

INSTITUTO POLITÉCNICO DO PORTO

CONCURSO PÚBLICO INTERNACIONAL

**AQUISIÇÃO E SERVIÇOS DE INSTALAÇÃO DE
SOLUÇÃO DE SEGURANÇA DE FIREWALL
PARA O INSTITUTO POLITÉCNICO DO PORTO**

REF^a. 27/000/A/578_2022

CADERNO DE ENCARGOS

PORTO, 2022

Índice

Cláusula 1. ^a	4
Objeto	4
Cláusula 2. ^a	4
Contrato	4
Cláusula 3. ^a	4
Prazo de execução	4
Cláusula 4. ^a	5
Obrigações principais do Fornecedor	5
Cláusula 5. ^a	5
Conformidade e operacionalidade dos bens	5
Cláusula 6. ^a	5
Inoperacionalidade, defeitos ou discrepâncias	5
Cláusula 7. ^a	5
Entrega e instalação dos bens objeto do contrato	5
Cláusula 8. ^a	6
Garantia técnica	6
Cláusula 9. ^a	7
Garantia de continuidade de fabrico	7
Cláusula 10. ^a	7
Objeto do dever de sigilo	7
Cláusula 11. ^a	7
Prazo do dever de sigilo	7
Cláusula 12. ^a	8
Proteção de dados pessoais	8
Cláusula 13. ^a	8
Requisitos técnicos, funcionais e ambientais mínimos dos bens	8
Cláusula 14. ^a	8
Preço contratual	8
Cláusula 15. ^a	9
Condições de pagamento	9
Cláusula 16. ^a	9
Penalizações	9
Cláusula 17. ^a	10
Atualização de equipamentos	10
Cláusula 18. ^a	10
Resolução do contrato por parte do contraente público	10

Cláusula 19. ^a	10
Resolução do contrato por parte do fornecedor	10
Cláusula 20. ^a	11
Casos fortuitos ou de força maior	11
Cláusula 21. ^a	11
Foro competente	11
Cláusula 22. ^a	11
Comunicações e notificações	11
Cláusula 23. ^a	11
Contagem dos prazos	11
Cláusula 24. ^a	11
Legislação aplicável	11
ANEXO I – ESPECIFICAÇÕES TÉCNICAS	12
1. Arquitetura:	12
2. Certificações e Conformidade	14
3. Funcionalidades da Solução de Segurança:	14
4. Funcionalidades de Firewall, VPN e IPS/IDS e Proteção contra ameaças:	16
5. Administração, Monitorização e Diagnósticos:	18
6. Integração com redes de comunicações:	19
7. Especificações técnicas dos equipamentos, quantidades e manutenção e suporte em conformidade com a Tabela 1. Especificações técnicas dos equipamentos/serviços e quantidades	19
ANEXO II – MORADAS E CONTACTOS	29

CADERNO DE ENCARGOS**Cláusula 1.ª****Objeto**

O presente Caderno de Encargos compreende as cláusulas a incluir no contrato a celebrar na sequência do procedimento pré-contratual de concurso público internacional, que tem por objeto principal a **Aquisição e Serviços de Instalação de Solução de Segurança de Firewall para o Instituto Politécnico do Porto (P.PORTO)**.

Cláusula 2.ª**Contrato**

1. O contrato é composto pelo respetivo clausulado contratual e os seus anexos.
2. O contrato a celebrar integra ainda os seguintes elementos:
 - 2.1. Os suprimientos dos erros e das 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;
 - 2.2. Os esclarecimentos e as retificações relativos ao Caderno de Encargos;
 - 2.3. O presente Caderno de Encargos;
 - 2.4. A proposta adjudicada;
 - 2.5. Os esclarecimentos sobre a proposta adjudicada prestados pelo adjudicatário.
3. Em caso de divergência entre os documentos referidos no número anterior, a respetiva prevalência é determinada pela ordem pela qual aí são indicados.
4. Em caso de divergência entre os documentos referidos no n.º 2 e o clausulado do contrato e seus anexos prevalecem os primeiros, salvo quanto aos ajustamentos propostos de acordo com o disposto no artigo 99.º do Código dos Contratos Públicos (doravante designado CCP, aprovado pelo Decreto-Lei n.º 18/2008, de 29 de janeiro, na sua redação atual) e aceites pelo adjudicatário nos termos do disposto no artigo 101.º desse mesmo diploma legal.

Cláusula 3.ª**Prazo de execução**

1. O contrato iniciará a sua execução aquando da assinatura, devendo os bens ser fornecidos e instalados e os serviços executados no prazo de **115 dias**.
2. O contrato vigorará até ao término do prazo de garantia e suporte, 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.

Cláusula 4.ª**Obrigações principais do Fornecedor**

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 fornecedor as seguintes obrigações principais:

1. Obrigação de entrega dos bens identificados na sua proposta;
2. Obrigação de execução dos serviços identificados na sua proposta;
3. Obrigação de garantia dos bens;
4. Obrigação de comunicar ao P.PORTO, factos que tornem total ou parcialmente impossível o fornecimento de bens objeto do contrato de acordo com prazo definido pelo presente caderno de encargos, bem como o cumprimento de qualquer outra das suas obrigações nos termos do disposto no contrato, logo que tenha conhecimento dos mesmos.

Cláusula 5.ª**Conformidade e operacionalidade dos bens**

1. O fornecedor obriga-se a entregar ao contraente público os bens objeto do contrato com as características, especificações e requisitos técnicos previstos nas especificações técnicas presentes neste Caderno de Encargos, que dele fazem parte integrante.
2. Os bens objeto do contrato devem ser fornecidos em perfeitas condições de serem utilizados para os fins a que se destinam.
3. É aplicável, com as necessárias adaptações, o disposto na lei que disciplina os aspetos relativos à venda de bens de consumo e das garantias a ela relativas, no que respeita à conformidade dos bens.
4. O fornecedor é responsável perante o P.PORTO por qualquer defeito ou discrepância dos bens objeto do contrato que existam no momento em que os bens lhe são fornecidos.

Cláusula 6.ª**Inoperacionalidade, defeitos ou discrepâncias**

1. No caso dos bens objeto do contrato não estarem em conformidade com as exigências legais, ou no caso de existirem defeitos ou discrepâncias com as características, especificações e requisitos técnicos definidos no presente Caderno de Encargos, o P.PORTO deve disso informar, por escrito, o fornecedor.
2. No caso previsto no número anterior, o fornecedor deve proceder, à sua custa e no prazo razoável que for determinado pelo P.PORTO, às reparações ou substituições necessárias para garantir a operacionalidade dos bens e o cumprimento das exigências legais e das características, especificações e requisitos técnicos exigidos.

Cláusula 7.ª**Entrega e instalação dos bens objeto do contrato**

1. O prazo de entrega e instalação dos equipamentos e o prazo de execução dos serviços são os referidos a seguir, contados após a outorga do contrato:

- 1.1. Fase I – A entrega dos equipamentos, Appliances de Segurança de Firewall e componente de gestão, deve ser efetuada no prazo máximo de **40 dias** após a outorga do contrato.
- 1.2. Fase II – Os serviços de instalação e configuração dos equipamentos em paralelo com a solução atual de segurança de Firewall (item 8.1 das especificações técnicas), devem ser finalizados no prazo de **50 dias** após a outorga do contrato. Estes serviços poderão ser efetuados pelo fornecedor em paralelo nas várias escolas ou unidades orgânicas, com base em planeamento prévio proposto ao P.PORTO até 10 dias antes do final da Fase I. Planeamento esse que deverá ser aprovado pelo P.PORTO, no prazo de 7 dias após entrega do planeamento.
- 1.3. Fase III – Serviços de migração das políticas de segurança da solução de segurança de firewall CheckPoint atual para a nova solução (item 8.2 das especificações técnicas) e serviço de implementação de regras de *routing* dinâmico BGP entre o Data Center do P.PORTO e Data Center do ISEP (item 8.3 das especificações técnicas), finalizados no prazo máximo de **90 dias** após a outorga do contrato.
- 1.4. Fase IV – Serviços de testes e arranque, a ser finalizados no prazo máximo de **104 dias** após a outorga do contrato.
 - 1.4.1. Realização de conjunto de testes de funcionamento (item 8.4 das especificações técnicas), deverão ser realizados após a finalização da Fase III), em datas a propor ao P.PORTO, e finalizados no prazo máximo de **7 dias**.
 - 1.4.2. Serviço de arranque em produção e acompanhamento da solução de segurança, (item 8.5 das especificações técnicas), deverão ser realizados após a finalização da Fase IV i), em datas a propor ao P.PORTO, e finalizados no prazo máximo de **7 dias**.
- 1.5. Fase V – Serviços de formação (item 8.6 das especificações técnicas), deverão ser realizados após a finalização da Fase IV), a ser finalizados no prazo máximo de **115 dias** após a outorga do contrato.
2. Os bens objeto do contrato devem ser entregues e instalados nas entidades referidas no Anexo I ao presente Caderno de Encargos, nas moradas indicadas no Anexo II.

Cláusula 8.^a

Garantia técnica

1. Nos termos da presente cláusula e da lei que disciplina os aspetos relativos à venda de bens de consumo e das garantias a ela relativas, o fornecedor garante os equipamentos objeto do contrato, pelo prazo indicado para cada item no Anexo I ao presente Caderno de Encargos, ou no prazo mínimo de 3 anos se for omissivo, a contar da entrega dos bens, contra quaisquer defeitos ou discrepâncias com as exigências legais e com as características, especificações e requisitos técnicos definidos nas Especificações Técnicas do presente Caderno de Encargos, que se revelem a partir da respetiva aceitação do bem.
2. A garantia prevista no número anterior abrange:
 - 2.1. O fornecimento, a montagem ou a integração de quaisquer peças ou componentes em falta;

- 2.2. O fornecimento, a instalação e configuração de quaisquer softwares ou componentes de firmware que façam parte da solução proposta;
- 2.3. A desmontagem das peças, componentes ou bens defeituosos ou discrepantes;
- 2.4. A reparação ou a substituição das peças, componentes ou bens defeituosos ou discrepantes;
- 2.5. O fornecimento, a montagem ou instalação das peças, componentes ou bens reparados ou substituídos;
- 2.6. O transporte do bem ou das peças ou componentes defeituosos ou discrepantes para o local da sua reparação ou substituição e a devolução daqueles bens ou a entrega das peças ou componentes em falta, reparados ou substituídos;
- 2.7. A deslocação ao local da instalação ou de entrega;
- 2.8. A mão-de-obra.

Cláusula 9.^a

Garantia de continuidade de fabrico

O fornecedor deve assegurar a continuidade do fabrico e do fornecimento de todas as peças, componentes e equipamentos que integram os bens objeto do contrato pelo prazo de 10 anos, a contar da respetiva entrega.

Cláusula 10.^a

Objeto do dever de sigilo

- 1. O fornecedor deve guardar sigilo sobre toda a informação e documentação, técnica e não técnica, comercial ou outra, relativa ao P.PORTO, de que possa ter conhecimento ao abrigo ou em relação com a execução do contrato.
- 2. A informação e a documentação cobertas pelo dever de sigilo não podem ser transmitidas a terceiros, nem objeto de qualquer uso ou modo de aproveitamento que não o destinado direta e exclusivamente à execução do contrato.
- 3. Exclui-se do dever de sigilo previsto a informação e a documentação que fossem comprovadamente do domínio público à data da respetiva obtenção pelo fornecedor ou que este seja legalmente obrigado a revelar, por força da lei, de processo judicial ou a pedido de autoridades reguladoras ou outras entidades administrativas competentes.

Cláusula 11.^a

Prazo do dever de sigilo

O dever de sigilo mantém-se em vigor por tempo indeterminado após o cumprimento ou cessação, por qualquer causa, do contrato, sem prejuízo da sujeição subsequente a quaisquer deveres legais relativos, designadamente, à proteção de segredos comerciais ou da credibilidade, do prestígio ou da confiança devidos às pessoas coletivas.

Cláusula 12.ª**Proteção de dados pessoais**

1. As partes obrigam-se a cumprir, nos seus precisos termos, o disposto na legislação nacional e comunitária relativa à proteção da privacidade e de dados pessoais, nomeadamente o Regulamento Geral Sobre a Proteção de Dados (Regulamento (EU) 2016/679, de 27 de abril).
2. A entidade adjudicatária obriga-se ainda durante a vigência do contrato e após a sua cessação, a respeitar a confidencialidade sobre todos os dados pessoais e quaisquer elementos ou informações que tenham sido confiados pela contraparte ou de que tenham tido conhecimento, por força da adjudicação do presente procedimento, na estrita observância das instruções emitidas pelo P.PORTO e da legislação aplicável.
3. A entidade adjudicatária garante a segurança e proteção de dados, através do estabelecimento de uma política de segurança, de controlos adequados e de gestão de riscos.
4. Sempre que a relação contratual implique a subcontratação, deve ser garantido pelo cocontratante, sucessivamente, que terceiros que envolva na execução do contrato, respeitem as obrigações de sigilo e confidencialidade, bem como as relativas à proteção jurídica de bases de dados e ao tratamento de dados pessoais, nos termos legalmente previstos na legislação à proteção de dados pessoais, designadamente as constantes do artigo 28.º do Regulamento Geral Sobre Proteção de Dados. As obrigações previstas na presente cláusula são aplicáveis no caso de cessão da posição contratual.

Cláusula 13.ª**Requisitos técnicos, funcionais e ambientais mínimos dos bens**

1. O adjudicatário deve garantir o cumprimento da Diretiva n.º 2011/65/UE (RoHS), de 8 de junho, transposta para a ordem jurídica interna pelo Decreto-Lei n.º 79/2013, de 11 de junho, da Diretiva n.º 2012/19/UE (REEE), de 4 de julho, e da Diretiva n.º 2006/66/CE, de 6 de setembro, transposta para a ordem jurídica interna pelo Decreto-Lei n.º 152-D/2017, de 11 de dezembro.
2. Os cocontratantes devem, igualmente, garantir o cumprimento do Decreto-lei n.º 98/2010, de 11 de agosto, respeitante à classificação, embalagem e rotulagem das substâncias perigosas.

Cláusula 14.ª**Preço contratual**

1. Pelo fornecimento dos bens objeto do contrato, bem como pelo cumprimento das demais obrigações constantes do presente Caderno de Encargos, o P.PORTO deve pagar ao fornecedor o preço constante da proposta adjudicada, o qual não pode, porém, ser superior ao total de **€267.000,00 (Duzentos e sessenta e sete mil euros)**, valor acrescido de IVA à taxa legal em vigor.
2. Os preços referidos no número anterior incluem todos os custos, encargos e despesas cuja responsabilidade não esteja expressamente atribuída ao P.PORTO, incluindo as despesas de aquisição, transporte, armazenamento e manutenção de meios materiais bem como quaisquer encargos decorrentes da utilização de marcas registadas, patentes ou licenças.

Cláusula 15.ª**Condições de pagamento**

1. A quantia devida nos termos da cláusula anterior deve ser paga da seguinte forma:
 - 1.1. Conclusão da Fase I: Pagamento do valor correspondente a 60% da proposta adjudicada;
 - 1.2. Conclusão da Fase II: Pagamento do valor correspondente a 10% da proposta adjudicada;
 - 1.3. Conclusão da Fase III: Pagamento do valor correspondente a 20% da proposta adjudicada.
 - 1.4. Conclusão da Fase IV: Pagamento do valor correspondente a 5% da proposta adjudicada.
 - 1.5. Conclusão da Fase V: Pagamento do valor correspondente a 5% da proposta adjudicada.
2. A quantia devida pelo Instituto Politécnico do Porto, nos termos da cláusula anterior, deve ser paga no prazo de 30 dias após a receção da respetiva fatura, a qual só pode ser emitida após o vencimento da obrigação respetiva.
3. Para os efeitos do número anterior, a obrigação considera-se vencida com o cumprimento de entrega e instalação dos equipamentos referentes a cada uma das fases referidas no n.º 1 da cláusula 7.ª.
4. Os bens e serviços constantes do Anexo I do presente Caderno de Encargos, deverão ser faturados ao P.PORTO e as faturas enviadas para a morada Rua D. Roberto Frias, 712, 4200-465 Porto.
5. Em caso de discordância por parte do P.PORTO, quanto aos valores indicados nas faturas, deve este comunicar ao fornecedor, por escrito, os respetivos fundamentos, ficando o fornecedor obrigado a prestar os esclarecimentos necessários ou proceder à emissão de novas faturas corrigidas.
6. Desde que devidamente emitidas e observado o disposto no n.º 1, as faturas são pagas, preferencialmente, através de transferência bancária.

Cláusula 16.ª**Penalizações**

1. Excetuando as situações de forma maior devidamente justificadas e com enquadramento legal, pelo incumprimento de obrigações emergentes do Contrato, o Politécnico do Porto pode exigir do fornecedor o pagamento de uma pena pecuniária, de montante a fixar em função da gravidade do incumprimento, nos seguintes termos:
 - 1.1. Pelo incumprimento das datas e prazos de entrega dos bens:
 - 1.1.1. Um por cento do valor da encomenda, nos primeiros 30 (trinta) dias;
 - 1.1.2. Dois por cento do valor da encomenda, a partir do trigésimo primeiro dia e até ao sexagésimo dia; e
 - 1.1.3. Três por cento do valor da encomenda, a partir do sexagésimo primeiro dia.
 - 1.2. Por qualquer outro incumprimento a indemnização não excederá o quantitativo correspondente a 15% (quinze por cento) dos valores do contrato ainda por faturar.

2. Na determinação da gravidade do incumprimento, o Politécnico do Porto tem em conta, nomeadamente, a duração da infração, a sua eventual reiteração, o grau de culpa do fornecedor e as consequências do incumprimento.
3. Nas situações enquadráveis no número anterior, de acordo com o disposto no n.º 2 do artigo 308.º do CCP, e atento o preceituado na alínea c) do n.º 2 do artigo 307.º do CCP, deverá ser assegurado ao Fornecedor o direito de audiência prévia, tal como regulado no Código do Procedimento Administrativo, relativamente à intenção de aplicação da sanção.
4. O Instituto Politécnico do Porto pode compensar os pagamentos devidos ao abrigo do Contrato com as penas pecuniárias devidas nos termos da presente Cláusula.
5. As penas pecuniárias previstas na presente Cláusula não obstam a que o Instituto Politécnico do Porto exija uma indemnização pelo dano excedente.

Cláusula 17.ª

Atualização de equipamentos

1. Sempre que se verificar a descontinuidade de um modelo ou gama, o fornecedor deve pedir a sua substituição, devendo o fornecedor submeter esse pedido de atualização ao P.PORTO, por escrito, juntamente com uma declaração que confirme a descontinuidade emitida pelo fabricante do equipamento ou pelo representante oficial em Portugal.
2. As características técnicas do novo equipamento terão de ser iguais ou superiores às da proposta inicial.
3. O pedido de substituição tem de ser aceite pela entidade adjudicante, por escrito.

Cláusula 18.ª

Resolução do contrato por parte do contraente público

1. Sem prejuízo de outros fundamentos de resolução previstos na lei, o P.PORTO pode resolver o contrato, a título sancionatório, no caso de o fornecedor violar de forma grave ou reiterada qualquer das obrigações que lhe incumbem.
2. O direito de resolução referido no número anterior exerce-se mediante declaração enviada ao fornecedor.

Cláusula 19.ª

Resolução do contrato por parte do fornecedor

1. Sem prejuízo de outras situações de grave violação das obrigações assumidas pelo contraente público especialmente previstas no contrato e independentemente do direito de indemnização, o cocontratante tem o direito de resolver o contrato nas seguintes situações:
 - 1.1. Incumprimento de obrigações pecuniárias pelo contraente público por período superior a seis meses; ou
 - 1.2. Quando o montante em dívida exceda 25% do preço contratual, excluindo juros.
2. Nos casos previstos no n.º 1, o direito de resolução pode ser exercido mediante declaração ao contraente público, produzindo efeitos 30 dias após a receção dessa declaração, salvo se o

contraente público cumprir as obrigações em atraso nesse prazo, acrescidas dos juros de mora a que houver lugar.

Cláusula 20.^a

Casos fortuitos ou de força maior

1. Nenhuma das partes incorrerá em responsabilidade se, por caso fortuito ou de força maior, for impedida de cumprir as obrigações assumidas no contrato.
2. Entende-se por caso fortuito ou de força maior qualquer situação ou acontecimento imprevisível e excecional, independente da vontade das partes, e que não derive de falta ou negligência de qualquer delas.
3. A parte que invocar casos fortuitos ou de força maior deverá comunicar e justificar tais situações à outra parte, bem como informar o prazo previsível para restabelecer a situação.

Cláusula 21.^a

Foro competente

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

Cláusula 22.^a

Comunicações e notificações

4. 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 CCP, para o domicílio ou sede contratual de cada uma, identificados no contrato.
5. Qualquer alteração das informações de contacto constantes do contrato deve ser comunicada à outra parte.

Cláusula 23.^a

Contagem dos prazos

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

Cláusula 24.^a

Legislação aplicável

O contrato é regulado pelo CCP e pela demais legislação portuguesa aplicável.

ANEXO I – ESPECIFICAÇÕES TÉCNICAS

Pretende-se o fornecimento de uma solução de segurança de firewall para a rede de computadores do Instituto Politécnico do Porto, bem como os serviços de instalação, configuração e migração, de acordo com a arquitetura e especificações técnicas definidas para os itens, quantidades e condições de garantia definidas a seguir.

Qualquer especificação técnica a seguir indicada que faça referência a um fabricante ou proveniência determinados, a um processo específico de fabrico, a marcas, patentes ou modelos e a uma dada origem ou produção, deverá ser entendida como acompanhada da menção “ou equivalente”. Da mesma forma, todas as especificações técnicas a seguir indicadas devem ser entendidas como especificações mínimas, podendo ser apresentadas propostas equivalentes ou superiores.

1. Arquitetura:

- 1.1 Solução de firewall em *appliances* de hardware de grande desempenho de Next-Generation Firewall (NGFW) que permita a melhoria da filtragem ao nível aplicacional do tráfego de rede dependente do conteúdo do pacote, permitindo um conhecimento e controle mais profundos sobre aplicativos individuais, assim como recursos de inspeção pela firewall mais profundos, permitindo obter segurança corporativa com visibilidade total e proteção contra as ameaças.
- 1.2 Arquitetura de alta disponibilidade (High Availability – HA), conforme esquema apresentado na Figura 1 – Arquitetura da solução de Firewall, com componentes redundantes em hot-standby em cada um dos 3 níveis da firewall. Ao nível WAN ou acesso à Internet com uma *appliance* no Data Center do P.PORTO e outra no Data Center do ISEP, ao nível DMZ ou Aplicacional com 2 *appliances* no Data Center do P.PORTO e ao nível da rede local de cada escola / unidade orgânica com 2 *appliances* em cada escola ou unidade orgânica. Uma componente de analisador de logs centralizando a gestão e análise dos logs. Finalmente, a gestão de políticas de segurança dos 3 níveis de firewall deverá ser assegurada por acesso web seguro.
- 1.3 A arquitetura da solução proposta deverá ser validada de forma solidária quer pelo fornecedor da proposta quer pelo respetivo fabricante da *firewall*, para o que deve ser junta declaração assinada conjuntamente – Declaração da Arquitetura Proposta.

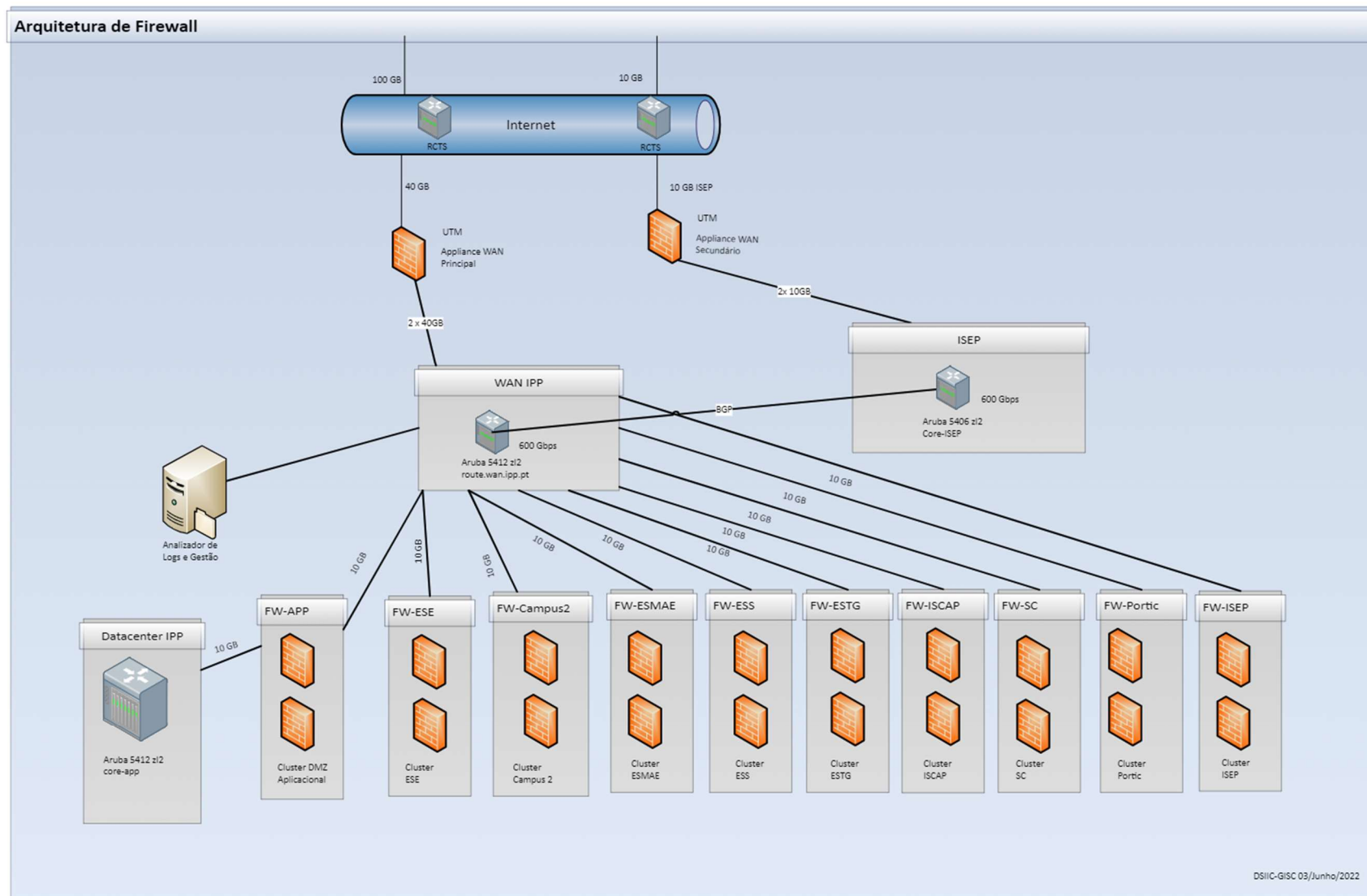


Figura 1– Arquitetura da solução de Firewall

2. Certificações e Conformidade

- 2.1 O P.PORTO tem como grande prioridade a proteção dos dados críticos dos seus sistemas e utilizadores, bem como dá um grande enfoque nas diversas áreas da Cibersegurança, pelo que os fabricantes das soluções de firewall propostas deverão comprovar a sua liderança em soluções de segurança (Firewall, prevenção de intrusões e UTP) ano após ano, em análises/relatórios de entidades independentes. Desta forma são exigidas as certificações seguintes:
- 2.1.1 Equipamentos propostos com testes e validações de entidades independentes na eficácia e desempenho de segurança, nomeadamente a entrega das certificações ICSA Labs: Firewall, IPsec, IPS, Antivirus, SSL-VPN, USGv6/IPv6.
- 2.1.2 A solução proposta deve ainda assentar em equipamentos e aplicações de software de fabricantes que tenham obtido a classificação de Leaders no estudo anual mais recente denominado de "Magic Quadrant for Network Firewalls" elaborado de forma independente pela empresa Gartner.

3. Funcionalidades da Solução de Segurança:

- 3.1 Detecção de segurança de milhares de aplicativos dentro do tráfego de rede para inspeção profunda e aplicação de políticas granulares. Proteção contra Malware, explorações e sites maliciosos em tráfego criptografado e não criptografado. Prevenção na deteção de ataques conhecidos e desconhecidos usando inteligência de ameaças contínua com tecnologia de Inteligência Artificial (IA) dos serviços de segurança do fabricante.
- 3.2 Integrando processadores de segurança de alto desempenho na proteção contra ameaças e de latência ultrabaixa, fornecendo alto desempenho e proteção para tráfego criptografado SSL.
- 3.3 Disponibilização de recursos avançados de rede que se integrem perfeitamente com a segurança avançada de camada 7 do modelo OSI, bem como domínios virtuais para disponibilizar grande flexibilidade de instalação, multi-localizações e uma utilização eficaz de recursos. Disponibilizando também uma combinação flexível e de alta densidade de várias interfaces de alta velocidade em instalações de Data Center e WAN.
- 3.4 Consola de gestão web segura, eficaz, simples de usar e que forneça automação e visibilidade de rede abrangentes, apresentando a agregação de dados de múltiplas fontes num interface unificado. Análise de verificação de conformidade da instalação, salientando as melhores práticas de segurança da solução.
- 3.5 Permita a integração de produtos de segurança adicionais, para uma visibilidade mais ampla e deteção integrada de ponto-a-ponto, e partilha de inteligência de ameaças e de correção automatizada.
- 3.6 Conjunto de serviços de Unified Threat Protection (UTP):
- 3.6.1 Serviço de controlo de aplicações – detetar e agir contra o tráfego de rede com base no aplicativo que gerou o tráfego, utilizando decodificadores de protocolo com assinaturas que analisam o tráfego de rede, mesmo que o tráfego use portas ou protocolos não padrão. Possibilitar um controle mais granular, como permitir *logins* mas não interagindo em sites pré-selecionados. Permitir também a aplicação de Traffic Shaping ao tráfego do aplicativo

permitido. Adicionalmente, permitir a gestão das mudanças nos padrões de tráfego do aplicativo pelo monitoramento contínuo.

- 3.6.2 Filtragem Web e Vídeo – classificação massiva de conteúdo da Web, bases de dados de URL, e filtragem de Web e Vídeo potenciada por ambientes de análise com IA. Proteção de riscos internos e externos, mesmo para tráfego criptografado em alto desempenho e cache dinâmico da Web e de vídeo. Permitindo o bloqueio granular e filtragem de categorias Web e de vídeo, para permitir fazer log ou bloquear, para proteção abrangente e conformidade. Com atualizações de assinaturas contínuas e automatizadas que protegem contra injeção de SQL, Cross-Site Scripting e outros ataques com centenas de tipos de dados e padrões de Web-robot, assinaturas de vulnerabilidades de *scanning* e URLs suspeitos.
- 3.6.3 Proteção de DNS – proteção contra táticas de ataque malicioso de bloqueio de domínio como encapsulamento de DNS, identificação de servidores de Comando e Control (C2) e algoritmos de geração de domínios.
- 3.6.4 Antibot – para bloqueio de tentativas não autorizadas de comunicação com servidores remotos comprometidos, de receber comandos maliciosos ou envio de informação extraída.
- 3.6.5 Geo IP – proteção adicional fornecendo informações de localização no tráfego IP para ajudar a gerir ameaças baseadas em região.
- 3.6.6 Cloud Sandbox – análise de Malware estático e dinâmico baseado em comportamento e potenciado em IA para lidar com ameaças em rápida evolução e mais direcionadas, incluindo Ransomware, Cripto-Malware e outros numa larga superfície de ataque digital. Permitindo inteligência e prevenção acionáveis em tempo real por meio da automação da detecção e resposta avançada de Malware de Zero-Day.
- 3.6.7 Prevenção de Intrusão (IPS) – bloqueio das mais recentes ameaças ao nível de rede e intrusões de rede, com interligação com a biblioteca IPS mais abrangente do fabricante, com milhares de assinaturas e apoiada pela pesquisa do fabricante com centenas de descobertas de Zero-Day. Para incorporar nativamente em políticas com reconhecimento de contexto para controle completo dos métodos de detecção de ataques de resposta a aplicativos de segurança complexos e resistência a técnicas de evasão.
- 3.6.8 Antivírus – com atualizações automatizadas que protegem contra os mais recentes componentes de ataque de polimorfismo, vírus, Spyware e outras ameaças ao nível do conteúdo. Com mecanismos de detecção avançados para impedir que ameaças novas e em evolução se instalem na rede, Endpoint e nuvens e acedam a conteúdos críticos.
- 3.6.9 Antispam – serviço para reduzir drasticamente o volume de spam no perímetro, permitindo grande controle de ataques e infeções por e-mail, e maior proteção do que as comuns *blacklists* de tempo real.
- 3.6.10 Proteções adicionais como Malware de dispositivos móveis (para 4G, 5G), proteção de credenciais, desarme e reconstrução de conteúdo, prevenção de ataques de vírus, Data Loss Prevention, etc.

- 3.6.11 Serviços de suporte e atualização, disponibilizados por equipa de especialistas de suporte e melhoria tecnológica, implementação, assistência de suporte e cuidados proativos para maximizar a segurança e desempenho das soluções do fabricante, incluindo as atualizações permanentes das várias componentes de firewall e assinaturas IPS, UTP, Antimalware, Antispam, etc.
- 3.7 Suporte às funcionalidades de alta disponibilidade: Interfaces de *heartbeat* redundantes. Interfaces reservadas para a rede de gestão. Sem custos de licenciamento para suporte de funcionalidades de alta-disponibilidade. Reposição automática de serviço – *failover*, com *failover* em menos de 1 segundo, notificações de eventos de *failover*, monitorização de portas e links (locais e remotos) e sem perda de sessões. Diferentes opções de arquitetura: HA com agregação de links, Full mesh HA e suporte para HA com equipamentos geograficamente dispersos. Opção de sincronização de sessões em equipamentos configurados em modo Standalone ou Cluster geográfico.

4. Funcionalidades de Firewall, VPN e IPS/IDS e Proteção contra ameaças:

- 4.1 Deverá suporta as funcionalidades de Firewall: Modos de operação NAT/Route e Transparente/Bridge. Agendamento de políticas: recorrentes ou apenas uma vez. Session helpers e ALGS: dcerpc, dns-tcp, dns-udp, ftp, H.323, MGCP, MMS, PMAP, PPTP, RAS, RSH, RTSP, SIP, TFTP, GTP-C, GTP-U, GTP-B, TNS (Oracle). Suporte para tráfego VoIP: SIP/H.323 /SCCP NAT traversal, RTP pinhole. Suporte para diferentes tipos de protocolos: SCTP, TCP, UDP, ICMP, IP.
- 4.2 Deverá permitir a visualização de políticas de forma global ou por pares de interfaces. A definição de objetos para utilização em políticas incluindo pré-definidos, customizados, agrupamento de objetos, tagging e definição de cor de objetos. Definição de objetos de endereços de diferentes tipos: IP, Subnet, intervalo de IPs, Geografia e FQDN. Utilização de objetos de serviços Internet (ex: Azure, Office365) com atualização automática das gamas de IP e portas. Configuração de NAT: por política e tabela central de NAT. Suporte de NAT: NAT64, NAT46, NAT estático, NAT dinâmico, PAT, Full Cone NAT, STUN.
- 4.3 Suporte a 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.
- 4.4 Suporte às funcionalidades de VPN de IPSEC VPN em *peers* remotos (clientes *dialup* compatíveis com IPSEC, *peers* com IP estático ou DNS dinâmico). Mecanismos de autenticação (certificados ou Pre-shared Key). IPSEC Phase 1 mode. Opções de aceitação de peers: qualquer ID, ID específico, ID num grupo de utilizadores dialup. Suporte de IKEv1, IKEv2. Suporte de IKE mode configuration (como servidor ou cliente) e DHCP over IPSEC. Phase 1/Phase 2 Proposal encryption: DES, 3DES, AES128, AES192, AES256. Phase 1/Phase 2 Proposal authentication: MD5, SHA1, SHA256, SHA384, SHA512. Suporte XAuth como cliente ou servidor. Duração configurável da chave de encriptação IKE e da frequência do NAT Traversal Keepalive. Dead Peer Detection e Replay Detection. Autokey keep-alive na Phase 2 SA.

- 4.5 Implementação de VPNs IPSEC nos modos: *gateway-to-gateway*, *hub-and-spoke*, *full mesh*, *redundant-tunnel*, terminação de VPNs em modo transparente. Suporte a ADVPN. Suporte de configuração *full-mesh* VPN One-click. Opções de configuração de VPNs IPsec: baseado em *routing* ou baseado em políticas.
- 4.6 Suporte a VPNs SSL com Portal de VPN SSL configurável. Suporte para domínio de SSL VPN (com customização de múltiplos portais VPN SSL associados a grupos de utilizadores, incluindo URL do portal e desenho). Atalhos (*bookmarks*) com Single Sign-on e 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. Suporte para VPN SSL em modo túnel, disponível para MAC OSX, Windows, IOS, Android e Windows Mobile. Suporte para VPN SSL em modo *port-forwarding*. Suporte a validação da integridade do dispositivo cliente e do sistema operativo, opção para limpeza de cache aquando do termino da sessão VPN SSL e opção de utilização de desktop virtual.
- 4.7 Suporte a 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.
- 4.8 Capacidade da Firewall de ser um *proxy point* ou um *enforcement point* de ZTNA (Zero Trust Network Access). Capacidade de triar túneis TLS automáticos a partir do *endpoint*. Validação da identidade do utilizador, da identidade do dispositivo, da postura de segurança do dispositivo e dos privilégios de acesso do utilizador antes de dar acesso às aplicações.
- 4.9 Suporte de IPS com mais de 12000 assinaturas, deteção de anomalias nos protocolos, assinaturas customizadas, atualização manual ou automática das assinaturas (*push* ou *pull*), integração com enciclopédia de ameaças para melhor informação/visualização de ataques detetados. Suporte a diferentes ações de IPS: monitorizar, bloquear, apagar sessão ou quarentena do IP de ataque com definição de duração. Possibilidade de registo integral do pacote onde foi detetado o ataque. Definição de diferentes perfis de IPS de forma manual ou baseada em filtro (severidade, alvo, sistema operativo, aplicação e/ou protocolo). Aplicação de perfis de IPS por política de firewall para maior flexibilidade. Opção de excluir a aplicação de assinaturas de IPS específicas com base em IPs. Proteção de DoS sobre IPv4 e IPv6 com definições contra TCP Syn-flood, *port scan* TCP/UDP/SCTP, ICMP *sweep*, *session flooding* TCP/UDP/ SCTP/ICMP.
- 4.10 Possibilidade de implementação de IDS em modo *sniffer*. Possibilidade de criar novas assinaturas. Possibilidade de incluir assinaturas específicas para proteção de comunicações e equipamentos. Suporte a aplicação de perfis de controlo de aplicações por política de firewall. Deteção de aplicações mesmo dentro de ligações proxy. Diferentes ações de controlo de aplicações: bloquear, *reset* de sessão, monitorização ou aplicação de gestão de largura de banda. Inspeção SSL (suporte TLS 1.3).
- 4.11 Proteção contra ameaças com a possibilidade de inspeção aplicacional de tráfego encriptado por SSL, incluindo as seguintes funcionalidades: IPS, controlo de aplicações, Antivírus, Web filtering e DLP (Data Loss Prevention). Capacidade de descriptação de sessões SSL com cópia de tráfego descriptado 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. Possibilidade de 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). Integração com solução de Sandboxing (Cloud ou On-premises).

- 4.12 Suporte a deteção de Web Filtering: diferentes mecanismos de deteção de sites Web (*proxy-based*, *flow-based* de DNS). Possibilidade de definição manual de filtros de sites com base em URL, conteúdo web e cabeçalho MIME. Categorização dinâmica em tempo real, baseada na Cloud, com mais de 250 milhões de sites categorizados e de 70 idiomas. Opção para forçar a utilização de mecanismos de busca segura (*safe search*) disponibilizados pelos principais motores de busca, e definição customizada de YouTube Education Filter. Opção para ativar as 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 a inspeção SSL de tráfego encriptado em determinadas categorias relevantes à manutenção da privacidade dos utilizadores. Definição de quotas de utilização Web com base em categorias. Definição de categorias customizadas e sobreposição de categorização. Mecanismos de exceção à utilização de perfis pré-definidos. Suporte a deteção e limitação de acesso a conteúdos vídeo de forma granular (Video Filter). Mecanismos de deteção e mitigação de utilização de *proxy-avoidance*. Prevenção e proteção de fugas de informação – DLP. Suporte de protocolos na análise de mensagens: HTTP-POST, SMTP, POP3, IMAP, MAPI, NNTP. Possibilidade de executar as ações: registar, bloquear, quarentena de utilizador/IP/Interface. Filtros pré-definidos incluindo cartões de crédito e número de segurança Social. Suporte de protocolos na análise de ficheiros: HTTP-POST, HTTP=GET, SMTP, POP3, IMAP, MAPI, FTP, NNTP. Opções de filtro disponíveis: tipo de ficheiro, *watermark*, conteúdo e deteção de encriptação. Utilização de mecanismos de DLP *watermarking*, com disponibilização de ferramentas gratuitas de watermarking para Windows e Linux. Fingerprinting de ficheiros. Armazenamento de ficheiros detetados para inspeção forense, incluindo: todo o conteúdo de e-mail, FTP, IM, NNTP e tráfego Web. Integração nativa com plataformas externas de filtragem de email, Sandbox e WAF. Feeds de ameaças por Domain Name e/ou IP Address. Controlo de Endpoints com visibilidade centralizada sobre diversos elementos de rede, nomeadamente vulnerabilidades nos endpoints e indicadores de compromisso.

5. Administração, Monitorização e Diagnósticos:

- 5.1 Suporte a acesso de gestão gráfica e texto: HTTPS com recurso a web browser. Acesso de gestão em modo de texto: SSH, Telnet ou consola. Suporte para gestão local e gestão centralizada em simultâneo. Suporte para gestão centralizada com integração em plataforma específica para o efeito. Integração com plataformas externas de gestão e monitorização, incluindo SNMP, sFlow, Syslog e Netflow. Implementação rápida da solução incluindo mecanismos de auto instalação por USB, execução local e remota de scripts. Visualização em tempo real do estado do equipamento através de interface gráfica (acesso HTTPS com recurso a web-browser) incluindo diversos conteúdos e funcionalidades. Integração com outras soluções (externas) através de scripts CLI e APIs. Wizards de configuração para implementação rápida da solução. Integração com soluções VMWare e Openstack. Automação, por exemplo para colocar em Quarentena um dispositivo com um elevado Indicador de compromisso.

- 5.2 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 tráfego: tráfego enviado, bloqueado, sessões violadas, tráfego local, pacotes inválidos. Organização de registos de acordo com a categoria: administração de sistema (para auditoria), *routing* e *networking*, VPN, autenticação de utilizadores e wireless. Opção para registo parcial ou completo de eventos. Resolução de nomes de endereços IPs e protocolos. Mecanismo nativo de visualização de eventos de forma estática, com ferramentas de busca e *drill-down* disponível através de recurso com web browser.

6. Integração com redes de comunicações:

- 5.3 A solução deverá suportar as funcionalidades de Servidor de DHCP, NTP, DNS e DNS Proxy.
- 5.4 Deverá suportar múltiplos modos de configuração de interfaces: Sniffer, Agregação de portas (802.3ad), Loopback, VLANs (802.1Q e trunk), Software switch. Deverá suportar *routing* estático e baseado em políticas (PBR – Policy Based Routing). Suporte a balanceamento e redundância de múltiplos links. Suporte para protocolos de *routing* dinâmico: RIPng, OSPFv3 e BGP4+. Suporte de tráfego *multicast*: PIM, *sparse* e *dense mode*. Routing baseado em conteúdos: WCCP e ICAP. Suporte a VXLAN. Suporte a NAT64 e NAT46. Controlador de switching integrado.
- 5.5 Suporte de IPv6: na gestão, protocolos de *routing* dinâmico, *tunneling*, processamento de firewall e UTM, e VPN IPSec. Suporte de dupla stack IPv4 e IPv6 em simultâneo.
- 5.6 Identificação de utilizadores e dispositivos: em base de dados local, autenticação de utilizadores em servidores remotos: LDAP, RADIUS, TACACS+. Suporte a sistema de Single Sign-on de utilizadores: Windows AD, RADIUS, Autenticação de utilizadores no acesso (802.1x, portal cativo).
- 5.7 Suporte a PKI e certificados: Certificados X.509, SCEP, criação de Certificate Signing Request (CSR), auto renovação de certificados antes da data de expiração e suporte a OCSP.
- 5.8 Suporte a autenticação de 2 fatores: servidor integrado de autenticação por *tokens* físicos, *tokens* por software e SMS. Integração com terceiras partes.
- 5.9 Suporte a identificação de dispositivos (incluindo dispositivos IoT): reconhecimento de dispositivo e sistema operativo, classificação automática de dispositivos, gestão de inventário de dispositivos e suporte de autenticação e bypass feitos por MAC Address. Implementação de políticas de segurança com base em utilizador ou dispositivos.

7. Especificações técnicas dos equipamentos, quantidades e manutenção e suporte em conformidade com a Tabela 1. Especificações técnicas dos equipamentos/serviços e quantidades

- 6.1 Deverá ser apresentada Declaração de Conformidade dos requisitos técnicos do Caderno de Encargos (desde o Item 1 até ao Item 8), conforme modelo a seguir.

Item.	Designação	Descrição / Critério	Cumpre Sim/Não	Nome do Documento do fabricante	Nº da Página
1. Appliance de WAN Principal (Acesso á Internet Principal)					
1.1.	<i>Throughput</i> mínimo das funcionalidades de firewall com <i>logging</i> ativo:				
1.1.1.	Suporte a ligações até: 100 GbE				
1.1.2.	Firewall Throughput (pacotes por segundo): 180 Mpps				
1.1.3.	Firewall Throughput (UDP, 1518 bytes): 180 Gbps				
1.1.4.	IPS Throughput: 24 Gbps				
1.1.5.	NGFW throughput (Firewall, IPS, Application Control – HTTP 64K): 19 Gbps				
1.1.6.	...				

6.2 Deverão ser apresentadas todas as Datasheets e outros documentos técnicos emitidos pelo fabricante que permitam verificar as conformidades solicitadas na Declaração de Conformidade.

Tabela 1. Especificações técnicas dos equipamentos/serviços e quantidades

Item.	Designação	Descrição	Quant. / Unidade orgânica
1. Appliance de WAN Principal (Acesso á Internet Principal)			
1.2.	Throughput mínimo das funcionalidades de firewall com logging ativo:		1 Data Center P.PORTO
1.2.1.	Suporte a ligações até: 100 GbE		
1.2.2.	Firewall Throughput (pacotes por segundo): 180 Mpps		
1.2.3.	Firewall Throughput (UDP, 1518 bytes): 180 Gbps		
1.2.4.	IPS Throughput: 24 Gbps		
1.2.5.	NGFW throughput (Firewall, IPS, Application Control – HTTP 64K): 19 Gbps		
1.2.6.	Threat Protection (Firewall, IPS, Application Control – HTTP 64K, Malware Protection): 17 Gbps		
1.2.7.	Sessões TCP concorrentes: 18 Milhões		
1.2.8.	Novas sessões TCP/seg.: 500.000		
1.2.9.	Políticas de Firewall: 50.000		
1.2.10.	Tuneis IPsec VPN: Gateway-a-Gateway 5.000, Cliente-a-Gateway 25.0000		
1.2.11.	Desempenho SSL-VPN: 16 Gbps		
1.2.12.	Utilizadores SSL-VPN concorrentes: 20.000 utilizadores licenciados		
1.2.13.	Desempenho de SSL Inspection (IPS, média de HTTPS): 20 Gbps		
1.2.14.	SSL Inspection (IPS, média de HTTPS) conexões/seg.: 16.000		
1.2.15.	SSL Inspection de sessões concorrentes (IPS, média HTTPS): 2.5 Milhões		
1.2.16.	Desempenho de controlo aplicacional (HTTP 64K): 60 Gbps		
1.2.17.	Domínios virtuais: 10		
1.2.18.	Suporte a configurações de Alta Disponibilidade: cluster Ativo-Ativo ou Ativo-Passivo.		
1.2.19.	Consumos energéticos: médio até 450 W e máximo até 550 W.		
1.3.	Interfaces (mínimo): consola RJ45, porta USB, 2x GE RJ45 rede de gestão "Out of Band"		
1.3.1.	16x10 GE/GE RJ45		
1.3.2.	16x 25 GE SFP28 / 10 GE SFP+ / GE SFP		
1.3.3.	4x 100 GE QSFP28 / 40 GE QSFP+ (inclusão de: 2x 40 GE QSFP+ transceiver, 1x QSFP-100G-SR4 transceiver, 2x cabo MPT/MPO de 12 fibras, 5m).		
1.4.	Componentes adicionais, rack e redundância:		
1.4.1.	Armazenamento interno de 2x 1 TB NVME SSD.		
1.4.2.	Kit de rails para montagem em rack, dimensão máxima de 2U.		
1.4.3.	Fontes de alimentação redundantes.		
1.5.	Subscrições: 5 anos de bundle de Unified Threat Protection.		

Item.	Designação	Descrição	Quant. / Unidade orgânica
2. Appliance de WAN Secundária (Acesso à Internet de Backup)			
2.1.	Throughput mínimo das funcionalidades de firewall com logging ativo:		1 Data Center ISEP
2.1.1.	Suporte a ligações até 25 GbE		
2.1.2.	Firewall Throughput (Pacotes por segundo): 90 Mpps		
2.1.3.	Firewall Throughput (UDP, 1518 bytes): 120 Gbps		
2.1.4.	IPS Throughput: 12 Gbps		
2.1.5.	NGFW throughput (Firewall, IPS, Application Control – HTTP 64K): 10 Gbps		
2.1.6.	Threat Protection (Firewall, IPS, Application Control – HTTP 64K, Malware Protection): 9 Gbps		
2.1.7.	Sessões TCP concorrentes: 7 Milhões		
2.1.8.	Novas sessões TCP/seg.: 250.000		
2.1.9.	Políticas de Firewall: 50.000		
2.1.10.	Tuneis IPsec VPN: Gateway–a–Gateway 1.000, Cliente–a–Gateway 25.000		
2.1.11.	Desempenho SSL–VPN: 4 Gbps		
2.1.12.	Utilizadores SSL–VPN concorrentes: 2000 utilizadores licenciados		
2.1.13.	Desempenho de SSL Inspection (IPS, média de HTTPS): 9 Gbps		
2.1.14.	SSL Inspection (IPS, média de HTTPS) conexões/seg.: 5.000		
2.1.15.	SSL Inspection de sessões concorrentes (IPS, média HTTPS): 400.000		
2.1.16.	Desempenho de controlo aplicacional (HTTP 64K): 30 Gbps		
2.1.17.	Domínios virtuais: 10		
2.1.18.	Suporte a configurações de Alta Disponibilidade: cluster Ativo–Ativo ou Ativo–Passivo.		
2.1.19.	Consumos energéticos: médio até 180 W e máximo até 300 W.		
2.2.	Interfaces (mínimo): consola RJ45, porta USB, 2x GE RJ45 rede de gestão "Out of Band",		
2.2.1.	16x GE RJ45 Ports.		
2.2.2.	8x GE SFP		
2.2.3.	4x 10 GE SFP+ / GE SFP		
2.2.4.	4x 25 GE SFP28 / 10 GE SFP+ (inclusão de 3x 10 GE SFP+ transceiver).		
2.3.	Componentes adicionais, rack e redundância:		
2.3.1.	Armazenamento interno de 2x 240 GB NVME SSD		
2.3.2.	Kit de rails para montagem em rack, dimensão máxima de 2U.		
2.3.3.	Fontes de alimentação redundantes.		
2.4.	Subscrições: 5 anos de bundle de Unified Threat Protection.		

Item.	Designação	Descrição	Quant. / Unidade orgânica
3. Appliance DMZ / Aplicacional (Cluster)			
3.1.	Throughput mínimo das funcionalidades de firewall com logging ativo:		2 Data Center P.PORTO
3.1.1.	Suporte a ligações até 10 GbE		
3.1.2.	Firewall Throughput (Pacotes por segundo): 36 Mpps		
3.1.3.	Firewall Throughput (UDP, 1518 bytes): 32 Gbps		
3.1.4.	IPS Throughput: 7Gbps		
3.1.5.	NGFW throughput (Firewall, IPS, Application Control – HTTP 64K): 6 Gbps		
3.1.6.	Threat Protection (Firewall, IPS, Application Control – HTTP 64K, Malware Protection): 5 Gbps		
3.1.7.	Sessões TCP concorrentes: 4 Milhões		
3.1.8.	Novas sessões TCP/seg.: 250.000		
3.1.9.	Políticas de Firewall: 5.000		
3.1.10.	Tuneis IPsec VPN: Gateway-a-Gateway 1.000, Cliente-a-Gateway 25.000		
3.1.11.	Desempenho SSL-VPN: 4 Gbps		
3.1.12.	Utilizadores SSL-VPN concorrentes: 5.000 utilizadores licenciados		
3.1.13.	Desempenho de SSL Inspection (IPS, média de HTTPS): 4 Gbps		
3.1.14.	SSL Inspection (IPS, média de HTTPS) conexões/seg.: 4.000		
3.1.15.	SSL Inspection de sessões concorrentes (IPS, média HTTPS): 200.000		
3.1.16.	Desempenho de controlo aplicacional (HTTP 64K): 12 Gbps		
3.1.17.	Domínios virtuais: 5		
3.1.18.	Suporte a configurações de Alta Disponibilidade: cluster Ativo-Ativo ou Ativo-Passivo.		
3.1.19.	Consumos energéticos: médio até 130 W e máximo até 250 W.		
3.2.	Interfaces (mínimo): consola RJ45, porta USB,		
3.2.1.	2x GE RJ45 rede de gestão "Out of Band",		
3.2.2.	8x GE RJ45 Ports.		
3.2.3.	8x GE SFP (inclusão de 2x SFP transceiver).		
3.2.4.	8x 10 GE SFP+ (inclusão de 2x 10 GE SFP+ transceiver).		
3.3.	Componentes adicionais, rack e redundância:		
3.3.1.	Armazenamento interno de 2x 240 GB NVME SSD		
3.3.2.	Kit de rails para montagem em rack, dimensão máxima de 1U.		
3.3.3.	Fontes de alimentação redundantes.		
3.4.	Subscrições: 5 anos de bundle de IPS.		

Item.	Designação	Descrição	Quant. / Unidade orgânica
4. Appliance FW-ISEP			
4.1.	Throughput mínimo das funcionalidades de firewall com logging ativo:		2 Data Center ISEP
4.1.1.	Suporte a ligações até 10 GbE		
4.1.2.	Firewall Throughput (Pacotes por segundo): 36 Mpps		
4.1.3.	Firewall Throughput (UDP, 1518 bytes): 32 Gbps		
4.1.4.	IPS Throughput: 7Gbps		
4.1.5.	NGFW throughput (Firewall, IPS, Application Control - HTTP 64K): 6 Gbps		
4.1.6.	Threat Protection (Firewall, IPS, Application Control - HTTP 64K, Malware Protection): 5 Gbps		
4.1.7.	Sessões TCP concorrentes: 4 Milhões		
4.1.8.	Novas sessões TCP/seg.: 250.000		
4.1.9.	Políticas de Firewall: 5.000		
4.1.10.	Tuneis IPsec VPN: Gateway-a-Gateway 1.000, Cliente-a-Gateway 25.000		
4.1.11.	Desempenho SSL-VPN: 4 Gbps		
4.1.12.	Utilizadores SSL-VPN concorrentes: 5.000 utilizadores licenciados		
4.1.13.	Desempenho de SSL Inspection (IPS, média de HTTPS): 4 Gbps		
4.1.14.	SSL Inspection (IPS, média de HTTPS) conexões/seg.: 4.000		
4.1.15.	SSL Inspection de sessões concorrentes (IPS, média HTTPS): 200.000		
4.1.16.	Desempenho de controlo aplicacional (HTTP 64K): 12 Gbps		
4.1.17.	Domínios virtuais: 5		
4.1.18.	Suporte a configurações de Alta Disponibilidade: cluster Ativo-Ativo ou Ativo-Passivo.		
4.1.19.	Consumos energéticos: médio até 130 W e máximo até 250 W.		
4.2.	Interfaces (mínimo): consola RJ45, porta USB,		
4.2.1.	2x GE RJ45 rede de gestão "Out of Band",		
4.2.2.	8x GE RJ45 Ports.		
4.2.3.	8x GE SFP		
4.2.4.	8x 10 GE SFP+ (inclusão de 3x 10 GE SFP+ transceiver).		
4.3.	Componentes adicionais, rack e redundância:		
4.3.1.	Armazenamento interno de 2x 240 GB NVME SSD.		
4.3.2.	Kit de rails para montagem em rack, dimensão máxima de 1U.		
4.3.3.	Fontes de alimentação redundantes.		

Item.	Designação	Descrição	Quant. / Unidade orgânica
5. Appliance FW-ESE, FW-Campus 2, ESMAE, ESS, ESTG, ISCAP, SC, PORTIC			
5.1.	Throughput mínimo das funcionalidades de firewall com logging ativo:		16 Total: 2 ESE 2 Campus 2 2 ESMAE 2 ESS 2 ESTG 2 ISCAP 2 SC 2 PORTIC
5.1.1.	Suporte a ligações até 10 GbE		
5.1.2.	Firewall Throughput (Pacotes por segundo): 15 Mpps		
5.1.3.	Firewall Throughput (UDP, 1518 bytes): 20 Gbps		
5.1.4.	IPS Throughput: 2,5 Gbps		
5.1.5.	NGFW throughput (Firewall, IPS, Application Control – HTTP 64K): 1,5 Gbps		
5.1.6.	Threat Protection (Firewall, IPS, Application Control – HTTP 64K, Malware Protection): 1 Gbps		
5.1.7.	Sessões TCP concorrentes: 1,5 Milhões		
5.1.8.	Novas sessões TCP/seg.: 55.000		
5.1.9.	Políticas de Firewall: 5.000		
5.1.10.	Tuneis IPsec VPN: Gateway-a-Gateway 1.000, Cliente-a-Gateway 10.000		
5.1.11.	Desempenho SSL-VPN: 1 Gbps		
5.1.12.	Utilizadores SSL-VPN concorrentes: 500 utilizadores licenciados		
5.1.13.	Desempenho de SSL Inspection (IPS, média de HTTPS): 1 Gbps		
5.1.14.	SSL Inspection (IPS, média de HTTPS) conexões/seg.: 1.800		
5.1.15.	SSL Inspection de sessões concorrentes (IPS, média HTTPS): 130.000		
5.1.16.	Desempenho de controlo aplicacional (HTTP 64K): 2,2 Gbps		
5.1.17.	Domínios virtuais: 5		
5.1.18.	Suporte a configurações de Alta Disponibilidade: cluster Ativo-Ativo ou Ativo-Passivo.		
5.1.19.	Consumos energéticos: médio até 40 W e máximo até 50 W.		
5.2.	Interfaces (mínimo): consola RJ45, porta USB, 2x GE RJ45 rede de gestão "Out of Band",		
5.2.1.	14x GE RJ45 Ports.		
5.2.2.	4x GE SFP		
5.2.3.	2x 10 GE SFP+ (inclusão de 2x 10 GE SFP+ transceiver).		
5.3.	Componentes adicionais, rack e redundância:		
5.3.1.	Kit de rails para montagem em rack, dimensão: altura de 1U e largura 19".		
5.3.2.	Fontes de alimentação redundantes.		

Item.	Designação	Descrição	Quant. / Unidade orgânica
6. Serviços de suporte, atualizações e garantias			
6.1. Serviços incluídos:			
6.1.1. Atualizações de Software com acesso a portal de suporte técnico para downloads de software, boletins técnicos, gestão de ativos.			
6.1.2. Plataforma web e suporte telefónico para abertura de incidentes de suporte técnico. Tratamento de tickets assegurada por equipa de suporte técnico, que dará o suporte necessário na resolução de incidentes, a encontrar soluções de problemas relativos à falha do sistema, produto ou configuração.			
6.2. Disponibilidade e tempos de resposta dos serviços:			
6.2.1. Disponibilidade 24x7x365 dias.			
6.2.2. Deverão ser assegurados os tempos de resposta aos tickets de acordo com as prioridades seguintes:			
5.1.1.1. 1 hora para incidente que causem uma perda total, instabilidade contínua ou impacto significativo de funcionalidade crítica num ambiente de rede em produção;			
5.1.1.2. Next Business Day (NBD) em incidente com impacto mínimo nas operações da instituição;			
5.1.1.3. N2BD para informações adicionais, assistência básica em configurações existentes, erros na documentação ou defeitos menores que não afetem os serviços da instituição. Se o ticket técnico não for resolvido em tempo útil deverão ser escaladas notificações na cadeia de gestão do fabricante, à medida que o tempo avança e de acordo com a prioridade do ticket.			
6.3. Subscrição dos Serviços: 5 anos 24x7 com tempo de resposta NBD.			
6.4. Atualizações: acesso às atualizações de software, atualizações de <i>features</i> e versões de atualização, sempre que publicadas pelo fabricante.			
6.5. Garantia de hardware: 5 anos 24x7 com tempo de resposta de 1 hora em caso de problema crítico ou NBD se não crítico. A substituição do hardware será <i>on-site</i> .			
7. Plataforma de gestão de logs, análise e relatórios			
7.1. Requisitos:			
7.1.1. Plataforma de gestão de logs, análise de segurança e relatórios em painel único para operações de segurança simplificadas, identificação e correção proativas de riscos e visibilidade completa de toda a superfície de ataque.			
7.1.2. Integração com os recursos avançados de deteção de ameaças, para fornecer análise de segurança centralizada e consciencialização e controle completos do nível de segurança ponta a ponta, ajudando a equipa de segurança a identificar e eliminar ameaças antes que uma violação possa ocorrer.			
7.2. Funcionalidades de relatórios e ferramentas de visualização:			
7.2.1. Visualização dos endereços dos destinos, sites web e ameaças.			
7.2.2. Visualização e filtraçem dos Top Users de utilização das VPNs.			

Item.	Designação	Descrição	Quant. / Unidade orgânica
		7.2.3. Deverá ter por omissão vários modelos de relatórios tipo. Permitir aos administradores aprovisionarem/configurarem e gerarem relatórios. Relatórios com o sumário do UTP e tráfego. 7.2.4. Capacidade de monitorizar e alertar o administrador de TIC sobre eventos importantes. 7.3. Funcionalidades de visualização de logs: 7.3.1. Visualização de Logs em tempo real ou por histórico. 7.3.2. Visualizar pelo tipo de tráfego ou por logs de segurança. 7.3.3. Visualizar pelo tipo de dispositivo ou domínio virtual. 7.3.4. Filtragem de Logs. Visualização de Logs de forma granular. 7.3.5. Apresentação dos Logs com pictogramas das bandeiras dos países e aplicações. 7.4. Funcionalidades de gestão de eventos: 7.4.1. Criação de alertas de forma simples. 7.4.2. Desencadear alertas consoante o nível de severidade, eventos específicos, por tipo de ações e destinos. 7.4.3. Definir vários limites pelo número de eventos por um determinado tempo. 7.4.4. Visualizar ou procurar alertas através do histórico. 7.4.5. Notificar por email, traps SNMP, envio de eventos por syslog. 7.5. Outras funcionalidades: 7.5.1. Investigar arquivos de DLP e suporte aos tipos de arquivo: email, HTTP, FTP, IM. 7.5.2. Funcionalidade de IOC (Indicator of Compromise) na capacidade de voltar a reanalisar eventos/logs do passado com novo conhecimento de ataques, sites maliciosos, IPs, ficheiros confirmadamente considerados maus. 7.5.3. Funcionalidade de SOC (Security Operations Center) nas capacidades de SIEM para analisar, normalizar e correlacionar logs de produtos do fabricante e Security Event Logs de hosts Windows e Linux, e gestão de incidentes com automação via <i>playbooks</i> já pré-definidos ou criados pelo administrador. 7.5.4. Funcionalidade de Outbreak Alert Service na capacidade de receber automaticamente alertas de novos <i>outbreaks</i> e na criação automática de templates de relatório específicos para o novo <i>outbreak</i>, criação de relatório sobre o estado atual do <i>outbreak</i> e de criação de gestor de eventos relevantes para o <i>outbreak</i>. 7.6. Capacidades: 7.6.1. Logging até 10GB/dia, armazenamento até 10 TB em armazenamento do P.PORTO. 7.6.2. Dispositivos ou Dispositivos virtuais suportados até 10.000. 7.7. Requisitos de virtualização e Cloud: 7.7.1. VMware ESX 6.5 e superior. Public Cloud: Microsoft Azure. 7.7.2. Suporte a vCPU mínimo / máximo: 4 / ilimitado. Suporte de memória ilimitada a 64-bit. 7.8. Subscrição: licença de subscrição de VM (máquina virtual) com 5 anos de suporte.	

Item.	Designação	Descrição	Quant. / Unidade orgânica
8. Serviços de Instalação			
8.1.	Instalação dos equipamentos: instalação e configuração dos equipamentos a fornecer, em paralelo com a solução atual de segurança do P.PORTO.		
8.2.	Migração das políticas de segurança: nos vários níveis de gestão de políticas de segurança, WAN, DMZ/Aplicacional, e cada uma das escolas descritas a seguir, deverá ser efetuada a migração dos objetos e políticas de segurança para a nova solução, devendo ser contemplados para isso 30 dias de trabalho de técnico especializado .		
8.2.1.	WAN: políticas de segurança; regras de NAT; contas de acesso VPN; ligações gateway a gateway.		
8.2.2.	DMZ/Aplicacional: políticas de segurança; regras de NAT; ligações gateway a gateway.		
8.2.3.	ISEP: políticas de segurança; regras de NAT; ligações gateway a gateway.		
8.2.4.	ESE: políticas de segurança; regras de NAT; ligações gateway a gateway.		
8.2.5.	Campus 2: políticas de segurança; regras de NAT; ligações gateway a gateway.		
8.2.6.	ESMAE: políticas de segurança; regras de NAT; ligações gateway a gateway.		
8.2.7.	ESS: políticas de segurança; regras de NAT; ligações gateway a gateway.		
8.2.8.	ESTG: políticas de segurança; regras de NAT; ligações gateway a gateway.		
8.2.9.	ISCAP: políticas de segurança; regras de NAT; ligações gateway a gateway.		
8.2.10.	SC: políticas de segurança; regras de NAT; ligações gateway a gateway. Parte dos objetos e da política de segurança serão para migrar para as appliances da PORTIC.		
8.3.	Implementação de BGP: implementação de regras de routing dinâmico BGP entre a Appliance de WAN Principal (Data Center do P.PORTO) e a Appliance de WAN Secundária (Data Center do ISEP). Os switches de core de layer 3 são respetivamente os switches Aruba 5412R z12 do Data Center do P.PORTO e Aruba 5406R z12 do Data Center do ISEP.		
8.4.	Testes: realização de conjunto de testes de funcionamento abrangentes a todas as funcionalidades e componentes da solução.		
8.5.	Arranque em produção e acompanhamento da solução de segurança: efetuar o arranque da solução de segurança com desligamento da solução atual.		
8.6.	Formação: formação aos técnicos do P.PORTO e escolas, versando os módulos de administração da solução de segurança e de acordo com o plano de formação do fabricante da solução.		

ANEXO II – MORADAS E CONTACTOS

P.PORTO OU SERVIÇOS COMUNS DO INSTITUTO POLITÉCNICO DO PORTO (SC) Rua D. Roberto Frias, 712 4200-465 Porto A/C: José Estrela
P.PORTO / PORTIC Rua Arquitecto Lobão Vital, 172 4200-375 Porto A/C: Jorge Resende
CAMPUS 2 Rua D. Sancho I, 981 4480-876 Vila do Conde A/C: Dr. Jorge Sarmento
ESCOLA SUPERIOR DE EDUCAÇÃO (ESE) Rua D. Roberto Frias, 602 4200-465 Porto A/C: José Freitas
ESCOLA SUPERIOR DE SAÚDE (ESS) Rua Dr. António Bernardino de Almeida, 400 4200-072 Porto A/C: Dr. Sérgio Moreira
ESCOLA SUPERIOR DE TECNOLOGIA E GESTÃO (ESTG) Rua do Curral, Casa do Curral, Margaride 4610-156 Felgueiras A/C: Eng. Pedro Afonso

**ESCOLA SUPERIOR DE MÚSICA E ARTES DO ESPECTÁCULO
(ESMAE)**

Rua da Alegria, 503
4000-045 Porto
A/C: Eng. Gilberto Pereira

**INSTITUTO SUPERIOR DE CONTABILIDADE E ADMINISTRAÇÃO DO PORTO
(ISCAP)**

Rua Jaime Lopes Amorim, s/n
4465-004 S. Mamede de Infesta
A/C: Eng. Rui Pereira

**INSTITUTO SUPERIOR DE ENGENHARIA DO PORTO
(ISEP)**

Rua Dr. António Bernardino de Almeida, 431
4249-015 Porto
A/C: Eng.º Nuno Vinha da Silva