deverá ter a capacidade de produzir logs de todas as políticas (30k logs/seg);
- A solução deverá ter a capacidade de consolidar os logs de todas as componentes de segurança que se encontrem ativas na platafora: IPS, Application Control, URL Filtering, Anti-Virus, Anti-Bot, Anti-Spam, User Identity, Mobile Access;
- A solução deverá suportar um mecanismo de captura de pacotes para eventos de IPS, para facilitar despiste e análise forense;
- A solução deverá implementar um mecanismo seguro de forwarding de logs, com autenticação e encriptação, para evitar potenciais ataques (ex. Eavesdropping):
  - ✓ Os logs deverão ser transferidos de forma segura entre a FW gateway, o log server, e o utilizador final
- A solução deverá disponibilizar detalhes sobre o estado de todos os túneis IPSEC, site-to-site e remote access (client-to-site);

- A solução deverá possibilitar a customização de valores de threshold, para execução de ações, uma vez atingido/ultrapassado esse threshold: log, alert, snmp-trap, email notification.

Correlação de eventos e reporting

- A solução deverá integrar a componente de reporting e correlação de eventos com a sua componente de gestão centralizada;
- A solução deverá ter a capacidade de correlacionar eventos de todas as funcionalidades ativas nas demais gateways (FW, IPS, URL-F, etc.);
- A solução deverá possibilitar a criação de filtros de logging, com base em qualquer característica, tal como: aplicação, ip de origem e destino, serviço, tipo de evento, severidade do ataque, país de origem e destino, etc.;
- A solução deverá disponibilizar um mecanismo para assignar os filtros criados a diferentes tipos de gráficos, a serem atualizados periodicamente, apresentando todos os eventos que igualem o filtro aplicado, permitindo ao operador focar-se nos eventos mais importantes;
- A solução deverá assegurar a possibilidade de pesquisar na lista de eventos, e garantir o "drill down" de detalhes em pesquisas e análise forense;
- A solução deverá ter capacidade de detectar e alertar para eventos de login de administradores, em horários não frequentes;
- A solução deverá detetar ataques de "credential guessing / brute force";
- A solução deverá reportar todos os eventos de alteração/instalação de políticas de segurança;
- A solução deverá incluir relatórios horários, diários, semanais e mensais predefinidos, incluindo pelo menos: Top Events, Top Sources, Top Destinations, Top Services, etc.;
- A solução de reporting deverá disponibilizar informação consolidada sobre:
  - ✓ Volume de ligações bloqueadas por uma regra de segurança em particular
  - ✓ Top de origens bloqueadas, e os destinos e serviços respetivos
  - ✓ Top de regras mais utilizadas na política de segurança
  - ✓ Top de ataques detetados no perímetro, com informação das origens e destinos associados
  - ✓ Atividade web por user, com top de web users e websites mais utilizados

Compliance e Boas Práticas

- A solução deverá contemplar Risk Governance e Compliance totalmente integrado na componente de gestão centralizada;

- A solução deverá ter uma opção para controlar o cumprimento em tempo real de todos os serviços de segurança do produto;
- A solução deverá ter uma opção para entregar a avaliação em tempo real de acordo com as regulamentações principais (tais como: PCI-DSS, HIPAA,SOX, GDPR...);
- A solução deverá ter uma opção para notificação imediata sobre as mudanças nas políticas que afetem o cumprimento das certificações;
- A solução deverá ter uma opção para disponibilizar recomendações práticas para melhorar a conformidade de segurança;
- A solução deverá ter uma opção para recomendar Práticas recomendadas de segurança;
- A solução deverá ter uma opção para traduzir os requisitos regulamentares em melhores práticas de segurança acionáveis;
- A solução deverá ter uma opção para monitorizar constantemente a configuração das gateways com as melhores práticas de segurança;
- A solução deverá ter uma opção para gerar relatórios de avaliação automatizados para avaliar a conformidade com os principais regulamentos;
- A solução deverá ter uma opção para integrar plenamente na infra-estrutura de arquitetura de Software e Gestão;
- A solução deverá ter uma opção para verificar a conformidade com cada mudança de política para todas as funcionalidades dos equipamentos de firewall.

SSL Inspection (inbound / outbound)

- A solução deverá suportar inspecção SSL (inspection/decryption) com performance comprovada em todas as tecnologias de mitigação;
- A solução deverá suportar Perfect Forward Secrecy (PFS , ECDHE cipher suites);
- A solução deverá suportar AES-NI,AES-GCM for improved throughput;
- A solução deverá suportar a integração das tecnologias de emulação/sandboxing com inspecção SSL;
- A solução deverá permitir a reutilização da base de dados de URL Filtering, para criação de políticas de inspeção de SSL granulares.

Suporte e Manutenção

O suporte e manutenção, deve ser assegurado diretamente pelo fabricante. A manutenção pretendida é a seguinte:

Manutenção de 12 meses incluindo peças e mão-de-obra.

- SLA 24x7 com tempo de resposta nas instalações no dia útil seguinte;
- Prestação de assistência contínua até à solução da avaria.

Serviços de Instalação

- Instalação da FW no Bastidor;
- Inicialização da FW na rede e domínio do cliente;
- Adição da FW a consola de gestão;
- Ativação das funcionalidades adicionais;
- Configuração das redes;
- Migração das regras da FW existente para nova FW;
- Revisão das regras e aplicação de regras adicionais;
- Testes de funcionamento.

Passivos

- 3 x Cabo U/UTP Cat.6 LSZH caixa 305m – violeta
- 2 x Painel vazio p/ 24xRJ45 Cat.6 1HU preto (para con. 61000BB/FW)
- 2 x Patch Guide 1HU 4 argolas metal preto
- 16 x Conector UTP Cat.6
- 13 x Cordão Cat.6 1.0m LSOH cinza
- 13 x Cordão UTP Cat.6 0,5m cz
- 13 xTomada simples saliente
- 100 x Cabo FO 4x50/125 OM4 LSZH loose tube int./ext.
- 300 x Cabo FO 8x50/125 OM4 LSZH loose tube int./ext.
- 12 x Adaptador LC dx MM
- 24 x Pigtail LC OM4 50/125 1m
- 24 x Mangas
- 24 x Fusoes
- 4 x Cordão LC/LC 50/125 OM4 duplo 2m
- 3 x Organizador de fibras opticas
- 3 x Painel FO 24xSC sx / 24xLC dx / 24xE2000 1HU extraível
- 40 xCalha 32/16 Efapel

Serviços de Instalação

- Substituição das fibras de ligação existentes entres o Bastidores do Biotério e o Data Center (FO 8), e o Bastidor Biotério e o Bastidor Secundário;

- Passagem de Cabo Cat6 para ligação de 3 camaras CCTV e 9 pontos de acessos dispersos pelo edifício Biotério;
- Prever na proposta calha para a eventualidade de não existir caminho de cabos para algum dos pontos de rede;
- Certificação das Fusões de Fibra;
- Certificação das ligações Cat6.