Termo de Referencia

AMBIENTE DE INFORMÁTICA - DATACENTER

Objeto: Contratação de Empresa para fornecimento de solução de infraestrutura, composta por: Processamento de dados com virtualização, armazenamento de dados, Rede Lan e wireless com gerenciamento centralizado, sistema de segurança e demais componentes que compõem a solução - DATACENTER.

A solução deverá ser fornecida por uma único licitante afim de garantir a perfeita integração a empresa vencedora devera prover os serviço de manutenção suporte e gestão da solução proposta. Todos os equipamentos integrantes da solução deverão ser novos sem uso anterior, os equipamento rede, wireless e software de gerenciamento deverão ser do mesmos fabricante, para garantir a integração e o gerenciamento centralizado.

Descrição dos equipamentos e serviços que compõem a solução:

1. Serviços de implementação da solução de infraestrutura:

1.1. Instalação do rack fornecido no presente edital, incluindo regularem e nivelamento do mesmo;

1.2. Instalação física de todos os equipamentos do presente edital (storage, gavetas, discos, servidores e switches) incluindo desembalagem, montagem, afixação e cabeamento nos racks fornecidos, englobando ligações elétricas, lógicas (LAN e SAN) e ativação da solução;

1.3. Energização dos equipamentos e análise do funcionamento do ambiente;

1.4. Identificação de todas as conexões efetuadas para futuras manutenções e alterações na configuração;

1.5. Atualização do firmware dos componentes de hardware da solução (módulos de gerenciamento, módulos LAN e SAN, controladoras, gavetas, discos, BIOS de servidores) para a última versão disponível conforme matriz de compatibilidade do fabricante;

1.6. Configuração dos parâmetros de BIOS dos servidores e interfaces para atender as recomendações dos fabricantes para o software de virtualização;

1.7. Criação do RAID na controladora de discos locais;

1.8. Execução do zonning e ISLs dos switchs SAN

1.9. Criação de VLANs nos módulos LAN dos para o ambiente de rede da PM de Vacaria;

1.10. Instalação, atualização e configuração do software de gerenciamento da solução, incluindo configuração das contas de administrador para acesso à solução, e-mails de alerta, filtragem de eventos e envio de SNMP para software de monitoramento;

1.11. Adição dos equipamentos no ambiente do software de gerenciamento;

1.12. Sessão de orientação onde será abordada a utilização do software de gerenciamento e do software de monitoramento, incluindo criação de novos usuários, configuração de autorizações na plataforma. A PM Vacaria deve ter a capacidade de adição de novos equipamentos e/ou recursos, implementar configurações, consultar as configurações existentes, efetuar o monitoramento da solução, enfim, a completa utilização da ferramenta;

2. Configuração da solução de armazenamento

2.1. Instalação do software de gerenciamento, replicação e movimentação de dados no storage, incluindo patches e atualizações necessárias;

2.2. Habilitação das funcionalidades e recursos previstas na solução disponibilizada;

2.3. Sessão de orientação onde será abordada a utilização do software e do hardware de armazenamento do presente edital, incluindo criação de snapshots, clones, mirror, utilização de Thin Provisioning e Tierização, criação de disk groups, monitoramento de utilização e carga, enfim, a completa utilização da ferramenta e do hardware adquirido;

3. Instalação do software de virtualização

3.1. Instalação do software de virtualização (hypervisor) VMware vSphere 5.1 em sua última release nos servidores, conforme matriz de compatibilidade dos equipamentos;

3.2. Instalação de patches e atualizações necessários;

3.3. Instalação e configuração da ferramenta de gerenciamento do ambiente virtualizado VMware vCenter Server 5.1;

3.4. Configuração da integração do software de virtualização com o software de replicação da storage e reconhecimento das áreas de discos replicadas;

3.5. Configuração da replicação das máquinas virtuais no software de backup e replicação;

3.6. Instalação e configuração da ferramenta de alta disponibilidade de entre servidores (módulo HA). Os servidores de virtualização deverão operar em um ambiente de alta disponibilidade onde, em caso de falha de qualquer um dos servidores, as máquinas virtuais deste servidor poderão ser reiniciadas automaticamente em qualquer outro servidor de virtualização;

3.7. Configuração da funcionalidade de migração online de máquinas virtuais entre servidores físicos sem interrupção do processamento;

3.8. Criação de clusters de alta-disponibilidade entre os hypervisors;

3.9. Instalação e configuração da ferramenta de recuperação de desastres disponibilizada na solução e todos os seus componentes;

3.10. Criação de até 2 (duas) politicas de replicação e recuperação de desastres para até 5 (cinco) máquinas virtuais.

3.11. Demonstração da verificação do perfeito funcionamento do plano de recuperação, em ambiente isolado, sem afetar as máquinas virtuais em produção;

3.12. A configuração dos softwares vMware vCenter Server 5.1 deve ser efetuada em máquina virtual hospedada nos clusters de alta disponibilidade e não em servidores externos ao ambiente caso houver;

3.13. Criação de até 2 (dois) templates de máquinas virtuais a ser utilizado no ambiente da PM de Vacaria,

3.14. Criação de novas máquinas virtuais através de modelos pré-definidos ou de forma manual e individual;

3.15. Deverá permitir o gerenciamento dos recursos físicos e virtuais do ambiente de virtualização, com estatísticas online do uso destes recursos, como I/O, Memória, Processamento, Latência;

4. Conversão de máquinas físicas

4.1. Conversão de 2 (duas) máquinas físicas existentes na infraestrutura de TI da PM de Vacaria para máquinas virtuais no novo ambiente de virtualização;

4.2. Instalação de ferramentas de otimização nas máquinas virtuais convertidas de forma a funcionar com perfeita integração e máximo desenho no novo ambiente de virtualização;

4.3. A contratada deverá garantir que os servidores inicializem corretamente o sistema operacional após a conversão;

4.4. A conversão não será executada em lote, sendo que a cada conversão será feita a validação dos serviços e do funcionamento da máquina virtual antes de iniciar a migração da próxima máquina virtual;

5. Instalação e Configuração da solução de segurança, Firewall;

5.1. A instalação dos equipamentos deverá ser feita por profissionais devidamente qualificados e certificados pelo fabricante contemplando os itens abaixo:

5.1.1. Análise da topologia e arquitetura da rede da contratante, considerando os roteadores e switches de backbone instalados, acesso à Internet, sites remotos, serviços de rede oferecidos aos funcionários da contratante, serviços externos, regras de firewall existentes, bem como qualquer outro equipamento ou sistema relevante na segurança do perímetro, sendo então feitas as configurações gerais do sistema de firewall de acordo com a configuração atual.

5.1.2. Para as regras específicas de usuários e aplicações deverá ser repassado o modo de criação do modelo destas regras, ficando a cargo deste órgão o desenvolvimento conforme suas políticas.

5.1.3. Durante toda a implantação do projeto, o técnico da contratada deverá demonstrar aos técnicos da contratante como instalar e configurar o firewall (instalação assistida). Esta demonstração deverá ser no formato treinamento hands-on com no mínimo 08(oito) horas de duração, contemplando os conceitos das tecnologias utilizadas pelo equipamento e a operação dos principais recursos dos produtos ofertados.

5.1.4. Todo o processo de instalação e configuração do sistema deverá ser documentado pela contratada sob a forma de relatório ou roteiro, de forma que os técnicos da contratante possam reproduzir a instalação do firewall quando necessário consultando a documentação.

6. Instalação e Configuração da solução de Rede Wireless;

6.1. A instalação dos equipamentos deverá ser feita por profissionais devidamente qualificados e certificados pelo fabricante contemplando os itens abaixo:

6.1.1. Deve contemplar todos os acessórios de fixação e a controladora e os access points com os respectivos injetores deverão ser instalados e fixados em local apropriado de forma que cubram toda a área determinada no site survay.

6.1.2. A fixação deverá ser precedida de análise técnica para determinação da melhor altura e posicionamento dos access points e as configurações devem ser realizadas de tal forma que seja obtido o melhor desempenho para transmissão de dados.

6.1.3. As atividades instalação e configuração solução deverão abranger aspectos acerca da disposição dos equipamentos, cronograma de implantação definido após contratação, parâmetros, topologia de rede, conectorização e plano de testes. Tais informações serão confeccionadas e validadas junto à equipe técnica da CONTRATANTE e deverão ser otimizadas para garantir total operabilidade e desempenho no ambiente computacional, considerando:

6.1.3.1. Preparação do atual ambiente para integração com os novos equipamentos;

6.1.3.2. Configuração de interfaces, endereçamento e serviços de rede;

6.1.3.3. Definição e configuração de VLANs para rede WLAN, gerenciamento, roteamento, entre outros;

6.1.3.4. Definição e configuração de métricas de priorização de tráfego de dados, gerência, entre outros;

6.1.3.5. Definição e configuração de parâmetros de roteamento dinâmico, trunking e de agregação de links entre os equipamentos wireless e equipamentos atuais;

6.1.3.6. Definição e configuração de parâmetros de gerenciamento SNMP;

6.1.3.7. Definição e configuração de parâmetros de segurança, incluindo autenticação de usuários e regras de acesso;

6.1.3.8. Plano de testes de conformidade da solução, com acompanhamento de técnico certificado na tecnologia.

6.1.3.9. Todos custos referentes à configuração e instalação dos access points, fornecimento de material, mão de obra e realização dos serviços acima mencionados deverão estar incluídos na proposta.

6.1.4. A empresa deverá configurar a rede sem fio de acordo com as necessidades do CONTRATANTE;

6.1.5. A empresa deverá fornecer a documentação do projeto especificada neste item impressa, encadernada e em arquivo digital.

6.1.5.1. Documentação de site survey

6.1.5.2. Cronograma do projeto;

6.1.5.3. Memorial dos serviços executados contendo marca e modelo dos equipamentos utilizados;

6.1.5.4. Relatório de testes contemplando os aspectos: Testes de Performance; Testes de PER (Packet Error Rate) – erros nos pacotes detectados pelo CRC devido, sobretudo, a efeitos de multi-percurso ou colisões na rede.

6.1.5.5. Testes de Interferências:

6.1.5.6. Análise de Cobertura da rede;

6.1.5.7. Verificação do cumprimento dos requisitos;

6.1.5.8. Verificação do projeto da rede e documentação disponível.

7. Instalação e Configuração Switch Core de Rede e Distribuição;

7.1. Entende-se como Equipamento de Core todos os dispositivos modulares ofertados. Os serviços a serem fornecidos para este atendimento são:

7.1.1. Instalação física de chassi em rack;

7.1.2. Instalação de fontes de alimentação, principais e redundantes, com respectivos cabos de energia;

7.1.3. Configuração básica de endereçamento IP, sistema e dados SNMP.;

7.1.4. Configuração do equipamento, com todas as funcionalidades solicitadas e necessárias para seu correto funcionamento: VLAN, Rotas estáticas ou dinâmicas, configuração SNMP, configuração de segurança, ACL, 802.1x.

7.2. Deve ser fornecida documentação com configurações dos equipamentos e diagrama da rede instalada;

7.3. O cabeamento logico e elétrico necessário para implantação de toda a solução será de responsabilidade da contratada, assim não sendo necessário a contemplar no projeto.

Ferramenta de Gerenciamento Centralizado

Quantidade: 01 unidade

1. Descobrimento, Mapeamento e Configuração Básica

1.1. Deve permitir o gerenciamento de configurações, desempenho e falhas na rede;

1.2. Deve permitir sua instalação nas seguintes plataformas:

- Windows Server 2003
- Windows XP
- Windows Server 2008 Enterprise
- Windows 7
- Windows 8
- Red Hat Enterprise Linux
- SuSE Linux versions 10 and 11
- Ubuntu 11.10 Desktop version
- VMware ESXi 4.0, 4.1, 5.0 or 5.1 server

1.3. O software de gerenciamento deve suportar o protocolo SNMP de gerenciamento de versão 1, 2 e 3;

1.4. Deve permitir o gerenciamento de todos os agentes SNMP dos dispositivos que compõe a infra-estrutura de TI; isto é; deve permitir a coleta e alteração das informações contidas nos objetos da Management Information Base (MIB) dos mesmos;

1.5. Deve permitir o descobrimento de equipamentos presentes em uma ou mais sub-redes, a fim de garantir uma auditoria constante na infra-estrutura de TI;

1.6. Deve permitir a criação de topologias / mapas automáticos da rede através de protocolos Layer 2 e Layers 3 (OSFP)

1.6.1. O mapa deve permitir a identificação de problemas com os dispositivos visualmente;

1.6.2. Permitir a visão agrupada da topologia conforme configuração do usuário;

1.7. O software deve permitir a criação, edição, remoção de VLANs nos dispositivo e associação das portas as mesmas;

1.8. Deve possuir um servidor de TFTP e BOOTP integrado a ferramenta, possibilitando o upgrade e downgrade de softwares dos dispositivos;

1.9. Deve permitir a identificação do status das portas dos dispositivos up ou down, enable ou disable, tecnologia e velocidade das portas;

1.10. Deve permitir a configuração do Dynamic Egress dos switches da rede;

1.11. Deve permitir a configuração de alertas da estação de gerenciamento, baseado nos eventos, severidade, tipo e categoria;

1.12. A ferramenta deve permitir a configuração gráfica de múltiplos domínios spanning tree (MSTP);

1.13. A ferramenta deve permitir a configuração gráfica de um servidor SMTP externo para o envio de informações de gerenciamento da ferramenta.

1.14. Deve permitir a alteração dos valores de um conjunto de objetos da MIB, em vários dispositivos;

1.15. Deve permitir exportar a tabela de dados coletados e alarmes, para os formatos “csv e html”;

1.16. Deve permitir envio de e-mail ou execução de um script ou programa integrado com a ferramenta para alertas;

1.17. A ferramenta deve permitir o gerenciamento dos dispositivos através de uma página WEB customizável;

1.18. Permitir a localização de um dispositivo da rede baseado nos argumentos endereço IP, endereço MAC, user name, nome da máquina e sub-rede;

1.19. Permitir integração com a base de dados do framework HP Open View;

1.20. Deve permitir a otimização do processo de busca na tabela Node/Alias dos dispositivos da rede;

1.21. A solução deverá prover recursos de "troubleshooting" capaz de mostrar por meio do RMON dados presentes nos switches performance ou estatísticas de utilização;

2. Configurações de Segurança e QoS:

2.1. Deve permitir o gerenciamento das configurações de filas e priorização de tráfego dos dispositivos da rede;

2.2. Deve permitir a criação de perfis de classificação do tráfego nos dispositivos, baseado em usuários;

2.3. Deve permitir a criação e o gerenciamento de políticas de acesso a rede nos dispositivos;

2.4. Deve suportar e gerenciar graficamente as características do padrão IEEE 802.1X;

2.5. Deve permitir a configuração para atribuição de perfil de usuário com regras e QoS especifico conforme autenticação do usuário;

2.6. A ferramenta deve permitir a configuração gráfica das taxas de inbound rate limit – IRL;

2.7. A ferramenta deve permitir a configuração estática e dinâmica da funcionalidade MAC Locking ou Port Security, para executar o LOCK de MAC Address na rede;

2.8. A ferramenta deve permitir a configuração gráfica de vários métodos de autenticação, atendendo no mínimo a configuração da autenticação WEB, autenticação MAC e autenticação IEEE 802.1x;

2.9. A ferramenta deve permitir a configuração de classes de serviços, utilizando no mínimo os parâmetros de Class of Service – COS, 802.1p priority e IP Type of Service – TOS;

2.10. A ferramenta deve permitir a configuração gráfica dos parâmetros da RFC 3580 (VLAN dinâmica conforme autenticação) nos dispositivos de rede;

2.11. Deve permitir o agrupamento de portas automático e/ou manual para atribuição de regras de seguranças. (ex. Uplinks em fibra)

2.12. A ferramenta deve permitir a configuração gráfica dos parâmetros de re-autenticação dos usuários nas portas dos switches;

2.13. A ferramenta deve permitir a configuração da autenticação CEP – Convergence End Point, para atribuição automática de VLAN ou perfil de equipamentos com suporte a CEP – ex. telefones IP, câmeras IP, etc.

3. Controle de Inventario e Backup

3.1. A ferramenta deve permitir o inventário detalhado de atributos dos dispositivos da rede, atendendo no mínimo números seriais, versão de firmware, tipo de CPU e memória;

3.2. A ferramenta deve permitir o armazenamento histórico das configurações dos dispositivos;

3.3. A ferramenta de permitir a comparação da configuração atual do dispositivo com a configuração armazenada na ferramenta;

3.4. A ferramenta deve possuir a capacidade de gerar relatórios de para planejamento de capacidade, atendendo no mínimo a geração de relatórios da utilização mínima de chassis e portas, informações sobre FRU – Field Replaceable Upgradeable nos dispositivos;

3.5. Deve permitir o upgrade da PROM de BOOT dos dispositivos, unitariamente e para um grupo de dispositivos;

3.6. A ferramenta deve permitir a execução do reset dos dispositivos através do protocolo SNMP;

4. Resposta Automática para Eventos de Segurança

4.1. Permitir a criação de um grupo de VLANs com características pré-definidas, permitindo uma implementação ou auditoria instantânea dos domínios de colisão criados nos dispositivos da rede

4.2. Capacidade de localizar o usuário originador de um ataque ou exploração de vulnerabilidade, proveniente da identificação do IDS, através das tabelas Node Alias dos switches;

4.3. Capacidade de localização de um usuário em qualquer porta de um switch, através do protocolo SNMP, quando detectado a ação worms e vírus na rede;

4.4. A ferramenta deve possuir um trigger test que permita o teste de comunicação entre os mecanismos de segurança e localização dos usuários na rede;

Switch de Acesso – 24 portas Giga UTP e 04 portas SFP

Quantidade: 05 unidades

Características Físicas

1. Deve possuir estrutura do tipo desktop, para instalação em rack padrão EIA (19") e possuir kits completos para instalação;

1.1. Deve possuir altura máxima de 1 RU;

1.2. Deve possuir fonte de alimentação interna ao equipamento, que opere com tensões de entrada entre 100 e 240 VAC e suporte freqüência entre 50/60 Hz;

1.3. Deve suportar fonte redundante externa.

Quantidade de Portas

1.4. Deve possuir porta console RS-232 com conectores DB9 ou RJ-45;

1.5. Deve estar configurado com pelo menos:

1.5.1. 24 (vinte e quatro) portas fixas em Gigabit Ethernet, 10/100/1000Base-T em conectores RJ-45;

1.5.2. 04 (quatro) portas do tipo SFP;

1.6. O equipamento deve permitir o uso simultâneo de todas as interfaces solicitadas.

Capacidade e Performance

1.7. Deve possuir capacidade de throughtput de, no mínimo 40 Mpps;
1.8. Deve possuir capacidade de switching de, no mínimo 55 Gbps;
1.9. Deve implementar tabela de endereçamento para, no mínimo, 16.000 endereços MAC;
1.10. Deve implementar, no mínimo, 250 VLANs (IEEE 802.1Q);
1.11. Deve permitir, no mínimo, 4.090 identificadores de VLAN (VID).

Funcionalidades

1.12. Deve permitir agregação de links conforme o padrão IEEE802.3ad suportando no mínimo 05 grupos LAG com no mínimo 08 portas por grupo LAG;
1.13. Deve implementar espelhamento de tráfego para análise de rede;
1.14. Deve implementar gerenciamento via protocolo SNMP v1, v2c e v3. Sendo que para a versão 3 deve implementar autenticação via MD5 e criptografia DES;
1.15. Deve suportar o gerenciamento via interface gráfica;
1.16. Deve implementar autenticação IEEE802.1x;
1.17. Deve implementar autenticação MAC.

Protocolos

1.18. Deve implementar IEEE 802.1Q (VLAN Tagging);
1.19. Deve implementar IEEE 802.1s (Multiple Spanning Tree);
1.20. Deve implementar IEEE 802.3x (Flow Control);
1.21. Deve implementar IEEE 802.1D (MAC Bridges);
1.22. Deve implementar IEEE 802.1w (Rapid Spanning Tree);
1.23. Deve implementar IGMP snooping v1, v2 e v3;
1.24. Deve implementar Jumbo Frame;
1.25. Deve implementar o padrão IEEE 802.1AB e LLDP-MED.

Roteamento

1.26. Deve implementar roteamento IP através de rotas estáticas.

Qualidade de serviço

1.27. Deve implementar IEEE 802.1p (Classificação de tráfego);
1.28. Deve implementar Rate Limiting;
1.29. Deve possuir, no mínimo, 06 filas de prioridade por porta;
1.30. Deve possuir algoritmo de enfileiramento Strict Priority e Weighted Round Robin.

Segurança

1.31. Deve permitir o controle de acesso a rede baseado no endereço MAC;

1.32. Deve implementar ACL ou outra funcionalidade de filtragem de tráfego por por endereço MAC de origem/destino e por endereço IP de origem/destino;

1.33. Deve possuir facilidade que permita desabilitar automaticamente uma interface de acesso que esteja recebendo pacotes BPDU (Bridge Protocol Data Unit), através de funcionalidade BPDU Guard ou similar;

1.34. Deve implementar funcionalidade que bloqueie a operação de servidores DHCP inválidos (DHCP Spoof Protection);

1.35. Deve implementar funcionalidade de ARP Spoof Protection;

1.36. Deve permitir o isolamento de portas pertencente à uma mesma VLAN, através da funcionalidade Private VLAN ou similar.

Gerenciamento

1.37. Deve implementar SSHv2;

1.38. Deve implementar SNMP v1, v2c e v3;

1.39. Deve implementar NTP ou SNTP;

1.40. Deve implementar Syslog;

1.41. Deve possibilitar autenticação em base remota por meio do protocolo RADIUS;

1.42. Deve implementar RADIUS ou TACACS+ para controle de gerenciamento do switch;

1.43. Deve implementar Telnet;

1.44. Deve implementar TFTP;

1.45. Deve implementar CLI;

1.46. Deve implementar, no mínimo, 04 grupos de RMON – Statistics, History, Alarms e Events.

Deve possuir as seguintes RFC and MIB

- GVRP – Generic VLAN Registration Protocol
- IEEE 802.1X MIB – Port Access
- ANSI/TIA-1057 – LLDP-MED MIB
- IEEE 802.1AB – LLDP MIB
- RFC 768 – UDP
- RFC 783 – TFTP
- RFC 791 – IP
- RFC 792 – ICMP
- RFC 793 – TCP
- RFC 826 – Ethernet ARP
- RFC 854 – Telnet

- RFC 1157 – SNMP
- RFC 1213 – MIB/MIB II
- RFC 1493 – BRIDGE-MIB
- RFC 1643 – Ethernet-like MIB
- RFC 2618 – RADIUS Authentication Client MIB
- RFC 2620 – RADIUS Accounting Client MIB
- RFC 2737 – Entity MIB (physical branch only)
- RFC 2819 – RMON-MIB
- RFC 2933 – IGMP MIB
- RFC 3413 – SNMP v3 Applications MIB
- RFC 3584 – SNMP Community MIB

Solução Wireless – Controlador

Quantidade: 01 unidades

1) Características Básicas

1.1) Deve ser fornecido em hardware do tipo appliance, ou máquina virtual para ambiente VMWare ESXi, dedicado à funcionalidade de gerenciamento e controle de Access Points, possuindo firmware ou sistema operacional próprio;

1.2) Deve suportar a adição de funcionalidade de IDS/IPS, seja por adição de software ou appliance de mesmo fabricante;

1.3) A solução deve permitir, através de adição de licenças, o gerenciamento de pelo menos 240 APs e estar licenciada para gerenciar pelo menos 80 APs.

1.4) Em caso de fornecimento em Appliance, deve ser montável em rack padrão EIA 19" (dezenove polegadas) e possuir kits completos para instalação.

1.5) Equipamento do tipo WLAN Controller, para controle de access points distribuídos pela infraestrutura de rede.

1.6) Deve permitir gerenciar simultaneamente access points nos padrões IEEE802.11a, IEEE802.11b, IEEE802.11g e IEEE802.11n.

1.7) Deve suportar configuração automática para os access points.

1.8) Deve implementar controles automatizados de rádio frequência tais como ajustes de canal e potência.

1.9) Deve ser capaz de detectar falhas na cobertura wireless e automaticamente corrigi-las.

1.10) O WLAN Controller poderá estar diretamente e/ou remotamente conectado aos access points por ele gerenciados, inclusive via roteamento nível 3 da camada OSI.

1.11) Implementar varredura de RF contínua, programada ou sob demanda, com identificação de access points ou clientes irregulares.

1.12) Permitir o armazenamento de sua configuração em memória não volátil podendo, numa queda e posterior restabelecimento da alimentação, voltar à operação normalmente na mesma configuração anterior à queda de alimentação.

1.13) Cada unidade da solução deve possuir tamanho máximo de 1 RU e ser aplliance único somente para a função de WLAN Controller. Não serão aceitas soluções onde o WLAN Controller seja módulo ou sub módulo de algum switch.

1.14) Deve ser acompanhado de todos os acessórios necessários para operacionalização do equipamento, tais como: softwares, cabos de console, cabos de energia, kits para montagem no rack, documentação técnica e manuais que contenham informações suficientes que possibilitem a instalação, configuração e operacionalização dos equipamentos.

2) Interfaces e Fontes (em caso de Appliance)

2.2) Deve possuir, no mínimo, 2 portas 10/100/1000BaseT ou 1000BaseT, em conector RJ45 fêmea, diretamente instalado no equipamento.

2.3) Deve possuir, no mínimo, 1 interface dedicada ao gerenciamento do tipo Gigabit Ethernet 10/100/1000.

2.4) Deve possuir fonte de alimentação interna ao equipamento, que opere com tensões de entrada entre 110-240VAC e frequência 50/60hz.

3) Funcionalidades

3.1) Deve implementar sincronismo de relógio interno via NTP ou SNTP.

3.2) O WLAN controller deve suportar modo de operação em alta disponibilidade operando em conjunto com um ou mais WLAN Controllers.

3.3) Deve implementar o padrão 802.1q.

3.4) Deve possuir servidor DHCP interno.

3.5) Implementar DHCP relay e DHCP Server.

3.6) Deve suportar armazenamento de imagens para os access points.

3.7) Deve implementar RADIUS Client.

3.8) Deve implementar TFTP Client ou FTP Client.

3.9) Deve implementar Syslog.

3.10) Deve possuir localmente no WLAN Controller um portal web para autenticação dos usuários visitantes, sendo possível a customização com informações e características visuais (mensagem, logo, banner, etc).

3.11) O portal web de autenticação, bem como a ferramenta de administração e gerência, devem ser acessadas via web nativo, sem a necessidade de instalação de nenhum software ou plug-in adicional.

3.12) A base de usuários visitantes deve ser interno ao WLAN Controller, não sendo necessário alterações (inclusão/exclusão/alteração) na base de dados dos usuários corporativos (Active Directory/LDAP).

3.13) A criação das contas de visitantes deve possibilitar a criação de no mínimo os seguintes parâmetros:

- Nome do usuário
- Senha
- Descrição da conta
- Data de inicio e término de validade
- Horário permitido
- Tempo de sessão

3.14) A ferramenta de criação dos usuários visitantes deverá ter uma página onde constem as informações de conta e políticas de uso da instituição, sendo possível a impressão destas informações para entrega ao visitante no momento do registro.

3.15) Implementar sistema de balanceamento de carga para associação de clientes entre access points próximos, para otimizar a performance.

3.16) Permitir configuração em Cluster, suportando em conjunto pelo menos 480 APS, Se um WLAN Controller falhar, os access points relacionados deverão se associar a um WLAN Controller alternativo (isso deve ocorrer somente se houver 2 WLAN Controller instalados em paridade).

4) Capacidades

4.1) Deve ser capaz de gerenciar, através de um ponto central, os access points que estejam conectados em ativos da infra-estrutura de rede existente, em diversas vlans e sub-redes IP.

4.2) Cada WLAN Controller deve gerenciar, no mínimo, 80 access points ativos simultaneamente e permitir o upgrade através de licenças para até 240 access points ativos simultaneamente.

5) Voz

5.1) Deve implementar 802.11e.
5.2) Deve implementar WMM (Wi-Fi Multimedia).
5.3) Deve implementar CAC (Call Admission Control) para as chamadas de voz.
5.4) Deve implementar U-APSD para economia de bateria dos clientes.
5.5) Deve implementar Roaming entre diferentes subredes.
5.6) Deve implementar Roaming entre WLAN Controllers.

6) Segurança

6.1) Deve implementar mecanismo de AAA para para usuários da rede wireless.
6.2) Deve implementar o protocolo de autenticação IEEE802.1x com atribuição dinâmica de VLAN.
6.3) Deve implementar autenticação de usuário conforme o padrão IEEE 802.1x com suporte a atribuição automática de filtros de acesso no access point de acordo com os parâmetros do usuário.
6.4) Deve implementar o protocolo de autenticação IEEE802.1x com suporte aos seguinte métodos: EAP-TLS, PEAP, EAP-FAST, EAP-MD5.
6.5) Deve implementar autenticação através de endereço MAC.
6.6) Deve implementar os seguintes algorítimos de criptografia: AES (CCMP), RC4 – 40, 128-bit (TKIP, WEP).
6.7) Deve implementar Wi-Fi Protected Access (WPA) e WPA2.
6.8) Deve implementar 802.11i.
6.9) Deve implementar autenticação remota via RADIUS Server.
6.10) Implementar mecanismo de minimização do tempo de roaming (deslocamento) de clientes autenticados via 802.1x (Fast Secure Roaming) entre dois access points no mesmo segmento de rede ou em segmentos de rede distintos.

7) Gerenciamento

7.1) Deve ser gerenciado através de web browser comum via protocolo HTTPS.
7.2) Deve implementar gerenciamento via linha de comando através de Telnet e SSH.
7.3) Deve possuir uma porta console para configuração local via linha de comando CLI (Command Line Interface).
7.4) Deve suportar SNMP versão 3.

Wireless - Access Point 802.11 a/b/g/n

Quantidade: 8 unidades

Access Point 802.11a/b/g/n

1. **Características Básicas**
   1.1. Equipamento do tipo access point, que opere em conjunto com WLAN Controller.
   1.2. Deve ser do mesmo fabricante do WLAN Controller.
   1.3. O equipamento deve suportar os padrões IEEE 802.11a, IEEE 802.11b, IEEE 802.11g e IEEE 802.11n.

1.4. Possuir certificação da Wi-Fi Alliance para 802.11a/b/g/n.
1.5. Deve operar simultaneamente com usuários configurados nos padrões 802.11a/b/g e n.
1.6. Deve possuir obrigatoriamente antenas internas, de forma a impedir sua remoção e possíveis furtos.
1.7. Deve possuir antenas internas com ganho de no mínimo 3 dBi para 2,4GHz e no mínimo 6 dBi para 5 GHz.
1.8. Deve implementar as técnicas de modulação 802.11a OFDM; 802.11g DSSS e OFDM; 802.11b DSSS; MIMO 2x2para 802.11n.
1.9. Deve possuir 1 interface Gigabit Ethernet 10/100/1000 Base-T, com conector RJ-45.
1.10. Deve possuir leds de indicação de status do access point e de conectividade.
1.11. Deve implementar funcionalidade de descoberta automática do WLAN Controller.
1.12. Deve implementar até 16 SSIDs.
1.13. Permitir criptografia, Qos e gerenciamento de RF.
1.14. Permitir a continuidade da sessão do usuário no caso de queda do WLAN Controller principal (isso deve ocorrer somente se houver 2 WLAN Controller instalados em paridade).
1.15. Permitir, no mínimo, 120 usuários simultâneos por rádio.
1.16. Deve suportar a função de alimentação de energia elétrica do equipamento através de cabo UTP categoria 5 ou superior.
1.17. Deve suportar a alimentação elétrica do access point gerenciado via interface de rede 10/100/1000 Mbps, de acordo com o padrão PoE (power over ethernet), mantendo todas as suas funcionalidades em plena capacidade, sem perda do desempenho máximo do access point e consumindo apenas 1 porta do access point e do switch.
1.18. O equipamento deve suportar fonte de alimentação com as tensões de alimentação 100-240 VAC.
1.19. Deverá ser fornecido junto com Acess Point módulo PoE, compatível.
1.20. Deve possuir, no mínimo, as seguintes taxas de dados:
1.21. 802.11a: 6, 9, 12, 18, 24, 36, 48, 54 Mbps
1.22. 802.11b: 1, 2, 5.5, 11 Mbps
1.23. 802.11g: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps
1.24. 802.11n: 6,5 Mbps a 300 Mbps
1.25. Deve possuir, no mínimo, a sensibilidade de recepção dos rádios conforme abaixo:
1.26. -90 dBm operando em 802.11b com velocidade de 11 Mbps
1.27. -81 dBm operando em 802.11g com velocidade de 54 Mbps
1.28. -80 dBm operando em 802.11a com velocidade de 54 Mbps
1.29. -68 dBm operando em 802.11n 5Ghz HT40 MSC15 300 Mbps
1.30. -69 dBm operando em 802.11n 2.4 Ghz HT40 MCS15 300 Mbps
1.31. Deve estar em conformidade com os seguintes padrões de segurança: UL / IEC / EN 60950.
1.32. Deve estar em conformidade com os seguintes padrões: EN 301 893; EN 300 328; EN 301 489 -1 & 17; EN 60601-1-2.
1.33. O ponto de acesso poderá estar diretamente ou remotamente conectado ao WLAN Controller, inclusive via roteamento nível 3 da camada OSI.
1.34. Permitir habilitar e desabilitar a divulgação do SSID.
1.35. Possuir porta de console para gerenciamento e configuração via linha de comando (CLI – comand line interface).
1.36. Implementar cliente DHCP, para configuração automática de rede.
1.37. Implementar 802.1X do access point à rede, isto é, autenticação através de 802.1x do próprio access point.

1.38. Deve ser acompanhado de todos os acessórios necessários para operacionalização do equipamento, tais como: softwares, cabos de energia elétrica, estrutura para fixação em paredes e teto, documentação técnica e manuais que contenham informações suficientes para possibilitar a instalação, configuração e operacionalização do equipamento.

2. Voz

2.1. Deve implementar Call Admission Control (CAC).
2.2. Deve implementar U-APSD para economia de bateria dos clientes.
2.3. Implementar qualidade de serviço WMM, 802.11e.
2.4. Permitir até 12 chamadas de voz simultâneas (802.11b, G.711).

3. Segurança

3.1. Permitir suporte a passagem de tráfego VPN IPSec, PPTP, L2TP.
3.2. Implementar segurança via WEP, WPA (TKIP), WPA2 (AES), 802.11i, 802.1x para acesso dos clientes wireless.
3.3. Implementar Fast Secure Roaming e handover com Pre-authentication e Opportunistic Key Caching.
3.4. Deve possuir funcionalidade de rogue detection.
3.5. Deve poder trabalhar como sensor WIPS.

Solução Segurança - Firewall

Quantidade: 01 unidades

1. Requisitos Gerais:

1.1. Deve ser fornecida Solução de Segurança;

1.2. Solução de segurança de informação perimetral que inclui dois firewall, administração de largura de banda de serviço de internet (QoS), suporte para conexões VPN IPSec e SSL, proteção contra ameaças de vírus e malware, bem como controle de transmissão de dados e acesso a internet.

1.3. Deverá incluir um módulo de proteção contra ameaças de rede, bloqueio de vírus, spyware, controle de transferência de arquivos, controle da navegação de internet e bloqueio de arquivos por tipo.

1.4. O firewall devem ter a capacidade de operar de forma simultânea mediante o uso das suas interfaces físicas nos seguintes modos: Modo sniffer (monitoramento e análise do tráfego de rede), camada 2 (l2) e camada 3 (l3).

1.4.1. Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede.

1.4.2. Modo Camada – 2 (L2), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação.

1.4.3. Modo Camada – 3 (L3), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação. Gerar roteamento virtual para pelo menos 10 roteadores virtuais e administração do tráfego entre diferentes áreas de segurança e sub-redes, suportando pelo menos 30 áreas de segurança e um mínimo de 5 sistemas virtuais.

1.4.4. Modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas.

1.5. Suporte para múltiplos sistemas virtuais lógicos (Contextos) no firewall Físico.

1.6. Os contextos virtuais devem suportar todas as funcionalidades base desde edital, como por exemplo, Firewall, VPN, Controle de Aplicações, IPS, Anti-virus, Anti-Spyware, NAT, Filtro de URL, de-criptografia de SSL e Identificação de usuários.

Deverá contar com suporte para os serviços a seguir:

1.7. Redes Virtuais, vlans 802.1q, 802.3ad link aggregation;

1.8. Tradução de endereços da rede (NAT) por origem e destino, por endereços ip dinâmicos e pool de portas.

1.9. PPPOE, bgp, ospf e rip2, dhcp server e dhcp relay.

1.10. Protocolos de encriptação IKE, 3Des (com criptografia de 128, 192 e 256 bits), AES, SHA1 e MD5.

1.11. Deverá suportar pelos menos os seguintes protocolos de VOIP: H.323, SIP, SCCP e MGCP.

1.12. Identificação, Controle e visibilidade sendo:

1.12.1. Identificação, Controle (Uso de aplicações por usuário mediante interação com Ldap, Active Directory ou Radius e endereço ip).

1.12.2. Identificação deve ser de modo independente à porta lógica e/ou aplicações que utilizam as portas 80 e 443 (Implica a descrição bidirecional de SSL e Identificação de aplicações que encapsuladas em túnel SSL).

1.12.3. Visibilidade de pelo menos 1400 aplicações incluindo peer-to-peer, facebook, twitter e web 2.0.

1.12.4. Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como Ultrasurf, Skype e ataques mediante a porta 443.

1.13. Em caso de protocolos desconhecidos, poderão designar-se assinaturas próprias.

1.14. Descrição e controle de tráfego SSHv2.

1.15. Detecção de aplicações dinâmicas dentro de sessões de proxy HTTP.

1.16. Controle de tráfego IPv4 e IPv6, este último inclui visibilidade e inspeção de ameaças em aplicações e controle de conteúdo. O IPV6 deve ser suportado em interfaces trabalhando em L2 e L3.

1.17. A solução deve ser ofertada em Appliance/hardware especifico para o proposito solicitado, não sendo aceito soluções baseadas em servidores abertos.

1.18. A Solução deve utilizar sistema operacional próprio “hardenizado”, não sendo aceitos sistemas operacionais Linux ou baseados em distribuições abertas.

1.19. A plataforma deve ser otimizada para analise de conteúdo de aplicações em camada 7.

2. Controles por Politicas de Firewall

2.1. Deverá suportar controles por zona de segurança.

2.2. Suportar as seguintes características:

2.2.1. Controles de politicas por porta e protocolo.

2.2.2. Controle de politicas por Aplicações e categorias de aplicações.

2.2.3. Controle de politicas por Usuários, Grupos de Usuários, Ips, Redes e Zonas de segurança.

2.2.4. Controle de politicas por código de Pais (Por exemplo: BR, USA, UK, RUS).

2.2.5. Controle de inspeção e de-criptografia de SSL por politica para trafego de entrada (Inbound) e Saida (Outbound).

2.2.6. Controle de inspeção e de-criptografia de SSH por politica.

2.3. Bloqueios dos seguintes tipos de arquivos: bat, cab, dll, exe, pif, e reg.

2.4. Traffic shaping QoS baseado em Politicas (Prioridade, Garantia e Máximo)

2.5. QoS baseado em políticas para marcacão de pacotes (diffserv marking).

2.6. Suporte a objetos e regras IPV6.

2.7. Suporte a objetos e regras multicast.

2.8. Suporta a atribuição de agendamento as politicas com o objetivo de habilitar e desabilitar politicas em horários pré-definidos automaticamente.

3. Controle de Aplicações

3.1. Deverá contar com ferramentas de visibilidade que permitam administrar o tráfego de aplicações, permitindo a execução de aplicações autorizadas e bloqueio de aplicações não autorizadas.

3.2. O controle de aplicações deve identificar as mesmas independente das portas e protocolos assim como técnicas de evasão utilizadas.

3.3. Descrever técnicas utilizadas pela solução para a detecção das aplicações (Assinaturas, Heurística, etc).

3.4. Deverá suportar múltiplos métodos de identificação e classificação das aplicações.

3.5. O controle de aplicações é baseado em Inspeção IPS ou inspeção profunda de pacotes (Deep Packet Inspection).

3.6. Para manter a segurança da rede eficiente, deve suportar o controle sobre aplicações desconhecidas e não somente sobre aplicações conhecidas.

3.7. Deverá suportar a criação de aplicações customizadas pela interface gráfica do produto.

3.8. Deverá incluir a capacidade de atualização para identificar novas aplicações.

3.9. Deverá atualizar a base de assinaturas de aplicações automaticamente.

3.10. O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas do fabricante.

3.11. Deverá alertar o usuário quando uma aplicação foi bloqueada.

3.12. Deverá possibilitar que o controle de portas seja aplicado para todas as aplicações.

3.13. Deverá possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, emule, neonet, etc.) possuindo granularidade de controle/politicas para os mesmos.

3.14. Deverá possibilitar a diferenciação de tráfegos de Instant Messaging (AIM, YIM, Facebook Chat, etc.) possuindo granularidade de controle/politicas para os mesmos.

3.15. Deverá possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o YIM chat e bloquear a transferência de arquivos.

3.16. Deverá possibilitar a diferenciação de aplicações Proxies (ultrasurf, ghostsurf, freegate, etc.) possuindo granularidade de controle/politicas para os mesmos.

3.17. Deverá incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via ldap, Active Directory, E-diretório e base de dados local.

3.18. Deverá possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em Usuários e Grupos de usuários.

3.19. Deverá possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em Usuários e Grupos de usuários.

3.20. Deverá possuir integração com Ldap para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em Usuários e Grupos de usuários.

3.21. Deverá incluir a capacidade de criação de políticas baseadas no controle por aplicação, categoria de aplicação, subcategoria, tecnologia e fator de risco.

3.22. Deverá incluir a capacidade de criação de políticas baseadas no controle por usuário, grupos de usuários ou endereço ip.

3.23. Deverá incluir a capacidade de criação de políticas baseadas em “traffic shaping” por aplicação, usuário, origem, destino, túnel vpn-ipsec-ssl.

3.24. Deverá permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (Captive Portal).

3.25. Suporte a autenticação Kerberos.

3.26. Deverá possuir suporte a identificação de usuários em ambiente Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços.

4. Prevenção de ameaças.

4.1. IPS

4.1.1. Para proteção do ambiente contra ataques, deve ser incluído modulo de IPS integrado na própria ferramenta de Firewall ou entregue com composição com outro fabricante.

4.1.2. O módulo de IPS oferecido deve ter passado nos testes da NSS Labs para produtos de IPS com pelo menos 90% de efetividade, ter 100% de efetividade nos testes de evasão e estar entre os recomendados do relatório.

4.1.3. Deverá suportar granularidade nas politicas de IPS, possibilitando a criação de diferentes politicas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens.

4.1.4. Deverá possibilitar a criação de diferentes profiles de IPS a serem aplicados por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens.

4.1.5. Deverá permitir o bloqueio de vulnerabilidades.

4.1.6. Deverá permitir o bloqueio de exploits conhecidos.

4.1.7. Deverá incluir proteção contra ataques de negação de serviços.

4.1.8. Deverá possuir os seguintes mecanismos de inspeção de IPS:

4.1.8.1. Análise de padrões de estado de conexões

4.1.8.2. Análise de decodificação de protocolo

4.1.8.3. Análise para detecção de anomalias de protocolo

4.1.8.4. Análise heurística

4.1.8.5. IP Defragmentation

4.1.8.6. Remontagem de pacotes de tcp

4.1.8.7. Bloqueio de pacotes malformados

4.1.9. Deverá possuir assinaturas para bloqueio de ataques "buffer overflow".

4.1.10. Deverá possuir assinaturas para auxilio no bloqueio de ataques DoS/DDoS.

4.1.11. Deverá suportar o reconhecimento de ataques em trafego IPV6.

4.1.12. Deverá possuir assinaturas e mecanismos de detecção de anomalias prontas.

4.1.13. Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto.

4.1.14. Deverá ser possível a criação de exceções/exclusões por hosts para determinadas assinaturas.

4.1.15. Deverá suportar referencia cruzada com CVE.

4.1.16. Deverá possuir granularidade de ajustes com opções para sobrescrever assinaturas individualmente.

4.1.17. Deverá suportar atualização automática das assinaturas através de conexão segura.

4.1.18. Todos os modelos de equipamentos devem utilizar as mesmas assinaturas.

4.1.19. Deverá suportar varias técnicas de prevenção, incluindo Drop e tcp-rst (Cliente, Servidor e ambos).

4.1.20. Deverá suportar ações por assinaturas.

4.1.21. Suportar notificações e alertas via e-mail, SNMP traps e log de pacotes.

4.2. Antivírus / Anti-Spyware

4.2.1. Para proteção do ambiente contra Malware conhecido, deve ser incluído modulo de Anti-virus e Ant-Spyware de gateway integrado na própria ferramenta de Firewall ou entregue com composição com outro fabricante.

4.2.2. Deverá permitir o bloqueio de Malwares e Spywares.

4.2.3. Deverá ser possível a inspeção de Antivírus para pelo menos nos seguintes tipos de tráfegos: HTTP, SMTP, POP3, IMAP e SMB.

4.2.4. Deverá incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms.

4.2.5. Proteção contra downloads involuntários usando HTTP de arquivos executáveis. maliciosos.

4.2.6. Rastreamento de vírus em pdf.

4.2.7. Deverá permitir a inspeção em arquivos comprimidos que utilizam o algoritmo deflate (zip, gzip, etc.)

4.2.8. Deverá suportar bloqueio de arquivos por tipo (pelo menos 50 tipos).

4.2.9. A atualização de assinaturas deverá ser diária, semanal e de emergência.

4.2.10. Deve suportar atualização automática das assinaturas através de conexão segura.

4.2.11. As atualizações de ameaças, Antivírus e Anti-spyware não devem depender de reboot do equipamento para efetivação.

4.2.12. Todos os modelos de equipamentos devem utilizar as mesmas assinaturas.

4.2.13. Suportar notificações e alertas via e-mail, SNMP traps e log de pacotes.

4.3. Deve suportar, e estar licenciada, análise de Malware "In Cloud"

4.3.1. Devido aos Malwares hoje em dia serem muito dinâmicos e um antivírus comum reativo não ser capaz de detectar os mesmos com a mesma velocidade que suas variações são criadas, a solução ofertada dever possuir funcionalidades para análise de Malwares não conhecidos incluídas na própria ferramenta ou entregue com composição com outro fabricante.

4.3.2. Para ameaças/Malwares não conhecidos, o produto deve ser capaz de enviar o arquivo para análise automática "In Cloud". Onde o arquivo será executado e simulado em ambiente controlado.

4.3.3. Essa analise deve suportar a monitoração do arquivo para mais de 60 comportamentos maliciosos.

4.3.4. Esse sistema automático de analise "In Cloud" deve prover:

4.3.4.1. Informações Sobre as ações do Malware na máquina infectada.

4.3.4.2. Informações sobre quais aplicações são utilizadas para causar/propagar a infecção.

4.3.4.3. Detectar aplicações não confiáveis utilizadas pelo Malware.

4.3.4.4. Gerar assinaturas de Antivírus e Anti-Spyware automaticamente.

4.3.4.5. Definir URLs não confiáveis utilizadas pelo novo Malware.

4.3.4.6. Entre outros provendo uma maior segurança para a rede do cliente.

5. Filtro de URL

5.1. Para maior controle e visibilidades dos acessos dos usuários do ambiente, deve ser incluído modulo de filtro de URL integrado na própria ferramenta de Firewall ou entregue com composição com outro fabricante.

5.2. Deve ser possível a criação de politicas por Usuários, Grupos de Usuários, Ips, Redes e Zonas de segurança.

5.3. Deve ser possível definir horários para o funcionamento da politica.

5.4. Deverá incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, autenticação via ldap, Active Directory, E-diretório e base de dados local.

5.5. Deverá possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em Usuários e Grupos de usuários.

5.6. Deverá possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em Usuários e Grupos de usuários.

5.7. Deverá possuir integração com Ldap para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em Usuários e Grupos de usuários.

5.8. Deverá incluir a capacidade de criação de políticas baseadas no controle por URL e Categoria de URL.

5.9. Deverá permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (Captive Portal).

5.10. Deverá possuir suporta a identificação de usuários em ambiente Citrix e Microsoft Terminal Server, permitindo visibilidade e controle sobre o uso das URLs que estão sendo acessadas através destes serviços.

5.11. Deve possibilitar base de URLs local no Appliance, evitando delay de comunicação/validação da URLs.

5.12. Deverá possuir pelo menos 50 categorias de URLs.

5.13. Deverá possibilitar a criação Categorias de URLs customizadas.

5.14. Deverá possibilitar a exclusão de URLs do bloquei por categoria.

5.15. Deve possibilitar a customização de pagina de bloqueio.

5.16. Deve possibilitar o bloqueio e continuação (Possibilitando que o usuário acesse um site potencialmente bloqueado informando o mesmo na tela de bloqueio e possibilitando a utilização de um botão "Continuar" para possibilitar o usuário continuar acessando o site por um tempo).

5.17. Os logs do produto devem incluir informações das atividades dos usuários.

5.18. A atualização da base de dados deve ser automática com a opção de ser feita manualmente via tftp.

6. Filtro de Dados

6.1. Deve ser possível a criação de filtros para arquivos e dados pré-definidos.

6.2. Os arquivos devem ser identificados por extensão e assinaturas.

6.3. O firewall deve ser capaz de identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (ex. MS Office, PDF,etc) identificados sobre aplicações (Ex. P2P, IM, SMB, etc).

6.4. Deve ser possível a identificação de arquivos compactados e a aplicações de politicas sobre o conteúdo desses tipos de arquivos.

6.5. O firewall deve ser capaz de identificar e opcionalmente prevenir a transferência de informações sensíveis (Ex. Numero de cartão de credito, etc) possibilitando a criação de novos tipos de dados via expressão regular.

6.6. Listar o número de aplicações suportadas para controle de dados.

6.7. Listar o numero de tipos de arquivos suportados para controle de dados.

7. QoS

7.1. Deverá permitir o controle de políticas de uso com base nas aplicações: permitir, negar, agendar, inspecionar e controlar o uso da largura de banda que utilizam cada aplicação ou usuário.

7.2. Com a finalidade de controlar aplicações e trafego cujo consumo possa ser excessivo, (como youtube, ustream, etc.) e ter um alto consumo de largura de banda, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, deva ter a capacidade de controlá-las por políticas de máximo de largura de banda quando forem solicitadas por diferentes usuários ou aplicações, tanto de áudio como de vídeo streaming.

7.3. Suportar a criação de políticas de QoS por:

7.3.1. Endereço de origem

7.3.2. Endereço de destino

7.3.3. Por usuário ou Grupo do AD.

7.3.4. Por aplicações (como por exemplo Skype, Bittorrent, YouTube, Azureus)

7.3.5. Por aplicações estaticamente ou grupos dinamicamente (como por exemplo Instant Messaging ou grupo de aplicações P2P)

7.3.6. Por porta

7.4. O QoS deve possibilitar a definição de classes por:

7.4.1. Banda Garantida

7.4.2. Banda Máxima

7.4.3. Fila de Prioridade.

7.5. Suportar priorização RealTime de protocolos de voz (VOIP) como H.323, SIP, SCCP, MGCP e aplicações como Skype.

7.6. Suportar marcação de pacotes Diffserv

7.7. Disponibilizar estatísticas RealTime para classes de QoS.

7.8. Deverá permitir o monitoramento do uso que as aplicações fazem por bytes, sessões e por usuário.

8. GeoLocation

8.1. Suportar a criação de políticas por Geo Localização, permitindo o trafego de determinado Pais/Países sejam bloqueados.

8.2. Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos.

8.3. Deve possibilitar a criação de regiões geográficas pela interface gráfica e criar politicas utilizando as mesmas.

9. De-criptografia SSL/SSH

9.1. Deve identificar, de-criptografar e analisar o trafego SSL em conexões de saída (Outbound)

9.2. Deve identificar, de-criptografar e analisar o trafego SSL em conexões de entrada (Inbound)

9.3. Deve identificar, de-criptografar e analisar o trafego SSH em conexões de saída (Outbound)

9.4. Deve identificar, de-criptografar e analisar o trafego SSH em conexões de entrada (Inbound)

9.5. A inspeção de SSL deve permitir a diferenciação de conexões pessoais (Bancos, Shopping, etc) e tráfegos não Pessoais.

9.6. Deve de-criptografar o trafego em todos os tipos de implementação, como:

9.6.1. Tap mode

9.6.2. Modo Transparente/Bridge

9.6.3. Layer 2

9.6.4. Layer 3

10. Identificação de Usuários.

10.1. Deve suportar pelo menos os seguintes serviços de autenticação para identificação de usuários:

10.1.1. Active Directory

10.1.2. LDAP

10.1.3. eDirectory

10.1.4. RADIUS

10.1.5. Kerberos

10.1.6. Client Certificate

10.2. Deve suportar a criação de politicas baseado em Grupos e Usuários do Active Directory adicionalmente a IP Origem / Destino.

10.3. Deve possibilitar a identificação de usuários sem a necessidade de instalação de agente individualmente em cada equipamento da rede.

10.4. Deve suportar a identificação de usuários em ambientes Citrix e Terminal server, assim como a utilização dos mesmos nas politicas de acesso.

10.5. Deve popular todos os logs de trafego, IPS, URL, Data, Aplicações entre outros com as informações dos usuários.

10.6. Os logs de identificação de usuários deve ser feito RealTime e não correlacionado após a ocorrência do Trafego em questão.

11. Funcionalidades de Rede

11.1. Suportar funcionamento em Tap Mode (Via porta espelhada, Tap ou SPAN port).

11.2. Suportar funcionamento em mode transparente (Bridge ou similar).

11.3. Suportar funcionamento em Layer 2

11.4. Suportar funcionamento em Layer 3

11.5. Suportar a implementação simultânea em todos os modos descritos acima (Tap, Transparente, Layer2 e Layer3) no mesmo equipamento.

11.6. Deve suportar Vlan Tagging (802.1Q) em todas os cenários de implementação acima (Tap, Transparente, Layer2 e Layer3) .

11.7. Deve suportar controle de aplicações em IPV6 em todas os cenários de implementação acima (Tap, Transparente, Layer2 e Layer3).

11.8. Suportar sub-interfaces ethernet logicas.

12. NAT

12.1. Deverá suportar:

12.1.1. Porta/IP Nat dinâmico (Many-to-1 e Many-to-Many).

12.1.2. IP Nat dinâmico (Many-to-Many).

12.1.3. IP Nat estático (1-to-1, Many-to-Many, Ips).

12.1.4. Nat estático bidirecional 1-to-1.

12.2. IP Virtual (VIP)

12.3. Tradução de porta (PAT).

12.4. NAT de Origem

12.5. NAT de Destino

12.6. Suportar NAT de Origem e NAT de Destino simultaneamente.

12.7. Prover capacidade de NAT Traversal, suportando aplicações e Serviços VoIP.

13. VPN

13.1. Suportar VPN Site-to-Site e Cliente-To-Site.

13.2. Suportar IPSec VPN

13.3. Suportar SSL VPN

13.4. Suportar atribuição de Ips nos clientes remotos de VPN.

13.5. Suportar atribuição de DNS nos clientes remotos de VPN.

13.6. Estar licenciada para 2000 clientes de VPN simultâneos.

13.7. IPSec VPN deve suportar:

13.7.1. DES, 3DES, AES

13.7.2. Autenticação MD5 e SHA-1

13.7.3. Diffie-Hellman Group 1 , Group 2 e Group 5

13.7.4. Algoritmo Internet Key Exchange (IKE)

13.7.5. AES 128, 192 & 256 (Advanced Encryption Standard).

13.8. Deve possuir interoperabilidade com os seguintes fabricantes:

13.8.1. Cisco

13.8.2. Checkpoint

13.8.3. Juniper

13.8.4. Palo Alto Networks

13.8.5. Fortinet

13.8.6. Sonic Wall

13.9. O módulo de VPN IPSec deve suportar pelo menos 2.000 túneis e ter performance de pelo menos 500 Mbps de throughput.

13.10. Deverá permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL.

13.11. Deverá contar com um software cliente de VPN-SSL para os sistemas operacionais Windows SP, Vista (32 e 64 bits) e Windows 7 (32 e 64 bits).

13.12. Deverá permitir criar políticas para tráfego VPN-SSL.

13.13. SSL VPN com suporte a proxy arp e uso de interfaces PPPOE.

13.14. Deverá suportar pelo menos 2.000 usuários simultâneos via SSL VPN.

13.15. Suporte para autenticação de VPNs SSL, Ldap, Secure id e base de dados própria.

14. Roteamento

14.1. Deve suportar as seguintes funcionalidades de roteamento:

14.1.1. Estático e Dinâmico.

14.1.2. RIP v2

14.1.3. OSPF

14.1.4. BGP v4

14.1.5. EIGRP

14.2. Suporte a roteamento IPv6.

14.3. Suporte a roteadores Virtuais (Virtual Routers).

14.4. Suporte a "Policy Based Fowarding" por:

14.4.1. Zona de segurança

14.4.2. Endereço de Origem e Destino

14.4.3. Porta de Origem e Destino

14.4.4. Aplicação

14.4.5. Usuários e/ou Grupos da base AD/LDAP

14.4.6. Combinação de todos acima.

15. Alta Disponibilidade

15.1. Configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo:

15.1.1. Em modo Transparente.

15.1.2. Em layer 2

15.1.3. Em layer 3

15.2. O H.A. deve sincronizar:

15.2.1. Todas as sessões.

15.2.2. Certificados de-criptogafados

15.2.3. Todas Associações de Segurança das VPNs

15.2.4. Todas as assinaturas de Antivírus, Anti-spyware e Aplicações.

15.2.5. Todas as configurações

15.2.6. Tabelas FIB.

15.3. O H.A. deve possibilitar tracking de IP

15.4. Monitoração de falha de link.

16. Suporte à Segurança nos equipamentos host da instituição

16.1. Deverá suportar um agente que quando instalado nos equipamentos desktop ou laptop da instituição, transportem as políticas e todas as características de segurança do Firewall a tal equipamento.

16.2. O Agente de software a ser instalado nos equipamentos desktop e laptops, deverá ser capaz de ser distribuído de maneira automática via SMS, Active Directory e ser descarregado diretamente desde o seu próprio portal, o qual residirá no Firewall.

16.3. O agente deverá comunicar-se com o portal para determinar as políticas de segurança do usuário,

16.4. Deverá Manter uma conexão segura com o portal durante a sessão.

16.5. Determinar o perfil de host com base em: Sistema Operacional e seus níveis de instalação de patches, versão de anti-malware no host, versão de Firewall no host, criptografia do disco, chaves de registros e processos ativos.

16.6. Deverá ser possível a criação de perfis customizados com base em Sistema Operacional e seus níveis de instalação de patches, versão de anti-malware no host, versão de Firewall no host, criptografia do disco, chaves de registros e processos ativos.

16.7. O portal deverá enviar ao agente a lista de portais trabalhando como gateways ativos, os quais serão administrados centralmente e deverá trabalhar com os certificados de autenticação correspondentes a cada usuário. O cliente poderá encontrar a melhor rota com base nos gateways disponíveis e a localização do host, determinando a rota com o tempo de resposta mais rápido.

16.8. Em conformidade com o perfil de segurança detectado, se o end-point não for suficientemente seguro, serão determinadas políticas de segurança novas com base no seu perfil. Estas políticas estarão baseadas em: Sistema Operacional e seus níveis de instalação de patches, versão de anti-malware no host, versão de Firewall no host, criptografia do disco, chaves de registros e processos ativos.

16.9. Deverá estabelecer um túnel VPN-SSL do cliente ao Gateway, fornecendo uma solução de single-sign-on aos usuários, integrando-se com as ferramentas de Windows-login.

16.10. Deverá ter suporte para os sistemas operacionais Windows SP, Vista (32 e 64 bits) e Windows 7 (32 e 64 bits).

17. Requerimentos de Hardware e Performance, cada unidade da solução.

17.1. O equipamento deve possuir:

17.1.1. 12 interfaces 10/100/1000 Copper Ethernet

17.1.2. 8 Interfaces 1GB SFP

17.2. O equipamento deve possuir interface “Out-Of-Band” dedicada para gerenciamento.

17.3. Suportar pelo menos 4 Gbps de throughput para Firewall.

17.4. Suportar pelo menos 2 Gbps de throughput para controle de aplicações.

17.5. Suportar pelo menos 2 Gbps de throughput para controle de Anti-virus e Antispyware.

17.6. Suportar pelo menos 2 Gbps de throughput de IPS.

17.7. Suportar pelo menos 500 Mbps de throughput para VPN IPSec.

17.8. Suportar pelo menos 2 Gbps de throughput para as funcionalidades de Firewall, Controle de Applicações, IPS, Anti-virus e Anti-Spyware habilitados simultaneamente.

17.9. Deve suportar pelo menos 500.000 sessões concorrentes.

17.10. Deve suportar pelo menos 50.000 novas sessões por segundo.

17.11. Deve suportar pelo menos 2.000 Interfaces Tunel de VPN IPSec

17.12. Suportar pelo menos 2.000 Usuários concorrentes de SSL VPN.

17.13. Deve suportar pelo menos 5 Sistemas Virtuais (Contextos).

18. Gerenciamento

18.1. Deve ser suportado o gerenciamento por:

18.1.1. CLI via SSH

18.1.2. WebUI via HTTPS

18.1.3. Console

18.1.4. API Aberta

18.2. O gerenciamento local do equipamento deve permitir/Possuir:

18.2.1. Criação e administração de politicas

18.2.2. Administração de políticas de IPS, Anti-virus e Anti-Spyware

18.2.3. Politica de Filtro de Dados e Filtro de URLs.

18.2.4. Monitoração de logs.

18.2.5. Ferramentas de investigação de logs

18.2.6. Debugging

18.2.7. Captura de pacotes.

18.3. Deverá suportar solução de gerenciamento centralizado, possibilitando o gerenciamento de diversos equipamentos.

18.4. O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o trafego que passar pelos gateways de segurança.

18.5. Deverá possuir relatórios de utilização dos recursos por aplicações, URL, Ameaças, etc.

18.6. Prover uma visualização sumarizada de todas as aplicações, ameaças e URLs que passaram pela solução.

18.7. Deverá possuir mecanismo "Drill-Down" para navegação nos relatórios RealTime.

18.8. Nas opções de "Drill-Down", ser possível identificar o usuário que fez determinado acesso.

18.9. Deverá ser possível exportar os logs CSV.

18.10. Deverá ser possível acessar o equipamento a aplicar configurações durante momentos onde o trafego é muito alto e a CPU e memória do equipamento estiver totalmente utilizada.

18.11. Deverá ser possível capturar as URLs acessadas para todas as sessões HTTP.

18.12. Deverá possibilitar a criação de diferentes profiles de administração separando pelo menos: Leitura, Alterações, Relatórios e Monitoração.

18.13. Deverá ser possível de forma granular, assinar permissões para os administradores criarem outros usuários, alterarem configurações, Ler configurações, etc.

18.14. Deverá ser possível administrar o firewall localmente ou remotamente sem causar problemas de sincronismo de configurações.

18.15. Deverá possuir interface ethernet "Out-of-Band" para gerenciamento:

18.15.1. SSH

18.15.2. HTTPS

18.16. Gerar alertas automáticos via:

18.16.1. email

18.16.2. SNMP

18.16.3. syslog

18.17. Habilidade de upgrade via SCP, TFTP e Web-UI.

18.18. Suportar Rollback de configuração para a ultima configuração salva.

18.19. Suportar Rollback de Sistema Operacional para a ultima versão local.

18.20. Validação de regras antes da aplicação.

18.21. Possibilitar o bloqueio da interface para alterações, evitando o conflito de configurações entre administradores quando tiver mais de um administrador executando alterações simultaneamente.

18.22. Deve possibilitar a visualização e comparação de configurações Atuais, configuração anterior e configurações antigas.

18.23. Deve possibilitar a integração com outras soluções de SIEM de mercado (third-party SIEM vendors)

18.24. Controle sobre todos os Firewalls em uma única console, com administração de privilégios ou funções.

18.25. O gerenciamento centralizado deve possibilitar a instalação como virtual appliance sobre VMware, fornecendo a flexibilidade para instalar-se em diferentes combinações de Hardware e sistemas operacionais.

18.26. Administração baseada em Web e Linha de comandos.

18.27. Deverá suportar autenticação de administradores usando base de dados local e Radius.

18.28. Linha de comandos mediante SSHv2, telnet

18.29. Geração de relatórios de atividades do usuário.

18.30. Controle Global de Políticas

18.31. Deve suportar organização em grupos de Firewalls: Os sistemas virtuais serão administrados como dispositivos individuais, os grupos podem ser geográficos, por Funcionalidade (por exemplo, como IPS), e distribuição.

18.32. Objetos e políticas compartidas.

18.33. Relatórios predefinidos e relatórios projetados pelo usuário (custom), todos os relatórios deverão poder ser exportados a formatos CSV e PDF.

19. Autenticação

19.1. Para autenticação dos administradores da solução deve ser suportado:

19.1.1. LDAP

19.1.2. Radius

19.1.3. Soluções Baseadas em Token (i.e. Secure-ID)

19.2. Kerberos

19.3. Para autenticação de VPN SSL deve ser suportado:

19.3.1. LDAP

19.3.2. Radius

19.3.3. Soluções Baseadas em Token (i.e. Secure-ID)

19.3.4. Kerberos

20. Captura de pacotes.

20.1. Deverá ser possível a captura de pacotes por:

20.1.1. Endereço de Origem

20.1.2. Endereço de destino

20.1.3. Aplicações

20.1.4. Aplicações desconhecidas

20.1.5. Portas

20.1.6. IPS

20.1.7. Antivírus

20.1.8. Anti-Spyware

20.1.9. Filtro de dados.

20.1.10. Qualquer combinação acima.

21. Relatórios

21.1. Deverá incluir a capacidade de proporcionar um resumo gráfico de aplicações utilizadas e ameaças encontradas diariamente.

21.2. Deverá permitir o controle de transferência de dados não autorizados com ferramenta para realizar padrões definidos por usuário.

21.3. Deverá contar com a funcionalidade para exportação de logs, captura de tráfego URL e ameaças.

21.4. Deverá permitir a criação de relatórios personalizáveis.

21.5. Deverá contar com ferramenta para criar filtros de monitoramento das sessões históricas no firewall seja por aplicação, ip origem e ip destino.

21.6. Deverá ter a capacidade de gerar um relatório gráfico que permita visualizar as mudanças na utilização de aplicações na rede no que se refere a um período de tempo anterior, para permitir comparar os diferentes consumos realizados pelas aplicações no tempo presente com relação ao passado.

21.7. Geração de relatórios com mapas geográficos gerados em tempo real para a visualização de origens e destinos do tráfego gerado na instituição.

21.8. O equipamento deverá proporcionar os seguintes conjuntos de relatórios:

21.8.1. Utilização de largura de banda de entrada e saída por aplicação (TOP 10)

21.8.2. Numero de Sessões por aplicação (TOP 10)

21.8.3. Comparativo semanal de aplicações utilizadas na rede que possam induzir Latência. (TOP 10)

21.8.4. Taxa de transferência (em bytes) por aplicação (TOP 10).

21.8.5. Origem e destino do tráfego por aplicação – Usuário (TOP 10)

21.8.6. Sessões e E-mail público

21.8.7. Utilização de navegação

21.8.8. Eventos / Ataques por: Origem, Categoria, Ameaça, Protocolo. (TOP 10)

21.8.9. Nível de risco da rede

21.8.10. Principais protocolos e aplicações que circulam pelo Firewall (TOP 25).

21.8.11. Principais endereços de IP destino por protocolo (TOP 25).

21.8.12. Os principais endereços IP para cada um dos protocolos e aplicações principais (TOP 50);

ESPECIFICAÇÃO DOS SERVIDORES

1 SERVIDORES

Quantidade: 02 unidades

1.1 Deverá ser entregue o total de 2 (dois) servidores de produção para o ambiente virtualizado, contendo as características mínimas:

1.1.1 Microcomputador do tipo servidor rack, com tecnologia Octa-Core ou superior, compatível com o padrão x86 e desenvolvido para servidores, com, no mínimo, 2 (dois) discos rígidos SAS, unidade gravadora de DVD.

1.1.2 O servidor deverá possuir fonte redundante com, no mínimo, dois cabos de alimentação ou sistema que garanta a conexão em duas fases de energia elétrica distintas, com comprimento mínimo de 1,80m;

1.1.3 O servidor deverá possuir interface SVGA, ou superior que garanta resolução mínima de 1280x1024;

1.1.4 O servidor deverá possuir registro no Windows Server Catalog – WSC na categoria Hardware para Windows Server 2008 ou superior.

1.1.5 O servidor deverá possuir plena compatibilidade com sistema operacional Linux Debian com o kernel 2.6.24.6 ou superior.

1.1.6 O servidor deverá possuir ventilação redundante tipo “Hot Swap”

1.1.7 O servidor e seus componentes eletro-eletrônicos deverão possuir conformidade comprovada com a diretiva RoHS (Restriction of Hazardous Substances).

1.1.8 Performance

1.1.8.1 O servidor deverá ter índice de, no mínimo, 260 pontos de SPECint2006rate_base, medidos pelo SPEC.org.

1.1.8.2 Não serão aceito servidores com processadores diferentes dos processadores auditados.

1.2 GABINETE

1.2.1 Gabinete rack com botão Liga/Desliga, LEDs indicativos de equipamento ativo, acionamento de disco rígido no painel frontal e indicadores de falha no equipamento, padrão 19” com no máximo 1U de altura.

1.2.2 Possuir sistema de fontes de alimentação redundantes hot-plug ou hot-swap, com dispositivo de alerta no caso de falha e com capacidade suficiente para suportar todos os dispositivos internos na configuração máxima admitida pelo equipamento (processadores, placa-mãe, interfaces, discos rígidos, memória RAM e todos os fans);

1.2.3 Possuir sistema de ventilação redundante e hot-plug ou hot-swap adequado para o perfeito funcionamento do equipamento, conforme recomendações do fabricante do processador, o sistema devera ter a capacidade de alterar a rotação dos ventiladores conforme a necessidade, visando a economia energia;

1.2.4 Possuir baia instalada internamente ao servidor, mas com acesso externo, que permita a utilização de, no mínimo, 8 (oito) discos rígidos Hot-Swap ou hot plug;

1.2.5 Não possuir “cantos vivos”, arestas ou bordas, internas ou externas, que sejam cortantes;

1.2.6 O servidor deverá permitir a abertura sem a necessidade da utilização ferramentas.

1.3 PROCESSADOR

1.3.1 Possuir, no mínimo, 2 processadores padrão x86 com tecnologia Octa-Core ou superior e desenvolvido para servidor, com tecnologia QPI – Quick Patch Interconnect ou similar;

1.3.2 Confeccionado com tecnologia de 32nm;

1.3.3 Possuir freqüência de clock igual ou superior a 2,0Ghz;

1.3.4 Possuir potência de dissipação máxima de 60W(rms) por socket;

1.3.5 Possuir FAN Intelligent System ou tecnologia similar, que possibilite alta dispersão térmica e seja auxiliado por ventilação forçada do gabinete para garantir a vida útil do processador bem como dissipador de alta dispersão calórica, implementados de acordo com as recomendações do fabricante do processador;

1.3.6 Suporte a SMP (multiprocessamento simétrico);

1.3.7 Possuir barramento interno de, no mínimo, 5.86 GT/s.

1.3.8 Possuir recursos para virtualização de I/O e de CPU.

1.3.9 Suporta as tecnologias: SSE 4.2 (Streaming SIMD Extensions 4), AES (Advanced Encryption Standard).

1.3.10 Suporta memórias com até 1333MHz de frequência.

1.4 PLACA PRINCIPAL

1.4.1 Memória RAM instalada, no mínimo, 64 (sessenta de quatro) Gigabytes em pentes de 8 (oito) Gigabytes, ou maiores, com arquitetura DDR3, freqüência de operação mínima de 1333Mhz e consumir no máximo 1.35 V cada.

1.4.2 Permitir a expansão da memória RAM a, no mínimo, 256 (duzentos e cinquenta e seis) Gigabytes sem a necessidade de troca de componentes;

1.4.2 Possuir sistemas de proteção a memória com suporte a: Error Correcting Code –ECC, memory Spare, memory mirroring, Advanced ECC ou chipkill;

1.4.3 Possuir, no mínimo, 12(doze) slots compatíveis com a memória ofertada;

1.4.4 Disponibilidade de, no mínimo, 1 (um) slot de expansão padrão PCI-e (PCI Express) Gen 2 com barramento x16 ou superior, livre após a instalação de todos os dispositivos;

1.4.5 Possuir 1 (uma) interface para conexão de teclado com conector padrão PS/2 fêmea ou USB;

1.4.6 Possuir 1 (uma) interface para conexão de mouse padrão PS/2 fêmea ou USB;

1.4.7 Possuir, no mínimo, 2 (duas) saídas com conector tipo DB15 para monitor;

1.4.8 Interface de vídeo compatível com padrão SVGA, ou superior, embutida, com pelo menos 16(dezesseis) Megabytes de memória de vídeo e interface de interconexão com a placa no padrão PCI Express ou tecnologicamente superior;

1.4.9 Possuir, no mínimo, 1 (uma) interface serial com conector tipo DB-9;

1.4.10 Possuir, no mínimo, 4 (quatro) interfaces USB (Universal Serial BUS) padrão 2.0 ou superior;

1.4.11 Não serão aceitas interfaces USB instaladas por meio de Placas de expansão de portas ou qualquer outro tipo de interface que não seja nativa do equipamento;

1.4.12 Possuir recurso tecnológico integrado que garanta que o servidor seja automaticamente reinicializado em caso de instabilidade grave do sistema (como por exemplo travamento devido a memory leak, overclocking, instabilidade elétrica, falha de processador etc).

1.5 BIOS

1.5.1 Bios do fabricante;

1.5.2 Tipo flash EPROM (atualizável por software);

1.5.3 Senha de acesso ativada e desativada via setup;

1.5.4 Relógio não-volátil.

1.6 UNIDADE DE DISCO RÍGIDO

1.6.1 Possuir, no mínimo, 2 (dois) discos com tecnologia Serial Attached SCSI - SAS (todos idênticos) de, no mínimo, 300 (trezentos) Gbytes cada e dimensões máximas de 2,5'', compatíveis com a controladora SAS cotada com o equipamento;

1.6.2 Cada unidade de disco utilizada deve possuir:

1.6.2.1 Rotação de, no mínimo, 10.000 RPM

1.6.2.2 Interface SAS 6(seis) Gb/s;

1.6.2.3 Taxa de transferência externa mínima de 600 (seissentos) MB/s;

1.6.2.4 Montagem interna ao gabinete do servidor, em baia específica de 2,5” cada;

1.6.2.5 Cabo de comunicação entre o disco rígido e a controladora SAS cotada com o equipamento.

1.6.2.6 Possuir facilidade hot swap.

1.7 CONTROLADOR SAS

1.7.1 Possuir, no mínimo, 1 (um) controlador SAS com processador embarcado;

1.7.2 Compatível com os padrões RAID 0, RAID 1, RAID 0+1 , RAID 5 , RAID 6 e RAID 60 por hardware;

1.7.3 Oferecer detecção e recuperação automática de falhas e reconstrução transparente do RAID;

1.7.4 Memória cache de, no mínimo, 512 (quinhentos e doze) MB, com sistema de proteção ECC e servida por bateria;

1.7.5 Operar com taxa de transferência de, no mínimo, 6(seis)Gbit/s;

1.7.6 Operar comunicação no modo Full Duplex;

1.7.7 Possuir suporte a “hot-swap”e“hot-spare”;

1.7.8 Ser totalmente compatível com os discos ofertados;

1.7.9 Suportar, no mínimo, 8 (oito) unidades de disco;

1.8 UNIDADE GRAVADORA DE DVD/CD

1.8.1 Capacidade de gravação de DVD-R e DVD-RW de camada dupla;

1.8.2 Velocidade de gravação de DVD-R de no mínimo 8x para DVD-R de camada dupla;

1.8.3 Velocidade de gravação de DVD+RW de no mínimo 8x;

1.8.4 Interface SATA ou superior.

1.9 INTERFACES

1.9.1 Possuir, no mínimo, 4 (quatro) portas padrão Gigabit Ethernet (100-1000BASE-TX), com as seguintes características:

1.9.1.1 Operar comunicação no modo full-duplex

1.9.1.2 Possuir conector RJ-45 fêmea

1.9.1.3 Possuir barramento PCI, ou superior, de 64 bits e 100 MHz

1.9.1.4 Compatível com o padrão IEEE 802.3

1.9.1.5 Leds indicadores de link ativo e de tráfego;

1.9.1.6 Permitir a configuração via software (jumperless);

1.9.1.7 Oferecer opção de configuração automática da interface (auto-sense);

1.9.1.8 Compatível com Plug & Play;

1.9.1.9 Suporte ao gerenciamento SNMP;

1.9.1.10 Possuir software de diagnóstico, capaz de identificar o funcionamento correto dos componentes;

1.9.1.11 Suporte a Wake UP on LAN;

1.9.1.12 Suporte a PXE;

1.9.1.13 Permitir balanceamento de carga;

1.9.1.14 Permitir Link Aggregation;

1.9.1.15 Possuir fail-over automático;

1.9.1.16 Suporte a TOE;

1.9.1.17 Suporte aos protocolos: 802.1q (VLAN tagging), 802.3x (flow control), 802.3ad (LACP);

1.10 INTERFACE DE VÍDEO

1.10.1 Possuir, no mínimo, 16 MB de memória de vídeo com interface PCI Express compatível com o padrão SVGA ou tecnologicamente superior;

1.10.2 Capacidade para trabalhar com resolução de 1280x1024;

1.11 FONTE DE ALIMENTAÇÃO

1.11.1 O servidor devera possuir, no mínimo, duas fontes redundantes que suporte o servidor em sua capacidade máxima.

1.11.2 Devem ser de, no máximo, 800w.

1.11.3 As fontes devem alternar entre 110 e 220W automaticamente.

1.12 SOFTWARE DE GERENCIAMENTO

1.12.1 Todos os servidores devem ser fornecidos com uma solução completa de hardware e software para gerenciamento remoto de sistemas, com todas as funcionalidades habilitadas para pleno gerenciamento remoto dos equipamentos, com no mínimo as seguintes características:

1.12.1.2 Possui microprocessador e memória próprios;

1.12.1.3 Possuir conexão que permita o acesso à console do equipamento através da rede. Esta conexão deve possuir 1 (uma) interface 10/100Mbits/s, ou superior, exclusiva;

1.12.1.4 Possuir acesso a console através de HTTPS ou software proprietário, possuindo usuário e senha de conexão, com criptografia de dados trafegados;

1.12.1.5 Permitir gerenciar e monitorar remotamente o sistema, mesmo quando ele estiver fora do ar;

1.12.1.6 Gerenciar servidores remotamente de qualquer lugar por meio de uma conexão IP;

1.12.1.7 Permitir instalação de software de qualquer lugar, por meio de uma conexão IP, de forma criptografada;

1.12.1.8 Possuir console de vídeo contínuo independente de SO que capture a última tela e acompanhe a reinicialização do servidor;

1.12.1.9 Permitir monitorar o status do servidor remoto durante uma reinicialização;

1.12.1.10 Permitir autenticação e autorização do Active Directory para melhor segurança;

1.12.1.11 Possuir a capacidade de reiniciar um servidor desligado e desligar um servidor remotamente;

1.12.1.12 Permitir autoridade baseada em funções através da atribuição de permissões para diferentes tarefas de gerenciamento de sistemas;

1.12.1.13 Possui a funcionalidade de emitir alertas para problemas potenciais de nós gerenciados por meio de mensagens de e-mail ou SNMP;

1.12.1.14 Possui analise de pré-falha por hardware para, pelo menos, processador, memórias e discos;

1.12.1.15 O software deve ter a capacidade de monitora e controla o consumo de energia do servidor, com possibilidade de se estabelecer limites para o servidor;

1.12.1.16 Permitir o deployment de sistema operacional para um grupo de servidores;

1.12.1.17 Permitir trabalhar com ambientes e ferramentas virtualizados, incluindo Microsoft Virtual Server, VMware e virtualização Xen executando funcionalidades como descoberta de máquinas virtuais, inventário , topologia, monitoração da saúde dos servidores virtuais, operações de ligar e desligar, realocação e thresholds;

1.12.1.18 Permitir a visualização dos sistemas de acordo com a VLAN; Coleta e visualização dos componentes de network virtuais ou físicos; Suporte as soluções dos principais fabricantes de mercado Qlogic, Brocade, Cisco e Juniper;

1.12.2 Caso seja necessário software proprietário, este deve ser entregue em quantidade suficiente para administrar todos os servidores fornecidos e com todas as funcionalidades habilitadas;

1.13 SOFTWARE DE VIRTUALIZAÇÃO

1.13.1 Deverá ser fornecido licenciamento VMware vSphere 5.1 Essentials Plus para a capacidade total do servidor.

1.13.2 Deve possuir suporte 9x5 e direito a atualizações por 3 (três) anos direto pelo fabricante da solução, não sendo aceito licenciamento em regime de OEM.

ESPECIFICAÇÃO DO STORAGE

Quantidade: 01 unidades

1. Controladoras

1.1. Possuir controladora redundante, sendo que a falha de uma das controladoras não acarrete interrupção ou degradação dos serviços, sendo capaz de suportar a capacidade máxima de discos suportada pelo equipamento;

1.2. Suportar no mínimo os padrões RAID 0, 1, 5, 6 e 10;

1.3. Permitir reconstrução transparente do RAID sem necessidade de reiniciar o equipamento;

1.4. Suportar reconfigurações dinâmicas, inclusão de LUN, assinalamento de HOST, sem necessidades de parada dos demais serviços

1.5. O equipamento deverá permitir a adição de gavetas e serviços sem parada do equipamento

2. Cache

2.1. Possuir memória cache líquido, isto é, disponível para aplicativos de, no mínimo, 4 GB por controladora, espelhado entre as controladoras, que garanta integridade dos dados presentes na memória e ainda não gravados em disco, em caso de falha de uma das controladoras ou falta súbita de energia;

2.2. As soluções protegidas por bateria deverão ter autonomia mínima de 24 (vinte e quatro) horas, exceção feita às tecnologias que tenham autonomia interna suficiente para efetuar a gravação dos dados presentes na memória em disco ou Flash Drive e posterior desligamento do equipamento, mesmo em caso de falta súbita de energia;

2.3. Recurso que garanta que os dados residentes no cache sejam salvos para uma unidade “Flash Drive” ou em discos rígidos, em caso de falta de alimentação elétrica;

2.4. Expansível a, no mínimo, 8GB por controladora, sem que seja necessária a aquisição de novas controladoras ou clusterização;

2.5. Possuir nativamente pelo menos 8 (oito) interfaces externas (front-end) para conexão à SAN, padrão Fibre Channel de 8 Gbps;

2.6. Possuir no mínimo 4 (quatro) interfaces externas (front-end) para conexão à SAN, padrão iSCSI de 1 Gbps;

3. Capacidade de armazenamento e unidades de disco

3.1. Suportar recurso de hot-spare para as unidades de disco rígido, ou seja, havendo falha de qualquer disco em determinado array/gaveta, o sistema deverá substituir, automaticamente, o disco defeituoso pelo disco spare;

3.2. Os discos deverão ser hot-plug/hot-swap;

3.3. Permitir a instalação de discos com capacidades diferentes, dentro da mesma gaveta de discos (enclosure);

3.4. Possuir capacidade instalada inicial de:

3.4.1. 12 (doze) unidades de disco padrão SAS de 6 Gbps com capacidade bruta mínima individual de 900 GB e velocidade rotacional de 10k RPM;

3.4.2. Capacidade de expansão da quantidade de discos instalada a um total de, pelo menos, 120 (cento e vinte) discos, através da simples adição de gavetas de expansão de capacidade;

4. Alimentação e Ventilação

4.1. Possuir fontes de alimentação e sistema de ventilação redundante e tipo “hot-swap”, que mantenham o equipamento em operação integral, sem prejuízo do desempenho, em caso de falha de uma das fontes ou ventiladores, quaisquer que sejam a temperatura e a tensão de alimentação, respeitados os limites máximos e mínimos de operação;

4.2. As fontes de alimentação deverão operar na faixa de 100 a 240 Volts, 60 Hz, com seleção automática;

5. Funcionalidades e Gerenciamento

5.1. Possuir software(s) para monitoração, controle, gerenciamento e configuração do storage através de interface única, com as seguintes funções:

5.1.1. Permitir o envio de mensagens de e-mail ao administrador em caso de falhas;

5.1.2. Permitir o envio de mensagens de e-mail ao suporte técnico do fabricante do equipamento em caso de falhas – sendo que o atendimento de suporte técnico deve ser oferecido em idioma português;

5.1.3. Permitir a criação e configuração, através do software de gerenciamento, de RAID groups e volumes lógicos (LUNs);

5.1.4. Permitir a adição de capacidade de armazenamento e expansão de volumes de forma dinâmica;

5.1.5. Permitir a configuração de LUN Masking, LUN Partitioning ou similar, ou seja, restringir o acesso a determinado volume lógico (LUN) para um servidor ou conjunto de servidores, físicos ou virtuais (VMware);

5.1.6. Permitir o envio de alertas SNMP para uma console de gerenciamento centralizada;

5.1.7. Deve permitir gerar registros para todos os eventos relacionados ao storage, sejam eles de falhas ou configurações;

5.2. Além do software gerenciamento, devem ser incluso os seguintes software / facilidades abaixo, licenciados para a capacidade total instalada, e com o mesmo prazo manutenção/garantia do hardware ofertado;

5.2.1. Permitir a realização de cópias instantâneas (snapshots / flashcopy) de volumes online em tempo real e cópias completas do volume (full copy), sendo que estas funcionalidades deverão estar licenciadas para a capacidade total de armazenamento suportada pelo equipamento;

5.2.2. Permitir o provisionamento nativo da capacidade realmente utilizada pelos aplicativos e usuários através de funcionalidade de thin provisioning, sendo que esta funcionalidade deverá ser licenciada para a capacidade total de armazenamento suportada pelo equipamento. Não será aceita a implementação da funcionalidade através de equipamentos externos.

5.2.3. Deverá possuir a capacidade de realizar a migração de dados de sistemas de armazenamento (storages), do mesmo fabricante do equipamento ofertado e de outros fabricantes do mercado, para a área interna do sistema de armazenamento ofertado, de forma transparente. Caso o equipamento ofertado não possua a funcionalidade solicitada de forma nativa, deverão ser fornecidos juntamente com a solução os equipamentos e softwares necessários a essa finalidade;

5.2.4. Deverá permitir a implementação futura de tecnologia que possibilite a movimentação automática e nativa dos dados mais ativos no Storage para discos de estado sólido (SSD), com o objetivo de aumento de desempenho. Não será aceita a implementação da funcionalidade através de equipamentos externos;

5.2.5. Permitir o espelhamento de volumes em diferentes gavetas de armazenamento de dados com o objetivo do aumento da disponibilidade em caso de falha da gaveta, sendo que essa funcionalidade deverá ser licenciada para a capacidade total suportada pelo equipamento;

5.2.6. Permitir o monitoramento de desempenho em tempo real do sistema das seguintes métricas: % de utilização de portas; % de utilização de processadores; taxas de I/O; taxas de transferência (MB/seg), e Latência;

5.2.7. Incluir drives de multipathing do próprio fabricante para a quantidade de hosts/servidores suportada pelo equipamento.

5.2.8. Suportar integração com VMware vStorage API for Array Integration (VAAI), suportar gerenciamento via VMWare vCenter, e suportar Recuperação de Desastres com VMWare SRM, sendo que esta funcionalidade deverá ser licenciada para a capacidade total de armazenamento suportada pelo equipamento;

5.2.9. O software de gerenciamento deverá estar licenciado para a capacidade total de armazenamento suportado pelo equipamento;

5.2.10. Todos os softwares envolvidos deverão ser fornecidos na modalidade de licenciamento perpétuo;

6. Características Gerais

6.1. O equipamento deverá ser fornecido com todos os elementos necessários para sua correta fixação em rack padrão 19” (trilhos, parafusos...) bem como cabos de alimentação;

6.2. 04 (quatro) cordões óticos de 05 (cinco) metros de comprimento ou superior, com conectores do tipo LC-LC;

7. Compatibilidade

8.1 O Storage deverá suportar, no mínimo os Sistemas Operacionais Microsoft Windows 2008, Linux Red Hat 3, 4 e 5 e VMWare ESX 5.1;

8.2 A Solução de Storage deverá comprovar compatibilidade com a API do Vmware VAAI (vSphere APIs for Array Integration).

8.3 Comprovação de que o fabricante do equipamento ofertado deverá ser participante do SNIA (Storage Networking Industry Association), na qualidade de "Large Voting Member", com comprovação através do site: http://www.snia.org/member_com/member_directory/ e aderente ao GSI (Green Storage Initiative), com comprovação no site http://www.snia.org/forums/green/. Cópia do documento comprovando tal informação deverá estar contida na proposta.

8.4 Deverá ser compatível com as normas estabelecidas pela SNIA (Storage Networking Industry Association) e prover interface de gerenciamento de acordo com o padrão SMI-S (Storage Management Initiative Specification) versão 1.2 ou superior, para gerenciamento do ambiente através de ferramentas de gerência de infra-estrutura de armazenamento que utilizem esse padrão. A conformidade poderá verificada através de consulta ao site oficial do SNIA Interoperability Conformance Test Program (SNIA-CTP) http://www.snia.org/ctp/conformingproviders/index.html

9. Rede SAN (Storage Area Network)

9.1. Deverá ser entregue o total de 2 (dois) switches iscsi para interligação dos equipamementos (storage e servidores) na rede de armazenamento de dados , contendo as características mínimas do Switch de Acesso - Tipo 02 especificado em item anterior:

ESPECIFICAÇÃO DO RACK E NOBREAKS

1. Para acomodação física dos equipamentos propostos na solução deverá ser disponibilizado 1 (um) rack com as seguintes características mínima:

1.1. Possuir capacidade mínima de 42U de altura.

1.2. Estar de acordo o padrão de 19” polegadas;

1.3. Possuir no mínimo 2 (duas) PDU’s com as seguintes características:

1.3.1. Possuir 8 (oito) conexões AC 110/220v;

1.3.2. Possuir interruptor de carga;

1.3.3. Ser com padrão compatível com os equipamentos e no-breaks que compõe a solução;

1.4. Possuir portas frontal e traseira que permitam o devido fluxo de ar;

1.5. As portas devem possuir opção de bloqueio/fechadura;

1.6. As laterais devem possibilitar remoção no caso de manuseio dos equipamentos;

2. Deverá ser fornecido juntamente com a solução no mínimo 2 (dois) módulos de nobreak com as seguintes características mínimas:

2.1. Possuir montagem padrão de rack 19” e compatível com o rack disponibilizado na solução;

2.2. Possuir tensão de entrada para 220v

2.3. Possuir tensão de saída para 220v;

2.4. Suportar tecnologia de dupla conversão de forma on-line;

2.5. Possibilitar expansões futuras de outros bancos de baterias do mesmo fabricante;

2.6. As baterias devem ser livres de manutenção;

2.7. Deverá ser capaz de suportar toda solução disponibilizada em seu pleno funcionamento pelo período mínimo de 30 (trinta) minutos;

2.8. Capacidade inicial não deverá ser inferior a 3.000 VA

2.9. O fator de eficiência deve ser no mínimo de 95%;

2.10. Possuir interface para gerenciamento e monitoração;

ESPECIFICAÇÃO DO LICENCIAMENTO DE VIRTUALIZAÇÃO E BACKUP

1. Deverá ser fornecido licenciamento de VMware vCenter para gerenciamento dos servidores disponibilizados com VMware vSphere 5.1

1.1. Deve possuir suporte 9x5 e direito a atualizações por 3 (três) anos direto pelo fabricante da solução, não sendo aceito licenciamento em regime de OEM.

2. Software de Backup e replicação

2.1. Deverá ser fornecido licenciamento de software de backup para todo ambiente, contendo as seguintes características mínimas:

2.2. Ser homologado para hypervisor VMware

2.3. Possibilitar a recuperação granular de e-mail em plataforma Microsoft Exchange;

2.4. Permitir configuração de replicação das máquinas virtuais;

2.5. Ser licenciamento de forma perpétua para toda solução disponibilizada;

2.6. Caso o licenciamento seja por capacidade, deve ser considerada a capacidade máxima da biblioteca de fitas disponibilizada na solução;

2.7. Permitir a recuperação granular de servidor de arquivos;

2.8. Possibilitar a recuperação de máquinas virtuais em menos de 5 (cinco) minutos;

2.9. Deve possuir suporte 9x5 e direito a atualizações por 3 (três) anos direto pelo fabricante da solução, não sendo aceito licenciamento em regime de OEM.

2.10 Deverá ser entregue servidor no padrão rack para instalação da solução de backup, possuindo os requisitos mínimos de:

2.10.1. Possuir, no mínimo, 1 processador padrão x86 com tecnologia Six-Core ou superior;

2.10.1.1Possuir freqüência de clock igual ou superior a 2,0Ghz;

2.10.2 Memória RAM instalada, no mínimo, 16 (dezesseis) Gigabytes em pentes de 8 (oito) Gigabytes, ou maiores, com arquitetura DDR3, freqüência de operação mínima de 1333Mhz e consumir no máximo 1.35 V cada.

2.10.3 Permitir a expansão da memória RAM a, no mínimo, 128 (duzentos e cinquenta e seis) Gigabytes sem a necessidade de troca de componentes

2.10.4 Possuir, no mínimo, 6 (seis) discos com tecnologia Serial Attached SCSI - SAS (todos idênticos) de, no mínimo, 300 (trezentos) Gbytes cada e dimensões máximas de 2,5'', compatíveis com a controladora SAS cotada com o equipamento;

2.10.5 Possuir suporte a "hot-swap" e/ou "hot-spare" para discos;

2.10.6 Possuir sistema de fontes de alimentação e fans redundantes hot-plug ou hot-swap, com dispositivo de alerta no caso de falha e com capacidade suficiente para suportar todos os dispositivos internos na configuração máxima admitida pelo equipamento (processadores, placa-mãe, interfaces, discos rígidos, memória RAM e todos os fans);

2.10.7 Possuir, no mínimo, 1 (um) controlador SAS com processador embarcado;

2.10.8 Compatível com os padrões RAID 0, RAID 1, RAID 0+1 , RAID 5 , RAID 6 e RAID 60 por hardware

2.10.9 Deverá ser fornecido licenciamento Windows Server Standard 2008 ou superior para a capacidade total do servidor

2.10.10 Possuir controladora Fibre Channel (HBA) para conexão com a biblioteca de fitas contemplada na solução, no mínimo 2 (dois) canais padrão FC, com velocidade de conexão de 8 (oito) Gbps por canal.

2.10.11 Possuir controladora ethernet para conexão a rede SAN da contemplada na solução, com no mínimo 4 (quatro) portas, com velocidade de conexão gigabit.

2.10.12 As controladora devem ser compatíveis com sistemas operacionais Windows 2008 Server, vMware vSphere 5.1 e com os switchs SAN ofertados na solução.

2.11 Deverá ser entregue biblioteca de fitas interligada no servidor de backup. Esta deve ser no padrão rack para operação da solução de backup, possuindo os requisitos mínimos de:

2.11.1. Suportar, no mínimo, 2 (dois) drive half-height com a tecnologia LTO-5;

2.11.2. Possuir, no mínimo, 24 (vinte e quatro) slots de fitas de dados;

2.11.3. Padrão para instalação em rack de 19” de largura;

2.11.4. Possuir fontes de alimentação com tensão de entrada de 110/220 V e frequência de 60 Hz;

2.11.5. Possuir leitor de código de barras com o objetivo de identificar os cartuchos através das etiquetas;

2.11.6. Possuir drives com padrão de conexão FC;

2.11.7. A unidade de backup deve possuir capacidade de ler, no mínimo, duas gerações anteriores e gravar em uma geração anterior, ou seja, ler LTO-4 e LTO-3 e gravar em LTO-4;

2.11.8. Deverá ser entregue 22 (vinte dois) cartuchos padrão ultrium LTO5 e 2(dois) de cartuchos de limpeza;

2.11.9. Suportar gerenciamento via SNMP;

2.11.10 Suportar gerenciamento da unidade de backup remotamente através de um web-browser, incluindo as principais funções de operação e monitoração local da Biblioteca;

2.11.11. Possuir gerenciamento de erros e status de logs;

2.11.12. Suportar os protocolos de rede IPv6 e IPv4;

2.11.13. A unidade de backup deve ser capaz de:

2.11.14. Monitorar a utilização dos drives e cartuchos;

2.11.15. Reportar informações através de notificação do status do hardware como saúde e vida útil;

Serviço de Manutenção e Suporte

1. Deve possuir atendimento telefônico 0800 em língua portuguesa realizado pela equipe técnica especializada dos fabricante ou prestadora de serviço certificada pelo fabricante em horário comercial na modalidade 8X5, a licitante devera informar o ou os 0800 na proposta.
2. Defeitos em qualquer parte física da unidade incluindo fonte de alimentação e ventiladores;
3. Sistema operacional “IOS ou firmware” onde deve ser disponibilizado acesso direto ao site do fabricante para download de novas versões que contenham correções e/ou atualizações;
4. Suporte e Manutenção dos fabricantes ou empresa licitante, pelo período do contrato com atendimento On-Site, com tempo de atendimento de até 24 horas e solução de problemas pelo período máximo de 48 horas, contadas à partir da abertura do chamado.
5. Caso a solução do problema implique na substituição do equipamento defeituoso, o mesmo será entregue à contratada no momento da instalação do equipamento substituto.
6. A contratada deverá garantir o mais rigoroso sigilo sobre quaisquer dados, informações, documentos e especificações que a ela venham a ser confiados ou que venha a ter acesso em razão dos serviços prestados, não podendo, sob qualquer pretexto, revela-los, divulga-los, reproduzi-los ou dar conhecimento a quaisquer terceiro.
7. Possuir em seu quadro funcional, no mínimo, 01 técnico Certificado na Tecnologia de Rede para design, instalação e administração para switches empilháveis;
8. Autorização para comercialização dos equipamentos e técnico(s) certificados pelo fabricante para realizar a instalação, configuração e suporte técnico da solução ofertada;
9. Banco de horas em horário comercial para atendimento remoto ou caso necessário local/ on-site;
10. Limitado ao período do contrato;

11. Solicitações de complexidade nível 2 e 3;
12. Será disponibilizado acesso remoto sempre que necessário;
13. Contemplar coleta mensal do ambiente para análise e acompanhamento preventivo;

Treinamento:

Deverá ser ministrado treinamento sobre o gerenciamento de toda a nova estrutura e noções básicas de configurações de rotina, compreendendo em evento teórico-prático, customizado para a solução a ser implementada, baseado no acompanhamento, por até 04 (quatro) profissionais, que estarão envolvidos na instalação e configuração da solução.
A carga horária prevista para este treinamento deverá ser de no mínimo 20 (vinte) horas.
Ao final do treinamento, os profissionais destacados deverão ter o conhecimento necessário para instalar, configurar e administrar a solução em questão.
Deverá ser entregue um certificado de participação para os profissionais que completarem o treinamento.