



CADERNO DE ENCARGOS

**AQUISIÇÃO DE HARDWARE, SOFTWARE E SERVIÇOS DE IMPLEMENTAÇÃO
PARA UMA SOLUÇÃO DE SEGURANÇA DA INFORMAÇÃO - FIREWALL DO
HOSPITAL DIVINO ESPÍRITO SANTO DE PONTA DELGADA, EPER**

**Capítulo I
Disposições gerais**

**SECÇÃO I
Cláusula 1.^a
Caderno de Encargos**

O presente Caderno de Encargos e seus anexos compreende as cláusulas a incluir no contrato a celebrar na sequência do procedimento pré-contratual a efetivar pelo Hospital Divino Espírito Santo de Ponta Delgada, EPER (HDES), no âmbito do procedimento por ajuste direto, para a aquisição de hardware, software (licenciamento perpétuo e subscrição de serviços) e serviços de implementação para uma solução de segurança da informação - firewall

**Cláusula 2.^a
Objeto**

O presente caderno tem por objeto regular a aquisição de hardware, software (licenciamento perpétuo e subscrição de serviços) e serviços de implementação para uma solução de segurança da informação - firewall, de acordo com as cláusulas técnicas do presente Caderno de Encargos

**Cláusula 3.^a
Representantes das Partes**

1. Cada uma das partes obriga-se a nomear um representante responsável pelo acompanhamento da execução do contrato e que desempenhe o papel de interlocutor com a parte contrária para todos os fins associados à execução do contrato.



2. Cada uma das partes obriga-se a informar, por escrito, a outra parte da identidade e dos contratos dos respetivos representantes previstos nos números anteriores.

Cláusula 4.^a

Preço Base

O preço base do equipamento é de € 74.500,00 (setenta e quatro mil e quinhentos euros), não incluindo o imposto sobre o valor acrescentado.

SECÇÃO II

Contrato

Cláusula 5.^a

Contrato

1. O contrato é composto pelo respetivo clausulado contratual e os seus anexos, caso existam
2. O contrato a celebrar integra ainda os seguintes elementos:
 - a) Os suprimimentos dos erros e das omissões do Caderno 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 61.º do Código dos Contratos Públicos;
 - b) Os esclarecimentos e as retificações relativos 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 artigo 99.º do C.C.P. e aceites pelo adjudicatário nos termos no disposto no artigo 101.º desse mesmo diploma legal.



Cláusula 6.^a

Prazo de entrega

A entrega e implementação dos componentes da solução será efetuada no máximo de 45 (quarenta e cinco) dias a contar a emissão da nota de encomenda.

Cláusula 7.^a

Formalização do Contrato

1. A adjudicação é formalizada por contrato escrito, obrigando-se o adjudicatário a entregar toda a documentação necessária para a sua celebração.
2. Em simultâneo com a decisão da adjudicação é aprovada a minuta do contrato pelo órgão competente para a decisão de contratar.
3. A aprovação da minuta do contrato a celebrar e os ajustamentos propostos pelo órgão competente para a decisão de contratar consideram-se aceites pelo adjudicatário quando haja aceitação expressa ou quando não haja reclamação nos 5 (cinco) dias subsequentes à respetiva notificação.
4. As reclamações da minuta do contrato a celebrar são podem ter por fundamento a previsão de obrigações que contrariem ou não constam dos documentos que integrem o contrato nos termos do disposto nos n.ºs 2 e n.º 5 do artigo 96.º do Código dos Contratos Públicos, ou ainda a recusa dos ajustamentos propostos.
5. No prazo de 10 (dez) dias úteis a contar da reclamação, o órgão que aprova a minuta do contrato notifica o adjudicatário da sua decisão, equivalendo o silêncio à rejeição da reclamação.
6. Os ajustamentos ao contrato que sejam aceites pelo adjudicatário serão notificados ao concorrente.
7. O órgão competente para a decisão de contratar comunica ao adjudicatário com a antecedência mínima de 5 (cinco) dias, a data, a hora, e o local em que ocorrerá a outorga do contrato.
8. Todas as despesas inerentes à celebração do contrato, nomeadamente os emolumentos devidos ao Tribunal de Contas, são da responsabilidade do adjudicatário, caso estas existam.



Cláusula 8.^a

Subcontratação

O adjudicatário não poderá, por qualquer forma subcontratar terceiras entidades para a realização de tarefas relativas ao objeto do contrato, sem prévio consentimento da entidade adjudicante.

Cláusula 9.^a

Cessão da posição contratual

1. O adjudicatário não poderá ceder a sua posição contratual ou qualquer dos direitos e obrigações decorrentes do contrato sem autorização da entidade adjudicante.
2. Para efeitos de autorização do número anterior deve ser apresentado pelo cessionário toda a documentação exigida ao adjudicatário no presente procedimento.
3. À entidade adjudicante cabe apreciar, designadamente, se o cessionário não se encontra em nenhuma das situações previstas no artigo 55.º do Código dos Contratos Públicos.

Capítulo II

Disposições gerais

Obrigações contratuais

SECÇÃO I

Obrigações do fornecedor

Subsecção I

Disposições gerais

Cláusula 10.^a

Obrigações principais do fornecedor

Obrigações de fornecer à Entidade Contratante, os equipamentos objeto do fornecimento com as características, especificações e requisitos técnicos e operacionais previstos nas Cláusulas Técnicas do Caderno de Encargos e na proposta adjudicada.

Artigo 11.^a

Patentes, licenças e marcas registadas



1. Quaisquer encargos decorrentes da utilização, no fornecimento, de marcas e/ou patentes registadas ou licenças são da exclusiva responsabilidade do adjudicatário.
2. Caso a entidade adjudicante venha a ser demandada por ter infringido, na execução do contrato, qualquer dos direitos mencionados no número anterior, o adjudicatário indemniza-o de todas as despesas que, em consequência, haja de fazer e de todas as quantias que tenha de a pagar seja a que título for.

Subsecção II Dever de sigilo

Cláusula 12.^a Objeto do dever de sigilo

1. O fornecedor deve garantir sigilo sobre todas as informações e documentação, técnica e não técnica, comercial ou outra relativa ao Hospital Divino Espírito Santo de Ponta Delgada, EPER, 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 destino 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 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 componentes.

Cláusula 13.^a Prazo do dever de sigilo

O dever de sigilo mantém-se em vigor até ao termo do prazo de 5 (cinco) anos a contar do 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, de prestígio ou da confiança devidos às pessoas coletivas.

SECÇÃO II



Obrigações da entidade adjudicante

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, ao Hospital Divino Espírito Santo de Ponta Delgada, EPER 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 inclui todos os custos, encargos e despesas cuja responsabilidade não esteja expressamente atribuída ao Hospital Divino Espírito Santo de Ponta Delgada, EPER.

Cláusula 15.^a

Condições de pagamento

1. As quantias devidas pelo contraente público, nos termos da (s) cláusula(s) anterior(es), deve(m) ser paga(s) no prazo de 60 (sessenta) dias após a receção pelo contraente público das respetivas faturas, as quais só podem ser emitidas após vencimento da respetiva obrigação.
2. Em caso de discordância por parte do contraente público, 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 nova fatura corrigida.

Capítulo III

Penalidades contratuais e resolução

Cláusula 16.^a

Penalidades

1. Se o adjudicatário se atrasar na instalação dos equipamentos por razões que lhe sejam imputáveis, será aplicada uma penalização de 0,1% nos primeiros 15 dias (consecutivos) superiores ao prazo contratado, 0,2% nos 30 dias seguintes a este prazo e 0,3% para atrasos



superiores.

2. A falta de cumprimento dos prazos de assistência técnica em caso de avaria implica a aplicação de uma multa em função do valor da adjudicação que será definida no contrato.

Cláusula 17.^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 os efeitos não lhe fossem razoavelmente 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 grupo 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.

Cláusula 18ª

Resolução por Parte do Contraente Público

1. Sem prejuízo de outros fundamentos de resolução do contrato previstos na lei, Hospital Divino Espírito Santo de Ponta Delgada, EPER, 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 nos seguintes casos:
- a)- Atraso, total ou parcial, na conclusão dos serviços objeto do contrato superior a 8 (oito) dias ou declaração escrita do prestador de serviços de que o atraso em determinada entrega excederá esse prazo;
 - b)- Quebra de sigilo e confidencialidade nos termos definidos na cláusula 12ª;
 - c)- Provocação de conflitos com os trabalhadores do Hospital Divino Espírito Santo de Ponta Delgada, EPER ou com os seus utentes;
 - d)- A prática de atos com dolo ou negligência que prejudiquem o normal funcionamento do Hospital Divino Espírito Santo de Ponta Delgada, EPER;
 - e)- A recusa do adjudicatário em conformar a programação dos seus trabalhos com as necessidades e imperativos da atividade hospitalar;
 - f)- Oposição às visitas ou operações de verificação e controle;



g)- Quando se verificar que o resultado da prestação não corresponde às características que lhe são atribuídas na proposta apresentada pelo adjudicatário, que para o efeito ficará anexa ao contrato;

h)- Cessão da posição contratual, total ou parcial do objeto do presente contrato, sem autorização expressa do Hospital Divino Espírito Santo de Ponta Delgada, EPER;

i)- Utilização de colaboradores com vínculos não autorizados pela lei laboral, ou que não reúnam as condições profissionais legalmente exigíveis para o efeito;

j)- Se ocorrer o início da fase jurisdicional de um processo de falência ou insolvência, ou de um processo com fins análogos, relativamente ao prestador de serviços;

2. A intenção de resolução do contrato deverá ser comunicada ao prestador de serviços, por carta registada com aviso de receção, com a antecedência mínima de 60 (sessenta) dias.

3. 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 pelo Hospital Divino Espírito Santo de Ponta Delgada, EPER.

Capítulo IV Caução e Seguros

Cláusula 19.^a Execução da caução

1. Não será exigida caução, nos termos do n.º 2 do artigo 88.º do Código dos contratos Públicos.

Capítulo V Resolução de Litígios e Disposições finais

Cláusula 20.^a Foro competente

Para resolução de todos os litígios decorrentes do contrato fica estipulado a competência do tribunal administrativo de círculo de Ponta Delgada, com expressa renúncia a qualquer outro.



Cláusula 21.^a

Comunicações e notificações

1. Sem prejuízo de serem 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.
2. Qualquer alteração das informações de contato constantes no contrato deve ser comunicada à outra parte.

Cláusula 22.^a

Deveres de Informação

1. Cada uma das partes deve informar de imediato a co-contratante de quaisquer circunstâncias que cheguem ao seu conhecimento e possam afetar os respetivos interesses na execução do contrato, de acordo com a boa fé.
2. Em especial, cada uma das partes deve avisar de imediato a outra de quaisquer circunstâncias, constituam ou não força maior, que previsivelmente impeçam o cumprimento ou o cumprimento tempestivo de qualquer uma das suas obrigações, bem como do tempo e/ou da medida em que previsivelmente será afetada a execução do contrato.

Cláusula 23^a

Contagem de prazos

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

Cláusula 24.^a

Legislação aplicável

O contrato é regulado pela legislação portuguesa, em particular pelo CCP e pelo Decreto Legislativo Regional n.º 27/2015/A, de 29 de dezembro.

Solução de Segurança da Informação – Firewalls

O equipamento de segurança de informação, responsável pela gestão de acesso à internet pelos colaboradores, encontra-se em fim de ciclo de vida. Hoje as necessidades de segurança vão além do controlo do tráfego de internet sendo necessário adotar arquiteturas de “confiança zero” que abranjam todo o tráfego dentro da organização.

A solução a adquirir garante os requisitos indicados Resolução do Conselho de Ministros n.º 41/2018, que define orientações técnicas para a Administração Pública em matéria de arquitetura de segurança das redes e sistemas de informação relativos a dados pessoais bem como das normas do Decreto-Lei n.º 65/2021, de 30 de julho que Regulamenta o Regime Jurídico da Segurança do Ciberespaço e define as obrigações em matéria de certificação da cibersegurança em execução do Regulamento (UE) 2019/881 do Parlamento Europeu, de 17 de abril de 2019.

Especificações técnicas

Hardware

A firewall tem de garantir os seguintes requisitos:

- Portas 10/100/1000 Mbit/s RJ45 ≥ 12
- Portas 1/10 Gbit/s SPF+ ≥ 8
- Portas 40 Gbit/s WSFP+ ≥ 4
- Portas de gestão dedicada "Out of Band" 10/100/1000 Mbit/s ≥ 1
- Portas de alta disponibilidade 10/100/1000 Mbit/s ≥ 2
- Portas de alta disponibilidade 10 Gbit/s SPF+ ≥ 1

- Porta USB
- SSD ≥ 240 GB
- Fonte de alimentação redundante ≥ 2
- Consumo máximo de energia a 240 V CA: $\leq 1,0$ A
- Montável em rack padrão de 19" com U space $\leq 2U$
- Arquitetura com recursos de hardware dedicados e independentes entre os serviços de gestão e os serviços de inspeção. Deverá estar garantido que a appliance de Firewall quando gerida localmente e perante uma sobrecarga dos serviços de inspeção de tráfego não afete a performance dos serviços de gestão e vice-versa.

Performance

A firewall tem de garantir as seguintes métricas:

- Performance da appliance com a funcionalidade de firewall com identificação e controle de aplicações (inspeção L7 de todo o tráfego - valores de produção) ≥ 8 Gbps (pacotes HTTP /64Kb)
- Performance da appliance com as funcionalidades IDS/IPS, Antivírus e Anti-Spyware (valores de produção) ≥ 4 Gbps (pacotes HTTP /64Kb)
- Performance da appliance com a funcionalidade de VPN IPSec ≥ 5 Gbps (pacotes HTTP /64Kb)
- Número de novas sessões por segundo $\geq 100\ 000$ (transações HTTP de 1 byte)
- Número máximo de sessões $\geq 3\ 000\ 000$

Networking

A firewall tem de garantir as seguintes funcionalidades:

- As interfaces de rede da appliance suportam os seguintes modos de funcionamento: TAP, Layer 2, Layer 3
- Suporte de IEEE 802.1Q
- Suporte de IEEE 802.1AX, suportando até 8 grupos de agregação com 8 interfaces por cada grupo
- Suporte de protocolos dinâmicos de routing: RIP, OSPF, BGP
- Suporte de routing estático
- Suporte de DHCP, NAT e PAT
- Detecção de falhas bidirecionais entre a appliance e router para aplicar a protocolos de routing dinâmico ou rotas estáticas
- Realizar policy based routing através do IP ou rede de origem
- Realizar policy based routing através do tipo de aplicação
- Suporte de arquiteturas de alta disponibilidade do tipo ativo/passivo e ativo/ativo
- Criação de clusters de alta disponibilidade escaláveis pelo menos até 6 membros
- Suporte para TLS 1.3 e capacidade de descriptar este tráfego

Gestão localizada e centralizada

A firewall tem de garantir as seguintes funcionalidades:

- Gestão e administração da própria appliance através de interface web, linha de comandos e API XML, com possibilidade de criar diferentes perfis e cargos de administração para a gestão da appliance, com diferentes níveis de privilégio

- Criar na gestão centralizada e local perfis de administração que permitam segmentar a gestão em diferentes tenants (Por Firewall, por número de firewalls) - Multi-tenancy
- Criar na gestão centralizada e local diferentes perfis e cargos de administração para a gestão da appliance, com diferentes níveis de privilégio
- Editar na gestão centralizada e local configurações pendentes que ainda não foram aplicadas.
- Visualizar e validar na gestão centralizada e local alterações à configuração antes de estas alterações serem aplicadas
- Descartar alterações à configuração realizadas
- Armazenar diferentes versões da configuração
- Na gestão centralizada criar hierarquização da política de segurança para permitir ter políticas globais para toda infraestrutura instalada.
- Na gestão centralizada existe a capacidade de stacks de templates com configurações reutilizáveis para múltiplos equipamentos.
- A gestão centralizada garante um ponto centralizado para efectuar upgrades e atualizações de versões e assinaturas.
- Transformar políticas de layer4 em layer7 com machine learning e aprendizagem embebida na plataforma de gestão
- Na gestão centralizada existe "zero touch provisioning" para simplificar o deployment de firewalls remotas
- Gerir na gestão centralizada SD-WAN para localizações remotas.
- Na gestão centralizada gerir até 25 firewalls num único servidor de gestão. Com licenciamento adicional essa capacidade deve poder ser estendida.
- A gestão centralizada pode funcionar como controladora de gestão para várias máquinas de gestão centralizada.
- Correr a Gestão centralizada sobre hardware dedicado assim como numa Máquina Virtual em VMware ESXi™, KVM e Microsoft Hyper-V, ou então em clouds publicas incluindo

- Google Cloud Platform (GCP™), Amazon Web Services (AWS®), AWS GovCloud, Microsoft Azure e Azure GovCloud.
- Análise da utilização das regras para reduzir superfície de exposição e melhorar postura de segurança.
 - Envio de logs via SYSLOG, FTP, SCP e TFTP para retenção e posterior tratamento
 - Envio seletivo de logs, de acordo com o nível de severidade ou outros atributos como por exemplo o tipo de ameaça
 - Suporte de SNMP, incluindo a possibilidade de obter estatísticas relacionadas com o processamento de logs e com as funcionalidades de alta disponibilidade

Identificação de Utilizadores

A firewall tem de garantir as seguintes funcionalidades:

- Aplicar políticas baseadas em utilizadores e grupos, em vez de IP
- Integrar com sistemas de diretórios para obtenção de utilizadores e grupos, incluindo Microsoft Active Directory, Novell eDirectory e Sun ONE Directory
- Integrar com sistemas multiutilizador como Citrix ou Microsoft Terminal Server para identificação de utilizadores
- Analisar mensagens de SYSLOG com informação de LOGIN/LOGOUT para identificação de utilizadores
- Gerir utilizadores através de API XML
- Identificar utilizadores através de portal de autenticação próprio, fazendo uso dos seguintes protocolos: Kerberos, NTLM, SAML SSO, TACACS+, RADIUS, Certificados de Cliente e autenticação local
- Obter a identidade dos utilizadores a partir dos seguintes métodos: LDAP, Captive Portal, VPN, NACs (XML e API), Syslog, Terminal Services, XFF Headers, Server Monitoring, e client probing

Solução de Acessos Remotos e Gestão de Identidades

A firewall tem de garantir as seguintes funcionalidades:

- Estender as funcionalidades modulares avançadas da Firewall (Threat Prevention, URL Filtering e outros) aos utilizadores remotos
- Garantir a segurança dos acessos aos recursos internos como também as aplicações de cloud
- Garantir a segurança também do acesso á internet do utilizador que esteja fora da rede.
- Proteger os utilizadores remotos contra ataques de phishing e roubo de credenciais
- Colocar em quarentena utilizadores remotos utilizando parâmetros e características imutáveis.
- Suporte de VPNs por Aplicação e por utilizador
- Fornecer acesso seguro e sem agente para parceiros e entidades externas as organizações.
- Identificar de forma automatizada equipamentos que não são geridos pela entidade da firewall.
- Implementar Zero Trust efetuando uma identificação muito clara do utilizador.
- Efetuar a identificação de parâmetros do sistema operativo para poder criar regras de acesso do tipo NAC.
- Identificar os seguintes parâmetros do equipamento que esta aceder á rede: verificar se Patch Management está ativo, verificar se a Firewall local está ativa, verificar se Anti-Malware está instalado, verificar se Plataforma de Backups está ativa, verificar se Mecanismo de Encriptação de disco esta ativo, verificar se Modulo de DLP está ativo, bem como outros parâmetros customizados do sistema operativo (processos, registos ou listas de propriedades).
- Disponibilizar um agente com suporte para os seguintes sistemas operativos: Windows 7 e posterior, macOS 10.11 e

- posterior, iOS 10 e posterior, Android 5 e posterior, CentOS e RHEL 7.0 até 7.7 e Ubuntu 14.04 até 19.04.
- O mesmo agente de acessos remotos deve também poder funcionar como agente de identidades dentro da infraestrutura para identificação do utilizador e mapeamento de políticas baseadas em identidades.

Funcionalidades Gerais de Segurança

A firewall tem de garantir as seguintes funcionalidades:

- Agrupar interfaces da appliance em conjuntos independentes, formando diferentes zonas de segurança
- Definir a política de segurança por zonas de segurança, podendo incluir na mesma política várias zonas de origem e/ou destino para a análise de tráfego e processamento de regras de segurança
- Criar múltiplas regras de segurança entre zonas de origem e destino
- Identificar de aplicações em L7 com um mínimo de 2400 aplicações identificadas. Identificar obrigatoriamente na resposta as aplicações identificáveis através de url ou documento anexo
- Identificar de subfunções dentro de uma aplicação
- Aplicar e/ou excepcionar qualquer das funcionalidades de inspeção (IPS, Antivírus, etc.) apenas ao tráfego de determinadas aplicações L7
- Agrupar aplicações por categorias de forma que as políticas de segurança sejam aplicadas por categorias de aplicações
- Identificar as aplicações quando estas não utilizam os portos TCP/UDP por defeito em qualquer tipo de tráfego/protocolo e não somente HTTP
- Identificar aplicações proprietárias que usem os protocolos HTTP e TCP

- Identificar aplicações que sejam transportadas em túneis encriptados SSL
- Decifrar tráfego SSH e detetar aplicações não legítimas que utilizem este protocolo para comunicar (SSH tunneling)
- Criar regras de QoS segundo as aplicações utilizadas no tráfego
- Aplicar políticas de NAT de forma independente das restantes políticas de segurança
- Forçar o uso de MFA para acesso a aplicações internas

Relatórios & Logs

A firewall tem de garantir as seguintes funcionalidades:

- Gerar relatórios tanto predefinidos ou personalizados, utilizando os logs criados pelo próprio equipamento sem necessidade de equipamentos externos adicionais
- Gerar relatórios de atividade por utilizador, incluindo aplicações utilizadas e páginas web visitadas
- Gerar relatórios de forma automática assim como agrupar vários relatórios num único documento em formato pdf
- Entre os modelos de relatórios disponíveis devem constar relatórios com a largura de banda consumida pelas diferentes aplicações, relatórios sobre as origens e destinos geográficos das ameaças detetadas e relatórios sobre a análise do comportamento do tráfego observado que permita detetar equipamentos comprometidos que participem em botnets
- Programar o momento em que se deseja a geração do relatório pretendido e o seu envio através de e-mail, assim como o intervalo temporal que se pretende
- Armazenar os logs localmente tendo por única restrição a capacidade do disco do próprio equipamento

- Enviar logs para uma plataforma externa de gestão e processamento especializado de logs com o objetivo de manter os logs a longo prazo
- Dispor de um painel de instrumentos personalizável por utilizador de administração da appliance com pelo menos a seguinte informação: Aplicações mais utilizadas, Aplicações de alto risco, Informação geral do sistema, Estado das interfaces, Logs relativos às ameaças mais observadas, Logs de URLs filtrados, Recursos do sistema
- Dispor de estatística gerada a partir de logs, personalizável por utilizador que permita fornecer informações como: utilizadores que mais geram tráfego, regras de segurança que mais utilizam, vulnerabilidades mais detetadas e bloqueadas, equipamentos que acederam a domínios maliciosos, vírus detetados, informação enviado ao serviço de sandboxing e equipamentos internos comprometidos
- Utilizar um motor integrado de correlação de eventos dentro da própria appliance para que a partir dos logs criados se possa obter informações de alto nível

Outras Funcionalidades

A firewall tem de garantir ainda as seguintes funcionalidades:

- Definir aplicações e/ou vulnerabilidades customizadas mediante diferentes parâmetros como: Portos TCP/UDP que sejam usados na aplicação e combinação de padrões dentro dos "headers" dos pacotes ou mesmo no "payload" dos próprios pacotes que se devam cumprir para que se reconheça a aplicação e/ou vulnerabilidade
- Decifrar tráfego SSL e SSH para que se possa estabelecer políticas de descriptação baseadas em: zonas por onde passa o tráfego, IP de origem ou destino, utilizadores geram esse tráfego, portos utilizados

- Criar exceções à descriptação para determinado tipo de tráfego
- Decifrar tráfego com destino a sites web que utilizam certificados de curva elíptica (ECC)
- Enviar tráfego após descriptação para uma interface de port mirror para análise de terceiras partes
- Capturar tráfego em formato pcap, podendo ser estabelecido como critérios de captura do tráfego, uma determinada aplicação independentemente da origem ou destino desse tráfego
- Capturar tráfego em formato pcap exclusivamente quando se deteta um vírus ou um ataque em qualquer um dos motores de proteção

Threat Prevention - IDS/IPS / Antivírus & Anti-Malware

A firewall tem de garantir ainda as seguintes funcionalidades:

- Aplicar políticas de prevenção ou de deteção contra a exploração de vulnerabilidades, tanto no tráfego que vai para a Internet como no tráfego que vem da Internet, sem incorrer numa latência superior a 1ms para não penalizar a experiência do utilizador, efetuando a análise numa única passagem do tráfego para todas as ameaças
- Aplicar diferentes perfis proteção contra exploração de vulnerabilidades de acordo com as aplicações identificadas
- Selecionar proteções contra a exploração de vulnerabilidades que se apliquem apenas a clientes ou servidores ou a ambos
- Categorizar as vulnerabilidades por tipo e por nível de risco, de forma que a aplicação de perfis de proteção se possam realizar com base nestas categorias
- Identificar as proteções pela identificação CVE das vulnerabilidades

- Aplicar apenas as assinaturas necessárias para determinada aplicação identificada, através da seleção de perfis
- Converter e importar assinaturas snort e suricata
- Detetar equipamentos possivelmente comprometidos que tentem estabelecer comunicações com servidores de C&C
- Habilitar mecanismos de DNS sinkholing que permitam intercetar pedidos de resolução de nomes para domínios comprometidos com malware
- Definir políticas de antivírus, para que a transferência de ficheiros realizada no sentido Internet para rede interna ou vice-versa, sejam inspecionados e bloqueados se o seu conteúdo for malicioso
- Capacidade de aplicar políticas que permitam aplicar o motor de antivírus sobre protocolos como FTP, HTTP, IMAP, POP3, SMB ou SMTP, definindo para cada um destes protocolos a ação a realizar (permitir os ficheiros, descartar os ficheiros, desconectar a sessão ou registar mediante logs)
- Enviar o ficheiro para serviços de inspeção adicionais na cloud que permitam analisar e emitir um veredicto para que appliance possa tomar uma ação no caso de um ficheiro malicioso
- Aplicar políticas de antivírus de forma granular, permitindo aplicar essas políticas utilizadores ou grupos, a determinados segmentos de rede com determinada direção e a determinadas aplicações
- Identificar ficheiros não através das suas extensões, mas sim através do tipo MIME do ficheiro, permitindo no mínimo a identificação de 100 tipos de ficheiros. Identificar obrigatoriamente na resposta os tipos de ficheiros através de url ou documento anexo
- Aplicar políticas de bloqueio de ficheiros, de forma a poder bloquear a transferência de certo tipo de ficheiros ou que se permita após a confirmação por parte do utilizador e criando um log correspondente

- Aplicar políticas de bloqueio de ficheiros atendendo a critérios como origem e destino do tráfego, utilizador ou grupo, tipo de aplicação ou de tráfego que inicia a transferência do ficheiro
- Bloquear a transferência de ficheiros em URLs categorizados como perigosos do ponto de vista de ameaça de segurança
- Pesquisar padrões sensíveis no tráfego, evitando a exfiltração de dados
- Analisar ficheiros executáveis e scripts powershell com um motor de machine learning local que permita bloquear ficheiros maliciosos localmente em tempo real sem necessidade de estabelecer ligações externas. Este motor deve permitir bloquear malwares nunca antes observados e para os quais não existem assinaturas sem necessidade de recorrer a sandboxing.
- Receber updates em tempo real de forma a não ter que aguardar minutos/horas/dias por determinado update. Assim que um novo malware é detetado por qualquer cliente do fabricante essa informação deve ser propagada em tempo real a todos os clientes de forma a diminuir o tempo de exposição a ameaças.

URL Filtering

A firewall tem de garantir ainda as seguintes funcionalidades:

- Definir manualmente listas estáticas de URLs ou de IPs permitidos e não permitidos para a navegação, com a possibilidade de definir para os permitidos a ação a realizar (permitir, bloquear, permitir mas advertir, etc)
- Permitir a navegação baseando-se em categorias de URL, sendo estas categorias atualizadas periodicamente através de serviço em cloud

- Incluir listas de URLs e IPs dinâmicas relacionadas com ameaças para que possam ser bloqueadas automaticamente (listas de reputação)
- Detetar o envio de credenciais corporativas nas páginas de internet navegadas, de forma a poder advertir, bloquear ou permitir em função da categorização das páginas web
- A filtragem de URLs deve poder ser aplicada mediante diferentes perfis e deverá ser aplicada ao tráfego que sai para a Internet ou que vem da Internet
- A solução deve possuir um motor local de machine learning que seja aplicado às páginas web visitadas pelos utilizadores de forma a prevenir variantes maliciosas de javascript e acesso a páginas de phishing. Este motor deverá funcionar em tempo real e bloquear acesso a páginas que não estejam previamente categorizadas como maliciosas.

Sandboxing

A solução tem de garantir ainda as seguintes funcionalidades:

- Disponibilizar um serviço sandboxing na cloud capaz de analisar ficheiros do tipo desconhecido ou links recebidos em e-mails, de forma que se permita o envio desta informação para análise atendendo aos critérios: Tipo de aplicação utilizada para transferir o ficheiro, tipo de ficheiro que está a ser transferido, direção da transferência (download ou upload)
- Perante uma análise por parte do serviço de Sandboxing na cloud que categorize a informação enviada como maliciosa, criar assinaturas num prazo máximo de 5 minutos que possam ser utilizadas nos motores de Antivírus e URLF e que as descargas posteriores do mesmo ficheiro ou links sejam imediatamente bloqueadas (desta forma o malware desconhecido é transformado em malware conhecido automaticamente)
- Permitir consultar a informação enviada e avaliada e gerar os respetivos relatórios
- Inspeccionar protocolos como HTTP, HTTPS, SMTP, FTP, POP3 e IMAP
- Aálise de malware inteligente para analisar comportamentos do tipo "Call back" e IOC's durante a análise de malware e automaticamente criar assinaturas que permitam a prevenção de ameaças e que possam ser utilizadas pelas restantes funcionalidades da solução.
- Detetar malware direcionado a sistemas operativos de MacOS, Windows, Android e Linux
- Suportar Windows XP, Windows 7 e Windows 10 em termos de sistemas operativos Windows emulados
- Suporte para os seguintes ficheiros executáveis (EXE, DLL) e todos os tipos de ficheiros Microsoft Office, PDF, Flash, Java applets (JAR e CLASS), Android (ficheiros APK), macOS

- binaries (mach-O, DMG, PKG e application bundles) e Linux (ficheiros ELF)
- Suporte para ficheiros comprimidos (RAR, 7Zip) e conteúdo encriptado.
 - Desencriptar malware (unpacker) para utilização na análise estática e machine learning.
 - O malware cada vez mais utiliza técnicas de Anti-VM para detetar que está a ser executado num ambiente virtual e prevenir que seja detonado, escondendo o seu comportamento malicioso. A solução deve garantir a possibilidade de análise "Bare Metal", que é uma funcionalidade onde o malware é executado em host físico, o que impede que o malware utilize qualquer técnica de Anti-VM.

FUNCIONALIDADES ADICIONAIS

Deverá ser possível através de licenciamento adicional usar um módulo que disponibilize:

- **DNS Security** - serviço de proteção DNS baseado na cloud que seja capaz de bloquear acesso a domínios maliciosos conhecidos e desconhecidos
- **IOT Security** - serviço cloud de segurança para dispositivos IOT. Após a identificação dos dispositivos, a solução deve criar um padrão de comportamento para cada um e detetar automaticamente comportamentos anormais que possam sugerir que o dispositivo está comprometido. Para este tipo de eventos, devem ser gerados alertas no dashboard da solução. Deve ser possível receber estes alertas via email e sms também.
- **DLP - Data Loss Prevention** - serviço cloud que utilize supervised machine learning para identificar documentos sensíveis e atribuir-lhes uma categoria automaticamente

como por exemplo: Financeiros, Legais, Saúde, informação pessoal, etc.

- **SD-WAN** – serviço que permite escolher de forma inteligente e dinâmica os caminhos mais apropriados para envio de tráfego.

SERVIÇOS DE INSTALAÇÃO

Devem ser incluídos os serviços necessários à instalação das firewalls e sua interligação, incluindo os componentes necessários para o efeito, bem como a migração da atual configuração existente numa firewall Palo Alto 5250 cedida temporariamente pelo Governo Regional dos Açores (GRA), implementando alta disponibilidade no cluster.

Mapa de Quantidades

Descrição
Appliance de Segurança em alta disponibilidade (HA)
Máquina Virtual de Gestão centralizada para gerir até 25 Firewalls
Licenciamento, com subscrição de suporte funcionalidades por 12 meses: <ul style="list-style-type: none">● Firewall Aplicacional (Layer7), Análise de eventos e conteúdos dos ficheiros● Reporting e logs● Controlo de utilizadores● Threat Prevention: IDS/IPS / Antivírus & Anti-Malware● URL Filtering● Sandboxing e protecção zero day● Gestão Centralizada