CONSULTA PÚBLICA SEGER Nº 001/2020

Trata-se de questionamentos e sugestões ao Termo de Referência, cujo objeto é o Registro de Preços para serviços de telecomunicações necessários à implantação, operação, manutenção e gerenciamento de uma rede IP multisserviços, incluindo todos os serviços, materiais e equipamentos necessários à conexão entre os pontos de acesso previstos.

EMPRESA: ALTERNA TELECOMUNICAÇÕES E CONECTIVIDADE LTDA

Sugestão 1) Considerando que o Governo através do Prodest vem ampliando a extensão de sua rede não é de bom modo que se faça uma contratação com a expectativa de 60 meses, isto gera expectativa falsa no custo do projeto para o momento das licitantes formarem suas propostas e depois de contratado, ainda cria um entrave administrativo para os órgãos contratantes da ata de registro de preços formada, pois, estes, após já terem seus contratos celebrados, muitas vezes querem forçar que sejam aceitos cancelamentos quando já se ultrapassou o limite de 25%, ao qual o contratado está obrigado a aceitar. Nossa sugestão é que se faça uma contratação para 24 meses com possibilidade de renovações até o limite de 60 meses.

Resposta: O prazo contratual será alterado para 24 meses renovável até 60 meses.

Sugestão 2) O item 3.4.6 prevê que a contratante tem até 10 dias para realizar os testes e dar o aceite da ativação, contudo, o item 3.4.7 fixa que a data de início de faturamento será a data do aceite. A experiência nos mostra que muitas vezes o contratante não tem pessoal suficiente para realizar os testes de aceite e estes costumam perdurar por mais que 10 dias, não sendo justo que este custo da espera pelo aceite recaia sobre o fornecedor. Assim, sugerimos que a data do início do faturamento seja a data da entrega do link de dados pela contratada, salvo, se houver apontamento de outra data pelo fiscal. Caso este de apontamento que seria feito numa eventual exceção onde um link entregue venha a apresentar problema durante a sua validação.

Resposta: Sugestão não acatada.

Sugestão 3) Os itens 3.6.7, 3.6.8 e 3.6.9 falam sobre a quantidade de “localidades” a serem instaladas, todavia, o conceito de localidade causa dúvidas de entendimento, pois pode ser confundido 2 com localidade = cidade, ou localidade = site ou ponto de instalação. Assim, sugerimos rever o texto de forma que o conceito não fique ambíguo. Que seja descrito como parâmetro a quantidade de pontos de instalação a ser executados.

Resposta: O termo será ajustado para refletir o entendimento correto de “ponto de acesso”.

Sugestão 4) Os itens 3.6.10 e 3.7.7 prevê que no caso de não atendimento ao prazo de instalação deverá ser concedido um desconto de 5% sobre o valor da instalação. Este tipo de aplicação de penalidade pode vir a se tornar inócuo quando a contratada ofertar o serviço com taxa de instalação zero. Assim, para evitar que se perca a efetividade desta penalidade seria prudente que o desconto fosse exigido sobre o valor mensal do link de serviço a ser instalado.

Resposta: Será modificado o texto para incluir desconto no valor mensal do link.

Sugestão 5) O item 3.7.5 prevê que o valor do serviço de remanejamento deve ser menor ou igual ao serviço de instalação de novo circuito. Conforme o próprio conceito já explica nos itens anteriores o serviço de remanejamento é maior ou mais amplo, que o serviço de instalação, pois, naquele existe toda a instalação a ser feita e ainda existe os outros custos referentes a retirada do link do outro endereço. Desta forma não se torna coerente que seja imposta tal limitação de que o valor do remanejamento deva ser igual ou menor a instalação. Sugerimos que seja retirado essa imposição do item 3.7.5 e que seja feito uma distinção entre serviço de remanejamento interno e remanejamento externo. Para o remanejamento interno sim deve ser um valor menor ou igual a instalação, todavia para o remanejamento externo não.

Resposta: Sugestão não acatada.

Sugestão 6) Nos itens 11.7.1 e 11.7.2 falta escrever a palavra “dias” após o numeral 5.

Resposta: Texto será revisado.

Sugestão 7) Quanto ao procedimento a ser adotado com esta nova formatação pretendida no item 11 do termo de referência para que a contratada não emita a nota fiscal junto com os relatórios já no início do mês (entre os dias 1 e 3), concedendo inicialmente um prazo de 5 dias para o fiscal analisar os relatórios e só depois disso ser autorizado pelo fiscal para a emissão da nota fiscal, irá impactar demais no prazo de recebimento dos serviços. A experiência da forma como é praticado hoje, onde o fiscal já recebe junto com os relatórios a nota fiscal, o processo já se atraso na maioria dos órgãos, que não conseguem concluir o pagamento dentro dos prazos, e a se adotar a nova modalidade pretendida, passará a ter dois gargalos, o primeiro pelo fiscal que poderá estar sem tempo de analisar os relatórios e emitir a aprovação dentro do prazo de 5 dias para que a contratada possa emitir a nota fiscal, 3 provocando assim uma espera para se emitir a nota fiscal e depois ainda haverá uma nova contagem de tempo para o fiscal montar o processo e encaminhar para pagamento. Tal medida, se adotada irá impactar nos custos dos serviços prestados, onde o prestador já deverá incluir nos seus custos uma previsão de recebimento em prazos maiores. Assim, pedimos que seja reconsiderado tal condição, e que seja facultado a emissão conjunta dos relatórios com a nota fiscal e caso seja identificado algum erro no relatório que sejam devolvidos relatórios e a nota fiscal/fatura, e no caso que esteja tudo certo e aprovado o fiscal já poderá seguir o processo e não provocar um ponto de atraso para o pagamento.

Resposta: Sugestão não acatada.

Sugestão 8) O modelo adotado de partição em lotes de 3 áreas distintas (norte, sul e metropolitano) e considerando a grande capilaridade da rede própria do Prodest, pode deixar os lotes da região metropolitana sem competitividade e sem atratividade, pois é sabido que quase todos os órgãos tem migrado seus serviços para a rede do Prodest e já vem desativando os links contratados na Rede ES. Desta forma como forma de aumentar a sua atratividade seria importante colocar algumas das cidades vizinhas para serem atendidas por estes lotes metropolitanos. Por exemplo, cidades como Aracruz, Domingos Martins, Anchieta, ou seja, buscar uma ou outra cidade próxima para aumentar o volume de contratação no lote.

Resposta: Sugestão não acatada.

Sugestão 9) Muito importante que não volte a ocorrer casos tipo da Rede ES 2, onde se incluiu uma grande demanda fictícia, que depois acabou por não ser contratado nada, como, por exemplo, SEDU na região metropolitana. Citamos este exemplo, pois, é necessário que seja definido uma política de Estado quanto a se contratar ou não um link na Rede ES, para locais onde se tem a rede própria do Prodest, para evitar de surgir demanda que não se concretizará em contratação futura.

Respostas: As demandas serão respondidas por cada órgão partícipe da ARP.

EMPRESA: TELEMAR NORTE LESTE S.A. - OI

Sugestão 1) Considerando que o Jitter ocorre em momentos distintos, quando existem volumes menores ou maiores de pacotes para serem transmitidos, ocasionando redução ou aumento do retardo devido às filas internas dos dispositivos de rede, sugerimos que a Contratante exija um baixo retardo, porém variando a mesma por Classes de Serviços (CoS) conforme exemplo/valores abaixo citados:

Classe (CoS)	Perda de Pacotes
Voz	20ms
Vídeo	30ms
Prioritários	30ms
Críticos	30ms
Convencionais	30ms

Resposta: Sugestão não acatada.

Sugestão 2) Considerando que a especificação do SLA de disponibilidade mínima deve ter relação com o SLA de tempo de reparo, pois da forma que está sendo especificado

o SLA de disponibilidade, no caso de se ocorrer apenas um reparo por mês com duração de 4 horas para qualquer um dos circuitos da Grande Vitória citados neste termo de referência, já estaria infringindo o SLA, pois restaria uma disponibilidade por acesso de 99,44%, o que torna impossível manter essa taxa de disponibilidade TELEMAR NORTE LESTE S.A. Rua Lavradio, 71- Centro - Rio de Janeiro - Rio de Janeiro CEP: 22.230-070 CNPJ/MF: 33.000.118/0001-79 Inscrição Estadual: 81.680.469 Telefone: 0800 31 80 31 - Fax: (31) 3229-2715 Inscrição Municipal: 0038.534-4 de 99,5%. Ainda considerando que a dispersão e a capilaridade que tem dos diversos circuitos da rede de dados dentro dos referidos lotes e a suscetibilidade das mesmas que eventualmente podem ser acometida por eventos de vulto de terceiros, lembrando que a Contratante estará contratando Lotes Primários e Lotes Secundários atendimento da mesma demanda. Dado ao aqui exposto e o nosso entendimento, sugerimos a alteração deste SLA de Disponibilidade para 99,4% para todos os links de fora e também da Região Metropolitana com exceção do link de Conexão entre o Datacenter e a Rede, link este que sugerimos alterar o SLA para 99,90% já que para o mesmo está sendo solicitada uma redundância total do circuito.

Resposta: Sugestão não acatada.

Sugestão 3) Alterar a interface de 10GBASE-SR para 10GBASE-T evitando a contratação de Transceivers/SDH especificamente para esta abordagem no site. A entrega do link na condição técnica do Termo de Referência implica na contratação de parceiros ou altos investimentos específicos para abordagem do site, contratações estas que aumentarão significativamente o preço final a ser apresentado no certame.

Resposta: Sugestão não acatada.

Sugestão 4) Devido à complexidade técnica da solução solicitada pelo CONTRATANTE, e a quantidade de pontos envolvidos no projeto, uma vez que vários pontos necessitarão de projeto especial para serem atendidos, solicitamos uma flexibilização do prazo de instalação da seguinte forma: Prazo de ativação de até 60 (sessenta) dias para 70% dos pontos e de até 90 (noventa) dias para 30% dos pontos restantes. Contados após a disponibilização por parte da contratante, dos requisitos mínimos de infraestrutura exigidos, quando for o caso, a serem indicados pela CONTRATADA. TELEMAR NORTE LESTE S.A. Rua Lavradio, 71- Centro - Rio de Janeiro - Rio de Janeiro CEP: 22.230-070 CNPJ/MF: 33.000.118/0001-79 Inscrição Estadual: 81.680.469 Telefone: 0800 31 80 31 - Fax: (31) 3229-2715 Inscrição Municipal: 0038.534-4 O remanejamento externo de um link também é considerado como uma nova instalação, sendo assim sugerimos alterar o prazo para até 60 dias, prazo este igual o prazo de ativação.

Resposta: Prazo para remanejamento será alterado para 60 dias.

Sugestão 5) Sugerimos retirar este item, dado que não podemos efetuar serviços de galeria interna ou tubulação dos clientes, já que os mesmos não fazem parte da outorga de SCM.

Resposta: Sugestão não acatada.

Sugestão 6) Considerando que a conexão da Interface do CPE ao bastidor da Contratante deverá sempre ser efetuada pela mesma, levando em conta os padrões de segurança do cliente e a especificação técnica destes cabeamentos, sugerimos retirar este item deste Termo de Referência assim como também o mesmo citado no item 3.6.1

Resposta: Sugestão não acatada.

Sugestão 7) Considerando que o Estado do Espírito Santo possui 78 municípios, sendo que 7 deles compõem a região metropolitana da Grande Vitória, restando outros 71 munícipios, dos quais 4 são grandes cidades do interior, a saber: Colatina, São Mateus, Linhares e Cachoeiro. Tanto na região metropolitana quanto nestas 4 grandes cidades, a Oi e provavelmente os demais TELEMAR NORTE LESTE S.A. Rua Lavradio, 71- Centro - Rio de Janeiro - Rio de Janeiro CEP: 22.230-070 CNPJ/MF: 33.000.118/0001-79 Inscrição Estadual: 81.680.469 Telefone: 0800 31 80 31 - Fax: (31) 3229-2715 Inscrição Municipal: 0038.534-4 participantes desta licitação possuem equipes de manutenção residentes nestas localidades. Para os demais 67 municípios, os atendimentos dos serviços de reparos ocorrerão de maneira remota, ou seja, sempre que houver um chamado será deslocado um técnico, e com isso deve-se fazer consideração de um tempo médio de deslocamento de 2 horas para quaisquer destas localidades com atendimento remoto, sendo assim sugerimos um prazo de reparo de 4 horas na região metropolitana da Grande Vitória, e de 6 horas para as demais localidades.

Resposta: Sugestão não acatada.

Sugestão 8) A topologia citada na “figura 3 – Conexão de entrada no Datacenter”, demonstra que deverão ser entregues 2(duas) fibras em 2(dois) cpe´s distintos, porém restam as seguintes dúvidas a saber neste item:

a) O atendimento deverá ser efetuado também por estações/rotas distintas de fibra?

Resposta: Sim, as rotas de fibras para entrada no Data Center devem ser distintas. O Termo de Referência será ajustado.

b) Os links deverão ser configurados inicialmente como 10Gbps?

Resposta: Sim.

c) Estes links estão sendo citados/cotados na planilha de preços de cada lote?

Resposta: O valor deste link compõe o custo dos demais links.

Ainda, sugerimos implementação de soluções de segurança de rede, detalhadas abaixo:

Sugestão 1) SOLUÇÃO ANT-DDoS

1.1. Acesso corporativo exclusivo e dedicado à Internet;

1.2. A CONTRATADA deverá prover saída de Internet internacional que não utilize outras operadoras brasileiras como transito IP.

1.3. Implementação de acesso do NOME_CLIENTE à rede Internet, de forma dedicada, exclusiva, através de acesso Gigabit Ethernet, com garantia integral de banda, na velocidade de, no mínimo, XX Mbps (XX megabits por segundo) simétrico;

1.4. Para proteção deste acesso corporativo, 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);

1.4.1. 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.

1.4.2. 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.

1.4.3. A CONTRATADA deve possuir e disponibilizar no mínimo 2 (dois) centros de limpeza nacional cada um com capacidade de mitigação de no mínimo 40Gbps e no mínimo 1 (um) centro de limpeza internacional com capacidade de mitigação de no mínimo 200Gbps.

1.4.4. Não haverá taxa adicional por volume de mitigação de ataques (DDoS – Distributed Denial of Service) nos IP's monitorados.

1.4.5. 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 autorizados pelo NOME_CLIENTE.

1.4.6. O ataque deve ser mitigado separando o tráfego legítimo do malicioso, de modo que os serviços de Internet providos pelo cliente continuem disponíveis.

1.4.7. 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.

1.4.8. 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.

1.4.9. 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 do mesmo.

1.4.10. 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 (conforme item 2.4.3 cada centro nacional deve possuir capacidade de mitigação de no mínimo 40 Gbps 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.

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

1.4.12. Nos períodos de ataque a latência do circuito deverá ser de no máximo 100 ms (milissegundos) quando a mitigação se originar dos centros de limpeza nacionais e de no máximo 250 ms (milissegundos) quando se originar do(s) centro(s) internacionais.

1.4.13. 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.

1.4.14. 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.

1.4.15. 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.

1.4.16. A solução não poderá desviar o tráfego para empresas fora do Brasil.

1.4.17. A solução de mitigação de ataques volumétricos na nuvem da operadora deverá atuar com desvio de rotas via BGP para o host que está sendo atacado /32.

1.4.18. 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 de tempo considerado seguro por um determinado cliente.

1.4.19. A solução deve suportar a mitigação automática de ataques, utilizando múltiplas técnicas como White Lists, Black Lists, 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.

1.4.20. 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:

- 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);

1.4.21. Em nenhum caso será aceito bloqueio de ataques de DOS e DDOS por ACLs em roteadores de bordas da contratada.

1.4.22. 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.

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

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

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

1.4.26. 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 poderão ser disponibilizados em até 48 horas após um ataque mediante solicitação da CONTRATANTE.

1.4.27. Em nenhum caso será aceito bloqueio de ataques de DOS e DDOS por ACLs em roteadores de bordas da contratada.

1.4.28. 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).

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

1.4.30. A CONTRATADA deverá disponibilizar 02 (DOIS) Centros Operacional de Segurança no Brasil, com no mínimo 2 (dois) profissionais certificados na solução de AntiDDoS, responsável pelo monitoramento,

detecção e mitigação de ataques, em idioma português brasileiro, durante as 24 (vinte e quatro) horas do dia, nos 7 (sete) dias da semana, no período de vigência contratual.

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

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

1.4.33. 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.

1.4.34. A CONTRATADA deverá disponibilizar um dashboard on line e uma solução de monitoração e gerenciamento o qual deverá oferecer uma análise do comportamento dos circuitos, identificar de forma eficiente os impactos gerados na rede. Permitindo o acompanhamento em tempo real em relação aos ataques em andamento e ataques bloqueados classificados por severidade. Além da visão em real time, também deverá ser permitida também a consulta histórica dos ataques orientados ao ambiente. Devendo ser disponibilizado indicador em tempo real relacionado a quantidade de ataques em andamento, bloqueados e não bloqueados.

Sugestão 2) SOLUÇÃO DE PROTEÇÃO DNS

2.1. Para evitar ameaças avançadas que consideram capacidade analítica em tempo real para identificar comportamento malicioso e atividade botnet em dispositivos dentro e fora da rede, a CONTRATADA deverá entregar uma solução de proteção na camada de DNS como uma primeira linha de defesa e proteção contra ameaças da Internet, além de fornecer visibilidade em tempo real das atividades de Internet. Assim, NOME_CLIENTE alcançara os resultados desejados:

- Mitigar custos de remediação e quebras de segurança em tempo real;
- Reduzir o tempo para detectar e conter ameaças;
- Aumento de visibilidade e atividade internet em diversas localidades e usuários;
- Ganhar visibilidade sobre usuários e aplicações em uso.

2.2. A solução deverá implementar uma camada adicional de inteligência e prevenção contra ameaças avançadas que atua durante o processo de resolução de nomes para endereços IP (DNS) e segurança de conteúdo. Fornecendo, através de análise e aprendizado dos padrões de atividade, a detecção automática de ameaças, permitindo filtragem baseada em categorias, e o bloqueio proativo de arquivos maliciosos.

2.3. A solução não poderá ser intrusiva e deverá oferecer:

2.3.1. Proteção de usuários contra ameaças da Internet, como malwares, phishing e C2 callbacks.

2.3.2. Funcionar como uma nova camada de segurança preditiva, em qualquer dispositivo, em qualquer lugar.

2.3.3. Disponível em nuvem.

2.3.4. Disponibilizar um portal self-provisioning, de forma que a NOME_CLIENTE será a responsável pelo gerenciamento.

2.3.5. Prover visibilidade em tempo real da atividade na Internet.

2.4. O pacote Professional oferece cloud security platform com proteção contra malware, phishing e C2 callbacks para usuários dentro e fora da rede. Inclui web filtering e relatórios básicos.

2.5. A solução deverá atender os seguintes itens:

2.5.1. Ser disponibilizada em nuvem, sem a necessidade de hardware para instalar ou software para manter no NOME_CLIENTE;

2.5.2. Ser capaz de resolver mais de 88 bilhões de solicitações diariamente sem latência adicional;

2.5.3. Adicionar uma nova camada de segurança preditiva para qualquer dispositivo estando este em qualquer lugar;

2.5.4. Prevenir Malwares, Phishing e Callbacks C2 em qualquer porta;

2.5.5. Implementar políticas de uso aceitáveis usando 50 categorias de conteúdo;

2.5.6. Bloquear requisições de domínios maliciosos e respostas de IP na camada de DNS;

Sugestão 3) SOLUÇÃO DE AUTENTICAÇÃO MULTIFATOR

3.1. Para evitar ameaças avançadas que consideram capacidade analítica em tempo real para identificar comportamento malicioso e atividade botnet em dispositivos dentro e fora da rede, a CONTRATADA deverá entregar uma solução de proteção para as credenciais dos colaboradores, onde quer que estejam, provendo visibilidade completa sobre o uso desses aplicativos/plataformas/sites protegidos, bloqueando acessos indevidos por meio da autenticação das credenciais fornecidas, antes que cheguem a dados corporativos.

3.2. A solução deve prover:

3.2.1. Confiança sobre o Usuário: Confirmar a identidade de quem está solicitando o acesso à rede, garantindo que o usuário é realmente quem ele diz ser, ou se pode ser uma possível tentativa de spoofing de identidade, através de credenciais/senhas roubadas.

3.2.2. Controle de Acesso: O acesso do usuário deve ser garantido para que o mesmo consiga utilizar o recurso necessário de forma segura e garantida. Devendo possuir políticas por grupo de usuários e por aplicativo podendo restringir o acesso de usuários remotos a apenas o que precisam para realizar seu trabalho.

3.3. A solução deverá prover as funcionalidades:

3.3.1. Ser em nuvem, sem a necessidade de hardware para instalar ou software para manter;

3.3.2. Possuir notificações Push para iOS e Android;

3.3.3. Chaves de Segurança, U2F, OTP, SMS e Tokens físicos;

3.3.4. Possuir a facilidade de auto inscrição e autogerenciamento dos usuários;

3.3.5. Poder realizar atribuição e imposição de políticas de segurança globalmente ou por aplicação, com imposição de políticas baseadas em redes autorizadas.

3.4. A contratação de subscrição da solução de múltiplo fator de autenticação, considera a implantação para X.000 (X mil) usuários; (informar a quantidade de usuários e considerar margem de crescimento).

3.5. A CONTRATADA prestará serviço especializado para implantação, configuração e ativação da solução de múltiplo fator de autenticação, no ambiente da CONTRATANTE.

3.6. A solução deve permitir a autenticação de usuários com múltiplo fator para os seguintes ambientes e produtos:

3.6.1. Microsoft Outlook Web Access – OWA - Microsoft Exchange 2016 e ou superior.

3.6.2. VPN Cisco AnyConnect (servidor Cisco ASA) em estações de trabalho e dispositivos móveis com sistema operacional Android, iOS e Windows, no mínimo. A solução deve permitir que o servidor de VPN obtenha a lista de grupos autorizados para o usuário a partir do diretório de autenticação.

3.6.3. Virtual Desktop Infrastructure – VDI, da VMware, permitindo aos usuários o uso do cliente VMware Horizon 7 (ou superior) ou o uso de navegador para iniciar conexões, com no mínimo Windows, MacOs, Linux, Android e iOS.

3.6.4. Microsoft Remote Desktop Protocol – RDP, com o uso do Microsoft Remote Desktop Gateway.

3.6.5. Microsoft Remote Desktop Protocol – RDP, sem o uso do Microsoft Remote Desktop Gateway.

3.6.6. Microsoft Office 365.

3.6.7. Estações de trabalho Microsoft Windows 10 e superiores.

3.6.8. Servidores Windows 2012 R2 e superiores.

3.6.9. Secure Shell – SSH para acesso a servidores Linux através de estações de trabalho e dispositivos móveis que utilizam no mínimo Windows, Android e iOS. A solução deve suportar autenticação de usuários em diretório OpenLdap e AD, protocolo ssh suportado nas versões de Sistemas operacionais Oracle Linux 6, 7, 8 e superiores, Red Hat 6, 7, 8 e superiores.

3.7. A solução deverá fornecer Application Programming Interface - APIs ou Software Development kit - SDKs que possam ser utilizadas por aplicações da CONTRATANTE para autenticação de usuários e provisionamento de dispositivos.

3.8. A solução fornecida deverá possuir funcionalidade que permita compartilhar os logs, em tempo real e/ou por agendamento, e para tanto deverá suportar no mínimo um dos padrões entre os citados: FTP, XML, CVS, SFTP, HTTP, HTTPS, NFS, SSH, SCP, CIFS, WMI ou Syslog. A CONTRATANTE reserva-se, ao seu critério, o direito de definir e utilizar a funcionalidade mais adequada.

3.9. A solução deverá possibilitar que as conexões de saída para a internet sejam realizadas através de servidor de proxy.

3.10. A solução deverá possuir mecanismos de contingência para que, caso ocorra a interrupção da conexão de internet ou indisponibilidade do serviço da CONTRATADA, os usuários possam continuar se autenticando no ambiente da CONTRATANTE.

3.11. A solução deverá ter capacidade de avisar o usuário, quando ocorrer algum erro, através de mensagens que ajudem a identificar a causa sem expor informações críticas.

3.12. A solução deverá possuir capacidade de integração com o Security Assertion Markup Language - SAML.

3.13. A solução deverá possuir capacidade de integração com o Active Directory Federation Services – ADFS.

3.14. A solução deverá possuir capacidade de integração com Remote Authentication DialIn User Service - RADIUS.

3.15. A solução deverá possuir capacidade de disponibilizar pelo menos os seguintes fatores de autenticação:

3.15.1. Push Notification (Notificação enviada para app instalado no dispositivo do usuário);

3.15.2. Software Token – OTP (One Time Password);

3.15.3. OTP enviado por e-mail; 3.15.4. OTP enviado por Short Message Service - SMS.

3.16. A solução deverá possuir capacidade de permitir criação de políticas para definir quais usuários terão obrigatoriedade de utilização de múltiplo fator de autenticação.

3.17. A solução deverá possuir capacidade de permitir criação de políticas baseadas no comportamento do usuário para permitir o acesso ou não ao ambiente da CONTRATANTE, pelo menos para os seguintes itens: localização do usuário, endereço IP de origem, horário de acesso, avaliação de segurança (saúde) do dispositivo utilizado para aprovação.

3.18. A solução deverá ser compatível, com no mínimo, os navegadores Microsoft Internet Explorer 11, Microsoft Edge e/ou Google Chrome 75 ou superior, esta, por sua vez, também deve ser compatível com navegadores de dispositivos móveis com sistema operacional Android e iOS no mínimo.

3.19. Caso necessário cadastrar e-mail de usuário na solução da CONTRATADA, o endereço deve ser exclusivamente do domínio X.com.br (@X.com.br) ou outro informado pela CONTRATANTE, sem possibilidade de ser alterado pelo usuário.

3.20. A solução deverá desconectar a interface de administração quando houver período de tempo definido sem atividade;

3.21. A solução deve permitir que os usuários possam optar, a cada autenticação, por acessar estações de trabalho e servidores Microsoft Windows através de uma das formas abaixo:

3.22. Utilizando cartão inteligente com certificado x.509 protegido por senha (PIN), solução já utilizada no ambiente da CONTRATANTE, sem a exigência de fator de autenticação adicional da solução;

3.23. Utilizando conta e senha do Active Directory, com a exigência de fator de autenticação adicional da solução.

3.24. A solução deverá permitir portabilidade de informações, dados, base de conhecimento e configurações, nos formatos: CSV, XML, PDF ou outro formato de arquivo estruturado.

3.25. A solução deverá armazenar de forma segura as senhas de contas de administradores não sincronizadas com diretório (AD/LDAP) definido pela CONTRATANTE.

3.26. A solução deverá ser acessível para os administradores da solução, via interface web e não necessitar de complementos, plug-ins ou extensões para seu pleno funcionamento.

3.27. A solução deverá possuir documentação de suporte com informações da solução.

3.28. A solução deverá possuir manual, acessível para consulta, durante vigência do contrato.

3.29. A solução deverá permitir a criação de diferentes perfis de usuários, com diferentes níveis de autorização, permissões e visões, garantindo que as permissões de acesso sejam gerenciadas a partir da interface da solução da CONTRATADA.

3.30. A solução deverá possuir suporte à integração Single Sign On - SSO, permitindo a autenticação na interface de administração utilizando recursos de

federação, através do uso de Security Assertion Markup Language – SAML. Neste cenário deve ser possível exigir fator adicional de autenticação da solução.

3.31. A solução deverá possuir recurso para o provisionamento e desprovisionamento dos usuários, devendo ser utilizada a integração e sincronização com o serviço de diretório AD e/ou LDAP da CONTRATANTE ou através de chamadas de API pela CONTRATANTE.

3.32. A solução deverá permitir que somente usuários administradores devam ser capazes de criar, alterar ou remover usuários e suas permissões associadas conforme perfis.

3.33. Para o provisionamento das autorizações de acesso dos usuários na interface de administração da solução da CONTRATADA, deverá ser utilizada uma das seguintes alternativas:

3.33.1. Integração com o serviço de diretório AD ou LDAP da CONTRATANTE: a associação de usuários aos grupos de usuários (perfis) deve ser obtida do serviço de diretório AD ou LDAP da CONTRATANTE.

3.33.2. Uso de API fornecida pela CONTRATADA para que a CONTRATANTE crie ou remova associações de usuários aos perfis.

3.34. A solução deverá suportar múltiplos domínios de Microsoft Active Directory.

3.35. A solução deverá suportar a utilização pelo usuário para autenticação em múltiplos dispositivos, com no mínimo os sistemas operacionais Windows, Android e iOS.

3.36. A solução deve permitir que o usuário possa desprovisionar seu (s) próprio (s) dispositivo (s) ou fornecer API para chamada pela CONTRATANTE.

3.37. A solução não deve permitir que o usuário remova a exigência do uso do fator adicional da solução.

3.38. A solução deve ser capaz de registrar todas as atividades realizadas, tanto de usuários quanto de administradores, gerando log com, no mínimo, as informações de data e hora, usuário, endereço de origem e informações completas das operações.

3.39. A solução deve registrar as falhas e exceções em log com informações suficientes para identificação da falha, com no mínimo as informações de data e hora, usuário, endereço de origem, informações completas das operações e depuração da falha ou exceção.

3.40. A solução deve manter o histórico de todas as informações geradas pela solução e que sofreram inclusões, alterações e exclusões por parte dos usuários da solução, pelo prazo definido pela CONTRATANTE.

3.41. A solução deve garantir que estes registros estejam protegidos contra alteração e exclusão.

3.42. A solução deve permitir a consulta e exportação das trilhas de auditoria, logs e históricos.

3.43. A solução deverá possuir relatório de utilização do múltiplo fator de autenticação.

3.44. A solução deverá permitir geração de relatório em ao menos um dos formatos: HTML, XML, DOCX, PDF ou CSV.

Sugestão 4) SEGURANÇA UTM E SDWAN GERENCIADA

4.1. A solução deverá implementar mecanismo de proteção contra degradação dos links que compõem a solução SD-WAN;

4.2. A solução deverá realizar medições de “Latência”/”Jitter”/”Descarte de Pacotes” para cada destino em cada uma das interfaces dos CPEs SD-WAN;

4.3. A solução SD-WAN deverá suportar exportação de registros Netflow / IPFIX;

4.4. Os equipamentos/appliances, softwares e licenciamentos para solução de SD-WAN (Software Defined Wide Area Network)

4.5. O appliance SD-WAN deve permitir a configuração de regras onde o Failback (retorno à condição inicial) apenas ocorrerá quando o link monitorado recuperado veja avaliado. Deve suportar especificar um valor variando de 1 a 100.

4.6. Permitir atualização e sincronização automática de "clock", de forma que os relatórios e todas as informações sejam sincronizadas com a hora do Banco via NTP (Network Time Protocol);

4.7. A solução deverá ser capaz de realizar NAT (Network Address Translation), a exemplo de NAT64, NAT46, NAT1:1, NAT dinâmico e eventuais outras categorias de tradução de endereços, de forma a garantir o perfeito funcionamento e a integração da Rede IP, no que diz respeito à implementação tanto protocolo IPv4 quanto protocolo IPv6;

4.8. A solução deve implementar políticas de encaminhamento de tráfego por aplicação

4.9. O reconhecimento das aplicações deve ser baseado em DPI (Deep Packet Inspetion), com assinaturas de aplicação sempre atualizadas com a última versão disponível no fabricante.

4.10. Permitir upgrade de sistema operacional das unidades remotas de forma centralizada, via ferramenta de gerência.

4.11. Permitir ao administrador definir políticas de encaminhamento de tráfego que levem em consideração a disponibilidade e o congestionamento dos links e, em caso de falha ou congestionamento dos circuitos de comunicação, o tráfego deverá ser desviado automaticamente para o link em melhores condições de tráfego no momento.

4.12. A solução deve suportar a marcação DSCP dos pacotes.

4.13. A solução SD-WAN deve permitir a configuração das políticas de encaminhamento no CPE de forma centralizada.

4.14. Os equipamentos de SD-WAN fornecidos deverão implementar zero-touch em sua primeira implementação ou substituição.

4.15. A solução deverá ser capaz de medir o status de saúde da rede.

4.16. A solução deverá permitir modificar configuração de tempo de checagem para cada um dos links.

4.17. A solução deverá permitir a configuração de políticas de QoS em camada 7, definindo os valores unitários ou percentuais por classes de serviços.

4.18. A solução deverá permitir a configuração de políticas de QoS em valores onde o máximo corresponda à totalidade de largura de banda disponível no equipamento.

4.19. Solução deverá ser capaz de suportar uma arquitetura de transporte Multicast IPv4 através de tuneis VPN IPSEC.

4.19.1. Solução deverá possuir capacidade de autenticar usuários para administração do Equipamento, através de base de dados Local e Integrada a servidor Microsoft Active Directory.

4.20. Appliance Tipo 1 – Para Site Com Até 3000 Usuários E 200 Túneis Ipsec

4.20.1. O equipamento deve se instalar em rack com largura padrão de 19 polegadas, padrão EIA-310, ocupando no máximo 2U (88,90 mm) do referido rack;

4.20.2. Dispor de fonte de alimentação redundante interna com tensão de entrada de 110V / 220V AC automática e frequência de 50-60 Hz, Hot swapping;

4.20.3. Possuir painel/led indicador on/off, disco e devices de rede;

4.20.4. Possuir throughput de no mínimo 38.000 Mbps para tráfego UDP;

4.20.5. Suportar no mínimo 6.000.000 (seis milhões) conexões simultâneas;

4.20.6. Suportar no mínimo 195.000 (cento e noventa e cinco mil) novas conexões por segundo;

4.20.7. Possuir throughput mínimo de 9 Gbps para tráfego IPS/IDS;

4.20.8. Possuir throughput mínimo de 7.5 Gbps para tráfego VPN IPSEC com criptografia (AES-128);

4.20.9. Possuir throughput mínimo de 6.4 Gbps para tráfego VPN SSL com criptografia (AES128);

4.20.10. Possuir throughput mínimo de 9 Gbps/2.9 Gbps para tráfego Proxy Web filter/SSL Inspection;

4.20.11. Possuir throughput mínimo de 4 Gbps para tráfego NGFW (habilitadas as funcionalidades de Firewall, IPS e Controle de Aplicativo);

4.20.12. Possuir pelo menos 08 (oito) interfaces de rede Gigabit Ethernet 10/100/1000 com leds indicativos de link e atividade, as portas entregues deverão ser roteáveis, ou seja, não será aceito equipamento com porta do tipo switch;

4.20.13. Possuir dispositivo de armazenamento interno de no mínimo 480 GB padrão SSD;

4.20.14. Possuir no mínimo 1 (uma) porta console de conexão para acesso a interface de comando CLI especifica para esta finalidade, utilizando cabo do tipo serial RS-232 ou RJ-45;

4.20.15. Possuir pelo menos 2 (duas) portas USB para conexão de dispositivos externos;

4.21. Appliance Tipo 2 – Para Site Com Até 1000 Usuários E 100 Túneis Ipsec

4.21.1. O equipamento deve se instalar em mesa ocupando no máximo 1U (44,45mm) da referida mesa;

4.21.2. Dispor de fonte de alimentação com tensão de entrada de 110V / 220V AC automática e frequência de 50-60 Hz;

4.21.3. Deverão ser fornecidos todos os cabos de energia, serial (RS-232/RJ45), para instalação e funcionamento do dispositivo;

4.21.4. Possuir led indicador on/off, disco e devices de rede;

4.21.5. Possuir throughput mínimo de 19000 Gbps para tráfego UDP;

4.21.6. Suportar no mínimo 1.900.000 (duzentos e vinte mil) conexões simultâneas;

4.21.7. Suportar no mínimo 100.000 (quinze mil) novas conexões por segundo;

4.21.8. Possuir throughput mínimo de 5.5 Gbps para tráfego IPS/IDS;

4.21.9. Possuir throughput mínimo de 3.5 Gbps para tráfego VPN IPSEC com criptografia (AES-128);

4.21.10. Possuir throughput mínimo de 1.8 Gbps para tráfego VPN SSL com criptografia (AES-128);

4.21.11. Possuir throughput mínimo de 3,6 Gbps / 1.8 Gbps para tráfego Proxy Web filter/SSL Inspection;

4.21.12. Possuir throughput mínimo de 1.2 Gbps para tráfego NGFW (habilitadas as funcionalidades de Firewall, IPS e Controle de Aplicativo);

4.21.13. Possuir no mínimo 8 (oito) interfaces de rede Gigabit Ethernet 10/100/1000 com leds indicativos de link e atividade, as portas entregues deverão ser roteáveis, ou seja, não será aceito equipamento com porta do tipo switch;

4.21.14. Possuir dispositivo de armazenamento interno de no mínimo 240 GB padrão SSD;

4.21.15. Possuir no mínimo 1 (uma) porta console de conexão para acesso a interface de comando CLI especifica para esta finalidade, utilizando cabo do tipo serial RS-232 ou RJ-45;

4.21.16. Possuir pelo menos 1 (uma) portas USB para conexão de dispositivos externos;

4.21.17. Funções Básicas;

4.21.18. VPN SSL, VPN IPSec (Client-to-site e Site-to-site);

4.21.19. Controle de Aplicações;

4.21.20. Proxy Web e Filtro de Conteúdo Web (URL Filtering);

4.21.21. Detecção e prevenção de intrusos – IPS;

4.21.22. Qualidade de serviço – QOS;

4.21.23. Anti-Malware; 4.21.24. SD-WAN;

4.22. Appliance Tipo 3 – Para Site Com Até 5000 Usuários E 80 Túneis Ipsec

4.22.1. O equipamento deve se instalar em mesa ocupando no máximo 1U (44,45mm) da referida mesa;

4.22.2. Dispor de fonte de alimentação com tensão de entrada de 110V / 220V AC automática e frequência de 50-60 Hz;

4.22.3. Deverão ser fornecidos todos os cabos de energia, serial (RS-232/RJ45), para instalação e funcionamento do dispositivo;

4.22.4. Possuir led indicador on/off, disco e devices de rede;

4.22.5. Possuir throughput mínimo de 12.000 Gbps para tráfego UDP;

4.22.6. Suportar no mínimo 1.400.000 (duzentos e vinte mil) conexões simultâneas;

4.22.7. Suportar no mínimo 75.000 (quinze mil) novas conexões por segundo;

4.22.8. Possuir throughput mínimo de 3.9 Gbps para tráfego IPS/IDS;

4.22.9. Possuir throughput mínimo de 1.5 Gbps para tráfego VPN IPSEC com criptografia (AES-128);

4.22.10. Possuir throughput mínimo de 1.2 Gbps para tráfego VPN SSL com criptografia (AES-128);

4.22.11. Possuir throughput mínimo de 2 Gbps / 900 Mbps para tráfego Proxy Web filter/SSL Inspection;

4.22.12. Possuir throughput mínimo de 1 Gbps para tráfego NGFW (habilitadas as funcionalidades de Firewall, IPS e Controle de Aplicativo);

4.22.13. Possuir no mínimo 8 (oito) interfaces de rede Gigabit Ethernet 10/100/1000 com leds indicativos de link e atividade, as portas entregues

deverão ser roteáveis, ou seja, não será aceito equipamento com porta do tipo switch;

4.22.14. Possuir dispositivo de armazenamento interno de no mínimo 240 GB padrão SSD;

4.22.15. Possuir no mínimo 1 (uma) porta console de conexão para acesso a interface de comando CLI especifica para esta finalidade, utilizando cabo do tipo serial RS-232 ou RJ-45;

4.22.16. Possuir pelo menos 1 (uma) portas USB para conexão de dispositivos externos;

4.23. Appliance Tipo 4 – Para Site Com Até 100 Usuários E 40 Túneis Ipsec

4.23.1. O equipamento deve se instalar em mesa ocupando no máximo 1U (44,45mm) da referida mesa;

4.23.2. Dispor de fonte de alimentação com tensão de entrada de 110V / 220V AC automática e frequência de 50-60 Hz;

4.23.3. Deverão ser fornecidos todos os cabos de energia, serial (RS-232/RJ45), para instalação e funcionamento do dispositivo;

4.23.4. Possuir led indicador on/off, disco e devices de rede;

4.23.5. Possuir throughput mínimo de 3.7 Gbps para tráfego UDP;

4.23.6. Suportar no mínimo 900.000 (duzentos e vinte mil) conexões simultâneas;

4.23.7. Suportar no mínimo 50.000 (quinze mil) novas conexões por segundo;

4.23.8. Possuir throughput mínimo de 1.5 Gbps para tráfego IPS/IDS;

4.23.9. Possuir throughput mínimo de 950 Mbps para tráfego VPN IPSEC com criptografia (AES-128);

4.23.10. Possuir throughput mínimo de 790 Mbps para tráfego VPN SSL com criptografia (AES-128);

4.23.11. Possuir throughput mínimo de 250 Mbps/390 Mbps para tráfego Proxy Web filter/SSL Inspection;

4.23.12. Possuir throughput mínimo de 400 Mbps para tráfego NGFW (habilitadas as funcionalidades de Firewall, IPS e Controle de Aplicativo);

4.23.13. Possuir no mínimo 4 (quatro) interfaces de rede Gigabit Ethernet 10/100/1000 com leds indicativos de link e atividade, as portas entregues deverão ser roteáveis, ou seja, não será aceito equipamento com porta do tipo switch;

4.23.14. Possuir dispositivo de armazenamento interno de no mínimo 120 GB padrão SSD;

4.23.15. Possuir no mínimo 1 (uma) porta console de conexão para acesso a interface de comando CLI especifica para esta finalidade, utilizando cabo do tipo serial RS-232 ou RJ-45;

4.23.16. Possuir pelo menos 1 (uma) portas USB para conexão de dispositivos externos;

4.25. Funções Básicas Para Todos Appliances De Segurança

4.25.1. VPN SSL, VPN IPSec (Client-to-site e Site-to-site);

4.25.2. Controle de Aplicações;

4.25.3. Proxy Web e Filtro de Conteúdo Web (URL Filtering);

4.25.4. Detecção e prevenção de intrusos – IPS;

4.25.5. Qualidade de serviço – QOS;

4.25.6. Anti-Malware; 4.25.7. SD-WAN;

4.26. Funções De Firewall Para Todos Appliances De Segurança

4.26.1. Possuir capacidade de processamento de pacotes e interfaces de acordo com a tabela de performance dos equipamentos;

4.26.2. Permitir a conexão simultânea de vários administradores, com poderes de alteração de configurações e/ou apenas de visualização das mesmas;

4.26.3. O sistema ainda Irá contemplar um recurso de cópia de segurança do tipo snapshot, que contemple a cópia completa das configurações dos serviços e recursos do sistema;

4.26.4. Possibilitar a restauração do snapshot através da interface web de qualquer ponto remoto, de modo a contribuir para uma restauração imediata sem a necessidade de reinicialização do sistema;

4.26.5. Permitir habilitar ou desabilitar o registro de log por política de firewall;

4.26.6. Possuir controle de acesso à internet por endereço IP de origem e destino;

4.26.7. Possuir controle de acesso à internet por sub-rede;

4.26.8. Possuir suporte a tags de VLAN (802.1q);

4.26.9. Suportar agregação de links, segundo padrão IEEE 802.3ad;

4.26.10. Possuir ferramenta de diagnóstico do tipo tcpdump;

4.26.11. Possuir integração com Servidores de Autenticação RADIUS, TACACS+, LDAP e Microsoft Active Directory;

4.26.12. Possuir métodos de autenticação de usuários para qualquer aplicação que se execute sob os protocolos TCP (HTTP, HTTPS, FTP e Telnet);

4.26.13. Possuir a funcionalidade de tradução de endereços estáticos – NAT (Network Address Translation), um para um e vários para um.

4.26.14. Permitir controle de acesso à internet por períodos do dia, permitindo aaplicação de políticas por horários e por dia da semana;

4.26.15. Permitir controle de acesso à internet por domínio, exemplo: gov.br, org.br, edu.br;

4.26.16. Possuir a funcionalidade de fazer tradução de endereços dinâmicos, muitos para um, PAT;

4.26.17. Possuir suporte a roteamento dinâmico RIP V1, V2, OSPF, BGP;

4.26.18. Possuir funcionalidades de DHCP Cliente, Servidor e Relay;

4.26.19. Suportar aplicações multimídia como: H.323, SIP;

4.26.20. Possuir tecnologia de firewall do tipo Stateful;

4.26.21. Possuir opção de alta disponibilidade (HA), trabalhando no esquema de redundância do tipo ativo/passivo;

4.26.22. Permitir o funcionamento em modo transparente tipo “bridge”;

4.26.23. Permitir a criação de pelo menos 20 VLANS no padrão IEEE 802.1q;

4.26.24. Possuir conexão entre estação de gerência e appliance criptografada tanto em interface gráfica quanto em CLI (linha de comando);

4.26.25. Suportar forwarding de multicast;

4.26.26. Permitir criação de serviços por porta ou conjunto de portas dos seguintes protocolos, TCP, UDP, ICMP e IP;

4.26.27. Permitir o agrupamento de serviços;

4.26.28. Permitir o filtro de pacotes sem a utilização de NAT;

4.26.29. Permitir a abertura de novas portas por fluxo de dados para serviços que requerem portas dinâmicas;

4.26.30. Possuir mecanismo de anti-spoofing;

4.26.31. Permitir criação de regras definidas pelo usuário;

4.26.32. Permitir o serviço de autenticação para HTTP e FTP;

4.26.33. Possuir a funcionalidade de balanceamento e contingência de links;

4.26.34. Possuir técnicas de detecção de programas de compartilhamento de arquivos (peer-to-peer) e de mensagens instantâneas, suportando ao menos: Yahoo! Messenger, MSN Messenger, ICQ, AOL Messenger, BitTorrent, eDonkey, GNUTella, KaZaa, Skype e WinNY.

4.27. Identificação De Usuários Para Todos Appliances De Segurança

4.27.1. Possuir a capacidade de criação de políticas de acesso de Firewall, VPN, IPS e Controle de aplicações integradas ao repositório de usuários sendo: Active Directory, LDAP, TACAC´S e Radius;

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

4.27.3. Para usuários não registrados ou não reconhecidos no domínio, a solução deverá ser capaz de fornecer uma autenticação baseada em navegador (Captive Portal), sem a necessidade de agente;

4.27.4. Possuir Captive Portal com suporte a Autenticação Social (Facebook, Twitter, Google);

4.27.5. A solução será capaz de identificar nome do usuário, login, máquina/computador registrados no Microsoft Active Directory;

4.27.6. Na integração com o AD, todos os domain controllers em operação na rede do cliente deverão ser cadastrados de maneira simples e sem utilização de scritps de comando;

4.27.7. A solução de identificação de usuário Irá se integrar com as funcionalidades Firewall, controle de aplicação e IPS, sendo elas do mesmo fabricante;

4.27.8. A solução deverá suportar a opção de instalação de softwares agentes nos PCs/Laptops para que os próprios PCs/Laptops enviem suas credenciais de IP/nome de usuário do domínio/nome da máquina para o gateway diretamente, sem que este tenha que fazer Queries no AD;

4.28. Funções De Vpn Para Todos Appliances De Segurança

4.28.1. VPN baseada em appliance;

4.28.2. Possuir algoritmos de criptografia para túneis VPN: AES, DES, 3DES;

4.28.3. Suporte a certificados PKI X.509 para construção de VPNs;

4.28.4. Possuir suporte a VPNs IPSec site-to-site:

4.28.5. O Criptografia, 3DES, AES128, AES256, AES-GCM-128

4.28.6. O Integridade MD5, SHA-1, SHA-256, SHA384 e AES-XCBC;

4.28.7. O Algoritmo Internet Key Exchange (IKE) versões I e II;

4.28.8. O AES 128 e 256 (Advanced Encryption Standard);

4.28.9. Possuir suporte a VPN SSL;

4.28.10. Possuir capacidade de realizar SSL VPNs utilizando certificados digitais;

4.28.11. Suportar VPN SSL Clientless, sem a necessidade de utilização de Java, no mínimo, para os serviços abaixo:

4.28.11..1. RDP;

4.28.11..2. VNC;

4.28.11..3. SSH;

4.28.11..4. WEB;

4.28.11..5. SMB.

4.28.12. Permitir a arquitetura de vpn hub and spoke;

4.28.13. Suporte a VPNs IPSec client-to-site;

4.28.14. Possuir cliente próprio para Windows para o estabelecimento da VPN clienttosite;

4.28.15. Suporte à inclusão em autoridades certificadoras (enrollment) mediante SCEP (Simple Certificate Enrollment Protocol);

4.28.16. Possuir funcionalidades de Auto-Dicovery VPN capaz de permitir criar tuneis de VPN dinâmicos entre múltiplos dispositivos (spokes) com um gateway centralizador (hub);

4.28.17. A funcionalidade de AD-VPN Irá suportar criar os seguintes tipos de tuneis:

4.28.17..1. Site-to-Site;

4.28.17..2. Full-Mesh;

4.28.17..3. Star.

4.29. Funções De Detecção De Intrusão Para Todos Appliances De Segurança

4.29.1. A detecção de Intrusão será baseada em appliance;

4.29.2. Capacidade de detecção de mais de 22.000 ataques;

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

4.29.4. Possuir tecnologia de detecção baseada em assinatura;

4.29.5. Suportar a implantação em modo Gateway, in ine e em modo sniffer;

4.29.6. Suportar implementação de cluster do IPS em linha se o equipamento possuir interface do tipo by-pass;

4.29.7. O sistema de detecção e proteção de intrusão Irá possuir integração à plataforma de segurança;

4.29.8. Possuir opção para administrador das listas de blacklist, whitelist e quarentena com suporte a endereços IPv6;

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

4.29.10. Possuir capacidade de agrupar assinaturas para um determinado tipo de ataque, por exemplo: agrupar todas as assinaturas relacionadas a web-server para que seja usado para proteção específica de Servidores Web;

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

4.29.12. Mecanismos de detecção/proteção de ataques;

4.29.13. Reconhecimento de padrões;

4.29.14. Análise de protocolos;

4.29.15. Detecção de anomalias;

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

4.29.17. Proteção contra ataques de Windows ou NetBios;

4.29.18. Proteção contra ataques de SMTP (Simple Message Transfer Protocol) IMAP (Internet Message Access Protocol, Sendmail ou POP (Post Office Protocol);

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

4.29.20. Proteção contra ataques a FTP, SSH , Telnet e rlogin;

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

4.29.22. Alarmes na console de administração;

4.29.23. Alertas via correio eletrônico;

4.29.24. Monitoração do comportamento do appliance através de SNMP, o dispositivo será capaz de enviar traps de SNMP quando ocorrer um evento relevante para a correta operação da rede;

4.29.25. Capacidade de resposta/logs ativa a ataques;

4.29.26. Terminação de sessões via TCP resets;

4.29.27. Atualizar automaticamente as assinaturas para o sistema de detecção de intrusos;

4.29.28. O Sistema de detecção de Intrusos Irá atenuar os efeitos dos ataques de negação de serviços;

4.29.29. Possuir filtros de ataques por anomalias;

4.29.30. Permitir filtros de anomalias de tráfego estatístico de: flooding, scan, source e destination session limit;

4.29.31. Permitir filtros de anomalias de protocolos;

4.29.32. Suportar reconhecimento de ataques de DoS, reconnaissance, exploits e evasion;

4.29.33. Suportar verificação de ataque nas camadas de aplicação;

4.30. Funções De Antivírus

4.30.1. Possuir funções de antivírus, anti-spyware;

4.30.2. Possuir antivírus em tempo real, para ambiente de gateway internet integrado a plataforma de segurança para os seguintes protocolos: HTTP, SMTP, POP3 e FTP;

4.30.3. Permitir o bloqueio de malwares (adware, spyware, hijackers, keyloggers, etc.);

4.30.4. Permitir o bloqueio de download de arquivos por extensão e tipo de arquivo;

4.30.5. Permitir o bloqueio de download de arquivos por tamanho.

4.31. Funções De Proxy E Filtro De Controle De Conteúdo Web Para Todos Appliances De Segurança

4.31.1. Possuir solução de filtro de conteúdo web integrado a solução de segurança;

4.31.2. Possuir pelo menos 75 categorias para classificação de sites web;

4.31.3. Possuir base mínima contendo, 40 milhões de sites internet web já registrados e classificados;

4.31.4. Possuir categoria exclusiva, no mínimo, para os seguintes tipos de sites web como:

4.31.4..1. Webmail;

4.31.4..2. Instituições de Saúde;

4.31.4..3. Notícias;

4.31.4..4. Pornografia;

4.31.4..5. Restaurante;

4.31.4..6. Mídias Sociais;

4.31.4..7. Esporte;

4.31.4..8. Educação;

4.31.4..9. Games;

4.31.4..10. Compras;

4.31.5. Permitir a monitoração do tráfego internet sem bloqueio de acesso aos usuários;

4.31.6. Possuir sistema de cache interno, armazenando requisições WEB em disco local e memória;

4.31.7. Permitir a definição do tamanho mínimo dos objetos salvos em cache no disco;

4.31.8. Permitir a definição do tamanho máximo dos objetos salvos em cache em memória;

4.31.9. Atender a estrutura de navegação através de hierarquia de proxy com e sem autenticação;

4.31.10. Possibilitar a integração com servidores de cache WEB externos;

4.31.11. Ser capaz de armazenar cache dinâmico para as atualizações Microsoft Windows Update, Youtube, MSN Vídeos, Facebook, Google Maps;

4.31.12. Possuir a capacidade de excluir URL's específicas do cache web, configurável por listas de palavras chaves com suporte inclusive a expressões regulares;

4.31.13. Integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo contas e grupos de usuários cadastrados;

4.31.14. Prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory;

4.31.15. Exibir mensagens de bloqueio customizável pelos Administradores para resposta aos usuários na tentativa de acesso a recursos proibidos pela política de segurança da contratante;

4.31.16. Permitir a filtragem de todo o conteúdo do tráfego WEB de URLs conhecidas como fonte de material impróprio e códigos (programas/scripts) maliciosos em applets Java, cookies, activeX através de: base de URL própria atualizável;

4.31.17. Permitir o bloqueio de páginas web através da construção de filtros específicos com mecanismo de busca textual;

4.31.18. Permitir a criação de listas personalizadas de URLs permitidas – lista branca e bloqueadas – lista negra;

4.31.19. Permitir o bloqueio de URLs inválidas cujo campo CN do certificado SSL não contém um domínio válido;

4.31.20. Garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de filtragem de conteúdo web;

4.31.21. Permitir a criação de regras para acesso/bloqueio por grupo de usuários do serviço de diretório LDAP;

4.31.22. Permitir a criação de regras para acesso/bloqueio por endereço IP de origem;

4.31.23. Permitir a criação de regras para acesso/bloqueio por sub-rede de origem;

4.31.24. Ser capaz de categorizar a página web tanto pela sua URL como pelo seu endereço IP;

4.31.25. Permitir o bloqueio de páginas web por Classificação como páginas que facilitam a busca de áudio, vídeo e URLs originadas de spam;

4.31.26. Permitir a criação de listas personalizadas de URLs permitidas – lista branca e bloqueadas – lista negra;

4.31.27. Funcionar em modo Proxy Explícito para HTTP, HTTPS, e FTP e em Proxy Transparente;

4.31.28. Permitir configurar a porta do Proxy Explícito.

4.32. Funções De Controle De Aplicações Para Todos Os Appliances De Segurança

4.32.1. As funcionalidades devem ser baseadas em appliance;

4.32.2. Deverá reconhecer no mínimo 700 aplicações;

4.32.3. Deverá possuir pelo menos 10 categorias para classificação de aplicações;

4.32.4. Deverá possuir categoria exclusiva, no mínimo, para os seguintes tipos de aplicações como:

4.32.4..1. P2P;

4.32.4..2. Web;

4.32.4..3. Transferência de arquivos;

4.32.4..4. Chat;

4.32.4..5. Social;

4.32.5. Permitir a monitoração do tráfego de aplicações sem bloqueio de acesso aos

4.32.6. Usuários;

4.32.7. Ontegrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados;

4.32.8. Prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory;

4.32.9. Permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do Microsoft Active Directory;

4.32.10. Permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do serviço de diretório LDAP;

4.32.11. Permitir a criação de regras para acesso/bloqueio por endereço IP de origem;

4.32.12. Permitir a criação de regras para acesso/bloqueio por sub-rede de origem e destino;

4.32.13. Garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de controle de aplicações.

4.33. Funções De Sistema De Proteção Anaçada De Ameaças – Para Todos Appliances De Segurança

4.33.1. Possuir sistema de proteção avançada contra ameaças (ATP) nativo;

4.33.2. O sistema de ATP Irá monitorar e analisar o tráfego da rede, identificar aplicativos e ameaças de ataques direcionados e persistentes e efetuar os respectivos bloqueios;

4.33.3. Ser baseado em uma lista de assinaturas eletrônicas que atue em tempo real analisando a camada de aplicação, capaz de identificar o conteúdo dos pacotes, fazer log (registros) das assinaturas trafegadas, inspecionar os pacotes e efetuar o descarte automático do pacote quando identificado assinaturas de pacotes maliciosos, inapropriados para o uso no ambiente corporativo;

4.33.4. A base de assinaturas do sistema de ATP nativo será fornecida pelo período do contrato;

4.33.5. Possuir um mínimo de 31 mil (trinta e um mil) assinaturas;

4.33.6. Permitir a identificação de aplicativos e ameaças independente das portas e protocolos;

4.33.7. Permitir a atualização automática das assinaturas por meio de agendamento diário;

4.33.8. Possuir capacidade de inspecionar e bloquear em tempo real, ameaças do tipo: activex, malware, malware-backdoors, ataques P2P, trojans, worms, user_agents, pua (adware, p2p, toolbars) malwares para mobile, blacklist, botcc, exploits-kits, file executable, file-flash, file-identify, file-image, file-java, file-multimedia, file-office, fileother, file-pdf, games, inappropriate e vulnerabilidades conhecidas;

4.33.9. Possuir uma ferramenta de bloqueio de execução de aplicativos, integrado a base de antivírus e antimalware;

4.33.10. Possuir capacidade de inspecionar e bloquear em tempo real, aplicativos do tipo: ads, cloud, colaboração, download, e-mail, games, mobile, p2p, proxy, remote, redes sociais; storage, streaming, update, voip e web;

4.33.11. Possuir capacidade de inspecionar e bloquear em tempo real, aplicativos de VoIP tais como: Hotline, Asterisk, Linphone, SIP, Skype, Xlite SIP, X-Pro SIP, Cisco SIP, OpenSIP, Bria, ClearSea e Nero SIP;

4.33.12. Possuir capacidade de inspecionar e bloquear em tempo real, aplicativos de Redes Sociais tais como: Aol Instant Messenger, Badoo, BaiduHi, Airtime, Blogger, BoldChat, ChatON, China.com, Facebook, Flickr, FC2, Fring, Google Analytics, Google App, ICQ, Linkdin, Meetup, MSM Messenger, Netlog, Skype, Tinder, Tuenti, Twitter, WhatssApp, WeChat e Zoho Chat;

4.33.13. Possuir capacidade de inspecionar e bloquear em tempo real, aplicativos e transferências de arquivos do tipo P2P (peer to peer) tais como: BitTorrent, Gnutella, FastTrack, IceShare, Napster, Shareman e de Storages, tais como: Dropbox, Easyshare, Google Drive, Megashare, MegaUpload, Rapidshare, OneDrive, Yahoo Box, SoundCloud e Filemail, DivShare;

4.33.14. Suportar exceção de ameaças por assinatura; IP de origem ou IP de destino;

4.33.15. Suportar exceção de aplicativos por assinatura; IP de origem ou IP de destino;

4.33.16. Possuirá mecanismos para gerar gráfico do histórico da relação de eventos entre as “ameaças detectadas” e as “ameaças bloqueadas”;

4.33.17. Possuirá mecanismos para gerar gráfico do histórico da relação de eventos entre os “aplicativos detectados” e os “aplicativos bloqueados”;

4.33.18. Possuirá mecanismos para gerar log dos registros das incidências, classificados em pelo menos 3 (três) níveis de impacto: “baixo; médio e alto”;

4.33.19. Gerar registro do tipo Top Level, dos 10(dez) mais, inclusive da relação de eventos entre usuários e ameaças, usuário e aplicativos, aplicativos e ameaças identificados e bloqueados;

4.34. Gerenciamento Centralizado

4.34.1. Funcionalidades De Gerenciamento

4.34.1..1. Como boa prática de segurança e de mercado, a solução de gerência deverá ser separada do gateway de segurança, onde irá gerenciar políticas de segurança de todos os firewalls e funcionalidades solicitadas neste projeto;

4.34.1..2. A CONTRATADA deverá possuir uma solução de gerenciamento centralizado que possibilite o gerenciamento de todos os Firewall contratados.

4.34.1..3. Centralizar a administração de regras e políticas do(s) cluster(s), usando uma única interface de gerenciamento;

4.34.1..4. A solução deverá permitir seu gerenciamento por: CLI (Command Line Interface) via SSH, Web GUI utilizando protocolo HTTPS ou console gráfica;

4.34.1..5. Deve manter um canal de comunicação segura, com encriptação baseada em certificados, entre todos os componentes que fazem parte da solução de firewall, gerência, armazenamento de logs e emissão de relatórios;

4.34.1..6. A solução deve incluir a opção de segmentar a base de regra utilizando rótulos ou títulos de seção para organizar melhor a política facilitando a localização e gestão do administrador;

4.34.1..7. A solução de gerência deverá prover fácil administração na aplicação das políticas para os gateways, sendo capaz de realizar o processo de alteração de regras e configuração de todas as soluções de segurança, que pode ser aplicada nos gateways remotos em uma única sessão, evitando qualquer tipo de retrabalho.

4.34.1..8. Deve possibilitar a realização de “backup” e restauração de dados.

4.34.1..9. Deve possibilitar o envio dos “logs” gerados a outro concentrador de “logs” externo a solução.

4.34.1..10. Deve possibilitar a gerência de “logs”, realizando as configurações de relatórios de todos os “firewalls” integrados.

4.34.1..11. Deve permitir buscas e realizar análise de usuários e grupos, rastreando toda a sua atividade e uso da internet.

4.34.1..12. O gerenciamento central da CONTRATADA deve permitir/possuir:

4.34.1..13. Criação e administração de políticas de Firewall, Controle de aplicação e IPS, Antivírus e Anti-Malware, Filtro de URL e prevenção contra ameaças avançadas;

4.34.1..14. Monitoração de logs;

4.34.1..15. Debugging;

4.34.1..16. Acesso concorrente de administradores;

4.34.1..17. Deve permitir usar palavras chaves para facilitar identificação de regras;

4.34.1..18. Definição de perfis de acesso à console com permissões granulares como: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações;

4.34.1..19. Autenticação integrada à base de dados local;

4.34.1..20. Deve possuir ferramenta para localização de objetos (por exemplo: endereço IP, Range de IP, subrede) na base de regras;

4.34.1..21. Criação de regras que fiquem ativas em horário definido;

4.34.1..22. Backup das configurações e rollback de configuração para a última configuração salva;

4.34.1..23. Habilidade de upgrade via interface de gerenciamento;

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

4.34.1..25. Controle sobre todos os equipamentos da plataforma de proteção em uma única console, com administração de privilégios e funções;

4.34.1..26. Deve permitir controle global de políticas para todos os equipamentos que compõe a plataforma de proteção;

4.34.1..27. Deve permitir a criação de objetos e políticas compartilhadas;

4.34.1..28. Capacidade de definir administradores com diferentes perfis de acesso com, no mínimo, as permissões de Leitura/Escrita e somente Leitura;

4.34.1..29. Solução deve ser capaz de detectar ataques de tentativa de login e senha utilizando tipos diferentes de credencias;

4.34.1..30. A solução deve permitir gerenciar templates de customização visual e marca do produto do sistema de gerenciamento centralizado e permitir aplicar no UTM´s gerenciados. Portanto, deve ser possível customizar a interface gráfica nos seguintes itens:

4.34.1..30.1. Título da Página;

4.34.1..30.2. Ícone (favicon);

4.34.1..30.3. Logotipo;

4.34.1..30.4. Imagem de fundo;

4.34.1..30.5. Cores do menu (primária e secundária);

4.34.2. Funcionalidades De Analise De Log

4.34.2..1. Deverá prover análise de tráfego de rede de modo centralizado;

4.34.2..2. Deve possuir análise de tráfego de rede e ameaças por geolocalização;

4.34.2..3. Deverá ser capaz de receber os logs e eventos com o objetivo de prover os seguintes tipos de análises:

4.34.2..4. Análise de ameaças e incidentes de segurança;

4.34.2..5. Análise de tráfego e uso de categorias Web;

4.34.2..6. Análise de tráfego e uso de aplicativos;

4.34.2..7. Análise de tráfego e ameaças por usuário;

4.34.2..8. Análise de desempenho de políticas de segurança;

4.34.2..9. A solução ofertada deve ser capaz de fazer o gerenciamento centralizado de logs, consolidação de logs, arquivamento de logs, busca avançada de logs;

4.34.2..10. Deverá possuir ferramenta para salvar consultas avançadas;

4.34.2..11. Deve possuir relatórios personalizados;

4.34.2..12. Deverá ser capaz de efetuar o arquivamento de relatórios;

4.34.2..13. Deve possuir agendamento de relatórios;

4.34.2..14. Os Relatórios deverão, no mínimo, serem exportados em formatos flexíveis (PDF, CSV);

Sugerimos deixar estes itens como explícitos no termo de referência, visando uma competitividade igualitária entre os participantes neste Certame.

Resposta: Sugestões relativas à inclusão de Solução Ant-DDoS, Proteção DNS, Autenticação Multifator e Segurança UTM e SDWAN gerenciada não foram acatadas.