Respostas 1ª Diligência - Pregão 15/2021 - Balanceadores (CGU)

Especificações Técnicas:

a) 1.2.2 - Deve suportar, no mínimo, 100 (cem) transações por segundo de SSL com chave de 2048.

Questionamento:

Para o item 1.2.2, indicação do documento que comprove o desempenho suporta, no mínimo, 100 (cem) transações por segundo de SSL com chave de 2048.

Resposta:

A comprovação para o requisitado pelo item 1.2.2 não está disponível em documentação pública ou datasheet do fabricante, para a solução ofertada. Por esse motivo, foi apresentada uma carta pelo fabricante, com arquivo nome "Brazil Wy Tecnologia CGU Pregao Eletronico 15-2021_signed.pdf", onde está sendo feito a declaração do atendimento ai tem. Na carta pela Fortinet está declarado "Por meio desta carta, informamos que a solução FortiADC, modelo FAD-VM04, possui .... Também informamos que o mesmo modelo, suporta 100 (cem) transações por segundo de SSL com chave de 2048 bits.". Desta forma, fica apresentado declaração do fabricante quanto ao atendimento ao item.

b) 1.3.5 - A solução deverá ser capaz de autenticar usuários administradores em bases de dados remotas por LDAP, incluindo, mas não limitado, a Microsoft Active Directory.

Questionamento:

Para o item 1.3.5, indicação do documento cujo conteúdo se refira à autenticação de usuários da interface web do ADC.

Resposta:

Para fins de deixar mais claro o atendimento ao item, apresentando documentação do fabricante onde deixa claro a possibilidade de criação de usuários administrativos com a possibilidade de autenticação dos mesmo através de um servidor RADIUS ou LDAP. Pelo link https://docs.fortinet.com/document/fortiadc/6.2.1/handbook/444791/create-administrator-users, é possível ver onde se diz "If you want to use RADIUS or LDAP authentication, you must have already have created the RADIUS server or LDAP server configuration". Para a configuração prévia de integração com o

servidor LDAP, basta seguir as instruções no link https://docs.fortinet.com/document/fortiadc/6.2.1/handbook/628325/using-an-ldap-authentication-server. Desta forma, entendemos que deixamos claro o atendimento ao item quanto a capacidade de autenticar usuários administrativos em base remota LDAP.

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

Questionamento:

Para o item 1.3.8.7, indicação do documento que demonstre a quantidade de conexões SSL, Transações SSL por segundo (SSL TPS) ou Conexões SSL por segundo (SSL CPS).

Resposta:

As informações sobre Conexões concorrentes e conexões por segundo podem ser visualizadas de duas formas. Primeiramente no Dahsboard inicial da solução, em sua GUI, são apresentadas Widgets com informações gerais sobre estatísticas atuais passando pela solução. Como pode ser observado pelo link https://docs.fortinet.com/document/fortiadc/6.2.1/handbook/769237/widgets , o widget the "Server Load Balance" apresenta informações de throuhgput, conexões concorrentes e conexões por segundo, disponibilizados em forma de gráfico.

A segunda forma de se visualizar informação de conexões concorrentes e conexões por segundo é individualmente para cada Virtual Server. Essa informação vai estar disponível no menu FortiView -> Virtual Servers, como pode ser observado pelo link https://docs.fortinet.com/document/fortiadc/6.2.1/handbook/819463/virtual-servers e nas figuras disponíveis neste site. Também é apresentado informação de throughput, conexões concorrentes e conexões por segundo para cada Virtual Server criado. Desta forma, entedemos que deixamos claro o atendimento ao item referido;

d) 1.4.5 - Deve suportar, no mínimo, 1000 VLANs;

Questionamento:

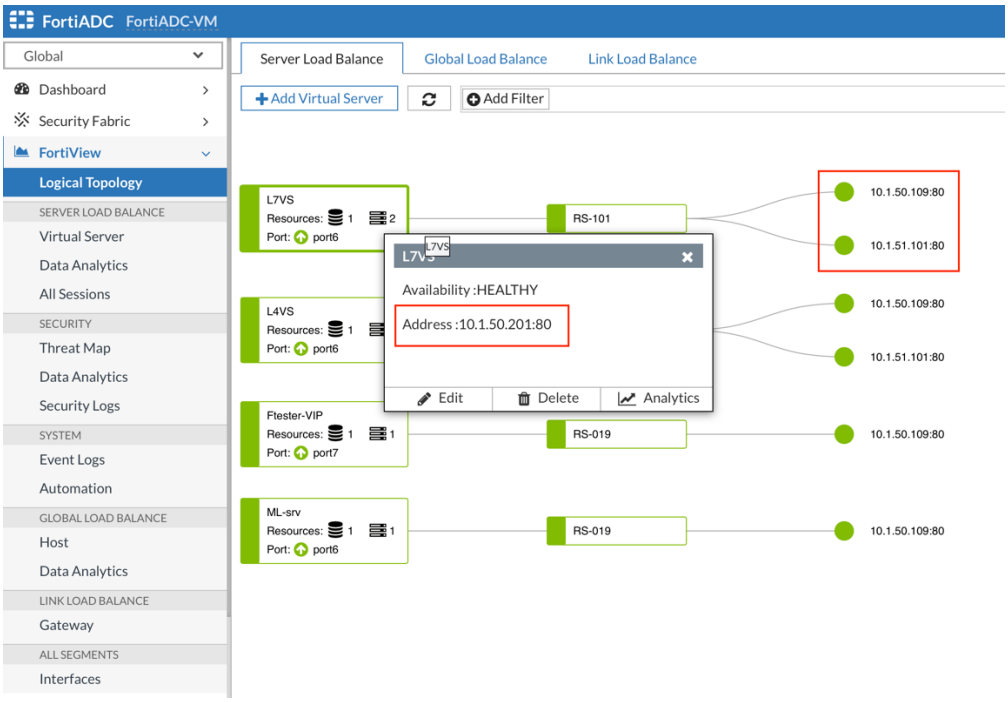
Para o item 1.4.5, esclarecer se as 2 (duas) licenças do modelo ofertado (VM-04), cada uma com limite de 512 (quinhentos e doze) VLANs, totalizam 1024 VLANs.

Resposta:

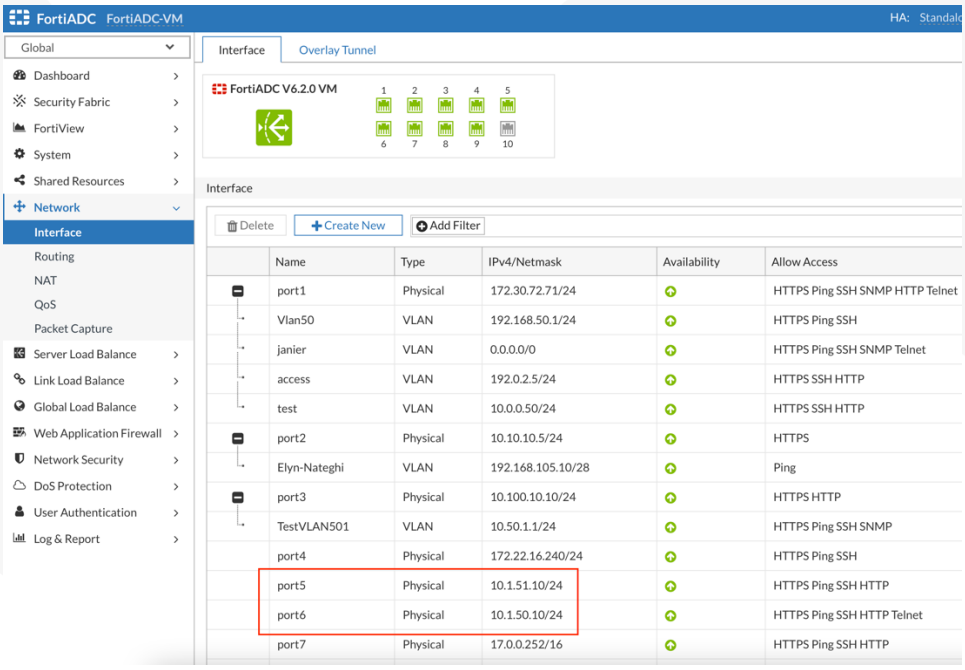
Durante a fase de questionamentos deste pregão, enviamos o questionamento seguinte. "*Entendemos que a solução ofertada deve, em sua totalidade, suportar no mínimo 1000 VLANs conforme apresentado no item 1.4.5. Está correto nosso entendimento?*". A resposta que recebemos foi: *"Em atendimento ao questionamento, confirmo o entendimento da empresa WYTECNOLOGIA. Conforme*

o Anexo I, item 1.4.5, do Termo de Referência, a Solução de Balanceamento deve suportar, no mínimo, 1000 VLANs;". Nosso entendimento é que a solução inteira precisa suportar as 1000 VLANs, onde em nosso entendimento a solução interia são o cluster de Appliance Virtual de Application Delivery Controllers para o ambiente On-Premisses e também o cluster de Appliance Virtual de Application Delivery Controllers para o ambiente de Nuvem. Cada um dos clusters irá suportar 512 VLANs totalizando o suporte de 1024 VLANs para a solução.
Desta forma, entedemos que deixamos claro o atendimento ao item referido;

e) 1.4.9 - Permitir a configuração de servidores reais em endereços de sub-redes diferentes dos endereços IP virtuais;
Questionamento:
Para o item 1.4.9, indicar documento no qual esteja demonstrada a possibilidade de configuração de servidores reais em endereços de sub-redes diferentes dos endereços IP virtuais.
Resposta:
Para fins de deixar claro o atendimento ao item, complementando a descrição da configuração de servidores reais apresentando na documentação, apresentamos abaixo tela da solução FortiADC ofertada onde pode ser observado as sessões abertas para um Virtual Server (VIP 10.1.50.201) onde se apresenta também o endereço IP real dos servidores (10.1.50.109 e 10.1.51.101). Veja na outra figura que as redes 10.1.50/24 e 10.1.51/24 estão em segmentos e interfaces diferentes.



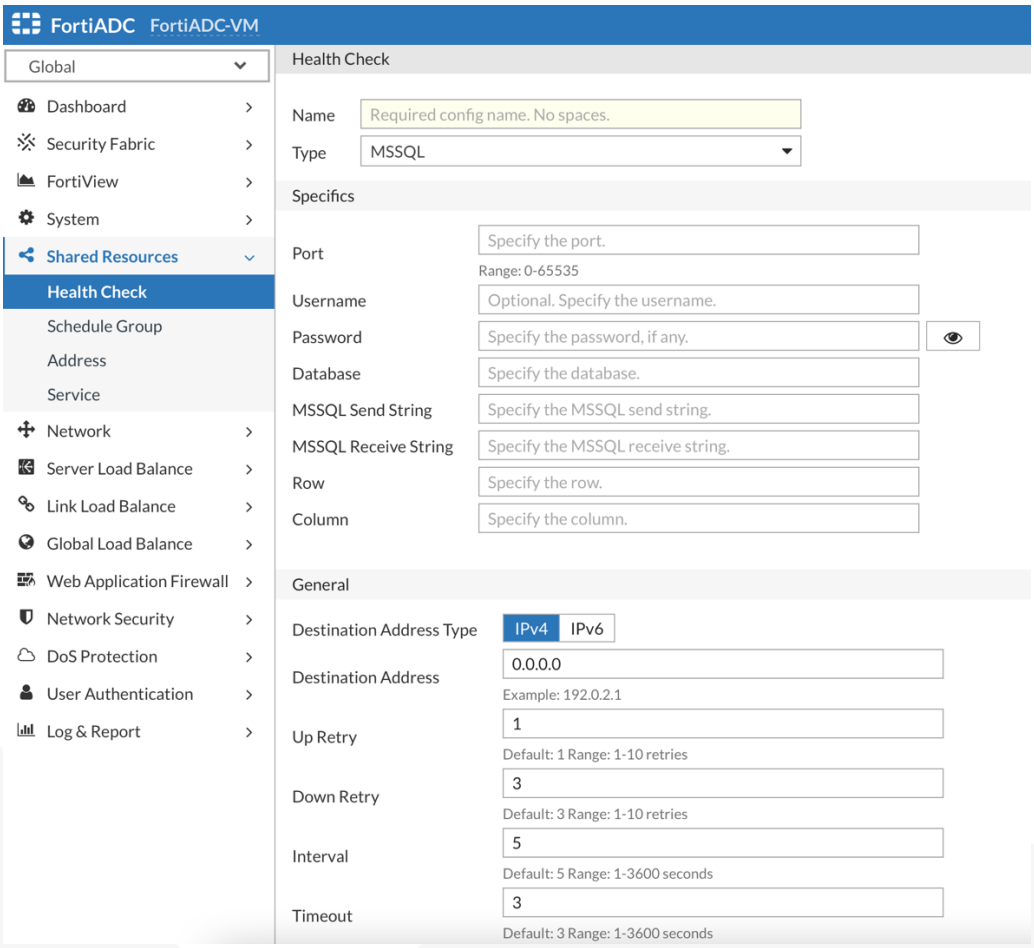
Abaixo configuração das interfaces da solução FortiADC de demo.



Esta informação pode ser validada através do site de demostração da solução do fabricante pelo link https://fortiadc.fortidemo.com/ui/#navigate/Login, usando de usuário **demo** e senha **demo**;

f) 1.4.16 - Quando um servidor novo for adicionado, deve ser possível configuração que permita otimizar a entrada e a performance dos novos servidores na rede. O sistema deve ser capaz de implementar Slow Start, ou seja, crescimento gradativo do número de novas sessões;
Questionamento:
Para o item 1.4.16, indicar documento que demonstre a possibilidade de configuração que permita otimizar a entrada e a performance dos novos servidores na rede, quando um servidor novo for adicionado. O sistema deve ser capaz de implementar Slow Start, ou seja, crescimento gradativo do número de novas sessões.
Resposta:
Como pode ser observado pelo link https://docs.fortinet.com/document/fortiadc/6.2.1/handbook/740387/using-real-server-pools, o conceito de Slow Start é apresentado no momento da configuração do Server Pool como "Warm Up" e "Warm Rate". Veja que a documentação explica as possibilidades de configuração onde é necessária uma combinação de warm up com o warm rate. Desta forma, entedemos que deixamos claro o atendimento ao item referido;

g) 1.4.18.3 – Layer 7 – Conexões específicas ao protocolo de aplicação, com, no mínimo, os seguintes monitores (Health Checks) na camada 7 predefinidos: HTTP, HTTPS, LDAP, MSSQL, RADIUS, SMTP, SNMP, deverão ser suportados;
Questionamento:
Para o item 1.4.18.3, indicar documento que demonstre que o modelo ofertado atende também ao MSSQL (Microsoft SQL Server).
Resposta:
Infelizmente a documentação não está atualizada com todos as informações sobre os monitores (Health Checks) suportados. Para isso, estamos adicionado abaixo tela de configuração da solução onde é apresentado o suporte a monitoração de MSSQL:



Esta informação pode ser validada através do site de demostração da solução do fabricante pelo link https://fortiadc.fortidemo.com/ui/#navigate/Login, usando de usuário **demo** e senha **demo**. No memu, após o login, escolher as opções Shared Resources -> Health Check -> Create New e na opção Type escolher MSSQL;

h) 1.5.8 – A solução deve permitir a inspeção ou controle de upload de arquivos para os servidores de aplicação;

Questionamento:

Para o item 15.8, esclarecer se há necessidade um componente extra (FortiSandbox e/ou FortiGuard) para que a solução permita a inspeção ou controle de upload de arquivos para os servidores de aplicação.

Resposta:

Não será necessário componente extra para a inspeção e controle de upload de arquivos para os servidores de aplicação. O controle e inspeção de arquivos será

feito através da política de WAF para tipos e tamanhos de arquivos permitidos. Como pode ser observado pelo link https://docs.fortinet.com/document/fortiadc/6.2.1/handbook/776134/configuring-input-validation#File, onde é possível a criação de política dentro do perfil de WAF, restringindo o tamanho e o tipo do arquivo a ser feito o upload.

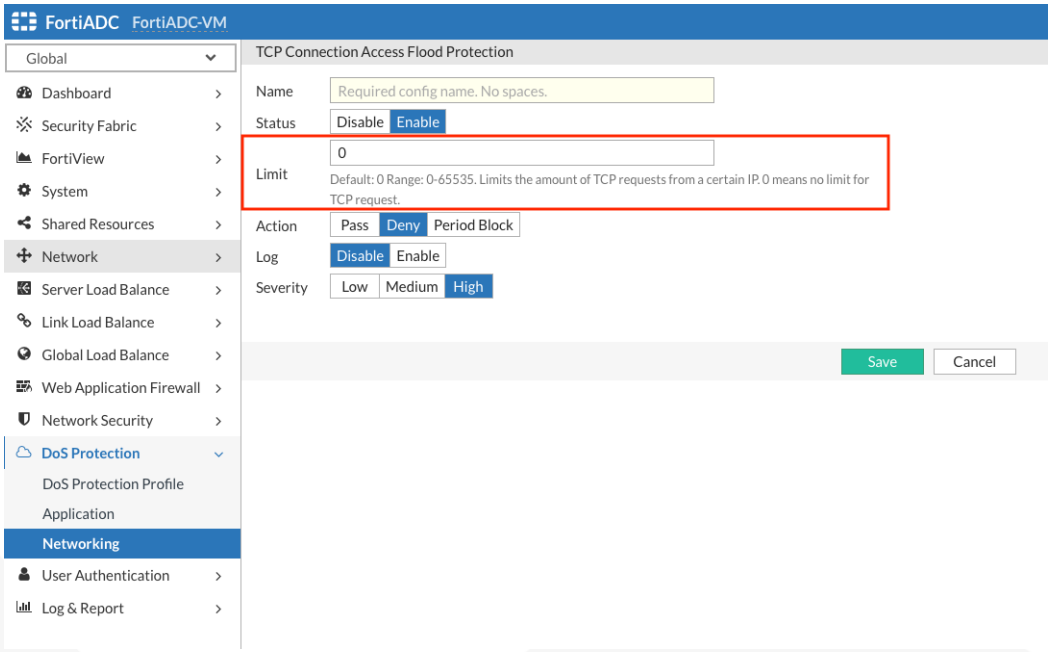
Upload File Status	Allow: Only allow the selected file type to upload. Block: Block any upload of the selected file type.
Upload File Size	The maximum size of the uploaded file.

Desta forma, entedemos que deixamos claro o atendimento ao item referido;

i) 1.5.14.2 - Número de requisições por segundo enviados de um IP específico;
Questionamento:
Para o item 1.5.14.2, indicar documento que demonstre que a configuração do modelo ofertado possue a opção de indicar qual é o IP ou subrede a ser bloqueada.
Resposta:
Para deixar mais claro o atendimento ao item, pode ser observado pelo link https://docs.fortinet.com/document/fortiadc/6.2.1/handbook/76901/configuring-http-access-limit-policy a possibilidade da solução de configurar uma política de "HTTP access limit" dentro do perfil de DoS Protection. Como pode ser observado pela descrição da funcionalidade, esta permite limitar o número de requisições por segundo HTTP de um determinado endereço IP, onde diz *"Limits the amount of HTTP requests per second from a certain IP"*. Entendemos que desta forma deixamos claro o atendimento ao item.

j) 1.5.14.4 - Número máximo de transações por segundo (TPS) de um determinado IP;
Questionamento:
Para o item 1.5.14.4, a documentação indicada cita limitação de banda para conexões com o mesmo session cookie e o que está sendo pedido é limitação por número de TPS (Transações por Segundo). Portanto, indicar documento que demonstre possibilidade de configuração de detecção de ataque de DoS pelo número de TPS de determinado IP.
Resposta:
Na solução ForitADC, é possível também fazer o controle de número de conexões TCP de um determinado endereço IP. Esta funcionalidade está documentada no CLI Guide da solução ofertada. Como pode ser observado pelo link https://docs.fortinet.com/document/fortiadc/6.2.1/cli-

reference/224156/config-security-dos-tcp-access-flood-protection, é possível limitar o número de conexões TCP de um ip de origem, onde diz *"Limit the number of TCP connection per source IP address"*. A mesma informação pode ser observada na figura abaixo, da GUI da solução.



Também pode ser utilizado a funcionalidade de "HTTP access limit" (https://docs.fortinet.com/document/fortiadc/6.2.1/handbook/76901/configuring-http-access-limit-policy), como descrito na comprovação do item 1.5.14.2. Entendemos que desta forma deixamos claro o atendimento ao item.

k) 1.5.15.6 - Sequestro de sessão; e

Questionamento:

Para o item 1.5.15.6, esclarecer o motivo de o documento indicado não mencionar "SESSION HIJACKING", que seria o sequestro de sessão, ou Cookie Poisoning, pois cita apenas "SESSION FIXATION".

Resposta:

Para fins de deixar a comprovação do item mais clara, pode ser observado no link https://docs.fortinet.com/document/fortiadc/6.2.1/handbook/289274/web-application-firewall-basics a possibilidade de proteção contra Session Hijacking através das proteções de Cookie Security e configuração de políticas de autenticação.

6	Session Hijacking	It can be prevented by enabling Cookie Security and configuring Authentication policy.

Desta forma, entedemos que deixamos claro o atendimento ao item referido;

l) 1.5.17 - Capacidade de aprendizagem automática sobre o funcionamento de aplicações web.
Questionamento:
Para o item 1.5.17, indicar documento no qual demonstre que o modelo ofertado atende a especificação de aprendizagem do comportamento de uma aplicação.
Resposta:
Para o atendimento ao item, apresentamos a possiblidade da solução FortiADC fazer o reconhecimento automático da aplicação e suas vulnerabilidades, a partir de um scan onde é criado um peril de segurança de WAF originado do scan aprendido. Como observado pelo link https://docs.fortinet.com/document/fortiadc/6.2.1/handbook/99930/web-vulnerability-scanner, a solução possui esta funcionalidade de aprendizado da aplicação e suas vulnerabilidades que podem ser acionados a qualquer momento. Uma vez feito este scan e aprendizado, uma política de WAF é gerada automaticamente, como pode ser observado pelo link https://docs.fortinet.com/document/fortiadc/6.2.1/handbook/670196/scan-history#Generating_Policy

Generating Automatic Policy

By analyzing the scan results in the imported report, FortiADC automatically generates a WAF profile to prevent the reported attacks. In the Automatic Policy, you will required to specify the name of the generated WAF profile and the actions to be taken upon the attacks.

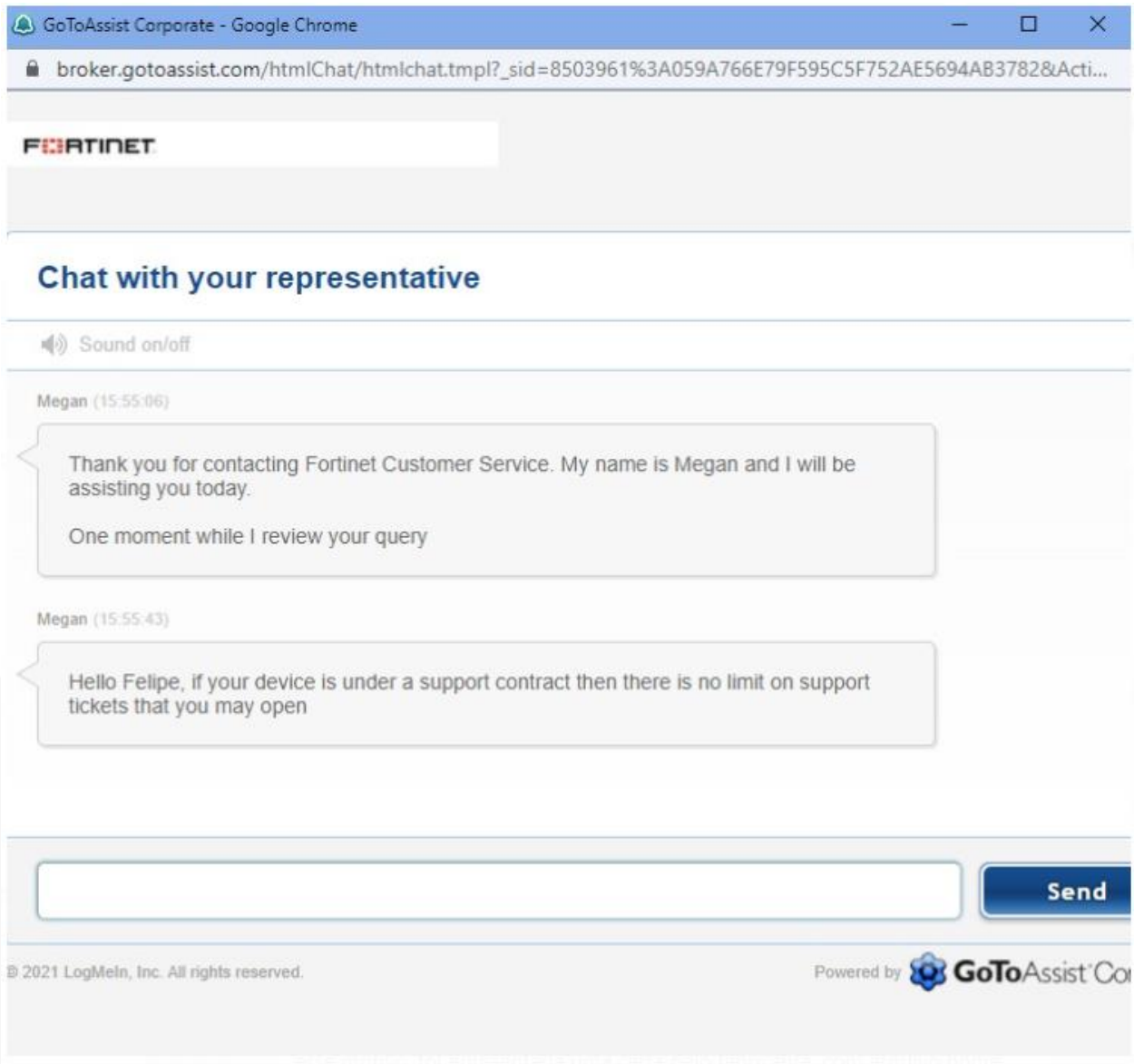
Desta forma, entedemos que deixamos claro o atendimento ao item referido;

Requisitos da contratação:

Item:
a) 4.4.1.2 - Deverá contar com canal de atendimento, para abertura e acompanhamento de chamados, que deverá estar disponível 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, por e-mail, web ou telefone 0800 ou DDD 61.
Resposta:
Para o item 4.4.1.2 entendemos que no site do fabricante da solução possui a informação requerida:
https://www.fortinet.com/br/support/contact

Ao escolher a nossa região (Brasil) o telefone 0800 aparece: 0800 892 3898 (ligação gratuita)

Item:
b) 4.4.1.3 - Deverá contar com possibilidade de abertura ilimitada de chamados;
Resposta:
De acordo com o documento: “SD-FortiCareSupportServices.PDF” item 1, página 1 (Introduction). Descreve que o Forticare Technical Support fornece serviços de manutenção voltados para a operação e sustentando produtos Fortinet. Inclui atendimento ao cliente e assistência técnica para resolver incidentes técnicos. Dessa forma, não existe limitação para a quantidade de chamados, visto que, não é possível prever a quantidade de incidentes que poderão acontecer.
Trecho: This document describes FortiCare Technical Support, which provides focused maintenance services aimed at operating and sustaining Fortinet products. It includes customer service and technical support assistance to resolve technical incidents, as well as software updates, access to on-line tools and the replacement of defective hardware.
Também foi questionado com um representante do suporte técnico, e a resposta foi a seguinte:



Item:
c) 4.5.2 - As Licenças perpétuas com Direito de Atualização e Suporte Técnico, item 1 ou 2, deverão ser entregues até o final do Serviço de Instalação e Configuração, para tanto poderão ser utilizadas licenças trial durante o período do Serviço de Instalação e Configuração;
Resposta:
Para o item 4.5.2 Entendemos que podemos oferecer uma licença Trial de 60 dias para a instalação e configuração, antes da efetiva ativação dos serviços. O

documento "Fortinet-Service-Offering-Terms.pdf" na página 4, sessão 4. Evaluations, item 4.3 diz:
"4.3. Unless otherwise noted on the Evaluation Software entitlement, the Evaluation Software license is limited to sixty (60) days from the start date provided by Fortinet ("Term"). The Customer must cease use of the Evaluation Software upon expiration of the Term. At Fortinet's discretion, a new Software license may be provided for additional Evaluation."

Item:
d) 4.5.3 - O Direito de Atualização e Suporte Técnico das licenças, prestado diretamente pelo fabricante, deverá ser de, no mínimo, 60 (sessenta) meses, contados do recebimento definitivo Serviço de Instalação e Configuração;
Resposta:
De acordo com o documento: "Fortinet-Service-Offering-Terms.pdf" após a ativação dos Serviços Forticare, o cliente tem direito de atualização e suporte técnico pelo período contratado (página 2 item 2 subitem 2.1). O trecho diz:
"Upon activation of a FortiCare Service Contract and pursuant to Active Service Coverage Level applicable to the Product, the Customer will obtain the following entitlements to the extent within the scope of its Service Contract: (a) access to the Support Portal; (b) access to the TAC for Customer Service assistance as well as resolution of Technical Tickets; (c) access to Software updates (maintenance and feature releases) exclusively for the Products covered by the FortiCare Service Contract; and (d) the replacement of Hardware determined by Fortinet to be defective exclusively for the Hardware covered by the FortiCare Service Contract. For more details refer to the FortiCare Technical Support Service and Fortinet's policies."
Documento: Fortinet-Service-Offering-Terms.pdf

Item:
e) 4.7.1 - A língua da interface de gerência da solução deve ser em português do Brasil ou inglês;
Resposta:
De acordo com o link abaixo, temos a opção de inglês ou Chinês simplificado:

https://docs.fortinet.com/document/fortiadc/6.2.1/handbook/654503/configuring-basic-system-settings

To configure basic system settings:

1. Go to **System > Settings**.

   The configuration page displays the Basic tab.

2. Complete the configuration as described in Basic settings configuration.

3. Save the configuration.

Settings	Guidelines
Hostname	You can configure a hostname to facilitate system management. If you use SNMP, for example, the SNMP system name is derived from the configured hostname.The hostname can be up to 35 characters in length. It can include US-ASCII letters, numbers, hyphens, and underscores, but not spaces and special characters. The System Information widget and the `get system status` CLI command display the full hostname. If the hostname is longer than 16 characters, the name is truncated and ends with a tilde (~) to indicate that additional characters exist, but are not displayed.
Language	English or Simplified Chinese.
Idle Timeout	Log out an idle administrator session. The default is 30 minutes.
HTTP Port	Specify the port for the HTTP service. Usually, HTTP uses port 80.
Redirect to HTTPS	When enabled, all HTTP connections to FortiADC will be

Item:
f) 4.11.3 – Níveis de severidade e seus subitens;
g) 9.4.1 - A tabela a seguir apresenta os níveis de serviço mínimo exigidos para o serviço de suporte, de acordo com as severidades previstas no item 4.12 – REQUISITOS DE GARANTIA E MANUTENÇÃO:
Severidade Prazo de Início de Atendimento
1 (URGENTE) 1 (uma) hora
2 (ALTA) 2 (duas) horas
3 (MÉDIA) Próximo dia útil
4 (BAIXA) Próximos 2 dias úteis;

Resposta:
A Fortinet, na média, inicia o atendimento em 5 minutos para qualquer severidade (https://www.fortinet.com/br/support). As prioridades são modificadas de acordo com o a complexidade, conforme descrito no documento: **"SD-FortiCareSupportServices.PDF"**

Item:
h) 15.5.1.1 - Declaração que ateste a não ocorrência do registro de oportunidade, de modo a garantir o princípio constitucional da isonomia e a seleção da proposta mais vantajosa para a Administração Pública, conforme disposto na Lei nº 8.666, de 1993, e em atendimento ao item 1.7 do Anexo da IN SGD/ME nº 01/2019;
Resposta:
Documento anexo: Declaração de não registro de RO.pdf

Item:
i) 15.5.1.2 - Declaração que a solução fornecida e todos os seus componentes serão da versão mais atual disponibilizada pelo fabricante e que não há anúncio de end-of-sales e end-of-support.
Resposta:
Documento Anexo: Declaração de oferta da solução atual.pdf

Item:
1.2.1 Para tanto, solicitamos ainda que a referida empresa apresente documentos comprobatórios e declarações, quando for o caso, em atendimento aos itens suprarelacionados.
Resposta:
Todos os documentos de apoio foram enviados juntos com este documento.

FILIPE SERAFIM DE PAULA:73257931115

Assinado de forma digital por FILIPE SERAFIM DE PAULA:73257931115
Dados: 2021.11.30 17:51:07 -03'00'

FILIPE SERAFIM DE PAULA
DIRETOR EXECUTIVO