1. OBJETO

1.1. Contratação de empresa especializada para fornecimento de links dedicados de acesso à internet e links IP/MPLS, por fibra óptica, interligando as unidades remotas no interior com a sede administrativa, dispondo também de solução integrada de proteção de rede com características de Next Generation Firewall (NGFW), conectividade WIFI, firewall de aplicação, gerenciamento de logs, oferecendo serviço de segurança multicamada, atendendo assim às necessidades do Tribunal de Justiça do Estado do Acre (TJAC), conforme disposições deste Termo de Referência.

2.JUSTIFICATIVA DA NECESSIDADE DA CONTRAÇÃO

2.1.MOTIVAÇÃO

2.1.1. A contratação desse serviço visa a continuidade da disponibilidade de acesso à rede mundial de computadores, por meio da Internet, de forma ininterrupta. Se justifica pela necessidade deste Tribunal de Justiça demandar acesso à internet com velocidade e eficiência adequadas para as mais diversas funções das unidades do interior do estado, tais como: acesso à rede e aos sistemas SAJ, SEI, Malote Digital, E-mail, Videoconferências, dentre outros.

2.1.2. Tendo em vista que as soluções de TIC estão sendo cada vez mais utilizadas na gestão deste órgão, onde cada vez mais os sistemas dependem de conexão online, como o SAJ, SEI, Malote Digital, Ponto Digital, Videomonitoramento, E-mail, dentre outros, é de extrema importância a contratação de link de internet por este Tribunal.

2.1.3. A contratação de links de internet deverá suportar um conjunto de aplicações e sistemas, visto que atenderá a sede e as unidades no interior.

2.1.4. De igual modo, o TJAC precisa garantir a segurança de seus sistemas computacionais. O advento de novas ameaças tecnológicas requer a adoção de novas soluções de segurança para garantir a integridade dos dados armazenados dentro da nossa infraestrutura de tecnologia da informação. A solução deverá conter atualização constante para garantir a excelência da tecnologia empregada, visando se antecipar a possíveis falhas, brechas e problemas.

2.1.5. Vale ressaltar que as soluções de firewall, gerenciamento de logs e o serviço de segurança multicamada irão auxiliar na proteção dos dados e na prevenção de vazamentos, favorecendo para que este ente fique em conformidade com a Lei Geral de Proteção de Dados (LGPD), que foi sancionada em agosto

de 2018, bem como a aplicação da Resolução 396/2021 do CNJ - Estratégia Nacional de Segurança Cibernética.

2.2. FUNDAMENTAÇÃO

2.2.1. O objeto da contratação está previsto no Plano de Contratações Anual, conforme detalhamento a seguir:

I) ID PCA no PNCP: 04034872000121-0-000003/2024;

II) Data de publicação no PNCP: 10/04/2024;

III) Id do item no PCA: 162;

IV) Classe/Grupo: 491 - SERVIÇOS DE PROCESSAMENTOS DE DADOS - PESSOA JURÍDICA

2.3. JUSTIFICATIVA PARA O AGRUPAMENTO DE ITENS

2.3.1. O objeto da presente licitação foi agrupado por LOTES, à luz do art. 40, da Lei Geral de Licitações, 14.133/21, de maneira que a fragmentação em itens acarretaria a perda do conjunto; perda da economia de escala; redundaria em prejuízo à celeridade da licitação; ocasionaria a excessiva pulverização de contratos ou resultaria em contratos de pequena expressão econômica.

a) Do agrupamento por lote de itens que guardem homogeneidade entre si.

Nas licitações de objetos divisíveis o Tribunal de Contas da União entende que o julgamento seja feito por item, e não por preço global. Contudo, há situações em que se faz necessário aglutinar os itens com o intento de casar aquisições, visto que poderá haver um vínculo entre eles, ou se comprados separadamente prejudicarão o resultado esperado pela Administração.

Nesse caso, apesar dos objetos serem divisíveis, eles guardam estrita identidade de natureza e características semelhantes, além de guardar correspondência com sua composição, podendo cada lote ser fornecido por um mesmo fornecedor, por se tratarem de objetos comuns ao ramo de empresa de comercialização de Serviços de Telecomunicação e Serviços de Transmissão de dados, concretizando, assim, os princípios da competitividade.

b) Da fragmentação em itens acarretar a perda do conjunto.

O parcelamento do objeto somente se justifica e fundamenta quando houver viabilidade técnica e, principalmente, ganho econômico para a Administração Pública. No presente caso não há viabilidade técnica, uma vez que a falta de um componente prejudicaria todo o conjunto, de nada adiantaria ter a Internet Dedicada, sem ter o sistema de transmissão, como por exemplo. Há necessidade que todos os itens estejam disponíveis para o funcionamento do Sistema.

c) Da perda da economia de escala.

O § 3°, inciso I do art. 40, da Lei n. 14.133/2021 determina que as compras efetuadas pela Administração sejam divididas em tantas parcelas quantas se comprovarem técnica e economicamente viáveis, procedendo-se a licitação com vistas ao melhor aproveitamento dos recursos disponíveis no mercado e a ampliação da competitividade sem perda da economia de escala.

Quanto maior a quantidade a ser comprada, maior poderá ser o desconto na compra de bens e serviços. Esse ganho está relacionado com o aumento da quantidade adquirida sem um aumento proporcional no custo e está intrinsecamente relacionado ao princípio da economicidade insculpido no art. 70 de nossa Carta Magna.

A economia de escala é definida como aquela que ocorre a partir de determinado patamar de quantidade de itens comercializados e pode acarretar relevante desconto na aquisição dos bens e serviços.

De tal modo, que no caso em tela a adoção critério de julgamento menor preço por lote permite o melhor aproveitamento dos recursos disponíveis no mercado e a ampliação da competitividade, sem perda da economia de escala, como por exemplo, a empresa que ganhar o lote fornecerá todos os itens, acarretando, consequentemente, uma diminuição nos custos e economia de escala.

d) Do prejuízo à celeridade da licitação.

Um dos fatores que pode ser levado em conta na elaboração de um edital por lote é o interesse na celeridade do processo, que busca simplificar procedimentos de rigorismos excessivos e de formalidades desnecessárias. As decisões, sempre que possível, devem ser tomadas no momento da sessão.

e) Da pulverização de contratos.

A licitação por itens corresponde, na verdade, a uma multiplicidade de licitações, cada qual com existência própria e dotada de autonomia jurídica, mas todas desenvolvidas conjugadamente em um único procedimento, documentado nos mesmos autos. Esta exagerada divisão de objeto pode ocasionar uma excessiva pulverização dos contratos, tornando mais dispendiosa a contratação.

Por outro lado, neste caso a adoção do critério de julgamento menor preço por lote para a Contratação de empresa de Telecomunicações especializadas para prestação de Serviços Continuado de: Comunicação dedicada para acesso à rede mundial de computadores- Internet- na modalidade terrestre suportando aplicações TCP/IP, resultaria na contratação da quantidade necessária de empresas fornecedora/licitante, não ocorrendo a pulverização de contratos. Ainda há, com base no interesse público, maior segurança ao cumprimento do contrato.

Por fim, há que se observar o caso concreto, avaliando a conveniência e oportunidade, de modo a satisfazer da melhor forma o interesse público, pois cada contratação tem suas especificidades, in casu a aquisição por lote é mais vantajosa para a

Administração, em decorrência dos riscos inerentes à própria execução, pois, não restam dúvidas, o objeto pretendido, quando executado por inúmeros contratados, poderá não ser integralmente entregue, tendo em vista problemas na relações jurídicas mantidas com diversos contratados.

f) Dos contratos de pequena expressão econômica.

Em razão da adoção do critério de menor preço por lote, não será celebrado contrato de pequena expressão econômica. Em caso contrário, a licitação por itens similares geraria a situação de celebrar vários contratos de pequena expressão econômica.

3. DA PADRONIZAÇÃO – SOLUÇÃO DE SEGURANÇA DE BORDA

3.1. Atualmente, o Tribunal de Justiça do Estado do Acre possui 19 (dezenove) firewalls corporativos de nova geração (NGFW), 53 (cinquenta e três) pontos de acesso WIFI, 02 (dois) firewalls de aplicação (em cluster), um gerenciador de logs e um concentrador de gerenciamento centralizado que foram oriundos do Contrato nº 02/2022 e suas alterações, sem indicação de fabricante, mas que fossem capazes de operar em ambientes corporativos com fluxo massivo de dados.

3.2. Observa-se também que a totalidade, ou seja, 100% (cem por cento) das soluções de firewall administrado por esta GESEG, que se encontram atualmente em produção, são do fabricante FORTINET, sendo o modelo Fortigate 501E na Sede, bem como os modelos Fortigate 30E e Fortigate 100D nas unidades do interior. As boas práticas na área de TI recomendam, visando garantir desempenho homogêneo, adoção de padronização dos ativos e equipamentos de segurança de rede.

3.3. Ademais, a legislação vigente permite fazer tal procedimento, como nos ensina o Art. 40, Inciso V, da Lei 14.133/2021, in verbis:

> "Art. 40. As compras, sempre que possível, deverão:
>
> V - atender ao princípio da padronização, que imponha compatibilidade de especificações técnicas e de desempenho, observadas, quando for o caso, as condições de manutenção, assistência técnica e garantia oferecidas;"

3.4. Sobre o tema, importante destacar a doutrina jurídica de Marçal Justen Filho (2000, p. 143), que diz que a cláusula "sempre que possível" não remete à discricionariedade da Administração. Não é equivalente a "quando a Administração Pública quiser". A fórmula verbal torna impositiva e obrigatória a adoção das providências constantes do elenco, ressalvadas as hipóteses em que tal for "impossível".

3.5. Nota-se claramente que a atenção à padronização com base em nível de desempenho e qualidade vem elevada a caráter de princípio lógico, portanto, tido como regra geral a ser adotada nas compras governamentais.

3.6. Uma das principais vantagens que a padronização pode proporcionar, sob os aspectos técnico e

econômico, é o aproveitamento do know-how utilizado na manutenção e conservação dos novos produtos – tendo por paradigma as experiências anteriores – bem como o uso dos mesmos insumos que passarão a atender não só aos antigos equipamentos como a todos os novos, padronizados.

3.7. Deve-se, neste sentido, seguir o padrão de fabricante das soluções de segurança, levando em consideração ainda, que a equipe de Gerência de Segurança da Informação deste TJAC, já realizou ao longo do tempo, várias capacitações e treinamentos em soluções do fabricante FORTINET, possuindo grande expertise nesse tipo de solução, com mais de 5 anos de utilização, sendo necessário portanto, para manutenção da continuidade do negócio, atendendo a padrões mínimos de segurança, a padronização das soluções ora existentes.

4. DETALHAMENTO DO OBJETO

4.1. A CONTRATADA deverá fornecer links urbanos e interurbanos para interligação das unidades do Poder Judiciário do Estado do Acre na capital e interior, localizadas nos endereços indicados a seguir, utilizando tecnologia MPLS ou semelhante superior e de acesso à internet com disposições e características, conforme abaixo:

LOTE 01 – LINK PRINCIPAL CAPITAL E COMARCAS DO INTERIOR			
ITEM	DESCRIÇÃO	VELOCIDADE	QUANTIDADE
1	Serviço de acesso à Internet, tipo dedicado, com garantia de banda e entrega de endereço IP no barramento /27, com proteção em backbone contra ataques DDoS e Serviço de Monitoramento proativo e solução de segurança de borda para o **Anexo I da Sede do Tribunal de Justiça DC 1 e/ou no DC 2 localizado na Cidade da Justiça**. (O licitante vencedor deste LOTE não poderá ser o vencedor do LOTE II).	1Gb	1
2	Concentrador MPLS com suporte a banda total dos links remotos. No **Anexo I da Sede do Tribunal de Justiça DC 1 e/ou no DC 2 localizado na Cidade da Justiça**.	1,2Gb	1
3	Link Interurbano do tipo MPLS para o **Fórum de Senador Guiomard**. Avenida Castelo Branco, S/N – CEP 69.925-000. Senador Guiomard.	50Mb	1

4	Link Interurbano do tipo MPLS para o **Fórum de Plácido de Castro**. Rua Juvenal Antunes, 1079 – CEP 69.928-000. Plácido de Castro.	50Mb	1
5	Link Interurbano do tipo MPLS para o **Fórum de Acrelândia**. Avenida Governador Edmundo Pinto, 581 – CEP 69.945-000. Acrelândia.	50Mb	1
6	Link Interurbano do tipo MPLS para o **Fórum de Capixaba**. Rua Francisco Cordeiro de Andrade, S/N – CEP 69.922-000. Capixaba.	50Mb	1
7	Link Interurbano do tipo MPLS para o **Fórum de Xapuri**. Rua Floriano Peixoto, 62 – CEP 69.930-000. Xapuri.	50Mb	1
8	Link Interurbano do tipo MPLS para o **Fórum de Sena Madureira**. Rua Cunha Vasconcelos, 689 – CEP 69.940-000. Sena Madureira.	50Mb	1
9	Link Interurbano do tipo MPLS para o **Fórum de Manoel Urbano**. Rua Mendes de Araujo, 1.267 – CEP 69.950-000. Manoel Urbano.	50Mb	1
10	Link Interurbano do tipo MPLS para o **Fórum de Feijó**. Travessa Floriano Peixoto, 206 – CEP 69.960-000. Feijó.	50Mb	1
11	Link Interurbano do tipo MPLS para o **Fórum de Tarauacá**. Avenida Antônio Frota, S/N – CEP 69.970-000. Tarauacá.	50Mb	1
12	Link Interurbano do tipo MPLS para **Cidade da Justiça de Cruzeiro do Sul**. BR 307, KM 09, nº 4090 – CEP 69.980-000. Cruzeiro do Sul.	100Mb	1
13	Link Interurbano do tipo MPLS para o **Fórum de Mâncio Lima**. Rua Joaquim G. de Oliveira, 160 – CEP 69.990-000. Mâncio Lima.	50Mb	1
14	Link Interurbano do tipo MPLS para o **Fórum de Brasiléia**. Avenida Geny Assis, S/N – CEP 69.932-000. Brasiléia.	50Mb	1

15	Link Interurbano do tipo MPLS para o **Fórum de Epitaciolândia**. BR 317, KM 01 – CEP 69.934-000 - Epitaciolândia.	50Mb	1

16	Link Interurbano do tipo MPLS para o **Fórum de Assis Brasil**. Rua Dom Giocondo Maria Grotti, 281 – CEP 69.935-000. Assis Brasil.	50Mb	1
17	Link Interurbano do tipo MPLS para o **CIC – Centro Integrado de Cidadania**. Rua do Comércio, S/N – CEP 69.921-000. Porto Acre	50Mb	1
18	Link Interurbano do tipo MPLS para o **CIC – Centro Integrado de Cidadania**. Avenida Presidente Vargas, S/N – CEP: 69.985-000. Rodrigues Alves.	50Mb	1
19	Link Interurbano do tipo MPLS para o **Fórum de Bujari**. BR 364, KM 28, Nº 390, Bujarí - Acre – CEP 69.923-000	50Mb	1
20	Link Interurbano do tipo MPLS para **Centro Cultural do Juruá**, Praça João Pessoa, n.° 300, Centro. CEP: 69.980-000	50Mb	1
21	Link Interurbano do tipo MPLS para o **Palácio da Justiça**, Rua Benjamin Constant, 277, Centro, Rio Branco - Acre - 69905-072	50Mb	1

LOTE 02 – LINK REDUNDANTE CAPITAL/INTERIOR			
ITEM	DESCRIÇÃO	VELOCIDADE	QUANTIDADE
1	Serviço de acesso à Internet, tipo dedicado, com garantia de banda e entrega de endereço IP no barramento /27, com proteção em backbone contra ataques DDoS e Serviço de Monitoramento proativo para o Anexo I da Sede do Tribunal de Justiça e/ou no DATACENTER localizado na Cidade da Justiça. (O vencedor deste LOTE não poderá ser o mesmo vencedor do LOTE I)	1Gb	1

2	Serviço de acesso à Internet, tipo dedicado, com garantia de banda e entrega de endereço IP no barramento /30, com proteção em backbone contra ataques DDoS e Serviço de Monitoramento proativo para o Fórum de Senador Guiomard. Avenida Castelo Branco, S/N – CEP 69.925-000. Senador Guiomard. (O vencedor deste LOTE não poderá ser o mesmo vencedor do LOTE I)	50Mb	1
3	Serviço de acesso à Internet, tipo dedicado, com garantia de banda e entrega de endereço IP no barramento /30, com proteção em backbone contra ataques DDoS e Serviço de Monitoramento proativo para o Fórum de Plácido de Castro. Rua Juvenal Antunes, 1079 – CEP 69.928-000. Plácido de Castro.	50Mb	1
4	Serviço de acesso à Internet, tipo dedicado, com garantia de banda e entrega de endereço IP no barramento /30, com proteção em backbone contra ataques DDoS e Serviço de Monitoramento proativo para o Fórum de Acrelândia. Avenida Governador Edmundo Pinto, 581 – CEP 69.945-000. Acrelândia.	50Mb	1
5	Serviço de acesso à Internet, tipo dedicado, com garantia de banda e entrega de endereço IP no barramento /30, com proteção em backbone contra ataques DDoS e Serviço de Monitoramento proativo para o Fórum de Capixaba. Rua Francisco Cordeiro de Andrade, S/N – CEP 69.922-000. Capixaba.	50Mb	1

6	Serviço de acesso à Internet, tipo dedicado, com garantia de banda e entrega de endereço IP no barramento /30, com proteção em backbone contra ataques DDoS e Serviço de Monitoramento proativo para o Fórum de Xapuri. Rua Floriano Peixoto, 62 – CEP 69.930-000. Xapuri.	50Mb	1
7	Serviço de acesso à Internet, tipo dedicado, com garantia de banda e entrega de endereço IP no barramento /30, com proteção em backbone contra ataques DDoS e Serviço de Monitoramento proativo para o Fórum de Sena Madureira. Rua Cunha Vasconcelos, 689 – CEP 69.940-000. Sena Madureira.	50Mb	1
8	Serviço de acesso à Internet, tipo dedicado, com garantia de banda e entrega de endereço IP no barramento /30, com proteção em backbone contra ataques DDoS e Serviço de Monitoramento proativo para o Fórum de Manoel Urbano. Rua Mendes de Araújo, 1.267 – CEP 69.950-000. Manoel Urbano.	50Mb	1
9	Serviço de acesso à Internet, tipo dedicado, com garantia de banda e entrega de endereço IP no barramento /30, com proteção em backbone contra ataques DDoS e Serviço de Monitoramento proativo para o Fórum de Feijó. Travessa Floriano Peixoto, 206 – CEP 69.960-000. Feijó.	50Mb	1
10	Serviço de acesso à Internet, tipo dedicado, com garantia de banda e entrega de endereço IP no barramento /30, com proteção em backbone contra ataques DDoS e Serviço de Monitoramento proativo para o Fórum de Tarauacá. Avenida Antônio Frota, S/N – CEP 69.970-000. Tarauacá.	50Mb	1

Assinado eletronicamente por **AMILAR SALES ALVES**, **Técnico Judiciário**, em 19/04/2024 11:10:31
Assinado eletronicamente por **ELSON CORREIA DE OLIVEIRA NETO**, **Gerente de Segurança da Informação**, em 19/04/2024 11:09:14

11	Serviço de acesso à Internet, tipo dedicado, com garantia de banda e entrega de endereço IP no barramento /30, com proteção em backbone contra ataques DDoS e Serviço de Monitoramento proativo para o Cidade da Justiça de Cruzeiro do Sul. BR 307, KM 09, nº 4090 – CEP 69.980-000. Cruzeiro do Sul.	100Mb	1
12	Serviço de acesso à Internet, tipo dedicado, com garantia de banda e entrega de endereço IP no barramento /30, com proteção em backbone contra ataques DDoS e Serviço de Monitoramento proativo para o Fórum de Mâncio Lima. Rua Joaquim G. de Oliveira, 160 – CEP 69.990-000. Mâncio Lima.	50Mb	1
13	Serviço de acesso à Internet, tipo dedicado, com garantia de banda e entrega de endereço IP no barramento /30, com proteção em backbone contra ataques DDoS e Serviço de Monitoramento proativo para o Fórum de Brasiléia. Avenida Geny Assis, S/N – CEP 69.932-000. Brasiléia.	50Mb	1
14	Serviço de acesso à Internet, tipo dedicado, com garantia de banda e entrega de endereço IP no barramento /30, com proteção em backbone contra ataques DDoS e Serviço de Monitoramento proativo para o Fórum de Epitaciolândia. BR 317, KM 01 – CEP 69.934-000. Epitaciolândia.	50Mb	1

15	Serviço de acesso à Internet, tipo dedicado, com garantia de banda e entrega de endereço IP no barramento /30, com proteção em backbone contra ataques DDoS e Serviço de Monitoramento proativo para o Fórum de Assis Brasil. Rua Dom Giocondo Maria Grotti, 281 – CEP 69.935-000. Assis Brasil.	50Mb	1

16	Serviço de acesso à Internet, tipo dedicado, com garantia de banda e entrega de endereço IP no barramento /30, com proteção em backbone contra ataques DDoS e Serviço de Monitoramento proativo para o CIC – Centro Integrado de Cidadania. Rua do Comércio, S/N – CEP 69.921-000. Porto Acre	50Mb	1
17	Serviço de acesso à Internet, tipo dedicado, com garantia de banda e entrega de endereço IP no barramento /30, com proteção em backbone contra ataques DDoS e Serviço de Monitoramento proativo para o CIC – Centro Integrado de Cidadania. Avenida Presidente Vargas, S/N – CEP: 69.985-000. Rodrigues Alves.	50Mb	1
18	Serviço de acesso à Internet, tipo dedicado, com garantia de banda e entrega de endereço IP no barramento /30, com proteção em backbone contra ataques DDoS e Serviço de Monitoramento proativo para o Fórum de Bujari. BR 364, KM 28, Nº 390, Bujarí - Acre – CEP 69.923-000	50Mb	1
19	Serviço de acesso à Internet, tipo dedicado, com garantia de banda e entrega de endereço IP no barramento /30, com proteção em backbone contra ataques DDoS e Serviço de Monitoramento proativo para o Centro Cultural do Juruá, Praça João Pessoa, n.º 300, Centro. CEP: 69.980-000	50Mb	1

20	Serviço de acesso à Internet, tipo dedicado, com garantia de banda e entrega de endereço IP no barramento /30, com proteção em backbone contra ataques DDoS e Serviço de Monitoramento proativo para o Palácio da Justiça, Rua Benjamin Constant, 277, Centro, Rio Branco - Acre - 69905-072	50Mb	1

Assinado eletronicamente por **AMILAR SALES ALVES**, **Técnico Judiciário**, em 19/04/2024 11:10:31
Assinado eletronicamente por **ELSON CORREIA DE OLIVEIRA NETO**, **Gerente de Segurança da Informação**, em 19/04/2024 11:09:14

21	Serviço de acesso à Internet extra, tipo dedicado, com garantia de banda e entrega de endereço IP no barramento /30, com proteção em backbone contra ataques DDoS e Serviço de Monitoramento proativo para capital e interior do Estado do Acre, onde há disponibilidade de fibra óptica de alta velocidade.	50Mb	2

LOTE 03 – SOLUÇÃO DE SEGURANÇA DA INFORMAÇÃO			
ITEM	DESCRIÇÃO	UNIDADE	QUANTIDADE
1	Serviço de Firewall Corporativo TIPO I, com funcionalidades de SDWAN, Firewall, IPS e Controle de Aplicação habilitadas simultaneamente em Alta Disponibilidade (HA)	CLUSTER	2
2	Serviço de Firewall Corporativo TIPO II, com funcionalidades de SDWAN, Firewall, IPS e Controle de Aplicação habilitadas simultaneamente	UNIDADE	4
3	Serviço de Firewall Corporativo TIPO III, com funcionalidades de SDWAN, Firewall, IPS e Controle de Aplicação habilitadas simultaneamente	UNIDADE	1
4	Serviço de Firewall Corporativo TIPO IV com funcionalidades de SDWAN, Firewall, IPS e Controle de Aplicação habilitadas simultaneamente	UNIDADE	28
5	Serviço de Gerenciamento Centralizado licenciado para pacotes mínimos de 100 dispositivos	PACOTE	4
6	Serviço de Relatoria e de Análise de Logs em tempo real	UNIDADE	1
7	Serviço de Firewall de Aplicação Web capaz de prover proteção aos servidores de aplicação	CLUSTER	2
8	Serviço de Segurança de Endpoint com recursos de EPP e ZTNA	LICENÇA	3000
9	Serviço de Gerenciamento de Identidade licenciado para pacotes mínimos de 1000 usuários locais ou remotos com autenticação multifator, incluindo token de usuário individual	PACOTE	3
10	Serviço de Loab Balance capaz de prover balanceamento de carga de aplicações	CLUSTER	2

11	Serviço de conectividade de rede WIFI com pontos de acesso tipo “indoor”	UNIDADE	150

4.2. DETALHAMENTO DOS OBJETOS GERAIS

4.2.1. A CONTRATADA deve estar devidamente autorizada pela Agência Nacional de Telecomunicações – ANATEL para prestação de serviço dos LOTES 01 e 02;

4.2.2. A CONTRATADA do LOTE 01, não poderá ser a CONTRATADA do LOTE 02 e vice-versa. Objetivando atender aos requisitos de saídas distintas de conectividade para promover a redundância do serviço;

4.2.3. Inclui-se, na execução dos serviços a serem contratados, o fornecimento de equipamentos necessários ao funcionamento do objeto deste Termo de Referência, bem como a instalação, garantia, suporte e assistência técnica, objetivando atender nossa necessidade atual de comunicação, com manutenção e reposição de partes e peças;

4.2.4. A solução proposta deverá contemplar todos os equipamentos necessários, tais como: modem, roteadores, sub-bastidor, fontes, softwares, numeração IP e serviços necessários para implantação e manutenção. O valor, tanto de instalação, quanto mensal do circuito de dados, bem como roteador e equipamentos necessários, deverão estar previstos na formação de preço dos itens;

4.2.5. As licitantes a serem contratadas aplicarão nos equipamentos, quando necessário, substituição de partes e peças originais, adequadas, novas ou, quando não, que mantenham as especificações técnicas do fabricante, ficando desde logo, autorizada pelo TJAC;

4.2.6. O Tribunal de Justiça do Estado do Acre não estará obrigado a adquirir os quantitativos dispostos neste Termo de Referência, devendo adquirir os serviços de acordo com a sua necessidade, mediante emissão de nota de empenho e ordem de serviço;

4.2.7. Os serviços que não forem adquiridos imediatamente ficarão contratados aguardando a emissão de ordem de serviço, mediante disponibilidade orçamentária e financeira, sendo ativados conforme necessidade e conveniência da CONTRATANTE;

4.2.8. Os itens do LOTE 03 devem possuir características de Next Generation Firewall (NGFW), com funcionalidades de SD-WAN (Software Defined WAN), além de outras funcionalidades inerentes a solução de segurança de rede;

Todos os itens citados são de serviço contínuo, que serão pagos de forma MENSAL, desde que devidamente formalizado a Autorização de Fornecimento.

4.2.9. Todos os itens citados são de serviço contínuo, que serão pagos de forma MENSAL, desde que devidamente formalizado a Autorização de Fornecimento.

5. ENDEREÇOS DE IP E VELOCIDADES

5.1. As velocidades estão de acordo com a resolução 211/2015 do CNJ Art. 24 Item VI, onde exige 2 (dois) links de comunicação do órgão com a internet, mas com operadoras distintas para o acesso à rede de dados, com o máximo de comprometimento de banda de 80%, como é demonstrado nos LOTE 1 e LOTE 2, do Termo de Referência. Visa ainda atender a Resolução CNJ 370/2021 que não anula as ações/iniciativas do TJAC para atender os requisitos mínimos do nivelamento tecnológico da infraestrutura de TIC, conforme recomendado na Resolução 211/2015 no Art. 24, item VI, conforme deliberado na reunião com CNJ, em 10/03/2021, constante no SEI 0000550-59.2021.0000 item 18 (0944980):

"Com A Revogação da Res. CNJ nº 211/2015 e a publicação da Res. CNJ nº 370/2021 novas estratégias foram traçadas. Entendemos que, pelo bem da Administração Pública, as estratégias passadas se tornaram boas práticas que merecem ser continuadas ou mesmo aperfeiçoadas."

5.2. O serviço dedicado de acesso à internet deve ser entregue com no mínimo 16 (dezesseis) endereços IPs públicos fixos (rede /27) válidos para os links de 1 Gbps (ITEM 1 dos LOTES 01 e 02) e 02 (dois) IPs públicos fixos (rede /30) válidos para os demais itens do LOTE 02, livres para uso pela CONTRATANTE, sendo que esses IPs não deverão ser do mesmo bloco utilizado pelos usuários de IPs dinâmicos, ou terem sido anteriormente de blocos de endereços IP utilizados para este fim;

D5.3. everá constar em sua proposta técnica de atendimento, quais os blocos livres em seu "AS" (Autonomous System) serão utilizados para atendimento no grupo de itens pretendidos, e os referidos IPs devem constar em consulta pública de prefixos na internet (Ex.: https://bgp.he.net/);

5.4. A CONTRATADA deverá reservar estes endereços IP exclusivamente para o CONTRATANTE, independente de utilização;

5.5. Os endereços fornecidos não deverão constar em nenhum tipo de lista de bloqueio (RBL: Real-time Blackhole List ou DNSBL: DNS-based Blackhole List), seja qual for o motivo.

6. CARACTERÍSTICAS E ESPECIFICAÇÕES – LOTE 01 E LOTE 02

6.1. A CONTRATADA deverá disponibilizar meios de aferir a velocidade do link instalado. Caso esse requisito não seja atendido, a CONTRATADA não poderá refutar os meios utilizados pela CONTRATANTE para aferir as velocidades contratadas;

6.2. Os serviços de acesso deverão ficar disponíveis na modalidade 24h/dia, 7 (sete) dias/semana, sem a necessidade de procedimentos para conexão/desconexão;

6.3. O link de acesso à internet deverá possuir dimensionamento correto para garantir a transmissão de dados de acordo com as velocidades contratadas;

6.4. Não possuir nenhum tipo de restrição de uso, operando 24h/dia, 7 (sete) dias/semana, sem limite de quantidade de dados trafegados, nem restrição de tipo de dados trafegados, porta lógica ou serviço, devendo ser considerada a banda disponível em cada acesso;

6.5. Não será permitido acesso XDSL;

6.6. Não será permitido o fornecimento de enlaces via satélite, para os LOTES 01 e 02.

7. SERVIÇO DE PROTEÇÃO NO BACKBONE CONTRA ATAQUES DDOS – LOTE 01 – ITEM 01 E

TODOS ITENS LOTE 02.

7.1. A CONTRATADA deverá disponibilizar em seu backbone proteção contra ataques de negação de serviço, evitando assim a saturação da banda da internet e indisponibilidade dos serviços em momentos de ataques DOS (Denial of Service) e DDOS (Distributed Denial of Service);

7.2. A CONTRATADA deve disponibilizar pelo menos um Centro Operacional de Segurança (ou SOC – Security Operations Center) no Brasil, com equipe especializada em monitoramento, detecção e mitigação de ataques, com opção de atendimento em idioma português brasileiro através de telefone 0800, correio eletrônico, durante as 24 (vinte e quatro) horas do dia, nos 7 (sete) dias da semana, no período de vigência contratual;

7.3. O acesso à internet (circuito de dados) não poderá ser subcontratado de terceiros, devendo a CONTRATADA fornecer ambos os serviços, solução ANTI-DDOS e circuito de dados;

7.4. A técnica ANTI-DDOS utilizada deverá ser por métrica de volumetria, assim a CONTRATADA deverá enviar junto com a proposta técnica, qual a estratégia utilizada para mitigação de ataques DDOS sobre o circuito de dados;

7.5. A solução ANTI-DDOS deverá prover o serviço de mitigação de ataques de negação de serviço (DoS – Denial of Service) para o circuito de conectividade IP dedicada à internet, sejam eles distribuídos (DDoS – Distributed Denial of Service) ou não;

7.6. A CONTRATADA deve possuir e disponibilizar no mínimo 1 (um) centro de limpeza nacional cada um com capacidade de mitigação de no mínimo 20 Gbps e no mínimo 1 (um) centro de limpeza internacional com capacidade de mitigação de no mínimo 40 Gbps;

7.7. Não haverá taxa adicional por volume de mitigação de ataques DDoS (Distributed Denial of Service) nos IPs monitorados;

7.8. A alteração de capacidade de mitigação deverá ser implementada em um prazo máximo de 5 dias úteis, a contar da data de solicitação formal através de correio eletrônico encaminhado via chave oficial ou de autorizado pelo Tribunal de Justiça do Acre;

7.9. O ataque deve ser mitigado separando o tráfego legítimo do malicioso, de modo que os serviços de internet providos pelo CONTRATANTE continuem disponíveis;

7.10. A limpeza do tráfego deverá ser seletiva e atuar somente sobre os pacotes destinados ao IP atacado, todo tráfego restante não deverá sofrer nenhuma forma de limpeza ou desvio;

7.11. A solução deve possuir mecanismos para filtragem de pacotes anômalos, garantindo a validade das conexões, sem efetuar qualquer limitação com base no número de sessões ou de pacotes por

endereço, de

modo a evitar o bloqueio de usuários legítimos;

7.12. A CONTRATADA deve tomar todas as providências necessárias para recompor a disponibilidade do link em caso de incidentes de ataques de DDoS, recuperando o pleno funcionamento deste;

7.13. Para a mitigação dos ataques o tráfego só deverá ser encaminhado para limpeza fora do território brasileiro nos casos em que os centros nacionais não suportarem a capacidade de mitigação e a demanda de ataques, no restante os ataques de origem nacional deverão ser tratados nos centros nacionais e os de origem internacional nos centros internacionais;

7.14. O envio de tráfego para mitigação em centros internacionais deverá ser justificado em relatório;

7.15. A solução deve implementar mecanismos capazes de detectar e mitigar todos e quaisquer ataques que façam o uso não autorizado de recursos de rede, para protocolo IPv4, incluindo, mas não se restringindo aos seguintes:

7.15.1. Ataques de inundação (Bandwidth Flood), incluindo Flood de UDP e ICMP;

7.15.2. Ataques à pilha TCP, incluindo mal-uso das Flags TCP, ataques de RST e FIN, SYN Flood e TCP Idle Resets;

7.15.3. Ataques que utilizam fragmentação de pacotes, incluindo pacotes IP, TCP e UDP;

7.15.4. Ataques de Botnets, Worms e ataques que utilizam falsificação de endereços IP origem (IP Spoofing).

7.16. Em nenhum caso será aceito bloqueio de ataques de DOS e DDOS por ACLs em roteadores de borda da CONTRATADA;

7.17. Caso o volume de tráfego do ataque ultrapasse as capacidades de mitigação especificadas ou sature as conexões do AS, devem ser tomadas contramedidas tais como aquelas que permitam o bloqueio seletivo por blocos de IP de origem no AS pelo qual o ataque esteja ocorrendo, utilizando técnicas como Remote Triggered Black Hole;

7.18. Realizar a comunicação da ocorrência do ataque à CONTRATANTE imediatamente após a detecção;

7.19. A solução deve permitir a proteção, no mínimo, do tráfego dos serviços web (HTTP/HTTPS), DNS, VPN, FTP e correio eletrônico;

7.20. Outras configurações deverão ser possíveis, como exemplo monitoração de um cliente por sub-interface no PE;

7.21. A CONTRATADA deverá disponibilizar relatórios mensais de mitigação de ataques, contendo no mínimo horário de início do ataque, horário de início de ação de mitigação, horário de sucesso da mitigação e horário de fim do ataque. Em conjunto com o relatório mensal relatórios dinâmicos deverão ser disponibilizados em até 48 horas após um ataque por solicitação da CONTRATANTE;

7.22. A CONTRATADA deverá comprovar por meio de Atestado de Capacidade Técnica, fornecido por pessoa jurídica de direito público ou privado, declarando ter a empresa licitante fornecido ou estarem fornecendo serviço de limpeza contra ataques DDOS (Distributed Denial of Service);

7.23. A CONTRATADA deverá apresentar relatório analítico, enviado mensalmente ao cliente;

7.24. A CONTRATADA terá no máximo 15 minutos para iniciar a mitigação de ataques de DOS e DDOS;

7.25. A interface digital a ser conectada no backbone do TRIBUNAL DE JUSTIÇA DO ACRE deverá seguir o padrão Gigabit Ethernet, ou superior quando necessário;

7.26. Os serviços ofertados deverão operar no regime 24x7 (vinte e quatro horas por dia, sete dias por semana);

7.27. O backbone IP do provedor deve ter saída com destino direto a outros provedores de backbone IP nacionais de nível Tier 1, 2 e 3, com banda de 100 Gbps no mínimo;

7.28. Nos períodos de ataque a latência do circuito deverá ser de no máximo 150 ms (milissegundos) quando a mitigação se originar do(s) centro(s) de limpeza nacional(is) e de no máximo 250 ms (milissegundos) quando se originar do(s) centro(s) internacional(is);

7.29. A solução deverá possuir funcionalidades de monitoramento, detecção e mitigação de ataques, mantidas em operação ininterrupta durante as 24 (vinte e quatro) horas do dia, nos 7 (sete) dias da semana, no período de vigência contratual;

7.30. A análise realizada para fins da solução deverá ser passiva sem utilização de elementos da rede da CONTRATANTE para coleta dos dados a serem analisados;

7.31. A mitigação de ataques deve ser baseada em arquitetura na qual há o desvio de tráfego suspeito comandado pelo equipamento de monitoramento, por meio de alterações do plano de roteamento;

7.32. A solução deve manter uma lista dinâmica de endereços IP bloqueados, retirando dessa lista os endereços que não enviarem mais requisições maliciosas após um período considerado seguro por um determinado cliente;

7.33. A solução deve suportar a mitigação automática de ataques, utilizando múltiplas técnicas como whitelists, blacklists, limitação de taxa, técnicas desafio-resposta, descarte de pacotes malformados, técnicas de mitigação de ataques aos protocolos HTTP/HTTPS, DNS, VPN, FTP, NTP, UDP, ICMP, correio eletrônico, bloqueio por localização geográfica de endereços IP, dentre outras;

7.34. A solução deve implementar mecanismos capazes de detectar e mitigar todos e quaisquer ataques que façam o uso não autorizado de recursos de rede, para protocolo IPv4 e IPv6, incluindo, mas não se restringindo aos seguintes:

7.35.Ataques de inundação (Bandwidth Flood), incluindo Flood de UDP e ICMP;

Ataques à pilha TCP, incluindo mal-uso das Flags TCP, ataques de RST e FIN, SYN Flood e TCP Idle Resets;

Ataques que utilizam Fragmentação de pacotes, incluindo pacotes IP, TCP e UDP;

Ataques de Botnets, Worms e ataques que utilizam falsificação de endereços IP origem (IP Spoofing).

8. DA ESPECIFICAÇÃO DO SERVIÇO DE FIREWALL CORPORATIVO – LOTE 03 – ITENS 01 a 04

8.1. Não serão aceitas soluções baseadas em PCs de uso geral. Todos os equipamentos a serem fornecidos

deverão ser do mesmo fabricante para assegurar a padronização e compatibilidade funcional de todos os recursos;

8.2. Os equipamentos devem ser novos, ou seja, de primeiro uso, de um mesmo fabricante. Na data da proposta, nenhum dos modelos ofertados poderão estar listados no site do fabricante em listas de end-of-life ou end-of-sale;

8.3. Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste Termo de Referência deverão ser fornecidos e atualizados durante a vigência do contrato, seja ele utilizado de forma virtual ou física, local ou em nuvem;

8.4. O licenciamento das soluções de segurança devem estar ativos durante toda a vigência do contrato, sendo de responsabilidade da CONTRATADA realizar a ativação em tempo hábil para que as proteções de segurança e todas as funcionalidades das soluções estejam disponíveis. O atraso na ativação das licenças, deixando o ambiente da CONTRATADA vulnerável ou com funcionalidades limitadas, poderá acarretar responsabilização contratual;

8.5. O gerenciamento das soluções de segurança de primeiro nível, ficará a cargo da equipe da CONTRATANTE;

8.6. A CONTRATADA será responsável pelos serviços de suporte nível 2 (dois) e nível 3 (três), bem como, a instalação/implantação e a migração das soluções do LOTE;

8.7. Caso haja necessidade a CONTRATANTE poderá solicitar auxílio mediante solicitação para realizar quaisquer atividades inerentes às soluções de segurança ora especificadas à CONTRATADA.

9. DA GARANTIA DE BANDA – LOTE 01 E LOTE 02

9.1. Os serviços de acesso à internet e conectividade MPLS por meio dos links dedicados deverão possuir garantia mínima de 99,35% (noventa e nove vírgula trinta e cinco por cento) da banda contratada, para download e upload;

9.2. Os serviços de acesso à internet deverão possuir latência (A latência é o tempo que um pacote IP leva para ir e voltar (round-trip) de um ponto a outro da rede) menor que 80 (oitenta) milissegundos e no máximo 2% de perda de pacotes no circuito, comprovados através de relatórios estatísticos de acompanhamento. Os relatórios poderão ser solicitados pela CONTRATANTE à CONTRATADA a qualquer tempo;

9.3. Requisitos obrigatórios para os links urbanos e interurbanos:

ITEM	REFERÊNCIA	URBANO (CAPITAL INTERNET)	INTERURBANO (INTERIOR INTERNET)	INTERURBANO (INTERIOR MPLS)

Tipo de Acesso	Acesso por Fibra Óptica, que garantam o funcionamento de todas as especificações deste Termo de Referência	Sim	Sim	Sim

Assinado eletronicamente por **AMILAR SALES ALVES**, **Técnico Judiciário**, em 19/04/2024 11:10:31
Assinado eletronicamente por **ELSON CORREIA DE OLIVEIRA NETO**, **Gerente de Segurança da Informação**, em 19/04/2024 11:09:14

Disponibilidade de Serviço	Relação entre o tempo de operação plena e prejudicada no período de 30 dias	99,35%	99,35%	99,35%
Tempo Máximo de Retardo Admissível	O tempo máximo de retardo na comunicação unilateral entre o ponto de conexão e o roteador de borda da Proponente para um pacote de 32 bytes	Fibra Óptica: = ou < 80 MS	Fibra Óptica: = ou < 100 MS	Fibra Óptica: = ou < 50 MS
Banda Mínima Garantida	Banda mínima disponível para acesso à Internet para cada um dos pontos contemplados	Fibra Óptica: 100% da banda	Fibra Óptica: 100% da banda	Fibra Óptica: 100% da banda
Ativação	Período entre a solicitação e ativação do Serviço	Até 60 (sessenta) dias	Até 60 (sessenta) dias	Até 60 (sessenta) dias
Prazo de Manutenção	Período máximo para o restabelecimento do serviço, contado a partir do momento da abertura do chamado até a finalização do atendimento	12 (doze) horas	24 (vinte e quatro) horas	24 (vinte e quatro) horas
Prazo Mínimo de notificação de Manutenção Preventiva ou Atualização de Recursos Técnicos	Período mínimo entre a notificação do cliente pela operadora até o início da interrupção programada	07 (sete) dias	07 (sete) dias	07 (sete) dias

Abertura de Chamado	Disponibilidade de atendimento para solicitações de reparos, *HELPDESK* da Operadora CONTRATADA e discagem sem cobrança (0800) em língua portuguesa	24 x 07 (00:00 às 24:00 de Segunda a Domingo)	24 x 07 (00:00 às 24:00 de Segunda a Domingo)	24 x 07 (00:00 às 24:00 de Segunda a Domingo)
Horário de Reparo	Disponibilidade de atendimento técnico a partir da abertura da chamada	24 x 07 (00:00 às 24:00 de Segunda a Domingo)	24 x 07 (00:00 às 24:00 de Segunda a Domingo)	24 x 07 (00:00 às 24:00 de Segunda a Domingo)
	Casos de responsabilidade da CONTRATADA: (Período máximo para o restabelecimento do serviço, contado a partir do momento da abertura do chamado até a finalização do atendimento)	Em Rio Branco: Máximo de 03 (três) horas	Até 300 km de Rio Branco: Máximo de 06 (seis) horas	Acima de 300 km de Rio Branco: Máximo de 12 (doze) horas

10. CARACTERÍSTICAS DOS SERVIÇOS – REDE TJAC.NET

10.1 A rede TJAC será composta pelos links listados nos LOTE 1 e LOTE 2, deste Termo de Referência;

10.2. A LICITANTE deverá fornecer senha de acesso com permissão a acesso de leitura dos equipamentos, a fim de proporcionar ao TJAC ferramentas de avaliação técnica, proporcionando adoção de ações preventivas ou corretivas;

10.3. Os roteadores fornecidos pela LICITANTE deverão estar com SNMP, COMUNIDADE, RMON e TRAP habilitados para leitura, de sorte a proporcionar ao TJAC ferramentas de avaliação técnica, proporcionando adoção de ações preventivas ou corretivas;

10.4. O link concentrador deverá ser entregue pela CONTRATADA em um único meio físico, sem fracionar (Mux, modem óptico ou outro equipamento);

10.5. Seguir o padrão DSCP (DiffServ Code Point), conforme a RFC 2474;

10.6. Possuir suporte à tradução de endereços IP (NAT);

10.7. Possuir suporte a classe de serviço para fragmentação de pacotes;

10.8. Possuir suporte a classe de serviço para reserva de banda;

10.9. Possuir suporte a classe de serviço para listas de controle de acesso;

10.10. A topologia da rede TJAC deverá ser full-mesh ou hub-spoke, mediante solicitação da CONTRATANTE, sendo o padrão full-mesh;

10.11. Os serviços de intranet são os acessos à rede virtual privada (VPN), a ser criada pela CONTRATADA em seu backbone IP/MPLS, por onde fluirá o tráfego de dados entre as diversas unidades do CONTRATANTE;

10.12. Garantir o roteamento das conexões dedicadas utilizando protocolo MPLS – Multiprotocol Label Switching;

10.13. Cada acesso não poderá ser compartilhado com nenhum outro cliente da CONTRATADA e deverá ser capaz de absorver 100% (cem por cento) do tráfego referente à velocidade contratada;

10.14. Operar em conformidade com, no mínimo, as seguintes RFCs:

10.14.1. RFC 3031: “Multiprotocol Label Switching Architecture”;

10.14.2. RFC 3032: “MPLS Label Stack Encoding”;

10.14.3. RFC 3270: “Multi-Protocol Label Switching (MPLS) Support of Differentiated Services”;

10.14.4. RFC 2474: “Definition of the Differentiated Services Field in the IPv4 and IPv6 Headers”;

10.14.5. RFC 2475: “An Architecture for Differentiated Services”.

10.15. Permitir a classificação e marcação de diferentes níveis de tráfego (CoS e QoS), sendo implementadas as seguintes classes de serviço:

10.15.1. Tempo Real Voz e/ou Vídeo: Aplicações sensíveis ao retardo (delay) e variações de retardo da rede (jitter), que exigem a priorização de pacotes de dados e reserva de banda na rede;

10.15.2. Dados Prioritários: Aplicações interativas, que exigem entrega garantida e tratamento prioritário. São os dados envolvidos nas aplicações essenciais às atividades fins do CONTRATANTE;

10.15.3. Dados Comuns (mínimo 25% da banda total do acesso): Aplicações com mensagens de tamanho muito variado e não imprescindíveis às atividades fins do CONTRATANTE, aplicativos de dados que não necessitam de priorização, como páginas web, e-mails. Para esta classe a rede deverá permitir o fluxo do tráfego de dados por meio da técnica best effort e impedindo que esse tráfego afete negativamente as demais classes.

10.16. A banda a ser definida para cada classe de serviço em cada acesso da rede será acordada futuramente entre o CONTRATANTE e a CONTRATADA, quando da solicitação do serviço;

10.17. O serviço contratado deverá permitir modificações ou ampliações sem que estas impliquem na interrupção do restante das conexões da rede;

10.18. Poderão ser solicitados, durante a vigência do contrato, novos acessos, alterações de velocidade, de tipo, de classes de serviços ou mudanças de endereço;

10.19. Quaisquer alterações dos serviços serão solicitadas pelo CONTRATANTE, através de documento próprio a ser definido após a assinatura do contrato;

10.20. É de responsabilidade do CONTRATANTE definir o endereçamento IP da rede, bem como suas regras de roteamento;

10.21. Caso o CONTRATANTE necessite alterar o endereçamento IP e/ou as regras de roteamento, o prazo de atendimento será acordado entre as partes e a solicitação será mediante ofício entregue a CONTRATADA.

11. SUBSTITUIÇÃO OU TROCA DOS EQUIPAMENTOS

11.1. Todos os equipamentos entregues no âmbito deste Termo de Referência e da futura contratação, deverão ser substituídos sem ônus ao CONTRATANTE, a qualquer tempo, durante a vigência do contrato, nos seguintes casos:

11.1.1. Caso entre em end-of-support pelo fabricante do equipamento;

11.1.2. Caso esteja em end-of-sale no momento da entrega;

11.1.3. Caso deixe de receber atualizações de firmware ou sistema operacional do fabricante que contenham novas funcionalidades ou otimizações, sendo desconsiderado atualizações críticas de segurança;

11.1.4. Caso a utilização de memória ou processamento estejam afetando o desempenho do equipamento, após diagnóstico com a CONTRATADA ou fabricante;

11.1.5 Em outros casos, quando necessário, avaliados em conjunto com a CONTRATADA, sempre levando em consideração a disponibilidade dos serviços e a prestação jurisdicional.

11.2. A CONTRATADA terá 60 dias corridos para realizar a substituição ou troca, a contar da formalização do pedido pela CONTRATANTE ou a detecção proativa da necessidade por parte da CONTRATADA; 11.3.Os equipamentos substitutos, deverão ter a especificação igual ou superior a contida neste Termo de Referência;

11.4. No caso “11.1.4”, a especificação do equipamento substituto deverá ser suficiente para atender a demanda do CONTRATANTE, de modo a solucionar o problema de utilização de processamento ou memória.

12. CONDIÇÕES GERAIS

12.1. Para quaisquer itens a serem fornecidos, a CONTRATADA não poderá fornecer IP fixo PRIVADO, somente IPs PÚBLICOS e válidos para a rede pública de internet;

12.2. A CONTRATADA será responsável pelo fornecimento, de todos os insumos necessários (modens, roteadores, equipamentos para fibra óptica etc.) para o correto funcionamento de acesso à internet, conforme especificado neste Termo de Referência;

12.3. A CONTRATADA deve realizar a instalação do link no rack de telecomunicações da CONTRATANTE em cada endereço fornecido na Ordem de Serviço ou em rack próprio, fornecido pela CONTRATADA, caso necessário;

12.4. O preparo da infraestrutura, os serviços de instalação e configuração de todos os equipamentos fornecidos será de responsabilidade da CONTRATADA;

12.5. A CONTRATADA deverá garantir o funcionamento de todos os equipamentos e acessórios instalados nas dependências da CONTRATANTE sem a necessidade de operadores locais;

12.6. A CONTRATADA será responsável pelos serviços de manutenção dos links de acesso internet e de todos os equipamentos fornecidos conforme definido neste Termo de Referência;

12.7. Caberá a CONTRATANTE a responsabilidade por toda infraestrutura elétrica (aterramento, DG etc.) interna às unidades dos órgãos necessária para o funcionamento adequado do serviço;

12.8. O serviço deverá ser prestado 24 horas por dia, 07 dias por semana, todos os dias do ano, durante todo o período de vigência do contrato, salvaguardados os casos de interrupções programadas, devidamente autorizadas pelo CONTRATANTE;

12.9. Qualquer interrupção programada pelo provedor para manutenção preventiva e/ou substituição dos equipamentos e meios utilizados, desde que possa causar interferência no desempenho do serviço prestado, deverá ser comunicada à CONTRATANTE com antecedência mínima de 5 (cinco) dias úteis, por meio de correio eletrônico ou WhatsApp, e somente será realizada com a concordância do CONTRATANTE;

12.10. As interrupções programadas deverão ser efetuadas no período compreendido entre 22h e 05h do horário do Acre;

12.11. A CONTRATADA deverá fornecer as conexões dedicadas à CONTRATANTE obrigatoriamente terrestres e implementadas por meio de fibra óptica;

12.12. O serviço deverá ser ofertado com velocidades simétricas, links full duplex;

12.13. A CONTRATADA deverá instalar os links de Internet, sendo que tal acesso não poderá ser compartilhado com nenhum outro cliente da CONTRATADA, com a garantia de qualidade de serviços mínima exigida;

12.14. A equipe técnica da CONTRATANTE definirá e repassará à CONTRATADA o “range” de endereçamento IP LAN utilizado na rede local tanto da Sede do TJAC quanto de suas unidades do interior, quando da instalação dos links de acesso à internet e configurações dos equipamentos. O endereçamento IP LAN a ser utilizado é privado;

12.15. O endereçamento IP WAN a ser utilizado pela(s) CONTRATADA(s) nas conexões dedicadas fornecidas deve ser restrito da respectiva operadora, ou seja, IP não divulgado e nem utilizado pelo público Internet;

12.16. Os equipamentos fornecidos, bem como os links de internet deverão suportar e implantar o roteamento de endereços IPv4 e IPv6 nativamente;

12.17. A CONTRATADA deverá respeitar integralmente os índices de SLA (Service Level Agreement ou Acordo de Nível de Serviço) definidos neste Termo de Referência;

12.18. A CONTRATADA deverá fornecer circuito com conectividade direta com a internet através de acessos dedicados em fibra óptica em anel redundante automaticamente, e portas IP exclusivas com o

fornecimento total de conectividade IP (Internet Protocol) com suporte a aplicações TCP/IP;

12.19. A CONTRATADA deverá prover o acesso direto à internet, de forma não compartilhada, devendo estar disponível 24 (vinte e quatro) horas por dia, durante os 07 (sete) dias da semana, e constituir-se de acessos permanentes, dedicados, e com total conectividade IP, interligando a CONTRATADA à internet através de canais privativos que possuam redundância de rota até ao backbone da CONTRATADA fora do Estado;

12.20. A CONTRATADA deverá prover gerência proativa da porta IP, a qual consiste em monitorar a porta do roteador instalado na CONTRATANTE, efetuando a verificação automática da disponibilidade do link no máximo a cada 05 (cinco) minutos. Caso o roteador da CONTRATANTE não responda após 03 (três) tentativas, deverá ser disparado procedimentos de correção e a CONTRATANTE deverá ser avisada em até 30 minutos;

12.21. A CONTRATANTE poderá solicitar, de acordo com sua necessidade, mudança de numeração de bloco de endereços IPs válidos, sem custo adicional;

12.22. O backbone oferecido deve possuir, em operação, canais próprios e dedicados, interligado diretamente a pelo menos 1 (um) outro sistema autônomo (AS Autonomous Systems) nacional com saída a partir do estado do Acre, e a pelo menos 1 (um) outro sistema autônomo (AS Autonomous Systems) internacional. Deverá o somatório das bandas de saída entre os AS (nacional e internacional) ser de pelo menos 1 Gigabit/s;

12.23. A CONTRATADA deverá disponibilizar sistema que permita aferir a qualidade do backbone de internet ao qual o CONTRATANTE está conectado, fornecendo, no mínimo: latência do backbone, perda de pacotes do backbone, se limitando ao serviço prestado pela CONTRATADA, o monitoramento entre o CPE (Customer Premises Equipment) e PE (Provider Edge) e disponibilidade do backbone.

13. ACORDO DO NÍVEL DE SERVIÇOS (SLA) – LOTE 01 E LOTE 02

13.1. Entende-se por disponibilidade média mensal do núcleo da rede o índice que mede o tempo que uma rede esteve operacional para transmissão e recepção de pacotes IP;

13.2. A CONTRATADA deverá garantir que todos os links tenham SLA (Service Level Agreement) estabelecido de, no mínimo, 99,35% (noventa e nove vírgula trinta e cinco por cento) de disponibilidade, a ser medida mensalmente através de ferramenta disponibilizada, sem custo, pela CONTRATADA;

13.3. O Índice de Disponibilidade Mensal será calculado através da seguinte fórmula:

Id = ((Tm - Ti) / Tm) * 100

Onde:

Id = Índice de Disponibilidade Mensal dos serviços

Ti = Somatório dos Períodos de Indisponibilidade, em minutos, no mês de faturamento

Tm = Tempo Total Mensal de operação, em minutos, no mês de faturamento

13.4. Para o cálculo do índice de disponibilidade, o “Tempo Total Mensal” será calculado a partir do total de

dias da prestação do serviço vezes 1440 (mil quatrocentos e quarenta) minutos.

13.5. Com base no Id - Índice de Disponibilidade Mensal, será calculado a DIFANS - Diferença entre contratado (meta a cumprir) e o Id - Índice de Disponibilidade Mensal.

CÁLCULO DIFANS DESCRIÇÃO DIFANS = MC - ID

DIFANS - Diferença entre o ANS contratado (meta a

cumprir) e o Índice de Disponibilidade Mensal calculado

ID - Índice de Disponibilidade Mensal

MC - Meta a cumprir

13.6. MC - Meta a cumprir é o percentual mínimo de disponibilidade que o link deve estar operante durante o respectivo mês, considerando o ANS e o tipo de link, conforme a seguir:

TIPOS DE ACESSO	**MC**
Links de acesso a Internet e MPLS, urbanos ou interurbanos.	99,35%

Com base no DIFANS - Diferença entre o ANS contratado (meta a cumprir) e Índice de Disponibilidade Mensal, será definido o desconto a ser aplicado sobre o valor mensal do respecitvo link, conforme a seguir:

FAIXA DE DIFERENÇA	**DESCONTO**
$0 < DIFANS \leq 0,5$	2%
$0,5 < DIFANS \leq 1,5$	5%
$1,5 < DIFANS \leq 3,0$	10%
$3,0 < DIFANS \leq 6,0$	20%
$DIFANS > 6,0$	40%

13.5. A CONTRATADA deverá enviar, juntamente com o faturamento mensal, em relatório, o cálculo de DIFANS já com a glosa de acordo o resultado do Índice de Disponibilidade Mensal, já deduzido o valor no faturamento mensal, quando houve. Sem prejuízo do ajuste do cálculo de acordo as medições do CONTRATANTE.

13.6. Quando houver incidência de desconto, será aplicado no mês seguinte à ocorrência.

13.7. Será aplicada multa de 1,0% sobre o valor mensal referente ao link, nos casos de não atendimento ao ANS contratado a cada período igual a 3 (três) meses, seguidos ou não (em qualquer tempo).

13.8. Não serão considerados os tempos de parada do(s) link(s) nos casos considerados como indisponibilidade justificada, ou seja, falta de energia nas dependências do CONTRATANTE, manutenções programadas e motivos de força maior.

13.9 Qualidade

13.9.1 Para cada link, a partir da data do respectivo aceite de instalação, serão monitorados mensalmente parâmetros de qualidade referentes à operação do link;

13.9.2. Para apuração da qualidade, serão considerados pelo CONTRATANTE os seguintes indicadores, a serem obtidos por meio de relatórios gerenciais do Sistema de Monitoramento do CONTRATANTE:

13.9.2.1. O tempo máximo de resposta dos pacotes TCP/IP e/ou ICMP/IP (tempo de latência) entre uma conexão dedicada e seu respectivo concentrador deverá ser de no máximo 50ms para links MPLS, no máximo 80ms para links de internet da capital e de 100ms para links de internet do interior.

13.9.2.2. A taxa máxima de erros permitida (relação entre a quantidade de bits recebidos com erro e o total de bits recebidos) deverá ser de até 2% ao mês.

13.9.2.3. Observada a primeira ocorrência de Latência acima do especificado e/ou taxa de erros acima de 2% no respectivo mês, inicialmente será aberto chamado junto à CONTRATADA para correção do problema. Em caso de reincidência, será aplicado desconto sobre o valor mensal do respectivo link, conforme a seguir:

OCORRÊNCIA DESCONTO

Latência > 80 ms e/ou Taxa de Erros acima de 2% ao mês para links de internet capital. 3%

Latência > 100 ms e/ou Taxa de Erros acima de 2% ao mês para links de internet interior. 3%

Latência > 50 ms e/ou Taxa de Erros acima de 2% ao mês para links MPLS do interior. 3%

13.9.2.4. Quando houver incidência de desconto, será aplicado no mês seguinte à ocorrência.

13.9.2.5. Será aplicada multa de 1,0% sobre o valor mensal referente ao link, nos casos de não atendimento ao ANS contratado a cada período igual a 3 (três) meses, seguidos ou não (em qualquer tempo).

13.9.2.6. Não serão considerados os tempos de parada do(s) link(s) nos casos considerados como indisponibilidade justificada, ou seja, falta de energia nas dependências do CONTRATANTE, manutenções programadas e motivos de força maior.

14. USO DE TRUNKING

14.1. Será permitido, se for o caso, o uso de “trunking”, ou seja, o uso de mais de um enlace para atingir a

velocidade para cada link contratado;

14.2. Para utilização de “trunking” a CONTRATADA deve observar que o link somente será considerado ativo caso todos os enlaces que compõem o “trunking” estejam funcionando corretamente, ou seja, a falha em um dos enlaces que compõem o “trunking” significa que o link contratado não estará ativo corretamente, implicando em abertura de chamado de manutenção.

15. FORNECIMENTO DE EQUIPAMENTOS E ACESSÓRIOS

15.1 Os seguintes insumos devem ser fornecidos para o funcionamento dos links de acesso à internet dedicados:

15.1.1. Cabos e adaptadores;

15.1.2. Cabo de conexão do roteador com modem ou outro equipamento utilizado para acesso à internet;

15.1.3. Cabos de energia elétrica para todos os equipamentos fornecidos;

15.1.4. Adaptadores ópticos para conexões implementadas por meio de fibra óptica;

15.1.5. Para os LOTES 01 e 02, cordões e cartões GBIC compatível com as interfaces disponíveis, para conexão de LAN ou outros itens necessários.

15.2. Deve ser fornecido modem (convencional, óptico, rádio digital, dentre outros) ou outro equipamento para permitir a conexão do Roteador CPE ao ambiente WAN da CONTRATADA;

15.3. Deve ser fornecido roteador CPE (Customer Premise Equipment) ou poderá ser fornecido também equipamento híbrido que realize as duas funções (modem e roteador) ou ainda, desde que previamente acordado com a CONTRATADA, utilização dos equipamentos de segurança de borda como CPE;

15.4. Deve ser dimensionado para que tenham capacidade de encaminhamento de pacotes IP, em pacotes por segundo, compatíveis com as velocidades dos links conectados, limitado o uso de processador e memória a 60% do total disponível quando da carga máxima do link;

15.5. Caso seja identificado, durante a execução do contrato, um roteador com uso máximo de CPU e memória acima dos limites estabelecidos, o equipamento deverá ser substituído ou atualizado, em um prazo máximo de até 5 (cinco) dias úteis, sem ônus para a CONTRATANTE;

15.6. O equipamento roteador deverá ser fornecido pela empresa e acoplável a rack de 19”, atendendo às seguintes especificações para o ITEM 01 do LOTE 01 e do LOTE 02:

15.6.1. Possuir, no mínimo, 01 (uma) interface porta óptica de acordo com os Standarts ITU-G.984 GPON;

15.6.2. Possuir, no mínimo, 04 (quatro) interfaces Gigabit Ethernet 10/100/1000 de detecção automática que sejam compatíveis com os padrões ISSO 8802.3 e IEE 802.3;

15.6.3. A interface física da porta LAN deverá ser fornecida no padrão RJ-45 (10BASE-T), para cabos UTP, CAT 6 ou AUI;

15.6.4. Possuir opção de boot local via memória flash ou similar;

15.6.5. Permitir ser alimentado de forma automática por tensões de 110/220 VAC, frequência 60 Hz com

duas fontes redundantes inclusas;

15.6.6. Deverá suportar e implementar serviços de DHCP Server.

15.7. Possuírem todas as facilidades de gerenciamento que permitam o fornecimento adequado de todos os serviços especificados, destacando:

15.7.1. Gerenciamento SNMP compatível com as versões v2c e v3;

15.7.2.Protocolo SNMP habilitado, com acesso de leitura por parte da CONTRATANTE;

15.7.3. Permissão para a configuração de "traps" por parte da CONTRATADA, a pedido da CONTRATANTE, para monitoração de eventos específicos. Caso necessária, esta configuração será solicitada com pelo menos 15 (quinze) dias de antecedência da data real de monitoramento;

15.7.4. Suporte a MIB-II e RMON;

15.7.5. Suporte à classificação de tráfego.

15.8. A CONTRATADA deverá fornecer acesso à leitura de configuração por parte da

15.9. CONTRATANTE, através de "usuário" e "senha" específicos;

15.10. Deve manter a hora sincronizada através do protocolo NTP (Network Time Protocol) – RFC 1305 ou protocolo SNTP (Simple Network Time Protocol) versão 4 – RFC 2030;

15.11. Todos os equipamentos fornecidos devem ser capazes de operar em 110/220V.

16. DAS INSTALAÇÕES

16.1. A CONTRATADA realizará a instalação dos links de acesso à internet considerando as velocidades definidas pela CONTRATANTE para cada item e cada localidade de acordo com o Termo de Referência;

16.2. Todos os materiais e serviços de instalação dos links de acesso à internet até o rack da CONTRATANTE que acomoda os equipamentos de comunicação de dados, são de inteira responsabilidade da CONTRATADA, incluindo o acesso aos prédios por via aérea ou subterrânea, quando necessário, sem acarretar nenhum ônus adicional à CONTRATANTE;

16.3. Deve haver planejamento do horário de trabalho de instalação dos links de acesso à internet conjuntamente com a equipe da CONTRATANTE, de maneira a interferir o mínimo possível nos trabalhos normais de cada localidade;

16.4. A CONTRATADA deverá recompor obras civis e pintura eventualmente afetadas quando da passagem dos cabos, mantendo o padrão local, excetuando-se os casos em que estas ocorrências sejam consequência de adaptações na infraestrutura necessária para passagem dos cabos.

17. DOS TESTES PARA ACEITE DOS LINKS INSTALADOS

17.1. Realizar testes de funcionamento de cada link dedicado, emitindo relatórios de testes em duas vias, as quais deverão ser assinadas pelos executores e pelos servidores designados para acompanhar as

instalações;

17.2. Aferição da velocidade do link instalado, tanto para download como para upload;

17.3. Verificação da performance dos links instalados e perdas de pacotes;
17.4. Verificação da conformidade técnica dos insumos com o exigido no Termo de Referência;
17.5. Caso o resultado dos testes seja desfavorável, a CONTRATADA deverá solucionar os problemas no prazo máximo de 05 (cinco) dias úteis a partir do recebimento da notificação. 17.6. Caberá a CONTRATANTE dar o aceite ou não a solução dada para o problema;
17.7. Para fins de pagamento, o link só deverá começar a ser faturado após a aceitação dada com base na avaliação dos testes pela equipe técnica da CONTRATANTE.

18. ALTERAÇÃO QUALITATIVA

18.1. É facultado à CONTRATANTE solicitar alteração de velocidade dos links de acesso à internet contratados por meio de aditivo contratual qualitativo, nos limites estabelecidos na legislação, sempre com cotações prévias para constatação da vantajosidade do preço de mercado, desde que haja viabilidade prévia da CONTRATADA;
18.2. Após a alteração de velocidades, a CONTRATADA deverá realizar os testes de funcionamento, sempre acompanhados pelos técnicos do CONTRATANTE, e emitir os relatórios de testes em duas vias, os quais deverão ser assinados pelos executores e pelo responsável em cada local de instalação;
18.3. Sempre que necessário as partes poderão em comum acordo realizar melhorias qualitativas visando a adequação a uma ou várias tecnologias disponíveis para a correta execução do serviço. (Ex. infraestrutura de par metálico para fibra (GPON), ou de estrutura de endereçamento de IPV4 para IPV6).

19. MUDANÇA DE ENDEREÇO

19.1. Em caso de mudança de endereço da unidade da CONTRATANTE onde existir link de acesso à internet ou MPLS instalado, um novo link será solicitado para o novo endereço para não haver interrupção do serviço da CONTRATANTE;
19.2. O link instalado no endereço anterior será desativado assim que o novo enlace for instalado conforme solicitado. Portanto, não haverá solicitação de um novo link e sim, ativação de link existente em outra localidade, logo, não devendo haver ônus a CONTRATANTE;
19.3. A providência de equipamentos para suportar novos links, conforme especificados neste Termo de Referência, será de inteira responsabilidade da CONTRATADA, que deve manter a estrutura de equipamentos do link em uso até que seja solicitada sua desativação;
19.4. Até 45 dias corridos para realizar a mudança após o aceite na solicitação. As mudanças de endereço dentro dos limites do município da instalação dos links, serão de forma não onerosa à CONTRATANTE. Havendo a necessidade de desenvolvimento de projetos especiais para mudança de endereço e/ou adição de novas unidades, a CONTRATADA deverá apresentar uma planilha de valores referente à alteração/adição, para prévia aprovação da CONTRATANTE, em até 15 dias corridos da solicitação de mudança.

20. DESATIVAÇÕES DOS LINKS DE ACESSO À INTERNET

20.1. Toda desativação deverá ocorrer somente após solicitação formal da equipe técnica do CONTRATANTE, obedecendo os limites de supressão impostos no § Art. 125 da Lei n. º 14.133/2021;
20.2. Todos os equipamentos inerentes ao link desativado deverão ser recolhidos pela CONTRATADA no prazo máximo de 30 (trinta) dias a partir da data da solicitação de desativação do link, mediante agendamento prévio.

21. MANUTENÇÃO

21.1. O serviço de manutenção deve ser prestado pela CONTRATADA, que deve atender obrigatoriamente às seguintes condições:
21.2. O serviço será considerado indisponível a partir do início de uma interrupção identificada pela CONTRATANTE, devidamente registrada através de abertura do chamado na central de atendimento da CONTRATADA, até o restabelecimento do circuito às condições normais de operação com a respectiva constatação do CONTRATANTE através da autorização para o encerramento do chamado;
21.3. Quando não for possível a CONTRATANTE realizar a abertura de chamado na central de atendimento da CONTRATADA, a indisponibilidade será considerada a partir da efetiva interrupção registrada pelos sistemas da CONTRATANTE e/ou CONTRATADA;
21.4. Entende-se como condições normais de operação a estabilidade dos serviços prestados, sem a ocorrência de novas interrupções no curto prazo, e a manutenção de todos os parâmetros de qualidade dentro dos níveis especificados;
21.5. Todos os serviços de manutenção dos links de acesso à internet e MPLS são de inteira responsabilidade da CONTRATADA e devem ser efetuados desde o início até o final do contrato, bem como devem estar totalmente cobertos pelo pagamento mensal relativo ao fornecimento de cada um dos links de acesso, sem quaisquer custos adicionais à CONTRATANTE;
21.6. Efetuar manutenção corretiva assim que for detectado algum mau funcionamento de enlaces e equipamentos, ou problemas em instalações feitas, de forma que voltem a funcionar perfeitamente;
21.7. Entende-se por manutenção corretiva os serviços prestados para recolocar os links de acesso à internet ou MPLS em modo operacional e na velocidade contratada, compreendendo, inclusive, substituições e configurações dos equipamentos fornecidos em comodato;
21.8. Entende-se por manutenção preventiva os serviços prestados para detectar possíveis falhas, perda de pacotes, instabilidades, sobrecarga nos equipamentos, ajustes de configurações etc., com objetivo de antecipar as devidas correções e evitar mau funcionamentos dos links nos períodos críticos;
21.9. Realizar o serviço de manutenção no local de instalação do equipamento sempre que possível. Caso

seja necessário remover o equipamento, a CONTRATADA deve providenciar a substituição do equipamento

por outro idêntico ou superior, em perfeito funcionamento, para então retirar o equipamento com defeito e encaminhá-lo para a manutenção;

21.10. Permitir efetuar a “Abertura de Chamado de Manutenção” junto a “Central de Atendimento” da CONTRATADA por meio de um telefone “0800” ou e-mail ou WhatsApp desde que seja gerado um número ou protocolo de atendimento;

21.11. Entende-se por “conclusão do atendimento” o pleno restabelecimento da funcionalidade e do desempenho dos serviços de acesso à internet, incluindo a troca de peças ou componentes e a execução de quaisquer procedimentos corretivos que se façam necessários;

21.12. A conclusão do atendimento será registrada. Essa informação será utilizada para averiguar o cumprimento dos acordos de nível de serviço previstos;

21.13. A conclusão de um atendimento requer a concordância, por parte de um membro da equipe técnica da CONTRATANTE;

21.14. O tempo para atendimento por atendente em sistemas de autoatendimento não poderá ser superior ao definido no Art. 27 da Resolução nº 632 de 07/03/2014, da ANATEL;

21.15. A CONTRATADA deve ser responsável por todos os técnicos que forem realizar manutenção dos enlaces em qualquer uma das localidades onde houver links de acesso à internet instalados;

21.16. Garantir que os técnicos de suporte tenham conhecimento completo sobre toda a arquitetura de rede utilizada, e de todos os equipamentos e softwares de responsabilidade da CONTRATADA que integram a modalidade de acesso à internet.

21.17. O término do PNF (Período de Não Funcionamento do Link) será computado a partir do aceite da manutenção (fechamento do chamado) feito pela equipe técnica do CONTRATANTE, sendo necessária a identificação do técnico responsável pelo fechamento do chamado;

21.18. O somatório de PNF em minutos, durante um mês, que exceder o tempo de parada permitido neste mesmo período, será tomado como base de desconto da parcela mensal de pagamento (do concentrador ou conexão dedicada remota que teve seu serviço interrompido) no mês subsequente. A consolidação dos “períodos de não funcionamento do enlace” será feita com base nas informações obtidas no Sistema de Monitoramento do CONTRATANTE.

22. MONITORAMENTO DO CONTRATANTE

22.1. A CONTRATADA deverá disponibilizar acesso via protocolo SNMP, com permissão de leitura nos equipamentos referentes aos links contratados no regime 24x7 (24 horas por dia, 7 dias por semana), durante a vigência do contrato;

22.2. A CONTRATADA deverá ter conhecimento e ciência do Sistema de Monitoramento do CONTRATANTE para fins de aferição dos serviços prestados;

22.3. Para o monitoramento a CONTRATANTE fará uso de ferramentas de coleta de dados como ZABBIX,

via protocolo SNMP, nos equipamentos da CONTRATADA;

22.4 Os dados coletados nos equipamentos da CONTRATADA, pelo Sistema de Monitoramento do CONTRATANTE, serão usados como mecanismo de aferição, contraprova, e terão validade administrativa na verificação do cumprimento da DISPONIBILIDADE dos serviços.

23. ESPECIFICAÇÕES MÍNIMAS PARA A SOLUÇÃO DE GERÊNCIA DE REDE

23.1. A CONTRATADA deverá prover Solução de Gerência da Rede que contemple os módulos de gerência de falhas, desempenho, disponibilidade, capacity planning, relatórios, tickets e de nível de serviço:

23.2. A Solução de Gerência da Rede deverá disponibilizar a visualização de informações on-line (de forma gráfica) da rede para o acompanhamento e monitoração do estado global e detalhado do ambiente;

23.3. Em caso de formação de consórcio deverá ser provida uma única Solução de Gerência de Rede;

23.4. A Solução de Gerência da Rede da CONTRATADA deverá atuar de forma proativa, antecipando-se aos problemas na rede e garantindo o cumprimento do Acordo de Nível de Serviço (ANS), realizando abertura, acompanhamento e fechamento de chamados de falhas relacionados com indisponibilidade, operando em regime 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, todos os dias do ano;

23.5. A Solução de Gerência da Rede fornecida deve permitir acesso a todos os recursos e módulos através de única autenticação, sem a necessidade de realizar outros logins para acessar qualquer outro recurso de gerenciamento;

23.6. A Solução de Gerência da Rede deverá ser operada e administrada através de uma console única, portanto, não serão aceitas soluções que possuem acessos segmentados aos módulos;

23.7. Deverá ser escalável, permitindo futuras ampliações no número de elementos de rede a serem gerenciados;

23.8. Deverá permitir acessos de usuários com perfis diferenciados com limitação de acesso a consoles, dispositivos, menus, alarmes, indicadores etc.;

23.9. Deverá permitir acesso de até 5 (cinco) usuários logados simultaneamente;

23.10. A Solução de Gerência da Rede deverá permitir a criação de grupos de perfis de acesso, que serão associados a tipos de usuários;

23.11. Os perfis deverão prever configurações em níveis de alertas, equipamentos, interfaces, aplicações, funcionalidades de monitoração, capacity planning, inventário etc.;

23.12. A Solução de Gerência da Rede deverá ser 100% web sem necessidade de instalação de clientes específicos, portanto, não serão aceitas soluções que não sejam nativas em web ou que requeiram a instalação de agentes ou plugins nos desktops dos colaboradores da CONTRATANTE;

23.13. O acesso deverá ser via web padrão HTTP e suportar HTTPS, e em português, portanto não serão aceitas soluções que não possuam toda a sua estrutura em português;

23.14. A Solução de Gerência da Rede deverá ser compatível para acesso através de smartphones e tablets,

portanto não serão aceitas soluções que não possuam essa compatibilidade;

23.15. A Solução de Gerência da Rede deverá ser escalável, mas transparente para a CONTRATANTE em termos de console única;

23.16. A Solução de Gerência da Rede deverá ser acessível através dos principais browsers do mercado, tais como: Internet Explorer, Firefox, Google Chrome e Safari;

23.17. Deverá permitir a exportação das informações para relatórios em formatos comerciais;

23.18. A Solução de Gerência da Rede deverá gerar alertas quando os thresholds "limites" configurados para um componente monitorado são excedidos, a exemplo de: utilização de CPU, memória, interfaces, volume de erros, tempo de resposta de serviços;

23.19. A Solução de Gerência da Rede deverá fornecer, através do portal, visualização de informações on line (em intervalos de 5 minutos e de forma gráfica) da rede que deverá apresentar, no mínimo, os seguintes itens para cada um dos elementos monitorados:

23.19.1. Topologia da rede, incluindo os roteadores CPE e seus enlaces, com visualização do estado operacional de todos os elementos da rede (enlaces e equipamentos). O estado operacional dos elementos da rede deverá ser atualizado automaticamente na Solução de Gerência da Rede, sempre que estes sofrerem alterações;

23.19.2. Alarmes e eventos ocorridos na rede com informações de data, hora e duração de ocorrência e identificação dos recursos gerenciados;

23.19.3. Consumo de banda dos enlaces (entrada e saída) separados por dia e mês;

23.19.4. Consumo de banda por classe de serviço separados por dia e mês;

23.19.5. Ocupação de memória e CPU dos roteadores CPE;

23.19.6. Retardo dos enlaces separados por dia e mês;

23.19.7. Perda de pacotes (descarte) no sentido IN e OUT em %;

23.19.8. Taxa de erros em erros por segundo;

23.19.9. Latência em milissegundos.

23.20. A Solução de Gerência de Rede de possuir gráficos de Capacity Planning que permita criar uma série de cenários para projeções de tendências de um determinado recurso;

23.21. A Solução de Gerência da Rede deverá permitir a apresentação de indicadores que reflitam o nível de SLA (Service Level Agreement) e SLM (Service Level Management) dos serviços contratados;

23.22. Backup de configuração dos elementos gerenciados, alarmes para alterações realizadas, relatório de mudanças;

23.23. Inventário dos equipamentos e enlaces da rede contendo, no mínimo, as seguintes informações:

23.23.1. Enlace: designação, tecnologia e nível de serviço;

23.23.2. Roteador CPE: fabricante, modelo e configuração física (interfaces, memória, slots, dentre outros);

23.23.3. . Endereçamento lógico: endereços IPs e máscaras.

23.24. A Solução de Gerência da Rede deverá permitir adicionar a nomenclatura conhecida pelo CONTRATANTE para os recursos gerenciados;

25.25. A Solução de Gerência da Rede deverá permitir a criação, no mínimo dos seguintes relatórios:

25.25.1. Relatórios de desempenho sumarizado por período específico;

25.25.2. Relatórios de desempenho classificados em uma visão TOP N. Ex.: Top N Roteadores % de utilização de CPU, Top N Interfaces % de utilização, Top N Interfaces com descartes, Top N Interfaces com eventos de Latência;

25.25.3. Relatórios de disponibilidade com períodos específicos;

25.25.4. Permitir exportar os relatórios conforme os principais métodos como: pdf, csv, pacote office.

25.26. Possuir dashboards relacionando falhas, desempenho, capacity e disponibilidade;

25.27. Possuir dashboards executivos com visão sumarizadas de indicadores operacionais (Pro atividade, Taxa de Reincidência, Reparos no Prazo e Taxa de Falha);

25.28. A Solução de Gerência da Rede deverá realizar registro de todas as ocorrências de alarmes/eventos em log de históricos e/ou em base de dados contendo informações de data e hora de ocorrência, identificando os recursos gerenciados;

25.29. A Solução de Gerência da Rede deverá armazenar os dados de acesso e aplicações de internet por um período de 6 (seis) meses, na forma do Art. 15 da Lei Federal nº 12.965/2014 (Lei do Marco Civil da Internet).

24. DA ENTREGA E DO RECEBIMENTO DO OBJETO

2241. A entrega do Lote 01 e 02, acompanhado dos acessórios e equipamentos será conforme especificado em cada item;

24.2. Os endereços informados poderão sofrer alterações até o momento da solicitação de instalação dos serviços pela CONTRATANTE, desde que se obedeça aos limites do município a qual o item foi contratado;

24.3. A entrega deverá contemplar as seguintes localidades:

LOCAL	**ENDEREÇO**
DITEC	Anexo I da Sede do Tribunal de Justiça DC 1 e/ou no DC 2 localizado na Cidade da Justiça.
Cidade da Justiça	Av. Paulo Lemos de Moura Leite, 878. Portal da Amazônia 69915-777 – Rio Branco-AC
Fórum de Senador Guiomard	Avenida Castelo Branco, S/N – CEP 69.925-000. Senador Guiomard
Fórum de Plácido de Castro	Rua Juvenal Antunes, 1079 – CEP 69.928- 000. Plácido de Castro.
Fórum de Acrelândia	Avenida Governador Edmundo Pinto, 581 – CEP 69.945-000. Acrelândia

Fórum de Capixaba	Rua Francisco Cordeiro de Andrade, S/N – CEP 69.922-000. Capixaba
Fórum de Xapuri	Rua Floriano Peixoto, 62 – CEP 69.930-000. Xapuri
Fórum de Sena Madureira	Rua Cunha Vasconcelos, 689 – CEP 69.940-000. Sena Madureira
Fórum de Manoel Urbano	Rua Mendes de Araujo, 1.267 – CEP 69.950-000. Manoel Urbano
Fórum de Feijó	Travessa Floriano Peixoto, 206 – CEP 69.960-000. Feijó
Fórum de Tarauacá	Avenida Antônio Frota, S/N – CEP 69.970-000. Tarauacá
Cidade da Justiça de Cruzeiro do Sul	BR 307, KM 09, nº 4090 – CEP 69.980-000. Cruzeiro do Sul
Fórum de Mâncio Lima	Rua Joaquim G. de Oliveira, 160 – CEP 69.990-000. Mâncio Lima
Fórum de Brasiléia	Avenida Geny Assis, S/N – CEP 69.932-000. Brasiléia
Fórum de Epitaciolândia	BR 317, KM 01 – CEP 69.934-000. Epitaciolândia.
Fórum de Assis Brasil	Rua Dom Giocondo Maria Grotti, 281 – CEP 69.935-000. Assis Brasil
CIC – Centro Integrado de Cidadania	Rua do Comércio, S/N – CEP 69.921-000. Porto Acre
CIC – Centro Integrado de Cidadania	Avenida Presidente Vargas, S/N – CEP: 69.985-000. Rodrigues Alves
Fórum de Bujari	BR 364, KM 28, Nº 390, Bujarí - Acre – CEP 69.923-000
Centro Cultural do Juruá	Praça João Pessoa, n.° 300, Centro. CEP: 69.980-000
Palácio da Justiça	Rua Benjamin Constant, 277, Centro, Rio Branco - Acre - 69905-072

24.4. Havendo interesse e solicitação da CONTRATANTE, a CONTRATADA deverá instalar mais de um link em uma mesma localidade, para atendimento das demandas da CONTRATANTE, sendo esse um link adicional, obedecendo o saldo da quantidade de links para o município contratado;

24.5. Os serviços/equipamentos serão objeto de inspeção, que será realizada por técnico do setor responsável, e constará das seguintes fases:

24.6. Comprovação de que o serviço/equipamento atende às especificações mínimas exigidas e/ou aquelas superiores oferecidas pela CONTRATADA;

24.7. Instalação e configuração do equipamento para atendimento dos serviços ora contratado;

24.8. Teste de eficácia nos serviços/equipamentos contratados, se for o caso.

24.9. O período de inspeção será de até 10 (dez) dias úteis, contados a partir da data de emissão do TERMO DE RECEBIMENTO PROVISÓRIO;

24.10. Findo o prazo de inspeção e comprovada a conformidade dos serviços/equipamentos com as especificações técnicas exigidas no Edital e aquelas oferecidas pela CONTRATADA, o setor responsável emitirá o TERMO DE RECEBIMENTO DEFINITIVO do objeto contratado;

24.11. Nos casos de substituição do equipamento, iniciar-se-ão os prazos e procedimentos estabelecidos nestas CONDIÇÕES DE RECEBIMENTO.

Para o LOTE 03, temos que:

Evento	Descrição	Prazo	Responsável
01	Ordem de Serviço	Entrega em 60 dias corridos	CONTRATANTE
02	Entrega (Emissão do Termo de Recebimento Provisório)	T_0	CONTRATADA
03	Instalação e Configuração (Emissão do Termo de Recebimento Definitivo)	T_0 + 10 dias corridos	CONTRATADA

24.11. Todos os equipamentos deverão ser entregues nas dependências do Tribunal de Justiça do Estado do Acre, nos endereços especificados nste Termo de Referência.

25. DOS PRAZOS E DO TEMPO DE REPARO

25.1. Os seguintes prazos devem ser observados para entrega dos links de internet, MPLS e das soluções de segurança;

25.1.1. Prazo de Instalação:

DIA D: Solicitação formal de instalação de novo link de acesso à internet ou MPLS e instalação de solução de segurança de rede, encaminhada pela CONTRATANTE para a CONTRATADA;

D+60 dias: Conclusão da Instalação;

25.2. Caso a CONTRATADA vencedora seja atualmente fornecedora dos serviços de acesso à internet ou MPLS para a CONTRATANTE e considerando que o novo contrato substituirá os atualmente vigentes, a CONTRATADA poderá utilizar a mesma estrutura e equipamentos do link em uso (modem, roteador, cabeamento, cabos etc.), no entanto, o tempo de parada para substituição do link antigo pelo novo link não poderá ser superior a 04 (quatro) horas durante o expediente.

25.3. Prazo para Desativação:

DIA K: Solicitação formal de desinstalação/desativação do link de acesso à Internet ou MPLS encaminhada pela CONTRATANTE para a CONTRATADA;

K+30: Desinstalação/desativação do link de acesso à internet efetivada;

25.4. Para fins de pagamento/faturamento será considerado desativado o link de acesso à internet ou MPLS na data da solicitação formal (Dia K), data a partir da qual os usuários deixarão de utilizar os serviços.

1. Nível	1. Descrição	1. Tempo de atendimento	1. Tempo de solução
1. 1	1. Problemas que tornem a solução inoperante	1. Até 01 (uma) hora para o primeiro atendimento	1. Até 6 horas para solução de chamados de hardware, exceto onde houver a necessidade de reposição de peças 2. Até 4 horas para solução de contorno de problemas de software.
1. 2	1. Problemas ou dúvidas que prejudiquem a operação do equipamento, mas que não interrompem o acesso aos dados	1. Até 04 (quatro) horas para atendimento	1. Até 12 horas para solução de chamados de hardware, exceto onde houver a necessidade de reposição de peças 2. Até 24 horas para solução de contorno de problemas de software

1. 3	1. Problemas ou dúvidas que criam algumas restrições à operação do equipamento	1. Até 01 (um) dia útil para atendimento	1. Até o próximo dia útil para solução de chamados de hardware, exceto onde houver a necessidade de reposição de peças, 2. Até 7 dias corridos para solução de contorno de problemas de software

26. TEMPO DE REPARO DOS LINKS

26.1. A CONTRATADA deve iniciar os procedimentos de reparo dos links de acesso à internet ou MPLS em até 1 (uma) hora após a identificação da falha, sendo prazo para solução do problema e restabelecimento do serviço de 6 (seis) horas para a Capital Rio Branco e de 12 (doze) horas para as localidades no interior do Estado;

26.2. Cabe à CONTRATADA a identificação proativa de falhas e abertura de chamados para correção;

26.3. Durante o procedimento de manutenção ou indisponibilidade do link deverá ser computado o PNF – Período de Não Funcionamento do Link;

26.4. O PNF será computado em minutos a partir da "abertura do chamado de manutenção" feito pela Central de Atendimento da CONTRATADA;

26.5. O término do PNF será computado a partir do aceite da manutenção (fechamento do chamado) feito pela equipe técnica do CONTRATANTE, sendo necessária a identificação do técnico responsável pelo fechamento do chamado;

26.7. O somatório de PNF em minutos, durante um mês, que exceder o tempo de parada permitido neste mesmo período, será tomado como base de desconto da parcela mensal de pagamento (do concentrador ou conexão dedicada remota que teve seu serviço interrompido) no mês subsequente. A consolidação dos "períodos de não funcionamento do enlace" será feita com base nas informações obtidas no Sistema de Monitoramento do CONTRATANTE;

26.8. Os serviços classificados como: Prioridade Normal, correspondem as implementações, ajustes e configurações que não afetam o funcionamento do serviço;

26.9. Os serviços classificados como: Prioridade Alta, correspondem às manutenções corretivas, ou seja, o funcionamento das soluções de segurança quando estiver inoperante ou quando precisar ser paralisado;

26.10. Se no atendimento ficar constatado que a única solução para normalizar o serviço é no caso de RMA (Troca de Equipamento), o prazo para a troca poderá ser negociado com a CONTRATANTE, não podendo ultrapassar 24 (vinte e quatro) horas, podendo ser prorrogado por igual período mediante justificativa, e aprovada pela CONTRATANTE;

26.11. O regime de atendimento será de 8h x 5 dias de segunda a sexta-feira, no horário do Acre. Poderá haver regime de plantão, fora do horário comercial para manutenções programadas de até 04 horas em dias úteis e/ou de até 06 horas aos sábados, domingos e feriados, que serão informados à CONTRATADA até o segundo dia útil de cada mês pelo TJAC;

26.12. A CONTRATADA deve permitir a “Abertura de Chamado” junto a “Central de Atendimento” da CONTRATADA por meio de um telefone “0800”, ou e-mail, ou WhatsApp, ou sistema próprio de

chamados, desde que seja gerado um número de atendimento ou protocolo de atendimento.

27. TEMPO DE REPARO DAS SOLUÇÕES DE SEGURANÇA

27.1.O atendimento deverá ser realizado na modalidade “24x7”, ou seja, 24 horas por dia, sete dias por semana, incluindo-se feriados. A CONTRATADA deverá entregar suporte técnico em conjunto a fabricante dos equipamentos presentes nesta contratação sob a mesma condição de níveis mínimos de serviço;

27.2. Deverá ser disponibilizada uma Central de Atendimento em português para abertura de chamado de Assistência Técnica disponível na modalidade “24x7”, indicando 0800, canal web para envio de tíquetes e e-mail de suporte;

27.3. Deve ser gerado, para cada chamado aberto, protocolo de início de atendimento;

27.4. A CONTRATANTE poderá, adicionalmente, solicitar que os chamados sejam registrados diretamente com o fabricante dos produtos, bem como seus respectivos atendimentos;

27.5. O atendimento de hardware ocorrerá mediante manutenção corretiva dos equipamentos e deverá cobrir todo e qualquer defeito apresentado, incluindo a substituição de peças, componentes, ajustes, reparos e correções necessárias;

27.6. A substituição de peças e/ou componentes mecânicos ou eletrônicos por outros de marcas e/ou modelos diferentes dos originais cotados pela CONTRATADA somente poderá ser efetuada em caso de descontinuidade do componente originalmente cotado na proposta e ainda mediante análise e autorização do CONTRATANTE;

27.7. Todas as peças e componentes mecânicos ou eletrônicos substituídos deverão apresentar padrões de qualidade e desempenho iguais ou superiores aos utilizados na fabricação do(s) equipamento(s), sendo sempre novos e de primeiro uso.

28. NÍVEIS DE SEVERIDADE

Nível	Descrição	Tempo de atendimento	Tempo de solução
1	Problemas que tornem a solução inoperante	Até 01 (uma) hora para o primeiro atendimento	Até 6 horas para solução de chamados de hardware, exceto onde houver a necessidade de reposição de peças Até 4 horas para solução de contorno de problemas de software
2	Problemas ou dúvidas que prejudiquem a operação do equipamento, mas que não interrompem o acesso aos dados	Até 04 (quatro) horas para atendimento	Até 12 horas para solução de chamados de hardware, exceto onde houver a necessidade de reposição de peças Até 24 horas para solução de contorno de problemas de software

3	Problemas ou dúvidas que criam algumas restrições à operação do equipamento	Até 01 (um) dia útil para atendimento	Até o próximo dia útil para solução de chamados de hardware, exceto onde houver a necessidade de reposição de peças, Até 7 dias corridos para solução de contorno de problemas de software

28.1 Considera-se tempo de atendimento o tempo entre o registro do chamado até o primeiro contato realizado por técnico especialista do produto (nesse momento ainda não há solução para o problema);

28.2. Considera-se tempo de solução o tempo gasto entre o registro do chamado até o momento em que é aplicada uma solução para restabelecer o serviço, eliminar prejuízos ou restrições de operação da solução ou que tenha a dúvida sanada;

28.3. A solução definitiva para chamados de software deverá ser de até 90 dias corridos, em casos que se faça necessária a criação de patches de update ou eventos similares;

28.4. A solução definitiva para a troca do equipamento deverá ser de até 1 dia útil do transporte do equipamento até o Tribunal de Justiça do Estado do Acre, onde ficará a encargo do TJAC transportar o equipamento até a localidade exata.

29. DA QUALIFICAÇÃO TÉCNICA

29.1. Atestado de capacidade técnica, expedido por pessoas jurídicas de direito público ou privado, que comprovem ter o licitante fornecido satisfatoriamente os materiais ou serviços pertinentes e compatíveis com o objeto desta licitação. Podendo ser exigido da proposta melhor classificada, em diligência, que apresente cópia autenticada do contrato da prestação do serviço ou da respectiva nota fiscal, que deram origem ao Atestado;

29.2. A LICITANTE também deverá apresentar a relação explícita ou a declaração formal da sua disponibilidade de equipamentos, ferramental, instalações físicas apropriadas e específicas, bem como pessoal técnico especializado para realização dos serviços que são objeto deste certame;

29.3. A CONTRATADA deverá apresentar declaração que se compromete a realizar toda a instalação de acordo com os termos deste edital;

29.4. A CONTRATADA deverá apresentar declaração que se compromete a disponibilizar equipe de suporte técnico de modo a atender os termos deste edital e de acordo com os níveis de SLA contemplados;

29.5. Deverá apresentar uma declaração expressa que utilizará equipamentos e componentes com certificação de qualidade e aprovado pelos órgãos competentes, sendo-lhe imputada total responsabilidade civil, administrativa e criminal em caso de uso de produtos e bens não atendendo à normatização existente;

29.6. Declaração expressa que as informações transmitidas serão tratadas com total sigilo, não havendo disponibilização a outrem, sob qualquer aspecto ou forma, sob pena de responsabilidade criminal, civil e administrativa;

29.7. Para os Lotes 01 e 02, a LICITANTE deverá, além dos itens de 27.1 a 27.7;

29.8. A LICITANTE deverá comprovar através de atestados, registros ou documentos que possui POPs em operação na Capital Rio Branco, este registro deverá constar a Razão Social e o CNPJ da CONTRATADA;

29.9. Possuir na sua equipe, 01 (um) profissional Engenheiro de Telecomunicações ou equivalente,

devidamente inscrito e regularizado no Conselho Regional de Engenharia, Arquitetura e Agronomia - CREA, cujo vínculo profissional deve ser comprovado da seguinte forma:

29.10. Mediante apresentação de cópia autenticada da CTPS – Carteira de Trabalho e Previdência Social acompanhada de cópia do Registro de Empregados, no caso de empregado da licitante, ou;

29.11. Contrato de prestação de serviço celebrado de acordo com a legislação civil, ou;

29.12. No caso de dirigente ou sócio, do Contrato Social.

29.13. A CONTRATADA deverá apresentar Termo de Autorização expedida pela ANATEL para prestação de Serviço de Comunicação Multimídia (SCM);

29.14. A CONTRATANTE deve comprovar a implantação da solução de Anti DDoS em seu Backbone através de declaração, certificado ou carta do fabricante da solução.

29.15. Para o LOTE 03, a LICITANTE deverá, além dos itens de 27.1 a 27.7;

29.16. Comprovar ser parceira do fabricante FORTINET das soluções de Firewall NGFW, através de carta de Parceria ou outro documento que comprove esta relação;

29.17. Possuir na sua equipe profissionais com as seguintes certificações obrigatórias e indispensáveis em face da complexidade da prestação dos serviços requeridos:

02 (dois) profissionais certificados na solução de segurança que compreende os ITENS 1, 2, 3 e 4 do respectivo lote;

01 (um) profissional certificados na solução de gerenciamento centralizado;

01 (um) profissional certificados na solução de relatoria e análise de logs;

01 (um) profissional com certificação de gerência de projetos nível PMP ou certificação equivalente;

01 (um) profissional com pelo menos umas das certificações listadas: CISSP, OSCE, CEH ou demais certificações na área de segurança da informação ou hacker ético.

29.18. As comprovações de vínculos profissionais deverão ser feitas da seguinte forma:

Mediante apresentação de cópia autenticada da CTPS – Carteira de Trabalho e Previdência Social acompanhada de cópia do Registro de Empregados, no caso de empregado da licitante, ou;

Contrato de prestação de serviço celebrado de acordo com a legislação civil, ou;

No caso de dirigente ou sócio, do Contrato Social.

30. CATÁLOGOS, MANUAIS, FOLDERS E PROSPECTOS

31.1. Será necessária a apresentação de catálogo de cada um dos itens, para a verificação da compatibilidade com as especificações definidas neste Termo de Referência. Não havendo a informação completa no catálogo, poderá ser enviado uma declaração técnica complementar informando as características pendentes no catálogo.

31.2. É obrigatória a comprovação técnica das características exigidas para os equipamentos e softwares por meio da especificação, na proposta, dos part-numbers que compõem cada item;

31.3. Descrição de marca/fabricante, modelo ofertado e versões de softwares empregadas;

31.4. A comprovação dos itens deverá ser feita por meio de documentos que sejam de acesso público cuja origem seja exclusivamente do fabricante dos produtos, a exemplo de: catálogos, manuais, ficha de especificação técnica, ou informações obtidas em sites oficiais do fabricante através da Internet (devidamente referenciados);

31.5. Não será aceita a entrega de cartas/declarações comprobatórias para nenhum item técnico deste edital. Toda documentação apresentada deverá ter cunho público e oficial para corroborar a comprovação técnica;

31.6. Os documentos oficiais poderão ser entregues em língua portuguesa ou inglesa;

31.7. Todos os documentos comprobatórios deverão ter sido publicados pelo fabricante e com data de publicação anterior a do certame licitatório;

31.8. Não serão aceitos documentos emitidos em caráter adhoc, ou seja, apenas com a finalidade de atender às exigências deste instrumento;

31.9. A falta de documentos comprobatórios das exigências deste instrumento poderá implicar a desclassificação da licitante;

31.10. Formulário denominado "Planilha de Comprovação Técnica" para demonstrar o atendimento aos itens e subitens obrigatórios constantes deste Termo de Referência;

31.11. No formulário deverá ser informada a localização exata da informação que garanta o atendimento ao item, explicitando o documento/página;

31.12. Comprovação através de domínio público das fabricantes ofertadas, ou através de carta específica para este processo, indicando que as fabricantes autorizam a licitante a comercializar seu produto, bem como descrevem que ela tem aptidão para executar os serviços solicitados;

31.13. Durante a análise de propostas, os produtos ofertados deverão possuir todas as características técnicas obrigatórias exigidas no Termo de Referência. Não serão aceitos produtos cujas funcionalidades ainda estejam em desenvolvimento ou previstas em releases futuras.

31.14. Caso persistam dúvidas acerca da veracidade do(s) documento(s), poderá(ão) ser efetuado(s) pelo pregoeiro diligência(s) para sanar quaisquer eventuais dúvidas.

32. DA SUBCONTRATAÇÃO

33.1. É vedada a subcontratação total, cessão ou a transferência do objeto deste Edital a terceiros;

33.2. No caso de subcontratação da última milha de terceiros, a CONTRATADA deverá assumir inteira responsabilidade pelo funcionamento e disponibilidade deste recurso, com níveis de serviço compatíveis com o acordo de nível de serviço estabelecido no Termo de Referência;

33.4. Na hipótese de subcontratação, tendo em vista que a subcontratada não celebra avença com a Administração, permanece a responsabilidade integral da CONTRATADA pela perfeita execução contratual, cabendo à CONTRATADA realizar a supervisão e coordenação das atividades da subcontratada, bem como responder perante a CONTRATANTE pelo rigoroso cumprimento das obrigações contratuais correspondentes ao objeto da contratação.

34. DA FORMA E CONDIÇÕES DE PAGAMENTO

34.1. A CONTRATADA entregará a fatura referente ao objeto deste CONTRATO/EMPENHO, acompanhadas das certidões atualizadas conforme relação seguinte:

34.1.1. Certidão Conjunta de Débitos Relativos a Tributos Federais e Dívida Ativa da União, expedida pela Secretaria da Receita Federal do Brasil e Procuradoria Geral da Fazenda Nacional;

34.1.2. Certidão Negativa de Contribuições Previdenciárias, expedida pela Secretaria da Receita Federal do Brasil;

34.1.3. Certificado de Regularidade do Fundo de Garantia por tempo de serviço (FGTS), expedida pela Caixa Econômica Federal;

34.1.4. Certidão Negativa de Débitos (CND) - expedida pela Secretaria Municipal de Finanças;

34.1.5. Certidão de Quitação de Tributos Estaduais da Empresa e do(s) sócio(s), expedida pela Secretaria de Estado da Fazenda;

34.1.6. Certidão Negativa em relação à Dívida Ativa de Tributos Estaduais - expedida pela Procuradoria Geral do Estado - PGE;

34.1.7. Certidão Negativa de Débitos Trabalhistas.

34.1.8. O TJAC, nos termos da Lei nº 9.430, de 27 de dezembro de 1996, e IN SRF nº 1234/2012, fará retenção, na fonte, de Contribuição Social Sobre o Lucro Líquido – CSLL, Contribuição para a Seguridade Social – COFINS, Contribuição para o PIS e Imposto sobre a Renda de Pessoa Jurídica - IRPJ.

35. VIGÊNCIA CONTRATUAL

35.1. O prazo da vigência da Contratação é de 24 meses contados da data de sua assinatura, prorrogável por até 10 anos, na forma dos artigos 106 e 107 da Lei nº 14.133, de 2021.

35.2. No caso de alteração do valor do contrato, ou prorrogação de sua vigência, a garantia deverá ser readequada ou renovada nas mesmas condições.

36. OBRIGAÇÕES DA CONTRATADA

36.1. Fornecer material novo e de boa qualidade para assegurar a prestação dos serviços a serem contratados, em estrita conformidade com as especificações constantes neste Termo de Referência;

36.2. Cumprir as cláusulas contratuais e sempre que solicitado, deverá dirimir quaisquer esclarecimentos julgados necessários;

36.3. A CONTRATADA, no ato do pagamento tem que estar em dia com todas as obrigações legais e apresentar todas as certidões que comprovem tal regularidade;

36.4. Responder por qualquer prejuízo que seus empregados ou prepostos causarem ao Patrimônio do CONTRATANTE ou a terceiros, seja por ação ou omissão culposa ou dolosa, procedendo imediatamente aos reparos ou indenizações cabíveis e assumindo o ônus decorrente;

36.5. Comunicar ao CONTRATANTE toda e qualquer irregularidade ocorrida ou observada no cumprimento das obrigações assumidas;

36.6. Não transferir a outrem, no todo ou em parte, o objeto do presente contrato;

36.7. Responsabilizar-se pela garantia do Objeto, dentro dos padrões adequados de qualidade, segurança, eficiência e desempenho, conforme previsto na legislação em vigor e na forma exigida neste Termo de Referência;

36.8. Entregar o objeto contratado com manutenção em dia;

36.9. Responsabilizar-se única e exclusivamente pelo pagamento de todos os encargos e demais despesas, diretas ou indiretas, decorrente da execução do objeto do presente Termo de Referência, tais como impostos, taxas, contribuições fiscais, previdenciárias, trabalhistas, fundiárias; enfim, por todas as obrigações e responsabilidades, sem nenhum ônus ao CONTRATANTE;

36.10. Garantir a melhor eficiência dos objetos, atendidas as especificações exigidas neste Termo de Referência;

36.11. Não veicular em hipótese alguma, publicidade ou qualquer outra informação acerca das atividades referentes ao fornecimento do Objeto deste Termo de Referência, sem prévia autorização da CONTRATANTE, mantendo total sigilo das informações (escritas, faladas, áudio, vídeo, imagens e produtos);

36.12. Comunicar ao CONTRATANTE qualquer situação que caracterize descumprimento das obrigações

constantes deste Termo de Referência;

36.13. Manter durante a vigência do Contrato as condições de habilitação exigidas para fins de contratação pela Administração Pública, apresentando, sempre que exigido pelo CONTRATANTE, os respectivos comprovantes;

36.14. Indicar preposto, quando for o caso, aceito pelo CONTRATANTE, para representá-la sempre que for necessário;

36.15. Observar, no que couber, as disposições do Código de Defesa do Consumidor (Lei nº 8.078, de 11 de setembro de 1990), o Código Civil Brasileiro, as Normas Técnicas, as Leis e os regulamentos pertinentes;

36.16. O equipamento/serviço deverá ser entregue acompanhado respectivamente de nota fiscal ou instituto equivalente com o nome e a caracterização clara e precisa, contendo também o número da Nota de Empenho firmada com o CONTRATANTE;

36.17. Corrigir, às suas expensas, em no máximo 15 (quinze) dias consecutivos, a contar da recusa de recebimento, devolução, ou comunicação por escrito, os serviços que apresentarem erros e/ou defeitos, bem como incompatibilidade com a proposta.

37. OBRIGAÇÕES DA CONTRATANTE

37.1. Efetuar o pagamento de acordo com o previsto neste Termo de Referência;

37.2. Exercer, a seu critério e através de servidor ou de pessoas previamente designadas, ampla, irrestrita e permanente fiscalização da execução do contrato;

37.3. Prestar todas as informações e esclarecimentos pertinentes ao objeto deste Termo de Referência;

37.4. Não responder por quaisquer compromissos assumidos pela CONTRATADA com terceiros, ainda que vinculados à execução do presente, bem como, por qualquer dano causado a terceiros em decorrência de ato da CONTRATADA e de seus empregados, prepostos ou subordinados.

38. SANÇÕES ADMINISTRATIVAS (PENALIDADES)

38.1. Se a CONTRATADA incidir nas Condutas previstas na Lei Federal nº 14.133, de 1 de abril de 2021 ou no Decreto Estadual n° 5.965/2010, o CONTRATANTE poderá, garantida a prévia defesa, aplicar-lhe, observando a legislação citada e a gravidade das faltas cometidas, as seguintes sanções:

38.1. Advertência por escrito formal ao fornecedor, em decorrência de atos menos graves e que ocasionam prejuízos para a Administração (CONTRATANTE), desde que não caiba a aplicação de sanção mais grave e, se for o caso, conferindo prazo para a adoção de medidas corretivas cabíveis;

38.2. Multa de 2,0% (dois por cento) por dia sobre o valor da nota de empenho em caso de atraso na execução dos serviços, limitada a incidência a 15 (quinze) dias. Após o décimo quinto dia e a critério da Administração, no caso de execução com atraso, poderá ocorrer a não aceitação do objeto, de forma a configurar, nessa hipótese, inexecução total da obrigação assumida, sem prejuízo da rescisão unilateral da avença;

38.3. Multa de 30% (trinta por cento) sobre o valor da nota de empenho, em caso de inexecução total da obrigação assumida;

38.4. Multa de 10% (dez por cento) aplicado sobre o percentual de 20% (vinte por cento) do valor da proposta do licitante, por ilícitos administrativos no decorrer do certame;

38.5. Suspensão temporária de licitar e de contratar com o órgão, entidade ou unidade administrativa pela qual a Administração Pública opera e atua concretamente, pelo prazo não superior a 2 (dois) anos.

38.6. Declaração de inidoneidade para licitar ou contratar com Estado do Acre (Tribunal de Justiça do Estado

do Acre), enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade, que será concedida sempre que a CONTRATADA ressarcir o CONTRATANTE pelos prejuízos causados e depois de decorrido o prazo não superior a 02 (dois) anos.

39. DA GARANTIA CONTRATUAL

39.1. No caso de alteração do valor do contrato, ou prorrogação de sua vigência, a garantia deverá ser readequada ou renovada nas mesmas condições. Se o valor da garantia for utilizado total ou parcialmente em pagamento de qualquer obrigação, a CONTRATADA obriga-se a fazer a respectiva reposição no prazo máximo de 10 (dez) dias úteis, contados da data em que for notificada.

40. DA FUNDAMENTAÇÃO LEGAL

40.1. A contratação prevista neste termo tem amparo legal na Lei nº 14.133, de 1 de abril de 2021; na Lei nº 8.078, de 11 de setembro de 1990; e nos Decretos Estaduais nº 5.965, nº 5.967 e nº 5.972, de 30 de dezembro de 2010.

ANEXO I

ESPECIFICAÇÃO DETALHADA DOS ITENS

CONDIÇÕES GERAIS PARA SOLUÇÕES DE SEGURANÇA

1. REQUISITOS GERAIS

1.1 Não serão aceitas soluções baseadas em PCs de uso geral. Todos os equipamentos a serem fornecidos deverão ser do mesmo fabricante para assegurar a padronização e compatibilidade funcional de todos os recursos;

1.1.2. Os equipamentos devem ser novos, ou seja, de primeiro uso, de um mesmo fabricante. Na data da proposta, nenhum dos modelos ofertados poderão estar listados no site do fabricante em listas de end-of-life ou end-of-sale.

1.1.3. A solução deve consistir em plataforma de proteção de rede baseada em appliance físico com funcionalidades de Next Generation Firewall (NGFW), não sendo permitido appliances virtuais ou solução open source (produto montado especificamente para este certame);

1.1.4. Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões.

1.1.5. A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7;

1.1.6. O gerenciamento da solução deve suportar acesso via SSH, cliente ou web via HTTPS e API;

1.1.7. Os equipamentos de proteção de rede devem possuir suporte a VLANs;

1.1.8. Os equipamentos de proteção de rede devem possuir suporte a roteamento multicast (PIM-SM e PIM- DM);

1.1.9. Deve suportar roteamento estático;

1.1.10. Deve suportar BGP, OSPF e RIP;

1.1.1. Os equipamentos de proteção de rede devem possuir suporte a DHCP Server;

1.1.12. Os equipamentos de proteção de rede devem possuir suporte a DHCP Relay;

1.1.13. Os equipamentos de proteção de rede devem suportar sub-interfaces ethernet lógicas;

1.1.14. Deve suportar NAT dinâmico (Many-to-Many);

1.1.15. Deve suportar NAT estático (1-to-1);

1.1.16. Deve suportar NAT estático bidirecional 1-to-1;

1.1.17. Deve suportar Tradução de porta (PAT);

1.1.18. Deve suportar NAT de Origem;

1.1.19. Deve suportar NAT de Destino;

1.1.20. Deve suportar NAT de Origem e NAT de Destino simultaneamente;

1.1.21. Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico;

1.1.22. Deve suportar NAT64;

1.1.23. Deve permitir monitorar via SNMP o uso de CPU, memória, espaço em disco, VPN, situação do cluster e violações de segurança;

1.1.24. Enviar log para sistemas de monitoração externos;

1.1.25. Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo SSL;

1.1.26. Proteção anti-spoofing;

1.1.27. Deve suportar Modo Camada 3 (Layer 3), para inspeção de dados em linha e visibilidade do tráfego;

1.1.28. Suporte a configuração de alta disponibilidade ativo/passivo e ativo/ativo;

1.1.29. A configuração em alta disponibilidade deve sincronizar: Sessões, Configurações, incluindo, mas não limitado a: Políticas de Firewall, NAT, QOS e objetos de rede, associações de segurança das VPNs e Tabelas FIB;

1.1.30. O modo de alta disponibilidade (HA) deve possibilitar monitoração de falha de link.

1.1.31. Suporte a controle, inspeção e decriptografia de SSL para tráfego de saída (Outbound);

1.1.32. Deve descriptografar tráfego outbound em conexões negociadas com TLS 1.2.

1.1.33. A solução deve suportar integração nativa com Let’s Encrypt, para obtenção de certificados válidos, de forma automática.

1.2. POLÍTICAS

1.2.1. Deverá suportar controles por zonas de segurança;

1.2.2. Deverá suportar controles de políticas por porta e protocolo;

1.2.3. Deverá suportar controles de políticas por aplicações, grupos estáticos de aplicações e grupos dinâmicos de aplicações;

1.2.4. Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança;

1.2.5. Controle de políticas por código de País (Por exemplo: BR, US, UK, RU);

1.2.6. Deve permitir o bloqueio de arquivo por sua extensão e possibilitar a correta identificação do arquivo por seu tipo mesmo quando sua extensão for renomeada;

1.2.7. Suporte a objetos e regras IPV6;

1.2.8. Suporte a objetos e regras multicast;

1.2.9. Suportar a atribuição de agendamento das políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente.

1.3. CONTROLE DE APLICAÇÕES

1.3.1. Os equipamentos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo;

1.3.2. Deve ser possível a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos;

1.3.3. Reconhecer pelo menos 1700 aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;

1.3.4. Reconhecer pelo menos as seguintes aplicações: bittorrent, gnutella, skype, facebook, linkedin, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, onedrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google- docs;

1.3.5. Deve inspecionar o payload do pacote de dados com o objetivo de detectar assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo;

1.3.6. Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas;

1.3.7. Para tráfego criptografado SSL, deve descriptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;

1.3.8. Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo. A decodificação de protocolo também deve identificar funcionalidades específicas dentro de uma aplicação;

1.3.9. Identificar o uso de táticas evasivas via comunicações criptografadas;

1.3.10. Atualizar a base de assinaturas de aplicações automaticamente;

1.3.11. Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no Domain Controller, nem nas estações dos usuários;

1.3.12. Deve ser possível adicionar controle de aplicações em múltiplas regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras;

1.3.13. Deve suportar vários métodos de identificação e classificação das aplicações, por pelo menos: checagem de assinaturas e decodificação de protocolos;

1.3.14. Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante;

1.3.15. O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;

1.3.16. Deve alertar o usuário quando uma aplicação for bloqueada;

1.3.17. Deve possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, emule, etc) possuindo granularidade de controle/políticas para os mesmos;

1.3.18. Deve possibilitar a diferenciação de tráfegos de Instant Messaging (AIM, Hangouts, Facebook Chat, etc) possuindo granularidade de controle/políticas para os mesmos;

1.3.19. Deve possibilitar a diferenciação e controle de partes das aplicações como, por exemplo, permitir o Hangouts e bloquear a chamada de vídeo;

1.3.20. Deve possibilitar a diferenciação de aplicações Proxies, possuindo granularidade de controle/políticas para os mesmos;

1.3.21. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: tecnologia utilizada nas aplicações (Client-Server, Browser Based, Network Protocol, etc);

1.3.22. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: nível de risco da aplicação e categoria da aplicação;

1.3.23. Deve ser possível a criação de grupos estáticos de aplicações baseados em características das aplicações como: Categoria da aplicação.

1.4. PREVENÇÃO DE AMEAÇAS

1.4.1. Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware) integrados no próprio appliance;

1.4.2. Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade;

1.4.3. Deve implementar os seguintes tipos de ações para ameaças detectadas pelo IPS: permitir, permitir e gerar log, bloquear e quarentenar o IP do atacante por um intervalo de tempo;

1.4.4. As assinaturas devem poder ser ativadas ou desativadas, ou ainda habilitadas apenas em modo de monitoração;

1.4.5. Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança;

1.4.6. A criação de exceções por IP de origem ou de destino devem ser possíveis nas regras ou assinatura a assinatura;

1.4.7. Deve suportar granularidade nas políticas de IPS, Antivírus e Anti-Spyware, possibilitando a criação de diferentes políticas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;

1.4.8. Deve permitir o bloqueio de vulnerabilidades;

1.4.9. Deve permitir o bloqueio de exploits conhecidos;

1.4.10. Deve incluir proteção contra ataques de negação de serviços;

1.4.11. Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS.

1.4.12. Ser imune e capaz de impedir ataques básicos como: Syn flood, ICMP flood, UDP flood, etc;

1.4.13. Detectar e bloquear a origem de portscans;

1.4.14. Bloquear ataques efetuados por worms conhecidos;

1.4.15. Possuir assinaturas para bloqueio de ataques de buffer overflow;

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

1.4.17. Deve permitir usar operadores de negação na criação de assinaturas customizadas de IPS ou anti spyware, permitindo a criação de exceções com granularidade nas configurações;

1.4.18. Permitir o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;

1.4.19. Identificar e bloquear comunicação com botnets;

1.4.20. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas: o nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;

1.4.21. Deve possuir a função de proteção a resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos de botnets conhecidas;

1.4.22. Os eventos devem identificar o país de onde partiu a ameaça;

1.4.23. Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms;

1.4.24. Possuir proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos;

1.4.25. Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas do firewall considerando usuários, grupos de usuários, origem, destino, zonas de segurança;

1.4.26. Deve ser capaz de mitigar ameaças avançadas persistentes (APT), através de análises dinâmicas para identificação de malwares desconhecidos;

1.4.27. A solução de sandbox deve ser capaz de criar assinaturas e ainda incluí-las na base de antivírus do firewall, prevenindo a reincidência do ataque;

1.4.28. A solução de sandbox deve ser capaz de incluir no firewall as URLs identificadas como origens de tais ameaças desconhecidas (blacklist), impedindo que esses endereços sejam acessados pelos usuários de rede novamente;

1.4.29. Dentre as análises efetuadas, a solução deve suportar antivírus, query na nuvem, emulação de código, sandboxing e verificação de callback;

4.30. A solução deve analisar o comportamento de arquivos suspeitos em um ambiente controlado.

1.5. FILTRO DE URLs

1.5.1. Permitir especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);

1.5.2. Deve ser possível a criação de políticas por grupos de usuários, IPs, redes ou zonas de segurança;

1.5.3. Deve possuir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com Active Directory e base de dados local;

1.5.4. A identificação pela base do Active Directory deve permitir Single Sign On (SSO), de forma que os usuários não precisem logar novamente na rede para navegar pelo firewall;

1.5.5. Suportar a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;

1.5.6. Suportar proxy explícito;

1.5.7. Suportar a criação de limites diários de tempo e banda consumida por categoria;

1.5.8. Possuir pelo menos 60 categorias de URLs;

1.5.9. Deve possuir a função de exclusão de URLs do bloqueio;

1.5.10. Permitir a customização de página de bloqueio;

1.5.11. Permitir a restrição de acesso a canais específicos do Youtube, possibilitando configurar uma lista de canais liberado ou uma lista de canais bloqueados;

1.5.12. Deve bloquear o acesso a conteúdo indevido ao utilizar a busca em sites como Google, Bing e Yahoo, independentemente de a opção Safe Search estar habilitada no navegador do usuário;

5.13. Os requisitos de filtro de URL descritos acima aplicam-se apenas ao firewall.

1.6. IDENTIFICAÇÃO DOS USUÁRIOS

1.6.1. Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com LDAP, Active Directory, E-directory e base de dados local;

1.6.2. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;

1.6.3. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, suportando Single Sign On (SSO). Essa funcionalidade não deve possuir limites licenciados de usuários;

1.6.4. Deve possuir integração com RADIUS para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;

1.6.5. Deve possuir integração com LDAP para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em Usuários e grupos de usuários;

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

1.6.7. Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços;

1.6.8. Deve implementar a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP/AD.

1.7. FILTRO DE DADOS

1.7.1. Permitir identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, etc) identificados sobre aplicações;

1.7.2. Suportar identificação de arquivos compactados ou a aplicação de políticas sobre o conteúdo desses tipos de arquivos;

1.7.3. Suportar a identificação de arquivos criptografados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos;

1.7.4. Permitir identificar e opcionalmente prevenir a transferência de informações sensíveis, incluindo, mas

não limitado a número de cartão de crédito, possibilitando a criação de novos tipos de dados via expressão regular.

1.8. GEOLOCALIZAÇÃO

1.8.1. Suportar a criação de políticas por geolocalização, permitindo o bloqueio do tráfego de determinado País/Países;

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

1.9. RECURSOS DE SD-WAN

1.9.1. A solução deve prover recursos de roteamento inteligente, definindo, mediante regras pré- estabelecidas, o melhor caminho a ser tomado para uma aplicação;

1.9.2. Deve ser possível criar políticas que definam os seguintes critérios para match:

1.9.2.1. Endereços de origem;

1.9.2.2. Grupos de usuários;

1.9.2.3. Endereços de destino;

1.9.2.4. DSCP;

1.9.3. Aplicação de camada 7 utilizada (O365 Exchange, AWS, Dropbox e etc).

1.9.4. A solução deverá ser capaz de monitorar e identificar falhas mediante a associação de health check, permitindo testes de resposta por ping, http, tcp/udp echo, dns, tcp-connect e twamp;

1.9.5. O SD-WAN deverá balancear o tráfego das aplicações entre múltiplos links simultaneamente, inclusive 4G;

1.9.6. O SD-WAN deverá analisar o tráfego em tempo real e realizar o balanceamento dos pacotes de um mesmo fluxo (sessão) entre múltiplos links simultaneamente;

1.9.7. Deverá ser permitida a criação de políticas de roteamento com base nos seguintes critérios: latência, jitter, perda de pacote, banda ocupada ou todos ao mesmo tempo;

1.9.8. A solução de SD-WAN deve possibilitar o uso de túneis VPN dinâmicos, entre localidades remotas, para aplicações sensíveis. Uma vez que seja realizada a troca das informações entre as localidades, é feito o bypass do hub;

1.9.9. Deve permitir a duplicação de pacotes entre dois ou mais links, de forma seletiva, objetivando uma melhor experiência de uso de aplicações de negócio;

1.9.10. A solução deve permitir a definição do roteamento para cada aplicação;

1.9.11. Diversas formas de escolha do link devem estar presentes, incluindo: melhor link, menor custo e definição de níveis máximos de qualidade a serem aceitos para que tais links possam ser utilizados em um determinado roteamento de aplicação;

1.9.12. Deve possibilitar a definição do link de saída para uma aplicação específica;

1.9.13. Deve implementar balanceamento de link por hash do IP de origem;

1.9.14. Deve implementar balanceamento de link por hash do IP de origem e destino;

1.9.15. Deve-se implementar balanceamento de link por peso. Nesta opção deve ser possível definir o

percentual de tráfego que será encaminhado por cada um dos links. Deve suportar o balanceamento de, no mínimo, três links;

1.9.16. Deve implementar balanceamento de links sem a necessidade de criação de zonas ou uso de instâncias virtuais;

1.9.17. A solução de SD-WAN deve possuir suporte a policy based routing ou policy based forwarding;

1.9.18. Para IPv4, deve suportar roteamento estático e dinâmico (BGP e OSPF);

1.9.19. Deve possuir recurso para correção de erro (FEC), possibilitando a redução das perdas de pacotes nas transmissões;

1.9.20. Deve permitir a customização dos timers para detecção de queda de link, bem como tempo necessário para retornar com o link para o balanceamento após restabelecido;

1.9.21. A solução de SD-WAN deve suportar nativamente conectores com pelo menos as seguintes clouds públicas: Azure, AWS e GCP;

1.9.22. Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo, (como youtube, facebook, etc), impactando no bom uso das aplicações de negócio, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, tenha capacidade de controlá-las por políticas de shaping. Dentre as tratativas possíveis, a solução deve contemplar:

1.9.23. Suportar a criação de políticas de QoS e Traffic Shaping por endereço de origem, endereço de destino, usuário e grupo de usuários, aplicações e porta;

1.9.24. O QoS deve possibilitar a definição de tráfego com banda garantida;

1.9.25. O QoS deve possibilitar a definição de tráfego com banda máxima;

1.9.26. Além de possibilitar a definição de banda máxima e garantida por aplicação, deve também suportar o match em categorias de URL, IPs de origem e destino, logins e portas.

1.9.27. Deve ainda possibilitar a marcação de DSCP, a fim de que essa informação possa ser utilizada ao longo do backbone para fins de reserva de banda;

1.9.28. O QoS deve possibilitar a definição de fila de prioridade;

1.9.29. Permitir agendar intervalos de tempo para habilitar as políticas de QoS/Traffic Shaping;

1.9.30. Deve possibilitar a definição de bandas distintas para download e upload;

1.9.31. A solução de SD-WAN deve prover estatísticas em tempo real a respeito da ocupação de banda (upload e download) e performance do health check (packet loss, jitter e latência);

1.9.32. A solução de SD-WAN deve suportar IPv6;

1.9.33. Deve possibilitar roteamento distinto a depender do grupo de usuário selecionado na regra de SD-WAN;

1.9.34. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo;

1.9.35. O SD-WAN deverá possuir serviço de Firewall Stateful;

1.9.36. A solução SD-WAN deverá fornecer criptografia AES de 128 bits ou AES de 256 bits em sua VPN;

1.9.37. A solução SD-WAN deverá simplificar a implantação de túneis criptografados de site para site;

1.9.38. Deve ser capaz de bloquear acesso às aplicações;

1.9.39. Deve suportar NAT dinâmico bem como NAT de saída;

1.9.40. Deve suportar balanceamento de tráfego por sessão e pacote;

1.9.41. Suportar VPN IPSec Site-to-Site;

1.9.42. A VPN IPSEC deve suportar criptografia 3DES, AES128, AES192 e AES256 (Advanced Encryption Standard);

1.9.43. A VPN IPSEc deve suportar Autenticação MD5, SHA1, SHA256, SHA384 e SHA512;

1.9.44. A VPN IPSEc deve suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14, Group 15 até 21 e Group 27 até 32;

1.9.45. A VPN IPSEc deve suportar Algoritmo Internet Key Exchange (IKEv1 e v2);

1.9.46. A VPN IPSEc deve suportar Autenticação via certificado IKE PKI;

1.9.47. Deve suportar o uso de DDNS, para casos onde uma ou ambas as pontas possuam IPs dinâmicos;

1.9.48. Deve suportar VPN dial up, no caso da ponta remota não possui IP estático na WAN;

1.9.49. Deve possuir suporte e estar licenciamento para uso de VRFs.

1.10. CARACTERÍSTICAS GERAIS DO SUPORTE TÉCNICO

1.10.1. A implantação, configuração, gerenciamento, manutenção, suporte e monitoramento dos serviços ofertados deverão ser realizados pela CONTRATADA;

1.10.2. É de responsabilidade da CONTRATADA todas as despesas com materiais, mão-de-obra, transportes, hospedagem, equipamentos, máquinas, impostos, seguros, taxas, tributos, incidências fiscais, trabalhistas, previdenciárias, salários, custos diretos e indiretos, encargos sociais e contribuições de qualquer natureza ou espécie, necessários à perfeita execução do objeto;

1.10.3. Em situações que forem identificadas como origem do incidente falhas nos links de comunicação e estes serem causados por contratos da CONTRATANTE com outras empresas, a CONTRATANTE deverá realizar o acionamento e acompanhamento do suporte técnico da referida empresa fornecedora do link afetado, para que esta realize a normalização dos seus serviços;

1.10.4. É de responsabilidade da CONTRATADA o fornecimento dos serviços de suporte técnico especializado de segundo e terceiro nível para o ambiente contratado, inclusive de forma presencial quando este for necessário para o atendimento dos chamados e/ou normalização do ambiente;

1.10.5. Todos os chamados, sejam abertos pela CONTRATANTE ou pela CONTRATADA de forma proativa e/ou reativa, deverão ser registrados em ferramenta para este fim, a qual deverá possibilitar a extração das informações de acordo com os relatórios exigidos mensalmente;

1.10.6. Os chamados abertos pelo CONTRATANTE serão referentes às atividades sob responsabilidade da CONTRATADA, englobando: instalação, configuração, recuperação, alteração e remoção de equipamentos, configurações nas soluções, endereçamento IP, SNMP, organização e atualização da gerência e todos os serviços contratados de maneira a assegurar a integridade, a qualidade e desempenho dos serviços dentro dos limites estabelecidos;

1.10.7. A CONTRATADA deverá manter atualizados no seu sistema de chamados as informações e status de andamento no atendimento dos incidentes/requisições;

1.10.8. Eventuais paradas nas soluções contratadas, em qualquer nível, ou qualquer outra parada de

responsabilidade da CONTRATADA, deverá ser comunicada tempestivamente a CONTRATANTE através de e-mail ou telefone(s) que possam garantir contato imediato a ser(em) informados pela CONTRATANTE;

1.10.9. Todas as interrupções programadas deverão ser comunicadas ao CONTRATANTE com antecedência mínima de 5 (cinco) dias úteis, e deverão ser realizadas preferencialmente aos domingos e feriados, ou em data e horário pré-definidos pelo CONTRATANTE, de acordo com o fuso horário da localidade onde ocorrerá a interrupção. As paradas programadas deverão ser autorizadas pelo CONTRATANTE antes de sua execução;

1.10.10. O CONTRATANTE poderá solicitar, a qualquer tempo, os dados e demais informações armazenadas pela CONTRATADA, relativos ao projeto do CONTRATANTE;

1.10.11. Os dados e informações armazenados poderão ser solicitados pelo CONTRATANTE, a qualquer tempo à CONTRATADA que deverá disponibilizá-los no prazo máximo de 5 (cinco) dias úteis, em meio a ser definido pela CONTRATANTE.

2. LOTE 03 – ITEM 01 – SERVIÇO DE FIREWALL CORPORATIVO TIPO 01

2.1. COMPONENTES DE HARDWARE

2.1.1. Cada unidade de CLUSTER deverá ser composta por 2 (dois) equipamentos;

2.1.2. O equipamento de referência adotado nesta especificação se baseia no modelo Fortigate 901G;

2.1.3. Throughput de, no mínimo, 22 Gbps com a funcionalidade de NGFW. Ou seja, com funcionalidades de Firewall, IPS e Controle de Aplicação habilitadas simultaneamente;

2.1.4. Throughput de, no mínimo, 74 Gbps para Controle de Aplicação;

2.1.5. Throughput de, no mínimo, 164 Gbps para Firewall, considerando pacotes UDP de 1518 bytes;

2.1.6. Suporte a, pelo menos, 16 milhões de sessões concorrentes TCP;

2.1.7. Suporte a, pelo menos, 720 mil novas sessões TCP por segundo;

2.1.8. Suportar no mínimo 16 Gbps de throughput de Inspeção SSL;

2.1.9. Throughput de, no mínimo, 26 Gbps de IPS;

2.1.10. Throughput de, no mínimo, 55 Gbps de VPN IPSec;

2.1.11. Throughput de, no mínimo, 10 Gbps de VPN SSL;

2.1.12. Suportar pelo menos 2.000 túneis IPSec Site-to-Site;

2.1.13. Suportar pelo menos 50.000 túneis IPSec Site-to-Client;

2.1.14. Possuir ao menos 16 interfaces RJ45 Gigabit Ethernet, 8 interfaces SFP Gigabit Ethernet, 4 interfaces SFP+ Gigabit Ethernet, 4 interfaces SFP28 Gigabit Ethernet de Baixa Latência, 1 interface RJ45 para gerenciamento e 1 interface RJ45 para alta disponibilidade (HA);

2.1.15. Cada equipamento deverá ser entregue com 4 Transceivers 25GBASE-SR e 4 Transceivers 10GBASE-SR;

2.1.16. Suportar a criação de, no mínimo, 10 instâncias virtuais;

2.1.17. Armazenamento interno de, no mínimo, 2 discos SSD de 480 GB;

2.1.18. Deve ser fornecido com fontes redundantes do tipo hot swap;

2.1.19. Deve suportar a instalação em rack padrão 19” ou ser entregue com bandeja para a instalação em rack;

2.1.20. Deve estar homologado na ANATEL até a data da licitação.

2.2. MONITORAMENTO ATRAVÉS DE CENTRO DE OPERAÇÃO DE SEGURANÇA

2.2.1. A CONTRATADA deverá realizar o monitoramento de toda a solução ofertada no LOTE 3, atuando de forma proativa e reativa a eventos que possam causar impactos ou indisponibilidade na prestação dos serviços contratados;

2.2.2. A CONTRATADA deverá fornecer a partir dos logs coletados dos dispositivos a correlação de eventos e detecção em tempo real de ameaças persistentes avançadas (APTs), vulnerabilidades e indicadores de comprometimento (IOC) para as soluções de segurança e prover visibilidade profunda e insights críticos da rede;

2.2.3. A CONTRATADA deverá fornecer notificações, relatórios e painéis em tempo real para visibilidade das soluções de segurança ofertadas;

2.2.4. A CONTRATADA deverá ter capacidade para detectar malwares, incluindo um relatório informativo com o resumo de como o malware funciona;

2.2.5. A CONTRATADA deverá ter capacidade para identificar uso suspeito e artefatos maliciosos observados na rede ou em um sistema operacional, determinados por meio de indicadores de comprometimento (IOC) como sendo infecções maliciosas ou intrusões;

2.2.6. A CONTRATADA deverá possuir automação para resposta a incidentes com fluxos de trabalho integrados de gerenciamento de incidentes e conectores nas soluções de segurança.

2.3. SUPORTE ESPECIALIZADO NA SOLUÇÃO DE SEGURANÇA

2.3.1. É de responsabilidade da CONTRATADA o fornecimento dos serviços de suporte técnico especializado de segundo e terceiro nível para o ambiente contratado, inclusive de forma presencial quando este for necessário para o atendimento dos chamados e/ou normalização do ambiente;

2.3.2. Por suporte técnico de segundo nível, mas não se limitando as seguintes ações a serem executadas pela CONTRATADA quando demandada pela CONTRATANTE:

2.3.3. Auxiliar na configuração de políticas de firewall;

2.3.4. Análise de problemas relacionados a SSL VPN;

2.3.5. Análise de problemas relacionados a VPN Site-to-Site;

2.3.6. Análise de problemas relacionados a bloqueios indevidos;

2.3.7. Ajustes de configurações iniciais (NTP Server, Hostname, Timezone);

2.3.8. Auxílio na criação de objetos no firewall;

2.3.9. Auxílio na reserva de IPv4 com base em DHCP/MAC Address;

2.3.10. Criação e/ou Alteração de perfis de segurança (AV, WEB, APP, DNS, IPS);

2.3.11. Criação e/ou Alteração de configuração de túneis VPN Site-to-Site, Dial-up e SSLVPN;

2.3.12. Criação e/ou Alteração de interfaces de rede;

2.3.13. Criação e/ou Alteração em políticas de roteamento;

2.3.14. Criação e/ou Alteração de configuração em integração com servidores LDAP e/ou RADIUS.

2.3.15. Por suporte técnico de terceiro nível, mas não se limitando as seguintes ações a serem executadas pela CONTRATADA quando demandada pela CONTRATANTE:

2.3.16. Análise de disponibilidade;

2.3.17. Criação e configuração de VPN Site-to-Site em VXLAN;

2.3.18. Auxílio na reserva de IPv6 com base em DHCP/MAC Address;

2.3.19. Tratativas relacionadas a IPv6;

2.3.20. Problemas relativos a Certificado Digital;

2.3.21. Análise e resolução de problemas de comunicação com servidores LDAP;

2.3.22. Análise e resolução de problemas via CLI (VPN, SSO, RADIUS, dentre outros);

2.3.23. Configuração de VPN SSL com certificado próprio;

2.3.24. Auxílio na confecção de políticas com inspeção de pacotes;

2.3.25. Integrações com demais soluções de segurança presentes nesta contratação;

2.3.26. Configuração de alta disponibilidade;

2.3.27. Configuração do Single Sign On (SSO);

2.3.28. Restauração da solução a partir de backup;

2.3.29. Configuração de inspeção profunda de pacotes e SSL nas políticas de firewall;

2.3.30. Tratamento de incidentes junto ao fabricante da solução;

2.3.31. Tratamento de RMA junto ao fabricante da solução.

2.3.32. Demais solicitações da CONTRATANTE que se fizerem necessárias nas soluções contratadas devem ser previamente acordadas com a CONTRATADA.

3. LOTE 03 – ITEM 02 – SERVIÇO DE FIREWALL CORPORATIVO

TIPO 02 3.1.COMPONENTES DE HARDWARE

3.1.1. O equipamento de referência adotado nesta especificação se baseia no modelo Fortigate 201F;

3.1.2. Throughput de, no mínimo, 3,5 Gbps com a funcionalidade de NGFW. Ou seja, com funcionalidades de Firewall, IPS e Controle de Aplicação habilitadas simultaneamente;

3.1.3. Throughput de, no mínimo, 13 Gbps para Controle de Aplicação;

3.1.4. Throughput de, no mínimo, 27 Gbps para Firewall, considerando pacotes UDP de 1518 bytes;

3.1.5. Suporte a, pelo menos, 3 Milhões de sessões concorrentes TCP;

3.1.6. Suporte a, pelo menos, 280 mil novas sessões TCP por segundo;

3.1.7. Suportar no mínimo 4 Gbps de throughput de Inspeção SSL;

3.1.8. Throughput de, no mínimo, 5 Gbps de IPS;

3.1.9. Throughput de, no mínimo, 13 Gbps de VPN IPSec;

3.1.10. Throughput de, no mínimo, 2 Gbps de VPN SSL;

3.1.11. Possuir ao menos 16 interfaces RJ45 Gigabit Ethernet, 8 interfaces SFP Gigabit Ethernet, 4 interfaces SFP+ Gigabit Ethernet, 1 interface RJ45 para gerenciamento e 1 interface RJ45 para alta disponibilidade (HA);

3.1.12. Armazenamento interno de, no mínimo, 1 disco SSD de 480 GB;

3.1.13. Possuir fontes redundantes;

3.1.14. Deve suportar a instalação em rack padrão 19” ou ser entregue com bandeja para a instalação em rack;

3.1.15. Deve estar homologado na ANATEL até a data da licitação.

.3.2. MONITORAMENTO ATRAVÉS DE CENTRO DE OPERAÇÃO DE SEGURANÇA

3.2.1. A CONTRATADA deverá realizar o monitoramento de toda a solução ofertada no LOTE 3, atuando de forma proativa e reativa a eventos que possam causar impactos ou indisponibilidade na prestação dos serviços contratados;

3.2.3. A CONTRATADA deverá fornecer a partir dos logs coletados dos dispositivos a correlação de eventos e detecção em tempo real de ameaças persistentes avançadas (APTs), vulnerabilidades e indicadores de comprometimento (IOC) para as soluções de segurança e prover visibilidade profunda e insights críticos da rede;

3.2.4. . A CONTRATADA deverá fornecer notificações, relatórios e painéis em tempo real para visibilidade das soluções de segurança ofertadas;

3.2.5. A CONTRATADA deverá ter capacidade para detectar malwares, incluindo um relatório informativo com o resumo de como o malware funciona;

3.2.6. A CONTRATADA deverá ter capacidade para identificar uso suspeito e artefatos maliciosos observados na rede ou em um sistema operacional, determinados por meio de indicadores de comprometimento (IOC) como sendo infecções maliciosas ou intrusões;

3.2.7. A CONTRATADA deverá possuir automação para resposta a incidentes com fluxos de trabalho integrados de gerenciamento de incidentes e conectores nas soluções de segurança.

3.3. SUPORTE ESPECIALIZADO NA SOLUÇÃO DE SEGURANÇA

3.3.1. É de responsabilidade da CONTRATADA o fornecimento dos serviços de suporte técnico especializado de segundo e terceiro nível para o ambiente contratado, inclusive de forma presencial quando este for necessário para o atendimento dos chamados e/ou normalização do ambiente;

3.3.2. Por suporte técnico de segundo nível, mas não se limitando as seguintes ações a serem executadas pela CONTRATADA quando demandada pela CONTRATANTE:

3.3.2.1. Auxiliar na configuração de políticas de firewall;

3.3.2.2. Análise de problemas relacionados a SSL VPN;

3.3.2.3. Análise de problemas relacionados a VPN Site-to-Site;

3.3.2.4. Análise de problemas relacionados a bloqueios indevidos;

3.3.2.5. Ajustes de configurações iniciais (NTP Server, Hostname, Timezone);

3.3.2.6. Auxílio na criação de objetos no firewall;

3.3.2.7. Auxílio na reserva de IPv4 com base em DHCP/MAC Address;

3.3.2.8. Criação e/ou Alteração de perfis de segurança (AV, WEB, APP, DNS, IPS);

3.3.2.9. Criação e/ou Alteração de configuração de túneis VPN Site-to-Site, Dial-up e SSLVPN;

3.3.2.10. Criação e/ou Alteração de interfaces de rede;

3.3.2.11. Criação e/ou Alteração em políticas de roteamento;

3.3.2.12. Criação e/ou Alteração de configuração em integração com servidores LDAP e/ou RADIUS.

3.3.3. Por suporte técnico de terceiro nível, mas não se limitando as seguintes ações a serem executadas pela CONTRATADA quando demandada pela CONTRATANTE:

3.3.3.1. Análise de disponibilidade;

3.3.3.2. Criação e configuração de VPN Site-to-Site em VXLAN;

3.3.3.3. Auxílio na reserva de IPv6 com base em DHCP/MAC Address;

3.3.3.4. Tratativas relacionadas a IPv6;

3.3.3.5. Problemas relativos a Certificado Digital;

3.3.3.6. Análise e resolução de problemas de comunicação com servidores LDAP;

3.3.3.7. Análise e resolução de problemas via CLI (VPN, SSO, RADIUS, dentre outros);

3.3.3.8. Configuração de VPN SSL com certificado próprio;

3.3.3.9. Auxílio na confecção de políticas com inspeção de pacotes;

3.3.3.10. Integrações com demais soluções de segurança presentes nesta contratação;

3.3.3.11. Configuração de alta disponibilidade;

3.3.3.12. Configuração do Single Sign On (SSO);

3.3.3.13. Restauração da solução a partir de backup;

3.3.3.14. Configuração de inspeção profunda de pacotes e SSL nas políticas de firewall;

3.3.3.15. Tratamento de incidentes junto ao fabricante da solução;

3.3.3.16. Tratamento de RMA junto ao fabricante da solução.

3.3.4. Demais solicitações da CONTRATANTE que se fizerem necessárias nas soluções contratadas devem ser previamente acordadas com a CONTRATADA.

4. LOTE 03 – ITEM 03 – SERVIÇO DE FIREWALL CORPORATIVO TIPO 03

4.1. COMPONENTES DE HARDWARE

4.1.1. O equipamento de referência adotado nesta especificação se baseia no modelo Fortigate 101F;

4.1.2. Throughput de, no mínimo, 1.6 Gbps com a funcionalidade de NGFW. Ou seja, com funcionalidades de Firewall, IPS e Controle de Aplicação habilitadas simultaneamente;

4.1.3. Throughput de, no mínimo, 2,2 Gbps para Controle de Aplicação;

4.1.4. Throughput de, no mínimo, 20 Gbps para Firewall, considerando pacotes UDP de 1518 bytes;

4.1.5. Suporte a, pelo menos, 1,5 milhões sessões concorrentes TCP;

4.1.6. Suporte a, pelo menos, 56 mil novas sessões TCP por segundo;

4.1.7. Suportar no mínimo 1 Gbps de throughput de Inspeção SSL;

4.1.8. Throughput de, no mínimo, 2,6 Gbps de IPS;

4.1.9. Throughput de, no mínimo, 11,5 Gbps de VPN IPSec;

4.1.10. Throughput de, no mínimo, 1 Gbps de VPN SSL;

4.1.11. Possuir ao menos 12 interfaces RJ45 Gigabit Ethernet, 4 interfaces SFP Gigabit Ethernet, 2 interfaces SFP+ Gigabit Ethernet, 1 interface RJ45 para gerenciamento e 1 interface RJ45 para alta disponibilidade (HA);

4.1.12. Armazenamento interno de, no mínimo, 1 disco SSD de 480 GB;

4.1.13. Possuir fontes redundantes;

4.1.14. Deve suportar a instalação em rack padrão 19” ou ser entregue com bandeja para a instalação em rack;

4.1.15. Deve estar homologado na ANATEL até a data da licitação.

4.2. MONITORAMENTO ATRAVÉS DE CENTRO DE OPERAÇÃO DE SEGURANÇA

4.2.1. A CONTRATADA deverá realizar o monitoramento de toda a solução ofertada no LOTE 3, atuando de forma proativa e reativa a eventos que possam causar impactos ou indisponibilidade na prestação dos serviços contratados;

4.2.2. A CONTRATADA deverá fornecer a partir dos logs coletados dos dispositivos a correlação de eventos e detecção em tempo real de ameaças persistentes avançadas (APTs), vulnerabilidades e indicadores de comprometimento (IOC) para as soluções de segurança e prover visibilidade profunda e insights críticos da rede;

4.2.3. A CONTRATADA deverá fornecer notificações, relatórios e painéis em tempo real para visibilidade das soluções de segurança ofertadas;

4.2.4. A CONTRATADA deverá ter capacidade para detectar malwares, incluindo um relatório informativo com o resumo de como o malware funciona;

4.2.5. A CONTRATADA deverá ter capacidade para identificar uso suspeito e artefatos maliciosos observados na rede ou em um sistema operacional, determinados por meio de indicadores de comprometimento (IOC) como sendo infecções maliciosas ou intrusões;

4.2.6. A CONTRATADA deverá possuir automação para resposta a incidentes com fluxos de trabalho integrados de gerenciamento de incidentes e conectores nas soluções de segurança.

4.3. SUPORTE ESPECIALIZADO NA SOLUÇÃO DE SEGURANÇA

4.3.1. É de responsabilidade da CONTRATADA o fornecimento dos serviços de suporte técnico especializado de segundo e terceiro nível para o ambiente contratado, inclusive de forma presencial quando este for necessário para o atendimento dos chamados e/ou normalização do ambiente;

4.3.2. Por suporte técnico de segundo nível, mas não se limitando as seguintes ações a serem executadas pela CONTRATADA quando demandada pela CONTRATANTE:

4.3.2.1. Auxiliar na configuração de políticas de firewall;

4.3.2.2. Análise de problemas relacionados a SSL VPN;

4.3.2.3. Análise de problemas relacionados a VPN Site-to-Site;

4.3.2.4. Análise de problemas relacionados a bloqueios indevidos;

4.3.2.5. Ajustes de configurações iniciais (NTP Server, Hostname, Timezone);

4.3.2.6. Auxílio na criação de objetos no firewall;

4.3.2.7. Auxílio na reserva de IPv4 com base em DHCP/MAC Address;

4.3.2.8. Criação e/ou Alteração de perfis de segurança (AV, WEB, APP, DNS, IPS);

4.3.2.9. Criação e/ou Alteração de configuração de túneis VPN Site-to-Site, Dial-up e SSLVPN;

4.3.2.10. Criação e/ou Alteração de interfaces de rede;

4.3.2.11. Criação e/ou Alteração em políticas de roteamento;

4.3.2.12. Criação e/ou Alteração de configuração em integração com servidores LDAP e/ou RADIUS.

4.3.2.13. Por suporte técnico de terceiro nível, mas não se limitando as seguintes ações a serem executadas pela CONTRATADA quando demandada pela CONTRATANTE:

4.3.2.14. Análise de disponibilidade;

4.3.2.15. Criação e configuração de VPN Site-to-Site em VXLAN;

4.3.2.16. Auxílio na reserva de IPv6 com base em DHCP/MAC Address;

4.3.2.17. Tratativas relacionadas a IPv6;

4.3.2.18. Problemas relativos a Certificado Digital;

4.3.2.19. Análise e resolução de problemas de comunicação com servidores LDAP;

4.3.2.20. Análise e resolução de problemas via CLI (VPN, SSO, RADIUS, dentre outros);

4.3.2.21. Configuração de VPN SSL com certificado próprio;

4.3.2.22. Auxílio na confecção de políticas com inspeção de pacotes;

4.3.2.23. Integrações com demais soluções de segurança presentes nesta contratação;

4.3.2.24. Configuração de alta disponibilidade;

4.3.2.25. Configuração do Single Sign On (SSO);

4.3.2.26. Restauração da solução a partir de backup;

4.3.2.27. Configuração de inspeção profunda de pacotes e SSL nas políticas de firewall;

4.3.2.28. Tratamento de incidentes junto ao fabricante da solução;

4.3.2.29. Tratamento de RMA junto ao fabricante da solução.

4.3.2.30. Demais solicitações da CONTRATANTE que se fizerem necessárias nas soluções contratadas devem ser previamente acordadas com a CONTRATADA.

5. LOTE 03 – ITEM 04 – SERVIÇO DE FIREWALL CORPORATIVO TIPO 04

5.1. COMPONENTES DE HARDWARE

5.1.1. O equipamento de referência adotado nesta especificação se baseia no modelo Fortigate 40F;

5.1.2. Throughput de, no mínimo, 800 Mbps com a funcionalidade de NGFW. Ou seja, com funcionalidades de Firewall, IPS e Controle de Aplicação habilitadas simultaneamente;

5.1.3. Throughput de, no mínimo, 990 Mbps para Controle de Aplicação;

5.1.4. Throughput de, no mínimo, 5 Gbps para Firewall, considerando pacotes UDP de 1518 bytes;

5.1.5. Suporte a, pelo menos, 700 mil sessões concorrentes TCP;

5.1.6. Suporte a, pelo menos, 35 mil novas sessões TCP por segundo;

5.1.7. Suportar no mínimo 310 Mbps de throughput de Inspeção SSL;

5.1.8. Throughput de, no mínimo, 1 Gbps de IPS;

5.1.9. Throughput de, no mínimo, 4,4 Gbps de VPN IPSec;

5.1.10. Throughput de, no mínimo, 490 Mbps de VPN SSL;

5.1.11. Possuir ao menos 3 interfaces RJ45 Gigabit Ethernet;

5.1.12. Deve suportar a instalação em rack padrão 19” ou ser entregue com bandeja para a instalação em rack;

5.1.13. Deve estar homologado na ANATEL até a data da licitação.

5.2. MONITORAMENTO ATRAVÉS DE CENTRO DE OPERAÇÃO DE SEGURANÇA

5.2.1. A CONTRATADA deverá realizar o monitoramento de toda a solução ofertada no LOTE 3, atuando de forma proativa e reativa a eventos que possam causar impactos ou indisponibilidade na prestação dos serviços contratados;

5.2.2. A CONTRATADA deverá fornecer a partir dos logs coletados dos dispositivos a correlação de eventos e detecção em tempo real de ameaças persistentes avançadas (APTs), vulnerabilidades e indicadores de comprometimento (IOC) para as soluções de segurança e prover visibilidade profunda e insights críticos da rede;

5.2.3. A CONTRATADA deverá fornecer notificações, relatórios e painéis em tempo real para visibilidade das soluções de segurança ofertadas;

5.2.4. A CONTRATADA deverá ter capacidade para detectar malwares, incluindo um relatório informativo com o resumo de como o malware funciona;

5.2.5. A CONTRATADA deverá ter capacidade para identificar uso suspeito e artefatos maliciosos observados na rede ou em um sistema operacional, determinados por meio de indicadores de comprometimento (IOC) como sendo infecções maliciosas ou intrusões;

5.2.6. A CONTRATADA deverá possuir automação para resposta a incidentes com fluxos de trabalho

integrados de gerenciamento de incidentes e conectores nas soluções de segurança.

5.3. SUPORTE ESPECIALIZADO NA SOLUÇÃO DE SEGURANÇA

5.3.1. É de responsabilidade da CONTRATADA o fornecimento dos serviços de suporte técnico especializado de segundo e terceiro nível para o ambiente contratado, inclusive de forma presencial quando este for necessário para o atendimento dos chamados e/ou normalização do ambiente;

5.3.2. Por suporte técnico de segundo nível, mas não se limitando as seguintes ações a serem executadas pela CONTRATADA quando demandada pela CONTRATANTE:

5.3.2.1 Auxiliar na configuração de políticas de firewall;

5.3.2.2. Análise de problemas relacionados a SSL VPN;

5.3.2.3. Análise de problemas relacionados a VPN Site-to-Site;

5.3.2.4. Análise de problemas relacionados a bloqueios indevidos;

5.3.2.5. Ajustes de configurações iniciais (NTP Server, Hostname, Timezone);

5.3.2.6. Auxílio na criação de objetos no firewall;

5.3.2.7. Auxílio na reserva de IPv4 com base em DHCP/MAC Address;

5.3.2.8. Criação e/ou Alteração de perfis de segurança (AV, WEB, APP, DNS, IPS);

5.3.2.9. Criação e/ou Alteração de configuração de túneis VPN Site-to-Site, Dial-up e SSLVPN;

5.3.2.10. Criação e/ou Alteração de interfaces de rede;

5.3.2.11. Criação e/ou Alteração em políticas de roteamento;

5.3.2.12. Criação e/ou Alteração de configuração em integração com servidores LDAP e/ou RADIUS.

5.3.3. Por suporte técnico de terceiro nível, mas não se limitando as seguintes ações a serem executadas pela CONTRATADA quando demandada pela CONTRATANTE:

5.3.3.Análise de disponibilidade;

5.3.3.1. Criação e configuração de VPN Site-to-Site em VXLAN;

5.3.3.2. Auxílio na reserva de IPv6 com base em DHCP/MAC Address;

5.3.3.4. Tratativas relacionadas a IPv6;

5.3.3.5. Problemas relativos a Certificado Digital;

5.3.3.6. Análise e resolução de problemas de comunicação com servidores LDAP;

5.3.3.7. Análise e resolução de problemas via CLI (VPN, SSO, RADIUS, dentre outros);

5.3.3.8. Configuração de VPN SSL com certificado próprio;

5.3.3.9. Auxílio na confecção de políticas com inspeção de pacotes;

5.3.3.10. Integrações com demais soluções de segurança presentes nesta contratação;

5.3.3.11. Configuração de alta disponibilidade;

5.3.3.12. Configuração do Single Sign On (SSO);

5.3.3.13. Restauração da solução a partir de backup;

5.3.3.14. Configuração de inspeção profunda de pacotes e SSL nas políticas de firewall;

5.3.3.15. Tratamento de incidentes junto ao fabricante da solução;

5.3.3.16. Tratamento de RMA junto ao fabricante da solução.

5.3.4. Demais solicitações da CONTRATANTE que se fizerem necessárias nas soluções contratadas devem ser previamente acordadas com a CONTRATADA.

6. LOTE 03 – ITEM 05 – SERVIÇO DE GERENCIAMENTO CENTRALIZADO

6.1. CARACTERÍSTICAS GERAIS

6.1.1. A solução de referência adotada nesta especificação se baseia no modelo FortiManager-VM;

6.2.2. Considerando o volume de equipamentos e escala do projeto, faz-se necessária uma solução de gerenciamento centralizado dos equipamentos ofertados;

6.2.3. Devem ser do mesmo fornecedor das soluções ofertadas no LOTE 03, suportando nativamente todos os recursos listados;

6.2.4. Deve considerar o volume de equipamentos ofertados, considerando todo o licenciamento necessário para a correta gestão dos equipamentos de segurança de rede.

6.2. FUNCIONALIDADES GERAIS

6.2.1. O gerenciamento da solução deve suportar acesso via SSH, cliente ou web (HTTPS) e API;

6.2.2. Deverá suportar contas de usuário/senha estáticas;

6.2.3. Permitir acesso concorrente de administradores;

6.2.4. Definição de perfis de acesso à solução com permissões granulares como: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações;

6.2.5. O sistema deverá suportar o método de autenticação externo usuário/conta do servidor RADIUS;

6.2.6. Todo o provisionamento de serviços deverá ser feito via GUI no sistema de gerenciamento centralizado;

6.2.7. Todas as alterações de configuração deverão ser registradas e arquivadas para fins de auditoria;

6.2.8. A solução deverá informar o status UP/DOWN/SPEED das interfaces LAN e WAN;

6.2.9. Deverá permitir que todos os alarmes e eventos sejam registrados na solução de gerenciamento centralizado;

6.2.10. O gerenciamento deve possibilitar a criação e administração de políticas de firewall e controle de aplicação;

6.2.11. O gerenciamento deve possibilitar a criação e administração de políticas de IPS, Antivírus e Anti Spyware;

6.2.12. O gerenciamento deve possibilitar a criação e administração de políticas de Filtro de URL;

6.2.13. Permitir localizar em quais regras um objeto está sendo utilizado;

6.2.14. Permitir criação de regras que fiquem ativas em horário definido;

6.2.15. A solução deve possibilitar a distribuição e instalação remota, de maneira centralizada, de novas versões de firmware dos appliances;

6.2.16. Deve ser capaz de gerar relatórios ou exibir comparativos entre duas sessões diferentes, resumindo todas as alterações efetuadas;

6.2.17. Deve permitir criar fluxos de aprovação na solução de gerência, onde um administrador possa criar todas as regras, mas estas somente sejam aplicadas após aprovação de outro administrador;

6.2.18. Possuir "wizard" na solução de gerência para adicionar os dispositivos via interface gráfica utilizando IP, login e senha dos equipamentos;

6.2.19. Permitir que eventuais políticas e objetos já presentes nos dispositivos sejam importados quando este for adicionado à solução de gerência;

6.2.20. Permitir visualizar, a partir da estação de gerência centralizada, informações detalhadas dos dispositivos gerenciados, tais como hostname, serial, IP de gerência, licenças, horário do sistema e firmware;

6.2.21. Possuir "wizard" na solução de gerência para instalação de políticas e configurações dos dispositivos;

6.2.22. Permitir criar na solução de gerência de templates de configuração dos dispositivos com informações de DNS, SNMP, configurações de log e administração;

6.2.23. Permitir criar scripts personalizados, que sejam executados de forma centralizada em um ou mais dispositivos gerenciados, através dos comandos de CLI destes;

6.2.24. Possuir histórico dos scripts executados nos dispositivos gerenciados pela solução de gerência;

6.2.25. Permitir configurar e visualizar balanceamento de circuitos nos dispositivos gerenciados de forma centralizada;

6.2.26. Permitir criar vários pacotes de políticas que serão aplicados/associados à dispositivos ou grupos de dispositivos;

6.2.27. Deve permitir criar regras de NAT64 e NAT46 de forma centralizada;

6.2.28. Permitir criar regras anti DDoS de forma centralizada;

6.2.29. Permitir criar os objetos que serão utilizados nas políticas de forma centralizada;

6.2.30. Através da análise de tráfego de rede, web e DNS, deve suportar a verificação de máquinas potencialmente comprometidas ou usuários com uso de rede suspeito;

6.2.31. Suporte a definição de perfis de acesso a solução com permissão granular, como: acesso de gravação, acesso de leitura, criação de novos usuários e alterações nas configurações gerais;

6.2.32. Deve conter um assistente gráfico para adicionar novos dispositivos, usando seu endereço IP, usuário e senha.

6.3.SUPORTE ESPECIALIZADO NA SOLUÇÃO DE SEGURANÇA

6.3.1. É de responsabilidade da CONTRATADA o fornecimento dos serviços de suporte técnico especializado de segundo e terceiro nível para o ambiente contratado, inclusive de forma presencial quando este for necessário para o atendimento dos chamados e/ou normalização do ambiente;

6.3.2. Por suporte técnico de segundo nível, mas não se limitando as seguintes ações a serem executadas pela CONTRATADA quando demandada pela CONTRATANTE:

6.3.2.1. Criação e/ou Alteração de interfaces de rede;

6.3.2.2. Configuração das soluções de segurança através da ferramenta;

6.3.2.3. Atualização dos firmwares das soluções de segurança através da ferramenta;

6.3.2.4. Gerência do Task Monitor;

6.3.2.5. Análise dos eventos das soluções de segurança através da ferramenta;

6.3.2.6. Auxílio na gerência das soluções de segurança através da ferramenta.

6.3.3. Por suporte técnico de terceiro nível, mas não se limitando as seguintes ações a serem executadas pela CONTRATADA quando demandada pela CONTRATANTE;

6.3.3.1. Análise e resolução de problemas via

CLI; 6.3.3.2.Configuração do servidor de autenticação

remota; 6.3.3.3.Atualização do Single Sign On (SSO);

6.3.3.4.Atualização do SAML SSO;

6.3.3.5.Tratamento de incidentes junto ao fabricante da solução.

6.3.4. Demais solicitações da CONTRATANTE que se fizerem necessárias nas soluções contratadas devem ser previamente acordadas com a CONTRATADA.

7. LOTE 03 – ITEM 06 – SERVIÇO DE RELATORIA E DE ANÁLISE DE LOGS

7.1. CARACTERÍSTICAS GERAIS

7.1.1. O equipamento de referência adotado nesta especificação se baseia no modelo FAZ-810G;

7.1.2. Capacidade de receber e processar no mínimo 200 GB de logs por dia;

7.1.3. Sustentar taxa de análises de logs de 4.000 logs por segundo;

7.1.4. Deve possuir no mínimo 8TB para armazenamento de logs, após configuração do RAID;

7.1.5. Suportar no mínimo 800 dispositivos e VDOMS;

7.1.6. Tamanho máximo de 1U;

7.1.7. Deve possuir discos removíveis;

7.1.8. Deve ser fornecido com fontes redundantes do tipo hot swap.

7.2. FUNCIONALIDADES GERAIS

7.2.1. Deve permitir o encaminhamento de log no formato syslog;

7.2.2. Deve permitir o encaminhamento de log no formato CEF (Common Event Format);

7.2.3. Suporte a geração de relatórios de tráfego em tempo real, em formato de mapa geográfico;

7.2.4. Suporte a geração de relatórios de tráfego em tempo real, no formato de gráfico de bolhas;

7.2.5. Suporte a geração de relatórios de tráfego em tempo real, em formato de tabela gráfica;

7.2.6. Deve ser possível ver a quantidade de logs enviados de cada dispositivo monitorado;

7.2.7. Deve possuir mecanismos de remoção automática para logs antigos;

7.2.8. Permitir importação e exportação de relatórios;

7.2.9. Deve ter a capacidade de criar relatórios no formato HTML e CSV;

7.2.10. Deve permitir exportar os logs no formato CSV;

7.2.11. Deve permitir a geração de logs de auditoria, com detalhes da configuração efetuada, o administrador que efetuou a alteração e seu horário;

7.2.12. Os logs gerados pelos dispositivos gerenciados devem ser centralizados nos servidores da plataforma, mas a solução também deve oferecer a possibilidade de usar um servidor syslog externo ou similar;

7.2.13. A solução deve ter relatórios predefinidos;

7.2.14. Deve permitir o envio automático dos logs para um servidor FTP externo a solução;

7.2.15. Deve ter a capacidade de personalizar a capa dos relatórios obtidos;

7.2.16. Deve permitir centralmente a exibição de logs recebidos por um ou mais dispositivos, incluindo a capacidade de usar filtros para facilitar a pesquisa nos logs;

7.2.17. Os logs de auditoria das regras e alterações na configuração do objeto devem ser exibidos em uma lista diferente dos logs relacionados ao tráfego de dados;

7.2.18. Deve ter a capacidade de personalizar gráficos em relatórios, como barras, linhas e tabelas;

7.2.19. Deve ter um mecanismo de pesquisa detalhada ou “Drill-Down” para navegar pelos relatórios em tempo real;

7.2.20. Deve permitir que os arquivos de log sejam baixados da plataforma para uso externo;

7.2.21. Deve ter a capacidade de gerar e enviar relatórios periódicos automaticamente;

7.2.22. Permitir a personalização de qualquer relatório pré-estabelecido pela solução, exclusivamente pelo administrador, para adotá-lo de acordo com suas necessidades;

7.2.23. Permitir o envio de relatórios por e-mail automaticamente;

7.2.24. Deve permitir que o relatório seja enviado por e-mail para destinatário específico;

7.2.25. Permitir a programação da geração de relatórios, conforme calendário definido pelo administrador;

7.2.26. Permitir a exibição graficamente e em tempo real da taxa de geração de logs para cada dispositivo gerenciado;

7.2.27. Deve permitir o uso de filtros nos relatórios;

7.2.28. Deve permitir definir o design dos relatórios, incluir gráficos, adicionar texto e imagens, alinhamento, quebras de página, fontes, cores, entre outros;

7.2.29. Permitir especificar o idioma dos relatórios criados;

7.2.30. Gerar alertas automáticos via e-mail, SNMP e syslog, com base em eventos especiais em logs, gravidade do evento, entre outros;

7.2.31. Deve permitir o envio automático de relatórios para um servidor SFTP ou FTP externo;

7.2.32. Deve ser capaz de criar consultas SQL ou similares nos bancos de dados de logs, para uso em gráficos e tabelas em relatórios;

7.2.33. Possibilidade de exibir nos relatórios da GUI as informações do sistema, como licenças, memória, disco rígido, uso da CPU, taxa de log por segundo recebido, total de logs diários recebidos, alertas do sistema, entre outros;

7.2.34. Deve fornecer as informações da quantidade de logs armazenados e as estatísticas do tempo restante armazenado;

7.2.35. Deve permitir aplicar políticas para o uso de senhas para administradores de plataforma, como tamanho mínimo de caracteres permitidos;

7.2.36. Deve permitir visualizar em tempo real os logs recebidos;

7.2.37. Deve permitir gerar alertas de eventos a partir de logs recebidos.

7.3. SUPORTE ESPECIALIZADO NA SOLUÇÃO DE SEGURANÇA

7.3.1. É de responsabilidade da CONTRATADA o fornecimento dos serviços de suporte técnico especializado de segundo e terceiro nível para o ambiente contratado, inclusive de forma presencial quando este for necessário para o atendimento dos chamados e/ou normalização do ambiente;

7.3.2. Por suporte técnico de segundo nível, mas não se limitando as seguintes ações a serem executadas pela CONTRATADA quando demandada pela CONTRATANTE:

7.3.2.1. Utilização geral do monitoramento de eventos e incidentes na ferramenta;

7.3.2.2. Configuração de envio de relatórios padrão;

7.3.2.3. Análise de logs através da ferramenta.

7.3.3. Por suporte técnico de terceiro nível, mas não se limitando as seguintes ações a serem executadas pela CONTRATADA quando demandada pela CONTRATANTE:

7.3.3.1. Configuração de perfil para envio de

relatórios; 7.3.3.2.Criação de relatórios personalizados;

7.3.3.3.Gerência do banco de dados via CLI;

7.3.3.4.Configuração do servidor de autenticação remota;

7.3.3.5.Configuração de alta disponibilidade;

7.3.3.6.Integrações com demais soluções de segurança presentes nesta contratação;

7.3.3.7.Tratamento de incidentes junto ao fabricante da solução;

7.3.3.8.Tratamento de RMA junto ao fabricante da solução.

7.3.4. Demais solicitações da CONTRATANTE que se fizerem necessárias nas soluções contratadas devem ser previamente acordadas com a CONTRATADA.

8. LOTE 03 – ITEM 07 – SERVIÇO DE FIREWALL DE APLICAÇÃO WEB

8.1. ESPECIFICAÇÃO DO HARDWARE

8.1.1. O CLUSTER deverá ser composto por 2 (dois) equipamentos;

8.1.2. O equipamento de referência adotado nesta especificação se baseia no modelo FORTIWEB 1000F;

8.1.3. Throughput de, no mínimo, 2,5 Gbps. Com funcionalidade de proteção de aplicações web;

8.1.4. Possuir funcionalidades de alta disponibilidade, ativo/ativo e ativo/passivo;

8.1.5. Possuir ao menos 8 interfaces RJ45 Gigabit Ethernet com funcionalidade de bypass, 4 interfaces SFP Gigabit Ethernet sem bypass, 2 interfaces SFP+ Gigabit Ethernet;

8.1.6. Possuir processamento SSL/TLS por hardware;

8.1.7. Armazenamento interno de, no mínimo, 2 discos SSD de 480GB;

8.1.8. Possuir tamanho máximo de 2U;

8.1.9. Deve ser fornecido com fontes redundantes do tipo hot swap.

8.2. FUNCIONALIDADES GERAIS

8.2.1. A solução deverá ser do tipo appliance, destinada a finalidade de firewall de aplicação web (Web Application Firewall – WAF), bem como as licenças necessárias para o seu funcionamento e proteção de servidores e aplicações web;

8.2.2. A implantação da solução deverá ser planejada previamente em conjunto com a CONTRATANTE, onde deverão ser definidos todos os passos necessários para a instalação, incluindo o cronograma de implantação, planos de testes e homologação da solução.

8.3. FUNCIONALIDADES DE REDE

8.3.1. A solução deve ser capaz de ser implementada no modo Proxy (Transparente e Reverso), Passivo e Inline Transparente (Bridge);

8.3.2. A solução deve ser capaz de ser implementada com protocolo WCCP;

8.3.3. Suportar VLANs no padrão IEEE 802.1q;

8.3.4. Suportar endereçamento IPv4 e IPv6 nas interfaces físicas e virtuais (VLANs);

8.3.5. A solução deve suportar roteamento por política (policy route).

8.4. FUNCIONALIDADES DE GERÊNCIA

8.4.1. O sistema operacional/firmware deve suportar interface gráfica web para a configuração das funções do sistema operacional, utilizando protocolo HTTPS, e através de interface de linha de comando (CLI), acessando localmente, via porta de console, ou remotamente via SSH;

8.4.2. Deve possuir administração baseada em interface web;

8.4.3. Deve possuir administração baseada em interface de linha de comando via Telnet;

8.4.4. Possuir auto complementação de comandos na CLI;

8.4.5. Possuir ajuda contextual na CLI;

8.4.6. A solução deve possuir um Dashboard com informações sobre o sistema (Informações do Cluster, hostname, número de série, modo de operação, tempo em serviço, versão do firmware);

8.4.7. Deverá ser possível visualizar através da interface gráfica informações de licenças, assinaturas e contrato de suporte;

8.4.8. A solução ofertada deverá possuir acesso à linha de comando CLI via interface gráfica;

8.4.9. Deve prover, na interface gráfica, informações de consumo de CPU e estatísticas das conexões;

8.4.10. Deve ser possível visualizar na interface gráfica as informações de consumo de memória;

8.4.11. Deverá possuir dashboard que permita visualizar os últimos logs de ataque detectados/bloqueados;

8.4.12. Deve prover na interface de gráfica informações de: estatísticas de throughput HTTP em tempo real, estatísticas dos eventos de ataque detectados/bloqueados, estatísticas de requisições HTTP em tempo real e últimos logs de eventos do sistema;

8.4.13. Possuir na interface gráfica estatísticas de conexões concorrentes de conexões por segundo e de políticas de segurança do sistema;

8.4.14. Possuir um painel de visualização com informações das interfaces de rede do sistema;

8.4.15. A configuração de administração da solução deve possibilitar a utilização de perfis;

8.4.16. Deve ser possível executar e restaurar backup via interface web (GUI);

8.4.17. Deve ter a opção para criptografar o backup utilizando algoritmo AES 128-bit ou superior;

8.4.18. Deve ser possível executar e restaurar backup utilizando-se FTP;

8.4.19. Deve ser possível executar e restaurar backup utilizando-se SFTP e TFTP;

8.4.20. Deve ser possível antes de aplicar uma nova versão de firmware testar o mesmo em memória RAM sem instalação em disco;

8.4.21. Deve ser possível instalar um firmware alternativo em disco e inicializá-lo em caso de falha do firmware principal;

8.4.22. Deve ter suporte ao protocolo de monitoração SNMP v1, SNMP v2c e SNMP v3;

8.4.23. Deve ser capaz de realizar notificações de eventos de segurança através de e-mail, traps SNMP e syslog;

8.4.24. A solução deverá ter a capacidade de armazenar logs localmente em disco e em servidor externo via protocolo syslog;

8.4.25. Ter a capacidade de armazenar logs em appliance remoto;

8.4.26. A solução deve ter a capacidade de enviar alertas por e-mail de eventos baseados em severidades e/ou categorias;

8.4.27. A solução deve possuir dados analíticos contendo localização geográfica dos clientes web;

8.4.28. A solução deve possuir dados analíticos, sendo possível visualizar a contagem total de ataques e percentual de cada país de origem, o volume total de tráfego em bytes e percentual de cada país de origem e o total de acessos (hits) e percentual de cada país de origem;

8.4.29. Deverá ter a capacidade de gerar relatórios detalhados baseados em tráfego/acessos/atividades do usuário;

8.4.30. Deve ter suporte a RESTful API para gerenciamento de configurações.

8.5. FUNCIONALIDADES DE AUTENTICAÇÃO

8.5.1. Os usuários devem ser capazes de autenticar através do cabeçalho de autorização HTTP/HTTPS;

8.5.2. Os usuários devem ser capazes de autenticar através de formulários HTML embutidos;

8.5.3. A solução deverá ser capaz de autenticar usuários através de certificados digitais pessoais;

8.5.4. Deve possuir base local para armazenamento e autenticação de contas de usuários;

8.5.5. A solução deve ter a capacidade de autenticar usuários em bases externas/remotas LDAP e RADIUS;

8.5.6. Os usuários devem ser capazes de autenticar através de contas de usuários em base remota NTLM;

8.5.7. A solução deve ser capaz de criar grupos de usuários para acessos semelhantes na autenticação;

8.5.8. Deve suportar CAPTCHA e Real Browser Enforcement (RBE);

8.5.9. Deve suportar autenticação de duplo fator.

8.6. ITENS REGULATÓRIOS E CERTIFICAÇÕES

8.6.1. A solução deve suportar o modelo de segurança positiva definido pelo OWASP, pelo menos o que consta no TOP 10;

8.6.2. O equipamento deve possuir certificação FCC Class A part 15;

8.6.3. O equipamento deve possuir certificação C-Tick;

8.6.4. O equipamento deve possuir certificação VCCI;

8.6.5. O equipamento deve possuir certificação CE;

8.6.6. O equipamento deve possuir certificação UL/cUL;

8.6.7. O equipamento deve possuir certificação CB.

8.7. FUNCIONALIDADES DE WEB APPLICATION FIREWALL

8.7.1. Deve ter suporte nativo de HTTP/2;

8.7.2. Deve suportar tradução de HTTP/2 a HTTP 1.1;

8.7.3. Deve suportar interoperabilidade com OpenAPI 3.0;

8.7.4. Deverá ser capaz de identificar e bloquear ataques através de um banco de dados de assinaturas de vírus e IP reputation, atualizado de forma automática;

8.7.5. A solução deve permitir escolher entre usar o banco de dados completo ou apenas uma base de dados contendo ameaças mais recentes;

8.7.6. Deve ter algoritmos para detecção de ameaças avançadas baseados em aprendizagem de máquina com inteligência artificial (IA);

8.7.7. Deverá minimizar a ocorrência de falsos positivos e falsos negativos utilizando Inteligência Artificial;

8.7.8. Possuir mecanismo de aprendizado automático capaz de identificar todos os conteúdos das aplicações, incluindo URLs, parâmetros URLs, campos de formulários e o que se espera de cada campo;

8.7.9.10. O perfil aprendido de forma automatizada pode ser ajustado e editado;

8.7.11. Ter a capacidade de criação de assinaturas de ataque customizáveis;

8.7.12. Ter a capacidade de proteção para ataques do tipo Adobe Flash binary (AMF) protocol;

8.7.13. Ter a capacidade de proteção para ataques do tipo Botnet;

8.7.14. Ter a capacidade de proteção para ataques do tipo Browser Exploit Against SSL/TLS (BEAST);

8.7.15. A solução deverá possuir funcionalidade de proteção contra ataques de força bruta;

8.7.16. Deve suportar detecção a ataques de Clickjacking;

8.7.17. Deve suportar detecção a ataques de alteração de cookie;

8.7.18. Identificar e prevenir ataques do tipo Credit Cart Theft;

8.7.19. Identificar e prevenir ataques Cross Site Request Forgery (CSRF);

8.7.20. A solução deverá possuir funcionalidade de proteção contra ataques como cross site scripting (XSS);

8.7.21. Deve possuir proteção contra ataques de Denial of Service (DoS);

8.7.22. Ter a capacidade de proteção para ataques do tipo HTTP header overflow;

8.7.23. Ter a capacidade de proteção para ataques do tipo Local File inclusion (FLI);

8.7.24. Ter a capacidade de proteção para ataques do tipo Man-in-the Middle (MITM);

8.7.25. Ter a capacidade de proteção para ataques do tipo Remote File Inclusion (RFI);

8.7.26. Ter a capacidade de proteção para ataques do tipo Server Information Leakage;

8.7.27. Proteção contra envios de comandos SQL escondidos nas requisições enviadas a bases de dados (SQL Injection);

8.7.28. Ter a capacidade de proteção para ataques do tipo Malformed XML;

8.7.29. Identificar e prevenir ataques do tipo Low-rate DoS;

8.7.30. Prevenção contra Slow POST attack;

8.7.31. Proteger contra ataques Slowloris;

8.7.32. Ter a capacidade de proteção para ataques do tipo SYN flood;

8.7.33. Ter a capacidade de proteção para ataques do tipo Forms Tampering;

8.7.34. A solução deverá possuir funcionalidade de proteção contra ataques de manipulação de campo escondido;

8.7.35. Ter a capacidade de proteção para ataques do tipo Directory Traversal;

8.7.36. Ter a capacidade de proteção do tipo Access Rate Control;

8.7.37. Reconhecer e remediar Zero Day Attacks;

8.7.38. Ter a habilidade de configurar proteção do tipo TCP SYN flood-style para prevenção de DoS para qualquer política, através de Syn Cookie e Half Open Threshold;

8.7.39. Permitir configurar regras de bloqueio a métodos HTTP indesejados;

8.7.40. Permitir que sejam configuradas regras de limite de upload por tamanho de arquivo;

8.7.41. Deve permitir que o administrador bloqueie o tráfego de entrada e/ou tráfego de saída com base nos

países, sem a necessidade de gerir manualmente os ranges de endereços IP correspondentes a cada país;

8.7.42. Deve suportar a criação de políticas por geolocalização, permitindo que o tráfego de determinado país seja bloqueado;

8.7.43. Permitir configurar listas negras de bloqueio e listas brancas de confiança, baseadas em endereço IP de origem;

8.7.44. Permitir a liberação temporária ou definitiva (allow list) de endereços IP bloqueados por terem originados ataques detectados pela solução;

8.7.45. Deve permitir adicionar, automaticamente ou manualmente, em uma lista de bloqueio, os endereços IP de origem, de acordo com a base de IP Reputation;

8.7.46. Ter a capacidade de conectar-se a uma base de dados na Internet para validar que as credenciais que usam os usuários para acessar a algum sistema não sejam credenciais roubadas;

8.7.47. Ter a capacidade de Prevenção ao Vazamento de Informações (DLP), bloqueando o vazamento de informações de cabeçalho HTTP;

8.7.48. Ter a funcionalidade de proteger o website contra ações de desfiguração (defacement), com restauração automática e rápida do site caso ocorra à falha;

8.7.49. Ter a funcionalidade de antivírus integrada para inspeção de tráfego e arquivos, sem a necessidade de instalação de outro equipamento;

8.7.50. Ter a capacidade de investigar e analisar todo o tráfego HTTP para atestar se está em conformidade com a respectiva RFC, bloqueando ataques e tráfego em não-conformidade;

8.7.51. Deverá ser capaz de fazer aceleração de SSL, onde os certificados digitais são instalados na solução e as requisições HTTP são enviadas aos servidores sem criptografia;

8.7.52. A solução deve ser capaz de funcionar como terminador de sessões SSL para a aceleração de tráfego;

8.7.53. Para SSL/TLS offload suportar no mínimo SSL 3.0, TLS 1.0, 1.1 e 1.2;

8.7.54. A solução deve ter a capacidade de armazenar certificados digitais de CA's;

8.7.55. A solução deve ser capaz de gerar CSR para ser assinado por uma CA;

8.7.56. A solução deve ser capaz de validar os certificados que são válidos e não foram revogados por uma lista de certificados revogados (CRL);

8.7.57. A solução deve conter as assinaturas de robôs conhecidos como link checkers, indexadores de web, search engines, spiders e web crawlers que podem ser colocados nos perfis de controle de acesso, bem como resetar tais conexões;

8.7.58. A solução deve ter um sistema de reputação de endereços IP públicos conhecidos como fontes de ataques DDoS, botnets, spammers etc. Tal sistema deve ser atualizado automaticamente;

8.7.59. A solução deverá ser capaz de limitar o total de conexões permitidas para cada servidor real de um pool de servidores;

8.7.60. A solução deve permitir a customização ou redirecionar solicitações e respostas HTTP no HTTP Host, Request URL HTTP, HTTP Referer, HTTP Body e HTTP Location;

8.7.61. A solução deve permitir criar regras definindo a ordem em que as páginas devem ser acessadas para prevenir ataques como cross-site request forgery (CSRF);

8.7.62. A solução deve ter a capacidade de definir restrições a métodos HTTP;

8.7.63. A solução deve ter a capacidade de proteger contra a detecção de campos ocultos;

8.7.64. Permitir que sejam criadas assinaturas customizadas de ataques e DLP, através de expressões regulares;

8.7.65. A solução deve incluir capacidade de atuar como um scanner de vulnerabilidades para diagnóstico e identificação de ameaças nos servidores web, software desatualizado e potenciais buffers overflows;

8.7.66. Deve gerar perfil de proteção automaticamente a partir de relatório em formato XML gerado por scanner de vulnerabilidade de terceiros;

8.7.67. Deve permitir agendar a verificação de vulnerabilidades;

8.7.68. A solução deve gerar um relatório da análise de vulnerabilidades no formato HTML;

8.7.69. Suportar redirecionamento e reescrita de requisições e respostas HTTP;

8.7.70. Permitir redirecionar requisições HTTP para HTTPS;

8.7.71. Permitir reescrever a linha URL no cabeçalho de uma requisição HTTP;

8.7.72. Permitir reescrever o campo “Host:” no cabeçalho de uma requisição HTTP;

8.7.73. Permitir reescrever o campo “Referer:” no cabeçalho de uma requisição HTTP;

8.7.74. Permitir redirecionar requisições para outro web site;

8.7.75. Permitir enviar resposta HTTP 403 Forbidden para requisições HTTP;

8.7.76. Permitir reescrever o parâmetro “Location:” no cabeçalho HTTP de uma resposta de redirecionamento HTTP de um servidor web;

8.7.77. Permitir reescrever o corpo (“body”) de uma resposta HTTP de um servidor web;

8.7.78. Permitir adicionar o campo X-Forwarded-For para identificação do endereço real do cliente quando no modo de proxy reverso;

8.7.79. A solução deve suportar regras para definir se as solicitações HTTP serão aceitas com base na URL e a origem do pedido e, se necessário, aplicar uma taxa específica de transferência (rate limit);

8.7.80. A solução deve suportar o mecanismo de combinação de controle de acesso e autenticação utilizando mecanismos como HTML Form, Basic e Suporte a Single Sign On, métodos como LDAP e RADIUS para consultas e integração dos usuários da aplicação;

8.7.81. Possuir capacidade de caching para aceleração web;

8.7.82. A solução deve ser capaz de submeter arquivos para solução de sandboxing do mesmo fabricante, através de uma política de restrição de carregamento de arquivo;

8.7.83. Deve permitir ao administrador a criação de novas assinaturas e/ou alteração de assinaturas já existentes.

8.8. SUPORTE ESPECIALIZADO NA SOLUÇÃO DE SEGURANÇA

8.8.1. É de responsabilidade da CONTRATADA o fornecimento dos serviços de suporte técnico especializado de segundo e terceiro nível para o ambiente contratado, inclusive de forma presencial quando este for necessário para o atendimento dos chamados e/ou normalização do ambiente;

8.8.2. Por suporte técnico de segundo nível, mas não se limitando as seguintes ações a serem executadas pela CONTRATADA quando demandada pela CONTRATANTE:

8.8.2.1. Configurações de Redes;

8.8.2.2. Configuração de Políticas;

8.8.2.3. Configuração de Objetos;

8.8.2.4. Configuração de Políticas de Entrega de Aplicação;

8.8.2.5. Gerência dos Certificados.

8.8.3. Por suporte técnico de terceiro nível, mas não se limitando as seguintes ações a serem executadas pela CONTRATADA quando demandada pela CONTRATANTE:

8.8.3.1. Integrações com demais soluções de segurança presentes nesta

contratação; 8.8.3.2.Gerência do ambiente Web Protection;

8.8.3.3. Gerência do ambiente DoS Protection;

8.8.3.4. Gerência do ambiente Auto Learn;

8.8.3.5. Análise e resolução de problemas via CLI;

8.8.3.6. Atualização de configuração de certificado próprio;

8.8.3.7. Tratamento de incidentes junto ao fabricante da solução;

8.8.3.8. Tratamento de RMA junto ao fabricante da solução.

8.8.4. Demais solicitações da CONTRATANTE que se fizerem necessárias nas soluções contratadas devem ser previamente acordadas com a CONTRATADA.

9. LOTE 03 – ITEM 08 – SERVIÇO DE SEGURANÇA DE ENDPOINT

9.1. CARACTERÍSTICAS GERAIS

9.1.1. A solução de referência adotada nesta especificação se baseia no modelo FortiClient EPP;

9.1.2. Deverá permitir a instalação, gerência e atualizações das funcionalidades para 3000 (três mil) endpoints, durante toda a vigência contratual;

9.1.3. Deverá permitir o gerenciamento dos endpoints remotamente, a partir de uma console de administração central do próprio fabricante;

9.1.4. A solução deve prover um método de controlar o acesso identificando o dispositivo do usuário, autenticação e postura com base em tags de Zero Trust;

9.1.5. A solução de ZTNA deve ser composta pelos agentes a serem instalados nas máquinas dos usuários finais, bem como por um proxy de acesso, o qual concentrará as requisições dos agentes para acesso às aplicações corporativas;

9.1.6. A solução de proxy de acesso deve prover suporte a um método de publicação de aplicações corporativas sem necessidade de agente, tal como mediante um portal web SSL a ser acessado por cada usuário;

9.1.7. O licenciamento deve se basear no número de agentes registrados na solução.

9.2. FUNCIONALIDADES GERAIS

9.2.1. Deve ser compatível com pelo menos os seguintes sistemas operacionais:

9.2.1.Microsoft Windows: 7 (32 e 64 bits), 8.1 (32 e 64 bits), 10 (32 e 64 bits) e 11 (64 bits);

9.2.1.Microsoft Windows Server: 2008 R2, 2012, 2012 R2, 2016, 2019 e 2022;

9.2.1.Mac OS X: versões 13, 12, 11 e 10.15;

9.2.1.Linux: Ubuntu 18.04 e posterior, Debian 11 e posterior, CentOS Stream 8, CentOS 7.4 e posterior, RedHat 7.4 e posterior, Fedora 36 e posterior.

9.2.1.Tanto mediante agente ou sem agente deve ser possível habilitar MFA (autenticação multifator) no processo de autenticação dos usuários;

9.2.1.A console central deve emitir, assinar, revogar e instalar automaticamente um certificado para os agentes contendo ID único de cada agente, número de série do certificado e número de série da console central. O certificado emitido deverá ser único por agente e deverá ainda ser compartilhado com o proxy de acesso;

9.2.1.O certificado emitido deve ser utilizado no processo de autenticação via ZTNA para identificar o dispositivo do usuário final junto ao proxy de acesso;

9.2.1.Deve suportar pelo menos os seguintes níveis de log: emergência, alerta, crítico, erro, aviso, informativo, debug;

9.2.1.Deve ser possível exportar os logs diretamente a nível de agente;

9.2.1.Deve ser possível exigir uma senha para desconectar o agente da console central;

9.2.1.Deve existir a possibilidade de restringir o usuário de realizar backup da configuração do agente;

9.2.1.Deve ser possível evitar que o usuário realize um shutdown do agente após estar registrado à console central;

9.2.1.Deve ser possível enviar os logs para uma ferramenta de consolidação de logs do mesmo fabricante, visando consolidar os logs do proxy de acesso ZTNA em conjunto com os logs dos agentes;

9.2.1.Deve ser possível configurar o agente para usar proxy;

9.2.1.Deve existir a possibilidade de criar um convite para que os usuários realizem o registro do agente à console central;

9.2.1.Deverá ser possível enviar uma notificação por e-mail contendo o código de registro para os usuários finais informados, bem como um link para download do instalador do agente;

9.2.1.A console central de agentes deve dispor de métodos para determinar se um usuário está on-net ou off-net, ou seja, dentro ou fora da rede corporativa. Deve ser possível ainda criar perfis de configurações distintos para os usuários on-net e off-net;

9.2.1.Deve ser possível atribuir grupos de agentes a perfis de políticas específicos;

9.2.1.Deve ser possível atribuir um nível de prioridade a um perfil de política visando priorizar qual política será utilizada caso um grupo de agentes esteja associado a mais de um perfil de política;

9.2.1.A console central deve apresentar um resumo das informações de cada endpoint, tais como: nome do dispositivo, sistema operacional, IP privado, endereço mac, IP público, estado da conexão com a console central, zero trust tags associadas, detalhes da conexão de rede cabeada e WIFI, detalhes do hardware como

modelo do dispositivo, fabricante, CPU, RAM, número de série e capacidade de armazenamento;

9.2.1.Deve permitir ainda facilmente ver detalhes de qual política está associada com cada agente, qual versão de agente está em uso em um respectivo endpoint, número de série do agente, identificador único e número de série do certificado emitido para o processo de ZTNA;

9.2.1.O proxy de acesso deve atuar como proxy reverso para aplicações baseadas em HTTP, HTTPS, RDP, SMB, CIFS, SSH, SMTP, SMTPS, IMAP, IMAPS, POP3 e POP3S;

9.2.1.Para regras de encaminhamento de tráfego TCP, deve ser possível vincular o servidor com um FQDN visando ofuscar o endereço IP privado do servidor. Deste modo, o agente deve manipular o host file do endpoint visando criar entradas DNS;

9.2.1.Deve ser possível definir um pool de IPs no proxy de acesso como IPs de origem para comunicação interna com as aplicações privadas;

9.2.1.A console central deve permitir mapear as regras de destinos de ZTNA a serem sincronizadas com os endpoints e permitir ainda definir para qual tráfego deve ser aplicada criptografia, tal como para tráfego HTTP sem criptografia nativa;

9.2.1.Deve permitir criação de regras de conformidade que avaliem à postura do dispositivo e auxiliem o administrador no controle de acesso à recursos da infraestrutura, impedindo que um cliente não conforme possa se conectar a redes críticas;

9.2.1.As regras de conformidade devem gerar tags que são sincronizadas entre os elementos da solução de ZTNA visando controlar a postura de um determinado endpoint diretamente no proxy de acesso;

9.2.1.A postura deve ser monitorada continuamente para que, caso ocorra uma alteração, o proxy de acesso termine e passe a bloquear a conexão em desacordo com as regras de compliance definidas;

9.2.1.Deve ser possível construir tags com verificações no endpoint, as quais podem variar de acordo com o suporte ao sistema operacional, tais como se o endpoint está logado no domínio, versão do sistema operacional, chave de registro, processo, nível de vulnerabilidade, CVEs, arquivos existentes em um caminho específico e até mesmo se o antivírus está instalado e sendo executado, além de ser possível validar se as assinaturas estão atualizadas;

9.2.1.A console central deve permitir exportar e importar tags entre sistemas diferentes por meio de um arquivo JSON;

9.2.1.Deve ser possível verificar quais endpoints estão associadas com cada tag;

9.2.1.Deve ser possível criar regras no proxy de acesso determinando se um dispositivo necessita estar de acordo com uma ou mais tags simultaneamente, caso a política possua vínculo com diversas tags;

9.2.1.Deve ser possível criar regras no proxy de acesso vinculando interface de origem, IP de origem, IP de destino, servidor ZTNA, tag ZTNA, grupo de usuários ou usuário;

9.2.1.Para validação da autenticação dos usuários em conjunto com as regras de proxy de acesso, a solução deve suportar SAML, LDAP, RADIUS ou base de dados local;

9.2.1.Deve possibilitar definir funções administrativas relacionadas às permissões dos endpoints, de políticas e de configurações gerais;

9.2.1.A console central deve possuir funcionalidade de rastreamento de vulnerabilidades a nível de endpoint, permitindo ainda definir o rastreamento no momento do registro, quando ocorrer uma atualização de uma assinatura vulnerável, bem como patches e atualizações de segurança a nível de sistema operacional;

9.2.1.Deverá ser possível agendar quando o rastreamento deve ocorrer ou vinculá-lo em conjunto com a janela de manutenção automática do Windows;

9.2.1.Deve permitir que o usuário inicie uma análise de vulnerabilidade sob demanda diretamente no agente;

9.2.1.Deve ser possível aplicar um patch automático com base no nível de criticidade definido, tal como atualizar automaticamente patches considerados críticos;

9.2.1.Caso não seja possível aplicar um patch automático para corrigir uma vulnerabilidade, requerendo assim um patch manual, deve ser possível excluir essa aplicação da verificação de compliance;

9.2.1.Deve ser possível excluir determinadas aplicações da verificação de compliance e até mesmo desabilitar o patch automático;

9.2.1.O agente deve dispor de um sistema de notificação do tipo popup visando alertar o usuário;

9.2.1.As vulnerabilidades encontradas devem ser exibidas diretamente no agente com um link para análise de mais detalhes, englobando nome da vulnerabilidade, severidade, produtos afetados, CVE IDs, descrição, informação do fabricante do software e, quando disponível, link para download do patch no site público do fabricante do software;

9.2.1.Os resultados da verificação de vulnerabilidades devem incluir pelo menos: lista de vulnerabilidades, número de vulnerabilidades classificadas como críticas, altas, médias e baixas, bem como disponibilizar ainda a possibilidade de aplicar a remediação imediatamente;

9.2.1.Deve possuir módulo para execução de filtro web a nível de endpoint mediante uso do agente local, realizando a filtragem diretamente no endpoint, podendo ainda ser possível bloquear, permitir, alertar ou monitorar o tráfego web com base na categoria de URL ou filtro de URL customizado;

9.2.1.O agente deve realizar consultas online ao centro de inteligência do próprio fabricante para determinar a categoria de uma determinada URL visando aplicar o controle de acesso à Internet;

9.2.1.Deve ser possível configurar o filtro de URL com base em expressões regulares (regex) com as opções de permitir, bloquear ou monitorar;

9.2.1.O agente para Windows deve permitir inspeção de tráfego HTTPS mediante instalação de plugin disponibilizado pelo mesmo fabricante do agente, o qual deve ser compatível com Google Chrome, Mozilla Firefox e Microsoft Edge;

9.2.1.Deve ser possível verificar as violações de filtro web diretamente no agente, especificando ainda a URL, categoria, quando a violação ocorreu e usuário;

9.2.1.Deve ser possível determinar quando o filtro web entrará em ação no agente, se deverá estar sempre ativo ou somente quando o usuário estiver fora da rede corporativa;

9.2.1.Deve ser possível configurar o proxy de acesso para atuar como CASB (Cloud Access Security Broker) em linha, inline do inglês, visando controlar o acesso a aplicações SaaS;

9.2.1.O proxy de acesso deve manter uma base de aplicações dinâmica, a qual deve ser compartilhada pelo centro de inteligência do fabricante da solução.

10. LOTE 03 – ITEM 09 – SERVIÇO DE GERENCIAMENTO DE IDENTIDADE

10.1. CARACTERÍSTICAS GERAIS

10.1.1. A solução de referência adotada nesta especificação se baseia no modelo FortiAuthenticator-VM com FortiToken;

10.1.2. A solução deverá ser instalada nas dependências do órgão, através de Appliance Virtual compatível com os seguintes Hypervisors: VMware, Hyper-V e NUTANIX.

10.2. FUNCIONALIDADES GERAIS

10.2.1. Deverá possuir um servidor LDAP interno que permite ser configurado de forma hierárquica, para a correta administração por grupos ou unidades organizacionais dos usuários locais;

10.2.2. Deverá permitir a geração em massa de usuários na base de dados local pelo administrador, possibilitando que uma lista de usuários seja importada a partir de um arquivo externo;

10.2.3. Deverá realizar backup automatizado (agendados por critérios pré-definidos), não somente sob demanda;

10.2.4. Deverá permitir o backup completo da solução, incluindo toda a configuração: interfaces, endereços IP, base de usuários, grupos e tokens. O arquivo de restauração deverá permitir recuperar o equipamento diretamente da interface gráfica;

10.2.5. Deverá suportar a opção de backup criptografado;

10.2.6. Deverá suportar Single Sign On (SSO) por estrutura RSSO (Radius Single Sign On);

10.2.7. Deverá permitir ordenação de logs de acordo com a necessidade do administrador: por usuário que realizou a mudança, por data, por forma ascendente e por forma descendente;

10.2.8. Deverá suportar filtragem dos usuários que irão utilizar recurso de SSO, separando-os de grupos que não necessitam;

10.2.9. Deverá suportar a validação de certificados de fontes externas;

10.2.10. Deverá funcionar como servidor LDAP (Lightweight Directory Access Protocol), proporcionando autenticação aos dispositivos compatíveis com tal protocolo;

10.2.11. Deverá suportar captura de pacotes através da interface gráfica para resolução de problemas (troubleshoot) avançado em wireshark ou outra ferramenta de análise de pacotes;

10.2.12. Deverá suportar a criação de usuários em base local independente, que poderão ser utilizados na autenticação dos dispositivos conforme necessidade, contudo em canal de comunicação seguro;

10.2.13. Deverá permitir definir uma lista de usuários de SSO que serão ignorados, evitando assim interferência de contas de serviços tais como antivírus ou scripts via GPO;

10.2.14. Deverá suportar SCEP (Simple Certificate Enrollment Protocol), assinando petições de certificados digitais assinados (CSR), automaticamente ou manualmente;

10.2.15. Deverá permitir a criação de grupos de usuários, que poderão ser utilizados na autenticação dos dispositivos conforme necessidade;

10.2.16. Deverá permitir que a geração dos usuários na base de dados local seja feita de forma que o equipamento gere uma senha aleatória e envie automaticamente ao usuário;

10.2.17. Deverá permitir enviar e-mails aos administradores relacionados a reinicialização de senha, aprovação de novos usuários e autenticação de segundo fator (token);

10.2.18. Deverá atuar como autoridade certificadora (CA);

10.2.19. Deverá permitir associar os tokens aos usuários criados localmente na base de dados;

10.2.20. Deverá possibilitar, a critério da CONTRATANTE, a autenticação de dispositivos conhecidos com o mínimo de interação dos usuários através de autenticação por endereço MAC, ou seja, MACs previamente conhecidos, cadastrados e autorizados são automaticamente autenticados pela solução sem necessidade de interação do usuário final (como redigitar usuário e senha);

10.2.21. Deverá permitir, que usuários visitantes, que não possuam uma conta local ou em mídias sociais,

também se autentiquem em uma rede sem fio apropriada, com cadastro rápido, que garanta o mínimo de rastreabilidade, através da validação de endereços de e-mail e/ou números de telefone;

10.2.22. A solução deve suportar a integração com servidor RADIUS remoto;

10.2.23. Deverá prover repositório para autenticação de VPN Site-to-Site através de certificados;

10.2.24. Deverá suportar a gerência centralizada de usuários, em todos os aspectos e recursos disponibilizados pela solução;

10.2.25. Deverá funcionar como servidor RADIUS (Remote Authentication Dial-In User Server), proporcionando autenticação aos dispositivos compatíveis com tal protocolo;

10.2.26. Deverá suportar designação automática de VLANs para usuários, com base em critérios pré- definidos pelo administrador;

10.2.27. Deverá prover um portal web, para o auto registro dos usuários, de forma que ele possa ingressar em um portal e registrar seus dados;

10.2.28. Deverá permitir que o usuário possa recuperar sua senha através de um correio eletrônico ou pergunta de segurança, que poderão ser configuráveis pelo usuário;

10.2.29. Deverá prover capacidade de serviço Single Sign On (SSO), com autenticação transparente (passiva) de usuários em sistemas compatíveis;

10.2.30. Deverá permitir que a solução garanta a geração dos usuários na base de dados local seja feita pelo administrador, que poderá definir uma senha no momento de geração do usuário;

10.2.31. Deverá permitir criar políticas de bloqueio automático de usuários após uma quantidade de falhas de autenticação, evitando assim ataques de força bruta contra o usuário;

10.2.32. Deve suportar o protocolo de verificação online de status de certificado OCSP (Online Certificate Status Protocol) para que se possa fornecer uma lista de certificados revogados (CRL);

10.2.33. Deverá permitir desabilitar um token quando este seja roubado ou extraviado, permitindo sua reativação posterior quando/se for recuperado;

10.2.34. Deverá suportar customização de mensagens padrão em páginas web, como páginas de erro, portais de autenticação, auto registro, reset de senha e outros. Suportar também a inclusão, alteração e remoção de imagens nas páginas sem a necessidade de recursos ou conectividade externa;

10.2.35. Deverá permitir e implementar a integração com servidor LDAP remoto (como Microsoft Active Directory);

10.2.36. Deve ser capaz de integrar-se a um diretório ativo (Windows AD) e poder oferecer a funcionalidade de SSO (Single Sign On), onde se utilizam as mesmas credenciais que o usuário utiliza ao autenticar-se no domínio em seu computador pessoal;

10.2.37. Deverá possuir indicador visual, centralizado, de informações críticas: versão de firmware, consumo de CPU/memória/disco, quantidade de usuários criados e licenciados;

10.2.38. Deverá permitir ao administrador do sistema gerar, assinar e revogar certificados digitais para os usuários;

10.2.39. Ser capaz de importar outros certificados de CA’s assim como a lista de certificados revogados;

10.2.40. Deverá permitir criar e assinar certificados X509 para utilização em servidores HTTPS e SSH, assim como para os clientes de serviços VPN e IPSEC;

10.2.41. Deverá permitir remoção de usuários inativos por bulk (remoção massiva), baseado em critérios definidos;

10.2.42. Deverá suportar a sincronização com dispositivo em hardware de geração de OTP (One Time Password);

10.2.43. Deverá suportar análise de arquivos syslog enviados de fonte remota, para uso pelo serviço de SSO (Single Sign On);

10.2.44. Deverá suportar bypass de autenticação 802.1x para dispositivos não compatíveis, e autenticá-los através de mac address (mac address authentication bypass);

10.2.45. Deverá suportar nativamente (sem redirecionamentos) a integração e autenticação de switches e outros dispositivos compatíveis com o padrão 802.1x;

10.2.46. Deve gerar o CN (Common Name) dos usuários, para a integração com serviços e/ou dispositivos que o requeiram;

10.2.47. Deverá suportar o envio de e-mails atuando como servidor próprio (localhost) ou integrar-se com servidor(es) externo(s) para envio das mensagens aos usuários ou administradores;

10.2.48. Deverá permitir a utilização de mecanismo de autenticação de dois fatores, utilizando aplicativo que gerem códigos a intervalos não superiores a 60 segundos, e com ao menos 6 dígitos (token mobile). O aplicativo deve ser compatível para IOS ou Android que fornece segurança de autenticação forte sem hardware adicional;

10.2.49. Deverá permitir que se configure um perfil de complexidade mínimo para as senhas de todos os usuários que sejam cadastrados na base de dados locais, possibilitando a definição de número mínimo de letras minúsculas, letras maiúsculas, caracteres numéricos e caracteres especiais;

10.2.50. Deverá permitir autenticação de usuários visitantes por método de validação com base em credenciais de mídias sociais: facebook, twitter, linkedin, google+, etc;

10.2.51. Deverá suportar NTP (Network Time Protocol), visando sincronismo com ativos existentes com base em fonte central para fornecimento de hora/data corretos;

10.2.52. Prover os seguintes métodos 802.1x eap: peap (mschapv2), eap-ttls, eap-tls, eap-gtc;

10.2.53. Deverá permitir definir perfis de administradores para a solução, de modo que possa segmentar a responsabilidade dos administradores por tarefas operativas.

10.3. SUPORTE ESPECIALIZADO NA SOLUÇÃO DE SEGURANÇA

10.3.1. É de responsabilidade da CONTRATADA o fornecimento dos serviços de suporte técnico especializado de segundo e terceiro nível para o ambiente contratado, inclusive de forma presencial quando este for necessário para o atendimento dos chamados e/ou normalização do ambiente;

10.3.2. Por suporte técnico de segundo nível, mas não se limitando as seguintes ações a serem executadas pela CONTRATADA quando demandada pela CONTRATANTE:

10.3.2.1. Configuração de “Reports/Messaging”;

10.3.2.2. Configuração e/ou atualização de Usuários;

10.3.2.3. Gerência de “User Account Policies”;

10.3.2.4. Configuração do “Self Service Portal”;

10.3.2.5. Configuração do Guest Portal;

10.3.2.6. Configuração de “Remote Authentication Servers”;

10.3.2.7. Configuração do Single Sign On (SSO);

10.3.2.8. Configuração do RADIUS SSO;

10.3.2.9. Gerência dos Certificados (CA e Local).

10.3.3. Por suporte técnico de terceiro nível, mas não se limitando as seguintes ações a serem executadas pela CONTRATADA quando demandada pela CONTRATANTE:

10.3.3.1. Atualização do serviço do RADIUS;

10.3.3.2. Atualização do serviço do LDAP;

10.3.3.3. Atualização do serviço Oauth;

10.3.3.4. Atualização do SAML SSO;

10.3.3.5. Análise e resolução de problemas através da solução;

10.3.3.6. Tratamento de incidentes junto ao fabricante da solução.

10.3.4. Demais solicitações da CONTRATANTE que se fizerem necessárias nas soluções contratadas devem ser previamente acordadas com a CONTRATADA.

11. LOTE 03 – ITEM 10 – SERVIÇO DE BALANCEAMENTO DE CARGA DE APLICAÇÕES

11.1. REQUISITOS DO CLUSTER E LICENCIAMENTO

11.1.1. O CLUSTER deverá ser composto por 2 (dois) equipamentos;

11.1.2. O equipamento de referência adotado nesta especificação se baseia no modelo FortiADC 300F;

11.1.3. As licenças de uso de software serão adquiridas em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante ou seu representante;

11.1.4. Ao fim do contrato de garantia, a solução deverá estar completamente funcional, capaz de criar, customizar e gerenciar políticas e regras, gerar relatórios, manipular dashboard e entre outras funções necessárias ao manuseio da solução.

11.2. MÍNIMOS DE PERFORMANCE

11.2.1. Throughput de, no mínimo 8 (oito) Gbps para tráfego balanceado na camada 4 e na camada 7;

11.2.2. Deve possuir capacidade mínima de tratar 100.000 (cem mil) conexões por segundo em camada 7;

11.2.3. Deve possuir capacidade de realizar, no mínimo, 4.000 (quatro mil) transações SSL, por segundo, na camada 7, com chaves de 2048 bits;

11.2.4. Deve possuir taxa de transferência SSL mínima de 3 (três) Gbps;

11.2.5. Armazenamento interno de, no mínimo, 1 disco SSD de 120GB;

11.2.6. Deve possuir no mínimo 04 (quatro) interfaces 1GE RJ45;

11.2.7. Deve possuir no mínimo 04 (quatro) interfaces 1GE SFP;

11.2.8. Deve possuir fonte de alimentação bivolt (100/240V);

11.2.9. Capacidade mínima de compressão de tráfego de 6 (seis) Gbps;

11.2.10. Deve suportar, no mínimo 300.000 (trezentas mil) conexões simultâneas em camada 4.

11.3. REQUISITOS MÍNIMOS DE FUNCIONALIDADES

11.3.1. A solução deverá ser entregue em appliance, devendo o equipamento ser instalado em local a ser definido pela CONTRATANTE, devendo estar licenciado e ser compatível para atender os requisitos de performance da solução;

11.3.2. Todos os equipamentos que compõem a solução devem ser entregues com a última versão de software homologada e recomendada pelo fabricante;

11.33.3. Deve permitir a virtualização de serviços através da criação de instâncias virtuais (contextos) independentes de balanceamento de carga de aplicações;

11.3.4. Deve implementar, no mínimo, 10 (vinte) instâncias virtualizadas;

11.3.5. Deve possibilitar a alocação de recursos para cada instância, com base nos seguintes parâmetros:

11.3.6. L4 CPS;

11.3.7. L7 CPS e L7 RPS;

11.3.8. Quantidade de Interfaces de Rede;

11.3.9. Quantidade de largura de banda (Throughput);

11.3.10. SSL CPS e sessões concorrentes.

11.3.11. Deve permitir o gerenciamento completo, individual e independente das instâncias virtualizadas;

11.3.12. Nos casos de criação, edição, exclusão ou falhas de uma instância virtual, a disponibilidade e operação das demais instâncias virtualizadas, não devem ser afetadas;

11.3.13. Deve permitir a definição de níveis de garantia de recursos para as instâncias virtuais, possibilitando a dedicação de recursos para determinados contextos;

11.3.14. Deve permitir a redistribuição dos recursos do equipamento entre instâncias sem que isto afete a disponibilidade ou operação das demais instâncias;

11.3.15. Deve garantir o total isolamento de domínios de segurança, administração, recursos de hardware e de rede entre as instâncias;

11.3.16. Cada instância virtual de balanceamento de carga de aplicações deve possuir:

11.3.17. Tabelas de roteamento isoladas e independentes;

11.3.18. Segurança e isolamento do tráfego de gerenciamento.

11.3.19. Definição de índices e o envio de alertas baseados na taxa de utilização de, no mínimo, os seguintes recursos:

11.3.20. Uso de CPU;

11.3.21. Uso de Memória.

11.3.22. Deve permitir a conexão direta, em ambas as direções, a recursos de backend, ou endereços IPs que estejam em redes roteadas pelo balanceamento de carga de aplicações;

11.3.23. Deve permitir a utilização de endereços IPs duplicados, quando utilizados em instâncias diferentes;

11.3.24. Deve possibilitar a adição, edição ou supressão de mensagens HTTP de retorno aos clientes;

11.3.25. Deve efetuar o redirecionamento de portas e protocolo de comunicação, obrigando o cliente a utilizar um protocolo de comunicação seguro ou possibilitando encaminhamento de comunicação aos recursos de backend em porta TCP/UDP diferente da requisitada pelo cliente;

11.3.26. Deve possibilitar a priorização das transações de tráfego com base em parâmetros de camada 3 à camada 7;

11.3.27. Deve ter a capacidade de criação de automações, para que quando ocorra determinados eventos como de segurança, SLB e sistema possa ser criado uma ação com execução automática;

11.3.28. O equipamento deve possuir aceleradores ou processadores auxiliares específicos para o processamento de tarefas de criptografia;

11.3.29. Deve possuir interface de console para a acesso local à configuração dos equipamentos;

11.3.30. Deve permitir o gerenciamento de todas as suas funcionalidades via CLI (Command Line Interface) e GUI (Graphic User Interface), tanto dos equipamentos quanto das instâncias virtualizadas;

11.3.31. Deve implementar mecanismo de controle de acesso RBAC (Role Based Access Control);

11.3.32. Deve possibilitar a configuração de filtros e definição de protocolos seguros para o acesso às interfaces de gerenciamento físicas ou virtuais;

11.3.33. Deve permitir a definição de, no mínimo, 4 (quatro) diferentes níveis de acesso à interface de gerência, limitando o acesso às configurações, relatórios e logs da solução;

11.3.34. Deve implantar serviços de Autenticação, Autorização e Contabilização (AAA - Authentication, Authorization and Accounting), utilizando os métodos:

11.3.35. Usuário/Senha local;

11.3.36. RADIUS (Remote Authentication Dial-In User Service);

11.3.37. NTLM (NT LAN Manager);

11.3.38. Certificado de cliente.

11.3.39. Permitir integração com o serviço de diretório AD (Active Directory) para identificação de usuários e de grupos de usuários, permitindo maior granularidade por meio de controles e de políticas baseadas em usuários e grupos de usuários;

11.3.40. A integração deve permitir identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários.

11.3.41. Suportar SSO (Single-Sign-On) utilizando:

11.3.42. LDAP (Lightweight Directory Access Protocol);

11.3.43. Kerberos;

11.3.44. SAML 2.0 (Security Assertion Markup Language);

11.3.45. NTLM.

11.3.46. Deve suportar os protocolos SNMPv2c e SNMPv3 (Simple Network Management Protocol) para

coleta de dados de gerenciamento e estatísticas;

11.3.47. Deve estar disponível para download a MIB (Management Information Base) privada dos equipamentos que compõem a solução;

11.3.48. Deve possuir suporte a MIB II (RFC 1213).

11.3.49. Deve ser capaz de efetuar registro (logging) dos comandos executados por determinado usuário e eventuais tentativas não autorizadas de execução de comandos (accounting);

11.3.50. Deve efetuar os registros em log com a informação de data, hora e fuso horário;

11.3.51. Deve ser capaz de enviar logs do sistema através de syslog;

11.3.52. Deve possibilitar gerenciamento out-of-band, via interface de rede específica e independente;

11.3.53. Deve suportar transferência remota para atualização do sistema operacional;

11.3.54. Quando implementada em alta disponibilidade, a solução deve permitir a definição de endereço físico (Mac Address) virtual único para ambos os equipamentos operando em paridade;

11.3.55. Em ambientes de balanceamento ativo/passivo, deve possibilitar o gerenciamento da paridade de balanceamento de carga de aplicações através de endereço VIP (Virtual IP) onde somente o ativo deve responder;

11.3.56. Cada instância virtualizada deve possuir endereços de gerência e VIP específicos;

11.3.57. Deve possibilitar customização da página de autenticação (login page);

11.3.58. Deve implementar de forma nativa mecanismo de monitoramento e detecção de falhas em suas fontes de alimentação;

11.3.59. Deve suportar o protocolo SNTP (Simple Network Time Protocol) e/ou NTP;

11.3.60. Permitir consultas de DNS com resolução de nomes em endereços IPv4 e IPv6;

11.3.61. Dever prover NAT (Network Address Translation), pelo menos nos tipos one-to-one e many-to-one e PAT (Port Address Translation), em modo estático e dinâmico;

11.3.62. Deve prover NAT Bidirecional, de client e server;

11.3.63. Deve permitir a realização de NAT do IP do recurso de backend quando este iniciar uma conexão;

11.3.64. Deve prover tradução stateful de endereços de rede IPv6 para IPv4;

11.3.65. Deve prover tradução estática e stateless de endereços de rede IPv4 para IPv6;

11.3.66. Deve prover DNS64 (Domain Name System);

11.3.68. Deve prover DNSSEC (Domain Name System Security Extensions);

11.3.69. Deve prover DNS Autoritativo;

11.3.70. Deve prover DNS Signing;

11.3.71. Deve prover VRRPv2 (Vitual Router Redundancy Protocol) ou funcionalidade similar de FHRP (First Hop Redundancy Protocol);

11.3.72. Deve prover VXLAN (Virtual Extensible LAN) (RFC 7348).

11.3.73. Implementar Policy Route ou PBR (Policy Based Routing) ou PBF (Policy Based Forwarding);

11.3.74. Implementar listas de controle de acesso (ACLs) de camada 3 e camada 4, nos protocolos IPv4 e IPv6;

11.3.75. Suportar a definição de endereços IPv4 e IPv6 nas interfaces de comunicação;

11.3.76. Suportar, tanto em IPv4 quanto IPv6, a definição de rotas estáticas, rotas estáticas monitoradas e rotas estáticas com peso;

11.3.77. Suportar, OSPFv2 (Open Shortest Path First);

11.3.78. Suportar, BGP v4 (Border Gateway Protocol);

11.3.79. Suportar ICMP e ICMPv6 (Internet Control Message Protocol);

11.3.80. Suportar ARP (Address Resolution Protocol) e GARP (Gratuitous Address Resolution Protocol);

11.3.81. Dever prover Link Aggregation (802.3ad);

11.3.82. Dever prover VLAN (Vitual Local Area Network) (802.1q);

11.3.83. Deve permitir a configuração de ambientes de balanceamento ou alta disponibilidade nos modos ativo/ativo, ativo/passivo;

11.3.84. Permitir a configuração de grupo de balanceamento ou recurso de backend de backup, que deve ser ativado somente em caso de indisponibilidade do grupo ou recurso de backend ativo principal;

11.3.85. Deve ser capaz de balancear links de comunicação e servidores físicos ou virtuais com qualquer especificação de hardware, sistema operacional e tipo de aplicação;

11.3.86. Deve permitir a total flexibilização da quantidade de tráfego encaminhada para cada um dos recursos de backend pertencentes a um mesmo grupo de balanceamento, possibilitando que hardwares com performances diferentes cooperem;

11.3.87. Deve permitir que o VIP (Virtual IP) de um mesmo servidor virtual atenda às requisições em protocolos e portas específicas simultaneamente;

11.3.88. Nos casos de servidores virtuais que atendem simultaneamente diversos protocolos e portas, as requisições devem ser atendidas priorizando os parâmetros de protocolo e porta de comunicação TCP/UDP;

11.3.89. Deve permitir a criação de grupos de recursos de backend que devem compartilhar configurações e parâmetros definidos pelo usuário;

11.3.90. Deve permitir a operação e associação de um mesmo recurso de backend a mais de 1 (um) grupo de balanceamento simultaneamente;

11.3.91. Deve permitir que um mesmo recurso de backend atenda, simultaneamente, requisições em protocolos e portas de comunicação TCP/UDP diferentes;

11.3.92. Deve operar nos seguintes cenários:

11.3.93. Cliente em IPv4 e recurso de backend em IPv4;

11.3.94. Cliente em IPv4 e recurso de backend em IPv6;

11.3.95. Cliente em IPv6 e recurso de backend em IPv4;

11.3.96. Cliente em IPv6 e recurso de backend em IPv6.

11.3.97. Deve suportar os seguintes métodos de balanceamento de carga:

11.3.98. ROUND ROBIN: Deve encaminhar as requisições para os recursos de backend de maneira ordenada e rotacional;

11.3.99. MENOR NÚMERO DE CONEXÕES: Deve encaminhar a requisição para o recurso de backend que estiver atendendo ao menor número de requisições de clientes;

11.3.100. MENOR TEMPO DE RESPOSTA: Deve encaminhar a requisição para o recurso de backend com o tempo de resposta mais rápido;

11.3.101. HASH DE ENDEREÇO IP DE DESTINO: Deve encaminhar as requisições para o recurso de backend baseado no hash de IP de destino.

11.3.102. Deve efetuar técnicas de SSL Offloading, possibilitando os processos de criptografia e de- criptografia, ou vice-versa, do tráfego entre clientes e servidores;

11.3.103. Deve permitir a utilização de Certificados Digitais assinados por Autoridades Certificadoras distintas para servidores virtuais e seus recursos de backend;

11.3.104. Deve suportar MTLS (Mutual Transport Layer Security);

11.3.105. Deve suportar a especificação de protocolo e portas de comunicação, limitando a comunicação aceita para determinados servidores virtuais;

11.3.106. Deve suportar a criação de servidores virtuais que aceitem requisições de qualquer protocolo e/ou porta de comunicação na conexão do cliente;

11.3.107. Deve suportar as versões 1.0, 1.1 e 2.0 do protocolo HTTP (Hyper Text Transfer Protocol), com suas respectivas especificidades e funcionalidades, provendo características de content filter, caching, compression, redirecionamento de URL (Uniform Resource Locator);

11.3.108. Deve suportar a criação de políticas baseadas em valores especificados no corpo ou cabeçalho HTTP;

11.3.109. Deve possibilitar uso de Caching tanto para conteúdo estático quanto conteúdo dinâmino;

11.3.110. Deve ser capaz de manter e gerenciar todo o tráfego criptografado com os protocolos SSL 3.0, TLS 1.1, TLS 1.2 e TLS 1.3;

11.3.111. Deve suportar detalhes específicos do protocolo FTP;

11.3.112. Deve possibilitar a definição de persistência de sessão em comunicações de clientes com os recursos de backend, garantindo que, por determinado período, o mesmo servidor receba as requisições de determinado cliente;

11.3.113. Deve possibilitar a utilização da persistência de sessão mesmo para comunicações que utilizem criptografia;

11.3.114. Deve operar com, no mínimo, os protocolos HTTP, HTTPS, TCP, UDP;

11.3.115. Deve operar com os protocolos HTTP e HTTPS;

11.3.116. Deve permitir a customização e operação com, no mínimo, os protocolos HTTP, HTTPS e TCP;

11.3.117. Deve suportar funcionalidade de compressão de HTTP;

11.3.118. Deve possibilitar a compressão de requisições e respostas;

11.3.119. Deve implantar funcionalidades Content Routing, baseando-se, no mínimo, nos seguintes atributos dos pacotes recebidos:

11.3.120. Tipo de dispositivo: Deve identificar o tipo de agente utilizado pelo cliente para posterior definição de encaminhamento;

11.3.121. Linguagem do dispositivo: Deve identificar a língua utilizada pelo agente do cliente para posterior definição de encaminhamento;

11.3.122. Cookie: Deve encaminhar a requisição do cliente baseado em cookie presente no cabeçalho da requisição HTTP;

11.3.123. URL: Deve possibilitar a edição de filtros para bloqueio ou redirecionamento baseado de forma customizável em informações de URL.

11.3.124. Quando efetuado um bloqueio, a solução deve ser capaz de apresentar mensagem personalizável ao usuário;

11.3.125. Deve implantar módulos de controle de resposta (Responder), reescrita (Rewrite) e redirecionamentos (Redirect) personalizados;

11.3.126. Deve efetuar a reescrita do cabeçalho HTTP e elementos de payload baseado em políticas bidirecionais;

11.3.127. Deve possibilitar reescrita no corpo de URL;

11.3.128. Deve criar políticas de redirecionamento baseado nas requisições recebidas;

11.3.129. Deve encaminhar a requisição HTTP baseado no método utilizado;

11.3.130. Deve encaminhar as requisições baseado nos IPs de Origem ou Destino, Porta de Origem ou Destino, ou outras informações presentes nos cabeçalhos TCP ou UDP;

11.3.131. Deve implementar funcionalidade de GSLB (Global Server Load Balancing), levando em consideração:

11.3.132. Status de saúde do site;

11.3.133. Persistência;

11.3.134. Proximidade geográfica;

11.3.135. Número de conexões.

11.3.136. Deve considerar a disponibilidade de um site, utilizando métricas de carga de conexões, probes RTT e taxa de tráfego de pacotes;

11.3.137. Deve possibilitar a definição de 1 (um) ou mais endereços IPs específicos como origem na comunicação com determinados recursos de backend;

11.3.138. Deve suportar o encaminhamento do IP real do cliente ao recurso de backend, seja alterando o IP de ORIGEM do cabeçalho TCP/UDP ou encaminhando através de campo específico de cabeçalho de comunicação;

11.3.139. Deve ser compatível com as diretivas de utilização do cabeçalho X-ForwardedFor;

11.3.140. Deve suportar a utilização de Caching para aplicações com conteúdo estático e dinâmico;

11.3.141. Implementar checagem de métodos HTTP utilizados (GET, POST, HEAD, OPTIONS, PUT,

TRACE, DELETE, CONNECT e PURGE);

11.3.142. Implementar proteção contra técnicas de SQL Injection, bloqueando comandos SQL escondidos em requisições enviadas a base de dados;

11.3.143. Deve implementar proteção contra a lista de técnicas/ataques listados no OWASP TOP 10 (Open Web Application Security Project);

11.3.144. A solução deve ter um sistema de reputação de endereços IP públicos conhecidos como fontes de ataques DDoS, botnets, spammers etc. Tal sistema deve ser atualizado automaticamente;

11.3.145. Deve possibilitar a edição de cabeçalho HTTP, removendo ou alterando informações enviadas ao servidor ou ao cliente;

11.3.146. Deve implementar recursos embarcados de antivírus para análise de arquivos, detecção e bloqueio de malwares que possam comprometer os servidores possuindo integração com a nuvem do fabricante para obter atualizações, enviar e receber amostras de malware para análise/verificação;

11.3.147. Deve implementar recursos de Sandbox para análise de malware moderno;

11.3.148. Implementar proteção contra ataques de Cross-Site Scripting;

11.3.149. Implementar a funcionalidade de Cookie Proxy ou Cookie Encryption;

11.3.150. Deve suportar a criação de políticas por geolocalização, permitindo que o tráfego de determinado país seja bloqueado;

11.3.151. Deve implementar monitores ou mecanismos de health check que, baseado em parâmetros customizáveis, automaticamente, efetue a desativação e/ou reativação dos respectivos recursos de backend;

11.3.152. Os monitores devem ser customizáveis e permitir a utilização de diferentes scripts e protocolos, suportar tanto IPv4 quanto IPv6;

11.3.153. Deve suportar, no mínimo, os seguintes métodos de sondagem dos recursos de backend, seja de forma nativa ou através do uso de monitores personalizados:

11.3.154. Camada 3 – ICMP;

11.3.155. Camada 4 – Teste de porta de comunicação (TCP/UDP) utilizada pelo respectivo serviço/servidor;

11.3.156. Camada 7 – Verificação específica à aplicação, possibilitando a utilização de scripts personalizados e suportando, no mínimo, os protocolos: HTTP, HTTPS, FTP, SMTP, LDAP, POP3, SIP, SNMP;

11.3.157. Permitir a criação de regras e políticas de acesso, customizáveis, de camada 3 (três) e camada 4 (quatro), definidas por:

11.3.158. Protocolo de Transporte (UDP ou TCP);

11.3E.159. ndereço IP, Endereço de sub-rede ou rede de origem;

11.3.160. Porta TCP ou UDP de origem;

11.3.161. Endereço IP, Endereço de sub-rede ou rede de destino;

11.3.162. Porta TCP ou UDP de destino.

11.3.163. A solução deverá atuar diretamente na camada 7 (aplicação) do modelo OSI e ser capaz de interceptar todas as requisições do cliente e as respostas do servidor web;

11.3.164. Deve efetuar a filtragem de conteúdo, bloqueando requisições HTML (Hyper Text Markup Language) inapropriadas aos recursos de backend;

11.3.165. Deve prover funcionalidade que inspecione e monitore todo o tráfego de dados HTTP, até a camada de aplicação, incluindo cabeçalhos, campos de formulários e conteúdo, além de inspecionar os requests e responses;

11.3.166. A solução deve possuir políticas automáticas que bloqueiam endereços IP que realizem violações;

11.3.167. A solução deve permitir liberação (whitelist) de endereços IP que possam ser bloqueados devido violação detectada;

11.3.168. Deve permitir a utilização de modelo positivo e negativo de segurança para proteção contra ataques aos protocolos HTTP e HTTPS, e as aplicações web acessíveis através destes protocolos;

11.3.169. Deve prover modelo de segurança negativo com assinaturas atualizadas automaticamente para proteger contra vulnerabilidades de camada 7 (sete) e protocolo HTTP de aplicações;

11.3.170. Deve possibilitar a definição de expressões regulares para a criação de regras e políticas de segurança;

11.3.171. A solução deve prover as seguintes funcionalidades e capacidades relacionadas a proteção de Web Services XML:

11.3.171.1. . Firewall XML integrado, com suporte a filtros e validação de funções XML específicas da aplicação;

11.3.171.2. xDos (XML Denial of

service); 11.3.171.3. XML SQL Injection;

11.3.171.4. Validação de mensagens XML;

11.3.172. Capacidade de definir e restringir métodos do WebService via definição em WSDL (Web Services Description Language).

11.3.173. Deve possibilitar a integração com ferramentas externas de escaneamento de outros fabricantes;

11.3.174. Deve prevenir a sobrecarga dos recursos de backend, monitorando rajadas e ajustando a taxa de encaminhamento das conexões e requisições para todos ou determinado recurso de backend;

11.3.175. Implementar proteção contra ataques DoS (Denial of Service) e SYN Flood;

11.3.176. Implementar SYN Cookie;

11.3.177. Deve possibilitar a utilização de limites e controle de resposta para requisições de ICMP e UDP;

11.3.178. proteger contra os ataques de força bruta que explorem:

11.3.178.1. Controles de acesso da aplicação;

11.3.178.1.2. Solicitações repetidas ao mesmo recurso, em qualquer parte/URL da aplicação;

11.3.178.3. Deve proteger contra os ataques de força bruta especificados acima, mantendo a continuidade do atendimento aos usuários legítimos;

11.3.179. Aplicações web que não retornam o erro 401 por meio da identificação de expressão regular no retorno/página de erro da aplicação;

11.3.180. Gerenciamento de sessão (muitas sessões de um único endereço IP ou a um range de IPs);

11.3.181. Clientes automatizados (robôs, requisições muito rápidas);

11.3.182. Deve possibilitar a criptografia fim-a-fim, entre cliente e recursos de backend;

11.3.183. Deve armazenar, de forma segura, arquivos de segurança como certificados digitais e chaves criptográficas;

11.3.184. Deve possibilitar a geração de chaves RSA (Rivest-Shamir-Adleman) e ECDSA (Elliptic Curve Digital Signature Algorithm);

11.3.185. Deve gerar chaves criptográficas RSA de, no mínimo, 2048 bits;

11.3.186. Deve implementar o algoritmo de hash SHA-256;

11.3.187. Deve permitir a importação e exportação de chaves, certificados de servidores, e checagem de lista de certificados revogados;

11.3.189. Deve possibilitar a criação de CSR (Certificate Signing Request) para a assinatura de Certificados Digitais;

11.3.190. Deve permitir a definição de CN (Commom Name);

11.3.191. Deve permitir a integração com solução de HSM (Hardware Security Module);

11.3.192. Permitir a identificação de usuários através de leitura do campo "X-ForwardedFor", registrando nos logs do firewall o endereço IP, bem como o usuário de rede responsável pelo acesso;

11.3.193. Deve possuir serviço que entrega, continuamente, lista atualizada de endereços IPs maliciosos.

11.4. SUPORTE ESPECIALIZADO NA SOLUÇÃO DE SEGURANÇA

11.4.1. É de responsabilidade da CONTRATADA o fornecimento dos serviços de suporte técnico especializado de segundo e terceiro nível para o ambiente contratado, inclusive de forma presencial quando este for necessário para o atendimento dos chamados e/ou normalização do ambiente;

11.4.2. Por suporte técnico de segundo nível, mas não se limitando as seguintes ações a serem executadas pela CONTRATADA quando demandada pela CONTRATANTE:

11.4.2.1. Gerência da solução;

11.4.2.2. Configuração de serviços associados a solução (Virtual Server, Real Server e Health Check);

11.4.2.3. Análise e resolução de problemas relacionados a solução.

11.4.3. Por suporte técnico de terceiro nível, mas não se limitando as seguintes ações a serem executadas pela CONTRATADA quando demandada pela CONTRATANTE:

11.4.3.1. Análise e resolução de problemas via CLI;

11.4.3.2. Aprovação de novas métricas para o Health Check;

11.4.3.3. Tratamento de incidentes junto ao fabricante da solução;

11.4.3.4. Tratamento de RMA junto ao fabricante da solução.

11.4.4. Demais solicitações da CONTRATANTE que se fizerem necessárias nas soluções contratadas devem ser previamente acordadas com a CONTRATADA.

12. LOTE 03 – ITEM 11 – SERVIÇO DE CONECTIVIDADE WIFI

12.1. CARACTERÍSTICAS GERAIS

12.1.1. O equipamento de referência adotado nesta especificação se baseia no modelo FortiAP 231F;

12.1.2. Deve permitir a conexão de dispositivos wireless que implementem os padrões IEEE 802.11a/b/g/n/ac/ax de forma simultânea;

12.1.3. Deve possuir capacidade dual-band com rádios 2.4GHz e 5GHz operando simultaneamente, além de permitir configurações independentes para cada rádio;

12.1.4. O ponto de acesso deve possuir rádio WIFI dedicado para executar funções de sensor com objetivo de identificar interferências e ameaças de segurança em tempo real e com operação 24x7;

12.1.5. Deve possuir rádio BLE (Bluetooth Low Energy) integrado e interno ao equipamento;

12.1.6. Deve permitir a conexão de 400 (quatrocentos) clientes wireless simultaneamente;

12.1.7. Deve possuir 2 (duas) interfaces Ethernet padrão 10/100/1000Base-T com conector RJ-45 para permitir a conexão com a rede LAN;

12.1.8. Deve implementar link aggregation de acordo com o padrão IEEE 802.3ad;

12.1.9. Deve possuir interface console para gerenciamento local com conexão serial padrão RS-232 e conector RJ45 ou USB;

12.1.10. Deve permitir sua alimentação através de Power Over Ethernet (PoE) conforme os padrões 802.3af ou 802.3at. Adicionalmente deve possuir entrada de alimentação 12VDC;

12.1.11. Deve permitir operação em modo Mesh;

12.1.12. Deve possuir potência de irradiação mínima de 21dBm em ambas as frequências;

12.1.13. Deve suportar, no mínimo, operação MIMO 2x2 com 2 fluxos espaciais permitindo data rates de até 1200 Mbps em um único rádio;

12.1.14. Deve suportar modulação de até 1024 QAM para os rádios que operam em 2.4 e 5GHz servindo clientes wireless 802.11ax;

12.1.15. Deve possuir sensibilidade mínima de -94dBm quando operando em 5GHz com MCS0 (HT20);

12.1.16. Deve possuir antenas internas ao equipamento com ganho mínimo de 4dBi em 2.4GHz e 5GHz;

12.1.17. Deve ser capaz de operar em ambientes com temperaturas entre 0 e 45º C;

12.1.18. Deve possuir sistema antifurto do tipo Kensington Security Lock ou similar;

12.1.19. Deve possuir indicadores luminosos (LED) para indicação de status;

12.1.20. Deve permitir a conexão de dispositivos wireless que implementem os padrões IEEE 802.11a/b/g/n/ac/ax e IEEE P80.11be;

12.1.21. Deve permitir a conexão de dispositivos wireless que transmitam tráfego IPv4 e IPv6;

12.1.22. A solução deve implementar recursos que possibilitem a identificação de interferências provenientes de equipamentos que operem nas frequências de 2.4GHz, 5GHz e 6GHz;

12.1.23. A solução deve implementar recursos de análise de espectro que possibilitem a identificação de interferências provenientes de equipamentos não WIFI e que operem nas frequências de

2.4GHz, 5GHz ou

6GHz. A solução deve ainda apresentar o resultado dessas análises de maneira gráfica na interface de gerência;

12.1.24. A solução deve permitir o balanceamento de carga dos usuários conectados à infraestrutura wireless de forma automática. A distribuição dos usuários entre os pontos de acesso próximos deve ocorrer sem intervenção humana e baseada em critérios como número de dispositivos associados em cada ponto de acesso;

12.1.25. A solução deve permitir o agrupamento de VLANs para que sejam distribuídas múltiplas sub redes em um determinado SSID, reduzindo assim o broadcast e aumentando a disponibilidade de endereços IP;

12.1.26. A solução deve permitir a criação de múltiplos domínios de mobilidade (SSID) com configurações distintas de segurança e rede. Deve ser possível especificar em quais pontos de acesso ou grupos de pontos de acesso que cada domínio será habilitado;

12.1.27. A solução deve permitir ao administrador da rede determinar os horários e dias da semana que as redes (SSIDs) estarão disponíveis aos usuários;

12.1.28. Deve permitir restringir o número máximo de dispositivos conectados por ponto de acesso e por rádio;

12.1.29. A solução deve implementar o padrão IEEE 802.11r para acelerar o processo de roaming dos dispositivos através do recurso conhecido como Fast Roaming;

12.1.30. A solução deve implementar o padrão IEEE 802.11k para permitir que um dispositivo conectado à rede wireless identifique rapidamente outros pontos de acesso disponíveis em sua área para que ele execute o roaming;

12.1.31. A solução deve implementar o padrão IEEE 802.11v para permitir que a rede influencie as decisões de roaming do cliente conectado através do fornecimento de informações complementares, tal como a carga de utilização dos pontos de acesso que estão próximos;

12.1.32. A solução deve implementar o padrão IEEE 802.11w para prevenir ataques à infraestrutura wireless;

12.1.33. A solução deve suportar priorização via WMM e permitir a tradução dos valores para DSCP quando os pacotes forem destinados à rede cabeada;

12.1.34. A solução deve apresentar informações sobre os dispositivos conectados à infraestrutura wireless e informar ao menos as seguintes informações: nome do usuário conectado ao dispositivo, fabricante e sistema operacional do dispositivo, Endereço IP, SSID ao qual está conectado, ponto de acesso ao qual está conectado, canal ao qual está conectado, banda transmitida e recebida (em Kbps), intensidade do sinal considerando o ruído em dB (SNR), capacidade MIMO e horário da associação;

12.1.35. Para garantir uma melhor distribuição de dispositivos entre as frequências disponíveis e resultar em melhorias na utilização da radiofrequência, a solução deve ser capaz de distribuir automaticamente os dispositivos dual-band para que conectem primariamente em 5GHz através do recurso conhecido como Band Steering;

12.1.36. A solução deve permitir a configuração de quais data rates estarão ativos na ferramenta e quais serão desabilitados;

12.1.37. A solução deve suportar recurso para automaticamente desconectar clientes wireless que estejam com sinal fraco ou distantes. Deve permitir definir o limiar de sinal para que os clientes sejam desconectados;

12.1.38. A solução deve registrar todos os logs de eventos com bloqueios e liberações das aplicações que foram acessadas na rede wireless;

12.1.39. A solução deve implementar mecanismos de proteção para identificar ataques à infraestrutura wireless. Ao menos os seguintes ataques devem ser identificados:

12.1.39. Ataques de flood contra o protocolo EAPOL (EAPOL Flooding);

12.1.40. Association Flood;

12.1.41. Authentication Flood;

12.1.42. Broadcast Deauthentication;

12.1.43. Spoofed Deauthentication;

12.1.44. ASLEAP;

12.1.45. Null Probe Response or Null SSID Probe Response;

12.1.46. Long Duration;

12.1.47. Ataques contra Wireless Bridges;

12.1.48. Weak WEP;

12.1.49. Invalid MAC OUI.

12.1.50. A solução deve implementar mecanismos de proteção para mitigar ataques à infraestrutura wireless. Ao menos ataques de negação de serviço devem ser mitigados pela infraestrutura através do envio de pacotes de deauthentication;

12.1.51. A solução deve implementar mecanismos de proteção contra ataques do tipo ARP Poisoning na rede wireless;

12.1.52. Permitir configurar o bloqueio na comunicação entre os clientes wireless conectados a um determinado SSID;

12.1.53. Em conjunto com os pontos de acesso, a solução deve implementar os seguintes métodos de autenticação: WPA (TKIP) e WPA2 (AES);

12.1.54. Em conjunto com os pontos de acesso, a solução deve ser compatível e implementar o método de autenticação WPA3;

12.1.55. A solução deve permitir a configuração de múltiplas chaves de autenticação PSK para utilização em um determinado SSID;

12.1.56. Quando usando o recurso de múltiplas chaves PSK, a solução deve permitir a definição de limite quanto ao número de conexões simultâneas para cada chave criada;

12.1.57. A solução deve implementar o protocolo IEEE 802.1X com associação dinâmica de VLANs para os usuários com base nos atributos fornecidos pelos servidores RADIUS;

12.1.58. A solução deve implementar o mecanismo de mudança de autorização dinâmica para 802.1X, conhecido como RADIUS CoA (Change of Authorization) para autenticações 802.1X;

12.1.59. Em conjunto com os pontos de acesso, a solução deve suportar os seguintes métodos de autenticação EAP: EAP-AKA, EAP-SIM, EAP-FAST, EAP-TLS, EAP-TTLS e PEAP;

12.1.60. A solução deve implementar recurso para autenticação dos usuários através de página web HTTPS, também conhecido como captive portal. A solução deve limitar o acesso dos usuários enquanto estes não informarem as credenciais válidas para acesso à rede;

12.1.61. A solução deve permitir a customização da página de autenticação, de forma que o administrador de rede seja capaz de alterar o código HTML da página web formatando texto e inserindo imagens;

12.1.62. A solução deve permitir a coleta de endereço de e-mail dos usuários como método de autorização para ingresso à rede;

12.1.63. A solução deve permitir que a página de autenticação seja hospedada em servidor externo;

12.1.64. A solução deve permitir a configuração do captive portal com endereço IPv6;

12.1.65. A solução deve permitir o cadastramento de contas para usuários visitantes na memória interna. A solução deve permitir ainda que seja definido um prazo de validade para a conta criada;

12.1.66. A solução deve possuir interface gráfica para administração e gerenciamento das contas de usuários visitantes, não permitindo acesso às demais funções de administração da solução;

12.1.67. Após a criação de um usuário visitante, a solução deve enviar as credenciais por e-mail para o usuário cadastrado;

12.1.68. A solução deve implementar recurso de DHCP Server (em IPv4 e IPv6) para facilitar a configuração de redes visitantes;

12.1.69. A solução deve identificar automaticamente o tipo de equipamento e sistema operacional utilizado pelo dispositivo conectado à rede wireless;

12.1.70. A solução deve permitir a configuração de redes mesh entre os pontos de acesso;

12.1.71. A solução deve possuir recurso para realizar testes de conectividade nos pontos de acesso a fim de validar se as VLAN estão apropriadamente configuradas no equipamento ao qual os pontos de acesso estejam fisicamente conectados;

12.1.72. A solução deve apresentar graficamente a topologia lógica da rede, representar os elementos da rede gerenciados, além de informações sobre os usuários conectados com a quantidade de dados transmitidos e recebidos por eles;

12.1.73. A solução deve permitir a identificação do firmware utilizado por cada ponto de acesso gerenciado e permitir a atualização via interface gráfica;

12.1.74. A solução deve permitir a atualização de firmware individualmente nos pontos de acesso, garantindo a gestão e operação simultânea de pontos de acesso com firmwares diferentes;

12.1.75. A solução deve enviar e-mail de notificação aos administradores da rede em caso de evento de indisponibilidade de um ponto de acesso;

12.1.76. A solução ofertada deve possuir recursos para onboard seguro de dispositivos wireless, baseando-se em atributos dos elementos, tais como: usuários, mac address, tipo, família, SO, hardware e fabricante, dentro outros;

12.1.77. Uma vez que seja um dispositivo reconhecido, ele deve ser colocado na respectiva VLAN. Do contrário, permanecerá em uma VLAN isolada.

Rio Branco-AC, 25 de janeiro de 2024.

Documento assinado eletronicamente por **Elson Correia de Oliveira Neto** , **Gerente**, em 05/02/2024, às 15:29, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **Amilar Sales Alves**, **Supervisor(a) Administrativo(a)**, em 05/02/2024, às 17:20, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **Raquel Cunha da Conceicao** , **Diretora**, em 06/02/2024, às 07:13, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.tjac.jus.br/verifica informando o código verificador **1687495** e o código CRC **77DDF05A**.

Assinado eletronicamente por **AMILAR SALES ALVES**, **Técnico Judiciário**, em 19/04/2024 11:10:31
Assinado eletronicamente por **ELSON CORREIA DE OLIVEIRA NETO**, **Gerente de Segurança da Informação**, em 19/04/2024 11:09:14