ITEM 1 - Aquisição de solução SWG – Secure Web Gateway

Análise da Documentação Técnica ATA Comércio e Serviços

Proposta comercial não detalha hardware e software

ITEM 1 – DESEMPENHO, CAPACIDADE E ALTA DISPONIBILIDADE:

1.

a –

Página corrigida para a 2816 onde trata-se de proxy de http e https. Atende

Página 209 fala de filtro de conteúdo com o Fortiguard, categorização de sites e aplicativos. Atende

Pagina 2742 fala de topologia de web caching. Atende.

Página 183 fala de estatística de ATP services e não da funcionalidade de ATP, é preciso explicitar a função. Atende

Página 117 faz referência a uma configuração de ssl inspection. Atende

Monitoramento de layer 4. Atende

b – Proposta comercial não traz garantia de continuidade do serviço de proxy. Não atende, precisamos de comprovação do que foi adquirido na proposta comercial, ou seja todo o licenciamento dos equipamentos que estarão compondo a proposta.

c – OK.

d – OK.

e – OK.

f – OK

g – OK.

h – OK.

i -OK.

j – OK.

k – OK.

l – OK.

m – OK.

n – "Possuir quantidade de memória e capacidade de processamento necessários ao seu funcionamento pleno com todas as funcionalidades descritas nesta especificação e com desempenho adequado".

O documento apesar de dizer que suporta até 8000 usuários concorrentes não explicita qual o desempenho da solução com as políticas e filtros habilitados no equipamento, logo o documento apresentado não é suficiente para comprovação. Não atende.

ITEM 2 – GERENCIAMENTO

a – OK

b – OK

c – OK

d – OK

e – OK

f – OK

g – OK

h – OK

i – OK

ITEM 3 – CONTROLE DE APLICAÇÕES

a – OK

b – "Suportar os protocolos HTTP, HTTPS e FTP, em seus modos ativo e passivo;"
Encontrado na documentação explicação sobre suporte a FTP nos modos passivo e ativo, utilizando session-helper, mas não para os protocolos HTTP e HTTPS. Não atende.

ITEM 4 – FILTRO DE ACESSO

a – OK.

b – OK

c – "A solução deve atuar como "man in the middle", intermediando e repassando todas as requisições. Deve suportar certificados on-box, importando certificados validos ou gerando auto-assinados. Deve permitir a emissão de páginas amigáveis e customizáveis de erro também aos sites criptografados."
Certificados – OK
"Man in the middle" - Não encontrado em documentação oficial fornecida a funcionalidade de "man in the middle" para trafego com filtro de acesso, ou seja, política de controle de acesso à internet, o que está sendo proposto na página 2798 do documento é offloading de ssl para wan opt, que trata de feature de caching na wan e não de de-criptografia de tráfego https. Não atende
Páginas amigáveis e customizáveis de erro também aos sites criptografados – não foi encontrado na página 7 referência a criação e/ou edição de páginas amigáveis e customizáveis para sites criptografados.

d – OK.

e – OK

f – "Deve possuir mecanismo de classificação em tempo real dos sites visitados ou sistema de filtro de reputação que permita estabelecer uma reputação para cada endereço IP dos servidores de destino. A rede de reputação não deve somente ser baseada em informações de fluxo da própria base de appliances instalados, mas sim em correlações entre outros parâmetros: Listas negras de URL, listas Brancas de URL, listas de equipamentos comprometidos, volume global de trafego, histórico dos sites, dados de categorização de URLs e web crawlers."
O mesmo documento na página 3 mostra um infográfico das categorias de acesso do produto e nós acreditamos que categorias "Unrated"(Não classificada), "Unknow"(desconhecida) para filtro de URL e "All other know applications"(Todas as outras aplicações conhecidas) e "All other unknow applications"(Todas as outras aplicações desconhecidas) para filtro de aplicações não são categorias válidas, o produto deve possuir inteligência para, ao analisar o conteúdo do site e/ou aplicação, já o categorizar corretamente. Não atende.

g – OK.

h – OK.

ITEM 5 – FILTRO DE ACESSO
a – "Deve possuir mecanismo que gere alertas via e-mail quando há uma tentativa excessiva a um site bloqueado. Este alerta será disparado quando atingido o número de tentativas bloqueadas previamente pelo administrador para cada categoria."
Encontrado em documentação oficial fornecida a funcionalidade de envio de e-mail, todavia, como mostra a documentação em http://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-system-administration-54/Monitoring/Alert%20email.htm, não é possível, no exemplo citado, configurar que sejam enviados logs de IPS após 10 logs, por exemplo. Não atende.

ITEM 6 – MANIPULAÇÃO DE SITES
a – OK.

ITEM 7 – RELATÓRIOS
a – OK.

b – OK.

c – "Deve emitir relatórios do tipo Top 10 Usuário/Categorias/Url, Top Usuários Bloqueados."
Documento citado para defesa é de um equipamento chamado FortiAnalyzer, no documento de Ponto a Ponto enviado pelo proponente, o mesmo coloca na composição um cluster de Fortigate 300D e um FortiManager-VM, assim como na composição não há Analyzer não podemos aceitar defesa utilizando documentação do mesmo. Não atende.

d – "Deve emitir relatórios por tipo da ameaça."
Documento citado para defesa é de um equipamento chamado FortiAnalyzer, no documento de Ponto a Ponto enviado pelo proponente, o mesmo coloca na composição um cluster de Fortigate 300D e um FortiManager-VM, assim como na composição não há Analyzer não podemos aceitar defesa utilizando documentação do mesmo. Não atende.

e – "Deve exibir relatórios de atividades do usuário onde a, saibamos quais os sites/categorias acessados,

Ponto enviado pelo proponente, o mesmo coloca na composição um cluster de Fortigate 300D e um FortiManager-VM, assim como na composição não há Analyzer não podemos aceitar defesa utilizando documentação do mesmo. Não atende.

f – "...produzindo documentos de múltiplos níveis"

Documento citado para defesa é de um equipamento chamado FortiAnalyzer, no documento de Ponto a Ponto enviado pelo proponente, o mesmo coloca na composição um cluster de Fortigate 300D e um FortiManager-VM, assim como na composição não há Analyzer não podemos aceitar defesa utilizando documentação do mesmo. Não atende.

g – OK.