



# CÂMARA MUNICIPAL DE ITAPECERICA DA SERRA

## **ITEM 1 - TERMO DE REFERÊNCIA TÉCNICA MÍNIMA DO SERVIDOR PADRÃO RACK (2Us) - 2 PROCESSADORES**

### **1. GABINETE DA CPU**

- 1.1.** Gabinete tipo rack padrão 19", com altura de no máximo 2U original do fabricante do equipamento;
- 1.2.** Novo e sem uso anterior, com trilhos, manuais e quaisquer outros componentes necessários para instalação em rack ofertados como padrão do produto;
- 1.3.** Possuir display embutido no painel frontal do gabinete para exibição de alertas de funcionamento dos componentes internos, tais como falhas de processador, memória RAM, fontes de alimentação, disco rígido e ventilador;
- 1.4.** Possuir projeto tool-less, ou seja, não necessita de ferramentas para abertura do gabinete e instalação/desinstalação de placas de expansão;
- 1.5.** Possuir no mínimo 8 baias para HD's Hot Swap

### **2. SISTEMA DE VENTILAÇÃO**

- 2.1.** Possuir ventilação adequada para a refrigeração do sistema interno do equipamento na sua configuração máxima e dentro dos limites de temperatura adequados para operação;
- 2.2.** Ventiladores redundantes e hot-pluggable, ou seja, podem ser substituída mesmo com o equipamento em funcionamento;

### **3. FONTE DE ALIMENTAÇÃO**

- 3.1.** Fontes de Alimentação redundantes e hot-pluggable com potência de no mínimo 750 Watts cada, suficiente para o funcionamento na sua configuração máxima;
- 3.2.** Faixa de tensão de entrada de 100-240 VAC em 60 Hz com chaveamento automático de voltagem;
- 3.3.** Fornecer cabos de alimentação para cada fonte de alimentação de forma a possibilitar a instalação em circuitos elétricos distintos;

### **4. PROCESSADORES**

- 4.1.** Equipado com 02 (dois) processadores de 6 seis núcleos (Six-Core) ou superior, padrão x86, originalmente concebido para servidores
- 4.2.** Frequência de clock interna de no mínimo 2.40GHz;
- 4.3.** Memória cachê L3 de 12 MB;
- 4.4.** Controladora de memória integrada com suporte à DDR3 de no mínimo 1333MHz;
- 4.5.** Link de comunicação do processador com o restante do sistema de 6.4 GT/s;
- 4.6.** Possuir tecnologia de otimização para virtualização;



# CÂMARA MUNICIPAL DE ITAPEÇERICA DA SERRA

- 4.7. Suportar operações em 64 bits.
- 4.8. O processador deverá consumir no máximo 130 W,
- 4.9. Tecnologia 32nm

## 5. CHIPSET E SLOTS DE EXPANSÃO

- 5.1. O chipset deve ser da mesma marca do fabricante dos processadores e suportar a velocidade de comunicação com os mesmos;
- 5.2. Deverá possuir no mínimo 4 (quatro) slots padrão PCI-Express sendo 2 (dois) slots PCI-e x4 e 2 (dois) slots PCI-e x8

## 6. BIOS

- 6.1. Possuir recursos de controle de permissão através de senhas, uma para inicializar o equipamento e outra para acesso e alterações das configurações do BIOS;
- 6.2. A BIOS deve possuir o número de série/serviço do equipamento e campo editável que permita inserir identificação de ativo podendo ser consultada por software de gerenciamento;

## 7. MEMÓRIA RAM

- 7.1. Módulos de memória tipo DDR3 RDIMM (Registered DIMM) com tecnologia de correção ECC (Error Correcting Code) e velocidade de 1.333 MHz;
- 7.2. Possuir 64 GB (quarenta e oito gigabytes) de memória RAM instalada em pentes de 16GB.
- 7.3. Suportar expansão de memória RAM para até 384 GB (trezentos e oitenta e quatro gigabytes)
- 7.4. Suportar espelhamento de memória (Memory Mirroring);

## 8. PORTAS DE COMUNICAÇÃO

- 8.1. Todos os conectores das portas de entrada/saída de sinal são identificados pelos nomes ou símbolos;
- 8.2. Possuir no mínimo 04 (quatro) portas USB versão 2.0, sendo (no mínimo) 02 (duas) delas situadas na parte frontal do gabinete;
- 8.3. Possuir 02 (duas) portas para monitor de vídeo padrão VGA (DB-15), uma localizada na parte frontal do gabinete e outra na parte traseira do gabinete;
- 8.4. Possuir 01 (uma) porta serial (DB-9) integrada

## 9. INTERFACES DE REDE

- 9.1. Possuir 04 (quatro) interfaces de rede RJ-45 através de controladoras integradas;
- 9.2. As interfaces de rede devem ser padrão Gigabit Ethernet com tecnologia TOE (TCP/IP Offload Engine);
- 9.3. Operar automaticamente nas velocidades de comunicação de 10/100/1000 Mbps, modulo full-duplex;



# CÂMARA MUNICIPAL DE ITAPECERICA DA SERRA

- 9.4.** Capacidade de suportar boot iSCSI;
- 9.5.** Suportar boot através de PXE;
- 9.6.** Suportar a tecnologia de Receive Side Scaling (RSS);
- 9.7.** Suportar Virtual LANs, Jumbo Frames e Link aggregation;

## **10. CONTROLADORA RAID**

- 10.1.** Controladora RAID, compatível com discos rígido padrão SAS e SATA com Interface de 6Gb/s
- 10.2.** Memória cache de no mínimo, 512MB (quinhentos e doze megabytes) padrão DDR2 800MHz;
- 10.3.** Suportar RAID 0, 1, 5, 6, 10, 50 e 60;
- 10.4.** Suportar expansão de capacidade de forma on-line;
- 10.5.** Permita detecção e recuperação automática de falhas e reconstrução, também de forma automática, dos volumes de RAID sem impacto para as aplicações e sem necessidade de reiniciar o equipamento;
- 10.6.** Suporte a recursos de hot swap para as unidades de disco rígido;
- 10.7.** Suportar implementação de disco Global Hot-spare;
- 10.8.** Suportar migração de nível de RAID;
- 10.9.** Suportar Self-Monitoring Analysis and Reporting Technology (SMART);

## **11. ARMAZENAMENTO**

- 11.1.** Armazenamento bruto (raw) local de, no mínimo, 600gb composto por, no mínimo, 02 (duas) unidades de discos rígidos tipo SAS (Serial Attached SCSI) de 10.000 rpm, hot pluggable, de 2,5 ou 3,5 pol e interface de 6Gb/s
- 11.2.** Hot plug e hot swap, que permita sua substituição sem necessidade de desligar o equipamento, garantindo a continuidade das operações sem impacto para as aplicações;
- 11.3.** Não serão aceitos discos em gabinetes externos ao servidor;
- 11.4.** Compatível com a controladora RAID descrita acima

## **12. CONTROLADORA DE VÍDEO**

- 12.1.** Tipo: On board ou placa de vídeo;
- 12.2.** Barramento compatível: PCI ou PCI Express;
- 12.3.** Capacidade da memória cache de vídeo ou da placa de vídeo: mínimo de 08 MB;
- 12.4.** Resolução gráfica de 1280 x 1024 pixels ou superior;
- 12.5.** KVM de 17" do mesmo fabricante;

## **13. UNIDADE DE LEITURA DE DVD-ROM**

- 13.1.** Possuir 01 (uma) unidade de leitura de CD/DVD interna ao gabinete;
- 13.2.** Compatível com leitura de mídias: CD e DVD;



# CÂMARA MUNICIPAL DE ITAPECERICA DA SERRA

## 14. GERENCIAMENTO E INVENTÁRIO

- 14.1. O equipamento ofertado deverá possuir placa de gerenciamento remoto que possibilite o gerenciamento "out-of-band" através de porta RJ-45, não sendo essa nenhuma das interfaces de controladora de rede;
- 14.2. A placa de gerenciamento deve ter total compatibilidade com o mesmo e integração total com software de gerenciamento solicitado.
- 14.3. Utilizar de protocolos para criptografia SSL para acesso a console WEB e SSH para console CLI;
- 14.4. Permitir controle remoto tipo virtual KVM mesmo quando o sistema operacional estiver inoperante;
- 14.5. Suportar autenticação via Active Directory;
- 14.6. Possuir tecnologia de mídia virtual possibilitando que drivers do tipo CD/DVD/Floppy localizados em estação de gerenciamento remota, sejam emulados no servidor gerenciado, permitindo inclusive a inicialização (boot) através dessa mídia;
- 14.7. Capacidade de monitorar o consumo de energia do servidor;
- 14.8. Permitir desligar e reiniciar o servidor através da console de gerenciamento, mesmo em condições de indisponibilidade do sistema operacional;
- 14.9. Realizar inventário de hardware, BIOS e firmware e possibilitar a geração de relatórios customizados;
- 14.10. Suportar update de BIOS e Firmware
- 14.11. Emitir alertas de falha de hardware e permitir a criação de filtros de alertas isolados e notificação por e-mail;

## 15. COMPATIBILIDADE COM SISTEMA OPERACIONAL

- 15.1. O modelo do equipamento ofertado deverá suportar o sistema operacional Windows Server 2008 versões x86, x64 e R2 x64. Esse item deverá ser comprovado através do HCL (Hardware Compatibility List) da Microsoft no link: <http://www.windowsservercatalog.com>
- 15.2. O modelo do equipamento ofertado deverá suportar o sistema operacional Red Hat Enterprise Linux 4.7 ou posterior. Esse item deverá ser comprovado através do HCL (Hardware Compatibility List) da Red Hat no link: <https://hardware.redhat.com/hwcert/index.cgi>
- 15.3. O modelo do equipamento ofertado deverá suportar o sistema de virtualização VMware ESX 4.0 ou posterior. Esse item deverá ser comprovado através do Compatibility Guide da VMware no link: <http://www.vmware.com/resources/compatibility>

## 16. SISTEMA OPERACIONAL

- 16.1. O servidor deverá ser oferecido com sistema operacional Windows server enterprise com hypervision e 10 cal.
- 16.2. Devera ser fornecido junto com o equipamento os treinamentos de Implementação e gerenciamento de uma infraestrutura de rede Windows server e o de implementação e gerenciamento de active directory



# CÂMARA MUNICIPAL DE ITAPECERICA DA SERRA

## **17. DRIVERS**

**17.1.** Acompanhar mídia de inicialização e configuração do equipamento contendo todos os drivers de dispositivos de forma a permitir a fácil instalação do equipamento.

**17.2.** O fabricante do equipamento deve disponibilizar no seu respectivo web site, download gratuito de todos os Drivers de dispositivos, BIOS e Firmwares permitindo todas as atualizações de melhoria necessárias

## **18. ACESSÓRIOS**

**18.1.** Devem ser fornecidos junto com o servidor, todos os acessórios e cabos necessários para o pleno funcionamento do mesmo;

**18.2.** Kit de trilhos e braço organizador de cabos para fixação dos equipamentos em rack padrão 19 polegadas, permitindo o deslizamento do equipamento a fim de facilitar a manutenção;

## **19. CERTIFICADOS**

**19.1.** Deve ser entregue certificação comprovando que o equipamento está em conformidade com a norma IEC 60950, para segurança do usuário contra incidentes elétricos e combustão dos materiais elétricos;

## **20. SERVIÇOS DE INSTALAÇÃO**

**20.1.** Serviço de instalação física em local indicado pela contratante, incluindo a devida energização para teste dos equipamentos

## **21. GARANTIA E SUPORTE**

**21.1.** Os equipamentos devem possuir garantia por um período mínimo de 36 (trinta e seis ) meses com um período de disponibilidade para chamada de manutenção de 24 horas por dia, 7 dias por semana;

**21.2.** A contratada deve possuir Central de Atendimento tipo (0800) para abertura dos chamados de garantia, comprometendo-se a manter registros dos mesmos constando a descrição do problema;

**21.3.** Durante o prazo de garantia será substituída sem ônus para o contratante, a parte ou peça defeituosa, salva quando o defeito for provocado por uso inadequado dos equipamentos;

**21.4.** Os serviços de reparo dos equipamentos especificados serão executados onde se encontram (ON-SITE) ou na impossibilidade, no centro de manutenção da contratada;

**21.5.** O prazo máximo para atendimento e reparo/solução do(s) problema(s) que ocasionou(aram) o chamado dos equipamentos, contado a partir da abertura do chamado e dentro do período de disponibilidade para atendimento, de NBD;



# CÂMARA MUNICIPAL DE ITAPECERICA DA SERRA

## ITEM 2 - TERMO DE REFERÊNCIA TÉCNICA MÍNIMA DO FIREWALL

<b>1</b>	Funcionalidades de Firewall
1.1	O equipamento oferecido deve ser do tipo UTM, na forma de appliance, com suporte a: <ul style="list-style-type: none"><li>- Proteção imediata contra ameaças (default threat protection / zero day threat protection)</li><li>- Filtro de Conteúdo</li><li>- IPS</li><li>- Anti-spam</li><li>- Anti-virus</li><li>- Autoridade de Reputação (Reputation Authority)</li><li>- Controle de Aplicações</li></ul>
1.2	O equipamento deve oferecer suporte a no mínimo três zonas de segurança: zona externa, privada e opcional (DMZ).
1.3	O equipamento deve oferecer suporte à configuração de endereços IP estáticos e dinâmicos (por DHCP e PPPoE) em interfaces externas.
1.4	Vazão de firewall (firewall throughput): o equipamento deve suportar 1.4 Gbps de vazão de firewall.
1.5	Vazão de UTM (XTM throughput): o equipamento deve suportar 400 Mbps de vazão de UTM.
1.6	Sessões concorrentes: o equipamento deve suportar 50.000 sessões concorrentes bidirecionais.
1.7	O equipamento deve oferecer suporte a regras de firewall com autenticação de usuários (sem limites ao número de usuários) a partir de base de dados interna e servidores de autenticação RADIUS, SecureID, LDAP e Active Directory.
1.8	O equipamento deve oferecer suporte a serviço de DNS dinâmico (Dynamic DNS) no caso de interfaces externas serem configuradas com endereços IP dinâmicos.
1.9	O equipamento deve apresentar ausência de discos rígidos a fim de minimizar a possibilidade de falhas.
1.10	O sistema deve oferecer suporte à implementação de regras de firewall de tipo proxy (em camada 7 ou camada de aplicação) para, no mínimo, protocolos HTTP, HTTPS, POP3, SMTP, FTP, DNS, VoIP (H.323 e SIP) e TCP-UDP.
1.11	As regras de firewall de tipo proxy para protocolo HTTP devem permitir controlar, no mínimo, os seguintes aspectos do protocolo: <ul style="list-style-type: none"><li>- HTTP Request: General Settings (Configurações Gerais)</li><li>- HTTP Request: Request Methods (Métodos HTTP)</li><li>- HTTP Request: URL Paths (URLs)</li></ul>



## CÂMARA MUNICIPAL DE ITAPECERICA DA SERRA

	<ul style="list-style-type: none"><li>- HTTP Request: Header Fields (Campos de Header)</li><li>- HTTP Request: Authorization (Autorização)</li><li>- HTTP Response: General Settings (Configurações Gerais)</li><li>- HTTP Response: Header Fields (Campos de Header)</li><li>- HTTP Response: Content Types (Tipos MIME)</li><li>- HTTP Response: Cookies (Cookies)</li><li>- HTTP Response: Body Content Types (Tipos de Arquivos)</li><li>- Use a Caching Proxy Server (Uso de Servidor de Cache)</li><li>- Exceptions (Exceções)</li><li>- Safe Search Enforcement (Suporte a Busca Segura)</li><li>- WebBlocker (Filtro de Conteúdo)</li><li>- AntiVirus (Anti-virus)</li><li>- Reputation Enabled Defense (Defesa por Autoridade de Reputação)</li><li>- Deny Message (Mensagem de Bloqueio)</li><li>- Proxy and AV Alarms (Geração de Alarmes)</li></ul>
1.12	<p>As regras de firewall de tipo proxy para protocolo HTTPS devem permitir controlar, no mínimo, os seguintes aspectos do protocolo:</p> <ul style="list-style-type: none"><li>- General Settings (Configurações Gerais)</li><li>- Content Inspection (Inspeção de Conteúdo)</li><li>- Bypass List (Lista de Bypass)</li><li>- WebBlocker (Filtro de Conteúdo)</li><li>- Certificate Names (Certificados Digitais)</li><li>- Proxy and AV Alarms (Geração de Alarmes)</li></ul>
1.13	<p>As regras de firewall de tipo proxy para protocolo POP3 devem permitir controlar, no mínimo, os seguintes aspectos do protocolo:</p> <ul style="list-style-type: none"><li>- General Settings (Configurações Gerais)</li><li>- Authentication (Autenticação)</li><li>- Content Types (Tipos MIME)</li><li>- File Names (Nomes de Arquivos)</li><li>- Headers (Headers)</li><li>- Deny Message (Mensagem de Bloqueio)</li><li>- AntiVirus (Anti-virus)</li><li>- spamBlocker (Anti-spam)</li><li>- Proxy and AV Alarms (Geração de Alarmes)</li></ul>
1.14	<p>As regras de firewall de tipo proxy para protocolo SMTP devem permitir controlar, no mínimo, os seguintes aspectos do protocolo:</p> <ul style="list-style-type: none"><li>- General Settings (Configurações Gerais)</li></ul>



## CÂMARA MUNICIPAL DE ITAPECERICA DA SERRA

	<ul style="list-style-type: none"><li>- Greeting Rules (Regras do Protocolo)</li><li>- ESMTTP Settings (Configurações de ESMTTP)</li><li>- TLS Encryption (Criptografia via TLS)</li><li>- Authentication (Autenticação)</li><li>- Content Types (Tipos MIME)</li><li>- File Names (Nomes de Arquivos)</li><li>- Mail From / Rcpt To (Origem / Destino)</li><li>- Headers (Headers)</li><li>- AntiVirus (Anti-virus)</li><li>- Deny Message (Mensagem de Bloqueio)</li><li>- spamBlocker (Anti-spam)</li><li>- Proxy and AV Alarms (Geração de Alarmes)</li></ul>
1.15	<p>As regras de firewall de tipo proxy para protocolo FTP devem permitir controlar, no mínimo, os seguintes aspectos do protocolo:</p> <ul style="list-style-type: none"><li>- General Settings (Configurações Gerais)</li><li>- Commands (Comandos)</li><li>- Content – Upload (Upload de Arquivos)</li><li>- Content - Download (Download de Arquivos)</li><li>- AntiVirus (Anti-virus)</li><li>- Proxy and AV Alarms (Geração de Alarmes)</li></ul>
1.16	<p>As regras de firewall de tipo proxy para protocolo DNS devem permitir controlar, no mínimo, os seguintes aspectos do protocolo:</p> <ul style="list-style-type: none"><li>- General Settings (Configurações Gerais)</li><li>- OPcodes (Códigos de Operação)</li><li>- Query Types (Tipos de Consulta DNS)</li><li>- Query Names (Nomes de Consulta DNS)</li></ul>



## CÂMARA MUNICIPAL DE ITAPECERICA DA SERRA

	- Proxy and AV Alarms (Alarmes)
1.17	As regras de firewall de tipo proxy / application layer gateway para protocolo H.323 devem permitir controlar, no mínimo, os seguintes aspectos do protocolo: <ul style="list-style-type: none"><li>- General Settings (Configurações Gerais)</li><li>- Access Control (Controle de Acesso)</li><li>- Denied Codecs (Codecs Bloqueados)</li></ul>
1.18	As regras de firewall de tipo proxy / application layer gateway para protocolo SIP devem permitir controlar, no mínimo, os seguintes aspectos do protocolo: <ul style="list-style-type: none"><li>- General Settings (Configurações Gerais)</li><li>- Access Control (Controle de Acesso)</li><li>- Denied Codecs (Codecs Bloqueados)</li></ul>
<b>2</b>	<b>Suporte a VPNs (Virtual Private Networks)</b>
2.1	Vazão de VPN (VPN throughput): o equipamento deve suportar 350 Mbps de vazão de VPN.
2.2	A solução deve oferecer suporte a VPNs Móveis (Usuário – Equipamento) sobre protocolos IPSec, SSL e PPTP.
2.3	Deve incluir licenciamento para 100 usuários móveis usando protocolo IPSec.
2.4	Deve incluir licenciamento para 1/75 usuários móveis usando protocolo SSL.
2.5	Deve suportar no mínimo 75 VPNs Fixas (Equipamento – Equipamento ou entre localidades) usando protocolo IPSec.
2.6	O equipamento deverá poder suportar a configuração de VPNs Fixas com qualquer outro produto que ofereça suporte ao padrão IPSec.
2.7	Os seguintes mecanismos de autenticação devem ser suportados pela solução: DES, 3DES, AES 128-, 192-, 256-bit
2.8	Os seguintes mecanismos de cifra devem ser suportados pela solução: SHA-1, MD5, IKE Pre-Shared Key, certificados digitais.
2.9	Deve oferecer suporte a Dead Peer Detection (DPD).



## CÂMARA MUNICIPAL DE ITAPECERICA DA SERRA

2.10	Deve oferecer suporte a VPN Failover.
2.11	Deve oferecer suporte a tráfego de broadcast e multicast sobre VPNs.
<b>3</b>	<b>Filtro de Conteúdo</b>
3.1	O equipamento deverá poder suportar funcionalidades de Filtro de Conteúdo via subscrição adicional, renovável anualmente, sem a necessidade de equipamento dedicado.
3.2	As funcionalidades de Filtro de Conteúdo devem incluir a opção de filtro por categorias, devendo contar com um mínimo de 54 categorias.
3.3	As funcionalidades de Filtro de Conteúdo deverão poder ser configuradas granularmente por usuário, grupo de usuários, endereço IP, grupo de endereços IP, sub-redes e horários específicos, devendo contar com um mínimo de 54 categorias.
3.4	A solução deve permitir estabelecer exceções quanto ao Filtro de Conteúdo, tanto no sentido de permissão (allow) quanto de bloqueio (deny).
3.5	A solução deve permitir filtrar conteúdo em múltiplos idiomas.
3.6	A funcionalidade de Filtro de Conteúdo deverá possibilitar a consulta a uma base de dados local (sobre interfaces privadas ou opcionais - DMZ), além da possibilidade de consultar uma base de dados externa.
3.7	A solução de Filtro de Conteúdo deverá suportar, no mínimo, os protocolos HTTP e HTTPS.
3.8	A solução de Filtro de Conteúdo deverá suportar recursos on-line que possibilitem solicitar a inclusão, exclusão ou mudança de classificação de novos sites ou sites existentes.
<b>4</b>	<b>Anti-virus</b>
4.1	O equipamento deverá poder suportar funcionalidades de serviço de Anti-virus via subscrição adicional, renovável anualmente, sem a necessidade de equipamento dedicado.
4.2	A solução deve permitir suportar a descompressão de arquivos comprimidos pelos algoritmos mais comuns (formatos .rar, .tar, .tgz, .gz, .zip, .gzip, .jar, .chm, .lha, .pdf, container XML/HTML, container OLE - documentos do Microsoft Office, .cab, .arj, .ace, .bz2 - Bzip e .swf) em até 6 níveis.
4.3	A atualização das assinaturas da solução de Anti-virus deverá ser programável e automática, havendo adicionalmente a possibilidade de atualização de forma manual, a critério do administrador.
4.4	A solução de Anti-virus deverá suportar serviços de quarentena, remoção de arquivos infectados, bloqueio de conexão (drop) e bloqueio de endereços (block).
4.5	A máquina (engine) de verificação de código hostil utilizada pela solução de Anti-virus deverá se fornecida por uma empresa reconhecida por sua especialização no assunto.



## CÂMARA MUNICIPAL DE ITAPECERICA DA SERRA

4.6	A solução de Anti-virus deverá suportar a detecção e bloqueio de código hostil em geral, incluindo vírus, cavalos de troia (trojans), vermes (worms), spyware e rogueware.
4.7	A solução de Anti-virus deverá suportar os protocolos HTTP, HTTPS, FTP, SMTP, TCP-UDP e POP3.
<b>5</b>	<b>Anti-spam</b>
5.1	O equipamento deverá poder suportar funcionalidades de Anti-spam via subscrição adicional, renovável anualmente, sem a necessidade de equipamento dedicado.
5.2	A solução de Anti-spam deverá poder suportar mecanismos de detecção de padrões recorrentes (RPD – Recurrent Pattern Detection) de modo a minimizar a necessidade de processamento no próprio equipamento.
5.3	A solução de Anti-spam deverá poder suportar serviços de quarentena de mensagens, bem como de modificação do campo de assunto (subject) da mensagem, bloqueio de conexão (drop) e recusa de mensagens de correio (deny).
5.4	A solução de Anti-spam deverá integrar a detecção de epidemia de vírus na análise de spam (VOD – Vírus Outbreak Detection).
5.5	A solução deve permitir bloquear spam em múltiplos idiomas.
5.6	A solução deve permitir bloquear tanto spam baseado em imagens quanto spam baseado em texto.
5.7	A solução de Anti-spam deverá suportar os protocolos SMTP e POP3.
5.8	A solução de Anti-spam deverá suportar a utilização de um serviço baseado no uso de recursos de “computação em nuvem” (cloud-based) de categorização de mensagens de correio eletrônico.
<b>6</b>	<b>IPS (Intrusion Prevention System)</b>
6.1	O equipamento deverá poder suportar funcionalidades de serviços de IPS via subscrição adicional, renovável anualmente, sem a necessidade de equipamento dedicado.
6.2	A atualização das assinaturas de ataques utilizadas pela solução de IPS deverá ser programável e automática, havendo adicionalmente a possibilidade de atualização de forma manual, a critério do administrador.
6.3	A solução de IPS deverá permitir a classificação das ameaças por nível de risco / severidade dos ataques, com a possibilidade de geração de alarmes e registros de log.
6.4	A solução de IPS deverá suportar ações de bloqueio de conexão (drop) e de bloqueio de endereços fonte de ataques (block), bem como a geração de alarmes.
6.5	A solução de IPS deverá suportar a detecção de ameaças em todos os protocolos e portas, independente do tipo de regra de firewall utilizada.



## CÂMARA MUNICIPAL DE ITAPECERICA DA SERRA

6.6	A solução de IPS deverá suportar a configuração de exceções quanto à análise de tráfego de rede por assinaturas de ataques.
6.7	A solução de IPS deverá oferecer um portal, acessível via Internet, na forma de uma base de dados onde possam ser obtidas informações adicionais sobre as assinaturas de ataques utilizadas na detecção de ameaças.
6.8	A solução de IPS deverá suportar por default (default threat protection), proteção imediata contra ataques e ameaças do tipo ataques de inundação (SYN flood attacks, IPSec flood attacks, IKE flood attacks, ICMP flood attacks, UDP flood attacks), ataques de falsificação (spoofing attacks), ataques de varredura de portas e endereços (port / address space probes) e ataques de negação de serviços (DoS) / negação de serviços distribuída (DDoS).
6.9	Devem ser configuráveis, pelo administrador da solução, os limites para a detecção de ataques de inundação (flood) e de ataques de negação de serviços (DoS / DDoS).
<b>7</b>	<b>NAT (Network Address Translation)</b>
7.1	O equipamento deverá suportar serviços de NAT nas seguintes modalidades:
7.1.1	NAT estático.
7.1.2	NAT dinâmico.
7.1.3	NAT 1-to-1.
7.1.4	IPSec NAT Traversal.
7.1.5	NAT sobre VPN (1-to-1 NAT Through VPN).
7.1.6	NAT baseado em políticas (Policy-Based Dynamic NAT).
7.2	O equipamento deverá suportar serviços de PAT (Port Address Translation).
7.3	O equipamento deverá oferecer suporte à divisão de cargas entre servidores (server load-balance).
<b>8</b>	<b>Características de Networking</b>
8.1	O equipamento deverá suportar um número mínimo de 06 interfaces 10/100/1000 no padrão RJ45 (cobre), as quais devem poder ser configuradas em qualquer das zonas de segurança disponíveis, a saber, zona externa, privada ou opcional (DMZ), bem como interfaces de gerência.
8.2	O equipamento deverá suportar no mínimo 1 interface de gerência no padrão serial RS232 RJ45 e 1 interface USB.
8.3	O equipamento deverá oferecer serviços de multi-wan (suporte a múltiplos links / enlaces externos), com suporte a no mínimo quatro interfaces destinadas à zona externa de segurança, com possibilidade de



## CÂMARA MUNICIPAL DE ITAPECERICA DA SERRA

	funcionamento em modo fail-over ou em modo de divisão de carga (load-balancing), neste caso com possibilidade de definição pelo administrador do algoritmo a ser utilizado (round-robin, weighted round-robin, routing table ou interface overflow).
8.4	O equipamento deverá suportar no mínimo 75 VLANs
8.5	O equipamento deverá suportar serviços de gerência de tráfego (traffic management) e de QoS (Quality of Services – qualidade de serviços).
8.6	O equipamento deverá poder ser implementado em modo de roteador (modo routed), em modo semi-transparente (modo drop-in, com endereço IP único para todas as interfaces de rede) e em modo transparente (modo bridge ou switch).
8.7	O equipamento deverá suportar rotas estáticas, rotas dinâmicas (protocolos RIP v1 e v2, OSPF e BGP) e rotas baseadas em políticas (PBR - possibilidade de escolha pelo administrador de qual interface externa utilizar para enviar o tráfego), tanto em modo standalone quanto em cluster.
8.8	O equipamento deverá poder ser implementado em forma de cluster, tanto na modalidade ativo / passivo (suporte a alta disponibilidade) quanto na modalidade ativo / ativo (suporte a divisão de carga).
8.9	O equipamento deve oferecer suporte a IPv6 em conformidade com o IPv6 Forum (Product Classification = Router; IPv6 Ready Phase 2 - Gold Logo).
<b>9</b>	<b>Características de Gerência</b>
9.1	A administração do equipamento, bem como de todos os elementos distintos da solução, deverá poder realizar-se integralmente através de interface gráfica de administração, tanto em modo on-line / em tempo real quanto em modo off-line.
9.2	A solução deverá permitir monitorar e desconectar usuários internos ou externos do equipamento, em tempo real e por espaço de tempo definido pelo administrador, sem necessidade de criação de regras ou políticas de segurança adicionais.
9.3	A solução deverá permitir a geração e envio de alarmes / notificações por protocolo SNMP v2 ou v3, janela de pop-up ou mensagem de email.
9.4	Deverá permitir suportar a gerência centralizada de múltiplos equipamentos simultaneamente, com suporte adicional a múltiplos operadores com níveis distintos de acesso aos equipamentos.
9.5	Deverá permitir a criação facilitada de VPNs entre equipamentos pelo uso de procedimentos de "drag-and-drop VPN / Add VPN Wizard".
9.6	A solução deverá suportar o protocolo DVCP de gerência.
9.7	A solução deverá permitir a criação, exclusão e modificação de políticas e regras de segurança de forma gráfica em modo off-line.
9.8	A solução deverá suportar múltiplos operadores com níveis distintos de acesso aos equipamentos (management Server), cujas contas possam ser autenticadas contra um servidor Windows Active Directory



## CÂMARA MUNICIPAL DE ITAPECERICA DA SERRA

9.9	A solução deverá suportar administração via interface CLI (Command Line Interface), por interface serial ou por interface de rede, sobre protocolo SSH2.
9.10	A solução deverá suportar administração via interface web (browser), por interface de rede, sobre protocolo seguro HTTPS.
9.11	A solução deverá suportar administração via interface gráfica (WSM - sistema específico de gestão), por interface de rede, sobre protocolo HTTPS.
9.12	A solução deverá suportar recursos visualização de conexões simultâneas a partir de elementos de rede em quaisquer de suas interfaces de rede (hostwatch).
9.13	A solução deverá oferecer uma console que permita acompanhar em modo gráfico o desempenho do equipamento (performance console) em termos de informações do sistema (uso de CPU e memória), informações sobre as interfaces de rede e informações sobre as políticas e regras de segurança.
9.14	A solução deverá oferecer a possibilidade de visualização on-line de (i) usuários autenticados (authentication list) e de (ii) endereços IP bloqueados (blocked sites).
<b>10</b>	<b>Registros (Logs) e Relatórios</b>
10.1	O sistema sendo oferecido deve permitir a implementação de servidores de registros (logs) de maneira a centralizar o armazenamento dos registros gerados pelo equipamento.
10.2	O serviço de armazenamento de registros deve estar baseado em protocolo TCP/IP e utilizar uma base de dados SQL, a qual deverá estar incluída como parte integral da proposta, permitindo-se opcionalmente a utilização de uma base de dados compatível pré-existente.
10.3	O tamanho máximo da base de dados deve ser configurável pelo administrador, bem como se deve poder configurar alertas a serem gerados quando se aproximar a base de dados do tamanho máximo definido.
10.4	A solução deverá suportar a configuração de múltiplos servidores de logs.
10.5	Os equipamentos devem poder ser configurados com um mínimo de dois servidores de logs, sendo um principal e outro a ser usado em caso de falhas do principal.
10.6	A transmissão dos logs deve ser feita de maneira cifrada (encriptada), sem que para tal se requeira a configuração de VPNs.
10.7	A solução deverá oferecer suporte à utilização opcional de serviços de logs de sistema (syslog) para armazenamento de logs.
10.8	A solução deverá suportar a geração de relatórios a partir de múltiplos servidores de logs.
10.9	O serviço de geração de relatórios deverá permitir gerar relatórios em formato PDF, CSV e HTML.



## CÂMARA MUNICIPAL DE ITAPECERICA DA SERRA

10.10	O serviço de geração de relatórios deverá permitir automatizar a geração de relatórios.
10.11	A solução deverá oferecer acesso por um portal web para a visualização de relatórios.
10.12	Os serviços de registros (logs) e de geração de relatórios devem poder ser instalados em equipamentos com sistema operacional Windows (Windows XP, 2003, Vista, 2008 ou 7).
<b>11</b>	<b>Certificações de Segurança</b>
11.1	O equipamento deverá cumprir, ou estar em processo de cumprir, com as certificações de segurança eletrônica (ICSA Firewall, ICSA IPsec VPN, FIPS 140-2, Common Criteria EAL4+ e VPNC).
<b>12</b>	<b>Outras Características Técnicas</b>
12.1	O equipamento deverá apresentar dimensões padrão para instalação em armários de tipo "rack", com altura máxima de 2 unidades (2U), bem incluir todos os acessórios necessários à sua montagem.
12.2	O equipamento deverá apresentar fontes de energia as quais possam operar sobre uma voltagem de 100 a 240 VAC (autosensing).
12.3	O equipamento deverá poder operar em temperaturas 0 e 40 graus centígrados com percentual de umidade relativa entre 10% e 85%.
<b>13</b>	<b>Autoridade de Reputação (Reputation Authority)</b>
13.1	A solução deverá suportar a utilização de um serviço baseado no uso de recursos de "computação em nuvem" (cloud-based) de categorização de sites, categorização esta baseada na reputação designada ao site por uma Autoridade de Reputação (Reputation Authority, serviço este destinado ao controle de navegação web de usuários, com melhoria de desempenho do equipamento).
13.2	O equipamento deverá poder suportar esta funcionalidade de serviços de Autoridade de Reputação via subscrição adicional, renovável anualmente, sem a necessidade de equipamento dedicado.
13.3	Com base na utilização deste serviço de Autoridade de Reputação, a solução deverá ser capaz de desativar, de maneira dinâmica, o uso do serviço de Anti-virus para a navegação HTTP a sites web de boa reputação, com o intuito de melhorar a performance do equipamento.
13.4	De maneira análoga, também com base na utilização deste mesmo serviço de Autoridade de Reputação, a solução deverá ser capaz de poder bloquear a navegação HTTP a sites web de má reputação (por exemplo, com



## CÂMARA MUNICIPAL DE ITAPECERICA DA SERRA

	histórico de disseminação de spam e vírus), com o intuito de melhor controlar a navegação web dos usuários.
13.5	O serviço de Autoridade de Reputação deverá oferecer um portal, acessível via Internet, a partir do qual possam ser obtidas informações adicionais acerca da reputação atribuída aos sites.
<b>14</b>	<b>Controle de Aplicações (Application Control)</b>
14.1	A solução deverá suportar a utilização de um serviço de controle granular de aplicações (em nível de comando / comportamento / função da aplicação - exemplo: transferência de arquivos) tais como IM, Redes Sociais e P2P, dentre outras, serviço este baseado em assinaturas e independente de portas utilizadas pelas aplicações. <a href="http://www.watchguard.com/SecurityPortal/AppDB.aspx">http://www.watchguard.com/SecurityPortal/AppDB.aspx</a> .
14.2	O equipamento deverá poder suportar esta funcionalidade de serviços de Controle de Aplicações via subscrição adicional, renovável anualmente, sem a necessidade de equipamento dedicado.
14.3	A atualização das assinaturas de aplicações utilizadas pela solução de Controle de Aplicações deverá ser programável e automática, havendo adicionalmente a possibilidade de atualização de forma manual, a critério do administrador.
14.4	A solução de Controle de Aplicações deverá oferecer um portal, acessível via Internet, na forma de uma base de dados onde possam ser obtidas informações adicionais sobre as aplicações passíveis de serem controladas.



## CÂMARA MUNICIPAL DE ITAPECERICA DA SERRA

### ITEM 3 - TERMO DE REFERÊNCIA TÉCNICA MÍNIMA DO NOBREAK 3000 VA

<b>CARACTERÍSTICAS DO PRODUTO</b>	<b>Nobreak</b> microprocessado com sistema de regulação on line. Chave liga/desliga embutida ou temporizada, evitando desligamentos acidentais Filtro de linha integrado, com proteção contra surtos de tensão Forma de onda senoidal Sistema de recarga automática das baterias, mesmo com o nobreak desligado O equipamento deve permitir ser ligado na ausência de rede elétrica Painel frontal dotado de leds indicativos de tensão e alarme audiovisual intermitente em caso de queda de rede Porta fusível externo, com unidade sobressalente Gerenciamento do equipamento, através de conectividade RS-232
<b>POTÊNCIA NOMINAL</b>	3000 VA (mínima)
<b>TENSÃO NOMINAL DE ENTRADA (Faixas de regulação com tolerância de <math>\pm 6\%</math>)</b>	Entrada 115/127. Faixa de regulação de entrada mínima em rede 115/127V – 95 a 135V.
<b>FREQUÊNCIA NOMINAL</b>	60 Hz (valor máximo) $\pm 3\%$ para operação em bateria
<b>TENSÃO NOMINA DE SAÍDA</b>	115 V Faixa de regulação de saída $\pm 3\%$ para operação em bateria Faixa de regulação de saída $+3\% \sim -10\%$ para operação em rede Fator de potência de saída 9 (no mínimo)



## CÂMARA MUNICIPAL DE ITAPECERICA DA SERRA

<b>TOMADAS</b>	06 tomadas de saída disponíveis (no mínimo) Tomadas de entrada e saída no padrão NBR14136
<b>BATERIA INTERNA</b>	02 (duas) baterias 12 V, com no mínimo 17Ah (ligadas em paralelo)
<b>GABINETE</b>	TIPO RACK
<b>GARANTIA</b>	24 meses a contar da data da entrega dos equipamentos, com garantia de troca imediata (prazo de 48 horas) dos equipamentos defeituosos nos primeiros 90 (noventa) dias. A garantia deverá ser prestada diretamente pelo vencedor, ficando às suas expensas a retirada dos equipamentos danificados, o envio e custas da manutenção, no período da garantia.
<b>OUTRAS INFORMAÇÕES</b>	A proponente deverá apresentar junto à proposta técnica o Catálogo Oficial do Produto, em português, que apresente todas as especificações técnicas detalhadas, em conformidade com o descrito no edital (as informações constantes do catálogo devem estar disponíveis no site do fabricante), sendo que cada item exigido deverá estar destacado neste catálogo, a fim de facilitar a identificação. A proponente deverá declarar que é revenda autorizada a comercializar os equipamentos e que vai honrar os termos da garantia e assistência técnica dos mesmos, nos termos e prazos acima descritos. O equipamento deverá acompanhar manual e demais documentação em português e todos os cabos necessários à instalação plena do equipamento.



# CÂMARA MUNICIPAL DE ITAPECERICA DA SERRA

## ITEM 4 - TERMO DE REFERÊNCIA TÉCNICA MÍNIMA DO NOBREAK 1200 VA

### **Características do Produto:**

No-break microprocessado com sistema de regulação on line, com função True-RMS;  
Chave liga/desliga embutida ou temporizada, evitando desligamentos acidentais;  
Filtro de linha integrado, com proteção contra surtos de tensão;  
Forma de onda semi-senoidal;  
Sistema de recarga automática das baterias, mesmo com o no-break desligado;  
O equipamento deve permitir ser ligado na ausência de rede elétrica;  
Painel frontal dotado de leds indicativos de tensão e alarme audiovisual intermitente em caso de queda de rede;  
Porta fusível externo, com unidade sobressalente;  
Gerenciamento do equipamento, através de conectividade USB.

### **Saída mínima:**

Capacidade de Potência de Saída: 600 Watts / 1200 VA  
Tensão nominal de saída: 115V  
Frequência de Saída (sincronizada com rede elétrica): 60 Hz  
Tipo de Forma de Onda: Senoidal aproximada  
Conexões de Saída: NBR 14136

### **Entrada mínima:**

Tensão nominal de entrada: 115V / 220V  
Frequência de entrada: 60 Hz  
Tipo de Conexão de Entrada: NBR 14136  
Comprimento do Cabo: 1.22 metros

### **Baterias & Tempo de operação mínimo:**

Tipo de bateria: Bateria selada Chumbo - Acido livre de manutenção: a prova de vazamentos  
Tempo de recarga típico: 12 horas(s)  
Quantidade de RBC™: 2

### **Comunicação & Gerenciamento:**

Painel de controle: Display de LED status com indicadores para On line: Troca de bateria: e Falha no cabeamento  
Alarme sonoro: Soar alarme quando na bateria: Alarme distinto de pouca bateria: tom de alarme continuamente sobre carregado

### **Físico:**

Dimensões máximas de altura: 217.00 mm  
Dimensões máximas de largura: 134.00 mm



## CÂMARA MUNICIPAL DE ITAPECERICA DA SERRA

Dimensões máximas de profundidade: 379.00 mm

Peso Líquido: 11.85 KG

Peso para Transporte: 12.46 KG

Altura para Transporte: 245.00 mm

Largura para Transporte: 151.00 mm

Largura (com embalagem): 423.00 mm

Unidades na Embalagem de Transporte: 1.00

Cor: Preto

### **Ambiental:**

Ambiente de Operação: 0 - 40 °C

Umidade Relativa de Operação: 0 - 90%

Elevação de Operação: 0-3000 metros

Temperatura de Armazenamento: -15 - 45 °C

Umidade Relativa de Armazenamento: 0 - 90%

Elevação de Armazenamento: 0-9000 metros

### **Conformidade mínima:**

Garantia Padrão: 2 anos para reparo ou substituição (não inclui baterias) e 1 ano para baterias

### **Outras Informações:**

A proponente deverá apresentar junto à proposta técnica o Catálogo Oficial do Produto, em português, que apresente todas as especificações técnicas detalhadas, em conformidade com o descrito no edital (as informações constantes do catálogo devem estar disponíveis no site do fabricante), sendo que cada item exigido deverá estar destacado neste catálogo, a fim de facilitar a identificação.

A proponente deverá declarar que é revenda autorizada a comercializar os equipamentos e que vai honrar os termos da garantia e assistência técnica dos mesmos, nos termos e prazos acima descritos.

O equipamento deverá acompanhar manual e demais documentação em português e todos os cabos necessários à instalação plena do equipamento.