ANEXO I

ESPECIFICAÇÃO TÉCNICA

1 - DO OBJETO

Prestação de serviços continuados de comunicação de dados entre as comarcas e demais unidades do Poder Judiciário de Santa Catarina e a sede do Tribunal, com instalação, configuração e manutenção de links da rede MPLS e de conexões de fibra óptica "ponto a ponto", além do fornecimento e configuração de equipamentos Fortinet necessários para implementação da rede SD-WAN com alta disponibilidade.

2 - DO SERVIÇO

1. A CONTRATADA deverá fornecer os serviços em todas as localidades informadas na forma dos subitens 9.3.1 e 9.3.2.1 do edital que forem acionadas durante a vigência do contrato, obrigatoriamente.
2. Cabe ao CONTRATANTE determinar a distribuição das velocidades nas localidades.
3. O CONTRATANTE pode requerer a mudança das velocidades das localidades.
4. O CONTRATANTE e a CONTRATADA manterão uma tabela associando as localidades e suas respectivas velocidades.
5. A CONTRATADA deverá disponibilizar, durante a vigência do contrato, o circuito de fibra ótica da última milha que chega em cada uma das unidades do PJSC indicadas por ocasião do credenciamento, os equipamentos para implementar os serviços de comunicação de dados MPLS, além dos equipamentos da Fortinet necessários para implementação da rede SD-WAN nas unidades a serem definidas pelo contratante, em quantidade proporcional ao número de links por ela instalados em relação ao número total de unidades existentes no PJSC;
6. A CONTRATADA deverá prestar os serviços de suporte técnico e manutenção dos equipamentos, a fim de garantir a alta disponibilidade e o bom funcionamento dos serviços contratados, em conformidade com os requisitos de qualidade de serviço e os acordos de nível de serviço;
7. A manutenção e reposição dos equipamentos e infraestrutura necessária, como cabos, conectores, adaptadores serão de responsabilidade da CONTRATADA;
8. O PJSC disponibilizará o espaço físico adequado, na sede do PJSC e nos demais fóruns das comarcas, onde ficarão os equipamentos de terminação;
9. A CONTRATADA deverá garantir sigilo e inviolabilidade das informações que eventualmente possa ter acesso durante os procedimentos de instalação e manutenção de seus equipamentos, bem como durante a operação do serviço;
10. Não serão permitidos pontos de concentração que possam estabelecer estrangulamento de tráfego ou interdependência de funcionamento entre as unidades do PJSC no backbone MPLS.
11. A rede MPLS das contratadas deve garantir a velocidade e o RTT contratados, sem que haja estrangulamento de tráfego em nenhum ponto da sua rede;

12. A topologia da rede de comunicação de dados utilizada será a full-mesh (topologia de rede na qual todos os nós se comunicam entre si indistintamente).

3 - DA INFRAESTRUTURA MÍNIMA REQUERIDA

1. A infraestrutura requerida será constituída no mínimo do ponto concentrador da rede MPLS e do acesso principal das comarcas e demais unidades, 2 Fortigates 100E, ou 2 Fortigates 200E em unidades específicas, que deverão funcionar em alta disponibilidade se comunicando com os concentradores da rede SD-WAN no PJSC e autenticados no Fortimanager.

2. Ponto Concentrador da rede: será o ponto de interconexão de rede entre a sede e as comarcas e demais unidades do PJSC.

3. A velocidade do ponto concentrador deverá ser igual a soma das velocidades dos links de cada operadora, multiplicado pelo coeficiente de aproveitamento. O Coeficiente de Aproveitamento é a variável que será aplicada na soma de todas as velocidades dos links de cada operadora, sendo este um valor que vai dizer quanto o link concentrador deverá ter de velocidade na sede do Poder Judiciário Catarinense. Inicialmente, será de 50%, podendo conforme necessidade, ir aumentando de 10 em 10 até atingir 100%, ou seja, 50,60,70,80,90,100.

4. Velocidade de download igual a de upload para todos os circuitos MPLS fornecidos;

5. Monitoramento 24 x 7;

6. O Acesso Principal das comarcas e demais unidades: interligará as comarcas e demais unidades do PJSC entre si e ao Ponto Concentrador de rede, via MPLS.

7. Para a implementação da rede SD-WAN em cada uma das unidades deverá ser instalado 2 Fortigates 100E funcionando em HA (alta disponibilidade), ou 2 Fortigates 200E em unidades específicas. Os 2 equipamentos deverão ser fornecidos pela mesma empresa credenciada. Atualmente temos apenas um equipamento Fortigate 100E implantado, ou Fortigate 200E, e a Seção de Administração de Redes irá em conjunto com as operadoras planejar a instalação do segundo Fortigate. O número de Fortigates por empresa será proporcional ao número de links instalados na razão de unidades existentes no PJSC, conforme demonstrado abaixo:

Fornecedoras	1o. Fortigate
ALGAR	92
ALT	9
Unifique	6
MhNet	30
OI	0

Atualmente são 140 unidades, o que gera a necessidade de 280 Fortigates. Baseado nisso, segue abaixo o escopo atual da quantidade de Fortigates a serem fornecidos pelas empresas credenciadas.

Operadora	Contagem de Links Ativos	% do total de links (355)	% do total de links sobre o total de Fortigates necessários (280)	Número de Fortigates a serem Instalados
ALGAR	91	26	72	-20
ALT	51	14	40	31
MHNET	40	11	32	2
OI	106	30	84	84
UNIFIQUE	67	19	53	47
(vazio)		0	0	
Total Geral	355			

8. No ponto concentrador deverá ser instalado um roteador concentrador MPLS que deverá ser conectado ao equipamento concentrador da rede SD-WAN, Fortinet 1500 D .

9. Uma única operadora credenciada irá fornecer os 2 equipamentos concentradores da rede SD-WAN, Fortinet 1500D, que funcionam em HA (alta disponibilidade). Somente esta empresa estará apta a receber a mensalidade respectiva a estes equipamentos, item 31 ta tabela de preço de referência.

10. Não serão aceitos equipamentos com end-of-sale e end-of-life anunciados pelo fabricante.

4 – DAS CARACTERÍSTICAS TÉCNICAS

1. O acesso físico do acesso principal desde o ponto de presença da CONTRATADA até a sede do PJSC deverá ser efetuado exclusivamente de fibra óptica e não poderá utilizar redes intermediárias compartilhadas;

2. A CONTRATADA é responsável pela entrega do circuito até o rack da sala de informática, podendo utilizar a estrutura interna da comarca para a passagem de fibra óptica.

3. O acesso físico do ponto de presença da CONTRATADA até aos demais sites do PJSC deverá ser efetuado exclusivamente por meio de fibra óptica.

4. O equipamento no ponto de presença que recebe o link deve ser próprio da CONTRATADA;

5. Não será permitida, em hipótese alguma, a utilização de equipamentos com tecnologia de transmissão via satélite ou rádio, pois este tipo de tecnologia é muito suscetível às intempéries, podendo ocasionar problemas na transmissão de dados, vídeo e voz, estes dois últimos necessitando de extrema confiabilidade para o bom funcionamento dos serviços.

6. A Operadora deverá entregar o link até o Rack da sala de informática.

7. No momento da ativação do circuito, as localidades deverão ser vistoriadas, a fim de se mensurar a necessidade de obras civis para execução da rede interna, quando necessária. Se forem encontrados problemas que necessitem de obras civis, a CONTRATADA deverá submeter ao PJSC justificativa por escrito, que será submetida a Diretoria de Engenharia.

8. A rede deverá utilizar Multiprotocol Label Switching (MPLS), para os circuitos dos sites do interior, para interligação com a sede do PJSC;

9. A conexão na rede MPLS é feita por meio de roteadores, denominados Customer Premises Equipment (CPE) que deverão ser instalados no rack na unidade, um por localidade. A exceção poderá ocorrer quando a operadora for a proprietária do Fortigate na unidade e utilizá-lo diretamente como conexão do seu circuito MPLS, dispensando assim o uso do roteador.

10. Os links de comunicação MPLS deverão permitir a comunicação de todas as redes locais entre si através da nuvem MPLS;

11. A rede deve ser *full mesh*, ou seja, o tráfego entre 2 links MPLS deve transitar diretamente entre estes, sem intermediários;

12. A CONTRATADA deverá garantir em 100% do tempo a velocidade mínima contratada;

13. O link deverá operar em *full duplex*;

14. Deve suportar MTU de 1500 bytes entre dois pontos quaisquer;

15. As velocidades de transmissão nos dois sentidos, emissão e recepção, deverão ser simétricas;

16. O atraso entre o roteador de concentração dos circuitos e qualquer outro ponto da rede não poderá ser superior a 100 ms, considerando a métrica RTT (Round Trip Time). Este valor deverá ser aferido por medições efetuadas através do envio de mensagens ICMP Echo Request, com tamanho de pacote de 64 bytes. Essa condição será determinante para o aceite do link.

17. O percentual de pacotes recebidos com erro na Rede não poderá ser superior a 2%. Este valor refere-se à quantidade de pacotes cuja verificação de CRC resultou em erros em relação ao total de pacotes transmitidos no enlace. Essa condição será determinante para o aceite do link.

18. Tanto o delay quanto a perda de pacotes serão monitorados após a instalação e caso a situação gere degradação do serviço serão imputadas sanções na mensalidade como sendo de indisponibilidade do link.

19. A arquitetura de roteamento será definida em conjunto pelo CONTRATANTE e CONTRATADA;

20. Deverá utilizar o protocolo iBGP;

21. Todo o roteamento necessário para a comunicação através da rede MPLS é de responsabilidade do CONTRATADA, assim como a sua integração com as redes dos centros de dados;

22. A CONTRATADA deverá planejar, implementar e gerenciar a operação do roteamento;

23. A rede deverá ser isolada de fim a fim de qualquer outra entidade, ou seja, apenas o tráfego do CONTRATANTE é permitido entrar ou sair da rede;

24. A CONTRATADA garantirá o sigilo e a inviolabilidade das informações que possa ter acesso durante os procedimentos de instalação e manutenção de seus equipamentos, bem como durante toda a prestação do serviço;

25. A CONTRATADA não poderá implementar nenhum tipo de filtro de pacotes que possa incidir sobre o tráfego originado ou destinado ao CONTRATANTE, a menos que tenha expressa concordância do CONTRATANTE;

26. A CONTRATADA deverá manter os sistemas operacionais, firmwares e outros softwares utilizados atualizados, devidamente licenciados e com suporte ao software pelo fabricante para entrega do serviço contratado, a fim de manter sua segurança, confiabilidade e níveis de serviço exigidos, bem como durante todo o período da contratação.

27. Caso seja necessário, os circuitos MPLS deverão realizar a priorização de pacotes (QoS) conforme classes de serviços e aplicações definidas abaixo:

1. Classe de serviço de voz, onde trafegarão as aplicações de voz através de endereços IPs e portas a serem definidos pelo PJSC;

2. Classe de serviço de vídeo, onde trafegarão as aplicações de vídeo através de endereços IPs e portas a serem definidos pelo PJSC;

3. Classe de serviço de Dados Críticos, onde trafegarão as aplicações críticas através de endereços IPs e portas a serem definidos pelo PJSC;

4. Classe de serviço de Dados Prioritários, onde trafegarão as aplicações que exigem uma certa prioridade através de endereços IPs e portas a serem definidos pelo PJSC;

5. Classe de serviço de Dados de Baixa Prioridade, onde trafegarão as demais aplicações de rede (e-mail, internet, etc.) através de endereços IPs e portas a serem definidos pelo PJSC.

6. As frações de banda não utilizadas na Classe de Serviço de Vídeo e na Classe de Serviço de Voz deverão ser alocadas, dinamicamente, para a Classe inferior;

26.1. Caberá ao CONTRATANTE a definição das bandas que serão utilizadas em cada classe de serviço, por circuito, podendo dispor, dentro do limite de velocidade do circuito, os valores mais adequados as suas necessidades. As frações de banda não utilizadas na Classe de Serviço de Vídeo e na Classe de Serviço de Voz deverão ser alocadas, dinamicamente, para a Classe inferior. O PJSC poderá, a qualquer tempo, solicitar à CONTRATADA a alteração das aplicações (portas) e endereços IPs priorizados em cada classe de serviço, sem nenhum custo adicional;

27. Os equipamentos Fortinet deverão apresentar a mesma configuração em todas as unidades, sendo cada empresa responsável pela configuração dos respectivos equipamentos. Em cada unidade do PJSC deverão existir 2 Fortigates 100 E da propriedade de uma única operadora.

28. Todo equipamento Fortinet instalado será monitorado pelo Central Manager da empresa credenciada responsável, até que o PJSC consiga montar a sua própria estrutura com um FortiManager próprio. A partir deste momento, a Seção de Administração de Redes irá em conjunto com a CONTRATADA planejar a migração dos equipamentos Fortinet para o Central Manager do PJSC.

29. A Seção de Administração de Redes terá a liberdade de solicitar a configuração ou liberação de acesso aos equipamentos que achar necessário para suas atividades sem custo adicional, como também configurações que se fizerem necessário.

30. Todos os equipamentos deverão permitir acesso para monitoramento das ferramentas internas da Seção de Administração de Redes, tais como PRTG, Zabbix ou ferramentas internas, para isso será necessário configurar o SNMP nos equipamentos com community padrão a ser definida, em quaisquer das interfaces que se faça necessário o monitoramento e permissão de leitura ou de escrita, quando se fizer necessário.

31. Os circuitos MPLS deverão realizar o roteamento IP Multicast conforme especificação de endereçamento do PJSC devendo ser configurados no momento que se fizer necessário.

32. O PJSC poderá, a qualquer tempo, solicitar à CONTRATADA a alteração do roteamento e endereçamento IP Multicast, sem nenhum custo adicional que deve executado num prazo de 5 dias úteis.

33. A solução SD-WAN também deverá estar apta a realizar Multicast. Essas necessidades serão definidas ao longo do contrato e a CONTRATADA deverá fazer as configurações necessárias.

34. O CONTRATANTE deverá ter acesso aos equipamentos (roteadores e Fortigates) através de acesso SSH.

35. Após a implantação da rede, onde toda a configuração será feita em conjunto com a equipe técnica do PJSC, a CONTRATADA deverá efetuar todas as configurações necessárias e solicitadas pelo PJSC em até 5 dias úteis, caso a CONTRATADA não consiga deverá apresentar razões técnicas para o atraso, podendo ou não ser acatadas pela Seção de Administração de Redes.

5 – DAS CARACTERÍSTICAS TÉCNICAS DOS EQUIPAMENTOS A SEREM FORNECIDOS PELA CONTRATADA

5.1 - Especificação Mínima do Roteador nas Comarcas

1. Possuir pelo menos 2 (duas) interfaces Ethernet 1000Base-T;

2. Possibilitar a configuração dinâmica de portas por software, permitindo a definição de portas ativas/inativas;

3. Implementar VLANs por porta;

4. Implementar VLANs compatíveis com o padrão IEEE 802.1q;

5. Implementar mecanismo de seleção de quais VLANs serão permitidas através de trunk 802.1q;

6. Possuir porta de console para ligação, direta e através de modem, de terminal RS-232 para acesso à interface de linha de comando. Poderá ser fornecida porta de console com interface USB;

7. Possuir configuração de CPU e memória (RAM e Flash) suficiente para a implementação de todas as funcionalidades descritas nesta especificação;

8. Permitir ser montado em rack padrão de 19 (dezenove) polegadas, incluindo todos os acessórios necessários;

9. Possuir LEDs para a indicação do status das portas e atividade;

10. Implementar os padrões abertos de gerência de rede SNMPv2c e SNMPv3, incluindo a geração de traps;

11. Possibilitar a obtenção da configuração do equipamento através do protocolo SNMP;

12. Possibilitar a obtenção via SNMP de informações de capacidade e desempenho da CPU, memória, portas e tráfego;

13. Permitir o gerenciamento via CLI e Web, utilizando SSH e HTTPS;

14. O equipamento deve suportar a configuração com um único endereço IP para gerência e administração, para uso dos protocolos: SNMP, NTP, HTTPS, SSH, Telnet, TACACS+ e RADIUS, provendo identificação gerencial única ao equipamento de rede;

15. Implementar Telnet/SSH para acesso à interface de linha de comando;

16. Permitir a atualização remota do sistema operacional e arquivos de configuração utilizados no equipamento via interfaces ethernet e serial;

17. Deve permitir a atualização de sistema operacional através do protocolo TFTP ou FTP;

18. Suportar protocolo SSH para gerenciamento remoto, implementando pelo menos o algoritmo de encriptação de dados 3DES;

19. Permitir a gravação de log externo (syslog). Deve ser possível definir o endereço IP de origem dos pacotes Syslog gerados pelo roteador;

20. 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;

21. Possuir ferramentas para depuração e gerenciamento em primeiro nível, tais como debug, trace, log de eventos;

22. Deve suportar IPv6;

23. Implementar NAT (Network Address Translation);

24. A informação coletada deve ser automaticamente exportável em intervalos pré-definidos através de um protocolo ipfix (Net Flow ou SFlow ou JFlow ou HFlow) padronizado;

25. Implementar DHCP Relay e DHCP Server;

26. Implementar roteamento estático;

27. Implementar roteamento dinâmico RIPv2 (RFC 2453 e 2082);

28. Implementar protocolo de roteamento dinâmico OSPF (RFC 2328, 3101, 3137, 3623 e 2370);

29. Implementar protocolo de roteamento BGPv4 (RFC 4271, 3065, 4456, 1997, 1965, 1966, 4897, 2858 e 2385);

30. Permitir o roteamento nível 3 entre VLANs;

31. Permitir a virtualização das tabelas de roteamento camada 3. As tabelas virtuais deverão ser completamente segmentadas;

32. Suporte ao protocolo de Tunelamento GRE (General Routing Encapsulation - RFCs 2784), contemplando, no mínimo, os seguintes recursos:

33. Suporte a QoS (qualidade de serviço) - deve ser possível a cópia da informação de classificação de tráfego existente no cabeçalho do pacote original para os pacotes transportados com encapsulamento GRE;

34. Implementar roteamento baseado em origem, com possibilidade de definição do próximo salto camada 3, baseado em uma condição de origem;

35. Implementar filtragem de pacotes (ACL - Access Control List), para IPv4;

36. Implementar listas de controle de acesso (ACLs), para filtragem de pacotes, baseadas em endereço IP de origem e destino, portas TCP e UDP de origem e destino e flags TCP;

37. Proteger a interface de comando do equipamento através de senha;

38. Permitir a criação de listas de acesso baseadas em endereço IP para limitar o acesso ao switch via Telnet, SSH e SNMP. Deve ser possível definir os endereços IP de origem das sessões Telnet e SSH;

39. Permitir a inserção de um certificado digital PKI para autenticação do protocolo SSH e Túneis IPSEC;

40. Implementar mecanismos de AAA (Authentication, Authorization e Accounting) com garantia de entrega;

41. Implementar a criptografia dos pacotes de forma totalmente transparente e automática, sem a alteração dos cabeçalhos incluindo endereços IP de origem e destino, e portas de origem e destino;

42. Suportar funcionalidades de QoS de “Traffic Shaping” e “Traffic Policing”.

43. Deve ser possível a especificação de banda por classe de serviço;

44. Para os pacotes que excederem a especificação, deve ser possível configurar ações tais como: transmissão do pacote sem modificação, transmissão com remarcação do valor de DSCP, descarte do pacote;

45. Implementar Multicast;

46. Deverá suportar a velocidade contratada do link instalado, com throughput adequado.

47. Deverá apresentar usuário específico para acesso

5.2 - Especificação Mínima do Roteador Concentrador no Tribunal de Justiça de SC

1. Possuir pelo menos 2 (duas) interfaces Ethernet 1000Base-T;

2. Possibilitar a configuração dinâmica de portas por software, permitindo a definição de portas ativas/inativas;

3. Implementar VLANs por porta;

4. Implementar VLANs compatíveis com o padrão IEEE 802.1q;

5. Implementar mecanismo de seleção de quais VLANs serão permitidas através de trunk 802.1q;

6. Possuir porta de console para ligação, direta e através de modem, de terminal RS-232 para acesso à interface de linha de comando. Poderá ser fornecida porta de console com interface USB;

7. Possuir configuração de CPU e memória (RAM e Flash) suficiente para a implementação de todas as funcionalidades descritas nesta especificação;

8. Permitir ser montado em rack padrão de 19 (dezenove) polegadas, incluindo todos os acessórios necessários;

9. Possuir LEDs para a indicação do status das portas e atividade;

10. Implementar os padrões abertos de gerência de rede SNMPv2c e SNMPv3, incluindo a geração de traps;

11. Possibilitar a obtenção da configuração do equipamento através do protocolo SNMP;

12. Possibilitar a obtenção via SNMP de informações de capacidade e desempenho da CPU, memória, portas e tráfego;

13. Permitir o gerenciamento via CLI e Web, utilizando SSH e HTTPS;

14. O equipamento deve suportar a configuração com um único endereço IP para gerência e administração, para uso dos protocolos: SNMP, NTP, HTTPS, SSH, Telnet, TACACS+ e RADIUS, provendo identificação gerencial única ao equipamento de rede;

15. Implementar Telnet/SSH para acesso à interface de linha de comando;

16. Permitir a atualização remota do sistema operacional e arquivos de configuração utilizados no equipamento via interfaces ethernet e serial;

17. Deve permitir a atualização de sistema operacional através do protocolo TFTP ou FTP;

18. Suportar protocolo SSH para gerenciamento remoto, implementando pelo menos o algoritmo de encriptação de dados 3DES;

19. Permitir a gravação de log externo (syslog). Deve ser possível definir o endereço IP de origem dos pacotes Syslog gerados pelo roteador;

20. 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;

21. Possuir ferramentas para depuração e gerenciamento em primeiro nível, tais como debug, trace, log de eventos;

22. Deve suportar IPv6;

23. Implementar NAT (Network Address Translation);

24. A informação coletada deve ser automaticamente exportável em intervalos pré-definidos através de um protocolo ipfix (Net Flow ou SFlow ou JFlow ou HFlow) padronizado;

25. Implementar DHCP Relay e DHCP Server;

26. Implementar roteamento estático;

27. Implementar roteamento dinâmico RIPv2 (RFC 2453 e 2082);

28. Implementar protocolo de roteamento dinâmico OSPF (RFC 2328, 3101, 3137, 3623 e 2370);

29. Implementar protocolo de roteamento BGPv4 (RFC 4271, 3065, 4456, 1997, 1965, 1966, 4897, 2858 e 2385);

30. Permitir o roteamento nível 3 entre VLANs;

31. Permitir a virtualização das tabelas de roteamento camada 3. As tabelas virtuais deverão ser completamente segmentadas;

32. Suporte ao protocolo de Tunelamento GRE (General Routing Encapsulation - RFCs 2784), contemplando, no mínimo, os seguintes recursos:

33. Suporte a QoS (qualidade de serviço) - deve ser possível a cópia da informação de classificação de tráfego existente no cabeçalho do pacote original para os pacotes transportados com encapsulamento GRE;

34. Implementar roteamento baseado em origem, com possibilidade de definição do próximo salto camada 3, baseado em uma condição de origem;

35. Implementar filtragem de pacotes (ACL - Access Control List), para IPv4;

36. Implementar listas de controle de acesso (ACLs), para filtragem de pacotes, baseadas em endereço IP de origem e destino, portas TCP e UDP de origem e destino e flags TCP;

37. Proteger a interface de comando do equipamento através de senha;

38. Permitir a criação de listas de acesso baseadas em endereço IP para limitar o acesso ao switch via Telnet, SSH e SNMP. Deve ser possível definir os endereços IP de origem das sessões Telnet e SSH;

39. Permitir a inserção de um certificado digital PKI para autenticação do protocolo SSH e Túneis IPSEC;

40. Implementar mecanismos de AAA (Authentication, Authorization e Accounting) com garantia de entrega;

41. Implementar a criptografia dos pacotes de forma totalmente transparente e automática, sem a alteração dos cabeçalhos incluindo endereços IP de origem e destino, e portas de origem e destino;

42. Suportar funcionalidades de QoS de “Traffic Shaping” e “Traffic Policing”.

43. Deve ser possível a especificação de banda por classe de serviço;

44. Para os pacotes que excederem a especificação, deve ser possível configurar ações tais como: transmissão do pacote sem modificação, transmissão com remarcação do valor de DSCP, descarte do pacote;

45. Implementar Multicast quando solicitado;

46. Deverá suportar a soma de todas as velocidades dos links instalados da operadora em questão, com throughput adequado.

5.3 Especificação do Fortigate 100 E nas comarcas

Interfaces	
1. Porta USB	5. 2x Portas GE RJ45 HA
2. Porta de Console	6. 14x GE RJ45 Portas
3. 2x GE MGMT RJ45/DMZ Portas	7. 2x GE RJ45/Shared SFP Media Pares
4. 2x GE RJ45 Portas WAN	

ESPECIFICAÇÕES	
Especificações de Hardware	
GE RJ45 Portas de Switch	14
GE RJ45 Gestão/HA/DMZ Portas	1/2/1
GE SFP Slots	-
GE RJ45 PoE/+ Portas	-
GE RJ45 Portas WAN	2
GE RJ45 ou Portas SFP Compartilhados	2
Porta USB	1
Porta de Console	1
Armazenamento interno	-
Incluído Transceptores	0
O Desempenho do sistema de Empresa-Mix de Tráfego	
IPS Throughput 2	500 Mbps
Throughput NGFW 2, 4	360 Mbps
Proteção Contra ameaças Throughput 2, 5	250 Mbps
O Desempenho do sistema	
Firewall de Transferência (1518/512/64 byte de pacotes UDP)	7.4 Gbps
Firewall de Latência (64 byte de pacotes UDP)	3 us
Throughput de Firewall (Pacotes Por Segundo)	6.6 Mpps
Sessões simultâneas (TCP)	2 milhões
Novas Sessões/Segundo (TCP)	30,000
Políticas de Firewall	10,000
IPsec VPN Throughput (512 byte) 1	4 Gbps
Gateway-to-Gateway VPN IPsec Túneis	2,000
Cliente-to-Gateway VPN IPsec Túneis	10,000
SSL-VPN Throughput	250 Mbps
Usuários simultâneos SSL-VPN (Máxima Recomendada, o Túnel Do Modo)	500
Throughput de Inspeção SSL (IPS, avg. HTTPS) 3	130 Mbps
Inspeção SSL CPS (IPS, avg. HTTPS) 3	130
Sessão Simultânea de Inspeção SSL (IPS, avg. HTTPS) 3	125,000
Aplicação de Controle de Vazão (HTTP 64 K) 2	1 Gbps
CAPWAP Throughput (HTTP 64 K)	1.5 Gbps
Domínios virtuais (Padrão/Máximo)	10/10
Número máximo de Switches Suportados	24
Número máximo de FortiAPs (Total/Modo Túnel)	64/32
Número máximo de FortiTokens	5,000
Número máximo de Registrado FortiClients	600

Configurações de alta Disponibilidade	Active / Active, Active / Passive, Clustering
Dimensões	
Altura x Largura x Comprimento (polegadas)	1.75 x 17 x 10
Altura x Largura x Comprimento (mm)	44.45x432x254
Peso	Montagem Em Rack, 1 RU
Fator de forma	£ 7.28 (3.3 kg)

Ambiente	
Tensão Elétrica	100–240V AC, 50–60 Hz
Máxima Corrente	100V / 0.52A, 240V / 0.22A
Consumo de Energia (Média/ Máximo)	23.0 W / 28.6 W; 51.9 VA
Dissipação de Calor	97.6 BTU/h

5.3.1 - Definições de Operação nas Unidades do PJSC

1. O equipamento Fortigate 100E poderá agregar até 4 circuitos físicos, de tecnologia MPLS ou similar, disponibilizados por fornecedores distintos, conectados a uma mesma estrutura de roteamente, em um único canal lógico. Dessa forma, terá a possibilidade de redundância e failover para todos os acessos físicos, permitindo que quando um dos links apresentar falhas, o outro acesso ligado a estrutura assuma a transmissão dos dados.

2. O equipamento Fortigate 100E deverá executar o balanceamento de tráfego entre os links ativos, baseado em volumetria, com roteamento inteligente para a priorização de tráfego.

3. Controle de caminho automático, baseado em políticas previamente aplicadas, com recursos para comutação dinâmica dos caminhos, selecionando o melhor caminho, no mínimo, a partir dos seguintes parâmetros, simultâneos ou não:

1. tipo de aplicação;
2. prioridade de negócio;
3. banda;
4. latência
5. jitter;
6. perda de pacotes.

4. A prorização do tráfego baseado em aplicação deverá ser feito pelas operadoras credenciadas sem custo adicional ao PJSC e a empresa terá o prazo de no máximo 5 dias úteis para execução desta configuração, caso a CONTRATADA não consiga deverá apresentar razões técnicas para o atraso, podendo ou não ser acatadas pela Seção de Administração de Redes.

5. Implementação de segurança fim-a-fim, utilizando solução de criptografia para fornecer, de maneira automática, proteção às redes WANs privadas que transitam por redes públicas compartilhadas;

6. Prover visibilidade fim-a-fim dos fluxos de comunicação das aplicações sobre a rede SD-WAN;

7. Prover visibilidade do desempenho da rede em tempo real, baseada nas aplicações e nos parâmetros de uso de banda, perda de pacote e latência;

8. Prover visualização de todas as configurações, políticas e status dos terminais da solução SD-WAN;

9. Preservar todas as licenças permanentes necessárias para suportar os requisitos de SD-WAN, de modo que todas as funções sejam plenamente atendidas.

5.4 Especificação do Fortigate 200 E para unidades ponto a ponto

Especificações de Hardware

Produto	**FORTIGATE 200E**
GE RJ45 WAN Interfaces	2
GE RJ45 Management/HA Ports	2
GE RJ45 Ports	14
GE SFP Slots	4
USB (Client / Server)	1/1
Console (RJ45)	1
Local Storage	-
Included Transceivers	0

Performance do Sistema

IPS Throughput 2	2.2 Gbps
NGFW Throughput 2, 4	1.8 Gbps
Threat Protection Throughput 2, 5	1.2 Gbps
Firewall Throughput(1518 / 512 / 64 byte UDP packets)	20 / 20 / 9 Gbps
Firewall Latency (64 byte UDP packets)	3 µs
Firewall Throughput (Packets Per Second)	13.5 Mpps
Concurrent Sessions (TCP)	2 Million
New Sessions/Second (TCP)	135,000
Firewall Policies	10,000
IPsec VPN Throughput (512 byte) 1	9 Gbps
Gateway-to-Gateway IPsec VPN Tunnels	2,00
Client-to-Gateway IPsec VPN Tunnels	10,00
SSL-VPN Throughput	900 Mbps
Concurrent SSL-VPN Users	500
SSL Inspection Throughput (IPS, avg. HTTPS) 3	820 Mbps
SSL Inspection CPS (IPS, avg. HTTPS) 3	1,000
SSL Inspection Concurrent Session (IPS, avg. HTTPS) 3	240,000
Application Control Throughput (HTTP 64K) 2	3.5 Gbps

CAPWAP Throughput (1444 byte, UDP)	1.5 Gbps
Virtual Domains (Default / Maximum)	10/10
Maximum Number of FortiSwitches Supported	24
Maximum Number of FortiAPs(Total / Tunnel Mode)	128 / 64
Maximum Number of FortiTokens	5,000
Maximum Number of Registered FortiClients	600
High Availability Configurations	Active / Active, Active / Passive, Clustering

5.5 Especificação do Fortigate 1500 D no Tribunal de Justiça de SC

Interfaces e Módulos

Produto	**FG-1500D**
10 GE SFP+ Slots	8
GE SFP Slots	16
10 GE RJ45 Ports	-
GE RJ45 Ports	16
GE RJ45 Gerência / HA Ports	2
USB Ports (Client / Server)	1/1
Console	1
Armazenamento Onboard	2x 240 GB
Transceivers	2x SFP + (SR 10GE)

Performance do Sistema

Produto	**FG-1500D**
IPv4 Firewall Throughput (1518 / 512 / 64 byte, UDP)	80 / 80 / 55 Gbps
IPv6 Firewall Throughput (1518 / 512 / 86 byte, UDP)	80 / 80 / 55 Gbps
Firewall Latency (64 byte, UDP)	3 µs
Firewall Throughput (Packet per Second)	82,5 Mpps
Concurrent Sessions (TCP)	12 Mil
New Sessions/Second (TCP)	300.000
Firewall Policies	100.000
IPsec VPN Throughput (512 byte)	50 Gbps
Gateway-to-Gateway IPsec VPN Tunnels	20.000
Client-to-Gateway IPsec VPN Tunnels	50.000
SSL-VPN Throughput	4 Gbps

Concurrent SSL-VPN Users (Recommended Maximum)	10.000
IPS Throughput (HTTP / Enterprise Mix)	15 / 13 Gbps
SSL Inspection Throughput	10,5 Gbps
Application Control Throughput	12 Gbps
NGFW Throughput	7 Gbps
Threat Protection Throughput	5 Gbps
CAPWAP Throughput	20 Gbps
Virtual Domains (Default / Maximum)	10 / 250
Maximum Number of FortiAPs (Total / Tunnel)	4.096 / 1.024
Maximum Number of FortiTokens	5.000
Maximum Number of Registered Endpoints	8.000
High Availability Configurations	Active-Active, Active-Passive, Clustering

5.6 Em relação a todos os equipamentos acima especificados, deverão ser observadas as seguintes exigências:

1. A CONTRATADA deverá fornecer, instalar, configurar e manter todos os equipamentos necessários para a operação de todos os canais de comunicação descritos no contrato e seus anexos;

2. Os equipamentos ofertados devem possuir capacidade de velocidade e processamento compatível com o circuito disponibilizado;

3. O PJSC deverá ter acesso à configuração de todos os equipamentos e acesso a todos os comandos de diagnóstico a serem previamente definidos;

4. A CONTRATADA deverá configurar nos equipamentos uma comunidade SNMP de leitura definida pelo PJSC, para que esta possa monitorar os circuitos e equipamentos disponibilizados;

5. O CONTRATANTE deverá ter acesso aos equipamentos (roteadores e Fortigates) através de acesso SSH;

6. Caso necessite, o CONTRATANTE poderá solicitar acesso aos equipamentos com a permissão (leitura/escrita) que achar necessário.

7. A construção da topologia de rede será feita em conjunto, com a equipe técnica da CONTRATANTE e da CONTRATADA. Caso haja interesse do CONTRATANTE, as demais empresas contratadas no presente credenciamento poderão ser envolvidas para ajustes dos enlaces de rede.

8. A configuração inicial e a manutenção da estrutura de configuração da rede lógica serão realizadas pela CONTRATADA que colocou o equipamento na localidade do CONTRATANTE. O CONTRATANTE deverá ter acesso total e irrestrito às configurações lógicas do equipamento, podendo em comum acordo alterar suas configurações para atender demanda iminente ou, ainda, a qualquer momento, solicitar à CONTRATADA para que o faça com prazo de 24 horas para cada localidade. Sendo uma configuração ampla, que atinja toda a rede do Poder Judiciário, a contratada terá o prazo

máximo de 21 dias úteis para efetivar as alterações, cabendo à CONTRATADA informar a programação de realização das mudanças pretendidas.

9. A CONTRATADA somente poderá retirar o equipamento da localidade atendida e o equipamento concentrador a pedido do CONTRATANTE, ao final do contrato ou quando houver acordo entre as partes, sob pena de indenizar o CONTRATANTE por possíveis prejuízos decorrentes de despesas não previstas, com outras operadoras e pela necessidade de adequações próprias, quando for feito uso exclusivamente pelo equipamento instalado.

10. A CONTRATADA somente poderá retirar os equipamentos concentradores ao final do contrato ou quando houver acordo entre as partes, sob pena de indenizar o CONTRATANTE por possíveis prejuízos decorrente de despesas não previstas, com outras operadoras e pela necessidade de adequações próprias, quando for feito uso exclusivamente pelo equipamento instalado. A partir do pedido de retirada, a CONTRATADA somente poderá retirar os equipamentos após 24 meses decorridos ou quando solicitado expressamente pelo PJSC.

11. A CONTRATADA deverá garantir que o equipamento concentrador da rede MPLS atenderá a capacidade dos links contratados, mesmo em caso de aumento ou diminuição de banda e de aumento ou diminuição do quantitativo dos circuitos, garantindo assim o funcionamento adequado da solução.

12. A CONTRATADA deverá garantir que o equipamento concentrador da rede SD-WAN atenderá a capacidade da rede, mesmo em caso de aumento das unidades, garantindo assim o funcionamento adequado da solução.

6 - DO MONITORAMENTO

Obrigações da CONTRATADA no monitoramento:

1. Disponibilizar um Portal de Gerência para o monitoramento “on-line” do serviço fornecido, através da Web, incluindo informações sobre o desempenho, taxa de erros e utilização dos links, para as linhas com tecnologia MPLS e circuito de acesso dedicado à internet. Este portal deverá ser apresentado previamente a Diretoria de Tecnologia da Informação - Divisão competente, para validação. Feito isto será dado o aceite do portal.

2. Oferecer e comprovar, através de relatórios gráficos mensais de desempenho (banda/disponibilidade), a garantia de largura de banda mínima contratada, durante o período de vigência do contrato;

3. Supervisionar, através de monitoração permanente, a disponibilidade do circuito, bem como a identificação e correção de falhas (gerência proativa);

4. Efetuar testes de verificação de qualidade da conexão, sempre que houver solicitação do PJSC, sem custos adicionais.

5. As CONTRATADAS deverão manter uma infraestrutura própria de gerenciamento de redes e serviços com capacidade para gerenciamento de todos os circuitos e de todos os serviços.

6. A Gerência das CONTRATADAS deverá operar 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana, todos os dias do ano;

7. Os chamados técnicos só poderão ser encerrados por um técnico da DTI, em conjunto com a Central de Atendimento, que deverá entrar em contatado com a DTI, para

encerrar os chamados solucionados. Não será admitido o fechamento do chamado técnico por técnicos das unidades do PJSC;

8. O acompanhamento da qualidade dos serviços da rede, acompanhamento dos chamados e do SLA estabelecido, será feito através de relatórios disponibilizados pela CONTRATADA;

9. Mensalmente, ao encaminhar suas faturas, a CONTRATADA deverá também apresentar um relatório ao PJSC já definido na minuta contratual.

10. Devem ser configurados em todos os equipamentos de rede no mínimo duas comunidades SNMP, de leitura, para controle interno do PJSC.

11. Todos os roteadores devem fornecer informações do tráfego de rede via Net Flow ou SFlow ou JFlow ou HFlow ou semelhante.

12. As instalações iniciais serão pagas uma única vez, a mensalidade dos circuitos e suas respectivas classes de serviço será paga após a instalação inicial. Entende-se como instalação inicial a instalação do circuito e os serviços associados conforme tabela em anexo.

13. A implementação ou configuração de classe de serviço seja de voz, seja de vídeo, deverá estar instalada em um prazo não superior a 5 dias, a partir da solicitação do PJSC. Caso não aconteça no prazo citado, ocorrerá redução do pagamento conforme as regras de indisponibilidade de circuito, além da aplicação de sanções cabíveis;

14. A CONTRADADA deverá disponibilizar acesso remoto, somente leitura, via telnet e/ou ssh, à console de gerenciamento dos fortigates, roteadores instalados nos fóruns e também no roteador concentrador instalado na sede do PJSC, devendo ser possível executar comandos de verificação de conectividade como ping, traceroute, listagem das tabelas de mac-address, arp e roteamento assim como listagem de todas as configurações necessárias para o funcionamento do QoS e Multicast" e demais comandos que se façam necessários;

15. Qualquer mudança na configuração deverá ser feita através de abertura pelo 0800, e contato com o consultor, tendo como prazo máximo 10 dias úteis nos casos não especificados;

16. Em casos de erro do técnico da Operadora de habilitação de serviços que não estejam contratados, como por exemplo habilitação do serviço de “DHCP”, deverá ser permitida abertura de chamado através de help desk 0800 e o tempo de resolução do problema deverá ser o mesmo de um chamado normal, cabendo multas conforme previsto em caso de não atendimento.

17. Os equipamentos Fortigate da CONTRATADA deverão inicialmente ser monitorados pelo FortiManager de uma empresa credenciada. Caso esta empresa rompa o contrato sendo que o PJSC não tenha adquirido ainda esta solução, esta deverá somente retirar o acesso após 24 meses a partir do pedido de rompimento do contrato ou então quando o PJSC solicitar.

18. 20.O PJSC poderá adquirir a qualquer momento a solução de gerenciamento centralizado, o FortiManager. A partir de sua instalação todos os Fortigates das operadoras credenciadas deverão ser registrados no FortiManager do PJSC.

7 - PRAZOS

Além dos prazos definidos no modelo de execução, são estabecidos os seguintes prazos:

1. vigência: 24 (vinte e quatro) meses, a contar da data da assinatura, podendo ser prorrogado, nos termos do art. 57, II, da Lei n. 8.666/1993, mediante termo aditivo, se houver interesse das partes;

2. instalação e ativação de novo circuito de dados: 180 (cento e oitenta) dias contados do recebimento da ordem de serviço de vistoria e instalação;

3. mudança de endereço e ativação de circuito de dados em novo local: 180 (cento e oitenta) dias contados do recebimento da ordem de serviço de vistoria e instalação ou email de comunicação;

4. atendimento de chamados técnicos: 6 (seis) horas, contadas da sua abertura na central de atendimento disponibilizados pelas operadoras;

5. atendimento de chamados técnicos referente ao concentrador da rede SD-WAN ou do concentrador MPLS: 2 (duas) horas, contadas da sua abertura na central de atendimento disponibilizada pela operadora;

6. entrega de serviço NOC: 24 (vinte e quatro) horas contados da ativação do concentrador e do primeiro circuito ativo;

7. informação sobre viabilidade técnica: 7 (sete) dias, contados do recebimento da notificação;

8. aumento e diminuição de velocidade de circuitos: 10 (dez) dias úteis, contados do recebimento da notificação;

9. retirada do roteador: no máximo 30 (trinta) dias, contados do recebimento da notificação;

10. aumento e diminuição do coeficiente de aproveitamento: 10 (dez) dias úteis, contados do recebimento da notificação;

11. correção de problemas no circuito após a instalação inicial: 10 (dez) dias, contados do recebimento da notificação;

12. agendamento de instalação: antecedência mínima de 48 (quarenta e oito) horas, em data a ser acordada com a Diretoria de Tecnologia da Informação e unidade a ser atendida, de acordo com a disponibilidade;

13. apresentação do link de acesso ao NOC de monitoramento do circuito: 24 horas após a instalação;

14. mudança de configuração dos Fortigates e roteadores: 10 dias úteis, contados do recebimento da notificação;

15. configuração de Multicast, quando solicitado: 10 dias úteis, contados do recebimento da notificação.

8 - EQUIPE TÉCNICA

As empresas que atingirem a qualquer momento do contrato 70% do total de links propostos pelo PJSC disponibilizarão recursos humanos de seu quadro para a execução dos serviços do objeto do contrato para a realização das seguintes atividades:

1. Alteração de QOS;

2. Configuração de traffic shape;

3. Configuração do roteamento de tráfego para links de outras operadoras que foram interligados nos seus equipamentos Fortigate;

4. Alteração de configuração dos seus equipamentos Fortigate;

5. configuração de Multicast nos equipamentos que se fizerem necessários;

6. Monitoramento dos links de comunicação de dados e abertura de chamado ou com a ação corretiva necessária agilizando o tempo de indisponibilidade;

7. Monitoramento dos equipamentos de aceleração com a devida abertura ou com a ação corretiva necessária agilizando o tempo de indisponibilidade;

8. Gerar relatórios de disponibilidade de links, de acordo com a necessidade do PJSC.

Para isto, o(s) membro(s) da equipe técnica deverá apresentar o seguinte perfil:

1. Técnico Pleno;

2. Atuação na área de Telecom/Redes com pelo menos 3 (três) anos de experiência;

3. Bons conhecimentos em endereçamento IP;

4. Bons conhecimentos em roteamento para atender as demandas de conexões de rede;

5. Experiência em análise nas solicitações de acesso entre redes;

6. Conhecimentos em configurações de equipamentos de rede;

7. Bons conhecimentos de TCP/IP e Roteamento.

As atividades executadas por este técnico poderão ser remotas e se justificam pelo tamanho da rede contratada, pois quanto mais links de uma contratada maior a probabilidade de falha e mais tempo é dispendido na abertura de chamados pelo grupo técnico da Seção de Administração de Redes, que apresenta equipe reduzida. Atualmente, o contrato da OI prevê esse tipo de serviço e vericamos que a pró-atividade no atendimento a falhas dos links é muito grande, diminuindo os tempos de indisponibilidade dos links, como também houve melhora nos processos de alterações de configuração dos equipamentos. Este requisio foi levantado junto as credenciadas nas reuniões realizadas para discussão do novo credenciamento e todas aceitaram.

9 - METODOLOGIA DE AVALIAÇÃO DA QUALIDADE, PRAZOS E CONDIÇÕES DE ACEITE, ALTERAÇÃO E CANCELAMENTO

1. Para o recebimento da prestação de serviço de Link de dados, os servidores designados deverão verificar se todas as condições previstas estão sendo cumpridas, quais sejam:

1. Qualidade do serviço do link MPLS, através de testes de conectividade, capacidade de Transmissão e NOC de monitoramento;

2. Valores apresentados no pedido de pagamento dos circuitos idêntico ao informado no contrato;

3. Prazos de instalação dos circuitos atendidos dentro do prazo;

2. Constatada qualquer irregularidade quando da instalação do link MPLS, o PJSC, por intermédio da Diretoria de Tecnologia da Informação - Divisão competente, deverá imediatamente notificar a CONTRATADA, para o qual será dado o prazo máximo de 5 dias úteis, a partir da comunicação por escrito, para regularizar/substituir os equipamentos/serviços que apresentarem defeitos ou estiverem em desacordo com as especificações do edital.

3. Quando do pedido de cancelamento do serviço de link de dados, a Diretoria de Tecnologia da Informação - Divisão competente, deverá verificar se todas as condições previstas estão sendo cumpridas, quais sejam:

1. Desligamento dentro do prazo determinado;

2. Retirada do roteador fornecido pela operadora, no endereço de instalação;

3. Cobrança de mensalidade proporcional à data de solicitação.

4. Quando da abertura de chamado técnico referente ao serviço de link de dados, a Diretoria de Tecnologia da Informação - Divisão competente, deverá verificar se todas as condições previstas estão sendo cumpridas, quais sejam:

1. Atendimento dentro do prazo determinado;

2. Reestabelecimento dos serviços.

10 - FORMAS DE RECEBIMENTO PROVISÓRIO E DEFINITIVO, BEM COMO DE AVALIAÇÃO DA QUALIDADE DOS BENS E/OU SERVIÇOS ENTREGUES

A Divisão de Redes de Comunicação, da Diretoria de Tecnologia da Informação, atestará a regularidade do serviço, sendo que para isso o link MPLS deverá apresentar dimensionamento correto para garantir a transmissão de dados de acordo com a velocidade contratada, além da rede SD-WAN estar funcionando em alta disponibilidade.

A adequação do recebimento observará o seguinte:

1. Necessário que forneça conectividade para a comarca até o core da rede do PJSC via rede MPLS da CONTRATADA;

2. Fortigate da unidade instalada deverá se autenticar no FortiManager para que possa ser gerenciado;

3. Circuito ser monitorado pelas ferramentas de monitoramento do PJSC e pelo NOC da CONTRATADA;

4. Teste de validação do equipamento Fortigate fornecido. No momento da instalação do segundo Fortigate, serão efetuados testes que validem a condição de alta disponibilidade;

5. A Seção de Administração de Redes deverá ter acesso aos equipamentos Fortinet e aos roteadores com usuário próprio.

6. Teste de Capacidade de Transmissão do circuito.

Constatada qualquer irregularidade, a CONTRATADA, devidamente comunicada, por escrito, terá o prazo máximo de 5 (cinco) dias, a partir da notificação, para fazer a regularização necessária.

O recebimento definitivo dos produtos/serviços será dado somente após a verificação do atendimento de todas as condições descritas.