SCGÁS COMPANHIA DE GÁS DE SANTA CATARINA	GETIN - Gerência de Tecnologia da Informação
	Memorial Descritivo
	Renovação da solução de proteção de EndPoint já existente na SCGÁS

Resumo: Renovação da solução de proteção de EndPoint já existente na SCGÁS pelo período de 12 meses.

OBJETO:

Renovação da solução de proteção de EndPoint já existente na SCGÁS pelo período de 12 meses.

1. **Especificações técnicas mínimas necessárias para a solução de proteção de EndPoint:**

1.1. A solução de ZTNA (Zero Trust Network Access) ou Acesso à Rede de Confiança Zero, deve ser composta pelos agentes a serem instalados nas máquinas dos usuários finais, bem como por um proxy de acesso, o qual concentrará as requisições dos agentes para acesso às aplicações corporativas.
1.2. Deve ser compatível com o firewall Fortinet FortiGate, permitindo o aproveitamento da base instalada e menor complexidade para os recursos de ZTNA.
1.3. Deve ser fornecido para pelo menos até 500 (quinhentos) dispositivos com suporte por 12 meses.
1.4. A solução de ZTNA deve prover um método de controlar o acesso identificando o dispositivo do usuário, autenticação e postura com base em tags de Zero Trust.
1.5. A solução de ZTNA deve controlar o acesso por sessão, validando o usuário e dispositivo, bem como estabelecendo um túnel criptografado de modo automático para cada sessão.
1.6. A solução de proxy de acesso deve prover suporte a um método de publicação de aplicações corporativas sem necessidade de agente, tal como mediante um portal web SSL a ser acessado por cada usuário.
1.7. Deve permitir o gerenciamento dos agentes remotamente, a partir de uma console central do próprio fabricante a ser disponibilizada em nuvem.
1.8. O licenciamento deve se basear no número de agentes registrados na console de gerenciamento central do mesmo fabricante.
1.9. A solução de ZTNA deve dispor de mecanismos para analisar a requisição TLS Client hello e o cabeçalho HTTP User-Agent para determinar e controlar se a requisição está partindo de um dispositivo não passível de gerenciamento pela console central, tal como um dispositivo móvel.
1.10. A comunicação de controle entre os agentes e a console central deve ser criptografada e acontecer através de TCP e TLS 1.3.

Resumo: Renovação da solução de proteção de EndPoint já existente na SCGÁS pelo período de 12 meses.

1.11. Tanto mediante agente ou sem agente deve ser possível habilitar MFA (autenticação multifator) no processo de autenticação dos usuários.
1.12. A console central deve emitir, assinar e instalar automaticamente um certificado para os agentes contendo ID único de cada agente, número de série do certificado e número de série da console central. O certificado emitido deverá ser único por agente e deverá ainda ser compartilhado com o proxy de acesso.
1.13. Deve ser possível revogar o certificado de um agente por meio da console central.
1.14. O certificado emitido deve ser utilizado no processo de autenticação via ZTNA para identificar o dispositivo do usuário final junto ao proxy de acesso.
1.15. No passo de identificação do dispositivo mediante certificado deve ser possível averiguar se o identificador único do agente e número do certificado coincidem com o que o proxy de acesso conhece. Caso algum desses dados esteja diferente, o acesso deverá ser bloqueado por padrão.
1.16. Deve ser possível configurar o idioma que o agente utiliza para, pelo menos, inglês, português, espanhol ou ainda usar o idioma do sistema operacional.
1.17. A solução deve prover backup automático diariamente, permitindo que em um evento crítico seja possível restaurar os dados de até cinco dias anteriores ao ocorrido.
1.18. Deve ser possível determinar para quais funcionalidades o log deve estar habilitado e permitir que esses dados sejam enviados para a console central.
1.19. Deve suportar pelo menos os seguintes níveis de log: emergência, alerta, crítico, erro, aviso, informativo, debug.
1.20. Deve ser possível exportar os logs diretamente a nível de agente.
1.21. Deve ser possível exigir uma senha para desconectar o agente da console central.
1.22. Deve existir a possibilidade de restringir o usuário de realizar back up da configuração do agente.
1.23. Deve ser possível evitar que o usuário realize um shutdown do agente após estar registrado à console central.
1.24. Deve ser possível enviar os logs para uma ferramenta de consolidação de logs do mesmo fabricante, visando consolidar os logs do proxy de acesso ZTNA em conjunto com os logs dos agentes. Deve ser possível ainda atribuir tags aos endpoints de acordo com o indíce de

Resumo: Renovação da solução de proteção de EndPoint já existente na SCGÁS pelo período de 12 meses.

comprometimento detectado pela solução de consolidação de logs, desde que haja licenciamento instalado para tal.

1.25. Deve ser possível configurar o agente para usar Proxy.
1.26. O agente deve permitir a configuração local via XML (eXtensible Markup Language);
1.27. Deve existir a possibilidade de criar um convite para que os usuários realizem o registro do agente à console central.
1.28. Este convite deve gerar um código a ser inserido no passo de registro do agente e deve ser possível ainda adicionar um passo de verificação da autenticação do usuário, podendo associar a autenticação via base de dados local, LDAP e SAML.
1.29. Deverá ser possível enviar uma notificação por e-mail contendo o código de registro para os usuários finais informados, bem como um link para download do instalador do agente.
1.30. Deve ser possível especificar a validade do código de registro.
1.31. A console central de agentes deve dispor de métodos para determinar se um usuário está on-net ou off-net, ou seja, dentro ou fora da rede corporativa. Deve ser possível ainda criar perfis de configurações distintos para os usuários on-net e off-net.
1.32. A solução deve suportar casos de uso utilizando IPv6 puro, bem como IPv6 em conjunto com IPv4.
1.33. Deve ser possível agrupar agentes em grupos.
1.34. Deve ser possível atribuir grupos de agentes a perfis de políticas específicos.
1.35. Deve ser possível atribuir um nível de prioridade a um perfil de política visando priorizar qual política será utilizada caso um grupo de agentes esteja associado a mais de um perfil de política.
1.36. A console central deve apresentar um resumo das informações de cada endpoint, tais como nome do dispositivo, sistema operacional, IP privado, endereço mac, IP público, estado da conexão com a console central, zero trust tags associadas, detalhes da conexão de rede cabeada e WiFi, detalhes do hardware como modelo do dispositivo, fabricante, CPU, RAM, número de série e capacidade de armazenamento. Deve permitir ainda facilmente ver detalhes de qual política está associada com cada agente, qual versão de agente está em uso em um respectivo endpoint, número de série do agente, identificador único e número de série do certificado emitido para o processo de ZTNA.

Resumo: Renovação da solução de proteção de EndPoint já existente na SCGÁS pelo período de 12 meses.

1.37. O proxy de acesso deve atuar como proxy reverso para aplicações baseadas em HTTP, HTTPS, RDP, SMB, CIFS, SSH, SMTP, SMTPS, IMAP, IMAPS, POP3 e POP3S.
1.38. Para aplicações HTTP e HTTPS deve ser possível realizar um balanceamento de carga entre os servidores cadastrados usando algoritmos como round robin, por peso, baseado no host field do cabeçalho HTTP ou baseado em disponibilidade do servidor.
1.39. Para regras de encaminhamento de tráfego TCP, deve ser possível vincular o servidor com um FQDN visando ofuscar o endereço IP privado do servidor. Deste modo, o agente deve manipular o host file do endpoint visando criar entradas DNS.
1.40. Deve ser possível definir um pool de IPs no proxy de acesso como IPs de origem para comunicação interna com as aplicações privadas.
1.41. A console central deve permitir mapear as regras de destinos de ZTNA a serem sincronizadas com os endpoints e permitir ainda definir para qual tráfego deve ser aplicada criptografia, tal como para tráfego HTTP sem criptografia nativa.
1.42. Deve permitir criação de regras de conformidade que avaliem à postura do dispositivo e auxiliem o administrador no controle de acesso à recursos da infraestrutura, impedindo que um cliente não conforme possa se conectar a redes críticas.
1.43. As regras de conformidade devem gerar tags que são sincronizadas entre os elementos da solução de ZTNA visando controlar a postura de um determinado endpoint diretamente no proxy de acesso.
1.44. A postura deve ser monitorada continuamente para que, caso ocorra uma alteração, o proxy de acesso termine e passe a bloquear a conexão em desacordo com as regras de compliance definidas.
1.45. Deve ser possível construir tags com verificações no endpoint, as quais podem variar de acordo com o suporte ao sistema operacional, tais como se o endpoint está logado no domínio, versão do sistema operacional, chave de registro, processo, nível de vulnerabilidade, CVEs, arquivos existentes em um caminho específico e até mesmo se o antivírus está instalado e sendo executado, além de ser possível validar se as assinaturas estão atualizadas.
1.46. A console central deve permitir exportar e importar tags entre sistemas diferentes por meio de um arquivo JSON.
1.47. Deve ser possível verificar quais endpoints estão associadas com cada tag.

Resumo: Renovação da solução de proteção de EndPoint já existente na SCGÁS pelo período de 12 meses.

1.48. Deve ser possível criar regras no proxy de acesso determinando se um dispositivo necessita estar de acordo com uma ou mais de uma tag simultaneamente, caso a política possua vínculo com diversas tags.
1.49. Deve ser possível criar regras no proxy de acesso vinculando interface de origem, IP de origem, IP de destino, servidor ZTNA, tag ZTNA, grupo de usuários ou usuário.
1.50. Para validação da autenticação dos usuários em conjunto com as regras de proxy de acesso, a solução deve suportar SAML, LDAP, Radius ou base de dados local.
1.51. Deve possibilitar definir funções administrativas realcionadas às permissões dos endpoints, de políticas e de configurações gerais.
1.52. Deve possibilitar aos usuários definirem suas identidades mediante inserção manual, vínculo com LinkedIn, Google ou Salesforce, podendo ainda notificá-los para que esse vínculo possa ser realizado.
1.53. A console central deve possuir funcionalidade de rastreamento de vulnerabilidades a nível de endpoint, permitindo ainda definir o rastreamento no momento do registro, quando ocorrer uma atualização de uma assinatura vulnerável, bem como patches e atualizações de segurança a nível de sistema operacional.
1.54. Deverá ser possível agendar quando o rastreamento deve ocorrer ou vinculá-lo em conjunto com a janela de manutenção automática do Windows.
1.55. Deve permitir que o usuário inicie uma análise de vulnerabilidade sob demanda diretamente no agente.
1.56. Deve ser possível aplicar um patch automático com base no nível de criticidade definido, tal como atualizar automaticamente patches considerados críticos.
1.57. Caso não seja possível aplicar um patch automático para corrigir uma vulnerabilidade, requerendo assim um patch manual, deve ser possível excluir essa aplicação da verificação de compliance.
1.58. Deve ser possível excluir determinadas aplicações da verificação de compliance e até mesmo desabilitar o patch automático.
1.59. O agente deve dispor de um sistema de notificação do tipo popup visando alertar o usuário.
1.60. Deve fornecer informações sobre a vulnerabilidade, patches, versões afetadas, severidade, bem como o CVE correspondente.
1.61. Deve suportar a criação de várias versões de pacotes de instalação.
1.62. As vulnerabilidades encontradas devem ser exibidas diretamente no agente com um link para análise de mais detalhes, englobando nome da vulnerabilidade, severidade, produtos afetados, CVE IDs, descrição,

Resumo: Renovação da solução de proteção de EndPoint já existente na SCGÁS pelo período de 12 meses.

informação do fabricante do software e, quando disponível, link para download do patch no site público do fabricante do software.

1.63. Os resultados da verificação de vulnerabilidades devem incluir pelo menos: lista de vulnerabilidades, número de vulnerabilidades classificadas como críticas, altas, médias e baixas, bem como disponibilizar ainda a possibilidade de aplicar a remediação imediatamente.

1.64. Deve possuir módulo para execução de filtro web a nível de endpoint mediante uso do agente local, realizando a filtragem diretamente no endpoint, podendo ainda ser possível bloquear, permitir, alertar ou monitorar o tráfego web com base na categoria de URL ou filtro de URL customizado.

1.65. O agente deve realizar consultas online ao centro de inteligência do próprio fabricante para determinar a categoria de uma determinada URL visando aplicar o controle de acesso à Internet.

1.66. Deve ser possível configurar o filtro de URL com base em caracteres curingas ou expressões regulares (regex) com as opções de permitir, bloquear ou monitorar.

1.67. O agente para Windows deve permitir inspeção de tráfego HTTPS mediante instalação de plugin disponibilizado pelo mesmo fabricante do agente, o qual deve ser compatível com Google Chrome, Mozilla Firefox e Microsoft Edge.

1.68. Deve ser possível verificar as violações de filtro web diretamente no agente, especificando ainda a URL, categoria, quando a violação ocorreu e usuário.

1.69. Deve ser possível determinar quando o filtro web entrará em ação no agente, se ele deverá estar sempre ativo ou somente quando o usuário estiver fora da rede corporativa.

1.70. Deve ser possível configurar o proxy de acesso para atuar como CASB (Cloud Access Security Broker) em linha, inline do inglês, visando controlar o acesso a aplicações SaaS.

1.71. O proxy de acesso deve manter uma base de aplicações dinâmica, a qual deve ser compartilhada pelo centro de inteligência do fabricante da solução.

1.72. Deve incluir funcionalidades de antivírus, englobando, no mínimo:

1.72.1. Antivírus com recursos de inteligência artificial para detecção;

1.72.2. Controle de dispositivos removíveis (pen drive);

1.72.3. Quarentena automatizada;

1.72.4. Firewall de aplicações instaladas no sistema;

Resumo: Renovação da solução de proteção de EndPoint já existente na SCGÁS pelo período de 12 meses.

1.72.5. Proteção contra ransonware.

2. CONDIÇÕES DE PAGAMENTO

ITEM	PRAZO
Licenciamento	À vista, conforme cronograma de pagamentos da SCGÁS, após o recebimento formal das licenças.
Serviços de Atualização e Configuração	À vista, conforme cronograma de pagamentos da SCGÁS, após a Entrega Total do Projeto.

3. CONDIÇÕES GERAIS:

3.1. O CONTRATADO deverá fornecer as subscrições com validade para 12 meses.

3.2. Todos os serviços e ferramentas a serem contratados devem incluir o serviço de implementação no ambiente existente, bem como a integração com a solução de firewall Fortinet existente, garantindo o perfeito funcionamento. O fornecedor e/ou fabricante deverá enviar previamente todos os requisitos necessários para implementação e realizar a ativação dos produtos e serviços.

3.3. A solução ofertada deverá funcionar em período de 24x7 durante todos os dias de vigência do contrato.

3.4. O prazo de entrega das subscrições é de até 7 (sete) dias após assinatura do contrato.

3.5. O serviço de renovação da solução ofertada poderá ser realizado de forma on-site ou remoto.

3.6. Se o serviço de renovação da solução ofertada for realizado de forma on-site, o CONTRATADO deverá levar em consideração:

3.6.1 As despesas de deslocamento (passagens, táxi, traslados, pedágios, estacionamentos etc.), estadia e alimentação ficam sob responsabilidade do CONTRATADO.

Resumo: Renovação da solução de proteção de EndPoint já existente na SCGÁS pelo período de 12 meses.

3.6.2 Serão responsabilidade integral do CONTRATADO todos os serviços a serem realizados em horário não comercial, eventuais acréscimos sobre o valor-hora normal de seus profissionais, atividades realizadas em Sábados, Domingos e Feriados etc.

3.7. O CONTRATADO deverá manter durante toda a vigência do Contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação.

3.8. Guardar sigilo sobre todas as informações obtidas em decorrência do cumprimento do Contrato, de acordo com o Termo de Confidencialidade disposto no Anexo do Contrato.

3.9. Estar em conformidade com a Lei Nº 13.709, de 14 de agosto de 2018, a LGPD – Lei Geral de Proteção de Dados.

3.10. O CONTRATADO deverá disponibilizar o acesso ao suporte imediatamente após a assinatura do contrato.

3.11. O CONTRATADO deverá disponibilizar por um período de 12 (doze) meses um canal de comunicação (0800, e-mail, site) para suporte técnico ilimitado quando necessário.

3.12. O CONTRATADO deverá disponibilizar durante período de vigência do contrato qualquer versão nova da solução ofertada sem custos para a SCGÁS.

3.13. O CONTRATADO deverá encaminhar as chaves de acesso por e-mail, ou disponibilizar via download ao fiscal do contrato ou pelo correio para a SEDE da SCGÁS, 2º Andar, Gerência de Finanças e Sistemas de Informação, localizada na Rua Antônio Luz, 255 - Centro Empresarial Hoepcke - 88010-410 - Florianópolis - SC.

ASSINADO DIGITALMENTE
Validade jurídica assegurada conforme MP 2.200-2/2001, que instituiu a ICP-Brasil
BRyTecnologia

ALISON LUIZ MARTINS SCHVEITZER:91992362919.923.629-04
Emitido por: AC SyngularID Multipla
Data: 10/11/2025

Alison Luiz Martins Schveitzer
Analista de Tecnologia da Informação