GOVERNO DO ESTADO DE MINAS GERAIS

Secretaria de Estado de Planejamento e Gestão

Diretoria Central de Gestão de Serviços e Infraestrutura de TIC

Anexo nº A - Lote 100/SEPLAG/DCGSITIC/2025

PROCESSO Nº 1500.01.0079973/2024-83

ANEXO A – LOTE 100 – SERVIÇO DE VIRTUALIZAÇÃO DE COMUNICAÇÃO DE DADOS (SD-WAN)

1. REQUISITOS TÉCNICOS BÁSICOS

Padrões e Topologia de Rede - A rede contratada deverá ser implementada conforme os padrões TCP/IP, devendo suportar o tráfego dos protocolos desenvolvidos segundo essa padronização. A solução pretendida é a disponibilização de acesso a comunicação de dados de forma que as Unidades de Governo possam se conectar ao ponto central, na UGO ou acessar serviços na Internet com o controle dos conteúdos acessados, sendo esta comunicação protegida contra acessos indevidos a partir da Internet.

Será tratado como controladora o conjunto de equipamentos e soluções instalados on premisse na UGO responsáveis por todas as ações necessárias para o correto funcionamento e conexão dos equipamentos CPE´s instalados nas unidades dos clientes em conformidade com o solicitado neste termo de referência.

Deverá ser instalada uma controladora na UGO Prodemge e uma controladora na UGO/SEF. As diferenças existentes entre a instalação da controladora na UGO/SEF em relação às características referenciadas neste anexo, serão tratadas no Anexo G – Especificidades da Secretaria de Estado da Fazenda - SEF

Não serão admitidas soluções baseadas somente em tecnologia VPN (Virtual Private Network);

Os serviços de conectividade IP deverão estar completamente protegidos, tanto de redes públicas, como de outras VPN´s e deverá seguir os padrões de segurança especificados no item 7.13 do Termo de Referência.

As redes locais das Unidades de Governo não poderão ser acessadas diretamente a partir da Internet. São considerados acessos provenientes da Internet somente aqueles que ingressam no equipamento CPE fora do túnel estabelecido entre o CPE e a controladora SD-WAN.

Acessos externos à unidade deverão obrigatoriamente ter origem dentro da rede corporativa do Estado. O tráfego dentro dos túneis da solução SD-WAN será considerado como pertencente à rede corporativa do Estado.

Não será permitido o uso dos IPs públicos relativos aos links para o provimento da comunicação para acesso ao ambiente interno da unidade, para qualquer finalidade.

Todo o acesso a recursos externos à unidade será controlado pelos equipamentos CPE SD-WAN instalado no local. Para manter o controle da segurança da informação, não poderá ser instalado na unidade links de acesso à Internet que não estejam conectados ao CPE SD-WAN, pois este acesso seria um ponto de conexão sem controle do mundo externo e representaria um risco de entrada de malwares, ransomware e vazamento de dados na rede corporativa do Estado de Minas Gerais.

Plano de Endereçamento - O plano de endereçamento IP nas redes locais dos clientes deverá ser definido pela UGO.

CPEs – O fornecedor vencedor do lote 100 deverá prover os recursos necessários à interligação dos equipamentos que serão instalados na unidade dos clientes aos links de comunicação de dados disponibilizados pelo cliente, em suas unidades.

As interfaces previstas deverão ser Ethernet padrão 10/100/1000 BaseTx, conector RJ45 ou, caso sejam interfaces SFP, deverão ser fornecidos os conversores para o conector RJ45, sem custo adicional, exceto para o caso das interfaces 10 Gbps solicitadas para o modelo 11, que deverão ser SFP+.

Deverão ser permitidos todos os tipos de acessos e protocolos necessários para o gerenciamento dos roteadores, gateways, CPEs e/ou servidores e estações de trabalho nas redes de clientes.

Suporte a gerenciamento - O equipamento de conexão disponibilizado pelo fornecedor deverá suportar, pelo menos, o protocolo SNMP-(V2 e V3), para gerenciamento remoto, monitoração e estatísticas de tráfego, entre outros. Neste equipamento deverá ser permitido à UGO a coleta de informações por meio de “polling” SNMP e por meio do uso do protocolo ICMP.

Capacidade dos equipamentos SD-WAN das unidades – Deverão ser disponibilizados 11 modelos de equipamentos, que suportam as capacidades de processamento informadas na tabela 1

Modelo	Capacidade
Modelo 1	300 Mbps (4 interfaces)
Modelo 2	500 Mbps (4 interfaces)
Modelo 3	700 Mbps (4 interfaces)
Modelo 4	1,5 Gbps (4 interfaces)
Modelo 5	3 Gbps (4 interfaces)
Modelo 6	300 Mbps (6 interfaces)
Modelo 7	500 Mbps (6 interfaces)
Modelo 8	700 Mbps (6 interfaces)
Modelo 9	1,5 Gbps (6 interfaces)
Modelo 10	3 Gbps (6 interfaces)
Modelo 11	10 Gbps (8 interfaces, sendo pelo menos 6 de 1 Gbps e 2 de 10 Gbps)

Tabela 1 - Modelos e capacidades de equipamentos SD-WAN

Não poderá haver restrição ao uso das interfaces como LAN ou WAN nos equipamentos, ou seja, as interfaces poderão ser utilizadas para qualquer finalidade. Caso haja restrição, deverá haver um adicional de 2 interfaces ao número de interfaces definidas para o modelo para uso exclusivo para rede LAN e as demais interfaces para uso como rede WAN.

O cliente deverá solicitar o serviço de virtualização da comunicação informando a capacidade do equipamento que ele deseja utilizar na prestação do serviço.

O fornecedor deverá informar o valor da mensalidade da prestação do serviço para cada modelo de equipamento disponibilizado.

Será vencedor do lote o fornecedor que oferecer o menor preço pelo serviço contemplando o fornecimento, instalação e configuração da controladora mais os equipamentos CPE necessários para atender a estimativa de demanda de contratação do serviço enviada pelos órgãos.

Deverá haver diferença de preços para a prestação de serviço de acordo com o modelo de equipamento a ser ofertado. Um modelo de equipamento pode atender a diferentes capacidades. Mesmo nesta situação, deverá haver diferença entre os preços, sendo esta diferença mínima de R$ 5,00 entre os equipamentos.

O fornecedor deverá disponibilizar uma solução que garanta pelo menos os seguintes requisitos:

- Prover ponto de conexão primária, ou seja, uma solução (hardware, software e licenciamento) concentradora das conexões remotas que deverá ser instalada na UGO (SEF e PRODEMGE), conforme item 8.2 – Interoperabilidade do Termo de Referência.
- Ser composta por uma Controladora Central na UGO (on-premises), que será responsável por fazer toda a configuração dos appliances SD-WAN, incluindo priorização de tráfego, configurações de QoS,

que deverão ocorrer de forma centralizada via software de gerência.

  - O uso de controladora on-premises é obrigatória devido a criticidade do serviço contratado. Com esta configuração diminuímos a quantidade de elementos existentes na comunicação entre a controladora e a rede corporativa, permitindo maior eficiência na comunicação das unidades remotas no uso de sistemas corporativos. O uso de controladoras em nuvem faria com que toda a comunicação das unidades fosse ao ambiente em nuvem e tivesse que retornar para a rede corporativa, aumentando o número de elementos que participariam desta comunicação.
  - Outro fator que torna obrigatório o uso da solução on-premises é manter a independência da operação da rede corporativa do Estado em relação ao ambiente de nuvem dos provedores de serviço. O uso de soluções em nuvem obrigaria o Estado a seguir a agenda de atualizações e manutenções do ambiente do provedor do serviço, que muitas vezes é incompatível com a agenda de manutenções e atualizações dos entes do governo participantes do projeto. A instalação da solução on-premises manterá a independência do Estado para decidir pela agenda de atividades conforme as necessidades dos entes participantes do projeto.

- Deverá ser utilizado o link Internet disponibilizado pela Prodemge para que a concentradora receba as conexões advindas dos CPE's SD-WAN instalados nas unidades de Governo remotas, exceto no caso da controladora instalada na UGO/SEF.
- A solução controladora deve ser capaze de tratar o conjunto de acessos de cada Unidade de Governo de forma independente, com políticas específicas para cada uma.
- A capacidade de processamento e throughput inicial da controladora deve ser capaz de suportar todo o tráfego previsto para atendimento a todos os acessos deste lote. A Prestadora deverá se responsabilizar pelo dimensionamento e upgrades necessários na solução de forma a garantir o perfeito funcionamento até o final da vigência do contrato, sem ônus para a UGO.

    - Para permitir um melhor dimensionamento da controladora, podemos estimar que esta deverá ter a capacidade de processamento de tráfego de 5% da capacidade total dos CPEs SD-WAN solicitados pelos órgãos. Exemplo:

      Caso sejam contratados 10 equipamentos com capacidade de 300 Mbps, 5 com capacidade de 500 Mbps e 2 com capacidade de 1 Gbps, o somatório das capacidades dos equipamentos totalizará 7,5 Gbps. A estimativa de tráfego que passará pela controladora com destino à rede corporativa será de 375 Mbps.

    - Estes valores servem somente como uma base de cálculo para o dimensionamento da solução e é baseado na expectativa de tráfego com destino à rede corporativa conforme o observado no tráfego de dados atual.

    - O prestador de serviço, porém, deverá ampliar a controladora para que ela suporte o volume de tráfego caso este ultrapasse a previsão de 5% da capacidade total contratada para os CPEs informadas neste termo de referência.

    - Caso o tráfego para as controladoras ultrapasse os 5% estimados, e a controladora esteja apresentando consumo de CPU acima do previsto no item 8.2.3.3, o prestador de serviço terá o prazo de até 120 dias para efetuar o upgrade da controladora para que ela suporte o tráfego real consumido no projeto.

- Deverá analisar o tráfego em tempo real e realizar o balanceamento dos pacotes de um mesmo fluxo entre múltiplos links simultaneamente em uma extremidade;
- Deverá monitorar a latência, o jitter e o descarte de pacotes em cada um dos links individualmente em intervalos inferiores a 5 segundos.
- Deverá realizar a redistribuição do balanceamento do tráfego entre os links de comunicação utilizados pelos CPEs, em caso de falhas nesses links, ou de acordo com as políticas de qualidade pré-definidas;

Compõem a solução da controladora todos os equipamentos, software e licenciamento necessários para que seja possível fazer a operação e gestão dos recursos inerentes a comunicação de dados remota e integração com o ambiente da Rede Governo.

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

A controladora deverá realizar medições de “Latência”/”Jitter”/”Descarte de Pacotes” para cada destino em cada uma das interfaces dos CPEs SD-WAN;
A controladora SD-WAN deverá ser capaz de gerar informações relativas a fluxo de tráfego para análise.
Os equipamentos/appliances, softwares e licenciamentos para controladora de SD-WAN (Software Defined Wide Area Network) e seus respectivos appliances ou servidores de gerência fazem parte do escopo de atendimento a este lote.
Todos os produtos que compõem a controladora devem ser fornecidos com o devido licenciamento, incluindo garantia de atualização de software, de manutenção e de troca do hardware pelo período de vigência do Contrato estabelecido pelo Edital.
Deverá ser ministrado treinamento oficial do fabricante da solução controladora com no mínimo 40 horas para 06 (seis) técnicos da UGO/Prodemge habilitando-os administração da solução, operação e configuração dos equipamentos CPE. Os detalhes do treinamento, que deverá ser online, serão acordados com a UGO durante a fase do acordo operacional e deve ser ministrado antes do período da conclusão da fase de transição.

O fornecedor será responsável pela manutenção da solução e prestação de suporte aos funcionários da UGO na resolução de problemas no uso da solução. Durante 6 (seis) meses, a contar do final da fase do Acordo Operacional, a fornecedor deverá trabalhar em modo de operação assistida junto a equipe da UGO a fim de acelerar o processo de absorção de conhecimentos na fase inicial de operação da solução.

A instalação e a configuração da solução SD-WAN na UGO são de responsabilidade do fornecedor, bem como o fornecimento de toda a conexão de cabos e demais necessidades envolvidas na solução entregue. O planejamento da interconexão da controladora com a infraestrutura central de rede da UGO deverá ser feito junto a equipe da PRODEMGE e os detalhes técnicos tratados no acordo operacional, respeitando o item 8.2 do Termo de Referência.

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);

- Deverão ser utilizados os servidores de NTP disponibilizados pela UGO para esta sincronização

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;

A solução deve implementar políticas de encaminhamento de tráfego por aplicação. 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, conforme planejamento de atualização realizado com a UGO.

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

● O equipamento CPE das unidades remotas deverá ter recurso para se recuperar automaticamente de uma atualização de software ou configuração malsucedida. Caso o equipamento fique inoperante ou sem gerência, este deve retornar à configuração anterior em um prazo máximo de 5 minutos ou após reboot automático, reestabelecendo a comunicação da unidade.

Permitir a distribuição de configurações padrão a todos os equipamentos instalados nas unidades remotas deste lote.

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.

A solução deve suportar a marcação DSCP dos pacotes, inclusive nos CPE´S, de acordo com a aplicação e as políticas configuradas para que a UGO dê o tratamento adequado aos pacotes.

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

Deverá implementar no mínimo cinco classes de QoS, com suas respectivas filas, com mecanismos de priorização de tráfego e gerenciamento de largura de banda (traffic shaping) por classe de QoS e/ou aplicação.

Caso algum link não esteja disponível ou congestionado, a solução deverá permitir ao administrador definir políticas de engenharia de tráfego que levem em consideração as métricas de jitter, latência e perda de pacotes para selecionar, de forma automática ou manual, a critério da UGO, qual caminho uma aplicação irá utilizar de forma dinâmica;

Os equipamentos de SD-WAN fornecidos para as unidades remotas deverão implementar zero-touch em sua primeira implementação ou substituição. Dessa forma, deverá ser possível provisionar a configuração do equipamento a partir da controladora SD-WAN, mesmo antes do equipamento ser conectado à rede.

Será de responsabilidade da prestadora a configuração, envio e instalação dos equipamentos CPE SD-WAN nas unidades remotas.

Nas unidades remotas, em caso de indisponibilidade dos equipamentos da controladora do serviço SD-WAN, a solução deverá manter sob o controle das últimas políticas de segurança aplicadas no equipamento remoto, todo e qualquer tráfego destinado ou proveniente da Internet. A falha da unidade controladora do serviço de SD-WAN não deverá deixar indisponível a comunicação direta com a internet na unidade remota.

A UGO deverá ter acesso irrestrito à solução controladora a ser instalada em seu Datacenter. A solução deverá permitir, no mínimo, 10 (dez) acessos de usuários simultâneos.

A solução oferecida não deverá colocar restrições ao tráfego de Voz sobre IP para os pontos de conexão dos clientes (pontos remotos).

1.1. **Características do CPE´s SD-WAN a serem instalados nas Unidade de Governo**

Deverão suportar endereço IP secundário nas interfaces LAN (IP aliasing).

Deverão suportar vários links de acesso, suportando pelo menos os links previstos nos lotes informados neste termo de referência.

Deverá balancear o tráfego das aplicações entre múltiplos links simultaneamente;

Deverá ser fornecido em formato de equipamento físico dedicado.

Deverá implementar OSPF;

Deverá implementar BGP;

Os equipamentos modelos 1, 2, 3, 4 e 5 deverão possuir pelo menos 4 conexões/interfaces de rede que poderão ser utilizadas por links banda larga, MPLS, satélite ou rádio e comunicação de dados 4G ou superior;
Os equipamentos modelos 6, 7, 8, 9, 10 e 11, deverão possuir pelo menos 6 conexões/interfaces de rede que poderão ser utilizadas por links banda larga, MPLS, satélite ou rádio e comunicação de dados 4G ou superior;

As interfaces do CPE deverão suportar o padrão IEEE 802.1Q.

Deverá implementar a função DHCP Relay Agent e DHCP Server para múltiplas VLANs.

Deverá ser capaz de realizar a identificação do fluxo de aplicações para efetuar o encaminhamento dos pacotes pela melhor rota e para realizar o monitoramento detalhado de tráfego por aplicação.

Deverá permitir o bloqueio e desbloqueio de tráfego por aplicação, IP ou subrede de origem ou destino e porta TCP/UDP.

Deverá possuir capacidade de encaminhamento adequada para tratamento de tráfego das classes Tempo Real sem perda de desempenho das aplicações que fizerem o uso dessas classes.

O equipamento CPE deverá possuir recurso para trabalhar como filtro de conteúdo, filtrando o conteúdo acessado na Internet baseado no usuário que estiver utilizando o acesso.

As URL's deverão ser classificados de forma a ser possível permitir o acesso por categorias.

O recurso de filtro de conteúdo deverá possibilitar a criação de grupos de usuários e ser possível aplicar regras diferenciadas por grupo.

O equipamento CPE não deverá ter nenhum limite de licença para a quantidade de usuários ou dispositivos que estarão internos à rede da unidade.

Os equipamentos CPEs que serão instalados nas unidades deverão estar homologados na ANATEL até a data prevista para a conclusão do ACORDO OPERACIONAL.

1.2. **Sistema de Gerenciamento SD-WAN**

O sistema de Gerenciamento, que será tratada por CONSOLE no item 1.2, é parte integrante da controladora e deverá ser centralizado para o serviço de SD-WAN, concentrando todas as configurações via central de gerenciamento SD-WAN para todos os equipamentos envolvidos nessa solução, através de única interface gráfica

A console deverá suportar contas de usuário/senha estáticas;

A console deverá suportar o método de autenticação externo usuário/conta do servidor Radius;

Todo o provisionamento de serviços deverá ser feito obrigatoriamente por meio de interface GUI e/ou HTTPS na console de gerenciamento;

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

A CONSOLE deverá informar a utilização de Inbound e Outbound de cada circuito de comunicação. Esta capacidade deverá cobrir todos os circuitos contratados e manter a informação de utilização dos circuitos por pelo menos 1 ano. Poderá ser utilizado uma solução diferente da console de gestão do SD-WAN para atender ao item.

A CONSOLE deverá fornecer informações de latência, jitter, descartes de pacotes e erros de cada circuito de comunicação.

A CONSOLE deverá ser do mesmo fabricante dos demais equipamentos da solução.

A CONSOLE deverá informar o status UP/DOWN/SPEED das interfaces LAN e WAN dos equipamentos CPEs;

A CONSOLE deverá informar o status ACESSÍVEL/INACESSÍVEL/CONFIGURATION SYNC/ TUNNELS UP/ TUNNELS DOWN de cada CPE SD-WAN;

A CONSOLE deverá permitir o envio de mensagens syslog referentes aos CPEs SD-WAN para um servidor syslog externo;

A CONSOLE deverá permitir a coleta das medições de “Latência”/”Jitter”/”Descarte de Pacotes” e as estatísticas de interface deverão ser coletadas de cada CPE SD-WAN;

As medições de “Latência”/”Jitter”/”Descarte de Pacotes” deverão ser visíveis na interface gráfica (GUI ou HTTPS) da CONSOLE;

Possuir os contadores de estatísticas de LAN e WAN dos CPEs SD-WAN (bits RX/TX, entrada/saída de pacotes, descartes de pacotes e erros)

A CONSOLE deverá permitir a medição dos fluxos de aplicativos;

Os resultados de desempenho de link e aplicativos deverão ser visualizados em forma de gráfico a partir da GUI da CONSOLE;

1.3. **NÍVEIS DE SERVIÇO**

A controladora deverá ser instalada com redundância de seus equipamentos de modo a permitir alta disponibilidade do ambiente. Na falha de um dos equipamentos da controladora deverá haver outro equipamento que assuma suas funções e mantenha a disponibilidade do ambiente.

A disponibilidade da controladora deverá obedecer ao mesmo nível dos acessos com Redundância Crítica previsto para o perfil I.

1.4. **INFORMAÇÕES ADICIONAIS**

Caberá à Prestadora vencedora toda e qualquer disponibilização de insumos, tanto para os serviços prestados na fase de implantação, operação e manutenção, quanto para a realização do suporte desses serviços aos Pontos Remotos.

Será de responsabilidade do órgão fornecer o cabeamento e infraestrutura na unidade necessária para fazer conexão do acesso adicional ao CPE.

Na instalação do equipamento CPE, será de responsabilidade do fornecedor vencedor do lote 100 fazer as conexões dos links que estiverem disponíveis na unidade para este serviço e certificar que a configuração do equipamento SD-WAN está adequada e utilizando todos os links conectados.

Será de responsabilidade do fornecedor realizar a configuração na controladora e no CPE SD-WAN para que o equipamento instalado na unidade possa receber as configurações iniciais.

Após o recebimento da OS, aberta no portal da Rede Governo, solicitando a instalação do equipamento CPE SD-WAN, o fornecedor terá até 15 dias corridos para realizar a instalação dos equipamentos, porém observadas as seguintes condições:

- Quando a solicitação de instalação for feita de forma automática pelo portal o prazo de instalação de 15 dias passará a contar somente após o aceite da instalação do link que deu início ao processo.
- Seguir o processo de agendamento de instalação previstos neste termo de referência e detalhados no Acordo Operacional.

A conexão de acessos adicionais ao CPE, deverá ser solicitada como alteração de configuração de CPE no portal da Rede Governo e não prevê o deslocamento do técnico do fornecedor da solução SD-WAN até a localidade para realizar a configuração. A configuração dos novos links no CPE será feita remotamente pela Prestadora. Será de responsabilidade do órgão efetuar a ligação dos cabos dos links que estão ligados a sua rede Interna ao equipamento SD-WAN.

Caso seja solicitado pelo gestor do órgão o deslocamento do técnico do fornecedor da solução até a unidade para fazer a(s) configuração(ões) do(s) acesso(s) ao CPE, será cobrado o valor de 50 UFEMG. Este valor será cobrado somente 1 vez por solicitação, independentemente do número de visitas que se fizerem necessárias pelo técnico, até que a(s) conexão(ões) ao equipamento sejam concluídas, exceto se, na(s) visita(s), for constatado pelo técnico e aceito pelo gestor do Órgão, que existem pendências por parte da unidade para que se possa(m) fazer a(s) conexão(ões) dos acessos ao CPE SD-WAN. Neste caso, será cobrado novamente o valor caso seja feita nova solicitação de deslocamento do técnico.

O fornecedor da solução SD-WAN não será responsável, em nenhuma hipótese, sobre a qualidade ou indisponibilidade dos acessos conectados ao CPE SD-WAN.

O CPE SD-WAN instalado deverá comportar o tráfego total previsto para seu modelo neste edital sem comprometimento da performance, mesmo com todos os recursos habilitados e todas as interfaces de dados utilizadas.

O consumo de CPU do equipamento não poderá ter sua média de utilização acima de 65% no horário compreendido entre 09:00h e 11:30h e 14:30h e 16:30h, exceto se os equipamentos estiverem

sob ataque de malware. Esta medição deverá considerar somente os recursos de Firewall, VPN, Identificação de usuário, filtro de conteúdo e controle de aplicação dos equipamentos CPE, excluindo-se para a medição os recursos de Advanced Threat Prevention (ATP) e a criptografia TLS.

Caso o equipamento esteja ultrapassando a média de consumo de CPU prevista e o tráfego de dados não esteja superando a capacidade prevista para seu modelo, o prestador de serviço deverá efetuar a troca do equipamento por outro com maior capacidade de processamento sem ônus para o cliente. Esta troca não poderá ser caracterizada como troca de modelo que ensejaria um aumento de custos para o cliente.

Por exemplo, caso o cliente contrate um CPE SD-WAN do modelo 1, com a capacidade prevista de tráfego até 300 Mbps, quando o tráfego atingir 150 Mbps, caso o equipamento esteja com o consumo de CPU acima de 65% na média com 5 minutos de monitoramento, o fornecedor deverá substituir o equipamento por outro de maior capacidade sem caracterizar que houve troca de modelo, mesmo que o equipamento ofertado seja idêntico a um de modelos superiores, que comportem um tráfego maior, como 500 ou 700 Mbps, sem ônus para o cliente.

Com o uso dos CPE´s SD-WAN, a saída para Internet poderá ocorrer diretamente da unidade, caso estejam utilizando acessos dos lotes 90, 110 e 120, ou a partir de um ponto central. Caso saía diretamente para a Internet a partir da unidade, este acesso deverá ser controlado por recursos do equipamento CPE SD-WAN instalado na unidade utilizando políticas instaladas a partir da controladora.

As unidades para as quais forem contratados acessos nos lotes 90, 110 e 120 deverão obrigatoriamente ter um equipamento CPE SD-WAN e terão todo o tráfego de saída para a Internet direcionado a estes equipamentos. Embora a unidade possa navegar na Internet sem a necessidade que este tráfego vá até a controladora, ele deverá obrigatoriamente passar pelo equipamento CPE SD-WAN que fará o controle de navegação com políticas implantadas a partir da controladora central e em conformidade com os recursos solicitados nos itens abaixo.

A navegação na Internet poderá ser feita de forma autenticada, quando será exigido do usuário que informe usuário e senha para navegação ou de forma não autenticada. O equipamento CPE SD-WAN da unidade deverá permitir no 2º caso que se possa realizar o acesso na Internet sem a necessidade do usuário se autenticar em uma base centralizada e aplicar um conjunto de políticas padrão no equipamento para o acesso deste usuário.

O tráfego corporativo será obrigatoriamente direcionado ao túnel SD-WAN, já o tráfego de acesso à Internet será opcional.

O cliente, porém, poderá direcionar todo o tráfego para o túnel SD-WAN caso queira manter soluções de controle de navegação centralizado já existentes ou que venham a ser instalados pelos Órgãos.

O acesso à Internet diretamente a partir da Unidade será controlado pelo CPE SD-WAN.

Ao contratar link IP dos lotes 90, 110 ou 120, o cliente receberá automaticamente um equipamento CPE SD-WAN, caso a unidade ainda não possua um instalado, do modelo da capacidade imediatamente superior ao link contratado. Para os acessos do lote 110 e 120, será instalado o equipamento do modelo 1.

O cliente, porém, poderá solicitar a substituição do equipamento por um modelo de maior capacidade. Não será aceito a substituição do equipamento por um modelo de menor capacidade que o link contratado.

A cobrança do serviço de virtualização será caracterizada pela capacidade do equipamento CPE SD-Wan e terá seu valor cobrado separadamente do link.

Será possível o cliente contratar o equipamento SD-WAN separadamente, independente de possuir link contratado na Rede Governo.

O link MPLS será contratado sem o equipamento SD-WAN, porém, poderá ser instalado em um equipamento SD-WAN, caso o cliente queira fazer composição de links entre os diversos lotes.

O cliente poderá utilizar qualquer combinação de links no equipamento CPE SD-WAN, limitado à quantidade de interfaces disponíveis nos equipamentos.

A gestão das políticas de segurança da solução SD-WAN ficará a cargo da UGO, que fará a aplicação das políticas de segurança e navegação conforme a solicitação dos clientes obedecendo premissas de segurança da Rede IP Multisserviços.

Será de responsabilidade do vencedor do lote 100 o envio e instalação dos equipamentos CPE SD-WAN nas unidades dos clientes, incluindo as configurações na controladora e equipamento CPE necessárias para o seu funcionamento. Não poderá haver cobrança adicional ao valor mensal do serviço para esta atividade.

1.5. INFORMAÇÕES TÉCNICAS ADICIONAIS DA SOLUÇÃO (CONTROLADORA E CPES)

Toda configuração dos CPEs deverá estar armazenada na controladora central e somente a partir dela deverá ser possível a criação e alteração das configurações.

Deverá ser possível reinstalar as configurações dos equipamentos CPE a partir da controladora central.

O fornecedor será responsável pela instalação, suporte e manutenção da solução.

A autenticação do usuário da solução deverá suportar base de dados externas e a solução deverá ser capaz de autenticar em várias bases distintas, sejam elas LDAP (OpenLDAP) ou Active Directory da Microsoft, concomitantemente.

- Todo hardware, software e licenciamento necessários deve ser considerado;
- Não deverá haver limite para a quantidade de usuários existentes nas bases externas
- Não será exigida a replicação e/ou sincronismo das bases externas com uma base centralizada.
- Uma vez autenticado, a solução deve passar para o CPE SD-WAN, a informação de grupo ou atributo, para que ela seja capaz de definir o nível de acesso do usuário à Internet e redes internas, bem como vincular a credencial aos acessos efetuados, para fins de rastreabilidade;

As bases de autenticação poderão ser distintas conforme o grupo de usuários, ou seja, deve ser possível criar grupos de usuários distintos e cada grupo utilizar uma base de autenticação distinta. O CPE SD-WAN deve ter mecanismo para conseguir coletar informações suficientes do usuário para conseguir identificar a qual domínio pertence para que seja possível, consultar a base de usuário correta para a sua autenticação.

Deverá ser possível a aplicação de políticas por cliente, por grupo, por unidade ou por usuário

Deverá ser possível criar regras referenciando a URL diretamente. As resoluções de nomes das URLs devem ser atualizadas dinamicamente e automaticamente. A solução ofertada não deverá estar restrita a criação de regras somente por endereço IP e portas.

Deverá ser possível fazer backup da base de objetos e das políticas de segurança.

Deverá ser possível restaurar o backup das bases de dados e das políticas diretamente nos menus, de forma rápida, ou seja, abre-se o arquivo das políticas e/ou objetos que se deseja e aplica-se a política novamente nos equipamentos.

Deverá ser possível restaurar a configuração dos equipamentos a partir de recuperação do arquivo de backup feito após última configuração aplicada ao equipamento.

O fabricante da solução ofertada, deverá possuir programas de capacitação e certificação disponíveis para os produtos componentes da solução.

1.5.1. Detalhamento das características técnicas

1.5.1.1. Especificação da solução

1.5.1.1.1. Os equipamentos CPE deverão possuir recursos de Firewall, VPN, IPS, Identificação de usuário, filtro de conteúdo e controle de aplicação.

1.5.1.1.2. As funcionalidades de Firewall, VPN, IPS, Identificação de usuário, filtro de conteúdo e controle de aplicação dos equipamentos CPE devem compartilhar o mesmo equipamento, exceto para o

modelo 11, onde será aceito que as funcionalidades estejam distribuídas em até 3 equipamentos.

1.5.1.2. Capacidade e desempenho

1.5.1.2.1. Suportar no mínimo 128 VLANS.

1.5.1.2.2. Suportar no mínimo 128 VLANS por interface.

1.5.1.3. Alta disponibilidade

1.5.1.3.1. A solução fornecida deverá operar em cluster oferecendo alta disponibilidade com tolerância a falhas tanto para a controladora central quanto para os equipamentos CPE que forem instalados em redundância crítica.

1.5.1.3.2. Na falha de um dos elementos do cluster, não poderá haver nenhuma degradação ou indisponibilidade dos serviços, inclusive das conexões/sessões TCP/IP já estabelecidas no sistema.

1.5.1.3.3. O tempo de convergência entre os equipamentos, caso um dos elementos se torne inoperante, não poderá exceder 60 segundos.

1.5.1.4. Função de FIREWALL dos equipamentos CPE

1.5.1.4.1. Implementar protocolo similar a tecnologia Stateful Inspection baseada em análise granular de informações de estado de comunicação e aplicação para conceder o controle de acesso apropriado.

1.5.1.4.2. Oferecer controle de acesso com suporte a aplicações, serviços e protocolos pré- definidos.

1.5.1.4.3. Permitir a definição de regras a serem verificadas em intervalos regulares de tempo, em determinados dias da semana e horários, em determinados dias e horários do mês.

1.5.1.4.4. Suportar a integração com diretórios LDAP e Microsoft Active Directory (AD) para a autenticação de usuários, de modo que o Firewall possa tomar proveito das informações de profile de usuários armazenadas no LDAP ou AD para realizar a autenticação.

1.5.1.4.5. Suportar pelo menos um dos esquemas de autenticação de usuários tanto para Firewall quanto para VPN's: RADIUS, senha do próprio Firewall, diretório LDAP ou Microsoft Active Directory.

1.5.1.4.6. Suportar controle de aplicações multimídia, tais como voz sobre IP, áudio e vídeo streaming.

1.5.1.4.7. Proteção e suporte às tecnologias de Voz sobre IP SIP e H.323.

1.5.1.4.8. Suportar H.323.

1.5.1.4.9. Suportar IPv6.

1.5.1.4.10. Capacidade de suportar SNMP v2 e v3.

1.5.1.5. Função IPS dos equipamentos CPE

1.5.1.5.1. As funcionalidades devem ser implementadas em um mesmo appliance e a comunicação entre eles deverá ser interna, sem a necessidade de uso de quaisquer interfaces externas, exceto para o modelo 11.

1.5.1.5.2. Deve incluir pelo menos os seguintes mecanismos de detecção/inspeção de IPS:

1.5.1.5.2.1. Assinaturas de vulnerabilidades e exploits;

1.5.1.5.2.2. Assinaturas de ataque;

1.5.1.5.2.3. Bloqueio via lista de reputação de URL e IP com atualização no mínimo diária.

1.5.1.5.2.4. Validação de protocolo;

1.5.1.5.2.5. Detecção de anomalia

1.5.1.5.2.6. Detecção de ataque volumétrico;

1.5.1.5.2.7. Detecção baseada em comportamento.

1.5.1.5.3. O administrador deve ser capaz de configurar a inspeção somente para tráfego entrante (inbound) ou somente para tráfego de saída (outbound).

1.5.1.5.4. O IPS deve incluir definições de ataques que protejam tanto clientes quanto servidores.

1.5.1.5.5. O IPS deve oferecer políticas pré-definidas que podem ser usadas imediatamente.

1.5.1.5.6. O IPS deve incluir a habilidade de interromper temporariamente as proteções para fins de troubleshooting, ou pelo menos suportar que o profile de IPS possa ser configurado em modo monitor.

1.5.1.5.7. O mecanismo de inspeção deve receber e implementar em tempo real atualizações para os ataques emergentes sem a necessidade de reiniciar o equipamento.

1.5.1.5.8. O administrador deve ser capaz de ativar novas proteções baseado em parâmetros configuráveis (severidade da ameaça, proteção dos clientes, proteção dos servidores).

1.5.1.5.9. A solução deve ser capaz de detectar e prevenir as seguintes ameaças: Exploits e vulnerabilidades específicas de clientes e servidores, mau uso de protocolos, comunicação outbound de malware, tentativas de tunneling, controle de aplicações, ataques genéricos sem assinaturas pré-definidas.

1.5.1.5.10. Deve oferecer proteções contra aplicações específicas como peer-to-peer, com a opção de bloquear estas aplicações.

1.5.1.5.11. Para cada assinatura, a descrição da vulnerabilidade e da ameaça e a severidade da ameaça devem estar inclusos.

1.5.1.5.12. Para cada assinatura, ou para todas as assinaturas suportadas, deve incluir a opção de adicionar exceções baseadas na origem e destino.

1.5.1.5.13. A solução deve fazer captura de pacotes para proteções específicas.

1.5.1.5.14. A solução deve ser capaz de detectar e bloquear ataques nas camadas de rede e aplicação, protegendo pelo menos os seguintes serviços: Aplicações web, serviços de e-mail, DNS, FTP, serviços Windows (Microsoft Networking) e VoIP.

1.5.1.5.15. Deve incluir a habilidade de detectar e bloquear ataques conhecidos e desconhecidos, protegendo de, pelo menos, os seguintes ataques conhecidos: IP Spoofing, Ping of death, ICMP Flooding, Port Scanning, SQL Injection, Cross-site scripting e man-in-the-middle.

1.5.1.5.16. A solução deve ser capaz de inspecionar/filtrar portas conhecidas (como http 80 e https 443) a fim de buscar aplicações que possam comprometer a segurança, como P2P (KaZaa, Gnutella, BitTorrent) e IMs (ICQ), mesmo quando elas pareçam ser tráfego válido

1.5.1.5.17. O administrador deve ser capaz de bloquear funcionalidades específicas de páginas Web ou aplicações. Por exemplo: bloquear o chat e a visualização de vídeos no Facebook; bloquear somente a transferência de arquivos no Skype, etc.

1.5.1.5.18. A solução deve possuir capacidade de visualização situacional a fim de monitorar a quantidade de alertas com diferentes severidades.

1.5.1.5.19. A solução deve permitir a configuração de inspeção do IPS baseado em políticas que utilizem o posicionamento geográfico de origens e destinos do tráfego.

1.5.1.5.20. A solução deve permitir a inspeção de tráfego sobre o protocolo HTTPS (Inbound/outbound).

1.5.1.5.20.1. O fornecimento dos certificados necessários ao funcionamento deste recurso será de responsabilidade do fornecedor.

1.5.1.5.21. A solução deve permitir a pré-configuração de perfis de proteção de IPS que podem ser utilizados a qualquer momento.

1.5.1.6. Controle de Aplicação e filtragem de conteúdo

1.5.1.6.1. A solução deve prover a possibilidade de criação de políticas integradas para controle de navegação via navegador e controle de aplicações que utilizem ou não o navegador.

1.5.1.6.2. Deve identificar, permitir ou bloquear aplicações e páginas da Internet.

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

1.5.1.6.4. Reconhecer aplicações de tráfego relacionado, no mínimo, 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, e os softwares bittorrent, gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, anydesk, ultraviewer, ms-rdp, vnc, gmail, youtube, http-proxy, httptunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, googledocs, dentre outras.

1.5.1.6.5. Deve aplicar heurística a fim de detectar aplicações através de análise comportamental do tráfego observado, incluindo, mas não limitado a Encrypted Bittorrent e aplicações VOIP que utilizam criptografia proprietária.

1.5.1.6.6. Deve prover a possibilidade de integrar as funções de controle de aplicações e controle de URL's no mesmo equipamento, sem impossibilitar a ativação de outras funcionalidades de segurança, tais como IPS ou antivírus.

1.5.1.6.7. A administração das políticas de segurança de controle de aplicação e controle de URL's deverá ser centralizada na controladora

1.5.1.6.8. A solução deve possibilitar a criação de políticas granulares para as funcionalidades de controle de aplicação e filtro de URL.

1.5.1.6.9. Deve possibilitar permitir ou bloquear aplicações ou páginas da Internet por pelo menos 5 dos mecanismos abaixo:

a. Aplicação;
b. URL;
c. Categorias ou sub-categorias;
d. Nível de risco;
e. IP/Range de IP's/Redes;
f. Usuários;
g. diferentes grupos de usuários.

1.5.1.6.10. Deve suportar a integração da solução com base externa do Microsoft Active Directory e LDAP, para criação de políticas, possibilitando a criação de regras utilizando:

a. Usuários;
b. Grupo de usuários;
c. Máquinas/host (estações de trabalho);
d. Endereço IP;
e. Endereço de Rede;
f. Combinação das opções acima.

1.5.1.6.11. Deve prover repositório para consulta em tempo real para URL's e aplicações não categorizadas.

1.5.1.6.12. Deve prover serviço de classificação baseado em "nuvem" (Cloud based) para categorização dinâmica do tráfego Web.

1.5.1.6.13. Deve possibilitar a customização de aplicações, páginas da Internet, categorias e grupos que não estão na base de aplicações e URL, para utilização na criação de políticas.

1.5.1.6.14. Deve possibilitar a utilização de no mínimo 2 ações nas regras de controle de URL:

a. liberar;
b. bloquear;

1.5.1.6.15. Deve possibilitar a customização da tela de interação com o usuário.

1.5.1.6.16. Deve permitir o controle de tempo de acesso a URLs de uma determinada categoria. EX: o usuário tem 60 minutos diários para acessar URL´s da categoria “redes sociais” ou o usuário só pode acessar URLs da categoria "redes sociais" em um horário pré-determinado.

1.5.1.6.17. Deve permitir a configuração na própria regra limite de utilização de banda tanto para tráfego de "download" quanto para "upload".

1.5.1.6.18. Deve inspecionar o payload de pacote de dados com o objetivo de detectar através de expressões regulares assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo. A checagem de assinaturas também deve determinar se uma aplicação está utilizando a porta default ou não, incluindo, mas não limitado a RDP na porta 80 ao invés de 3389.

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

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

1.5.1.6.20.1. O fornecimento de certificados necessários para este recurso é de responsabilidade do fornecedor da solução.

1.5.1.6.21. 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 especificas dentro de uma aplicação, incluindo, mas não limitado a compartilhamento de arquivos. Além de detectar arquivos e outros conteúdos que devem ser inspecionados de acordo as regras de segurança implementadas.

1.5.1.6.22. Atualizar a base de assinaturas de aplicações automaticamente.

1.5.1.6.23. Limitar a banda (download/upload) usada por aplicações (traffic shaping), baseado no IP de origem, usuários e grupos do LDAP/AD.

1.5.1.6.24. 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.

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

1.5.1.6.26. Deve suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas, decodificação de protocolos e análise heurística.

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

1.5.1.6.28. 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, mantendo a confidencialidade das aplicações do órgão.

1.5.1.6.29. A criação de assinaturas personalizadas deve permitir o uso de expressões regulares, usando posição no payload dos pacotes TCP e UDP para a criação de assinaturas, minimamente, dos protocolos: HTTP, HTTPS, FTP, SMTP, Telnet, SSH, MS-SQL, IMAP, IMAP e RTSP

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

1.5.1.6.31. Deve possibilitar que o controle de portas seja aplicado para todas as aplicações.

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

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

1.5.1.6.34. Deve possibilitar a diferenciação de aplicações Proxies ou VPNs permitindo o bloqueio.

1.5.1.6.35. Deve ser possível a criação de grupos estáticos de aplicações e grupos dinâmicos de aplicações baseados em características das aplicações como:

1.5.1.6.35.1. Tecnologia utilizada nas aplicações (Client-Server, Browse Based, NetworkProtocol, etc).

1.5.1.6.35.2. Aplicações que usem técnicas evasivas, utilizadas por malwares, como transferência de arquivos e/ou uso excessivo de banda, etc.

1.5.1.6.35.3. Aplicações que usem técnicas evasivas, utilizadas por malwares, como transferência de arquivos e/ou uso excessivo de banda, etc.

1.5.1.7. **CONTROLADORA**

1.5.1.7.1. A administração de todos os elementos do ambiente, deverá ser realizada através da controladora central instalada na UGO.

1.5.1.7.2. As logs deverão ser integradas à controladora centralizada, fazendo com que todos os logs possam ser consultados a partir de um único ponto, facilitando a visualização dos mesmos

1.5.1.7.3. O acesso deve ocorrer obrigatoriamente por meio de interface GUI e/ou HTTPS.

1.5.1.7.4. A controladora deve permitir a criação de regras por intervalo de tempo e/ou período (data e horário de início e fim de validade) para, pelo menos, as funções de Firewall e
Controle de Aplicação e filtragem de conteúdo nos CPEs.

1.5.1.7.5. A controladora deve suportar diferentes perfis de administração, disponibilizando, pelo menos, os seguintes: read/write, read only, gerenciamento de usuários/configurações de sistema e visualização de logs.

1.5.1.7.6. A controladora deve incluir a capacidade de confiar em CAs externas ilimitadas com a opção de verificar o certificado de cada gateway externo ou deve, pelo menos, criptografar a conexão com os gateways gerenciados.

1.5.1.7.7. A controladora deve permitir a criação de diversos perfis de IPS a serem aplicados a diferentes gateways.

1.5.1.7.8. A controladora deve possuir facilidade de busca com, no mínimo, as opções de consulta: quais objetos contêm IP´s específicos ou parte deles, busca por objetos duplicados, busca por objetos não utilizados e listar em quais regras e equipamentos um objeto é utilizado.

1.5.1.7.9. A controladora deve possuir a opção de segmentar as regras de segurança através de rótulos, aplicações ou sessões com a finalidade de organizar as políticas.

1.5.1.7.10. A controladora deve prover a opção de salvar automaticamente ou manualmente versões de políticas.

1.5.1.7.11. A controladora deve possibilitar que sejam efetuadas alterações na política dos CPEs e ou objetos para posterior aplicação das mesmas, em horário pré-definidos, assim não impactando o ambiente durante o horário comercial.

1.5.1.7.12. A controladora deve prover a funcionalidade de mover objetos e serviços entre as regras e de uma lista de objetos e serviços para uma regra.

1.5.1.7.13. Na consulta às logs deve ser possível a filtragem de eventos baseado em diversas categorias (IP origem, porta origem, IP destino, porta destino, interface, categoria ou nome do ataque,

translated IP, translated port, entre outras) simultaneamente e possibilitar a filtragem de eventos relacionados a ação do administrador, tais como login/logout e alterações de política.

1.5.1.7.14. A controladora deve estar habilitada para integração com soluções de mercado focadas em correlação de eventos.

1.5.1.7.15. A Controladora deve incluir um mecanismo automático de captura de pacotes nos CPEs para eventos de IPS com a finalidade de facilitar análise forense.

1.5.1.7.16. A controladora deverá diferenciar os logs para atividades comuns de usuário e logs relacionados à gerencia de políticas de segurança.

1.5.1.7.17. A controladora deverá permitir configurar para cada tipo de regra ou evento pelo menos três das opções: log, alerta, enviar trap SNMP ou envio de e-mail.

1.5.1.7.18. A controladora deve ser capaz de exportar os logs para uma base de dados ou repositório externo.

1.5.1.7.19. Deve permitir que os logs e relatórios sejam reiniciados automaticamente baseado no tempo em que estão armazenados na solução, assim como no espaço em disco usado.

1.5.1.7.20. A controladora deve permitir a visualização do uso dos recursos dos CPEs, tais como utilização de CPU, quantidade de conexões/sessões simultâneas, situação do dispositivo e do cluster (caso estejam instalados com redundância crítica) , status das interfaces de forma centralizada.

1.5.1.7.21. A controladora deve permitir a criação de filtros com base em pelo menos as seguintes características do evento: endereço IP de origem e destino, serviço, tipo de evento, severidade do evento e nome do ataque.

1.5.1.7.22. A controladora deve permitir ao administrador o agrupamento de eventos baseado em qualquer uma das opções de filtragem.

1.5.1.7.23. A controladora deve prover funcionalidades para análise avançada, tais como visualizar a quantidade de tráfego utilizado de aplicações, gráficos e estatísticas.

1.5.1.7.24. A controladora deve suportar a detecção de ataques de força bruta para quebra de credencial.

1.5.1.7.25. A controladora deve permitir a geração de relatórios com horários predefinidos, diários e semanais.

1.5.1.7.26. . A Controladora deverá gerar relatórios consolidados das logs dos CPEs para os itens que se pede abaixo, ou caso não possua alguma das informações abaixo em relatório padrão, deve, pelo menos, permitir a customização do mesmo, inserindo não apenas o que se pede, mas também outras estatísticas úteis:

1.5.1.7.26.1. Principais origens de conexões bloqueadas, seus destinos e serviços;

1.5.1.7.26.2. Principais regras usadas pelos CPE's;

1.5.1.7.26.3. Principais ataques detectados pelos CPE's e indicação das suas principais origens e destinos;

1.5.1.7.26.4. Principais serviços de rede;

1.5.1.7.27. A controladora deve suportar pelo menos os seguintes filtros: unidade, endereço de origem, endereço de destino, usuário e número ou nome do ataque.

1.5.1.7.28. A controladora deve permitir a criação de relatórios personalizados e a personalização de relatórios pré-definidos.

1.5.1.7.29. Deve suportar a distribuição automática de relatórios por e-mail.

Responsável

Alber Vinicius Duque da Silveira/M14782932

Aprovação

Daniel Machado Maia/M13148267

Documento assinado eletronicamente por **Rogério Zupo Braga**, **Superintendente**, em 10/01/2025, às 09:02, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 47.222, de 26 de julho de 2017.

Documento assinado eletronicamente por **Evandro Nicomedes Araujo**, **Servidor(a) Público(a)**, em 10/01/2025, às 09:55, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 47.222, de 26 de julho de 2017.

Documento assinado eletronicamente por **Bruno Meira Tenorio Dalbuquerque**, **Auditor(a) Fiscal da Receita Estadual**, em 10/01/2025, às 11:11, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 47.222, de 26 de julho de 2017.

Documento assinado eletronicamente por **Daniel Machado Maia**, **Diretor (a)**, em 10/01/2025, às 14:36, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 47.222, de 26 de julho de 2017.

Documento assinado eletronicamente por **Alber Vinicius Duque da Silveira**, **Servidor(a) Público(a)**, em 16/01/2025, às 10:17, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 47.222, de 26 de julho de 2017.

A autenticidade deste documento pode ser conferida no site http://sei.mg.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **104942652** e o código CRC **DD9B7E72**.

Referência: Processo nº 1500.01.0079973/2024-83 SEI nº 104942652