

# **Projeto Básico SUPSI 01378/2010**

## **Título**

### **CONSULTA PÚBLICA ELETRÔNICA para contratação de serviços de Filtro de Conteúdo Web**

## **1.0 Objeto**

Consulta Pública Eletrônica para contratação de serviços de Filtro de Conteúdo Web.

## **2.0 Especificação do Objeto a ser Contratado**

### **2.1. Serviços de Filtro de Conteúdo Web**

Os Serviços de Filtro de Conteúdo Web deverão, obrigatoriamente, apresentar as seguintes características:

#### **CARACTERÍSTICAS TÉCNICAS**

2.1.1. A solução terá que ser compatível com a estrutura atual de topologia do Serpro composta pelos seguintes equipamentos:

2.1.1.1. Brocade ServerIron;

2.1.1.2. Protocolo TCS (Transparent Cache Switching);

2.1.2. Atuar como proxy transparente através do redirecionamento de conexões utilizando TCS (Transparent Cache Switching);

2.1.3. A cada appliance da solução deverá suportar pleno funcionamento através de parâmetros definidos pelo SERPRO, baseados no equipamento Foundry Server Iron:

2.1.3.1. Peak Connect – (PeakConn) de no mínimo 45000;

2.1.3.2. Curr Connect – (CurrConn) de no mínimo 25000;

2.1.4. Possuir fonte redundante;

2.1.5. Possuir filtro de URL baseado em categorias;

2.1.6. Possuir solução anti-malware;

2.1.7. Caso não esteja na mesma máquina o fornecedor será responsável pela integração entre as aplicações e a sua funcionalidade efetiva solicitada neste edital;

#### **FUNCIONALIDADES DA SOLUÇÃO**

2.1.8. A solução deverá prover as funcionalidades de Proxy HTTP/HTTPS, Filtro de Conteúdo, Anti-Malware e Inspeção de Tráfego SSL, com capacidade de reconhecimento e tratamento destes conteúdos em quaisquer portas TCP através da análise de atributos de camada 4 a 7;

2.1.9. Deverá ser provido todo o licenciamento de software e sistemas operacionais necessários para compor todas as funcionalidades descritas para a solução, durante a vigência do contrato de 36 (trinta e seis) meses;

2.1.10. A solução de gerencia deve replicar entre si as configurações relativas as políticas de acesso definidas, ou seja, ao ser aplicada uma configuração em uma máquina, automaticamente todas os outros nós da solução deverão receber essa atualização de configuração, ficando todas as máquinas com as mesmas definições de políticas;

2.1.11. Base de URLs;

2.1.12. A solução deverá estar baseada em um banco de dados de no mínimo 20 milhões de sites com pelo menos 50 (cinquenta) categorias previamente definidas e possibilidade de criação de categorias personalizadas;

2.1.13. A solução deverá classificar os sites de acordo com o assunto, possuindo, no mínimo, as

categorias que abrangem os assuntos: pornografia, nudez, sites maliciosos, hacking, spyware, phishing, software ilegal, p2p, anonymizers, apostas, jogos, instant messaging, chat, web mail, shareware/freeware, rádio e tv, streaming, download de mídia, sites de relacionamento, armazenamento pessoal de arquivos, compartilhamento de arquivos, acesso remoto e de governo;

2.1.14. A solução deverá reconhecer URLs não cadastradas e possibilitar o envio destas ao fabricante para a devida categorização;

2.1.15. A base de dados de URLs deverá ser atualizada automaticamente pela solução via Internet, através de downloads incrementais;

2.1.16. A solução deverá permitir que qualquer site seja colocado manualmente nas categoria customizadas diferente da original de acordo com a necessidade;

2.1.17. A solução deve possuir maneira de se consultar em qual categoria determinado site está relacionado, seja via website do fabricante, ou interface local;

## **CACHING E PROXY**

2.1.18. Suportar os protocolos HTTP, HTTPS e FTP;

2.1.19. Suportar active/passive mode FTP over HTTP;

2.1.20. Possuir a possibilidade de configuração da porta ou portas utilizadas para o serviço de proxy;

2.1.21. Possuir a capacidade de utilizar o proxy com o método CONNECT para portas configuráveis;

2.1.22. Capaz de hospedar arquivos tipo PAC;

2.1.23. Possuir a capacidade de eliminar o conteúdo do cache(purge), caso tenha a funcionalidade de Cache;

2.1.24. Capacidade de criar listas de um ou mais domínios que não deverão ser processados;

2.1.25. Deve ser capaz de criar lista de destinos (Endereços IP e dominios) que poderão pular as regras de proxy e políticas;

2.1.26. Possuir a capacidade de atuar como proxy explícito e transparente;

2.1.27. Deve manter o IP de origem da conexão no pacote TCP e não somente no cabeçalho HTTP, ao se conectar com a Internet (IP SPOOFING). Assim, regras de firewall e monitoração podem ser mantidas;

2.1.28. Servidor Proxy deverá ser compatível com qualquer browser e sistema;

## **AUTENTICAÇÃO E AUTORIZAÇÃO**

2.1.29. A solução deverá permitir autenticação e autorização de usuários e grupos baseados em diretório padrão AD, LDAP (X.500) e Radius, utilizando certificados digitais X.509 e userid e password;

2.1.30. A solução deverá permitir que políticas diferentes possam ser definidas por usuários, grupos, IPs ou conjunto de IPs. Cada política poderá ter regras diferentes para liberação e bloqueio de acesso a sites e download de arquivos;

2.1.31. A solução deverá fazer a autenticação do usuário via NTLM de modo transparente, ou seja, utilizando usuário já autenticado em domínio Windows sem pedir novamente a senha para o usuário;

2.1.32. A solução deverá permitir que seja acrescentado ao cabeçalho HTTP da requisição as informações do IP do cliente e do usuário que está autenticado;

2.1.33. A solução deverá autorizar os usuários sem a necessidade de replicação da base de usuários do diretório AD e LDAP, ou seja prover o acesso Remoto a um diretório AD ou LDAP existente;

## **LIBERAÇÃO E BLOQUEIO**

2.1.34. As regras para liberação e bloqueio de acesso deverão se basear tanto na requisição quanto na resposta http;

2.1.35. A solução deverá permitir que as políticas possam, para cada categoria:

- 2.1.35.1. Permitir o acesso livremente;
- 2.1.35.2. Bloquear o acesso incondicionalmente;
- 2.1.35.3. Monitorar;
- 2.1.36. A solução deverá permitir o bloqueio do download de determinados tipos de arquivo. A filtragem deverá utilizar, obrigatoriamente, todas as seguintes formas de bloqueio de arquivo:
  - 2.1.36.1. Pela extensão do arquivo a ser recebido;
  - 2.1.36.2. Pela verificação do conteúdo dos arquivos compactados;
- 2.1.37. A solução deverá possuir um conjunto de Content-Types cadastrados e deverá ser possível o cadastramento de novos Content-Types;
- 2.1.38. A solução deverá possibilitar criação de políticas baseada em tempo (dias da semana, hora do dia, etc) para o Filtro de URL;
- 2.1.39. A solução deverá detectar, monitorar e interceptar o acesso feito às páginas abertas dentro de servidores remotos, como:
  - 2.1.39.1. Servidores de tradução;
  - 2.1.39.2. Proxies anônimos;
- 2.1.40. As transações que forem detectadas, conforme o item anterior, deverão estar de acordo com as políticas estabelecidas pela empresa, onde o conteúdo não permitido que for acessado sob este mecanismo deverá ser bloqueado e os que estiverem de acordo com as políticas, que permitem o acesso, deverão ser acessados;

## **GERAÇÃO DE LOGS E BANCO DE DADOS**

- 2.1.41. A solução deverá gerar log para todo e qualquer acesso, onde conste no mínimo: data e hora do acesso, endereço IP da estação cliente, usuário, URL de destino da requisição (site visitado), categoria do site, tamanho do objeto solicitado (em bytes) e ação tomada pela solução (bloqueado, permitido);
- 2.1.42. A solução deverá gerar dados com estatísticas de acessos internet;
- 2.1.43. O fornecedor deverá prover funcionalidade de geração de relatórios para exportação dos logs de acesso em armazenamento externo e em separado do ambiente de Filtragem de conteúdo, para Banco de Dados disponíveis no Ambiente do SERPRO;

## **CONSOLE DE MONITORAÇÃO**

- 2.1.44. A solução deverá permitir o acesso à console de monitoração, protegido por autenticação usuário/senha, sendo que o administrador deverá poder criar tais usuários;
- 2.1.45. A solução deverá possuir console de monitoração do tráfego em tempo real que mostre categorias, usuários e sites mais acessados;
- 2.1.46. As páginas de erro e de bloqueio deverão poder ser personalizadas;
- 2.1.47. Deverá ser possível exportar e importar as configurações, para backup/restore;
- 2.1.48. Se for necessária a utilização de equipamento separado para a console de configuração centralizada para todos os itens da tabela, o mesmo deverá ser fornecido bem como todas as licenças de software necessárias durante a vigência do contrato;
- 2.1.49. Possuir interface de relatórios integrada ao equipamento com informações em tempo real;
- 2.1.50. Possuir a possibilidade de exportar os dados dos relatórios para diversos tipos de arquivos;
- 2.1.51. Possuir no mínimo os seguintes relatórios:
  - 2.1.51.1. Visão do sistema (utilização e carga dos itens de hardware - CPU, memória e interfaces);
  - 2.1.51.2. Atividades do site;
  - 2.1.51.3. Detalhes do site;
  - 2.1.51.4. Atividades do usuário;
  - 2.1.51.5. Detalhes do usuário;
  - 2.1.51.6. Detalhes da categoria;
- 2.1.52. Todos relatórios são passível de conter os seguintes campos: - login/ip do usuário, nome/ip do servidor, tempo, volume de dados, hits, categoria;

- 2.1.53. A solução deve possuir ainda uma interface de geração de relatórios com informações de histórico, não necessariamente integrada ao equipamento, com as seguintes características:
  - 2.1.53.1. Deve permitir a exportação dos dados dos relatórios para diversos tipos de arquivos;
  - 2.1.53.2. Deve permitir o correlacionamento de informações, possibilitando a criação de relatórios personalizados;
- 2.1.54. A interface de relatórios de informações que não são de tempo real deve ter, no mínimo, as seguintes funcionalidades:
  - 2.1.54.1. Relatório de sites e categorias acessados (geral e por usuário);
  - 2.1.54.2. Relatório de sites bloqueados (geral e por usuário);
  - 2.1.54.3. Relatórios de malwares (geral e por usuário);
  - 2.1.54.4. Definição de um intervalo de dia e hora para os relatórios;
  - 2.1.54.5. Sites mais acessados;
  - 2.1.54.6. Usuários com mais acessos;
- 2.1.55. A atualização de todos os mecanismos de checagem deve ocorrer de forma regular e automática, efetuando o download de forma incremental;
- 2.1.56. Deverá conter em sua console, ferramenta de Trace das políticas para que o Administrador possa testar as políticas/regras antes de serem aplicadas definitivamente, ou até mesmo para Troubleshooting;
- 2.1.57. Inspeção de Tráfego SSL;
- 2.1.58. A solução deverá ser capaz de inspecionar tráfego SSL;
- 2.1.59. A solução deverá possuir a capacidade de decryptar conexões HTTPS baseado na categoria do site de destino e/ou baseado na reputação do site de destino;
- 2.1.60. O conteúdo decryptografado deve ser inspecionado pelo filtro de URL e pelo componente antimalware;
- 2.1.61. A solução deverá atuar como um entreposto (man in the midle), e deverá suportar certificados on-box, importando certificados válidos ou gerando certificados auto-assinados;
- 2.1.62. Para a inspeção do tráfego SSL, a solução deverá gerar certificados digitais para os site acessado com HTTPS. Dessa forma, fechará um túnel SSL com o cliente e outro com o servidor do site acessado;
- 2.1.63. A solução deverá checar os certificados digitais do site acessado com HTTPS. No caso de certificados digitais inválidos, a solução deverá ser configurável para, de acordo com preferência do administrador, bloquear o acesso ao site;
- 2.1.64. Para verificar a validade dos certificados digitais, a solução deverá permitir configurar quais são as Autoridades Certificadoras Raiz confiáveis;

## **ANTI-MALWARE**

- 2.1.65. A solução deverá possuir análise de arquivos para detecção e bloqueio de malware;
- 2.1.66. Para detecção de malware, a ferramenta deverá ter uma base de assinaturas de no mínimo 200 mil assinaturas de malwares conhecidos, que deverá ser atualizada automaticamente;
- 2.1.67. Deverá ser possível o bloqueio de sites com reputação má ou de categoria desconhecida;
- 2.1.68. A ferramenta deverá descompactar arquivos compactados como '.zip', '.gzip', '.tar', '.arj' e '.rar', bem como analisar seu conteúdo;
- 2.1.69. Se a detecção de malware não for feita no mesmo equipamento fornecido para filtro de conteúdo, a contratante deverá fornecer os appliances (conjunto de hardware e software de mesmo fabricante) para compor a solução, observando-se os requisitos de alta disponibilidade;
- 2.1.70. O mecanismo de verificação de malware deve reconhecer códigos maliciosos pelo menos nas seguintes ameaças:
  - 2.1.70.1. Adware;
  - 2.1.70.2. Phishing;
  - 2.1.70.3. Tracking cookies;
  - 2.1.70.4. Session hijackers;
  - 2.1.70.5. Rootkits;

#### 2.1.70.6. Keyloggers.

### 2.2. Do prazo e locais da prestação dos serviços

2.2.1. Os serviços deverão ser iniciados, em sua totalidade, nas localidades indicadas, em até 30 (trinta) dias úteis contados a partir da data de assinatura do contrato.

#### 2.2.2. Locais de Prestação dos Serviços e CNPJs:

<b>Regional Brasília (DF)</b> Endereço: SGAN - Av. L2 Norte, Quadra 601 - Módulo G - Brasília/DF - CEP: 70830-900 CNPJ: 33.683.111/0002-80
<b>Regional Rio de Janeiro – Horto (RJ)</b> Endereço: Rua Pacheco Leão, nº 1235 - Jardim Botânico - Rio de Janeiro/RJ - CEP: 22460-905 CNPJ: 33.683.111/0008-75
<b>Regional São Paulo – Socorro (SP)</b> Endereço: Rua Olívia Guedes Penteado, 941 - Socorro - São Paulo/SP - CEP: 04766-900 CNPJ: 33.683.111/0009-56

2.2.3. O recebimento e aceite será realizado em até 10 (dez) dias úteis em função da conformidade da vistoria dos serviços em funcionamento.

### 3.0 Níveis de Serviço

3.1. A CONTRATADA deverá atender aos chamados para manutenção corretiva, 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, e substituir quaisquer módulos defeituosos nos equipamentos, nas localidades contempladas;

3.2. O prazo de atendimento estipulado para qualquer uma das localidades é de 02 (duas) horas. Este prazo contempla o atendimento, identificação e solução do problema;

3.3. A substituição dos recursos defeituosos, quando necessária, deverá ocorrer em até 8 (oito) horas;

3.4. A CONTRATADA deverá fornecer canal de suporte on-line 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, durante o contrato de manutenção.

3.5. A CONTRATADA deverá disponibilizar uma Central de Atendimento Telefônico 0800 (gratuita) para registro de abertura de chamados técnicos e controle de atendimento por todo o período do contrato. O atendimento deverá ser efetuado no idioma português.

3.6. O não atendimento dentro dos prazos estabelecidos para os chamados de Severidade Alta ensejará aplicação de multa à CONTRATADA no valor equivalente a 1,0% (um por cento) do valor do contrato, por hora ou fração de hora de atraso.

### 4.0 Especificação de Valores

Não se aplica

### 5.0 Justificativa da Contratação

Não se aplica

## **6.0 Seleção do Contratado**

Não se aplica

## **7.0 Justificativa para Aceitação de Preços**

Não se aplica

## **8.0 Gerenciamento do Contrato**

8.1. O processo será acompanhado pelos empregados Giovanni Ferreira, telefone (61) 2021-7513, endereço eletrônico giovanni.ferreira@serpro.gov.br, e Fernando Marques, telefone (61) 2021-8382, endereço eletrônico fernando.marques@serpro.gov.br, lotados na SUPSI, e Fernando Lima, telefone (61) 2021-9098, endereço eletrônico fernando.lima@serpro.gov.br, lotado na SUPOP.

8.2. A LICITANTE com a proposta de menor preço deverá apresentar documentação técnica do fabricante dos equipamentos comprovando o atendimento a todos os requisitos do edital contidos no anexo de Especificação Técnica correspondente, nas seguintes condições:

8.2.1. Documentação técnica fornecida pelo fabricante. Nessa documentação, a LICITANTE deve fornecer uma planilha ponto a ponto indicando documento e página onde consta o cumprimento de cada um dos requisitos das especificações técnicas.

8.2.2. Cada documento apresentado deve descrever claramente a referência ao modelo apresentado na proposta, não sendo válidas referências genéricas.

8.2.3. Será aceita Carta do Fabricante, como comprovação de atendimento de requisitos técnicos e de compatibilidade especificados neste edital, apenas para os itens que não constarem na documentação da maioria dos fabricantes ou que não puderem ser mensurados.

8.2.4. Relação de componentes, incluindo módulos, fontes e acessórios, de cada equipamento, contendo o código do produto (fabricante) e as respectivas quantidades em cada item.

8.2.5. Caso a documentação apresentada deixe de comprovar o atendimento de um único item da especificação técnica a proposta será desclassificada, não passando para a etapa seguinte de testes das funcionalidades especificadas.

8.3. A proposta comercial a ser apresentada pela CONTRATADA deverá discriminar os valores dos equipamentos ofertados, bem como dos seus acessórios.

8.4. A CONTRATADA deverá garantir a atualização dos micro-códigos, firmwares, drivers e softwares instalados, provendo o fornecimento de novas versões por necessidade de correção de problemas ou por implementação de novos releases, a partir do aceite pelo SERPRO, durante todo o período de contrato.

### **8.5. Das obrigações das partes**

#### **8.5.1. Da empresa contratada**

8.5.1.1. Entregar e garantir o perfeito funcionamento dos serviços nos prazos estipulados neste instrumento.

8.5.1.2. Comunicar ao SERPRO, com a antecedência necessária, eventuais falhas, atrasos ou fatos relevantes que possam inviabilizar o cumprimento dos prazos estabelecidos, ou que acarretem a necessidade de prorrogação de prazos.

#### **8.5.2. Do SERPRO**

8.5.2.1. Recusar, com a devida justificativa, qualquer material ou serviço prestado fora das especificações, bem como qualquer documento ou Nota Fiscal, apresentado em desacordo com as condições estabelecidas no Contrato a ser firmado.

8.5.2.2. Substituir em caso de necessidade os Termos de Recebimento, de Instalação, de Aceitação e Laudo de Funcionamento Definitivo, por Notas Técnicas acompanhados de explanação dos motivos da substituição.

8.5.2.3. O SERPRO se reserva o direito a qualquer momento de realizar diligências junto à CONTRATADA e aos fabricantes dos equipamentos para esclarecimento de dúvidas.

## **8.6. Recebimento e Aceitação**

8.6.1. O recebimento dos serviços, de caracterização provisória, será realizado pelo Responsável Técnico Operacional, nomeado para este processo nas localidades contempladas, mediante a emissão de Termo de Recebimento Serviços.

8.6.2. A aceitação dos serviços, de caracterização definitiva, será realizada pelas Comissões de Recebimento e Aceitação das Regionais (CORACs) que atuam sobre as localidades contempladas, instituídas pelas Decisões Setoriais vigentes, lavrando-se a Ata de Aceitação de Serviços.

## **8.7. Da instalação**

8.7.1. Deverá ser agendada uma reunião inicial entre a CONTRATADA e o SERPRO, em até 5 (cinco) dias úteis após a assinatura do contrato, para definição do escopo inicial dos trabalhos de instalação e configuração, e a CONTRATADA deverá entregar um plano de trabalho, com cronograma de instalação e configuração dos equipamentos, o qual deverá ser aceito previamente pelo corpo técnico do SERPRO.

## **8.8. Da capacitação técnica**

8.8.1. A CONTRATADA deverá realizar a capacitação técnica de 8 (oito) profissionais do SERPRO, a serem indicados, abrangendo todos os itens ofertados, em: instalação e operação, configuração básica, configuração de gerência e segurança, contemplando todas funcionalidades solicitadas nas especificações técnicas dos itens;

8.8.2. A capacitação deverá possuir carga horária mínima de 40 (quarenta) horas e deverá ocorrer em período integral;

8.8.3. A capacitação deverá ser realizada utilizando conteúdo teórico e prático, através de laboratório preparado com equipamentos equivalentes aos ofertados, onde estarão disponíveis as mesmas funcionalidades solicitadas nas especificações técnicas dos itens;

8.8.4. A CONTRATADA deverá prover toda a logística e todo o material necessário à execução da capacitação teórica e prática, ou seja, instalações adequadas, equipamentos, manuais e apostilas didáticas. Os manuais e apostilas fornecidos devem ser originais e oficiais do fabricante;

8.8.5. A capacitação deverá ser ministrada por profissionais certificados e credenciados pelo fabricante ou empresa credenciada para tal finalidade;

8.8.6. A capacitação técnica deverá ter início em até 30 (trinta) dias após a assinatura do contrato, podendo ser adiada por conveniência do SERPRO, quando então, em comum acordo com a CONTRATADA, será marcada a data definitiva;

8.8.7. A capacitação deverá ser realizada em Brasília-DF, e os custos de deslocamento dos profissionais do SERPRO selecionados para a capacitação técnica, quando existirem, será de responsabilidade do SERPRO.

8.9. A gestão do contrato será exercida pela Coordenação de Gestão de Contratos (COOGC).

## **9.0 Considerações Gerais**

9.1. O objeto da presente contratação está caracterizado como bens ou serviços de informática ou automação, conforme definição constante no Art. 16-A da Lei nº 8.248, de 23 de outubro de 1991.

9.2. Em atendimento ao estabelecido no Decreto Nº 5.450, de 31 de maio de 2005, por se tratar de bens comuns e ter os padrões de desempenho e qualidade objetivamente definidos, através de especificações usuais de mercado, a contratação deverá ser na Modalidade de Pregão na forma eletrônica e registro de preços.

9.3. O pregão deverá ocorrer por lote único. O fornecedor deverá apresentar a proposta com valor unitário, e será vencedora a proposta de menor preço global.

9.4. A vigência do contrato será de 36 (trinta e seis) meses.