

## TERMO DE REFERÊNCIA FIREWALL

### 1. OBJETO

O presente objeto se destina a aquisição de dois appliances de firewall (UTM ou NGFW) que se integrem como uma solução de segurança completa para permitir gerenciamento centralizado, visibilidade da segurança e qualidade para segurança de rede do Prefeitura Municipal do Rio Grande. A solução ofertada deve compreender dois equipamentos idênticos em configuração de hardware e licenciados para operar com todas suas funcionalidades em cluster ativo/passivo ou ativo/ativo por 60 meses.

Os equipamentos ofertados deverão ser novos, estarem atualmente em linha de produção e constar no catálogo mais recente do fabricante. Não serão aceitos equipamentos usados, remanufaturados, de demonstração ou composições feitas única e exclusivamente para o presente certame.

### 2. JUSTIFICATIVA

A Prefeitura Municipal do Rio Grande, visando melhor prestação de serviços, performance e controle de seus sistemas, sites e dados, necessita a implantação de equipamentos de como firewall com alto desempenho, que possibilitem velocidade, confiabilidade e disponibilidade para todos os serviços e dados processados e armazenados no Datacenter do município. Pensando na atualização tecnológica necessária para atender a demanda dos sistemas internos e dos serviços e sites disponibilizados, se faz necessário realizar a substituição dos equipamentos legados que possuem baixo desempenho, falta de garantia e suporte por parte do fabricante e alto consumo de energia elétrica. O que os configura como defasados.

### 3. TABELA

Item	Produto	Quantidade	Média*
01	Dispositivo de Segurança de Redes (Firewall Utm) Primário com Assinatura e Suporte por 60 Meses	01	267.257,48
02	Dispositivo De Segurança De Redes (Firewall Utm) Secundário Com Assinatura E Suporte Por 60 Meses	01	51.041,90
Total			318.299,38

\*O valor máximo da proposta serão os valores médios da Tabela 3.

### 4. CARACTERÍSTICAS

- 4.1.O equipamento de firewall deve suportar configuração de quatro zonas de segurança, sendo externa, privada, opcional (DMZ) e customizada.
- 4.2.O equipamento de firewall deve suportar endereçamento IP estático e dinâmico [DHCP e PPPoE nas interfaces externas].
- 4.3.O equipamento de firewall deve possuir funcionalidades de DHCP relay que permitam a adição de três servidores DHCP simultâneos.
- 4.4.O equipamento de firewall deve permitir DHCPv6 em interfaces externas.
- 4.5.O equipamento de firewall deve possuir um throughput de 34 (trinta e quatro) Gbps para firewall e 5.4 (cinco ponto quatro) Gbps para UTM (combinando GAV e IPS).
- 4.6.O equipamento de firewall deve suportar no mínimo 8.200,000 (oito milhões e duzentas mil) conexões simultâneas.
- 4.7.O equipamento de firewall deve possuir funcionalidades de UTM/NgFW, incorporando as funcionalidades de filtro WEB e URL, IPS, GAV, Controle de

*Doe órgãos, doe sangue: Salve vidas!*



Aplicação, DLP e proteção contra ameaças day-zero, filtro DNS e possuir capacidade de detecção e resposta de malwares, utilizando correlação de dispositivos de rede.

- 4.8. O equipamento de firewall deve suportar a implementação de políticas de segurança na camada de aplicação (camada 7), funcionalidade também conhecida como proxies de aplicação.
- 4.9. O equipamento de firewall deve possuir políticas na camada de aplicação pré-configuradas com proteção padrão para suportar os seguintes protocolos:
- a) HTTP / HTTPS
  - b) POP3 / POP3S
  - c) IMAP / IMAPS
  - d) SMTP / SMTPS
  - e) FTP
  - f) DNS
  - g) SIP
  - h) H323
- 4.10. O equipamento de firewall deve suportar autenticação via RADIUS, SecurID, LDAP e Active Directory.
- 4.11. O equipamento de firewall deve suportar autenticação transparente de usuários (Single Sign On) de AD e RADIUS.
- 4.12. O equipamento de firewall deve permitir habilitar e desabilitar SSLv3 em proxies de HTTPS/SMTP.
- 4.13. O equipamento de firewall deve suportar a configuração de regras de proxy explícito para aceitar solicitações de clientes e buscar informação em nome dos clientes.
- 4.14. O equipamento de firewall deve suportar a habilidade de configurar um proxy SMTP para analisar documentos com macros embutidas e o

equipamento também deve possuir uma opção para remover estes macros antes de enviar o documento para seus destinatários.

- 4.15. O equipamento de firewall deve possuir certificados digitais do tipo self-signed para executar deep inspection de pacotes via proxy SMTP sobre TLS.
- 4.16. O equipamento de firewall deve executar deep content inspection de dados em proxy HTTPS.
- 4.17. O equipamento de firewall deve limitar o acesso de usuários a contas Google pessoais, e simultaneamente permitir acesso ao Google Apps for Work/Google Apps for Educators.
- 4.18. O equipamento de firewall deve permitir definir o intervalo de tempo entre tentativas de login incorretas para disparar ações de bloqueio.
- 4.19. O equipamento de firewall deve possuir a funcionalidade de NTP server e possuir uma política criada automaticamente de NTP para equipamentos conectados em sua rede interna.
- 4.20. O equipamento de firewall deve suportar DNS dinâmico em pelo menos 3 (três) dos seguintes provedores:
  - a) DynDNS.org
  - b) No-IP.com
  - c) dynu.com
  - d) dnsdynamic.org
  - e) afraid.org
  - f) duckdns.org
- 4.21. O equipamento de firewall deve possuir defesas de ataques fragmentados, permitindo que o firewall monte os pacotes fragmentados antes de encaminhá-los a redes internas.
- 4.22. O equipamento de firewall deve conseguir filtrar conteúdo nos protocolos mais comuns, assim como filtrar conteúdo tipo "MIME".

- 4.23. O equipamento de firewall deve proteger e-mails internos contra open relay. Ele deve ser capaz e ser configurado para domínios de e-mail aceitos no ambiente.
- 4.24. O equipamento de firewall deve permitir a configuração de limites para detecção de ataques de flood e Denial of Service (DoS) além de distributed denial of service (DDoS).
- 4.25. O equipamento de firewall deve suportar Protocol Anomaly Detection (PAD) para DNS e outros tipos de protocolos.
- 4.26. O equipamento de firewall deve suportar Server Name Indication (SNI) para configurar domínios para funcionalidades de bloqueio, inspeção ou permissão.
- 4.27. O equipamento de firewall deve suportar bloqueio e gerenciamento de tráfego por domínios especificados por FQDNs (Fully Qualified Domain Names) a fim de bloquear sites disponibilizados por Content Delivery Networks (CDNs).
- 4.28. O equipamento de firewall deve suportar o bloqueio de domínios através de wildcard.
- 4.29. O equipamento de firewall deve permitir a criação de políticas por IP utilizando wildcard.
- 4.30. O equipamento de firewall deve suportar configuração por política de bloqueio de conexões inbound e outbound para um país (ou conjunto de países).
- 4.31. O equipamento de Firewall deve suportar o cliente a atender ao menos 06 requerimentos do padrão PCI DSS, sendo estes:
- a) Requerimento 1
  - b) Requerimento 2
  - c) Requerimento 5
  - d) Requerimento 6
  - e) Requerimento 10

*Doe órgãos, doe sangue: Salve vidas!*



- f) Requerimento 11
- 4.32. O equipamento deve suportar ações baseadas em conteúdo HTTP e HTTPS, permitindo o roteamento de solicitações HTTP ou HTTPS descritografadas para diferentes servidores da web internos com base no conteúdo do cabeçalho do host HTTP e da solicitação HTTP.
- 4.33. A ação baseada em conteúdo HTTP e HTTPS deve permitir, além do redirecionamento baseado em cabeçalho do host, o descarregamento de TLS/SSL.
- 4.34. A ação baseada em conteúdo HTTP e HTTPS deve suportar acionamento via padrão do cabeçalho e via expressão regular.
- 4.35. O equipamento de firewall deve possuir pelo menos 3 (três) das seguintes certificações/compliance:
- a) ANATEL
  - b) CE
  - c) FCC
  - d) RoHS
  - e) WEEE
  - f) REACH
  - g) IC
  - h) VCCI Class A ITE
  - i) Taiwan Class A
- 4.36. O equipamento de firewall deve integrar a autenticação com mecanismos de Autenticação Forte de Múltiplo Fator (MFA) através do protocolo SAML.
- 4.37. O equipamento de firewall deve oferecer integração a mecanismos de Autenticação Forte de Múltiplo Fator (MFA) através do Protocolo Radius para as formas de VPN suportadas, sendo no mínimo SSL VPN (cliente), através da implementação PAP, L2TP (clientless) através da implementação

MSCHAPv2 e IKEv2 (clientless) através da implementação EAP-MSCHAPv2.

- 4.38. O Fabricante da solução deve disponibilizar uma plataforma de abertura de chamados para suporte sem limite de número de chamados enquanto o licenciamento do dispositivo estiver válido.
- 4.39. O Fabricante deve possuir estoque de RMA dentro do Brasil a fim de agilizar a entrega de produtos em caso de falha/quebra.
- 4.40. O equipamento de firewall deve aplicar políticas granulares para restringir o tráfego de países considerados arriscados de acordo com a política de segurança do órgão contratante de acordo com o tipo de tráfego, porta, protocolo, endereço, usuário ou grupo de origem assim como destino.
- 4.41. O equipamento de firewall deve permitir outros tipos de tráfego que não ofereçam ameaças semelhantes, como DNS ou Mail para / de países que tenham certos protocolos bloqueados quando considerados perigosos pela política de segurança do órgão.
- 4.42. A solução de UTM deve possuir funcionalidade de Gateway Wireless Controller (GWC) incluída e licenciada na solução;
- 4.43. A solução de UTM deve suportar SSO para soluções RADIUS.
- 4.44. A solução de UTM deve rastrear as sessões de usuários via SSO para RADIUS.
- 4.45. A solução de UTM deve suportar o download e alteração de diferentes versões de configuração para equipamentos, possibilitando utilizar a mesma configuração para hardwares distintos e versões de SO distintas.
- 4.46. A solução de UTM deve suportar SSO redundantes a fim de eliminar o ponto único de falha de um único agente SSO garantindo maior disponibilidade de recursos em rede.
- 4.47. A solução de segurança deve ser capaz de proteger cada localidade de ameaças provenientes da internet utilizando UTM (Unified Threat Management), combinando serviços de firewall, proteção anti-virus,

***Doe órgãos, doe sangue: Salve vidas!***



prevenção de intrusão, filtro de conteúdo, anti-spam, DLP, proteção contra malware avançado e VPN site-to-site e client-to-site para usuários remotos, em um único equipamento.

- 4.48. A solução de UTM deve suportar VPN Mobile.
- 4.49. A solução de UTM deve estar licenciada para suportar pelo menos 700 (setecentas) VPNs Mobile usando IPsec.
- 4.50. A solução de UTM deve estar licenciada para suportar ao menos 700 (setecentos) usuários mobile usando VPN SSL.
- 4.51. A solução de UTM deve permitir o download do cliente de VPN SSL através do próprio firewall ou apenas do arquivo de configuração para ser importado em clientes de mercado.
- 4.52. A solução de UTM deve ser compatível com clientes SSL para Windows XP, Vista, 7, 8, 10, MAC OS, Android e IOS.
- 4.53. A solução de UTM deve suportar VPN entre localidades (site-to-site VPN).
- 4.54. A solução de UTM deve estar licenciada para suportar pelo menos 700 (setecentas) VPNs entre escritórios utilizando IPsec.
- 4.55. A solução de UTM deve suportar iterações com outros produtos e fabricantes que suportem o padrão IPsec.
- 4.56. A solução de UTM deve suportar os seguintes métodos de autenticação:
  - a) DES
  - b) 3DES
  - c) AES 128 -, 192-, 256-bit
- 4.57. A solução de UTM deve suportar pelo menos 2 (dois) dos seguintes métodos de criptografia:
  - a) SHA-2
  - b) MD5
  - c) IKE Pre-Shared Key

*Doe órgãos, doe sangue: Salve vidas!*



- d) 3rd Party Cert.
- e) AES with CBC and GCM
- 4.58. A solução de UTM deve suportar Dead Peer Detection (DPD).
- 4.59. A solução de UTM deve suportar VPN site-to-site com IKEv2.
- 4.60. A solução de UTM deve suportar VPN client-to-site com IKEv2.
- 4.61. A solução de UTM deve suportar Perfect Forward Secrecy (PFS) com chaves Diffie-Hellman (ou Diffie-Hellman-Merkle).
- 4.62. A solução de UTM deve suportar VPN Failover (reestabelecer a VPN através de um segundo link em caso de falha do link primário).
- 4.63. A solução de UTM deve suportar VPN IPSEC (UDP1518) com um throughput igual ou maior que 7 (sete) Gbps.
- 4.64. A solução de UTM deve permitir criar interfaces virtuais para VPNs e rotear tráfego utilizando VPNs site-to-site com protocolos de roteamento dinâmico.
- 4.65. A solução de UTM deve suportar VPN site-to-site sobre TLS.
- 4.66. A solução de UTM deve suportar VPN client-to-site com SSL com VLANs e redes secundárias através de configuração de roteamento.
- 4.67. A solução de UTM deve permitir visualizar estatísticas de VPN em interfaces virtuais, gateways, tunnel types, para qualquer tipo de usuário.
- 4.68. A solução de UTM deve permitir visualizar mensagens de diagnóstico de VPN para ajudar a remediar e realizar a resolução de problema pelos administradores do sistema.
- 4.69. A solução de UTM deve suportar VPN em interfaces virtuais e realizar Failover entre as mesmas.
- 4.70. A solução de UTM deve suportar filtro de conteúdo Web.
- 4.71. A solução de UTM deve suportar filtro de conteúdo URL.
- 4.72. A solução deve permitir que o filtro trabalhe por categorias, ajustado por grupos de usuário e possuir um mínimo de 82 (oitenta e duas) categorias.

***Doe órgãos, doe sangue: Salve vidas!***



- 4.73. A solução de UTM deve permitir exceções no filtro de conteúdo por meio de whitelist.
- 4.74. A solução de UTM deve apresentar ao usuário uma tela de aviso indicando que a categoria do website acessado não está de acordo com as políticas do órgão, permitindo ao mesmo seguir adiante após clicar em um "aceite".
- 4.75. A solução de UTM deve suportar uma base de dados atualizada dinamicamente localizada na nuvem ou disponível em uma solução de máquina virtual compatível com VMWARE ou Hyper-V.
- 4.76. A solução de UTM deve filtrar conteúdo em múltiplas línguas, incluindo, mas não limitado a: português, inglês, alemão, espanhol, francês, italiano, holandês, japonês, chinês tradicional e simplificado.
- 4.77. A solução de UTM deve identificar e bloquear no mínimo 1800 (mil e oitocentas) aplicações diferentes, incluindo controle granular de aplicação, como telas de login e metodologias específicas de transferência de arquivo.
- 4.78. A solução de UTM deve suportar atualização automática de assinaturas de aplicação.
- 4.79. A solução de UTM deve reconhecer pelo menos as seguintes aplicações: bittorrent, gnutella, skype, facebook, linked-in, twitter, , twitter reply, twitter retweet, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs, aol mail, msft-store, spotify, twitch.tv, vevo, winamp, appletalk echo, sftp, sql-net, vmnet, quic, cisco tdp, openvpn, tinyvpn, dotvpn, tor, yammer, fortnite, diablo3, cs game, call of duty, LoL, second life, edonkey, emule, netscout, klogin, etc.

- 4.80. A solução de UTM deve suportar o bloqueio de tráfego vindo de IPs maliciosos reconhecidos por base de dados de blacklists disponíveis no mercado.
- 4.81. A solução de UTM deve suportar o bloqueio de tráfego de botnets reconhecidos por base de dados de blacklist disponíveis no mercado.
- 4.82. A solução de UTM deve suportar e estar licenciada para aplicar filtro de aplicação no próprio hardware UTM.
- 4.83. A solução de UTM deve suportar a configuração de exceções para filtro de aplicação.
- 4.84. A solução de UTM deve ter suas assinaturas de aplicação atualizadas automaticamente e regularmente.
- 4.85. A solução de UTM deve suportar e esta licenciada para a funcionalidade de antivírus de borda fornecida por fabricantes líderes no segmento de antivírus no mesmo equipamento UTM.
- 4.86. A solução de UTM deve receber atualizações de assinaturas de antivírus automaticamente.
- 4.87. A solução de UTM deve suportar a opção de quarentena para e-mails recebidos.
- 4.88. A solução de UTM deve suportar whitelists para e-mails a fim de receber mensagens de domínios confiáveis em seu ambiente.
- 4.89. A solução de UTM deve ter a capacidade de detectar e bloquear spyware.
- 4.90. A solução de UTM deve ser capaz de classificar Potentially Unwanted Programs (PUPs) como malware.
- 4.91. A solução de UTM deve ser capaz de escanear todos os arquivos comprimidos (.zip, .tar, .rar, .gzip) com até 5 (cinco) níveis de compressão ou mais.
- 4.92. A solução de UTM deve permitir separar uma ação configurável para tratar arquivos criptografados.

*Doe órgãos, doe sangue: Salve vidas!*



- 4.93. A solução de UTM deve suportar os principais protocolos: HTTP, FTP, SMTP, POP3.
- 4.94. A solução de UTM deve possuir pontuação de reputação para cada URL/IP acessado, permitindo o by-pass do escaneamento do AV a fim de otimizar a performance da solução ofertada. O score deve ser estipulado baseado em informação recebida pela nuvem do fabricante.
- 4.95. A solução de UTM deve possuir pontuação de reputação para cada URL/IP acessado, permitindo o bloqueio a estes endereços com reputação (score) baixa devido a histórico de vírus e/ou outros tipos de malware. O score deve ser estipulado baseado em informação recebida pela nuvem do fabricante.
- 4.96. A solução de UTM deve possuir máquina (engine) de antivírus de borda.
- 4.97. A solução de UTM deve possuir máquina (engine) de análise heurística avançada de borda.
- 4.98. A solução de UTM deve possuir máquina (engine) de antivírus de borda com inteligência artificial.
- 4.99. A solução de UTM deve detectar perfis de arquivos maliciosos e benignos. Esses perfis incluem comportamentos e características de arquivos para fornecer uma visão abrangente da ameaça em potencial.
- 4.100. A solução de UTM deve avaliar a ameaça em potencial. O Antivírus com Inteligência Artificial deve identificar ameaças considerando elementos de um arquivo, sem abrir ou executar o malware.
- 4.101. A solução de UTM deve bloquear malware sem assinaturas. O Antivírus com Inteligência Artificial deve identificar uma ameaça, e bloquear o malware automaticamente, impedindo que a carga mal-intencionada entre em sua rede.
- 4.102. A solução de Antivírus com Inteligência Artificial não deve necessitar estar em contato com qualquer sistema de base de dados externo ou baixar

*Doe órgãos, doe sangue: Salve vidas!*



assinaturas para operar, protegendo apenas através da tecnologia de Machine Learning sem qualquer tipo de atualização.

- 4.103. A solução de UTM deve possuir capacidades de Anti-Spam ativadas e licenciadas no mesmo hardware.
- 4.104. A solução de UTM deve possuir em sua solução de anti-spam uma opção de quarentena.
- 4.105. A solução de UTM deve possuir em sua solução de anti-spam integração com análise de antivírus com o anti-spam (detecção e surto de vírus).
- 4.106. A solução de UTM deve possuir em sua solução de anti-spam capacidade para bloquear spam em diversos idiomas.
- 4.107. A solução de UTM deve possuir em sua solução de anti-spam capacidade para bloquear spam baseado em imagem além de spam baseado em texto.
- 4.108. A solução de UTM deve estar completamente licenciada e apta para funcionalidade de IPS no mesmo hardware.
- 4.109. A solução de UTM deve oferecer suporte para atualizações automáticas de assinaturas de IPS.
- 4.110. A solução de UTM deve oferecer suporte para o IPS conduzir análises na camada de aplicativos (camada 7), definir o nível de severidade do ataque e gerar alarmes remotos para notificações de eventos.
- 4.111. A solução de UTM deve oferecer suporte para bloqueio automático de fontes conhecidas de ataque.
- 4.112. A solução de UTM deve oferecer suporte a todos os principais protocolos: HTTP, FTP, SMTP, POP3, IMAP.
- 4.113. A solução de UTM deve oferecer throughput de IPS de, no mínimo, 10 (dez) Gbps.
- 4.114. A solução de UTM deve oferecer suporte para acessar atualizações de assinatura e, manualmente, instalar assinaturas em modo off-line.

***Doe órgãos, doe sangue: Salve vidas!***



- 4.115. A solução de UTM deve permitir que cada ameaça de IPS seja tratada de forma específica, de acordo com seu nível de ameaça.
- 4.116. A solução de UTM deve estar plenamente licenciada para oferecer recursos de prevenção contra perda de dados (DLP) no mesmo hardware.
- 4.117. A solução de UTM deve oferecer suporte DLP para iniciativas de conformidade com PCI e HIPAA.
- 4.118. A solução de UTM deve oferecer suporte a regras predefinidas de DLP para números de identidade nacionais/internacionais, dados de cartão de crédito, dados de endereço, informações pessoais identificáveis (PII) e informações sobre saúde.
- 4.119. A solução de UTM deve fornecer regras predefinidas de DLP para o Brasil.
- 4.120. A solução de UTM deve estar plenamente licenciada para oferecer com recursos de detecção de malware avançado no mesmo hardware.
- 4.121. A solução de UTM deve oferecer suporte para emulação completa de sistema para detectar malware avançado durante o tempo de execução em uma Next Generation Sandbox na nuvem, totalmente mantida pelo fornecedor.
- 4.122. A solução de UTM deve oferecer suporte de APT para todos os executáveis de Windows, zip, PDF, objeto do Microsoft Office, Mac OS, Javascript e tipos de arquivo APK do Android.
- 4.123. A solução de UTM deve fornecer relatórios detalhados com análises acionáveis que identificam um arquivo como malware.
- 4.124. A solução de UTM deve incluir uma lista sumário de indicadores de ameaças que informam por que o arquivo foi bloqueado como malware.
- 4.125. A solução de UTM deve incluir um serviço em nuvem que forneça correlação em tempo real entre eventos de segurança de end-point e de rede através da análise de logs de UTM, um agente instalado no end point, um agente instalado do Active Directory e uma Nuvem de sincronia e coleta

*Doe órgãos, doe sangue: Salve vidas!*



de dados forenses sobre diferentes tipos de ameaças que ocorrem ao redor do mundo.

- 4.126. O agente para end-point deve estar licenciado para proteger no mínimo 220 (duzentas e vinte) estações de trabalho/servidores.
- 4.127. A solução de UTM deve prover detecção de ameaças em tempo real através da correlação da inteligência sobre ameaças, análise comportamental, análise heurística avançada, sandboxing e machine learning.
- 4.128. A solução de UTM deve normalizar, priorizar e dar um score para cada evento de segurança que ocorre na rede e no end-point.
- 4.129. A solução de UTM deve prover resposta automática aos incidentes e indicadores de níveis de ameaça.
- 4.130. A solução de UTM deve prover emulação completa do sistema a fim de detectar malware avançado durante a execução em uma Next Generation Sandbox na nuvem para conteúdo suspeito detectado no end-point.
- 4.131. A solução de UTM deve escalar e responder cada evento automaticamente baseado no resultado da análise do sandbox.
- 4.132. A solução de UTM deve prover detecção de malware avançado compatível com os sistemas Windows, macOS e Linux.
- 4.133. A solução de UTM deve utilizar informação de ataques de forma inteligente, compartilhando estes dados entre o UTM e os end-points.
- 4.134. A solução de UTM deve prover relatórios detalhados com análise que identifica as atividades de infecção e remediação.
- 4.135. A solução de UTM deve possuir uma solução de host ransomware prevention (prevenção ao sequestro de dados) e e prevenir localmente, sem a necessidade de acesso a internet, tentativas de criptografia do host.
- 4.136. A solução deve possibilitar a criação de diversas regras por grupo de máquinas, mais, ou menos restritivas, de acordo com as políticas de segurança definidas pelo administrador do sistema.

***Doe órgãos, doe sangue: Salve vidas!***



- 4.137. A solução de UTM deve fornecer proteção anti-malware de blacklists de domínios por filtro de DNS.
- 4.138. A solução de UTM deve fornecer filtro de conteúdo a nível de domínio.
- 4.139. A solução de UTM deve prover educação contra Phishing para usuários que visitem domínios maliciosos.
- 4.140. A solução de UTM deve prover detalhes de contexto da ameaça em cada alerta.
- 4.141. A solução de UTM deve fornecer relatórios com dados detalhados e análise aprofundada identificando o arquivo como malware.
- 4.142. A solução de UTM deve prover gerenciamento centralizado da funcionalidade de Filtro de DNS em nuvem proprietária do fabricante.

## 5. PORTAL DE ACESSO

- 5.1. Deve permitir a administradores realizar o suporte de implementação e acesso centralizado às aplicações na nuvem e recursos internos via RDP e SSH. SAML deve prover integração com soluções de SSO e provedores de MFA além das autenticações permitidas pelo UTM, inclusive, Active Directory, RADIUS e Base de Dados local.
- 5.2. A solução de UTM deve incluir no suporte a SAML no portal de acesso para a integração com SSO e provedores de MFA, que atuem como identity provider (IDP).
- 5.3. A solução de UTM deve suportar a criação de acesso remoto de sessões RDP ou SSH sem a necessidade de hardware adicional (ou seja, clientless).
- 5.4. A solução de UTM deve possuir um local centralizado e customizável a fim de prover um ponto de login único para acesso a aplicações em nuvem e recursos RDP/SSH internos.
- 5.5. A solução de UTM deve integrar a autenticação do portal de acesso com mecanismos de autenticação do firewall, incluindo RADIUS.

## 6. DESCOBERTA DE REDE

*Doe órgãos, doe sangue: Salve vidas!*



- 6.1. Deve permitir que administradores de rede realizar o escaneamento a rede a partir do Firewall, gerando um mapa visual de cada nó (end point) na rede além de ter visibilidade de quais protocolos, sistemas operacionais e portas estão abertas na rede. O dashboard de visibilidade e gerenciamento desta funcionalidade deve ser customizável e configurável de forma simples e intuitiva, podendo ser realizado em minutos.
- 6.2. A solução de UTM deve escanear a rede a fim de descobrir os equipamentos conectados e apresentar as suas portas abertas, IP, MAC Address, host, serviços e versão de sistema operacional.
- 6.3. A solução de UTM deve aproveitar a funcionalidade de escaneamento para detectar equipamentos não aprovados e aprovados na rede.
- 6.4. A solução de UTM deve utilizar as seguintes ferramentas para detectar e determinar os detalhes de dispositivos no mapa de rede:
- a) Varredura de rede.
  - b) Detecção de DHCP.
  - c) Detecção HTTP.
  - d) Detecção SSL VPN e IKE para dispositivos móveis.
- 6.5. A solução de UTM deve coletar os seguintes detalhes dos dispositivos no mapa de rede:
- a) IP address.
  - b) Device name and host name.
  - c) MAC address.
  - d) Operating system and services.
  - e) Open network ports.
- 6.6. O escaneamento de redes pode ser agendado para ocorrer automaticamente ou iniciar manualmente via interface web.

## 7. CAPACIDADES DE REDE

- 7.1. Cada unidade de Firewall deve possuir, ao menos, as seguintes interfaces:

*Doe órgãos, doe sangue: Salve vidas!*



- a) 8 (oito) interfaces x 10/100/1000 BaseT.
- b) 1 (uma) interface serial dedicada ao gerenciamento com conector padrão RJ45.
- c) 4 (quatro) interfaces 10Gbe livres para uso, com transceptores SFP+ no padrão 10GBase-SR inclusos.
- d) As interfaces do equipamento devem permitir serem configuradas como qualquer uma das zonas de segurança indicadas no item 4.1.
- e) O firewall deve possuir ao menos 1 (uma) interface USB que possa ser utilizadas para:
  - 7.1.e.1. Acesso failover por Modem USB;
  - 7.1.e.2. Storage Externo para salvar copias de Backup automaticamente de Configuração, sistema operacional e arquivos de troubleshooting;
- 7.2. O firewall deve suportar configurações de multi-wan, permitindo, ao menos, 4 (quatro) conexões externas com a internet simultaneamente.
- 7.3. O firewall deve operar com interfaces em modo de failover.
- 7.4. O firewall deve suportar a funcionalidade de failover para um modem USB diretamente conectado.
- 7.5. O firewall deve suportar a configuração de um modem USB como uma interface a ser utilizada em Failover de WAN.
- 7.6. O firewall deve suportar interfaces externas configuradas em modo Round Robin, com pesos configuráveis.
- 7.7. O firewall deve suportar interfaces externas configuradas com a funcionalidade de "overflow", permitindo o uso de links externos secundários quando o principal for excedido.
- 7.8. O firewall deve suportar um mínimo de 700 (setecentas) VLANs.
- 7.9. O firewall deve suportar controle de banda por usuário, grupo de usuários, políticas e protocolo.
- 7.10. O firewall deve suportar controle de banda por interface.

***Doe órgãos, doe sangue: Salve vidas!***



- 7.11. O firewall deve suportar controle de banda por endereço de IP e VLAN.
- 7.12. O firewall deve suportar controle de banda por aplicação e categorias de aplicações.
- 7.13. O firewall deve suportar consumo de banda e cota de tempo por usuário. Em caso de atingimento de cota, uma mensagem deve ser apresentada ao browser do usuário notificando o atingimento da cota.
- 7.14. O firewall deve suportar sua implementação como Rounting Mode e Transparent Bridge Mode.
- 7.15. O firewall deve operar em modo de alta-disponibilidade, podendo atuar como ATIVO-PASSIVO e ATIVO-ATIVO.
- 7.16. Firewall deve suportar NAT e PAT.
- 7.17. Firewall deve suportar load balancing entre links
- 7.18. Firewall deve suportar NAT Estático (Port Forwarding).
- 7.19. Firewall deve suportar NAT Dinâmico.
- 7.20. Firewall deve suportar NAT 1 para 1.
- 7.21. Firewall deve suportar IPSEC NAT Traversal.
- 7.22. Firewall deve suportar NAT baseado em política.
- 7.23. Firewall deve possuir capacidade de atuar como um roteador multicast para encaminhamento de tráfego multicast da origem até os destinos dentro da rede.
- 7.24. Firewall deve suportar a detecção e mitigação de flood UDP.
- 7.25. A solução deve contemplar e estar plenamente licenciada para suportar funcionalidade SD-WAN.
- 7.26. A solução de SD-WAN UTM deve suportar roteamento baseado por política de SD-WAN, permitindo que administradores especifiquem parâmetros para definir por qual interface WAN certo tipo de tráfego será enviado.

- 7.27. A solução de SD-WAN UTM deve permitir a configuração da funcionalidade de SD-WAN em qualquer interface WAN de forma agnóstica, independente se a mesma for MPLS, internet, 4G/LTE, entre outras.
- 7.28. A solução de SD-WAN UTM deve ser compatível com a solução de VPN do UTM, permitindo que suas características e análises sejam realizadas nas VPNs assim como em links WAN.
- 7.29. A solução de SD-WAN UTM possuir uma lógica de roteamento que deve medir o desempenho do circuito de roteamento quase em tempo real; portanto, permitindo que os algoritmos de roteamento ativo-ativo de melhor caminho considerem também a melhor resiliência do site em comparação com a lógica tradicional de roteamento.
- 7.30. A solução de SD-WAN UTM deve possuir roteamento Baseado em Políticas e múltiplas saídas (e tipos de saídas) WANs.
- 7.31. A solução de SD-WAN UTM pode ser configurada para realizar failover entre links principais e secundários caso os links utilizados ultrapassem os limites previamente definidos de jitter, latência e perda de pacotes. Estes limites podem ser configurados para forçar o failover caso apenas um ou todos os limites sejam atingidos simultaneamente.
- 7.32. A solução de SD-WAN UTM deve ser compatível com VPNs montadas em interfaces virtuais com roteamento dinâmico.
- 7.33. A solução de SD-WAN UTM deve realizar o gerenciamento de tráfego por tipo de aplicação.
- 7.34. A solução de SD-WAN UTM deve considerar um modem USB conectado diretamente ao firewall como uma interface WAN válida.
- 7.35. A solução de SD-WAN UTM deve suportar atualizações automáticas de endereço IP via serviço de DNS Dinâmico.
- 7.36. A solução de SD-WAN UTM deve selecionar o melhor caminho baseado em tipo de tráfego e do host de origem.

- 7.37. A solução de SD-WAN UTM deve verificar JITTER, LATÊNCIA e PERDA DE PACOTES de cada link externo com endereços distintos na internet.
- 7.38. A solução de SD-WAN UTM deve suportar o monitoramento de link com DNS ou HTTP.
- 7.39. A solução de SD-WAN UTM deve suportar o monitoramento de link com PING.
- 7.40. A solução de SD-WAN UTM deve suportar o monitoramento de links VPN (Interfaces Virtuais).
- 7.41. A solução de SD-WAN UTM deve permitir a exportação de informações via Netflow.

## **8. FUNÇÕES DE GERENCIAMENTO**

- 8.1. A solução de UTM deve prover administração em tempo real de diversos firewalls através de uma única interface de gerência.
- 8.2. A solução de UTM deve suportar monitoramento em tempo real de logs de tráfego, alarmes, eventos, diagnósticos e estatísticas.
- 8.3. A solução de UTM deve enviar diversos alertas via SNMP ou email.
- 8.4. A solução de UTM deve permitir o uso de NAT para conexões via gateway de aplicação SNMP.
- 8.5. A solução de UTM deve permitir ser gerenciado através de múltiplos computadores simultaneamente.
- 8.6. A solução de UTM deve permitir a edição de políticas através de Windows interface Web e CLI.
- 8.7. A solução de UTM deve suportar autenticação via Windows Active Directory.
- 8.8. A solução de UTM deve suportar gerenciamento via Web Browser.
- 8.9. A solução de UTM deve suportar single sign-on (SSO) para logins via RDP.
- 8.10. A solução de UTM deve suportar single sign-on (SSO) para IPv6.

- 8.11. A solução de UTM deve suportar via SSO diversos usuários em uma única máquina para Windows Vista, Windows 7, Windows 8, Server 2008, and Server 2012 e superiores.
- 8.12. A solução de UTM deve suportar gerenciamento via linha comando através de porta serial e via SSH.
- 8.13. A solução de UTM deve suportar o rastreo de configurações e indicar as alterações realizadas entre configurações criadas anteriormente (comparação de versão de configurações).
- 8.14. A solução de UTM deve suportar a instalação em locais remotos sem a presença de técnicos no local, através de armazenamento de configuração do Firewall em nuvem que pode ser diretamente entregue ao firewall em sua primeira ativação.
- 8.15. A solução de UTM deve possuir a funcionalidade de ser configurada de forma automática, sem a necessidade de uma equipe de TI treinada presente no local da implementação para ajudar na configuração inicial do dispositivo.
- 8.16. A solução de Implantação Remota deve operar sempre que o equipamento for iniciado em configurações de padrão de fábrica (Factory Reset) e com um acesso a internet, forçando assim com que o Firewall UTM entre em contato automaticamente com um portal disponibilizado pelo fabricante para baixar um arquivo de configuração, se disponível.
- 8.17. A solução de Implantação remota deve possuir as seguintes formas de configuração:
- a) Implantação via Portal.
  - b) Implantação via Servidor de Gerência.
- 8.18. A O opção de Início Rápido permite que o firewall UTM baixe e use automaticamente um arquivo de configuração criado pelo fabricante da solução com as configurações recomendadas de firewall e segurança,

garantindo assim uma proteção eficiente do ambiente no momento inicial de implantação da solução.

- 8.19. A opção de Implantação via Portal permite que o firewall UTM seja configurado remotamente através do carregamento de uma configuração do firewall no site do Fabricante da solução.
- 8.20. A opção de Implantação via Portal permite que o arquivo a ser injetado no Firewall UTM tenha qualquer configuração e política previamente definida pelo administrador do ambiente, desta forma, garantindo que o Firewall esteja quase ou totalmente configurado, dentro das políticas de segurança do órgão, antes de permitir qualquer acesso de end points a internet.
- 8.21. A opção de Implantação Servidor de Gerência deve permitir que o Firewall UTM se conecte automaticamente a solução de gerência centralizada fornecida pelo Fabricante da solução a fim de que o administrador do ambiente possa realizar a configuração de diversos firewalls simultaneamente através do uso de Templates e/ou configuração de cada firewall separadamente.
- 8.22. A opção de Implantação Servidor de Gerência deve suportar a configuração de diversos firewalls simultaneamente em sua plataforma com o uso de um template de registro e configuração de equipamentos.
- 8.23. A opção de Implantação Servidor de Gerência deve suportar o registro dos firewalls previamente definidos a sua plataforma de maneira automática, permitindo assim que o administrador do ambiente possa validar quando um Firewall UTM remoto foi ligado pela primeira vez ou então iniciado em modo de Reset de Fábrica.
- 8.24. A solução de UTM deve implantar servidores externos ao firewall de forma a centralizar os logs e relatórios.
- 8.25. A solução de armazenamento de logs e relatórios não deve ter custo adicional ou deve estar plenamente licenciada para atender as especificações deste edital.

***Doe órgãos, doe sangue: Salve vidas!***



- 8.26. A solução de logs e relatórios deve suportar um banco de dados relacional para garantir a escalabilidade.
- 8.27. A solução de UTM deve permitir o envio de logs para diversos servidores simultaneamente.
- 8.28. A solução de UTM deve permitir a configuração de servidores de log de backup para que, no caso de falha do primário, o segundo continue a receber os logs.
- 8.29. A solução de UTM deve criptografar a transmissão dos logs.
- 8.30. A solução de logs e relatórios deve possuir ao menos 40 (quarenta) relatórios pré-configurados.
- 8.31. A solução de logs e relatórios deve permitir o envio de alertas quando a base de dados atingir um tamanho previamente definido.
- 8.32. A solução de logs e relatórios deve suportar a extração de relatórios no formato de PDF e CSV.
- 8.33. A solução de logs e relatórios deve gerar relatórios contendo dados do último dia, semana ou mês, automaticamente e enviá-los por e-mail e FTP.
- 8.34. A solução de logs e relatórios deve permitir em seu painel principal o aprofundamento para maiores detalhes dos logs.
- 8.35. A solução de logs e relatórios deve suportar o envio de todos os relatórios por e-mail para períodos específicos.
- 8.36. A solução de logs e relatórios deve suportar perfis de acesso distintos para usuários de administração e usuários somente leitura para acessos ao sistema.
- 8.37. A solução de logs e relatórios deve possuir uma imagem virtual pronta para a importação em servidores locais.
- 8.38. A solução de logs e relatórios deve ser compatível com solução VMWare.
- 8.39. A solução de logs e relatórios deve ser compatível com solução Hyper-V.

***Doe órgãos, doe sangue: Salve vidas!***



- 8.40. A solução de logs e relatórios deve prover uma vista para indicar os tipos de tráfego passando pelo firewall em um layout gráfico.
- 8.41. A solução de logs e relatórios deve prover uma visão de mapa mundi, indicando a origem e destino do tráfego de aplicação, pacotes negados e eventos de IPS.
- 8.42. A solução de logs e relatórios deve possuir relatórios de IPS.
- 8.43. A solução de logs e relatórios deve suportar a agregação de diversos firewalls a fim de criar um relatório de grupos de firewall.
- 8.44. A solução de logs e relatórios deve apresentar os FQDNs de clientes do Firewall em relatórios por usuário.
- 8.45. A solução de logs e relatórios deve indicar o consumo de banda e tempo utilizado por usuário em forma de relatório

## **9. DAS OBRIGAÇÕES DA CONTRATADA**

- 9.1. Instalação física do equipamento no local informado pela Prefeitura Municipal do Rio Grande, situado no mesmo município em local a definir;
- 9.2. Energização do equipamento e conexão do equipamento na rede lógica para permitir gerência do equipamento através da rede da Prefeitura Municipal do Rio Grande;
- 9.3. Migração das regras de firewall presentes hoje em solução de software livre para que funcionamento atual do firewall seja replicado;
  - a) A migração deve ser efetuada em janelas de horários a combinar com a equipe de tecnologia da SMDIER, de forma que não prejudiquem a prestação de serviços ao cidadão;
- 9.4. Habilitação e configuração de todas as funcionalidades citadas neste termo de referência;
- 9.5. Treinamento prático da estrutura implementada de 20 horas para 3 participantes, permitindo que a equipe da Superintendência de TI da Prefeitura Municipal do Rio Grande possa gerenciar com autonomia a

***Doe órgãos, doe sangue: Salve vidas!***



estrutura em atividades de gerência, como manutenção em unidades lógicas e alteração de regras de segurança na estrutura.

9.6. Manter, sem custo adicional para o Contratante, em caráter permanente à frente do contrato, um preposto que, além de possuir os conhecimentos e a capacidade profissionais necessários ao atendimento aos serviços contratados, deverá ainda ter competência para resolver imediatamente todo e qualquer assunto relacionado com os mesmos.

9.7. O preposto deverá ser capaz de:

- a) Atuar em todas as fases do projeto e/ou tarefas, avaliando o seu desenvolvimento e promovendo ações que assegurem o alcance das funcionalidades e dos produtos/serviços contratados;
- b) Executar os serviços técnicos profissionais com seu pessoal, com recursos tecnológicos e físicos disponibilizados para este fim, nas suas instalações de maneira remota.
- c) Tratar como "segredos comerciais e confidenciais" todos os produtos e subprodutos relativos aos serviços contratados com relação aos dados do Município.
- d) Não divulgar quaisquer informações a que tenha acesso em virtude dos trabalhos a serem executados ou de que tenha tomado conhecimento em decorrência da execução do objeto, sem autorização, por escrito, do Contratante, sob pena de aplicação das sanções cabíveis.
- e) Responsabilizar-se por quaisquer ônus, despesas ou obrigações trabalhistas, previdenciária, fiscais, de acidentes de trabalho, bem como alimentação, transporte ou outros benefícios de qualquer natureza, decorrentes da contratação dos serviços.
- f) Recrutar em seu nome e sob sua inteira responsabilidade os profissionais necessários à perfeita execução dos serviços, cabendo-lhe efetuar os pagamentos de salários e arcar com as demais obrigações trabalhistas, previdenciárias, fiscais e comerciais, inclusive

***Doe órgãos, doe sangue: Salve vidas!***



responsabilidades decorrentes de acidentes, indenizações, substituições, seguros, assistência médica e quaisquer outros, em decorrência da sua condição de empregadora, sem qualquer solidariedade por parte do Contratante.

- 9.8. Não se valer do Contrato a ser celebrado para assumir obrigações perante terceiros, dando-o como garantia, nem utilizar os direitos de crédito, a serem auferidos em função dos serviços prestados, em quaisquer operações de desconto bancário, sem prévia autorização do Contratante.
- 9.9. Arcar com quaisquer danos ou prejuízos causados ao Contratante. Nos casos de danos, prejuízos, avarias ou subtração de bens, os valores correspondentes deverão ser descontados da(s) fatura(s) seguinte(s) da Contratada, ou ajuizada, se for o caso, a dívida, sem prejuízo das demais sanções previstas no Contrato;
- 9.10. Comunicar ao Contratante, de forma detalhada, toda e qualquer ocorrência de acidentes verificada no curso da execução contratual.
- 9.11. Não usar as informações sigilosas ou de uso restrito, quando tais atos forem praticados por quem tenha sido alocado à execução do objeto deste Termo de Referência, sob pena de responsabilidade civil e/ou criminal.
- 9.12. Responsabilizar-se pelo comportamento dos seus empregados e por quaisquer danos que estes ou seus prepostos venham porventura a ocasionar ao Contratante, ou a terceiros, durante a execução dos serviços.
- 9.13. Efetuar o pagamento dos seguros, tributos, encargos sociais e de toda e qualquer despesa referente aos serviços contratados e dos documentos a eles relativos, se necessários.
- 9.14. Responder adequadamente a todas as observações, reclamações e exigências efetuadas, no sentido do cumprimento do Contrato e da melhoria dos serviços executados.
- 9.15. Cumprir os prazos estipulados nos cronogramas acordados e aprovados com a Contratante.

***Doe órgãos, doe sangue: Salve vidas!***



- 9.16. Informar ao Contratante toda ocorrência que esteja prejudicando a prestação dos serviços e o cumprimento dos níveis de serviços acordados.
- 9.17. Aceitar que o Contratante possa rejeitar, no todo ou em parte, os serviços executados em desacordo com as normas estabelecidas no Contrato.
- 9.18. Aceitar que o Contratante possa solicitar, com justificativa, a substituição de qualquer profissional que considere inadequado para a função, cabendo à Contratada a apresentação de novo profissional.
- 9.19. Aceitar que o Contratante poderá determinar a imediata retirada do local de trabalho do empregado que estiver sem crachá, que embaraçar ou dificultar a sua fiscalização ou cuja permanência, a seu exclusivo critério, julgar inconveniente, solicitando sua substituição imediata.
- 9.20. Manter, em observância às obrigações assumidas, todas as condições de habilitação e qualificação exigidas no processo de licitação.

## 9. CONTATO

Dúvidas para esclarecimento técnico deverão ser encaminhadas à Superintendência de Tecnologia da Informação preferencialmente pelo e-mail [informatica@riogrande.rs.gov.br](mailto:informatica@riogrande.rs.gov.br) pelo número (53)3233-7365.



*Matheus Gondran dos Santos*  
Mat. 12830-9  
Superintendente de TI

***Doe órgãos, doe sangue: Salve vidas!***