

Senhores,

A seguir, respostas aos questionamentos referentes ao **Pregão Presencial nº 01/15**:

Questionamento 1:

1.1.10.23. Suportar QoS com as seguintes funcionalidades: **garantia e reserva de banda**, limite de utilização de banda, prioridade de tráfego e DSCP(Differentiated Services Code Point);

Q: As funcionalidades de garantia e reserva de banda precisam ser atendidas por um device que ofereça suporte a CBWFQ (Class-Based weighted fair queueing), e essas funcionalidades são comuns apenas em roteadores. Normalmente essa funcionalidade é utilizada em rede privada (MPLS) que ofereçam suporte a QOS. Caso haja real necessidade de utilização do CBWFQ, poderá ser atendida pelos roteadores posicionados à frente do firewall. As funcionalidades de limite de utilização de banda (traffic-shapping) e priorização de tráfego (Priority-Queueing) são atendidas nos equipamentos propostos. Podemos tratar desta forma?

Resposta:

Os termos "garantia e reserva de banda" e "limite de utilização de banda" referem-se unicamente à capacidade de definir, no equipamento, a largura mínima garantida ou máxima ofertada de banda em função do tipo de tráfego identificado por regras.

Questionamento 2:

1.1.10.42. Permitir a limitação do número de conexões incompletas("half- open") por IP origem ou por IP destino;

Q: Sessões TCP half-open devem ser tratadas de forma global, pois conexões neste tipo de estado podem sugerir tentativas de SYN Flood e outros métodos de DDoS. Há algum motivo específico para filtro baseado em ip/origem e ip/destino, já que sessões embrionárias ou half-open precisam ter o mesmo tipo de controle e tratativa?

Resposta:

A funcionalidade é exigida para permitir a mitigação de ataques SYNFLOOD originados ou destinados a alvos específicos.

Questionamento 3:

1.1.10.43. Permitir a inspeção dos protocolos DNS, FTP, HTTP, HTTPS, IMAP, IMAPS, SMTP, SSH, NetBIOS, SMB, SMB2, Microsoft RPC, POP3, POP3S, SIP e TFTP;

Q: As tratativas de filtros para os protocolos NetBios, SMB2, Microsoft RPC e TFTP poderão ser realizadas em camada 4 (Filtro TCP/UDP). Podemos tratar desta forma?

Resposta:

Sim, pode ser tratado desta forma.

Questionamento 4:

1.2.1.4. Suportar a criação de túneis IPSEC com criptografia AES-128, AES-256, 3DES, **AES-GCM-128 e AES-GCM-256**;

Q: Atualmente oferecemos suporte para o padrão 3DES, AES-128 e AES-256, que são suportados em todas as soluções de segurança de mercado, e que oferecem o mesmo nível de criptografia do padrão AES-GCM. Há alguma aplicação ou cenário específico que demande o padrão AES-GCM? Podemos substituí-los por padrão 3DES ou AES-128 ou AES-256?

Resposta:

Não. Nenhum dos padrões exigidos poderá ser substituído. A exigência dos padrões criptográficos listados no item 1.2.1.4 objetiva manter o equipamento atualizado com as mais novas normas de segurança e oferecer o maior desempenho, com base no descrito na RFC 5288 (<https://tools.ietf.org/html/rfc5288>).

Questionamento 5:

1.2.1.7. Suportar os seguintes algoritmos criptográficos: AES-XCBC-MAC, MD5, SHA-1, SHA-2-256 e SHA-2-512;

Q: O algoritmo AES-XCBC é um padrão pouco utilizado para hash na grande maioria das soluções de segurança (128bits). Suporte apenas em Checkpoint segundo pesquisa. Há alguma infraestrutura que atualmente demande este tipo de algoritmo hash? Caso negativo, aconselhamos a utilização SHA-2 256 ou 512.

Resposta:

Sim. Os algoritmos criptográficos são exigidos para manter compatibilidade com os padrões suportados pelos sistemas Linux e PFSense utilizados em nossa infraestrutura. Assim, será mantida a exigência por todos os algoritmos criptográficos solicitados no edital.

Questionamento 6:

1.2.1.8. Suportar o estabelecimento de túneis VPN IPSEC através dos seguintes sistemas operacionais: Windows Vista, Windows 7 (32 e 64 bits), Windows 8(32 e 64-bits) e superiores, Mac OS 10.6(32 e 64-bits) e superiores;

Q: Considerando que o Windows Vista terá seu suporte pela Microsoft interrompido em breve, sendo que os usuários serão obrigados a instalar um sistema mais atual, favor eliminar essa exigência do edital.

Resposta:

A exigência não será retirada, já que ainda possuímos computadores com o sistema operacional Windows Vista que terão acesso à VPN.

Atenciosamente,

**Seção de Licitações
Tribunal de Contas do Estado de São Paulo**