TRIBUNAL REGIONAL ELEITORAL DO RIO GRANDE DO NORTE
SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO
COORDENADORIA DE INFRAESTRUTURA TECNOLÓGICA
SEÇÃO DE REDES E INFRAESTRUTURA

Análise de Viabilidade de Contratação

1 Definição e especificação de requisitos

1.1 Requisitos de negócio

1.1.1 . Garantir o funcionamento adequado da secretaria e suas seções nas novas instalações do prédio sede atualmente em construção no que se refere a equipamentos de infraestrutura de informática e telecomunicação.

1.1.2 . Garantir a interligação lógica entre as estações de trabalho e equipamentos de telecomunicação da nova sede às salas técnicas e entre estas e o *Data Center*, todos localizados no mesmo prédio.

1.1.3 . Prover circuito elétrico estabilizado para os equipamentos de informática e telecomunicação instalados no prédio da nova sede.

1.1.4 . Prover rede de comunicação sem fio aos usuários da instituição segundo a portaria nº 99/2015 GP/TRE-RN.

1.1.1 . Garantir que o *hardware* dos equipamentos adquiridos possuam garantia pelo período de no mínimo 2 anos para *nobreaks*, 3 para equipamentos de *networking* e 1 ano para equipamentos de telefonia VoIP.

1.2 Requisitos Tecnológicos

1.2.1 . Todos os equipamentos devem estar de acordo com o projeto de instalações elétricas e de cabeamento estruturado(rede lógica de dados e de voz) seguindo as normas:

- NBR 14565/ABNT
- NBR 5410/ABNT
- EIA/TIA 568B
- EIA/TIA 569B

1.2.2 . Todos equipamentos de informática e telecomunicação serão ligados a circuito elétrico específico que garanta fornecimento de energia elétrica

Documento assinado digitalmente por:		
Joao Paulo de Araujo Bezerra 23/06/2017 11:43:39	Ernesto Leca Pinto 23/06/2017 11:50:37	Daniel Cesar Gurgel Coelho Ponte 02/08/2017 14:07:01

confiável durante pequenas interrupções de fornecimento da concessionária.

1.2.3 . Todos os equipamentos de informática e telecomunicação se ligarão à rede lógica do prédio através do cabeamento horizontal do espaço de trabalho até os armários de telecomunicação como descrito nas normas de cabeamento estruturado NBR 14565/ABNT e EIA/TIA 568B.

1.2.4 . Todas as estações de trabalho deverão possuir aparelho específico para prover a comunicação por voz entre o servidor alocado nessa estação e as outras unidades ou contatos exteriores ao prédio.

1.2.5 . Ao público com acesso autorizado por norma interna será disponibilizado, em todo o prédio, o acesso à internet através de conexões de rede sem fio protegida por senha de uso particular.

1.3 Análise da demanda

1.3.1 . Dimensionamento circuitos estabilizados

- A demanda estimada baseia-se nas características do projeto elétrico, uma autonomia média de 15 minutos e projeção de crescimento de carga para os próximos 3 anos em 30%.

Sala Técnica	Potência Atual (VA)	Potência Futura (VA)
1	10200	13260
2	4000	5200
3	11000	14300
4	9200	11960
5	12400	16120

1.3.2 . **Necessidade de Aparelhos telefônicos**

- Para cada estação de trabalho um aparelho telefônico deverá ser instalado. A partir do projeto de ambientação, da quantidade de estações atuais na secretaria do tribunal e levando-se em consideração uma projeção de crescimento calculou-se a demanda na tabela a seguir:

Ano	Numero de Usuarios	Numero de Telefones
2017	325	150
2018	350	250
2019	370	350

1.3.3 . **Solução de acesso à rede sem fio**

- A demanda por um sistema de acesso à rede sem fio por parte do público da secretaria exigirá a expansão do atual sistema empregado atualmente por controladora e A*ccess Points*. A partir da análise do projeto chegou-se a seguinte estimativa:

Ano	Público Alvo	Número de Pontos Projetados
2017	325	30
2018	350	36
2019	370	40

1.3.4 . **Equipamentos de interconexão**

- Levando-se em consideração o número de pontos e a distribuição lógica das salas técnicas do projeto de cabeamento estruturado justifica-se utilizar um modelo hierárquico de interconexão.
- A concentração de pontos de interligação na camada de acesso será distribuída entre várias salas técnicas em pavimentos distintos segundo o projeto construtivo. Dessa maneira o número de equipamentos de comutação tende a aumentar.
- Em aparelhos finais que possuam compatibilidade necessária a alimentação elétrica será fornecida pelo switch de acesso no mesmo cabeamento lógico utilizando a tecnologia PoE (Power Over Ethernet)
- A evolução tecnológica atingida na interligação entre a camada de acesso e à camada de núcleo com a utilização de conexões em 10 e 40 Gigabits exige que no CPD seja utilizado equipamentos que possam comportar tais velocidades.
- A tabela a seguir apresenta a demanda calculada a partir da análise do projeto estrutural e de cabeamento estruturado:

Categoria no modelo Hierárquico	Portas Gigabit	Portas 10GE	Portas 40GE
Núcleo	40	40	12
Distribuição	-		14
Acesso	1.200	36	-
Topo de Rack		48	4

1.3.5 . **Equipamento Firewall**

- Atualmente este regional conta com dois links de conexão à internet contratados por meio de dois fornecedores distintos com o objetivo de redundância e tolerância a Falha.
- Há a possibilidade de manter-se o prédio sede atual em funcionamento mesmo após a transferência da secretaria para o novo prédio sede. Essa possibilidade permite que cada link de Internet seja instalado em um prédio distinto.
- Assim mais um equipamento de segurança *firewall* será necessário para a infraestrutura.

1.4 Detalhamento Necessidades Tecnológicas

1.4.1 . Dados os requisitos de negócio elencados, da demanda calculada, análise do projetos elétrico e de cabeamento identifica-se necessidade de equipamentos nas seguintes categorias para atender os requisitos da área demandante :

- **Comutadores (*switches*) -** Classe de equipamentos responsável por interligar logicamente os equipamentos de rede e prover alimentação elétrica em equipamentos PoE (*Power over Ethernet*) para equipamentos tais como câmeras, telefones VoIP e *access points*.

Switch de Núcleo
Quantidade
2
Especificação
1. **Switch Modular - Core** **1.1. Características técnicas mínimas;** 1.1.1. Deve possuir no mínimo 10 slots para módulos de interface; 1.1.2. Deve possuir capacidade de comutação de, no mínimo, 950 Gbps; 1.1.3. Deve possuir capacidade de encaminhamento de, no mínimo, 570 Milhões de pps; 1.1.4. Deve ser fornecido com no mínimo 20 Portas Gigabit Base-T PoE+; 1.1.5. Deve ser fornecido com no mínimo 20 Portas 10GE em SFP+; 1.1.6. Deve ser fornecido com no mínimo 6 Portas 40GE em QSFP+; 1.1.7. Deve ser fornecido com no minimo 8 Portas 1/2.5/5 Gigabit PoE+; 1.1.8. Depois de plenamente instalados os itens 1.1.4,1.1.5,1.1.6 e 1.1.7, deverão restar ainda 5 slots livres para futuras expansões. 1.1.9. Deve ser fornecido com no minimo 15 transceivers 10GE Multimodo LC que suporte pelo menos 300 metros de distância quando uma fibra OM4; 1.1.10. Deve ser fornecido com no minimo 4 transceivers 40GE Multimodo LC que suporte pelo menos 100 metros de distância uando uma fibra OM4; 1.1.11. Serão aceitos transceivers 40GE que usem MPO4, desde que seja fornecidos conectores MPO4 para LC;

Documento assinado digitalmente por:		
Joao Paulo de Araujo Bezerra 23/06/2017 11:43:39	Ernesto Leca Pinto 23/06/2017 11:50:37	Daniel Cesar Gurgel Coelho Ponte 02/08/2017 14:07:01

1.1.12. Deve der fornecido com 01 cabo DAC QSFP+ de 3 Metros;
1.1.13. Deve possuir no mínimo 4 fontes de alimentação internas redundantes 220VAC;
1.2. **Disponibilidade**;
1.2.1. Deve implementar virtualização de chassis, possibilitando que dois chassis distintos possam operar como um único switch no que se refere a comutação e roteamento, podendo ser administrados ainda por um único endereço IP;
1.2.2. Deve permtir a criação de links agregados contendo portas presentes em dois chassis físicos distintos;
1.2.3. A implementação de virtualização de chassis deve permitir que os elementos do conjunto sejam interconectados por interfaces 10 Gigabit Ethernet padrão ou 40 Gigabit Ethernet padrão, com fibra óptica, permitindo o agrupamento de equipamentos geograficamente distantes;
1.2.4. Deve possuir módulos de switch fabric redundantes;
1.2.5. Deve suportar alimentação redundante;
1.3. **Switching**;
1.3.1. Deve implementar o protocolo 802.3X;
1.3.2. Deve implementar registro dinâmico de VLANs (GVRP e MVRP);
1.3.3. Implementar o protocolo Spanning Tree;
1.3.4. Implementar o protocolo Rapid Per-VLAN Spanning Tree (RPVST+);
1.3.5. Deve implementar 4094 VLANs;
1.3.6. Deve implementar VLANs por porta, baseadas em MAC, baseadas em protocolo e subnet IP;
1.3.7. Deve implementar IEEE 802.1Q;
1.3.8. Deve implementar IEEE 802.1ad QinQ;
1.3.9. Deve suportar Jumbo Frames de até 9200;
1.3.10. Deve implementar Jumbo frames nas interfaces Gigabit Ethernet e 10-Gigabit Ethernet
1.3.11. Deve suportar 64.000 entradas na tabela MAC;
1.4. Roteamento
1.4.1. Deve implementar roteamento estático Ipv4;
1.4.2. Deve implementar roteamento estático Ipv6;
1.4.3. Deve implementar os seguintes protocolos de roteamento IPv4: RIPv2, OSPF, e BGP4;
1.4.4. Deve implementar os seguintes protocolos de roteamento IPv6: RIPng e OSPFv3;
1.4.5. Deve implementar o protocolo VRRP;
1.5. Segurança
1.5.1. Deve implementar SSHv2;
1.5.2. Deve implementar 802.1x;
1.5.3. Deve implementar accounting RADIUS;
1.5.4. Deve suportar port-security;
1.6. Gerenciamento
1.6.1. O equipamento ofertado deve permitir múltiplos arquivos de configuração;
1.6.2. Deve suportar espelhamento remoto;
1.6.3. Deve ser fornecido com todas as licenças de software necessárias para o funcionamento integral de todas as funcionalidades disponíveis para o equipamento;
1.6.4. O equipamento ofertado deve possuir certificado de homologação na Anatel, de acordo com a resolução nº 242;
1.7. Garantia e Suporte;
1.7.1. Deve possuir garantia e suporte por 36 meses;
1.7.2. O equipamento proposto deverá possuir garantia do Fabricante de 3 anos para entrega de peças on-site a qual dever ser comprovada mediante documento oficial fabricante;
1.7.3. Não serão aceitos transceivers que não sejam do mesmo fabricante do equipamento;
1.7.4. Os serviços serão solicitados mediante a abertura de um chamado efetuado por técnicos da contratante, via chamada telefônica local, a cobrar ou 0800, e-mail, website ou chat do fabricante ou à empresa autorizada (em português ou inglês – para o horário comercial – horário oficial de Brasília) e constatada a necessidade, o fornecedor deverá providenciar o deslocamento

Documento assinado digitalmente por:		
Joao Paulo de Araujo Bezerra 23/06/2017 11:43:39	Ernesto Leca Pinto 23/06/2017 11:50:37	Daniel Cesar Gurgel Coelho Ponte 02/08/2017 14:07:01

do equipamento, bem como seu retorno ao local de origem sem qualquer ônus ao contratante;

Switch de Distribuição
Quantidade
2
Especificação
1. Switch - Distribuição **1.1. Características técnicas mínimas;** 1.1.1. Deve possuir no mínimo 6 slots para módulos de interface; 1.1.2. Deve possuir capacidade de comutação de, no mínimo, 950 Gbps; 1.1.3. Deve possuir capacidade de encaminhamento de, no mínimo, 570 Milhões de pps; 1.1.4. Deve ser fornecido com no mínimo 20 Portas Gigabit Base-T PoE+; 1.1.5. Deve ser fornecido com no mínimo 12 Portas 10GE em SFP+; 1.1.6. Deve ser fornecido com no mínimo 3 Portas 40GE em QSFP+; 1.1.7. Deve ser fornecido com no mínimo 8 Portas 1/2.5/5 Gigabit PoE+; 1.1.8. Deve ser fornecido com no mínimo 10 transceivers 10GE Multimodo LC que suporte pelo menos 300 metros de distância quando uma fibra OM4; 1.1.9. Deve ser fornecido com no mínimo 2 transceivers 40GE Multimodo LC que suporte pelo menos 100 metros de distância quando uma fibra OM4; 1.1.10. Serão aceitos transceivers 40GE que usem MPO4, desde que sejam fornecidos conectores MPO4 para LC; 1.1.11. Deve ser fornecido com 02 cabos DAC QSFP+ 40GE de no mínimo 3 metros; 1.1.12. Deve ser fornecido com 04 cabos DAC SFP+ 10GE de no mínimo 3 metros; 1.1.13. Deve possuir no mínimo 2 fontes de alimentação internas redundantes 220VAC de pelo 900 Watts cada; **1.2. Disponibilidade;** 1.2.1. Deve implementar virtualização de chassis, possibilitando que dois chassis distintos possam operar como um único switch no que se refere a comutação e roteamento, podendo ser administrados ainda por um único endereço IP; 1.2.2. Deve permitir a criação de links agregados contendo portas presentes em dois chassis físicos distintos; 1.2.3. A implementação de virtualização de chassis deve permitir que os elementos do conjunto sejam interconectados por interfaces 10 Gigabit Ethernet padrão ou 40 Gigabit Ethernet padrão, com fibra óptica,permitindo o agrupamento de equipamentos geograficamente distantes; 1.2.4. Deve possuir módulos de switch fabric redundantes; 1.2.5. Deve suportar alimentação redundante; **1.3. Switching;** 1.3.1. Deve implementar o protocolo 802.3X; 1.3.2. Deve implementar registro dinâmico de VLANs (GVRP e MVRP); 1.3.3. Deve Implementar o protocolo Spanning Tree; 1.3.4. Deve Implementar o protocolo Rapid Per-VLAN Spanning Tree (RPVST+); 1.3.5. Deve implementar 4094 VLANs; 1.3.6. Deve implementar VLANs por porta, baseadas em MAC, baseadas em protocolo e subnet IP; 1.3.7. Deve implementar IEEE 802.1Q; 1.3.8. Deve implementar IEEE 802.1ad QinQ; 1.3.9. Deve suportar Jumbo Frames de 9000 bytes; 1.3.10. Deve implementar Jumbo frames nas interfaces Gigabit Ethernet e 10-Gigabit Ethernet

Documento assinado digitalmente por:		
Joao Paulo de Araujo Bezerra 23/06/2017 11:43:39	Ernesto Leca Pinto 23/06/2017 11:50:37	Daniel Cesar Gurgel Coelho Ponte 02/08/2017 14:07:01

1.3.11. Deve suportar 64.000 entradas na tabela MAC;

1.4. Roteamento

1.4.1. Deve implementar roteamento estático Ipv4;
1.4.2. Deve implementar roteamento estático Ipv6;
1.4.3. Deve implementar os seguintes protocolos de roteamento IPv4: RIPv2, OSPF, e BGP4;
1.4.4. Deve implementar os seguintes protocolos de roteamento IPv6: RIPng e OSPFv3;
1.4.5. Deve implementar o protocolo VRRP;

1.5. Segurança

1.5.1. Deve implementar SSHv2;
1.5.2. Deve implementar 802.1x;
1.5.3. Deve implementar accounting RADIUS;
1.5.4. Deve suportar port-security;

1.6. Gerenciamento

1.6.1. O equipamento ofertado deve permitir múltiplos arquivos de configuração;
1.6.2. Deve suportar espelhamento remoto;
1.6.3. Deve ser fornecido com todas as licenças de software necessárias para o funcionamento integral de todas as funcionalidades disponíveis para o equipamento;
1.6.4. Deve permitir gerenciamento integrado com software de gerência do próprio fabricante.
1.6.5. O equipamento ofertado deve possuir certificado de homologação na Anatel, de acordo com a resolução nº 242;

1.7. Garantia e Suporte;

1.7.1. O equipamento proposto deverá possuir garantia do Fabricante de 36 meses para entrega de peças on-site a qual dever ser comprovada mediante documento oficial fabricante;
1.7.2. Todos os transceivers e cabos devem ser totalmente compatíveis com o equipamento fornecido.
1.7.3. Os serviços serão solicitados mediante a abertura de um chamado efetuado por técnicos da contratante, via chamada telefônica local, a cobrar ou 0800, e-mail, website ou chat do fabricante ou à empresa autorizada (em português ou inglês – para o horário comercial – horário oficial de Brasília) e constatada a necessidade, o fornecedor deverá providenciar o deslocamento do equipamento, bem como seu retorno ao local de origem sem qualquer ônus ao contratante;

Switch de Acesso POE
Quantidade
21
Especificação

1. Switch

1.1. Características técnicas mínimas;

1.1.1. Deve possuir no mínimo 48 portas Switch Gigabit Ethernet 10/100/1000BaseT PoE+;
1.1.2. Deve possuir 4 portas 10 Gigabit Ethernet SFP+;
1.1.3. Deve possuir 1 interface RJ-45 ou serial para acesso console local;
1.1.4. Deve implementar o padrão IEEE 802.3at em todas as interfaces 10/100/1000BaseT;
1.1.5. Deve der fornecido com 01 cabo DAC SFP+ de 3 Metros;
1.1.6. Deve possuir latência de, no máximo, 4 µs;
1.1.7. Deve possuir fonte de alimentação interna 110/220VAC;

1.2. **Disponibilidade**;

1.2.1. Deve possuir capacidade de, no mínimo, 4 (quatro) equipamentos membros da mesma pilha;

1.3. **Switching**;

1.3.1. Deve possuir tabela para 32.000 endereços MAC;
1.3.2. Deve implementar VLANs baseadas em MAC;

Documento assinado digitalmente por:		
Joao Paulo de Araujo Bezerra 23/06/2017 11:43:39	Ernesto Leca Pinto 23/06/2017 11:50:37	Daniel Cesar Gurgel Coelho Ponte 02/08/2017 14:07:01

1.3.3. Deve suportar 4094 VLAN IDs;
1.3.4. Deve implementar registro dinâmico de VLAN com MVRP;
1.3.5. Deve suportar protocolo OpenFlow 1.3;
1.3.6. Deve implementar Jumbo frames nas interfaces Gigabit Ethernet e 10-Gigabit Ethernet
1.3.7. Deve implementar Jumbo frames com tamanho de até 9000 bytes;
1.3.8. Deve implementar Ethernet link aggregation
1.3.9. Deve implementar IEEE 802.1ad QinQ;
1.3.10. Deve implementar agregação de links em modo estático e dinâmico (LACP), com suporte a criação de até 144 grupos.
1.3.11. Deve implementar IEEE 802.3x;
1.3.12. Deve implementar STP BPDU Protection (BPDU Guard);
1.3.13. Deve implementar IEEE 802.1w Rapid Reconfiguration of Spanning Tree;
1.3.14. Deve implementar MSTP IEEE 802.1s com pelo menos 64 instâncias;

1.4. Roteamento

1.4.1. eve implementar roteamento estático Ipv4;
1.4.2. Deve implementar roteamento estático Ipv6;
1.4.3. Deve implementar os seguintes protocolos de roteamento IPv4: RIPv2, OSPF, e BGP4;
1.4.4. Deve implementar os seguintes protocolos de roteamento IPv6: RIPng e OSPFv3;
1.4.5. Deve implementar o protocolo VRRP;

1.5. Segurança

1.5.1. Deve implementar SSHv2;
1.5.2. Deve implementar 802.1x;
1.5.3. Deve implementar accounting RADIUS;
1.5.4. Deve suportar port-security;

1.6. Gerenciamento

1.6.1. O equipamento ofertado deve permitir múltiplos arquivos de configuração;
1.6.2. Deve suportar espelhamento remoto;
1.6.3. Deve ser fornecido com todas as licenças de software necessárias para o funcionamento integral de todas as funcionalidades disponíveis para o equipamento;
1.6.4. O equipamento ofertado deve possuir certificado de homologação na Anatel, de acordo com a resolução nº 242;

1.7. Garantia e Suporte;

1.7.1. O equipamento proposto deverá possuir garantia do Fabricante de 36 meses para entrega de peças on-site a qual dever ser comprovada mediante documento oficial fabricante;
1.7.2. Não serão aceitos transceivers que não sejam do mesmo fabricante do equipamento;
1.7.3. Os serviços serão solicitados mediante a abertura de um chamado efetuado por técnicos da contratante, via chamada telefônica local, a cobrar ou 0800, e-mail, website ou chat do fabricante ou à empresa autorizada (em português ou inglês – para o horário comercial – horário oficial de Brasília) e constatada a necessidade, o fornecedor deverá providenciar o deslocamento do equipamento, bem como seu retorno ao local de origem sem qualquer ônus ao contratante;

Switch de Acesso
Quantidade
23
Especificação
1 Switch **1.1 Características técnicas mínimas;** 1.1.1 . Deve possuir no mínimo 48 portas Switch Gigabit Ethernet 10/100/1000BaseT ;

Documento assinado digitalmente por:		
Joao Paulo de Araujo Bezerra 23/06/2017 11:43:39	Ernesto Leca Pinto 23/06/2017 11:50:37	Daniel Cesar Gurgel Coelho Ponte 02/08/2017 14:07:01

1.1.2 . Deve possuir 4 portas 10 Gigabit Ethernet SFP+;
1.1.3 . Deve possuir 1 interface RJ-45 ou serial para acesso console local;
1.1.4 . Deve implementar o padrão IEEE 802.3at em todas as interfaces 10/100/1000BaseT;
1.1.5 . Deve der fornecido com 01 cabo DAC SFP+ de 3 Metros;
1.1.6 . Deve possuir latência de, no máximo, 4 µs;
1.1.7 . Deve possuir fonte de alimentação interna 110/220VAC;

1.2 **Disponibilidade**;
1.2.1 . Deve possuir capacidade de, no mínimo, 4 (quatro) equipamentos membros da mesma pilha;

1.3 **Switching**;
1.3.1 . Deve possuir tabela para 32.000 endereços MAC;
1.3.2 . Deve implementar VLANs baseadas em MAC;
1.3.3 . Deve suportar 4094 VLAN IDs;
1.3.4 . Deve implementar registro dinâmico de VLAN com MVRP;
1.3.5 . Deve suportar protocolo OpenFlow 1.3;
1.3.6 . Deve implementar Jumbo frames nas interfaces Gigabit Ethernet e 10-Gigabit Ethernet
1.3.7 . Deve implementar Jumbo frames com tamanho de até 9000 bytes;
1.3.8 . Deve implementar Ethernet link aggregation
1.3.9 . Deve implementar IEEE 802.1ad QinQ;
1.3.10 . Deve implementar agregação de links em modo estático e dinâmico (LACP), com suporte a criação de até 144 grupos.
1.3.11 . Deve implementar IEEE 802.3x;
1.3.12 . Deve implementar STP BPDU Protection (BPDU Guard);
1.3.13 . Deve implementar IEEE 802.1w Rapid Reconfiguration of Spanning Tree;
1.3.14 . Deve implementar MSTP IEEE 802.1s com pelo menos 64 instâncias;

1.4 Roteamento
1.4.1 . eve implementar roteamento estático Ipv4;
1.4.2 . Deve implementar roteamento estático Ipv6;
1.4.3 . Deve implementar os seguintes protocolos de roteamento IPv4: RIPv2, OSPF, e BGP4;
1.4.4 . Deve implementar os seguintes protocolos de roteamento IPv6: RIPng e OSPFv3;
1.4.5 . Deve implementar o protocolo VRRP;

1.5 Segurança
1.5.1 . Deve implementar SSHv2;
1.5.2 . Deve implementar 802.1x;
1.5.3 . Deve implementar accounting RADIUS;
1.5.4 . Deve suportar port-security;

1.6 Gerenciamento
1.6.1 . O equipamento ofertado deve permitir múltiplos arquivos de configuração;
1.6.2 . Deve suportar espelhamento remoto;
1.6.3 . Deve ser fornecido com todas as licenças de software necessárias para o funcionamento integral de todas as funcionalidades disponíveis para o equipamento;
1.6.4 . O equipamento ofertado deve possuir certificado de homologação na Anatel, de acordo com a resolução nº 242;

1.7 Garantia e Suporte;
1.7.1 . O equipamento proposto deverá possuir garantia do Fabricante de 36 meses para entrega de peças on-site a qual dever ser comprovada mediante documento oficial fabricante;
1.7.2 . Não serão aceitos transceivers que não sejam do mesmo fabricante do equipamento;
1.7.3 . Os serviços serão solicitados mediante a abertura de um chamado efetuado por técnicos da contratante, via chamada telefônica local, a cobrar ou 0800, e-mail, website ou chat do fabricante ou à empresa autorizada (em português ou inglês – para o horário comercial – horário oficial de Brasília) e constatada a necessidade, o fornecedor deverá

Documento assinado digitalmente por:		
Joao Paulo de Araujo Bezerra 23/06/2017 11:43:39	Ernesto Leca Pinto 23/06/2017 11:50:37	Daniel Cesar Gurgel Coelho Ponte 02/08/2017 14:07:01

providenciar o deslocamento do equipamento, bem como seu retorno ao local de origem sem qualquer ônus ao contratante;

Switch Topo de Rack (ToR)
Quantidade
2
Especificação

1. Switch

1.1. Características técnicas mínimas;

1.1.1. Deve possuir 48 portas 10 Gigabit Ethernet SFP+;
1.1.2. Deve possuir no mínimo 4 Portas 40GE em QSFP+;
1.1.3. Deve possuir 1 interface RJ-45 ou serial para acesso console local;
1.1.4. Deve ser fornecido com 05 cabos DAC SFP+ de 3 metros;
1.1.5. Deve ser fornecido com 05 cabos DAC SFP+ de 1 metro;
1.1.6. Deve ser fornecido com 01 cabo DAC QSFP+ de 5 metros;
1.1.7. Deve ser fornecido com 01 cabo DAC QSFP+ de 3 metros;
1.1.8. Deve ser fornecido com 01 cabo DAC QSFP+ de 1 metro;
1.1.9. Todos os cabos DAC oferecidos deverão ser completamente compatíveis com o equipamento fornecido;
1.1.10. Deve ser fornecido com 10 cabos LC/LC (duplos) tipo OM4 de no mínimo 3 metros completamente compatíveis com o transceiver 10GE fornecido;
1.1.11. Deve ser fornecido com no mínimo 2 cabos LC/MPO4 tipo OM4 com no mínimo 10 metros, completamente compatíveis com o transceiver 40GE fornecido;
1.1.12. Deve ser fornecido com no mínimo 8 transceivers 10GE Multimodo LC que suporte pelo menos 300 metros de distância usando uma fibra OM4;
1.1.13. Deve ser fornecido com no mínimo 2 transceivers 40GE Multimodo MPO que suporte pelo menos 100 metros de distância usando uma fibra OM4;
1.1.14. Todos os transceivers oferecidos deverão ser completamente compatíveis com o equipamento fornecido;
1.1.15. Deve possuir latência de, no máximo 1 µs em 10GE (para pacotes de 64 bytes);
1.1.16. Deve possuir capacidade de comutação de, no mínimo, 1420 Gbps;
1.1.17. Deve possuir capacidade de encaminhamento de, no mínimo, 1024 Milhões de pps;
1.1.18. Deve possuir 2 fontes de alimentação internas e redundantes de 220VAC;

1.2. Disponibilidade

1.2.1. Deve possuir capacidade de empilhamento de no mínimo 8 (oito) equipamentos membros da mesma pilha utilizando-se das portas 40GE existentes;
1.2.2. caso seja necessário módulos e cabos específicos para empilhamento, eles deverão ser fornecidos bem como licenciados;
1.2.3. não serão aceitos empilhamentos somente com finalidade de gerenciamento;
1.2.4. Deve suportar empilhamento de equipamentos da mesma família que tenham suporte a portas 100 GE;
1.2.5. Deve vir equipado com bandejas de ventilação tipo back to front ;

1.3. Switching

1.3.1. Deve suportar e já vir licenciado para o uso de VXLAN e EVPN L2/L3;
1.3.2. Deve possuir tabela para no mínimo 250.000 endereços MAC;
1.3.3. Deve implementar VLANs baseadas em MAC;
1.3.4. Deve suportar 4094 VLAN Ids;
1.3.5. Deve suportar protocolo OpenFlow;
1.3.6. Deve implementar Jumbo frames nas 10-Gigabit Ethernet
1.3.7. Deve implementar Jumbo frames com tamanho de no mínimo 9000 bytes;

Documento assinado digitalmente por:		
Joao Paulo de Araujo Bezerra 23/06/2017 11:43:39	Ernesto Leca Pinto 23/06/2017 11:50:37	Daniel Cesar Gurgel Coelho Ponte 02/08/2017 14:07:01

1.3.8. Deve implementar Ethernet link aggregation
1.3.9. Deve implementar os seguintes protocolos:
1.3.9.1. IEEE 802.1ad Q-in-Q
1.3.9.2. IEEE 802.1AX-2008 Link Aggregation
1.3.9.3. IEEE 802.1D MAC Bridges
1.3.9.4. IEEE 802.1p Priority
1.3.9.5. IEEE 802.1Q VLANs
1.3.9.6. IEEE 802.1s Multiple Spanning Trees
1.3.9.7. IEEE 802.1w para IEEE 802.3ad
1.3.9.8. Link Aggregation Control Protocol (LACP) IEEE 802.3ae 10-Gigabit Ethernet
1.3.9.9. IEEE 802.3ag Ethernet OAM
1.3.9.10. IEEE 802.3ah Ethernet in First Mile over Point to Point Fiber—EFMF
1.3.10. Deve implementar agregação de links em modo estático e dinâmico (LACP), com suporte a criação de no mínimo 128 grupos com pelo menos 30 portas cada.
1.3.11. Deve implementar IEEE 802.3x;
1.3.12. Deve suportar o uso de port security;
1.3.13. Deve implementar MSTP IEEE 802.1s com pelo menos 64 instâncias;

1.4. Roteamento

1.4.1. Deve implementar roteamento estático Ipv4;
1.4.2. Deve suportar uma tabela de roteamento IPv4 de pelo menos 120.000 entradas;
1.4.3. Deve suportar uma tabela de roteamento IPv6 de pelo menos 62.000 entradas;
1.4.4. Deve implementar roteamento estático Ipv6;
1.4.5. Deve implementar os seguintes protocolos de roteamento IPv4: RIPv2, OSPF, IS-IS e BGP4;
1.4.6. Deve implementar os seguintes protocolos de roteamento IPv6: RIPng, IS-IS e OSPFv3;
1.4.7. Deve implementar o protocolo VRRP;

1.5. Segurança

1.5.1. Deve implementar SSHv2;
1.5.2. Deve implementar 802.1x;
1.5.3. Deve implementar accounting RADIUS;

1.6. Gerenciamento

1.6.1. eve prover um controle completo do switch através de CLI (command line interface);
1.6.2. Deve permitir espelhamento de porta para monitoramento;
1.6.3. O equipamento ofertado deve permitir múltiplos arquivos de configuração;
1.6.4. Deve ser fornecido com todas as licenças de software necessárias para o funcionamento integral de todas as funcionalidades disponíveis para o equipamento;
1.6.5. Deve permitir gerenciamento integrado através de software de gerência.
1.6.6. Deve permitir o uso e duas imagens flash independentes (primária e backup) para atualizações;
1.6.7. Deve permitir configuração automática via DHCP;
1.6.8. O equipamento ofertado deve possuir certificado de homologação na Anatel, de acordo com a resolução nº 242;

1.7. Garantia e Suporte

1.7.1. O equipamento proposto deverá possuir garantia e suporte do Fabricante de 36 meses para entrega de peças on-site, na modalidade próximo dia útil, a qual deve ser comprovada mediante documento oficial do fabricante;
1.7.2. Todos os transceivers e cabos devem ter total compatibilidade com o equipamento fornecido, sob pena de não aceite dos equipamentos;
1.7.3. Os serviços serão solicitados mediante a abertura de um chamado efetuado por técnicos da contratante, via chamada telefônica local, a cobrar ou 0800, e-mail, website ou chat do fabricante ou à empresa autorizada (em português ou inglês – para o horário comercial – horário oficial de Brasília) e constatada a necessidade, o fornecedor deverá providenciar o deslocamento do equipamento, bem como seu retorno ao local de origem
1.7.4. sem qualquer ônus ao contratante;

Documento assinado digitalmente por:		
Joao Paulo de Araujo Bezerra 23/06/2017 11:43:39	Ernesto Leca Pinto 23/06/2017 11:50:37	Daniel Cesar Gurgel Coelho Ponte 02/08/2017 14:07:01

- **Sistema de UPS (Uninterruptible Power Supply) -** Também conhecidos como *Nobreaks*, Equipamentos disponíveis no mercado que atendem o requisito de prover alimentação estabilizada e autonomia mínima para possibilitar o desligamento adequado dos equipamentos de informática e telefonia.

NOBREAK
Quantidade
15
Especificação
1 Equipamento UPS de no mínimo 20000 VA Trifásico. **1.1 Características Gerais** 1.1.1 Deverá possuir tecnologia Dupla Conversão, True on Line, com retificador e inversor ambos dotados de funcionamento com IGBT. 1.1.2 Deverá ser composto de retificador/carregador de baterias independente, inversor, chave estática, bypass de manutenção interno, e ter cada um seu próprio banco de baterias, que não poderá ser ligado diretamente ao barramento DC quando em operação dentro da faixa de aceitação da tensão de entrada, não podendo estar sujeito a riple de tensão em seus terminais e de forma a otimizar seu prazo de vida útil. **1.2 Características de Entrada** 1.2.1 Deverá possuir tensão nominal de entrada configurável para 220 Volts, 230 Volts, 240 Volts Monofásico ou 380 Volts, 400 Volts, 415 Volts Trifásico. Deverá possuir a possibilidade de ligação monofásica e trifásica. Não será aceito transformadores de entrada e saída para regulação das tensões. 1.2.2 Deverá possuir capacidade de sobrecarga de 125% por 1 (um) minuto; e 150% por 30 (trinta) segundos. 1.2.3 Deverá possuir eficiência minima a plena carga de 94%. 1.2.4 Deverá possuir proteção de regulação de freqüência e tensão. 1.2.5 Deverá possuir proteção de cargas conectadas contra surtos, picos e outros distúrbios elétricos. 1.2.6 Deverá possuir correção de fator de potência de saída. 1.2.7 Deverá permitir ligar o no-break (Partida a Frio) para fornecer energia temporária de emergência mesmo quando não há energia elétrica. 1.2.8 Deverá possuir minidisjuntor rearmável para proteção de contra curtos circuitos. Não serão aceitos fusíveis. 1.2.9 Deverá possuir proteções contra sobrecarga e surtos de tensão. 1.2.10 Deverá possuir reinício automático no caso de restabelecimento de energia elétrica após a descarga das baterias. 1.2.11 Deverá possuir proteção contra surtos, filtragem de pólos múltiplos de ruídos e tempo de resposta de “clamping” zero. **1.3 Características de Saída** 1.3.1 Deverá possuir capacidade mínima de Potência Nominal Ativa de no mínimo 16000 Watts; 1.3.2 Deverá possuir capacidade mínima de Potência Nominal Aparente de 20000 Volt Àmpere; 1.3.3 Deverá possuir tensão nominal de saída configurável para 220 Volts, 230 Volts, 240 Volts Monofásico ou 380 Volts, 400 Volts, 415 Volts Trifásico. Deverá possuir a possibilidade de ligação monofásica e trifásica. 1.3.4 Não serão aceitos transformadores de entrada e saída para regulação das tensões; 1.3.5 Deverá possuir forma de onda na saída senoidal pura com Dupla Conversão, não sendo

aceitas formas de ondas modificadas.

1.4 Características do Hardware

1.4.1 Deverá possuir display para indicar carga de bateria ou se o no-break está on-line;

1.4.2 Deverá possuir capacidade de ser instalado em rack do padrão 19 polegadas;

1.5 Baterias e Tempo de Operação

1.5.1 Deverá possuir Baterias Chumbo-Ácido selada regulada por válvula, livre de manutenção, a prova de vazamento, própria para uso em equipamentos do tipo UPS; Não será aceito equipamento com uso de bateria do tipo automotiva ou similar;

1.5.2 Deverá energizar o equipamento com partida a frio, somente pelas baterias;

1.5.3 Deverá possuir autonomia mínima de 15 minutos, para meia carga;

1.5.4 Deverá possuir capacidade expansível por uso de baterias externas;

1.5.5 Deverá possuir no máximo tempo de recarga das baterias de 7 horas;

1.5.6 Deverá ser possível a substituição das baterias com o equipamento ligado (hot-swap).

1.6 Comunicação e Gerenciamento

1.6.1 Deverá possuir Gerenciamento remoto, via browser através de porta ethernet no equipamento;

1.6.2 Deverá possuir porta de interface DB-9 RS-232, RJ-45 10/100 Base-T;

1.6.3 Deverá já vir licenciado para software de gerenciamento do próprio fabricante.

1.6.4 Deverá suportar gerenciamento de pelo menos 20 equipamentos semelhantes através de software do próprio fabricante.

1.7 Garantia Conformidades e Documentação

1.7.1 Deverá vir com garantia mínima de 24 meses do próprio fabricante (não serão aceitas nenhum outro tipo de garantia que não seja do próprio fabricante) em regime 8x5;

1.7.2 Deverá ser instalado através de serviço ofertado pelo próprio fabricante, para ser realizado sob agendamento a critério do órgão em dias úteis, de segunda a sexta, e horário comercial.

1.7.3 Deverá possuir documentação técnica necessária (manual de usuário) a instalação, configuração, operação e verificação das propostas;

1.7.4 Deverá possuir conformidade a diretiva RoHS (Restriction of Certain Hazardous Substances) certificada.

1.8 Dimensões Físicas e Rendimento Ambiental

1.8.1 Deverá possuir altura máxima de 12 UA para montagem em rack de 19 polegadas;

1.8.2 Deverá possuir dimensão máxima de profundidade de 800 mm;

1.8.3 Deverá suportar montagem em racks e auto-portante do tipo Torre;

1.8.4 Deverá possuir Temperatura de operação de 16 a 40°C;

1.8.5 Não deverá ter dissipação térmica superior a 4000 BTU/hora;

1.8.6 Deverá possuir Umidade de operação de 0 a 95% sem condensação;

1.8.7 Deverá possuir Alarmes Visual e Sonoro.

- **Aparelhos de telefonia –** Pontos finais do sistema de telecomunicação por voz interno e externo. Será ampliado o sistema de telefonia VoIP atualmente instalado de modo a equipar todos as estações de trabalho.

Aparelhos Telefônicos VoIP
Quantidade
250
Especificação
1. Telefone IP-Gigabit: 1.1. Deverá suportar no mínimo 03 (três) contas SIP. 1.2. Deverá possuir agenda telefônica local para no mínimo 1000 entradas. 1.3. Deverá possuir pelo menos os seguintes recursos:

1.3.1. Conferência a 3 (três).
1.3.2. DND (não perturbe).
1.3.3. Discagem rápida.
1.4. Agenda telefônica remota via XML e LDAP.
1.5. Histórico de chamadas não atendidas, recebidas, discadas e transferidas.
1.6. Ajuste de volume.
1.7. Seleção de tom de chamada.
1.8. Deverá possuir suporte ao idioma português do Brasil na tela do telefone.
1.9. Deverá er totalmente compatível com o Asterisk e o FreePBX.
1.10. Deverá possui suporte a pelo menos os seguintes codecs de áudio:
1.10.1. G722 (Wideband).
1.10.2. G711, G723.1, G726, G729AB.
1.11. Deverá possuir auto-falante full duplex (para o viva-voz);.
1.12. Deverá possuir suporte a SIP v1 (RFC2543) e v2(RFC3261);.
1.13. Deverá suportar auto-provisionamento via FTP/TFTP/HTTP
1.14. Deverá ser configurável via navegador de internet/interface do telefone/auto-provisionamento.
1.15. Deverá suportar VLAN (802.1 pq) e QoS.
1.16. Deverá possuir pelo menos uma porta RJ9 para conexão de fones de ouvido.
1.17. Deverá possuir pelo menos duas portas Ethernet RJ45 10/100/1000 (gigabit ethernet) ou superior.
1.18. Deverá permitir configuração em modo bridge ou router.
1.19. Deverá vir acompanhado de fonte de alimentação com tensão de entrada automática (full range).
1.20. Deverá suportar o padrão Power over Ethernet (IEEE 802.3af).

2. Garantia do fabricante de, no mínimo, 01 (um) ano, com assistência técnica local.

- **Solução de conexão de rede sem fio -** Formada por controladora de acesso e pontos de acesso distribuídos no novo edifício sede.

Solução de Conexão de Rede Sem Fio
Quantidade:
1
Especificação
1. **Controladora de Acesso (quantidade: 1 ativa e 1 failover)** 1.1. Características Gerais 1.1.1. Deve ser do tipo appliance virtual ou Controlador virtual distribuído, desde que permita compreender todos os pontos de acesso em um único cluster; 1.1.1.1. Deve suportar o gerenciamento de Access Points nos padrões 802.11a/b/g/n/ac wave 2; 1.1.2. Deve suportar e já vir licenciado para o gerenciamento de no mínimo 50 Access Points; 1.1.3. Deve suportar o gerenciamento sem a necessidade de roteamento através da controladora, permitindo a operação autônoma dos Access Points em unidades remotas; 1.1.4. Deve suportar no mínimo 1000 dispositivos simultâneos; 1.1.5. Deve permitir sua configuração em alta disponibilidade (High Availability) do tipo ativo-ativo, com outro controlador de igual capacidade; 1.1.6. Caso necessite de licença ou qualquer peça de hardware e software para a implementação de alta disponibilidade as mesmas devem estar inclusas na solução

ofertada.
1.1.7. Cada controladora deve ser licenciada a operar independentemente todos Access Points especificados aqui;
1.1.8. Deve suportar roaming em uma mesma sub-rede e entre sub-redes diferentes;
1.1.9. Deve suportar, no mínimo, 64 SSIDs;
1.1.9.1. Será aceito o suporte de, no mínimo, 32 SSIDs (16 SSIDs por rádio) por Ponto de Acesso caso fluxo de dados do cliente não seja centralizado, configurando assim que as funções de controle serão executadas através de processamento distribuído nos pontos de acesso;
1.1.10. Deve implementar DHCP Server, Relay e Client;
1.1.11. Deve implementar 802.1d;
1.2. Roteamento
1.2.1. Deve implementar roteamento inter-vlan e OSPFv2;
1.3. QoS
1.3.1. Deve suportar limitação de banda por SSID
1.3.2. 1.3.2 Deve implementar rate-limiting;
1.3.3. Deve suportar limitação de banda por usuário;
1.3.4. Deve suportar limitação de banda por VLAN;
1.3.5.
1.4. Segurança
1.4.1. Deve suportar WPA e WPA2;
1.4.2. Deve suportar gerenciamento através de SSHv2;
1.4.3. Deve suportar gerenciamento através de HTTP com SSL;
1.4.4. Deve implementar 802;1x e autenticação e accounting com EAP: PEAP/EAP-GTC, PEAP/EAP-MSCHAPv2, EAP-TLS com utilização de base de usuários interna ou servidor RADIUS externo;
1.4.5. Deve suportar a configuração de servidores de RADIUS accounting diferentes por SSID;
1.4.6. Deve implementar autenticação baseada em endereço MAC;
1.4.7. Deve implementar portal para autenticação de clientes via web;
1.4.8. Deve suportar autenticação de Access Points através de 802.1x, para evitar Aps não autorizados;
1.4.9. Deve suportar autenticação integrada com Active Directory e LDAP;
1.4.10. Deve suportar ACLs por usuário;
1.4.11. Deve possibilitar a conexão de pontos de acesso através de túnel criptografado;
1.4.12. Deve suportar wireless IDS, com suporte a detecção das seguintes ameaças:
1.4.12.1. Rogue Aps
1.4.12.2. Floods de disassociação;
1.4.12.3. Floods de associação;
1.4.12.4. Flood de autenticação;
1.4.12.5. Flood de desautenticação;
1.5. Gerenciamento
1.5.1. Deve suportar LLDP;
1.5.2. Deve implementar SNMP v2c e V3;
1.5.3. Deve implementar syslog;
1.5.4. Incluir seguintes itens;
1.5.5. Deve implementar seleção automática de canais;
1.5.6. Deve implementar ajuste automático de potência, baseado nas condições do ambiente;
1.5.7. Deve implementar análise de espectro, permitindo a detecção e classificação

Documento assinado digitalmente por:		
Joao Paulo de Araujo Bezerra 23/06/2017 11:43:39	Ernesto Leca Pinto 23/06/2017 11:50:37	Daniel Cesar Gurgel Coelho Ponte 02/08/2017 14:07:01

de fontes de interferência como fornos de microondas e telefones sem-fio.

1.5.8. Deve implementar balanceamento de carga de clientes entre Aps vizinhos;

1.5.9. Deve implementar Airtime Fairness, de forma que seja alocado um tempo transmissão igual para os clientes wireless.

1.5.10. Deve estar homologado pela Anatel conforme resolução 242;

1.5.10.1. Não será necessário comprovar a homologação pela Anatel caso a solução seja composta por appliances virtuais ou controladoras virtuais;

1.6. Demais acessórios

1.6.1. Os equipamentos deverão vir acompanhados dos acessórios para fixação em rack, a saber: parafusos, adaptadores e/ou trilhos, bem como cabos de força;2.

1.6.2.

2. **Pontos de acesso para rede sem fio wave 2 (quantidade: 40)**

2.1. Deve possuir pelo menos uma interface 10/100/1000;

2.2. Deve possuir interface de console serial com conectores RJ-45 ou DB-9 ou proprietário, desde que fornecido cabo de console e acesso via SSH;

2.3. Deve ser capaz de operar em capacidade máxima (ambos rádios ativos) com alimentação PoE 802.3af;

2.4. Deve suportar os padrões IEEE 802.11b, 802.11g, 802.11a, 802;11n e 802.11ac;

2.5. Deve suportar no mínimo 2x2 MIMO para taxas de 400 Mbps por rádio 2.4-Ghz e no mínimo 4x4 MIMO para taxas de 1733 Mbps por rádio 5-Ghz;

2.6. Deve suportar pelo menos 4 streams para SU-MIMO de 1733 Mbps;

2.7. Deve suportar pelo menos 4 streams para MU-MIMO de 1733 Mbps;

2.8. Deve possuir duplo rádio permitindo operação simultânea nas faixas de 2.4 GHZ e 5 GHz;

2.9. Deve permitir a conexão simultânea de usuários do padrão 802.11ac e do padrão 802.11n;

2.10. Deve ser fornecido com no mínimo 4 antenas internas e integradas. Não serão aceitos equipamentos com antenas aparentes;

2.11. Deve estar homologado pela Anatel conforme resolução 242;

2.12. Deve suportar o gerenciamento centralizado por controlador wireless e ser capaz de operar de forma autônoma;

2.13. A operação de forma autônoma dos APs, previamente configurados pela controladora dever poder entrar em vigor quando as controladoras estiverem inoperantes de modo a prover mecanismo de acesso redundante a falhas nas controladoras;

2.14. O Access Point deverá ter a funcionalidade de cluster;

2.15. Deve permitir o gerenciamento centralizado de dispositivos de rede sem fio: Controladores de Acesso (AC's), Pontos de Acesso gerenciados (FIT AP's) e Pontos de Acesso autônomos (FAT AP's);

2.16. Em funcionamento no modo auto-gerenciado deve disponibilizar um firewall statefull interno à solução, com definição das políticas baseadas na identidade do usuário autenticado;

2.17. Deve implementar 802.1x com suporte a EAP: EAP-MD5, EAP-FAST, EAP-TLS, PEAP-GTC, PEAP-MSCHAPv2;

2.18. Deve implementar o isolamento de clientes wireless, permitindo a comunicação direta de dispositivos associados ao mesmo AP;

2.19. Deve implementar filtragem de endereço IP;

2.20. Deve implementar sistema integrado de detecção e prevenção contra intrusão, não dependendo de controlador de ponto de acesso sem fio;

2.21. Deve suportar a configuração taxa de dados de mínima por SSID;

2.22. Deve implementar autenticação via MAC;

2.23. Deve implementar RADIUS Client conforme as RFCs 2865 e 2866;

Documento assinado digitalmente por:		
Joao Paulo de Araujo Bezerra 23/06/2017 11:43:39	Ernesto Leca Pinto 23/06/2017 11:50:37	Daniel Cesar Gurgel Coelho Ponte 02/08/2017 14:07:01

2.24. Deve suportar o estabelecimento de conexão wireless entre dois Access Points;
2.25. Deve implementar ajuste automático de potência, baseado nas condições do ambiente;
2.26. Deve suportar a atualização automática de firmware através do controlador;
2.27. Deve implementar análise de espectro, permitindo a detecção e classificação de fontes de interferência como fornos de microondas e telefones sem-fio.
2.28. Deve implementar balanceamento de carga de clientes entre Aps vizinhos;
2.29. Deve implementar Airtime Fairness, de forma que seja alocado um tempo transmissão igual para os clientes wireless.
2.30. Deve suportar controle de banda por usuário;
2.31. Deve suportar o padrão 802;1Q;
2.32. Deve implementar Beamforming;
2.33. Deve implementar mecanismo que permita o direcionamento de clientes 802;11n capazes de suportar 5 GHz para esta faixa de frequência automaticamente (Bandsteering);
2.34. Deve suportar, no mínimo, 10 chamadas VoIP simultaneamente;
2.35. Deve suportar a alocação automática de canais de frequência;
2.36. Deve implementar 802;11i;
2.37. Deve suportar WPA com algoritmo de criptografia TKIP e MIC e WPA2 com algoritmo de criptografia AES 128/256 bits;
2.38. Deve suportar, no mínimo, 16 SSIDs;
2.39. Deve possuir certificação Wi-Fi;
2.40. Deve suportar, no mínimo, 250 clientes por rádio;
2.41. Deve suportar Jumbo Frame;
2.42. Deve implementar túnel criptografado para modo de operação remota;

- **Firewall –** Necessário para oferecer camadas de segurança entre a rede externa ao Tribunal e a Rede Interna.

Firewall
[1]Quantidade
1
Especificação
1. Características Gerais 1.1. Os produtos de hardware ofertados devem ser novos, nunca terem sido utilizados e não terem sido descontinuados, ou seja, devem constar na linha atual de comercialização e suporte do fabricante; 1.2. A solução deverá utilizar a tecnologia de firewall Stateful Packet Inspection com Deep Packet Inspection (suportar a inspeção da área de dados do pacote) para filtragem de tráfego IP. 1.3. Os produtos ofertados deverão vir acompanhados de todos os cabos e acessórios necessários à completa instalação e operação dos mesmos; 1.4. Os produtos ofertados deverão vir acompanhados de documentação impressa ou em mídia DVD/CD ou via download, em idioma português ou inglês, contendo orientações para configuração e operação do produto fornecido; 1.5. Em appliance com no máximo 2U de altura, com kit de montagem em rack de 19”.

1

1.6. Deve ser entregue com todos os cabos e itens necessários para a sua correta instalação e fixação no rack, tais como: suportes, trilhos, parafusos, etc;
1.7. Não serão permitidas soluções baseadas em sistemas operacionais abertos como Free BSD, Debian ou mesmo Linux.
1.8. O equipamento deverá ser baseado em hardware desenvolvido com está finalidade, ou seja, de um firewall não sendo baseado em plataforma X86 ou equivalente.
1.9. Mínimo de 2 GB de memória RAM para maior confiabilidade do sistema.
1.10. Sistema Operacional do Tipo “Harderizado” não serão aceitos. Apenas os que forem armazenados em memória flash.
1.11. Fonte de alimentação com operação automática entre 110/220V.
1.12. Possuir redundância do sistema de refrigeração do produto (Fan) redundante, com no mínimo dois ventiladores
1.13. Deverá possuir pelo menos duas interfaces de 10 GbE SFP+;
1.14. Deverá possuir pelo menos quatro interfaces de 1 GbE SFP;
1.15. Suportar 12 interfaces 10/100/1000 Gbe. Todas operando em modo autosense e em modo half/full duplex, com inversão automática de polaridade configuráveis pelo administrador do firewall para atendendo os segmentos de segurança e rede para:
a) Segmento WAN , ou externo.
b) Segmento WAN, secundário com possibilidade de ativação de recurso para redundância de WAN com balanceamento de carga e WAN Failover por aplicação. O equipamento deverá suportar no mínimo balanceamento de 4 links utilizando diferentes métricas pré-definidas pelo sistema.
c) Segmento LAN ou rede interna.
d) Segmento LAN ou rede interna podendo ser configurado como DMZ (Zona desmilitarizada)
e) Segmento LAN ou rede interna ou Porta de sincronismo para funcionamento em alta disponibilidade
f) Segmento ou Zona dedicada para controle de dispositivos Wireless dedicado com controle e configuração destes dispositivos.
1.16. Possuir uma interface de rede dedicada operando em 1Gbps para o gerenciamento do produto. Seu processamento deverá ser de forma isolada ao processamento dos demais tráfegos que passam pelo produto.
1.17. Performance de Firewall SPI (Stateful Packet Inspection) igual ou superior a 3 Gbps.
1.18. Performance para inspeção de Anti-Malware integrado no mesmo appliance: 600 Mbps ou superior
1.19. Não serão permitidas soluções baseadas em redirecionamento de tráfego para dispositivos externos ao appliance para análise de arquivos ou pacotes de dados. A atualização das assinaturas deverá ocorrer de forma automática sem há necessidade de intervenção humana.
1.20. A solução de Gateway Antivírus deverá suportar análise de pelo menos os protocolos, CIFS, NETBIOS, HTTP, FTP, IMAP, SMTP e POP3.
1.21. Performance de IPS de 1.0 Gbps ou superior
1.22. Não serão permitidas soluções baseadas em redirecionamento de tráfego para dispositivos externos ao appliance para análise de arquivos ou pacotes de dados.
1.23. A atualização das assinaturas deverá ocorrer de forma automática sem a necessidade de intervenção humana.
1.24. Performance de todos os serviços ativos UTM (Gateway Antivírus, Gateway Anti Spyware, IDS, IPS e Filtro de Conteúdo) deverá ser de 800 Mbps ou superior. Caso o fornecedor não possa comprovar este item em documentações públicas, o mesmo poderá comprovado através de testes em bancada com gerador de pacotes.
1.25. Os Throughputs devem ser comprovados por documento de domínio público do

Documento assinado digitalmente por:		
Joao Paulo de Araujo Bezerra 23/06/2017 11:43:39	Ernesto Leca Pinto 23/06/2017 11:50:37	Daniel Cesar Gurgel Coelho Ponte 02/08/2017 14:07:01

fabricante. A ausência de tais documentos comprobatórios reservará ao órgão o direito de aferir a performance dos equipamentos em bancada, assim como atendimento de todas as funcionalidades especificadas neste edital. Caso seja comprovado o não atendimento das especificações mínimas nos testes de bancada, o fornecedor será considerado inabilitados. Todos os custos oriundos do teste de bancada serão por conta do fornecedor;

1.26. Capacidade mínima de conexões suportadas em modo firewall deverá ser de no mínimo ou superior 300.000 Mil conexões.

1.27. Capacidade mínima de conexões suportadas em modo DPI (analise produnda de pacotes com os serviços IPS, Anti-Malware (Anti-Virus e Anti-Spyware) deverá ser de no mínimo ou superior a 150.000 Mil de conexões.

1.28. Suportar no mínimo 20.000 novas conexões por segundo.

1.29. Suportar no mínimo 256 interfaces de vlan (802.1q) suportando a definição de seus endereços IP através da interface gráfica;

1.30. O equipamento deve ter a capacidade de analisar tráfegos criptografados HTTPS/SSL onde o mesmo deverá ser descriptografado de forma transparente a aplicação, verificado possíveis ameaças e então re-criptografado enviado juntamente ao seu destino caso este não contenha ameaças ou vulnerabilidades. Sua performance mínima para esta funcionalidade deverá ser de 300 Mbps.

1.31. Performance de VPN IPSEC (3DES & AES 256) deverá ser de 1.5 Gbps ou superior.

1.32. Possuir porta console (serial) para possíveis manutenções no produto. Configurações básicas via interface CLI como suporte a comandos para debug deverão ser suportadas por esta interface.

2. Funcionalidades de Firewall

2.1. Possibilitar o controle do tráfego para os protocolos TCP, UDP, ICMP e serviços como FTP, DNS, P2P entre outros, baseados nos endereços de origem e destino;

2.2. Possibilitar o controle sobre aplicações de forma granular com criação de políticas sobre o fluxo de dados de entrada, saída ou ambos e;

2.3. Devem ser aplicados por usuário e por grupo e;

2.4. Associado sua ação políticas de horários e dias da semana e;

2.5. Podem ser associados a endereçamento IP baseados em sub-redes e;

2.6. Permitindo a restrição de arquivos por sua extensão e bloqueio de anexos através de protocolos SMTP e POP3 baseado em seus nomes ou tipos mime.

2.7. Permitir a filtragem de e-mails pelo seu conteúdo, através da definição de palavras-chave e a sua forma de pesquisa;

2.8. Prover matriz de horários que possibilite o bloqueio de serviços com granularidade baseada em hora, minutos, dia, dias da semana, mês e ano que a ação deverá ser tomada.

2.9. O appliance deve permitir a utilização de políticas de segurança associadas as políticas Anti Malware, IPS/IDS e filtro de Conteúdo em diferentes segmentos e diferentes combinações podendo ser aplicadas inclusive em sub-interfaces estruturadas em Vlans, por sua vez associadas a diferentes zonas de segurança.

2.10. Possuir flexibilidade para liberar aplicações da inspeção profunda de pacotes, ou seja, excluir a aplicação da checagem de recursos como Anti Malwares, IPS entre outros.

2.11. Possibilitar o controle do tráfego para os protocolos GRE, H323 Full v1-5, suporte a tecnologia a gatekeeper, SIP e IGMP baseados nos endereços origem e destino da comunicação,

2.12. Controle e gerenciamento de banda para a tecnologia VoIP sobre diferentes segmentos de rede/segurança com inspeção profunda de segurança sobre este serviço.

2.13. Prover mecanismo contra ataques de falsificação de endereços (IP Spoofing) através da especificação da interface de rede pela qual uma comunicação deve se originar;

2.14. Prover mecanismos de proteção contra ataques baseados em “DNS Rebinding” protegendo contra códigos embutidos em páginas Web com base em JavaScript, Flash e base

Documento assinado digitalmente por:		
Joao Paulo de Araujo Bezerra 23/06/2017 11:43:39	Ernesto Leca Pinto 23/06/2017 11:50:37	Daniel Cesar Gurgel Coelho Ponte 02/08/2017 14:07:01

Java com “malwares”. O recurso deverá prevenir ataques e analises aos seguintes endereços:
a) Node-local address 127.0.0.1
b) Link-local address 169.254.0.0/24
c) Multicast address 224.0.0.0/24
d) Host que pertence há alguma das sub-nets conectadas a: LAN, DMZ ou WLAN.

2.15. Prover servidor DHCP Interno suportando múltiplos escopos de endereçamento para a mesma interface e a funcionalidade de DHCP Relay;

2.16. Prover a capacidade de encaminhamento de pacotes UDPs multicast/broadcast entre diferentes interfaces e zonas de segurança como como IP Helper suportando os protocolos e portas:
a) Time service—UDP porta 37
b) DNS—UDP porta 53
c) DHCP—UDP portas 67 e 68
d) Net-Bios DNS—UDP porta 137
e) Net-Bios Datagram—UDP porta 138
f) Wake On LAN—UDP porta 7 e 9
g) mDNS—UDP porta 5353

2.17. Possuir mecanismo de forma a possibilitar o funcionamento transparente dos protocolos FTP, Real Áudio, Real Vídeo, SIP, RTSP e H323, mesmo quando acessados por máquinas através de conversão de endereços. Este suporte deve funcionar tanto para acessos de dentro para fora quanto de fora para dentro;

2.18. Implementar mecanismo de sincronismo de horário através do protocolo NTP. Para tanto o appliance deve realizar a pesquisa em pelo menos 03 servidores NTP distintos, com a configuração do tempo do intervalo de pesquisa;

2.19. Prover mecanismo de conversão de endereços (NAT), de forma a possibilitar que uma rede com endereços reservados acesse a Internet a partir de um único endereço IP e possibilitar também um mapeamento 1-1 de forma a permitir com que servidores internos com endereços reservados sejam acessados externamente através de endereços válidos;

2.20. Permitir, sobre o recurso de NAT, o balanceamento interno de servidores e suas aplicações sem a necessidade de inserção de um equipamento como switches de que atuam entre as camadas 4 (quatro) e 7 (sete) do modelo ISO/OSI.

2.21. Possuir mecanismo que permita que a conversão de endereços (NAT) seja feita de forma dependente do destino de uma comunicação, possibilitando que uma máquina, ou grupo de máquinas, tenham seus endereços convertidos para endereços diferentes de acordo com o endereço destino;

2.22. Possuir mecanismo que permita conversão de portas (PAT);

2.23. Possuir gerenciamento de tráfego de entrada ou saída, por serviços,endereços IP e regra de firewall, permitindo definir banda mínima garantida e máxima permitida em porcentagem (%) para cada regra definida.

2.24. Possuir controle de número máximo de sessões TCP, prevenindo a exaustão de recursos do appliance e permitindo a definição de um percentual do número total de sessões disponíveis que podem ser utilizadas para uma determinada conexão definida por regra de acesso.

2.25. Implementar 802.1p e classe de serviços CoS (Class of Service) de DSCP (Differentiated Services Code Points);

2.26. Permitir remarcação de pacotes utilizando TOS e/ou DSCP;

2.27. Possuir roteamento RIP, OSPF e BGP, com configuração pela interface gráfica;

2.28. Possuir suporte ao protocolo SNMP versões 2 e 3;

2.29. Possui suporte a log via syslog;

2.30. Possuir mecanismo para possibilitar a aplicação de correções e atualizações para o firewall remotamente através da interface gráfica;

2.31. Permitir a visualização em tempo real de todas as conexões TCP e sessões UDP que se encontrem ativas através do firewall.

2.32. Permitir a geração de gráficos em tempo real, representando os serviços mais utilizados e

Documento assinado digitalmente por:		
Joao Paulo de Araujo Bezerra 23/06/2017 11:43:39	Ernesto Leca Pinto 23/06/2017 11:50:37	Daniel Cesar Gurgel Coelho Ponte 02/08/2017 14:07:01

as máquinas mais acessadas em um dado momento;

2.33. Permitir a visualização de estatísticas do uso de CPU do appliance o através da interface gráfica remota em tempo real;

3. Alta Disponibilidade

3.1. Possuir mecanismo de Alta Disponibilidade operando em modo Ativo/Standby, com as implementações de Fail Over e Load Balance, sendo que na implementação de Load Balance o estado das conexões e sessões TCP e UDP devem ser replicadas sem restrições de serviços como, por exemplo, tráfego multicast.

3.2. Não serão permitidas soluções de cluster (HA) que façam com que o equipamento (s) reinicie após qualquer modificação de parâmetro/configuração seja realizada pelo administrador.

3.3. O recurso de Alta Disponibilidade deverá ser suportado em modo Bridge

3.4. Funcionalidade de Prevenção de Intrusão

3.5. Possuir Mecanismo de IPS / IDS, com suporte a pelo menos 3.000 assinaturas de ataques completamente integrados ao Firewall;

3.6. O Sistema de detecção e proteção de intrusão deverá estar orientado à proteção de redes;

3.7. Possuir tecnologia de detecção baseada em assinatura;

3.8. Possuir capacidade de remontagem de pacotes para identificação de ataques;

3.9. Deverá possuir capacidade de agrupar assinaturas para um determinado tipo de ataque. Exemplo: agrupar todas as assinaturas relacionadas à webserver para que seja usado para **proteção específica de Servidores Web;**

3.10. Deverá possuir capacidade de análise de tráfego para a detecção e bloqueio de anomalias como Denial of Service (DoS) do tipo Flood, Scan, Session e Sweep.

3.11. Atualizar automaticamente as assinaturas para o sistema de detecção de intrusos sem intervenção do administrador

3.12. Reconhecimento de padrões;

3.13. Análise de protocolos;

3.14. Detecção de anomalias;

3.15. Detecção de ataques de RPC (Remote procedure call);

3.16. Proteção contra ataques DNS (Domain Name System);

3.17. Proteção contra ataques de ICMP (Internet Control Message Protocol);

3.18. Suportar reconhecimento de ataques de DDoS, reconnaissance, exploits e evasion;

4. Filtro de Conteúdo

4.1. Possuir base contendo no mínimo 20 milhões de sites internet web já registrados e classificados com atualização automática;

4.2. Suporte a filtragem para, no mínimo, 56 categorias e com, pelo menos, as seguintes categorias: violência, nudismo, roupas intimas/banho, pornografia, armas, ódio / racismo, cultos / ocultismo,drogas / drogas ilegais, crimes / comportamento ilegal, educação sexual, jogos, álcool / tabagismo, conteúdo adulto, conteúdo questionável, artes e entretenimento, bancos / e-trading, chat, negócios e economia, tecnologia de computadores e Internet, e-mail pessoal, jogos de azar , hacking, humor, busca de empregos, newsgroups, encontros pessoais, restaurantes / jantar, portais de busca, shopping e portais de compras, MP3, download de software, viagens e WEB hosting;

4.3. Capacidade de submissão de novos sites através de portal web ou suporte do Fabricante

4.4. Implementar filtro de conteúdo transparente para o protocolo HTTP, de forma a dispensar a configuração dos browsers das máquinas clientes.

4.5. O administrador poderá adicionar filtros por palavra-chave de modo específico;

4.6. A política de Filtros de conteúdo deverá ser baseada em horário do dia e dia da semana.

4.7. Suportar recurso de autenticação única para todo o ambiente de rede, ou seja, utilizando a plataforma de autenticação atual que pode ser de LDAP ou AD; o perfil de cada usuário deverá ser obtido automaticamente para o controle das políticas de Filtro de Conteúdo sem a necessidade de uma nova autenticação.

4.8. Permitir a criação de listas personalizadas de URLs permitidas – lista branca e bloqueadas,

Documento assinado digitalmente por:		
Joao Paulo de Araujo Bezerra 23/06/2017 11:43:39	Ernesto Leca Pinto 23/06/2017 11:50:37	Daniel Cesar Gurgel Coelho Ponte 02/08/2017 14:07:01

assim como, lista negra;

4.9. Deverá permitir a criação de regras para acesso/bloqueio por endereço IP de origem;
4.10. Deverá permitir a criação de regras para acesso/bloqueio por subrede de origem;
4.11. Deverá permitir o bloqueio Web através de senha pré configura pelo administrador
4.12. Deverá permitir criar política de confirmação de acesso
4.13. Deverá bloquear sites embarcados dentro outro sites como por exemplo translate.google.com.br
4.14. Exibir mensagens de bloqueio customizável pelos Administradores para resposta aos usuários na tentativa de acesso a recursos proibidos pela política de segurança interna;
4.15. Permitir a criação de pelo menos 5 categorias personalizadas;
4.16. Permitir a filtragem de todo o conteúdo do tráfego WEB de URLs conhecidas como fonte de material impróprio e códigos (programas/scripts) maliciosos em applets Java, cookies, activeX através de base de URL própria atualizável;
4.17. Para atender este sistema, poderá ser incluído equipamento externo desde que oficialmente homologado pela fabricante da solução;
4.18. Possuir a capacidade de análise de ameaças não conhecidas;
4.19. Selecionar através de política de Firewall quais tipos de arquivos sofrerão esta análise e tamanho de arquivos;
4.20. Implementar a análise de arquivos maliciosos em ambiente controlado com, no mínimo, sistema operacional Windows XP, Windows 7, Windows 10, MacOS, Android, Linux
4.21. Implementar a monitoração de arquivos trafegados na internet (HTTP, FTP, HTTPS, SMTP, IMAP, CIFS, TCP Stream, POP);
4.22. A análise “In Cloud” ou local deve prover informações sobre as ações do Malware na máquina infectada, informações sobre quais aplicações são utilizadas para causar/propagar a infecção, detectar aplicações não confiáveis utilizadas pelo Malware, gerar assinaturas de Antivírus e Antispyware automaticamente, definir URLs não confiáveis utilizadas pelo novo Malware e prover Informações sobre o usuário infectado (seu endereço IP e seu login de rede);
4.23. O sistema automático de análise "In Cloud" ou local deve mostrar em tela ou emitir relatório com identificação de quais soluções de Antivírus existentes no mercado possuem assinaturas para bloquear o Malware;
4.24. Implementar a visualização dos resultados das análises de malwares de dia zero nos diferentes sistemas operacionais dos ambientes controlados (sandbox) suportados;
4.25. Implementar a análise de arquivos executáveis, DLLs, ZIP e criptografados em SSL no ambiente controlado;
4.26. Suportar a análise de arquivos do pacote office (.doc, .docx, .xls, .xlsx, .ppt, .pptx) e Android APKs no ambiente controlado;
4.27. Suporte a submissão de arquivos para análise através do serviço de Sandbox.

5. Controle de Aplicações

5.1. Deverá reconhecer no mínimo 1.500 aplicações;
5.2. Capacidade para realizar filtragens/inspeções dentro de portas TCP conhecidas por exemplo porta 80 http, buscando por aplicações que potencialmente expõe o ambiente como: P2P, Kazaa, Morpheus, BitTorrent ou messengers
5.3. Controlar o uso dos serviços de Instant Messengers como MSN, YAHOO, Google Talk, ICQ, de acordo com o perfil de cada usuário ou grupo de usuários, de modo a definir, para cada perfil, se ele pode ou não realizar download e/ou upload de arquivos, limitar as extensões dos arquivos que podem ser enviados/recebidos e permissões e bloqueio de sua utilização baseados em horários pré-determinados pelo administrador será obrigatório para este item.
5.4. Deverá controlar software FreeProxy tais como ToR, Ultrasurf, Freegate,etc.
5.5. Deverá permitir a criação de regras para acesso/bloqueio por endereço IP de origem;
5.6. Deverá permitir a criação de regras para acesso/bloqueio por subrede de origem e destino;
5.7. Funcionalidade de Controle de Banda (QoS)

5.8. Permitir o controle e a priorização do tráfego, priorizando e garantindo banda para as aplicações (inbound/outbound) através da classificação dos pacotes (Shaping), criação de filas de prioridade e gerência de congestionamento;
5.9. Limitar individualmente a banda utilizada por aplicação
5.10. Deverá integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados;
5.11. Deverá prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory e LDAP;
5.12. Deverá controlar (limitar) individualmente a banda utilizada por grupo de usuários do Microsoft Active Directory e LDAP;
5.13. Deverá controlar (limitar) individualmente a banda utilizada por subrede de origem e destino;
5.14. Deverá controlar (limitar) individualmente a banda utilizada por endereço IP de origem e destino.

6. VPN

6.1. Suportar no mínimo 1000 túneis VPN IPSEC do tipo site-to-site já licenciadas.
6.2. Suportar no mínimo 50 túneis VPN IPSEC do tipo client-to-site já licenciadas podendo suportar no futuro, baseado na aquisição de licenciamento, 1.000 túneis.
6.3. Suportar no mínimo 2 conexões clientes do tipo SSL sem custo e 350 licenças/conexões futuras baseadas em licenciamento adicional.
6.4. Suportar políticas de roteamento sobre conexões VPN IPSEC do tipo site-to-site com diferentes métricas e serviços. A rota poderá prover aos usuários diferentes caminhos redundantes sobre todas as conexões VPN IPSEC.
6.5. Implementar os esquemas de troca de chaves manual, IKE e IKEv2 por Pré-Shared Key, Certificados digitais e XAUTH client authentication;
6.6. Permitir a definição de um gateway redundante para terminação de VPN no caso de queda do circuito primário;
6.7. Permitir que seja criado políticas de roteamentos estáticos utilizando IPs de origem, destino, serviços e a própria VPN como parte encaminhadora deste tráfego sendo este visto pela regra de roteamento, como uma interface simples de rede para encaminhamento do tráfego.
6.8. Suportar a criação de túneis IP sobre IP (IPSEC Tunnel), de modo a possibilitar que duas redes com endereço inválido possam se comunicar através da Internet;

7. Autenticação

7.1. Permitir a utilização de LDAP, AD e RADIUS;
7.2. Permitir o cadastro manual dos usuários e grupos diretamente na interface de gerencia remota do Firewall, caso onde se dispensa um autenticador remoto para o mesmo;
7.3. Permitir a integração com qualquer autoridade certificadora emissora de certificados X509 que seguir o padrão de PKI descrito na RFC 2459, inclusive verificando as CRLs emitidas periodicamente pelas autoridades, que devem ser obtidas automaticamente pelo firewall via protocolos HTTP e LDAP;
7.4. Permitir o controle de acesso por usuário, para plataformas Windows Me, NT, 2000, 2000, XP, Windows 7 , Windows 8 e Windows 10 de forma transparente, para todos os serviços suportados, de forma que ao efetuar o logon na rede, um determinado usuário tenha seu perfil de acesso automaticamente configurado;
7.5. Permitir a restrição de atribuição de perfil de acesso a usuário ou grupo independente ao endereço IP da máquina que o usuário esteja utilizando.
7.6. Suportar recurso de autenticação única para todo o ambiente de rede, ou seja, utilizando a plataforma de autenticação atual que pode ser de LDAP ou AD; o perfil de cada usuário deverá ser obtido automaticamente através de regras no Firewall DPI (Deep Packet Inspection) sem a necessidade de uma nova autenticação como por exemplo, para os serviços de navegação a Internet atuando assim de forma toda transparente ao usuário. Serviços como HTTP, HTTPS devem apenas consultar uma base de dados de usuários e grupos de servidores 2008/2012

Documento assinado digitalmente por:		
Joao Paulo de Araujo Bezerra 23/06/2017 11:43:39	Ernesto Leca Pinto 23/06/2017 11:50:37	Daniel Cesar Gurgel Coelho Ponte 02/08/2017 14:07:01

com AD;

8. Administração

8.1. Suportar no mínimo 20.000 usuários autenticados com serviços ativos e identificados passando por este dispositivo de segurança em um único dispositivo de segurança. Políticas baseadas por grupos de usuários deverão ser suportadas por este dispositivo. Está comprovação poderá ser exigida em testes sobe o ambiente de produção com o fornecimento do produto para comprovação deste e demais itens.

8.2. Permitir a criação de perfis de administração distintos, de forma a possibilitar a definição de diversos administradores para o firewall, cada um responsável por determinadas tarefas da administração;

8.3. Fornecer gerência remota, com interface gráfica nativa;

8.4. Fornecer interface gráfica para no mínimo 3 usuários;

8.5. A interface gráfica deverá possuir assistentes para facilitar a configuração inicial e a realização das tarefas mais comuns na administração do firewall, incluindo a configuração de VPN IPSECs, NAT, perfis de acesso e regras de filtragem;

8.6. Possuir mecanismo que permita a realização de cópias de segurança (backups) e sua posterior restauração remotamente, através da interface gráfica, sem necessidade de se reinicializar o sistema;

8.7. Possuir mecanismo para possibilitar a aplicação de correções e atualizações para o firewall remotamente através da interface gráfica;

8.8. Permitir a visualização em tempo real de todas as conexões TCP e sessões UDP que se encontrem ativas através do firewall e a remoção de qualquer uma destas sessões ou conexões;

8.9. Permitir a geração de gráficos em tempo real, representando os serviços mais utilizados e as máquinas mais acessadas em um dado momento;

8.10. Permitir a visualização de estatísticas do uso de CPU, memória da máquina onde o firewall está rodando e tráfego de rede em todas as interfaces do Firewall através da interface gráfica remota, em tempo real e em forma tabular e gráfica;

8.11. Permitir a conexão simultânea de vários administradores, sendo um deles com poderes de alteração de configurações e os demais apenas de visualização das mesmas. Permitir que o segundo ao se conectar possa enviar uma mensagem ao primeiro através da interface de administração.

8.12. Possibilitar o registro de toda a comunicação realizada através do firewall, e de todas as tentativas de abertura de sessões ou conexões que forem recusadas pelo mesmo;

8.13. Possuir interface orientada a linha de comando para a administração do firewall a partir do console ou conexão SSH sendo está múltiplas sessões simultâneas.

8.14. Possuir mecanismo que permita inspecionar o tráfego de rede em tempo real (sniffer) via interface gráfica, podendo opcionalmente exportar os dados visualizados para arquivo formato PCAP e permitindo a filtragem dos pacotes por protocolo, endereço IP origem e/ou destino e porta IP origem e/ou destino, usando uma linguagem textual;

8.15. Permitir a visualização do tráfego de rede em tempo real tanto nas interfaces de rede do Firewall quando nos pontos internos do mesmo: anterior e posterior à filtragem de pacotes, onde o efeito do NAT (tradução de endereços) é eliminado;

8.16. Possuir sistema de respostas automáticas que possibilite alertar imediatamente o administrador através de e-mails, janelas de alerta na interface gráfica, execução de programas e envio de Traps SNMP;

9. Relatórios

9.1. Ser capaz de visualizar, de forma direta no appliance e em tempo real, as aplicações mais utilizadas, os usuários que mais estão utilizando estes recursos informando sua sessão, total de pacotes enviados, total de bytes enviados e média de utilização em Kbps, URLs acessadas e ameaças identificadas.

9.2. Possibilitar a geração de pelo menos os seguintes tipos de relatório com cruzamento de informações, mostrados em formato HTML: máquinas acessadas X serviços bloqueados,

Documento assinado digitalmente por:		
Joao Paulo de Araujo Bezerra 23/06/2017 11:43:39	Ernesto Leca Pinto 23/06/2017 11:50:37	Daniel Cesar Gurgel Coelho Ponte 02/08/2017 14:07:01

usuários X URLs acessadas, usuários X categorias Web bloqueadas (em caso de utilização de um filtro de conteúdo Web);

9.3. Possibilitar a geração de pelo menos os seguintes tipos de relatório, mostrados em formato HTML: máquinas mais acessadas, serviços mais utilizados, usuários que mais utilizaram serviços, URLs mais visualizadas, ou categorias Web mais acessadas (em caso de existência de um filtro de conteúdo Web), maiores emissores e receptores de e-mail;

9.4. Permitir o envio dos relatórios, através de email para usuários prédefinidos;

9.5. Possuir relatórios prédefinidos na solução e permitir a criação de relatórios customizados;

9.6. Possibilitar a geração dos relatórios sob demanda e através de agendamento diário, semanal e mensal. No caso de agendamento, os relatórios deverão ser publicados de forma automática

9.7. Disponibilizar download dos relatórios gerados;

10. Garantia, Suporte e Licenciamento

10.1. O licenciamento para todos os serviços de Next Generation Firewall deverá ser de 60 meses.

10.2. A garantia deverá ser de 60 meses.

10.3. Deve contemplar suporte do Fabricante pelo período vigente. Com no mínimo, as seguintes características:

a) O suporte do fabricante deve ter um sistema de abertura de chamados para acompanhamento – funcionando 24 horas por dia e 7 dias por semana

b) Deve assegurar a utilização de novas versões de software da solução sem ônus a Licitante, sempre que esta estiver disponível a qualquer cliente

c) Deve permitir o acesso à base de conhecimento da solução.

11. **Conformidade**

11.1. O Fabricante deve comprovar participação no MAPP da Microsoft;

11.2. A tecnologia deve possuir pelo menos uma certificação da ICSA Labs, ICSA Firewall ou Antivírus;

11.3. O fabricante da solução deverá ser avaliado pela NSS Labs (Network Security Services) no desempenho do Next Generation Firewall Comparative Analysis mais recente, estando no “Security Value Map” acima de 90% (noventa por cento) da avaliação de segurança efetiva.

11.4. No momento da entrega dos equipamentos a proponente vencedora deverá fornecer declaração do(s) fabricante(s), em papel timbrado com firma reconhecida, dos produtos ofertados, declarando que a proponente possui credenciamento do mesmo para a implantação e suporte técnico de seus produtos;

1.8 Custos levantadas em projetos Similares realizados por outros órgãos da administração

Solução de Switches	
Descrição	Switches de Núcleo, Distribuição, Acesso
Órgão ou Entidade da Adm Pública que a Utiliza	TRE-MS, DPF-MJ
Fornecedor	HP, Cisco, extreme
Custo da Solução	U$ 620.000,00 = R$ 1.933.317,00

Solução de Conexão de Rede sem Fio	
Descrição	Solução de conexão de rede sem fio composta por Access Points, Controladora, Licenças quando for o caso.
Órgão ou Entidade da Adm Pública que a Utiliza	CAESB, TRT-17

Fornecedor	HP, Cisco, extreme
Custo da Solução	U$ 130.000,00 = R$ 405.372,00

Solução de Nobreaks	
Descrição	Nobreak de 20kva
Órgão ou Entidade da Adm Pública que a Utiliza	Ministério da Educação, Governo do Acre
Fornecedor	APC, Engetron
Custo da Solução	R$ 720.000,00

Aparelhos Telefônicos VoIP	
Descrição	Aparelhos telefônicos VoIP com alimentação PoE
Órgão ou Entidade da Adm Pública que a Utiliza	TRE-RN, IFSC, cmd do éxercito/ESA,UFRN
Fornecedor	Yealink, Grandstream
Custo da Solução	R$ 1.000,00 x 250 = R$ 250.000,00

Firewall	
Descrição	Firewall
Órgão ou Entidade da Adm Pública que a Utiliza	TRE-AL , Governo do Estado do Pará
Fornecedor	Sonicwall, paloalto
Custo da Solução	R$ 100.000,00

1.9 Levantamento das alternativas

1.9.1 . Solução 1:

- Utilização dos equipamentos atualmente existentes no prédio secretaria para equipar o novo prédio sede adaptando-se às necessidades encontradas.

1.9.2 . Solução 2:

- Buscar atas registradas em outros orgãos na esfera federal localizando todo os itens necessários para equipar o novo prédio sede.

1.9.3 . Solução 3:

- Realização de licitação própria com o objetivo de adquirir todos os equipamentos necessários à infraestrutura do novo prédio sede.

1.10 Análise e comparação dos custos totais das soluções identificadas

Requisito	Solução	Sim	Não	Não se Aplica
A Solução encontra-se implantada em outro órgão ou entidade da	1	x		
	2	x		

Administração Pública Federal?	3	x		
A Solução está disponível no Portal do Software Público Brasileiro?	1			x
	2			x
	3			x
A Solução é um software livre ou software público?	1			x
	2			x
	3			x
A Solução é aderente às regulamentações da ICP-Brasil?	1			x
	2			x
	3			x
A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões MNI, e-MAG?	1			x
	2			x
	3			x
A solução observa as orientações, premissas e especificações do Moreq-Jus e e-Arq	1			x
	2			x
	3			x

1.11 Escolha da solução e justificativa

1.11.1 . A solução de reaproveitamento da infraestrutura existente no prédio atual da secretaria não pode ser aplicada por não comportar o aumento significativo da demanda calculada para o novo prédio sede conforme verifica-se pela análise feita no item 1.3. Além disso, durante o período de transição, no qual haverá o deslocamento das seções para a nova sede, ambos os prédios precisarão continuar funcionando simultaneamente.

1.11.2 . A solução de pesquisa em atas registradas por outros orgãos poderia ser aplicada, no entanto devido à quantidade de itens necessários e a variedade destes a busca poderia terminar na seleção de um grande número de atas. Essa complexidade coloca essa solução em segundo lugar dentre as alternativas identificadas.

1.11.3 . A solução de adquirir os itens necessários por meio da execução de processo licitatório próprio constitui-se uma alternativa viável por possibitar um maior controle sobre todas as etapas, acompanhando-as com maior nível de detalhes. Diante disso esta é a solução mais adequada.

1.12 Necessidades de adequação do ambiente para execução contratual

1.12.1 . Toda a adequação do ambiente já foi prevista durante o processo de projeto e construção estando o novo prédio sede adequado para receber todos os equipamentos descritos nesse documento.

Sustentação do Contrato

1. **Definição dos Recursos Humanos e Materiais**
   - 1.1. **Representante Técnico na licitação**
     - a. Apoiar o pregoeiro durante todo processo licitatório
     - b. Responder os questionamentos dos licitantes durante o certame**.**
   - 1.2. **Técnico de Infraestrutura**
     - a. Analisar se todos requisitos técnicos exigidos foram atendidos durante o processo de entrega da solução.
     - b. Monitorar a solução no estágio de produção.
     - c. Acionar o suporte de garantia quando necessário.
   - 1.3. **Equipe de Recebimento**
     - a. Monitorar a entrega da solução quanto ao prazo e os requisitos técnicos e administrativos.

2. **Definição das atividades de transição e encerramento do contrato**
   - 2.1. Após efetivada a entrega do objeto da contratação em perfeitas condições, conforme as especificações, quantidade, prazo e local, a fornecedora da solução deverá entregar catálogos, manuais, licenças dos sistemas operacionais, página impressa do sítio do fabricante na Internet ou quaisquer outros documentos que comprovem o atendimento das especificações técnicas.
   - 2.2. No caso de entrega parcial do objeto da contratação em função de substituição ou rescisão antecipada, ou sempre que houver descontinuidade ou alteração nos modelos de bens propostos, a fornecedora da solução também deverá entregar os documentos descritos no item 2.1 da sustentação do contrato.

Documento assinado digitalmente por:		
Joao Paulo de Araujo Bezerra 23/06/2017 11:43:39	Ernesto Leca Pinto 23/06/2017 11:50:37	Daniel Cesar Gurgel Coelho Ponte 02/08/2017 14:07:01

3. **Elaboração de estratégia de independência**

3.1. Não se aplica.

Documento assinado digitalmente por:		
Joao Paulo de Araujo Bezerra 23/06/2017 11:43:39	Ernesto Leca Pinto 23/06/2017 11:50:37	Daniel Cesar Gurgel Coelho Ponte 02/08/2017 14:07:01

Análise de Riscos

1. **Identificação dos Riscos**

1.1. **Riscos do processo de contratação**

a. Impugnação do Edital

Dano	Id	Ação Preventiva	Responsável
Frustração da contratação	1	Detalhar e esclarecer todos os itens do Termo de Referência	Equipe de planejamento
	Id	**Ação de contingência**	**Responsável**
		Corrigir o edital e realizar novo certame	Equipe de planejamento
Probabilidade de ocorrência: **Baixa**			

b. Licitação Deserta, fracassada ou anulada

Dano	Id	Ação Preventiva	Responsável
Frustração da contratação	1	Elaborar Termo de Referência sem definir especificações restritivas, demasiadamente rigorosas, sem a devida justificativa técnica de modo a prevenir vícios de legalidade.	Equipe de Planejamento
	2	Na elaboração do Termo de Referência não subestimar o preço	Equipe de Planejamento
	Id	**Ação de Contingência**	
	1	Adequação das exigências técnicas, mantendo-se os padrões de qualidade e alcance dos resultados pretendidos para a realização de nova licitação	Equipe de Planejamento
Probabilidade de ocorrência: **Baixa**			

1.2. **Riscos da Solução de TIC**

Documento assinado digitalmente por:		
Joao Paulo de Araujo Bezerra 23/06/2017 11:43:39	Ernesto Leca Pinto 23/06/2017 11:50:37	Daniel Cesar Gurgel Coelho Ponte 02/08/2017 14:07:01

a. Atraso na Entrega da Solução

Dano	Id	Ação Preventiva	Responsável
Impossibilidade, parcial ou total, da transferência das unidades do órgão para o novo prédio sede.	1	Definir data limite para entrega dos bens	Equipe de planejamento
	2	Gerenciar o cronograma de entrega dos bens	Equipe de Recebimento
	3	Estabelecer tabela de infrações contratuais no Termo de Referência	Equipe de Planejamento
	Id	**Ação de contingência**	**Responsável**
	1	Acionar o fornecedor com nova data limite para entrega e tomar medidas administrativas previstas na contratação	Equipe de Recebimento
	2	Verificar com área demandante o impacto na área de negócio	Equipe de Recebimento
Probabilidade de ocorrência: **Média**			

b. Entrega de Equipamento Incompatível (especificações)

Dano	Id	Ação Preventiva	Responsável
Impossibilidade, parcial ou total, da transferência das unidades do órgão para o novo prédio sede.	1	Verificar se o equipamento está de acordo com as especificações mínimas exigidas no ato de entrega para fins de ateste provisório	Equipe de recebimento
	Id	**Ação de contingência**	**Responsável**
	1	Solicitar ao fornecedor a subistituição do equipamento incompatível	Equipe de Recebimento
	2	Informar à administração sobre problemas contratuais de garantia por conta de equipamentos incompatíveis	Técnico de Infraestrutura
Probabilidade de ocorrência: **Baixa**			

c. Entrega de equipamento defeituoso

Dano	Id	Ação Preventiva	Responsável
Ineficácia na execução dos serviços prestados pelo	1	Verificar a integridade do equipamento no ato de entrega para fins de ateste provisório	Equipe de Recebimento

órgão	**Id**	**Ação de contingência**	**Responsável**
	1	Solicitar o fornecedor para a substituição do equipamento defeituoso	Equipe de Recebimento
	2	Verificar a integridade do equipamento entregue após chamado de garantia	Técnico de Infraestrutura
	3	Verificar as sanções cabíveis no caso de não atendimento da garantia conforme contratação	Administração
Probabilidade de ocorrência: **Baixa**			

d. Inadequação da Infraestrutura para instalação dos equipamentos

Dano	**Id**	**Ação Preventiva**	**Responsável**
Ineficácia na execução dos serviços prestados pelo órgão	1	Antecipar adequações de infraestrutura necessárias para a instalação da solução	Equipe de Planejamento/ Técnico de Infraestrutura
	Id	**Ação de contingência**	**Responsável**
	1	Solicitar à administração para realizar as adequações necessárias em caráter de urgência.	Técnico de Infraestrutura
	2	Pausar a instalação dos equipamentos até que as demandas de adequação sejam efetuadas.	Administração
Probabilidade de ocorrência: **Baixa**			

Conclusão dos Estudos Preliminares

1. Declaração de viabilidade da contratação.

Natal, 23 de Junho de 2017

Equipe de Planejamento da Contratação

Integrante Técnico:
João Paulo de Araújo Bezerra
SRI/CIT/STIC

Integrante Demandante:
Daniel César Gurgel Coelho Ponte
SRI/CIT/STIC

Integrante Administrativo:
Ernesto Leça Pinto
SCS/CMP/SAO

Documento assinado digitalmente por:		
Joao Paulo de Araujo Bezerra 23/06/2017 11:43:39	Ernesto Leca Pinto 23/06/2017 11:50:37	Daniel Cesar Gurgel Coelho Ponte 02/08/2017 14:07:01