Resposta a Pedido de Esclarecimento

QUESTIONAMENTOS:

1.3.9.5. e 2.3.12. - Deve implementar balanceamento de link:
1.3.9.5.2. e 2.3.12.3. - Através de políticas por usuário e grupos de usuário do LDAP/AD;
O Balanceamento é realizado por Redes ou Grupos de IP, por esse processo ser baseado no módulo de Rede, o mesmo não trata a autenticação nessa fase.
Para melhorar a ampla concorrência solicitamos a retirada do ítem.
RESPOSTA: a solução deve permitir identificar o usuário ou grupo e aplicar uma regra de balanceamento do link baseado no perfil de autenticação. A avaliação efetuada previamente identificou que diversos fabricantes atendem essa demanda, portanto, não será aceita a solicitação de retirada do item;

1.8.1. e 2.8.1. - Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via ldap, active directory, e-directory e base de dados local; Atendemos parcialmente este item. Não suportamos Novell E-directory (muito antigo).
Qual a real necessidade de suportar esse método de autenticação, o mesmo existe na infraestrutura do DETIC-RO?
Para casos como esse normalmmente é utilizado o suporte ao protocolo LDAPv3, esse não seria o suficiente para atender essa necessidade?
Para melhorar a ampla concorrência solicitamos a retirada do ítem.
RESPOSTA: serão aceitos equipamentos que não suportem o serviço de diretório e-directory, tendo em vista ser bastante antigo, porém os demais se mantém obrigatórios;

1.9.2. e 2.9.2. - Suportar a criação de políticas de QoS por:
1.9.2.2. e 2.9.2.2. - Por usuário e grupo do LDAP/AD.
Esse item se torna retundante pois o mesmo já é especificado no 1.5.1.13.
Não trabalhamos com política de QoS por usuário/grupo de LDAP/AD.
Trabalhamos apenas o "traffic shaping" por usuário/grupo de LDAP/AD. Conforme descrito no item 1.5.1.13. -"Limitar a banda (download/upload) usada por aplicações (traffic shaping), baseado no IP de origem, usuários e grupos do LDAP/AD;"
Ou seja, atendemos este item se considerarmos novamente o "traffic shaping" como uma política de QoS. Não deixa de ser, porém, como já informei, há um item tratando exclusivamente disso.
Para melhorar a ampla concorrência solicitamos a retirada do ítem.
RESPOSTA: a solução ofertada deve ser capaz de criar políticas de QoS (qualidade de serviço) baseadas no usuário ou grupo por questões de segurança interna. A avaliação efetuada previamente identificou que diversos fabricantes atendem essa demanda, portanto, não será aceita a solicitação de retirada do item;

1.9.5. e 2.9.5. - Suportar marcação de pacotes Diffserv, inclusive por aplicação;
Entendemos que a marcação de pacotes deve ser via porta/services, ou seja, para qualquer outro controle a nivel de aplicação, entendemos que serão aceitas soluções que possuem engines de traffic shapping. Está correto entendimento?
RESPOSTA: não está correto o entendimento. A solução deve suportar a marcação Diffserv porporta, protocolo e aplicação.O item visa atender a necessidade de efetuar a marcação do pacote com as opções do Diffserv nas aplicações que trafegam no ambiente de informática;

1.10.3. e 2.10.3. - Deve permitir visualizar nos logs e criar políticas para liberar e bloquear tráfego de países por: tipo de arquivo, aplicação e categoria de URL;
Para maior participação da concorrência, entendemos que serão aceitas as empresas que possuirem a solução que permite a liberação e bloqueio de acesso por paises. Está correto o entendimento?
RESPOSTA: SIM.

1.11.4.5. e 2.11.4.5. - AES 128, 192 e 256 (Advanced Encryption Standard);
Para permitir a participação de outros fabricantes, entendemos que será aceita a solução que apresentar o menor e maior valor do tipo de encriptografia. Está correto o entendimento?
RESPOSTA: não está correto o entendimento. O item deve ser atendido integralmente, pois o tamanho da chave (key) com mais de uma opção (128, 192 e 256) garante a interoperabilidade com os outros parceiros que precisam estabelecer o túnel VPN, além de garantir a segurança com o tamanho de chave variável;

1.12.1. - O gerenciamento da solução deve suportar acesso via SSH, WEB (HTTPS);
2.12.1. - O gerenciamento da solução deve suportar acesso via SSH, WEB (HTTPS) e API aberta;
Para permitir a participação de outros fabricantes, entendemos que será aceita a solução que possui console de gerencia do próprio fabricante. Está correto o entendimento?
RESPOSTA: não está correto o entendimento, os itens devem ser atendidos integralmente. Atualmente aplicações do tipo cliente/servidor que são proprietárias dificultam o acesso a gerência da solução. Interfaces do tipo WEB são muito mais fáceis de acessar e não precisam que sejam instaladas no desktop do usuário. Qualquer browser pode acessar o Firewall inclusive de terminais móveis;

1.12.3. e 2.12.3. - Caso haja a necessidade de instalação de cliente para administração da solução o mesmo deve ser compatível com sistemas operacionais Windows e Linux;
Atendemos parcialmente este item (Windows). Sendo os Sistemas Linux/Unix muito abrangentes, no momento não temos solução homologada para esses Sistemas.
Para melhorar a ampla concorrência solicitamos adequação ou a retirada do ítem.

RESPOSTA: será obrigatória a compatibilidade com sistema operacional Windows OU Linux;

1.12.11. e 2.12.12. - Autenticação integrada ao Microsoft Active Directory e servidor Radius;
Seguindo premissas de Melhores Práticas de Segurança, não suportamos a integração ao AD para autenticação à console de gerência e monitoração. Essa autenticação é suportada através de servidor Radius.
Para melhorar a ampla concorrência solicitamos adequação ou a retirada do ítem.
RESPOSTA: s itens não serão alterados e o atendimento deve ser integral, pois toda a base de usuários atualmente está concentrada em servidores Windows, portanto a integração com a Microsoft Active Directory é de extrema importância;

2.2.2.1. 3 Gbps com a funcionalidade de controle de aplicação habilitada para todas as assinaturas que o fabricante possuir;
Normalmente essa solicitação vem atrelada à uma quantidade mínima de assinaturas, exemplo se um determinado Firewall tem 40.000 assinaturas e outro apenas 10.000, o Firewall com menor quantidade de assinaturas é beneficiado.
O item em questão acaba beneficiando fabricantes que possuem baixo número de assinaturas, ou seja, tornando fabricantes de grande nome do mercado de segurança e referenciados pelo Garnet e NSS LABS não atenderem o edital por ter 3 a 4 vezes mais assinaturas que outros fabricantes, sendo assim, tornaria alguns fabricantes mais baratos e outros mais caros.
Também vale ressaltar que esse tipo de item torna a competição desleal uma vez que beneficiaria apenas algumas empresas e outras ficariam de fora.
Para melhorar a ampla concorrência solicitamos adequação ou a retirada do ítem.
2.2.2.2. 2 Gbps com as seguintes funcionalidades habilitadas simultaneamente para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: controle de aplicação IPS, Antivírus e Antispyware. Caso o fabricante divulgue múltiplos números de desempenho para qualquer uma destas funcionalidades, somente o de menor valor será aceito;
Normalmente essa solicitação vem atrelada à uma quantidade mínima de assinaturas, exemplo se um determinado Firewall tem 40.000 assinaturas e outro apenas 10.000, o Firewall com menor quantidade de assinaturas é beneficiado.
O item em questão acaba beneficiando fabricantes que possuem baixo numero de assinaturas, ou seja, tornando fabricantes de grande nome do mercado de segurança e referenciados pelo Garnet e NSS LABS não atenderem o edital por ter 3 a 4 vezes mais assinaturas que outros fabricantes, sendo assim, tornaria alguns fabricantes mais baratos e outros mais caros.
Também vale ressaltar que esse tipo de item torna a competição desleal uma vez que beneficiaria apenas algumas empresas e outras ficariam de fora.
Para melhorar a ampla concorrência solicitamos adequação ou a retirada do ítem.
RESPOSTA: quando definimos o número de assinaturas ocorrem outros questionamentos, pois todos os fabricantes que possuem números menores se consideram prejudicados e alegam

que as especificações estão privilegiando apenas alguns. Serão aceitos equipamentos que atendam a velocidade descrita no edital considerando os controles e análises ali descritas, levando-se em conta a efetiva aferição da funcionalidade. Assim sendo, não causando prejuízos à ampla disputa do processo licitatório;

2.2.4. Possuir ao menos 21 interfaces de rede nas seguintes quantidades mínimas:
2.2.4.3. 04 (quatro) interfaces de rede 40 Gbps SFP+;
De acordo com a solicitação do Throughput nos itens 2.2.2.1 e 2.2.2.2 percebe-se que o equipamento solicitado é de pequeno para médio porte, porém o volume de interfaces fisicas incluindo 04 interfaces de 40Gb SFP+, deixa algumas duvidas se realmente o throughput solicitado nos itens 2.2.2.1 e 2.2.2.2 não estão incorrentos ou se a composição das interfaces não estão corretas.
Quase todos os fabricantes de mercado que possuem o volume de interfaces solicitados no item 2.2.4 e o tipo de interface conforme item 2.2.4.3, trata se de equipamentos de grande porte onde faz no minimo 10Gbps de throughput com as funcionalidades de Next Generation Firewall + Antivirus, anti-malware e IPS. Especificamente nesse caso, a referência deixa em dúvida em como se chegou ao Throughput informado, ou se realmente existe a necessidade das interfaces de 40Gbps, pois com a inserção da mesma o Custo de um equipamento para atender a demanda é quase o dobro de um equipamento de menor porte que atenderia ao Throughput informado.
Por isso solicitamos a Correção do Throughput ou a retirada do item 2.2.4.3, referente às 04 interfaces de 40Gbps.
RESPOSTA: os itens não serão alterados e o atendimento deve ser integral, a solução ora adquirida será conectada em um barramento com conexão de interfaces de 40 Gbps, portanto, será necessário que o produto ofertado possua interface com velocidade de 40 Gbps;