

Ofício SDGI \_\_\_\_\_2020

Rio, 28 de abril de 2020.

Ilmo Sr.

Wagner Victer

Diretor Geral da ALERJ

Assunto: VIABILIZAÇÃO DO ATO N/MD/Nº 654/ 2020 - Pandemia de corona vírus.'

Para atender a publicação do ATO N/MD/Nº 654/ 2020, que Disciplina o Teletrabalho na Assembleia Legislativa, em face dos Decretos nº 46.973 16/03/2020 e 46.980 19/03/2020 e do Decreto nº 46.984 20/03/2020 decretando o estado de calamidade pública devido a Pandemia do COVID-19. Se faz necessário a aquisição de uma solução de Next Generation Firewall em alta disponibilidade e serviços de suporte técnico. Entre outras funcionalidades é a URL Filtering, que permite implementar políticas de segurança para bloquear serviços que não são permitidos e, outras funcionalidades agregadas como controle de acesso de usuários ou *sites* remotos através de *Virtual Private Network – VPN*, inspeção de tráfego criptografados (*SSL Inspection*).

Sendo assim segue Termo de Referência para atender as necessidades da ALERJ.

Atenciosamente,

Renato Loureiro Stavale

Matr. 308.350-8

Subdiretoria Geral de Informática

## TERMO DE REFERÊNCIA

### 1. OBJETO

O objeto desta contratação é o fornecimento de solução de Next Generation Firewall em alta disponibilidade e serviços de suporte técnico durante a vigência do contrato, com o objetivo de prover a segurança, proteção de dados de sistemas e da infraestrutura de Tecnologia da Informação e Comunicação da Informação e da rede lógica da ALERJ – Assembleia Legislativa do Estado do Rio de Janeiro.

### 2. METODOS E ESTRATEGIAS DE SUPRIMENTO

O prazo para o início da prestação dos serviços será de 30 dias corridos, e começará a fluir no dia seguinte ao recebimento, pela empresa vencedora, do ofício de início da prestação dos serviços, a ser emitido pela Subdiretoria-Geral de Informática.

O início da prestação dos serviços será acordado com a Subdiretoria-Geral de Informática, na Rua da Alfândega, no. 8, 11º. Andar, Centro, Rio de Janeiro – RJ. O telefone para contato é: (21) 2588-8456.

01	Next Generation Firewall implantado com Alta Disponibilidade e de acordo com as especificações técnicas abaixo Appliance.	2		
02	Conjunto de Funcionalidades de IDS/IPS	2		
03	Conjunto de Funcionalidades de antimalware	2		
04	Conjunto de Funcionalidades de Tratamento de Conteúdo Web	2		
05	Conjunto de Funcionalidades de Controle de Aplicações	2		
06	Treinamento Oficial para 5 pessoas	Und		
07	Solução de Gerência Centralizada	Und		
08	Serviço de Suporte Técnico	36 meses		

#### 2.1. ESPECIFICAÇÕES TÉCNICAS - FUNCIONALIDADES

**2.1.1.** O equipamento appliance de firewall deve suportar configuração de quatro zonas de segurança, sendo externa, privada, opcional (DMZ) e customizada.

**2.1.2.** O equipamento de firewall deve suportar endereçamento IP estático e dinâmico [DHCP e PPPoE nas interfaces externas]

- 2.1.3. O equipamento de firewall deve possuir funcionalidades de DHCP relay que permitam a adição de três servidores DHCP simultâneos.
- 2.1.4. O equipamento de firewall deve permitir DHCPv6 em interfaces externas.
- 2.1.5. O equipamento de firewall deve possuir as seguintes performances em *“throughput”*:
  - 2.1.5.1. 80 Gbps para as funções de firewall.
  - 2.1.5.2. 27 Gbps para as funções de firewall e *“Application Visibility and Control”* quando as mesmas estiverem operando de forma simultânea.
  - 2.1.5.3. 26 Gbps para as funções de firewall, *“Application Visibility and Control”* e *“Intrusion Prevention System”* quando as mesmas estiverem operando de forma simultânea.
- 2.1.6. O equipamento de firewall deve suportar ao menos as seguintes funcionalidades:
  - 2.1.6.1. Stateful firewall;
  - 2.1.6.2. Roteamento (estático e dinâmico);
  - 2.1.6.3. Site-to-Site VPN;
  - 2.1.6.4. Remote Access VPN;
  - 2.1.6.5. Next-Generation Intrusion Prevention System (NGIPS);
  - 2.1.6.6. Application Visibility and Control (AVC);
  - 2.1.6.7. URL filtering;
  - 2.1.6.8. Advanced Malware Protection (AMP).
- 2.1.7. 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.
- 2.1.8. Interface em português e inglês;
- 2.1.9. Permitir exportar backups da solução para um armazenamento remoto com suporte a conexões do tipo, FTP, SFTP, TFTP e SCP
- 2.1.10. Possuir mecanismo que permita a realização de cópias de segurança (backups) do sistema e restauração remota, através da interface gráfica, a solução deve permitir o agendamento diário ou semanal;
- 2.1.11. O sistema deve permitir configurar o período ou número de cópias que deseja manter no repositório remoto e executar a manutenção de período automaticamente.
- 2.1.12. O sistema deve permitir configurar uma chave de criptografia de forma a garantir segurança, confiabilidade e confidencialidade dos arquivos de backup;
- 2.1.13. O equipamento de firewall deve suportar autenticação via RADIUS, LDAP e Active Directory.
- 2.1.14. O equipamento de firewall deve suportar autenticação transparente de usuários (Single Sign On) de AD e RADIUS.
- 2.1.15. O equipamento de firewall deve definir o intervalo de tempo entre tentativas de login incorretas por conexão.
- 2.1.16. 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
- 2.1.17. O equipamento de firewall deve conseguir filtrar conteúdo nos protocolos mais comuns, assim como filtrar conteúdo tipo *“MIME”*

- 2.1.18. 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).
- 2.1.19. O equipamento de firewall deve suportar Server Name Indication (SNI) para configurar domínios para funcionalidades de bloqueio, inspeção ou permissão.
- 2.1.20. O equipamento de firewall deve complementar capacidades e bloqueio de CN existentes com SNI com a finalidade de bloquear domínios específicos do Google.
- 2.1.21. 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).
- 2.1.22. O equipamento de firewall deve suportar o bloqueio de domínios através de *wildcard*.
- 2.1.23. O equipamento de firewall deve permitir a criação de políticas por IP utilizando *wildcard*.
- 2.1.24. O equipamento de firewall deve suportar a configuração por política de bloqueio de conexões *inbound* e *outbound* para um país (ou conjunto de países).
- 2.1.25. O equipamento de firewall deve possuir as seguintes certificações/compliance:
  - 2.1.25.1. ANATEL
  - 2.1.25.2. CE
  - 2.1.25.3. FCC
  - 2.1.25.4. RoHS
- 2.1.26. O equipamento de firewall deve aplicar políticas granulares para restringir o tráfego de países considerados arriscados de acordo com a política de segurança da empresa contratante de acordo com o tipo de tráfego, porta, protocolo, endereço, usuário ou grupo de origem assim como destino.
- 2.1.27. O equipamento de firewall deve permitir outros tipos de tráfego que não ofereçam ameaças semelhantes, como DNS ou Mail de países que tenham certos protocolos bloqueados quando considerados perigosos pela política de segurança da empresa.
- 2.1.28. A solução deve permitir que o administrador de rede realize uma configuração em modo "offline" para posteriormente ser injetada ao firewall.
- 2.1.29. A solução deve suportar SSO para soluções RADIUS.
- 2.1.30. A solução deve rastrear as sessões de usuários via SSO para RADIUS.

## **2.2. ESPECIFICAÇÕES TÉCNICAS – CRIPTOGRAFIA E VPN**

- 2.2.1. A solução deve suportar Remote Access VPN.
- 2.2.2. A solução deve suportar ao menos 5.000 Remote Access VPN usando SSL.
- 2.2.3. A solução 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.
- 2.2.4. A solução deve suportar VPN entre localidades (site-to-site VPN).
- 2.2.5. A solução deve suportar pelo menos 5.000 VPNs entre escritórios utilizando IPSec.

- 2.2.6.** A solução deve suportar iterações com outros produtos e marcas que suportem o padrão IPsec.
- 2.2.7.** A solução deve suportar os seguintes métodos de autenticação:
  - 2.2.7.1.** 3DES
  - 2.2.7.2.** AES 128 -, 192-, 256-bit
- 2.2.8.** A solução deve suportar os seguintes métodos de criptografia:
  - 2.2.8.1.** SHA-2
  - 2.2.8.2.** MD5
  - 2.2.8.3.** IKE Pre-Shared Key
  - 2.2.8.4.** AES with CBC and GCM
- 2.2.9.** A solução deve suportar Dead Peer Detection (DPD).
- 2.2.10.** A solução deve suportar VPN site-to-site com IKEv2.
- 2.2.11.** A solução deve suportar VPN client-to-site com IKEv2
- 2.2.12.** A solução deve suportar Perfect Forward Secrecy (PFS) com chaves Diffie-Hellman (ou Diffie-Hellman-Merkle) em pacotes web e email.
- 2.2.13.** A solução deve suportar VPN Failover (reestabelecer a VPN através de um segundo link em caso de falha do link primário).
- 2.2.14.** A solução deve suportar VPN IPSEC com um throughput igual ou maior que 8 Gbps.
- 2.2.15.** A solução deve permitir criar interfaces virtuais para VPNs e rotear tráfego utilizando VPNs site-to-site com protocolos de roteamento dinâmico.
- 2.2.16.** A solução deve suportar VPN site-to-site sobre TLS.
  - 2.2.16.1.** A decifração TLS deve ser em hardware com throughput mínimo de 6 Gbps utilizando AES256-SHA com chave RSA 2048B.
- 2.2.17.** A solução deve suportar VPN client-to-site com SSL com VLANs e redes secundárias através de configuração de roteamento.
- 2.2.18.** A solução deve permitir visualizar estatísticas de VPN em interfaces virtuais, gateways, tunnel types, etc. para qualquer tipo de usuário.
- 2.2.19.** A solução deve permitir visualizar mensagens de diagnóstico de VPN para ajudar a remediar e realizar o troubleshooting pelos administradores do sistema.
- 2.2.20.** A solução deve suportar túneis VPN site-to-site estáticos (políticas) e dinâmicas (roteadas) para MS Azure.
- 2.2.21.** A solução deve suportar túneis VPN site-to-site estáticos (políticas) e dinâmicas (roteadas) para AWS.
- 2.2.22.** A solução deve suportar VPN em interfaces virtuais e realizar Failover entre as mesmas.
- 2.2.23.** Possuir funcionalidades de Auto-Discovery VPN capaz de permitir criar túneis de VPN dinâmicos entre múltiplos dispositivos (spokes) com um gateway centralizador (hub).;
- 2.2.24.** A funcionalidade de AD-VPN deve suportar criar os seguintes tipos de túneis:
  - 2.2.25.** Site-to-Site;
  - 2.2.26.** Full-Mesh;
  - 2.2.27.** Star.

## **2.3. ESPECIFICAÇÕES TÉCNICAS – FILTRO DE CONTEÚDO WEB E URL**

- 2.3.1.** A solução deve ser fornecida com filtro de conteúdo Web totalmente licenciado.
- 2.3.1.1.** Caso o licenciamento seja por subscrição, deve ser considerado um período mínimo de 36 meses.
- 2.3.2.** A solução deve permitir que o filtro trabalhe por categorias, ajustado por grupos de usuário e possuir um mínimo de 80 categorias.
- 2.3.3.** Deve ser capaz de armazenar cache dinâmicos para as atualizações Microsoft Windows Update®, Youtube®, MSN Vídeos®, Facebook®, Google Maps®;
- 2.3.4.** A solução deve permitir exceções no filtro de conteúdo por meio de whitelist.
- 2.3.5.** A solução deve apresentar ao usuário uma tela de aviso indicando que a categoria do website acessado não está de acordo com as políticas da empresa.
- 2.3.6.** A solução 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.
- 2.3.7.** Deve possuir tratamento de certificados, permitindo bloqueio em caso de certificados inválidos;
- 2.3.8.** A solução deve identificar e bloquear mais de 1800 aplicações diferentes, incluindo controle granular de aplicação, como telas de login e metodologias específicas de transferência de arquivo.
- 2.3.9.** A solução deve suportar updates automáticos de assinaturas de aplicação.
- 2.3.10.** A solução 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.
- 2.3.11.** A solução deve suportar validação de URL com *content filtering* através de um proxy server externo.

## **2.4. ESPECIFICAÇÕES TÉCNICAS – LISTA DE BACKLIST IP'S**

- 2.4.1.** A solução deve suportar o bloqueio de tráfego vindo de IPs maliciosos reconhecidos por base de dados de blacklists disponíveis no mercado.
- 2.4.2.** A solução deve suportar o bloqueio de tráfego de botnets reconhecidos por base de dados de blacklist disponíveis no mercado.

## **2.5. ESPECIFICAÇÕES TÉCNICAS – CONTROLE DE APLICAÇÕES**

- 2.5.1.** A solução deve suportar o filtro de aplicação no próprio hardware.
- 2.5.2.** A solução deve suportar a configuração de exceções para filtro de aplicação.
- 2.5.3.** A solução deve ter suas assinaturas de aplicação atualizadas automaticamente e regularmente.

## **2.6. ESPECIFICAÇÕES TÉCNICAS – AMP – ADVANCED MALWARE PROTECTION**

- 2.6.1.** Deve suportar operação em ambientes configurados para alta disponibilidade
- 2.6.2.** O dispositivo de proteção deve ser capaz de enviar arquivos trafegados de forma automática para análise "*In Cloud*" ou local, onde o arquivo será executado e simulado em ambiente controlado.
  - 2.6.2.1.** Deve ser fornecido todo o hardware e software necessário para implementação desta funcionalidade. Caso seja licenciado por meio de subscrição, deve ser considerado um período mínimo de 36 meses.
- 2.6.3.** Deve permitir de forma automática a criação e manutenção de um histórico ou fluxo de trabalho forense no qual seja possível identificar:
  - 2.6.3.1.** Inserção de malware no ambiente de rede, movimento lateral, mesmo quando esta não seja detectada inicialmente como malware.
- 2.6.4.** Deve permitir selecionar através de políticas granulares quais tipos de arquivos sofrerão esta análise incluindo, mas não limitado a: endereço IP de origem/destino, usuário/grupo do AD/LDAP, aplicação, porta, URL/categoria de URL de destino, tipo de arquivo e todas estas opções simultaneamente;
- 2.6.5.** Deve suportar a monitoração, detecção e prevenção em tempo real de arquivos trafegados nos seguintes protocolos HTTPS, FTP, HTTP, SMTP, IMAP, POP3 como também arquivos trafegados internamente entre servidores de arquivos usando SMB em todos os modos de implementação: sniffer, transparente e L3;
- 2.6.6.** Deve permitir especificar o tipo de arquivo, inclusive os comprimidos que serão analisados em cada política de controle de malware, permitindo especificar um contexto de análise para redes, vlans e outros objetos associados ao controle de acesso do ambiente protegido.
- 2.6.7.** Permitir que seja definido o tamanho máximo dos arquivos a serem inspecionados.
- 2.6.8.** Deve utilizar mecanismo de proteção baseado em reputação global em tempo-real, permitindo assim que sejam adotadas ações automáticas de alerta e bloqueio de arquivos suspeitos ou malwares já encontrados anteriormente.
- 2.6.9.** O dispositivo não deve depender ou utilizar de forma exclusiva mecanismos de análise em ambiente virtualizado para que seja feita a detecção e o bloqueio de ameaças malwares em tempo-real.
- 2.6.10.** A utilização de recursos de execução virtualizada, não deve depender da configuração manual de imagens ou escolha de versões específicas de sistemas operacionais;
- 2.6.11.** Deve possuir mecanismo blacklist para implementar controles customizados de forma automatizada.
- 2.6.12.** Deve possuir mecanismo whitelist para implementar controles customizados de forma automatizada.
- 2.6.13.** Deve possuir capacidade para detecção de Malwares em comunicações de entrada e saída, incluindo a detecção de mecanismos de Comando e Control.

- 2.6.14.** Deve identificar ataques como: ataques direcionados, Zero Day, exploração de vulnerabilidades, indicadores de obfuscação e indicadores de comprometimento automáticos.
- 2.6.15.** Deve possuir tecnologia proprietária de execução para verificação de Malwares avançados inclusive mecanismos tipo sandbox.
- 2.6.16.** Deve implementar a identificação e capacidade de controle de acesso em tempo real nos seguintes tipos de arquivo: MSEXE, 9XHIVE, DMG, DMP,ISO,NTHIVE,PCAP,PGD,SYLKc,SYMANTEC,VMDK,DWG,IMG\_PICT,MAYA, PSD,WMF,SCRENC,UUENCODED,PDF,EPS,AUTORUN,BINARY\_DATA,BINHEX, EICAR, ELF,ISHIELD\_MSI, MACHO, RPM, TORRENT, AMR, FFMPEG, FLAC, FLIC, FLV, IVR, MIDI, MKV,MOV,MPEG,OGG,PLS,R1M,REC,RIFF,RIFX,RMF,S3M,SAMI,SMIL,SWF,WA V,WEBM,7Z,ARJ,BZ,CPIO\_CRC,CPIO\_NEWC,CPIO\_ODC,,JAR,LHA,MSCAB,MS SZDD,OLD\_TAR,POSIX\_TAR,RAR,SIS,SIT,ZIP,ZIP\_ENC,ACCDB,HLP,MAIL,MDB, MDI,MNY,MSCHM,MSOLE2,MSWORD\_MAC5,MWL,NEW\_OFFICE,ONE,PST,RT F,TNEF,WAB,WP,WRI,XLW,XPS. Adicionalmente, deve implementar em tempo-real a inspeção, detecção e bloqueio autónomo (prevenção sem a necessidade de integrar com outros sistemas terceiros para que seja feito o bloqueio da ameaça) na rede para os seguintes tipos de arquivos: 7Z, ACCDB, ARJ, BINARY\_DATA, BINHEX, BZ, CPIO\_CRC, CPIO\_NEWC, CPIO, ODC, EICAR, FLV, GZ, ISHIELD\_MSI, JAR, JARPACK, LHA, MAIL, MDB, MDI, MNY, MSCAB, MSCHM, MSEXE, MSOLE2, MSWORD\_MAC5, NEW\_OFFICE, OLD\_TAR, PDF, POSIX\_TAR, PST, RAR, RTF, SIS, SIT, SWF, TNEF, WAB, WRI, XLW, XPS, ZIP, ZIP\_ENC;
- 2.6.17.** Deve implementar atualização a base de dados da Rede de Inteligência de forma automática.
- 2.6.18.** Para recursos de análise virtualizada existente, deve ser mantido um histórico dos resultados de avaliações prévias de um arquivo e utilizar esta informação para determinar de forma configurável que o arquivo seja considerado malware a partir de certo limite.
- 2.6.19.** Dispor de múltiplos motores e mecanismos de detecção e prevenção para verificação de Malwares e códigos maliciosos incluindo:
- 2.6.19.1.** Machine learning
  - 2.6.19.2.** Reputação global
  - 2.6.19.3.** Detecção customizada local por blacklist e regras customizadas de detecção de tráfego de rede
  - 2.6.19.4.** Análise dinâmica (sandbox)
- 2.6.20.** O processo de análise de comunicações, Malwares e sua prevenção deve ocorrer em tempo real, não sendo aceitas tecnologias que dependam de

verificações que induzam latência suficiente para postergar a entrega de arquivos ao seu destino original

**2.6.21.** Deve permitir o download dos malwares identificados a partir da própria interface de gerência;

**2.6.22.** Caso a solução seja fornecida em appliance local, deve possuir, no mínimo, 8 ambientes controlados (sand-box) independentes para execução simultânea de arquivos suspeitos;

**2.6.23.** Caso sejam necessárias licenças de sistemas operacional e softwares para execução de arquivos no ambiente controlado (sand-box), as mesmas devem ser fornecidas em sua totalidade, sem custos adicionais para a contratante;

**2.6.24.** Suportar a análise de arquivos executáveis, DLLs e ZIP no ambiente controlado;

**2.6.25.** Suportar a análise de arquivos do pacote office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), arquivos java (.jar e .class) ;

**2.6.26.** Permitir o envio de arquivos para análise no ambiente controlado de forma automática;

## **2.7. ESPECIFICAÇÕES TÉCNICAS – IPS – INTRUSION PREVENTION SYSTEM**

**2.7.1.** Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos;

**2.7.2.** Deve sincronizar as assinaturas de IPS quando implementado em alta disponibilidade;

**2.7.3.** Deve implementar os seguintes tipos de ações para ameaças detectadas pelo IPS: permitir, permitir e gerar log, bloquear, bloquear IP do atacante por um intervalo de tempo e enviar tcp-reset;

**2.7.4.** Deve permitir ativar, desativar e habilitar apenas em modo de monitoração as assinaturas de prevenção contra invasão;

**2.7.5.** Exceções por IP de origem ou de destino devem ser possíveis nas regras e assinatura a assinatura;

**2.7.6.** Deve suportar granularidade nas políticas de IPS , possibilitando a criação de diferentes políticas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens.

**2.7.6.1.** Deve permitir o bloqueio de vulnerabilidades.

**2.7.6.2.** Deve permitir o bloqueio de exploits conhecidos.

**2.7.6.3.** Deve incluir proteção contra ataques de negação de serviços.

**2.7.6.4.** Deverá possuir os seguintes mecanismos de inspeção de IPS:

**2.7.6.5.** Análise de padrões de estado de conexões;

**2.7.6.6.** Análise de decodificação de protocolo;

**2.7.6.7.** Análise para detecção de anomalias de protocolo;

**2.7.6.8.** IP Defragmentation;

**2.7.6.9.** Remontagem de pacotes de TCP;

**2.7.6.10.** Bloqueio de pacotes malformados

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

**2.7.6.12.** Detectar e bloquear a origem de portscans;

- 2.7.6.13.** Bloquear ataques efetuados por worms conhecidos, permitindo ao administrador acrescentar novos padrões;
- 2.7.6.14.** Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS;
- 2.7.6.15.** Possuir assinaturas para bloqueio de ataques de buffer overflow;
- 2.7.6.16.** Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto;
- 2.7.6.17.** Deve permitir usar operadores de negação na criação de assinaturas customizadas de IPS e anti-spyware, permitindo a criação de exceções com granularidade nas configurações;
- 2.7.6.18.** Permitir o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;
- 2.7.6.19.** Suportar bloqueio de arquivos por tipo;
- 2.7.6.20.** Identificar e bloquear comunicação com botnets;
- 2.7.6.21.** Registrar na console de monitoração as seguintes informações sobre ameaças identificadas:
  - 2.7.6.22.** O nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;
- 2.7.6.23.** Deve suportar a captura de pacotes (PCAP), por assinatura de IPS e controle de aplicação;
- 2.7.6.24.** Deve possuir a função de proteção a resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos de botnets conhecidas;
- 2.7.6.25.** Os eventos devem identificar o país de onde partiu a ameaça;
- 2.7.6.26.** Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms;
- 2.7.6.27.** Proteção contra downloads involuntários usando HTTP de arquivos executáveis, maliciosos;
- 2.7.6.28.** Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas do firewall considerando Usuários, Grupos de usuários, origem, destino, zonas de segurança, etc, ou seja, cada política de firewall poderá ter uma configuração diferente de IPS, sendo essas políticas por Usuários, Grupos de usuário, origem, destino e zonas de segurança.

## **2.8. ESPECIFICAÇÕES TÉCNICAS – CAPACIDADE DE REDE**

- 2.8.1.** O Firewall deve possuir, ao menos, as seguintes interfaces:
  - 2.8.1.1.** 1 interface console RJ45;
  - 2.8.1.2.** 8 interfaces 1/10 GbE com suporte a transceiver do tipo SFP+ para Fibra Óptica MultiModo.
  - 2.8.1.3.** Firewall deve permitir a instalação de módulos de expansão de interfaces, podendo ser:
    - 2.8.1.3.1.** 8 interfaces x 10/100/1000 BaseT;



- 2.8.21. Quando uma interface física ou subinterface é compartilhada por mais de um dispositivo lógico, o firewall deve gerar um endereço MAC único para cada dispositivo lógico.
- 2.8.22. Firewall deve suportar NAT e PAT.
- 2.8.23. Firewall deve suportar NAT Estático (Port Forwarding).
- 2.8.24. Firewall deve suportar NAT Dinâmico.
- 2.8.25. Firewall deve suportar NAT 1 para 1.
- 2.8.26. Firewall deve suportar IPSEC NAT Traversal.
- 2.8.27. Firewall deve suportar NAT baseado em política.
- 2.8.28. Firewall deve possuir capacidade de atuar como um roteador multicast para encaminhamento de tráfego multicast da origem até os destinos dentro da rede.
- 2.8.29. Firewall deve suportar a detecção e mitigação de flood UDP.

## **2.9. ESPECIFICAÇÕES TÉCNICAS – PROGRAMABILIDADE**

- 2.9.1. O firewall deve possuir “Application Programming Interface (API)” no padrão RESTFUL que permita a interação com o firewall através do protocolo HTTPS.
- 2.9.2. Os objetos devem ser representados utilizando JavaScript Object Notation (JSON).
- 2.9.3. O firewall deve possuir um API Explorer com a descrição de todos os recursos e objetos JSON disponíveis.
- 2.9.4. A descrição deve incluir informações detalhadas sobre os pares atributo/valor de cada objeto.
- 2.9.5. A descrição também deve conter exemplos das URLs necessárias para cada recurso do firewall.
- 2.9.6. O firewall deve suportar ao menos os seguintes métodos HTTP:
  - 2.9.6.1. GET, para leitura de dados do sistema;
  - 2.9.6.2. POST, para criar novos objetos;
  - 2.9.6.3. PUT, para modificar objetos existentes;
  - 2.9.6.4. DELETE, para remover objetos definidos por usuários.
- 2.9.7. O firewall deve vir com um certificado auto assinado, para que se possa iniciar as comunicações HTTPS com o dispositivo.
- 2.9.8. O firewall deve possuir mecanismos de by-pass da checagem do certificado auto assinado quando da utilização de comandos CURL.
- 2.9.9. As chamadas dos clientes devem ser autenticadas utilizando o método Oauth 2.0, conforme RFC 6749.
- 2.9.10. O firewall deve suportar JSON Web Token (JWT) conforme RFC 7519
- 2.9.11. O firewall deve permitir configurar um servidor RADIUS AAA externo para autenticar e autorizar o acesso do usuário à API REST.

## **2.10. ESPECIFICAÇÕES TÉCNICAS – PLATAFORMA DE GERENCIAMENTO**

- 2.10.1. A solução deve prover administração em tempo real de diversos firewalls através de uma única interface de gerência.
- 2.10.2. A solução deve ser fornecida em hardware próprio para gerenciar os firewalls ou em modo máquina virtual. Em caso de a plataforma de gerenciamento for em modo máquina virtual, a mesma deve ser compatível com ao menos os seguintes hipervisores:

- 2.10.2.1.** VMware
- 2.10.2.2.** KVM
- 2.10.3.** A solução deve suportar monitoramento em tempo real de logs de tráfego, alarmes, eventos, diagnósticos e estatísticas.
- 2.10.4.** A solução deve enviar diversos alertas via SNMP ou email.
- 2.10.5.** A solução deve permitir ser gerenciado através de múltiplos computadores simultaneamente.
- 2.10.6.** A solução deve permitir a criação de templates para configurações de VPN hub-and-spoke.
- 2.10.7.** A solução deve permitir a criação de templates para configurações compartilhadas entre firewalls de diversos locais remotos, podendo ser implementada simultaneamente em todos os dispositivos escolhidos.
- 2.10.8.** A solução deve suportar o agendamento para a aplicação de configurações compartilhadas de um ou diversos firewalls UTM simultaneamente assim como o rollback de configurações prévias salvas na solução de gerenciamento centralizado.
- 2.10.9.** A solução deve suportar a função de “roll back” para configurações anteriores.
- 2.10.10.** A solução deve permitir a configuração e edição de políticas através de interface GUI de maneira offline, sem estar diretamente conectada ao equipamento.
- 2.10.11.** A solução deve permitir a edição de políticas através de Windows GUI, interface Web e CLI.
- 2.10.12.** A solução deve suportar a configuração de acessos distintos para administradores.
- 2.10.13.** A solução deve suportar autenticação via Windows Active Directory.
- 2.10.14.** A solução deve suportar gerenciamento via Web Browser.
- 2.10.15.** A solução deve suportar single sign-on (SSO) para IPv6
- 2.10.16.** A solução deve suportar via SSO diversos usuários em uma única máquina para Windows 8, Server 2008, and Server 2012.
- 2.10.17.** A solução deve possuir gerenciamento via linha comando através de porta serial e/ou via SSH.
- 2.10.18.** A solução 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 (Vide item “F. Implantação Remota do Firewall”).
- 2.10.19.** A solução deve suportar o agendamento para o update do sistema operacional em um ou diversos firewalls UTM simultaneamente.

## **2.11. ESPECIFICAÇÕES TÉCNICAS – FUNCIONALIDADES DE LOGGING E REPORTING**

- 2.11.1.** A solução deve permitir a implementação de servidores externos ao firewall de forma a centralizar os logs e relatórios.

- 2.11.2.** A solução deve permitir o envio de logs para diversos servidores simultaneamente.
- 2.11.3.** A solução deve criptografar a transmissão dos logs sem que seja necessária a criação de uma VPN para tal.
- 2.11.4.** A solução de logs e relatórios deve possuir ao menos 07 relatórios pré-configurados, sem qualquer custo adicional.
- 2.11.5.** A solução de logs e relatórios deve suportar a extração de relatórios no formato de PDF e CSV.
- 2.11.6.** A solução de logs e relatórios deve possuir um relatório executivo com um sumário de informação high level.
- 2.11.7.** A solução de logs e relatórios deve permitir em seu dashboard o pivotamento ou aprofundamento para maiores detalhes dos logs.
- 2.11.8.** A solução de logs e relatórios deve suportar acessos distintos de administração e somente leitura para acessos a logs para diferentes firewalls conectados a solução.
- 2.11.9.** A solução de logs e relatórios deve possuir uma imagem virtual pronta para a importação em servidores locais.
- 2.11.10.** A solução de logs e relatórios deve ser compatível com solução VMWare.
- 2.11.11.** A solução de logs e relatórios deve ser compatível com solução Hyper-V.
- 2.11.12.** 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.
- 2.11.13.** A solução de logs e relatórios deve possuir relatórios de IPS que detalhem as informações
- 2.11.14.** A solução de logs e relatórios deve suportar a agregação de diversos firewalls a fim de criar um relatório de grupos de firewall.
- 2.11.15.** A solução de logs e relatórios deve indicar o consumo de banda e tempo utilizado por usuário em forma de relatório, acessível pelo appliance ou WebUI.
- 2.11.16.** A solução de logs e relatórios deve possuir um dashboard possibilitando o bloqueio de IPs de origens de ataques.
- 2.11.17.** A solução de logs e relatórios deve possuir a capacidade de criação de políticas de firewall.
- 2.11.18.** A solução de logs e relatórios deve possuir um dashboard indicando o uso de cada política, inclusive informando as políticas não utilizadas no firewall.
- 2.11.19.** A solução de logs e relatórios deve possuir um dashboard indicando geograficamente o fluxo do tráfego do firewall, políticas acionadas assim como o IP de origem e destino do tráfego.

## **2.12. SERVIÇO DE SUPORTE E MANUTENÇÃO DA PLATAFORMA**

- 2.12.1.** O serviço de Suporte e Manutenção da Plataforma consiste em manter todos os componentes da solução atualizados e funcionando durante toda a vigência do contrato.

## **2.13. ESCOPO DO SERVIÇO**

**2.13.1.** O escopo do Serviço de Suporte Técnico a ser provido pela CONTRATADA deverá ser provido através de um Centro de Operações de Segurança e Suporte, com operação 24 horas por dia, 7 dias por semana e 365 dias do ano (24x7x365)

e os serviços a serem prestados incluem:

- 2.13.1.1.** Setup Inicial da Solução (Adoção do cliente)
  - 2.13.1.1.1.** Planejamento de implantação da solução;
  - 2.13.1.1.2.** Aprovação dos planos de implantação junto ao cliente;
  - 2.13.1.1.3.** Execução das atividades de implantação remotamente;
  - 2.13.1.1.4.** Entrega da documentação resultado do Projeto;
  - 2.13.1.1.5.** Início dos serviços de suporte.
- 2.13.1.2.** Suporte de Segurança Remoto
  - 2.13.1.2.1.** Permitir a abertura, acompanhamento e validação de chamados através de e-mail, web site (portal do cliente) e telefone (0800) no regime 24x7x365 e com atendimento em português.
  - 2.13.1.2.2.** Possuir processo de escalção funcional, mapeamento e documentado, com os seguintes níveis de atendimento: N1, N2 e N3 conforme melhores práticas descritas pelo ITIL;
  - 2.13.1.2.3.** Possuir canal de interface com os fabricantes dos equipamentos envolvidos na solução dos incidentes que requeiram o envolvimento desses, bem como ser responsável pela abertura e acompanhamento do chamado;
  - 2.13.1.2.4.** Possuir análise técnica documentada pelo N3 do SOC antes do envolvimento dos fabricantes dos equipamentos a fim de garantir o processo de escalção funcional.
  - 2.13.1.2.5.** Possuir os processos de gerenciamento de incidente, requisição, eventos, problemas, mudanças, incidentes críticos e atendimento aos usuários VIPS mapeados e documentados de acordo com as melhores práticas descritas pelo ITIL;
  - 2.13.1.2.6.** O suporte será em formato de dupla custódia, mantendo os administradores de tecnologia do cliente com total controle da plataforma e responsabilidade pela operação diária da solução.
  - 2.13.1.2.7.** Permitir o suporte ao ambiente por profissionais contratados em regime CLT e com as seguintes certificações:
    - 2.13.1.2.7.1. Project Management Professional (PMP)
    - 2.13.1.2.7.2. ITIL Foundation Certificate
    - 2.13.1.2.7.3. Certificação do Fabricante da solução
- 2.13.1.3.** Suporte Presencial
  - 2.13.1.3.1.** Assegurar o atendimento de suporte presencial previamente acordado nas seguintes situações críticas:
    - 2.13.1.3.2.** Migração de versionamento dos equipamentos gerenciados;



- 2.13.1.6.7.** Rever periodicamente as políticas e processos do SOC a fim de contribuir com a melhoria contínua da operação, de forma documentada e em conformidade com as melhores práticas do ITIL;
- 2.13.1.6.8.** Confeccionar e disponibilizar dashboards de acompanhamento em tempo real da operação do SOC que permitam a validação dos indicadores acordados;
- 2.13.1.6.9.** Apoio consultivo para melhoria contínua da segurança do ambiente;
- 2.13.1.6.10.** Confeção de relatórios técnicos pontuais sob demanda;
- 2.13.1.6.11.** Alinhamento e negociação dos indicadores de serviço;
- 2.13.1.6.12.** Desenvolvimento e manutenção do plano de comunicação;
- 2.13.1.7.** Canais para Comunicação
  - 2.13.1.7.1.** Ferramenta de service desk web;
  - 2.13.1.7.2.** E-mail;
  - 2.13.1.7.3.** Telefone.
- 2.13.1.8.** Ferramenta de Service Desk
  - 2.13.1.8.1.** Todas as solicitações deverão ocorrer, por meio da interface web site (portal do cliente) segura através de sistema próprio e que contenha as seguintes características:
    - 2.13.1.8.2.** Módulos de incidente/solicitação, requisição de mudança, eventos, problemas, ICs, Contratos, Clientes, Fornecedores, Empresas, SLAs, Criticidades, Analistas, Base de conhecimento, Usuários e Avisos;
    - 2.13.1.8.3.** Realizar notificações por e-mail;
    - 2.13.1.8.4.** Catálogo de Serviços;
    - 2.13.1.8.5.** Integração com a ferramenta de monitoramento;
    - 2.13.1.8.6.** Tenha certificação nos processos de Gerenciamento de Mudança; Gerenciamento de Evento, Gerenciamento de Incidente, Gerenciamento de conhecimento, Cumprimento de Requisição, Gerenciamento de Catálogo de Serviço, Gerenciamento de Nível de Serviço, Gerenciamento de Portfólio de Serviço, Gerenciamento de problema, Gerenciamento de ativo de Configuração e Ativo de Serviço.
  - 2.13.1.8.7.** O referido sistema de Service Desk da CONTRATADA permitirá o acompanhamento dos chamados em aberto bem como a consulta dos chamados já finalizados (BASE HISTÓRICA DE INCIDENTES) e validação do chamado antes do encerramento do mesmo.
  - 2.13.1.8.8.** As solicitações de serviço, sejam de suporte ou consultoria, só poderão ser realizadas pelos contatos cadastrados, através dos métodos abaixo, em qualquer horário do dia ou da noite, sem restrição.
- 2.13.1.9.** Horário de Atendimento
  - 2.13.1.9.1.** Remoto - Suporte e Monitoramento remoto pelos canais: telefônico, web ou e-mail em regime 24 horas por dia, 7 dias por

semana e 365 dias do ano (24x7) para incidentes e solicitações elegíveis de se resolver remotamente.

**2.13.1.9.2.** Presencial - Suporte presencial de incidentes e solicitações elegíveis de se resolver presencialmente.

**2.13.1.10.** Níveis de Serviços (Service Level Agreement – SLA)

<b>Criticidade</b>	<b>Atendimento Remoto</b>	<b>Prazo de Solução</b>	<b>Observações</b>
<b>Alta</b> Quando há indisponibilidade de uso de qualquer elemento da solução	Início de atendimento em até 02 (duas) horas em dias úteis e, sábados, domingos e feriados com prévio agendamento	6 (seis) horas	O tempo de atendimento remoto refere-se ao tempo para o profissional da CONTRATADA entrar em contato com o suporte do cliente e serão considerados a partir da abertura dos chamados.
<b>Média</b> Quando há falha simultânea ou não de qualquer elemento da solução, porem apresentando problemas	Início de atendimento em até 04 (quatro) horas.	8 (oito) horas	Após o 1.º retorno e a devida análise do problema, a severidade poderá ser redefinida pela CONTRATADA.
<b>Baixa</b> Revisão de documentação, configurações e outras atividades que não causem impacto em qualquer funcionalidade da solução	Início de atendimento em até 1(um) dia útil.	2 (dois) dias uteis	

**2.13.2.** que o licitante é uma revenda autorizada a comercializar e dar suporte na solução.

### **3 . CRONOGRAMA FÍSICO FINANCEIRO**

**Itens 1 a 5**

**Pagamento após a entrega definitiva da solução.**

**Itens 6 a 8**

**Pagamento após a implantação do projeto todo**

Rio de janeiro 28 de abril de 2020,

**Renato L. Stavale**

**Matr. 308.350-8**

**Subdiretoria Geral de Informática**