

Ao

CGU - CONTROLADORIA GERAL DA UNIÃO

EDITAL DE LICITAÇÃO CGU Nº 15/2021 - PROCESSO Nº 00190.105856/2020-32

Ilustríssimo (a) Senhor (a) Pregoeiro (a).

FAST HELP INFORMÁTICA LTDA., pessoa jurídica de direito privado, inscrita no CNPJ/MF sob o nº 05.889.039/0001-25, com sede no SIA TRECHO 03 LOTE 990 ED. ITAÚ, CEP 71.200-030, Brasília/DF, já qualificada nos autos, vem tempestivamente à presença de V. Sa., nos termos do art. 4º, XVIII da Lei nº 10.520/2002, art. 26 do Decreto 5.450/2005 e demais cominações legais aplicadas de forma subsidiária, contidas na Lei 8.666/93, a seguir doravante designada somente como FASTHELP, ora RECORRENTE, apresentar:

1. DOS FATOS

Contra a decisão que determinou a classificação da empresa Add Value Participações, Comercio e Serviços de Informática, designada somente como Add Value, ora RECORRIDA, no Pregão Eletrônico nº 56/2021, e, ato contínuo, habilitou e a declarou vencedora do certame, inscrita no CNPJ sob o número 10.864.910/0001-76, pelas razões de fato e de direito, a seguir aduzidas:

A CONTROLADORIA GERAL DA UNIÃO, deflagrou procedimento licitatório, modalidade Pregão Eletrônico, por meio de Sistema de Registro de Preços (SRP), tipo menor preço Global por grupo, para a aquisição do licenciamento de direito de uso permanente de 4 (quatro) Appliances virtuais de Application Delivery Controllers (ADC), com Direito de Atualização e Suporte Técnico pelo período de 60 (sessenta) meses, para os ambientes On-Premises e Cloud da Controladoria-Geral da União – CGU, e serviços de implantação e Repasse de Conhecimento, para atender às necessidades do CGU, de acordo com as especificações e quantitativo, que constam no Edital e seus anexos.

Em 25 de novembro de 2021, às 09:00 horas, aberta a sessão pública, após a fase de lances, a empresa Add Value sagrou-se arrematante do certame com o menor lance ofertado de R\$ 649.600,00, após a desclassificação da empresa WY Tecnologia LTDA por não atendimento de itens técnicos do edital.

A empresa Add Value ofertou o produto Citrix ADC VPX 3000 MB Premium Edition do Fabricante CITRIX, produto este que não atende integralmente a todos os itens solicitados no Termo de Referência, bem tais como não atende como produto aos quais o Edital exige, com itens e

subitens aos quais não serão atendidas pelo produto da fabricante CITRIX, este incluso na proposta comercial ofertada pela empresa ora RECORRIDA.

Foi registrada no Sistema *Comprasnet*, dentro de forma tempestiva, a seguinte intenção de recurso pela RECORRENTE:

“Prezado Sr. Pregoeiro, fazendo uso do direito expresso no art. 44 do Decreto nº 10.024/2019, vimos manifestar nossa intenção de recurso contra a habilitação da empresa AddValue Participações, Comercio e Serviços de Informática tendo em vista o não cumprimento dos itens de habilitação e a comprovação técnica dos itens 1.3.8.3, 1.3.8.4, 1.4.5, 1.4.17.1, e outros, conforme comprovaremos nas razões recursais.”

2. DAS RAZÕES

2.1 DA REALIZAÇÃO DE DILIGÊNCIAS

Em 10 de dezembro de 2021, a Recorrida, obteve o resultado positivo no pregão, após apresentar respostas a diligência a itens técnicos do edital.

Houve equívoco e contradição quanto ao aceite da proposta da licitante Add Value, baseando-se numa inconformidade das respostas aos itens técnicos diligenciados e a demais itens aos quais não são atendidos pelo produto Citrix ADC VPX 3000 MB ofertado.

A observância do princípio da vinculação ao edital de licitação é medida que se impõe, interpretado este como um todo, de forma sistemática. Desta maneira, os requisitos estabelecidos nas regras editalícia devem ser cumpridos fielmente, sob pena de inabilitação do concorrente

O ato feriu o direito líquido e certo da RECORRENTE, conforme demonstraremos a seguir.

3. DO NÃO ATENDIMENTO AOS ITENS DO EDITAL PELA RECORRIDA

Imperioso ressaltar que o tratamento ao qual foi dado a empresa Add Value em sua diligência, cuja proposta mesmo sem comprovar o atendimento a diversos dos itens do edital através respostas incompletas ou que não respondiam aos itens do edital com como solicitados, fica claro que a RECORRIDA não atende a diversos destes itens diligenciados, e que está ainda assim teve a proposta aprovada.

A decisão contra a qual a proposta da empresa Add Value, declarada vencedora da licitação por meio do pregão eletrônico Nº 15/2021, qual seja, o objeto de aquisição do licenciamento de direito de uso permanente de 4 (quatro) Appliances virtuais de Application Delivery Controllers

(ADC), com Direito de Atualização e Suporte Técnico pelo período de 60 (sessenta) meses, para os ambientes On-Premises e Cloud da Controladoria-Geral da União – CGU, e serviços de implantação e Repasse de Conhecimento, por meio de Sistema de Registro de Preços (SRP).

Os fundamentos que indicaram a necessidade de reforma da decisão da RECORRIDA são basicamente de cunho técnico e se dirigem à demonstração de que o produto ofertado pela Add Value não atende às especificações técnicas do edital de licitação, bem como a documentação apresentada foi em desacordo com o exigido no edital.

O princípio da vinculação ao instrumento convocatório obriga a Administração e o licitante a observarem as regras e condições previamente estabelecidas no edital.

É importante salientar que ofereceremos a explicação do não atendimento de cada um dos itens ao separar as explicações por tópicos, vide texto abaixo:

Passemos aos argumentos.

1.3.8 Deverá possuir estatísticas em tempo real das aplicações via interface WEB e console bem como também deve responder a consultas SNMP (snmp query) pelo menos para os seguintes parâmetros:

1.3.8.7 Quantidade de conexões SSL, Transações SSL por segundo (SSL TPS) ou Conexões SSL por segundo (SSL CPS)

O item 1.3.8 e seu subitem 1.3.8.7, deixa claro a necessidade do produto ofertado informar na Interface WEB ou interface de console (CLI) as estatísticas de quantidade de conexões SSL, transações por segundo ou conexões SSL por segundo, isso também deve ser suportado utilizando o protocolo SNMP. Na documentação enviada na proposta inicial da empresa Add Value, foi informado a comprovação somente via SNMP, com um documento genérico e que não deixava nem um pouco claro o atendimento do item. Conforme imagem abaixo:

1.3.8.7 Quantidade e de conexões SSL, Transações SSL por segundo (SSL TPS) ou Conexões SSL por segundo (SSL CPS)	https://docs.citrix.com/en-us/citrix-adc/current-release/system/snmp/configuring-snmpv1-snmpv2-queries.html	Página Única Link Direto	
	https://docs.citrix.com/en-us/citrix-adc/current-release/system/snmp/configuring-snmpv3-queries.html		

Após serem diligenciados pela competente equipe técnica da CGU, foi respondido pela Add Value com links que mencionam maneiras de coletar tais estatísticas via linha de comando (console CLI). Conforme a seguir:

g) 1.3.8.7 - Quantidade de conexões SSL, Transações SSL por segundo (SSL TPS) ou Conexões SSL por segundo (SSL CPS);	No ADC podemos consultar as estatísticas de SSL através referenciando-se abaixo: https://developer-docs.citrix.com/projects/citrix-adc-configuration-ssl-vserver https://docs.citrix.com/en-us/citrix-adc/current-release/providers/NS_TCP_optimization/ns_tcp_opt_realtime_statistics
--	--

Percebe-se que na resposta, em nenhum momento houve menção que comprova a possibilidade da solução da Citrix apresentar as estatísticas solicitadas via interface Web. Isso é uma falha grave, já que as soluções de ADC são ponto fundamental na utilização do protocolo SSL em qualquer ambiente. Nesse caso, como o administrador da solução de ADC/WAF poderia tomar decisões cruciais ou verificar o status do ambiente de ADC via interface WEB da Citrix? De fato, tal falha deixa nítido o desacordo com o edital, devendo resultar na desclassificação da proposta.

1.4.5 Deve suportar, no mínimo, 1000 VLANs;

Item solicita que o produto deve suportar no mínimo 1000 VLANs. Apesar da recorrida enviar um link que a fabricante Citrix permite 4,096 entidades de VLANs, é claro considerar que se pode habilitar as Tags nesse range de IDs, porém fica claro que o produto não suporta habilitar essa quantidade de quantitativo de VLANs ao mesmo tempo, conforme link: <https://support.citrix.com/article/CTX217458>.

Ao verificar o texto deste link retirado do próprio sítio do Fabricante, nota-se a limitação do quantitativo de 64 VLANs, conforme imagem abaixo:

Solution

CAUSE 1

- Changing allowed VLANs on the SVM for the VPX interface to "any number-" should resolve the issue.
- There were 69 VLAN in total on the VPX.
- Customer was able to bind 64 of them to interface 10/1 on the VPX but getting the following error message when binding more VLANs:
 - "Maximum number of tagged VLANs bound to the interface exceeded or the binding of this VLAN is not allowed on the interface"
- Issue could not be because of article: CTX200925 because XS version is 6.5 in our case and this issue described in this article affects only version 6.0.
- SVM -> Instances -> Edit -> Data Interfaces -> Edit Interface -> VLANs is blank.
- By default we can only bind 64 VLAN's at max unless we specify the VLAN list on SVM.
 - Put 2-4095 under VLANs and then try again.

Diante dessa evidente limitação, como a CGU poderia habilitar o quantitativo de 1000 VLANs solicitadas? É muito seguro afirmar que a solução ofertada pela recorrida não atende todo o certame.

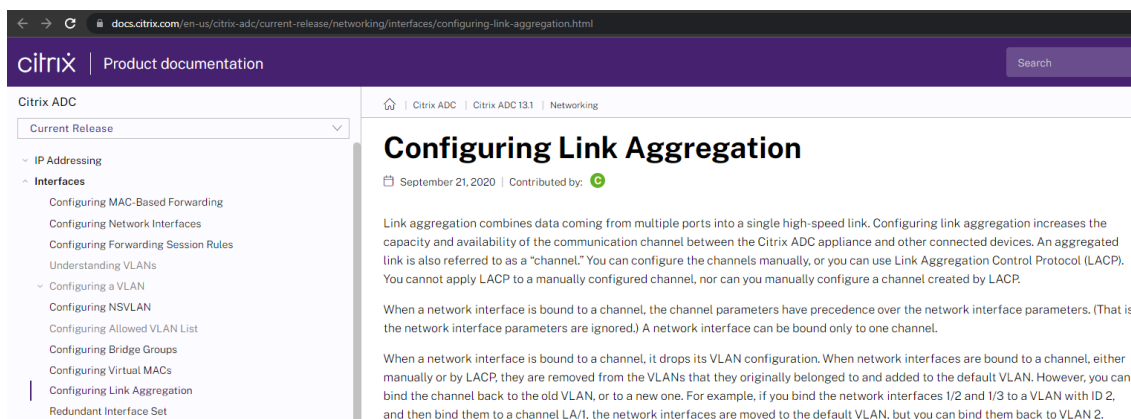
1.5.5 Deve implementar funcionalidade de proteção contra ataques tipo defacement;

É correto afirmar que ataques de defacement aos portais das organizações é algo corriqueiro e que as soluções de Firewall de Aplicações Web devem ser aptas a proteger contra esses tipos de

ataques. No entanto, a empresa Add Value não demonstrou a comprovação de que a solução da fabricante Citrix possui tal capacidade, vejamos a tentativa de comprovação:

1.5.5 Deve implementar funcionalidade de proteção contra ataques de tipo defacement;	https://docs.citrix.com/en-us/citrix-adc/current-release/networking/interfaces/configuring-link-aggregation.html	Página Única Link Direto	
--	---	--------------------------	--

O link enviado pela recorrida trata da capacidade de agregar interfaces de rede para prover alta disponibilidade de interconexão do appliance físico com o switch. Ora, isso nem se quer diz respeito a uma funcionalidade de segurança. Vejamos com mais detalhes o conteúdo do link:



The screenshot shows a web browser displaying the Citrix ADC documentation page for 'Configuring Link Aggregation'. The page title is 'Configuring Link Aggregation' and it was last updated on September 21, 2020. The content explains that link aggregation combines data from multiple ports into a single high-speed link. It also notes that LACP cannot be applied to manually configured channels. The page includes sections on channel parameters and VLAN configuration when interfaces are bound to a channel.

Diante dessa evidente irregularidade em atender uma funcionalidade tão importante solicitada, a recorrida não deve ser considerada como habilitada.

1.5.6 Deve implementar, no mínimo, os seguintes mecanismos de proteção contra ataques (lista retirada no documento OWASP top 10, disponível no sítio Web: <https://owasp.org/www-project-top-ten/>, em agosto de 2021):

A1:2017-Injection

A2:2017-Broken Authentication

A3:2017-Sensitive Data Exposure

A4:2017-XML External Entities (XXE)

A5:2017-Broken Access Control

A6:2017-Security Misconfiguration

A7:2017-Cross-Site Scripting XSS

A8:2017-Insecure Deserialization

A9:2017-Using Components with Known Vulnerabilities A10:2017-Insufficient Logging & Monitoring

O item é bastante enfático sobre a necessidade de proteção para cada categoria de ataque retirada do documento OWASP top 10. Ocorre que, a empresa Add Value inseriu na comprovação ponto a ponto (incluído na proposta) o link genérico de introdução ao Citrix Web Application Firewall, conforme tela a seguir:



<p>1.5.6 Deve implementar, no mínimo, os seguintes mecanismos de proteção contra ataques (lista retirada no documento OWASP top 10, disponível no sitio Web: https://owasp.org/www-project-top-ten/, em agosto de 2021):</p> <ul style="list-style-type: none"> A1:2017-Injection A2:2017-Broken Authentication A3:2017-Sensitive Data Exposure A4:2017-XML External Entities (XXE) A5:2017-Broken Access Control A6:2017-Security Misconfiguration A7:2017-Cross-Site Scripting XSS A8:2017-Insecure Deserialization A9:2017-Using Components with Known Vulnerabilities A10:2017-Insufficient Logging & Monitoring 	<p>https://docs.citrix.com/en-us/citrix-adc/current-release/application-firewall/introduction-to-citrix-web-app-firewall.html</p>	<p>Página Única Link Direto</p>	
---	--	---------------------------------	--

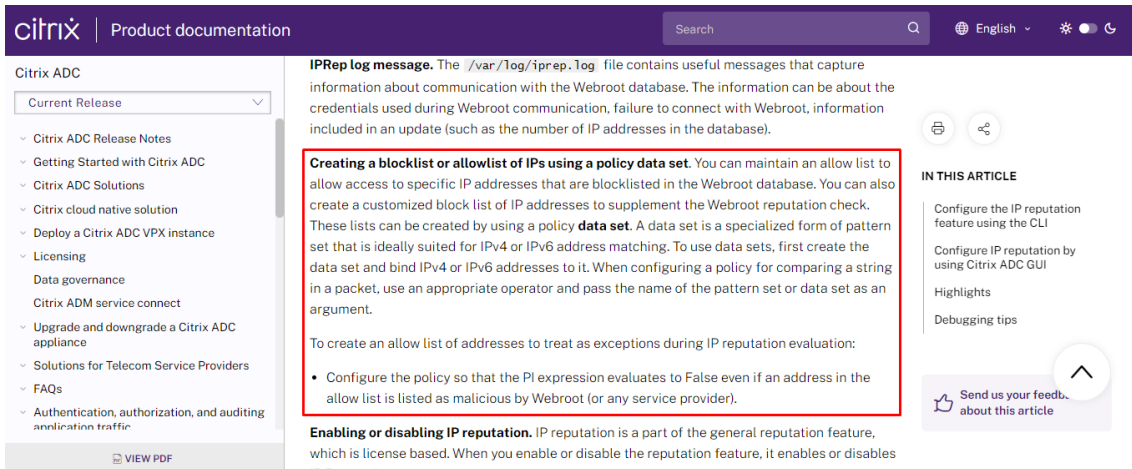
Ao abrir o link (<https://docs.citrix.com/en-us/citrix-adc/current-release/application-firewall/introduction-to-citrix-web-app-firewall.html>) da comprovação enviada pela recorrida, não existe a menção do termo OWASP top 10 no texto. É importante frisar que o item cita cada uma das técnicas que devem ser protegidas e a solução deve proteger cada um deles. Tal falta de proteção é algo muito grave e que pode comprometer a segurança do ambiente de aplicações Web da Controladoria Geral da União.

1.5.9 A solução deve permitir incluir, automaticamente, em blacklist os endereços IPs que repetidamente falharem a desafios no browser. Ao entrar em Blacklist o sistema automaticamente bloqueia os pacotes enviados por esse endereço por um período de tempo.

Com relação ao item 1.5.9, é facilmente entendível a necessidade da solução ofertada de suportar a funcionalidade de criação automática de blacklist de IPs para os pacotes oriundos de conexões que falham em desafios no browser. Esses pacotes devem ser bloqueados por um período de tempo. Ocorre que, na planilha de comprovação ponto a ponto, a empresa Add Value apresentou de reputação de IP, conforme abaixo:

<p>1.5.9 A solução deve permitir incluir, automaticamente, em blacklist os endereços IPs que repetidamente falharem a desafios no browser. Ao entrar em Blacklist o sistema automaticamente bloqueia os pacotes enviados por esse endereço por um período de tempo</p>	<p>https://docs.citrix.com/en-us/citrix-adc/current-release/reputation/ip-reputation.html#:~:text=Creating%20a%20blocklist%20or%20allowlist%20of%20IPs%20using%20a%20policy%20data%20set</p>	<p>Página Única Link Direto</p>	<p>Creating a blocklist or allowlist of IPs using a policy data set</p>

Foi mencionado que a sessão “Creating a blocklist or allowlist of IPs using a policy data set” contém as informações de comprovação. Ao analisar o texto da documentação:



The screenshot shows the Citrix Product documentation interface. The main content area is titled "IPRep log message" and describes the `/var/log/iprep.log` file. A red box highlights a section titled "Creating a blocklist or allowlist of IPs using a policy data set," which explains how to create a customized block list of IP addresses to supplement the Webroot reputation check. The text states that these lists can be created by using a policy data set, which is a specialized form of pattern set. It also mentions that to use data sets, one must first create the data set and bind IPv4 or IPv6 addresses to it. A bullet point indicates that the policy should be configured so that the IP expression evaluates to False even if an address in the allow list is listed as malicious by Webroot. Below this, there is a section for "Enabling or disabling IP reputation."

Ao analisar atentamente a documentação apresentada, essa função de criar blocklist ou allowlist de IPs via “policy data set” é uma forma “manual” para o administrador complementar a funcionalidade de reputação de IP da Webroot, criando listas próprias de permissão ou bloqueios de IP, senão vejamos:

*“You can also create a customized block list of IP addresses to supplement the Webroot reputation check. These lists can be created by using a policy **data set**. A data set is a specialized form of pattern set that is ideally suited for IPv4 or IPv6 address matching. To use data sets, first create the data set and bind IPv4 or IPv6 addresses to it.”*

Como se pode notar, em nenhum momento, comprova-se a possibilidade de criação automática de blacklists de IPs que falharam repetidas vezes o desafio do Browser das aplicações que porventura, fossem publicadas através da solução da Citrix. Diante disso, conclui-se mais uma vez que a proposta da empresa Add Value está em desacordo com as especificações do edital.

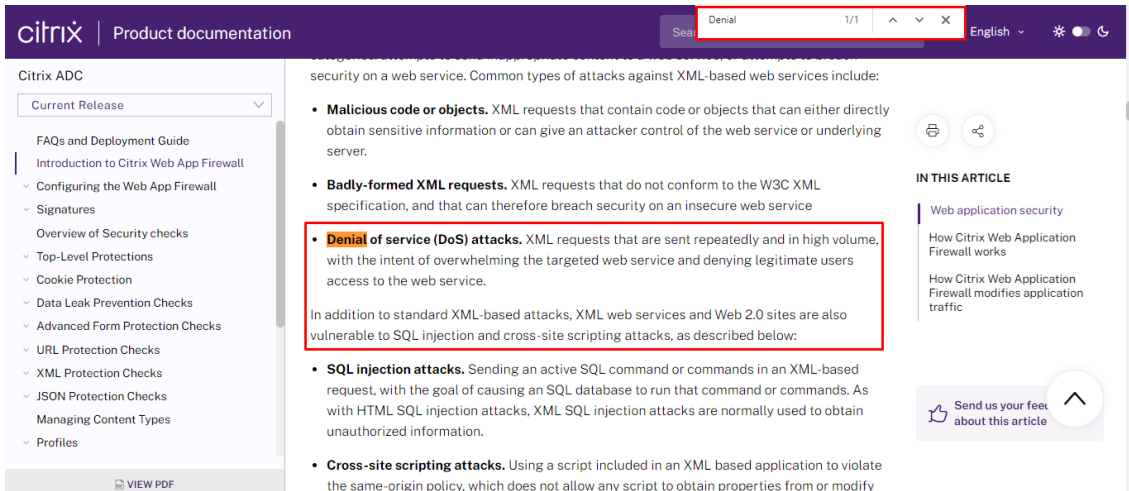
1.5.14 O equipamento oferecido deverá possuir as seguintes formas de detecção de ataques DoS na camada de aplicação.

1.5.14.1 Número de requisições por segundo enviados a uma URL específica

Mais uma vez, temos um item que não está atendido pela proposta da Add Value. Como se pode notar, o item 1.5.14 e seu subitem 1.5.14.1, solicitam que a solução ofertada tenha a proteção de DoS – Denied of Service, na camada de aplicação. Além disso, para esse tipo de funcionalidade, deve-se usar o método de detectar essa modalidade de ataques por requisições por segundo enviados a uma URL específica. Em sua proposta, a empresa Add Value apresentou a seguinte comprovação:

<p>1.5.14 O equipamento oferecido deverá possuir as seguintes formas de detecção de ataques DoS na camada de aplicação</p>	<p>https://docs.citrix.com/en-us/citrix-adc/current-release/application-firewall/introduction-to-citrix-web-app-firewall.html</p>	<p>Página Única Link Direto</p>	
<p>1.5.14.1 Número de requisições por segundo enviados a uma URL específica</p>	<p>https://docs.citrix.com/en-us/citrix-adc/current-release/application-firewall/introduction-to-citrix-web-app-firewall.html</p>	<p>Página Única Link Direto</p>	

Ao procurar a informação contida no link que comprovaria o correto atendimento do item, percebe-se que a documentação oficial da solução Citrix ADC, menciona somente uma vez o termo Denial of Service. Adicionalmente, a fabricante cita que a proteção de Denial of Service do produto está restrito a requisições XML e não detalha como funcionaria essa proteção.



The screenshot shows the Citrix Product documentation website. A search bar at the top contains the word "Denial". The search results list several articles related to XML-based attacks. One article, titled "Denial of service (DoS) attacks", is highlighted with a red box. The text of this article states: "XML requests that are sent repeatedly and in high volume, with the intent of overwhelming the targeted web service and denying legitimate users access to the web service." Other articles listed include "Malicious code or objects", "Badly-formed XML requests", "SQL injection attacks", and "Cross-site scripting attacks".

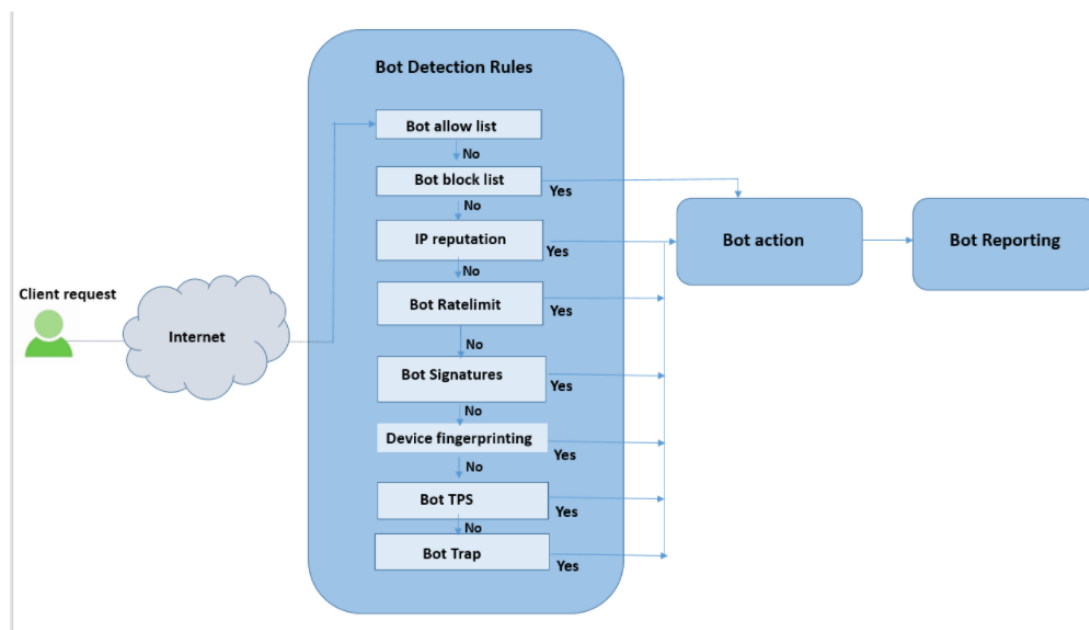
Como pode-se perceber, em nenhum momento da documentação enviada pela Add Value, menciona a possibilidade de detecção de ataque de DOS por meio de quantidade de conexões por segundo em uma URL específica. Portanto, frisa-se que o item não é atendido e conclui-se que é uma clara evidência para que a recorrida seja desclassificada.

1.5.14.3 Detecção através de código executado no cliente com o objetivo de detectar interação humana ou comportamento de robôs (bots)

Ainda com relação ao item 1.5.14, agora sobre o subitem 1.5.14.3, é exigido que a solução de WAF detecte o comportamento de robô ao utilizar a técnica de injeção de código no cliente (navegador). A recorrida apresentou os seguintes links como comprovação:

1.5.14.3 Detecção através de código executado no cliente com o objetivo de detectar interação humana ou comportamento de robôs (bots)	https://docs.citrix.com/en-us/citrix-adc/current-release/bot-management.html https://docs.citrix.com/en-us/citrix-adc/current-release/bot-management/bot-detection.html	Página Única Link Direto	
---	--	--------------------------	--

Ocorre que, em nenhum dos links enviados, comprovam a proteção contra Bots pela técnica de código executado no cliente, somente pelas seguintes regras pulicadas pela fabricante Citrix:



É evidente a não disponibilidade de utilizar a citada técnica de proteção na solução da fabricante Citrix. Portanto, mais um grave descumprimento do que é solicitado no termo de referência e demonstra a necessidade de desclassificação da proposta apresentada pela empresa Add Value.

A Constituição Federal brasileira determina que a administração pública obedeça aos princípios da legalidade, impessoalidade, moralidade, publicidade e eficiência (art. 37, caput). Explícita ainda a Constituição a necessidade de observância desses princípios ao exigir que as obras,

serviços, compras e alienações sejam contratados mediante processo de licitação pública que assegure igualdade de condições a todos os concorrentes (art. 37, inciso XXI).

Dentre as principais garantias, pode-se destacar a vinculação da Administração ao edital que regulamenta o certame licitatório. Trata-se de uma segurança para o licitante e para o interesse público, extraída do princípio do procedimento formal, que determina à Administração que observe as regras por ela própria lançadas no instrumento que convoca e rege a licitação.

Segundo Lucas Rocha Furtado, Procurador-Geral do Ministério Público junto ao Tribunal de Contas da União, o instrumento convocatório é a lei do caso, aquela que irá regular a atuação tanto da administração pública quanto dos licitantes. Esse princípio é mencionado no art. 3º da Lei de Licitações, e enfatizado pelo art. 41 da mesma lei que dispõe que “a Administração não pode descumprir as normas e condições do edital, ao qual se acha estritamente vinculada”. (Curso de Direito Administrativo, 2007, p.416)

Ainda sobre a vinculação ao edital, Marçal Justen Filho afirma que “Quando o edital impuser comprovação de certo requisito não cogitado por ocasião do cadastramento, será indispensável a apresentação dos documentos correspondentes por ocasião da fase de habilitação” (Pregão. Comentários à Legislação do Pregão Comum e do Eletrônico, 4ª ed., p. 305). Como exemplo de violação ao referido princípio, o referido autor cita a não apresentação de documento exigido em edital e/ou a apresentação de documento em desconformidade com o edital (como documento enviado por fac-símilesem apresentação dos originais posteriormente).

DO PEDIDO

Por todo o exposto, a Fast Help requer:

Que seja desconsiderada a decisão que habilitou a empresa Add Value, uma vez que se baseou em itens que não atendem o Edital, faz-se necessário a desclassificação da RECORRIDA.

A convocação da empresa Fast Help (próxima colocada) com o retorno da fase de habilitação, fundamentando-se na obediência aos princípios licitatórios.

Nestes termos, Pede Deferimento.