



Caderno de Encargos

“AQUISIÇÃO DE EQUIPAMENTO SECURITY GATEWAY APPLIANCES”



ARTIGO 1.º

OBJECTO

1. O presente Caderno de Encargos compreende as cláusulas a incluir no contrato a celebrar entre a Fundação para a Ciência e a Tecnologia, I.P. e adjudicatário na sequência da adjudicação no âmbito da consulta para aquisição de equipamento Security Gateway Appliances.
2. O **CONTRATO** a celebrar integra, para além do clausulado contratual:
 - a) os suprimientos dos erros ou 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, nos termos do artigo 50º do Código dos Contratos Públicos;
 - b) os esclarecimentos e retificações relativos ao caderno de encargos que sejam emitidos ao abrigo do artigo 50º do Código dos Contratos Públicos;
 - c) o caderno de encargos;
 - d) a proposta adjudicada;
 - e) os esclarecimentos sobre a proposta adjudicada prestados pelo adjudicatário.
3. Em caso de divergência entre os documentos referidos nas diferentes alíneas do número anterior, a prevalência obedece à ordem por que vêm enunciados nas suas diferentes alíneas.
4. Em caso de divergência entre os documentos referidos nas diferentes alíneas do nº 2 e o clausulado contratual, prevalecem os primeiros, salvo quanto aos ajustamentos propostos de acordo com o disposto no artigo 99º do Código dos Contratos Públicos e aceites pelo adjudicatário nos termos do disposto no artigo 101º do mesmo diploma.

ARTIGO 2.º

OBRIGAÇÕES DO ADJUDICATÁRIO

1. O adjudicatário obriga-se a executar o Contrato em termos que se conformem com o estabelecido no Caderno de Encargos, nos anexos que dele fazem parte integrante e na legislação aplicável.
2. Para além de outras obrigações previstas na lei ou no presente caderno de encargos, o adjudicatário obriga-se a:
 - a) Assegurar que o objeto da prestação obedece às especificações técnicas exigidas;
 - b) Cumprir os prazos estabelecidos, designadamente, para a execução das prestações a que se obriga;
 - c) Assegurar a manutenção, suporte e serviços de capacitação e evolução para a solução adjudicada;
 - d) Prestar informação;
 - e) Assegurar o sigilo.

ARTIGO 3.º

ESPECIFICAÇÕES TÉCNICAS

O adjudicatário obriga-se a assegurar que o objeto de aquisição obedece às especificações técnicas que constam do Anexo I ao presente Caderno de Encargos, do qual faz parte integrante.

ARTIGO 4.º

PRAZOS

O adjudicatário obriga-se ao pontual cumprimento de todos os prazos de execução das prestações objeto do contrato, os quais são os que constam do clausulado deste ou de outros documentos referidos no nº 2 do artigo 1º.

ARTIGO 5.º

ENTREGA

1. O bem ou serviço objeto de adjudicação considera-se entregue após a respetiva aceitação por parte da FCT, I.P, a qual será comunicada por escrito ao adjudicatário.
2. O adjudicante poderá promover a realização de testes de aceitação, destinados à verificação da conformidade dos bens ou serviços objeto de adjudicação com os requisitos técnicos constantes do presente Caderno de Encargos.

3. Os testes referidos no número anterior devem ocorrer no prazo de 30 dias corridos após a receção de todos os bens objeto do contrato a qual deve ocorrer nas instalações do Instituto Politécnico de Viseu, sitas na Avenida Cor. José Maria Vale de Andrade, Campus Politécnico Santa Maria, em Viseu no prazo máximo de 60 dias corridos contados a partir da entrada em vigor do contrato.
4. Os bens ou serviços consideram-se aceites na data em que a FCT, I.P. disso expressamente notificar, por escrito, o adjudicatário ou, na ausência de notificação, no dia subsequente ao fixado no número anterior como limite para a realização de testes de aceitação.
5. Se nos termos dos testes de aceitação a FCT, I.P. constatar que os bens ou serviços não cumprem os requisitos técnicos constantes do presente Caderno de Encargos, disso dará conhecimento ao adjudicatário, abrindo-se um prazo de 7 (sete) dias corridos para que este desenvolva as diligências necessárias a que aqueles requisitos sejam cumpridos, e o equipamento seja de novo submetido a testes.
6. Se, estes testes de aceitação, não forem concluídos com êxito, persistindo a desadequação aos requisitos técnicos exigidos, a FCT, I.P. poderá conceder ao adjudicatário novo prazo de 7 (sete) dias corridos para que este desenvolva novas diligências para que os bens ou serviços cumprem os requisitos do Caderno de Encargos ou, em alternativa, considerar incumprida a obrigação de fornecimento dos adaptadores óticos e rescindir o Contrato.

ARTIGO 6.º

OBRIGAÇÃO DE MANUTENÇÃO E GARANTIA

1. Caso se verifique qualquer anomalia no bem objeto de adjudicação que impeça ou prejudique o desempenho da sua função, o adjudicatário obriga-se a proceder às operações necessárias à reposição deste nas mesmas condições que deram origem à aceitação nos termos e condições referidas no Anexo I ao presente Caderno de Encargos.

2. O prazo de garantia do equipamento fornecido respeita os termos e abrangência previstos na lei geral aplicável.
3. O adjudicatário deve assegurar, sem qualquer encargo para a entidade adjudicante, os serviços de manutenção online no regime de 24horasx7diasx4horas.
4. Os serviços de manutenção abrangem eventuais atualizações (updates e ugrades), bem como renovações de licenciamento.

ARTIGO 7.º

OBRIGAÇÃO DE PRESTAÇÃO DE INFORMAÇÃO

O adjudicatário obriga-se a prestar à FCT, I.P., por escrito, toda a informação que lhe for solicitada relativa ao objeto da adjudicação ou à sua atuação em cumprimento das obrigações que para si decorrem do contrato.

ARTIGO 8.º

OBRIGAÇÃO DE SIGILO

O adjudicatário obriga-se a não divulgar informações que obtenha em virtude da execução do **CONTRATO** durante a vigência deste e por um período de dois anos contados a partir da data da sua cessação.

ARTIGO 9.º

PREÇO E CONDIÇÕES DE PAGAMENTO

1. O preço base da aquisição a que se refere o presente caderno de encargos, entendido como o preço máximo que a FCT, I.P. se dispõe a pagar pela execução de todas as prestações que constituem o seu objeto é de 136.377,30 € (cento e trinta e seis mil trezentos e setenta e sete euros e trinta cêntimos) sem IVA incluído.

2. Pela aquisição do bem e/ou serviço objeto da presente aquisição, a FCT, I.P. pagará ao adjudicatário a quantia de ____ Euros [valor indicado na proposta], acrescida de IVA à taxa legal em vigor nos termos do número seguinte.
3. A quantia prevista no número anterior deve ser satisfeita através do pagamento de uma fatura, emitida, após a entrega do bem/serviço nos termos a que se refere o artigo 5º.
4. A fatura a emitir pelo adjudicatário assume a forma de fatura eletrónica, com os requisitos legais, nomeadamente os resultantes do artigo 299º-B do CCP.
5. A fatura referida no número anterior será paga no prazo máximo de trinta dias a contar da sua receção.

ARTIGO 10.º

VIGÊNCIA DO CONTRATO

1. O CONTRATO inicia a sua vigência na data da respetiva assinatura.
2. O CONTRATO cessa vigência no prazo de 3 anos.

ARTIGO 11.º

RESPONSABILIDADE DO ADJUDICATÁRIO

1. O adjudicatário responde pelos danos que causar à **FCT, I.P.** em razão do incumprimento culposo das obrigações que sobre ele impendam, nos termos das normas gerais de direito e do presente artigo.
2. O adjudicatário responde ainda perante a **FCT, I.P.** pelos danos causados pelos atos e omissões de terceiros, por si empregues na execução de obrigações emergentes do **CONTRATO**, como se tais atos ou omissões fossem praticados por aquele.
3. O adjudicatário responde, independentemente de culpa, pelos danos causados à **FCT, I.P.** pela execução deficiente do **CONTRATO**.
4. Nenhuma das partes responde por danos causados à outra parte em virtude de incumprimento de obrigações emergentes do **CONTRATO** decorrente de caso fortuito ou força maior.
5. A parte que pretenda beneficiar-se do regime acolhido no número anterior deve, para o efeito, informar a outra parte da verificação de uma situação de incumprimento decorrente de caso fortuito ou de força maior, fazendo menção dos factos que, em seu entender, permitem atribuir

esta origem ao incumprimento e, ainda, do prazo que estima necessário para cumprir a obrigação em causa.

ARTIGO 12.º

CLÁUSULA PENAL

1. Pelo incumprimento dos prazos a que o adjudicatário se obriga na execução do contrato não abrangidos pelo nº 2, a FCT, I.P. pode, sem prejuízo do n.º 4 do artigo anterior, exigir do adjudicatário o pagamento de uma pena pecuniária calculada de acordo com a seguinte fórmula:

$$P=V \times A/10$$

P – Montante da Penalidade

V – Preço Contratual

A – Nº de dias em atraso, incluindo sábados, domingos e feriados

2. Pelo incumprimento (falhas ou falta de fornecimento) dos prazos referentes aos serviços de manutenção online, a FCT, I.P. pode, sem prejuízo do n.º 4 do artigo anterior, exigir do adjudicatário o pagamento de uma pena pecuniária calculada de acordo com a seguinte fórmula:

$$P=V \times A/150$$

$$a) P = V \times A / 150$$

Em que:

P = montante da penalidade;

V = preço contratual;

A = Número de falhas na resolução dos erros/ocorrências e/ou faltas no fornecimento superiores ao número de horas acordadas no âmbito do contrato, comunicadas pelos serviços da **FCT, I.P.**

3. Entende-se por falha na resolução de erros/ocorrências, a não reposição num prazo até ao número de horas acordadas no âmbito do contrato, da operação normal de funcionalidade e/ou dados da aplicação, inclusive quando causada por propagação de erros na resolução dos erros/ocorrências originais e/ou na realização de tarefas manutenção/atualização por parte do adjudicatário, após comunicação da mesma por parte da **FCT, I.P.**

4. Entende-se por falta no fornecimento, a não realização de serviço e não resposta a um pedido de suporte, num prazo até ao número de horas acordadas para a realização do serviço/suporte no âmbito do contrato, após comunicação da mesma por parte da **FCT, I.P.**

5. Os modos de comunicação de falha considerados são: por telefone, por email, em sistema de suporte disponibilizado pela empresa.

ARTIGO 13.º

RESCISÃO

1. A FCT, I.P. pode rescindir o CONTRATO:

- a) quando, estando o adjudicatário em mora, este não realize a prestação no prazo que lhe haja razoavelmente sido fixado pela FCT, I.P.;
- b) com fundamento em incumprimento das obrigações previstas no artigo 2º que determine a perda objetiva de interesse nas prestações que constituam o seu objeto;

2. A rescisão do CONTRATO ao abrigo do disposto no número anterior determina a perda da caução prestada pelo adjudicatário, caso esta tenha sido prestada nos termos da lei e a extinção dos créditos de que este seja titular em virtude do referido CONTRATO.

3. A perda da caução ao abrigo do número anterior não extingue o direito da **FCT, I.P.** de ser ressarcida da totalidade dos danos que lhe hajam sido causados pela conduta do adjudicatário que haja fundamentado a rescisão.

ARTIGO 14.º

DESPESAS

Correm por conta do adjudicatário todas as despesas em que este haja de incorrer em virtude do cumprimento de obrigações emergentes do CONTRATO.

ARTIGO 15.º

LEI APLICÁVEL

O CONTRATO rege-se pela lei portuguesa.

ARTIGO 16.º

INTERPRETAÇÃO DO CONTRATO

1. Em caso de dúvida sobre a interpretação das regras aplicáveis à execução do **CONTRATO**, o adjudicatário deve solicitar por escrito um esclarecimento à **FCT, I.P.**
2. O adjudicatário obriga-se a ter em conta as orientações que lhe forem transmitidas por escrito pela **FCT, I.P.**, na medida em que as mesmas não colidam com as regras aplicáveis à execução do **CONTRATO**.

ARTIGO 17.º

COMUNICAÇÕES

1. Para efeitos de comunicações relativas à fase de execução do contrato, as partes podem recorrer aos seguintes meios de comunicação:
 - a) correio postal, através de carta registada ou de carta registada com aviso de receção;
 - b) correio eletrónico;
 - c) outro meio de transmissão eletrónica de dados.
2. Todas as comunicações devem ser escritas e redigidas em língua portuguesa.
3. Para efeitos de estabelecimento das comunicações a que se refere o presente artigo, as partes identificam os seguintes contactos, através dos quais as mesmas se devem concretizar:

a) Pela FCT, I.P.:

Nome do representante:

Endereço postal: Av. do Brasil, 101 1700-066 Lisboa

Endereço eletrónico:

Número de fax:

b) Pelo adjudicatário:

Nome do representante:

Endereço postal:

Endereço eletrónico:

Número de fax:

ARTIGO 18.º

GESTOR DO CONTRATO

Para o exercício das funções de acompanhamento da execução do contrato nos termos regulados pelo artigo 290º-A do Código dos Contratos Públicos é designado o Especialista de Informática, Eng. Luís Daniel Maia de Almeida.

ARTIGO 19.º

CESSÃO DA POSIÇÃO CONTRATUAL

1. A cessão da posição contratual do adjudicatário é possível nos termos do artigo 318º do Código dos Contratos Públicos.
2. Em caso de incumprimento contratual pelo adjudicatário que seja suscetível de conduzir à resolução do contrato, a sua posição contratual pode ser cedida aos concorrentes do procedimento pré-contratual classificados nas posições subsequentes à do adjudicatário, nos termos do estabelecido no artigo 318º-A do Código dos Contratos Públicos.

ARTIGO 20.º

DADOS PESSOAIS

1. No tratamento de dados pessoais por conta do adjudicante, o adjudicatário obriga-se ao escrupuloso cumprimento do Regulamento Geral sobre a Proteção de Dados (Regulamento 2016/679) e demais legislação aplicável.
2. O tratamento referido no número anterior é apenas o necessário à execução do contrato e feito durante a sua vigência, aplicando-se, em especial, o estabelecido no nº 3 do artigo 28º do Regulamento Geral sobre a Proteção de Dados.

ARTIGO 21º

(ASSINATURA DO CONTRATO)

O contrato a celebrar entre a FCT, I.P. e o adjudicatário será celebrado com recurso preferencial, por ambas as partes, à assinatura eletrónica qualificada, tal como definida pelo Decreto-lei nº 290D/99, de 2 de agosto, com as alterações introduzidas pelos Decretos-lei n.º 62/2003, de 3 de abril, 165/2004, de 6 de julho e 116-A/2006, de 16 de junho.

ARTIGO 22.º

(TRIBUNAL DE CONTAS)

1. O contrato poderá estar sujeito a fiscalização prévia do Tribunal de contas, nos termos do disposto nº 2, do artigo 318.º da LOE 2020, conjugado com o nº 2 do artigo 48.º da Lei de Organização e Processo do Tribunal de Contas, na sua redação atual
2. Caso se verifique o previsto no número anterior, o contrato apenas produz efeitos financeiros a partir data de obtenção do referido Visto;
3. Os emolumentos devidos, no valor legal, serão suportados pelo adjudicatário.

ANEXO I

(ANEXO TÉCNICO)

Este documento contém as especificações técnicas aplicáveis ao fornecimento de equipamentos e respetivos serviços de instalação com vista à implementação nas instalações do Instituto Politécnico de Viseu (IPV), no âmbito do projeto RCTS100, de interligação das entidades de ensino superior em rede de alto débito.

Equipamento Security Gateway Appliances

O adjudicatário obriga-se a fornecer um cluster de duas appliances de segurança, em alta disponibilidade com funcionalidades/proteções ativas com as seguintes características mínimas por unidade:

Requisitos físicos por unidade:

- **Cinco *slot's* (portas de expansão) para interfaces de I/O, ocupados no mínimo da seguinte forma:**
 - Módulo de 8 interfaces 10/100/1000Base-T RJ45
 - Módulo de 2 interfaces 10GBase-F SFP+
 - Módulo de 4 interfaces 10GBase-F SFP+
 - Possuir no mínimo 2 interfaces Gigabit Ethernet OnBoard
 - Todos os interfaces I/O de fibra ótica devem estar preenchidos com os respetivos transceivers SR 10G
- **Duas portas de expansão livres que permitam no mínimo:**
 - Dois módulos de duas portas cada de 40G QSFP+
 - Dois módulos de duas portas cada de 100/25G QSFP28
 - O Chassis a fornecer deverá ser modular de forma a possibilitar a introdução gradual de cartas expansoras de rede;
 - Deverá ser possível assegurar, no mesmo Chassis, qualquer uma das seguintes combinações a nível de portas:
 - 16x1Gbps UTP (Cobre) + 12x10Gbps FO;
 - 16x1Gbps UTP (Cobre) + 8x10Gbps FO + 2x40Gbps FO;

- 8x1Gbps UTP (Cobre) + 12x10Gbps FO + 2x40Gbps FO;
- 8x1Gbps UTP (Cobre) + 8x10Gbps FO + 4x40Gbps FO;
- 8x1Gbps UTP (Cobre) + 4x10Gbps FO + 4x40Gbps FO + 2x100/25Gbps;
- O chassis deverá disponibilizar duas portas USB para possibilitar ligação de mais do que um dispositivo de segurança em simultâneo;
- Interface LOM.
- O chassis deverá disponibilizar as seguintes opções a nível de storage interno:
 - 2x1TB HDD ou 1x480GB SSD em RAID-1;
- Duas Fontes de alimentação redundantes AC, e Hot Swappable;
- 64G de memória RAM, com possibilidade de expansão até 128GB;
- Dois Processadores com 24x cores físicos e 48x virtual cores;

Requisitos de Performance:

Parâmetros	Métrica (valores mínimos)
Threat Prevention Throughput	> 16Gbps
Firewall Throughput	128 Gbps of UDP 1518 byte packet firewall
NGFW Throughput com Firewall, Application Control and IPS	>20 Gbps
VPN Throughput	> 25 Gbps
Número de novas ligações por segundo	320000
Número de ligações concorrentes	>25 Milhões
Número de acessos remotos simultâneos VPN	200

Requisitos mínimos do licenciamento de software da Firewall:

- Licenciamento para 10 Contextos Virtuais (mínimo assegurado no fornecimento), com possibilidade de expansão até 150;

Next Generation Threat Prevention (NGTP):

- Requisitos para 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 ou v3);
 - Suporte para multicast.
 - Suporte para Routing Multicast:
 - L2 (IGMP v1 ou v2);
 - L3 (PIM-SM, PIM-SSM, PIM-DM).
- Requisitos de alta disponibilidade:
 - Activo/Passivo ou Activo/Standby.
 - VRRP ou IP Virtual ou ClusterXL.
 - Active/Active L2, Active/Passive L2 and L3
 - Failover:
 - Falhas de routing;
 - Falhas de dispositivo;
 - Falhas de ligação (link);
 - Sincronização de sessões entre membros do cluster.

Intrusion Prevention System (IPS):

- O IPS deve ser baseado nos seguintes mecanismos de deteção:
 - Assinaturas;
 - Anomalias no protocol;

- 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 de pacotes/evidências para proteções específicas.
- O IPS deve ser capaz de detetar e bloquear ataques na camada de rede de aplicação, protegendo pelo menos os seguintes tipos de serviços:
 - Serviços de e-mail;
 - 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 controlos remotos, incluindo as que são capazes de realizar tunneling sobre o tráfego http.
- O IPS deve ter proteções SCADA.

- O 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 um browser, numa base de dados local, para utilizadores ou dispositivos que não pertençam ao domínio.
- Deve ter um agente que possa ser instalado nos endpoint's, para reportar à firewall as identidades dos utilizadores.
- A solução deve integrar-se perfeitamente com Microsoft Active Directory, IF-MAP, Radius, Cisco pxGrid, Terminal Servers e terceiros via Web API.
- O impacto do uso da solução de aquisição de identidade no processador dos servidores 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.

Application and URL Filtering:

- A solução deve reconhecer e controlar no mínimo 6000 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 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 instruir ou para confirmarem as suas ações com base nas políticas 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.

Antivírus e AntiBot:

- O fornecedor deve ter solução de Anti-Bot e Antivírus 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 deteção baseado em vários pontos. Reputação de endereços IP, URLs e DNS e detetar padrões de comunicação de bots.
- A proteção anti-bot deve ter capacidade de efetuar Scan a ações de bot.
- A solução deve apoiar a deteção e prevenção de vírus e variantes de Cryptors & ransomware (por exemplo, Wannacry, Cryptlocker, CryptoWall, etc...) 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 comand and control (C&C) DNS hideouts nomeadamente:
 - Pesquisa de padrões de tráfego de comand and control (C&C), não apenas no destino de DNS;
 - Engenharia inversa do respetivo Malware para descobrir o seu DGA (Domain Name Generation);

- DNS Trap, como parte da política de ameaças, interceptar e analisar tentativas de comunicações do endpoint com comand and control (C&C).
- A solução deve detetar e prevenir ataques de DNS tunneling.
- A política de anti-bot e Antivírus deve ser gerida a partir de uma consola central.
- A solução de anti-bot e Antivírus 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 antivírus devem ter atualizações em tempo real na cloud.
- O antivírus deve ser capaz de impedir a entrada de ficheiros maliciosos.
- O antivírus deve ser capaz de analisar ficheiros compactados.
- Políticas antivírus e anti-bot devem ser geridas centralmente e ser possível a parametrização das mesmas.
- O antivírus deve suportar a análise de links dentro de emails.
- O antivírus deve analisar os ficheiros que passam em protocolos CIFS.

IPsec VPN:

- A solução deve 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 deve suportar criptografia 3DES e AES-256 para IKE Phase 1 e 2;
- A solução deve suportar criptografia IKEv2 plus "Suite-B-GCM-128" e "Suite-B-GCM-256" for IKE Phase 2;
- A solução deve 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 deve suportar os seguintes tipos de mecanismos de integridade de dados: md5, sha1, SHA-256, SHA-384 and AES-XCBC.
- A solução proposta deve 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 VPNs de acesso remoto “clientless” e “client based”;
 - Suporte para aplicação de políticas de segurança específicas, para controlo de tráfego associado à comunidade VPN.

Sistemas Virtuais:

- Capacidade e licenciamento para criação de pelo menos 10 sistemas virtuais por nó de cluster.
- Capacidade de redundância dos sistemas virtuais entre os clusters.

Gestão de Segurança:

- A solução deve possibilitar a segmentação da política de segurança numa estrutura de subpolíticas.
- A solução deve possibilitar a segmentação da política de segurança numa estrutura de camadas.
- A solução deve 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 deve suportar role based access control, para segregar acessos de administração para gestão de política e visualização de logs.

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

Componente de gestão, logging e reporting

Deverá ser fornecida em conjunto com a solução:

- Uma plataforma (Hardware ou Software) dedicada para gestão centralizada de firewall e/ou respectivos contextos, com capacidade de gerir diversos clusters de firewall e da firewall já existente.
- Uma plataforma (Hardware ou Software) dedicada para centralização de logs, correlação de eventos e produção de relatórios (relatórios devem ser possíveis de personalizar consoante as necessidades do utilizador);
- A solução de logging, deve estar integrada na componente de gestão centralizada, possibilitar a visualização de logs afetos a políticas específicas, sem ser necessário recorrer a uma nova janela, ou aplicação.

- A solução deve poder ser integrada na componente de gestão centralizada, ou numa appliance/máquina virtual dedicada.
- A solução deve ter a capacidade de produzir logs de todas as políticas (30k logs/seg).
- A solução deve ter a capacidade de consolidar os logs de todas as componentes de segurança que se encontrem ativas na plataforma: IPS, Application Control, URL Filtering, Antivírus, Anti-Bot, User Identity e futuros componentes.
- A solução deve suportar um mecanismo de captura de pacotes para eventos de IPS, para facilitar despiste e análise forense.
- A solução deve 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 servidor de logs e o utilizador final.
- A solução deve disponibilizar detalhes sobre o estado de todos os túneis IPSEC, site-to-site e remote access (client-to-site).
- A solução deve possibilitar a customização de valores de threshold, para execução de ações, uma vez atingido/ultrapassado esse threshold: log, alert, snmp-trap, email notification.

Análise e correlação de eventos:

- A solução deve integrar a componente de report e correlação de eventos com a sua componente de gestão centralizada;
- A solução deve ter a capacidade de correlacionar eventos de todas as funcionalidades ativas nas demais gateways (FW, IPS, URL-F, etc.);
- A solução deve possibilitar a criação de filtros de logging, com base em qualquer característica, tal como: aplicação, IP de origem, IP destino, serviço, tipo de evento, severidade do ataque, país de origem e destino, etc.;

- A solução deve disponibilizar um mecanismo para associar os filtros criados a diferentes tipos de gráficos, atualizados periodicamente, apresentando todos os eventos que igualem o filtro aplicado, permitindo ao administrador focar-se nos eventos mais importantes;
- A solução deve assegurar a possibilidade de pesquisar na lista de eventos, e garantir o “drill down” de detalhes em pesquisas e análise forense;
- A solução deve ter capacidade de detetar e alertar para eventos de login de administradores, em horários não frequentes;
- A solução deve detetar ataques de “credential guessing/brute force”;
- A solução deve reportar todos os eventos de alteração/instalação de políticas de segurança;
- A solução deve incluir relatórios horários, diários, semanais e mensais predefinidos, incluindo pelo menos: Top Events, Top Sources, Top Destinations, Top Services, etc.;

A solução de reporting deve disponibilizar informação consistente sobre:

- Volume de ligações bloqueadas por uma regra de segurança em particular;
- Top de origens bloqueadas, 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 utilizador, com top de utilizadores web e sites mais visitados.

SSL Inspection (inbound / outbound):

- A solução deve suportar inspeção SSL (inspection/decryption) com performance comprovada em todas as tecnologias de mitigação;
- A solução deve suportar Perfect Forward Secrecy (PFS, ECDHE cipher suites);
- A solução deve suportar AES-NI, AES-GCM para throughput melhorado;

- A solução deve suportar a integração das tecnologias de emulação/sandboxing com inspeção SSL;
- A solução deve permitir a reutilização da base de dados de URL Filtering, para criação de políticas de inspeção de SSL granulares.

Requisitos Genéricos:

- A solução não poderá em instante algum abdicar da segurança em detrimento da performance (por exemplo: desabilitar inspeção end-to-end em cenários de “carga” na plataforma).
- A solução proposta deve conter uma plataforma de gestão dedicada com centralização de políticas, logs, reports, sem limite de armazenamento com base em requisitos de licenciamento.
- O servidor de gestão deve 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.
- A Solução deve estar em conformidade com o GDPR European Union's General Data Protection Regulation.

Possíveis futuras expansões:

A solução deve permitir acrescentar algumas funcionalidades futuras, através de licenciamentos de “módulos” de software/funcionalidades de forma unificada, suportadas e desenvolvidas somente pelo mesmo fabricante a integrar na plataforma única de gestão e controlo, a saber:

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 no e-mail.

Cenários de implementação:

- A solução deve fazer parte da arquitetura de prevenção de ameaças (com IPS, AV, AB, URLF, APP FW).
- A solução deve suportar a emulação de ameaças baseada em rede.
- A solução deve suportar a emulação de ameaças baseada em host.
- A solução deve fornecer opção de implementação On Prem e Cloud Based.
- A solução deve suportar integração com terceiros (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 e-mail e proteção Web;
- A solução deve suportar a implementação em modo cluster.

Tipos de ficheiros suportados:

- A solução deve ser capaz de emular ficheiros 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, 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 ficheiros executáveis, arquivos, documentos, JAVA e flash, que sejam transmitidos pelos protocolos:
 - HTTP;
 - HTTPS;
 - FTP;
 - SMTP;
 - CIFS (SMB);
 - TLS SMTP.

Suporte de sistemas operativos:

- 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 detetar 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 motores de deteção baseados em automated machine learning.
- A solução deve detetar 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 detetar ROP e outras técnicas de exploitation (por exemplo, elevação de privilégios), analisando o processador.
- A solução deve suportar a análise de links no corpo do e-mail para deteção de Malware Zero Day.
- A solução deve ser capaz de verificar o histórico de URLs registados nos últimos “x” e-mails e verificar se a classificação foi alterada (por exemplo: de clean para malicious).
- O tempo médio de emulação, para um veredito de malware suspeito como benigno não deve ser muito superior a 1 minuto.

- O 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", permitindo 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% da 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 comand e control (C&C) de acordo com a reputação dinâmica de ip/url.
- A solução deve ser capaz de emular e extrair ficheiros incorporados em documentos.
- A solução deve ser capaz de analisar documentos com URLs.
- Na funcionalidade de Sandboxing/Scrubbing, a solução proposta deve ter a capacidade de suportar deteção de ameaças e técnicas de evasão (com tentativas de explorar vulnerabilidades de sistemas operativos) ao nível do processador, 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, diferente do driver ser carregado - isso deve ser controlado pelo item acima mencionado);
- Análise 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 deve ter capacidade de deteção de técnicas de evasão (emulação/sandboxing) para posterior reação e mitigação de ameaças.
- A solução deve ser resiliente, 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 deve ser resiliente e detetar atrasos implementados na execução de código malicioso (malware/shell-code).
- A solução deve 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 deve ter a capacidade de eliminar ameaças existentes em conteúdos dinâmicos/objetos embebidos em ficheiros.
- A solução deve ter a capacidade de reconstrução dos ficheiros, excluindo os conteúdos ativos, e mantendo apenas conteúdos seguros.
- A solução deve 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 experiência de utilização.

- A solução deve ser configurável e flexível, de forma a possibilitar manter o formato do ficheiro original, especificando o tipo de conteúdo a ser removido.

Anti-Spam & Segurança do Correio eletrónico:

- A solução deve ser agnóstica em relação ao conteúdo, ter a capacidade de classificar ameaças em tempo real, protegendo a infraestrutura com base em padrões comportamentais e não com base no conteúdo.
- A solução deve incluir mecanismos de proteção com base em serviços online de IP reputation, de forma a evitar falsos positivos.
- A solução deve incluir mecanismos de proteção imediata (zero-hour) para novos vírus propagados por correio eletrónico e spam.

Funcionalidades técnicas:

- Suporte para Proxy Implícito e Explícito;
- Suporte para balanceamento de carga entre contextos de firewall (possibilita contextos ativos numa appliance física, e outros ativos na appliance secundária);
- Mecanismo de clustering, deverá suportar mais do que dois elementos no cluster de firewall;