CÂMARA MUNICIPAL DE POMBAL

DEPARTAMENTO MUNICIPAL DE FINANÇAS
DIVISÃO DE INFORMÁTICA

CADERNO DE ENCARGOS

"AQUISIÇÃO DE PLATAFORMA DE SEGURANÇA PERIFÉRICA (FIREWALL APLICACIONAL)"- PROCESSO N.º 022/AJD/SA/14"

(Ajuste Direto nos termos do Código dos Contratos Públicos, aprovado pelo Decreto-lei n.º 18/2008, de 29 de janeiro, retificado nos termos da Declaração de Retificação n.º 18-A/2008 de 28 de março, alterado e republicado pelo Decreto-Lei n.º 278/2009, de 2 de outubro, alterado pelo Decreto-Lei nº 149/2012 de 12 de junho).

Aprovado 05/05/2014

O Presidente da Câmara,

(Diogo Alves Mateus)

CADERNO DE ENCARGOS

PARTE I
Cláusulas Jurídicas

Artigo 1.º
Objeto

O presente anexo tem como objetivo definir as especificações técnicas obrigatórias a fornecer na plataforma de segurança periférica - Processo n.º 022/AJD/SA/14.

Artigo 2.º
Entidade pública contratante

A entidade pública contratante é o Município de Pombal, sito no Largo do Cardal, 3100-440 Pombal, com o número de telefone 236 210 500, endereço eletrónico sa@cm-pombal.pt e plataforma eletrónica de contratação pública com endereço www.compraspublicas.com

Artigo 3.º
Preço Base

1. Para o presente procedimento é fixado o preço base de € 11.000,00 (onze mil euros), acrescido de IVA à taxa legal em vigor, transporte incluído.

2. O preço base é o preço máximo que a entidade adjudicante se dispõe a pagar pela execução de todas as prestações do presente contrato.

3. As propostas de valor superior ao preço base fixado serão excluídas, por força da disposição da alínea d) do n.º 2, do Artigo 70.º, do C.C.P.

Artigo 4.º
Condições de Pagamento

1. O valor, referente aos serviços prestados, será pago, mediante apresentação da respetiva fatura.
2. Os pagamentos serão efetuados a 60 dias, contados da data de apresentação das faturas.

Artigo 5.º
Obrigações do adjudicatário

1. Sem prejuízo de outras obrigações previstas na legislação aplicável, no presente caderno de encargos ou nas cláusulas contratuais, da celebração do contrato decorrem para o adjudicatário, em conformidade com a absoluta subordinação aos princípios da ética profissional, isenção, independência, zelo e competência, as seguintes obrigações principais:
    a) Obrigação de entrega dos bens identificados na sua proposta;
    b) Obrigação de garantia dos bens;
    c) Obrigação de continuidade de fabrico;
    d) Obrigação de prestar e cumprir as condições fixadas para o fornecimento, nomeadamente:
        i. Obrigação de assumir a responsabilidade por eventuais danos causados nos equipamentos e outros bens existentes nas instalações do Município de Pombal, bem como quaisquer outros resultantes das atividades inerentes ao fornecimento;
        ii. Obrigação de prestar ao Município de Pombal, ou à entidade por ela designada, em qualquer tempo na pendência do fornecimento, as informações e esclarecimentos relativos ao mesmo, prestados no âmbito do contrato a celebrar, em conformidade com as cláusulas do presente caderno de encargos;
        iii. Obrigação de responsabilizar-se pelos atos praticados por todas as pessoas que no âmbito do contrato a celebrar, exerçam funções por sua conta, considerando-se para esse efeito como órgãos ou agentes do adjudicatário;
2. A título acessório, o adjudicatário fica ainda obrigado, designadamente, a recorrer a todos os meios humanos, materiais e informáticos que sejam necessários e adequados ao bom funcionamento dos equipamentos, bem como ao estabelecimento do sistema de organização necessário à perfeita e completa execução das tarefas a seu cargo.

Artigo 6.º
Conformidade e operacionalidade dos bens

1. O adjudicatário obriga-se a entregar os bens objeto do contrato com as caraterísticas, especificações e requisitos técnicos previstos no presente documento.
2. Os bens objeto do contrato devem ser entregues em perfeitas condições de serem utilizados para os fins a que se destinam e dotados de todo o material de apoio necessário à sua entrada em funcionamento.
3. É aplicável, com as necessárias adaptações, o disposto na lei que disciplina os aspetos relativos à venda de bens de consumo e das garantias a ela relativas, no que respeita à conformidade dos bens.
4. O adjudicatário é responsável perante o Município de Pombal, por qualquer defeito ou discrepância dos bens objeto do contrato que existam no momento em que os bens lhe são entregues.

Artigo 7.º
Garantia de continuidade de fabrico

O adjudicatário deve assegurar que o fabricante se compromete a garantir pelo período mínimo de 5 (cinco) anos a disponibilização de qualquer peça que permita a substituição/reparação dos bens propostos.

Artigo 8.º
Retenção sobre pagamentos

Não serão feitas retenções sobre os pagamentos, sem prejuízo do integral cumprimento do contrato.

Artigo 9.º
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 da autorização prevista no número anterior, pode o Município solicitar os documentos que lhe permitam aferir da capacidade económica e técnica do cessionário.

Artigo 10.º
Casos Fortuitos ou de Força Maior

1. Nenhuma das partes incorrerá em responsabilidade se por caso fortuito ou de força maior, designadamente greves ou outros conflitos colectivos de trabalho, for impedido de cumprir as obrigações assumidas no contrato.
2. A parte que invocar casos fortuitos ou de força maior deverá comunicar e justificar tais situações à outra parte, bem como informar o prazo previsível para restabelecer a situação.

Artigo 11.º
Patentes, Licenças e Marcas Registadas

1. São da responsabilidade do adjudicatário quaisquer encargos decorrentes da utilização, no fornecimento, de marcas registadas, patentes registadas ou licenças.
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 pagar seja a que título for.

PARTE II
Especificações Técnicas

Artigo 12.º
Bens e serviços a adquirir

Os bens a adquirir no âmbito do presente ajuste direto contempla o fornecimento de uma "appliance", montagem, configuração e formação de 3 dias no mínimo.

Artigo 13.º
Prazo

Deverão ser incluídas na proposta, os valores para utilização das funcionalidades inscritas no presente caderno de encargos para o período de um ano.

Artigo 14.º
Local de Entrega

Os bens e trabalhos objeto do contrato devem ser entregues no Município de Pombal, Largo do Cardal, 3100-440 Pombal, no prazo máximo de 30 (trinta) dias.

Artigo 15.º
Prazo de Entrega

1. A entidade fornecedora obriga-se a entregar os bens enunciados no presente caderno de encargos no prazo máximo de 30 (trinta) dias úteis, contados a partir da data da notificação de adjudicação.
2. Sem prejuízo do disposto no número anterior, o prazo de entrega poderá ser acordado entre a entidade adquirente e a entidade fornecedora.

Artigo 16.º
Funcionalidades obrigatórias

1. Componente Firewall:
    a. Stateful Inspection
    b. Suporte Clustering (Activo-Activo e Activo-Passivo)
    c. Firewall Aplicacional (Detecção em tempo real de protocolos dinâmicos) ex: FTP, SIP,H323, etc..
    d. Detecção/Bloqueio de Serviços como P2P, Instant Messaging por aplicação (voz, vídeo ou file sharing)
    e. Agrupamento de Regras
    f. NAT de Aplicações Tempo Real
    g. PAT
    h. NAT/PAT baseado em regras
    i. Permitir autenticação de serviços

j. Integração com Active Directory sem Agente no cliente e no DC
k. Integração com LDAP
l. Base de dados local de utilizadores
m. 2 factor authentication: Com tokens físicos, Soft tokens, SMS e e-mail.
n. As regras têm que permitir a ser implementadas com data de expiração ou em intervalos de tempo definidos.
o. Regras com objectos baseados na geografia
p. Identificação de utilizadores automaticamente no sistema de logs.
q. Reputação de Clientes
r. Solução tem que suportar proxy de HTTP & HTTPs
s. Criação de Regras por Utilizador ou Grupo de Utilizador
t. Utilizadores que não pertencem a rede serem confrontados com um Captive Portal para os autenticar.
u. Suporte para contas Guest com gestão independente
v. Identificação de dispositivos (incluindo Fabricante e SO)
w. Regras baseadas em dispositivos ou grupos de dispositivos
x. Endpoint Control
y. Instalação em modo Router e modo Transparente
z. Suporte de instâncias Virtuais de Firewall com gestão independente

2. Componente VPN:
   a. Suporte de IKEv1 e IKEv2
   b. Tem que suportar criptograficamente 3DES e AES-256 para IKE Phase I e II IKEv2
   c. Tem que suportar pelo menos os seguintes grupos de Diffie-Hellmas: Group 1 (768 bit), Group 2 (1024 bit), Group 5 (1536 bit), Group 14 (2048 bit)
   d. IKE Phase2 – Encriptação de Dados (DES, 3DES, AES-128, AES-192, AES-256,e NULL)
   e. IKE Phase2 - Suporte Integridade dos Dados (MD5, SHA1, SHA256, SHA384, SHA512 e NULL)
   f. Suporte de VPNs Site to Site – Full Mesh (all to all) ou Star (Remote to center)
   g. Suporte de IKE com PKI e pre-shared Secret
   h. Aprovisionamento automático de VPNs site-to-site
   i. Gestão automática de túneis IPSec de backup
   j. Suporte routing dinâmico em VPN IPSec
   k. Cliente VPN (Windows XP, MacOS, iOS, Android)
   l. Suporte de One-Time Password para VPN sem recurso a terceiros fabricantes ou servidores adicionais
   m. Criptografia (3DES, IKE, AES)
   n. Aplicação de políticas e restrições de acesso por utilizador ou por grupo de utilizadores
   o. Single Sign On VPN
   p. SSL VPN para 50 utilizadores concorrentes (mínimo)
3. Componente de Gestão:
   a. Interface de gestão em plataforma Web por HTTPS
   b. Alertas (Email, SMS, Consola, Traps SNMP)
   c. Comunicação Cliente-Servidor cifrada
   d. SNMP v2/v3
   e. Possibilidade de alta disponibilidade da componente de Gestão

   f. Os módulos de inspeção e de gestão deverão correr na mesmo equipamento físico
   g. Suporte de "Change Management" embebida
4. Funcionalidades de Logging:
   a. Logging de toda a comunicação que atravessa o firewall
   b. Logging de toda a comunicação rejeitada pelo firewall
   c. Permitir a análise de logs com programa apropriado
   d. Logging de todas as configurações alteradas no Firewall (explicitando Quem/Quando/o Quê?)
5. Componente Networking:
   a. Suporte Multiplos Links WAN - Redundância
   b. Suporte Multiplos Links WAN - Balanceamento de carga
   c. Routing baseado em políticas
   d. Rotas Estáticas
   e. IPv6
   f. 802.1q- VLAN Tagging
   g. DHCP Relay e DHCP Server
   h. Spanning-Tree (802.1d)
   i. Suporte 802.3.ad e também LACP – Agregação de Links (Activo-Activo ou Activo-Passivo)
   j. Suporte de Dead Gateway Detection
   k. Job Scheduler
   l. Suporte TOS/DiffServ
   m. Suporte para Virtual Switch
6. Componente de Networking em IPv6:
   a. Rotas estáticas
   b. RIPv6
   c. BGP4+
   d. OSPFv3
   e. DNS
   f. Endereçamento de interfaces
   g. IPv6 Tunnel sobre IPv4
   h. IPv4 tunnel sobre IPv6
   i. Packet e network sniffing
   j. NAT
   k. Troubleshooting específico IPv6
7. Protocolos de Routing:
   a. OSPF
   b. BGP
   c. RIP
   d. IGMP
   e. PIM SM
   f. PIM DM
8. Requisitos mínimos Performance:
   a. Firewall performance: >=5 Gbps
   b. VPN performance: >=1.2 Gbps
   c. Conexões Concorrentes (Firewall) >= 1,2 Milhões

d. Novas sessões por segundo (Firewall) >= 40000
e. Nº túneis IPsec VPN >= 25000
f. Nº Vlans >=1024
g. Nº conexões concurrentes em modo Next Generation FW (FW, Application Control, URL Filtering, AV) >= 20000
h. Nº de transações HTTP por segundo em modo Next Generation FW (FW, Application Control, URL Filtering, AV) >= 2700
i. Nº de utilizadores concurrentes suportados em modo Next Generation FW (FW, Application Control, URL Filtering, AV) >= 250
j. Nº de novas conexões por segundo em modo Next Generation FW (FW, Application Control, URL Filtering, AV) >= 650

9. Certificações necessárias:
   a. ICSA Labs IPSec 1.3
   b. ICSA Labs Corporate Firewall
   c. Common Criteria EAL2+ e EAL4+
   d. DoD UC APL
   e. AVA VLA.3
   f. VPN Consortium - VPNC Certified
   g. FIPS 140-2 Nível 1 e Nível 2
10. Monitorização e Reporting:
   a. Visualização em tempo real das ligações activas
   b. Capacidade de Criação reports directamente dentro da Firewall
   c. O módulo de reporting e e de correlação de eventos de segurança deverá correr no mesmo equipamento que faz a inspeção do tráfego
   d. Estatisticas da performance do hardware
   e. Gráficos de utilização por protocolo, máquina, utilizadores num determinado momento
   f. Top de ataques de segurança
   g. Top de destinos de ataques
   h. Top de origem de ataques
   i. Top Serviços
   j. Top de regras usadas
   k. Top de regras de rejeição
   l. Top de regras de aprovação
   m. Top de tráfego por serviço de rede
   n. Top de tráfego por utilizador
   o. Top de tráfego Web
11. Funcionalidade de Application Control e URL Filtering:
   a. Actualização de assinaturas automática
   b. Reconhecimento de widgets Web 2.0 >=240000
   c. Reconhecimento de aplicações >=4700
   d. Solução tem que ter categorizado >= 200 milhões URLs e ter uma cobertura de mais do que 85% da Alexa's top 1Milhão de sites
   e. Controlo por largura de banda de cada aplicação Web 2.0
   f. Inspecção SSL
   g. Criação de assinaturas personalizadas e privadas
   h. Criação de regras pelo índice de criticidade de segurança da aplicação

i. Criação de regras pelo índice de popularidade da aplicação
j. Criação de regras pela categoria da aplicação
k. Criação de regras pela tecnologia da aplicação
l. Criação de regras pelo fabricante da aplicação
m. Controlo de utilizadores dentro de uma solução de VDI ou Terminal Services
n. Inspeccionar o trafego mesmo dentro de SSL encriptado. Trafego tanto Inbound como Outbound
o. Alertar e questionar os utilizadores através de popups sobre a utilização das diferentes aplicações.

12. Componente de Antivirus:
    a. Fabricante deve ter um Anti-Virus integrado na firewall de próxima geração.
    b. O modulo de Anti -Virus deve ser administrado a partir de uma consola central.
    c. O modulo de Anti-Virus deve ter uma correlação de eventos centralizado e mecanismo de reporting.
    d. Aplicação de anti-vírus deve ser capaz de impedir o acesso a sites mal-intencionados
    e. Modulo de anti-vírus deve ser capaz de inspecionar tráfego com criptografia SSL.
    f. Anti-Virus deve ser ter atualizações em tempo real a partir de um serviço baseado na nuvem do fabricante.
    g. Anti-Virus deve ser capaz de parar a entrada de ficheiros maliciosos.
    h. Políticas anti-vírus deve ser gerido centralmente com uma política granular e eficaz.

Artigo 17.º
Estimativas de valores para anos futuros

Deverão ser apresentados os valores estimados de manutenção e de assinaturas das funcionalidades contratadas, para os três anos seguintes ao primeiro ano.

Artigo 18.º
Configurações necessárias efetuar

Deverão ser garantidas na *appliance* a instalar, todas as configurações atualmente em vigor no equipamento Cisco ASA 5500.