

ILUSTRÍSSIMA SENHORA PREGOEIRA DA PRODAM - PROCESSAMENTO DE DADOS
AMAZONAS S/A

Pregão Eletrônico n. 06/2019

DFTI COMÉRCIO E SERVIÇOS DE INFORMÁTICA LTDA., já devidamente qualificada no presente processo licitatório, vem respeitosamente à presença de V. Senhoria, na forma do item 4.3 do edital, apresentar CONTRARRAZÕES ao recurso administrativo interposto pela licitante GLOBAL TTI SOLUÇÕES EM TECNOLOGIA LTDA, o que faz com base nas razões de fato e de direito a seguir expostas.

1 TEMPESTIVIDADE

Inicialmente, frise-se que esta resposta é tempestiva. De acordo com o previsto no edital de licitação, as contrarrazões ao recurso podem ser apresentadas em cinco dias úteis, contados da apresentação das razões do recurso, o que se deu em 05/11/2019. Assim, contado na forma do item 20.5 do edital de licitação, o prazo de contrarrazões iniciou-se em 06/11/2019, encerrando-se em 12/11/2019, data até a qual esta peça será tempestiva.

2 SÍNTESE E MÉRITO

Em breve síntese, trata-se de resposta a recurso administrativo por meio do qual a recorrente – que havia sido a arrematante originária na licitação – pretende a reversão da sua exclusão da disputa, alegando que o exame técnico de sua proposta foi incorreto.

Conforme ficará evidente, tal medida baseia-se tão somente em caráter protelatório, uma vez que TODOS os argumentos apresentados, face as exigências mínimas exigidas, não foram ao menos questionados! Salieta-se que o processo teve suas especificações

técnicas alteradas mediante republicação e que, em nenhum momento a recorrente pronunciou-se na tentativa de tornar a tecnologia a qual representa aderente através de solicitação de esclarecimentos, no prazo hábil.

Para tanto, a sua peça traz argumentos técnicos por meio dos quais tenta refutar a sua desclassificação, alegando cumprimento integral a todas as exigências do edital. Veremos, no entanto, que tal não se deu, e que a decisão proferida pela Ilma. Pregoeira, com apoio na avaliação técnica realizada por seus profissionais acerca da solução apresentada pela recorrente, é a mais correta no caso em apreço.

2.1 Do não atendimento às especificações técnicas do edital pela proposta da recorrente

A fim de identificar os descumprimentos de requisitos do edital em cada ponto, o exame subsequente será feito pela transcrição de cada exigência do edital, acompanhada na sequência pelos comentários da recorrida.

EDITAL:

6.1.2. Suportar 4.000.000 (quatro milhões) de conexões simultâneas;

O equipamento M470, ofertado na proposta comercial da licitante GlobalTTI, não atende ao item, que deixa claro que deve suportar 4.000.000 (quatro milhões) de conexões simultâneas. O equipamento ofertado suporta 3.800.000 de conexões simultâneas, ficando 200.000 abaixo do solicitado, conforme pode ser comprovado na própria documentação enviada pela licitante GlobalTTI (documento “Datasheet_firebox_M470_M570-670.pdf”):

Firebox	M470
THROUGHPUT	
Firewall	19.6 Gbps
Firewall (IMIX)	5.6 Gbps
VPN (UDP 1518)	5.2 Gbps
VPN (IMIX)	1.8 Gbps
HTTPS (IPS enabled)	2.0 Gbps
Antivirus	3.5 Gbps
IPS (fast/full scan)	5.7/3.0 Gbps
UTM (fast/ full scan)	3.1/2.1 Gbps
CAPACITY	
Interfaces 10/100/1000*	8 (optional modules available)
I/O interfaces	1 SRL/2 USB
Concurrent connections	3,800,000
Concurrent connections (proxy)	310,000
New connections per second	82,000
VLANs	300
WSM licenses (incl)	4
TDR Host Sensors included	200
Authenticated users limit	Unrestricted

EDITAL:

6.2.6. Possui SSD integrado para armazenamento e sistema operacional;

Não há informações que comprovem o atendimento ao item, já que nada consta sobre a utilização de SSD no equipamento na documentação apresentada. Tal evidência indica não atendimento ao subitem 14.1.2 do edital, segundo o qual se exige “Catálogo (s), folheto(s) e manual(is), deverão estar preferencialmente na língua portuguesa com especificações técnicas detalhadas da solução ofertada, para comprovação de características técnicas obrigatórias, informando, inclusive, marca, modelo, tipo, fabricante e procedência da solução, detalhados de forma clara, evitando-se jargões de uso duvidoso ou ainda não consagrados na terminologia de informática” (grifo nosso).

A empresa GlobalTTI, em seu recurso (ou seja, de forma extemporânea, já que a informação deveria constar obrigatoriamente da documentação remetida quando da proposta), informa noutra documentação a utilização de discos SSD em seus equipamentos. Porém, analisando a documentação enviada (documento “WatchGuard Firebox M4600 –

Hardware Guide”), percebe-se que não há comprovação de utilização de discos SSD no equipamento ofertado M4600. Veja-se a informação constante do seguinte link: <https://www.watchguard.com/help/docs/hardware%20guides/Firebox_M4600_Hardware_Guide.pdf>:

About Your Hardware

Hardware Specifications

Processor	Intel Xeon E3-1275V3
Storage:	2 GB CFAST CARD + 320GB 2.5" SATA HDD
Memory: DDR3	8 GB
Power supply	Dual power supplies 300W 100-240VAC/5-3A/50-60Hz
Dimensions	Depth: 18.42" (46.8 cm) Width: 16.96" (43.1 cm) Height: 1.73" (4.4 cm) - 1U
Weight	17.63 lbs (8 Kg)

Interface Specifications

Network interfaces	8x 1000 Base-TX (10/100/1000 Mbps), RJ45 connector
I/O interfaces	2 USB 3.0 1 RJ45 RS232 console port

This specification describes the interfaces that are on the Firebox M4600 as shipped. The Firebox also has two slots where you can install additional interface modules. The supported interface modules are described in the Hardware Description section.

Por tais razões, fica claro o não atendimento ao edital de licitação.

EDITAL:

6.3.2. Suportar 8.000.00 (oito milhões) de conexões simultâneas;

O equipamento M4600, ofertado na proposta comercial da licitante GlobalTTI, suporta 7.500.000 (sete milhões e quinhentas mil) conexões simultâneas, ficando 500.000 abaixo do solicitado, conforme pode ser comprovado na documentação enviada pela licitante (documento "Datasheet_Firebox_M4600_M5600.pdf"). Veja-se:

Firebox	M4600 base + 4 x 10 Gb interfaces
THROUGHPUT	
Firewall throughput*	40 Gbps
VPN throughput*	10 Gbps
AV throughput*	9 Gbps
IPS throughput*	13 Gbps
UTM throughput*	8 Gbps
Interfaces (installed)	8 x 1Gb
I/O interfaces	1 serial/2 USB
Concurrent connections (bi-directional)	7.5 million
New connections per second	160,000
VLANs	1,000
Authenticated users limit	unrestricted

Evidente, assim, o não atendimento às exigências do edital.

EDITAL:

6.3.3. Suportar mínimo 200.000 (duzentos mil) novas conexões por segundo;

O equipamento ofertado pela licitante GlobalTTI suporta 160.000 novas conexões, ficando 40.000 abaixo do solicitado, conforme comprovado na documentação enviada pela GlobalTTI (documento: "Datasheet_firebox_M4600_M5600.pdf"). Veja-se:

Firebox	M4600 base + 4 x 10 Gb interfaces
THROUGHPUT	
Firewall throughput*	40 Gbps
VPN throughput*	10 Gbps
AV throughput*	9 Gbps
IPS throughput*	13 Gbps
UTM throughput*	8 Gbps
Interfaces (installed)	8 x 1Gb
I/O interfaces	1 serial/2 USB
Concurrent connections (bi-directional)	7.5 million
New connections per second	160,000
VLANs	1,000
Authenticated users limit	unrestricted

Novamente, comprovado o não atendimento às exigências do edital.

EDITAL:

6.3.6. Possui SSD integrado para armazenamento e sistema operacional;

Não há informações que comprovem o atendimento ao item, já que nada consta sobre a utilização de SSD no equipamento na documentação apresentada. Tal evidência indica não atendimento ao subitem 14.1.2 do edital, segundo o qual se exige “Catálogo (s), folheto(s) e manual(is), deverão estar preferencialmente na língua portuguesa com especificações técnicas detalhadas da solução ofertada, para comprovação de características técnicas obrigatórias, informando, inclusive, marca, modelo, tipo, fabricante e procedência da solução, detalhados de forma clara, evitando-se jargões de uso duvidoso ou ainda não consagrados na terminologia de informática” (grifo nosso).

A empresa GlobalTTI, em seu recurso (ou seja, de forma extemporânea, já que a informação deveria constar obrigatoriamente da documentação remetida quando da proposta), informa noutra documentação a utilização de discos SSD em seus equipamentos. Porém, analisando a documentação enviada (documento “WatchGuard Firebox M4600 – Hardware Guide”), percebe-se que não há comprovação de utilização de discos SSD no equipamento ofertado M4600. Veja-se a informação constante do seguinte link: <https://www.watchguard.com/help/docs/hardware%20guides/Firebox_M4600_Hardware_Guide.pdf>:

About Your Hardware

Hardware Specifications

Processor	Intel Xeon E3-1275V3
Storage:	2 GB CFAST CARD + 320GB 2.5" SATA HDD
Memory: DDR3	8 GB
Power supply	Dual power supplies 300W 100-240VAC/5-3A/50-60Hz
Dimensions	Depth: 18.42" (46.8 cm) Width: 16.96" (43.1 cm) Height: 1.73" (4.4 cm) - 1U
Weight	17.63 lbs (8 Kg)

Interface Specifications

Network interfaces	8x 1000 Base-TX (10/100/1000 Mbps), RJ45 connector
I/O interfaces	2 USB 3.0 1 RJ45 RS232 console port

This specification describes the interfaces that are on the Firebox M4600 as shipped. The Firebox also has two slots where you can install additional interface modules. The supported interface modules are described in the Hardware Description section.

Evidente, portanto, o não atendimento ao edital.

EDITAL:

6.4.6. Possui SSD integrado para armazenamento e sistema operacional;

Não há informações que comprovem o atendimento ao item, já que nada consta sobre a utilização de SSD no equipamento na documentação apresentada. Tal evidência indica não atendimento ao subitem 14.1.2 do edital, segundo o qual se exige “Catálogo (s), folheto(s) e manual(is), deverão estar preferencialmente na língua portuguesa com especificações técnicas detalhadas da solução ofertada, para comprovação de características técnicas obrigatórias, informando, inclusive, marca, modelo, tipo, fabricante e procedência da solução, detalhados de forma clara, evitando-se jargões de uso duvidoso ou ainda não consagrados na terminologia de informática” (grifo nosso).

A empresa GlobalTTI, em seu recurso (ou seja, de forma extemporânea, já que a informação deveria constar obrigatoriamente da documentação remetida quando da proposta), informa noutra documentação a utilização de discos SSD em seus equipamentos. Porém, analisando a documentação enviada (documento “WatchGuard Firebox M5600 – Hardware Guide”), percebe-se que não há comprovação de utilização de discos SSD no equipamento ofertado M5600. Veja-se a informação constante do seguinte link: <https://www.watchguard.com/help/docs/hardware%20guides/Firebox_M5600_Hardware_Guide.pdf>:

About Your Hardware

Hardware Specifications

Processor	Intel Xeon E5-2680V2
Storage:	2GB CFAST CARD + 250 GB 2.5" SATA HDD
Memory: DDR3	16 GB
Power supply	Dual power supplies 400W 100-240VAC/6-3A/47-63Hz
Dimensions	Depth: 22.83" (58 cm) Width: 17.25" (43.8 cm) Height: 1.73" (4.4 cm) - 1U
Weight	26.45 lbs (12 Kg)

Interface Specifications

Network Interfaces	9x 1000 Base-TX (10/100/1000 Mbps), RJ45 connector 4x 10 G SFP+ ports
I/O Interfaces	2 USB 2.0 1 RJ45 RS232 console port

This specification describes the interfaces that are on the Firebox M5600 as shipped. The Firebox also has two empty bays where you can install additional optional interface modules. The supported interface modules are described in the Hardware Description section.

Não atendido o edital, portanto, o que indica a necessidade de desprovisionamento do recurso interposto.

EDITAL:

6.5.1.6.1. Suporte a, no mínimo, 1024 VLAN Tags 802.1q, policy based routing ou policy based forwarding, roteamento multicast (PIM-SM), DHCP Relay, DHCP Server;

Não há informações que comprovem o atendimento ao item. Tal evidência indica não atendimento ao subitem 14.1.2 do edital, segundo o qual se exige “Catálogo (s), folheto(s) e manual(is), deverão estar preferencialmente na língua portuguesa com especificações técnicas detalhadas da solução ofertada, para comprovação de características técnicas obrigatórias, informando, inclusive, marca, modelo, tipo, fabricante e procedência da solução, detalhados de forma clara, evitando-se jargões de uso duvidoso ou ainda não consagrados na terminologia de informática” (grifo nosso).

O produto ofertado pela recorrente **NÃO atende ao quantitativo de 1024 VLAN** exigido neste item, como se pode ver no sítio do próprio fabricante na coluna do produto M470, linha VLAN, em que se informa atendimento a somente 300 VLANs. A informação consta do seguinte link: <<https://www.watchguard.com/wgrd-resource-center/docs/watchguard-product-matrix-en>> para o Tipo 1. Perceba-se a existência de somente 1000 para o Tipo 2 e 3.

WatchGuard® Network Security Products at a glance

	Firebox T1s/T1s-W	Firebox T35/T35-W/T35-R*	Firebox T55/T55-W	Firebox T70	Firebox M270	Firebox M370	Firebox M440	Firebox M470	Firebox M570	Firebox M670	Firebox M4600 base + 4 x 10 Gb ports	Firebox M5600 base + 4 x 10 Gb ports
Throughput and Connections												
Firewall throughput	400 Mbps	640 Mbps	1 Gbps	4 Gbps	4.9 Gbps	8 Gbps	6.7 Gbps	19.6 Gbps	26.6 Gbps	34 Gbps	40 Gbps	60 Gbps
VPN throughput	150 Mbps	560 Mbps	360 Mbps	740 Mbps	1.6 Gbps	4.6 Gbps	3.2 Gbps	5.2 Gbps	5.8 Gbps	7.6 Gbps	10 Gbps	10 Gbps
All throughput	120 Mbps	325 Mbps	636 Mbps	1.2 Gbps	2.1 Gbps	3.0 Gbps	2.3 Gbps	3.5 Gbps	3.5 Gbps	6.2 Gbps	9 Gbps	12 Gbps
IPS throughput	160 Mbps	573 Mbps	636 Mbps	1.5 Gbps	2.3 Gbps	4.8 Gbps	2.3 Gbps	5.7 Gbps	8.0 Gbps	10.4 Gbps	13 Gbps	18 Gbps
UTM throughput	90 Mbps	278 Mbps	523 Mbps	1.1 Gbps	1.6 Gbps	2.6 Gbps	1.6 Gbps	3.1 Gbps	4.4 Gbps	5.4 Gbps	8 Gbps	11 Gbps
Interfaces	3 x 1 Gb	5* x 1 Gb	5* x 1 Gb	8 x 1 Gb	8 x 1 Gb	8 x 1 Gb	25 x 1 Gb copper** 2 x 10 Gb SFP+	8**	8**	8**	8 x 1 Gb additional ports available***	8 x 1 Gb + 4 x 10 Gb fiber additional ports available***
I/O Interfaces	1 Serial / 1 USB	1 Serial / 2 USB	1 Serial / 2 USB	1 SBL/2 USB	1 SBL / 2 USB	1 Serial / 2 USB	1 Serial / 2 USB	1 Serial / 2 USB	1 Serial / 2 USB	1 Serial / 2 USB	1 Serial / 2 USB	1 Serial / 2 USB
Concurrent connections	95,000	125,000	125,000	800,000	2,000,000	3,300,000	4,000,000	3,800,000	8,300,000	8,500,000	7,500,000	12,900,000
New connections per second	2,400	6,800	9,300	27,000	40,000	51,000	62,000	82,000	115,000	140,000	100,000	240,000
VLAN support	10	50	75	75	100	200	400	300	500	750	1,000	Unrestricted
Authentication users limit	200	500	500	500	500	500	Unrestricted	Unrestricted	Unrestricted	Unrestricted	Unrestricted	Unrestricted
VPN Tunnels												
Branch Office VPN	5	25	40	50	50	100	300	250	500	750	5,000	Unrestricted
Mobile VPN IPSec	5	25	50	60	75	100	300	250	500	750	10,000	Unrestricted
Wireless												
Wireless Access Points (APs)	WatchGuard offers a family of AP devices that allow all Firebox security capabilities to be extended to the WLAN. APs can be managed in the WiFi Cloud or through the Firebox's built-in wireless controller. For managing more than 20 APs, WatchGuard recommends WiFi Cloud. More info at watchguard.com/wifi											
Max APs advised per model	4	20	20	20	20	20	20	20	20	20	20	20
Integrated Wireless	Integrated 802.11a/b/g/n available for Firebox T10-W. Integrated 802.11a/b/g/n/ac is available for Firebox T35-W and T55-W											
Operating System Features												
General	Integrated 802.11a/b/g/n available for Firebox T10-W. Integrated 802.11a/b/g/n/ac is available for Firebox T35-W and T55-W/Operating											
Advanced Networking	Dynamic routing (BGP, OSPF, RIPv1,2) / SD-WAN dynamic path selection / NAT: static, dynamic, 1:1, IPSec traversal, policy-based PAT / Traffic shaping & QoS: 8 priority queues, DiffServ, modified strict queuing / Virtual IP for server load balancing											
Availability	High availability - active/passive, and active/active for clustering (not available on wireless models) / VPN failover / Multi-WAN failover / Multi-WAN load balancing / Link aggregation (802.3ad dynamic, static, active/backup)											
Security Services												
Basic Security Suite	Application Control / Intrusion Prevention Service / WebBlocker / Gateway AntiVirus / Reputation Enabled Defense / Network Discovery / spamBlocker / Standard Support (24 x 7)											
Total Security Suite	Application Control / Intrusion Prevention Service / WebBlocker / Gateway AntiVirus / Reputation Enabled Defense / Network Discovery / spamBlocker / Data Loss Prevention / APT Blocker / Threat Detection and Response / DNSWatch / Access Portal**** / IntelligentAV**** / Dimension Command / Gold Support (24 x 7, plus escalated response time)											
Management Upgrades	Dimension Command is a suite of management tools for WatchGuard Dimension that allows administrators to manage policies directly from Dimensions visibility dashboards, create VPNs, roll back configurations, and more. Included in Total Security Suite											

*Firebox T35-R is a rugged, IP65-rated device designed for harsh environment.
 **Firebox M470, M570 and M670 ship with one empty bay that can accommodate one of the following: 4 x 10 Gb fiber, 8 x 1 Gb fiber, or 8 x 1 Gb copper.
 ***Firebox M5600 and M4600 throughput rates are determined using base configuration + 4 x 10 Gb ports. Both models ship with two empty bays that can accommodate any combination of the following: 4 x 10 Gb fiber, 8 x 1 Gb fiber, 8 x 1 Gb copper, 2 x 40 Gb fiber.
 ****Available on latest generation M Series appliances

EDITAL:

6.9.2. Possibilitar autenticação via LDAP, Active Directory, Radius, eDirectory, TACACS+ e via base de dados local, para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;

O produto ofertado não atende integralmente ao item, uma vez que a integração com TACACS+ não é suportada pelo produto, conforme documentação enviada pela licitante GlobalTTI (documentos: “Datasheet_firebox_M4600_M5600.pdf” e “Datasheet_firebox_M470_M570-670.pdf”). Veja-se:

VPN & AUTHENTICATION

Cloud providers	AWS (Static/Dynamic), Azure (Static/Dynamic)
Encryption	AES 256-128 bit, 3DES, DES
IPSec	SHA-2, IKEv1/v2, IKE pre-shared key, 3rd party cert, Suite B
Single sign-on	Windows, Mac OS X, mobile operating systems, SAML 2.0, RADIUS
Authentication	RADIUS, LDAP, Windows Active Directory, VASCO, RSA SecurID, internal database, SAML 2.0, SMS Passcode

Mesmo com diligência para esclarecer as informações, ainda assim é muito claro que a oferta não atende aos requisitos solicitados, conforme matriz do produto em que não se menciona a possibilidade de autenticação em TACACS+ e nem eDirectory. Veja-se a informação constante do seguinte link: <<https://www.watchguard.com/wgrd-resource-center/docs/watchguard-product-matrix-en>>.

EDITAL:

6.9.4. Deve permitir autenticação em modos: transparente, autenticação proxy (NTLM e Kerberos) e autenticação via clientes nas estações com os sistemas operacionais Windows, MAC OS X e Linux 32/64.

Não há informações que comprovem o atendimento ao item. Tal evidência indica não atendimento ao subitem 14.1.2 do edital, segundo o qual se exige “Catálogo (s), folheto(s) e manual(is), deverão estar preferencialmente na língua portuguesa com especificações técnicas detalhadas da solução ofertada, para comprovação de características técnicas obrigatórias, informando, inclusive, marca, modelo, tipo, fabricante e procedência da solução, detalhados de forma clara, evitando-se jargões de uso duvidoso ou ainda não consagrados na terminologia de informática” (grifo nosso).

Mesmo que se realizasse diligência, é muito claro que a oferta não atende aos requisitos solicitado, eis que a matriz do produto não menciona a possibilidade de autenticação em NTLM e Kerberos, como se vê no seguinte link: <<https://www.watchguard.com/wgrd-resource-center/docs/watchguard-product-matrix-en>>.

VPN & AUTHENTICATION

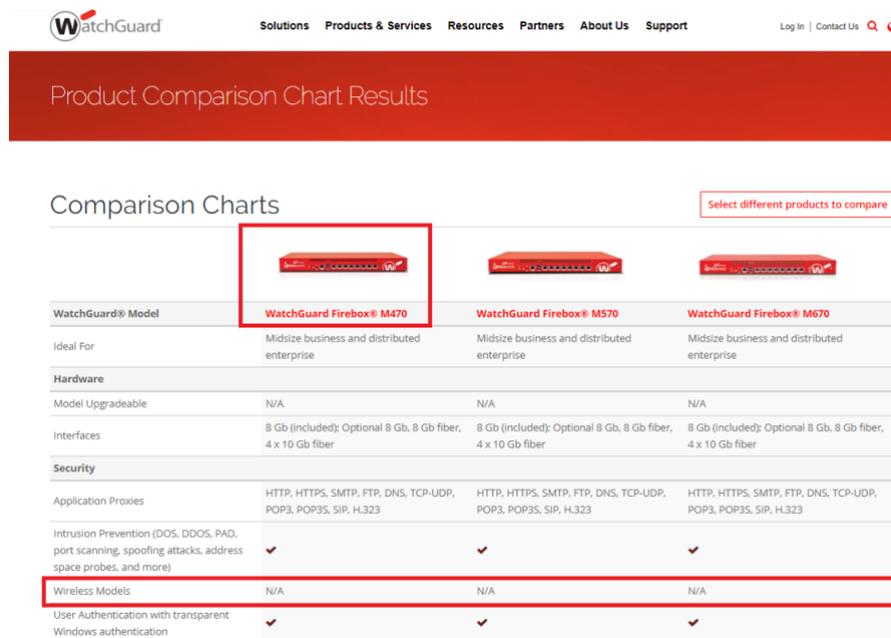
Cloud providers	AWS (Static/Dynamic), Azure (Static/Dynamic)
Encryption	AES 256-128 bit, 3DES, DES
IPSec	SHA-2, IKEv1/v2, IKE pre-shared key, 3rd party cert, Suite B
Single sign-on	Windows, Mac OS X, mobile operating systems, SAML 2.0, RADIUS
Authentication	RADIUS, LDAP, Windows Active Directory, VASCO, RSA SecurID, internal database, SAML 2.0, SMS Passcode

EDITAL:

6.1.7. Possuir Wireless com padrão 802.11a/b/g/n/ac (2.4 GHz / 5 GHz);

Analisando a documentação do produto, o equipamento M470, informado na proposta da licitante GlobalTTI, NÃO possui wireless com padrão 802.11a/b/g/n/ac (2.4 GHz / 5 GHz) em seu EQUIPAMENTO NGFW TIPO – 1, conforme exigido no item do edital. Isso pode ser constatado pela informação disponível no seguinte link: <<https://www.watchguard.com/wgrd-products/appliances-compare/15021/15026/15031>>.

Veja-se a cópia da tela abaixo:



The screenshot shows the WatchGuard website's product comparison chart. The 'Comparison Charts' section is active, and the 'WatchGuard Firewall® M470' is selected and highlighted with a red box. Below the product names is a table comparing features across three models: M470, M570, and M670. The 'Wireless Models' row is also highlighted with a red box, showing 'N/A' for all three models.

WatchGuard® Model	WatchGuard Firewall® M470	WatchGuard Firewall® M570	WatchGuard Firewall® M670
Ideal For	Midsize business and distributed enterprise	Midsize business and distributed enterprise	Midsize business and distributed enterprise
Hardware			
Model Upgradeable	N/A	N/A	N/A
Interfaces	8 Gb (included); Optional 8 Gb, 8 Gb fiber, 4 x 10 Gb fiber	8 Gb (included); Optional 8 Gb, 8 Gb fiber, 4 x 10 Gb fiber	8 Gb (included); Optional 8 Gb, 8 Gb fiber, 4 x 10 Gb fiber
Security			
Application Proxies	HTTP, HTTPS, SMTP, FTP, DNS, TCP-UDP, POP3, POP3S, SIP, H.323	HTTP, HTTPS, SMTP, FTP, DNS, TCP-UDP, POP3, POP3S, SIP, H.323	HTTP, HTTPS, SMTP, FTP, DNS, TCP-UDP, POP3, POP3S, SIP, H.323
Intrusion Prevention (DOS, DDOS, PAD, port scanning, spoofing attacks, address space probes, and more)	✓	✓	✓
Wireless Models	N/A	N/A	N/A
User Authentication with transparent Windows authentication	✓	✓	✓

Evidente, novamente, o não atendimento ao edital.

EDITAL:

6.5.1.1. Por funcionalidades de proteção de rede e próxima geração entende-se: reconhecimento e controle granular de aplicações, prevenção de ameaças, identificação de usuários, IPS, Firewall, Antispam, VPN IPsec, SSLVPN e SSL Inspection;

A licitante recorrente não informou qual licenciamento seria fornecido com os equipamentos, o que impede que se constate o atendimento ao item do edital.

EDITAL:

6.5.1.6.1. **Suporte a, no mínimo, 1024 VLAN Tags 802.1q**, policy based routing ou policy based forwarding, roteamento multicast (PIM-SM), DHCP Relay, DHCP Server;

Os equipamentos **M470** e **M4600** ofertados na proposta **NÃO** atendem ao quantitativo de 1024 VLAN exigido neste item, como se pode ver no sítio do próprio fabricante nas colunas dos produtos M470 e **M4600**, linha VLAN, **que informam atendimento a somente 300 VLANs e 1000 VLANs**. Veja-se a informação disponível em: <https://www.watchguard.com/wgrd-resource-center/docs/watchguard-product-matrix-en-para-o-Tipo-1>:



	Firebox T15/T15-W	Firebox T35/T35-W/T35-R*	Firebox T55/T55-W	Firebox T70	Firebox M270	Firebox M370	Firebox M440	Firebox M470	Firebox M570	Firebox M670	Firebox M4600 base + 4 x 10-Gb-ports	Firebox M5600 base + 4 x 10-Gb-ports
Throughput and Connections												
Firewall throughput	400 Mbps	940 Mbps	1 Gbps	4 Gbps	4.9 Gbps	8 Gbps	6.7 Gbps	19.6 Gbps	26.6 Gbps	34 Gbps	40 Gbps	60 Gbps
VPN throughput	150 Mbps	360 Mbps	360 Mbps	740 Mbps	1.6 Gbps	4.6 Gbps	3.2 Gbps	5.2 Gbps	5.8 Gbps	7.6 Gbps	10 Gbps	10 Gbps
AV throughput	120 Mbps	325 Mbps	636 Mbps	1.2 Gbps	2.1 Gbps	3.0 Gbps	2.2 Gbps	3.5 Gbps	5.4 Gbps	6.2 Gbps	9 Gbps	12 Gbps
IPS throughput	160 Mbps	573 Mbps	636 Mbps	1.5 Gbps	2.3 Gbps	4.8 Gbps	2.2 Gbps	5.7 Gbps	8.0 Gbps	10.4 Gbps	13 Gbps	18 Gbps
UTM throughput	90 Mbps	278 Mbps	523 Mbps	1.1 Gbps	1.6 Gbps	2.6 Gbps	1.6 Gbps	3.1 Gbps	4.4 Gbps	5.4 Gbps	8 Gbps	11 Gbps
Interfaces	3 x 1Gb	5 ^o x 1 Gb	5 ^o x 1 Gb	8 x 1 Gb	8 x 1 Gb	8 x 1 Gb	25 x 1 Gb copper ^o 2 x 10 Gb SFP+	8**	8**	8**	8 x 1 Gb additional ports available***	8 x 1 Gb + 4 x 10 Gb fiber additional ports available***
VO Interfaces	1 Serial / 1 USB	1 Serial / 2 USB	1 Serial / 2 USB	1 SBL/2 USB	1 SBL/2 USB	1 Serial / 2 USB	1 Serial / 2 USB	1 Serial / 2 USB	1 Serial / 2 USB	1 Serial / 2 USB	1 Serial / 2 USB	1 Serial / 2 USB
Concurrent connections	95,000	135,000	135,000	800,000	2,000,000	3,300,000	4,000,000	3,800,000	8,300,000	8,500,000	7,500,000	12,700,000
New connections per second	2,400	6,800	9,500	27,000	40,000	51,000	62,000	82,000	115,000	140,000	160,000	240,000
VLAN support	10	50	75	75	100	200	400	300	500	750	1,000	Unrestricted
Authenticated users limit	200	500	500	500	500	500	Unrestricted	Unrestricted	Unrestricted	Unrestricted	Unrestricted	Unrestricted
VPN Tunnels												
Branch Office VPN	5	25	40	50	50	100	300	250	500	750	5,000	Unrestricted
Mobile VPN IPsec	5	25	50	60	75	100	300	250	500	750	10,000	Unrestricted
Wireless												
Wireless Access Points (APs)	WatchGuard offers a family of AP devices that allow all Firebox security capabilities to be extended to the WLAN. APs can be managed in the WiFi Cloud or through the Firebox's built-in wireless controller. For managing more than 20 APs, WatchGuard recommends WiFi Cloud. More info at watchguard.com/wifi											
Max APs advised per model	4	20	20	20	20	20	20	20	20	20	20	20
Integrated Wireless	Integrated 802.11a/b/g/n available for Firebox T10-W. Integrated 802.11a/b/g/n/ac is available for Firebox T35-W and T55-WD operating											
Operating System Features												
General	Integrated 802.11a/b/g/n available for Firebox T10-W. Integrated 802.11a/b/g/n/ac is available for Firebox T35-W and T55-WD operating											
Advanced Networking	Dynamic routing (RIP, OSPF, RIPv1,2) / SD-WAN dynamic path selection / NAT: static, dynamic, 1:1, IPsec traversal, policy-based PAT / Traffic shaping & QoS 8 priority queues, DiffServ, modified strict queuing / Virtual IP for server load balancing											
Availability	High availability - active/passive, and active/active for clustering (not available on wireless models) / VPN failover / Multi-WAN failover / Multi-WAN load balancing / Link aggregation (802.3ad dynamic, static, active/backup)											
Security Services												
Basic Security Suite	Application Control / Intrusion Prevention Service / WebBlocker / Gateway AntiVirus / Reputation Enabled Defense / Network Discovery / spamBlocker / Standard Support (24 x 7)											
Total Security Suite	Application Control / Intrusion Prevention Service / WebBlocker / Gateway AntiVirus / Reputation Enabled Defense / Network Discovery / spamBlocker / Data Loss Prevention / APT Blocker / Threat Detection and Response / DNSWatch / Access Portal**** / IntelligentAV**** / Dimension Command / Gold Support (24 x 7, plus escalated response time)											
Management Upgrades	Dimension Command is a suite of management tools for WatchGuard Dimension that allows administrators to manage policies directly from Dimension's visibility dashboards, create VPNs, roll back configurations, and more (Included in Total Security Suite)											

EDITAL:

6.5.1.20. A solução deve permitir o tráfego de cotas baseados por usuários para upload/download e pelo tráfego total, sendo cíclicas ou não-cíclicas.

Contrariamente ao solicitado no edital, não é possível customizar cotas para upload/download. A solução ofertada realiza cotas apenas para tráfego total, desatendendo claramente à solicitação técnica do edital. Essa informação pode ser conferida no seguinte link:

https://www.watchguard.com/help/docs/help-center/en-US/Content/en-US/Fireware/policies/quota_about_c.html?tocpath=Fireware%7CFireware%20Help%7CControl%20Network%20Traffic%7CPolicies%7CAbout%20Quotas%7C_____0.

EDITAL:

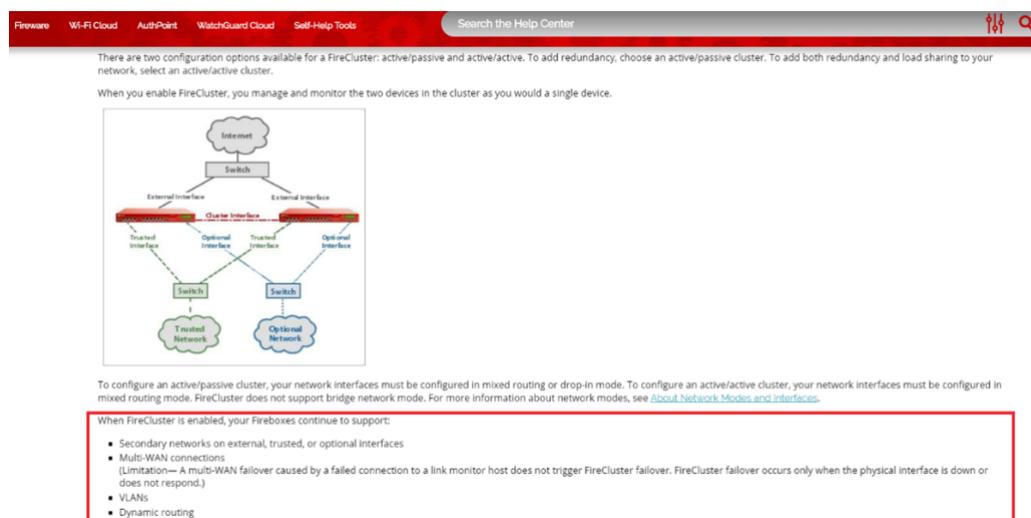
6.5.1.24. O HA (modo de alta disponibilidade) deve suportar o uso de dois equipamentos em modo ativo-passivo ou modo ativo-ativo e deve possibilitar monitoração de falha de link

A solução ofertada possui limitação na monitoração de link ao utilizar cluster, conforme informação do fabricante, cujo site aponta a seguinte informação:

Limitation— A multi-WAN failover caused by a failed connection to a link monitor host does not trigger FireCluster failover. FireCluster failover occurs only when the physical interface is down or does not respond.

Esse dado está disponível no seguinte link:

https://www.watchguard.com/help/docs/help-center/en-US/Content/en-US/Fireware/ha/cluster_about_wsm.html?tocpath=Configure%20Network%20Settings%7CFireCluster%7C_____0. Veja-se a imagem:



Fica claro, assim, o não atendimento às exigências do edital de licitação.

EDITAL:

6.5.1.27. O sistema de objetos deverá permitir a definição de redes, serviços, hosts períodos de tempos, usuários e grupos, clientes e servidores.

Não foram encontradas informações sobre os objetos citados acima na documentação técnica enviada pela licitante Global TTI, e não foi possível localizar no site do fabricante (documentação disponível em: <<https://www.watchguard.com/wgrd-support/find-answers/technical-documentation>>).

EDITAL:

6.6.2. O controle de políticas deverá monitorar as políticas de redes, usuários, grupos e tempo, bem como identificar as regras não-utilizadas, desabilitadas, modificadas e novas políticas.

Não foram encontradas informações sobre os objetos citados acima na documentação técnica enviada pela licitante Global TTI, e não foi possível localizar no site do fabricante (documentação disponível em: <<https://www.watchguard.com/wgrd-support/find-answers/technical-documentation>>).

EDITAL:

6.7.3.2. Reconhecer pelo menos 2.000 (dois mil) aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, *update* de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;

O fabricante da solução traz a seguinte informação em seu site (informação disponível em: <https://www.watchguard.com/help/docs/help-center/en-US/Content/en-US/Fireware/services/app_control/app_control_intro_c.html?tocpath=Manage%20Security%20Services%7CApplication%20Control%7C_____0>):

Application Control uses signatures that can identify and block over 1800 applications.

O que o fabricante indica é que a solução ofertada suporta mais de 1800 aplicações, o que não deixa claro o atendimento ao item, uma vez que é solicitado o suporte a pelo menos 2000 aplicações.

Veja-se a imagem do site do fabricante:



[Fireware](#) > [Fireware Help](#) > [Manage Security Services](#) > [Application Control](#)

Application Control

Application Control is a subscription service that enables you to monitor and control the use of applications on your network. Application Control uses signatures that can identify and block over 1800 applications. In the Application Control action, you select the applications by name, and choose to block or allow traffic for each application or application category. Then you apply the Application Control action to the applicable policy.

For more information, see:

- [About Application Control](#)
- [How Application Control Identifies Applications](#)
- [Policy Guidelines for Application Control](#)
- [Configure Application Control for Policies](#)
- [Global Application Control Action](#)
- [Configure Application Control Actions](#)
- [Enable Application Control in a Policy](#)
- [Configure the Application Control Update Server](#)
- [Monitor Application Control](#)
- [Troubleshoot Application Control](#)
- [Get Information About Applications](#)

[Give Us Feedback](#) • [Get Support](#) • [All Product Documentation](#) • [Technical Search](#)

© 2016 WatchGuard Technologies, Inc. All rights reserved. WatchGuard and the WatchGuard logo are registered trademarks or trademarks of WatchGuard Technologies in the United States and/or other countries. All other trademarks are the property of their respective owners.

EDITAL:

6.7.3.3. Reconhecer micro app como: Facebook (Applications, Chat, Commenting, Events, Games, Like Plugin, Message, Pics Download e Upload, Plugin, Post Attachment, Posting, Questions, Status Update, Video Chat, Video Playback, Video Upload, Website), Freerate Proxy, Gmail (Android Application, Attachment), Google Drive (Base, File Download, File Upload), Google Earth Application, Google Plus, LinkedIn (Company Search, Compose Webmail, Job Search, Mail Inbox, Status Update), SkyDrive File Upload e Download, Twitter (Message, Status Update, Upload, Website), Yahoo (WebMail, WebMail File Attach) e Youtube (Video Search, Video Streaming, Upload, Website), não limitando-se somente a estes.

Não foram encontradas informações sobre os objetos citados acima na documentação técnica enviada pela licitante Global TTI, e não foi possível localizar no site do fabricante (documentação disponível em: <https://www.watchguard.com/wgrd-support/find-answers/technical-documentation>).

EDITAL:

6.8.1.4. Possuir pelo menos 90 categorias de URLs;

Não foram encontradas informações sobre os objetos citados acima na documentação técnica enviada pela licitante Global TTI. Verificando o site do fabricante, no campo/documento "Help Center", não foi possível identificar quantidade de categorias mínima exigida no item (90 categorias de URLs). Isso pode ser visto no seguinte link: https://www.watchguard.com/help/docs/help-center/en-US/Content/en-US/Fireware/services/webblocker/categories_to_block_select_c.html?Highlight=category%20Urls:



Fireware > Fireware Help > Manage Security Services > WebBlocker > About WebBlocker

About WebBlocker

If you give users unlimited website access, your company can suffer lost productivity and reduced bandwidth. Uncontrolled internet browsing can also increase security risks and legal liability. The WebBlocker security subscription gives you control of the websites that are available to your users.

WebBlocker uses a database that groups website addresses into content categories. When a user on your network tries to connect to a website, the Firewall looks up the address in the WebBlocker database and takes the action you specify for the content category. You can also specify the action WebBlocker takes for uncategorized websites.

EDITAL:

6.8.1.9. Suportar a exclusão de URLs do bloqueio, por categoria;

A solução ofertada não atende ao item. Não é possível criar exclusão de URLs por categoria, conforme descrito no documento disponível em:

<https://www.watchguard.com/help/docs/help-center/en-US/Content/en-US/Fireware/services/webblocker/wb_exceptions_add_c.html>. Veja-se:



Fireware > Fireware Help > Manage Security Services > WebBlocker > About WebBlocker Exceptions > Configure WebBlocker Exceptions

Configure WebBlocker Exceptions

If you want WebBlocker to always allow or always deny access to a website, regardless of the content category, you can add a WebBlocker exception for that site. You can add a WebBlocker exception that is an exact match of a URL, a pattern match of a URL, or a regular expression.



WebBlocker does not include query strings (the part of a URL that starts with the ? character) in the categorization request it sends to the WebBlocker Server. This means that you cannot create a WebBlocker exception to deny specific queries.

Exact match

Exact matches match an exact URL or IP address, character by character. You cannot use wildcards, and you must type each character exactly as you want it to be matched. For example, if you enter an exception to allow `www.yahoo.com` as an exact match only, and a user types `www.yahoo.com/news`, the request is denied.

Pattern match

Pattern matches match a pattern in the URL or IP address, for example "pattern" in `www.pattern.com`. Make sure to drop the leading "http://" and include "/" at the end. Use the wildcard symbol, "*", to match any character. You can use more than one wildcard in one pattern. For example, the pattern `www.somesite.com/*` will match all URL paths on the `www.somesite.com` website. To enter a network address, use a pattern match that ends in a wildcard. For example, to match all the websites at 1.1.1.1 on port 8080, set the directory to `*:8080`.

Regular expression

Regular expression matches use a Perl-compatible regular expression to make a match. For example, `\.[a-z]{3}` matches `.org`, `.net`, `.com`, or any other three-letter combination of one letter from each bracket, in order. When you create a regular expression to match URL paths, do not include the leading "http://". Regular expressions support wildcards used in shell scripts. For example:

- The regular expression: `(www\.)?watchguard\.[a-z]{3}` matches URL paths such as `www.watchguard.com`, `www.watchguard.net`, `watchguard.com`, and `watchguard.net`.
- The regular expression: `1.1.1.[1-9]` matches all IP addresses from 1.1.1.1 to 1.1.1.9.



Regular expressions are more efficient than pattern matches, in terms of CPU usage. For best performance, we recommend that you use regular expressions rather than pattern matches to define your WebBlocker exceptions, when several exceptions are configured. You can create a regular expression that is equivalent to a pattern match. For example, the pattern match `*.hostname.com/*` is equivalent to the regular expression `^[0-9a-zA-Z\-_]{1,256}hostname\.com`.

For more information about regular expressions, see [About Regular Expressions](#).

EDITAL:

6.9.6. Deve possuir portal do usuário para que os usuários tenham acesso ao uso de internet pessoal, troquem senhas da base local e façam o download de softwares para as estações presentes na solução.

Não foram encontradas informações sobre os objetos citados acima na documentação técnica enviada pela licitante Global TTI, e não foi possível localizar no site

do fabricante (documentação disponível em: <<https://www.watchguard.com/wgrd-support/find-answers/technical-documentation>>).

EDITAL:

6.10.5. Bloquear ataques conhecidos, permitindo ao administrador acrescentar novos padrões de assinaturas e customizações;

A solução ofertada, não atende ao item, visto que não é possível customizar padrões de assinaturas, conforme informação disponível em: <https://www.watchguard.com/help/docs/help-center/en-US/Content/en-US/Fireware/services/ips/ips_intro_c.html?tocpath=Fireware%7CFireware%20Help%7CManage%20Security%20Services%7CIntrusion%20Prevention%20Service%7C_____0>.

EDITAL:

6.10.6. Exceções por usuário, grupo de usuários, IP de origem ou de destino devem ser possíveis nas regras;

A solução não atende ao item, pois não cria exceções nas regras, conforme solicitado no item. A exceção é criada na assinatura de IPS. Veja-se a informação em: <https://www.watchguard.com/help/docs/help-center/en-US/Content/en-US/Fireware/services/ips/ips_config_exceptions_c.html>.

EDITAL:

6.12.4. Suportar L2TP e PPTP.

Não foram encontradas informações sobre os objetos citados acima na documentação técnica enviada pela licitante Global TTI, e não foi possível localizar no site do fabricante (documentação disponível em: <<https://www.watchguard.com/wgrd-support/find-answers/technical-documentation>>).

EDITAL:

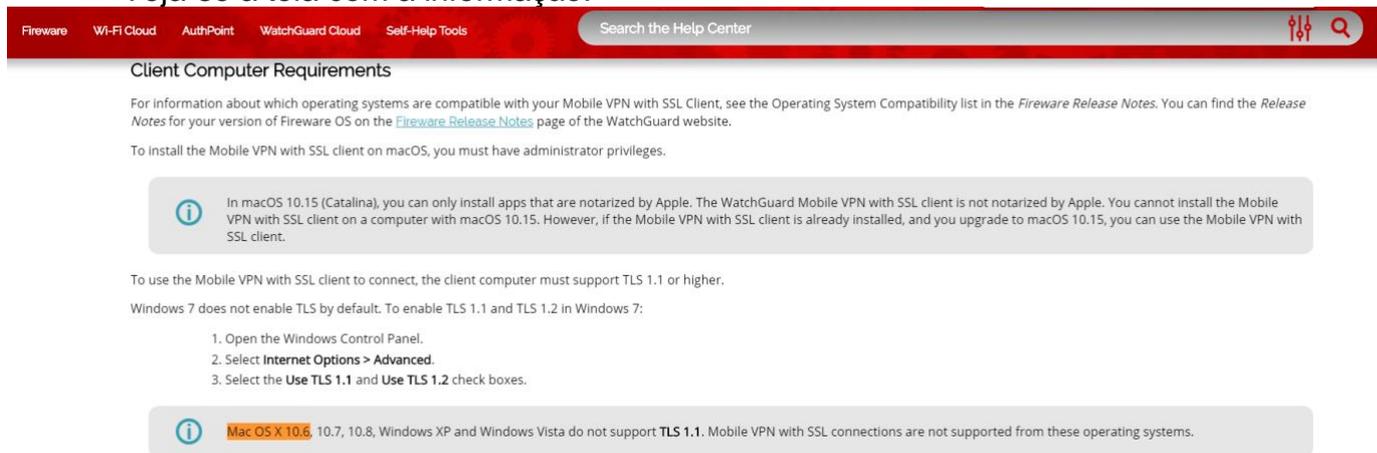
6.12.6.7. O agente de VPN SSL client-to-site deve ser compatível com pelo menos: Windows XP, Vista, Windows 7, Windows 8, Windows 10 e MacOS X;

Cliente de VPN SSL não é suportada pelos sistemas operacionais MacOS X10.6, 10.7, 10.8, Windows XP e Windows Vista, conforme documentação do fabricante. No link disponível em: <<https://www.watchguard.com/help/docs/help-center/en-US/Content/en->

US/Fireware/mvpn/ssl/mvpn_ssl_client-install_c.html#sysreqs>, consta a seguinte informação:

Mac OS X 10.6, 10.7, 10.8, Windows XP and Windows Vista do not support **TLS 1.1**. Mobile VPN with SSL connections are not supported from these operating systems.

Veja-se a tela com a informação:



The screenshot shows the 'Client Computer Requirements' page in the WatchGuard Help Center. The page header includes navigation links for Fireware, Wi-Fi Cloud, AuthPoint, WatchGuard Cloud, and Self-Help Tools, along with a search bar and a user profile icon. The main content area is titled 'Client Computer Requirements' and contains the following text:

For information about which operating systems are compatible with your Mobile VPN with SSL Client, see the Operating System Compatibility list in the *Fireware Release Notes*. You can find the *Release Notes* for your version of Fireware OS on the [Fireware Release Notes](#) page of the WatchGuard website.

To install the Mobile VPN with SSL client on macOS, you must have administrator privileges.

i In macOS 10.15 (Catalina), you can only install apps that are notarized by Apple. The WatchGuard Mobile VPN with SSL client is not notarized by Apple. You cannot install the Mobile VPN with SSL client on a computer with macOS 10.15. However, if the Mobile VPN with SSL client is already installed, and you upgrade to macOS 10.15, you can use the Mobile VPN with SSL client.

To use the Mobile VPN with SSL client to connect, the client computer must support TLS 1.1 or higher.

Windows 7 does not enable TLS by default. To enable TLS 1.1 and TLS 1.2 in Windows 7:

1. Open the Windows Control Panel.
2. Select **Internet Options > Advanced**.
3. Select the **Use TLS 1.1** and **Use TLS 1.2** check boxes.

i **Mac OS X 10.6**, 10.7, 10.8, Windows XP and Windows Vista do not support **TLS 1.1**. Mobile VPN with SSL connections are not supported from these operating systems.

EDITAL:

6.12.6.9. Permitir estabelecer um túnel SSL VPN com uma solução de autenticação via LDAP, Active Directory, Radius, eDirectory, TACACS+ e via base de dados local;

A solução não suporta integração com TACACS+ e nem eDirectory, conforme já mencionado nos comentários ao subitem 6.9.2. Veja-se a informação constante da documentação encaminhada pela licitante (página 2 dos documentos “Datasheet_firebox_M4600_M5600.pdf” e “Datasheet_firebox_M470_M570-670.pdf”).

EDITAL:

6.13.11. Deve ter controle das alterações feitas por usuários administrativos, comparar diferentes versões de configurações e realizar o processo de roll back de configurações para mudanças indesejadas;

Não foram encontradas informações sobre os objetos citados acima na documentação técnica enviada pela licitante Global TTI, e não foi possível localizar no site do fabricante (documentação disponível em: <<https://www.watchguard.com/wgrd-support/find-answers/technical-documentation>>).

EDITAL:

6.14.9. Deve fornecer relatórios de compliance SOX, HIPAA e PCI.

A solução ofertada para gerenciamento de logs não atende ao item, pois não possui relatório de compliance SOX (Sarbanes-Oxley), conforme documentação do fabricante disponível em: <https://www.watchguard.com/help/docs/help-center/en-US/Content/en-US/Fireware/dimension/reports_report-list_d.html?Highlight=compliance>.

EDITAL:

6.14.11. Deve fornecer relatórios sobre os acessos de procura no Google, Yahoo, Bing e Wikipedia.

Não foram encontradas informações sobre os objetos citados acima na documentação técnica enviada pela licitante Global TTI, e não foi possível localizar no site do fabricante (documentação disponível em: <<https://www.watchguard.com/wgrd-support/find-answers/technical-documentation>>).

EDITAL:

6.14.12. Deve fornecer relatórios de tendências.

Não foram encontradas informações sobre os objetos citados acima na documentação técnica enviada pela licitante Global TTI, e não foi possível localizar no site do fabricante (documentação disponível em: <<https://www.watchguard.com/wgrd-support/find-answers/technical-documentation>>).

Por todos esses motivos, pugna-se pelo desprovisionamento do recurso.

3 CONCLUSÃO

Diante do exposto, pugna-se pelo desprovisionamento do recurso administrativo, mantendo-se a declaração de vitória da recorrida na licitação, além das sanções decorrentes do caráter procrastinatório do recurso apresentado pela recorrente, na medida da lei.

Nesses Termos,
Pede Deferimento.
Brasília, 11 de novembro de 2019.

DFTI COMÉRCIO E SERVIÇOS DE INFORMÁTICA LTDA.
CNPJ/MF: 09.650.283/0001-91