



# Proposta Comercial

**Cliente**

MINISTÉRIO DO  
PLANEJAMENTO,  
DESENVOLVIMENTO E  
GESTÃO - MPOG

**Projeto**

Solução lote 2 - Edital  
05/2017

**Validade**

90 dias

São Paulo, 03 de Outubro de 2017

**AMÉRICA LATINA**

Rua Eng. Francisco Piza 8000 CEP - 2º andar  
São Paulo - SP - 04756-000 - Brasil  
Fone: +55 11 3055 8000

**AMÉRICA DO NORTE**

701 Waterford Way - 4th floor  
Miami - FL 33176 - United States  
Phone: +1 305 479 4662

**EUROPA**

2 Kingsdon Street - 8th floor  
Paddington - London - W2 6BD - England  
Phone: +44 2011 340 4071

Ao  
MINISTÉRIO DO PLANEJAMENTO, DESENVOLVIMENTO E GESTÃO  
SECRETARIA DE GESTÃO  
DEPARTAMENTO DE AQUISIÇÕES

Referência: Pregão Eletrônico nº 05/2017  
Processo: 04300.0204177/2015-44  
Tipo: PREGÃO ELETRÔNICO  
Abertura: 03/10/2017 às 10hs  
Proponente: Blockbit Tecnologia Ltda.  
CNPJ: 02.423.535/0001-09

Prezados(as) Senhores(as),

A **Blockbit Tecnologia Ltda.**, vem pela presente apresentar Proposta de Preços para Registro de Preços para eventual aquisição, de soluções de segurança de redes compostas de firewall corporativo e multifuncional para prover segurança e proteção da rede de computadores, contemplando gerência unificada com garantia de funcionamento pelo período de 60 (sessenta) meses, incluindo todos os softwares e suas licenças de uso, gerenciamento centralizado, serviços de implantação, garantia de atualização contínua e suporte técnico durante o período de garantia com repasse de conhecimento da solução a fim de atender às necessidades dos contratantes.

ITEM	DESCRIÇÃO	PÁGINA
1.	PROPOSTA COMERCIAL	02-03
2.	DECLARAÇÃO DE CUMPRIMENTO DA LEI 12305	04
3.	DECLARAÇÃO DE NÃO UTILIZAÇÃO DE PRODUTOS	05
4.	DECLARAÇÕES COMPLEMENTARES	06 e 07
5.	ESPECIFICAÇÃO TÉCNICA – Lote 2	08 - 27
6.	COMPROVAÇÃO PONTUAL – Lote 2	28 - 50
7.	SÍLIO NA INTERNET DO FABRICANTE	51
8.	DECLARAÇÃO DO FABRICANTE	52 e 53
9.	ESCOPO DO SERVIÇO DE INSTALAÇÃO	54 e 55
10.	FOLHA DE ENCERRAMENTO	66

Ressaltamos que estamos cientes das condições do presente certame, assumimos total responsabilidade pela autenticidade de todos os documentos apresentados, forneceremos quaisquer informações complementares solicitadas pelo **MINISTÉRIO DO PLANEJAMENTO, DESENVOLVIMENTO E GESTÃO** e tomaremos todas as medidas para assegurar um controle de qualidade adequado.

Atenciosamente,

Brasília/DF, 03 de outubro de 2017

  
**Blockbit Tecnologia Ltda**  
CNPJ Nº 02.423.535/0001-09  
Inscrição Estadual: 115.395.122.119  
Cleber Ribas de Oliveira  
Vice-Presidente  
RG: 0912795-0 SSP/MT  
CPF: 788.962.231-72

Ao  
MINISTÉRIO DO PLANEJAMENTO, DESENVOLVIMENTO E GESTÃO  
SECRETARIA DE GESTÃO  
DEPARTAMENTO DE AQUISIÇÕES

Referência: Pregão Eletrônico nº 05/2017  
Processo: 04300.0204177/2015-44  
Tipo: PREGÃO ELETRÔNICO  
Abertura: 03/10/2017 às 10hs  
Proponente: Blockbit Tecnologia Ltda.  
CNPJ: 02.423.535/0001-09

A empresa **Blockbit Tecnologia Ltda.**, inscrita no CNPJ sob o nº 02.423.535/0001-09, sediada à Rua Engenheiro Francisco Pitta Brito, 779 – 3º andar - Lado A - Jardim Promissão - São Paulo – SP - CEP: 04753-080, por intermédio de seu representante legal, vem apresentar sua Proposta de Preços.

**PROPOSTA COMERCIAL**

Item	Descrição	Quantidade	Valor Unitário (R\$)	Valor Total (R\$)
Item 8	Firewall multifuncional Tipo 2 – BLOCKBIT UTM BB 100 – BBHWUTM028	94	R\$ 29.000,00	R\$ 2.726.000,00
Item 9	Conjunto de funcionalidades IPS/IDS do FW Tipo 2 – UTM Subscription – IPS/IDS – BBHWUTM327	92	R\$ 2.500,00	R\$ 230.000,00
Item 10	Conjunto de funcionalidades antivírus e anti-malware do FW Tipo 2 – UTM Subscription – AV/AM – BBHWUTM328	92	R\$ 2.800,00	R\$ 257.600,00
Item 11	Conjunto de funcionalidades para tratamento de conteúdo web do FW Tipo 2 – UTM Subscription – WF – BBHWUTM329	92	R\$ 2.800,00	R\$ 257.600,00
Item 12	Conjunto de funcionalidades para controle de aplicações e análise profunda do FW Tipo 2 – UTM Subscription – AC/DFI – BBHWUTM330	92	R\$ 2.500,00	R\$ 230.000,00
Item 13	Treinamento oficial até 5 pessoas do FW Tipo 2 BLOCKBIT Treinamento UTM – BB100 – BBSSR00332	22	R\$ 9.000,00	R\$ 198.000,00
Item 14	Solução de gerência centralizada do FW Tipo 2 BLOCKBIT GSM – BBVGSM333	20	R\$ 500,00	R\$ 10.000,00
<b>TOTAL</b>				<b>R\$ 3.909.200,00</b>

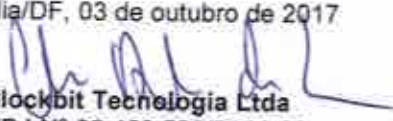
1. Os equipamentos serão entregues em no máximo 60 (sessenta) dias corridos, contados a partir da emissão da ordem de serviço, nos endereços indicados pela Contratante, acondicionados em caixas e embalagens adequadas, a fim de evitar avarias e deteriorações durante o percurso do transporte e estarão sujeitos a aceitação, à qual caberá o direito de recusa, caso os equipamentos não estejam de acordo com o especificado no Edital;



2. Declaramos que aceitamos os acréscimos ou supressões até o limite de 25% (vinte e cinco por cento) sobre as quantidades individuais registradas, de acordo com o disposto no § 1º do artigo 65 da Lei nº 8.666/93, caso venhamos a ser considerada vencedora do certame.
4. Declaramos que nos responsabilizamos pelo ônus e a logística da retirada e devolução dos equipamentos para realização de serviços de garantia, bem como da substituição de equipamentos não aceitos, cabendo à CONTRATANTE a emissão de documento fiscal ou equivalente necessário ao transporte do equipamento, quando for o caso.
5. Declaramos que nos responsabilizamos pelo fornecimento dos itens, objeto do Contrato, respondendo administrativa, civil e criminalmente por todos os danos, perdas e prejuízos que, por dolo ou culpa sua, de seus empregados, prepostos, ou terceiros no exercício de suas atividades, vier a, direta ou indiretamente, causar ou provocar à CONTRATANTE e a terceiros.
6. Declaramos fornecer o objeto para o qual se sagrar vencedora, em estrita conformidade com as especificações e condições exigidas no Termo de Referência, bem como naquelas resultantes de sua proposta, devendo já estar inclusos nos valores propostos todos os custos, impostos, taxas e demais encargos pertinentes à execução do objeto do contrato. Não sendo aceitas quaisquer modificações.
7. Declaramos que a garantia da solução ofertada, incluindo hardware, atualização de software e firmware é de 60 (sessenta) meses.

Validade da Proposta:	90 (noventa) dias a contar da data do recebimento dos envelopes		
Empresa:	BLOCKBIT TECNOLOGIA LTDA		
CNPJ:	02.423.535/0001-09	Insc. Estadual:	115.395.122.119
Endereço:	Rua Engenheiro Francisco Pitta Brito, 779 - 3º andar - Lado A - Jardim Promissão - São Paulo - SP - CEP: 04753-080		
Telefone/Fax:	(11) 21658888	E-mail:	cribas@blockbit.com
Responsável pela assinatura do contrato	Cleber Ribas de Oliveira		
Banco:	Itaú	Agência:	2000
		C.Corrente:	38097-8

Brasília/DF, 03 de outubro de 2017

  
Blockbit Tecnologia Ltda  
CNPJ Nº 02.423.535/0001-09  
Inscrição Estadual: 115.395.122.119  
Cleber Ribas de Oliveira  
Vice-Presidente  
RG: 0912795-0 SSP/MT  
CPF: 788.962.231-72

Ao  
MINISTÉRIO DO PLANEJAMENTO, DESENVOLVIMENTO E GESTÃO  
SECRETARIA DE GESTÃO

REF.: PREGÃO ELETRÔNICO Nº 05/2017

**DECLARAÇÃO DE CUMPRIMENTO DA LEI Nº 12.305/2010**

**BLOCKBIT TECNOLOGIA LTDA.**, com sede na Rua Engenheiro Francisco Pitta Brito, nº 779, Conjunto 32, Lado A, Parte I, 3º andar, Santo Amaro, São Paulo – SP, CEP 04753-090, inscrita no CNPJ/MF nº 02.423.535/0001-09, DECLARA, sob as penas da lei e para os devidos fins, junto ao **MINISTÉRIO DO PLANEJAMENTO, DESENVOLVIMENTO E GESTÃO**, relativamente ao **EDITAL Nº 05/2017**, que providenciará a coleta dos equipamentos, objeto do fornecimento, quando e se for o caso, após cumprido o disposto no Decreto nº 99.658, de 30 de outubro de 1990, e disponibilizará mecanismo de logística reversa de amplitude nacional, que consistirá em instrumento de desenvolvimento econômico e social, caracterizado por um conjunto de ações, procedimentos e meios destinados a viabilizar a coleta e restituição dos resíduos sólidos ao setor empresarial, para reaproveitamento, em seu ciclo ou em outros ciclos produtivos, ou outra destinação final ambientalmente adequada, em conformidade com as diretrizes estabelecidas na Lei nº 12.305, de 2 de agosto de 2010, que instituiu a Política de Resíduos Sólidos

São Paulo, 03 de outubro de 2017.

  
**BLOCKBIT TECNOLOGIA LTDA.**

André Vieira Rolim

CPF/MF: 157.073.798-35

Ao  
MINISTÉRIO DO PLANEJAMENTO, DESENVOLVIMENTO E GESTÃO  
SECRETARIA DE GESTÃO

REF.: PREGÃO ELETRÔNICO Nº 05/2017

**DECLARAÇÃO DE NÃO UTILIZAÇÃO DE PRODUTOS PERIGOSOS E ADERÊNCIA  
AOS REQUISITOS DE SUSTENTABILIDADE AMBIENTAL**

**BLOCKBIT TECNOLOGIA LTDA.**, com sede na Rua Engenheiro Francisco Pitta Brito, nº 779, Conjunto 32, Lado A, Parte I, 3º andar, Santo Amaro, São Paulo – SP, CEP 04753-090, inscrita no CNPJ/MF nº 02.423.535/0001-09, DECLARA, sob as penas da lei e para os devidos fins, junto ao **MINISTÉRIO DO PLANEJAMENTO, DESENVOLVIMENTO E GESTÃO**, relativamente ao **EDITAL Nº 05/2017**, que no processo de fabricação/produção dos equipamentos cotados não há emprego de substâncias perigosas de acordo com as exigências do Edital.

São Paulo, 03 de outubro de 2017.

  
**BLOCKBIT TECNOLOGIA LTDA.**

André Vieira Rolim  
CPF/MF: 157.073.798-35



Ao  
**MINISTÉRIO DO PLANEJAMENTO, DESENVOLVIMENTO E GESTÃO**  
**SECRETARIA DE GESTÃO**  
**DEPARTAMENTO DE AQUISIÇÕES**

**Referência:** Pregão Eletrônico nº 05/2017  
**Processo:** 04300.0204177/2015-44  
**Tipo:** PREGÃO ELETRÔNICO  
**Abertura:** 03/10/2017 às 10hs  
**Proponente:** Blockbit Tecnologia Ltda.  
**CNPJ:** 02.423.535/0001-09

### **DECLARAÇÕES COMPLEMENTARES**

A empresa **Blockbit Tecnologia Ltda.**, inscrita no CNPJ sob o nº 02.423.535/0001-09, sediada à Rua Engenheiro Francisco Pitta Brito, 779 – 3º andar - Lado A - Jardim Promissão - São Paulo – SP - CEP: 04753-080, por intermédio de seu representante legal, DECLARA que:

1. Declaramos o pleno conhecimento e aceitação dos termos e condições do Edital e seus anexos, além da obrigação de cumpri-los fielmente, por sua conta e risco e pelos preços ora propostos, não cabendo nenhum acréscimo ou indenização posterior decorrentes de erro de cálculo em sua elaboração;
2. Declaramos ciência do dever de apresentar proposta atualizada, equalizada proporcionalmente, em até 48 (quarenta e oito) horas, caso sejamos vencedores do certame, exceto se outro prazo for fixado por motivos justificados e aceitos;
3. Declaramos ciência do compromisso em fornecer os bens e serviços objeto da presente licitação, em total conformidade com as especificações do Edital e seus anexos;
4. Cumpriremos fielmente o objeto do Edital, mediante o fornecimento em conformidade com as especificações constantes do Anexo B - Termo de Referência, de acordo com as condições propostas e consignadas no presente instrumento;
5. Corrigiremos, às suas expensas, no todo ou em parte, o objeto da Ata de Registro em que se verificarem erros ou vícios na execução, não atender as especificações ou, se for o caso, não estiver em conformidade com as amostras apresentadas;
6. Forneceremos diretamente o objeto deste edital, sem transferência de responsabilidades ou subcontratações não autorizadas pelo contratante;
7. Manteremos, durante a vigência da Ata de Registro, em compatibilidade com as obrigações ali assumidas todas as condições de habilitação e qualificação exigidas na licitação;
8. Responderemos por qualquer prejuízo que nossos empregados ou prepostos causarem ao patrimônio do contratante ou a terceiros, em virtude de ação ou omissão, culposa ou dolosa, procedendo imediatamente aos reparos ou às indenizações cabíveis e assumindo o ônus decorrente;
9. Assumiremos toda e qualquer responsabilidade pela imperfeição do objeto entregue;
10. Responderemos por toda responsabilidade solidária ou subsidiária;
11. Acataremos a fiscalização do serviço contratado, realizada pelo Gestor do contrato, que terá suas solicitações atendidas imediatamente;
12. Disponibilizaremos ao setor competente, telefones, fax, e-mail e outros meios de contato para atender às requisições;
13. Permitiremos e oferecemos condições para a mais ampla e completa fiscalização durante a vigência da Ata de Registro, fornecendo informações, propiciando o acesso à documentação pertinente e atendendo às observações e exigências do setor responsável pela fiscalização;

14. Assumiremos, com exclusividade, todos os impostos e taxas que forem devidos em decorrência dos fornecimentos, bem como as contribuições devidas à Previdência Social, encargos trabalhistas, prêmios de seguro e de acidentes de trabalho, além de quaisquer outras despesas que se fizerem necessárias ao cumprimento do objeto pactuado;
15. Aceitaremos nas mesmas condições avençadas, os acréscimos ou supressões nos valores adstritos aos quantitativos do ITEM adjudicado, em até 25% (vinte e cinco por cento);
16. Responsabilizaremos-nos por quaisquer ônus decorrentes de omissões ou erros na elaboração da estimativa de custos;
17. Assumiremos a responsabilidade e o ônus pelo recolhimento de todos os impostos, taxas, tarifas, contribuições ou emolumentos federais, estaduais e municipais que incidam ou venham a incidir sobre a execução da presente Ata de Registro, sendo apresentados os respectivos comprovantes quando solicitados pelo Ministério do Planejamento, Desenvolvimento e Gestão;
18. Responsabilizaremos-nos integralmente pelo objeto fornecido, nos termos da legislação vigente;
19. Forneceremos o objeto quando requisitado pelo setor competente, observando o preço unitário, o prazo, o local de entrega e as demais condições fixadas neste instrumento e no termo de referência;
20. Responsabilizaremos-nos integralmente pelos danos causados direta ou indiretamente à Administração ou a terceiros, decorrentes de culpa ou dolo na execução do fornecimento do objeto desta licitação, não excluindo ou reduzindo essa responsabilidade a fiscalização realizada pelo setor competente;
21. Seremos responsáveis pelo pagamento de mão-de-obra, encargos e obrigações trabalhistas, impostos, e todos os demais encargos que se fizerem necessário para a execução dos serviços;
22. Declaramos que estamos cientes de que a apresentação da nossa proposta implica obrigatoriedade do cumprimento das disposições nela contida, e assumimos o compromisso de executar os serviços nos seus termos, bem como fornecer todos os materiais, equipamentos, ferramentas e utensílios necessários, em quantidades e qualidades adequadas à perfeita execução contratual, promovendo, quando requerido, sua substituição;
23. Declaramos a inexistência de qualquer fato impeditivo à nossa participação no presente certame, bem como estamos cientes da obrigação de declarar quando ocorrido durante o certame;
24. Declaramos que estamos cientes de que a participação na presente licitação implica a concordância, com todos os termos e condições deste Edital.

Brasília/DF, 03 de outubro de 2017

  
**Blockbit Tecnologia Ltda**

**CNPJ Nº 02.423.535/0001-09**

**Inscrição Estadual: 115.395.122.119**

**Cleber Ribas de Oliveira**

**Vice-Presidente**

**RG: 0912795-0 SSP/MT**

**CPF: 788.962.231-72**



Ao  
MINISTÉRIO DO PLANEJAMENTO, DESENVOLVIMENTO E GESTÃO  
SECRETARIA DE GESTÃO  
DEPARTAMENTO DE AQUISIÇÕES

Referência: Pregão Eletrônico nº 05/2017  
Processo: 04300.0204177/2015-44  
Tipo: PREGÃO ELETRÔNICO  
Abertura: 03/10/2017 às 10hs  
Proponente: Blockbit Tecnologia Ltda.  
CNPJ: 02.423.535/0001-09  
Marca: BLOCKBIT  
Modelo: BB 100 - UTM

## ESPECIFICAÇÃO TÉCNICA – Lote 2

### 1. OBJETO:

Registro de preços para eventual aquisição, de soluções de segurança de redes compostas de firewall corporativo e multifuncional para prover segurança e proteção da rede de computadores, contemplando gerência unificada com garantia de funcionamento pelo período de 60 (sessenta) meses, incluindo todos os softwares e suas licenças de uso, gerenciamento centralizado, serviços de implantação, garantia de atualização contínua e suporte técnico durante o período de garantia com repasse de conhecimento da solução a fim de atender às necessidades dos contratantes.

**Pais de Origem:** Brasil

### 2. ESPECIFICAÇÕES

2.1. Requisitos gerais comuns a todos os Firewalls multifuncionais dos lotes 1,2,3,4 e 5

2.1.1. Todos os equipamentos firewall e a solução de gerência são integradas e são do mesmo fabricante, inclusive os sistemas operacionais executados por esses equipamentos, observado, o disposto no item 2.1.10.

2.1.2. Todos os equipamentos e seus componentes são novos, sem uso, e entregues em perfeito estado de funcionamento, sem marcas, amassados, arranhões ou outros problemas físicos, acondicionados em suas embalagens originais e acompanhados de todos os acessórios, cabos, conectores, kits de fixação, trilhos, fibras óticas (incluindo sua fusão, se necessário), patchcords, transceivers, etc, necessários às suas instalações e operação em rack de 19" padrão EIA-310. No caso dos lotes 1, firewall multifuncionais de 100, será fornecido os insumos como bandejas para colocação dos mesmos em racks.

2.1.3. Não será fornecido equipamentos em modo End of Support durante a vigência da garantia ou que entre em modo End of Life pelo período de 2 anos após a assinatura do contrato, não deixaremos de atender ao item 2.1.6 durante toda a vigência da garantia.

2.1.4. O fabricante irá atualizar firmwares e softwares da solução para novas versões durante toda a vigência da garantia.

2.1.5. Todas as funcionalidades adquiridas de hardware e software irão operar conforme disposto neste Termo de Referência durante o prazo de garantia dos equipamentos, ou seja, iremos garantir a atualização completa das funcionalidades no prazo referido, não haverá a cobrança de quaisquer valores adicionais pelo uso dos hardwares e softwares para esse período. As funcionalidades irão permanecer ativas, mesmo que não sejam atualizadas após o fim do prazo da garantia.



2.1.5.1. Após o prazo da garantia, os equipamentos irão permanecer com todas as funcionalidades operacionais, com as atualizações imediatamente anteriores a data final da garantia dos equipamentos.

2.1.5.2. Somente a funcionalidade de filtro de conteúdo web irá ser desativada ao final do prazo de garantia do equipamento, em razão de sua natureza técnica de acesso on-line as suas bases de dados.

2.1.5.3. A garantia referida no item 2.1.5 terá início com a emissão do termo de recebimento definitivo da solução a ser gerado pela CONTRATANTE conforme disposto no item 12.4.

2.1.6. As licenças de atualização de software (firmware ou drivers) e licenças de atualização de assinaturas deverão ser fornecidas pelo prazo mínimo de 60 (sessenta) meses, a contar da data do recebimento definitivo dos produtos, sem ônus adicional para as atualizações e seu uso.

2.1.7. Todos os equipamentos funcionam com alimentação nominal de 100~120VAC e 210~230VAC e frequência de 50 ou 60 Hz, ou auto-ranging. Será acompanhado de cabo de alimentação com, no mínimo, 1,80m (6 pés), com plug tripolar 2P+T no padrão ABNT NBR 14136.

2.1.8. O equipamento possui 1 (uma) porta de console para configuração e gerenciamento por interface de linha de comando (CLI).

2.1.8.1. Será fornecido pelo menos 1 (um) cabo conversor Serial para USB, compatível com a porta de console do equipamento.

2.1.9. O equipamento será fornecido com todas as suas portas de comunicação, interfaces e afins habilitadas, operacionais e sem custos adicionais, mesmo que para futuras utilizações do órgão ou entidade CONTRATANTE.

2.1.9.1. A CONTRATADA irá entregar a quantidade de transceivers equivalente ao dobro da quantidade mínima de portas exigidas em cada lote conforme os itens 3.15.1.4, 3.22.1.4 e 3.29.1.4.

2.1.9.2. Em caso de defeito ou mau funcionamento dos transceivers, estes estarão cobertos pela garantia da solução.

2.1.10. O equipamento será fornecido em hardware dedicado tipo appliance ou chassi, com sistema operacional otimizado, do mesmo fabricante, para o uso como firewall corporativo multifuncional.

2.1.10.1. Os equipamentos dos lotes 1, 2, 3 e 4 da solução ofertada, não irão exceder, individualmente, 4 Unidades de Rack, sendo "caixas" únicas, sem empilhamentos.

2.1.11. Possui fonte(s) de energia atendendo aos itens 3.1.1.3, 3.8.1.3, 3.15.1.3, 3.22.1.3 e 3.29.1.3.

2.1.12. Suporta topologias de cluster redundante de alta disponibilidade (failover) no mínimo aos pares, nos modos ativo-ativo e ativo-passivo, com sincronização, em tempo real, de configuração e de estados das sessões. No caso de falha de um dos equipamentos do cluster, não haverá perda das configurações e nem das sessões já estabelecidas e a transição entre os equipamentos deverá acontecer de forma transparente para o usuário.

2.1.13. Suporta a implementação tanto em modo transparente (camada 2) quanto em modo gateway (camada 3).

2.1.14. Possui filtragem de pacote por endereço IP de origem e destino, por aplicação (independentemente da porta ou protocolo utilizados pela aplicação), por sub-rede e por períodos do dia, permitindo a aplicação de regras por horários e por dias da semana.

2.1.15. Permite criação de serviços por porta ou conjunto de portas para, no mínimo, os protocolos TCP, UDP, ICMP e IP.

2.1.16. Suporta tags de VLAN;

2.1.17. Permite a criação de no mínimo 25 VLANs padrão 802.1q para os firewalls especificados nos lotes 1, no mínimo 50 VLANs padrão 802.1q para os firewalls do lote 2 e no mínimo 500 VLANs padrão 802.1q para os firewalls especificados nos lotes 3, 4 e 5.

2.1.18. É capaz de aceitar comandos de scripts acionados por sistemas externos como, por exemplo, correlacionadores de eventos;

2.1.19. Suporta o bloqueio de tráfego em função da localização geográfica dos IPs de origem e de destino;



- 2.1.20. Suporta agregação de links, segundo padrão IEEE 802.3ad, nos equipamentos firewall descritos nos lotes 3, 4 e 5.
- 2.1.21. Possui ferramenta de diagnóstico do tipo tcpdump.
  - 2.1.21.1. Suporta e efetuar a captura de pacotes no formato PCAP.
  - 2.1.21.2. Suporta e efetuar o download dos arquivos PCAP.
- 2.1.22. Não possui restrições de licenciamento em relação às características, requisitos e funcionalidades presentes nos subitens do item 2.1, inclusive em relação ao número ou tipo de clientes, usuários, máquinas e endereços IP.
- 2.1.23. Suporta, no próprio firewall, autenticação de usuários locais e integração com serviços de autenticação de diretório LDAP, Microsoft Active Directory e RADIUS, sendo que:
  - 2.1.23.1. Não existe limitações de licenciamento quanto ao número de usuários, a não ser o limite operacional do equipamento, respeitado o quantitativo mínimo especificado em cada lote;
  - 2.1.23.2. Registra a identificação do usuário em todos os eventos associados gerados pelo equipamento, tais como (mas não restrito a) eventos de autenticação, registros de acesso ou bloqueio e eventos associados a ameaças;
  - 2.1.23.3. Provê identificação de forma transparente aos usuários autenticados por single sign-on, no mínimo, por meio dos serviços Microsoft Active Directory e RADIUS;
  - 2.1.23.4. Provê portal ou pop-up de login para identificação dos usuários dos demais serviços de LDAP não listados no item anterior;
  - 2.1.23.5. Permite a criação de regras de acesso/bloqueio baseadas em usuários ou grupo de usuários do LDAP e do Microsoft Active Directory;
  - 2.1.23.6. Não será utilizado agentes instalados nos equipamentos dos usuários;
  - 2.1.23.7. Possui métodos de autenticação de usuários para aplicações executadas sobre os protocolos TCP, tais como (mas não restritos a) aplicações HTTP, HTTPS e FTP;
- 2.1.24. Suporta Network Address Translation (NAT 1-1, NAT 1-N, NAT N-1) de acordo com a RFC 3022, nos modos estático e dinâmico;
- 2.1.25. Suporta no mínimo NAT 64.
- 2.1.26. Possui a funcionalidade de fazer tradução de endereços dinâmicos um-para-N, PAT (Port Address Translation);
- 2.1.27. Suporta nativamente IPv6;
  - 2.1.27.1. Suporta, no mínimo, os protocolos de roteamento dinâmico OSPF v3 e BGP, bem como as funcionalidades de roteamento estático e roteamento policy-based;
- 2.1.28. Possui funcionalidades de DHCP client, server e relay;
- 2.1.29. Possui proteção e suporte a protocolos de Real Time, contemplando no mínimo: Real Time Transport Protocol (RTP), H323 e SIP sobre os protocolos IPV4 ou IPV6.
- 2.1.30. Possui tecnologia de firewall stateful;
- 2.1.31. Permite a realização de backup e restore das regras, configurações e políticas, e a transferência desse backup para armazenamento em servidores externos;
- 2.1.32. Possui funcionalidade de detecção e bloqueio de, no mínimo, os seguintes tipos de ataques: IP Spoofing, SYN Flood, UDP Flood, Port Scanning, ICMP Flood, ICMP sweep, Ataques de Força Bruta ataques Man-in-the-Middle e variações de reflexão;
- 2.1.33. Suporta sincronização de horário por NTP;
- 2.1.34. Possui funcionalidade de geração de relatórios e exportação de logs;
- 2.1.35. Suporta no mínimo 250 regras ou políticas de firewall para os equipamentos do lote 1 e 1.000 regras ou políticas de firewall para os equipamentos dos lotes 2,3,4 e 5.
- 2.1.36. Permite a abertura de novas portas por fluxo de dados para serviços que requerem portas dinâmicas;
- 2.1.37. Possui mecanismo de anti-spoofing;
- 2.1.38. Possui funcionalidade de exceção em SSL Inspection para sites e aplicações bancárias, não decriptando o tráfego dessas sessões.
- 2.1.39. Possui inspeção profunda de pacotes para tráfego criptografado (no mínimo em tráfego VPN e HTTPS);
- 2.1.40. Possui, no mínimo, suporte a SNMP v2 e v3;
- 2.1.41. Possui MIB própria contemplando, no mínimo, indicadores de estado do hardware e de performance do equipamento;



2.1.42. Identifica os países de origem e destino de todas as sessões estabelecidas através do equipamento, exceto para sessões no âmbito da rede interna (não roteadas).

2.1.43. Permite a criação de políticas de segurança baseadas em geolocalização, permitindo o bloqueio de tráfego com origem ou destino a determinado país ou grupo de países.

2.1.44. Possibilita a visualização dos países de origem e destino nos logs de eventos, de acessos e ameaças.

2.1.45. Provê interface de gerência local do firewall ou do cluster (virtual ou físico) do qual o firewall faz parte, por meio de interface gráfica (GUI) e linha de comando – (CLI) ou via SSH. Especificamente a interface gráfica (GUI) deve atender as funcionalidades gerenciais previstas nos subitens 2.1.45.1 ao 2.1.45.14.

2.1.45.1. Possui a capacidade de definir administradores com diferentes perfis de acesso. Os perfis de acesso devem ser, no mínimo, de leitura/escrita e somente leitura.

2.1.45.2. Permite a delegação de funções de administração.

2.1.45.3. Registra em log as ações dos usuários administradores.

2.1.45.4. Suporta a identificação e utilização de usuários nas políticas de segurança.

2.1.45.5. Suporta agrupamento lógico de objetos ("object grouping") para criação de regras.

2.1.45.6. Possibilita o gerenciamento (incluindo a criação, alteração, monitoramento e exclusão) de objetos de rede. Deverá ainda permitir detectar se e onde, na base de regras, está sendo utilizado determinado objeto de rede. Os tipos de objetos deverão permitir especificar de forma distinta grupos e objetos de rede e serviços, diferenciando-os e agrupando-os conforme suas características ou descrição de maneira a permitir o reaproveitamento dos mesmos em diferentes políticas.

2.1.45.7. Contabiliza a utilização ("hit counts") ou o volume de dados trafegados correspondente a cada regra de filtragem individualmente.

2.1.45.8. Possibilita a especificação de política por tempo, ou seja, permitir a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora).

2.1.45.9. Suporta a geração de alertas automáticos via email, SNMP e Syslog.

2.1.45.10. Permite a exportação de logs via SCP ou FTP.

2.1.45.11. Informa a utilização dos recursos de CPU, memória, armazenamento interno e atividade de rede dos equipamentos gerenciados.

2.1.45.12. Informa o número de sessões simultâneas e de novas sessões por segundo dos equipamentos gerenciados.

2.1.45.13. Possui visualização mínima sumarizada de: aplicações, ameaças, URLs, endereços de origem, endereços de destino, levando-se em conta o quantitativo de sessões, de consumo de banda e categorização.

2.1.45.14. Suporta gerência remota (via rede local ou WAN) ou por meio da gerência centralizada, sendo que:

2.1.45.14.1. A comunicação entre a estação ou sistema de gerência e o firewall ou cluster local é criptografada e autenticada;

2.1.46. Permite o controle e a priorização do tráfego, priorizando e garantindo banda para as aplicações (inbound/outbound) através da classificação dos pacotes (shaping);

2.1.47. Possui gerenciamento gráfico centralizado das funcionalidades de QoS/Traffic Shaping integrado tanto com a gerência local do equipamento, quanto com a gerência centralizada da solução;

2.1.48. Suporta a criação de políticas de controle de uso de largura de banda, limitando ou expandido individualmente, baseadas em: porta ou protocolo, endereço IP de origem ou destino, grupo de usuários do Microsoft Active Directory e LDAP e aplicações (por exemplo, Youtube e WhatsApp).

2.1.49. As funcionalidades de VPN não possui qualquer restrição de licenciamento, inclusive em relação ao número de clientes, aos softwares instalados nos clientes, IPs e máquinas, limitado apenas à capacidade de throughput do equipamento para VPN.

2.1.50. Permite a arquitetura de VPN hub and spoke IPSec, tanto para topologias site-to-site ("Full Meshed" e "Estrela") como para client-to-site (remote access);



- 2.1.51. Permite a criação de túneis VPN SSL/TLS;
- 2.1.52. Permite a criação de túneis VPN IPSec;
- 2.1.54. Permite que o usuário realize a conexão VPN por meio de cliente instalado no sistema operacional do seu equipamento ou por meio de interface Web do tipo portal.
  - 2.1.54.1. Caso não existam clientes (softwares) dos próprios fabricantes instaláveis para os sistemas operacionais: Linux, Mac OS X, Apple iOS e Google Android, a Licitante irá fornecer gratuitamente softwares de terceiros que sejam totalmente compatíveis com os sistemas operacionais referidos.
  - 2.1.54.2. O acesso por meio da interface Web será compatível com, no mínimo, os navegadores Internet Explorer 9 ou superior e Firefox 4.0 ou superior.
- 2.1.55. Suporta a customização da interface Web para acesso a VPN pelos administradores do sistema, incluindo quais aplicativos, servidores e sistemas estarão acessíveis via portal;
  - 2.1.56. Suporta algoritmos de criptografia para túneis VPN AES-128 e AES-256;
  - 2.1.57. Suporta os algoritmos para definição de chave de cifração 3DES e AES;
  - 2.1.58. Suporta os algoritmos RSA, Diffie-Hellman/RSA;
  - 2.1.59. Suporta Certificado Digital X.509 v3;
  - 2.1.60. Suporta a inclusão (enrollment) de autoridades certificadoras;
  - 2.1.61. Permite alteração dos algoritmos criptográficos das VPNs;
  - 2.1.62. Suporta IKE – Internet Key Exchange, fases I e II;
  - 2.1.63. Suporta os protocolos de roteamento RIPv2, OSPFv2 ou OSPFv3 para as funcionalidades de VPN;
  - 2.1.64. Implementa autenticação de usuários utilizando LDAP, Microsoft Active Directory, RADIUS e certificados digitais e suportar, no mínimo, autenticação two-way com certificado digital e LDAP ou Microsoft Active Directory ou RADIUS
  - 2.1.65. Suporta certificados emitidos por autoridade certificadora no padrão ICP-Brasil;
  - 2.1.66. Suporta leitura e verificação de Certificate Revocation List (CRL);
  - 2.1.67. Suporta NAT Transversal Tunneling (NAT-T);
  - 2.1.68. Possui gerenciamento gráfico das funcionalidades de VPN e monitoramento de seus eventos de forma integrada tanto com a gerência local do equipamento ou do cluster quanto com a gerência centralizada da solução.
  - 2.1.69. VPN gateway-a-gateway possui interoperabilidade com os gateways de VPN pelo menos dos seguintes fabricantes: Cisco, Checkpoint, Juniper, Palo Alto Networks, Fortinet, AKER, BluePEX, PFSense e SonicWall.
  - 2.1.70. Permite a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis de SSL.
  - 2.1.71. O equipamento é apropriado para o uso em ambiente tropical com umidade relativa na faixa de 20 a 85% (sem condensação) e temperatura ambiente na faixa de 5 a 40°C.
- 2.2. Solução de gerência centralizada
  - 2.2.1. Será fornecida solução de gerência centralizada dos firewalls, do mesmo fabricante e independente (externa) em relação aos equipamentos, sendo que:
    - 2.2.1.1. A solução será fornecida em "appliance virtual" - solução de software executada em máquina virtual que pode ser instalado e executado em ambientes virtuais ou componentes de software instaláveis em sistemas operacionais padrão servidor;
    - 2.2.1.3. A solução appliance virtual, é capaz de ser executada em pelo menos uma das seguintes plataformas virtualizadoras: VMware ESXi, Xen, KVM ou Microsoft Hyper-V, cujo ambiente será fornecido pela CONTRATANTE, não sendo necessário o fornecimento da licença da plataforma virtualizadora.
  - 2.2.2. Permite a gerência centralizada dos equipamentos e contextos virtuais que compõem a solução de alta disponibilidade, devendo ser dimensionada e devidamente licenciada para atender, no mínimo, o número total de equipamentos físicos gerenciados e o número total de contextos virtuais possíveis, compatível com o limite operacional dos equipamentos e clusters gerenciados.
  - 2.2.3. É licenciada de forma a não limitar número de usuários, objetos, regras de segurança, NAT e endereços IP.



2.2.4. É licenciada de forma a permitir a captura e filtragem de todos os eventos gerados por todos os equipamentos e contextos virtuais que compõe a solução de alta disponibilidade.

2.2.5. Permite a criação e distribuição de políticas de segurança e de objetos de rede de forma centralizada.

2.2.6. Permite a criação de relatórios customizados.

2.2.7. Possibilita a filtragem dos logs do equipamento por, no mínimo: aplicação, endereço IP de origem e destino, país de origem e destino, usuário e horário.

2.2.8. Possui relatórios com informações consolidadas sobre: as mais frequentes fontes de sessões bloqueadas com seus destinos e serviços, os mais frequentes ataques e ameaças de segurança detectadas com suas origens e destinos, os serviços de rede mais utilizados, as aplicações maiores consumidoras de banda de Internet, os usuários que consomem mais banda de Internet, os sites na Internet mais visitados.

2.2.9. Permite a geração automática e agendada dos relatórios.

2.2.10. É capaz de automatizar a aplicação das regras, objetos e políticas desejadas em tempo real a todos os equipamentos e contextos virtuais administrados.

2.2.11. Utiliza comunicação segura criptografada entre a solução de gerência e os equipamentos gerenciados.

2.2.12. Mantém o histórico de configurações enviadas aos equipamentos e deverá permitir o rollback das configurações.

2.2.13. Permite distribuição centralizada de pacotes de atualização.

2.2.14. Permite validar as regras antes, durante ou depois de aplicá-las.

2.2.15. É capaz de testar a conectividade dos equipamentos gerenciados.

2.2.16. Provê funcionalidade de detecção de regras conflitantes ou regras equivalentes.

2.3. Conjunto de funcionalidades IPS/IDS

2.3.1. Possui tecnologia de detecção e prevenção de ataques e intrusões baseada em assinatura;

2.3.2. Possui, no mínimo, um conjunto de 2.000 (duas mil) assinaturas de detecção e prevenção de ataques, devendo também detectar ataques baseados em anomalias;

2.3.3. Decodifica múltiplos formatos de Unicode;

2.3.4. Suporta fragmentação e desfragmentação IP;

2.3.5. Detecta protocolos independentemente da porta utilizada, identificando aplicações conhecidas em portas não-padrão;

2.3.6. Detecta e Protege contra, no mínimo, ataques de RPC (Remote Procedure Call), Windows ou NetBios, SMTP (Simple Message Transfer Protocol), IMAP (Internet Message Access Protocol), Sendmail ou POP (Post Office Protocol), DNS (Domain Name System), FTP, SSH, Telnet, ICMP (Internet Control Message Protocol), SIP, SNMP, SSDP ou CHARGEN, RDP (Remote Desktop Protocol), DoS (Denial of Service) e ataques com assinaturas complexas, tais como ataques TCP hijacking.

2.3.7. Possui proteção contra os ataques como, mas não restringindo-se aos mesmos: 1) Ataques de Worm, Trojan, Backdoors, Portscans, IP Spoofing, DoS, Spywares, Botnets e malwares em geral; 2) Ataques e utilização de tecnologia P2P; 3) Ataques de estouro de pilha (buffer overflow); 4) Tráfego mal formado; 5) Cabeçalhos inválidos de protocolo; 6) Ataques de injeção (SQL Injection, LDAP Injection) e de Cross-Site Scripting; 7) Elevação de privilégio e 8) Exploits - Web Server, Web Browser ActiveX, JavaScript, Browser Plug-ins/Add-ons.

2.3.8. Emissor de alarmes na console de administração integrada, alertas via correio eletrônico, syslog e traps SNMP;

2.3.9. Permite monitoração do comportamento do equipamento mediante o protocolo SNMP;

2.3.10. Atualiza automaticamente as assinaturas para o sistema de detecção de intrusos;

2.3.11. Permite filtros de anomalias de tráfego estatístico de flooding, scan e source session limits;

2.3.12. Permite filtros de anomalias de protocolos, inclusive protocolos de aplicação (ex.: HTTP, SMTP, NTP, NetBIOS, HTTPS, FTP, DNS, SMB, RPC, SSH e Telnet);



2.3.13. Deve resistir a técnicas de evasão ou ataques direcionados ao próprio equipamento, suportando, no mínimo, as técnicas: IP Packet Fragmentation, Stream Segmentation, RPC Fragmentation, URL Obfuscation, HTML Obfuscation, Payload Encoding, FTP Evasion e Layered Evasions.

2.3.14. Possui funcionalidade que permita desativar a análise de assinaturas e protocolos;

2.3.15. Possui funcionalidade que permita desativar a análise de ataques a partir de endereços/faixa IP específicos;

2.3.16. Permite o funcionamento mínimo do engine de IPS mesmo que a comunicação com o site do fabricante esteja fora de operação;

2.3.17. Possui as estratégias de bloqueio e liberação selecionáveis, tanto por conjuntos de assinaturas quanto por cada assinatura;

2.3.18. Suporta a verificação de ataques na camada de aplicação;

2.3.19. Possui gerenciamento gráfico centralizado das funcionalidades de IPS/IDS e monitoramento de seus eventos de forma integrada com a gerência local e a gerência centralizada da solução.

2.3.20. Reconhece assinaturas seletivas e filtros de ataque que protege, contra ataques de negação de serviços automatizados, worms e vulnerabilidades conhecidas.

2.4. Conjunto de funcionalidades antivírus e anti-malware

2.4.1. Possui módulo de proteção de antivírus, anti-malware e anti-bot no mesmo equipamento do firewall;

2.4.2. Possui funcionalidade de varredura contra vírus e malwares em tráfego nos seguintes protocolos: HTTPS, HTTP e pelo menos dois dos seguintes: FTP, POP3, IMAP e SMTP

2.4.3. É capaz de, se houver algum atraso ou falha na realização da atualização automática, o equipamento deve ter a capacidade de alertar imediatamente o administrador através de logs, e-mail ou outros meios de alerta

2.4.4. Possui serviço de atualização automática e manual de assinaturas com o fabricante

2.4.5. Suporta funcionamento mínimo da engine de antivírus e anti-malwares mesmo que a comunicação com o site do fabricante esteja fora de operação;

2.4.6. Possui gerenciamento gráfico centralizado das funcionalidades de antivírus e anti-malware integrado com a gerência local e a gerência centralizada da solução.

2.4.7. Identifica, classifica e bloqueia malwares, contemplando no mínimo, Trojan, Spywares, Backdoors, Worms e Vírus;

2.5. Conjunto de funcionalidades para tratamento de conteúdo web

2.5.1. Possui funcionalidades de tratamento de conteúdo web, devendo sua base de dados conter, no mínimo, 10 (dez) milhões de sites internet web já registrados e classificados, distribuídos em, no mínimo, 40 (quarenta) categorias ou subcategorias pré-definidas;

2.5.2. Permite a criação de categorias personalizadas;

2.5.3. Permite a categorização e reclassificação de sites web por URL;

2.5.4. Suporta filtragem e categorização das URLs;

2.5.5. Possui integração com serviços de diretório LDAP e Microsoft Active Directory para autenticação de usuários;

2.5.6. Permite a criação de regras de acesso/bloqueio baseadas em usuários ou grupo de usuários do LDAP e do Microsoft Active Directory;

2.5.7. Permite a criação de regras para acesso/bloqueio por endereço IP de origem e sub-rede de origem;

2.5.8. Permite a criação de quotas de utilização por horário, ou por categorias, ou por aplicações;

2.5.9. É capaz de exibir mensagem de bloqueio customizável pelos Administradores para resposta aos usuários, na tentativa de acesso a recursos proibidos ou restringidos pela política de segurança do órgão;

2.5.10. Permite o bloqueio de páginas web por meio da construção de filtros específicos com mecanismo de busca textual;



2.5.11. Permite o bloqueio de URLs cujo campo CN ou DN não contém um domínio válido para o certificado SSL;

2.5.12. Permite o bloqueio de páginas web por classificação, tais como páginas de streaming, rádio e tv online, P2P, URLs originadas de spam, sites de proxy anônimos, entre outros.

2.5.13. Permite a criação de listas personalizadas de URLs permitidas – lista branca e bloqueadas – lista negra;

2.5.14. Possui categorização de sites governamentais nacionais, mesmo não tendo domínio “.gov” ou “.gov.br.”

2.5.15. Categoriza as URLs com taxa de acerto mínima de 80% (oitenta por cento), não sendo consideradas neste percentual categorização genérica ou similar.

2.5.16. Suporta e força pesquisas seguras em pelo menos dois sistemas de buscas, contemplando Google e/ou Bing e/ou Yahoo.

2.6. Conjunto de funcionalidades para controle de aplicações e análise profunda

2.6.1. Possui módulo de filtro de aplicações e de conteúdo desenvolvido e mantido pelo próprio fabricante, no mesmo equipamento do firewall;

2.6.2. É capaz de identificar as aplicações mesmo que não estejam utilizando sua porta default.

2.6.3. É capaz de identificar aplicações encapsuladas dentro de protocolos, como HTTP e HTTPS.

2.6.4. É capaz de identificar aplicações que utilizam comunicação criptografada através de SSL.

2.6.5. Permite o agrupamento de aplicações em grupos personalizados;

2.6.6. Garante que as atualizações regulares do produto sejam realizadas de forma transparente, sem paradas perceptíveis dos serviços;

2.6.7. Identifica aplicações e permitir ou bloquear sua utilização, independentemente das portas e protocolos utilizados para conexão (inclusive tráfego criptografado), assim como possuir categorias para classificação das aplicações, bem como das técnicas de evasões utilizadas;

2.6.8. Possui, no mínimo, proteção para aplicações do tipo P2P, Instant Messaging, Web e VOIP;

2.6.9. Possui perfis/políticas de segurança de aplicações pré-definidas/pré-configuradas na solução;

2.6.10. Possui atualização manual e automática de novas assinaturas;

2.6.11. Permite a criação de regras de acesso/bloqueio baseadas em usuários ou grupo de usuários do LDAP e do Microsoft Active Directory;

2.6.12. É capaz de identificar e filtrar um mínimo de 1.500 (mil e quinhentas) aplicações, contemplando no mínimo: peer to peer, streaming e download de áudio, streaming e download de vídeo, update de software, instant messaging, redes sociais, proxies, anonymizers, acesso e controle remoto, VOIP e email.

2.6.13. Identifica, bloqueia e restringe em profundidade e granularidade de aplicações, contemplando no mínimo: Bittorrent, Youtube, Livestream, Skype, Viber, WhatsApp, Snapchat, Facebook, Facebook Messenger, Google+, Google Talk, Google Docs, Instagram, Twitter, LinkedIn, Dropbox, Google Drive, One Drive, Logmein, Teamviewer, MSRDP, VNC, Ultrasurf, TOR e Webex.

2.7. Treinamento oficial para até 5 pessoas

2.7.1. Será fornecido Voucher para treinamento oficial do fabricante.

2.7.2. A carga horária do treinamento não é inferior a 24 horas, sendo cada voucher apto para até 5 pessoas. O treinamento é composto por turmas que podem ser formadas de um ou mais Vouchers de uma entidade CONTRATANTE, ou ainda, ser uma turma compartilhada por mais de uma entidade CONTRATANTE. Nos dois casos cada turma se limita a no máximo 10 pessoas.

2.7.3. Os treinamentos serão realizados no Brasil, em português, na modalidade presencial, em local fornecido pela CONTRATADA.



2.7.3.1. O local de treinamento possui todas as facilidades para um perfeito desempenho das atividades, incluindo os recursos áudio visuais e laboratórios necessários, sem ônus algum para a CONTRATANTE.

2.7.4. A CONTRATADA irá prover todos os recursos didáticos necessários à realização do treinamento, incluindo (mas não se restringindo a) sala de aula, data show, apostilas, bloco de anotações e caneta para cada treinando.

2.7.5. Os treinamentos irão ocorrer usando-se turnos diários de até 4 horas cada, podendo ser dois turnos no mesmo dia ou um turno por dia a ser acordado com a CONTRATANTE, com intervalos de, no mínimo, 15 minutos em cada turno e de pelo menos 1 hora entre os turnos que ocorrerem no mesmo dia.

2.7.6. Toda a documentação didática necessária aos cursos de treinamento será disponibilizada em papel impresso e mídia digital.

2.7.7. Os cursos referentes a equipamentos e softwares que façam parte do objeto irão usar o material oficial de treinamento do respectivo fabricante por meio de qualquer um dos seus respectivos centros autorizados de treinamento.

2.7.8. São produtos de todos os treinamentos:

2.7.8.1. Aulas teóricas e práticas.

2.7.8.2. Material didático contratado e aprovado pela CONTRATANTE.

2.7.8.3. Referências para estudos e pesquisas complementares.

2.7.9. A CONTRATANTE poderá, a seu critério, reproduzir o material didático usado e treinar multiplicadores para repetir o treinamento sem custos adicionais. E tal ação não representa a quebra do direito de propriedade do fabricante ou da empresa CONTRATADA. Isso porque o material fornecido não será usado para fins comerciais, mas apenas para uso interno do órgão ou entidade CONTRATANTE com o intuito de disseminar o conhecimento da solução entre os seus servidores profissionais técnicos.

2.7.10. Os custos referentes ao deslocamento, hospedagem e alimentação dos treinados é de responsabilidade da CONTRATANTE.

2.7.11. A ementa do curso abrange conteúdos que vão desde configurações básicas até as avançadas dos equipamentos de hardware e de softwares que compõem a solução, bem como sua operação.

### 3. DEFINIÇÃO DOS LOTES E ITENS

3.8. LOTE 2 - item 01: Firewall multifuncional tipo 2

3.8.1. Requisitos específicos:

3.8.1.1. Atende a todos os requisitos do item 2.1;

3.8.1.2. Possui, no mínimo, o throughput de 250 Mbps para todas as funcionalidades dos itens 2.1, 2.2, 2.3, 2.4, 2.5 e 2.6, ativadas simultaneamente e com inspeção integral de todos os pacotes de dados, independentemente de seu tamanho ou direção de fluxo, levando-se em consideração o perfil de tráfego descrito no ANEXO E.

3.8.1.3. O equipamento possui no mínimo 01 (uma) fonte de alimentação, que pode ser interna ou externa, com alimentação nominal de 100~ 120VAC e 210~ 230VAC e frequência de 50 ou 60 Hz, ou auto-ranging. Deverá vir acompanhado de cabo de alimentação com, no mínimo, 1,80m (6 pés), com plug tripolar 2P+T no padrão ABNT NBR 14136.

3.8.1.4. Possui no mínimo 4 (quatro) portas de 10/100/1000 BASE-T.

3.8.1.5. Suporta a quantidade de sessões simultâneas 90.000.

3.8.1.6. Quantidade de novas sessões por segundo 12.000.

3.8.1.7. Possui Throughput mínimo de 50 Mbps para IPSec VPN.

3.9. LOTE 2 – item 2: Conjunto de funcionalidades IPS/IDS

3.9.1. Atende a todos os requisitos do item 2.3;

3.10. LOTE 3 - item 3: Conjunto de funcionalidades antivírus e anti-malware

3.10.1. Atende a todos os requisitos do 2.4;

3.11. LOTE 2 – item 4: Conjunto de funcionalidades para tratamento de conteúdo web

3.11.1. Atende a todos os requisitos do item 2.5;

3.12. LOTE 2 – item 5: Conjunto de funcionalidades para controle de aplicações e análise profunda

3.12.1. Atende a todos os requisitos do item 2.1.39 e do item 2.6; 3.13. LOTE 2 - item 6: Treinamento oficial para até 5 pessoas 3.13.1. Atender a tudo o que foi exposto no item 2.7.;

- 3.14. LOTE 2 - item7: Solução de gerência centralizada
- 3.14.1. Requisitos específicos
- 3.14.1.1. Atende a todos os requisitos do item 2.2;
- 3.14.1.2. Possuir capacidade mínima de 250 GB para armazenamento de logs e eventos quando adicionado disco na solução virtualizada.

Brasília/DF, 03 de outubro de 2017

  
Blockbit Tecnologia Ltda  
CNPJ Nº 02.423.535/0001-09  
Inscrição Estadual: 115.395.122.119  
Cleber Ribas de Oliveira  
Vice-Presidente  
RG: 0912795-0 SSP/MT  
CPF: 788.962.231-72



**B BLOCKBIT**

Solução revolucionária de segurança de redes que unifica tecnologias de Next Generation Firewall, IPS, VPN, Filtro Web Avançado, Proteção Avançada Contra Ameaças e muito mais.

## Unified Threat Management

**UTM**

**BLOCKBIT**

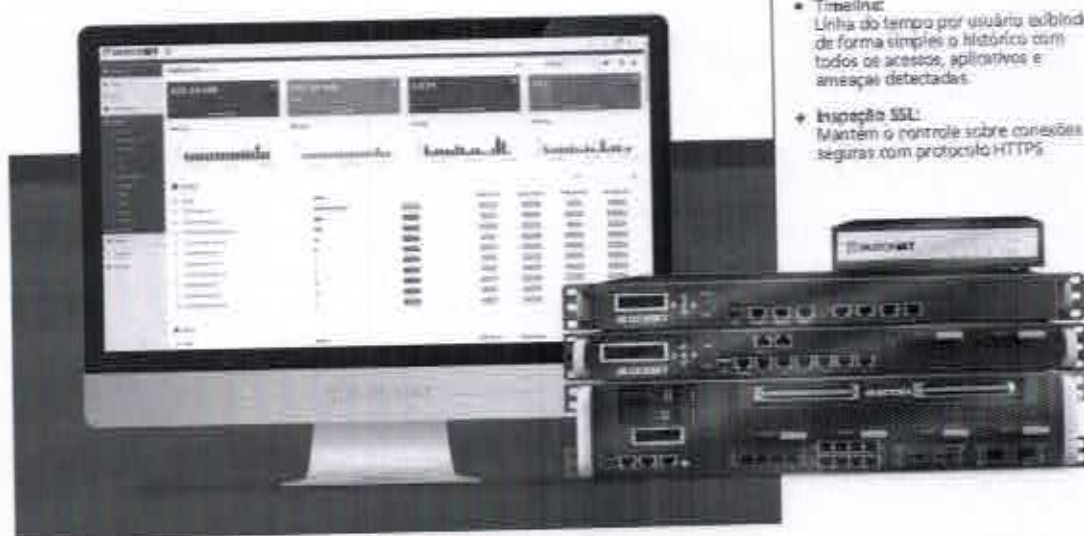
Gerenciamento Unificado de Ameaças

**Proteção Completa e Fácil de Usar.**  
Rápida Visão, Gestão e Tomada de decisão.

Riqueza protegida de ataques e ameaças globais, escolhendo a ferramenta correta. O BLOCKBIT UTM simplifica a gestão de redes, usuários, conexões e múltiplos dispositivos, economiza tempo e dinheiro, reduz possíveis erros de configuração e minimiza os riscos de segurança para a sua empresa.

### Destaques

- **Controle Avançado de Aplicações:** Gerencie facilmente o acesso a aplicações Web 2.0 como Facebook, LinkedIn, Google, Twitter, Dropbox, entre outros.
- **Proteção Avançada Contra Ameaças:** Segurança inovadora contra malware avançado e callback.
- **GSM - Global Security Management:** Gerencie facilmente múltiplos dispositivos com o BLOCKBIT GSM - que tem integração nativa com o BLOCKBIT UTM. Administra os perfis de dispositivos, gerenciamento e automação, inventário e monitoramento.
- **Panel Unificado de Políticas:** Controle de acesso ágil, com aplicação de políticas por grupos de usuários, que unifica recursos de forma simples e inovadora.
- **Timeline:** Linha do tempo por usuário exibindo de forma simples o histórico com todos os acessos, aplicativos e ameaças detectadas.
- **Inspeção SSL:** Mantém o controle sobre conexões seguras com protocolo HTTPS.



O BLOCKBIT UTM é um produto de cibersegurança da última geração que unifica tecnologias de: Next Generation Firewall, Filtro Web Avançado, ATP - Proteção Avançada Contra Ameaças e muito mais.

Todos os recursos são gerenciados por meio de uma interface web intuitiva, com informações agrupadas em um dashboard que permite a visualização rápida de informações sobre conexões, dados, dispositivos conectados, usuários e ameaças detectadas, compatível com as últimas versões dos navegadores Internet Explorer, Firefox, Chrome e Safari. Você pode tomar decisões mais rápidas com uma visão global do seu ambiente.

A tecnologia do BLOCKBIT UTM é atualizada constantemente pelo Inteligence Lab da BLOCKBIT, que trabalha 24x7x365 na pesquisa e análise de novas ameaças para melhorar a segurança da sua empresa.

## Implantação Flexível

Escolha a melhor opção para o seu ambiente:

### Hardware Appliances

- Desempenho Máximo
- Estabilidade Garantida
- Instalação Rápida



### Virtual Appliances

- Suporta VMware ESXi e Xen
- Recuperação de Desastres Mais Rápida
- Otimização da Infraestrutura



[www.blockbit.com](http://www.blockbit.com)

### Destaques

- **Controle Avançado de Aplicações:** Gerencie facilmente o acesso a aplicações Web 2.0 como Facebook, LinkedIn, Google, Twitter, Dropbox, entre outras.
- **Proteção Avançada Contra Ameaças:** Segurança inovadora contra malware avançado e callback.
- **GSM - Global Security Management:** Gerencie facilmente múltiplos dispositivos com o BLOCKBIT GSM - que tem integração nativa com o BLOCKBIT UTM. Administra os perfis de dispositivos, gerenciamento e automação, inventário e monitoramento.
- **Painel Unificado de Políticas:** Controle de acesso fácil, com aplicação de políticas por grupos de usuários, que unifica recursos de forma simples e inovadora.
- **Timeline:** Linha do tempo por usuário exibindo de forma simples o histórico com todos os acessos, aplicativos e ameaças detectadas.
- **Inspecção SSL:** Mantém o controle sobre conexões seguras com protocolo HTTPS.

Fale conosco ou visite nosso site para mais informações:



(11) 2165 8888

[www.blockbit.com](http://www.blockbit.com)

**UTM** BLOCKBIT  
Unificação Total da Segurança

**Proteção Completa**  
e  
**Fácil de Usar**

Rápida Visão, Gestão e Tomada de Decisão





## Dashboard

As informações coletadas pelos módulos de segurança do BLOCKBIT UTM são exibidas em um dashboard completo com dados agrupados por usuário, grupos de usuários, serviços em execução e ameaças detectadas, sessões simultâneas, novas sessões por segundo, visualização mínima resumida de aplicações, URLs, endereços de origem, endereços de destino, levando-se em conta o quantitativo de sessões, de consumo de banda e categorização permitindo uma rápida visão, gestão e tomada de decisão.



## GSM Global Security Management

Com o BLOCKBIT GSM, é possível criar e distribuir políticas de segurança e de objetos de rede de forma centralizada. Permite a criação de relatórios consolidados e customizados, possibilita a filtragem dos logs por aplicações, endereços IP e país de origem e destino, usuários e horários de acesso, sessões bloqueadas com seus destinos e serviços, ataques mais frequentes e ameaças de segurança detectadas com suas origens e destinos, serviços de rede mais utilizados, aplicações e usuários de maior consumo de banda de Internet, sites mais visitados e geração automática e agendada dos relatórios. Com o BLOCKBIT GSM é fácil automatizar as aplicações das regras, objetos e políticas desejadas, tudo em tempo real, com comunicação criptografada entre a solução de gerência e os equipamentos gerenciados, mantendo todo o histórico de configurações enviadas aos equipamentos e o rollback das configurações. Os pacotes de atualização são distribuídos de modo centralizado, e permitem validar as regras antes e depois de aplicá-las. É capaz de testar a conectividade dos equipamentos gerenciados e de prover funcionalidades de detecção de regras conflitantes. O BLOCKBIT UTM tem integração nativa com o BLOCKBIT GSM (Global Security Management), que possibilita gerenciar múltiplos dispositivos através de um ponto central.

**Proteção Avançada  
Contra Ameaças**

Segurança integrada com detecção e proteção em tempo real contra malware avançado, malware maliciosos e até mesmo ataques desconhecidos.

**Controle Avançado  
de Aplicações**

Sempre facilite o acesso a serviços e aplicações atribuindo "regras" aos níveis de "confiança ou perigo", o que agiliza a gestão, melhora a segurança e reduz a necessidade de complexos limites de protocolos.

**Timeline**

Acompanhe o histórico de acessos, ameaças detectadas e aplicações em execução em uma linha do tempo visual apenas por administradores e gestores.

**Painel Unificado  
de Políticas**

Políticas de conformidade e níveis de acesso podem ser definidos e aplicados por grupos, de forma simples e intuitiva, reduzindo os erros de configuração e as falhas de segurança. Simples e a determinação de regras por usuário, grupos de usuários, serviços e aplicações em execução.

**Controle de  
Banda Flexível**

Gerencie a largura de banda das conexões de acordo com sua prioridade. Você pode definir velocidades de acesso para usuários, grupos, categorias e até tipos de serviço e mais.

**Antivírus  
e  
Anti-Malware**

Crie e com recursos avançados de Antivírus e Anti-Malware integrados para impedir a execução de aplicações não autorizadas e potencialmente perigosas. Faça a verificação de arquivos protegidos por senha e tráfego nos protocolos HTTP ou HTTPS para impedir downloads maliciosos.

**Acesso Remoto  
sem Aplicação  
Cliente**

Permite que seus usuários se conectem de maneira segura a sua rede sem a necessidade de instalação de qualquer software adicional. O BLOCKBIT UTM utiliza tecnologia proprietária de maneira nativa com sistemas Windows, iOS e Android.

**Balanceamento  
de Link  
por Política**

Gerencie múltiplos links de internet e roteadores, atribua conexões de dados de acordo com cada política de segurança, tenha maior flexibilidade ao determinar conexões por endereços de rede, conteúdo de conexão, categorias web, aplicações, usuários, grupos de usuários e mais.

*A*



### Next Generation Firewall

O BLOCKBIT UTM é muito mais que um firewall. Une a mais avançada tecnologia de gestão de rede a capacidade avançada de detecção e proteção contra ataques e ameaças digitais. O Next Generation Firewall do BLOCKBIT UTM simplifica a criação de políticas e regras de segurança complexas, utilizando endereços, usuários, grupos de usuários, aplicações, ameaças e serviços em suas configurações, que podem ser nomeados para facilitar a compreensão das políticas e garantir controle total do seu ambiente.

### IPS - Sistema de Prevenção de Intrusos

O BLOCKBIT UTM protege continuamente sua rede contra o número crescente de ameaças digitais. O IPS conta com milhares de assinaturas para identificação de ameaças em um banco de dados atualizado diariamente pelo Intelligence Lab da BLOCKBIT. Inclui informações sobre sistemas operacionais, protocolos, servidores de aplicação, bancos de dados, SQL injections e mais. Detecta protocolos independentemente da porta utilizada e identifica aplicações conhecidas em portas não-padrão. O IPS possibilita a visualização de alertas na console de administração, e o envio de alertas via correio eletrônico, syslog e traps SNMP. Possui técnicas de evasão, tais como, IP Packet Fragmentation, Stream Segmentation, RPC Fragmentation, URL Obfuscation, HTML Obfuscation, Payload Encoding, TTP Evasion e Layered Evasions. Permite desativar a análise de assinaturas, protocolos e ataques a partir de endereços ou faixa de endereços de rede específicos. O dashboard exibe informações sobre ameaças detectadas de maneira detalhada, permitindo uma rápida e eficiente análise de risco.

### VPN IPsec

O BLOCKBIT UTM permite a criação de redes privadas virtuais com criptografia de tunelamento nativa, que garante a interoperabilidade com outros produtos e aumenta a segurança. Suporta arquitetura de VPN hub and spoke IPsec, tanto para topologias site-to-site ("Full Meshed" e "Star") como para client-to-site (remote access).

### VPN IPsec RAS - Remote Access

O BLOCKBIT UTM permite que seus usuários acessem a rede de qualquer parte do mundo sem instalar qualquer software adicional por contar com compatibilidade nativa com Windows, iOS e Android.

### Inspecção SSL

A maioria das informações que trafegam na web usam conexões criptografadas. O BLOCKBIT UTM conta com descriptografia de SSL para inspeção de tráfego, garantindo o controle total de acesso e aplicação de recursos avançados, como ATP e Filtro de Conteúdo.

### Filtragem de Conteúdo

O BLOCKBIT UTM possui mais de 40 milhões de endereços classificados em mais de 85 categorias, além de estar integrado com os bancos de dados de URLs dos navegadores web. Essas informações, em conjunto com a inspeção SSL, permitem controlar totalmente o acesso ao conteúdo online, que pode ser configurado de maneira particular para usuários, grupos de usuários, IPs, largura de banda, prioridade de conexão, links, diferentes navegadores e suas versões. Você também pode determinar limites para tamanho de arquivos para download, execução de aplicações web, tempo permitido de navegação e muito mais.

4

### ATP - Proteção Avançada Contra Ameaças

O BLOCKBIT UTM conta com tecnologias sofisticadas de segurança e inteligência que detectam e protegem sua empresa contra ameaças conhecidas e desconhecidas. O BLOCKBIT UTM pode detectar malware avançados como trojans e vírus, ameaças persistentes avançadas e ataques de callbacks maliciosos. O ATP também pode bloquear IPs com má reputação em diferentes categorias (abusers, anonymizers, attackers, malware, reputation, spam) além de ataques por geolocalização.

### Controle Web 2.0

O avanço da Internet permitiu a criação de aplicações, como Facebook, Youtube, Google Apps, Twitter, LinkedIn e Dropbox, que se tornaram muito populares e podem impactar a produtividade de suas equipes se não utilizadas constantemente. O BLOCKBIT UTM permite que você controle totalmente o acesso à Web 2.0, restringindo ou permitindo acesso de acordo com as regras do seu negócio.

### QoS - Qualidade de Serviço

O BLOCKBIT UTM conta com recurso de QoS exclusivo, que permite via interface gráfica centralizada e local, a priorização de tráfego e controle de largura de banda de acordo com as políticas de segurança e conformidades configuradas e classificação de pacotes (shaping). O recurso de QoS avançado, categoriza conexões de acordo com sua importância e possibilita priorizar pacotes usando protocolos DSCP e TOS.

### Multilink

O BLOCKBIT UTM suporta múltiplas conexões de dados com a Internet e oferece grande flexibilidade na gestão dos serviços e aplicações em execução, com distribuição de tráfego baseada nas suas políticas de segurança. A opção de alta disponibilidade e recurso de failover permitem ao BLOCKBIT UTM um uptime de 99.99%.

### Alta Disponibilidade

O BLOCKBIT UTM tem suporte nativo a implementações H.A. (high availability). O recurso mantém um appliance em modo backup, que entra em operação imediatamente caso o appliance primário sofra uma falha. O suporte H.A. espelha sessões de firewall e autenticação de usuário entre os dispositivos primário e secundário para que o switch over seja transparente e rápido.

### Captive Portal

Com o BLOCKBIT UTM é fácil gerenciar o acesso de visitantes por meio da autenticação que o navegador web utiliza. O Captive Portal permite auto-registro, personalização de políticas de acesso, controle de conteúdo e gestão de usuários, troca de senhas de acesso e relatórios personalizados.

### Suporte a Gerenciamento Centralizado

O BLOCKBIT UTM tem integração nativa com o BLOCKBIT GDM (Global Security Management), que possibilita gerenciar múltiplos dispositivos, com conexão criptografada e autenticada, por meio de um portal central. Permite o gerenciamento centralizado e local das funcionalidades de IPS/IDS e Anti-Malware, monitorando seus eventos de forma integrada.

### Outros Recursos

Balanceamento Dinâmico, VLAN, DNS Dinâmico, integração do Active Directory, SNMP, Servidor DHCP, Link Aggregation -- Ethernet Bonding (BOND3ad) e Snapshot.

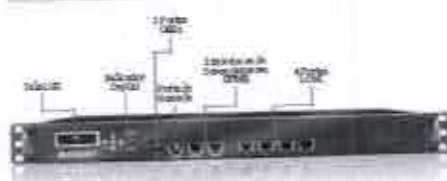
D



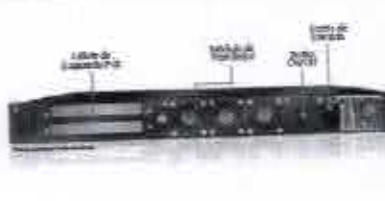
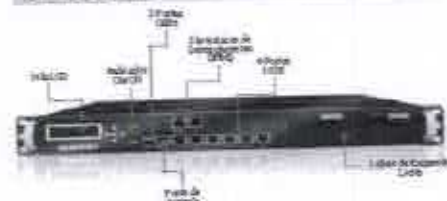
**Modelo BB 2 | BB 5 | BB 10**
**Pequenas Empresas**

**Especificação**

Memória de 4GB  
 1000 Mbps  
 1U 19"

**Modelo BB 50 | BB 100**
**Médias Empresas**

**Especificação**

Memória de 8GB  
 1000 Mbps  
 1U 19" (2 Bayes de 5.25")

**Modelo BB 500 | BB 1000**
**Grandes Empresas**

**Especificação**

Memória de 16GB  
 1000 Mbps  
 2U 19" (4 Bayes de 5.25")  
 2 slots de expansão LATA  
 Expansão de LATA por Slot (opcional)  
 de 1GB 5.25" ou de 2GB 3.5"

**Modelo BB 10000**
**Corporações & Datacenters**

**Especificação**

Memória de 32GB  
 1000 Mbps  
 4U 19" (8 Bayes de 5.25")  
 4 slots de expansão LATA  
 Expansão de LATA por Slot (opcional)  
 de 1GB 5.25" ou de 2GB 3.5"

	Processador (CPU)	Memória de LATA por unidade	Memória de LATA por produto	
BBV 2	200 MHz	2	4	
BBV 5	500 MHz	2	4	
BBV 10	1.0 GHz	2	4	
BBV 50	1.0 GHz	3	6	
BBV 100	1.0 GHz	3	6	
BBV 500	1.0 GHz	3	24	
BBV 1000	1.0 GHz	3	24	
BBV 5000	1.0 GHz	3	24	
BBV 10000	1.0 GHz	3	24	

Nota: Os dados de especificação representam o desempenho de um único processador e não representam o desempenho de um sistema inteiro. Para obter mais informações, consulte o site [www.blockbit.com](http://www.blockbit.com).  
 O desempenho pode variar dependendo do tipo de carga de trabalho e da configuração do sistema.  
 O desempenho pode variar dependendo do tipo de carga de trabalho e da configuração do sistema.

**Virtual Appliances**






- Interfaces:
  - Ethernet
  - WAN: tel-Agile por VoIP (Voice over IP)
- Suporte ao Protocolo SNMP (v2 e v3):
- N/A, IANA (Discontinuidade):
- Atenuação de data e N/A (não suporte à verificação RTP (Real-time Transport Protocol))
- Cópia de Atualizações Automáticas e Redução do Sistema para Correção de Problemas
- Administração VRRP (VRRP)
- Otimização de Gerenciamento
- Disaster Recovery (Backup / Recuperação)
- Link Aggregation
- Ethernet Bonding (BGP fail)
- Suporte a protocolos de gerenciamento por gerenciamento remoto
- TFTP/FTP (Protocolo de transferência de arquivos) e download do firmware (Firmware)
- Registro de alterações no sistema de atualizações, status, integridade e erro(s)
- IPv6
- NetBIOS, NetWare e NFS
- Suporte para atualizações automáticas no modo SNMP (Simple Network Management Protocol)

- **Arquitetura:**
  - HPE
  - DC (i400)
- **Armazenamento Dispositivo:**
  - Armazenamento NTA
  - BOM
  - CPM
  - BPA
- **Tolerância a falhas**
- **Arquitetura Policy Based**
- **Segmentação de Usuários e Grupos com Serviços Windows AD e Serviços LDM**
- **Autenticação (se possível, automaticamente)**
  - Local Windows AD / LDAP / Local Windows Single Sign On
  - Autenticação Offline: X-moto para Servidores VPN, Autenticação em Servidores RADIUS, SSO (Passes Single Sign On) Identificação de Condições de Sessão
- **Segurança**
- **Exatidão e alta taxa de recuperação SCD**

- Suporte a Múltiplos Níveis de Autenticação
- Captive Portal
- Gerenciador de SL
- Objetos de Recursos
- Inspeção IP
- Inspeção MAC
- Servidor de Proxy e ProxyCache
- Web de Ho-404s
- Intervalo de Período e Data
- Estatísticas Conjuntas de Políticas para Especificações Regulares
- Filtro de Conteúdo
- Servidor DHCP (Estatísticas, Configuração, Proxy)
- DHCP Relay
- DNS (DNS Resolvers)
- DNS Client (Navegador DNS)
- Serviço Splitting
- Cui (Interfície de União de Controle para Gerenciamento e Administração)

	HD 2	HD 5	HD 10	HD 50	HD 100	HD 200	HD 300	HD 500
Forward Throughput (IOPS)	304 Mops	600 Mops	1.1 Gops	3.0 Gops	6.1 Gops	9 Gops	9 Gops	40 Gops
Forward Throughput (IOPS)	304 Mops	600 Mops	1.1 Gops	3.0 Gops	6.1 Gops	9 Gops	9 Gops	21.5 Gops
Compressed I/O (MB/sec)	15,000	15,000	250,000	340,000	1,000,000	1,999,000	2,499,000	6,300,000
Compressed I/O per second	3,000	3,000	17,000	70,000	55,000	85,000	100,000	200,000
Write Filter Throughput (IOPS/MB/sec)	100 Mops	130 Mops	610 Mops	600 Mops	600 Mops	1.5 Gops	2.7 Gops	9.5 Gops
Write Filter + OS, Sequential Throughput	100 Mops	100 Mops	1.0 Gops	1.0 Gops	2.0 Gops	4.0 Gops	8.0 Gops	1.4 Gops
OS Throughput	100 Mops	170 Mops	190 Mops	500 Mops	610 Mops	1.2 Gops	3.0 Gops	3.3 Gops
ATP Throughput	140 Mops	190 Mops	190 Mops	300 Mops	610 Mops	1.8 Gops	3.0 Gops	3.6 Gops
Write Filter + OS, Sequential + ATP Throughput	32 Mops	60 Mops	100 Mops	100 Mops	200 Mops	3.0 Mops	5.0 Mops	1.0 Gops
SEC, VPM Throughput (AES 256 + MD5 + Gzip 3)	80 Mops	100 Mops	200 Mops	400 Mops	700 Mops	1.5 Gops	3.26 Gops	6.5 Gops
OS, VPM Throughput (AES 128)	95 Mops	130 Mops	240 Mops	400 Mops	650 Mops	1.0 Gops	1.8 Gops	7 Gops
Write Filter + OS, SEC, VPM (AES 128)	5	5	30	50	100	200	400	1,000
Optimizations								
Write Filter (Extended Global I/O)	64KB / 128KB	64KB / 128KB	128KB / 65536	1MB / 2	1MB / 2	4096B	4096B	64KB / 2
Write Filter (Per-IO Size - 4 pages 25%)	-	-	-	-	-	3x	2x	3x
Write Filter (Per-IO Size - 8 pages 10%)	-	-	-	-	-	3x	2x	3x
Write Filter (Per-IO Size - 16 pages 5%)	-	-	-	140B	160B	320B	320B	64KB



**B BLOCKBIT**

É fácil estar seguro

Fale conosco  
ou visite nosso  
site para mais  
informações.



**NORTH AMERICA**


700 Appleton Way - 4th Floor  
Miami - FL 33136 - United States  
Phone: +1 305 573 4466

**EUROPE**

2 Theobald Street - 6th Floor  
Netherlands - 1017 CA Amsterdam  
Phone: +31 20 335 505 4121

**AMERICA LATINA**

Rua Tupy, Francisco Faria 8 de 275 - 2º e 3º and.  
São Paulo - SP - 04533-000 - Brazil  
Phone: +55 11 265 8889

 [www.blockbit.com](http://www.blockbit.com)



Ao  
MINISTÉRIO DO PLANEJAMENTO, DESENVOLVIMENTO E GESTÃO  
SECRETARIA DE GESTÃO  
DEPARTAMENTO DE AQUISIÇÕES

Referência: Pregão Eletrônico nº 05/2017  
Processo: 04300.0204177/2015-44  
Tipo: PREGÃO ELETRÔNICO  
Abertura: 03/10/2017 às 10hs  
Proponente: Blockbit Tecnologia Ltda.  
CNPJ: 02.423.535/0001-09

### COMPROVAÇÃO PONTUAL – Lote 2

LOTE	ITEM	ITEM	DESCRIÇÃO	PROPOSTA ATENDE? (SIM OU NÃO)	REFERENCIA NA DOCUMENTAÇÃO TÉCNICA	OBSERVAÇÃO
2		2.	ESPECIFICAÇÕES			
2	1	2.1.	Requisitos gerais comuns a todos os Firewalls multifuncionais dos lotes 1,2,3,4 e 5			
2	1	2.1.1.	Todos os equipamentos firewall e a solução de gerência integrada devem ser do mesmo fabricante, inclusive os sistemas operacionais executados por esses equipamentos, observado, o disposto no item 2.1.10.	SIM	CONFORME PROPOSTA DE PREÇO	
2	1	2.1.2.	Todos os equipamentos e seus componentes deverão ser novos, sem uso, e entregues em perfeito estado de funcionamento, sem marcas, amassados, arranhões ou outros problemas físicos, acondicionados em suas embalagens originais e acompanhados de todos os acessórios, cabos, conectores, kits de fixação, trilhos, fibras óticas (incluindo sua fusão, se necessário), patchcords, transceivers, etc, necessários às suas instalações e operação em rack de 19" padrão EIA-310. No caso dos lotes 1 e 2, firewall multifuncionais de 100 e 250 Mbps, poderá ser fornecido os insumos como bandejas para colocação dos mesmos em racks.	SIM	CONFORME PROPOSTA DE PREÇO	

2	1	2.1.3.	Não serão aceitos equipamentos em modo End of Support durante a vigência da garantia ou que entre em modo End of Life pelo período de 2 anos após a assinatura do contrato, não deixando de atender ao item 2.1.6 durante toda a vigência da garantia.	SIM	CONFORME PROPOSTA DE PREÇO
2	1	2.1.4.	O fabricante deverá atualizar firmwares e softwares da solução para novas versões durante toda a vigência da garantia.	SIM	CONFORME PROPOSTA DE PREÇO
2	1	2.1.5.	Todas as funcionalidades adquiridas de hardware e software devem operar conforme disposto neste Termo de Referência durante o prazo de garantia dos equipamentos, ou seja, o fornecedor deve garantir a atualização completa das funcionalidades no prazo referido, não sendo permitida a cobrança de quaisquer valores adicionais pelo uso dos hardwares e softwares para esse período. As funcionalidades deverão permanecer ativas, mesmo que não sejam atualizadas após o fim do prazo da garantia.	SIM	CONFORME PROPOSTA DE PREÇO
2	1	2.1.5.1.	Após o prazo da garantia, os equipamentos deverão permanecer com todas as funcionalidades operacionais, com as atualizações imediatamente anteriores a data final da garantia dos equipamentos.	SIM	CONFORME PROPOSTA DE PREÇO
2	1	2.1.5.2.	Somente a funcionalidade de filtro de conteúdo web poderá ser desativada ao final do prazo de garantia do equipamento; em razão de sua natureza técnica de acesso on-line as suas bases de dados.	SIM	CONFORME PROPOSTA DE PREÇO
2	1	2.1.5.3.	A garantia referida no item 2.1.5 terá início com a emissão do termo de recebimento definitivo da solução a ser gerado pela CONTRATANTE conforme disposto no item 12.4.	SIM	CONFORME PROPOSTA DE PREÇO
2	1	2.1.6.	As licenças de atualização de software (firmware ou drivers) e licenças de atualização de assinaturas deverão ser fornecidas pelo prazo mínimo de 60 (sessenta) meses, a contar da data do recebimento definitivo dos produtos, sem ônus adicional para as atualizações e seu	SIM	CONFORME PROPOSTA DE PREÇO



			USO.		
2	1	2.1.7.	Todos os equipamentos devem funcionar com alimentação nominal de 100~120VAC e 210~230VAC e frequência de 50 ou 60 Hz, ou auto-ranging. Deverá vir acompanhado de cabo de alimentação com, no mínimo, 1,80m (6 pés), com plug tripolar 2P+T no padrão ABNT NBR 14136.	SIM	Datasheet-BB-UTM-pt-BR-v1-4-28-08-2017-L1.pdf - PÁG 07
2	1	2.1.8.	O equipamento deve possuir 1 (uma) porta de console para configuração e gerenciamento por interface de linha de comando (CLI).	SIM	Datasheet-BB-UTM-pt-BR-v1-4-28-08-2017-L1.pdf - PÁG 07
2	1	2.1.8.1.	Deve ser fornecido pelo menos 1 (um) cabo conversor Serial para USB, compatível com a porta de console do equipamento.	SIM	Datasheet-BB-UTM-pt-BR-v1-4-28-08-2017-L1.pdf - PÁG 07
2	1	2.1.9.	O equipamento deve ser fornecido com todas as suas portas de comunicação, interfaces e afins habilitadas, operacionais e sem custos adicionais, mesmo que para futuras utilizações do órgão ou entidade CONTRATANTE.	SIM	CONFORME PROPOSTA DE PREÇO
2	1	2.1.9.1.	A CONTRATADA deve entregar a quantidade de transceivers equivalente ao dobro da quantidade mínima de portas exigidas em cada lote conforme os itens 3.15.1.4, 3.22.1.4 e 3.29.1.4.	NÃO SE APLICA	
2	1	2.1.9.2.	Em caso de defeito ou mau funcionamento dos transceivers, estes devem estar cobertos pela garantia da solução.	NÃO SE APLICA	
2	1	2.1.10.	O equipamento deve ser fornecido em hardware dedicado: tipo appliance ou chassi, com sistema operacional otimizado, do mesmo fabricante, para o uso como firewall corporativo multifuncional.	SIM	CONFORME PROPOSTA DE PREÇO
2	1	2.1.10.1.	Os equipamentos dos lotes 1, 2, 3 e 4 da solução ofertada, não deverão exceder, individualmente, 4 Unidades de Rack, sendo "caixas" únicas, sem empilhamentos.	SIM	CONFORME PROPOSTA DE PREÇO

2	1	2.1.10.2.	O equipamento do lote 5 da solução ofertada, pode ser baseado em appliance ou chassi, deverá ter atestada, pelo fabricante, a compatibilidade entre os módulos e o chassi e deverá suportar agregação de enlaces multi-chassi (MC-LAG), segundo padrão IEEE 802.1ax.	NÃO SE APLICA		
2	1	2.1.11.	Deve possuir fonte(s) de energia atendendo aos itens 3.1.1.3, 3.8.1.3, 3.15.1.3, 3.22.1.3 e 3.29.1.3.	SIM	Datasheet-BB-UTM-pt-BR-v1-4-28-08-2017-L1.pdf - PÁG 07	
2	1	2.1.12.	Deve suportar topologias de cluster redundante de alta disponibilidade (failover) no mínimo aos pares, nos modos ativo-ativo e ativo-passivo, com sincronização, em tempo real, de configuração e de estados das sessões. No caso de falha de um dos equipamentos do cluster, não deverá haver perda das configurações e nem das sessões já estabelecidas e a transição entre os equipamentos deverá acontecer de forma transparente para o usuário.	SIM	user_manual_utm_pt_BR.compressed.pdf - pag. 45	
2	1	2.1.13.	Deve suportar a implementação tanto em modo transparente (camada 2) quanto em modo gateway (camada 3).	SIM	Datasheet-BB-UTM-pt-BR-v1-4-28-08-2017-L1.pdf - PÁG 08	
2	1	2.1.14.	Possuir filtragem de pacote por endereço IP de origem e destino, por aplicação (independentemente da porta ou protocolo utilizados pela aplicação), por sub-rede e por períodos do dia, permitindo a aplicação de regras por horários e por dias da semana.	SIM	user_manual_utm_pt_BR.compressed.pdf - pag. 280, 282, 287, 290.	
2	1	2.1.15.	Permitir criação de serviços por porta ou conjunto de portas para, no mínimo, os protocolos TCP, UDP, ICMP e IP.	SIM	user_manual_utm_pt_BR.compressed.pdf - pag. 96 à 98	
2	1	2.1.16.	Suportar tags de VLAN;	SIM	user_manual_utm_pt_BR.compressed.pdf - pag. 34	
2	1	2.1.17.	Permitir a criação de no mínimo 25 VLANs padrão 802.1q para os firewalls especificados nos lotes 1, no mínimo 50 VLANs padrão 802.1q para os firewalls do lote 2 e no mínimo 500 VLANs padrão 802.1q para os firewalls especificados nos lotes 3, 4 e 5.	SIM	Datasheet-BB-UTM-pt-BR-v1-4-28-08-2017-L1.pdf - PÁG 09	
2	1	2.1.18.	Ser capaz de aceitar comandos de scripts acionados por sistemas	SIM	Datasheet-BB-UTM-pt-BR-v1-4-28-08-2017-L1.pdf - PÁG 09	



			externos como, por exemplo, correlacionadores de eventos;			
2	1	2.1.19.	Suportar o bloqueio de tráfego em função da localização geográfica dos IPs de origem e de destino;	SIM	user_manual_utm_pt_BR.compressed.pdf - pag. 195	
2	1	2.1.20.	Suportar agregação de links, segundo padrão IEEE 802.3ad, nos equipamentos firewall descritos nos lotes 3, 4 e 5.	NÃO SE APLICA		
2	1	2.1.21.	Possuir ferramenta de diagnóstico do tipo tcpdump.	SIM	Datasheet-BB-UTM-pt-BR-v1-4-28-08-2017-L1.pdf - PÁG 09	
2	1	2.1.21.1.	Suportar e efetuar a captura de pacotes no formato PCAP.	SIM	Datasheet-BB-UTM-pt-BR-v1-4-28-08-2017-L1.pdf - PÁG 09	
2	1	2.1.21.2.	Suportar e efetuar o download dos arquivos PCAP.	SIM	Datasheet-BB-UTM-pt-BR-v1-4-28-08-2017-L1.pdf - PÁG 09	
2	1	2.1.22.	Não deve possuir restrições de licenciamento em relação às características, requisitos e funcionalidades presentes nos subitens do item 2.1, inclusive em relação ao número ou tipo de clientes, usuários, máquinas e endereços IP.	SIM	CONFORME PROPOSTA DE PREÇO	
2	1	2.1.23.	Deve suportar, no próprio firewall, autenticação de usuários locais e integração com serviços de autenticação de diretório LDAP, Microsoft Active Directory e RADIUS, sendo que:	SIM	Datasheet-BB-UTM-pt-BR-v1-4-28-08-2017-L1.pdf - PÁG 09	
2	1	2.1.23.1.	Não deverão existir limitações de licenciamento quanto ao número de usuários, a não ser o limite operacional do equipamento, respeitado o quantitativo mínimo especificado em cada lote;	SIM	CONFORME PROPOSTA DE PREÇO	
2	1	2.1.23.2.	Deve registrar a identificação do usuário em todos os eventos associados gerados pelo equipamento, tais como (mas não restrito a) eventos de autenticação, registros de acesso ou bloqueio e eventos associados a ameaças;	SIM	Datasheet-BB-UTM-pt-BR-v1-4-28-08-2017-L1.pdf - PÁG 09	
2	1	2.1.23.3.	Deve prover identificação de forma transparente aos usuários autenticados por single sign-on, no mínimo, por meio dos serviços Microsoft Active Directory e RADIUS;	SIM	user_manual_utm_pt_BR.compressed.pdf - pag. 118, 135	
2	1	2.1.23.4.	Deve prover portal ou pop-up de login para identificação dos usuários dos demais serviços de LDAP não listados no item anterior;	SIM	user_manual_utm_pt_BR.compressed.pdf - pag. 140	

2	1	2.1.23.5.	Deve permitir a criação de regras de acesso/bloqueio baseadas em usuários ou grupo de usuários do LDAP e do Microsoft Active Directory;	SIM	user_manual_utm_pt_BR.compressed.pdf - pag. 113, 283	
2	1	2.1.23.6.	Não será permitida a utilização de agentes instalados nos equipamentos dos usuários;	SIM	CONFORME PROPOSTA DE PREÇO	
2	1	2.1.23.7.	Possuir métodos de autenticação de usuários para aplicações executadas sobre os protocolos TCP, tais como (mas não restritos a) aplicações HTTP, HTTPS e FTP;	SIM	user_manual_utm_pt_BR.compressed.pdf - pag. 280, 283, 284	
2	1	2.1.24.	Suportar Network Address Translation (NAT 1-1, NAT 1-N, NAT N-1) de acordo com a RFC 3022, nos modos estático e dinâmico;	SIM	Datasheet-BB-UTM-pt-BR-v1-4-28-08-2017-L1.pdf - PÁG 08	
2	1	2.1.25.	Deve suportar no mínimo NAT 64,	SIM	Datasheet-BB-UTM-pt-BR-v1-4-28-08-2017-L1.pdf - PÁG 09	
2	1	2.1.26.	Possuir a funcionalidade de fazer tradução de endereços dinâmicos um-para-N, PAT (Port Address Translation);	SIM	Datasheet-BB-UTM-pt-BR-v1-4-28-08-2017-L1.pdf - PÁG 08	
2	1	2.1.27.	Suportar nativamente IPv6;	SIM	Datasheet-BB-UTM-pt-BR-v1-4-28-08-2017-L1.pdf - PÁG 09	
2	1	2.1.27.1.	Suportar, no mínimo, os protocolos de roteamento dinâmico OSPF v3 e BGP, bem como as funcionalidades de roteamento estático e roteamento policy-based	SIM	Datasheet-BB-UTM-pt-BR-v1-4-28-08-2017-L1.pdf - PÁG 09	
2	1	2.1.28.	Possuir funcionalidades de DHCP client, server e relay;	SIM	user_manual_utm_pt_BR.compressed.pdf - pag. 210 Installation_guide_utm-pt_BR_01-01-marco-v1.pdf - pag. 19, 20	
2	1	2.1.29.	Possuir proteção e suporte a protocolos de Real Time, contemplando no mínimo: Real Time Transport Protocol (RTP), H323 e SIP sobre os protocolos IPV4 ou IPV6,	SIM	Datasheet-BB-UTM-pt-BR-v1-4-28-08-2017-L1.pdf - PÁG 08	
2	1	2.1.30.	Possuir tecnologia de firewall stateful;	SIM	user_manual_utm_pt_BR.compressed.pdf - pag. 150	
2	1	2.1.31.	Permitir a realização de backup e restore das regras, configurações e políticas, e a transferência desse backup para armazenamento em servidores externos;	SIM	user_manual_utm_pt_BR.compressed.pdf - pag. 74, 75	
2	1	2.1.32.	Possuir funcionalidade de detecção e bloqueio de, no mínimo, os seguintes tipos de ataques: IP Spoofing, SYN Flood, UDP Flood, Port Scanning, ICMP Flood, ICMP sweep, Ataques de Força Bruta ataques Man-In-the-	SIM	Datasheet-BB-UTM-pt-BR-v1-4-28-08-2017-L1.pdf - PÁG 08	



			Middle e variações de reflexão;			
2	1	2.1.33.	Suportar sincronização de horário por NTP;	SIM	user_manual_utm_pt_BR.compressed.pdf - pag. 31, 413	
2	1	2.1.34.	Possuir funcionalidade de geração de relatórios e exportação de logs;	SIM	user_manual_utm_pt_BR.compressed.pdf - pag. 27, 29	
2	1	2.1.35.	Suportar no mínimo 250 regras ou políticas de firewall para os equipamentos do lote 1 e 1.000 regras ou políticas de firewall para os equipamentos dos lotes 2,3,4 e 5.	SIM	DECLARAÇÃO DO FABRICANTE	
2	1	2.1.36.	Permitir a abertura de novas portas por fluxo de dados para serviços que requerem portas dinâmicas;	SIM	Datasheet-BB-UTM-pt-BR-v1-4-28-08-2017-L1.pdf - PÁG 08	
2	1	2.1.37.	Possuir mecanismo de anti-spoofing;	SIM	Datasheet-BB-UTM-pt-BR-v1-4-28-08-2017-L1.pdf - PÁG 08	
2	1	2.1.38.	Possuir funcionalidade de exceção em SSL Inspection para sites e aplicações bancárias, não decriptando o tráfego dessas sessões.	SIM	user_manual_utm_pt_BR.compressed.pdf - pag. 285	
2	1	2.1.39.	Possuir inspeção profunda de pacotes para tráfego criptografado (no mínimo em tráfego VPN e HTTPS);	SIM	Datasheet-BB-UTM-pt-BR-v1-4-28-08-2017-L1.pdf - PÁG 08	
2	1	2.1.40.	Possuir, no mínimo, suporte a SNMP v2 e v3;	SIM	Datasheet-BB-UTM-pt-BR-v1-4-28-08-2017-L1.pdf - PÁG 09	
2	1	2.1.41.	Deve possuir MIB própria contemplando, no mínimo, indicadores de estado do hardware e de performance do equipamento;	SIM	CONFORME PROPOSTA DE PREÇO	
2	1	2.1.42.	Deve identificar os países de origem e destino de todas as sessões estabelecidas através do equipamento, exceto para sessões no âmbito da rede interna (não roteadas).	SIM	Datasheet-BB-UTM-pt-BR-v1-4-28-08-2017-L1.pdf - PÁG 08	
2	1	2.1.43.	Deve permitir a criação de políticas de segurança baseadas em geolocalização, permitindo o bloqueio de tráfego com origem ou destino a determinado país ou grupo de países.	SIM	Datasheet-BB-UTM-pt-BR-v1-4-28-08-2017-L1.pdf - PÁG 08	
2	1	2.1.44.	Deve possibilitar a visualização dos países de origem e destino nos logs de eventos, de acessos e ameaças.	SIM	Datasheet-BB-UTM-pt-BR-v1-4-28-08-2017-L1.pdf - PÁG 08	

2	1	2.1.45.	Deve prover interface de gerência local do firewall ou do cluster (virtual ou físico) do qual o firewall faz parte, por meio de interface gráfica (GUI) e linha de comando – (CLI) ou via SSH. Especificamente a interface gráfica (GUI) deve atender as funcionalidades gerenciais previstas nos subitens 2.1.45.1 ao 2.1.45.14.	SIM	user_manual_utm_pt_BR.compressed.pdf - pag. 151	
2	1	2.1.45.1.	Deve possuir a capacidade de definir administradores com diferentes perfis de acesso. Os perfis de acesso devem ser, no mínimo, de leitura/escrita e somente leitura.	SIM	user_manual_utm_pt_BR.compressed.pdf - pag. 61	
2	1	2.1.45.2.	Deve permitir a delegação de funções de administração.	SIM	user_manual_utm_pt_BR.compressed.pdf - pag. 61	
2	1	2.1.45.3.	Deve registrar em log as ações dos usuários administradores.	SIM	user_manual_utm_pt_BR.compressed.pdf - pag. 64	
2	1	2.1.45.4.	Deve suportar a identificação e utilização de usuários nas políticas de segurança.	SIM	user_manual_utm_pt_BR.compressed.pdf - pag. 283	
2	1	2.1.45.5.	Deve suportar agrupamento lógico de objetos ("object grouping") para criação de regras.	SIM	user_manual_utm_pt_BR.compressed.pdf - pag. 90	
2	1	2.1.45.6.	Deve possibilitar o gerenciamento (incluindo a criação, alteração, monitoramento e exclusão) de objetos de rede. Deverá ainda permitir detectar se e onde, na base de regras, está sendo utilizado determinado objeto de rede. Os tipos de objetos deverão permitir especificar de forma distinta grupos e objetos de rede e serviços, diferenciando-os e agrupando-os conforme suas características ou descrição de maneira a permitir o reaproveitamento dos mesmos em diferentes políticas.	SIM	user_manual_utm_pt_BR.compressed.pdf - pag. 90 à 110. CONFORME PROPOSTA DE PREÇO	
2	1	2.1.45.7.	Deve contabilizar a utilização ("hit counts") ou o volume de dados trafegados correspondente a cada regra de filtragem individualmente.	SIM	user_manual_utm_pt_BR.compressed.pdf - pag. 19	
2	1	2.1.45.8.	Deve possibilitar a especificação de política por tempo, ou seja, permitir a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora).	SIM	user_manual_utm_pt_BR.compressed.pdf - pag. 290, 100, 101, 102	
2	1	2.1.45.9.	Deve suportar a geração de alertas automáticos via email, SNMP e Syslog.	SIM	Datasheet-BB-UTM-pt-BR-v1-4-28-08-2017-L1.pdf - PÁG 09	



2	1	2.1.45.10.	Deve permitir a exportação de logs via SCP ou FTP.	SIM	Datasheet-BB-UTM-pt-BR-v1-4-28-08-2017-L1.pdf - PÁG 09	
2	1	2.1.45.11.	Deve informar a utilização dos recursos de CPU, memória, armazenamento interno e atividade de rede dos equipamentos gerenciados.	SIM	user_manual_utm_pt_BR.compressed.pdf - pag. 22, 340	
2	1	2.1.45.12.	Deve informar o número de sessões simultâneas e de novas sessões por segundo dos equipamentos gerenciados.	SIM	Datasheet-BB-UTM-pt-BR-v1-4-28-08-2017-L1.pdf - PÁG 03	
2	1	2.1.45.13.	Deve possuir visualização mínima sumarizada de: aplicações, ameaças, URLs, endereços de origem, endereços de destino, levando-se em conta o quantitativo de sessões, de consumo de banda e categorização.	SIM	Datasheet-BB-UTM-pt-BR-v1-4-28-08-2017-L1.pdf - PÁG 03	
2	1	2.1.45.14.	Deverá suportar gerência remota (via rede local ou WAN) ou por meio da gerência centralizada, sendo que:	SIM	Datasheet-BB-UTM-pt-BR-v1-4-28-08-2017-L1.pdf - PÁG 06	
2	1	2.1.45.14.1.	A comunicação entre a estação ou sistema de gerência e o firewall ou cluster local deverá ser criptografada e autenticada;	SIM	Datasheet-BB-UTM-pt-BR-v1-4-28-08-2017-L1.pdf - PÁG 06	
2	1	2.1.46.	Deve permitir o controle e a priorização do tráfego, priorizando e garantindo banda para as aplicações (inbound/outbound) através da classificação dos pacotes (shaping);	SIM	Datasheet-BB-UTM-pt-BR-v1-4-28-08-2017-L1.pdf - PÁG 06	
2	1	2.1.47.	Deve possuir gerenciamento gráfico centralizado das funcionalidades de QoS/Traffic Shaping integrado tanto com a gerência local do equipamento, quanto com a gerência centralizada da solução;	SIM	Datasheet-BB-UTM-pt-BR-v1-4-28-08-2017-L1.pdf - PÁG 06	
2	1	2.1.48.	Deve suportar a criação de políticas de controle de uso de largura de banda, limitando ou expandido individualmente, baseadas em: porta ou protocolo, endereço IP de origem ou destino, grupo de usuários do Microsoft Active Directory e LDAP e aplicações (por exemplo, Youtube e WhatsApp).	SIM	user_manual_utm_pt_BR.compressed.pdf - pag. 293, 281 à 298	
2	1	2.1.49.	As funcionalidades de VPN não podem possuir qualquer restrição de licenciamento, inclusive em relação ao número de clientes, aos softwares instalados nos clientes, IPs e máquinas, limitado apenas à capacidade de throughput do equipamento para VPN.	SIM	CONFORME PROPOSTA DE PREÇO	

2	1	2.1.50.	Deve permitir a arquitetura de VPN hub and spoke IPSec, tanto para topologias site-to-site ("Full Meshed" e "Estrela") como para client-to-site (remote access);	SIM	Datasheet-BB-UTM-pt-BR-v1-4-28-08-2017-L1.pdf - PÁG 05	
2	1	2.1.51.	Deve permitir a criação de túneis VPN SSL/TLS;	SIM	user_manual_utm_pt_BR.compressed.pdf - pag. 251	
2	1	2.1.52.	Deve permitir a criação de túneis VPN IPSec;	SIM	user_manual_utm_pt_BR.compressed.pdf - pag. 229	
2	1	2.1.53.	A funcionalidade de VPN prevista no item anterior poderá ser atendida por meio de dispositivo standalone, caso o appliance do firewall não possua tal funcionalidade, sem prejuízo do gerenciamento centralizado da solução previsto nos itens 2.1.69 e 2.2;	SIM	NÃO APLICÁVEL	
2	1	2.1.54.	Deve permitir que o usuário realize a conexão VPN por meio de cliente instalado no sistema operacional do seu equipamento ou por meio de Interface Web do tipo portal.	SIM	user_manual_utm_pt_BR.compressed.pdf - pag. 251	
2	1	2.1.54.1.	Caso seja por meio de cliente instalado, deverá estar disponível, no mínimo, para os sistemas operacionais Windows (Vista, 7, 8 e 10). Caso não existam clientes (softwares) dos próprios fabricantes instaláveis para os sistemas operacionais: Linux, Mac OS X, Apple iOS e Google Android, deverá a Licitante fornecer gratuitamente softwares de terceiros que sejam totalmente compatíveis com os sistemas operacionais referidos.	SIM	CONFORME PROPOSTA DE PREÇO	
2	1	2.1.54.2.	O acesso por meio da Interface Web deverá ser compatível com, no mínimo, os navegadores Internet Explorer 9 ou superior e Firefox 4.0 ou superior.	SIM	Datasheet-BB-UTM-pt-BR-v1-4-28-08-2017-L1.pdf - PÁG 02	
2	1	2.1.55.	Deve suportar a customização da Interface Web para acesso a VPN pelos administradores do sistema, incluindo quais aplicativos, servidores e sistemas estarão acessíveis via portal;	SIM	user_manual_utm_pt_BR.compressed.pdf - pag. 251 à 269	
2	1	2.1.56.	Suportar algoritmos de criptografia para túneis VPN AES-128 e AES-256;	SIM	Datasheet-BB-UTM-pt-BR-v1-4-28-08-2017-L1.pdf - PÁG 08	
2	1	2.1.57.	Suportar os algoritmos para definição de chave de cifração 3DES e AES;	SIM	Datasheet-BB-UTM-pt-BR-v1-4-28-08-2017-L1.pdf - PÁG 08	
2	1	2.1.58.	Suportar os algoritmos RSA, Diffie-Hellman/RSA;	SIM	Datasheet-BB-UTM-pt-BR-v1-4-28-08-2017-L1.pdf - PÁG 08	



2	1	2.1.59.	Suportar Certificado Digital X.509 v3;	SIM	Datasheet-BB-UTM-pt-BR-v1-4-28-08-2017-L1.pdf - PÁG 08	
2	1	2.1.60.	Suportar a inclusão (enrollment) de autoridades certificadoras;	SIM	Datasheet-BB-UTM-pt-BR-v1-4-28-08-2017-L1.pdf - PÁG 08	
2	1	2.1.61.	Permitir alteração dos algoritmos criptográficos das VPNs;	SIM	Datasheet-BB-UTM-pt-BR-v1-4-28-08-2017-L1.pdf - PÁG 08	
2	1	2.1.62.	Suportar IKE – Internet Key Exchange, fases I e II;	SIM	Datasheet-BB-UTM-pt-BR-v1-4-28-08-2017-L1.pdf - PÁG 08	
2	1	2.1.63.	Suportar os protocolos de roteamento RIPv2, OSPFv2 ou OSPFv3 para as funcionalidades de VPN;	SIM	Datasheet-BB-UTM-pt-BR-v1-4-28-08-2017-L1.pdf - PÁG 08	
2	1	2.1.64.	Implementar autenticação de usuários utilizando LDAP, Microsoft Active Directory, RADIUS e certificados digitais e suportar, no mínimo, autenticação two-way com certificado digital e LDAP ou Microsoft Active Directory ou RADIUS	SIM	Datasheet-BB-UTM-pt-BR-v1-4-28-08-2017-L1.pdf - PÁG 08	
2	1	2.1.65.	Suportar certificados emitidos por autoridade certificadora no padrão ICP-Brasil;	SIM	Datasheet-BB-UTM-pt-BR-v1-4-28-08-2017-L1.pdf - PÁG 08	
2	1	2.1.66.	Suportar leitura e verificação de Certificate Revocation List (CRL);	SIM	Datasheet-BB-UTM-pt-BR-v1-4-28-08-2017-L1.pdf - PÁG 08	
2	1	2.1.67.	Suportar NAT Transversal Tunneling (NAT-T);	SIM	Datasheet-BB-UTM-pt-BR-v1-4-28-08-2017-L1.pdf - PÁG 08	
2	1	2.1.68.	Possuir gerenciamento gráfico das funcionalidades de VPN e monitoramento de seus eventos de forma integrada tanto com a gerência local do equipamento ou do cluster quanto com a gerência centralizada da solução.	SIM	DECLARAÇÃO DO FABRICANTE	
2	1	2.1.69.	VPN gateway-a-gateway deverá possuir interoperabilidade com os gateways de VPN pelo menos dos seguintes fabricantes: Cisco, Checkpoint, Juniper, Palo Alto Networks, Fortinet, AKER, BluePEX, PFSense e SonicWall.	SIM	DECLARAÇÃO DO FABRICANTE	
2	1	2.1.70.	Deve permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis de SSL.	SIM	user_manual_utm_pt_BR.compressed.pdf - pag. 285	
2	1	2.1.71.	O equipamento deve ser apropriado para o uso em ambiente tropical com umidade relativa na faixa de 20 a 85% (sem condensação) e temperatura ambiente na faixa de 5 a 40°C.	SIM	Datasheet-BB-UTM-pt-BR-v1-4-28-08-2017-L1.pdf - PÁG 07	
2	14	2.2.	<b>Solução de gerência centralizada</b>			



2	14	2.2.1.	Deverá ser fornecida solução de gerência centralizada dos firewalls, do mesmo fabricante e independente (externa) em relação aos equipamentos, sendo que:	SIM	CONFORME PROPOSTA DE PREÇO
2	14	2.2.1.1.	A solução poderá ser fornecida baseada em "appliance especializado" – equipamento especializado para gerência centralizada, ou "appliance virtual" - solução de software executada em máquina virtual que possa ser instalado e executado em ambientes virtuais ou componentes de software instaláveis em sistemas operacionais padrão servidor;	SIM	CONFORME PROPOSTA DE PREÇO
2	14	2.2.1.2.	Quando a solução for baseada em "appliance especializado", ou quando quaisquer outros equipamentos forem fornecidos para compor a solução, deverão:	SOLUÇÃO SERÁ ENTREGUE EM APPLIANCE VIRTUAL	
2	14	a)	ser compatíveis com rack padrão 19 polegadas;		
2	14	b)	possuir, no mínimo, duas interfaces de rede Gigabit Ethernet;		
2	14	c)	possuir fonte de energia com os mesmos parâmetros definidos no item 2.1.7;e		
2	14	d)	possuir, no mínimo, o espaço de armazenamento solicitado no respectivo item 7 de cada um dos lotes do item 3;		
2	14	2.2.1.3.	Quando a solução for baseada em appliance virtual, deverá ser capaz de ser executada em pelo menos uma das seguintes plataformas virtualizadoras: VMware ESXi, Xen, KVM ou Microsoft Hyper-V, cujo ambiente será fornecido pela CONTRATANTE, não sendo necessário o fornecimento da licença da plataforma virtualizadora. Caso o equipamento ou ambiente virtualizado disponibilizado pela CONTRATANTE seja incompatível com os requisitos mínimos necessários para execução completa da solução baseada em appliance virtual, a ponto de inviabilizar ou prejudicar o seu funcionamento e a fabricante da solução não possua	SIM	Datasheet-BB-UTM-pt-BR-v1-4-28-08-2017-L1.pdf - PÁG 02



			outra alternativa de fornecimento dentre aquelas dispostas nos itens 2.2.1.1, 2.2.1.2 e 2.2.1.4, deverá ser fornecido equipamento com ambiente virtual compatível, observado o disposto no item 2.2.1.2;			
2	14	2.2.1.4.	Quando a solução for baseada em componentes de software, deverão ser fornecidas e implantadas, em caráter perpétuo, todas as licenças dos softwares e sistemas operacionais necessários ao funcionamento da solução, em versões para servidor, sendo que a versão fornecida de sistema operacional não poderá entrar em modo End of Support nos 60 (sessenta) meses a contar da data de assinatura do contrato.	SOLUÇÃO SERÁ ENTREGUE EM APPLIANCE VIRTUAL		
2	14	2.2.2.	Deve permitir a gerência centralizada dos equipamentos e contextos virtuais que compõem a solução de alta disponibilidade, devendo ser dimensionada e devidamente licenciada para atender, no mínimo, o número total de equipamentos físicos gerenciados e o número total de contextos virtuais possíveis, compatível com o limite operacional dos equipamentos e clusters gerenciados.	SIM	CONFORME PROPOSTA DE PREÇO	
2	14	2.2.3	Deve ser licenciada de forma a não limitar número de usuários, objetos, regras de segurança, NAT e endereços IP.	SIM	CONFORME PROPOSTA DE PREÇO	
2	14	2.2.4.	Deve ser licenciada de forma a permitir a captura e filtragem de todos os eventos gerados por todos os equipamentos e contextos virtuais que compõe a solução de alta disponibilidade.	SIM	CONFORME PROPOSTA DE PREÇO	

2	14	2.2.5.	Deve permitir a criação e distribuição de políticas de segurança e de objetos de rede de forma centralizada.	SIM	Datasheet-BB-UTM-pt-BR-v1-4-28-08-2017-L1.pdf - PÁG 03	
2	14	2.2.6.	Deve permitir a criação de relatórios customizados.	SIM	Datasheet-BB-UTM-pt-BR-v1-4-28-08-2017-L1.pdf - PÁG 03	
2	14	2.2.7.	Deve possibilitar a filtragem dos logs do equipamento por, no mínimo: aplicação, endereço IP de origem e destino, país de origem e destino, usuário e horário.	SIM	Datasheet-BB-UTM-pt-BR-v1-4-28-08-2017-L1.pdf - PÁG 03	
2	14	2.2.8.	Deve possuir relatórios com informações consolidadas sobre: as mais frequentes fontes de sessões bloqueadas com seus destinos e serviços, os mais frequentes ataques e ameaças de segurança detectadas com suas origens e destinos, os serviços de rede mais utilizados, as aplicações maiores consumidoras de banda de Internet, os usuários que consomem mais banda de Internet, os sítios na Internet mais visitados.	SIM	Datasheet-BB-UTM-pt-BR-v1-4-28-08-2017-L1.pdf - PÁG 03	
2	14	2.2.9.	Deve permitir a geração automática e agendada dos relatórios.	SIM	Datasheet-BB-UTM-pt-BR-v1-4-28-08-2017-L1.pdf - PÁG 03	
2	14	2.2.10.	Deve ser capaz de automatizar a aplicação das regras, objetos e políticas desejadas em tempo real a todos os equipamentos e contextos virtuais administrados.	SIM	Datasheet-BB-UTM-pt-BR-v1-4-28-08-2017-L1.pdf - PÁG 03	
2	14	2.2.11.	Deverá utilizar comunicação segura criptografada entre a solução de gerência e os equipamentos gerenciados.	SIM	Datasheet-BB-UTM-pt-BR-v1-4-28-08-2017-L1.pdf - PÁG 03	
2	14	2.2.12.	Deverá manter o histórico de configurações enviadas aos equipamentos e deverá permitir o rollback das configurações.	SIM	Datasheet-BB-UTM-pt-BR-v1-4-28-08-2017-L1.pdf - PÁG 03	
2	14	2.2.13.	Deve permitir distribuição centralizada de pacotes de atualização.	SIM	Datasheet-BB-UTM-pt-BR-v1-4-28-08-2017-L1.pdf - PÁG 03	
2	14	2.2.14.	Deve permitir validar as regras antes, durante ou depois de aplicá-las.	SIM	Datasheet-BB-UTM-pt-BR-v1-4-28-08-2017-L1.pdf - PÁG 03	
2	14	2.2.15.	Deve ser capaz de testar a conectividade dos equipamentos gerenciados.	SIM	Datasheet-BB-UTM-pt-BR-v1-4-28-08-2017-L1.pdf - PÁG 03	
2	14	2.2.16.	Deve prover funcionalidade de detecção de regras conflitantes ou regras equivalentes.	SIM	Datasheet-BB-UTM-pt-BR-v1-4-28-08-2017-L1.pdf - PÁG 03	
2	9	2.3.	<b>Conjunto de funcionalidades IPS/IDS</b>			
2	9	2.3.1.	Possuir tecnologia de detecção e prevenção de ataques e intrusões	SIM	Datasheet-BB-UTM-pt-BR-v1-4-28-08-2017-L1.pdf - PÁG 08	



			baseada em assinatura;		
2	9	2.3.2.	Possuir, no mínimo, um conjunto de 2.000 (duas mil) assinaturas de detecção e prevenção de ataques, devendo também detectar ataques baseados em anomalias;	SIM	Datasheet-BB-UTM-pt-BR-v1-4-28-08-2017-L1.pdf - PÁG 08
2	9	2.3.3.	Decodificar múltiplos formatos de Unicode;	SIM	Datasheet-BB-UTM-pt-BR-v1-4-28-08-2017-L1.pdf - PÁG 08
2	9	2.3.4.	Suportar fragmentação e desfragmentação IP;	SIM	Datasheet-BB-UTM-pt-BR-v1-4-28-08-2017-L1.pdf - PÁG 08
2	9	2.3.5.	Detectar protocolos independentemente da porta utilizada, identificando aplicações conhecidas em portas não-padrão;	SIM	Datasheet-BB-UTM-pt-BR-v1-4-28-08-2017-L1.pdf - PÁG 05
2	9	2.3.6.	Detectar e Proteger contra, no mínimo, ataques de RPC (Remote Procedure Call), Windows ou NetBios, SMTP (Simple Message Transfer Protocol), IMAP (Internet Message Access Protocol), Sendmail ou POP (Post Office Protocol), DNS (Domain Name System), FTP, SSH, Telnet, ICMP (Internet Control Message Protocol), SIP, SNMP, SSDP ou CHARGEN, RDP (Remote Desktop Protocol), DoS (Denial of Service) e ataques com assinaturas complexas, tais como ataques TCP hijacking.	SIM	2.3.6. Assinaturas de IPS.pdf
2	9	2.3.7.	Possuir proteção contra os ataques como, mas não restringindo-se aos mesmos: 1) Ataques de Worm, Trojan, Backdoors, Portscans, IP Spoofing, DoS, Spywares, Botnets e malwares em geral; 2) Ataques e utilização de tecnologia P2P; 3) Ataques de estouro de pilha (buffer overflow); 4) Tráfego mal formado; 5) Cabeçalhos inválidos de protocolo; 6) Ataques de injeção (SQL Injection, LDAP Injection) e de Cross-Site Scripting; 7) Elevação de privilégio e 8) Exploits - Web Server, Web Browser, ActiveX, JavaScript, Browser Plug-ins/Add-ons.	SIM	2.3.7. Assinaturas de IPS.pdf
2	9	2.3.8.	Emitir alarmes na console de administração integrada, alertas via correio eletrônico, syslog e traps SNMP;	SIM	Datasheet-BB-UTM-pt-BR-v1-4-28-08-2017-L1.pdf - PÁG 05
2	9	2.3.9.	Permitir monitoração do comportamento do equipamento mediante o protocolo SNMP;	SIM	Datasheet-BB-UTM-pt-BR-v1-4-28-08-2017-L1.pdf - PÁG 09

2	9	2.3.10.	Atualizar automaticamente as assinaturas para o sistema de detecção de intrusos;	SIM	Datasheet-BB-UTM-pt-BR-v1-4-28-08-2017-L1.pdf - PÁG 08	
2	9	2.3.11.	Permitir filtros de anomalias de tráfego estatístico de flooding, scan e source session limits;	SIM	Datasheet-BB-UTM-pt-BR-v1-4-28-08-2017-L1.pdf - PÁG 08	
2	9	2.3.12.	Permitir filtros de anomalias de protocolos, inclusive protocolos de aplicação (ex.: HTTP, SMTP, NTP, NetBIOS, HTTPS, FTP, DNS, SMB, RPC, SSH e Telnet);	SIM	Datasheet-BB-UTM-pt-BR-v1-4-28-08-2017-L1.pdf - PÁG 08	
2	9	2.3.13.	Deve resistir a técnicas de evasão ou ataques direcionados ao próprio equipamento, suportando, no mínimo, as técnicas: IP Packet Fragmentation, Stream Segmentation, RPC Fragmentation, URL Obfuscation, HTML Obfuscation, Payload Encoding, FTP Evasion e Layered Evasions.	SIM	Datasheet-BB-UTM-pt-BR-v1-4-28-08-2017-L1.pdf - PÁG 05	
2	9	2.3.14.	Possuir funcionalidade que permita desativar a análise de assinaturas e protocolos;	SIM	Datasheet-BB-UTM-pt-BR-v1-4-28-08-2017-L1.pdf - PÁG 05	
2	9	2.3.15.	Possuir funcionalidade que permita desativar a análise de ataques a partir de endereços/faixa IP específicos;	SIM	Datasheet-BB-UTM-pt-BR-v1-4-28-08-2017-L1.pdf - PÁG 05	
2	9	2.3.16.	Permitir o funcionamento mínimo do engine de IPS mesmo que a comunicação com o site do fabricante esteja fora de operação;	SIM	CONFORME PROPOSTA DE PREÇO	
2	9	2.3.17.	Possuir as estratégias de bloqueio e liberação selecionáveis, tanto por conjuntos de assinaturas quanto por cada assinatura;	SIM	CONFORME PROPOSTA DE PREÇO	
2	9	2.3.18.	Suportar a verificação de ataques na camada de aplicação;	SIM	Datasheet-BB-UTM-pt-BR-v1-4-28-08-2017-L1.pdf - PÁG 08	
2	9	2.3.19.	Possuir gerenciamento gráfico centralizado das funcionalidades de IPS/IDS e monitoramento de seus eventos de forma integrada com a gerência local e a gerência centralizada da solução.	SIM	Datasheet-BB-UTM-pt-BR-v1-4-28-08-2017-L1.pdf - PÁG 06	
2	9	2.3.20.	Reconhecer assinaturas seletivas e filtros de ataque que devem proteger contra ataques de negação de serviços automatizados, worms e vulnerabilidades conhecidas.	SIM	Datasheet-BB-UTM-pt-BR-v1-4-28-08-2017-L1.pdf - PÁG 08	
2	9	2.3.21.	Caso o IPS/IDS não trate parcialmente ou totalmente DoS, será aceito funcionalidade específica complementar.	SIM	NÃO APLICÁVEL	
2	10	2.4.	Conjunto de funcionalidades			

L



		<b>antivirus e anti-malware</b>			
2	10	2.4.1.	Possuir módulo de proteção de antivírus, anti-malware e anti-bot no mesmo equipamento do firewall;	SIM	Datasheet-BB-UTM-pt-BR-v1-4-28-08-2017-L1.pdf - PÁG 08
2	10	2.4.2	Possuir funcionalidade de varredura contra vírus e malwares em tráfego nos seguintes protocolos: HTTPS, HTTP e pelo menos dois dos seguintes: FTP, POP3, IMAP e SMTP	SIM	Datasheet-BB-UTM-pt-BR-v1-4-28-08-2017-L1.pdf - PÁG 08
2	10	2.4.3.	Deve ser capaz de, se houver algum atraso ou falha na realização da atualização automática, o equipamento deve ter a capacidade de alertar imediatamente o administrador através de logs, e-mail ou outros meios de alerta	SIM	DECLARAÇÃO DO FABRICANTE
2	10	2.4.4.	Deve possuir serviço de atualização automática e manual de assinaturas com o fabricante	SIM	user_manual_utm_pt_BR.compressed.pdf - pag. 44
2	10	2.4.5.	Suportar funcionamento mínimo da engine de antivírus e anti-malwares mesmo que a comunicação com o site do fabricante esteja fora de operação;	SIM	CONFORME PROPOSTA DE PREÇO
2	10	2.4.6.	Possuir gerenciamento gráfico centralizado das funcionalidades de antivírus e anti-malware integrado com a gerência local e a gerência centralizada da solução.	SIM	Datasheet-BB-UTM-pt-BR-v1-4-28-08-2017-L1.pdf - PÁG 06
2	10	2.4.7.	Identificação, classificação e bloqueio de malwares, contemplando no mínimo, Trojan, Spywares, Backdoors, Worms e Virus;	SIM	Datasheet-BB-UTM-pt-BR-v1-4-28-08-2017-L1.pdf - PÁG 08
2	11	2.5.	<b>Conjunto de funcionalidades para tratamento de conteúdo web</b>		
2	11	2.5.1.	Deve possuir funcionalidades de tratamento de conteúdo web, devendo sua base de dados conter, no mínimo, 10 (dez) milhões de sites internet web já registrados e classificados, distribuídos em, no mínimo, 40 (quarenta) categorias ou subcategorias pré-definidas;	SIM	Datasheet-BB-UTM-pt-BR-v1-4-28-08-2017-L1.pdf - PÁG 08
2	11	2.5.2.	Permitir a criação de categorias personalizadas;	SIM	Datasheet-BB-UTM-pt-BR-v1-4-28-08-2017-L1.pdf - PÁG 08
2	11	2.5.3.	Permitir a categorização e reclassificação de sites web por URL;	SIM	Datasheet-BB-UTM-pt-BR-v1-4-28-08-2017-L1.pdf - PÁG 08
2	11	2.5.4.	Suportar filtragem e categorização das URLs;	SIM	Datasheet-BB-UTM-pt-BR-v1-4-28-08-2017-L1.pdf - PÁG 08
2	11	2.5.5.	Possuir integração com serviços de diretório LDAP e Microsoft Active	SIM	Datasheet-BB-UTM-pt-BR-v1-4-28-08-2017-L1.pdf - PÁG 08



			Directory para autenticação de usuários;			
2	11	2.5.6.	Permitir a criação de regras de acesso/bloqueio baseadas em usuários ou grupo de usuários do LDAP e do Microsoft Active Directory;	SIM	user_manual_utm_pt_BR.compressed.pdf - pag. 283, 113	
2	11	2.5.7.	Permitir a criação de regras para acesso/bloqueio por endereço IP de origem e sub-rede de origem;	SIM	user_manual_utm_pt_BR.compressed.pdf - pag. 282	
2	11	2.5.8.	Permitir a criação de quotas de utilização por horário, ou por categorias, ou por aplicações;	SIM	user_manual_utm_pt_BR.compressed.pdf - pag. 294	
2	11	2.5.9.	Deve ser capaz de exibir mensagem de bloqueio customizável pelos Administradores para resposta aos usuários, na tentativa de acesso a recursos proibidos ou restringidos pela política de segurança do órgão;	SIM	user_manual_utm_pt_BR.compressed.pdf - pag. 183	
2	11	2.5.10.	Permitir o bloqueio de páginas web por meio da construção de filtros específicos com mecanismo de busca textual;	SIM	Datasheet-BB-UTM-pt-BR-v1-4-28-08-2017-L1.pdf - PÁG 08	
2	11	2.5.10.1.	O item 2.5.10 pode ser atendido através da criação de aplicações em camada 7 customizadas.	NÃO SE APLICA		
2	11	2.5.11.	Permitir o bloqueio de URLs cujo campo CN ou DN não contém um domínio válido para o certificado SSL;	SIM	Datasheet-BB-UTM-pt-BR-v1-4-28-08-2017-L1.pdf - PÁG 08	
2	11	2.5.12.	Permitir o bloqueio de páginas web por classificação, tais como páginas de streaming, rádio e tv online, P2P, URLs originadas de spam, sites de proxy anônimos, entre outros.	SIM	Datasheet-BB-UTM-pt-BR-v1-4-28-08-2017-L1.pdf - PÁG 08	
2	11	2.5.13.	Permitir a criação de listas personalizadas de URLs permitidas – lista branca e bloqueadas – lista negra;	SIM	Datasheet-BB-UTM-pt-BR-v1-4-28-08-2017-L1.pdf - PÁG 08	
2	11	2.5.14.	Possuir categorização de sites governamentais nacionais, mesmo não tendo domínio “.gov” ou “.gov.br.”	SIM	CONFORME PROPOSTA DE PREÇO	
2	11	2.5.15.	Categorizar as URLs com taxa de acerto mínima de 80% (oitenta por cento), não sendo consideradas neste percentual categorização genérica ou similar.	SIM	DECLARAÇÃO DO FABRICANTE	
2	11	2.5.16.	Suportar e forçar pesquisas seguras em pelo menos dois sistemas de buscas, contemplando Google e/ou Bing e/ou Yahoo.	SIM	user_manual_utm_pt_BR.compressed.pdf - pag. 185	



2	12	2.6.	Conjunto de funcionalidades para controle de aplicações e análise profunda			
2	12	2.6.1.	Possuir módulo de filtro de aplicações e de conteúdo desenvolvido e mantido pelo próprio fabricante, no mesmo equipamento do firewall;	SIM	CONFORME PROPOSTA DE PREÇO	
2	12	2.6.2.	Deve ser capaz de identificar as aplicações mesmo que não estejam utilizando sua porta default.	SIM	DECLARAÇÃO DO FABRICANTE	
2	12	2.6.3.	Deve ser capaz de identificar aplicações encapsuladas dentro de protocolos, como HTTP e HTTPS.	SIM	Datasheet-BB-UTM-pt-BR-v1-4-28-08-2017-L1.pdf - PÁG 08	
2	12	2.6.4.	Deve ser capaz de identificar aplicações que utilizam comunicação criptografada através de SSL.	SIM	Datasheet-BB-UTM-pt-BR-v1-4-28-08-2017-L1.pdf - PÁG 08	
2	12	2.6.5.	Permitir o agrupamento de aplicações em grupos personalizados;	SIM	Datasheet-BB-UTM-pt-BR-v1-4-28-08-2017-L1.pdf - PÁG 08	
2	12	2.6.6.	Garantir que as atualizações regulares do produto sejam realizadas de forma transparente, sem paradas perceptíveis dos serviços;	SIM	CONFORME PROPOSTA DE PREÇO	
2	12	2.6.7.	Identificar aplicações e permitir ou bloquear sua utilização, independentemente das portas e protocolos utilizados para conexão (inclusive tráfego criptografado), assim como possuir categorias para classificação das aplicações, bem como das técnicas de evasões utilizadas;	SIM	DECLARAÇÃO DO FABRICANTE	
2	12	2.6.8.	Possuir, no mínimo, proteção para aplicações do tipo P2P, Instant Messaging, Web e VOIP;	SIM	2.6.8. P2P, Instant Messaging, Web e VOIP.pdf	
2	12	2.6.9.	Possuir perfis/políticas de segurança de aplicações pré-definidas/pré-configuradas na solução;	SIM	Datasheet-BB-UTM-pt-BR-v1-4-28-08-2017-L1.pdf - PÁG 08	
2	12	2.6.10.	Possuir atualização manual e automática de novas assinaturas;	SIM	Datasheet-BB-UTM-pt-BR-v1-4-28-08-2017-L1.pdf - PÁG 08	
2	12	2.6.11.	Permitir a criação de regras de acesso/bloqueio baseadas em usuários ou grupo de usuários do LDAP e do Microsoft Active Directory;	SIM	user_manual_utm_pt_BR.compressed.pdf - pag. 282	
2	12	2.6.12.	Deve ser capaz de identificar e filtrar um mínimo de 1.500 (mil e quinhentas) aplicações, contemplando no mínimo: peer to peer, streaming e download de áudio, streaming e download de vídeo, update de software, instant	SIM	Datasheet-BB-UTM-pt-BR-v1-4-28-08-2017-L1.pdf - PÁG 08 2.6.12. Aplicações Reconhecidas.pdf	

			messaging, redes sociais, proxies, anonymizers, acesso e controle remoto, VOIP e email.			
2	12	2.6.13.	Identificação, bloqueio e restrição em profundidade e granularidade de aplicações, contemplando no mínimo: Bittorrent, Youtube, Livestream, Skype, Viber, WhatsApp, Snapchat, Facebook, Facebook Messenger, Google+, Google Talk, Google Docs, Instagram, Twitter, LinkedIn, Dropbox, Google Drive, One Drive, Logmein, Teamviewer, MSRDP, VNC, Ultrasurf, TOR e Webex.	SIM	2.6.13. Aplicativos reconhecidos.pdf	
2	13	2.7.	<b>Treinamento oficial para até 5 pessoas</b>			
2	13	2.7.1.	Deverá ser fornecido Voucher para treinamento oficial do fabricante.	SIM	CONFORME PROPOSTA DE PREÇO	
2	13	2.7.2.	A carga horária do treinamento não poderá ser inferior a 24 horas, sendo cada voucher apto para até 5 pessoas. O treinamento é composto por turmas que podem ser formadas de um ou mais Vouchers de uma entidade CONTRATANTE, ou ainda, ser uma turma compartilhada por mais de uma entidade CONTRATANTE. Nos dois casos cada turma se limita a no máximo 10 pessoas.	SIM	CONFORME PROPOSTA DE PREÇO	
2	13	2.7.3.	Os treinamentos deverão ser realizados no Brasil, em português, na modalidade presencial, em local fornecido pela CONTRATADA.	SIM	CONFORME PROPOSTA DE PREÇO	
2	13	2.7.3.1.	O local de treinamento deverá possuir todas as facilidades para um perfeito desempenho das atividades, incluindo os recursos áudio visuais e laboratórios necessários, sem ônus algum para a CONTRATANTE.	SIM	CONFORME PROPOSTA DE PREÇO	
2	13	2.7.4.	Caberá à CONTRATADA prover todos os recursos didáticos necessários à realização do treinamento, incluindo (mas não se restringindo a) sala de aula, data show, apostilas, bloco de anotações e caneta para cada treinando.	SIM	CONFORME PROPOSTA DE PREÇO	

1



2	13	2.7.5.	Os treinamentos deverão ocorrer usando-se turnos diários de até 4 horas cada, podendo ser dois turnos no mesmo dia ou um turno por dia a ser acordado com a CONTRATANTE, com intervalos de, no mínimo, 15 minutos em cada turno e de pelo menos 1 hora entre os turnos que ocorrerem no mesmo dia.	SIM	CONFORME PROPOSTA DE PREÇO
2	13	2.7.6.	Toda a documentação didática necessária aos cursos de treinamento deverá ser disponibilizada em papel impresso e mídia digital.	SIM	CONFORME PROPOSTA DE PREÇO
2	13	2.7.7.	Os cursos referentes a equipamentos e softwares que façam parte do objeto deverão usar o material oficial de treinamento do respectivo fabricante por meio de qualquer um dos seus respectivos centros autorizados de treinamento.	SIM	CONFORME PROPOSTA DE PREÇO
2	13	2.7.8.	São produtos esperados de todos os treinamentos:	SIM	CONFORME PROPOSTA DE PREÇO
2	13	2.7.8.1.	Aulas teóricas e práticas.	SIM	CONFORME PROPOSTA DE PREÇO
2	13	2.7.8.2.	Material didático contratado e aprovado pela CONTRATANTE.	SIM	CONFORME PROPOSTA DE PREÇO
2	13	2.7.8.3.	Referências para estudos e pesquisas complementares.	SIM	CONFORME PROPOSTA DE PREÇO
2	13	2.7.9.	A CONTRATANTE poderá, a seu critério, reproduzir o material didático usado e treinar multiplicadores para repetir o treinamento sem custos adicionais. E tal ação não representa a quebra do direito de propriedade do fabricante ou da empresa CONTRATADA. Isso porque o material fornecido não será usado para fins comerciais, mas apenas para uso interno do órgão ou entidade CONTRATANTE com o intuito de disseminar o conhecimento da solução entre os seus servidores profissionais técnicos.		
2	13	2.7.10.	Os custos referentes ao deslocamento, hospedagem e alimentação dos treinados serão de responsabilidade da CONTRATANTE.	SIM	CONFORME PROPOSTA DE PREÇO
2	13	2.7.11.	A ementa do curso deve abranger conteúdos que vão desde configurações básicas até as avançadas dos equipamentos de hardware e de softwares que compõem a solução, bem como sua	SIM	CONFORME PROPOSTA DE PREÇO

			operação.		
2	1	3.	DEFINIÇÃO DOS LOTES E ITENS		
2	1	3.8.	LOTE 2 - item 01: Firewall multifuncional tipo 2		
2	1	3.8.1.	Requisitos específicos:		
2	1	3.8.1.1.	Atender a todos os requisitos do item 2.1;	SIM	CONFORME PROPOSTA DE PREÇO
2	1	3.8.1.2.	Possuir, no mínimo, o throughput de 250 Mbps para todas as funcionalidades dos itens 2.1, 2.2, 2.3, 2.4, 2.5 e 2.6, ativadas simultaneamente e com inspeção integral de todos os pacotes de dados, independentemente de seu tamanho ou direção de fluxo, levando-se em consideração o perfil de tráfego descrito no ANEXO E.	SIM	CONFORME PROPOSTA DE PREÇO
2	1	3.8.1.3.	O equipamento deve possuir no mínimo 01 (uma) fonte de alimentação, que pode ser interna ou externa, com alimentação nominal de 100~ 120VAC e 210~ 230VAC e frequência de 50 ou 60 Hz, ou auto-ranging. Deverá vir acompanhado de cabo de alimentação com, no mínimo, 1,80m (6 pés), com plug tripolar 2P+T no padrão ABNT NBR 14136.	SIM	Datasheet-BB-UTM-pt-BR-v1-4-28-08-2017-L1.pdf - PÁG 07
2	1	3.8.1.4.	Possuir no mínimo 4 (quatro) portas de 10/100/1000 BASE-T.	SIM	Datasheet-BB-UTM-pt-BR-v1-4-28-08-2017-L1.pdf - PÁG 07
2	1	3.8.1.5.	Quantidade de sessões simultâneas 90.000.	SIM	Datasheet-BB-UTM-pt-BR-v1-4-28-08-2017-L1.pdf - PÁG 09
2	1	3.8.1.6.	Quantidade de novas sessões por segundo 12.000.	SIM	Datasheet-BB-UTM-pt-BR-v1-4-28-08-2017-L1.pdf - PÁG 09
2	1	3.8.1.7.	Throughput mínimo de 50 Mbps para IPSec VPN.	SIM	Datasheet-BB-UTM-pt-BR-v1-4-28-08-2017-L1.pdf - PÁG 09
2	9	3.9.	LOTE 2 – item 2: Conjunto de funcionalidades IPS/IDS		
2	9	3.9.1.	Atender a todos os requisitos do item 2.3;		CONFORME PROPOSTA DE PREÇO
2	10	3.10.	LOTE 3 - item 3: Conjunto de funcionalidades antivírus e anti-malware		
2	10	3.10.1.	Atender a todos os requisitos do 2.4;		CONFORME PROPOSTA DE PREÇO
2	11	3.11.	LOTE 2 – item 4: Conjunto de funcionalidades para tratamento de conteúdo web		
2	11	3.11.1.	Atender a todos os requisitos do item 2.5;		CONFORME PROPOSTA DE PREÇO



2	12	3.12.	LOTE 2 – item 5: Conjunto de funcionalidades para controle de aplicações e análise profunda		
2	12	3.12.1.	Atender a todos os requisitos do item 2.1.39 e do item 2.6; 3.13. LOTE 2 - item 6: Treinamento oficial para até 5 pessoas 3.13.1. Atender a tudo o que foi exposto no item 2.7.;		CONFORME PROPOSTA DE PREÇO
2	14	3.14.	LOTE 2 - item 7: Solução de gerência centralizada		
2	14	3.14.1.	Requisitos específicos		
2	14	3.14.1.1.	Atender a todos os requisitos do item 2.2;		CONFORME PROPOSTA DE PREÇO
2	14	3.14.1.2.	Possuir capacidade mínima de 250 GB para armazenamento de logs e eventos		SOLUÇÃO SERÁ ENTREGUE EM APPLIANCE VIRTUAL

Brasília/DF, 03 de outubro de 2017



Blockbit Tecnologia Ltda  
CNPJ Nº 02.423.535/0001-09  
Inscrição Estadual: 115.395.122.119  
Cleber Ribas de Oliveira  
Vice-Presidente  
RG: 0912795-0 SSP/MT  
CPF: 788.962.231-72

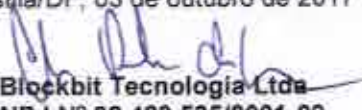
Ao  
MINISTÉRIO DO PLANEJAMENTO, DESENVOLVIMENTO E GESTÃO  
SECRETARIA DE GESTÃO  
DEPARTAMENTO DE AQUISIÇÕES

Referência:	Pregão Eletrônico nº 05/2017
Processo:	04300.0204177/2015-44
Tipo:	PREGÃO ELETRÔNICO
Abertura:	03/10/2017 às 10hs
Proponente:	Blockbit Tecnologia Ltda.
CNPJ:	02.423.535/0001-09

### SÍTIO NA INTERNET DO FABRICANTE

PORTAL	<a href="https://www.blockbit.com/pt-br/unified-threat-management-utm/">https://www.blockbit.com/pt-br/unified-threat-management-utm/</a>
--------	---

Brasília/DF, 03 de outubro de 2017

  
Blockbit Tecnologia Ltda  
CNPJ Nº 02.423.535/0001-09  
Inscrição Estadual: 115.395.122.119  
Cleber Ribas de Oliveira  
Vice-Presidente  
RG: 0912795-0 SSP/MT  
CPF: 788.962.231-72



Ao  
MINISTÉRIO DO PLANEJAMENTO, DESENVOLVIMENTO E GESTÃO  
SECRETARIA DE GESTÃO  
DEPARTAMENTO DE AQUISIÇÕES

Referência:	Pregão Eletrônico nº 05/2017
Processo:	04300.0204177/2015-44
Tipo:	PREGÃO ELETRÔNICO
Abertura:	03/10/2017 às 10hs
Proponente:	Blockbit Tecnologia Ltda.
CNPJ:	02.423.535/0001-09

## DECLARAÇÃO DO FABRICANTE

A **BLOCKBIT TECNOLOGIA LTDA**, inscrita no CNPJ sob o nº 02.423.535/0001-09, sediada R. ENGENHEIRO FRANCISCO PITTA BRITO, 779, JARDIM PROMISSAO, São Paulo/SP – CEP: 04.753-080, por intermédio de seu representante legal infra-assinado, DECLARA que atende integralmente a exigências abaixo descritas, porém não constam em manual, datasheet ou documentação técnica.

- 2.1.35. Suportar no mínimo 250 regras ou políticas de firewall para os equipamentos do lote 1 e 1.000 regras ou políticas de firewall para os equipamentos dos lotes 2,3,4 e 5.
- 2.1.68. Possuir gerenciamento gráfico das funcionalidades de VPN e monitoramento de seus eventos de forma integrada tanto com a gerência local do equipamento ou do cluster quanto com a gerência centralizada da solução.
- 2.1.69. VPN gateway-a-gateway deverá possuir interoperabilidade com os gateways de VPN pelo menos dos seguintes fabricantes: Cisco, Checkpoint, Juniper, Palo Alto Networks, Fortinet, AKER, BluePEX, PFSense e SonicWall.
- 2.4.3. Deve ser capaz de, se houver algum atraso ou falha na realização da atualização automática, o equipamento deve ter a capacidade de alertar imediatamente o administrador através de logs, e-mail ou outros meios de alerta
- 2.5.15. Categorizar as URLs com taxa de acerto mínima de 80% (oitenta por cento), não sendo consideradas neste percentual categorização genérica ou similar.
- 2.6.2. Deve ser capaz de identificar as aplicações mesmo que não estejam utilizando sua porta default.
- 2.6.7. Identificar aplicações e permitir ou bloquear sua utilização, independentemente das portas e protocolos utilizados para conexão (inclusive

tráfego criptografado), assim como possuir categorias para classificação das aplicações, bem como das técnicas de evasões utilizadas;

Declaramos que os equipamentos que compõem nossa proposta de preços possuem as seguintes dimensões físicas.

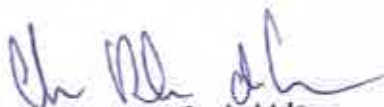
#### LOTE 1

- Quantidade de U's para instalação em rack: 1U
- Necessidade de espaço de guarda: 300mm x 230mm x 46mm
- Mecanismo de refrigeração: Estrutura de Cooler FANLESS
- Consumo de energia: 40W
- Dissipação térmica: 40 BTU/h
- Peso: 1.8 kg

#### LOTE 2

- Quantidade de U's para instalação em rack: 1U
- Necessidade de espaço de guarda: 426mm x 44mm x 318mm
- Mecanismo de refrigeração: 1 x system FAN with smart FAN
- Consumo de energia: 100W
- Dissipação térmica: 136 BTU/h
- Peso: 4.5 kg

Brasília/DF, 03 de outubro de 2017



Blockbit Tecnologia Ltda  
CNPJ Nº 02.423.535/0001-09  
Inscrição Estadual: 115.395.122.119  
Cleber Ribas de Oliveira  
Vice-Presidente  
RG: 0912795-0 SSP/MT  
CPF: 788.962.231-72



Ao  
MINISTÉRIO DO PLANEJAMENTO, DESENVOLVIMENTO E GESTÃO  
SECRETARIA DE GESTÃO  
DEPARTAMENTO DE AQUISIÇÕES

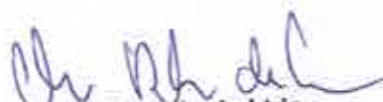
Referência:	Pregão Eletrônico nº 05/2017
Processo:	04300.0204177/2015-44
Tipo:	PREGÃO ELETRÔNICO
Abertura:	03/10/2017 às 10hs
Proponente:	Blockbit Tecnologia Ltda.
CNPJ:	02.423.535/0001-09

### **Escopo do Serviço de Instalação**

- A BLOCKBIT irá prover o fornecimento de ferragens e todos os acessórios necessários para instalação dos equipamentos em rack padrão 19" polegadas, exceto para os lotes 1 e 2, conforme descrito no Anexo B deste TR. Não fazendo parte do presente escopo de fornecimento cabeamento e racks para interconectar a solução à rede local do órgão CONTRATANTE.
- A BLOCKBIT irá prover o fornecimento de todos os serviços necessários ao planejamento e a execução da instalação, incluindo projetos, configuração dos equipamentos, planos de retorno e contingenciamento, de acordo com as necessidades da CONTRATANTE.
- A BLOCKBIT irá executar todas as atividades (físicas e lógicas) de migração dos serviços que se encontrem em operação, incluindo a elaboração do De/Para de portas e a configuração dos equipamentos quando for o caso. A BLOCKBIT irá disponibilizar a topologia de rede existente para que estas atividades sejam efetuadas.
- O plano de retorno e contingenciamento visa garantir a disponibilidade total dos serviços durante e imediatamente após o processo de instalação dos novos equipamentos. Assim, a BLOCKBIT, no caso de algum incidente que comprometa os serviços da CONTRATANTE, irá retomar toda solução conforme estado imediatamente anterior ao processo de instalação. Isso inclui fallback tanto de eventuais configurações alteradas (lógicas), bem como também do respectivo cabeamento (físico).
- Para garantir esse perfeito funcionamento e a transição das mudanças, a BLOCKBIT irá disponibilizar, conforme acionamento da CONTRATANTE, durante o período de aceitação previsto nos itens 8.2.1 e 8.2.10, um técnico qualificado, com as respectivas ferramentas necessárias, para solucionar o problema ou restabelecer a rede original em até 2 (duas) horas. Caso não seja obedecido o prazo anterior, a BLOCKBIT estará sujeita as penalidades previstas na Tabela 3 - Descumprimento dos Níveis Mínimos de Serviço e Penalidades do item 14.1, conforme severidade apontada na Tabela 2 – Classificação de Incidentes do item 11.1.1.
- A BLOCKBIT irá ainda, independente de outras atividades necessárias para garantir a disponibilidade total dos serviços, executar:
  - Todos os backups necessários e relacionados à atividade em questão dos equipamentos da rede em produção;
  - Todos os testes, antes e após as atividades de intervenção e/ou instalação, dos serviços em funcionamento no órgão que tenham relação com os equipamentos em questão.

- A BLOCKBIT irá fornecer à equipe de gestão da implantação do órgão demandante, com antecedência mínima de 5 (cinco) dias úteis anteriores a instalação dos equipamentos, em cada localidade indicada pela CONTRATANTE no ANEXO C, os nomes dos técnicos, juntamente com os respectivos números de documento de identidade, para que sejam identificados durante o procedimento de instalação.
- Os serviços de instalação serão executados e supervisionados por pelo menos 1 (um) técnico certificado da solução proposta.
- Os acessórios, peças e manuais não utilizados durante a instalação, assim como as embalagens dos equipamentos serão removidas pela BLOCKBIT antes da emissão do Termo de Recebimento Definitivo, para que não permaneça no local de instalação nenhum resíduo da embalagem ou qualquer peça solta.
- A BLOCKBIT irá realizar a configuração inicial do equipamento para acesso remoto, assim como prestar o fornecimento de quaisquer outros acessórios e serviços que sejam necessários para a completa operacionalização da rede, de acordo com as necessidades da CONTRATANTE.
- A BLOCKBIT irá realizar a instalação dos firmwares necessários para o funcionamento e a operação completa dos equipamentos, sendo obrigatória a inclusão no equipamento, no momento da instalação, da versão estável mais atual de todos os firmwares.
- Todos os softwares necessários à operação dos equipamentos e soluções serão entregues instalados e operacionais. Também estará incluídos e licenciados (se for o caso) todos os componentes de software básico necessários ao funcionamento dos equipamentos, tais como: sistemas operacionais, controladores de dispositivos e outros pertinentes.

Brasília/DF, 03 de outubro de 2017

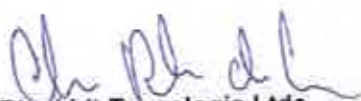


Blockbit Tecnologia Ltda  
CNPJ Nº 02.423.535/0001-09  
Inscrição Estadual: 115.395.122.119  
Cleber Ribas de Oliveira  
Vice-Presidente  
RG: 0912795-0 SSP/MT  
CPF: 788.962.231-72



**FOLHA DE ENCERRAMENTO DA PROPOSTA DE PREÇOS**

Brasília/DF, 03 de outubro de 2017



Blockbit Tecnologia Ltda  
CNPJ Nº 02.423.535/0001-09  
Inscrição Estadual: 115.395.122.119  
Cleber Ribas de Oliveira  
Vice-Presidente  
RG: 0912795-0 SSP/MT  
CPF: 788.962.231-72