"SOLUÇÃO DE SEGURANÇA PARA REDES DE COMUNICAÇÕES"

Parte I

CLÁUSULAS JURÍDICAS

CLÁUSULAS JURÍDICAS 3

CLÁUSULA 1.ª Objeto 3

CLÁUSULA 2.ª Preço base 3

CLÁUSULA 3.ª Contrato 3

CLÁUSULA 4.ª Prazo e Vigência do Contrato 3

CLÁUSULA 5.ª Obrigações principais do adjudicatário 4

CLÁUSULA 6.ª Objeto do Dever de Sigilo 4

CLÁUSULA 7.ª Prazo do Dever de Sigilo 4

CLÁUSULA 8.ª Proteção de dados pessoais 4

CLÁUSULA 9.ª Preço contratual 5

CLÁUSULA 10.ª Revisão de preços 5

CLÁUSULA 11.ª Condições de pagamento 5

CLÁUSULA 12.ª Penalidades contratuais 5

CLÁUSULA 13.ª Força maior 6

CLÁUSULA 14.ª Resolução por parte do contraente público 7

CLÁUSULA 15.ª Subcontratação e cessão da posição contratual 7

CLÁUSULA 16.ª Comunicações e notificações 7

CLÁUSULA 17.ª Regras ambientais e S.S.T. 7

CLÁUSULA 18.ª Contagem dos prazos 8

CLÁUSULA 19.ª Foro competente 8

CLÁUSULA 20.ª Legislação aplicável 8

PARTE II

CLÁUSULAS TÉCNICAS

1. MEMÓRIA DESCRITIVA - ARQUITETURA 9
2. ÂMBITO DA SOLUÇÃO PRETENDIDA 9
3. REQUISITOS GENÉRICOS 10
4. REQUISITOS DE PERFORMANCE E HARDWARE PARA A APPLIANCE A INSTALAR NA SEDE DA INOVA 11
4.1 REQUISITOS DE PERFORMANCE 11
4.2 REQUISITOS DE HARDWARE 12
5. REQUISITOS DE HARDWARE PARA A APPLIANCE A INSTALAR NA LOJA DO CIDADÃO DA INOVA 13
5.1 REQUISITOS DE PERFORMANCE 13
5.2 REQUISITOS DE HARDWARE 13
6. REQUISITOS PARA A PLATAFORMA DE GESTÃO 14
6.1 GESTÃO DE POLÍTICAS DE SEGURANÇA (SECURITY MANAGEMENT) 14
6.2 MONITORIZAÇÃO E VISUALIZAÇÃO DE LOGS 14
6.3 CORRELAÇÃO DE EVENTOS E RELATÓRIOS 15
6.4 COMPLIANCE E BOAS PRÁTICAS 16
7. FIREWALL 16
7.1 REQUISITOS - FUNCIONALIDADES DE REDE 16
7.2 REQUISITOS DE ALTA DISPONIBILIDADE 17
7.3 REQUISITOS TÉCNICOS/LÓGICOS 17
8. SISTEMA DE PREVENÇÃO DE INTRUSÕES (IPS) 18
9. AQUISIÇÃO DE IDENTIDADE DE UTILIZADORES (USER ID ACQUISITION) 20
10. CONTROLO DE APLICAÇÕES E ACESSO A SITES 20
11. ANTI-BOT E ANTI-VIRUS 21
12. EMULAÇÃO E EXTRAÇÃO DE AMEAÇAS 22
13. DETEÇÃO DE ATIVIDADES EM SISTEMA 23
14. MECANISMOS ANTI-EVASÃO 24
15. EXTRAÇÃO DE AMEAÇAS (FILE SCRUBBING/FLATTENING) 24
16. ANTI-SPAM & EMAIL SECURITY 24
17. IPSEC VPN 25
18. SSL INSPECTION (INBOUND / OUTBOUND) 25

Parte I

CLÁUSULAS JURÍDICAS

CLÁUSULA 1.ª
Objeto

1. O presente Caderno de Encargos compreende as cláusulas a incluir no contrato a celebrar na sequência de procedimento pré-contratual (concurso público) que tem por objeto principal a aquisição de uma SOLUÇÃO DE SEGURANÇA PARA REDES DE COMUNICAÇÕES.
2. Vocabulário principal: Código CPV - 72910000-2; Descrição - Serviços informáticos de segurança.

CLÁUSULA 2.ª
Preço base

O preço base do presente procedimento é de 26.501,00 € (Vinte e seis mil, quinhentos e um euros) ao qual acresce IVA à taxa legal em vigor, contemplando o valor pecuniário de todas as prestações objeto do presente Caderno de Encargos.

CLÁUSULA 3.ª
Contrato

1. O contrato é composto pelo respetivo clausulado contratual e os seus respetivos anexos.
2. O contrato a celebrar integra ainda os seguintes elementos:
   a) Os suprimentos 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;
   b) Os esclarecimentos e as retificações relativas ao Caderno de Encargos;
   c) O presente 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 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 art.º 99º do Decreto-Lei n.º 18/2008, de 29 de janeiro, alterado pelo Decreto-Lei n.º 111-B/2017, de 31 de agosto, e demais alterações, adiante designado por CCP, e aceites pelo adjudicatário nos termos do disposto no art.º 101º desse mesmo diploma legal.

CLÁUSULA 4.ª
Prazos e Vigência do Contrato

1. Os prazos de entrega e prestação dos serviços de instalação e configuração são os seguintes:
   a) Entrega dos equipamentos, 30 dias após a celebração do contrato;

b) Instalação e configuração, até 45 dias úteis após a data referida na alínea anterior.

2. A prestação de serviços de suporte à solução tem uma vigência de três anos, contados a partir da data da configuração, de acordo com os requisitos.

CLÁUSULA 5.ª
Obrigações principais do adjudicatário

Sem prejuízo de outras obrigações previstas na legislação aplicável, no presente Caderno de Encargos ou nas cláusulas contratuais, da celebração do contrato decorre para o adjudicatário a obrigação da prestação do serviço identificado na proposta, em conformidade com o presente Caderno de Encargos.

CLÁUSULA 6.ª
Objeto do Dever de Sigilo

1. O adjudicatário deve guardar sigilo sobre toda a informação e documentação, técnica e não técnica, comercial ou outra, relativa à entidade adjudicante, 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 sejam comprovadamente do domínio público à data da respetiva obtenção pelo prestador de serviços 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 7.ª
Prazo do Dever de Sigilo

O dever de sigilo mantém-se em vigor até ao momento da adjudicação do processo, 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 8.ª
Proteção de dados pessoais

O adjudicatário e a entidade adjudicante obrigam-se, durante a vigência do contrato e, sempre que exigível, após a sua cessação, a dar rigoroso cumprimento ao disposto na respetiva legislação aplicável, nomeadamente, ao Regulamento (EU) 2016/679, do Parlamento Europeu e do Conselho, de 27 de abril, sem prejuízo das obrigações que possam resultar igualmente para terceiros.

CLÁUSULA 9.ª
Preço contratual

1. Pela prestação de serviço objeto do contrato, bem como pelo cumprimento das demais obrigações constantes do presente Caderno de Encargos, a entidade adjudicante deve pagar ao fornecedor o preço constante da proposta adjudicada, acrescido de IVA à taxa legal em vigor, se este for legalmente devido.
2. O preço referido no número anterior deve incluir todos os custos, encargos e despesas cuja responsabilidade não esteja expressamente atribuída ao contraente público.

CLÁUSULA 10.ª
Revisão de preços

Durante a vigência do contrato, não haverá lugar à revisão de preços.

CLÁUSULA 11.ª
Condições de pagamento

1. As quantias devidas pela entidade adjudicante, nos termos da (s) cláusula (s) anterior (es) deve (m) ser paga (s) nos seguintes prazos:
   a) Equipamentos, 30 dias após a entrega;
   b) Serviços, 30 dias após a conclusão e aceitação do projeto.
2. Em caso de discordância por parte da entidade adjudicante quanto aos valores indicados nas faturas, deve esta comunicar ao prestador de serviços, por escrito, os respetivos fundamentos, ficando o prestador de serviços obrigado a prestar os esclarecimentos necessários ou proceder à emissão de nova fatura corrigida ou atuar de acordo com normas fiscais e contabilísticas legalmente aceites.

CLÁUSULA 12.ª
Penalidades contratuais

1. Pelo incumprimento de obrigações emergentes do contrato, a entidade adjudicante pode exigir do prestador de serviços o pagamento de uma pena pecuniária, de montante a fixar em função da gravidade do incumprimento, nos seguintes termos:
   a) Pelo incumprimento das datas e prazos das prestações de serviço objeto do contrato, até 5% do preço contratual;
   b) Pelo incumprimento da obrigação de continuidade da prestação do serviço, até 15% do preço contratual e em último caso a resolução do próprio contrato.
2. Em caso de resolução do contrato por incumprimento do prestador de serviços, a entidade adjudicante, pode exigir-lhe uma pena pecuniária de até 15% do valor do contrato.
3. Ao valor da pena pecuniária prevista no número anterior são deduzidas as importâncias pagas a qualquer título pelo prestador de serviços.
4. Na determinação da gravidade do incumprimento, a entidade adjudicante tem em conta, nomeadamente, a duração da infração, a sua eventual reiteração, o grau de culpa do prestador de serviços e as consequências do incumprimento.

5. A entidade adjudicante pode compensar os pagamentos devidos ao abrigo do contrato com as penas pecuniárias devidas nos termos da presente cláusula.
6. As penas pecuniárias previstas na presente cláusula não obstam a que entidade adjudicante exija uma indemnização pelo dano excedente.

CLÁUSULA 13.ª
Força maior

1. Não podem ser impostas penalidades ao prestador de serviços, nem é havida como incumprimento, a não realização pontual das prestações contratuais a cargo de qualquer das partes que resulte de caso de força maior, entendendo-se como tal as circunstâncias que impossibilitem a respetiva realização, alheias à vontade da parte afetada, que ela não pudesse conhecer ou prever à data da celebração do contrato e cujos efeitos não lhe fosse exigível contornar ou evitar.
2. Podem constituir força maior, se se verificarem os requisitos do número anterior, designadamente, tremores de terra, inundações, incêndios, epidemias, sabotagens, greves, embargos ou bloqueios internacionais, atos de guerra ou terrorismo, motins e determinações governamentais ou administrativas injuntivas.
3. Não constituem força maior, designadamente:
    a) Circunstâncias que não constituam força maior para os subcontratados do prestador de serviços, na parte em que intervenham;
    b) Greves ou conflitos laborais limitados às sociedades do prestador de serviços ou a grupos de sociedades em que este se integre, bem como a sociedades ou grupos de sociedades dos seus subcontratados;
    c) Determinações governamentais, administrativas, ou judiciais de natureza sancionatória ou de outra forma resultantes do incumprimento pelo prestador de serviços de deveres ou ónus que sobre ele recaiam;
    d) Manifestações populares devidas ao incumprimento pelo prestador de serviços de normas legais;
    e) Incêndios ou inundações com origem nas instalações do prestador de serviços cuja causa, propagação ou proporções se devam a culpa ou negligência sua ou ao incumprimento de normas de segurança;
    f) Avarias nos sistemas informáticos ou mecânicos do prestador de serviços não devidas a sabotagem;
    g) Eventos que estejam ou devam estar cobertos por seguros.
4. A ocorrência de circunstâncias que possam consubstanciar casos de força maior deve ser imediatamente comunicada à outra parte.
5. A força maior determina a prorrogação dos prazos de cumprimento das obrigações contratuais afetadas pelo período de tempo comprovadamente correspondente ao impedimento resultante da força maior.

6. Para efeito deste procedimento, é considerada caso de força maior a eventual cessação do contrato de empreitada, por qualquer forma, que torne impossível a prestação de serviço objeto deste contrato.

CLÁUSULA 14.ª
Resolução por parte do contraente público

1. Sem prejuízo de outros fundamentos de resolução do contrato previstos na lei, a entidade adjudicante pode resolver o contrato, a título sancionatório, no caso de o prestador de serviços violar de forma grave ou reiterada qualquer das obrigações que lhe incumbem, designadamente, por atraso, total ou parcial, na prestação do serviço objeto do contrato.
2. O direito de resolução referido no número anterior exerce-se mediante declaração enviada ao prestador de serviços e não determina a repetição das prestações já realizadas, a menos que tal seja determinado pela entidade adjudicante.

CLÁUSULA 15.ª
Subcontratação e cessão da posição contratual

1. A subcontratação pelo adjudicatário e a cessão da posição contratual por qualquer das partes depende da autorização da outra, nos termos do Código dos Contratos Públicos.
2. Em caso de incumprimento, pelo adjudicatário, das suas obrigações, que reúna os pressupostos para a resolução do contrato, o adjudicatário cederá, nos termos do disposto no artigo n.º 318.º-A do CCP, a sua posição contratual ao concorrente do procedimento pré-contratual na sequência do presente procedimento, pela ordem sequencial da classificação dos concorrentes, sempre que tal seja aplicável.

CLÁUSULA 16.ª
Comunicações e notificações

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

CLÁUSULA 17.ª
Regras ambientais e S.S.T.

1. Os concorrentes obrigam-se a cumprir, em termos de S.S.T. e Normas Ambientais, as regras definidas na INOVA-EM, de acordo com os procedimentos existentes na organização, para além daqueles que legalmente estejam obrigados.

2. Faz-se nota que a entidade adjudicante se encontra certificada, ao abrigo das seguintes normas: Sistema de Gestão Ambiental – NP EN ISO 14001 e Sistema de Gestão de Segurança e Saúde no Trabalho, OHSAS 18001/NP 4397:2008 e Sistema de Gestão da Qualidade NP EN ISO 9001.

CLÁUSULA 18.ª

Contagem dos prazos

Os prazos previstos para efeitos do presente processo de concurso contam-se de acordo com o art.º 470º, do CCP, consoante a fase em que o procedimento se encontre.

CLÁUSULA 19.ª

Foro competente

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

CLÁUSULA 20.ª

Legislação aplicável

O contrato é regulado pelo disposto no CCP e restante legislação aplicável.

Parte II

CLÁUSULAS TÉCNICAS

1. MEMÓRIA DESCRITIVA - ARQUITETURA

A INOVA, EM pretende, adquirir em regime de aluguer operacional pelo período de 36 meses, uma Solução de Segurança para Redes de Comunicações, totalmente redundante no site principal ao nível das fontes de alimentação, de elevada performance, escalável, composta por hardware e software (HW e SW) que permita providenciar elevados níveis de segurança de perímetro à INOVA, EM.

A solução a fornecer deverá ser composta pelas seguintes componentes distintas:

- 1x Appliance de Hardware e Software para as instalações sede da INOVA, EM - Sede;
- 1x Appliance de Hardware e Software para as instalações da Loja do Cidadão de Cantanhede;
- Solução VPN Mobile para conexão até 50 utilizadores concorrentes;
- Suporte de manutenção do fabricante dos equipamentos para o HW e SW proposto por um período de 36 meses 24x7x NBD (Next Business Day);
- Suporte WEB e telefónico pelo período de 36 meses com incidências ilimitadas;
- Implementação e configuração da solução global de acordo com os requisitos a apresentar pela INOVA, EM;
- Restantes características, especificações e requisitos dos equipamentos descritas nos pontos a seguir descriminados.

2. ÂMBITO DA SOLUÇÃO PRETENDIDA

Pretende-se adquirir uma solução de firewall com gestão centralizada, para proteger a integridade das redes de comunicações da Sede da INOVA e Loja do Cidadão em Cantanhede.

A solução a apresentar tem de prevenir ataques de dia zero.

A gestão e monitorização de toda a solução deverá ser efetuada numa única plataforma.

A plataforma de gestão/monitorização tem de ter a capacidade de:

- Guardar o registo do tráfego gerado pelos utilizadores internos para a internet;
- Guardar o registo do tráfego gerado pelos utilizadores Externos nos acessos a plataforma;
- Guardar todas as tentativas de acesso ilegítimas externa e internas.

A solução deverá ser apresentada em três componentes:

- Appliance física a instalar na sede da INOVA em Cantanhede;
- Appliance física a instalar na Loja do Cidadão da INOVA em Cantanhede;
- Componente de gestão, virtual presente na Sede da INOVA em Cantanhede;

A solução a colocar na Sede da INOVA terá de permitir interligações em 10Gb, em Fibra, para a infraestrutura existente.

A solução a colocar na Loja do cidadão, terá de permitir interligações em 1Gb, em cobre, para a infraestrutura existente.

3. REQUISITOS GENÉRICOS

Devem ser garantidos os seguintes requisitos genéricos:

a) A solução deverá endereçar todos os requisitos de um equipamento de segurança NGFW (Firewall de última geração), tais como processamento de largura de banda, número de ligações, capacidade de segurança de aplicações de nova geração em todas as vertentes da rede (escritório, centro de dados) num único equipamento;

b) A solução deverá disponibilizar as mesmas funcionalidades de inspeção avançada (Firewall, intrusion prevention, application control, URL filtering, Anti-Bot, Anti-Virus, Sandboxing) em modelo físico e virtual, quaisquer destas geridas por uma única consola central e dedicada;

c) A solução proposta, deverá endereçar todas as funcionalidades que se seguem, de forma unificada, suportadas e desenvolvidas somente pelo mesmo fabricante (single vendor):
   - Statefull Inspection Firewall - A gateway deverá inspecionar end-to-end (não apenas “half-way” ou “header”) todos os fluxos de comunicação desde o estabelecimento da sessão (3-way handshake TCP), durante a transferência de informação (payload), até que esta seja terminada;
   - Intrusion Prevention System;
   - User Identity Acquisition
   - Application Control and URL filtering
   - Anti – Bot / Anti – Virus
   - Threat Emulation (Sandboxing)
   - Threat Extraction (scrubbing)
   - Anti – Spam and Email Security
   - IPSec VPN
   - Remote Access VPN (Mobile Access)

- Data Loss Prevention
- Logging and Status
- Event Correlation and Reporting

d) A solução proposta, não poderá em momento algum "sacrificar" a segurança em detrimento da performance (desabilitar inspeção end-to-end em cenários de "carga" na plataforma);

e) A solução proposta deverá conter uma plataforma de gestão dedicada com:
   - Centralização de políticas, logs, reports;
   - Sem limite de storage com base em requisitos de licenciamento;
   - O servidor de gestão deverá ter a capacidade de obter detalhes de configuração diretamente das gateways de firewall (fetch de informação de routing, interfaces, etc.) de forma "automática", e não apenas se estas forem instanciadas previamente via template, a partir do servidor de gestão;

4. REQUISITOS DE PERFORMANCE E HARDWARE PARA A APPLIANCE A INSTALAR NA SEDE DA INOVA

A appliance a propor terá de cumprir os requisitos mínimos abaixo descritos e permitir escalabilidade, quer em termos de interfaces quer de memoria, para poder acomodar requisitos futuros.

4.1 REQUISITOS DE PERFORMANCE

Parâmetro	Métrica
Threat Prevention/Extraction	≥ 1,8 Gbps
Next-Generation Firewall Throughput	≥ 3,72 Gbps
Intrusion Prevention System Throughput	≥ 4,65 Gbps
VPN Throughput	≥ 2,57 Gbps
Firewall Throughput	≥ 9 Gbps
Connections per second	67 K
Concurrent connections	2 M
VLAN's	1024 interfaces vlan
Acessos remotos simultâneos	50

4.2 REQUISITOS DE HARDWARE

4.2.1 Energia:

Parâmetro	Métrica
Fontes de alimentação redundantes	sim
Consumo Máximo	150W
Valor máximo de emissão de calor	426.3BTU/hr

4.2.2 Dimensões máximas:

Parâmetro	Métrica
Peso	7,5kg
Ocupação no Bastidor	1RU
Dimensões (WxDxH)	438 x 508 x 44 mm

4.2.3 Hardware mínimo:

Parâmetro	Métrica
Storage	1 x 240Gb SSD
Memória	8 GB
CPU	1x CPU, 4 Phy Core’s

4.2.4 Interfaces:

Parâmetro	Métrica
Porta de Consola - USB Type-C	Sim
Porta de Consola - RJ45	sim
Interface de Gestão Dedicado- 10/100/1000Base-T	1
10GBase-F SFP+ port card	4
SFP+ transceiver module for 10G fiber ports - short range	1
USB 3.0	2

4.2.5 Opções de Expansão da solução:

- Possibilitar a expansão da RAM até pelo menos 32 GB
- Possibilitar a expansão do número de acessos remotos concorrentes
- Permitir a adição de Contextos virtuais, por licenciamento

5. REQUISITOS DE HARDWARE PARA A APPLIANCE A INSTALAR NA LOJA DO CIDADÃO DA INOVA

A appliance a propor terá de cumprir os requisitos mínimos abaixo descritos.

5.1 REQUISITOS DE PERFORMANCE

Parâmetro	Métrica
Threat Prevention/Extraction	≥ 340 Mbps
NextGen Firewall	≥ 600 Mbps
Intrusion Prevention System	≥ 670 Mbps
VPN Throughput	≥ 970 Mbps
Firewall Throughput	≥ 1.9 Gbps
Connections per second	10,5 k
Concurrent Connections	500 k
VLANS	≥ 100 Vlans

5.2 REQUISITOS DE HARDWARE

5.2.1 Energia:

Parâmetro	Métrica
Fontes de alimentação redundantes	Não
Consumo Máximo	17.92 W
Valor máximo de emissão de calor	61.11 BTU/hr

5.2.2 Dimensões máximas:

Parâmetro	Métrica
Peso	450 g
Ocupação	Desktop
Dimensões (WxDxH)	210 x 160 x 37,5 mm

5.2.3 Interfaces:

Parâmetro	Métrica
Porta de Consola - USB Type-C	1
Interface WAN Dedicado (10/100/1000Base-T RJ-45 port)	1
Interfaces LAN (10/100/1000Base-T RJ-45 port)	5
USB 3.0	1

6. REQUISITOS PARA A PLATAFORMA DE GESTÃO

6.1 GESTÃO DE POLÍTICAS DE SEGURANÇA (SECURITY MANAGEMENT)

a) A solução deverá possibilitar a segmentação da política de segurança numa estrutura de subpolíticas;
b) A solução deverá possibilitar a segmentação da política de segurança numa estrutura de layers;
c) A solução deverá possibilitar a integração de logs e audit logs numa única consola, para contextualizar o administrador ao efetuar alterações sobre a política de segurança;
d) A solução de gestão deverá suportar role based access control, para segregar acessos de administração para gestão de política e visualização de logs;
e) A solução deverá implementar um mecanismo de comunicação segura, assente em certificados, entre todas as componentes de segurança integradas no sistema de gestão centralizada;
f) A solução deverá incluir um Certificate Authority x.509 com capacidade para gerir/gerar certificados internos, para autenticação de utilizadores em acessos VPN remotos;
g) A solução deverá disponibilizar um mecanismo de pesquisa para facilitar a utilização e identificação de objetos, com base no seu endereço IP;
h) A solução deverá disponibilizar métricas de “hit count” nas regras presentes na política de segurança;
i) A solução deverá possibilitar a utilização de etiquetas (labels) ou secções (tabs) para melhor organização da política de segurança;
j) A solução deverá permitir gravar a política de forma integral ou parcial;
k) A solução deverá disponibilizar um mecanismo de validação da política de segurança, antes da sua instalação nas gateways de firewall;
l) A solução deverá disponibilizar um mecanismo de backup e revisão da política de segurança, possibilitando comparar versões da política e reverter para versões anteriores, se necessário;

6.2 MONITORIZAÇÃO E VISUALIZAÇÃO DE LOGS

a) A solução de logging, deverá estar integrada na componente de gestão centralizada, e possibilitar a visualização de logs afetos a políticas específicas, sem ser necessário recorrer a uma nova janela, ou aplicação;
b) A solução deverá poder ser integrada na componente de gestão centralizada, ou numa appliance/máquina virtual dedicada;
c) A solução deverá ter a capacidade de produzir logs de todas as políticas (30k logs/seg);
d) A solução deverá ter a capacidade de consolidar os logs de todas as componentes de segurança que se encontrem ativas na plataforma: IPS, Application Control, URL Filtering, Anti-Virus, Anti-Bot, Anti-Spam, User Identity, Mobile Access;

e) A solução deverá suportar um mecanismo de captura de pacotes para eventos de IPS, para facilitar despiste e análise forense;
f) A solução deverá implementar um mecanismo seguro de forwarding de logs, com autenticação e encriptação, para evitar potenciais ataques (ex. Eavesdropping);
g) Os logs deverão ser transferidos de forma segura entre a FW gateway, o log server, e o utilizador final;
h) A solução deverá disponibilizar detalhes sobre o estado de todos os túneis IPSEC, site-to-site e remote access (client-to-site);
i) A solução deverá possibilitar a customização de valores de threshold, para execução de ações, uma vez atingido/ultrapassado esse threshold: log, alert, snmp-trap, email notification;

6.3 CORRELAÇÃO DE EVENTOS E RELATÓRIOS

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

6.4 COMPLIANCE E BOAS PRÁTICAS

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

7. FIREWALL

7.1 REQUISITOS - FUNCIONALIDADES DE REDE

a) Suporte para protocolos de agregação de links (LACP 802.3ad);
b) Suporte para funcionamento em modo L2 (bridging) e L3 (routing);
c) Suporte de NAT
    - Static, Hide, PAT;
    - NAT44, NAT46, NAT64, NAT66;
d) Suporte para routing estático;
e) Suporte para Policy Based Routing (PBR);
f) Suporte para protocolos de routing dinâmico:
    - BGP, OSPF (v2 | v3), RIP;
    - Suporte para multicast:
g) Routing Multicast;

h) L2 (IGMP v1 | v2);
i) L3 (PIM-SM, PIM-SSM, PIM-DM);
j) A appliance a propor para a loja do cidadão, não necessita de ter as funcionalidades associadas a IPV6

7.2 REQUISITOS DE ALTA DISPONIBILIDADE

A solução deve permitir a evolução para alta disponibilidade, com os seguintes requisitos:

a) Ativo/Passivo ou Activo/Standby:
   - VRRP ou IP Virtual;
   - Failover:
     - Falhas de routing;
     - Falhas de dispositivo;
     - Falhas de link;
   - Sincronização de sessões entre membros do cluster;

7.3 REQUISITOS TÉCNICOS/LÓGICOS

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

j) A solução tem de suportar as funções de DHCP server e Relay;
k) A solução tem de suportar o suportar a função de proxy em HTTP e HTTPS;
l) A solução tem de ter capacidade de trabalhar em modo transparente/Bridge (L2)
m) A solução tem de suportar alta disponibilidade ou load-sharing e sincronização de estados entre os dois membros do cluster;

8. SISTEMA DE PREVENÇÃO DE INTRUSÕES (IPS)

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

- proteções do servidor

m) 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.

n) 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) O IPS deve ser capaz de capturar de pacotes/evidencias para proteções específicas

p) O IPS deve ser capaz de detetar e bloquear ataques nas layers de network e application layer, protegendo pelo menos os seguintes tipos de serviços:
   - Serviços de email
   - DNS
   - FTP
   - Serviços do Windows (Microsoft Networking)

q) O fornecedor deve fornecer evidências de liderança na proteção de vulnerabilidades Microsoft

r) O IPS e/ou o Application Control deve incluir a capacidade de detetar e bloquear aplicações P2P e evasivas (Anonymizers)

s) O administrador deve poder definir exclusões a plataforma de IPS, baseadas em redes ou hosts.

t) A solução deve proteger DNS Cache Poisoning e impedir o acesso dos utilizadores a endereços de domínio bloqueados

u) Solução deve fornecer proteções para protocolos VOIP

v) O IPS e/ou o Application Control devem detetar e bloquear aplicações que permitam controlo remotos, incluindo as que são capazes de realizar tunneling sobre o tráfego HTTP

w) IPS deve ter proteções SCADA

x) IPS deve possibilitar a conversão de assinaturas SNORT

y) 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.

9. AQUISIÇÃO DE IDENTIDADE DE UTILIZADORES (USER ID ACQUISITION)

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

10. CONTROLO DE APLICAÇÕES E ACESSO A SITES

a) A solução deve reconhecer e controlar mais de 6000 aplicações conhecidas
b) 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
c) A solução deve permitir criar uma regra de filtragem de conteúdos com várias categorias
d) A solução deve permitir filtrar conteúdos de URL's baseada em HTTPS sem efetuar inspeção de SSL
e) A solução deve ser capaz de filtrar um único site sendo este identificado em várias categorias.
f) A solução deve permitir criar regras de segurança por utilizador ou grupo de utilizadores
g) A solução, após 4 semanas de produção, deve ter em cache cerca de 99% das solicitações de categorização.
h) A solução deve ter uma interface fácil de pesquisa de aplicações e URL's
i) A solução deve categorizar aplicações e URL's por fator de risco
j) A política de URLF e Application Control deve poder ser definida por identidade do utilizador
k) A base de dados de URLF e Application Control devem ser atualizados por um serviço Cloud
l) A solução deve ter o controlo de aplicações e URLF unificado na mesma política.

m) A solução deve ter mecanismos para informar ou perguntar ao utilizador em tempo real, para os educar ou para confirmarem as suas ações com base na política de segurança
n) A solução deve ter mecanismo que permita limitar o uso de aplicações com base no consumo de largura de banda
o) A solução deve permitir exceções com base em objetos de rede previamente definidos
p) A solução deve fornecer a opção de modificar a página de Bloqueio e redirecionar o utilizador para uma página de remediação.
q) A solução deve incluir um mecanismo de Black e White List, para permitir que se negue ou permita URL's específicos, independentemente da categoria
r) A solução deve fornecer um mecanismo de substituição na categorização de URL.

11. ANTI-BOT E ANTI-VIRUS

a) O fornecedor deve ter solução de Anti-Bot e Anti-Virus integrado na firewall;
b) A Solução de Anti-Bot deve ser capaz de detetar e parar comportamentos de rede suspeitos
c) O aplicativo Anti-Bot deve usar um mecanismo de deteção baseado em varias pontos. Reputação de endereços IP, URLs e DNS e detetar padrões de comunicação de bots.
d) A proteção Anti-Bot deve ter capacidade de efetuar Scan a ações de bot.
e) A solução deve apoiar a deteção e prevenção de vírus e variantes de Cryptors & ransomware (por exemplo, Wannacry, Cryptlocker, CryptoWall ...) através do uso de análise estática e/ou dinâmica.
f) A solução deve ter suporte para proteção contra-ataques de spear phishing
g) DNS based attacks - A solução deve ter recursos de deteção e prevenção para C&C DNS hideouts:
h) Pesquisa de padrões de tráfego de C & C, não apenas no destino de DNS
i) Reverse engineer do Malware para descobrir seu DGA (Domain Name Generation)
j) DNS Trap, como parte da politica de ameaças, interceta e analisa tentativas de comunicações do endpoint com C&C.
k) A solução deve detetar e prevenir ataques de DNS tunneling.
l) A política de Anti-Bot e Anti-Virus deve ser gerida a partir de uma consola central
m) A solução de Anti-Bot e Anti-Virus deve ter um mecanismo centralizado de correlação e relatório de eventos
n) A solução de antivírus deve ser capaz de impedir o acesso a sites maliciosos
o) A solução de antivírus deve poder inspecionar o tráfego SSL.
p) O Anti-Bot e o Anti-Virus devem ter atualizações em tempo real na cloud.
q) O Antivírus deve ser capaz de impedir a entrada de arquivos maliciosos
r) O Antivírus deve ser capaz de analisar arquivos compactados
s) Políticas antivírus e Anti-Bot devem ser geridas centralmente e ser possível a parametrização das mesmas.
t) O Antivírus deve suportar a analise de links dentro de emails
u) O antivírus deve analisar os ficheiros que estão passam no protocolo CIFS;

12. EMULAÇÃO E EXTRAÇÃO DE AMEAÇAS

a) A solução deve ter a capacidade de proteger contra ataques desconhecidos (malware Zero Day)antes que proteções de assinatura estática sejam criadas:
b) Proteção em Tempo Real para malware desconhecido na navegação Web
c) Proteção em Tempo Real para malware desconhecido em email
d) Cenários de implantação:
e) A solução deve fazer parte da arquitetura de prevenção de ameaças (com IPS, AV, AB, URLF, APP FW)
f) A solução deve fornecer solução de implementação On Prem e Cloud Based
g) Solução de Cloud pura
h) A solução deve suportar integração com 3rd party (public API)
i) A solução deve suportar implementação em modo in-line
j) A solução deve suportar a implementação modo MTA (Mail Transfer Agent)
k) A solução deve suportar implementação em modo de porta TAP / SPAN
l) A solução não deve exigir infraestrutura separada para proteção email e proteção Web
m) A solução deve suportar a implementação em modo cluster.
n) Tipos de ficheiros Suportados - A solução deve ser capaz de emular executáveis, arquivos, documentos, JAVA e flash especificamente:
    - 7z, cab, csv, doc, docm, docx, dot, dotm, dotx, exe, jar, pdf, potx, pps, ppsm, ppsx, ppt, pptm, pptx, rar, rtf, scr, swf, tar, xla, xls, xlsb, xlsm, xlsx, xlt, xltm, xltx, xlw, zip, pif, com, gz, bz2, tgz, apk(android), ipa (iphone), ISO, js, cpl, vbs, jse, vba, vbe, wsf, wsh;
o) A solução deve ser capaz de emular executáveis, arquivos, documentos, JAVA e flash, que sejam transmitidos pelos protocolos:
    - HTTP
    - HTTPS
    - FTP
    - SMTP
    - CIFS (SMB)
    - TLS SMTP
p) OS support:
q) O mecanismo de emulação deve suportar vários sistemas operativos, como XP e Windows7, 8,10 32/64 bits, incluindo imagens personalizadas
r) A solução deve suportar cópias LICENCIADAS de Microsoft WINDOWS e Microsoft Office através de um contrato com a Microsoft.
s) A solução deve detectar chamadas API, alterações em ficheiros, system registry, ligações de rede e processos do sistema

t) A solução deve suportar análise estática para windows, mac OS-X, Linux ou qualquer plataforma x86
u) O mecanismo de emulação deve ser capaz de inspecionar, emular, prevenir e compartilhar os resultados do evento de sandbox na infraestrutura de anti-malware
v) A solução deve permitir a emulação de ficheiros maiores que 10 Mb, em todos os tipos suportados
w) A solução deve suportar automated machine learning based detection engines
x) 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.
y) A solução deve detetar ROP e outras técnicas de exploitation (por exemplo, elevação de privilégios), analizando o CPU
z) A solução deve suportar a analise de links no corpo do e-mail para deteção de Malware Zero Day
aa) A solução deve ser capaz de verificar o histórico de URLs registrados nos últimos X e-mails e verificar se a classificação foi alterada (por exemplo: de Clean para malicious)
bb) Tempo médio de emulação, para um veredito de malware suspeito como benigno não deve ser muito superior a 1 minuto
cc) Tempo médio de emulação, para um veredito de malware suspeito como maligno não deve ser muito superior a 3 minutos
dd) A solução de emulação de ameaças deve permitir "Geo Restriction", que permite que as emulações sejam restritas a um país
ee) 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.
ff) O mecanismo de emulação deve exceder 90% na taxa de captura nos testes do Total de vírus em que os PDFs e os arquivos maliciosos conhecidos são modificados com cabeçalhos "não usados" para demonstrar a capacidade das soluções de detectar malwares desconhecidos
gg) A solução deve detectar o tráfego de C & C de acordo com a reputação dinâmica de ip / url
hh) A solução deve ser capaz de emular e extrair arquivos incorporados em documentos
ii) A solução deve ser capaz de analizar documentos com URL's
jj) Na funcionalidade de Sandboxing/Scrubbing, a solução proposta deverá ter a capacidade de suportar detecção de ameaças e técnicas de evasão (com tentativas de explorar vulnerabilidades de S.O.) ao nível do CPU – CPU-Level detection;

13. DETEÇÃO DE ATIVIDADES EM SISTEMA

a) A solução deve ter a capacidade de detetar atividades fora de "padrão de utilização/protocolo":
b) Chamadas de API
c) Alterações no sistema de arquivos
d) Alterações de Registo
e) Ligações de rede
f) Em Processos do sistema Operativo

g) Criar e eliminar arquivos
h) Modificação de arquivos
i) Adição de código ao kernel
j) Detetar tentativas de elevação de privilégios
k) Alterações no kernel (Alterações de memória realizadas pelo código do kernel, não o fato de que um driver ser carregado - isso é controlado pelo item acima)
l) Analise de comportamento do kernel (analisar a atividade do código, não as alterações efetuadas pelo utilizador)
m) Contornar UAC (user access control)

14. MECANISMOS ANTI-EVASÃO

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

15. EXTRAÇÃO DE AMEAÇAS (FILE SCRUBBING/FLATTENING)

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

16. ANTI-SPAM & EMAIL SECURITY

a) A solução deverá ser agnóstica em relação ao conteúdo, e ter a capacidade de classificar ameaças em tempo real, protegendo a infraestrutura com base padrões comportamentais, e não com base em conteúdo;

b) A solução proposta deverá incluir mecanismos de proteção com base em serviços online de IP reputation, de forma a evitar falsos positivos;
c) A solução deverá incluir mecanismos de proteção imediata (Dia Zero) para novos vírus propagados por email.

17. IPSEC VPN

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

18. SSL INSPECTION (INBOUND / OUTBOUND)

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

f) A appliance a propor para loja do cidadão apenas necessita ter a funcionalidade de SSL Inspection no sentido Outbound.

Cantanhede,

ANTÓNIO MANUEL DINIS MARQUES DE ALMEIDA

Assinado de forma digital por ANTÓNIO MANUEL DINIS MARQUES DE ALMEIDA
Dados: 2022.01.28 15:59:43 Z

(ANTONIO MANUEL DINIS MARQUES DE ALMEIDA)