GOVERNO DO ESTADO DO ESPÍRITO SANTO
SECRETARIA DE ESTADO DA FAZENDA
COMISSÃO DE LICITAÇÃO DO PROFAZ

PREGÃO ELETRÔNICO Nº 011/2017

AQUISIÇÃO DE TI - CLUSTER DE FIREWALL NEXTGEN

País: BRASIL

Nome do Projeto: PLANO DE DESENVOLVIMENTO DA ADMINISTRAÇÃO FAZENDÁRIA DO ESTADO DO ESPÍRITO SANTO – PROFAZ/ES

Nº do empréstimo: Contrato de Empréstimo nº 2245-OC/BR

Objeto: AQUISIÇÃO DE TI - CLUSTER DE FIREWALL NEXTGEN

REF.: Esclarecimentos às Empresas

Prezados Senhores,

Apresentamos a seguir os questionamentos apresentados pelas empresas interessadas, que se manifestaram durante o período de 18/08/2017 a 25/08/2017, em que edital foi tornado público, e respostas correspondentes. Os questionamentos foram transcritos literalmente, omitindo-se apenas a identificação da empresa que submeteu o pedido de esclarecimento.

A Secretaria de Estado da Fazenda agradece a todas as empresas que demonstraram interesse em fornecer o objeto a ser licitado.

Atenciosamente,

RICARDO ISHIMURA
Pregoeiro CPL-PROFAZ

Esclarecimento n° 01 –
1.5 Especificações de Desempenho e funcionalidades:

l. Não será aceito a comprovação de Throughput para funcionalidades de camada 7 (Controle de Aplicação e IPS, por exemplo), com tráfego UDP e RFCs baseadas neste protocolo;

>> Será aceito que usamos a metodologia do NSS Labs?

Sim, contanto que o documento dos testes do NSSLABS sejam do produto ofertado e realizado na metodologia versão 7, a mais recente, e com perfil de mix voltado ao Financial. Solicitamos que o documento do NSSLABS seja oficial e que venha descrito na metodologia as funcionalidades de camada 7, features a assinaturas testadas conforme item 1.5.

b. Suportar a análise de arquivos maliciosos em ambiente controlado com, no mínimo, sistema operacional Windows XP, Windows 7 (32 bits) e Windows 7 (64 bits);

>> Não temos mais Windows XP no FSA Cloud. O Windows XP já se encontra em End of Support total pela MS, não faz sentido utilizar uma versão de SO totalmente não suportada pelo fabricante. Esse item caracteriza favorecimento.

Sim, o Windows XP pode ser removido.

j***. Caso a solução seja fornecida em appliance local, deve possuir, no mínimo, 12 ambientes controlados (sandbox) independentes para execução simultânea de arquivos suspeitos;***

>> Questionar sobre a aplicabilidade/relevância do item, visto que a solução da PANW na nuvem só tem 3 ambientes, a nossa possui 4 e da CHKP 4. Sendo que PANW não tem Sandbox local, na minha opinião este item apenas favorece a Palo Alto, dificultando todos os outros.

Questionamento irrelevante, pois se trata de ambiente em appliance local, não se pode comparar ambiente local com nuvem.

f. Deve suportar autenticação via Kerberos para administradores da plataforma de segurança, Captive Portal e usuário de VPN SSL;

>> Não atendemos. A SEFAZ ES possui Kerberos no ambiente? caso não tenham, não faz sentido pedir este item, pois restringe a participação de outros fabricantes e caracteriza favorecimento de um fornecedor.

Iremos aceitar sem autenticação Kerberos.

2.1 Aquisição de serviços de suporte e garantia, conforme especificações abaixo:

a. O proponente e o fabricante devem oferecer suporte técnico em língua portuguesa através de ligação telefônica gratuita do tipo 0800, que deve estar disponível no regime de 24 a 7 a 365 (24 horas por dia, 7 dias na semana e 365 dias no ano);

>> A língua oficial do TAC é inglês e não temos gente 24x7 para atender o telefone em PT-BR. Questionar o cliente. Fornece o suporte 24x7 através do Parceiro no Brasil e não pelo Fabricante, será aceito?

Sim, contanto que parceiro obedeça os itens solicitados no edital.

Esclarecimento n° 02

. **Questionamento referente ao subitem "*b. Possuir suporte a implementação e compatibilidade a IPV6 em método de pilha dupla, bem como a ICMPv6 (RFC4890) de forma a permitir a criação de políticas baseadas no ICMP Type.*", do item "*1.5 Especificações de Desempenho e funcionalidades:*"**

Entendemos que a solução ofertada deverá possuir funcionalidades de dual stack (IPv4 e IPv6) e estar compliance com a RFC 4443, pois o mesmo descreve o funcionamento do ICMPv6 (Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification).
Está correto o nosso entendimento?

Sim.

2. **Questionamento referente ao item "*c. Deve suportar o recebimento eventos de autenticação de controladoras wireless, dispositivos 802.1x e soluções NAC via syslog, para a identificação de endereços IP e usuários;*".**

Entendemos que a solução deverá suportar autenticação LDAP para Active Directory que as demais maneiras de autenticação poderá ser realizado através de Captive Portal (Browser-Based Authentication) para os usuários que não estiverem no domínio.
Está correto o nosso entendimento?

Sim.

3. **Questionamento referente ao item "*l. Suportar a análise de arquivos executáveis, DLLs, ZIP e criptografados em SSL no ambiente controlado;*", do item "*1.9 Análise de malwares modernos*".**

Entendemos que o termo DLL também inclui os arquivos Microsoft Excel XLL (DLL based).
Está correto o nosso entendimento?

Deve atender conforme especificação técnica do edital.

4. **Questionamento referente ao item "*f. Deve suportar autenticação via Kerberos para administradores da plataforma de segurança, Captive Portal e usuário de VPN SSL*."**

Entendemos que a solução deverá suportar autenticação para administradores via Kerberos sob TACACS e/ou RADIUS Externo.
Está correto nosso entendimento?

Iremos aceitar sem autenticação Kerberos.

5. **Questionamento referente ao subitem "iv. AES 128, 192 e 256 (Advanced Encryption Standard)", do item "1.14 VPN**".

Entendemos que se a solução ofertada possuir o menor (AES 128) e o maior (AES 256) valor requisitado é o suficiente para atendimento completo do subitem "iv. AES 128, 192 e 256 (Advanced Encryption Standard)", do item "1.14 VPN".
Está correto o nosso entendimento?

Sim.

6. **Questionamento referente ao subitem "*a. Ferramenta de gerenciamento centralizado de firewall, armazenamento de logs e relatórios do mesmo fabricante dos equipamentos adquiridos nesse edital, que permitam gerencia dos appliances de froma centralizada, analise do trafego e identificação de possíveis ataques maliciosos, internos ou externos, com as seguintes características:*" do item "*1.2 Aquisição de solução de gerencia, relatórios e armazenamento de logs, conforme especificações técnicas abaixo*."**

Entendemos que a solução de gerenciamento centralizado de firewall poderá ser tanto em appliance físico quanto em appliance virtual compatível com hypervisor VMware.
Está correto o nosso entendimento?

Sim.

7. **Questionamento referente ao subitem "*a. Ferramenta de gerenciamento centralizado de firewall, armazenamento de logs e relatórios do mesmo fabricante dos equipamentos adquiridos nesse edital, que permitam gerencia dos appliances de froma centralizada, analise do trafego e identificação de possíveis ataques maliciosos, internos ou externos, com as seguintes características:*" do item "*b. Capacidade de armazenamento mínimo de log de 2TB, sendo no mínimo 10GB por dia;*

A solução ofertada em appliance virtual não possui limitadores de capacidade total de armazenamento de log e armazenamento diário em sua forma de licenciamento. A capacidade de armazenamento de logs está atrelado ao provisionamento que o administrador da solução irá disponibilizar de recursos computacionais para o appliance virtual.
Está correto o nosso entendimento que o órgão licitante fornecerá os recursos computacionais virtuais (vCPU, memória e disco) suficientes para utilização da solução de gerência?

Sim, a ferramenta precisa estar licenciada para a volumetria solicitada.

8. **Questionamento referente ao subitem "*a. Ferramenta de gerenciamento centralizado de firewall, armazenamento de logs e relatórios do mesmo fabricante dos equipamentos adquiridos nesse edital, que permitam gerencia dos appliances de froma centralizada, analise do trafego e identificação de possíveis ataques maliciosos, internos ou externos, com as seguintes características:*" do item "*g. Deve vir com ao menos 20 relatórios prontos para utilização;*"**

A solução ofertada possui por padrão 17 (dezessete) relatórios pré-configurados, porém entendemos que para atingir quantidade total solicitada no item, os demais templates de relatórios poderão ser feitos previamente antes da fase de implantação da solução.
Está correto o nosso entendimento?

Sim.

9. **Questionamento referente ao subitem "*a. O proponente e o fabricante devem oferecer suporte técnico em língua portuguesa através de ligação telefônica gratuita do tipo 0800, que deve estar disponível no regime de 24 a 7 a 365 (24 horas por dia, 7 dias na semana e 365 dias no ano);*" do item "2. LOTE 1 – ITEM 2 – AQUISIÇÃO DE SERVIÇOS DE SUPORTE E GARANTIA."**

Entendemos que a responsabilidade de acionamentos e interações com o fabricante da solução será de responsabilidade da proponente.
Está correto o nosso entendimento?

Sim.

10. **Questionamento referente ao item: "a. "Throughput de, no mínimo, 3 Gbps com as seguintes funcionalidades habilitadas simultaneamente e com assinaturas recomendadas pelo fabricante, caso o fabricante não possua um documento de melhores práticas, será considerada todas as assinaturas/proteções atuantes: Firewall, IPS, Controle de Aplicação, Antivírus, Sandboxing e Proteção contra Ameaças Avançadas;"**

Solicitamos a alteração da performance dos firewalls, de acordo com o seguinte texto: "Throughput de, no mínimo, 2,5 Gbps com as seguintes funcionalidades habilitadas simultaneamente e com assinaturas recomendadas pelo fabricante, caso o fabricante não possua um documento de melhores práticas, será considerada todas as assinaturas/proteções atuantes: Firewall, IPS, Controle de Aplicação, Antivírus, Sandboxing e Proteção contra Ameaças Avançadas;"

Deve atender conforme especificação técnica do edital.

11. Sugestões de alterações dos seguintes itens:

Texto Original:
j. Uma vez que a solução ofertada tenha sido atualizada na forma do item I, não será permitida mais nenhuma atualização adicional durante a execução de todo o Teste de Bancada.

Texto Novo:
j. Uma vez que a solução ofertada tenha sido atualizada na forma do item I, caso haja necessidade de atualização adicional durante a execução do Teste de Bancada, todos os itens deverão ser revalidados.

As alterações deverão ser realizadas na fase de configuração do equipamento, após o início da comprovação por teste de bancada, não será aceito atualização adicional.

Texto Original:
l. O teste de bancada irá aferir o desempenho dos equipamentos como as funcionalidades que fazem uso de assinaturas, habilitadas para todas as assinaturas que a plataforma de segurança possuir, bem como amostra de todos os recursos solicitados;

Texto Novo:
l. O teste de bancada irá aferir o desempenho dos equipamentos como as funcionalidades que fazem uso de assinaturas, com as assinaturas recomendadas pelo fabricante ativadas, caso o fabricante não possua um documento de melhores práticas, será considerada todas as assinaturas/proteções ativadas;

Sim.

Texto Original:
xiii. A amostra deve ser configurada de forma a registrar todos os acessos autorizados ou bloqueados, bem como todas as aplicações e ameaças detectadas pelo Firewall.

Texto Novo:
xiii. A amostra deve ser configurada de forma a registrar todos os acessos autorizados e bloqueados, início e fim de sessão, bem como todas as aplicações e ameaças detectadas pelo Firewall.

Sim.

Texto Original:
xiv. A amostra deve ser submetida ao seguinte padrão de tráfego de dados, similar ao encontrado nos links de internet da Secretaria de Estado da Fazenda do Espírito Santo:
1. (a) HTTP = 20% (conteúdo variável com imagens e textos, tamanho variável de 100bytes a 500kbytes)
2. (b) HTTPS – a ser decriptografado e inspecionado = 50% (conteúdo variável com imagens e textos, tamanho variável de 100bytes a 500kbytes)
3. (c) RTP UDP = 5% (distribuição de tamanho: 56% 64bytes, 17% 512bytes e 27% 1518bytes)
4. (d) VPN = 10% (IPSec, conteúdo variável com imagens e textos, tamanho variável de 100bytes a 500kbytes)
5. (e) Email = 5% (POP, SMTP e IMAP com conteúdo variável, incluindo arquivos anexos)
6. (f) Ameaças = 5% (A serem previamente definidas pela Surep a partir das informações fornecidas conforme o item i deste capítulo)
7. (g) Aplicações = 5% (A serem previamente definidas pela Surep a partir das informações fornecidas conforme o item i deste capítulo)

Texto Novo:
xiv. A amostra deve ser submetida ao seguinte padrão de tráfego de dados, similar ao encontrado nos links de internet da Secretaria de Estado da Fazenda do Espírito Santo:
1. (a) HTTP = 60% (conteúdo variável com imagens e textos, tamanho variável de 20Kbytes a 700kbytes)
2. (b) HTTPS – a ser decifrado e inspecionado = 10% (conteúdo variável com imagens e textos, tamanho variável de 10Kbytes a 100kbytes)
3. (c) EMAIL = 10% (SMTP e POP3 com conteúdo variável, incluindo arquivos anexos)
4. (d) DNS = 5% (DNS Query)
5. (e) Outros Protocolos = 5% (Telnet, RDP, FTP, etc)
6. (f) Ameaças = 5% (A serem previamente definidas pela Surep a partir das informações fornecidas conforme o item i deste capítulo)
7. (g) Aplicações = 5% (A serem previamente definidas pela Surep a partir das informações fornecidas conforme o item i deste capítulo)

No mínimo 30% de HTTPS

Texto Original:
xix. A amostra deverá ser inicialmente submetida a uma taxa de transferência de 1Gbps (um gigabit por segundo), durante 30 (trinta) minutos, com o objetivo de coleta de parâmetros que serão utilizados para verificação da performance do equipamento.

Texto Novo:
xix. A amostra deverá ser inicialmente submetida a uma taxa de transferência de 1Gbps (um gigabit por segundo), durante 30 (trinta) minutos, podendo ser divido em 3 (três) amostras de 10 (dez) minutos, com o objetivo de coleta de parâmetros que serão utilizados para verificação da performance do equipamento.

Sim.

Texto Original:
xx. A amostra será então submetida a uma taxa de transferência de 3Gbps (três gigabits por segundo), durante 30 (trinta) minutos, e não poderá apresentar prejuízo em sua performance.

Texto Novo:
xx. A amostra será então submetida a uma taxa de transferência de 2,5Gbps (dois vírgula cinco gigabits por segundo), durante 30 (trinta) minutos, podendo ser divido em 3 (três) amostras de 10 (dez) minutos e não poderá apresentar prejuízo em sua performance.

Deve atender conforme especificação técnica do edital.

Sugestões de Adição:

Após o item k.
ITEM1: O ambiente físico, bem como elétrico, para os testes de bancada serão disponibilizados pela licitante.

Sim

ITEM2: A infraestrutura e o acesso à internet serão disponibilizados pela licitante.

Sim

ITEM3: Apenas para fins de comprovação de throughput, não haverá necessidade de configuração em modo cluster.

Sim